

Modernized Thin & Zero Client Hardware and Software

WELCOME TO THE 10ZIG INSTRUCTIONAL GUIDE

	min coens			٩		
🚓 Scenth	Nerve	IP Address MAC Platform	Notel Ventor	Template System Drive	RVM Last Responded	=
v 📲 The (Data (1822)	E Johnson 749601	172184200 67.44380614FE PK06	10724 16.5.35.3	Developor 146421 430 CB	1.52 CB 9/23/2023 1.0448 FM	-
Customer Service (1088)	Rg CASte 593541	172184196 235315347062 PK08	1072g 16.5.061	Designe-571421 401-08	1.92.58 9/23/2023 1.64.49 PM	
France & Administration (558)	a 1-0mm-17/855	1/7384250 BATRONCE39. NOS	1045pm 16.5.78.1	Analyet-19/577 410101	1 87 BI 9/7/703 154-48 PB	
🛃 Harnen Rassartes (225)	H Smith 638650	17238430 AF99F7804054 NOS	0048qs 96.536.1	Manager 978531 4:00 CB	15168 9/22/2023 1.9 c/7 PM	
- 😴 (T & Security (581)	Bione 327816	172.184.79 30.50.F4.06.07.55 NOS	0048cy 16.5.36.1	Administrator 125. 400 CB	1.92 CB 0/22/2023 1.04.47 TM	
n (159)	Although 47741	1/2104104 20:002049101 PM25	849540 Th 525.1	Engrano-JWI GIS	15-46 GIL 9/27/2023 104-44 PM	
A South (125)	AL HATROATIVA	172181.00 3052409754.00 PK05	8905-02 16.4.31.8	Technician-685607 4.08-68	3.83 08 9/20/2023 10/18 PM	
- 1496/001	A black MAN	17718437 145400 D.IC. NOS	6348er (6.5.36.1	Consultant 215818 400 CB	9.85 CB 9'22/2023 1.04.45 TM	
and the second s	A (Antholization	177184392 41124(35)/20 MS	1048er \$4.5.00.0	Devlage-NRL/S 22058	335168 \$(77)707310444494	
Colorado (120)	- interview	THE REPORT OF THE REPORT OF THE	2017a 10.5.25.3	Telever202028 728.08	7.34 FM 6/21/2023 162-08 FM	
(Maragement (407)	CIMANWATER.	Direction and an array of the			M Distances Mid	
(2) Monitory (400)	C C rog 1 dg 2 3				In Alamin Meridia	
 Operations (760) 	Tere		det	Satur	Details	-
🛃 Quality Accurren (202)			C 1 mm 101310	172 18 4 215	71/12/2014/16	
Research & Development (3.05)	1013/2023 208.06 PM	172 164.102	10-0000	1211443	F144 70 HE 80 H	
🥐 Saka (887)	\$1112223.266.18.PM	177 184.128	A DECIMAL AND A	172104102	WH 3C 92 49 45	
	8/19/2023 12:34:28 PN	1/2.168.02	Participant -	172184154	AE 80 28 59 47 10	
	0/15/2023 EDE-31 AM	172.16.8.106	C911-8207	100000	J0191312A/57	
	W11/2022 REF.(B.AM	1/2.16.8.108	D-0410+-322331	1/2 in con	640 M 1177	
	EXX11 AM	172.16.8.106	A Junes 3(3)41	172.18.4.214	Concept in Entre	
	202201/14	1/215.8108	1-Gritt-4-0/04	1/2164156	In Ja	-
REPURPO 102/G	95					

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

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







 \rightarrow



102iG.

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 Cloudbased. 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 office, remote, or for 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 customimaged devices are built to provide the best performance possible in VDI and serverbased 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!



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, NOS[™] Zero Clients, and Trusted Zero Clients.



THIN CLIENTS FOR WINDOWS 10/11 IOT LTSC

(Models 4610q, 7010q, 7110q, 7510qTAA, & 7910q)



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 <u>link</u> to find out more at the end of this section.

Components Included: —

- Thin Client Device
- Power Supply

10ZiG

- 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 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 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 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 following example shows a typical setup to create a dedicated AVD connection for your ThinClientUser that will run only this app during logon.

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.

options appear.

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

and you'll see 4 menu





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

First step is to setup shell.	the default shell for those user(s) or grou	p(s) that have no defined
It is recommended b	by 10ZiG Technology that you set the def	fault shell to be
Ext Dried Drifter D	you can sui manage the windows oper	dung system.
- Set Default Shell for Sh	el Launcher	
Default shell(Must	be set to use the Shell Launcher). Explorer exe is	recommended for the default shell
Shell	C:\Windows\explorer.exe	Open File
Shell Optional Parame	C:\Windows\explorer.exe	Open File
Shell Optional Parame Unexpected Clo	C:\Windows\explorer.exe ters se Restart Shell	Open File
Shell Optional Parame Unexpected Clo Shell Launcher	C:\Windows\explorer.exe tors ters Restart Shell Version 2	Open File Default Shell

• 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)

second step is to define	the user(s) or group(s) their appropriate	shell.
When you use Shell Lau Merface, replacing the d Windows desktop app pecify a UWP app as th Is EXPLORER exe, so y	ncher, you can configu efault shell (explorer e lication as the replace le replacement shell, lou can manage the W	re a device that ru ixe). In Shell Laun ment shell. In She It is recommended /indows OS.	ins an application as the use cher V1, you can only specif ell Launcher V2, you can als d that you set the default shei
Set User or Group Shell Laur	cher		
User		*	
Group		•	
Shell Executable			Open File
Optional Parameters			
Unexpected Close	Restart Shell 💌		
Shell Launcher Verison	Version 2		Set Shell Launcher

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:

Second step is to defi	ne the user(s) or group(s) their appropriate shell	L
When you use Shell Li Interface, replacing the a Windows desktop a specify a UWP app as as EXPLORER.exe, so	auncher, you can configure a device that runs a default shell (explorer exe). In Shell Launcher oplication as the replacement shell. In Shell La the replacement shell. It is recommended that o you can manage the Windows OS.	n application as the us V1, you can only speci auncher V2, you can als t you set the default she
User	DESKTOP-5VT2K4K(ThinClientU)	
	· ·	
Group		
Group Shell Executable	C:\Program Files\Remote Desktop\msrdcw.exe	Open File
Group Shell Executable Optional Parameters	C:\Program Files\Remote Desktop\msrdcw.exe	Open File
Group Shell Executable Optional Parameters Unexpected Close	C.\Program Files\Remote Desktop\msrdcw.exe	Open File
Group Shell Executable Optional Parametera Unexpected Close Shell Launcher Vertso	C \Program Files\Remote Desktop \mardcov.exe Restart Shell	Open File -
Group Shell Executable Optional Parameters Unexpected Oose Shell Launcher Veriso	C \Program Files\Remote Desktop\mardcw.exe Restart Shell	Open File -

- 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.

The last step is to verify Sh the rest of the setup if need	ell Launcher in enabled. The defore the reboot.	his will require a reboot but you can finish
Shell Launcher Status		
Shell Launcher Version	Version 2	
Shell Launcher Status	Enabled	Disable
Default Shell	CustomShellHost exe - C:\V	Vindows\explorer exe

• 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 10/11 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 msrdcw.exe that allows us to login to our AVD and Windows 365 cloud pc desktops.



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

Change a password	
Task Manager	
Cancel	
	-
	Ċ,

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"

lighlight any key or co	mbination items in the table be	low and click "Allow"	or "Block". A	ll key items
sted are allowed by d	efault and any changes you m	ake are done in real-	time."	
Security Neys				
Key Combination	Description	Status	Allow	Block
Ctrl+Alt+Del	Secure Desktop	Allowed		
ShiftyOrlyEeo	Task Manager	Blocked		
OT BL TOULTEDU	1.1.0.1	Allowed		
Win+L	LOCK Console	revered		

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 Shift+Ctrl+Esc, launching the "Task Manager"



re allowed by defa	r combination items in the table below and cl ault and any changes you make are done in	real-time."	ck'. All key it	ems liste
Shell Keys				
Key Combination	Description	Status	Allow	Block
Win+PageDown	Cycle the Shell to the next Right Monitor	Allowed		· *
Win+PageUp	Cycle the Shell to the next Left Monitor	Allowed		
Win+Plus	Magnifier Zoom In	Allowed		
Win+Q	Open Search Charm	Allowed		
Win+R	Run Dialog	Blocked		
Win+Hight	Dock Current Window to the right	Allowed		
Win+Shift+Down	Restore Current Windows Vertical Size	Allowed		

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 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 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/



Windows 10/11 IoT LTSC VDI-DaaS Apps Installation



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

Windows Update Package	Windows Update Package
Windows Client Update	Windows Write Protection
Specify the update installer file and/or command line parameters.	Specify the options for the write protection if enabled.
Update File:	Disable EWF/UWF before execution (Requires initial reboot) E Enable EWF/UWF after execution (Requires reboot) EWF Options (Only applies to Windows 7 and prior) Commit EWF after execution Reboot to flush EWF prior to execution Previous Nistin Concel

PEAKOS (LINUX) THIN CLIENTS

(Models 4602/72q, 7002/72q, 7102/72q, 7502/72qTAA, & 7902/72q)



Components Included: –

- Thin Client Device
- Power Supply
- USB Wheel Mouse
- 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.

er License Agreeme i scroll to the end to agr

directly or indirectly export, re-export, or release the Products and Solutions to, or make the Products and Solutions or Documentation accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export) license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the Products and Solutions available outside the US.

f. FORCE MAJEURE: The parties acknowledge and agree that either party shall be excused from any delay or failure in its performance hereunder caused by any disruption or slow speed of the internet, break-downs of security or introduction of computer viruses (and the like) by third parties, any labor dispute, epidemic, pandemic government requirement, act of God, or any other cause beyond its reasonable control including, without limitation, the consequences of the COVID 19 pandemic. The parties shall use reasonable commercial efforts to cure any such failure or delay in performance arising from a force majeure condition, and shall timely advise each other of such efforts.

•00000





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

- 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

 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".

 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, rightclick 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, VMware, or Citrix, you will also have the option to tick the check box for auto reconnect.

NOS ZERO CLIENT FOR OMNISSA (FORMERLY VMWARE)

(Models 4648qv, 7048qv, 7148qv, 7548qvTAA, & 7948qv)





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 VMware Horizon (Omnissa) 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 VMware Horizon (Omnissa) server.



10ZiG

Components Included: `

- Zero Client Device
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)

Omnissa (Formerly VMware) Horizon Client

Select your "Connection Type" and enter your VMware Horizon (Omnissa) 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 VMware (Omnissa) Connection Server under the Login Option.

By Clicking OK on the VMware (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:





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 VMware (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.





18

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.
- 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".

 Enter your wireless settings including WEP/ WPA/WPA2 key.



Locking Down the Zero Client

Once you have set up the VMware (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".

NOS ZERO CLIENT FOR CITRIX

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



Components Included: -

- Zero Client Device
- Power Supply
- USB Wheel Mouse
- 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 VMware 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. Check the box use static DNS addresses to enter any DNS settings.

 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".

 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, 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.



102iG



Components Included: -

- Zero Client Device
- Power Supply
- USB Wheel Mouse
- 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.

Microsoft Connection Se	ttings
General	General
AVD/W365	
Logoff Action	Connection Type: AVD/W365
Logon Action	Feed discovery URL: AVD ARM 🗸
Resources	Custom feed URL:
Advanced	lise credentials: 🗸
	USername: 102/GTestUser
	Password:
	Dornain: 10ZiGTestDomain
	OK Cancel

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.
- 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".

 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".



HAVE YOU MET OUR 10ZIG MANAGER?

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

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

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

Web Console	Management Ministervances in	mega Retainey Sar	newy Sating								<u> 10</u> Zi
	17 09 0										
I MATERIA INACIAL	DI FRANK CHE INFORT		Jaco Stamont		a m.						
Despe					_		The Chest				
	Kane	9	Lastip	Platform	Medzi	Vosian	M10	Bysiem Drive	8.00	218	Last Responded
The Cheste (ME)	1020G-0108712	192.168.168.52	152,162,169,52	NCE	38480.6C	10.12.154.11	006000188712	1.87.08	1.81 08	140	23622018 152130
- OR (30)	Nor TRACE STREW ID	162, 163, 109-24	TH2, HS1, 109-24	NCO	SPROK	12 12 134 11	COLICINE NU	1.8/63	1.81 648	-	2952210938 30 38.47
2 115 192100	5. 10205-0108706	192.168.160.28	102.168.169.28	NCE	50480.0C	10.12.154.11	006000188796	1.87.08	1.81 08	NA	23422010 14:36:30
Constraint,	No. 10/002/10/06-08	IN2 184 189 24	112 851 129 24	MCS.	Milliple	10 17 154 11	OF REALIZED D	1.8/121	1.81 (28	2.4	22002204058 82 30 32
	🖏 10205-01b86ca	132 168 168 58	152.162.109.53	NCE	58480.6c	10 12 154 11	ODEOCTOBINES.	1.87.08	1.81 68	523	234229418 1521:30
		142, 164, 169 25	TH2. HE4. 100 21	NOS	official	12 12 104.11		1.8/ 648	1.51 6/8	140	2552213918 10/36.4/
	10235-5108613	192.168.169.20	192,968,169,20	NCS	58480.0C	10 12 154.11	006005180643	1.87.08	1.81 08	144	2642/3018 10:26:47
	 10/3G-116/0618 	FN2 858 108 51	192 861 109 51	NCS	SMADOR	10 12 154 11	-	1.07 03	1.01 GB	5.4	23420848 8521:35
	45 1071G-61b3691	102 163 160 20	102.963 189.20	NCC	SMOOR	10 12 154 11	000005103661	1.87.03	131.08	548	23627848 5436 37
		162.168.180.28	102, 162, 109 22	NC6	50430K	12.12.151.11	006000180432	1.87 68	1.81 68	140	25/62/2018 10.36.47
	1625/3-5 (6-8926	192.108.159-11	192, 993, 109-11	NOS	Strauk	13 82 154 81	006005180428	1.87.08	1.81 08	NA	234220418 15-01.32
	10/21G-/110/05 W	992.868.958.95	192,862,109,15	NC0	SMillofe	10 12 154 11	006405480417	1.87.03	1.51 08	NA	26/02/04/8 \$0:20:47
	😼 10/05-010/0518	1167 1948 1949 118	152 961 109 17	NET	MARCAL	10 17 154 11		1.8/121	1.01 (20	1.4	UNE21-918 \$125.47
		172.16.64.176	172.16.64.175	RPC6	RP08-02	12.1.127.4	19637384F2F2	232.85.68	3.55.04	14	2562/2018 11 67:03
	16250 516850	192.103.159.17	192.893.199.17	NOS	SPEck	10 82 154 81	0064054889975	1.87 GB	1.81 GB	11.4	26422/2618 10:28.47
	10/205-518/84:04	192.168.169.27	192, 862, 109 27	NCS	3848cdc	10 12 154 11	0060001885400	1.87 08	1.81 08		26/02/2018 10 41:47
	NO TRANSPORT	1107 1968 1009 240	1127 8961 1899 241	NO	MARCH	10 87 154 81		3.8/428	3.81128	-	23427748383438320
	5 10Z3G-6108404	192.168.160.27	102, 162, 100 27	NCE	684804C	12.12.154.11	008408102080480	1.87 08	1.01 048	141	234220418 54.36.30
	🐋 10/5G 610/01a7	1922 1083 1099 14	192, 892,109 16	NOS	SPERA	10.12.154.15	ODERCS NUMA7	1.87.03	1.81 GB	51.4	2602/2618 10/28 47
	10/205-01b840r	112 168 168 42	112, 168, 109 42	NC8	38480/K	13.12.154.11	006000180467	1.87.08	1.01 08	5.0	234220418 15-01:30
	No TRACLAMBRENE	1567 1968 1000 277	1527 853 1389 22	NET	Milliolat	10 87 554 83	OR REPORTED IN	3.6/121	1.011.020	51.4	PREF-818 8136 6/
	1023G-610-8009	192.162.160.43	102.862.109.43	NCE	58480.6C	10 12 154.11	006025182300	1.87 68	1.01 08	14	23620918 (5.41.30
	🐝 10/3G 810833#	162.163.109.25	192, 862, 109 24	NOS	SHEUK.	10.82.894.81	000002108384	1.87.63	1.81 GB	344	260208083041.47
d Lena op i Ladaei m	<										
None Tier Churle											
Description This Clients Root	Gr						Land Titula				

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.

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 <u>support@10ZiG.com</u> for the US, Canada, and South America or <u>support@10ZiG.eu</u> for EMEA.

* VNC is not supported on Trusted Zero Clients.

 \rightarrow

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 VMware, Citrix, MS Certified support team), and 3 years of software upgrades.





Check Our Our Product Brochure Video \rightarrow

www.10ZiG.com