WANrockIT

Setup Guide

Eli-v6.5.391

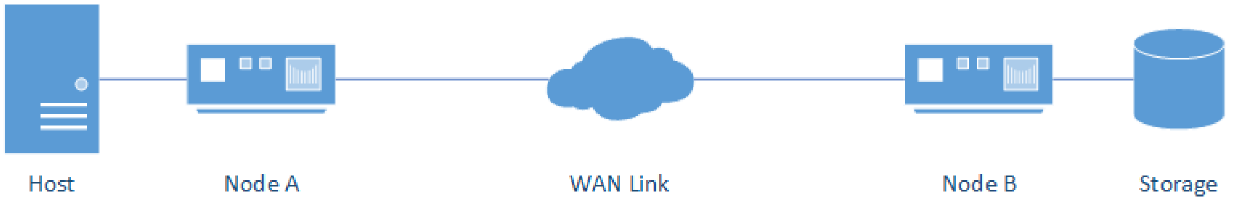
Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

1 Getting Started

The Bridgeworks latency mitigating technology allows you to accelerate your network traffic between two different sites. Each site will require a WANrockIT Node to accelerate your desired traffic. These nodes are available as physical hardware appliances.

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



This guide will take you through the steps necessary to set up this simple installation. You can then tailor your setup using the skills you have learnt from this guide. If you require any further information please refer to the User Manuals for more detailed information about a particular part of your setup.

2 Guide Layout

This guide is divided into a series of ordered steps that should be followed through in order. If at any point you run into trouble with a step, please refer to the Useful Links section at the end of this document.

The steps to be followed are listed below. It is recommended to print this list of steps out and check off each step when you have completed it:

□ Step 1. Initial Setup of your Bridgeworks Node

□ Step 2. Configuring Optional Feature Cards

□ Step 3. Configuring your WANrockIT Node to Present iSCSI Targets to an Off-Premise Site

□ Step 4. Configuring IPsec

□ Step 5. Establishing a Link Between Nodes

□ Step 6. Configuring your WANrockIT Node to Present iSCSI Targets from Off-Premise to On-Premise

□ Step 7. Refreshing iSCSI targets through your WAN link

3 Initial Setup of your Bridgeworks Node

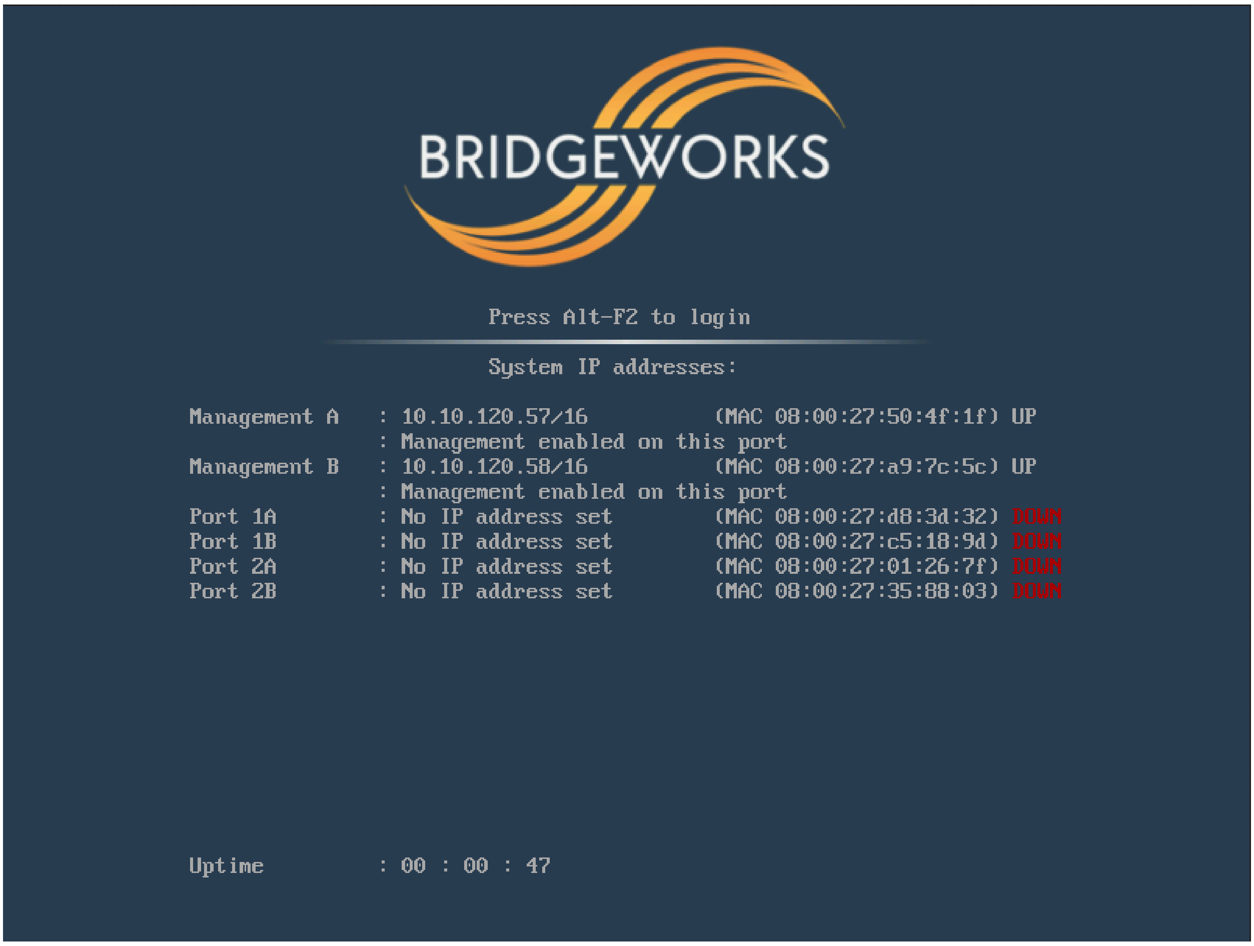
3.1 Finding Management IP addresses

The default management interfaces on hardware appliances will be named Management A and Management B, and both will have DHCP enabled by default.

You can enable or disable management capabilities on a per-port basis using the Port Mappings page, see Port Mappings (🔑) for more information.

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

To find the IP addresses of management interfaces easily, it is recommended to use the VGA or virtual console as shown below.

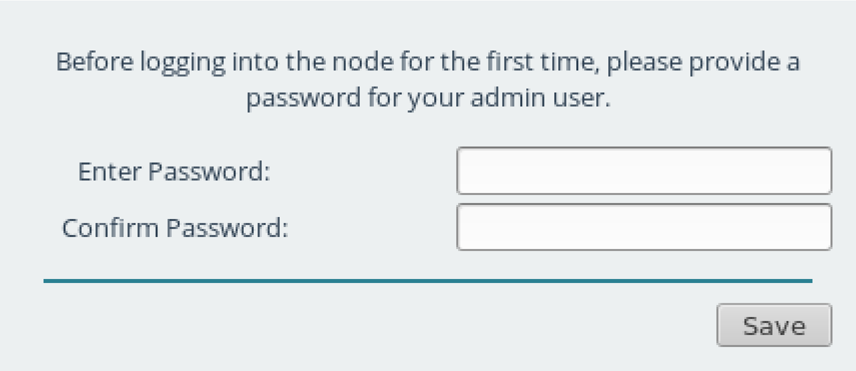


```
                         Press Alt-F2 to login

                         System IP addresses:

Management A   : 10.10.120.57/16          (MAC 08:00:27:50:4f:1f) UP
               : Management enabled on this port
Management B   : 10.10.120.58/16          (MAC 08:00:27:a9:7c:5c) UP
               : Management enabled on this port
Port 1A        : No IP address set        (MAC 08:00:27:d8:3d:32) DOWN
Port 1B        : No IP address set        (MAC 08:00:27:c5:18:9d) DOWN
Port 2A        : No IP address set        (MAC 08:00:27:01:26:7f) DOWN
Port 2B        : No IP address set        (MAC 08:00:27:35:88:03) DOWN






Uptime         : 00 : 00 : 47
```

3.2 First Time Login

Proceed to the web interface of the Node by entering the IP address of one of the Management enabled interfaces in to the address bar of your web browser.

On first access, the web interface displays an initial login page that requires a password to be set for the admin user account of the Node.



Before logging into the node for the first time, please provide a password for your admin user.

Enter Password:

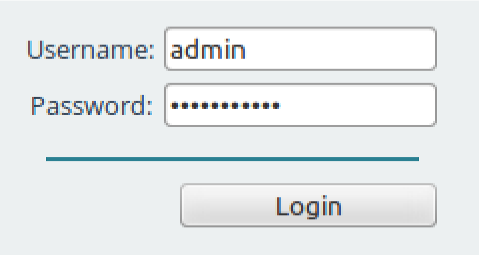
Confirm Password:

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.

The passwords typed in to the two provided fields must match. Passwords must be a minimum of 5 characters and a maximum of 64 characters in length.

3.3 Logging into the Node

When a valid password is submitted, you are redirected to the login screen. To access the *Node Management Console*, enter the login credentials with the admin username and the password set previously.

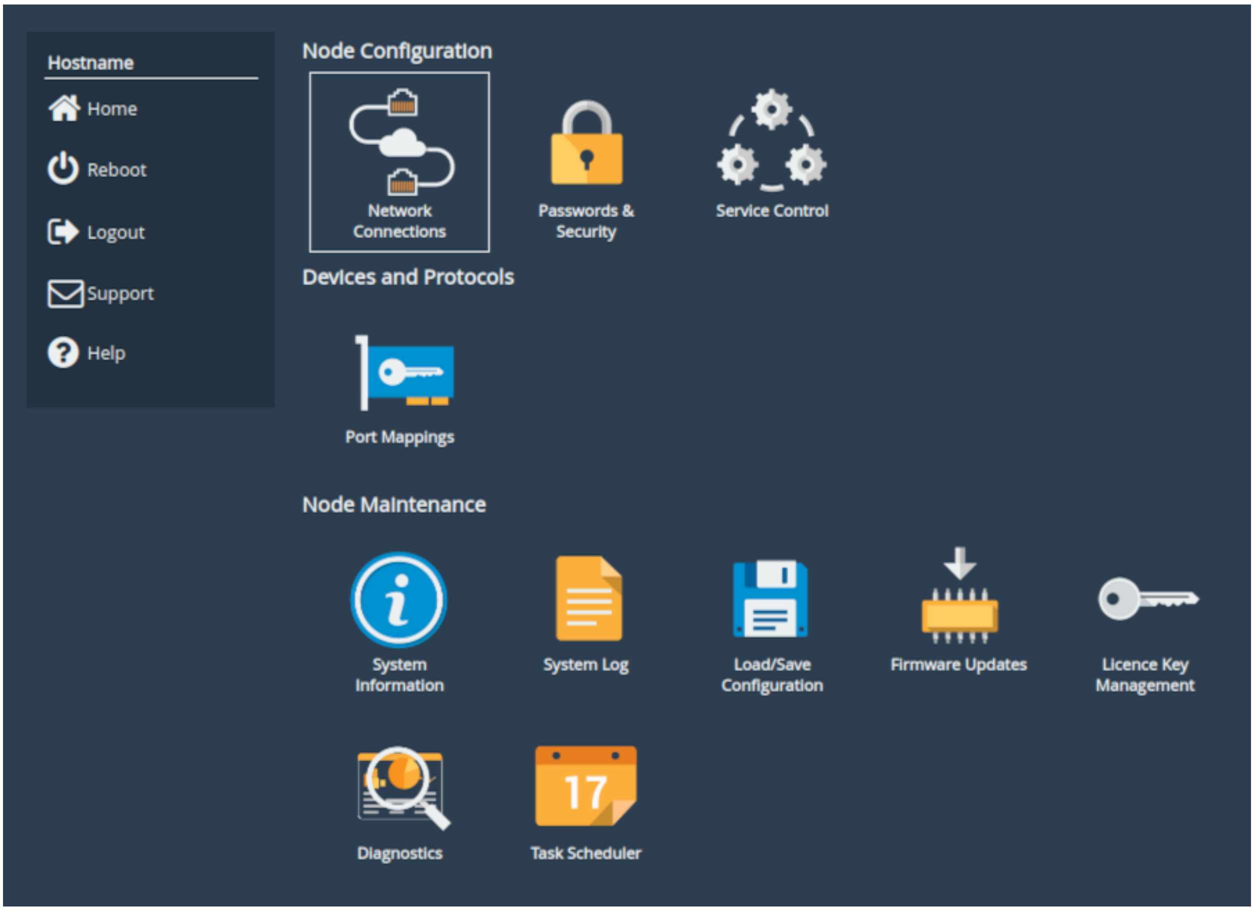


Username: admin

Password: ••••••••••••

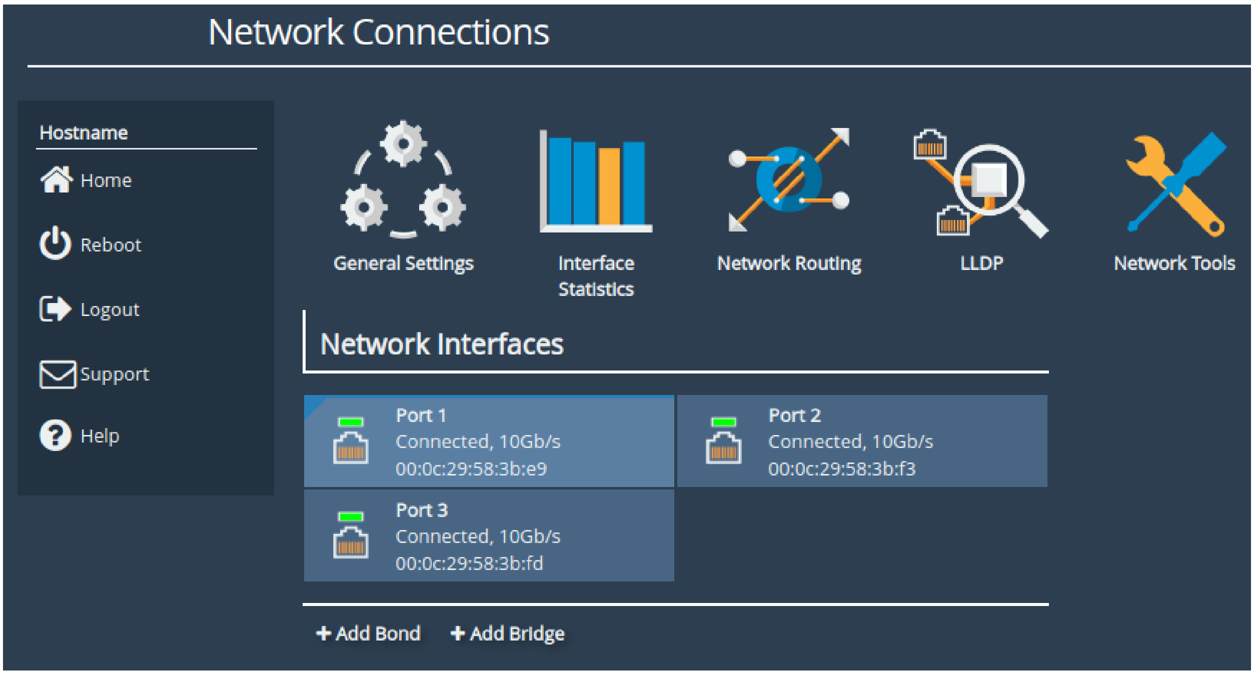
3.4 Network Connections ( )

The *Network Connections* page allows for the configuration of static IP addresses, and changing the hostname of the Node. To change the settings click the *Network Connections* icon as shown below.



3.4.1 Setting the Hostname/Node Name

Click on the *General Settings* icon on the *Network Connections* page as shown below.

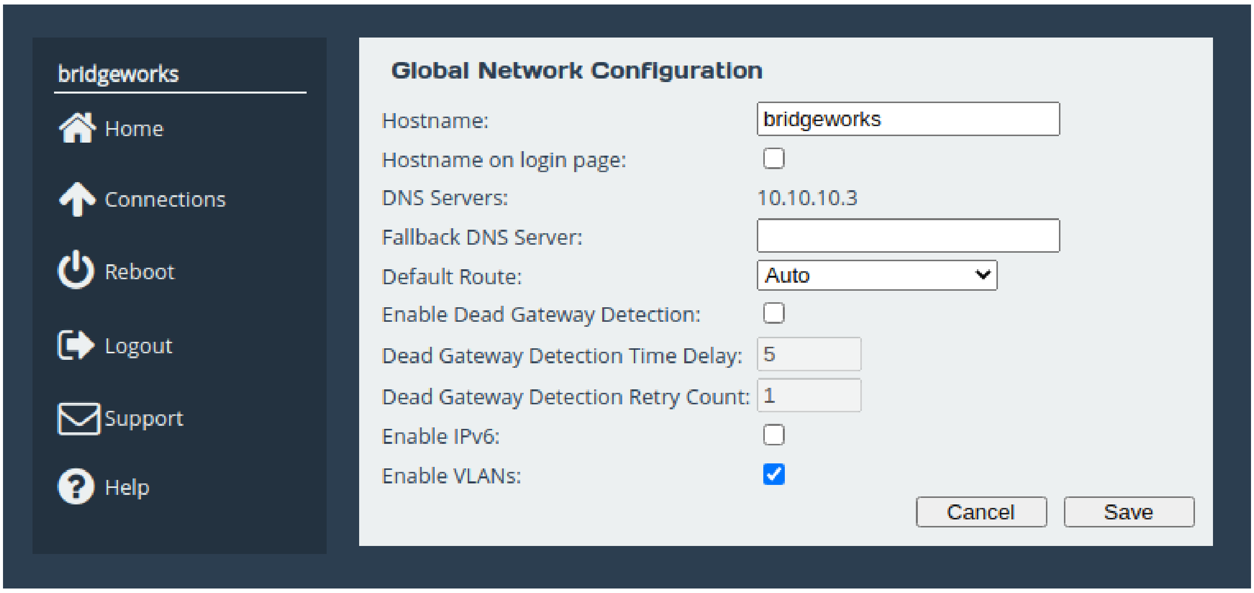


Port 1
Connected, 10Gb/s
00:0c:29:58:3b:e9

Port 2
Connected, 10Gb/s
00:0c:29:58:3b:f3

Port 3
Connected, 10Gb/s
00:0c:29:58:3b:fd

The hostname of the Node can be changed by replacing the default name `bridgeworks` with a name of your choice. This name is also the alias name used for identifying your Nodes under the *Node Management* section.



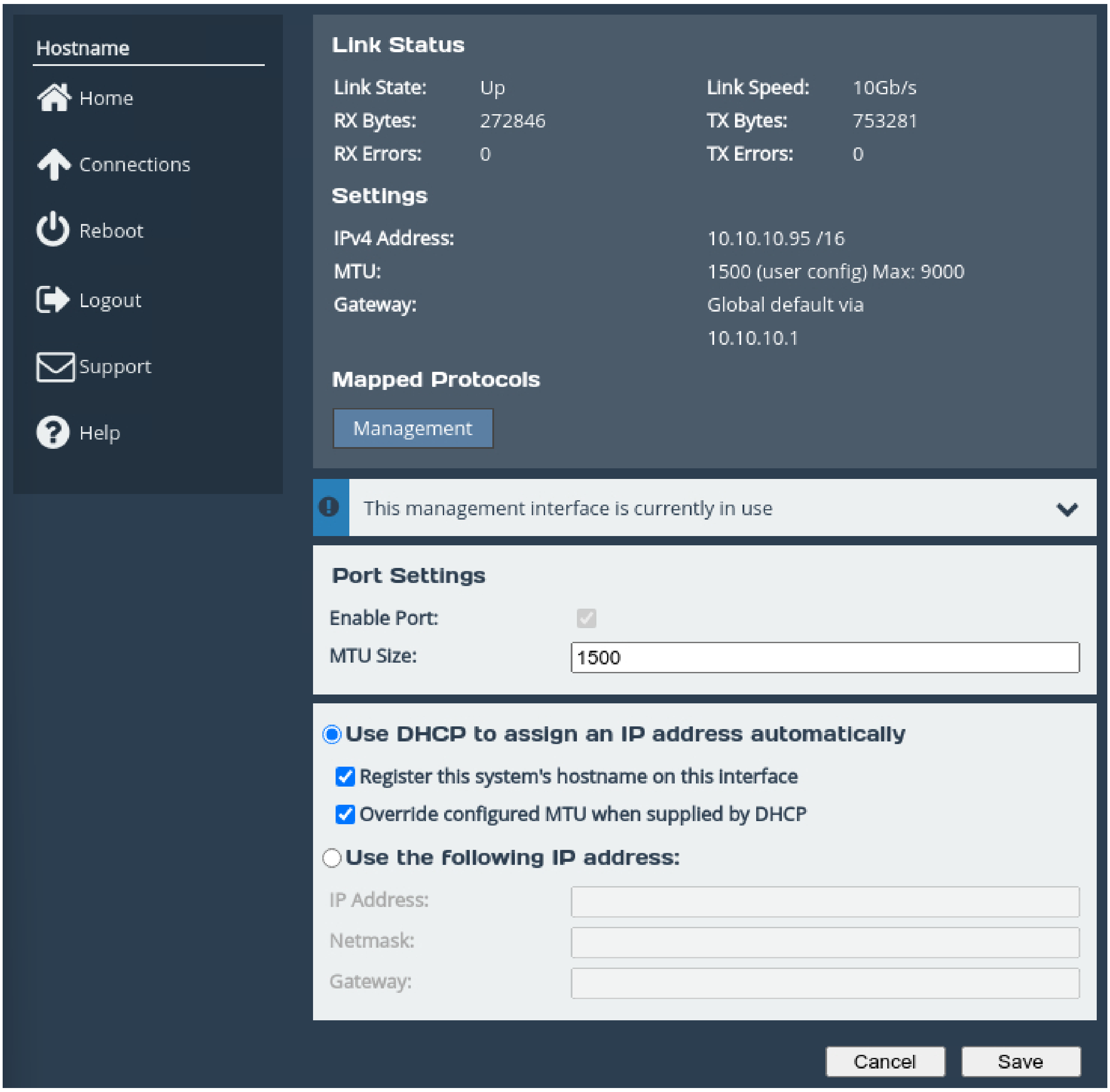
Global Network Configuration

Hostname:	bridgeworks
Hostname on login page:	□
DNS Servers:	10.10.10.3
Fallback DNS Server:	
Default Route:	Auto
Enable Dead Gateway Detection:	□
Dead Gateway Detection Time Delay:	5
Dead Gateway Detection Retry Count:	1
Enable IPv6:	□
Enable VLANs:	☑

When you have changed the hostname, click the *Save* button; A reboot is required for the change to take effect.

3.4.2 Configuring a Port

Icons representing each port are displayed underneath the *Network Interfaces* heading, alongside a summary of its current state. Clicking on a port leads to the port settings page.



Link Status

Link State:	Up	Link Speed:	10Gb/s
RX Bytes:	272846	TX Bytes:	753281
RX Errors:	0	TX Errors:	0

Settings

IPv4 Address:	10.10.10.95 /16
MTU:	1500 (user config) Max: 9000
Gateway:	Global default via 10.10.10.1

Mapped Protocols

This management interface is currently in use

Port Settings

Enable Port: ☑

MTU Size: 1500

● **Use DHCP to assign an IP address automatically**

☑ Register this system's hostname on this interface

☑ Override configured MTU when supplied by DHCP

○ **Use the following IP address:**

IP Address:

Netmask:

Gateway:

A disabled port will initially need to be enabled by selecting the *Enable Port* checkbox. This will bring the port online and allow you to edit its settings. A reboot will be required for the change to take effect.

For ports that have a WAN protocol mapped there will be an *Enable Forwarding* checkbox. This option enables IP forwarding which allows non-accelerated, non-VPN traffic received on the port not destined for the WANrockIT to be forwarded. Changes to IP forwarding do not require a reboot to take effect.

3.4.3 Changing IP Addresses

To manually assign an IP address to a port, select the radio button *Use the following IP address*. The fields *IP Address*, *Netmask* and *Gateway* are now available to be filled in. When all fields are complete, click the *Save* button. A reboot is required for the changes to take effect.

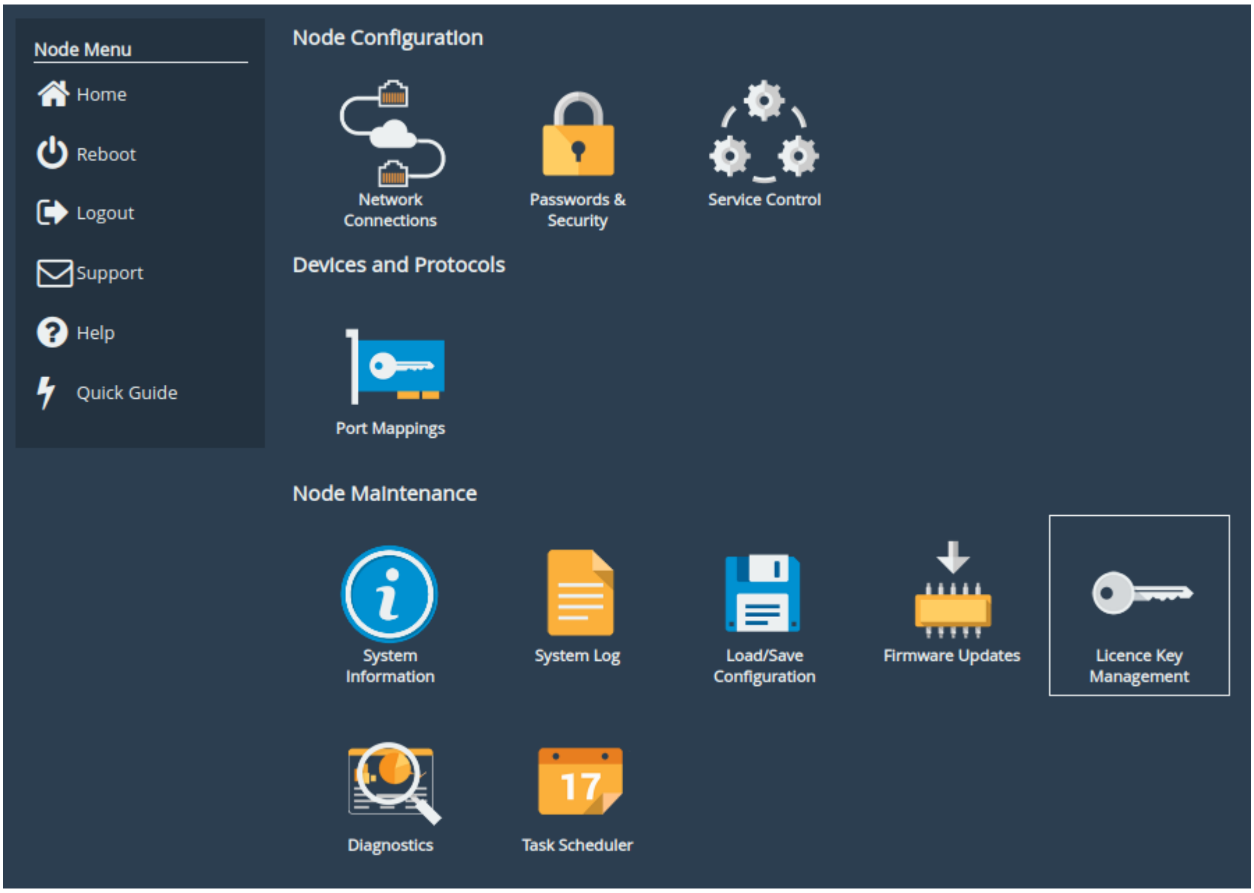
3.5 Licence Keys

All PORTrockIT and WANrockIT products require a licence key in order to unlock the acceleration features of the product.

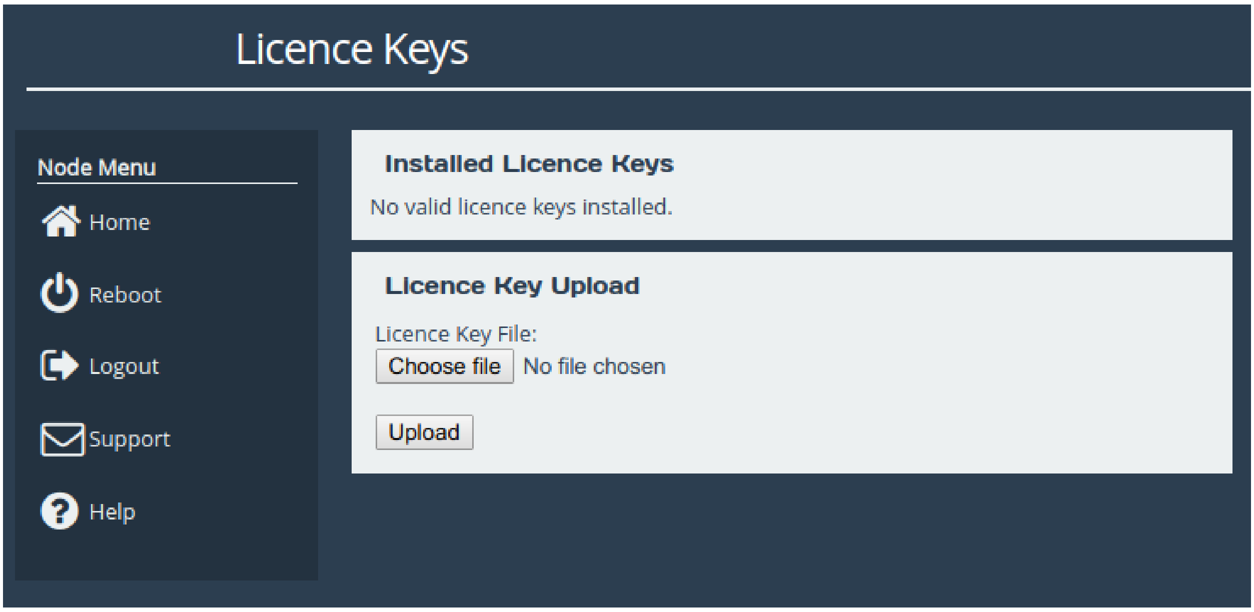
To determine whether there is a valid licence key, log into the Node and navigate to the *Licence Key Management* page. If the page displays *No valid licence keys installed* then you must obtain a licence key to unlock the Node's features. If you do not have a licence key or can no longer locate your key, please contact support@4bridgeworks.com.

3.5.1 Uploading a Licence Key

Once you have received the licence key, log into the web interface of the Node and go to the *Licence Key Management* page.



Click the *Choose file* button and select the licence key to upload.



Licence Keys

Installed Licence Keys

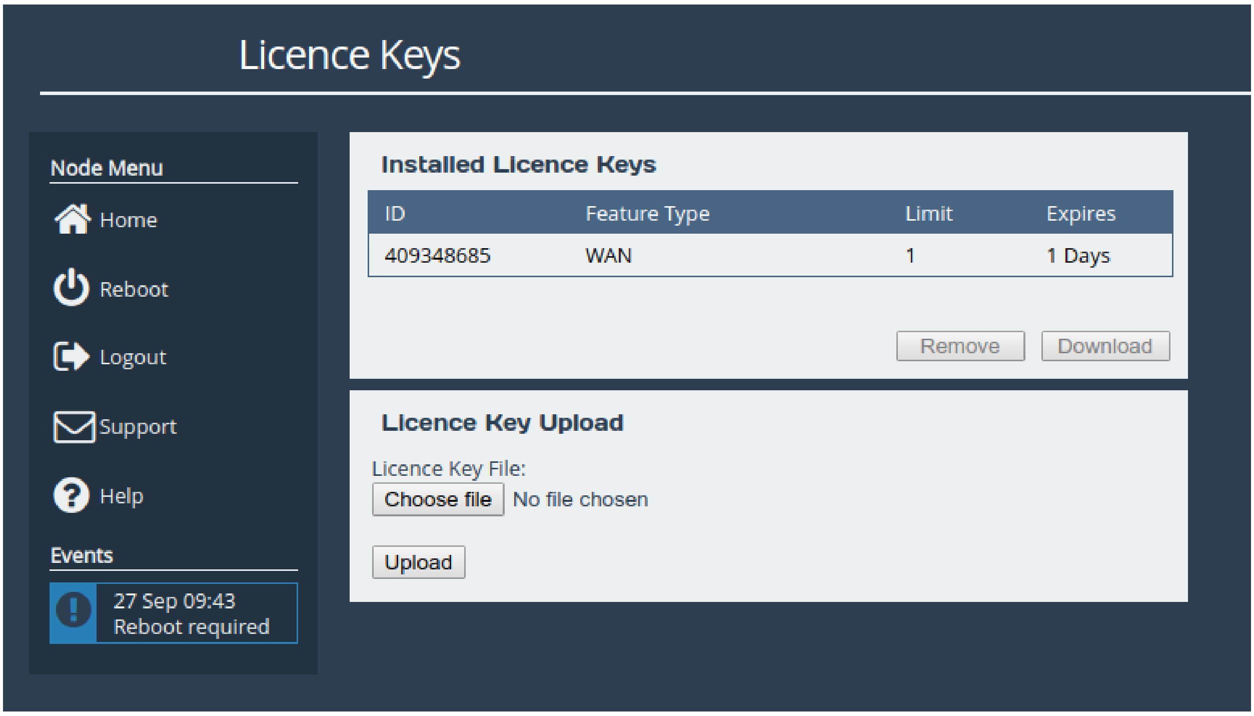
No valid licence keys installed.

Licence Key Upload

Licence Key File:

No file chosen

Click the *Upload* button. The licence key will appear in the table along with the length of time it will remain active.



Licence Keys

27 Sep 09:43
Reboot required

Installed Licence Keys

ID	Feature Type	Limit	Expires
409348685	WAN	1	1 Days

Licence Key Upload

Licence Key File:

No file chosen

A reboot is required for the licence key to take effect.

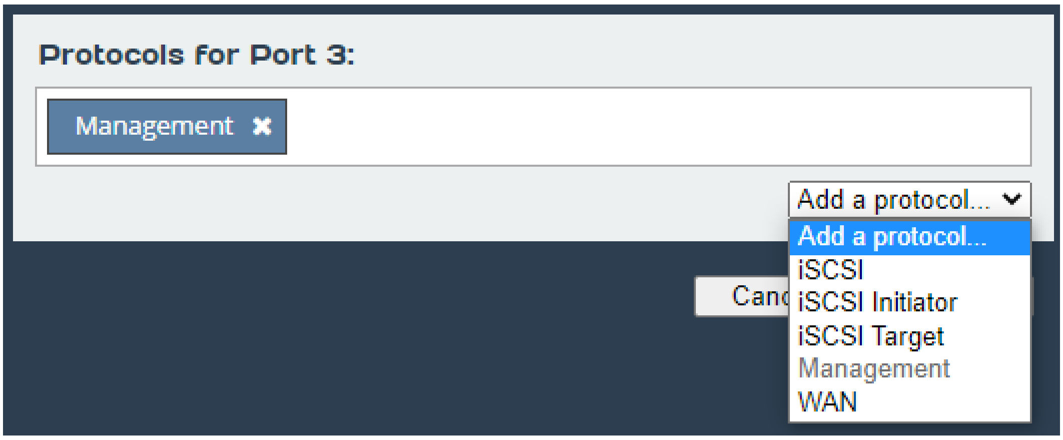
3.6 Port Mappings ( )

3.6.1 Overview

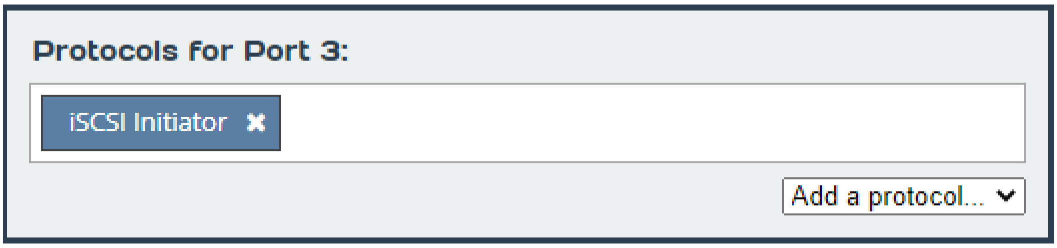
Port Mappings allows for the assignment of protocols to network interfaces. For example, adding *WAN* to a port will allow WAN connections and acceleration from that network port. For example, enabling iSCSI provides an iSCSI initiator and iSCSI target, used for sending and receiving iSCSI traffic between hosts and devices.

3.6.2 Setting Port Mappings

To assign a protocol to a network interface, select the desired protocol from the drop-down list underneath the port to which it should be assigned. Note that the protocol options will vary between PORTrockIT and WANrockIT Nodes.



After selecting a valid protocol from the drop-down list, the name of the protocol appears within a blue box underneath the port.



A mapping can be removed by clicking on the X next to the name of the protocol.

Once the configuration is complete, click on the *Save* button. A reboot is required for the changes to take effect.

4 Configuring Optional Feature Cards

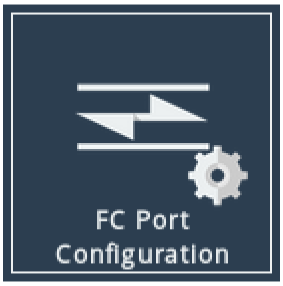
4.1 Introduction

This section describes how to configure optional feature cards in your WANrockIT.

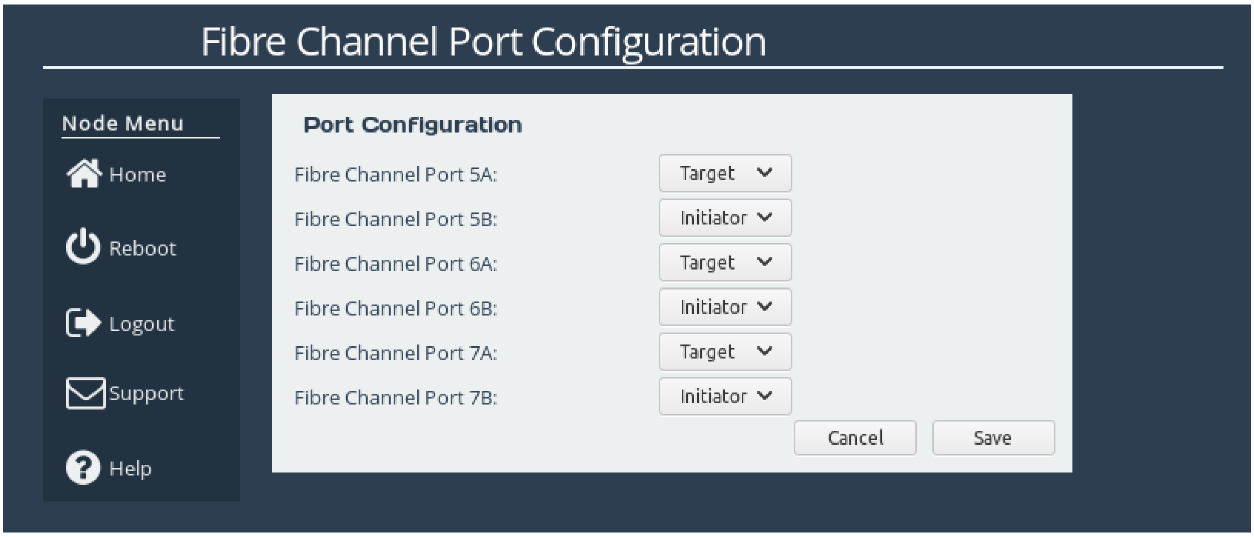
4.2 Fibre Channel Port Configuration

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

To designate whether a port is a target or an initiator, from the Home screen of the web interface, select the *FC Port Configuration* icon in the *Devices and Protocols* section.



You will see the following page:



Fibre Channel Port Configuration

Port Configuration

Fibre Channel Port 5A:	Target
Fibre Channel Port 5B:	Initiator
Fibre Channel Port 6A:	Target
Fibre Channel Port 6B:	Initiator
Fibre Channel Port 7A:	Target
Fibre Channel Port 7B:	Initiator

To change a port between a target or initiator use the drop down box next to the desired port and click on the *Save* button. Clicking *Cancel* will not save any changes made on the page.

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

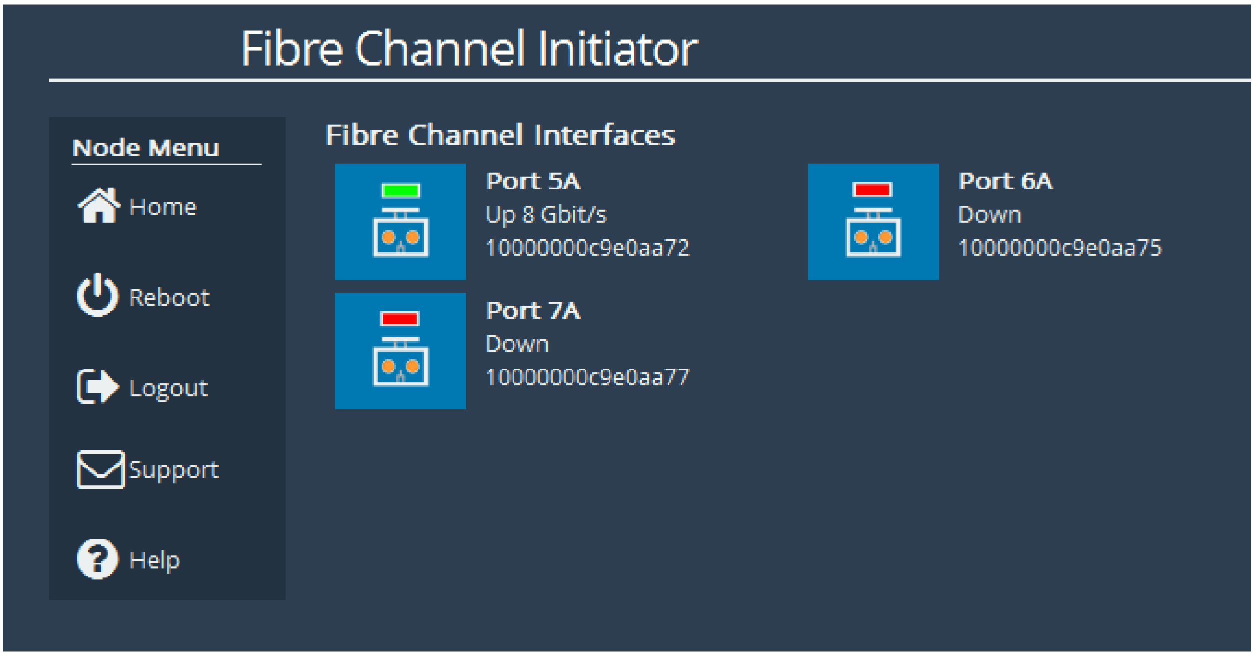
4.3 Fibre Channel Initiator Connections

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

This configuration page allows you to configure ports designated as Fibre Channel Initiator interfaces. To designate a Fibre Channel port as an initiator, see Section 4.2: Fibre Channel Port Configuration.

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

You will see the following page:



Fibre Channel Initiator

Fibre Channel Interfaces

Port 5A
Up 8 Gbit/s
10000000c9e0aa72

Port 6A
Down
10000000c9e0aa75

Port 7A
Down
10000000c9e0aa77

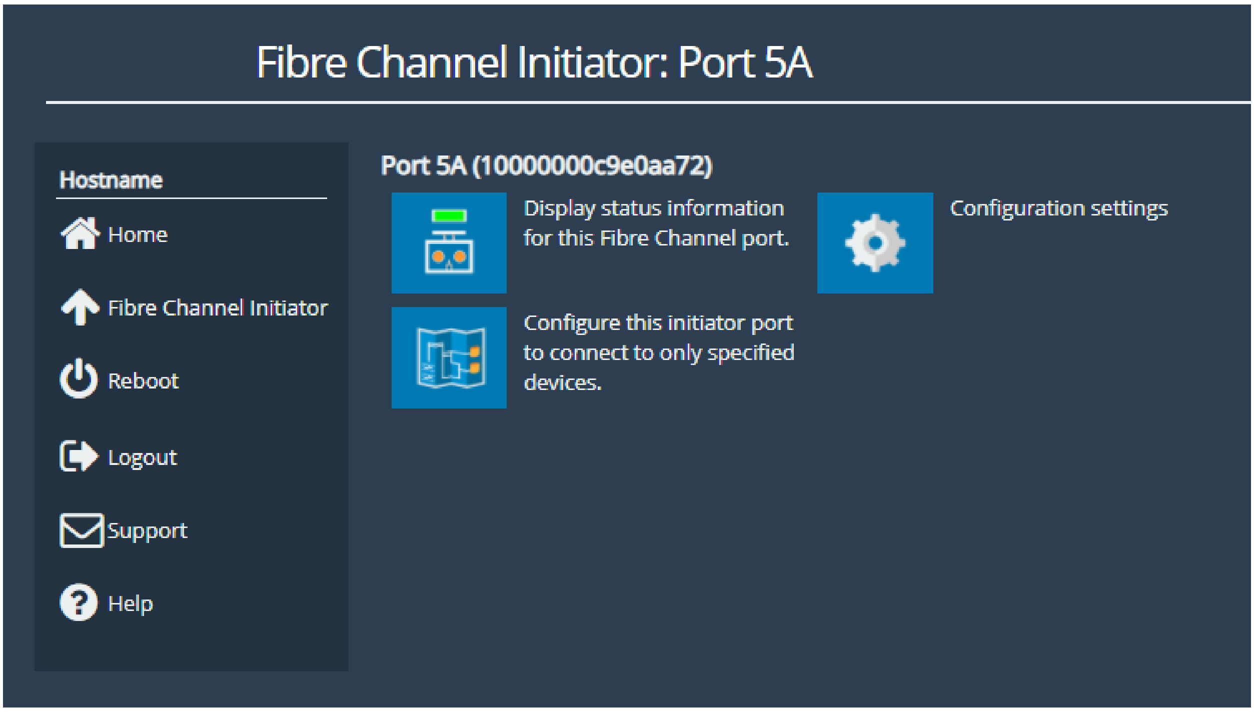
This page lists each Fibre Channel port which has been designated as an initiator. Three pieces of information are displayed about each port next to an icon. In order they are:

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

Current state This shows whether the Fibre Channel link for this port is up or down, and the speed of the link if it is currently up.

WWPN The unique World Wide Name identifier for this port.

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


Fibre Channel Initiator: Port 5A

Port 5A (10000000c9e0aa72)

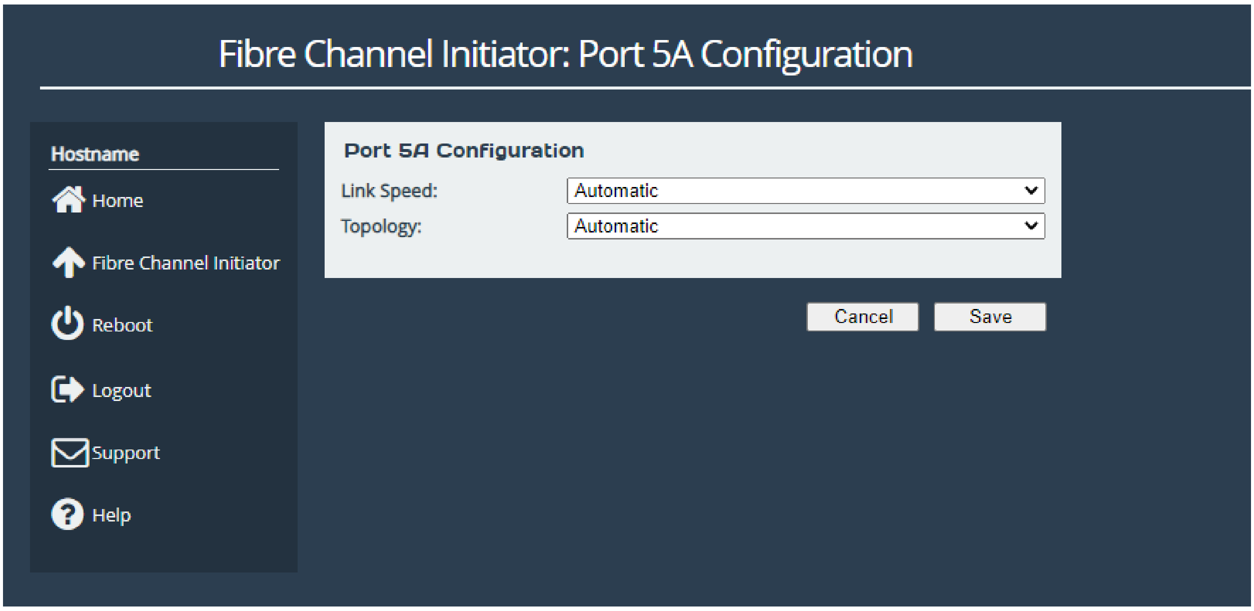
Display status information for this Fibre Channel port.

Configuration settings

Configure this initiator port to connect to only specified devices.

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

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


Fibre Channel Initiator: Port 5A Configuration

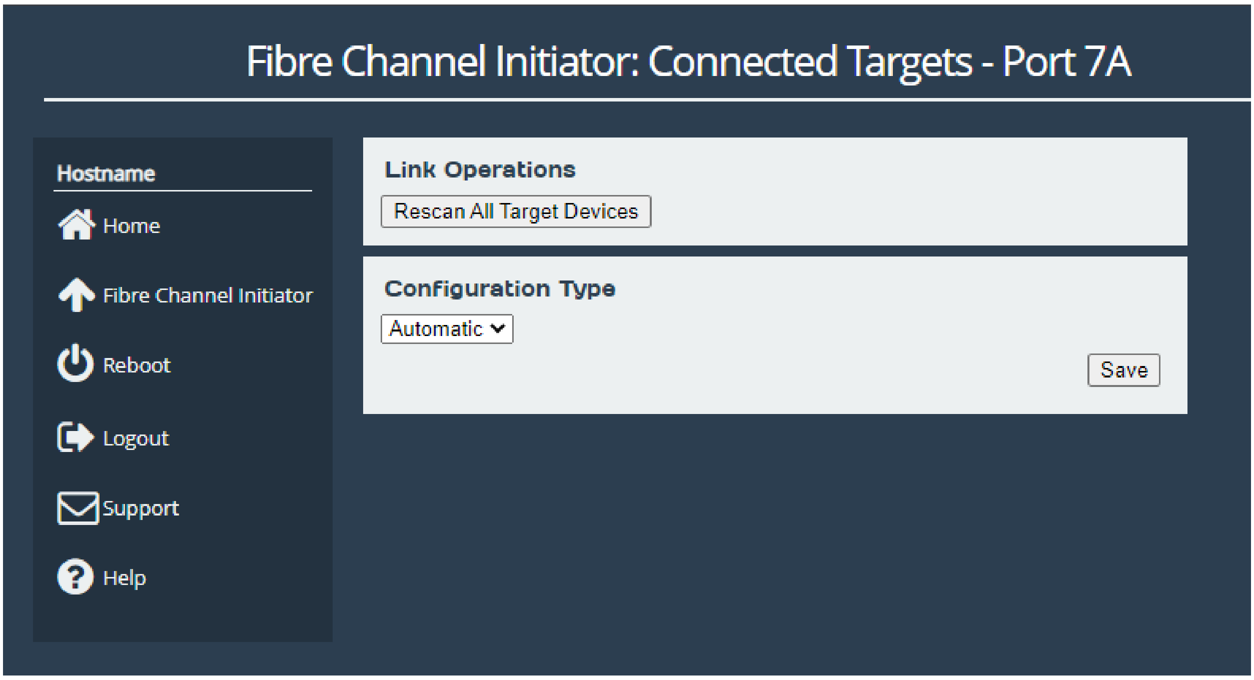
Port 5A Configuration

Link Speed: Automatic

Topology: Automatic

1. The *Link Speed* can be set to *Automatic* or one of the speeds supported by the Fibre Channel port. In most cases this option may be left set to *Automatic*. If you are unsure, set the link speed to the SFP speed. This option is not available on some products.
2. The *Topology* pull down menu has 3 options: *Automatic*, *Loop (arbitrated Loop, FC-AL)*, and *Point-to-Point (FC-P2P)*. It is recommended that you leave this option at *Automatic* unless you wish to force the link into a known topology.

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



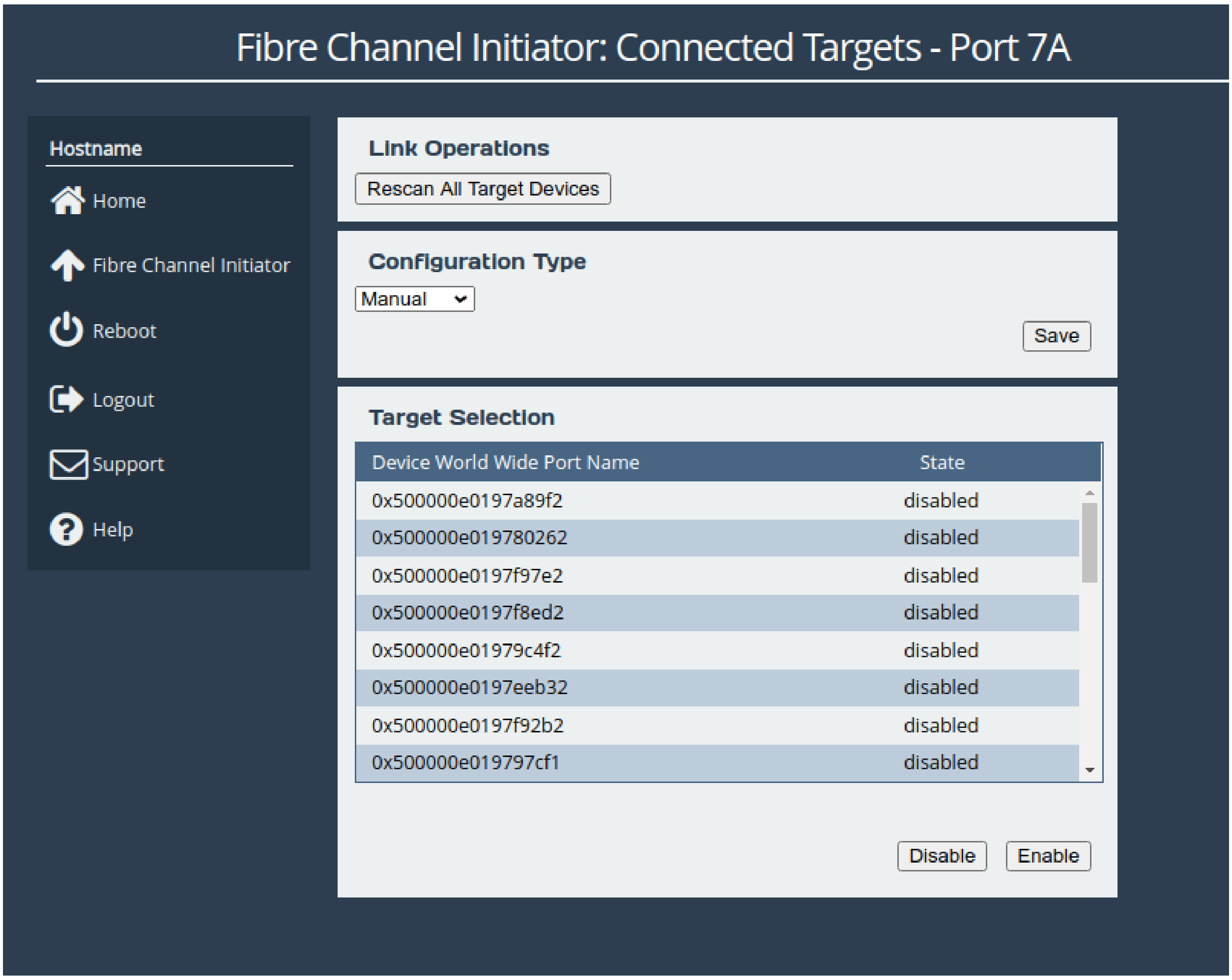
Fibre Channel Initiator: Connected Targets - Port 7A

Link Operations

Configuration Type

Automatic

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



Fibre Channel Initiator: Connected Targets - Port 7A

Configuration Type: Manual

Device World Wide Port Name	State
0x500000e0197a89f2	disabled
0x500000e019780262	disabled
0x500000e0197f97e2	disabled
0x500000e0197f8ed2	disabled
0x500000e01979c4f2	disabled
0x500000e0197eeb32	disabled
0x500000e0197f92b2	disabled
0x500000e019797cf1	disabled

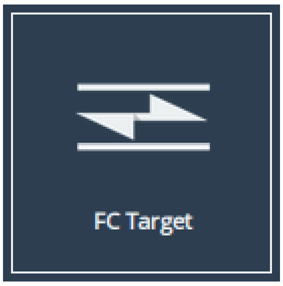
Select the FC target by clicking on its World Wide Port Name, and then click *Enable* or *Disable*.

4.4 Fibre Channel Target Connections

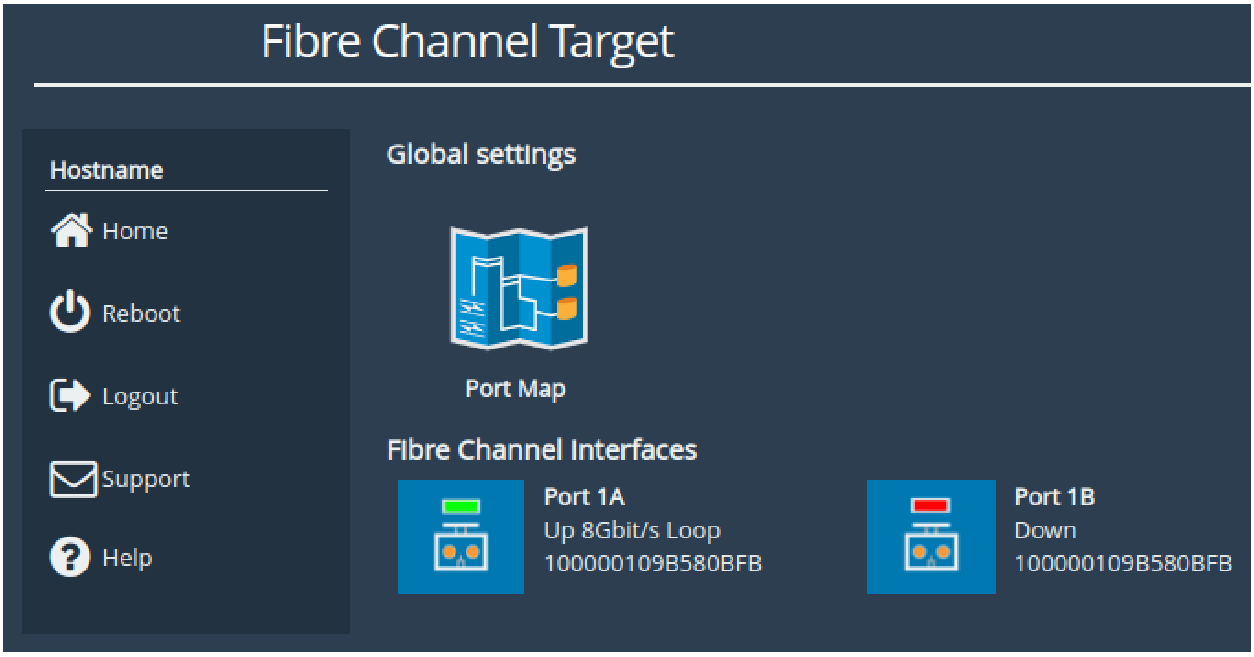
Note: You may skip reading this section if your WANrockIT does not have a Fibre Channel feature card installed.

This configuration page allows you to configure ports designated as Fibre Channel Target interfaces. To designate a Fibre Channel port as a target, see Section 4.2: Fibre Channel Port Configuration.

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



The web interface will then display the following:



Fibre Channel Target

Global settings

Fibre Channel Interfaces

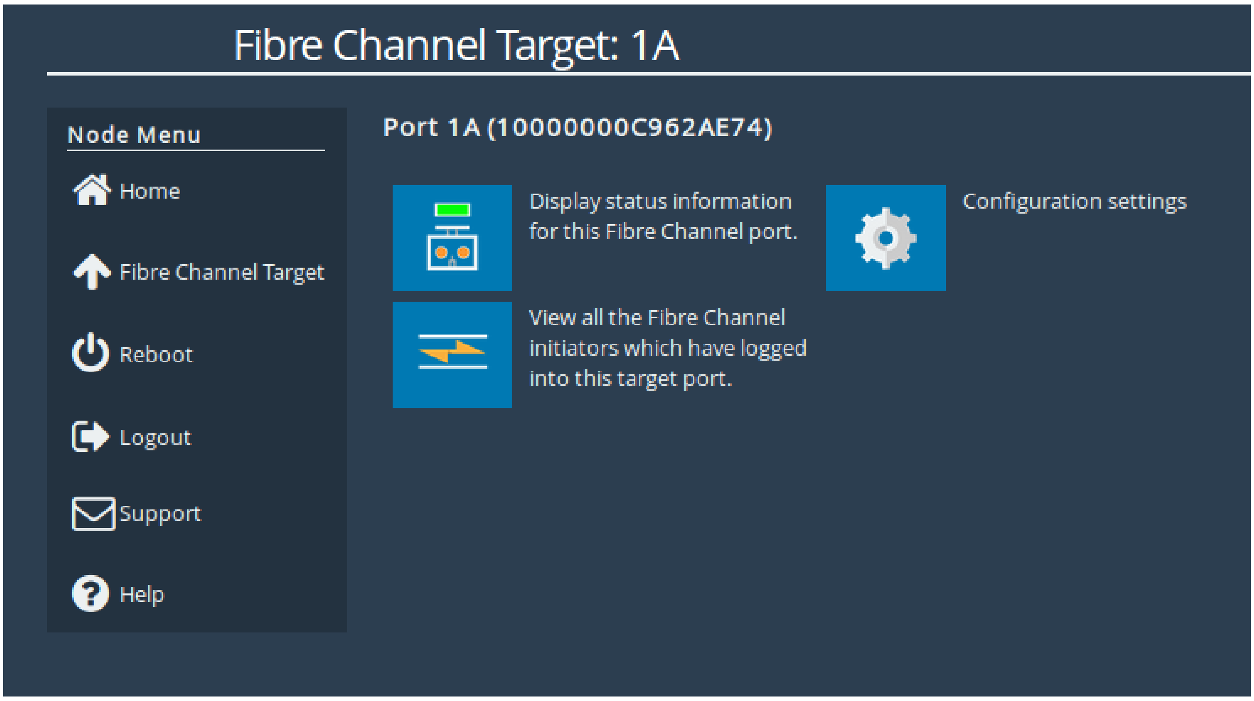
Port 1A
Up 8Gbit/s Loop
100000109B580BFB

Port 1B
Down
100000109B580BFB

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

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

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



Fibre Channel Target: 1A

Port 1A (10000000C962AE74)

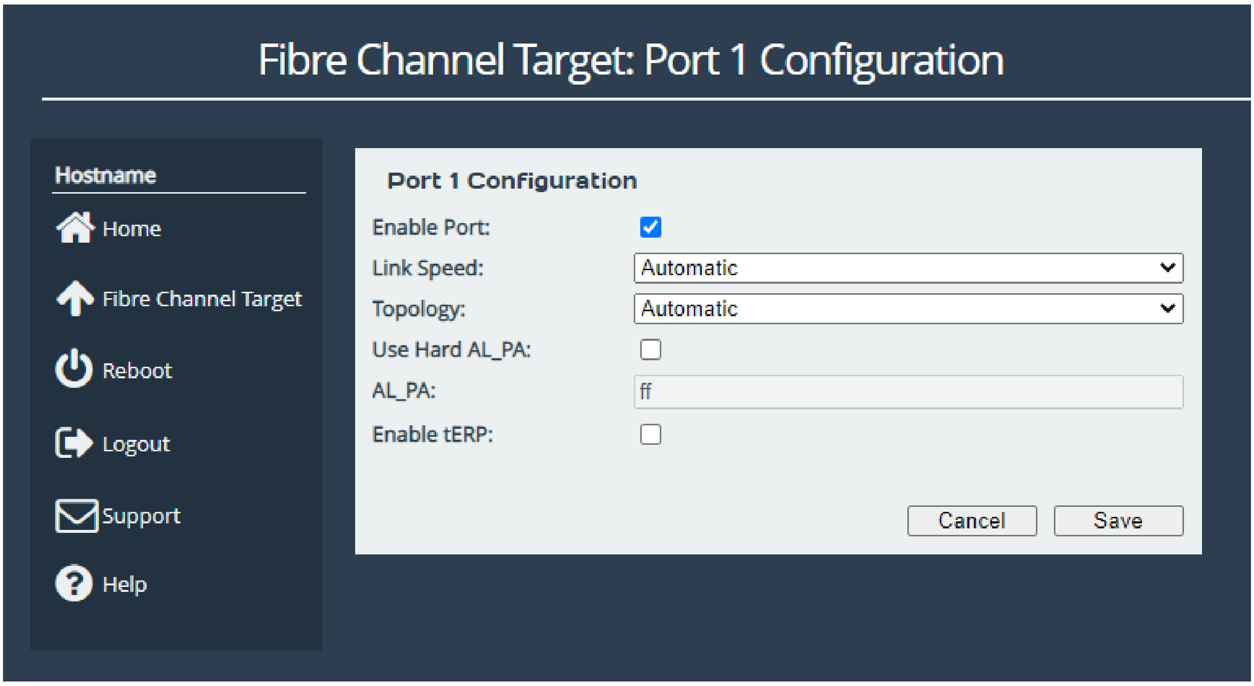
Display status information for this Fibre Channel port.

Configuration settings

View all the Fibre Channel initiators which have logged into this target port.

4.4.1 Port Configuration

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



Fibre Channel Target: Port 1 Configuration

Port 1 Configuration

Enable Port: ☑

Link Speed: Automatic

Topology: Automatic

Use Hard AL_PA: ☐

AL_PA: ff

Enable tERP: ☐

The first parameter is the *Enable Port* check box. This can be selected to enable the link onto the Fibre Channel Storage Area Network (SAN).

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

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

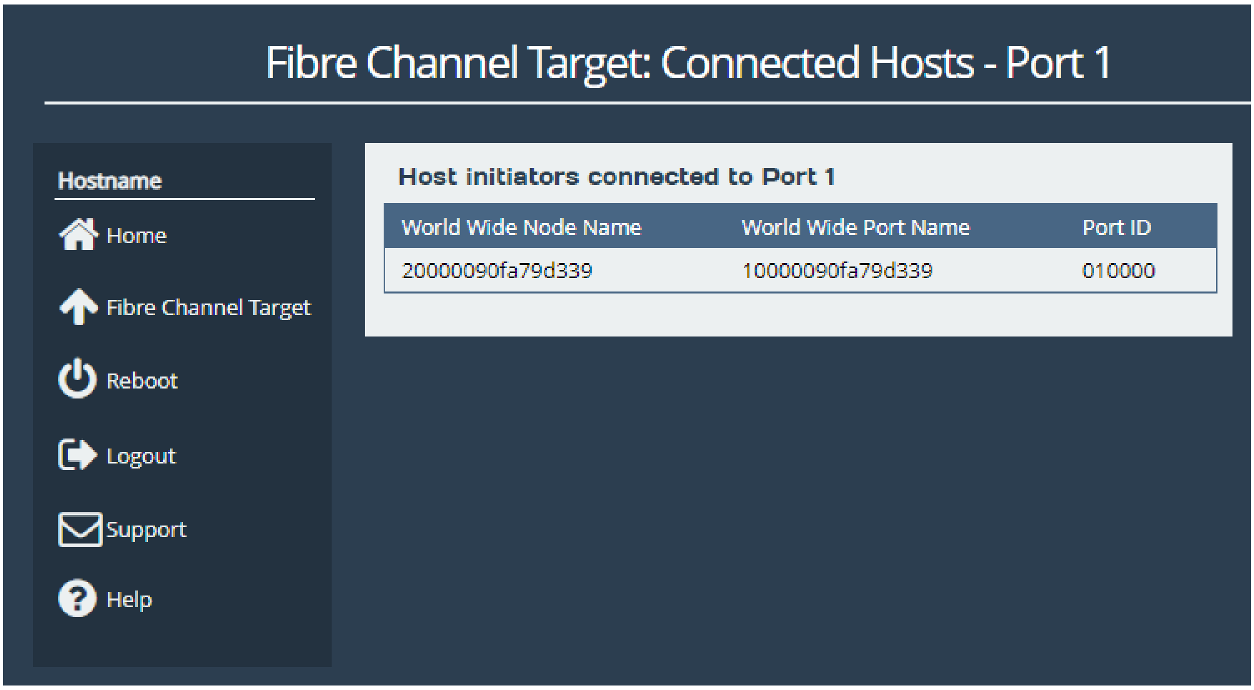
Note: It is recommended to leave *Hard AL_PA* unchecked unless you are familiar with the lower levels of the Fibre Channel protocol, as certain AL_PA addresses are reserved.

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

Clicking *Save* will save the configuration. A reboot is required for the changes to take effect.

4.4.2 Connected Hosts

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



Fibre Channel Target: Connected Hosts - Port 1

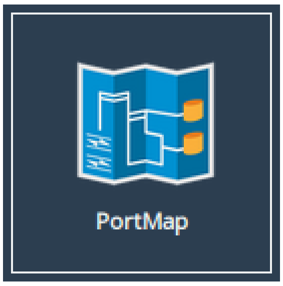
Host initiators connected to Port 1

World Wide Node Name	World Wide Port Name	Port ID
20000090fa79d339	10000090fa79d339	010000

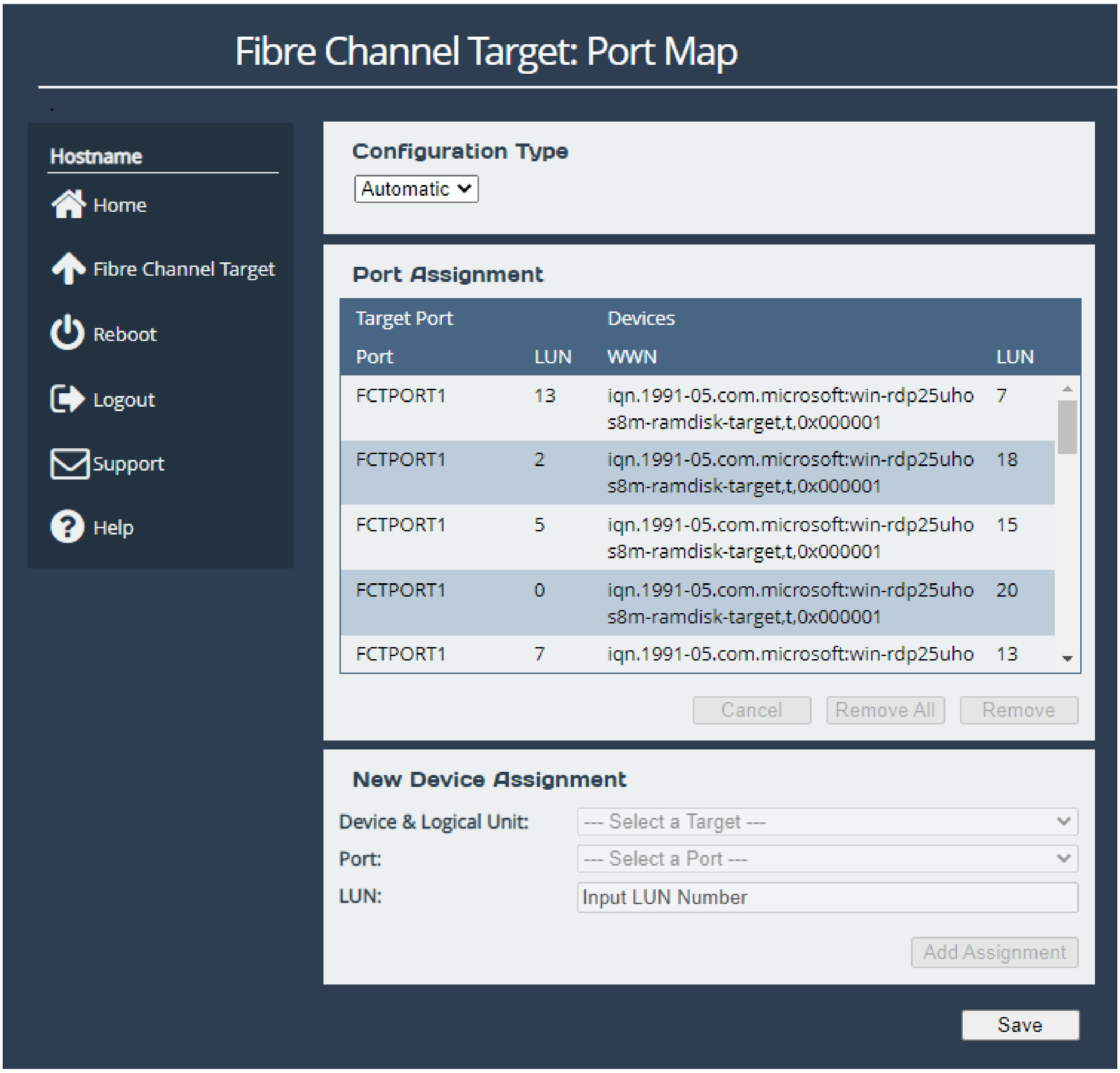
4.4.3 Port Map

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

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



A screen similar to the following will be displayed:



Fibre Channel Target: Port Map

Configuration Type

Automatic

Port Assignment

Target Port		Devices	
Port	LUN	WWN	LUN
FCTPORT1	13	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	7
FCTPORT1	2	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	18
FCTPORT1	5	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	15
FCTPORT1	0	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	20
FCTPORT1	7	iqn.1991-05.com.microsoft:win-rdp25uho	13

New Device Assignment

Device & Logical Unit: --- Select a Target ---

Port: --- Select a Port ---

LUN: Input LUN Number

There are two modes of operation:

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

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

When switching between modes, all changes are held pending until you select *Save*.

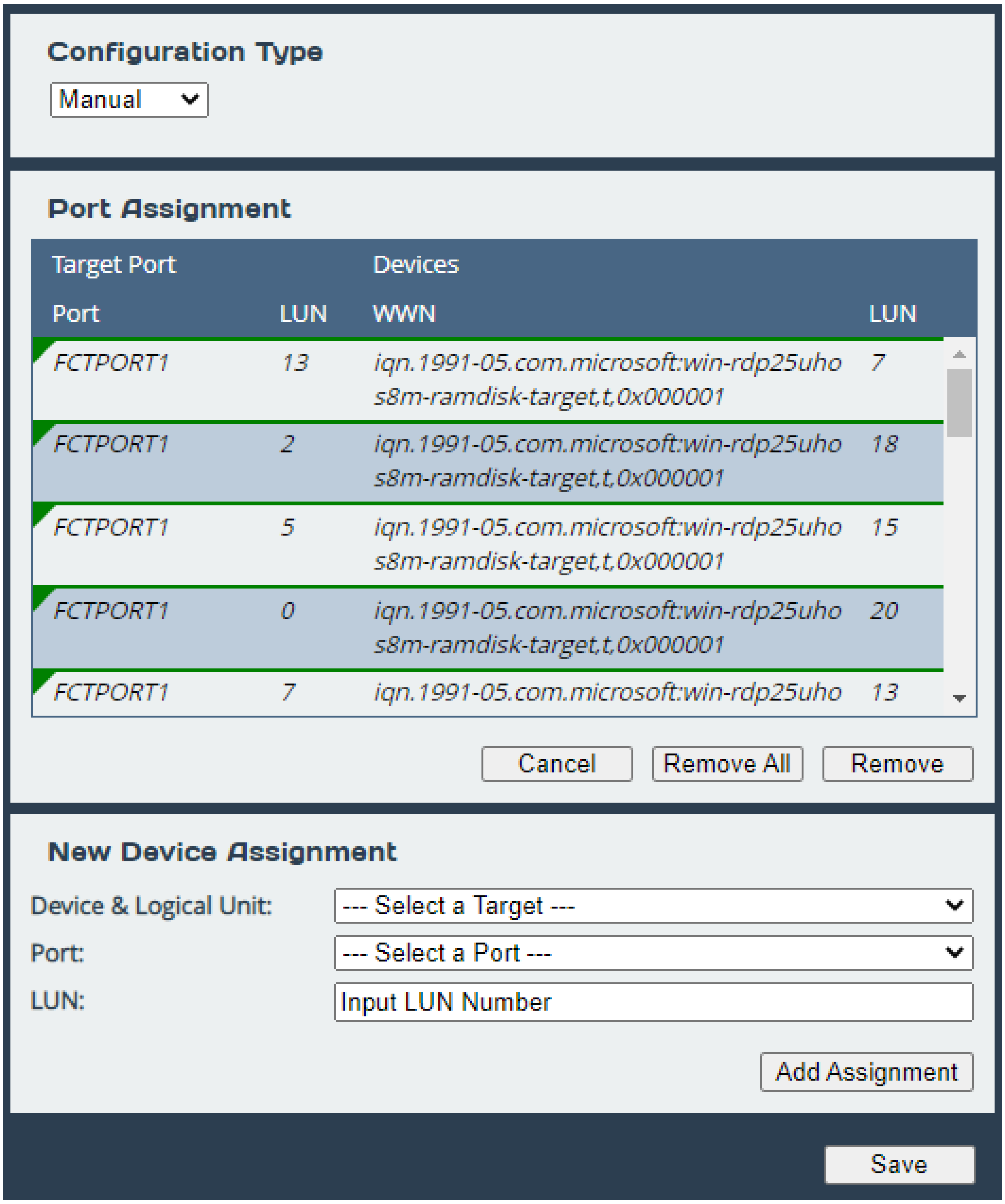
4.4.3.1 Automatic

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

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

4.4.3.2 Manual

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



Configuration Type

Manual

Port Assignment

Target Port		Devices	
Port	LUN	WWN	LUN
FCTPORT1	13	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	7
FCTPORT1	2	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	18
FCTPORT1	5	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	15
FCTPORT1	0	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	20
FCTPORT1	7	iqn.1991-05.com.microsoft:win-rdp25uho	13

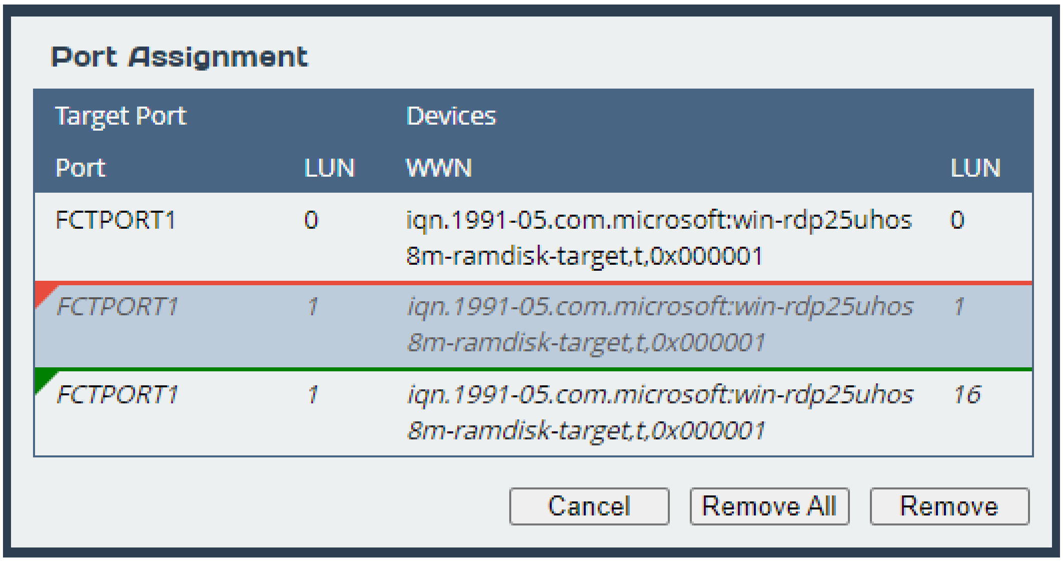
New Device Assignment

Device & Logical Unit: --- Select a Target ---

Port: --- Select a Port ---

LUN: Input LUN Number

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



Port Assignment

Target Port		Devices	
Port	LUN	WWN	LUN
FCTPORT1	0	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	0
FCTPORT1	1	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	1
FCTPORT1	1	iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target,t,0x000001	16

To assign a target device to a Fibre Channel Port:

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

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

Selecting *Cancel* allows you to abandon any pending changes.

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

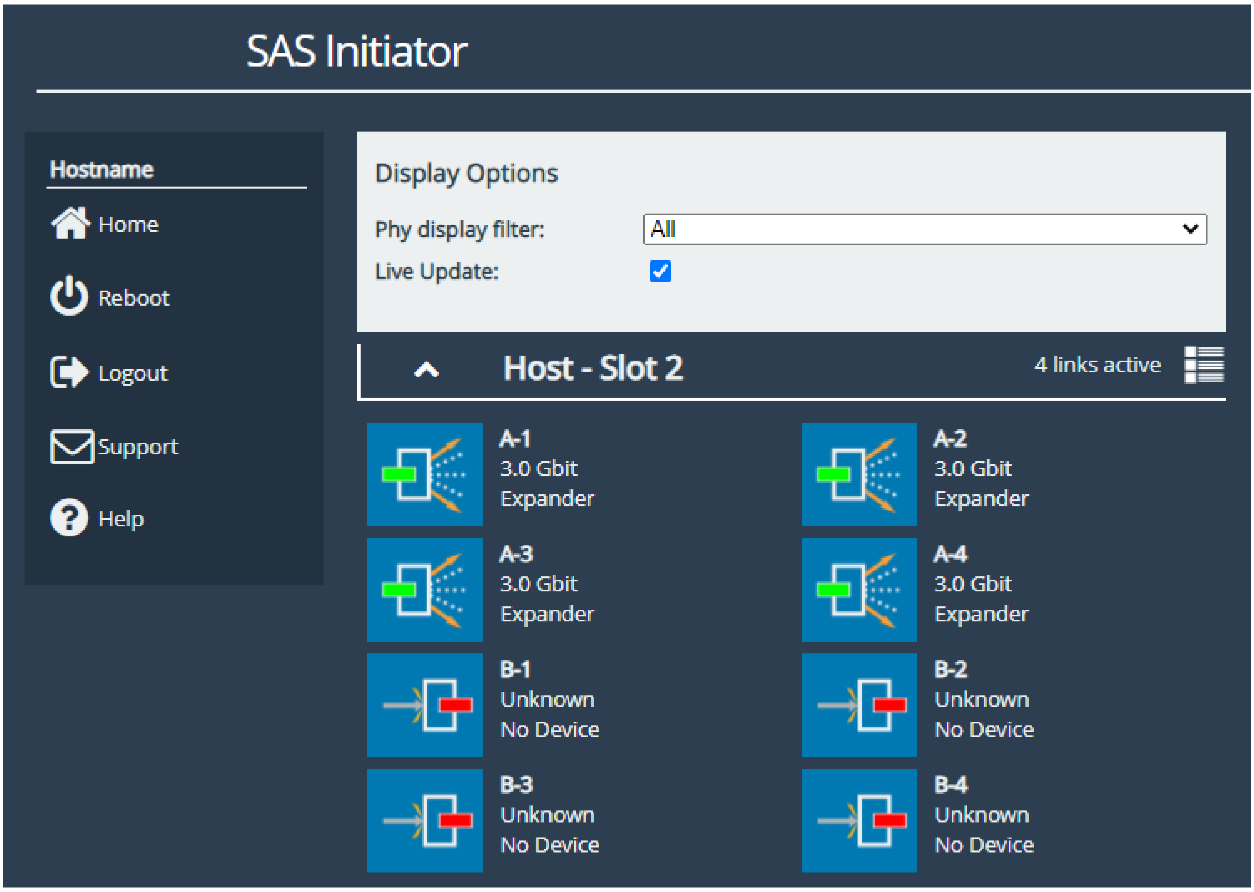
4.5 SAS Initiator

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

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

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

You will see the following page:



SAS Initiator

Hostname

- Home
- Reboot
- Logout
- Support
- Help

Display Options

Phy display filter: All

Live Update: ☑

Host - Slot 2 — 4 links active

A-1 3.0 Gbit Expander	A-2 3.0 Gbit Expander
A-3 3.0 Gbit Expander	A-4 3.0 Gbit Expander
B-1 Unknown No Device	B-2 Unknown No Device
B-3 Unknown No Device	B-4 Unknown No Device

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

4.5.1 SAS Initiator Page

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

4.5.1.1 Hosts

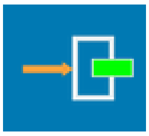
The heading of a host section shows the following information:

Chevron An arrow for expanding or collapsing the section.

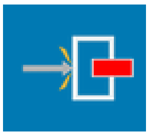
Name (e.g. Host 1).

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

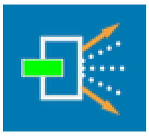
Under the host heading, a number of phys will be displayed. The icon represents their state.



End Device A device is connected



No Device No device is connected



Expander Device An expander is connected

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

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

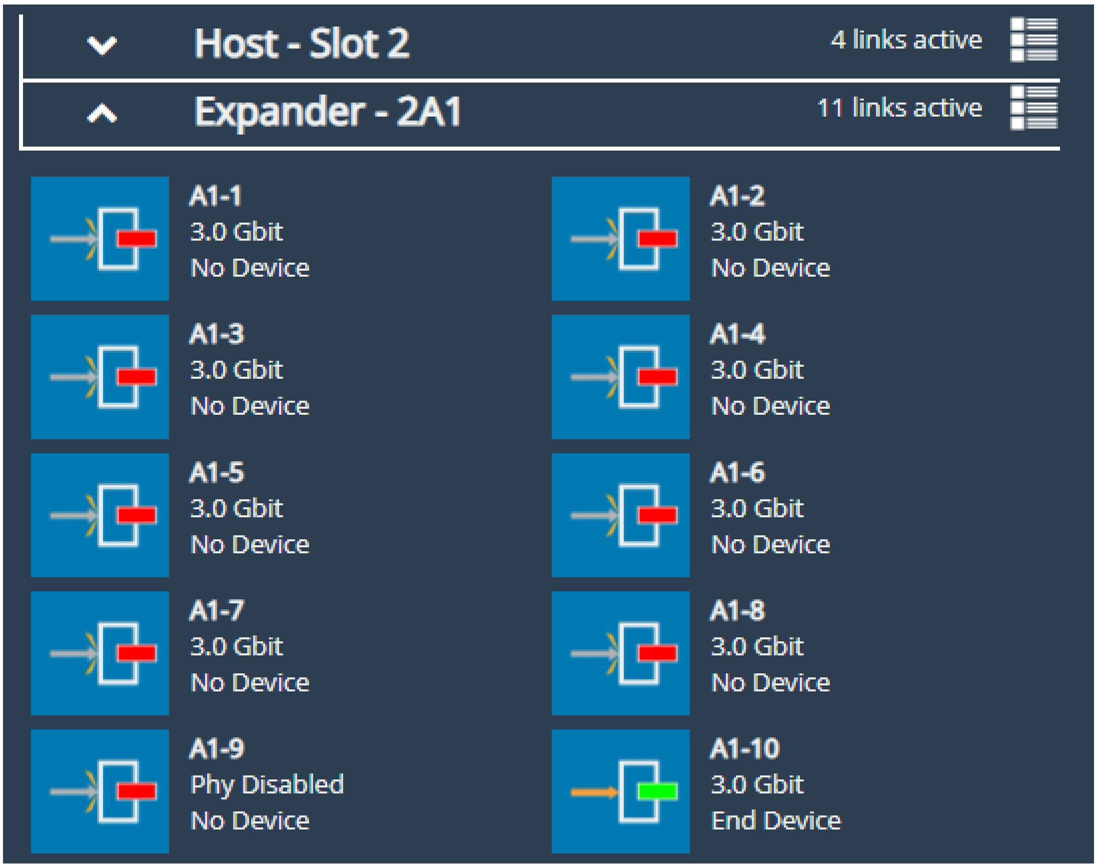
Link speed The negotiated link speed of the device. This will show a speed if a physical connection is made (e.g. “6.0 Gbit”), or otherwise displays “Unknown”.

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

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

4.5.2 Expanders

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



Host - Slot 2 4 links active

Expander - 2A1 11 links active

A1-1
3.0 Gbit
No Device

A1-2
3.0 Gbit
No Device

A1-3
3.0 Gbit
No Device

A1-4
3.0 Gbit
No Device

A1-5
3.0 Gbit
No Device

A1-6
3.0 Gbit
No Device

A1-7
3.0 Gbit
No Device

A1-8
3.0 Gbit
No Device

A1-9
Phy Disabled
No Device

A1-10
3.0 Gbit
End Device

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

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

4.5.2.1 Display Options

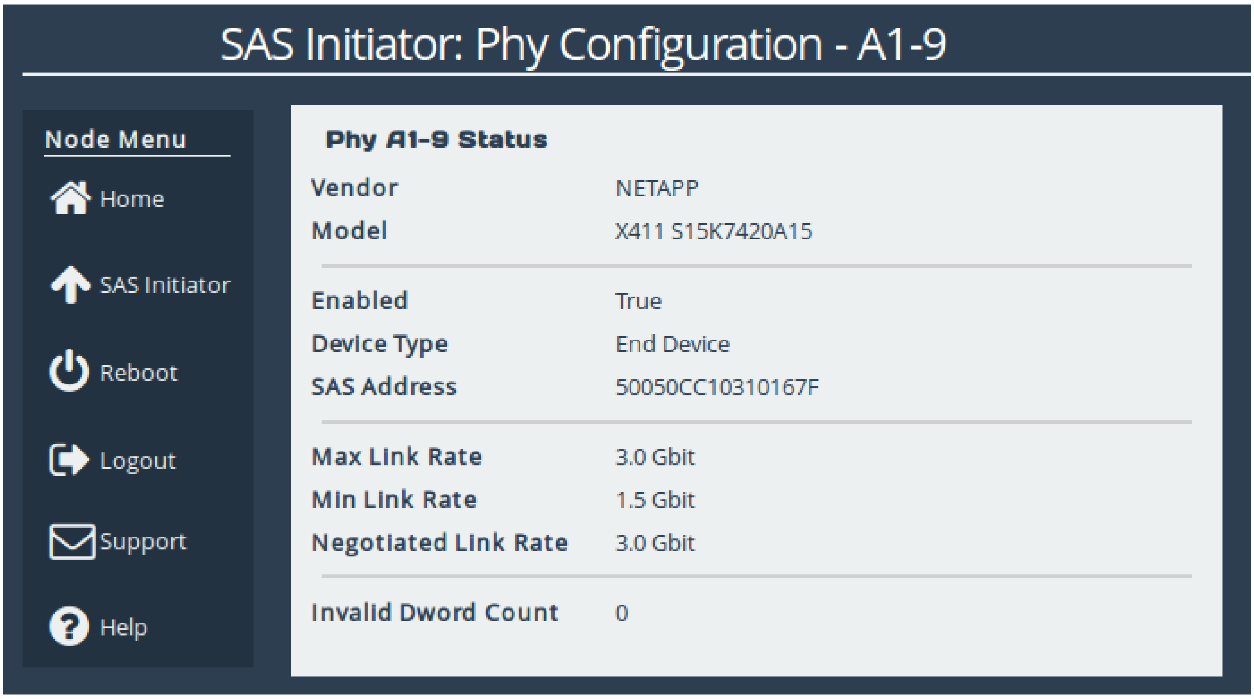
Options are available for configuring how devices are viewed. These are:

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

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

4.5.3 Phy Status Page

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



Phy A1-9 Status

Vendor	NETAPP
Model	X411 S15K7420A15
Enabled	True
Device Type	End Device
SAS Address	50050CC10310167F
Max Link Rate	3.0 Gbit
Min Link Rate	1.5 Gbit
Negotiated Link Rate	3.0 Gbit
Invalid Dword Count	0

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

Vendor Manufacturer of the device.

Product Product name of the attached expander.

Model Model name of the attached end device.

Enabled True or false.

Device Type No device, end device, or expander.

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

Max Link Rate Maximum link speed allowed by the hardware.

Min Link Rate Minimum link speed allowed by the hardware.

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

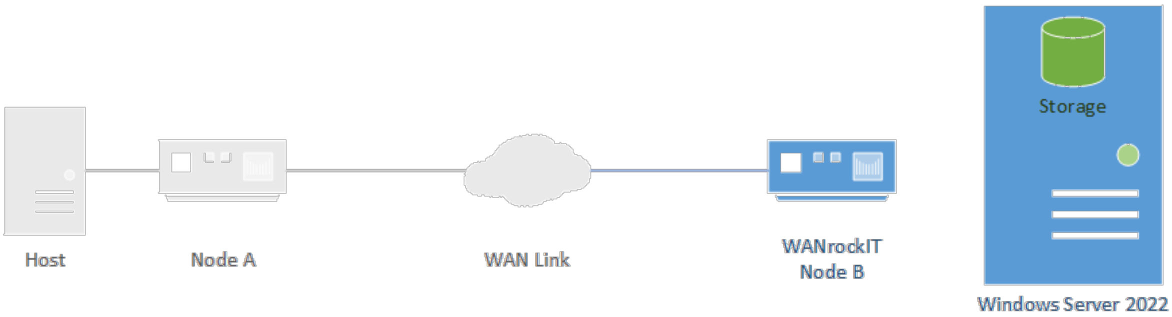
Invalid Dword Count Number of malformed Dwords received.

5 Configuring your WANrockIT Node to Present iSCSI Targets to an Off-Premise Site

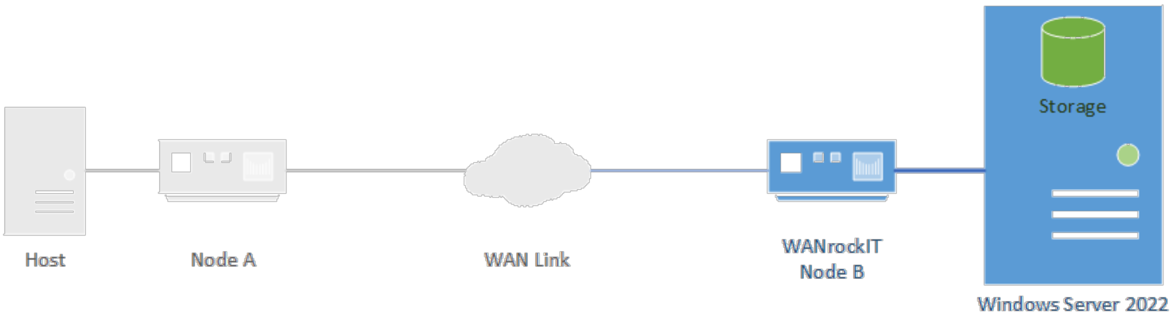
5.1 Introduction

This section describes how to log on to an iSCSI target from your Off-Premise WANrockIT Node. This allows the devices attached to the target to be presented over a WANrockIT connection into another Premise. This tutorial uses a Microsoft iSCSI virtual disk on a Windows Server 2022 machine and a WANrockIT Node.

The following diagram illustrates the described topology.

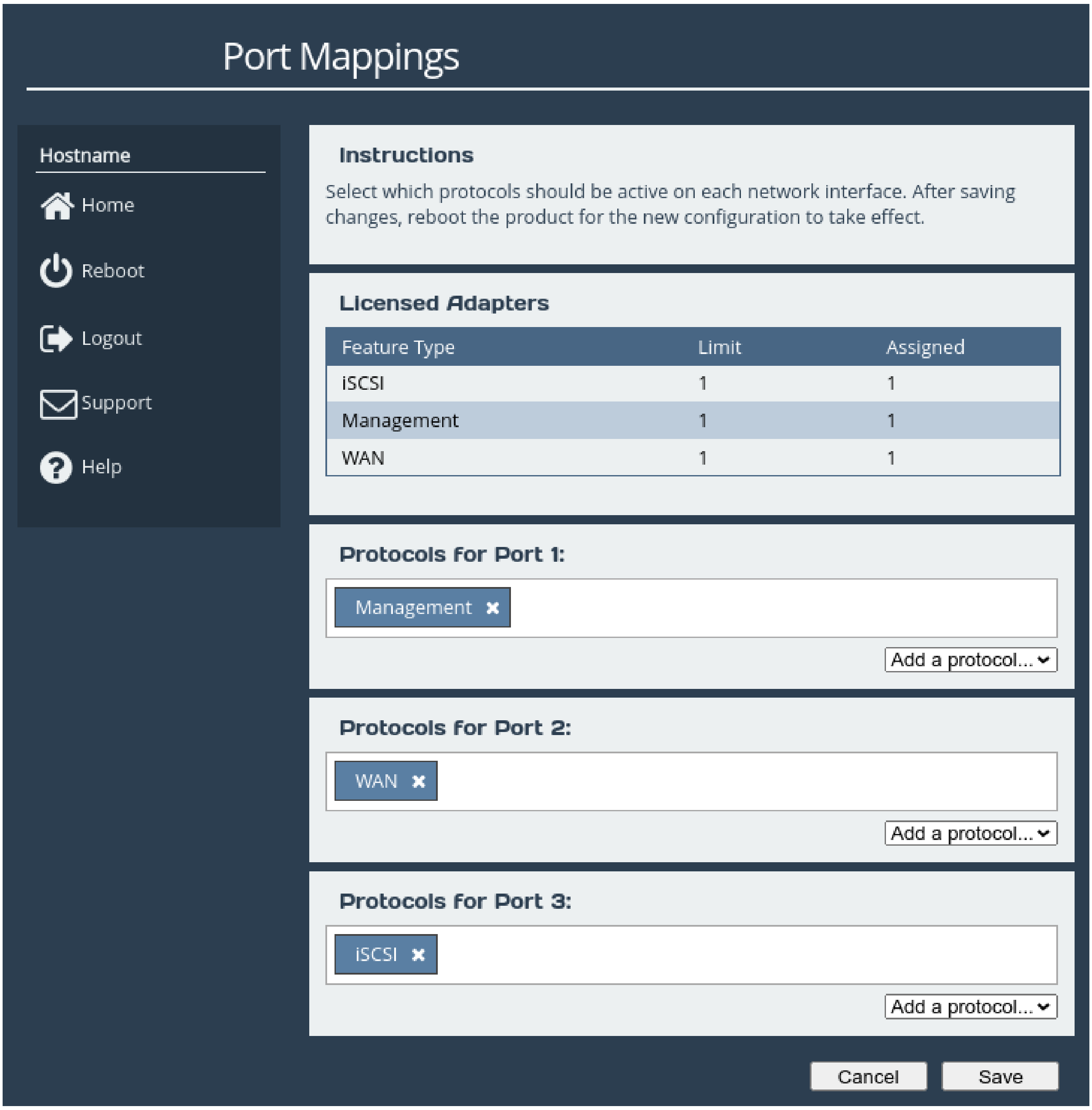


Once you have completed the following instructions your topology have changed to the following.



5.2 Configuring Features

Ensure that the port from which you wish to establish a connection has the iSCSI protocol mapped. In this example *Port 3* will be used, as shown in the image below. A reboot is required before any changes to the port mappings take effect. For a more detailed guide on port mappings please refer to the Port Mappings (🔑) section.



Port Mappings

Instructions

Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.

Licensed Adapters

Feature Type	Limit	Assigned
iSCSI	1	1
Management	1	1
WAN	1	1

Protocols for Port 1:

Management ✖

Add a protocol...

Protocols for Port 2:

WAN ✖

Add a protocol...

Protocols for Port 3:

iSCSI ✖

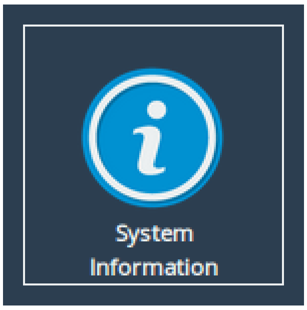
Add a protocol...

5.3 Setting up an Access Control List on Windows Server

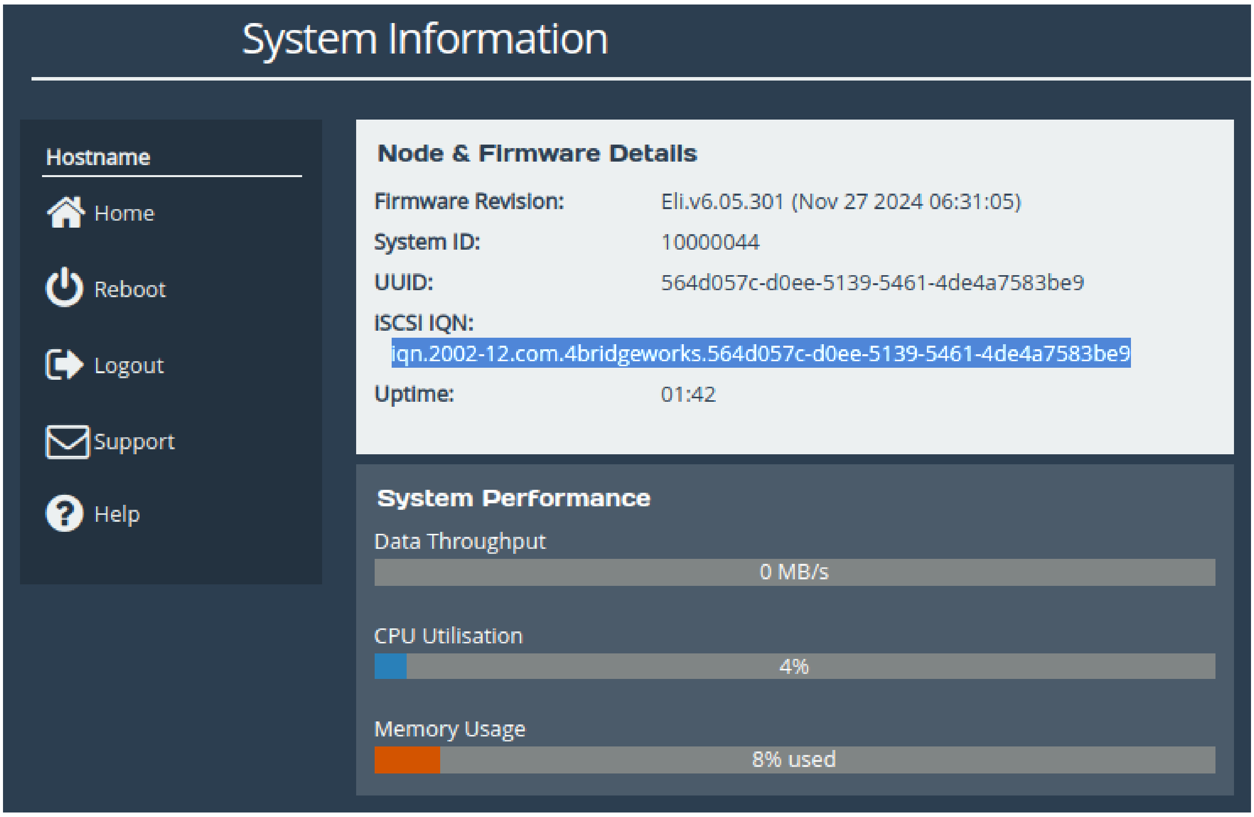
5.3.1 Retrieving the WANrockIT's IQN

The Microsoft iSCSI virtual disk target requires entries to be added to an access list. Typically, an IQN is added to the list. Alternatively, an IP address can be added. Not all targets require this method of authorisation, so this step may be skipped depending on your setup.

Navigate to the Home screen of the node and open the *System Information* page by clicking on the corresponding icon.



Copy the value in the iSCSI IQN field to the clipboard.



System Information

Node & Firmware Details

Firmware Revision:	Eli.v6.05.301 (Nov 27 2024 06:31:05)
System ID:	10000044
UUID:	564d057c-d0ee-5139-5461-4de4a7583be9
iSCSI IQN:	iqn.2002-12.com.4bridgeworks.564d057c-d0ee-5139-5461-4de4a7583be9
Uptime:	01:42

System Performance

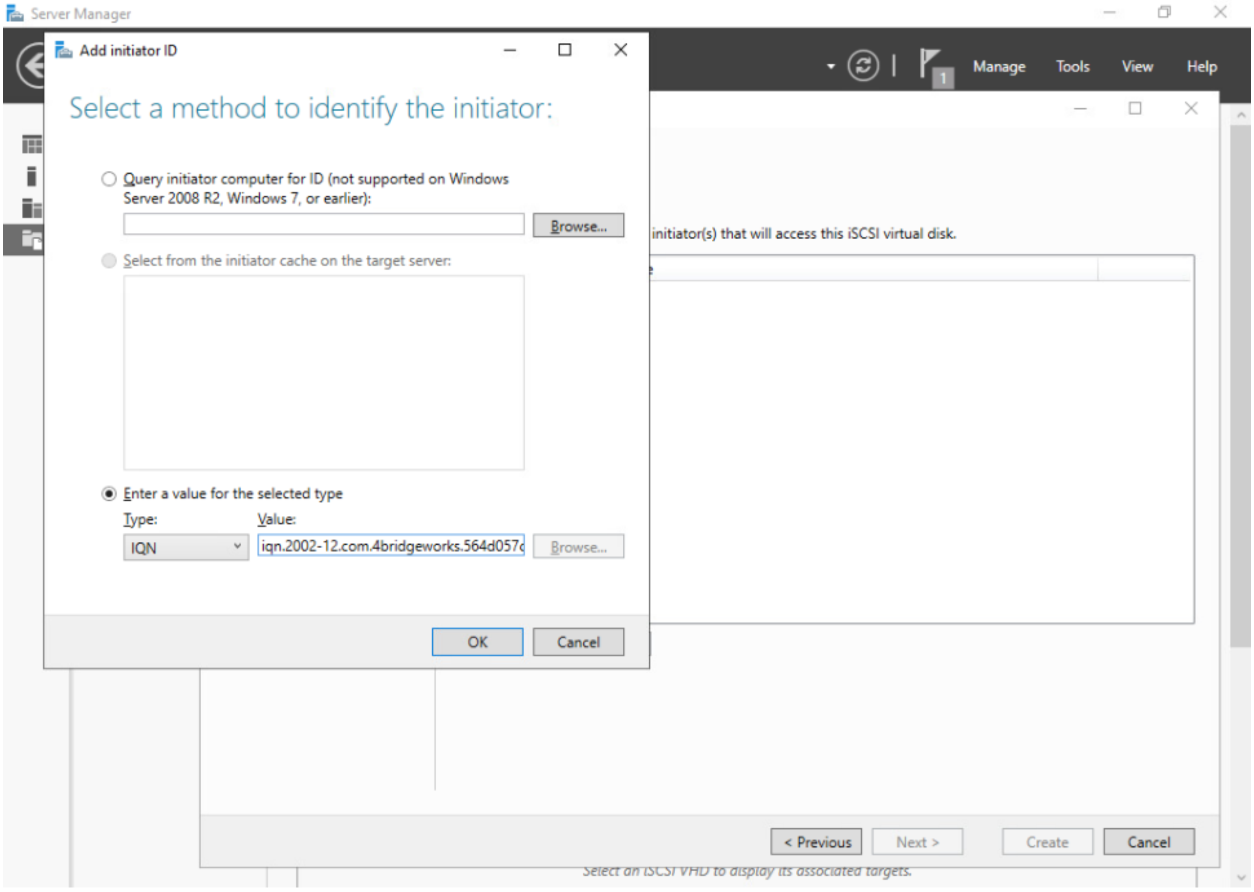
Data Throughput: 0 MB/s

CPU Utilisation: 4%

Memory Usage: 8% used

5.3.2 Adding the WANrockIT’s IQN to the Access Control list

From your Windows Server 2022 machine, navigate to the iSCSI Virtual Disk page. Under the iSCSI Targets subsection, right-click on the target to which you wish to connect and select *Properties*. Under the *Initiators* tab, add the IQN of the Node and click *OK* to confirm. The Node is now authorised to connect to the target.



Add initiator ID

Select a method to identify the initiator:

○ Query initiator computer for ID (not supported on Windows Server 2008 R2, Windows 7, or earlier):

Browse...

○ Select from the initiator cache on the target server:

● Enter a value for the selected type

Type: IQN

Value: iqn.2002-12.com.4bridgeworks.564d057c

Browse...

OK Cancel

initiator(s) that will access this iSCSI virtual disk.

< Previous Next > Create Cancel

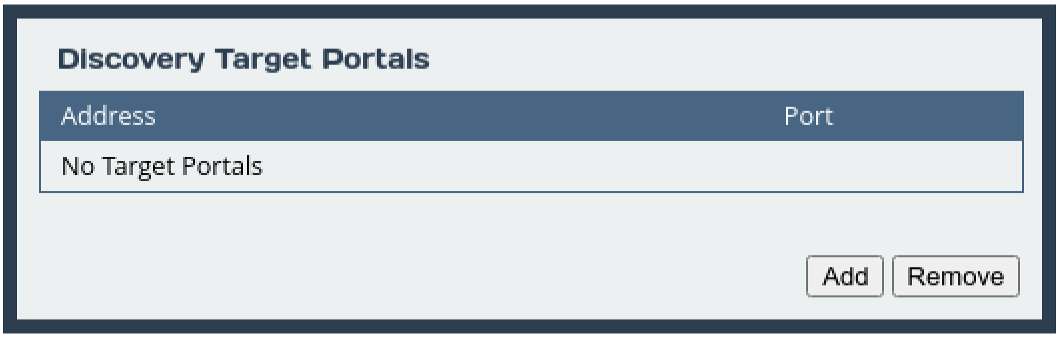
Select an iSCSI VHD to display its associated targets.

5.4 Logging onto the iSCSI Target

The next step is to perform a discovery on the target portal. Navigate to the Home screen of the Node and open to the *iSCSI Initiator* page by clicking on the corresponding icon.

iSCSI Initiator

Under the *Discovery Target Portal* subsection, click the *Add* button.

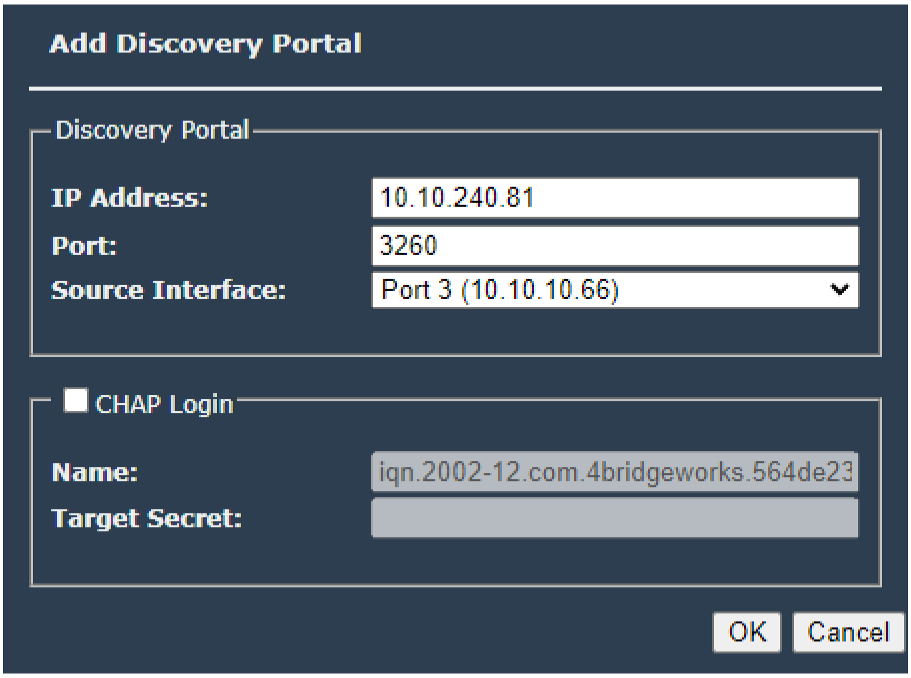


Discovery Target Portals

Address	Port
No Target Portals	

In the subsequent dialog, enter the IP address of the Microsoft iSCSI target portal in the *IP Address* field. The default port number assigned to iSCSI is 3260. If you have configured the Windows iSCSI target to use a different port number, enter this number in the Port field. If iSCSI is mapped to more than one interface, ensure the *Source Interface* drop-down has the correct interface selected to perform the discovery.

In this example CHAP authentication is not required. More detailed information on CHAP authentication can be found within the Bridgeworks user manuals, please refer to the Useful Links section.



Add Discovery Portal

Discovery Portal

IP Address: 10.10.240.81

Port: 3260

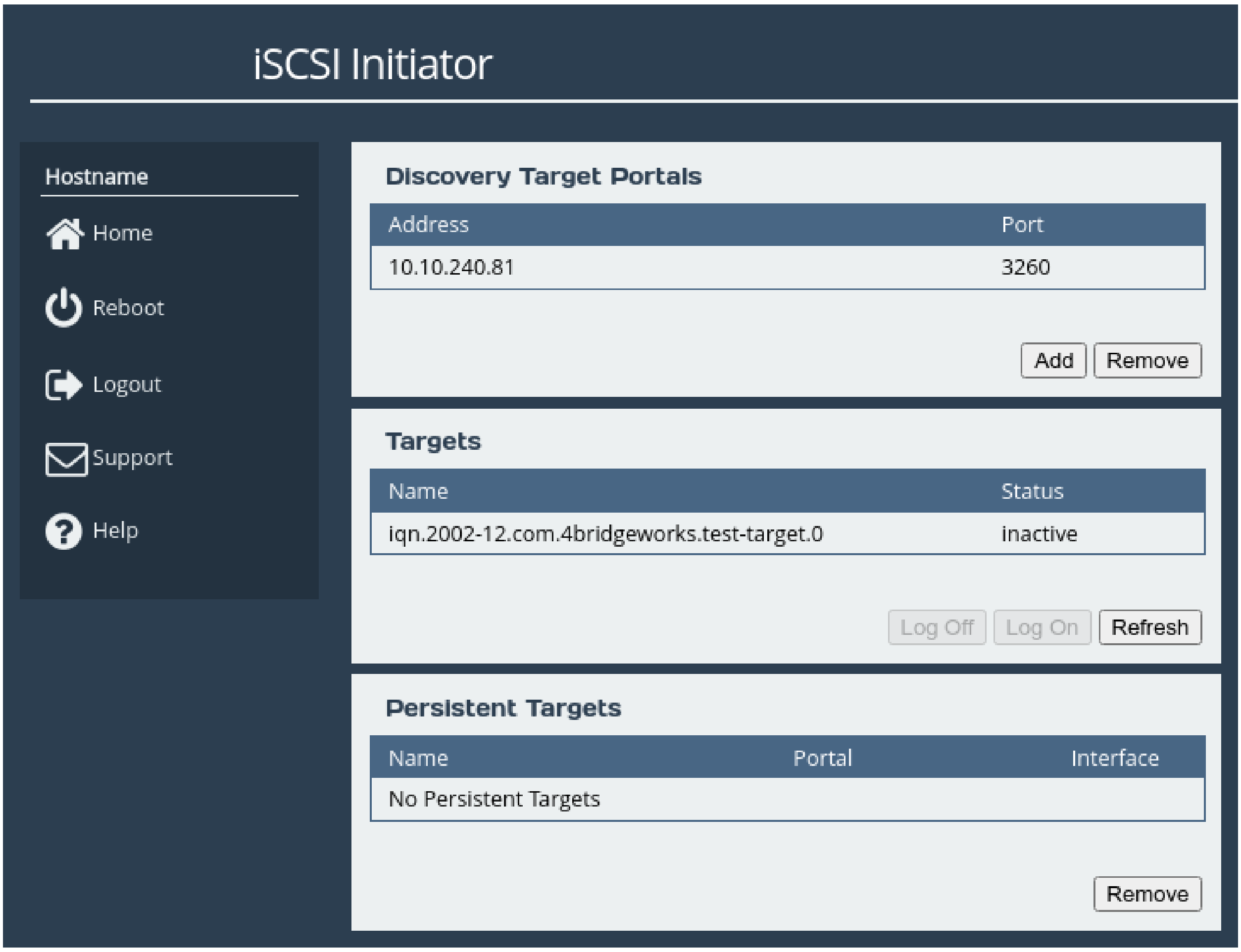
Source Interface: Port 3 (10.10.10.66)

□ CHAP Login

Name: iqn.2002-12.com.4bridgeworks.564de23

Target Secret:

When the discovery is complete, a list of targets presented by the portal is shown in the *Targets* subsection. The example shows a single target with an IQN of `iqn.2002-12.com.4bridgeworks.test-target.0` that is currently inactive (the iSCSI initiator is not currently logged onto the target).



Discovery Target Portals

Address	Port
10.10.240.81	3260

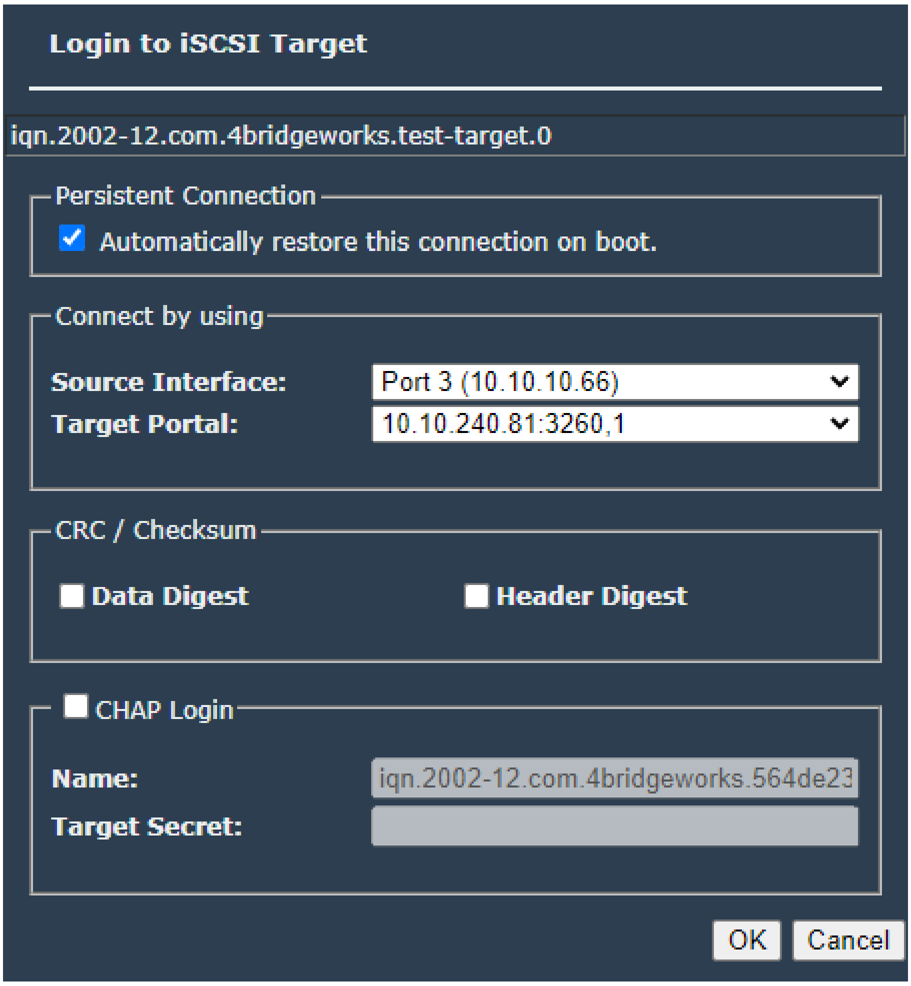
Targets

Name	Status
iqn.2002-12.com.4bridgeworks.test-target.0	inactive

Persistent Targets

Name	Portal	Interface
No Persistent Targets		

Now you are ready to log in to a target. Select the required target under the *Targets* section and click the *Log On* button. You will be presented with the following screen.



Login to iSCSI Target

iqn.2002-12.com.4bridgeworks.test-target.0

Persistent Connection

☑ Automatically restore this connection on boot.

Connect by using

Source Interface: Port 3 (10.10.10.66)

Target Portal: 10.10.240.81:3260,1

CRC / Checksum

□ Data Digest □ Header Digest

□ CHAP Login

Name: iqn.2002-12.com.4bridgeworks.564de23

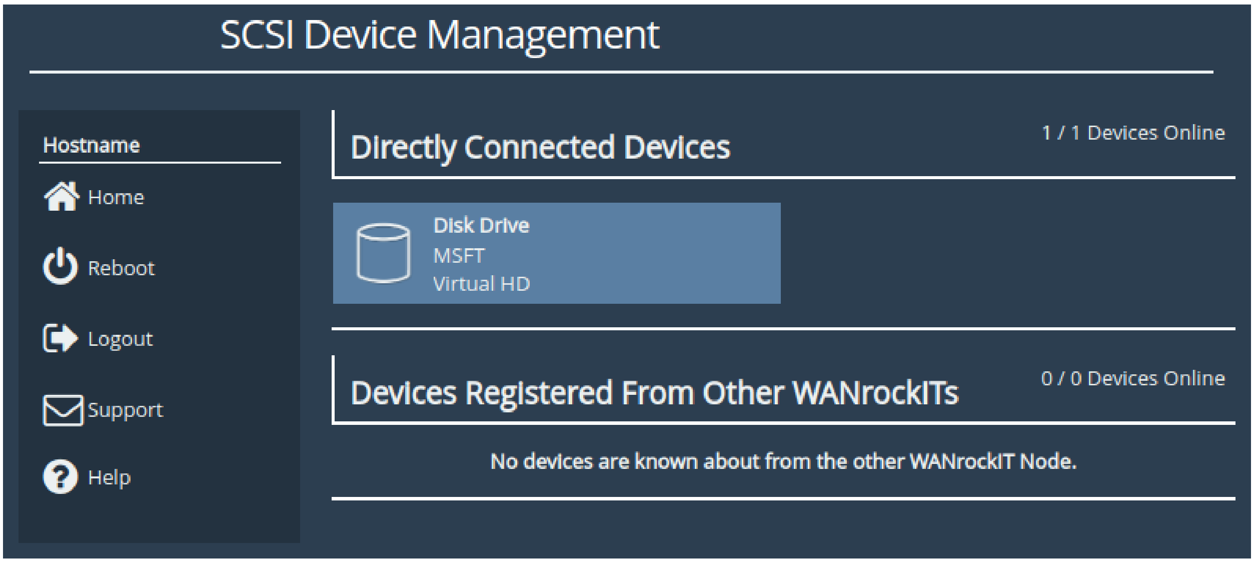
Target Secret:

If you do not require the Node to reconnect automatically to this target after a reboot, uncheck the *Persistent Connection* checkbox. As with the portal discovery, ensure that the correct interface is selected from the *Source Interface* drop-down. Ensure that the correct iSCSI target address is selected under the *Target Portal* drop-down.

Data Digest and *Header Digest* can be enabled in the CRC/Checksum subsection. As with the discovery, you can enter your relevant CHAP details if necessary, although this box remains unchecked in the example above. Click the *OK* button to log on. This will change the status of the target from *Inactive* to *Connected*. If the *Persistent Connection* checkbox was enabled, the target will also be listed in the Persistent Targets subsection. Any targets listed here will be logged on to after each reboot of the Node.

5.5 Verifying the Login

To verify that the login was successful, from the Home screen navigate to the *SCSI Device Management* page. The devices from the iSCSI target are shown in the list of *Directly Connected Devices*, as shown below. These devices are now presentable over a WANrockIT connection.



SCSI Device Management

Directly Connected Devices

1 / 1 Devices Online

Disk Drive
MSFT
Virtual HD

Devices Registered From Other WANrockITs

0 / 0 Devices Online

No devices are known about from the other WANrockIT Node.

6 Configuring IPsec

6.1 Introduction

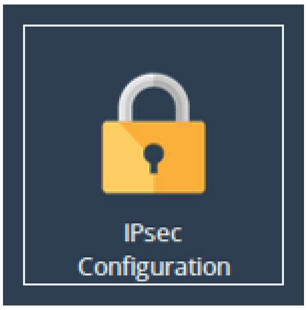
This step will guide you through how to configure IPsec to encrypt traffic between two Bridgeworks Nodes. Using IPsec ensures the integrity, confidentiality and authentication of data communications over an IP network. This step should be done before performing the step Establishing a Link Between Nodes. If you are already connecting your Nodes over an existing VPN link, or a private direct connection then this step is not necessary as your traffic will already be protected.

6.2 Important Notes

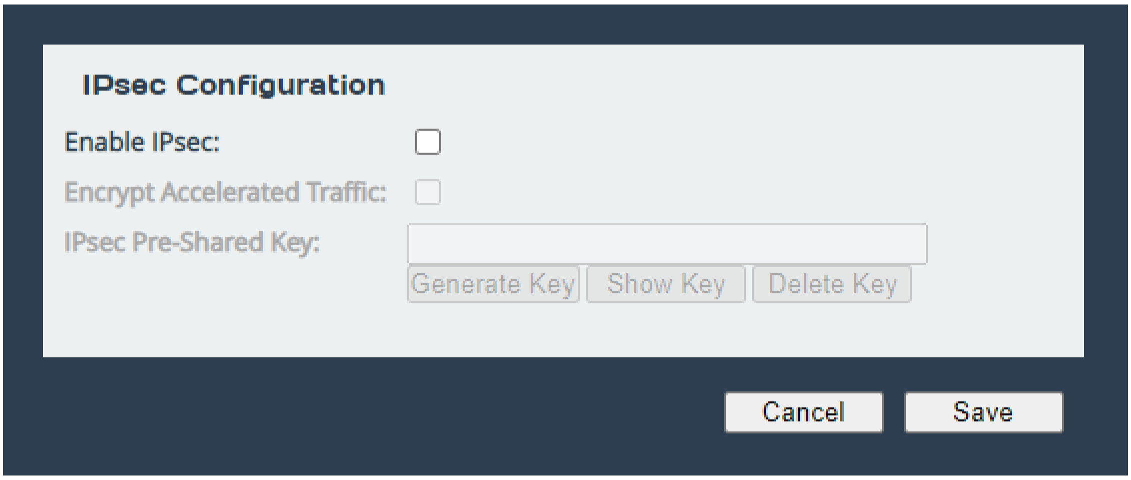
- Nodes with IPsec configured to *Encrypt Accelerated Traffic* will only allow connections from other IPsec-enabled Nodes with the same pre-shared key and settings enabled.
- It is recommended to only enable *Encrypt Accelerated Traffic* when data transfer is stopped as WAN communication will be broken until IPsec configuration has been completed on both Nodes.
- It is recommended that HTTPS is enabled (by default it will already be enabled) before configuring IPsec as this ensures that the Pre-Shared Key is transmitted securely between the Node and web browser.

6.3 Enabling IPsec

From the Node's web interface, navigate to the *Node Management* page, then to the *IPsec Configuration* page by clicking the corresponding icon in the top menu.



The IPsec service is disabled by default, so the Node's IPsec Configuration options will be disabled until the *Enable IPsec* checkbox is selected.



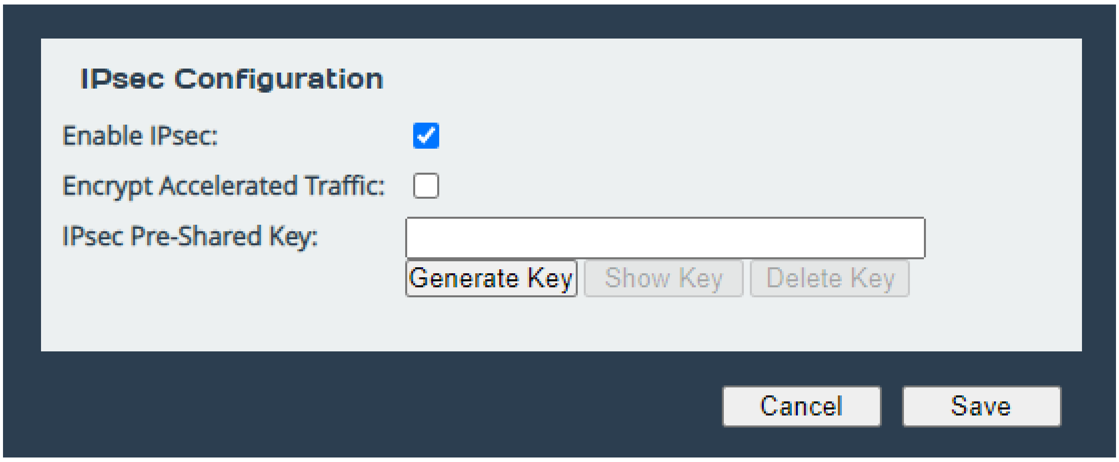
IPsec Configuration

Enable IPsec: □

Encrypt Accelerated Traffic: □

IPsec Pre-Shared Key:

Select the *Enable IPsec* checkbox and the section will be enabled as shown below:



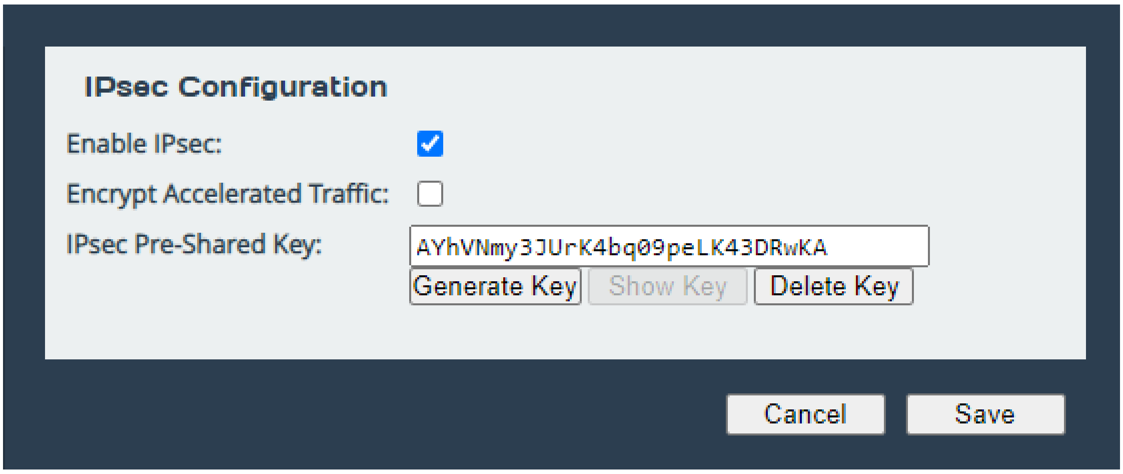
IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: □

IPsec Pre-Shared Key:

You can either enter in your own Pre-Shared Key or use the IPsec key generator by clicking *Generate Key*, which will fill in the *IPsec Pre-Shared Key* field as shown below:



IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: □

IPsec Pre-Shared Key: AYhVNmy3JUrK4bq09peLK43DRwKA

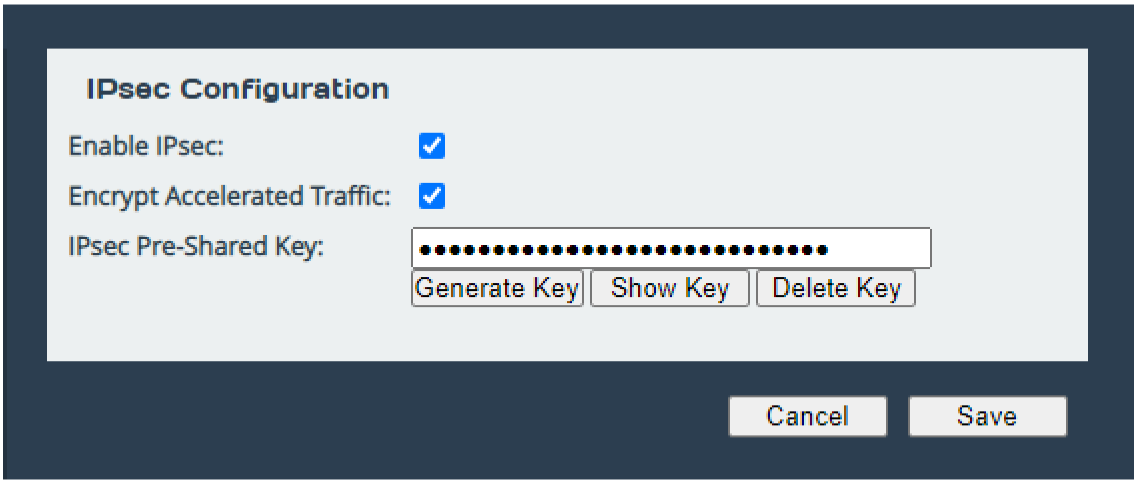
If the *Encrypt Accelerated Traffic* option is desired then tick the corresponding checkbox. This option will encrypt all WAN links between the two Nodes affecting all accelerated data being passed through them.

If only the VPN functionality is required, i.e. only unaccelerated traffic is required to be encrypted, the *Encrypt Accelerated Traffic* option can be left blank.

Click *Save* to store the IPsec configuration. This will become active straight away and, if *Encrypt Accelerated Traffic* is selected, any existing WAN connections will break unless they already have IPsec enabled with the same pre-shared key and settings.

6.4 Copying the Pre-Shared Key to other Bridgeworks Nodes

Return to the *IPsec Configuration* page. The PSK should now be hidden as shown:



IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: ☑

IPsec Pre-Shared Key: ••••••••••••••••••••••••••••••••

Click *Show Key* to display the stored pre-shared key. Select and copy this key to your clipboard. Please note that if HTTPS is not enabled then the Pre-Shared key will be sent to your web browser in plain text format.

From the web interface of any Bridgeworks Nodes you wish to connect to, follow this section again, but paste in the key from your clipboard instead of generating a new one.

7 Establishing a Link Between Nodes

7.1 Introduction

The following section demonstrates how to connect an On-Premise Node to an Off-Premise Node. The examples below illustrate the WAN connection of two Nodes labelled *Node A* and *Node B*. Establishing a WAN link from *Node A* to *Node B* is required in order to allow hosts/endpoints connected to *Node A* to access target devices or endpoints connected to *Node B*. This process will have to be repeated to establish a connection in the reverse direction if you want the hosts/endpoints at *Node B* to connect to targets connected to *Node A*. If you are using the PORTrockIT product range, it is recommended that you establish a connection both ways unless you are certain one way is sufficient.

There are different types of connection possible, depending on your network infrastructure. Throughout the following example topologies, the Nodes are referred to as *Node A* and *Node B* with a summary of which example IP addresses are used. These examples should be kept in mind through the remaining sections of this guide.

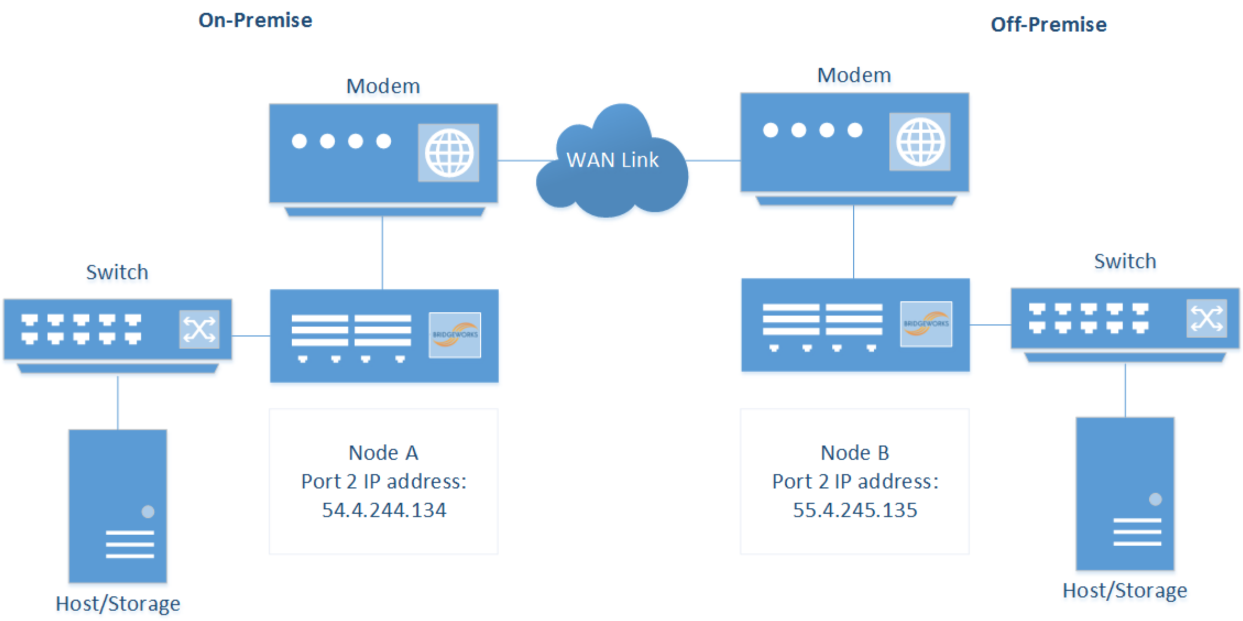
7.2 Firewall

If the WAN link being established is behind a firewall then the following firewall ports will have to be open in both the outbound and inbound direction.

Protocol/Port	Description
TCP 16665	WANrockIT/PORTrockIT main transfer port
UDP 4500	IPsec, used for encrypting WANrockIT/PORTrockIT traffic
UDP 500	IPsec, used for encrypting WANrockIT/PORTrockIT traffic
ESP	IPsec, used for encrypting WANrockIT/PORTrockIT traffic

7.3 Topology 1: Connecting Bridgeworks Nodes which have Public IP addresses

To connect to Bridgeworks Nodes, a public IP address can be assigned directly to the WAN interfaces (by default, *Port 2*) of both Nodes, as shown below. In this case, the WAN port is directly connected into a modem and faces directly out on to a WAN link with a public IP address.

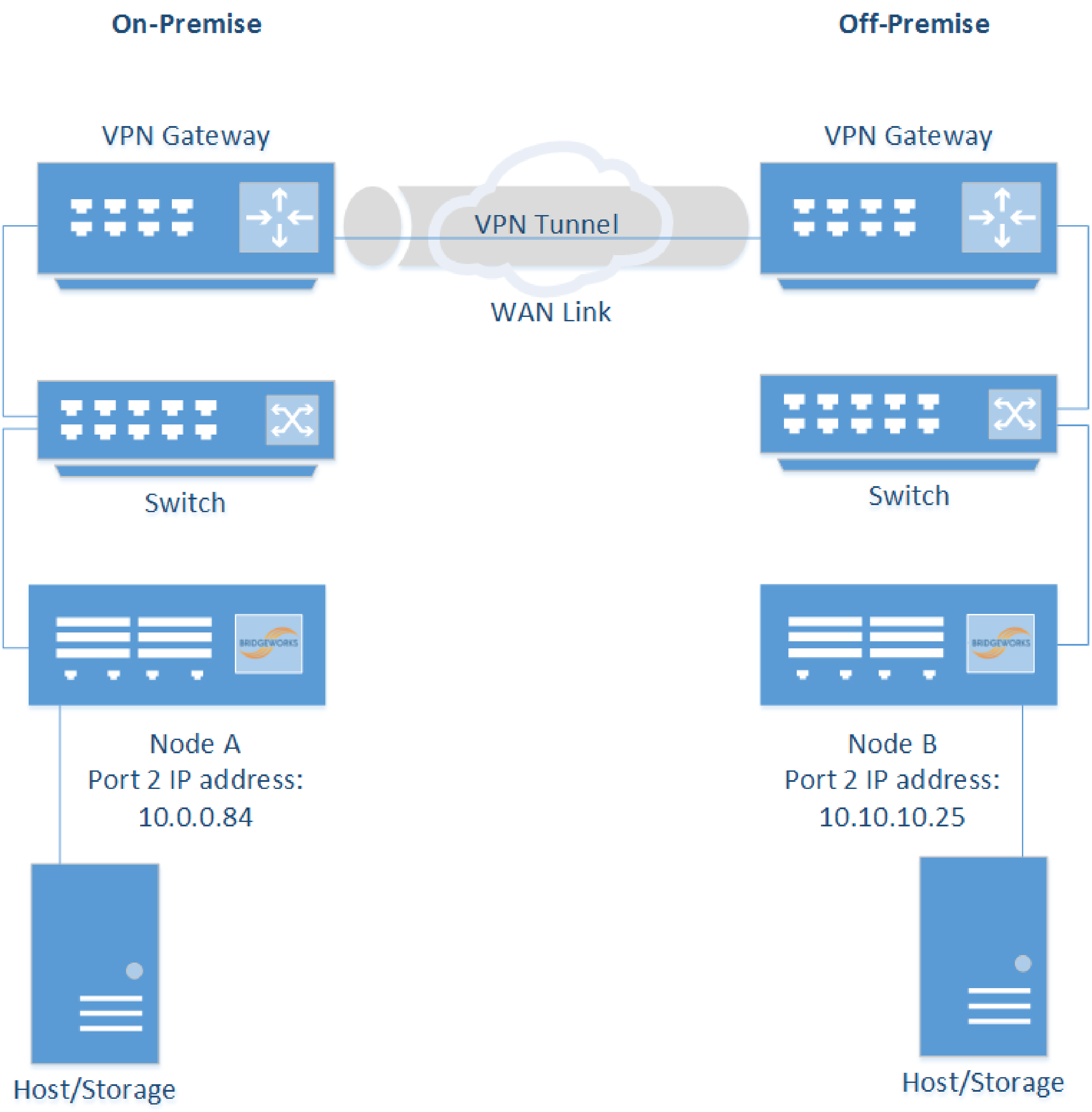


In this example the IP addresses for establishing a Nodal link are the public IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 54.4.244.134
- Node B: 55.4.245.135

7.4 Topology 2: Connecting Bridgeworks Nodes joined via an external VPN

If the On-Premise and Off-Premise sites that will be connected via the Bridgeworks Nodes are already connected via a VPN connection, as per the diagram below, then communication between the private IP addresses on the WAN interface (by default, *Port 2*) of the Bridgeworks Nodes should already be possible.



In this example the IP addresses for establishing a Nodal link are the private IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 10.0.0.84
- Node B: 10.10.10.25

7.5 Topology 3: Connecting Bridgeworks Nodes Using 2 Site NAT

It is possible to connect Bridgeworks Nodes which are behind a NAT, where a router, computer or firewall sits between an internal network and the WAN connection.

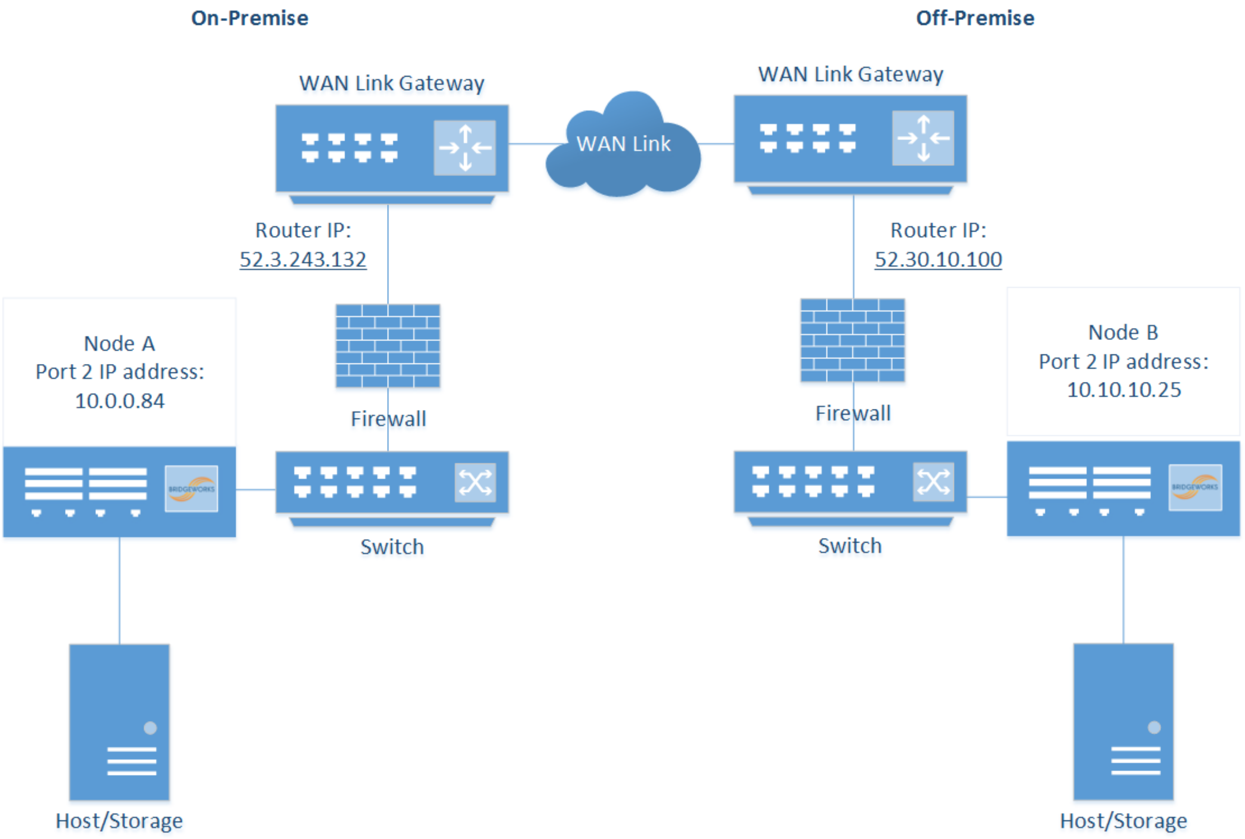
The firewall must be configured with the following sets of NAT port forwarding rules:

Protocol: TCP
Destination Port Range: 16665
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 16665

Protocol: UDP
Destination Port Range: 4500
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 4500

Protocol: UDP
Destination Port Range: 500
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 500

For further assistance with configuring your NAT, please contact your local network administrator. The following diagram gives an overview of an example NAT setup and where the Bridgeworks Nodes would be placed.

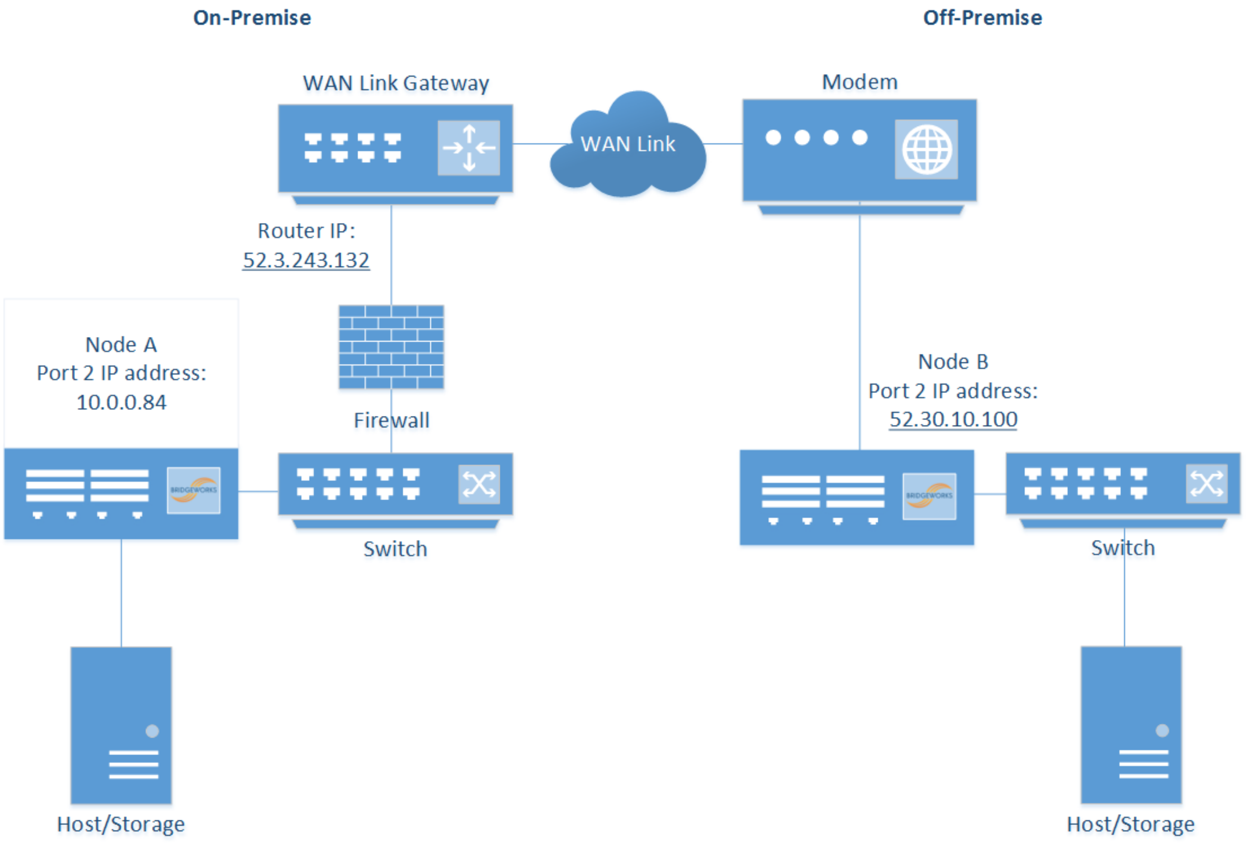


In this example the IP addresses for establishing a Nodal link are the IP addresses of the router, in this case:

- Node A: 52.3.243.132
- Node B: 52.30.10.100

7.6 Topology 4: Connecting to a Bridgeworks Node with a NAT on one site

An alternative to the above topology is for one Bridgeworks Node to be behind a NAT (where a router, computer, or firewall sits between an internal network and the WAN connection), and the second to be accessible through a public IP address. This is useful if you are unable to set any additional firewall policies.



In this example the IP addresses for establishing a Nodal link are the IP address of the router connected to Node A, and the public IP address of Node B.

- Node A: 52.3.243.132
- Node B: 52.30.10.100

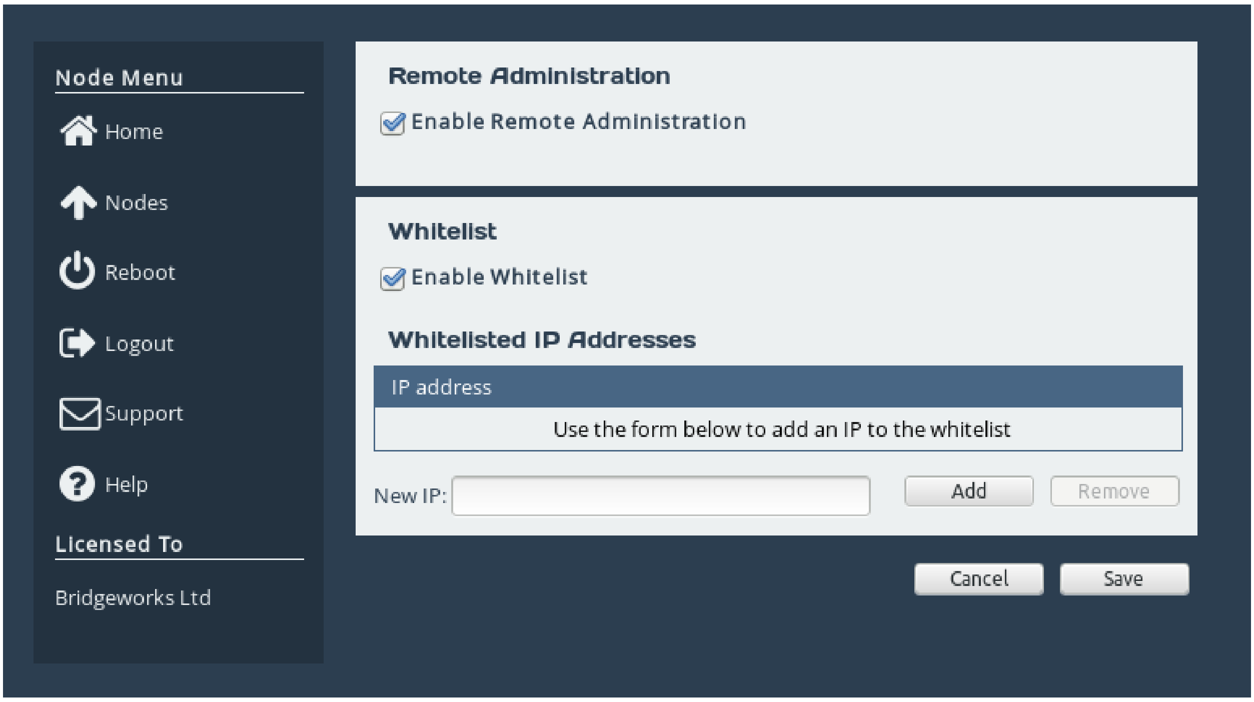
For a successful connection in this example without setting any firewall policies, Node A must first connect to Node B.

7.7 Access Control

Throughout the following sections which refer to *Node A* and *Node B*, use the IP address types found in the previous examples.

Navigate to the *Access Control* page of Node B by going to *Node Management* and clicking on the corresponding icon.

Ensure that under the heading *Whitelist* the *Enable Whitelist* checkbox is ticked. By default this should be the case.



Remote Administration

☑ Enable Remote Administration

Whitelist

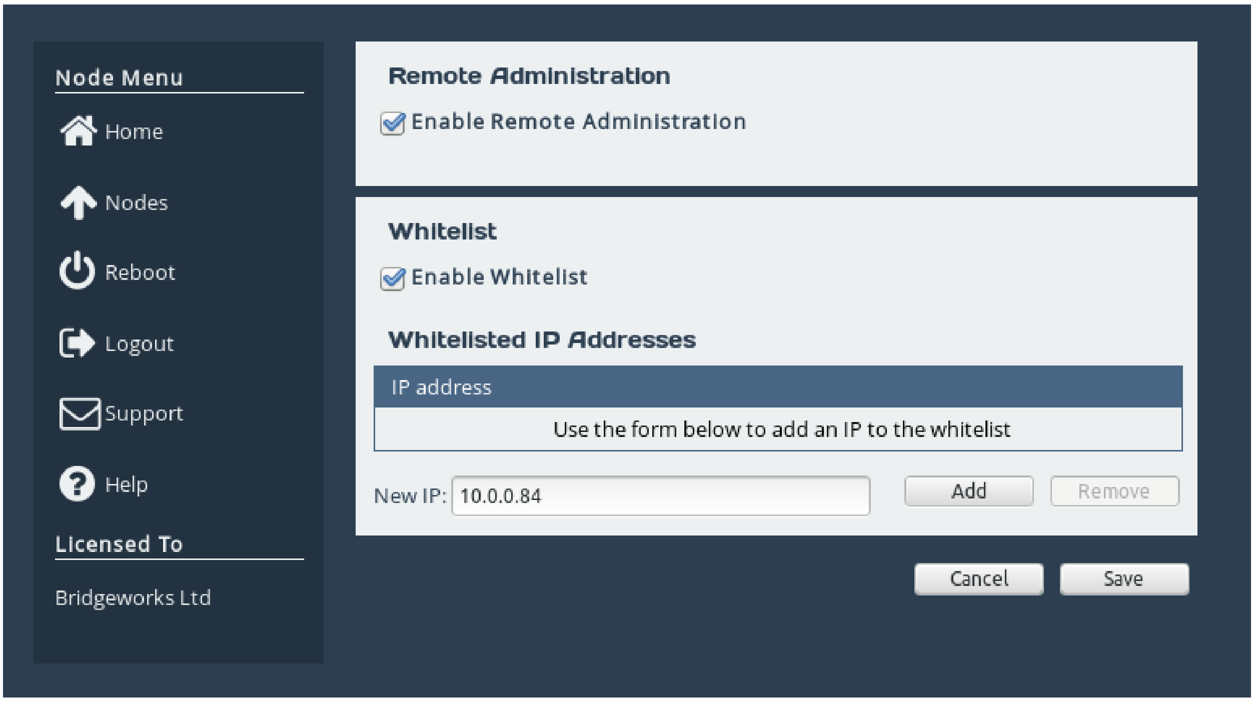
☑ Enable Whitelist

Whitelisted IP Addresses

IP address
Use the form below to add an IP to the whitelist

New IP:

Under *New IP*, enter the IP address of the WAN port of Node A in the entry box, and click the *Add* button.



Licensed To

Bridgeworks Ltd

Remote Administration

☑ Enable Remote Administration

Whitelist

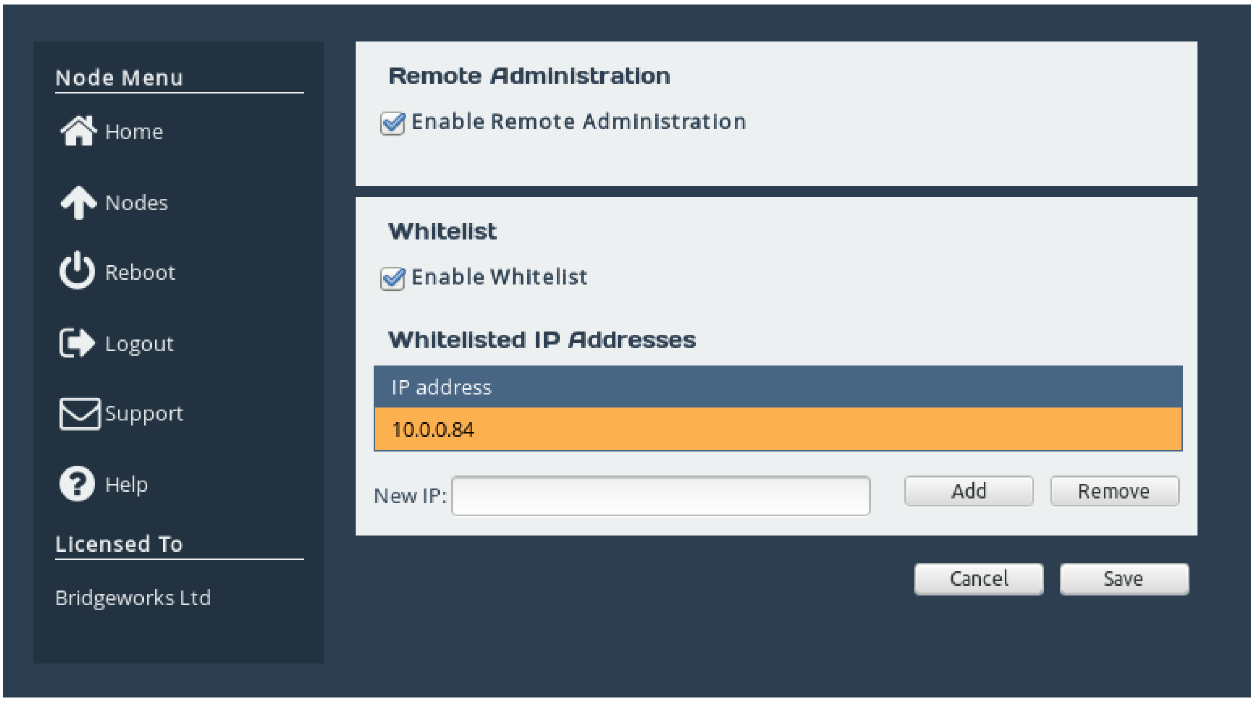
☑ Enable Whitelist

Whitelisted IP Addresses

IP address
Use the form below to add an IP to the whitelist

New IP: 10.0.0.84

When this has been added successfully you will see the IP address entry added to the list, as shown below.



Licensed To

Bridgeworks Ltd

Remote Administration

☑ Enable Remote Administration

Whitelist

☑ Enable Whitelist

Whitelisted IP Addresses

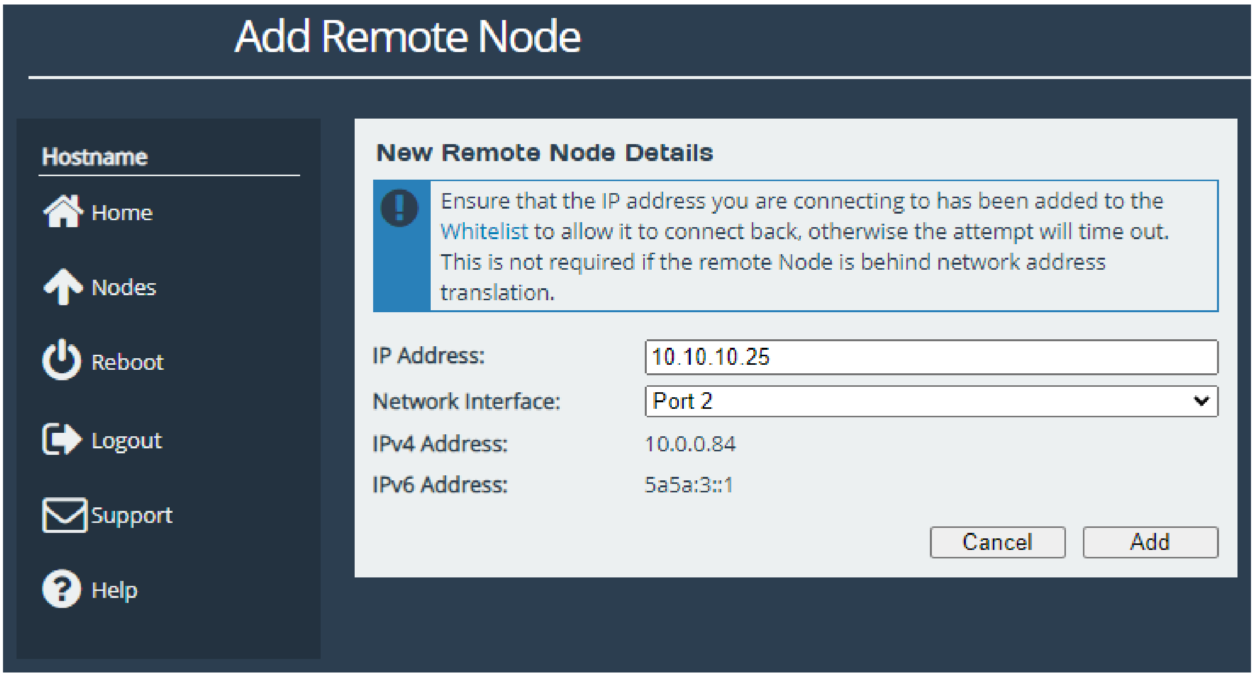
IP address
10.0.0.84

New IP:

Important: If Node B is not behind a NAT, repeat this process on Node A to add the IP address of Node B to the whitelist of Node A.

7.8 Node Management

The next stage is to perform the Node Discovery on the WAN link. From the *Node Management* page of Node A, click the *Add Remote Node* icon to navigate to the *Add Remote Node* page. Enter the IP address of Node B's WAN port in the address field. The *Network Interface* drop-down allows you to change the interface from which you wish to connect. Multiple options will be present if WAN is mapped to multiple network interfaces. Click *Add*, and a connection will be negotiated between the Nodes.



New Remote Node Details

Ensure that the IP address you are connecting to has been added to the Whitelist to allow it to connect back, otherwise the attempt will time out. This is not required if the remote Node is behind network address translation.

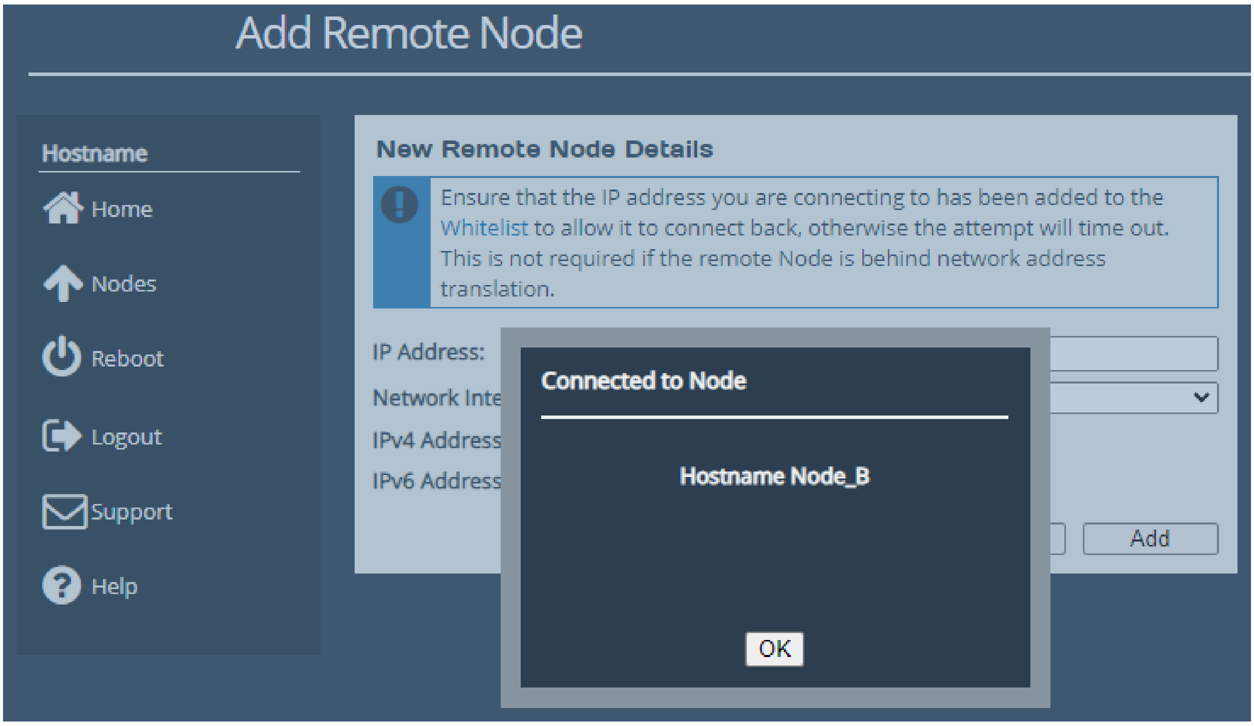
IP Address: 10.10.10.25

Network Interface: Port 2

IPv4 Address: 10.0.0.84

IPv6 Address: 5a5a:3::1

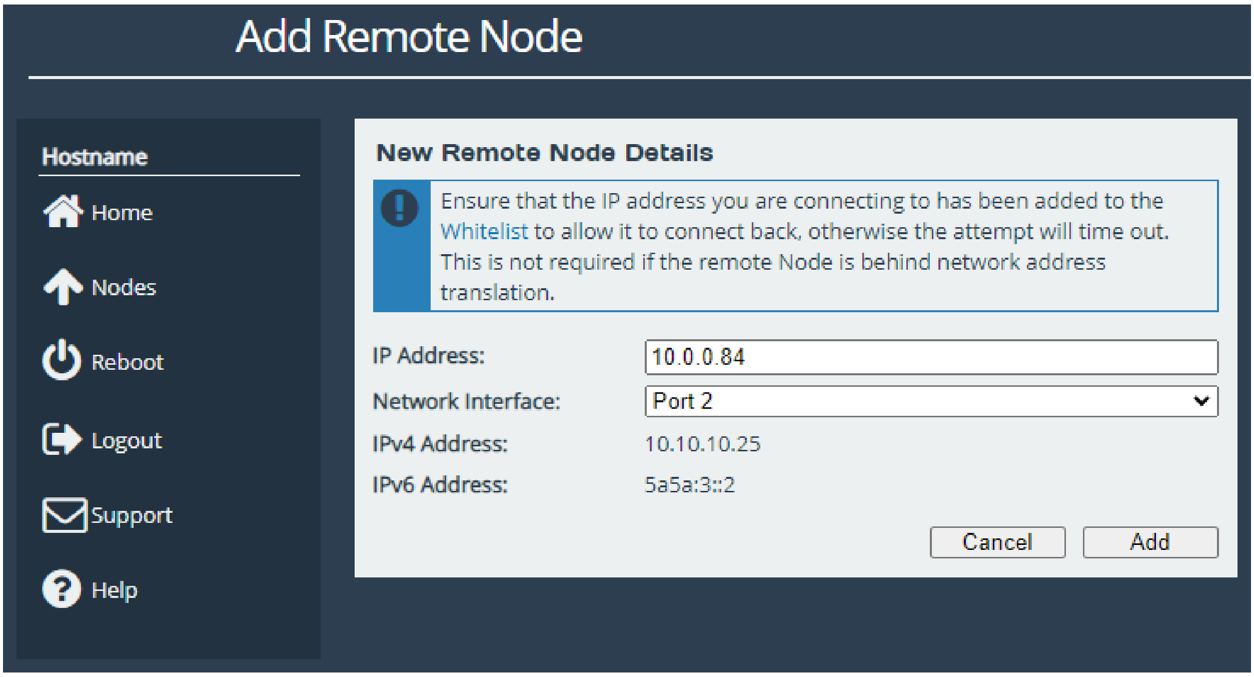
When the connection has been established, a dialog will show the hostname of the remote Node.


Add Remote Node
Hostname
Home
Nodes
Reboot
Logout
Support
Help
New Remote Node Details
Ensure that the IP address you are connecting to has been added to the Whitelist to allow it to connect back, otherwise the attempt will time out. This is not required if the remote Node is behind network address translation.
IP Address:
Network Inte
IPv4 Address
IPv6 Address
Add

Connected to Node

Hostname Node_B

The next stage is to perform Node discovery in the other direction. From the *Node Management* of Node B, click the *Add Node* button to bring up a dialog box, and enter the IP address of the WAN port of Node A. Click *Add* to negotiate a connection between the Nodes.

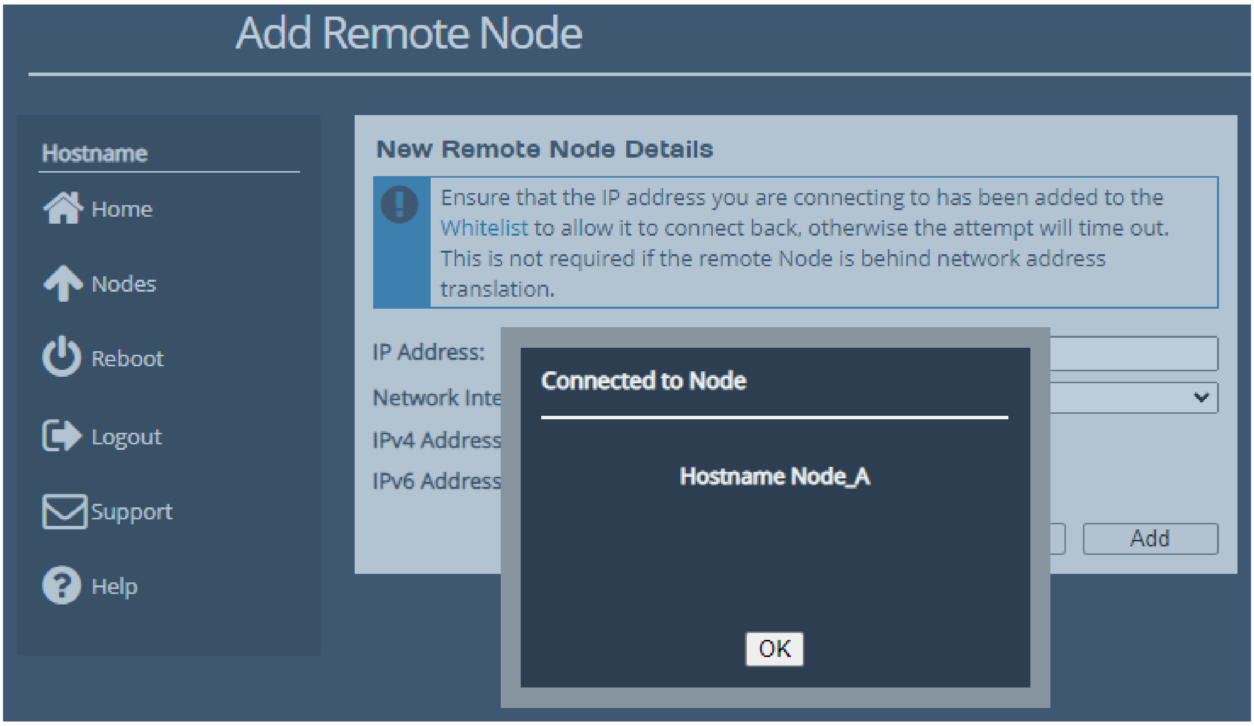


New Remote Node Details

Ensure that the IP address you are connecting to has been added to the Whitelist to allow it to connect back, otherwise the attempt will time out. This is not required if the remote Node is behind network address translation.

IP Address: 10.0.0.84
Network Interface: Port 2
IPv4 Address: 10.10.10.25
IPv6 Address: 5a5a:3::2

When the connection has been established, a dialog will appear.



Ensure that the IP address you are connecting to has been added to the Whitelist to allow it to connect back, otherwise the attempt will time out. This is not required if the remote Node is behind network address translation.

Connected to Node

Hostname Node_A

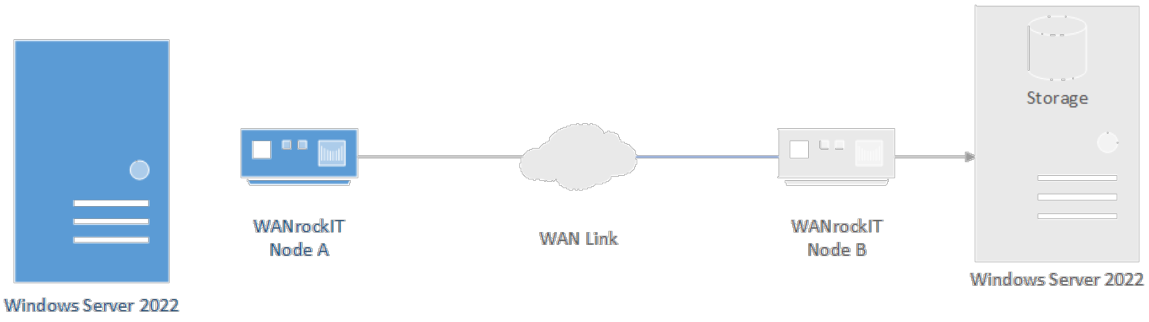
Congratulations, you have successfully set up a connection between your Nodes.

8 Configuring your WANrockIT Node to Present iSCSI Targets from Off-Premise to On-Premise

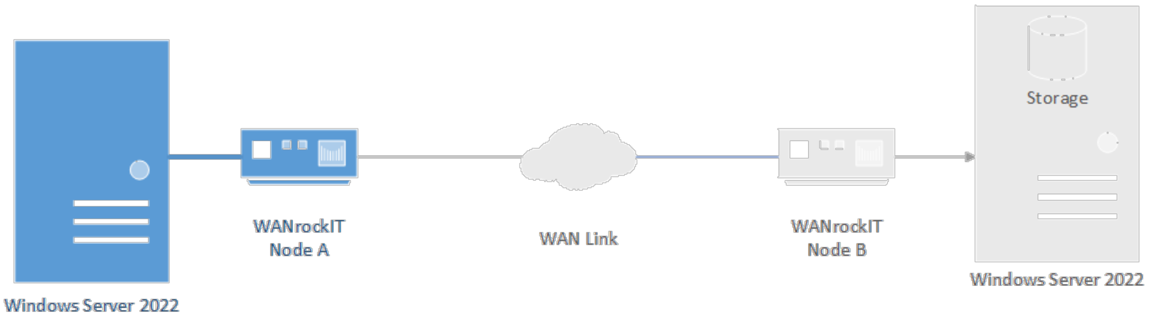
8.1 Introduction

This section describes how to log on to the iSCSI Target Portal from your On-Premise Node using a Windows Server 2022 machine, allowing the devices Off-Premises to be presented over a WANrockIT connection locally. This section uses the Microsoft iSCSI Initiator on a Windows Server 2022 machine and a WANrockIT Node.

The following diagram illustrates the described topology.



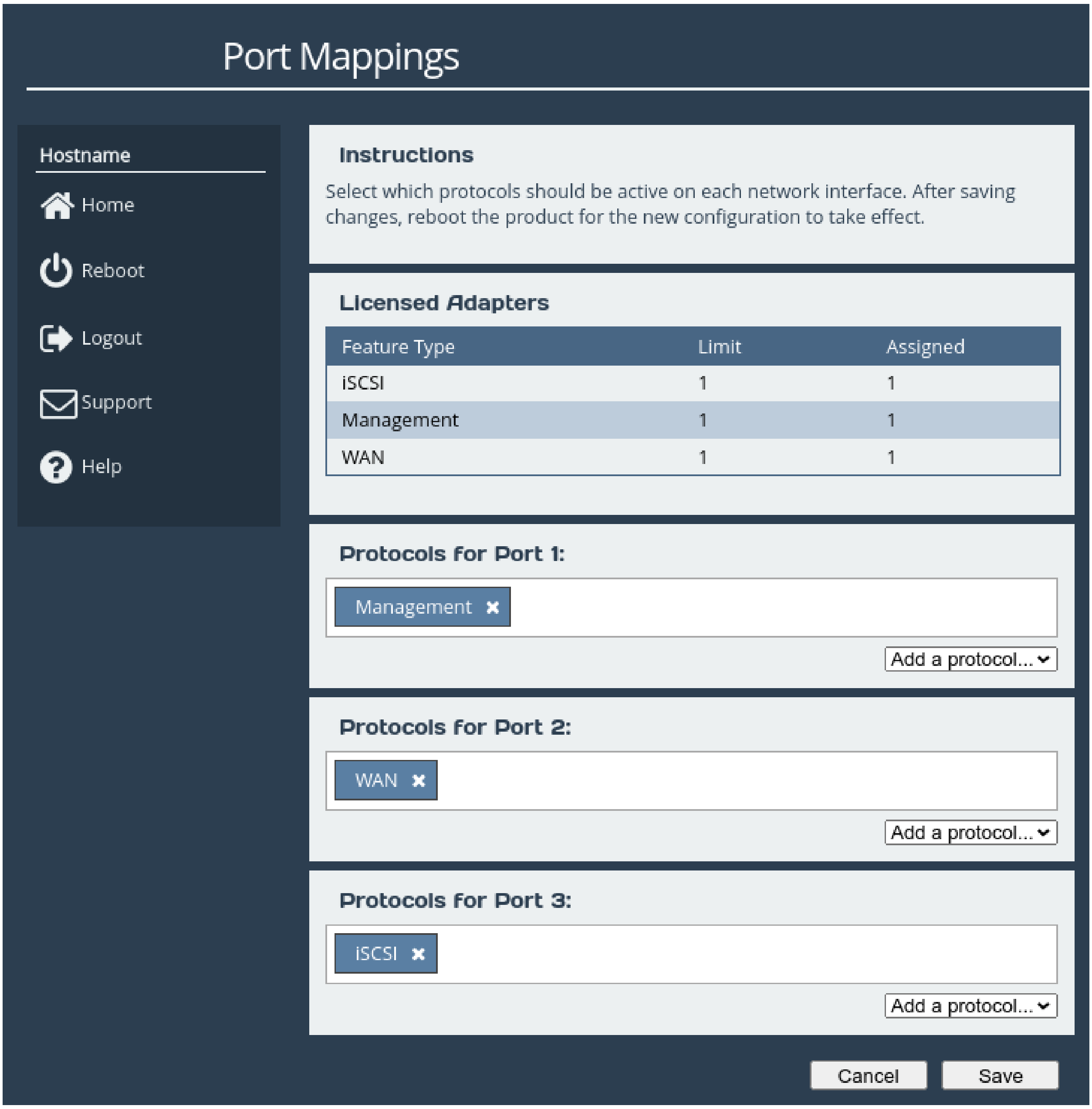
Once you have completed the following instructions your topology will have changed to the following.



8.2 Configuring Features

Proceed to the web interface of your WANrockIT Node through the IP address of the management interface (by default, *Port 1*). Enter the username `admin` along with your password to log in to the Node.

Ensure that the *iSCSI* protocol is mapped to the port from which you wish to establish a connection. In this case, *Port 3* is used, as shown in the image below. A reboot is required for any changes to the port mappings to take effect. For a more detailed guide on port mappings see Port Mappings.



Port Mappings

Instructions

Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.

Licensed Adapters

Feature Type	Limit	Assigned
iSCSI	1	1
Management	1	1
WAN	1	1

Protocols for Port 1:

Management ✖

Protocols for Port 2:

WAN ✖

Protocols for Port 3:

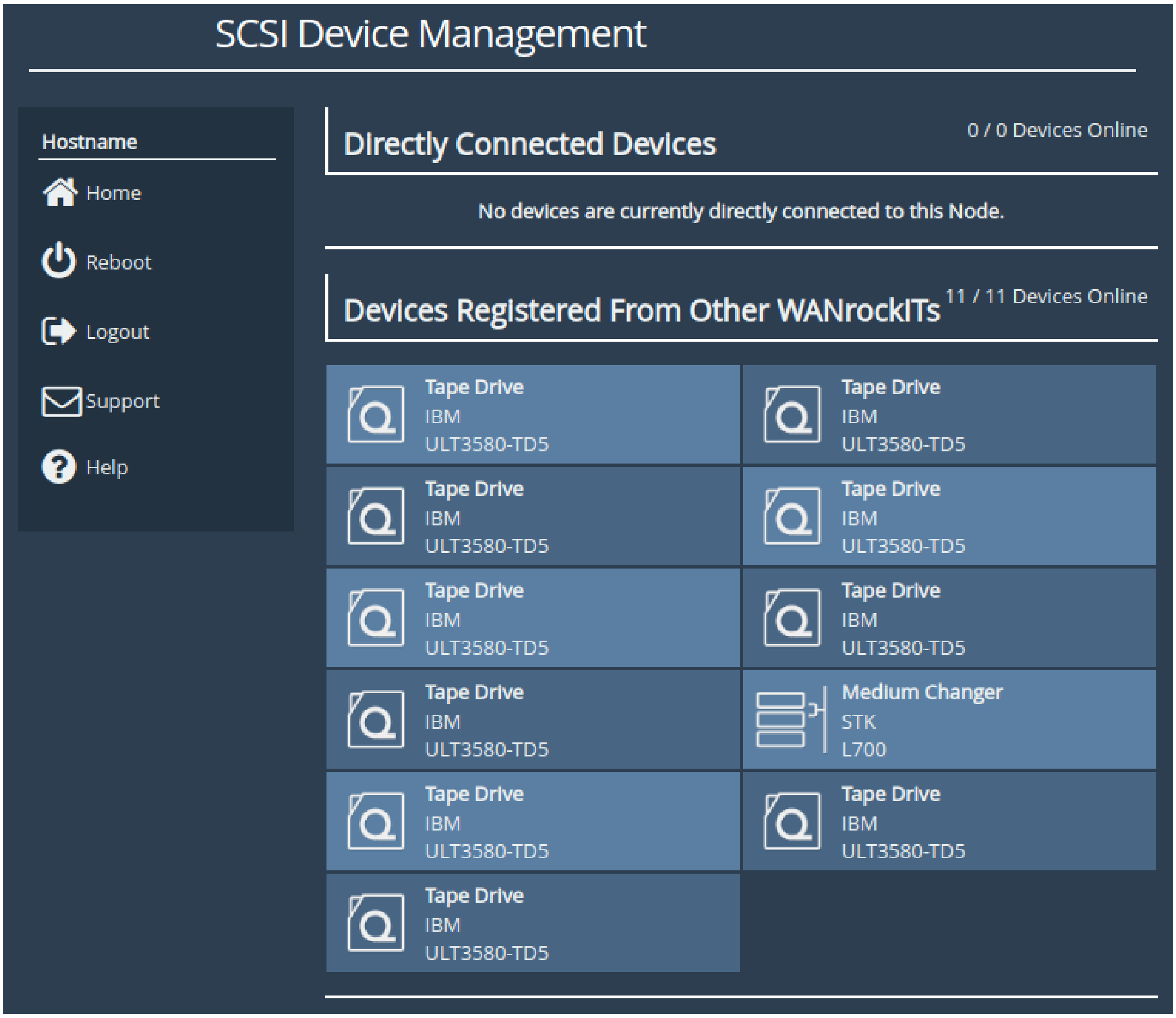
iSCSI ✖

8.3 Confirming the Presence of iSCSI targets

In order to confirm that iSCSI targets will be presented to your initiator, confirm that remote WANrockIT Nodes display devices present on your Node. To do this, navigate to *SCSI Device*

Management by clicking the corresponding icon as shown below.

The *Device List* page lists all devices connected to the current Node either as *Directly Connected Devices* (i.e. an iSCSI login was performed from this Node to an external iSCSI target) or as *Devices registered from other WANrockIT Nodes* (i.e. a WAN connection was established to another WANrockIT instance which has *Directly Connected Devices*.



SCSI Device Management

Directly Connected Devices

0 / 0 Devices Online

No devices are currently directly connected to this Node.

Devices Registered From Other WANrockITs

11 / 11 Devices Online

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Medium Changer
STK
L700

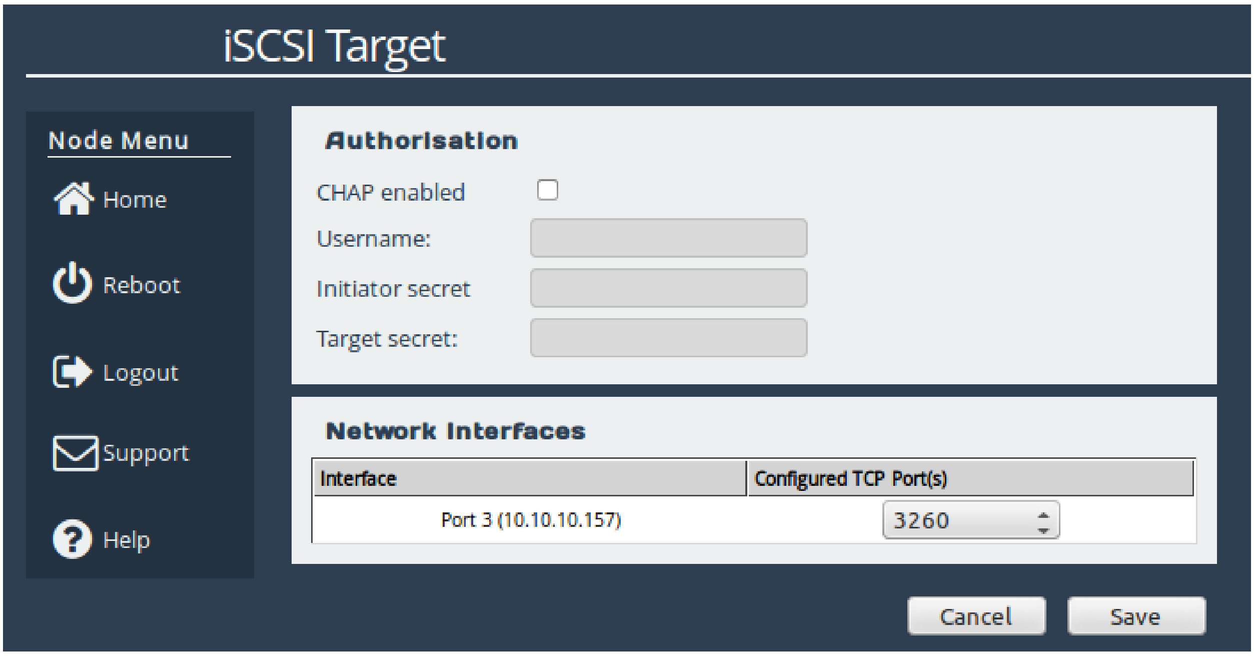
Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Tape Drive
IBM
ULT3580-TD5

Only devices which are registered from other WANrockIT Nodes will be available for a local iSCSI connection. As soon as your mappings are configured and you have confirmed that your devices are presented locally, return to the Home screen of the Node and navigate to the *iSCSI Target* page by clicking on the corresponding icon.

You will then be presented with the following screen.



Authorisation

CHAP enabled ☐

Username:

Initiator secret

Target secret:

Network Interfaces

Interface	Configured TCP Port(s)
Port 3 (10.10.10.157)	3260

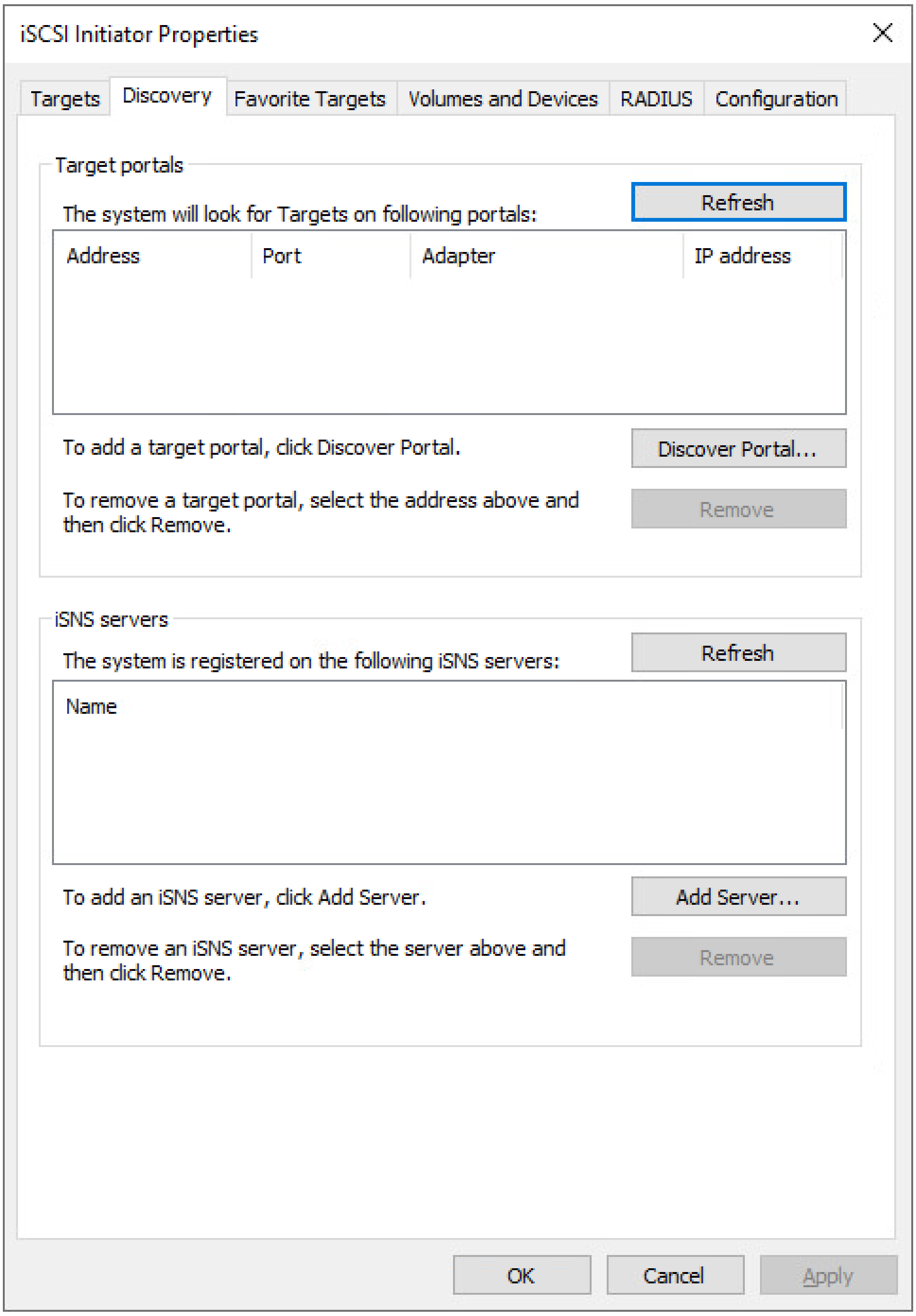
If you wish to enable one-way or mutual CHAP authentication, this can be done under the *Authorisation* subsection. Click the *CHAP enabled* check box and enter in your required details.

Under the *Network Interfaces* subsection, the TCP port on which iSCSI is available for each *Network Interface* can be altered from the default of
3260 to 860. Alternatively, you can enable both TCP ports. Make a note of the local IP address of the interface to which you wish to connect. If you have changed any settings on this page, click *Save* to confirm. Any changes made will take effect immediately.

You are now ready to perform an iSCSI discovery, and subsequently log on to remote devices.

8.4 Using the Microsoft iSCSI Initiator to Log onto Targets

Open the iSCSI initiator, then click on the *Discovery* tab. You should see the following window.



The system will look for Targets on following portals:

To add a target portal, click Discover Portal.

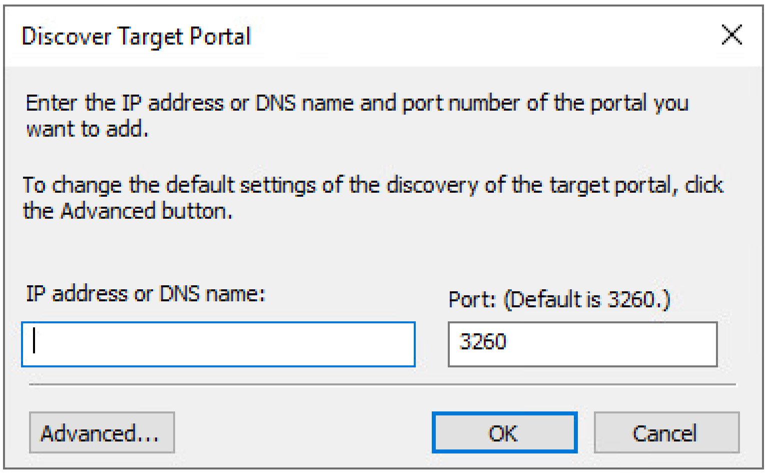
To remove a target portal, select the address above and then click Remove.

The system is registered on the following iSNS servers:

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

To add an iSCSI Target portal, click on *Discover Portal*. You will be presented with a second window.



Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

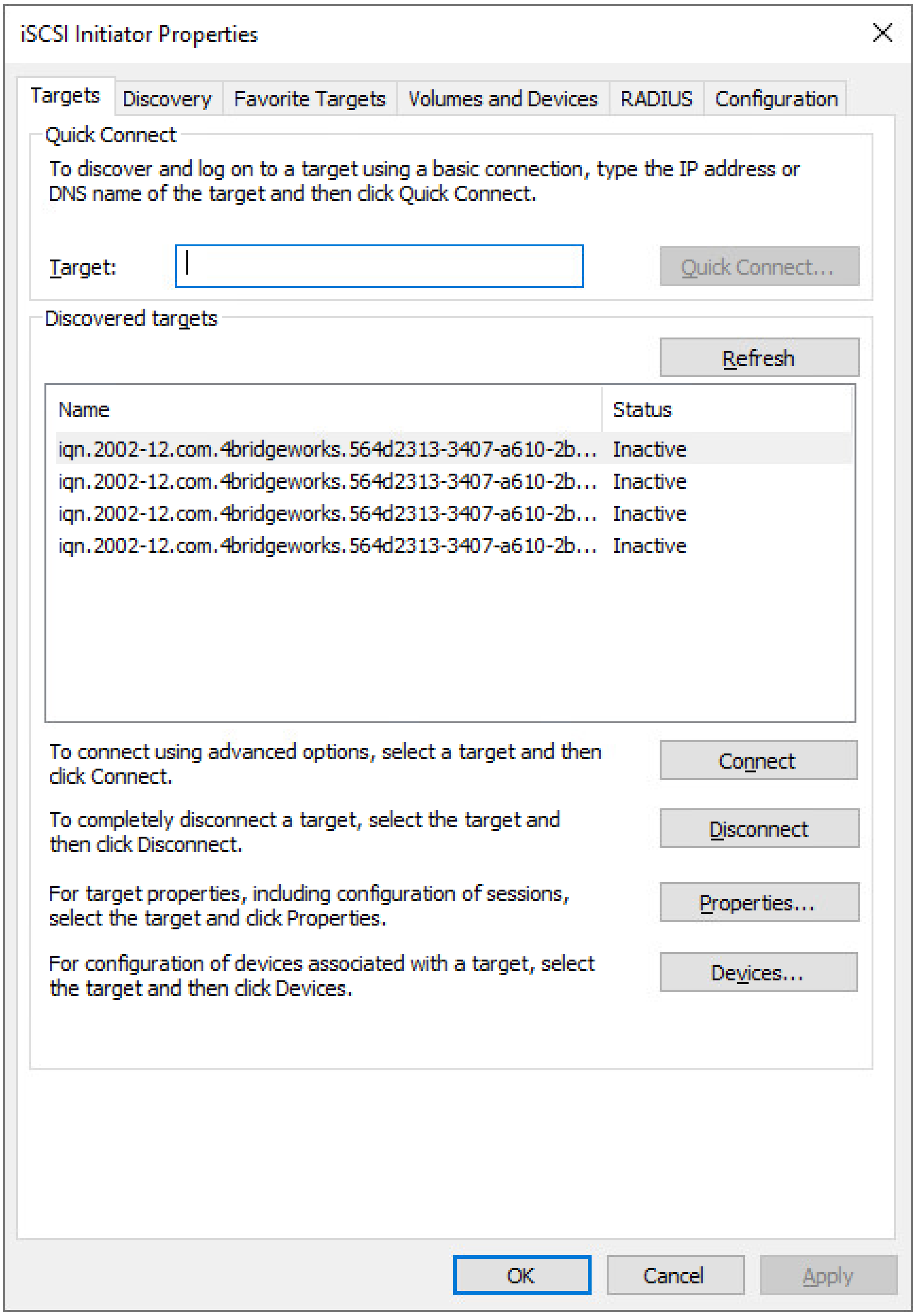
IP address or DNS name:

Port: (Default is 3260.) 3260

Enter the IP address noted down previously from the *iSCSI Target* page from the WANrockIT web interface. Ensure the port matches your iSCSI configuration, either the default of 3260, or 860.

Click *OK* and the Microsoft iSCSI Initiator shall perform the discovery. This can take up to a minute with multiple network ports.

Click on the *Targets* tab. The devices discovered should now be listed and shown as below.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Name	Status
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive

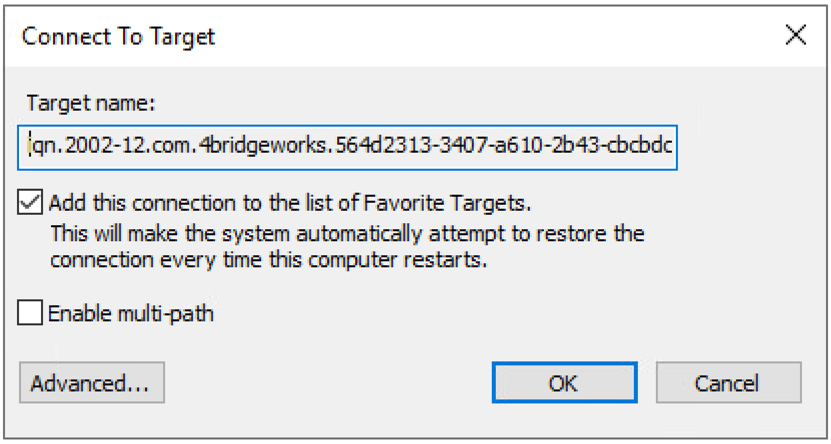
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

In the example above, multiple targets are now presented. To connect to one of the iSCSI targets, click on one of the target names and then click the *Connect* button. A window will appear.



Connect To Target

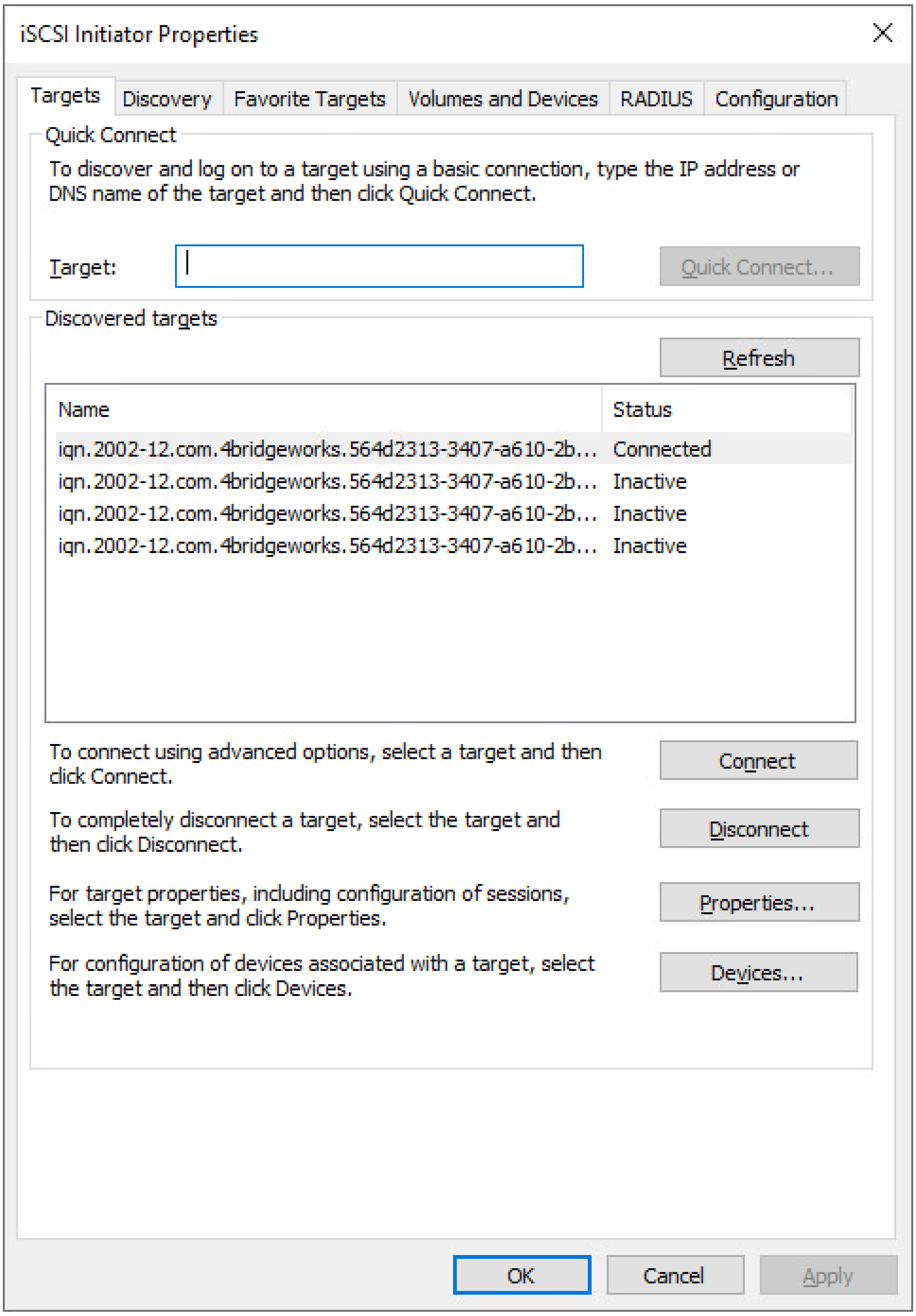
Target name:

iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b43-cbcbdc

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

Click the *OK* button and the status will change to *Connected*, as shown below.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Name	Status
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Connected
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive
iqn.2002-12.com.4bridgeworks.564d2313-3407-a610-2b...	Inactive

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

9 Refreshing iSCSI targets through your WAN link

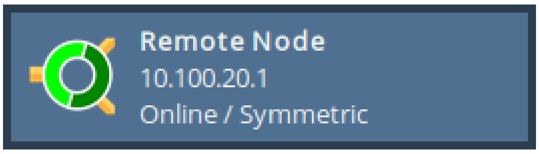
9.1 Introduction

From time to time, it may become necessary to refresh the devices presented though your WAN link. This occurs if you have added or removed devices after your initial setup. This is only available if you have an iSCSI protocol mapped to one of your network ports.

This section of the guide is helpful if your devices are missing, or you experience link slowdown caused by WANrockIT Nodes attempting to access devices that are no longer present.

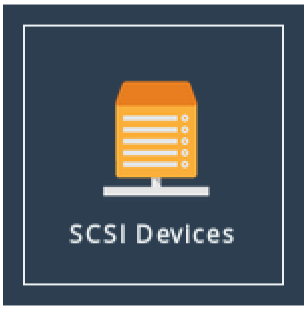
9.2 Refreshing Your Devices

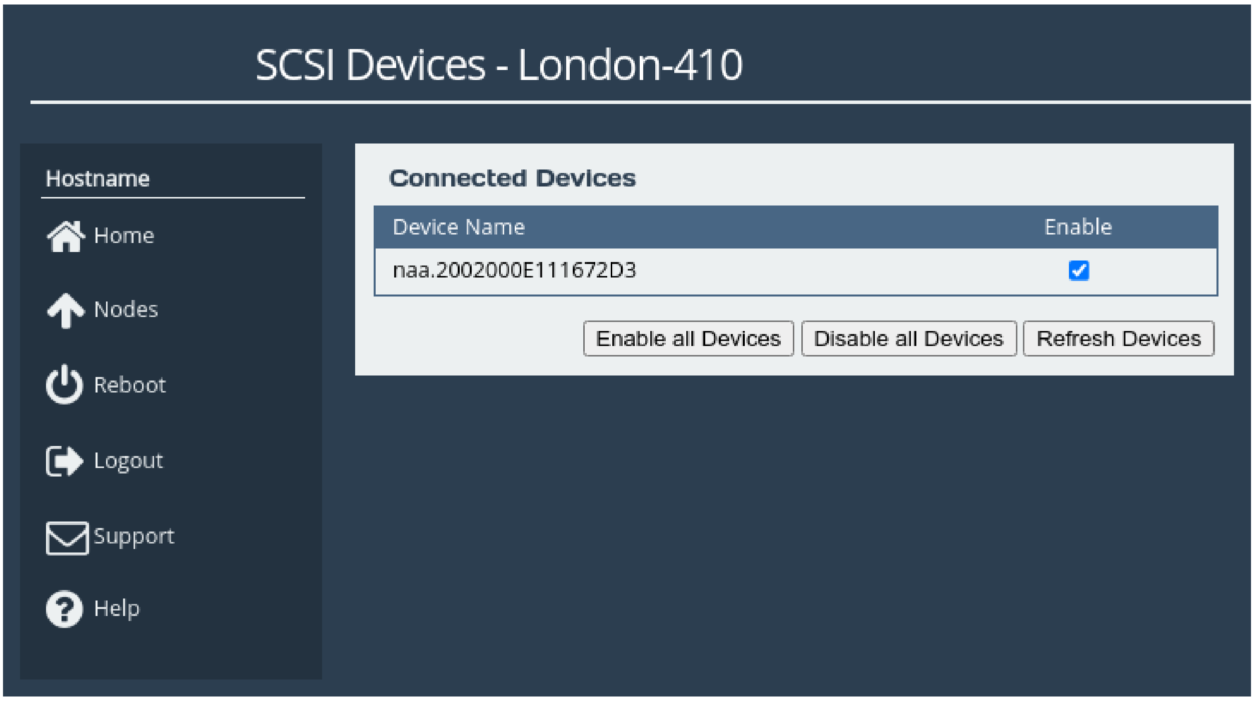
From the Node's web interface, navigate to the *Node Management page*, then click on the appropriate remote node like the following.



Remote Node
10.100.20.1
Online / Symmetric

After navigating to the remote node, the *SCSI Devices* page can be accessed by clicking the corresponding icon.



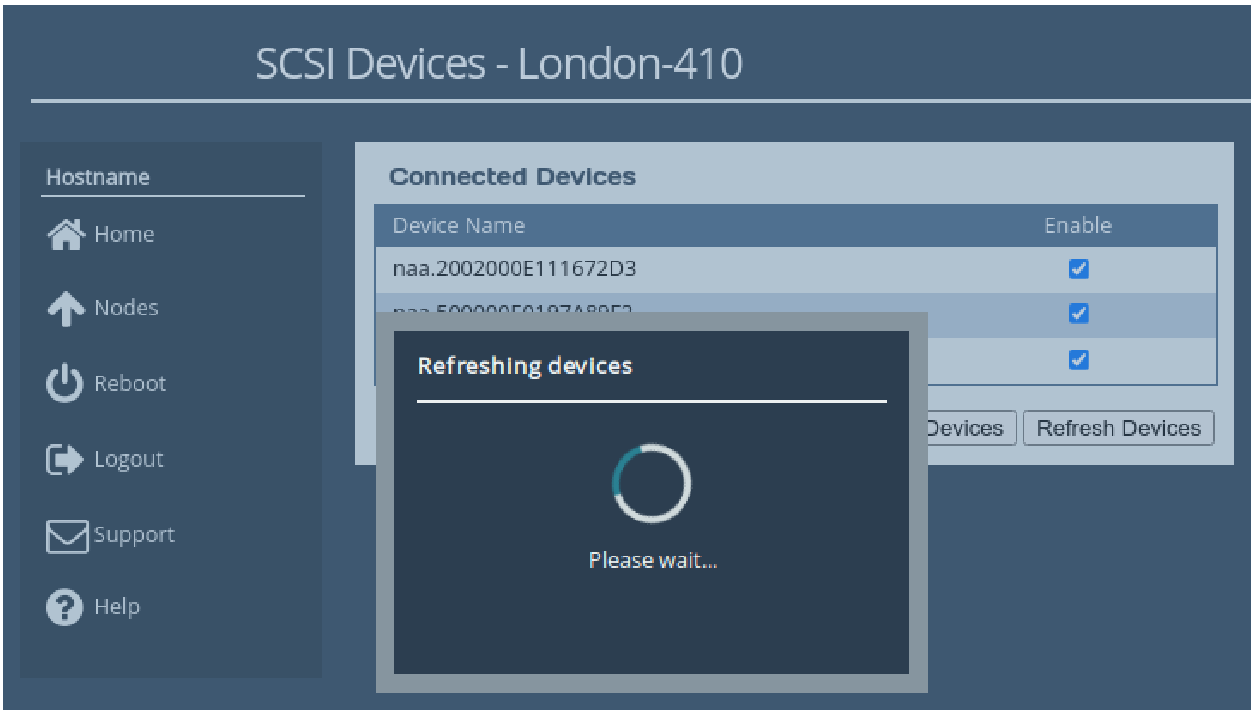


SCSI Devices - London-410

Connected Devices

Device Name	Enable
naa.2002000E111672D3	☑

A list of currently visible devices will be presented in the *Connected Devices* table. To refresh your Node for new devices click the *Refresh Devices* button.



SCSI Devices - London-410

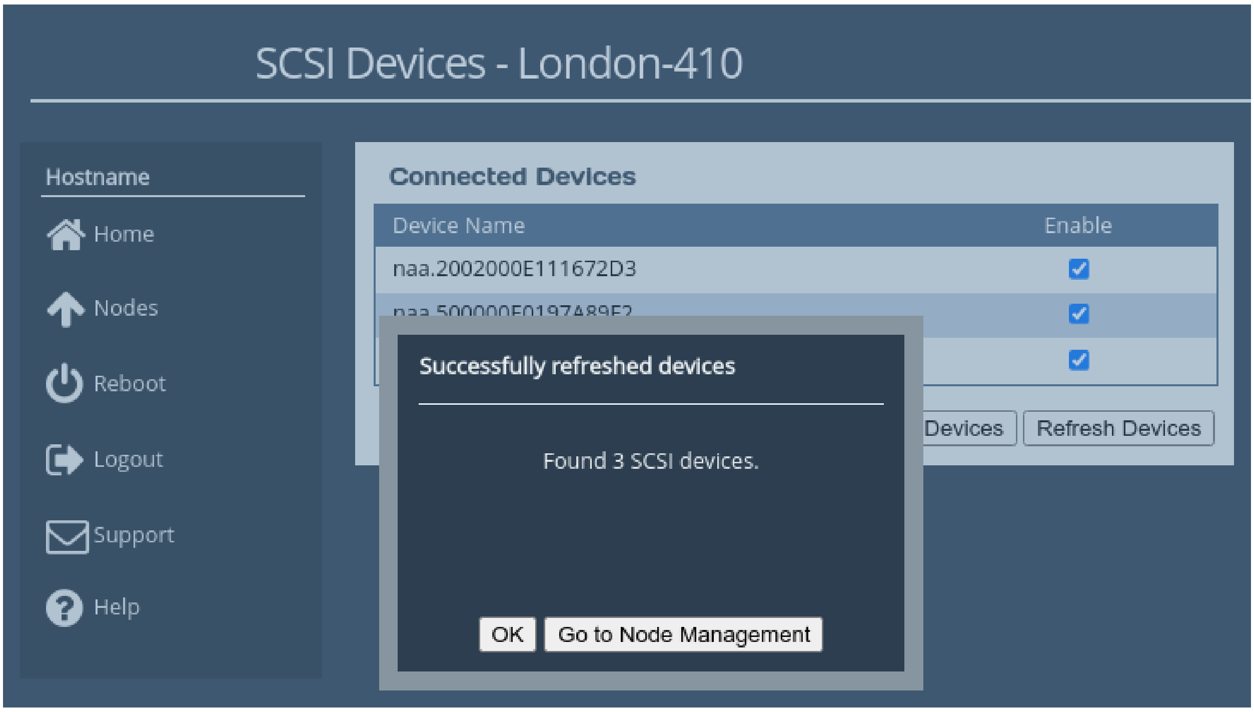
Connected Devices

Device Name	Enable
naa.2002000E111672D3	☑
[illegible]	☑
	☑

Refreshing devices

Please wait...

Upon completion a summary of the results is shown.


SCSI Devices - London-410

Connected Devices

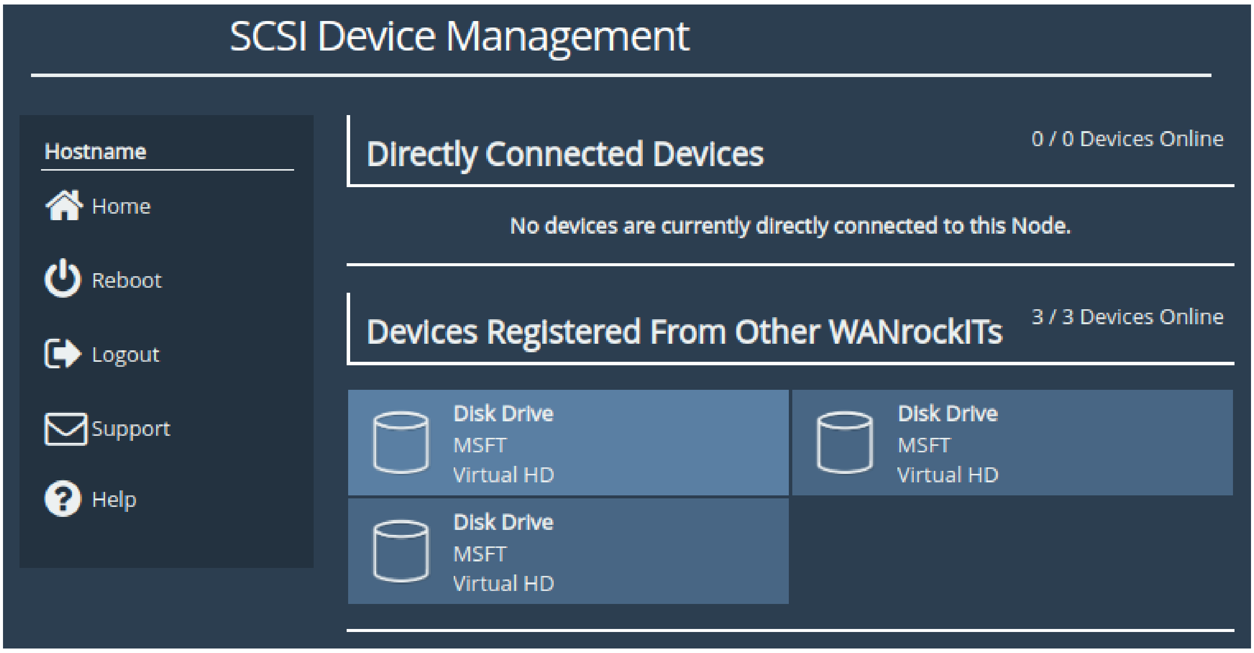
Device Name	Enable
naa.2002000E111672D3	☑
naa.500000E0197A89F2	☑
	☑

Successfully refreshed devices

Found 3 SCSI devices.

Click the *OK* button. The list of devices will now update to include the newly discovered targets.

For a more detailed view of the newly added devices, navigate to the Home screen and navigate to the *SCSI Device Management* page.


SCSI Device Management

Directly Connected Devices

0 / 0 Devices Online

No devices are currently directly connected to this Node.

Devices Registered From Other WANrockITs

3 / 3 Devices Online

Disk Drive
MSFT
Virtual HD

Disk Drive
MSFT
Virtual HD

Disk Drive
MSFT
Virtual HD

The three devices registered from the remote WANrockIT Node are displayed. Clicking on a target shows more information.

Congratulations, you have successfully refreshed and updated the targets presented over your WANrockIT link.

10 Completion

Congratulations, you have completed the setup of your WANrockIT Nodes. If you need any more help with your setup, please see the section below.

11 Useful Links

Further documentation and support is available through our website: https://support.4bridgeworks.com/

If your question is not answered in our documentation, please submit a ticket: https://support.4bridgeworks.com/contact/