Trusted Zero Client Administrators' Guide

23.06

Table of Contents
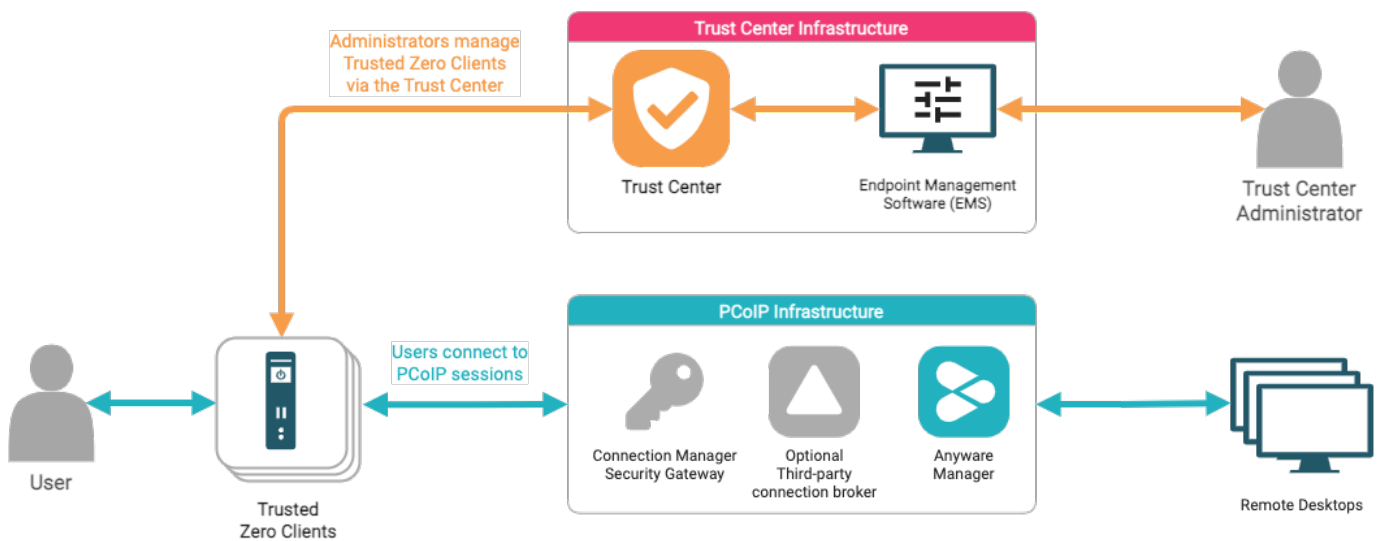
Anyware Trusted Zero Client Administrators' Guide

The **Trusted Zero Client** is HP's next-generation standalone PCoIP client, securely connecting users to their HP Anyware remote desktops, as well as Amazon WorkSpaces and VMware Horizon View using the PCoIP protocol (VMware Horizon support is currently in beta). Trusted Zero Clients are designed around strict zero-trust principles, providing extremely secure connections and ensuring device integrity wherever they are deployed.

Deployments of Trusted Zero Clients are monitored and managed by the *Anyware Trust Center*, which enforces security and configuration settings for each endpoint device in your deployment.

System administrators set policies and manage deployments of Trusted Zero Clients via a vendor-provided application called an *Endpoint Manager*, also referred to as *Endpoint Management Software (EMS)*, which acts through the Anyware Trust Center to ensure the most secure connection possible.

Device Management

Trusted Zero Client settings are managed by systems administrators using Endpoint Management Software (EMS), which is provided by your device's manufacturer. Some settings may be controlled by users via the client interface, when permitted by deployment policies.

A Trusted Zero Client cannot be used without an Anyware Trust Center.

- 6/60 -

What's New in This Release

This is the first public release of the Trusted Zero Client.

Requirements

All Trusted Zero Clients are factory-provisioned and ready to register with an **Anyware Trust Center**, which enforces zero-trust policies and features, and allows administrators to control Trusted Zero Client deployments.

Requirement	
Available Anyware Trust Center port	The Trusted Zero Client must be able to reach an Anyware Trust Center, on its connected network, on TCP port **32443**.
Available PCoIP ports	The Trusted Zero Client must be able to access required PCoIP components, such as brokers and agents. For a comprehensive list of ports used by PCoIP components, see What are the required TCP/UDP ports for PCoIP technology? in our Knowledge Base.
Anyware Trust Center FQDN	You must know the Anyware Trust Center's address (FQDN) in order to set up the Trusted Zero Client before first use, *unless* you are on a LAN and the `anywaretrustcenter` DNS route has already been configured by your IT administrators.

> 🔥 **Important: Registration with the Anyware Trust Center is required**
>
> The Trusted Zero Client must connect to and register with an Anyware Trust Center before it can connect to PCoIP sessions.

About Provisioning

Trusted Zero Clients are provisioned at the factory, where they are given birth certificates that are validated by the Anyware Trust Center. Provisioned Trusted Zero Clients can only be used with the Anyware Trust Center they are registered with.

About Registration

Provisioned Anyware Trusted Zero Clients must be *registered* with an Anyware Trust Center before they can connect to remote desktops. This process is described next, in Connect to an Anyware Trust Center.

After registration, a Trusted Zero Client is bound to its Anyware Trust Center. If you need to re-register a Trusted Zero Client with a different Anyware Trust Center, you must factory reset the device.

Setting up the Trusted Zero Client

The first time the Trusted Zero Client is powered up, you will complete a few one-time configuration steps; including setting the device's language and connecting to the Trusted Zero Client. Once these steps are completed, you will be ready to create desktop connections.

Set Your Interface Language

Choose the language you prefer for the client's *pre-session interface*. This setting controls most of the dialog and menu text that you see before connecting to a remote desktop. It does not affect the remote desktop language.
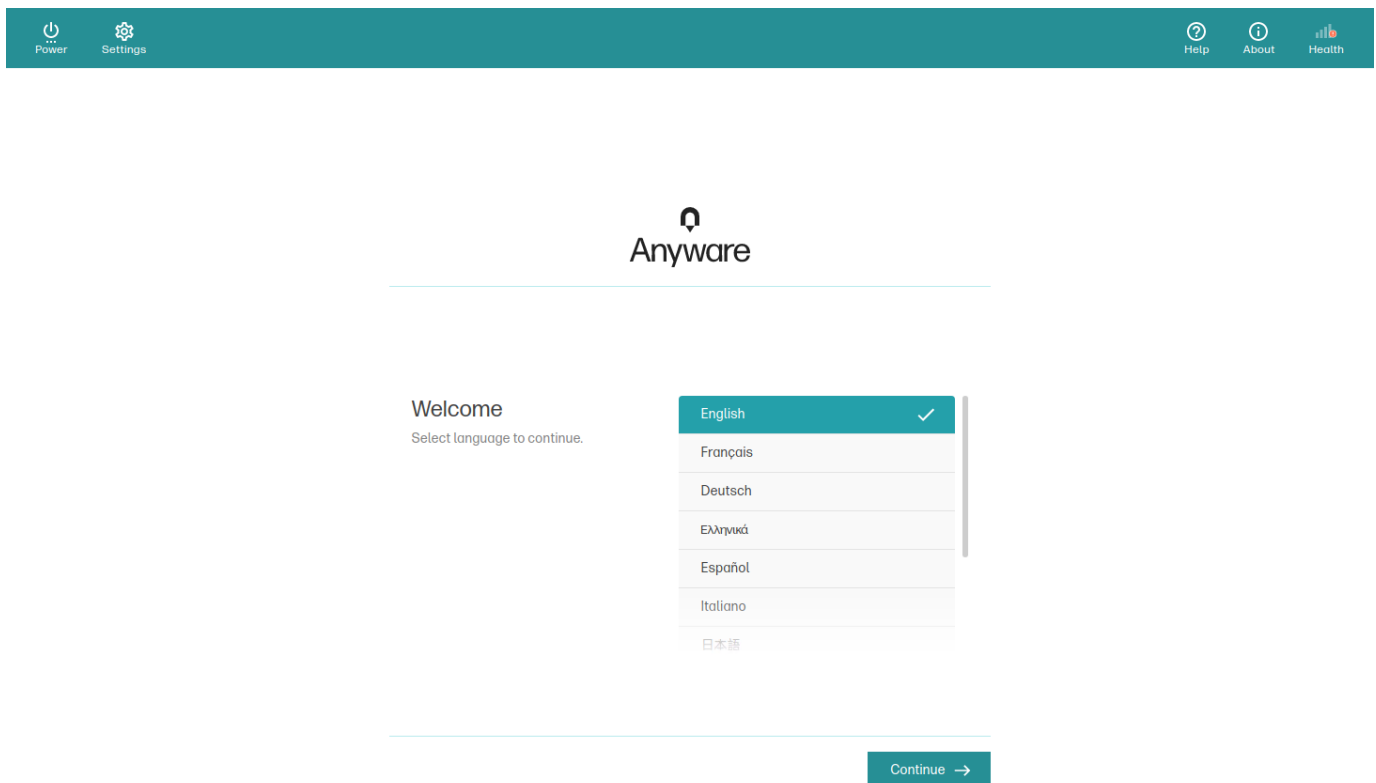
Note that there are some dialog screens, such as those provided by brokers, that are not localized and will not be affected by this setting.

Validate Network Settings

After setting the language, the Trusted Zero Client will validate your network settings. If there is a problem with your network connectivity, you will see an error similar to this:
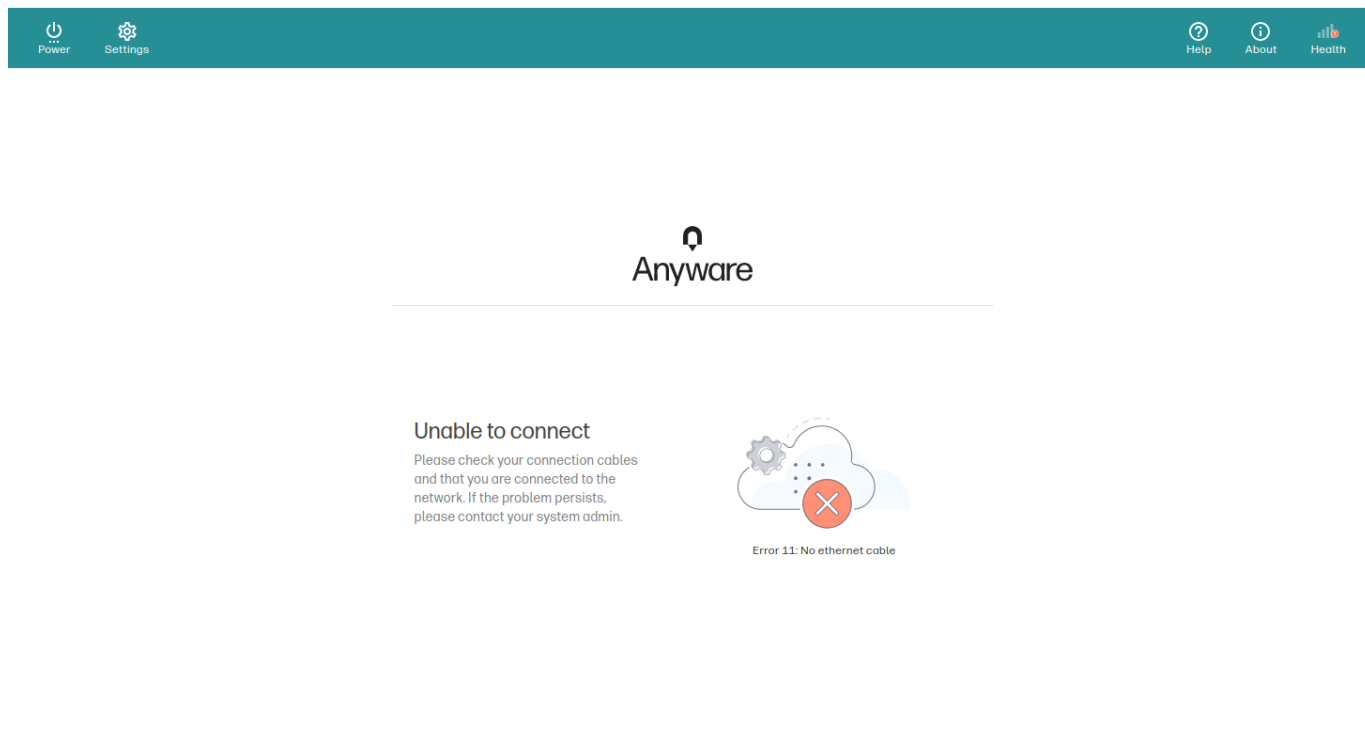
Connect to an Anyware Trust Center

Finally, register the device with an Anyware Trust Center. Once registered, your device will be able to connect to remote desktops and will be managed by the Anyware Trust Center.

> ✏️ **Note: This step is not required on a preconfigured LAN**
>
> If your IT administrators have already set up your network and you are on a LAN, this step is not required.

To register the Trusted Zero Client with your Anyware Trust Center:

1. Confirm that your network is configured to allow the Trusted Zero Client to reach the Anyware Trust Center on its configured connection port (by default, this is **port 32443**).

2. Connect the Trusted Zero Client to the network and power it on.

3. You will be prompted to select a language for the Trusted Zero Client's interface. Choose the language you want to use (you can change this later via the settings menu).

4. When prompted for a connection address, provide the FQDN of your Anyware Trust Center and click **Connect**.
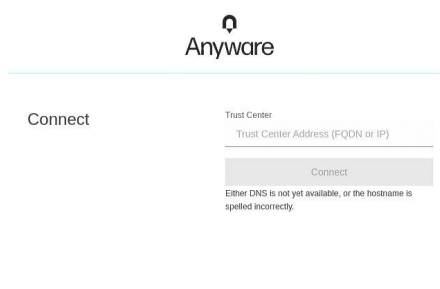
If the network configuration and FQDN are both correct, the Trusted Zero Client will automatically register itself with the Anyware Trust Center.

After the initial successful connection, the Trusted Zero Client will automatically connect to the Anyware Trust Center when it is powered on or restarts.

Updating the Trusted Zero Client

The Trusted Zero Client receives updates from the Anyware Trust Center using an over-the-air (OTA) update system. You do not need to manually download and install updates.

When a new release is available, the Anyware Trust Center acquires it automatically; your IT administrator then schedules downloads from the Anyware Trust Center to each Trusted Zero Client.

Once the new version has been downloaded by your device, you will be prompted to reboot to apply it.

Connecting

Connecting to a Remote Host

The Trusted Zero Client can connect to any Windows, Linux, or macOS host with a PCoIP agent installed, Remote Workstation Cards, and Amazon WorkSpaces desktops. Connections can be made directly (client direct to host), or brokered through Anyware Manager, an Anyware Connection Manager, or VMware Horizon (beta).

Creating Your First Connection

> 🔥 **Important: Connections are policy-controlled**
>
> The ability to create and modify connections may be limited or removed by your deployment administrators. If these views are not available, they have been preset on the Anyware Trust Center and you can skip to [Connecting to a Session](#).

The first step is to create a *connection* between your Trusted Zero Client and your remote desktop. This connection is made either to your connection broker, for managed deployments, or directly to a remote host.

1. Launch the Trusted Zero Client.

2. If this is your first connection, the Trusted Zero Client will prompt you to create one:
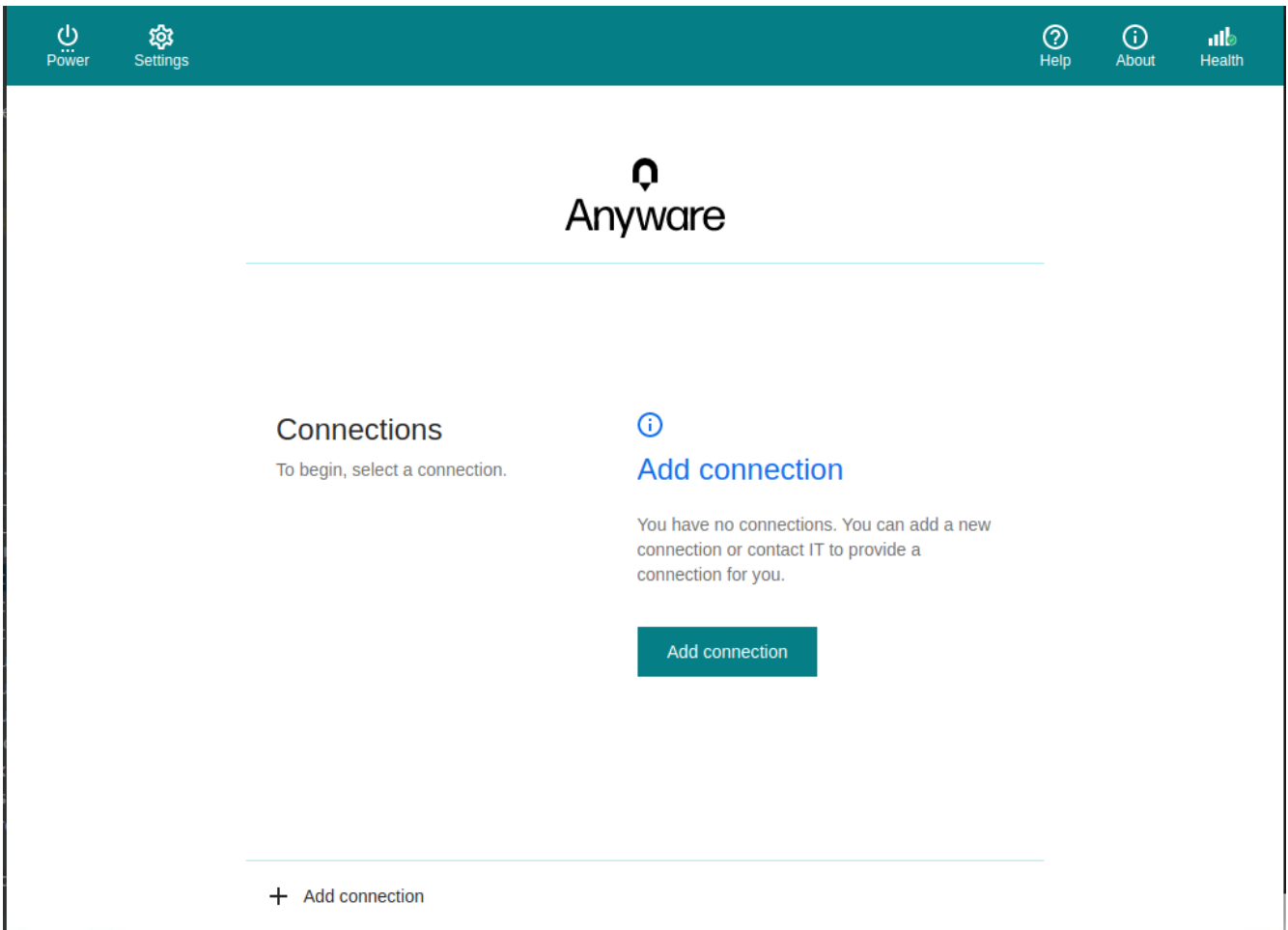
Click **Add a new connection**, and proceed to the next section.
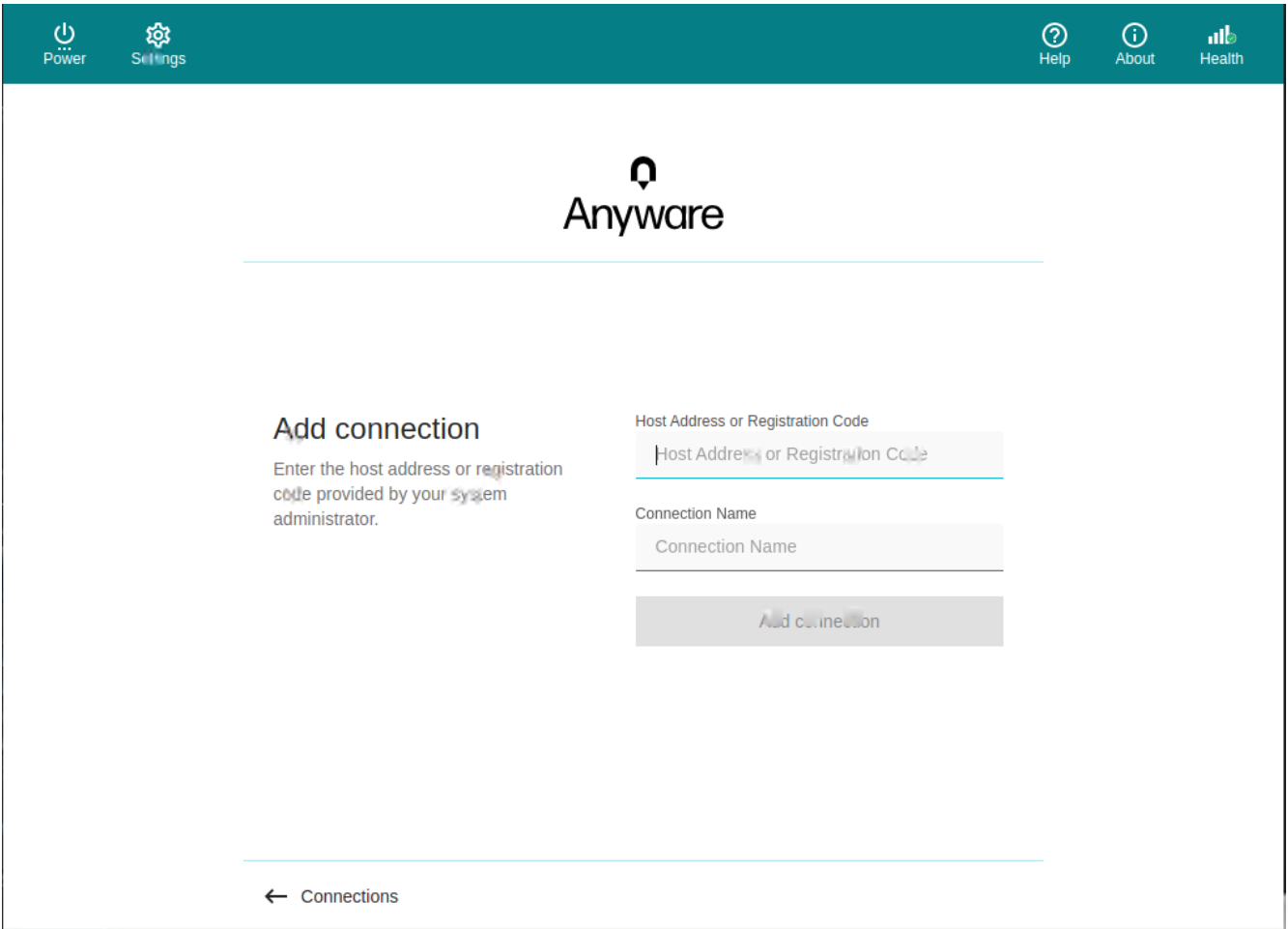
Creating a New Connection

> 🔥 **Important: Connections are policy-controlled**
>
> The ability to create and modify connections may be limited or removed by your deployment administrators. If these views are not available, they have been preset on the Anyware Trust Center and you can skip to [Connecting to a Session](#).

Create a new connection by clicking **+ Add a new connection** at the bottom of the *Connect* pane. You can add as many connections as you like.

1. In the *Add New Connection* pane, there are two fields to provide:

Copyright 2023 HP Development Company, L.P

- **Host Address or Registration Code**: Enter the address of the remote system you want to reach (you should have this information from your system administrator). This field accepts IP addresses, domain names, and registration codes, as in these examples:

  - *An IP address*: `123.456.789.012`

  - *A FQDN*: `remote-desktops.example.com`

  - *A registration code*: `a1b2c3!@#`

  > ✏️ **Note: Amazon WorkSpaces registration codes**
  >
  > If you are connecting to an Amazon WorkSpaces desktop, provide your WorkSpaces registration code in this field.

> ✏️ **Note: VMware Horizon connections (beta)**
>
> To connect to a VMware Horizons broker, provide the address of the Horizon broker in the *Host Address or Registration Code* field. Support for VMware Horizon connections is currently in beta, and may not always work as expected. If you use this feature and encounter problems, please open a support ticket and let us know what's happening.

- **Connection Name** *(optional)*: If desired, provide a name for this connection. This can be anything; you will use this name to select this connection in future sessions. You can always change it later.

2. Click **Add connection**.

Once this is done, your connection will appear as a button in the desktop selection list.

Connecting to a Session

1. If you have created at least one connection, the Trusted Zero Client will now look something like this:
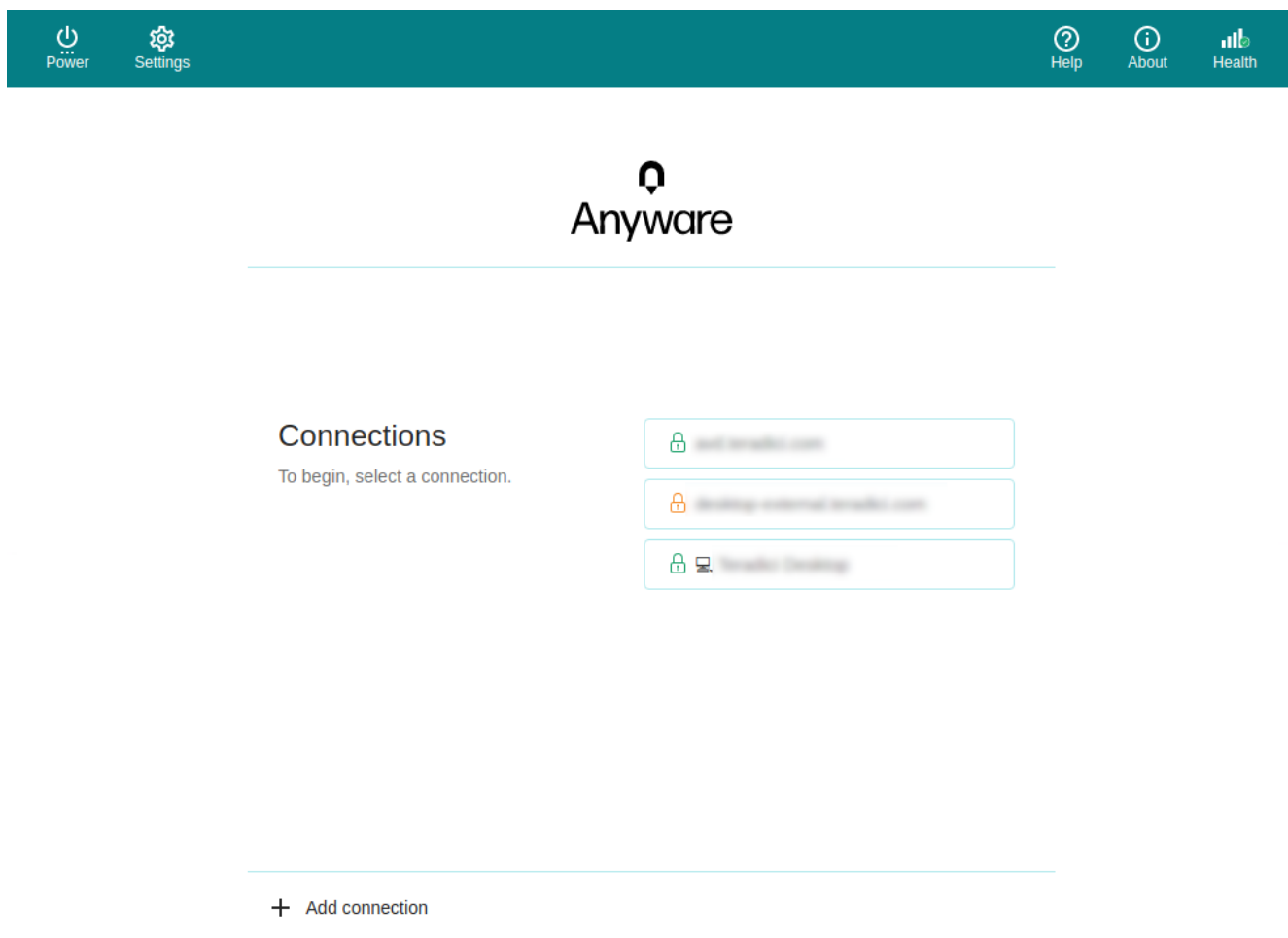
2. Click the name of the connection you want. Next, provide your username and password:

> ✏ **Note: About authentication credentials**
>
> For **managed connections**, the authentication screen and validation that happens here is provided by Anyware Manager or by your connection manager. The credentials are supplied to you by your system administrators, and are usually your corporate credentials.
>
> For **direct connections** where no broker is present, use the credentials for your user account on the remote machine.

3. If configured, you will see a *Multi-Factor Authentication* (MFA); the actual display shown will depend on your MFA provider and your IT policies. Follow the prompts provided in your interface.

4. Once your credentials are accepted:

- **If you have a single desktop** available, your connection credentials will be used to automatically log into it and your session starts immediately.

- **If you have multiple desktops** available, the shows you a list of desktops. Click the desktop you want to connect to.
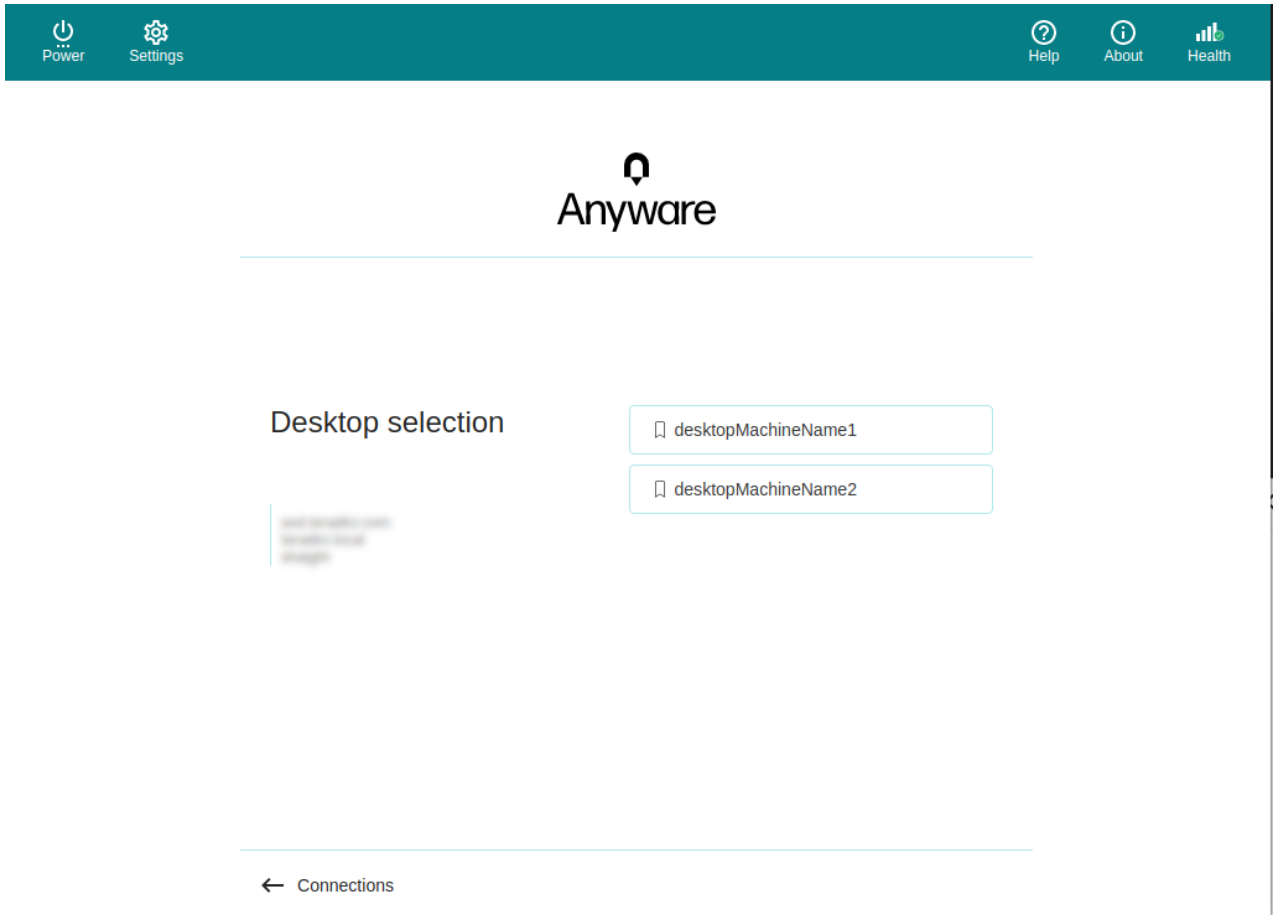
> 🔥 **Tip: Managing desktops**
>
> You can change the labels that appear in this list to make them easier to identify, and may be able to remotely restart them as well (if supported). See Managing Desktops for instructions.

Once you have selected your desktop, you will be connected to it and your PCoIP session will begin. The first time you connect to a desktop, there may be a slight delay before the connection is active.

There may be a delay of a few seconds before you have control of your mouse and keyboard; this is normal.

Managing Desktops

You can manage the desktops belonging to each of your defined connections. The following actions are available, when supported by the desktop:

- Rename the desktop's label in the client.

- Restart the remote desktop (if supported).

- Display information about the desktop, including its resource name and protocol.

To use these features, first authenticate display the list of desktops belonging to the connection, then select the action you want from the available desktops. These procedures are described next.

Rename a Desktop

By default, the Trusted Zero Client displays the *machine names* of your remote desktops. These names can often be automatically-generated strings that are difficult to identify or differentiate. You can modify the name shown in the desktop list to give them human-friendly names that are easier to understand.

> ✏️ **Note: Only labels are changed**
>
> This procedure changes the label shown in the client interface. It does not change the desktop's machine name.

To change a desktop label:

1. Display the desktop list as described above.

2. Click **Rename**:
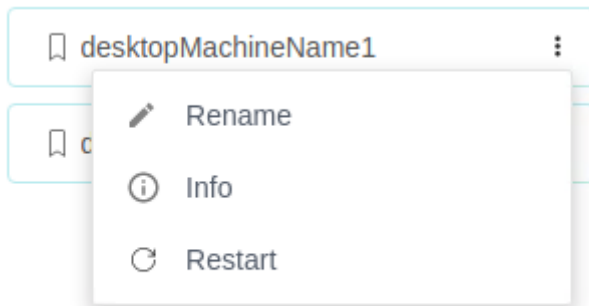
3. Provide a new name to use in the desktop list. Note that once this is done, the default machine name will no longer be visible; if you need to see it later, see <u>View Desktop Information</u>.

Restart a Desktop

You can send a restart command to a remote desktop from the client interface, if supported by your remote system.

> ✏️ **Note: Not all deployments support this feature**
>
> The restart option is only be available if your remote system supports it. If it does not, the option will be disabled.

To restart a remote desktop:

1. Display the desktop list as described <u>above</u>.

2. Click **Restart Desktop**:
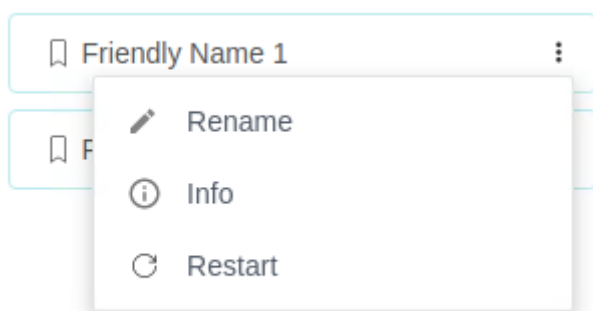
The remote desktop will be restarted. Note that it will be unavailable for connections until the restart is complete, which may take several minutes.

View Desktop Information

You can view detailed information about each of your available remote desktops, including resource names, IDs, and protocols.

> 🔥 **Tip: Desktop machine names**
>
> If you have [renamed a desktop](#), the original machine name is the *resoruce name* shown here.

To view desktop info:

1. Display the desktop list as described [above](#).

2. Click **Info**:

3. Review the displayed information.

4. To dismiss the info window, click **OK** or click the close button in the top corner.

Connecting to Amazon WorkSpaces

Amazon WorkSpaces connections use the same process described [above](). Provide your registration code in the *Host Address or Registration Code* field, and the Trusted Zero Client will recognize it as a WorkSpaces registration code and handle it appropriately.

Disconnecting from a Remote Host

To disconnect from a session, do one of the following:

- Press `Ctrl` + `Alt` + `Shift` + `F12` .

- Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of any display, and select either of the following options:

    - Select **Connection** > **Disconnect**.

    - Select **Anyware PCoIP Client** > **Quit Anyware PCoIP Client**.

In-Session Actions

Connecting USB Devices

Remote desktops can use USB devices that are attached to the client using a process called *redirection*. USB devices are not automatically redirected to the remote desktop; they must be specifically connected to the session.

> ✏️ **Note: Excludes Mice and Keyboards**
>
> Normal Human Interface Devices (HID), such as keyboards and mice, are always connected and used by the remote desktop. This page describes using non-HID USB devices such as tablets or cameras.

Important considerations

- **USB functionality depends on PCoIP Agent configuration**: The remote PCoIP agent must be configured to allow USB redirection. If it is not, the *Connection > USB Devices* option will not be visible in the Trusted Zero Client menu bar and only HID devices like keyboards and mice will be used.
- **Persistence**: USB device connections do not persist across multiple PCoIP sessions. You must connect your USB device each time you connect.
- **NoMachine USB Drivers**: The Trusted Zero Client is not compatible with NoMachine and No Machine USB drivers. For information on how to uninstall NoMachine USB drivers, see NoMachine's knowledge base.

Connecting a USB Device

Connecting a USB device to your session must be done after the session is established.

To Connect a USB device to the remote session:

1. Attach the USB device you want to connect to your Trusted Zero Client.

2. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

3. From the menu bar, select **Connection** > **USB Devices**.

   A list of all USB devices connected to your Trusted Zero Client appears. The name shown in the list is self-reported by the device; some devices will identify themselves only as *USB Device*.

   > 🔥 **Important: Connecting special HID devices**
   >
   > Because most Human Interface Devices (HID devices) are automatically processed by the Trusted Zero Client, they do not appear on this list even if they use a USB connection. However, certain HID devices—like Wacom tablets—actually do require processing on the remote host, and will not work as expected unless connected to the session.
   >
   > To show these hidden HID devices and allow them to be connected, enable the **Show Human Interface Devices** checbox. You may also need to perform additional configuration steps or install drivers on the remote machine.

4. Click **Connect** beside the USB device you want to use.

Disconnecting a USB Device

You can disconnect a USB device from the in-session menu:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **Connection > USB Devices**.

3. Click **Disconnect** beside the USB device you want to disconnect.

Connect USB Webcams

USB Webcams may be used in remote sessions by connecting them to a Windows remote session as USB devices. This feature has been tested with a limited number of popular webcams, including the Logitech C920. See [PCoIP Cloud Access Software Webcam Support](#) for a current list of tested webcams.

This feature is only supported by the Graphics Agent for Windows and the Standard Agent for Windows, and is limited to resolutions of 480p or lower.

Sending Ctrl+Alt+Del

You can send a `Ctrl` + `Alt` + `Del` command in two ways:

- By pressing the `Ctrl` + `Alt` + `Del` keys on your attached keyboard, or

- By using the menu bar command:

    a. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

    b. From the menu bar, select **Connection** > **Send CTRL+ALT+DEL**.

Features

Audio

Stereo audio output and mono audio input are supported and enabled by default. Only one audio device can be used at a time. Support for multiple audio devices will be added in a future release.

Enhanced A/V Sync

The Trusted Zero Client supports **Enhanced A/V Sync**, an enhanced audio and video synchronization feature that improves full-screen video playback. A/V lock reduces the difference in delays between the audio and video channels and smoothing frame playback on the client, improving lip sync and reducing video frame drops for movie playback.

Enhanced A/V Sync introduces a small lag in user interaction responsiveness when enabled. Using enhanced audio and video synchronization will reduce the maximum frame rate.

Enhanced A/V Sync is enabled separately for each display, so it can be selectively engaged on displays where synchronized audio and video are particularly important without affecting the frame rate or responsiveness of the other displays in session.

To enable Enhanced A/V Sync:

1. When in a remote session, reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **View** > **Enhanced AV Sync** for the display you want to enable.

Connection Health Indicator

The **Connection Health Indicator** gives you quick feedback on the quality of your active PCoIP session, including a general status indicator and several specific metrics that you can use to troubleshoot connection problems. The Connection Health Indicator can be opened before you join a PCoIP session or during a session.

Pre-Session Health Indicator
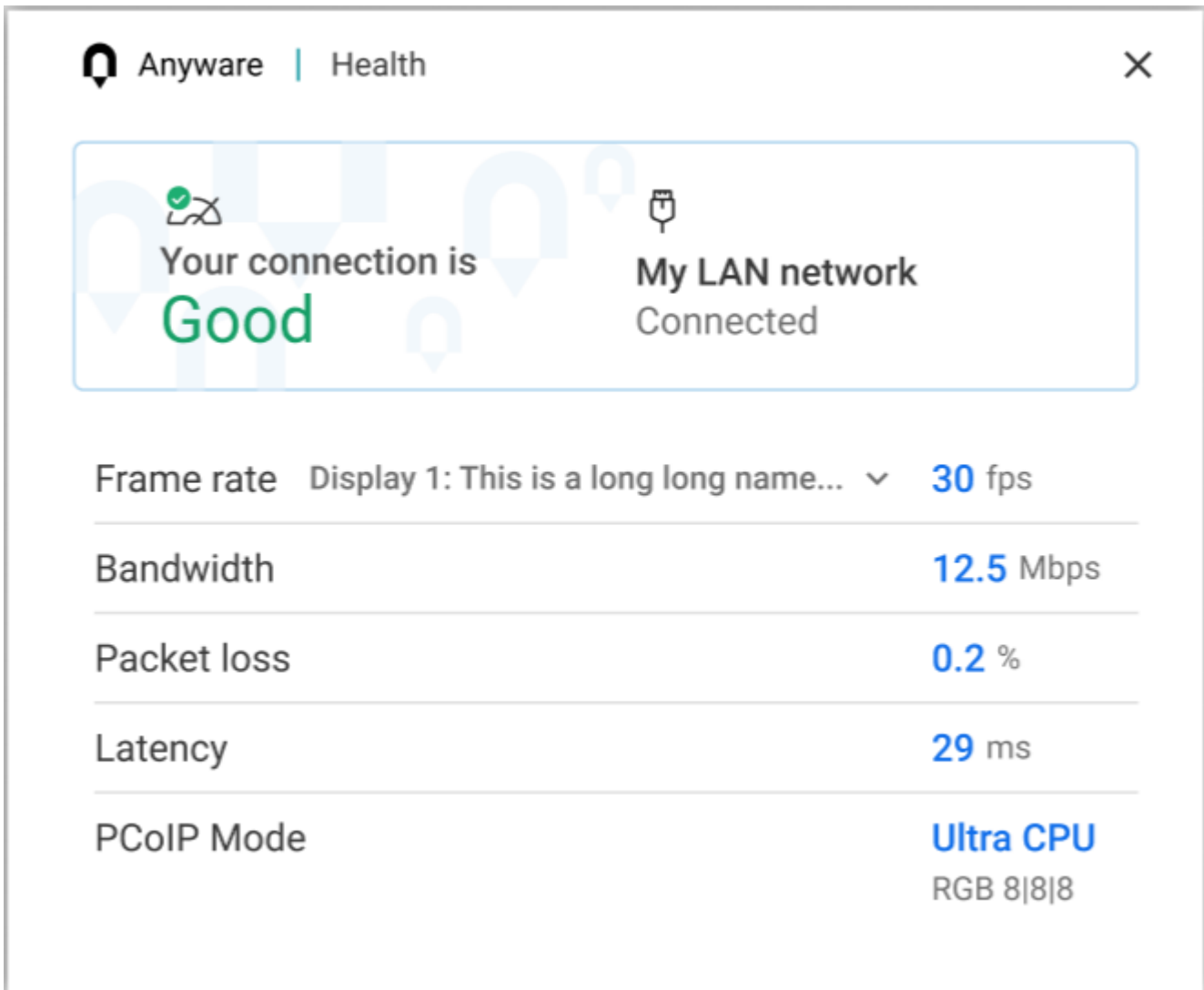
Before you select a desktop and join a session, the Health Indicator is available in the pre-session menu bar. To open it, click the **Health** icon.

In a pre-session state, the health indicator tells you if the Trusted Zero Client is connected to a network, and if it is connected to an Anyware Trust Center. If either of these conditions are not met, the may not be able to join a PCoIP session. Note that once a has registered with a , it can continue to connect even if the is not available.

If the Trusted Zero Client is connected to the network and to the Anyware Trust Center, the health indicator icon will be green.

In-Session Health Indicator

After joining the PCoIP session, launching the Connection Health Indicator provides additional telemetry on your general connection quality and stability.

To open the Connection Health Indicator:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **Health** > **Connection Health**.

The Anyware Health opens as a separate window on top of the current session. You can move the window as needed, including to a different monitor, but it will remain on top of the current session displays until it is closed.

The Anyware Health monitor shows the general network health status, identifies the type of network connection being used, and displays several real-time metrics.

Connection Health Status

The general connection health is described as *good*, *fair*, or *poor* depending on a combination of packet loss and latency statistics.

Connection Health Status	
Good	The network connection is healthy and should provide excellent PCoIP performance.
Fair	The network is experiencing packet loss greater than 0.25%, or latency greater than 50ms. PCoIP sessions may be degraded, and you may experience moderate dropped frames, image stutter, and sluggish responsiveness.
Poor	The network is experiencing packet loss greater than 0.5%, or latency greater than 100ms. PCoIP sessions will be significantly degraded and will suffer from dropped frames, stutter, poor responsiveness, and loss of image quality.

Network Connection Indicator

This identifies the type of connection your client is using for the current session, including the name of the connected network and its state.

Measured Statistics

The following real-time statistics are reported in the Anyware Health indicator:

Metric	Description	Notes
Frame rate	Displays the current frame rate for the PCoIP session.	If you have multiple displays, you can check the frame rate for each display by selecting it from the provided dropdown. Frame rates are dynamic in PCoIP sessions, varying by the amount of dynamic content shown on screen as well as network and hardware capacity. It is normal for PCoIP frame rates to drop as low as zero if the screen content is perfectly static.
Bandwidth	The total network bandwidth being used by the current PCoIP session.	Bandwidth utilization fluctuates based on many factors, including frequency and range of dynamic screen changes and audio output.
Packet loss	The percentage of PCoIP packets that are being lost to network quality.	Packet loss greater than 0.25% will negatively affect PCoIP performance; a loss of greater than 0.50% will result in severely degraded performance.
Latency	The total end-to-end network latency between the PCoIP client and PCoIP agent.	Latency greater than 50ms will negatively affect PCoIP performance; latency greater than 100ms will result in severely degraded performance.
PCoIP mode	The active PCoIP protocol mode.	Note that PCoIP Ultra Auto-Offload mode can employ different protocols on different screens simultaneously; you can select a specific display from the dropdown here to inspect them individually.

Display Support

The Trusted Zero Client supports a maximum of four displays, with a maximum resolution of 4K UHD (3840×2160). Currently, the display order cannot be changed.

> ✏️ **Note: Using multiple high-resolution displays**
>
> Systems with multiple high-resolution displays, such as quad 4K UHD topologies, require powerful system infrastructure. Be sure to use a system with sufficient bandwidth and client capability to support your required display topology.

Detect Monitors

Your local monitor configuration is detected automatically when you connect to the remote session. If the local display configuration changes *during* a session—for example, if you attach a new local monitor, or disconnect an old one—the display mapping between the local and remote topographies is no longer accurate,leading to unpredictable display behavior. You must be refresh the display mapping to accurately show the new configuration.

To synchronize local display changes:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **View** > **Detect Monitors**.

> ✏️ **Note: Alternate method**
>
> In some cases, using *Detect Monitors* may not work. If this happens, you can synchronize the displays by disconnecing from your session, plugging in all of your monitors, and reconnecting.

The local display configuration will synchronized with the remote. The local displays may flicker or go black momentarily while the remote system updates its display topography.

USB

USB Support

The Trusted Zero Client supports redirecting USB devices to a remote session. Administrators can set rules governing allowed and disallowed devices, device classes, or device protocols.

USB redirection is enabled by default. If you want to restrict or disable USB support for a specific desktop, you can globally disable or set rules governing USB behavior via settings on the Anyware Trust Center. USB rules can also be set on the remote desktop's PCoIP agent; disallowing a USB device from either *either* Anyware Trust Center or PCoIP agent will prevent it from working in-session.

Isochronous USB device support

USB devices that rely on time-sensitive information, such as webcams or storage volumes, are referred to as *isochronous* devices. Some isochronous devices are supported when connecting to the Trusted Zero Client. Unless support for an isochronous device is explicitly stated in this documentation, do not assume it will work.

Wacom Tablets

This section describes how the Trusted Zero Client supports Wacom Tablets, the different connection modes, and additional Wacom features available.

> 🔥 **Tip: Wacom terminology is changing**
>
> The terms we use to indicate these modes is changing. Existing users should note the following:
>
> • *Local termination* is now called **Tablet Performance** mode.
>
> • *Bridged mode* is now now called **LAN Connect** mode.
>
> Other products, such as Anyware Software Clients, may still use *bridged* and *local termination* internally and in documentation; those will change in the near future.

Wacom Tablet Support

Wacom Tablets can be connected to the remote PCoIP session using one of two modes: *Optimized* (the default), which provides highly responsive performance and better tolerance of high-latency networks, and *Override*, which is less performant and susceptible to latency issues, but may provide support for additional features such as force touch.

> ✏️ **Note: Tablets must be manually connected to PCoIP sessions**
>
> Tablets must be connected to the PCoIP session after the session is established. For more information, see [Connecting a Wacom Tablet](#) below.

TABLET PERFORMANCE MODE CONNECTION SUPPORT

> 🔥 **Tip: Terminology change**
>
> *Tablet Performance* mode is the new name for *local termination*. The feature is the same.

Wacom tablets that are connected via *Tablet Performance Mode* connections preprocess the tablet signal on the client before sending it on to the remote host. This results in improved responsiveness

and better tolerance for high-latency networks. Some advanced device functionality may not be available in this mode.

Tablet Performance mode is used automatically whenever it is supported for a connected Wacom tablet. In some cases, you may prefer to use *LAN connect* mode—if, for example, you must use sophisticated tablet features like touch, which is not supported by Tablet Performance mode—you can override this behavior by changing its connection type in settings.

Wacom tablets that can use *tablet performance mode* connections

	PCoIP agents (Windows)	PCoIP agents (Linux)	PCoIP Graphics Agent for macOS	PCoIP Remote Workstation Card
Intuos Pro Small *PTH-460*	✔	✔	—	—
Intuos Pro Medium *PTH-660*	✔	✔	✔	—
Intuos Pro Large *PTH-860*	✔	✔	✔	—
Cintiq Pro 16 *DTH-167*	✔	✔	—	—
Cintiq Pro 16 *DTH-1621*	✔	✔	—	—
Cintiq 22 *DTK-2260*	✔	✔	—	—
Cintiq 22HD *DTK-2200*	✔	✔	—	—
Cintiq Pro 24 *DTK-2420*	✔	✔	—	—
Cintiq 22HDT - Pen & Touch *DTH-2200*	—	—	—	—
Cintiq Pro 24 - Pen & Touch *DTH-2420*	✔	✔	—	—
Cintiq Pro 27 *DTH-271*	✔	✔	—	—
Cintiq 32 Pro - Pen & Touch *DTH-3220*	✔	✔	—	—

> 🔥 **Important: Touch is not supported**
>
> Touch features of Wacom devices are not supported with tablet performance mode connections.

LAN CONNECT CONNECTION SUPPORT

> 🔥 **Tip: Terminology change**
>
> *LAN Connect* mode is the new name for *bridged mode*. The feature is the same.

LAN Connect mode sends all Wacom tablet inputs directly to the remote host for processing. Because device processing is performed by the host's Wacom driver, this typically provides more complete support for advanced device features; however, because device events must complete a round trip from the device to the host and back before the artist sees the result of a change, it is not as performant as Tablet Performance mode.

Wacom tablets should only be connected using LAN Connect mode in low-latency environments. LAN connections in high-latency networks (greater than 25ms) will appear sluggish and difficult to use for artists, and are not recommended.

By default, LAN Connect mode is used to connect a tablet *only* if tablet performance mode connection support is not available for it. You can change the preferred handling for a specific device by [changing its connection type in settings](#).

> ✏️ **Note: Graphics Agent for macOS does not support LAN Connect mode for Wacom tablets**
>
> The Graphics Agent for macOS only supports tablet performance mode connections for Wacom devices, as indicated in the table above.

Wacom Tablets that can use LAN Connect connections

	PCoIP agents (Windows)	PCoIP agents (Linux)	PCoIP Graphics Agent for macOS	PCoIP Remote Workstation Card
Intuos Pro Small *PTH-460*	✔	✔	–	✔
Intuos Pro Medium *PTH-660*	✔	✔	–	✔
Intuos Pro Large *PTH-860*	✔	✔	–	✔
Cintiq Pro 16 *DTH-167*	✔	✔	–	–
Cintiq Pro 16 *DTH-1621*	✔	✔	–	–
Cintiq 22 *DTK-2260*	✔	✔	–	✔
Cintiq 22HD *DTK-2200*	✔	✔	–	✔
Cintiq Pro 24 *DTK-2420*	✔	✔	–	✔
Cintiq 22HDT - Pen & Touch *DTH-2200*	✔	✔ *Ubuntu only*	–	✔
Cintiq Pro 24 - Pen & Touch *DTH-2420*	✔	✔	–	✔
Cintiq Pro 27 *DTH-271*	✔	✔	–	–
Cintiq 32 Pro - Pen & Touch *DTH-3220*	✔	✔	–	✔

Connecting Cintiq Pro 32 Tablets

The Wacom Cintiq Pro 32 appears as *three* separate devices in the USB menu. You must connect all three USB devices to use this tablet:

- ExpressKey Remote

- Cintiq Pro 32 Touch

- Wacom Cintiq Pro 32
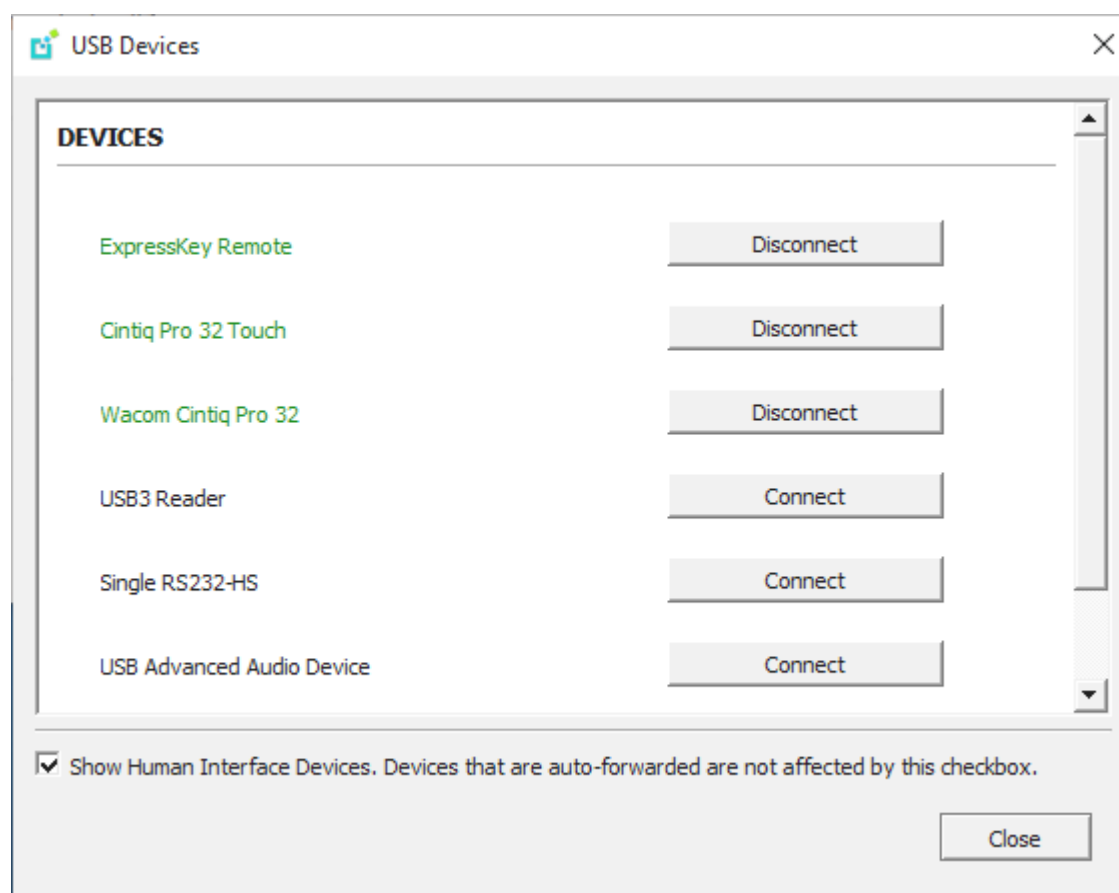
Working with Wacom Tablets

CONNECTING A WACOM TABLET

To use the Wacom tablet, **you must manually connect it to the PCoIP session**. Wacom tablets that are not connected will appear to the remote host as a mouse, resulting in a confusing situation where the tablet appears to work but only acts as a pointer.

ASSIGNING A TABLET MONITOR

You can select a monitor to use with your Wacom tablet.

To configure Tablet Monitor settings:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **View** > **Tablet Monitor**.

3. On the session desktop, open the Wacom Desktop Center and select **Wacom Tablet Properties**.

4. Select your device, tool and application.

5. Select your screen area from the dropdown menu.

CHANGING WACOM TABLET ORIENTATIONS

You can change the orientation of your Wacom tablet for left-handed use. The left-handed orientation configures the tablet for a left-handed orientation. Select **ExpressKeys Right** for a left-handed orientation, and **ExpressKeys Left** for a right-handed orientation. Rotate the tablet to the desired orientation.

To configure Tablet Orientation:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **View** > **Tablet Orientation Left-handed**.

3. On the session desktop, open the Wacom Desktop Center and select **Wacom Tablet Properties**.

4. Select your device, tool and application.

5. Select your tablet's orientation from the dropdown menu:

   • For left-handed orientation, select **ExpressKeys Right**.

   • For a right-handed orientation, select **ExpressKeys Left**.

MATCHING TABLET PROPORTIONS TO DISPLAY PROPORTIONS

You can enable the **Tablet Force Proportions** feature of your Wacom tablet in a PCoIP session. This feature constrains the device to match the horizontal and vertical proportions of your display, ensuing that there is no undesired stretching of your drawing.

For example: if you draw a perfect circle on the device, with *tablet force proportions* enabled the display will show a perfect circle; when it is disabled, the circle could appear as an ellipse depending on the screen proportions.

When this mode is enabled, some of the device's active surface may not be usable. Only the portion of the device that matches the proportion of the screen will be active.

> ✏ **Note: Wacom driver setting must match**
>
> The Wacom driver must also be configured to use force proportions, or this setting will have no effect.

To enable or disable *Tablet Force Proportions*:

1. Reveal the Trusted Zero Client's menu bar by moving the mouse cursor to the top of a display.

2. From the menu bar, select **View** > **Tablet Force Proportions** to toggle the setting.

Webcam Support

The Trusted Zero Client supports USB webcams when connecting to a PCoIP Agent for Windows. USB webcams can be used while in the remote desktop, including with applications such as Microsoft Teams or Zoom.

For detailed information which models have been tested and the performance metrics associated with these models see here. This knowledge base article also deals steps on how to test and verify other webcam models.

This feature is enabled by default.

Requirements

Webcam support requires the following:

- A Windows remote desktop, with installed PCoIP Standard Agent for Windows or PCoIP Graphics Agent for Windows, 21.03+
- A USB-attached webcam.

Notes and Limitations

If the browser on the remote desktop terminates when a webcam is connected, you must disable the webUSB setting in Chrome by running the following command in the search bar of the Chrome browser:

```
chrome://flags/#enable-webusb-device-detection
```

Open the Chrome menu and disable the webUSB flag.

Setup

On the Trusted Zero Client, connect the webcam as described in USB Bridging of Webcams.

Trusted Client Settings

The Trusted Zero Client allows users to configure a limited number of settings via the pre-session interface (before connecting to a PCoIP session). All configuration settings are available from the **Settings** menu at the top of the Trusted Zero Client pre-session display.

> ✏️ **Note: Settings are pre-session only**
>
> These settings are only available from the pre-session menu, before connecting to a PCoIP session, and globally affect the Trusted Zero Client and any remote connections it makes.

General Settings

Date and Time Settings

You can set the device's local time zone and choose a display format for both the date and time.

Task	Location	Options
Set Time zone	**Settings**>**General**>**Date & Time**>**Timezone**	Select your time zone from the dropdown list. This setting is pushed to the remote desktop when you connect.
Set Date Format	**Settings**>**General**>**Date & Time**>**Date Format**	Choose a date display format from the dropdown list. This setting affects the Trusted Zero Client display only.
Set Time Format	**Settings**>**General**>**Date & Time**>**Time Format**	Choose a time display format. This setting affects the Trusted Zero Client display only.

Language Settings

The Trusted Zero Client's display language can be customized. This setting affects the device's pre-session display and the in-session menu (viewed by hovering the mouse cursor at the top of the screen during a session).

Task	Location	Options
Change language	**Settings**>**General**>**Language**	Select your desired interface language from the dropdown list.

Client Version Information

You can find information about your Trusted Zero Client device, including its serial number, processor, memory, and endpoint ID via the settings menu.

Task	Location	Options
View Client Version Information	**Settings**>**General**>**Client Version Information**	Click **Client Information** to view the device's metadata in a new window.

Devices

These settings govern the behavior and connections of external devices attached to the Trusted Zero Client, like Wacom tablets, keyboards, and mice.

Connection

USB Devices and Connection Types

You can view information about the available USB devices attached to the Trusted Zero Client, and configure the ways they are connected to the remote desktop.

Task	Location	Options
View information	**Settings** > **Devices** > **Connection**	Your connected USB devices are displayed in a list. To view detailed information about any attached USB device, including its VID, PID, and status, expand its row in the table. You can also set each device's connection type.

Setting Connection Types

For each device, you can choose whether the device should be sent using an *optimized* connection, a *standard* connection, or not to forward the device at all. *Options will only be shown if they are available for the device*.

- **LAN Connect** *(Also referred to as "bridged")*: The device signal is sent to the remote session for processing by installed drivers there. Because the device signal must complete a round trip to the remote host and back before the screen is updated, this method is more susceptible to network latency, and is not as responsive as *tablet performance* mode; however, it will support a broader range of device features.

- **Tablet Performance** *(Also referred to as "Local termination")*: Preprocess the device signal locally at the Trusted Zero Client before sending it to the remote session. When available, this mode provides greatly improved responsiveness and better tolerance for high-latency networks. Some advanced features may not be available using this mode.

- **Universal**: Locally process simple input devices (keyboards, mice, and pointers, also known as KMP devices).

Network

Network Information

You can view detailed information about the networks your Trusted Zero Client is connected to, including the type of connection, speed, and IPv4/IPv6 addresses.

Task	Location	Options
View Network information	**Settings**>**Network**	Your connected networks are displayed in a list. To view more information for any network, click to expand its detail content.

Logs

The Trusted Zero Client collects logs that record information about its state, connection progress,session information, and user-initiated actions. Log verbosity can be adjusted for specific use cases; for example, when troubleshooting issues, our support team may ask you to set the log level to a higher value to capture more diagnostic information. You can also reduce the log level to collect fewer messages and use less storage space.

Task	Location	Options
Set Log Level	**Settings**>**Logs**>**Log Level**	Select your desired log level from the dropdown list. Available values are: • **0**: Critical system messages only • **1**: Error messages and critical system messages • **2**: Informational messages, including error and critical messages. This is the default setting. • **3**: Debug mode, which collects all of the above messages and also much more detailed diagnostic information intended for troubleshooting.
View Log File	**Settings**>**Logs**>**View Log File**	Click **View Log File** to open the device's log file in a log viewer, allowing you to search and filter log entries.

Advanced

The settings in this section can fundamentally alter the way the Trusted Zero Client device operates. You should only change these settings if you understand the implications of your changes.

Task	Location	Options
Perform a factory reset	**Settings>Advanced>Reset**	To perform a factory reset on this device, click the **Reset** button. All configuration and permission values will be reset to defaults. **The device will be unregistered from its Anyware Trust Center**, and you must register the device again. This is the only way to move a device from one Anyware Trust Center to another.
Set the Security Mode	**Settings>Advanced>Security Modes**	Select a connection from the dropdown list, then choose a security mode to assign to the connection. You can assign a mode to all connections at once by selecting *All connections*, or assign separate modes to individual connections by choosing them from the list. Available options are: • **Low**: Does not verify server identity certificates; all connections are enabled. • **Medium** (default): If the certificate cannot be verified, a warning may be displayed before connecting. • **High**: Connections will fail if the server certificate cannot be verified.
See the Trust Center's address	**Settings>Advanced>Trust Center**	View the Anyware Trust Center's address. The address provided must be reachable by the Trusted Zero Client device. The Trusted Zero Client uses this address for all transactions with the Anyware Trust Center, including device registration.

Tera2 PCoIP Zero Client Notes

If you are an existing Tera2 Zero Client user, or have prior experience using the Tera2 devices, this page will highlight some of the more important differences between the two.

Device Management

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
Device Administration	*Management Console* application	Third-party endpoint management software	The endpoint management software application connects to the Anyware Trust Center, which sets policies and enforces control on your deployment endpoints.
Firmware updates	Firmware builds are downloaded from the website and then uploaded to the device (or pushed from MC)	Updates are automatically downloaded to the trust center, which pushes updates to Trusted Zero Client devices when convenient for IT administrators.	The Anyware Trust Center is required for Trusted Zero Client software updates .
Initial Setup	The initial setup of a Tera2 device includes setting audio, network configuration (DHCP or IP address/subnet/gateway), and session type (managed by PCoIP Management Console or not, as documented here.	• Set Language • Set FQDN for Trust center • Connect to session	The Anyware Trust Center must be installed BEFORE setting up the first Trusted Zero Client.
On-Screen Display (OSD)		(limited)	Limited configuration options are available from the Trusted Zero Client in the pre-session UI. The available options can be further restricted by IT administrator via the Trust Center.
Web Interface (AWI)	(if enabled)	—	There is no web interface available for the Trusted Zero Client. Device configuration is set in the Anyware Trust Center.
Device configuration	Via Management Console, AWI (if enabled), or OSD	Via Trust Center or Pre-session UI.	IT administrators can override, restrict, or disable settings via the Trust Center. _The Trusted Zero Client has no AWI; administrators control settings via the

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
			Anyware Trust Center using their provider's management tool.
Certificate issuance	SCEP server path set via MC or via AWI	Trust Center maintains certs for broker and operational certs. 802.1x support coming in a future release.	The customer CA can be set on the Anyware Trust Center. Once set, the Anyware Trust Center then controls certificate issuance.
Device name	Can be changed on the Zero Client	Device name is the host name from the network (via DHCP), and cannot be changed.	

Connections

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
HP Anyware desktops			
Amazon WorkSpaces			
VMware Horizon View		(beta)	Full support expected in 2H 2023
Connection Management			Connections can be added, removed, and edited from both the device and the Anyware Trust Center.

Session Debugging and Analytics

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
Log streaming/ aggregation			Currently Anyware Trust Center only
Local log viewer			
Log retrieval	From AWI, limited from OSD	Push/pull between Anyware Trust Center and Trusted Zero Client	
Packet capture		—	
Health monitor	—		Health monitor also checks the connection to the Anyware Trust Center

Session Feature Support

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
Smartcard support			Limited support
Quad displays		(hardware dependent)	Display order cannot be changed (local display 1=1, 2=2, 3=3, 4=4)
Auto-discovery			Trusted Zero Clients will automatically register with Anyware Trust Centers on LANs with DNS
Device Policies	(Limited)		Desired properties can be set on the Trusted Zero Clients, so that every element of the UI can be controlled by the Trust Center. Users can be blocked from adjusting settings.
USB Authorization			Trusted Zero Clients can be configured to allow or deny USB devices by VID/PID or by Class/Subclass.
Automated backup and restore systems			If a Trusted Zero Client detects a problem during boot, it will automatically roll back to the last working firmware version.
Darksite Support		Early 2024	
Zero Trust for Device	—		
PCoIP Ultra	—		
USB 3.x / USB C	—		Depending on hardware selection.
Webcam Support			
Wacom		(Limited)	Improved support targeted for late 2023.
Secure Boot	—		
Encrypted Storage	—		
TPM backed Certificates	—		
Internationalization			Currently, only the Trusted Zero Client pre-session UI is localized; broker messages and in-session menus are not localized.
Monitor Topology Settings	(Limited)	Late 2023	
FIPS	140-2	140-3 ready in early 2024	

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
Wifi	—	Late 2024	
Bloomberg 4 Keyboards			
Bloomberg 5 Keyboards		(Limited)	Dual audio is not supported.
WWAN (5G)	—	Future development	
Bluetooth	—	Future development	
Touch Monitor			
Impravata		—	
Static IPs		Early 2024	
Audio Device Configuration		Late 2023	
Dark mode	—	Future development	

Support

If you encounter a problem setting up or using the Trusted Zero Client, there are a number of troubleshooting and support resources you can access.

- We maintain an extensive **knowledge base** which answers many questions and documents solutions to common problems. The knowledge base is part of the [Knowledge Center](#); click on the *Articles* tab to access it, or enter a search query in the search field at the top of the page.

- We host a **community forum**, allowing you to ask questions and get answers from other IT professionals and our support team, which monitors this channel. The forum is part of the [Knowledge Center](#); click on the *Discussions* tab to access it.

- If you need more help, open a [support ticket](#) and our support team will engage with you directly.

Logs

The Trusted Zero Client and its related components, including the Trust Center and the PCoIP agent, write log files that document processes and interactions with other services. These files are invaluable in diagnosing problems.

Logs affecting the Trusted Zero Client can be viewed and filtered using the log viewer in the [settings dialog](#). Logs can only be viewed outside of a PCoIP session.

Log Levels

The Trusted Zero Client logs can be tuned to record only major events, or highly verbose records used to debug problems. For more information about log levels and how to set them, see [Logs](#) in the settings section.