ThinLinX Management Software

FREE for TLXOS Customers

User Manual

Version 8.4.1

February 17, 2023

1 Introduction

ThinLinX Management Software (TMS) provides the ability to configure and manage any device running the ThinLinX Operating System (TLXOS) from anywhere in the World

TMS can be used for a variety of tasks, ranging from something as simple as rebooting a TLXOS device, applying hotfixes, to upgrading the device with the latest TLXOS software. TMS runs on Windows and Linux, supports all TLXOS devices including Raspberry Pi devices, Intel & AMD Small Factor devices such as the Intel NUC's & clones, Compute Sticks and Re-Purpose PC & Laptops.

2 TMS on Windows installation

TMS is available as a downloadable self-executable. The same executable runs on both 32 and 64 bit versions of Windows. To install TMS, download the .exe installer file from here https://thinlinx.com/download/ onto your Windows system, double click the downloaded file and follow the instructions.

3 TMS on Linux installation including TLXOS devices

TMS is available as a downloadable Ubuntu, RePC or RPi .deb package and as a Redhat / Centos .rpm package, to install the Ubuntu Linux package copy the file to your Linux system and install with the command

"dpkg –i tms-filename.deb"

To install the Redhat / Centos .rpm package, copy the Centos Linux package to your Linux system and install with command

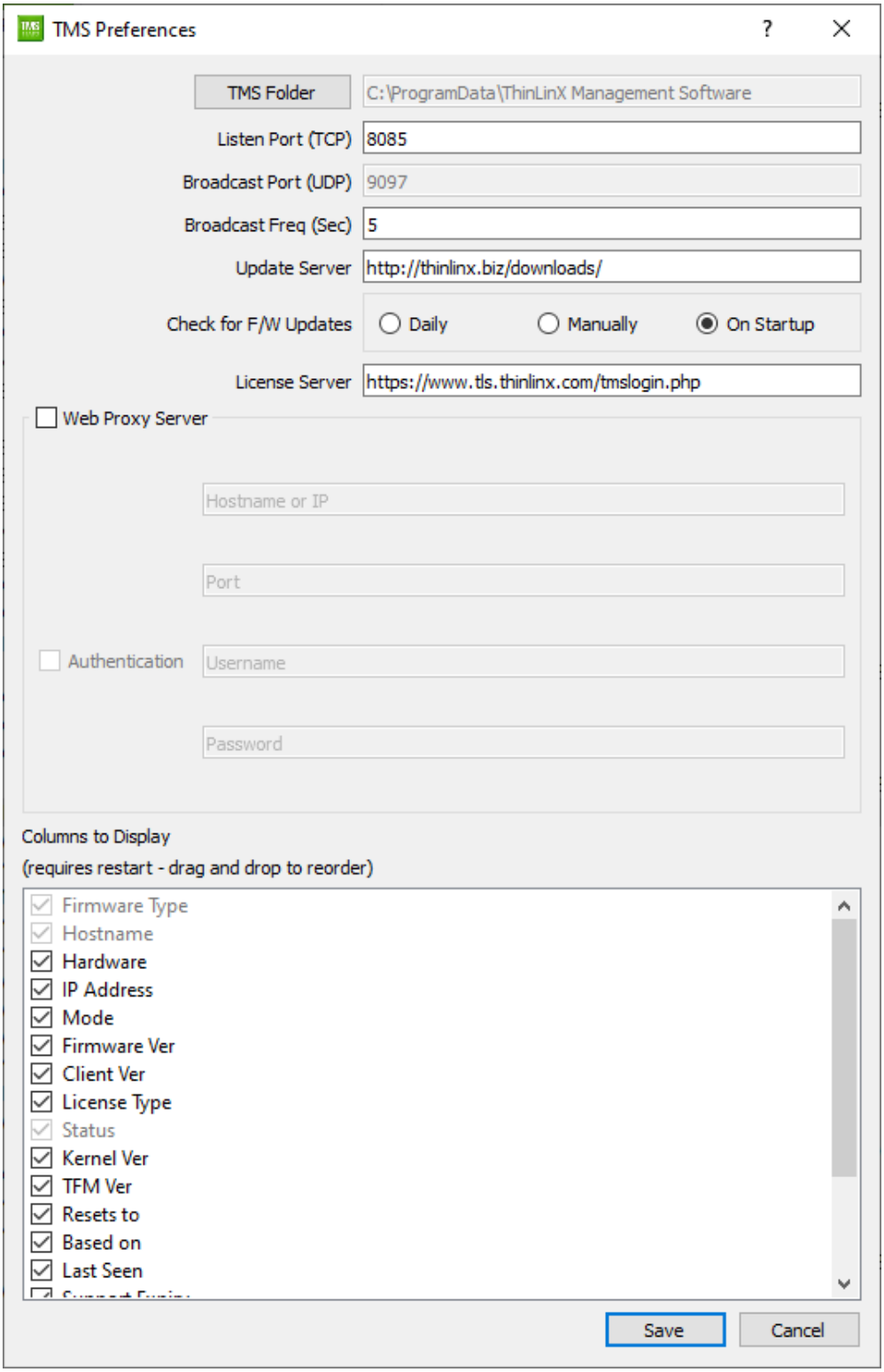
"rpm –i tms-filename.rpm"

4 Starting TMS

Start TMS by double clicking on the desktop shortcut

5 Configuring TMS

When installing TMS the recommended procedure is to accept the default installation directory. The first time TMS is run on a system, the TMS Preferences dialog appears. Any time after installation you can manually launch the TMS Preferences dialog if required by clicking on *Tools -> Options*. The TMS Preferences box is shown below



TMS Folder denotes where TMS will store firmware updates, hotfixes and temporary data and also department configuration files

Listen Port (TCP) denotes the SSL port number that will be used by TMS. All communications between TMS and TLXOS devices are SSL encrypted. The connection between the TLXOS client and TMS is initiated by the client allowing the encrypted data to travel through Firewalls allowing remote management from anywhere in the World. The default SSL port is 8085. If you change this port number on TMS, you need to close TMS and restart it. If you are using DHCP or Static TMS Discovery on TLXOS you must also change the Port number there to match the TMS Port number used by TMS. If you are running TMS on a Linux system, the SSL port must be > 1024 as any port number < 1024 can only be accessed by a program running with root permissions.

Broadcast port (UDP) denotes the port used by TMS to send broadcast packets to TMS Clients and is used for initial communication. The default port number is 9097 and cannot be changed

Broadcast frequency defines how often TMS transmits a UDP broadcast packet. This packet contains the TMS Hostname and Port number, the default value is 5 seconds. The TMS client end of the connection is integrated into TLXOS and by default listens for the UDP broadcast, then connects to TMS using the information provided in the UDP broadcast.

Update Server shows the default Server for downloading updates using TMS, do not change this unless you are operating a highly secure Network without Internet access and have purchased the ThinLinX Download and License Server Virtual Appliance.

Check for F/W updates you can check Daily, Manually or On Startup for Firmware updates, the default setting is On Startup

License Server shows the default License Server, do not change this unless you are operating a highly secure Network without Internet access and have purchased the ThinLinX Download and License Server Virtual Appliance.

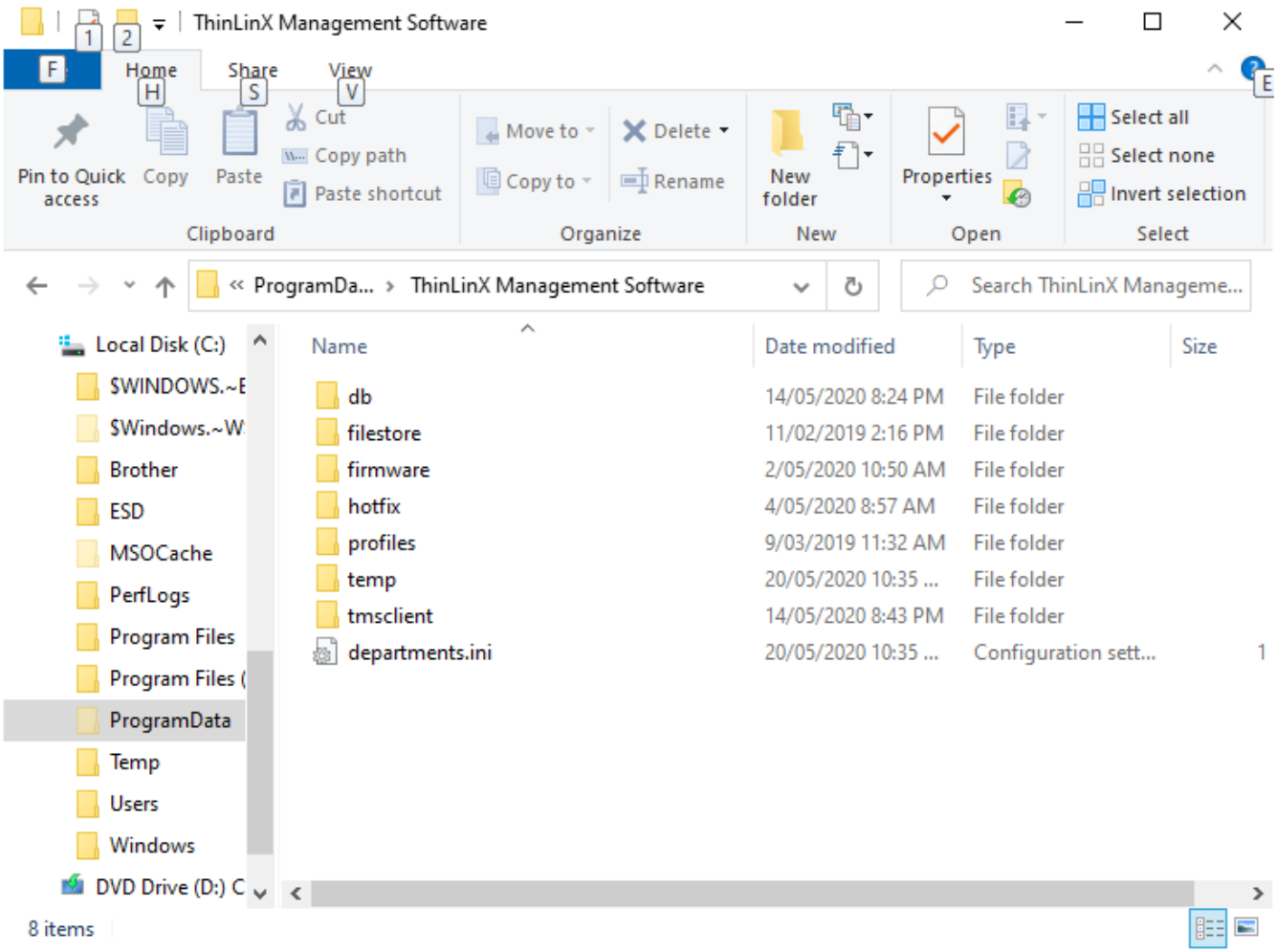
Web Proxy Server checkbox enables the TMS Administrator to set the Hostname or IP Address of a proxy server. This may be required to allow TMS to access the Internet on some Networks. Internet access is required to download Firmware updates and License Products running TLXOS.

Authentication some proxy servers require a Username & Password before allowing access to the Internet. Enter your Proxy Server User name and Password here

Columns to Display allows for custom fields to be displayed within the TMS device discovery frame. This includes the removal or addition of fields and the ability to reorder the fields in top to bottom preference order. Firmware Type, Hostname & Status are greyed out as they are always displayed.

If you make any changes to the above settings, you must restart TMS to allow the new settings to take effect.

In the image below you can see the seven subdirectories that are created when TMS is installed.



The db directory is the TLXOS devices configuration database which contains information on every TLXOS device ever detected by TMS. If you dispose of a device you can delete it from the TMS database by using TMS -> Device -> Delete Device

The filestore directory is reserved for a future release of TMS

All firmware images downloaded via the TMS Download Icon are automatically unzipped in the firmware directory.

All Hotfixes downloaded via the TMS Download Icon are automatically unzipped in the hotfix directory.

The profiles directory is used for storing profiles that are created with TMS and then deployed to one or more devices. To save a Configuration (Profile) highlight a TLXOS device, then choose TMS -> File -> Save Configuration. To copy that Configuration to any Highlighted devices of any type choose TMS -> File -> Load Configuration

The temp directory is used to store TMS configuration information such as which devices are located in each Department

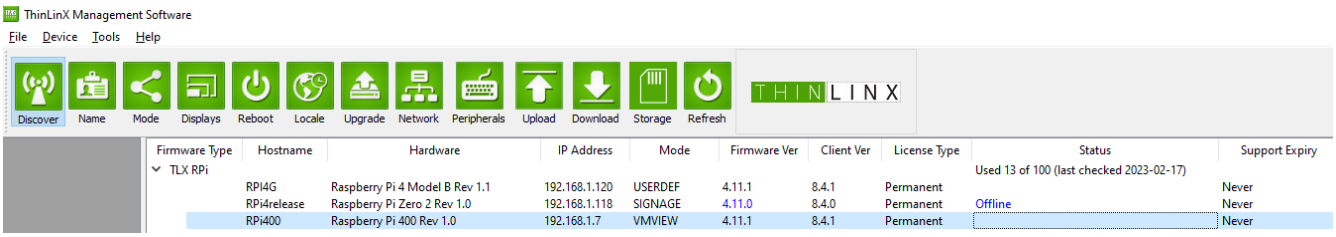
The tmsclient directory is used to store updated versions of the TMS client, these are downloaded using the TMS Download Icon

6 TLXOS device discovery via TMS

TMS utilizes four methods to discover TLXOS devices, the default is UDP Broadcast but this is only effective when the TLXOS device is on the same Network Subnet as the system running TMS. TLXOS devices listen for UDP broadcasts that contain the TMS server Hostname and port number. When TLXOS receives this broadcast, it extracts the information and connects to a TMS server over an encrypted SSL connection. Thereafter, all communication between TMS server and a TLXOS device is secured.

You can configure the UDP broadcast frequency in seconds using TMS -> Tools -> Options

To toggle the UDP broadcast on or off, click on the Discover Icon as shown below



The default setting is UDP discovery turned on. When TMS is launched this commences the TMS server packet broadcast via UDP to all TLXOS Clients. Once acknowledged, the TLXOS devices then connect to the TMS server and display/populate under the TMS client area

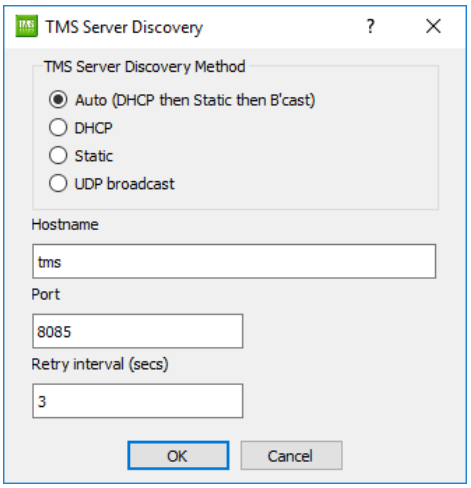
Highlighting one or more devices allows the Administrator to send commands to the highlighted TLXOS devices. This also allows for more than one TLXOS device to be selected and sent commands at the same time.

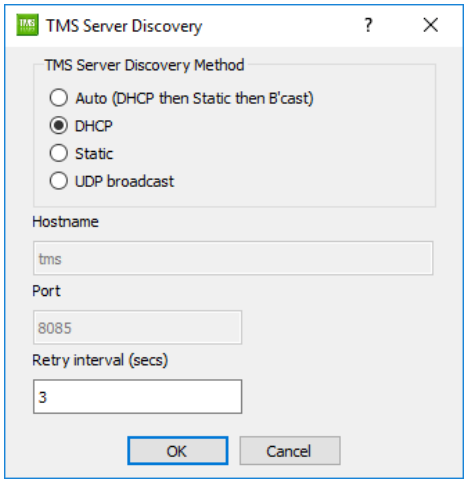
If UDP discovery is being used do NOT run more than one instance of TMS on the same Network

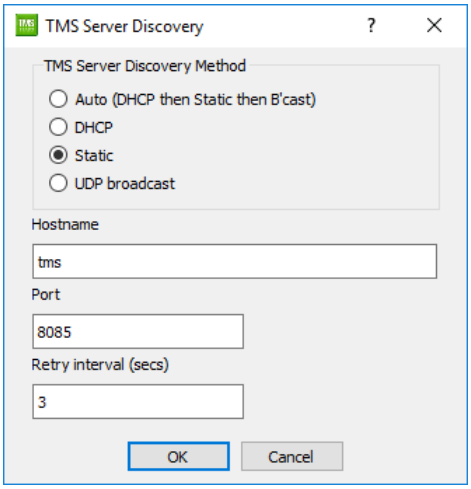
Subnet as the TLXOS clients will connect to the first instance of TMS that they receive UDP packets from. As they are already connected to TMS they will NOT appear on the second instance of TMS. In some circumstances some TLXOS devices will be connected to one instance of TMS and others will be connected to the second instance. The Golden rule is to only run one instance of TMS when UDP Discovery is used. TMS is not designed to be multi-user yet (but we are working on a multi user version), you should only run one instance, this is also important especially if you have configured TLXOS to connect to TMS at a fixed IP Address using DHCP Option flags or Static discovery

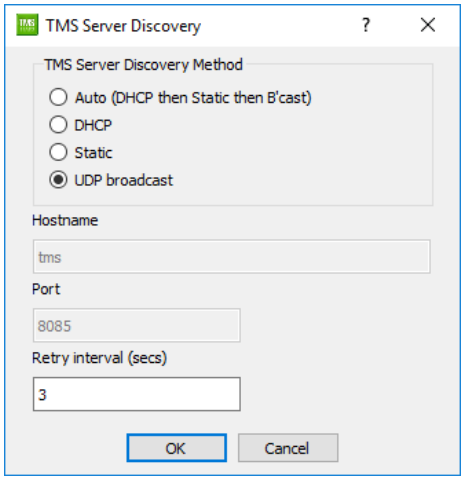
TMS and TLXOS devices must be on the same network subnet for UDP Broadcast discovery of TLXOS devices to be successful. If the TLXOS devices are to be located on a different Network Subnet or in a Branch Office then either DHCP or Static Discovery must be used unless one TLXOS device has been configured as a TMS Beacon.

To manually configure the TMS Discovery method, select TMS -> Device -> Network Configuration -> Configure TMS Discovery. For Static discovery a default Hostname of “tms” has already been entered in the Static and Auto Hostname dialog box by ThinLinX. The advantage of this method of discovery is the System Administrator can set a DNS CNAME which assigns “tms” to the Hostname of the system running TMS. No configuration is required at the client as TLXOS will be able to use DNS to resolve the “tms” Hostname and the default Auto choice will use Static Discovery if DHCP options have not been configured. Note in the images below that the DHCP & UDP Broadcast choices automatically “Grey” out the Hostname & Port









If a different Port number than the default 8085 is chosen you must also set the same Port number on TMS via the Tools Options Dialog Box. If you are using DHCP or Static TMS discovery you may need to select the checkbox next to DHCP or Static instead of Auto if discovery is not working on your Network after closing and then later re-opening TMS. If your devices do not reappear after you close TMS and then reopen TMS at a later time you should manually select Static or DHCP

7 DHCP option flags for TMS discovery & TLXOS configuration

DHCP option flags can also be used to point the TLXOS device to TMS which could be located on a system anywhere in the World. TLXOS just needs to know the Hostname & Port number to initiate the connection to TMS. As the connection is initiated by TLXOS from inside the Network it can tunnel out of the Network using a secure SSL connection to the TMS system located anywhere. This makes it possible to manage TLXOS devices located anywhere.

Vendor specific DHCP options (also known as site specific DHCP options) must be configured on the Network DHCP Server. When vendor specific DHCP options are used, TMS Clients automatically connect to a nominated TMS server on boot up, additional information may also be passed to TLXOS devices such as the Hostname of the Remote Desktop Server to connect to, the Mode to use for the connection, e.g. Citrix HDX, VMware Horizon, Microsoft RDP etc. Also Mode arguments specific to the selected Mode can also be passed using DHCP

The following vendor specific DHCP options are supported by TLXOS devices;

Note: The DHCP Data type MUST be configured as text NOT integer for all five options below

Option name	Code number in decimal	Data type
tlx-tms-server	231	text
tlx-tms-port	232	text
tlx-mode-server	233	text
tlx-mode	234	text
tlx-mode-args	235	text

tlx-tms-server specifies the Hostname or IP address of the TMS server on the network. When a TLXOS device detects this setting, it will attempt to automatically connect to a TMS server at this hostname or IP address on port number specified by option tlx-tms-port. When Option tlx-tms-server is specified, you **must** also specify Option tlx-tms-port.

tlx-tms-port specifies the SSL port on which the TMS server is listening. This setting **must** match the SSL Port setting in TMS preferences, which is configured using TMS -> Tools -> Options, otherwise TLXOS devices will be unable to connect to the TMS server.

tlx-mode-server specifies the Server Hostname or IP address that TLXOS devices should connect to for their Remote Desktops

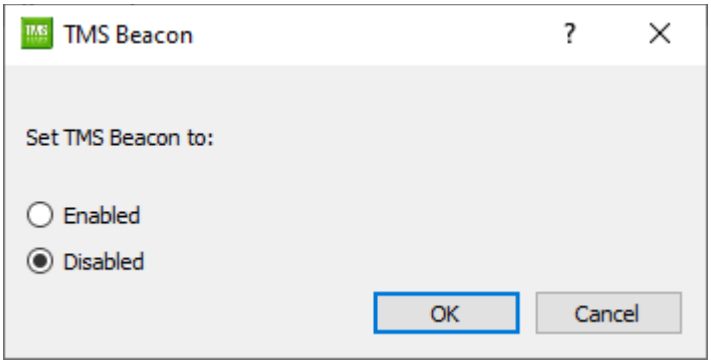
tlx-mode specifies the protocol that TMS Clients should use to connect to the remote server. Possible values must be lower case, and are dsi, hdx, vmview, desktop, mplayer, nx, rdp, spice, ssh, tn3270, tn5250, telnet, userdef, vnc, web, x11.

("dsi" means "digital signage", "local" means "Local Desktop", and "vmview" means "horizon")

tlx-mode-args specifies the optional argument to be added to the connection request. e.g. If your Windows Desktop HDX name in Storefront is Windows10 you would add Windows10 as the tlx-mode-args value

To connect to a Website in Kiosk mode you would set option 233 to http://wherever/whatever, Option 234 would be web and Option 235 would be –kiosk

8 TMS Beacon mode discovery



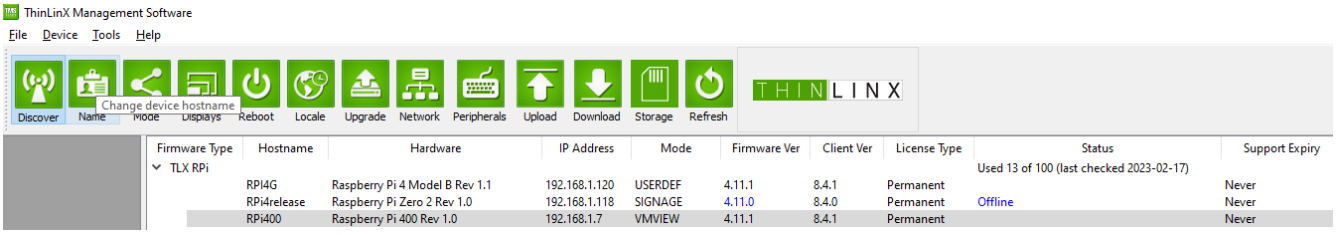
TMS Beacon mode can be switched on or off for any TLXOS device using Device -> Network Configuration -> Optional Services -> Configure TMS Beacon

Starting from TLXOS 4.10.0 and 4.8.2 LTS, we added the TMS beacon as a TMS discovery aid. This is a TMS broadcast repeater, which a nominated TLXOS client on a different subnet than the TMS server can be configured to start. Clients on the same IP subnet as the beacon that use (or fall through to) the broadcast discovery method will detect this signal and connect to the TMS server that it names. This will of course stop working if the client that runs the beacon is shut down or put into Maintenance Mode.

Once a client is connected to a TMS server, it will keep the connection open and talk to that server exclusively until it is rebooted (sending keepalives every few minutes to prevent intervening firewalls from closing the connection). If clients can fall through to UDP discovery, it is therefore important that you do not run multiple copies of TMS in the same IP subnet, or else clients will connect to whichever TMS instance they detect first and will not appear in the other.

9 Assigning a Hostname to a TLXOS device

TMS allows for the setting of a Hostname for selected TLXOS devices in the interest of better identification on the network. To assign a Hostname to a TLXOS Device, highlight the Line by clicking on it, then click on the *Name* Icon as shown below;

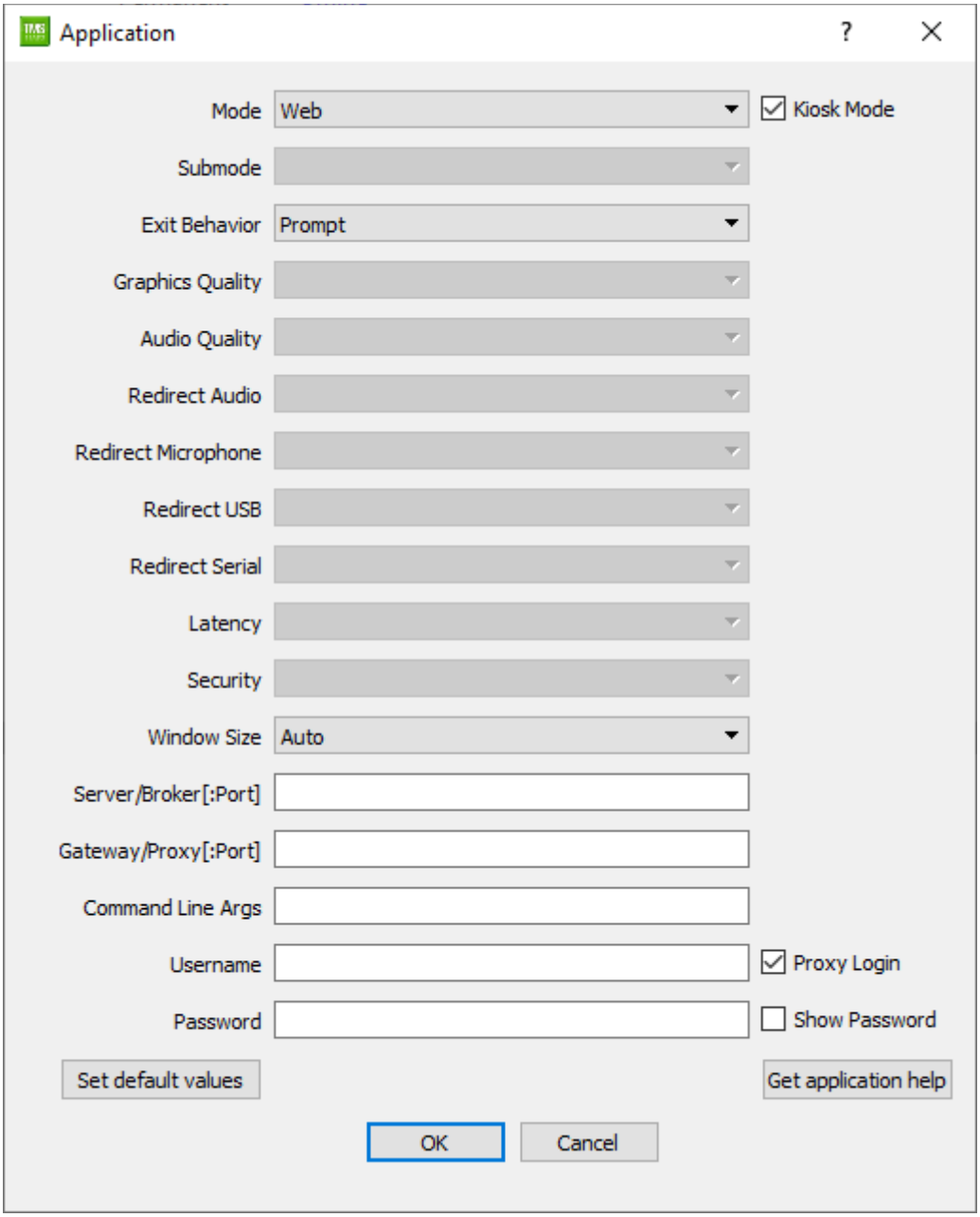


10 Setting the Remote Server and Connection Mode

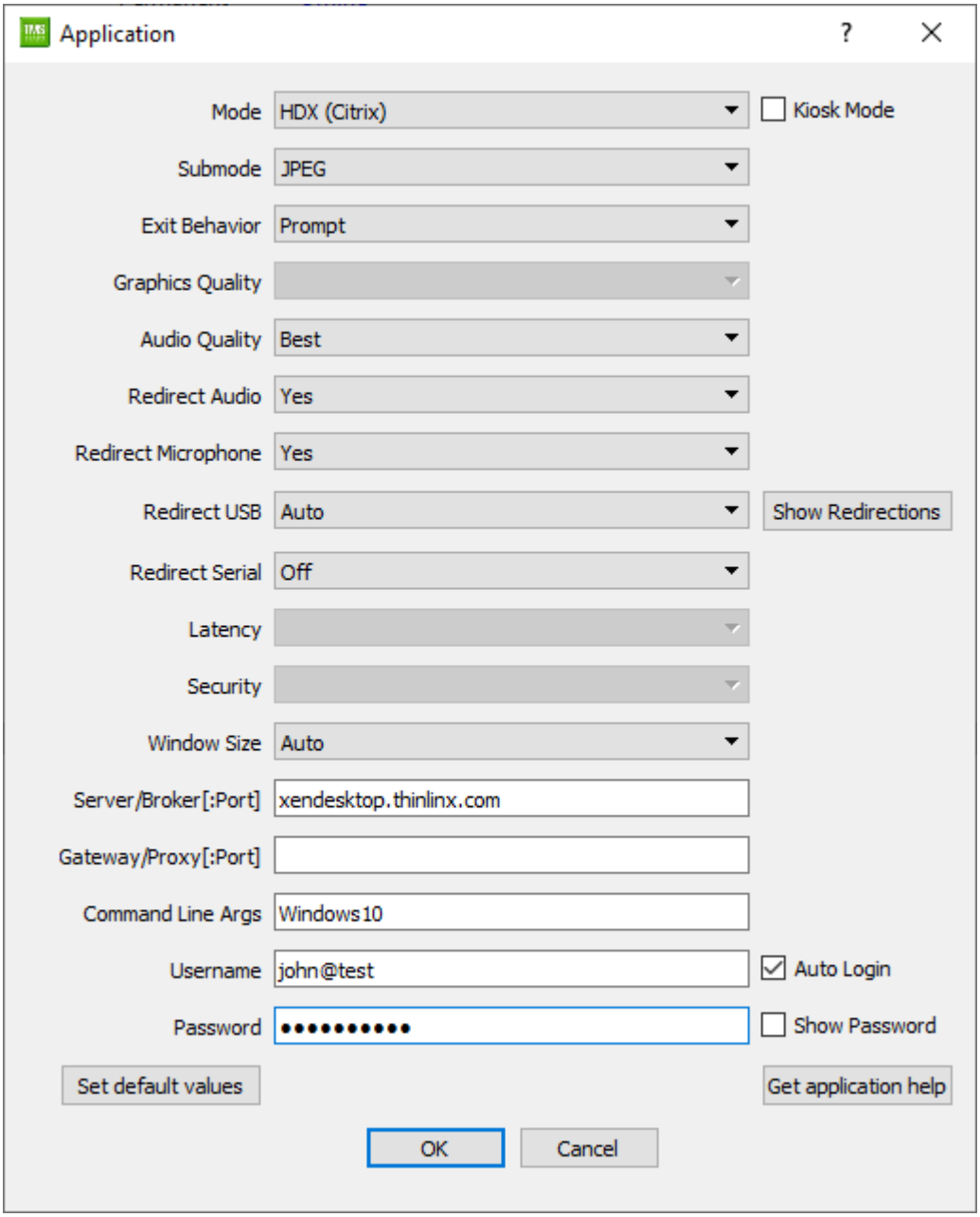
When a TLXOS device boots, if configured correctly it will automatically connect to a Remote Server using the specified connection Mode. Up to 18 different connection Modes can be configured. These connection types are

a) Digital Signage, changes the mode to Digital Signage. Please download and read the https://thinlinx.com/dsi-quick-start-guide.pdf
b) Digital Signage (Legacy) Please download and read the https://thinlinx.com/dsi-quick-start-guide.pdf
c) Citrix HDX, launches the native Citrix Receiver interface which supports secure SSL connections only to a Remote Citrix Storefront. To use this mode you must have set up Citrix Storefront to accept SSL connections and copied your CA Certificate using TMS to the TLXOS device. See more details in the FAQ's at the end of this document
d) Horizon (VMware) Connect to VMware Horizon Hardware Accelerated Blast sessions on the Raspberry Pi or on Intel Small Form Factor and Re-Purpose PC connect with either Blast or PCoIP
e) Local Desktop mode, this places a taskbar with Icons for launching any application that is supported as a Mode choice. You must first configure the required Modes using the Mode icon and you can then launch multiple modes on the Local Desktop by selecting the required modes from the "Auto hide" taskbar on the left side of the Local Desktop screen. The Local Desktop mode can be used to simultaneously launch any combination of the available Modes
f) Media Player, runs a local Video / Audio Player
g) NX (NoMachine) launches an Open Source NoMachine client
h) RAS/2X (Parallels)
i) RDP, detects the capability of the Remote Desktop and then automatically launches either a RemoteFX or standard RDP connection to that Desktop
j) Spice, launches a Red Hat Spice Protocol client
k) SSH, launches a SSH session
l) TN3270, launches the TN3270 IBM Mainframe client
m) TN5250, launches the TN5250 IBM Mainframe client
n) Telnet, launches an Telnet client
o) User Defined (Bespoke) Enables a custom App to be launched
p) VNC, Launches Turbo VNC Viewer
q) Video Conference – Microsoft Teams for Linux
r) Web, launches a Web Browser, for many users this is the preferred method of launching Citrix Receiver for a Storefront connection as it supports both http and https sessions. We suggest that the user selects the Kiosk mode checkbox and enters the Storefront URL in the Server Name [:Port] arguments box on the Web mode Dialog box
s) X11, launches a X11 client to connect to a Linux Desktop using XDMCP

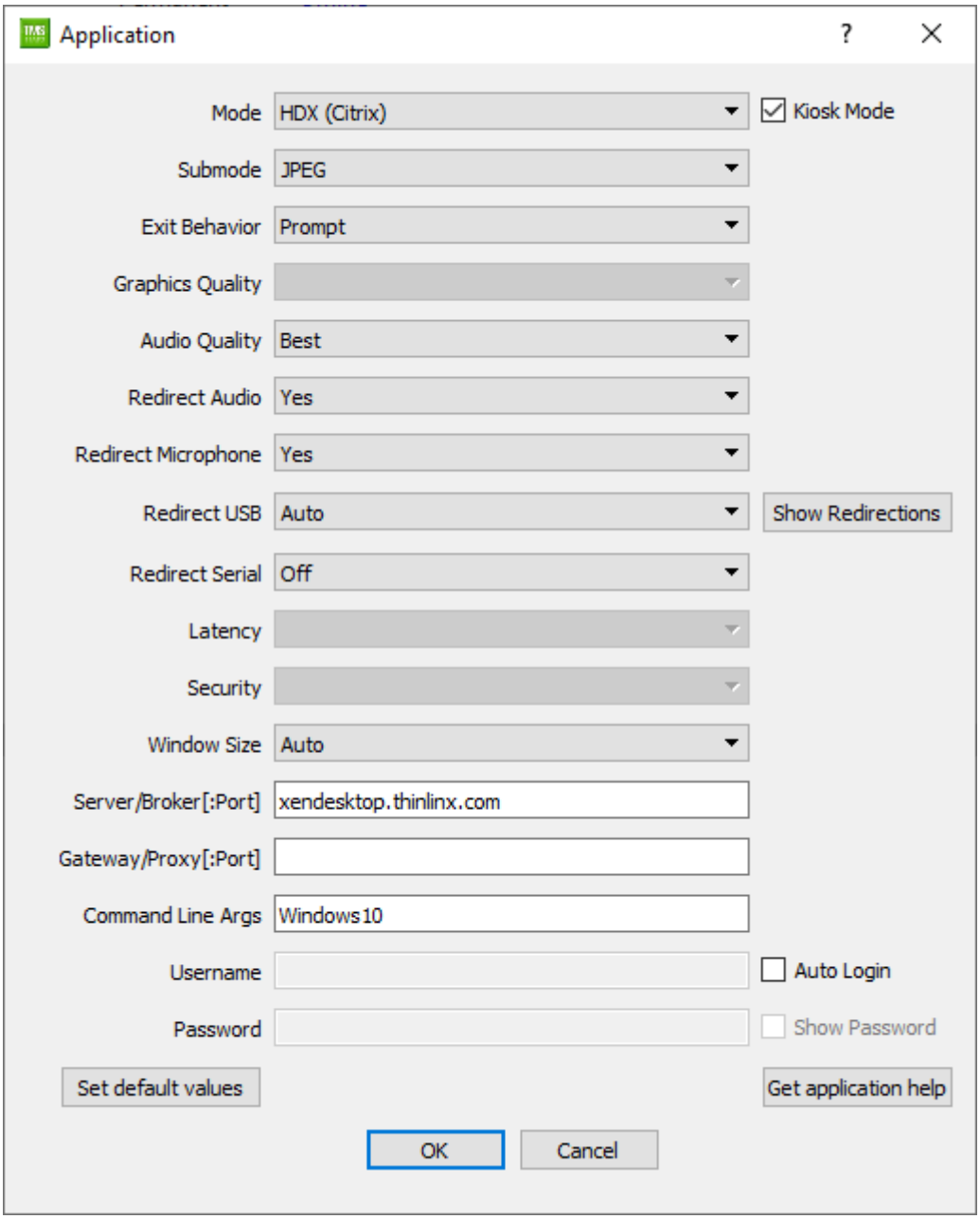
The hostname for a remote server can be configured via TMS. To configure the remote server, select one or more TLXOS Devices then click on the *Mode* Icon. Web mode is shown below, this has been configured with Kiosk mode selected to automatically launch a Citrix HDX session, and you may also select a Poxy Login in the case that you are using a NetScaler appliance as a connection broker. Note the greyed out selections which are not available



The image below shows a Citrix HDX native client session connection to Citrix Storefront, the Storefront name “xendesktop.thinlinx.com”, User Name, Domain and Password have been pre-configured, Auto Login is selected, the Desktop named Windows10 has been selected as the desktop to launch. This configuration will auto launch Windows10 and auto login

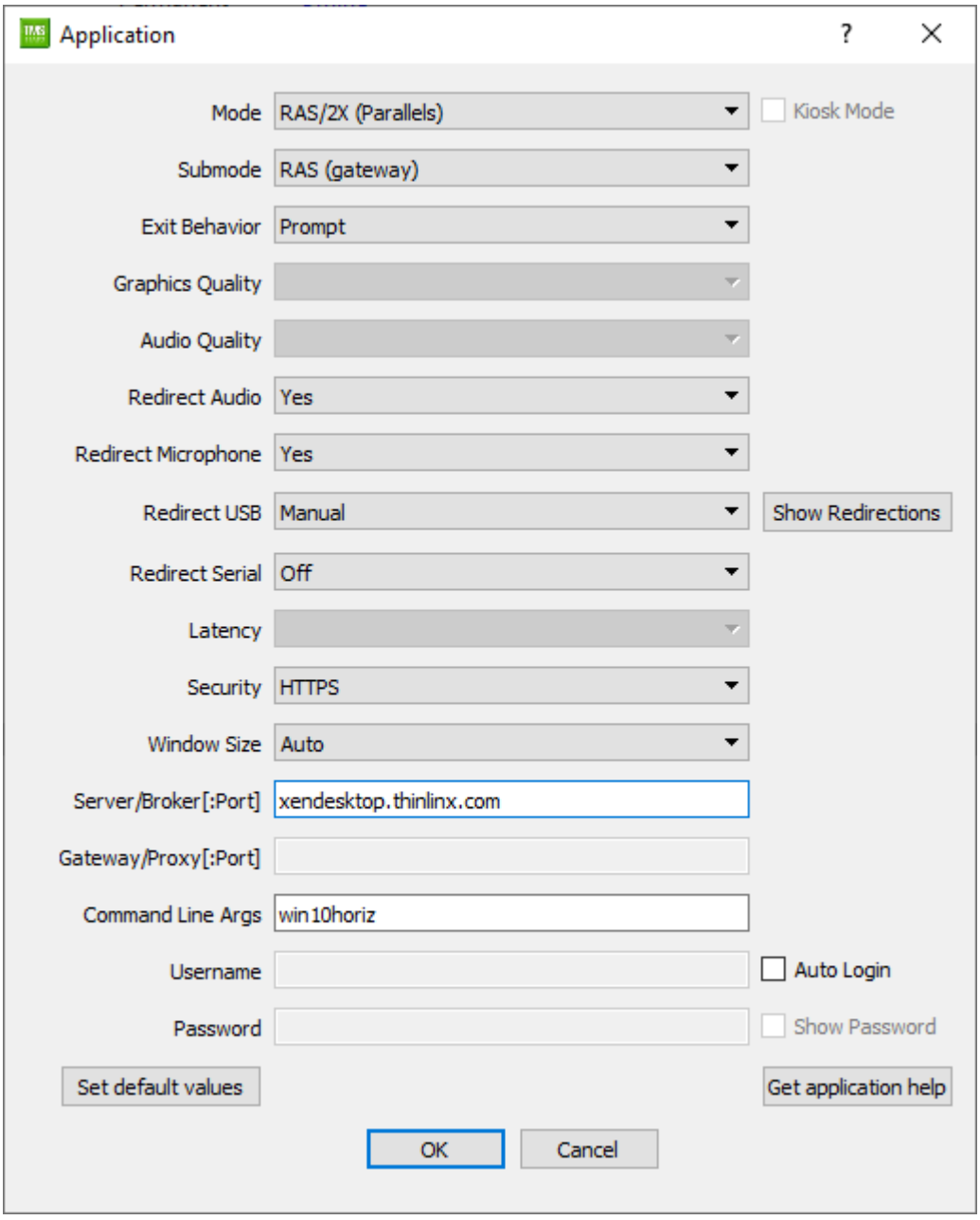


The image below shows a Citrix HDX native client session connection to Citrix Storefront, the Storefront name is “xendesktop.thinlinx.com” and the Desktop named Windows10 has been selected as the desktop to launch, the Kiosk Mode check box is ticked. This configuration will auto launch Windows10 and prompt for a Login ID & Password on first connection and also on every Log out of the Windows Desktop. This configuration locks down the desktop with the only dialog box on the Desktop being the Citrix Login Dialog



11 Configuring the new RAS/2X (Parallels) mode

The image below shows how to set up a RAS/2X (Parallels client). Enter the name of the Desktop or App (that you want to launch) into the Command Line Args dialog, in my case I have entered the name of my Windows10 VM which is win10horiz. I have also entered the RAS Server name of xendesktop.thinlinx.com in the Server/Broker [:Port] dialog



12 Setting the client protocol experience level

As per *Setting the connection type used to connect to a remote server,* the Application Protocol

dialogue box allows users to set various settings for TMS clients in relation to the experience level of various settings including;

Depending on the Mode selected many of these options will be greyed out

Color Depth sets the display color depth on the client, available settings are protocol dependent but may include 8 bit, High Color (16 bit), True Color (24), True Color (32) or Auto

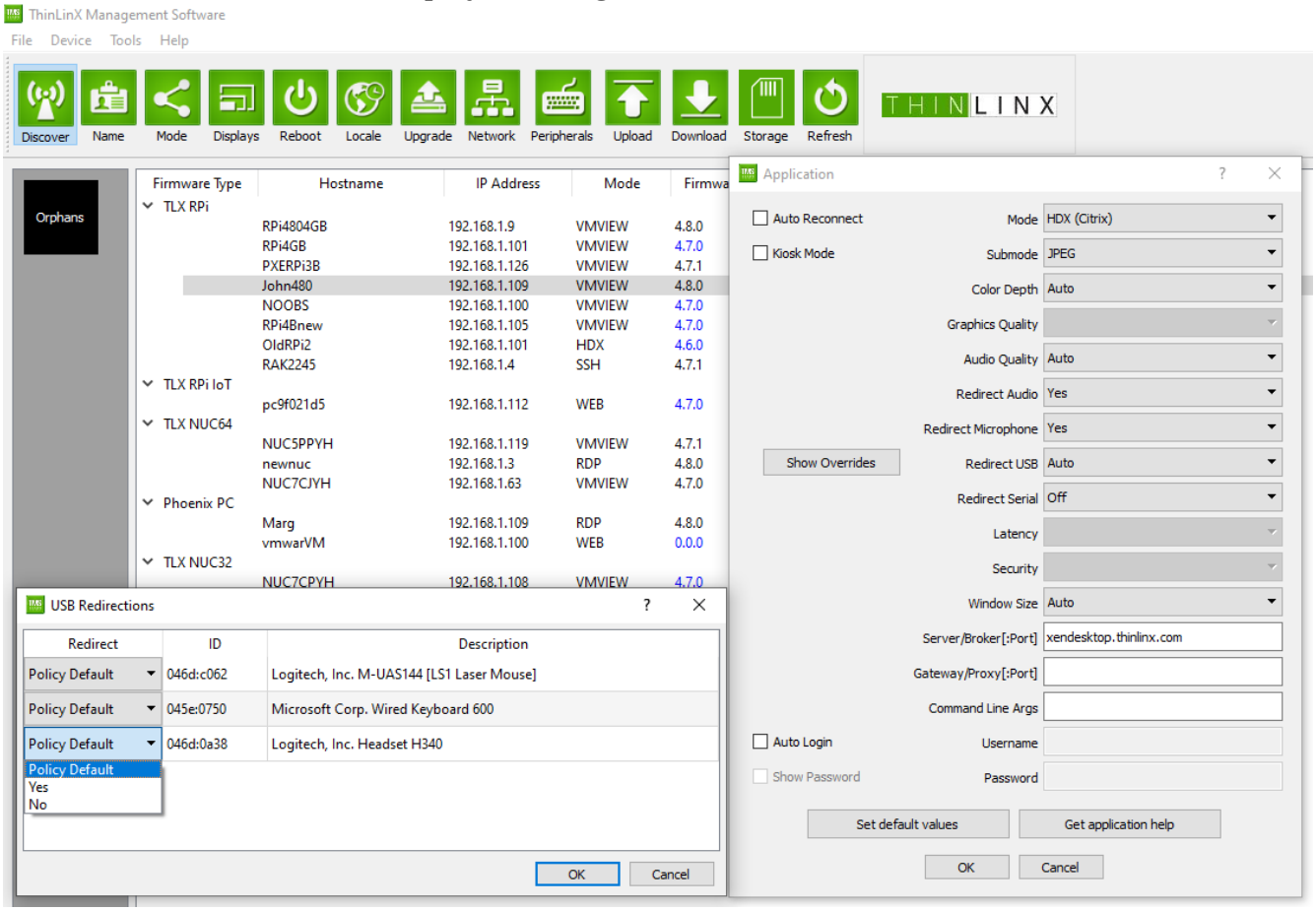
Graphics Quality sets the image quality and level of detail, translations depend greatly with protocol used: settings include High, Medium, Best or Auto

Audio Quality sets the audio quality, translations depend greatly with protocol used: settings include High, Medium, Best or Auto

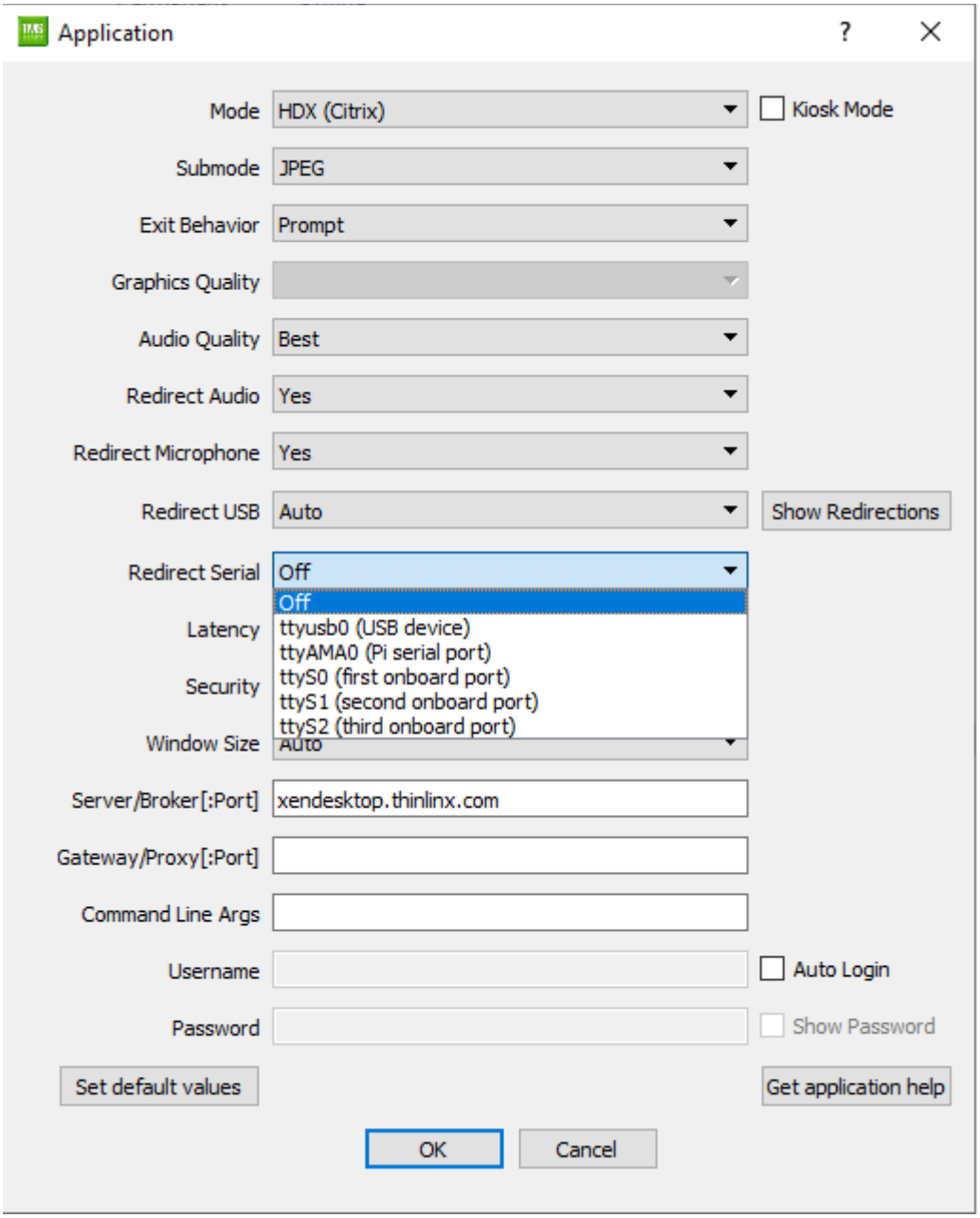
Redirect Audio enables the redirection of audio playback when available within the protocol selected, settings include Yes or No

Redirect mic enables the redirection of microphone input when available within the protocol selected, settings include Yes or No

Redirect USB normally set to Auto, Off or Manual depending on the Mode being configured, click on Show Overrides to display or change USB redirection defaults



Redirect Serial provides a list of serial devices to redirect



Latency sets optimizations for the type of network environment that the client faces when connecting to servers, settings include Low (LAN), Medium (WAN), High (Internet/VPN) or Auto

Security sets a security level baseline for the protocol used, depending on the Mode being configured, RDP options include Auto, NLA, SSL and RDP or if you are using VMware Horizon the Options are HTTPS (use for self-signed CA SSL Certificates) or HTTPS (strict validation) otherwise.

Window Size sets the window size for the established remote session on the client, options

include Full screen, percent of screen (see below) and Auto

Window Percentage is enabled when *percent of screen* is enabled within *Window Size*, options range from 0-100 percent, the default is 80%

Server/Broker[:Port] enter the Name or IP Address of the Remote Desktop, Citrix Storefront or VMware Horizon Server

Gateway/Proxy[:Port] enter the Name or IP Address of the Gateway/Proxy

Cmd line arguments enables the entry of command line strings that allow for specific features for the relevant protocol used, more information about these arguments can be found by clicking the *Get application help* Icon to display a list of available command line options

When entering command line arguments manually, you should not enter the command name or the hostname, just the command line arguments.

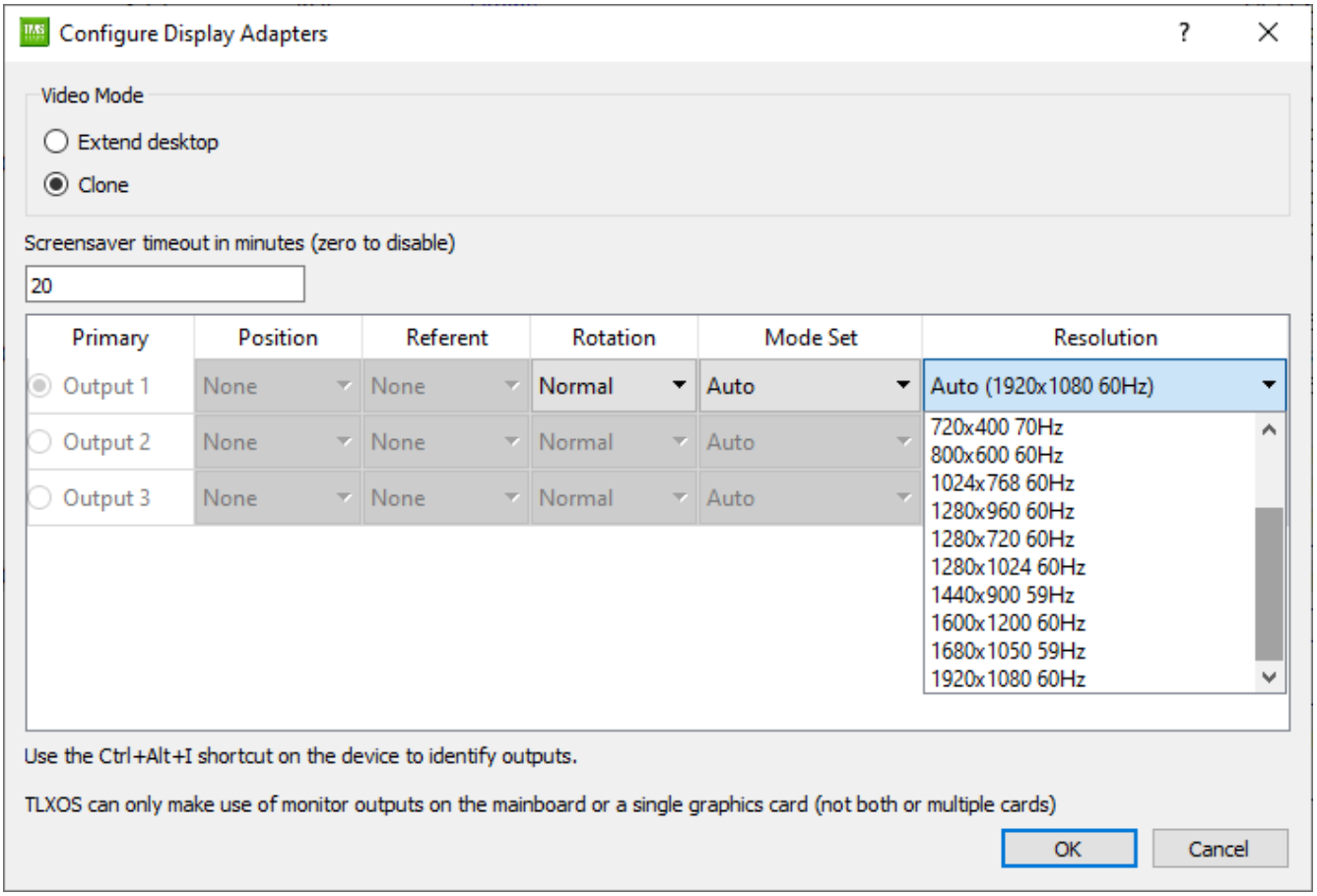
To delete previously set command line arguments, simply delete all commands and click on the OK Icon. To set new command line arguments, or to override previously set command line arguments, enter the new arguments and click on OK. If you just want to view the current command line arguments, double click on a TLXOS device or press Enter on any highlighted line

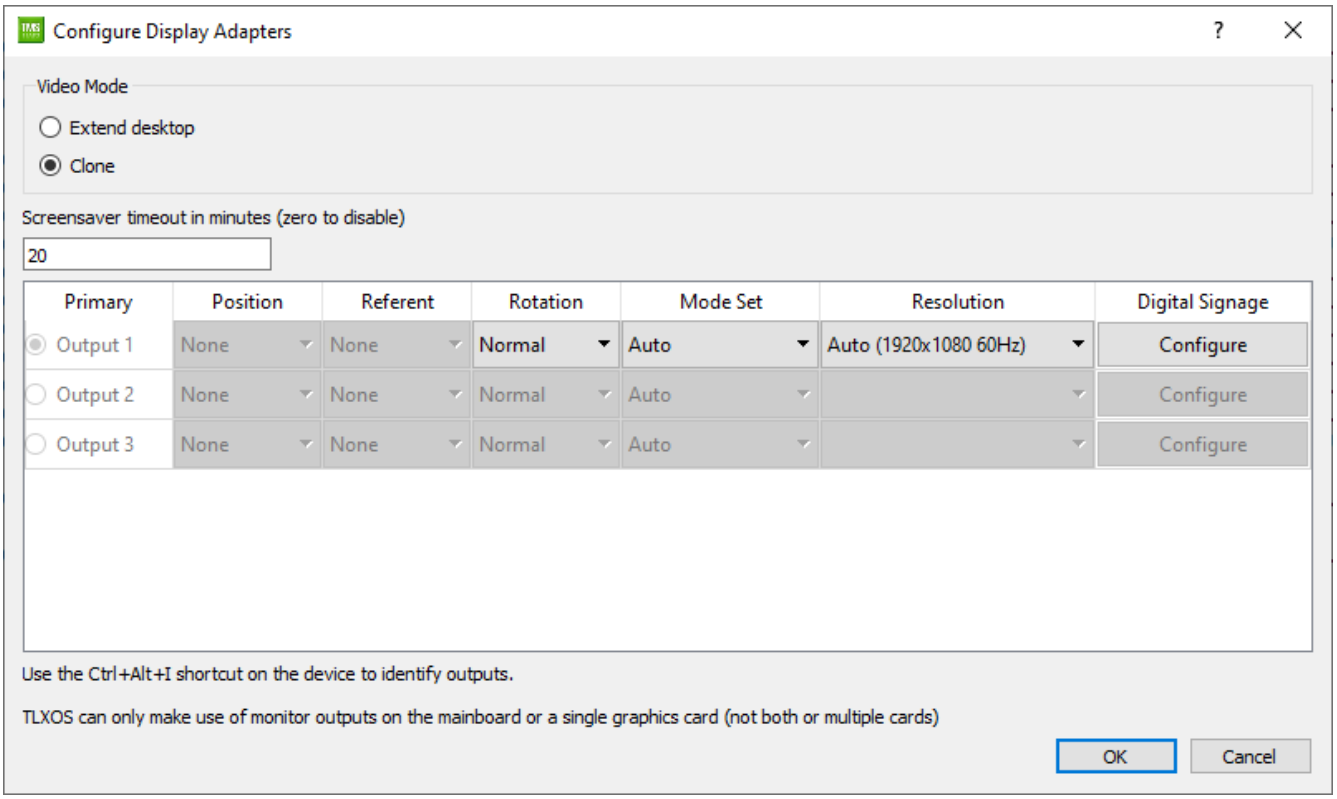
13 *Setting screen resolution & Screensaver on or off*

TMS allows you to set the Screen resolution on any TLXOS devices, this may be the Single or Dual Display Raspberry Pi, the Dual Display Intel NUC or a Re-Purposed PC. In most cases the Auto setting is the best option as it will select the most appropriate resolution for your Monitor. In the image below the Administrator wants to choose a valid mode from the RPi list below

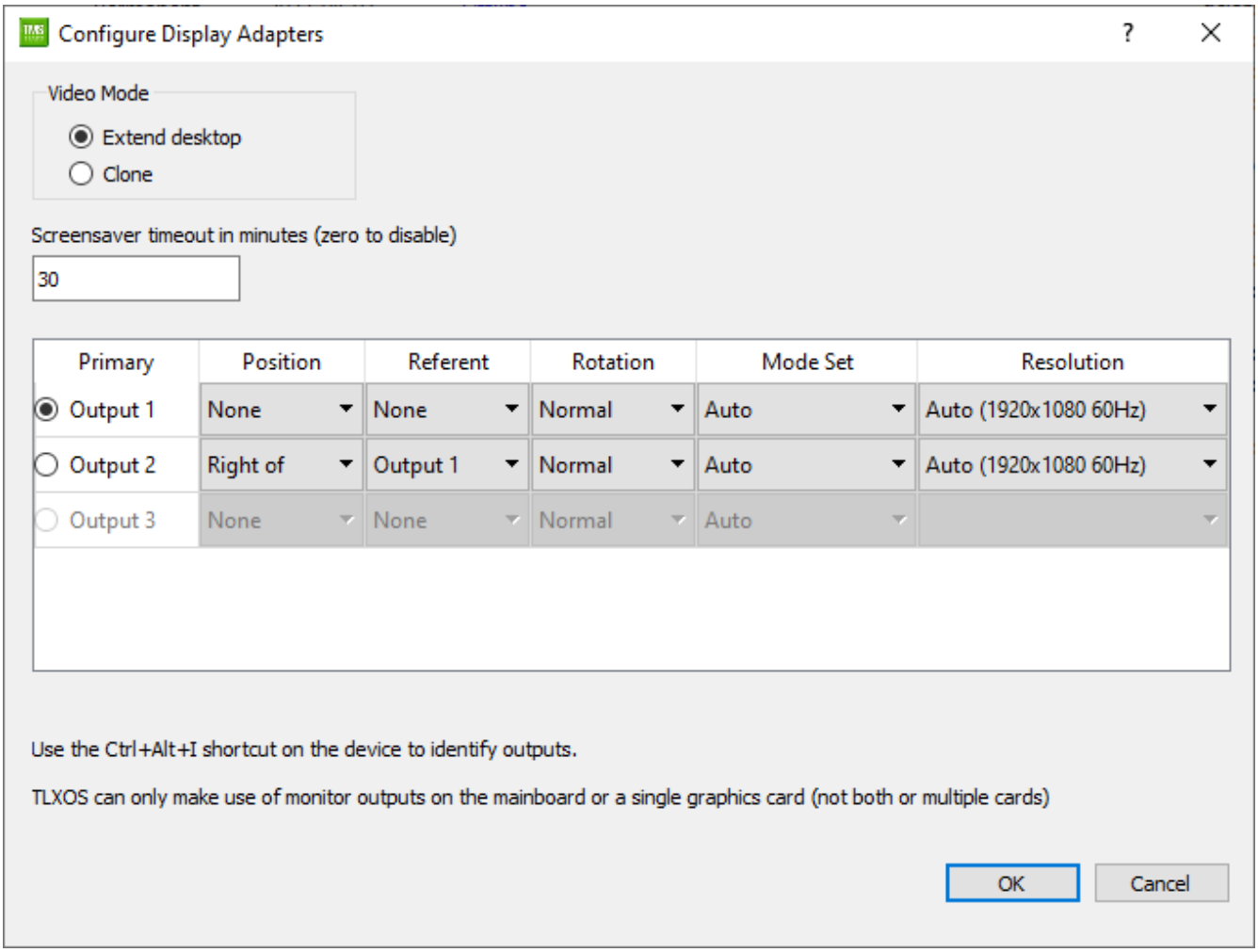
In the second image on the next page showing Configure Display Adapters if you have selected Digital Signage or Digital Signage (Legacy) as the mode you will notice that an extra column named “Digital Signage” appears on the far right with the button named “Configure” below it

Please download and read the https://thinlinx.com/dsi-quick-start-guide.pdf to understand how to configure Digital Signage.


Configure Display Adapters
Video Mode
Extend desktop
Clone
Screensaver timeout in minutes (zero to disable)
20
Primary
Position
Referent
Rotation
Mode Set
Resolution
Output 1
None
None
Normal
Auto
Auto (1920x1080 60Hz)
Output 2
None
None
Normal
Auto
Output 3
None
None
Normal
Auto
720x400 70Hz
800x600 60Hz
1024x768 60Hz
1280x960 60Hz
1280x720 60Hz
1280x1024 60Hz
1440x900 59Hz
1600x1200 60Hz
1680x1050 59Hz
1920x1080 60Hz
Use the Ctrl+Alt+I shortcut on the device to identify outputs.
TLXOS can only make use of monitor outputs on the mainboard or a single graphics card (not both or multiple cards)
OK
Cancel


Configure Display Adapters
Video Mode
Extend desktop
Clone
Screensaver timeout in minutes (zero to disable)
20
Primary
Position
Referent
Rotation
Mode Set
Resolution
Digital Signage
Output 1
None
None
Normal
Auto
Auto (1920x1080 60Hz)
Configure
Output 2
None
None
Normal
Auto
Configure
Output 3
None
None
Normal
Auto
Configure
Use the Ctrl+Alt+I shortcut on the device to identify outputs.
TLXOS can only make use of monitor outputs on the mainboard or a single graphics card (not both or multiple cards)
OK
Cancel

In the image below a Dual Display device has been configured, the Extend desktop checkbox is selected. In this case the secondary display on Output 2 is located to the right of the Primary display on Output 1. If you have set the Mode to Digital Signage you will see an extra column "Digital Signage" displayed as explained above



The Screen Rotation defaults to Normal but may be set to either Right, Left or Inverted

The Mode set defaults to Auto but may be set to CEA (TV) or DMT (Monitor)

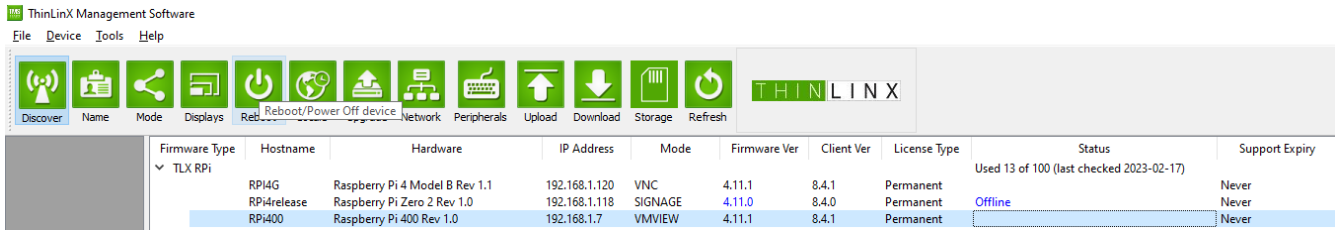
Set the Screensaver timeout in minutes to zero to disable the screensaver

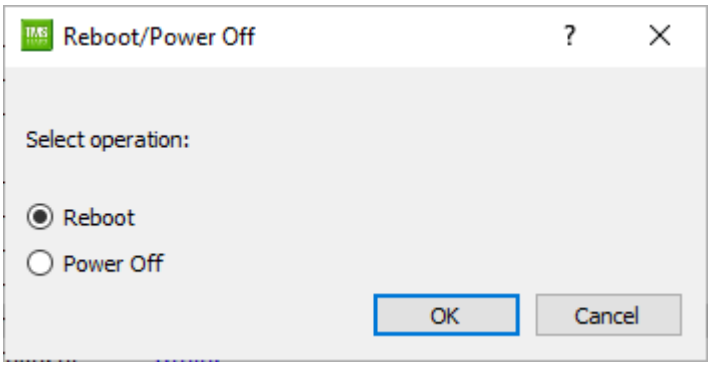
After changing the Display settings a reboot of the TLXOS device is required

14 Reboot or Power Off a TLXOS Device

To reboot or power off TLXOS devices, highlight the devices and then click on the *Reboot* Icon as per the image below, select either Reboot or Power Off

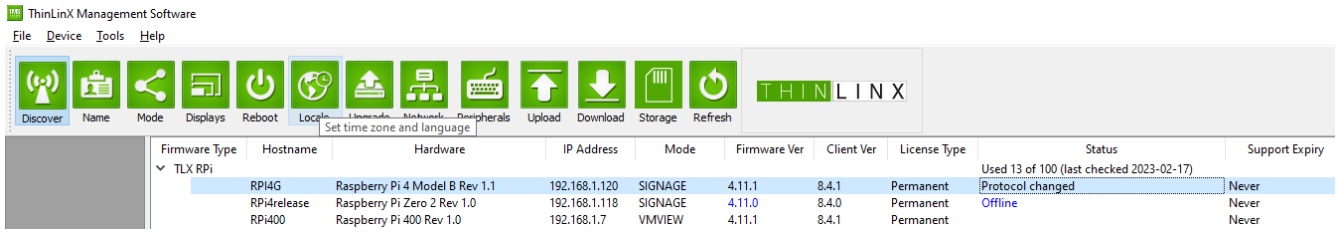
The TLXOS devices will update their status on TMS then reboot or power off. In the case of reboot, once the board reboots, it will reconnect to the TMS server as configured (either DHCP, Static or TMS broadcast).





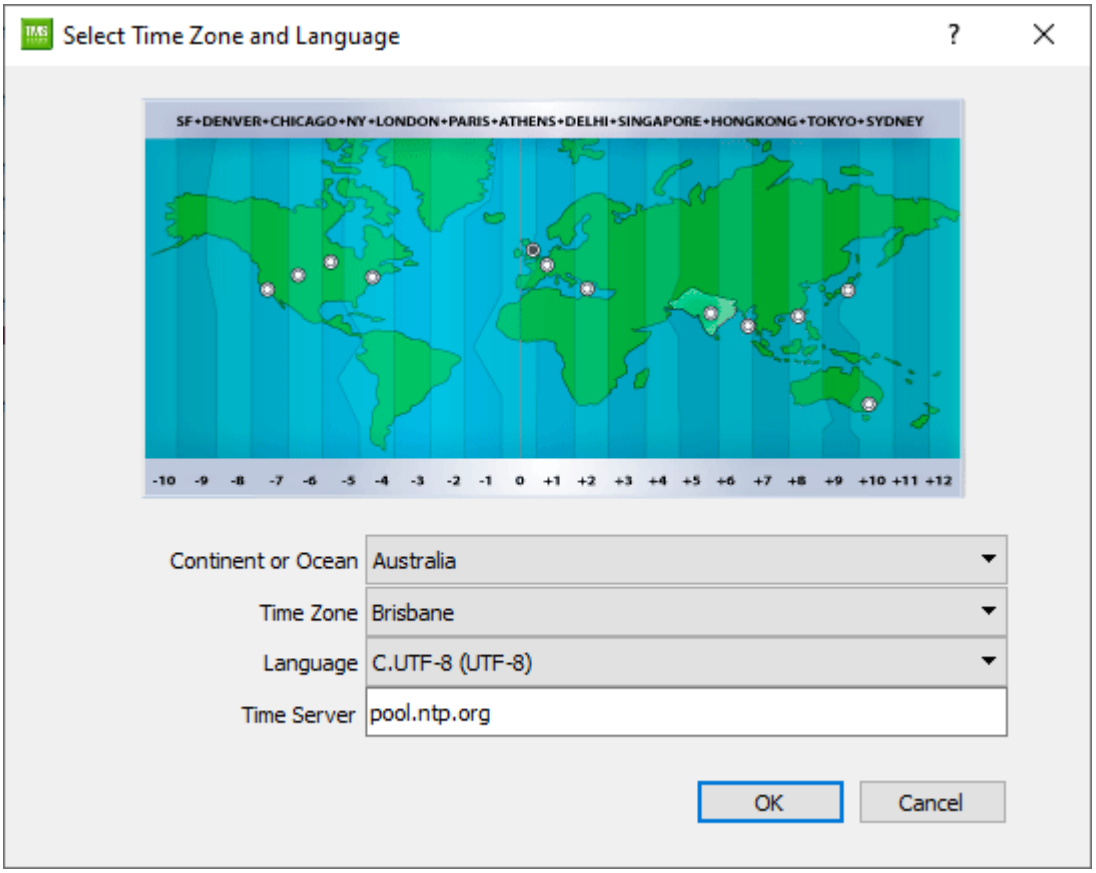
15 Setting the Time Zone and Server

When a TLXOS device is shipped, the default time zone is set to *GMT, UK*. To change the time zone and or the default Time Server, select one or more TMS Clients, then click on the Locale Icon as shown below



The following dialog box will appear allowing you select the *Continent or Ocean*, *Time zone*, *Language* as shown below. In addition to this a specific NTP *Time Server* value must also be

specified, by default TLXOS devices uses the pool.ntp.org Time Server. You may wish to set this to your local Network Time Server instead



Click the *OK* Icon to apply the time zone on the selected TLXOS devices(s).

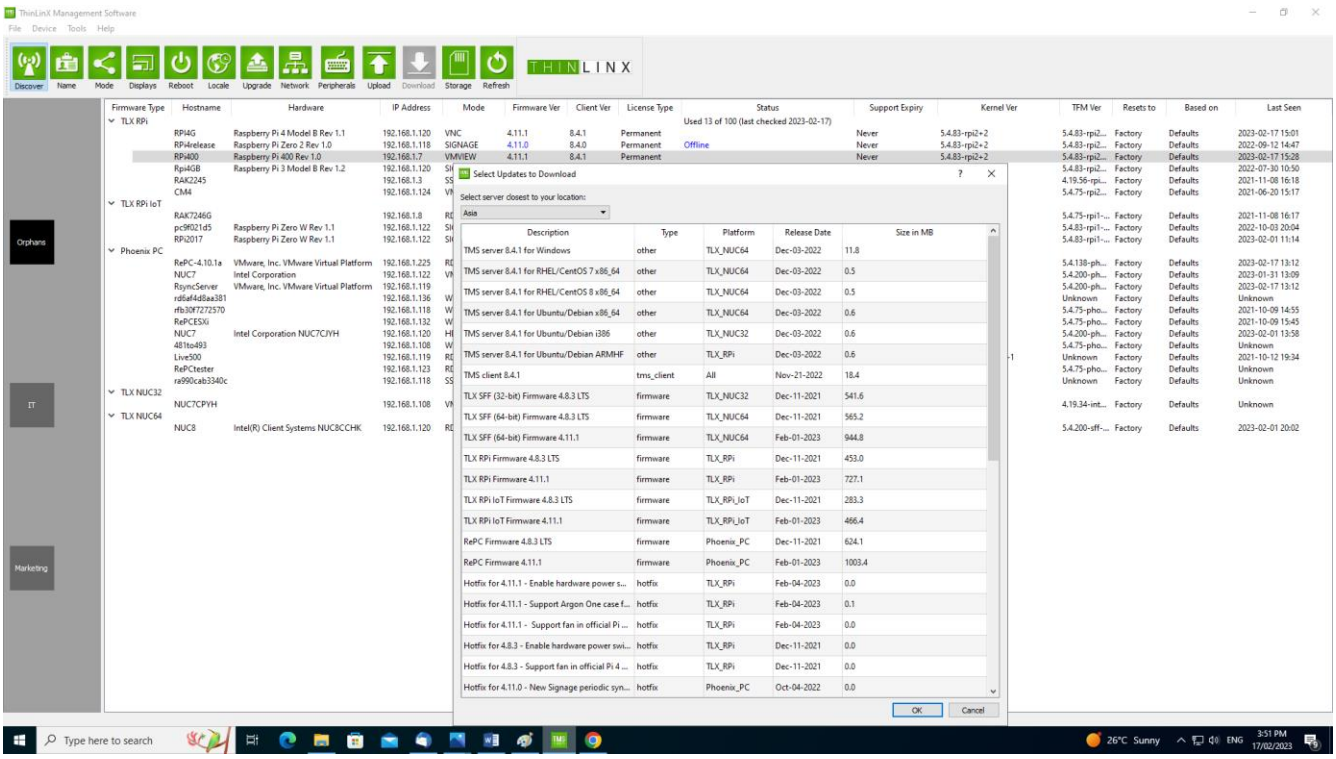
Setting a Time Server and the correct Time Zone values is recommended to avoid potential issues with SSL Certificates and other key security measures that rely on an accurate time values. This is particularly important on devices such as the Raspberry Pi which does not have an onboard battery backed Real Time Clock (RTC). The RPi obtains the time on boot up by connecting to a Time Server.

An incorrect time can also affect TMS Discovery of clients

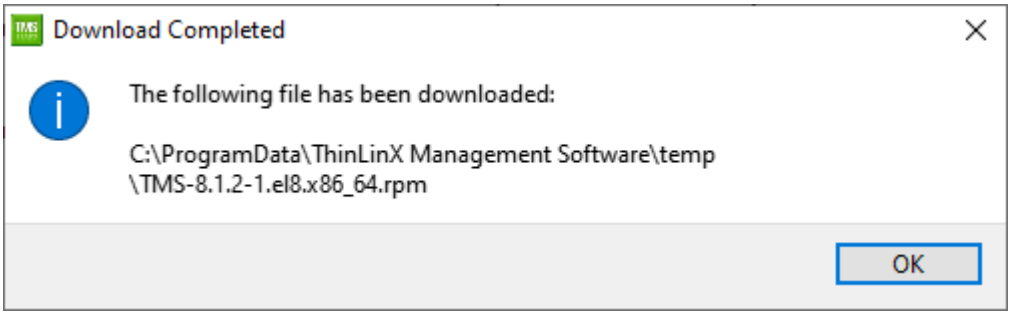
16 Downloading firmware updates for TLXOS Devices

Upgrading the firmware on a TLXOS device is very easy, simply click on the Download Icon, select a download Mirror, and click in the check box next to the Firmware, Hotfix, TMS client or TMS that you want to download then click on OK

The download will start with the download progress displayed at the bottom left of TMS, once the download completes the Firmware, Hotfix or TMS client is automatically unzipped in the TMS Firmware, Hotfix or Tmsclient directory.



If you have selected TMS Server for Windows, this will be downloaded and installed automatically replacing the current TMS for Windows. If you select the Linux versions of TMS you will need to use your distributions Linux package management tools to install the downloaded TMS for Linux which is downloaded to the TMS temp directory. We would recommend that you download the Linux version from our Website Download page



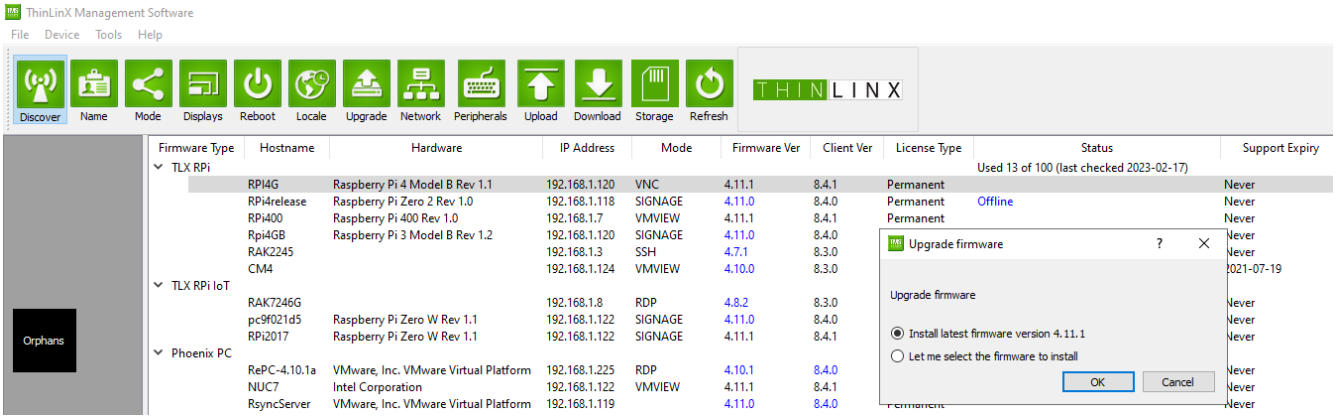
The Firmware, Hotfix or TMS client is downloaded once and can then be installed on many TLXOS devices simultaneously by highlighting each device that you want to update

In the case of a Firmware Upgrade click on the Upgrade Icon

In the case of a Hotfix select TMS -> Device -> Update -> Install Hotfix. In the case of a TMS client upgrade, select TMS -> Device -> Update -> Upgrade TMS client.

In the case of a Firmware install, a dialog box with the latest downloaded version of the firmware pre-selected will appear. Please note if the pre-selected Firmware is older than the current Firmware you will need to use the download Icon to select the latest Firmware and then download that first before clicking on the Upgrade Icon, otherwise you will be downgrading your Firmware Not Upgrading it

Click on OK to start the firmware upgrade process. In some cases depending on the firmware that has been previously downloaded you may need to select “Let me select the firmware to install” option to ensure you install the latest firmware.



When a TLXOS device receives the upgrade command it starts the upgrade process by rebooting the device into ThinLinX Maintenance Mode (TFM) mode, TMS displays, “going Offline”. Upgrade mode loads a tiny version of TLXOS which runs completely in RAM, this is necessary to allow the Boot, TFM & Root Partitions to be upgraded with the new version of TLXOS.

TMS displays periodic messages in the status column, this begins with the message “Downloading Kernel: 10%”, followed by “Downloading TFM: 10%”, followed by “Downloading RFS: 10%”. The percentage shows how much of each file has been downloaded. After the Boot, TFM and Root Filesystem have been downloaded the message “Writing Kernel” followed by “Writing TFM” followed by “Writing RootFS” appears in each device Status line. Many TLXOS devices can be upgraded simultaneously as they are all running independently of each other. Depending on the device being upgraded the upgrade can take anywhere from 5 minutes for fast storage up to 30 minutes for a slow SD Card. After the upgrade completes successfully each device reboots into Normal mode running the new version of TLXOS. When upgrading a Raspberry Pi running the NOOBS bootloader, you will notice that the RPi will initially reboot with the TFM Partition selected as the Boot partition, you will notice a 10 Second countdown, do not interrupt this process, you must allow TFM to boot to enable the upgrade to

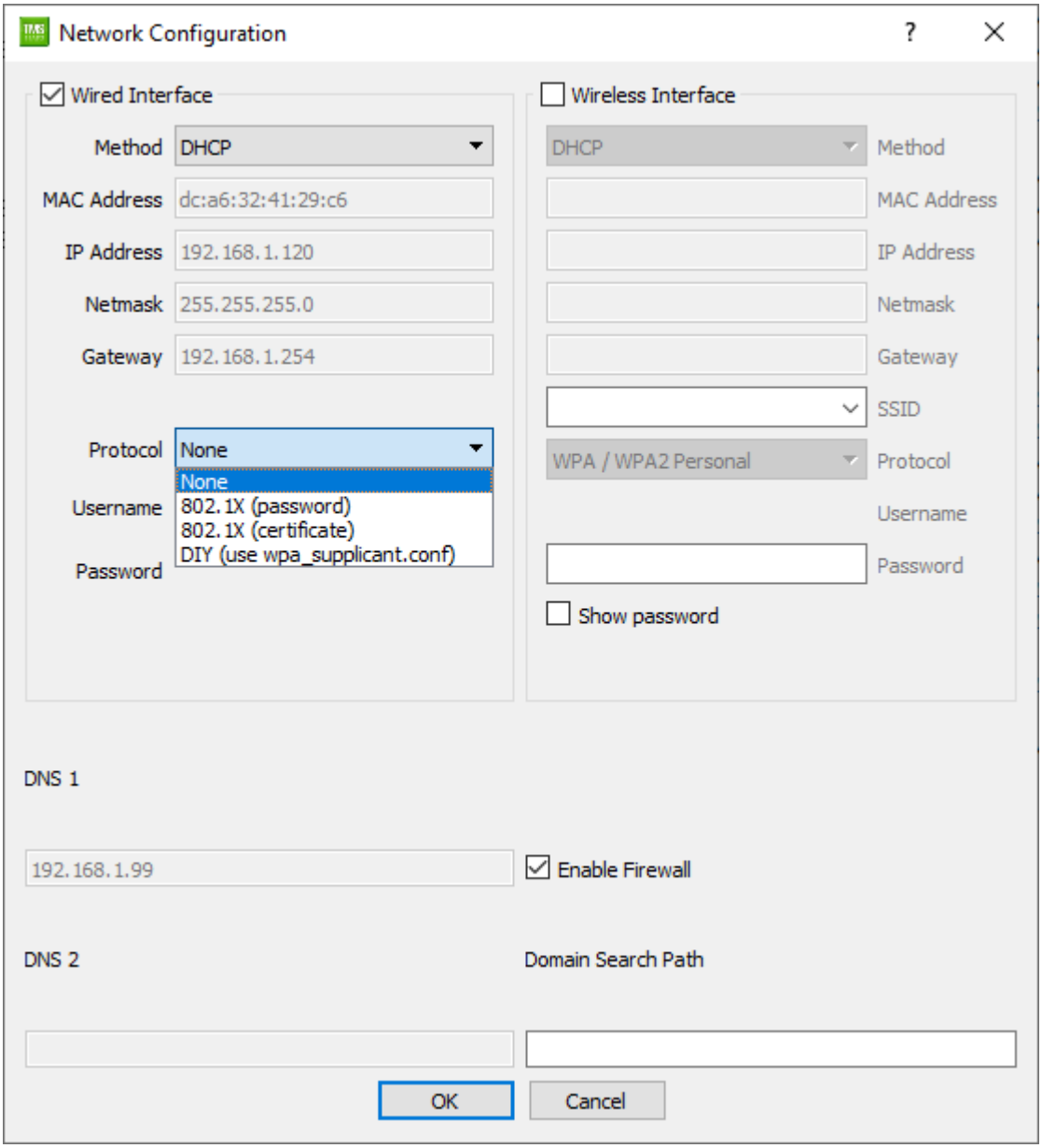
succeed.

16 Network Configuration

Click on the Network Icon to change the configuration of the Wired or Wireless interfaces. The default setting is DHCP, this can be changed to Static where all interface information must be manually entered. Another option is DHCP with DNS Override, this must be set if the DHCP Server is not providing DNS information in which case the DNS Server IP Address information may be manually entered.

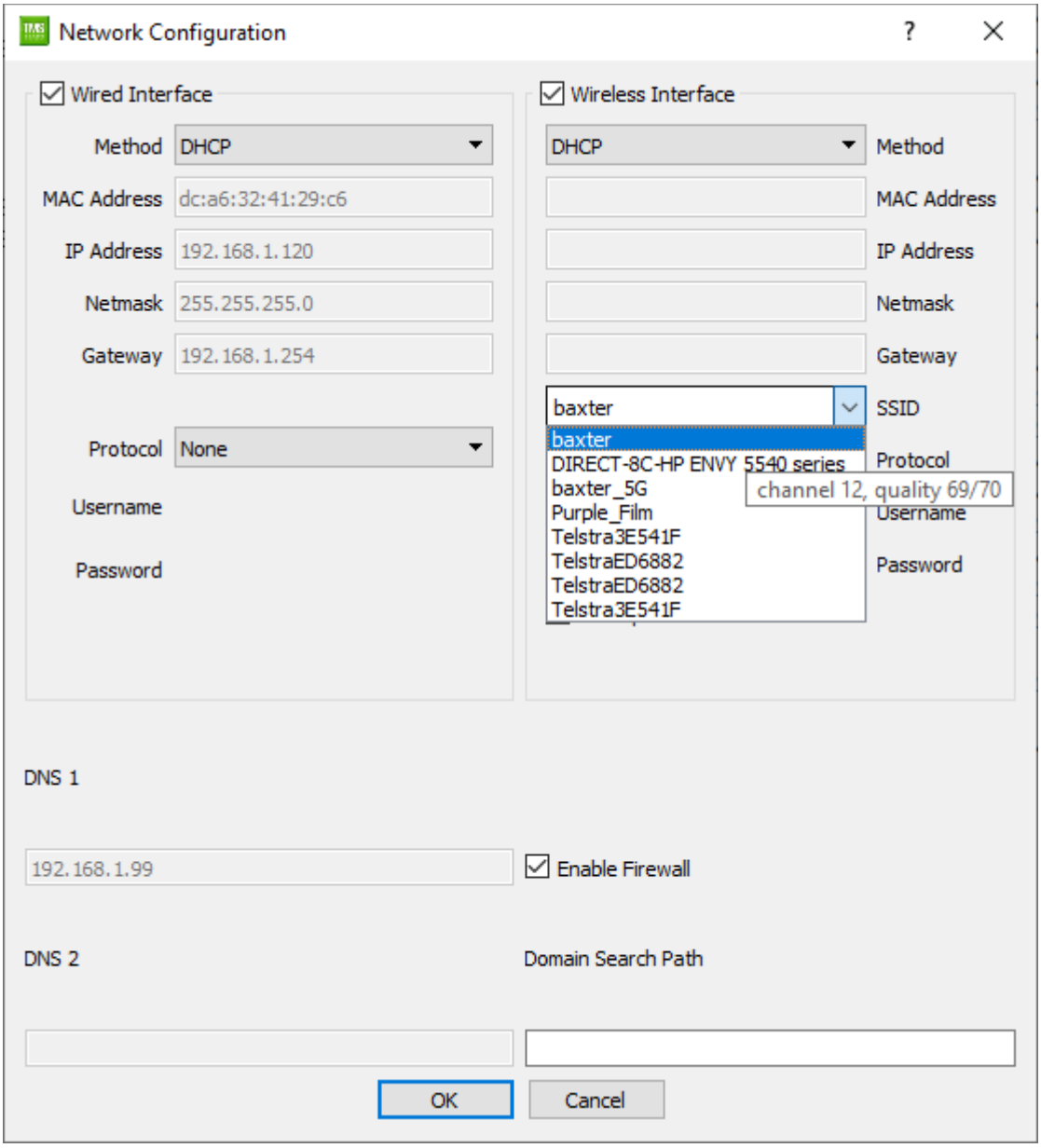
TLXOS supports different wired Protocols including 802.1X (password) where you are can enter a Username & Password, 802.1X (certificate) where you enter a Username and click on Upload PKCS#12 Certificate or DIY (use wpa_supplicant.conf) which you edit yourself

If you select DHCP the MAC Address, IP Address, Netmask and Gateway are automatically filled in and greyed out to show that they cannot be manually configured. You may need to reboot the device for this information to appear on TMS



If your device has WiFi support built in you can select the check box for Wireless interface, the default setting is DHCP, with Static or DHCP with DNS override available also. The secure encryption Protocols offered are WPA/WPA2 Personal (default), WPA2 Enterprise (password), WPA2 Enterprise (Certificate) or DIY (use wpa_supplicant.conf). We do NOT recommend the insecure choices of None or WEP.

You must select your WiFi Access Point SSID from the drop down SSID list, if you highlight a SSID by placing the mouse cursor over the name you will see the Channel number and Signal Strength. The detected list of WiFi access points are listed in order of Signal strength. Many access points transmit on dual frequencies in which case the name is duplicated if the access point has only one SSID covering both frequencies. Enter your WiFi password which must be at least 8 characters long (maximum of 63 characters)



17 Firewall Configuration

TLXOS has a firewall enabled as the default, if you wish to switch off the Firewall untick the Enable Firewall box

18 Peripherals Configuration

To configure your Keyboard, Mouse and Audio click on the Peripherals Icon, highlight the devices to be configured.

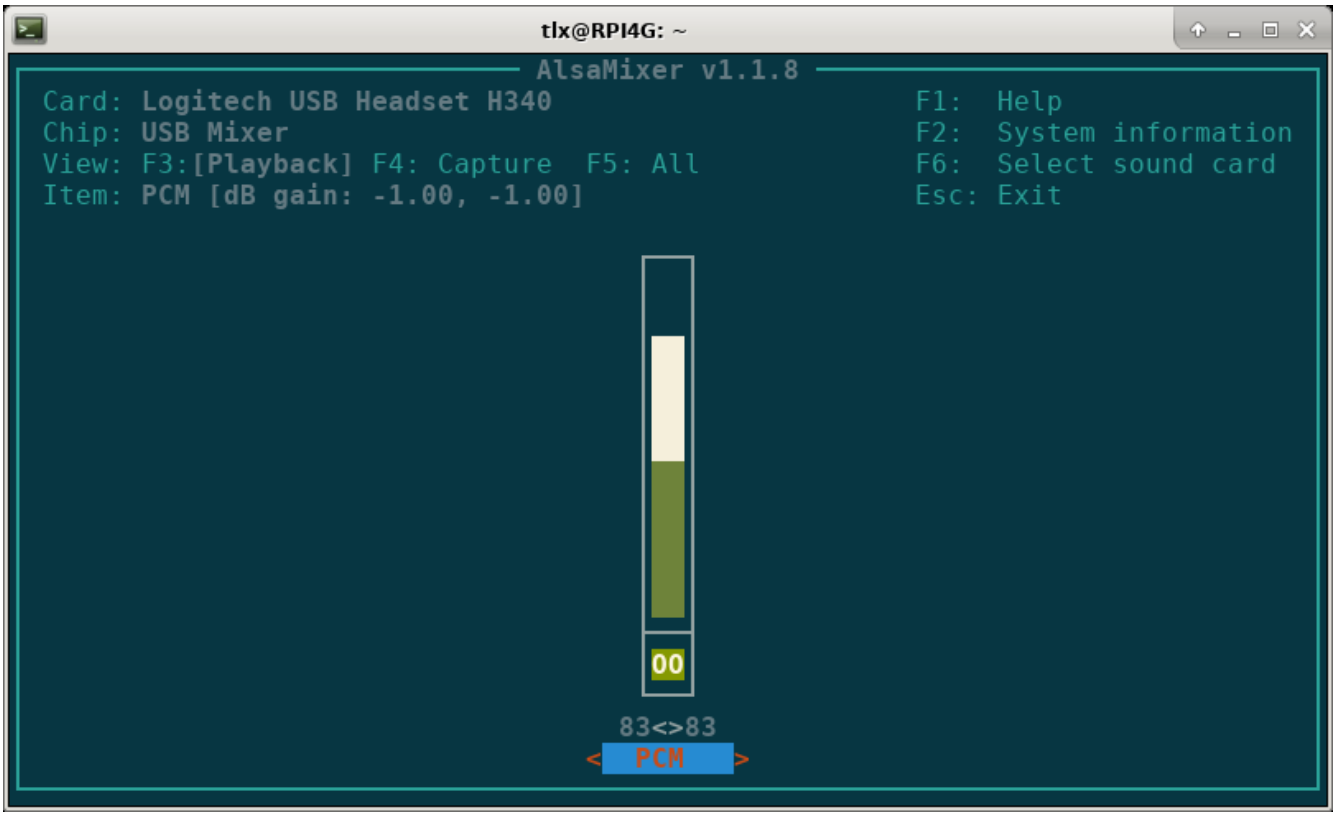
Mouse Orientation for Right handed or Left handed is selectable as is Mouse sensitivity

Numlock can be enabled (requires a reboot before taking effect)

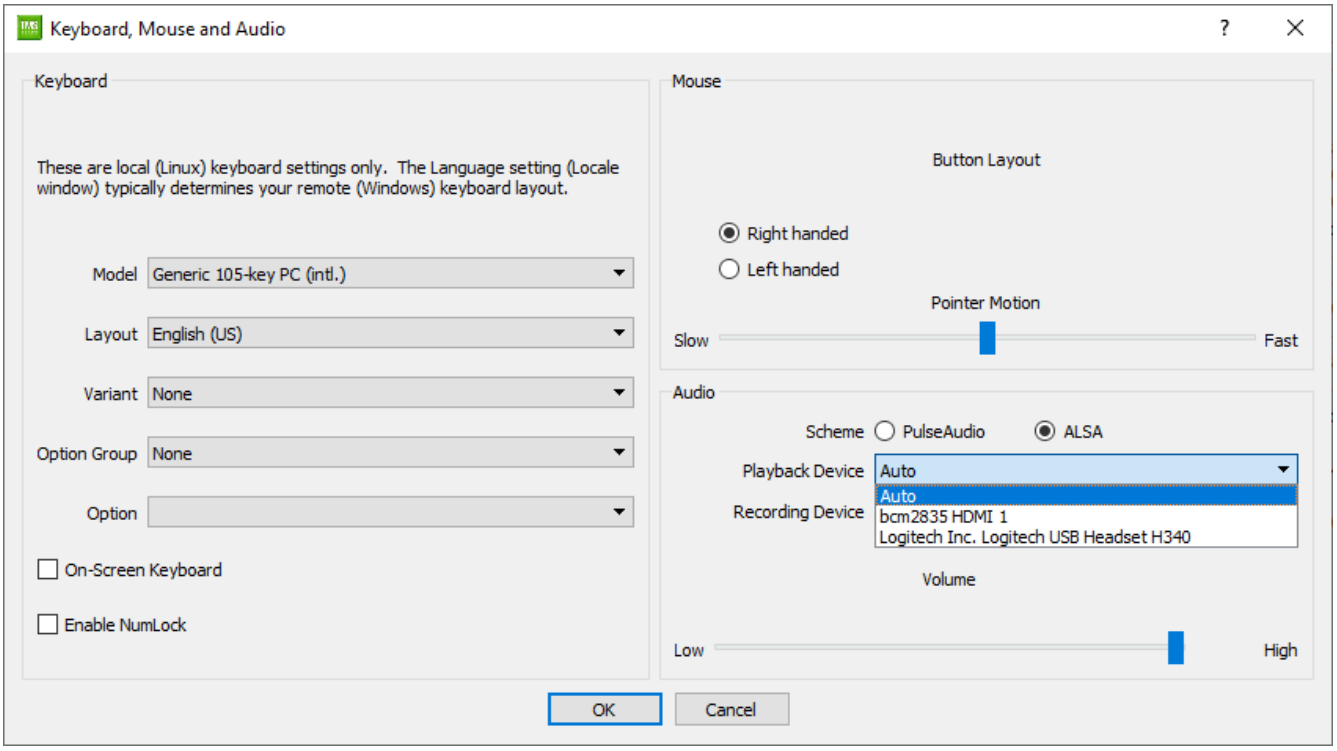
An On-Screen Keyboard can be switched on

We have added a new Audio capability to TLXOS 4.11.x and TMS 8.4.1 which is the ability to select either the PulseAudio Scheme or ALSA. We default this to ALSA on the RPi as it uses less system resources than PulseAudio which gives a better audio result than PulseAudio on the RPi

Audio Volume can be set for all TLXOS devices and Audio Output Port for Raspberry Pi devices can be set here. Default volume for a USB Headset cannot be set here, you must use the Key combination, Ctrl-Alt-t to launch an xterm then enter “alsamixer” which launches a dialog box where you can set USB Headphone and Microphone default Volume. If your USB Headset does not appear you may need to press F6 to select the USB as the default audio Card. The dialog box is launched on the local Desktop before connecting to the remote session). After setting the volumes you must reboot the RPi to save these default volumes.



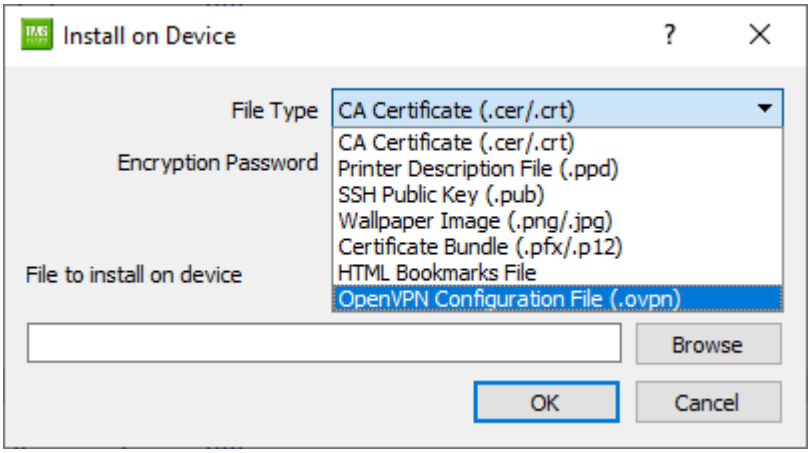
The RPi4B has two default Audio devices, one is HDMI audio if your monitor supports this and the other is the Audio out jack, neither of these support a Microphone. If you wish to use a Microphone a USB Headset is a good option



The Playback Device and Recording device default to Auto, which would select HDMI Audio first, Audio out jack second and USB Headset last. In this case you need to manually select the audio Playback and Recording devices from the dialog boxes shown above

19 Upload Files to your devices

Some file types can be uploaded to your devices by selecting the Upload Icon, these are CA Certificate, Printer PPD file, your Public SSH key, a Certificate bundle (.pfx), a Wallpaper PNG or JPEG image that is displayed after boot up as the background image, HTML Bookmarks file and an OpenVPN configuration file



(a) CA Certificate used for SSL connection with Citrix Receiver and VMware Horizon,

Use TMS to upload the client end SSL Certificate to the TLXOS devices by highlighting the devices, then click on the Upload Icon, Select CA Certificate (.cer), and browse to the Directory with the Certificate which must have a .pem extension. Certificates can be exported in either DER (binary) or PEM (ASCII) format. If you export your certificate using Windows it will be DER by default - use the "Base64-encoded" option instead; this is what Windows calls PEM. The ".cer" filename extension doesn't really mean anything and is used for both formants

(b) PPD file, you can upload a Printer PPD file to your device, then use the local configuration menu to select Web Browser mode, use the Web Browser CUPS Bookmark to configure a local Printer using your PPD file for a better printing experience than the built in drivers.

(c) SSH Key, you can upload your Public SSH key to the device to obtain root access, see FAQ on page 57

(d) Wallpaper PNG or JPEG image, upload your preferred Wallpaper using your own PNG or JPEG image.

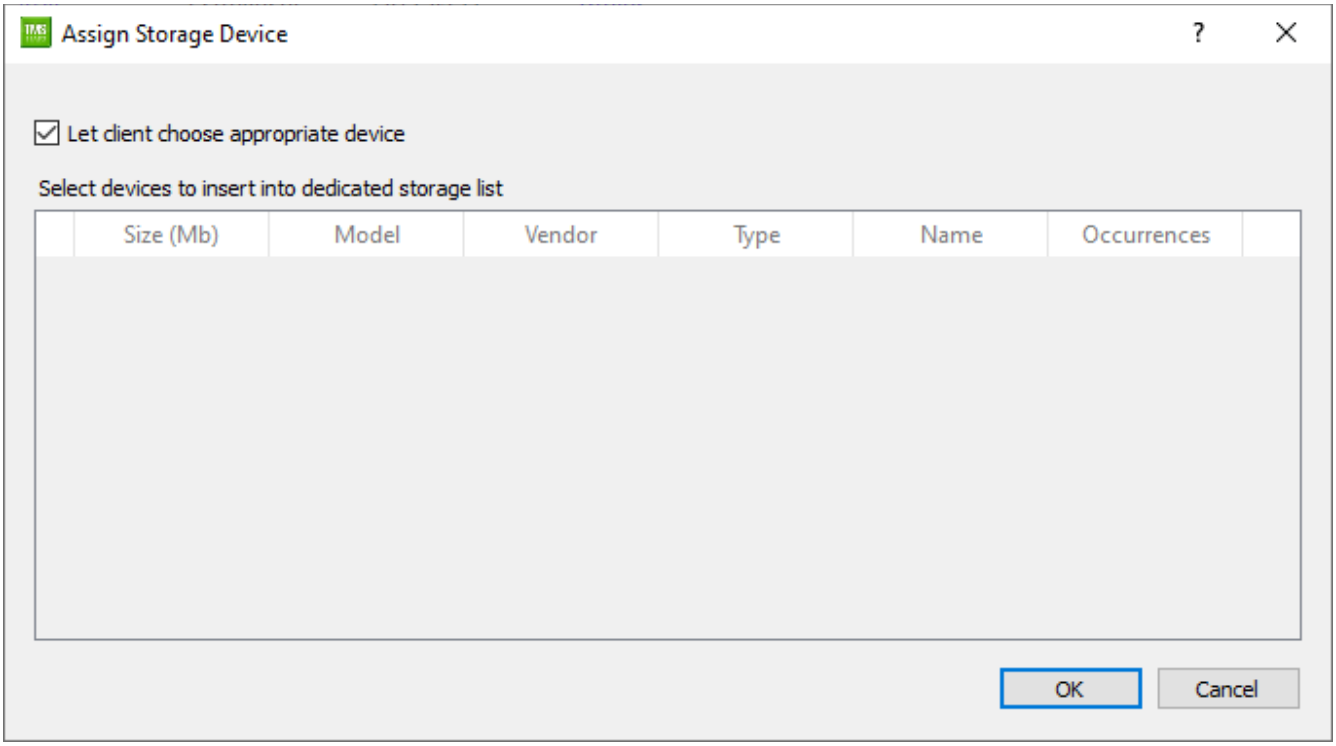
(e) Certificate bundle (.pfx) This is used for WiFi WPA2 Enterprise (Certificate) and Wired 802.1X (Certificate)

(f) HTML Bookmarks File, this will be uploaded to your local Web Browser replacing the Bookmarks file

(g) OpenVPN Configuration File (.ovpn) This uploads your custom .ovpn file which allows a TLXOS device to establish a secure encrypted tunnel between itself and an OpenVPN Server, typically at the remote Office

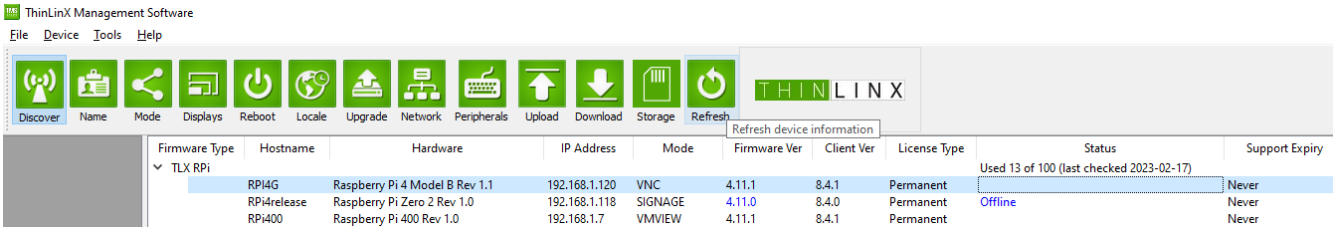
You must reboot your device to permanently save the uploaded files to the storage.

20 Storage Configuration



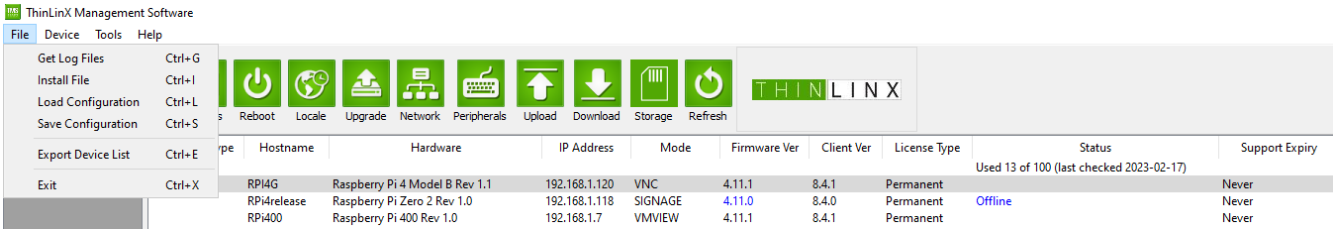
Storage Configuration is used in conjunction with a tiny SFF ISO Stub installer. This can be downloaded from the ThinLinX Website Downloads page. The CDROM ISO image is a small ThinLinX Firmware Maintenance image which runs entirely in RAM. After booting up the ISO the SFF device appears on the TMS Console, select the device, then click on the Storage Icon, this will detect the Disk drives in the SFF device, and you can either select the suggested default Disk Drive for installation or manually select the Disk Drive you wish to use for installation. This is useful if you have multiple Disk Drives and wish to preserve the contents of one of them. Next click on the Upgrade Icon and select the default latest SFF for installation or manually select a different version if you have downloaded multiple versions of the firmware. TLXOS will be installed on the selected Disk Drive, you will then be prompted to remove the CD Rom and then press any key to reboot to a running version of SFF

21 Refresh device information

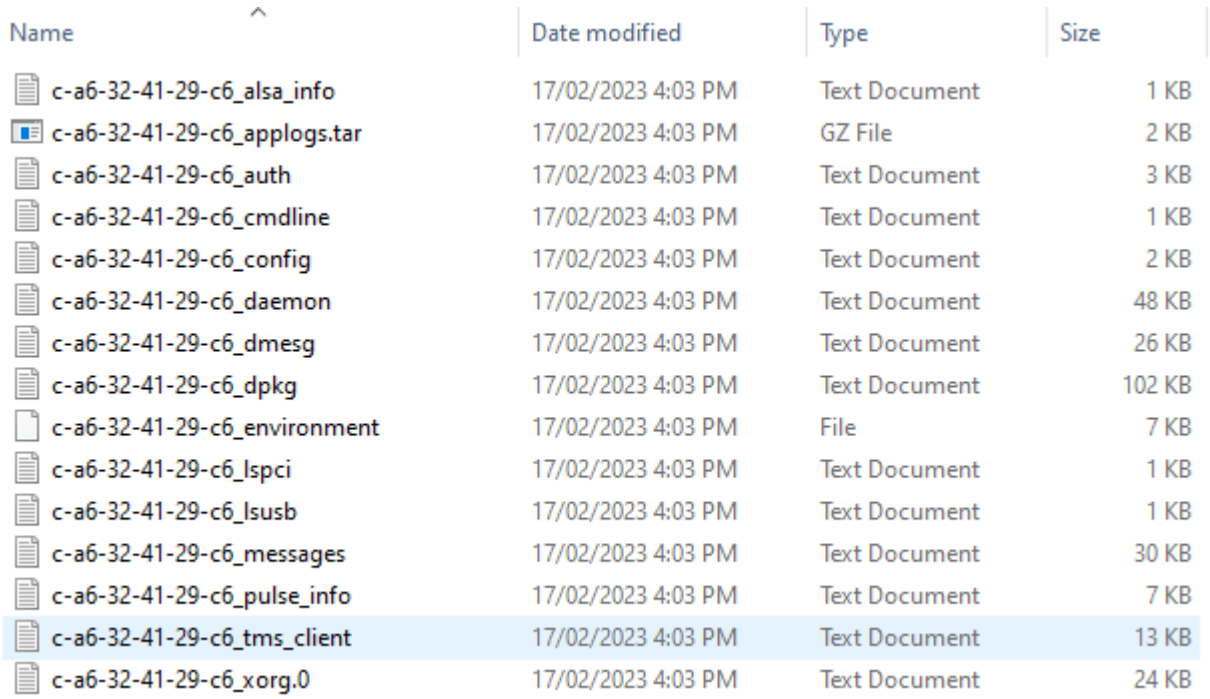


Click on the Refresh Icon to Refresh the selected devices information

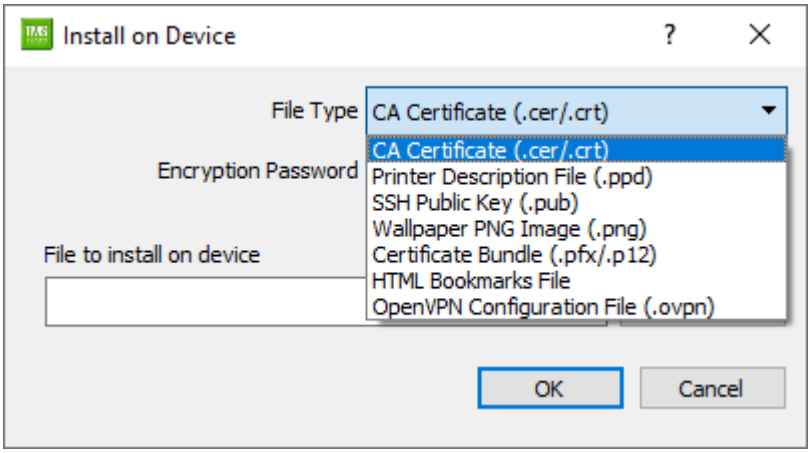
22 The File menu



Get Log files, this prompts for a directory to save the Log files in then will download the log files from the device as a zip file pre-pended with the device Mac Address, I have unzipped this file which you can see in the image below



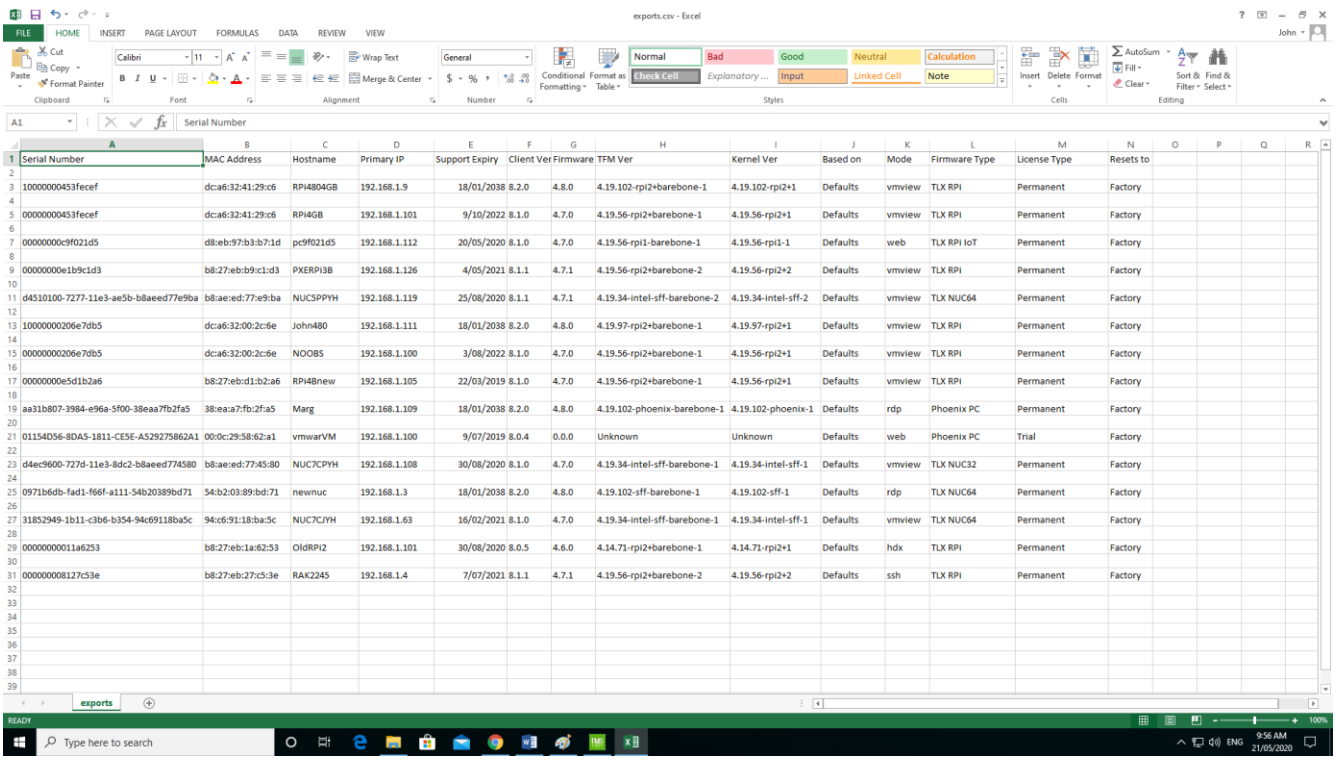
Install File – provides the same functions as the TMS Upload Icon



Load Configuration - Any previously saved Configuration can be copied to any Highlighted devices

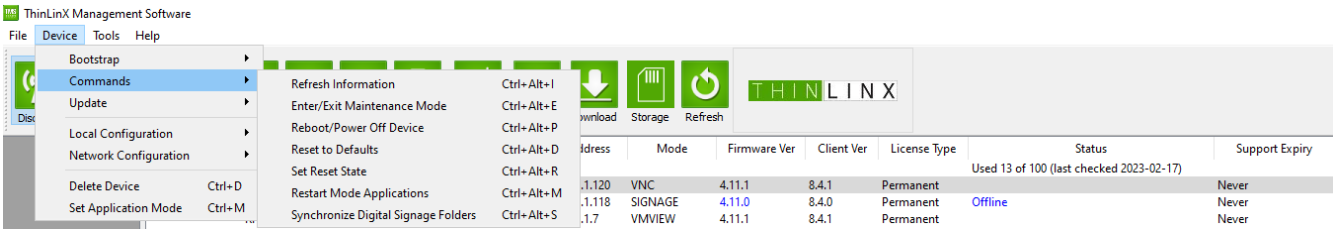
Save Configuration - allows the TMS user to save the Configuration of a highlighted device to a filename of the user's choice.

Export Device List – Exports all device information in the TMS Database as a .csv document



Serial Number	MAC Address	Hostname	Primary IP	Support Expiry	Client Ver	Firmware	TFM Ver	Kernel Ver	Based on	Mode	Firmware Type	License Type	Resets to
10000000453fecef	dc:a6:32:41:29:c6	RPI4804GB	192.168.1.9	18/01/2038	8.2.0	4.8.0	4.19.102-rpi2+barebone-1	4.19.102-rpi2+1	Defaults	vmview	TLX RPI	Permanent	Factory
00000000453fecef	dc:a6:32:41:29:c6	RPI4GB	192.168.1.101	9/10/2022	8.1.0	4.7.0	4.19.56-rpi2+barebone-1	4.19.56-rpi2+1	Defaults	vmview	TLX RPI	Permanent	Factory
00000000c9f021d5	d8:eb:97:b3:b7:1d	pc9f021d5	192.168.1.112	20/05/2020	8.1.0	4.7.0	4.19.56-rpi1-barebone-1	4.19.56-rpi1-1	Defaults	web	TLX RPI IoT	Permanent	Factory
00000000e1b9c1d3	b8:27:eb:b9:c1:d3	PXERPi3B	192.168.1.126	4/05/2021	8.1.1	4.7.1	4.19.56-rpi2+barebone-2	4.19.56-rpi2+2	Defaults	vmview	TLX RPI	Permanent	Factory
d4510100-7277-11e3-ae5b-b8aeed77e9ba	b8:ae:ed:77:e9:ba	NUC5PPYH	192.168.1.119	25/08/2020	8.1.1	4.7.1	4.19.34-intel-sff-barebone-2	4.19.34-intel-sff-2	Defaults	vmview	TLX NUC64	Permanent	Factory
10000000206e7db5	dc:a6:32:00:2c:6e	John480	192.168.1.111	18/01/2038	8.2.0	4.8.0	4.19.97-rpi2+barebone-1	4.19.97-rpi2+1	Defaults	vmview	TLX RPI	Permanent	Factory
00000000206e7db5	dc:a6:32:00:2c:6e	NOOBS	192.168.1.100	3/08/2022	8.1.0	4.7.0	4.19.56-rpi2+barebone-1	4.19.56-rpi2+1	Defaults	vmview	TLX RPI	Permanent	Factory
00000000e5d1b2a6	b8:27:eb:d1:b2:a6	RPi4Bnew	192.168.1.105	22/03/2019	8.1.0	4.7.0	4.19.56-rpi2+barebone-1	4.19.56-rpi2+1	Defaults	vmview	TLX RPI	Permanent	Factory
aa31b807-3984-e96a-5f00-38eaa7fb2fa5	38:ea:a7:fb:2f:a5	Marg	192.168.1.109	18/01/2038	8.2.0	4.8.0	4.19.102-phoenix-barebone-1	4.19.102-phoenix-1	Defaults	rdp	Phoenix PC	Permanent	Factory
01154D56-8DA5-1811-CE5E-A529275862A1	00:0c:29:58:62:a1	vmwarVM	192.168.1.100	9/07/2019	8.0.4	0.0.0	Unknown	Unknown	Defaults	web	Phoenix PC	Trial	Factory
d4ec9600-727d-11e3-8dc2-b8aeed774580	b8:ae:ed:77:45:80	NUC7CPYH	192.168.1.108	30/08/2020	8.1.0	4.7.0	4.19.34-intel-sff-barebone-1	4.19.34-intel-sff-1	Defaults	vmview	TLX NUC32	Permanent	Factory
0971b6db-fad1-f66f-a111-54b20389bd71	54:b2:03:89:bd:71	newnuc	192.168.1.3	18/01/2038	8.2.0	4.8.0	4.19.102-sff-barebone-1	4.19.102-sff-1	Defaults	rdp	TLX NUC64	Permanent	Factory
31852949-1b11-c3b6-b354-94c69118ba5c	94:c6:91:18:ba:5c	NUC7CJYH	192.168.1.63	16/02/2021	8.1.0	4.7.0	4.19.34-intel-sff-barebone-1	4.19.34-intel-sff-1	Defaults	vmview	TLX NUC64	Permanent	Factory
00000000011a6253	b8:27:eb:1a:62:53	OldRPI2	192.168.1.101	30/08/2020	8.0.5	4.6.0	4.14.71-rpi2+barebone-1	4.14.71-rpi2+1	Defaults	hdx	TLX RPI	Permanent	Factory
000000008127c53e	b8:27:eb:27:c5:3e	RAK2245	192.168.1.4	7/07/2021	8.1.1	4.7.1	4.19.56-rpi2+barebone-2	4.19.56-rpi2+2	Defaults	ssh	TLX RPI	Permanent	Factory

23 The Device menu

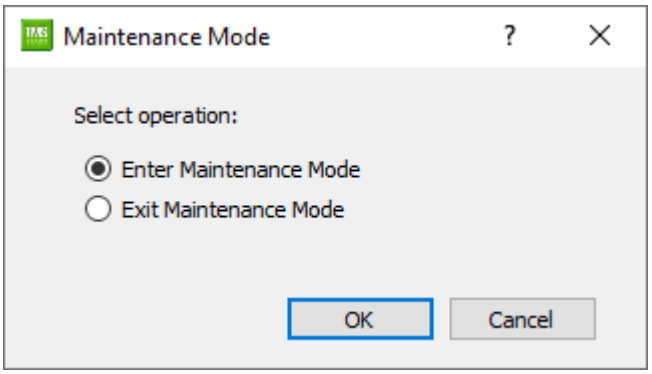


Bootstrap – This provides the same function as the TMS Storage Icon

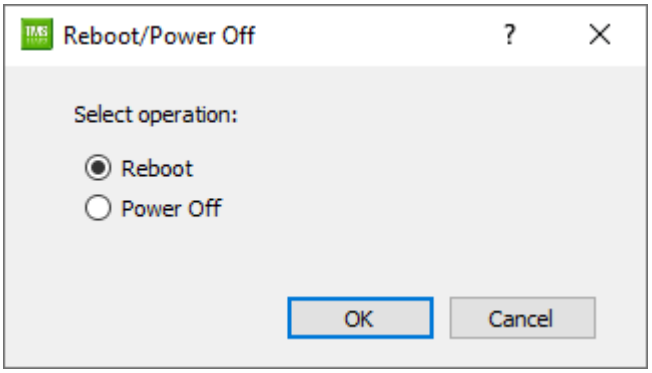
Commands

Refresh Information - Refreshes the TMS Database with latest information stored on each highlighted TLXOS device

Enter/Exit Maintenance Mode – All highlighted devices will reboot into ThinLinX Firmware Maintenance mode or Exit Maintenance Mode after selecting from the dialog box below and pressing OK

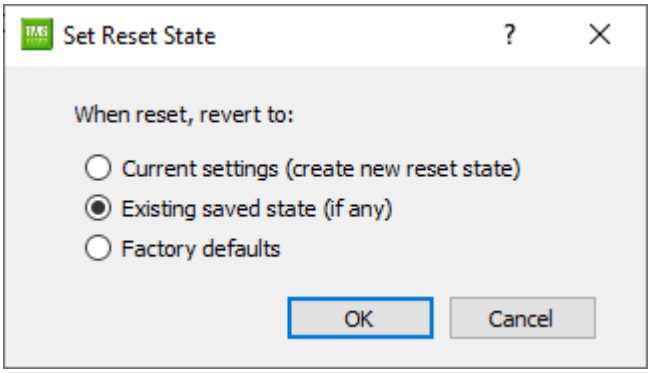


Reboot/Power Off device - All highlighted devices will either reboot or power off depending on the selection below



Reset to Defaults, this command resets all highlighted devices to the Reset state as configured in the "Set Reset State" dialog shown below. If nothing has been previously set, the devices will be reset to Factory Defaults

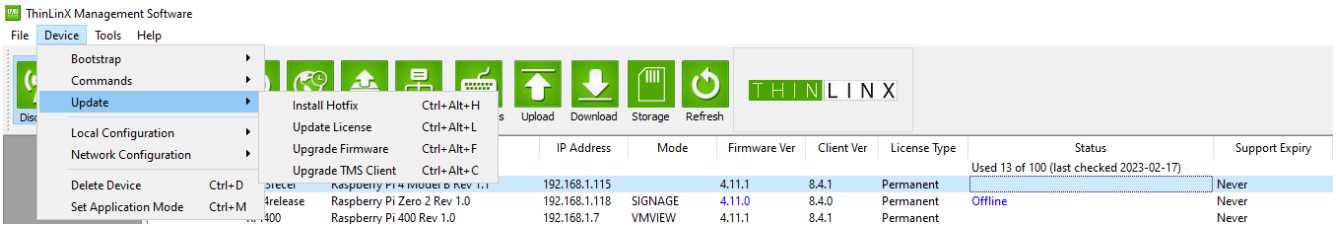
Set Reset State, allows you to set a Reset State which is loaded when you action the Reset to Defaults command, the Reset State can be one of the three choices in the image below



Restart Mode Applications

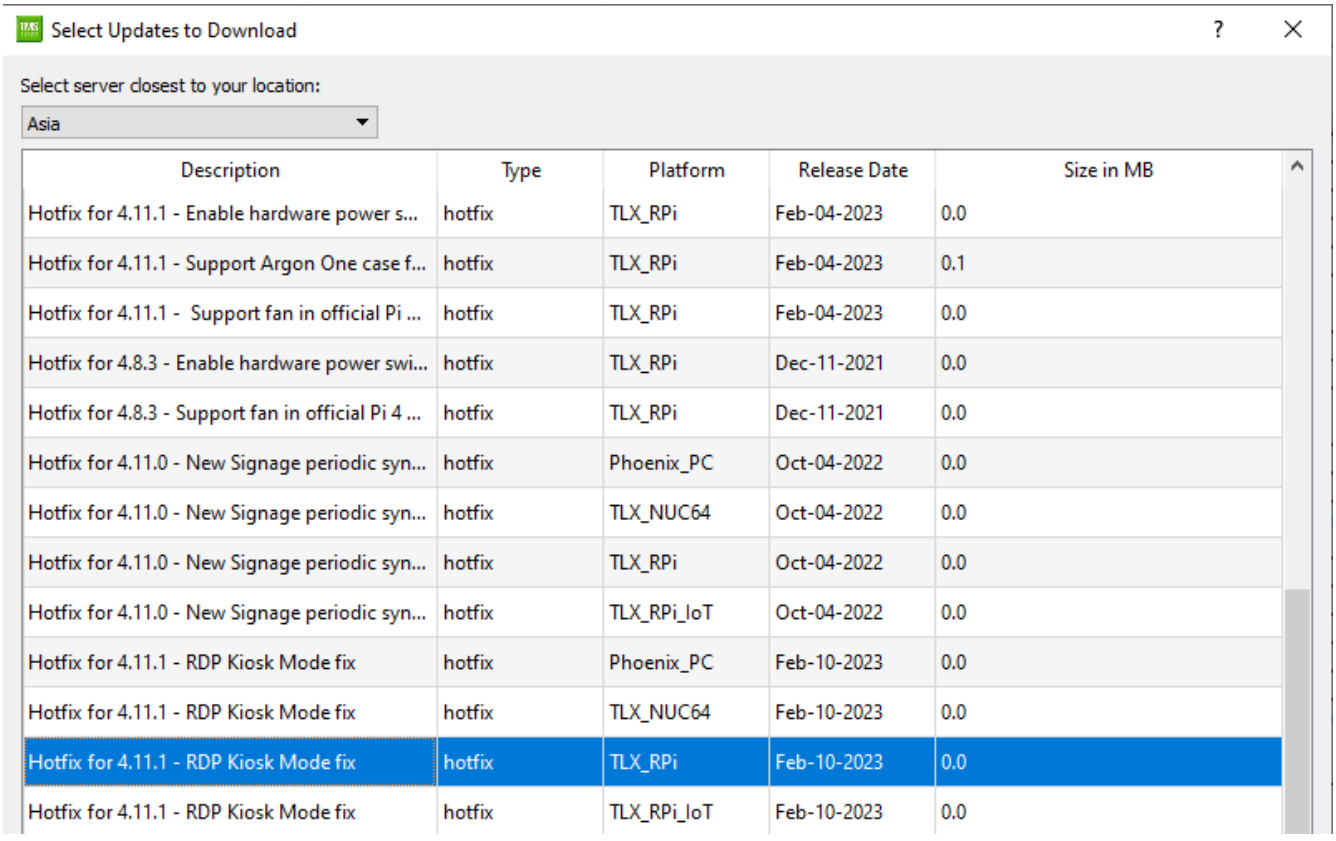
This will restart the mode that you have configured using the Mode Button

Synchronize Digital Signage Folders – All Digital Signage information has been moved to a separate user guide which you can download here https://thinlinx.com/dsi-quick-start-guide.pdf



Update

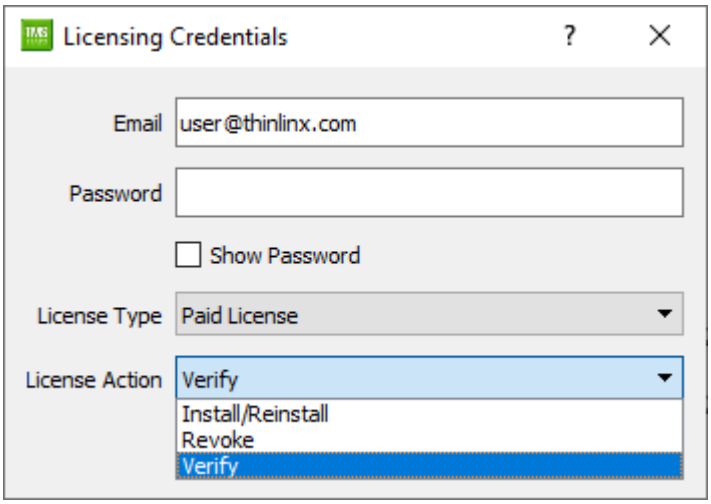
Install Hotfix - from time to time between new TLXOS Firmware releases a Hotfix may be released to correct a bug, update Citrix Receiver etc. To install a Hotfix, first click on the Download Icon, select the Hotfix from the Dialog box list, click OK to download the Hotfix to TMS. Select any devices that you wish to install the Hotfix to (by clicking on the lines with the devices to select them) then click on Device -> Update -> Install Hotfix to launch the selection dialog box shown below, click on the Hotfixes to install, then OK to copy the Hotfix to selected TLXOS devices. You will be prompted to reboot the devices to finalize the installation and permanently save the Hotfix to the devices storage. Please note that each Hotfix has a TLXOS version number as part of their names, you can only install Hotfixes for the same version of TLXOS as the device is running



Update License – The License Type in the Dialog box shown below defaults to “Paid License”, this can be changed to Free Trial if the automatic Free Trial failed to install during TLXOS installation for some reason. The Update License selection is used to either Install or Reinstall a Paid License, Revoke a License or Verify an existing License. All ThinLinX TLXOS Licenses are now perpetual and never need to be paid for again.

To carry out any of the License actions below just enter the email address and password that you registered at the ThinLinX Online Store into the Email and Password dialog boxes. You must have purchased at least one TLXOS License for the device type that you wish to License, either RPi 2,3,4,400, (RPi 1 or Zero IoT version), Re-Purpose PC / Laptop and Small Factor Devices.

To update a Free Trial to a Paid License select **Install/Reinstall**. The encrypted License is automatically created by the License Server and downloaded to the TLXOS device where it is stored. The License is deliberately erased during Firmware upgrades, but is automatically reinstalled after the upgrade on first boot up. In the very unlikely event that you have a SD Card Failure or you decide to use a faster SD Card you can just reinstall TLXOS on the new SD Card, which will automatically contact the License Server to check if the hardware is licensed. The License Server already has your hardware details in its database, it will send the previous License Key for your hardware to the new SD Card, and you do NOT need to buy a new License.



If you select **Verify** this will update the number of Licenses that you have used of each type as shown on TMS

Do not **Revoke** a License unless you never want to run TLXOS on that device again. Revoking a License allows you to reuse that License on another device. This is very useful in the case of a hardware failure where you want to reuse the License on a new device or in the case a device has been stolen or lost or if you upgrade from a RPi3 to a RPi4 and don’t want to run TLXOS ever again on the RPi3. The same applies to any TLXOS device, including RePC or ISFF

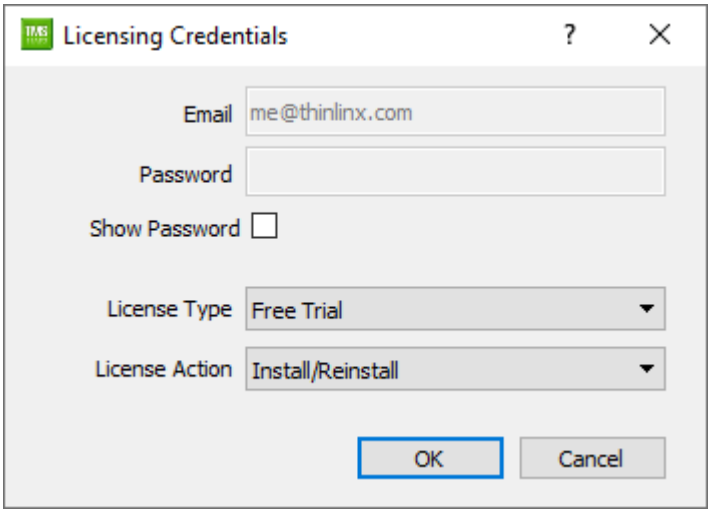
To be able to revoke a License it must be visible on TMS, which means that it must have been

detected at some point by TMS and displayed on the TMS console. You can only revoke a License on a device shown as offline on TMS

The TLXOS installer attempts to automatically License a 30 Day Free Trial on the installation device by connecting to the ThinLinX License Server at https://tls.thinlinx.com during the installation.

If the installer is unable to automatically License the device with the ThinLinX License Server at https://tls.thinlinx.com the device will open a Dialog Box with a four minute Countdown to give you time to use either the local configuration menu or TMS to install either a Free or Paid License. After 4 minutes a dialog box will appear advising a License has been acquired or if this was unsuccessful it will boot into ThinLinX Firmware Maintenance (TFM) mode. You can License a device that is in TFM mode by selecting it on TMS and then following the Install/Reinstall procedure above.

The failure to License can be caused either the wrong date on the device or a proxy server blocking the connection. If a Proxy Server is blocking the connection you need to use TMS -> Tools -> Options to launch the TMS Preferences dialog, enter your Proxy server information, click on Save, close TMS, then Open TMS to restart it. If your device boots into TFM mode due to the 30 Day Free Trial failing to License you can still use TMS -> Device -> Install License, select Free Trial to License the 30 Day Free trial. You cannot enter any information, just click on OK. To exit the TFM mode, either press Enter on the Local Desktop or use TMS -> Device -> Commands -> Enter/Exit Maintenance Mode

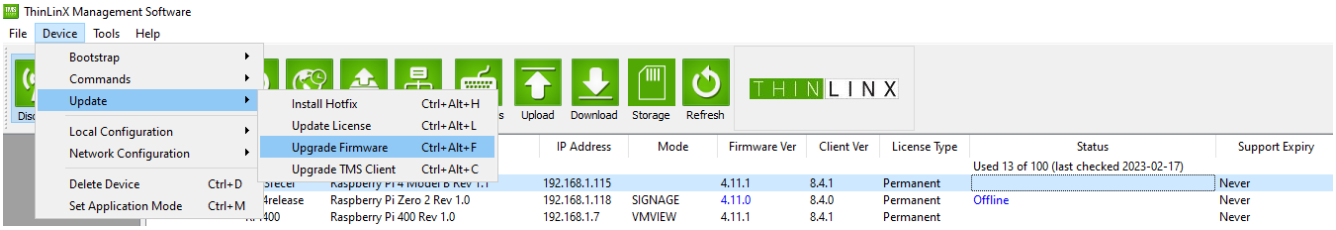


If the Free Trial failed because you are behind a Proxy Server please either follow the procedure above or edit the proxy.txt file on the USB stick installer or RPi SD Card installer to add your proxy server details before attempting installation

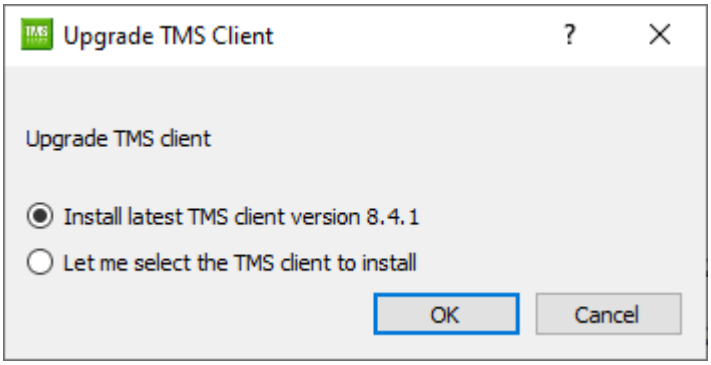
To obtain a Permanent License for a Product you must purchase a License from the ThinLinX online Store https://tls.thinlinx.com/store/index.php/

The Store accepts Paypal or Credit Cards through Paypal, contact ThinLinX at sales@thinlinx.com for other payment options.

Upgrade Firmware – This provides the same functionality as clicking on the TMS Upgrade Icon. You should check that you have downloaded the latest firmware for your TLXOS device before carrying out a Firmware Upgrade. To do this click on the TMS Download Icon and select the firmware for your device. The firmware is downloaded, unzipped and then can be deployed to any highlighted TLXOS device of the same class.

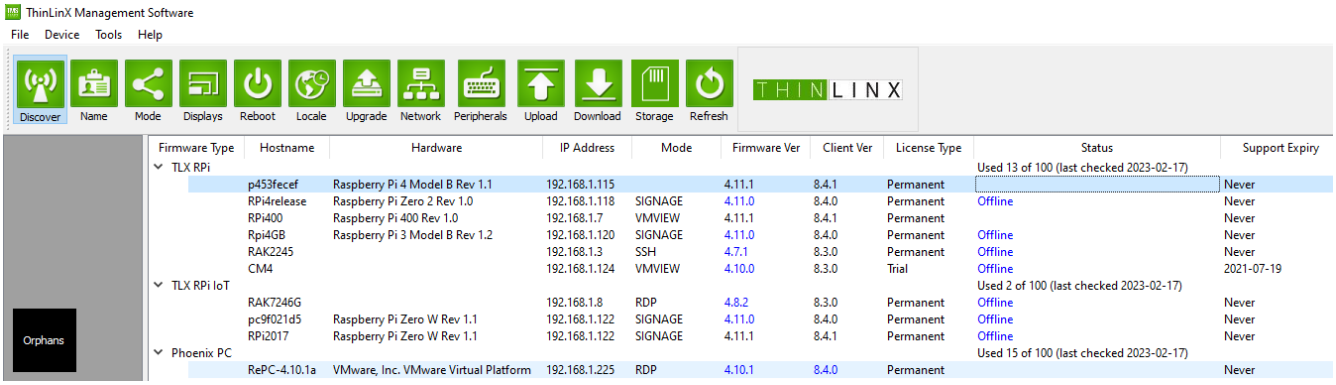


Upgrade TMS client - every TLXOS firmware release includes the latest TMS client which communicates information from the TLXOS device to the PC running TMS. In some circumstances a new version of the TMS client is made available between Firmware releases, this can be downloaded using the Download Icon and then copied to highlighted TLXOS devices by using this option. Whenever a newer version is available the Client Version number it is shown in Blue on the TMS console, see more information below

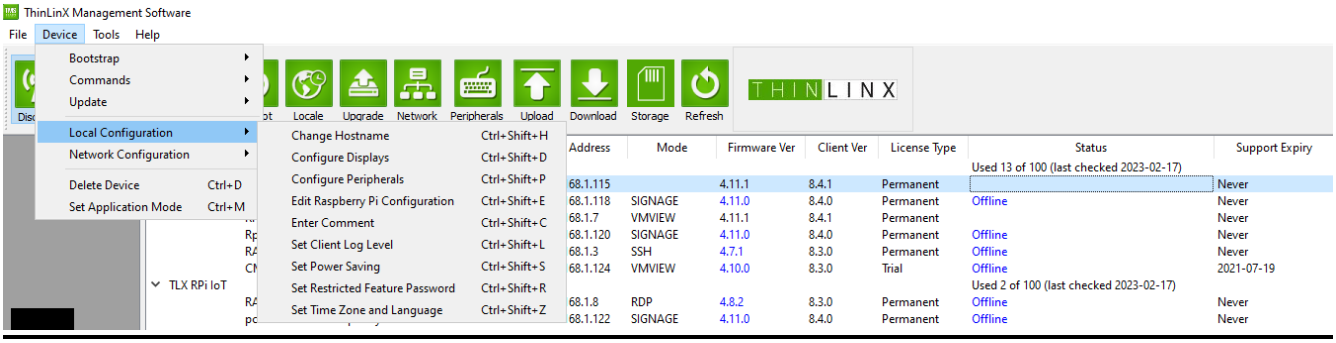


Whenever a newer version of either TLXOS Firmware or the integrated TMS client is available it is shown on the TMS console in Blue. In the example below you can see that there is a newer

version of TLXOS available for the Firmware Version shown in Blue as these are both older than the latest version. The same applies to the Client Version. TMS will default to check for Firmware and TMS client updates on startup. You can change this to check to either “Manually or Daily” which are selected on the TMS Preferences dialog reached by selecting TMS -> Tools -> Options



Local Configuration



Change Hostname – This option provides the same function as clicking on the “Name” Icon

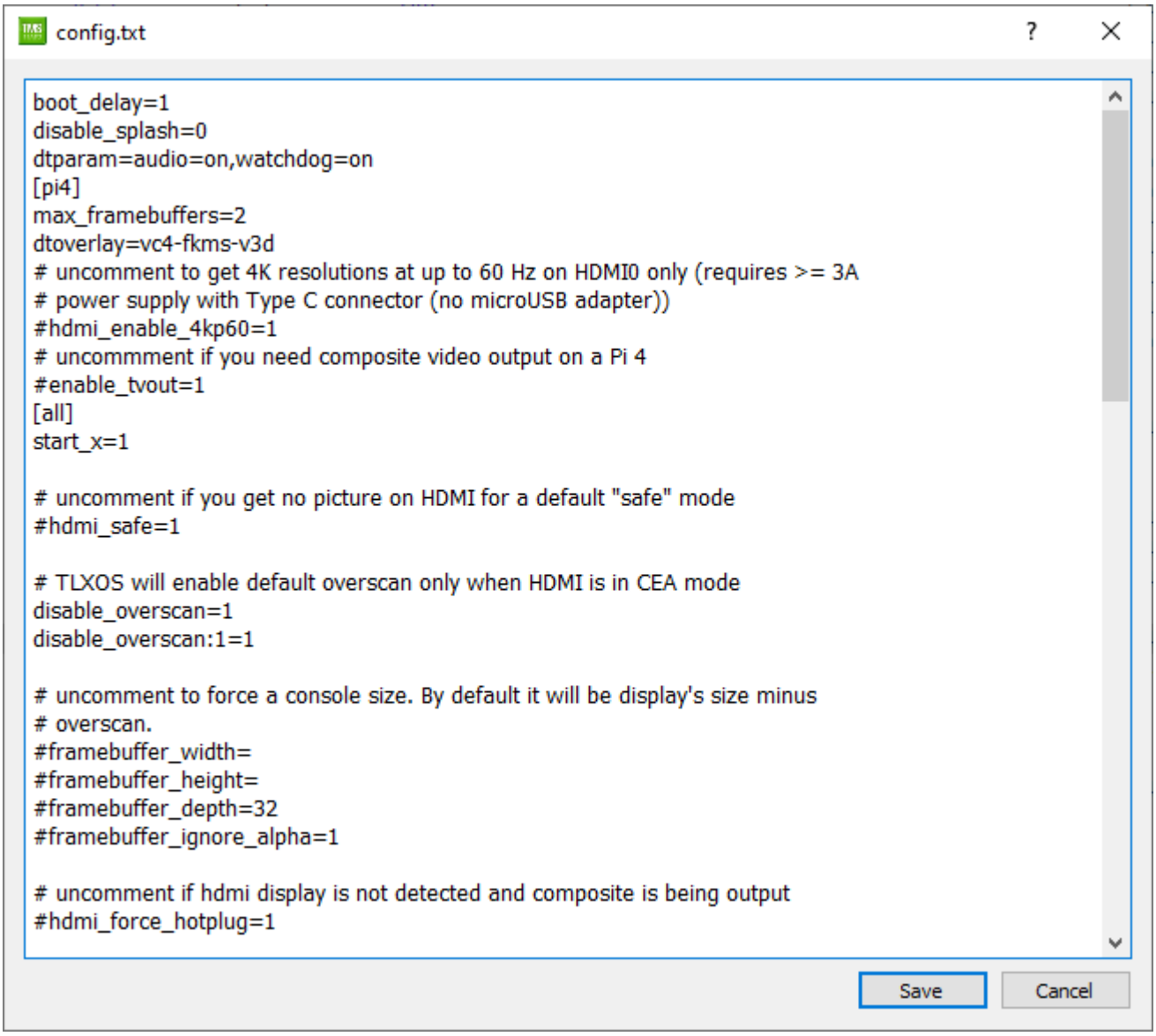
Configure Displays – This option provides the same function as clicking on the “Displays” Icon

Configure Peripherals – This option provides the same function as clicking on the Peripherals Icon

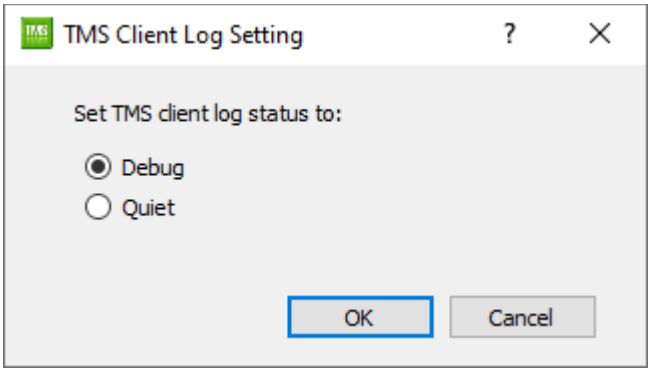
Edit Raspberry Pi Configuration – This launches an Editor that allows you to edit and save the RPi config.txt. You need to be careful when editing config.txt as a mistake could result in the RPi no longer booting. If this happens unplug the RPi Power remove the SD Card and try

editing it in a card reader. A last resort would be to reimage the SD Card

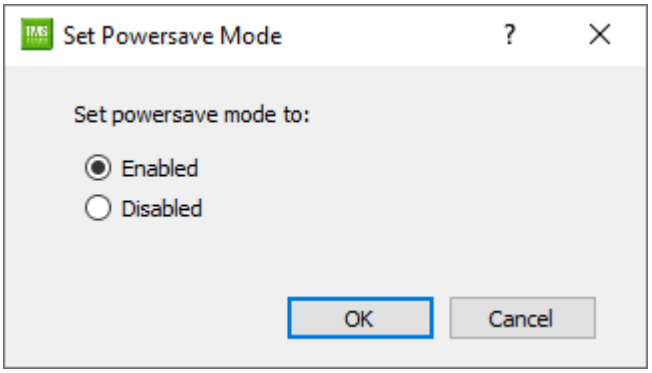
Please ensure you reboot after making any config.txt changes



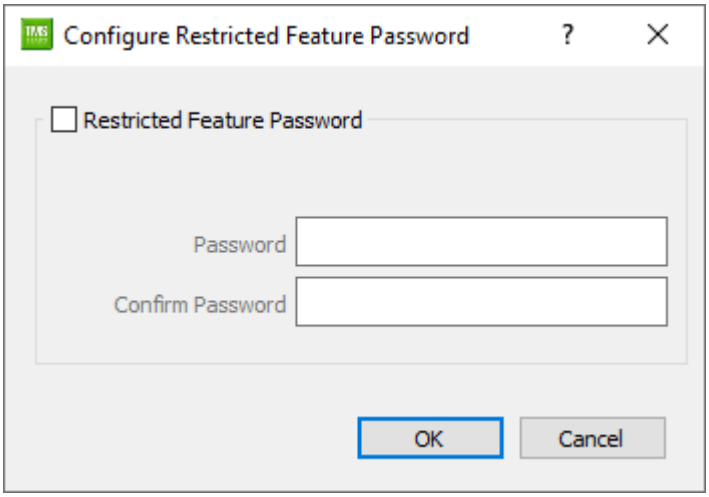
Set Client Log Level – Set client Log level to Debug or Quiet



Set Power Saving – Set Powersave mode to Enabled or Disabled

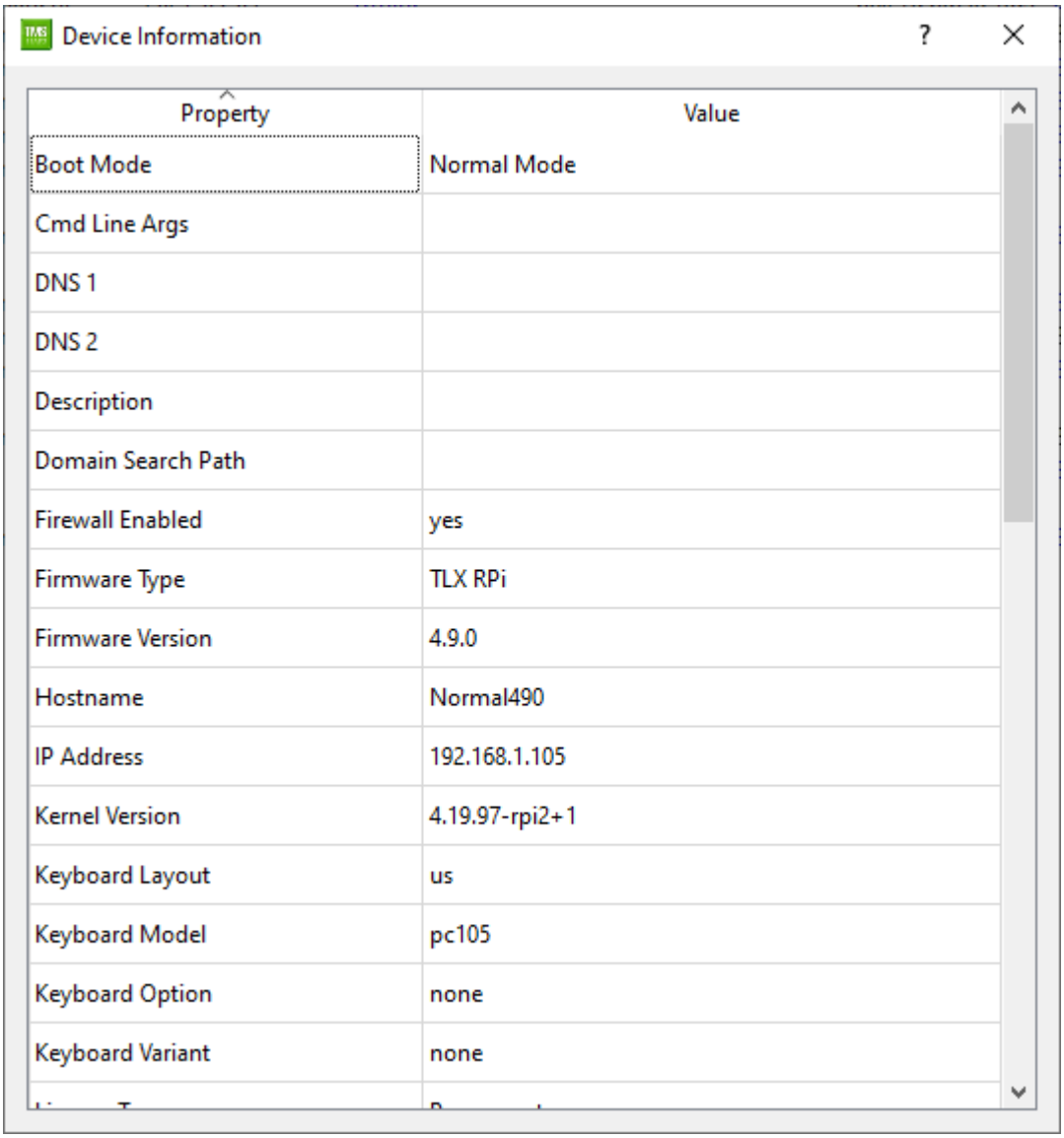


Set Restricted Feature Password – Set Restrictive Feature Password is very useful to lock end users out of the Tlxconfig local configuration menu. Highlight the devices that you want to be password locked and enter the details below

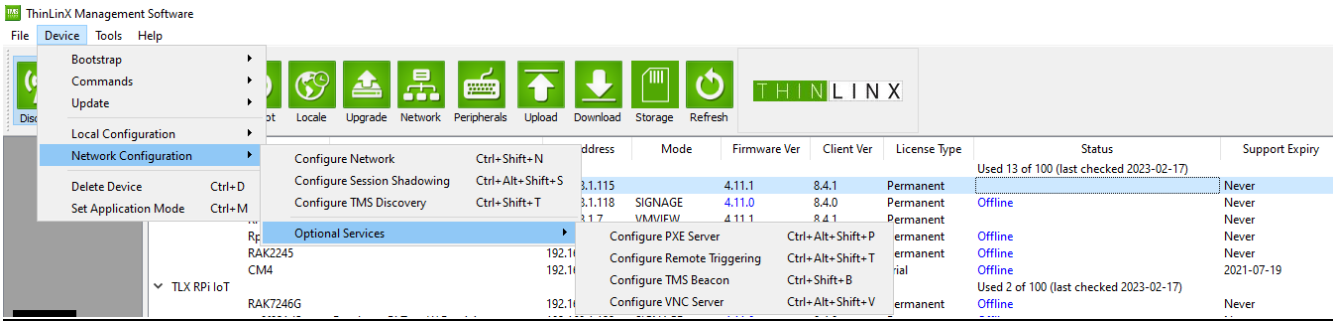


Set TimeZone and Language – This option provides the same features as the “Locale” Icon

You can highlight a device and press Enter to display all the Device information that TMS has stored in its database

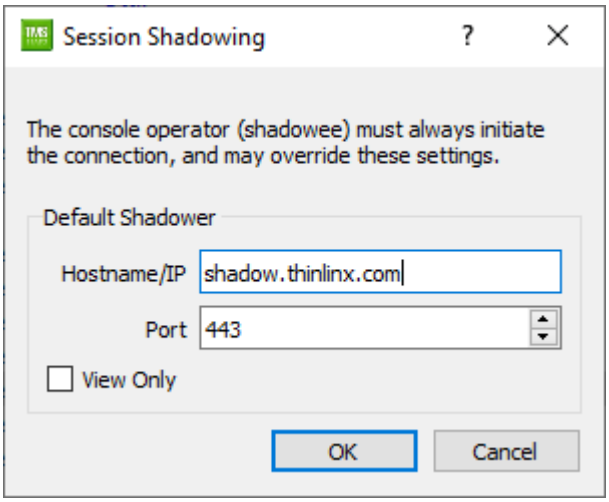


Network Configuration



Configure Network – This option provides the same features as the Network Icon

Configure Session Shadowing – If you need higher security than our basic VNC Server mode and want to traverse NAT boundaries you will need to use TLXOS session shadowing which can be accessed via the <ctrl><alt>s keyboard shortcut. Please read the TLXOS user guide for more information on this mode. You can configure which Server the client device will connect to using TMS as shown below



Configure TMS Discovery – This is covered earlier in this user manual

Optional Services

Configure PXE Server - This mode is used for Network installation of TLXOS or to enable Diskless Booting of devices.

Diskless booting is easy to set up, but will only work on the same subnet as the Diskless Server device as we use the ATA over Ethernet protocol

https://en.wikipedia.org/wiki/ATA_over_Ethernet

If you intend to use PXE boot Network Installation mode to install TLXOS, ThinLinX recommends that you set up a separate Network using a Router, even a DSL modem with a Switch port is a good option if you do not have access to a Router. This will isolate the PXE boot Network from your normal Network as only devices PXE booted on the isolated Network will boot our TLXOS installer

Plug the Router / DSL Modem WAN Port into your normal Network to provide Internet connectivity which is required for Automatic Licensing of the 30 Day Free trial. Plug your TLXOS device being configured as a PXE Server into one of the Switch ports on the Router / DSL Modem, plug you other devices of the same class to be installed with TLXOS into the other Switch Ports. If the TLXOS device you are using as a PXE Server is running RePC the devices will be installed with RePC, if you are running Small Form Factor (SFF) the devices will be installed with SFF. If you are using an RPi 4 or RPi400 you may need to update the bootloader to ensure that PXE booting is enabled, you also need a new Blank or newly formatted SD Card fitted to ensure that the RPi does not boot the SD Card before PXE Boot

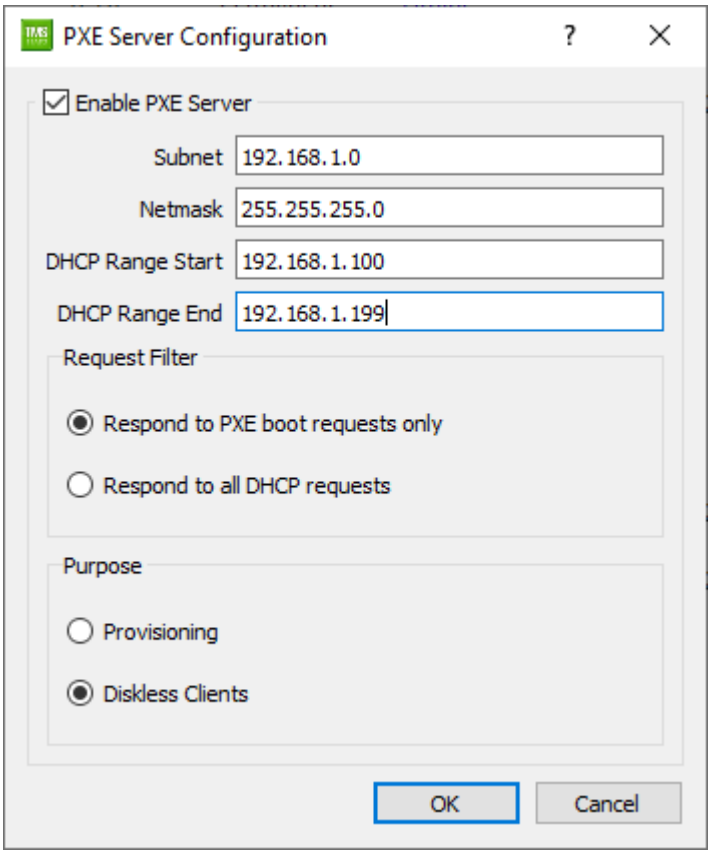
Use the Network information below as a guide but enter your own Network values. Reboot the TLXOS device which you just configured as the PXE Server to permanently save the values you have entered. You can now PXE boot any of the devices to be installed with TLXOS, they will download and install TLXOS from the PXE Server. The PXE Server mode runs in the background. You must be connected to the Internet for the 30 Day Free Trial to successfully register. If the Free trial fails to register due to a Web Proxy, you can use TMS to Register the Free Trial or Permanent License after installation of TLXOS.

You may configure Diskless Clients if you wish to boot devices without any storage fitted, you do NOT need to isolate these from your normal Network. A RPi400 is an excellent PXE Server for a small Network of Diskless RPi’s

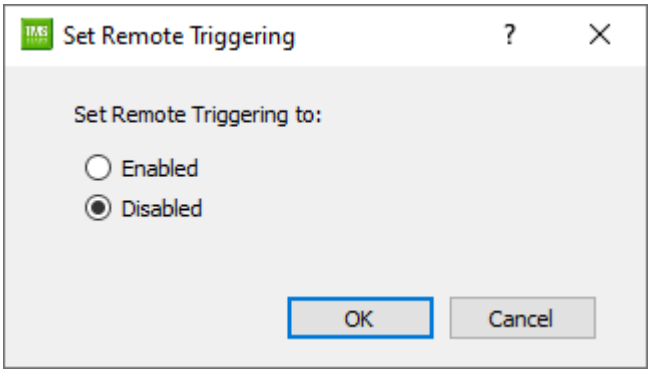
Each Diskless client is allocated 500MB of storage on the system running PXE Server mode, this 500MB of storage is used to hold configuration information but is also big enough to hold Hotfixes etc.

The latest versions of TLXOS 4.11.1 and 4.8.3 preserve the Diskless storage area during

upgrades which means you can use TMS to upgrade the PXE Server device to a newer version and all the diskless devices are then upgraded with their configuration preserved



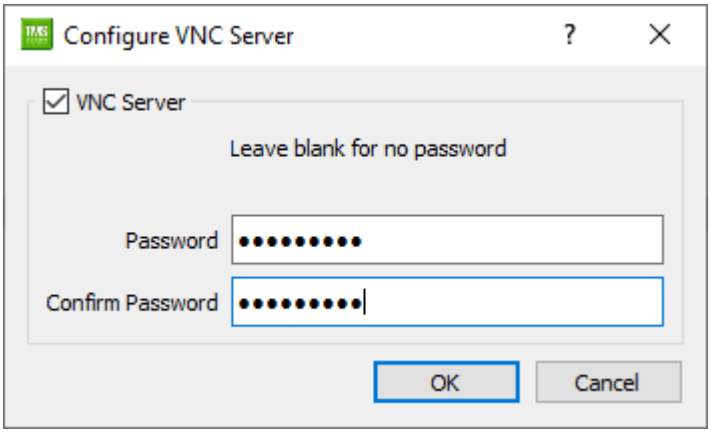
Configure Remote Triggering – Enables an application on TLXOS to be launched remotely



Configure TMS Beacon – This is covered earlier in this user manual

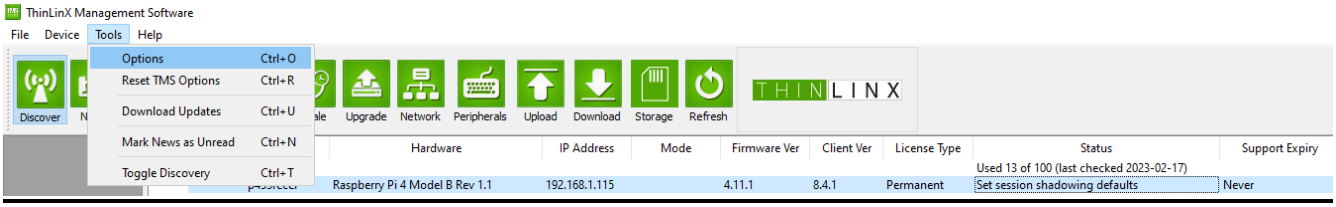
Configure VNC Server – there are use cases where non-interactive shadowing is a legitimate and reasonable requirement (e.g. when the TLXOS device never runs anything like a remote desktop session and no passwords or personal information is ever entered, such as digital signage and some kiosk uses

For such cases we have provided a simple (unencrypted, consent less, forward VNC) alternative. Use this feature at your own risk, adding an access password doesn't improve security much - the encryption used is weak, and is only used for authentication purposes; for session encryption you need SSL.



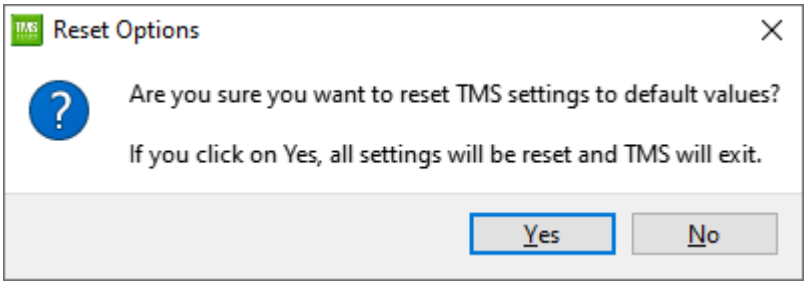
Delete Device – This will delete any highlighted devices on the TMS Console, you would normally only use this option to delete an offline device that you no longer have. If you delete a device by mistake it will reappear the next time that you boot it unless you “Revoke” the License. You will be given the option to “Revoke” the device’s License which frees up the License to be used on another device of the same class. Once you “Revoke” a License that device can NOT be licensed with TLXOS ever again, be very careful with this option

Tools



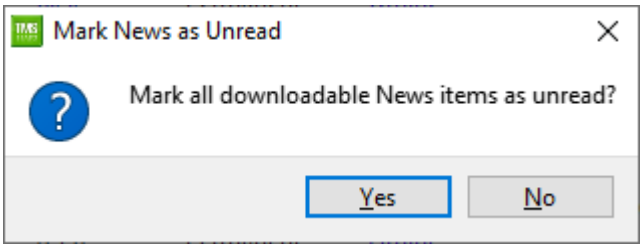
Options – This is explained in the first few pages of this user guide

Reset TMS Options – Resets TMS Options back to defaults

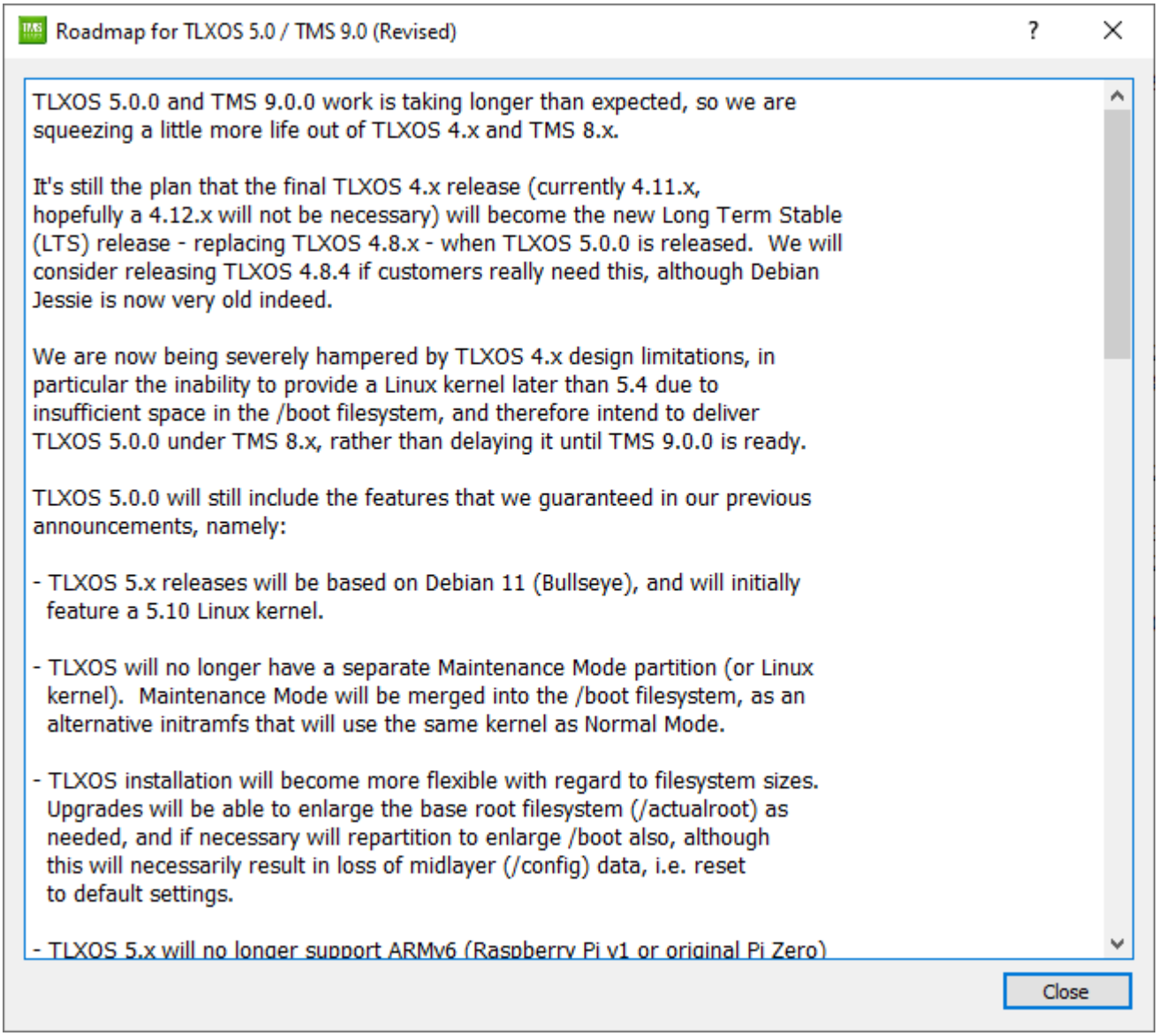


Download Updates – This open the Download Dialog box, you can also use TMS Download Icon to launch this dialog box. This allows you to download TLXOS Firmware Upgrades, TMS Upgrades, TMS Client Upgrades and Hotfixes

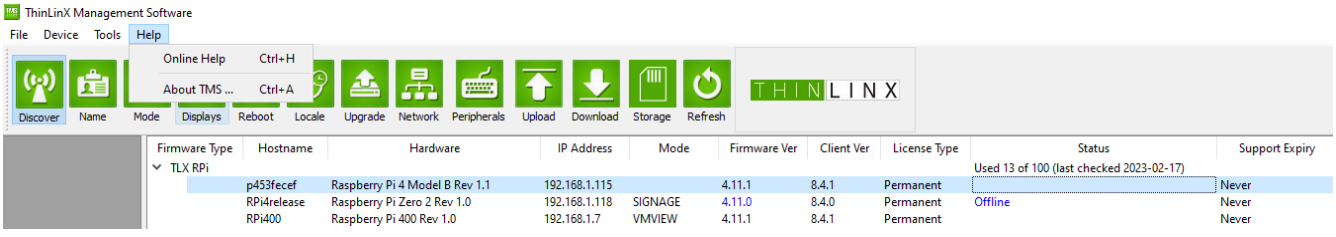
Mark News as Unread



If you select Yes, the next time you start TMS, all the latest TMS and TLXOS News appears on the TMS screen as shown in the example below



Toggle Discovery – This Enables or Disables UDP Device discovery, you can also click on TMS Discover Icon to toggle UDP Discovery on or off

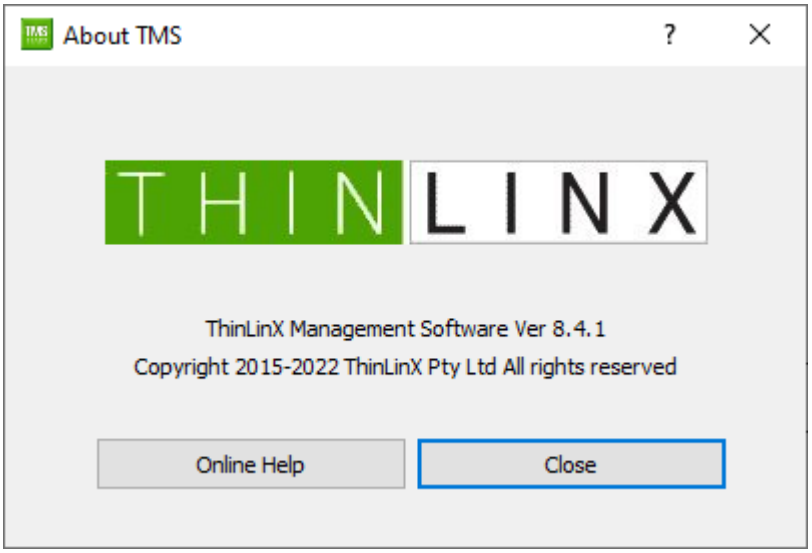


Help

Online Help – Downloads and displays the latest TMS User Manual on your default Web

Browser

About TMS – Launches a dialog box with the TMS version number and the ThinLinX Pty Ltd Copyright message



Wireguard a second VPN option for TLXOS – ThinLinX has integrated the Wireguard Kernel module into the latest TLXOS 4.11.1 and TLXOS 4.8.3

We did not have time for this latest release to update TMS and the local Tlxconfig menu to add Wireguard configuration graphical controls, but you can easily edit a /etc/wireguard/wg0.conf file yourself

Please follow the guide here

How do I obtain root access on a device running TLXOS?

http://help.thinlinx.com/knowledgebase.php?article=7

Once you are logged in as the root user run the commands below

apt-get update

apt-get -y install --no-install-recommends wireguard-tools

You need to create the Wireguard client end Private and Public Keys

cd /etc/wireguard

umask 077

wg genkey | tee client_privatekey | wg pubkey > client_publickey

You then need to create a wg0.conf file in /etc/wireguard

Run touch wg0 to create a blank wg0 file, then use the built in nano or vi editor to create your wg0.conf file

My /etc/wireguard/wg0.conf is pasted below with some comments with what I did

[Interface]
This Desktop/clients's private Key
PrivateKey = enter your private key as generated above

My Wireguard Client ip address
Address = 192.168.10.3/24

[Peer]
Your Server public key
PublicKey = Your Server public key goes here

set ACL ## My client end Network is 192.168.1.0/24 and the Remote
Wireguard Server Network is 192.168.0.0/24
My Wireguard VPN uses Client wg0 IP 192.168.10.3 and server IP 192.168.10.1

Allowed IP’s are my wg0 tunnel 192.168.10.0/24 and my remote network 192.168.0.0/24

The settings below allow me to access any device on my remote 192.168.0.0/24 network

AllowedIPs = 192.168.10.0/24, 192.168.0.0/24

Your server's public IPv4/IPv6 address and port
Endpoint = yourserverdomain:51820

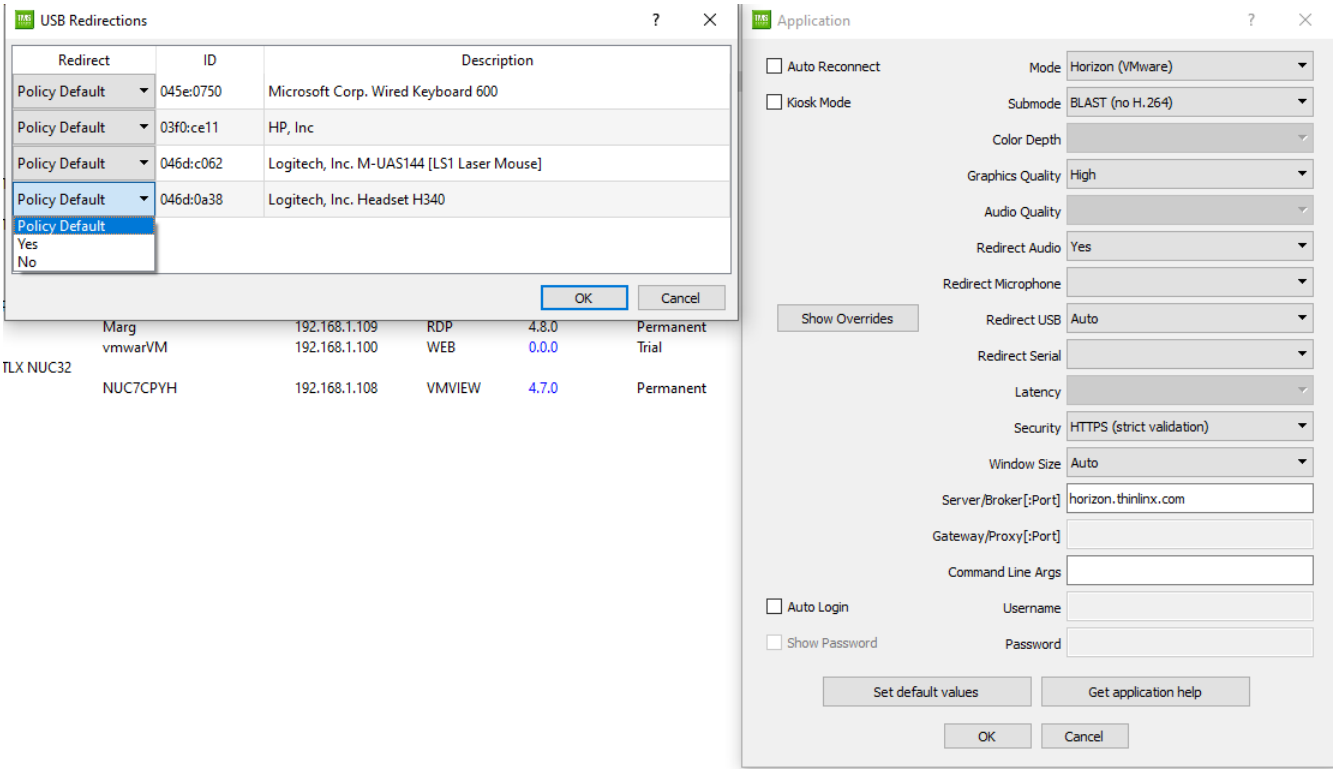
Key connection alive
PersistentKeepalive = 15

After you create the /etc/wireguard/wg0.conf file run the command below and then reboot

systemctl enable wg-quick@wg0

For more information on wireguard https://www.wireguard.com/

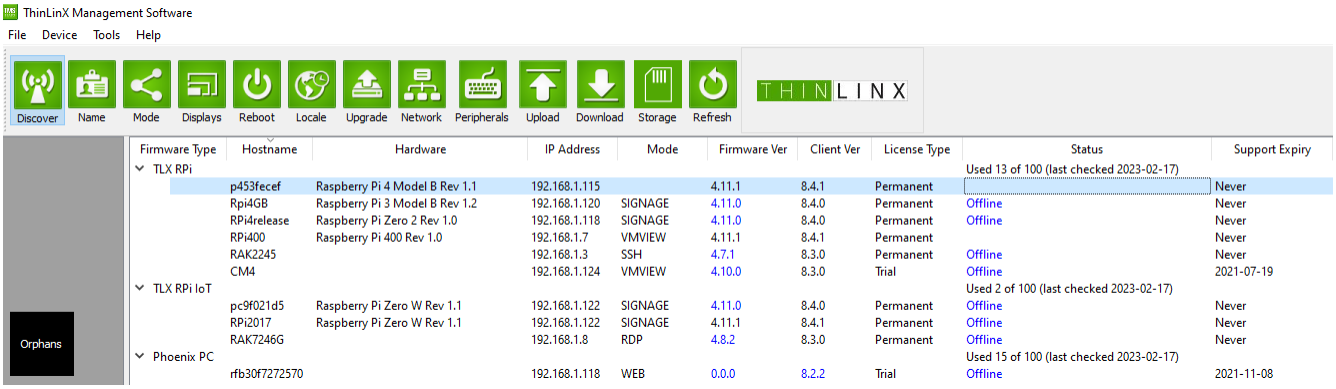
Notes on USB Redirection – Redirection of USB devices can be configured in Citrix HDX, VMware Horizon and RDP modes when Redirect USB is set to Auto or Manual. A “Show Overrides” Icon appears in the left side of the Mode configuration dialog box, you can fine tune USB settings by clicking on this Icon

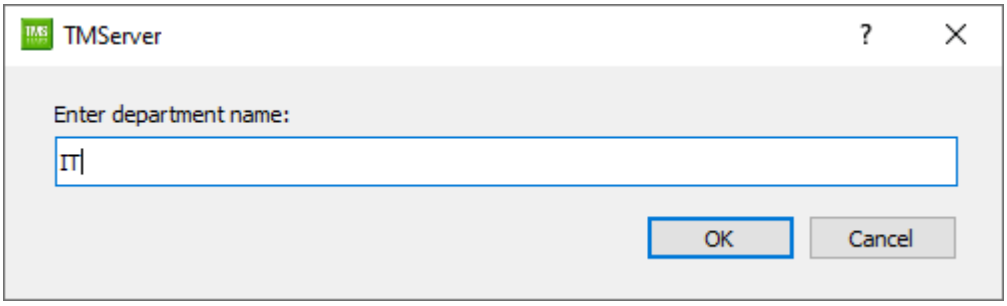


24 Sorting TMS Clients into departments

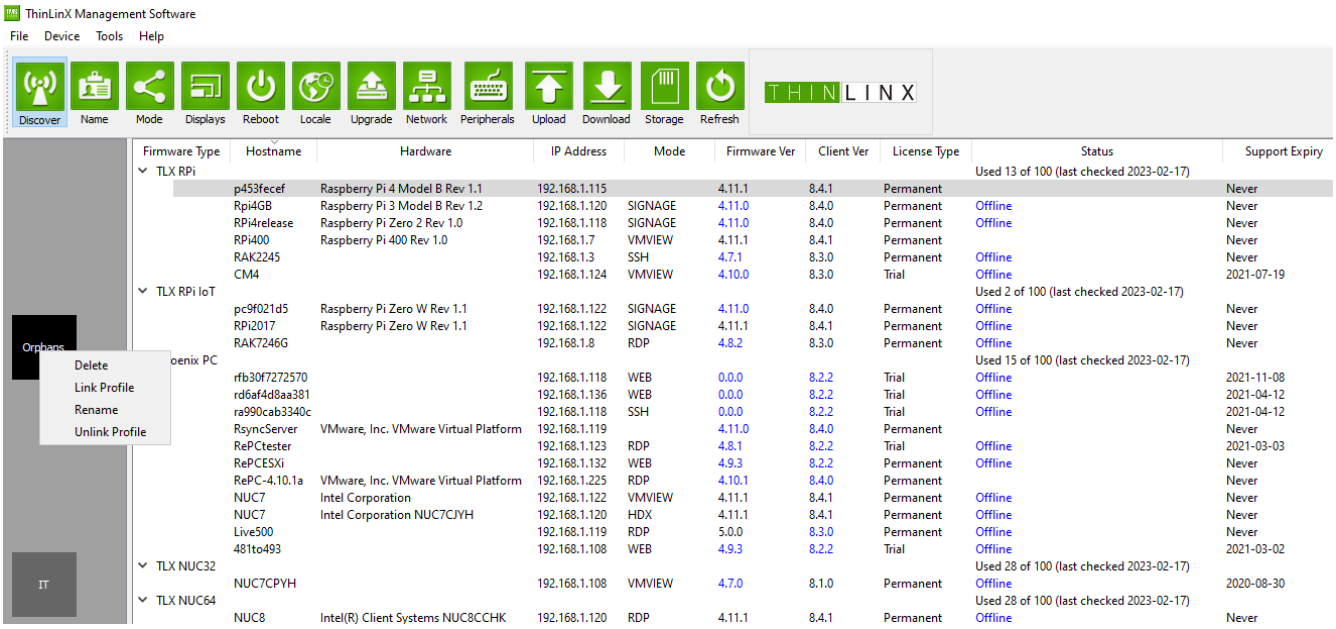
It’s recommended when managing a higher volume of TLXOS units that devices are grouped into sub folders or containers called departments. When TMS is first installed, a default department called *Orphans* is created and all TMS Clients that connect to TMS are stored in this department. You can create as many departments as you wish and store your TMS Clients in these departments.

To create a new department, right click in the *Department* section on the left hand side of the UI, then click on the *New Department* pop-up, as shown below, then enter a name for the department and click on the *OK* Icon.





Once a department has been created, you can rename, delete, link profile or unlink profile by right clicking on the department then clicking on the pop-up as shown below



Firmware Type	Hostname	Hardware	IP Address	Mode	Firmware Ver	Client Ver	License Type	Status	Support Expiry
TLX RPi								Used 13 of 100 (last checked 2023-02-17)	
	p453fecef	Raspberry Pi 4 Model B Rev 1.1	192.168.1.115		4.11.1	8.4.1	Permanent		Never
	Rpi4GB	Raspberry Pi 3 Model B Rev 1.2	192.168.1.120	SIGNAGE	4.11.0	8.4.0	Permanent	Offline	Never
	RPi4release	Raspberry Pi Zero 2 Rev 1.0	192.168.1.118	SIGNAGE	4.11.0	8.4.0	Permanent	Offline	Never
	RPi400	Raspberry Pi 400 Rev 1.0	192.168.1.7	VMVIEW	4.11.1	8.4.1	Permanent		Never
	RAK2245		192.168.1.3	SSH	4.7.1	8.3.0	Permanent	Offline	Never
	CM4		192.168.1.124	VMVIEW	4.10.0	8.3.0	Trial	Offline	2021-07-19
TLX RPi IoT								Used 2 of 100 (last checked 2023-02-17)	
	pc9f021d5	Raspberry Pi Zero W Rev 1.1	192.168.1.122	SIGNAGE	4.11.0	8.4.0	Permanent	Offline	Never
	RPi2017	Raspberry Pi Zero W Rev 1.1	192.168.1.122	SIGNAGE	4.11.1	8.4.1	Permanent	Offline	Never
	RAK7246G		192.168.1.8	RDP	4.8.2	8.3.0	Permanent	Offline	Never
oenix PC								Used 15 of 100 (last checked 2023-02-17)	
	rfb30f7272570		192.168.1.118	WEB	0.0.0	8.2.2	Trial	Offline	2021-11-08
	rd6af4d8aa381		192.168.1.136	WEB	0.0.0	8.2.2	Trial	Offline	2021-04-12
	ra990cab3340c		192.168.1.118	SSH	0.0.0	8.2.2	Trial	Offline	2021-04-12
	RsyncServer	VMware, Inc. VMware Virtual Platform	192.168.1.119		4.11.0	8.4.0	Permanent		Never
	RePCtester		192.168.1.123	RDP	4.8.1	8.2.2	Trial	Offline	2021-03-03
	RePCESXi		192.168.1.132	WEB	4.9.3	8.2.2	Permanent	Offline	Never
	RePC-4.10.1a	VMware, Inc. VMware Virtual Platform	192.168.1.225	RDP	4.10.1	8.4.0	Permanent		Never
	NUC7	Intel Corporation	192.168.1.122	VMVIEW	4.11.1	8.4.1	Permanent	Offline	Never
	NUC7	Intel Corporation NUC7CJYH	192.168.1.120	HDX	4.11.1	8.4.1	Permanent	Offline	Never
	Live500		192.168.1.119	RDP	5.0.0	8.3.0	Permanent	Offline	Never
	481to493		192.168.1.108	WEB	4.9.3	8.2.2	Trial	Offline	2021-03-02
TLX NUC32								Used 28 of 100 (last checked 2023-02-17)	
	NUC7CPYH		192.168.1.108	VMVIEW	4.7.0	8.1.0	Permanent	Offline	2020-08-30
TLX NUC64								Used 28 of 100 (last checked 2023-02-17)	
	NUC8	Intel(R) Client Systems NUC8CCHK	192.168.1.120	RDP	4.11.1	8.4.1	Permanent	Offline	Never

TMS does not allow you to delete departments that have TMS clients assigned to them. First reassign clients before deleting a department.

You can change the order in which the departments you created are displayed. Simply drag and drop them to create the order you want.

To move a TLXOS device to particular department, just drag it from the UI and drop it into the relevant department.

If a TLXOS device that was previously discovered and visible on TMS is no longer visible, check each department to see if you have misplaced it and in fact it is visible but hidden in a different department. When you click on a department you will only see devices that are in that department. If a device is still not visible it may need to be power cycled to force a reboot.

25 Helpful information and links

Please take the time to read the following additional user guides

https://thinlinx.com/tlxos-user-manual.pdf
https://thinlinx.com/faq/
http://help.thinlinx.com/knowledgebase.php

Changelog for TLXOS 4.10.0, TLXOS 4.8.2, Tlxconfig 4.6 / TMS Client and TMS 8.3.0.

http://help.thinlinx.com/knowledgebase.php?article=71
http://help.thinlinx.com/knowledgebase.php?article=72
http://help.thinlinx.com/knowledgebase.php?article=69
http://help.thinlinx.com/knowledgebase.php?article=70

Top FAQ's listed below

How does TLXOS Licensing work?
http://help.thinlinx.com/knowledgebase.php?article=8

What hardware does TLXOS support? What is each TLXOS edition for?
http://help.thinlinx.com/knowledgebase.php?article=35

Is there a virtual appliance for managing TLXOS devices?
http://help.thinlinx.com/knowledgebase.php?article=64

Is TLXOS 32-bit or 64-bit?

http://help.thinlinx.com/knowledgebase.php?article=29

How many gigabytes of RAM does my Pi need?

http://help.thinlinx.com/knowledgebase.php?article=46

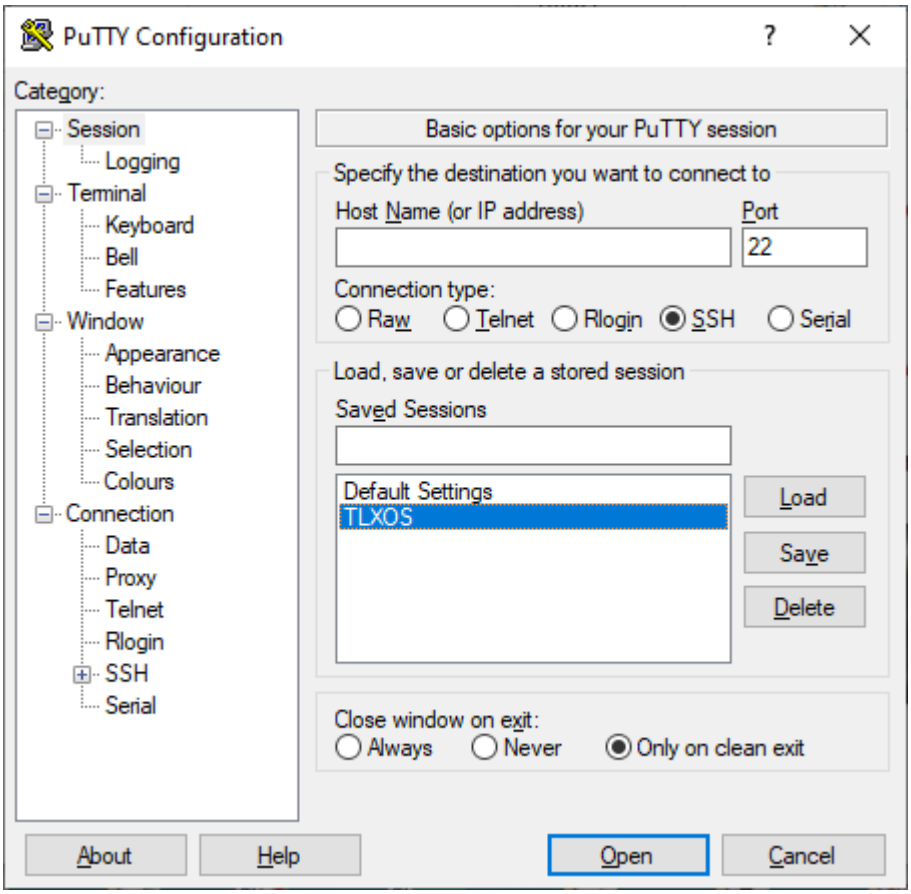
How can I protect clients from rogue/unauthorized TMS servers?

http://help.thinlinx.com/knowledgebase.php?article=73

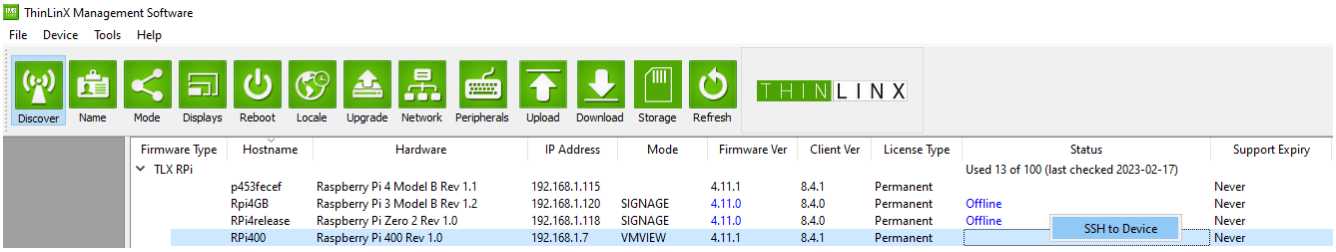
How do I obtain root access on a device running TLXOS?

http://help.thinlinx.com/knowledgebase.php?article=7

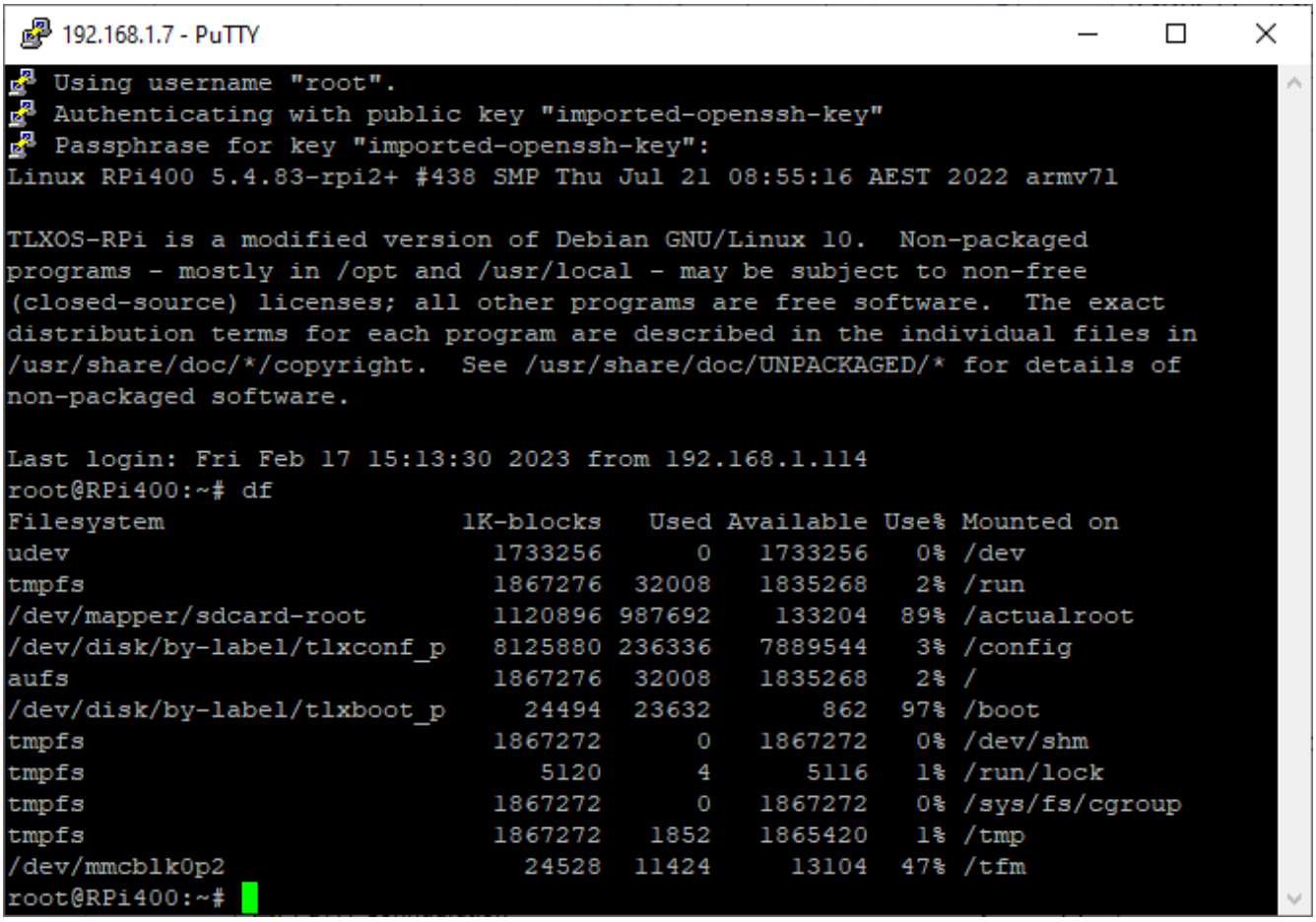
You can also use TMS to launch a ssh session using Putty if you save the session information as you configured it above with the name “TLXOS”



To ssh to a TLXOS using TMS, highlight the device by clicking on it, then right click to launch the SSH to Device option and then press Enter



Press Enter or Click on “SSH to Device” to launch the SSH Session, enter your Passcode when the Xterm SSH Window appears, you are now logged in as root.



Some of our users want to install additional software of their choice, of course they are free to do this if they wish, at their own risk

Any Software that is installed may be deleted / completely erased at any time by simply carrying out a

Factory reset using TMS or the Local Desktop

You can see in the above Putty xterm window that I have typed df to see the file system disk space usage on a 4GB RAM RPi400. Note that tmpfs is mounted on /run, this is the directory that is used to temporarily store any software that you install before storing it permanently to the SD Card or Disk drive on Shut down or Reboot of a TLXOS device

In the example above you can see there is a total of 1835268 1K-Blocks available in /run, if you are planning on installing some large software packages you may run out of space unless you run the following command to allocate more system memory to /run

“mount –o remount,size=85% /run” You can adjust the 85% to larger or smaller

The next step is to run “apt-get update”

Then apt-get install “your package name”

If you are installing a number of packages it is still possible to run out of Ram in which case you should run the “df” command between packages to see if the /run directory is nearly full

If so, simply reboot TLXOS, the shutdown / reboot will take longer than usual as the system is writing the installed packages to the SD Card / Hard Disk during the shutdown phase.

To continue installing new packages repeat the process above

How do I pair a Bluetooth Device?

We are planning on adding graphical controls to configure Bluetooth in a future TMS release, however this is not a priority due to lack of interest in Bluetooth on TLXOS

ThinLinX will add a GUI to make this easy but for now you have to ssh as root and then run the commands below, this example is for pairing a Bluetooth Keyboard (modify for your detected Hardware)

bluetoothctl

[NEW] Controller 00:10:20:30:40:50 pi [default]

[bluetooth]# agent KeyboardOnly

Agent registered

[bluetooth]# default-agent
Default agent request successful

[bluetooth]# scan on
Discovery started
[CHG] Controller 00:10:20:30:40:50 Discovering: yes
[NEW] Device 00:12:34:56:78:90 myLino
[CHG] Device 00:12:34:56:78:90 LegacyPairing: yes

```
[bluetooth]# pair 00:12:34:56:78:90
Attempting to pair with 00:12:34:56:78:90
[CHG] Device 00:12:34:56:78:90 Connected: yes
[CHG] Device 00:12:34:56:78:90 Connected: no
[CHG] Device 00:12:34:56:78:90 Connected: yes
Request PIN code
[agent] Enter PIN code: 1234
[CHG] Device 00:12:34:56:78:90 Paired: yes
Pairing successful
[CHG] Device 00:12:34:56:78:90 Connected: no

[bluetooth]# connect device 00:12:34:56:78:90
```

Copyright