Oresund FCE
FC to iSCSI Gateway
Software Manual

This manual covers the following products:

FCE102200

Eli-v6.1.68

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

Thank you for purchasing the Bridgeworks Oresund FCE Fibre Channel to iSCSI 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, Fibre Channel and iSCSI aspects of the Gateway.

1.1 Overview

The FCE creates an interface between a network, which utilises the Fibre Channel protocol, and devices that reside upon the iSCSI 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 Fibre Channel network to iSCSI data packets.

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

1.2 Manual Layout

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

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

1.3 Definitions

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

1.3.1 iSCSI Target Device

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

1.3.2 iSCSI Qualified Name (IQN)

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

1.3.3 iSCSI Challenge Handshake Authentication Protocol (CHAP)

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

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

1.3.4 Logical Unit Number (LUN)

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

2 Using the Web Interface

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

2.1 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.

2.2 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/`

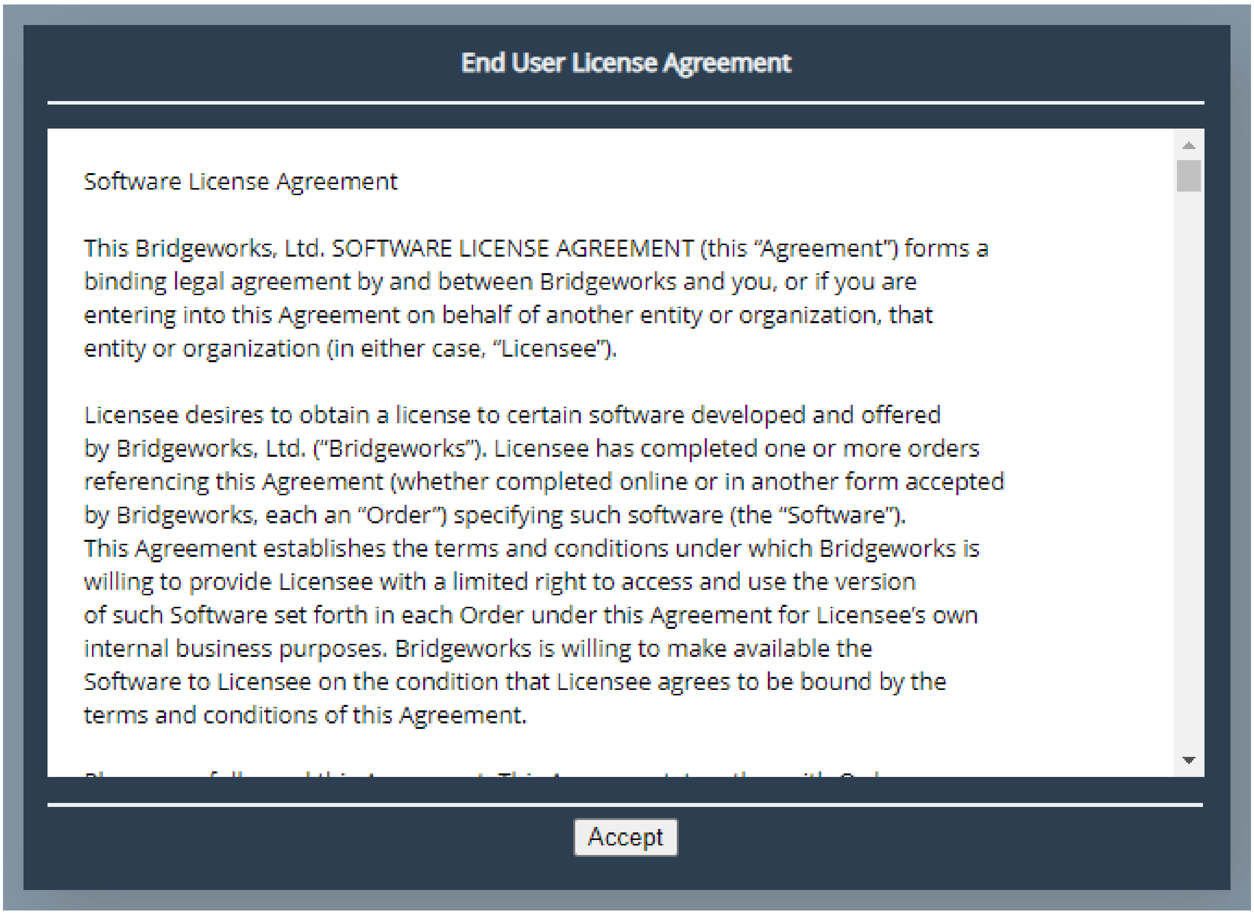
[1] Latest version as of release

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.



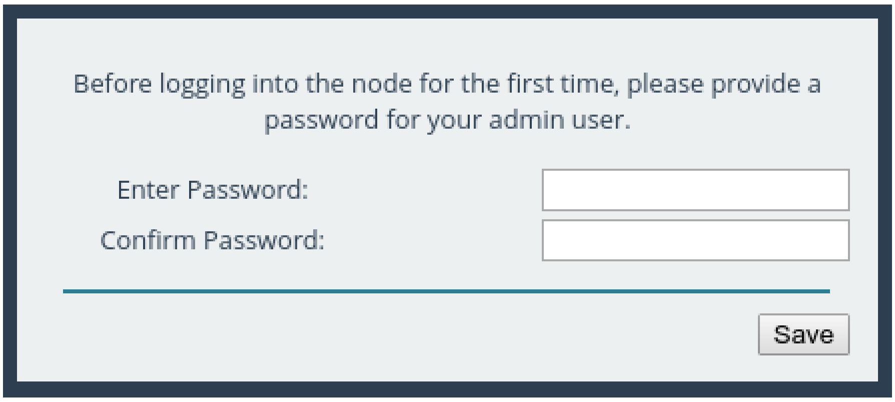
End User License Agreement

Software License Agreement

This Bridgeworks, Ltd. SOFTWARE LICENSE AGREEMENT (this "Agreement") forms a binding legal agreement by and between Bridgeworks and you, or if you are entering into this Agreement on behalf of another entity or organization, that entity or organization (in either case, "Licensee").

Licensee desires to obtain a license to certain software developed and offered by Bridgeworks, Ltd. ("Bridgeworks"). Licensee has completed one or more orders referencing this Agreement (whether completed online or in another form accepted by Bridgeworks, each an "Order") specifying such software (the "Software"). This Agreement establishes the terms and conditions under which Bridgeworks is willing to provide Licensee with a limited right to access and use the version of such Software set forth in each Order under this Agreement for Licensee's own internal business purposes. Bridgeworks is willing to make available the Software to Licensee on the condition that Licensee agrees to be bound by the terms and conditions of this Agreement.

You will then see the entry page shown below:

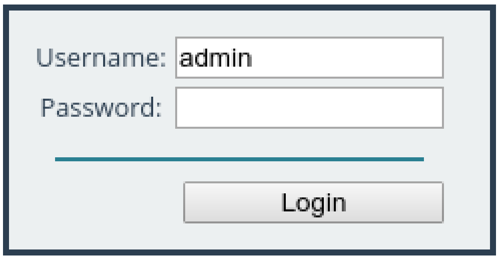


Before logging into the node for the first time, please provide a password for your admin user.

Enter Password:

Confirm Password:

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



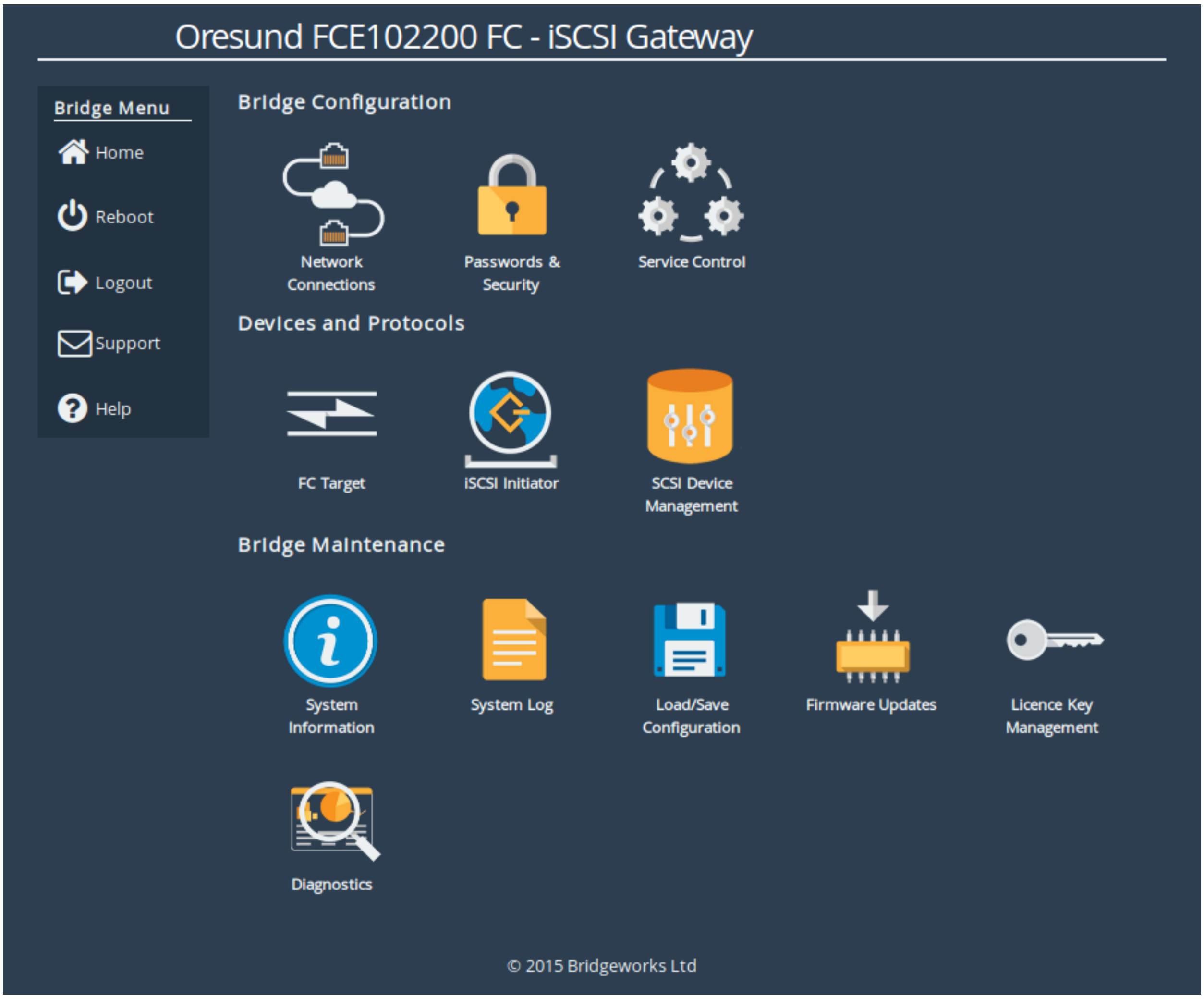
Username: admin

Password:

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

2.3 Management Console (Home screen)

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



Oresund FCE102200 FC - iSCSI Gateway

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.

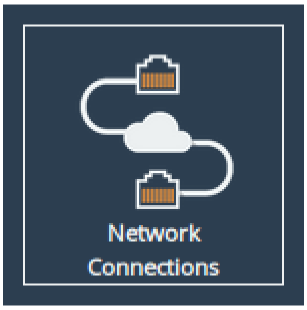
3 Bridge Configuration

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

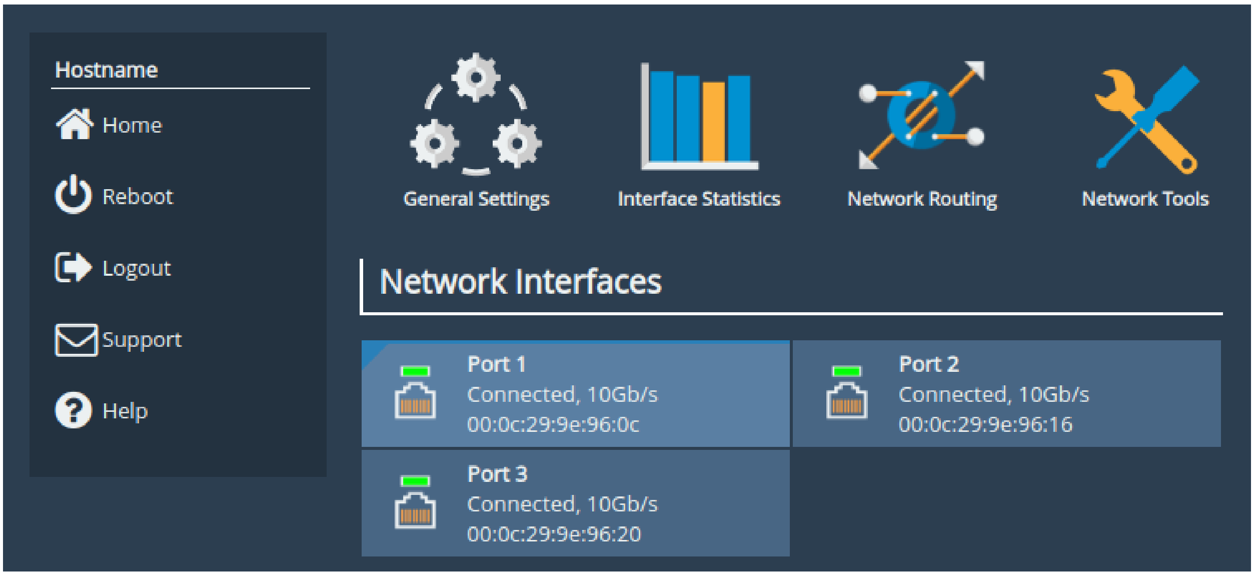
3.1 Network Connections

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

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



The web interface will display the following:



Network Interfaces

Port 1
Connected, 10Gb/s
00:0c:29:9e:96:0c

Port 2
Connected, 10Gb/s
00:0c:29:9e:96:16

Port 3
Connected, 10Gb/s
00:0c:29:9e:96:20

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

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

3.1.1 Network Interfaces

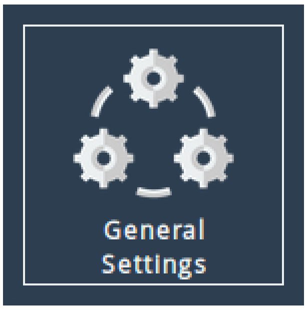
This section displays each network port present on the Gateway, along with its current status/link speed, and hardware identifier (MAC address).

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.

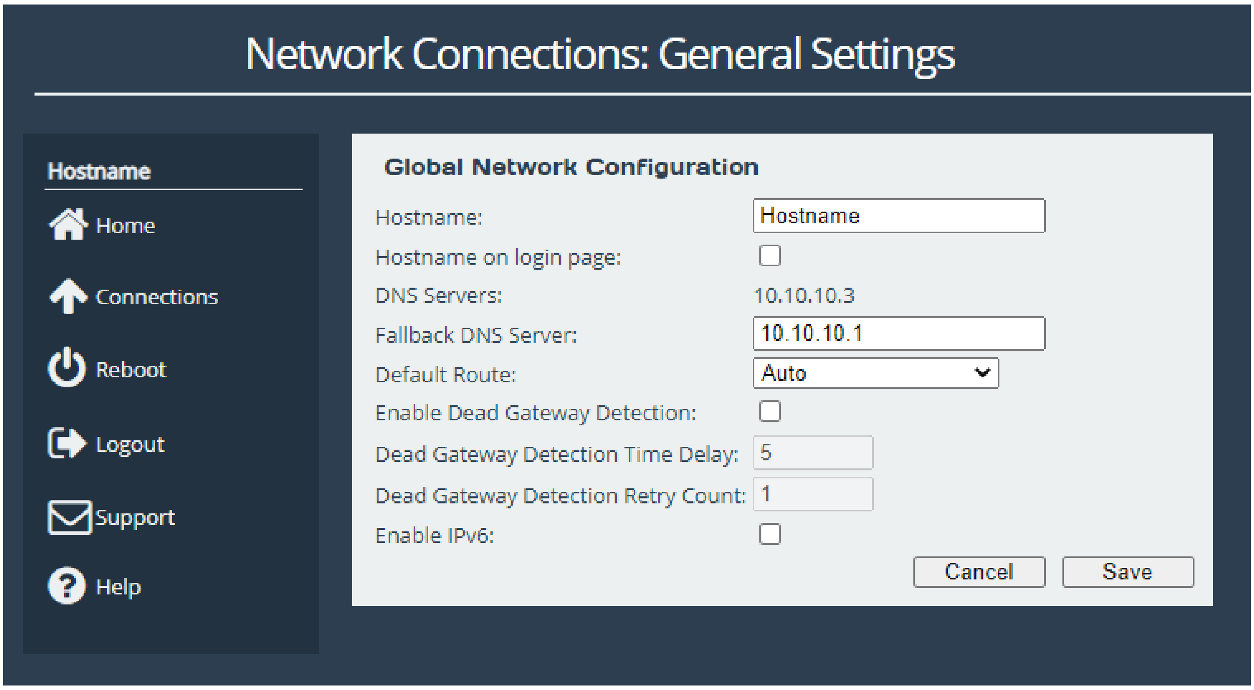
3.1.2 General Settings

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.



Global Network Configuration

Hostname:	Hostname
Hostname on login page:	□
DNS Servers:	10.10.10.3
Fallback DNS Server:	10.10.10.1
Default Route:	Auto
Enable Dead Gateway Detection:	□
Dead Gateway Detection Time Delay:	5
Dead Gateway Detection Retry Count:	1
Enable IPv6:	□

3.1.2.1 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.

3.1.2.2 Hostname on login page

When enabled, the Gateway's hostname will be displayed on the login screen before logging in.

3.1.2.3 DNS Servers

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

The *DNS Servers* field lists the DNS servers that are currently in use by the 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.

3.1.2.4 Default Route

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

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

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

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

3.1.2.5 Dead Gateway Detection

Selecting the *Enable Dead Gateway Detection* checkbox will allow the 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.

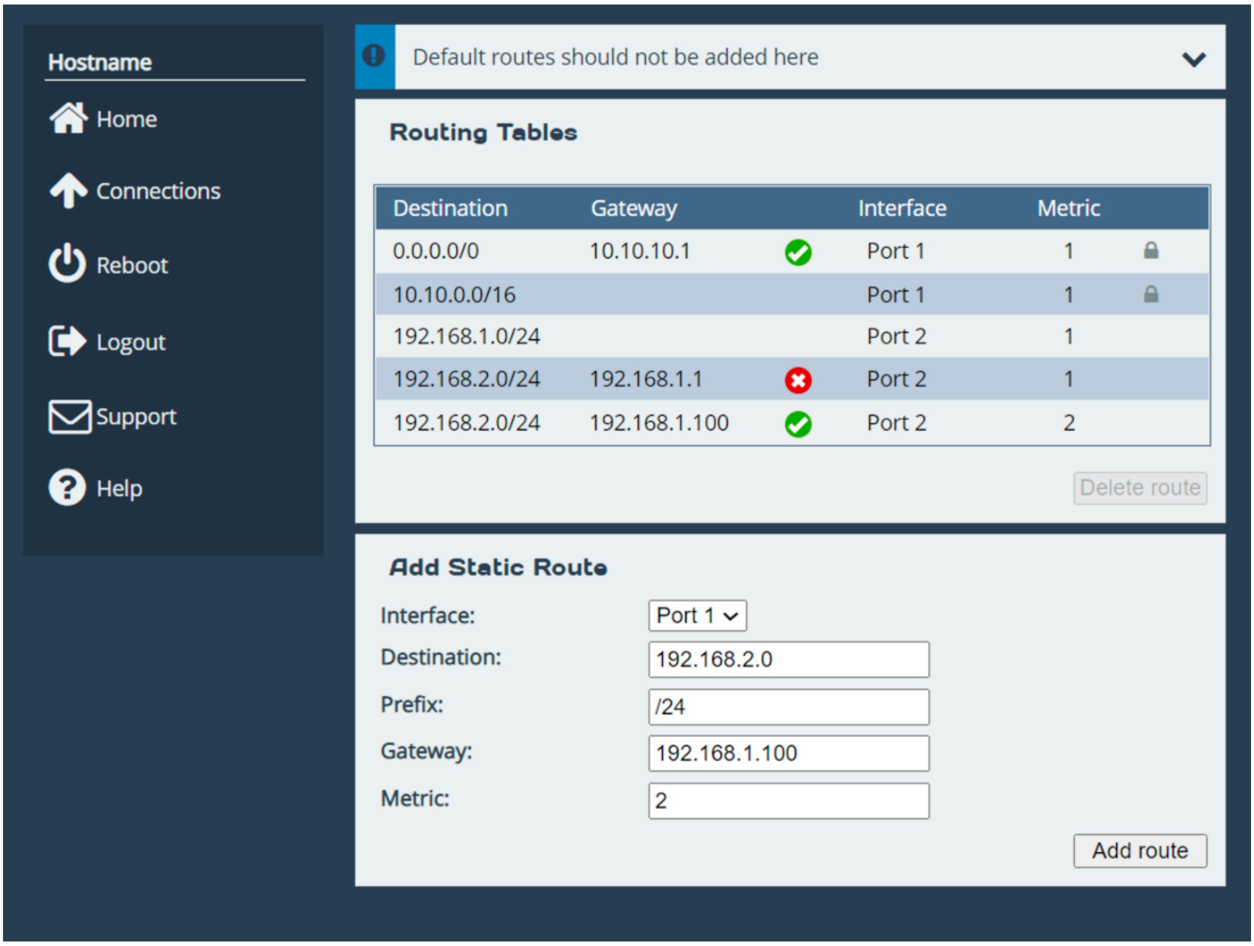
Dead Gateway Detection Retry Count refers to the number of times an unreachable gateway will be contacted before being set as a dead gateway and removed.

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.



Default routes should not be added here

Routing Tables

Destination	Gateway		Interface	Metric	
0.0.0.0/0	10.10.10.1	✓	Port 1	1	🔒
10.10.0.0/16			Port 1	1	🔒
192.168.1.0/24			Port 2	1	
192.168.2.0/24	192.168.1.1	✗	Port 2	1	
192.168.2.0/24	192.168.1.100	✓	Port 2	2	

Add Static Route

Interface: Port 1

Destination: 192.168.2.0

Prefix: /24

Gateway: 192.168.1.100

Metric: 2

In this example, dead gateway detection has been enabled and multiple redundant routes to

`192.168.2.0/24` have been added with different gateways (`192.168.1.1` and `192.168.1.100`) and different metrics (`1` and `2`, respectively).

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

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

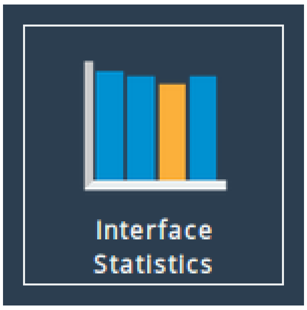
3.1.2.6 Enable IPv6

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

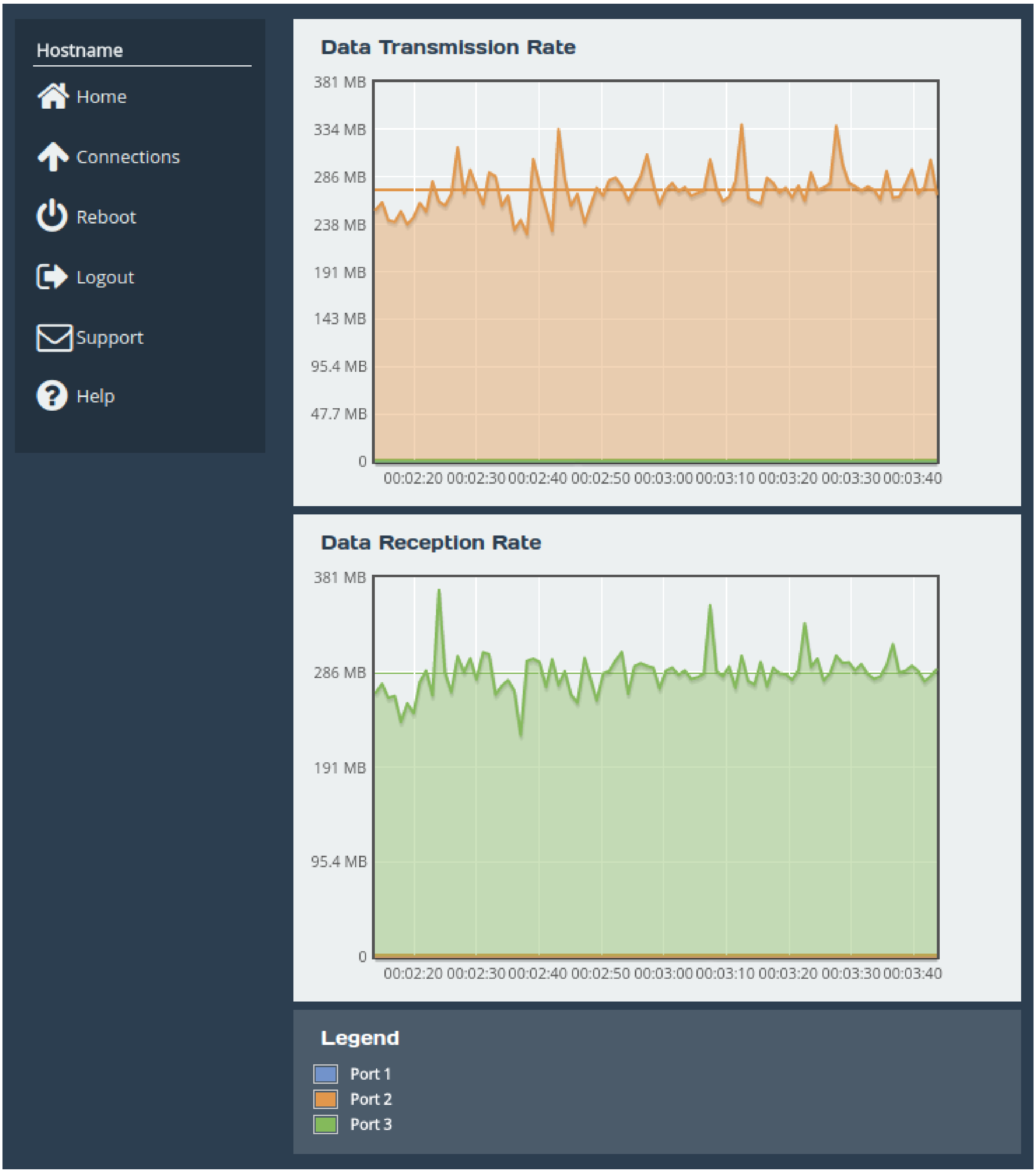
3.1.3 Interface Statistics

This page displays live network interface data rate statistics.

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



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



3.1.3.1 Data Transmission Rate

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

3.1.3.2 Data Reception Rate

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

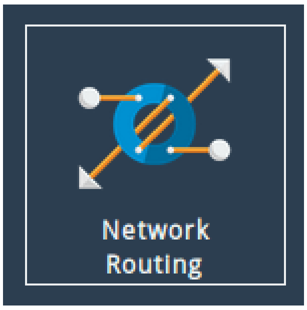
3.1.3.3 Legend

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

3.1.4 Network Routing

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

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



3.1.4.1 Add Static Route

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

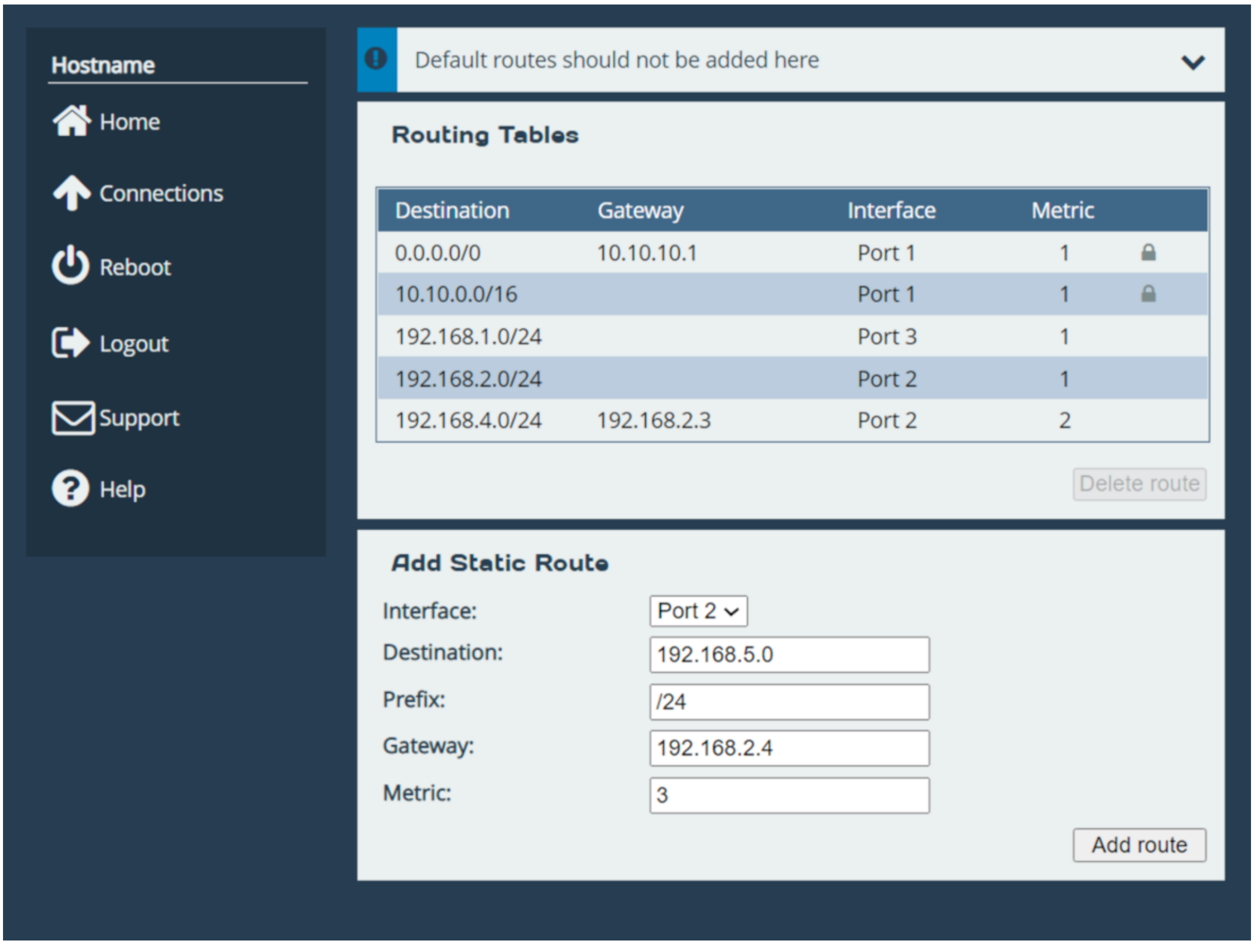
Interface The network interface to which the route applies.

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

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

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

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



Default routes should not be added here

Routing Tables

Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	🔒
10.10.0.0/16		Port 1	1	🔒
192.168.1.0/24		Port 3	1	
192.168.2.0/24		Port 2	1	
192.168.4.0/24	192.168.2.3	Port 2	2	

Add Static Route

Interface: Port 2
Destination: 192.168.5.0
Prefix: /24
Gateway: 192.168.2.4
Metric: 3

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

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

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

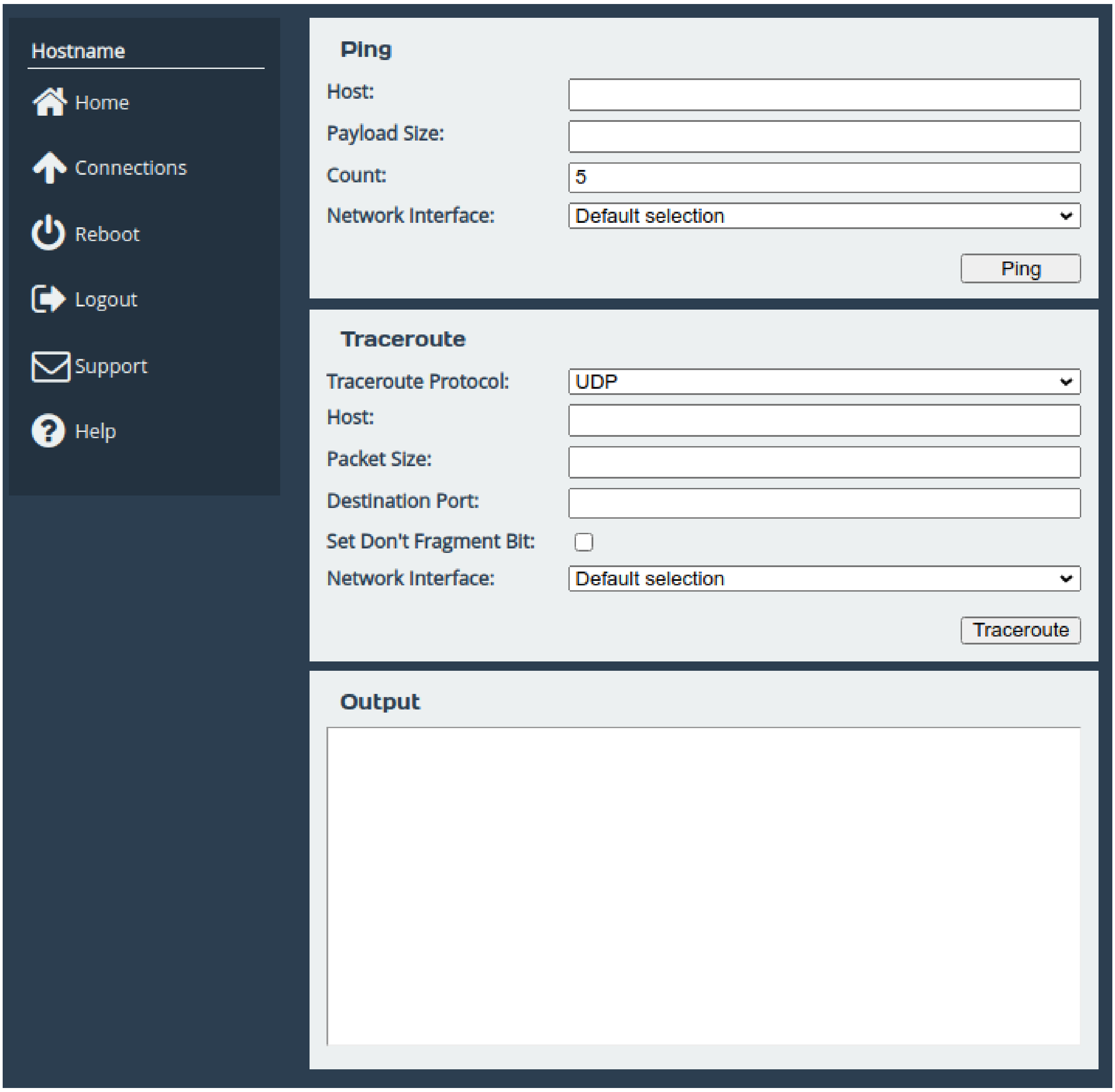
When dead gateway detection is enabled, each gateway in the table will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.2.5: Dead Gateway Detection for more information.

3.1.5 Network Tools

The 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

Host:

Payload Size:

Count: 5

Network Interface: Default selection

Traceroute

Traceroute Protocol: UDP

Host:

Packet Size:

Destination Port:

Set Don't Fragment Bit: □

Network Interface: Default selection

3.1.5.1 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.

3.1.5.2 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.

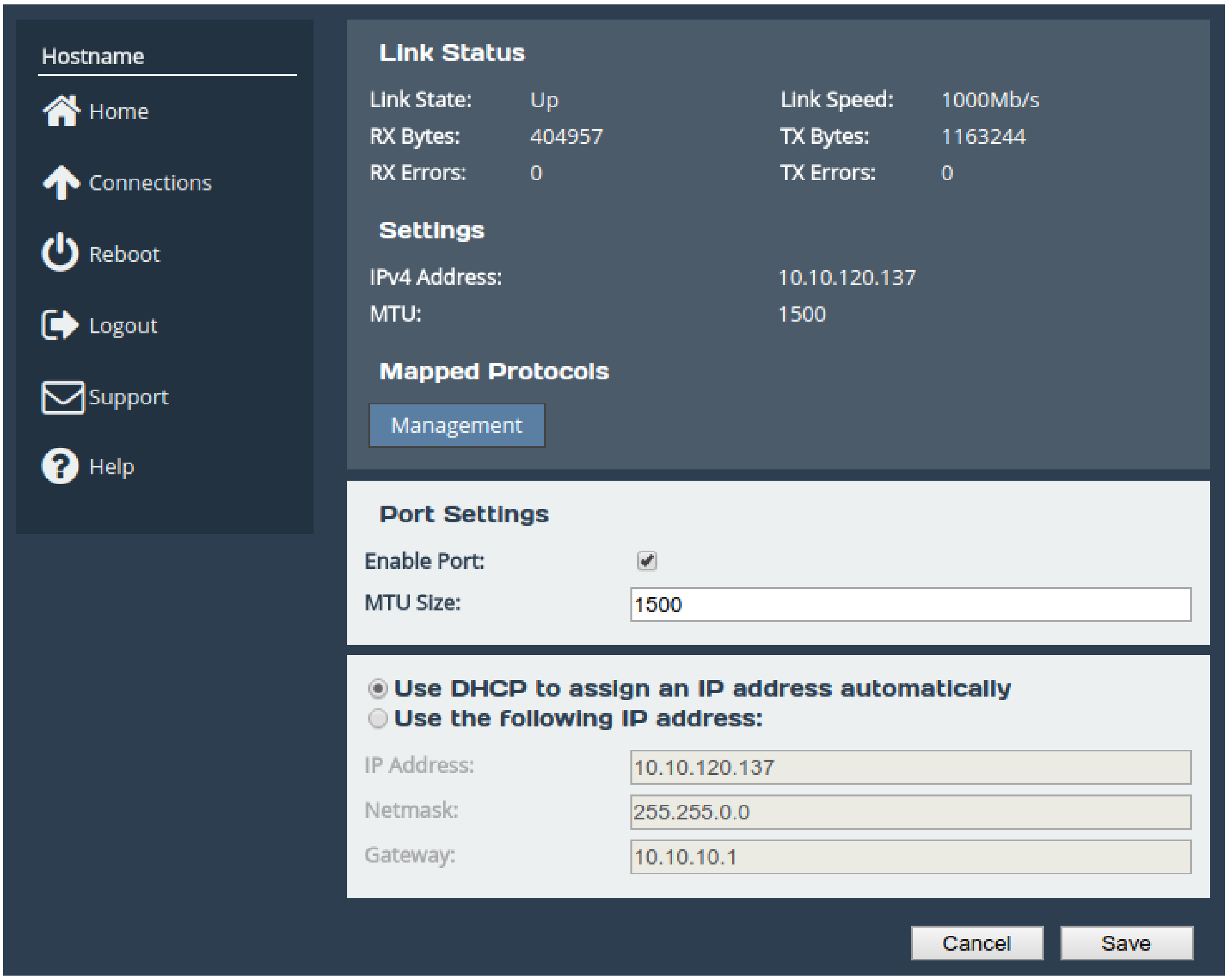
Use ICMP Echo Select to use ICMP echo requests instead of UDP datagrams. This can be useful when your firewall blocks UDP traffic.

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.

3.1.6 Port Settings

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



Link Status

Link State:	Up	Link Speed:	1000Mb/s
RX Bytes:	404957	TX Bytes:	1163244
RX Errors:	0	TX Errors:	0

Settings

IPv4 Address: 10.10.120.137

MTU: 1500

Mapped Protocols

Management

Port Settings

Enable Port: ☑

MTU Size: 1500

● Use DHCP to assign an IP address automatically

○ Use the following IP address:

IP Address: 10.10.120.137

Netmask: 255.255.0.0

Gateway: 10.10.10.1

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

3.1.6.1 Enable Port

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

3.1.6.2 Setting the MTU

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

3.1.6.3 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.

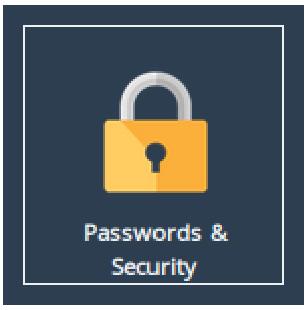
3.1.6.4 Committing the Changes

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

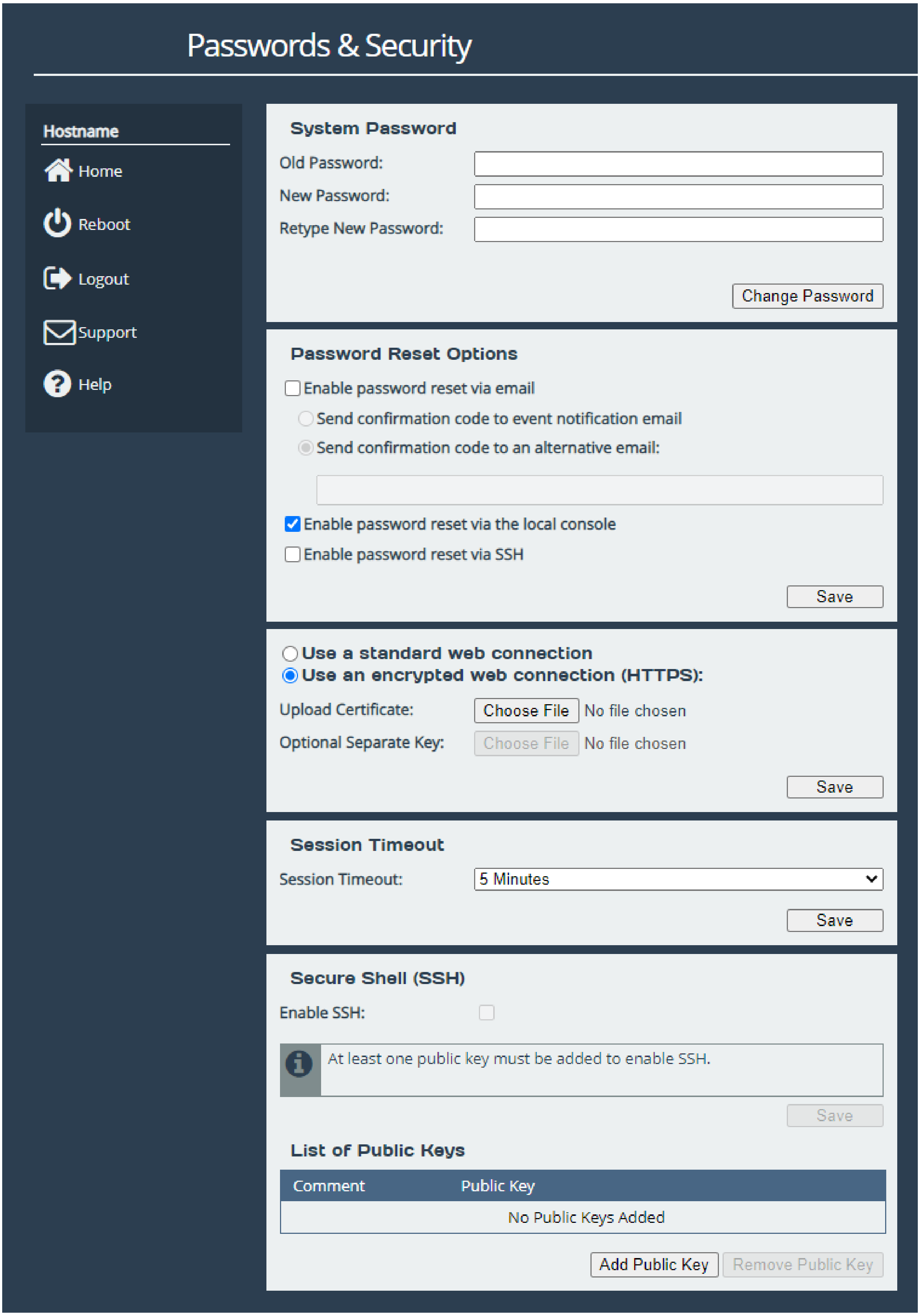
3.2 Passwords & Security

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:



Passwords & Security

System Password

Old Password:

New Password:

Retype New Password:

Password Reset Options

□ Enable password reset via email

○ Send confirmation code to event notification email

● Send confirmation code to an alternative email:

☑ Enable password reset via the local console

□ Enable password reset via SSH

○ Use a standard web connection

● Use an encrypted web connection (HTTPS):

Upload Certificate: Choose File No file chosen

Optional Separate Key: Choose File No file chosen

Session Timeout

Session Timeout: 5 Minutes

Secure Shell (SSH)

Enable SSH: □

At least one public key must be added to enable SSH.

List of Public Keys

Comment	Public Key
No Public Keys Added	

3.2.1 System Password

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

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

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

3.2.2 Password Reset Options

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

3.2.2.1 Password Reset via Email

3.2.2.1.1 Setup

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

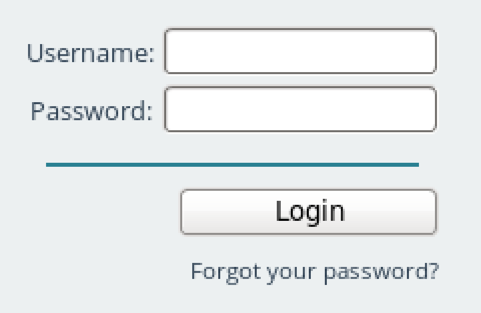
To enable password reset via email, SMTP settings will have to be configured first to allow the Gateway to send emails. Navigate to the *Service Control* page and enter your SMTP settings under the *Simple Mail Transfer Protocol (SMTP)* section. Refer to Section 3.3.3: Email for information on SMTP configuration.

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

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

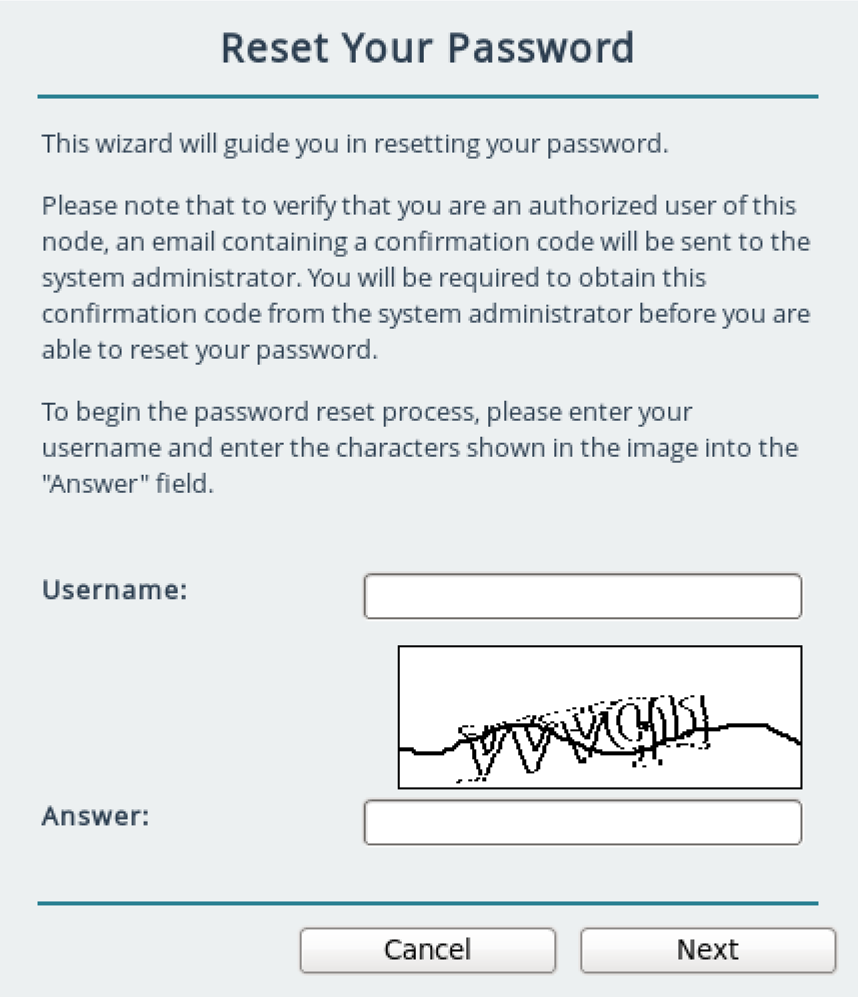
3.2.2.1.2 Using Password Reset via Email

To reset the password of a user account using the email method, navigate to the login page of the 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.



Reset Your Password

This wizard will guide you in resetting your password.

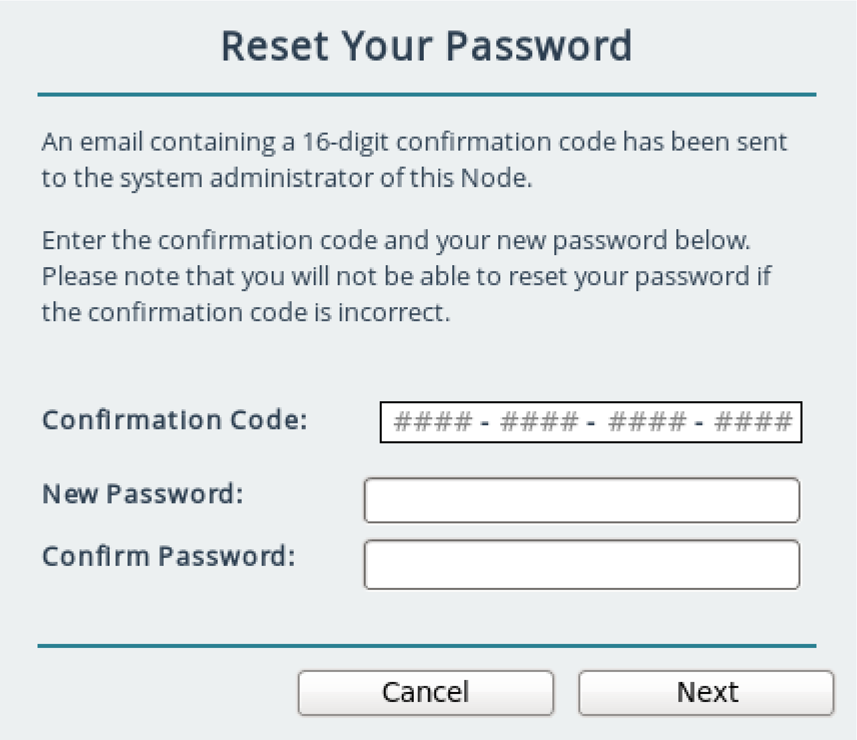
Please note that to verify that you are an authorized user of this node, an email containing a confirmation code will be sent to the system administrator. You will be required to obtain this confirmation code from the system administrator before you are able to reset your password.

To begin the password reset process, please enter your username and enter the characters shown in the image into the "Answer" field.

ⓘ 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.



Reset Your Password

An email containing a 16-digit confirmation code has been sent to the system administrator of this Node.

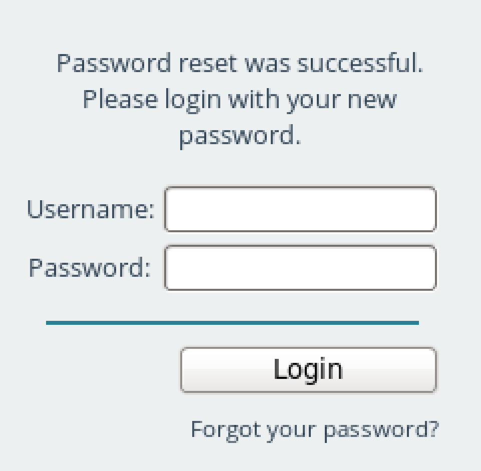
Enter the confirmation code and your new password below. Please note that you will not be able to reset your password if the confirmation code is incorrect.

Confirmation Code: #### - #### - #### - ####

New Password:

Confirm Password:

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



Password reset was successful. Please login with your new password.

Username:

Password:

3.2.2.2 Password Reset via Local Console or SSH

3.2.2.2.1 Setup

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

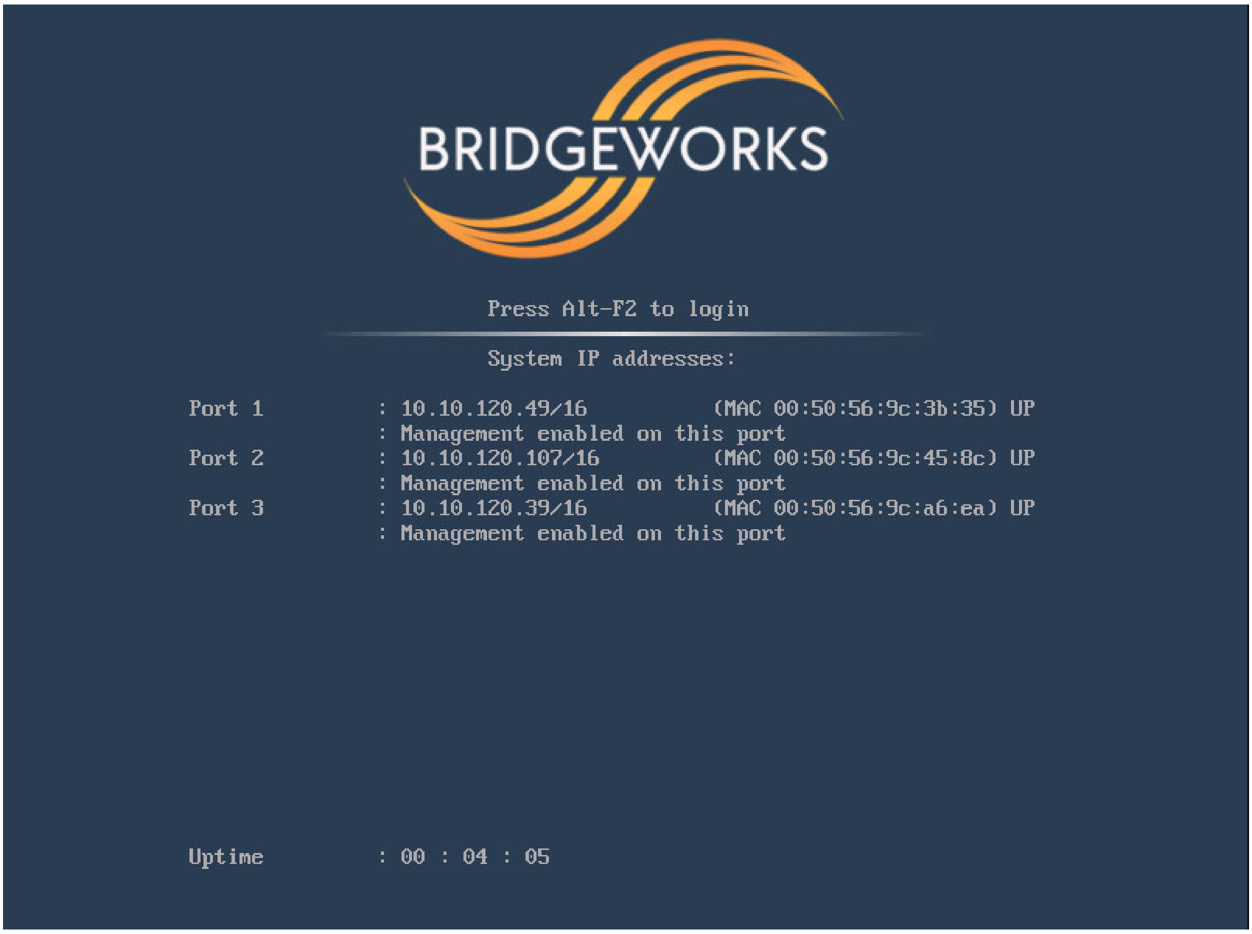
ℹ	Important: Resetting a password will log out any current sessions under that user name.

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*.

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

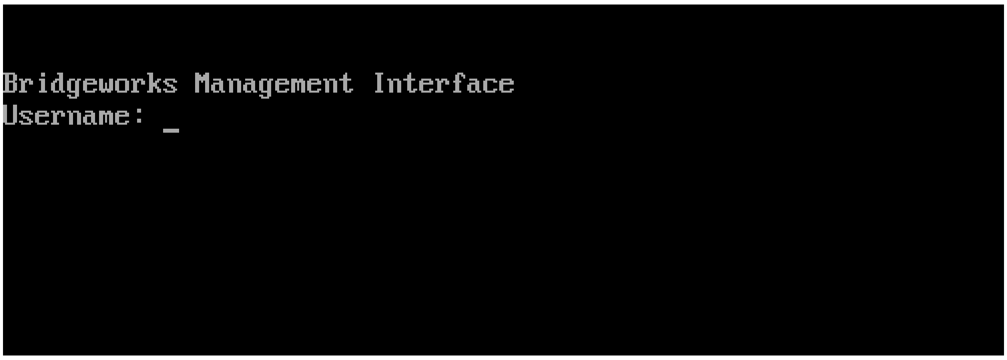
3.2.2.2.2 Using Password Reset via Local Console or SSH

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 Alt-F2 to login

System IP addresses:

Port 1          : 10.10.120.49/16          (MAC 00:50:56:9c:3b:35) UP
                : Management enabled on this port
Port 2          : 10.10.120.107/16         (MAC 00:50:56:9c:45:8c) UP
                : Management enabled on this port
Port 3          : 10.10.120.39/16          (MAC 00:50:56:9c:a6:ea) UP
                : Management enabled on this port




Uptime          : 00 : 04 : 05
```

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

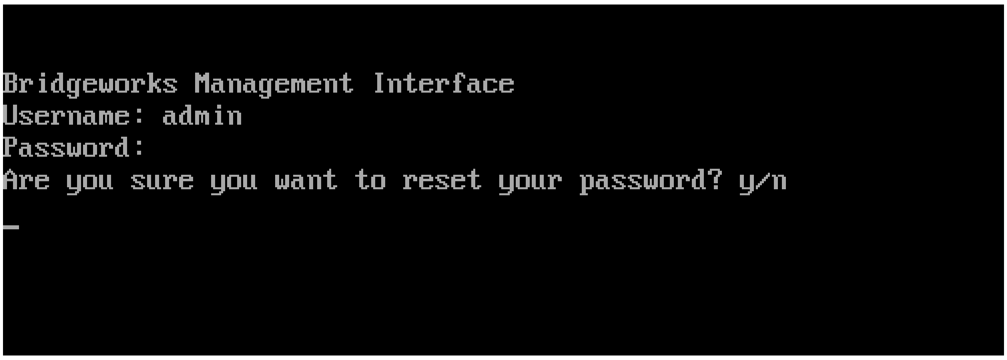


```
Bridgeworks Management Interface
Username: _
```

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.

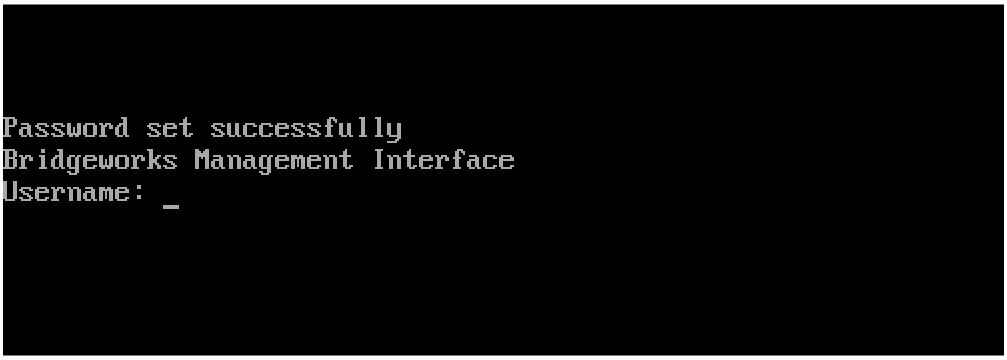


```
Bridgeworks Management Interface
Username: admin
Password:
Are you sure you want to reset your password? y/n
_
```

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:

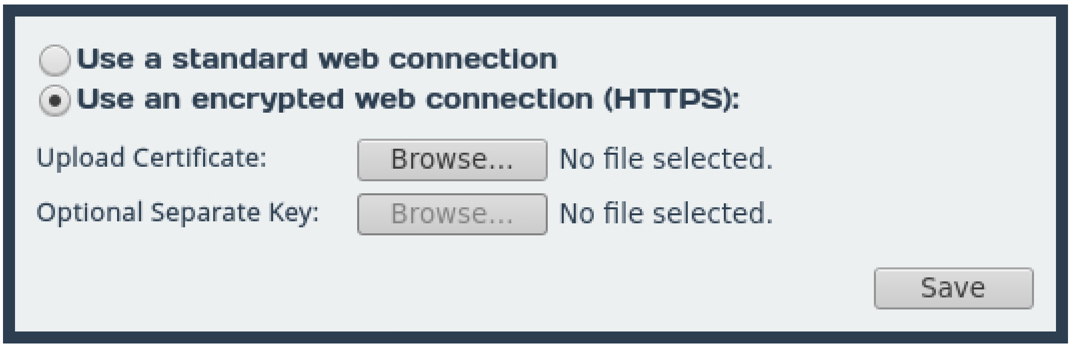


```
Password set successfully
Bridgeworks Management Interface
Username: _
```

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

3.2.3 Secure Connection

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



○ Use a standard web connection

● Use an encrypted web connection (HTTPS):

Upload Certificate: Browse... No file selected.

Optional Separate Key: Browse... No file selected.

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

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

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

3.2.4 Session Timeout

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

3.2.5 Secure Shell (SSH)

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

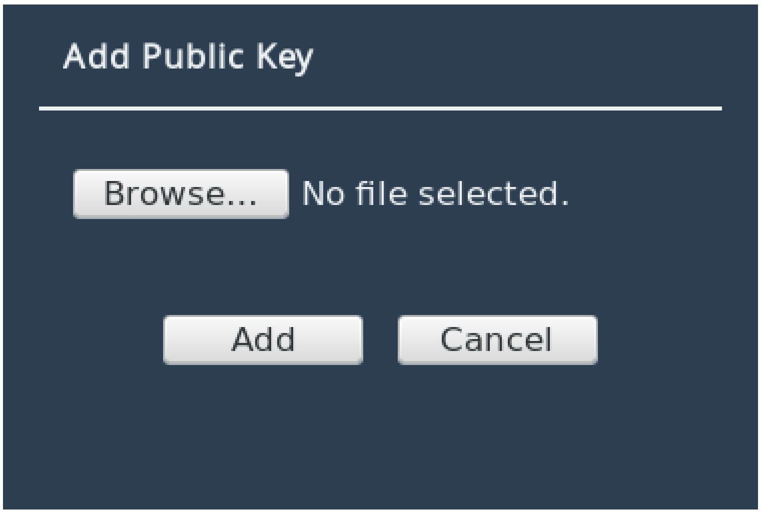
To enable SSH on network interfaces with the "Management" protocol mapped, tick the *Enable SSH* checkbox and click *Save*.

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

3.2.5.1 Managing Public Keys

To log on to a 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.


Add Public Key

No file selected.

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

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

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

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

3.2.5.2 Using SSH

To connect to a 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
```

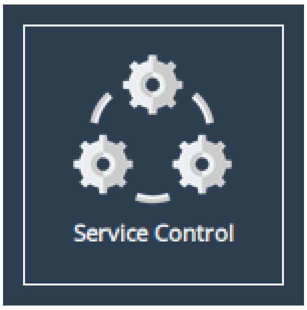
You will then be prompted for the username and password of the Gateway to log in to the configuration console.

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.

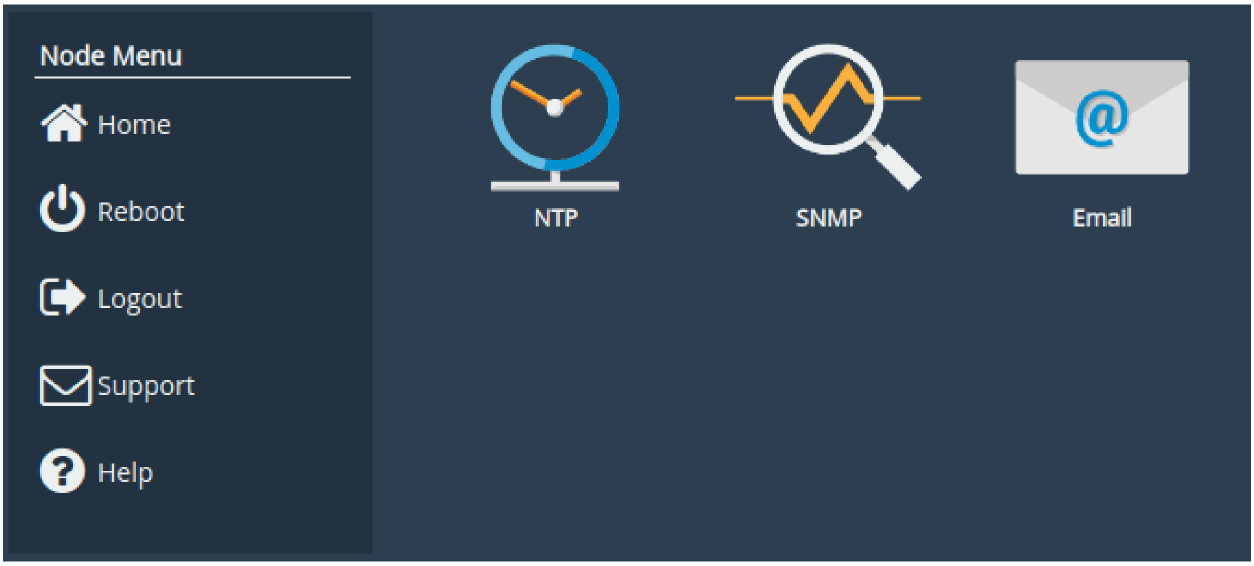
Important: Logging in as root user is disabled on SSH.

3.3 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:



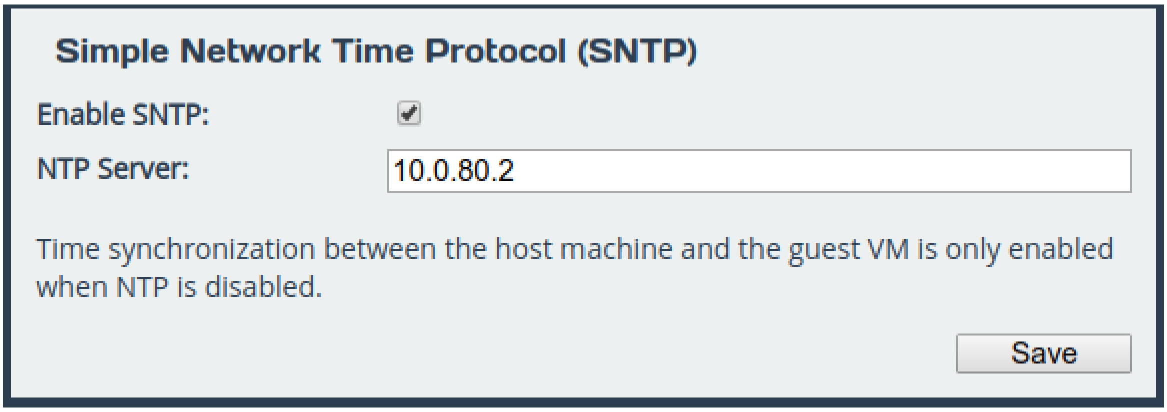
Each link leads to a different service.

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

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

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

3.3.1 Network Time Protocol (NTP)



Simple Network Time Protocol (SNTP)

Enable SNTP: ☑

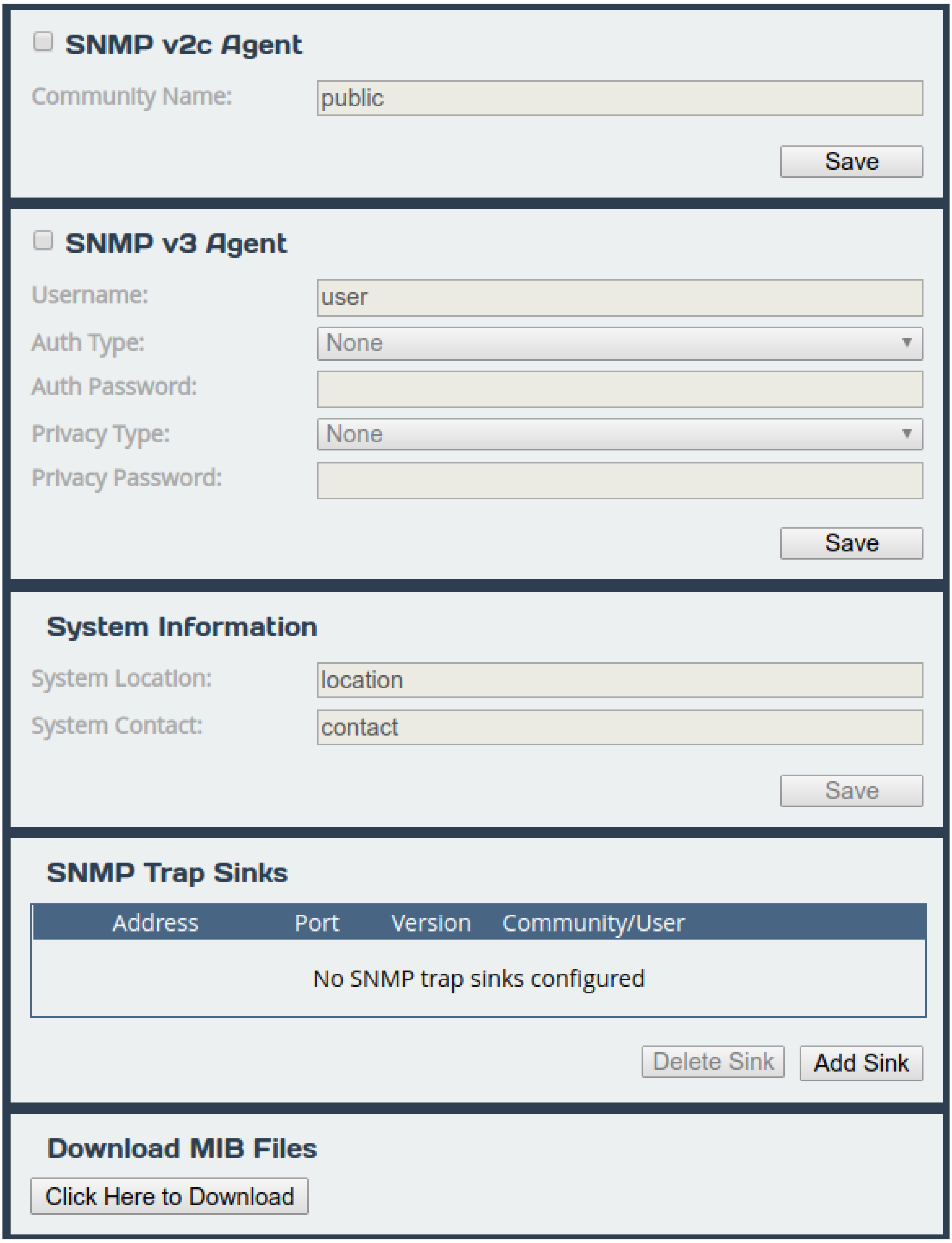
NTP Server: 10.0.80.2

Time synchronization between the host machine and the guest VM is only enabled when NTP is disabled.

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*.

3.3.2 Simple Network Management Protocol (SNMP)



□ **SNMP v2c Agent**

Community Name: public

□ **SNMP v3 Agent**

Username: user

Auth Type: None

Auth Password:

Privacy Type: None

Privacy Password:

System Information

System Location: location

System Contact: contact

SNMP Trap Sinks

Address	Port	Version	Community/User
No SNMP trap sinks configured			

Download MIB Files

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

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

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

3.3.2.1 System Information

The information configured here is accessible over SNMP.

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

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

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

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

3.3.2.3 Add SNMP Trap Sink

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

Port is the port of the trap sink.

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

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

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

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

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

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

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

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

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

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

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

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

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

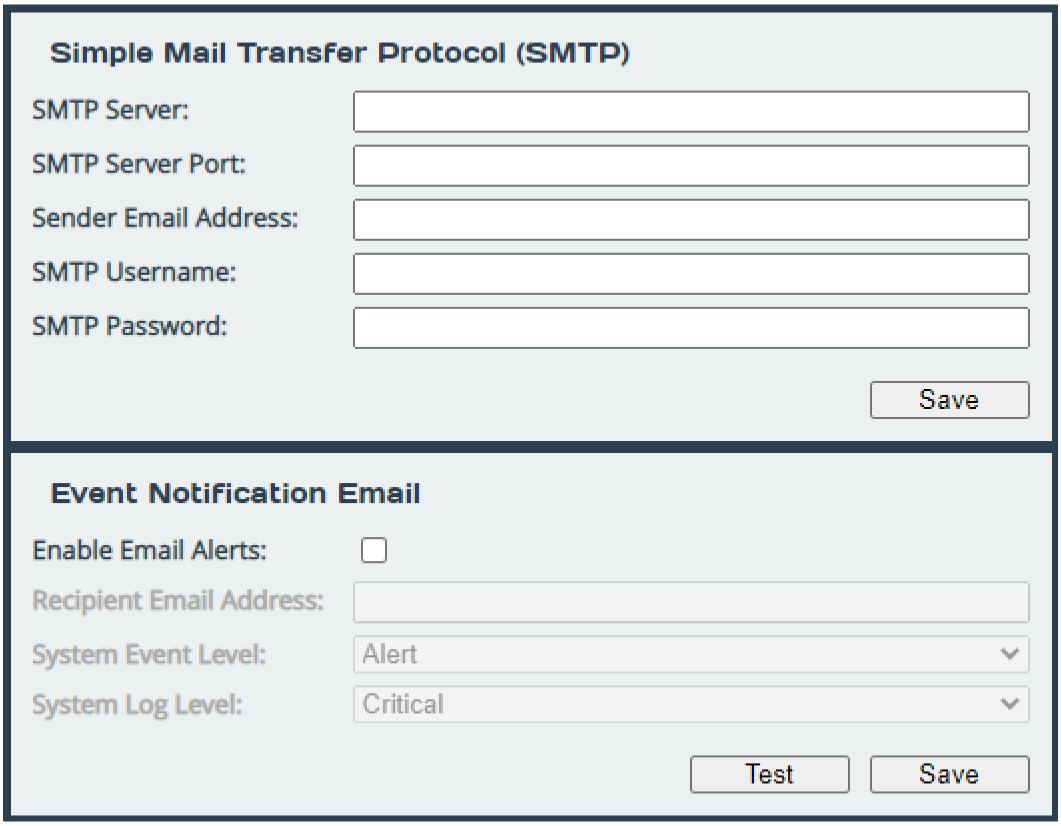
3.3.2.4 Download MIB Files

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

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

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

3.3.3 Email



Simple Mail Transfer Protocol (SMTP)

SMTP Server:

SMTP Server Port:

Sender Email Address:

SMTP Username:

SMTP Password:

Event Notification Email

Enable Email Alerts: □

Recipient Email Address:

System Event Level: Alert

System Log Level: Critical

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.
The server must be reachable from the Gateway's Management interface (or whichever port the default route is set to) on this address. Refer to Section 3.1.2.4: Default Route for information on setting the default route.

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

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

3.3.4 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: Email 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.

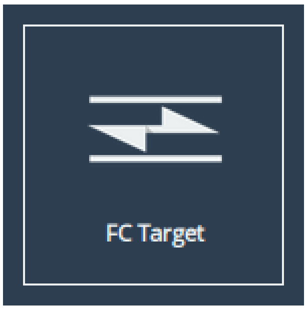
Confirm these settings by clicking *Save*.

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

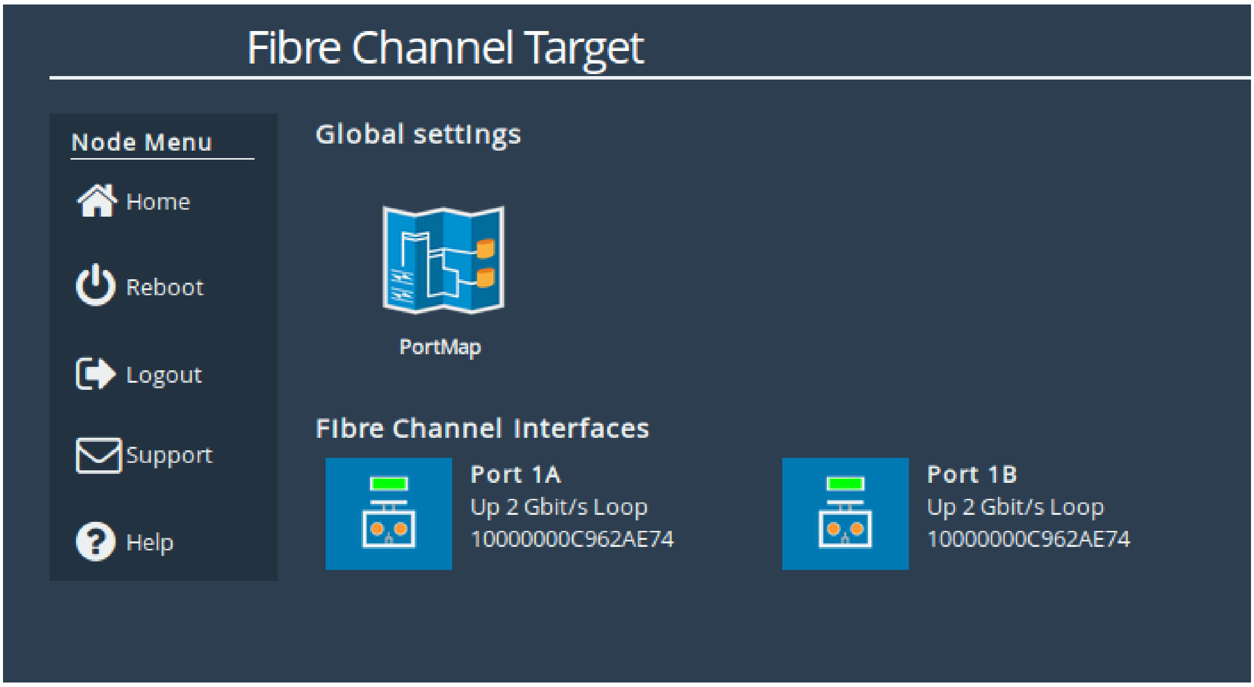
4 Fibre Channel Target Connections

This configuration page allows the user to configure ports designated as Fibre Channel Target interfaces.

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



The web interface will then display the following:



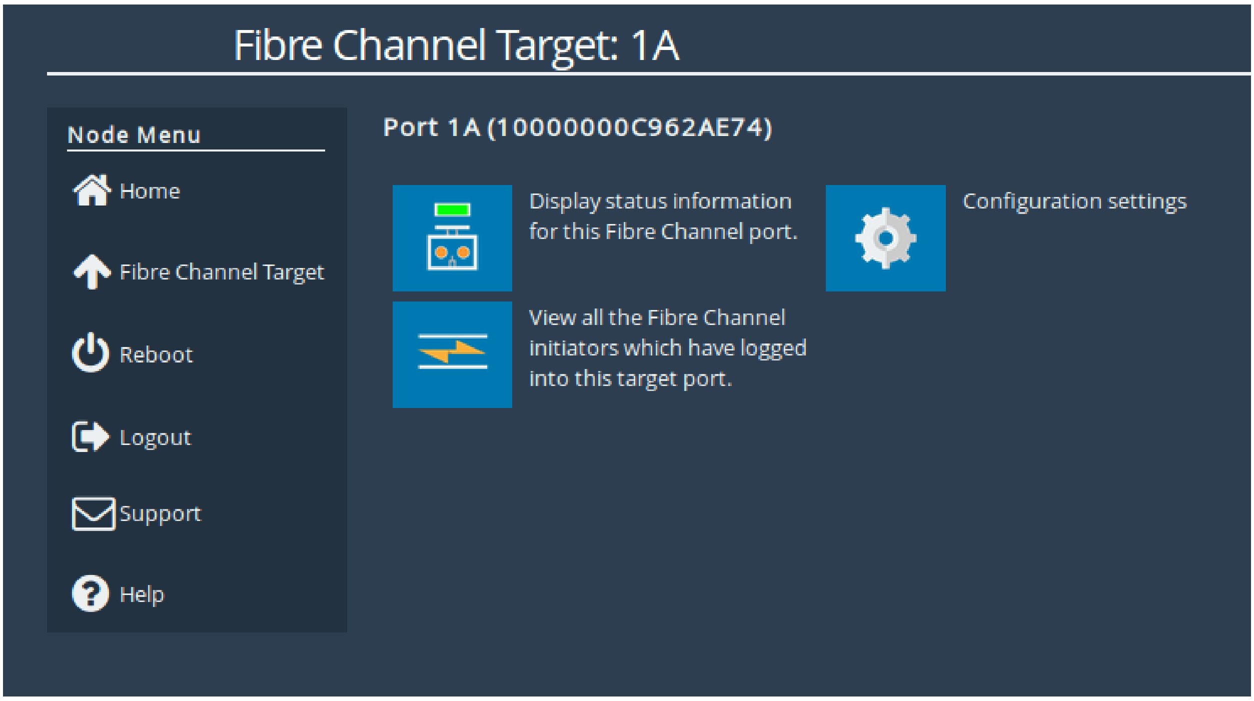
Port 1A
Up 2 Gbit/s Loop
10000000C962AE74

Port 1B
Up 2 Gbit/s Loop
10000000C962AE74

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

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

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



Fibre Channel Target: 1A

Port 1A (10000000C962AE74)

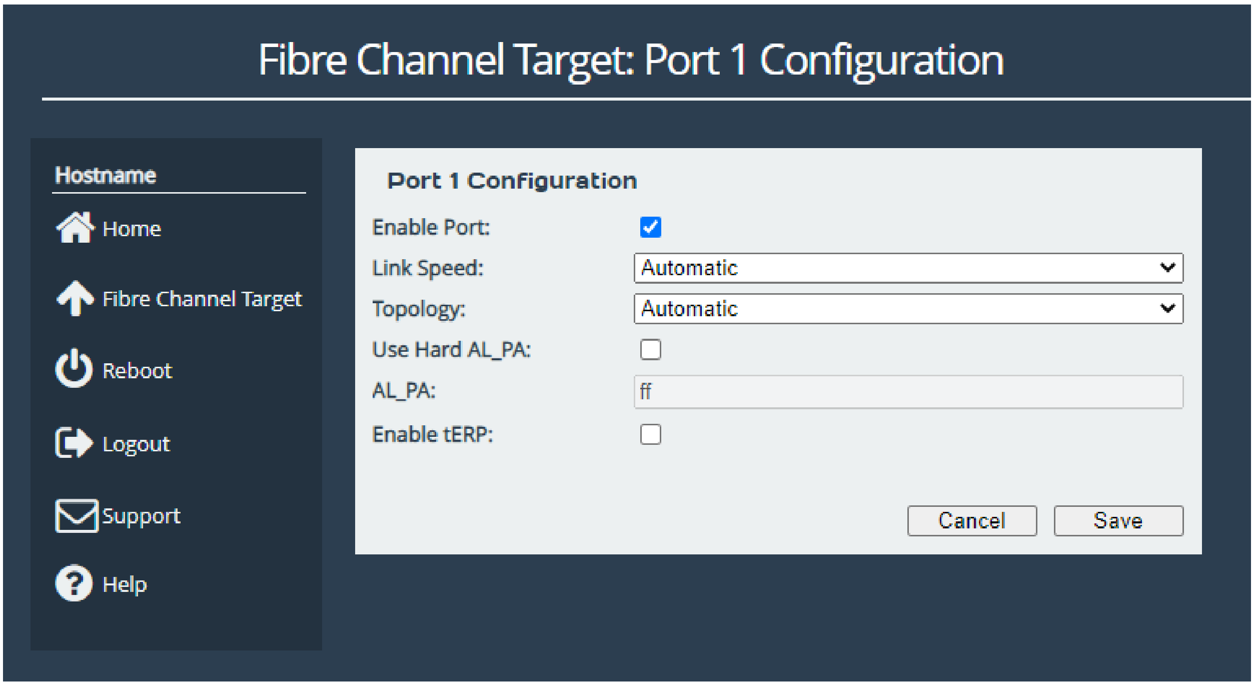
Display status information for this Fibre Channel port.

Configuration settings

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

4.1 Port Configuration

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



Fibre Channel Target: Port 1 Configuration

Port 1 Configuration

Enable Port: ☑

Link Speed: Automatic

Topology: Automatic

Use Hard AL_PA: □

AL_PA: ff

Enable tERP: □

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

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

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

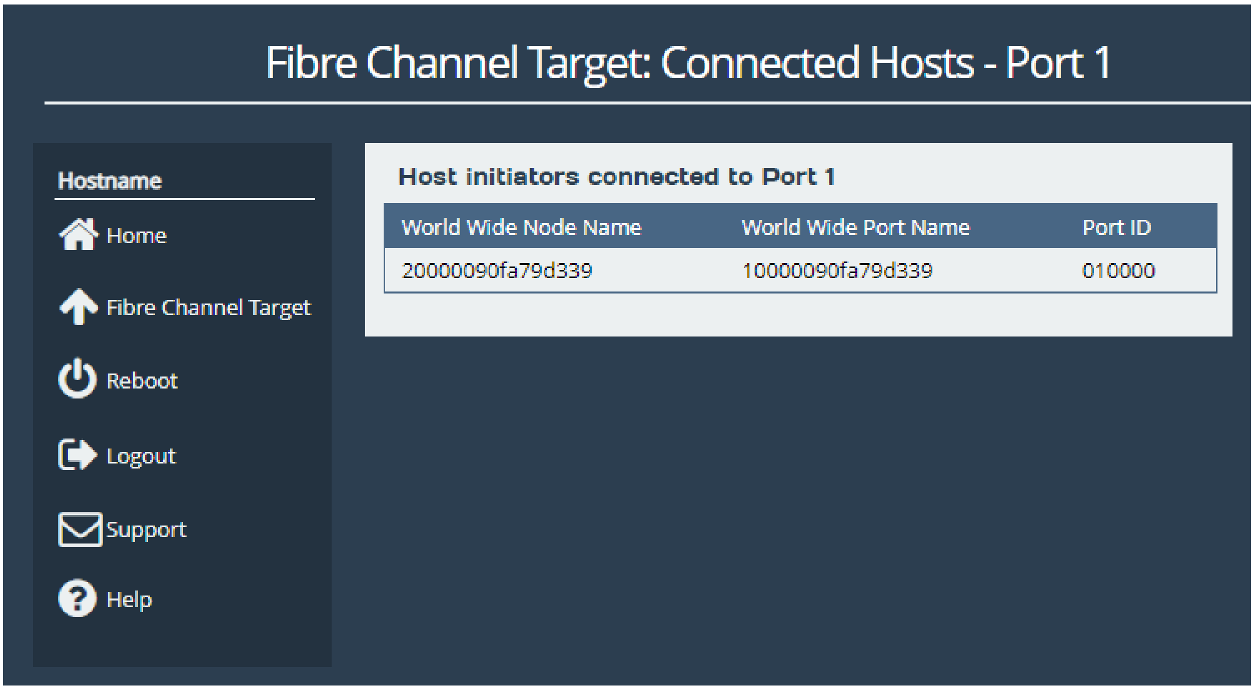
Note: It is recommended to leave *Hard AL_PA* unchecked unless you are conversant with the lower levels of the Fibre Channel protocol, as certain AL_PA addresses are reserved.

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

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

4.2 Connected Hosts

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



Fibre Channel Target: Connected Hosts - Port 1

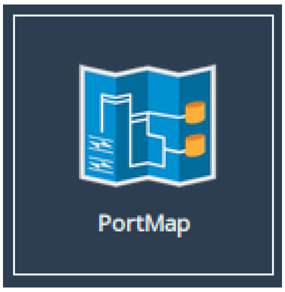
Host initiators connected to Port 1

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

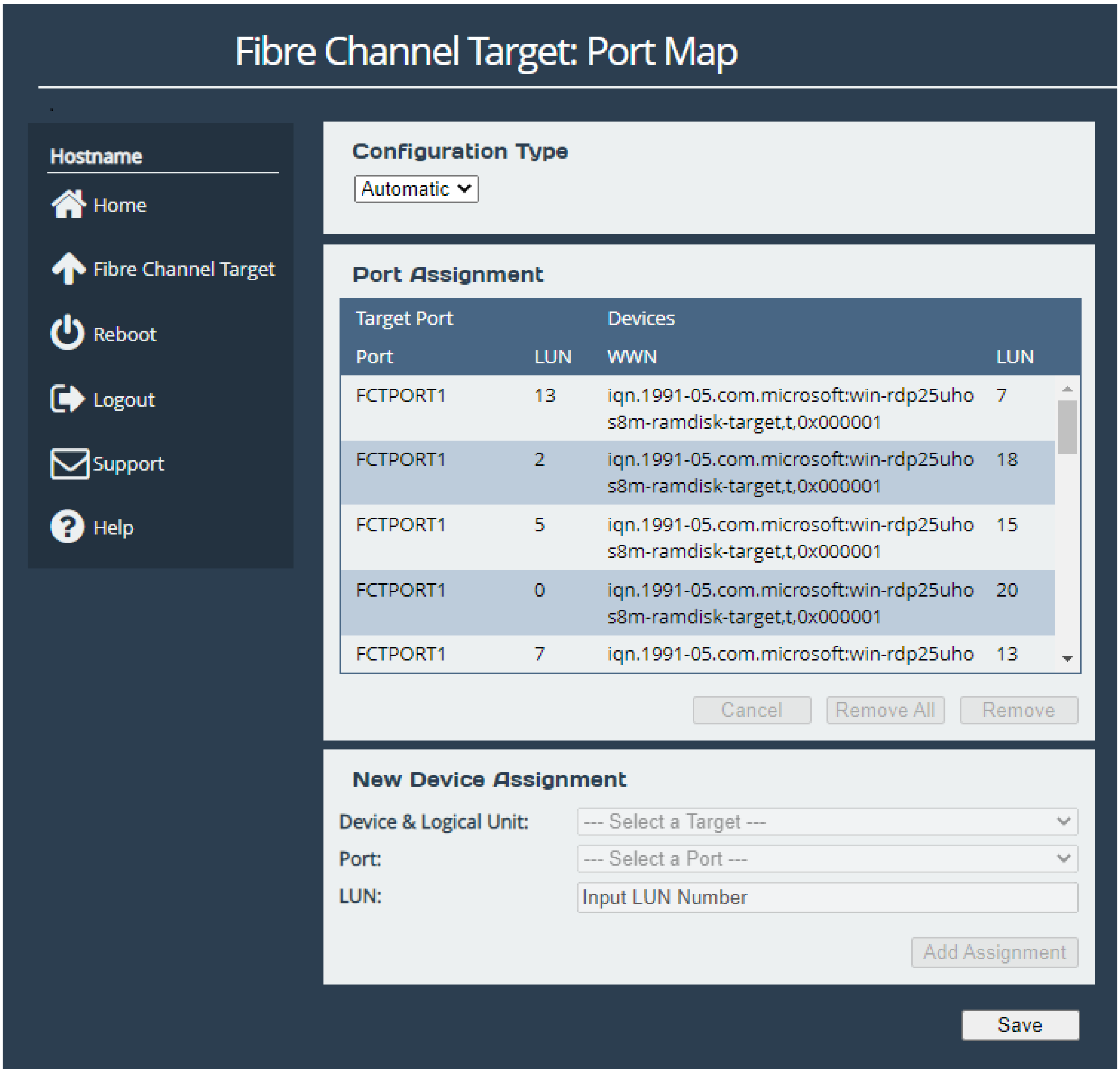
4.3 Port Map

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

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



A screen similar to the following will be displayed:



Fibre Channel Target: Port Map

Configuration Type

Automatic

Port Assignment

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

New Device Assignment

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

Port: --- Select a Port ---

LUN: Input LUN Number

There are two modes of operation:

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

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

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

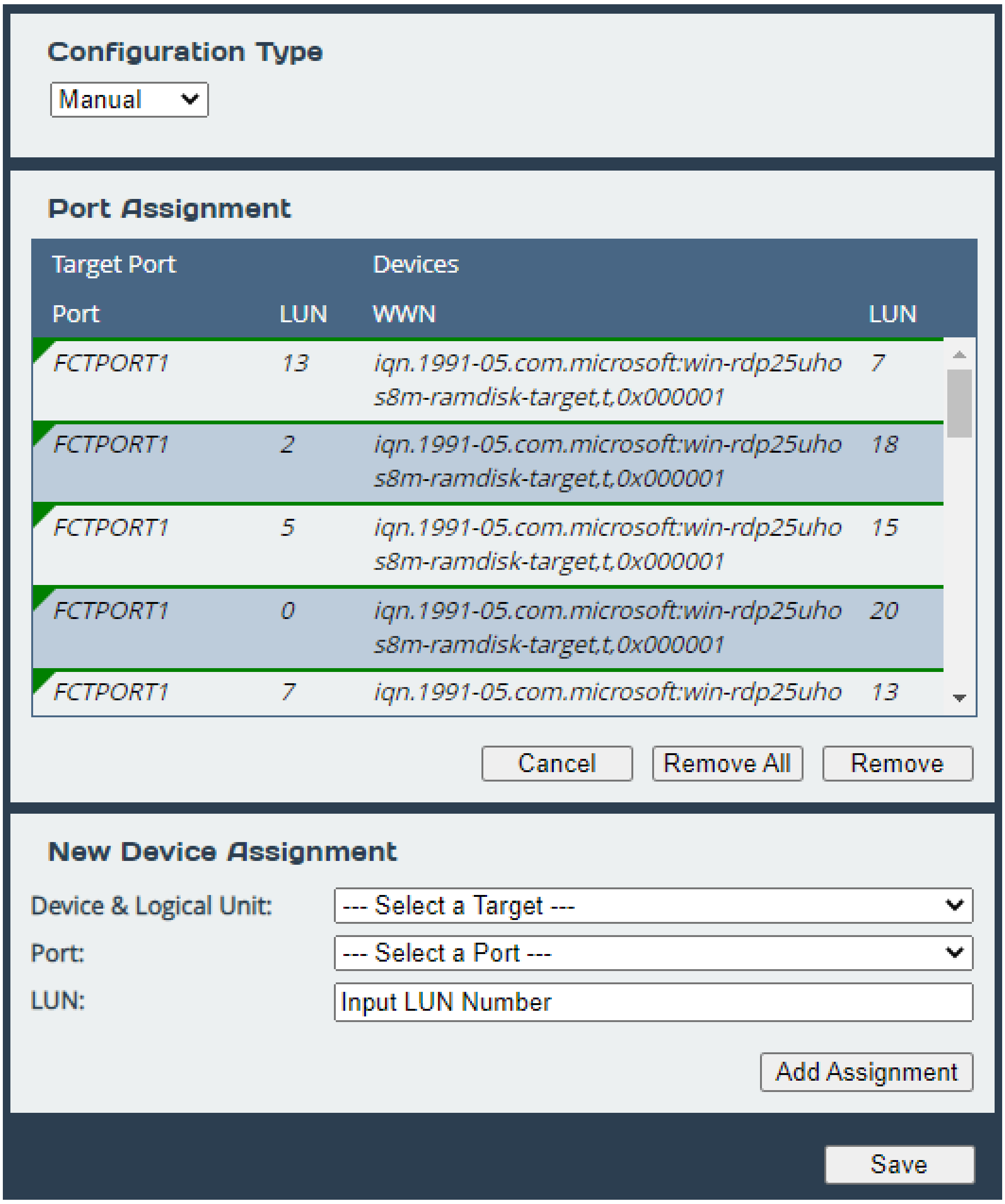
4.3.1 Automatic

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

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

4.3.2 Manual

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



Configuration Type

Manual

Port Assignment

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

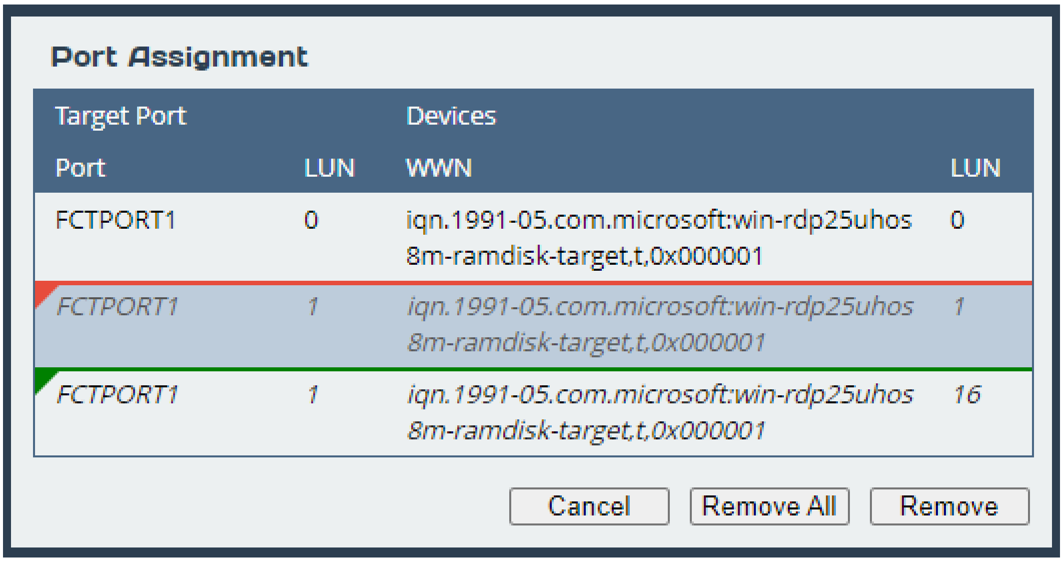
New Device Assignment

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

Port: --- Select a Port ---

LUN: Input LUN Number

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



Port Assignment

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

To assign a target device to a Fibre Channel Port:

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

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

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

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

5 iSCSI Initiator Configuration

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

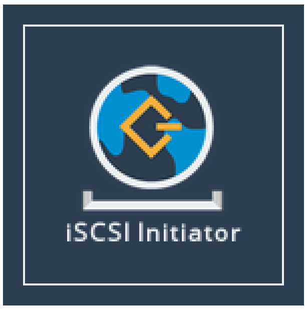
Adding a device to the iSCSI Gateway requires two basic steps:

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

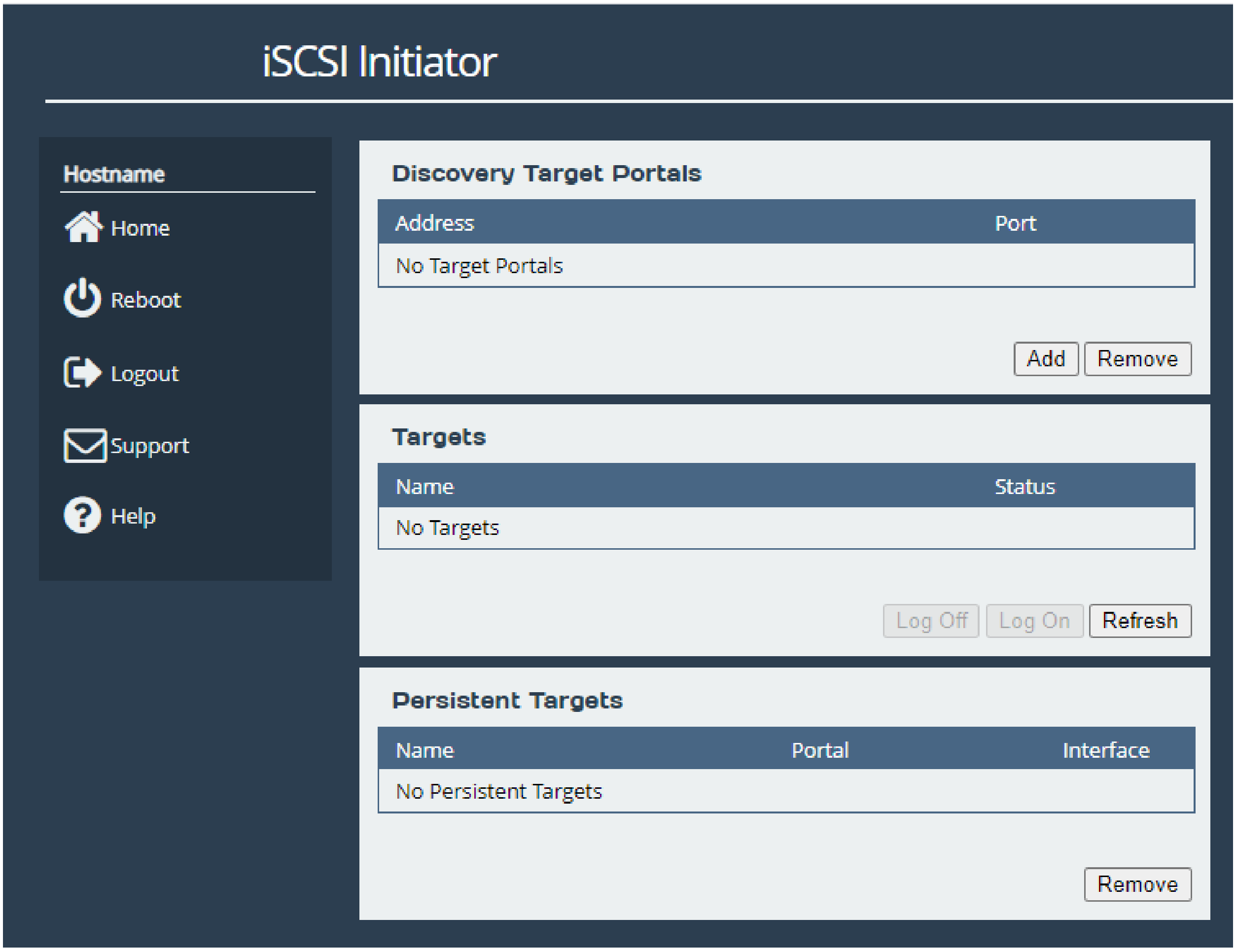
The following sequence is repeated for each device you wish to connect to the iSCSI Gateway.

5.1 Discovering an iSCSI Target

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



The web interface will then display the following:



Discovery Target Portals

Address	Port
No Target Portals	

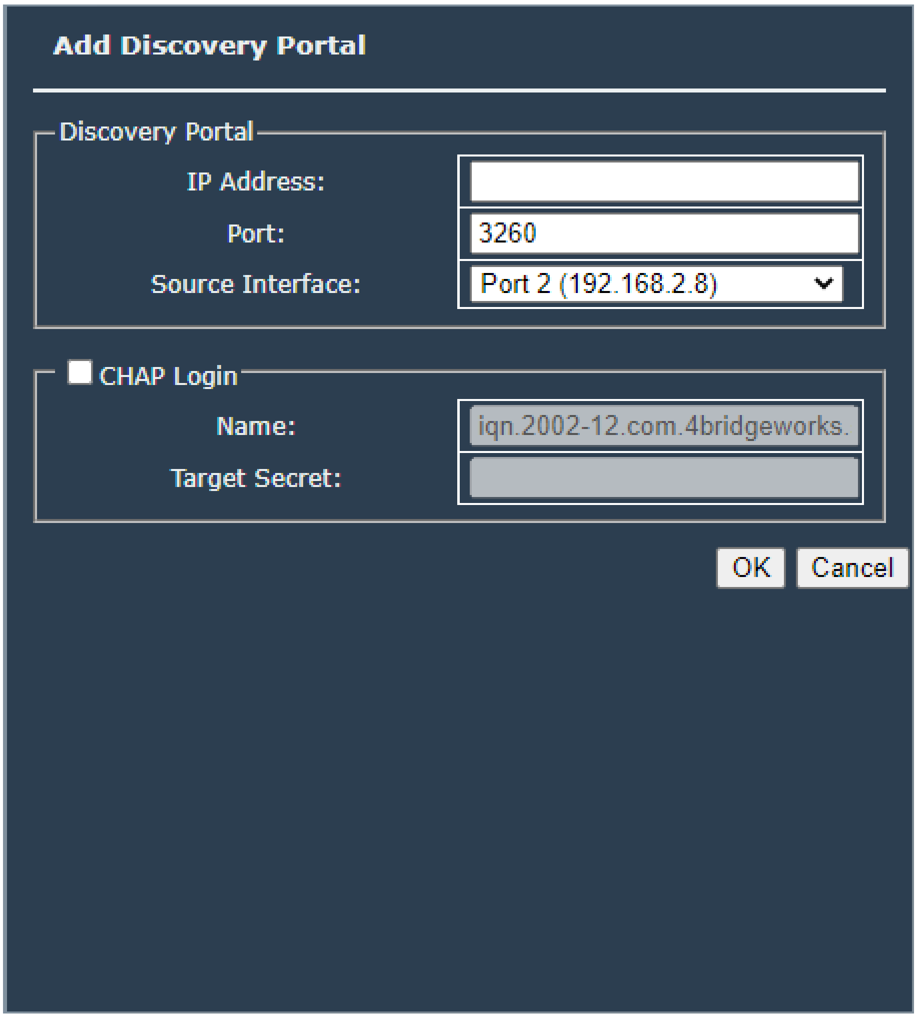
Targets

Name	Status
No Targets	

Persistent Targets

Name	Portal	Interface
No Persistent Targets		

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



Add Discovery Portal

Discovery Portal

IP Address:

Port: 3260

Source Interface: Port 2 (192.168.2.8)

□ CHAP Login

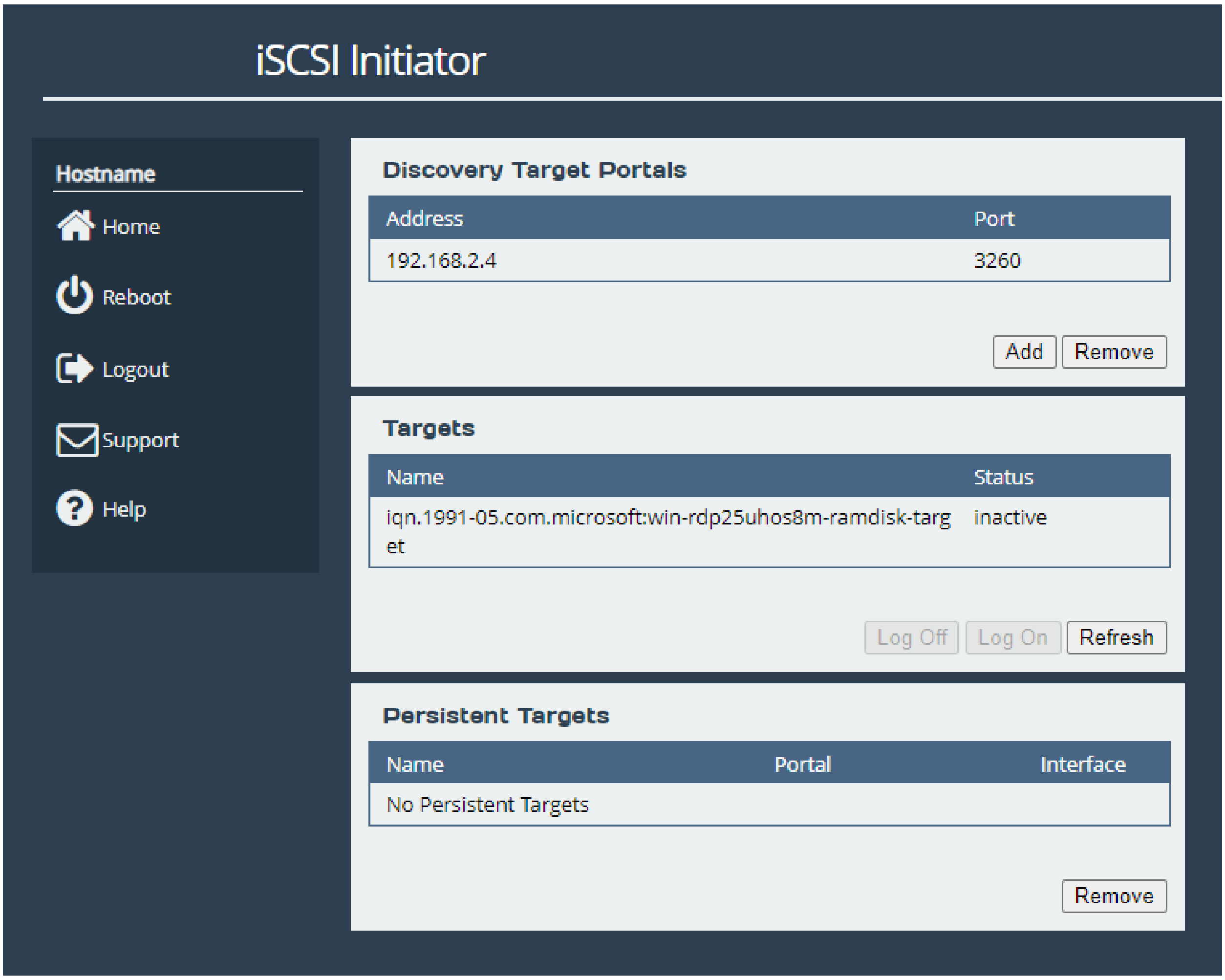
Name: iqn.2002-12.com.4bridgeworks.

Target Secret:

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

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

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



Discovery Target Portals

Address	Port
192.168.2.4	3260

Targets

Name	Status
iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target	inactive

Persistent Targets

Name	Portal	Interface
No Persistent Targets		

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

5.2 Removing an iSCSI Discovery Portal

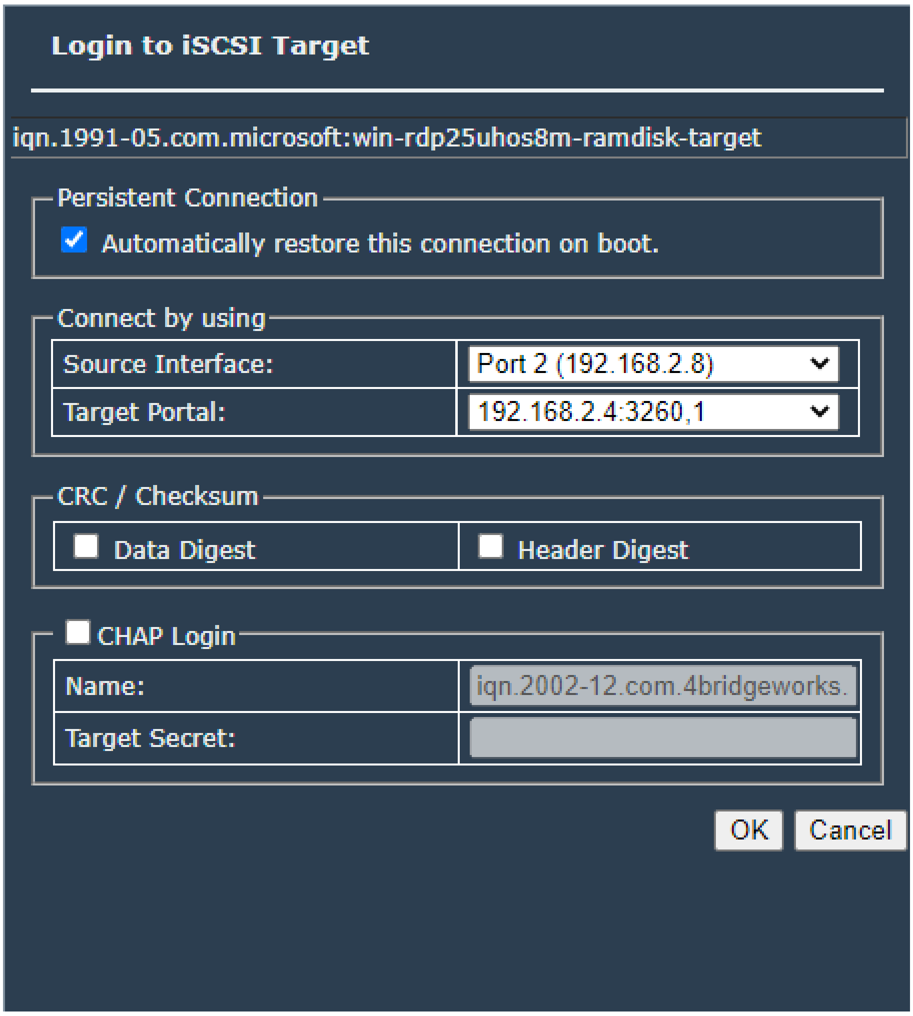
From the *Discovery Target Portals* list select the IP address of the target portal you wish to remove. The background colour of the IP address will change to yellow. Click the *Remove* button, and the following message will appear:

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

Click the *OK* button to confirm.

5.3 Log On to an iSCSI Target

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



Login to iSCSI Target

iqn.1991-05.com.microsoft:win-rdp25uhos8m-ramdisk-target

Persistent Connection

☑ Automatically restore this connection on boot.

Connect by using

Source Interface:	Port 2 (192.168.2.8)
Target Portal:	192.168.2.4:3260,1

CRC / Checksum

☐ Data Digest ☐ Header Digest

☐ CHAP Login

Name:	iqn.2002-12.com.4bridgeworks.
Target Secret:	

5.3.1 Persistent Connection

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

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

5.3.2 CRC/Checksum

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

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

When Header Digest is enabled, the system performs a checksum over each iSCSI PDU's header part and verifies using the CRC32C algorithm. This increases data integrity.

5.3.3 CHAP Login

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

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

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

5.4 Log Off an iSCSI Session

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

“Are you sure you want to Log Off?”

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

5.5 Refresh Targets

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

5.6 Remove Persistent Target

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

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

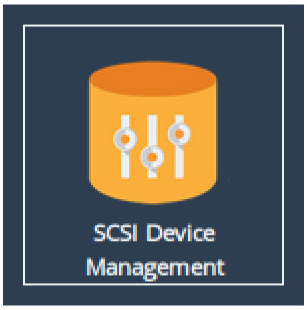
Click the *OK* button if you wish to stop the iSCSI session from restoring on reboot.

6 SCSI Device Management

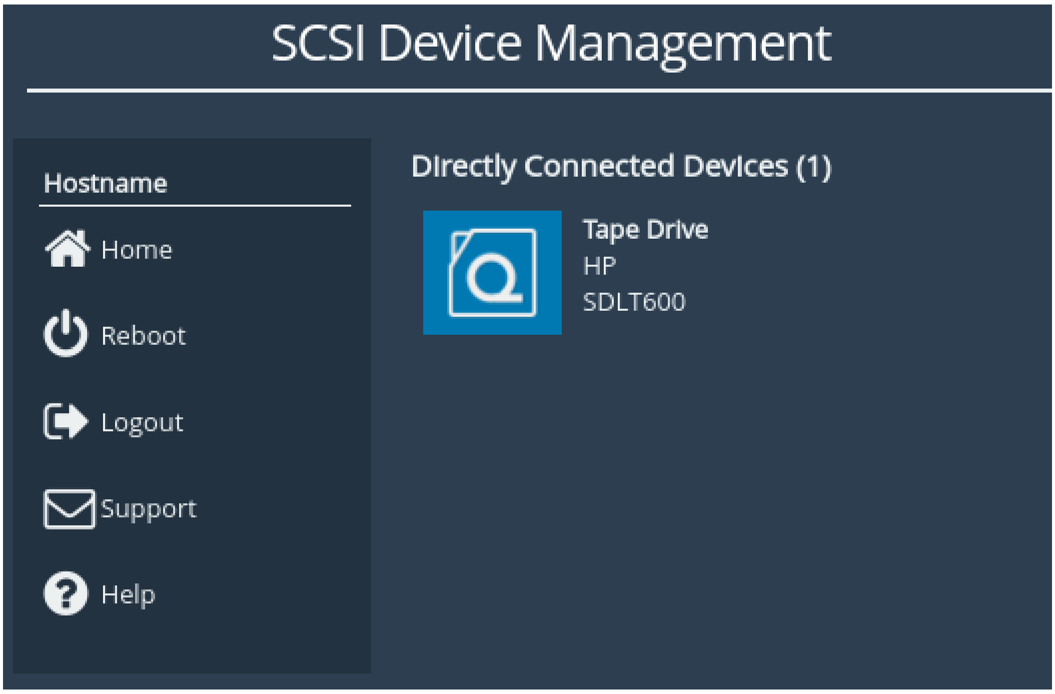
This page allows you to view details of devices connected to the FCE.

6.1 Viewing Attached Devices

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



The web interface will then display the following:

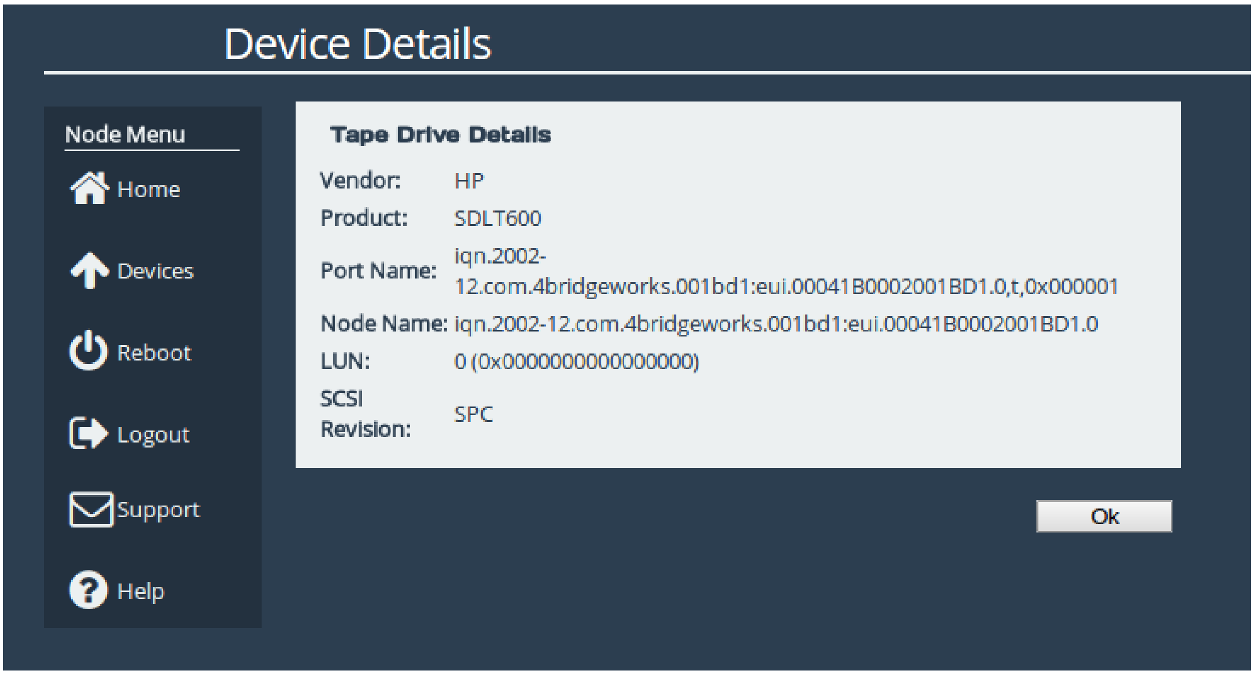


Directly Connected Devices (1)

Tape Drive
HP
SDLT600

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

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



Tape Drive Details

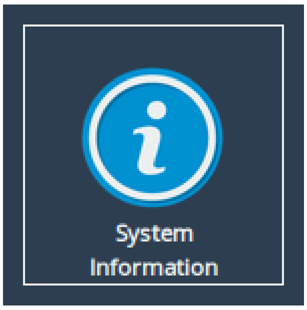
Vendor:	HP
Product:	SDLT600
Port Name:	iqn.2002-12.com.4bridgeworks.001bd1:eui.00041B0002001BD1.0,t,0x000001
Node Name:	iqn.2002-12.com.4bridgeworks.001bd1:eui.00041B0002001BD1.0
LUN:	0 (0x0000000000000000)
SCSI Revision:	SPC

7 Bridge Maintenance

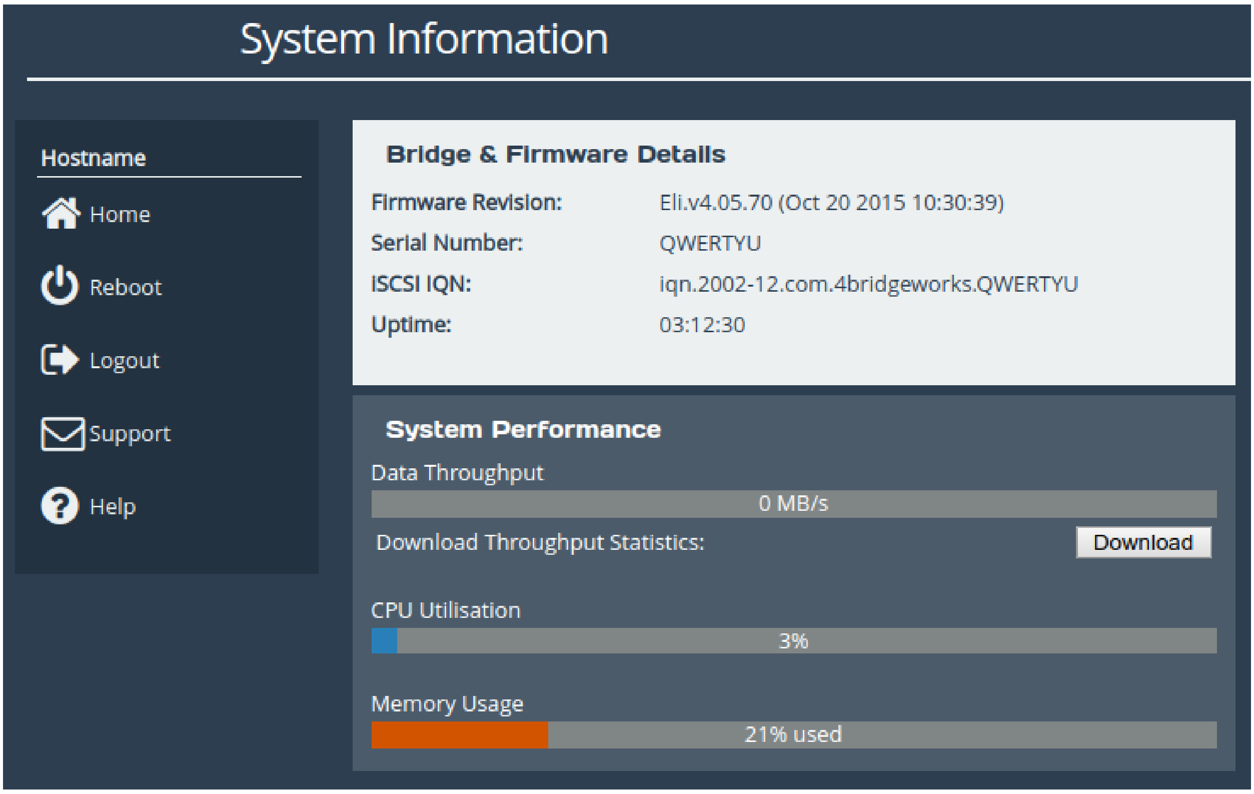
The following section describes the various pages that are available to the administrator to monitor performance and maintain the Gateway.

7.1 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:



System Information

Bridge & Firmware Details

Firmware Revision: Eli.v4.05.70 (Oct 20 2015 10:30:39)
Serial Number: QWERTYU
ISCSI IQN: iqn.2002-12.com.4bridgeworks.QWERTYU
Uptime: 03:12:30

System Performance

Data Throughput
0 MB/s

Download Throughput Statistics: Download

CPU Utilisation
3%

Memory Usage
21% used

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 FCE.

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

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

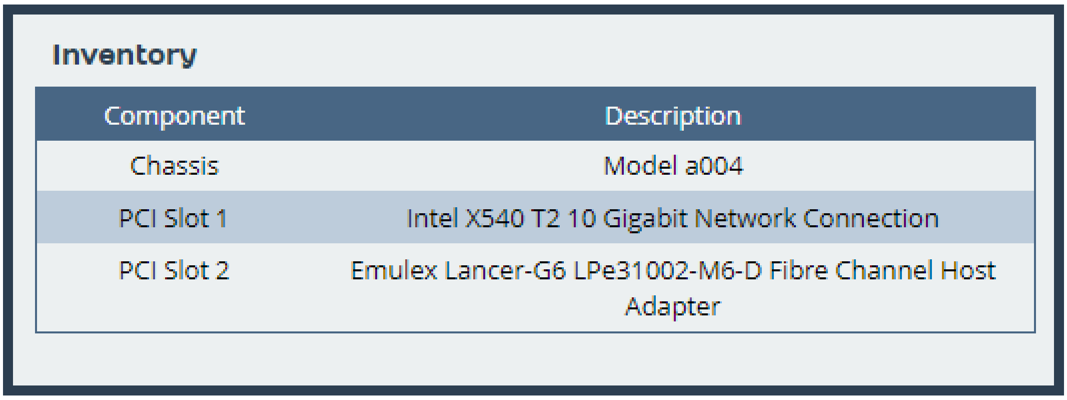
The *System Performance* section contains three meters which provide an approximation of the following performance parameters:

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

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

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

The following section will also appear on this page:



Inventory

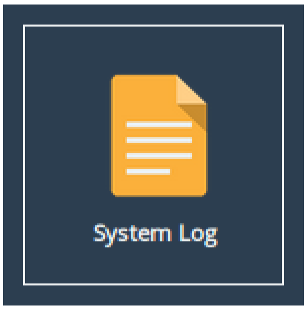
Component	Description
Chassis	Model a004
PCI Slot 1	Intel X540 T2 10 Gigabit Network Connection
PCI Slot 2	Emulex Lancer-G6 LPe31002-M6-D Fibre Channel Host Adapter

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

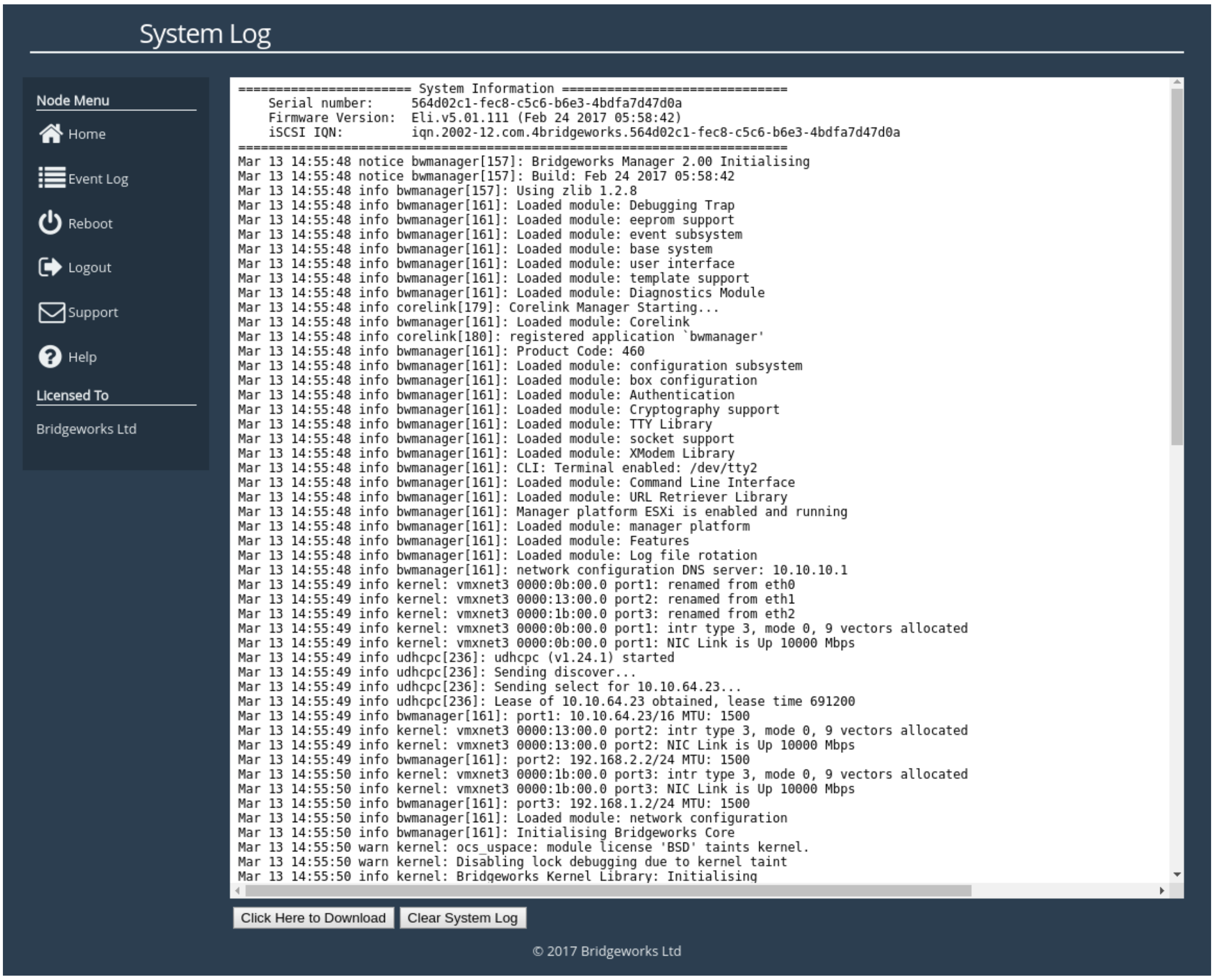
7.2 System Log

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:



```
======================= System Information ===============================
    Serial number:     564d02c1-fec8-c5c6-b6e3-4bdfa7d47d0a
    Firmware Version:  Eli.v5.01.111 (Feb 24 2017 05:58:42)
    iSCSI IQN:         iqn.2002-12.com.4bridgeworks.564d02c1-fec8-c5c6-b6e3-4bdfa7d47d0a
==========================================================================
Mar 13 14:55:48 notice bwmanager[157]: Bridgeworks Manager 2.00 Initialising
Mar 13 14:55:48 notice bwmanager[157]: Build: Feb 24 2017 05:58:42
Mar 13 14:55:48 info bwmanager[157]: Using zlib 1.2.8
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Debugging Trap
Mar 13 14:55:48 info bwmanager[161]: Loaded module: eeprom support
Mar 13 14:55:48 info bwmanager[161]: Loaded module: event subsystem
Mar 13 14:55:48 info bwmanager[161]: Loaded module: base system
Mar 13 14:55:48 info bwmanager[161]: Loaded module: user interface
Mar 13 14:55:48 info bwmanager[161]: Loaded module: template support
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Diagnostics Module
Mar 13 14:55:48 info corelink[179]: Corelink Manager Starting...
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Corelink
Mar 13 14:55:48 info corelink[180]: registered application `bwmanager'
Mar 13 14:55:48 info bwmanager[161]: Product Code: 460
Mar 13 14:55:48 info bwmanager[161]: Loaded module: configuration subsystem
Mar 13 14:55:48 info bwmanager[161]: Loaded module: box configuration
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Authentication
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Cryptography support
Mar 13 14:55:48 info bwmanager[161]: Loaded module: TTY Library
Mar 13 14:55:48 info bwmanager[161]: Loaded module: socket support
Mar 13 14:55:48 info bwmanager[161]: Loaded module: XModem Library
Mar 13 14:55:48 info bwmanager[161]: CLI: Terminal enabled: /dev/tty2
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Command Line Interface
Mar 13 14:55:48 info bwmanager[161]: Loaded module: URL Retriever Library
Mar 13 14:55:48 info bwmanager[161]: Manager platform ESXi is enabled and running
Mar 13 14:55:48 info bwmanager[161]: Loaded module: manager platform
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Features
Mar 13 14:55:48 info bwmanager[161]: Loaded module: Log file rotation
Mar 13 14:55:48 info bwmanager[161]: network configuration DNS server: 10.10.10.1
Mar 13 14:55:49 info kernel: vmxnet3 0000:0b:00.0 port1: renamed from eth0
Mar 13 14:55:49 info kernel: vmxnet3 0000:13:00.0 port2: renamed from eth1
Mar 13 14:55:49 info kernel: vmxnet3 0000:1b:00.0 port3: renamed from eth2
Mar 13 14:55:49 info kernel: vmxnet3 0000:0b:00.0 port1: intr type 3, mode 0, 9 vectors allocated
Mar 13 14:55:49 info kernel: vmxnet3 0000:0b:00.0 port1: NIC Link is Up 10000 Mbps
Mar 13 14:55:49 info udhcpc[236]: udhcpc (v1.24.1) started
Mar 13 14:55:49 info udhcpc[236]: Sending discover...
Mar 13 14:55:49 info udhcpc[236]: Sending select for 10.10.64.23...
Mar 13 14:55:49 info udhcpc[236]: Lease of 10.10.64.23 obtained, lease time 691200
Mar 13 14:55:49 info bwmanager[161]: port1: 10.10.64.23/16 MTU: 1500
Mar 13 14:55:49 info kernel: vmxnet3 0000:13:00.0 port2: intr type 3, mode 0, 9 vectors allocated
Mar 13 14:55:49 info kernel: vmxnet3 0000:13:00.0 port2: NIC Link is Up 10000 Mbps
Mar 13 14:55:49 info bwmanager[161]: port2: 192.168.2.2/24 MTU: 1500
Mar 13 14:55:50 info kernel: vmxnet3 0000:1b:00.0 port3: intr type 3, mode 0, 9 vectors allocated
Mar 13 14:55:50 info kernel: vmxnet3 0000:1b:00.0 port3: NIC Link is Up 10000 Mbps
Mar 13 14:55:50 info bwmanager[161]: port3: 192.168.1.2/24 MTU: 1500
Mar 13 14:55:50 info bwmanager[161]: Loaded module: network configuration
Mar 13 14:55:50 info bwmanager[161]: Initialising Bridgeworks Core
Mar 13 14:55:50 warn kernel: ocs_uspace: module license 'BSD' taints kernel.
Mar 13 14:55:50 warn kernel: Disabling lock debugging due to kernel taint
Mar 13 14:55:50 info kernel: Bridgeworks Kernel Library: Initialising
```

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.

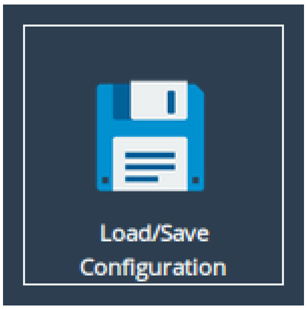
For information on troubleshooting your Gateway, see Chapter 8: Troubleshooting.

7.3 Load/Save Configuration

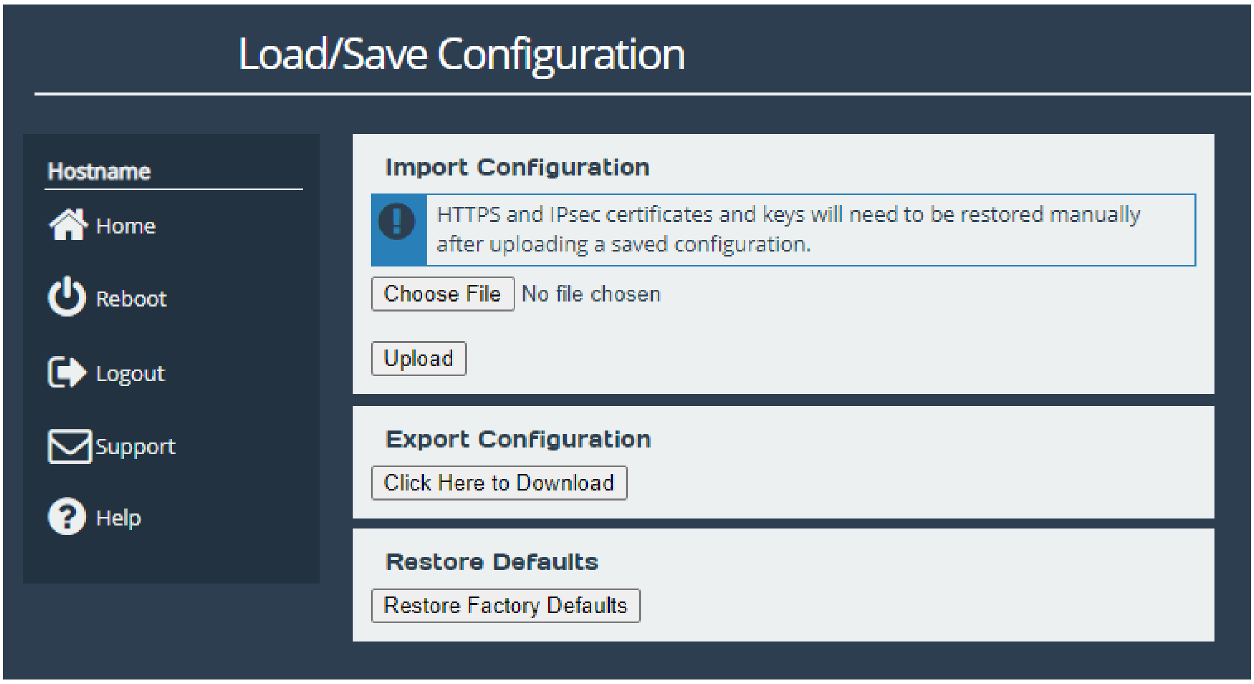
The configuration Load/Save feature allows you to save a copy of the Gateway's configuration to a file and optionally restore back to that configuration at a later time.

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:



Import Configuration

HTTPS and IPsec certificates and keys will need to be restored manually after uploading a saved configuration.

Export Configuration

Restore Defaults

7.3.1 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.

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

7.3.2 Saving the Configuration to Disk

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

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

7.3.3 Restoring to Factory Defaults

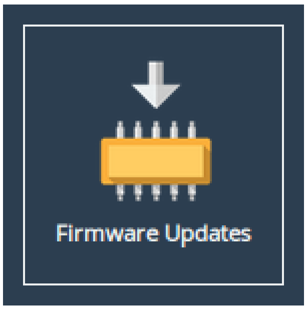
To restore the Gateway to factory defaults, click the *Restore Factory Defaults* button. This resets all configuration parameters including the hostname, IP addresses and passwords. This option is useful to protect sensitive information if a Gateway appliance is ever returned for maintenance.

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

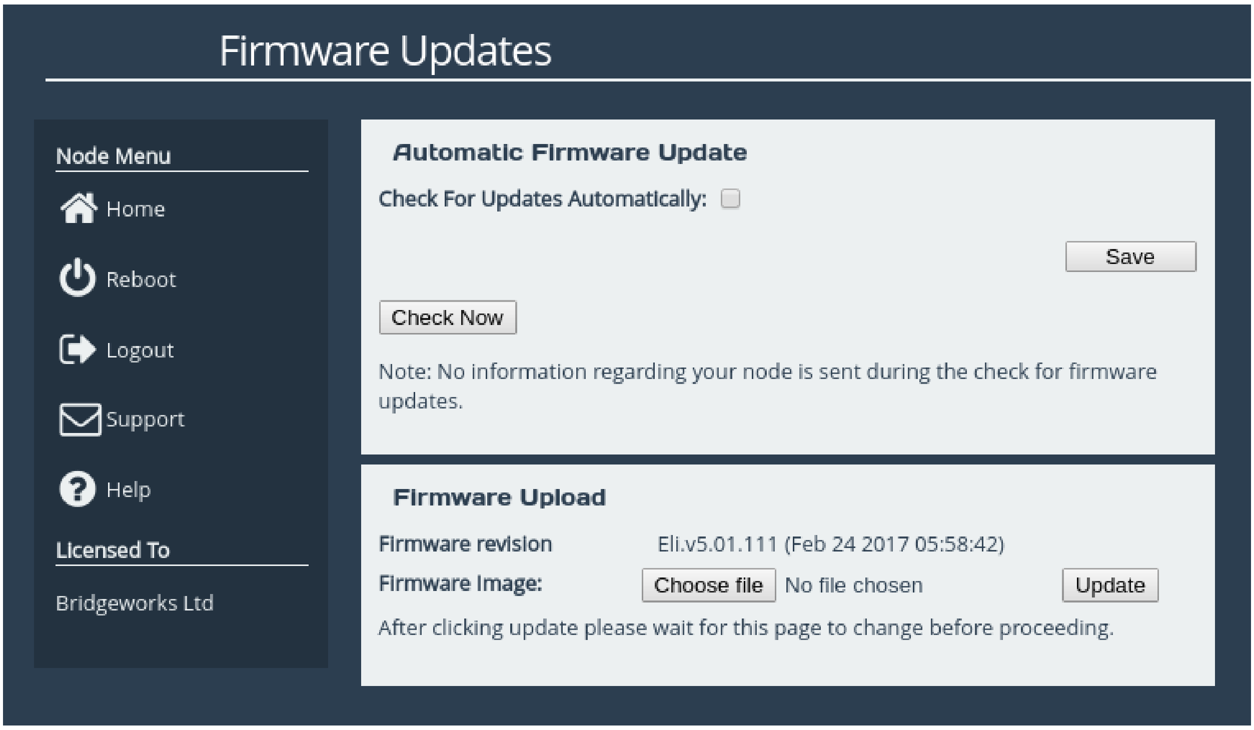
7.4 Firmware Updates

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:



Firmware Updates

Automatic Firmware Update

Check For Updates Automatically: □

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

Firmware Upload

Firmware revision Eli.v5.01.111 (Feb 24 2017 05:58:42)

Firmware Image: No file chosen

After clicking update please wait for this page to change before proceeding.

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.

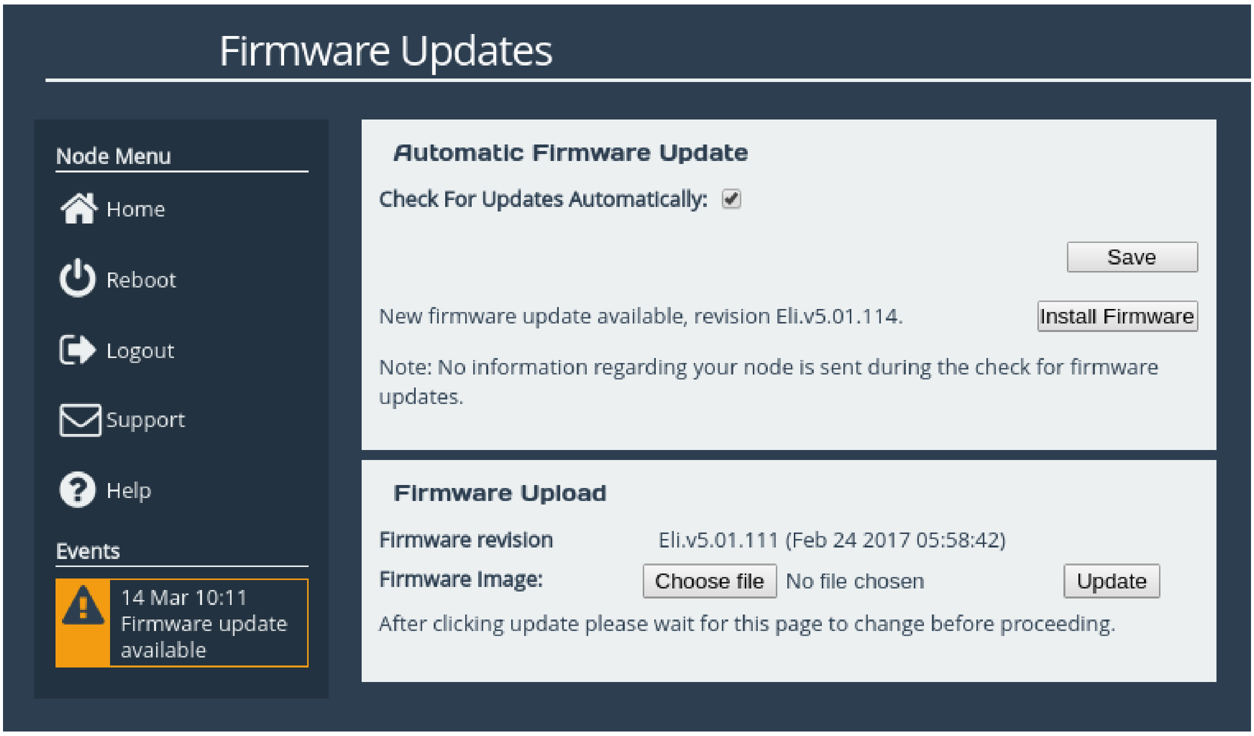
7.4.1 Automatic Firmware Update Checking

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*.



Firmware Updates

14 Mar 10:11 Firmware update available

Automatic Firmware Update

Check For Updates Automatically: ☑

New firmware update available, revision Eli.v5.01.114.

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

Firmware Upload

Firmware revision Eli.v5.01.111 (Feb 24 2017 05:58:42)

Firmware Image: Choose file No file chosen

After clicking update please wait for this page to change before proceeding.

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 FCE.
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.

7.4.2 Updating Firmware Manually

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

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

⚠	Warning: Do not load on a firmware which has an earlier release revision unless you have been instructed to by the Bridgeworks support team. Always ensure that you have the correct firmware for your product. **If in any doubt, please contact Bridgeworks support. See Appendix C: 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 FCE.
3. When the label above the progress bar changes to *Progress*, you can navigate away from this page and the installation will continue.

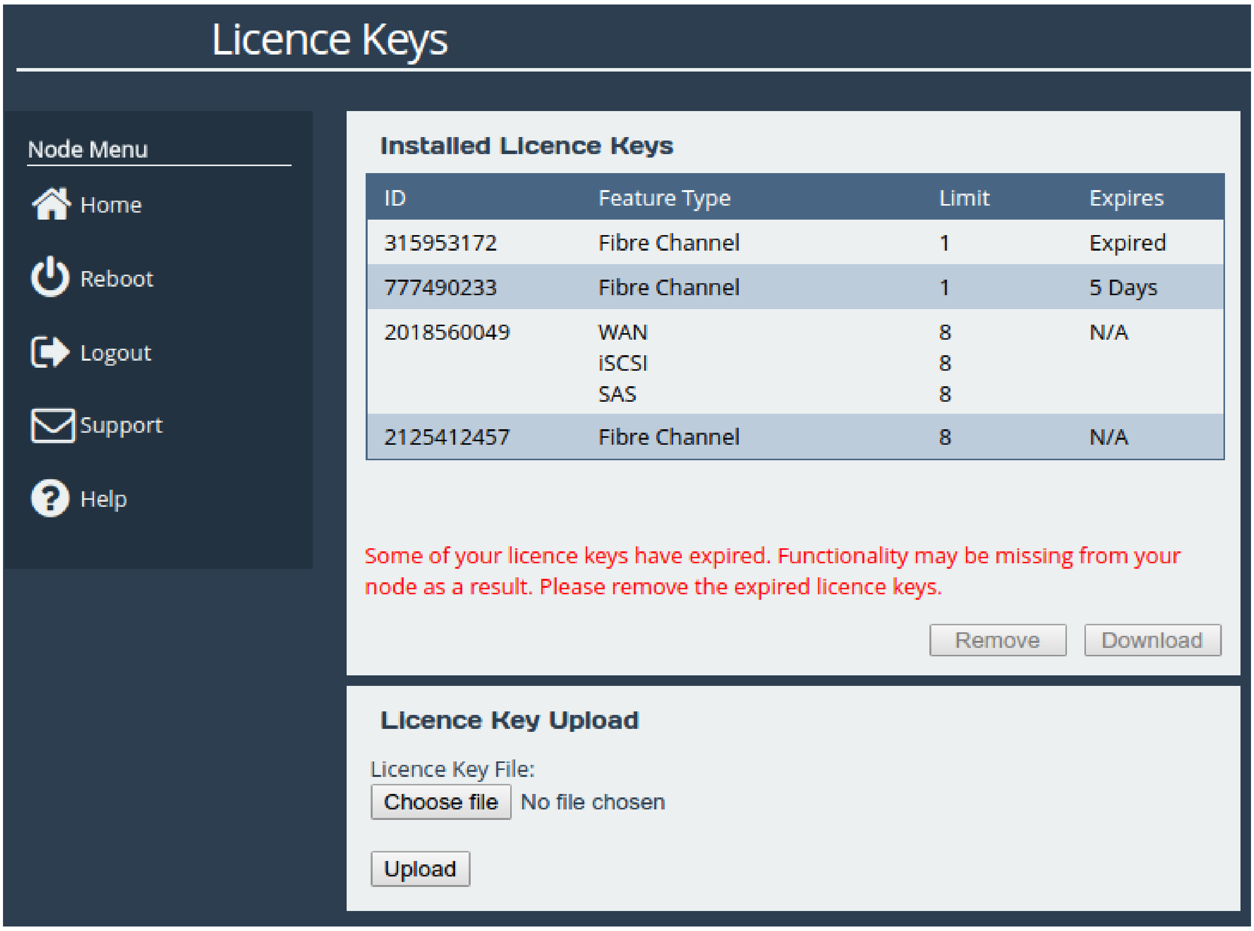
Updating the firmware will take a few minutes. After the update is complete, a notification will appear under the *Bridge Menu*, indicating that a system reboot is necessary. To reboot the Gateway, click on the *Reboot* button located in the *Bridge Menu* at the left side of the web interface.

7.5 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:



Installed Licence Keys

ID	Feature Type	Limit	Expires
315953172	Fibre Channel	1	Expired
777490233	Fibre Channel	1	5 Days
2018560049	WAN iSCSI SAS	8 8 8	N/A
2125412457	Fibre Channel	8	N/A

Some of your licence keys have expired. Functionality may be missing from your node as a result. Please remove the expired licence keys.

Licence Key Upload

Licence Key File:

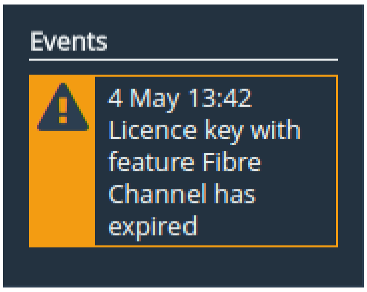
The *Installed Licence Keys* table displays the installed licence keys with the following information:

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.



4 May 13:42
Licence key with feature Fibre Channel has expired

7.5.1 Uploading a Licence Key

To upload a licence key:

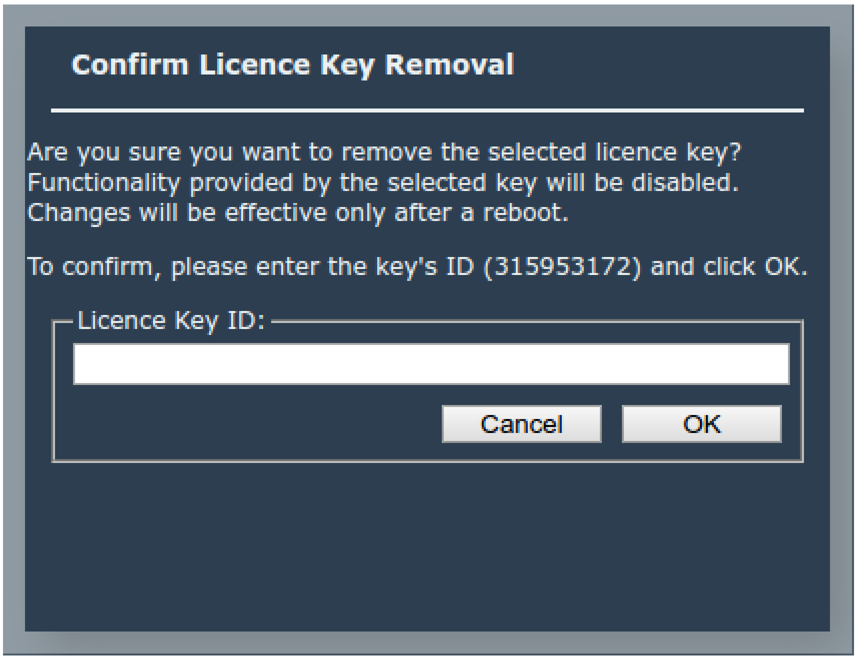
1. Click the *Choose file* button in the *Licence Key Upload* section.
2. Locate and select the licence key to upload.
3. Click the *Upload* button.

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

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

7.5.2 Removing a Licence Key

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



Confirm Licence Key Removal

Are you sure you want to remove the selected licence key?
Functionality provided by the selected key will be disabled.
Changes will be effective only after a reboot.

To confirm, please enter the key's ID (315953172) and click OK.

Licence Key ID:

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.

7.5.3 Downloading a Licence Key

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

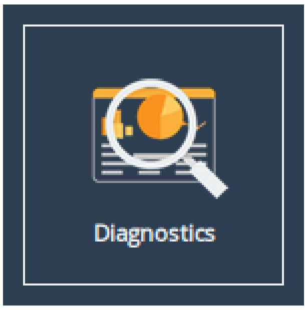
7.6 Diagnostics

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

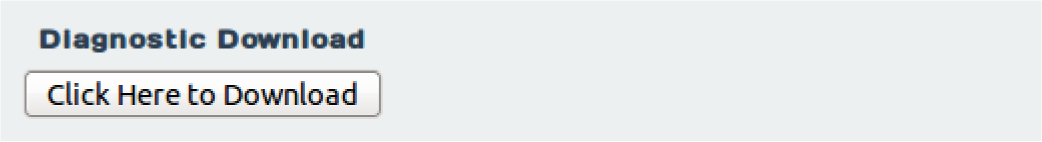
Important: If an issue arises with your FCE, check Chapter 8: Troubleshooting for information on how the issue may be resolved.

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.



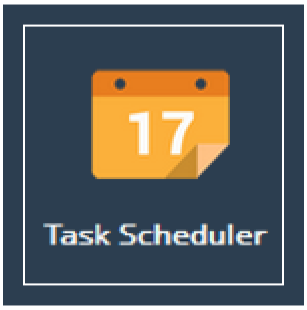
This will cause the FCE to collect data regarding various modules and store them in a single file. Once this process is complete, a download for "diagnostics.bin" will begin.

7.7 Task Scheduler

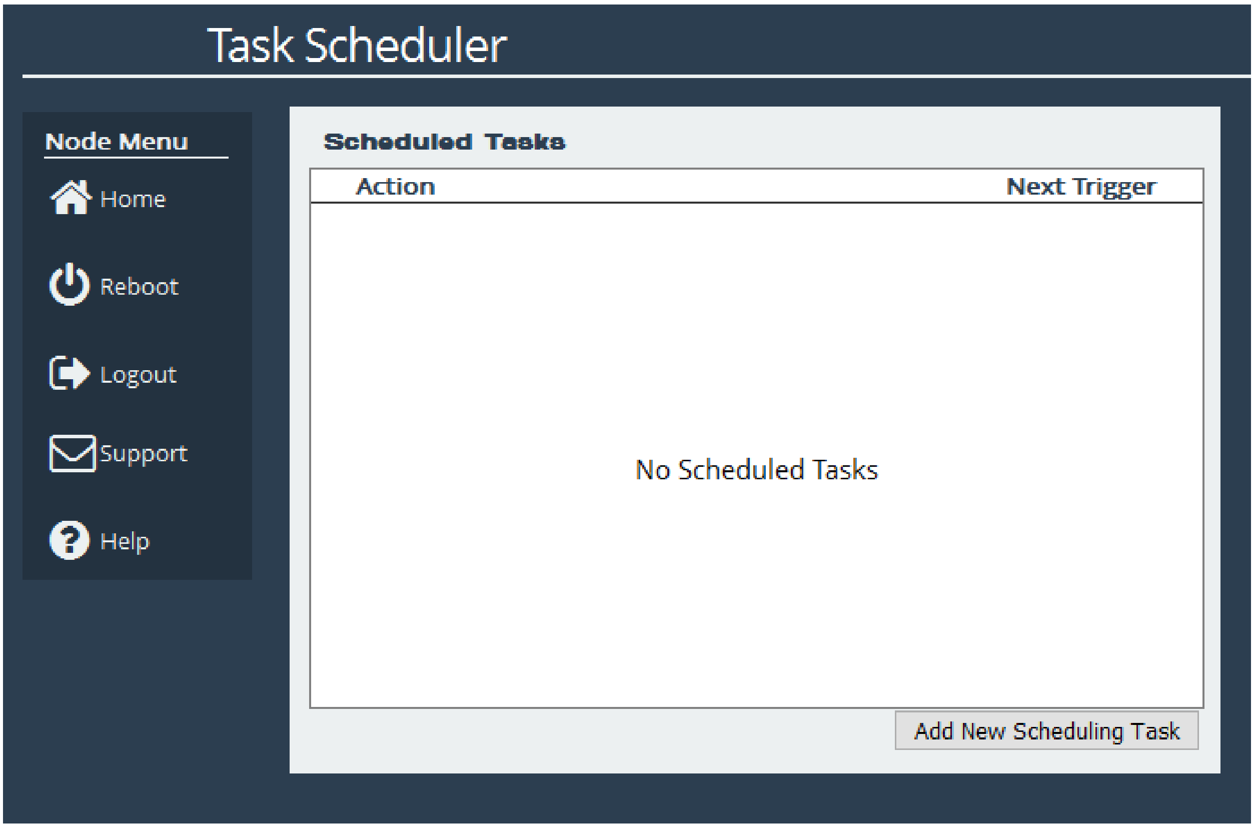
This page allows the administrator to schedule tasks with the following action:

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:



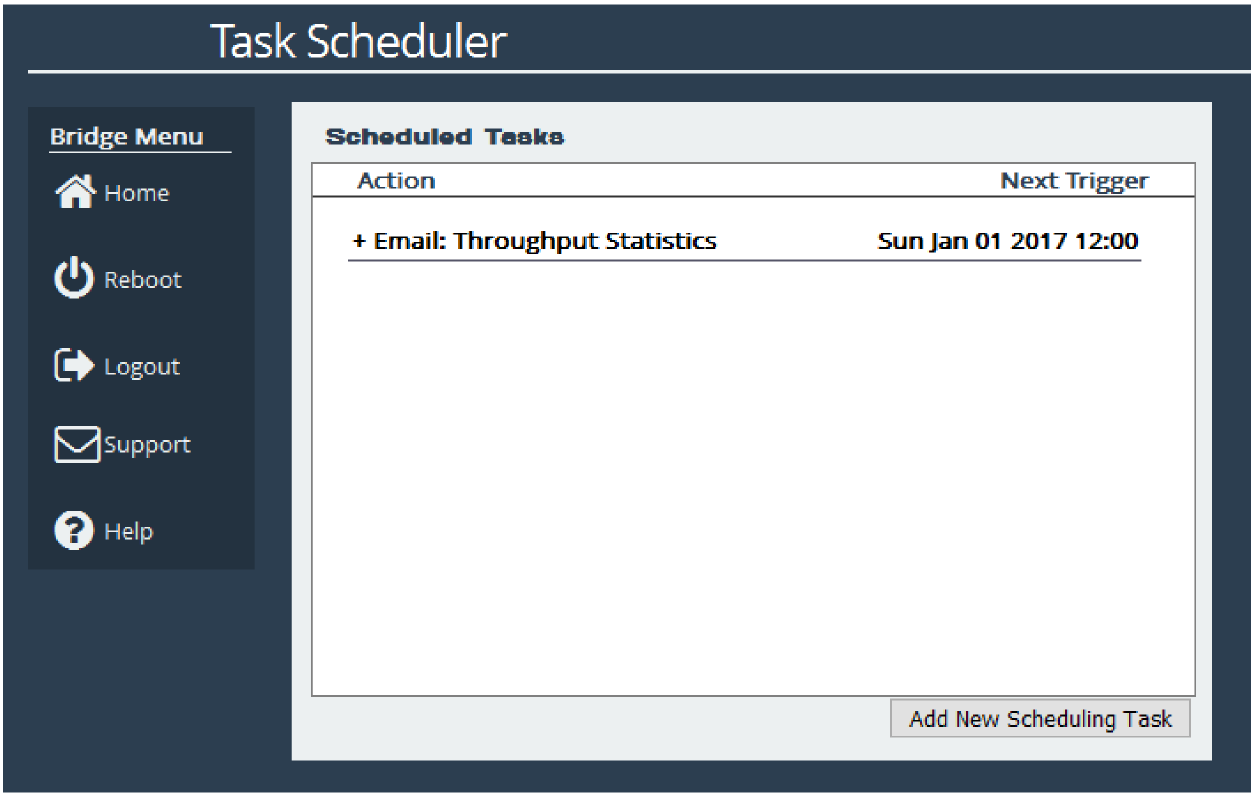
No Scheduled Tasks

7.7.1 Adding Tasks

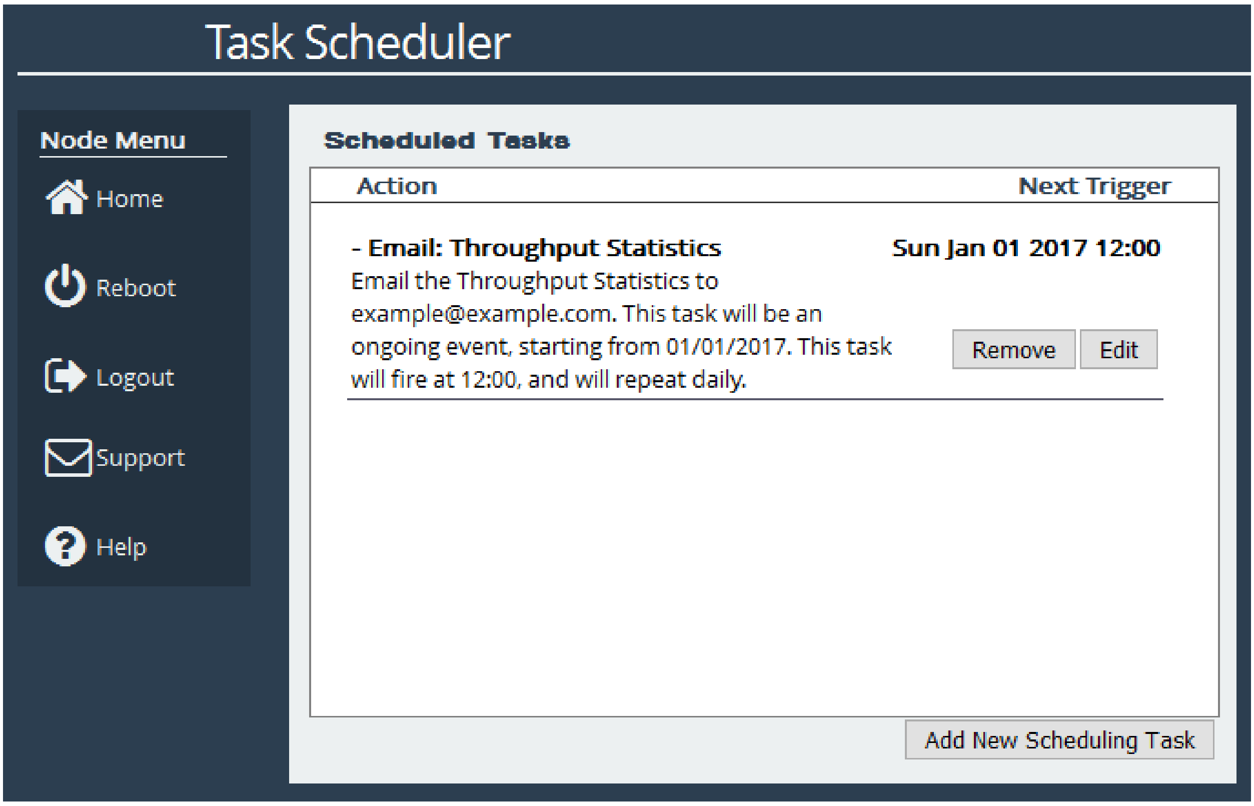
Tasks can be added by clicking on the *Add New Scheduling Task* button, which will start the task wizard.

7.7.2 Removing/Editing Tasks

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



Clicking on a task will expand it as shown:



Email the Throughput Statistics to example@example.com. This task will be an ongoing event, starting from 01/01/2017. This task will fire at 12:00, and will repeat daily.

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.

7.7.3 Task Wizard

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

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

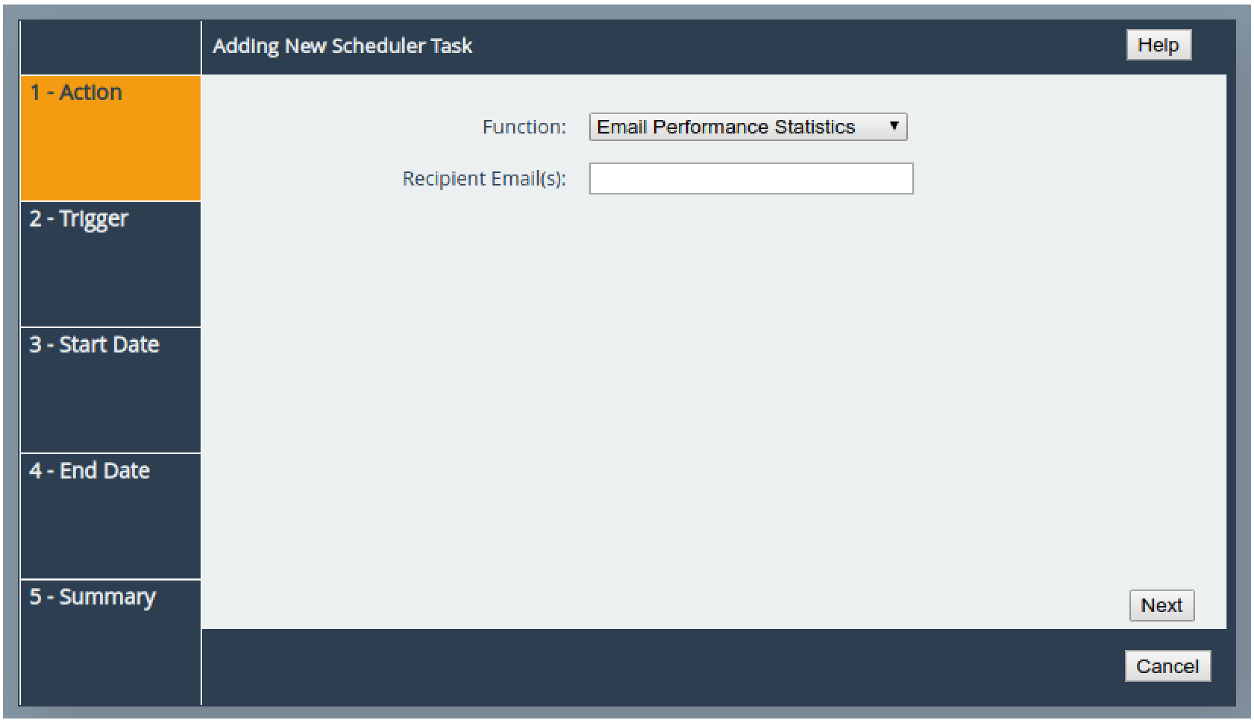
Cancel Clicking this button will discard the changes being made to the task and close the wizard.

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

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

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

7.7.3.1 Action - Email Performance Statistics



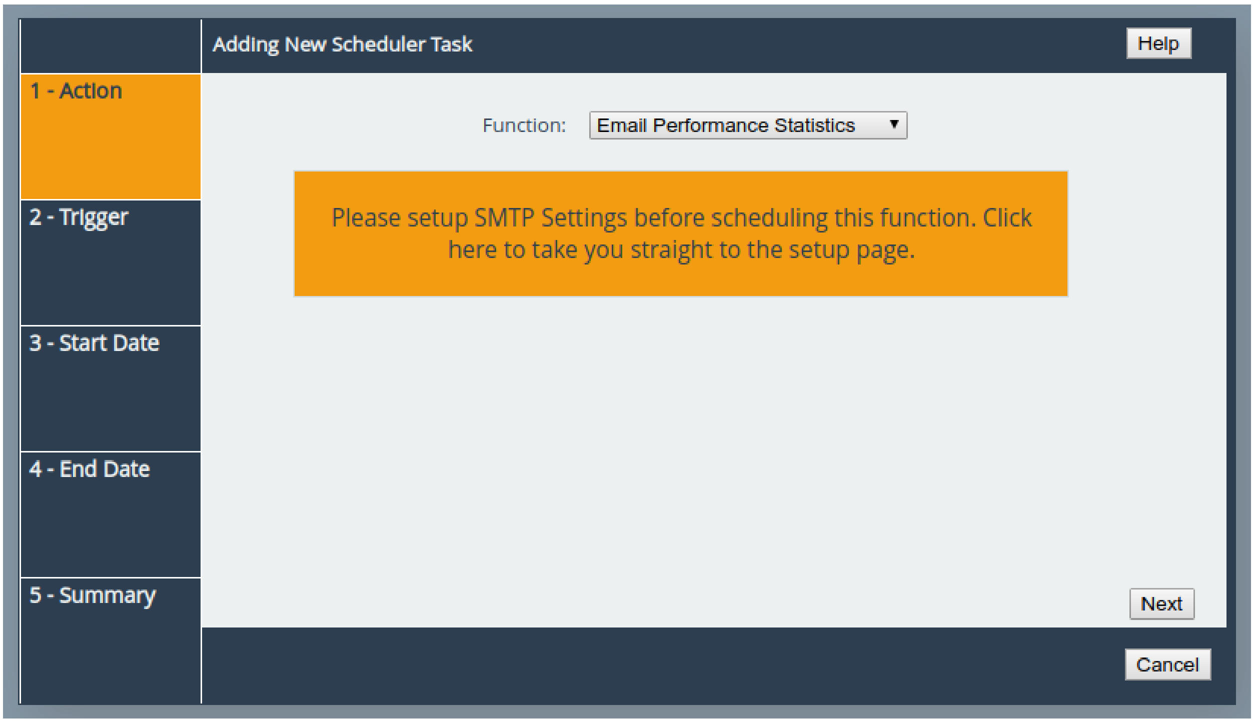
Adding New Scheduler Task

Function: Email Performance Statistics

Recipient Email(s):

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

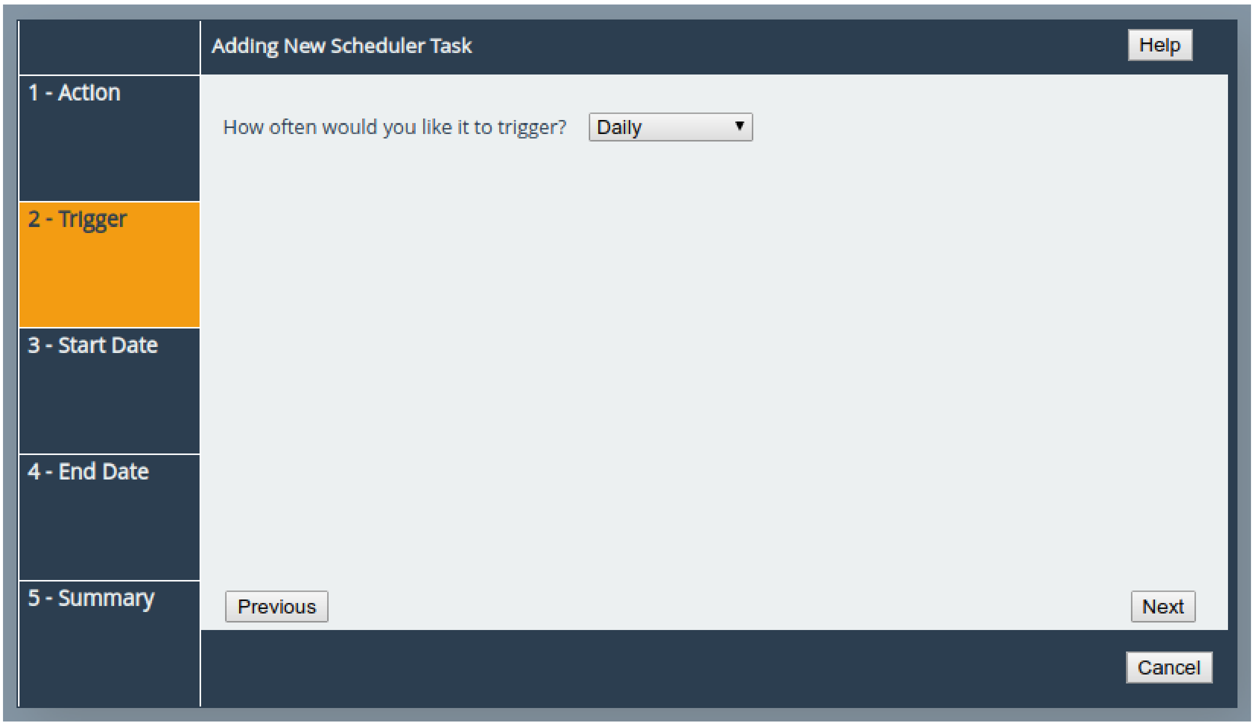
Important: If you see the following image, click on the yellow box to be taken to the Service Control page where SMTP can be set up. See Section 3.3.3: Email.



Function: Email Performance Statistics

Please setup SMTP Settings before scheduling this function. Click here to take you straight to the setup page.

7.7.3.2 Trigger



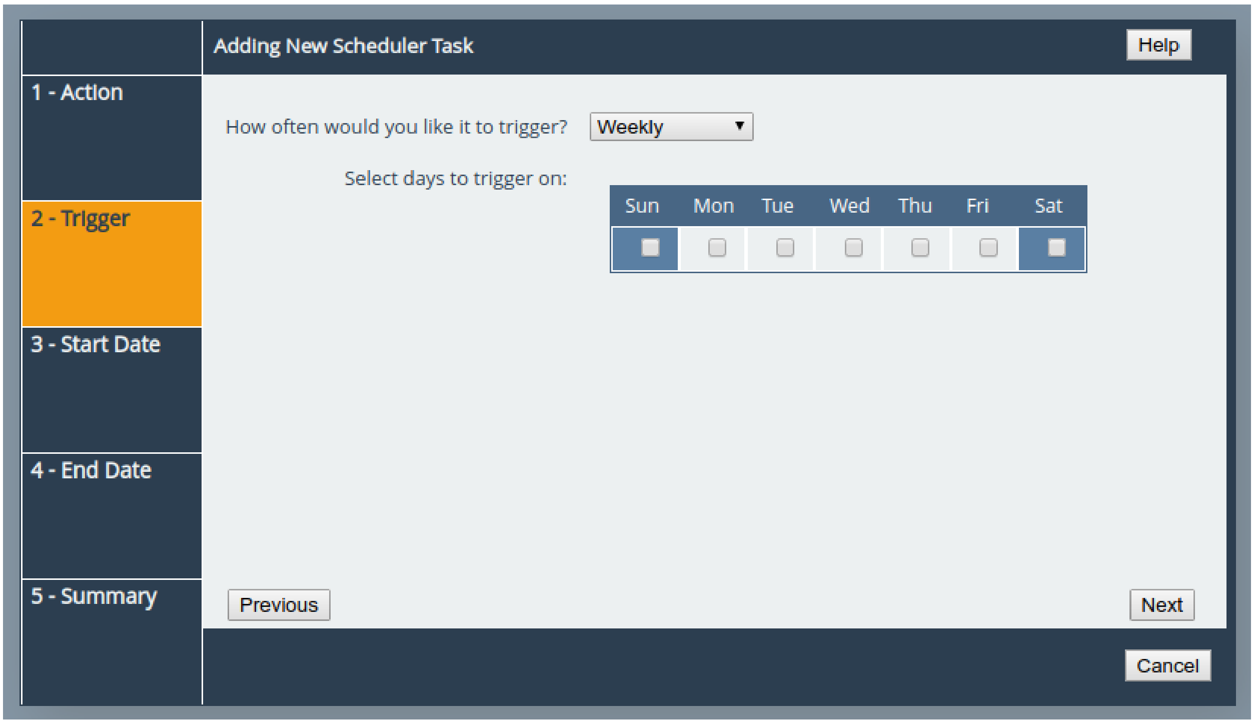
How often would you like it to trigger? Daily

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:

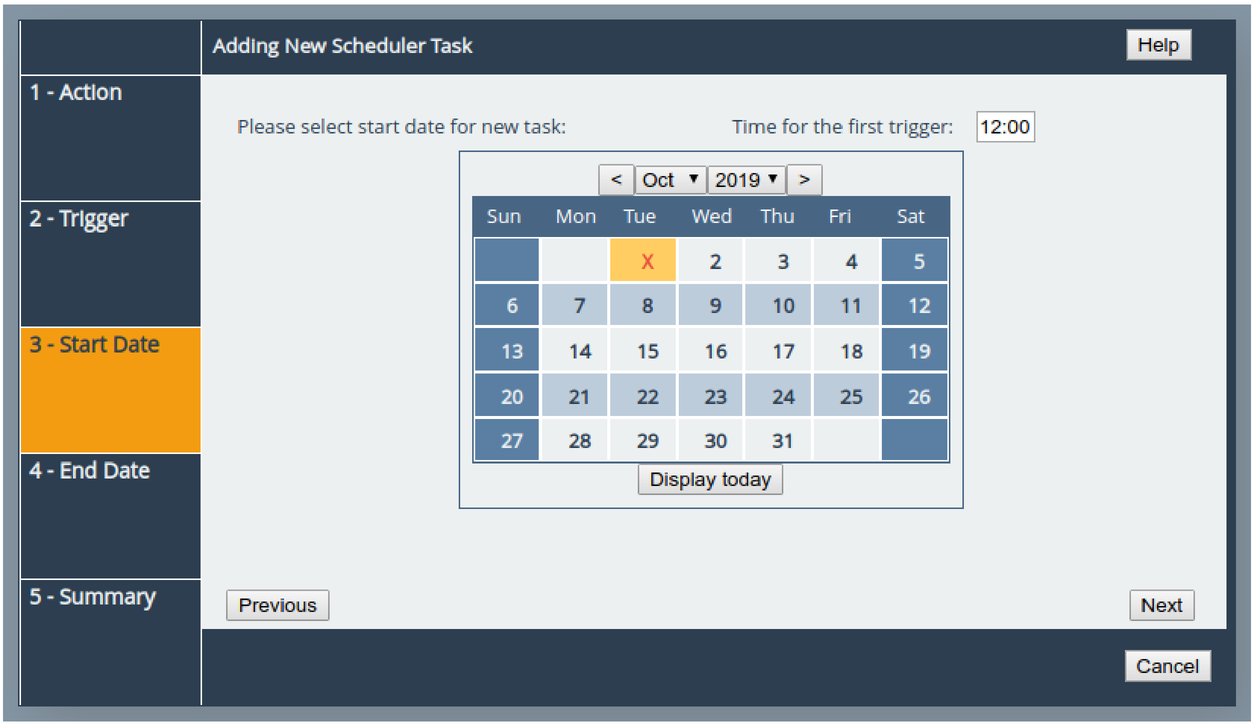


How often would you like it to trigger? Weekly

Select days to trigger on:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
□	□	□	□	□	□	□

7.7.3.3 Start Date



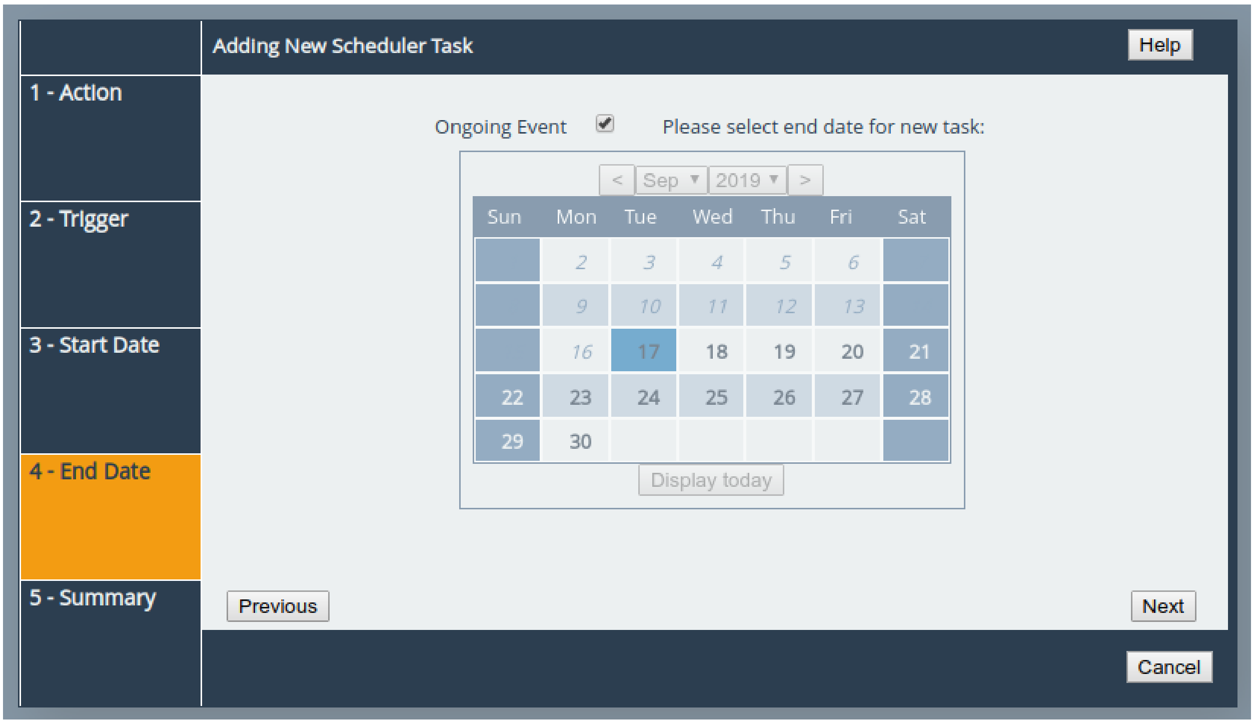
Please select start date for new task:

Time for the first trigger: 12:00

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		X	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

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.

7.7.3.4 End Date

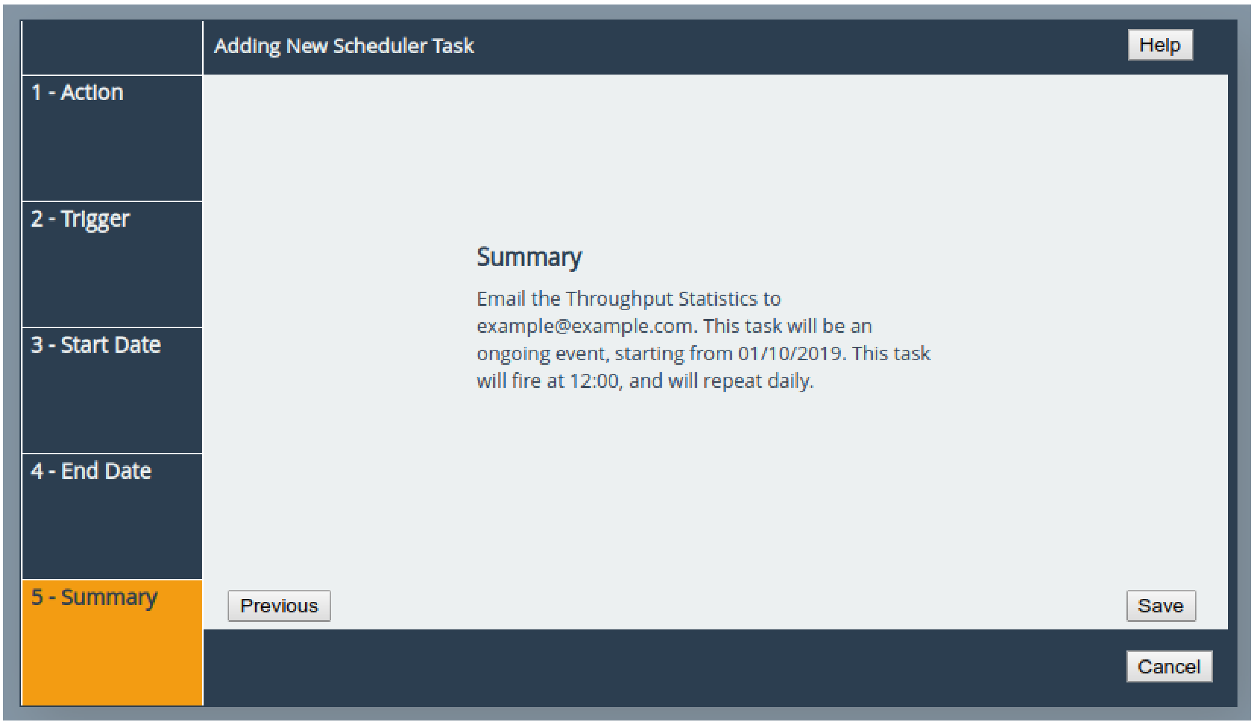


Please select end date for new task:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	2	3	4	5	6	
	9	10	11	12	13	
	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

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.

7.7.3.5 Summary



Summary

Email the Throughput Statistics to example@example.com. This task will be an ongoing event, starting from 01/10/2019. This task will fire at 12:00, and will repeat daily.

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.

8 Troubleshooting

8.1 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.

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

8.2 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.
- A common mistake is when enabling CHAP only for a device after the initial discovery by the initiator. It will be necessary to remove the address from the discoveries tab and recreate it with the appropriate CHAP settings, otherwise any rediscoveries will be attempted without CHAP and no devices will be returned.

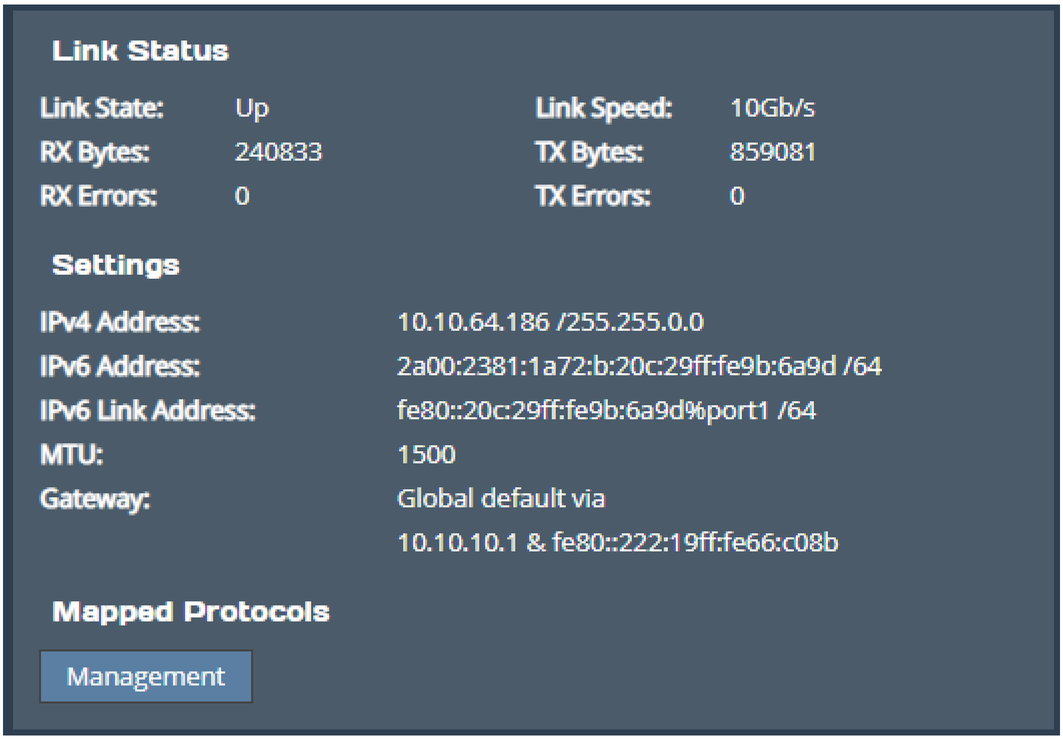
- Reboot the devices and the Gateway.

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

8.3 Network Performance Problems

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

- Ensure that the entire network cabling between the network and the 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.



Link Status

Link State:	Up	Link Speed:	10Gb/s
RX Bytes:	240833	TX Bytes:	859081
RX Errors:	0	TX Errors:	0

Settings

IPv4 Address:	10.10.64.186 /255.255.0.0
IPv6 Address:	2a00:2381:1a72:b:20c:29ff:fe9b:6a9d /64
IPv6 Link Address:	fe80::20c:29ff:fe9b:6a9d%port1 /64
MTU:	1500
Gateway:	Global default via 10.10.10.1 & fe80::222:19ff:fe66:c08b

Mapped Protocols

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

8.4 iSCSI Performance Problems

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

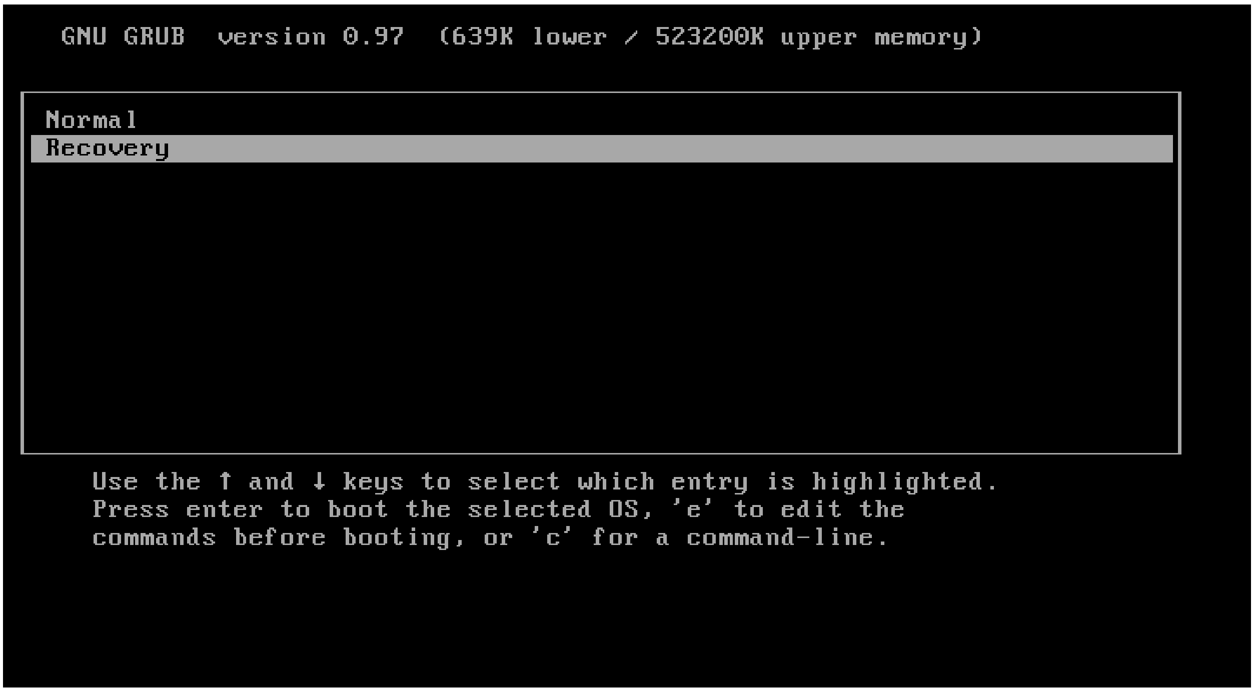
- *Data Digests* are an extra level of error checking on top of the standard TCP/IP checksum error checking (configured on the initiator). However, the calculation of these extra checksums can greatly affect overall performance. Therefore, *Header and Data Digests* should only be enabled where the integrity of the network connection is in doubt.
- 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 C: Useful Links for information on how to contact Bridgeworks Support.

8.5 Recovery Wizard

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

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



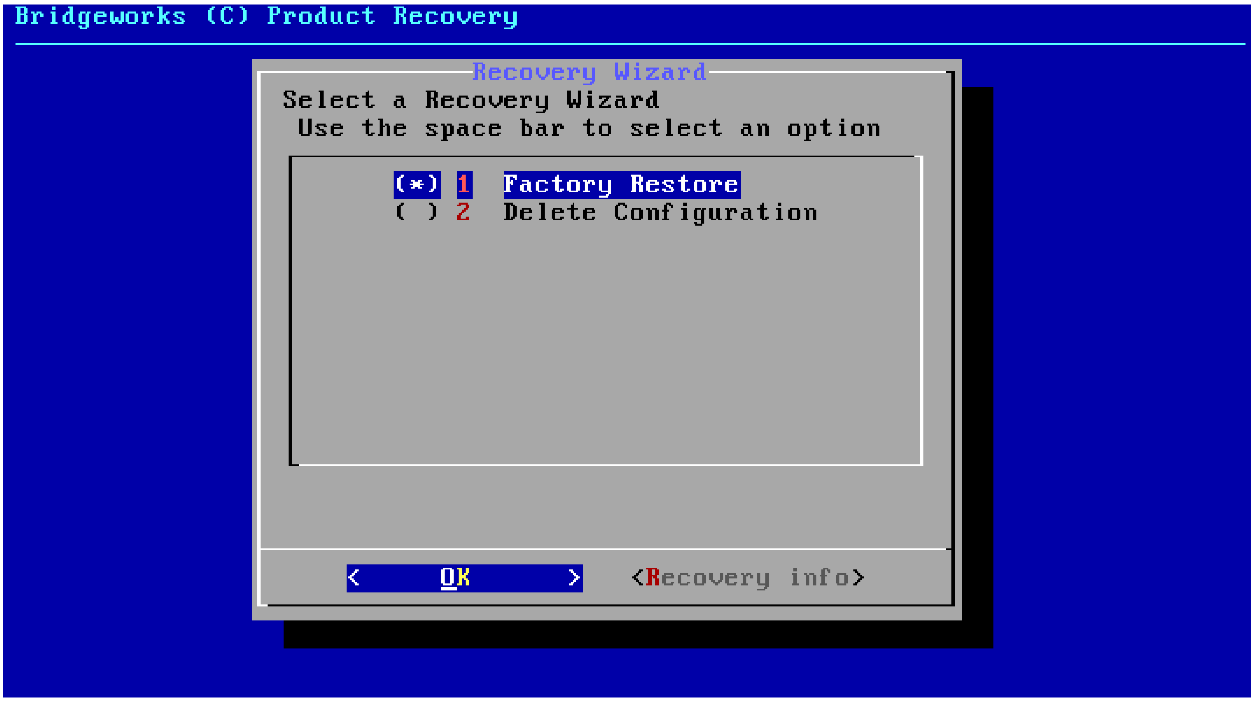
```
  GNU GRUB  version 0.97  (639K lower / 523200K upper memory)

 Normal
 Recovery

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the
     commands before booting, or 'c' for a command-line.
```

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

8.5.1 Factory Restore

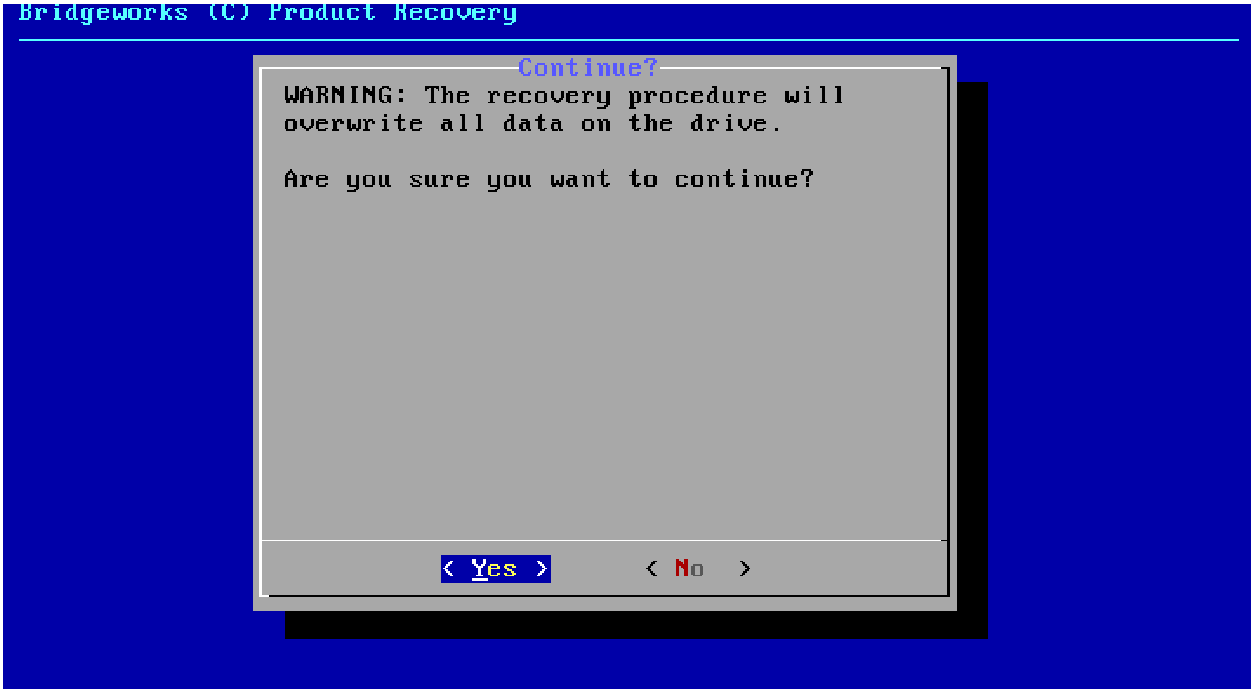
This option will restore your unit to its factory defaults, removing any current configuration on your system including your current firmware and licence keys.

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



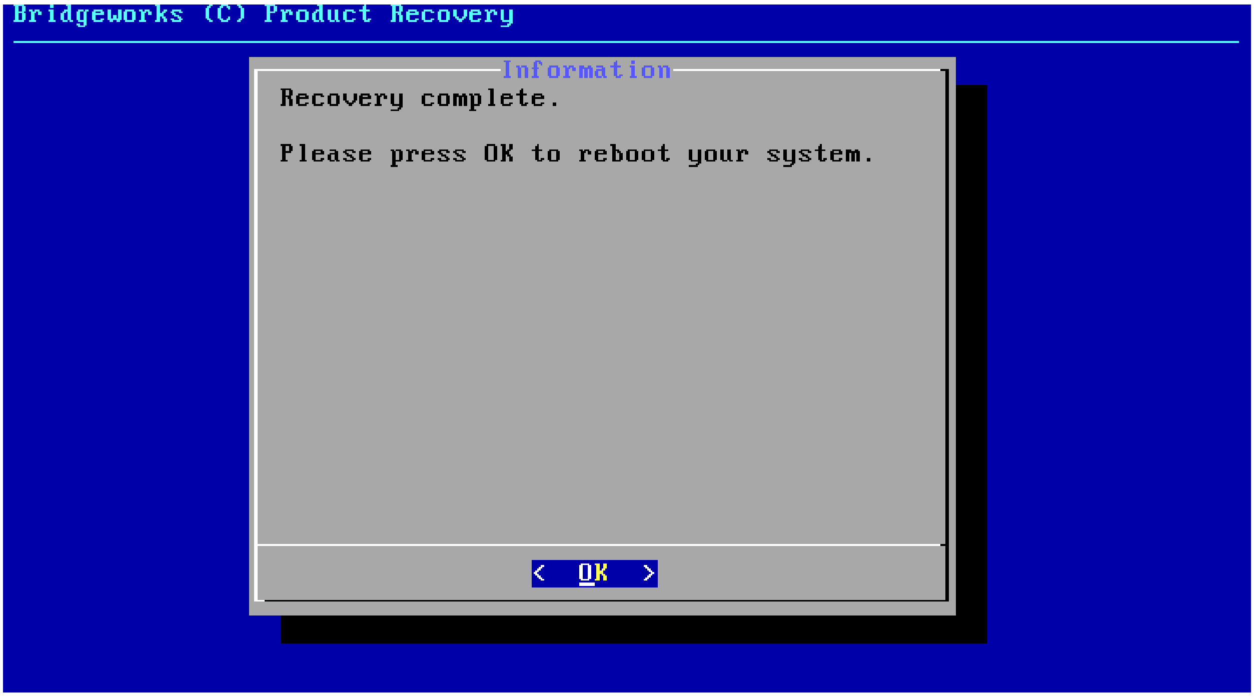
```
Bridgeworks (C) Product Recovery

                  Recovery Wizard
 Select a Recovery Wizard
  Use the space bar to select an option

        (*) 1  Factory Restore
        ( ) 2  Delete Configuration

      <    OK    >     <Recovery info>
```

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.



```
Bridgeworks (C) Product Recovery

Continue?
WARNING: The recovery procedure will
overwrite all data on the drive.

Are you sure you want to continue?
```

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

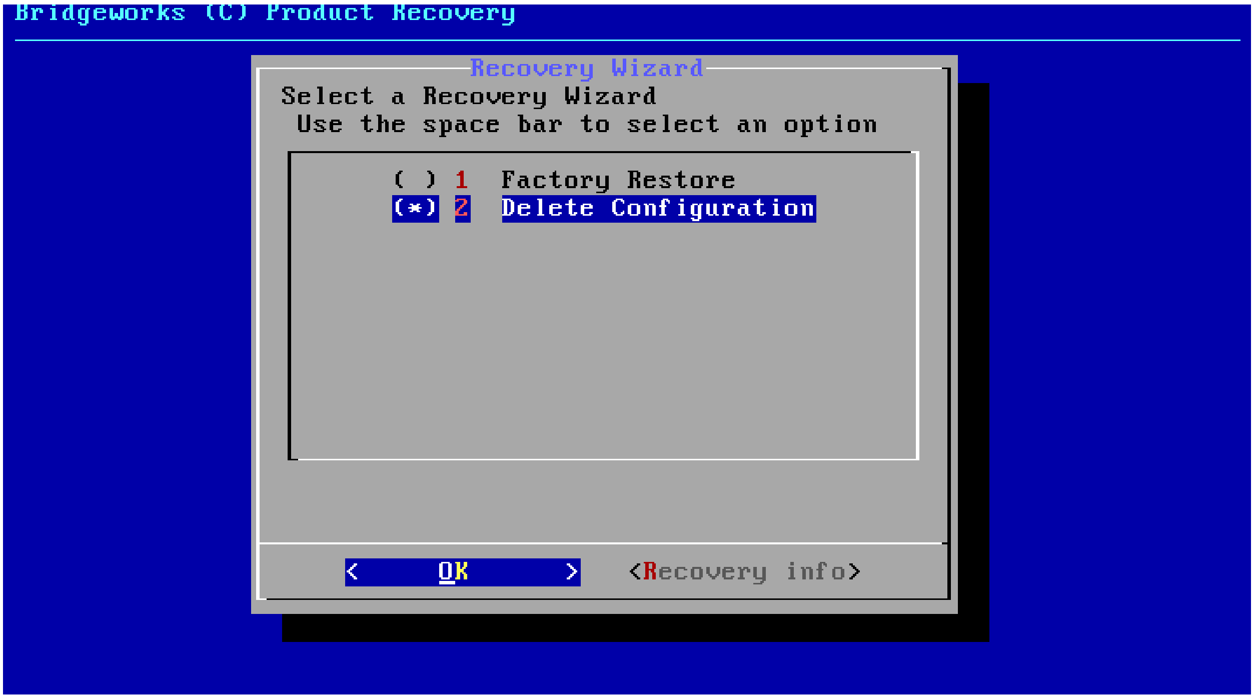


```
Bridgeworks (C) Product Recovery

Information
Recovery complete.

Please press OK to reboot your system.
```

8.5.2 Delete Configuration

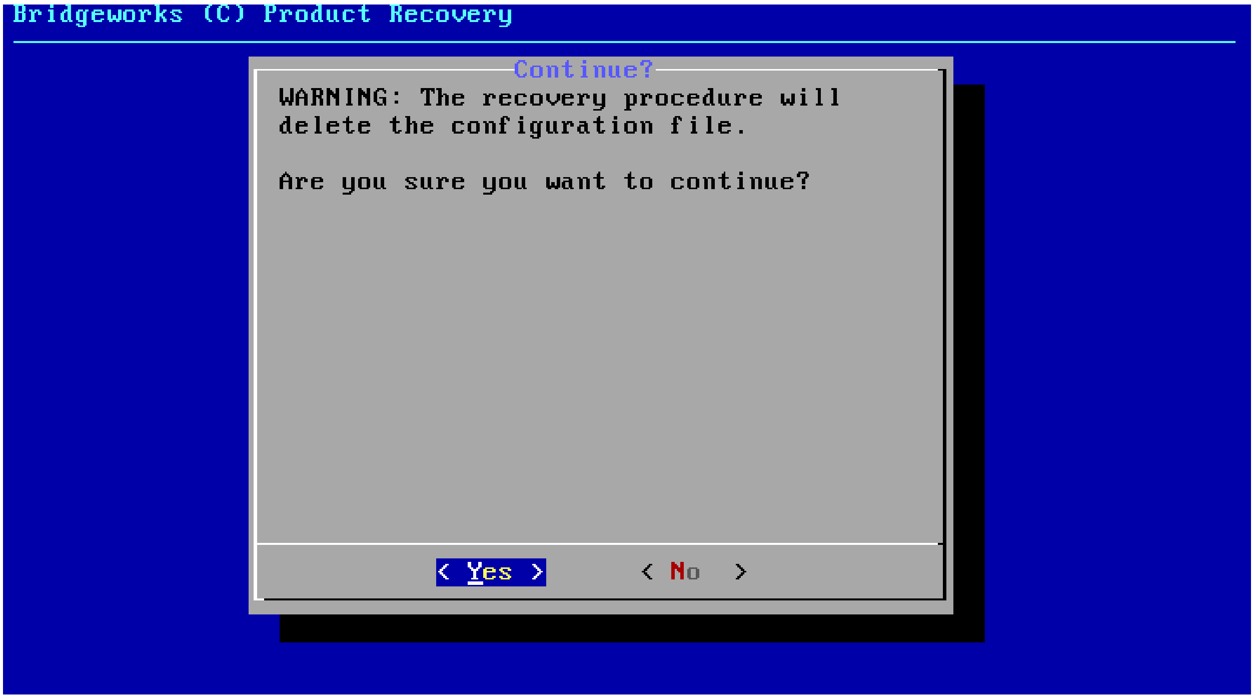
This option will delete your configuration file, removing any current configuration on your system but keeping your current firmware and licence keys.

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



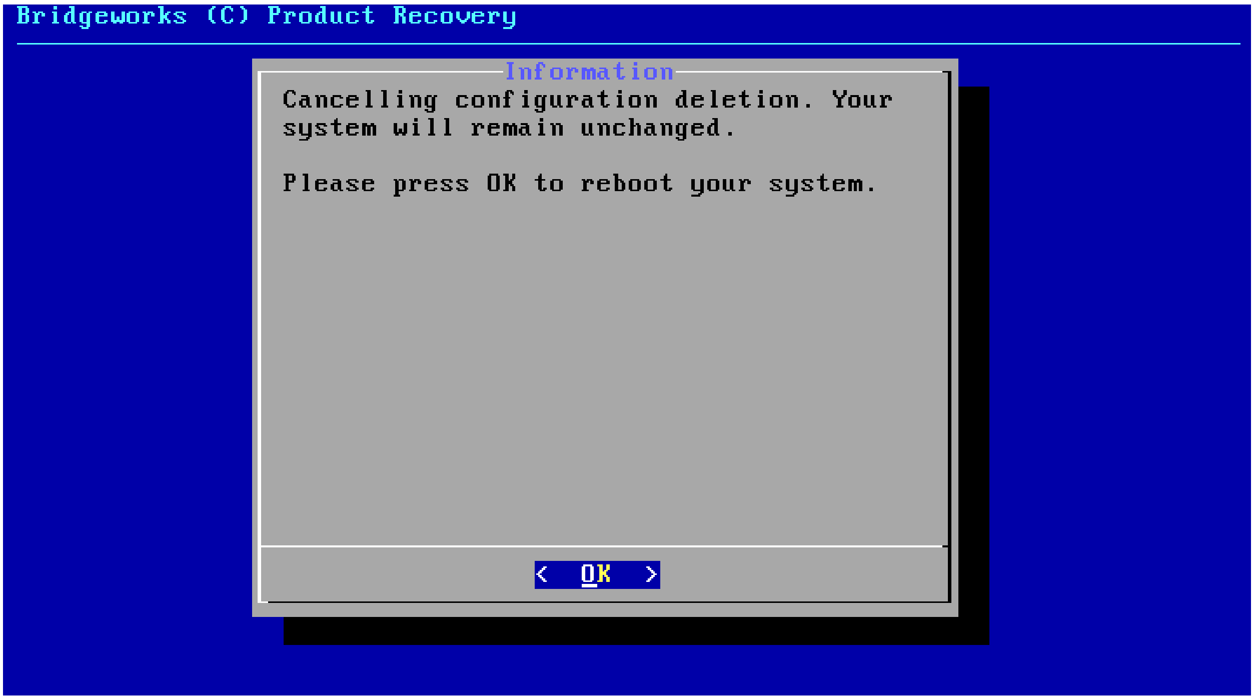
```
Bridgeworks (C) Product Recovery

Recovery Wizard
Select a Recovery Wizard
 Use the space bar to select an option

      ( ) 1  Factory Restore
      (*) 2  Delete Configuration
```

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.



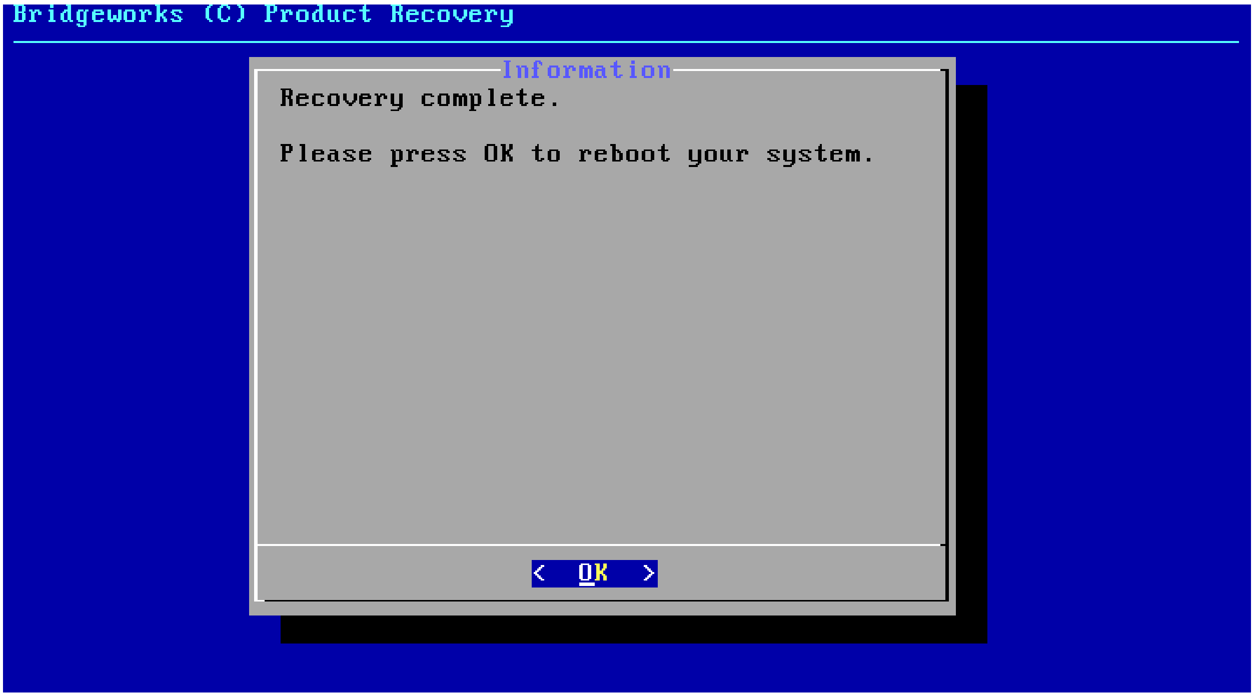
```
Bridgeworks (C) Product Recovery

Continue?
WARNING: The recovery procedure will
delete the configuration file.

Are you sure you want to continue?
```

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



```
Bridgeworks (C) Product Recovery

Information
Cancelling configuration deletion. Your
system will remain unchanged.

Please press OK to reboot your system.
```

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



```
Bridgeworks (C) Product Recovery

Information
Recovery complete.

Please press OK to reboot your system.
```

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

A IP Protocols and Port Numbers

For the 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.

A.1 Inbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 22	SSH	Required to access the configuration console through management interfaces when SSH is enabled. See Section 3.2.5: Secure Shell (SSH).
TCP 80	HTTP	Required to access the web interface through management interfaces when HTTP is enabled.
TCP 443	HTTPS	Required to access the web interface through management interfaces when HTTPS is enabled.
UDP 161	SNMP	Required for management interfaces to respond to Simple Network Management Protocol requests, see Section 3.3.2: Simple Network Management Protocol (SNMP).

A.2 Outbound LAN Protocols and Port Numbers

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

Note: The iSCSI Initiator uses TCP port 3260 by default, but may use any TCP port specified during target discovery. See Section 5.1: Discovering an iSCSI Target.

B 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.

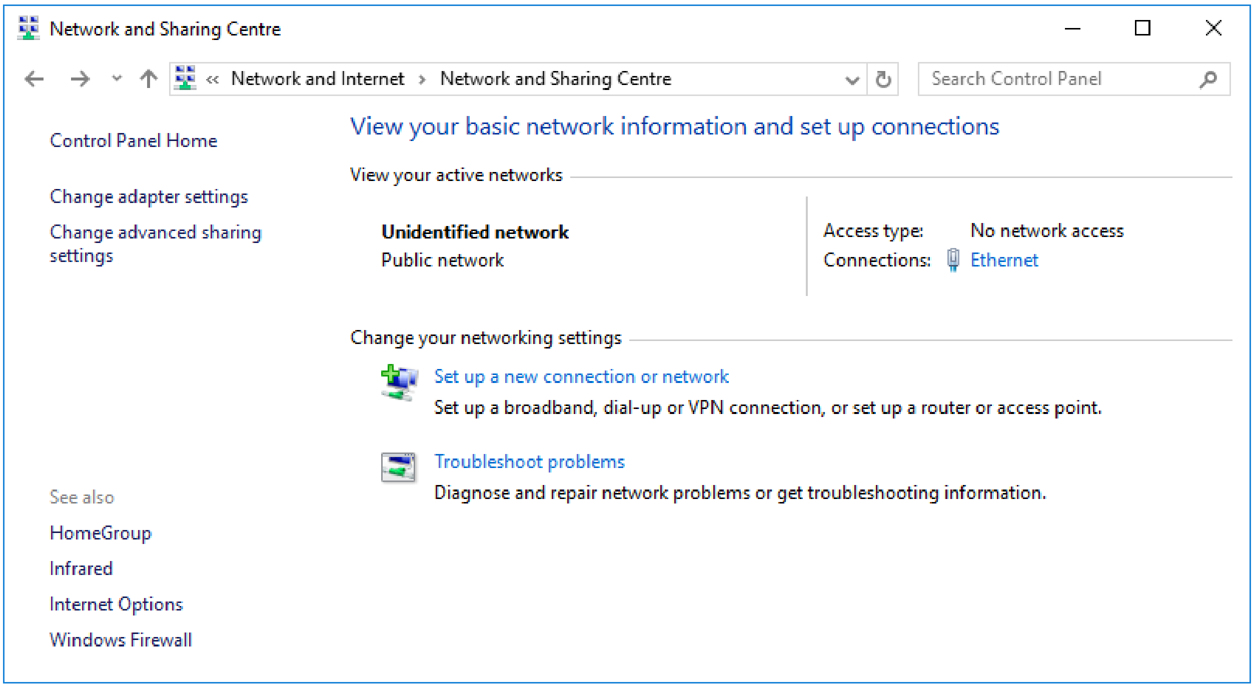
These instructions apply to Windows Vista, 7, 8, 10 and to Windows Server 2008, 2012, 2016, and their respective R2 versions.

⚠	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.



View your basic network information and set up connections

View your active networks

Unidentified network
Public network

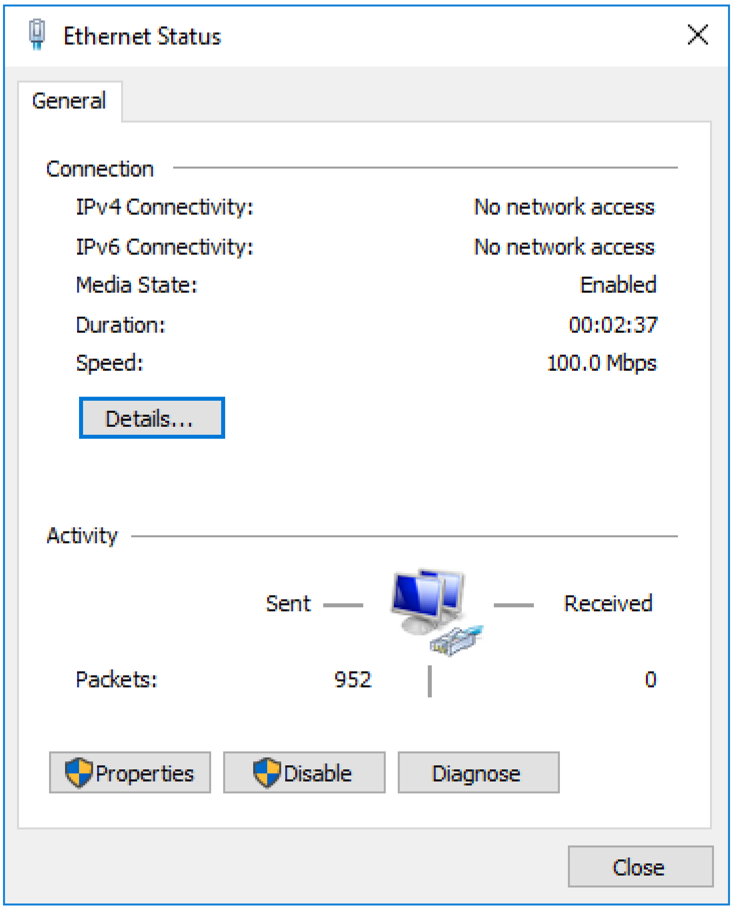
Access type: No network access
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up or VPN connection, or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems or get troubleshooting information.

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



Ethernet Status

General

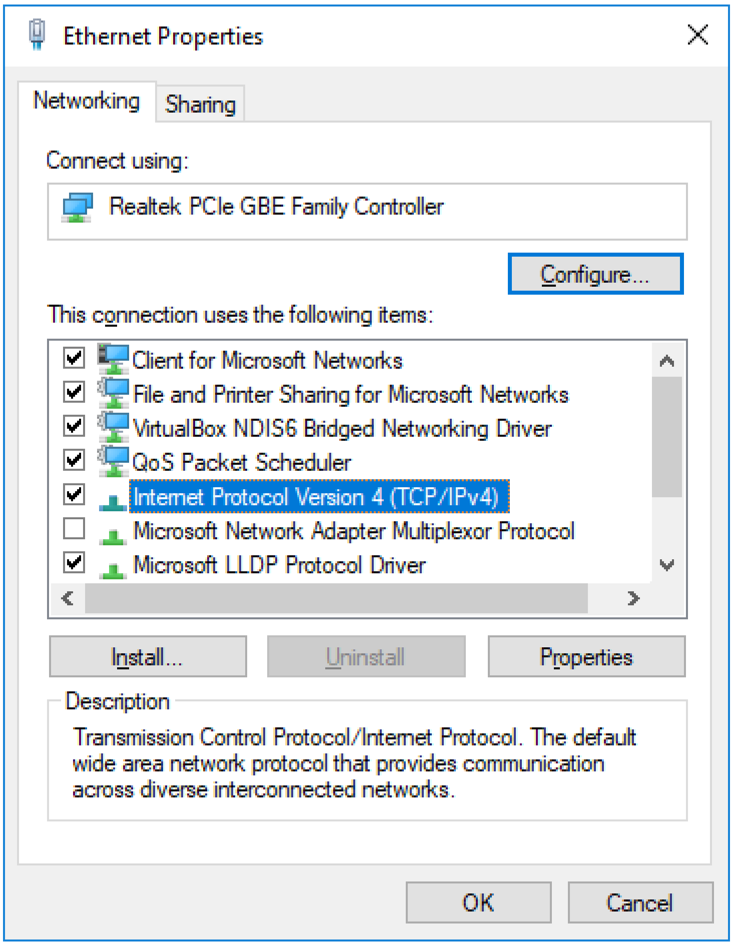
Connection

IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:02:37
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	952	0

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



Ethernet Properties

Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

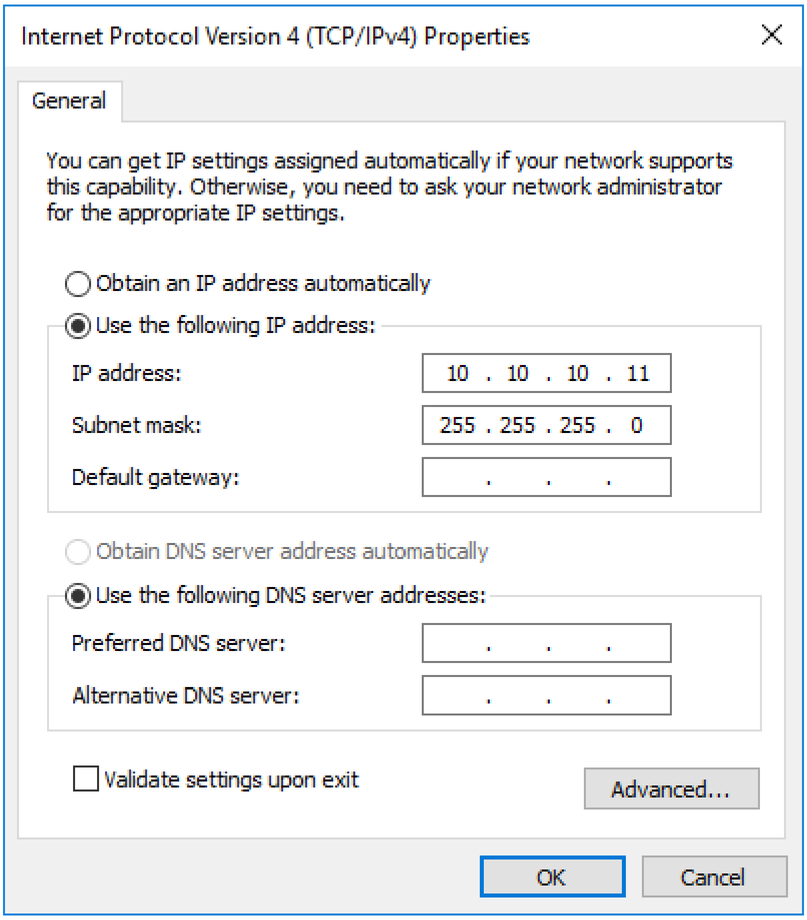
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

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

C Useful Links

Frequently Asked Questions If you experience problems with the FCE, 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 FCE, 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/.