Trusted Zero Client Administrators' Guide

25.03

Table of Contents

Anyware Trusted Zero Client Administrators' Guide 6

- Device Management 6

What's New in This Release 7

- Support for Multiple Audio Output Devices 7
- Support for Imprivata Authentication 7
- SIPR/NIPR Network Migration 7
- Introducing Zoom VDI for HP Anyware 8
- Support for Wi-Fi Networks 8
- Support for Xencelabs Pen Displays 8
- Other Update 9

Requirements 10

- About Provisioning 10
- About Registration 11

Setting up the Trusted Zero Client 12

- Set Your Interface Language 12
- Validate Network Settings 13
- Register With Your Anyware Trust Center 13

Updating the Trusted Zero Client 15

Moving a Device to a New Anyware Trust Center 16

Connecting 17

- Connecting to a Remote Host 17
  - Creating Your First Connection 17
  - Creating a New Connection 18
  - Connecting to a Session 20
  - Connecting to Amazon WorkSpaces 24
  - Connecting to Omnissa Horizon 24

- Using a Smart Card to Authenticate a Session 25
  - Prerequisites 25
  - Connecting Using a Smart Card 25
- Automatically Connecting to a Session 31
  - Notes 31
- Connecting to a Session in Kiosk Mode 34
  - Notes 34
- Connecting to Omnissa Horizon Hosts Using Proximity Cards 36
  - Compatibility Information 36
  - rf IDEAS Cards and Readers 37
  - Adding an Imprivata OneSign Server Connection 37
  - Authenticating a Connection Using Proximity Cards 38
- Customizing the Login Experience 42
- Managing Connections and Desktops 44
  - Managing Connections 44
  - Managing Desktops 44
- Disconnecting from a Remote Host 48

In-Session Actions 49

- Connecting USB Devices 49
  - Important considerations 49
  - Connecting a USB Device 49
  - Disconnecting a USB Device 50
  - Connect USB Webcams 50
- Sending Ctrl+Alt+Del 52
- Selecting Audio Devices in Session 53
  - Before You Begin 53
  - Disconnection Behavior 54

Features 55

Audio 55

Enhanced A/V Sync 55

Multiple Audio Device Support 56

Connection Health Indicator 57

Pre-Session Health Indicator 57

In-Session Health Indicator 57

Display Support 61

Detect Monitors 61

Support for Moving Devices Between SIPR/NIPR & Insecure Networks 63

Migrating Networks 63

USB 64

USB Support 64

Wacom Tablets 65

Webcam Support 73

Supported Xencelabs Pen Displays 75

Media Optimization 76

Media Optimization for Microsoft Teams and Zoom 76

Media Optimization for Teams 79

Media Optimization for Zoom 82

Trusted Client Settings 86

General Settings 86

Date and Time Settings 86

Language Settings 87

Client Version Information 87

Devices 87

USB 88

Displays 89

Sound 91

- Connections 91
- Network 91
  - Network Information 91
  - Wi-Fi Network 92
- Logs 92
- Advanced 94

Tera2 PCoIP Zero Client Notes 95
- Device Management 96
- Connections 98
- Session Debugging and Analytics 99
- Session Feature Support 100

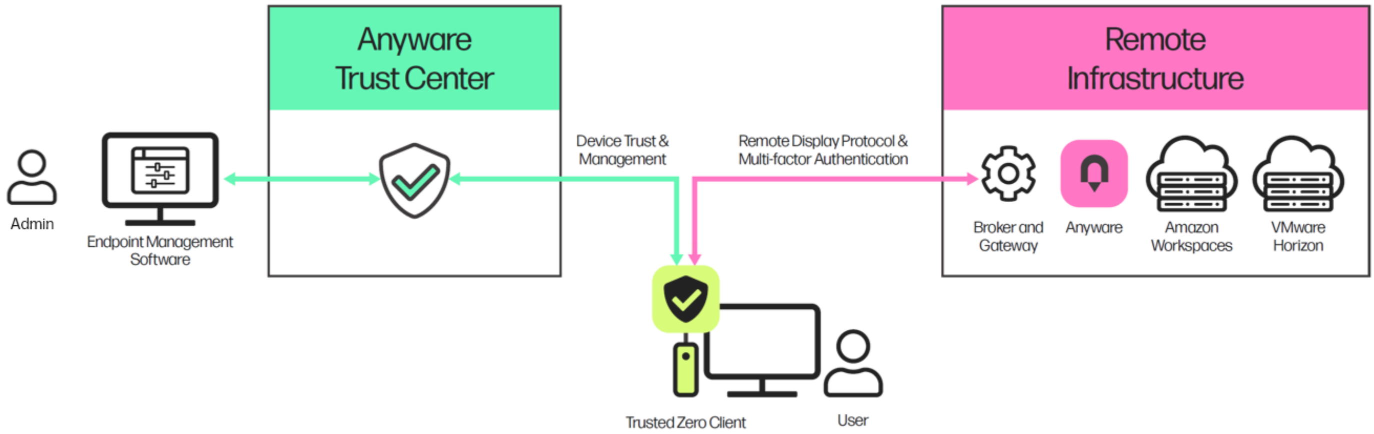
Support 103
- Logs 103
  - Log Levels 104
- Creating a Support Request 104
- Saving the Support Bundle to a Peripheral Device 104

Anyware Trusted Zero Client Administrators' Guide

The **Trusted Zero Client** is HP's next-generation standalone Anyware Client, securely connecting users to their HP Anyware remote desktops, as well as Amazon WorkSpaces and Omnissa Horizon View using the PCoIP and Blast protocols (support for Omnissa Horizon). 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.

What's New in This Release

Release 25.03 of the Trusted Zero Client contains bug fixes and stability enhancements. Additionally, it also includes the following new features:

Support for Multiple Audio Output Devices

Version 25.03 of the Trusted Zero Client introduces support for multiple audio output devices on the client side. You can now select **multiple audio output devices** for playing audio, in addition to a single audio input device while in session.

This capability is only supported on Linux clients and Trusted Zero Clients connecting to Windows Graphics agents or Windows Standard agents. For more information, see Selecting Multiple Audio Devices.

Support for Imprivata Authentication

Trusted Zero Client version 25.03 supports authentication of connections to Horizon hosts using Imprivata OneSign Single Sign-On. Imprivata OneSign enables users to access corporate networks, desktops, and applications with a single sign on. This reduces the need for maintaining separate passwords and prevents unauthorized access.

For more information, see Connecting Using Imprivata Authentication.

SIPR/NIPR Network Migration

In version 25.03, support has been added for securely migrating Trusted Zero Clients between SIPR, NIPR, and insecure networks. When re-commissioning a Trusted Zero Client for use on a SIPR/NIPR or insecure network, specific steps must be followed to completely erase all local data and configurations. This prevents accidental or malicious access to critical data during network migrations, and ensures compliance with security recommendations. A full set of instructions are available in Support for Moving Devices Between SIPR/NIPR & Insecure Networks.

Introducing Zoom VDI for HP Anyware

Version 25.03 of the Trusted Zero Client introduces support for Zoom VDI when connected to Windows Agents. The feature works the same as Omnissa Horizon Agents by offloading the audio and video streams from HP Anyware agent devices to HP Anyware client devices, which handle the processing and transmitting of these streams to and from Zoom servers. This results in reduced latency, and improved meeting experience during PCoIP sessions.

Once installed and configured on the Anyware Windows Agent, the capabilities of Zoom VDI enable quick adoption, leading to a seamless experience while starting and joining meetings. The Zoom VDI Plugin is similar to the Standard Zoom Client, and includes features such as optional end-to-end encryption, gallery view, speaker view, language interpretation, breakout rooms, and screen sharing. For more information, see Media Optimization for Zoom.

Support for Wi-Fi Networks

Trusted Zero Client can now connect to Wi-Fi Protected Access 2 (WPA2) networks using password authentication. This facilitates access from places where wired networks are unavailable, and permits the mobility of Trusted Zero Clients across networks. For the purpose of enabling Wi-Fi use, new menu options have been introduced in the client interface. These menu options are described in the Settings topic.

Support for Xencelabs Pen Displays

Version 25.03 of the Trusted Zero Client supports Xencelabs Pen Display 16 and Xencelabs Pen Display 24 while connecting to Windows Graphics or Standard agents. Support is available in the locally terminated mode, as well as the bridged mode. For more information, see Supported Xencelabs Pen Displays.

Info

This feature is currently in beta, and may be subject to future changes or may contain bugs.

Other Update

Previously, the Trusted Zero Client connected to Anyware Trust Center on TCP port 32443. Going ahead, it will connect on TCP port 443.

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 **443**.
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. See Create DNS Records for more information on the Trust Center address.

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 remote 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.

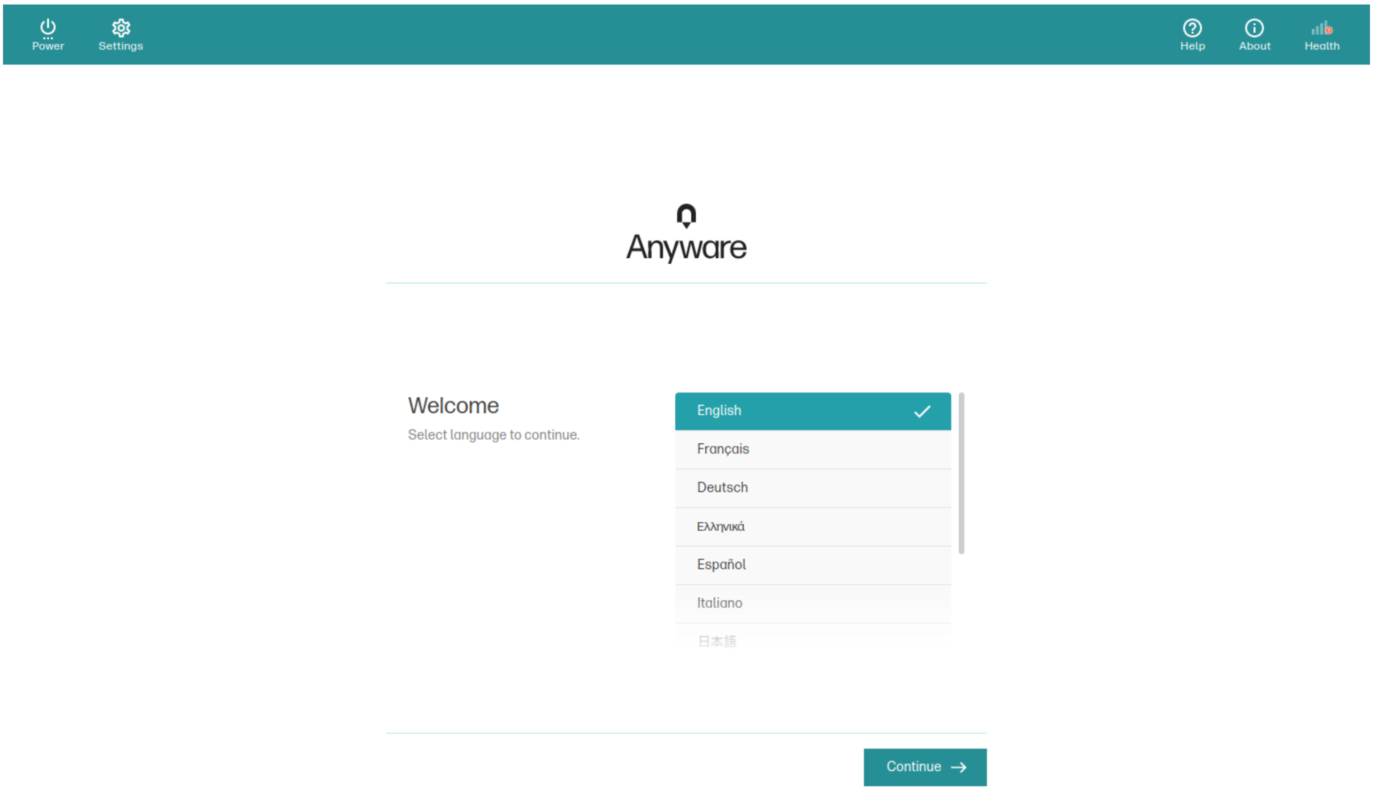
After registration, a Trusted Zero Client is bound to its Anyware Trust Center. If you need to re-register a Trusted Zero Client with a different Anyware Trust Center, you must factory reset the device.

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.



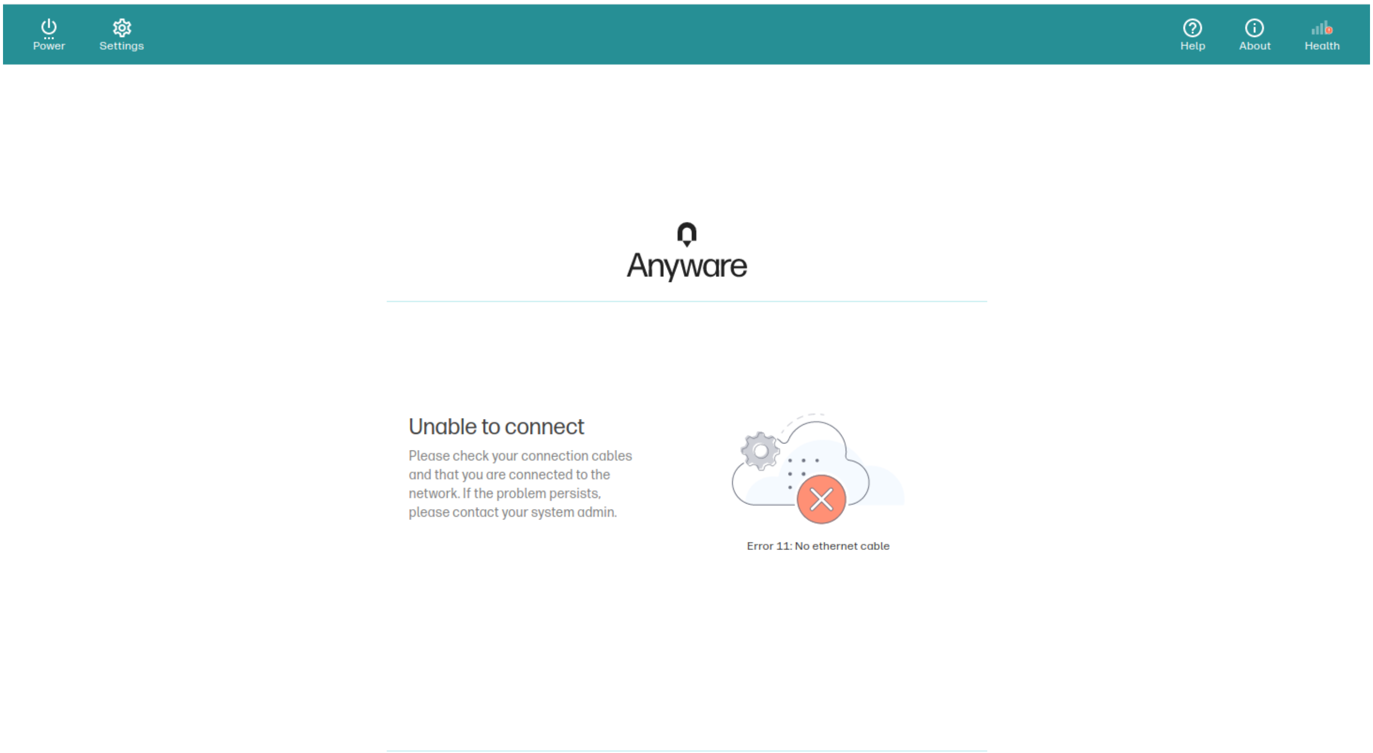
Welcome

Select language to continue.

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:



Unable to connect

Please check your connection cables and that you are connected to the network. If the problem persists, please contact your system admin.

Error 11: No ethernet cable

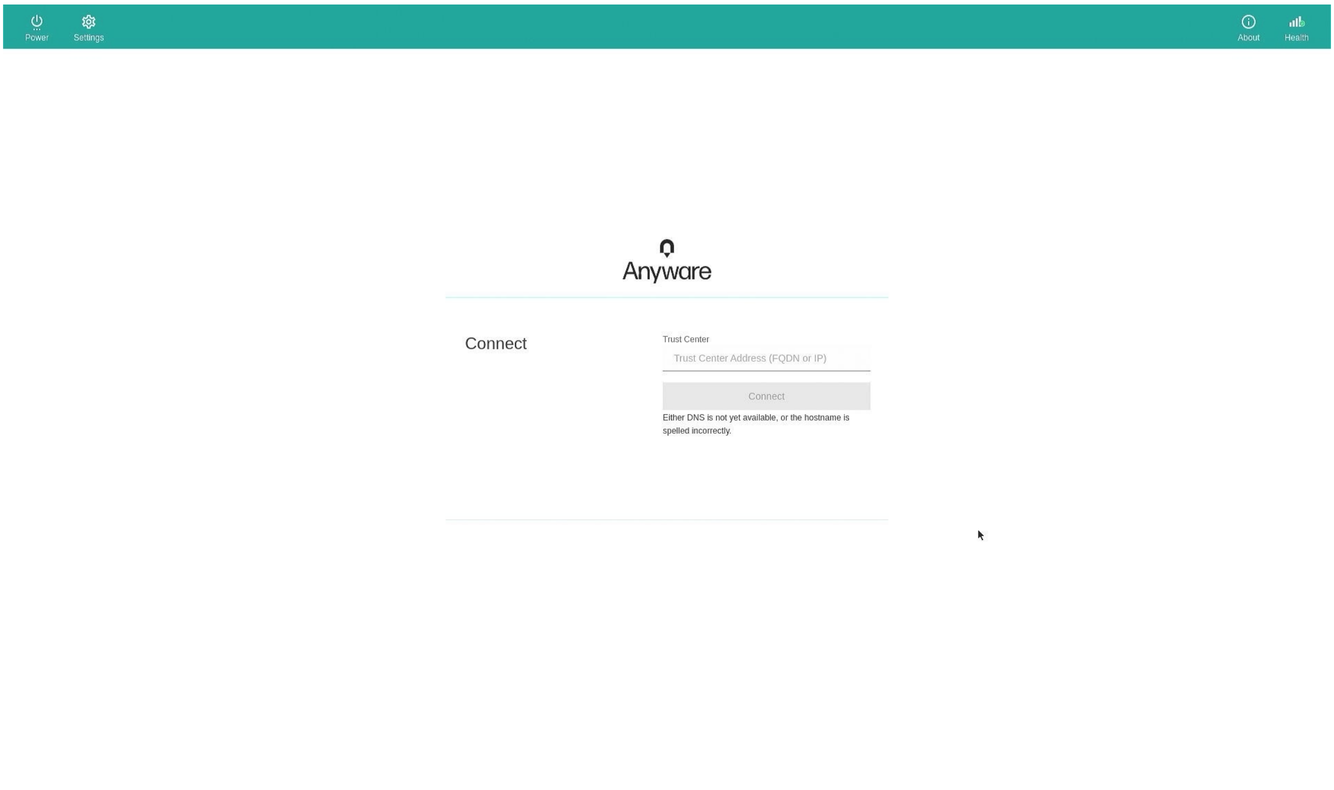
Register With Your Anyware Trust Center

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.

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**.



Either DNS is not yet available, or the hostname is spelled incorrectly.

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 Endpoint Management System to each Trusted Zero Client.

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

Moving a Device to a New Anyware Trust Center

To move your Trusted Zero Client to a new Trust Center, you must first disconnect it from its current Trust Center. To do this, perform a factory reset on the Trusted Zero Client, and then proceed to register with the new Trust Center.

1. Launch the Trusted Zero Client.
2. Perform a factory reset on this device:

    a. Go to **Settings** > **Advanced**.

    b. Click **Reset**.

    The device will be unregistered from its Anyware Trust Center, and you must register the device again.
3. Register with the new Trust Center.

Connecting

Connecting to a Remote Host

The Trusted Zero Client can connect to any Windows, Linux, or macOS host with an Anyware agent installed, as well as Amazon WorkSpaces desktops. Connections can be made directly (client direct to host), or brokered through Anyware Manager, an Anyware Connection Manager, or Omnissa Horizon using both PCoIP and Blast protocols.

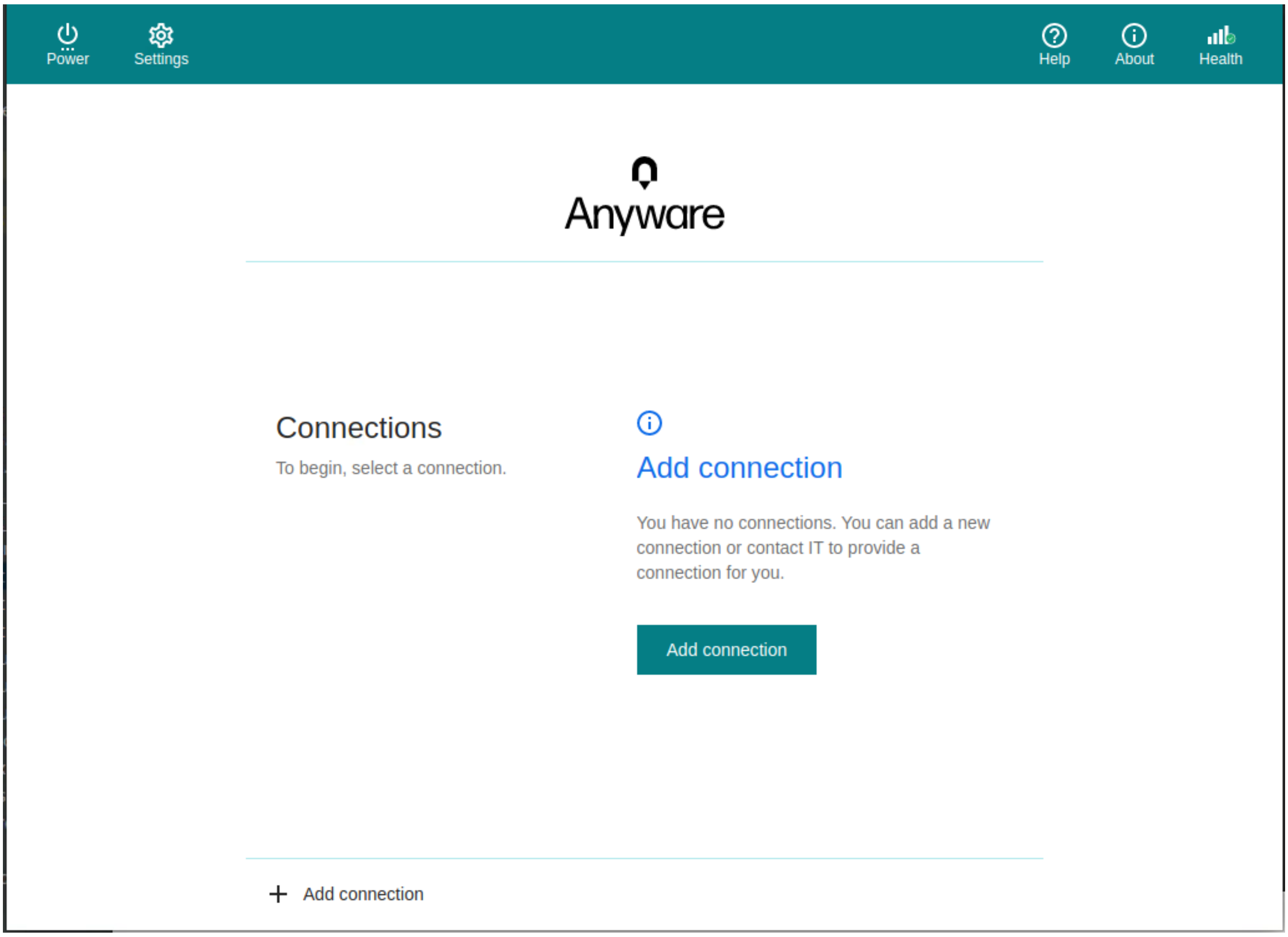
Creating Your First Connection

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:



Connections

To begin, select a connection.

Add connection

You have no connections. You can add a new connection or contact IT to provide a connection for you.

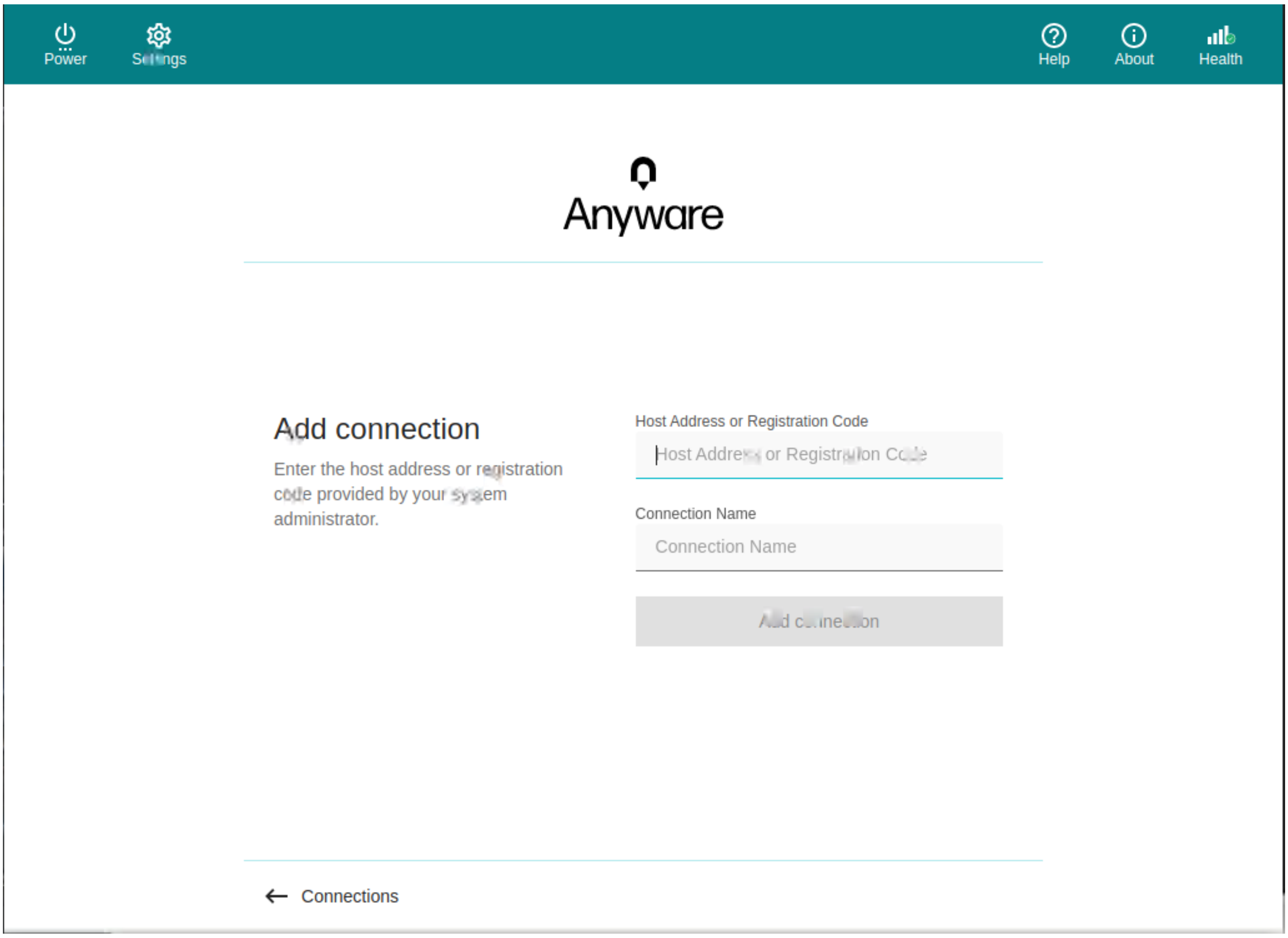
Click **Add a new connection**, and proceed to the next section.

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:



Add connection

Enter the host address or registration code provided by your system administrator.

Host Address or Registration Code

Host Address or Registration Code

Connection Name

Connection Name

- **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!@#`

  For Anyware connections using a connection broker (such as Anyware Manager or Leostream), this value will be the address (or FQDN) of the broker.

Note: Amazon WorkSpaces registration codes

If you are connecting to an Amazon WorkSpaces desktop, provide your WorkSpaces registration code in this field.

Note: Omnissa Horizon connections via PCoIP or Blast

To connect to a Omnissa Horizon broker, provide the address of the Horizon Connection Server in the *Host Address or Registration Code* field.

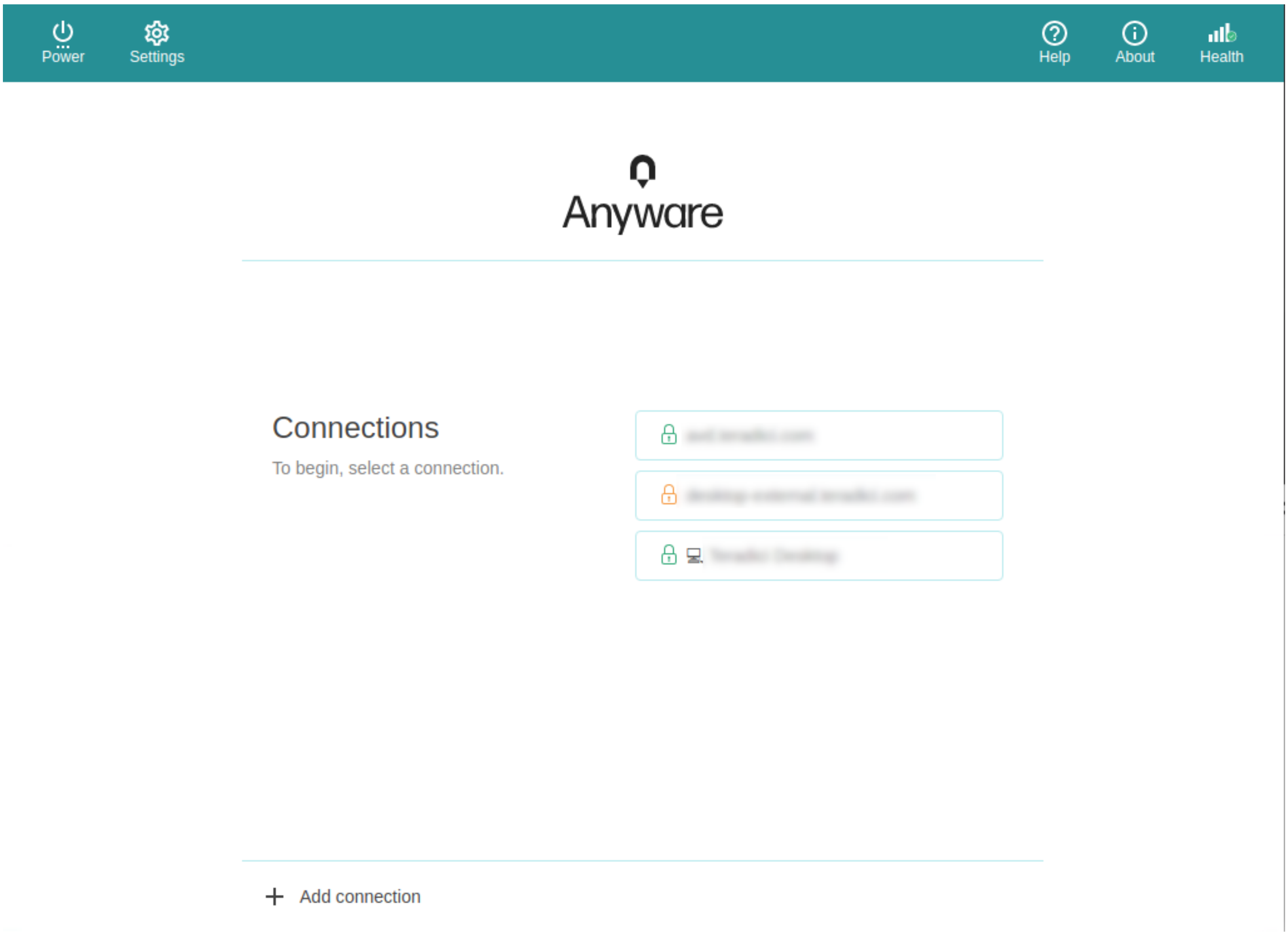
- **Connection Name** *(optional)*: If desired, provide a name for this connection. This can be anything; you will use this name to select this connection in future sessions. You can always change it later.

2. Click **Add connection**.

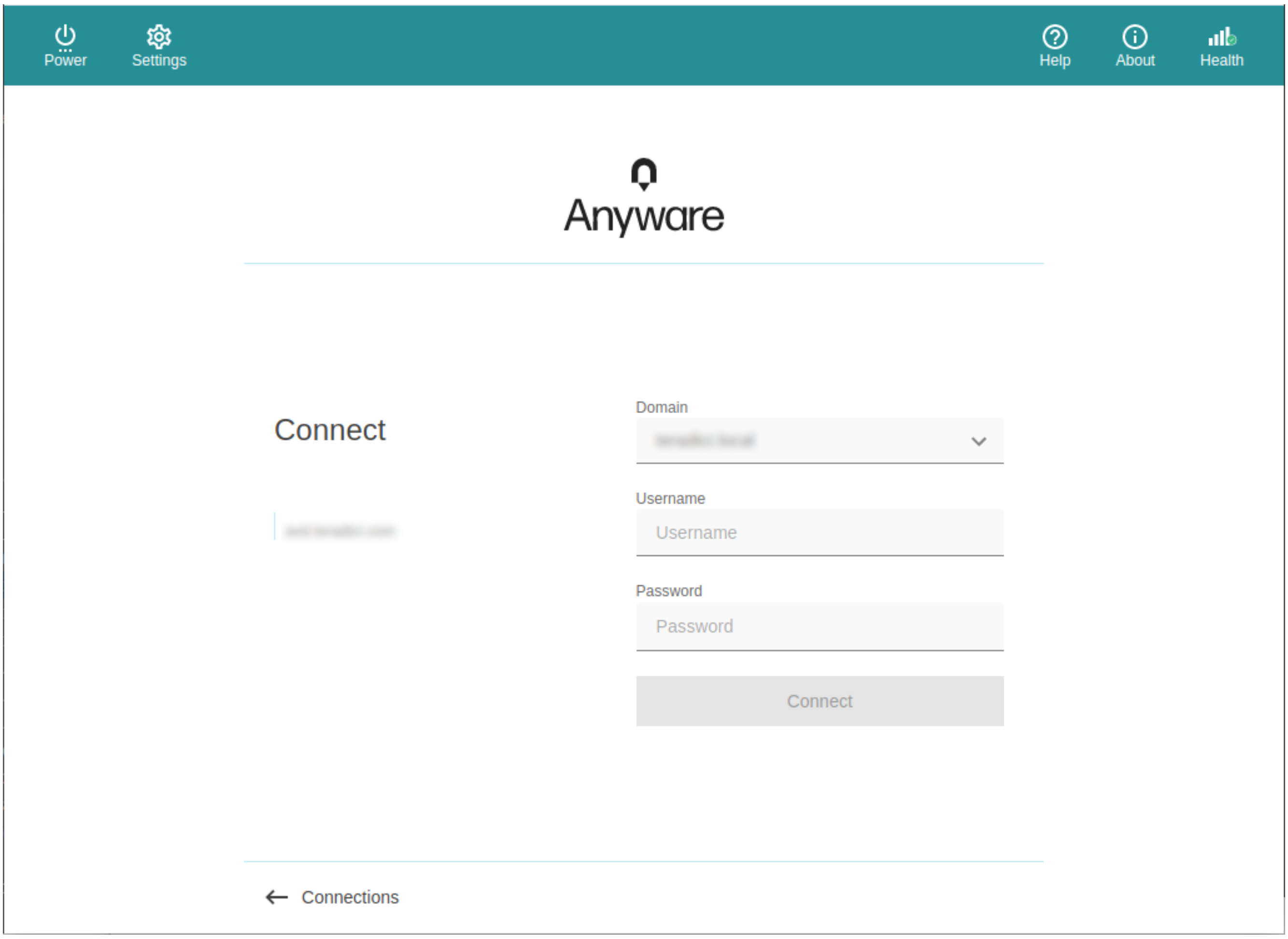
Once this is done, your connection will appear as a button in the desktop selection list.

Connecting to a Session

1. If you have created at least one connection, the Trusted Zero Client will now look something like this:

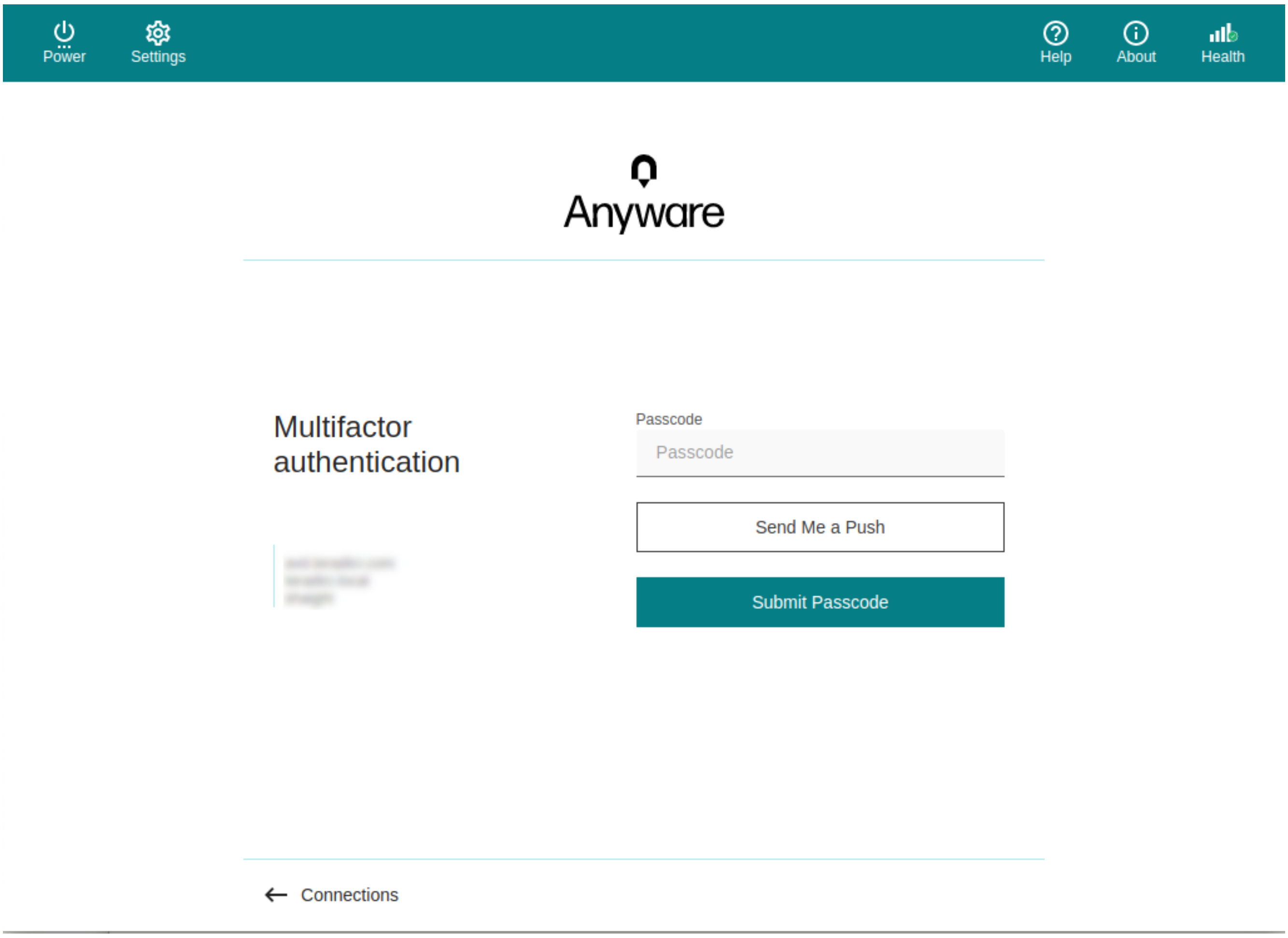


2. Click the name of the connection you want. Next, provide your username and password:



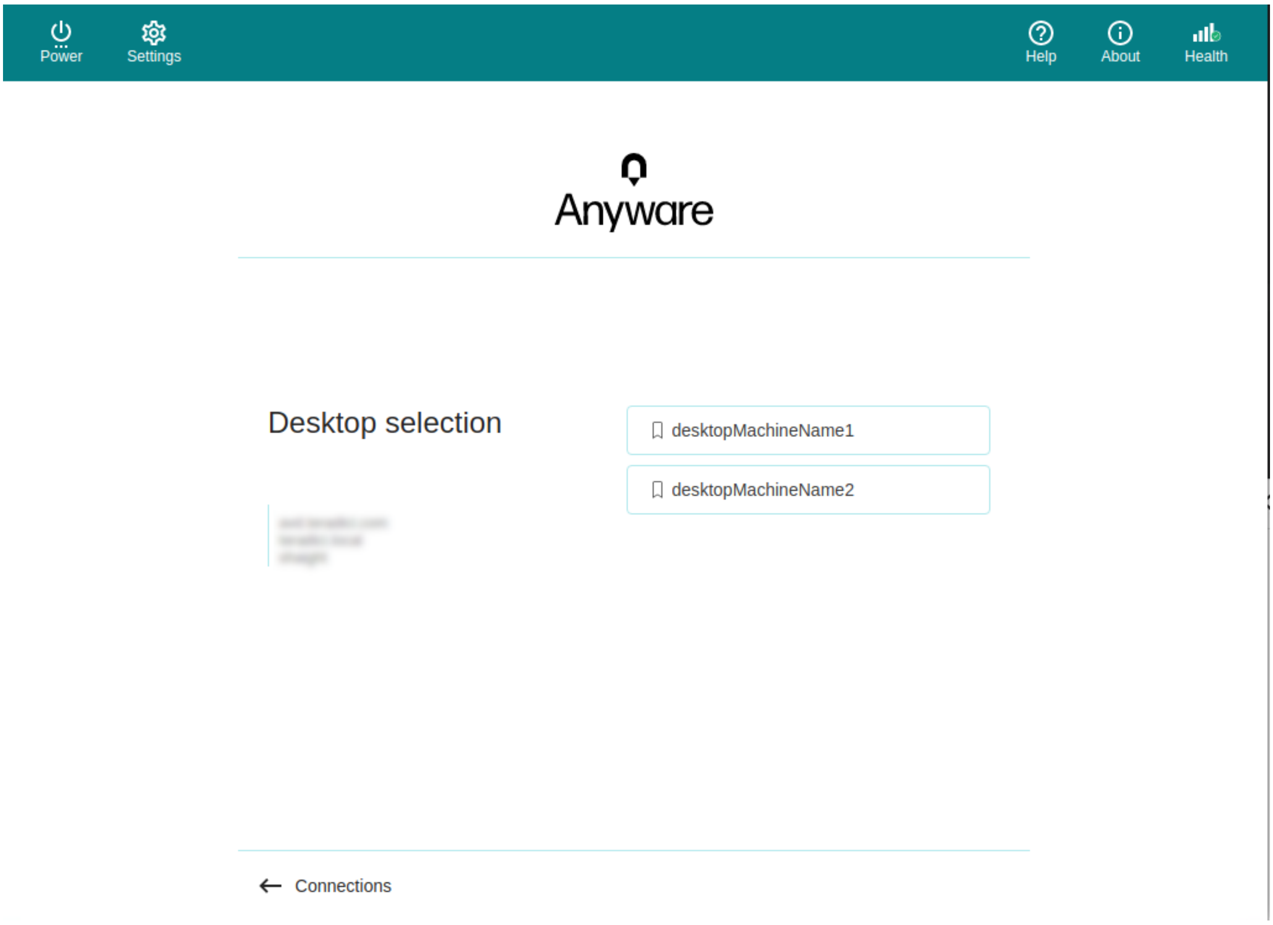
> ✎ **Note: About authentication credentials**
>
> For **managed connections**, the authentication screen and validation that happens here is provided by Anyware Manager or by your connection manager. The credentials are supplied to you by your system administrators, and are usually your corporate credentials.
>
> 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.



Desktop selection

desktopMachineName1

desktopMachineName2

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 remote 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.

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.

Connecting to Omnissa Horizon

Omnissa Horizon connections use the same process described above. Provide the address of your Horizon Connection Server in the *Host Address or Registration Code* field, and the Trusted Zero Client will recognize it and handle it appropriately. By default, the connection will be made using the Blast protocol.

Using a Smart Card to Authenticate a Session

The Trusted Zero Client supports pre-session smart card authentication when connecting to **Omnissa Horizon hosts**. Trusted Zero Clients can also read and process smart card information and allow SSO (single sign-on) authentication of the user prior to session establishment.

Prerequisites

- The following card/reader combination has been tested:
  - Identiv SCR3310
  - PIVKey C910

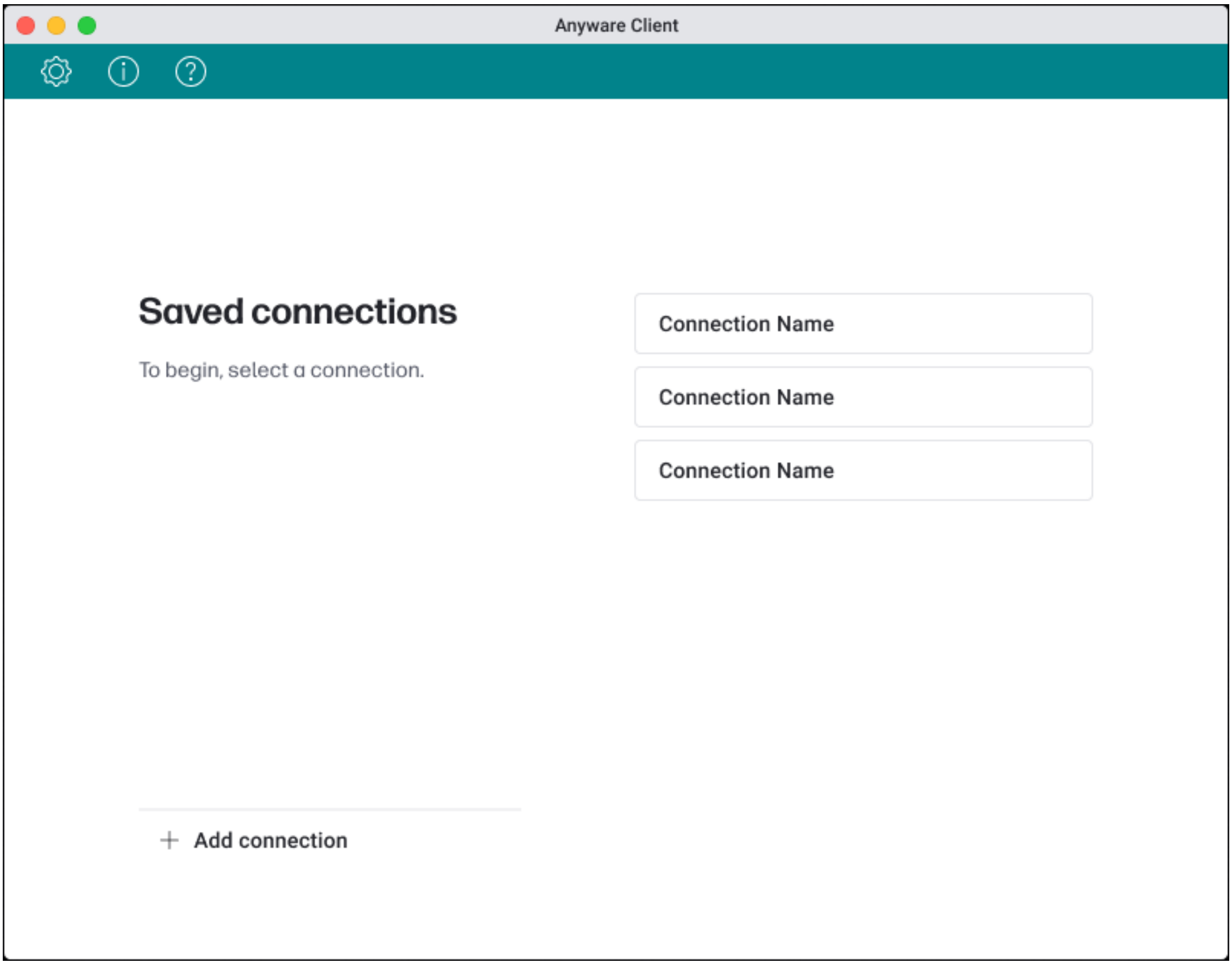
  Other CAC/ PIV cards are expected to work, but have not been tested.
- The client machine must be running Trusted Zero Client 24.03 or later.

Connecting Using a Smart Card

⚠ **Note: Concurrent Users Cannot Logon**

Concurrent users cannot log on to agent machines using the same smart card for authentication. Smart cards having multiple certificates allow only one user to log on at a time. To be able to log in, others users must wait until the current users logs off.

1. Attach the smart card reader to the Trusted Zero Client machine.
2. Launch the Trusted Zero Client.
3. On the **Saved Connections** window, select a connection.

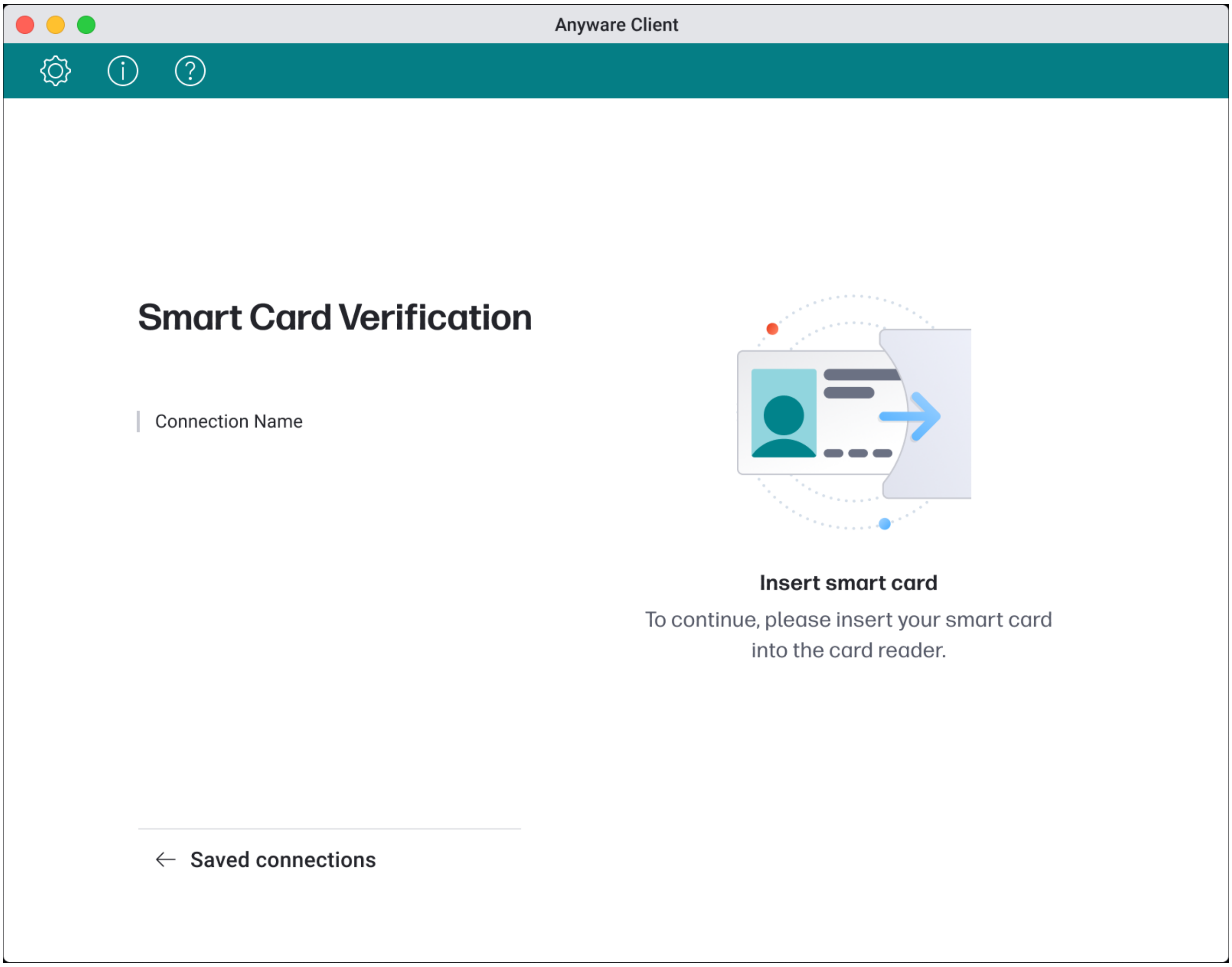


Anyware Client

Saved connections

To begin, select a connection.

4. When the **Smart Card Verification** window appears, insert your smart card and wait until it is verified.



Anyware Client

Smart Card Verification

Connection Name

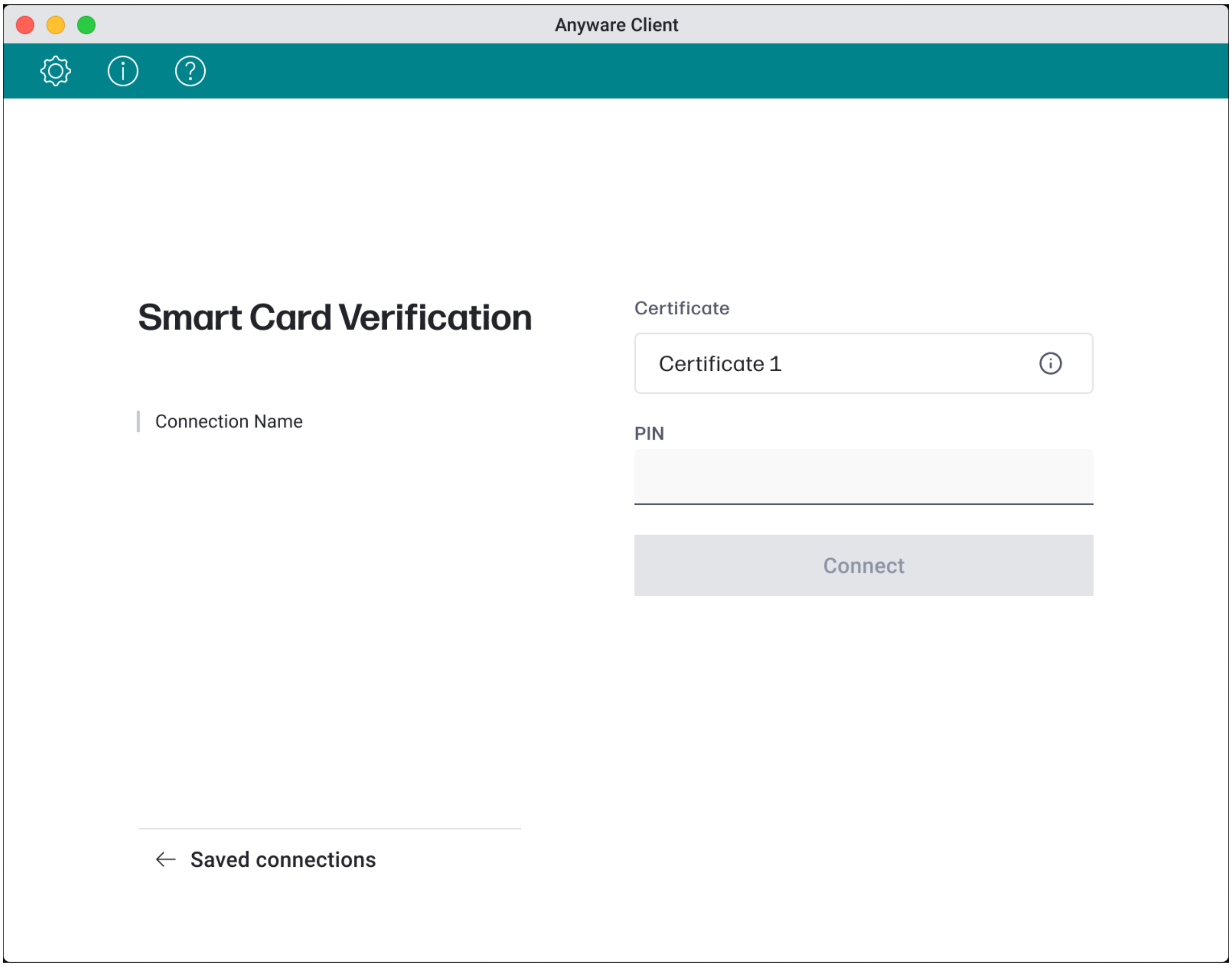
Insert smart card

To continue, please insert your smart card into the card reader.

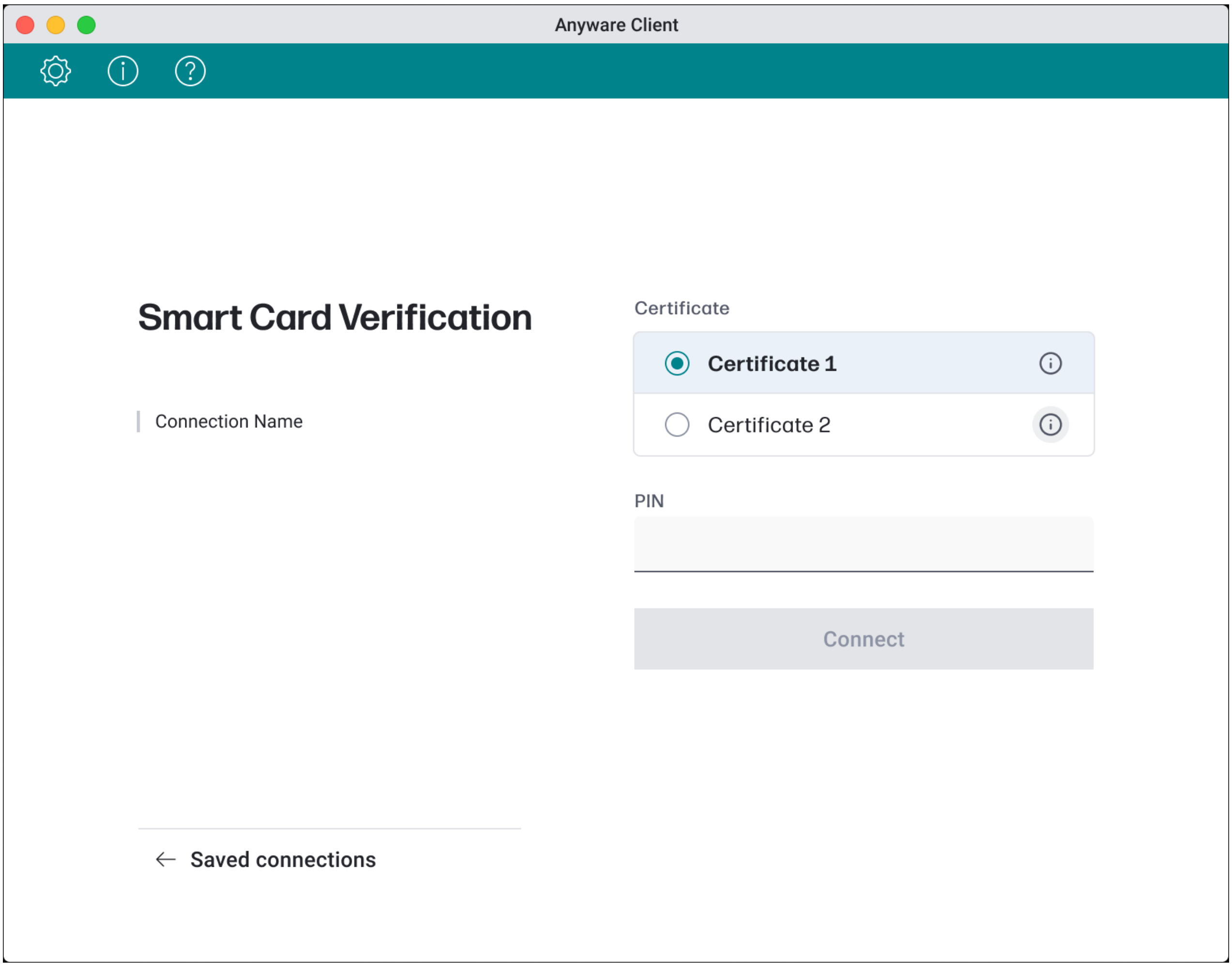
← Saved connections

5. Do one of the following:

   - If the client detects **only one certificate**, provide the smart card PIN and click **Connect** on the **Smart Card Verification** window.



- If the client detects **multiple certificates**, on the **Smart Card Verification** window, select a certificate, provide the smart card PIN, and click **Connect**.



Anyware Client

Smart Card Verification

Connection Name

Certificate

● Certificate 1

○ Certificate 2

PIN

Info

If an incorrect PIN is provided while using smart cards, information about the remaining number of attempts is displayed.

6. On the **Desktop Selection** window, select a desktop and connect to this session.

Note: Removing the Smart Card During Session

Removing the smart card while in session will end the session. However, the smart card will continue to be available on the client machine.

Viewing Certificate Information

You can view detailed information about each of the certificates detected by the client, such as certificate authority, certificate recipient, certification path, and certificate properties.

To view certificate information:

1. Launch the client, insert your smart card, and select a connection. Wait until it is verified.
2. From the available certificates, select the one for which you want to view details.

The following information related to the certificate is displayed on the **Certificate details** window:

- **Certificate information**: The purpose of this certificate.
- **Issued to**: The recipient of the certificate.
- **Issued by**: The certifying authority of the certificate.
- **Valid from**: The start date of the certificate's validity.
- **Valid to**: The end date of the certificate's validity.

Automatically Connecting to a Session

The Automatic Login feature enables you to bypass traditional login steps, and directly connect to your desktop without the need to provide your credentials. The ability to automatically login streamlines and simplifies the login experience.

You can connect to a session automatically, provided that Automatic Login has been enabled on the Trust Center.

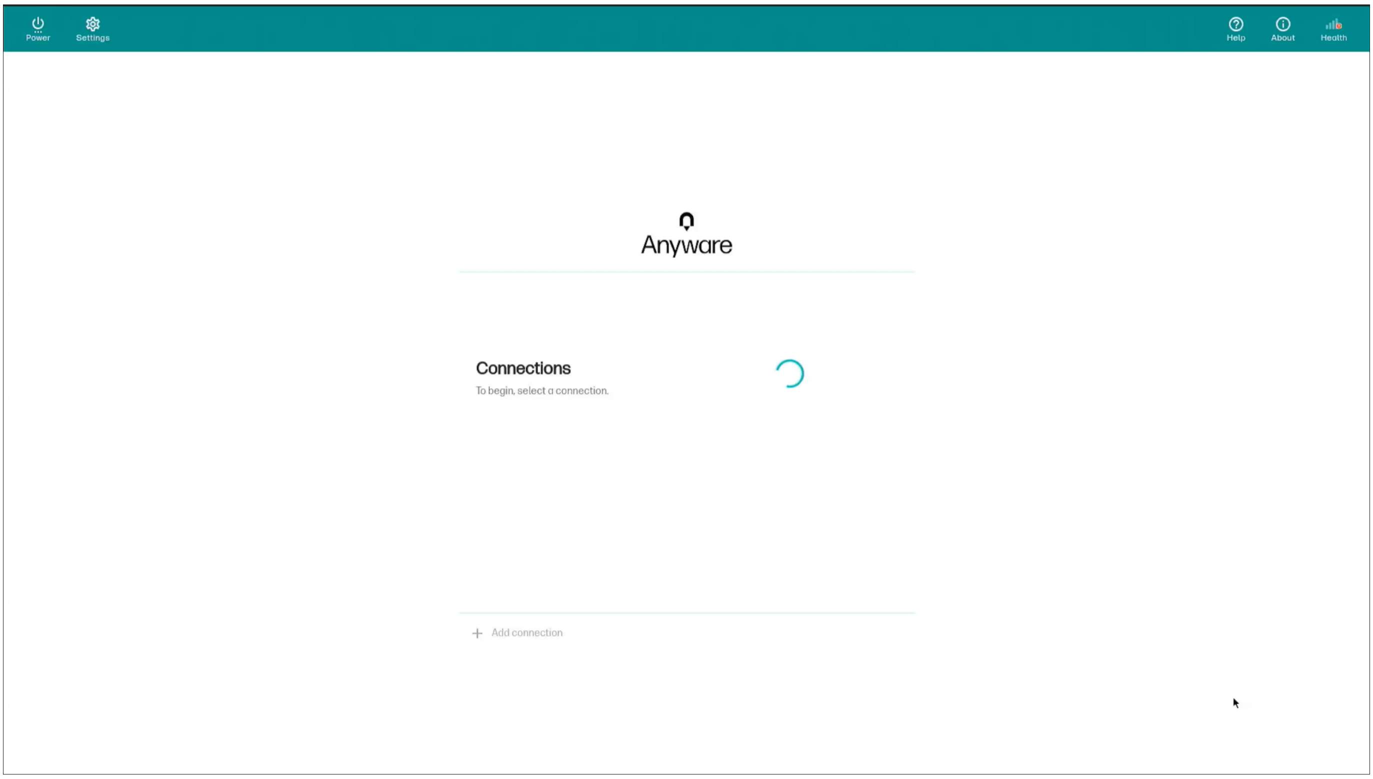
Notes

Automatic login works only if the following conditions are met:

- Only one broker is configured to connect to the host.
- Only one connection is available.
- Your credentials are current. If the username or the password have expired, you will be directed to the password change window.
- Only one desktop is configured for use. If multiple desktops are available, the **Desktop Selection** window opens, with a list of desktops from which you can select the desktop to connect to.

To connect automatically:

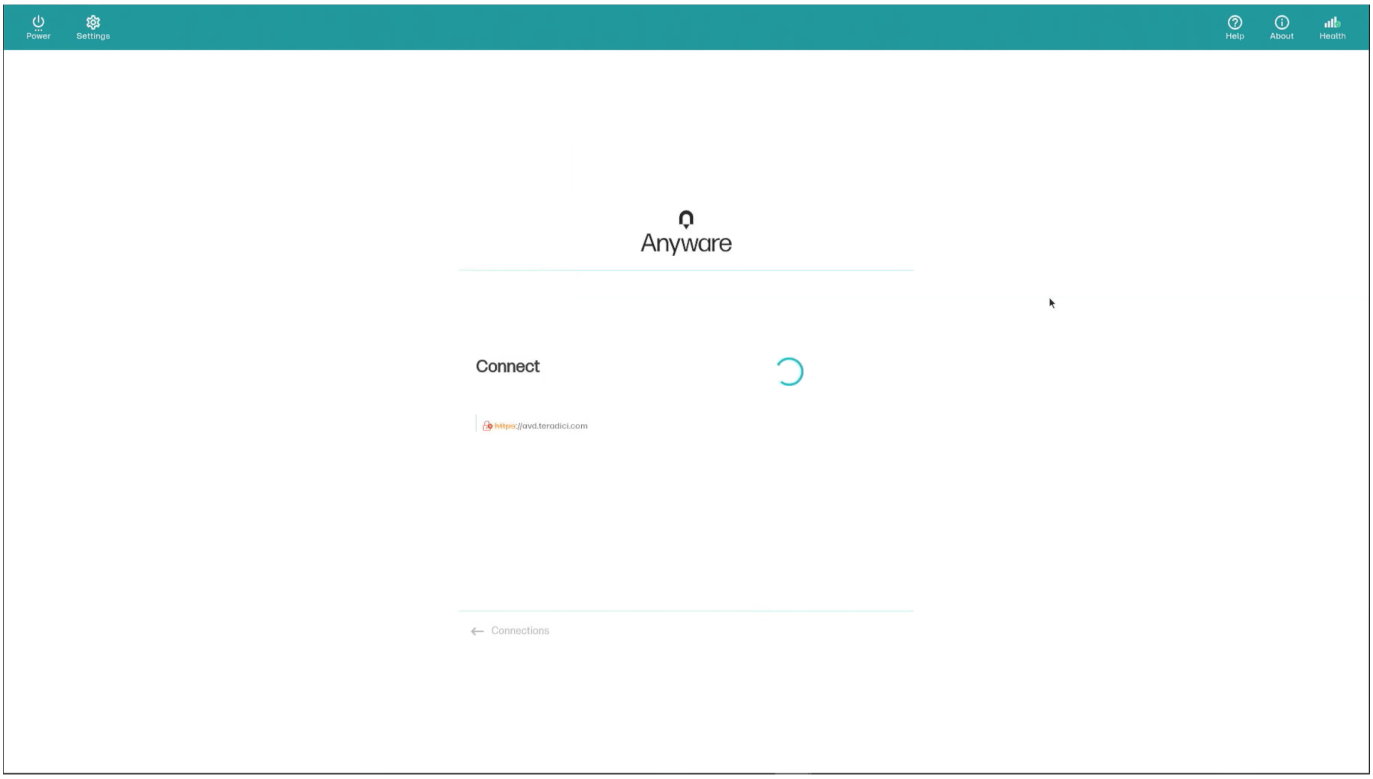
- Launch the Trusted Zero Client. The client will attempt to connect to the session, and will look like this:



Connections

To begin, select a connection.

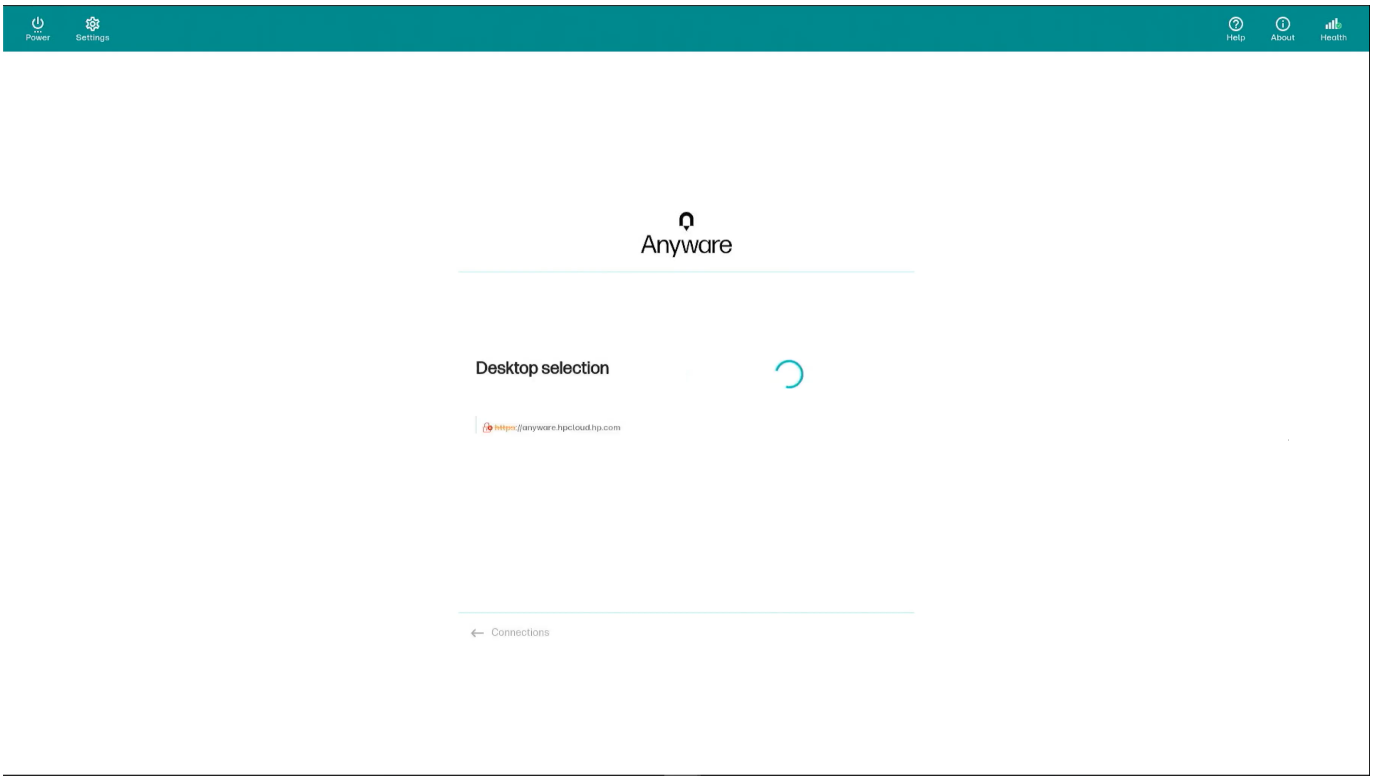
The client will attempt to login to the only connection available.



Connect

https://avd.teradici.com

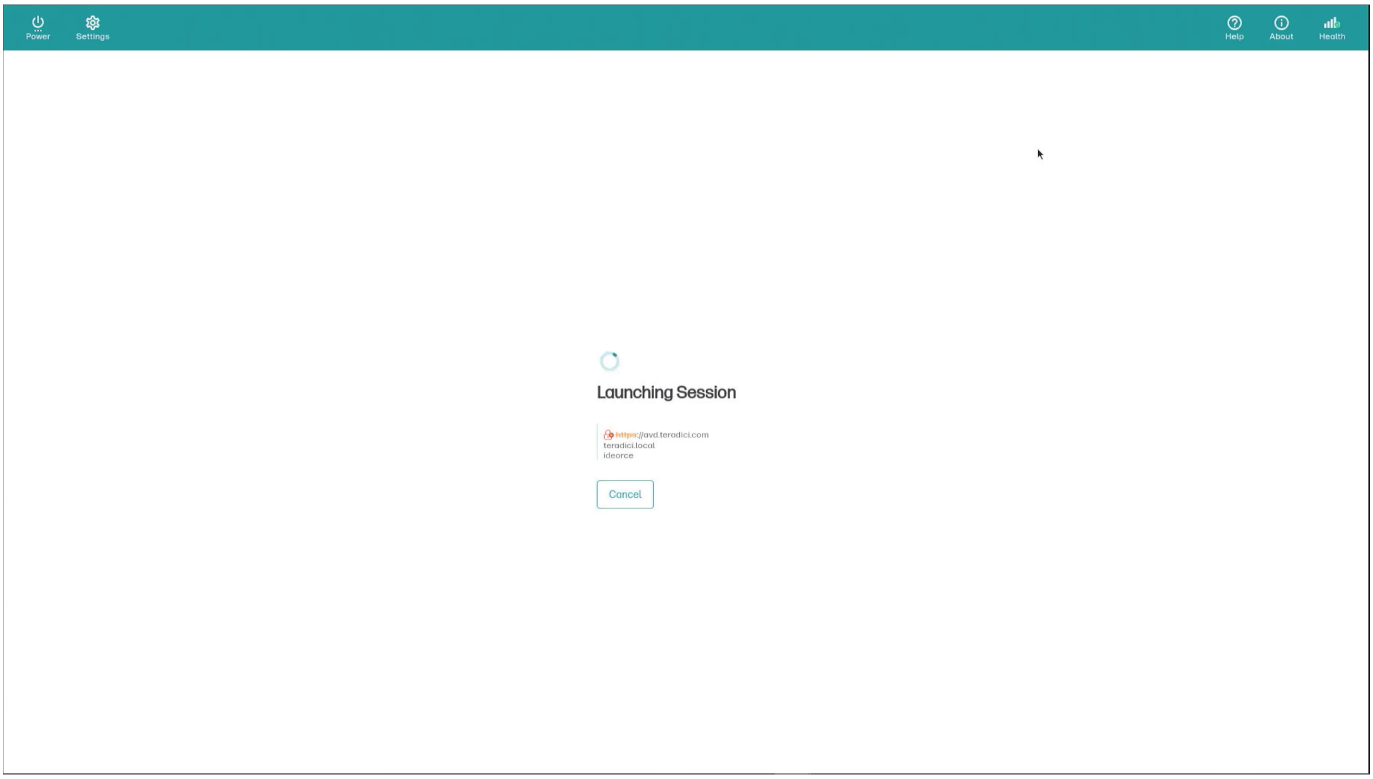
If the credentials (provided at the time of configuring the Trust center) are authenticated, the client will launch the desktop associated with this connection.



Desktop selection

~~https~~://anyware.hpcloud.hp.com

If the session launch is successful, you will see the following:



Launching Session

~~https~~://avd.teradici.com
teradici.local
ideorce

Connecting to a Session in Kiosk Mode

The Kiosk mode feature builds upon the existing Automatic login functionality, and allows for Trusted Zero Clients to connect to fixed purpose devices such as point-of-sale terminals and digital signs.

In the Kiosk Mode, you do not need to provide your Trusted Zero Client credentials. Launching the client will initiate the PCoIP session, and you will see a progress indicator. The ability to bypass traditional login steps ensures a seamless login process.

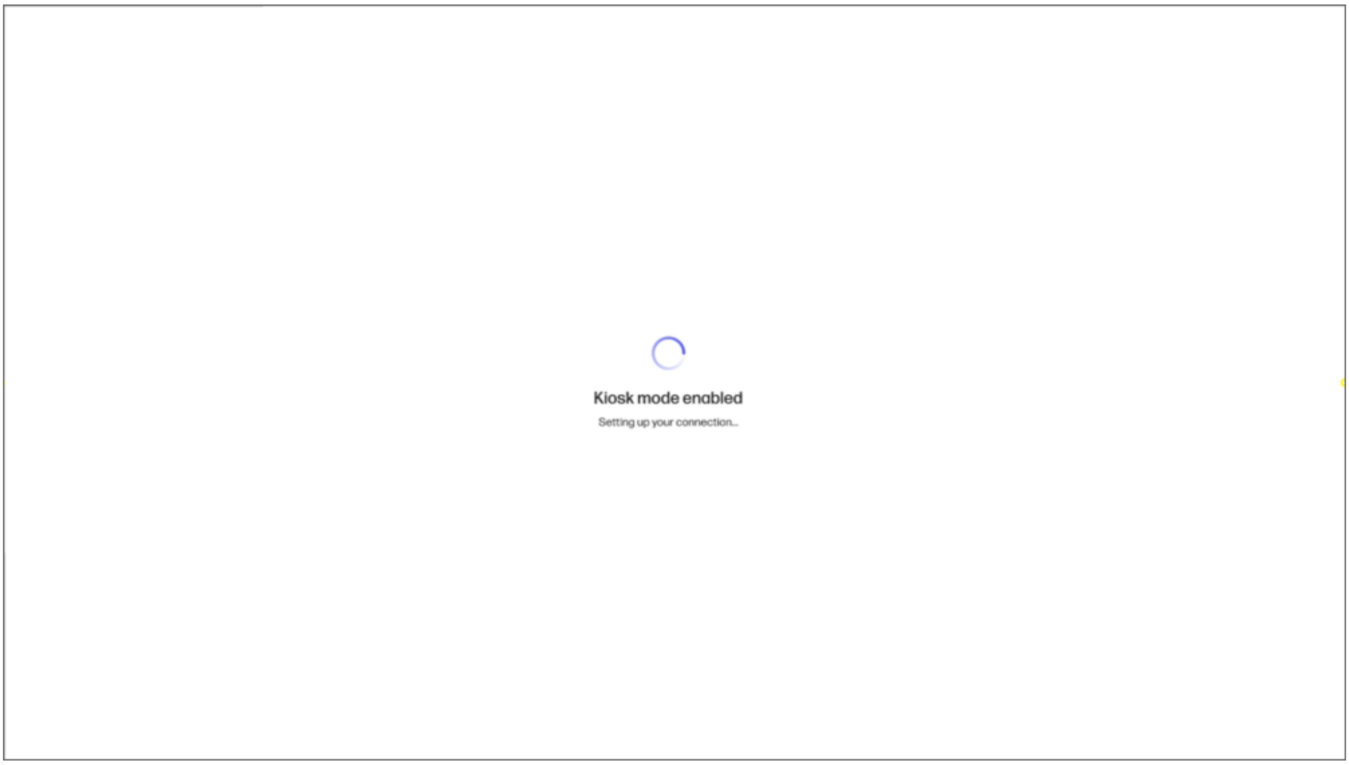
Notes

Kiosk Mode login works only if the following conditions are met:

- Only one broker is configured to connect to the host.
- Only one connection is available.
- Kiosk Mode is enabled from the Trust Center.
- Your credentials are current. If the username or the password have expired, you will be directed to the password change window.
- Only one desktop is configured for use. If multiple desktops are available, the **Desktop Selection** window opens, with a list of desktops from which you can select the desktop to connect to.

To connect using Kiosk mode:

- Launch the client. The client will attempt to connect to the session, and will look like this:



Kiosk mode enabled

Setting up your connection...

Next, the client will attempt to login to the only connection available. The following three scenarios are possible:

- If a network is not detected, you will see the following error message:

  No network detected *We can't find a connection to the internet. Please check your network settings, network cables and try again*.

  If the issue does not get resolved, get in touch with your system administrator.

- If your credentials cannot be validated, you will see the following error message:

  Unable to connect *We were not able to validate your username or password. Please ask your system admin to check they are correct and try again.*

  Get in touch with your system administrator to resolve this issue.

- If the client detects a network and your credentials are successfully validated, you will be connected to the remote host.

Connecting to Omnissa Horizon Hosts Using Proximity Cards

Imprivata OneSign enables users to access corporate networks, desktops, and applications with a single sign on. This reduces the need for maintaining separate passwords and prevents unauthorized access.

If Imprivata OneSign has been set up for your deployment, you can connect to Omnissa Horizon Hosts using the supported proximity cards.

Info

While Imprivata OneSign supports a range of authentication options, at present, only proximity cards are supported.

Compatibility Information

The following version of Imprivata OneSign has been tested:

- 24.1

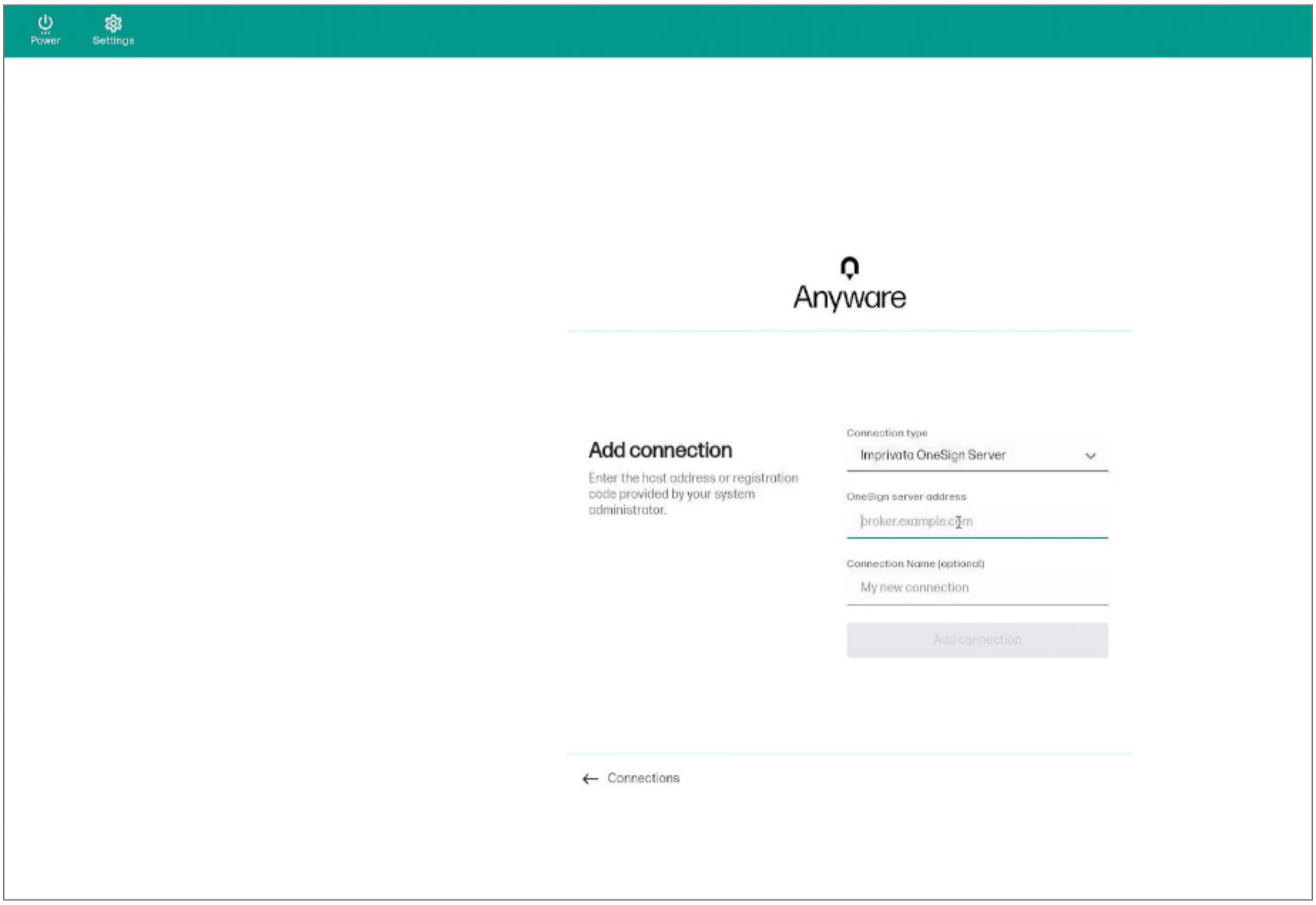
rf IDEAS Cards and Readers

This table lists the tested models of proximity card readers and cards.

Proximity Card Reader	Proximity Card
HDW-IMP-60	BDG1326
HDW-IMP-80-FIDO	—
HDW-IMP-75	• BDG-ISO-MIFARE-1K • BDG-2000 • BDG-5006
HDW-IMP-80-MINI-FIDO	—
RDR-80582AKU	• BDG-2000 • BDG-ISO-MIFARE-1K
RDR-7L82AKU	—
HDW-IMP-82-MINI	—

Adding an Imprivata OneSign Server Connection

1. Launch the Trusted Zero Client.
2. On the **Add connection** page, select **Imprivata OneSign Server** in the **Connection type** list.
3. Enter the OneSign server address.



Add connection

Enter the host address or registration code provided by your system administrator.

Connection type: Imprivata OneSign Server

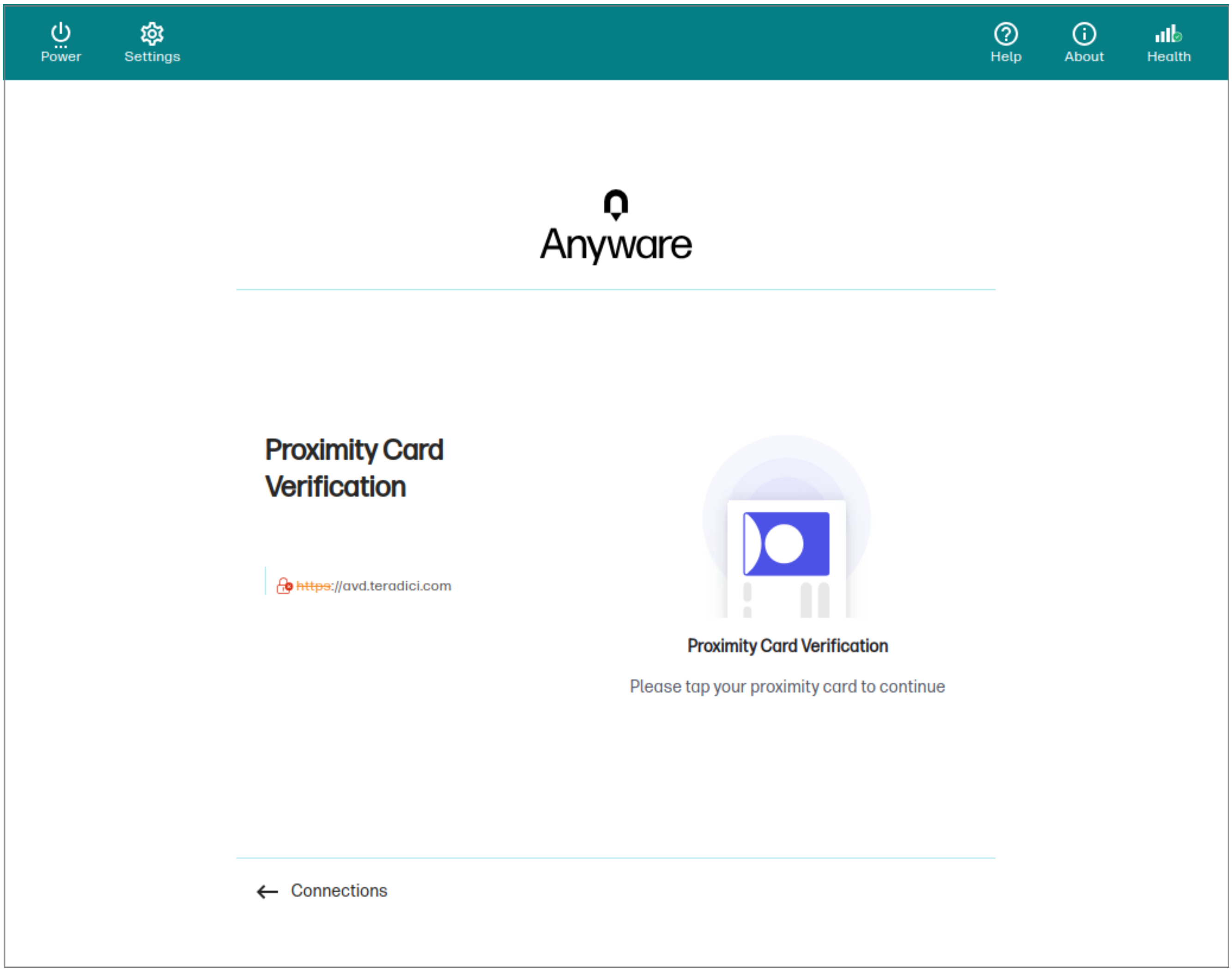
OneSign server address: broker.example.com

Connection Name (optional): My new connection

4. (Optional) Provide a connection name.
5. Click **Add connection**.

Authenticating a Connection Using Proximity Cards

1. Make sure that the card reader compatible with you proximity card is connected to the Trusted Zero Client machine.
2. Ensure that you have the correct proximity handy.
3. Launch the Trusted Zero Client.
4. On the **Connections** page, click the Imprivata connection you want to connect to.
5. When the **Proximity Card Verification** page appears, tap your proximity card on the card reader.



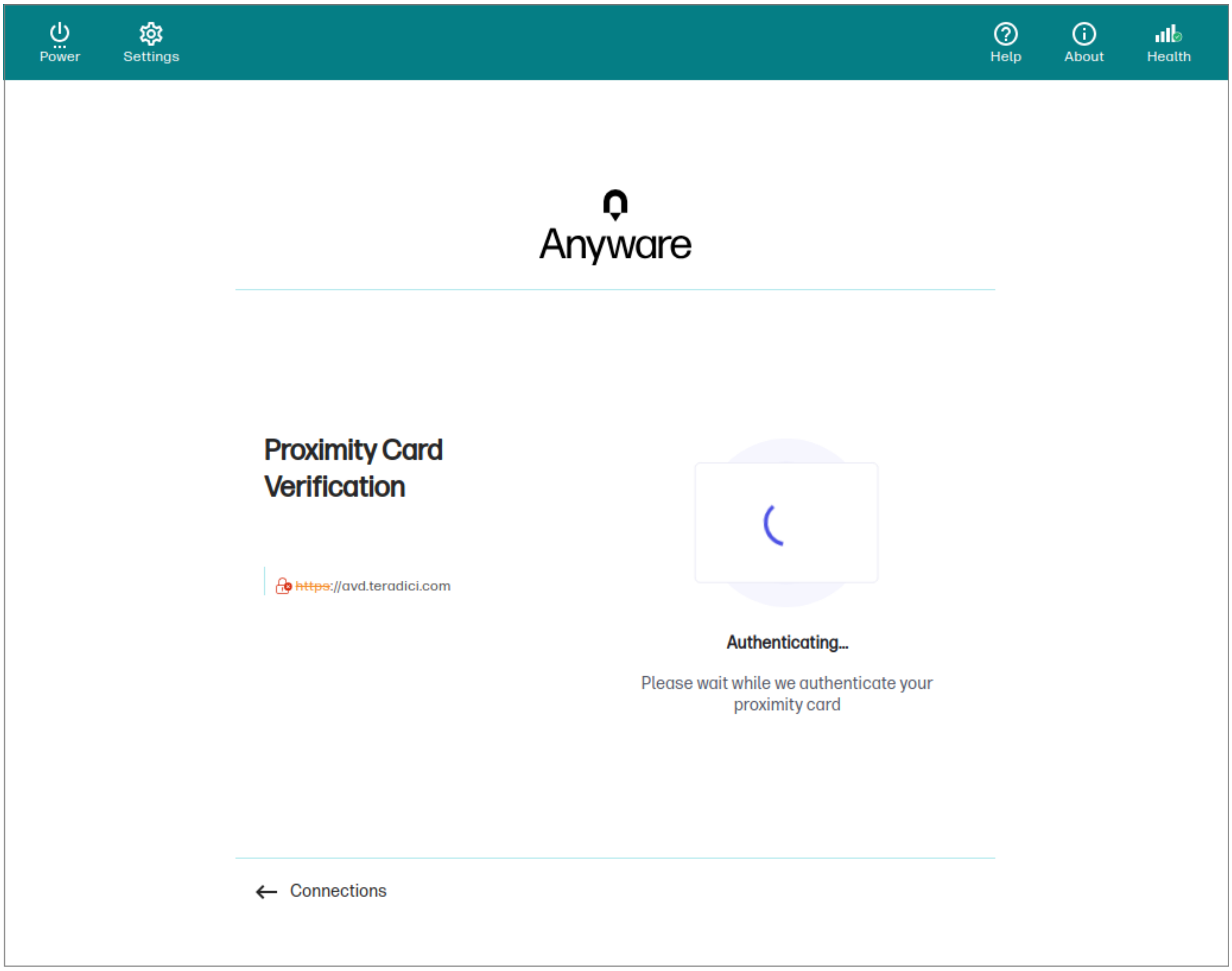
Proximity Card Verification

~~https~~://avd.teradici.com

Proximity Card Verification

Please tap your proximity card to continue

6. Wait while the proximity card is verified.



Proximity Card Verification

~~https~~://avd.teradici.com

Authenticating...

Please wait while we authenticate your proximity card

7. Once the proximity card is verified, on the **Desktop selection** page, select a desktop of your interest to initiate a PCoIP session. If you want to skip this step, follow the instructions given in Auto login if only one desktop is available.

Troubleshooting Common Connection Errors

While authenticating the proximity card, you might encounter the following issues:

- If the card reader is unable to read the card, an error message will appear.
  - To resolve this issue, tap your card again, or use another card.
- If the card verification fails, an error message will appear.
  - To resolve this issue, use another card.
- If the card is blocked, an error message is displayed.
  - Try another card, or contact your system admin for support.

- If you use an invalid card, the UI will display an error.
  - Retry with a valid card.
- After the session is launched, if you use an invalid card, the session will be terminated.
  - To resolve this issue, connect using the Imprivata OneSign Server again.

Customizing the Login Experience

The Settings page on the client UI has a Connections menu for personalizing your login experience. Trusted Zero Clients can be configured to skip one or more of the following login steps:

- Connecting to a broker
- Providing user credentials
- Selecting a desktop

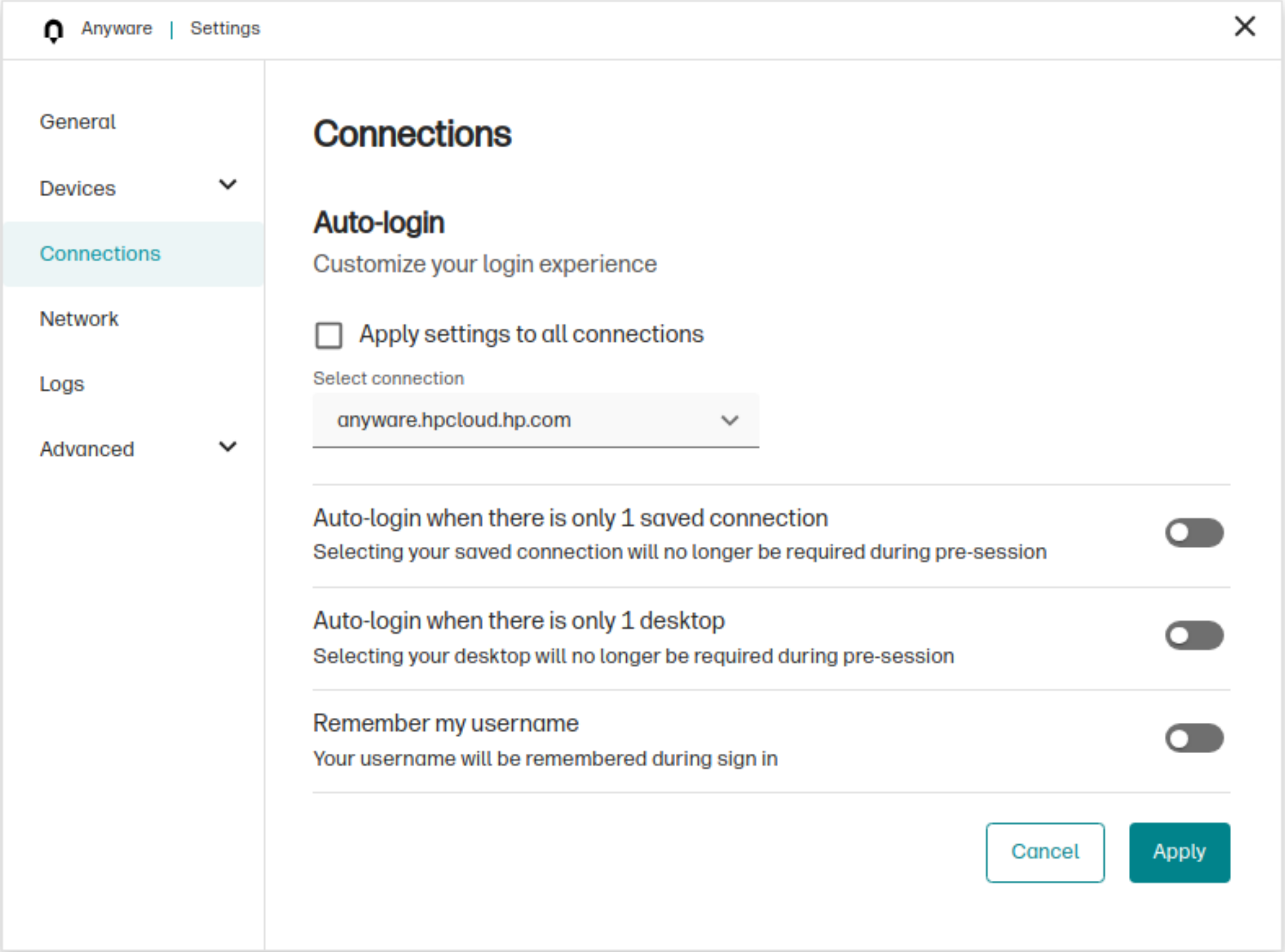
The ability to bypass one or more traditional login steps results in a simplified and streamlined the login experience.

Info

If the login options have been configured in Trust Center, they cannot be modified in the Trusted Zero Client UI.

To customize the login experience:

1. Launch the Trusted Zero Client.
2. Click the gear icon in the top-left corner.
3. In the left pane, click **Connections** to open the **Connections** page.



Connections

Auto-login

Customize your login experience

□ Apply settings to all connections

Select connection: anyware.hpcloud.hp.com

Auto-login when there is only 1 saved connection
Selecting your saved connection will no longer be required during pre-session

Auto-login when there is only 1 desktop
Selecting your desktop will no longer be required during pre-session

Remember my username
Your username will be remembered during sign in

4. Provide the following details:
   - **Select connection**: The connection to which you want to customize the login experience. You must have at least **one saved** connection prior.
   - **Auto-login when there is only 1 saved connection**: Use this toggle to enable or disable the ability to auto connect if only 1 saved connection (broker) is available.
   - **Auto-login when there is only 1 saved desktop**: Use this toggle to enable or disable the ability to auto connect if only 1 saved desktop is available.
   - **Remember my username**: Use this toggle to remember your username for future logins.
5. Select **Apply settings to all connections** if you want the same login experience while connecting to other brokers and desktops.
6. Click **Apply**.

Managing Connections and Desktops

You can manage connections and desktops that you previously added from the pre-session UI. Follow the instructions detailed in this topic to manage your connections and desktops.

Managing Connections

From the pre-session UI, the following actions are possible:

- Update the name and the address of the brokers or direct desktop connections
- Delete a connection
- On the **Saved connections** window, click the vertical ellipsis next to the connection to reveal the context menu.
- To rename the connection, select **Edit**.
- Update the **Host Address or Registration Code** or the **Connection Name** as necessary.
- Click **Save**.
- To delete the connection, from the context menu, click **Delete**.

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.

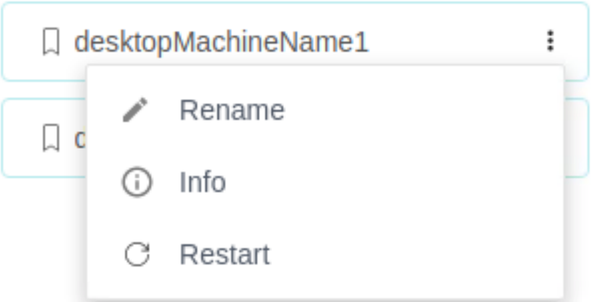
Rename a Desktop

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 View Desktop Information.

Restart a Desktop

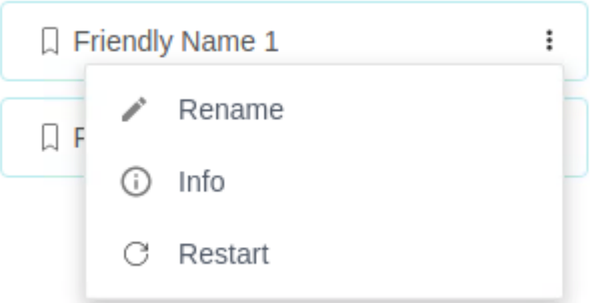
You can send a restart command to a remote desktop from the client interface, if supported by your remote system.

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 above.
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

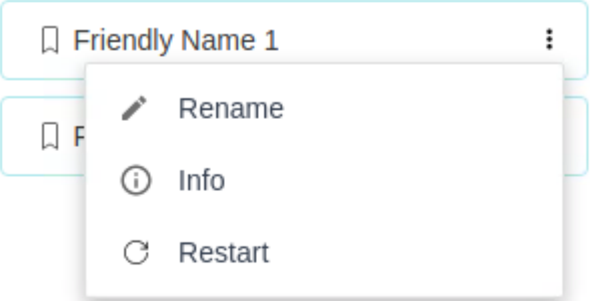
You can view detailed information about each of your available remote desktops, including resource names, IDs, and protocols.

Tip: Desktop machine names

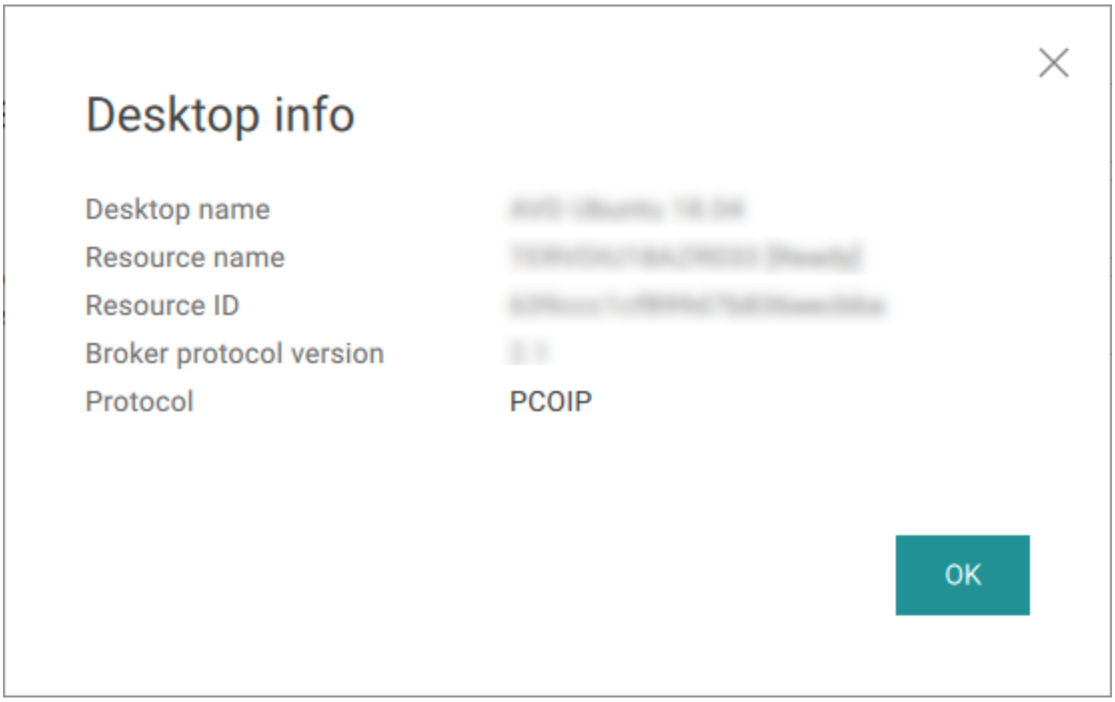
If you have renamed a desktop, the original machine name is the *resource name* shown here.

To view desktop info:

1. Display the desktop list as described above.
2. Click **Info**:



3. Review the displayed information.



Desktop info

Desktop name	[redacted]
Resource name	[redacted]
Resource ID	[redacted]
Broker protocol version	[redacted]
Protocol	PCOIP

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

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 Anyware Client** > **Quit Anyware Anyware 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 remote desktop configuration**: The remote agent (whether an Anyware agent, Omnissa Horizon Agent, or Amazon WorkSpaces 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 remote 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 HP Anyware Webcam Support for a current list of tested webcams.

This feature is only supported by the Anyware Graphics Agent for Windows and 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**.

Selecting Audio Devices in Session

While in session, you can select audio devices that will be forwarded to the agent. If more than one audio device is connected to the Trusted Zero Client machine, you can select **multiple audio output devices**, and **one audio input device** after a PCoIP session has been established.

> ⚠ **Warning**
>
> AV lock functionality will be disabled if you select more than one output audio device.

> ✎ **Note: Supported Client & Agents**
>
> This feature is only available on Trusted Zero Client machines connecting to Windows Graphics agents or Windows Standard agents.

Before You Begin

Before you begin, make sure that at least one audio device is connected to the Trusted Zero Client. If no device is connected, you will not see any device under the device list on the **Audio** dialog.

To select audio devices:

1. When in session, go to the **Connection** dropdown menu, and click **Audio**.
2. On the **Anyware | Audio** window, select the output devices:
3. Under **Output**, use the toggle buttons next to the output devices to select the devices of your interest. The Trusted Zero Client selects a default output device, for which the toggle button appears locked until you select another device.
4. Select another audio output device by using the toggle button next to the audio device. **Multiple output devices** can be selected at a time.
5. Under **Input**, use the toggle buttons next to the available input devices to select the input device of your interest. **Only 1 input device** can be selected at a time.
6. Wait until the devices have been selected.

Once selected, the audio devices are forwarded to the agent.

Disconnection Behavior

If a previously selected audio output device is unplugged, it will be removed from the **Output** section on the **Audio** windows. The next available output device is enabled in place of the unplugged device.

When an audio output device is disconnected, you will receive an alert message on your screen.

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 output devices has been added from the release 25.03 onwards.

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.

> **Info**
>
> Enhanced A/V Sync is currently supported on Anyware remote desktops.

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.

Multiple Audio Device Support

The Trusted Zero Client supports **multiple output devices** in addition to the existing capability of selecting one input device on the client side. Device selection is done when the client is in session with the agent.

This capability is supported on the following:

- Trusted Zero Clients connecting to Windows Graphics agents
- Trusted Zero Clients connecting to Windows Standard agents

Instructions on selecting audio devices are available in Selecting Audio Devices.

Connection Health Indicator

The **Connection Health Indicator** gives you quick feedback on the quality of your active remote 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 remote 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 remote session. Note that once a has registered with a , it can continue to connect even if the is not available.

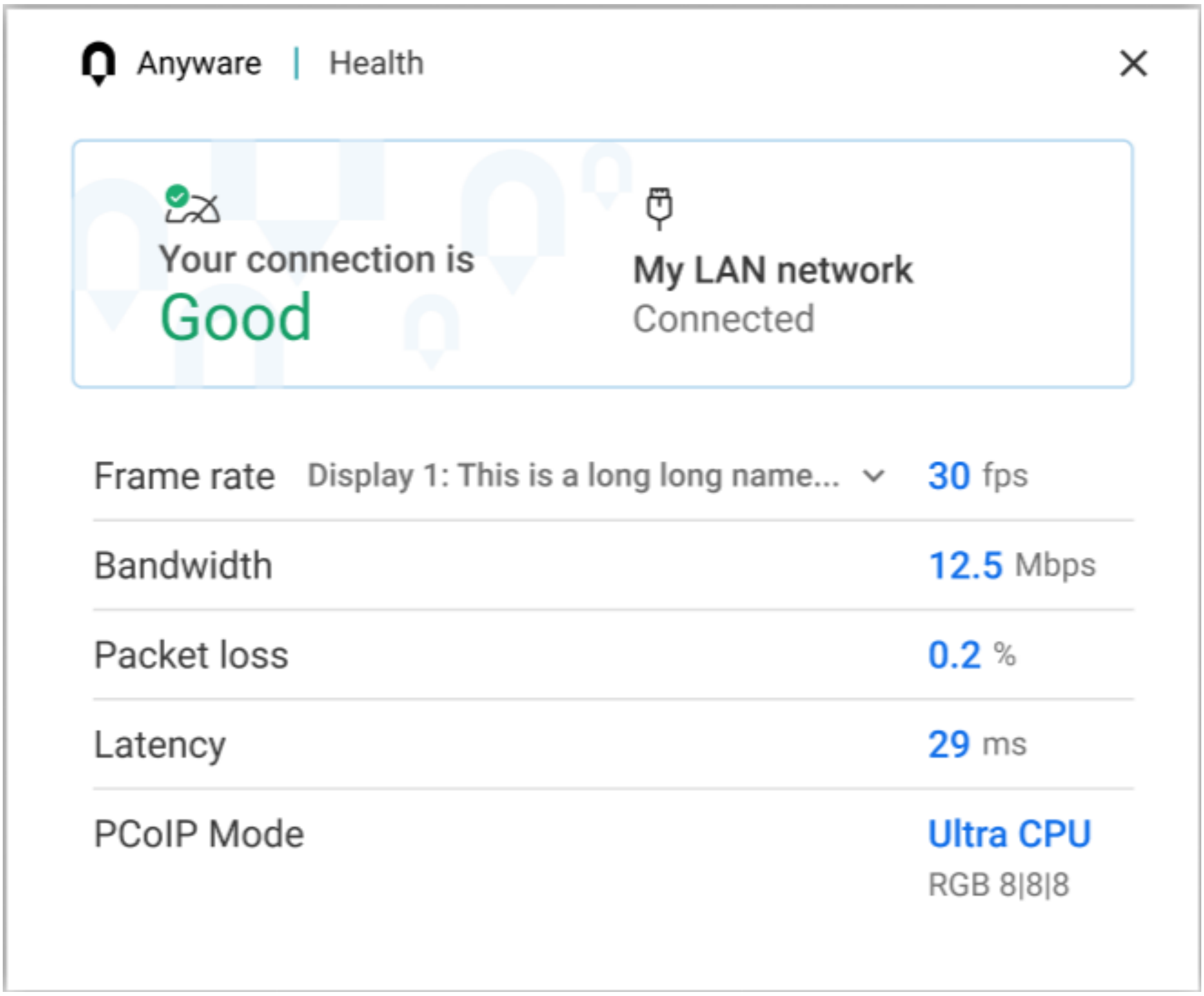
If the Trusted Zero Client is connected to the network and to the Anyware Trust Center, the health indicator icon will be green.

In-Session Health Indicator

Note: Anyware agent feature

In the current release, the in-session health indicator is only supported by Anyware agents.

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



Anyware | Health

Your connection is Good

My LAN network Connected

Frame rate Display 1: This is a long long name... 30 fps

Bandwidth 12.5 Mbps

Packet loss 0.2 %

Latency 29 ms

PCoIP Mode Ultra CPU RGB 8|8|8

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. remote 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. remote 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 remote 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 remote 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 remote 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 Anyware 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).

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.

Info

This procedure is only applicable to HP Anyware sessions. Horizon sessions auto-detect monitor changes and dynamically adjust the session according to 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.

Support for Moving Devices Between SIPR/NIPR & Insecure Networks

There are specific regulations applicable when moving devices between SIPR, NIPR, and insecure networks, with a goal of preventing data from one type of network from being transferred to a different type of network. In such scenario, there are certain steps the user/administrator must take when transferring a Trusted Zero Client from a SIPR network to NIPR or to an insecure network or vice versa.

Instructions for moving Trusted Zero Clients bettwen networks is available in the topic entitled "Support for Moving Devices Between SIPR/NIPR & Insecure Networks" in the Trust Center Guide.

Migrating Networks

When re-commissioning a Trusted Zero Client to be used on a SIPR or NIPR network, moving between SIPR and NIPR, or moving the Trusted Zero Client to an insecure network, local data and configuration must be removed from the Trusted Zero Client.

1. Unplug the Trusted Zero Client from the network (or deactivate wireless if configured).
2. Perform a factory reset of the Trusted Zero Client (**Settings** → **Advanced** → **Reset** in the client interface).
3. If reconnecting the Trusted Zero Client to the **same** Trust Center, but on a different network type, remove any configuration for the Trusted Zero Client from the current Trust Center.
4. Power off the Trusted Zero Client.
5. Make sure the Trusted Zero Client remains powered off while moving between networks.
6. Connect the Trusted Zero Client to the new network and power it on.
7. Register the Trusted Zero Client with Trust Center on the new network.

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 Anyware agent; disallowing a USB device from either *either* Anyware Trust Center or Anyware agent will prevent it from working in-session.

> **Note: Automatic redirecting in Omnissa Horizon sessions**
>
> USB devices will be automatically redirected irrespective of whether they are attached prior to the session or during 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

Important: Wacom support is an Anyware agent feature

Support for Wacom tablets is currently limited to Anyware agents. Support for Wacom tablets in Omnissa Horizon is untested.

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 session using one of two modes: *Tablet Performance* (the default), which provides highly responsive performance and better tolerance of high-latency networks, and *LAN Connect*, 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 remote sessions

Tablets must be connected to the remote 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 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

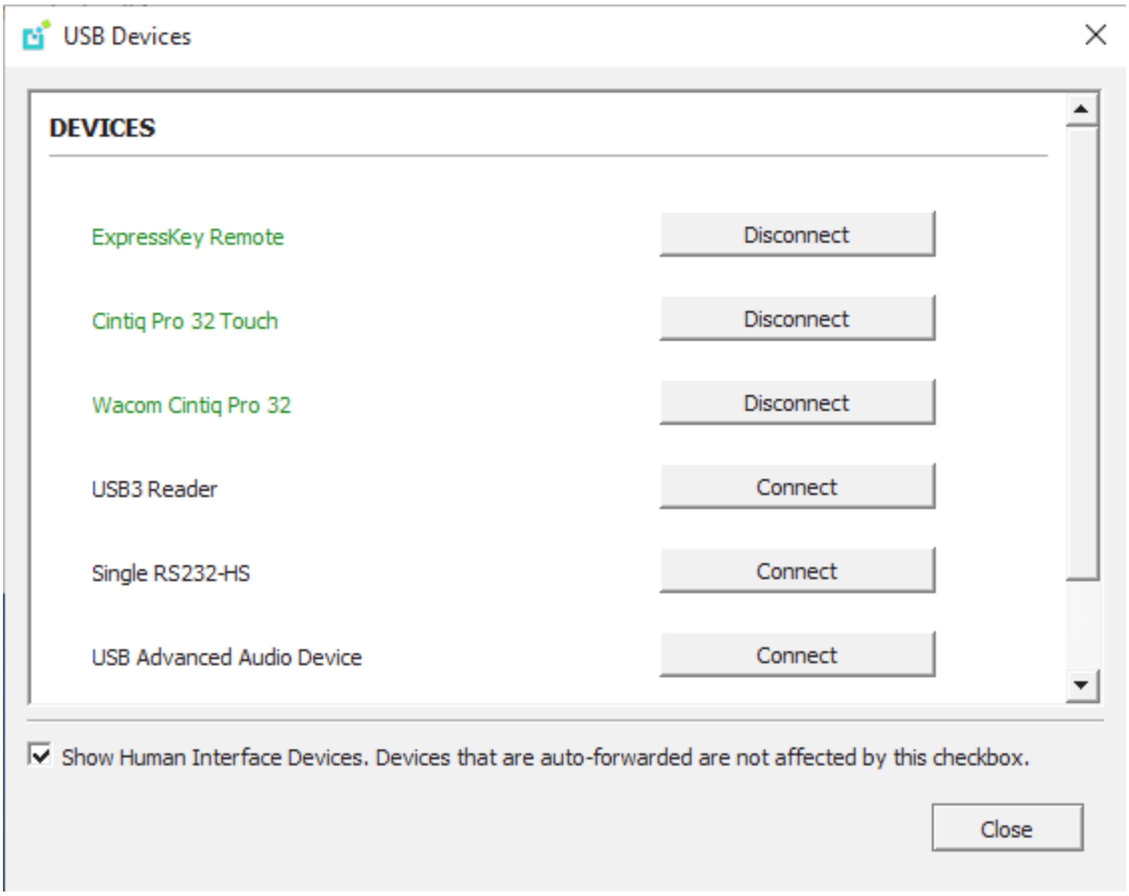
	PCoIP agents (Windows)	PCoIP agents (Linux)	PCoIP Graphics Agent for macOS	PCoIP Remote Workstation Card
Intuos Pro Small *PTH-460*	✔	✔	–	✔
Intuos Pro Medium *PTH-660*	✔	✔	–	✔
Intuos Pro Large *PTH-860*	✔	✔	–	✔
Cintiq Pro 16 *DTH-167*	✔	✔	–	–
Cintiq Pro 16 *DTH-1621*	✔	✔	–	–
Cintiq 22 *DTK-2260*	✔	✔	–	✔
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 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



USB Devices

DEVICES

ExpressKey Remote	Disconnect
Cintiq Pro 32 Touch	Disconnect
Wacom Cintiq Pro 32	Disconnect
USB3 Reader	Connect
Single RS232-HS	Connect
USB Advanced Audio Device	Connect

☑ Show Human Interface Devices. Devices that are auto-forwarded are not affected by this checkbox.

Working with Wacom Tablets

CONNECTING A WACOM TABLET

To use the Wacom tablet, **you must manually connect it to the remote 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. From the Wacom tablet screen, 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. From the Wacom tablet screen, 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 remote 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. From the Wacom tablet screen, 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 an **Anyware Agent for Windows** as well as an **Omnissa Horizon Agent**, although their functionalities may vary. USB webcams can be used while in the remote desktop, including with applications such as Microsoft Teams or Zoom.

This feature is **enabled by default**.

Notes

- Previously, Webcam support was only available for Anyware agents. While **support has been extended to Omnissa Horizon agents**, there are differences in the capabilities offered.

  For additional information related to webcam support on Omnissa Horizon agents, consult the Omnissa Product Documentation.
- Detailed information about the models that have been tested on the **Anyware Windows agents** and the performance metrics associated with these models see HP Anyware Webcam Support. This knowledge base article also has steps on how to test and verify other webcam models.

Requirements

- Anyware Standard Agent for Windows or Anyware Graphics Agent for Windows, 23.06+
- Omnissa Horizon Agent

  Consult the Omnissa Product Documentation for more information.
- A USB-attached webcam

Disabling the webUSB Flag

If the browser on the remote desktop terminates when a webcam is connected, you must disable the webUSB setting in Chrome. This is applicable for both **Anyware Agent and Omnissa Horizon Agent**.

1. In the search bar of the Chrome browser, run the following command:

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

2. Open the Chrome menu and disable the webUSB flag.

Bridging Webcams

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

Supported Xencelabs Pen Displays

Xencelabs Pen Displays are supported in the *locally terminated* mode, where peripheral data is processed locally on the Trusted Zero client. They are also supported in the *bridged* mode, where peripheral data is sent to the desktop for processing.

Support is available when a connection is initiated from a **Trusted Zero client to a Windows Graphics or Standard agent**.

The following Xencelabs Pen Display devices are supported:

- Xencelabs Pen Display 16
- Xencelabs Pen Display 24

Note: Xencelabs Device Firmware

For optimum performance, ensure that your Xencelabs device has the latest firmware.

Note: Xencelabs Device Drivers

Drivers for Xencelabs pen displays must be installed on **agent machines**.

Media Optimization

Media Optimization for Microsoft Teams and Zoom

Trusted Zero Client supports media optimization of Zoom and Teams, which allows for an enhanced video conferencing performance by offloading audio and video streams to the Trusted Zero clients. The clients handle the processing and transmitting of the streams to and from the Omnissa VDI, redirecting audio and video calls without overloading the network. This results in reduced latency, and improved meeting experience during sessions.

The following applications are supported for media optimization:

- Media Optimization of Zoom when **Trusted Zero Clients are connected to Omnissa Horizon agents and Anyware Agents**.
- Media Optimization of Microsoft Teams when **Trusted Zero Clients are connected to Omnissa Horizon agents**.

How Media Optimization for Microsoft Teams Works

Enabling media optimization requires no additional configuration aside from the installation of Microsoft Teams on Horizon agents. On client machines, no configuration is required; the redirection-related files are already contained in the SDK package.

The Trusted Zero Client's optimization for Microsoft Teams interfaces with the Microsoft Teams installed on Horizon agents by means of a virtual channel. This allows the client machines to process audio and video streams locally, and render the Teams meetings by superimposing it on the Trusted Zero Client window.

Authentication and signaling is processed on the agent machines, and remain unaffected by audio/ video redirection.

How Media Optimization for Zoom Works

Media Optimization for Zoom makes use of the following two components, which are two separate programs, each with their physical installation location:

- Zoom VDI Client, which is installed on the Horizon Agent or the Anyware agent machines.
- Zoom Plugin, which is installed on the Trusted Zero Client machines.

The Zoom VDI Client and the Zoom Plugin work in synchronization to render the Zoom meeting in layers, typically superimposing the meeting on the Trusted Zero Client window. Additionally, Instead of using USB Redirection, the Zoom VDI Plugin utilizes the media devices of the client machines to send audio and video data to the Zoom server.

This eliminates the need for sending audio and video data from the client machines to the agent machines, and then to the Zoom servers, thereby resulting in a seamless video conferencing experience.

How All Other Realtime Audio/Video Works

For Omnissa Horizon sessions, the Trusted Zero Client uses Real-Time Audio-Video (RTAV). RTAV allows Horizon 8 users to run Skype, Webex, Google Hangouts, and other online conferencing applications in their remote sessions. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote sessions.

This feature redirects video and audio data with a significantly lower bandwidth than can be achieved by using USB redirection. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications; and supports standard webcams, audio USB devices, and analog audio input.

⚠ **Note: Agent Setup Required**

For Media Optimization to work, agent setup is required. This is described in Enabling Media Optimization for Teams and Enabling Media Optimization for Zoom respectively.

Additional Reading

Further reading is available as follows:

- Detailed information on Zoom VDI is available on the Zoom Support site
- Omnissa Horizon documentation is available on the Omnissa Horizon Docs Site
- Information on installing and setting up Microsoft Teams is available on the Microsoft Learning Site

Media Optimization for Teams

Enabling Media Optimization for Microsoft Teams

This section contains instructions for enabling Media Optimization for Microsoft Teams. Instructions for Zoom are available in Enabling Media Optimization for Zoom.

SUPPORTED CONFIGURATION & AGENTS

Media optimization is supported when Trusted Zero Clients connect to Omnissa Horizon agents using the following protocols:

- Blast
- PCoIP

The following Horizon agents are supported:

- Horizon 8 (2006 and later)
- Horizon 7 version 7.13

AGENT SETUP

On Omnissa Horizon Agent 8 2212 or later, Media Optimization is controlled by means of a registry key `"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Horizon, Inc.\Horizon WebRTCRedir”` `teamsEnabled (REG_DWORD)`. This registry key is created at the time of agent installation, and its value is set to **1**. This turns on Media Optimization by default.

Deploying the Teams App on the Agent

1. Download the Teams App that matches your VM operating system from the Microsoft Teams Page.
2. Run the following command:

```
reg add "HKLM\SOFTWARE\Microsoft\Teams" /v IsWVDEnvironment /t REG_DWORD /d
1 /f
```

This process adds the registry key to the agent, and sets its value to "1".

1. Install Microsoft Teams by running the following command:

   ```
   msiexec /i "C:\Users\autolaab300\Downloads\Teams_windows_x64.msi" /l*v
   "msteams.log" ALLUSER=1 ALLUSERS=1
   ```

CLIENT SETUP

For Media Optimization of Microsoft Teams, no configuration is required on client machines. The redirection-related files are already contained installed on the Trusted Zero Client.

Ensure that the files are present in the SDK package.

Using Microsoft Teams

This section describes how to use the optimized Microsoft Teams to create or join meetings.

VALIDATING THE OPTIMIZED MICROSOFT TEAMS

1. Start Microsoft Teams on the agent machine.
2. Click the horizontal ellipsis next to the user name.
3. Go to **About** > **Version** to reveal the banner describing the Microsoft Teams version and pairing mode.
4. Ensure that this is **VMware Media Optimized, Media Optimization for Microsoft Teams**. This indicates that the audio and video streams are offloaded to the Trusted Zero client machine.

Creating or Joining a Teams Meeting

1. From the client machine, start a session with the agent machine on which Teams is installed.
2. Start the Teams application on the agent machine.
3. Create or join a meeting, as you would while using the standard Teams application.
4. Select the audio and video device of your choice. The audio and video devices connected to the client are enumerated in the Teams App.

Media Optimization for Zoom

Enabling Media Optimization for Zoom

Media Optimization for Zoom requires the Zoom VDI application. Zoom VDI consists of the following two components, which are separate programs:

- Zoom VDI Client

  Zoom VDI client must be installed on agent machines.
- Zoom Plugin

  Zoom Plugin is **included with** the Trusted Zero Client.

> **Note: Zoom Plugin is Included with the Trusted Zero Client**
>
> The Trusted Zero Client is already configured with the Zoom Plugin. No separate installation is necessary.

SUPPORTED CONFIGURATION & AGENTS

Media optimization is supported when Trusted Zero Clients connect to:

- Omnissa Horizon agents using the Blast and PCoIP protocol, and
- Anyware agents.

The following Horizon agents are supported:

- Horizon 8 (2006 and later)
- Horizon 7 version 7.13

The following Anyware agents are supported:

- Graphics Agent for Windows 25.03 or later
- Standard Agent for Windows 25.03 or later

AGENT SETUP

Before you begin, make sure that you have administrator privileges on the agent machine where you will install the Zoom VDI Client.

Note: Version Parity

The Zoom VDI Client version you select must be the same or higher than the version of the Zoom Plugin on client machines. Select version 6.2.12 or later.

1. On the agent machine, access the VDI releases and downloads page in a web browser.
2. Under **Compatible plugins**, locate the installer version. The version must be 6.2.12 or later.
3. Download either the 32-bit or the 64-bit installer, depending on your machine's configuration. The **ZoomInstallerVDI.msi** file will be downloaded to your agent computer.
4. If connected to a Zoom session, disconnect it.
5. Double-click the **ZoomInstallerVDI.msi** file to begin installation.
6. Follow the steps in the installation wizard to complete the installation.

Once the installation completes, client machines can join optimized Zoom meetings.

Using Zoom VDI

By default, the Zoom Plugin is automatically launched on the client machine every time a session is initiated. Once launched, the Zoom Plugin connects to the Zoom VDI Client on the Horizon agent to render Zoom meetings.

VALIDATING THE INSTALLATION

Perform the following steps to verify that the Zoom VDI app works in your VDI environment.

1. Start the Zoom VDI application on the agent machine.
2. Sign in to Zoom VDI.
3. Go to **Settings** > **Statistics** > **VDI**. You should see the VDI Plugin status. Make sure that it is "Connected".

Creating or Joining a Zoom Meeting

Zoom VDI presents a conferencing experience that is similar to a standard Zoom application. This section describes how to create or join a meeting using Zoom VDI.

1. From the client machine, start a session with the agent machine on which Zoom VDI is installed.

   Note: Use the Correct Application

   If your agent machine also has the standard Zoom application, make sure that you select **Zoom VDI**, and NOT **Zoom**.

2. Start the Zoom VDI application on the agent machine.
3. Create or join a meeting, as you would while using the standard Zoom application. For more information, see the Zoom Getting Started Guide.
4. Select the audio and video device of your choice. The audio and video devices connected to the client are enumerated in the Zoom VDI App.

Note: Disconnecting the Zoom Session

The Zoom Plugin disconnects from the Zoom VDI Client when the session is disconnected.

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 remote 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 remote session (PCoIP or Blast), 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, such as Wacom tablets, audio devices, and displays.

USB

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).

Displays

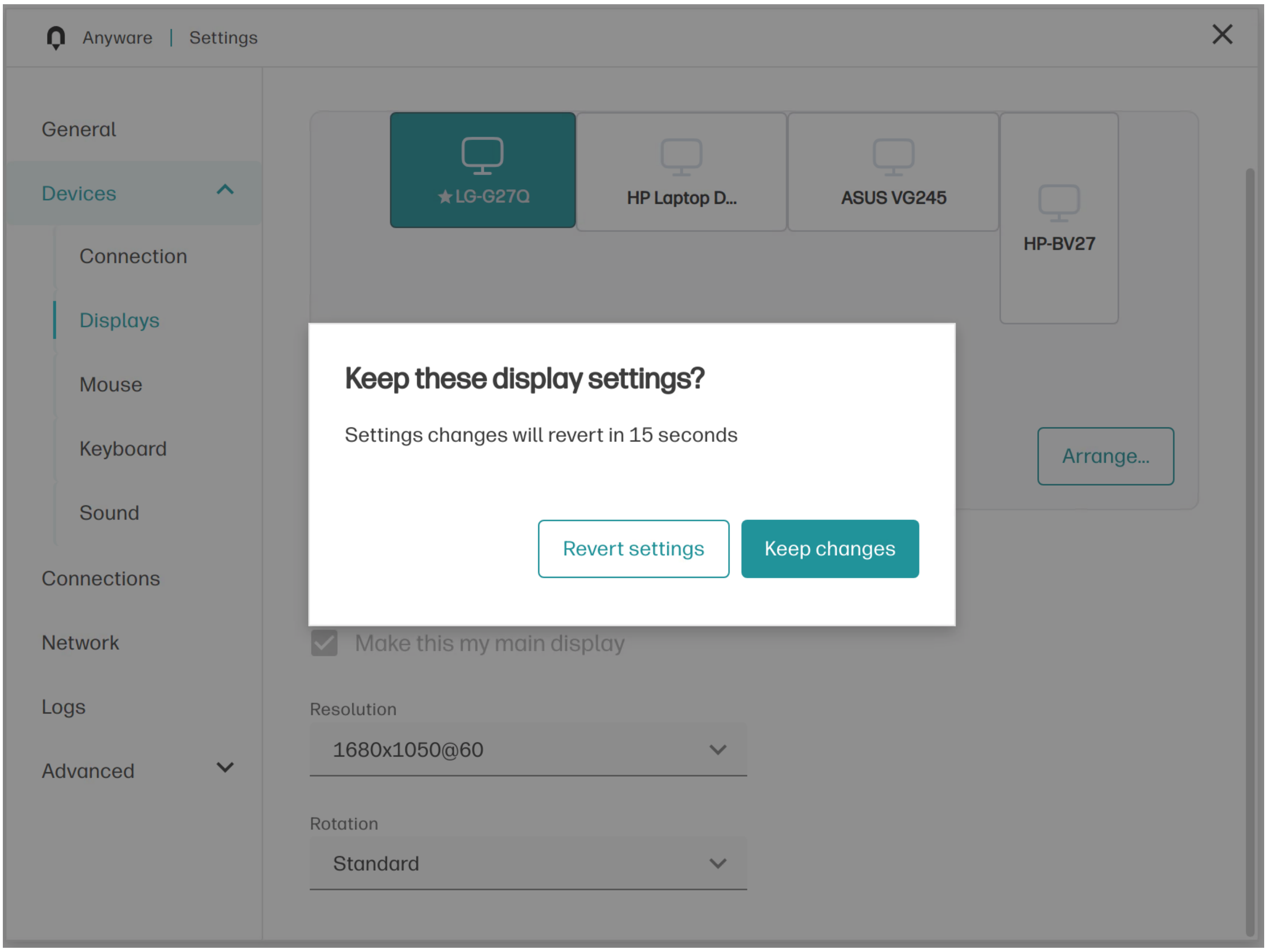
Display Configuration

You can see what displays or monitors are available on your Trusted Zero Client and change their resolution, orientation, set which monitor is your primary display, and arrange the monitors to match how they are physically set up on your desk.

Task	Location	Options
View Display Information	**Settings** > **Devices** > **Display**	Your displays and their current arrangement can be seen at the top of the page. To select which device you'd like to , click the radio button next to the device.
Arrange Displays	**Settings** > **Devices** > **Display** > **Arrange**	Click the **Arrange** button, and drag-and-drop your monitors to position them to match your physical layout.
Edit Display Settings	**Settings** > **Devices** > **Display**	Select a display to modify it. You can set each display's orientation and resolution, and set one monitor as the desktop's primary display.

- Confirm Changes: In the display settings modal dialog, click the **Keep changes** button to apply your adjustments.

- Revert to Original Settings: If you prefer to return to the original settings, click the **Revert settings** button



Keep these display settings?

Settings changes will revert in 15 seconds

☑ Make this my main display

Resolution: 1680x1050@60

Rotation: Standard

Note: User Interaction Timeout

A timeout of 20 seconds is set for you to interact with the modal dialog. If you do not interact with the modal before the timeout expires, any changes will be reverted.

Note: Trust Center Administrator Settings

If the Trust Center administrator sets enforced display properties while the modal dialog is open, those properties will apply, and the modal will be forced to close.

Sound

Sound Device Selection

You can see which audio devices are available on your Trusted Zero Client, and change which devices are used for input (such as microphones) or output (such as headphones or speakers).

Task	Location	Options
View Sound Devices	**Settings** > **Devices** > **Sound**	Your available sound devices are displayed in a list. To select the device you'd like to use, click the button beside it.

Connections

The **Connections** menu can be used for personalizing your login experience. Trusted Zero Clients can be configured to skip one or more of the following login steps:

- Connecting to a broker
- Providing user credentials
- Selecting a desktop

Task	Location	Options
Auto-login when there is only 1 saved connection	**Settings** > **Connections**	Use this toggle to enable or disable the ability to auto connect if only 1 saved connection (broker) is available.
Auto-login when there is only 1 saved desktop	**Settings** > **Connections**	Use this toggle to enable or disable the ability to auto connect if only 1 saved desktop is available.
Remember my username	**Settings** > **Connections**	Use this toggle to remember your username for future logins.

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.

To set the static IP address for a device, click the **Edit** button by the network connection and provide the desired value. This setting can also be pushed from the Anyware Trust Center.

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.

Wi-Fi Network

You can enable your Trusted Zero Client to connect to WPA2 networks, as well as select a Wi-Fi network from the list of available networks.

Info

If Wi-Fi is disabled for Trusted Zero Clients in your deployment, this option will not be available.

Task	Location	Options
Enable Wi-Fi Network	**Settings** > **Network** > **Wi-Fi networks**	Available Wi-Fi networks are displayed in a list. Click the Wi-Fi network that you want to connect to.

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.

You can use this view to create support bundles, which contain logs and other system information that help our team diagnose problems.

Note: Support bundles are stored on the Anyware Trust Center

Note that these support bundles are submitted to the Anyware Trust Center and reside there, and not directly to our support team, and must be forwarded manually when discussing a support case.

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)	✓	Pre-session UI	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; some settings may be changed in the device's pre-session interface.
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.

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
			The Trusted Zero Client has no AWI; administrators control settings via the 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 is supported with version 24.03.0 and later.	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	✓	✓	Trusted Zero Clients support PCoIP Ultra. Tera2 PCoIP Zero Clients support PCoIP with Horizon.
Amazon WorkSpaces	✓	✓	
Omnissa Horizon View	✓	✓	Both Blast and PCoIP protocols are supported
Connection Management	✓	✓	Connections can be added, removed, and edited from both the device and the Anyware Trust Center.
Imprivata OneSign Server	✓	✓	Connections to Horizon hosts are authenticated using the Imprivata OneSign Server.

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. Log retrieval from the Trusted Zero Client via USB mass storage device.	
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	✓	✓	
Quad displays	✓ model dependent (dual or quad)	✓ (hardware dependent)	
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	✓	✓	
Zero Trust for Device	–	✓	
PCoIP Ultra	–	✓	
Omnissa Horizon Blast	–	✓	
USB 3.x / USB C	–	✓	Depending on hardware selection.
Webcam Support	✓ (Limited Webcam support)	✓	
Wacom	✓	✓	
Secure Boot	–	✓	
Encrypted Storage	–	✓	
TPM backed Certificates	–	✓	
Internationalization		✓	Currently, only the Trusted Zero Client pre-session UI is localized; broker

Feature	Tera2 PCoIP Zero Client	Trusted Zero Client	Notes
			messages and in-session menus are not localized.
Monitor Topology Settings	(Limited)	✓	
FIPS	140-2	140-3	
Wifi	–	Early 2025	
Bloomberg 4 Keyboards		✓	
Bloomberg 5 Keyboards		✓	Multiple audio support is now supported.
WWAN (5G)	–	Future development	
Bluetooth	–	Future development	
Touch Monitor	✓	✓	Single-touch supported. Multi-touch with gestures is not yet supported.
Imprivata	✓	Mid-2025	Imprivata proximity cards tap-in / tap-out is supported for authentication; however they are not bridge in-session yet.
Static IPs	✓	✓	
Audio Device Configuration	✓	✓	
Dark mode	–	Future development	
Media Optimization with Zoom and Teams	–	✓	

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:

- An extensive **knowledge base** that 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.
- A **community forum** that allows 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.
- The ability to create support requests directly from the Trusted Zero Client. Your IT admin will receive the support bundles sent along with the support requests, which they can share with the Anyware Support team. This method is useful when Trusted Zero Clients can connect to the Trust Center.
- The ability to create support tickets. Support bundles from your Trusted Zero Client saved to USB devices can be attached along with the tickets. This method is useful when Trusted Zero Clients cannot connect to the Trust Center.

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 remote 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.

Creating a Support Request

If you require assistance from your IT Admin or Anyware Support, you can send them a support request from the Trusted Zero Client interface. The support request includes logs from your last session. Once you create a support request, your IT Admin will receive this bundle in their EMS and can coordinate with Anyware Support to help resolve your issue.

To create a support bundle:

1. During pre-session, click the help icon at the top right corner.
2. Enter a message describing the issue, and click **Send**.

Saving the Support Bundle to a Peripheral Device

If the Trusted Zero Client is unable to connect to the Trust Center, you can create a support bundle from the Trusted Zero Client UI and save it to a USB mass storage device formatted with a FAT32 file system. The support bundle will include logs from your last session, which can be used for issue resolution.

Support bundles created this way are not sent to the Trust Center. They can however, be shared with the support team by opening a support ticket.

To save the support bundle:

1. Ensure that a USB device is connected to the client machine.
2. During pre-session, click the help icon at the top right corner.
3. On the **Anyware | Help** window, click **Save support bundle**.

4. On the **Save support bundle** dialog, select the USB to which you want to save the support bundle, and click **Save bundle**.