Welcome to 10Zig

Instructional Booklet

Cutting-Edge Thin Clients & Zero Clients

# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 - 13</td>
<td>Windows 10 IoT Setup Instructions</td>
</tr>
<tr>
<td>14 - 21</td>
<td>WE8S Setup Instructions</td>
</tr>
<tr>
<td>22 - 27</td>
<td>WES7 Setup Instructions</td>
</tr>
<tr>
<td>28 - 31</td>
<td>PeakOS™ Linux Setup Instructions</td>
</tr>
<tr>
<td>32 - 35</td>
<td>VMware NOS™ Setup Instructions</td>
</tr>
<tr>
<td>36 - 39</td>
<td>Citrix NOS™ Setup Instructions</td>
</tr>
<tr>
<td>40 - 43</td>
<td>Parallels NOS™ Setup Instructions</td>
</tr>
<tr>
<td>44 - 47</td>
<td>RDP NOS™ Setup Instructions</td>
</tr>
<tr>
<td>48 - 51</td>
<td>PCoIP V1200 Series Setup Instructions</td>
</tr>
<tr>
<td>52 - 53</td>
<td>10ZiG Manager</td>
</tr>
<tr>
<td></td>
<td>• 10ZiG Manager Overview and Feature Set</td>
</tr>
<tr>
<td></td>
<td>• Installation/ Setup Instructions (Link to Cloud Setup)</td>
</tr>
<tr>
<td>53</td>
<td>10ZiG FAQ Site Overview</td>
</tr>
<tr>
<td>53</td>
<td>Product Warranty &amp; Terms</td>
</tr>
</tbody>
</table>
In case you did not know, we’ve been around for a while

When you think Thin & Zero Clients for virtual desktop infrastructure (VDI), think 10ZiG. Founded in 2003 and originally under the name of BOSaNOVA through 2009, 10ZiG quickly became premier Thin & Zero Client Technology specialists, from hardware to software to service.

Headquartered in Arizona, US and Leicester, UK, with offices in Germany and Australia, we offer full international coverage and serve customers from all over the world. As world market leaders in cutting-edge Thin & Zero Clients for VDI Solutions, our VMware, Citrix, and Microsoft ready Clients are designed to suit all user types in any environment.

The devices you want and the service you’ve wished for

10ZiG Technology offers a wide selection of powerful, reliable, easy-to-manage, affordable Thin & Zero Client 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.

Thin & Zero Clients by 10ZiG available operating systems cover PeakOS™ (Linux) to Windows Embedded 7/8 and Windows 10 IoT to NOS™ (Zero). We are certified for and/or support VMware (PCoIP & Blast Extreme), Citrix (HDX, HDX Premium, and HDX 3D Pro), Microsoft RDP and Parallels RAS (Remote Application Server). From low-level end users requiring Microsoft Office to power-users requiring HD Video/Audio, Flash/HTML5, video conferencing, 3D, CAD and 4K resolution, we have the perfect endpoints for your needs with the service you’ve always wanted!

Our difference makes all the difference

Unlike our competition, 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.

- The 10ZiG Manager: our custom software centralizes configuration, maintenance, control, and even reporting from all Linux and Windows based Thin & NOS™ Zero Client devices for traditional managed networks.
Setup instructions for 10ZiG
Windows, PeakOS™ (Linux) & NOS™ (Zero) Clients
Thin Clients for Windows 10 IoT  
(Models 4410, 5810q, 5910q & 7810q)

Initial Setup and Configuration

By default, when you first boot up your new Windows 10 IoT 10ZiG Thin Client, you are automatically logged in as “Administrator”. While logged in as Administrator, you will be able to set up, install and configure the Thin Client for use with any “locked down” users you may wish to create.

Administrator’s password: admin

Components included

☐ Thin Client Device
☐ Thin Client Stand
☐ Power Supply
☐ USB Wheel Mouse
☐ VESA Mounting Bracket (Optional)
☐ Wireless Adaptor (Optional)
☐ DVI to VGA Adaptor (Optional)
"ThinClientUser" Login

ThinClientUser has been developed to provide the administrator with a “locked down” user environment which has no rights to install, create, modify or delete. ThinClientUser is also unable to create shortcuts and is not allowed to run the “right click” context menu.

ThinClientUser’s password: ThinClientUser
10ZiG Quick Start Wizard

When the Thin Client first logs in under administrator, you will be prompted with the 10ZiG Quick Start Wizard. The 10ZiG Wizard is here to make your customized setup and configuration a breeze. Simply follow the step-by-step instructions, and be sure to note the Connections, User Accounts/Domain and Personalization tabs on the following screens.

1. User Accounts (under User Accounts/Domain tab) - It is easy to setup a new account with user or administrative privileges using the 10ZiG Quick Start Wizard. Simply select from the radio button whether the user should have user or administrative rights and type username and password as shown below:

![Create Account](image1)

Click the Create Account button when finished entering the data.

2. Domain Join (under User Accounts/Domain tab) – Domain join and/or change hostname is a snap. Select the appropriate radio button on whether it is a domain join with name change or just a name change. If applicable enter the domain name, hostname, username and password (must have rights to join the domain). As shown below:

![Join/Change](image2)

Click the Join/Change button when finished entering the data.
3. Set up the Date & Time (under Personalization tab) – To change the date and time, simply tab through the field and enter the date as shown below:

![Date & Time](image)

4. Enable/Disable the Unified Write Filter (UWF) (under Personalization tab) – By default, the Unified Write Filter is off. To turn it on/off is quite easy. (Please do not turn it on until you are finished configuring your Thin Client.) Please see document UWF Suggested Exclusions for extensive detail on UWF and setup. It can be downloaded here: https://www.10zig.com/resources/support_faq/unified-write-filter

Select the appropriate radio button for the desired action.

Click Change Write Filter. It will require a reboot to enable and the image will be protected from any changes.
Windows IoT comes with the 10ZiG UWF Wizard. You can use the UWF Wizard directly on a Windows IoT device to setup Shell Launcher, enable/disable and configure the Unified Write Filter. There is a status indicator telling you the status of UWF. The indicator is located in the system tray.

A green indicator means it is disabled. A red indicator means it is enabled. To launch the configuration, you must have administrator rights. You can right click or double click on the status indicator to enter into the configuration.

You can use Shell Launcher to replace the default Windows IoT shell with a custom shell. You can use any application or executable as your custom shell, such as a command window or a custom dedicated application. You can configure Shell Launcher to launch different shell applications for different users or user groups. You can set file/registry exclusions of changes you need to persist when UWF is enabled. There are settings to change UWF overlay if needed.

To the right is the look and feel of the 10ZiG UWF Wizard:
Removing Automated Logon Feature

By default, the 10ZiG Thin Client is configured to auto logon as Administrator. That can be easily changed or removed by using the 10ZiG Quick Start Wizard. If you have exited the wizard you can start it up again by clicking on the 10ZiG icon on the administrator desktop. Once the wizard is on the desktop, click on the User Accounts/Domain tab. Choose the appropriate radio button to remove/change auto logon.

Below is an example of removing the auto logon feature; please note your data might be different.

Wireless Setup

If your 10ZiG Thin Client came with a wireless network card, then click on the following icon. It will detect all the wireless networks that are in range to the Thin Client. Sample located below:

Locate the network you want to connect to and click on its name. If it is a network you know and you will connect to on a regular basis, you should select the option that says: “Connect automatically”. This way, whenever your device is in the networks range, it will automatically connect to it.

How to Set a Static IP Address

1. Click on Control Panel, Network and Sharing Center, Change Adapter Settings.
2. Right-click Local Area Connection and Select Properties.
3. Select Internet Protocol Version 4 and Click Properties
4. Enter the static IP address, the Subnet mask, the Default gateway and close the dialog box.
5. Click OK and OK again to close the Local Area Connection Properties box.

Tight VNC

The default password to connect to the Thin Client using the 10ZiG Manager is admin
Third Party Software Install

You can install additional third-party software that you may need to use on the Thin Client. Such items can include hardware or device drivers as well as any additional software that is required to run on the Thin Client device.

Write Filter

Windows IoT comes with the Unified Write filter installed on the 10ZiG Thin Client. Unified Write Filter (UWF) is a sector-based write filter that you can use to protect your storage media. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. This improves the reliability and stability of your device. You can use Hibernate Once/Resume Many (HORM). UWF also contains a file and registry filtering system. You can add specific files or folders on a protected volume to an exclusion list to exclude those files and folders from being filtered by UWF. When a file or folder is in the exclusion list for a volume, all writes to that file or folder bypass UWF filtering, and are written directly to the protected volume and persist after the device restarts.

You must use an administrator account to add or remove file or folder exclusions during runtime, and you must restart the device for new exclusions to take effect.

To determine if UWF and the filter status is enabled/disabled just look at the status indicator located in the system tray. Green is disabled and red is enabled.

For additional information on the UWF configuration double click or right click on the indicator icon and the screen below will tell you type, maximum size, critical and warning thresholds of the overlay...

For additional information on how to add/remove file/registry exclusions please use the UWF Wizard.

For UWF Servicing on Windows Updates, see the below link.

https://www.10zig.com/resources/support_faq/unified-write-filter
Initial Setup and Configuration

By default, when you first boot up your new Windows Embedded 8 Standard 10ZiG Thin Client, you are automatically logged in as “Administrator”. While logged in as Administrator, you will be able to set up, install and configure the Thin Client for use with any “locked down” users you may wish to create.

Administrator’s password: admin

Components included

- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
“ThinClientUser” Login

ThinClientUser has been developed to provide the administrator with a “locked down” user environment which has no rights to install, create, modify or delete. ThinClientUser is also unable to create shortcuts and is not allowed to run the “right click” context menu.

ThinClientUser’s password: ThinClientUser
10ZiG Quick Start Wizard

When the Thin Client first logs in under administrator you will be prompted with the 10ZiG Quick Start Wizard. The 10ZiG Wizard is here to make your customized setup and configuration a breeze. Simply follow the step-by-step instructions, and be sure to note the Connections, User Accounts/Domain and Personalization tabs on the following screens.

1. User Accounts (under User Accounts/Domain tab) - It is easy to setup a new account with user or administrative privileges using the 10ZiG Quick Start Wizard. Simply select from the radio button whether the user should have user or administrative rights and type username and password as shown below:

   ![Create Account](image)

   Click the Create Account button when finished entering the data.

2. Domain Join (under User Accounts/Domain tab) – Domain join and/or change hostname is a snap. Select the appropriate radio button on whether it is a domain join with name change or just a name change. If applicable enter the domain name, hostname, username and password (must have rights to join the domain) as shown below:

   ![Join/Change](image)

   Click the Join/Change button when finished entering the data.
3. Set up the Date & Time (under Personalization tab) – To change the date and time simply tab through the field and enter the date as shown below:

Click the Set Date/Time button.

4. Enable/Disable the Unified Write Filter (UWF) (under Personalization tab) – By default the Unified Write Filter is off. To turn it on/off is quite easy. (Please do not turn it on until you are finished configuring your Thin Client). Please see document UWF Suggested Exclusions for extensive detail on UWF and setup. It can be downloaded here: https://www.10zig.com/resources/support_faq/unified-write-filter

Select the appropriate radio button for the desired action. See below:

Click Change Write Filter. It will require a reboot to enable and the image will be protected from any changes.
Embedded Lockdown Manager

Windows Embedded 8 Standard comes with the Embedded Lockdown Manager. ELM is a snap-in to the Microsoft Management Console (MMC). You can use ELM directly on a Windows Embedded 8 Standard device or you can use ELM on a development computer and then remotely connect to the Thin Client device. ELM automatically detects which lockdown features are installed on the device, and displays configuration options for only those features. ELM uses Windows Management Instrumentation (WMI) to detect and change configuration settings.

You can use Shell Launcher to replace the default Windows Embedded 8 Standard shell with a custom shell. You can use any application or executable as your custom shell, such as a command window or a custom dedicated application. You can also configure Shell Launcher to launch different shell applications for different users or user groups. Here is the look and feel of the ELM as well as the features installed.

For additional information on how to add/remove file/registry exclusions please use the UWF Wizard.

For UWF Servicing on Windows Updates, see the below link.
https://www.10zig.com/resources/support_faq/unified-write-filter
Removing Automated Logon Feature

By default, the 10ZiG Thin Client is configured to auto logon as Administrator. That can be easily changed or removed by using the 10ZiG Quick Start Wizard. If you have exited the wizard, you can start it up again by clicking on the 10ZiG icon located on the Administrator’s desktop.

Once the application is active, click on User Accounts/Domain tab. Choose the appropriate radio button to remove/change auto logon. Snapshot below is removing the auto logon feature, please note your data might be different.

How to Set a Static IP Address

1. Click on Control Panel, Network and Sharing Center, Change Adapter Settings.
2. Right-click Local Area Connection and Select Properties.
3. Select Internet Protocol Version 4 and Click Properties
4. Enter the static IP address, the Subnet mask, the Default gateway and close the dialog box.
5. Click OK and OK again to close the Local Area Connection Properties box.

Tight VNC

The default password to connect to the Thin Client using the 10ZiG Manager is admin

Wireless Setup

If your 10ZiG Thin Client came with a wireless network card, click on the following icon. It will detect all the wireless networks that are in range to the Thin Client. Sample located below:

Locate the network you want to connect to and click on its name. If it is a network you know and you will connect to on a regular basis, you should select the option that says: “Connect automatically”. This way, whenever your device is in the networks range, it will automatically connect to it.

Once you click or tap Connect, Windows scans for the security settings of the network. Then, it will ask you for its security key.

Once you have entered the password required by the network click next. If you want to check the accuracy of your password, you can see it before pressing “Next” by clicking the eye-like icon on its right side. When connected to the network the network name will display “Connected” to the right-side.
Third Party Software Install

You can install additional third-party software that you may need to use on the Thin Client. Such items can include hardware or device drivers as well as any additional software that is required to run on the Thin Client device.

Write Filter

Windows Embedded 8 Standard comes with the Unified Write filter installed on the 10ZiG Thin Client.

Unified Write Filter (UWF) is a sector-based write filter that you can use to protect your storage media. UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. This improves the reliability and stability of your device. You can use Hibernate Once/Resume Many (HORM). UWF also contains a file and registry filtering system. You can add specific files or folders on a protected volume to an exclusion list to exclude those files and folders from being filtered by UWF. When a file or folder is in the exclusion list for a volume, all writes to that file or folder bypass UWF filtering, and are written directly to the protected volume and persist after the device restarts.

You must use an administrator account to add or remove file or folder exclusions during runtime, and you must restart the device for new exclusions to take effect.

To determine if UWF and the filter status is enabled/disabled, bring up an admin command prompt and type “uwfmgr get-config” or use the Embedded Lockdown Manager to determine status.

For additional information on suggested file/registry exclusions and UWF servicing on Windows Updates, see URL below:
https://www.10zig.com/resources/support_faq/unified-write-filter
A Wide Range of Devices to Fit Your Needs
Thin Clients for Windows 7 (WES7)
(Models 4417, 5817q & 7817q)

Initial Setup and Configuration

By default, when you first boot up your new Windows Embedded 7 Standard 10ZiG Thin Client, you are automatically logged in as “Administrator”. While logged in as Administrator, you will be able to set up, install and configure the Thin Client for use with any “locked down” users you may wish to create.

Administrator’s password: admin

Components included

- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
“ThinClientUser” Login

ThinClientUser has been developed to provide the administrator with a “locked down” user environment which has no rights to install, create, modify or delete. ThinClientUser is also unable to create shortcuts and is not allowed to run the “right click” context menu.

ThinClientUser’s password: ThinClientUser
10ZiG Quick Start Wizard

When the Thin Client first logs in under administrator, you will be prompted with the 10ZiG Quick Start Wizard. The 10ZiG Wizard is here to make your customized setup fast and easy. Simply follow the step-by-step instructions, and be sure to note the Connections, User Accounts/Domain and Personalization tabs on the following screens.

1. User Accounts (under User Accounts/Domain tab) - It is easy to setup a new account with user or administrative privileges using the 10ZiG Quick Start Wizard. Simply select from the radio button whether the user should have user or administrative rights and type username and password as shown below:

   ![Create Account](image1)

   Click the Create Account button when finished entering the data.

2. Domain Join (under User Accounts/Domain tab) – Domain join and/or change hostname is a snap. Select the appropriate radio button on whether it is a domain join with name change or just a name change. If applicable enter the domain name, hostname, username and password (must have rights to join the domain) as shown below:

   ![Join/Change](image2)

   Click the Join/Change button when finished entering the data.
3. Set up the Date & Time (under Personalization tab) – To change the date and time simply tab through the field and enter the date as shown below:

Click the Set Date/Time button.

4. Enable/Disable the Enhanced Write Filter (EWF) (under Personalization tab) – By default, the Enhanced Write Filter is off. To turn it on/off is easy. (Please do not turn it on until you are finished configuring your Thin Client).

Select the appropriate radio button for the desired action. See below:

Click Change Write Filter. It will require a reboot to enable and the image will be protected from any changes.
Removing Automated Logon Feature

By default, the 10ZiG Thin Client is configured to auto logon as Administrator. That can be easily changed or removed by using the 10ZiG Quick Start Wizard. If you have exited the wizard you can start it up again by clicking on the 10ZiG icon on the administrator desktop. Once the application is active click on User Accounts/Domain tab. Choose the appropriate radio button to remove/change auto logon. Snapshot below is removing auto logon feature, please note your data might be different.

How to Set a Static IP Address

1. Click on Control Panel, Network and Sharing Center, Change Adapter Settings.
2. Right-click Local Area Connection and Select Properties.
3. Select Internet Protocol Version 4 and Click Properties
4. Enter the static IP address, the Subnet mask, the Default gateway and close the dialog box.
5. Click OK and OK again to close the Local Area Connection Properties box.

Tight VNC

The default password to connect to the Thin Client using the 10ZiG Manager is admin

Wireless Setup

If your 10ZiG Thin Client came with a wireless network card, right-click on Network located on the All Programs Menu. It will bring up the following screen:

Click on Change Adapter setting located on the left-hand side. The following screen will be displayed.

Right-click on the wireless adapter and choose Connect /Disconnect. It will detect all the wireless networks that are in range to the Thin Client. Sample located below:
Locate the network you want to connect to and click on its name. If it is a network you know and you will connect to on a regular basis, you should select the option that says: “Connect automatically”. This way, whenever your device is in the network’s range, it will automatically connect to it.

Once you click or tap Connect, Windows scans for the security settings of the network. Then, it will ask you for its security key.

Once you have entered the password required by the network click ok. If you want to encrypt the security key check the “HideCharacters” box. When connected to the network the network name will display “Connected” to the right-side.

---

**Third Party Software Install**

You can install additional third-party software that you may need to use on the Thin Client. Such items can include hardware or device drivers as well as any additional software that is required to run on the Thin Client device.

**Write Filter**

Windows Embedded Standard 7 comes with the Enhanced Write filter installed on the 10ZiG Thin Client.

Enhanced Write Filter (EWF) provides the ability to write-protect a run-time image. By redirecting all write requests to either a separate disk partition RAM-REG. EWF allows the run-time image to maintain the appearance of a writeable run-time image.

RAM-REG overlays store overlay information in RAM. However, the configuration information about EWF is not stored in a separate EWF volume, but within the registry.

To determine if EWF status is enabled/disabled bring up an admin command prompt and type: `ewfmgr c:`

Or the disk icon located in the system tray. Green light means disabled and orange is enabled.

**PLEASE NOTE:** 10ZiG highly recommends keeping the EWF enabled at all times except when required to disable due to a need to apply update or make adjustment to the image.
Thin Client for PeakOS™ (Linux)
(Model 4402/72, 5802q/72q, 5902q/72q & 7802q/72q)

Initial Boot-Up
Upon initial boot-up, the unit will attempt to configure the network settings using DHCP. Once the unit has obtained an IP address, the default behavior of the unit will be based up which type of specific software model that it is.

Components included
- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
XX02

This model is in Desktop Mode by default which is similar to a Windows style desktop. From the desktop, Right-Click the Desktop and choose Terminal Properties to continue the initial configuration.

XX72

This model is in WBT Mode by default which is similar to a Windows style desktop. From the desktop, Right-Click the Desktop and choose Terminal Properties to continue the initial configuration.
Setting a Static IP Address and Wireless

1. Go to the Terminal Properties (using one of the methods above)
2. Double 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 then click the Refresh button to see which wireless networks are available for you to connect to
7. Enter your wireless settings including WEP/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, select the Configuration tab and then click the Add button, or from a desktop select Start Button > Programs and then next to the program you wish to add. For example, to add an Internet browser-based connection, you would select the menu option “Add Internet Browser”.

Locking Down the Thin Client

Once you have added all the applications you need you can lock the unit down to prevent changes from being made. This can be done either remotely by the 10ZiG Management Software or on the unit itself. Enter the Terminal Properties, go to the Security tab and click the hide connections configuration tab check box. Then add a password to the unit to prevent the user from entering the control panel to edit settings.
Auto Start Applications

Any connection can be set to automatically launch when the unit is powered on. In the configuration tab of the Connections Manager, highlight the connection you want to auto start and click the Startup button. Click the check boxes for auto-start, and/or for default connection. If this connection type is RDP, VMware or Citrix, you will also have a check box for auto reconnect.

Optional Power Plus Features

TN5250e Connections (Display & Printer) for direct line-up to AS/400 systems via Ethernet cable and TCP/IP protocol. TN3270e Connections (Display & Printer) for direct line-up to IBM 390 systems via Ethernet cable and TCP/IP protocol. Adobe PDF Viewer

5250 Hot Keys (Terminal Style)

Enter Right CTRL
Field Exit ENTER
Error Reset Left CTRL
Attention ESC
Rule Cursor Home
Dup Numpad
Roll Up Page Down
Roll Down Page Up
Split Screen CTRL-ALT-INSERT
Hot Key to Next Session ALT + TAB

Hot Keys

CTRL + ALT + END = Displays Terminal Connection Manager
CTRL + ALT - = Jumps back to previous session
CTRL + ALT + = Jumps back to the subsequent session
F2 = Enters Terminal Setup from the Terminal Connection Manager screen.
On power up if you hold down the space bar key it will get you to the quick set up screen.

Non-Destructive Backspace

Your 10ZiG PeakOS™ Thin Client can be configured but requires keyboard mapping. The keyboard mapping is done using the GUI configurator in desktop mode.
Zero Client for VMware NOS™
(Model 4448v, 5848qv/qdv & 5948qv)

Initial Boot-Up

Upon initial boot-up, the unit will attempt to configure the network settings using DHCP. Once the unit has obtained an IP address, 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 & Date. You will now be presented with your VMware View 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 server.

Components included

- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
VMware Horizon Client

Enter your VMware Horizon Connection Server address in the “Server Address” 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 Connection Server under the Login Option.

By Clicking OK on the VMware 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:

- Display Configuration
- Sound 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 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.
6. If you have a wireless card installed, click the Add button and then click the Refresh button to see which wireless networks are available for you to connect to.
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have setup the VMware 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 the 10ZiG Management Software or on the unit itself. Enter the System Settings – Control Panel. Under the System area click Security Settings and check the Lock down control panel check box. Then add a password to this to prevent the user from accessing the control panel.
Zero Client for **Citrix NOS™**
(Models 4448c, 5848qc/qdc & 5948qc)

**Initial Boot-Up**

Upon initial boot-up, the unit will attempt to configure the network settings using DHCP. Once the unit has obtained an IP address, 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 & Date.

You will now be able to enter your Citrix Settings to connect to your server. You may select the connection type (options include Storefront for Web, StoreFront for PNAgent, XML Broker) and carefully 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.
5848qc Zero Client for Citrix

5948qc Zero Client for Citrix

Components included

- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
**Launch Pad**

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

- Display Configuration
- Sound 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 of the Citrix 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.
6. If you have a wireless card installed, click the Add button and then click the Refresh button to see which wireless networks are available for you to connect to.
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have setup 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 the 10ZiG Management Software or on the unit itself. Enter the System Settings – Control Panel. Under the System area click Security Settings and check the Lock down control panel check box. Then add a password to this to prevent the user from accessing the control panel.
Thin Client for **Parallels RAS NOS™**
(Models 4448p, 5848qp/qpd & 5948qp)

**Initial Boot-Up**

Upon initial boot-up, the unit will attempt to configure the network settings using DHCP. Once the unit has obtained an IP address, 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 & Date. You will now be presented with the Parallels 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 Parallels server.

**Components included**

- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
Parallels Client Setup

Select your connection type, input your Connection Server network or IP address. If needed configure your Port and Connection Mode. Then Click OK.

You have the ability to preset your Username, Password and Domain settings to connect to your Parallels Server under the Authentication Option.

By Clicking OK on the Parallels settings, you will see the Dialog box shown right called the Launch Pad.
Launch Pad

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

- Display Configuration
- Sound 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 of the Parallels 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.
6. If you have a wireless card installed, click the Add button and then click the Refresh button to see which wireless networks are available for you to connect to.
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have setup the Parallels 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 the 10ZiG Management Software or on the unit itself. Enter the System Settings – Control Panel. Under the System area click Security Settings and check the Lock down control panel check box. Then add a password to this to prevent the user from accessing the control panel.
Thin Client for RDP NOS™
(Models 4448r, 5848qr/qdr & 5948qr)

Initial Boot-Up
Upon initial boot-up, the unit will attempt to configure the network settings using DHCP. Once the unit has obtained an IP address, 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 & Date. You will now be presented with your RDP 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 RDS server.

Components included
- Thin Client Device
- Thin Client Stand
- Power Supply
- USB Wheel Mouse
- VESA Mounting Bracket (Optional)
- Wireless Adaptor (Optional)
- DVI to VGA Adaptor (Optional)
RDP Client Setup

Enter your RDS server name or IP address in the Server field. You may include and save credentials here as well. Make sure to set Security settings; most 2008R2 and newer servers use NLA. If you use a load balancer or RD Gateway, you enter them under the RD Gateway option.

By clicking OK on the RDP settings, you will see the Dialog box shown right called the Launch Pad.
Launch Pad

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

- Display Configuration
- Sound 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 of the RDP 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.
6. If you have a wireless card installed, click the Add button and then click the Refresh button to see which wireless networks are available for you to connect to.
7. Enter your wireless settings including WEP/WPA/WPA2 key.

Locking Down the Zero Client

Once you have setup the RDP 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 the 10ZiG Management Software or on the unit itself. Enter the System Settings – Control Panel. Under the System area click Security Settings and check the Lock down control panel check box. Then add a password to this to prevent the user from accessing the control panel.
10ZiG PCoIP V1200 Series Zero Clients
(Models V1200-P, V1200-QP, V1206-P, V1206-PD, & V1206-PDS)

Components included

✔ Applicable V1200 Series Zero Client Model
✔ Power Supply
✔ Cable Adapter for Dual-Link DVI (Optional)
✔ Ethernet Cable
✔ Quick Start Guide
✔ VESA Mounting Bracket (Optional)

V1206-PD Zero Client
**Installation Steps**

1. Connect USB keyboard and mouse.
2. Connect one end of Ethernet cable of the Zero Client and the other end to a switch/router.
3. Connect monitor cables to the Zero Client.
4. Connect speakers and/or headphones (optional).
5. Connect power supply to the Zero Client and a power source.
6. Press front panel button to power on the Zero Client.

---

**Default IP Address**

The Portal is set to DHCP client mode by default. Normally, the IP address of the portal is assigned by the DHCP server on your IP network. If your IP network does not have a DHCP server, the portal will fall back to a static IP address mode after a timeout period of approximately 2 minutes. In the fall back static IP address mode, you can access the Portal web interface to disable DHCP client mode and assign a static IP address. The portal’s fall back IP address is 192.168.1.50.
Quick Configuration

Click on OPTIONS on the top menu bar and select, CONFIGURATION.

1. Set manual IP if desired on the NETWORK TAB, or IPV6 tab for manual IPv6 addresses.

2. On the SESSIONS tab choose the correct Connection Type which matches your PCoIP environment and/or the desired user experience.
   - Direct To Host: options for connecting directly to a 10ZiG PCoIP host card.
   - View Connection Server: option for connecting via a VMware View Server
   - Connection Management Interface: used to communicate with an external connection management server.

3. In the DNS Name Or IP Address box enter your VMware View Connection Server/10ZiG PCoIP Host Card/Connection Manager’s IP or DNS name.

4. Optional configuration settings such as Username, Password, Desktop etc. are presented depending on the Connection Type chosen.

5. Under the ADVANCED button on the SESSIONS tab you will have the chance to change various custom options such as Desktop Name, Port#, Auto Connect, Remember Username etc.

6. To create a password to lock out settings changes, you can click OPTIONS and then PASSWORD to create a password for the device. This will disallow settings changes via the On Screen Display without using the password. By default, the password field is left blank – just click the “login” button.

As you make changes remember to click APPLY to commit the changes and continue in the settings applet, or OK to commit the changes and close the settings applet. Some of the options and configuration settings can be dependent on your VMware View Network or Authentication configuration.
VMware View Certificate Checking Mode

(Unsecure & Secure Connections)
The default setting on any certified VMware View Client is to warn the user if you are connecting to an unsecured VMware View Connection Server. If you are not using https/SSL certificates to secure your VMware View environment you may set your V1200 Series unit to not verify the server’s identity.

1. Click on OPTIONS on the top menu bar and select USER SETTINGS
2. On the VMware View tab change the option from Warn Before Connection to Untrusted

Servers (Default) to the Do Not Verify Server Identity Certificates.
As you make changes remember to click APPLY to commit the changes and continue in the settings applet, or OK to commit the changes and close the settings applet.
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. 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.

Manager – Server or Web? Installation is Going To Be Easy

• Implement 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. Web Management allows management of your Clients from all major browsers (Firefox, Chrome, Internet Explorer, etc.), providing real-time status of all Clients from a single comprehensive page.

Cloud Management Technology? Yeah, We’ve Got That

• Our Cloud Agent supports internet connectivity and manages locations like smaller offices and home 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 and Configuration? We Have This Covered

• Whether manually or automatically populated, organized groups provide a simple, more logical way to configure, monitor, and manage devices. The 10ZiG Web Console includes a thorough configuration tool to quickly change all settings with nearly the same features as the 10ZiG Remote Console, as well as being able to use VNC with all clients.
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 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 on www.10zig.com. There, easily search by keyword or product type for tons of prepared and helpful information.

While you’re there, sign up to receive 10ZiG Technology & Firmware Updates! 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.com for EMEA. (Note: Suggestions for FAQs are always welcome for review.)

10ZiG Product Warranty & Terms

The 10ZiG Thin & Zero Client Warranty is one of the best standard warranties in the marketplace today. Our units are covered by a 3 year advance hardware exchange (return freight is also covered), 3 years of tech support and 3 years of software upgrades.

For full U.S. Product Warranty, see here:

For full EMEA Product Warranty, see here: