



Potomac ESAS iSCSI to SAS Bridge Quickstart Guide Eli-v6.5.391

Bridgeworks

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

1 Introduction

This guide is designed to help you through the steps required to power up and configure the basic settings on a Bridgeworks Potomac ESAS iSCSI to SAS Bridge. For more detailed configuration options please refer to the Potomac ESAS iSCSI to SAS Bridge Software Manual (<https://support.4bridgeworks.com/documents/manuals/>).

1.1 Overview

The Potomac ESAS iSCSI to SAS Bridge creates an interface between a network, which utilises the iSCSI protocol, and peripherals that utilise the SAS bus. The Bridge acts as a two-way interface converting the data packets that are received on the iSCSI network to SAS data packets. This data is then ready to be sent across a network to SAS-enabled storage devices such as disks and tape drives.

1.2 Definitions

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

1.2.1 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).

1.2.2 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

1.2.3 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.

2 Pre-Install Checklist

Before connecting any equipment, or performing any patching, please ensure you have completed the pre-installation checklist below.

- iSCSI and SAS connection details
- iSCSI and SAS cables
- IP Addresses for Management interface/s
- PC or Laptop connected to the Management LAN
- Licence Key saved to local machine
- Keyboard and monitor

3 Setup

3.1 Hardware

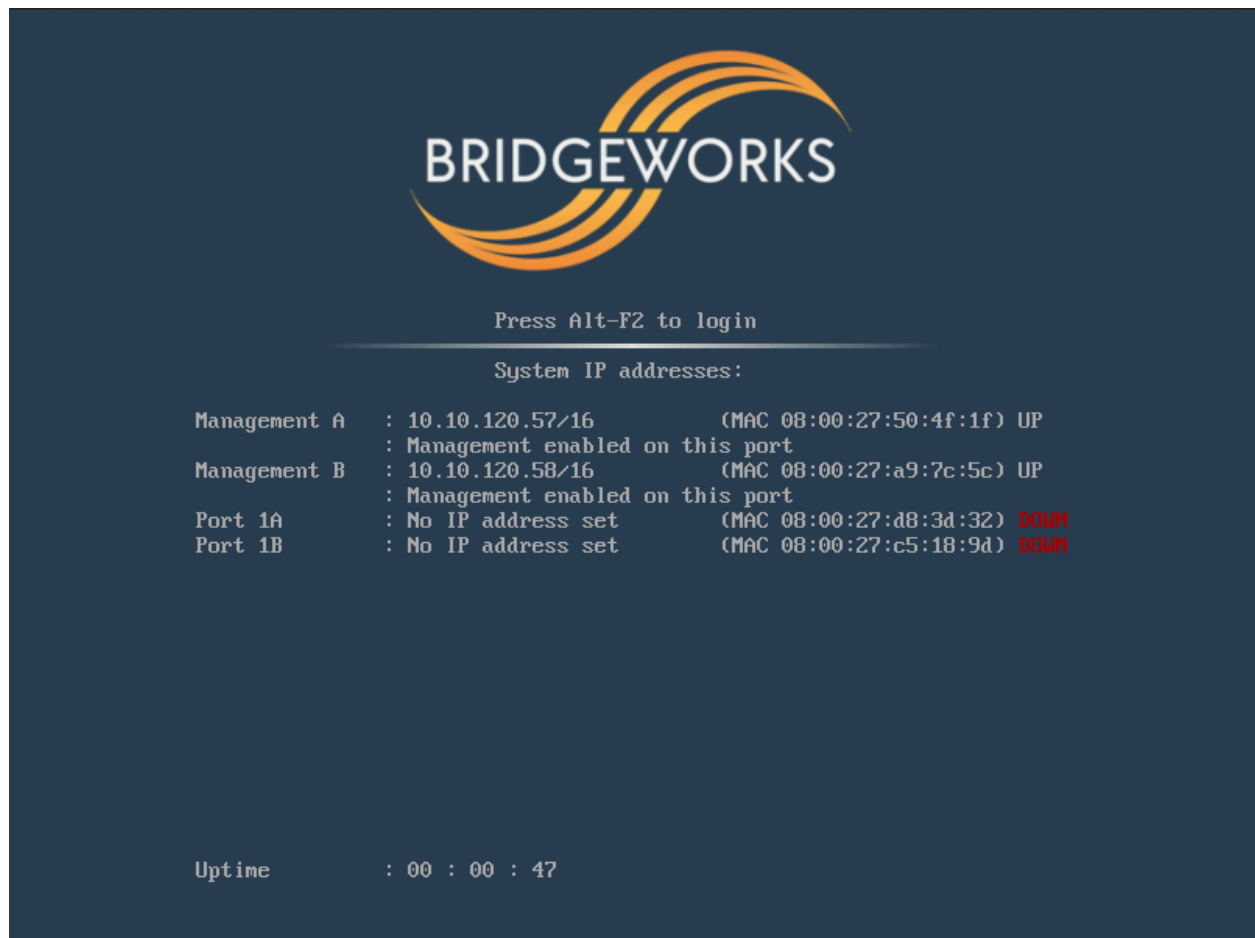
To set up a hardware Potomac ESAS iSCSI to SAS Bridge:

- Install the server into a rack using the included rails and ensure it is secure.
- Plug the power leads into the appropriate sockets.
- Connect an Ethernet cable to the management interface on Port A of the onboard Network Interface Controller (NIC).
- Connect the iSCSI and SAS cables to the appropriate interfaces.
- Connect the keyboard and monitor.



Warning: Ensure that the cables you are using are rated for the correct speed. If a cable is rated for a lower speed than the interface, the connection will not run at full capacity.

Now power on the device. The Bridge should boot with a display similar to the one below:



3.1.1 Configuring a Static IP

If the device is installed on a network that is not using DHCP you will need to configure a static IP Address so that you can access the Web GUI to complete the configuration of the Bridge.

Press *ALT-F2* to login to the Bridge.

As this will be the first time you have logged into the Bridge you will be required to set an administrator password for the device.

```
Bridgeworks Management Interface
No password configured - Enter new password: _
```

You can now log into the Bridge using the default username *admin*, and the password you set.

Within the Command Line Interface, you can select an option by entering the number next to it. Navigate to Network Connections using 1, then select the port you will be using to manage your Bridge.

```
1 Enable Port : Yes
2 MTU Size : 1500
3 Enable Forwarding : No
4 Use DHCP to assign an IP address automatically : Yes
5 DNS Registration : Yes
6 Use the following IP address : No
7 IP Address : 10.10.64.60
8 Netmask : 255.255.0.0
9 Gateway : 10.10.10.1

s Save
x Cancel
```

Ensure this port is enabled by checking the *Enable Port* option. If this says *No* next to it, select it, then press *y* to enable it.

DHCP will be enabled by default. To set a static IP address for your Bridge, select *Use the following IP address*.

Next, set your IP address by selecting *IP Address* and entering a valid IPv4 address. You may also need to adjust the netmask and default gateway. When you are done modifying your port settings, press *s* to save.

Once you have saved all your settings, press *x* to reboot your Bridge to apply them.

4 Configuration

You can now perform the rest of the configuration remotely via the web interface using the Management IP address.

If you have not used the CLI as above to configure an Admin password, you will be required to set the admin password for the device. This can be altered later on if required. Once set you will be returned to the login screen to enter the username "admin" with the password you have just configured.

Upon accessing the web interface for the first time, you will be required to accept the End User Licence Agreement.

You should now be on the Home page of the web interface for the Potomac ESAS iSCSI to SAS Bridge (as shown below).



A guide to configuring the following settings is shown below:

- Section 4.1: Changing the Hostname (Optional)
- Section 4.2: Installing the Licence Key
- Section 4.3: Diagnostics

During the configuration process you will be required to reboot the device several times.

4.1 Changing the Hostname (Optional)

To set the hostname for the device, first return to the Home page using the *Home* button in the sidebar on the left. Then select *Network Connections* and then *General Settings*. You can change


the hostname for the device here. If you wish to display the hostname of the node on the login page select the checkbox labelled "Hostname on Login Page:"

Once you've amended the settings, click *Save* and select *OK* to the prompt that appears. You can make additional configuration changes before rebooting the device.

Return to the Home screen by selecting *Home* at the top left.

4.2 Installing the Licence Key

The licence key for your device contains the licences for the protocols you can connect to.

	<p>Important: If the licence key is not uploaded you will not be able to add the Port Mappings to the ports later on!</p>
---	---

To upload the licence key, first navigate to the Home page using the *Home* button in the sidebar on the left. Next select *Licence Key Management*, then *Browse* and locate the licence key file saved to your local machine.

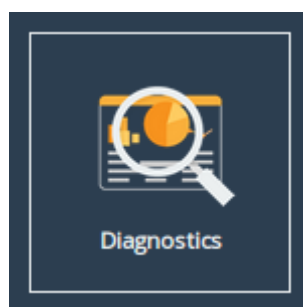
Select the licence key file and then click *Upload*. You should now see which protocols are licensed for your device in the window.

The device requires a reboot for the licence key to take effect. Select *Reboot* from the menu on the left and restart the device.

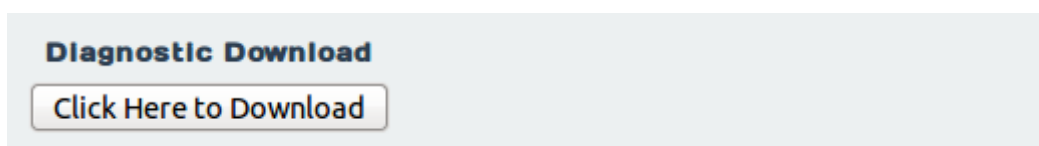
4.3 Diagnostics

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

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 Bridge 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.

5 SAS Initiator

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

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



You will see the following page:

SAS Initiator

Hostname

- Home
- Reboot
- Logout
- Support
- Help

Display Options

Phy display filter:

All

Live Update: ☒

Host - Slot 2

4 links active

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



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

5.1 SAS Initiator Page

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

5.1.1 Hosts

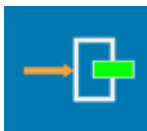
The heading of a host section shows the following information:

Chevron An arrow for expanding or collapsing the section.

Name (e.g. Host 1).

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

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



End Device A device is connected



No Device No device is connected



Expander Device An expander is connected

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

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

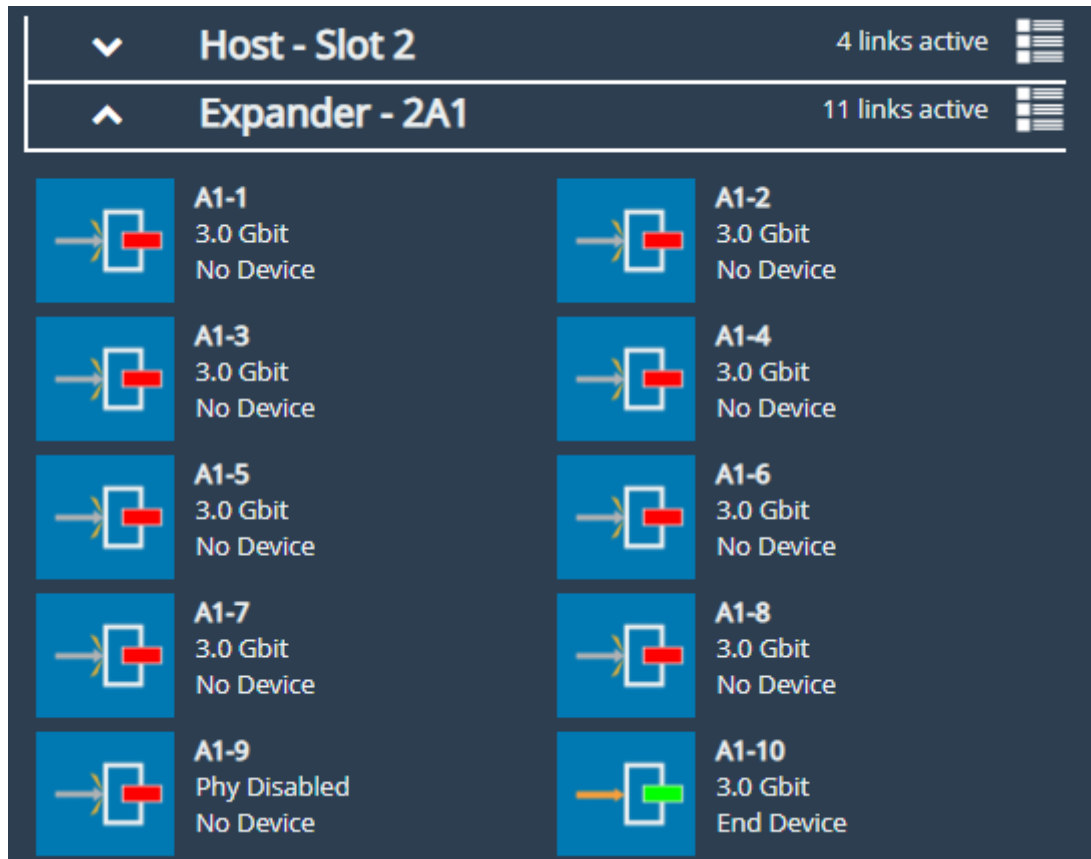
Link speed The negotiated link speed of the device. This will show a speed if a physical connection is made (e.g. “6.0 Gbit”), or otherwise displays “Unknown”.

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

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

5.1.2 Expanders

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



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

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

5.1.3 Display Options

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

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

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

5.2 Phy Status Page

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

SAS Initiator: Phy Configuration - A1-9

Node Menu

- Home
- SAS Initiator
- Reboot
- Logout
- Support
- Help

Phy A1-9 Status

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

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

Vendor Manufacturer of the device.

Product Product name of the attached expander.

Model Model name of the attached end device.

Enabled True or false.

Device Type No device, end device, or expander.

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

Max Link Rate Maximum link speed allowed by the hardware.

Min Link Rate Minimum link speed allowed by the hardware.

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

Invalid Dword Count Number of malformed Dwords received.

6 iSCSI Target Configuration

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

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



The web interface will then display the following:

A screenshot of the iSCSI Target configuration web interface. On the left is a dark blue sidebar with a 'Hostname' header and five menu items: 'Home' (house icon), 'Reboot' (power icon), 'Logout' (logout icon), 'Support' (envelope icon), and 'Help' (question mark icon). The main content area has a light blue background. At the top is the 'Authorisation' section, which includes a warning message: 'While secrets longer than 16 characters are allowed, they may be unsupported by some hosts.' Below this are three input fields: 'Enable CHAP:' with an unchecked checkbox, 'Username:', 'Initiator Secret:', and 'Target Secret:'. The bottom section is 'Network Interfaces', which contains a table with two columns: 'Interface' and 'Configured TCP Port(s)'. The table has two rows: 'Port 2 (10.10.10.50):' and 'Port 3 (10.10.11.50):', both with '3260' selected in a dropdown menu. At the bottom right are 'Cancel' and 'Save' buttons.

Interface	Configured TCP Port(s)
Port 2 (10.10.10.50):	3260
Port 3 (10.10.11.50):	3260

6.1 Authorisation (CHAP)

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

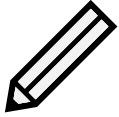
The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Bridge will authenticate itself with the initiator using the initiator secret.

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

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

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

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



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

6.2 Network Interfaces

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

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

6.3 iSCSI Sessions

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

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



The web interface will then display the following:

Hostname

Home

Reboot

Logout

Support

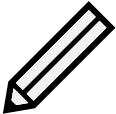
Help

iSCSI Sessions

Initiator	Target
iqn.1991-05.com.microsoft:kevin.test.d omain	iqn.2002-12.com.4bridgeworks.001bd 1:eui.00041B0002001BD1.0,t,0x00000

Refresh

This page lists current connections to iSCSI initiators. The IQN of the initiator is shown in the *Initiator* column, and the IQN of the device it is logged on to is shown in the *Target* column. See Section 1.2.2: iSCSI Qualified Name (IQN) for more information.



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

7 Additional Features

Congratulations on finishing the basic setup of your Potomac ESAS iSCSI to SAS Bridge. Consider browsing the manuals for a complete list of capabilities (available at <https://support.4bridgeworks.com/documents/manuals/>).

The following sections are recommended starting points for some useful additional features.

7.1 iSNS

iSNS enables automatic discovery of iSCSI devices by your Potomac ESAS iSCSI to SAS Bridge.

To enable iSNS, see the Internet Storage Name Service (iSNS) section of the Potomac ESAS iSCSI to SAS Bridge Software Manual.

8 Useful Links

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

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