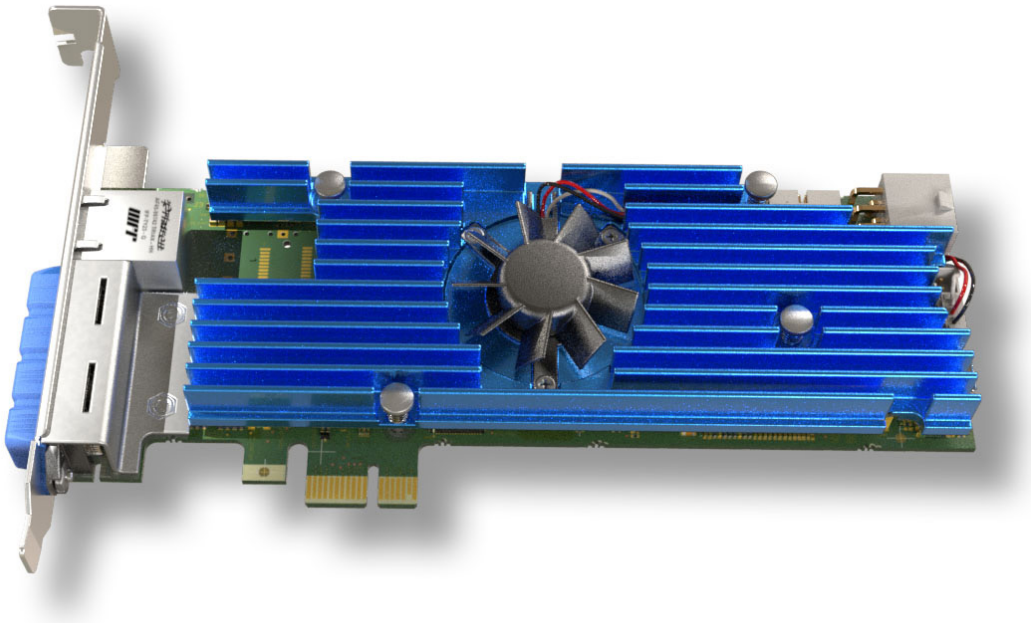
AMULET HOTKEY

Remote Workstation Host Cards



User manual

DXH4 and DXH4-M
HB-DXH4-0002
Revision 4.1 October 2020

teradici PCoIP®

CAUTION

To prevent damage to the DXH4:

- install in accordance with these instructions;
- always turn off and unplug the host computer before handling the DXH4;
- always use appropriate anti-static handling procedures when handling the DXH4;
- only use the DXH4 within an enclosed computer case. Do not operate an opened computer with a DXH4 installed;
- only use attachments and accessories approved by Amulet Hotkey;
- do not expose this appliance to moisture;
- do not place objects filled with liquids on or near the appliance;
- clean the product only with a dry cloth;
- refer all servicing to qualified personnel.

WARNING

- The heat sink on the DXH4 card can get hot when in use. Wait for it to cool before handling the card.

LASER SAFETY

The DXH4-M may be fitted with SFP network modules that contain Class 1 lasers. The SFP module emits invisible radiation which can cause harm if installed or serviced incorrectly. Follow the guidelines below:

Warning: Class 1 laser product.

Warning: Invisible laser radiation can be emitted from the aperture of the SFP port when no fibre is connected. To avoid exposure to laser radiation, do not stare into open apertures.

Warning: Only trained and qualified personnel may install, replace, or service this equipment.

Thank you

Thank you from everyone at Amulet Hotkey for purchasing this product. Much time and energy has gone into making this the best and most reliable solution available. We are confident we have provided a state-of-the-art unit that will provide you with long and reliable service regardless of the application.

To get the best from this product, follow this manual carefully.

Shipment and product inspection

Your product was carefully packed prior to despatch to guarantee safe transit. Make sure you thoroughly examine all packaging and contents for signs of physical damage before use.

If any damage has occurred, notify the shipping company and your supplier immediately. Otherwise, claims for damage or replacement may not be granted.

Retain the original packaging for use in the event that the equipment has to be stored, shipped or returned for service. If you choose to dispose of the packaging, please do so in an environmentally friendly fashion.

Technical support

If you have further questions , do not hesitate to contact Amulet Hotkey technical support for expert assistance:

www.amulethotkey.com/support

Declaration of conformity

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Title 47, Part 15 (47 CFR 15) of the Federal Communications Commission (FCC) Rules and Regulations establishes Radio Frequency (RF) emission limits for unlicensed emissions to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (personal computers, for example). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user. A label on the device shows which class (A or B) the equipment falls into. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label.

The DXH4 has been tested and found to comply with the limits for a Class B digital device, as defined by Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- reorient or relocate the receiving antenna;
- increase the separation between the equipment and receiver;
- connect the equipment into an outlet on a circuit different to that to which the receiver is connected;
- consult the dealer or an experienced radio or television technician for help.

EU Notice

This product complies with EMC Directive 2014/30/EU and the Low Voltage Directive 2014/35/EU. Conformity is shown by compliance with the applicable requirements of the following documents:

- EN 55032 (Class B) - Emissions
- EN 55024 - Immunity
- EN 61000-3-2 - Power Line Harmonics
- EN 61000-3-3 - Power Line Flicker
- EN 60950 - Product Safety

N27005

lead-free

Contents

1. Before you start 11

1.1 Introduction 11

1.1.1 PCoIP protocol 11

1.1.2 Video resolutions 11

1.1.3 Active cooling 11

1.2 DXH4 models 11

1.2.1 Network solutions 11

1.2.2 Terminology 11

1.3 Simple installation 11

1.4 Auxiliary power requirements 11

1.5 SFP modules 11

1.6 IP and MAC addresses 11

1.7 Wake on LAN and remote power cycling 12

1.7.1 WoL supported 12

1.7.2 WoL not supported - RPC cable required 12

1.8 Video inputs 12

1.8.1 Standard video resolution 12

1.8.2 High video resolution 12

1.9 Management tools and connection brokers 12

1.10 Change the I/O bracket (optional) 12

1.10.1 Change a full-height bracket to a low-profile bracket 12

1.10.2 Change a low-profile bracket to a full-height bracket 13

2. Your DXH4 15

2.1 I/O bracket features 15

2.2 I/O bracket status LEDs 16

2.2.1 Key 16

2.2.2 STATUS LED 16

2.2.3 Network ACTIVITY and network SPEED LEDs . 17

2.3 BSM status indication 17

2.4 Recessed button operations 17

2.4.1 While the DXH4 is starting up 17

2.4.2 When the DXH4 is powered up 17

2.5 Video inputs 17

2.5.1 Setup for quad monitors 17

2.5.2 Setup for dual monitors 17

2.5.3 Use the correct ports 17

2.6 Internal card connections 18

3. Set up the host card 19

3.1 STEP 1: Prepare the PC, Workstation or server 19

3.2 STEP 2: Fit the correct I/O bracket 19

3.3 STEP 3: Install the DXH4 19

3.4 STEP 4: Connect optional equipment 19

3.4.1 Connect auxiliary power (Optional) 19

3.4.2 Connect Remote Power Cable (Optional) 20

3.4.3 Connect SFP module (DXH4-M only) 20

3.5 STEP 5: Connect the video inputs 20

3.6 STEP 6: Connect the DXH4 to the network 20

3.7 STEP 7: Complete the installation 20

3.8 STEP 8: Change the default IP address... 20

3.9 STEP 9: Connect a zero client to the DXH4 21

3.9.1 Connect to a DXH4 using SLP Discovery 21

3.10 STEP 10: Change the default password.. 21

3.11 Set up is complete 21

4. How to install dual DXH4 cards 23

4.1 Before you install the DXH4s..... 23
4.2 Install the first DXH4 23
4.3 Install the second DXH4 24
4.4 Connect to the network..... 24
4.5 Connect the zero clients to the host PC. 24
4.6 Check the other Ethernet connection.... 24

5. Install a DXH4 with a network expansion card (DXEC) 25

5.1 Before you install a DXEC 25
5.2 Install the DXH4 25
5.3 Install the network expansion card..... 25
5.4 Connect the zero client to the host PC .. 25
5.5 Check the DXH4 Ethernet connection.... 25

6. Introduction to PCoIP..... 27

6.1 What is PCoIP?..... 27
6.1.1 Host rendering..... 27
6.1.2 Multi-codec display processing 28
6.1.3 Dynamically adapts to network conditions 28
6.2 About PCoIP hosts..... 28
6.2.1 Host function..... 28
6.2.2 Host types..... 28
6.3 About PCoIP zero clients..... 28
6.3.1 Functionality..... 28
6.3.2 Data handling 28
6.4 Benefits of PCoIP zero clients..... 28
6.4.1 Increased security 28
6.4.2 Low maintenance 29
6.4.3 Cost savings 29
6.5 PCoIP management tools..... 29
6.5.1 PCoIP Management Console 29
6.5.2 Administrative Web Interface (AWI)..... 30
6.5.3 On Screen Display (OSD)..... 30

7. Set up a PCoIP session..... 31

7.1 Power up the zero client 31
7.2 Types of PCoIP session 31
7.2.1 Auto Detect 31
7.2.2 Connect directly to a specified host 31
7.2.3 Connect to a choice of hosts using SLP Discovery 32
7.2.4 PCoIP Connection Manager..... 32
7.2.5 PCoIP Connection Manager + Auto-Logon 32
7.2.6 Connect using VMware View 32
7.2.7 Connect with View Connection Server and Auto-Logon 32
7.2.8 Connect using a connection broker..... 32
7.3 Set an automatic connection 33
7.4 Disconnect from a host PC or virtual desktop 33
7.5 Further information 33

8. Manage the network 35

8.1 Find the DXH4 MAC address 35
8.2 Discover the IP address..... 35
8.2.1 Use the DHCP server to identify the IP address 35
8.2.2 Use DOS command window to identify the IP addresses..... 35
8.2.3 Use a TFTP window to identify the IP address 35
8.3 How to change the IP address 35
8.4 Consider network bandwidth requirements 36
8.4.1 Factors affecting bandwidth..... 36
8.4.2 What happens when available bandwidth is

exceeded 36
8.5 Dual redundant network connections ... 36
8.6 Choose a connection broker if required 36
8.6.1 Role of the connection broker 36
8.6.2 Specify the connection broker 36
8.6.3 Using the connection broker 37
9. Firmware updates 38
9.1 Manage the DXH4 firmware 38
9.1.1 Teradici Administrative Web Interface (AWI) . 38
9.2 To login with the AWI 38
9.3 Check the Teradici firmware 39
9.3.1 Keep firmware up to date 39
9.3.2 Check the Teradici firmware 39
9.4 Update the Teradici firmware 39
9.4.1 Update the Teradici firmware 39
9.5 Check the BSM firmware is up to date .. 40
9.5.1 Check the BSM firmware on an individual host card 40
9.6 How to update the BSM firmware for Teradici host firmware 4.9.0 and later ... 40
9.6.1 Get the BSM firmware update file 40
9.6.2 Activate the BSM network remotely 40
9.6.3 Activate the BSM network locally (optional) .. 41
9.6.4 Upgrading multiple units 41
9.6.5 Transfer the firmware package to the target BSM 41
9.6.6 Confirm that the firmware has updated 41
9.6.7 Deactivate the BSM network interface 41
9.7 Update the BSM firmware for Teradici host firmware older than 4.9.0 42
9.7.1 Get the BSM firmware update file 42
9.7.2 Find the current version of the BSM firmware (optional) 42
9.7.3 Calculate the MAC address of the BSM 42
9.7.4 Activate the BSM network interface and acquire an IP address 43
9.7.5 Upgrading multiple units 43
9.7.6 Transfer the firmware package to the target BSM 43
9.7.7 Confirm that the firmware was updated 44
9.7.8 Deactivate the BSM network interface 44
10. Troubleshooting 46
10.1 How to remove the DXH4 46
10.2 Factory reset using a jumper 46
10.3 Check the function of the Ethernet connection in an octal configuration 47
10.4 Fan maintenance 47
10.4.1 Fan fault LED indication (firmware dependent) 47
11. Technical specifications 48
11.4.1 Warranty 48
11.4.2 Technology 48
11.4.3 Environment 49

List of figures

Figure 1:*Remove the full-height I/O bracket* 12

Figure 2:*Put the low-profile I/O bracket in place* 13

Figure 3:*Completed assembly with low-profile I/O bracket* 13

Figure 4:*Remove the low-profile I/O bracket* 13

Figure 5:*Put the full-height I/O bracket in place* 13

Figure 6:*Completed assembly with low-profile I/O bracket* 13

Figure 7:*Front panel features* 15

Figure 8:*STATUS (link) LED* 16

Figure 9:*Network LEDs on the DXH4* 17

Figure 10:*DXH4 connections* 18

Figure 11:*Examples of PCIe slots* 19

Figure 12:*PCIe auxiliary power socket* 19

Figure 13:*RPC cable connection* 20

Figure 14:*Example SFP modules* 20

Figure 15:*The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered* 21

Figure 16:*Dual DXH4 network solutions* 23

Figure 17:*PCIe slot examples* 23

Figure 18:*Connect the PCIe and Interlink cables* 24

Figure 19:*Check the status LEDs* 24

Figure 20:*Typical PCoIP set up* 27

Figure 21:*PCoIP Management Console home page* 29

Figure 22:*Administrative Web Interface* 30

Figure 23:*OSD Connect screen* 30

Figure 24:*Session selection drop down list* 31

Figure 25:*Direct to Host connection type* 31

Figure 26:*The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered* 32

Figure 27:*View Connection Server selection* 32

Figure 28:*Connection Management Interface selection* 32

Figure 29:*OSD Automatic connection screen* 33

Figure 30:*Disconnect option on the OSD*.....33

Figure 31:*Location of the MAC address on the card* 35

Figure 32:*Administrative Web Interface* 38

Figure 33:*AWI home screen* 38

Figure 34: *AWI hardware and firmware version information* 39

Figure 35:*Firmware Upload window*.....39

Figure 36:*Successful upload window* 39

Figure 37:*BSM network details* 40

Figure 38:*TFTP utility client settings window* 41

Figure 39:*Finding the IP address using the DHCP console* 43

Figure 40:*TFTP utility client settings window* 43

Figure 41:*Position of the jumper contacts* 46

Figure 42:*Status LEDs on the DXH4*.....47

List of tables

Table 1:*STATUS PCoIP LED activity* ..... .16

Table 2:*ACTIVITY status LED indication* ..... .17

Table 3:*SPEED status LED indication* ..... .17

Table 4:*Zero client management tools* ..... .29

Table 5:*PCoIP bandwidth requirements* ..... .36

Table 6:*TFTP utility client settings* ..... .41

Table 7:*MAC address conversions* ..... .42

Table 8:*TFTP utility client settings* ..... .44

Table 9:*Video, technology and network specifications* ..... .48

Table 10:*Environmental specifications* ..... .49

Before you start

1

1. Before you start

This manual is for the Amulet Hotkey DXH4 and DXH4-M Remote Workstation Host Cards. Before you install the DXH4 or DXH4-M, make sure you read the following information.

1.1 Introduction

The Amulet Hotkey DXH4 is a PCoIP workstation host card for remote desktop applications that require pixel-perfect video across multiple monitors.

1.1.1 PCoIP protocol

The DXH4 uses the Tera2240 PCoIP processor to remote up to four heads of pristine graphics in a secure and responsive way.

1.1.2 Video resolutions

It is an ideal host solution for remote desktop applications that require pixel perfect video across multiple monitors.

A single DXH4 card can support either

- four normal resolution 1920 x 1200 displays, or;
- two high resolution 2560 x 1600 displays.

1.1.3 Active cooling

The DXH4 uses dynamic fan cooling. The fan operates between 0-100% as required, depending on load and ambient conditions.

1.2 DXH4 models

The DXH4 is a x4 PCI express (PCIe) card that also fits in x8 and x16 slots. It is available with the following variations:

1.2.1 Network solutions

DXH4: The standard card has a single RJ45 network port;

DXH4-M: This model has a single network port that accepts either a fiber or copper SFP module (see 1.5 and Figure 7).

1.2.2 Terminology

The general term 'host card' is used throughout this manual to describe all network and thermal variants.

1.3 Simple installation

Installation is simple. The DXH4 has a half-height, half-length form factor. It comes fitted with either a low-profile (half-height) or full height I/O bracket with the other size included in the kit.

To change the I/O bracket, see 1.10.

The DXH4 requires no special drivers and installs into a PCIe slot (it can also run in standalone mode). The kit includes four cables to connect video outputs from the graphics cards to Mini DisplayPorts on the DXH4.

1.4 Auxiliary power requirements

Some versions of the DXH4 include a supplemental power socket (see 3.4.1 Connect auxiliary power (Optional)). If this socket is fitted, you can use it to power a DXH4 when there are no free PCIe sockets in the host computer.

Note: If you want to use a single DXH4 solely to provide additional video channels, it is possible to power the DXH4 from the supplemental power socket while using a local USB keyboard and mouse to control the host computer.

1.5 SFP modules

Amulet Hotkey can provide a range of suitable SFP modules, including 1Gbps and 100Mbps fiber SFP modules for single or multi-mode fiber and copper SFP modules with RJ45 connectors. See the Amulet Hotkey SFP Modules Datasheet for details of currently available modules.

Be aware that SFP modules have differing specifications, and the distances over which they can drive a signal can vary. This especially applies to fiber SFP modules.

Important! The DXH4-M only supports certain models of SFP module. If in doubt, contact Technical Support for advice.

1.6 IP and MAC addresses

Before you set up a host card, make a note of these details:

- MAC and IP address of the remote PCoIP host;
- MAC and IP address of the zero client.

You will find the MAC address information written on the underside of the zero client and on the configuration record/ serial number label of the remote host card. You can also use the AWI (see 6.5.2) to find the MAC addresses

If your network uses DHCP, the host and zero client obtain their IP addresses from the DHCP server. If no DHCP server is available, the host and zero client time out after approximately two minutes and adopt the following default IP addresses:

- **Zero client:** 192.168.1.50
- **Host card:** 192.168.1.100

It is important to set the default fallback IP address as soon as possible. See 3.8 STEP 8: Change the default IP address for how to set the IP address and 8.2 Discover the IP address for how to discover the IP address if it has been changed from the default.

1.7 Wake on LAN and remote power cycling

By default, the DXH4 supports Wake on LAN (WoL), allowing users to wake up the host from standby. To power down or power cycle the host computer from a remote zero client requires the installation of a Remote Power Cable (RPC).

There are two options for setting up WoL depending on whether your system supports it directly or not:

- WoL supported;
- WoL not supported - RPC cable required.

1.7.1 WoL supported

Most computers support WoL, though it may not be enabled by default. When WoL is enabled on the host computer, end-users can wake up the host computer automatically when they connect to it from a remote zero client.

WoL requires appropriate BIOS support. Refer to your host computer documentation for details about enabling this feature.

Example: To enable WoL for Windows 8 computers, you must edit the Magic Packet and power management properties of the appropriate network adapter.

1.7.2 WoL not supported - RPC cable required

For an alternative setup, you can install a Remote Power Control (RPC) cable assembly to interpose the DXH4 between the host computer's power switch and the associated motherboard header (see 3.4.2 Connect Remote Power Cable (Optional)). Specifically, connect the RPC cable to the RPC socket on the DXH4 (see 2.6 Internal card connections).

This allows users to power cycle the host computer from a remote zero client. Unlike the WoL setup, the RPC setup also allows users to power cycle, power up and fully power down the remote PC (for example, if it has blue-screened).

After connecting the RPC cable assembly:

- users of Amulet Hotkey DX zero clients can use the On Screen Display (OSD) to power cycle the host computer.

1.8 Video inputs

1.8.1 Standard video resolution

The DXH4 can support a standard video resolution of 1920 x 1200 on four screens when all four video inputs are used.

1.8.2 High video resolution

The DXH4 can support a high video resolution of 2560 x 1600 on two screens when two video inputs are used.

Note: The DisplayPort video inputs are dual mode. This means you can connect both DisplayPort and DVI-D outputs to the DXH4 video inputs using suitable cable adaptors.

1.9 Management tools and connection brokers

Management tools are available to establish and configure PCoIP links between the DXH4 and a zero client.

You can configure zero clients to use a third party connection broker (such as VMware View Connection Server) to dynamically assign DXH4 hosts to zero clients based on the identity of the end-user. Connection brokers can also allocate a pool of DXH4 hosts to a group of zero clients. See 8.6 for more information.

1.10 Change the I/O bracket (optional)

1.10.1 Change a full-height bracket to a low-profile bracket

1. Remove two screws from the bracket and keep. See Figure 1.

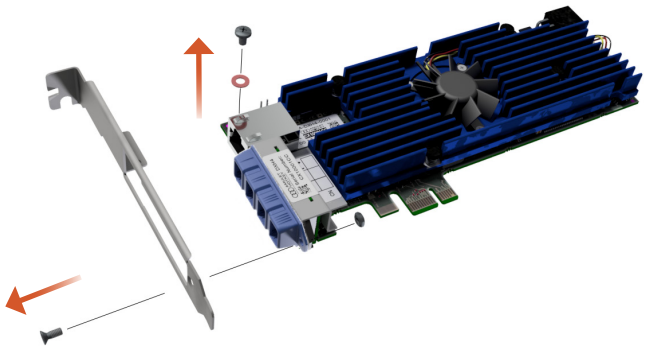


Figure 1: *Remove the full-height I/O bracket*

2. Remove the bracket carefully (the video connector molding is loose when the bracket is removed). See Figure 1.

3. Put the new bracket in place over the connector molding. See Figure 2.

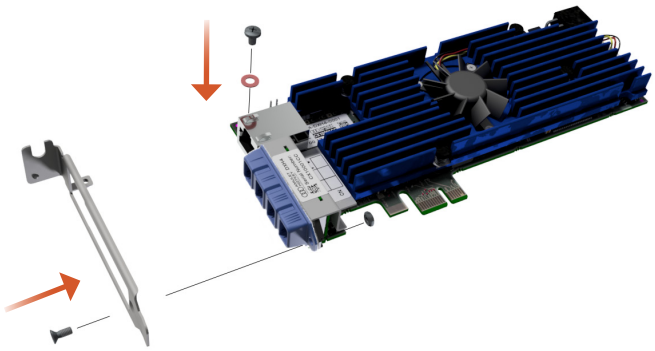


Figure 2: *Put the low-profile I/O bracket in place*

4. Install the two screws in the low-profile bracket to fix it in place. See Figure 2 and Figure 3.

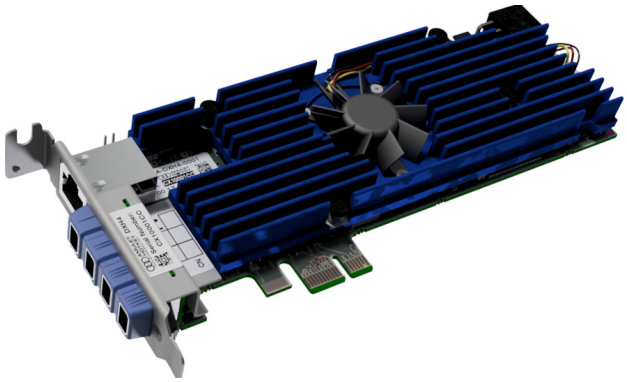


Figure 3: *Completed assembly with low-profile I/O bracket*

1.10.2 Change a low-profile bracket to a full-height bracket

1. Remove two screws from the bracket and keep. See Figure 4.

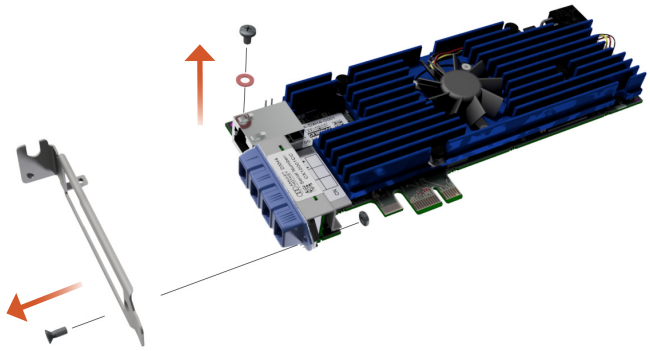


Figure 4: *Remove the low-profile I/O bracket*

2. Remove the bracket carefully (the video connector molding is loose when the bracket is removed). See Figure 4.

3. Put the new bracket in place over the connector molding. See Figure 5.

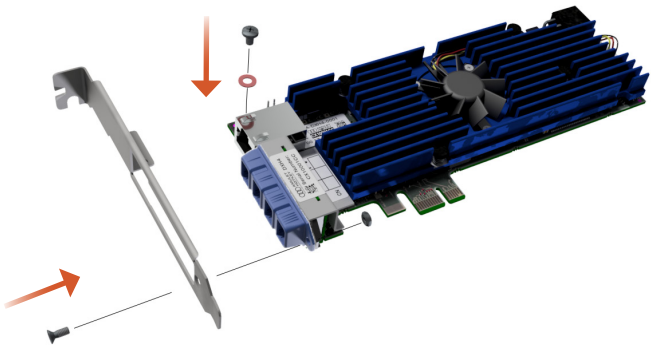


Figure 5: *Put the full-height I/O bracket in place*

4. Install the two screws in the full-height bracket to fix it in place. See Figure 5 and Figure 6.

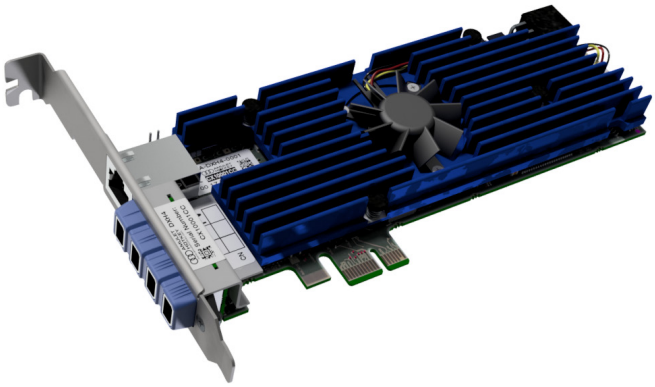


Figure 6: *Completed assembly with low-profile I/O bracket*

Your DXH4

2

2. Your DXH4

The DXH4 has four LEDs, a network port, four video input sockets and a recessed button. These are described in the sections that follow.

2.1 I/O bracket features

The standard DXH4 has a small (half-height and half-length) form- factor.

The DXH4 also comes with a standard-profile (full height) I/O bracket included in the kit.

See Figure 7 for the following description:

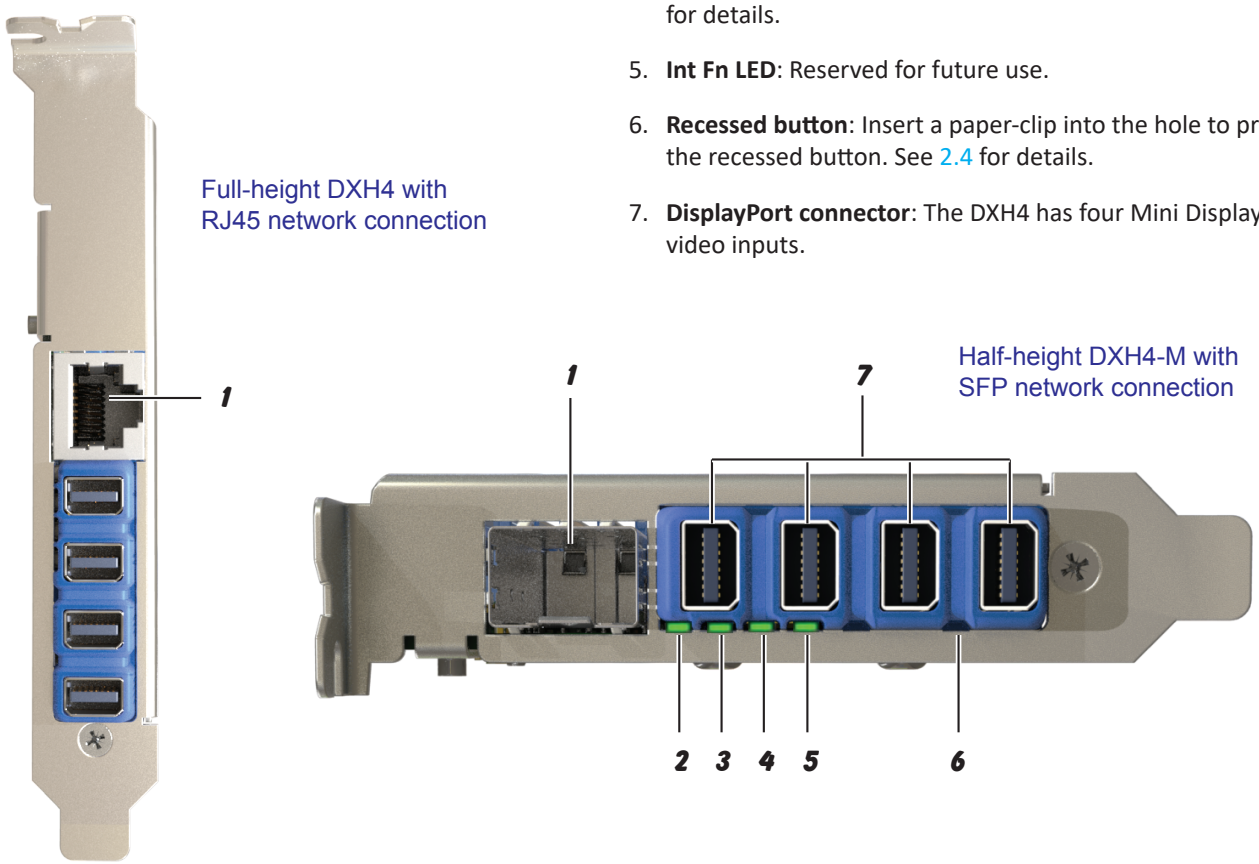


Figure 7: *Front panel features*

1. **Network port**: The standard DXH4 has an RJ45 socket. The DXH4-M has a socket that accepts an SFP module. See the SFP Datasheet for details of modules available separately from Amulet Hotkey.
2. **Network SPEED LED**: Indicates the network speed. See 2.2.3 for details.
3. **Network ACTIVITY LED**: In normal operation, this LED shows network activity. It can also show progress for firmware updates. See 2.2.3 for details.
4. **Network STATUS LED**: Shows the PCoIP link status. See 2.2.2 for details.
5. **Int Fn LED**: Reserved for future use.
6. **Recessed button**: Insert a paper-clip into the hole to press the recessed button. See 2.4 for details.
7. **DisplayPort connector**: The DXH4 has four Mini DisplayPort video inputs.

2.2 I/O bracket status LEDs

The status LEDs on the I/O bracket (see Figure 7) show the status of the network connection including:

- the connection type and speed;
- the current network activity;
- the status of the PCoIP connection to a zero client.

There are four LEDs on the front panel:

- INT FN LED (not used);
- STATUS (link) LED;
- ACTIVITY (PCoIP) status LED;
- and the SPEED status LED.

See Figure 7, Figure 8 and Figure 9.

2.2.1 Key

The tables in this section use the following conventions:

- Color - LED is on steady;
- Flash - LED is on and off evenly;
- Blink - LED is on more than off;
- Wink - LED is off more than on.

2.2.2 STATUS LED

The host card has a STATUS (link) LED to indicate the type and status of the network connection.

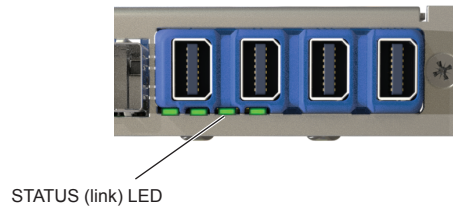


Figure 8: *STATUS (link) LED*

The STATUS LED displays the following indications.

LED status	Meaning
Off	No PCoIP link is established
Green wink	Copper network connection is detected (SFP module or RJ45). Network link is not in session
Green	Copper network connection with link established (SFP module or RJ45)
White flash	BSM status indication. See 2.3.
Red wink	Minor card error (for example cooling fan not working).
Red flash	Major card error
Red	Power error
For SFP Modules only:	
Green wink	SFP copper network connection is available but not in session (or no SFP module inserted)
Blue wink	SFP fiber network connection is available but not in session (or no SFP module inserted)
Blue	SFP fiber module detected; connected to network
Cyan wink	SFP module is not recognized

Table 1: *STATUS PCoIP LED activity*

2.2.3 Network ACTIVITY and network SPEED LEDs

The host card has two network LEDs, ACTIVITY (link) and SPEED (see Figure 9) on the rear panel that operate as follows:

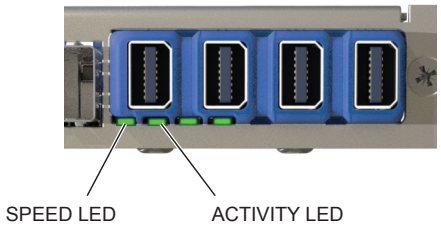


Figure 9: *Network LEDs on the DXH4*

1. **Network ACTIVITY LED**

In normal operation, this LED shows network activity and connection type. It can also show progress for firmware updates.

NORMAL MODE	
Status	**Meaning**
Off	No network connection
Green	Network connection full duplex; no traffic
Green blink	Network connection full duplex; traffic detected
Red wink	Fault with Teradici PCoIP: Half duplex connection **Warning:** A half duplex connection will severely limit a user's experience. PCoIP sessions may disconnect with large packet losses reported in the PCoIP connection statistics.
White flash	BSM status indication. See 2.3.
FIRMWARE UPDATE MODE	
Status	**Meaning**
Amber	BSM network port is open and attempting to obtain a DHCP address
Blue	BSM network port is open and has a valid IP address (either a DHCP address or the BSM fall-back address of 192.168.1.75)
Blue wink	BSM update is complete. The BSM network port is closed. Restart the host computer at a convenient time to apply the new firmware
Red wink	BSM update failed to complete (the checksum validation failed). The BSM network port is closed. Restart the host computer at a convenient time to flush the new firmware from flash memory
White	BSM status indication. See 2.3.

Table 2: *ACTIVITY status LED indication*

2. **SPEED status LED**

Status	Meaning
Off	No network connection
Amber	100 Mbit/s connection
Green	1 Gbit/s connection
White flash	BSM status indication. See 2.3.

Table 3: *SPEED status LED indication*

2.3 BSM status indication

When power is applied to the Board Support Micro-controller (BSM) or when the BSM is reset (for example, after a successful firmware update), all LEDs simultaneously flash white (or very pale blue) for one second.

2.4 Recessed button operations

2.4.1 While the DXH4 is starting up

- press the button to restore the DXH4 factory settings.

2.4.2 When the DXH4 is powered up

- A long press (hold the button for five seconds or more) toggles the Board Support Micro-controller (BSM) network interface ON or OFF.

  When the network interface is ON, you can update DXH4 firmware remotely by transferring a firmware package to the BSM.

2.5 Video inputs

2.5.1 Setup for quad monitors

The maximum video resolution is 1920 x 1200 per input.

2.5.2 Setup for dual monitors

If you need higher resolution monitors (up to 2560 x 1600 maximum), you can only use two video inputs on the DXH4.

2.5.3 Use the correct ports

You can use any of the available video inputs, make sure that the monitors are plugged into the two corresponding video outputs on the zero client. It is a good idea to use video inputs 1 and 2 on the DXH4 and video outputs 1 and 2 on the zero client.

Use the supplied video cables to connect the DXH4 video inputs to outputs on the host computer's graphics card.

Note: The DisplayPort video inputs are dual mode. This means you can connect both DisplayPort and DVI-D outputs to the DXH4 video inputs using suitable cable adaptors.

2.6 Internal card connections

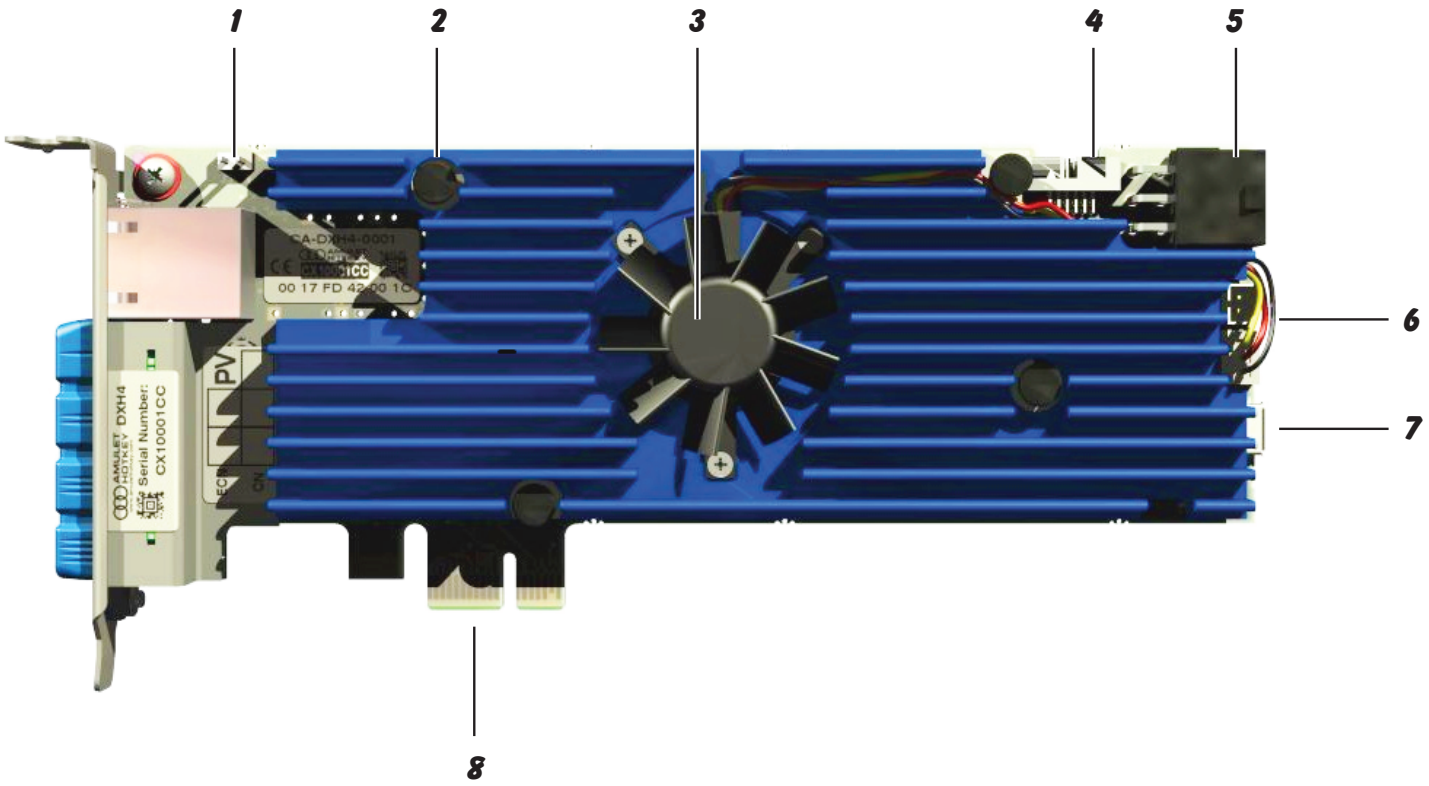
The DXH4 card has several internal sockets and jumpers. These connections are not accessible through the I/O bracket.

1. **Factory default reset jumper pin**: (Jumper is not fitted) To enable a factory reset without using the button, do the steps in 10.2. (To reset using the button see 2.1 and 2.4).
2. **Serial output jumper pins**: Reserved for factory use.
3. **Fan**: The fan speed adjusts automatically between 0-100%, depending on load and environmental conditions.

   Note: If prevailing conditions do not require fan-cooling, the fan may not spin at all. However, it will still activate briefly every hour for self-testing.
4. **Inter-card connection socket**: This socket is used to connect two DXH4s together for a maximum of eight displays (octal mode), or for connecting the DXEC expansion card. See 4. How to install dual DXH4 cards and 5. Install a DXH4 with a network expansion card (DXEC) for how to do this.
5. **Auxiliary ('aux') power socket**: Use this socket to power a DXH4 card if there are no free PCIe sockets in the host computer. See section 4.3 for details.
6. **RPC socket**: If required, this socket connects the DXH4 to the motherboard using a suitable Remote Power Control (RPC) cable assembly. This connection may be required to power cycle the host computer from a remote zero client.

   See 1.7 Wake on LAN and remote power cycling for details.
7. **Micro-USB Type AB**: This socket is not currently used by the DXH4, but allows an internal connection to a USB port on the host computer. Future versions of the DXH4 may use this socket for firmware updates or other new features.
8. **PCIe x4 edge connector**: This ×4 connector fits into a PCIe slot. It is also compatible with x8 and ×16 slots.

Figure 10: *DXH4 connections*



Install the DXH4

3

3. Set up the host card

This section describes how to set up your DXH4. For card information, see 2. Your DXH4.

3.1 STEP 1: Prepare the PC, Workstation or server

! Caution: *The host PC must be switched off before you install or remove the DXH4.*

1. Turn off the host computer.
2. Unplug the power cable.
3. Wait at least 60 seconds to allow the internal power rails to fully discharge.
4. Remove any covers to provide access to the PCIe sockets.

3.2 STEP 2: Fit the correct I/O bracket

Before you install the DXH4 card, make sure that the correct bracket (full-height or low-profile) is installed. See also Change the I/O bracket (optional) (on page 12).

To change the bracket:

1. Remove the screws from the bracket and retain.
2. Remove the bracket.
3. Hold the other bracket in position and replace the screws.

3.3 STEP 3: Install the DXH4

! Caution: *Make sure you wear a wriststrap and follow anti-static precautions before you handle any cards, or work on the PC.*

1. Make a note of the MAC address on the label of the DXH4. You may need this when pairing the DXH4 to a zero client.
2. Carefully install the DXH4 into a free x1, x4, ×8 or ×16 PCIe socket. See Figure 11.
3. Secure the I/O bracket.

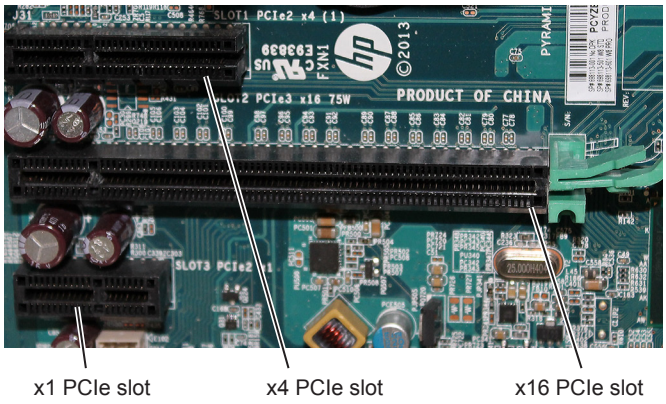


Figure 11: *Examples of PCIe slots*

3.4 STEP 4: Connect optional equipment

3.4.1 Connect auxiliary power (Optional)

The DXH4 can accept connection to auxiliary power within the host PC or Workstation (depending on your system) if no PCIe slot is available.

Contact Amulet Hotkey for auxiliary power cable advice.

1. If required, connect the host system's power or motherboard power supply to the auxiliary PCIe power socket. See Figure 12.

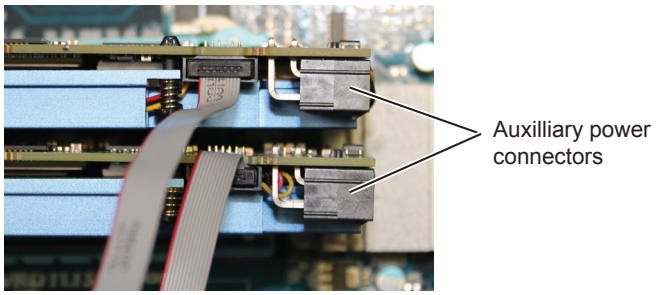


Figure 12: *PCIe auxiliary power socket*

3.4.2 Connect Remote Power Cable (Optional)

Important! Some workstations may require a RPC to implement remote power-cycling. See 1.7 Wake on LAN and remote power cycling.

Note: The DXH4 comes with a generic RPC cable assembly. We recommend that you contact Amulet Hotkey technical support to make sure this is suitable for your needs.

1. Disconnect the existing power cable between the power button (4) and the motherboard (3). See Figure 13.

2. Connect the RPC cable (1) between the RPC socket on the DXH4 (2) and the motherboard (3) and the PC power button (4).

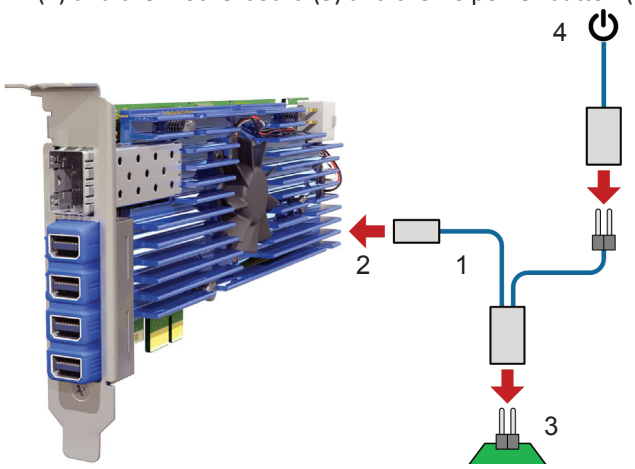


Figure 13: *RPC cable connection*

Key to Figure 13.

1. RPC assembly. **2.** RPC socket on the DXH4 **3.** Motherboard power switch header on the host computer **4.** Front panel power switch on the host computer

3.4.3 Connect SFP module (DXH4-M only)

1. Fit the required SFP module into the DXH4-M network socket.

This socket accepts a copper or fibre SFP module. The module can be 1 Gbit/s or 100 Mbit/s. See the SFP modules datasheet for more details of available modules.

Figure 14: *Example SFP modules*

3.5 STEP 5: Connect the video inputs

1. For quad monitors, use the supplied video cables to connect each of the DXH4 video inputs to outputs on the host computer's graphics card.

2. For dual monitors, you can use any of the available video inputs, but the monitors must plug into the two corresponding video outputs on the zero client.

Important! It is best to use video inputs 1 and 2 on the DXH4 and video outputs 1 and 2 on the zero client.

3.6 STEP 6: Connect the DXH4 to the network

1. Connect a network cable to the DXH4.

3.7 STEP 7: Complete the installation

1. Re-assemble the host computer, make sure all blanking plates are fitted, and reconnect the power cable.

2. Restart the computer.

The operating system detects the DXH4 and locates the appropriate drivers.

3. Install the driver on the host computer.

4. (Optional) If you need to install a second DXH4, see 4. How to install dual DXH4 cards.

5. (Optional) If you need to install a network extender card, see 5. Install a DXH4 with a network expansion card (DXEC).

Note: You may not install dual DXH4s and a network extender card in the same installation.

3.8 STEP 8: Change the default IP address

! Caution: *Change the default IP address as soon as possible.*

If your network uses DHCP, the DXH4 obtains its IP address from the DHCP server. If no DHCP server is available, the DXH4 times out after three minutes and adopts its default IP address of 192.168.1.100.

All DXH4 cards will revert to the same default IP address, this can cause conflicts as the network grows. Use the Administrative Web Interface (AWI) to assign a different static IP address from the default.

1. Enter the default IP address of the DXH4 into a browser to access the AWI. See 6.5.2 Administrative Web Interface (AWI) for more information.

2. Enter the default password **ahkdante** and click **Log In**.

3. From the **Configuration** menu select the **Network** option.

4. Make sure the **Enable DHCP** option is unchecked.

5. Enter the new fall-back default IP address into the **IP Address** fields.

6. Make sure the **Enable DHCP** option is checked.

3.9 STEP 9: Connect a zero client to the DXH4

1. Install and power up a zero client.

   If you are not sure how to do this, see the relevant Amulet Hotkey user manual or Quick Start Guide for the zero client.

After powering up the zero client, you are ready to establish a new PCoIP session.

The zero client connects to the DXH4 via the network port.

Note: We recommend reading 6. Introduction to PCoIP first if you are not already familiar with the concept of PCoIP.

3.9.1 Connect to a DXH4 using SLP Discovery

Important! This is one method you can use to quickly connect your zero client to a host. For a detailed description of all connection methods, see 7. Set up a PCoIP session.

If the zero clients and PCoIP hosts reside on the same subnet, you can use the **Direct to Host + SLP session** connection type to discover available PCoIP hosts on the subnet.

You must know the IP address (or MAC address) of the PCoIP host that you want to connect to.

1. Select the **Direct to Host + SLP Host Discovery** session connection type from the drop down list.

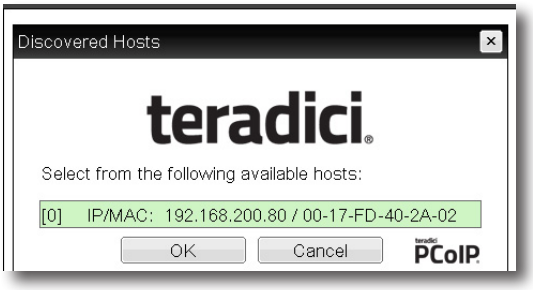


Figure 15: *The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered*

2. Select the host you want and click **OK**.

   If the zero client successfully connects to the host, the front panel PCoIP status LED illuminates green to indicate an active session.

3. (Optional) You can also set the **Enable Auto-Reconnect** in the advanced settings to remember the last connected PCoIP host.

Note: You must also configure a **Direct from Client** session connection type on the host.

3.10 STEP 10: Change the default password

1. For security, we recommend that you change the default password for your DXH4 at the earliest possibility.

Important! You must enter a password before changing the configuration of host cards and zero clients. The factory pre-set password for all Amulet Hotkey host cards and zero clients is **ahkdante**.

3.11 Set up is complete

If you wish to read further about network considerations, refer to 8. Manage the network.

For any configuration or deployment issues refer to 9. Firmware updates or contact Technical Support department (see contact details at the start of this manual).

Install dual DXH4 cards

4

4. How to install dual DXH4 cards

To set up an eight display configuration (octal mode), install two DXH4s and connect them with two zero clients.

This information tells you how to install two DXH4s into a regular PC. There may be slight variations for other PCs or workstations.

Note: There are three network solutions. See Figure 16.

A. Two DXH4 cards with independent network links

B. Two DXH4 cards with a single network link, linked internally

C. Two DXH4 cards with a two network links, linked internally

! Caution: *Do not install dual* DXH4 *cards with two network links (Option C below) onto a single network unless that network supports Spanning Tree Protocol (STP).*

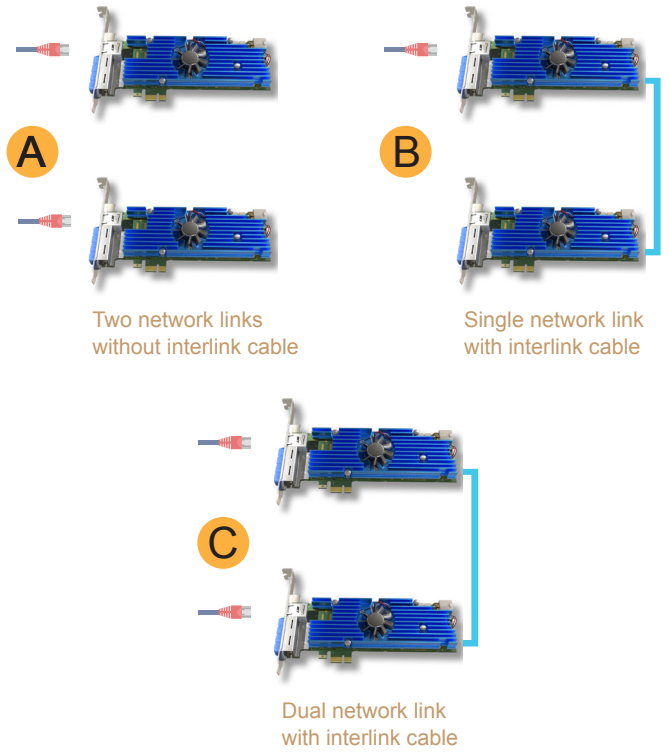


Figure 16: *Dual DXH4 network solutions*

4.1 Before you install the DXH4s

1. Make sure that the PC power cable is unplugged before you install the DXH4s.

2. Make sure you wear a wriststrap or follow suitable anti-static precautions before you handle any cards or work on the PC.

3. Make a note of the MAC address on the label on each DXH4.

Example: MAC: 00 17 FD 46 03 56

4.2 Install the first DXH4

You will need one interlink cable to connect the DXH4 cards.

1. (For network solution B only) Connect one end of the interlink cable to the connector on the first DXH4.

2. Install the first DXH4 into any free x8 or x16 PCIe slot in the host PC. See Figure 17.

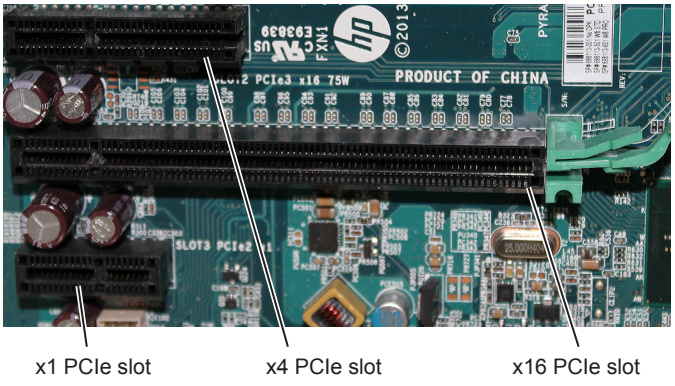


Figure 17: *PCIe slot examples*

4.3 Install the second DXH4

1. (For network solution B only) Connect the free end of the interlink cable to the second DXH4.

2. Install the second DXH4 into any free x1, x4, x8 or x16 PCIe slot in the host PC.

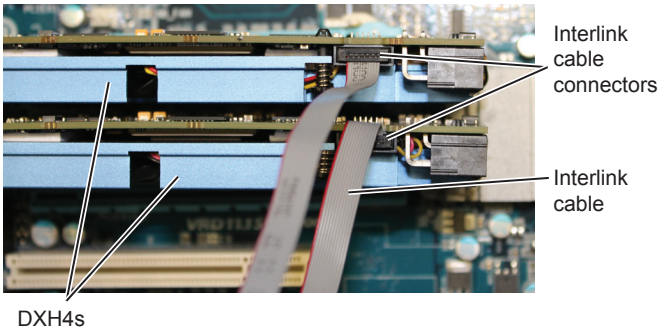


Figure 18: *Connect the PCIe and Interlink cables*

3. Make sure the DXH4 mounting bracket is fixed securely in the PC.

4.4 Connect to the network

1. For network solution B: connect an Ethernet cable to **one** of the DXH4s.

2. For network solution A: connect an Ethernet cable to **both** DXH4s.

4.5 Connect the zero clients to the host PC

1. Connect the power cable to the PC

2. Turn on the host PC and wait for both DXH4s to power up. See Figure 19.

   The STATUS and INT FN LEDs are GREEN and flash on both DXH4s.

   The ACTIVITY LED flashes GREEN to show network activity, the SPEED LED is AMBER (or GREEN depending on link speed) and ON on the DXH4 connected to the Ethernet cable.

   The ACTIVITY and SPEED LEDs are OFF on the DXH4 with no Ethernet cable.

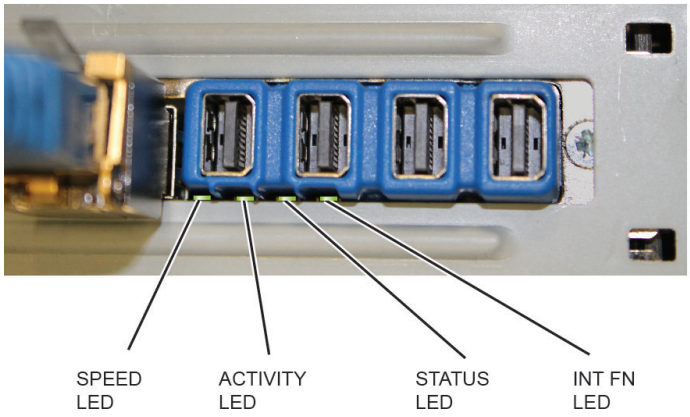


Figure 19: *Check the status LEDs*

3. Connect a zero client to the first DXH4.

   Example: Set the connection type to SLP and Host Discovery and select the MAC address from the available list of hosts on each zero client.

4. Connect a zero client to the second DXH4.

4.6 Check the other Ethernet connection

1. Make sure that eight heads of video are present.

2. Disconnect the Ethernet cable from the first DXH4 and connect to the second DXH4.

   When you swap the cable from the first DXH4 to the second DXH4 the zero clients temporarily indicate a loss of signal and then recover the connection.

   The SPEED LED lights AMBER and ON, the ACTIVITY LED flashes GREEN on the DXH4 connected to the Ethernet cable.

Install a network expansion card

5

5. Install a DXH4 with a network expansion card (DXEC)

The network expansion card can allow you to present an Ethernet connection to the back of a PC or workstation:

- in cases where the DXH4 is installed internally and its Ethernet port is not accessible;
- for the purpose of redundancy.

Note: DXECs are supplied fitted with either half-height or full-height slot brackets. Both versions come supplied with the alternative bracket type. Make sure you have the correct bracket fitted for your system before you install the DXEC.

The information below tells you how to install one DXH4 and a network expansion card into a standard PC. There may be slight variations for other PCs or workstations.

! Caution: *It is not possible to use a DXEC with an octal configuration.*

See also the *DXEC Quick Start Guide*.

5.1 Before you install a DXEC

1. Shut down the host PC.
2. Remove the power cable from the host PC.
3. Make sure you wear a wriststrap or follow suitable anti-static precautions before you handle any cards or work on the PC.
4. Make a note of the MAC address on the label on the DXH4.

Example: MAC: 00 17 FD 46 03 56

5.2 Install the DXH4

1. Connect one end of the interlink cable to the connector on the DXH4. See item 4. in Figure 10: DXH4 connections.
2. Install the DXH4 into a free x1, x4, x8 or x16 PCIe slot in the host PC or workstation.

5.3 Install the network expansion card

1. Push the interlink cable connector into connector A on the DXEC card.
2. Install the DXEC card into any free 1x, 4x, x8 or 16x PCIe slot in the host PC or workstation.
3. Connect an Ethernet cable into the expansion card.
4. Replace any covers.
5. Connect the power cable to the PC.
6. Turn on the host PC.

The large LED on the DXEC card is AMBER then GREEN to indicate that the DXH4 card has detected the expander card.

The small green LED flashes on the front of the DXEC card.

The STATUS LED is ON and GREEN on the DXH4.

The INT FN LED is flashing and GREEN on the DXH4.

5.4 Connect the zero client to the host PC

1. Connect a zero client to the DXH4.

Example: Set the connection type to SLP and Host Discovery and select the MAC address from the available list of hosts on each zero client. See 7. Set up a PCoIP session for more information on connection methods.

5.5 Check the DXH4 Ethernet connection

1. Disconnect the Ethernet cable from the DXEC card and push into the DXH4 Ethernet port.

When you swap the cable, the zero client temporarily indicates a loss of signal and then recovers the connection.

On the DXH4, the SPEED LED is ON and AMBER (or GREEN) and the ACTIVITY LED flashes GREEN.

The large LED on the DXEC card turns OFF.

Introduction to PCoIP

6

6. Introduction to PCoIP

6.1 What is PCoIP?

The PCoIP (PC-over-IP) protocol compresses, encrypts and encodes the entire computing experience on a host PC. In a PCoIP system, a PCoIP host transmits the computing experience from a host PC (pixels only) across a standard IP network to a remote zero client. Actual data never leaves the host PC and all pixel transfers are encrypted with advanced security algorithms.

PCoIP supports high resolution, full frame rate 3D graphics and HD media, multiple large displays, full USB peripheral connectivity, and high definition audio, all connected over the corporate LAN or WAN.

PCoIP technology allows all desktops in your enterprise to be centrally located and managed in a data centre, while providing remote users with full desktop performance. This may be in a geographically remote location if necessary.

There are three essential features of PCoIP:

- Host rendering;
- Multi-codec display processing;
- Dynamically adapts to network conditions.

6.1.1 Host rendering

PCoIP renders display images on the host PC (or virtual machine). Host rendering preserves the PC environment so applications perform as they should. After an image is rendered on the host, PCoIP broadcasts just the encrypted pixels (not the data) across the network to the remote client. This makes it possible to have stateless, decode-only client devices – called zero clients – with all the benefits they bring, such as low maintenance, increased security, and cost savings. See 6.2 for details.

> **Note:** This is an advantage over other remote protocols that use client rendering. To render an image on the client; each command from the host and response from the client must travel across the network. This degrades an application's performance while it waits for image rendering to complete.

Figure 20: *Typical PCoIP set up*

6.1.2 Multi-codec display processing

A PC display includes different types of image elements (text, graphics, icons, video). Using the same codec to encode all these elements would use excessive network bandwidth. Instead, PCoIP continuously analyses and decomposes image elements, using the right codec for each pixel.

PCoIP's intelligent image decomposition and encoding results in efficient transmission and decoding. This saves bandwidth while delivering the best user experience. In addition, PCoIP builds every pixel to a lossless state when they stop changing, ensuring a pixel-perfect image on the zero client regardless of network limitations.

6.1.3 Dynamically adapts to network conditions

The PCoIP protocol lets you easily set image quality settings to manage bandwidth use and delivers the best possible performance for the network conditions.

On congested networks, PCoIP adaptive encoders automatically adjust image quality within the limits you set. When the network is no longer congested, they automatically resume maximum image quality.

6.2 About PCoIP hosts

6.2.1 Host function

A PCoIP host is a card that converts a remote PC (or blade workstation) into a pixel broadcast centre. The host's Tera-series processor uses advanced algorithms to encode a user's full desktop environment, allowing the host to deliver high-end images to a zero client in any location.

In a PCoIP system, the PCoIP host is installed inside or near to the remote PC. The host takes digital video, audio and USB data generated by the PC and compresses and encrypts this data. It then transmits this data in real time over an IP network to the user's PCoIP zero client.

6.2.2 Host types

The DXP4 is a PCoIP host card that installs into a PCIe slot. Other Amulet Hotkey PCoIP hosts are available in various form factors. Some install inside a PC while others are located near to a PC and connect to video, USB and audio ports using standard cables.

Amulet Hotkey also supply a range of PCoIP blade workstations based on the class leading Tier 1 devices from Dell. These workstations include Amulet Hotkey BIOS and PCIe mezzanine cards to provide hardware GPU and PCoIP acceleration.

See our website for more information.

6.3 About PCoIP zero clients

PCoIP zero clients are secure, hardware-based endpoints that allow users to connect to a remote host PC or virtual desktop over a local or wide area IP network. They support multiple wide-screen formats, HD audio, and local USB peripherals, providing a rich multimedia experience for users.

6.3.1 Functionality

Zero clients can take many form factors, such as desktop boxes and rack-mounted cards. Amulet Hotkey DXZ4 zero clients are small, cased devices for your desktop.

Users can interact with their desktops from any type of zero client and can even continue the same session if they move between zero client devices.

6.3.2 Data handling

PCoIP zero clients use a highly integrated Tera-series processor to perform image decompression and decoding. At the desktop, they decrypt, decompress and distribute video, audio and USB data to the standard desktop peripherals, such as monitors, keyboard, mouse, and speakers or headset. A zero client also passes user-generated USB and audio data back to a remote PCoIP host (see 6.2).

To ensure desktop responsiveness, the process of image compression-encryption-transmission by the PCoIP host and then decryption-decompression by the zero client happens very quickly, typically in just one frame (or less than 15 msecs).

6.4 Benefits of PCoIP zero clients

Because zero clients just decode pixels to display images, they can be far simpler and more secure than a traditional desktop PC and other thin client solutions. They offer:

- Increased security;
- Low maintenance;
- Cost savings.

6.4.1 Increased security

As PCoIP zero clients have a stateless architecture and no local data storage, they are the most secure endpoint available.

Pixel transfers to the zero client are encrypted with advanced security algorithms. Zero clients are also immune to viruses and never need anti-virus updates. Finally, zero clients comply with the most stringent government and security mandates. In particular, they support robust USB hardware security authorization, including user authentication and single sign-on (SSO) based on smart cards, proximity cards and other SSO devices.

6.4.2 Low maintenance

Zero clients are extremely easy to manage and do not require regular updates or patches.

They have no application operating system, no general purpose CPU or RAM, no graphics processor. And they have no fan or hard disk to fail.

Because they perform only pure image decompression, they are future proof. A zero client never needs a new operating system or updates for drivers, media codecs, or anti-virus signatures. Also, a zero client does not need to know about the applications being used (it just has to decode the pixels to display the image), so there are no version dependencies between the zero client and the host PC. There is no risk that future versions of an application will render the zero client obsolete.

6.4.3 Cost savings

Zero clients have significantly lower costs than traditional PCs and thin clients. They use less power, generate less heat, and often have a smaller footprint.

Also, because they are simple devices, zero clients require minimal administration and have very low management costs. And because they are future proof, their extended life span is assured and they rarely need replacing.

For more general information about PCoIP zero clients, visit www.teradici.com.

6.5 PCoIP management tools

You can interact with PCoIP hosts and zero clients through various management tools. See Table 4.

Management tool	Description
PCoIP Management Console	Allows you to centrally administer a large numbers of PCoIP devices. You can organize zero clients into groups, define configuration profiles, and apply configuration profiles to groups.
Administrative Web Interface (AWI)	A web application that you can use to remotely configure individual zero clients and PCoIP hosts.
On Screen Display (OSD)	A user interface on the zero client that allows you to configure and view information about the local client.

Table 4: *Zero client management tools*

Note: For full details about these management tools, see the *Teradici PCoIP® Zero Client and Host Administrator Guide* (available to download from the Teradici website).

6.5.1 PCoIP Management Console

The PCoIP Management Console (see Figure 21) has a web interface that allows you to manage multiple devices (PCoIP zero clients and hosts) from a central console.

From the console, you can view the status and connection information of all PCoIP devices. You can manage devices individually or by group. For example, you can create device groups based on location or department.

In particular, you can assign configuration profiles to PCoIP devices and update device firmware (for the Teradici processor). You can also view device log files, reset devices, and control the power state of devices.

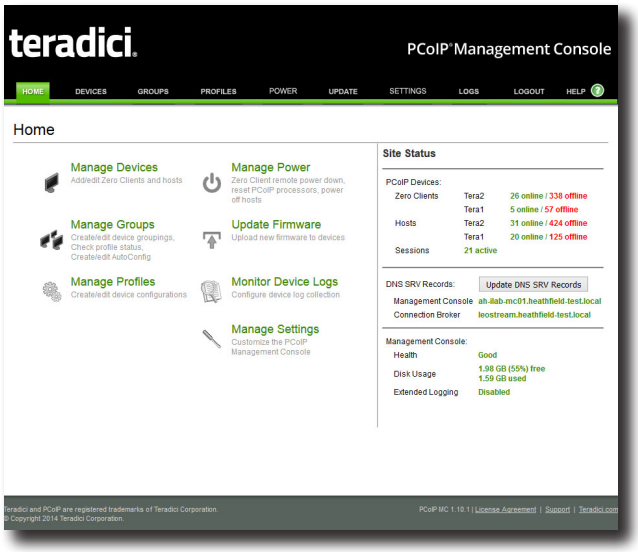


Figure 21: *PCoIP Management Console home page*

Note: The PCoIP Management Console plus supporting documentation is available for download. For more information on the PCoIP Management Console, contact Amulet Hotkey Technical Support.

6.5.2 Administrative Web Interface (AWI)

The AWI is an embedded HTTPS web interface for PCoIP devices. It enables you to remotely configure individual PCoIP hosts and zero clients using a web browser.

> **Example:** You can set device power settings, connection speeds, and define initial setup parameters. The AWI also provides tools for updating the device firmware (for the Teradici processor).

To access the AWI, browse to the IP address of the PCoIP host or zero client (see 1.6).

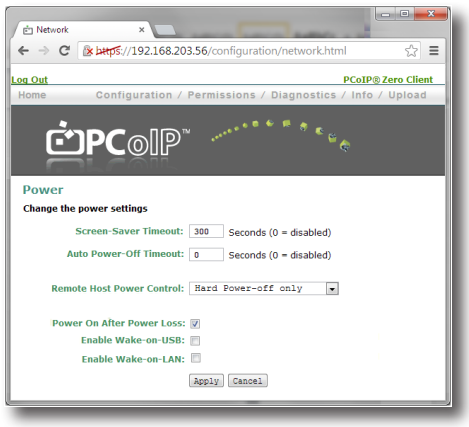


Figure 22: *Administrative Web Interface*

6.5.3 On Screen Display (OSD)

The OSD appears when the zero client is powered on and a PCoIP session is not in progress. The OSD Connect screen displays when you press the Menu button on the zero client front panel.

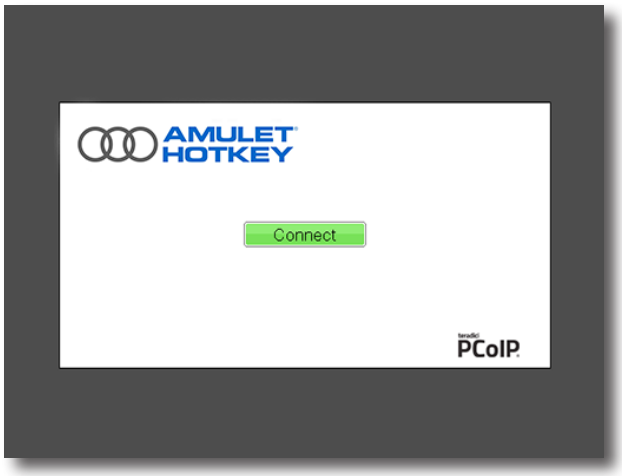


Figure 23: *OSD Connect screen*

If the zero client is in a low power state (no activity for five minutes) the zero client automatically goes into a low power state by turning off the monitors. In this case, pressing the menu button or a USB mouse/keyboard will wake the client back up. The first video head detected will show the OSD.

From the Connect screen, you can create a new PCoIP session between the zero client and a remote PCoIP host card or a virtual desktop.

The Options menu in the Connect screen gives access to various configuration pages (these pages provide a subset of the functionality provided by the AWI). You must enter a password to change any zero client settings; see STEP 10: Change the default password (on page 21).

GET CONNECTED

7

7. Set up a PCoIP session

This section describes how to connect a zero client to a remote PCoIP host or virtual desktop.

7.1 Power up the zero client

After you install the zero client, you must then establish a PCoIP session between the zero client and a remote PCoIP host or virtual desktop.

When you press the power switch on the zero client for the first time, it displays the On Screen Display (OSD) connection screen. If more monitors are connected, the menu displays on Video port 1. The connection screen will also display if the **Menu** button is pressed while the unit is on.

7.2 Types of PCoIP session

To set the type of PCoIP session the zero client will use to connect the host, use the OSD and change the configuration settings.

1. Select **Options > Configuration** and select the **Session** tab.
2. Click **Unlock and enter the password**. (Default is **ahkdante**)

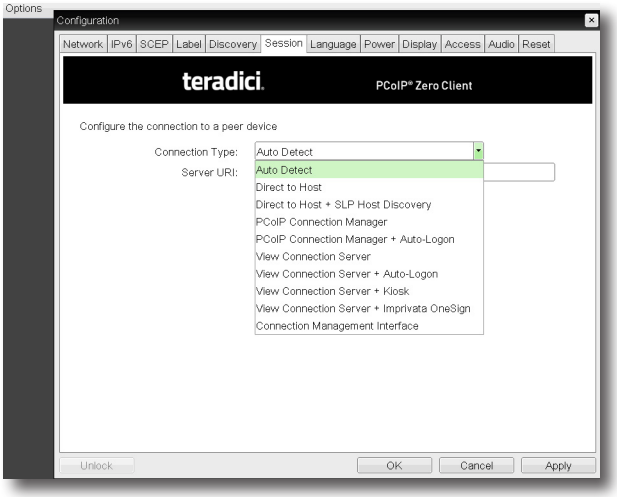


Figure 24: *Session selection drop down list*

The following connection methods are available:

- Auto Detect
- Connect directly to a specified host
- Connect to a choice of hosts using SLP Discovery
- PCoIP Connection Manager
- PCoIP Connection Manager + Auto-Logon
- Connect using VMware View
- Connect using a connection broker

Note: For full details about each connection method, refer to the Session Connection Types section of the *Teradici PCoIP® Zero Client and Host Administrator Guide*.

7.2.1 Auto Detect

With this setting, the zero client connects to the address of any specified server. This session type is used where the client must choose between virtual and physical hosts.

7.2.2 Connect directly to a specified host

Important! This connection method is not practical for very large PCoIP deployments.

1. Select the **Direct to Host** session connection type from the drop down list.

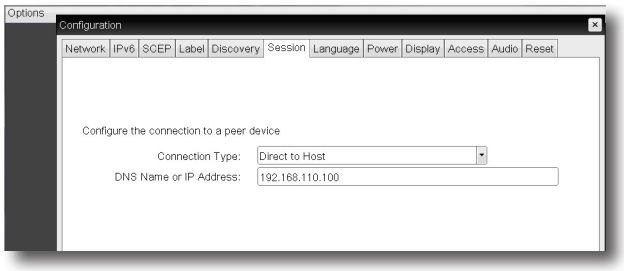


Figure 25: *Direct to Host connection type*

2. Enter the IP address (or DNS name) for the PCoIP host.

Note: You must also configure a **Direct from Client** session connection type on the host.

3. (Optional) You can also set the **Enable Auto-Reconnect** in the

advanced settings to remember the last connected PCoIP host.

7.2.3 Connect to a choice of hosts using SLP Discovery

If the zero clients and PCoIP hosts reside on the same subnet, you can use the **Direct to Host + SLP session** connection type to discover available PCoIP hosts on the subnet.

You must know the IP address (or MAC address) of the PCoIP host that you want to connect to.

> Important! Use this connection method mainly for testing and evaluation purposes.

1. Select the **Direct to Host + SLP Host Discovery** session connection type from the drop down list.

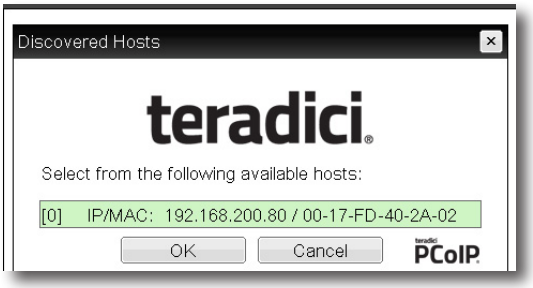


Figure 26: *The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered*

2. Select the host you want and click **OK**.

   If the zero client successfully connects to the host, the front panel PCoIP status LED illuminates green to indicate an active session.

3. (Optional) You can also set the **Enable Auto-Reconnect** in the advanced settings to remember the last connected PCoIP host.

> **Note:** You must also configure a **Direct from Client** session connection type on the host.

7.2.4 PCoIP Connection Manager

Using a PCoIP Connection Manager allows you to centrally administer a large number of PCoIP devices.

1. Select the **PCoIP Connection Manager** session connection type from the drop down list.
2. Enter the server URI of the PCoIP Connection Manager.

7.2.5 PCoIP Connection Manager + Auto-Logon

This connection type allows you to include the user name, password and domain of the user so that the connection and logon of the zero client is automatic.

1. Select the **PCoIP Connection Manager + Auto-Logon** session connection type from the drop down list.
2. Enter the server URI of the PCoIP Connection Manager.
3. Enter the user's Username, Password and Domain.

7.2.6 Connect using VMware View

You can configure zero clients to use PCoIP to connect to a virtual desktop in a VMware View environment.

If you want users to log on manually:

1. Set the session connection type to **View Connection Server**.

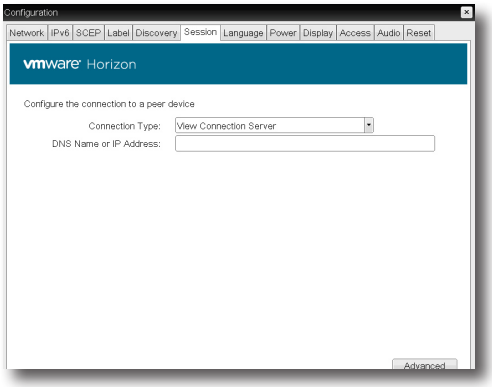


Figure 27: *View Connection Server selection*

2. Enter the IP address (or DNS name) of the VMware View Connection Server.

7.2.7 Connect with View Connection Server and Auto-Logon

1. Set the session connection type to **View Connection Server + Auto-Logon**.
2. Enter the IP address (or DNS name) of the VMware View Connection Server.
3. Enter the user's logon credentials.

Other virtual desktop connection types are also supported, such as kiosk implementations. For details, see the *Teradici PCoIP® Zero Client and Host Administrator Guide*.

7.2.8 Connect using a connection broker

A connection broker is a resource management application. The broker dynamically assigns zero clients to host PCs from the identity of the user connecting from the zero client.

1. Set the session connection type on both the zero client and PCoIP host to **Connection Management Interface**.

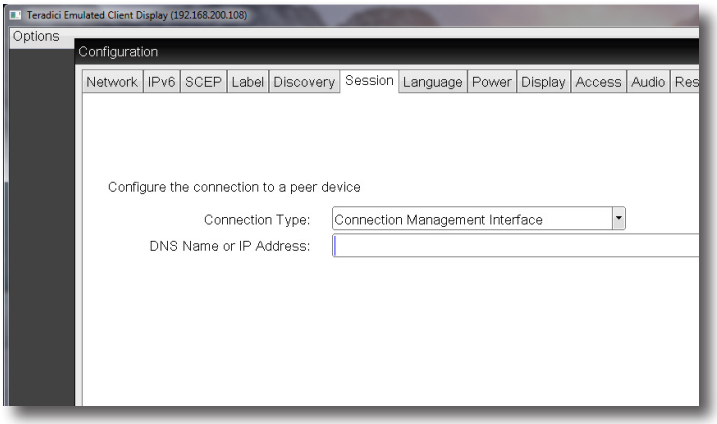


Figure 28: *Connection Management Interface selection*

2. Enter the IP address (or DNS name) for the third party connection broker.

3. Click **OK**.

See section 8.6 for more information about third party connection brokers.

7.3 Set an automatic connection

You can set up zero clients to automatically connect to a remote PCoIP host or virtual desktop when the end-user logs on. With this setup, there is minimal impact on the end-user.

Once set up, at the end of the day the user:

1. Logs out of Windows.

2. Powers off their monitors.

3. Presses the power switch on the zero client to put it in standby.

In the morning, the user:

1. Presses the power switch on the zero client to bring it out of standby.

2. Turns on their monitors.

   There is a pause while the zero client acquires the host IP address. The PCoIP On Screen Display (OSD) briefly shows a connection progress screen on the monitor attached to video output 1. See Figure 29.

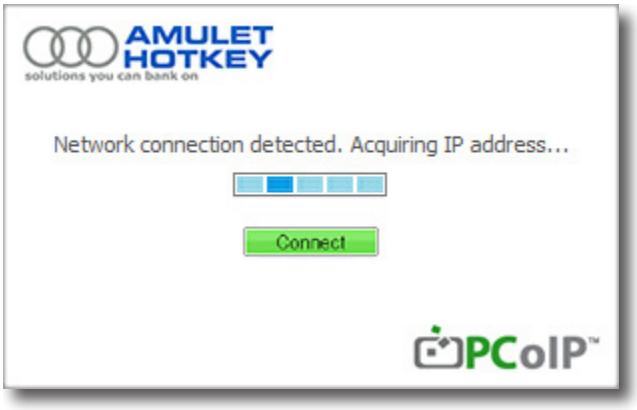


Figure 29: *OSD Automatic connection screen*

3. After a few seconds, the user logs on via the Windows login screen.

7.4 Disconnect from a host PC or virtual desktop

1. Press the front panel Menu button.

2. Choose **Disconnect** from the Zero Client Control Panel that appears on screen. See Figure 30.

Figure 30: *Disconnect option on the OSD*

7.5 Further information

For further information about zero client security, see the *Teradici PCoIP Zero Client and Host Admin Guide*, particularly the 'PCoIP Zero Client Security Overview' and 'Security settings Checklist' sections. This manual is available on the Doc Center page of the Teradici Support site at techsupport.teradici.com.

Network management

8

8. Manage the network

8.1 Find the DXH4 MAC address

A MAC address is a unique network identifier. The address can be found on a label on the card. See Figure 31.

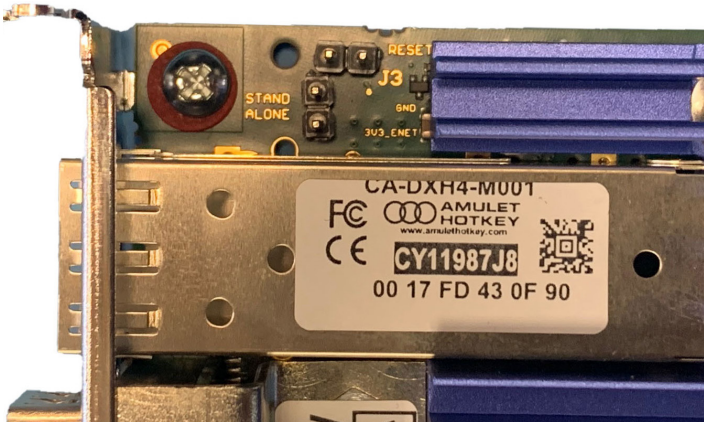


Figure 31: *Location of the MAC address on the card*

8.2 Discover the IP address

It may be necessary to know the IP address of the DXH4, for example to update the Teradici or Amulet Hotkey firmware.

> **Note:** The default IP address of the DXH4 is 192.168.1.100. However this is normally changed during setup.

To discover the IP address you will need to know the MAC address, these are on the product label, see 8.1.

Once you have the MAC address, use one of the following methods to discover the IP address:

- Use the DHCP server to identify the IP address;
- Use DOS command window to identify the IP addresses;
- Use a TFTP window to identify the IP address.

8.2.1 Use the DHCP server to identify the IP address

If you have access to the DHCP server, you can relate the MAC address on the product label.

8.2.2 Use DOS command window to identify the IP addresses

1. Type 'COM' into the Windows search bar to find the Command Window application.
2. Start the Command Window application.
3. Enter the following command:

```
arp -a
```

A list of IP and MAC addresses appears for the local network.

4. Find the MAC address written on the unit in the list and identify the IP address from the IP address listed next to it.

8.2.3 Use a TFTP window to identify the IP address

1. Open the TFTP 64 app on the host machine.
2. Select the **DHCP Server** tab.
3. Click on **Settings**.
4. Make sure there are values in the following fields, that are appropriate for your network:
   - IP Pool Start Address;
   - Size of Pool;

   Consult your IT department or contact Technical Support if you need assistance with this).
5. Select **OK**.
6. Refresh the DHCP server list. To do this:
   a). Select the **TFTP Client** tab;
   b). Select the **DHCP Server** tab.
7. Look for the IP address in the list that associates with the MAC address.

8.3 How to change the IP address

See STEP 8: Change the default IP address for how to change the static IP address to something else.

8.4 Consider network bandwidth requirements

PCoIP uses the Internet Protocol (IP) to transmit data between the host and client. The data can be routed over any IP-compatible infrastructure between offices or across continents. In every case, performance depends on the available bandwidth and signal latency.

8.4.1 Factors affecting bandwidth

The bandwidth required depends on several factors, including:

- the number of pixels changing from frame to frame;
- the number and resolution of screens to be encoded;
- settings made by the user.

Exact bandwidth requirements for PCoIP are difficult to predict, use the values in Table 5 as a guide only:

Setting	Bandwidth
Idle display	~ 0
No USB or audio data	~32Kbit/s per pair of monitors.
General office use (that is, writing documents)	300-500Kbit/s.
Audio	2 Mbit/s.
A significant display change (such as minimising or restoring a window)	4-5Mbit/s
USB transfers	< 6Mbit/s of traffic
Playing full-screen video	< 70Mbit/s

Table 5: *PCoIP bandwidth requirements*

Example1: A dual head configuration running a word processor, spreadsheets, and 2D illustrations/designs will typically use between 1 and 10 Mbit/s.

Example2: A quad video head system running real time full screen video might peak at 70 Mbit/s.

8.4.2 What happens when available bandwidth is exceeded

In all cases, PCoIP builds to a lossless image. If the required bandwidth is not available, PCoIP dynamically adjusts the quality to match. You can also use the zero client management tools (see 6.5 PCoIP management tools) to optimise performance for most conditions.

If bandwidth usage is a concern, we recommend testing and monitoring on your network. For assistance, please contact Amulet Hotkey Technical Support.

8.5 Dual redundant network connections

Important! In an octal configuration, both DXH4s can be linked via an additional cable so that traffic can be routed through either DXH4. The network ports are connected to an internal, unmanaged network switch. The DXH4 does not monitor its network links and relies on the LAN spanning tree to prevent switching loops and to provide redundancy.

If both network ports are connected when a connection between the zero client and PCoIP host is interrupted, the recovery process is as follows:

8. The Spanning Tree network protocol brings up the redundant path between the disconnected zero client and host.

9. The zero client attempts to resume the session. By default, it retries for up to 30 seconds. If the remote PCoIP host is reachable within this time, the session resumes seamlessly.

10. If the zero client cannot reach the host within the retry period, it displays the Connect screen of the On Screen Display. See 6.5.3 On Screen Display (OSD).

11. When the user re-authenticates themselves, they are reconnected to the previous session as it was at the time of the failure.

Note: If you use a connection broker to pair zero clients to PCoIP hosts (see 8.6), you can configure the session so that the Windows desktop is locked while disconnected.

8.6 Choose a connection broker if required

All Amulet Hotkey zero clients can be configured to use a third party connection broker (also known as a connection management server). For example, the following connection broker products include PCoIP support:

- VMware View Connection Server;
- Leostream Connection Broker.

8.6.1 Role of the connection broker

Connection brokers simplify the administration effort for managing large complex PCoIP systems.

A connection broker interacts with systems such as Active Directory to dynamically assign PCoIP hosts to zero clients based on the identity of the user establishing a connection from the zero client.

Connection brokers are also used to allocate a pool of hosts to a group of zero clients.

8.6.2 Specify the connection broker

You can use any of the available management tools (see section 6.5 PCoIP management tools) to specify the connection broker:

- you must provide the IP address or DNS name of the connection broker;
- you must also specify the **Connection Management Interface** connection type for the PCoIP session.

8.6.3 Using the connection broker

Instructions for using a connection broker to connect your zero clients to hosts are available in the *Teradici PCoIP® Zero Client and Host Administrator Guide* (available to download from techsupport.teradici.com).

Note: For further information about using connection brokers, contact Amulet Hotkey Technical Support. See also the Knowledge Base Article *Can I use a connection broker with PCoIP technology? (15134-24)* on the Teradici website.

FIRMWARE UPDATES

9

9. Firmware updates

9.1 Manage the DXH4 firmware

The DXH4 contains two different types of firmware:

- Teradici firmware;
- Board Support Microcontroller (BSM) firmware.

Use the following interface to update the firmware for the DXH4:

- Teradici Administrative Web Interface (AWI)

9.1.1 Teradici Administrative Web Interface (AWI)

Use the AWI to manage firmware updates for the system:

- See 9.2 to connect to the DXH4 with the AWI;
- See 9.3.2 to check the Teradici firmware;
- See 9.4.1 to download Teradici firmware to the DXH4;
- See 9.5 to check the BSM firmware;
- See 9.6 and 9.7 to update the BSM firmware.

9.2 To login with the AWI

1. Enter the IP address of the host in the browser window.

   Note: You can get this from the DHCP server if you know the MAC address of the host, or if the IP address has not been changed, use the default value in 1.6.

   The login screen appears.

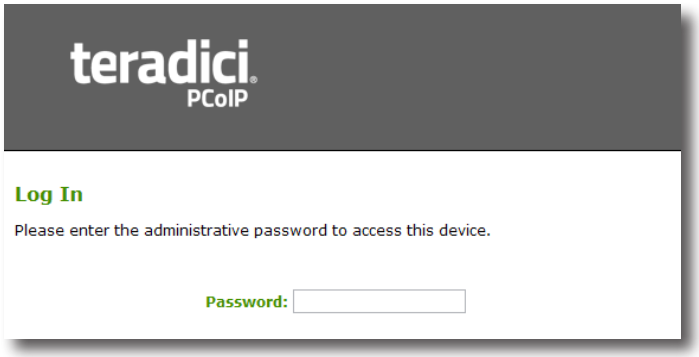


Figure 32: *Administrative Web Interface*

2. Enter the password and click **Log In**.

   The Teradici home screen appears.

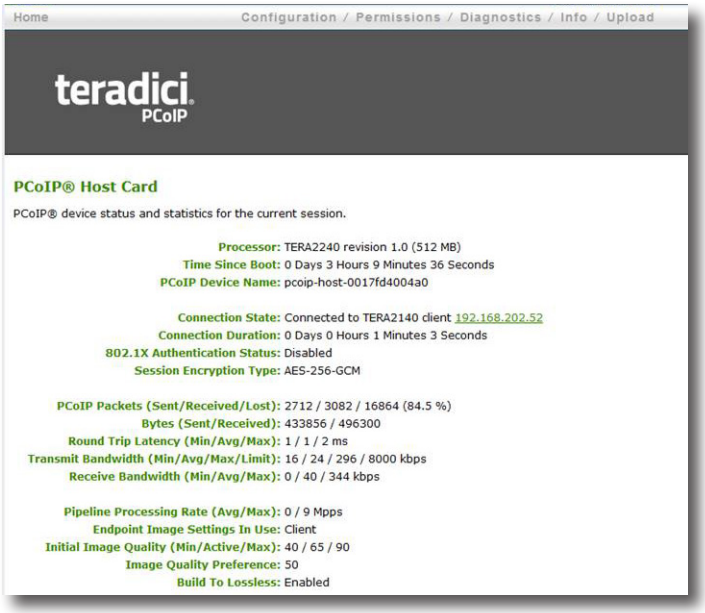


Figure 33: *AWI home screen*

! Caution: *On the home screen for the AWI, do not uncheck the box 'Teradici Host Driver function'. This box must be checked for the correct operation of the unit.*

9.3 Check the Teradici firmware

The DXH4 operates with embedded code known as firmware. There are several components within the unit that each require different firmware. Some of the firmware is provided by Teradici and other firmware components by Amulet Hotkey.

9.3.1 Keep firmware up to date

After you install the DXH4, check our website or with Technical Support for firmware updates and make sure you have the latest versions for each. To check the current versions of firmware, you must use the appropriate interface:

- Use the Teradici AWI for checking and updating Teradici firmware. See 9.3.2 and 9.4.1;

9.3.2 Check the Teradici firmware

1. Login in to the AWI. See 9.2 for how to do this.
2. Select **Version** from the **Info** menu.

   The firmware version is displayed.

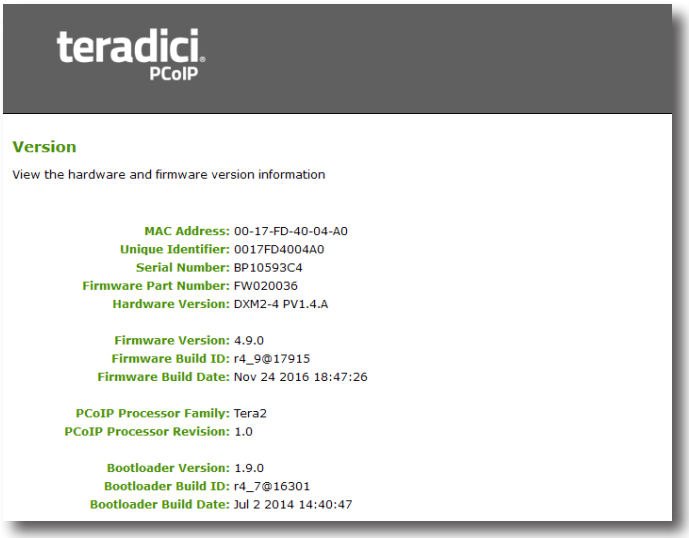


Figure 34: *AWI hardware and firmware version information*

9.4 Update the Teradici firmware

The firmware is constantly being improved and periodically updated.

9.4.1 Update the Teradici firmware

! Caution: *Check with technical support before you upgrade the firmware in your system.*

1. Login with the AWI. See 9.2 for how to do this.
2. Select **Firmware** from the **Upload** menu.

   The Firmware Upload window appears.

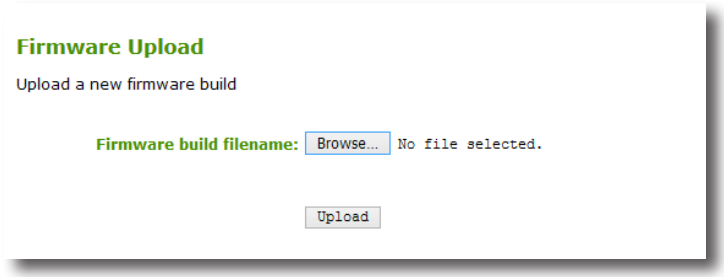


Figure 35: *Firmware Upload window*

3. Click **Browse** and navigate to the host firmware file.

   Note: This must be a *.all file.

   Example: tera2_4-9-0.all

4. Click **Upload** and select **OK** at the prompt.

   After the firmware has downloaded successfully, a prompt appears.

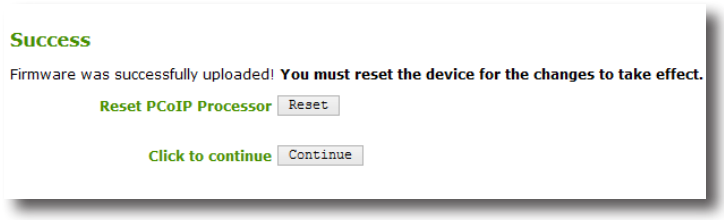


Figure 36: *Successful upload window*

5. Click **Reset**.

   Another prompt appears.

6. Click **OK** to continue.
7. Reboot the Host PC for the firmware update to complete.

9.5 Check the BSM firmware is up to date

PCoIP devices operate on embedded code known as firmware. The DXH4 has a Board Support Micro-controller (BSM) chip that can be upgraded periodically with new firmware. After you install the host card, check our website for firmware updates and make sure you have the latest version.

Important! Check with technical support before you upgrade the firmware for host cards in your system.

To check the current version of firmware of any PCoIP device, use the Administrative Web Interface (AWI) management tools built into the PCoIP hosts and zero clients. See 6.5 PCoIP management tools for details.

9.5.1 Check the BSM firmware on an individual host card

Important! Only available from Teradici host firmware version 4.9.0 onwards. For firmware before this, see 9.7.2.

1. Browse to the IP address of the host card and log on to the Administrative Web Interface (AWI).
2. Select **Network** from the **Configuration** tab.
3. Find the current version of the BSM firmware. This displays next to **BSM Firmware Version**:
4. If the firmware needs updating, see either 9.6 or 9.7.

9.6 How to update the BSM firmware for Teradici host firmware 4.9.0 and later

To update the BSM firmware (for versions 1.4.0 and later), do the steps that follow:

1. Get the BSM firmware update file;
2. Activate the BSM network remotely
3. Transfer the firmware package to the target BSM;
4. Confirm that the firmware has updated;
5. Deactivate the BSM network interface.

9.6.1 Get the BSM firmware update file

1. Download the BSM firmware update file for the DXH4 from Amulet Hotkey. The file name is in this format:

FW-<Part number>_N_N_N-GA.bsm

FW-<Part number>: is the internal Amulet Hotkey part number
N_N_N: is the firmware version number.

Example: The update file for the 1.4.1 firmware on a DXH4 is:

FW-DXH4-0010_1_4_1-GA.bsm

2. Verify the file. The Amulet Hotkey website lists the SHA-256 hash values for the firmware file. After downloading the file, use your preferred checksum tool to re-generate and verify the hash values and confirm there were no errors during the download.

9.6.2 Activate the BSM network remotely

In order to acquire an IP address, you temporarily activate the BSM network interface for the duration of the update process.

1. Verify that the DXH4 is powered On.
2. Log on to the Administrative Web Interface (AWI) for the DXH4

(The AWI uses the same IP address as the PCoIP session.)

Important! It does not matter whether the DXH4 is in a session or not. However, the DXH4 must not be in standby.

3. From the home page, choose **Configuration > Network**.
4. Select the **BSM network enable** check box. See Figure 37.
5. Click **Apply**. The BSM now acquires an IP address from the DHCP server.
6. Make a note of the BSM IP address from the network page. You may need to refresh the browser. See Figure 37.

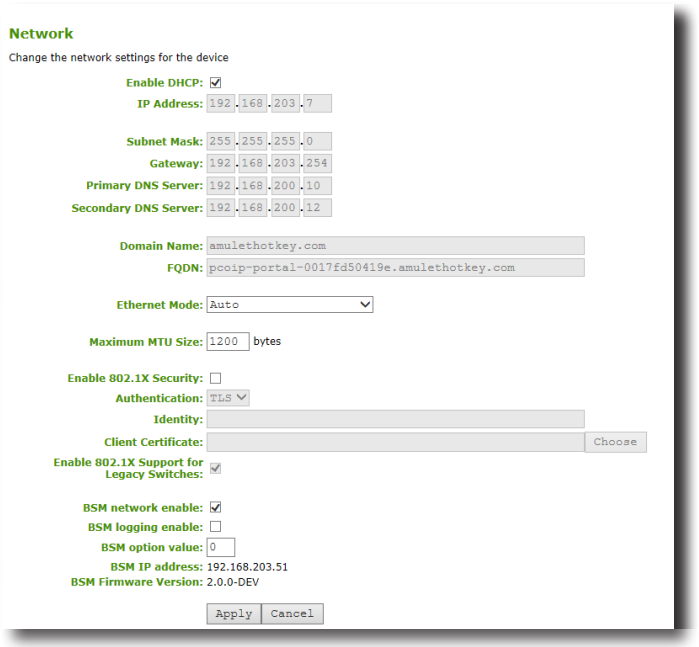


Figure 37: *BSM network details*

9.6.3 Activate the BSM network locally (optional)

Alternatively, you may want to activate the BSM network locally:

1. Verify that the DXH4 is powered On.

2. Press the recessed button on the card for more than **five** seconds. See 2.4.2.

3. Find the IP address assigned to the BSM by checking your DHCP server or by using a tool like FING (www.fing.com). See section 9.7.3 for how to determine the MAC address.

9.6.4 Upgrading multiple units

If you are upgrading the firmware on multiple units you can automate this process.

> **Example:** You can use a script to discover Amulet Hotkey BSMs on your network, querying the Address Resolution Protocol (ARP) cache for known MAC address patterns. Amulet Hotkey Technical Support can offer guidance on this.

(The ARP cache is a collection of Address Resolution Protocol entries that map IP addresses to MAC addresses.)

9.6.5 Transfer the firmware package to the target BSM

Use a TFTP server to transfer the .bsm file containing the firmware package. As an example, these instructions use the Tftpd64 utility, available from http://tftpd32.jounin.net/

1. Verify that the target DXH4 is on or in standby.

2. Launch the **Tftpd64** utility.

3. When Tftpd64 starts, go to the **Tftp Client** tab.

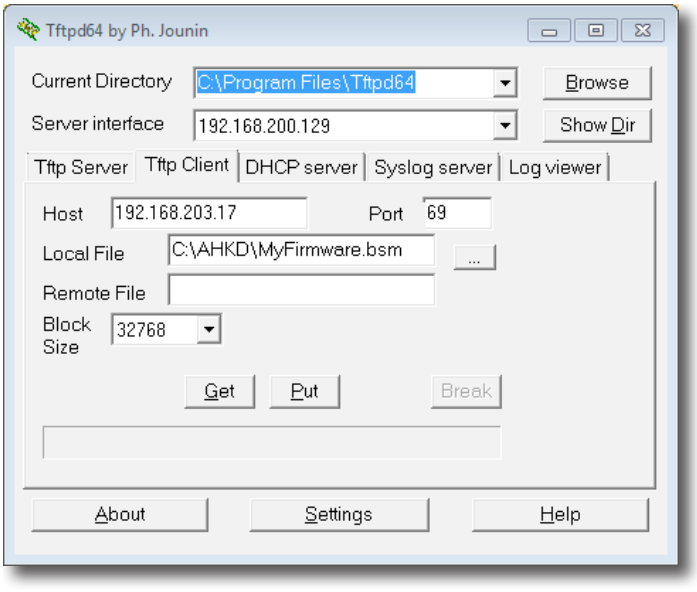


Figure 38: *TFTP utility client settings window*

4. Enter the following settings:

Setting	Value
Host:	Enter the BSM IP address.
Port	Set to port 69. Note that port 69 on the BSM is used to initiate the transfer. The actual port used during the transfer is randomly assigned.
Local File:	Browse to the .bsm file containing the firmware update. You can retrieve this file from anywhere accessible on your network.
Remote File:	Leave this setting blank.
Block Size:	DXH4 uses 512 bytes whatever this is set to.

Table 6: *TFTP utility client settings*

5. Click **Put** to start the package transfer.

6. After the BSM receives and validates the package, the BSM restarts automatically.

9.6.6 Confirm that the firmware has updated

> **Note:** The new firmware is only applied once you restart the host PC.

1. When the DXH4 restarts, log on to the AWI.

2. From the home page, select the **Configuration > Network** page. See Figure 37.

3. Check the firmware version next to **BSM Firmware Version** is the new version.

9.6.7 Deactivate the BSM network interface

Finally, you must deactivate the BSM network interface to free up the IP address acquired and assigned in 9.6.2 step 3.

1. In the AWI, choose **Configuration > Network.**

2. Clear the **BSM network enable** box.

3. Click **Apply** to deactivate the BSM network interface immediately.

The BSM firmware update is now complete.

9.7 Update the BSM firmware for Teradici host firmware older than 4.9.0

To update the BSM firmware when the Teradici firmware is earlier than 4.9.0, do the steps that follow:

1. Get the BSM firmware update file;
2. Find the current version of the BSM firmware (optional);
3. Calculate the MAC address of the BSM;
4. Activate the BSM network interface and acquire an IP address;
5. Transfer the firmware package to the target BSM;
6. Confirm that the firmware was updated;
7. Deactivate the BSM network interface.

9.7.1 Get the BSM firmware update file

1. Download the BSM firmware update file for the DXH4 from Amulet Hotkey. The file name is in this format:

FW-<Part number>_N_N_N-GA.bsm

FW-<Part number>: is the internal Amulet Hotkey part number
N_N_N: is the firmware version number.

Example: The update file for the 1.3.0 firmware on a DXH4 is:

FW-DXH4-0010_1_3_0-GA.bsm

2. Verify the file. The Amulet Hotkey website lists the SHA-256 hash values for the firmware file. After downloading the file, use your preferred checksum tool to re-generate and verify the hash values and confirm there were no errors during the download.

9.7.2 Find the current version of the BSM firmware (optional)

If you want to know the current version of the BSM firmware before performing an update, do the steps that follow:

1. Make sure that the DXH4 is powered on.
2. Log on to the Administrative Web Interface (AWI), see 9.2.
3. Find the current version of the BSM firmware. This is recorded in the zero client's event log:

   a). From the AWI home page, choose **Diagnostics > Event Log**.

   b). Click the **Event Log Messages View** button.

   c). When the log file displays, search for the final occurrence of these log entries:

MCU :(tera_mcu_read_eeprom_content): Reading MCU EEPROM - Pass.

MCU :HWID: 0x85, Major/Minor FW: <0xNN>/<0xNN>, <MAC address>

These log entries start with **MCU**. Within these entries, the BSM version number is represented by the 2nd, 3rd and 4th digits of the **FW: <0xNN>/<0xNN>** string.

Example: In the following log entry the BSM firmware version number is 0.4.8.

MCU :HWID: 0x85, Major/Minor FW: 0x80/0x48, MAC: 00:17:fd:50:00:20

9.7.3 Calculate the MAC address of the BSM

The BSM's MAC address derives from the MAC address of the Teradici processor on the DXH4. The BSM and Teradici MAC addresses are the same, except for the fourth group of two hexadecimal digits:

Using your preferred administrative tools, identify the MAC address of the Teradici processor.

Note: The Teradici MAC address is also printed on the DXH4. serial number label and displayed on the zero client's Administrative Web Interface (AWI).

Add 60hex to the fourth group of two hexadecimal digits of the Teradici MAC address.

Example:

50hex + 60hex = B0hex

The result forms the corresponding digits in the BSM MAC address. See the following example of MAC address conversions:

Teradici MAC address	Add 60hex	BSM MAC address
00.17.FD.50.12.34	—>	00.17.FD.B0.12.34

Table 7: *MAC address conversions*

Tip: All Amulet Hotkey products have a MAC address starting with 00.17.FD.xx.xx.xx. The fourth octet in the MAC address identifies the product type. In the examples above, '50' identifies the product as a standard DXR-Z4 unit, while '51' identifies a modular DXR-Z4-M unit.

You can now use the BSM's MAC address to look up its IP address.

9.7.4 Activate the BSM network interface and acquire an IP address

You now need to acquire an IP Address for the BSM firmware.

Use this IP address to transfer the firmware package to the BSM. In order to acquire an IP address, we currently use a Teradici power feature to temporarily activate the BSM network interface for the duration of the update process.

Note: You can only activate the BSM network interface locally by pressing the recessed button on the DXH4.

1. Press the recessed button on the front of the DXH4. See Figure 7: Front panel features on page 15.

   Important! It does not matter whether the host card is in a session or not. However, the DXH4 must not be in standby.

2. The BSM now acquires an IP address from the DHCP server.

3. Now determine the BSM IP address.

The simplest method is to use the BSM MAC address to look up the BSM IP address in the DHCP console. See Figure 39.

a). Launch the DHCP console.

b). In the left-hand pane, navigate to the Address Leases item (2) for your DHCP server (1).

c). The right-hand pane displays the leased IP address for devices on this server (4).

d). Now locate the BSM. To do this, find the MAC address of the BSM in the Unique ID column (3).

Tip: To speed up your search, you can filter on the MAC address pattern. All Amulet Hotkey products have MAC addresses starting with 00.17.FD.xx.xx.xx.

e). After locating the BSM, look up its associated IP address in the Client IP Address column.

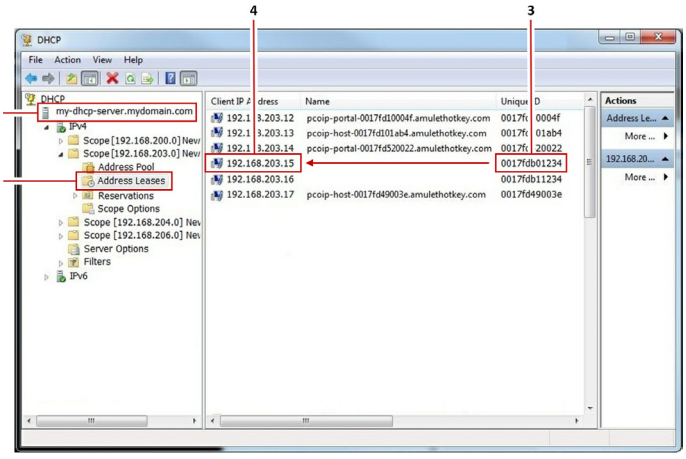


Figure 39: *Finding the IP address using the DHCP console*

Note: The BSM does not have a DNS name and so has no entry in the Name column.

9.7.5 Upgrading multiple units

If you are upgrading the firmware on multiple units you can automate this process.

Example: You can use a script to discover Amulet Hotkey BSMs on your network, querying the Address Resolution Protocol (ARP) cache for known MAC address patterns. Amulet Hotkey Technical Support can offer guidance on this.

(The ARP cache is a collection of Address Resolution Protocol entries that map IP addresses to MAC addresses.)

9.7.6 Transfer the firmware package to the target BSM

Use a TFTP server to transfer the .bsm file containing the firmware package. As an example, these instructions use the Tftpd64 utility, available from http://tftpd32.jounin.net/

1. Verify that the target DXH4 is on or in standby.

2. Launch the **Tftpd64** utility.

3. When Tftpd64 starts, go to the **Tftp Client** tab.

4. Make sure Block Size is set to 32768 (maximum).

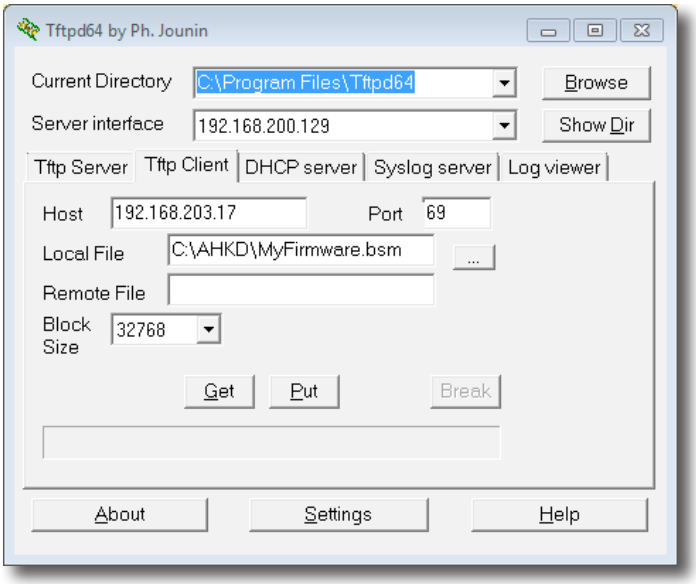


Figure 40: *TFTP utility client settings window*

5. Enter the following settings:

Setting	Value
Host:	Enter the BSM IP address.
Port	Set to port 69. Note that port 69 on the BSM is used to initiate the transfer. The actual port used during the transfer is randomly assigned.
Local File:	Browse to the .bsm file containing the firmware update. You can retrieve this file from anywhere accessible on your network.
Remote File:	Leave this setting blank.
Block Size:	Set to 32768 (maximum).

Table 8: *TFTP utility client settings*

6. Click **Put** to start the package transfer.

7. After the BSM receives and validates the package, the BSM restarts automatically.

9.7.7 Confirm that the firmware was updated

Check the log file to confirm that the firmware update was successfully applied.

1. The DXH4 restarts after a successful upgrade.

   Note: If the DXH4 was On and in a session while the firmware was updated, it restarts after the session has ended. The DXH4 does not apply the new firmware until it restarts.

2. When the DXH4 restarts, log on to the AWI.

3. From the home page, select **Diagnostics > Event Log**.

4. Click **View Event Log Messages**.

5. When the log file displays, search for log entries that start with 'MCU'. Within this log entry, the FW: section (shown in red) indicates the current BSM firmware version:

MCU :HWID: 0x85, Major/Minor FW: <0xNN>/<0xNN>, <MAC address>

Technical Support can advise on the correct firmware version number.

9.7.8 Deactivate the BSM network interface

Finally, you must deactivate the BSM network interface to free up the IP address acquired and assigned in 9.7.4.

1. Verify that the target DXH4 is powered on.

2. Log on to the AWI, and choose **Configuration > Power.**

3. Clear the **Enable Wake-on-USB** box.

4. Click **Apply** to deactivate the BSM network interface immediately.

The BSM firmware update is now complete.

10. Troubleshooting

10.1 How to remove the DXH4

1. Read the cautions and warnings in 3.1 STEP 1: Prepare the PC, Workstation or server and 3.3 STEP 3: Install the DXH4.
2. Turn off the host computer.
3. Unplug the power cable. Wait for at least 60 seconds.
4. Remove any covers to provide access to the PCIe sockets.
5. Wait for the DXH4 to cool down before you remove it from the PCIe socket.
6. Re-assemble the host computer and reconnect the power cable.

10.2 Factory reset using a jumper

Important! Using the reset button on the front of the card also performs a factory reset. Using the button avoids the need to handle the card or remove it. To reset the DXH4 to factory settings using the button, see 2.4.

1. Remove the DXH4. See 10.1.
2. Install a jumper on the contacts. See Figure 41.

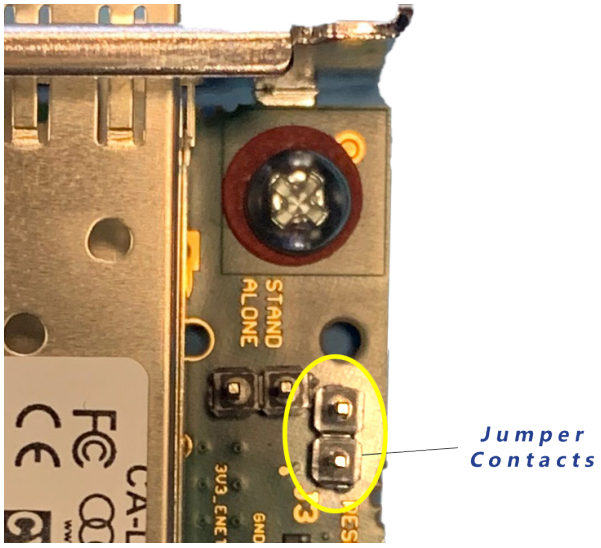


Figure 41: *Position of the jumper contacts*

3. Install the DXH4.
4. Plug in and power up the PC.

   The DXH4 resets to factory settings.
5. Remove the DXH4. See 10.1.
6. Remove the jumper.
7. Install the DXH4.
8. Plug in and power up the PC.

   The DXH4 factory reset is complete.

10.3 Check the function of the Ethernet connection in an octal configuration

1. Connect the PC to mains power.

   Both DXH4s power up.

2. Monitor the DXH4's STATUS and INT FN LEDs.

   On both DXH4s the STATUS LED will flash GREEN to indicate activity.

   On both DXH4s the INT FN LED will be ON and GREEN to show they are connected via the interlink cable.

3. Monitor the DXH4 ACTIVITY and SPEED LEDs.

   For the DXH4 with Ethernet cable connected, the ACTIVITY LED is flashing and the SPEED LED is ON and AMBER (or GREEN).

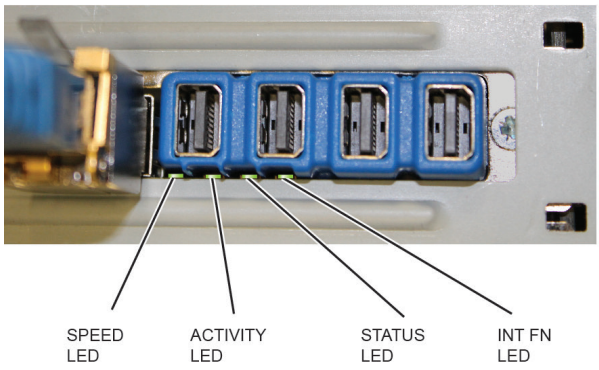


Figure 42: *Status LEDs on the DXH4*

4. Remove the external Ethernet connection and monitor the internal link LED.

   The ACTIVITY and SPEED LEDs are off on both cards.

5. Connect the external Ethernet to the other DXH4 and monitor the LEDs on both DXH4s.

   For the DXH4 with Ethernet cable connected, the ACTIVITY LED is flashing and the SPEED LED is ON and AMBER (or GREEN).

   The ACTIVITY and SPEED LEDs are OFF on the other DXH4.

6. Remove the Ethernet connector, and re-connect to the first DXH4 card.

10.4 Fan maintenance

The DXH4 is fan-cooled. Inspect the card regularly to make sure that the fan is free of dust and can turn freely.

10.4.1 Fan fault LED indication (firmware dependent)

For BSM firmware versions 0.1.2 and above:

If a fault arises and the fan is unable to turn, the Status LED flashes red (see 2.2 I/O bracket status LEDs). Contact Amulet Hotkey Technical for guidance.

SPECIFICATIONS

11

11. Technical specifications

11.4.1 Warranty

Your DXH4 remote workstation card comes with a 3 year warranty.

11.4.2 Technology

Description	Specification
PCoIP Processor	Teradici PCoIP Tera2 (2240 chipset)
Power supply	Internal from PCIe bus – maximum 15W, typically 12W
Bus type	Single lane PCIe x1. Compatible with x1 to x16 slots, PCIe spec 1.0 or above
Video input	4 x Mini DisplayPort (dual mode)
Display support	1920 x 1200 maximum (quad monitors) @ 60 fps 2560 x 1600 maximum (dual monitors) @ 60 fps
Audio connections	Internal from PCIe bus – card provides standard HD Audio controller; HDA codec is on the remote zero client HD Audio can be optionally disabled using the PCoIP Management Console or AWI
USB connections	Internal from PCIe bus – card provides both USB 2.0 OHCI and EHCI USB host controllers (unless powered only by the supplemental power socket)
Flash programmable	In system via Ethernet. After upload, requires a reboot on the host PC to apply update
Network connections Full duplex required	DXH4: Single RJ45: 10/100/1000 BaseT DXH4-M: Single SFP module: fiber or copper, 1 Gbit/s or 100 Mbit/s **Note:** See the SFP Modules Datasheet for a list of available modules
Wake-On-LAN	Via PCIe bus. Switch-able to RPC cable option **Note:** Because of the SFP module power requirements, the DXH4-M does not support Wake-on-LAN on some PCs. Contact Amulet Hotkey Technical Support for details
Remote power control of host PC	Requires RPC cable assembly
Compatible client	Amulet Hotkey DXZ series zero client

Table 9: *Video, technology and network specifications*

11.4.3 Environment

Description	Specification
Cooling	Dynamic fan cooling. Fan operates between 0-100% as required, depending on load and ambient conditions
PCIe form factor	**Card:** PCIe small form factor (low profile, half-length) **Bracket:** Half-height fitted as standard and full-height bracket supplied.
Unit weight	175g (0.4 lbs) - excludes packaging and other kit parts
Regulatory	All models conform to relevant parts of EN55024, EN55032 and FCC 15(b)
Temperature range	Operating: 15° to 55° C (59° to 131° F), refers to PC internal ambient temperature Storage: -10° to 60° C (14° to 140° F)

Table 10: *Environmental specifications*