Manuals+ — User Manuals Simplified.

4610q Thin and Zero Client Hardware and Software

10ZiG 4610q Thin and Zero Client Hardware and Software Installation Guide

Contents

10ZiG 4610q Thin and Zero Client Hardware and Software

FAQs

Q: Can I use the Thin Clients for Windows 10/11 IoT LTSC with remote desktop applications?

A: Yes, you can install and use remote desktop applications on the Thin Clients to access VDI/DaaS environments.

Q: How do I access the Quick Start Wizard?

A: The Quick Start Wizard is either loaded on the desktop or can be launched from the desktop icon provided.

PRODUCT INFORMATION

In case you didn't know, we've been around for a while:

When you think Thin & Zero Client endpoints for virtual desktops, think 10ZiG – for VDI, DaaS & SaaS, Web Apps, and anything Cloud-based. Founded in 2003 and originally under the name of BOSaNOVA through 2009, 10ZiG quickly became THE premier Thin & Zero Client Technology specialists, from hardware services to software services. Headquartered in Arizona, US, and Leicester, UK, with offices in Germany and Australia, we offer full international coverage and support customers from all over the world. As world market leaders of cutting-edge Thin & Zero Client endpoints and management & repurposing software for Cloud Workspaces and Virtual Desktops, our devices are designed to suit all user types in any virtual desktop environment – in the office, remote, or hybrid working.

The devices you want and the service you've wished for:

10ZiG Technology offers a wide selection of powerful, reliable, easy-to-manage, and affordable Thin & Zero Client hardware and software solutions. Our carefully customized devices are built to provide the best performance possible in VDI and server-based applications/desktops for hosted and Cloud environments. Thin & Zero Clients by 10ZiG are available with either Thin (PeakOS™) or Zero (NOS™) client firmware, or Windows 10/11 IoT LTSC. We are certified for and/or support Omnissa (formerly VMware), Citrix, Microsoft, Amazon WorkSpaces, and more. From entry-level end users requiring Microsoft Office basics to power users requiring HD Video/ Audio, HTML5, video conferencing, 3D, and 4K resolution… we have the perfect endpoints for your needs with the service you've always deserved!

Our difference makes all the difference:

- 10ZiG solely focuses on Thin & Zero Client Technology, and that's why we're the best:
- Fully Customizable Solutions: our unwavering commitment to providing you with custom-tailored solutions for any customer request is a level of service you will be hard-pressed to find anywhere else.
- Local Support: our service is backed by our certified support technicians across the U.S., Europe, and the Asia Pacific… we have a team near you.
- Unrivaled Product Warranty: our 3-Year Advance Exchange Warranty can't be beaten… as needed, we ship you a new device immediately without waiting on your current return.
- 10ZiG Manager™: our custom endpoint management software centralizes command and control, and maintenance and reporting for all 10ZiG Linux & Windows based Thin, NOS™ Zero Clients, and Trusted Zero Clients.

Initial Setup & Configuration

When you first boot up your Windows 10/11 IoT LTSC 10ZiG Thin Client, you are automatically logged in as "Administrator" with the password "admin."

Installing Your Preferred VDI/DaaS Applications

With 10ZiG Windows 10/11 IoT LTSC Thin Clients, you have the ability to install your favorite VDI/ DaaS apps, locally or remotely. Click this link to find out more at the end of this section.
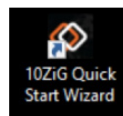
Components Included:

- Thin Client Device
- Power Supply
- USB Wheel Mouse

- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

The 10ZiG Quick Start Wizard

You will notice that the "10ZiG Quick Start Wizard" is loaded on the desktop or can be launched from the desktop icon above. This wizard gives you the ability to personalize your thin client and fully configure your device. Anything from creating custom user shells, to run a single application at startup, to filtering out specific keyboard shortcuts and "hotkeys" and even creating specific VDI connections with shortcuts that you can fully customize to your user's needs Within the Administrator account, you can set up specific applications and configure the unit for use with the secure, locked down "ThinClientUser" account. Let's discover some of the Quick Start Wizard's useful features over the next few.

## The Quick Start Wizard's Main Control Panel
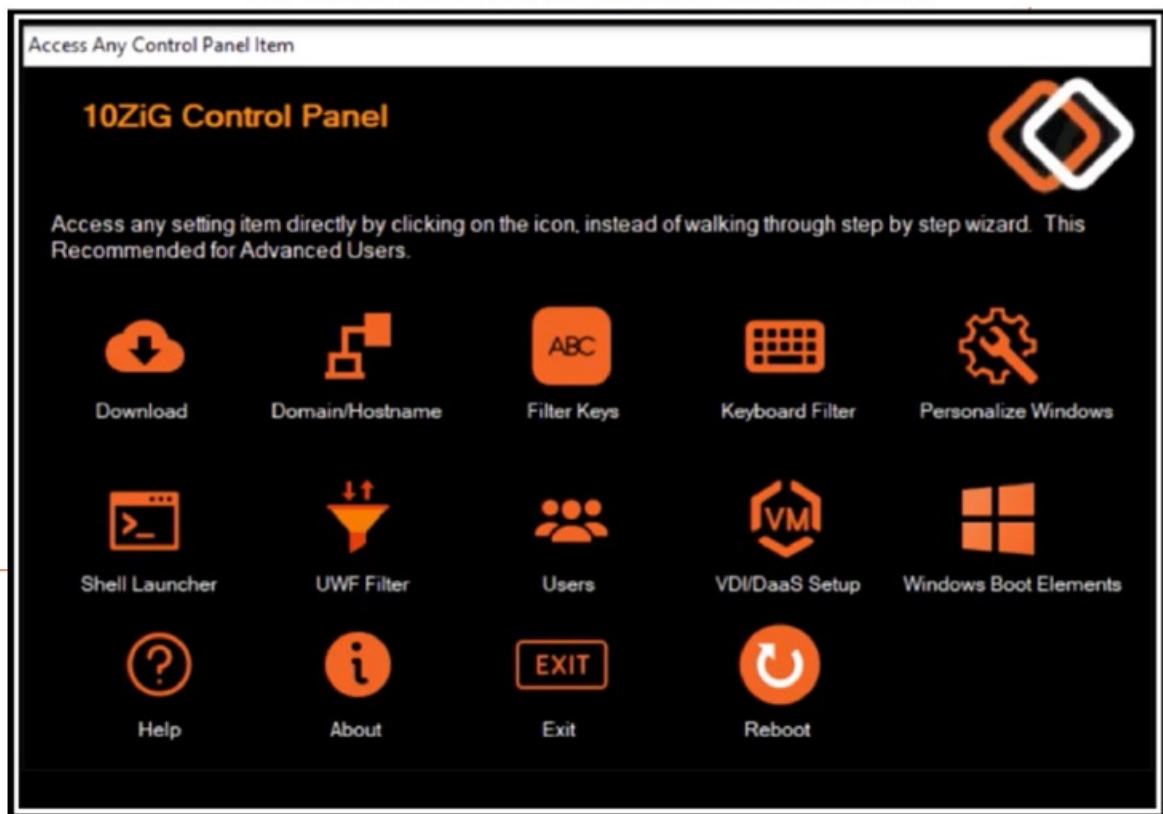
Creating a Custom Shell Experience

10ZiG has completely embraced the ability to securely build and manage your user'sdesktop and the Quick Start Wizard enables system Administrators to further configure the Windows 10/11 Thin Client to meet your own specific business needs. If you want a more specific and controlled desktop, then the "Shell Launcher" option gives you the ability to set up your user session, so it only launches a single application at logon. This gives your System Engineers and Administrators a more stable environment to manage, maintain, and modify. The following example shows a typical setup to create a dedicated AVD connection for your ThinClientUser that will run only this app during login. This simple 4-step process will get your ThinClientUser to automatically logon and run a single Remote Desktop Client app, in just a few minutes. This will enable you to connect to your AVD and Windows 365 cloud PC desktops.
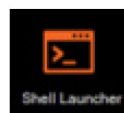
- Inside the 10ZiG Control Panel, click the "Shell Launcher" icon and you'll see 4 menu options appear.
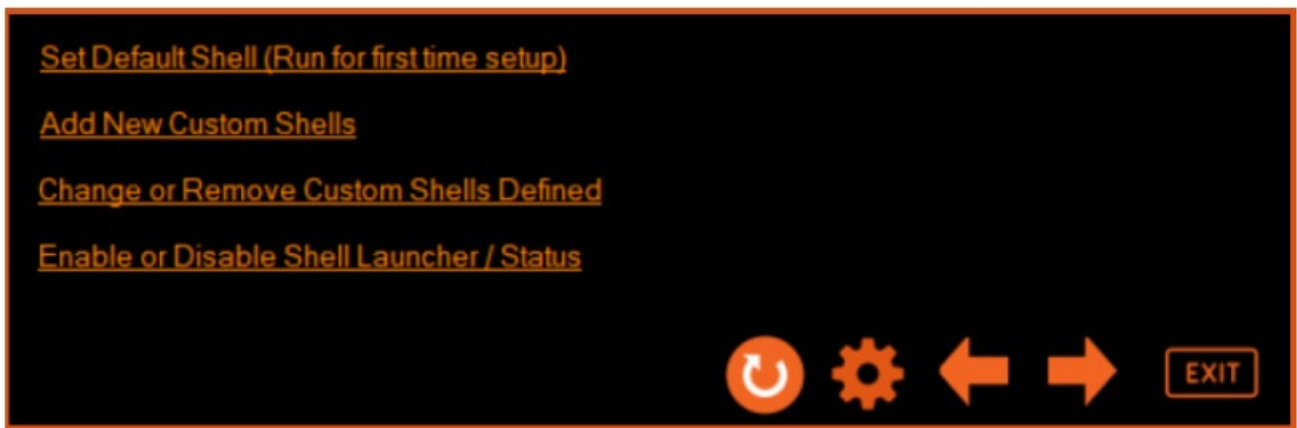
Before we set up our ThinClientUser single app at login, we must first set a default shell so that administrators still have a reliable user shell environment to be able to manage the machine in the unlikely event of a problem occurring.

STEP 1

Setting a Default Shell

- Inside the "Shell Launcher Settings" screen, click on the"Set Default Shell" menu option
- Click "Open File", browse to "C:\Windows\ Explorer.exe", highlight this and click "Open"
- Now, you will see the file named "C:\ Windows\Explorer. exe" in the "Shell Executable" field.
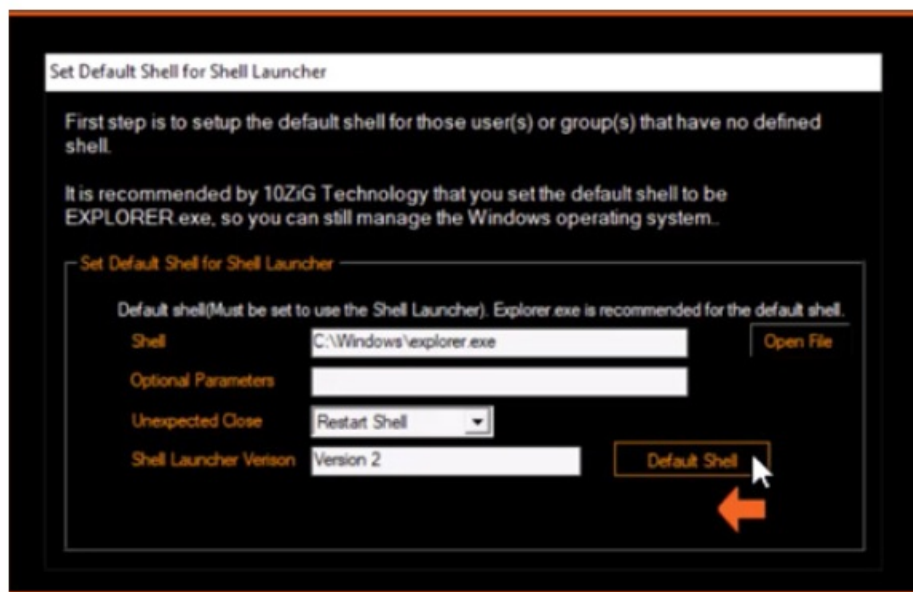
- Click "Default Shell" and you will be asked if you are sure to set this shell as default.
- Click "Yes" and the "OK" when the default path is set

- Click the right "orange" arrow that now appears, to move on to setting the shell executable
- (We have 3 more steps to complete before we need to reboot)

STEP 2

Creating a Custom User Shell

- We need to locate our custom shell and assign it to our specific user.
- Click on the "User" drop-down list in the "User or Group Shell Launcher" section
- From the list, click on the user named "ThinClientUser"
- Now that we have our user, we need to find our application to run at login. Click "Open File", browse to "C:\Program Files\Remote Desktop\msrdcw.exe", highlight this and click "Open"
- Your desktop should look something like this below:
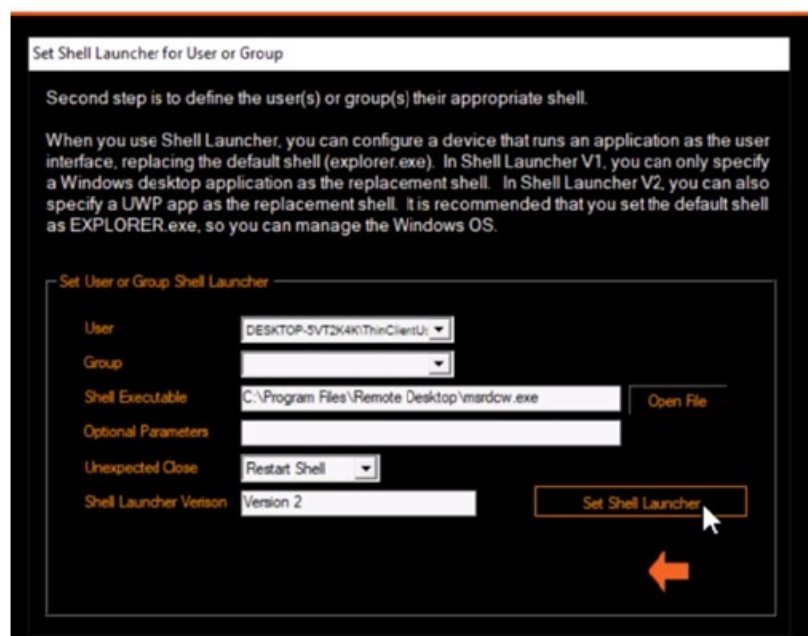
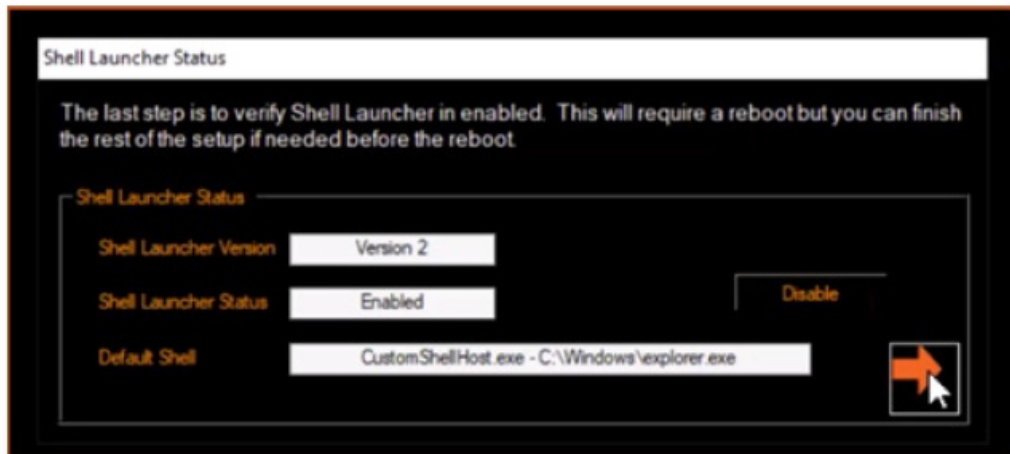- Click "Set Shell Launcher" and answer "Yes" when you are sure

- Click "OK" when the success message appears and click the right "orange" arrow again.

STEP 3

Checking the status of Windows Shell Launcher 2

This screen shows you the status of the "Shell Launcher" and should be set automatically once you have completed the previous 2 screens.
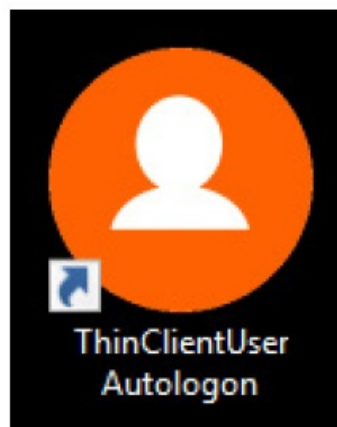

STEP 4

**Set Up Your 10ZiG Windows 10/11 IoT LTSC Device to Automatically logon as ThinClientUse**

Now we can get this device to logon automatically as ThinClientUser each time it boots up.

- "Double-click" the "ThinClientUser Autologon" icon on the "Administrator" desktop

- You will be asked inside a command window, the question "Thin Client will restart now : Press Y to restart N to cancel [Y/N]"
- Press "Y", then the command window will close and the Client will reboot.
- Once the device has rebooted, you will see it automatically log on as ThinClientUser as shown below:
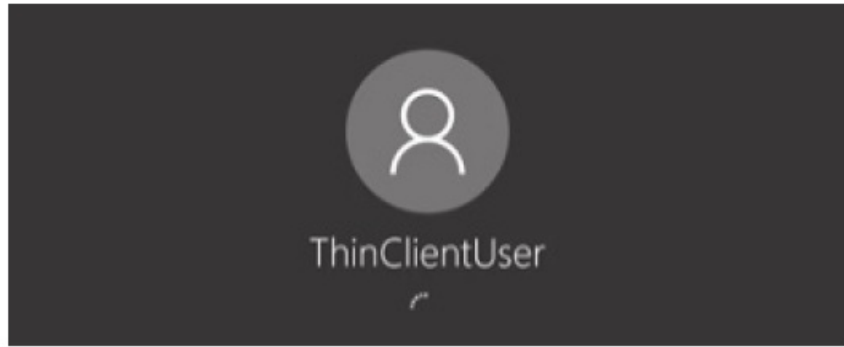
- When the user has logged on, you can see there is only one application running and this is the msrdcw.exe that allows us to login to our AVD and Windows 365 cloud PC desktops.
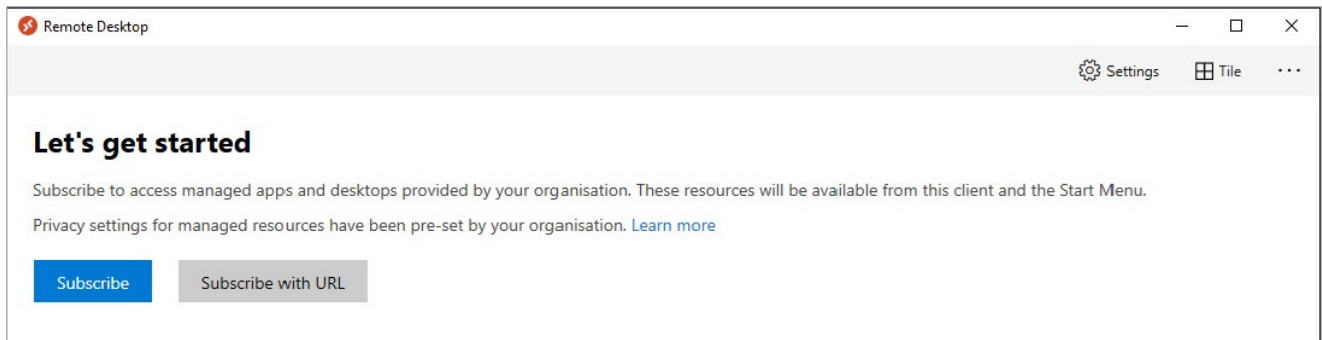

Boot Screens

### Customization of Welcome, Lock, and Boot Screens

The "Quick Start Wizard" also gives you the ability to configure welcome, lock, and boot screens and a whole host of keyboard hotkeys and shortcuts.

- Inside the 10ZiG Control Panel, click the "Windows Boot Elements" icon and you'll see several menu options appear
- Click the menu option named "Welcome Screen UI Elements" and you'll see several tick boxes that allow you to show or hide "Welcome", "Lock" and "Boot" screen content
- Tick the boxes named "Remove Power" and "Remove Network" and click "Apply", as shown below
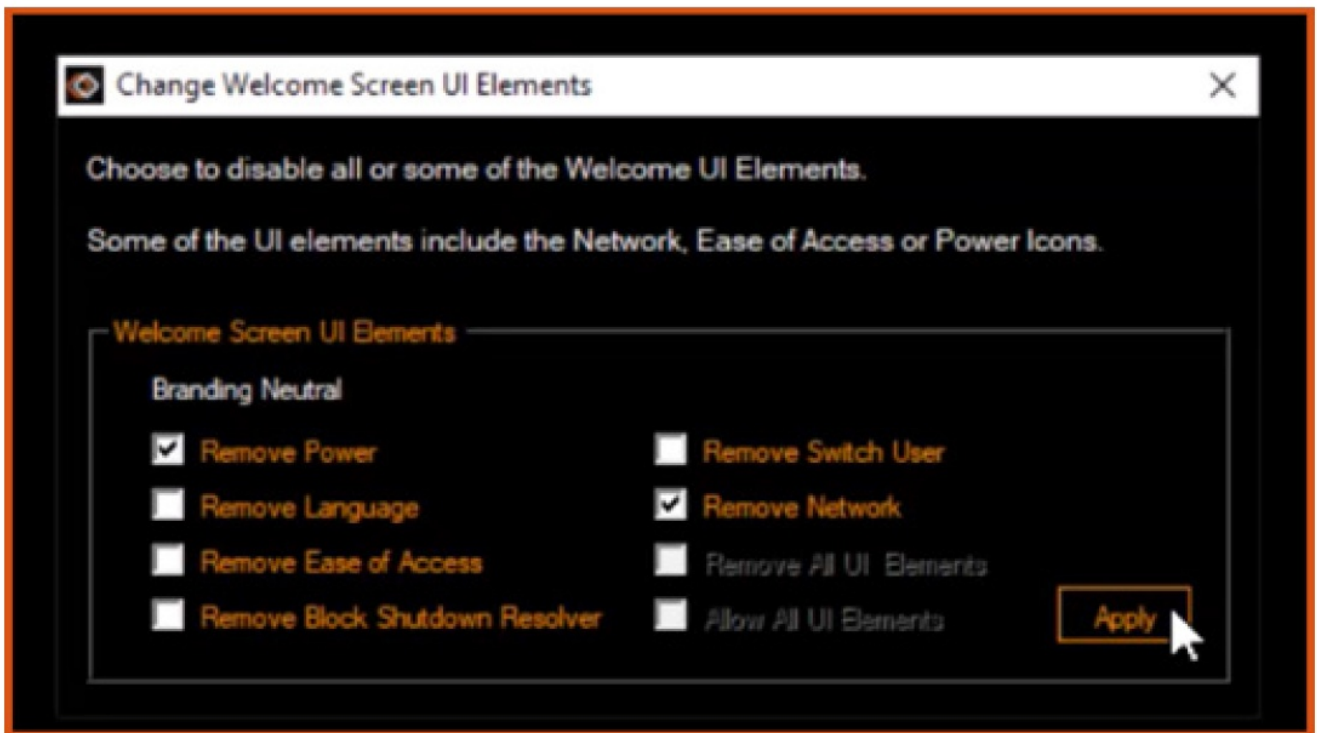
- When you press CTRL+ALT+DEL to go to the lock screen, the power button and network settings icons have been removed from user access and only "Ease of Access" is shown
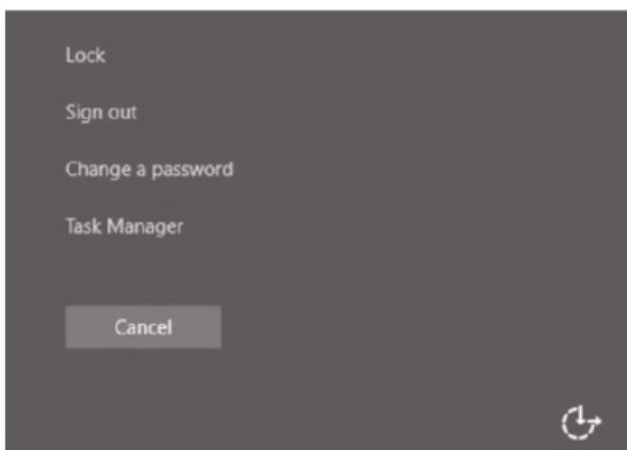
- Removing the power option is useful if you want to prevent the user from powering off the 10ZiG unit if it's performing as a public kiosk or digital signage product and the physical power switch is out of reach. The removal of network settings isn't compromised either, by preventing unwanted users from changing them, thus maintaining network connectivity.

Customization of Windows Keyboard Functions

Here we show you how to secure the Thin Client desktop by preventing your users from being able to access the "Task Manager" during a session, thus preventing them from being able to stop any running apps and start new ones.
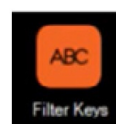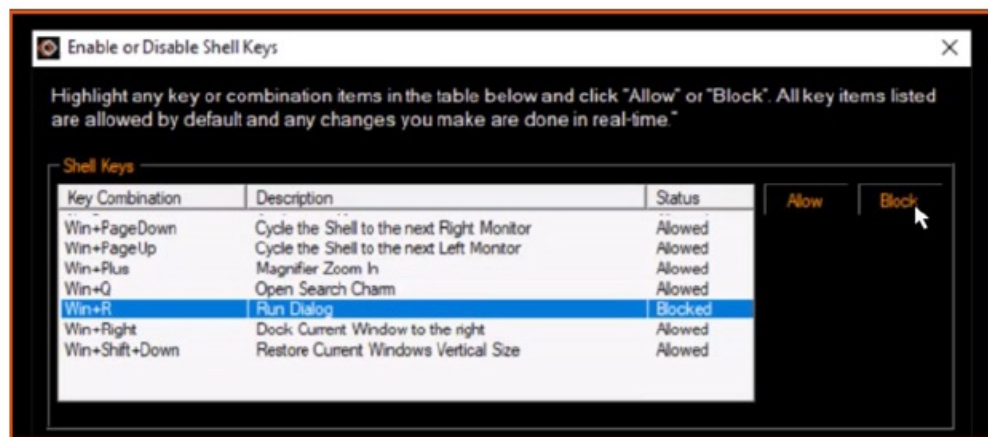
- Inside the 10ZiG Control Panel, click the "Filter Keys" icon and you'll see several menu options appear
- Click the menu option named "Setup Security Keys"

- Highlight the setting with the key combination "Shift+Ctrl+Esc", and a description of "Task Manager" and then click the "Block" button next to it. This will prevent any further action of Shift+Ctrl+Esc, launching the "Task Manager"
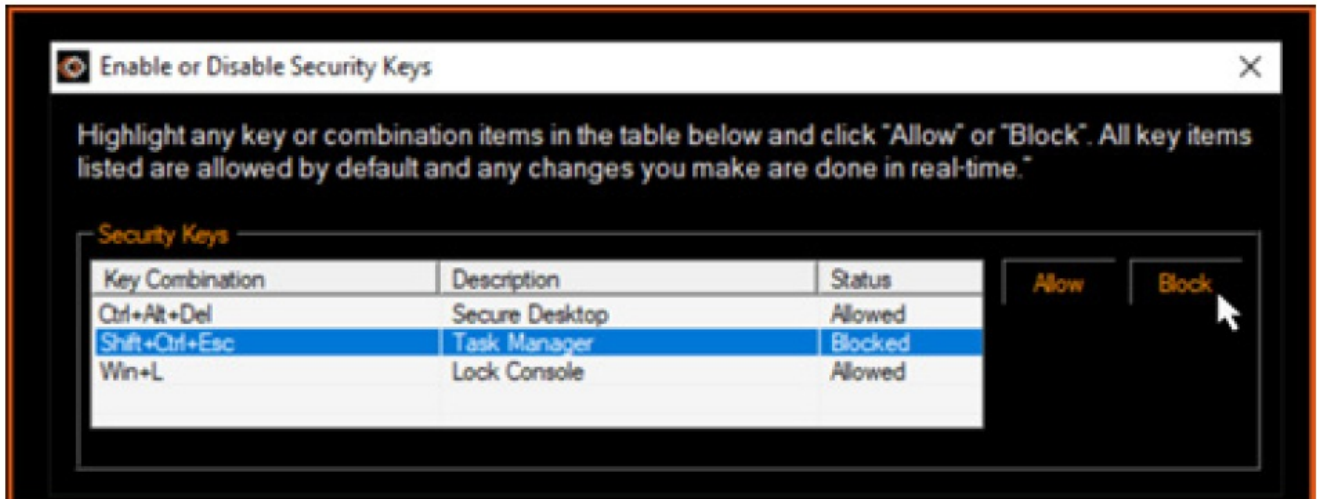

- Still within the "Filter Keys" menu, here's an example of how to prevent your users from using the "Windows key" + "R", that would normally launch the "Run" dialog box.
- Click the menu option named "Setup Shell Keys"
- Highlight the setting with the key combination "Win+R", and a description of "Run Dialog" and then click the "Block" button next to it. This will prevent any further action of Shift+Ctrl+Esc, launching the "Task Manager"

We don't want to apply these restrictions to our system Admin users, however, so the "Quick Start Wizard" allows us to bypass these restrictions as shown here.

- Inside the 10ZiG Control Panel, click the "Keyboard Filter" icon and you'll see three menu options
- Click the menu option named "Set Keyboard Filter for Administrator Accounts" and you'll see that it is "Disabled" by default. When you enable this option, any keyboard-specific filters will not be applied to Administrator accounts or groups, as shown below.
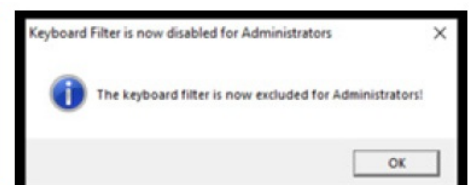
Microsoft's Unified Write Filter

10ZiG's "UWF Wizard" was designed to help you to manage Microsoft's "Unified Write Filter" that comes as part of Windows 10/11 IoT LTSC. It prevents data from being transmitted to specific areas of your physical storage and Windows registry – even bypassing your storage altogether, only using RAM as a temporary location.

UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. The UWF provides a clean experience for Thin Clients and workspaces that have frequent guests, like school, library, or hotel computers. Guests can work, change settings, and install software. After the device reboots, the next guest receives a clean experience.It increases security and reliability for kiosks, IoT-embedded devices, or other devices where new apps are not expected to be frequently added. "UWF Servicing Mode" is a feature of the UWF that allows you to run bulk Windows Updates, out of normal operating hours and gives full access to file and folder locations, that would otherwise be difficult for exclusions to manage alone. The "UWF Wizard" has this option built in, so that you can control "Servicing Mode" from within the console or from the command line. 10ZiG has written a comprehensive guide that explores Microsoft's UWF, entitled "Discovering_Microsofts_UWF_on_10ZiG_Windows_10_IoT_ LTSC_2021_Thin_Clients.pdf" and can be downloaded from the 10ZiG website at **https://www.10zig.com/10zig-uwfconfig1/**


Installing VDI/DaaS Applications for your 10ZiG Windows 10/11 IoT LTSC Thin Clients – Locally or Remotely

You have flexibility when it comes to installing your favorite VDI/DaaS apps on your 10ZiG Thin Client. You can visit the vendor's website for client downloads and install it locally if you wish. If you prefer to install your VDI/DaaS apps remotely on the other hand, then the 10ZiG Manager Web Console gives you the ability to custom build your favorite VDI/DaaS client into a Windows installer package, ready for deployment to your 10ZiG Windows 10/11 IoT LTSC devices. The Package

Manager's wizard takes you step by step through the installer build process and even accommodates the Windows 10 Unified Write Filter (UWF), if your devices are using this as part of their infrastructure. Click this link to download the more comprehensive 10ZiG guide to building and deploying your own VDI/DaaS installers. **Installing VDI-DaaS Applications on Windows 10 IoT LTSC 2021 Thin Clients.pdf**
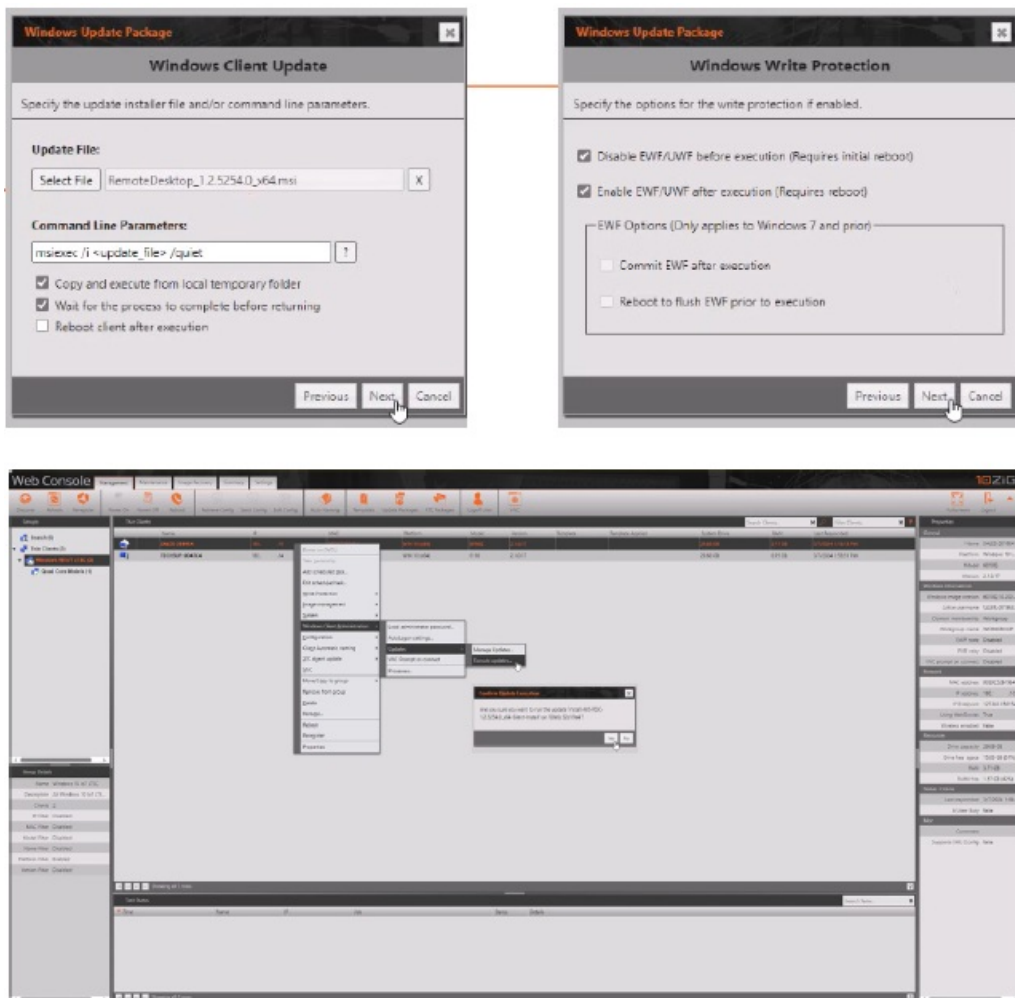
Requirements

The Trusted Zero Client must connect to and register with an Anyware Trust Center before it can connect to PCoIP sessions. 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 VMware 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.

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 anywaretrust center DNS route has already been configured by your IT administrators.

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 a 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 the front power button to power on the trusted zero client.
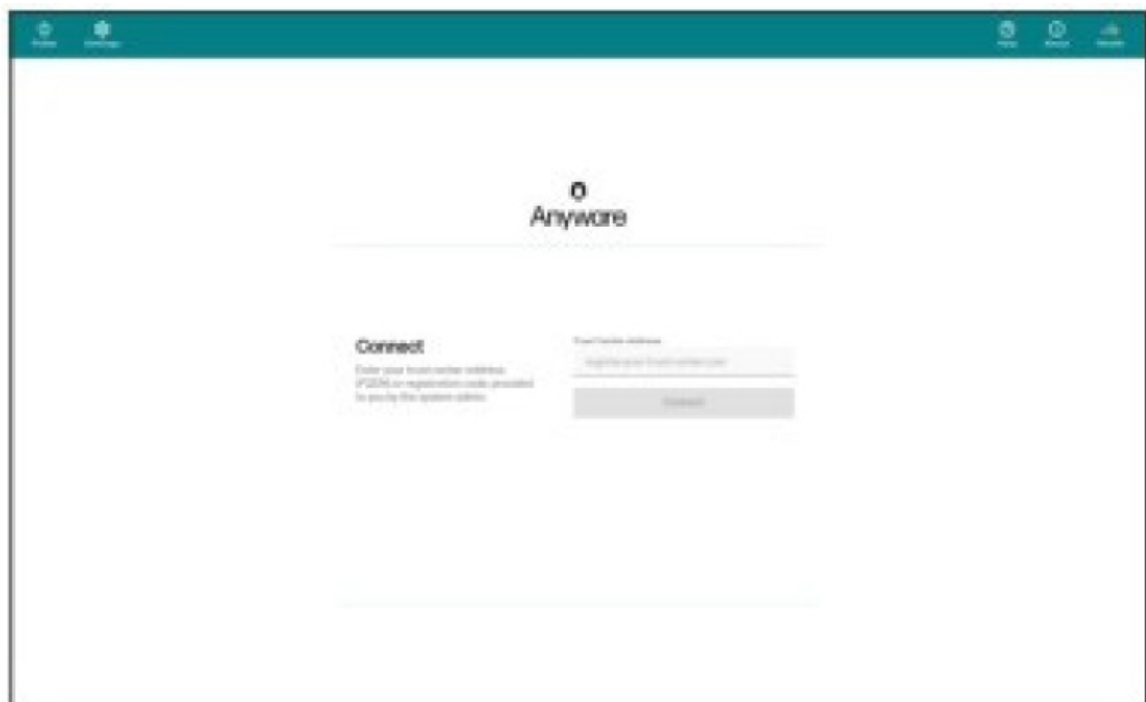
Setting up Your Trusted Zero Client

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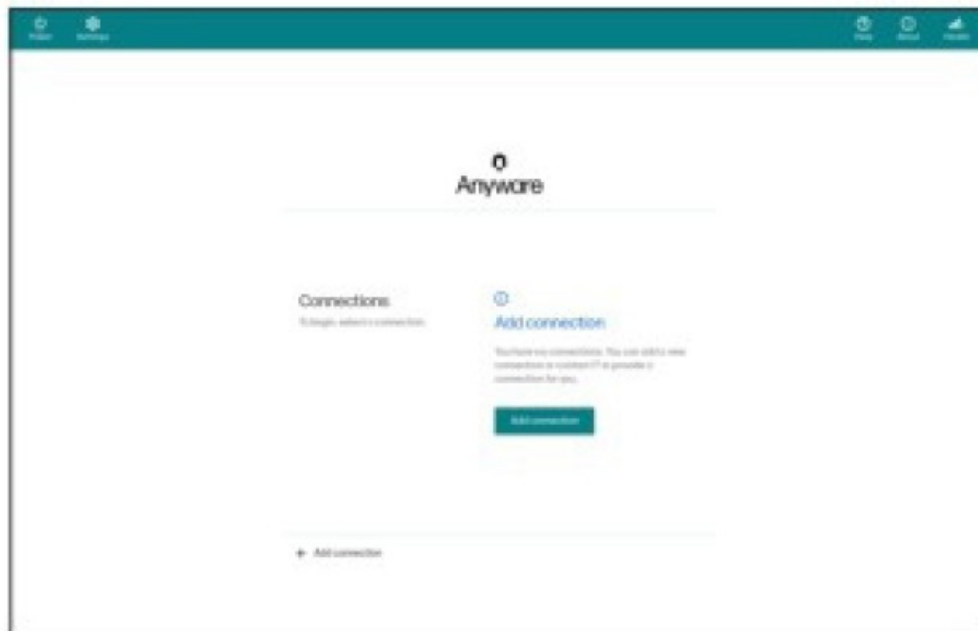
4. Once you have selected your desktop, you will be connected to it and your remote session will begin. The first time you connect to a desktop, there may be a slight delay before the connection is active.

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.

Installation is Going To Be Easy

Deploy and start managing in under an hour. A single-manager server-based installation, along with optional remote consoles, provides automated discovery and centralized device configuration. The 10ZiG Manager WebConsole allows management of your clients from all major browsers (Edge, Chrome, and Firefox), providing real-time status of all clients from a single comprehensive.

FAQs
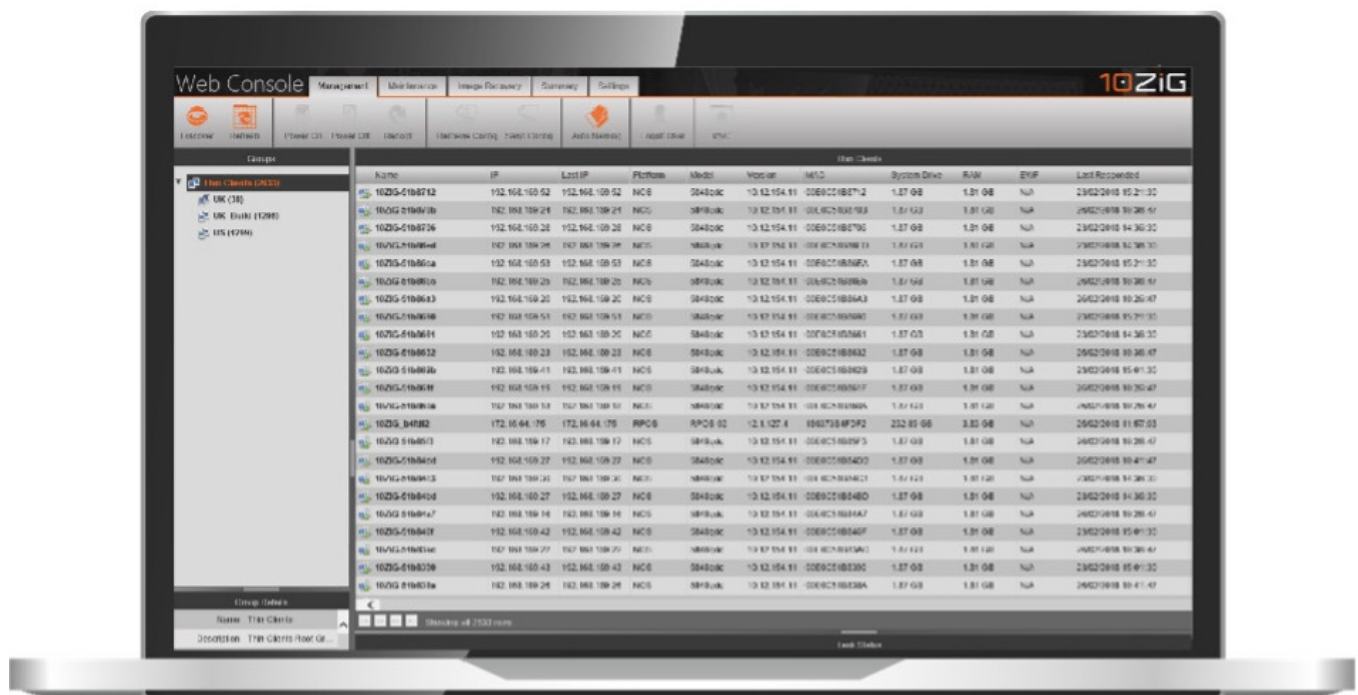
CLOUD MANAGEMENT TECHNOLOGY?

- **Yeah, We've Got That**
  - Our Secure Management Technology supports internet connectivity and manages locations like smaller offices and home-based networks. End users deploying VDI, SessionVirtualization, or Published Applications, not to mention Managed Service Providers, offering DaaS, SaaS, UCaaS, etc., are able to manage endpoints via the Cloud.

SAFE AND EFFICIENT CONNECTIVITY?

- **Wouldn't Have It Any Other Way**
  - The 10ZiG Manger utilizes SSL encryption with secure logins verified against your Active Directory domain with timeouts for user inactivity and failed login attempts. Detailed installation guide and pictures ensure the 10ZiG Web Console is installed right the first time.

GROUP MANAGEMENT & CONFIGURATION?

- **We Have This Covered**
  - Whether manually or automatically populated, organized groups provide a simple, logical way to configure, monitor, and manage devices. The 10ZiG Web Console provides a web-based configuration tool to manage clients, remote access with VNC* and apply firmware updates.

How Do I Install the 10ZiG Manager?

- The 10ZiG Manager is the easiest and most straightforward client management software on the market today. Please see the below link for our 10ZiG Manager Setup Guide:
  - **[10ZiG Manager Setup Guide](#)**

10ZiG FAQ SITE:

- **Do You Have Questions?**
  - Of course, you do! We're here to help. Many frequently asked questions can be answered at our Support FAQ site page:
    - **[Support & FAQ's](#)**
  - Once there, search by keyword or product type for helpful information. While you're there, sign up to receive 10ZiG Technology & Firmware Updates!
    - **[Sign Up Here](#)**
  - Not to worry, if you're really stumped, we've got your back at **support@10ZiG.com** for the US, Canada, and South America or **support@10ZiG.eu** for EMEA.

Warranty

The 10ZiG Thin & Zero Client Warranty is one of the best standard warranties in the marketplace today. Our units are covered by a comprehensive 3-year advance hardware exchange warranty (return freight is also covered), 3 years of technical support (by our US or UK-based VMware, Citrix, MS Certified support team), and 3 years of

software upgrades.

- **Full U.S. Product Warranty**
- **Full EMEA Product Warranty**

- **Check Our Our Product Brochure Video**
- **www.10ZiG.com**

Documents / Resources

	10ZiG 4610q Thin and Zero Client Hardware and Software [pdf] Installation Guide 4610q, 7010q, 7110q, 7510qTAA, 7910q, 4610q Thin and Zero Client Hardware and Software, 4610q, Thin and Zero Client Hardware and Software, Client Hardware and Software, Hardware and Software, Software

References

- 1⊡ **Thin and Zero Client Hardware & Software | 10ZiG**
- **User Manual**