



Modernized Thin & Zero Client Hardware and Software

## WELCOME TO THE 10ZiG TRUSTED ZERO CLIENT INSTRUCTIONAL GUIDE



Setup Instructions for 10ZiG Trusted Zero Clients

*Let's get your devices set-up and started!* →



SECURE



MANAGED



FLEXIBLE

### Ultra V2000 Series Setup Instructions

3

Requirements - For Trusted Zero Client and  
Anywhere Trust Center Deployments

6

Setting up Your Trusted Zero Client



# V2000 TRUSTED ZERO CLIENT SERIES FOR PCOIP ULTRA AND BLAST EXTREME

(Models V2200 & V2400)



The Trusted Zero Client is a next-generation standalone PCoIP Ultra and Blast Extreme Ultra client, securely connecting users to their HP Anyware remote desktops, as well as Amazon WorkSpaces and Omnisia 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 and 10ZiG Manager, which enforce security and configuration settings for each endpoint device in your deployment. A Trusted Zero Client cannot be used without an Anyware Trust Center.\*

\*Except for demonstration purposes, see requirements for standalone deployments section.



## Requirements – For Standalone Deployments \*Anyware Trust Center Not Required\*

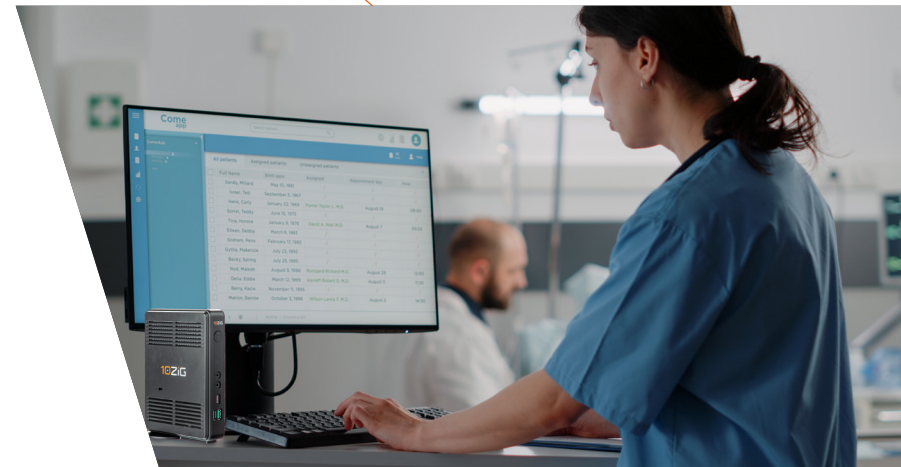
In this scenario the Trusted Zero Client has already been registered with an existing Anyware Trust Center. This process is normally performed at the 10ZiG factory during assembly and is requested beforehand with your 10ZiG representative. This scenario skips the requirement to install Anyware Trust Center and 10ZiG Manager for faster deployment. It is normally performed in scenarios where it's a requirement to test and validate the Trusted Zero Client functionality only, without the need for testing and validating Anyware Trust Center or 10ZiG Manager which provide zero-trust policies and remote configuration.

This scenario is only recommended in test scenarios, otherwise we recommend following the standard Requirements for Trusted Zero Clients and Anyware Trust Center for enforcing zero-trust policies and remote configuration.

If you are deploying as a Standalone Deployment, proceed immediately to **Trusted Zero Client - Installation Steps**, then **Setting up Your Trusted Zero Client** Step 3.

## Requirements - For Trusted Zero Client and Anyware Trust Center Deployments

The Trusted Zero Client must connect to and register with an Anyware Trust Center before it can be configured to connect to any configurable remote connections.. The Anyware Trust Center enforces zero-trust policies and features, and allows administrators to control Trusted Zero Client deployments. Trusted Zero Clients are designed with zero trust architecture security features and managed by HP Anyware Trust Center. Trusted Zero Clients have the ability to connect to HP Anyware, Amazon Workspaces, and Omnisia Horizon platforms so you're never locked into a single digital workspaces solution. In certain circumstances, for example demo environments 10ZiG can pre-register a Trusted Zero Client with a Trust Center on your behalf. Where this has been performed, this section can be ignored.



## Requirements - For Trusted Zero Client and Anyware Trust Center Deployments (continued)

Available Anyware Trust Center port	The Trusted Zero Client must be able to reach an Anyware Trust Center, on its connected network, on TCP port 32443.
Available PCoIP ports	The Trusted Zero Client must be able to access required PCoIP components, such as brokers and agents. For a comprehensive list of ports used by PCoIP components, see Trusted Zero Client Administrators' Guide.
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.

## Anyware Trust Center Installation Steps

**Register your Anyware Trust Center Subscription** [here](#) – Trusted Zero Clients shipped after July 27, 2023 includes a one-year subscription to Anyware Trust Center. This step requires you to provide your proof of purchase, which will provide your organization a download link to a one-year subscription to Anyware Trust Center. You can then choose to extend your subscription for ongoing and comprehensive support.

### Download and Install Anyware Trust Center [here](#)

1. Using the above link navigate to Management / Client Management and click Anyware Trust Center to proceed to download. **Note:** You will be required to Log in to download.
2. Install Anyware Trust Center by following the Administrators' Guide available for download at the above step.

### 10ZiG Manager Installation Steps

1. Download 10ZiG Manager and the Setup Guide found [here](#).  
**Note:** This step requires you to enter basic contact details before proceeding.
2. Continue to install 10ZiG Manager and Trust Center Connector referring to the Setup Guide in the above step.

## Trusted Zero Client - Installation Steps

---

1. Connect USB keyboard and mouse.
2. Prepare a network connection
  - If you are using a wired network connection, connect one end of the Ethernet cable to the trusted zero client and the other end to a switch/router. The switch or router should be on the same network as the host server or computer.
  - (For wireless zero client only) If you are using wireless connection, install two antennas on the zero client.
3. Connect a monitor cable to the trusted zero client.
4. Connect a headphone and/or a microphone (optional).
5. Connect the power supply to the trusted zero client's power jack, then plug the power supply into a surge-protected AC outlet. Please use the power supply that was shipped with the product
6. Press front power button to power on the trusted zero client.



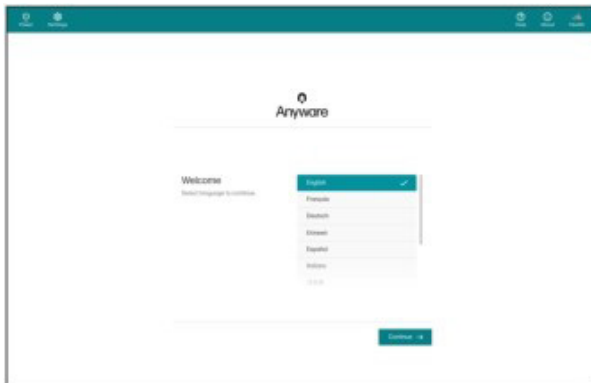


## Setting up Your Trusted Zero Client

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 must be registered with an Anyware Trust Center before they can connect to remote desktops. 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.

The first time the Trusted Zero Client is powered up, you will complete a few one-time configuration steps:

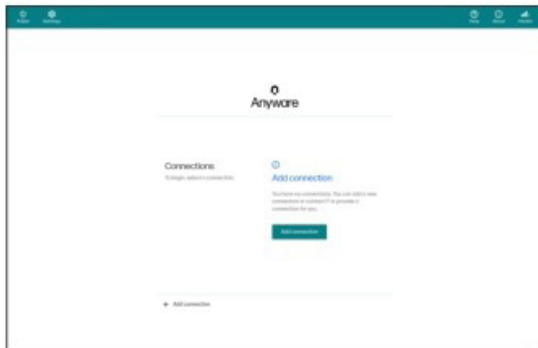
1. Select a language you prefer for the Trusted Zero Client's interface.



2. The Trusted Zero Client will validate your network settings. When prompted for a connection address, provide the FQDN of your Anyware Trust Center and click **Connect**.



3. Create your first connection between your Trusted Zero Client and your remote desktop by clicking + **Add connection**. You can add as many connections as you like.



4. 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.

**NOTE: 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 directly click the name of the connection you want.





10ZiG®

[www.10ZiG.com](http://www.10ZiG.com)

