AMULET HOTKEY

PCoIP ZERO CLIENTS

USER MANUAL

DXZ4 series, DXZC series and ZeroTop®
HB-DXZX-0001
Revision 2.3 March 2022

teradici PCoIP®

Health and Safety Information

CAUTION

To prevent damage to the zero client:

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

LASER SAFETY

The zero client 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.

Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

Warning: Class 1 laser product.

Warning: Invisible laser radiation can emit 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.

This device complies with part 15 of the FCC Rules. This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

Amulet Hotkey zero clients are ready for use with VMware® View® version 4 and above.

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:

ProCare Support Services

Amulet Hotkey ProCare provides customers with access to a global 24x7 service desk, with extensive expertise to resolve your technology questions and issues. Choose the ProCare package to suit your business needs.

All ProCare packages include an advanced replacement warranty and access to third party firmware and software. ProCare is a single point of contact with solution experts, collaborating with third party vendors for a rapid resolution.

Click here to find out more

Compliance Notice

See the Legislation Sheet LS-AHKL-0001 for details of current EU and FCC compliance.

Scope

This manual covers Amulet Hotkey® zero clients that use the Tera2 range of PCoIP® processors.

It describes the principle features of these zero clients, their specifications, operation and connection to desktop peripherals. It also explains how to create a PCoIP session between a zero client and remote PCoIP host. Images in this manual are current at the time of printing, but minor variations may occur over time.

For a full and detailed understanding of the PCoIP protocol, options for connection, security and management, see the *PCoIP Zero Client and Host Administrator Guide*. The guide is available from the Amulet Hotkey website, or directly from the Teradici website.

Contents

List of figures

List of tables

Before you start

1

1. Before you start

Familiarize yourself with the information in this chapter.

1.1 Types of zero client

This manual covers the Amulet Hotkey zero client products:

DXZ4, DXZ4-M, DXZ4-A, DXZ4-AM, DXZC, DXZC-A, DXZC-AM, DXZC-C, DXZC-M, DXZC-MC, DXZC-AC, DXZC-AMC, DXZC-E, DXZC-EC, DXZC-EM, DXZC-EMC, DXZC-5030, DXZ4-7030, ZT100 and ZT101.

Your model may have a selection of the following features:

- two or four heads of video;
- single or dual network port;
- RJ45 or SFP network connections;
- security features and certification;
- integral card reader.

1.1.1 DXZ4 series - four video heads

The DXZ4 series supports four heads of video with dual network connections. Also, two DXZ4 zero clients can be connected to give eight heads of video.

1.1.2 DXZC series and ZeroTop - two video heads

The DXZC series supports two heads of video with a single network connection.

1.1.3 ZeroTop® 15 (ZT100 and ZT101) - two video heads

The ZeroTop is a variant of the DXZC or DXZC-C in a ruggedised laptop case. Follow DXZC instructions except where noted.

1.1.4 DXZC-E series - extended USB connectivity

The 'E' series zero clients have an extended number of USB ports compared to the standard DXZC zero client. The DXZC-E and DXZC-EM have 8 USB ports in total, two of which may be used for charging high charge-current devices. See 6.2 Extended USB connectivity (DXZC-E series only) for more information.

Note: The DXZC-EC and DXZC-EMC have one less USB port as one port is used to support the internal card reader.

1.2 Terminology

There is a label on the bottom of the unit that identifies the zero client. To identify the particular model, use the following key:

- 'A' - NCSC-certified security;
- 'M' - SFP network ports for fiber or copper modules;
- 'C' - integral card reader;
- 'E' - Extended number of USB ports.

Example: A DXZ4-AM is a security-edition model that supports four heads of video, and has two SFP network ports.

Example 2: A DXZC-EC supports two heads of video, an RJ45 network port, additional USB ports and a card reader.

Note: This manual refers to all models as 'zero client' unless highlighting a specific feature or model.

1.3 Power supply

Amulet Hotkey zero clients come with a mains to DC power supply that self-senses the incoming voltage (110-240V AC). With the exception of the ZeroTop, this power supply has a locking DC connector. To release the connector, pull the locking sleeve away from the rear of the zero client.

Important! Use only this power supply with the product.

1.4 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 security edition zero clients (models described with 'AM') only support certain models of SFP module. If in doubt, contact Technical Support for advice.

1.5 IP and MAC addresses

Before you set up a zero client, 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. You can also use the AWI (see 1.7.2) 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

1.6 Cooling considerations

Amulet Hotkey zero clients are designed to operate efficiently, over a long period in a variety of applications. For reliable operation they must be correctly installed and ventilated.

Note: DXZ4 series and DXZC series zero clients are passively cooled. Certain components inside the zero client use the metal case as a heat sink, so the unit often feels warm or possibly hot to the touch. This is normal.

Always allow sufficient space around the zero client enclosure for cool air to enter the device and for hot air to escape:

- do not block the air vents;
- do not install in a fully sealed enclosure.

1.6.1 Recommended enclosure size

Where applicable, to ensure adequate cooling, the enclosure must allow the following minimum gaps around the unit:

- X=25mm, Y=25mm, Z=25mm.

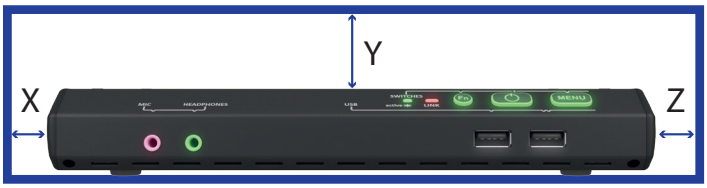


Figure 1: *Minimum gap around the zero client*

Note: Assuming room temperature is 25°C and the enclosure is fully open front and back for cable and switch access.

1.6.2 Use a spacer to stack units

If you need to stack zero clients on top of each other, we recommend that you separate the stacked units with spacers where S=25mm.

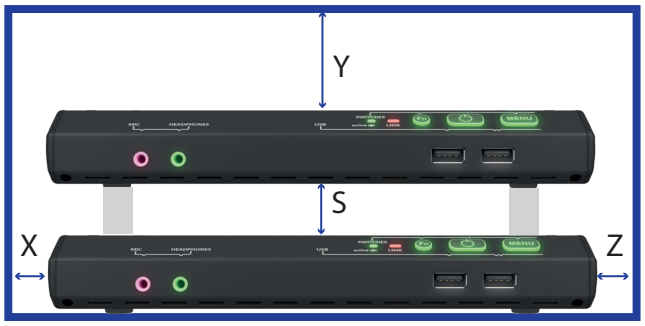


Figure 2: *Use of spacers with two zero-client*

Important! Do not stack units without using spacers. Without these spacers, airflow is restricted and can cause higher than usual temperatures in some units.

Figure 3: *Do not put zero clients together without spacers*

1.7 Zero client management tools

You can interact with PCoIP zero clients through various management tools. See Table 1.

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 1: *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).

1.7.1 PCoIP Management Console

The PCoIP Management Console (see Figure 4) 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 information of all PCoIP devices. You can manage devices individually or by group.

Example: You can create device groups based on location or department.

You can assign configuration profiles to PCoIP devices and update firmware. You can also view log files and reset devices.

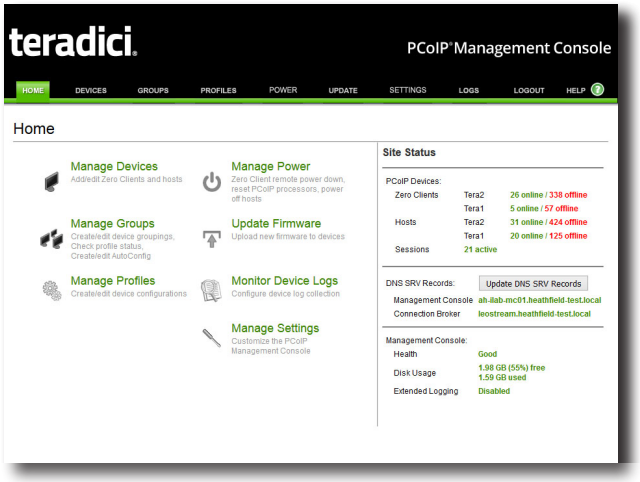


Figure 4: *PCoIP Management Console home page*

Note: For more information on the PCoIP Management Console, contact Amulet Hotkey Technical Support.

1.7.2 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 1.5).

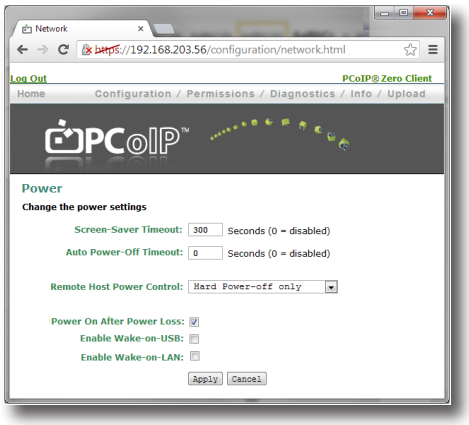


Figure 5: *Administrative Web Interface*

1.7.3 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.

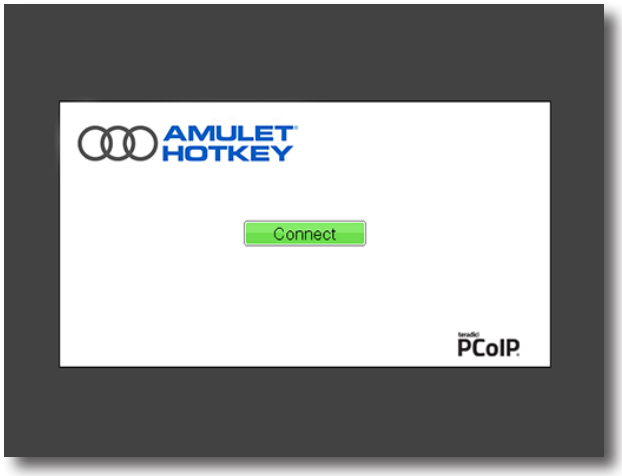


Figure 6: *OSD Connect screen*

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 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 4.6.

1.8 Under the desk bracket (optional)

Note: Not for use with ZeroTop zero clients.

An optional under the desk bracket is available to hold a zero client, if you want to keep the zero client out of the way below the desk.

Cable management is provided with the bracket and details on how to attach it to the desk are available on the Quick Start Guide and fixing template provided with the bracket.

See Figure 7 and Figure 8.

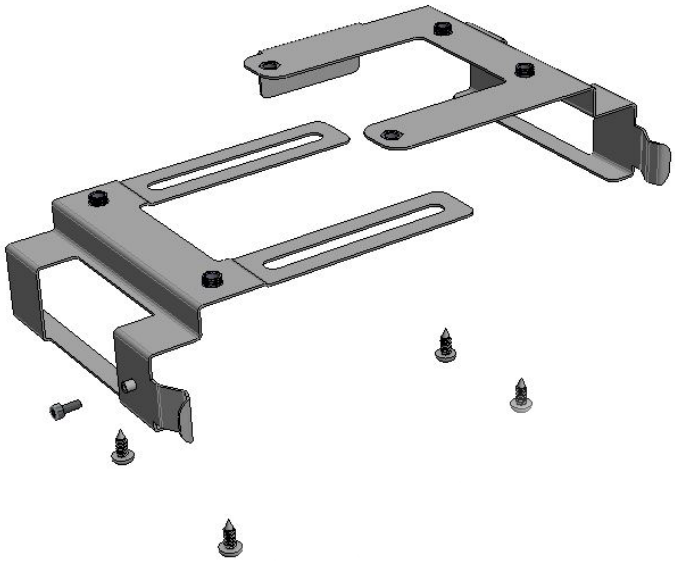


Figure 7: *Optional under the desk bracket for zero clients*

Figure 8: *Zero client fitted to under the desk bracket*

Your DXZC series zero client

2

2. Your DXZC series zero client

DXZC series zero clients have various ports and LEDs on the front and rear panels. Note that the ZeroTop portable zero client is also covered in this section.

2.1 Front panel features

See Figure 9 for the following description:

1. **Mic socket**: Microphone input on 3.5mm jack.
2. **Headset socket**: Stereo headset (combined headphones and microphone) input/output on 3.5mm jack.

   When a microphone is plugged into the Mic socket, the Headset socket switches to audio output only.
3. **Easy access USB ports**: Use these ports to connect a keyboard, mouse or other USB devices you need access to.
4. **Device LED**: Shows the device and network status. See 7.4.2 for details.
5. **PCoIP LED**: Shows the PCoIP status. See 7.4.2 for details.
6. **POWER / MENU switch**: Turns the unit on and off and also used for connecting the zero client to the host. See 2.3 for details.
7. **Smart card reader**: Supports CAC, PIV cards and SIPRNet tokens. See 2.4 for details.

DXZC series

DXZC-C series

Figure 9: *Front panel features for all DXZC series and DXZC-E series zero clients*

2.2 Rear panel features

See Figure 10 for the following description:

1. **Network port (RJ45 or SFP)**: The DXZC series zero clients have an RJ45 socket or a socket for SFP modules.
2. **Network LEDs**: The network port has an upper and lower network status LED: See 7.5 Rear panel status LEDs.
3. **Video output 1 and 2**: DisplayPort connectors.

   By default, the On Screen Display (OSD) displays on the monitor connected to video output 1.

   You can specify video output 2 as the OSD default by changing the configuration in the Display Topology screen.
4. **Rear panel USB ports**: Use these ports to connect any USB devices, including keyboard and mouse. Two of the ports on the DXZC-E series can also charge high-charge current devices (up to 1.5A).
5. **Audio socket**: Stereo line out or speaker output on 3.5mm jack.
6. **Locking DC inlet**: You must only use the approved PSU.
7. **Network port (SFP module)**: Models with the suffix 'M' have a socket that accepts an SFP module. See the SFP Datasheet for the modules available from Amulet Hotkey.

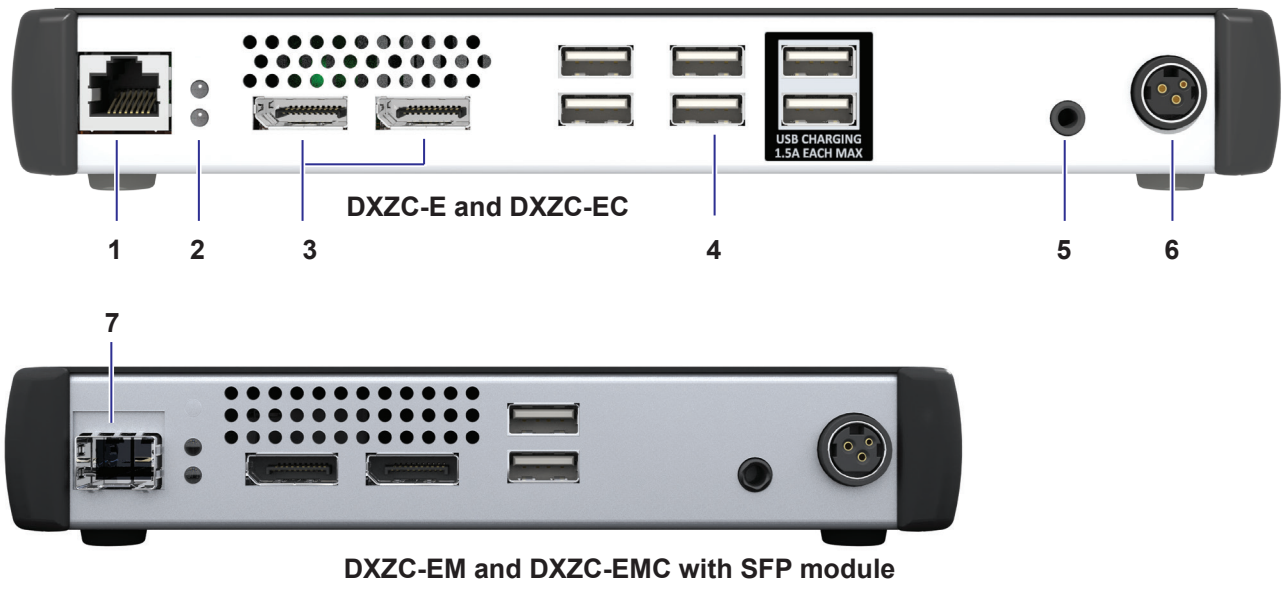


Figure 10: *Rear panel features for DXZC series and DXZC-E series zero clients*

2.3 Operation of the POWER / MENU button

When the unit is off:

- a short button press turns on the unit.

When the unit is on:

- a long button press turns off the unit;
- a short press of the Menu button causes the OSD to display the following options on one of its four monitor outputs (see Figure 11):

1. Disconnect;
2. Power Off Workstation;
3. Cancel.

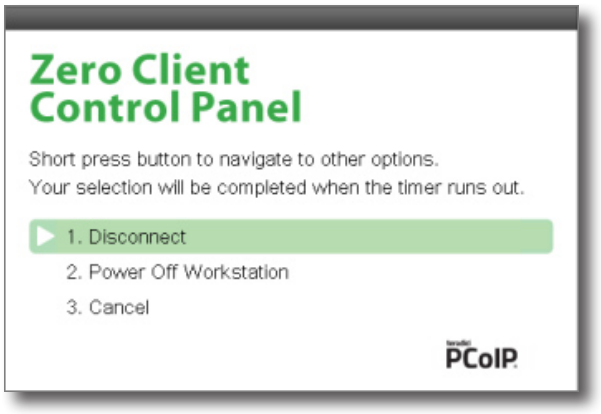


Figure 11: *OSD Zero Client Control Panel*

Note: When the host is a blade, the blade will power-cycle, not power-off. Other configurations may require additional setup.

2.3.1 Operation with a software PCoIP host

There is a different function for the Power/Menu button when connecting to a software PCoIP host (also called a PCoIP Software Agent) such as:

- VMware Horizon (and Horizon Air Cloud);
- Amazon Workspaces;
- Teradici PCoIP Workstation Access Software;
- Teradici Cloud Access Software (formerly called Pervasive Computing Platform).

Note: This list may change as Teradici signs up partners using the PCoIP software.

When connected in a session with these solutions a short press of the Power/Menu button will immediately disconnect the session (no message is displayed).

2.4 Smart card reader

The DXZC-C, DXZC-AC, DXZC-AMC, DXZC-EC and DXZC-EMC feature an integral smart card reader that supports 5V, 3V and 1.8V smart cards, including support for Common Access Card (CAC) smart cards and SIPRNet hardware tokens.

> Important! Always insert smart cards into the smart card reader with the chip facing down and forward-most.

See 9.2 Restrict access to the management tools for how to use the smart card with your zero client.

Depending on your requirements, you can configure the integral smart card reader for pre-session or in-session authentication.

2.4.1 Pre-session authentication

The smart card authenticates the user before a PCoIP session is established. This allows you to log on directly to your virtual desktop. After you enter your smart card PIN, you do not need to connect to your remote PCoIP host or log into your desktop.

The requirements for pre-session authentication are summarized in Teradici Knowledge Base article *Do PCoIP zero clients support pre-session smart card authentication? (15134-299)*.

2.4.2 In-session authentication

The smart card authenticates the user after a PCoIP session has been established. That is, the user first connects to their virtual desktop or remote workstation in the normal way. The smart card is then used to log the user into their desktop OS.

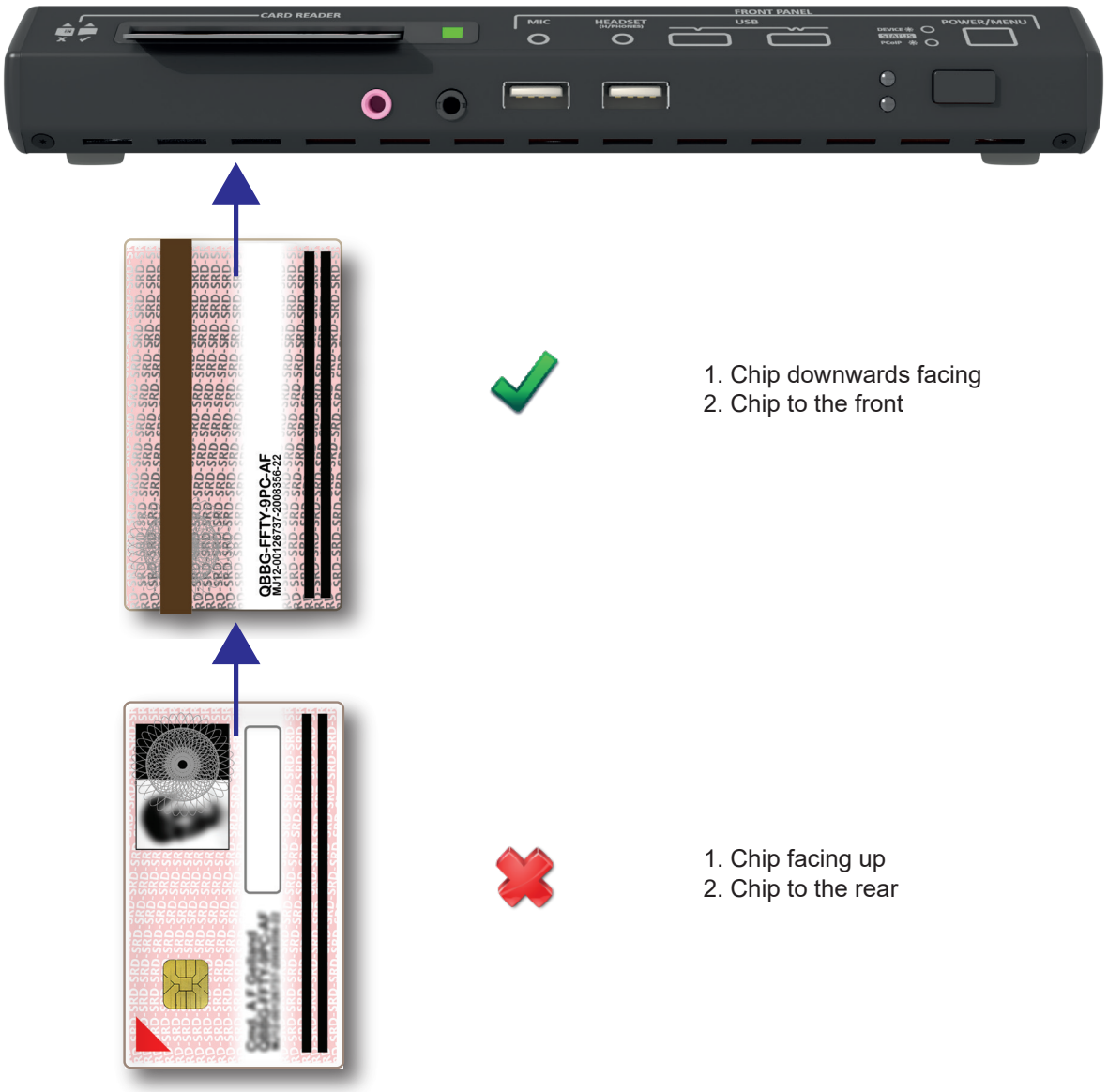


Figure 12: *How to insert a smart card into the reader*

2.5 ZeroTop portable zero client

The ZeroTop® 15 ZT100 (and ZT101) is an NCSC-certified adaptation of the DXZC zero client which features a built in keyboard, display and trackpad. It is a fully portable device with a ruggedised case. The ZT101 has an integral card-reader.

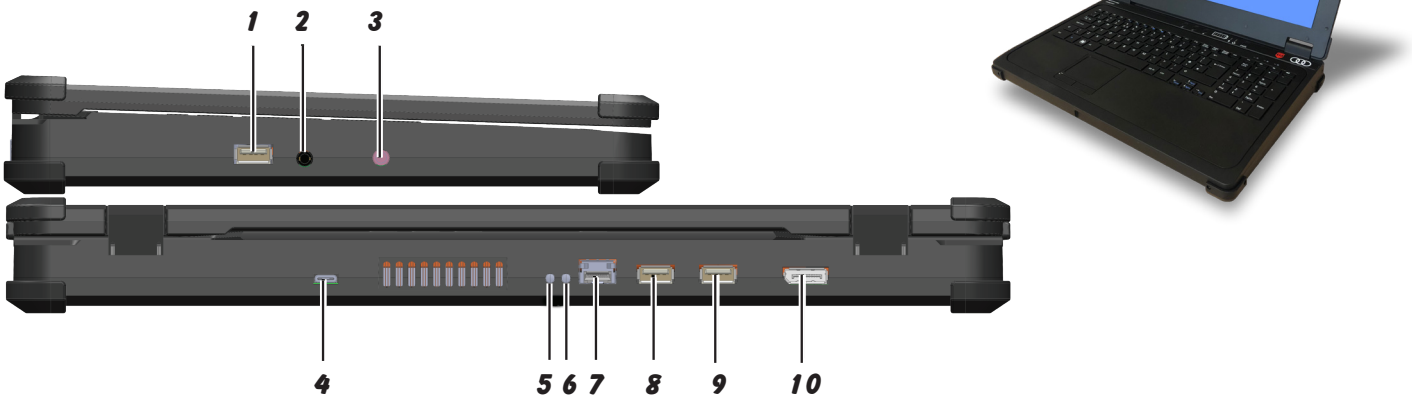


Figure 13: *ZeroTop connections*

2.5.1 ZeroTop connections

See Figure 13 for the following description:

1. **USB**: (USB type A) USB connection.
2. **Headset**: (3.5mm jack) Headset connection.
3. **Microphone**: (3.5mm jack) Microphone connection.
4. **Power**: (USB type C) DC inlet.
5. **Network Status**: LINK LED. See 7.5 for details.
6. **Network Status**: SPEED LED. See 7.5 for details.
7. **Network**: (SFP): network connection for PCoIP seesion.
8. **USB**: (USB type A) USB connection.
9. **USB**: (USB type A) USB connection.
10. **Video**: (Display port): Auxillary video output for optional second monitor.

2.5.2 ZeroTop controls and status LEDs

See Figure 14 for the following description:

11. **Status LED**: Battery charge status.
12. **POWER / MENU switch**: Turns the unit ON and OFF. Also connects the zero client to the host. See 2.3 for operation.
13. **Status LED**: Power status. Same operation as DEVICE LED on the DXZC. See 7.4 for details.
14. **Status LED**: PCoIP session status. Same operation as PCoIP LED on the DXZC. See 7.4 for details.
15. **Switches**: Display brightness controls.

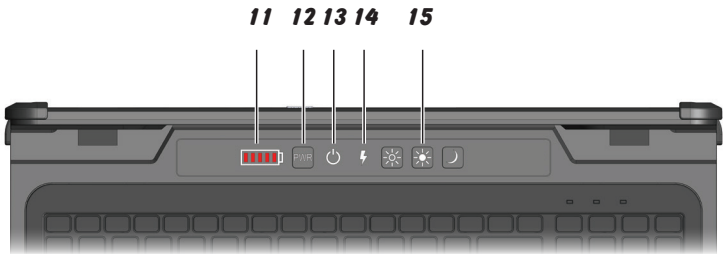


Figure 14: *ZeroTop controls and status LEDs*

2.6 Operation of the Power/Menu switch

Refer to section 2.3 for the operation of the Power button.

Your DXZ4 series zero client

3

3. Your DXZ4 series zero client

DXZ4 series zero clients have various ports and LEDs on the front and rear panels.

3.1 Front panel features

Figure 15 shows the following front panel features:

1. **Mic socket**: Microphone input on 3.5mm jack.
2. **Phones socket**: Stereo headphones output on 3.5mm jack.

   You may use any headset with separate mic and phone jacks.
3. **SWITCHES active LED**: Displays whether front panel switches are active or disabled. See 7.3 and 6.1 for details.
4. **PCoIP (LINK) LED**: Shows the PCoIP network status. See 7.4.1 for details.
5. **Function Switch**: Use in combination with other switches to set other operational modes. See 6.1 for details.
6. **POWER switch**: Turns the unit on and off and also gives indications of the network state. See 7.4.2 for details.
7. **Menu switch**: Displays the On-Screen Display (OSD). First press displays the menu, further presses cycle through available menu options.

   Note: When connected to at least one monitor.
8. **Keyboard USB port**: Use this port to connect to a keyboard or other USB device.
9. **Mouse USB port**: Use this port to connect a mouse or a high speed USB device.

   Important! See 10. Troubleshooting if you get any unexpected behaviour when connecting devices to this port.

Figure 15: *Front panel features*

3.2 Rear panel features

Figure 164 shows the following rear panel features:

1. **Network port (SFP module)**: The 'M' models have two sockets that accept an SFP module. See the SFP Datasheet for the modules available separately from Amulet Hotkey.

   Note: For details about dual redundant network connections, see 6.5.1 Dual redundant network connections on page 35.

2. **Network LEDs**: Each network port has an upper and lower network status LED: See 7.5 Rear panel status LEDs.

3. **Video outputs 1 to 4**: DisplayPort connectors.

   By default, the On Screen Display (OSD) displays on the monitor connected to video output 1.

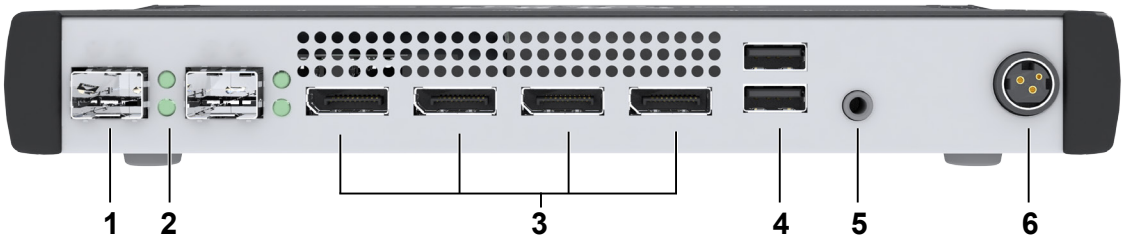
   You can specify a different video output as the OSD default by changing the configuration in the Display Topology screen.

4. **Rear panel USB ports**: Use these two ports to connect any USB devices, including keyboard and mouse.

5. **Audio socket**: Stereo line out or speaker output on a 3.5mm jack.

6. **Locking DC inlet**: Only use the approved PSU supplied.

7. **Network port (RJ45)**: The standard DXZ4 series zero client has two RJ45 sockets. You may use the second network port to connect to other networked devices or to provide redundancy (if the LAN spanning tree is active).



DXZ4-M and DXZ4-AM

DXZ4, DXZ4-7030 and DXZ4-A

Figure 16: *Rear panel features*

3.3 Operation of the POWER button

A short button press turns on the unit.

When the unit is on, a short button press puts the unit into standby.

3.4 Operation of the MENU button

3.4.1 Operation when connected to a host card

When the unit is on and connected to a host card, a short press of the Menu button causes the OSD to display the following options on one of its four monitor outputs (see Figure 17):

1. Disconnect;
2. Power Off Workstation;
3. Cancel.

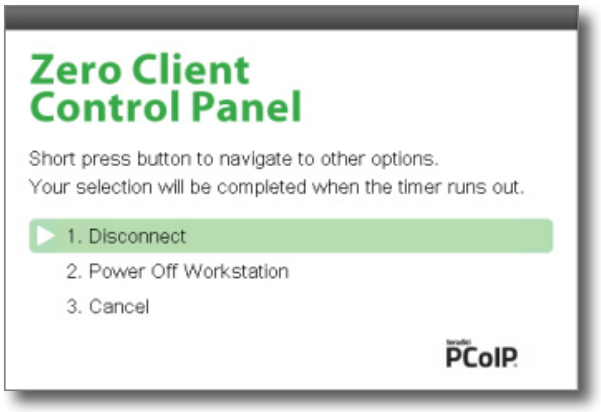


Figure 17: *OSD Zero Client Control Panel*

Note: When the host is a blade, the blade will power-cycle, not power-off. Other configurations may require additional setup.

3.4.2 Operation with a software PCoIP host

There is a different function for the Menu button when connecting to a software PCoIP host (also called a PCoIP Software Agent).

! Caution: *When connected in a session with these solutions a short press of the Menu button will immediately disconnect the session (no message is displayed).*

This applies to the following host solutions:

- VMware Horizon (and Horizon Air Cloud);
- Amazon Workspaces;
- Teradici PCoIP Workstation Access Software;
- Teradici Cloud Access Software (formerly called Pervasive Computing Platform).

Presing the menu button again will allow you to reconnect.

Set up the zero client

4

4. Set up the zero client

This section describes how to set up your zero client.
See 4.7 on page 27 for information on setting up the ZeroTop.

4.1 STEP 1: Connect the keyboard, mouse and optional audio devices

1. Connect a keyboard and mouse to any of the front or rear USB ports. See Figure 18 or Figure 19.
2. Connect audio devices, if used. See Figure 18.

   Use the front panel audio and mic sockets to connect either:

   a). a compatible headset with two jacks, or;

   b). a compatible headset with one jack (DXZC series only) see Figure 19, or;

   c). headphones and a separate microphone.

   You may connect speakers to the rear panel audio output socket. See Figure 20.

   You may also connect USB audio devices to any USB socket on the front or rear panel. See Figure 20.

Figure 19: *Front panel connections for the DXZC series*

Figure 18: *Front panel connections for the DXZ4 series*

4.2 STEP 2: Connect the monitors, network, peripherals and power

1. Connect at least one compatible monitor to the zero client, starting at the Video 1 port. See Figure 20.

   Tip! *You may use any rear panel video port for the monitor. However the default port is Video 1 port. You can change this default in the* ***Display Topology*** *tab of the OSD configuration menu later.*

2. Connect any additional monitors to the other Video ports.

   Note: The DXZ4 series zero client supports up to four monitors. The DXZC series zero client supports up to two monitors.

3. (Optional) Install the SFP modules (for SFP network).

4. Connect the network cables to the network ports (RJ45 or SFP). See Figure 20.

5. Connect the PSU. See Figure 20.

   Important! Use only the PSU supplied with the zero client.

4.3 STEP 3: Power on the unit and monitor

1. Press the POWER switch (see Figure 21). A short button press turns on the unit.

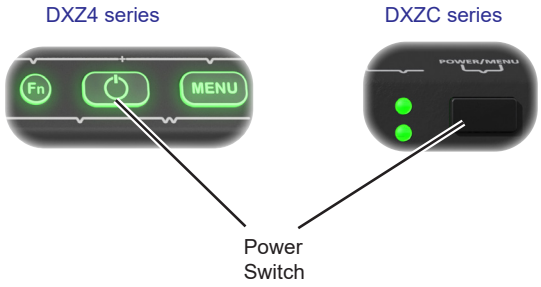


Figure 21: *Power on the unit*

2. Turn on the monitor and make sure the remote workstation is on.

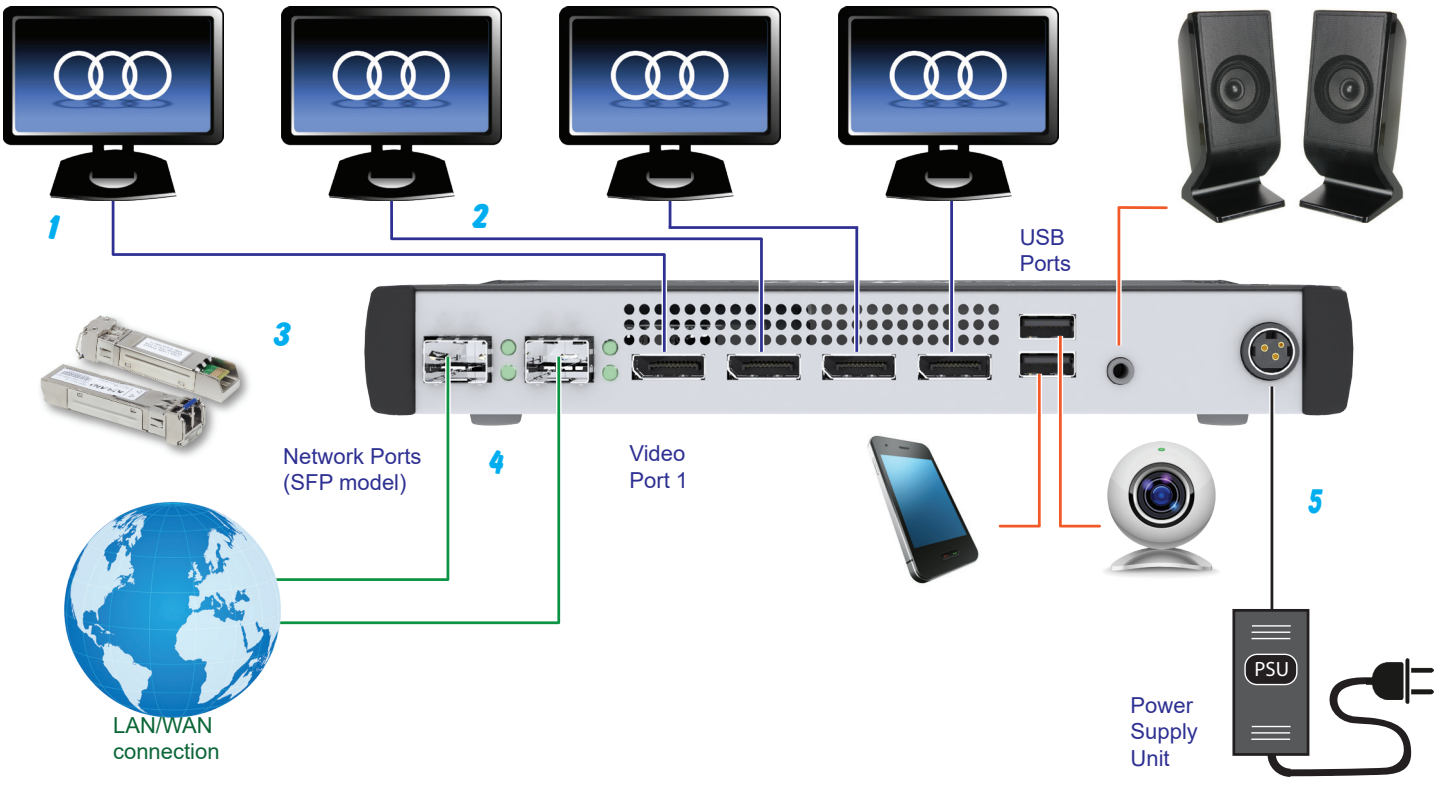


Figure 20: *Connecting up the zero client (DXZ4 series shown)*

4.4 STEP 4: Connect to a PCoIP host

After powering up the zero client, the zero client connects to a remote PCoIP host via the network port.

The zero client supports the following types of PCoIP host:

- Compatible Tera2 PCoIP host in hardware;
- Compatible Tera1 PCoIP host in hardware;
- Compatible PCoIP host in software (VMware® View™ 4 and above).

4.4.1 Connect to a host 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.

> Important! This is just one method you can use to quickly connect your zero client to a host. For a detailed description of all connection methods, see 5. Set up a PCoIP session.

Note: 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.

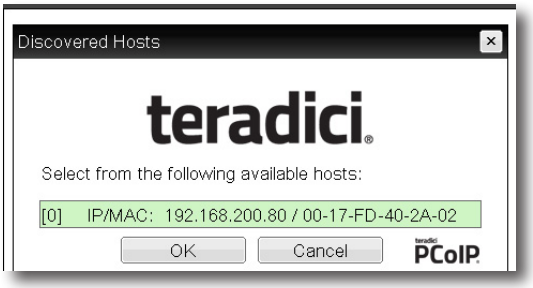


Figure 22: *The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered*

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

   If the zero client successfully connects to the host, the front panel status LED displays green to show 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.

4.5 STEP 5: Connect additional peripherals

Follow the manufacturer's instructions to set up any additional peripherals such as printers, web cams, tablets or similar.

4.6 STEP 6: Change the default password

You must enter a password before changing the configuration of the zero client. The factory set password for all Amulet Hotkey zero clients is **ahkdante**.

At first login, you are prompted for a new password. Make sure you choose a more secure password before using the zero client.

> Important! Although the zero client does not enforce a password policy for administrator logins, we recommend that you implement a robust and secure password policy. Where possible, use a machine-generated password of eight or more characters. We also recommend that you provide your users with guidance about the secure handling of passphrases.

4.7 Setting up the ZeroTop

As a fully intergated, portable zero client, the ZeroTop requires minimal preparation. Refer to Figure 23.

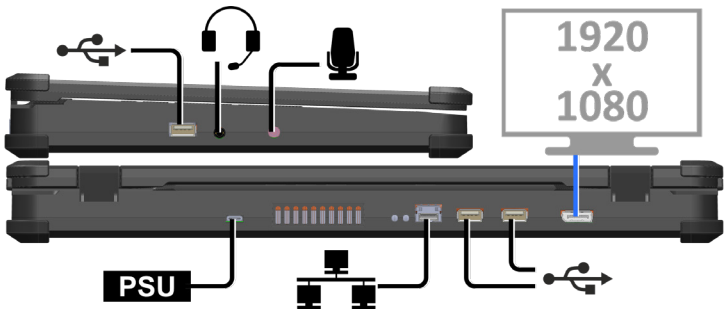


Figure 23: *Connecting up the ZeroTop*

4.7.1 Connecting to a PCoIP Host

After powering up the ZeroTop, follow steps 4.4, 4.5 and 4.6 above. When using the ZeroTop in a secure application, refer to Chapter 9: Security.

4.8 Set up an Octal configuration

An octal configuration is one that uses two DXZ4 series zero clients to provide eight heads of video.

For information on how to do this, see the Remote Desktop Configuration Manual HB-CONF-0001.

Other connection methods

5

5. Set up a PCoIP session

This section describes how to connect a DXZ4 series or DXZC series zero client with 4.x.x firmware to a remote PCoIP host or virtual desktop.

Important! For zero clients with firmware 5.x.x and 6.x.x there are changes in both functionality and setup. Contact Technical Support for assistance with these changes.

5.1 Power up the zero client

After you install the zero client, you establish a PCoIP session between the zero client and a remote 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.

5.2 Set the PCoIP session type

To change the type of PCoIP session that the zero client uses to connect to the host, select the configuration in the OSD.

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

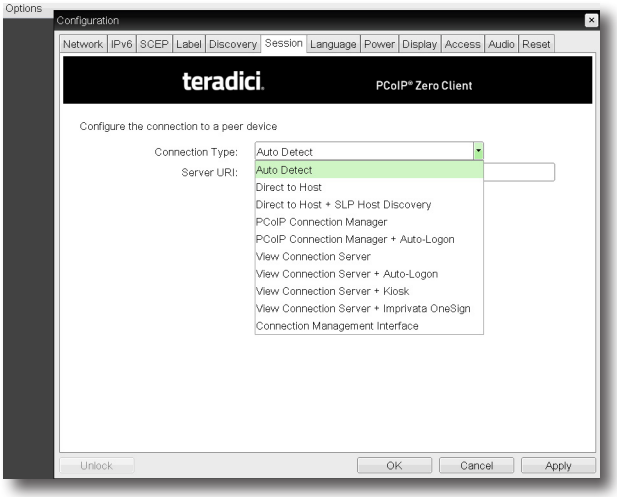


Figure 24: *Session selection drop down list*

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 in the *Teradici PCoIP® Zero Client and Host Administrator Guide*.

5.2.1 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.

5.2.2 Connect directly to a specified host

Important! This is not practical for large PCoIP deployments.

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

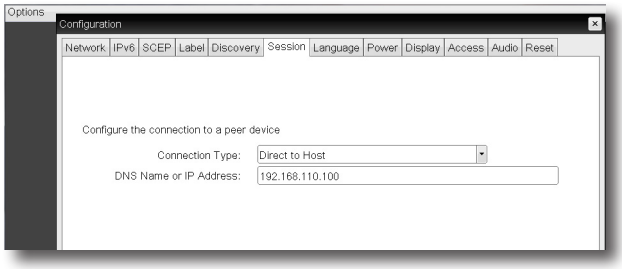


Figure 25: *Direct to Host connection type*

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.

5.2.3 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.

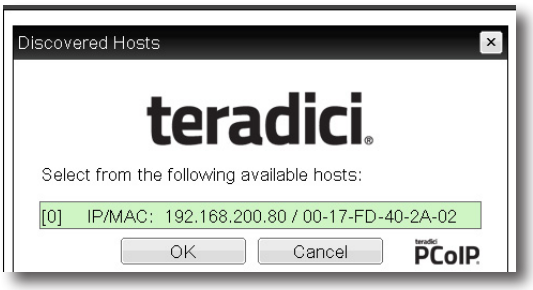


Figure 26: *The zero client OSD discovers and lists the first 10 available PCoIP hosts discovered*

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.

5.2.4 PCoIP Connection Manager

With a PCoIP Connection Manager you can 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.

5.2.5 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.

5.2.6 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**.

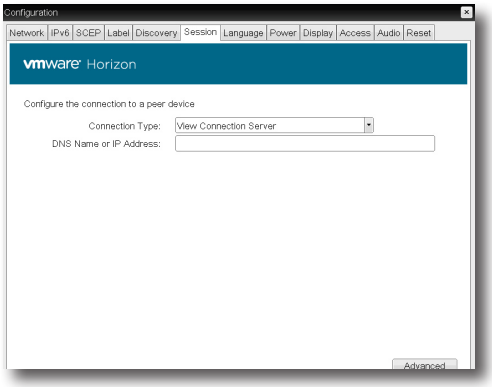


Figure 27: *View Connection Server selection*

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

5.2.7 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*.

5.2.8 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**.

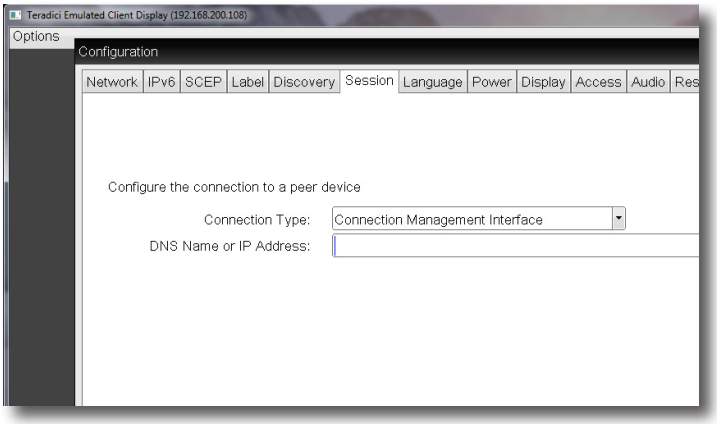


Figure 28: *Connection Management Interface selection*

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

3. Click **OK**.

See section 1.6 for more information about third party connection brokers.

5.3 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.

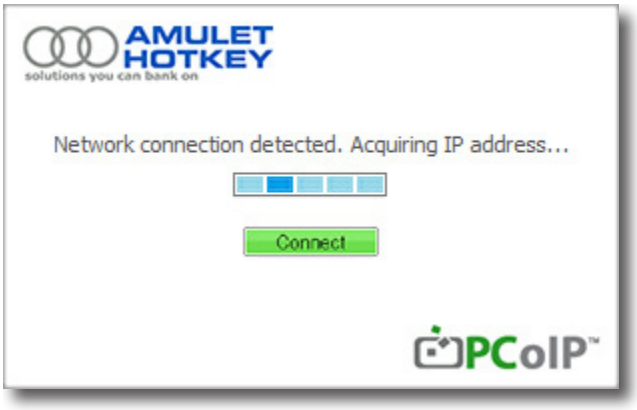


Figure 29: *OSD Automatic connection screen*

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

5.4 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*

5.5 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.

5.5.1 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.

5.5.2 Specify the connection broker

You can use any of the available management tools (see section 1.7) 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.

5.5.3 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.

ADDITIONAL INFORMATION

6

6. Additional information

6.1 Activate/deactivate the front panel switches (DXZ4 series only)

Amulet Hotkey zero clients can be installed in cable trays beneath desks or behind control panels.

To prevent accidental operation of the front panel switches, you can deactivate them. They are active by default.

6.1.1 Deactivate front panel switches

To deactivate the front panel switches:

1. Press and hold down the **Function** switch.
2. Press the **Menu** switch.

   The switch status LED goes off to indicate that the switches have been deactivated. See Table 4.

6.1.2 Activate the front panel switches

To activate the front panel switches:

1. Press and hold down the **Function** switch.
2. Press the **Menu** switch.

   The switch status LED illuminates green when the switches are active. See Table 4.

6.2 Extended USB connectivity (DXZC-E series only)

The DXZC-E series zero client is set apart from other zero clients by the extended number of available USB ports on the unit.

There are eight USB ports in total. These are either:

- Standard Downstream Ports (SDP), or;
- High charge-current ports that may be in either:

  a). Charging Downstream Port (CDP) mode when the unit is on, or;

  b). Dedicated Charging Port (DCP) mode when the unit is in standby.

See 6.2.1 USB-IF battery charging specification BC1.2 for definitions of the port types.

6.2.1 USB-IF battery charging specification BC1.2

BC1.2 defines the following modes. See Table 2.

Definition	Description
Standard Downstream Port (SDP)	Provides up to 0.5A charging current and data connection.
Charging Downstream Port (CDP)	Provides up to 1.5A charging current to suitable devices (that conform to the BC1.2 standard). Full data connection through charging ports when the DXZC-E is on.
Dedicated Charging Port (DCP)	Provides up to 1.5A charging current to suitable devices. No data connection when the DXZC-E is in standby.

Table 2: *Definitions from the USB-IF specification BC1.2*

6.2.2 Standard Downstream Ports (SDP)

There are six standard USB ports (SDP). The standard ports provide Wake on USB (WoU) capability when the unit is in standby.

If you plug a chargeable device into a standard port when the DXZC-E is in standby with WoU enabled, the DXZC-E will wake up, and the device will charge at up to 0.5A.

6.2.3 High charge-current ports

The zero client zero client (Rev2 onwards) offers two high charge-current ports on the rear panel. See Figure 31.

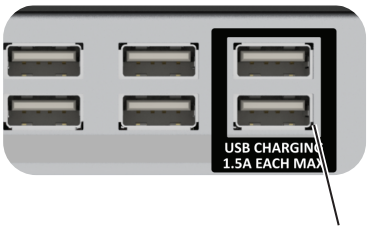


Figure 31: *High charge-current USB ports*

These ports can communicate with devices and allow a suitable device (that conforms to the BC1.2 standard) to charge at up to 1.5A.

> Important! The two high-charge-current ports cannot be used for Wake-on-USB operation when the DXZC-E is in standby.

6.2.4 Operation when the DXZC-E series is in standby mode

When the zero client is in standby with Wake-on-USB (WoU) enabled, the high charge-current ports are in DCP mode (see Table 2). The data lines are disconnected from the USB host so the port cannot be used for data, but some devices will charge at a higher rate than when connected to a CDP.

If you plug a chargeable device into a high charge-current port when the DXZC-E is in standby with WoU, the DXZC-E will not wake up, and the device will charge at up to 1.5A.

6.2.5 Operation when the DXZC-E series is powered on

When the DXZC-E is powered fully on, the high-charge-current ports are in CDP mode (see Table 2) and the port can be used for data as well as high speed charging.

6.3 Remote power cycling and BIOS access

In some cases it can be possible and useful to be able to power-cycle or reboot the host PC (or workstation) from the zero client. In addition, during the power-cycle, it may then be possible to access the BIOS from the zero client.

6.3.1 Power-cycle the Dell PowerEdge Blade Workstation

As Dell Blade PowerEdge Workstations contain an Amulet Hotkey BIOS, it is possible to power-cycle the host from the zero client. This can be done from the OSD screen when the keyboard is plugged into a USB port connected to the internal hub (any of the rear USB ports). Follow the on-screen instructions for accessing the BIOS on reboot of the host.

6.3.2 Power-cycle a remote PC

For remote host PCs that contain either a DXH4 or DXP4 card it may also be possible to reboot the PC remotely and access the BIOS. However this will depend on two factors:

- if the individual BIOS (such as Dell, HP, Lenovo) is supported for this;
- if a Remote Power Cable (RPC) is fitted to facilitate power-cycling.

There are several Knowledge Base Articles available for fitting different RPCs.

For power-cycling the remote PC, it is advisable to contact Amulet Hotkey Technical Support to discuss your individual set up.

6.4 Disable the audio (optional)

To disable audio:

1. Launch the AWI for the zero client that you want to configure.
2. From the home screen, choose **Permissions > Audio**.
3. Clear the **Enable HD Audio** check box.

6.5 Extended network connectivity (DXZ4 series only)

The DXZ4 series zero clients all have two network ports. The two network ports can be utilized for traffic or network redundancy.

The DXZ4 and DXZ4-A have two RJ45 ports for copper connections, whereas the DXZ4-M and DXZ4-AM have two ports that accept SFP modules for copper or fibre..

6.5.1 Dual redundant network connections

Important! Both main and auxiliary network ports (see Figure 20: Connecting up the zero client (DXZ4 series shown) on page 26) are connected to an internal, unmanaged network switch. The zero client 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:

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

2. 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.

3. If the zero client cannot reach the host within the retry period, it displays the Connect screen of the On Screen Display. See 1.7.3 On Screen Display (OSD).

4. 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 1.6), you can configure the session so that the Windows desktop is locked while disconnected.

6.6 Network performance

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. Performance depends on the available bandwidth and signal latency.

6.6.1 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 3 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 3: *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.

6.6.2 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 1.6 Cooling considerations) to optimise performance for most conditions.

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

Zero Client LEDs

7

7. LED descriptions

7.1 Key

The tables in this chapter 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.

7.2 Zero client front panel status LEDs

7.2.1 DXZ4 series

There are two status LEDs on the front panel, the SWITCHES active status LED and the LINK LED. There are also three illuminated switches, Fn, Power and Menu. See Figure 32.

Figure 32: *DXZ4 front panel LEDs*

7.2.2 DXZC series

There are two status LEDs on the front panel, the DEVICE LED and the PCoIP LED. See Figure 33.

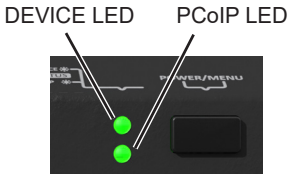


Figure 33: *DXZC front panel LEDs*

7.3 Status LEDs on the DXZ4 only

7.3.1 SWITCHES active status LED (DXZ4 only)

Tells you the state of the front panel switches.

LED status	Meaning
Off	Front panel switches are deactivated. See 6.1.
Green	Front panel switches are active

Table 4: *Switch status LED activity*

7.3.2 Menu and Fn switch LEDs (DXZ4 only)

Both of these LEDs light when the switch is pressed.

LED status	Meaning
Off	Switch is not pressed
Blue	Switch is pressed

Table 5: *Menu and Fn switch LEDs (DXZ4)*

7.4 Status LEDs on the DXZ4, DXZC and ZeroTop

7.4.1 LINK LED (PCoIP on the DXZC)

This LED shows the status of the PCoIP link. See Table 6.

LED status	Meaning
Off	No PCoIP link is established
Green wink	PCoIP link is available but not in session
Green	PCoIP session is active
Amber	Host is in sleep mode
Red	Fault with Teradici PCoIP

Table 6: *PCoIP status LED indications*

7.4.2 Power LED (or DEVICE LED on DXZC).

The power LED on the DXZ4 series and ZeroTop (DEVICE LED on the DXZC) zero client displays the following indications.

LED status	Meaning
Red	Unit is in standby; cannot be woken remotely (Wake-on-LAN, Wake on USB are not enabled)
Amber	Unit is in standby; can be woken remotely by Wake-on-LAN or USB activity
Amber wink	Unit is shutting down (DXZ4 only)
Amber flash	Unit is starting up (also shutting down for DXZC)
Green	Copper network connection with link established (SFP module or RJ45)
Green flash	Copper network connection is detected (SFP module or RJ45). No network link is established
For SFP Modules only (DXZC and DXZ4):	
Red flash	Fault condition, contact Technical Support
Blue	SFP fiber module detected; connected to network
Blue flash	No SFP fiber network connection (or no SFP module inserted)
Green	SFP copper module detected; connected to network
Green flash	No SFP copper network connection (or no SFP module inserted)
For DXZ4 SFP Modules only:	
Green/Blue flash	SFP copper module and SFP fiber module; no network connection
Long Green/ Short Blue cycle	SFP copper module and SFP fiber module. The Copper SFP module is connected to the network.
Long Blue/Short Green cycle	SFP copper module and SFP fiber module. The fiber SFP module is connected to the network.
Cyan flash	SFP module is not recognized (or no SFP module inserted)

Table 7: *Power LED (or DEVICE on DXZC) status LED activity*

7.5 Rear panel status LEDs

7.5.1 Network LINK and SPEED status LEDs

All zero clients have two network LEDs, LINK and SPEED (see Figure 34) on the rear panel that operate as follows:

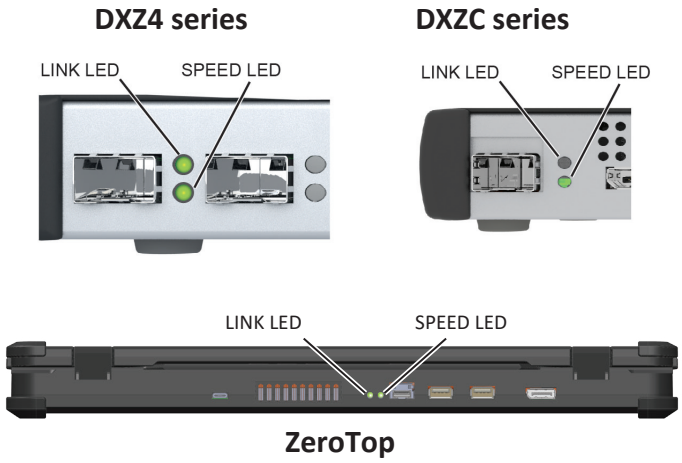


Figure 34: *Network LEDs on the rear panel*

1. **Network LINK status LED**

Status	Meaning
Off	No network connection
Amber (DXZ4)	Half-duplex network link, no traffic
Amber blink (DXZ4)	Half-duplex network link, traffic detected
Green	Network link up; no traffic
Green blink	Network link up, full duplex; traffic detected

Table 8: *LINK status LED indication*

2. **SPEED status LED**

Status	Meaning
Off	No network connection
Amber	100 Mbit/s connection
Green	1 Gbit/s connection

Table 9: *SPEED status LED indication*

7.6 Battery Status (ZeroTop)

The ZeroTop also has a battery indicator showing multiple LEDs. When the battery is fully charged, all the LEDs are lit indicating approximately 1.5 hrs battery life. As the power of the battery is used, the LEDs turn off one by one indicating the proportion of charge remaining. See 2.5 ZeroTop portable zero client for more details.

UPDATE THE FIRMWARE

8

8. Firmware updates

! Caution: *The security edition zero clients (DXZ4-A, DXZ4-AM, DXZC-A, DXZC-AM, DXZC-AMC, ZT100 & ZT101) use a version of firmware certified to comply with the National Cyber Security Centre (NCSC) requirements for Commercial Product Assurance (CPA). To maintain this certification, only upgrade these models with firmware certified by Amulet Hotkey. Contact Amulet Hotkey Support for further details.*

8.1 Manage the zero client firmware

The DXZ4, DXZC and ZeroTop zero clients all contain two different types of firmware:

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

The Teradici firmware is updatable on all models:

- See 8.1.1 Teradici firmware updates with the AWI for how to check and update the Teradici firmware;

Only the DXZ4 models can have user-updated BSM firmware.

- See 8.6 to check and update the BSM firmware for the DXZ4 series zero clients.

8.1.1 Teradici firmware updates with the AWI

Use the Administrative Web Interface (AWI) to manage firmware updates for the system:

- See 8.2 to connect to the zero client with the AWI;
- See 8.3.2 to check the Teradici firmware;
- See 8.4.1 to download Teradici firmware to the zero client;

8.1.2 Security measures for downloaded firmware files

Before you download a firmware update from the Amulet Hotkey or Teradici website:

1. Confirm that the SSL certificate for the webpage is valid and issued to the Amulet Hotkey or Teradici domain by clicking the padlock icon in the address bar of your browser.

After you download the file:

1. Confirm the file has not been modified by comparing its SHA-256 hash with the SHA-256 hash value listed next to the download link.

Note: Use the hash calculator of your choice to independently calculate the SHA-256 hash for the downloaded file.

8.2 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 1.5.

The login screen appears.

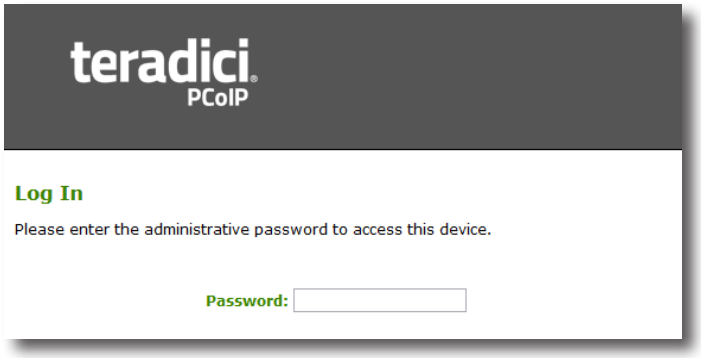


Figure 35: *Administrative Web Interface*

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

   The Teradici home screen appears.

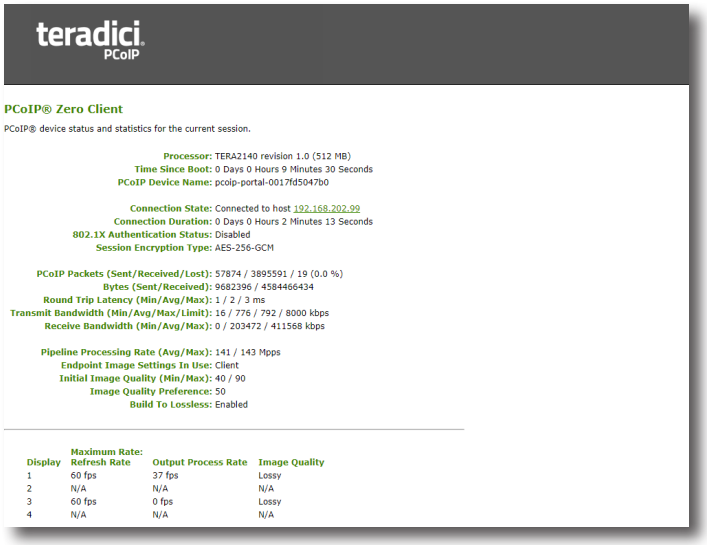


Figure 36: *AWI home screen*

! 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.*

8.3 Check the Teradici firmware

The zero client 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.

8.3.1 Keep firmware up to date

After you install the zero client, check the Amulet Hotkey and Teradici website and Amulet Hotkey 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 8.3.2 and 8.4.1;

8.3.2 Check the Teradici firmware

1. Login in to the AWI. See 8.2 for how to do this.
2. Select **Version** from the **Info** menu.

   The firmware version is displayed.

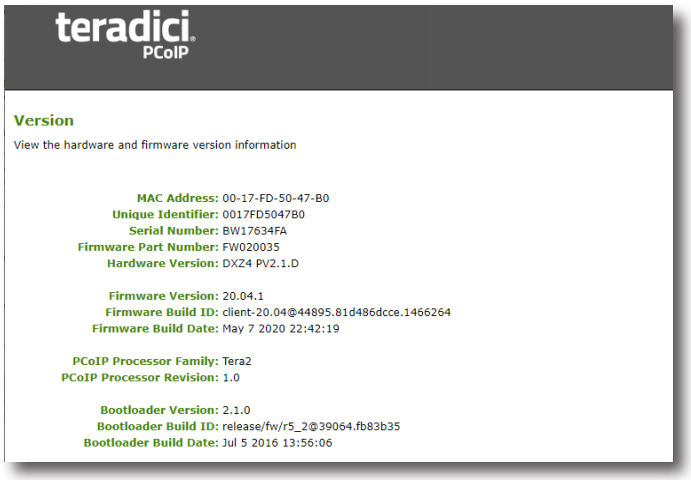


Figure 37: *AWI hardware and firmware version information*

8.4 Update the Teradici firmware

The firmware is constantly being improved and periodically updated.

8.4.1 Update the Teradici firmware

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

1. Login with the AWI. See 8.2 for how to do this.
2. Select **Firmware** from the **Upload** menu.

   The Firmware Upload window appears.

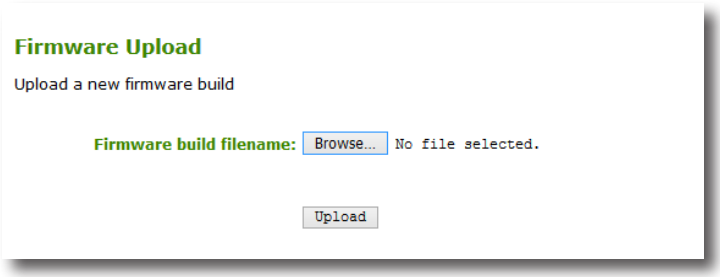


Figure 38: *Firmware Upload window*

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

   Note: This must be a *.all file.

   Example: tera2-zero-client-20-04-1-awi-upgrade.all

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

   After the firmware has downloaded successfully, a prompt appears.

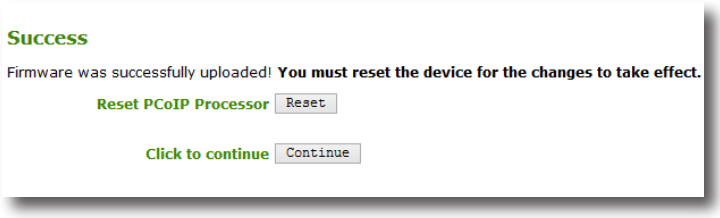


Figure 39: *Successful upload window*

5. Click **Reset**.

   Another prompt appears.

6. Click **OK** to continue.

8.5 BSM firmware updates

8.5.1 Firmware updates

! Caution: *The security edition zero clients (DXZ4-A and DXZ4-AM) use a version of BSM firmware certified to comply with the National Cyber Security Centre (NCSC) requirements for Commercial Product Assurance (CPA). To maintain this certification, only upgrade these models with certified firmware updates from Amulet Hotkey.*

! Caution: *BSM firmware updates are only possible on DXZ4 series zero client models. To update BSM firmware on DXZC series and ZeroTop zero clients, please contact Technical Support.*

Note: Firmware updates are supported on DXZ4 zero clients running BSM firmware version 2.0.0 or later.

Amulet Hotkey T2 PCoIP hosts and zero clients support remote updates for Board Support Micro-controller (BSM) firmware. You can update the BSM firmware by downloading a firmware update package over your network to the target BSM.

The are two methods to update BSM firmware depending on whether you are using Teradici firmware later than 5.2.0 and also BSM firmware versions later than 1.5.0.

Only the latest method is covered in this manual: For updating earlier versions, see our website or contact Technical Support.

- Update the BSM firmware for Teradici firmware version 5.2.0 and later;

We recommend that you apply new firmware releases at the earliest opportunity to make sure the latest improvements and patches are active in any deployment. The latest firmware release and instructions on how to update the zero client are available in the resources area of the Amulet Hotkey website.

Note: You may need to register on the Amulet Hotkey website to access some of the downloadable content.

8.6 Update the BSM firmware for Teradici firmware version 5.2.0 and later

To update the BSM firmware (for versions 1.5.0 and later), do the steps that follow:

1. Find the current version of the BSM firmware (optional);
2. Get the BSM firmware update file;
3. Transfer the firmware package to the target BSM;
4. Confirm that the firmware has updated;
5. Deactivate the BSM network interface.

8.6.1 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 zero client is powered on.
2. Browse to the IP address of the zero client and log on to the Administrative Web Interface (AWI).
3. Select **Network** from the **Configuration** tab.
4. Find the current version of the BSM firmware. This displays next to **BSM Firmware Version**:

8.6.2 Get the BSM firmware update file

1. Download the BSM firmware update file for Tera2 zero clients 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 0.4.8 firmware on a DXZ4 zero client is:

FW-DXZ4-0010_0_4_8-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.

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

You will use this IP address to transfer the firmware package to the BSM. In order to acquire an IP address, you temporarily activate the BSM network interface for the duration of the update process.

3. Log on to the Administrative Web Interface (AWI).

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

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

4. From the home page, choose **Configuration > Network**.
5. Select the **BSM network enable** check box. See Figure 40.

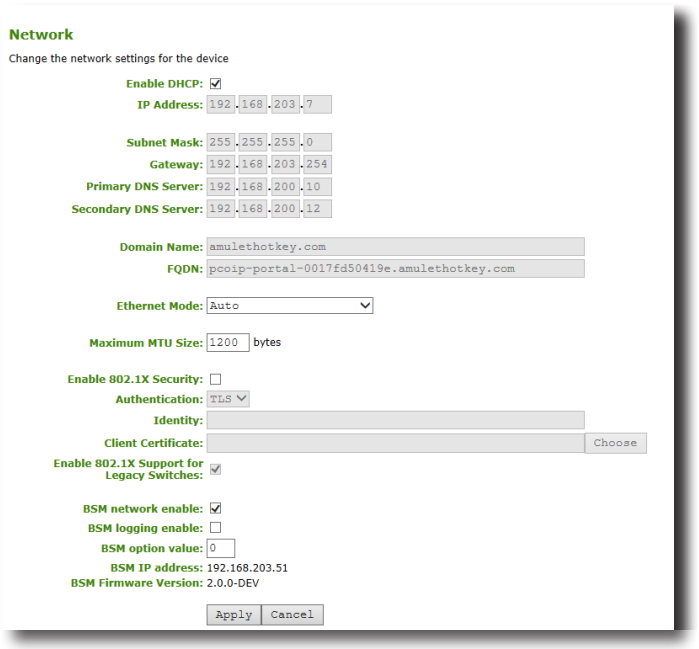


Figure 40: *BSM network enable option selected*

6. Verify that the target zero client is powered On.
7. Click **Apply**. The BSM now acquires an IP address from the DHCP server.
8. Now make a note of the BSM IP address from the network page. You may need to refresh the browser.

8.6.3 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 Tftpd32 utility, available from http://tftpd32.jounin.net/

1. Verify that the target zero client is on or in standby.
2. Launch the **Tftpd32** utility.
3. When Tftpd32 starts, go to the **Tftp Client** tab.

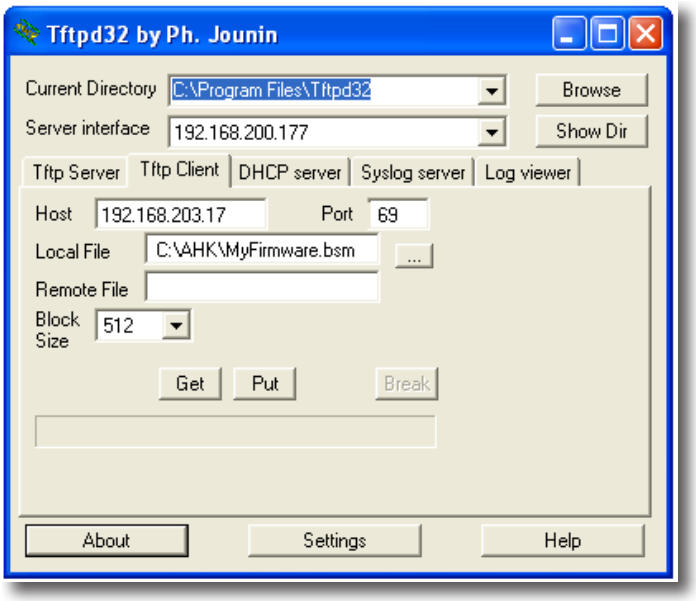


Figure 41: *TFTP utility client settings window*

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:	Set to 32768 bytes (Maximum).

Table 10: *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.

8.6.4 Confirm that the firmware has updated

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

1. When the zero client restarts, log on to the Administrative Web Interface (AWI).
2. From the home page, select the **Configuration > Network** page. See Figure 40.
3. Check the firmware version next to **BSM Firmware Version** is the new version.

8.6.5 Deactivate the BSM network interface

Finally, you must deactivate the BSM network interface to free up the IP address acquired and assigned in 8.6.2 step 2.

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.

8.6.6 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.)

SECURITY

9

9. Deployment security

This section describes how to improve security for your zero client network. This section is intended for those who have 'A' (security edition) zero client models. Some of these principles can be optionally implemented for other zero client models.

> Important! Some of the security measures described below recommend disabling the Administrative Web Interface (AWI). However, do not disable the AWI on your zero clients until after you have made all the security-based configuration changes in this chapter.

The National Cyber Security Centre (NCSC) document, *"Security Procedures: Amulet Hotkey Zero Clients"* (available at https://www.ncsc.gov.uk/products/amulet-hotkey) describes how to use your zero client and comply with the NCSC rating. See this document for a full description of the security considerations.

This chapter tells you how to:

- Check the anti-tamper seals (security models);
- Restrict access to the management tools;
- Set up the control of allowed USB devices;
- Disable the audio (optional);
- Use event logs;
- Dispose of zero clients securely.

9.1 Check the anti-tamper seals (security models)

We recommend that you store and use zero clients in an appropriately secure environment to reduce the potential for the device to be physically compromised.

Security zero clients and the ZeroTop are fitted with anti-tamper seals on the underside of the enclosure, see Figure 42. Inspect these seals when you receive the zero client and thereafter at regular intervals after deploying the zero client.

If you find any signs of interference or physical damage, you must immediately report this to the site security administrator and stop using the zero client.

Quarantine the zero client until the reason for interference or damage is fully understood and appropriate precautions have been taken.

Figure 42: *Location of the anti-tamper seals (not ZeroTop)*

9.2 Restrict access to the management tools

For additional security, we recommend that you disable the AWI and PCoIP Management Console interface on your zero clients before you deploy the zero clients to end-users.

With these interfaces disabled, you can only configure a zero client through its local On Screen Display (OSD). This security measure prevents malicious third parties from configuring your zero clients remotely.

9.2.1 Disable the AWI and PCoIP Management Console

> Important! Remember to complete the configuration procedures in this chapter before disabling the AWI.

To disable the AWI and Management Console interface and restrict configuration changes to the zero client's OSD:

1. From the **OSD Options** menu, choose **Configuration > Access**.
2. Select both of the following check boxes:
   - Disable Administrative Web Interface;
   - Disable Management Console Interface.

If you keep the AWI and CMI enabled, so that zero client administration is not restricted to the local OSD, make sure you perform any configuration changes from the trusted network on which the zero client is deployed.

If you want to make sure that the connection is confidential, you must use a Virtual Private Network assured to the classification of the data being exchanged.

9.3 Set up the control of allowed USB devices

Important! Make configuration changes using the AWI on each zero client and then disable the AWI before you deploy the unit to end-users (see 9.2).

The DXZ4 series and DXZC series zero client supports access control of peripheral USB and audio devices. We advise that you limit the USB devices accepted by the zero client to only include those devices that are critical for zero client usage.

9.3.1 Specify permissions for attached USB devices

To specify or deny permissions for attached USB devices:

1. Launch the AWI for the zero client that you want to configure.
2. From the home screen, choose **Permissions > USB**.
3. Specify lists of authorized and unauthorized USB devices. You can identify devices by ID (vendor or device) or by class (for example, 'Mass Storage' or 'Wireless').

   a). Add a 'white list' of any **authorized** USB devices;

   b). Add a 'black list' of **unauthorized** USB devices.

In both cases, you can use wild cards (* and ?) to define general device types that you want to allow or block.

Note: A list of hexadecimal vendor IDs and USB device IDs is available at www.linux-usb.org/usb.ids.

9.4 Disable the audio (optional)

Important! Make configuration changes using the AWI on each zero client and then disable the AWI before you deploy the unit to end-users (see 9.2).

We recommended that you disable the zero client audio inputs and outputs if they are not critical to the deployment operation.

To disable audio, see 6.4 Disable the audio (optional).

9.5 Use event logs

Important! Make configuration changes using the AWI on each zero client and then disable the AWI before you deploy the unit to end-users (see 9.2).

The DXZ4 series and DXZC series zero clients record a log of device activity and performance. The zero client supports Syslog and Network Time Protocol (NTP) to centralize and improve the accuracy of log data.

We recommend that you use both of these features. You can also specify a higher level of detail ('enhanced logging') in the zero client log for one specific category of log entry.

9.5.1 Enable event logs

To enable the Syslog and NTP protocols and set up enhanced logging:

1. Launch the AWI for the zero client.
2. From the home screen, select **Diagnostics > Event log**.
3. Enable and configure Syslog logging on the zero client.
4. Identify the Syslog server and choose a syslog facility for your zero clients.

   Note: You can also enable enhanced logging for a single category of log entries, such as USB entries.

5. From the home screen, choose **Configuration > Time**.
6. Configure the **Network Time Protocol** (NTP) parameters to allow zero client log entries to be time-stamped based on NTP time.
7. Make sure you specify an NTP server and the local time zone.

9.5.2 Check the event logs from the OSD

Inspect the event log at regular intervals for unexpected entries or activity. Follow your organisation's security procedure if the log includes unexpected or suspicious entries that indicate possible interference.

To use the OSD to inspect the event log:

1. Launch the On Screen Display.
2. From the **Connect** screen, choose **Options > Diagnostics > Event Log**.

To use the AWI to inspect the event logs:

1. Launch the Administrative Web Interface.
2. From the home screen, chose **Diagnostics > Event log**.
3. Click the **View** button.

9.6 Dispose of zero clients securely

The DXZ4 series and DXZC series zero clients support a factory reset option. This option resets all configuration and permission settings stored on the device.

If you intend to dispose of a device, make sure you apply the factory reset, and that this reset has been effective.

9.7 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.

10. Troubleshooting

10.1 Fault description and resolution

This section describes known fault conditions that may occur while using a zero client and how to resolve them.

If you need more information than is in the guide, please contact Technical Support through our website.

Symptom	Cause
Monitors display the incorrect display topology When using multiple monitors, the user experiences display problems. **Example:** Four monitors may be physically arranged in a grid or box, but the computer interprets mouse movements as though the monitors were arranged in a single row. This problem happens when a user connects to their usual PCoIP host from a different zero client. The problem repeats even after the user specifies the correct topology in the Display applet of Windows Control Panel.	This problem can occur when the following four conditions are met: • PCoIP Host Driver Function is enabled on the PCoIP host. • The PCoIP Host Software package is installed on the host computer. • The 'Use client topology settings…' check box is selected in the PCoIP Host Software Settings dialog. • An incorrect display topology is specified and enabled on the zero client. The zero client reports a specific display topology to the PCoIP Host Driver Function running on the host computer. In turn, the PCoIP Host Driver Function configures the Windows desktop to match the display topology reported by the zero client.
Devices attached to the Mouse USB port are blocked unexpectedly Resolve a problem with USB devices being unexpectedly rejected by the Mouse ports on the zero client front panel. If your organization has black-listed USB hubs (for example, to prevent users circumventing rules on prohibited USB devices), then any mouse, keyboard or other device plugged into the Mouse USB port on the DXZ4 series or DXZC series will be blocked. This is because the port's integral USB hub is itself rejected.	The DXZ4 series and DXZC series Mouse USB ports include an integral USB hub. Normally, the hub is transparent to the user. However, the hub can have unexpected consequences if your organization uses the **USB Permissions** feature of the PCoIP protocol to block unauthorized devices (black-listing) or only allow authorized devices (white-listing). If the Mouse USB ports on the zero client are white-listed to only allow specific HIDs (human interface devices such as a mouse or keyboard), then any HID attached to the rear ports will be rejected. This is because the DXZ4-A detects the hub behind the Mouse port, recognizes the hub as a non-HID, and blocks the attempted connection before the HID can be detected.
Primary desktop display does not consistently appear on zero client video 1 display output	Monitor emulation enabled on displays which have no physical monitor attached. Monitor emulation is a feature on the PCoIP Remote Workstation Card (also known as a host card) that ensures graphics cards see a valid EDID on a Display Port or DVI port on boot. This helps prevent the graphics card from driving DVI signals or DP signals on the wrong ports and monitors displaying a blank screen.
Some USB devices do not work correctly when connected to a zero client.	By default, when you connect a USB human interface device to a zero client, the zero client locally terminates the device. some USB devices require the use of specific drivers to make all their features operational.

Resolution

There are three possible resoulutions:

Fix 1: Configure the correct display topology on each zero client

If the user is likely to connect to their remote workstation from different zero clients (for example, in a hot-desking environment), the most reliable solution is to implement fix 1.

Note: We recommend this fix if the user is likely to connect to their remote workstation from different zero clients (for example, in a hot-desking environment).

Fix 2: Disable the display topology on each zero client

Note: We do not recommend fix 2 if the physical monitor arrangements are likely to differ for each zero client.

Fix 3: Disable the Use Client Topology Settings feature on the host computer

Note: We do not recommend fix 3 if the physical monitor arrangements are likely to differ for each zero client.

Note: The background and a workaround for this problem are described in Teradici knowledge base article, Why am I seeing display issues after installing firmware 4.0.2? (15134-1286):

If your organization needs to black-list USB hubs or white-list HID devices, any device connected to the zero client Mouse ports will be blocked. There are two possible workarounds:

- instruct users to connect their device to any other USB port on the DXZ4 series or DXZC series;
- if possible, remove USB hubs from the zero client's black list of unauthorized devices. (To compensate for this easing of restrictions, you may need to specify a corresponding white list of devices that are authorized for use in your organization. If so, users will need to connect these devices to the other USB ports.

Only enable monitor emulation on the PCoIP Remote Workstation Card display ports that will be used. Enabling monitor emulation on more ports than necessary can result in the operating system and graphics card using ports not in use on the client.

https://help.teradici.com/s/article/1310

Enable monitor emulation on head one only of the host card.

From the AWI select **Configuration > Monitor Emulation** and uncheck displays 2, 3 and 4.

With these drivers installed on the virtual desktop or remote workstation, the zero client must bridge the USB device to the remote PCoIP host instead of locally terminating the device.

Bridged devices use the drivers loaded on the associated workstation or virtual desktop. You can manually bridge up to 10 devices.

To bridge a USB device follow these instructions: https://resources.amulethotkey.com/download/AN_081_Bridging_USB_devices_on_a_PCoIP_zero_client_v1_2.pdf

Symptom	Cause
Poor performance with isochronous USB devices such as web cams, biometric or audio devices	When using a 1:1 PCoIP hardware configuration, all USB devices are transparently bridged from the zero client to the host, so in theory, all USB devices should work. Problematic devices are those which require a large amount of USB bandwidth to operate, such as HD webcams and USB audio devices. The reason why these devices can be problematic is that the USB transfer speed across PCoIP is limited in hardware. This is partly to ensure that the PCoIP session doesn't use too much network bandwidth (USB 2.0 could be up to 480Mbps), but also because USB does not compress as efficiently as audio/video data, and is much more reliant on packets arriving in order.
No Bloomberg biometrics support with zero clients and virtual machines	Some USB devices require specific drivers for all of their features to function (for example the Bloomberg biometrics, and the USB audio and message keys).
Zero client password reset	Unknown / Forgot password.
No video display output on Video port 1	Some GPUs in the host technology may default to displaying on other ports, for example Video port 2.

Resolution

The USB ports on the zero client connect to two different USB hubs:

- the first hub connects to the front USB port labelled 'keyboard' and both ports at the back of the zero client.
- the secon USB hub connects to the front USB port labelled Mouse is on a second USB hub.

For best results, make sure that each of the two different high speed USB devices are connected to the two different USB hubs within the zero client.

These devices may need to be bridged to the host workstation rather than be locally terminated at the zero client.

See the article on how to bridge a Bloomberg keyboard on a zero client:

https://resources.amulethotkey.com/download/AN_081_Bridging_USB_devices_on_a_PCoIP_zero_client_v1_2.pdf

Note: We have identified four VID and PID options for the Bloomberg STB100 keyboard. If you are using the Teradici Management Console to create a Profile to update the bridged device settings, make sure that all four VID and PIDs are added to the bridged device list.

STB100 variant #1	(VID=$1188, PID=$9544)
STB100 variant #2	(VID=$1188, PID=$9525)
STB100 variant #3	(VID=$1188, PID=$9535)
STB100 variant #4	(VID=$1188, PID=$9545)

See KBA attachment.

Remove the connection from Video port 1 and connect to Video port 2. If there is still no display output, try Video port 3 or Video port 4. If there is no display on any port, then contact Technical Support.

SPECIFICATIONS

11

11. Technical specifications

11.1 Warranty

Your zero client comes with a 3 year warranty.

11.2 Specifications common to all DXZ4 and DXZC series models

See 11.3.4 for ZeroTop specifications.

11.2.1 Common specifications

Description	Specification
Power consumption	Typically less than 12W (all models) excluding USB peripherals and DP-to-DVI adaptors
Power supply	DC adaptor. (Use only the adaptor supplied) **Output:** 12V DC. **Input:** 100-240V AC, 50-60Hz
Cooling	Passive
Case	Robust enclosure
Temperature range	Operating: 15° to 35° C (59° to 95° F), Storage: -10° to 60° C (15° to 145° F)
Humidity	10% to 90% (non-condensing)
Compliance	All models conform to the relevant parts of EN55024, EN55032, CE and FCC Part 15
Memory	512MB DDR3 RAM
Audio connections	Stereo line out, stereo mic. All 3.5mm jacks **Output:** 0Hz to 21.6kHz (48kHz sampling); 0Hz to 19.846kHz (44.1kHz). **Input:** 10Hz to 21.6kHz (48kHz sampling); 10Hz to 19.846kHz (44.1kHz).
Network connections	Standard models have an RJ45: 10/100/1000BaseT network port 'M' models have an SFP port that accepts fiber or copper modules, up to 1Gbps **Note:** Available modules are listed in the SFP Modules Datasheet
VDI	Compatible with VMware View
USB connections	4 x USB (SDP) 2.0 Type A (up to 0.5A charging current), including keyboard and mouse ports USB 2.0 devices are supported, but not in high speed mode. 'C' and 'E' models have different USB specifications
Flash programmable	Via Ethernet for Teradici firmware only

Table 11: *Common specifications to all zero client models*

11.2.2 PCoIP ports

PCoIP uses an IPSec datastream (ESP) with a TCP control channel. This channel uses port 4172. Depending on the type of deployment, other ports may be required, including:

- TCP port 50000 for a connection broker and the PCoIP Management Console;
- TCP port 80 and TCP port 443 for the Administrative Web Interface (AWI).

For a full list of ports and protocols used by PCoIP, contact Amulet Hotkey Technical Support.

11.3 Model specifications

11.3.1 DXZC series and DXZC-E series only

Description	Specification
Core technology	Teradici PCoIP Tera2 (2132 chipset)
Video output	2 x DisplayPort connectors. (Dual Mode)
Display support	1920 x 1200 maximum (dual monitors) @ 60 Hz 2560 x 1600 maximum (single monitor) @ 60 Hz
Audio connections	Front panel headset socket is wired for AHJ (American Headset Jack) headsets; alternative wiring options are available on request
Dimensions (H x W x D)	DXZC models: 34 x 176 x 131 mm (1.3 x 6.9 x 5.2”) DXZC-E and ‘C’ models: 34 x 230 x 131 mm (1.3 x 9.1 x 5.2”)
Unit weight (excluding packaging)	DXZC series: 0.6 kg (1.6 lbs) DXZC ‘C’ models: 0.8 kg (1.8 lbs) DXZC-E: 1.5 kg (3.3 lbs)

Table 12: *Video, technology and dimension specifications for DXZC and DXZC-E models*

11.3.2 DXZC-E series only

Description	Specification
DXZC-E series USB connections	6 x USB (SDP) 2.0 Type A (up to 0.5A charging current), including keyboard and mouse ports 2 x USB (CDP) Type A (up to 1.5A charging current)

Table 13: *USB port descriptions for DXZC-E series*

11.3.3 DXZ4 series only

Description	Specification
Core technology	Teradici PCoIP Tera2 (2140 chipset)
Video output	4 x DisplayPort 1.1 connectors. (Quad mode)
Display support	1920 x 1200 maximum (quad monitors) @ 60 Hz 2560 x 1600 maximum (dual monitors) @ 60 Hz
Dimensions (H x W x D)	34 x 230 x 131 mm (1.3 x 9.1 x 5.2”)
Unit weight	1.5 kg (3.3 lbs) excluding packaging

Table 14: *Video, technology and dimension specifications for DXZ4 series models*

11.3.4 ZeroTop

Description	Specification
Core technology	Teradici PCoIP Tera2 (2132 chipset)
Memory	512MB DDR3 RAM
Integrated Video	15.6” full HD (1920 x 1080) Laptop screen
Secondary video	Full HD (1920 x 1080) via rear panel DisplayPort
Audio connections	Stereo headset/headphones on 3.5mm jack, stereo microphone on 3.5mm jack
USB connections	3 x USB 2.0, type A
Network connections	Small Form Pluggable (SFP) accepting copper or fibre module
Power	DC inlet via USB type C connection from external supply
Battery	3.4Ah Lithium Ion (1.5 hr+ battery life)
Temperature range	Operating: -5 to 40C (23 to 104F) Storage: -10 to 60C (14 to 140F)
Size (H x W x D) & Weight	402mm x 256mm x 46.3mm (15.7 x 10.1 x 1.8”) lid closed, bump stops. 3.5kg (7.7lbs) exlcuding packaging
Security	Strong encryption and authentication including 256-bit AES and NSA Suite-B ciphers. Unique USB lockdown control
Compliance	TAA, CE

Table 15: *ZeroTop technical specifications*

11.4 Security specifications

All our zero clients have 802.1X network authentication; AES256 bit encryption. NSA Suite B ciphers. SIPR hardware token support.

Note: TEMPEST versions of the DXZ4 are available, approved to NATO SDIP-27 Level A and Level B by our TEMPEST-certified NCSC and NATO partners.

11.4.1 NCSC security edition (‘A’) zero clients and ZeroTop

Any model with an ‘A’ in the suffix (examples are DXZ4-A, DXZC-AM, or DXZC-AMC) and the ZeroTop have been evaluated by the NCSC Commercial Product Assurance Scheme and approved for use at foundation grade for Remote Desktop v1.0.

11.4.2 Card reader (‘C’) zero clients only

Any model with ‘C’ in the suffix and the ZeroTop ZT101 have CAC smart card and SIPR Net hardware token support.

Integral card reader models (DXZC-EC and DXZC-EMC)	
Standards	ISO 7816, EMV 2000 Level 1, GSA FIPS 201 approved product list
Protocols	T=0, T=1; 2-wire: SLE 4432/42 (S=10); 3-wire: SLE 4418/28 (S=9); I2C (S=8)
Supported card types	5V, 3V and 1.8V smart cards; ISO 7816 Class A, A and C
Smart card detection	Movement detection with auto power-off; automatic detection of smart card type; short circuit and thermal protection
Supported APIs	PC/SC driver (ready for 2.01); CT-API (on top of PC/SC); synchronous-API (on top of PC/SC); OCF (on top of PC/SC)
Durability	100,000 insertions
USB ports	3 x USB (SDP) 2.0 Type A (up to 0.5A charging current), including keyboard and mouse ports

Table 16: *Integrated smart card reader specifications*


AMULET®
HOTKEY