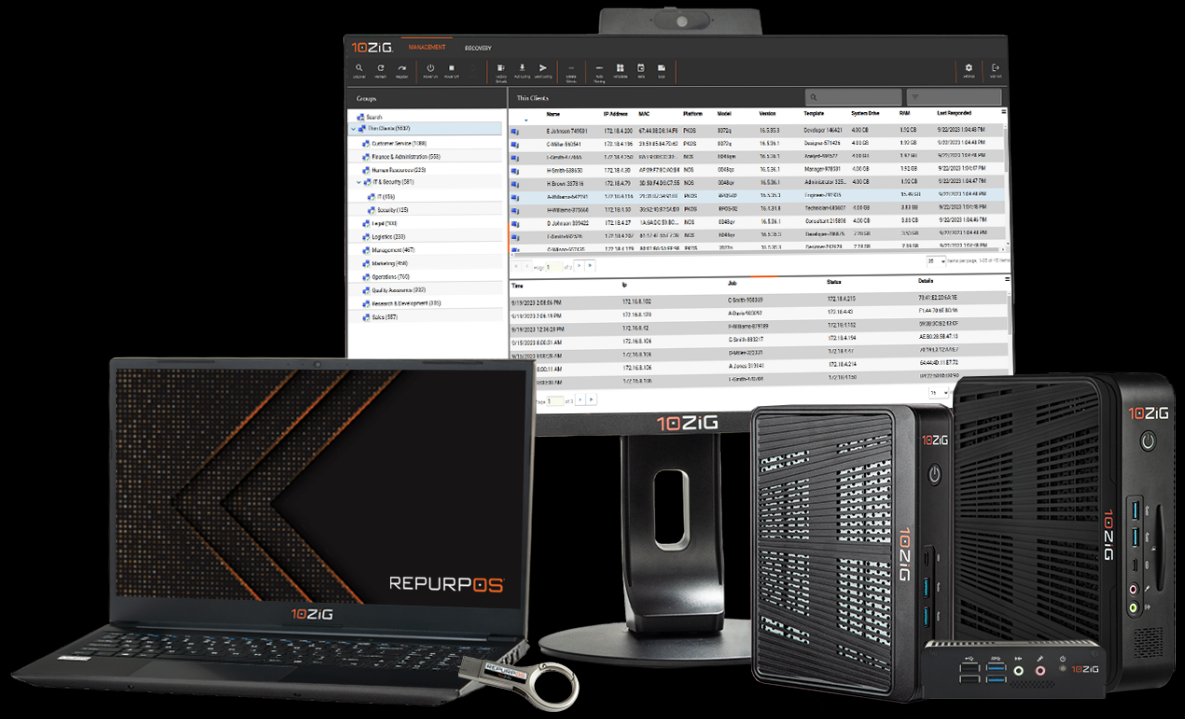
10ZiG®

VDI | DaaS | SaaS | Web Apps

Modernized Thin & Zero Client Hardware and Software

WELCOME TO THE 10ZiG INSTRUCTIONAL GUIDE



Setup Instructions for Windows, PeakOS™ (Linux), and NOS™

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

SECURE MANAGED FLEXIBLE

10ZiG

NOS PEAKOS REPURPOS MANAGER

JUST GETTING TO KNOW US?

Let's Get You Up and Running with the Modernization of 10ZiG Thin & Zero Clients

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 leader of Modernized Thin & Zero Client endpoints, Repurposing Software, and Management Software for Cloud Workspaces and Virtual Desktops, our Single-Vendor Full Service strategy is geared to suit all user types from task worker to power use, in any virtual desktop environment – in office, remote, or for hybrid working.

The devices and management you want, plus the service you've always wished for:

10ZiG Technology offers a wide selection of powerful, reliable, easy-to-manage, and affordable Modernized Thin & Zero Client hardware and software solutions. Our carefully custom-imaged devices are built to provide the best performance possible in VDI and server-based applications/desktops for hosted and Cloud environments.

10ZiG Thin & Zero Clients are available with either Thin (PeakOS™) or Zero (NOS™) client firmware, or Windows 11 IoT LTSC. We are certified for and/or support Omnissa, 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!

10ZiG 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 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 beat... 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, and NOS™ Zero Clients.

THIN CLIENTS FOR WINDOWS 11 IoT LTSC

(Models 4611q, 7011q, 7311q, 7111q, 7511qTAA, & 7911q)

Initial Setup & Configuration

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

Installing Your Preferred VDI/DaaS Applications

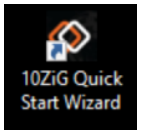
With 10ZiG Windows 11 IoT LTSC Thin Clients, you have the ability to install your favorite VDI/DaaS apps, locally or remotely. Click this link to find out more at the end of this section.

Components Included:

- Thin Client Device
- Power Supply
- Desktop Stand
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

10ZiG

The 10ZiG Quick Start Wizard

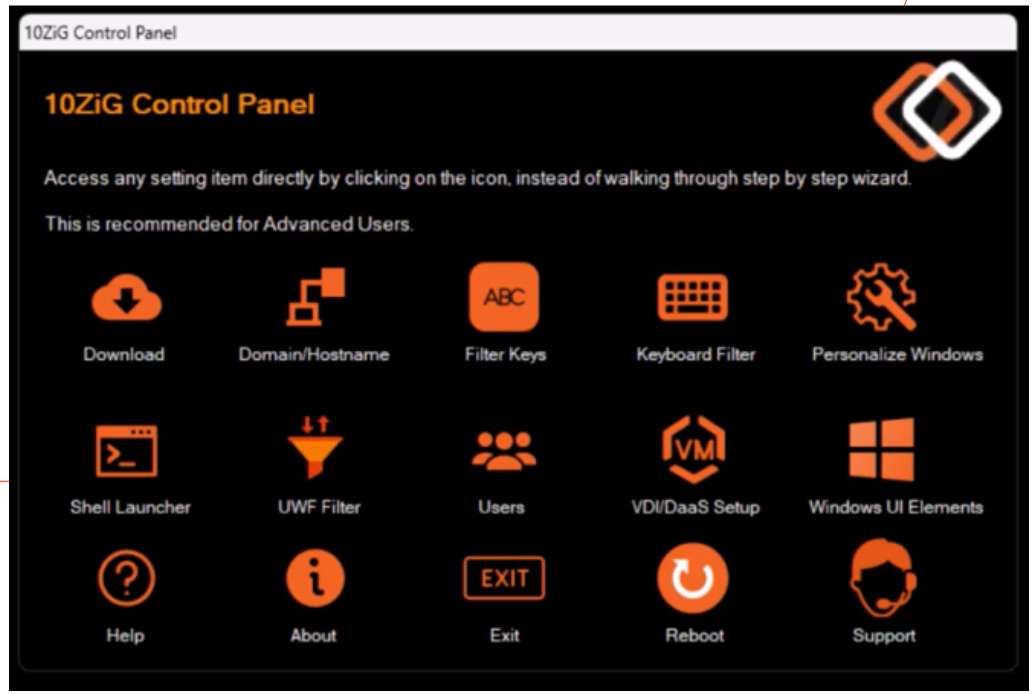


You will notice that the “10ZiG Quick Start Wizard” is loaded on the desktop or can be launched from the desktop icon above. This wizard gives you the ability to personalize your thin client and fully configure your device. Anything from creating custom user shells, to run a single application at startup, 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 pages.

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's desktop and the Quick Start Wizard enables system Administrators to further configure the Windows 11 Thin Client to meet your own specific business needs.

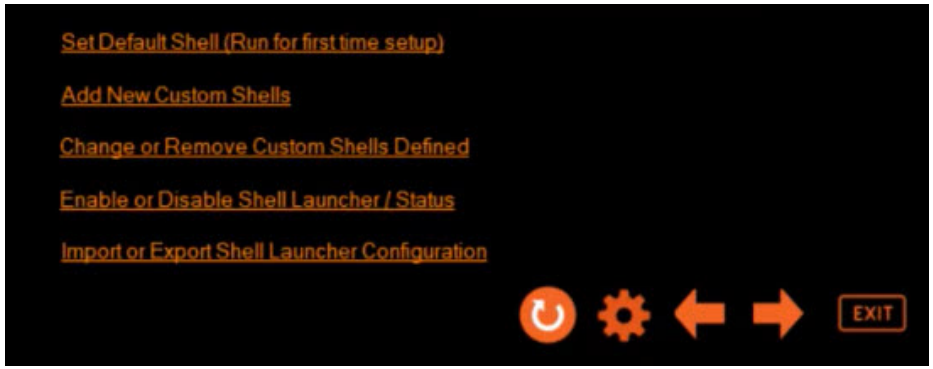
If you want a more specific and controlled desktop, then the "Shell Launcher" option gives you the ability to setup your user session, so it only launches a single application at logon. This gives your System Engineers and Administrators a more stable environment to manage, maintain, and modify.

The example on the following pages shows a typical setup to create a dedicated locked-down Microsoft Edge browser connection. The connection will be configured to launch the "Windows App" web client in a fullscreen kiosk on your ThinClientUser that will run only this app during logon.

This simple 4-step process will get your ThinClientUser to automatically logon and run this single "Windows App" web client, in just a few minutes. The Windows App can connect to Cloud PCs, Azure Virtual Desktop sessions, Remote Desktop Services, and remote PCs managed by your organization.

- Inside the 10ZiG Control Panel, click the "Shell Launcher" icon 

and you'll see 5 menu options appear.

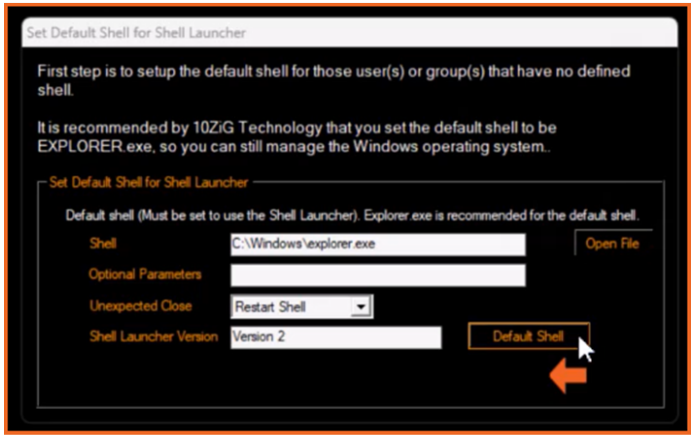


Before we set up our ThinClientUser single app at logon, we must first set a default shell so that administrators still have a reliable user shell environment to be able to manage the machine in the unlikely event of a problem occurring.

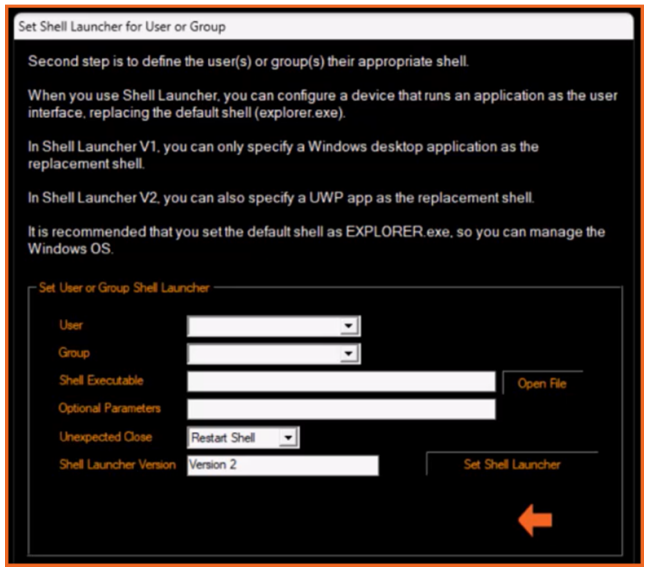
STEP 1

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 the Microsoft Edge browser application to run at login. Click “Open File”, browse to “C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe”, highlight this and click “Open”
- To setup the Edge browser to launch the “Windows App” web client, when it starts, you need to add the following text to the Optional Parameters field:

  --kiosk https://windows.cloud.microsoft/ --edge-kiosk-type=fullscreen --no-first-run --fast-start –guest

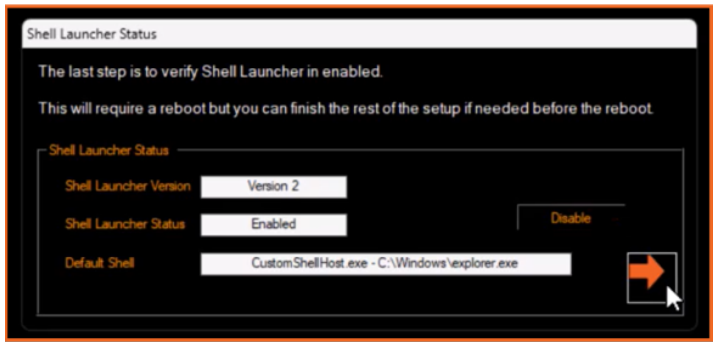
- Your desktop should look something like this below:

- 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.



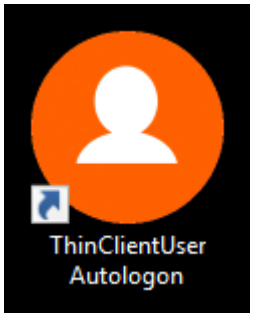
- To complete the shell setup, just click the right “orange” arrow and you’ll return to the “Shell Launcher” main menu.

STEP 4

Set Up Your 10ZiG Windows 11 IoT LTSC Device to Automatically logon as ThinClientUser

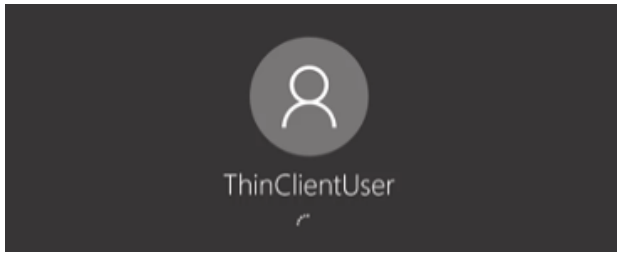
Now we can get this device to logon automatically as ThinClientUser each time it boots up.

- “Double-click” the “ThinClientUser Autologon” icon on the “Administrator” desktop

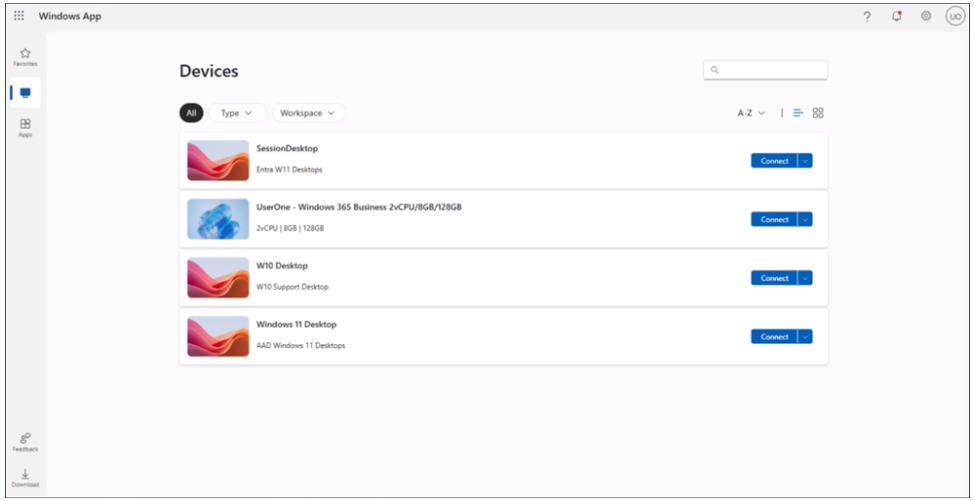


- You will be asked inside a command window, the question “Thin Client will restart now : Press Y to restart N to cancel [Y/N]”
- Press “Y”, then the command window will close and the Client will reboot.

Once the device has rebooted, you will see it automatically log on as ThinClientUser as shown below:



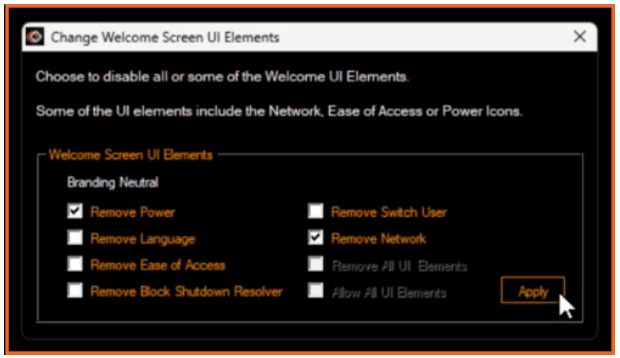
When the user has logged on, you can see there is only one application running and this is the Microsoft Edge Browser that allows you to login to your “Windows App” web client and gain access to Cloud PCs, AVD sessions, Remote Desktop Services, and remote PCs managed by your organization.



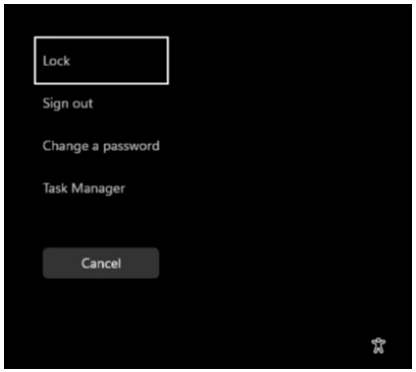
Customization of Welcome, Lock, and Boot Screens

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 UI 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

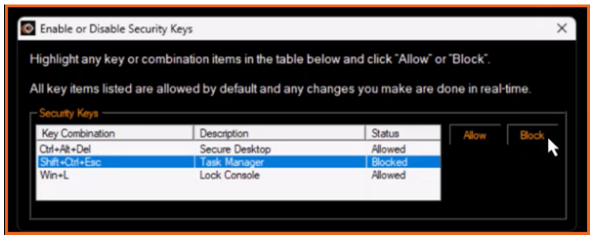


Removing the power option is useful if you want to prevent the user from powering off the 10ZiG unit if it’s performing as a public kiosk or digital signage product and the physical power switch is out of reach. The removal of network settings isn’t compromised either, by preventing unwanted users from changing them, thus maintaining network connectivity.

Customization of Windows Keyboard Functions

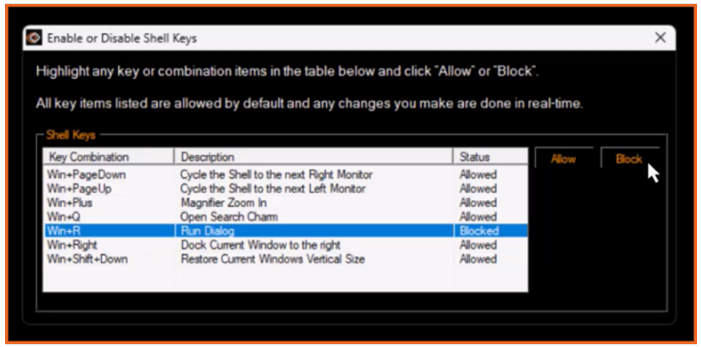
Here we show you how to secure the Thin Client desktop by preventing your users from being able to access the “Task Manager” during a session, thus preventing them from being able to stop any running apps and start new ones.

- 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 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.

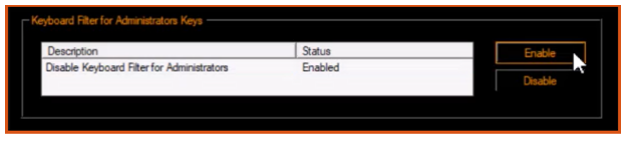
- Click the menu option named “Setup Shell Keys”
- Highlight the setting with the key combination “Win+R”, and description of “Run Dialog” and then click the “Block” button next to it. This will prevent any further action of “Windows key” + “R” key combination, from launching the “Run” dialog box

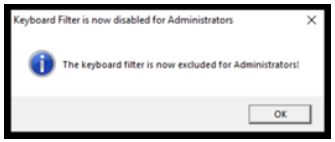


We don't want to apply these restrictions to our system Admin users however, so the "Quick Start Wizard" allows us to bypass these restrictions as shown here.

- 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 11 IoT LTSC. It prevents data writes 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.

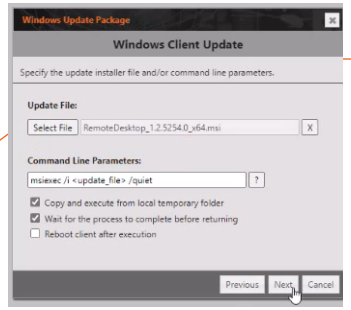
10ZiG have a comprehensive guide that explores the UWF for Windows 11 IoT Enterprise LTSC 2024 in more detail and can be downloaded from the 10ZiG website at https://www.10zig.com/10zig-uwfconfig1/

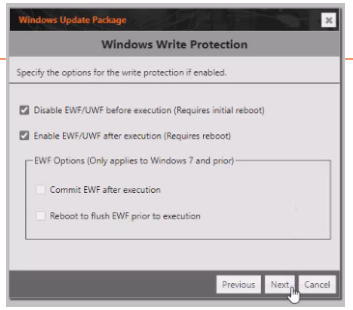
Windows 11 IoT LTSC VDI-DaaS Apps Installation

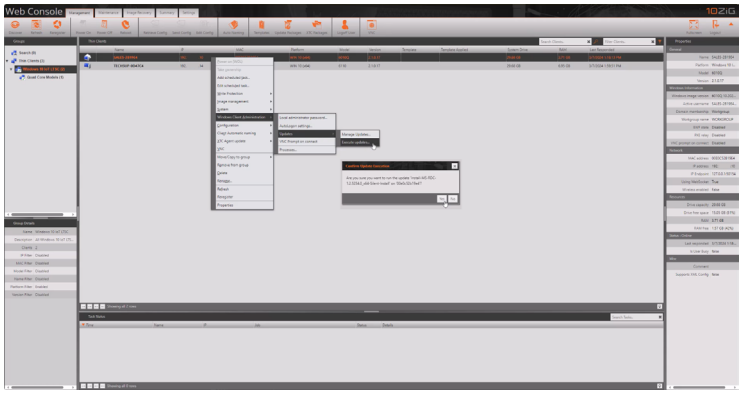
Installing VDI/DaaS Applications for your 10ZiG Windows 11 IoT LTSC Thin Clients - Locally or Remotely

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 11 IoT LTSC devices.

The Package Manager's wizard takes you step by step through the installer build process and even accommodates the Windows 11 Unified Write Filter (UWF), if your devices are using this as part of their infrastructure.







PEAKOS™ (LINUX) THIN CLIENTS

(Models 4672q, 7072q, 7372q 7172q, 7572qTAA, & 7972q)

Components Included:

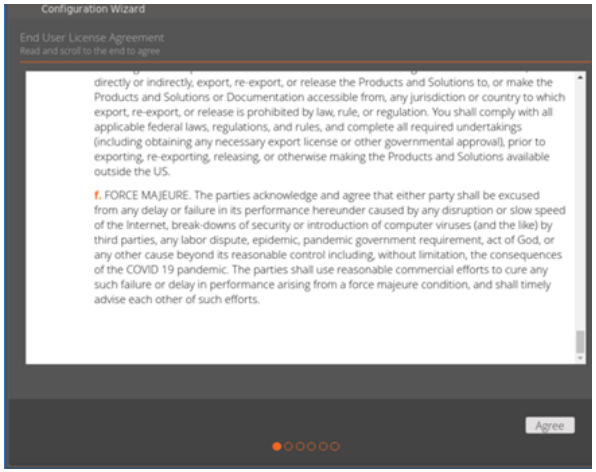
- Thin Client Device
- Power Supply
- Desktop Stand
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

Initial Boot-Up

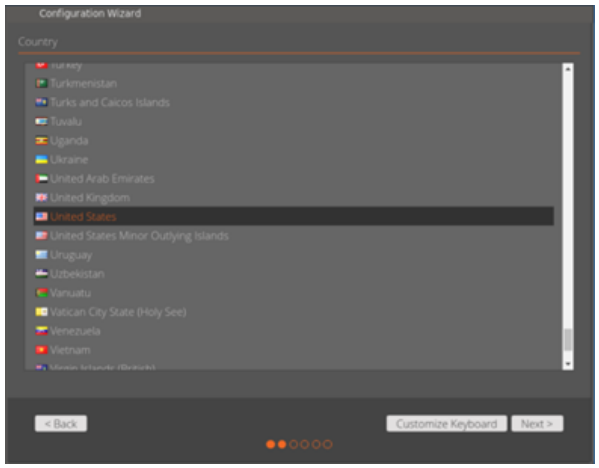
Upon initial boot-up, the “Configuration Wizard” will be launched.

Configuration Wizard

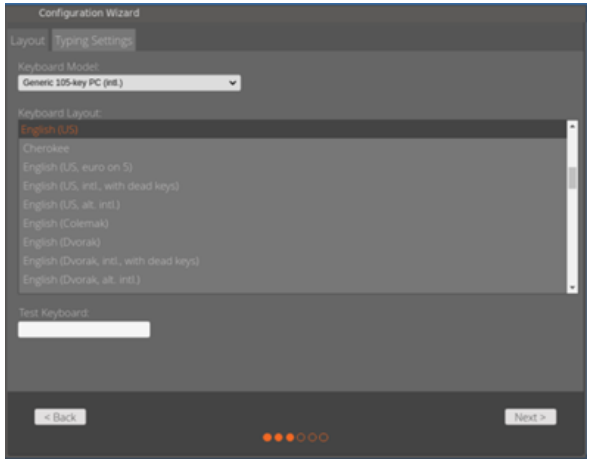
The Configuration Wizard is a series of screens that will allow you to customize PeakOS™ to suit your own time zone, region, and keyboard layout settings. The first screen in this series is the End User License Agreement. You will need to scroll down in order to click “Agree” and move on to the next wizard screen in the series.



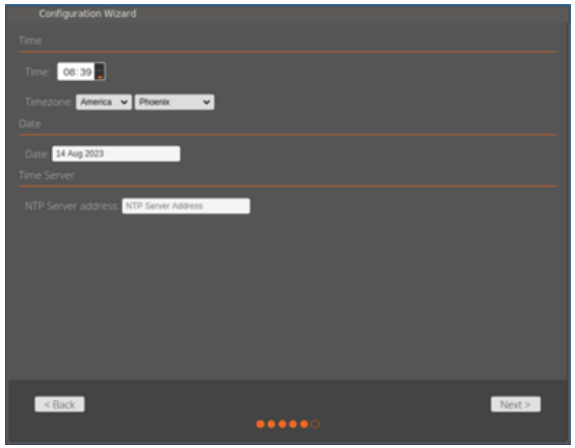
Once you have agreed to this disclaimer, you will be taken to the next “Configuration Wizard” screen, that allows you to select your “Country” of residence.



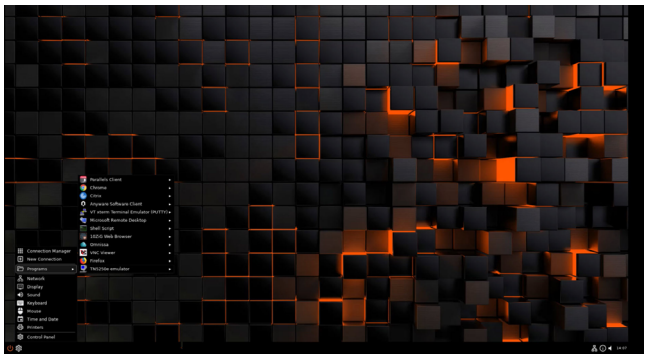
Once you’ve done this, you either have the option to click “Customize Keyboard” or move on to the next “Wizard” screen. If you click “Next” at this point, your keyboard will be set as a standard keyboard and layout that is typical to your country. If you click “Customize Keyboard” then you’ll be presented with the options to further customize the layout and any additional typing settings.



Once you’re happy with any changes in here, then click “Next” and you’ll be taken to the time zone configuration screen, where you can manually set the time zone, date, and also specify a particular time server location, if you wish.



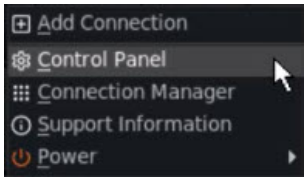
If you click “Next” on this screen, then you’ll see a message showing that the “Wizard” was completed, and you’ll be presented with the desktop.

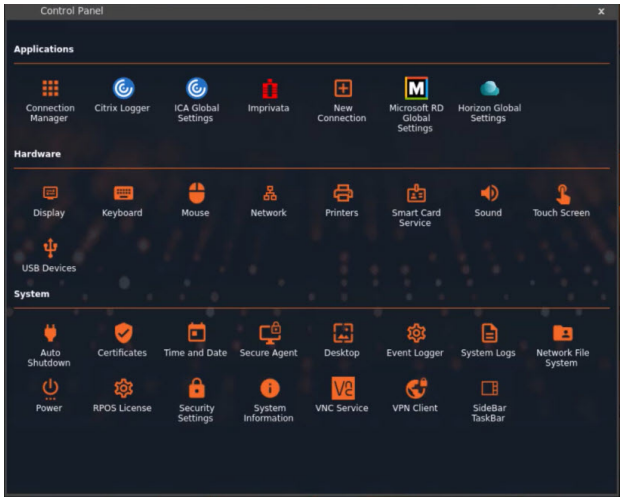


Control Panel

The Control Panel is where all your configuration items are located and categorized in 3 main areas, Applications, Hardware, and System.

To gain access to the control panel, either click on the “Gears” icon in the “Taskbar” and select the “Control Panel” item or right-click on the desktop and select “Control Panel” from the drop-down list.





Setting a Static IP Address and Wireless

1. Navigate to the Control Panel (using one of the methods above)
2. Click the Network icon, select Local Area, and click the Edit button
3. Go to the TCP/IP Properties tab and check the box “Use a Static IP”
4. Input your IP address, subnet mask and default gateway settings
5. Enter any DNS settings and click “OK” when you’re finished
6. If you have a wireless card installed, click the “Add” button and you’ll see which local wireless networks are available for you to connect to. If you need to find wireless connections again, just click the “Refresh” button.

   If you need to connect to a hidden wireless network, then click “Add hidden network”, type in the “SSID” of the hidden network and then click “OK”.
7. Enter your wireless settings including WEP/WPA/WPA2 keyWEP/WPA/WPA2 key

Configuring Applications

Your 10ZiG PeakOS™ Thin Client arrives with no connections pre-defined. You will need to manually configure the connections you wish to use. From the Connection Manager, click the “New” button, from the desktop, right-click and select “Add Connection” or from the taskbar, click the “Gears” icon > Programs and then select the program you wish to add.

Locking Down the Thin Client

Once you have added all the connections you need, you can lock the unit down to prevent changes from being made. This can be done either remotely by using “10ZiG Manager” or on the local device itself. Enter the “Control Panel”, click on the “Security Settings” icon, and tick the “Disable Connection Configuration” check box under the “System” settings heading. Then click “Require password to modify the terminal configuration”, and add a password to the unit to prevent any other users entering the control panel to edit settings. Once you have done this, click “Save”.

Auto Start Applications

Any connection can be set to automatically launch when the unit is powered on. You need to make sure that the client is not locked down before you try to do this.

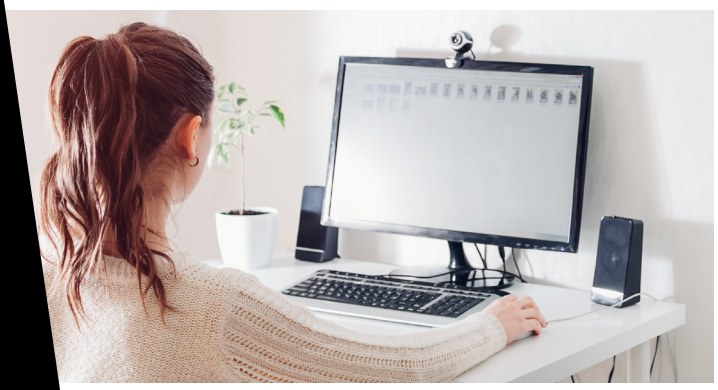
Right click on the connection icon that you wish to Auto-Start and select “Startup Options” from the context menu.

Once inside, tick the box labelled “Set this connection as Default connection”. If this connection type is RDP, Omnissa, or Citrix, you will also have the option to tick the check box for auto reconnect.

Access the Full User Guide here

NOS™ ZERO CLIENT FOR OMNISSA

(Models 4648qo, 7048qo, 7348qo, 7148qo, 7548qoTAA, & 7948qo)



Initial Boot-Up

Upon initial boot-up, once you click to agree the “End User License Agreement” the unit will attempt to configure the network settings, in the background using DHCP. You may continue through the remainder of the setup process by filling in the required information based on your preferences and geographical settings. On the following setup screens, you will be asked to complete your country location, the time zone you are in and the current time and date. These configuration screens are the same ones as mentioned previously in the PEAKOS section earlier in this guide.

You will now be presented with your Omnissa Horizon Settings to connect to your server.

Once you have completed these steps, you will be given a login dialog box to fill in your Username, Password and Domain settings to continue connecting to your Omnissa Horizon server.

Components Included:

- Zero Client Device
- Power Supply
- Desktop Stand
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

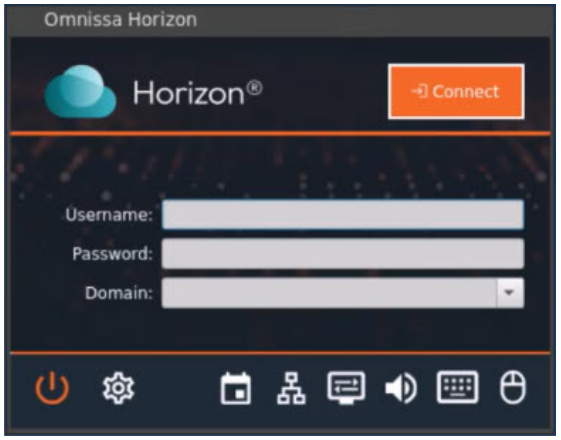
10ZiG

Omnissa Horizon Client

Select your “Connection Type” and enter your Omnissa Horizon Connection Server address in the “Server URL” Field. You may designate a specific desktop to connect to here as well.

You have the ability to preset your Username, Password and Domain settings to connect to your Omnissa Connection Server under the Login Option.

By Clicking OK on the Omnissa settings, you will see the dialog box shown below called the Launch Pad.



Launch Pad

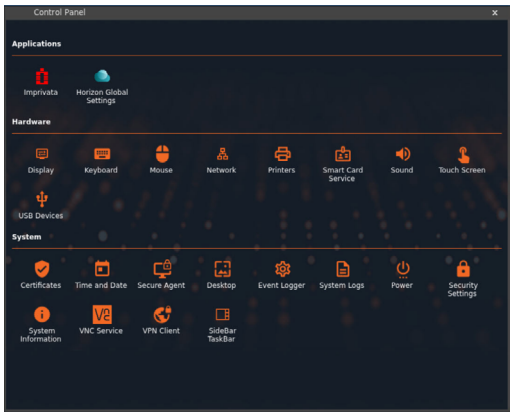
From the launch pad you can access the following for quick adjustments:

- Time/Date Configuration
- Network Configuration
- Display Configuration
- Sounds Configuration
- Keyboard Configuration
- Mouse Configuration

These options can be locked down under System Settings – Control Panel > System > Security Settings.

System Settings - Control Panel

At the bottom left of the Omnissa login dialog box, you will find a “Gear” icon in order to access the “Control Panel” applet.



Here you can manually configure the hardware, make changes, or view your system parameters.

Setting a Static IP Address and Wireless

1. Click Gear icon... to enter the Control Panel.
2. Click the Network icon, select Local Area and click the Edit button.
3. Go to the TCP/IP Properties tab and check the box Use Static IP.
4. Input your IP address, subnet mask and default gateway settings.
5. Enter any DNS settings and click “OK” when you’re finished.
6. If you have a wireless card installed, click the “Add” button and you’ll see which local wireless networks are available for you to connect to. If you need to find wireless connections again, just click the “Refresh” button.

   If you need to connect to a hidden wireless network, then click “Add hidden network”, type in the “SSID” of the hidden network and then click “OK”.
7. Enter your wireless settings including WEP/ WPA/WPA2 key.

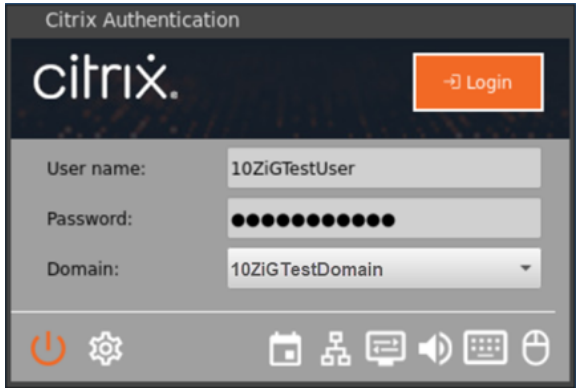
Locking Down the Zero Client

Once you have set up the Omnissa connection and made the desired changes to the system, you can lock the unit down to prevent future changes from being made. This can be done either remotely by 10ZiG Manager or on the unit itself. Click the “Gears” icon on the “Launchpad” and once inside the “Control Panel”, under the “System” area click “Security Settings”. Scroll down and under the “Control Panel” heading, tick the box named “Require password to modify the terminal configuration”, add a password to the unit to prevent any other users entering the control panel to edit settings. Once you have done this, click “Save”.

Access the Full User Guide here

NOS ZERO CLIENT FOR CITRIX

(Models 4648qc, 7048qc, 7348qc, 7148qc, 7548qcTAA, & 7948qc)



Components Included:

- Zero Client Device
- Power Supply
- Desktop Stand
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

Initial Boot-Up

Upon initial boot-up, once you click to agree the “End User License Agreement” the unit will attempt to configure the network settings, in the background using DHCP. You may continue through the remainder of the setup process by filling in the required information based on your preferences and geographical settings. On the following setup screens, you will be asked to complete your country location, the time zone you are in and the current time and date. These configuration screens are the same ones as mentioned previously in the PEAKOS section earlier in this guide.

You will now be able to enter your Citrix Settings to connect to your server. You may select the connection type > (options include Citrix Workspace, StoreFront for PNAgent/ WebAPI and Self-service) and then type in the “Server Address”.

You have the ability to preset your Username, Password and Domain settings to connect to your Citrix server under the Login Option. By clicking OK on the Citrix settings, you will see the dialog box shown below called the Launch Pad.

Launch Pad

From the launch pad you can access the following for quick adjustments:

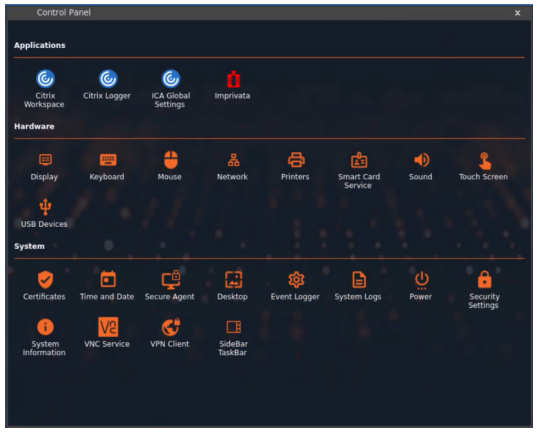
- Time/Date Configuration
- Network Configuration
- Display Configuration
- Sounds Configuration
- Keyboard Configuration
- Mouse Configuration

These options can be locked down under System Settings – Control Panel > System > Security Settings.

System Settings - Control Panel

At the bottom of the Omnissa login dialog box you will find a Gear icon in order to access the Control Panel applet.

[Access the Full User Guide here]



Here you can manually configure the hardware, make changes, or view your system parameters.

Setting a Static IP Address and Wireless

1. Click Gear icon... to enter the Control Panel.
2. Click the Network icon, select Local Area and click the Edit button.
3. Go to the TCP/IP Properties tab and check the box Use Static IP.
4. Input your IP address, subnet mask and default gateway settings.
5. Check the box use static DNS addresses to enter any DNS settings.
6. If you have a wireless card installed, click the “Add” button and you’ll see which local wireless networks are available for you to connect to. If you need to find wireless connections again, just click the “Refresh” button.

   If you need to connect to a hidden wireless network, then click “Add hidden network”, type in the “SSID” of the hidden network and then click “OK”.
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have set up the Citrix connection and made the desired changes to the system, you can lock the unit down to prevent future changes from being made. This can be done either remotely by 10ZiG Manager or on the unit itself. Click the “Gears” icon on the “Launchpad” and once inside the “Control Panel”, under the “System” area click “Security Settings”. Scroll down and under the “Control Panel” heading, tick the box named “Require password to modify the terminal configuration”, add a password to the unit to prevent any other users entering the control panel to edit settings. Once you have done this, click “Save”.

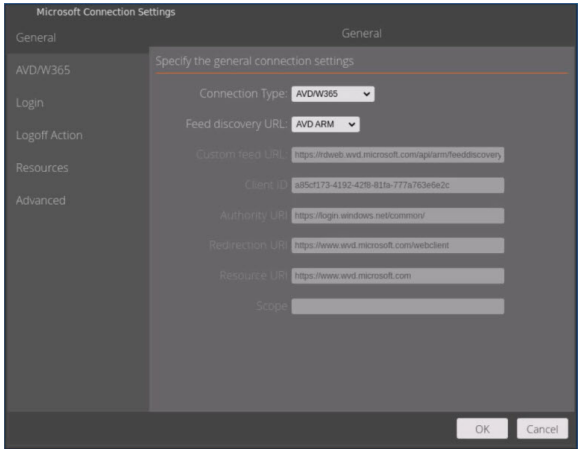
NOS ZERO CLIENT FOR MICROSOFT

(Models 4648qm, 7048qm, 7348qm, 7148qm, 7548qmTAA, & 7948qm)

Initial Boot-Up

Upon initial boot-up, once you click to agree the “End User License Agreement” the unit will attempt to configure the network settings, in the background using DHCP. You may continue through the remainder of the setup process by filling in the required information based on your preferences and geographical settings. On the following setup screens, you will be asked to complete your country location, the time zone you are in and the current time and date. These configuration screens are the same ones as mentioned previously in the PEAKOS section earlier in this guide.

Once this is complete, you will be presented with the “Microsoft Connection Settings” screen.



Components Included:

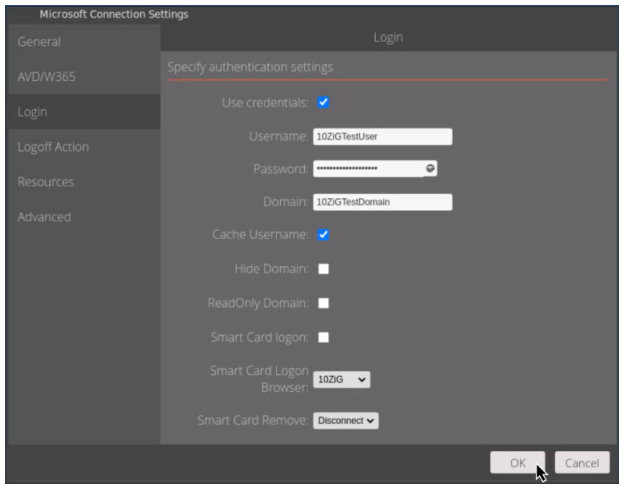
- Zero Client Device
- Power Supply
- Desktop Stand
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

You can connect to many different Microsoft hosts, depending on your environment. There are several connection types available, ranging from either RDWeb webfeed, Direct RDP or AVD/W365 (Azure Virtual Desktop/ Windows 365 Cloud PC).

If you access your resources in Azure AD, then you can connect to the Classic or ARM locations and even choose to point at any Customized AVD hosted areas you have.

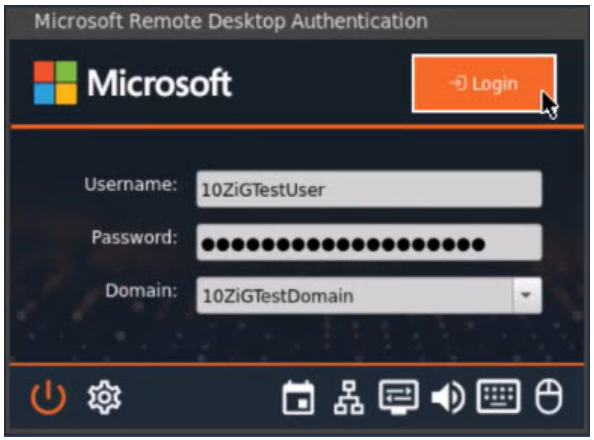
If you wish to access a Windows 365 Cloud PC, then you can leverage the AVD/W365 (Azure Virtual Desktop/Windows 365 Cloud PC) connection type.

In this example, we are connecting to a AVD ARM environment, so if we scroll down, we can complete our login details for our user and domain. Notice we have options to cache and save our zero client user credentials, so we do not have to supply them every time we wish to log in. This would be useful if you are using this unit in a more secure location such as a single office or for the more common home user environment.

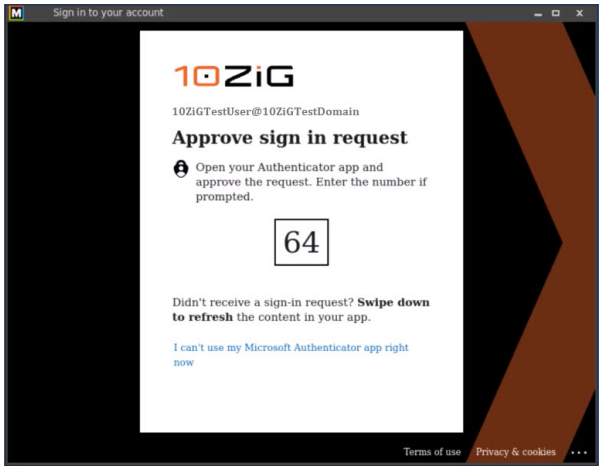


Once you are happy with the session settings, then click “OK” and close the Control Panel window.

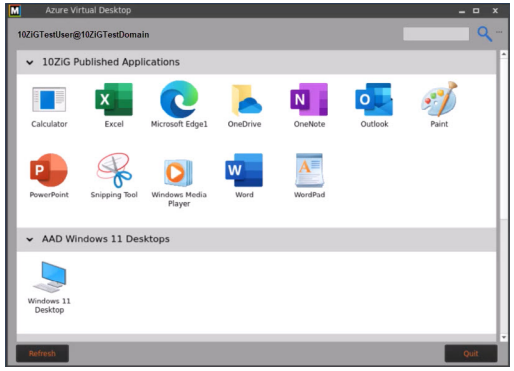
The “Microsoft Remote Desktop Authentication” login box is displayed, so simply click “Login”.



This user has MFA or Multi-Factor Authentication setup in the Azure AD, and so asks the user to key in the onscreen code on their mobile device, before MFA authentication is granted.



Once you have security clearance, you'll be logged into your AVD resource area inside the Azure Active Directory(AAD). You can see all the resources available to our user, including desktops and any published applications.



Launch Pad

From the launch pad you can access the following for quick adjustments:

- Time/Date Configuration
- Network Configuration
- Display Configuration
- Sounds Configuration
- Keyboard Configuration
- Mouse Configuration

These options can be locked down under System Settings – Control Panel > System Area > Security Settings.

System Settings - Control Panel

At the bottom left of the Microsoft login dialog box, you will find a "Gear" icon in order to access the "Control Panel" applet

Setting a Static IP Address and Wireless

1. Click gear icon... to enter the Control Panel
2. Click the Network icon, select Local Area and click the Edit button.
3. Go to the TCP/IP Properties tab and check the box Use Static IP.
4. Input your IP address, subnet mask and default gateway settings.
5. Enter any DNS settings and click "OK" when you're finished.
6. If you have a wireless card installed, click the "Add" button and you'll see which local wireless networks are available for you to connect to. If you need to find wireless connections again, just click the "Refresh" button.

   If you need to connect to a hidden wireless network, then click "Add hidden network", type in the "SSID" of the hidden network and then click "OK".
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have set up the Microsoft connection and made the desired changes to the system, you can lock the unit down to prevent future changes from being made. This can be done either remotely by 10ZiG Manager or on the unit itself. Click the "Gears" icon on the "Launchpad" and once inside the "Control Panel", under the "System" area click "Security Settings". Scroll down and under the "Control Panel" heading, tick the box named "Require password to modify the terminal configuration", add a password to the unit to prevent any other users entering the control panel to edit settings. Once you have done this, click "Save".

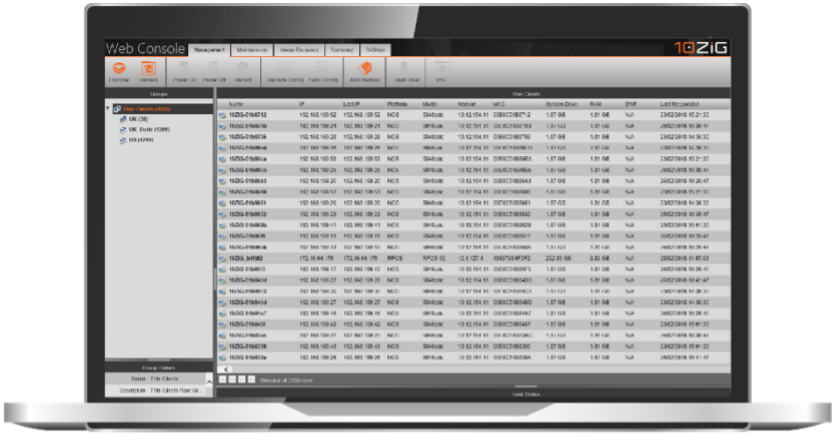
Access the Full User Guide here

HAVE YOU MET OUR 10ZiG MANAGER?

Let's get you introduced to the 10ZiG Manager:

Our simple-to-understand, user-friendly, highly functional Centralized Management Software Utility.

Web-console or server-console, 10ZiG Manager is always FREE with Thin & Zero Client purchases and makes endpoint management, configuration, and deployment efficient and effortless.



MANAGER

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 Web Console allows management of your clients from all major browsers (Edge, Chrome and Firefox), providing real-time status of all clients from a single comprehensive page.

10ZiG

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, Session Virtualization, 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.

10ZiG Product Warranty & Terms

The 10ZiG Thin & Zero Client Warranty is the 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 Omnissa, 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 →

10ZiG Support

USA/Americas
P: (866) 865-5250
support@10ZiG.com

EMEA Regions
P: +44 (0)116 214 8650
support@10ZiG.com

*10ZiG's Laptop and All-In-One (AIO) devices are similarly covered by a comprehensive 1-year Return-to-Base (RTB) warranty and are serviced by the same best in class US based support team providing support and firmware updates for the lifetime of your 10ZiG hardware.

10ZiG®

www.10ZiG.com