WANrockIT (iSCSI) Setup Guide Eli-v6.2.20

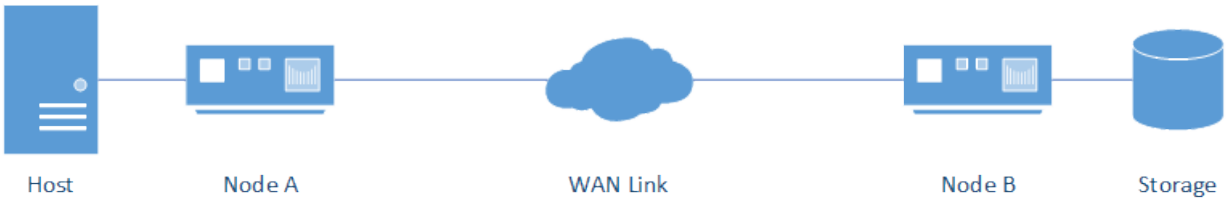
Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

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

☐ Step 3. Configuring IPsec

☐ Step 4. Establishing a Link Between Nodes

☐ Step 5. Configuring your WANrockIT Node to Present iSCSI Targets from Off-Premise to On-Premise

☐ Step 6. Refreshing iSCSI targets through your WAN link

3 Initial Setup of your Bridgeworks Node

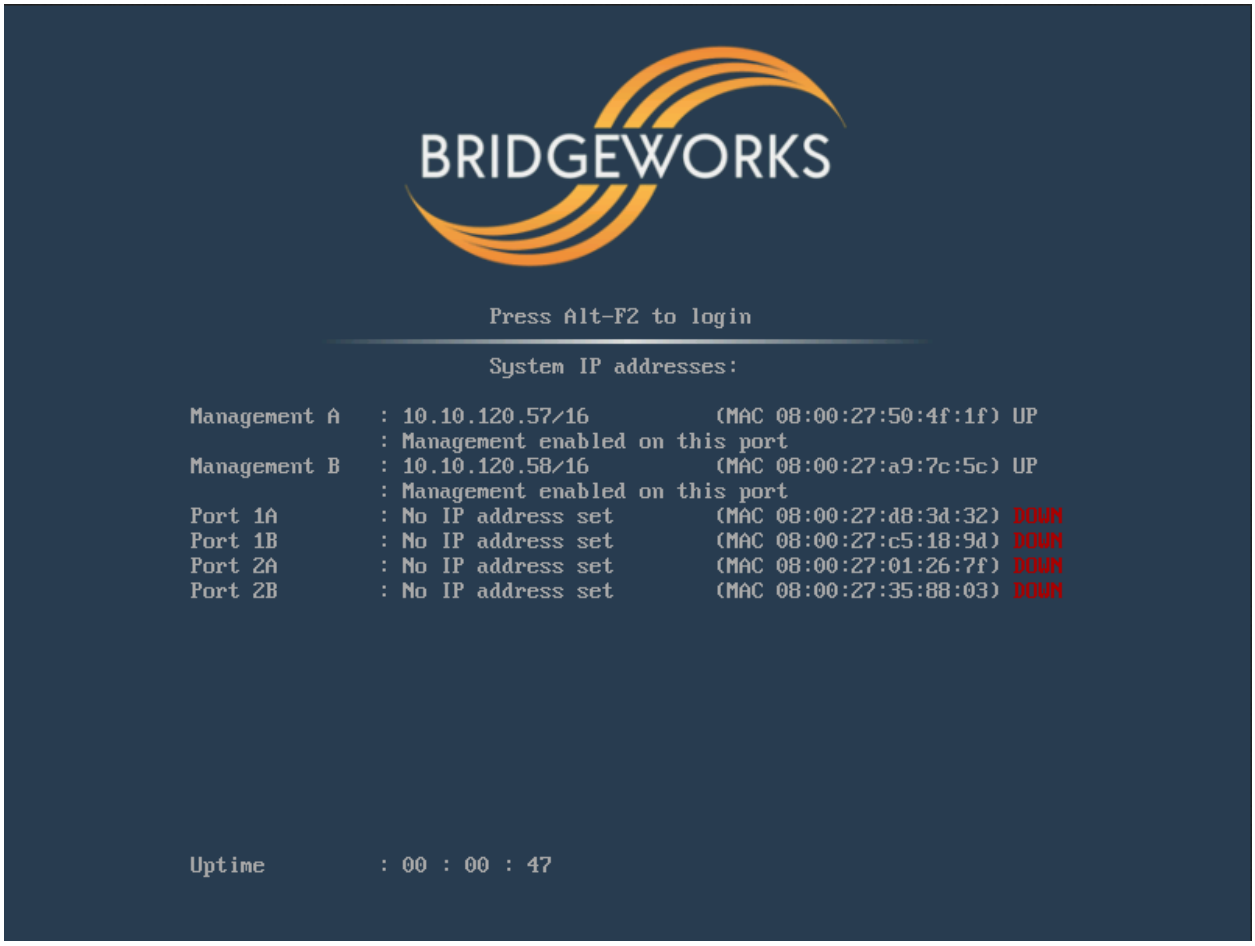
3.1 Finding Management IP addresses

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/`

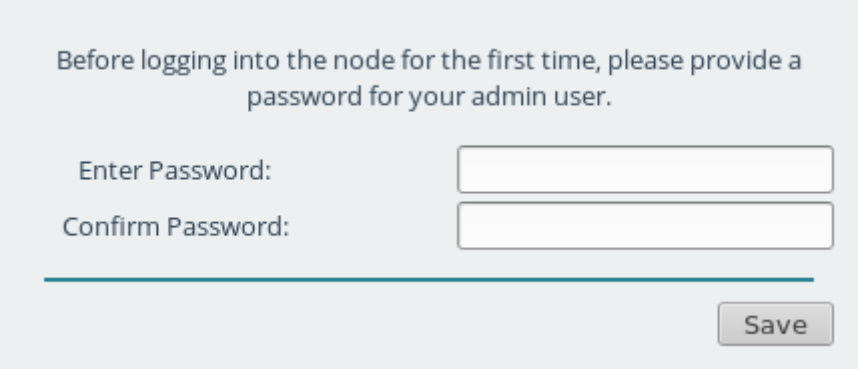
To find the IP addresses of management interfaces easily, it is recommended to use the VGA or virtual console as shown below.



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.

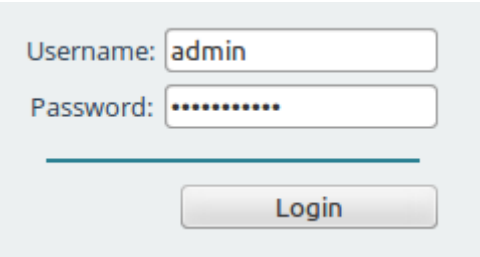


	Important: During deployment of Azure Nodes you are able to set the initial password if you choose to use password authentication. If you set up your password this way, you will be directed to the login screen.

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.

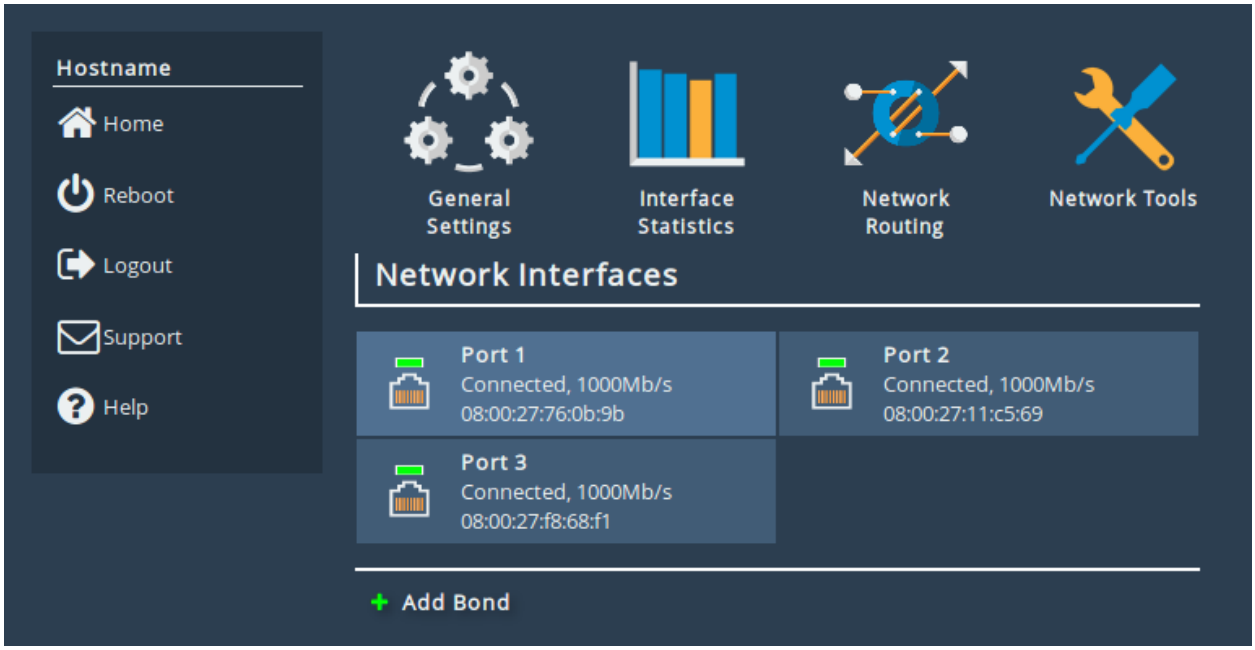


3.4 Network Connections ( )

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.

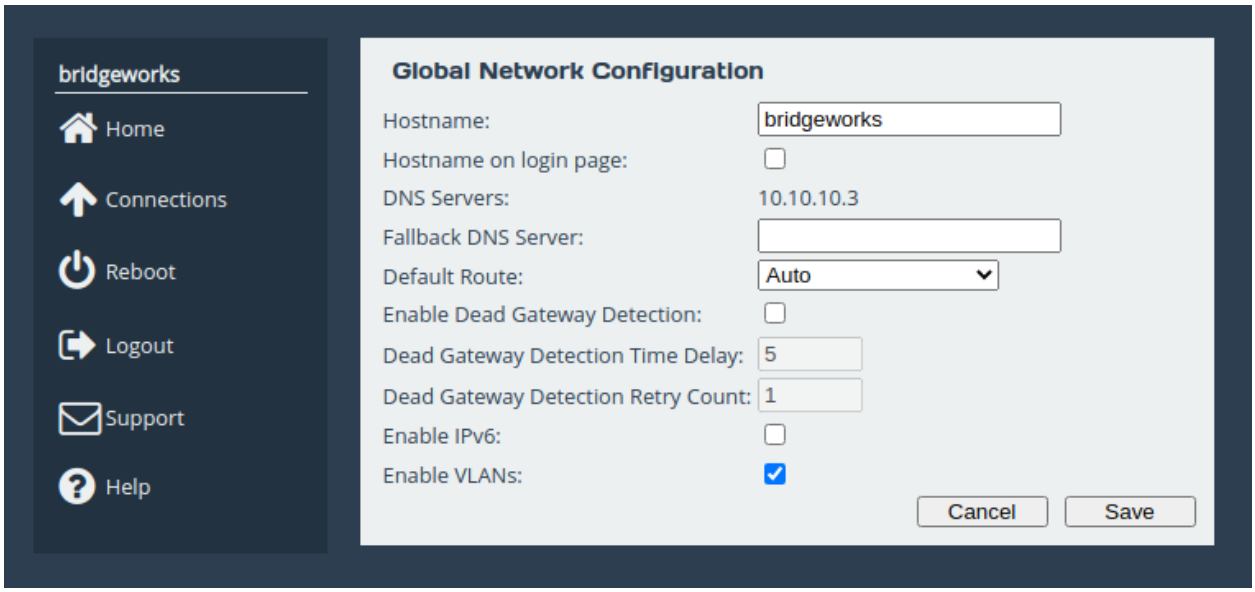
3.4.1 Setting the Hostname/Node Name

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



The hostname of the Node can be changed by replacing the default name

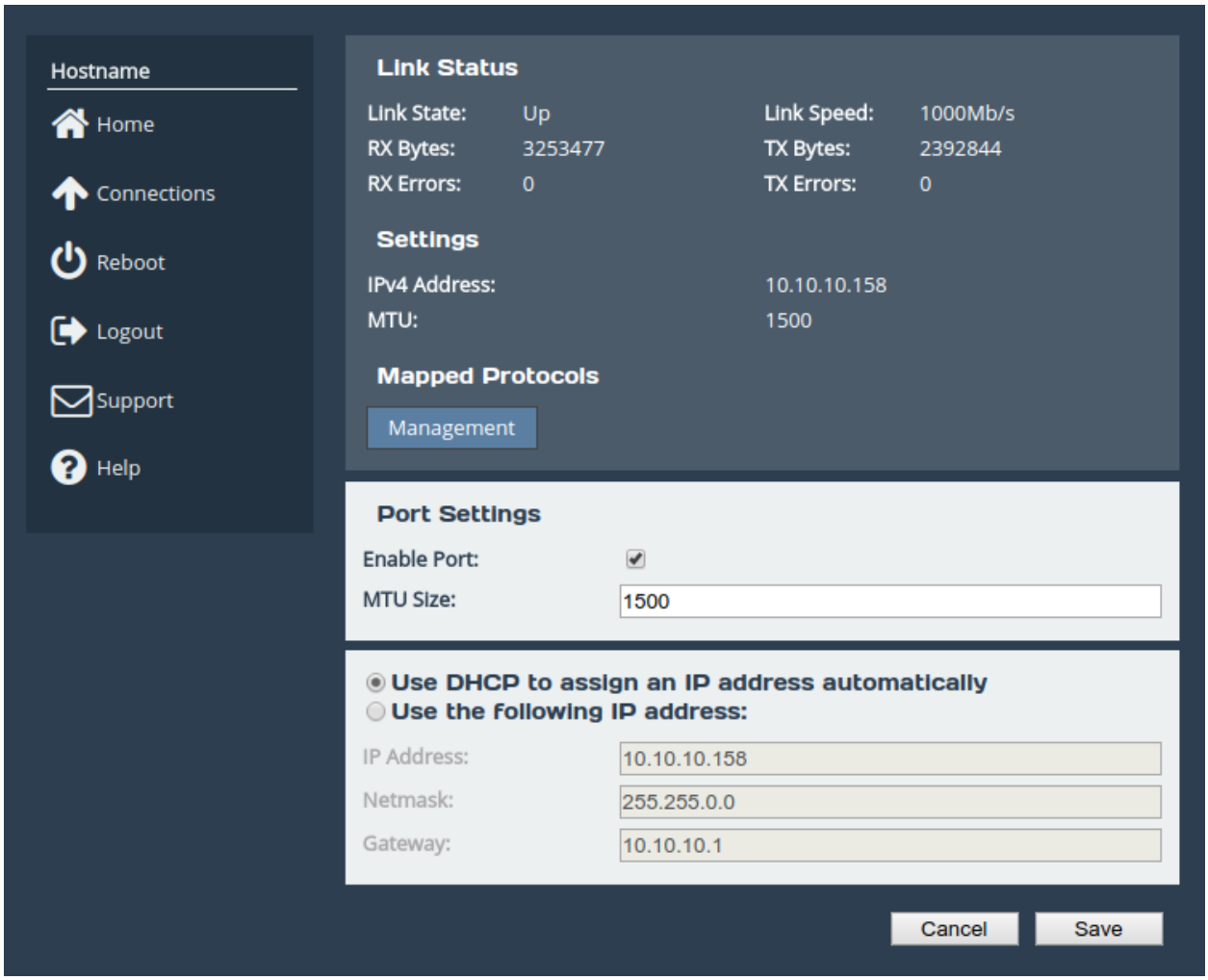
`bridgeworks` with a name of your choice. This name is also the alias name used for identifying your Nodes under the *Node Management* section.



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

3.4.2 Changing IP Addresses

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.



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.

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

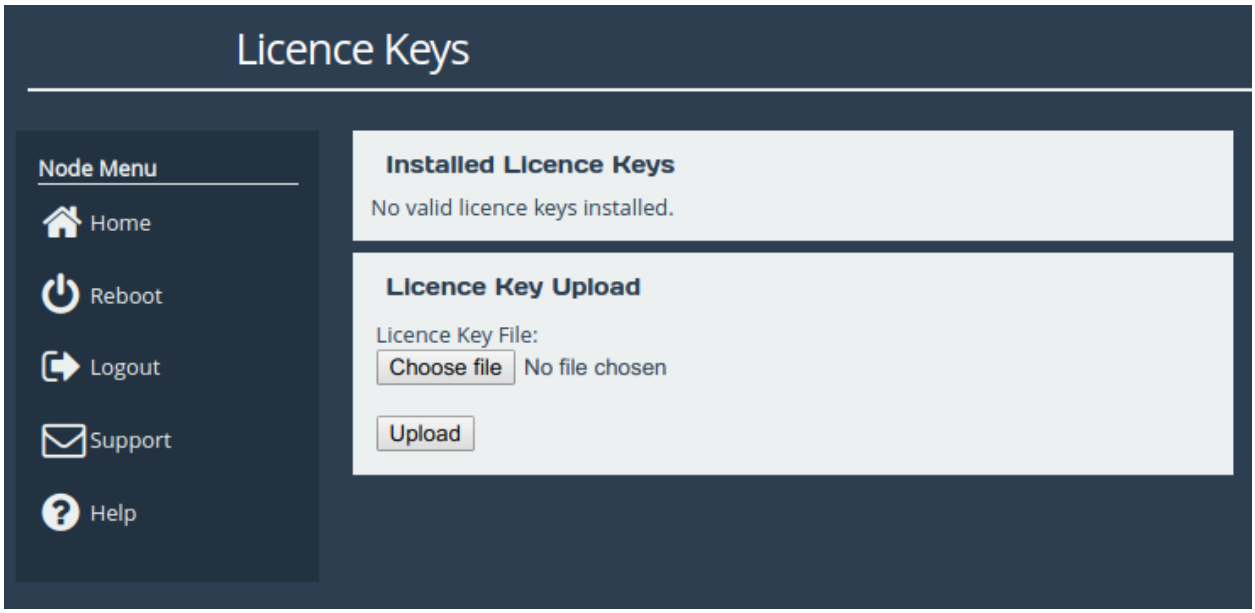
All PORTrockIT and WANrockIT products require a licence key in order to unlock the acceleration features of the product.

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

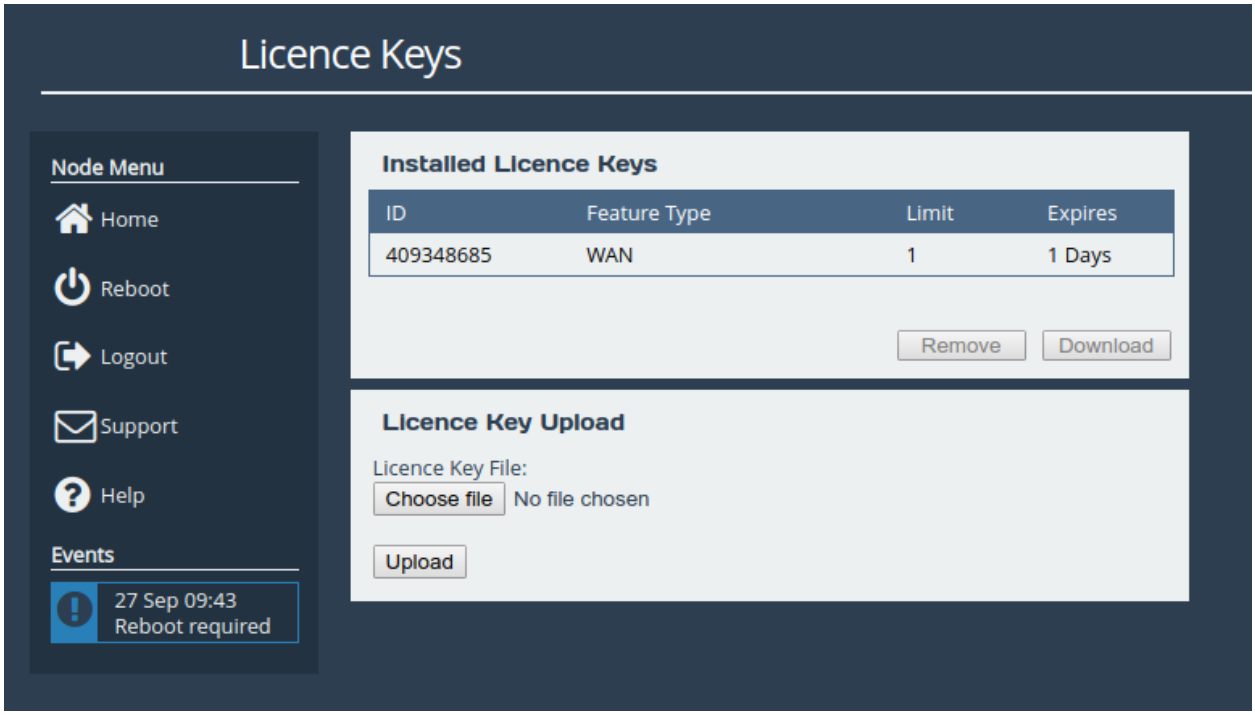
Once you have received the licence key, log into the web interface of the Node and go to the *Licence Key Management* page.

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



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

remain active.



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

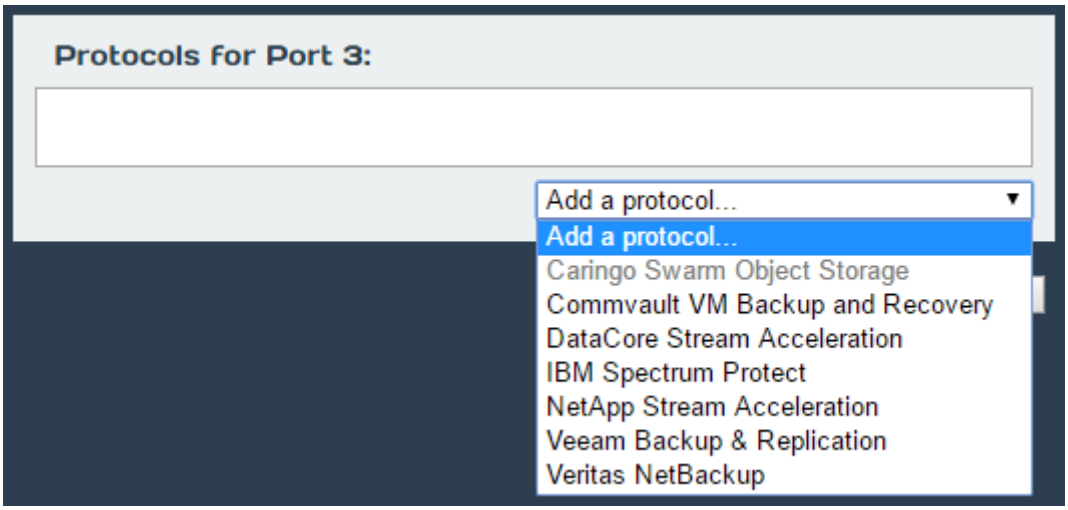
3.6 Port Mappings ( )

3.6.1 Overview

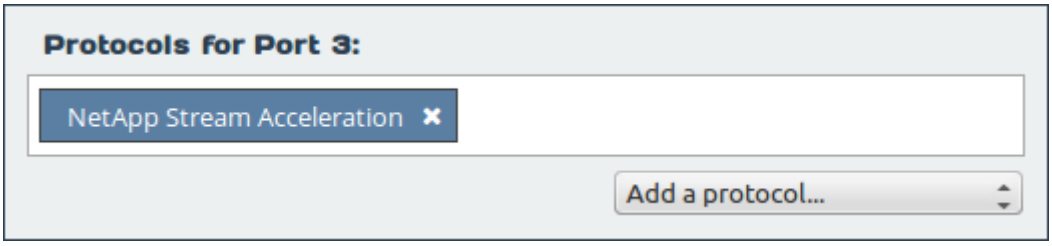
Port Mappings allows for the assignment of protocols to network interfaces. For example, adding *WAN* to a port will allow WAN connections and acceleration from that network port. Except for the WAN protocol, protocols are related to the types of traffic to be accelerated on that port. For example, enabling 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.

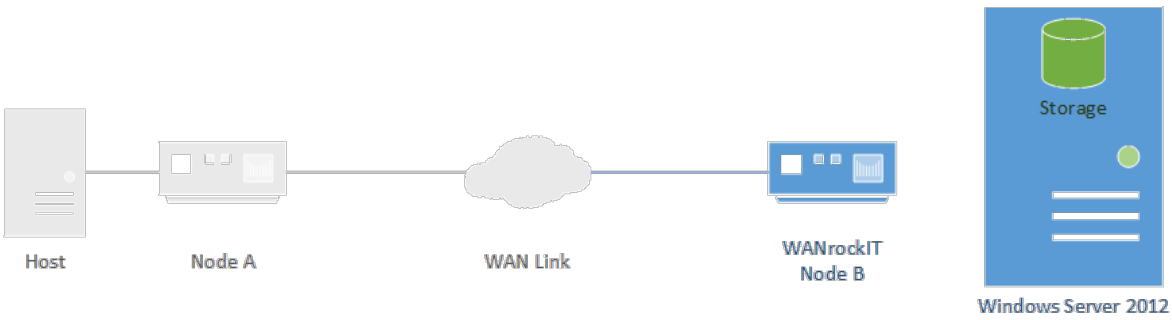
Once the configuration is complete, click on the *Save* button. A reboot is required for the changes to take effect.

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

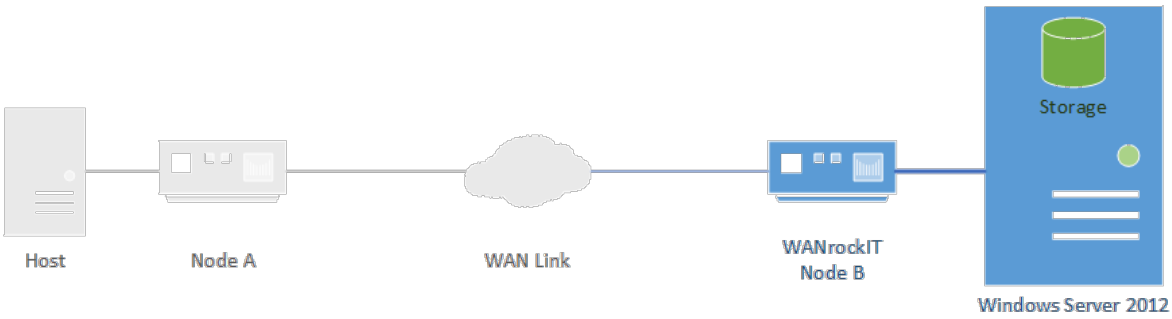
4.1 Introduction

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 2012 machine and a WANrockIT Node.

The following diagram illustrates the described topology.

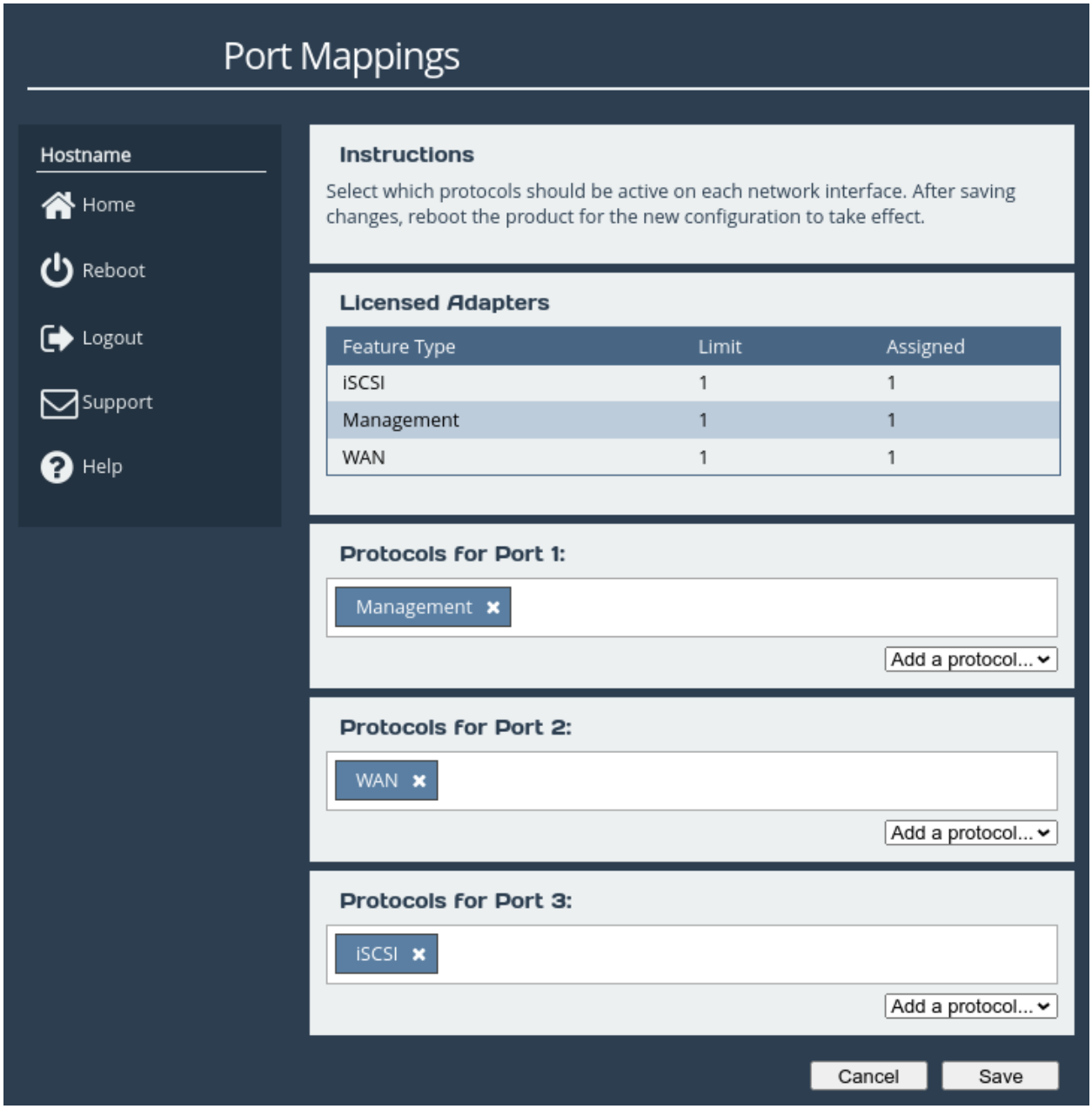


Once you have completed the following instructions your topology have changed to the following.



4.2 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.



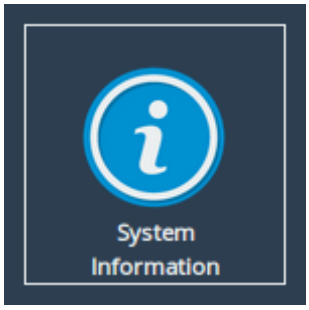
4.3 Setting up an Access Control List on Windows Server

4.3.1 Retrieving the WANrockIT's IQN

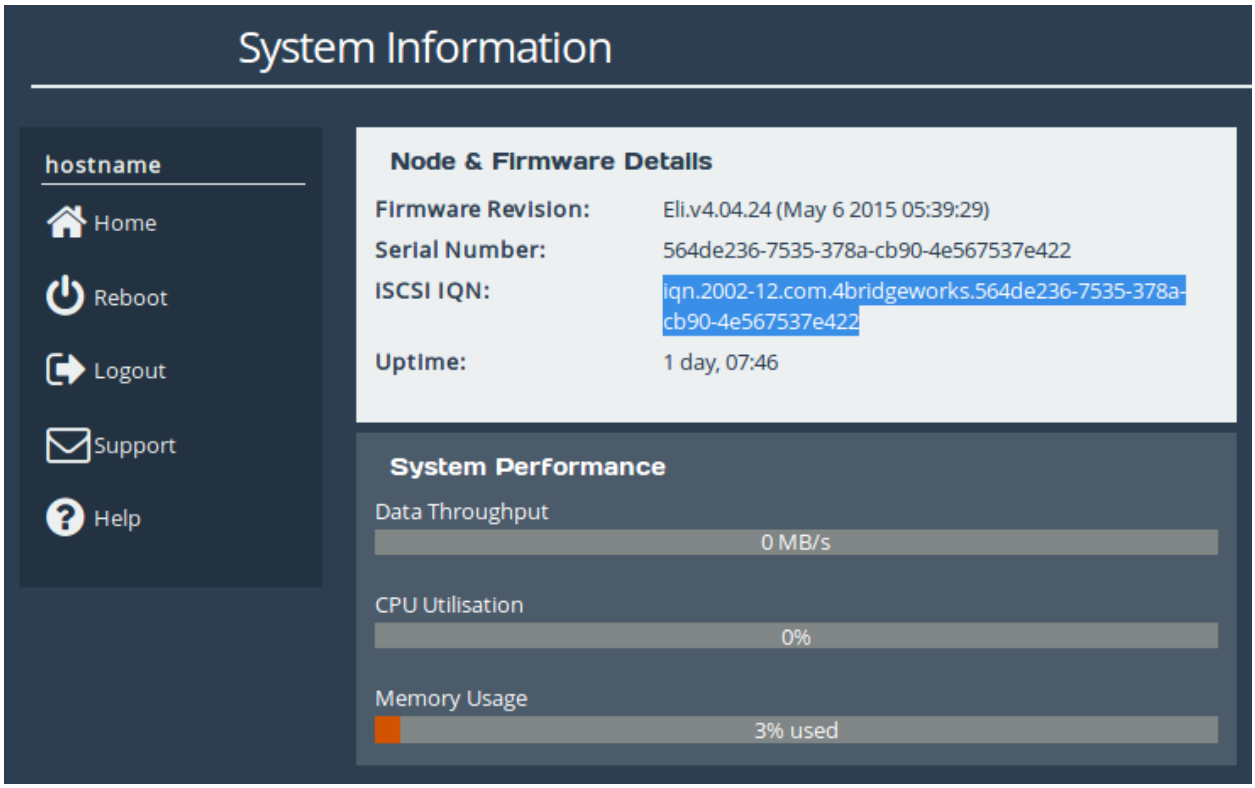
The Microsoft iSCSI virtual disk target requires entries to be added to an access list. Typically, an IQN is added to the list. Alternatively, an IP address can be added. Not all targets require this

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.

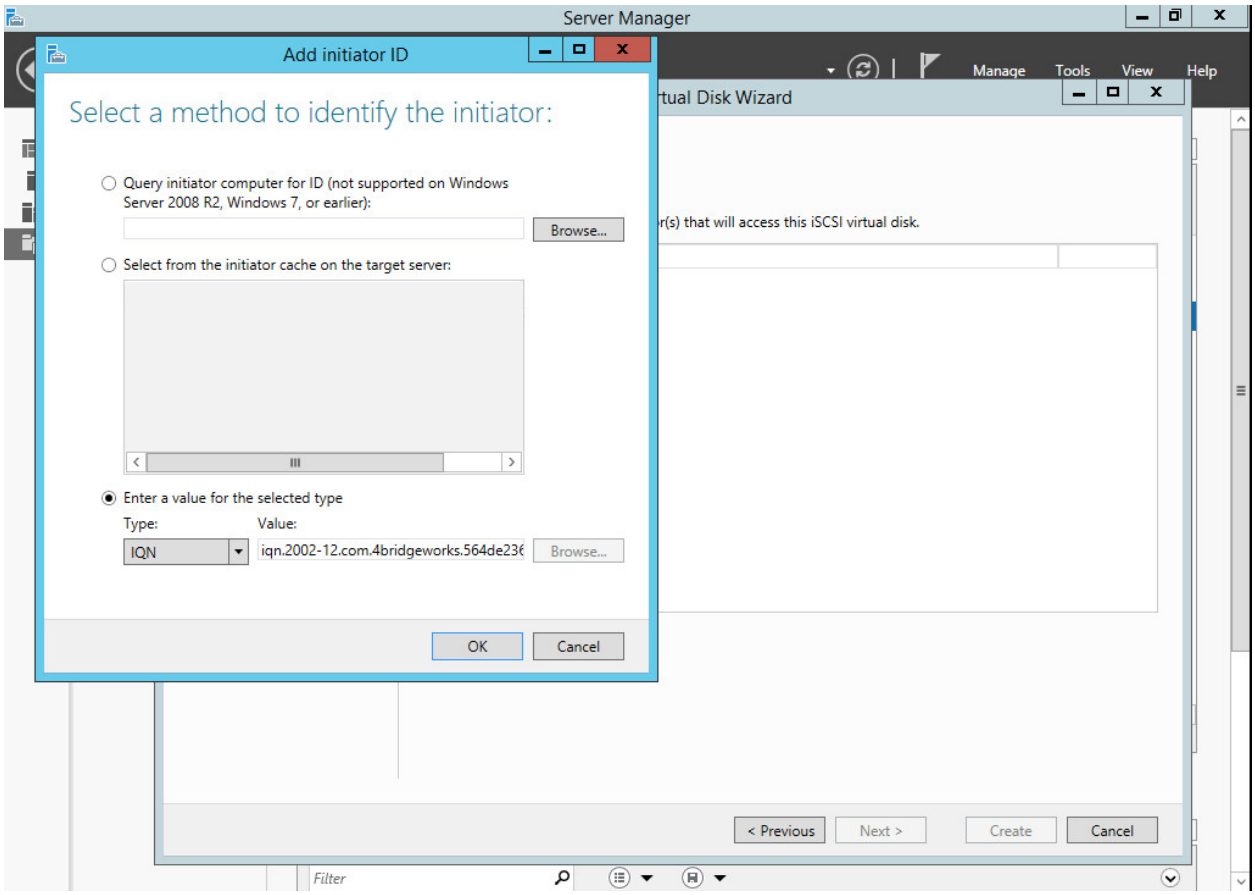


Copy the value in the iSCSI IQN field to the clipboard.



4.3.2 Adding the WANrockIT's IQN to the Access Control list

From your Windows Server 2012 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.



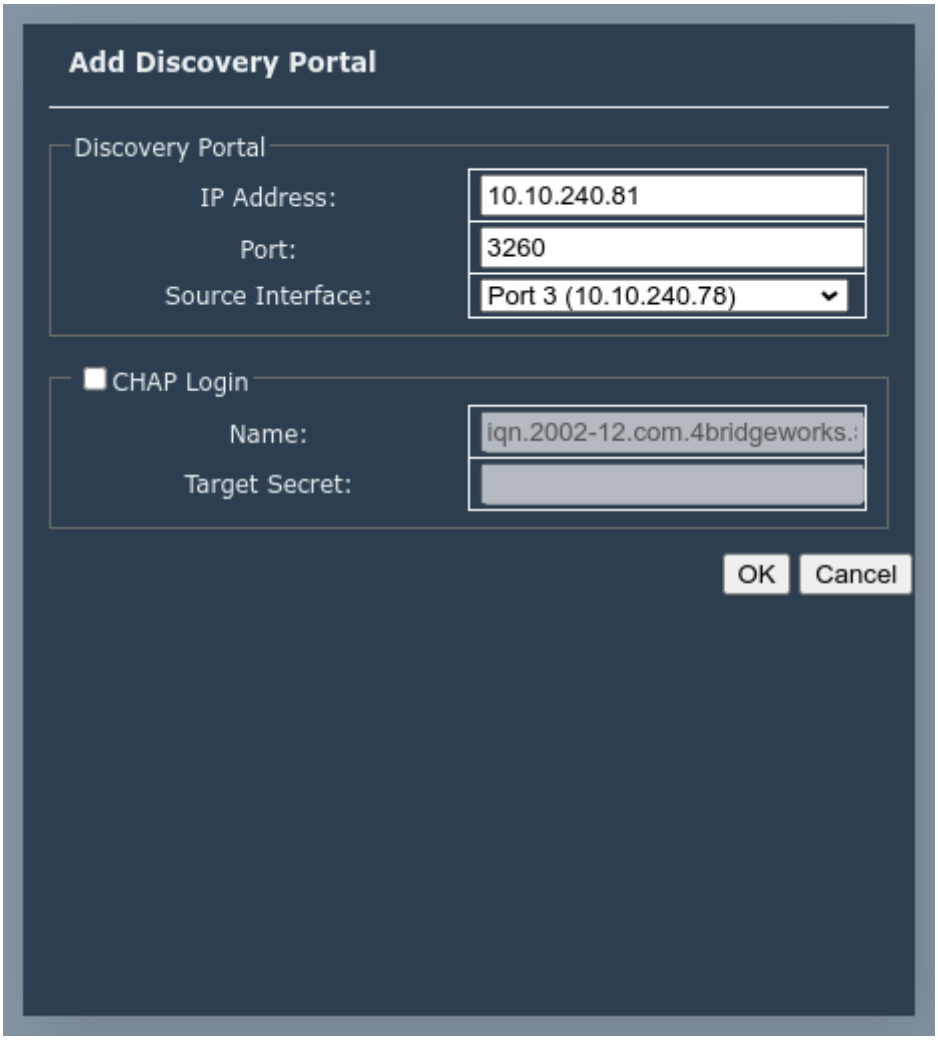
4.4 Logging onto the iSCSI Target

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.

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

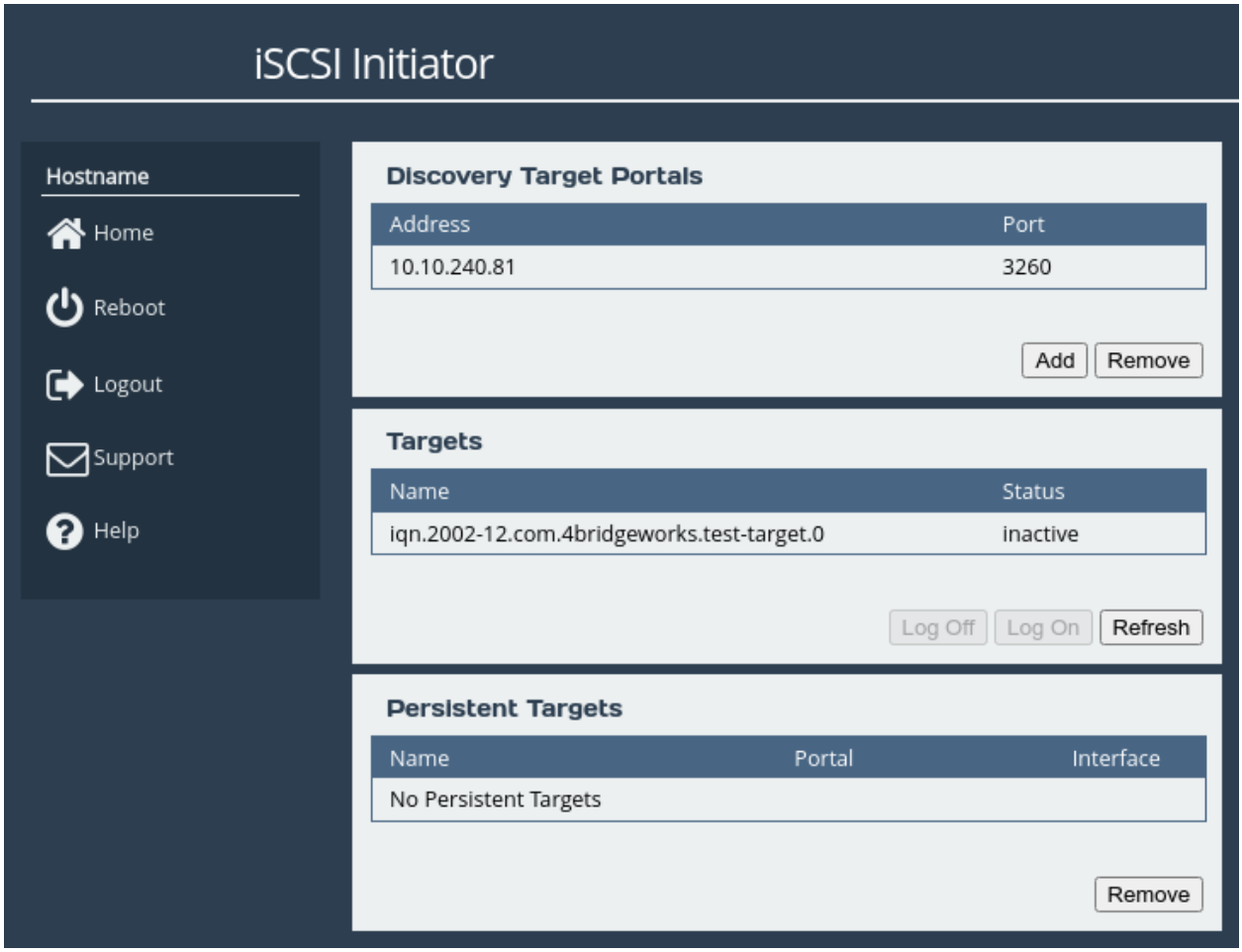
In the subsequent dialog, enter the IP address of the Microsoft iSCSI target portal in the *IP Address* field. The default port number assigned to iSCSI is 3260. If you have configured the Windows iSCSI target to use a different port number, enter this number in the Port field. If iSCSI is mapped to 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.

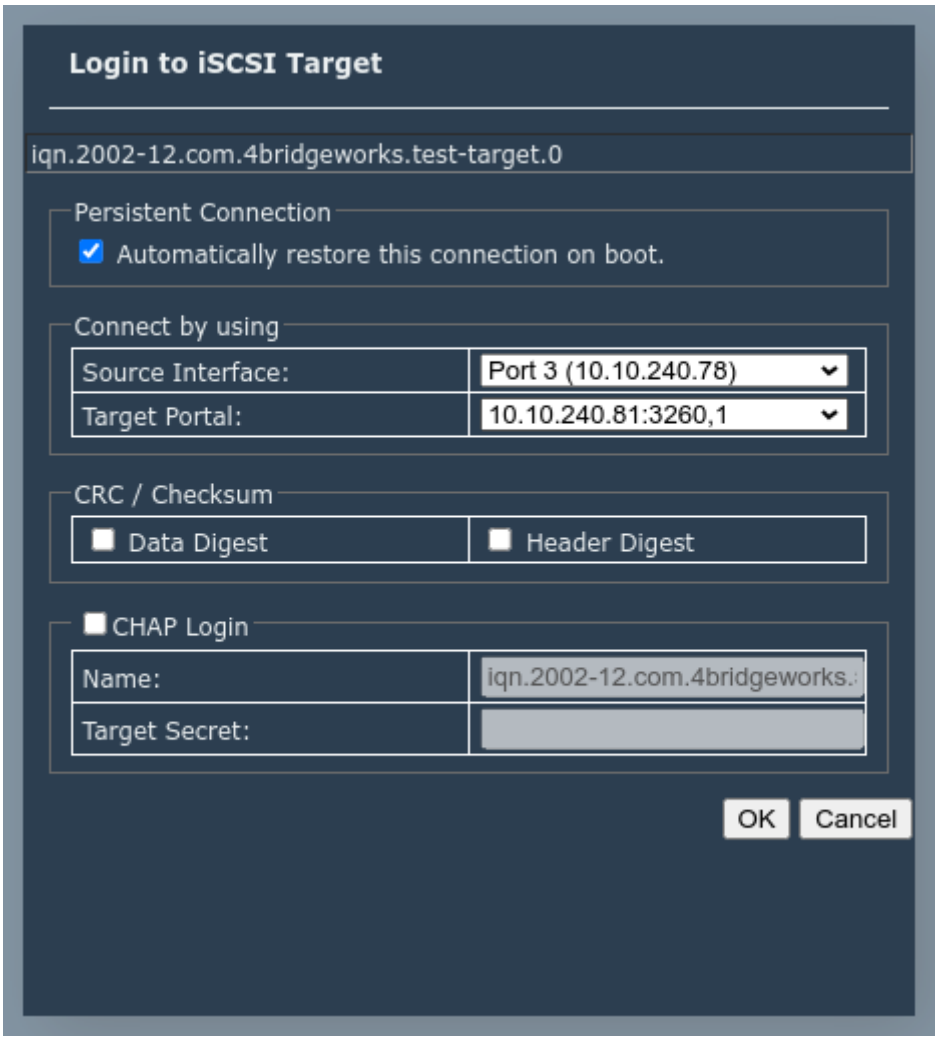


When the discovery is complete, a list of targets presented by the portal is shown in the *Targets* subsection. The example shows a single target with an IQN of `iqn.2002-12.com.4bridgeworks.test-target.0` that is currently inactive (the iSCSI initiator is

not currently logged onto the target).



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.



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.

4.5 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
Hostname
Home
Reboot
Logout
Support
Help
Directly Connected Devices (1)
Disk Drive
MSFT
Virtual HD
Devices registered from other WANrockIT Nodes (0)
No Devices are known about from other WANrockIT Nodes.

5 Configuring IPsec

5.1 Introduction

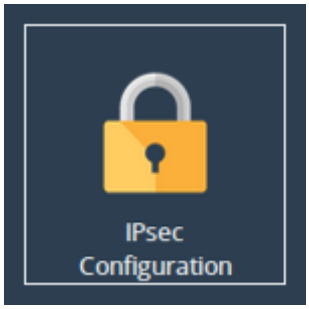
This step will guide you through how to configure IPsec to encrypt traffic between two Bridgeworks Nodes. Using IPsec ensures the integrity, confidentiality and authentication of data communications over an IP network. This step should be done before performing the step Establishing a Link Between Nodes. 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.

5.2 Important Notes

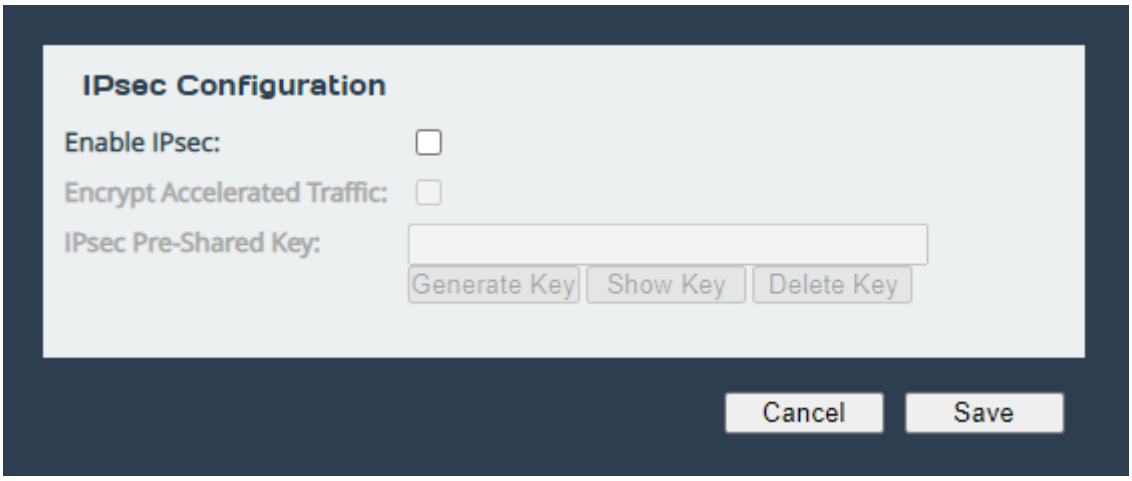
- Nodes with IPsec configured to *Encrypt Accelerated Traffic* will only allow connections from other IPsec-enabled Nodes with the same pre-shared key and settings enabled.
- It is recommended to only enable *Encrypt Accelerated Traffic* when data transfer is stopped as WAN communication will be broken 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.

5.3 Enabling IPsec

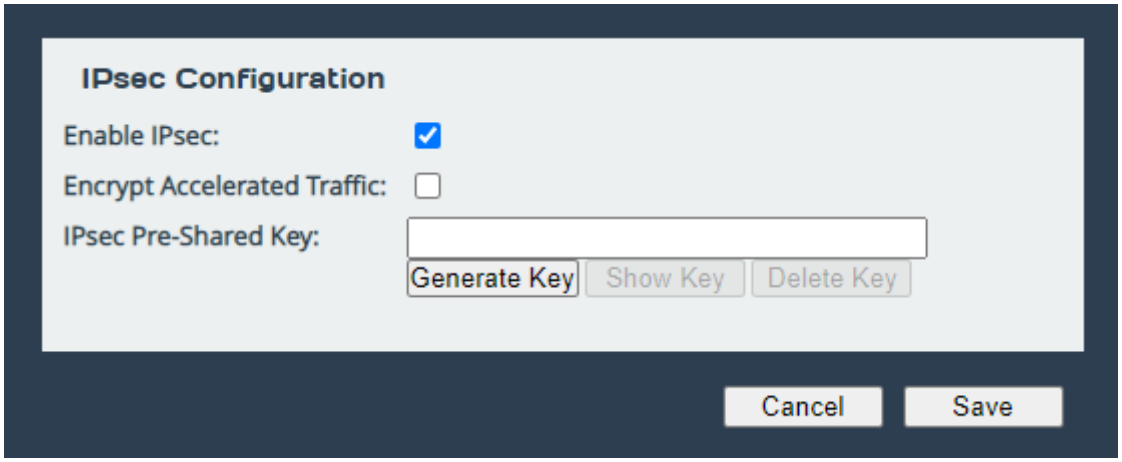
From the Node's web interface, navigate to the *Node Management* page, then to the *IPsec Configuration* page by clicking the corresponding icon in the top menu.



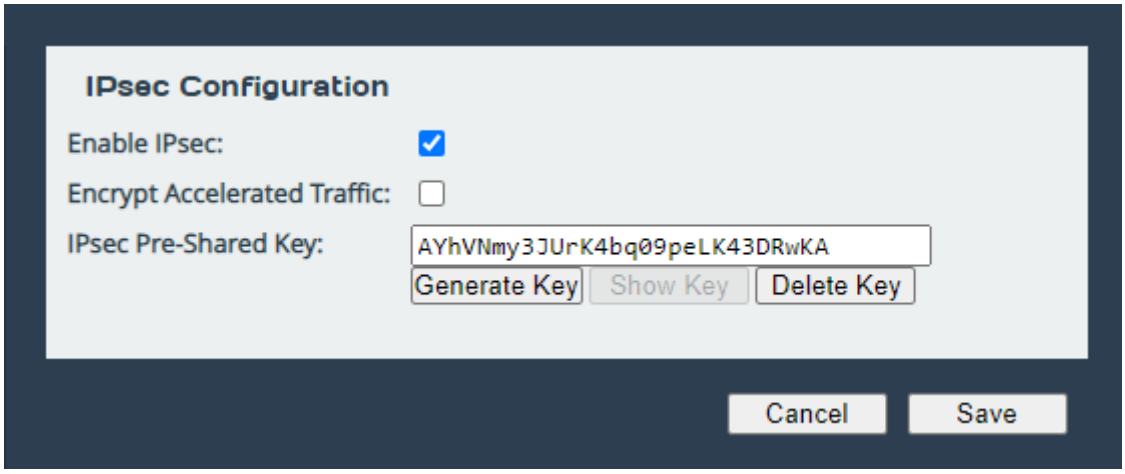
The IPsec service is disabled by default, so the Node's IPsec Configuration options will be disabled until the *Enable IPsec* checkbox is selected.



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



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:



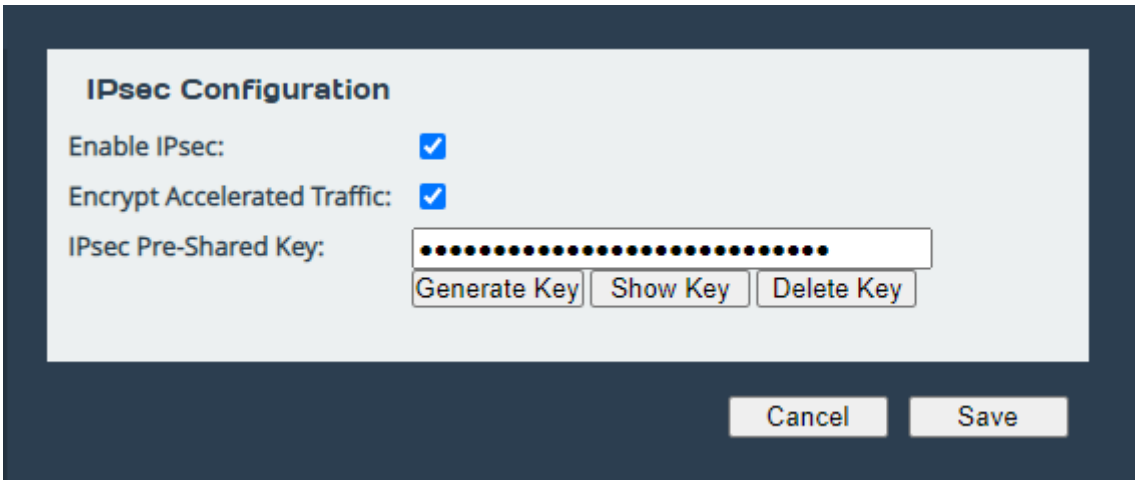
If the *Encrypt Accelerated Traffic* option is desired then tick the corresponding checkbox. This option will encrypt all WAN links between the two Nodes affecting all accelerated data being passed through them.

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.

5.4 Copying the Pre-Shared Key to other Bridgeworks Nodes

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



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.

6 Establishing a Link Between Nodes

6.1 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.

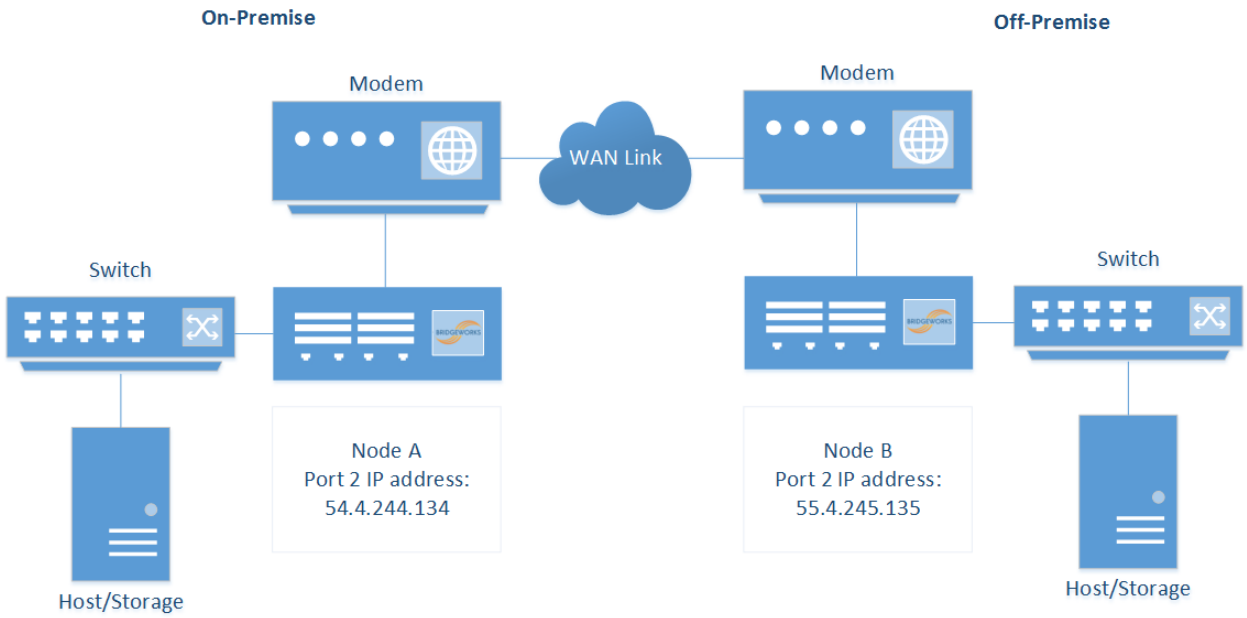
6.2 Firewall

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

6.3 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.

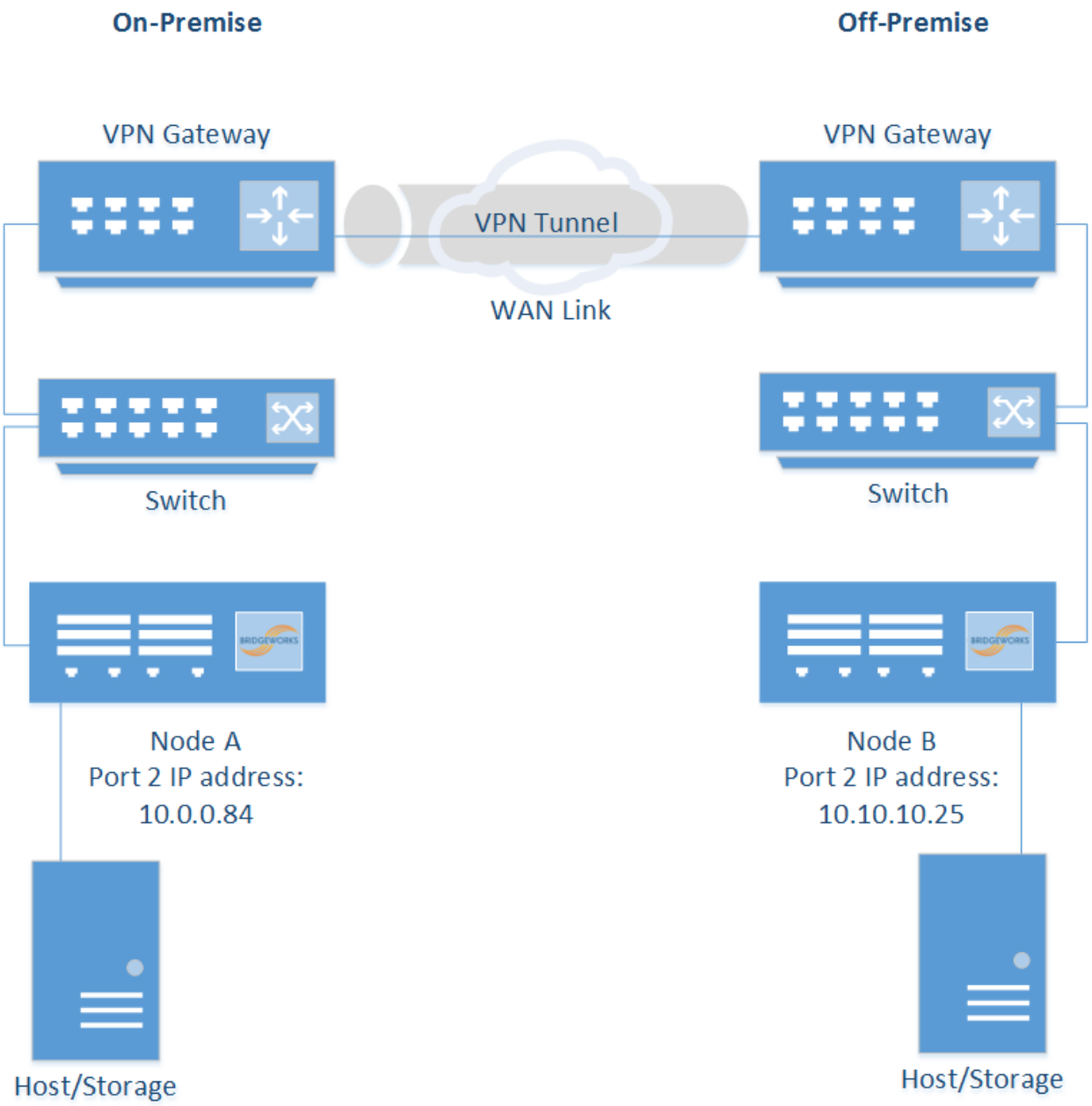


In this example the IP addresses for establishing a Nodal link are the public IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 54.4.244.134
- Node B: 55.4.245.135

6.4 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

6.5 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.

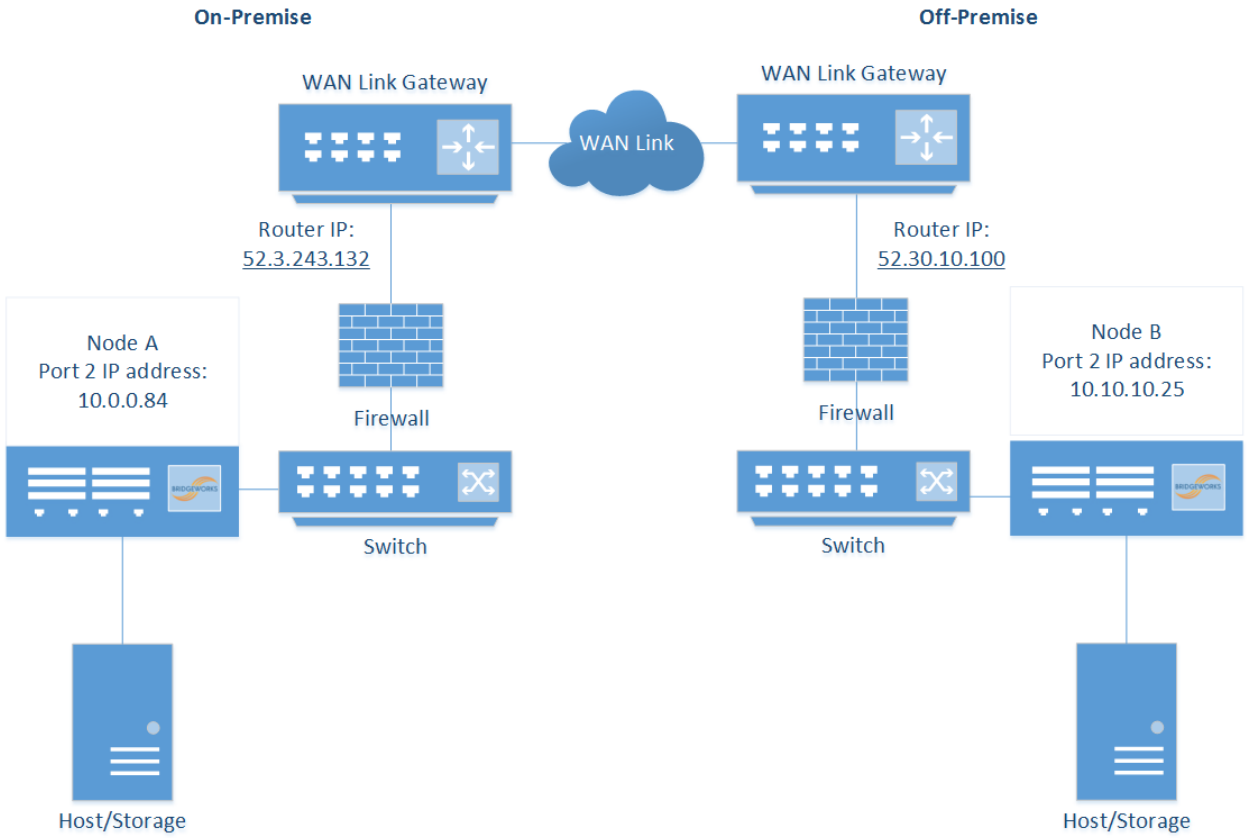
The firewall must be configured with the following sets of NAT port forwarding rules:

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.

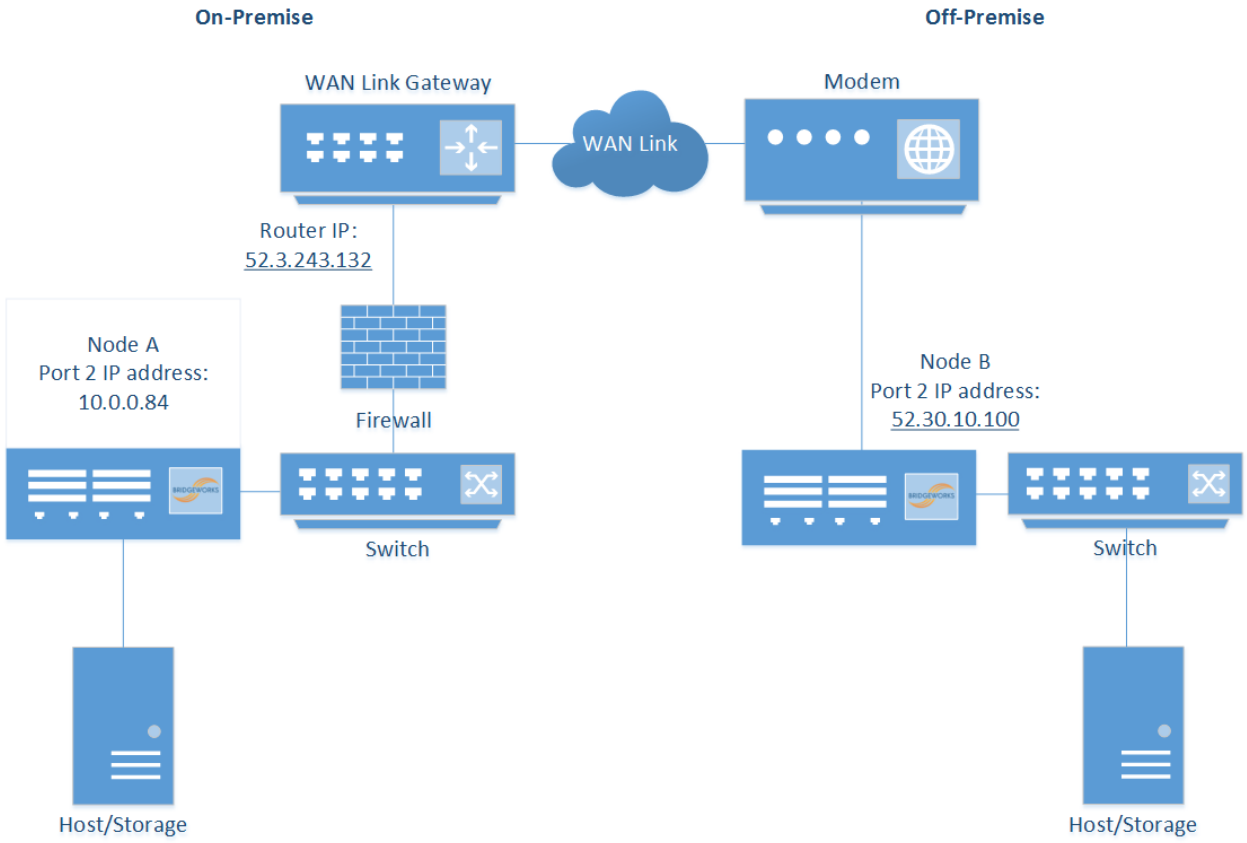


In this example the IP addresses for establishing a Nodal link are the IP addresses of the router, in this case:

- Node A: 52.3.243.132
- Node B: 52.30.10.100

6.6 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

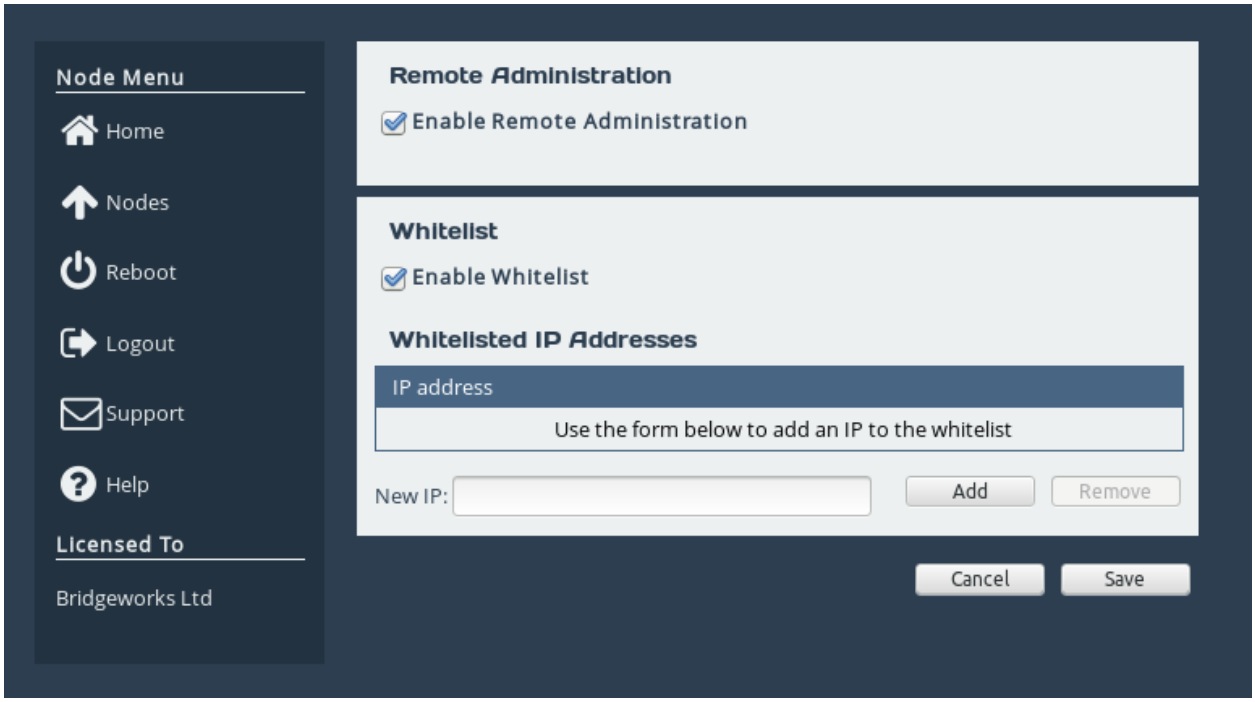
For a successful connection in this example without setting any firewall policies, Node A must first connect to Node B.

6.7 Access Control

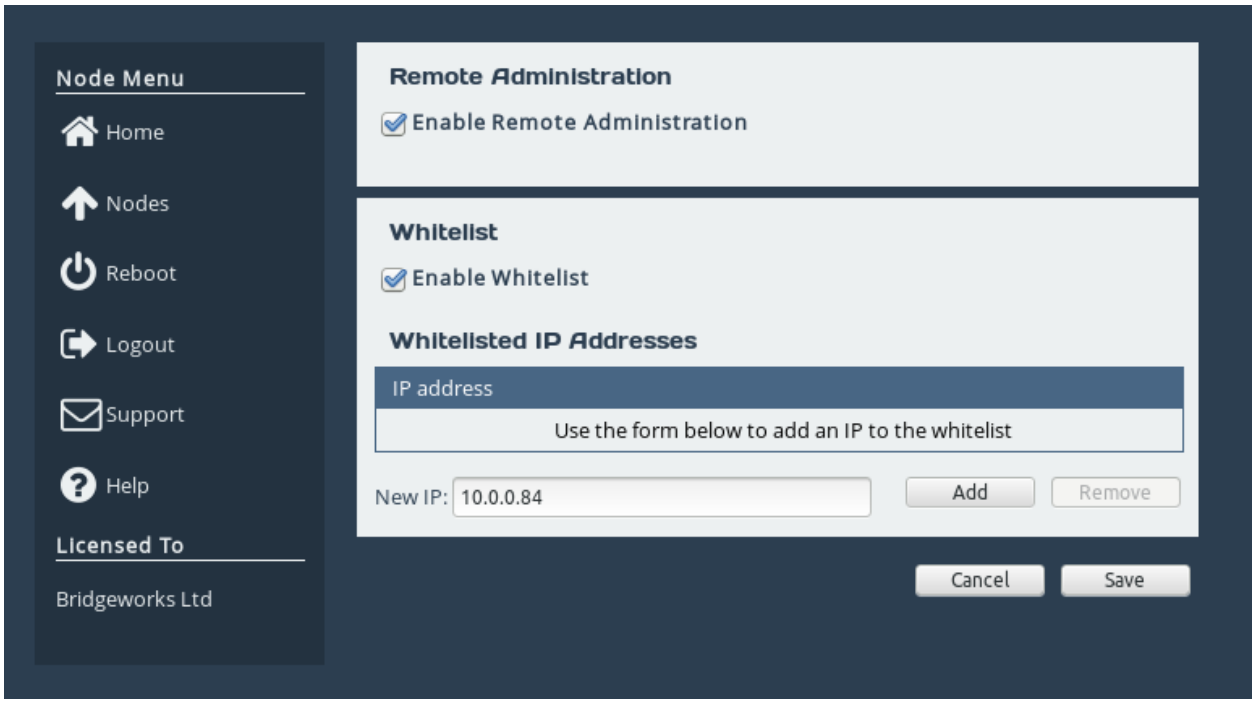
Throughout the following sections which refer to *Node A* and *Node B*, use the IP address types found in the previous examples.

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

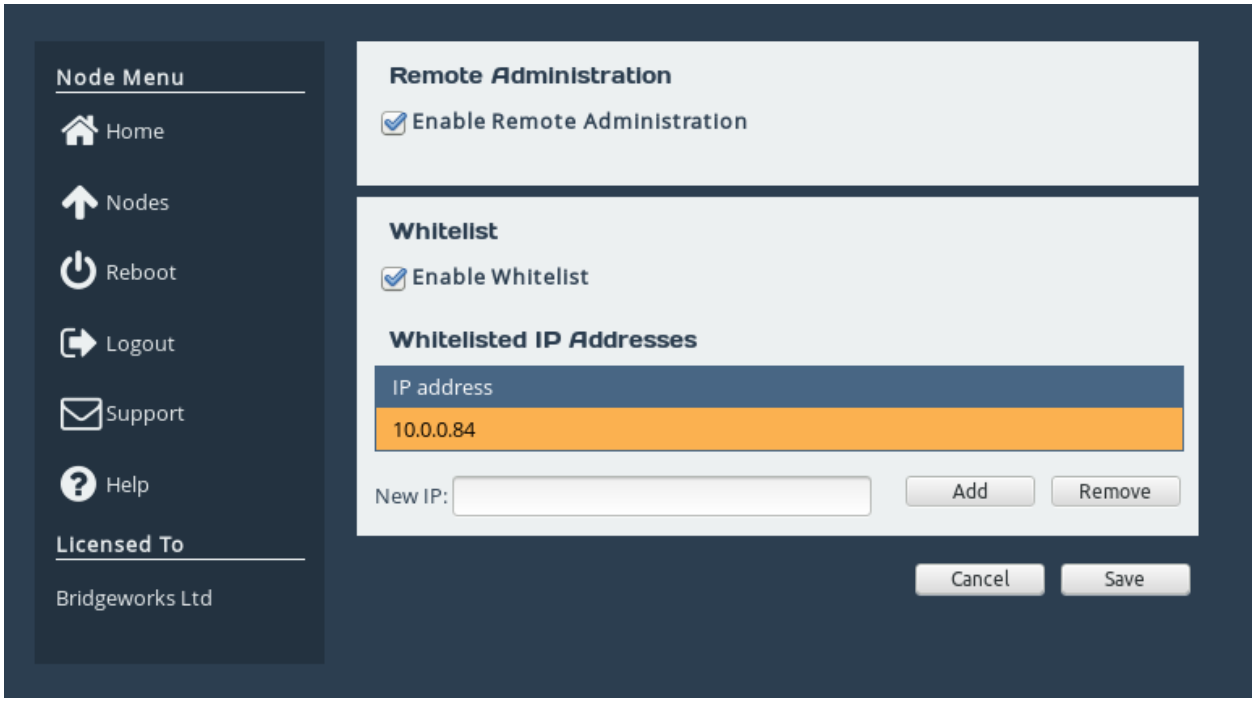
Ensure that under the heading *Whitelist* the *Enable Whitelist* checkbox is ticked. By default this should be the case.



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



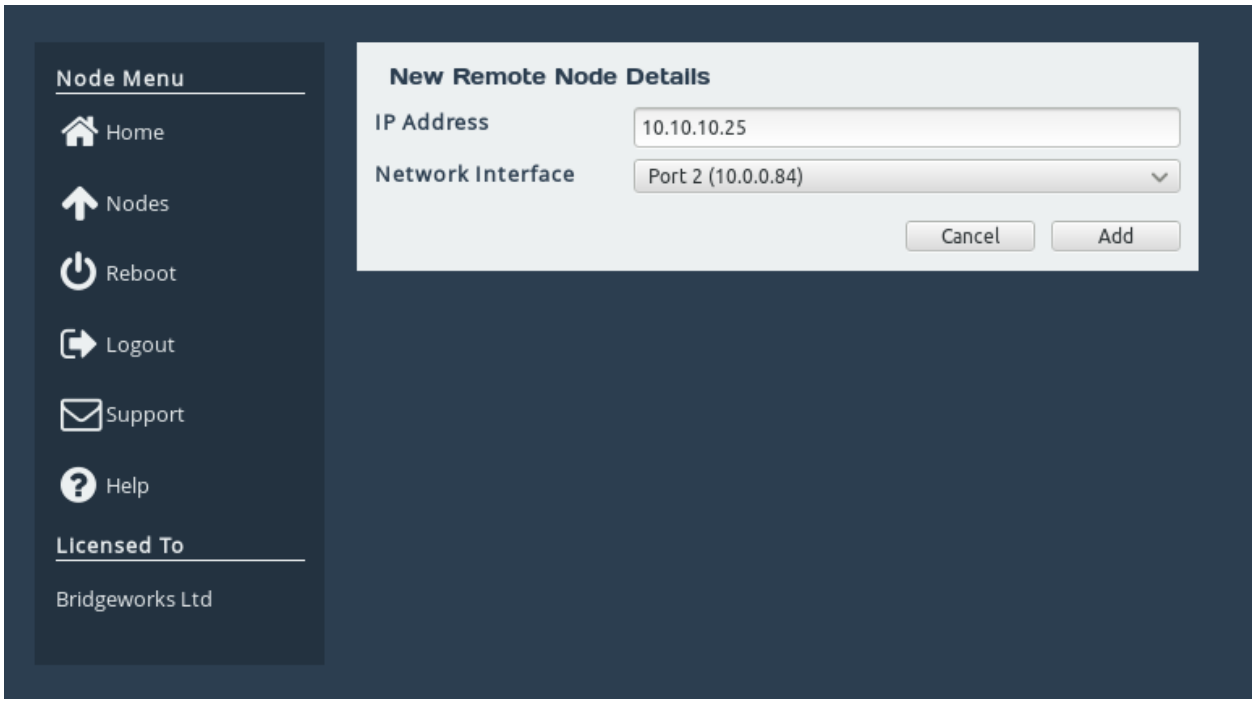
When this has been added successfully you will see the IP address entry added to the list, as shown below.



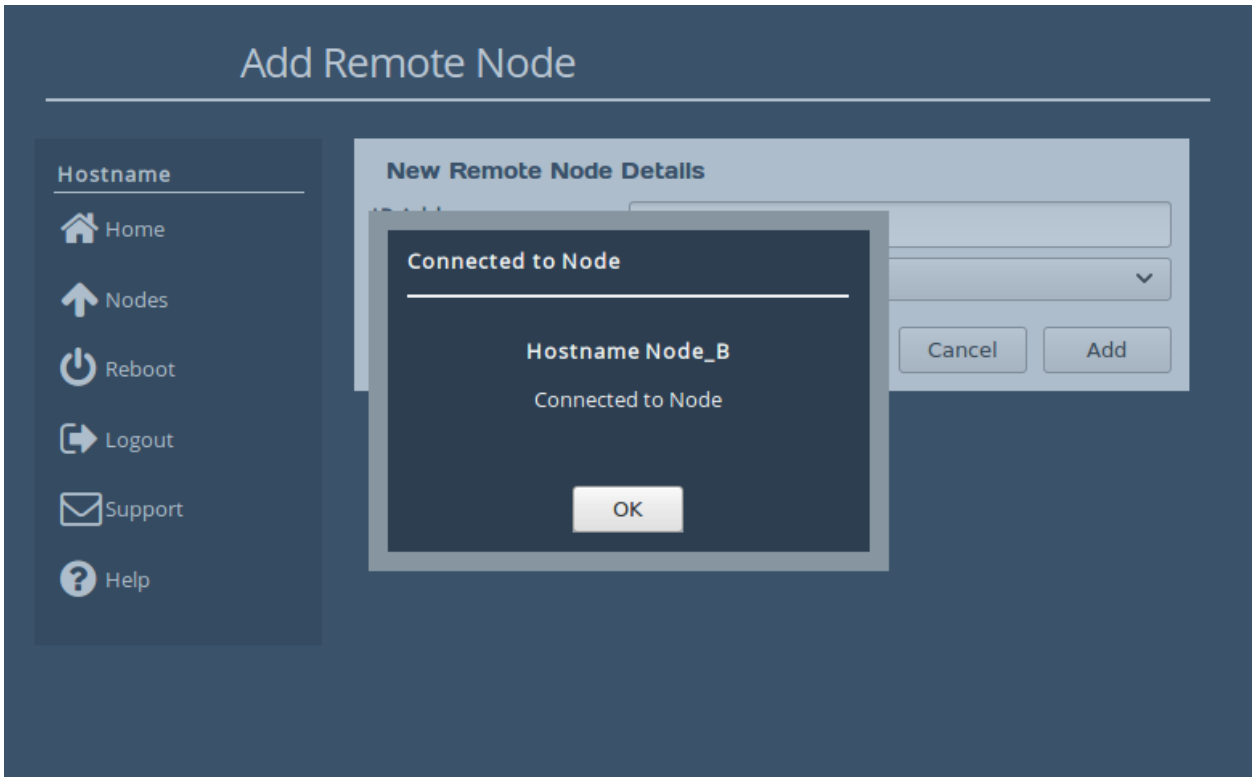
	Important: If Node B is not behind a NAT, repeat this process on Node A to add the IP address of Node B to the whitelist of Node A.

6.8 Node Management

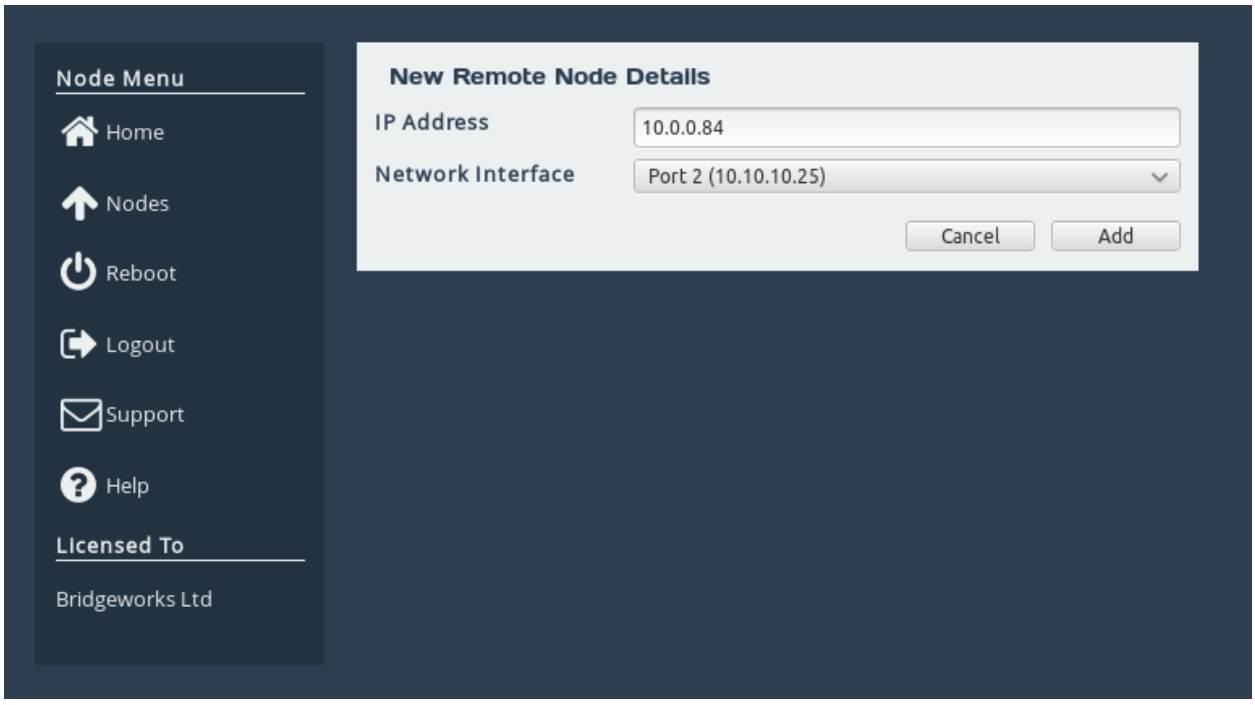
The next stage is to perform the Node Discovery on the WAN link. From the *Node Management* page of Node A, click the *Add Remote Node* icon to navigate to the *Add Remote Node* page. Enter the IP address of Node B's WAN port in the address field. The *Network Interface* drop-down allows you to change 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.



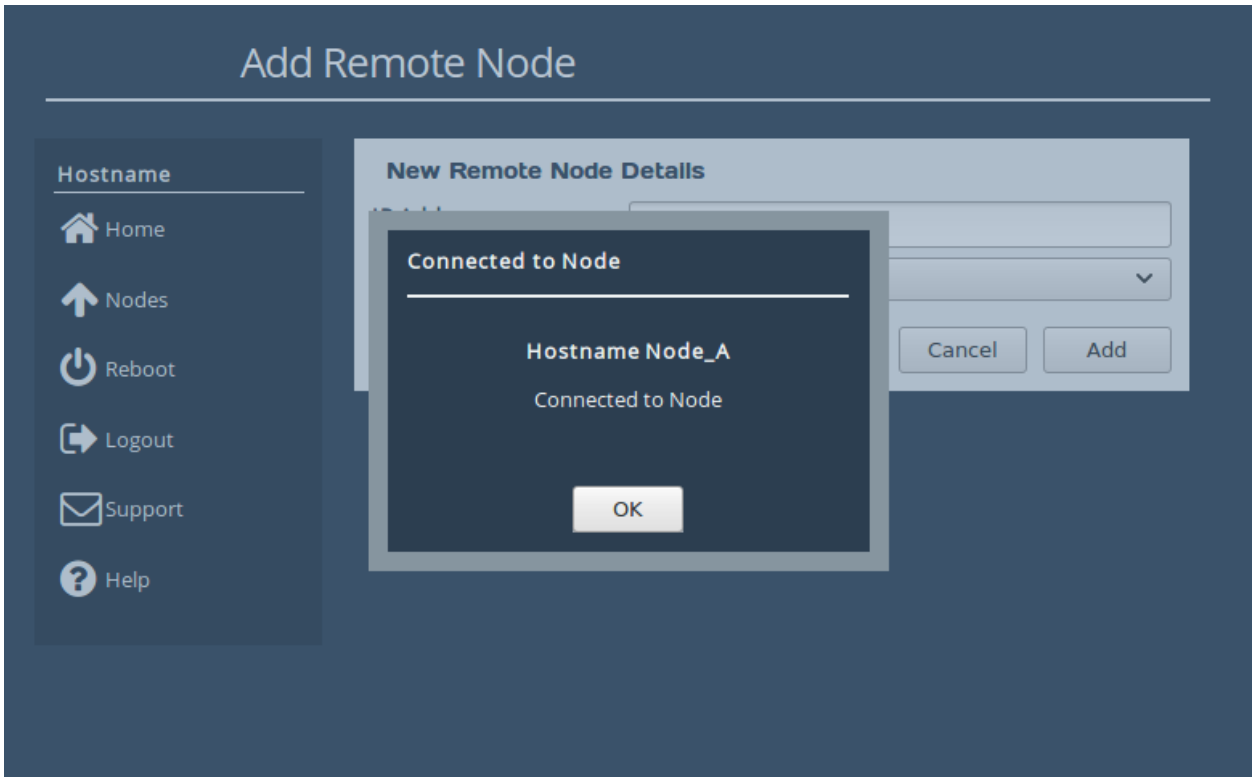
When the connection has been established, a dialog will show the hostname of the remote Node.



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.



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



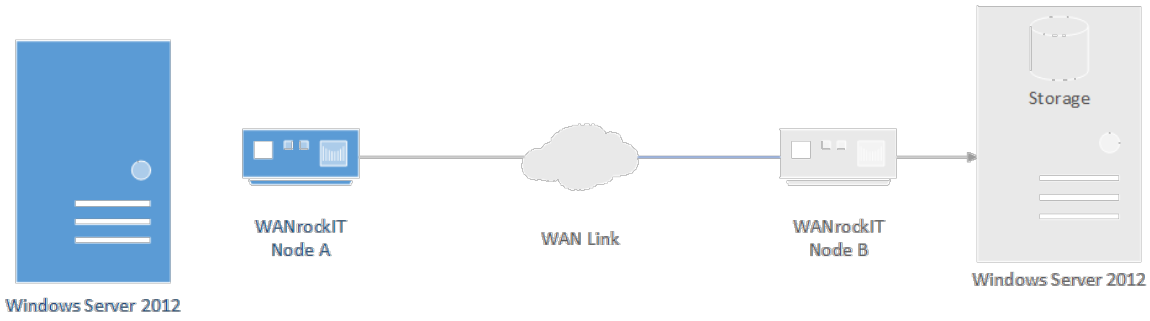
Congratulations, you have successfully set up a connection between your Nodes.

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

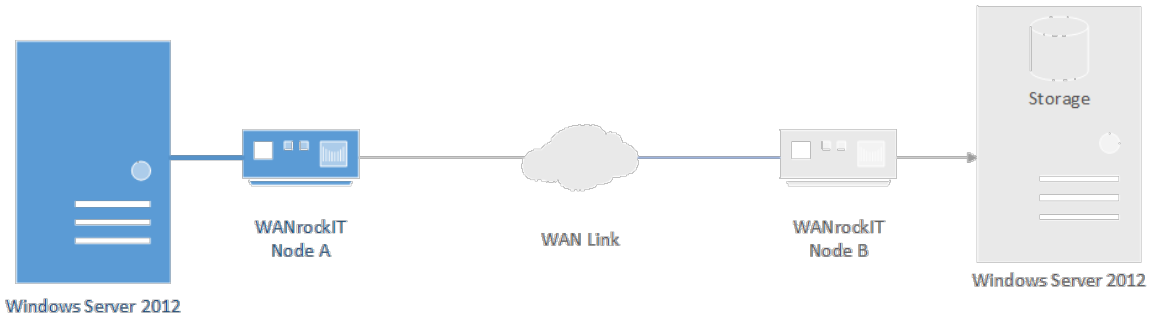
7.1 Introduction

This section describes how to log on to the iSCSI Target Portal from your On-Premise Node using a Windows Server 2012 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 2012 machine and a WANrockIT Node.

The following diagram illustrates the described topology.



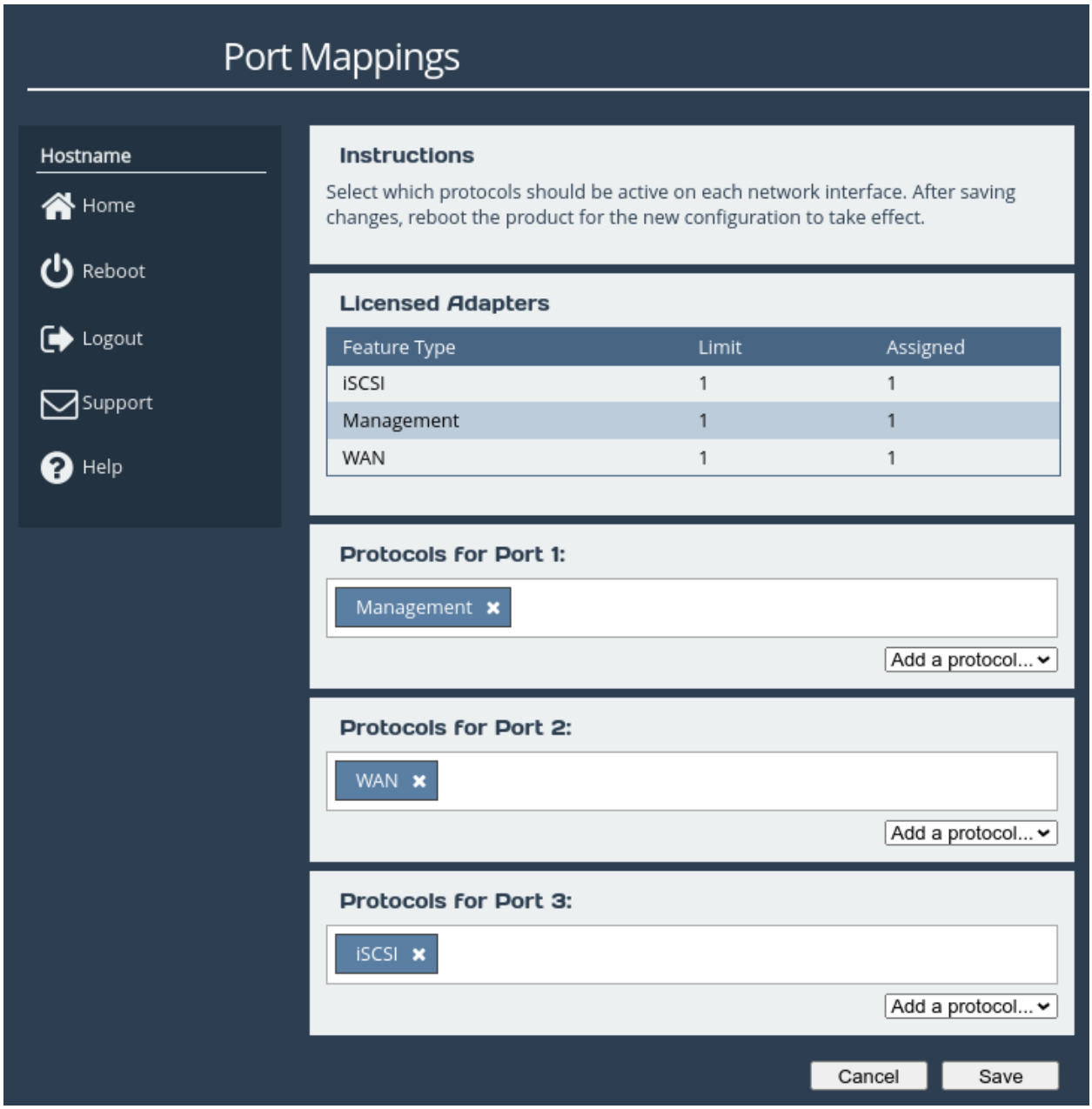
Once you have completed the following instructions your topology will have changed to the following.



7.2 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.

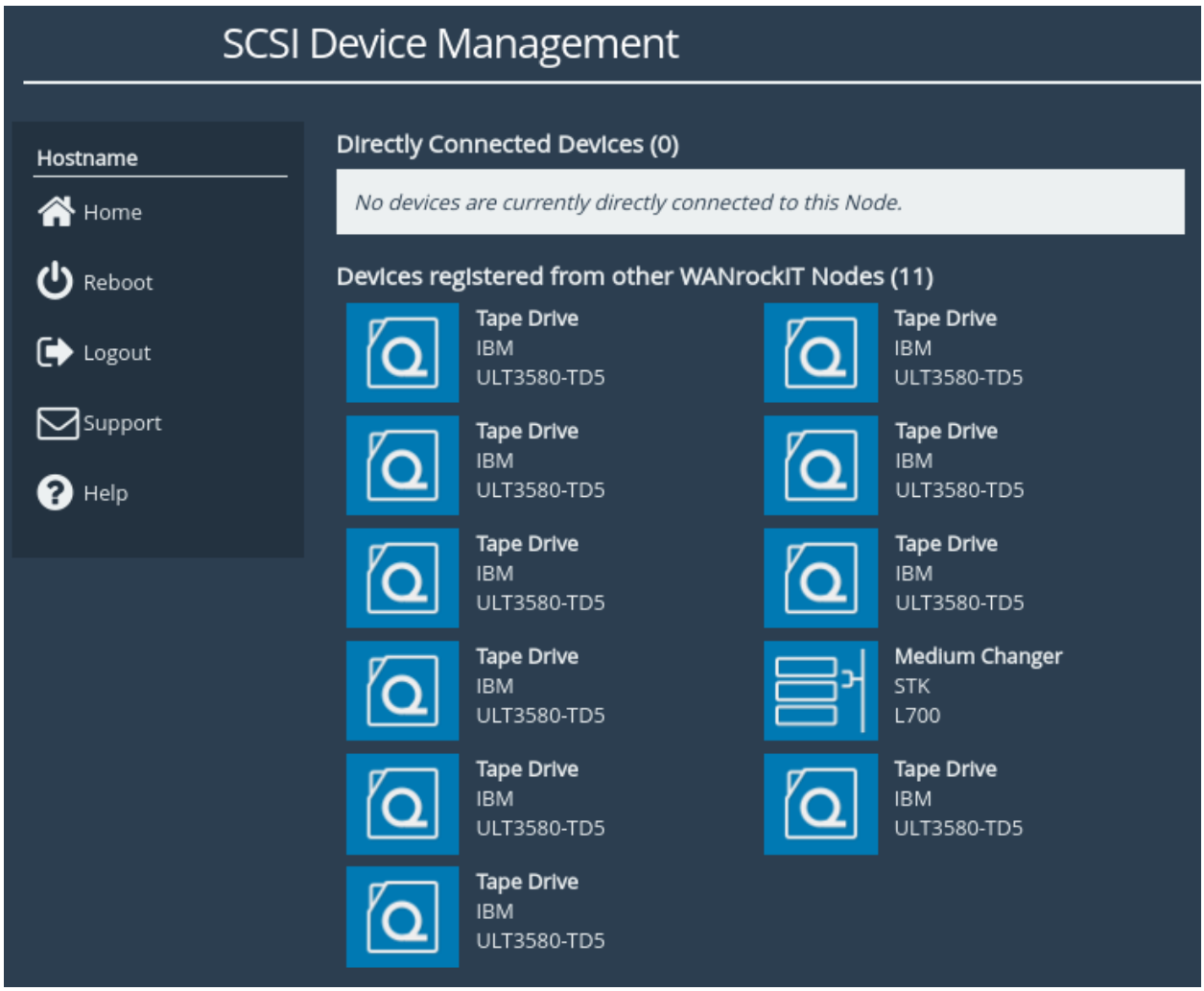


7.3 Confirming the Presence of iSCSI targets

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*

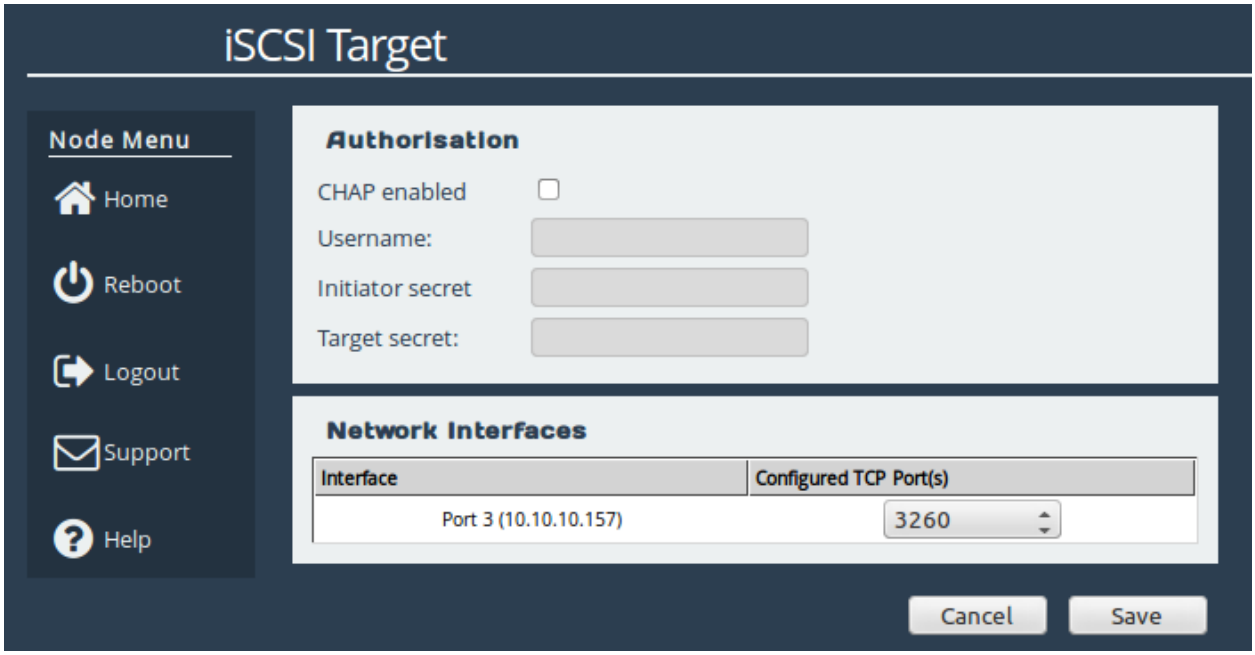
Management by clicking the corresponding icon as shown below.

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*.



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.



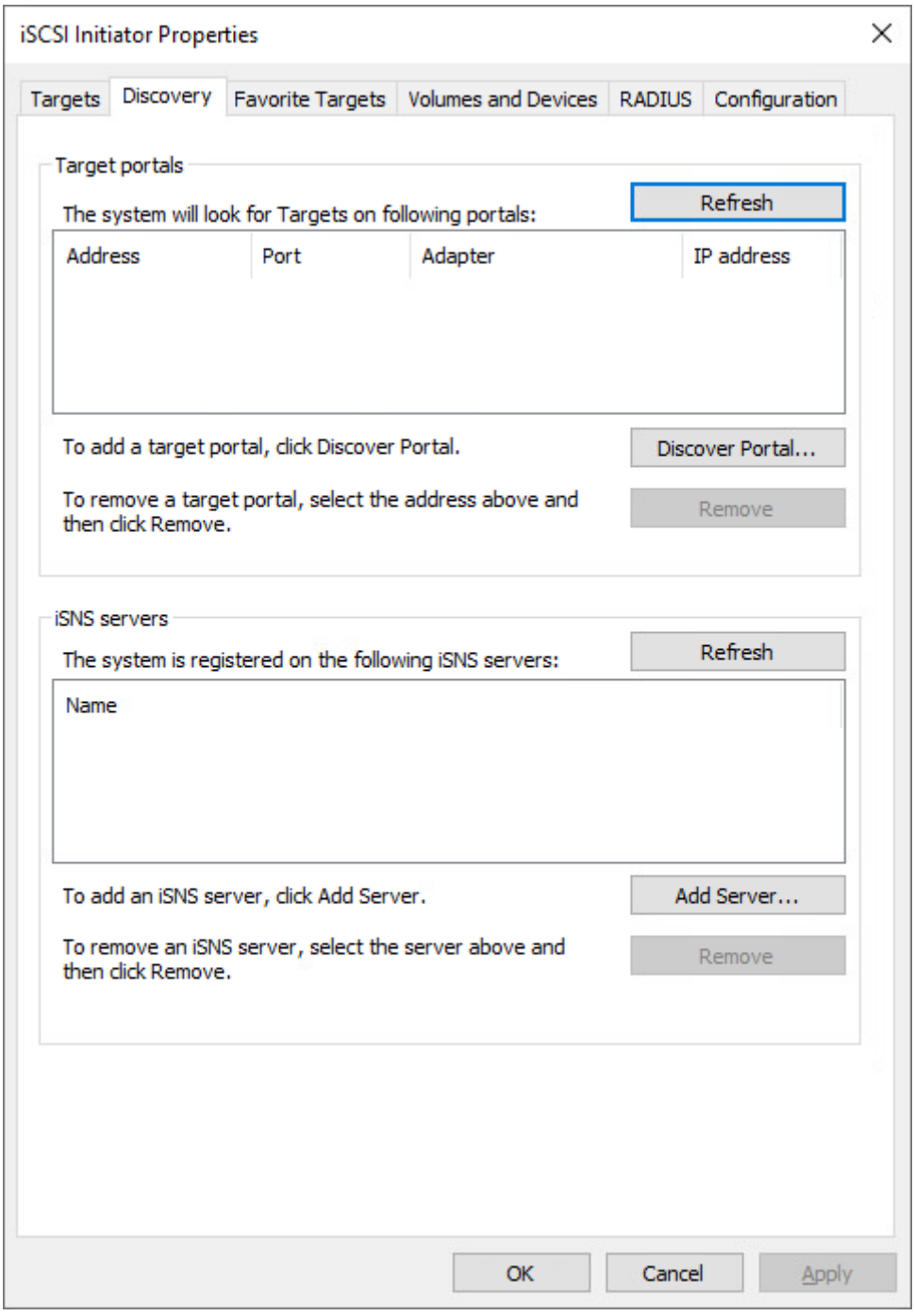
If you wish to enable one-way or mutual CHAP authentication, this can be done under the *Authorisation* subsection. Click the *CHAP enabled* check box and enter in your required details.

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.

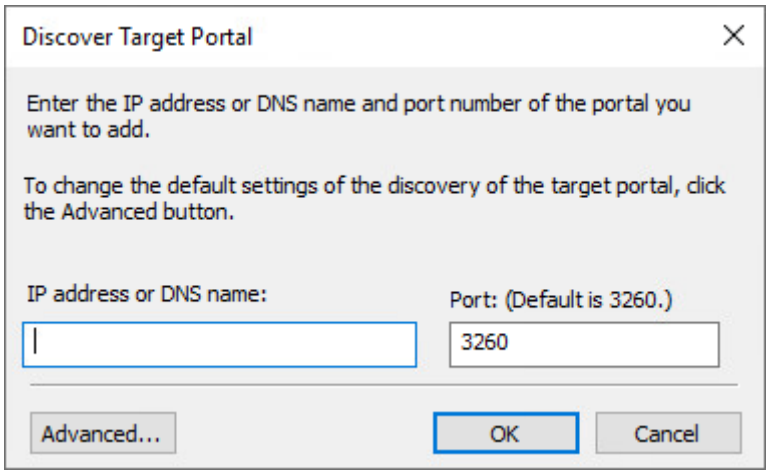
You are now ready to perform an iSCSI discovery, and subsequently log on to remote devices.

7.4 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.



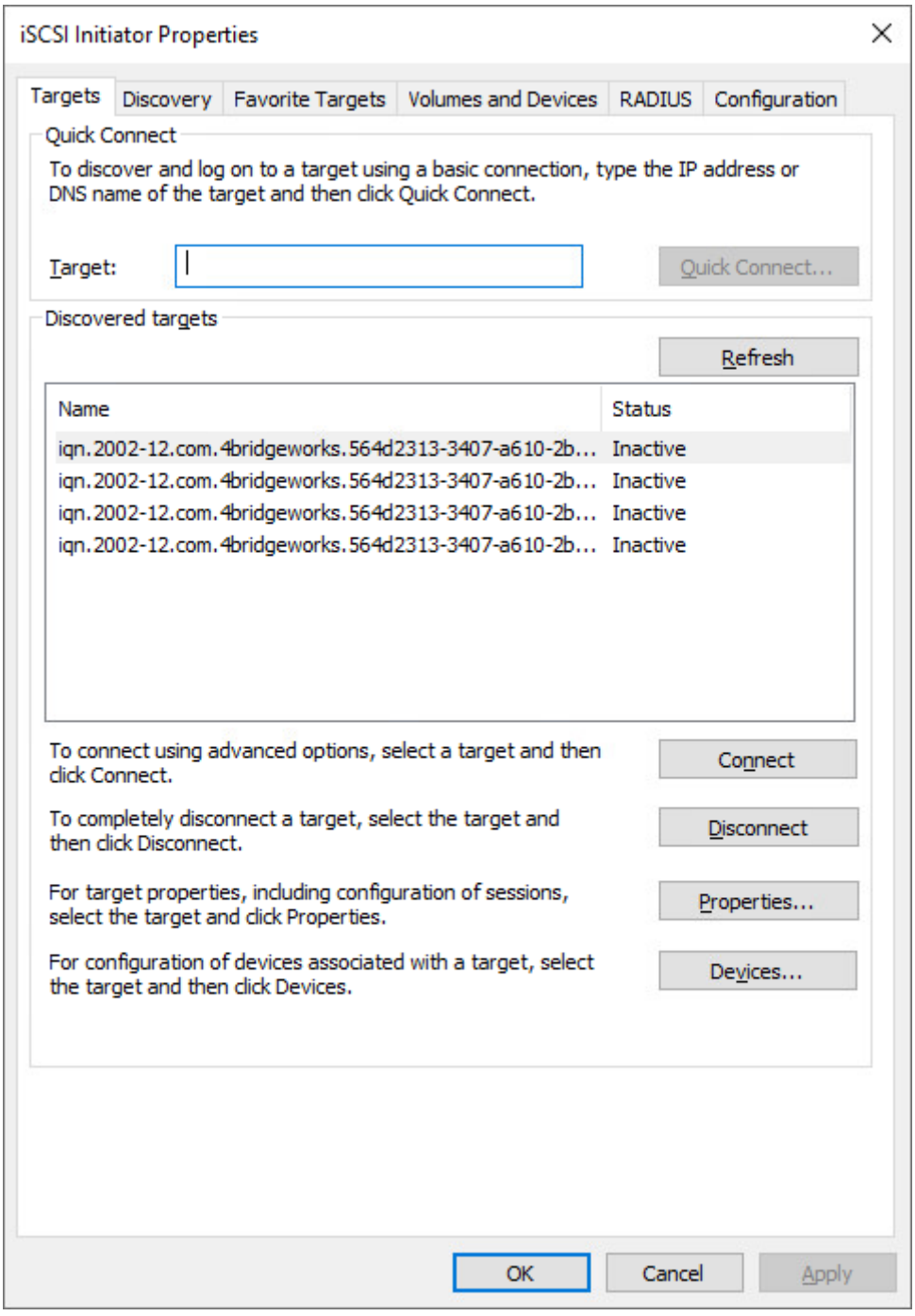
To add an iSCSI Target portal, click on *Discover Portal*. You will be presented with a second window.



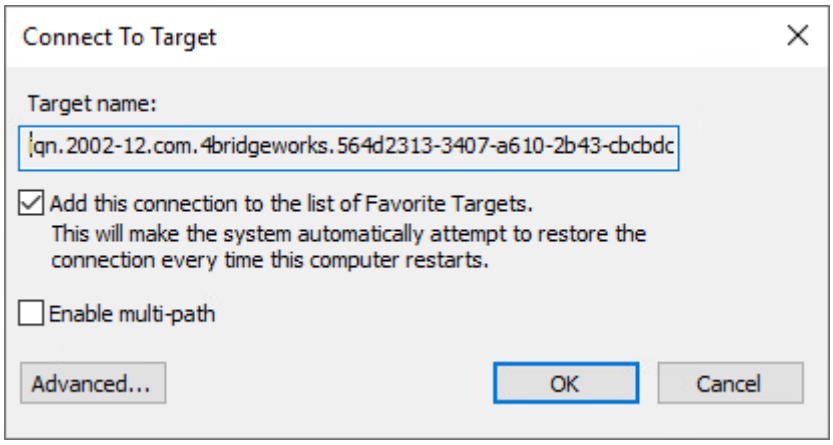
Enter the IP address noted down previously from the *iSCSI Target* page from the WANrockIT web interface. Ensure the port matches your iSCSI configuration, either the default of 3260, or 860.

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

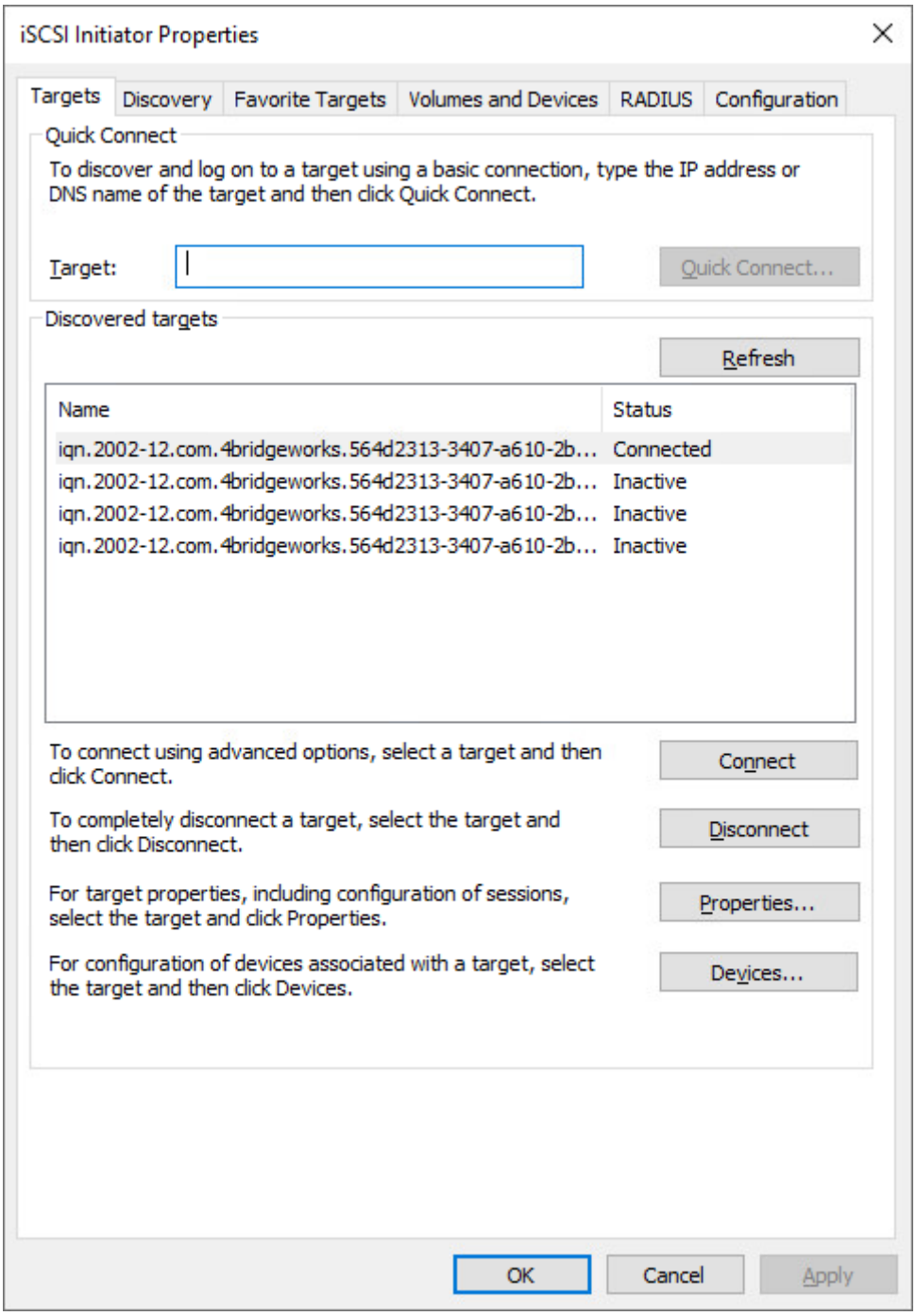
Click on the *Targets* tab. The devices discovered should now be listed and shown as below.



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.



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


iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
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.
Target:
Quick Connect...
Discovered targets
Refresh
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.
Connect
To completely disconnect a target, select the target and then click Disconnect.
Disconnect
For target properties, including configuration of sessions, select the target and click Properties.
Properties...
For configuration of devices associated with a target, select the target and then click Devices.
Devices...
OK
Cancel
Apply

8 Refreshing iSCSI targets through your WAN link

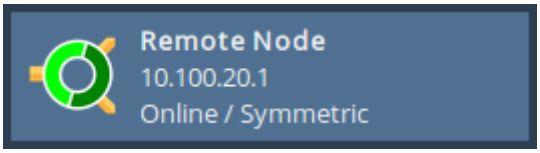
8.1 Introduction

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.

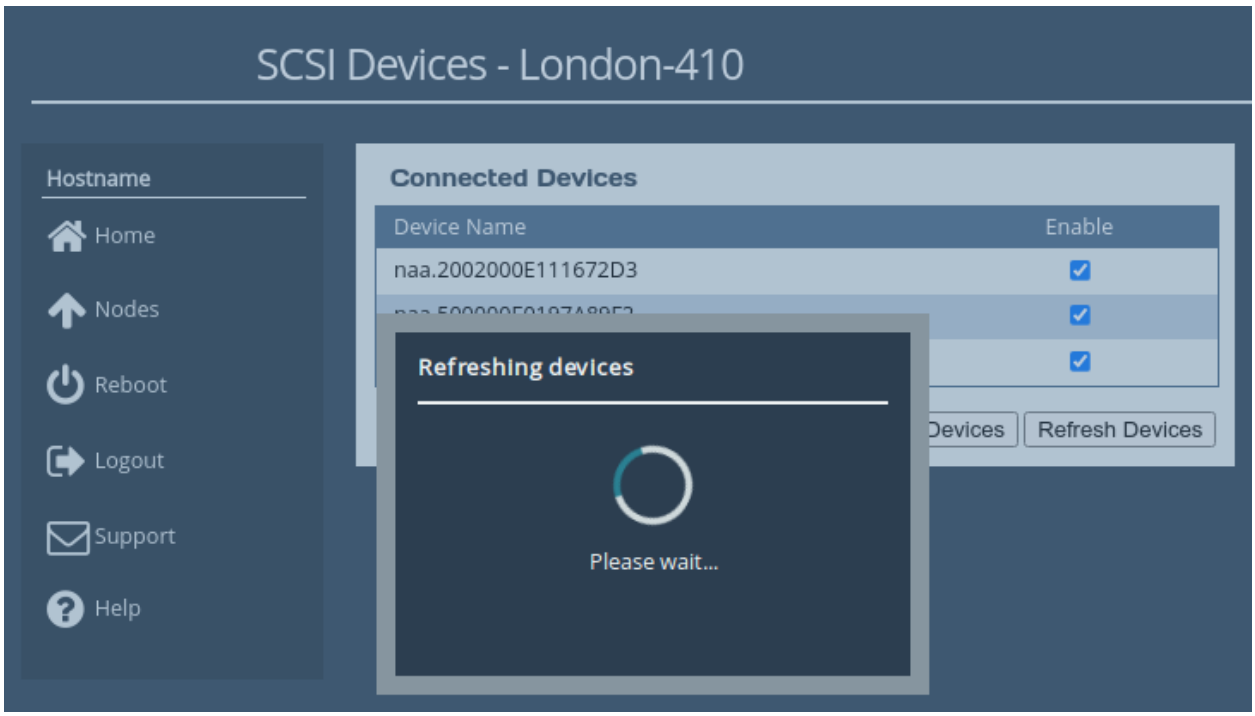
8.2 Refreshing Your Devices

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



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

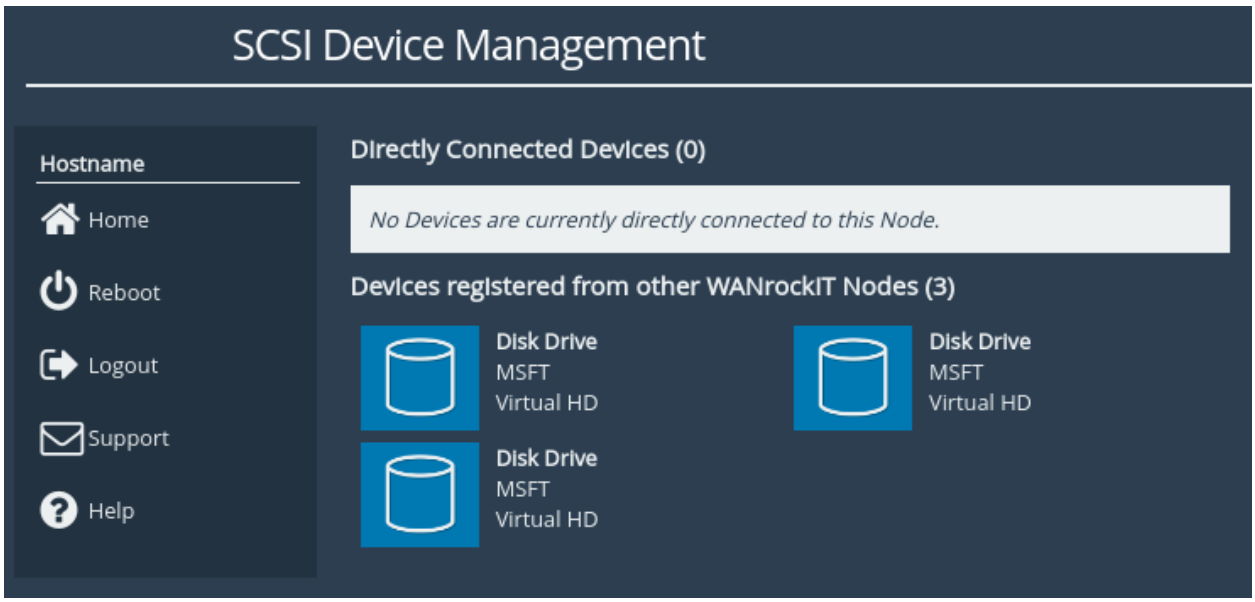
A list of currently visible devices will be presented in the *Connected Devices* table. To refresh your Node for new devices click the *Refresh Devices* button.



Upon completion a summary of the results is shown.

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.



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.

9 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.

10 Useful Links

The following section contains links to other guides and FAQs. Support is available through our website: https://support.4bridgeworks.com/

The following resources are available online:

- User Manuals
- Installation Guides
- General FAQ
- AWS FAQ

If your question is not answered in our documentation, please submit a ticket through our website.