Oresund EFC
iSCSI to FC Gateway
Software Manual

This manual covers the following products:

EFC102200
EFC402200
EFC1002800

Eli-v6.00.62

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

Table of Contents

1 Introduction **6**

1.1 Overview . . . 6

1.2 Manual Layout . . . 7

1.3 Definitions . . . 7

1.3.1 iSCSI Target Device . . . 7

1.3.2 iSCSI Qualified Name (IQN) . . . 7

1.3.3 iSCSI Challenge Handshake Authentication Protocol (CHAP) . . . 7

2 Using the Web Interface **8**

2.1 Browsers . . . 8

2.2 Connecting to the Web Interface . . . 8

2.3 Management Console (Home screen) . . . 11

3 Bridge Configuration **12**

3.1 Network Connections . . . 12

3.1.1 Network Interfaces . . . 13

3.1.2 General Settings . . . 13

3.1.2.1 Hostname . . . 13

3.1.2.2 DNS Servers . . . 14

3.1.2.3 Default Route . . . 14

3.1.2.4 Dead Gateway Detection . . . 14

3.1.2.5 Enable IPv6 . . . 15

3.1.3 Interface Statistics . . . 15

3.1.3.1 Data Transmission Rate . . . 16

3.1.3.2 Data Reception Rate . . . 17

3.1.3.3 Legend . . . 17

3.1.4 Network Routing . . . 17

3.1.4.1 Add Static Route . . . 17

3.1.5 Network Tools 18
3.1.5.1 Ping 19
3.1.5.2 Traceroute 20
3.1.6 Port Settings 21
3.1.6.1 Enable Port 21
3.1.6.2 Setting the MTU 21
3.1.6.3 Setting the IP Address 22
3.1.6.4 Committing the Changes 22
3.2 Passwords & Security 22
3.2.1 System Password 23
3.2.2 Password Reset Options 24
3.2.2.1 Password Reset via Email 24
3.2.2.1.1 Setup 24
3.2.2.1.2 Using Password Reset via Email 24
3.2.2.2 Password Reset via Local Console or SSH 26
3.2.2.2.1 Setup 26
3.2.2.2.2 Using Password Reset via Local Console or SSH 27
3.2.3 Secure Connection 28
3.2.4 Secure Shell (SSH) 29
3.2.4.1 Managing Public Keys 29
3.2.4.2 Using SSH 29
3.3 Service Control 30
3.3.1 Simple Network Time Protocol 31
3.3.2 SNMP Agent 31
3.3.2.1 System Information 32
3.3.2.2 SNMP Trap Sinks 32
3.3.2.3 Download MIB Files 32
3.3.3 Simple Mail Transfer Protocol (SMTP) 33
3.3.4 Event Notification Email 33
3.3.5 Internet Storage Name Service (iSNS) 34

4 Fibre Channel Initiator Connections 35

5 iSCSI Target Configuration 38

5.1 Authorisation (CHAP) . . . 38

5.2 Network Interfaces . . . 39

5.3 iSCSI Sessions . . . 39

6 SCSI Device Management 41

6.1 Viewing Attached Devices . . . 41

6.2 Viewing Device Mappings . . . 42

7 Bridge Maintenance 44

7.1 System Information . . . 44

7.2 System Log . . . 45

7.3 Load/Save Configuration . . . 46

7.3.1 Loading a Saved Configuration . . . 47

7.3.2 Saving the Configuration to Disk . . . 47

7.3.3 Restoring to Factory Defaults . . . 48

7.4 Firmware Updates . . . 48

7.4.1 Automatic Firmware Update Checking . . . 49

7.4.2 Updating Firmware Manually . . . 50

7.5 Licence Key Management . . . 51

7.5.1 Uploading a Licence Key . . . 53

7.5.2 Removing a Licence Key . . . 53

7.5.3 Downloading a Licence Key . . . 53

7.6 Diagnostics . . . 54

7.7 Task Scheduler . . . 54

7.7.1 Adding Tasks . . . 55

7.7.2 Removing/Editing Tasks . . . 55

7.7.3 Task Wizard . . . 57

7.7.3.1 Action - Email Performance Statistics . . . 57

7.7.3.2 Trigger . . . 58
7.7.3.3 Start Date . . . 59
7.7.3.4 End Date . . . 60
7.7.3.5 Summary . . . 60

8 Troubleshooting 62
8.1 Network Connectivity Problems . . . 62
8.2 SCSI Device Related Problems . . . 62
8.3 Network Performance Problems . . . 63
8.4 iSCSI Performance Problems . . . 64
8.5 Recovery Wizard . . . 64
8.5.1 Factory Restore . . . 65
8.5.2 Delete Configuration . . . 67

Appendix A IP Protocols and Port Numbers 70
A.1 Inbound LAN Protocols and Port Numbers . . . 70
A.2 Outbound LAN Protocols and Port Numbers . . . 70

Appendix B Accessing the Gateway from Windows using a static IP Address 71

Appendix C Connecting to an iSCSI Device using the Microsoft iSCSI Initiator 75
C.1 General Set up . . . 75
C.2 Discovery of Devices . . . 76
C.2.1 Adding an iSCSI Target Portal . . . 77
C.2.2 Adding an iSNS Server . . . 79
C.3 Connecting to a Target . . . 80
C.4 Viewing iSCSI Session Details . . . 83
C.5 Creating Multiple Connections (Optional) . . . 84
C.6 Logging off an iSCSI Session . . . 89

Appendix D Connecting to an iSCSI Device using iscsiadm 90
D.1 Discovering iSCSI Targets . . . 90

D.2 Logging into a target 91
D.3 Logging out of a target 93
D.4 Logging out of all targets 94

Appendix E Useful Links **96**

Introduction

Thank you for purchasing the Bridgeworks Oresund EFC iSCSI to Fibre Channel Gateway.

The Gateway has been designed to ensure that in the majority of installations it will require minimal setup before use. However, we suggest you read the following section which will guide you through setting up both the network, iSCSI and Fibre Channel aspects of the Gateway.

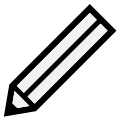
Overview

The EFC creates an interface between a network, which utilises the iSCSI protocol, and devices that reside upon the Fibre Channel Storage Area Network (SAN). The internal circuitry of the Gateway acts as a two-way interface converting the data packets that are received on the iSCSI network to Fibre Channel data packets.

This data is then ready to be sent across a network to Fibre Channel-enabled storage devices such as disks and tape drives.

Manual Layout

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

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

Definitions

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

iSCSI Target Device

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

iSCSI Qualified Name (IQN)

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

iSCSI Challenge Handshake Authentication Protocol (CHAP)

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

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

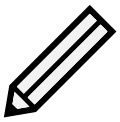
Using the Web Interface

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

Browsers

This Gateway supports the following browsers:

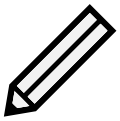
- Microsoft Internet Explorer 11
- Microsoft Edge[1]
- Mozilla Firefox[1]
- Google Chrome[1]



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

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

Connecting to the Web Interface



Note:

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

  Management A/Port 1 `10.10.10.10`

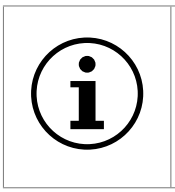
  Management B `10.10.10.12`

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

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

[1] Latest version as of release

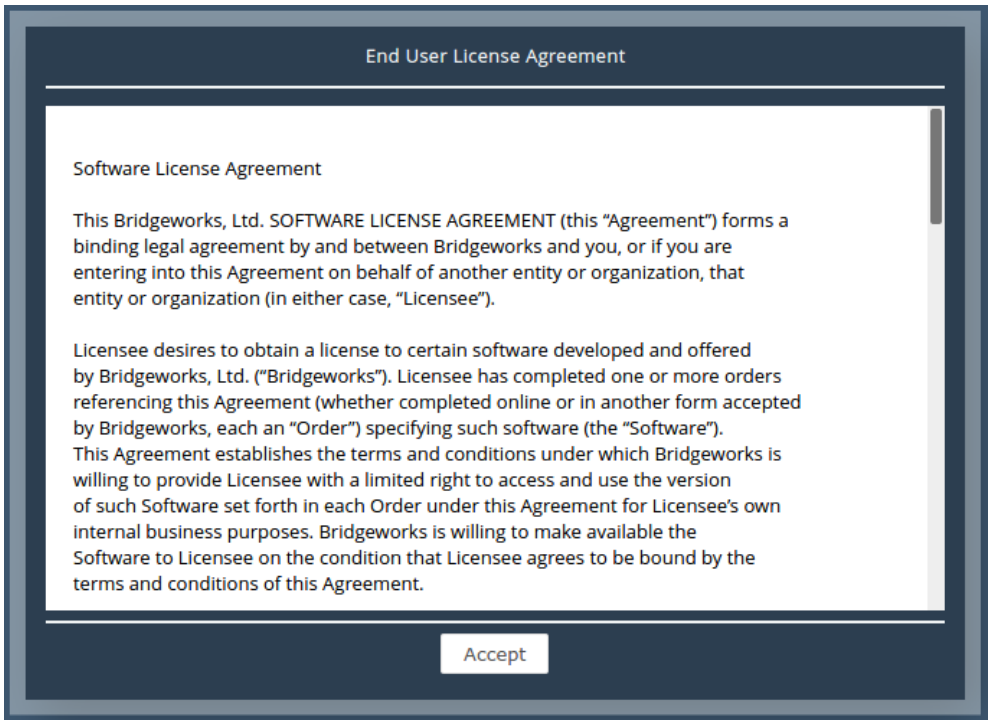
If the Gateway fails to receive a DHCP address, the web interface can be accessed from the default static IP address by navigating to: `http://10.10.10.10/` or `http://10.10.10.12/`



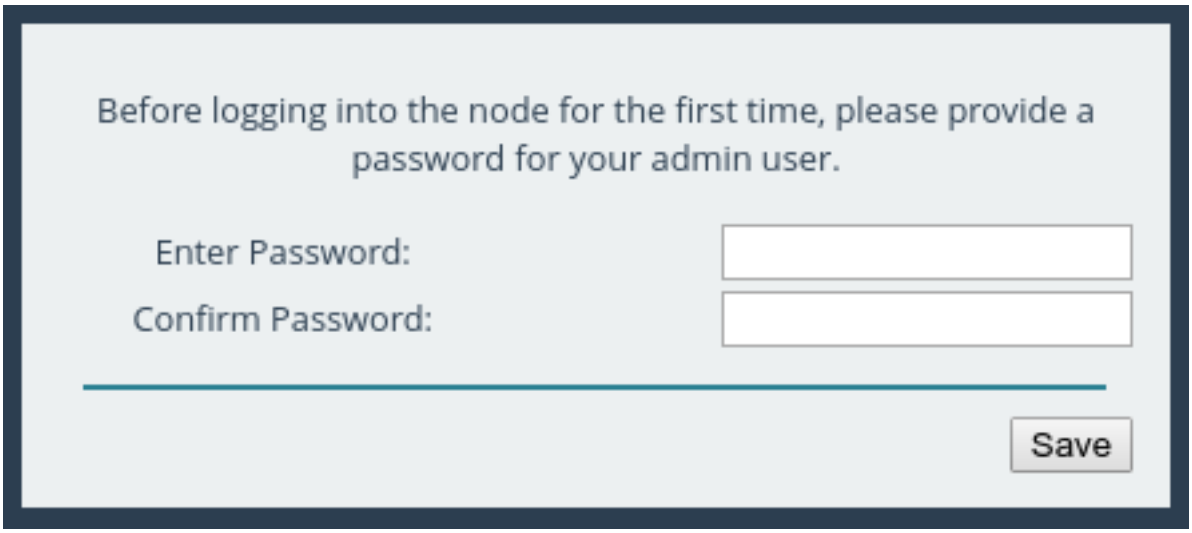
Important: Your host will likely need to be directly-connected to the Gateway if DHCP is not enabled, and its subnet set appropriately. See Appendix B: Accessing the Gateway from Windows using a static IP Address for help with accessing the Gateway web interface without DHCP.

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

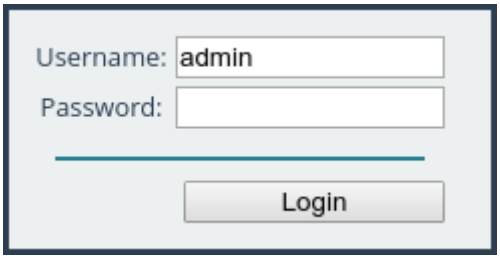
Once you have connected to the web interface on the Gateway you will be provided with the Bridgeworks End User License Agreement (EULA) which must be accepted before you are able to access the Gateway. Ensure you read this agreement thoroughly. To proceed, you must accept the agreement by clicking the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



You will then see the entry page shown below:



Enter and confirm the new web interface password to be presented with the login screen. The password must be between 5 and 65 characters and should contain both symbols and numbers.

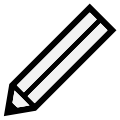


To access the web interface a username and password must be used. The default username is *admin*.

Management Console (Home screen)

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

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

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

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

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

Bridge Configuration

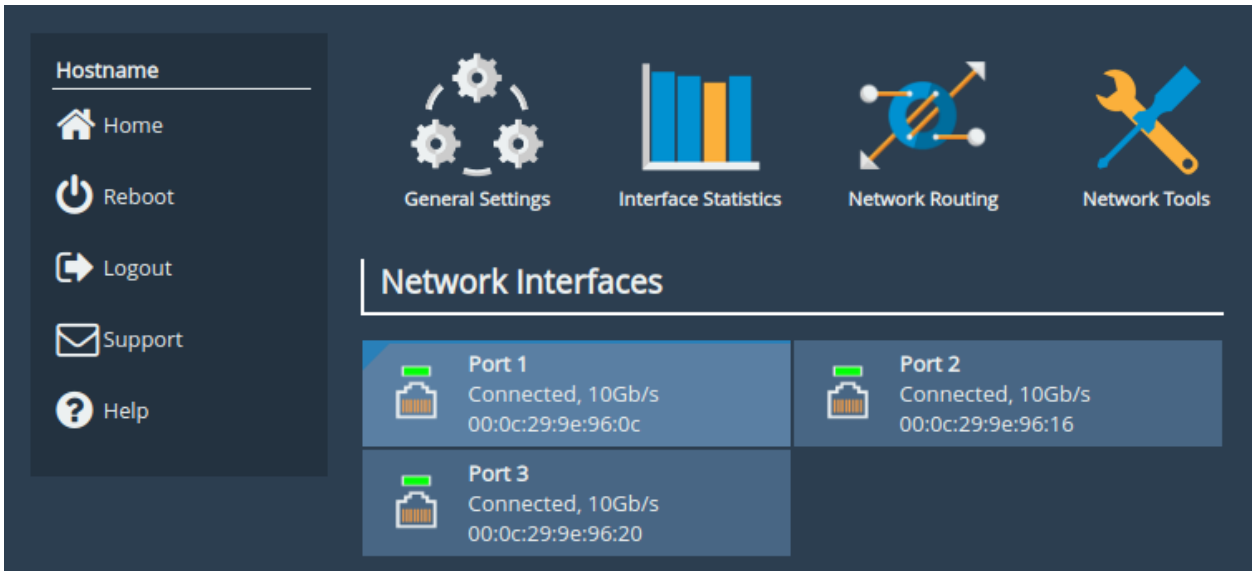
This section details the configuration of the Gateway's basic network and service settings.

Network Connections

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

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

The web interface will display the following:



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

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

Network Interfaces

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

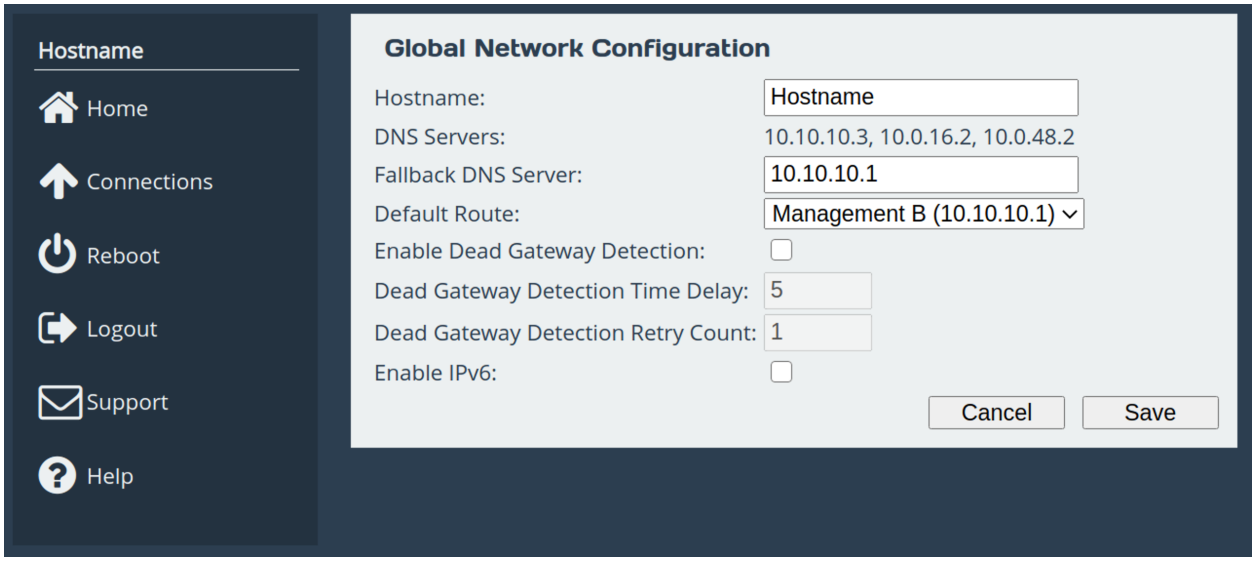
Clicking on a particular interface will navigate to a bespoke configuration page for that particular interface. More information on the different interface settings is available in Section 3.1.6: Port Settings.

General Settings

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

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

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



Hostname

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

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

DNS Servers

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

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

Default Route

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

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

Dead Gateway Detection

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

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

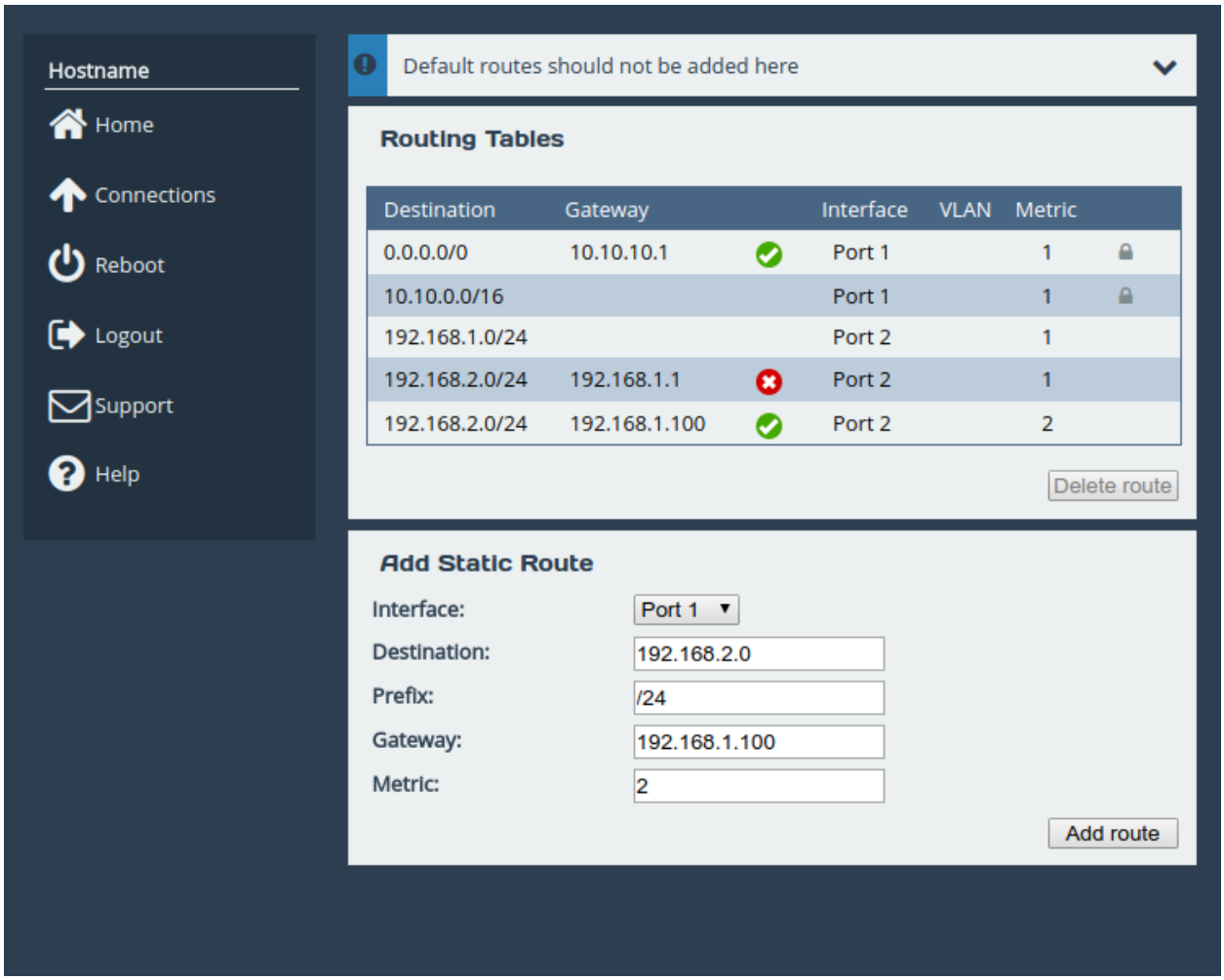
Dead Gateway Detection Retry Count refers to the number of times an unreachable gateway will be contacted before being set as a dead gateway and removed.

The status of each gateway is displayed on the *Routing* page. Refer to Section 3.1.4: Network Routing for information on viewing and modifying network routes. An icon next to each gateway indicates its state:

Live Gateway Represents a gateway that responds to ICMP echo

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

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



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

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

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

Enable IPv6

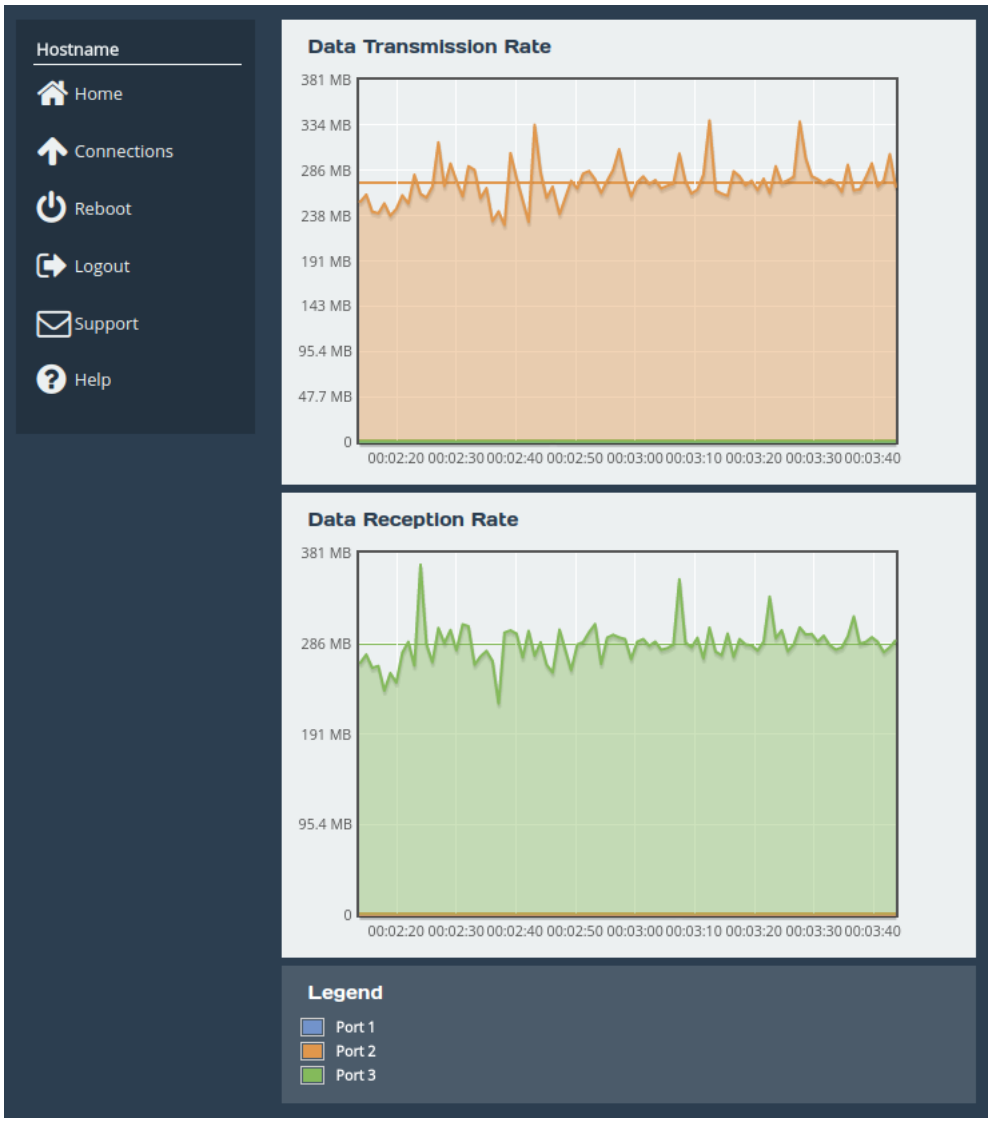
Selecting the *Enable IPv6* checkbox will enable the Gateway to use IPv6 addresses. As with IPv4, you can either choose automatic address assignment or assign a static IPv6 address.

Interface Statistics

This page displays live network interface data rate statistics.

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

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



Data Transmission Rate

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

Data Reception Rate

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

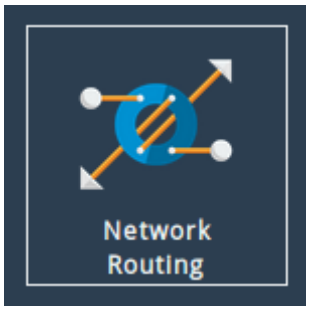
Legend

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

Network Routing

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

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



Add Static Route

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

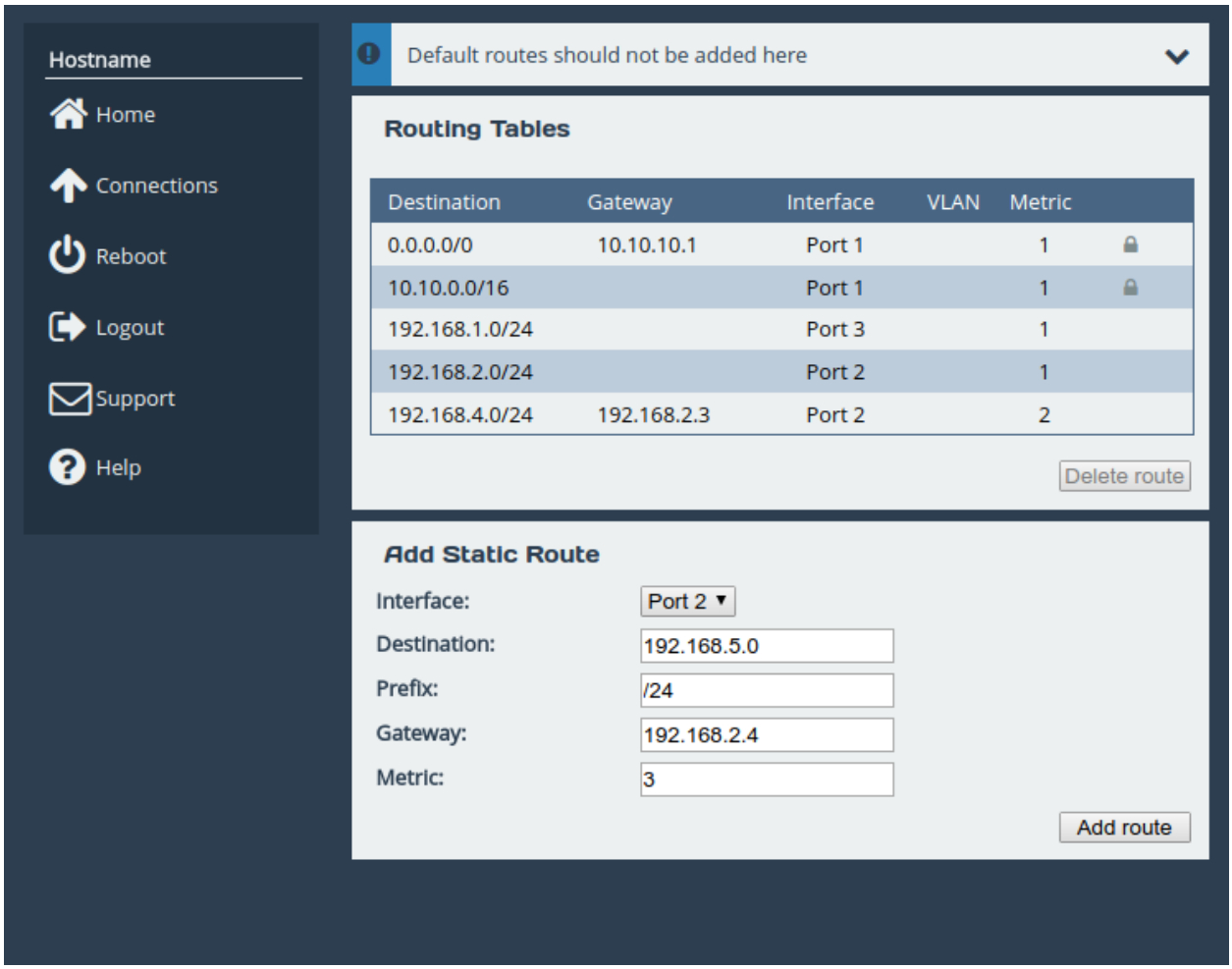
Interface The network interface to which the route applies.

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

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

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

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



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

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

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

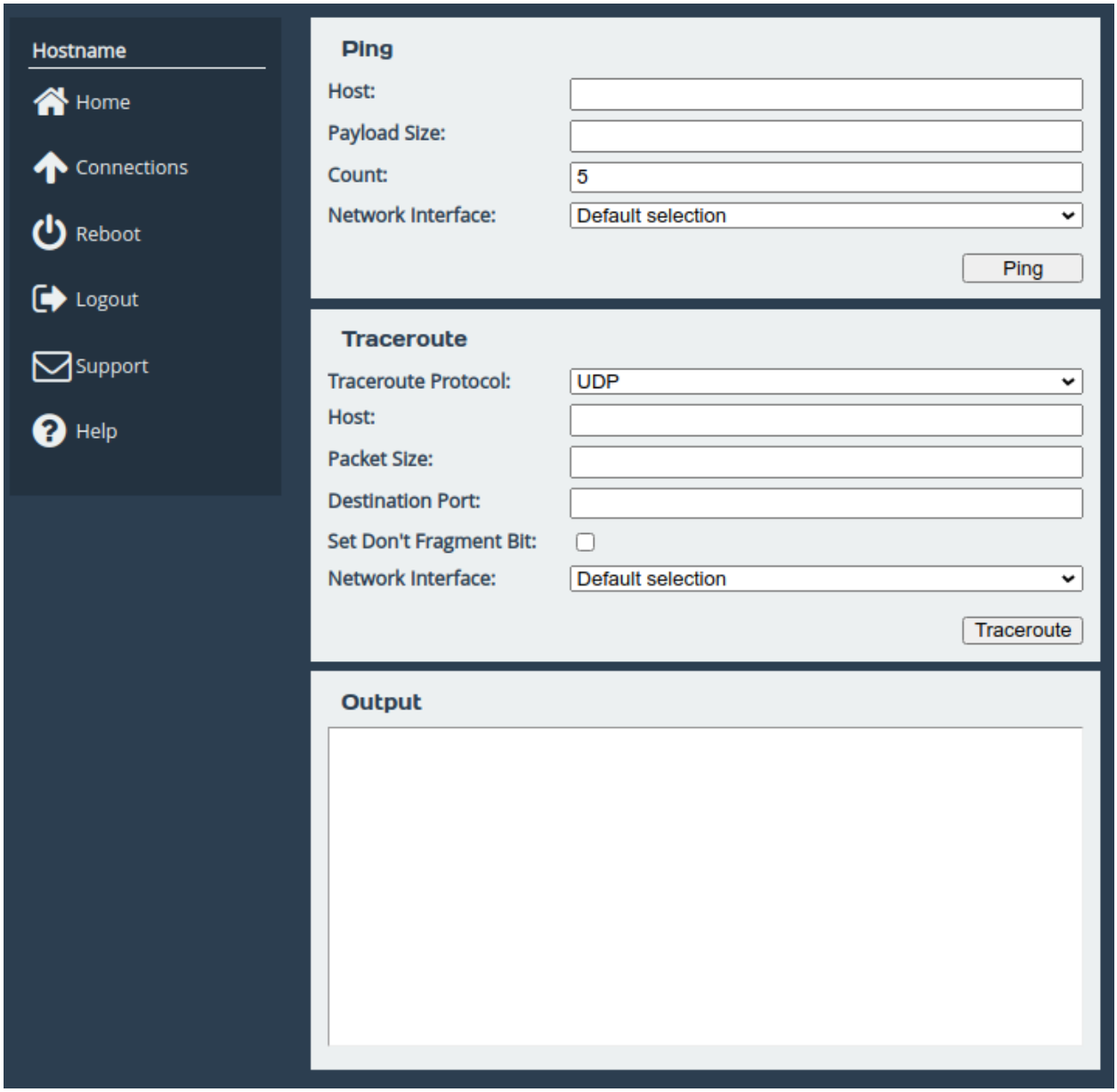
When dead gateway detection is enabled, each gateway in the table will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.2.4: Dead Gateway Detection for more information.

Network Tools

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

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

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



Ping

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

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

Host The IP address of the network host.

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

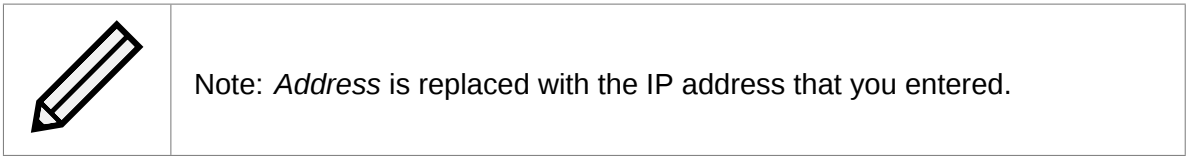
Count The number of ping attempts that you wish the Gateway to perform. Setting the count to 0 will send pings indefinitely, until the page is navigated away from, or another ping/traceroute operation is initiated.

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

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

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

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



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

Traceroute

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

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

Host The IP address of the network host.

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

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

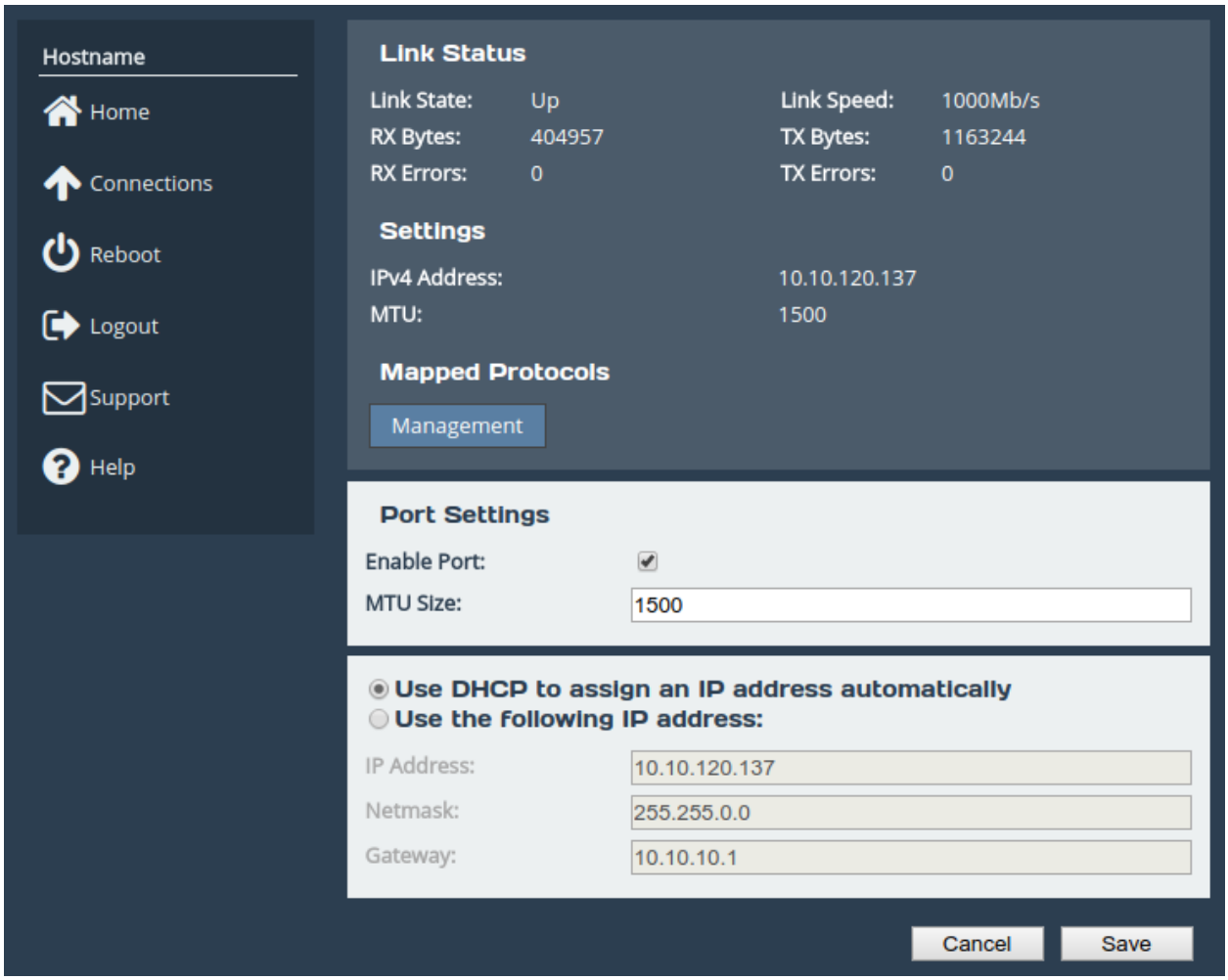
Use ICMP Echo Select to use ICMP echo requests instead of UDP datagrams. This can be useful when your firewall blocks UDP traffic.

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

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

Port Settings

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



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

Enable Port

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

Setting the MTU

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

Enabling larger frames on a jumbo frame-capable network can improve your network throughput.

Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU).

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

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

Setting the IP Address

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

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

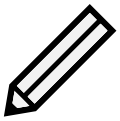
If the server is not found, this port will fall back to its saved static IP settings.

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

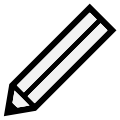
The gateway field may be left blank.

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

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



Note: DHCP is enabled by default on management interfaces.



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

Committing the Changes

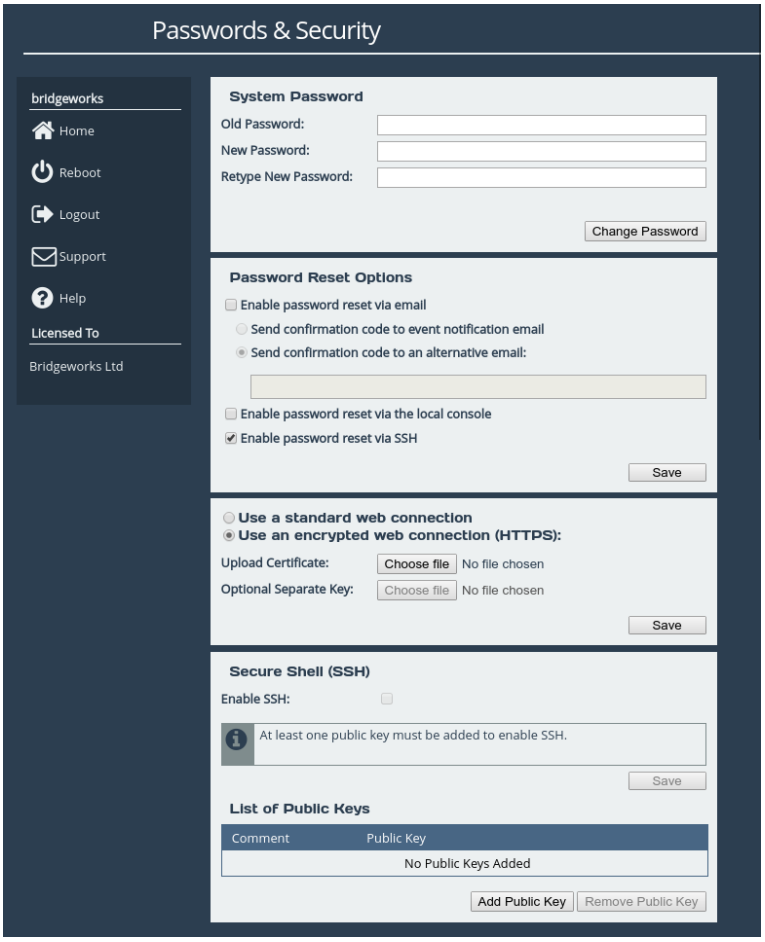
Click the *Save* button to save these parameters, then reboot the Gateway to apply them.

Passwords & Security

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

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

The web interface will display the following:



System Password

This section allows the administrator to change the access password for the web interface. The new password must be between 5 and 65 characters and should contain both symbols and numbers.

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

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

Password Reset Options

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

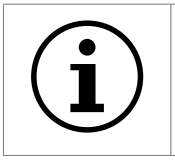
Password Reset via Email

3.2.2.1.1 Setup

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

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

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



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

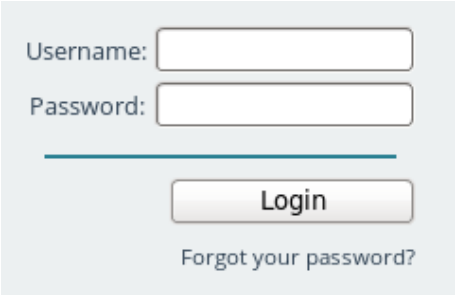
To enable password reset via email, SMTP settings will have to be configured first to allow the Gateway to send emails. Navigate to the *Service Control* page and enter your SMTP settings under the *Simple Mail Transfer Protocol (SMTP)* section. Refer to Section 3.3.3: Simple Mail Transfer Protocol (SMTP)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

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

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

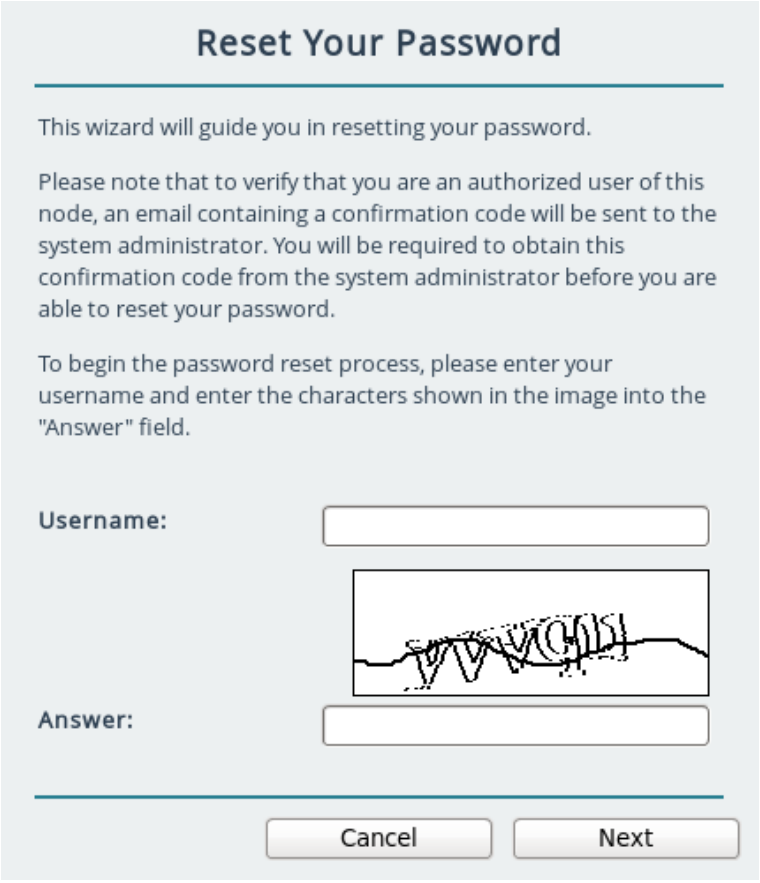
3.2.2.1.2 Using Password Reset via Email

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



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

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

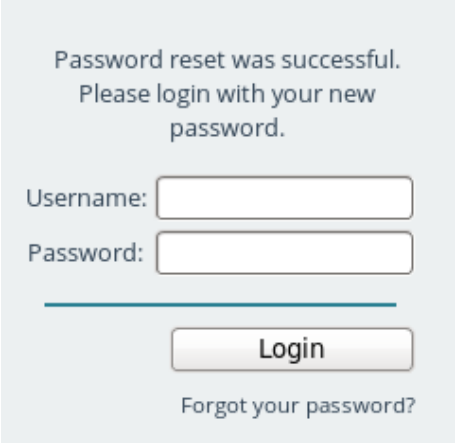


	Important: You can try a different captcha challenge by refreshing the web page.

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

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

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



Password Reset via Local Console or SSH

3.2.2.2.1 Setup

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

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

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

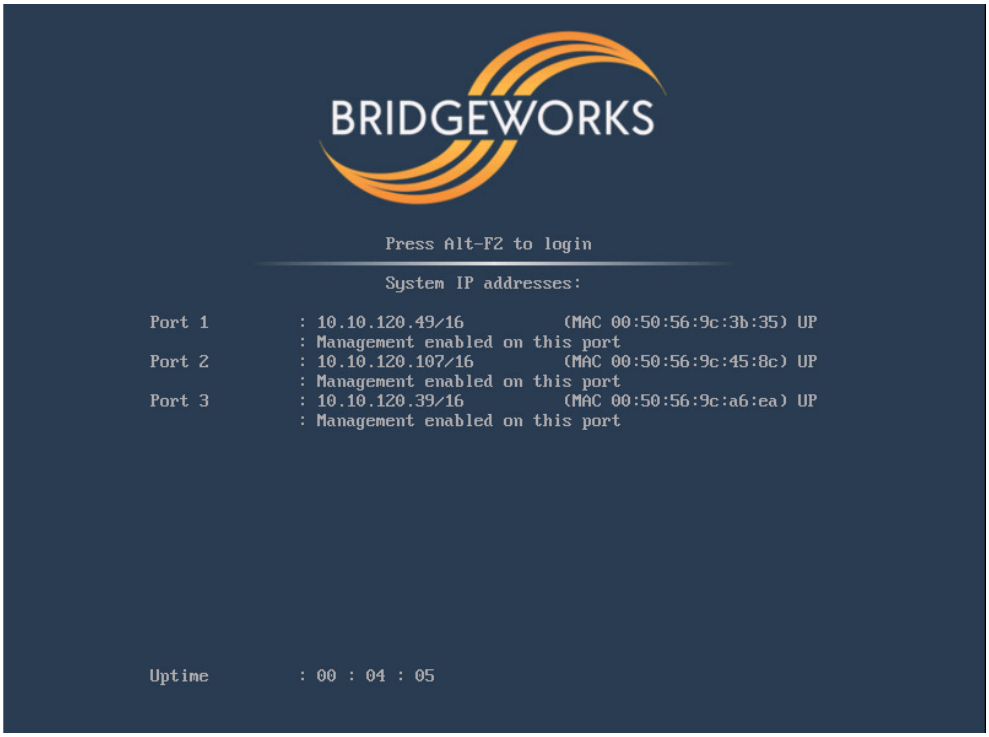
To enable password reset via local console, tick the *Enable password reset via the local console*

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

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

3.2.2.2.2 Using Password Reset via Local Console or SSH

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

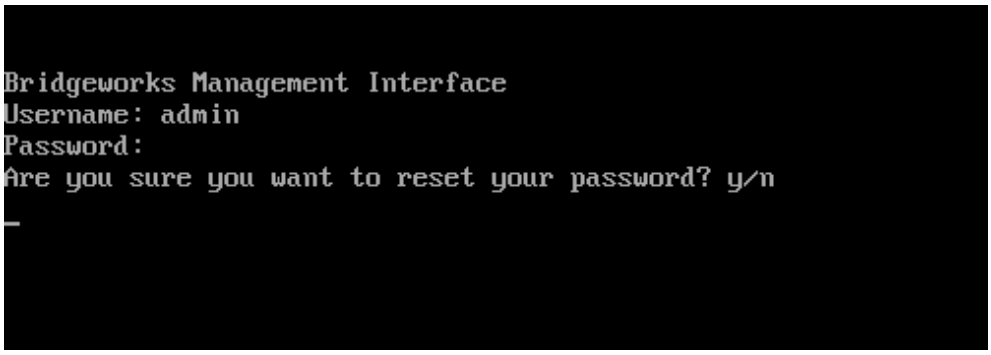


Press the “Alt” and “F2” keys at the same time to get access to the login prompt as shown:

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

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

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



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

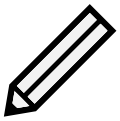
	Important: If the two passwords do not match, or you are attempting to set the password as “RESET”, then password reset will fail.

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

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

Secure Connection

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

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

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

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

Secure Shell (SSH)

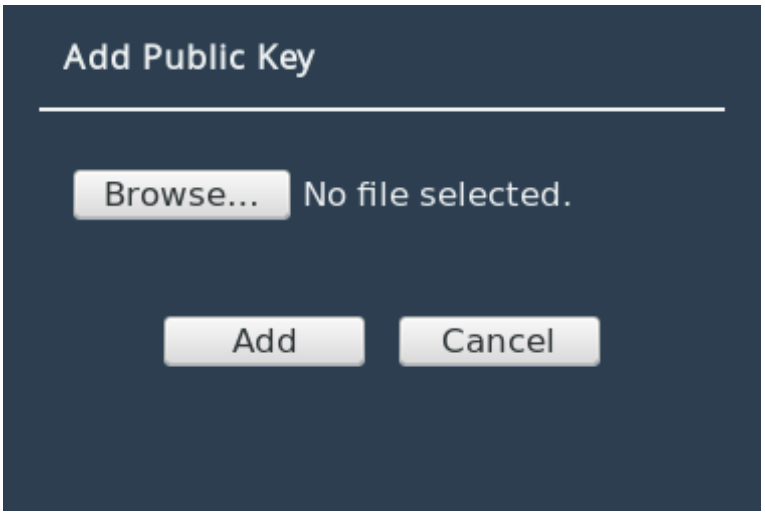
Secure Shell (SSH) is a protocol that allows for secure access to a Gateway's configuration console.

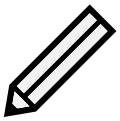
To enable SSH on network interfaces with the "Management" protocol mapped, tick the *Enable SSH* checkbox and click *Save*.

Managing Public Keys

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

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



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

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

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

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

Using SSH

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

```
ssh admin@192.168.0.20
```

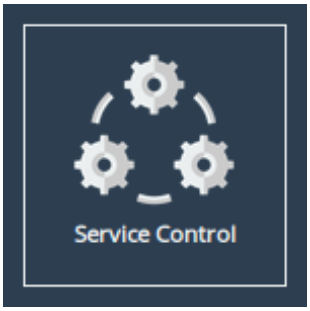
You will then be prompted for the username and password of the Gateway to log in to the configuration console.

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

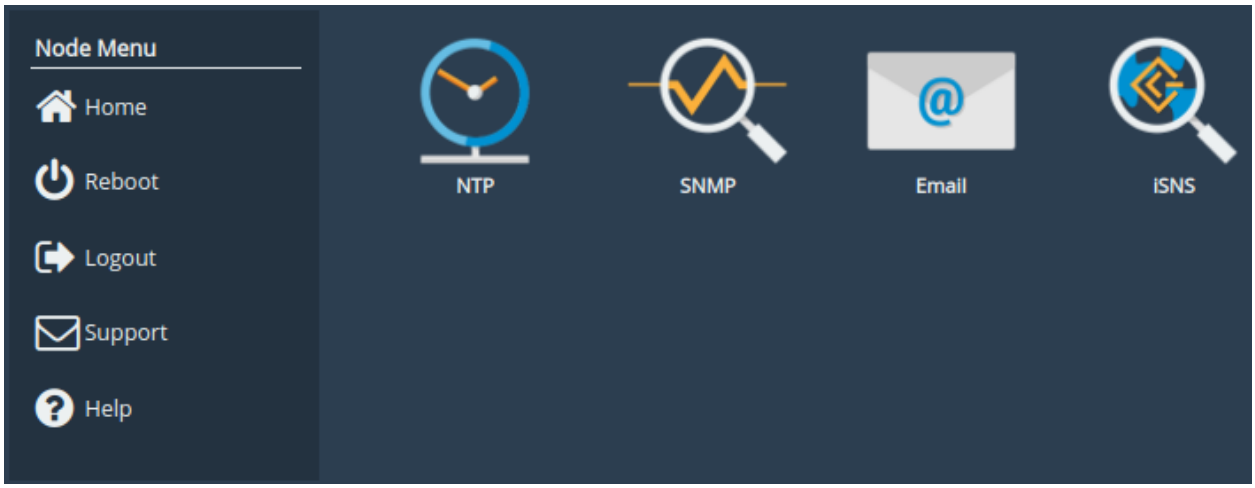
	Important: Logging in as root user is disabled on SSH.

Service Control

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



The web interface will display the following:



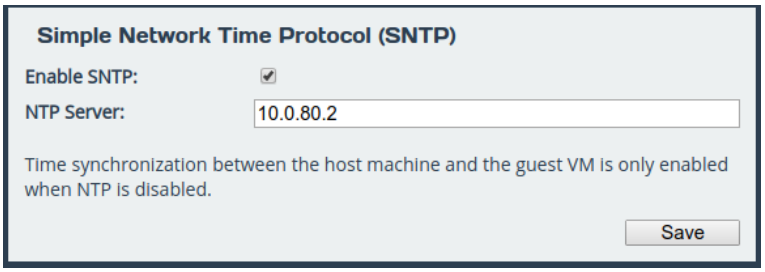
Each link leads to a different service.

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

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

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

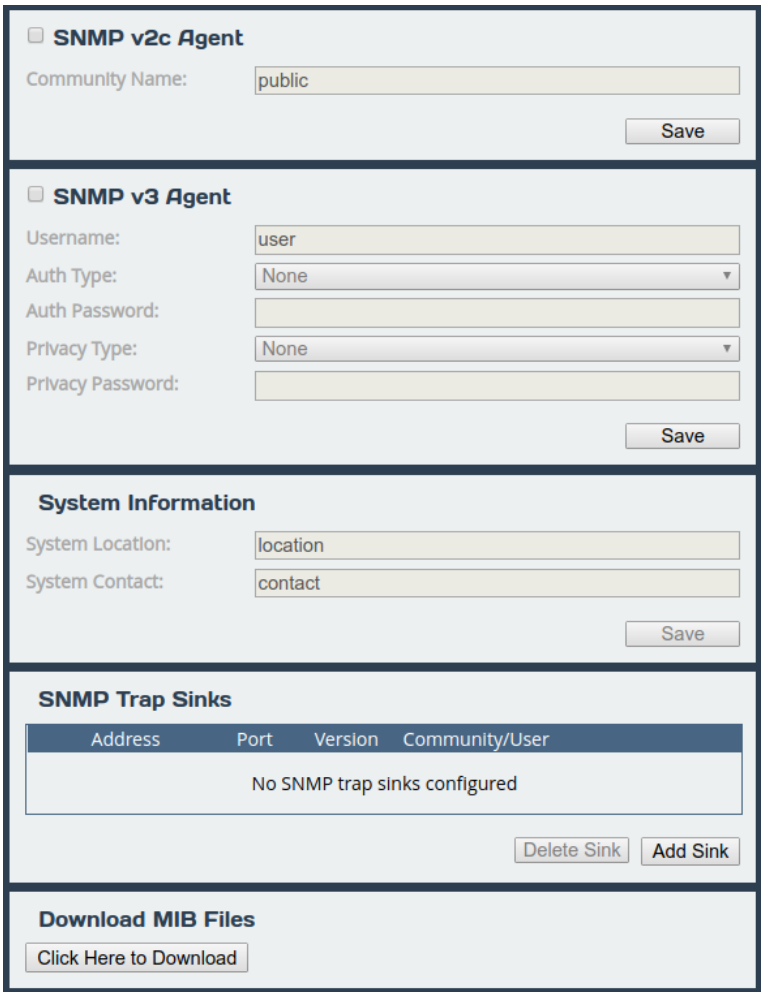
Simple Network Time Protocol



SNTP is a protocol for synchronising the clock of computer systems. This feature is critical if you are planning on using the scheduler or useful when viewing the logs to determine when an event occurred. Refer to Section 7.2: System Log for more information.

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

SNMP Agent



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

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

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

System Information

The information configured here is accessible over SNMP.

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

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

SNMP Trap Sinks

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

Click *Add Sink* to access the Sink Configuration dialogue. *Address* and *Port* are the network address of the trap sink. SNMP v1 only supported traps. v2c and v3 have a *Type* dropdown with an *Inform* option. An *Inform* requests a response from the manager, *Traps* do not. The other values must match your trap sink's configuration.

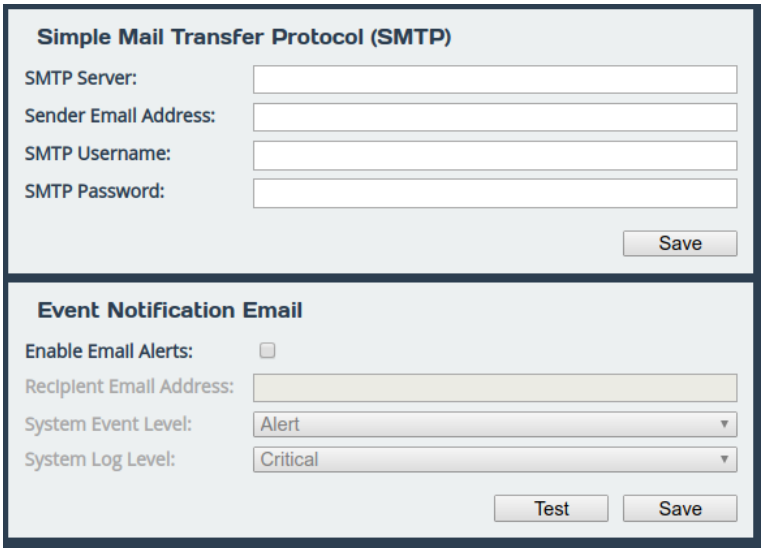
Download MIB Files

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

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

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

Simple Mail Transfer Protocol (SMTP)



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

The fields in this subsection are:

SMTP Server To enable an SMTP server, enter its IP address or hostname in this field. It must be reachable from the Gateway's Management interface (or whichever port the default route is set to) on this address. Refer to Section 3.1.2.3: Default Route for information on setting the default route.

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

Must be of the form: _____@_____.___

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

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

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

Event Notification Email

The Gateway can notify a systems administrator when events of a certain urgency occur in the Gateway log. Before this can be done, SMTP settings must be configured. Refer to Section 3.3.3: Simple Mail Transfer Protocol (SMTP) for information on SMTP settings.

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

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

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

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

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

Warning Example: An invalid configuration file was uploaded.

Confirm these settings by clicking *Save*.

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

Internet Storage Name Service (iSNS)

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

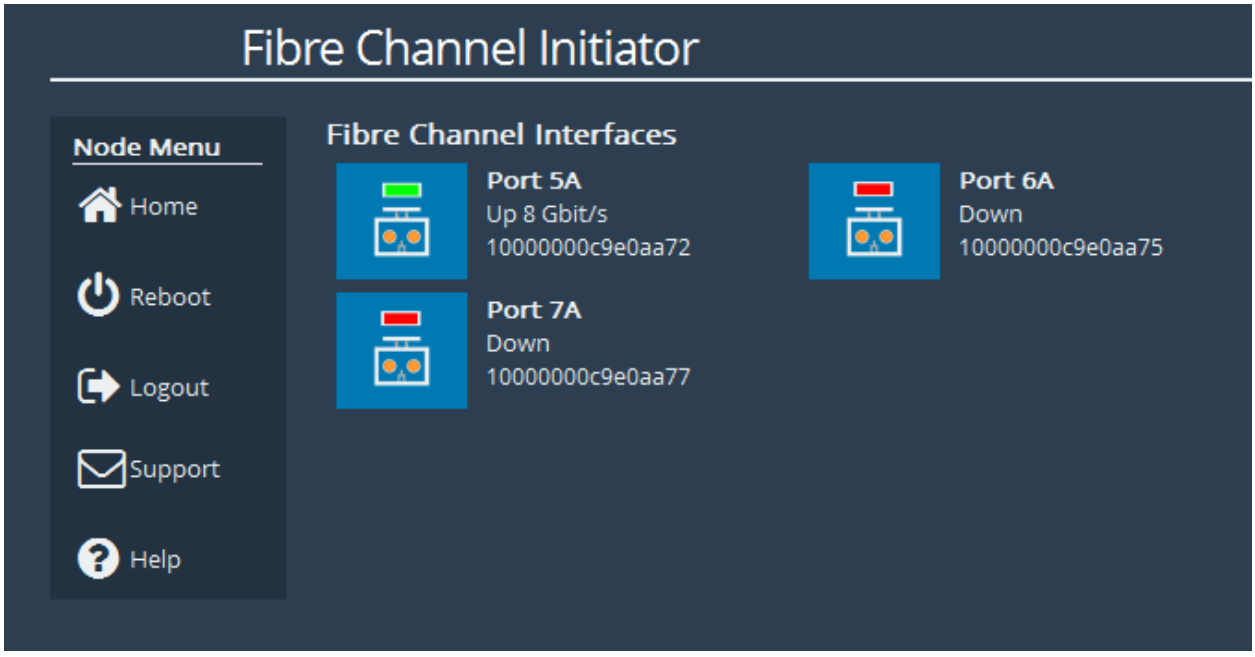
To enable this feature, select *Enable iSNS*, and enter the IP address or hostname of the iSNS server with which to register in the *iSNS Server* field. Then click *Save* to apply changes.

Fibre Channel Initiator Connections

This configuration page allows the administrator to configure ports designated as Fibre Channel Initiator interfaces.

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

You will see the following page:



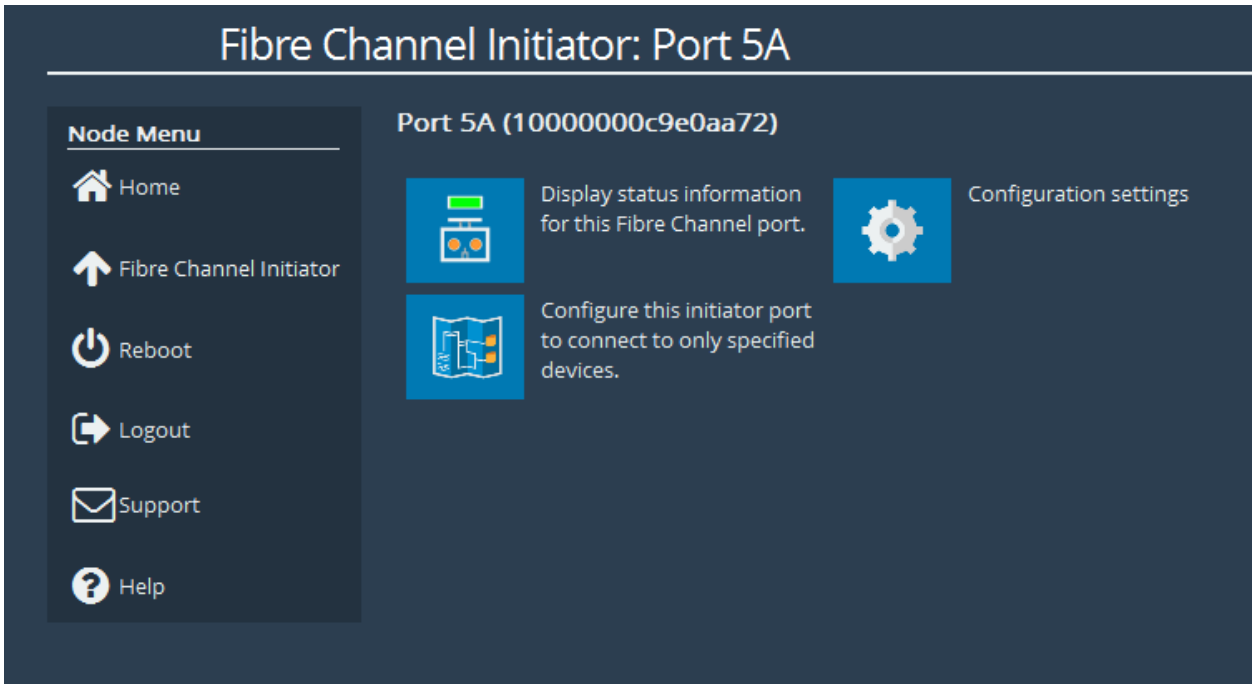
This page lists each Fibre Channel port which has been designated as an initiator. Three pieces of information are displayed about each port next to an icon. In order they are:

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

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

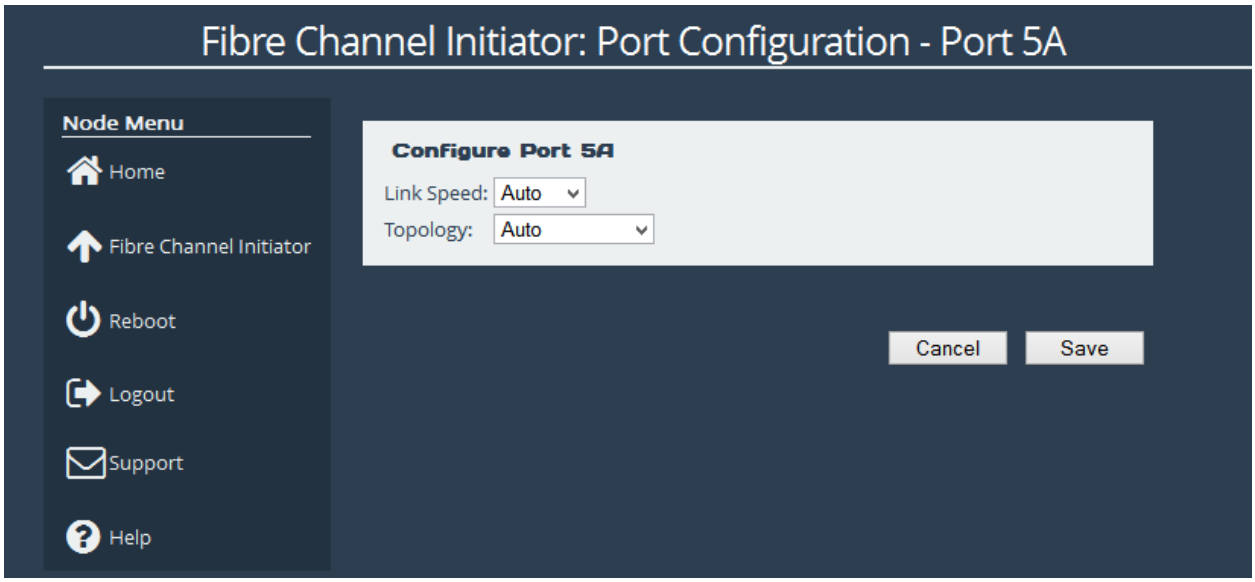
WWPN The unique World Wide Name identifier for this port.

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



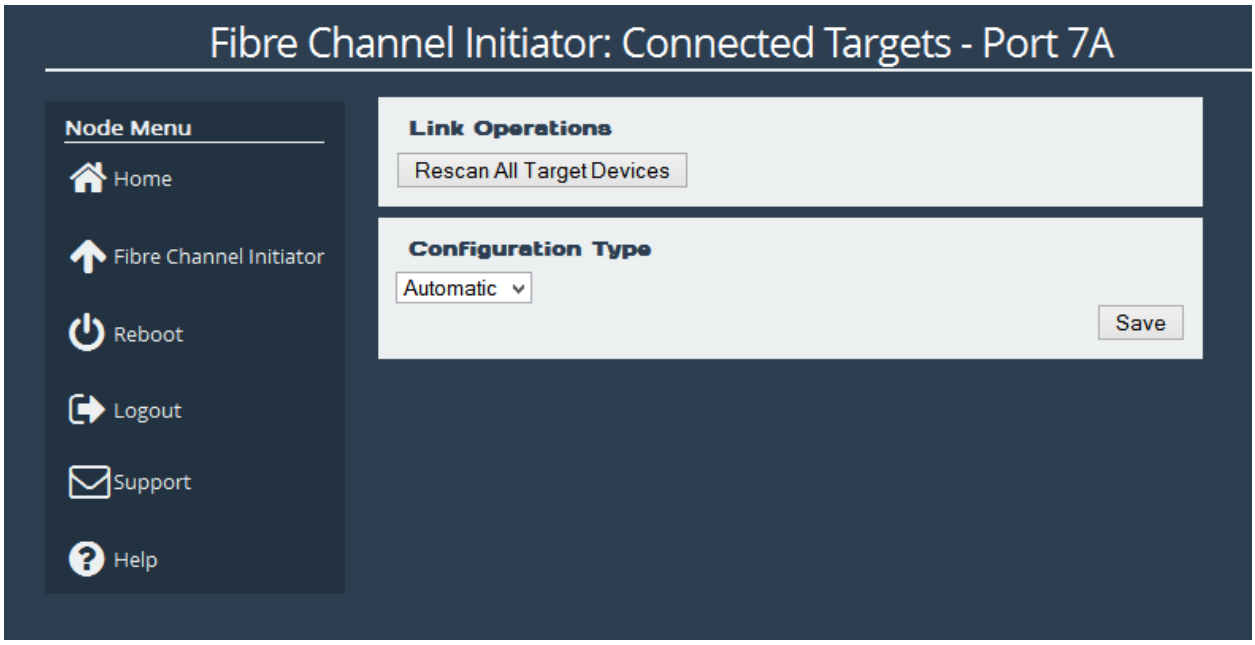
Display status information for this Fibre Channel port allows you to see verbose information about the Fibre Channel port.

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

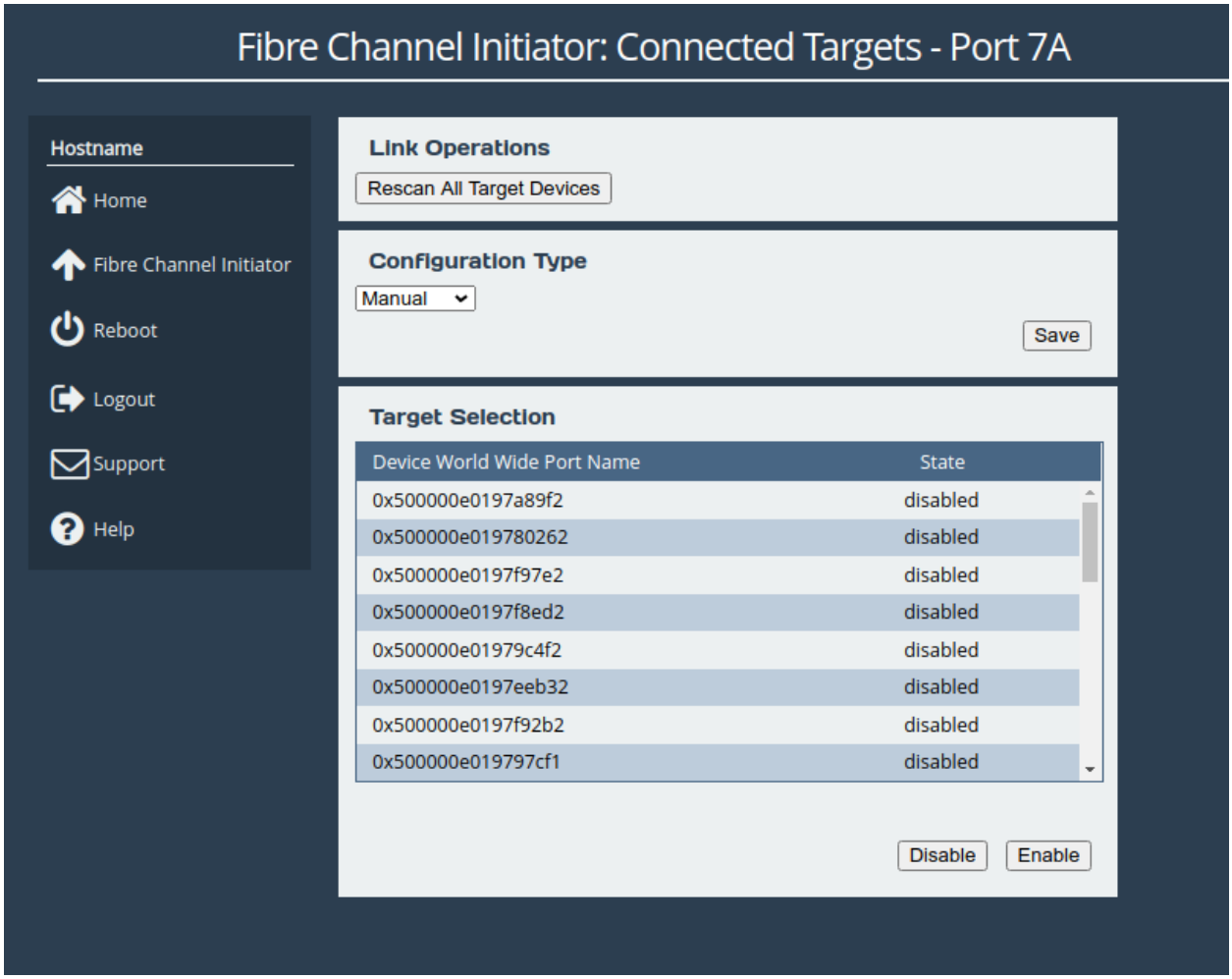


1. The *Link Speed* can be set to *Auto* or one of the speeds supported by the Fibre Channel port. In most cases this option may be left set to *Auto*. If you are unsure, set the link speed to the SFP speed. This option is not available on some products.
2. The *Topology* pull down menu has 3 options: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

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



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



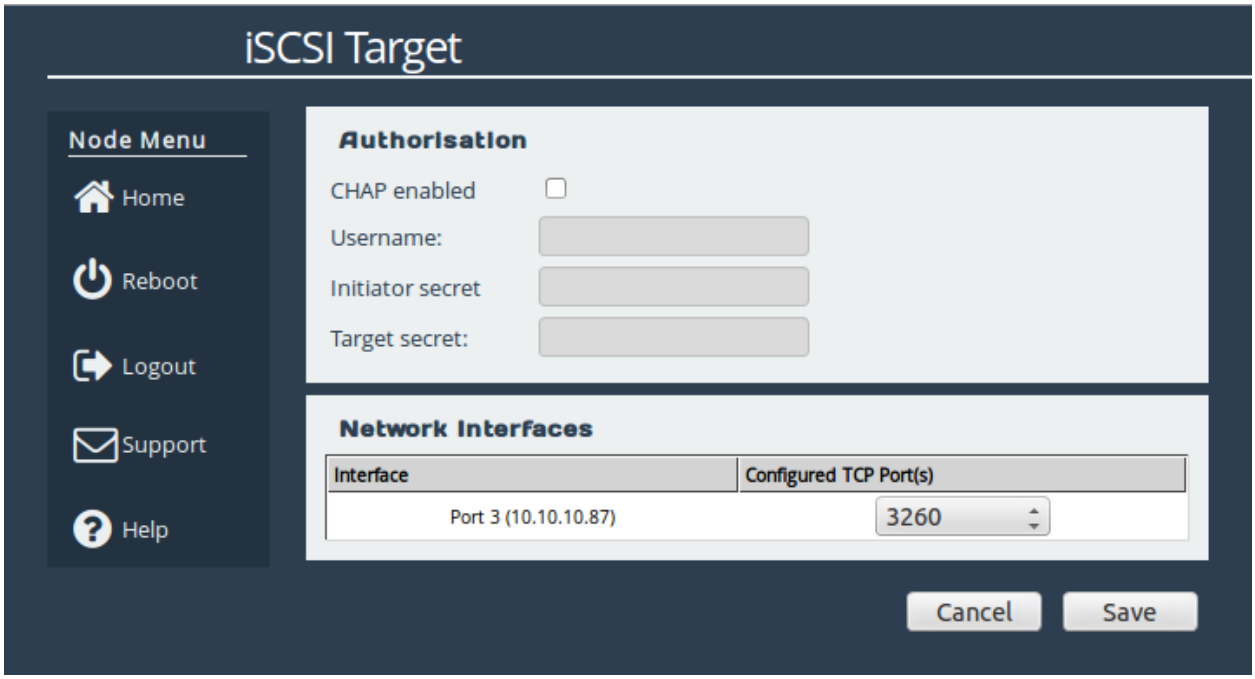
Select the FC target by clicking on its World Wide Port name, and then click *Enable* or *Disable*.

iSCSI Target Configuration

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

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

The web interface will then display the following:



Authorisation (CHAP)

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

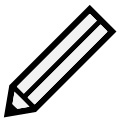
The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Bridge will authenticate itself with the initiator using the initiator secret.

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

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

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

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



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

Network Interfaces

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

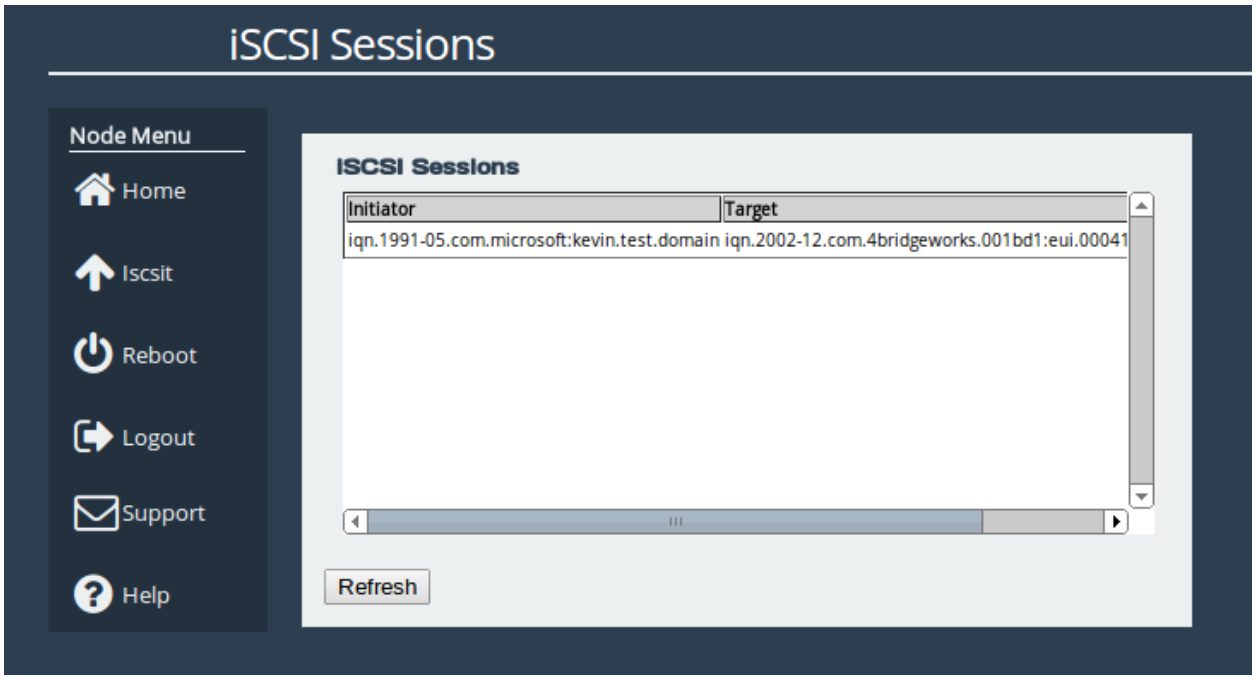
The iSCSI protocol officially uses two main TCP ports: 3260 and 860. For each iSCSI target interface, you can choose to enable either one these TCP ports, or both, or disable iSCSI on the interface completely, from the *Configured TCP Port(s)* dropdown.

iSCSI Sessions

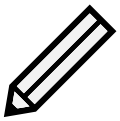
Each initiator will open at least one session with each target device it is logged on to. The iSCSI Sessions page in the web interface of the EFC can be used to review these connections.

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

The web interface will then display the following:



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

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

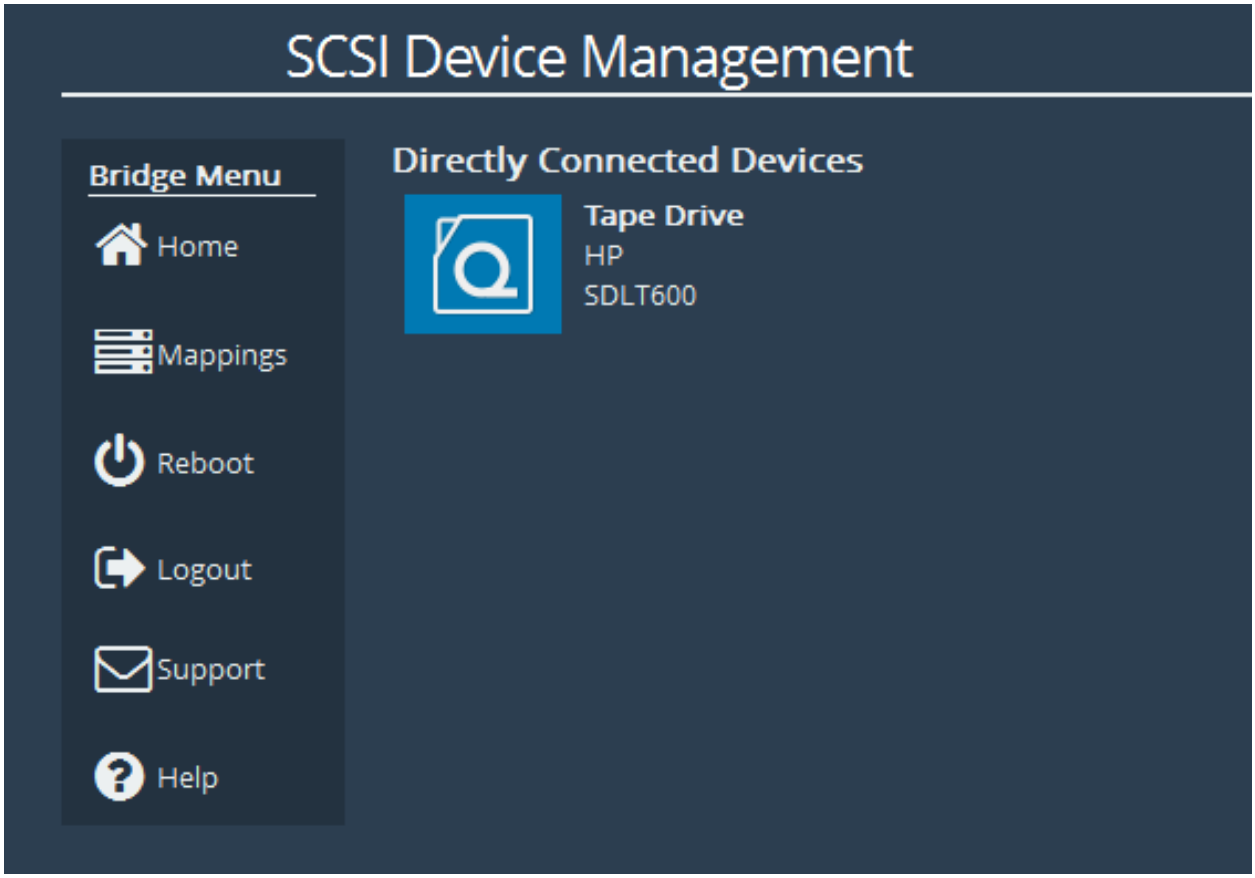
SCSI Device Management

This page allows you to view details of devices connected to the EFC.

Viewing Attached Devices

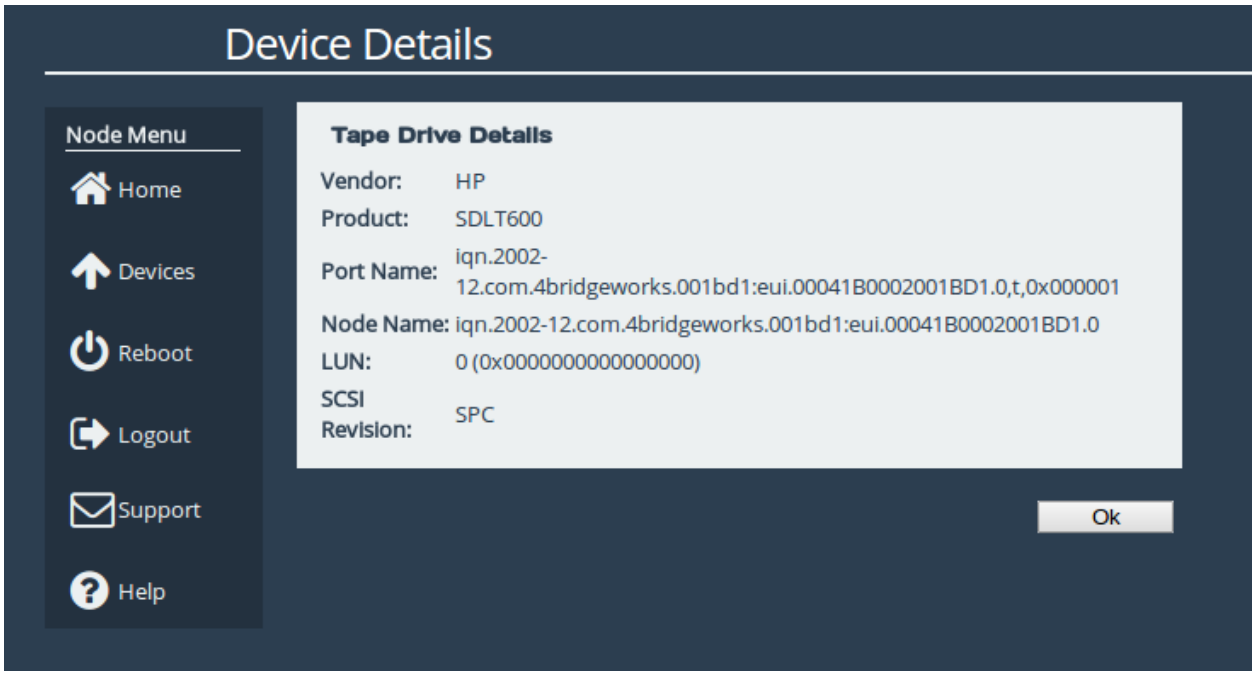
From within the Home screen of the web interface, select the *SCSI Device Management* icon under the *Devices and Protocols* section.

The web interface will then display the following:



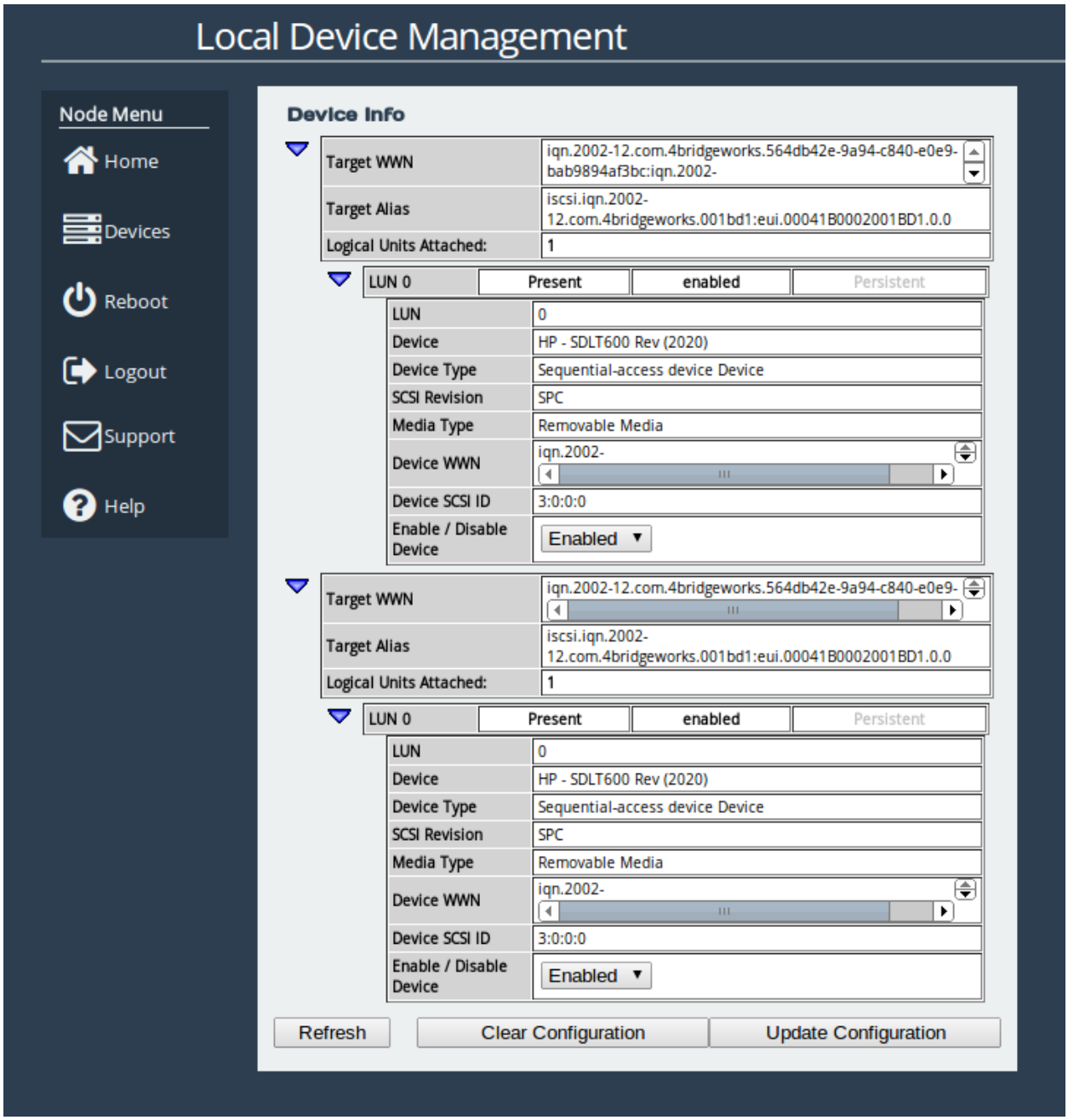
You will be presented with a list of all the devices connected to the EFC.

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



Viewing Device Mappings

Clicking on the Mappings option in the menu on the left-hand side of the page will display information about all connected devices, as shown in the following image.



A target entry exists on this page for each device that is presented on the system.

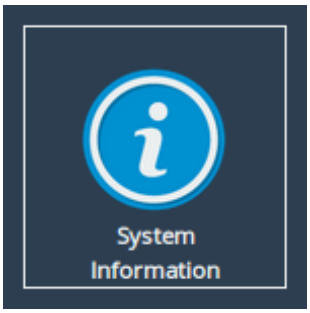
By clicking on the blue triangle in the *Device Info* section you can display further information about each device.

Bridge Maintenance

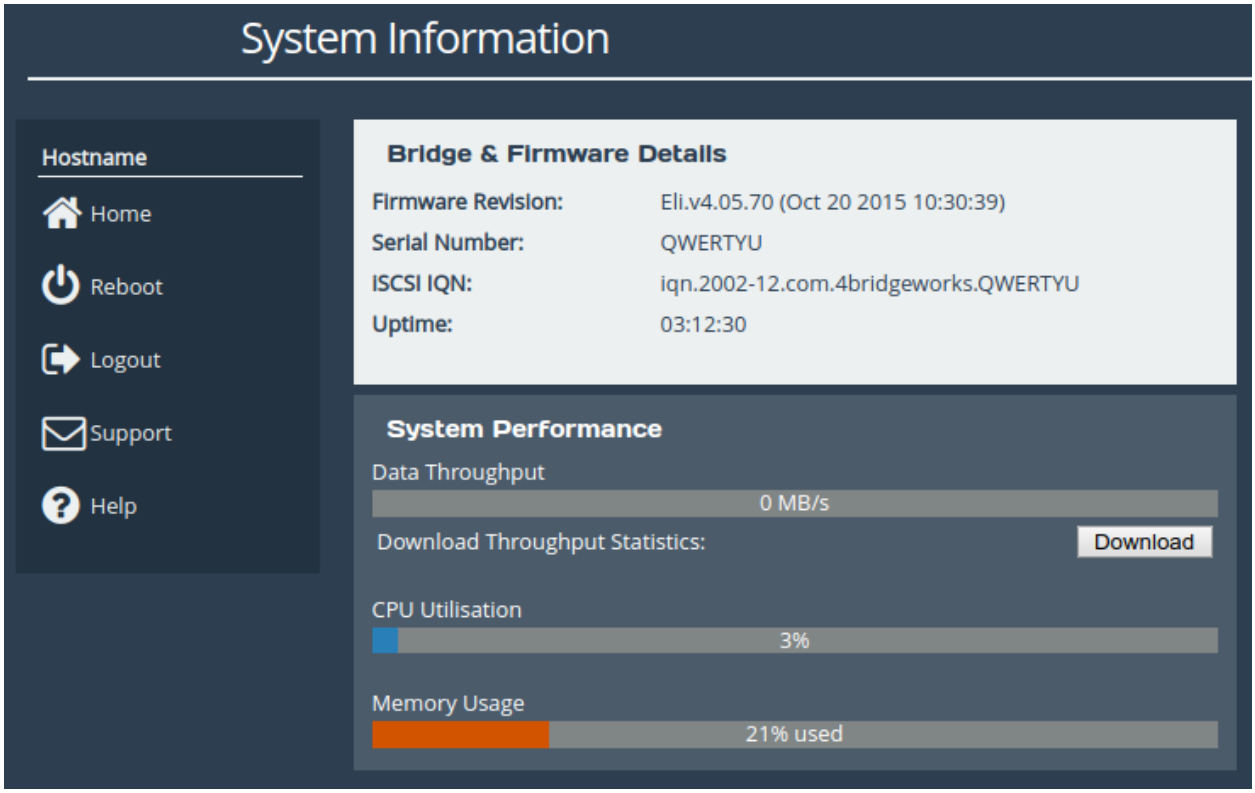
The following section describes the various pages that are available to the administrator to monitor performance and maintain the Gateway.

System Information

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



The following page will be displayed:



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

Firmware Revision is the installed firmware revision level.

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

iSCSI IQN is the iSCSI Qualified Name of that specific EFC.

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

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

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

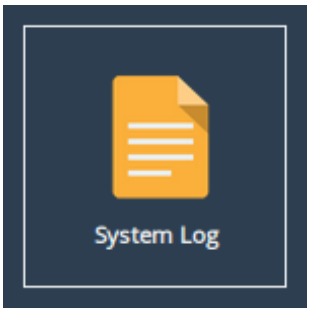
CPU Utilisation This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces.

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

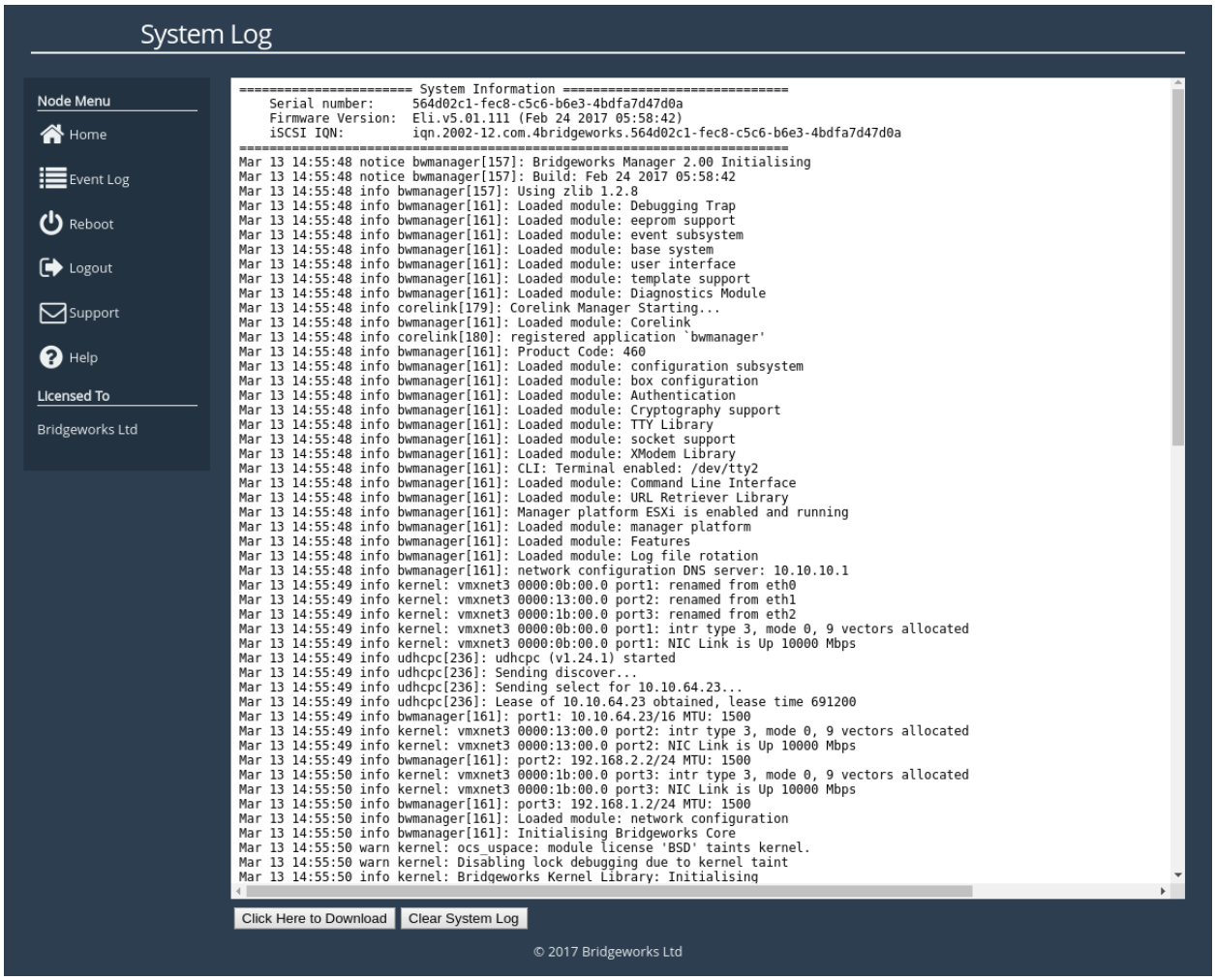
System Log

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

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



The web interface will now display the following:



Below the log display pane are two options:

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

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

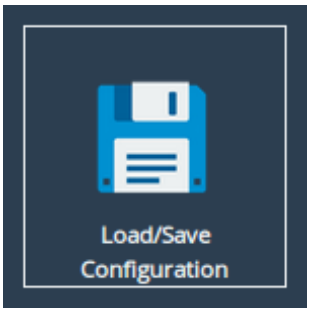
For information on troubleshooting your Gateway, see Chapter 8: Troubleshooting.

Load/Save Configuration

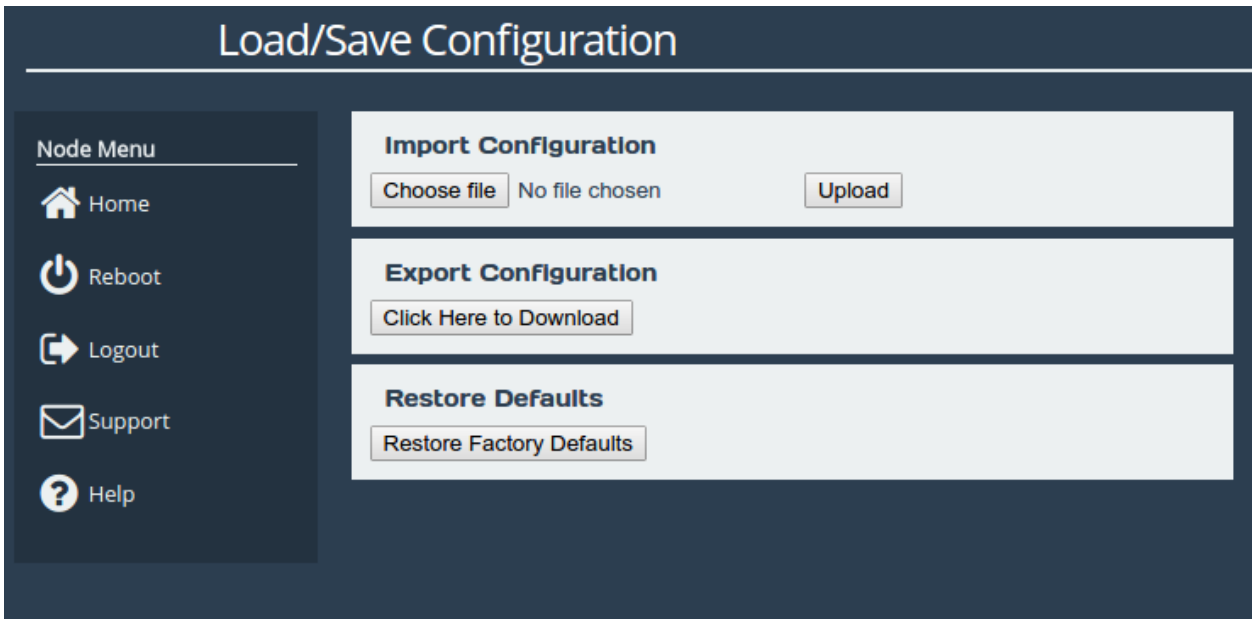
The configuration Load/Save feature allows you to save a copy of the Gateway's configuration to a file and optionally restore back to that configuration at a later time.

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

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



The following page will be displayed:



Loading a Saved Configuration

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

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

Saving the Configuration to Disk

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

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

Restoring to Factory Defaults

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

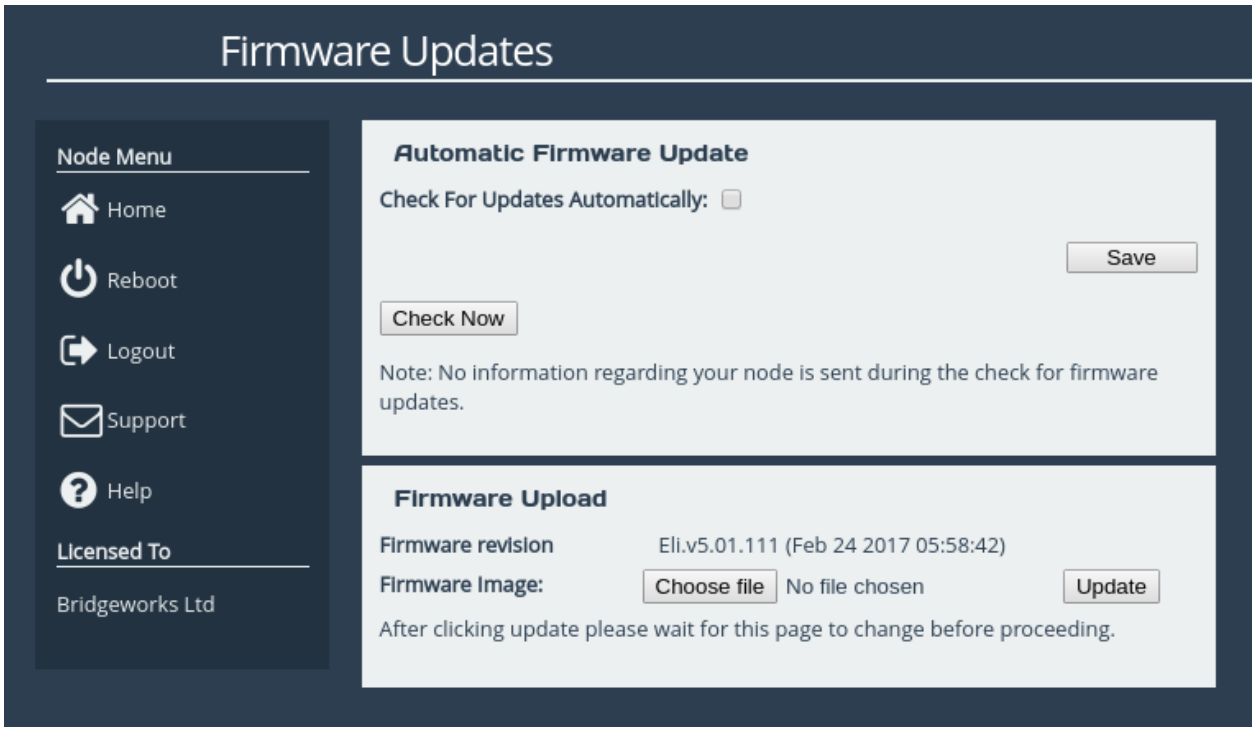
	Important: After clicking the *Restore Factory Defaults* button, a reboot will automatically occur.

Firmware Updates

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

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

The following page will be displayed:

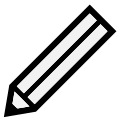


You can now instruct the Gateway to check for new firmware versions, alerting you when a new version is available and providing a button to perform the update. Alternatively, you can manually upload and update to a firmware version of your choosing.

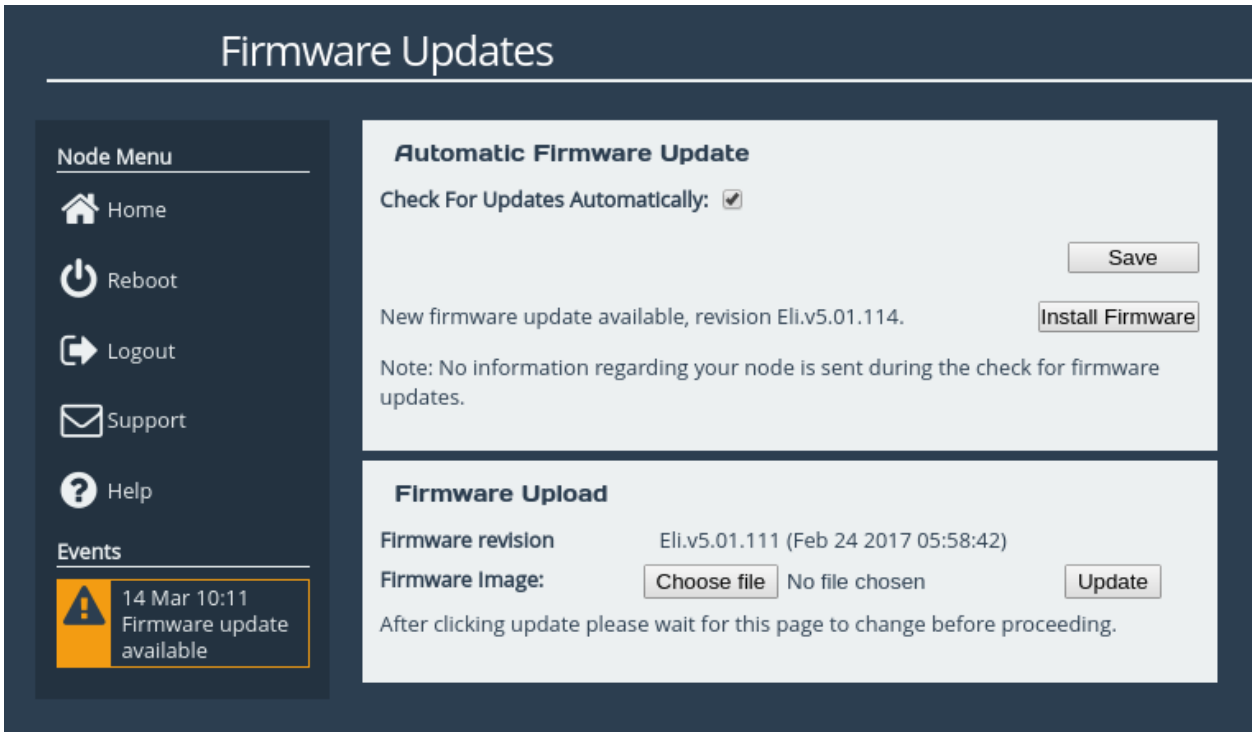
Automatic Firmware Update Checking

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

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

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

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



To start the firmware update process:

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

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

Updating Firmware Manually

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

https://support.4bridgeworks.com/download-firmware/

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

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

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

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

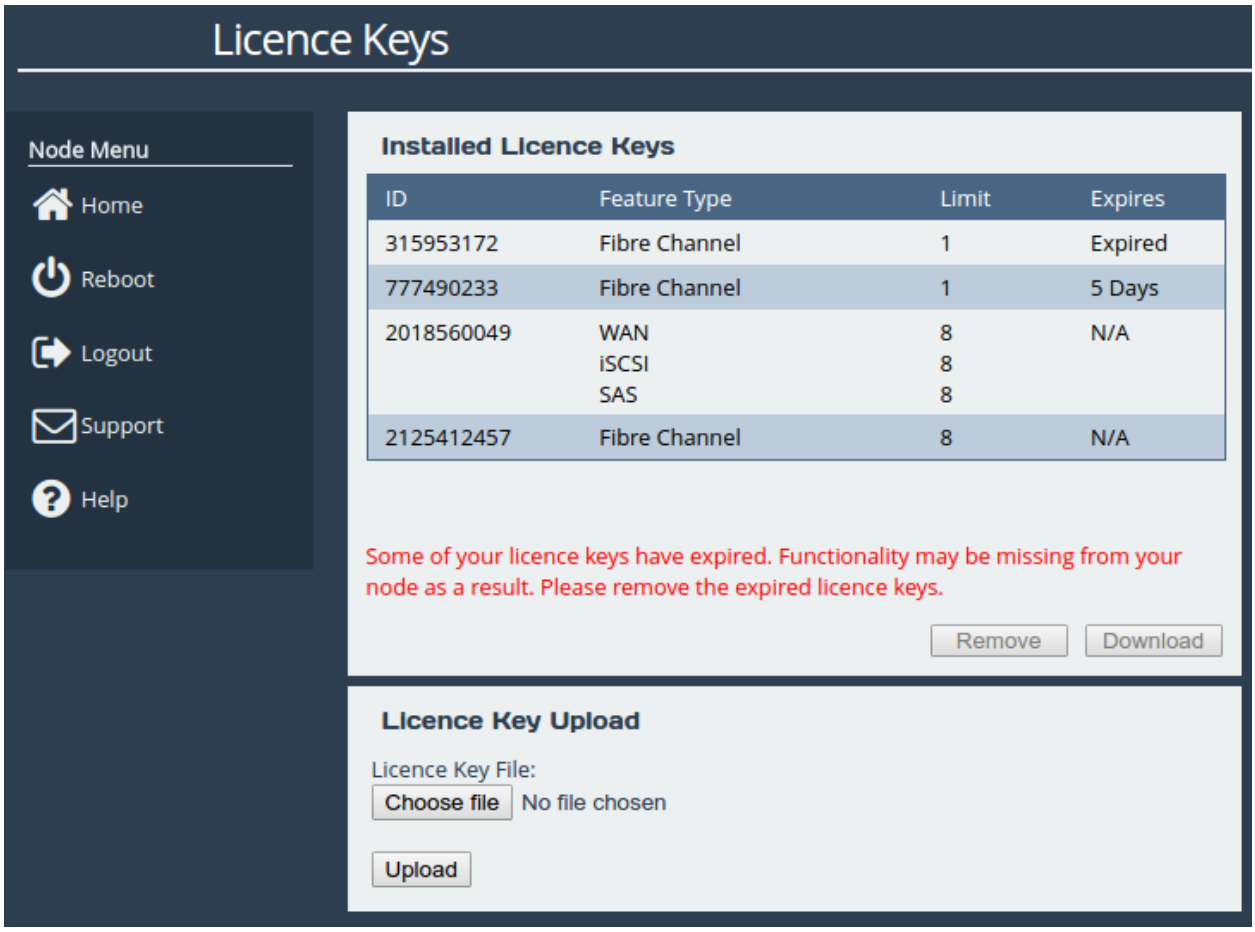
Updating the firmware will take a few minutes. After the update is complete, a notification will appear under the *Bridge Menu*, indicating that a system reboot is necessary. To reboot the Gateway, click on the *Reboot* button located in the *Bridge Menu* at the left side of the web interface.

Licence Key Management

This page allows you to view, upload, download or remove licence keys installed on the Gateway. Licence keys are required to enable features on installed feature cards.

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

The following page will be displayed:



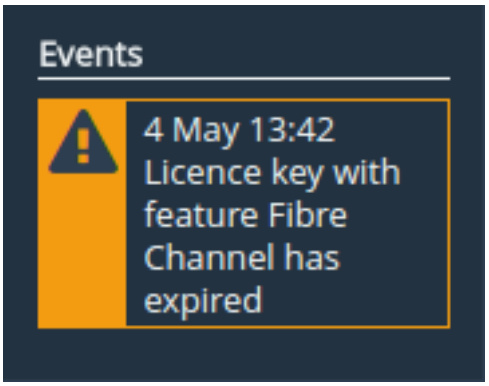
The *Installed Licence Keys* table displays the installed licence keys with the following information:

Feature Type The feature that the licence key enables.

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

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

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



Uploading a Licence Key

To upload a licence key:

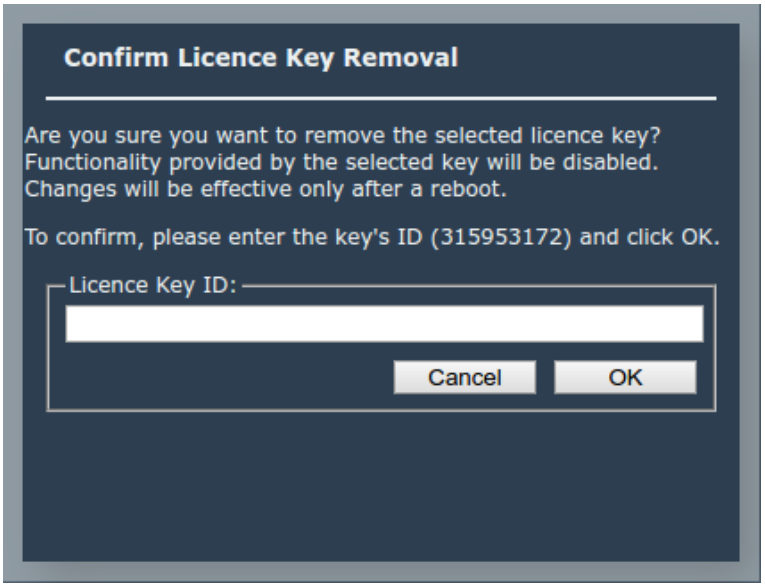
1. Click the *Choose file* button in the *Licence Key Upload* section.
2. Locate and select the licence key to upload.
3. Click the *Upload* button.

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

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

Removing a Licence Key

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



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

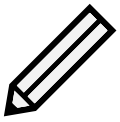
Downloading a Licence Key

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

Diagnostics

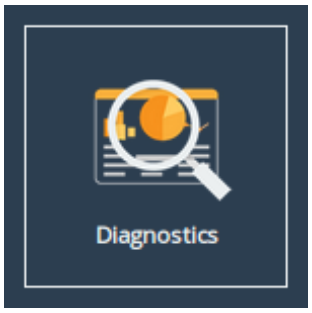
In the unlikely event that a problem arises with your EFC, you may be requested by Bridgeworks Support to provide a diagnostic file.

Important: If an issue arises with your EFC, check Chapter 8: Troubleshooting for information on how the issue may be resolved.

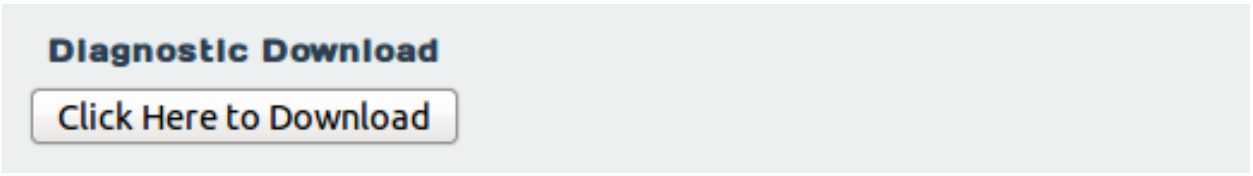


Note: The following instructions are demonstrated in the Bridgeworks Support Video “WANrockIT: Downloading Diagnostic Information” found at https://www.youtube.com/watch?v=8RZXFGCy3ZU.

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



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



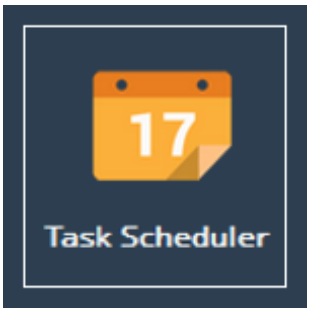
This will cause the EFC to collect data regarding various modules and store them in a single file. Once this process is complete, a download for “diagnostics.bin” will begin.

Task Scheduler

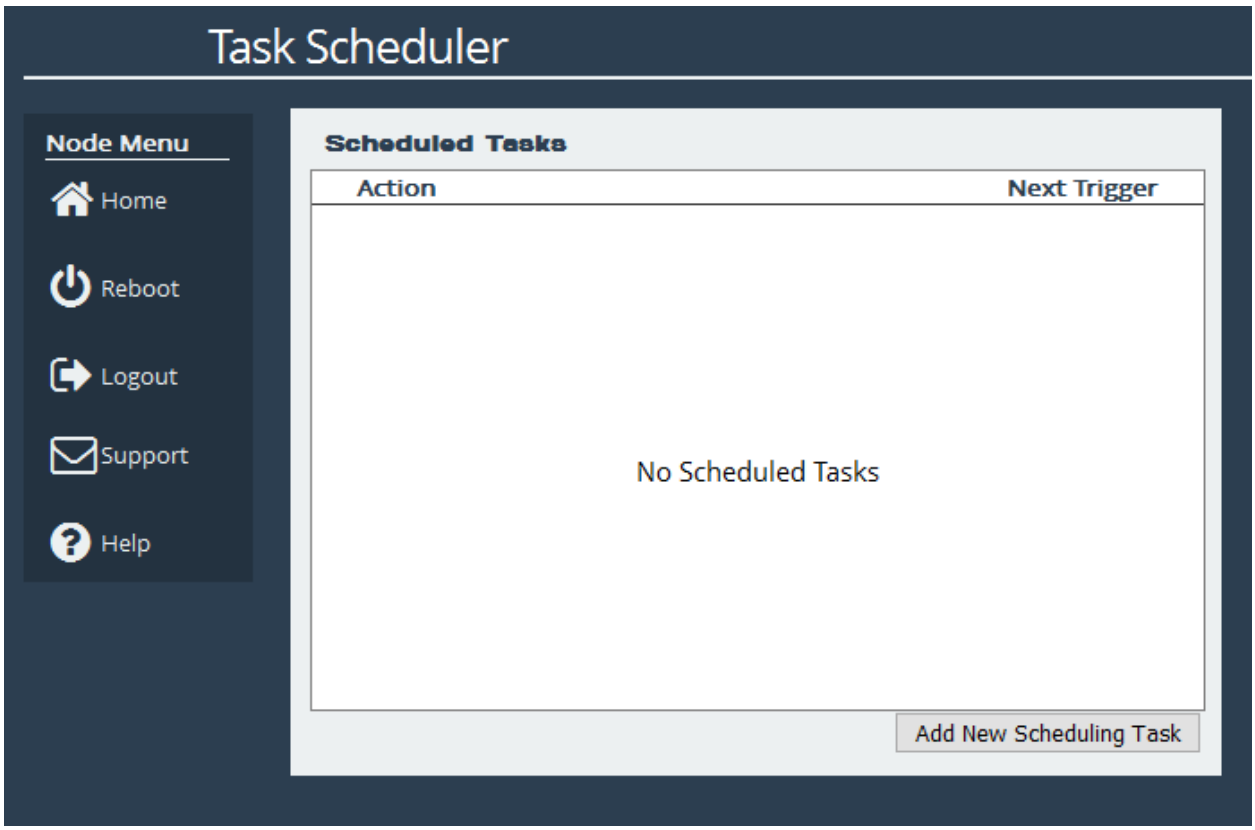
This page allows the administrator to schedule tasks with the following action:

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

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



The web interface will now display the following:

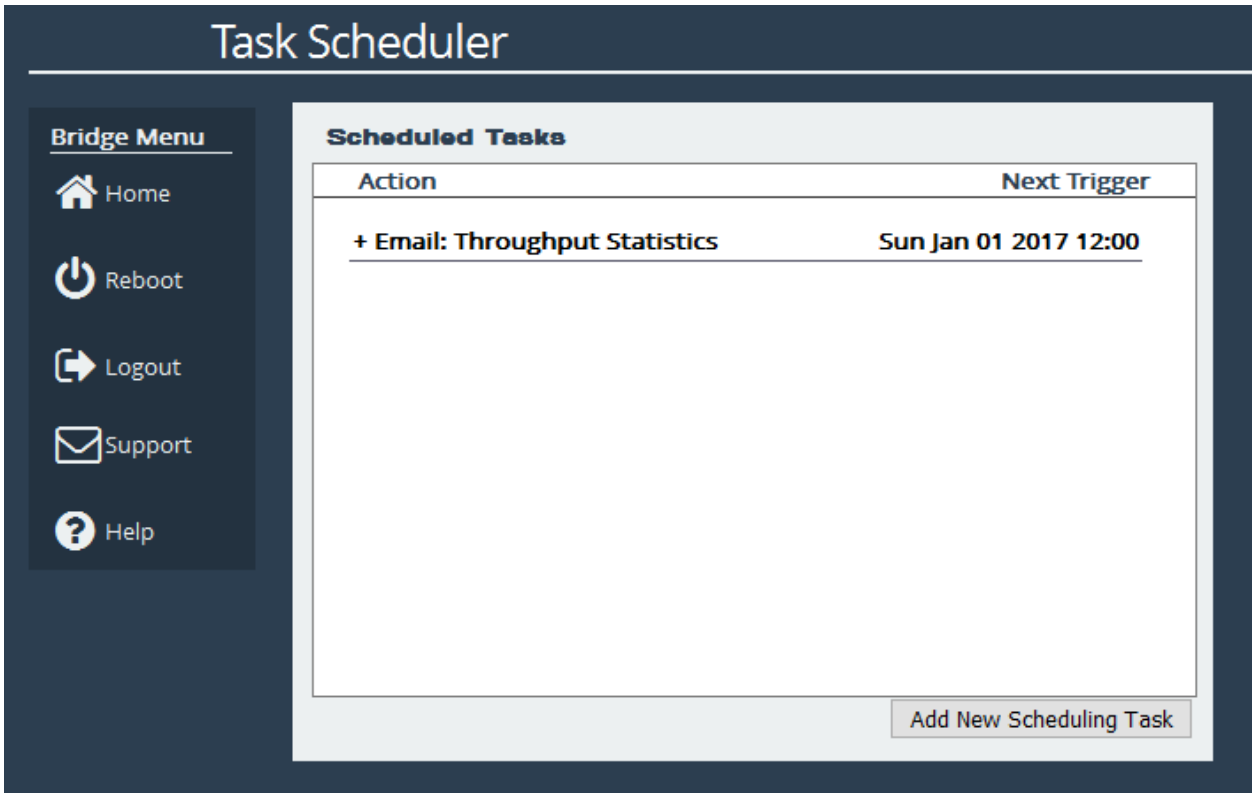


Adding Tasks

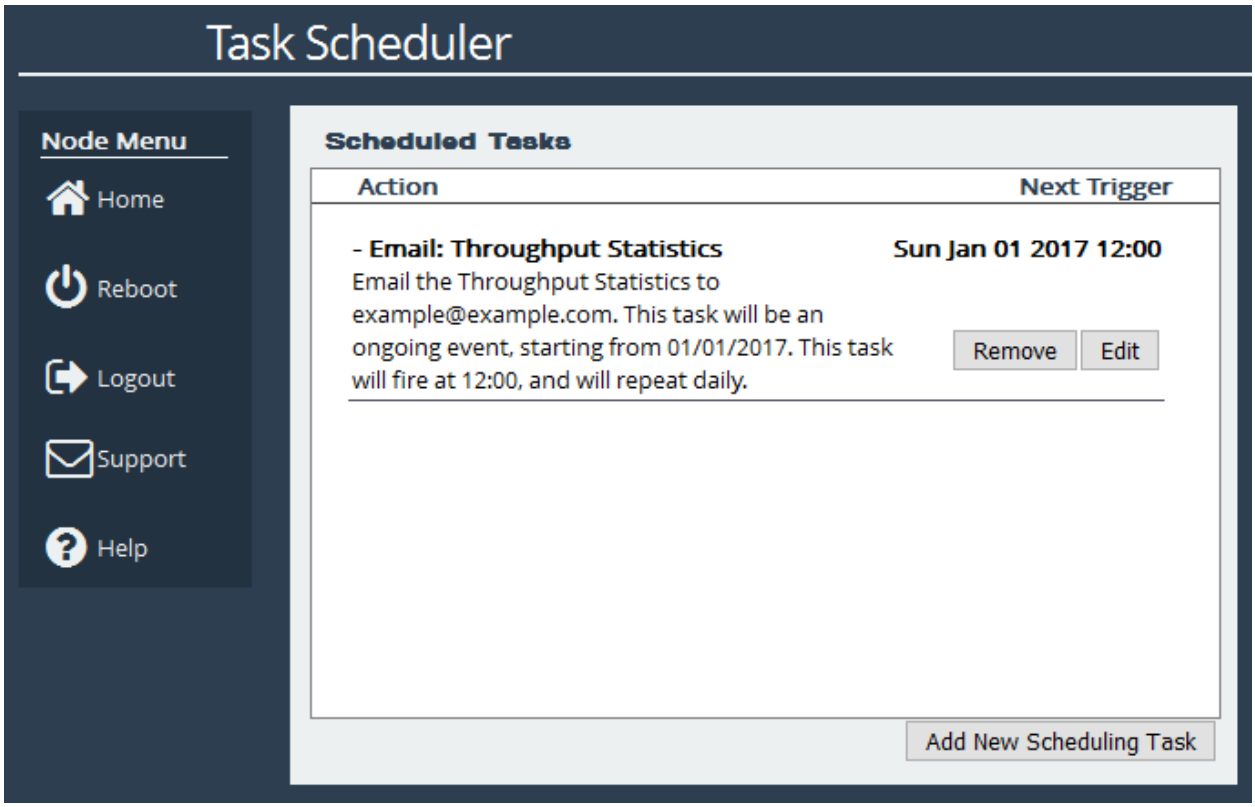
Tasks can be added by clicking on the *Add New Scheduling Task* button, which will start the task wizard.

Removing/Editing Tasks

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



Clicking on a task will expand it as shown:



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

Task Wizard

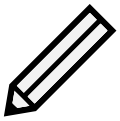
The task wizard will guide you through the adding or editing of scheduled tasks. There are a few common buttons across the individual sections of the wizard:

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

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

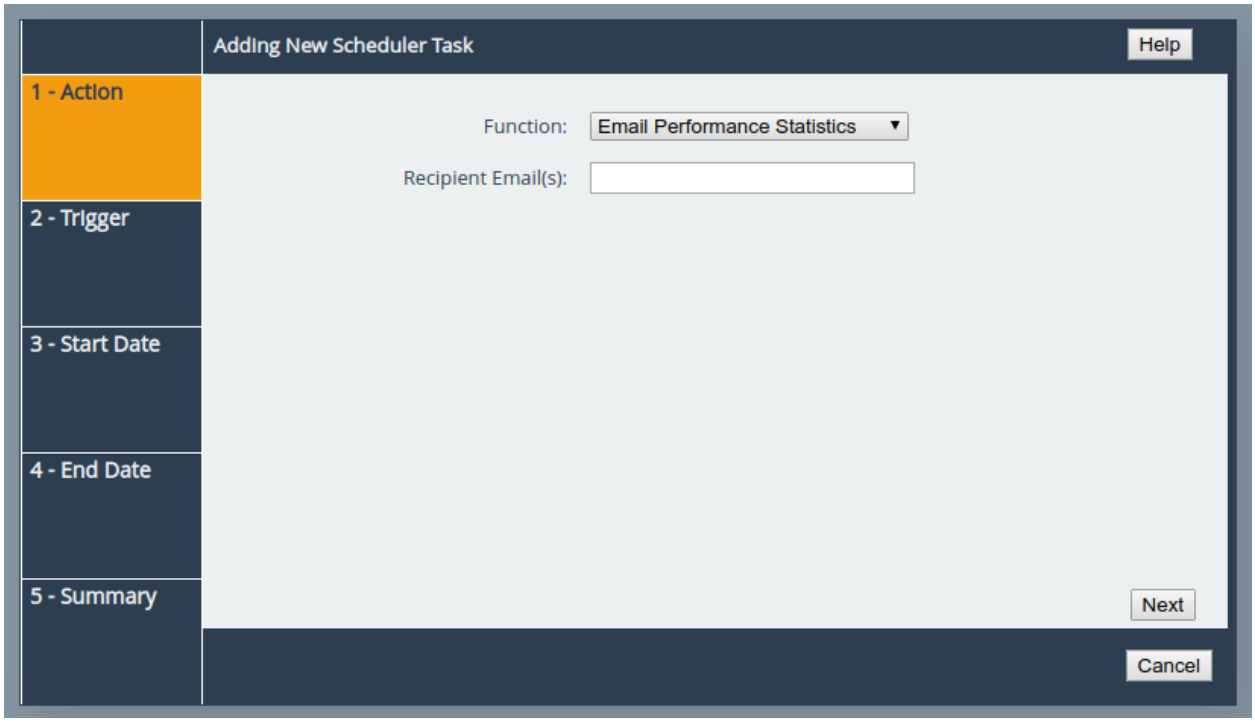
Next If present, this button will navigate you to the next section of the wizard.

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



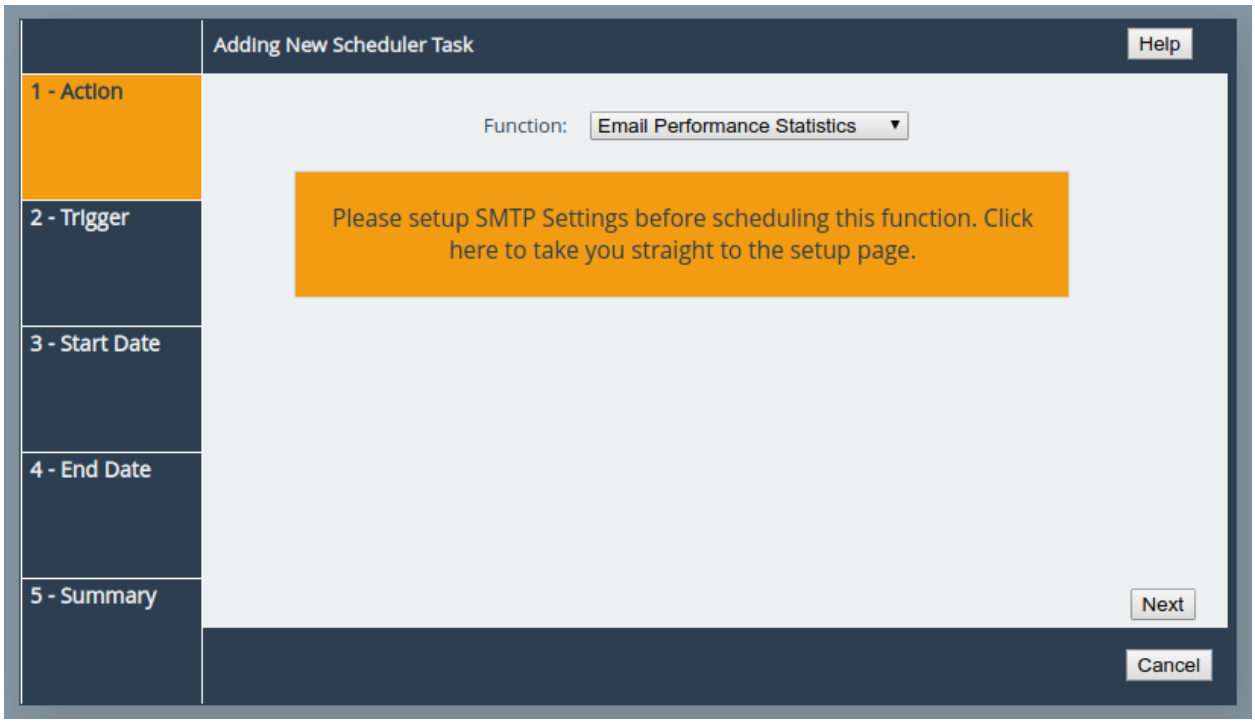
Note: The currently active section of the wizard will be highlighted in orange on the left-hand side.

Action - Email Performance Statistics

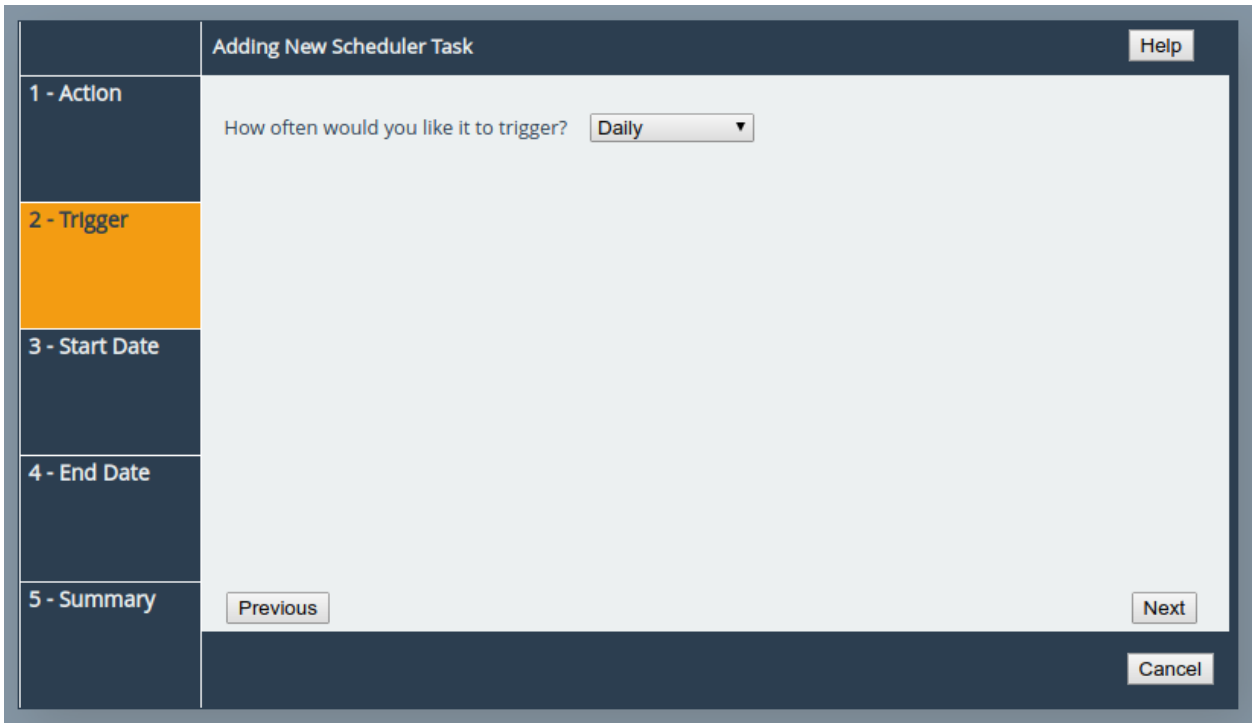


On the Action section of the wizard, enter the recipient email(s), separating multiple emails with either commas or semi-colons.

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



Trigger



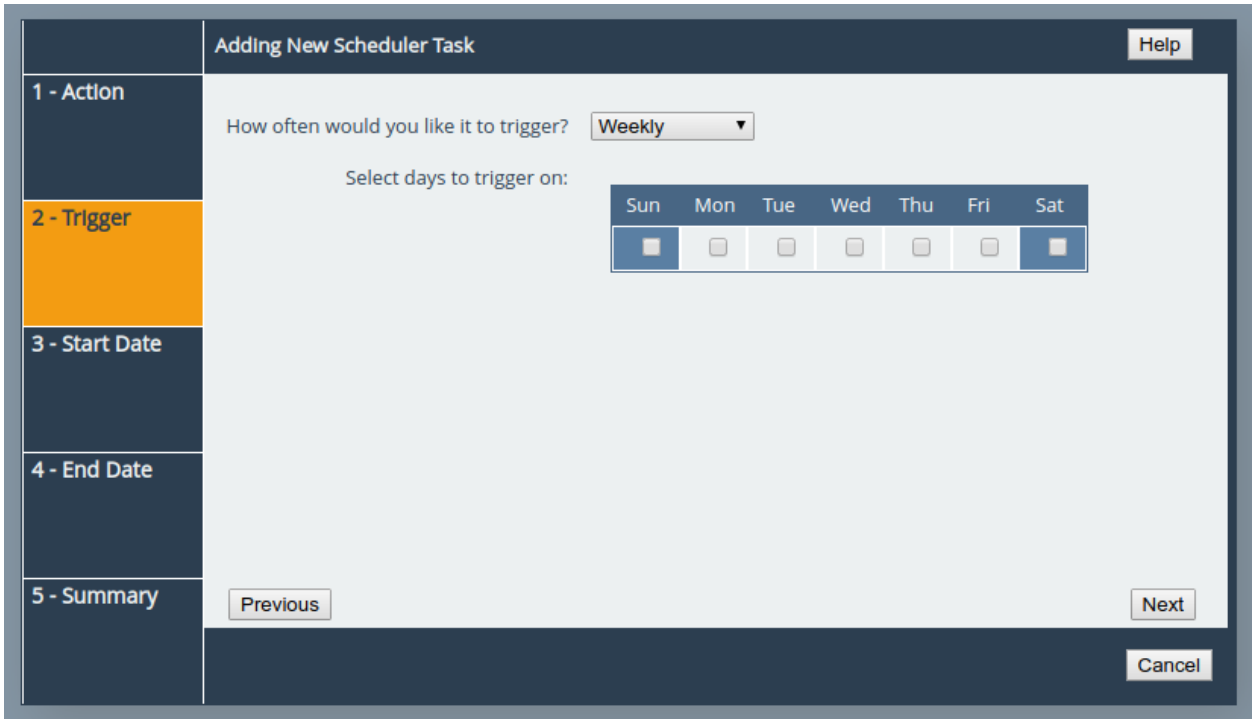
On the Trigger section of the wizard, you can pick the frequency of the event. The options are:

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

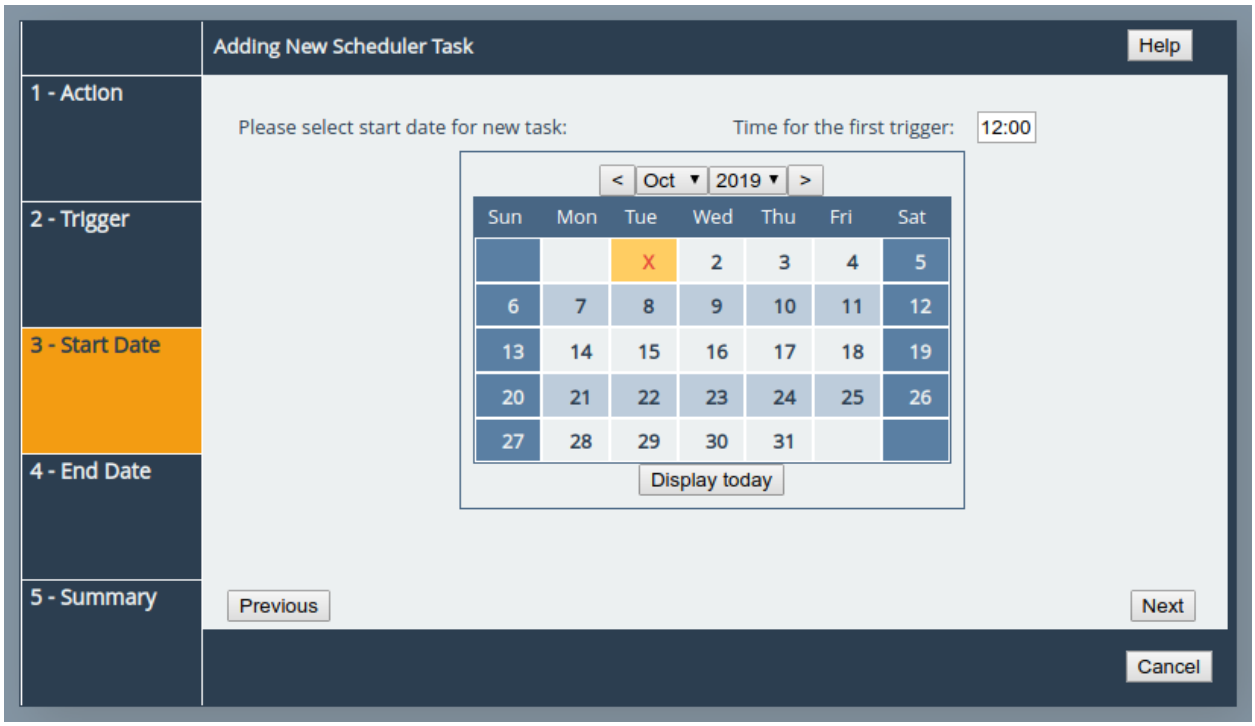
Daily This means the action will be performed every day at the specified time.

Weekly This means the action will be performed on specified days every week at the specified time. When selecting this option, you will be able to pick which days to trigger the action by

selecting checkboxes. Each day will have its own checkbox, as shown:

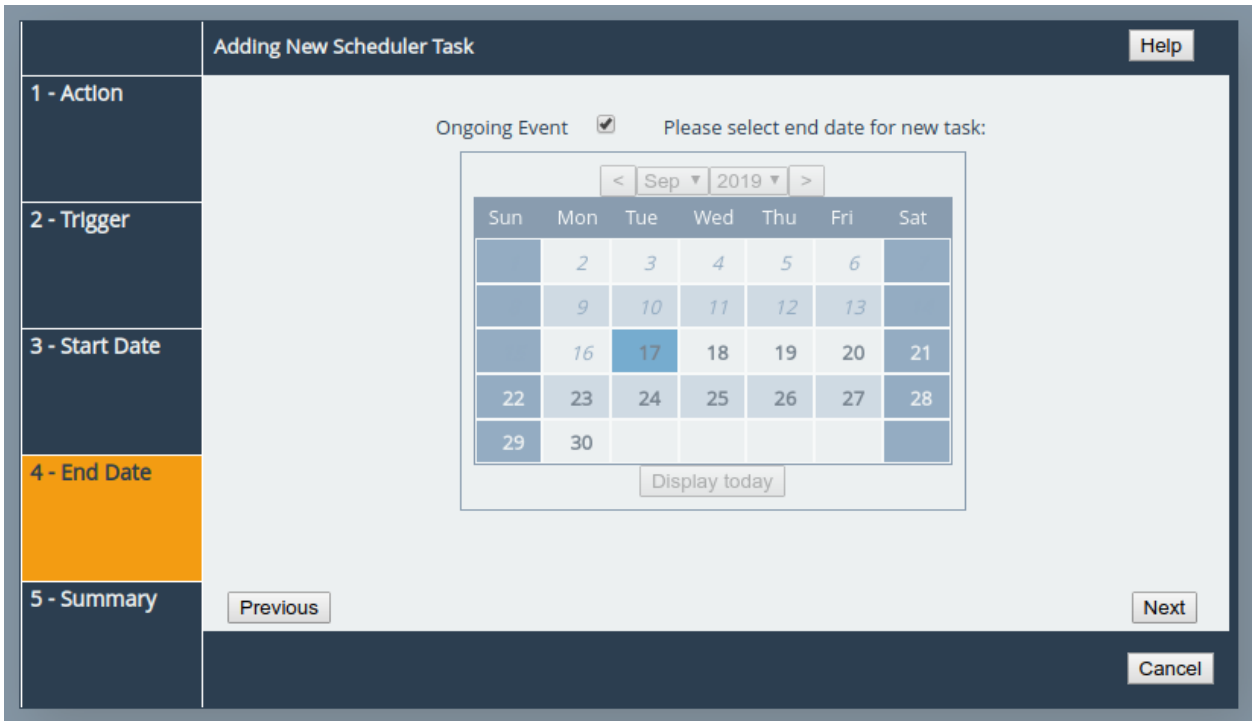


Start Date



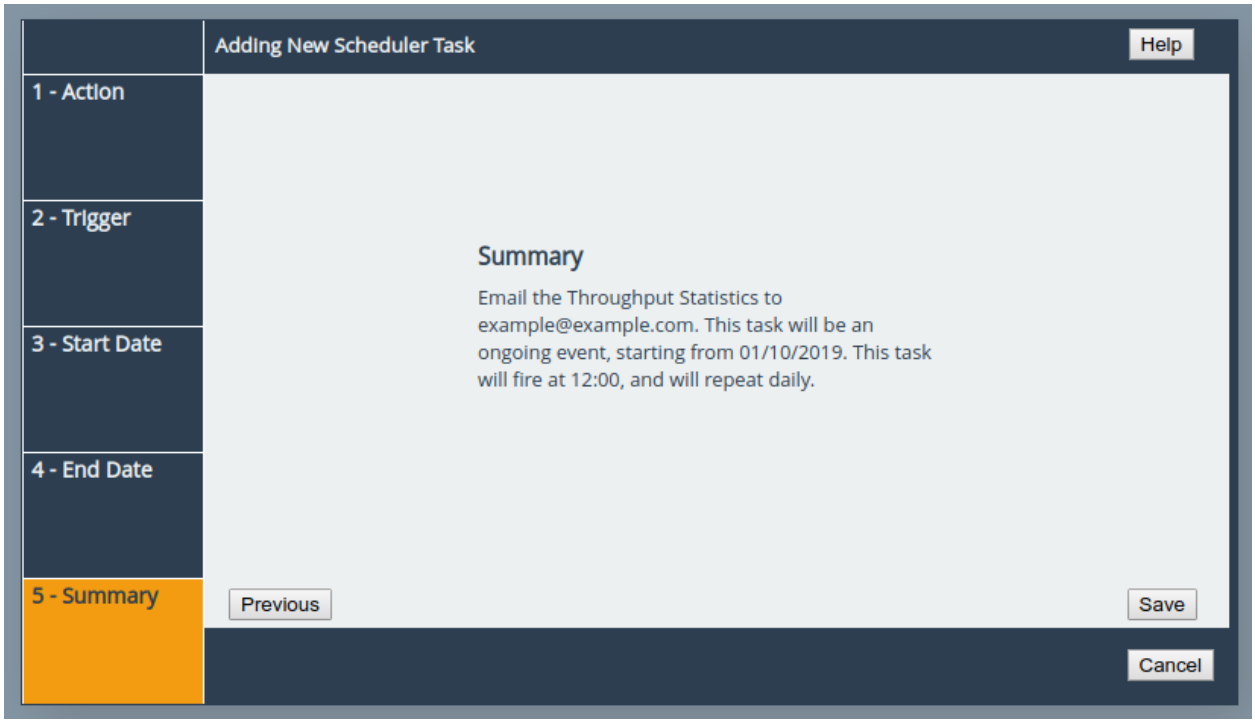
On the Start Date section of the wizard, you can pick the starting date and time for the new task. Enter a time into the *Time for the first trigger* box and select your start date using the calendar. The selected date will be marked with a red cross.

End Date



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

Summary



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

Troubleshooting

Network Connectivity Problems

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

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

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

SCSI Device Related Problems

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

- Ensure that the devices are powered on and are ready - some libraries can take 5 minutes or more before they are ready and appear on the Gateway. The power up status of libraries are usually displayed on the front panel.
- Ensure that the cables between the Gateway and the devices are connected.

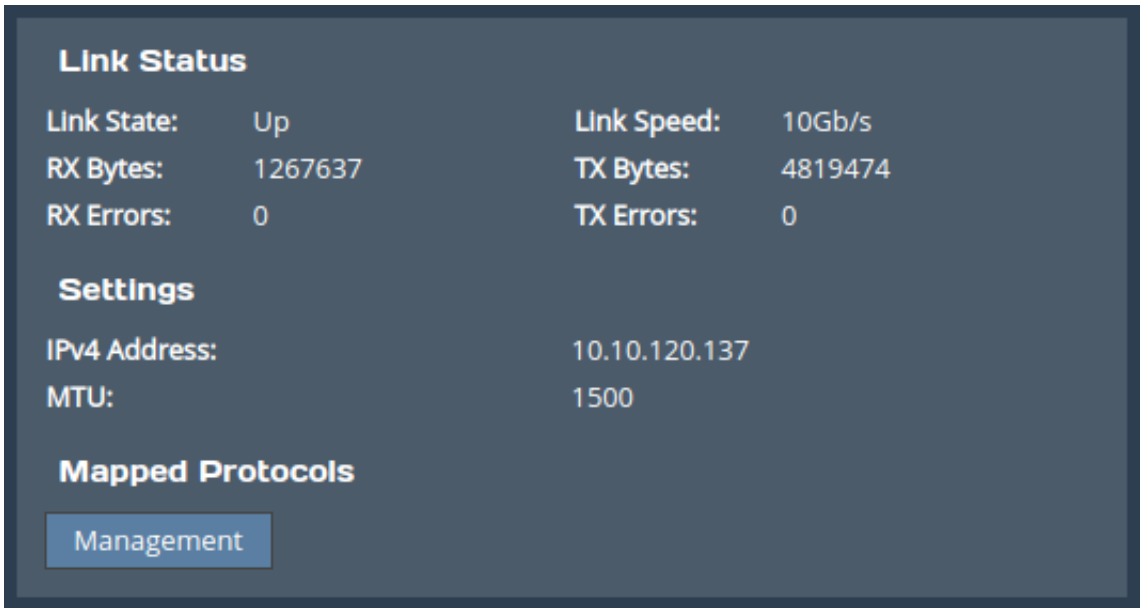
- Connect to the Gateway via the web interface and check that devices are present on the *Local Device Management* page, and that they are enabled. See Section 6.2: Viewing Device Mappings for checking device information.
- Ensure that the CHAP settings for the initiator and the Gateway are the same.
- Force a rediscovery from the initiating iSCSI host.
- Reboot the devices and the Gateway.

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

Network Performance Problems

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

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



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

iSCSI Performance Problems

Poor iSCSI performance can be caused by many differing reasons. The following list is provided as a guide to where you may find ways to improve performance in addition to those found in Section 8.3: Network Performance Problems.

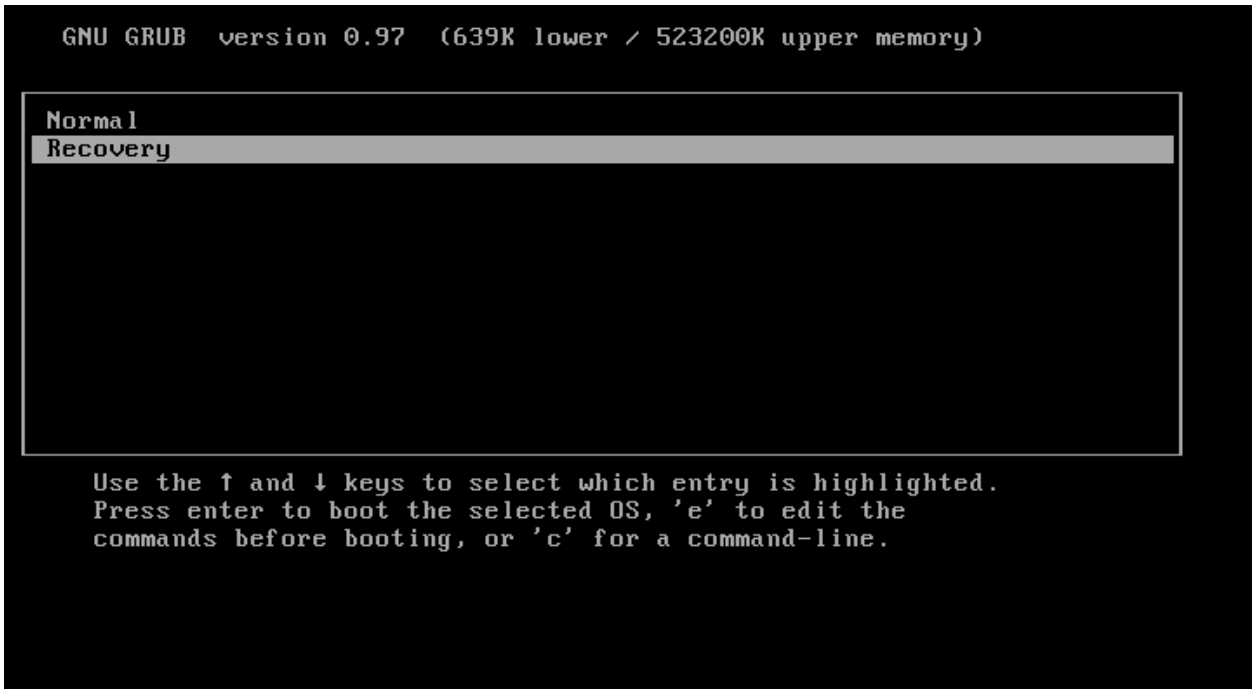
- *Data Digests* are an extra level of error checking on top of the standard TCP/IP checksum error checking (configured on the initiator). However, the calculation of these extra checksums can greatly affect overall performance. Therefore, *Header and Data Digests* should only be enabled where the integrity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

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

Recovery Wizard

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

To access the Recovery Wizard press the *Esc* key while the unit is booting. Select the *Recovery* option on the menu provided.

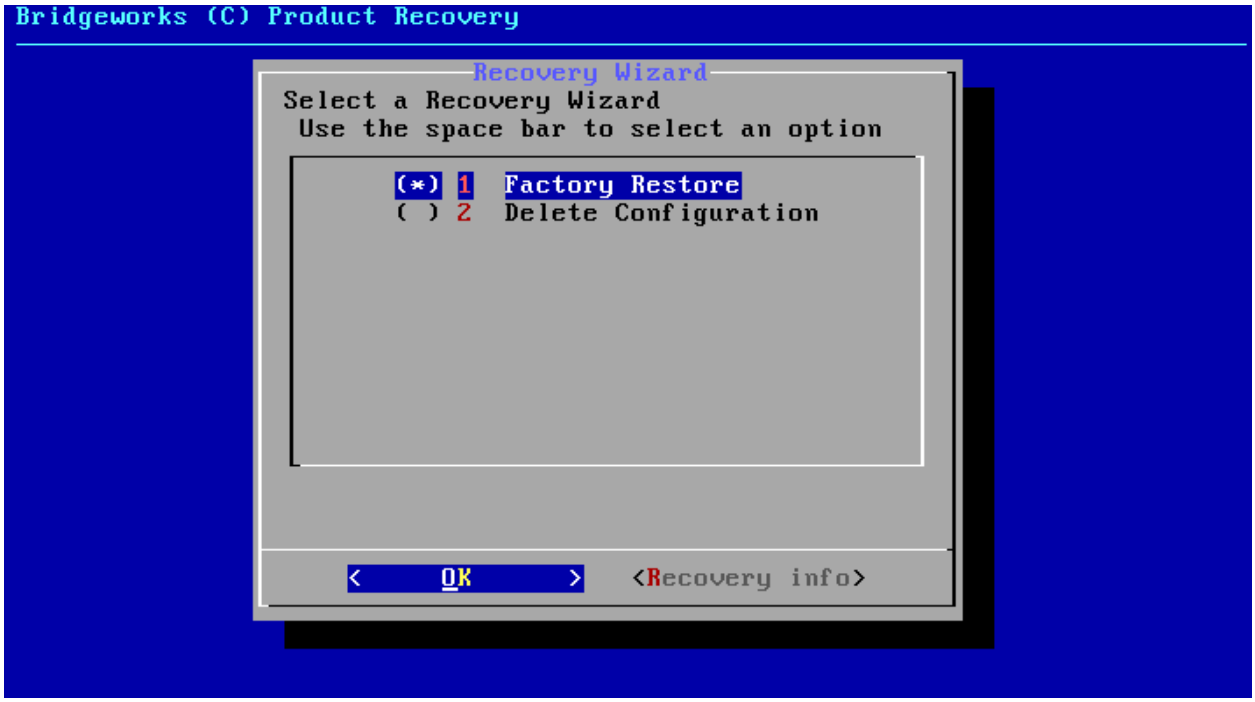


The Recovery Wizard provides two options for system recovery: restoring your unit to factory defaults, and deleting your configuration file.

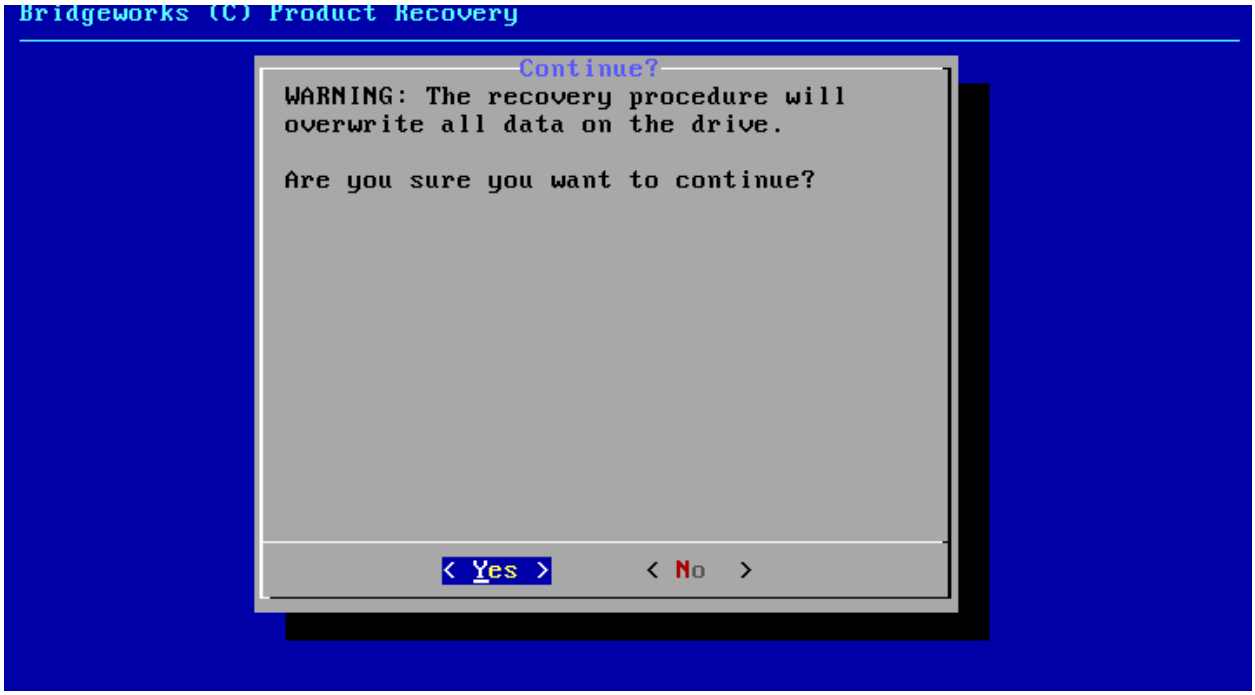
Factory Restore

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

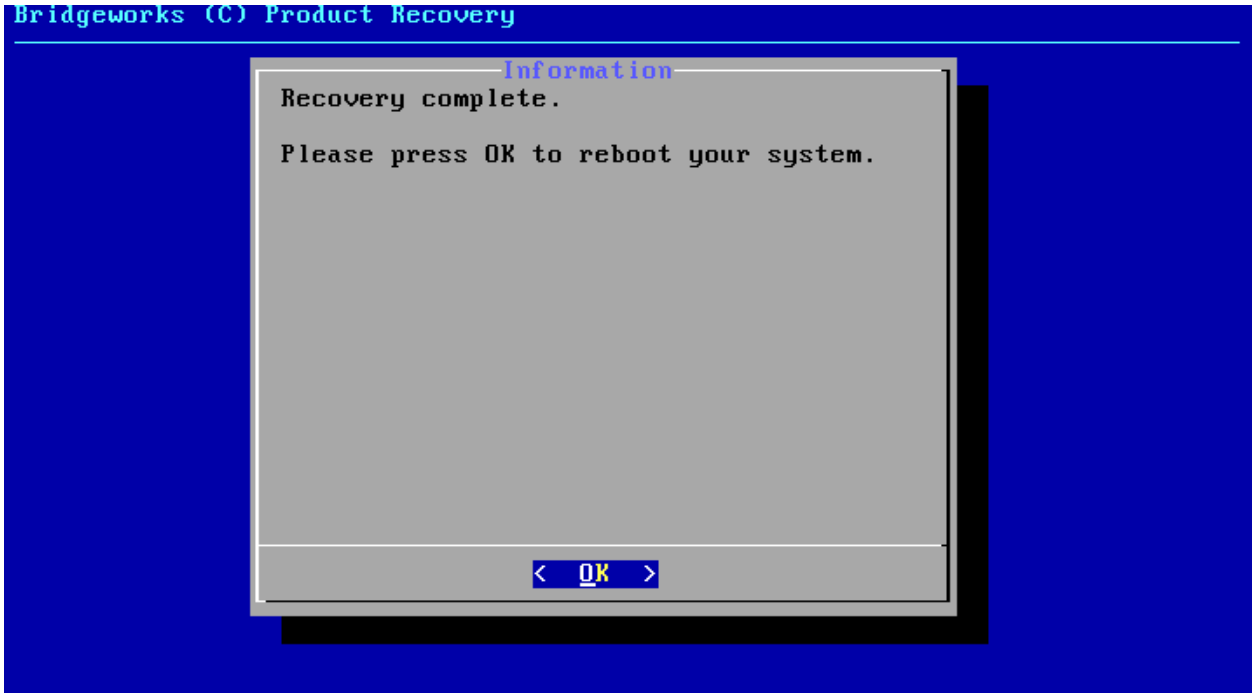
To restore your unit to defaults, ensure that the *Factory Restore* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the factory restore process.



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



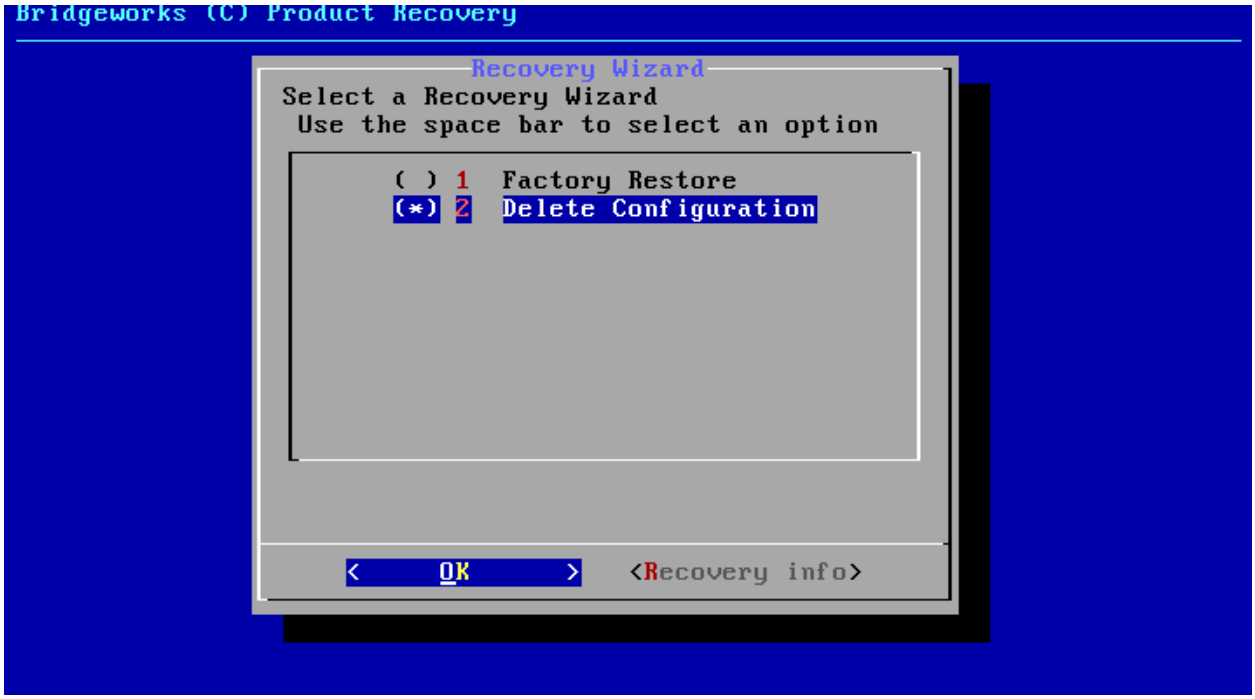
Once the factory restore procedure has completed successfully you will need to reboot your system.



Delete Configuration

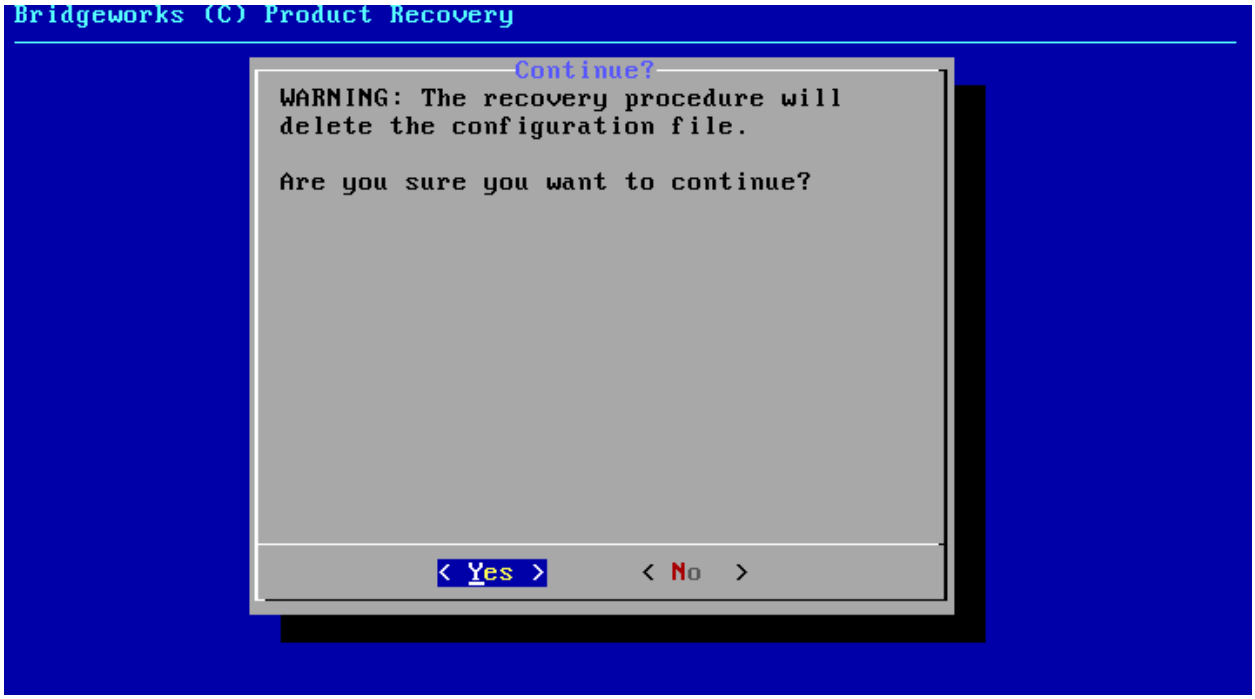
This option will delete your configuration file, removing any current configuration on your system but keeping your current firmware and licence keys.

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

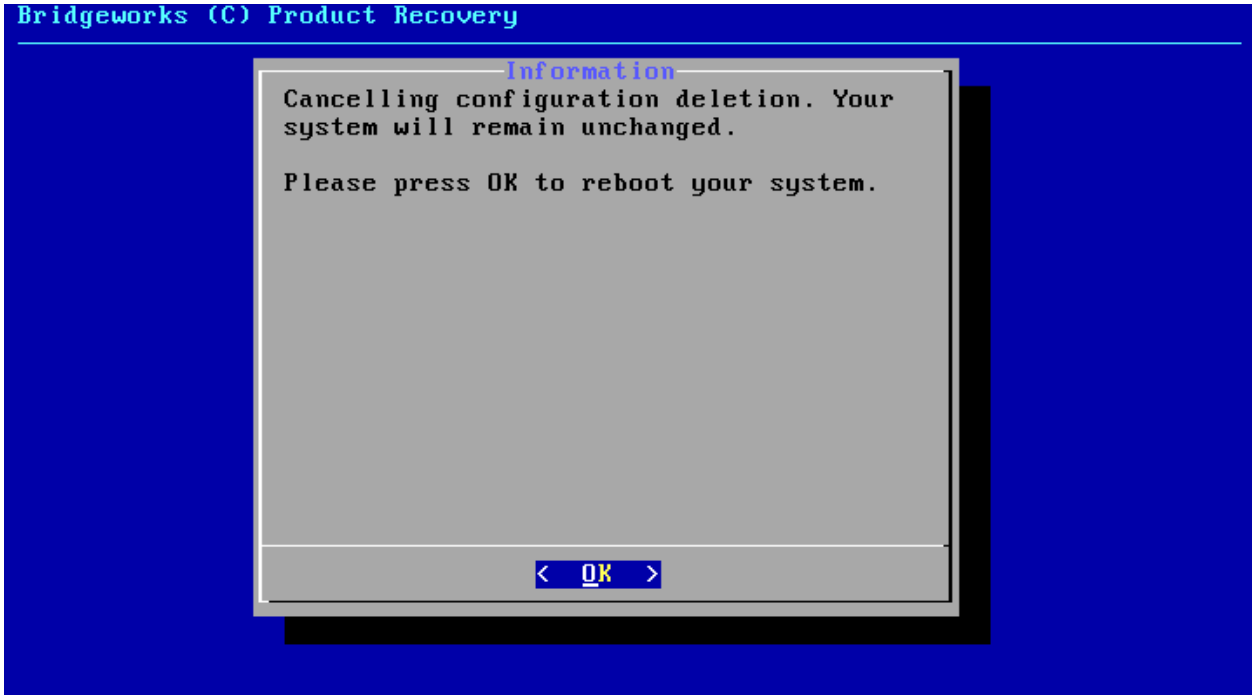


This procedure cannot be undone once complete; only continue if you are sure that you wish

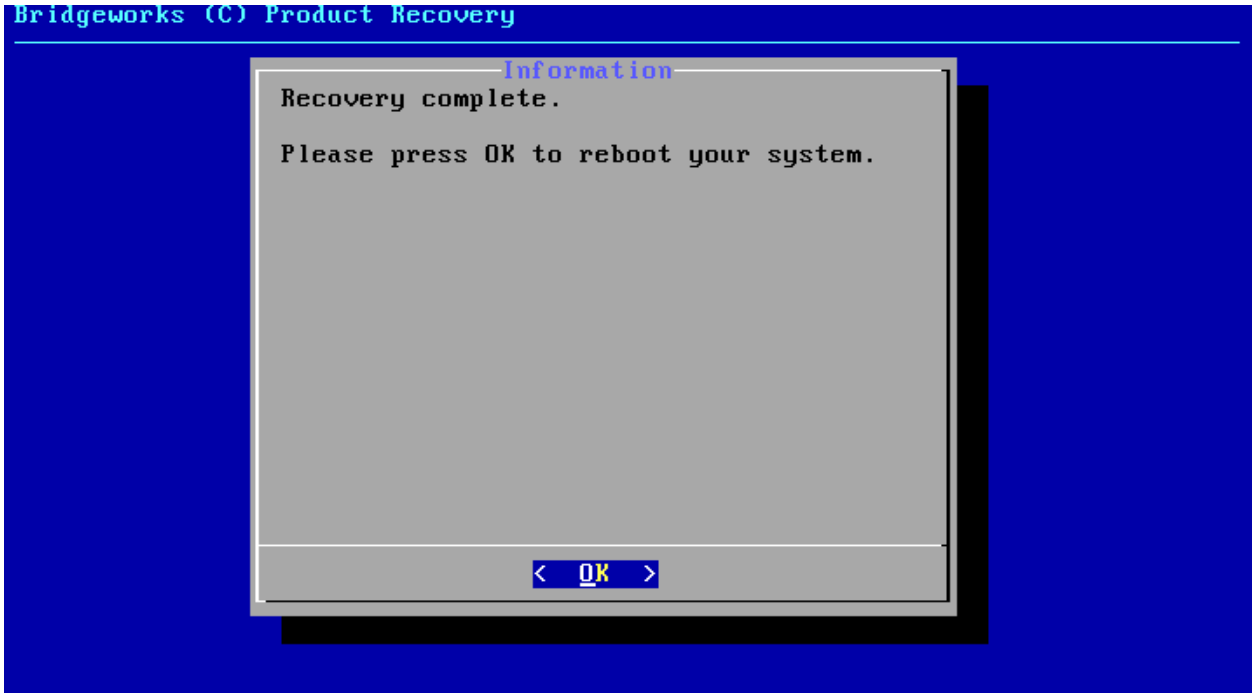
to do so. You will be asked to confirm that you wish to proceed. Choosing *Yes* will delete your configuration file and *No* will cancel the configuration deletion wizard.



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



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



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

IP Protocols and Port Numbers

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

Inbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 22	SSH	Required to access the configuration console through management interfaces when SSH is enabled. See Section 3.2.4: Secure Shell (SSH).
TCP 80	HTTP	Required to access the web interface through management interfaces when HTTP is enabled.
TCP 443	HTTPS	Required to access the web interface through management interfaces when HTTPS is enabled.
TCP 860/3260	iSCSI	The iSCSI Target can be configured to use one or both ports. See Chapter 5: iSCSI Target Configuration.
UDP 161	SNMP	Required for management interfaces to respond to Simple Network Management Protocol requests, see Section 3.3.2: SNMP Agent.

Outbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 25	SMTP	Simple Mail Transfer Protocol, see Section 3.3.3: Simple Mail Transfer Protocol (SMTP).
TCP 3205	iSNS	Internet Storage Name Service protocol, see Section 3.3.5: Internet Storage Name Service (iSNS).
UDP 123	NTP	Network Time Protocol, see Section 3.3.1: Simple Network Time Protocol.
ICMP		Internet Control Message Protocol. Required by dead gateway detection (see Section 3.1.2.4: Dead Gateway Detection) and network debugging tools (see Section 3.1.5: Network Tools).

Accessing the Gateway from Windows using a static IP Address

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

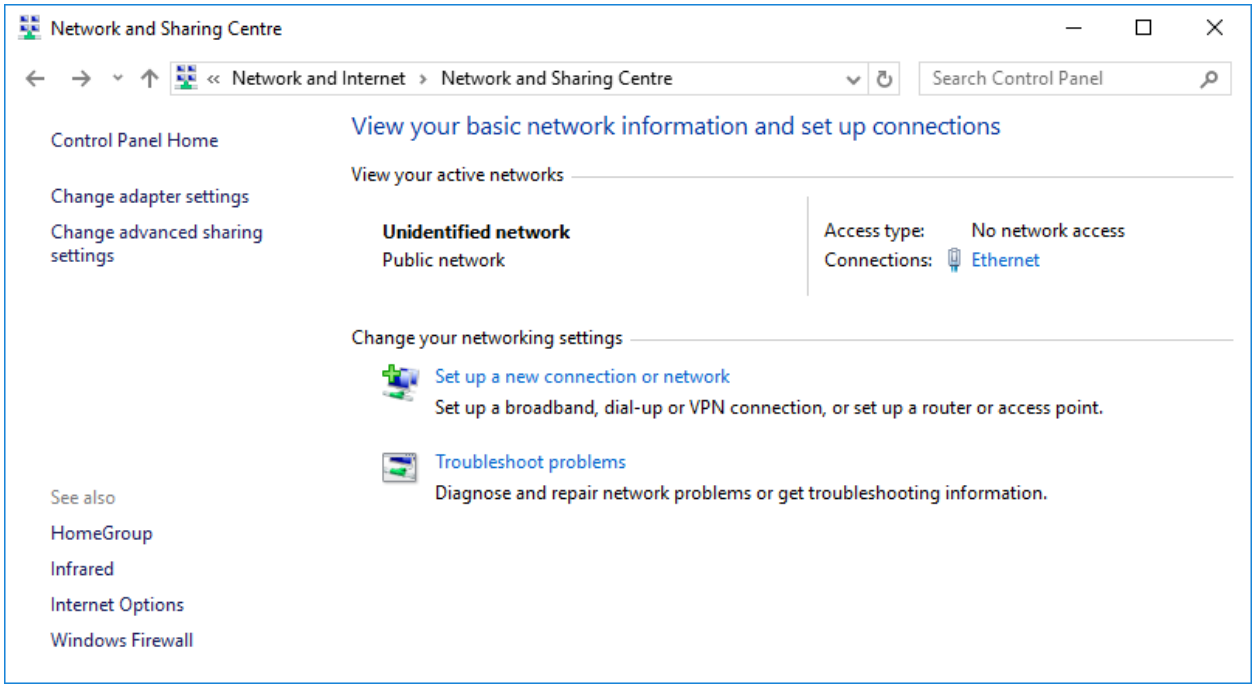
These instructions apply to Windows Vista, 7, 8, 10 and to Windows Server 2008, 2012, 2016, and their respective R2 versions.

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

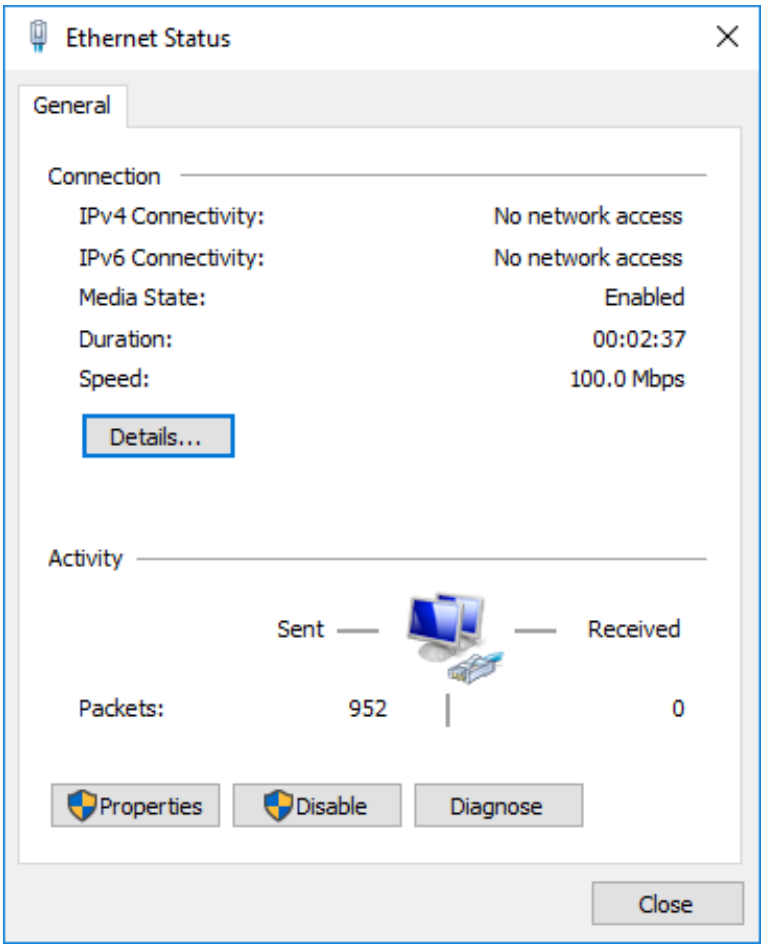
From the Start menu, select *Control Panel*.

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

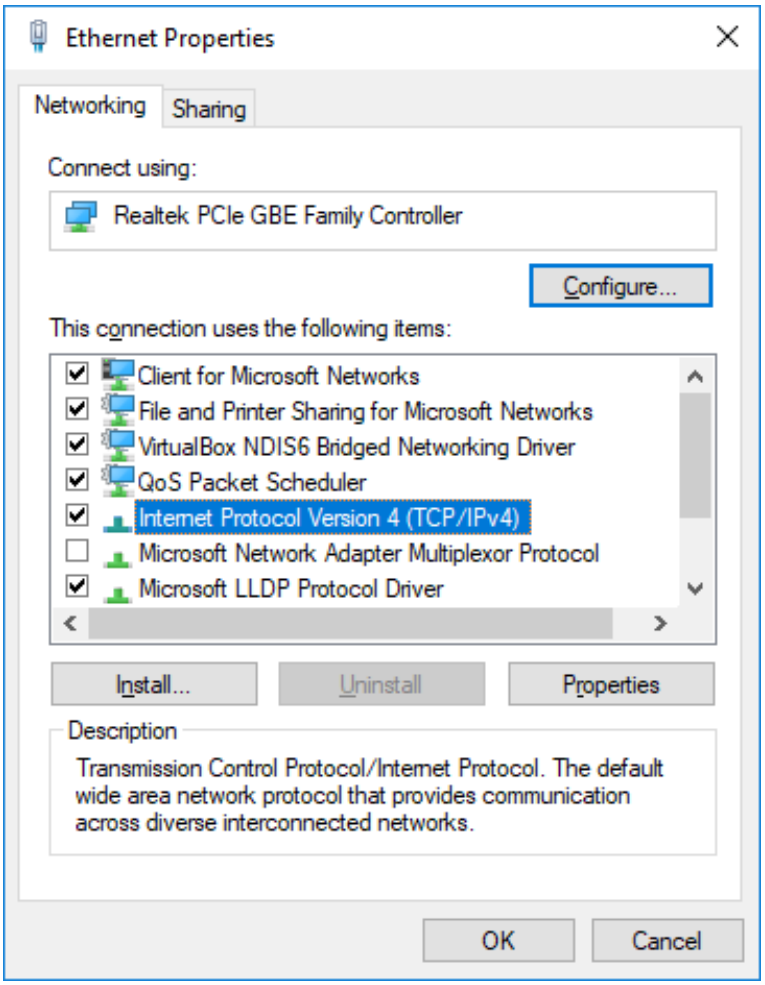
From the Control Panel select the *Network and Internet* link, followed by the *Network and Sharing Centre* link. Click on the link next to "Connections" for your respective network. This is named "Ethernet" in the screenshot below.



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

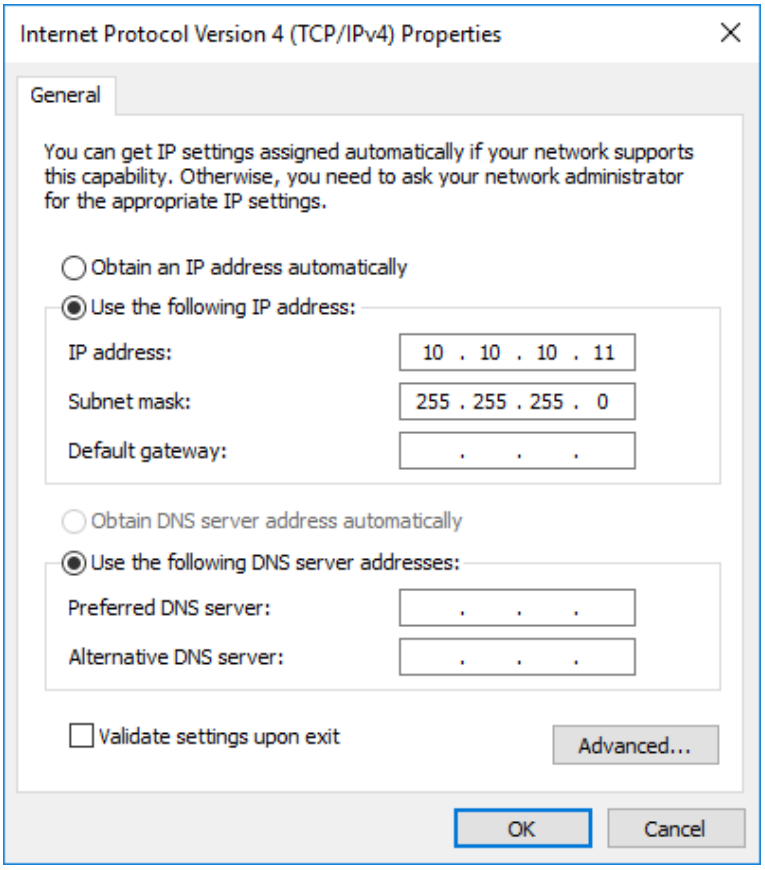


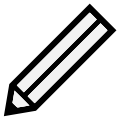
Select the *Internet Protocol Version 4 (TCP/IPv4)* entry and then *Properties*.



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

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





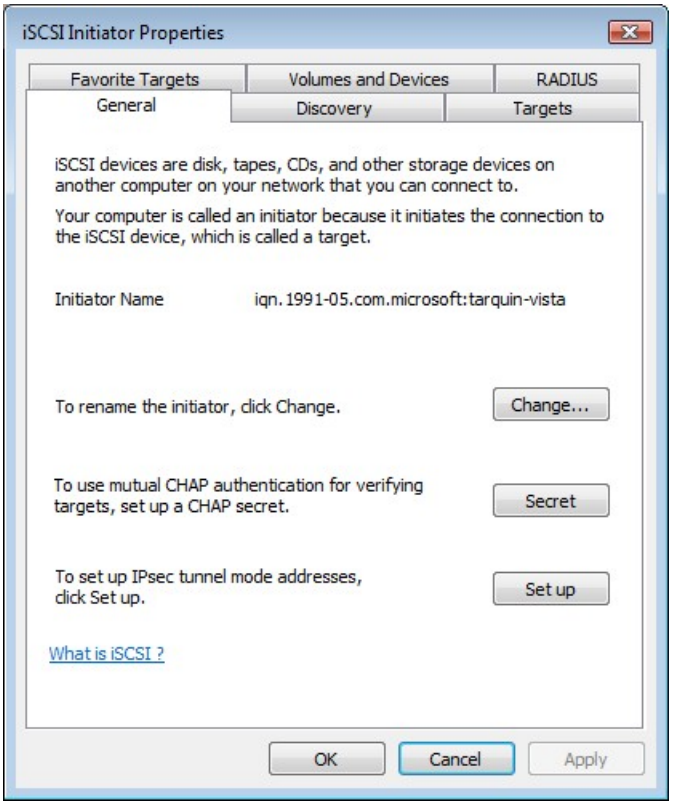
Note: Once you have completed the initial set up of the Gateway, return your computer to the original settings and reconnect to the Gateway.

Connecting to an iSCSI Device using the Microsoft iSCSI Initiator

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

General Set up

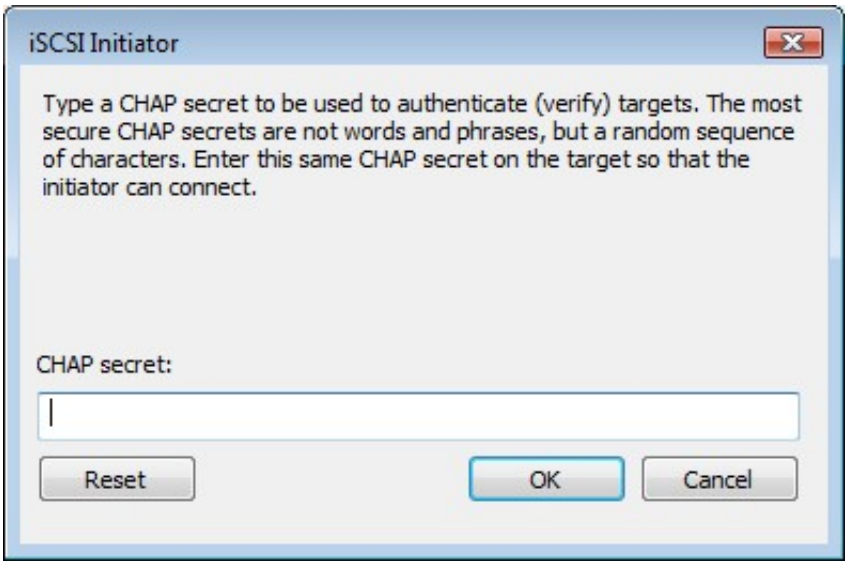
Open the iSCSI initiator and then click on the *General* tab. You should see the following page:



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

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

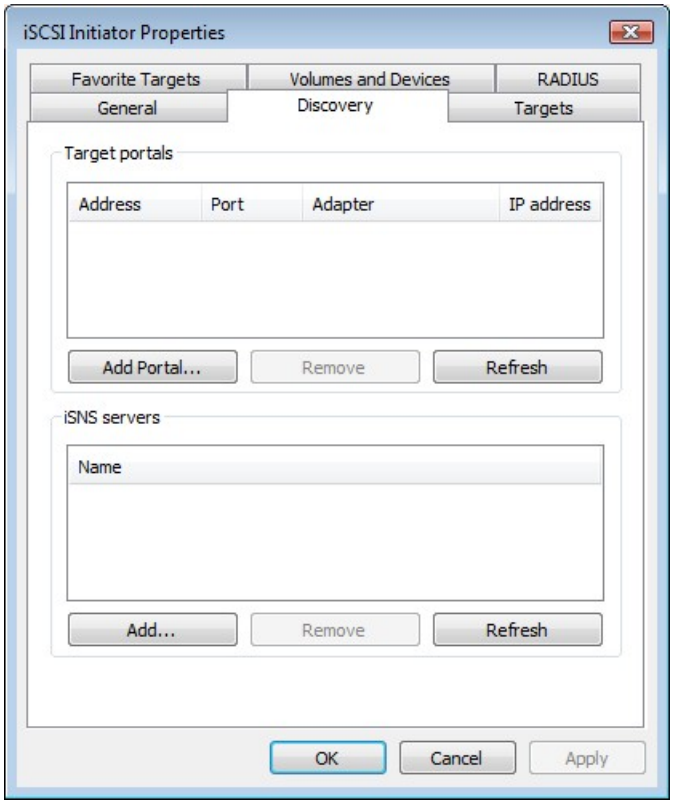
Click on the *Secret* button and the following window should be displayed:



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

Discovery of Devices

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

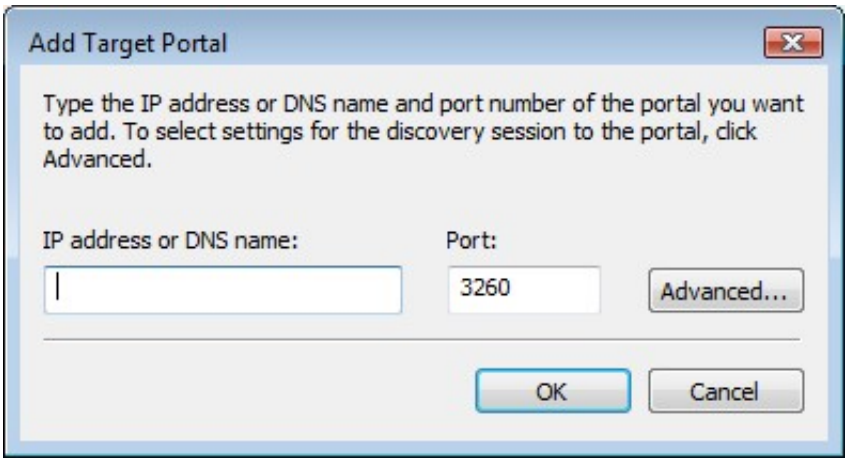


Devices can be discovered in one of two ways:

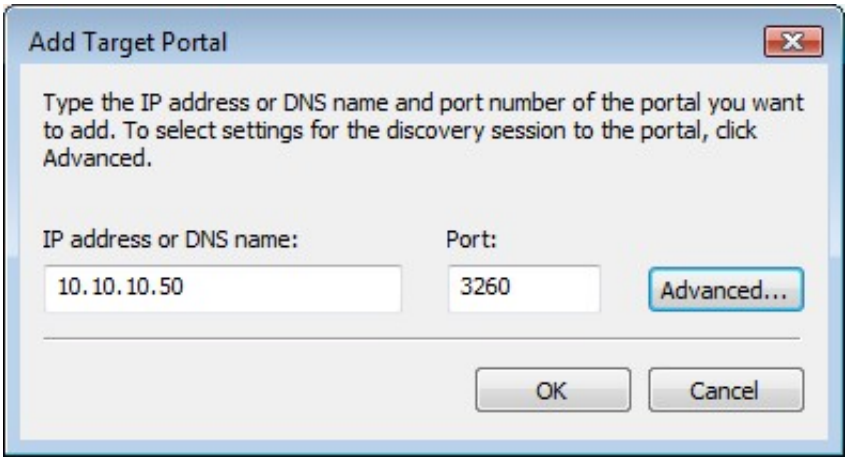
- Adding an iSCSI target portal and directly performing a discovery;
- Adding an iSNS server to which the target portal is registered.

Adding an iSCSI Target Portal

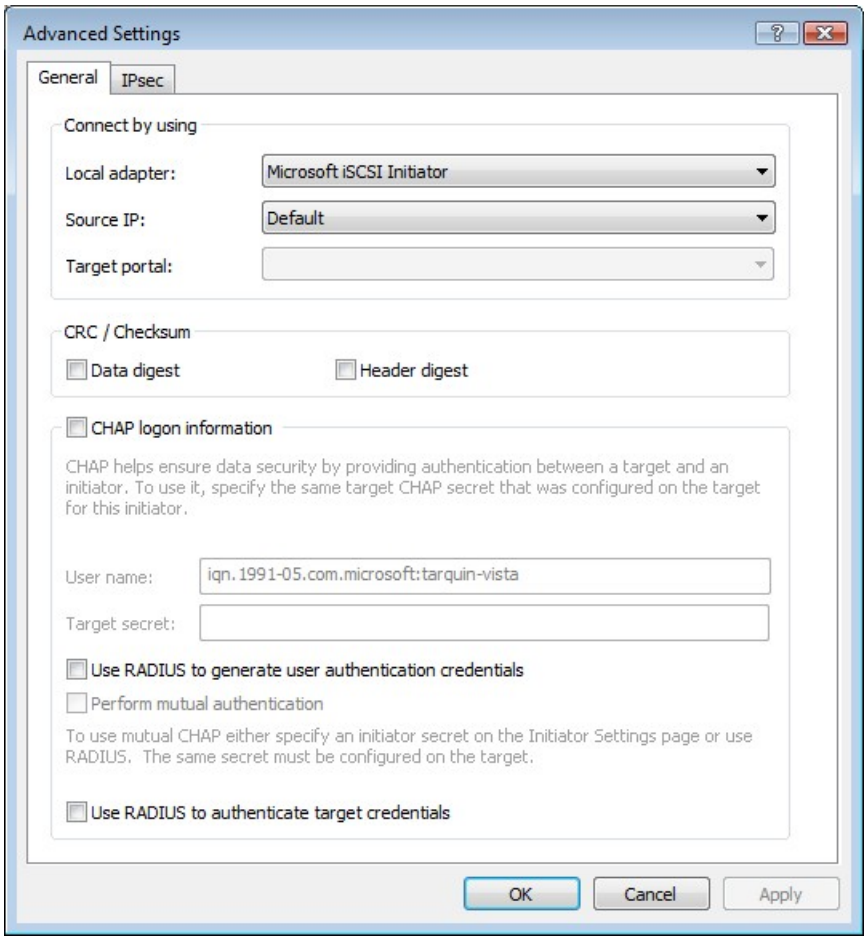
To add an iSCSI Target portal, click on *Add Portal*. You should now be presented with the following window:



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

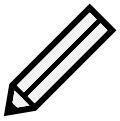


Leave the port at 3260 unless you have configured your iSCSI Gateway to only respond on port 860, in which case change it to 860. Click on the *Advanced* button to see the advanced options.



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

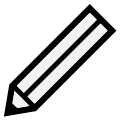
The *Source IP* is used to specify upon which network adapter the discovery will be done. In most cases you will want to leave this as default. If multiple network interfaces are installed in the Server and you wish to select a particular interface, select the IP address of that network interface from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

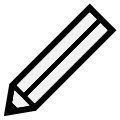


Note: You may need to select a specific local adapter in order to chose certain source IP addresses.

CRC/Checksum settings allow you to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

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

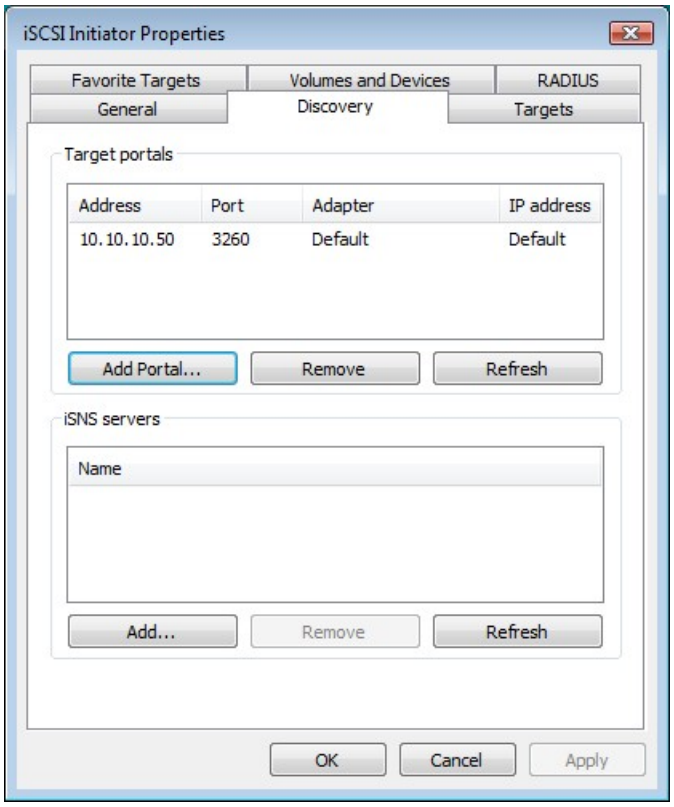
	Note: For mutual CHAP to be performed, the *Initiator Secret* must be set on the general tab, and be the same as the one configured on the iSCSI Gateway.

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

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

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

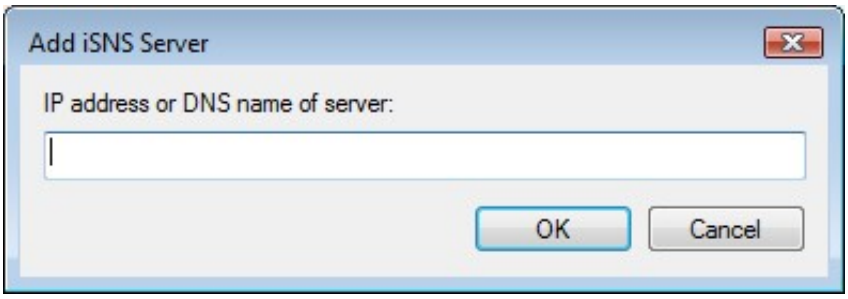
Once the discovery is complete, you should see the target listed in the *Target Portals* list:



Adding an iSNS Server

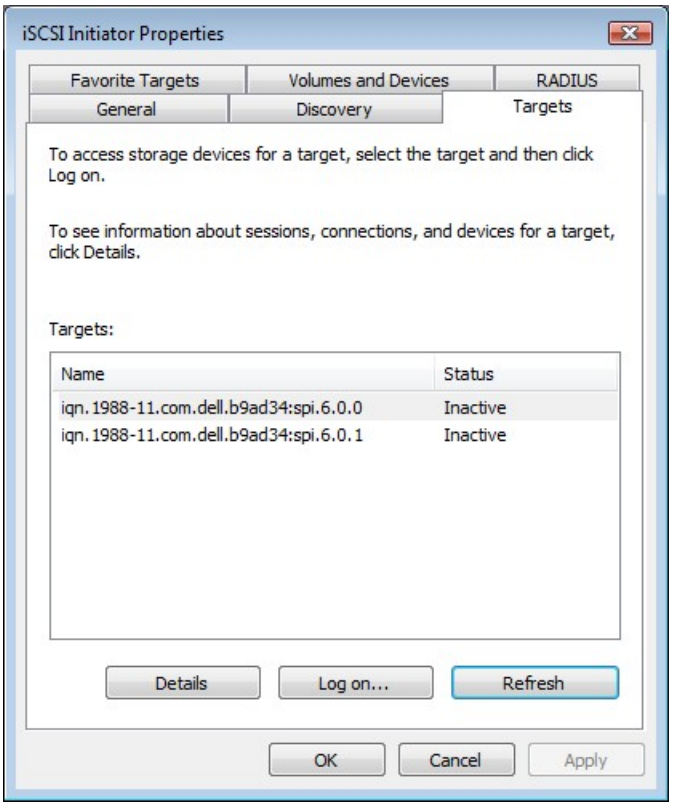
To discover iSCSI targets using this method, your iSCSI Gateway must be registered with your designated iSNS server. See Section 3.3.5: Internet Storage Name Service (iSNS) for more information.

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



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

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

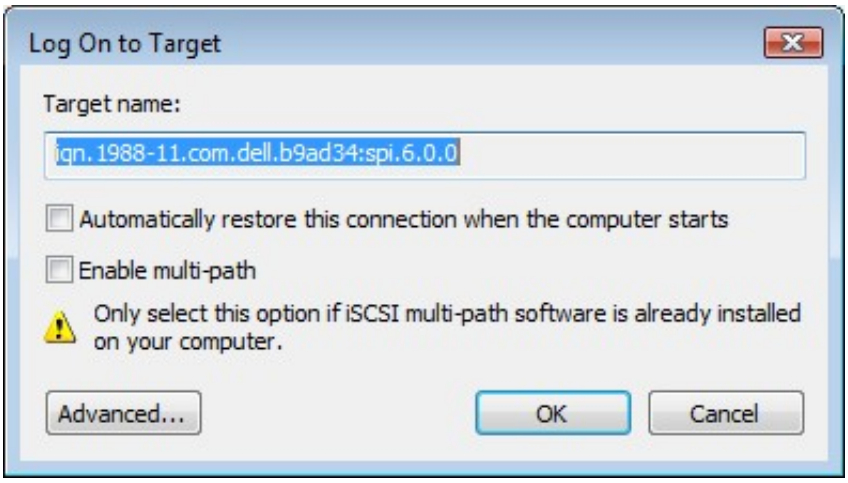


In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check that the settings used to perform the discovery, including CHAP settings, are correct. Then return to *Targets* tab and click *Refresh*.

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

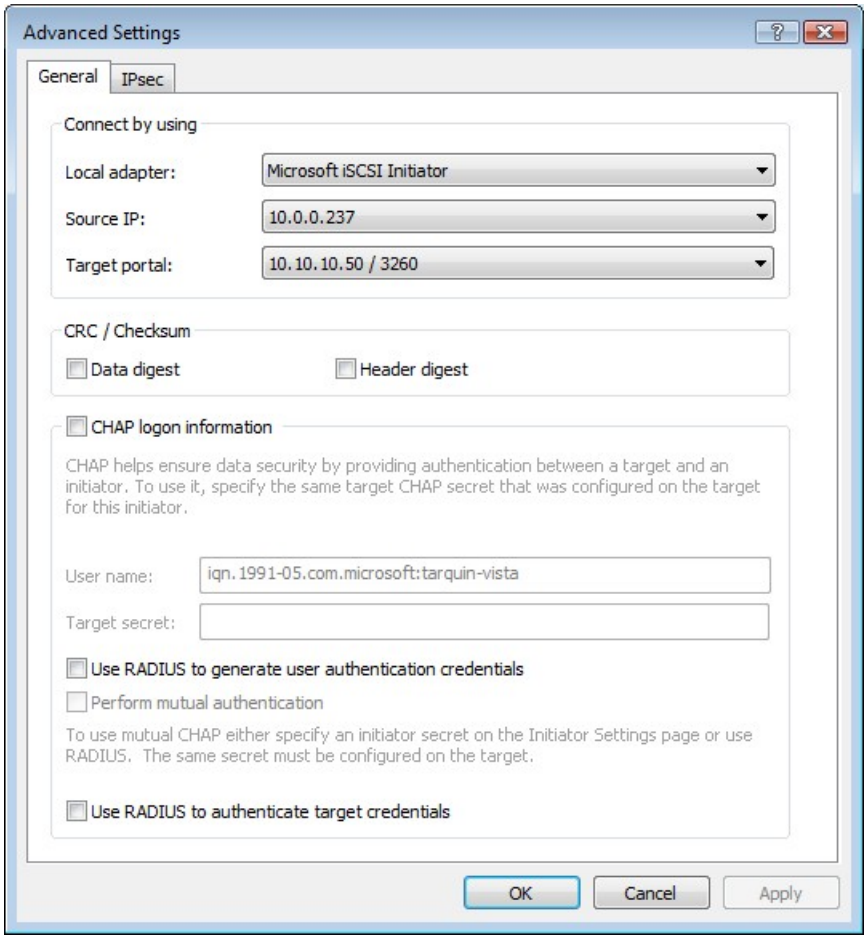
Connecting to a Target

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



If you wish to reconnect to the target automatically when this Windows server reboots, select the *Automatically restore this connection when the computer starts* checkbox.

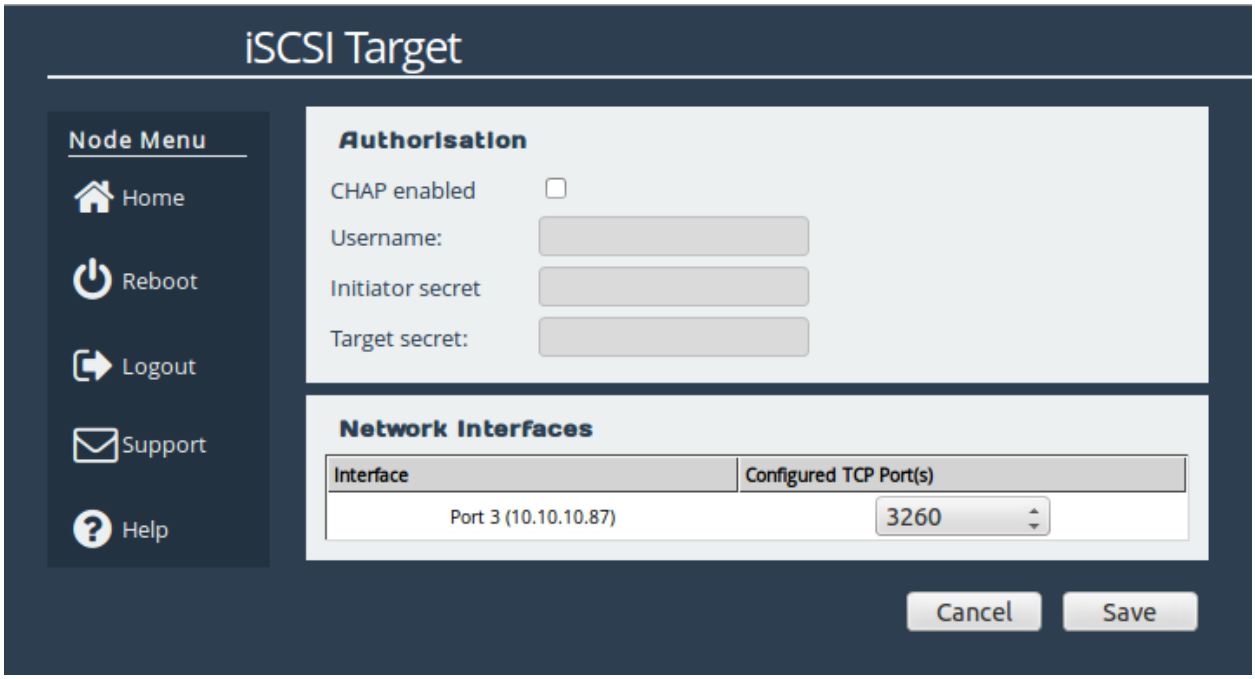
Click on the *Advanced* button to see the advanced settings. The following window should appear:



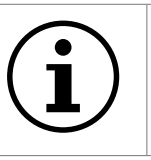
The Advanced Settings page is the same as that of the discovery except for one addition. In the *Connect by using* section, there is a *Target portal* option. This allows you to choose which interface of the iSCSI Gateway will be used to make the connection to the target. In this example we have chosen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

To see how this relates to the iSCSI Gateway configuration, note the IP addresses in the Network

Interfaces subsection, on the iSCSI Target page of the iSCSI Gateway's web interface:



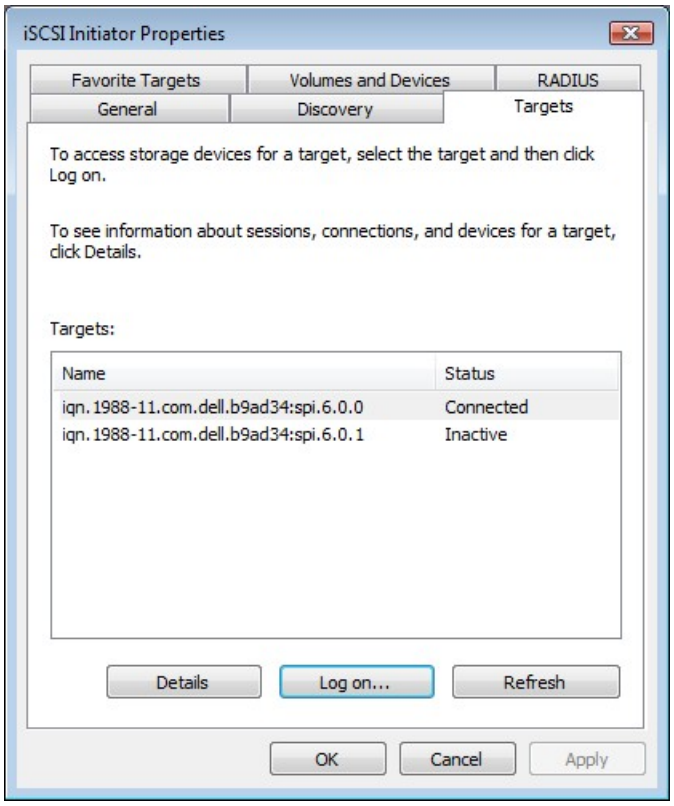
See Chapter 5: iSCSI Target Configuration for more information.



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

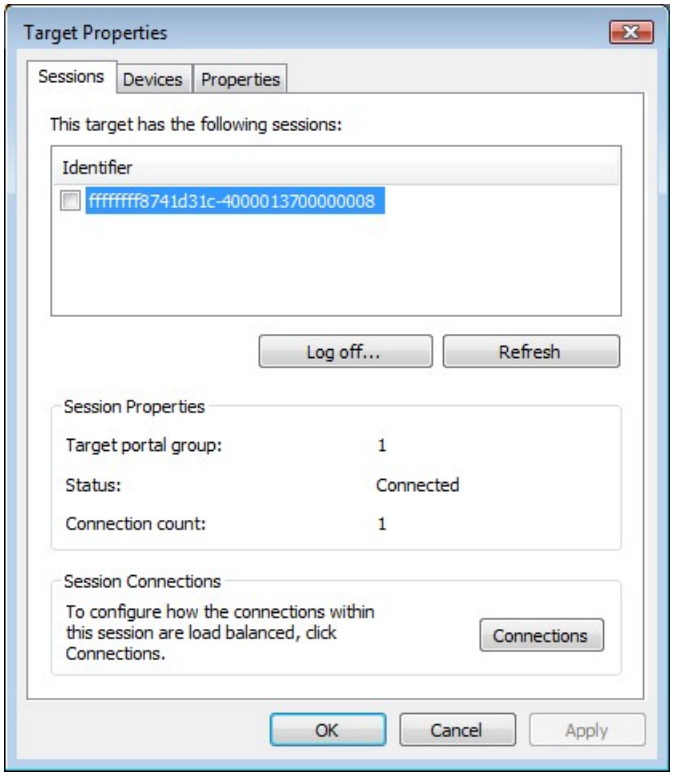
To set up the Digest and CHAP settings, see Appendix C.2: Discovery of Devices.

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



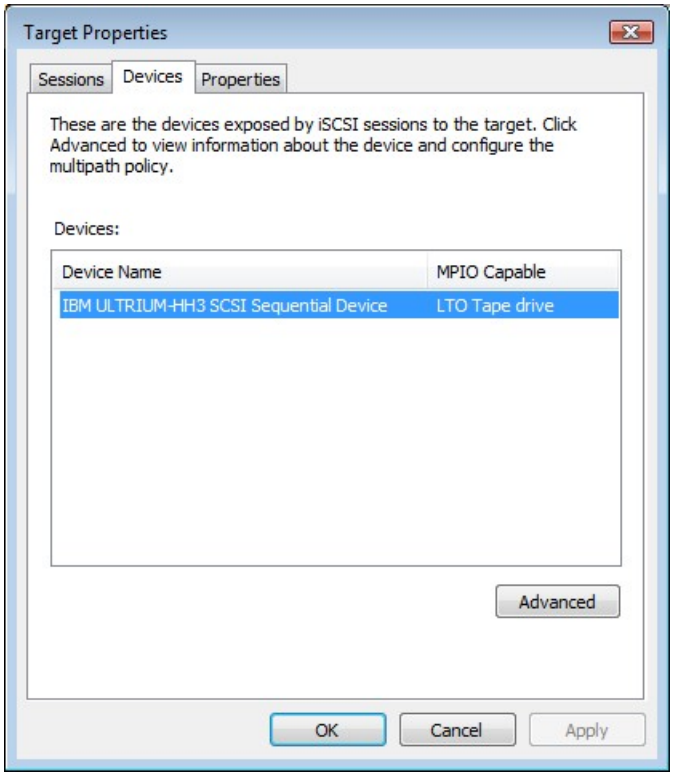
Viewing iSCSI Session Details

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



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

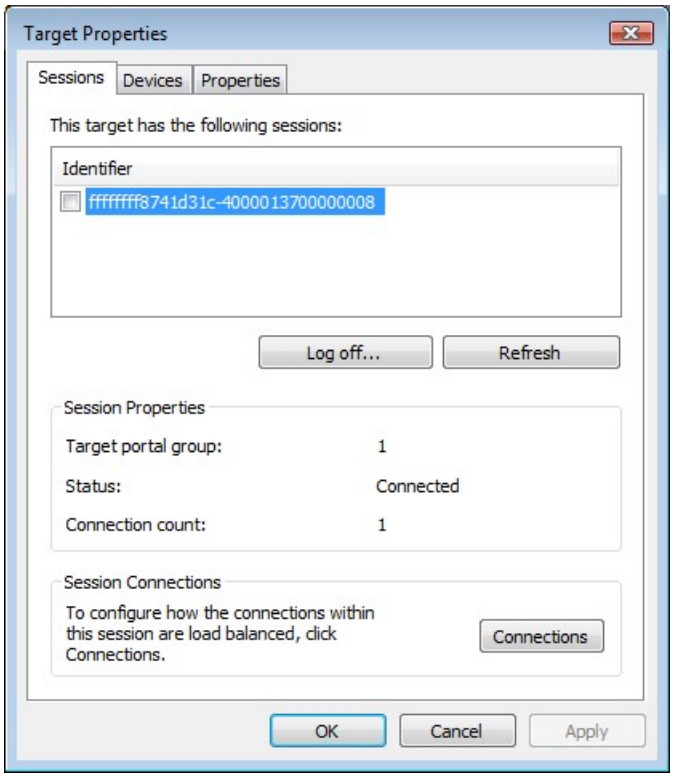
If you click on the *Device tab*, details of the target device will be displayed. Here for example, we can see that the device is an IBM LTO Tape drive.



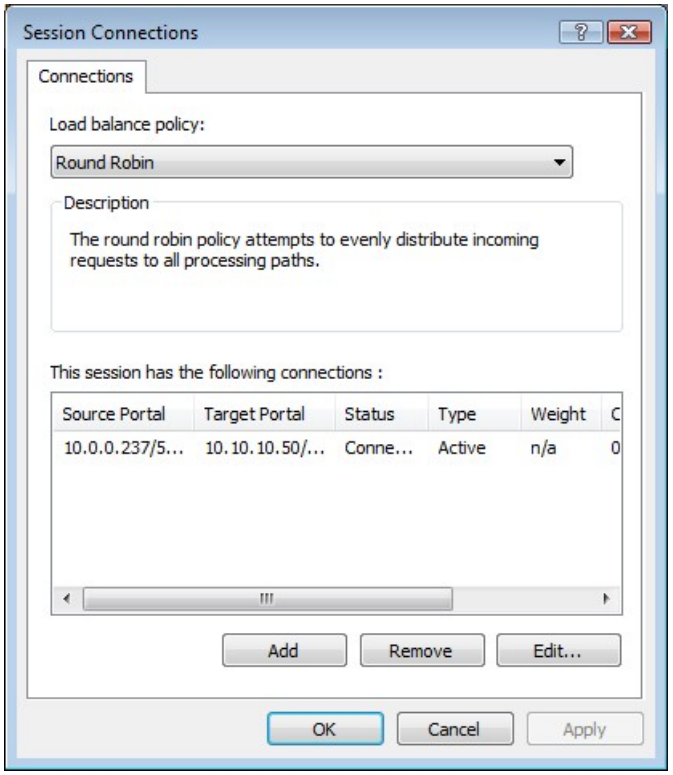
Creating Multiple Connections (Optional)

If you wish to create multiple connections to an iSCSI target, it is recommended to use Multiple Connections per Session (“MCS”) rather than creating multiple sessions (“MPIO”). This subsection will only cover the procedure for MCS.

Navigate the *Target Properties* window, by selecting the target from the *Targets* list and clicking *Details* if necessary. Navigate to the *Sessions* tab.



Click on the *Connections* button to open the *Session Connections* window:



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

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

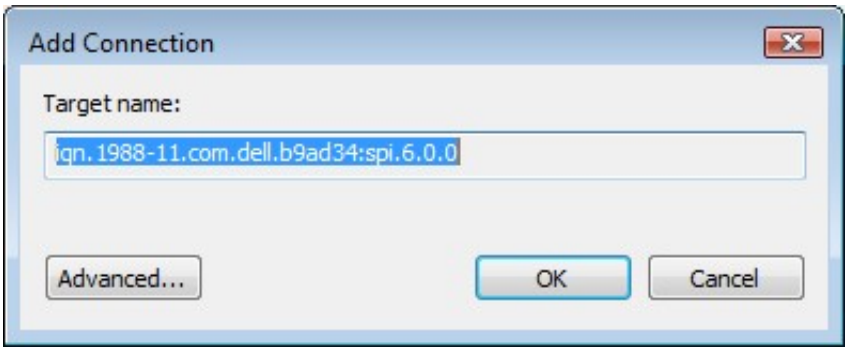
Note: The *Load balance policy* specifies how the data is distributed over multiple connections. The main policies that should be used are *Round Robin* and *Fail Over Only*:

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

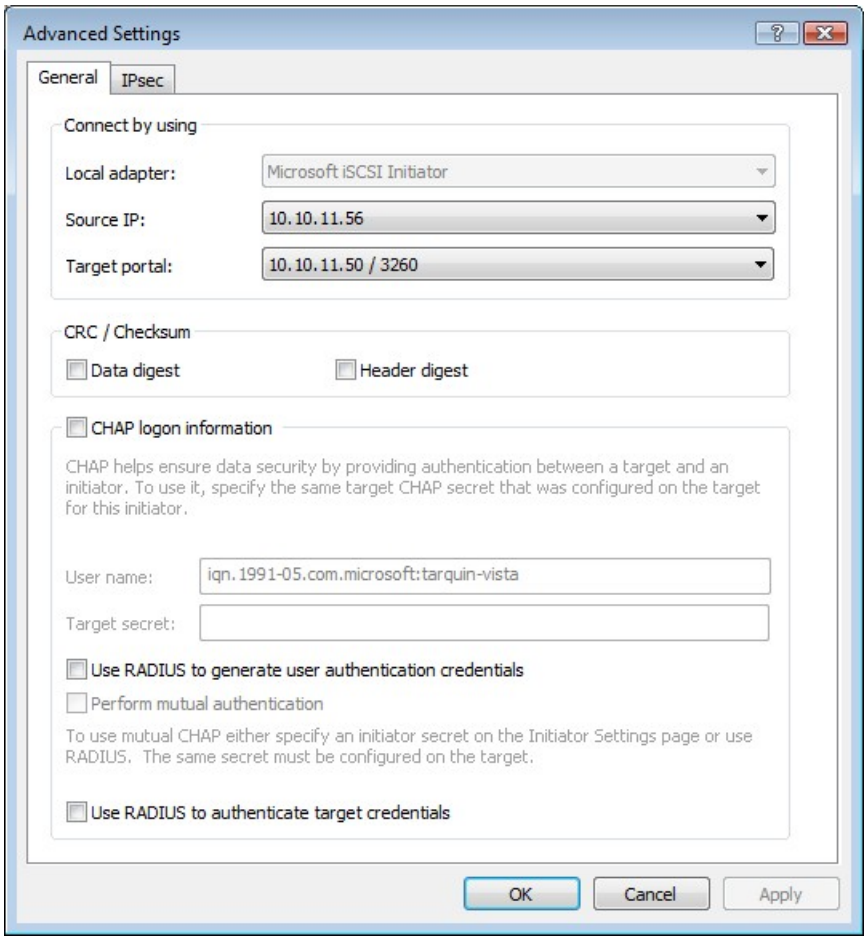
Fail Over Only will use the leading connection for data transfer. If a connection should go down then the data transfer shall switch to one of the other connections.

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

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

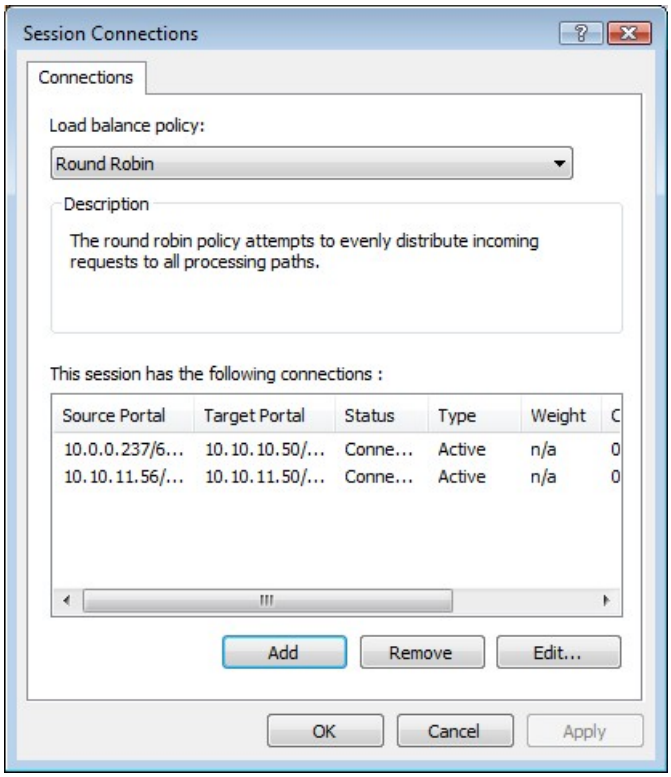


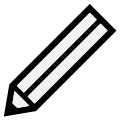
Then click *Advanced* to open *Advanced Settings*:



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

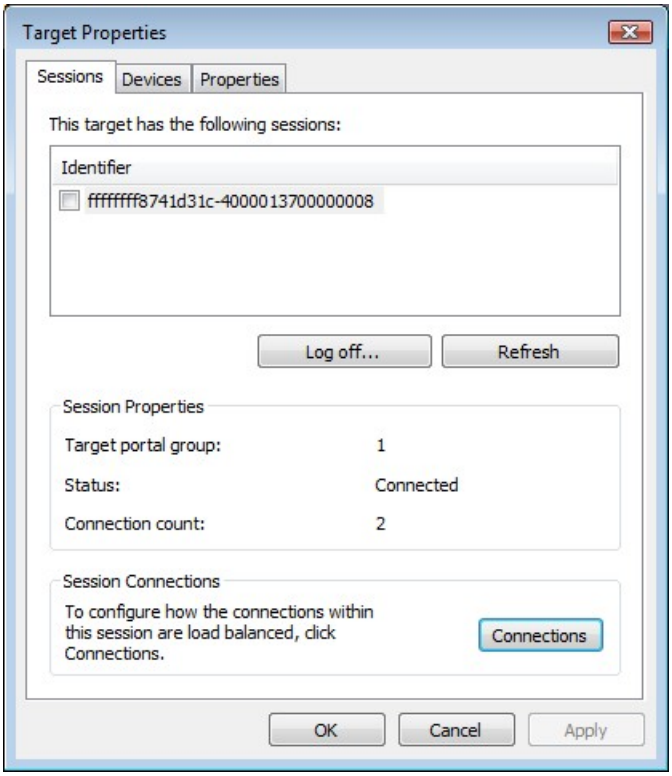
Configure CHAP and Header/Data Digest, and click OK. Then click OK within the *Add Connection* window. and now you should see the new, additional connection listed in the *Session Connections* window.



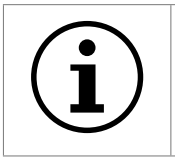


Note: Up to 8 connections can be added to one session.

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



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



Important: If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to Chapter 8: Troubleshooting.

Logging off an iSCSI Session

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

1. Open the Microsoft iSCSI Initiator and click on the *Targets* tab.
2. Click on the iSCSI session that you wish to log off and then click *Details*.
3. In the *Target Properties* window, select the *Sessions Tab* and select the identifier that is to be logged off.
4. Click the *Log off* button. This will log off all connections associated with the iSCSI Session.
5. The session identifier should now be removed from the identifier list. Click *OK* to return to the main iSCSI Initiator window.

The iSCSI device should now show as inactive.

Connecting to an iSCSI Device using iscsiadm

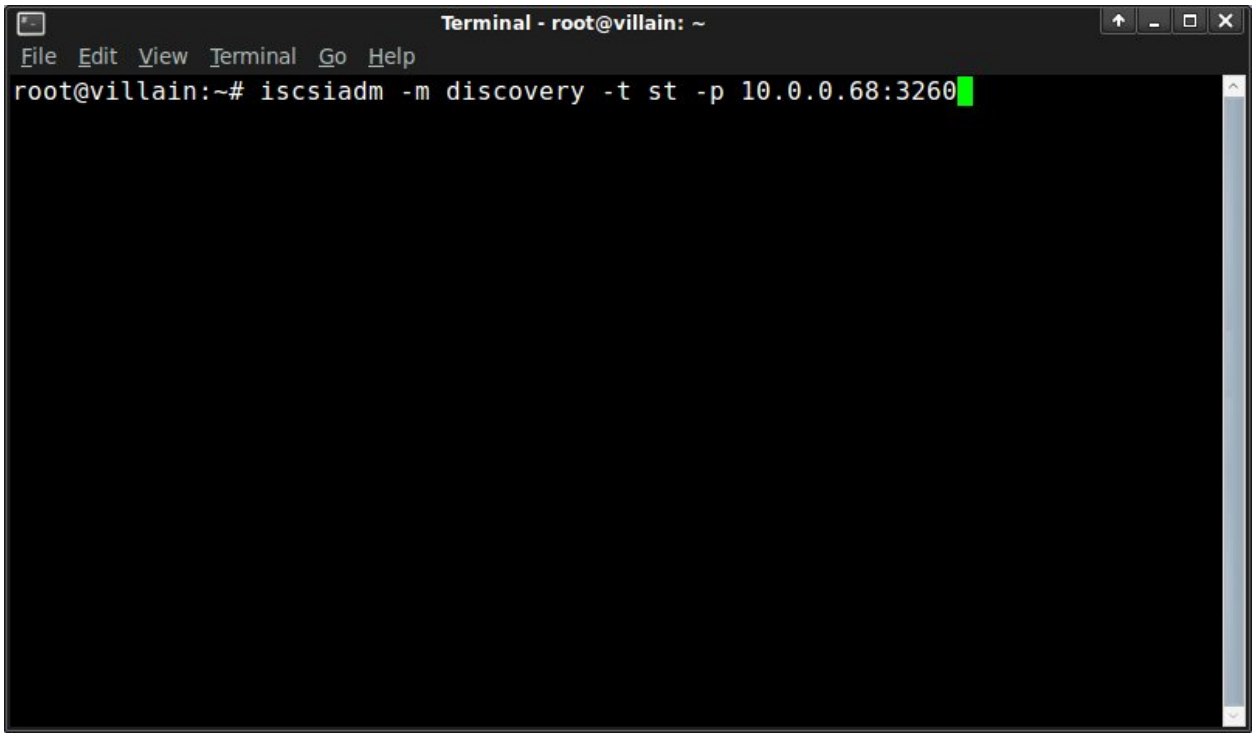
Important: The `iscsiadm` command may require root privileges to function. This guide will assume that the user has root privileges.

Discovering iSCSI Targets

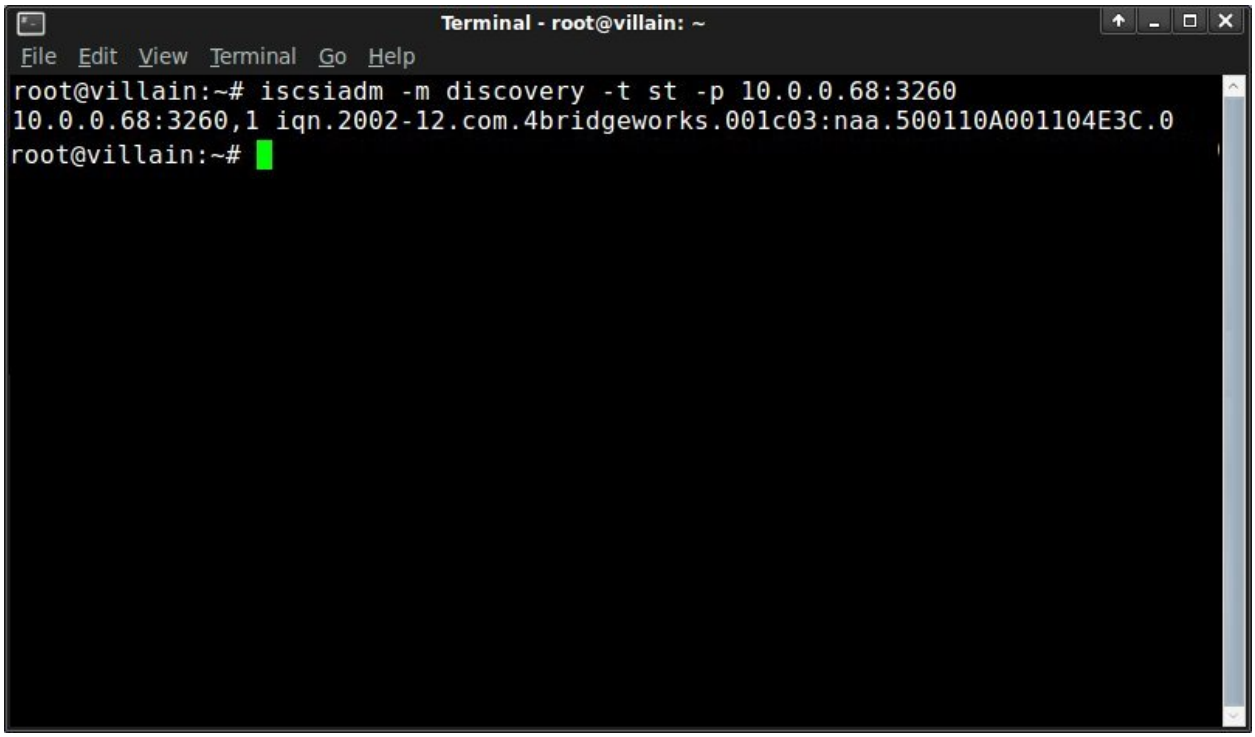
To get a list of available targets on the Gateway, run a discovery using the following command:

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

An example of this is shown below when performing a discovery on a target with the IP address 10.0.0.68 on port 3260.



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

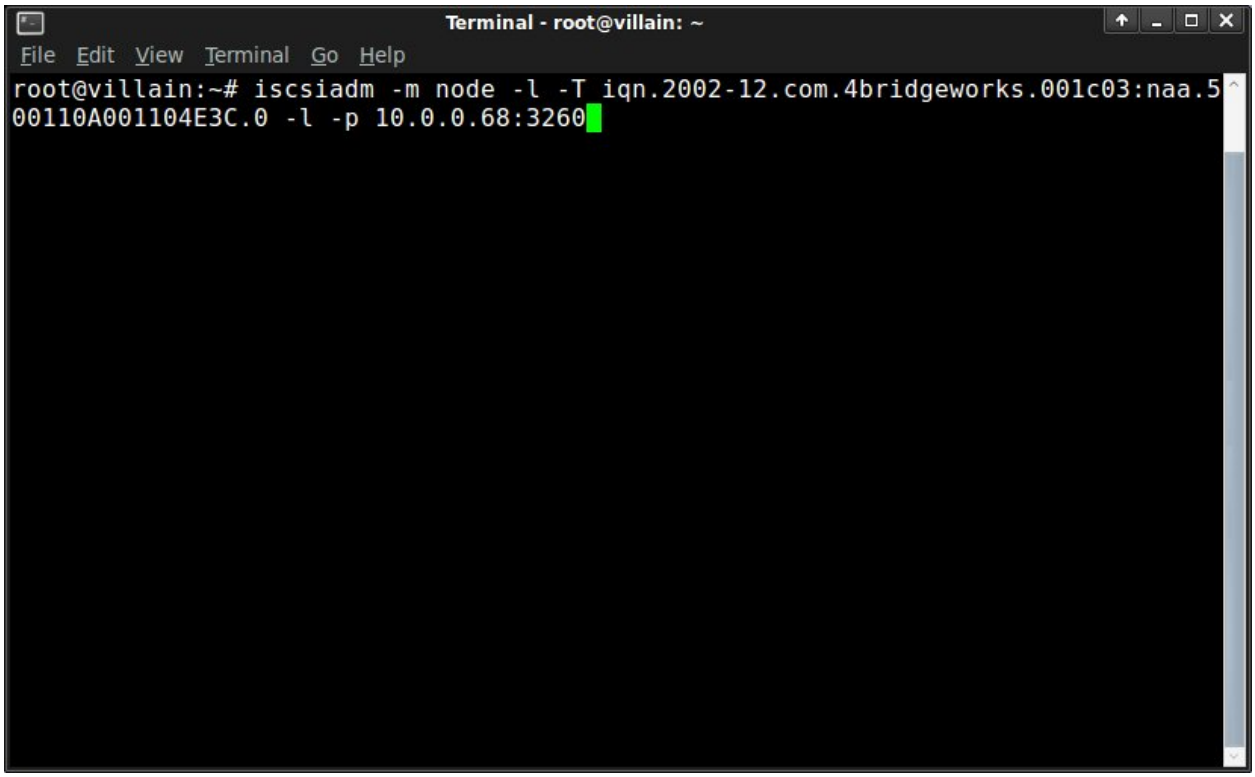


Logging into a target

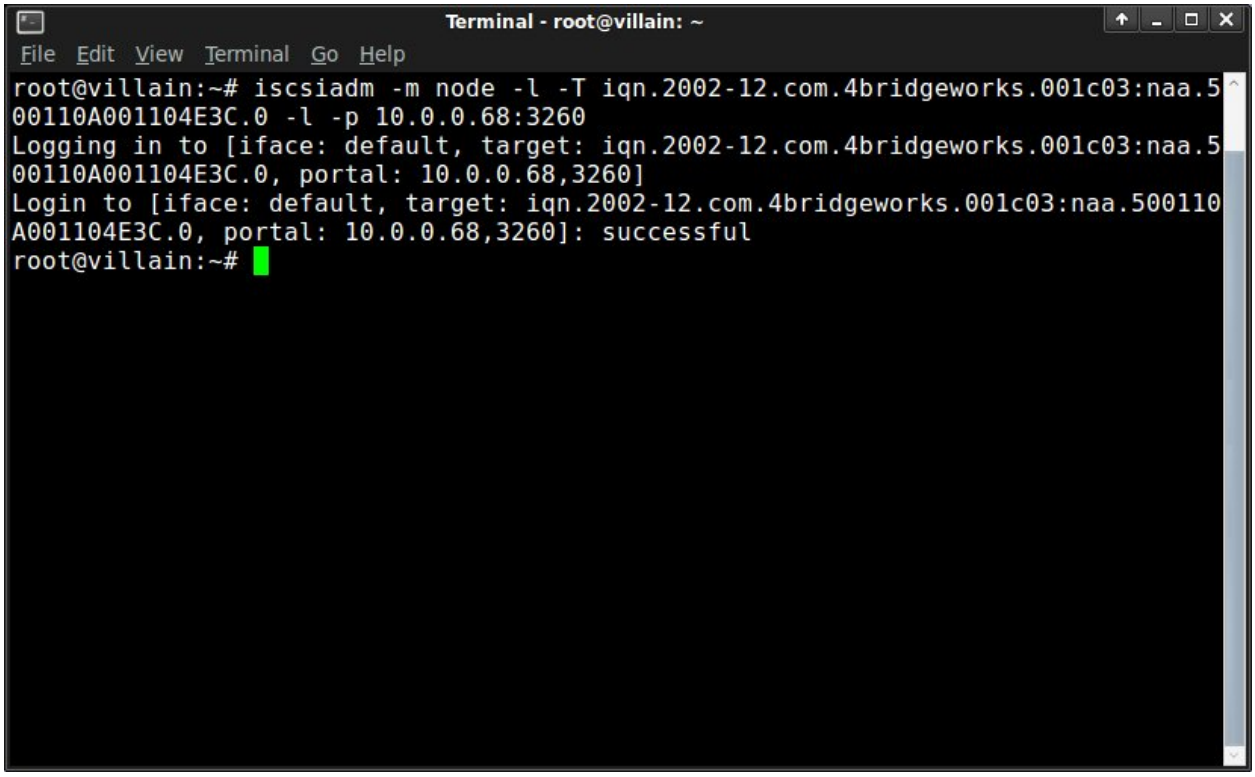
Once you have discovered the available targets, you can then login to the target. The following command will allow you to login to an individual target:

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

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



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



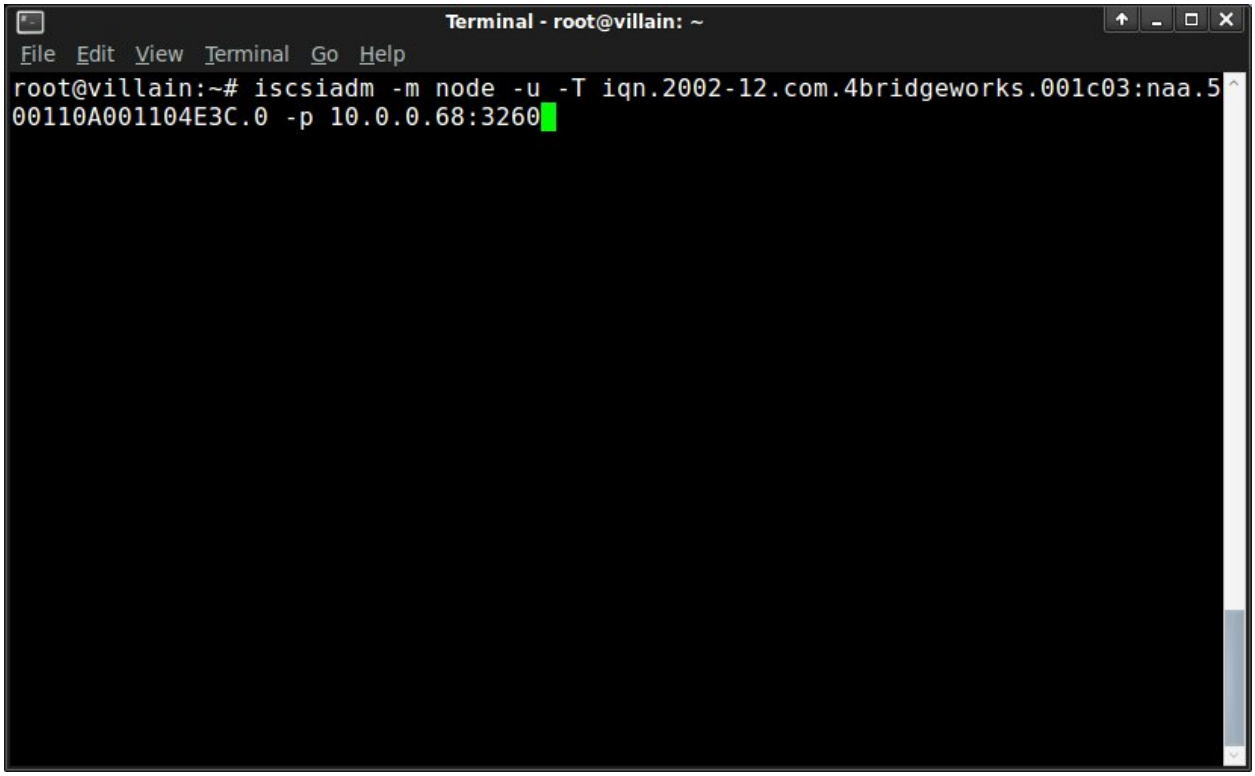
To login to all targets found, the following command can be used:

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

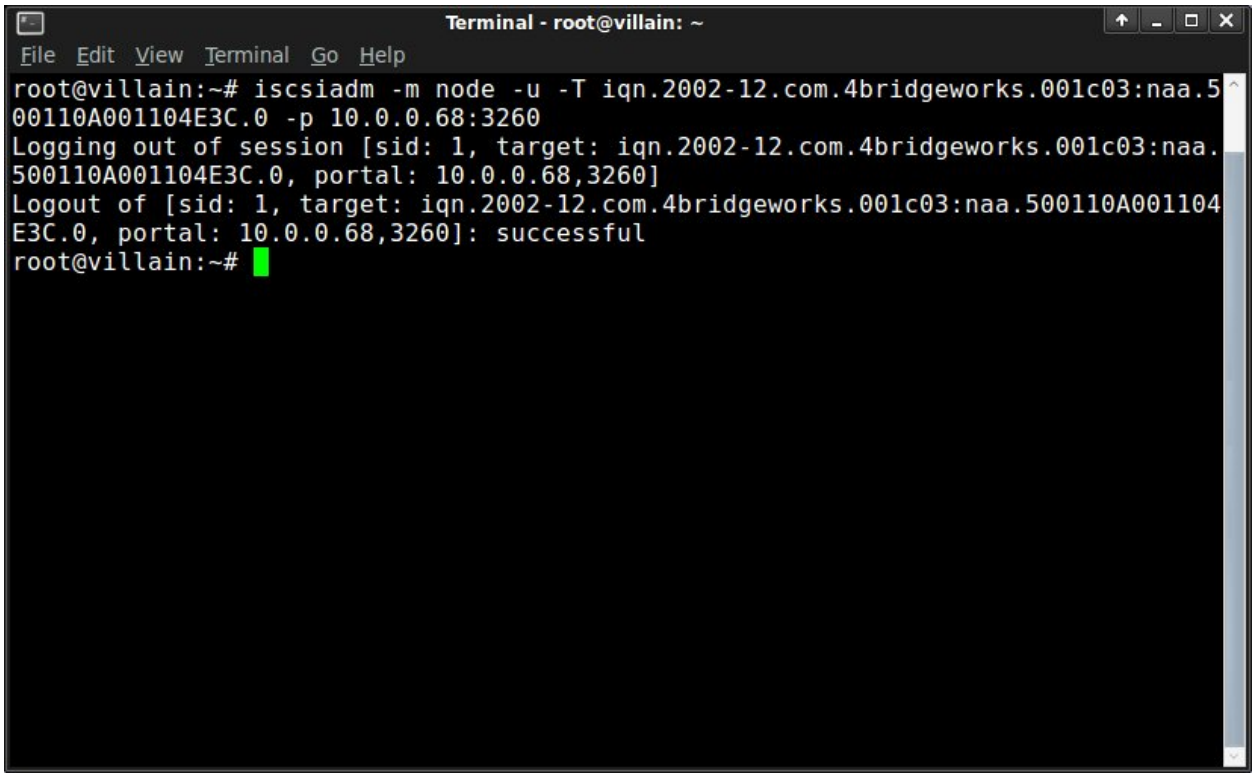
Logging out of a target

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

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



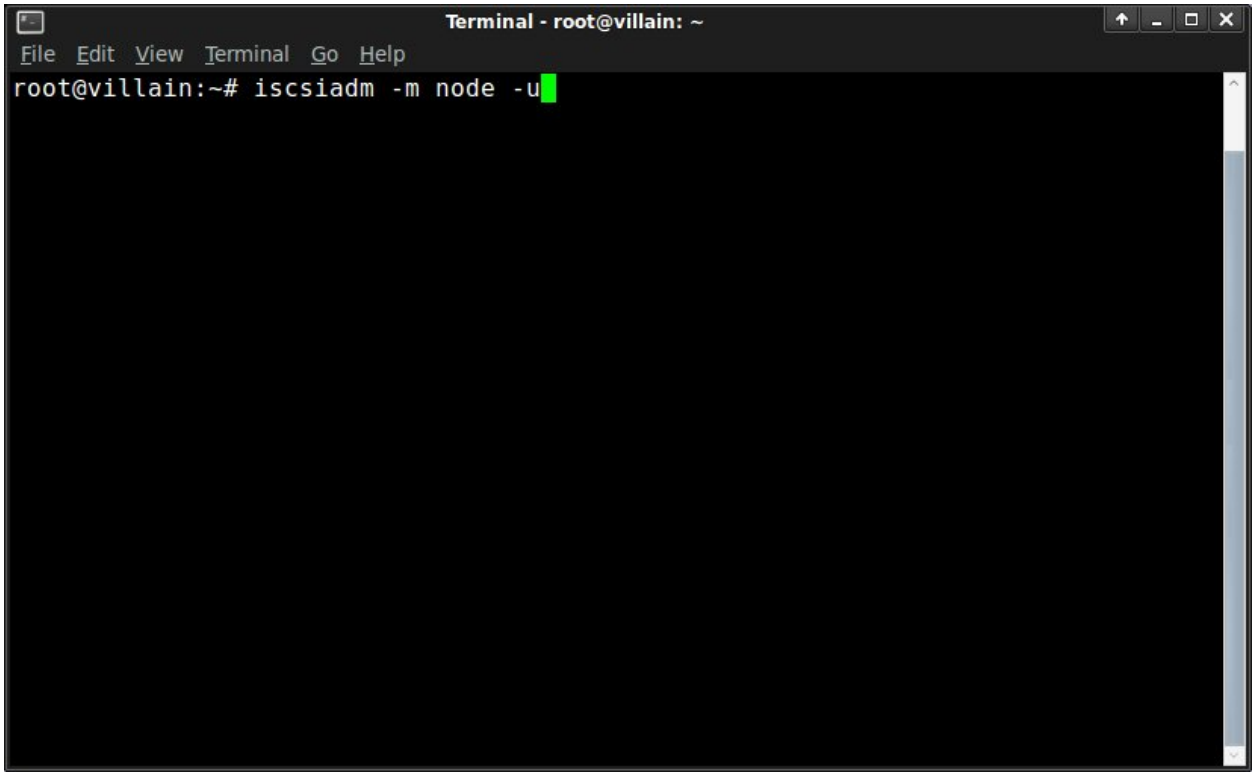
When you have successfully logged out of the target device, the screen should update as shown below:



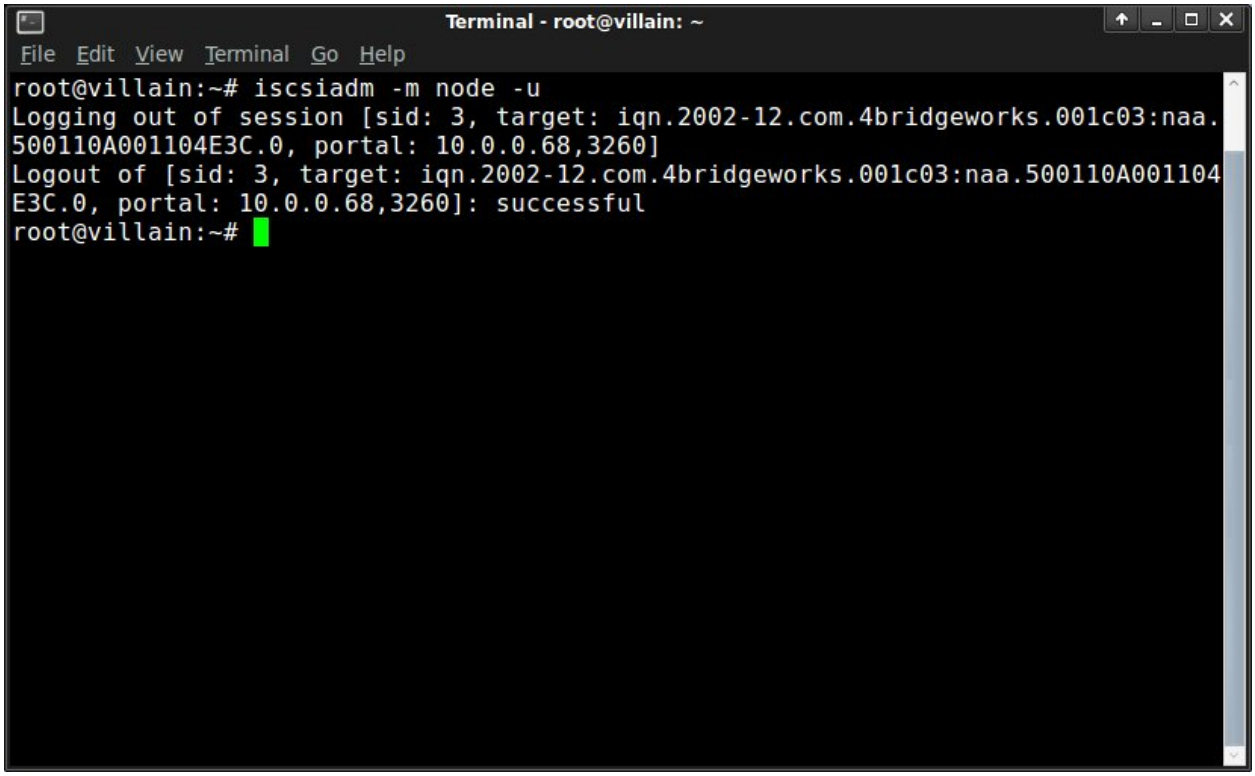
Logging out of all targets

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

```
iscsiadm -m node -u
```



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



Useful Links

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

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

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

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

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