



ThinLinX Management Software

User Manual

Version 8.0.0

November 10, 2017

1	INTRODUCTION	3
2	TMS ON WINDOWS INSTALLATION	3
3	TMS ON LINUX INSTALLATION	3
4	STARTING TMS.....	3
5	CONFIGURING TMS	3
6	TLXOS DEVICE DISCOVERY VIA TMS	7
7	DHCP OPTION FLAGS FOR TMS DISCOVERY & TLXOS CONFIGURATION.....	9
8	ASSIGNING A HOSTNAME TO A TLXOS DEVICE.....	10
9	SETTING THE REMOTE SERVER AND CONNECTION MODE	11
10	SETTING THE CLIENT PROTOCOL EXPERIENCE LEVEL	15
11	<i>SETTING SCREEN RESOLUTION</i>	16
12	REBOOTING A TLXOS DEVICE	18
13	SETTING THE TIME ZONE AND TIME SERVER	19
14	DOWNLOADING FIRMWARE UPDATES FOR TLXOS DEVICES	21
16	NETWORK CONFIGURATION	23
17	PERIPHERALS CONFIGURATION	24
18	FIREWALL CONFIGURATION	25
19	UPLOAD FILES TO YOUR DEVICES	25
20	STORAGE CONFIGURATION.....	26
21	THE FILE MENU	27
22	THE DEVICE MENU.....	27
23	SORTING TMS CLIENTS INTO DEPARTMENTS	43
24	FAQ.....	45

1 Introduction

ThinLinX Management Software (TMS) provides the ability to configure and manage any ARM or X86 Architecture device running the ThinLinX Operating System (TLXOS).

TMS can be used for a variety of tasks, ranging from something as simple as rebooting a TLXOS device, to upgrading the device with the latest TLXOS software. TMS runs on Windows and Linux, supports all TLXOS devices including Raspberry Pi devices, Intel Small Factor devices such as the Intel NUC's, Compute Sticks & clones 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 onto your Windows system, double click the downloaded file and follow the instructions.

3 TMS on Linux installation

TMS is available as a downloadable Ubuntu .deb package and as a Redhat .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 .rpm package, copy the Redhat Linux package to your Linux system and install with command

```
“rpm -i tms-filename.rpm”
```

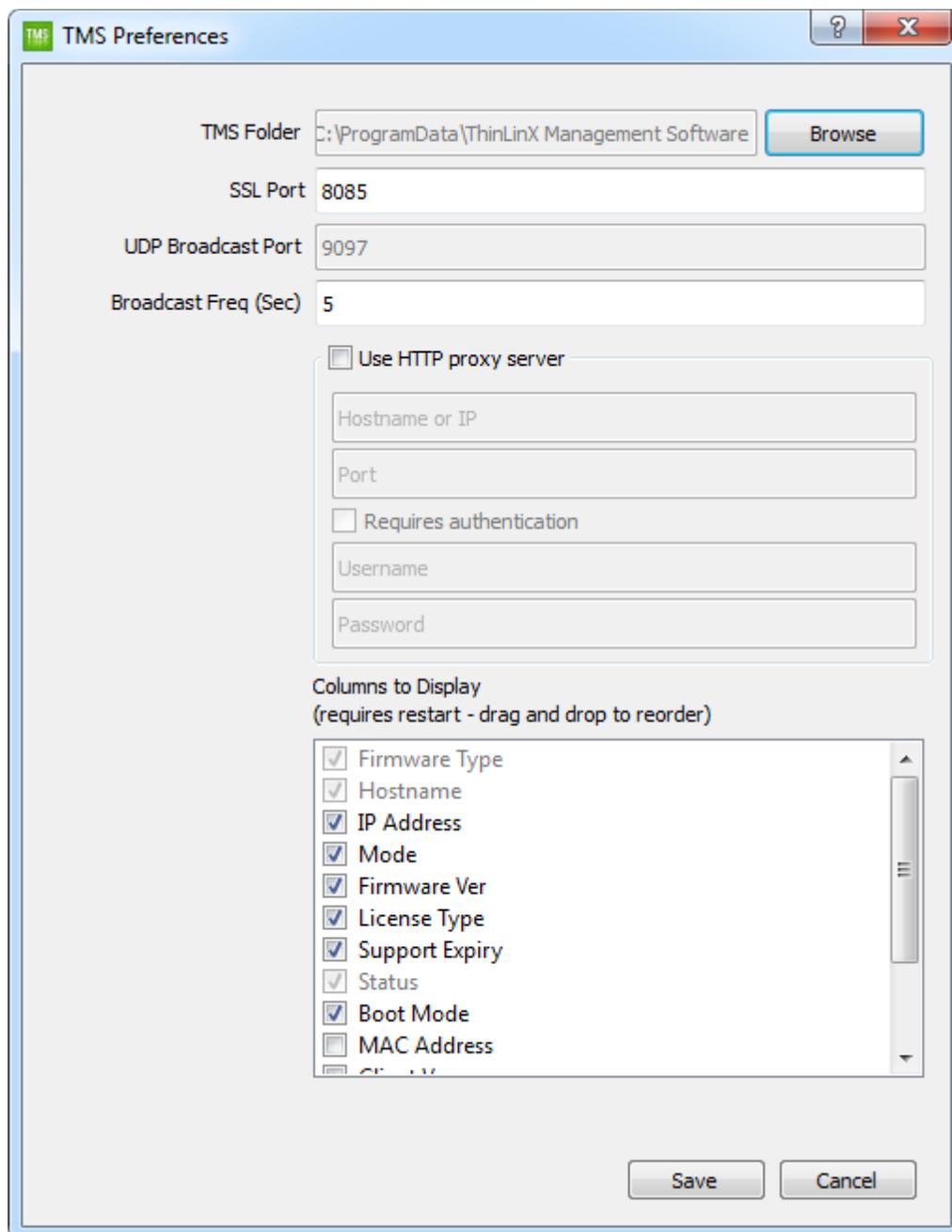
4 Starting TMS

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

SSL Port 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.

UDP broadcast port 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.

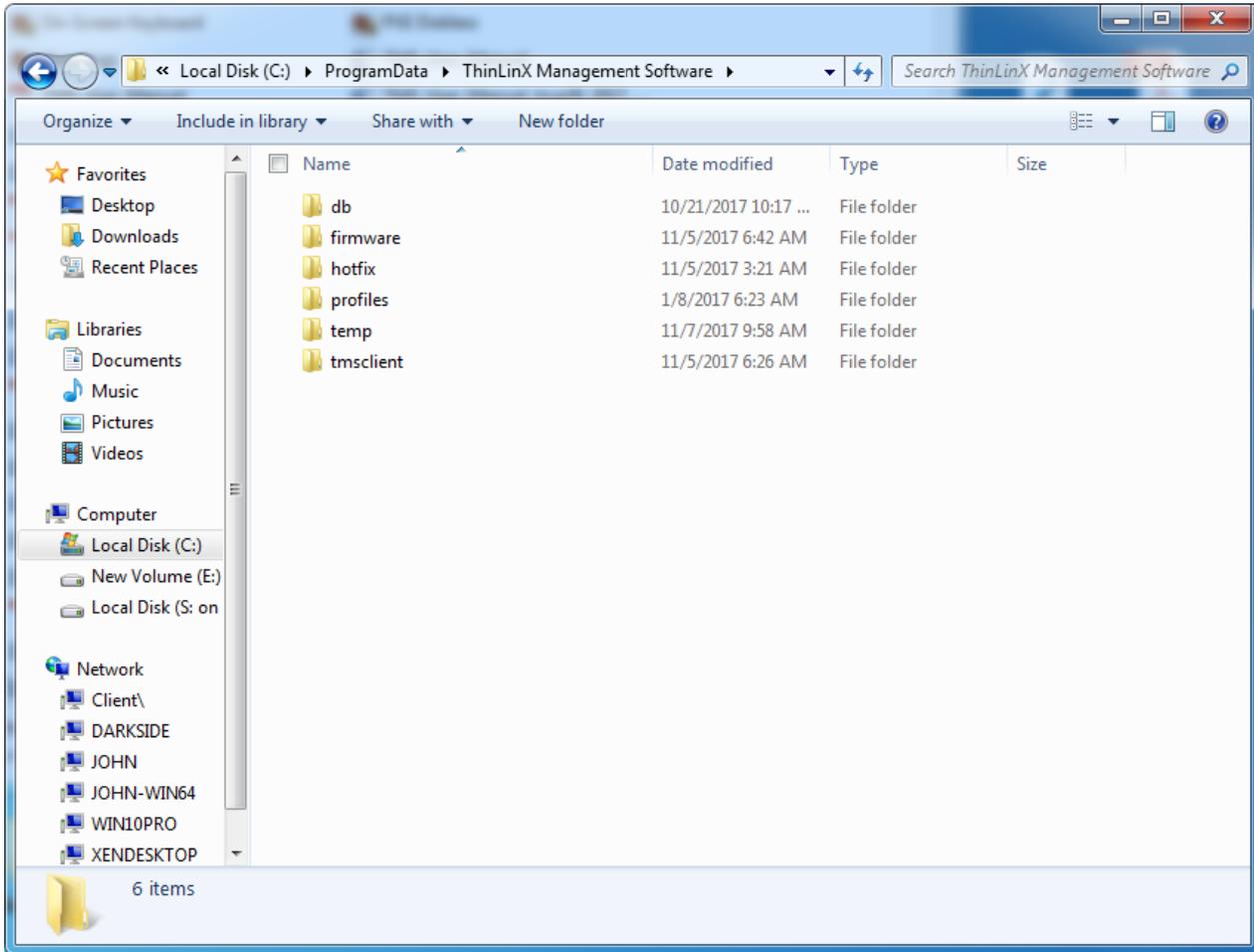
Use HTTP proxy server checkbox enables the TMS Administrator to set the Hostname or IP Address of a proxy server. This may be required to allow TMS to access the Internet on some Networks. Internet access is required to download Firmware updates and License Products running TLXOS.

Requires 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 six 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

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

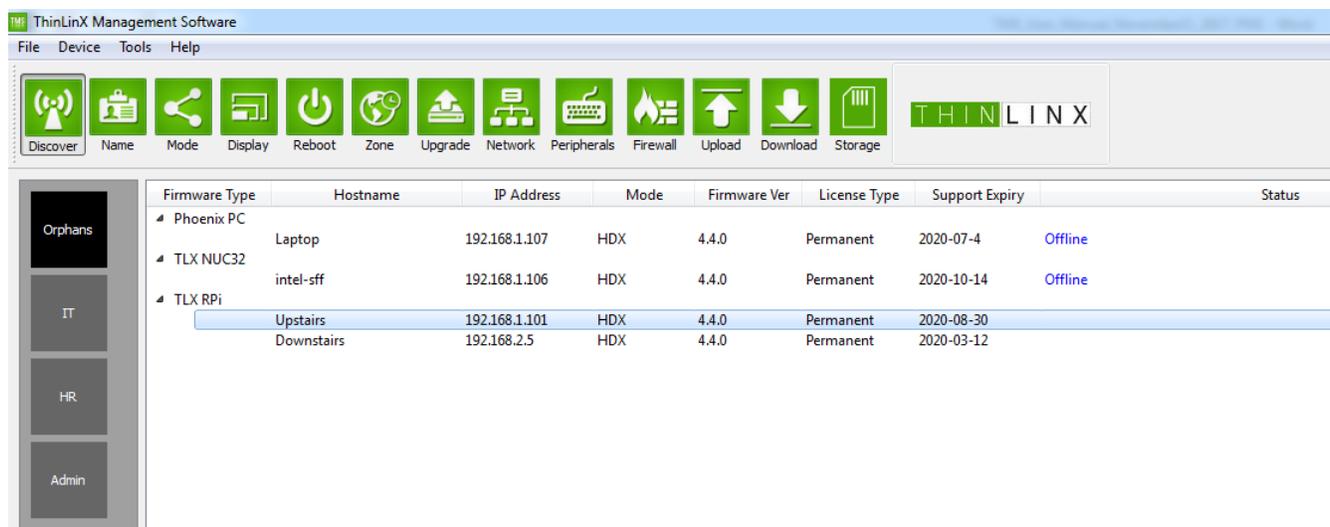
The tmsclient directory is used to store updated versions of the TMS client, these are downloaded using the TMS Download Icon

6 TLXOS device discovery via TMS

TMS utilizes three 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 using TMS -> Tools -> Options

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



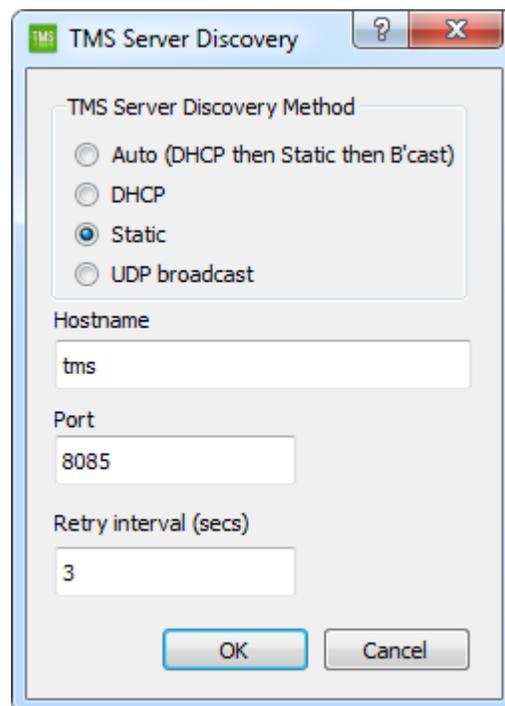
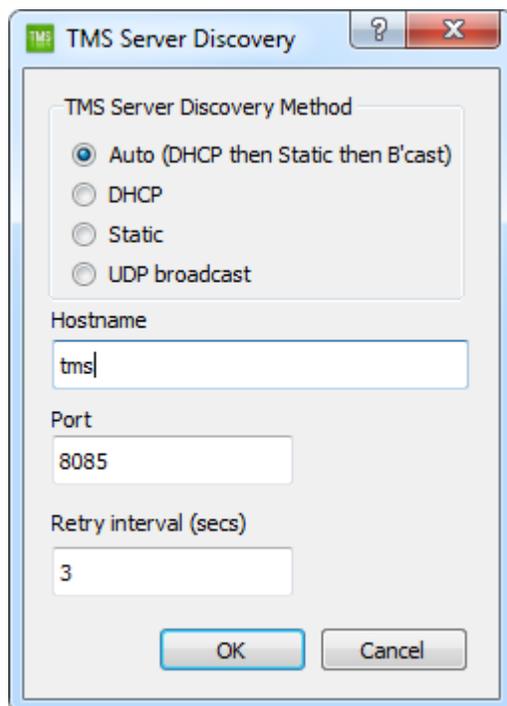
The default setting is UDP discovery turned on. When TMS is launched this commences the TMS server packet broadcast via UDP to all TLXOS Clients. Once acknowledged, the TLXOS devices then connect to the TMS server and display/populate under the TMS client area

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, 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.

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.



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. In other words 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`, `mplayer`, `netop`, `nx`, `perf`, `rdp`, `rfx`, `spice`, `ssh`, `telnet`, `tn3270`, `vmview`, `vnc`, `web`, `x11`.

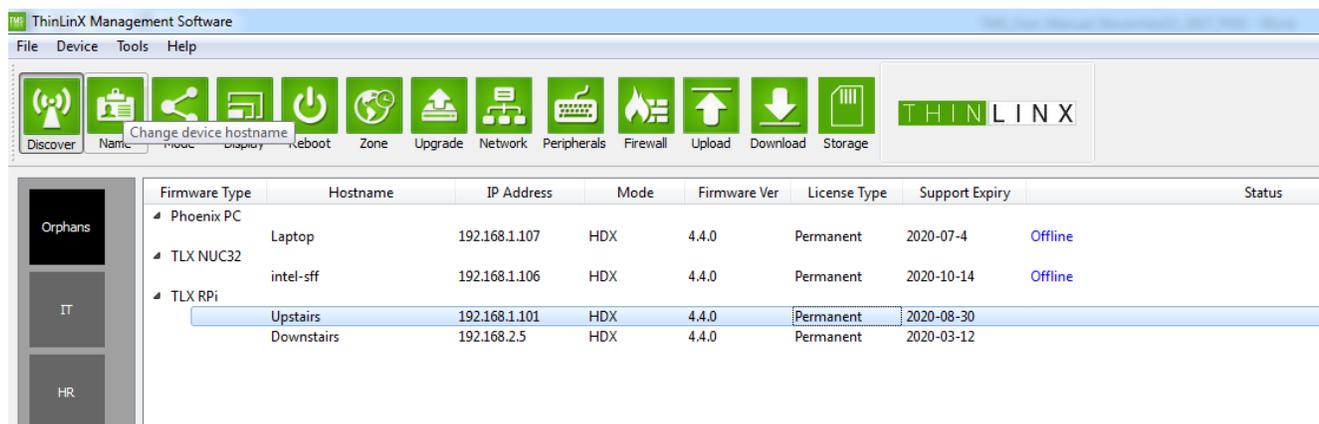
("dsi" means "digital signage", "netop" means "TCM", and "vmview" means "horizon")

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 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;



The administrator may also wish to set a descriptive name using Tools -> Quick Launch -> Change Description. You can display the descriptive name on TMS by selecting Edit -> Settings and then selecting the check box next to “Description” in the Columns to Display Dialog box

9 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 16 different connection Modes can be configured. These connection types are

- a) 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
- b) SSH, launches a SSH session
- c) RDP, launches a standard RDP (non VDI) connection to a Desktop, Submode RemoteFX launches a connection to a Microsoft RemoteFX VDI Desktop
- d) VNC, Launches Turbo VNC Viewer
- e) X11, launches a X11 client to connect to a Linux Desktop using XDMCP
- f) TCM, under development
- g) Spice, launches a Red Hat Spice Protocol client
- h) 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
- i) NoMachineNX, launches a NoMachine client
- j) Telnet, launches a Telnet client
- k) Tn3270, launches the Tn3270 IBM Mainframe client
- l) Horizon, launches the VMware Horizon client
- m) Performance monitor, launches nmon <http://nmon.sourceforge.net/pmwiki.php>
- n) User Defined (Bespoke) Enables a custom App to be launched
- o) Digital Signage, changes the mode to Digital Signage, play Images, Video, Web Content
- p) Media Player

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

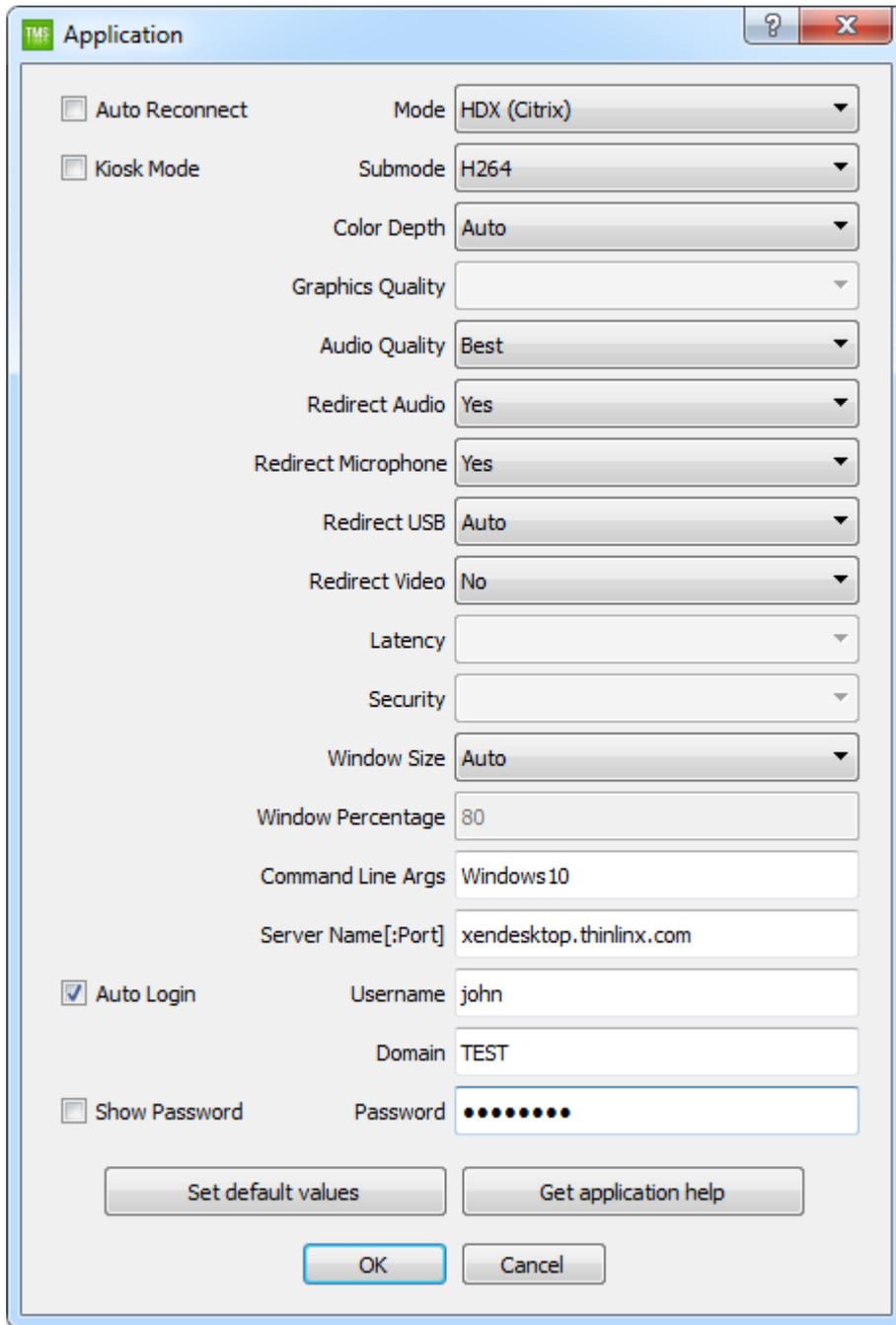
TMS Application [?] [X]

<input type="checkbox"/> Auto Reconnect	Mode	Web
<input checked="" type="checkbox"/> Kiosk Mode	Submode	
	Color Depth	
	Graphics Quality	
	Audio Quality	
	Redirect Audio	
	Redirect Microphone	
	Redirect USB	
	Redirect Video	
	Latency	
	Security	
	Window Size	Auto
	Window Percentage	80
	Command Line Args	
	Server Name[:Port]	xendesktop.thinlinux.com
<input type="checkbox"/> Auto Login	Username	
	Domain	
<input type="checkbox"/> Show Password	Password	

Set default values Get application help

OK Cancel

The image below shows a Citrix HDX native client session connection to Citrix Storefront, the Storefront name “xendesktop.thinlinux.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.thinlinux.com” and the Desktop named Windows10 has been selected as the desktop to launch, the Auto Reconnect 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

<input checked="" type="checkbox"/> Auto Reconnect	Mode	HDX (Citrix)
<input type="checkbox"/> Kiosk Mode	Submode	H264
	Color Depth	Auto
	Graphics Quality	
	Audio Quality	Best
	Redirect Audio	Yes
	Redirect Microphone	Yes
	Redirect USB	Auto
	Redirect Video	No
	Latency	
	Security	
	Window Size	Auto
	Window Percentage	80
	Command Line Args	Windows10
	Server Name[:Port]	xendesktop.thinlinux.com
<input type="checkbox"/> Auto Login	Username	
	Domain	
<input type="checkbox"/> Show Password	Password	

Buttons: Set default values, Get application help, OK, Cancel

10 Setting the client protocol experience level

As per *Setting the connection type used to connect to a remote server*, the Access Protocol dialogue box allows users to set various settings for TMS clients in relation to the experience level of various settings including;

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 or Off, if you are using RDP/RemoteFX you must set Manual to redirect USB devices, this will launch a USB Redirection Dialog box

Redirect Video enables Video to be redirected to the client for local decoding

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, options include Default, SSL and NLA. If using RDP or RemoteFX you will need to set this to NLA. 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.

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* button 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 button. 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

11 *Setting screen resolution*

TMS allows you to set the Screen resolution on any TLXOS devices, this may be the Single Display Raspberry Pi, the Dual Display Intel NUC or a Re-Purposed PC. In the case of the single display RPi, the only values that can be changed are the Resolution via the drop down Resolution box or the Orientation. 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

800 x 600

1024 x 768

1280 x 720

1280 x 960

1280 x 1024

1366 x 768

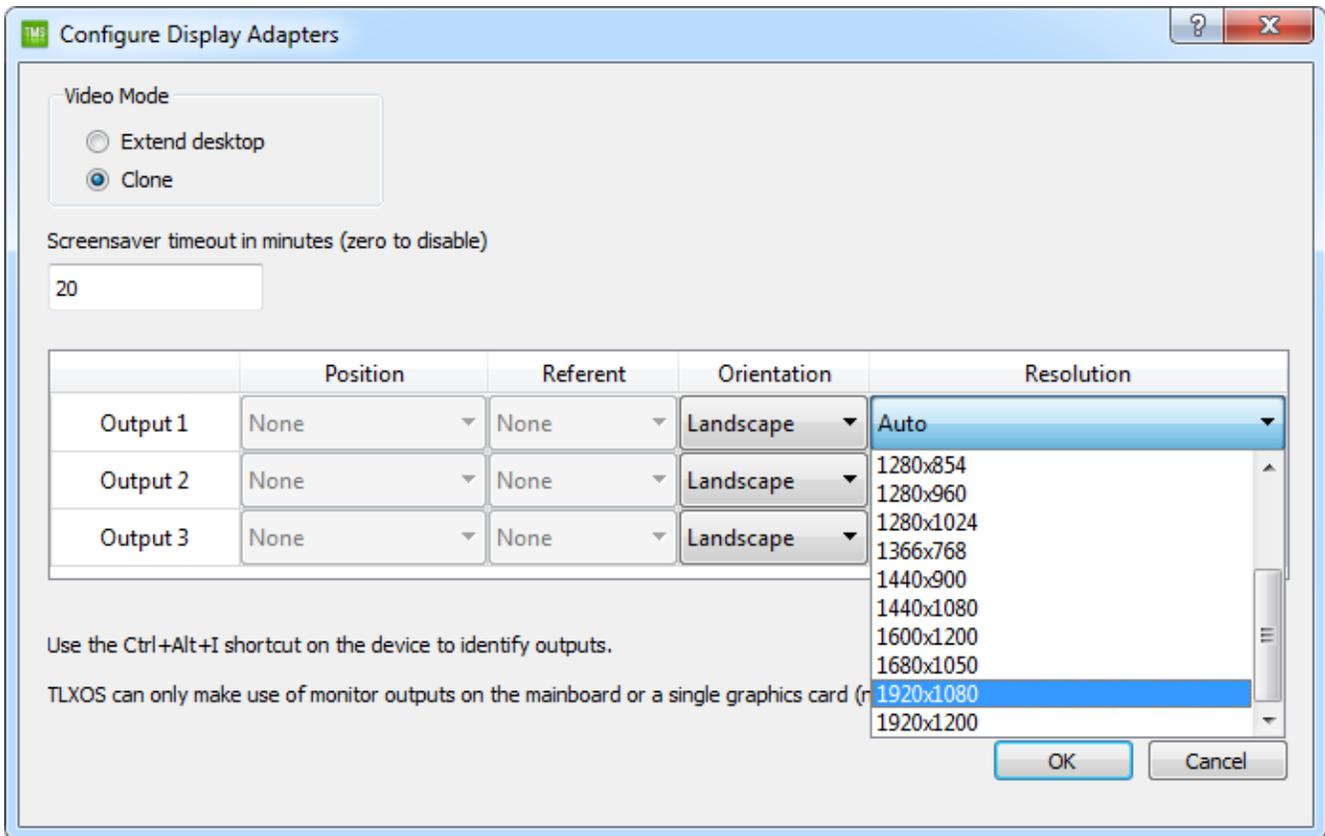
1440 x 900

1600 x 1200

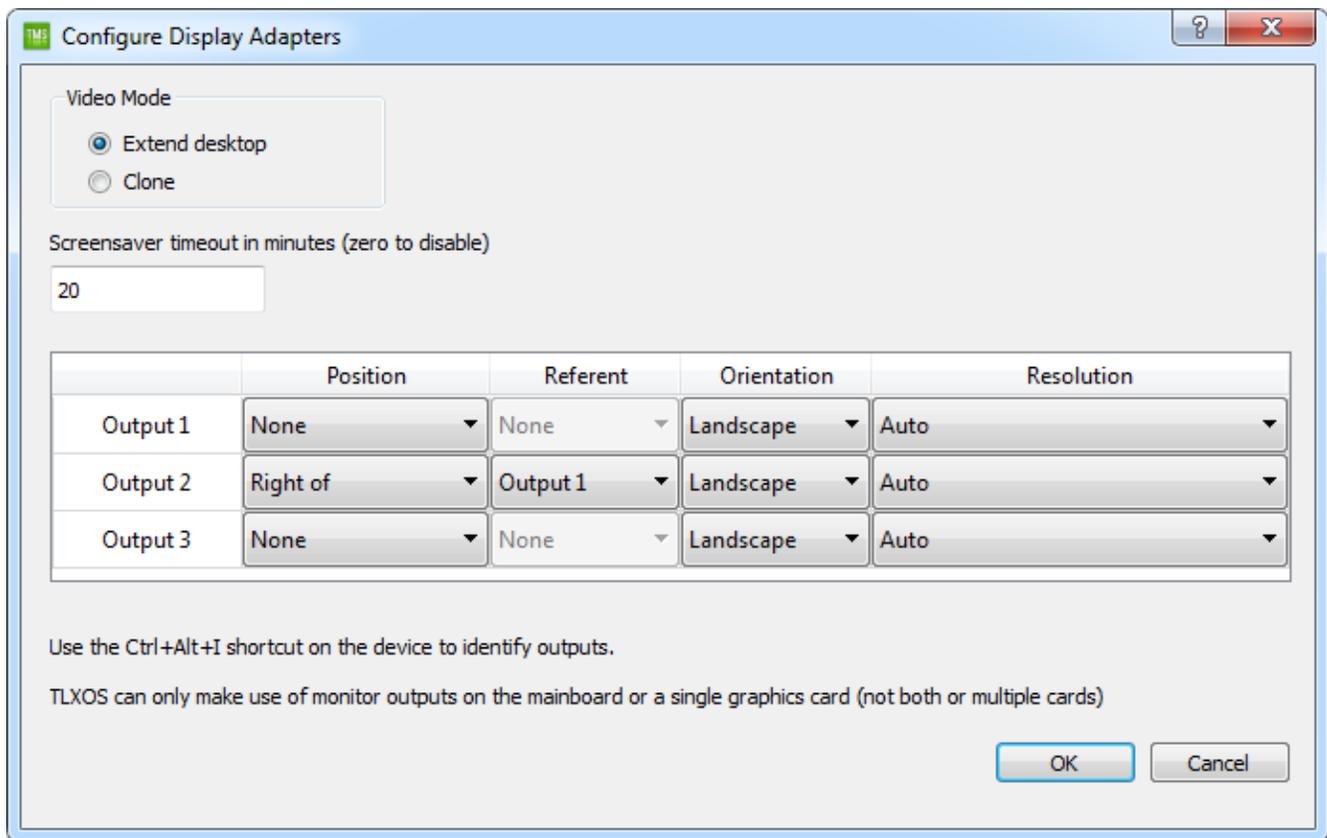
1680 x 1050

1920 x 1080 is also known as 1080p this is the default resolution on most Monitors

1920 x 1200



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

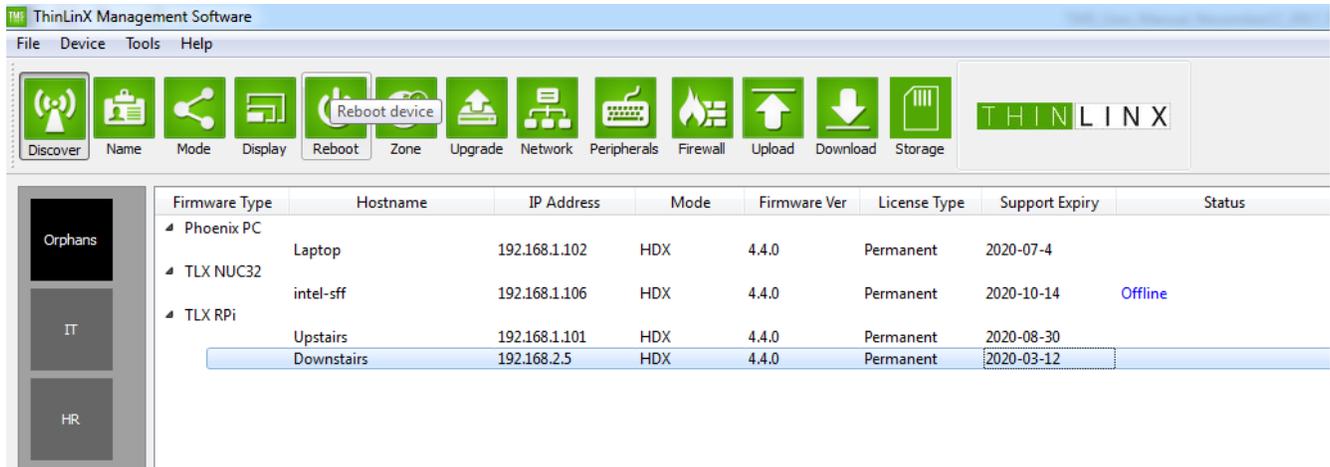


After changing the resolution a reboot of the TLXOS device is required

12 Rebooting a TLXOS Device

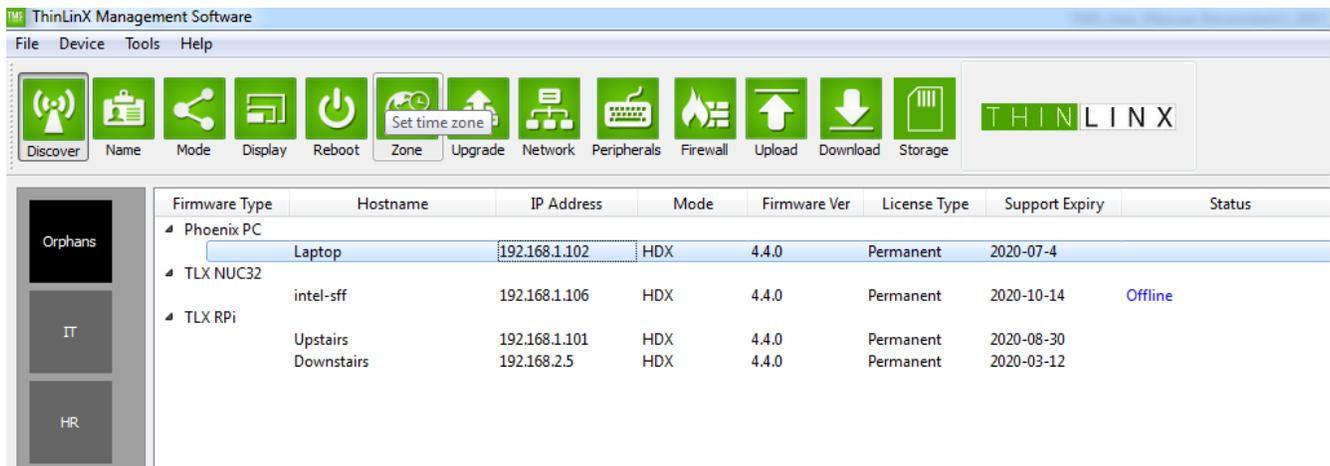
To reboot TLXOS devices, highlight the devices and then click on the *Reboot* button as per the image below

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

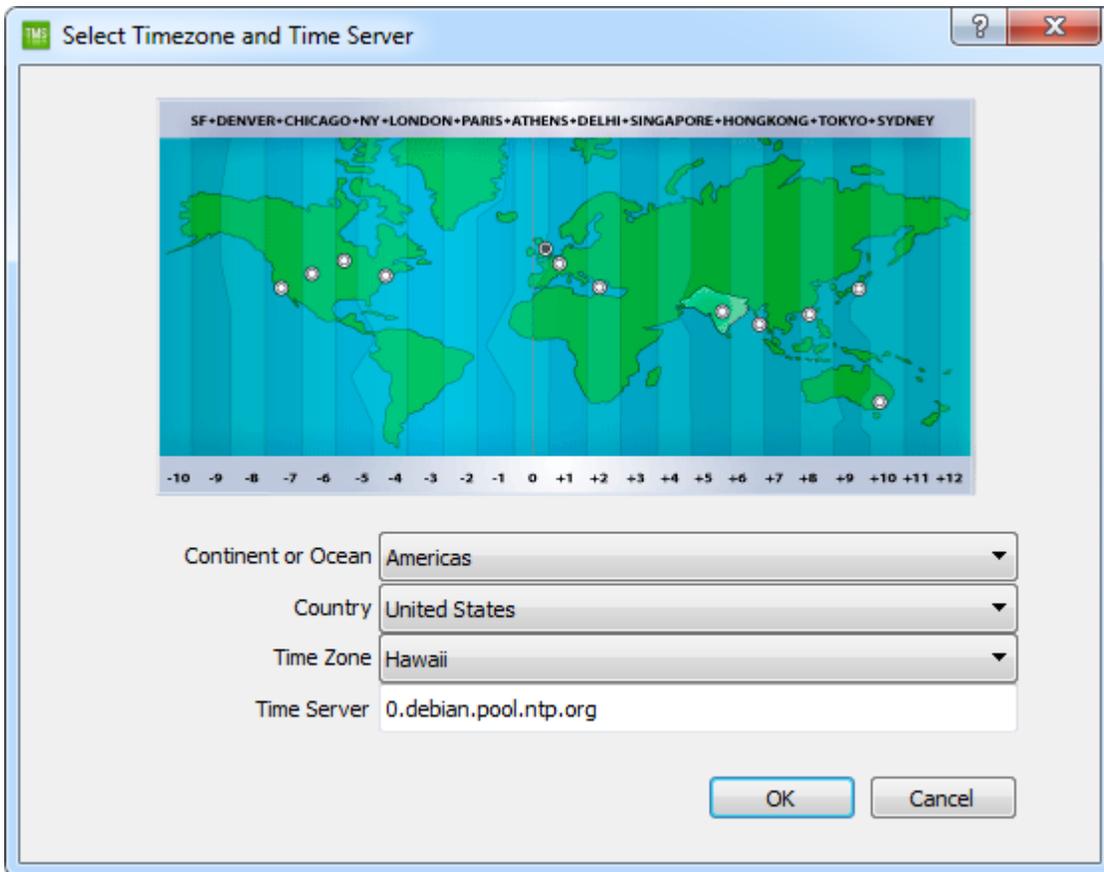


13 Setting the Time zone and Time Server

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



The following dialog boxes will appear allowing you select the *Continent*, *Country* and *Time zone* as shown below. In addition to this a specific NTP *Time Server* value must also be specified, by default TLXOS devices uses the *0.debian.pool.ntp.org* Time Server. You may wish to set this to your local Network Time Server instead



Click the *OK* button 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). An incorrect time can also affect TMS Discovery of clients

14 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 or Hotfix 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 or Hotfix is automatically unzipped in the TMS Firmware or Hotfix directory.

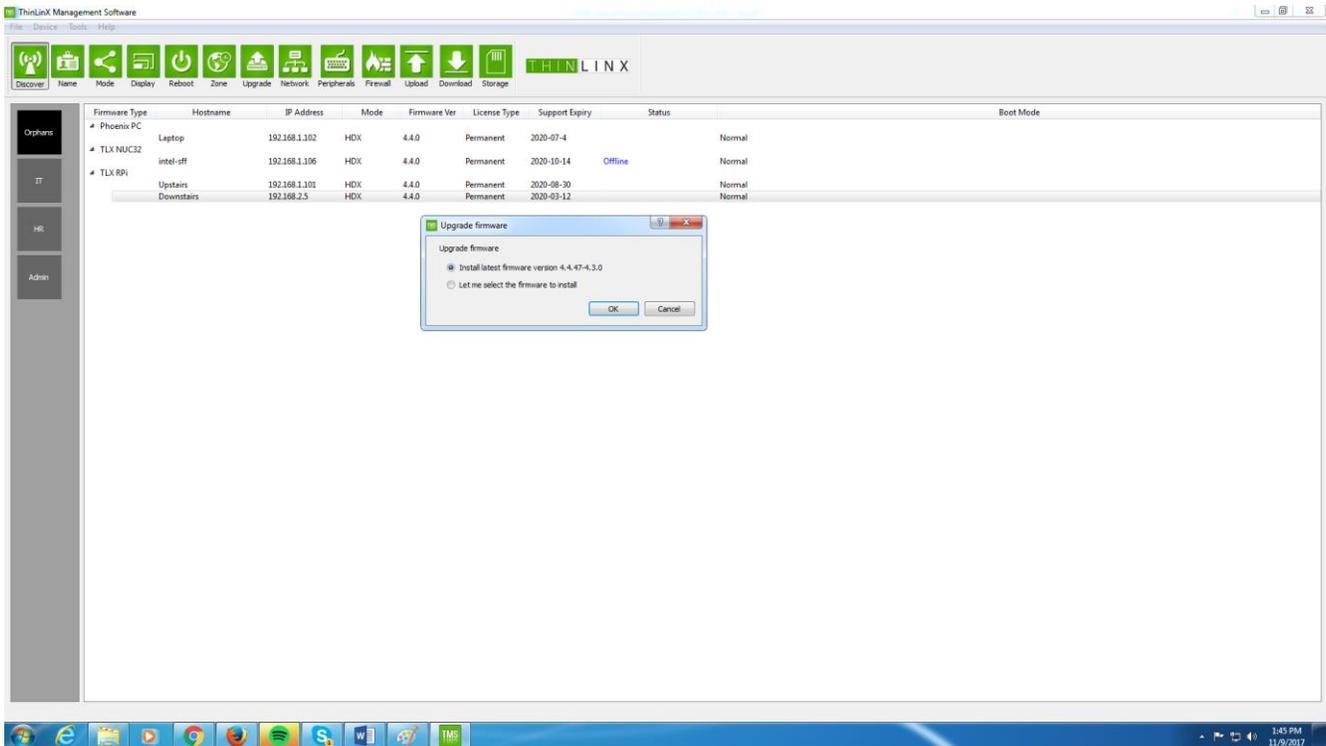
The screenshot shows the ThinLinX Management Software interface. The main window displays a table of devices with columns for Firmware Type, Hostname, IP Address, Mode, Firmware Ver, License Type, Support Expiry, and Status. A dialog box titled 'Select Updates to Download' is open, showing a list of updates with checkboxes for selection. The dialog box includes a dropdown menu for 'Select server closest to your location' set to 'Asia' and buttons for 'OK' and 'Cancel'.

Firmware Type	Hostname	IP Address	Mode	Firmware Ver	License Type	Support Expiry	Status
Phoenix PC	Laptop	192.168.1.102	HDX	4.4.0	Permanent	2020-07-4	
TLX NUC32	intel-sff	192.168.1.106	HDX	4.4.0	Permanent	2020-10-14	Offline
TLX RPi	Upstairs	192.168.1.101	HDX	4.4.0	Permanent	2020-08-30	
	Downstairs	192.168.2.5	HDX	4.4.0	Permanent	2020-03-12	

	Upgrade Type	Platform	Release Date	Size in MB	
1	<input type="checkbox"/>	TMS server 7.10.0 for Windows	TLX_NUC64	Jun-26-2017	6.48121
2	<input type="checkbox"/>	TMS server 7.10.0 for RHEL/CentOS 7 x86_64	TLX_NUC64	Jun-26-2017	0.550961
3	<input type="checkbox"/>	TMS server 7.10.0 for Ubuntu/Debian x86_64	TLX_NUC64	Jun-26-2017	0.644304
4	<input type="checkbox"/>	TMS client 7.13.2	Phoenix_PC	Aug-28-2017	1.21637
5	<input type="checkbox"/>	TMS client 7.13.2	TLX_NUC32	Aug-28-2017	1.21637
6	<input type="checkbox"/>	TMS client 7.13.2	TLX_NUC64	Aug-28-2017	1.21637
7	<input type="checkbox"/>	TMS client 7.13.2	TLX_RPi	Aug-28-2017	1.21637
8	<input type="checkbox"/>	TMS client 7.13.2	TLX_RPi_MC	Aug-28-2017	1.21637

The Firmware or Hotfix is downloaded once and can then be installed on many TLXOS devices simultaneously by highlighting each device then clicking on the Upgrade Icon or in the case of a Hotfix select TMS -> Device -> Install -> Install Hotfix. In the case of a Firmware

install, a dialog box with the latest version of the firmware pre-selected will appear. 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. 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, WPA2 Enterprise (password) and WPA2 Enterprise (Certificate). We do NOT recommend the insecure choices of None or WEP. You must enter your WiFi Access Point SSID and a password which must be at least 8 characters long (maximum of 63 characters) If you are unsure of your Wireless access point SSID you can scan for the SSID using a Mobile Phone set to WiFi mode. You may need to reboot to enable WiFi mode

The screenshot displays the ThinLinX Management Software interface. At the top, there is a menu bar with 'File', 'Device', 'Tools', and 'Help'. Below the menu is a toolbar with icons for Discover, Name, Mode, Display, Reboot, Zone, Upgrade, Network, Peripherals, Firewall, Upload, Download, and Storage. The main area shows a table of devices:

Firmware Type	Hostname	IP Address	Mode	Firmware Ver	License Type	Support Expiry	Status
Phoenix PC							
TLX NUC32	Laptop	192.168.1.102	HDX	4.4.0	Permanent	2020-07-4	
TLX RPi	intel-sff	192.168.1.106	HDX	4.4.0	Permanent	2020-10-14	Offline
	Upstairs	192.168.1.101	HDX	4.4.0	Permanent	2020-08-30	
	Downstairs	192.168.2.5	HDX	4.4.0	Permanent	2020-03-12	

A 'Network Configuration' dialog box is open, showing settings for both Wired and Wireless interfaces. The Wired Interface is set to DHCP. The Wireless Interface is also set to DHCP, with the SSID 'belkin.130' and WPA/WPA2 Personal encryption selected. The dialog includes fields for IP Address, Netmask, Gateway, SSID, Protocol, Username, Password, DNS 1, DNS 2, and Domain Search Path. 'OK' and 'Cancel' buttons are at the bottom right.

17 Peripherals Configuration

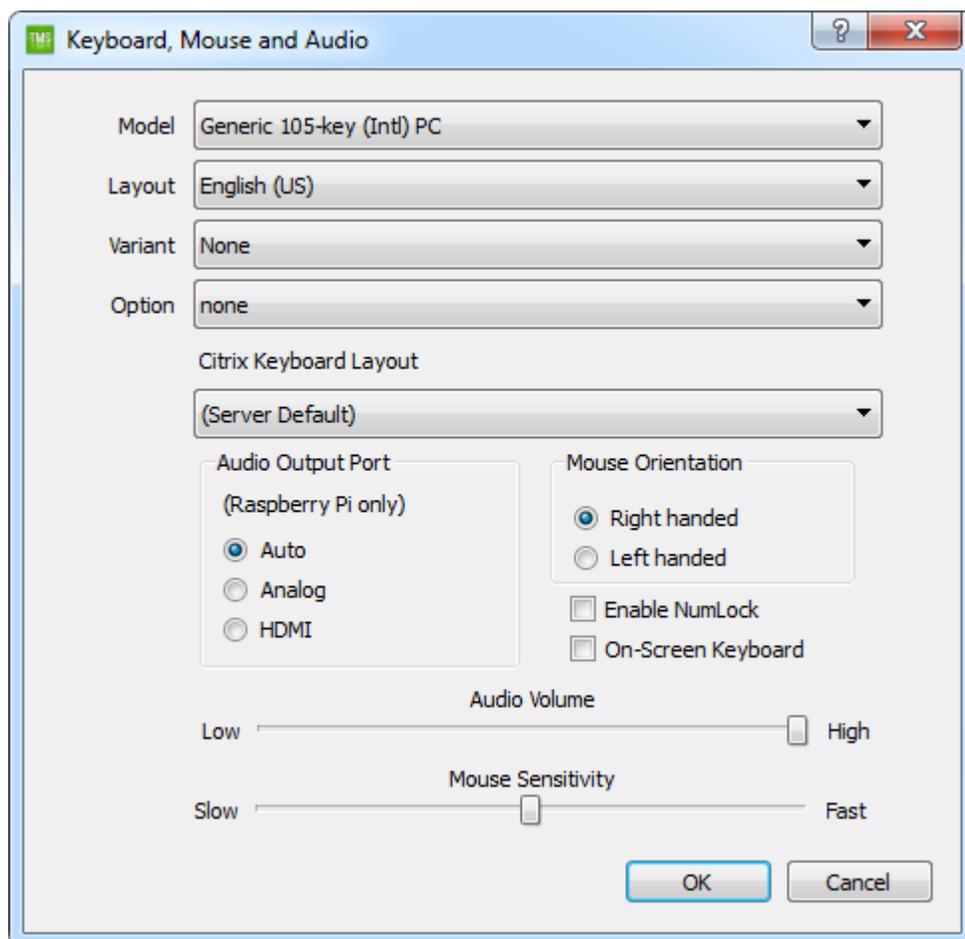
To configure your Keyboard, Mouse and Audio click on the Peripherals Icon, highlight the devices to be configured. The Citrix Keyboard Layout (Server Default) enables the configuration of the Citrix Keyboard Country at the Server side using Citrix Studio. Alternatively Citrix client side configuration can be achieved by selecting the Keyboard Country from the drop down Citrix Keyboard Layout list

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

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

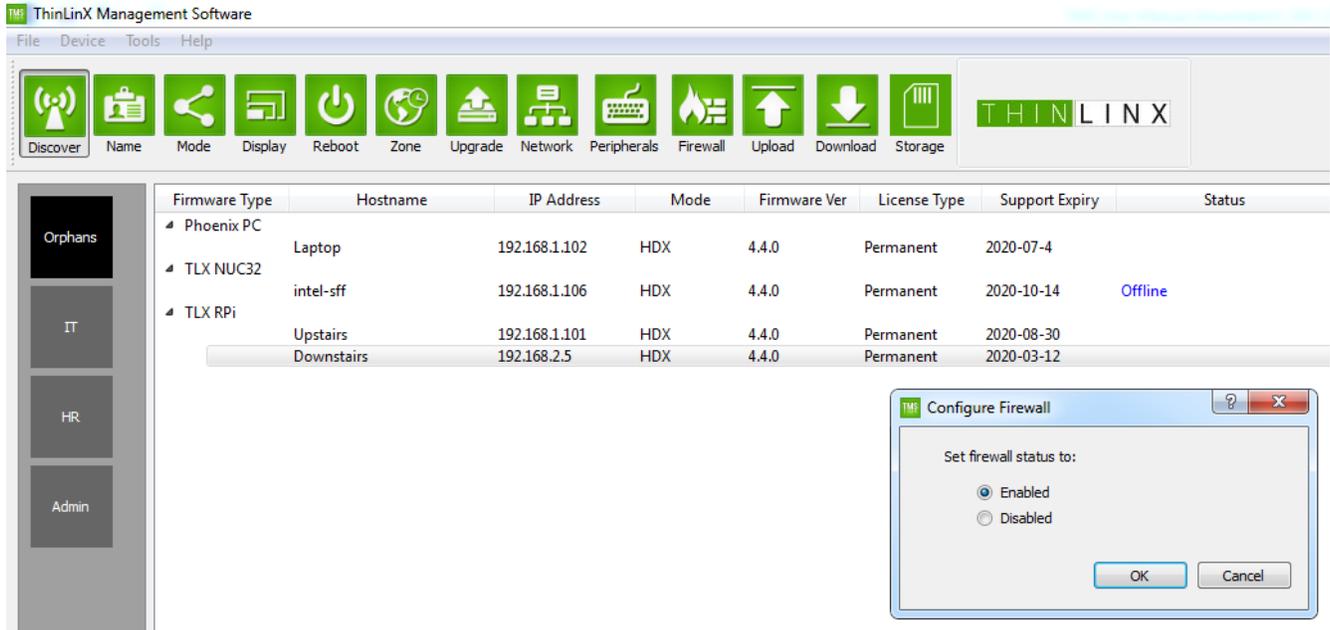
An On-Screen Keyboard can be switched on

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-v to launch the AlsaMixer dialog box where you can set USB Headphone and Microphone default Volume. (This dialog box is launched on the local Desktop before connecting to the remote session)



18 Firewall Configuration

TLXOS has a firewall enabled as the default, if you wish to switch off the device Firewall click on the Firewall Icon and select Disabled



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 image that is displayed after boot up as the background image.

- (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

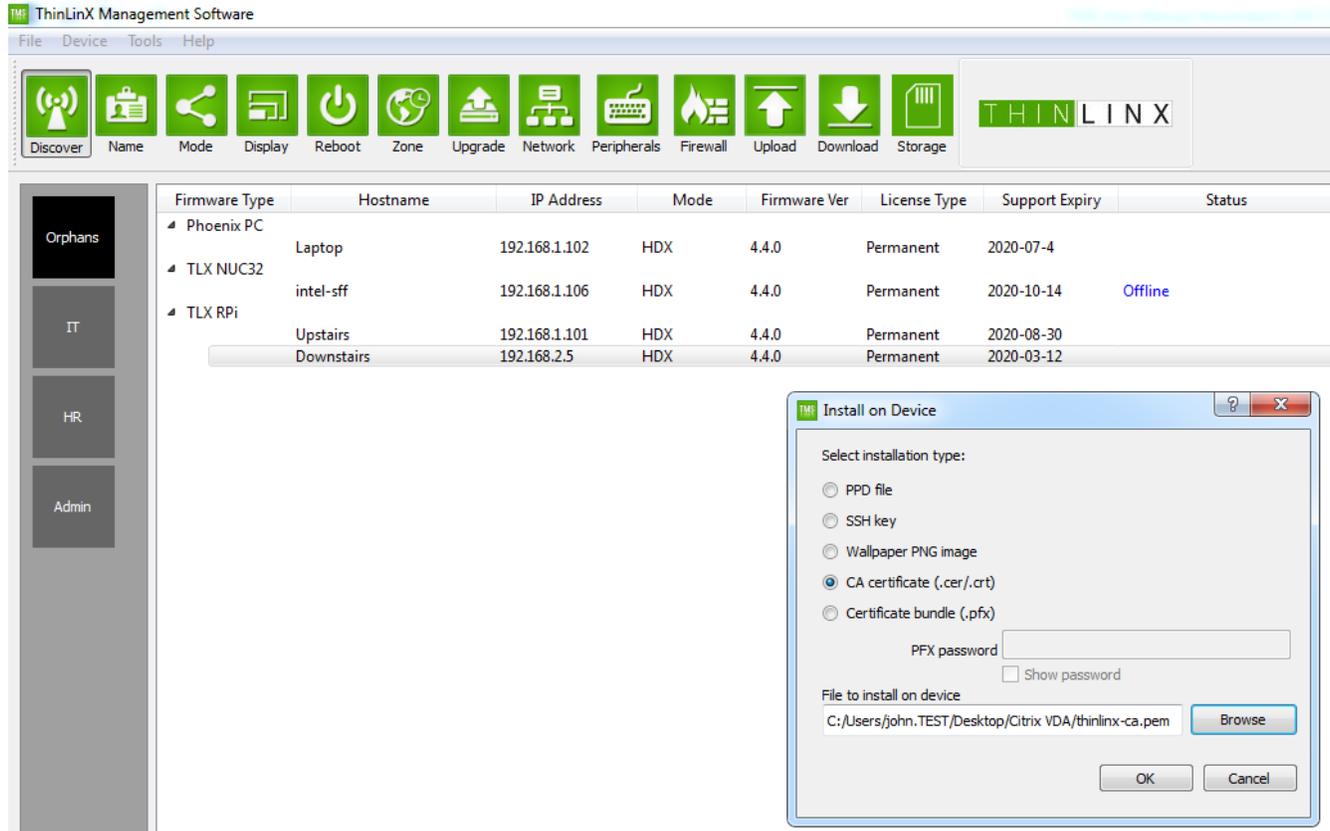
- (b) PPD file, you can upload a Printer PPD file to your device, then use the local configuration menu to select Web Browser mode, use the Web Browser CUPS Bookmark to configure a local Printer using your PPD file for a better printing experience than the built in drivers.

- (c) SSH Key, you can upload your Public SSH key to the device to obtain root access, see

FAQ on page 42

- (d) Wallpaper PNG image, upload your preferred Wallpaper using your own PNG image.
- (e) Certificate bundle (.pfx) This is used for WiFi WPA2 Enterprise (Certificate)

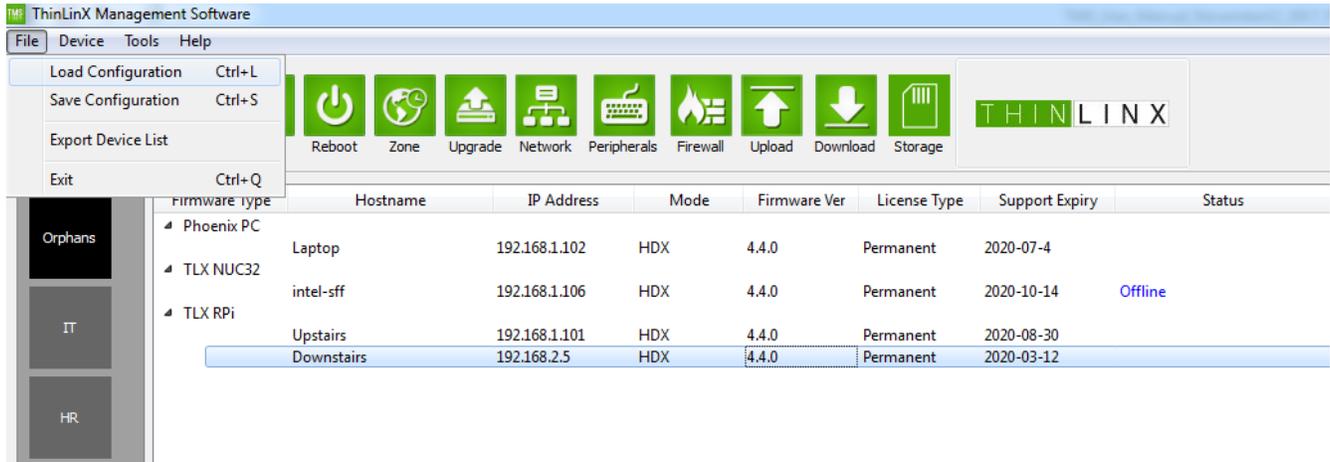
You must reboot your device to permanently save the uploaded files to the storage.



20 Storage Configuration

During TLXOS installation the device storage available is automatically detected and used for the TLXOS installation. In some rare circumstances where there may be multiple disk drives installed the Storage Icon can be used to select the Disk to install TLXOS to. This rarely needs to be used, and most likely only ever required for Re-Purpose PC installations where multiple Disk drives are fitted and it is important not to overwrite Disk drives that may still contain important Data. Please email info@thinlinx.com if you need to use this feature.

21 The File menu

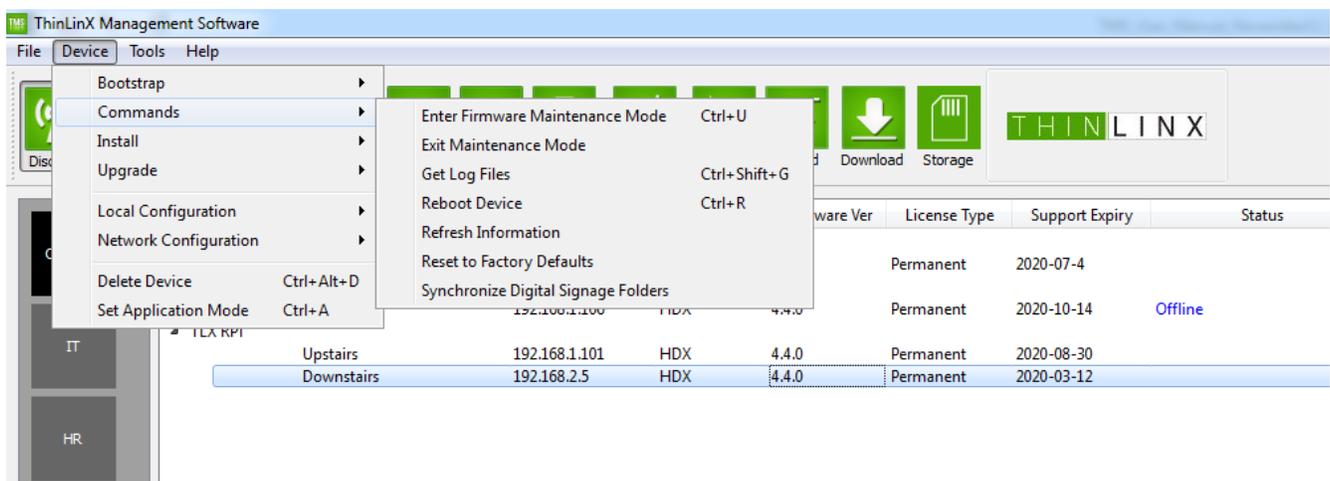


Load Configuration - Any previously saved Configuration can be copied to any Highlighted devices

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 – Please read the ThinLinX Connection user guide for information on this choice

22 The Device menu

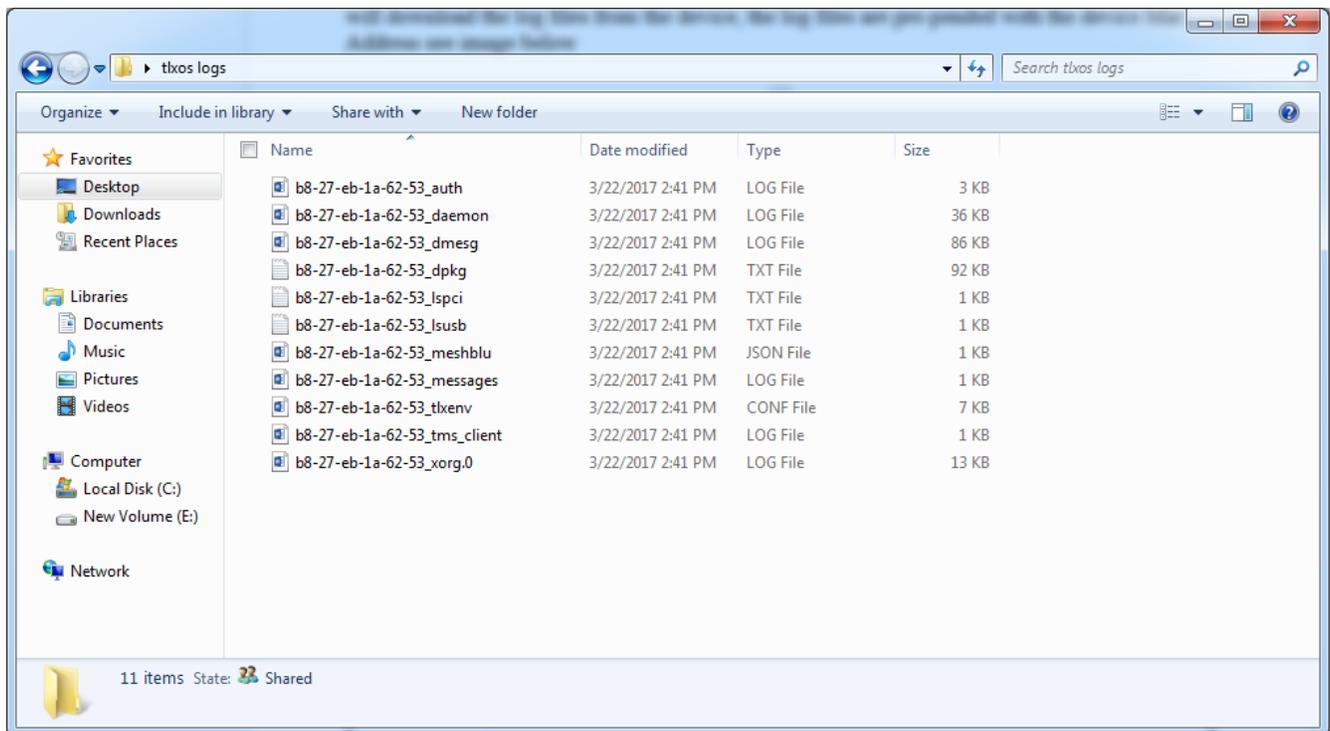


Commands

Enter Firmware Maintenance Mode – All highlighted devices will reboot into ThinLinX Firmware Maintenance mode

Exit Maintenance Mode - All highlighted devices will reboot into ThinLinX Firmware Normal mode if they have a valid License

Get Log files, this prompt for a directory to save the Log files in then will download the log files from the device, the log files are pre-pended with the device Mac Address see image below

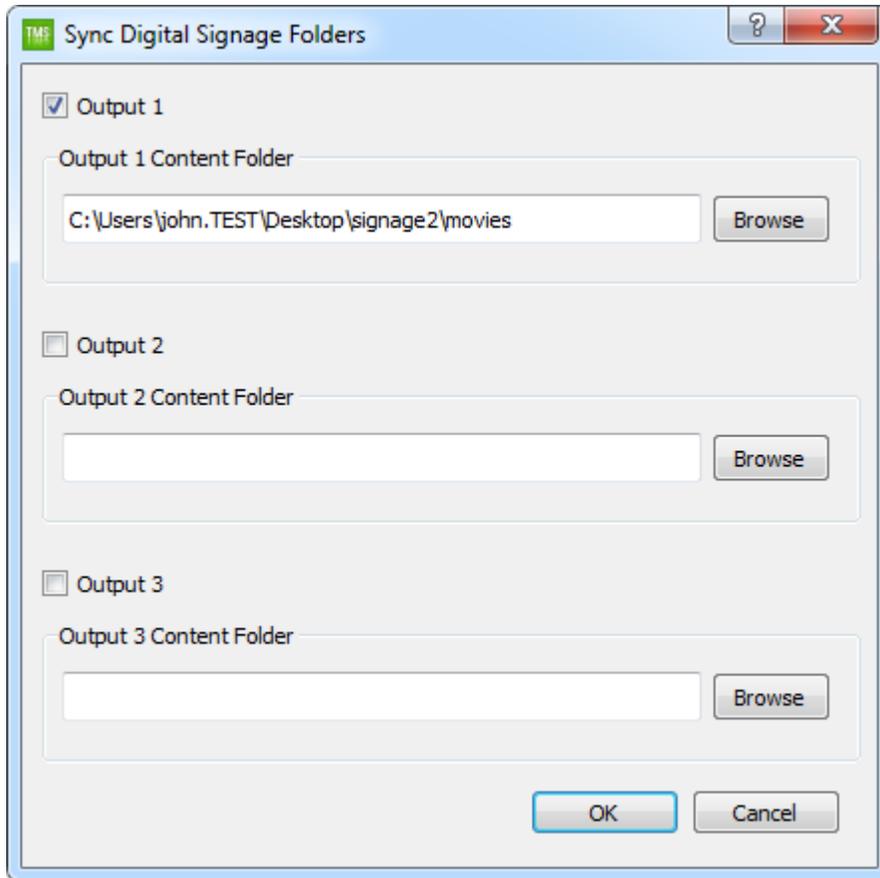


Reboot Device – Reboots all highlighted devices

Refresh Information – Reloads all TMS information from devices

Reset to Factory Defaults – All highlighted devices will be reset to Factory defaults, all configuration information is lost returning the device to a new install state.

Synchronize Digital Signage Folders - This will carry out a file sync with any Digital Signage folders that are checked, see image below. You can add or remove content to a Signage folders, then carry out a sync, this will add or remove content on the TLXOS device for that Output directory. See information below on Digital Signage configuration



One of the Protocols supported by your TLXOS device is Digital Signage for Advertising, Information, and Timetables etc. TLXOS supports up to three displays. The Digital Signage mode can play fixed Images, Videos or run a Web Browser in Kiosk mode.

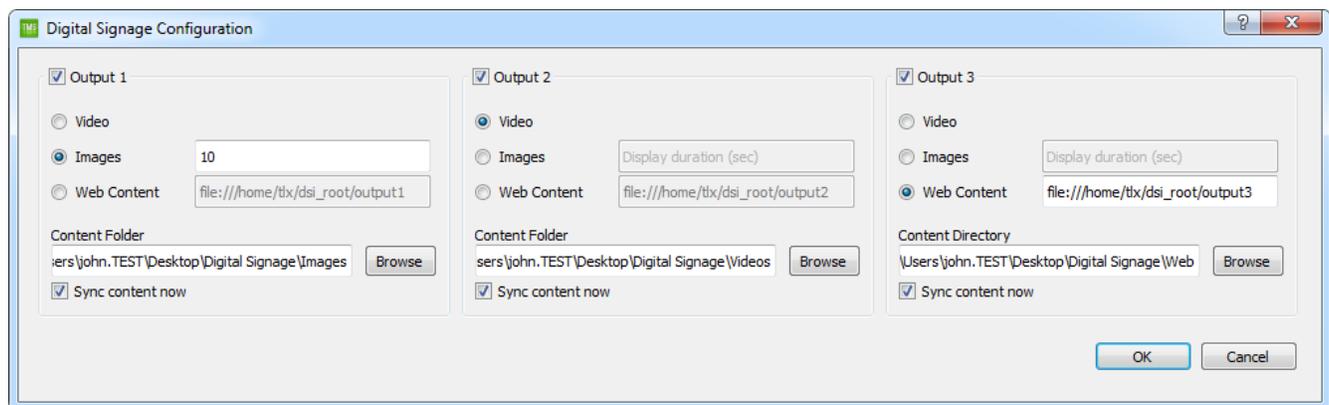
Depending on the number of Monitor Outputs on your TLXOS devices you should create up to three subdirectories on the PC running TMS, we recommend that you create a Digital Signage directory with three subdirectories named Images, Videos and Web

Copy Images to the Images directory, Videos to the Videos directory and html Web content to the Web directory. Do not mix Images, Videos or Web content in the one directory as this will lead to delays in the content being displayed as the player switches modes.

PowerPoint can be used to create amazing content which you save as a mpeg4 or .wmv file and then copy to the Videos directory using TMS

In this example we will configure Images to play on Output-1 and Videos to play on Output-2, and Website content on Output-3.

Step one is to use the TMS Mode Icon to switch your TLXOS device to Digital Signage mode, this will launch the Dialog box below. Next step is to click on the selection check box on each Output that you wish to use. In this example we have an Intel NUC that has three Video Outputs, so we select all three.



You have the same three choices on each of the three possible Outputs; Play Video, Play Images or Play Web Content.

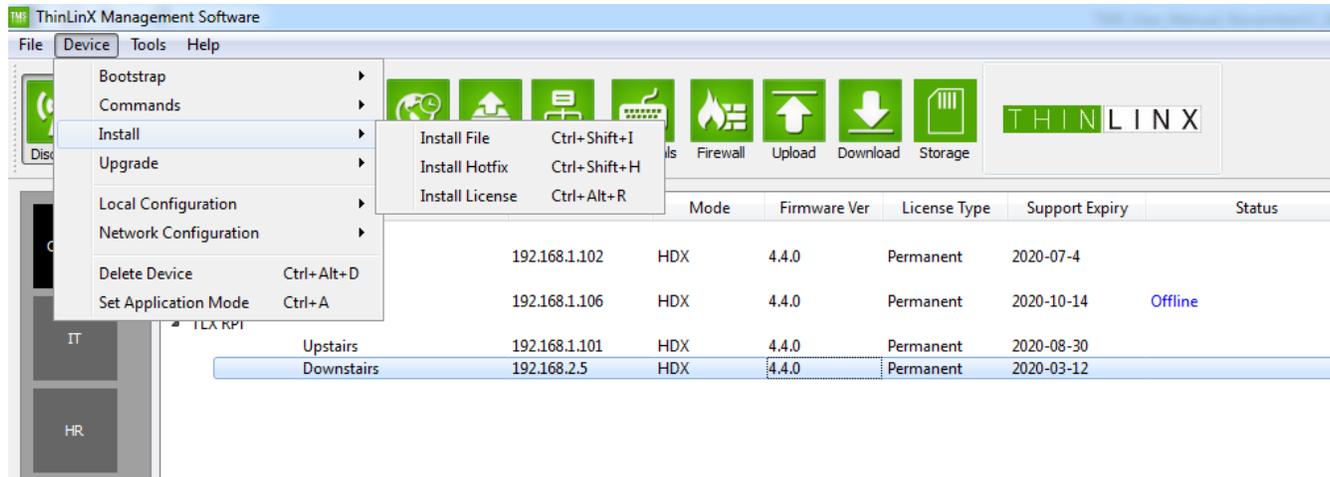
I have selected the Images checkbox on Output 1. Note that in the case of images you must also enter a time in seconds to wait before playing the next image. I have also clicked on the Browse button to enable me to select the Digital Signage directory on my PC that has images in it.

I have selected the Video checkbox on Output2. I have also clicked on the Browse button to enable me to select the Digital Signage directory on my PC that has Videos in it.

I have selected the Web checkbox on Output 3. I have also clicked on the Browse button to enable me to select the Digital Signage directory on my PC that has static Web content in it. You will note that alongside the Web Content Directory there is a text entry box pre-populated with the location of the Web Content on the TLXOS device file:///home/tlx/dsi_root/output3

Instead of using the Browse button to choose a Web content directory on my PC, I could enter a

URL in the text entry box, e.g. <http://www.thinlinx.com> which points the Web Brower to an online Website instead of the static version in the Digital Signage Web directory.

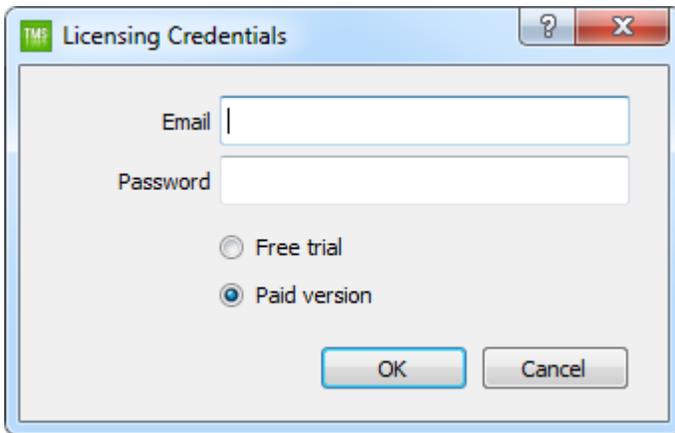


Install

Install File - this provides the same function as clicking on the Upload Icon.

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, then click on Tools -> Install -> Install Hotfix to copy the Hotfix to selected TLXOS devices

Install License – this option is used to License your TLXOS device, just enter the email address and password that you registered at the ThinLinX Online Store. You must have purchased a TLXOS License for the device type that you wish to License. Licensing takes approximately 5 seconds, the encrypted License is automatically created by the License Server and downloaded to the TLXOS device where it is stored. The License is preserved during Firmware upgrades.



The TLXOS installer attempts to automatically Register 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 register the device with the ThinLinX License Server at <https://tls.thinlinx.com> the device will boot into ThinLinX Firmware Maintenance (TFM) mode

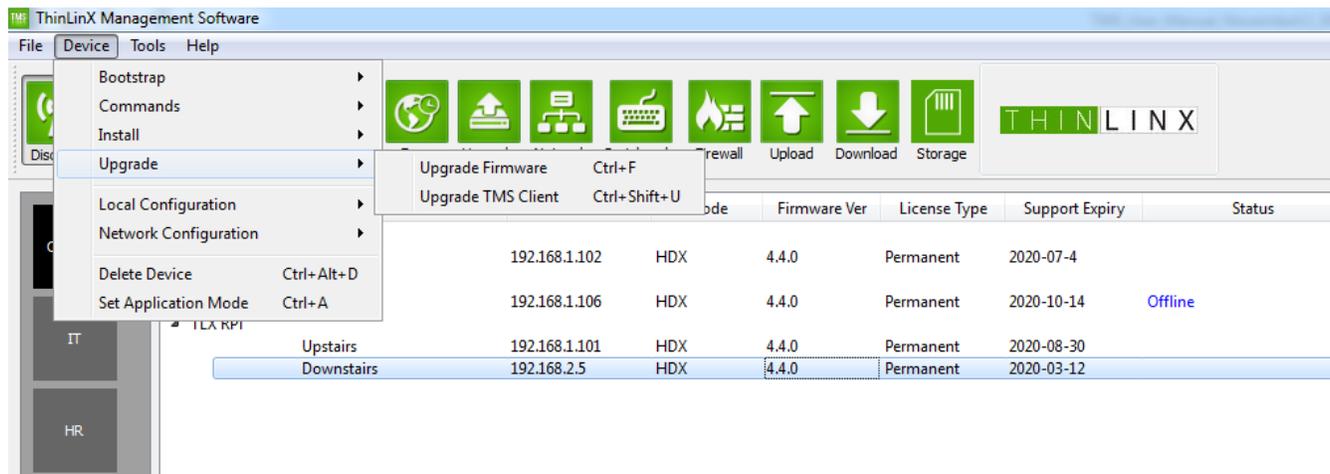
The failure to Register can be caused either the wrong date on the device or a proxy server blocking the connection. If your device boots into TFM mode due to the 30 Day Free Trial failing to register you can still use TMS -> Device -> Install License, select Free Trial to License the 30 Day Free trial. You cannot enter any information, just click on OK



If the Free Trial failed because you are behind a Proxy Server please configure TMS -> Tools -> Options to add your Proxy Server information and then try again. You can also edit the proxy.txt file on the USB stick installer or RPi SD Card installer to add your proxy server details before attempting installation

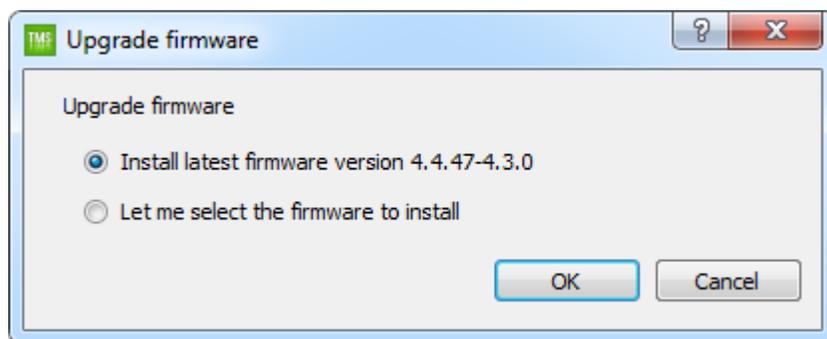
To obtain a Permanent License for a Product you must purchase a License from the ThinLinX online Store <https://tls.thinlinx.com/store/index.php/>

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

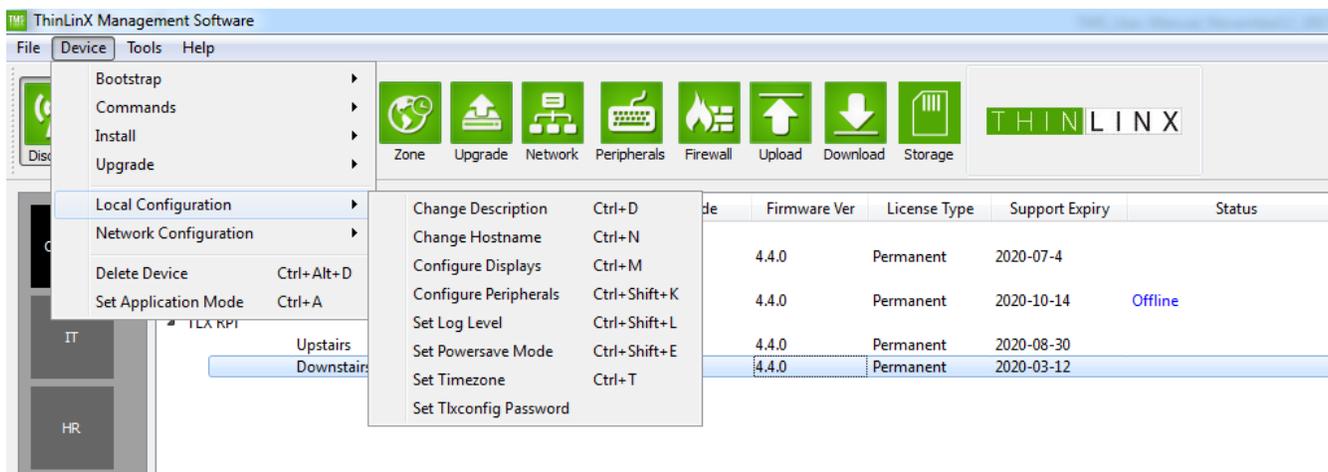
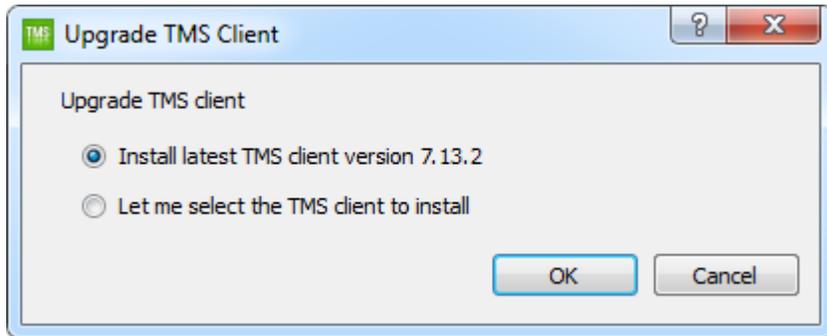


Upgrade

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 once 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



Local Configuration

Change Description – This option allows you add a description for the highlighted device, this is not related to the device Hostname that you configure using the TMS Name Icon. You can see the Device Information including the description for any device by highlighting a line and pressing enter or double clicking on a line to bring up the Device information Dialog shown below

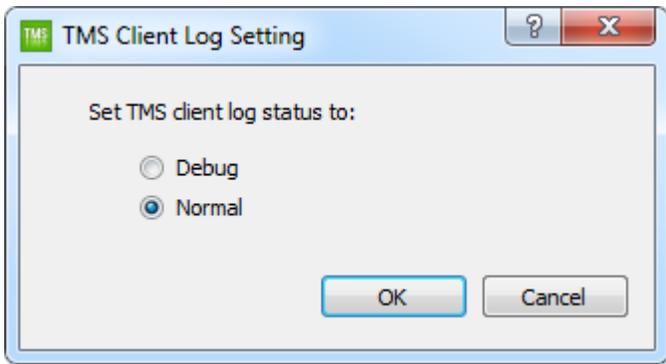
	Property	Value
1	Boot Mode	Normal Mode
2	Cmd Line Args	
3	DNS 1	
4	DNS 2	
5	Description	Set me
6	Domain Search Path	
7	Firewall Enabled	yes
8	Firmware Type	TLX RPi
9	Firmware Version	4.4.0
10	Hostname	Downstairs
11	IP Address	192.168.2.5
12	Kernel Version	4.9.33-rpi2+1
13	Keyboard Layout	us
14	Keyboard Model	pc105
15	Keyboard Option	none
16	Keyboard Variant	none

Change Hostname – This provides the same function as clicking on the TMS -> Name Icon

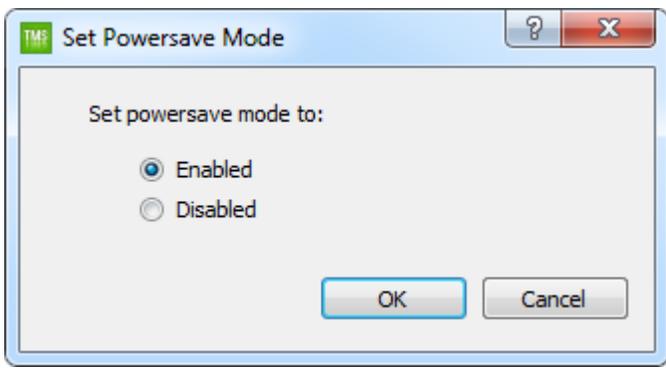
Configure Displays – This provides the same functionality as clicking on the TMS Display Icon

Configure Peripherals - This provides the same functionality as clicking on the TMS Peripherals Icon

Set Log Level – Sets log level to either Normal or Debug



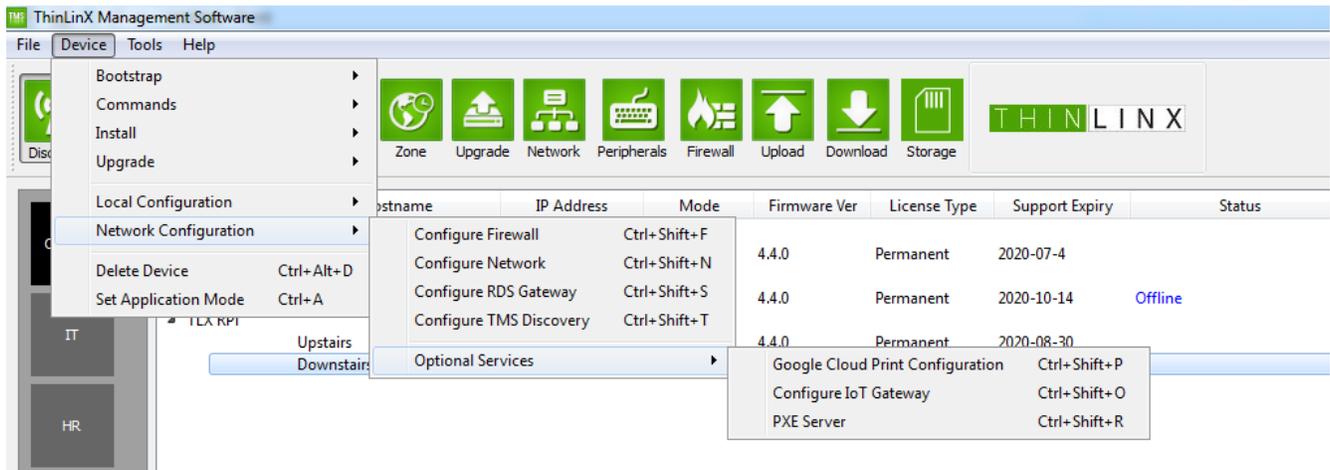
Set Powersave mode – Default is Enabled



Set Timezone – This opens the Timezone Dialog box, which can also be opened by clicking on the TMS Zone Icon

Set Tlxconfig password, this allows the setting of a password to disable access to the local TLXOS configuration menu





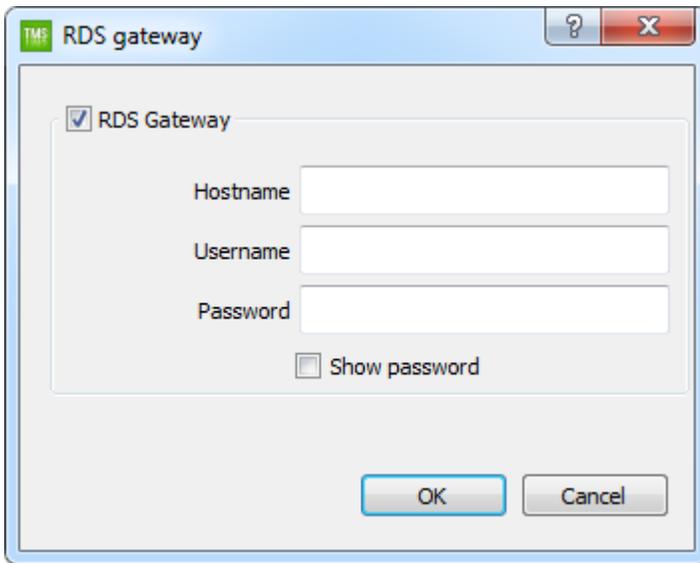
Network Configuration

Configure Firewall – TLXOS is protected by a Firewall, this is defaulted to on



Configure Network – This option opens the Network Configuration Dialog box, you can also open this by clicking on the TMS Network Icon

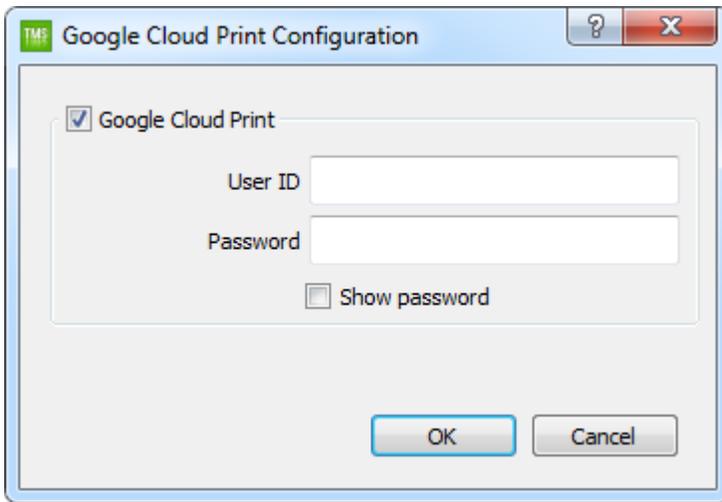
Remote Desktop Services Gateway configuration, for RDP & RemoteFX is configured via the Terminal services gateway Dialog box shown below



Configure TMS Discovery – This is explained in detail at the beginning of this user guide

Optional Services

Google Cloud Print configuration - allows your TLXOS device to act as a Google Cloud Print Server, just fill out the information below, ensure you have a Printer connected via USB or Ethernet, configure your Printer with CUPS via the local Web Browser bookmark



Configure IoT Gateway, allows the Open Source Octoblu GateBlu IoT Gateway to be switched on or off, see information on IoT configuration in the TLXOS user guide available at the link below

<https://www.thinlinx.com/tlxos-user-manual.pdf>

ThinLinX has plans to integrate other Linux IoT Gateways into TLXOS

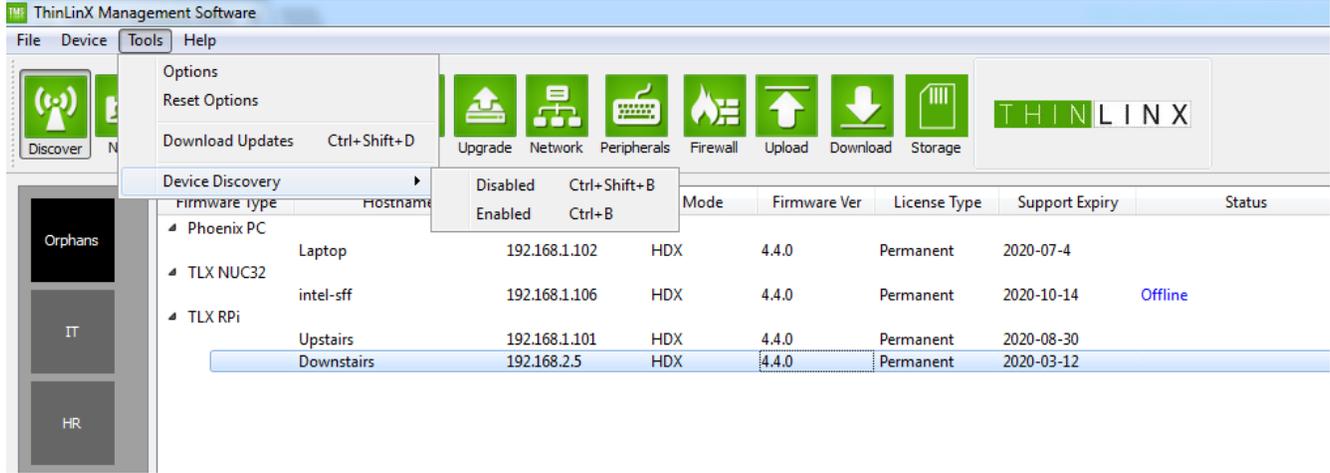


Set PXE Server configuration - is available for X86 devices only. This mode is used for Network installation of TLXOS or Diskless Booting of devices. Before you enable this mode ThinLinX recommends that you set up a separate Network using a Router, even a DSL modem with a Switch port is a good option if you do not have access to a Router.

Plug the Router / DSL Modem WAN Port into your normal Network to provide Internet connectivity which is required for Automatic Registration of the 30 Day Free trial. Plug your TLXOS X86 device being configured as a PXE Server into one of the Switch ports on the Router / DSL Modem, plug your X86 devices of the same class to be installed with TLXOS into the other Switch Ports. If you are using RePC the devices will be installed with RePC, if you are using the Intel Small Form Factor version of TLXOS, your devices must be Intel based

Configure the Network information below or use your own choice of values. Reboot the TLXOS X86 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

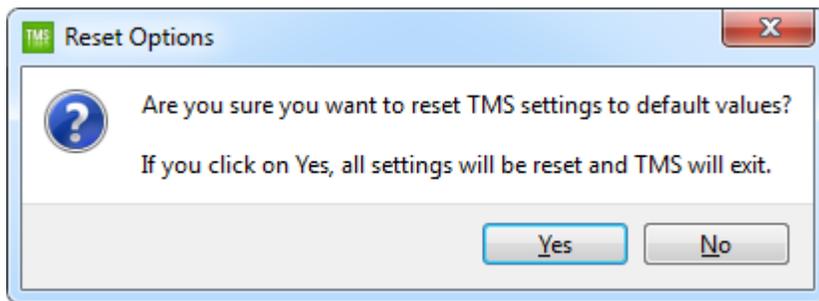
The screenshot shows a window titled "TMS PXE Server Configuration". It features a checked checkbox for "Enable PXE Server". Below this, there are four text input fields: "Subnet" (192.168.1.0), "Netmask" (255.255.255.0), "DHCP Range Start" (192.168.1.100), and "DHCP Range End" (192.168.1.199). Under the "Request Filter" section, the "Respond to PXE boot requests only" radio button is selected. Under the "Purpose" section, the "Diskless Clients" radio button is selected. The window concludes with "OK" and "Cancel" buttons.



Tools

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

Reset Options – Resets TMS Options back to defaults

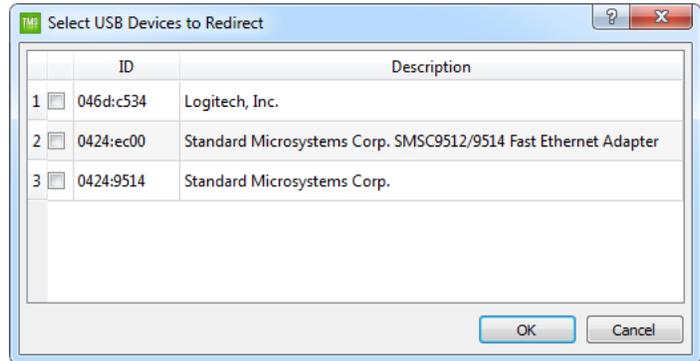
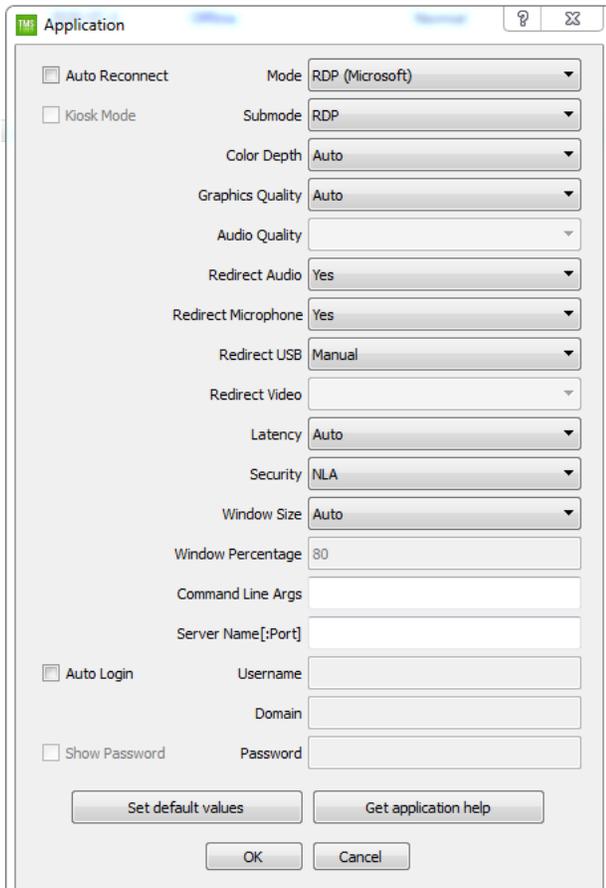


Download Updates – This opens the Download Dialog box, you can also use TMS Download Icon to launch this dialog box. This allows you to download TLXOS Firmware Upgrades, TMS Upgrades, TMS Client Upgrades and Hotfixes

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

Notes on USB Redirection – USB Redirection when using Citrix HDX or VMware Horizon does not require any TLXOS configuration but when using Microsoft RDP/RemoteFX you must configure this manually. To do this select the Mode to RemoteFX, in the image below you can see I have set Redirect USB to Manual, this will launch the “Select USB Devices to Redirect” Dialog box shown in the image below. This enables you to Redirect USB devices such as scanners etc.

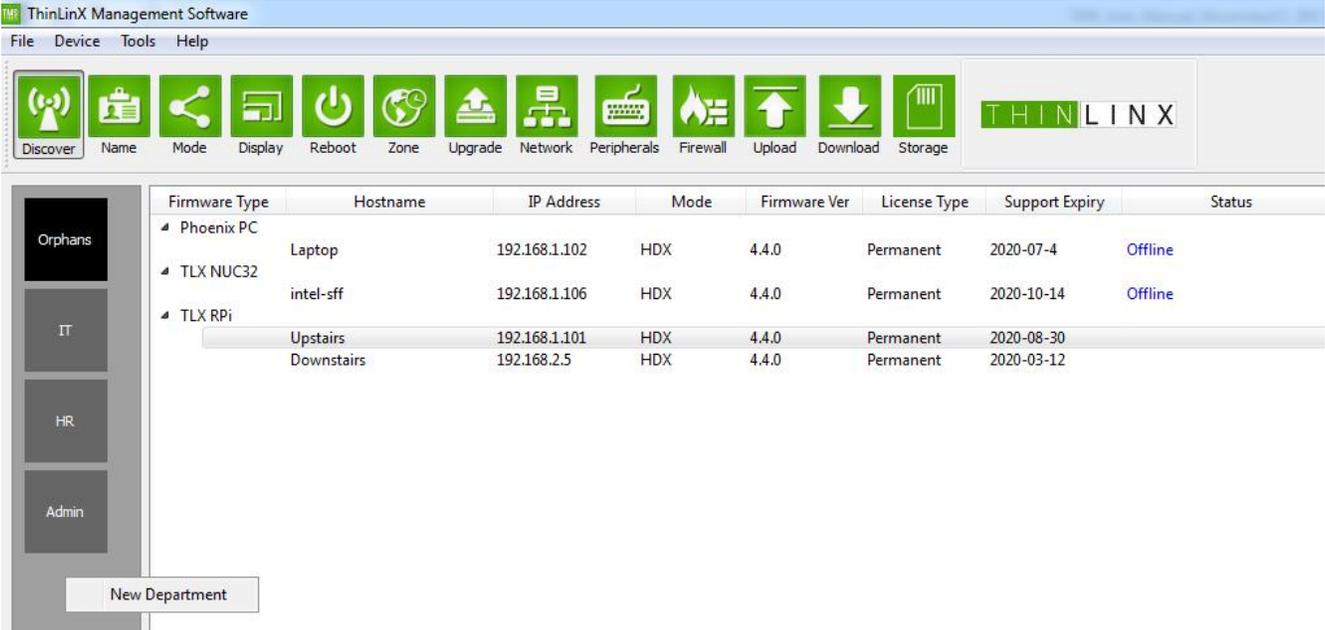
ThinLinX is considering adding a similar dialog box to Citrix HDX & VMware Horizon to allow fine tuning of devices to redirect.



23 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.

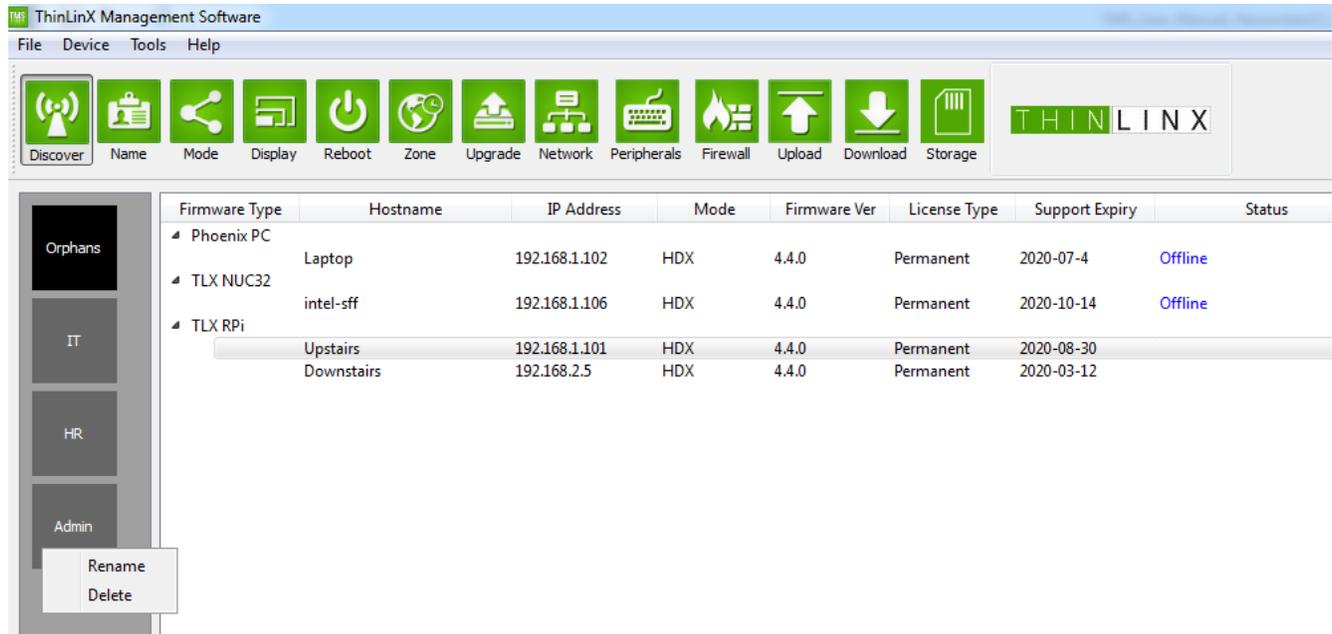
To create a new department, right click in the *Department* section on the left hand side of the UI, then click on the *New Department* pop-up, as shown below, then enter a name for the department and click on the *OK* button.



The screenshot shows the ThinLinX Management Software interface. The top menu bar includes 'File', 'Device', 'Tools', and 'Help'. Below the menu is a toolbar with icons for Discover, Name, Mode, Display, Reboot, Zone, Upgrade, Network, Peripherals, Firewall, Upload, Download, and Storage. The main area displays a table of devices with columns for Firmware Type, Hostname, IP Address, Mode, Firmware Ver, License Type, Support Expiry, and Status. The table is organized into departments: Orphans, IT, HR, and Admin. A 'New Department' button is visible at the bottom left of the interface.

Firmware Type	Hostname	IP Address	Mode	Firmware Ver	License Type	Support Expiry	Status
Phoenix PC	Laptop	192.168.1.102	HDX	4.4.0	Permanent	2020-07-4	Offline
TLX NUC32	intel-sff	192.168.1.106	HDX	4.4.0	Permanent	2020-10-14	Offline
TLX RPi	Upstairs	192.168.1.101	HDX	4.4.0	Permanent	2020-08-30	
	Downstairs	192.168.2.5	HDX	4.4.0	Permanent	2020-03-12	

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



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.

24 FAQ

Please take the time to read the following additional user guides

<https://www.thinlinx.com/tlxos-quick-start.pdf>

<https://www.thinlinx.com/tlxos-user-manual.pdf>

How do I install the 30 Day Free Trial of TLXOS for the Raspberry Pi2 or Pi3?

We offer two installation choices, the easiest installation is simply using the NOOBS bootloader SD Card which is available at the online stores that you buy the Rpi from. Boot the RPi using NOOBS while tapping the Shift key, the NOOBS bootloader will download a list of available Operating System installation choices, select TLXOS, click on Install. TLXOS will download and install onto the NOOBS SD Card, this will take about 15 minutes under normal conditions, but during periods of high download demand installation will take longer

The second option is to download our TLXOS RPi installer .exe file by clicking on the ThinLinX Website Downloads Icon and selecting “TLXOS Raspberry Pi SD Card Installer” When you double click the .exe file it runs Win32DiskImager which is designed to write a raw disk image to a removable device. To use this option you will need either a Laptop with a Micro SD Card slot or a USB to SD Card Reader. This is a better option than NOOBS if you are writing many SD Cards with TLXOS as you only download the “TLXOS Raspberry Pi SD Card Installer” once but then can use the installer to create an unlimited number of TLXOS SD Cards.

After TLXOS installation using either method above, on first boot up TLXOS will attempt to connect to the ThinLinX License Server at <https://tls.thinlinx.com> to Register the 30 Day Free trial. You must be connected to the Internet and not behind a Web Proxy for Registration to succeed. If you have a Web Proxy on your Network you can use the ThinLinX Management Software (TMS) -> Edit -> Settings to configure TMS Proxy Server settings, you then close TMS, reopen TMS and use TMS -> Tools -> Product Registration to Register your 30 Free Trial. If your RPi is in ThinLinX Firmware Maintenance (TFM) Mode due to failure to Register during installation you must use TMS -> Tools -> Product Registration to Register it, then use TMS -> Tools -> Exit Maintenance Mode to return to Normal Mode.

The first TLXOS boot will take a minute or more as TLXOS also runs the apt-get update command to download package lists from the repositories and "updates" them to get information on the newest versions of packages and their dependencies.

How do I install the TLXOS 30 Day Free Trial for Intel Small Form Factor devices?

Download our TLXOS ISFF installer .exe file by clicking on the ThinLinX Website Downloads Icon and selecting “TLXOS Intel Small Form Factor USB Stick Installer” When you run the .exe it launches

Win32DiskImager which is designed to write a raw disk image to a removable device. Insert a USB Stick into the PC, double click on the .exe file, this will unpack the TLXOS image and then write it to the USB Stick.

You can use a single USB Stick installer to write TLXOS to the local storage on an unlimited number of Intel devices such as Intel NUC's / Compute sticks etc. To save the cost of an internal Disk Drive, if your Intel NUC has a SD Card slot you can insert a SD Card as the NUC storage device. Insert the USB stick TLXOS installer, boot up while tapping F10, the installer will boot up in ThinLinX Firmware Maintenance (TFM) Mode Blue screen, a 10 second countdown will commence, press a key to stop the countdown, then use the cursor down arrow to select the second choice (Re) Install TLXOS (Warning: DESTRUCTIVE) Press Enter, a second screen will appear where you can select the default boot up Mode, press Enter. The storage device will be auto detected and TLXOS will be written from the USB Stick installer to the Storage device

After TLXOS installation, on first boot up TLXOS will attempt to connect to the ThinLinX License Server at <https://tls.thinlinx.com> to Register the 30 Day Free trial. You must be connected to the Internet and not behind a Web Proxy for Registration to succeed. If you have a Web Proxy on your Network you can use the ThinLinX Management Software (TMS) -> Edit -> Settings to configure TMS Proxy Server settings, you then close TMS, reopen TMS and use TMS -> Tools -> Product Registration to Register your 30 Day Free Trial. If your Intel device is in Firmware Maintenance (TFM) Mode due to failure to Register during installation you must use TMS -> Tools -> Product Registration to Register it, then use TMS -> Tools -> Exit Maintenance Mode to return to Normal mode

The first TLXOS boot will take a minute or more as TLXOS also runs the apt-get update command to download package lists from the repositories and "updates" them to get information on the newest versions of packages and their dependencies.

How do I install the TLXOS 30 Day Free Trial for Re-Purposing PC's and Laptops?

Download our RePC installer .exe file or RePC ISO CD Rom image by clicking on the ThinLinX Website Downloads Icon and selecting either "TLXOS Generic X86 RePC USB Stick Installer" or "TLXOS Generic X86 RePC Installer CD ISO version"

If you boot a PC or Laptop with the CD Rom Installer inserted in many cases the CD will auto run the TLXOS Installer, in some cases you may have to press either F10 or F12 to select boot from CD.

In the case of the USB Stick installer, when you run the .exe it launches Win32DiskImager which is designed to write a raw disk image to a removable device. Insert a USB Stick into the PC, double click on the .exe file, this will unpack the TLXOS image and then write it to the USB Stick. You can use a single USB Stick installer or CD Rom Installer to write TLXOS to the local storage on an unlimited number of PC's or Laptops. Insert the CD ROM or the USB stick TLXOS installer, boot up while tapping F10, the installer will boot up in the ThinLinX Firmware Maintenance (TFM) Mode Blue screen, a 10 second countdown will commence, press a key to stop the countdown, then use the cursor down arrow to select the second choice (Re) Install TLXOS (Warning: DESTRUCTIVE) Press Enter, a second screen will appear where you can select the default boot up Mode, press Enter. The storage device will be auto detected and TLXOS will be written from the CD ROM or USB Stick installer to the onboard Storage device.

In some cases you may have multiple Hard Disk drives in an older PC or Laptop and may wish to write TLXOS to the Hard drive of your choice instead of allowing the Installer to auto detect the Hard Disk drive to be used for installation. If this is the case in your situation do not interrupt the Installer at the ThinLinX Firmware Maintenance (TFM) Mode Blue screen, allow the 10 second countdown to continue as this will accept the default choice of Upgrade / Recover TLXOS In this case you must wait for the installer to display the message, "Waiting for a Whitelisted Storage device", then use the ThinLinX Management Software (TMS) / Storage Icon to obtain a list of the available Disk Drives. Uncheck the default "Let clients choose appropriate device" and then select the check box next to the Hard Drive of you choice. Click OK and the TLXOS image will be written to your selected device.

After TLXOS installation, on first boot up TLXOS will attempt to connect to the ThinLinX License Server at <https://tls.thinlinx.com> to Register the 30 Day Free trial. You must be connected to the Internet and not behind a Web Proxy for Registration to succeed. If you have a Web Proxy on your Network you can use the ThinLinX Management Software (TMS) -> Edit -> Settings to configure TMS Proxy Server settings, you then close TMS, reopen TMS and use TMS -> Tools -> Product Registration to Register your 30 Day Free Trial. If your RePC device is in Firmware Maintenance (TFM) Mode due to failure to Register during installation you must use TMS -> Tools -> Product Registration to Register it, then use TMS -> Tools -> Exit Maintenance Mode to return to Normal mode. The first TLXOS boot will take a minute or more as TLXOS also runs the apt-get update command to download package lists from the repositories and "updates" them to get information on the newest versions of packages and their dependencies.

How do I configure TLXOS Citrix HDX mode to auto connect and auto login?

Firstly set the time zone using the TMS Zone Icon, this must be set to the same time zone as the Citrix Server

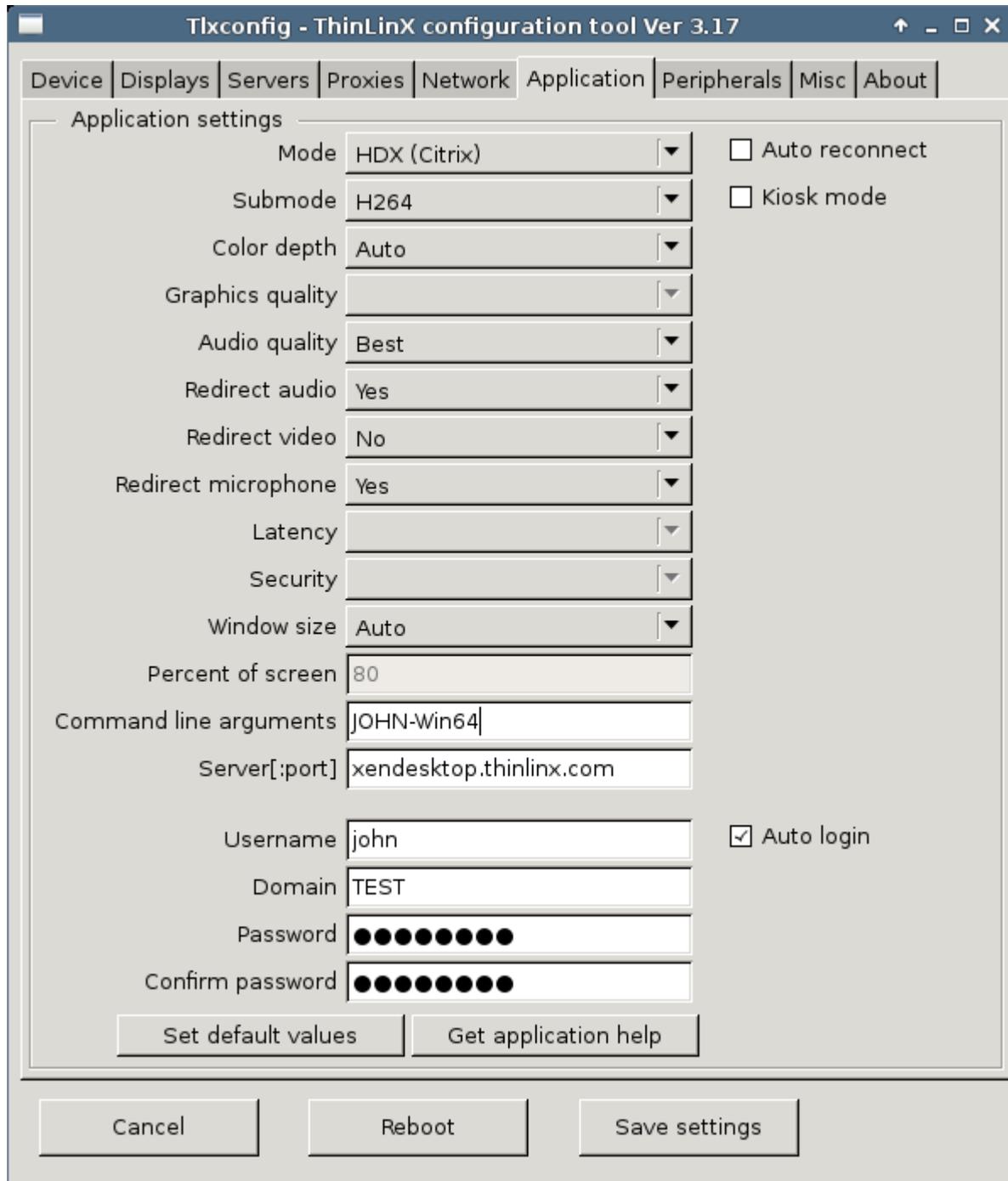
Use TMS to upload the client end SSL Certificate to the TLXOS devices by selecting the check boxes next to their names, then click on the Upload Icon, select CA Certificate (.cer), and browse to the Directory with the SSL certificate Certificates can be exported in either DER (binary) or PEM (ASCII) 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, ensure you rename your exported (ASCII) certificate with a .pem extension. After the Certificate is installed click on the TMS Reboot Icon to permanently save the certificate to the device's storage.

Use TMS Protocol Icon to select HDX mode put your StoreFront server name (must be the FQDN as exactly it appears in the server's SSL certificate!) in TMS' "Hostname[:Port]" box, your logon credentials in the TMS autologin boxes, and (optionally) the name of any application or desktop you want to automatically launch in the "Cmd line arguments" box. The application/desktop name is just the human readable label as it appears in StoreFront or the web UI, and you don't have to quote it if it contains spaces.

Reboot, The RPi will connect and Log into the Storefront, you will see all your authorised Apps and Desktops, or if you have added the App or Desktop name in the Cmd line arguments box the App or Desktop will auto launch

Ensure that you enabled http basic authentication on the storefront servers

See an example image below which is the configuration to use to auto launch and auto login into a HDX Windows Desktop named JOHN-WIN64



I am using NetScaler and cannot connect in HDX mode but Web mode works

Are you using a Netscaler gateway via HTTPS, with the back end HDX servers on your internal network using HTTP? Have your Windows Receiver clients been registry hacked to allow insecure HTTP StoreFront stores? If so, you should be aware that there is **no way** to perform an equivalent hack on Linux Receiver (we have asked Citrix to consider adding this). It is therefore essential that **both** the Netscaler gateway **and** the StoreFront server are configured to use HTTPS, and that the client is able to validate both (has all necessary CA certificates installed). Web mode has no such restriction, which is why it works for you in Web mode but not HDX.

When I attempt to register devices using TMS I get an error "SSL handshake error All product registration requests have been cancelled"

Some versions of Windows are missing the SSL Certificate that TMS needs, you can fix this easily by using Internet Explorer to connect to the ThinLinX License Server at <https://tls.thinlinx.com> Windows will download and install the missing SSL Certificate, close TMS, reopen TMS and now you will be able to register your RPIs

The ThinLinX Management Software (TMS) does not discover my TLXOS device, how can I fix this problem?

On some versions of Windows some dll files required by TMS are missing TMServer.exe uses the DLL msvcrt100.dll and srvcli.dll which are both in the folder "C:\Windows\SysWOW64\" These DLLs are most likely missing if you don't have "Microsoft Visual C++ 2010 SP1 Redistributable Package (x86)" installed. Downloaded it from here

<https://www.microsoft.com/en-us/download/details.aspx?id=8328>

TMS still can't discover the client

Press Control ALT and t Lower case t for terminal This will open an xterm, enter /sbin/ifconfig to see the IP ADDRESS and ping whatever you like. TMS in installation mode uses UDP broadcast, check your Firewall on the Server, also check that the date is correct by opening an xterm with Ctrl-Alt-t and entering date

What do I do if my USB Keyboard and Mouse do not work on the Intel NUC

This problem is easily fixed, just boot the NUC while pressing F2 to enter the BIOS, select USB Legacy to on. Depending on the version of the BIOS in your NUC you may have to select USB XHCI to Off. Save the BIOS changes, reboot the NUC

HOWTO set up your Printers

USB Locally connected Printers are easy if you are using Citrix or RemoteFX...In the case of Citrix plug the Printer into the NUC, boot the NUC and connect to the Remote Desktop, the Printer will be detected and the drivers will be installed. In some cases Windows won't be able to find the drivers in which case you will need to go the Printer Manufacturers Website, download and install the Drivers. In the case of RemoteFX, boot the NUC with the Printer attached and then use the ThinLinX Management Software (TMS) to redirect the printer using TMS -> Tools -> Setup USB Redirection. Select the checkbox next to the Printer and then reboot the NUC to save the configuration. Connect to your Remote Desktop the Printer will be detected and the drivers will be installed. In some cases Windows won't be able to find the drivers in which case you will need to go the Printer Manufacturers Website, download and install the Drivers.

In the case of a USB Printer using standard RDP or a Network Printer you must configure CUPS on the NUC to enable the remote system to see the Printer. Just select Web Mode to launch Chrome and then click on the Configure printers Bookmark at the top left. Chrome will connect to the Local CUPS Server running on TLXOS Please Google CUPS (Common Unix Printing System) for the fine print on how to set up CUPS printing. For the best results when you set up your local printer you should consider providing the Windows PPD file instead of using the closest Linux Printer Driver. This is particularly important for Multi Function Printers where no Linux PPD driver exists Once you have the Windows PPD file extracted from your Windows installation Disk you can use TMS to copy the PPD file to your TLXOS device. To copy the PPD file use TMS -> Upload -> select PPD file.

When you configure CUPS, select this PPD file, reboot the TLXOS device to save the PPD file to flash. You can also configure a Printer using CUPS as a RAW printer where the Server Printer Driver does all the work before sending the Raw data to the Printer.

In the case of Citrix and Network Printers, install the drivers as per <https://support.citrix.com/article/CTX140208> (note that you have to click the button to get updated driver from Windows Update before these models appear in the list, and that it can take Windows a very long time to virus scan the drivers when you click add (and it doesn't tell you it's doing this)

I can't install TLXOS

The most likely cause is that you removed the USB stick too early, you should wait until the installer prompt for its removal at the appropriate time.

How do I get out of fullscreen mode?

It depends on what mode you're in: HDX: shift-f2. Allegedly. RDP and RemoteFX: control-alt-enter. This will release pointer grab, but the FreeRDP window will still intercept keystrokes while the window is in focus. Spice: shift-f11 (and then shift-f12 to ungrab the keyboard and pointer). VNC: control-alt-shift-f, or use f8 to bring up the configuration menu and click on Full Screen to toggle it off. X11: you can't, but you can use control-shift to toggle key grab between local and remote window managers. This will allow you to use local keyboard shortcuts such windows-d to show the desktop, control-alt to switch windows and so forth. Everything else: there is no fullscreen mode, you just have a window that's been sized to fit the current screen resolution. You can use normal window manager controls to resize or minimize it.

I tried changing resolution but now my screen is black / my monitor says "scan rate out of range". I don't have TMS / can't get someone else to change settings using TMS. What can I do?

Use the appropriate key sequence to exit from fullscreen mode for whichever protocol you are currently using (see "How do I get out of fullscreen mode", above), and then press the control-alt-r key combination twice within two seconds. This will cause your client to reset to a safe default resolution (1024x768) and reboot.

Is there a way to bring up the configuration tool other than from the dialog window that comes up after a session has ended? I don't want to close my application right now.

Yes. First exit fullscreen or defocus your fullscreen application (see "How do I get out of fullscreen mode", above) and then use the control-alt-c key combination.

My thin client can't connect to anything and the configuration tool says that it has no IP address. What can I do?

Unplug the network cable, wait at least six seconds, and then plug in back in again. This will reset the interface and trigger a new DHCP request.

Can I share my display with another person (for training or troubleshooting purposes)?

Yes. RDP and HDX (ICA) protocols have their own session shadowing features – which may or may not work with our client implementations – but TLXOS also has a VNC server capability that you can use. To initiate a shadow connection, first exit fullscreen or defocus your fullscreen application (see "How do I get out of fullscreen mode", above), and then press control-alt-s and enter the hostname or IP address and TCP port number of the shadower in the window that appears. You have the option of either connecting to a listening VNC client over an SSL connection (active mode), or setting up a TCP port forward via an SSH tunnel and awaiting a connection (passive mode). Active mode has the

advantage of using ordinary HTTPS and being able to use a web proxy, which makes it suitable for highly secure environments that don't permit direct connection to the Internet. Passive mode has the advantage of also providing an SSH port forward, allowing SSH as well as VNC access from the remote SSH endpoint. Unlike typical VNC servers, both modes of operation "dial out" to a remote server, which permits traversal of firewalls and NAT gateways and implicitly ensures operator consent. For active mode, the shadowing system must be running stunnel (www.stunnel.org) redirecting to a VNC client application in listen mode (we recommend TurboVNC - www.virtualgl.org). Use of SSL is mandatory. For passive mode, the shadowing system must be running an SSH server that accepts publickey authentication and permits port forwarding, and has a user with a `~/.ssh/authorized_keys` file that contains TLXOS' SSH host public keys. A thin client using TLXOS can do both these things, and can therefore be used to shadow sessions on another TLXOS thin client.

What is TLXADM?

TLXADM is a Virtual Appliance (VA) developed by ThinLinX which has our Linux version of TMS pre-installed and also a built in Desktop Shadower which is described above. TLXADM is a ~700MB download and runs on Citrix XenServer, Microsoft Hyper-V, VMware, Oracle VirtualBox, Linux KVM

Once installed you can use any device running Citrix Receiver or RDP to display the TLXADM Desktop, this allows you to administer TLXOS devices from anywhere in the World, also to see and interact with their Desktops before they log into a Windows session and to ssh as the Root user to the TLXOS device being shadowed. The shadowed session has to be initiated by the user of the remote TLXOS device.

<https://www.youtube.com/watch?v=aWI3BB898GI&t=2s>

Please email info@thinlinx.com for download instructions for the Beta version of TLXADM

The web browser / Citrix / whatever says that the server SSL certificate is not trusted, but I'm sure that I have installed the correct CA certificate. What's wrong?

It's likely that your thin client's local clock is wrong. To verify this, you can start a terminal using control-alt-t and then enter "date" in the window that appears. This happens because the RPi has no battery-backed clock, so unless it can contact a network time server from which to get the current date and time, it will revert to a nonsensical value such as the year 2000 or 2027 whenever its power is reset. By default, it will try to contact Internet time servers, which may not succeed if there is an intervening firewall or if hostname lookups are failing. To fix the problem, use TMS or the local configuration tool to set the time server to the name or IP address of a local NTP server that the client will be able to connect to. Typically this would be the same as the local DNS server (if it is an Active Directory domain controller) or default gateway (if it is a router appliance).

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

The O/S has been tightly locked down to help prevent thin clients from being used as an attack vector against servers. Although SSH is installed, it does not support password authentication, and in any case none of the accounts on the system – including root – have password hashes; they are all locked accounts. The only way you can get root access is to SSH in as root using a trusted key. By default, only public keys belonging to ThinLinX developers are listed in /root/.ssh/authorized_keys, but it is possible to use TMS to install more via the TMS Upload Icon -> SSH Key. The public key that you upload must be in OpenSSH format. On Windows platforms, PuTTYgen (part of the PuTTY suite - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>) can be used to display the public key of a PPK file in OpenSSH format (copy and paste from the text box at the top – do not use the Save Public Key button, as creates keys in a non-OpenSSH format).

Requirements: TMS, PuTTYgen, PuTTY for Windows Devices. RPi with TLXOS installed and ready.

PuTTY is an SSH client for Windows that you will use to generate your SSH keys. You can download PuTTY from www.chiark.greenend.org.uk.

When you install the PuTTY client, you also install the PuTTYgen utility. PuTTYgen is what you will use to generate your SSH key for a Windows VM.

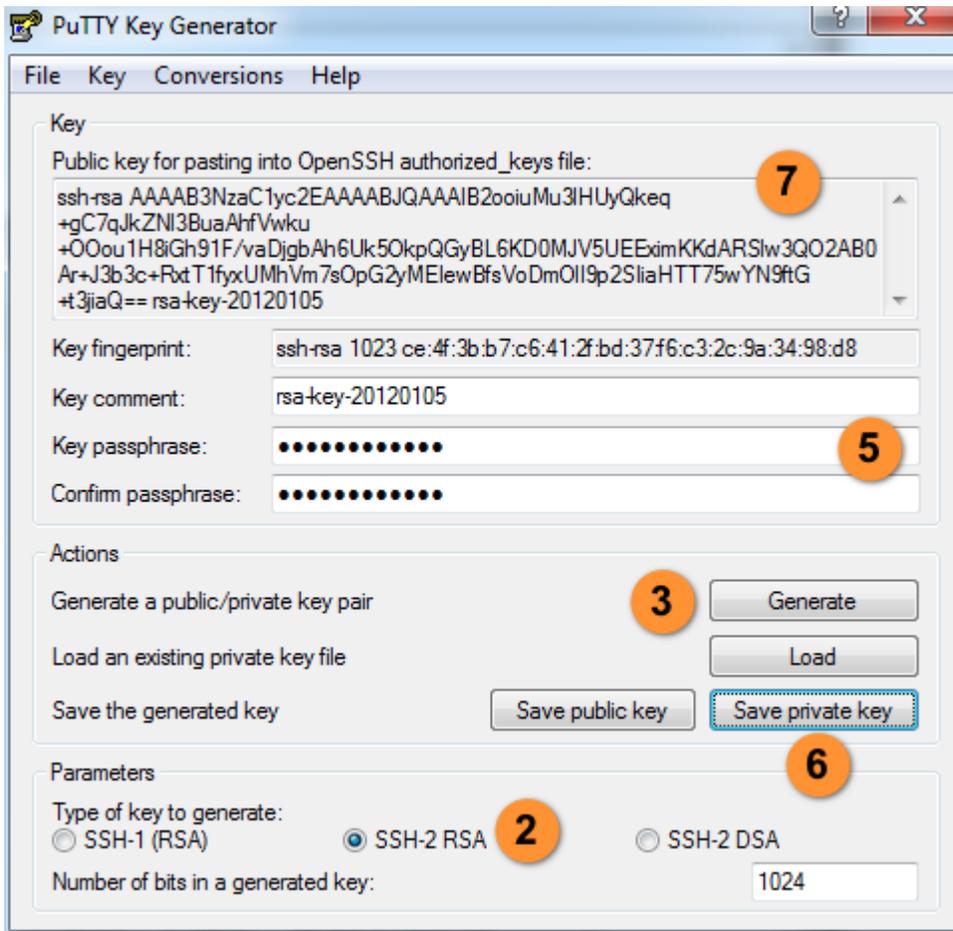


This page gives you basic information about using PuTTY and PuTTYgen to log in to your provisioned machine. For more information on PuTTY, see the [PuTTY documentation](#)

1. [Generating an SSH key](#)

To generate an SSH key with PuTTYgen, follow these steps:

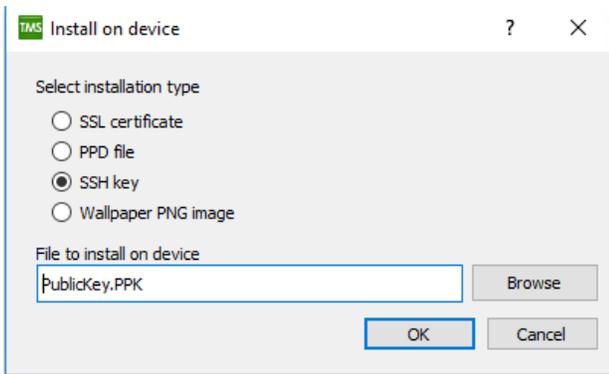
2. Open the PuTTYgen program.
3. For **Type of key to generate**, select **SSH-2 RSA**.
4. Click the **Generate** button.
5. Move your mouse in the area below the progress bar. When the progress bar is full, PuTTYgen generates your key pair.
6. Type a passphrase in the **Key passphrase** field. Type the same passphrase in the **Confirm passphrase** field. You can use a key without a passphrase, but this is not recommended.
7. Click the **Save private key** button to save the private key. You **must** save the private key. You will need it to connect to your machine.
8. Right-click in the text field labeled **Public key for pasting into OpenSSH authorized_keys file** and choose **Select All**.
9. Right-click again in the same text field and choose **Copy**.



10. Create a new text file (ex. Publickey.txt) and **Paste** the information into that text file.
11. Rename that file PPK extension (ex. Publickey.PPK) *Note:* this is file you will upload to the RPi with TLXOS.
12. Open the TMS manager
13. Locate and select the devices you want to upload the public key to.

Device name	Status	IP address
▼ TLX RPi <input checked="" type="checkbox"/> Set me		192.168.1.109

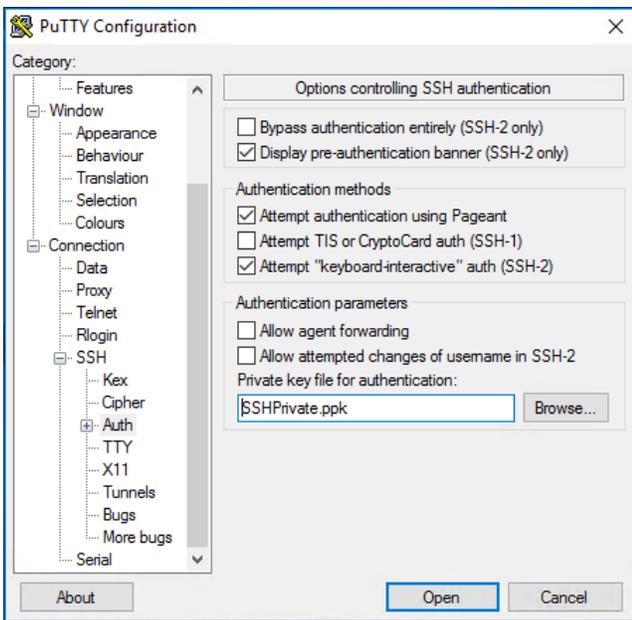
14. Click on **Upload** from menu bar.
15. Select: **SSH Key** and location the public key then Click **OK**



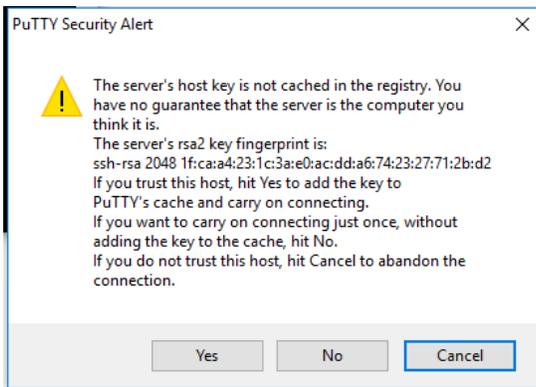
You will get a confirmation that the key has been up loaded successfully.

Once this is completed you will need Putty with the private key to get Root Access to the device.

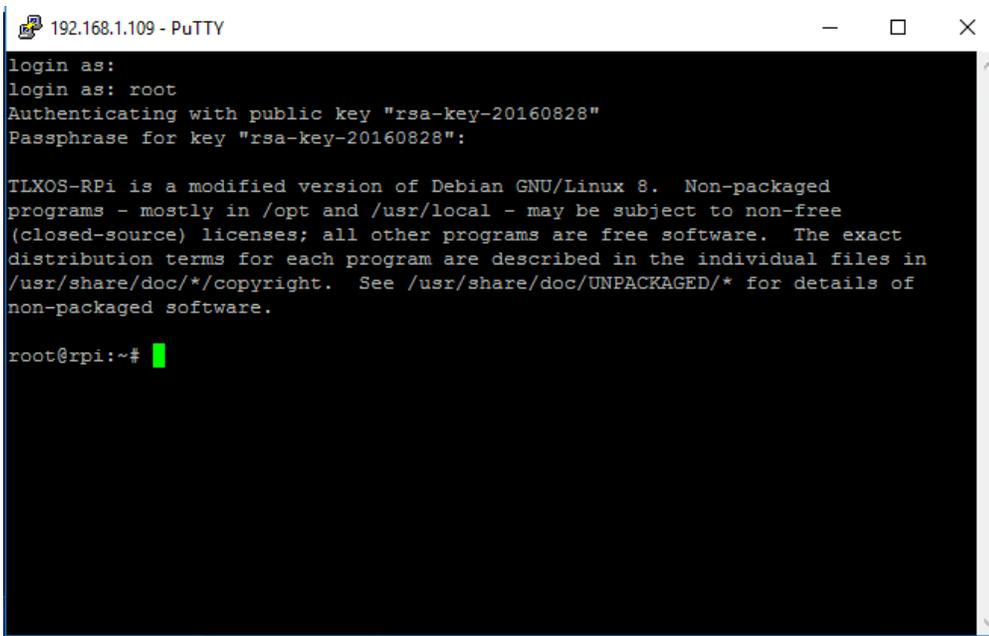
1. **Open** Putty
2. *Session*> *Host Name (or IP Address):* **X.X.X.X**
3. *SSH*>*Auth*> *Private key file or Authentication:* (Click on **Browser**) locate the Private PPK file



4. Click on **Open**
5. Click on Yes



6. Type **root** <Enter>; Passcode: **** <Enter>



You are now logged in as *root*.

How do I pair a Bluetooth Device?

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

© 2017 ThinLinX Pty Ltd All rights reserved.

Information in this manual is protected by copyright laws and is the intellectual property of ThinLinX Pty Ltd No changes may be made to this manual without the written consent of ThinLinX Pty Ltd No part of this manual may be copied, reproduced, translated or published in any form or by any means without prior written permission from ThinLinX Pty Ltd