

ViewSonic[®]



SC-T25 / SC-T36

ViewSonic Device Manager 3.0

User Guide

Contents

1.	Introduction.....	1
2.	VDM3.0 on Windows installation.....	1
3.	Starting VDM3.0	1
4.	Configuring VDM3.0	2
5.	Basic VTOS device configuration	4
6.	Basic VTOS device configuration via VDM3.0	5
7.	Assigning a name to a VTOS device	7
8.	Setting the Remote Server and Connection Protocol.....	7
9.	Setting the client protocol experience level	11
10.	Setting screen resolution.....	12
11.	Rebooting a VTOS Device.....	14
12.	Setting the timezone and time server	14
13.	Downloading firmware updates for VTOS Devices	16
14.	Network Configuration	18
15.	Keyboard Configuration	19
16.	Firewall Configuration	19
17.	Upload Files to your devices.....	20
18.	Storage & Wizard Configuration.....	21
19.	The Tools menu	21
20.	Displaying detailed VTOS device information.....	28
21.	Sorting VDM3.0 Clients into departments.....	29

1. Introduction

Viewsonic Device Manager 3.0 (VDM3.0) provides the ability to configure and manage Viewsonic's SC-T25, SC-T36 Thin Clients, and repurposed PC products. VDM3.0 can be used for a variety of tasks, ranging from something as simple as rebooting a VTOS device, to upgrading the device with the latest VTOS software. VDM3.0 runs on Windows and Linux.

A Linux version of VDM3.0 is integrated into VTOS, this can be enabled by changing the VTOS Protocol to VDM3.0.

2. VDM3.0 on Windows installation

VDM3.0 ships as a downloadable self-executable. The same executable runs on both 32 and 64 bit versions of Windows. To install VDM3.0, download the .exe installer file onto your Windows system, double click the downloaded file and follow the instructions.

To uninstall VDM3.0 on Windows, click;

Start > All Programs > Viewsonic > Uninstall ViewSonic Device Manager

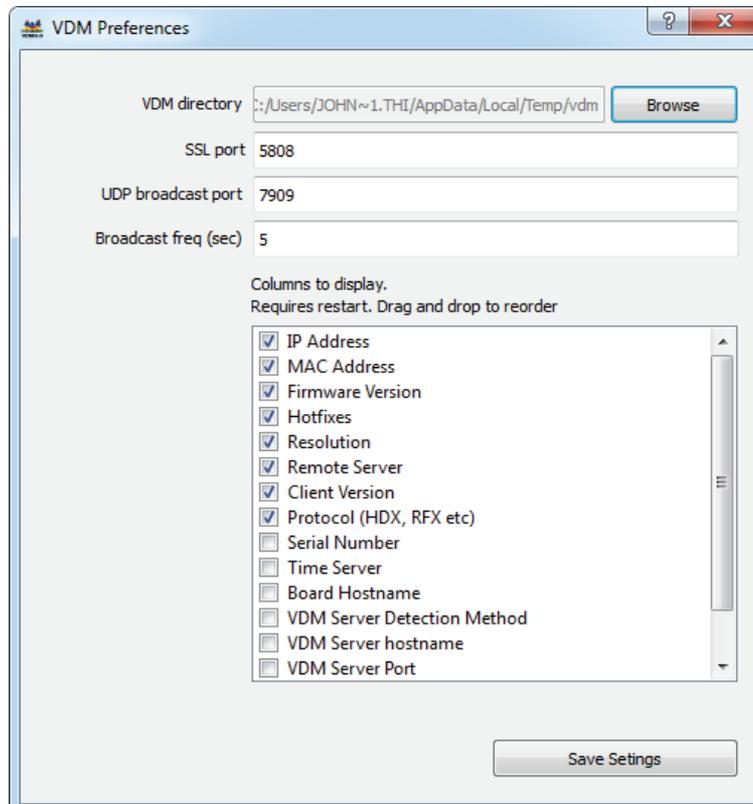
3. Starting VDM3.0

On Windows start VDM3.0 by double clicking on the desktop shortcut

4. Configuring VDM3.0

VDM3.0 is automatically configured during installation, the recommended procedure is to accept the default installation directory. The first time VDM3.0 is run on a system, the configuration dialog appears. Any time after installation you can manually launch the configuration dialog if required by clicking on Edit > Settings.

The configuration dialog box is shown below



VDM3.0 directory denotes where VDM3.0 will store client images, firmware updates and temporary data such as log files downloaded from VDM3.0 Clients and department configuration files.

See image below displaying the five subdirectories that are created when VDM3.0 is installed.

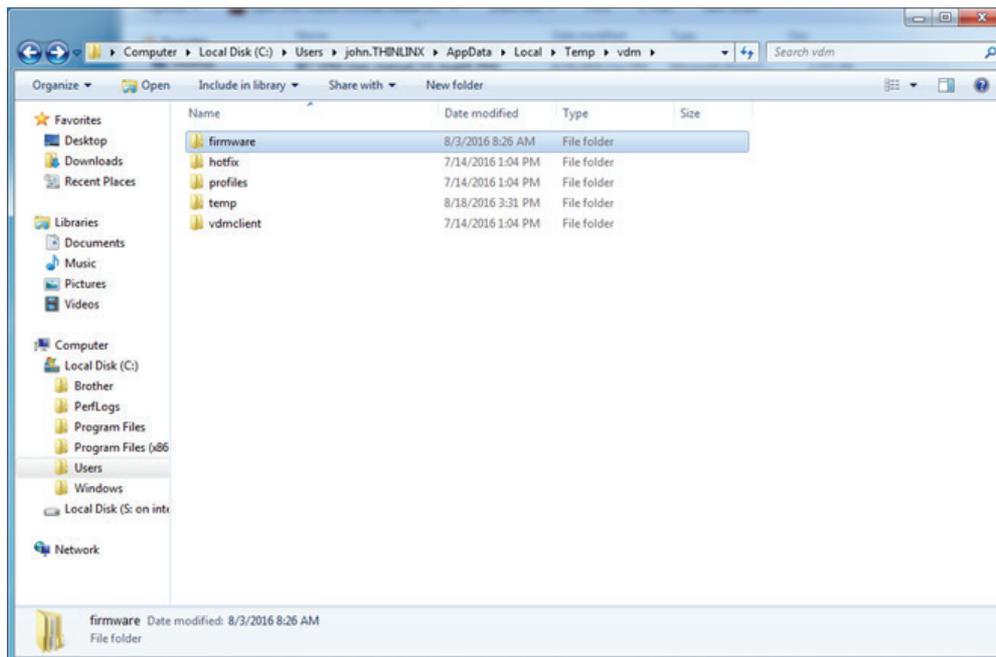
All firmware images downloaded via the VDM3.0 Download Icon for any VTOS device are automatically stored in the firmware directory.

All hotfixes are stored in the hotfix directory, these are also downloaded using the VDM3.0 Download Icon.

The profile directory is used for storing profiles that are created with VDM3.0 and then deployed to one or more devices, this feature is still under development.

The temp directory is used to store log files

The vdmclient directory is used to store updated version of the VDM3.0 client, these are downloaded using the VDM3.0 Download Icon



SSL Port denotes the SSL port number that will be used by VDM3.0. By default all communications between VDM3.0 and VTOS devices are SSL encrypted. The connection between the VTOS client and VDM3.0 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 5808. If you change this port number, you need to close VDM3.0 and restart it. If you are running VDM3.0 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 VDM3.0 to send broadcast packets to VDM3.0 Clients and is used for initial communication. The default port number is 7909 and should not be changed unless the port conflicts with existing network traffic.

Broadcast frequency defines how often VDM3.0 transmits a UDP broadcast packet. This packet contains the VDM3.0 Hostname and Port number, the default value is 5 seconds.

Columns to Display allows for custom fields to be displayed within the VDM3.0 device discovery frame. This includes the removal or addition of fields and the ability to reorder the fields in top to bottom preference order.

If you make any changes to the above settings, you must restart VDM3.0 to allow the new settings to take effect.

5. Basic VTOS device configuration

Some basic configuration must be performed on a VTOS device before it can be deployed. This involves setting each VTOS device to the desired Remote server IP Address, and setting the VDM3.0 server connection Protocol option.

There are two ways to do this, via VDM3.0 or via vendor specific DHCP options (also known as site specific DHCP options). When vendor specific DHCP options are used, VDM3.0 Clients automatically connect to a nominated VDM3.0 server.

The following vendor specific DHCP options are supported by VDM3.0 Clients;

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

Option name	Code number in decimal	Data type
tlx-tms-ip-address	231	text
tlx-tms-ssl-port	232	text
tlx-remote-server	233	text
tlx-connection-type	234	text

tlx-tms-ip-address specifies the IP address of the VDM3.0 server on the network. When a VTOS device detects this setting, it will attempt to automatically connect to a VDM3.0 server at this IP address on port number specified by option **tlx-tms-ssl-port**. When option **tlx-tms-ip-address** is specified, you must also specify option **tlx-tms-ssl-port**.

tlx-tms-ssl-port specifies the SSL port on which the VDM3.0 server is listening. This setting must match the SSL Port setting in VDM3.0 preferences, otherwise VTOS devices will be unable to connect to the VDM3.0 server.

tlx-remote-server specifies the host name or IP address that VTOS devices should connect to.

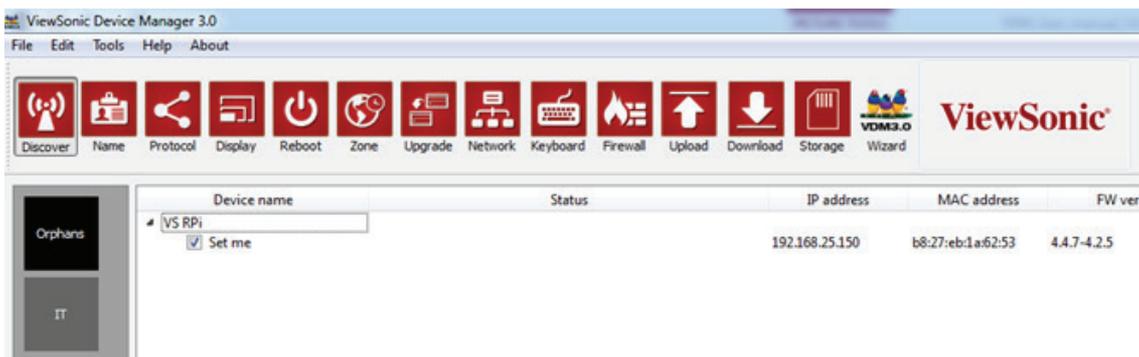
tlx-connection-type specifies the protocol that VDM3.0 Clients should use to connect to the remote server. Possible values are HDX, RFX, RDP, VNC, X11, WEB and VMW.

6. Basic VTOS device configuration via VDM3.0

When vendor specific DHCP options or Static assignment are not used, a VTOS device will not have enough information to connect to a VDM3.0 server. Therefore it listens for UDP broadcasts that contain the VDM3.0 server information. When it receives this broadcast, it extracts the information and connects to a VDM3.0 server over SSL. Thereafter, all communication between VDM3.0 server and a VTOS device is secured.

You can configure the UDP broadcast frequency using VDM3.0 Edit / Settings

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



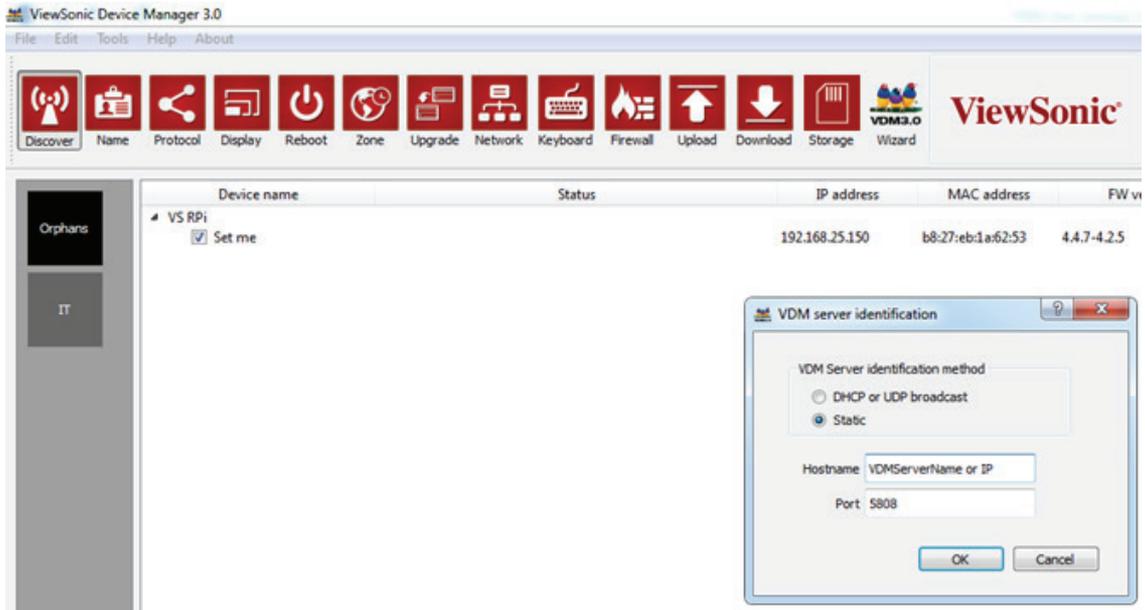
The default setting is UDP discovery turned on. When VDM3.0 is launched this commences the VDM3.0 server packet broadcast via UDP to all VTOS Clients. Once acknowledged, the VTOS device(s) then connect to the VDM3.0 server and display/populate under the VDM3.0 client area with an empty check mark box next to each client.

Selecting this check box allows the Administrator to send commands to the nominated VTOS device(s). This also allows for more than one VTOS device to be selected and sent commands at the same time.

Note: Highlighting a Device line by clicking on the line does NOT select the device, you must click in the selection box next to each client, a tick will appear in the selection box when a device has been selected

If UDP discovery is being used do NOT run more than one instance of VDM3.0 on the same Network Subnet as the VTOS clients will connect to the first instance of VDM3.0 that they receive UDP packets from. As they are already connected to VDM3.0 they will NOT appear on the second instance. In some circumstances some VTOS devices will be connected to one instance of VDM3.0 and others will be connected to the second instance. The Golden rule is to only run one instance of VDM3.0 when UDP Discovery is used.

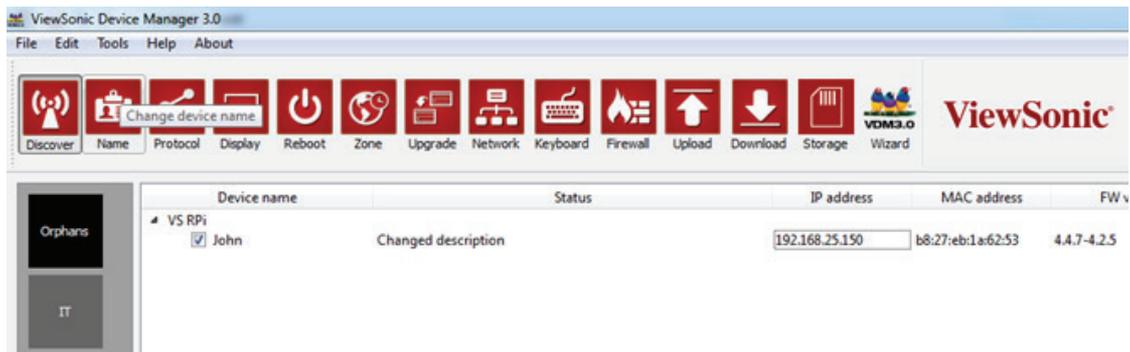
VDM3.0 and VTOS devices must be on the same network subnet for UDP Broadcast discovery of VTOS devices to be successful. If the VTOS devices are to be located on a different Network subnet or in a Branch Office then DHCP Discovery must be used or alternatively the VDM3.0 Hostname or IP Address and Port number must be specified using VDM3.0 / Tools / Configuration / VDM3.0 Server configuration, select Static in the Dialog Box, then enter the Hostname or IP Address and the Port number of the PC running VDM3.0. If a different Port number than the default 5808 is chosen you must also set the same Port number on VDM3.0 via the Edit Settings Dialog Box. See figure 1.2 below.



7. Assigning a name to a VTOS device

VDM3.0 allows the renaming of VTOS devices to more descriptive names in the interest of better identification on the network. This allows administrators to set device names in line with their Company policy. Note: Changing the Device name does NOT change the Device Hostname, this only changes the descriptive name on VDM3.0. Automatically changing the Hostname to the same name as the descriptive name is planned in a future release of VDM3.0

To assign a name of a VTOS Device, select the check box alongside “Set me”, then click on the Name Icon as shown below;



8. Setting the Remote Server and Connection Protocol

When a VTOS device boots, if configured correctly it will automatically connect to a Remote Server using the specified connection Protocol. Depending on the device running VTOS up to 16 different connection types 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
- b. RemoteFX, launches a connection to a Microsoft RemoteFX VDI Desktop, please ensure you set the default Security level to NLA
- c. RDP, launches a standard RDP (non VDI) connection to a Desktop, please ensure you set the default Security level to NLA
- d. VNC, Launches Turbo VNC Viewer
- e. X11, launches a X11 client to connect to a Linux Desktop using XDMCP
- f. Spice, launches a Red Hat Spice Protocol client
- g. NoMachineNX, launches a NoMachine 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 Cmd line arguments box on the Web mode Dialog box
- i. Viewsonic Connection Manager, see connection Manager documentation
- j. Telnet, launches a Telnet client
- k. Tn3270, launches the Tn3270 IBM Mainframe client
- l. VMware View, launches the VMware Horizon client
- m. Performance monitor, launches nmon <http://nmon.sourceforge.net/pmwiki.php>
- n. VDM3.0, Launches the Linux version of VDM3.0
- o. Digital Signage, changes the mode to Digital Signage, play Images, Video, Web Content
- p. Media Player, launches the SMPLayer Media Player

Connection types	SC-T36	SC-T25
Citrix HDX	v	v
RemoteFX	v	x
RDP	v	x
VNC	v	v
X11	v	v
Spice	v	x
NoMachine NX	v	x
Web	v	v
ViewSonic Connection Manager	v	x
Telnet	v	x
Tn3270	v	x
VMWare View	v	x
Performance monitor	v	v
VDM3.0	v	v
Digital signage	v	x
Media Player	v	x

v - Support / x - Not support

All the above connection types have various levels of configuration available via the individual Protocol configuration Dialog Box.

The hostname for a remote server can be configured via VDM3.0. To configure the remote server, select one or more VTOS Devices then click on the Protocol Icon. Web mode is shown below configured as Kiosk mode to automatically launch a Citrix HDX session by connecting to a Citrix Storefront;

The screenshot shows a dialog box titled "Access protocol" with the following configuration options:

- Connect using: Web (dropdown)
- Color depth: (dropdown)
- Graphics quality: (dropdown)
- Audio quality: (dropdown)
- Redirect audio: (dropdown)
- Redirect video: (dropdown)
- Redirect mic: (dropdown)
- Enable kiosk mode
- Window size: Auto (dropdown)
- Window percentage: 80 (text input)
- Cmd line arguments: xendesk.myserver.com/Citrix/StoreWeb (text input)
- Hostname[:port]: 0.0.0.0 (text input)
- Auto reconnect
- Auto login
- Domain: (text input)
- Username: (text input)
- Password: (text input)
- Confirm password: (text input)

Buttons at the bottom: "Set default values", "Get remote protocol help", "OK", and "Cancel".

The image below shows a RDP session connection to a Windows 2012R2 Server at IP Address 192.168.25.80, the Domain, User Name and Password have been pre-configured, Auto Login is selected, Security level is set to NLA.

The screenshot shows the 'Access protocol' dialog box in Windows. The 'Connect using' dropdown is set to 'RDP'. Other settings include 'Color depth' (Auto), 'Graphics quality' (Auto), 'Audio quality' (Best), 'Redirect audio' (Yes), 'Redirect video' (No), 'Redirect mic' (Yes), 'Latency' (Auto), 'Security' (NLA), and 'Window size' (Auto). The 'Window percentage' is set to 80. The 'Cmd line arguments' field is empty. The 'Hostname[:port]' field contains '192.168.25.80'. The 'Auto reconnect' checkbox is unchecked, and the 'Auto login' checkbox is checked. The 'Domain' field contains 'MYDOMAIN', the 'Username' field contains 'John', and both the 'Password' and 'Confirm password' fields are masked with dots. At the bottom, there are buttons for 'Set default values', 'Get remote protocol help', 'OK', and 'Cancel'.

Connect using	RDP
Color depth	Auto
Graphics quality	Auto
Audio quality	Best
Redirect audio	Yes
Redirect video	No
Redirect mic	Yes
Latency	Auto
Security	NLA
Window size	Auto
Window percentage	80
Cmd line arguments	
Hostname[:port]	192.168.25.80
Auto reconnect	<input type="checkbox"/>
Auto login	<input checked="" type="checkbox"/>
Domain	MYDOMAIN
Username	John
Password	••••••••
Confirm password	••••••••

9. 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 VDM3.0 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

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

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 remote protocol 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, right click on a VTOS device then click on Show device info pop-up.

The dropdown options available for settings under the Access Protocol dialogue box are dependent on the underlying protocol support for them and as such not all options are available. It's recommended that command line arguments are used where strict or advanced protocol options are required

10. Setting screen resolution

VDM3.0 allows you to set the Screen resolution on any VTOS devices, this may be the Single Display SC-T25, the Dual Display SC-T36 or a RePurposed PC. In the case of the single display SC-T25, the only value that should be changed if required is the resolution via the drop down Resolution box. 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 change the default resolution on the Single Display SC-T25, in this case just set Output 2 & Output 3 to None and choose a valid mode for the SC-T25 from the drop down Resolution box. The valid modes are

800 x 600

1024 x 768

1280 x 720

1280 x 960

1280 x 1024

1366 x 768

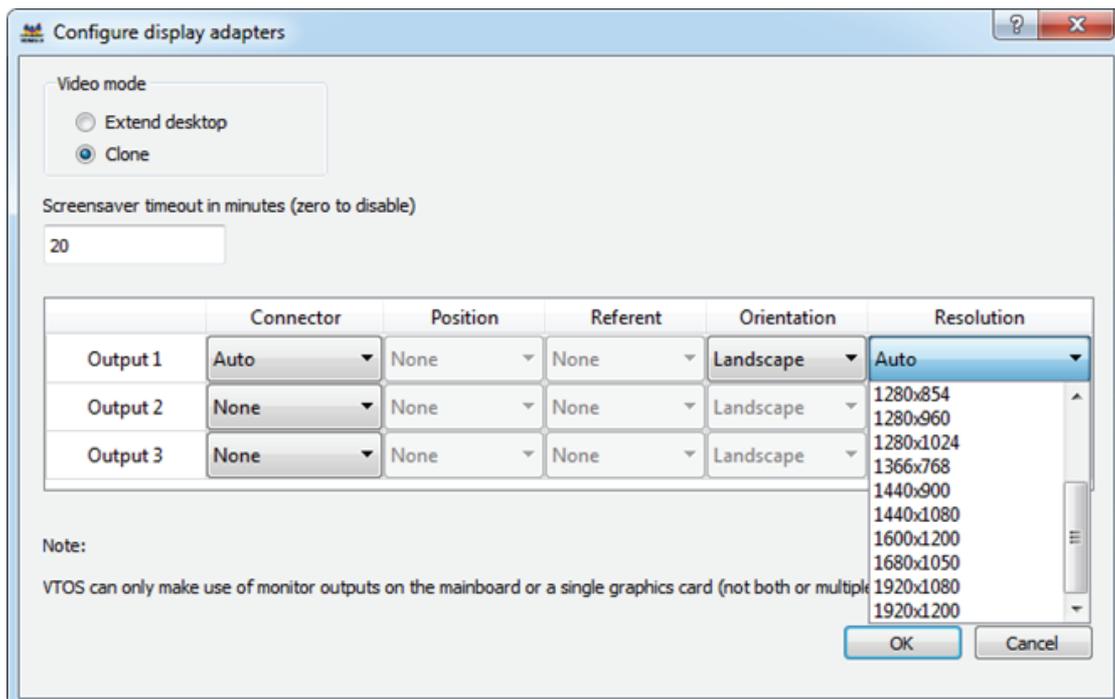
1440 x 900

1600 x 1200

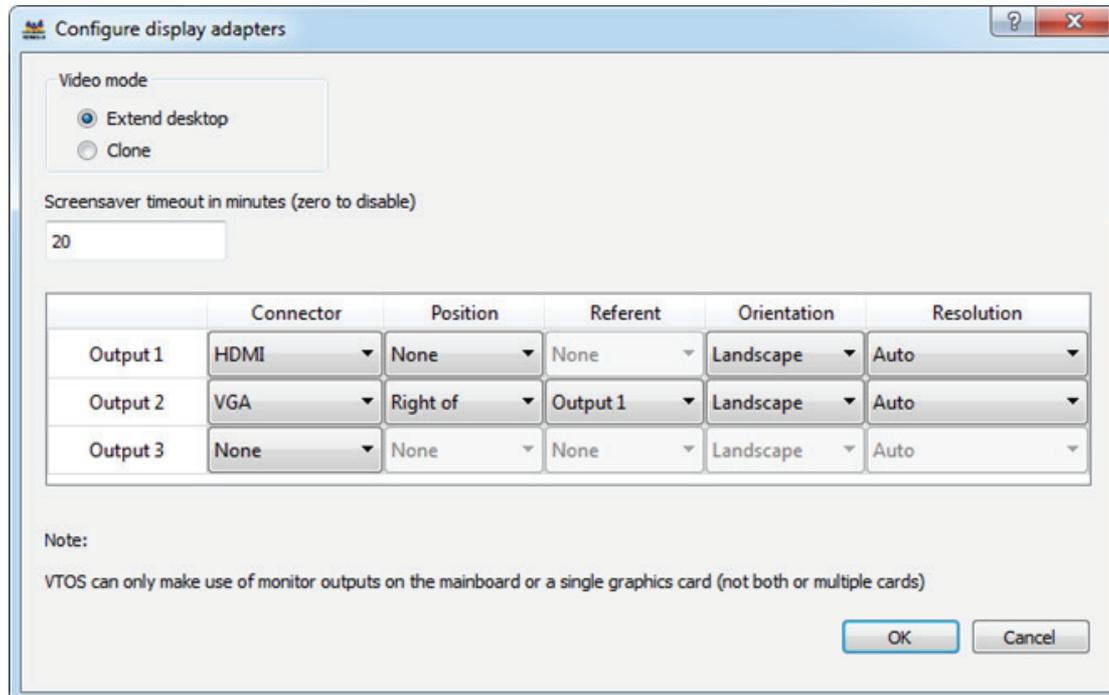
1680 x 1050

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, the Primary display has been set to HDMI and the secondary display to VGA. In this case the secondary display on Output 2 is located to the right of the Primary display on Output 1



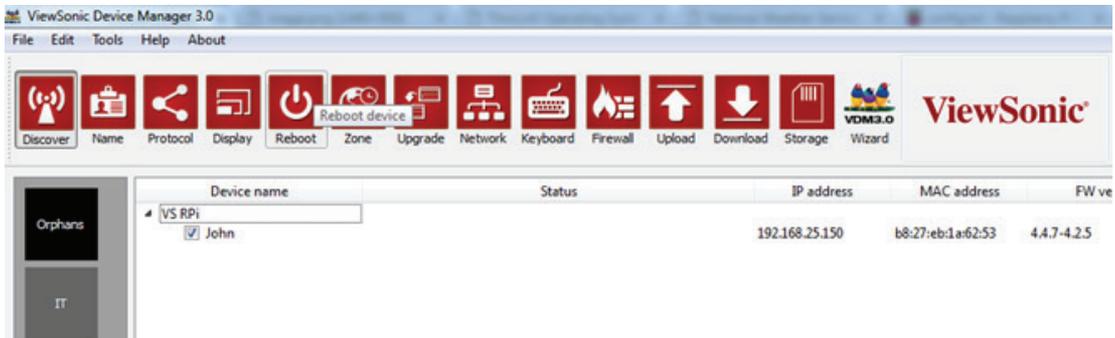
After changing the resolution a reboot of the VTOS device(s) is required

After the VTOS device reboot, the unit will reconnect to the VDM3.0 server either via Static settings, DHCP vendor options, or wait for a broadcast packet from VDM3.0 server.

11. Rebooting a VTOS Device

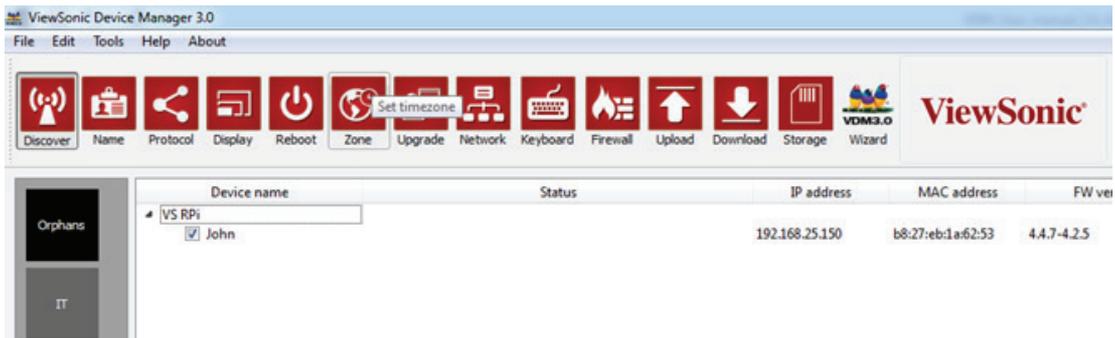
To reboot VTOS device(s), select the board(s) using the checkbox option and then click on the Reboot button as per Figure 2.0;

The VTOS device(s) will update their status on VDM3.0 then reboot. Once the board reboots, it will reconnect to the VDM3.0 server as configured (either DHCP, Static or VDM3.0 broadcast).

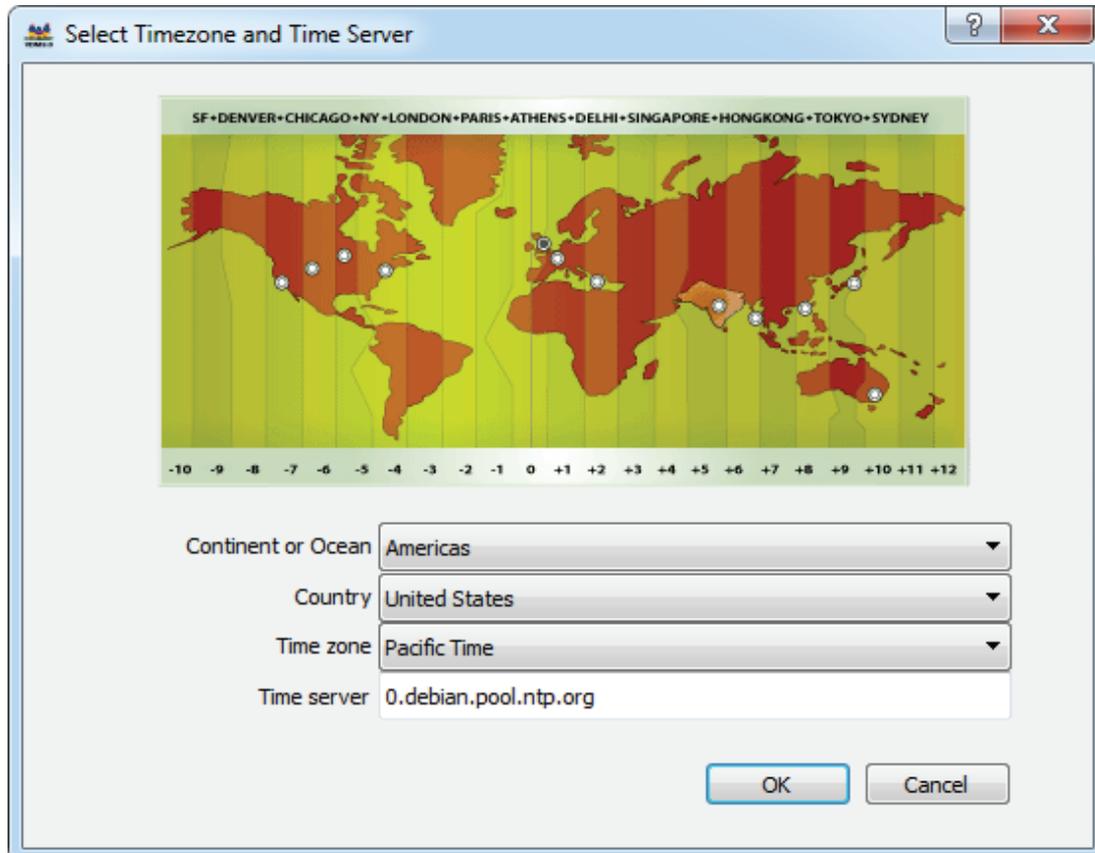


12. Setting the timezone and time server

When a VTOS device is shipped, the default timezone is set to Pacific Standard Time, US. To change the timezone, select one or more VDM3.0 Clients, then click on the Set Timezone button as shown below.



The following dialog boxes will appear allowing you select the Continent, Country and Timezone as shown below. In addition to this a specific NTP Time Server value must also be specified, by default VTOS devices uses the 0.debian.pool.ntp.org Time Server



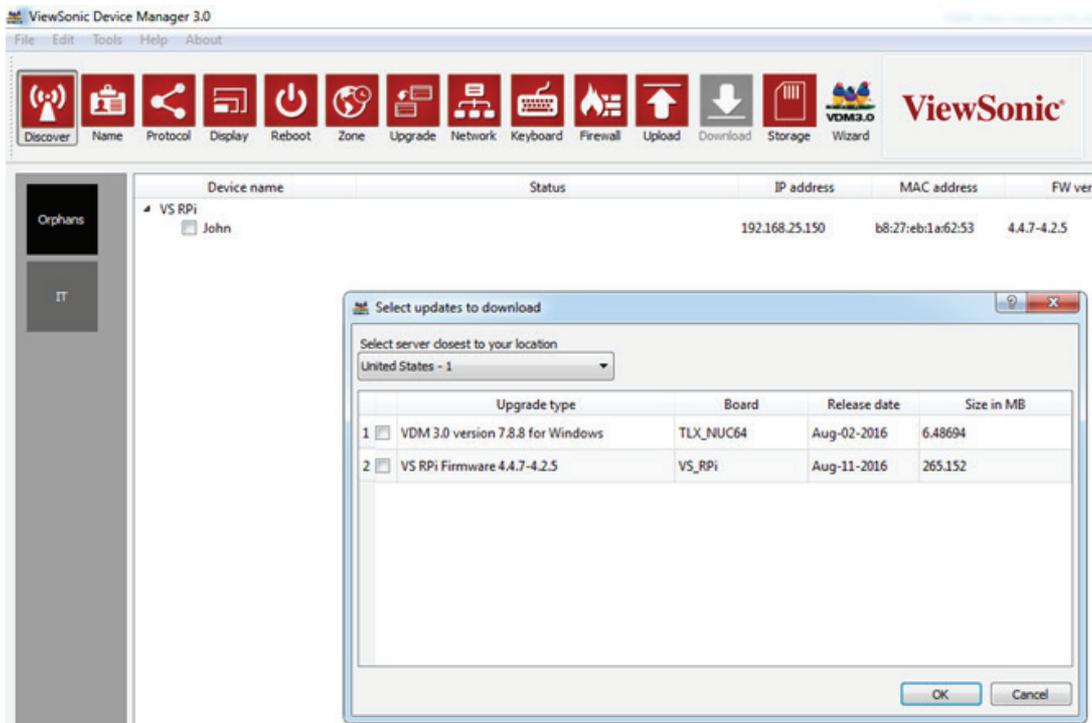
Click the OK button to apply the timezone on the selected VTOS devices(s).

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 SC-T25 which do not have an onboard battery backed Real Time Clock (RTC)

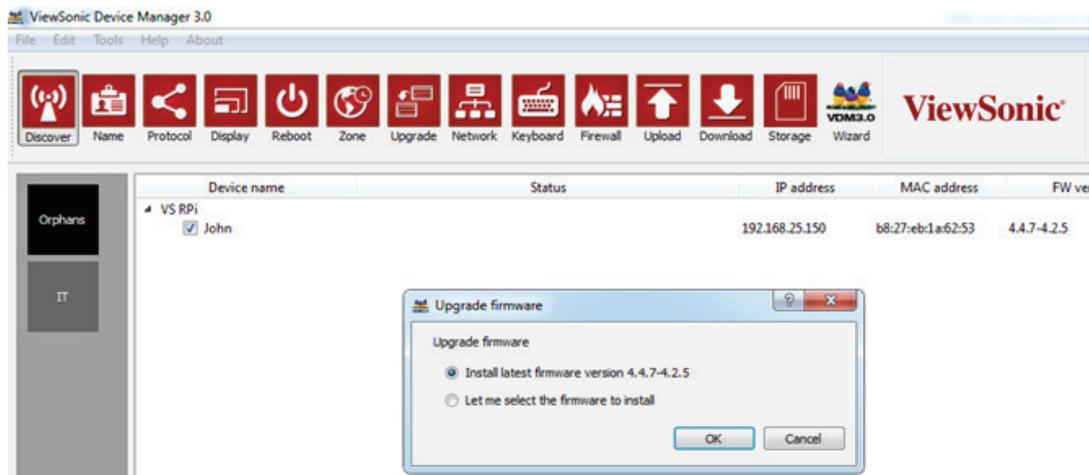
13. Downloading firmware updates for VTOS Devices

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

The download will start with the download progress displayed at the bottom left of VDM3.0, once the download completes the firmware is automatically copied and then unzipped in the VDM3.0 Firmware directory.



The firmware is downloaded once and can then be installed on many VTOS devices simultaneously by clicking on the check boxes for each device then clicking on the Upgrade Icon which will display a dialog box with the latest version of the firmware pre-selected. Click on OK to start the firmware upgrade process. If you wish to roll back to an earlier version of the firmware, choose the “Let me select the firmware to install” option.



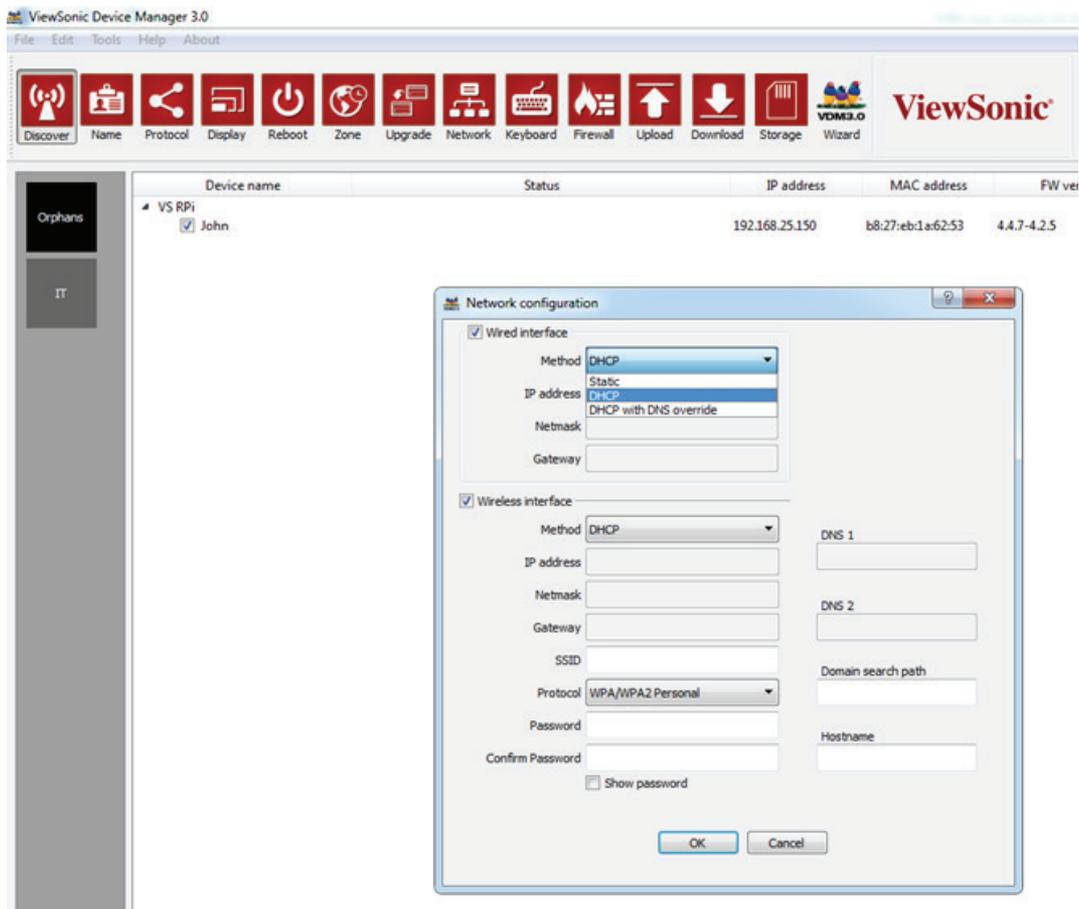
When a VTOS device receives the upgrade command it starts the upgrade process by rebooting the device into upgrade mode, VDM3.0 displays, “going Offline”. Upgrade mode loads a tiny version of VTOS which runs completely in RAM, this is necessary to allow the Kernel & RFS Partitions to be written with the new version of VTOS.

VDM3.0 displays periodic messages in the status column, this begins with the message “Downloading Kernel: 10%”, followed by “Downloading RFS: 10%”. The percentage shows how much of each file has been downloaded. After both the Kernel and RFS (Root Filesystem) have been downloaded the message “Writing Kernel” followed by “Writing RFS” appears in each device Status line. Many VTOS 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 VTOS.

14. Network Configuration

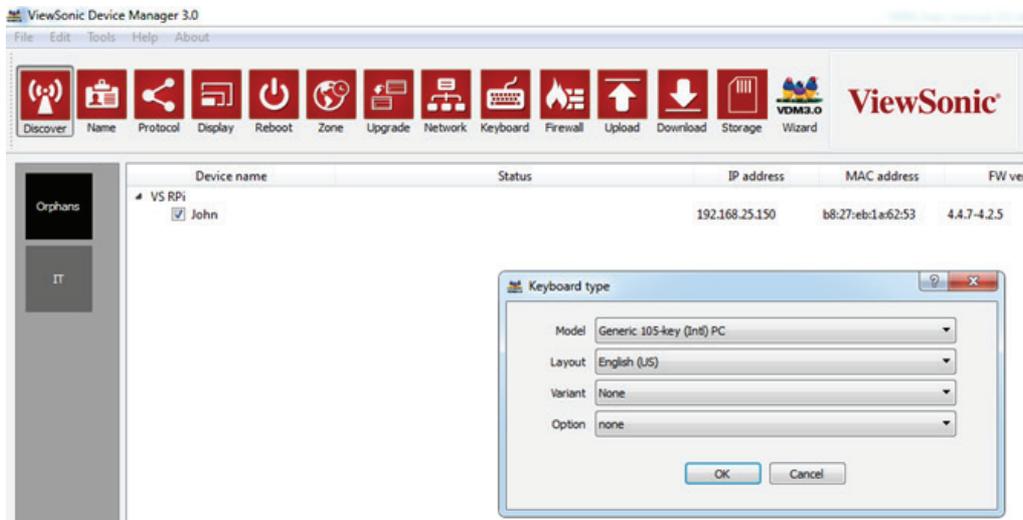
Click on the Network Icon to change the configuration of the Wired or Wireless interfaces. The default setting is DHCP, this can be changed to Static where all interface information must be manually entered. Another option is DHCP with DNS Override, this must be set if the DHCP Server is not providing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

If your device has WiFi support built in you can deselect the check box for Wired Interface and select the check box for Wireless interface, the default setting is DHCP, with Static or DHCP with DNS override available also. The only encryption protocol offered is the secure WPA/WPA2 Personal, WEP and No Encryption may be added to a future VTOS release due to customer requests for these options. 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 Wireless mode. On some devices you may need to reboot to ensure the WiFi mode is working.



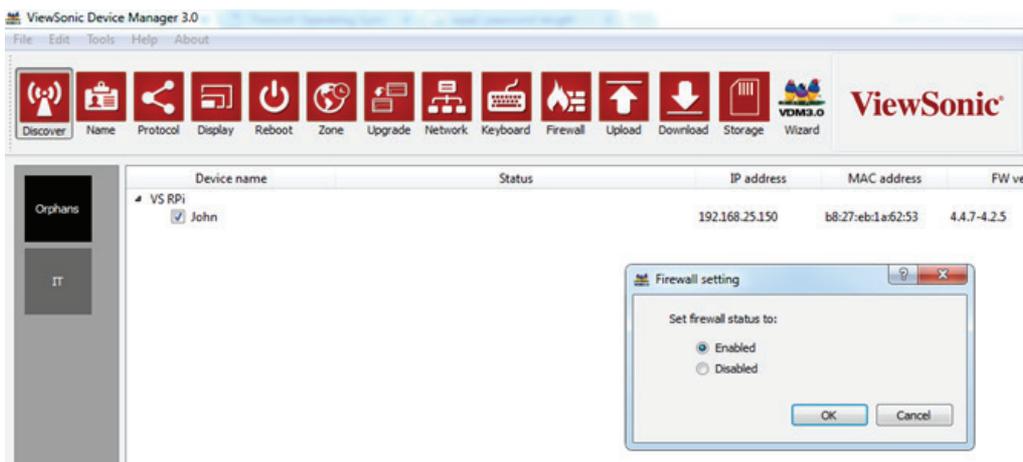
15. Keyboard Configuration

To configure your Keyboard, select the check boxes on devices to be configured, click the Keyboard Icon and enter the values required.



16. Firewall Configuration

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

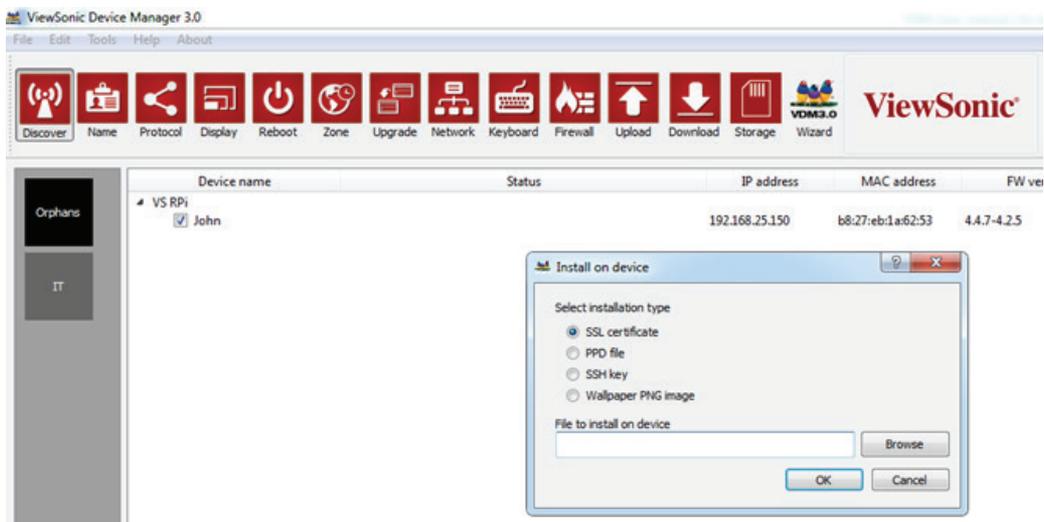


17. Upload Files to your devices

Some file types can be uploaded to your devices by selecting the Upload Icon, these are SSL Certificate, Printer PPD file, your Public SSH key, a Wallpaper image that is displayed after boot up as the background image.

- a. SSL Certificate, this should be your Root Certificate in .pem format, used for secure connection with Citrix Receiver
- 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
- d. Wallpaper PNG image, upload your preferred Wallpaper using your own image.

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

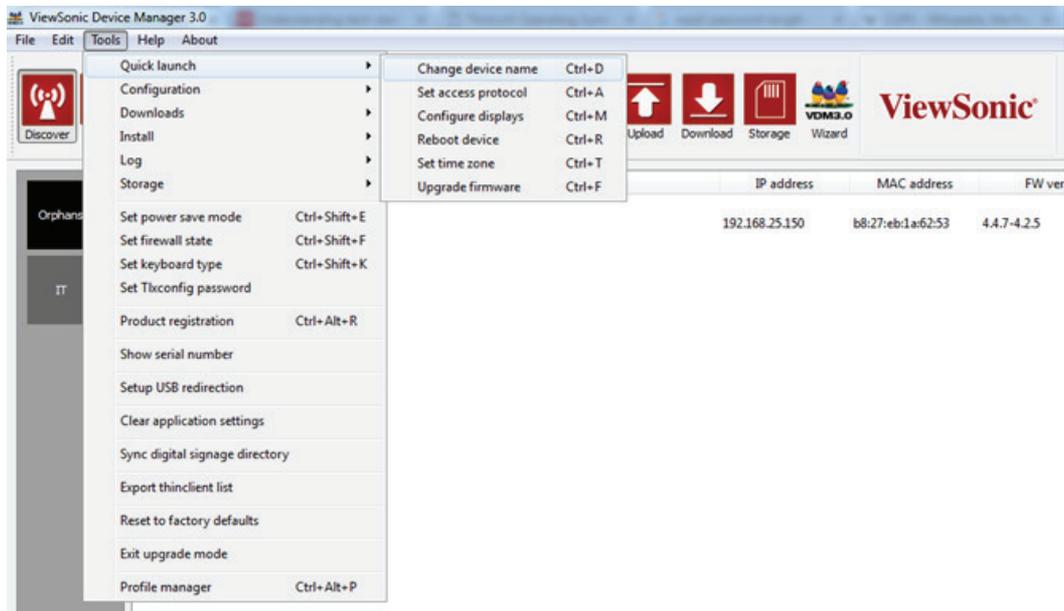


18. Storage & Wizard Configuration

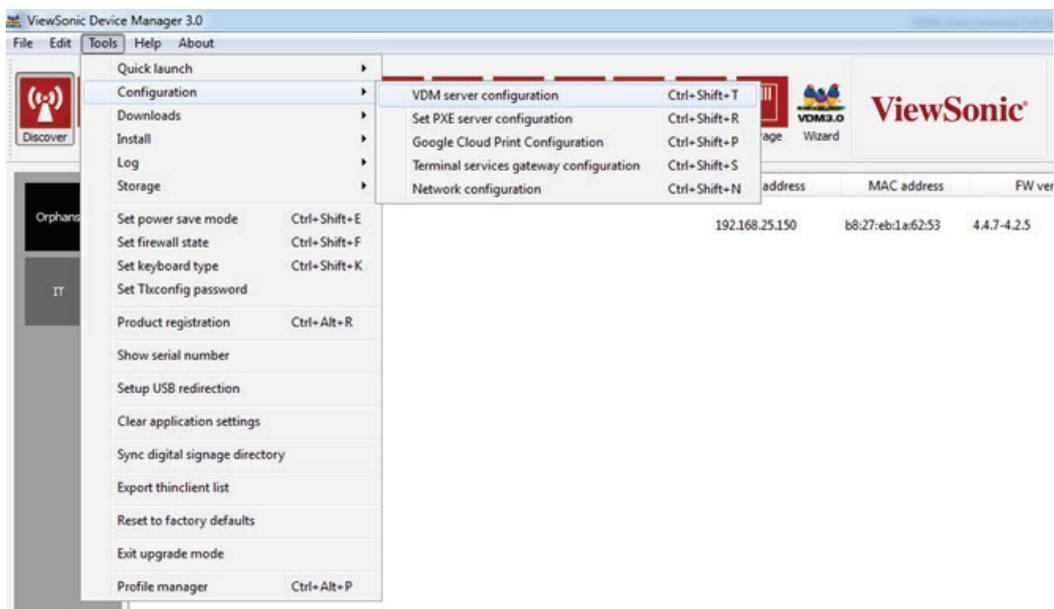
The Storage Icon & Wizard Icons are only used for Factory installations, you will not need to use these options

19. The Tools menu

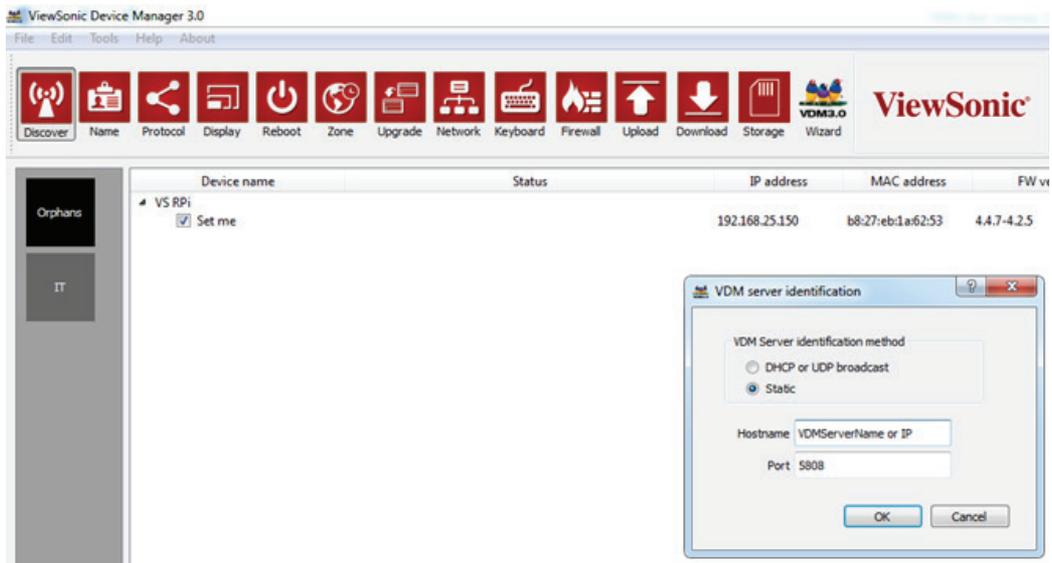
The Tools menu allows the configuration of many additional features and also displays Keyboard shortcuts hints, see Quick launch Dialog box below



The Tools / Configuration, menu has five sub menus which are shown below

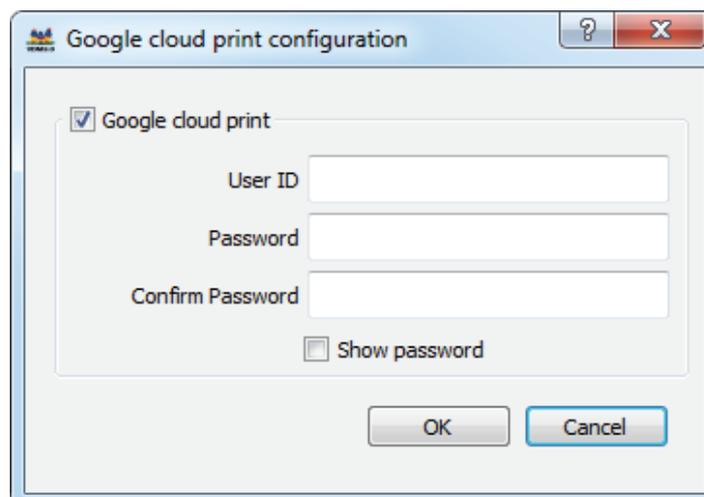


VDM3.0 Server configuration, this will point the VTOS device to the PC running VDM3.0

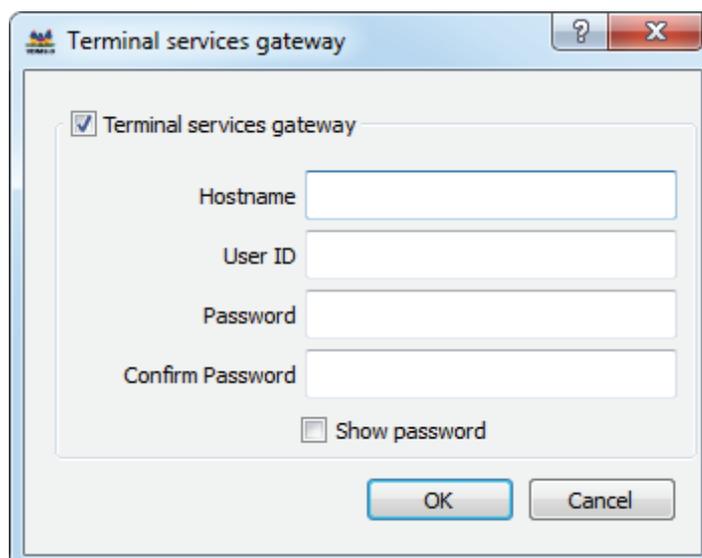


Set PXE Server configuration, is not currently supported by VDM3.0 / VTOS

Google Cloud Print configuration, allows your VTOS 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



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



Network configuration, launches the Network Configuration Dialog box as described earlier in this document

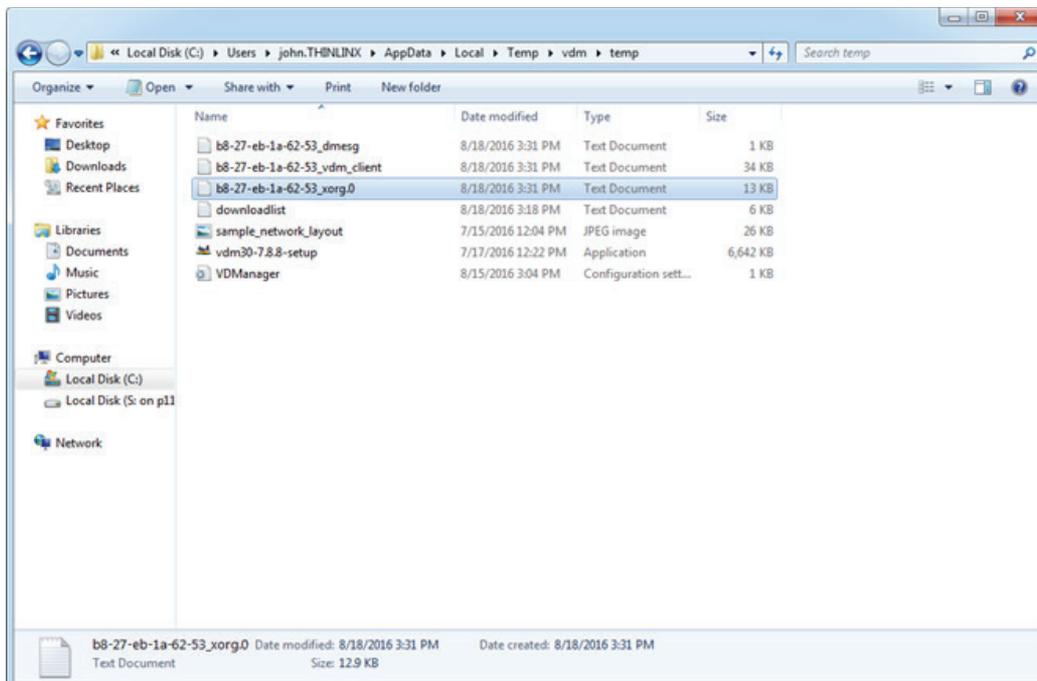
Tools / Downloads / Clear Updates Cache, clears the list of downloaded firmware files from VDM3.0. When the Download Icon is click on, a List of available firmware is displayed, firmware that has already been downloaded no longer appears in the list unless "Clear Updates Cache" is clicked on

Tools / Install / Install VDM3.0 client, every VTOS firmware release includes a VDM3.0 client which communicates information from the VTOS device to the PC running VDM3.0. In some circumstances a new version of the VDM3.0 client is made available, this can be downloaded using Download Icon and then copied to the VTOS device.

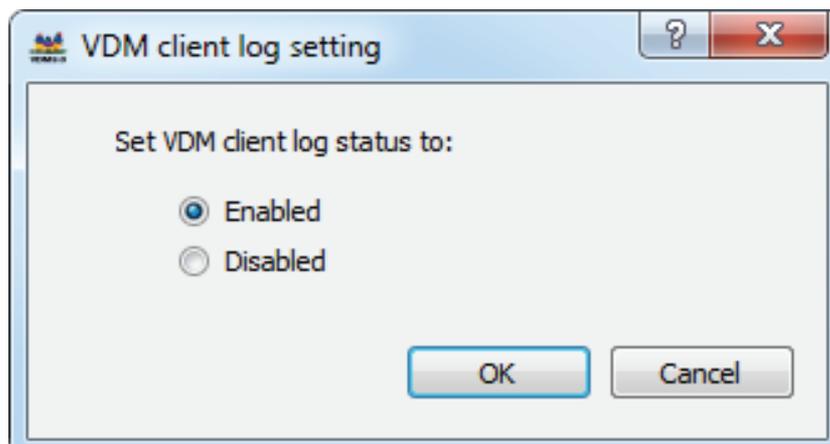
Tools / Install / Install Hotfix, from time to time between new VTOS Firmware releases a Hotfix may be released to correct a bug, update Citrix Receiver etc. To install a Hotfix, first click on the Download Icon, select the Hotfix from the Dialog box list, click on Tools / Install / Install Hotfix to copy the Hotfix to selected VTOS devices

Tools / Install / Install File on device, this provides the same function as clicking on the Upload Icon.

Tools / Log / Get device Log files, this will download the log files from the device, the three files are pre-pended with the device Mac Address and include Kernel dmesg, VDM3.0 client information, and the Xserver Log, see image below

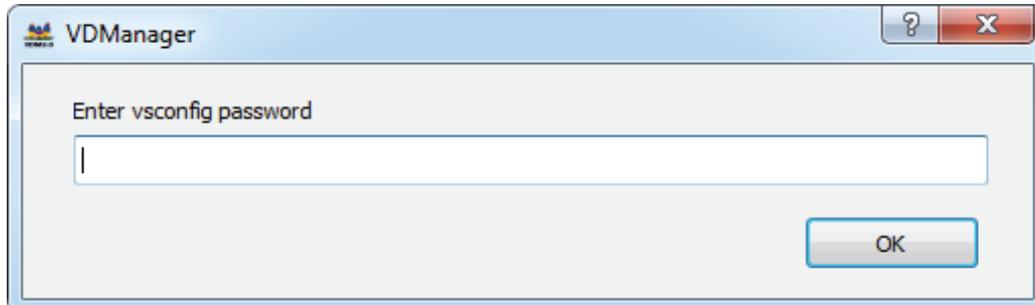


Tools / Log / Set device log state, the default is Enabled, if you wish to disable logging select the disabled check box.



Tools / Storage, dedicate Storage is a Factory option and is not required for standard VTOS installations

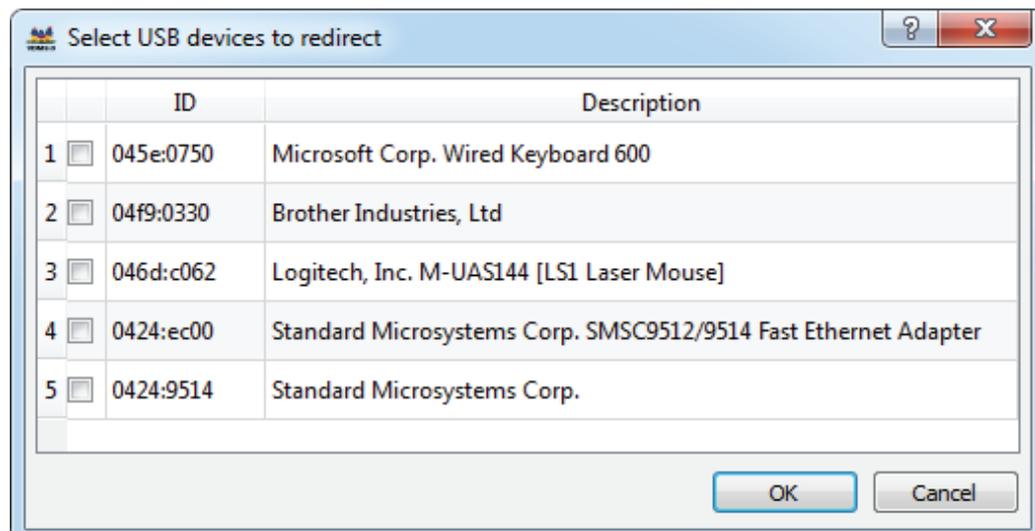
Tools / Set VSconfig password, this allows the setting of a password to disable access to the local VTOS configuration menu



Tools / Product Registration, this Registers a Re-Purposed PC

Tools / Show serial number, this will display the serial number of any selected devices in the Status line

Tools / setup USB redirection, this option is used to configure which USB devices to redirect inside a Microsoft RemoteFX VDI session, it has no effect in any other Protocols including RDP mode.



Tools / Sync Digital Signage Directory, one of the Protocols supported by your VTOS device is Digital Signage for Advertising / Information / Timetables etc. VTOS will support up to three displays. The Digital Signage mode can play fixed images, Videos or a Web Browser in Kiosk mode.

Depending on the number of Monitor Outputs on your VTOS devices you can create up to three subdirectories on the PC running VDM3.0, we recommend 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 switched modes.

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

In the Image below you can see that it is possible to synchronize content on your PC with the Digital Signage directories on your VTOS devices, there is one directory dedicated for each Output display. If your VTOS device has Dual Displays it is possible to play Images on one Display and Videos on the second, or Web Content on one display and either Videos or Images on the other.

In this example we will configure Images to play on Output-1 and Videos to play on Output-2, step one is to use the VDM3.0 Protocol Icon to switch your VTOS device to Digital Signage mode, this will automatically create three Digital Signage subdirectories on your device in the /home/VTOS/dsi_root directory. The device will attempt to play content which does not exist yet as you have not synchronized your Digital Signage Images, Videos, and Web directory content with the VTOS device

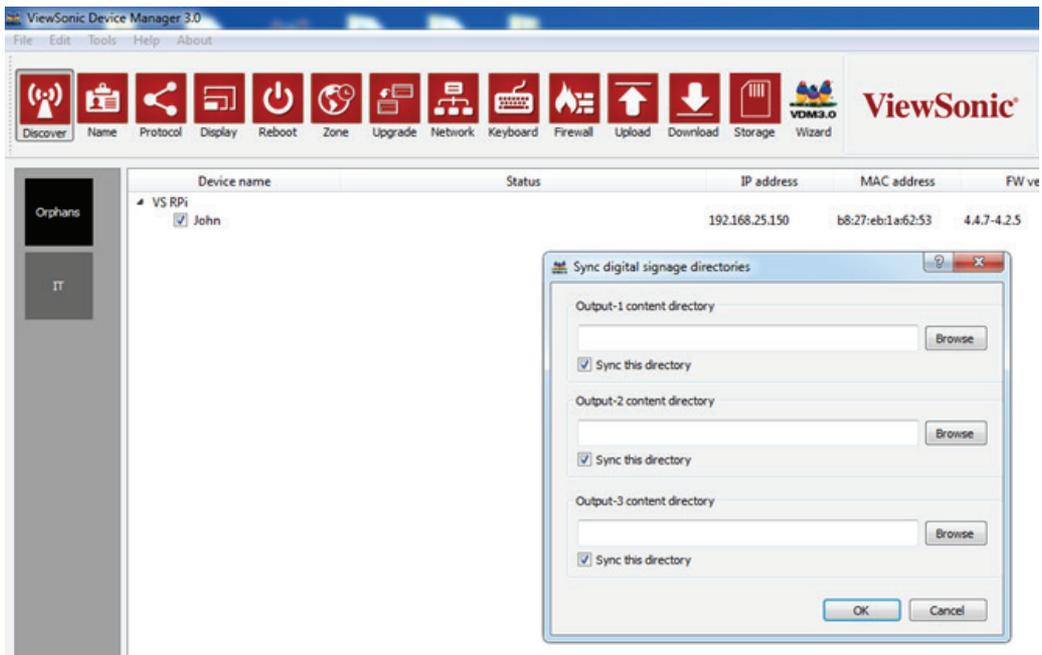
Use the Output-1 content directory Browse button to select your Digital Signage/ Images directory

Use the Output-2 content directory Browse button to select your Digital Signage/ Videos directory

Untick the Output-3 content directory "Sync this directory" check box, then click the OK button, the file synchronization will start with progress messages displayed.

After the synchronization is complete, click on the Reboot Icon, the VTOS device will reboot and start playing the content.

You can add or remove content in your PC's Digital Signage directories and then Synchronize again. If you want to erase the content on the VTOS device just erase the content in your corresponding Digital Signage directory and Synchronize again.



Tools / Export thin client list, is under development, do not use this option

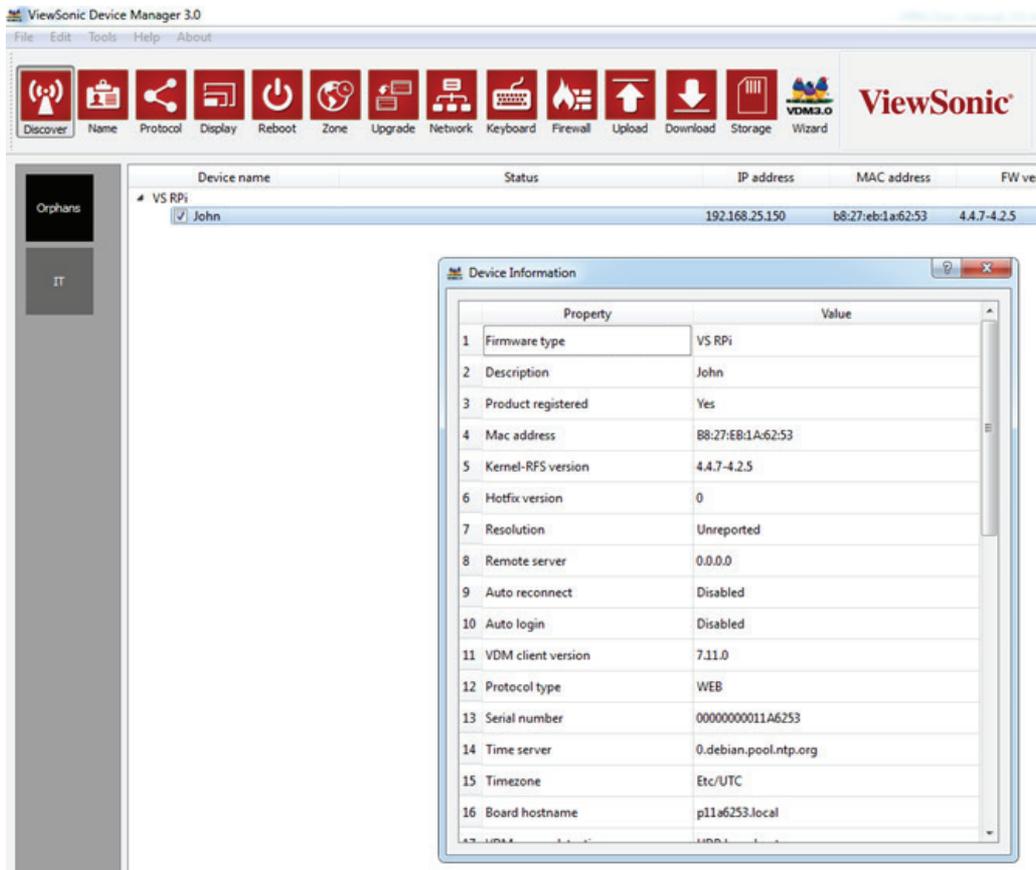
Tools / Reset to factory defaults, will reset the VTOS device to the shipped default settings erasing any changes that you have made to the initial configuration. This can also be carried out on the VTOS device itself by pressing Ctrl-Alt-r twice within 2 seconds, the device will reboot.

Tools / Exit upgrade mode, is used to return a device which has entered upgrade mode (due to License expiry) to normal mode if the device has been Registered

Tools / Profile manager, this option is under development, do not use this option

20. Displaying detailed VTOS device information

Every VTOS device has unique device information such as serial and MAC address details. To determine the detailed information of a VTOS Device, select the device, then right click and select Show device info. The serial number for the selected VTOS device will be displayed in the Device Information screen as shown below. This serial field or any other field allows the copy and paste function by pressing control + C (Windows) to copy the serial number to the clipboard then paste it into an email or other document.



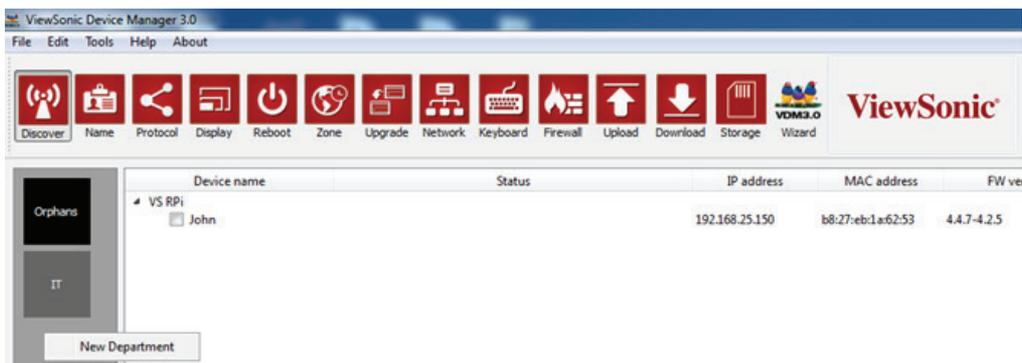
The screenshot displays the ViewSonic Device Manager 3.0 interface. The main window shows a table of devices under the 'VS RPi' category. The device 'John' is selected, and its details are shown in the 'Device Information' dialog box.

Property	Value
1 Firmware type	VS RPi
2 Description	John
3 Product registered	Yes
4 Mac address	B8:27:EB:1A:62:53
5 Kernel-RFS version	4.4.7-4.2.5
6 Hotfix version	0
7 Resolution	Unreported
8 Remote server	0.0.0.0
9 Auto reconnect	Disabled
10 Auto login	Disabled
11 VDM client version	7.11.0
12 Protocol type	WEB
13 Serial number	0000000011A6253
14 Time server	0.debian.pool.ntp.org
15 Timezone	Etc/UTC
16 Board hostname	p11a6253.local

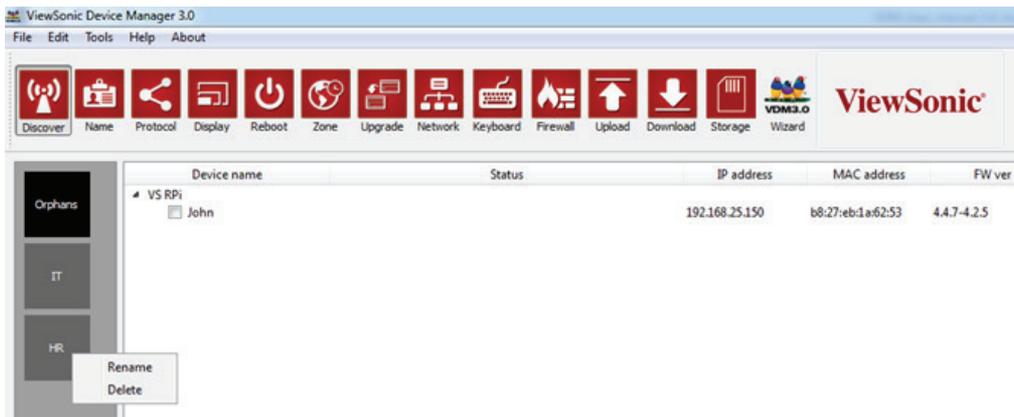
21. Sorting VDM3.0 Clients into departments

It's recommended when managing a higher volume of VTOS units that devices are grouped into sub folders or containers called departments. When VDM3.0 is first installed, a default department called Orphans is created and all VDM3.0 Clients that connect to VDM3.0 are stored in this department. You can create as many departments as you wish and store your VDM3.0 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.



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 below



VDM3.0 does not allow you to delete departments that have VDM3.0 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 VTOS device to particular department, just drag it from the UI and drop it into the relevant department.

If a VTOS device that was previously discovered and visible on VDM3.0 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.



ViewSonic®