Zero Client with vMatrix Server Manager

User Manual

Rev6: 12-29-2021

This guide applies to Windows Server 2022 and earlier versions. All screen shots shown were captured from Windows Server 2012 and 2022 installations. The installation, configuration and login screens are based on vMatrix Server Manager 2.7.0 Actual use may vary depending on the specific software used. Unless specifically noted, the installation screens are generally identical for all systems.

Table of Contents

Important Notices

Please note that reproduction of this User Guide in whole or in part, without express written permission from vCloudPoint, is not permitted.

vCloudPoint reserves the right to make improvements and/or changes to this User Guide and to the products, programs and/or specifications described herein at anytime without notice. Information contained in this document may have been obtained from internal testing or from a third party. vCloudPoint shall not be liable for any direct, indirect, special, incidental or consequential damages in connection with the use of this material. The latest version of this User Guide is obtainable at the “Download center” under the Support menu of the vCloudPoint website at: www.vcloudpoint.com.

Refer to the Limited Hardware Warranty applicable to your region for information on what is and what is not covered by the warranty, your responsibilities, exclusions, and how to obtain service.

Please refer to the End User License Agreement (EULA) and Terms of Use (TOU) that are presented for your review during the software installation process. The information contained in these documents is very important. The EULA and TOU constitute agreements between you and vCloudPoint and are accepted by you by installing and using the product. It is your responsibility to print a copy of the EULA and TOU directly from the installer in order to keep for your records.

This product gives users shared access to computer resources. It is not a computer, and may not support all software applications, especially 3D applications that are designed to be supported by computers with stand-alone graphic card. Similarly, it may not support all hardware peripherals that are designed to be supported by stand-alone computers.

Refer to your computer operating system and application software vendors license agreements for information on using these products with the vCloudPoint system. Additional software licenses may be required.

The vCloudPoint hardware and software products described in this user manual are protected by numerous granted and pending P.R.C and international patents.

© 2021 by Shenzhen Cloudpoint Technology Co., Ltd. All rights reserved. vCloudPoint and vMatrix are registered Trademark of Shenzhen Cloudpoint Technology Co., Ltd. – P.R.C. Microsoft and Windows are registered trademarks of Microsoft Corporation. All trademarks are the property of their respective owners.

Safety Information

Refer to the following information to prevent any physical injury or loss of assets caused by damage to the product. A user must read this User Guide carefully before use and properly follow the instructions.

- Make sure that the place of installation is not too hot (above 35°C), too cold (below 0°C), or too wet (above 85% relative humidity).
- Avoid any severe impacts to the product
- Make sure that the product is not exposed to direct sunlight or any hot machinery.
- Please keep the product away from any items which have strong magnetic properties.
- Do not disassemble, repair or rebuild the product.
- Please properly route all cables and power cords to avoid a tripping hazard. An electric shock, fire, damage to the product or physical injury may occur as a result of tripping over the cable.

Regulatory Compliance

FCC Information

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment to a power outlet on a circuit different from which the receiver is connected
- Consult your dealer or an experienced radio TV technician for help

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

European Community (CE):

The Bureau of Indian Standards (BIS):

IS 13252
R - 41025534

Disposal Information:

This symbol means that according to local laws and regulations your product should be disposed of separately from household waste. The separate recycling of your product will help ensure that it is recycled in a manner that protects human health and the environment.

Chapter 1. Product Overview

1.1 Brief Introduction

vCloudPoint zero clients with vMatrix Server Manager software provide an alternative solution to the traditional one PC per seat solution by powering multiple users with just one PC. vCloudPoint zero client is compact, network access device that contains no moving parts but allows each of its users to share the untapped resources of a single host PC. vMatrix Server Manager performs as the management role on the host side with a number of tools to assist IT administration, such as desktop broadcasting, monitoring and controlling, storage visibility configuration, and user policy setup, etc. vCloudPoint zero clients, combined with vMatrix Server Manager software, provide computing experience that is practically indistinguishable from running on a PC, but offer great advantages over traditional PCs, such as saved costs, enhanced security, reduced maintenance, and simplified deployment and management.

1.2 Package Contents

When you unpack your vCloudPoint box, you will find the following items:

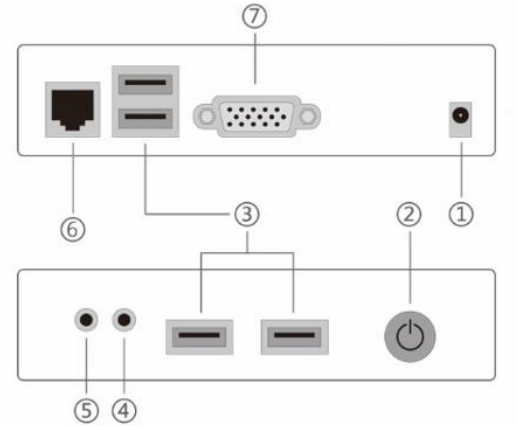
- A zero client terminal device
- A base/mounting bracket
- Two screws
- A 5V power adapter

If you find any damage or shortage of any accessories, please contact your local dealer.

Note: Your vCloudPoint zero client purchase was bundled with an entitlement to vMatrix Server Manager Software and Premium Support.

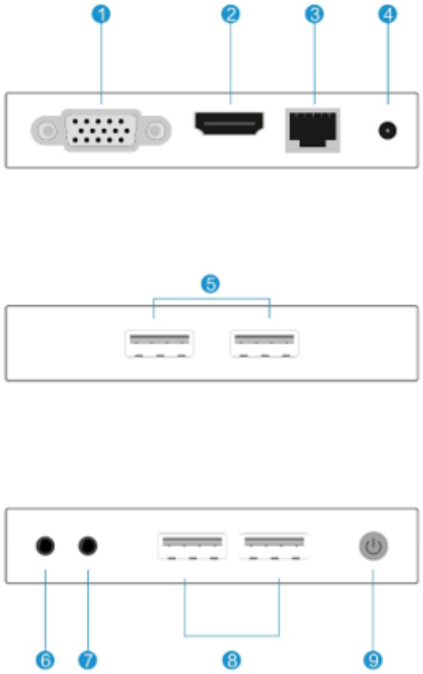
1.3 Device Connections

Model: S100



① 5V DC Power Input ② Power& Reset Button ③ USB2.0 Ports ④ 3.5mm Mic Jack
⑤ 3.5mm Speaker Jack ⑥ RJ45 Ethernet Input ⑦ VGA Display Port

Model: V1



① VGA Display Port ② HDMI Display Port ③ RJ45 Ethernet Input ④ 5V DC Power Input

⑤ 5V DC Power Input ⑥ 3.5mm Speaker Jack ⑦ 3.5mm Speaker Jack

⑧3.5mm Mic Jack ⑨ Power& Reset Button

Chapter 2. Panning for Deployment

2.1 Hardware Configuration

2.1.1 Host Configuration Reference

No. of Users	10	20	30	40	50	60
CPU	i5-7500	i7-7700k	i7-8700k	Intel E5 2670*2	Intel E5 2680 v2 *2	Intel E5 2680 v3 *2
Memory (Reserve 2G for the host itself)	1.5G per Task Users running office, browser, messenger, video on VLC player, etc..					
	2G per Power Users running Photoshop, Illustrator, Auto-CAD, etc..					
SSD (for System and Programs)	SSD 120G	SSD 120G	SSD 240G	SSD 480G	SSD 240*2 G	SSD 240*2 G
HDD (for User Data)	HDD; Storage size to be determined by actual needs.					
Bandwidth	Average 15Mbps per user within LAN.					

Note:

1) This recommended configuration is for supporting multiple users simultaneously running the same applications, for environments of running mix applications, please thoroughly evaluate expected workloads of every user and make some adjustments and fine tuning as your deployment progresses.

2) Hard Disk Partition Recommendations：

Use a Solid-State Disk (SSD) in a single partition for system and programs to ensure a smooth user experience and reserve 5GB per each user for storing users' cache date.

A hard disk(s) in at least 2 partitions for users shared and private data storage with the size to be determined by actual needs (e.g. 50GB per user).

2.1.2 Networking Configuration

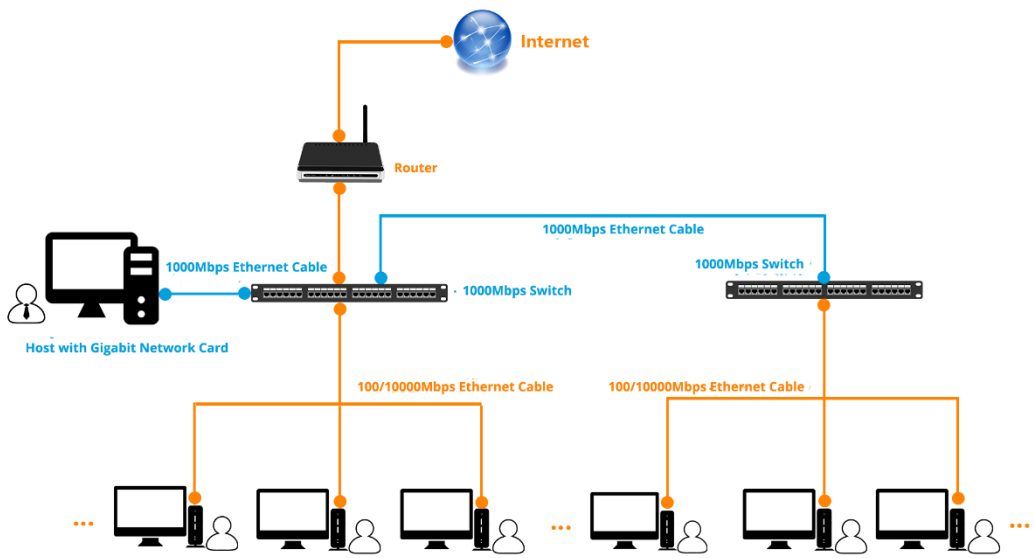
Host Network Controller		10/100/1000Mbps Base-T
Switch		10/100/1000Mbps Base-T
Cable	**Connecting zero clients**	10/100Mbps or 10/100/1000Mbps Base-T
	Connecting host to switches	10/100/1000Mbps Base-T

Note:

1) You are recommended to use reliable gigabyte networking devices and CAT-6 Ethernet cables for desirable multi-user experience.

2) Although vCloudPoint zero clients have a WIFI option, you are recommended to use standard Ethernet network as unreliable WIFI network may cause disconnection or experience compromised.

2.1.3 Network Wiring Diagram



2.2 Software Requirements

2.2.1 **vMatrix Server Manager** per shared host

The latest version of vMatrix Server Manager is obtainable at

https://www.vcloudpoint.com/support/installation-guide-and-downloads/.

2.2.2 **Windows Operating System** mounted on each shared host

Supported Operation Systems by vMatrix Server Manager:

- Microsoft Windows XP SP3 32-bit (Professional/ Ultimate)
- Microsoft Windows 7 32-bit & 64-bit (Professional/ Enterprise/ Ultimate)
- Microsoft Windows 8 32-bit & 64-bit (Professional/ Enterprise/)
- Microsoft Windows 8.1 32-bit & 64-bit (Professional/ Enterprise/)
- Microsoft Windows 10 32-bit & 64-bit (Professional/ Enterprise/)
- Microsoft Windows 11 (Professional)
- Microsoft Windows Server 2003 32 bits
- Microsoft Windows Server 2008R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Multipoint Server 2011
- Microsoft Windows Multipoint Server 2012

Note: do not use a 32-bit Windows operating system in your real deployment, as it supports only 3.25 GB maximum memory.

2.2.3 Multi-User Application

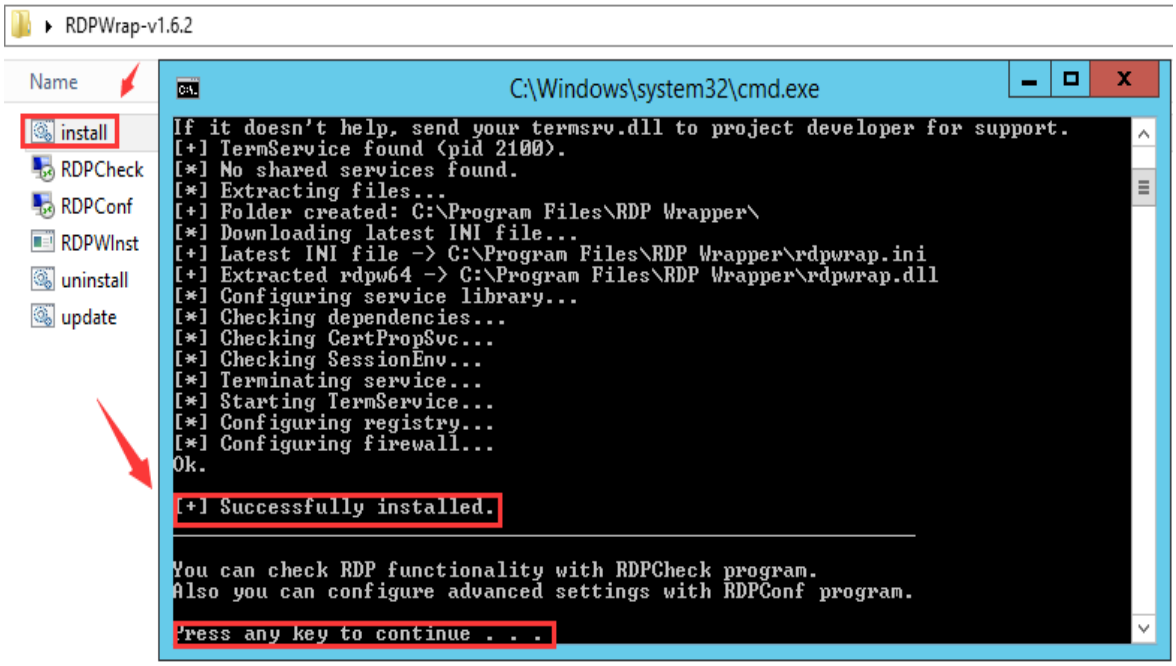
vMatrix doesn't contain a component or application to allow multiple users to access the host simultaneously. To allow a simultaneous multi-user login, you need to install RDP Wrapper (download and learn more at www.vcloudpoint.com/support/add-ons) or obtain Microsoft RDS CALs. To properly license vCloudPoint zero clients in a Microsoft environment, you are recommended to obtain Microsoft RDS CALs for each vCloudPoint seat. For more information on licensing with Microsoft operating systems see at www.vcloudpoint.com/support/help-center/.

- **RDP wrapper**

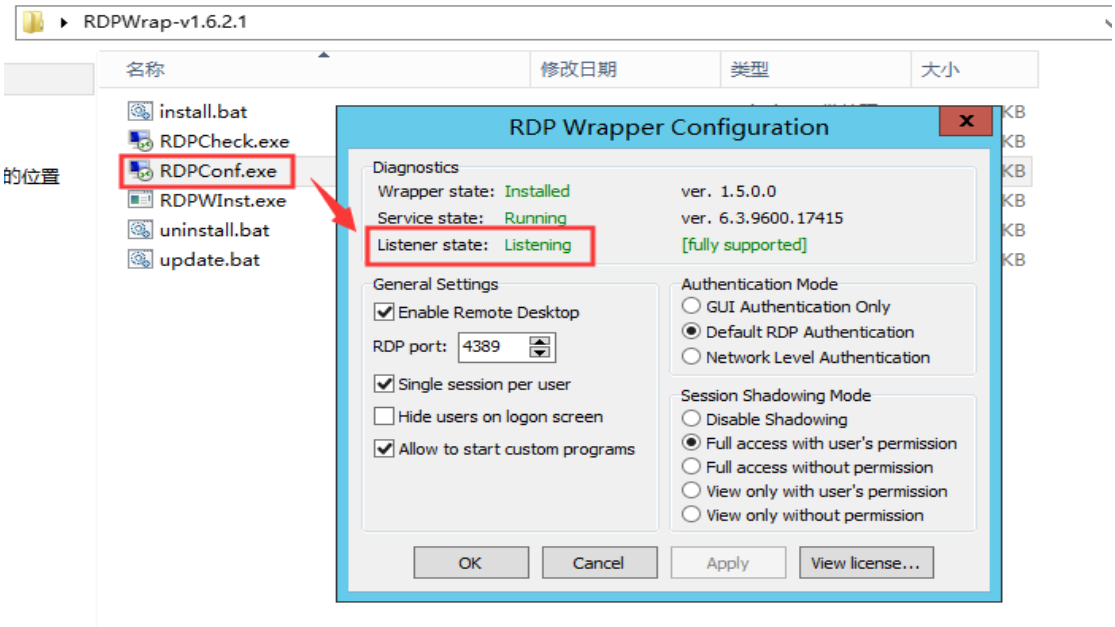
RDP Wrapper is a free open source project to enable Remote Desktop Host support. RDP Wrapper is obtainable at https://github.com/DrDrrae/rdpwrap/releases

Instructions:

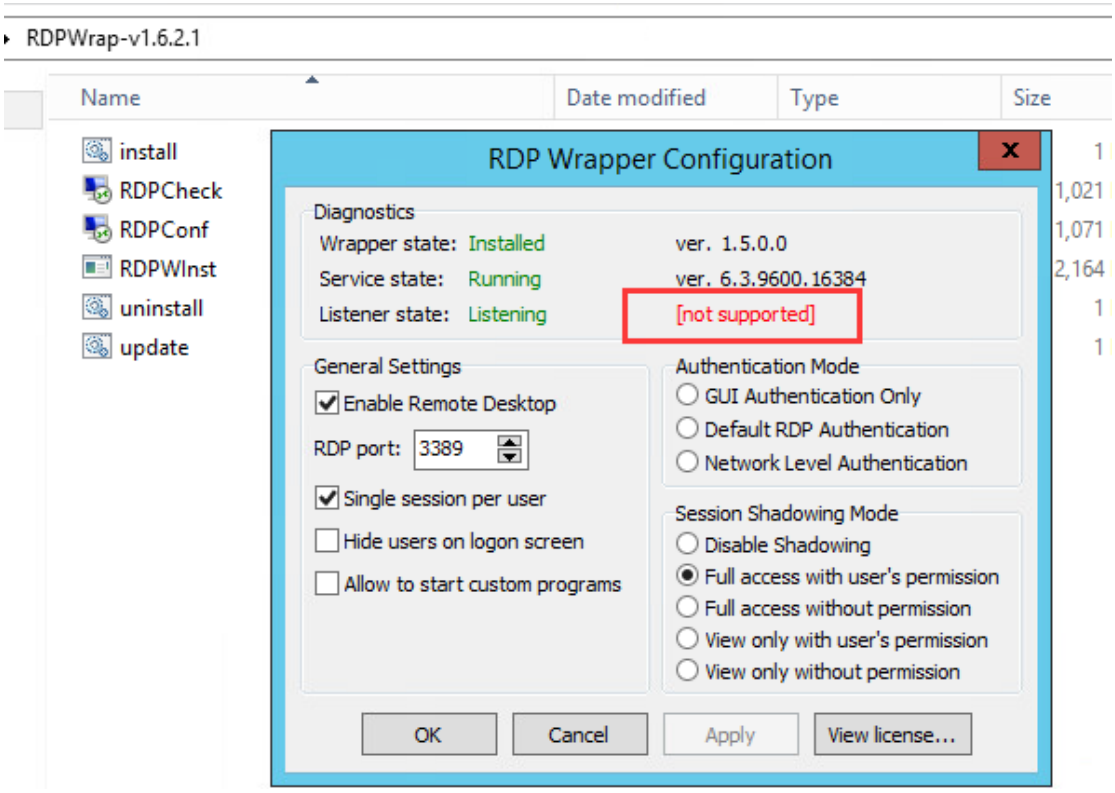
1) Download the RDPWrap.zip file and then unzip it. Simply run the insall.bat file and press any key when finished but make sure to disabled anti-virus software during installation.



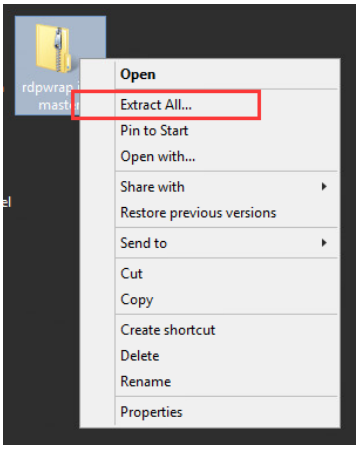
2) Check if the installation is successful by running “RDPConf.exe”



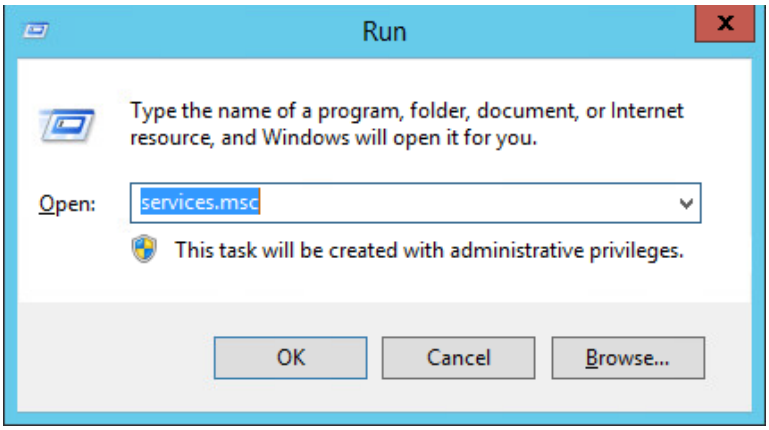
Reminder: update the “rdpwrap.ini” file if the configuration tool shows “[not supported]” in red.

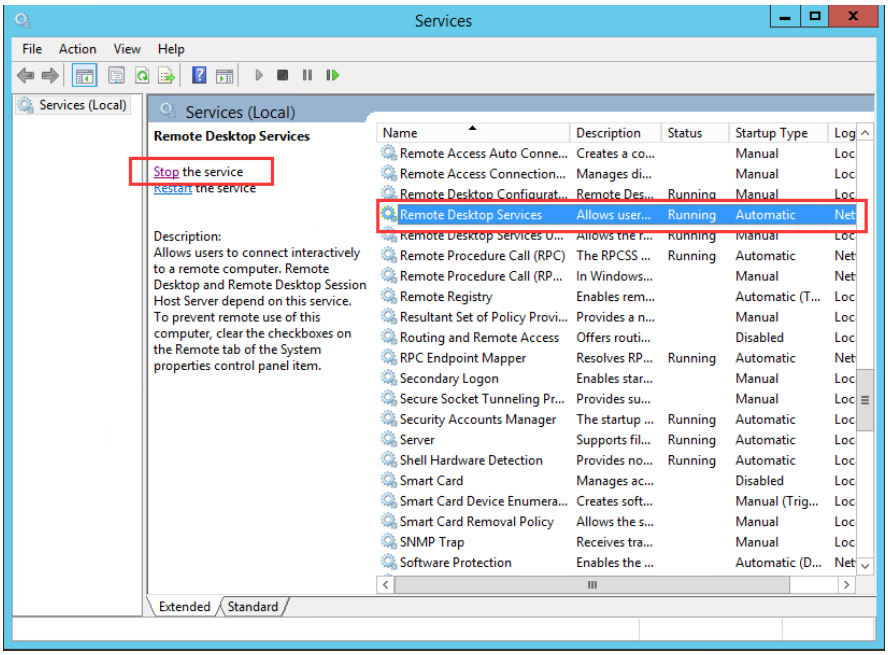


① Download the latest “rdpwrap.ini” compressed file and extract the files.
Download Url: https://codeload.github.com/sebaxakerhtc/rdpwrap.ini/zip/master.

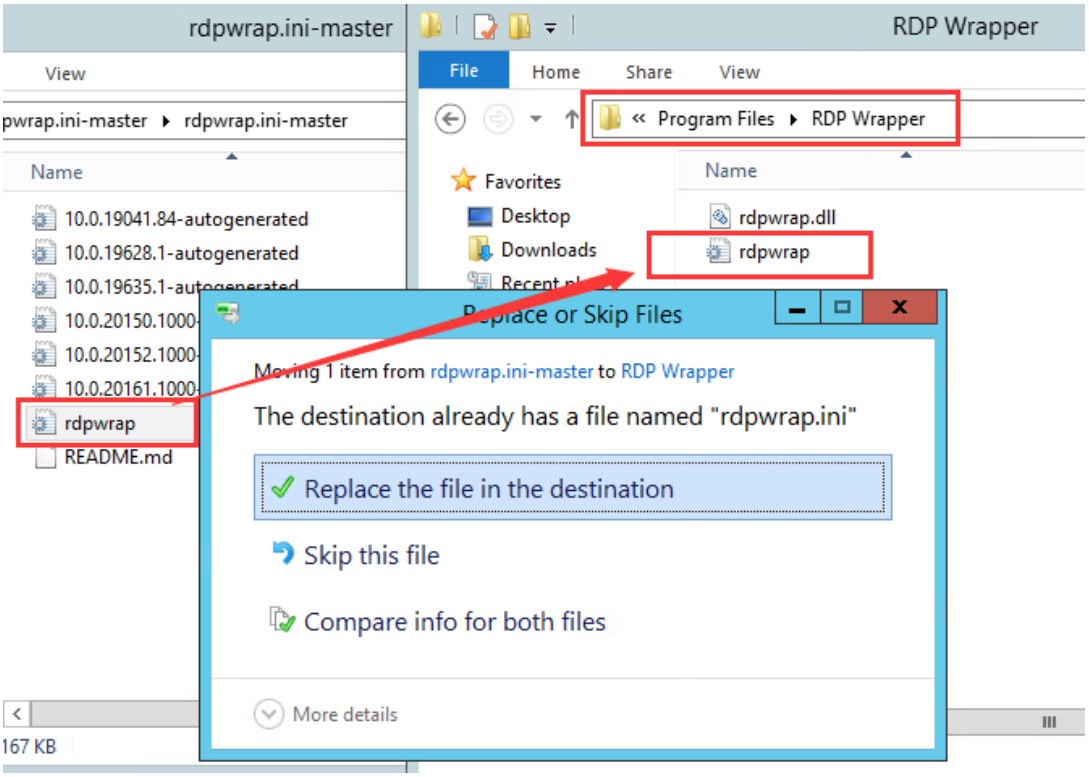


② Presss “Win”+“R” to run “services.msc”, and stop the “Remote Desktop Services”.

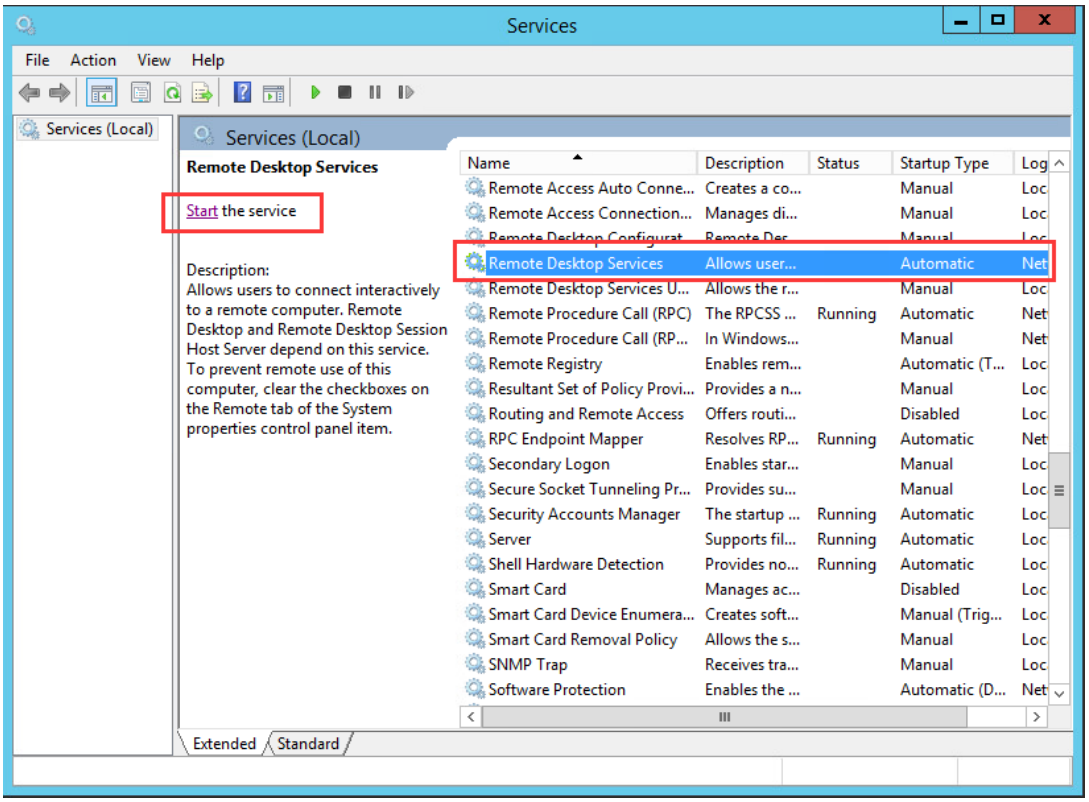




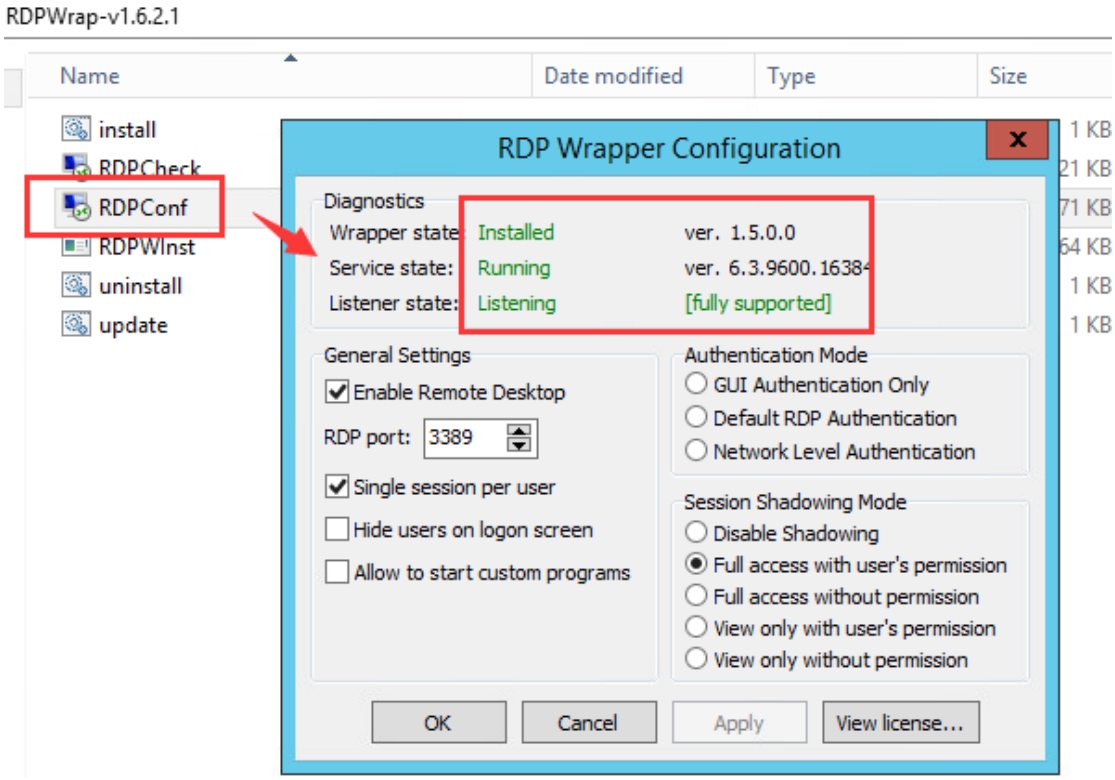
③ Replace the “rdpwrap.ini” file in the path of C:\Program Files\RDP Wrapper with the downloaded one.



④ Start “Remote Desktop Services”.



⑤ Run the "RDPconf.exe" file again to check if the multi-user patch is running properly.



- **Microsoft RDS CALs**

Refer to the following link to install the Microsoft RDS CALs

https://www.microsoft.com/en-us/Licensing/product-licensing/client-access-license.aspx

Note:

1) Microsoft RDS CALs are only available to Windows Server System installation. If you need to use Microsoft RDS CALs, please install Windows Server System (Server OS) first.

2) Run the RDP Wrapper files after extracting them to your local disk. Do not run them in the compress file.

3) Disable the security software and the Windows Defender before running install RDP Wrapper.

2.2.4 VLC Media Player

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs, and various streaming protocols. Beginning from vMatrix 2.0, vCloudPoint introduced a new feature that allows local videos played on the zero client with VLC player to be rendered locally by the client processor instead of the host cpu. This feature offloads 90% host-side CPU consumption on video playing and can help support more video users per host especially for cases where simultaneous video play is often required.

VLC player is obtainable at http://www.videolan.org/vlc/ or the official website of vCloudPoint: www.vcloudpoint.com/support/add-ons/.

Note:

1) Please install VLC player of 2.1.5 or newer versions.

2) As the media content is not rendered at the host side, there is a drawback of using this feature: media content within the VLC player cannot be viewed by the administrator through monitoring at the host side.

3) When running a video with VLC player, desktop refreshment of the desktop session other than the VLC player area will slow down. Therefore, to ensure desired performance, do not have a VLC player running at the back-end while you are running other applications.

4) vCloudPoint zero client rendering with VLC player only supports H.264/MPEG-4 AVC encoding format videos. H.265/HEVC videos played through VLC player will be lagging. The file suffix shown in the video file name is package format. If you encounter a video lagging problem, you can use “Mediainfo” to check the actual encoding format.

Chapter 3. Installation & Connection

3.1 vMatrix Installation

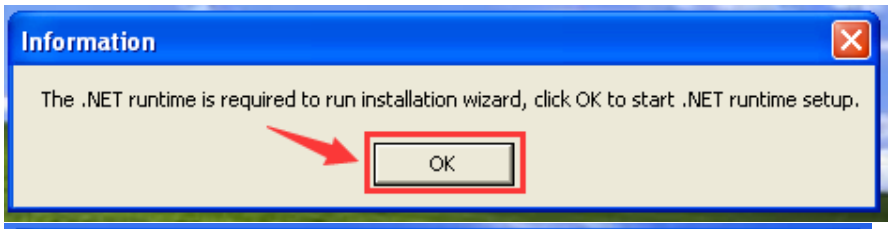
Before installation

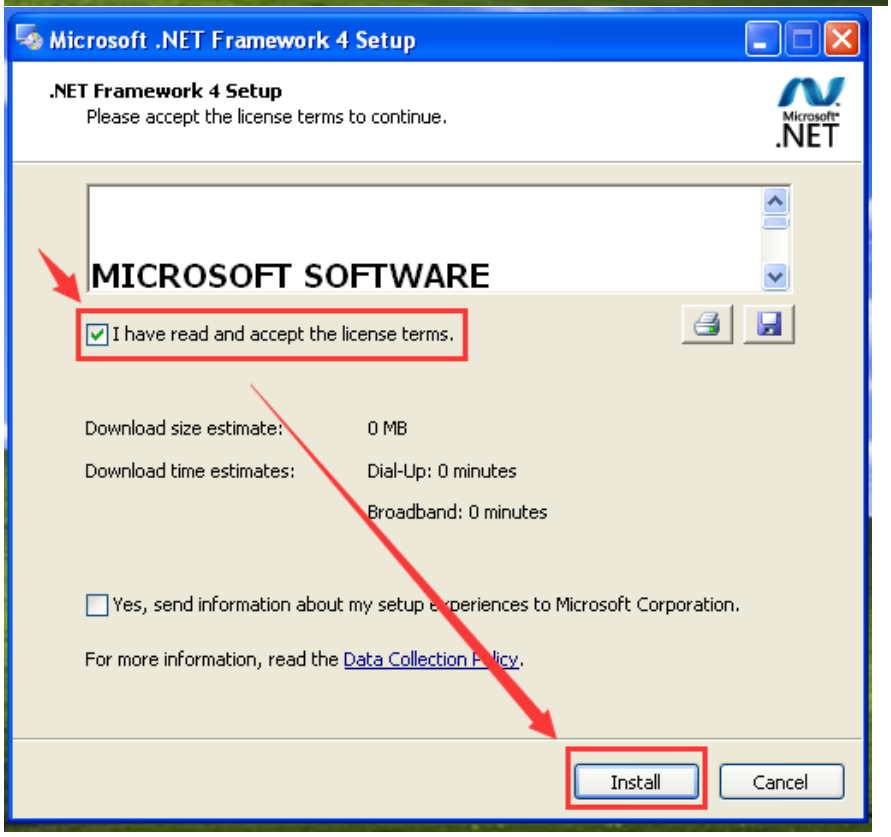
- It is recommended to use the new original operating system to avoid problems such as installation failure or use error due to file corruption or loss of the old system.
- Please download the original Windows system image on the official website of Microsoft to ensure system security and functional integrity.
- Please make sure to DISABLE secure boot (It is not necessary to disable the secure boot option in win10 or above systems) in the mainboard, and any Anti-Virus or Firewall software during the installation of vMatrix Server Manager. After installation has completed, you may re-enable Anti-Virus and Firewall software.
- The host hard disk is recommended to be partitioned into 3: a system C partition where the system and software are installed, a public partition for storing users' shared data and a private partition for storing users' personal date.
- Before installing vMatrix Server Manager, you are suggested to rename the computer name of the host.
- vMatrix Server Manager software requires Net framework 4.0 and VC++ 2010 Library on your host server, and vMatrix Server Manager will automatically install these two models during the process of installation.

Installation Steps:

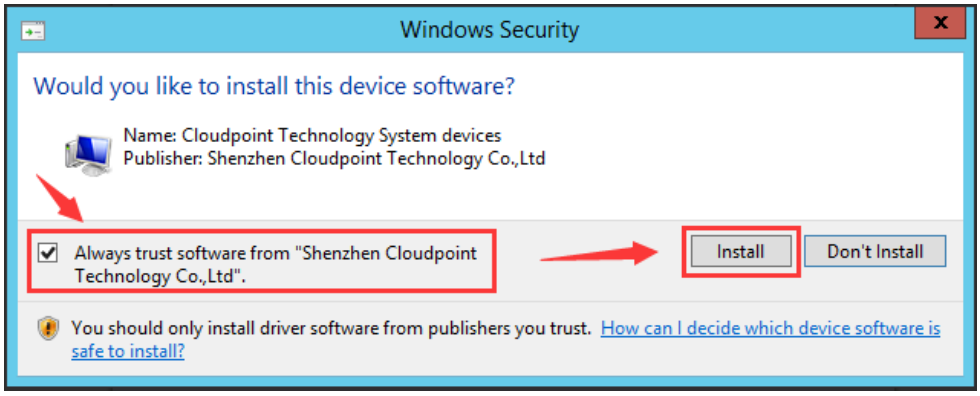
1) Run vMatrix installer. Click "**Install**" to start installation.

2) On initial installation, vMatrix Installer will detect if some required components are installed on the host. Allow installing required components if it prompts. For the Windows XP operating system, you have to manually install the components as shown below:



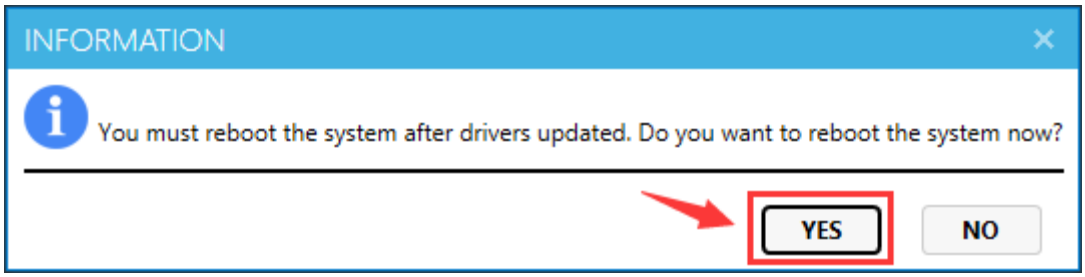


3) During installation, your will be prompted to install drivers, click “Install”. (This prompt will not be showed up in win 10 and later systems)

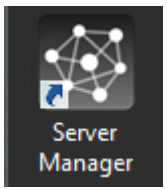


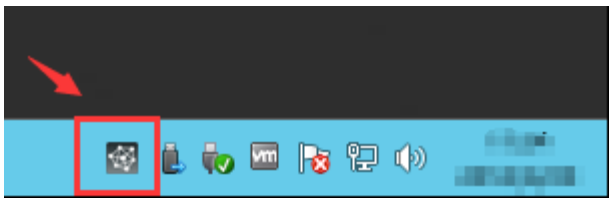
4) Click “Completed” and finish installation.

5) You will be asked to reboot the system. Click “yes”.

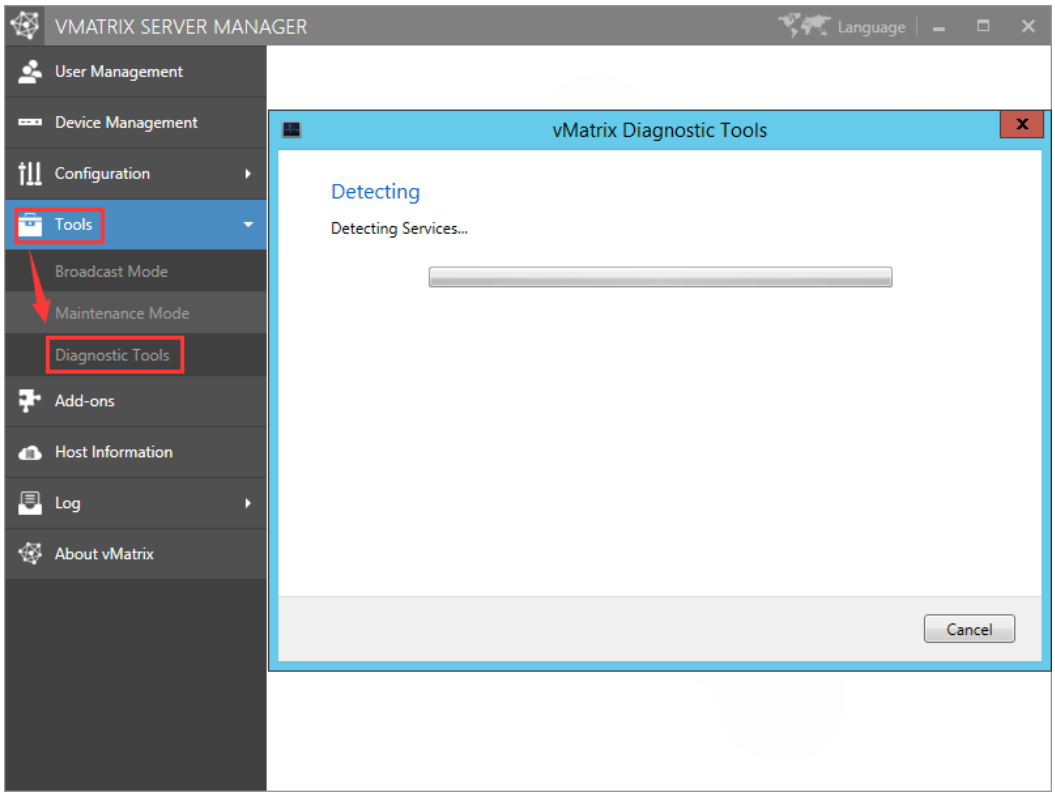


6) After reboot, double click the vMatrix icon at the desktop or click the vMatrix icon at the task tray to open vMatrix Server Management console.





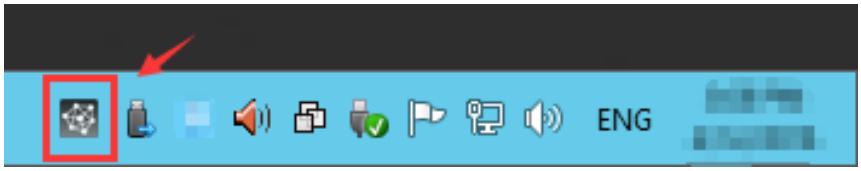
7) Run the “Diagnostic Tool” under the “Tools” menu to check if the vMatrx Server Manager is running properly. Follow the prompts to fix if there is any issue.



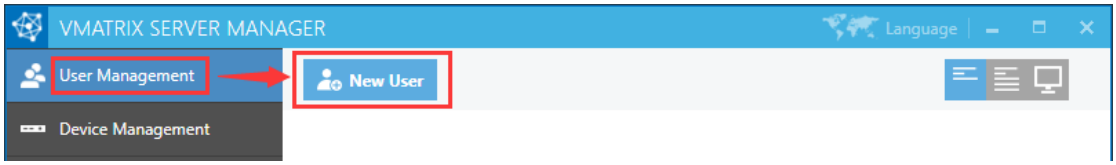
8) After vMatrix Server Manager is running properly, install Microsoft RDS CALs or RDP wrapper to support multi-user login.

3.2 User Creation

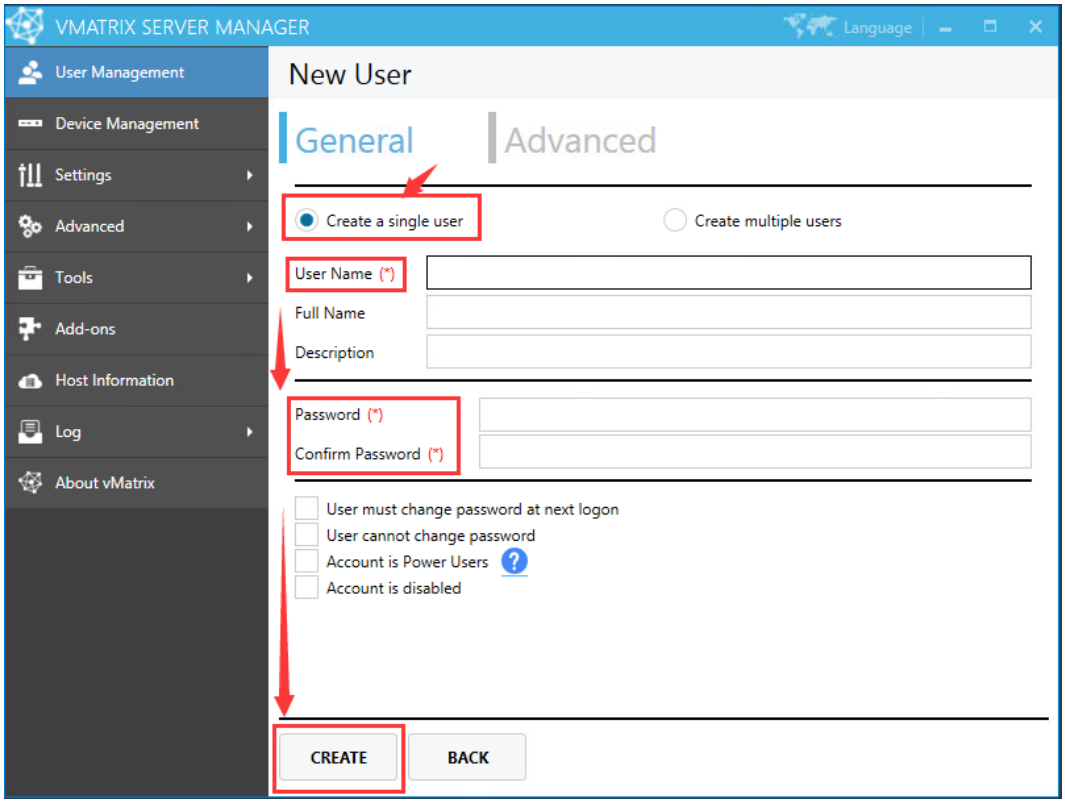
1) Open vMatrix Server Manager console.



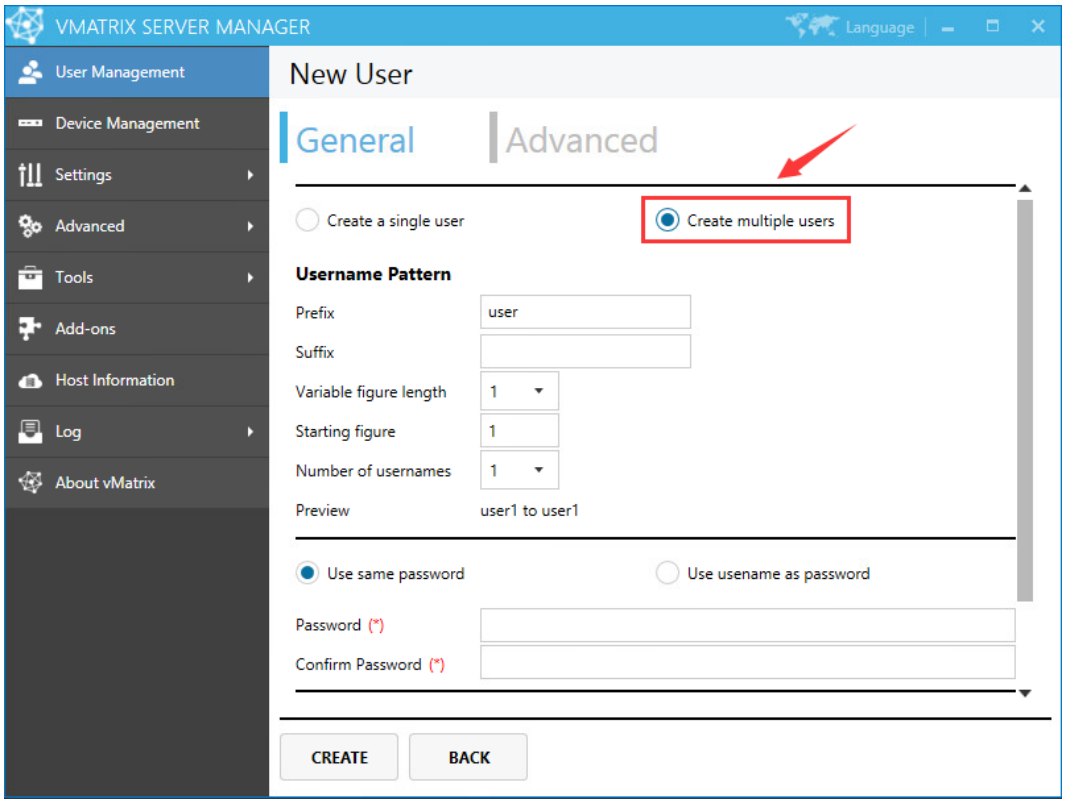
2) Go to “User Management” page, click “New User” to create user accounts.



Enter “User Name” and “Password” and click “Create” at the bottom.



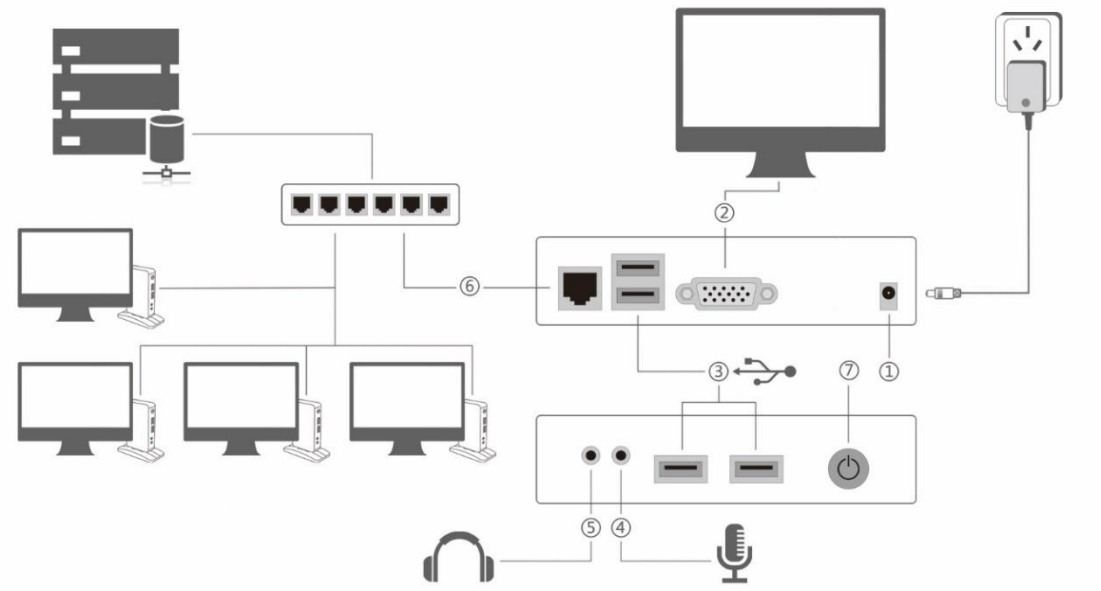
To create multiple users at a time, select “Create multiple users”, and then select the number of users and enter passwords or select to use user name as password for all users.



3.3 Device Connection

Connect the zero client to other peripherals as shown below.

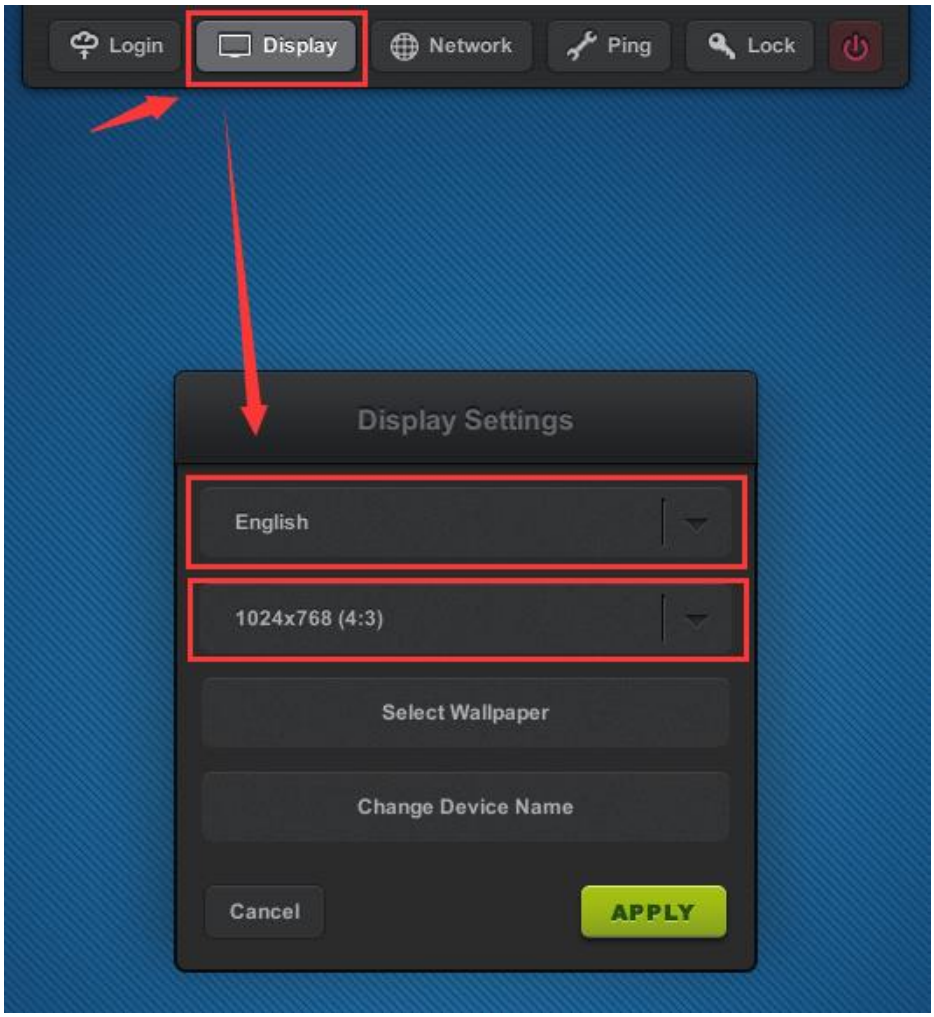
- Connect the zero client to the power adapter of 5V, 2A. Do not use power adapter of other specifications to avoid damage to the zero client.
- Connect the zero client to a monitor with VGA or HDMI port.
- Connect the zero client to USB keyboard and mouse and other USB devices if necessary.
- Connect the zero client to Mic and speaker through 3.5mm jacks if necessary (Audio devices through USB ports are also supported).
- Connect the zero client to the network through RJ45 type Ethernet cable to the switch or USB wireless antenna built with RT8188 chipset.
- Power/reset button, short press to power on, long press to reset the terminal.



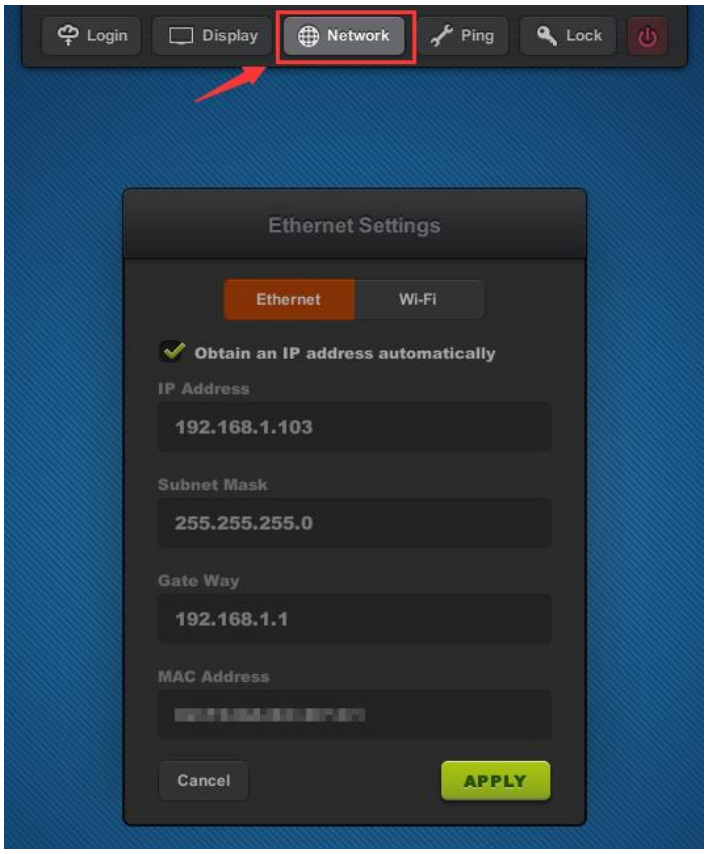
3.4 Device Login

1) After connecting to the peripherals, press the device power button.

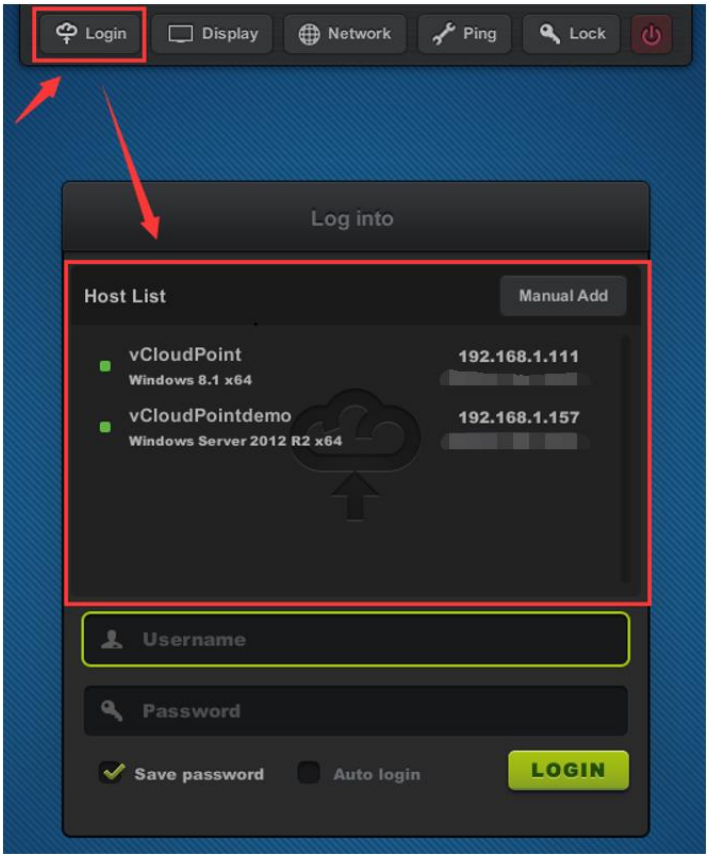
2) After system boot, go the display page, select your correct language and desktop resolution; factory default language is “English” and desktop resolution is “1024x768”.



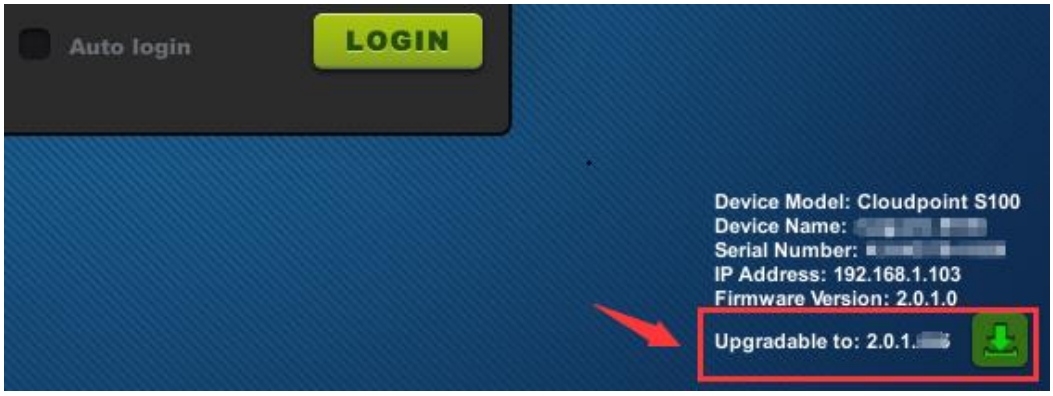
3) Go to “Network” page. If DHCP network service in available in your network, you can just use the default setting to obtain an IP address for this device automatically. Otherwise if you want to allocate an IP address manually, cancel the option and enter an IP address instead.



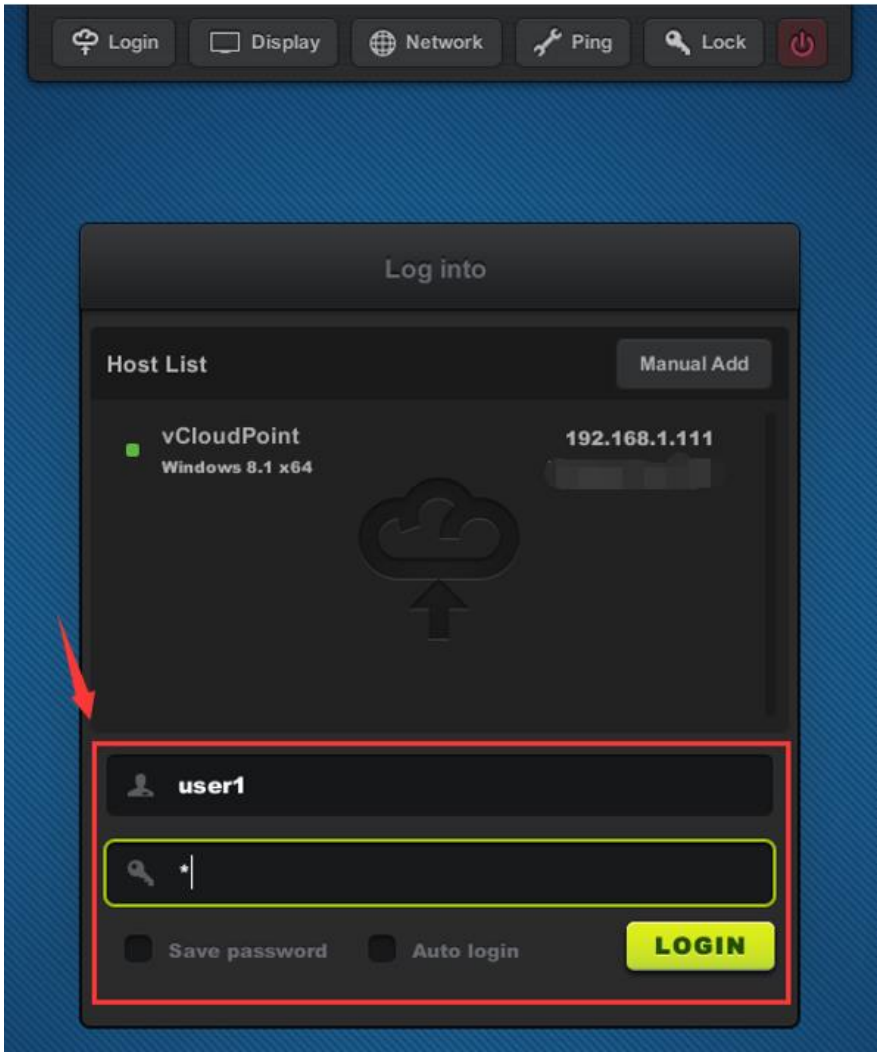
4) Go back to the “Login” page, select the host available in your network for connection.



5) Check for any new firmware to upgrade at the right bottom of the screen. If yes, click to upgrade.



6) Enter your user name and password, then click “Login”. If you use a new created user for initial login to the host, you may need to wait a few seconds to minutes for preparing a desktop.



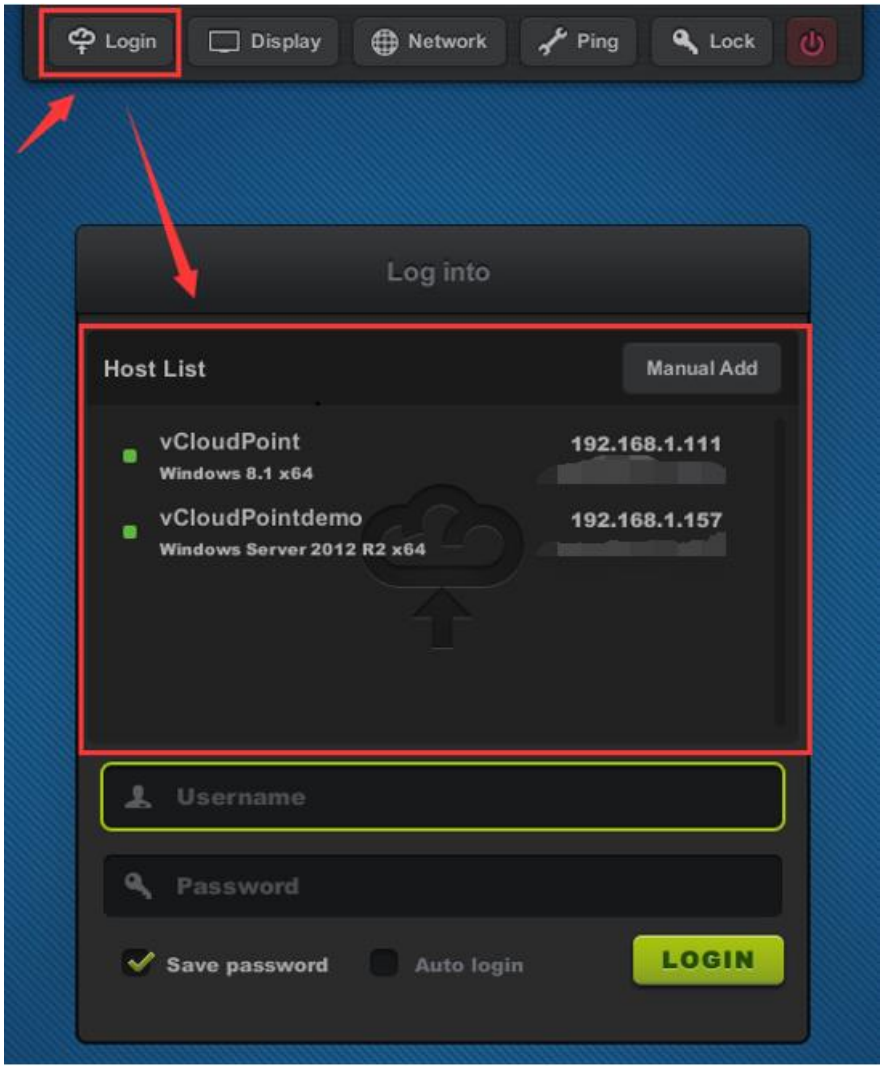
Chapter 4. Using the Zero Client

4.1 Menu Settings

4.1.1 Login

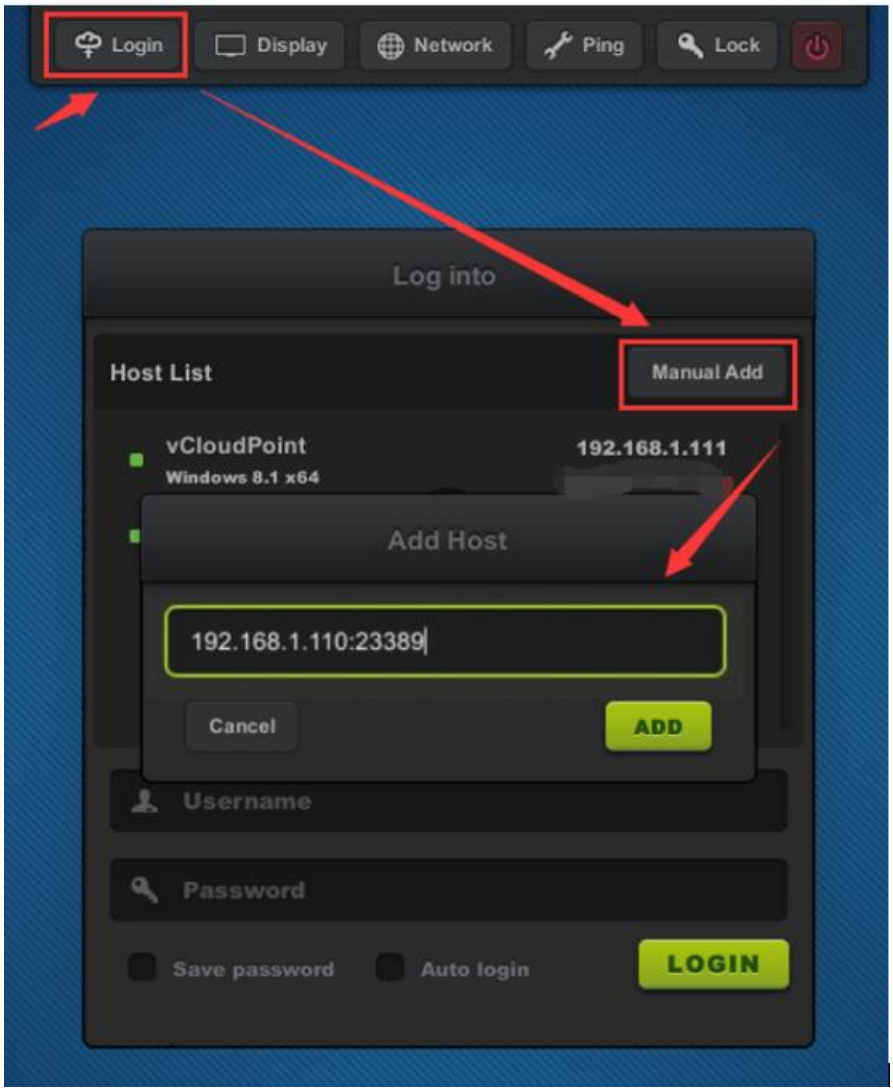
- Host List window shows all available hosts in the network. Host to be shown in the list are:

1) hosts with vMatrix Server Manager properly installed and running.
2) hosts in the same network segment as the device.



- To connect to an available host not shown in the list, you can manually add the host IP through the “Manual Add” button ((vMatrix default network port is 13389, if you have manually changed the port, add the port number when you manually add the

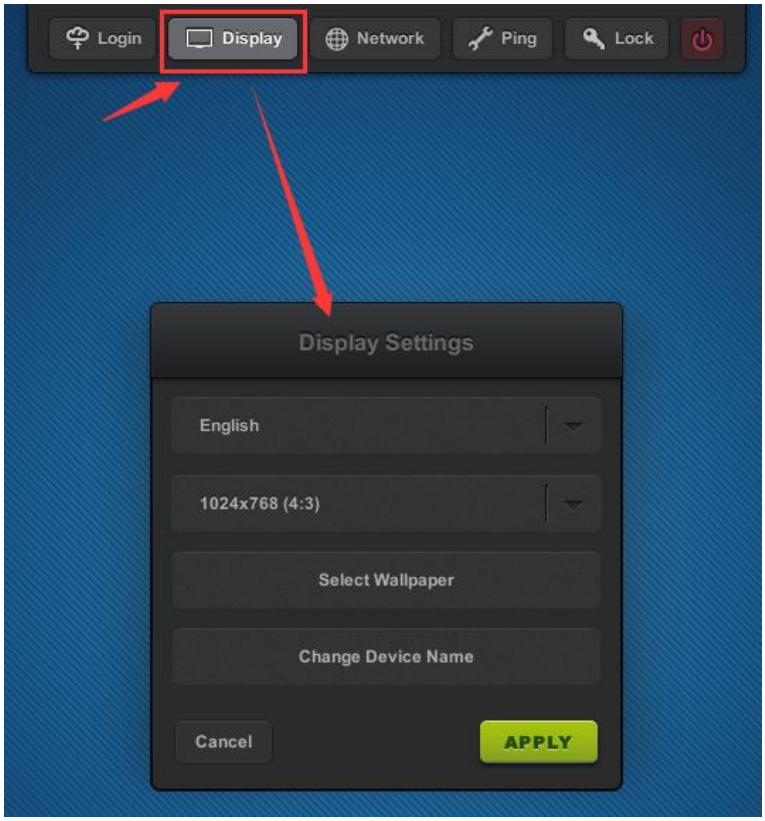
host).



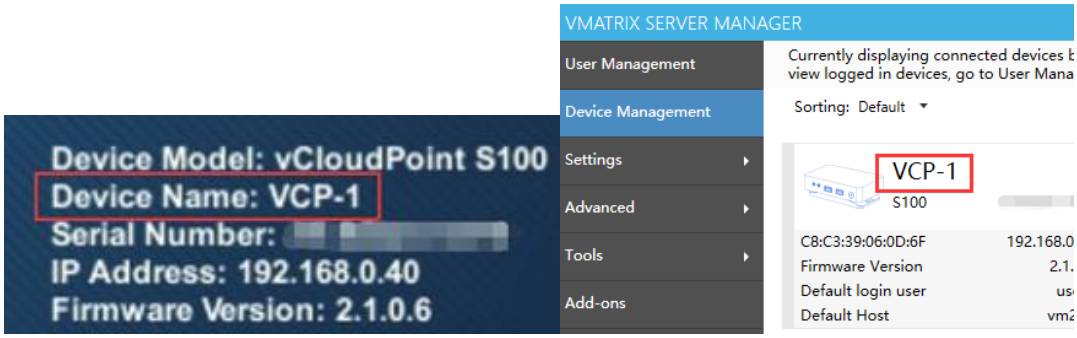
Note:

- Early version firmware of the terminal cannot fill in the port number when adding the host IP and use 13389 by default.
- Early version firmware of the terminal cannot find the hidden host even “Manual Add”.

4.1.2 Display



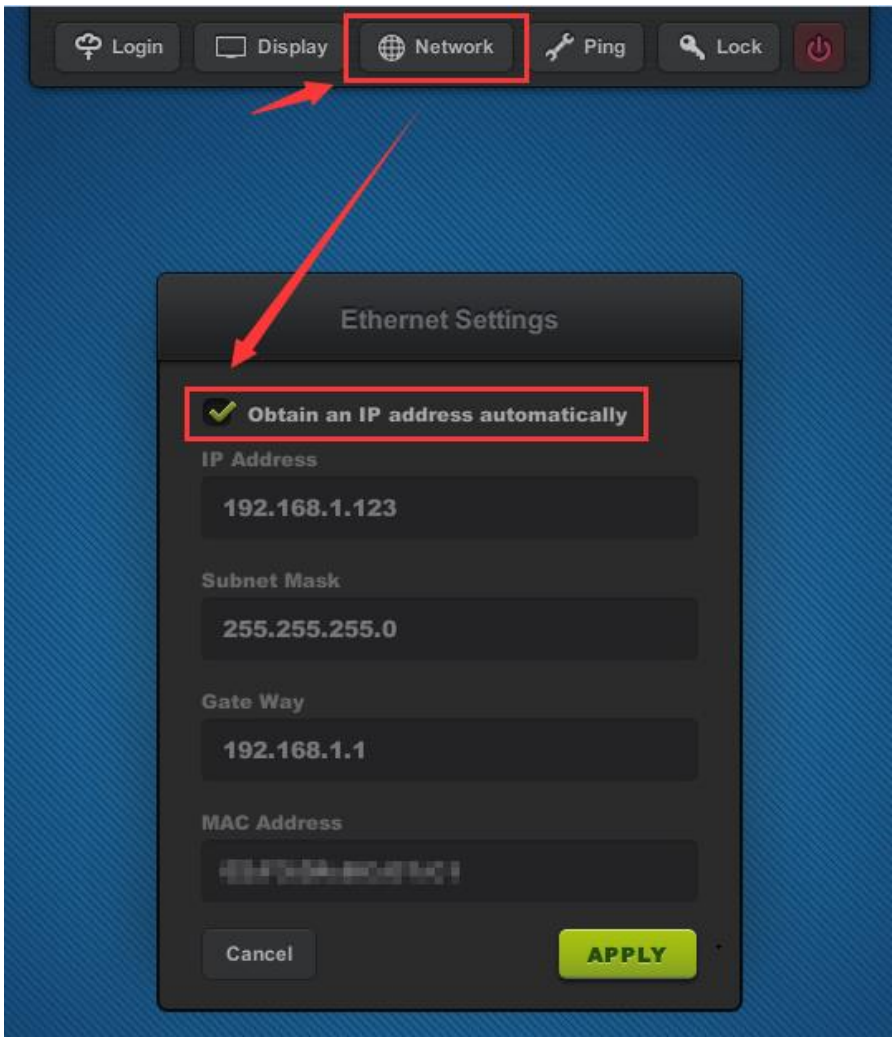
- **Language:** to change the device language; available languages: English Chinese, Russian, default: English.
- **Resolution:** to change the resolution for the device interface and user desktop; default: 1024x768 (4:3), maximum: 1920x1080.
- **Wallpaper:** to change wallpaper for the device interface.
- **Device Name:** to change device name; default: S100- (last 8 serial numbers). Device name is shown at the right bottom of device interface and User Management page on vMatrix Server Manager.



4.1.3 Network

Ethernet Settings

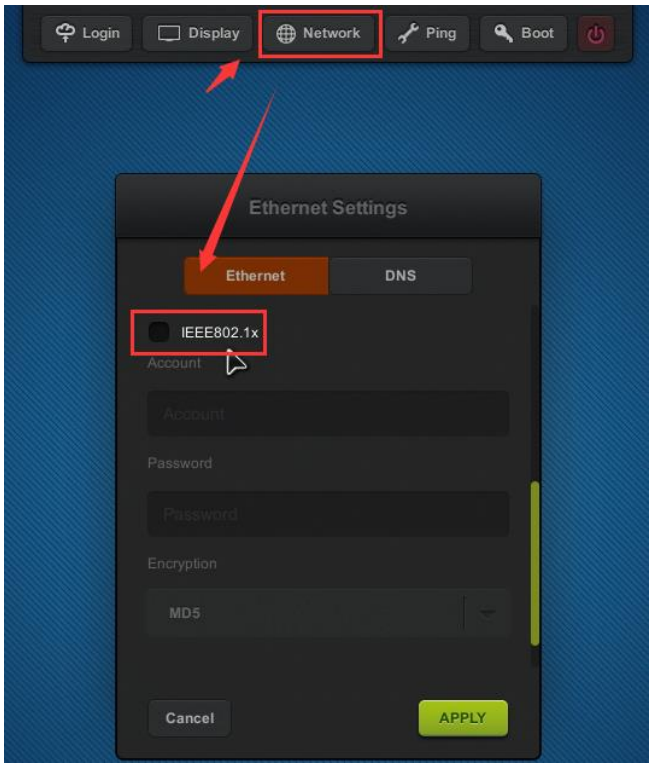
If DHCP network service in available in your network, you can just use the default setting to obtain an IP address for this device automatically. Otherwise, if you want to allocate an IP address manually, cancel the option and enter an IP address instead.



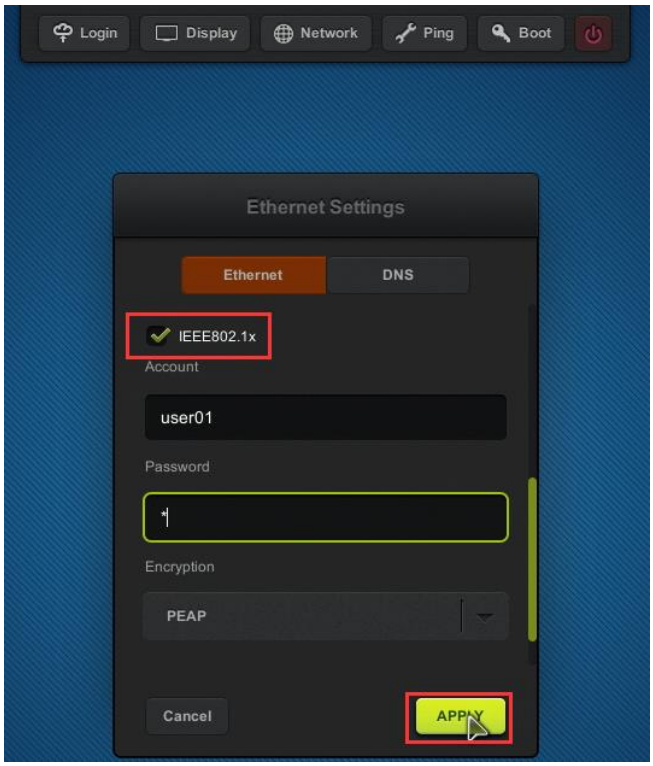
Note: IP address of the client device is for communication in LAN with vMatrix Server Manager only (for device management). After connecting to the host, the user desktop session will share the IP address of the host for network communication (for session management). If you want each user desktop session to have their own IP address, you need to enable IP virtualization at vMatrix Sever Manager.

IEEE802.1X

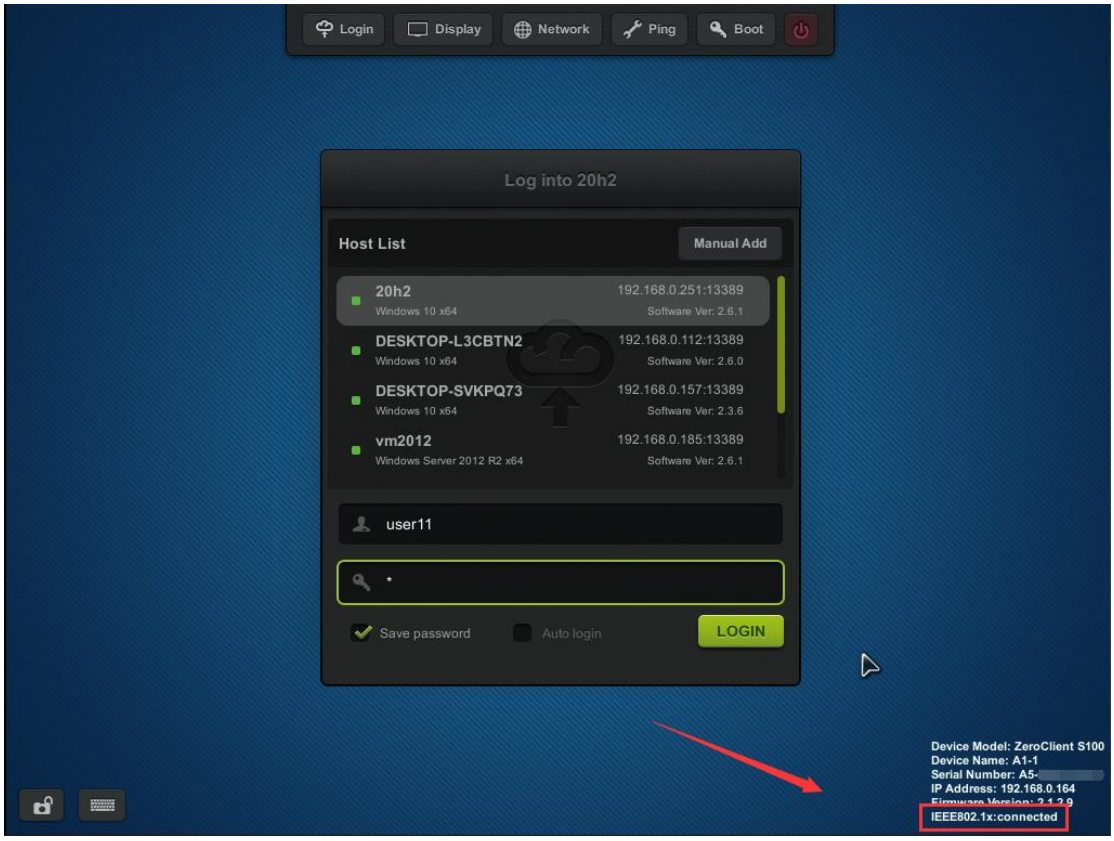
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides
an authentication mechanism to devices wishing to attach to a LAN or WLAN.
(More information：https://en.wikipedia.org/wiki/IEEE_802.1X)



How to use:
1) Connect the terminal device to the network that needs authentication.
2) Check to enable "IEEE802.1x", enter the correct account and password, select the corresponding encryption method and click "apply". (Currently only supports MD5 and PEAP two encryption methods.)



3) After the verification is passed, it successfully accesses the LAN and can log in to the host normally to use.



Note:

1) There are 3 states of IEEE802.1x: disabled, disconnected, connected.

- Disabled: IEEE802.1x is disabled.
- Disconnected: IEEE802.1x is enabled but failed to be authenticated and access the local network. (Possible cause: The account password or encryption method is incorrect, please check the log of the authentication server for detailed information)
- Connected: Successfully authenticated and connected to LAN.

2) If the terminal device is connected to a normal network instead of a network that requires authentication, enabling the IEEE802.1x authentication function will not have any impact.

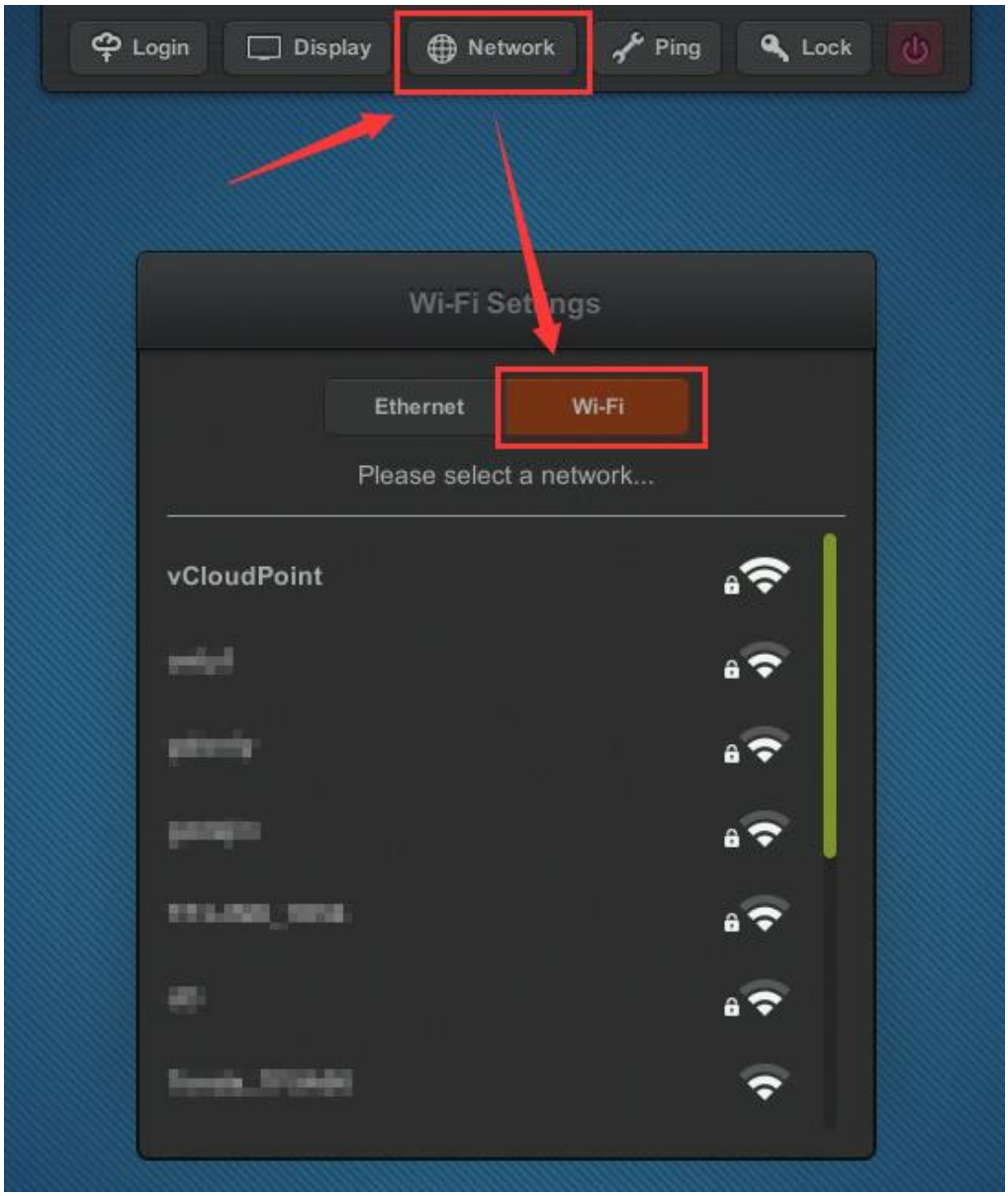
3) Currently only supports MD5 and PEAP two encryption methods, and cannot be used based on wireless network.

WIFI Settings

You will see the WIFI Settings sub-page only when the device is a WIFI model or connected to a supported USB WIFI antenna on device boot.

1) Connect the USB WIFI antenna to the zero client, and power the zero client on.

2) Click the “WIFI” button to enter WIFI Settings page.



3) Double click the WIFI network you want to connect, and then enter password.

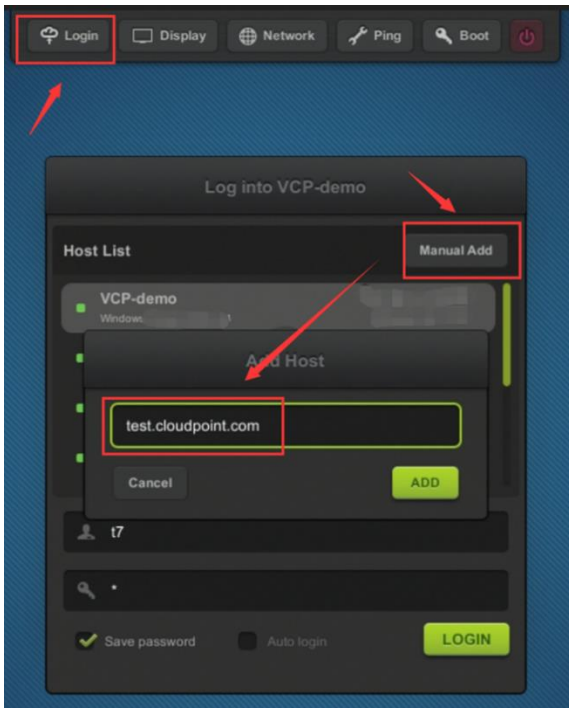
4) When the WIFI network you selected is displayed above the line divider, the WIFI connection is established.

Note:

1) Any antenna that is built with 2.4GHz RTL8188EUS/ETV chip or 5GHz RTL88xx chip and connects with USB 2.0 standard is supported by vCloudPoint zero clients.
2) Please connect the WIFI antenna before the zero client powered on.
3) Only one WIFI connection can saved on the zero client.
4) There is no option for entering the name of a WIFI option on the zero client; therefore, you cannot hide the name (SSID) of the WIFI network that you are decide to connect.
5) Although the vCloudPoint zero clients are with an WIFI option, for a reliable user experience, you are recommended to connect them through Ethernet cable, as WIFI network may fluctuates and causes unexpected lags and disconnections during operation.

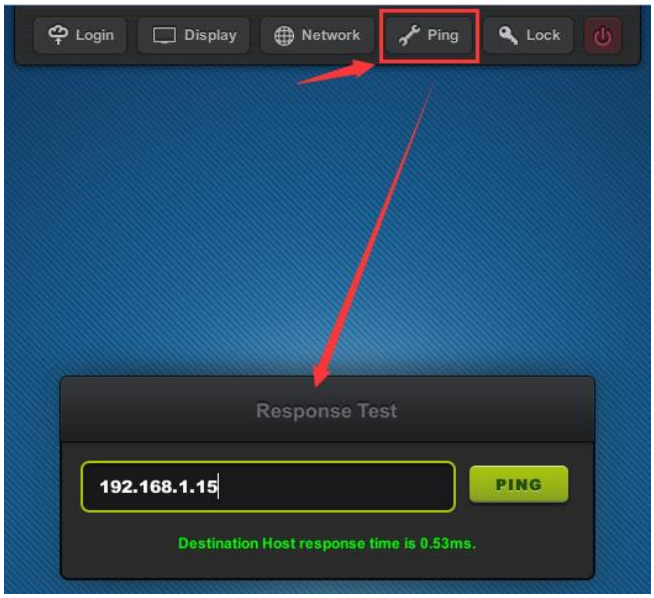
- **DNS Settings**

You could change the DNS of zero clients on this interface manually(If you leave the option with blank, zero clients will resolve IP address with DNS received from DHCP server) and you could use search vmatrix server host with domain name on login interface.



4.1.4 Ping

Ping test is to check the network connectivity between the current device and other device, usually the destination host in the network. Simply enter the IP address of the destination device and click the PING button. If you see a green message saying the response time, the network between these two devices connected fine.

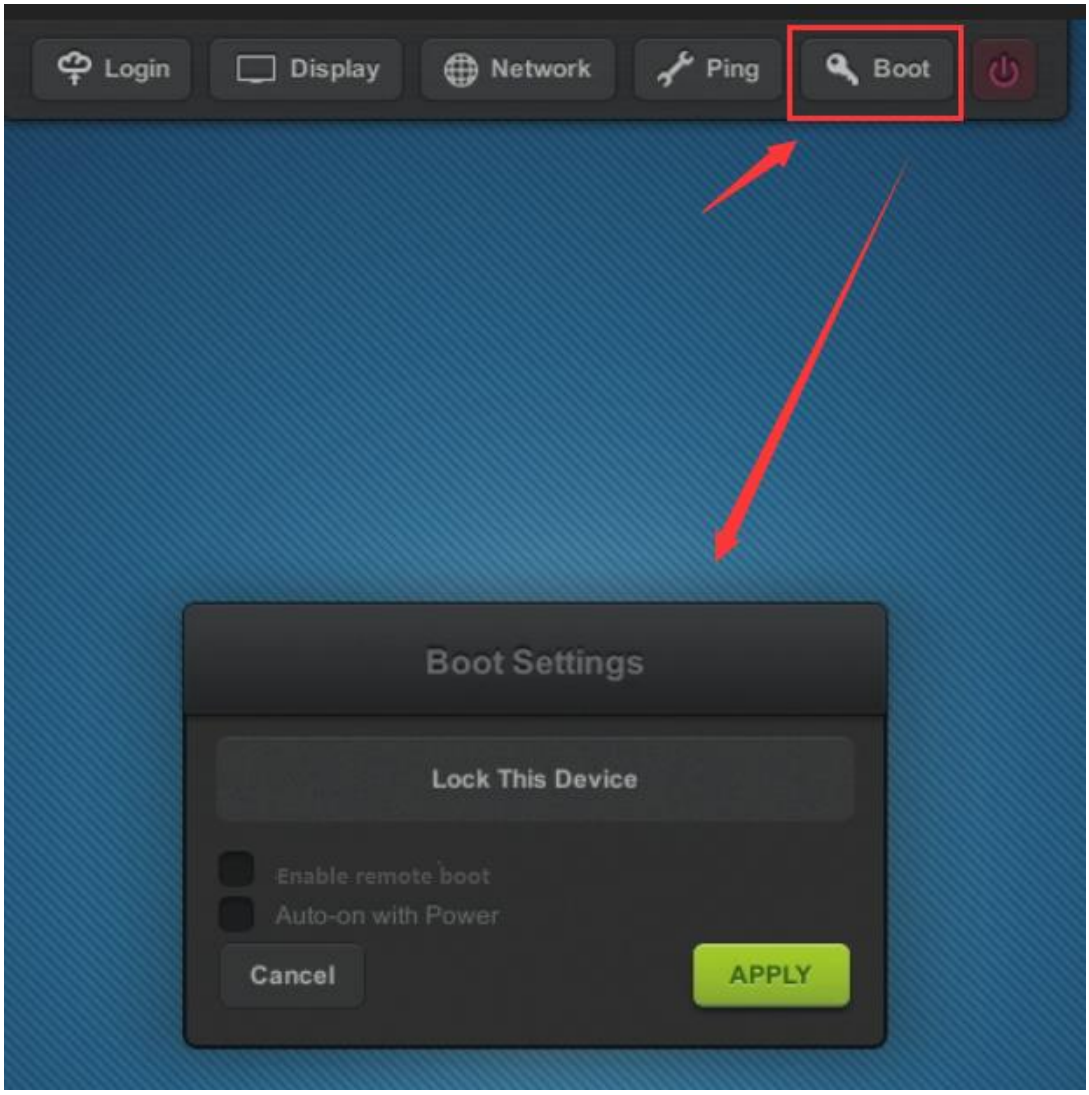


Note:

The shorter the response time, the better the connection. If the response time is too high, terminal operation will delay.

4.1.5 Boot

- To lock the device is to set up a password on device boot so that the user is required to enter password to use the device.
- When the option of “Enable remote boot” is checked, the client device can be booted from the server manager. (The client device can be powered on remotely only after it is powered off remotely via the management software or via the shutdown button on the client device UI. The client device that is powered off via the physical power button cannot be powered on remotely.)
- When the option of “Auto-on with Power” is checked, the client device will be automatically powered on with power supply.



Note:

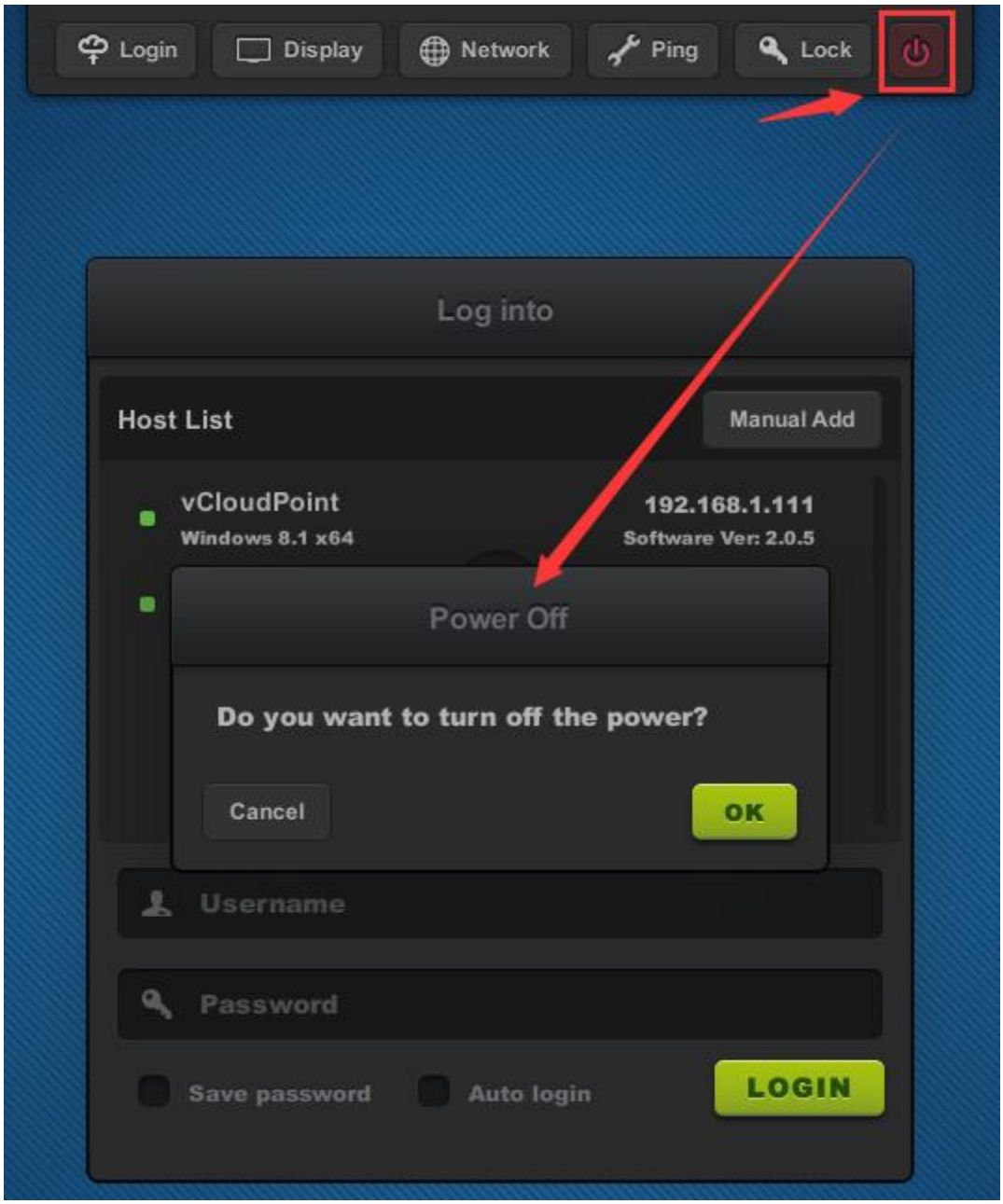
1) To unlock the device, just clear the password and apply.

2) If you forget the password, you have to reset the firmware to the factory default one.

3) Auto-Power function is not available with client devices with serial number starting with A1, A2 and A3.

4.1.6 Shutdown Button

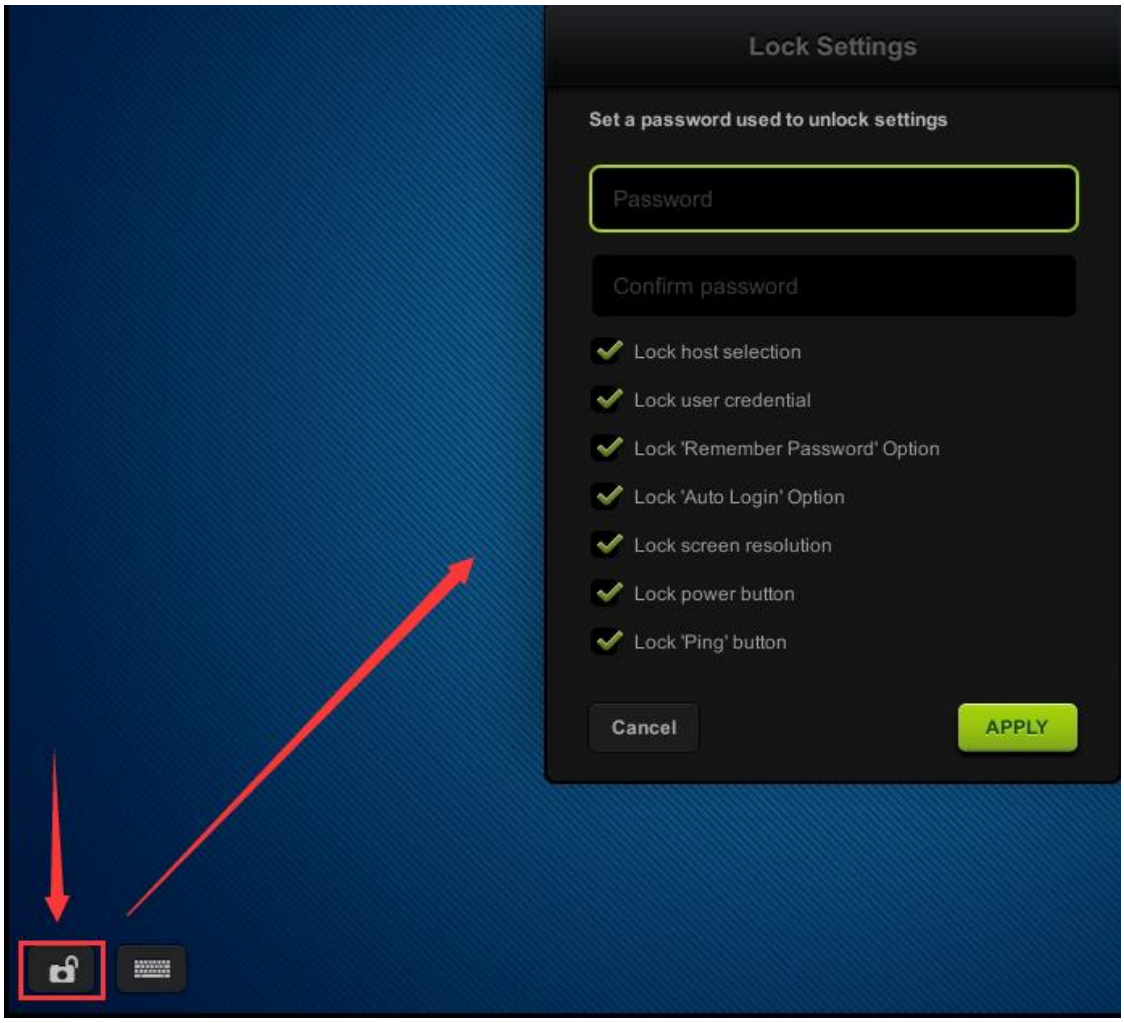
This button allows you to turn off the device without pressing the physical button on the device. This is helpful when the device is mounted at the back of the monitor.



4.2 Settings Lock

To lock settings is to lock down the settings on the Login, Display, Network and Lock menu in order to prevent other users from changing these settings.

- **Lock host selection:** to disable the host selection and force the user to login to the selected host. A host must be selected before this option is selected.
- **Lock user credential:** to disable the user to change user name and password and force the user to login with the saved user name and password. A correct user name and its related password must be saved before this option is selected.
- **Lock remember password and auto-login:** Check this option; remember password and auto-login will be locked.
- **Lock screen resolution:** to lock down resolution of the device and the desktop session. You can uncheck this option to lock other configurations, and users will not be able to customize other settings except for the resolution.
- **Lock shutdown button:** Check this option; the "Power Off" button in the upper right corner of the terminal interface will be locked.
- **Lock ping button:** Check this option; you will not be able to enter the ping page.



Note:

1) To unlock the device, click the icon in the lower left corner, enter the correct password and apply.

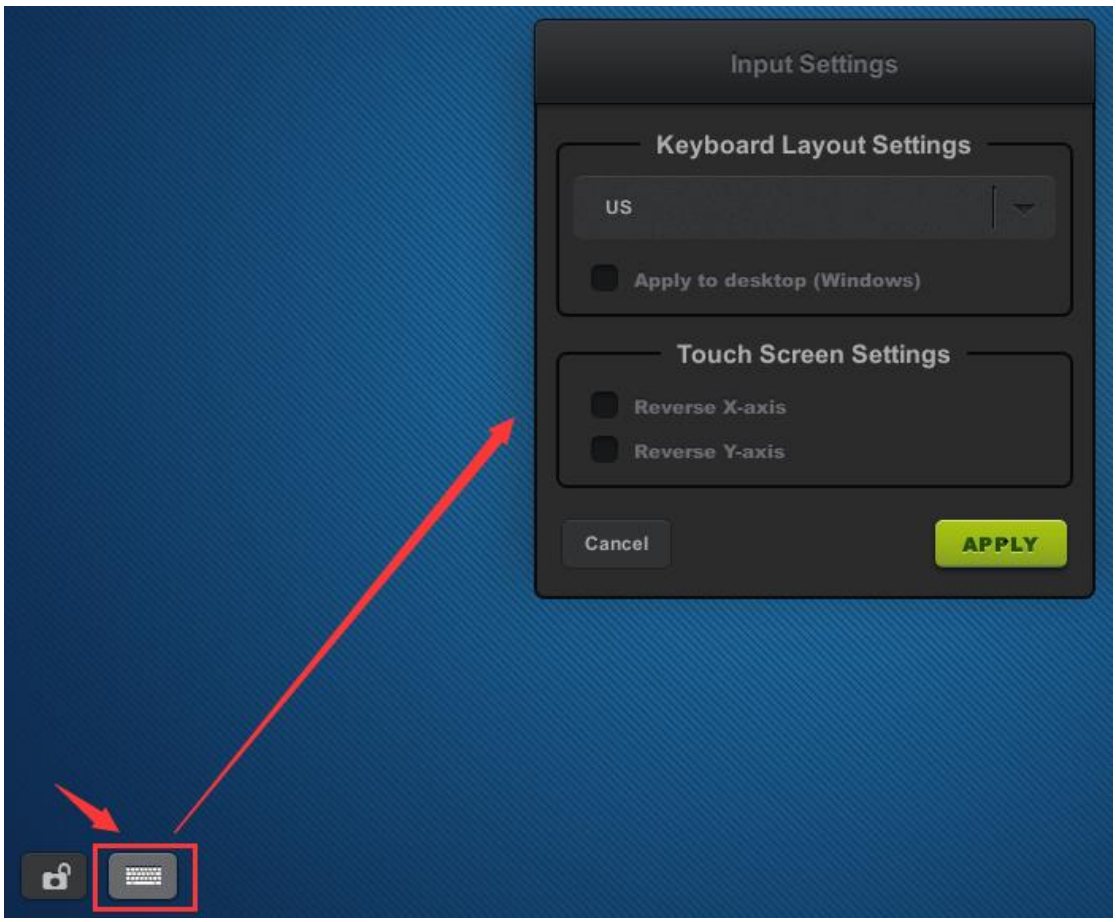
2) If you forget the password, you can:

- Select and right click the terminal to unlock the device at Device Management of vMatrix Server Manager.
- Long press the power button when the terminal is off to reset the firmware to the factory default one.

4.3 Keyboard Layout Settings

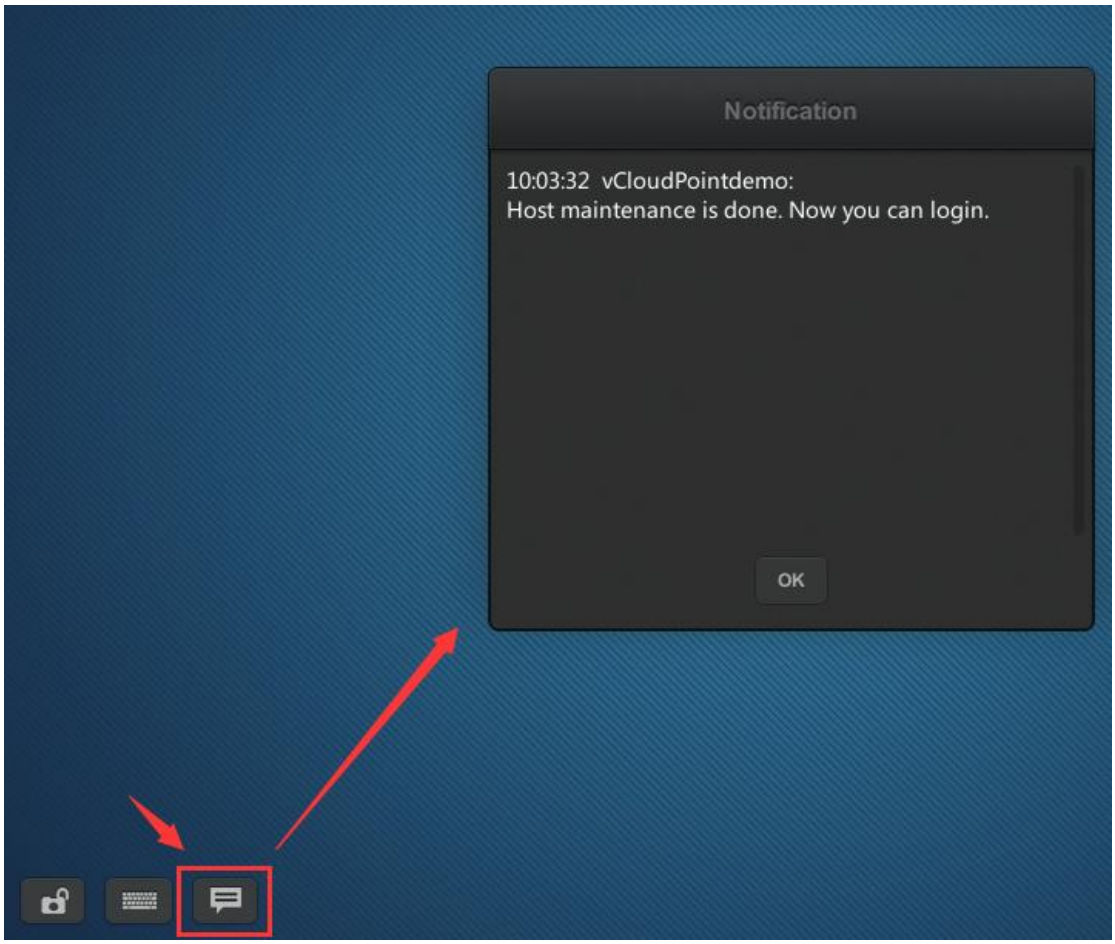
- **Keyboard Layout Settings:** to set up the language of the keyboard input; 111 languages are available, defaulted US; if the option “Apply to desktop (Windows)” is not selected, the setting applies to input on the device interface only.

- **Touch Screen Settings:** to set up the display direction when using touch screen for the device display. “Reverse X-axis” is to change the display direction from left-to-right to right-to-left. “Reverse Y-axis” is to change the display direction from up-to-down to down-to-up. vCloudPoint zero client supports Multi Touch Screens.



4.4 Notification Log

To view notifications sent to this device from vMatrix Server Manager on the host side. The notification icon displays only when there is notification sent to this device.



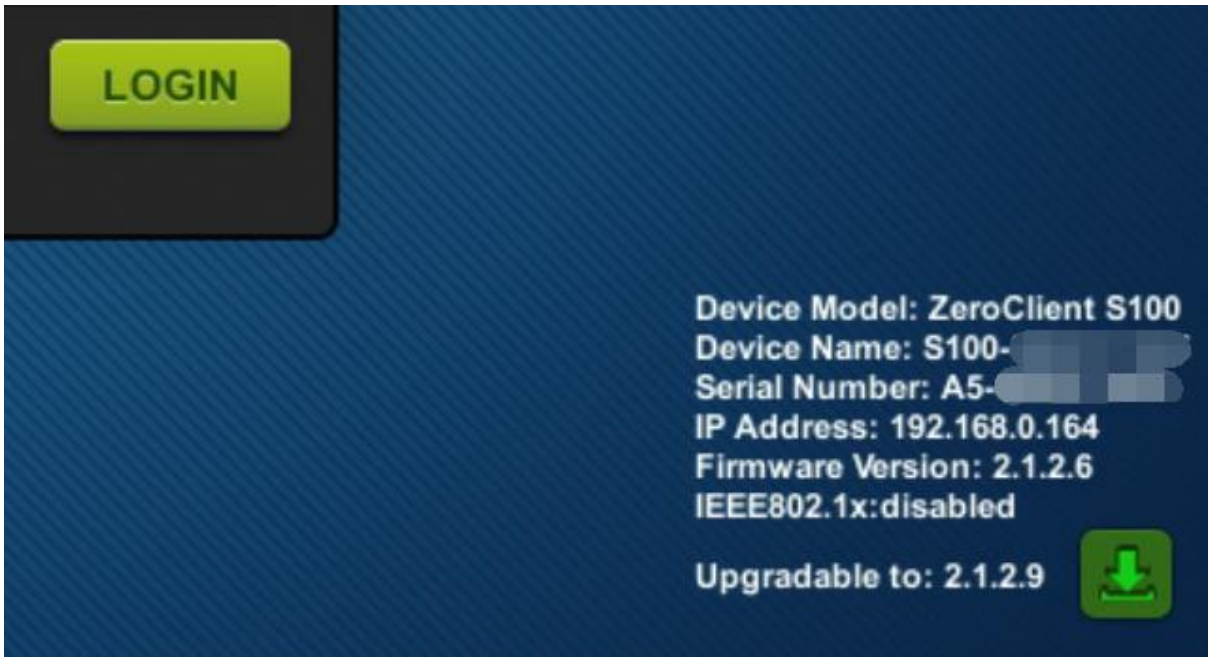
Note: Notifications will be cleared on each reboot or shutdown of the device.

4.5 Device Information

At the right bottom screen of the device interface, you can view the device information including:

- **Device Model:** the model of the device;
- **Device Name:** the name of the device; can be changed at the Display page;
- **Serial Number:** the unique 12-digit numbers for each device;
- **IP Address:** the IP address of the device in the LAN.
- **Firmware Version:** the current device firmware version.
- **IEEE802.1X:** The current working status of the IEEE802.1x.
- **Upgradable to:** the latest version of device firmware that is available in the network.

Click the download button to update.

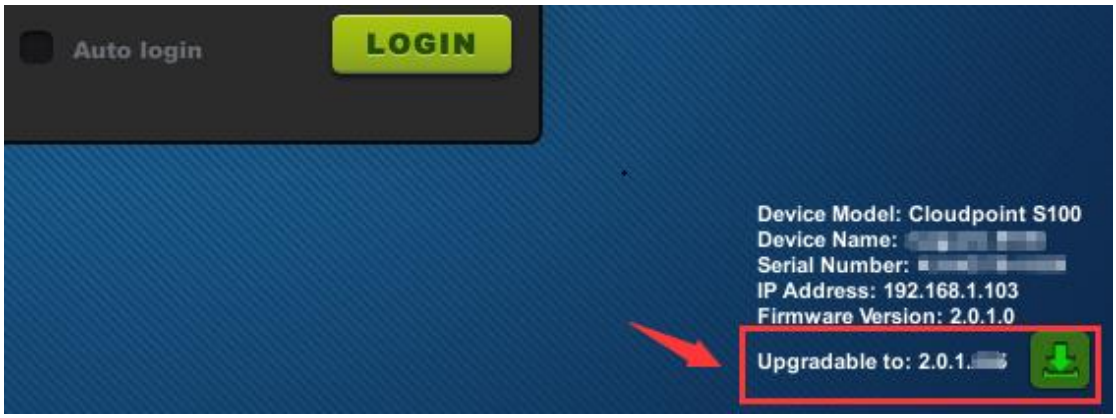


4.6 Firmware Update

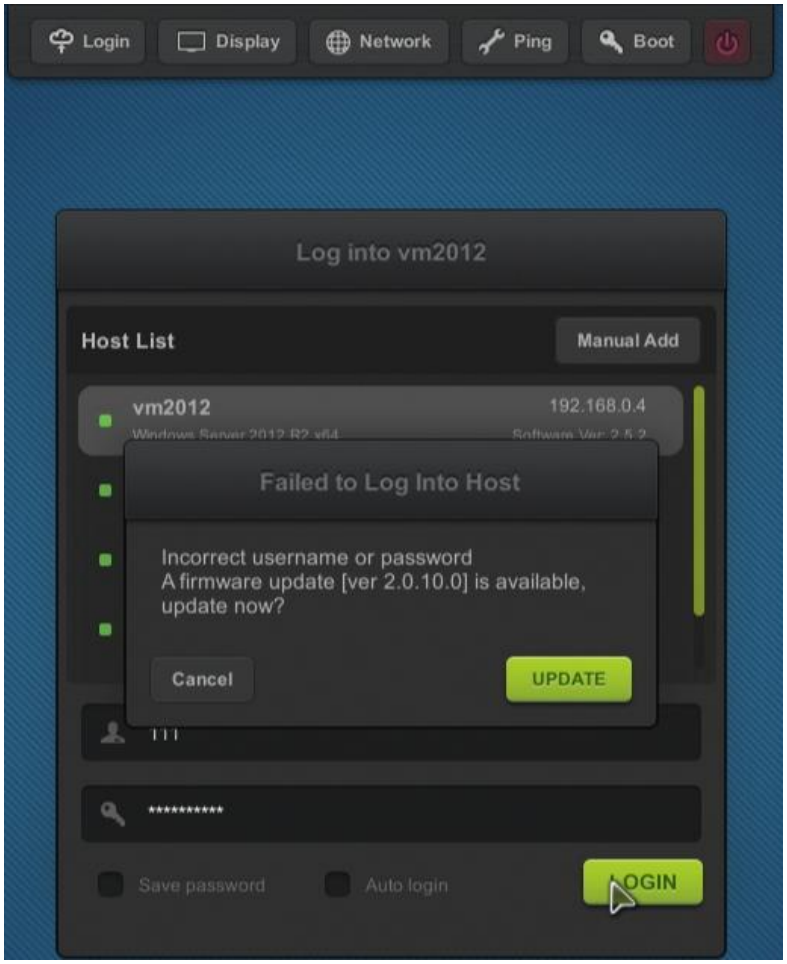
It is always recommended to use the latest available version of firmware on your vCloudPoint zero client. Each installation of vMatrix Server Manager includes the latest firmware, so no additional downloads are necessary to complete this process. When powered on, the zero client establishes connection with vMatrix Server Manager and checks for update, if there is a new version available. Firmware update is not always required when a new version of vMatrix Server Manager is used. However, some firmware of the device may be incompatible with the vMatrix Server Manager. In this case, firmware update is required for logging to the host.

There are three ways for you to update the firmware:

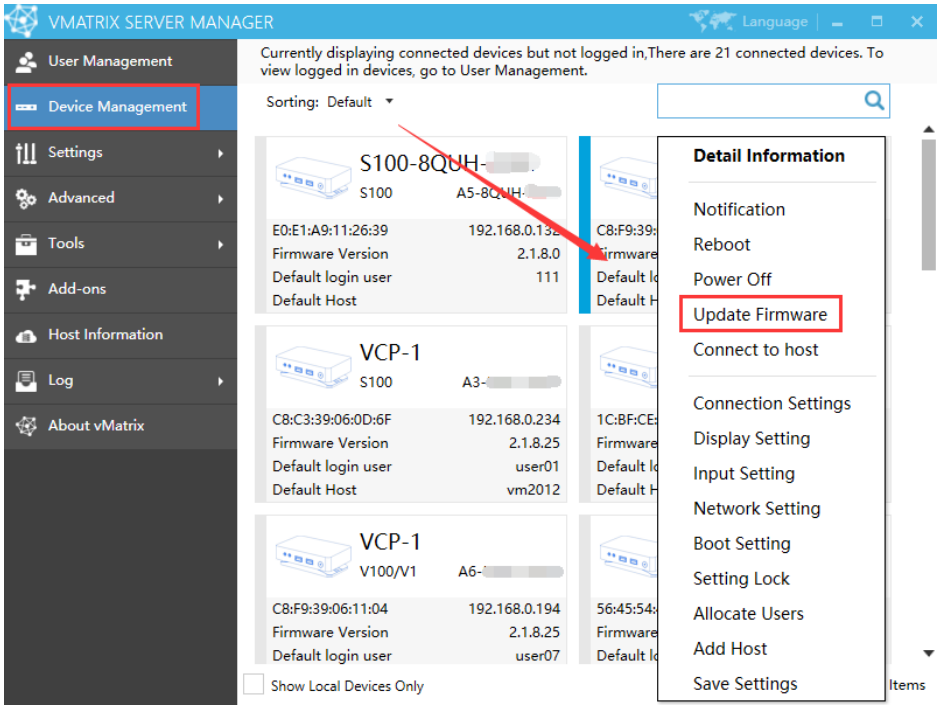
1) Click the download icon at the right bottom screen to update to the latest version available in the network.

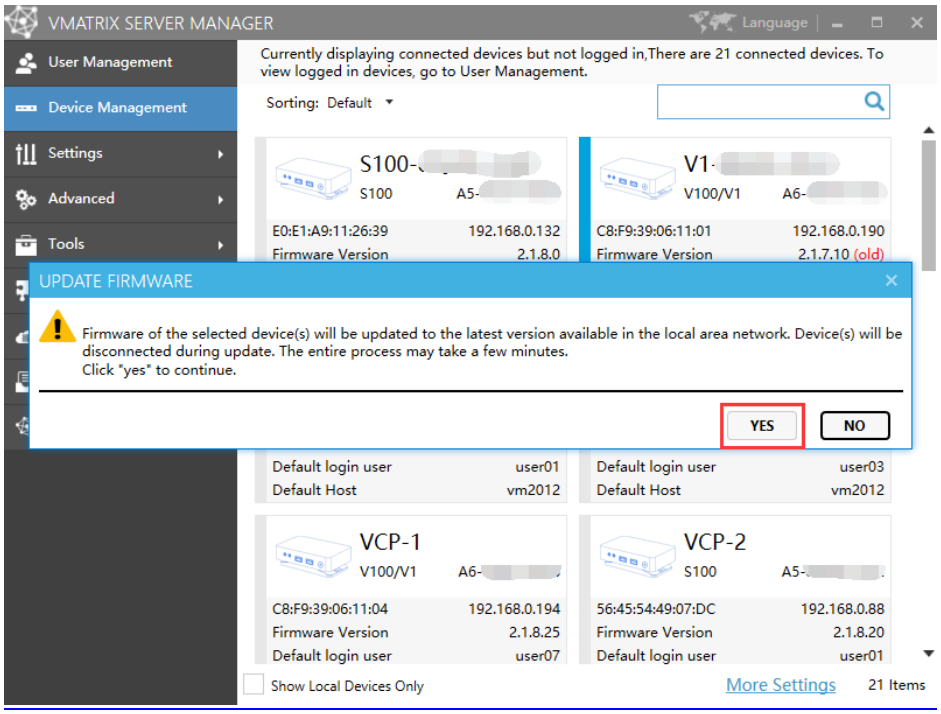


2) Select a host and purposely enter incorrect user name and password. Simply click the "UPDATE" button on the pop-up window to update with the new firmware (if there is) included in the vMatrix Server Manager on the host.



3) Select the terminal required to be updated in the Device Management page of the server manager. Right click to open menu and click "Update Firmware" .


VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Add-ons
Host Information
Log
About vMatrix
Currently displaying connected devices but not logged in,There are 21 connected devices. To view logged in devices, go to User Management.
Sorting: Default
S100-8QUH-
S100
E0:E1:A9:11:26:39
Firmware Version 2.1.8.0
Default login user 111
Default Host
VCP-1
S100
C8:C3:39:06:0D:6F 192.168.0.234
Firmware Version 2.1.8.25
Default login user user01
Default Host vm2012
VCP-1
V100/V1
C8:F9:39:06:11:04 192.168.0.194
Firmware Version 2.1.8.25
Default login user user07
Detail Information
Notification
Reboot
Power Off
Update Firmware
Connect to host
Connection Settings
Display Setting
Input Setting
Network Setting
Boot Setting
Setting Lock
Allocate Users
Add Host
Save Settings
Show Local Devices Only
Items


VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Currently displaying connected devices but not logged in,There are 21 connected devices. To view logged in devices, go to User Management.
Sorting: Default
S100-
S100
E0:E1:A9:11:26:39 192.168.0.132
Firmware Version 2.1.8.0
V1-
V100/V1
C8:F9:39:06:11:01 192.168.0.190
Firmware Version 2.1.7.10 (old)
UPDATE FIRMWARE
Firmware of the selected device(s) will be updated to the latest version available in the local area network. Device(s) will be disconnected during update. The entire process may take a few minutes.
Click "yes" to continue.
YES
NO
Default login user user01
Default Host vm2012
Default login user user03
Default Host vm2012
VCP-1
V100/V1
C8:F9:39:06:11:04 192.168.0.194
Firmware Version 2.1.8.25
Default login user user07
VCP-2
S100
56:45:54:49:07:DC 192.168.0.88
Firmware Version 2.1.8.20
Default login user user01
Show Local Devices Only
More Settings
21 Items

Note:

- Please DO NOT pause update and make sure the connection between host and device is reliable during firmware update. If the firmware is damaged, please reset and update again.
- No matter which method is used to update the firmware, you must ensure that the firmware version attached to the host is higher than the terminal firmware version before to update.
- Please keep the firmware up to date and avoid upgrading across multiple versions.
- The first and third upgrade methods will upgrade to the latest firmware in the LAN by default, and the second upgrade method will upgrade to the latest firmware included in the selected host.

4.7 Reset

Reset Configuration

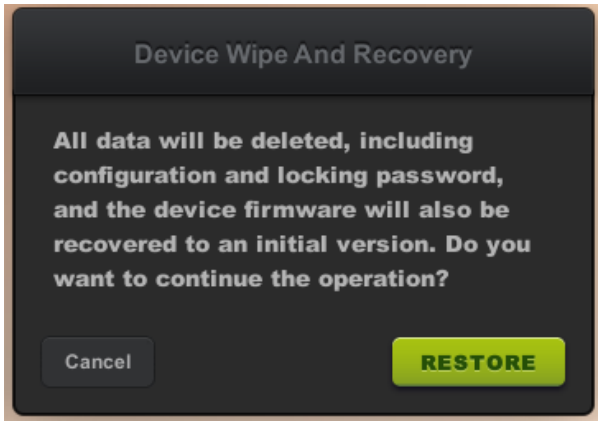
- press F2 key on device boot.

This is to restore all custom configurations to factory default. This is often used for restoring desktop resolution which is out of range of the monitor to 1027x768. If the Setting Lock is enabled, you are required to enter password.

Reset Firmware

- long press the switch button until you see the resetting window.

This is to reset the device firmware to the factory installed one. All configurations will be recovered to the factory defaults. This is often used when device system turns faulty or is damaged by improper firmware upgrade.



Note: The new batch of cloud terminals adds password verification when restoring factory settings. The password is the last character of each segment of the terminal serial number, and is case sensitive. (eg: The password of A5-8QVC-2021 is 5C1.)

4.8 Disconnect & Logout

- **Disconnect:** to disconnect the user session; user session is still running, files and applications are still opened and in place when user connects again. There are two methods for a user to disconnect his session on host:

- right click on the vmatrix icon on the taskbar and click ”Disconnect”.
- press the power button of the device.

- **Logout:** to logout the user; the user's session is ended; files applications are closed. Right click on the system's window button, choose “Shutdown or logout”, and then “logout”.
- **Logout and shutdown:** logout the user session and power off the client device.

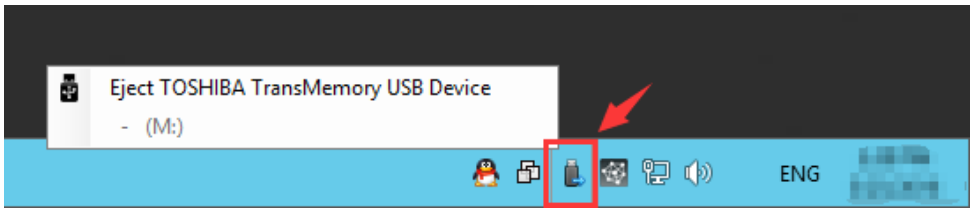
Note:

1) Terminal users have “Disconnect” and “Logout” for shut down option.

2) When the connection is disconnected, the user desktop session is still running on the host. If you do not use it. Please logout the user session and shutdown the client device when ending the work.

4.9 Use USB Devices

To use supported USB devices, simply connect them to the USB ports on the device. Some USB devices may require a driver to install on the host by an administrator. There is no client driver needed for the device. To avoid data loss or damage to a memory device plugged into the device, right click on the USB icon at the right task bar to eject the device before unplugging it.

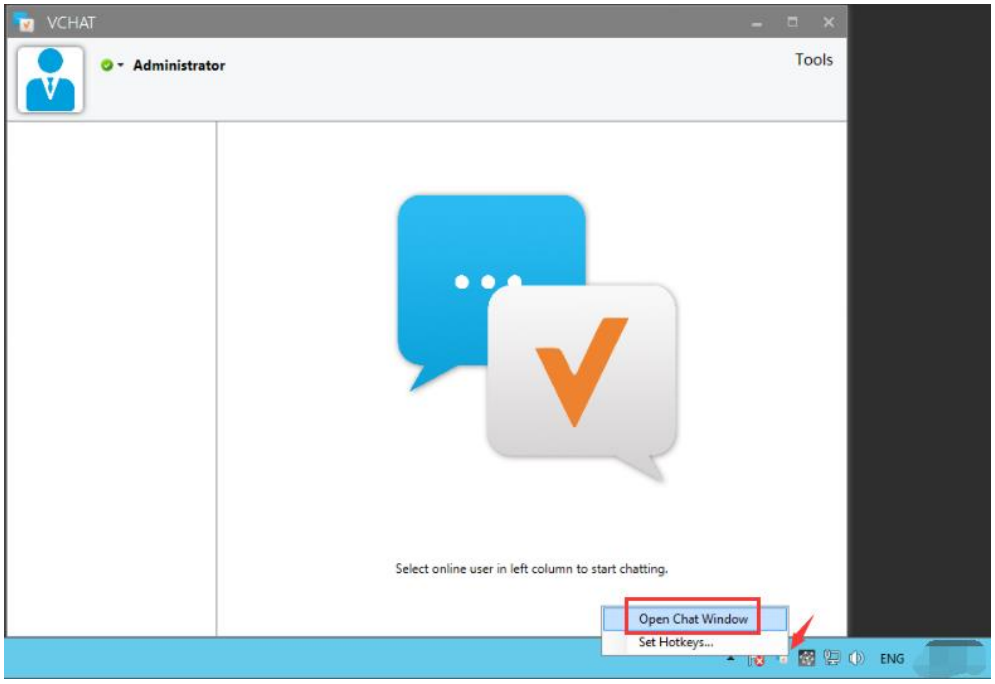


4.10 More Tools & Settings

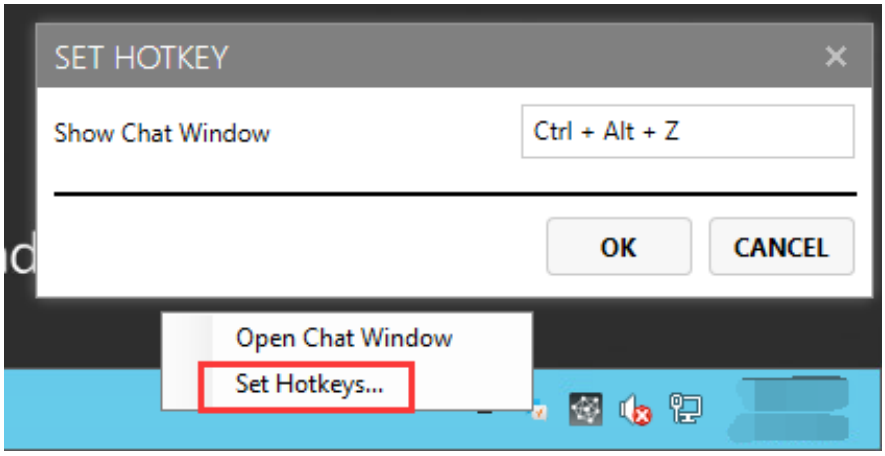
4.10.1 vChat Internal Messenger

The vChat Internal Messenger allows users to talk with other users in the same host.

- To run the vChat, right click on the vChat icon at the task bar and then click “Open Chat Window” or press the hotkey “CTRL” + “ALT” + “Z”.

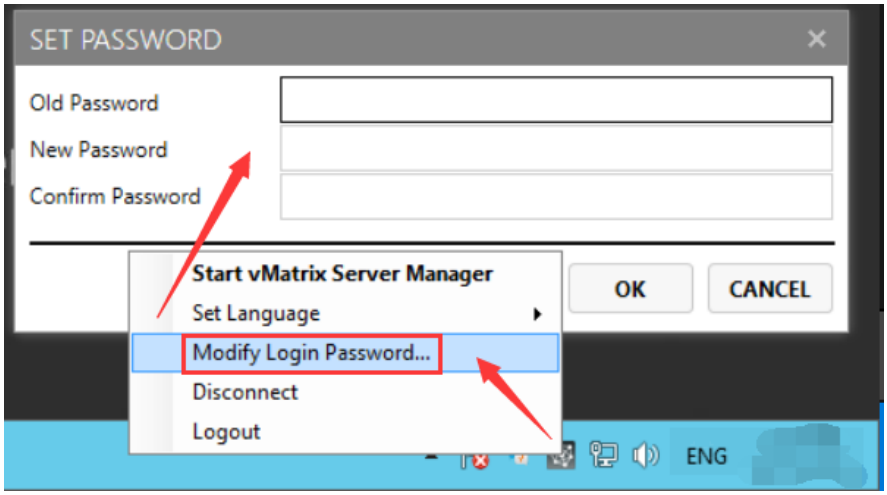


- Set the hotkey to open the chat tool. Right-click the vChat icon at the task bar, and click "Set Hotkeys" to set it.



4.10.2 Set Password

This allows the current user to reset his login password without doing at the system control panel. To reset password, right click on the vMatrx icon at the task bar, click on “Set Password …” and then enter passwords on the required fields.

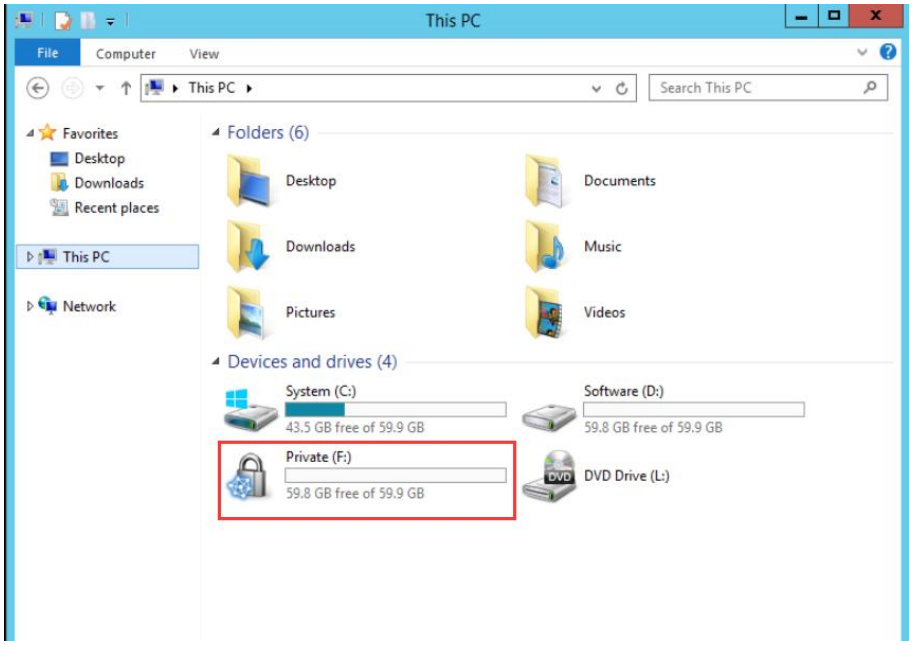


4.10.3 Set Language

This is to set language for displaying messages of the vCloudPoint system. Right click on the vMatrx icon at the task bar, click on “Set Language” and then available languages will be shown on the right.

4.10.4 Private Drive

The Private Drives marked with a lock icon are drives created by vMatrix Server Manager on an existing drive for storing terminal users' personal files. Files inside the Private Drives are visible to their owners and administrators. These files are inaccessible to other terminal users.



Note:

1) By default, the files on the user's desktop are stored in the C drive. It is recommended that users store personal files in Private Drive to prevent the issue of insufficient space of the C drive.

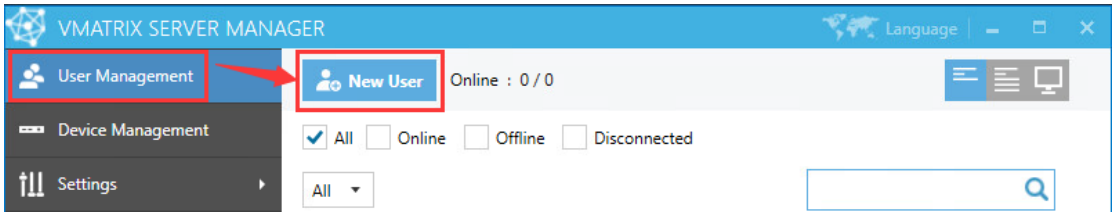
2) If a user deletes a file on the private disk, the file will be permanently deleted, and you cannot find the deleted file in the recycle bin.

Chapter 5. Using vMatrix Server Manager

5.1 User Management

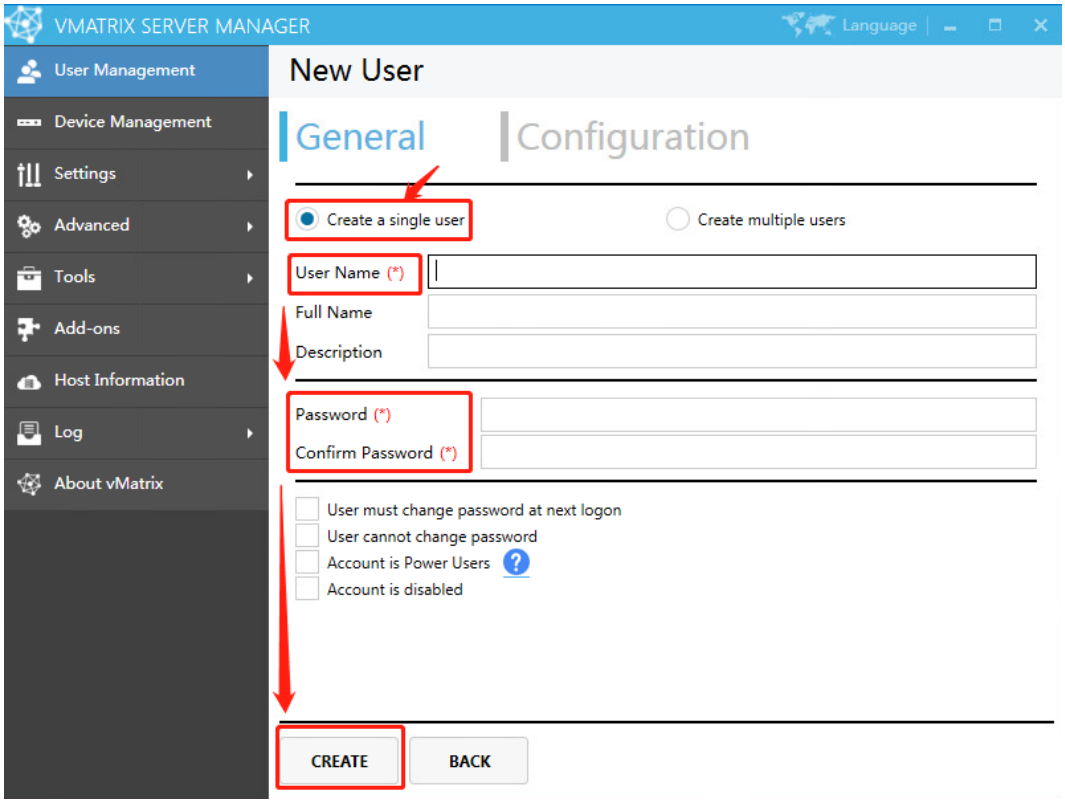
5.1.1 New User Creation

To create users, open vMatrix Server Manager, on the initial page, click “New User”.



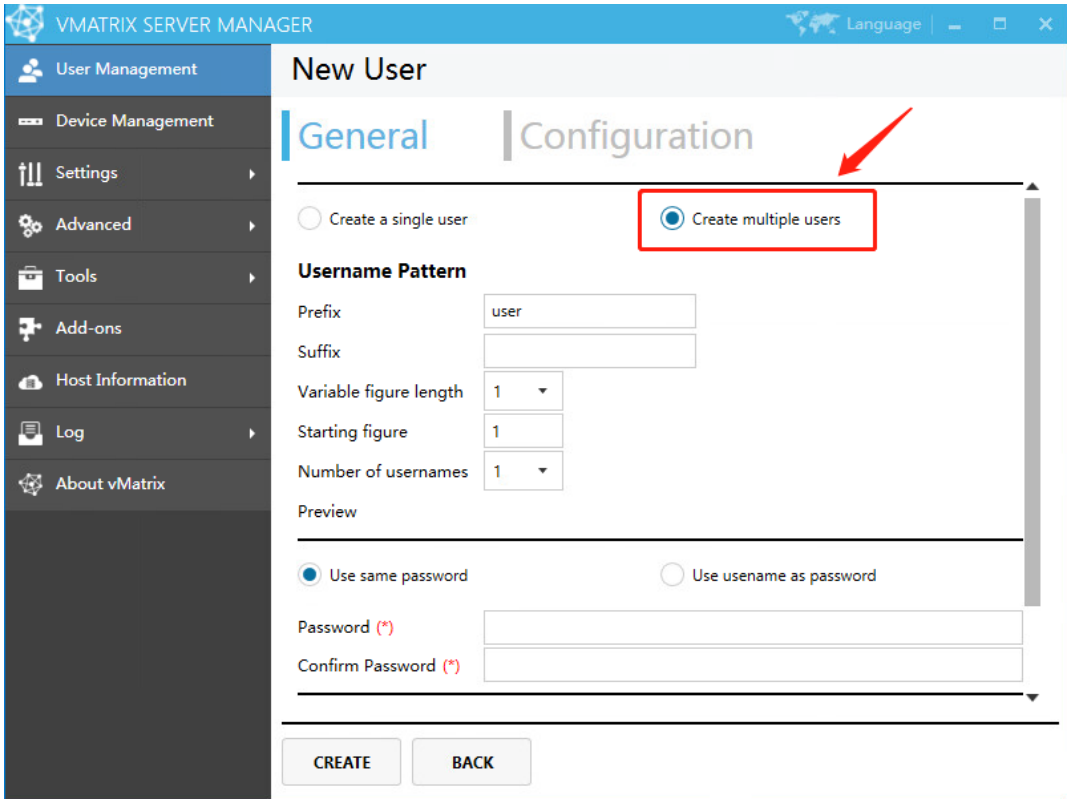
- Single user creation (defaulted)

To create a single user each time, you simply enter required user name and password and click “Create” at the bottom.

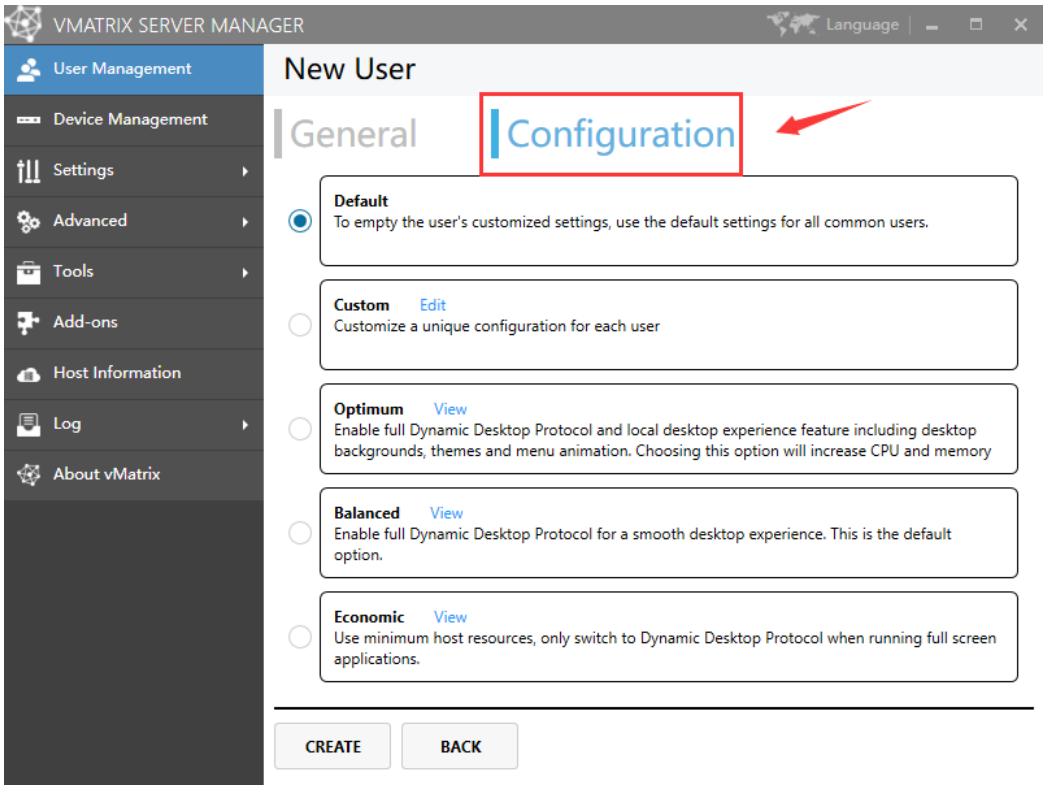


- Multiple user creation

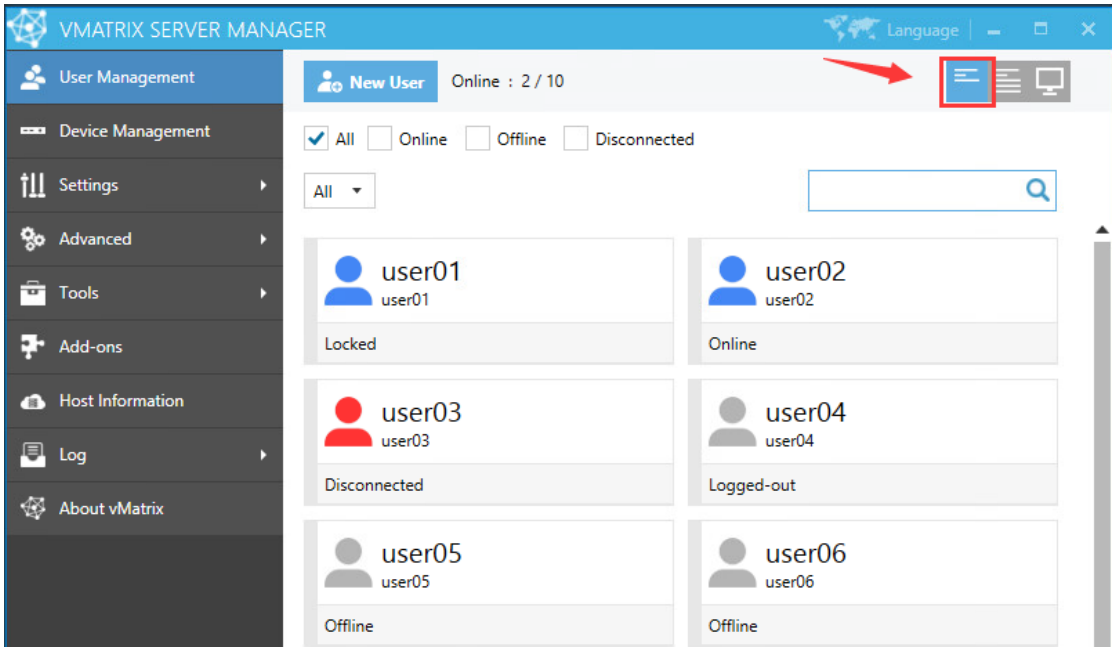
To create multiple users at a time, select “Create multiple users” and then you will be given a few more fields.



- **Username Pattern:** setting the Prefix, Suffix and other rules for the username
- **Configuration:** configure preset option to new users.



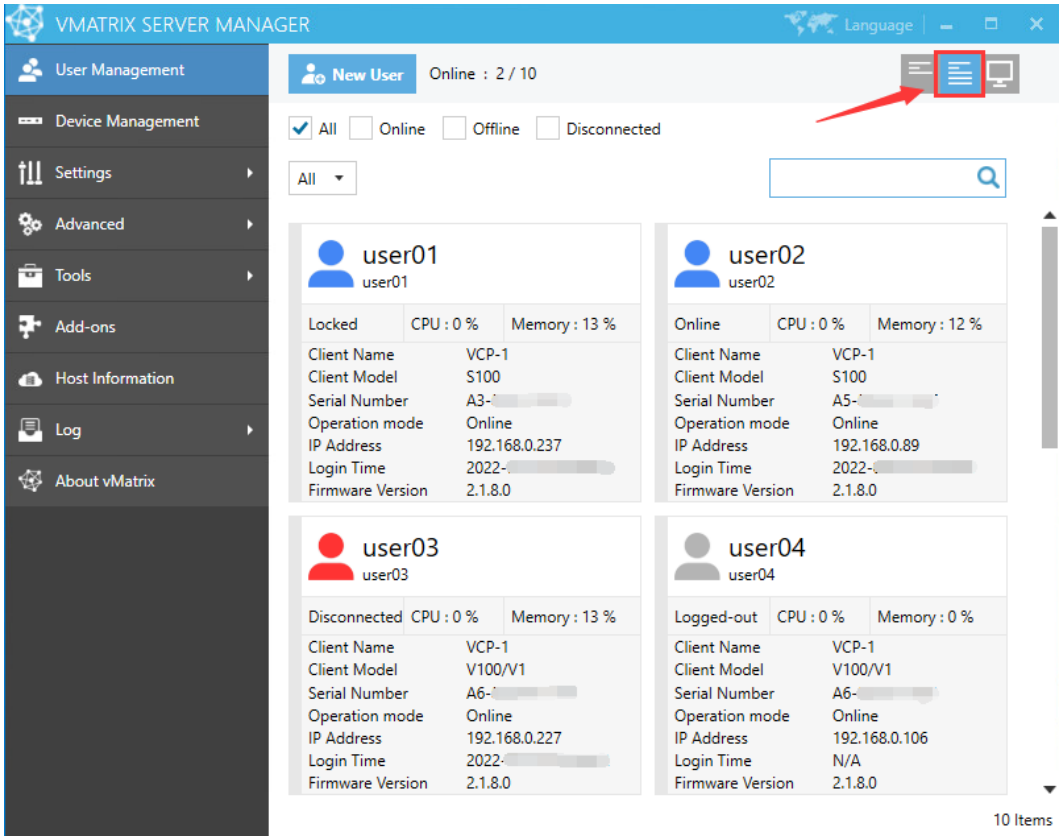
5.1.2 User Status View



On this selection, you can view CPU and Memory consumption for each user and their status including:

- **Offline:** the user has not logged into this host since host boot.
- **Online:** the user has logged in and is connecting to this host.
- **Disconnected:** the user has logged in but is not connecting to this host. User session is till running but screen goes back to device login page.
- **Logged-out:** the user logged into this host but has or has been logged out. User session has been ended and screen goes back to device login page.
- **Locked:** the user has logged into this host but user session has or has been locked. Screen goes to system login page where password is required for re-login.

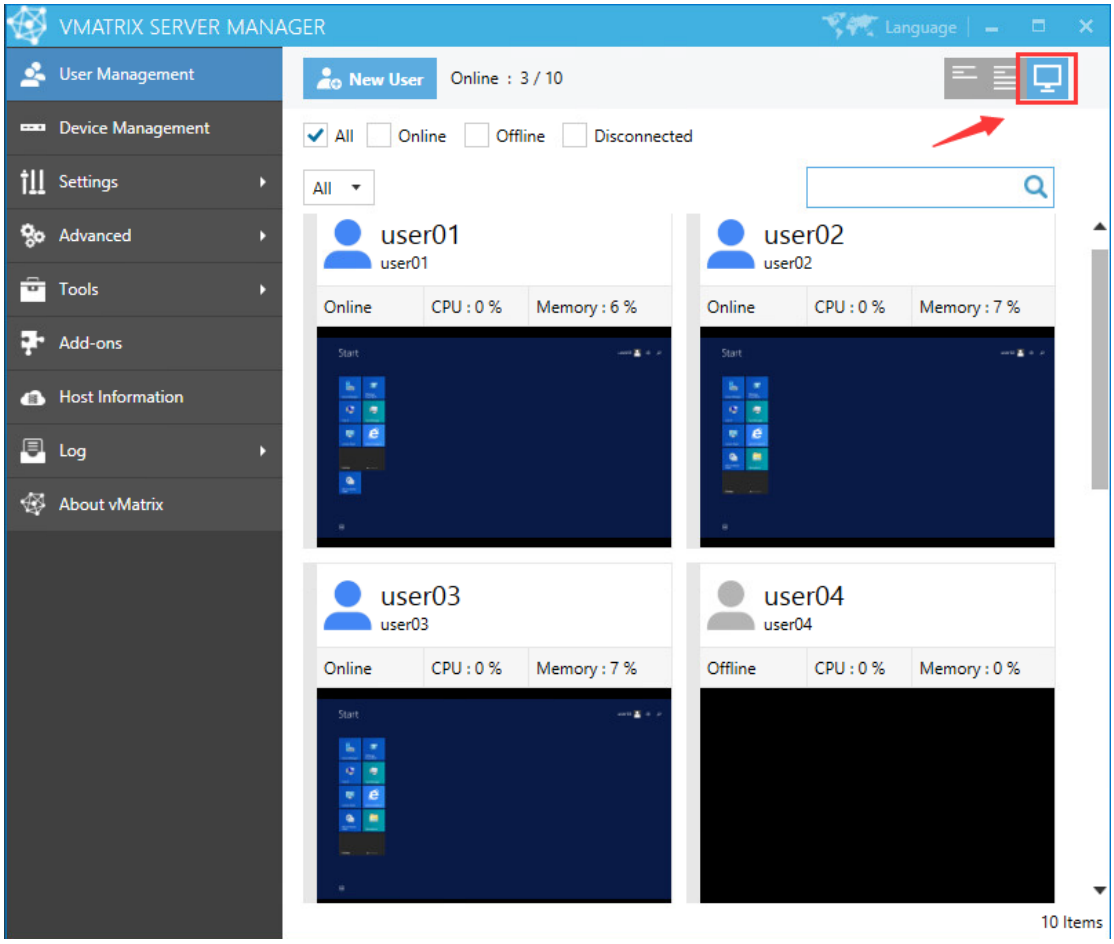
5.1.3 User Information View



On this selection, you can view CPU & Memory consumption and status for each user and their device information including:

- **Client Name:** name of the device.
- **Client Model:** model of the device.
- **Serial Number:** serial number of the device.
- **Operation Mode:** “Online”, “Offline”.
- **IP Address:** the physical IP address of the device.
- **Login Time:** the time when the user logged into this host.
- **Firmware Version：** the firmware version of user’s device

5.1.4 User Desktop View

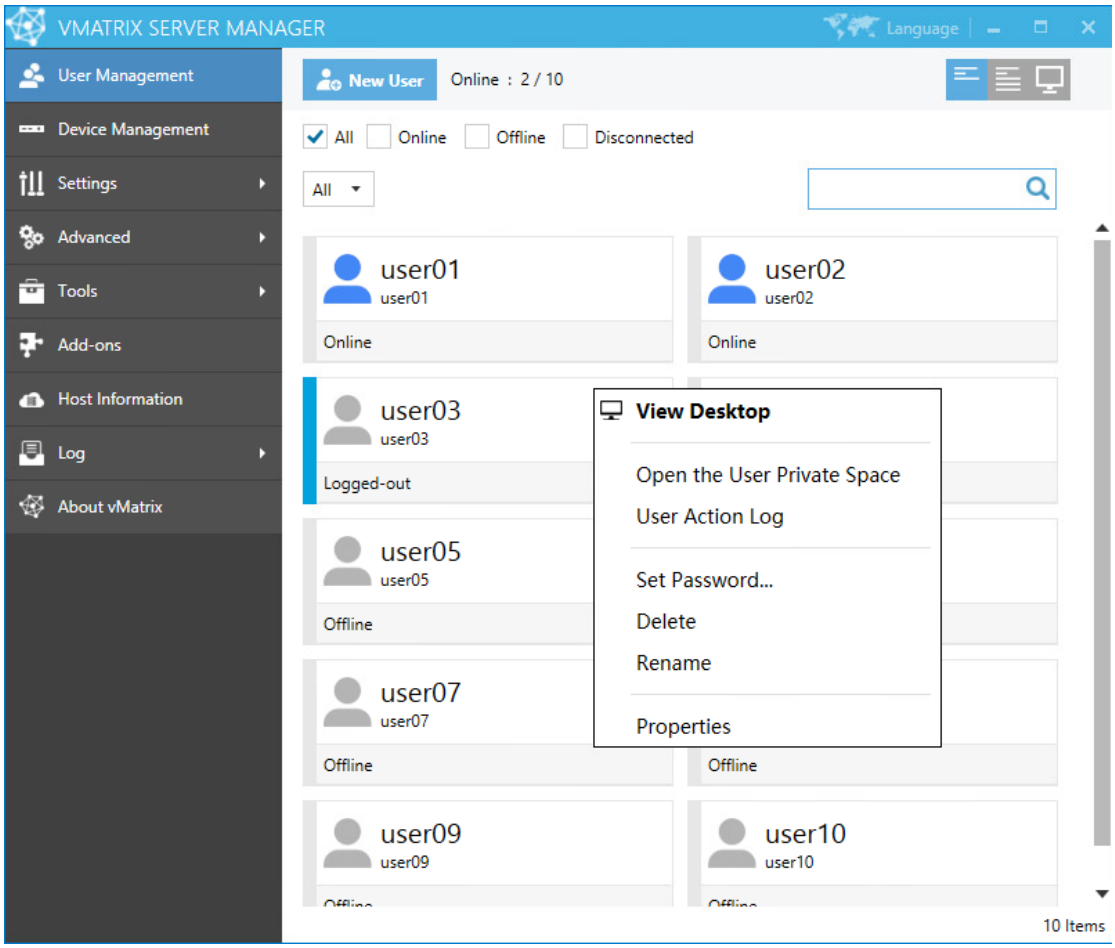


On this selection, you can view user's real time desktops in tiles.

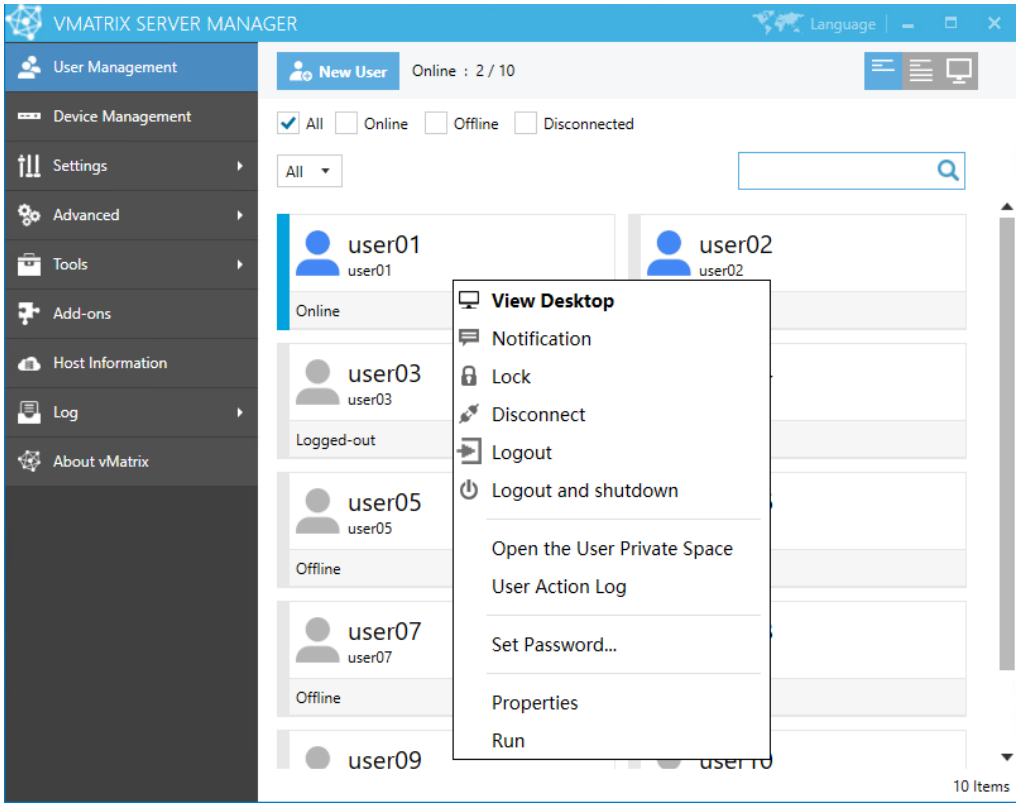
5.1.5 Right Click Menu

Right click on a single/group of offline/online user/users modules to open the user management menu. You can drag the mouse, or use shortcut keys like "shift" or "CTRL" + "A" to select multiple modules at a time.

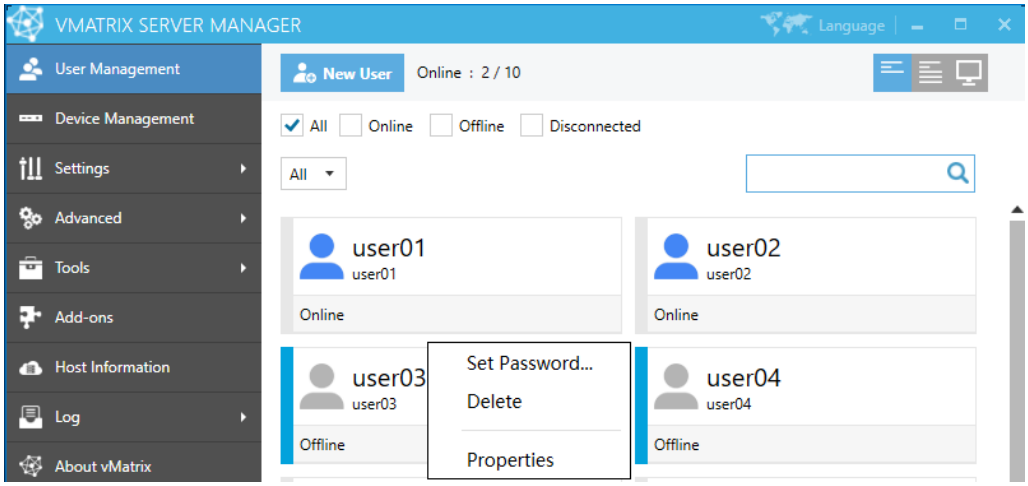
- **On a single offline user:** View Desktop, Open the User Private Space, User Action Log, Set Password..., Delete, Rename, Properties.



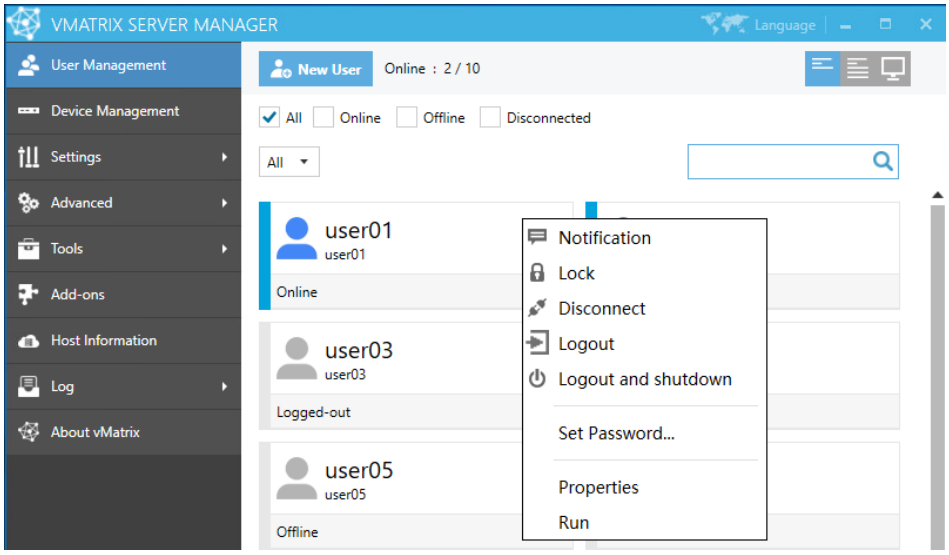
- **On a single online user:** View Desktop,Notification, Lock, Disconnect, Logout, Logout and shutdown, Open the User Private Space, User Action Log, Set Password..., Rename, Properties, Run.



- **On a group of offline users:** Set Password, Delete, Properties.

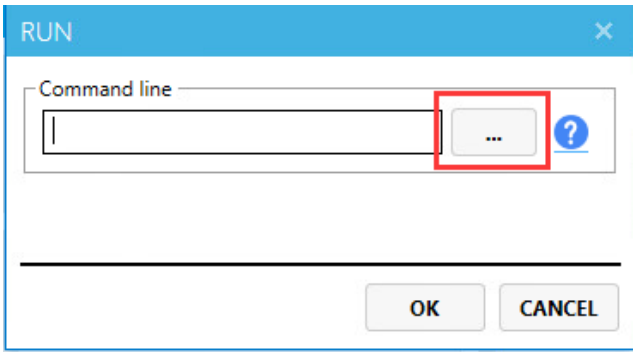


- **On a group of online users:** Notification, Lock, Disconnect, Logout, Logout and shutdown, Set Password..., Properties, Run.

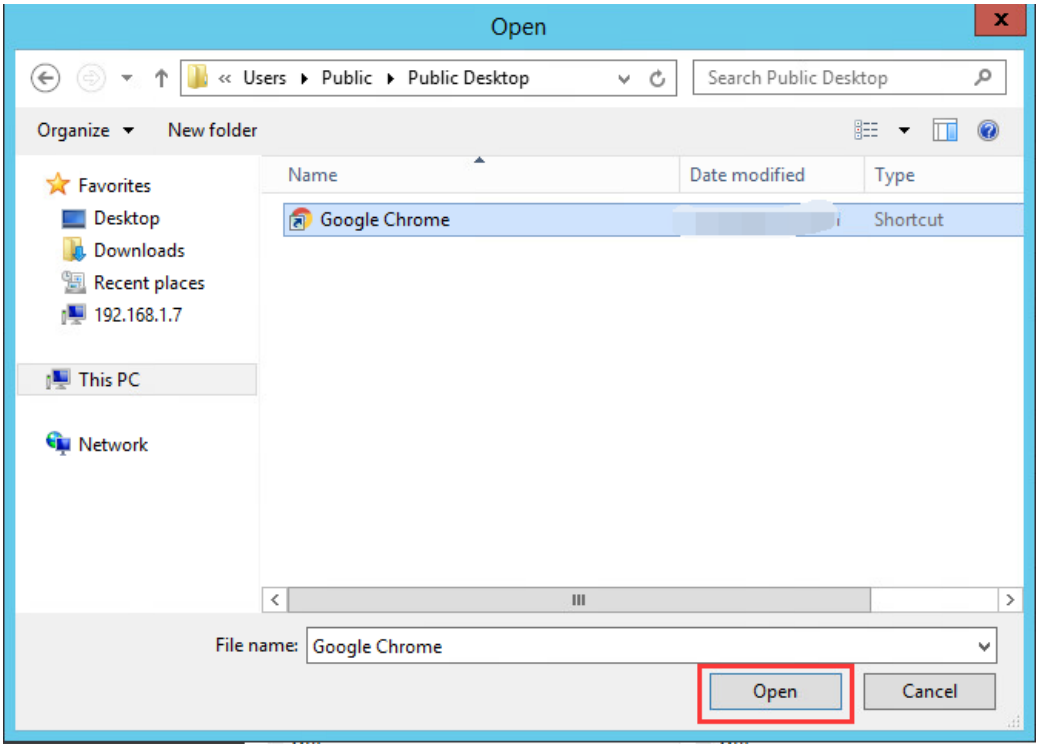


- **View Desktop:** Enter detailed information page of the user.
- **Notification:** to send a notification to the selected user in a small pop-up windows.
- **Lock:** to lock the selected user's desktop; the user's screen goes to system login page where password is required for re-login.
- **Disconnect:** to disconnect the selected user's session; the user session is still running but screen goes back to device login page.
- **Logout:** to log selected user's session out; the user's session is ended and screen goes back to device login page.
- **Logout and shutdown:** to log selected user's session out and shutdown the device.
- **Open the User Private Space:** to open the folder where the selected user's personal files are stored.
- **User Action Log:** to view all action log of the selected users on this host.
- **Set Password...:** to reset password for this user. This will take effect on next login.
- **Rename:** to rename the selected user. This will take effect immediately.
- **Delete:** to delete the selected user. This will take effect immediately.
- **Properties:** to change the selected user's personal settings.
- **Run:** run command lines or launch a program on the user session.

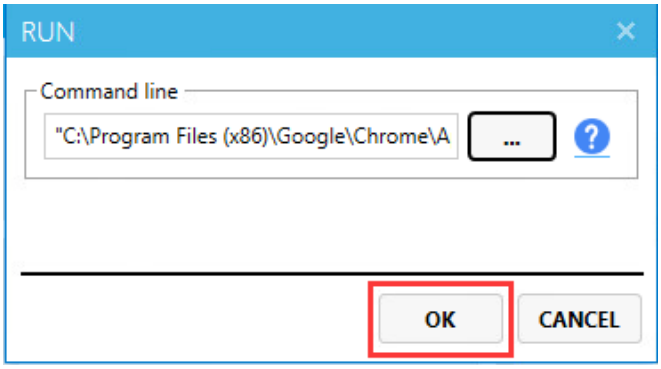
- Click "..." to browse the program or file.



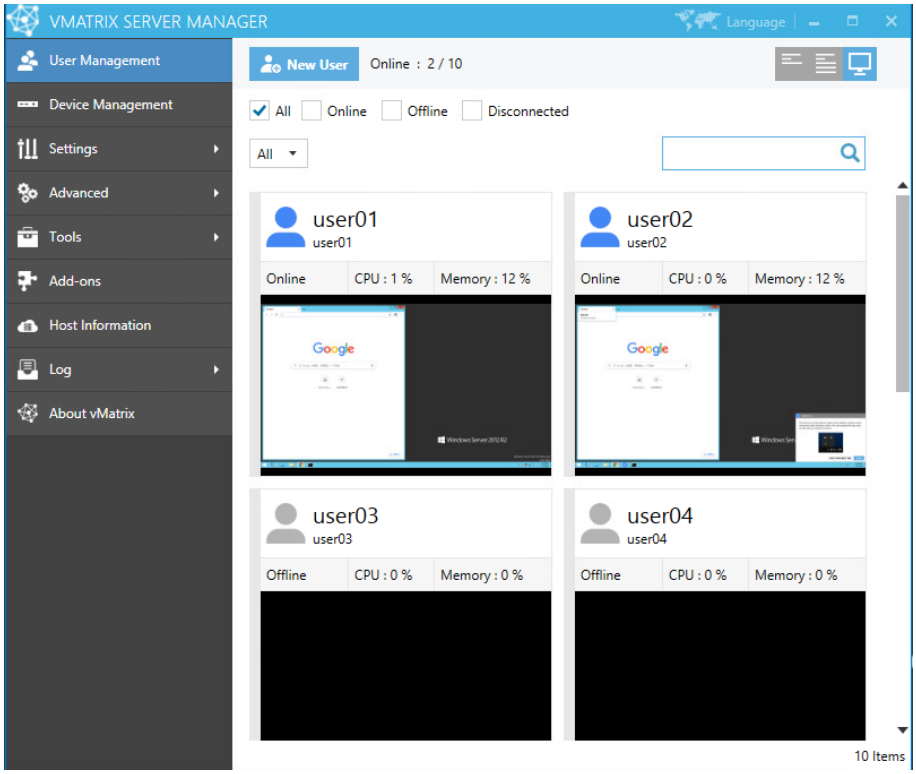
1) Select the program you want to run and click "Open".



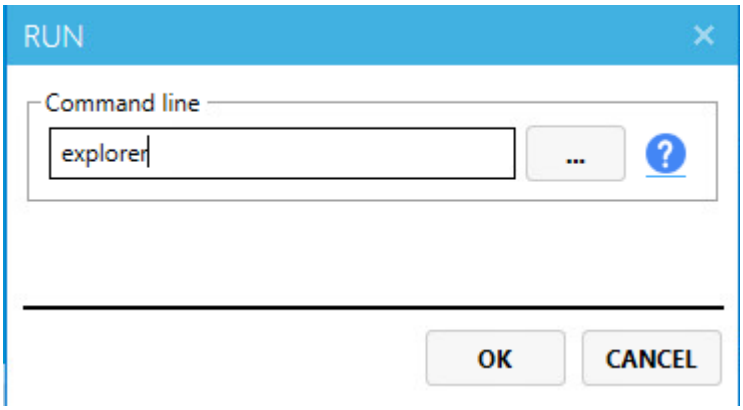
2) Click “OK”.



3) You can see the program running in the selected terminal user sessions.



- Enter the command line directly to run commands, programs, files, etc.



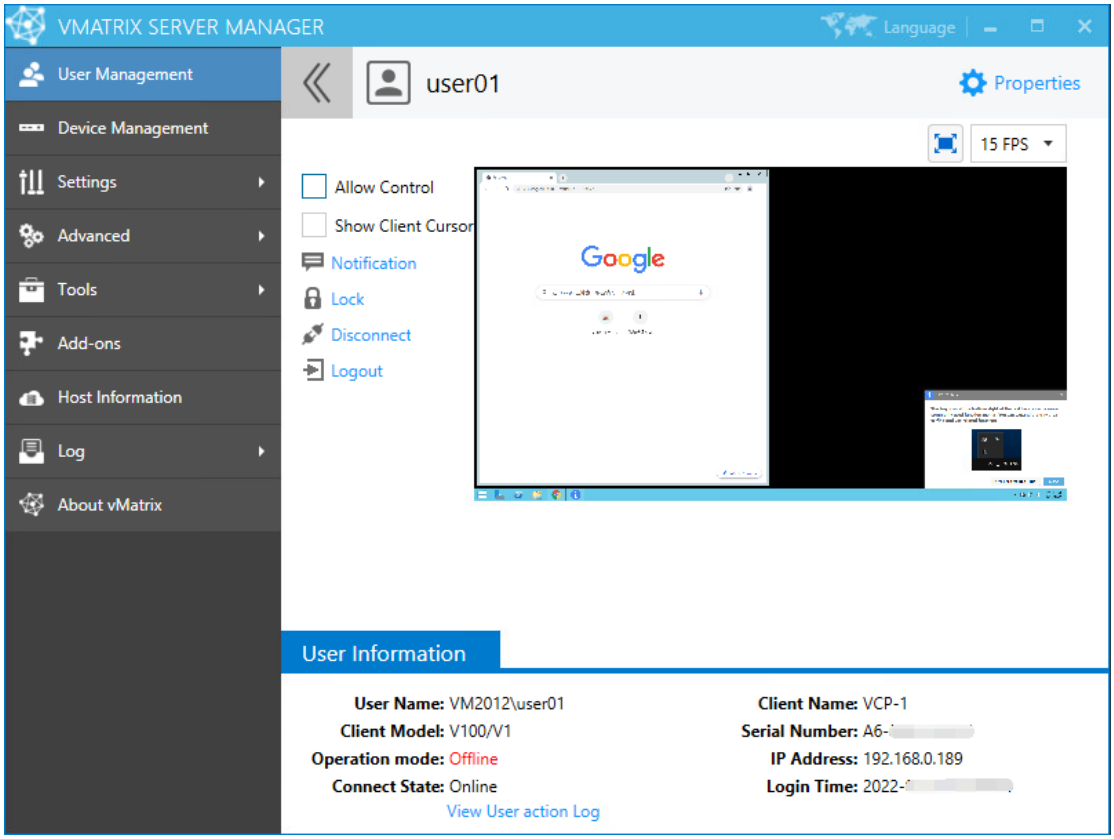
Notes:

- Example of system command with parameters ping localhost -t
- Example of running a file in default program: C:\test.mp4
- Example of running a file in specific program: notepad.exe C:\test.txt
- If the path contains spaces, the path string must be enclosed in double quotes, example: "C:\Program Files\test.exe" C:\test.mp4

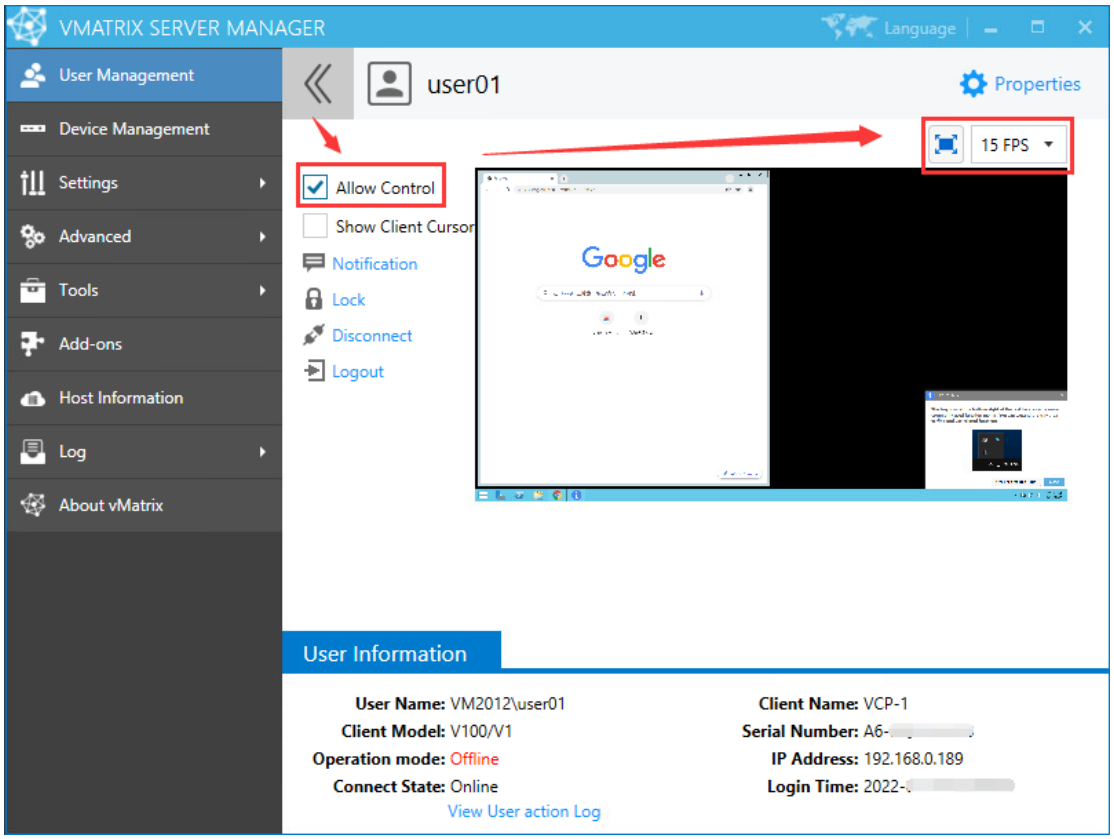
➢ For more about command lines, please refer to the Windows command line instructions.

5.1.6 Personal Monitoring & Controlling

Double click or right click on a single user module and then select "View Desktop", to enter the user's personal page. This page allows you to monitor and take control over a user desktop.

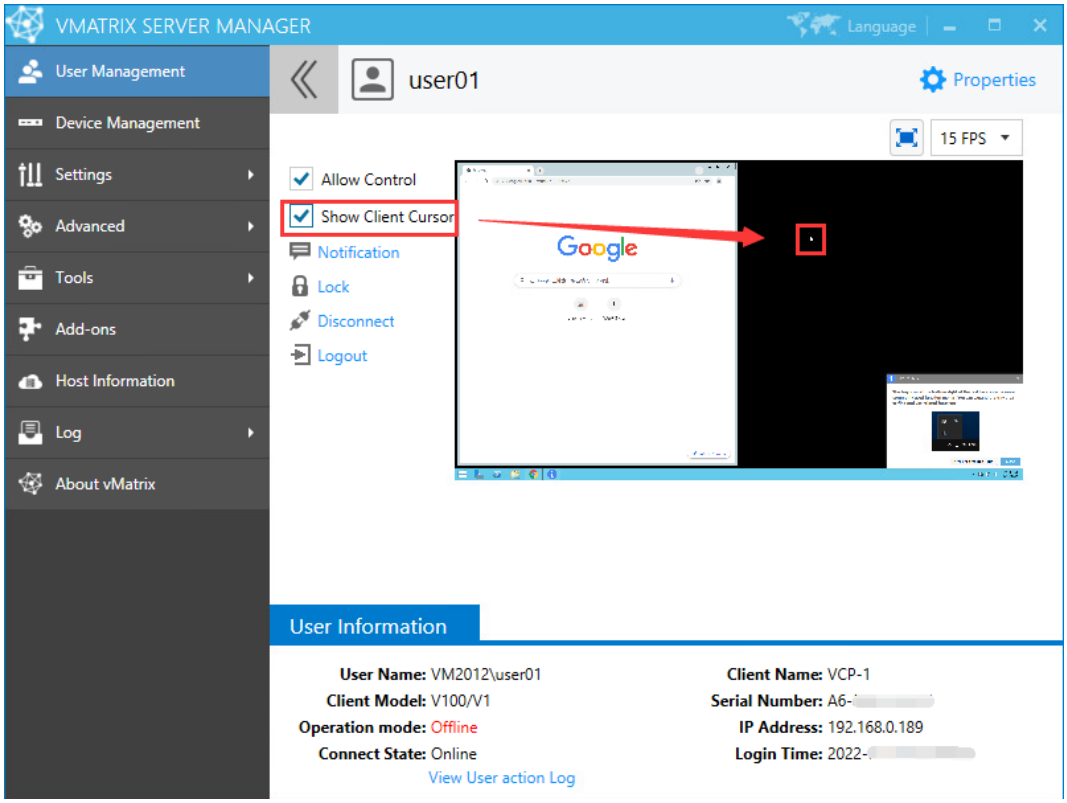


- **Allow Control:** if this option is checked, you can take control over the user's desktop.



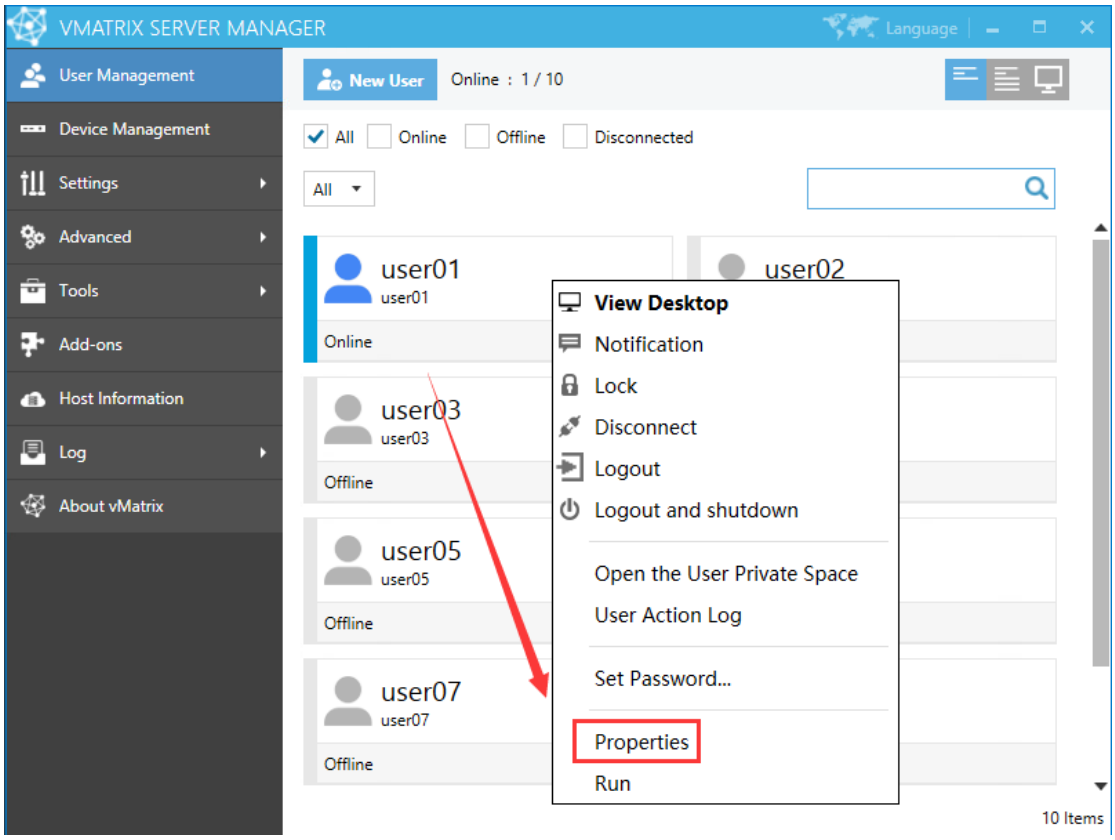
Note: click on this icon to extend the view the user's desktop in full screen. When entering full screen view, you can move the cursor to the right top corner to exit full screen view.

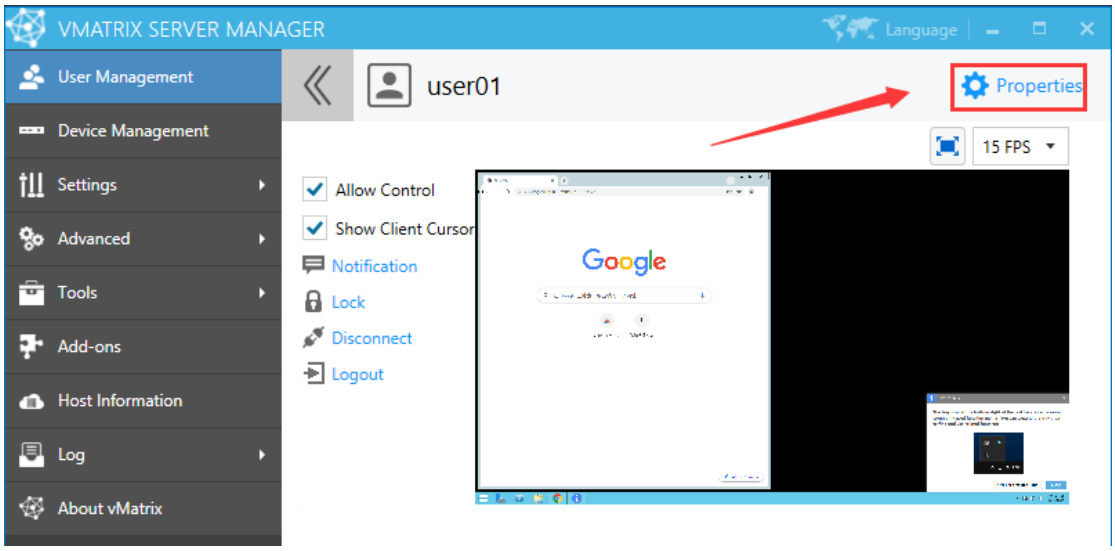
- **Client Cursor Visible:** if this option is checked, the mouse cursor of the client can be displayed in the monitoring screen.



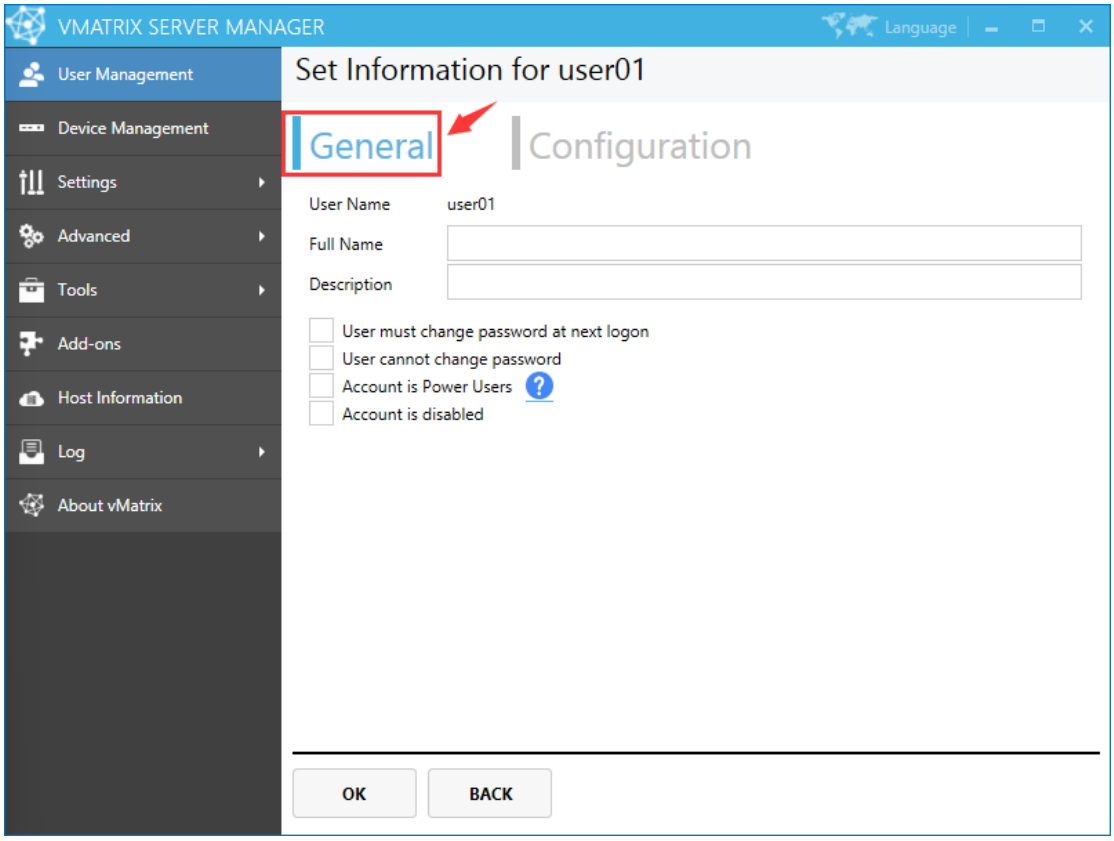
5.1.7 Personal User Settings

To enter the setting page for a selected user, you can right click on the user module on the initial User Management page, or click on the “Properties” option after entering Personal Monitoring & Controlling page.

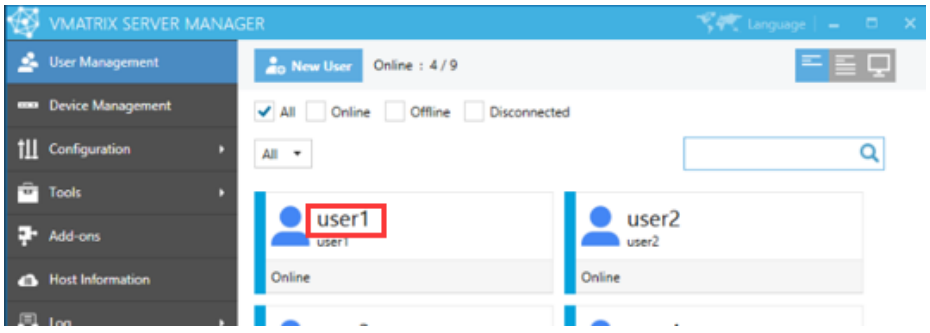

VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Add-ons
Host Information
Log
About vMatrix
New User
Online : 1 / 10
All
Online
Offline
Disconnected
All
user01
user01
Online
user02
user03
user03
Offline
user05
user05
Offline
user07
user07
Offline
View Desktop
Notification
Lock
Disconnect
Logout
Logout and shutdown
Open the User Private Space
User Action Log
Set Password...
Properties
Run
10 Items


VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Add-ons
Host Information
Log
About vMatrix
user01
Properties
15 FPS
Allow Control
Show Client Cursor
Notification
Lock
Disconnect
Logout
Google

❖ General Settings



- **User Name:** user name cannot be changed on this page but only by right clicking the user module on initial User Management page.
- **Full Name:** the user's full name is the top one beside the user icon on initial User Management page.

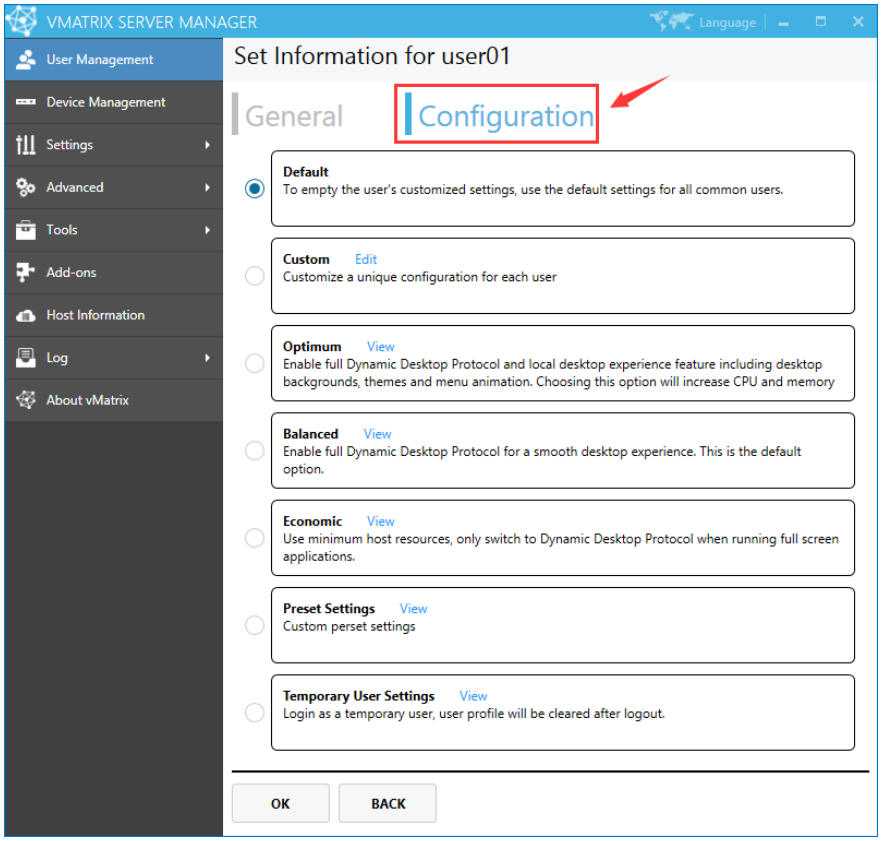


- **Description:** description of the user does not show at any other place.
- **User must change password at next logon:** selecting this option will force the user to change password at next logon.
- **User cannot change password:** selecting this option will disable the user to change

password.

- **Account is Power User:** Power User is given more rights to change system settings than a common user, but less than an Administrator.
- **Account is disabled:** selecting this option will disable the user account. This is often used when you want to disable the user temporarily, saving you trouble to delete and re-create.

❖ Configuration Settings



Configuration settings allows you assign various preset settings for one or multi user, to help you customize different department or job position. Changes will take effect at user's next login. Configuration settings include:

- **Default:** Apply the configuration as "Settings" - "Preset Settings".
- **Custom:** Customize a unique configuration for each user. (This option is not available when multi users are selected)
- **Optimum:** The preset settings of the program can only be viewed but cannot be modified.

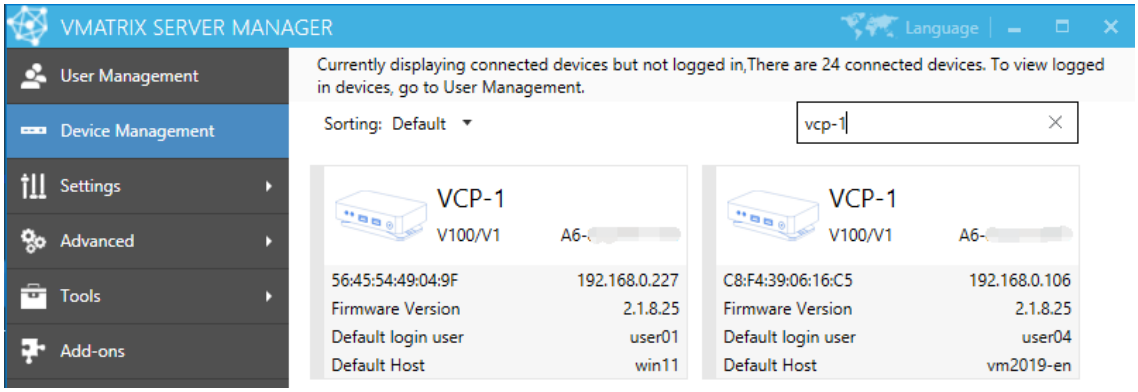
- **Balanced:** The preset settings of the program can only be viewed but cannot be modified.
- **Economic:** The preset settings of the program can only be viewed but cannot be modified.
- **Preset Settings:** The configuration newly created by the administrator in "Settings"-"Preset Settings ".
- **Temporary User Settings:** The configuration newly created by the administrator in "Settings"-"Preset Settings ".

Note: This page can only modify the customized configuration. If you need to modify other configurations, please go to the "Settings" -"User Configuration" page.

5.2 Device Management

5.2.1 Device Information View

On this page, you can view device information including: Device name, Device model, Serial number, Mac address, IP address, Firmware version, Default login user and Default host.



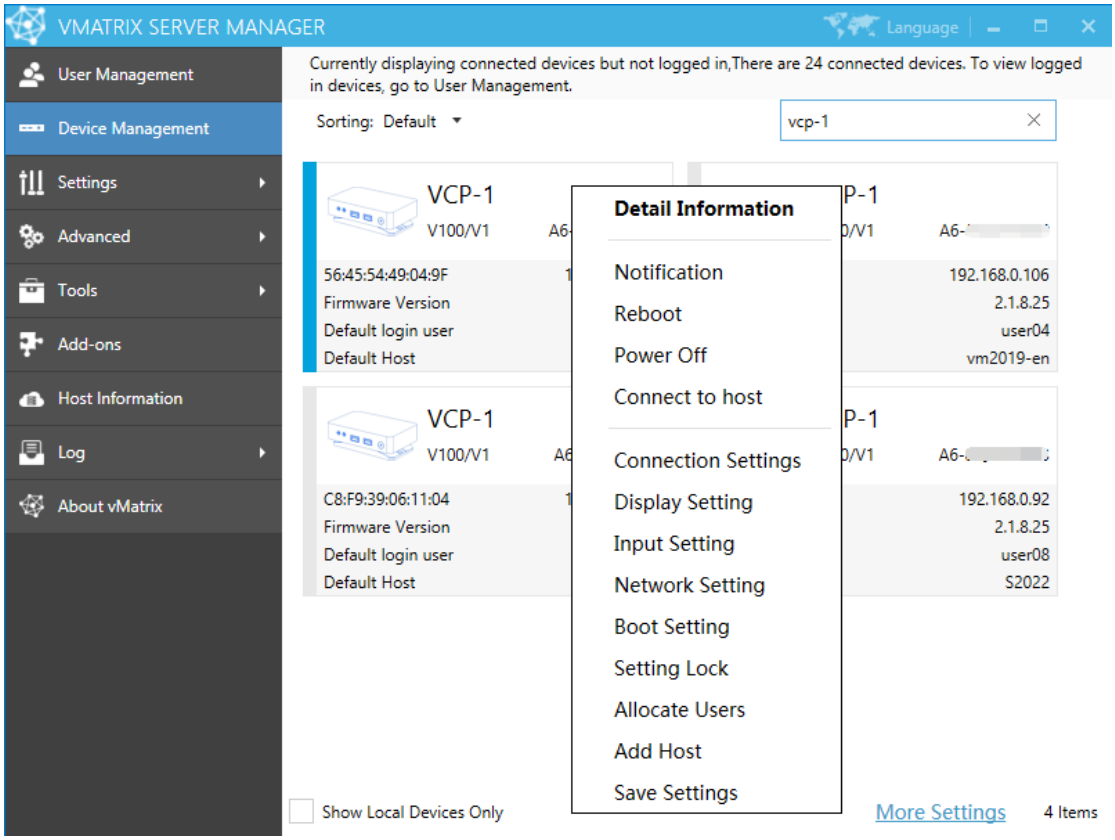
Note: This page displays connected devices (powered on devices in the same LAN as the host or powered on devices that has ever logged into the host) but not logged in. To view logged in devices, go to User Management.

5.2.2 Right Click Menu

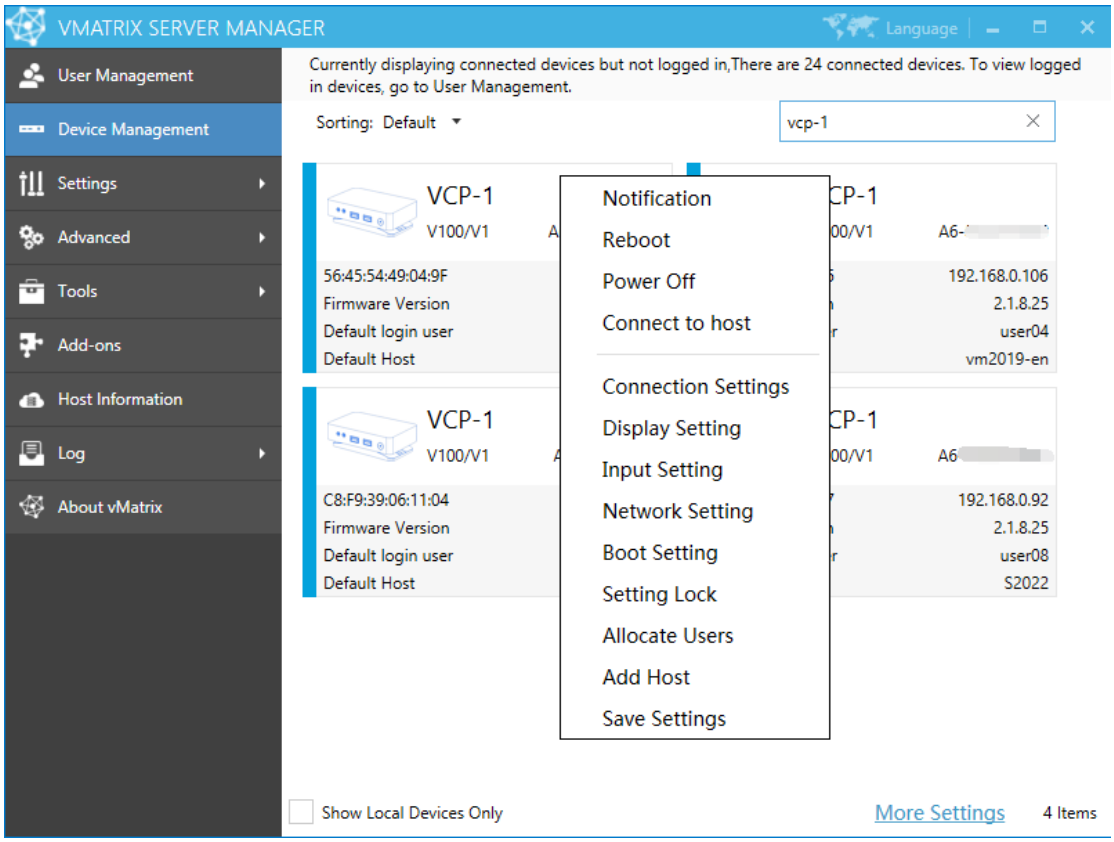
Right click on a single or multiple device modules to open the device management menu. Each of displayed options (except Notification) performs a function which can be found on the device interface, allowing administrators to set up or manage the devices centrally and remotely from the host side. You can drag the mouse, or use shortcut keys like "shift" or

"CTRL" + "A" to select multiple modules at a time.

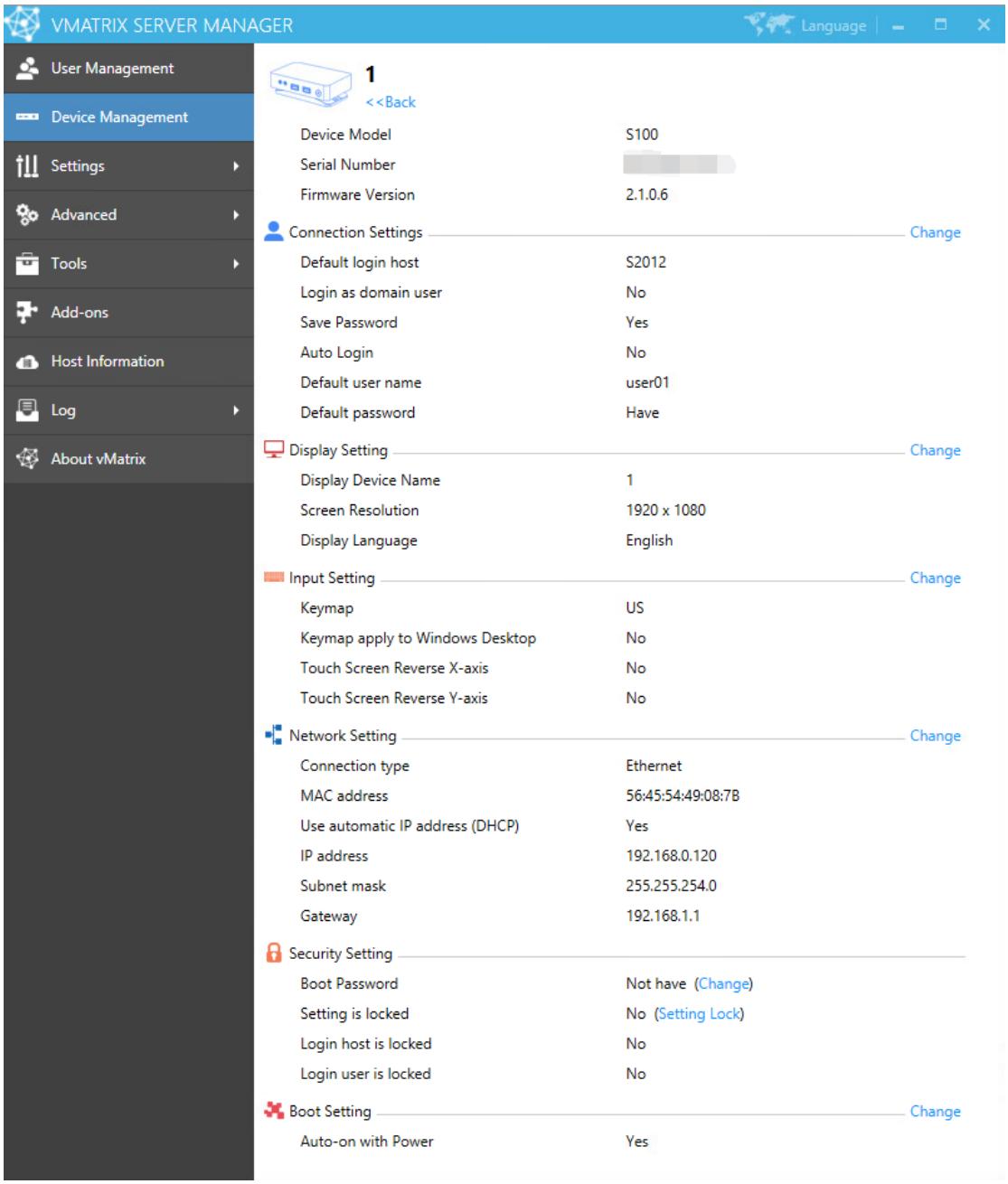
- **On a single device:** Detail Information, Notification, Reboot, Power off, Update Firmware, Connect to Host, Connection Setting, Display Setting, Input Setting, Network Setting, Boot Setting, Setting Lock(Unlock Settings), Allocate Users, Add Host, Save Settings.



- **On multiple devices:** Notification, Reboot, Power off, Update Firmware, Connect to Host, Connection Settings, Display Setting, Input Setting, Network Setting, Boot Setting, Setting Lock (Unlock Settings), Allocate Users, Add Host, Save Settings.

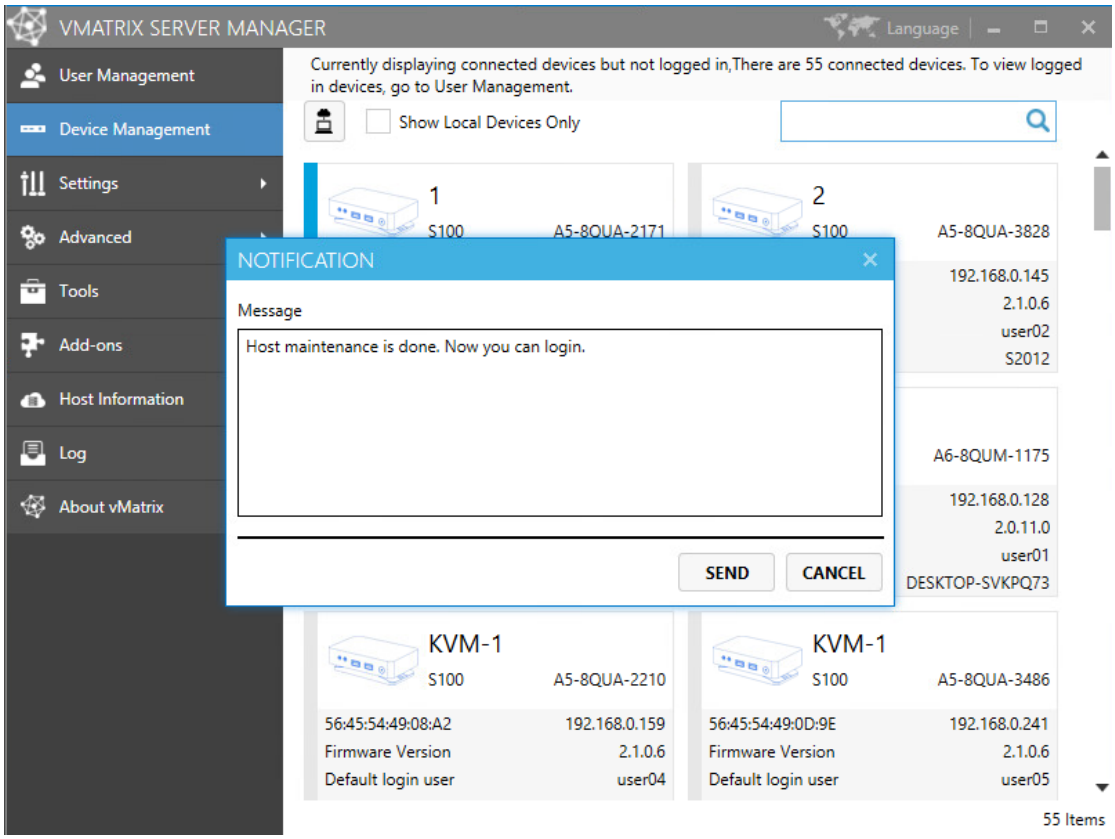


- **Detail Information:** to view the detail information of the selected device. To enter this page, you can either double click the device module or right click to select the option. To change any setting on this page, click “Change”.

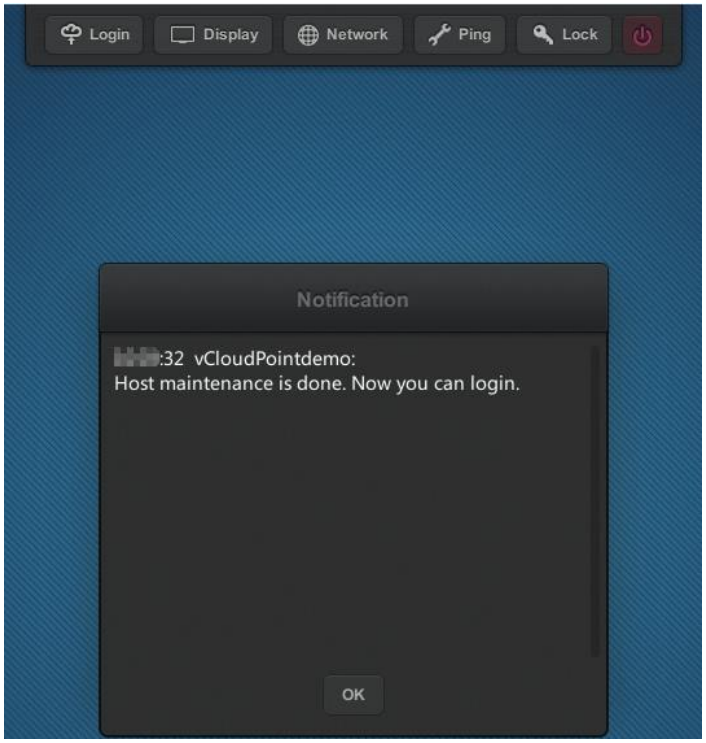


- **Notification:** to send a notification to the selected user.

Notification sent from host:



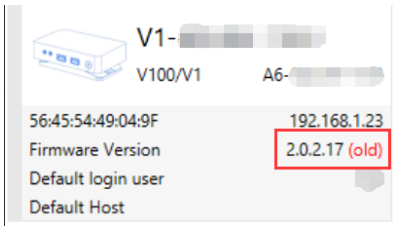
Notification to the device:



- **Reboot:** to reboot the selected devices.

- **Power off：** to shut down the selected devices.

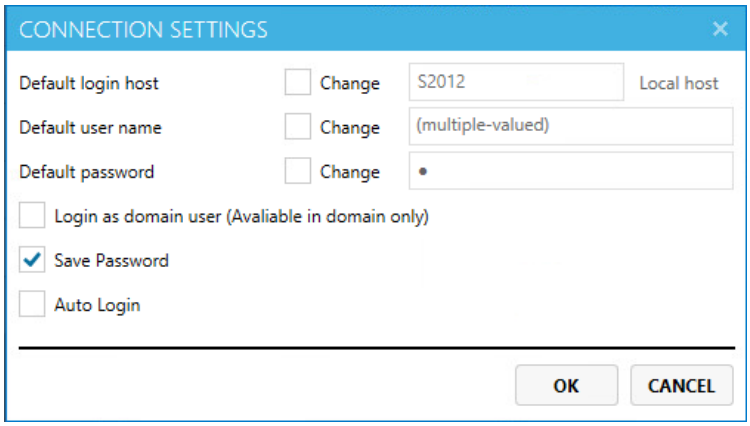
- **Update Firmware:** to update the firmware of the selected devices; only works on devices marked “(old)” in red.



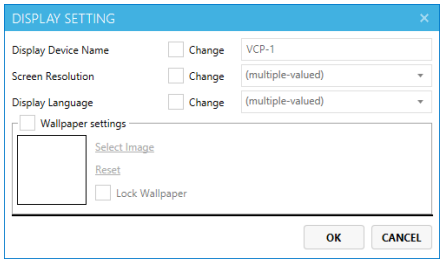
Notes: When any host in the same network segment has installed a new version of vMatrix Server software with a new firmware, vMatrix will prompt a new firmware for update. The new firmware may be incompatible with an old version of vMatrix Server Manager, so before updating the firmware, keep the vMatrix Server Manager of all hosts to the same version.

- **Connect to Host:** to log the selected devices into the designated host; only works on devices with default login settings.

- **Connection Settings:** to change the selected devices login settings including default login host, default user name, default password, domain selection, password saving selection and auto login selection which will be used for the devices next login. When multiple devices are selected, check “Change” to apply, if unchecked, it will leave the original value. The Default login host can be specified by host name or IP. If the host is in the domain while users are logging into the host as local users (rather than domain), cancel the selection of Login as domain users (Available in domain only).

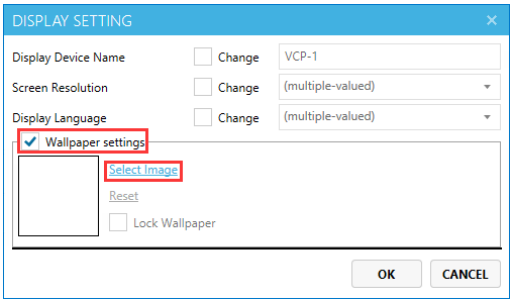


- **Display Setting:** to change the display settings of the selected devices including device name, screen resolution and language; Check "Change" to apply the setting, leave it unchecked to keep the original value.

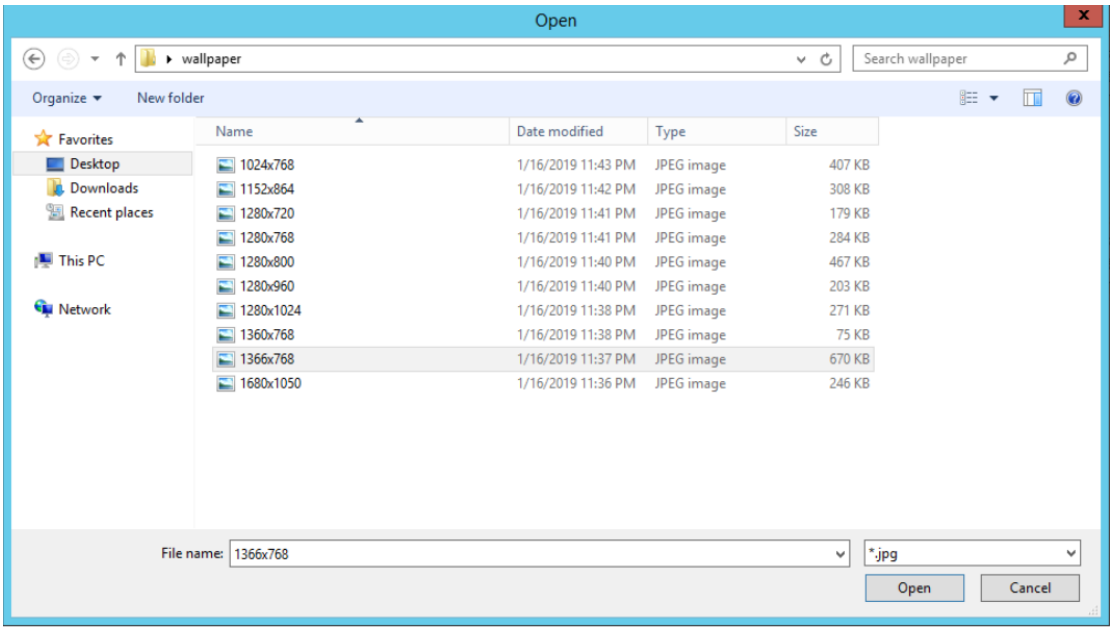


- **Wallpaper Configuration:** custom a wallpaper for the client device UI。

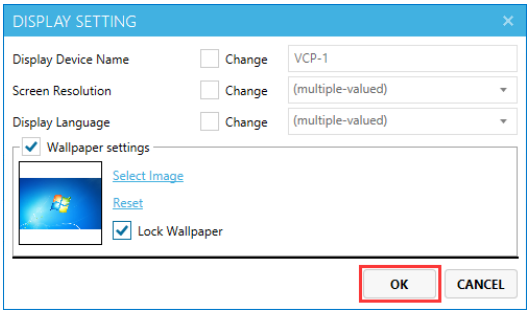
1. Check Wallpaper Configuration and click “SELECT IMAGE”;



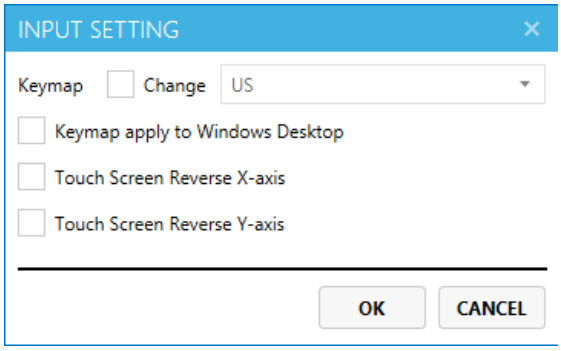
2. Select an image, only JPG image is supported;



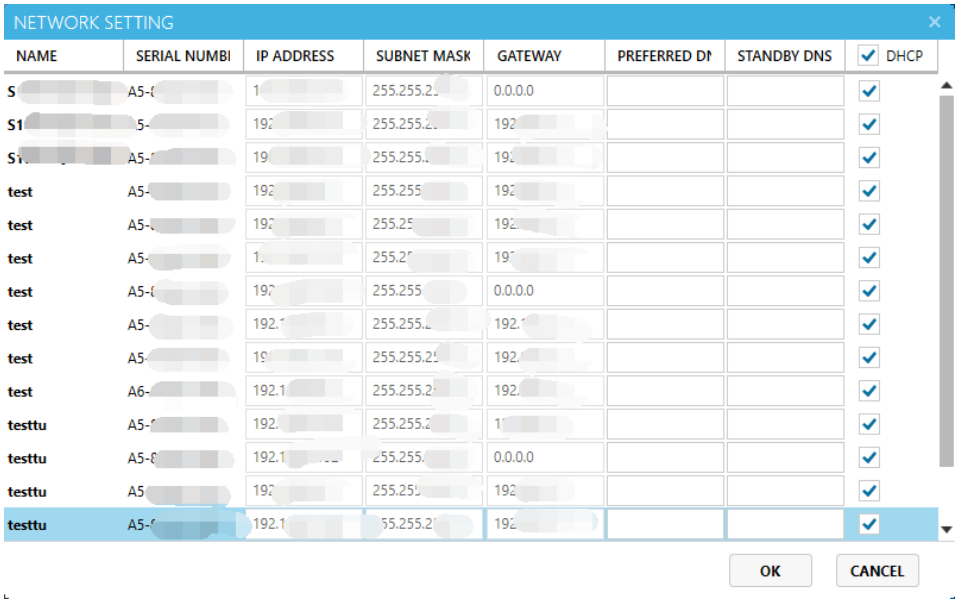
3. Then click "OK" to apply the configuration (if you lock down the wallpaper, users cannot change wallpaper on the client device.



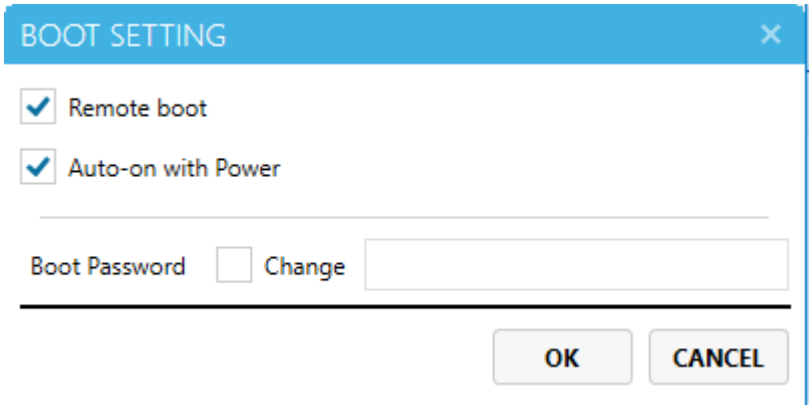
Input Setting: to change the input settings of the selected devices including keymap and touch screen X & Y axis.



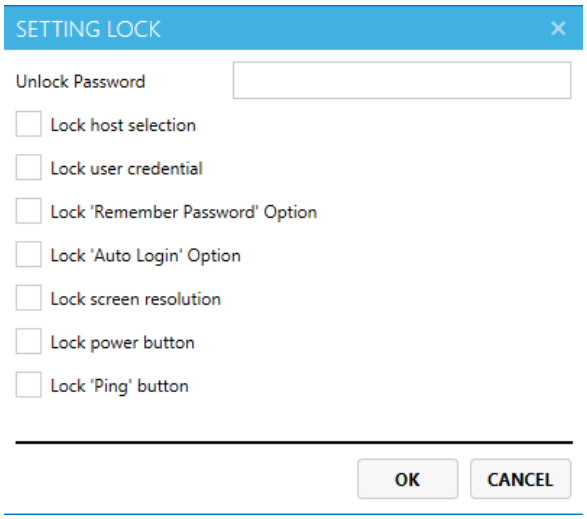
- **Network Setting:** The settings in the "Network" page of the terminal login interface. It can be set when single or multi terminals selected.



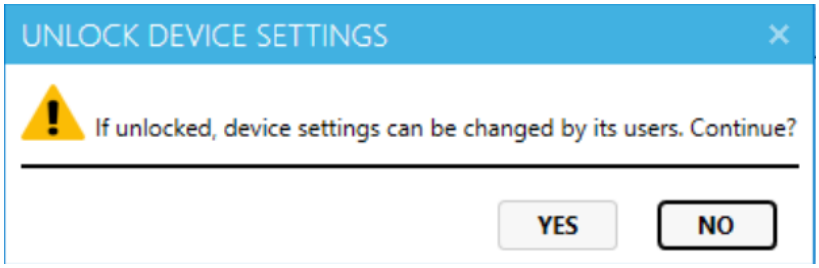
- **Boot Setting:** to enable "Auto-on with Power" and "Remote boot" for the client device. Check the “Remote boot” option to enable device boot from the vMatrix host. Check the “Auto-on with Power” option to enable auto device boot with power supply.



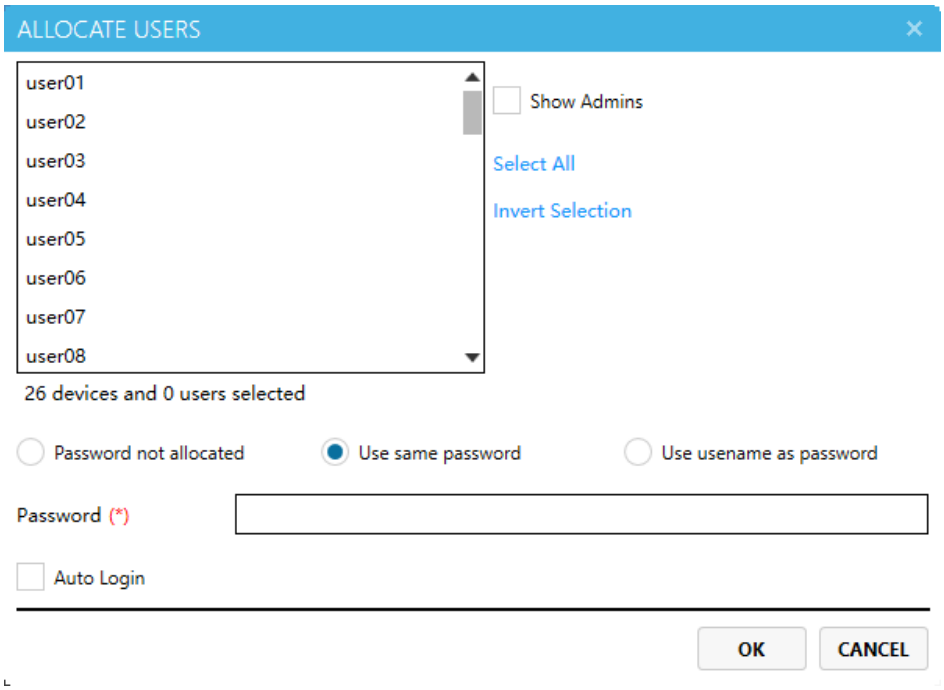
- **Setting Lock:** "SETTING LOCK" is to lock some feature of the terminal login interface. After checking "Lock host selection" and "Lock user credential", users will not be able to modify the login host, login user name and password, please allocate as needed in advance. After checking "Lock remember password" and "Lock auto-login", the option of "remember password" and "auto-login" of the terminal login interface will be locked. After checking "Lock screen resolution", users will not be able to change screen resolution of terminal. After checking the "Lock power button", the "power button" in the upper right corner of the terminal login interface will be locked. After checking the "Lock 'Ping' button", the terminal will not be able to enter the ping page.



- **Unlock Device Settings：** To unlock the device settings.



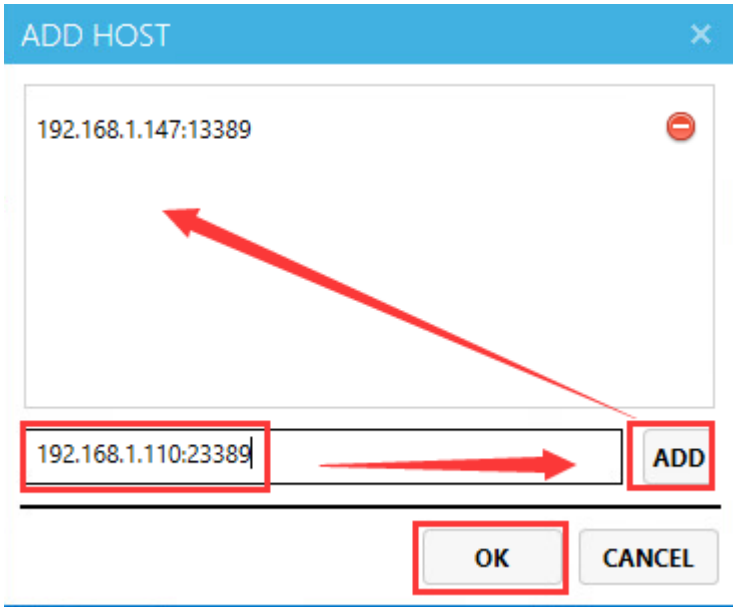
- **Allocate Users:** Allocate users created on the vMatrix Server Manager to the selected terminal. After enabling this function, the terminal automatically selects this machine as the login host.



Note:

- The allocation is randomly. If you need to specify the allocation, please set it separately.
- if the number of devices exceeds the number of existing users, some devices will not be allocated. The numbers of selected users ⩾The numbers of selected devices, to ensure each devices can be allocated.

- **Add host:** You can manually add a host for the terminal remotely. It is generally used to add hidden hosts for the terminals during deployment (hosts on cross-segment network or WAN).

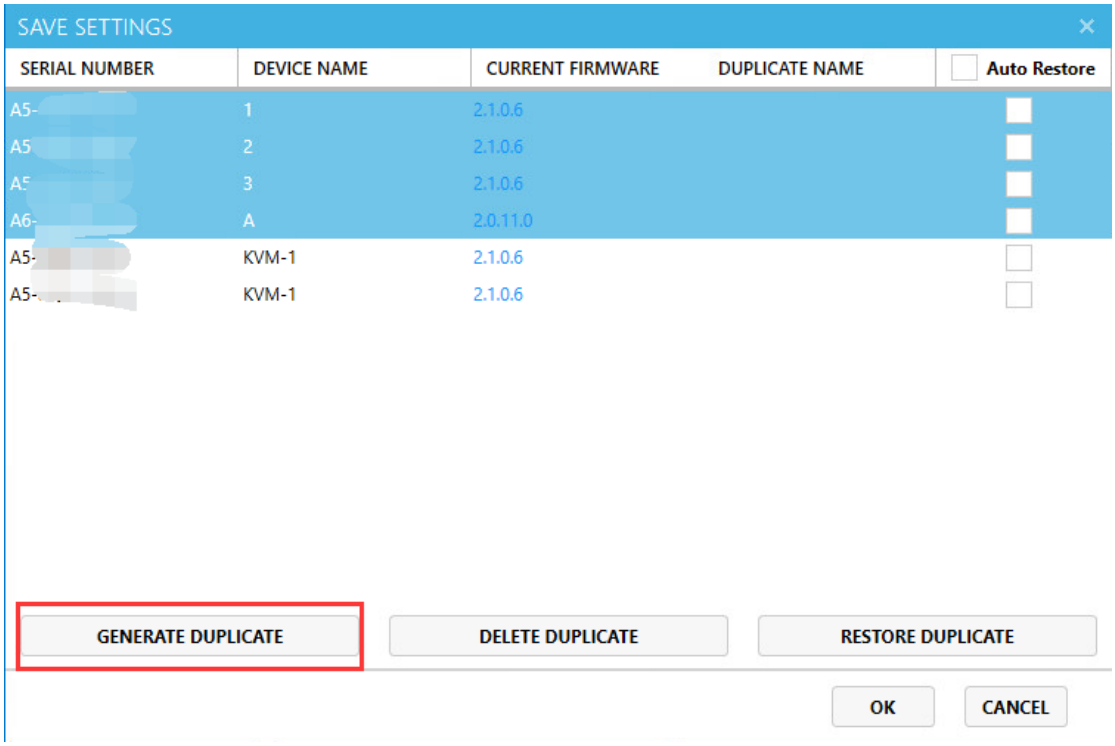


Notes:

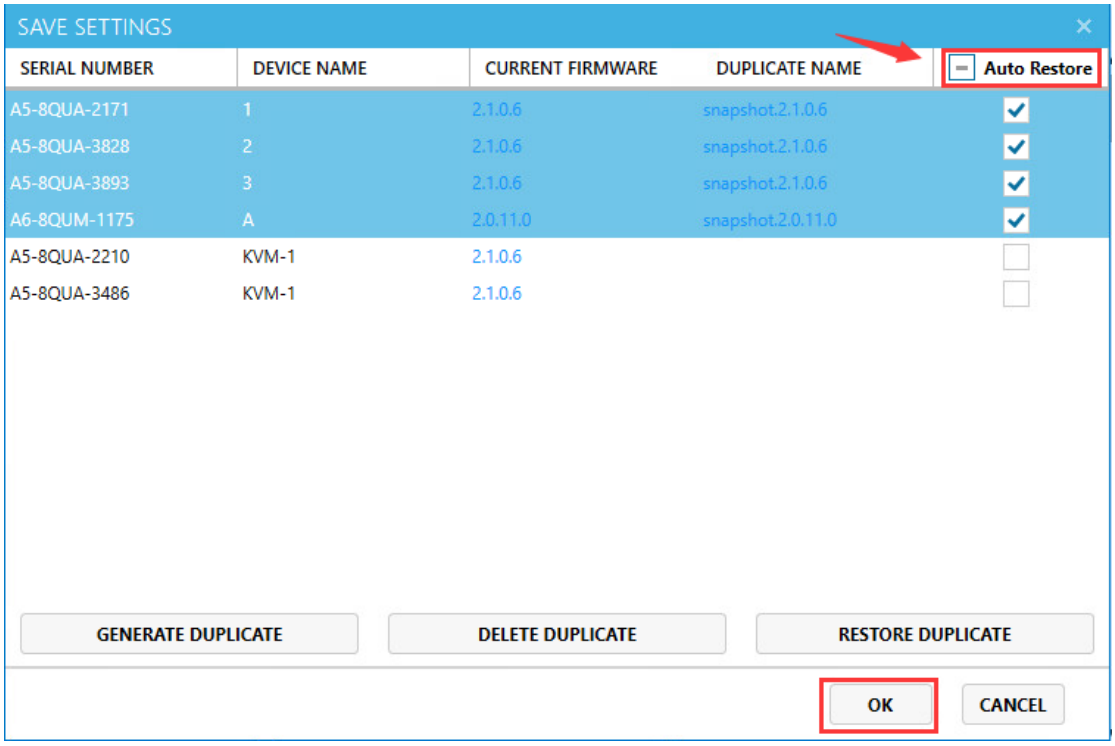
- If you do not specify a network port, the default network port for remote desktop connection is 13389. If you have manually modified the host's network port in its network settings, you need to include the network port in the host IP address as well, for example, 192.168.1.110**:23389**.
- When selecting multiple client devices, the displayed added host in the host list is the host added from the first selected client device.

- **Save Settings:** save device settings to the host for restoration in case of settings lost by resetting.

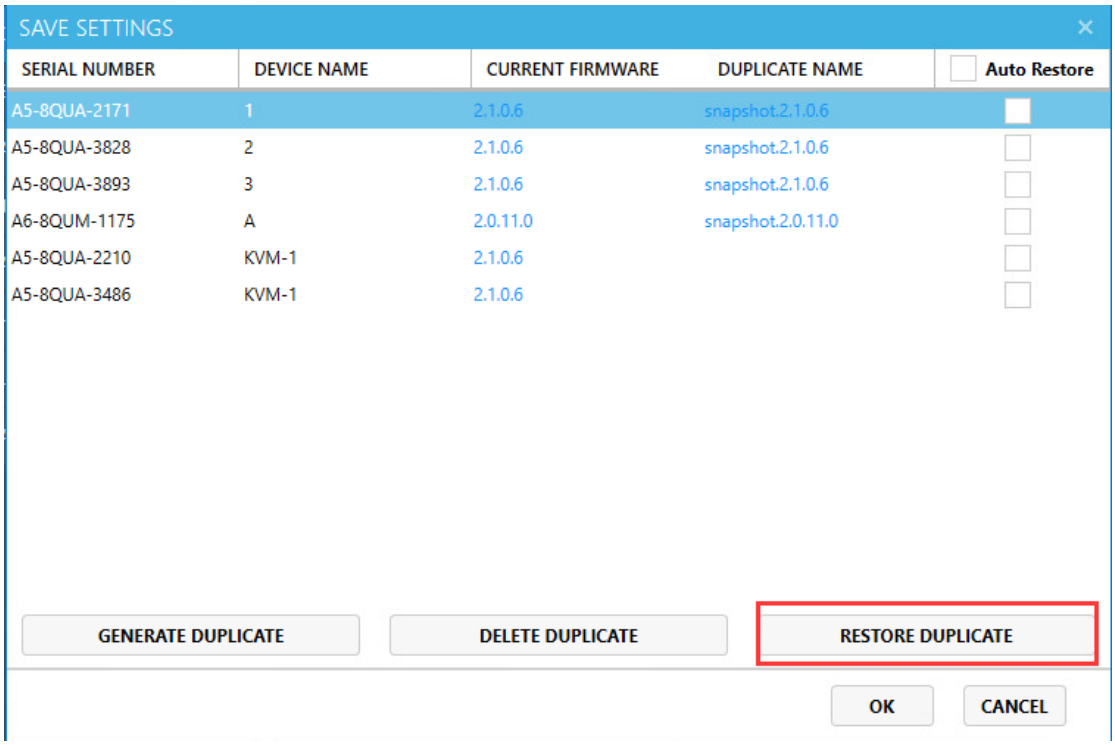
    1. Select the devices to generate duplicates.



2. Check "Auto Restore" and click "OK".



3. If you want to restore the settings in manually, uncheck the “Auto Restore” option, select a terminal and click “RESTORE DUPLICATE”.



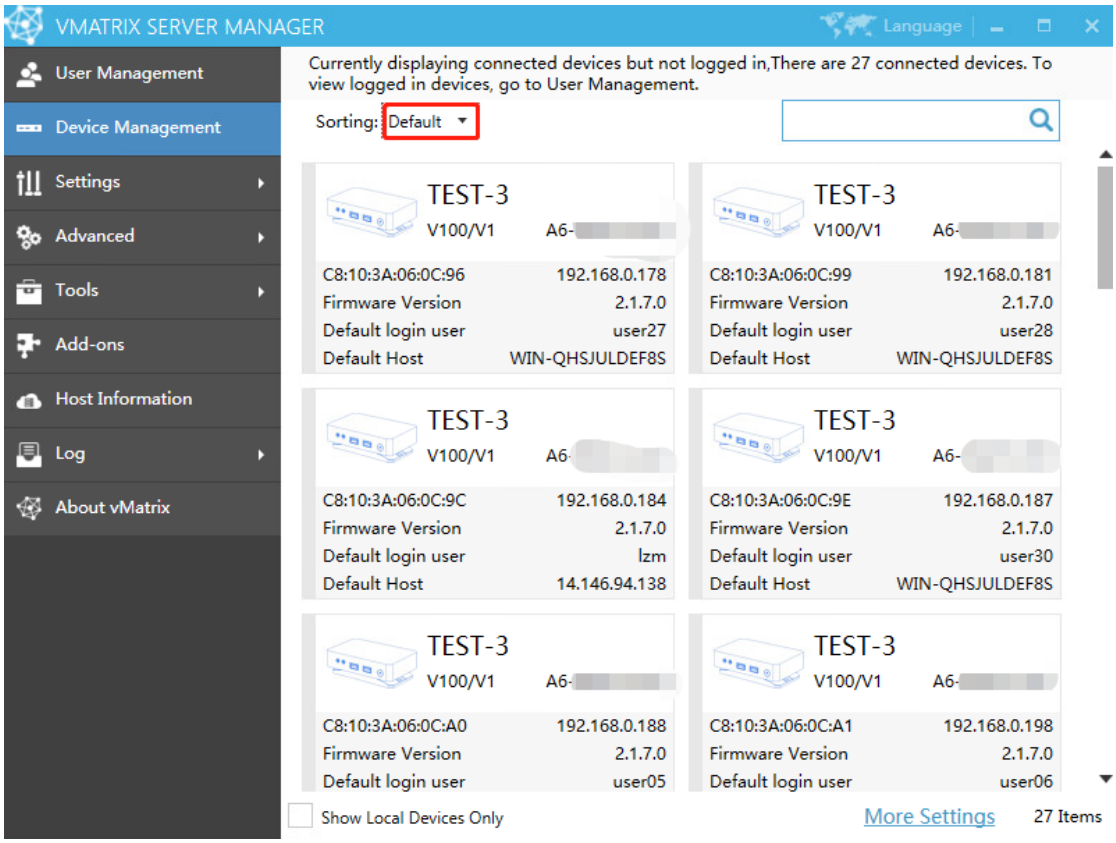
Notes:

- The client devices shall be connected to the host when “GENERAL DUPLICATE” and “RESTORE DUPLICATE”.
- ”AUTO RESTORE” and “RESTORE DUPLICATE” can only be used after “GENERAL DUPLICATE”.
- When a client device is configured with ”AUTO RESTORE” on settings, any changes to its settings will be recovered when it is powered on, disconnected, or logged off.
- If the device firmware has been reset to the factory default, when “RESTORE DUPLICATE”, a firmware update will be executed first before recovering the settings.

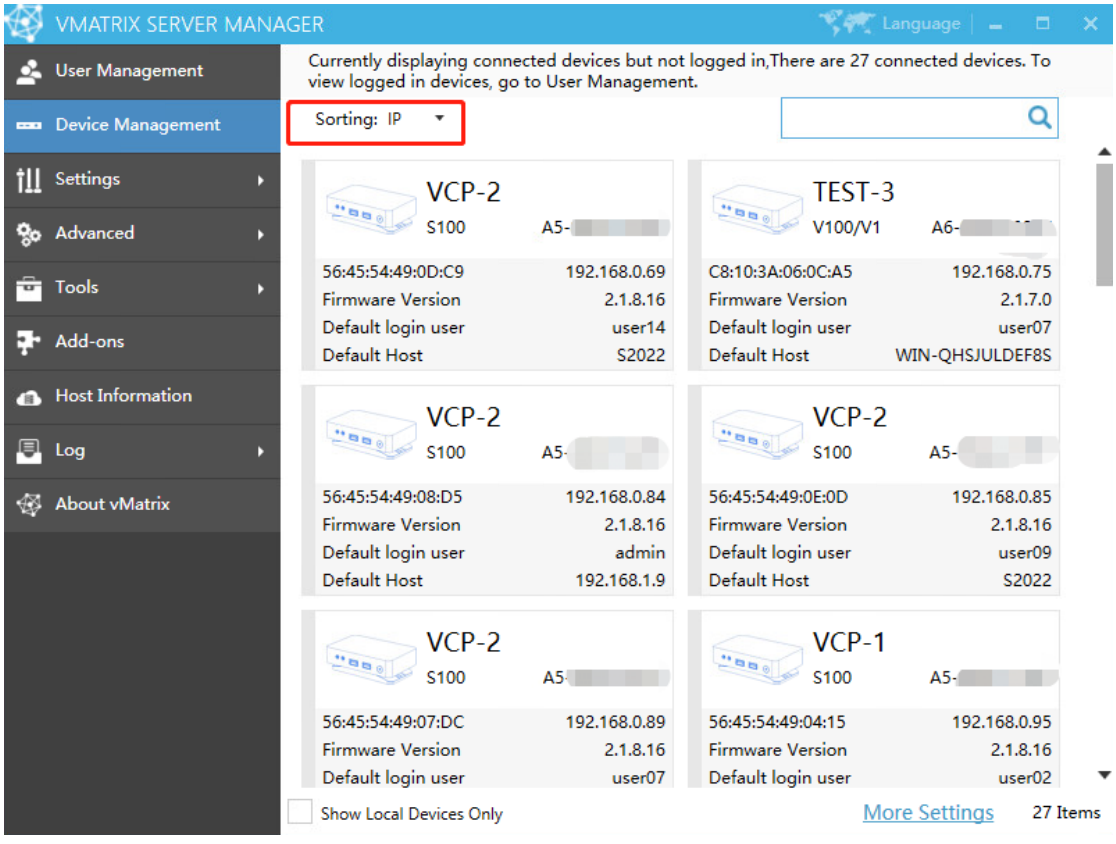
5.2.3 Sorting

The sorting function allows administrators to locate and manage terminals more conveniently and quickly.

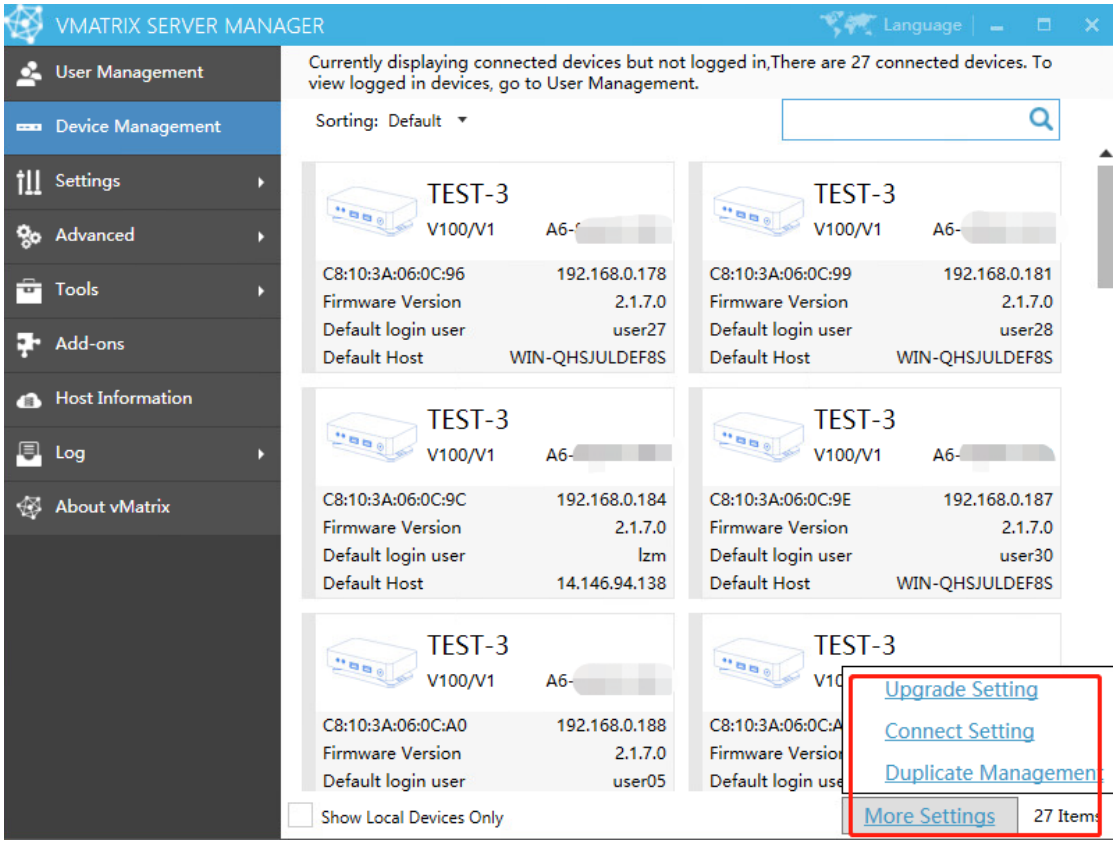
Sort by Default: listed in ascending order of Device Name and Serial Number.



Sort by IP: listed in ascending order of terminal IP address.



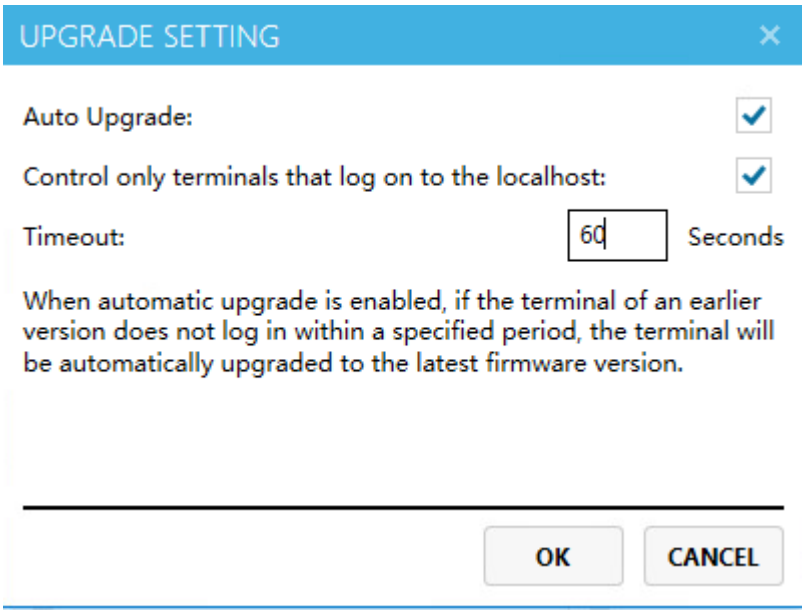
5.2.4 More Settings



■ **Upgrade Settings**

When automatic upgrade is enabled, if the terminal of an earlier version does not log in within a specified period (Customized by administrator), the terminal will be automatically upgraded to the latest firmware version.

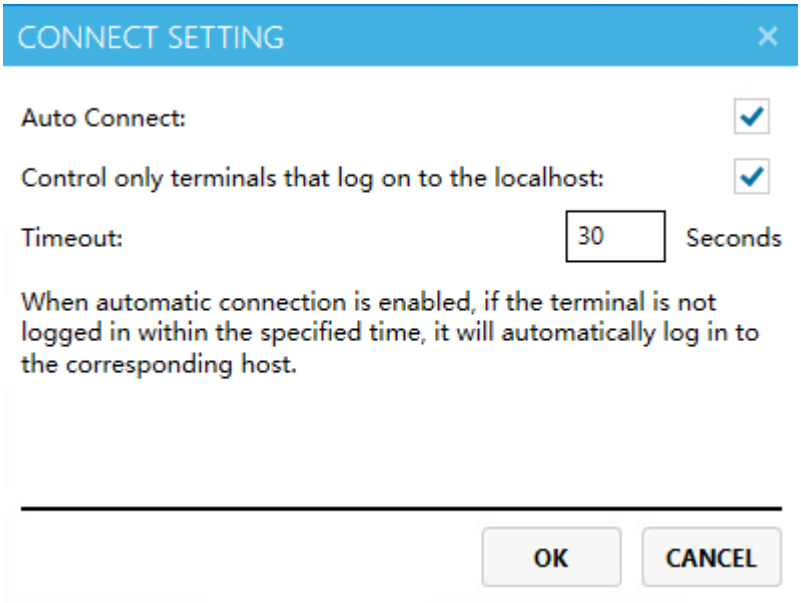
Check “Auto Upgrade”, check “Control only terminals that log on the localhost” if you need, enter a suitable waiting time and then click “OK”, the terminal will be automatically upgraded to the latest firmware version after the specified time.



- **Connect Setting**

When automatic connection is enabled, if the terminal is not logged in within the specified time (Customized by administrator), it will automatically log in to the corresponding host.

Check “Auto Connect”, check “Control only terminals that log on the localhost” if you need, enter a suitable waiting time and then click “ok”, the terminal will be automatically log in to the corresponding host after the specified time.



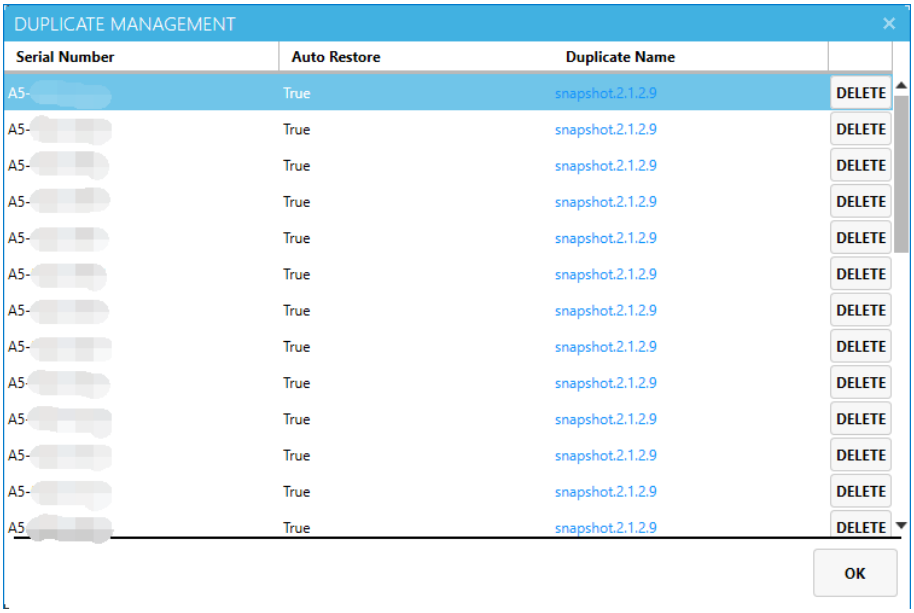
- **Duplicate Management**

View and delete the Duplicate stored in this host.

In some cases, setting up Auto Restore may cause some problems. E.g., if you set a

static IP for the terminal to generate duplicates and set Auto Restore, and the IP is occupied, the terminal cannot connect to the host. Then even if you modify the IP to connect to the network later, it will automatically restore to the previously generated IP, causing the terminal to not work normally.

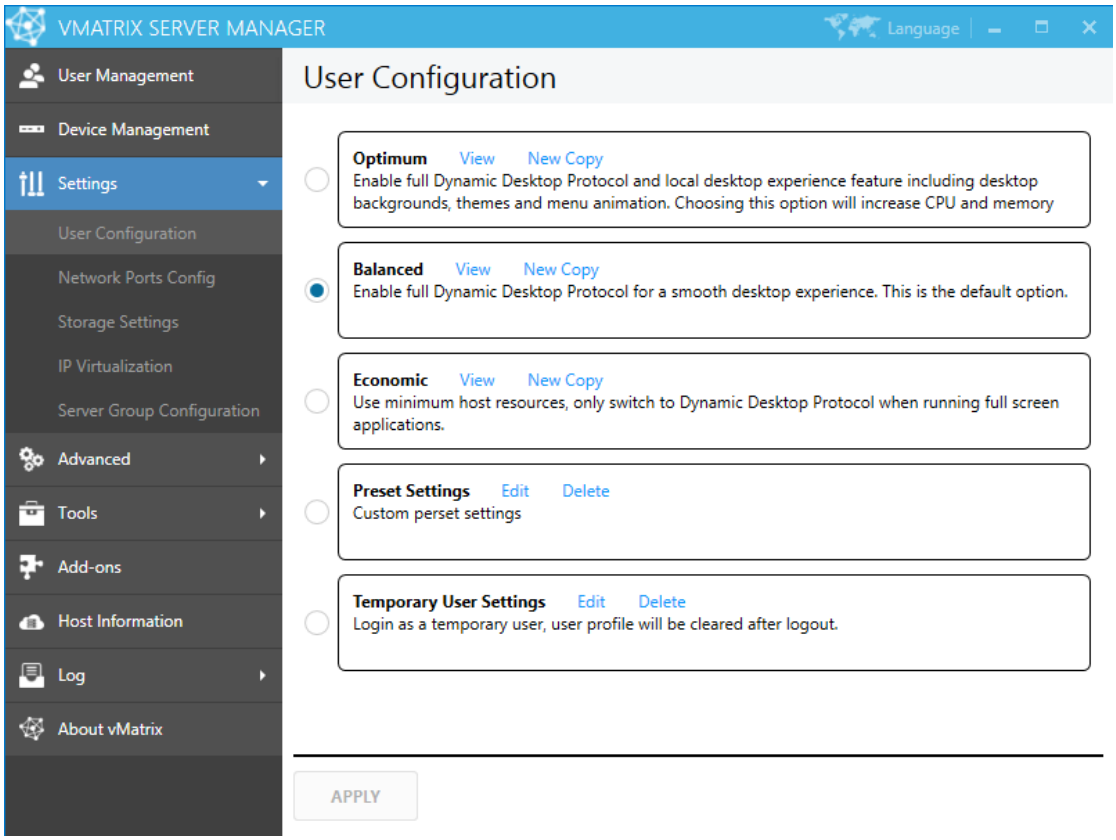
Find the corresponding duplicate in “Duplicate Management” according to the serial number and click "Delete".



5.3 Setting

5.3.1 User Configuration

Users who select "Default" in "Configuration Settings" will apply the User Configuration selected here, and the default is "Balance". You can create multiple configuration copies by yourself, and the newly created copies will be displayed in "Configuration Settings", to help you customize different department or job position. The preset "Optimum", "Balanced", and "Economic" cannot be modified or deleted.

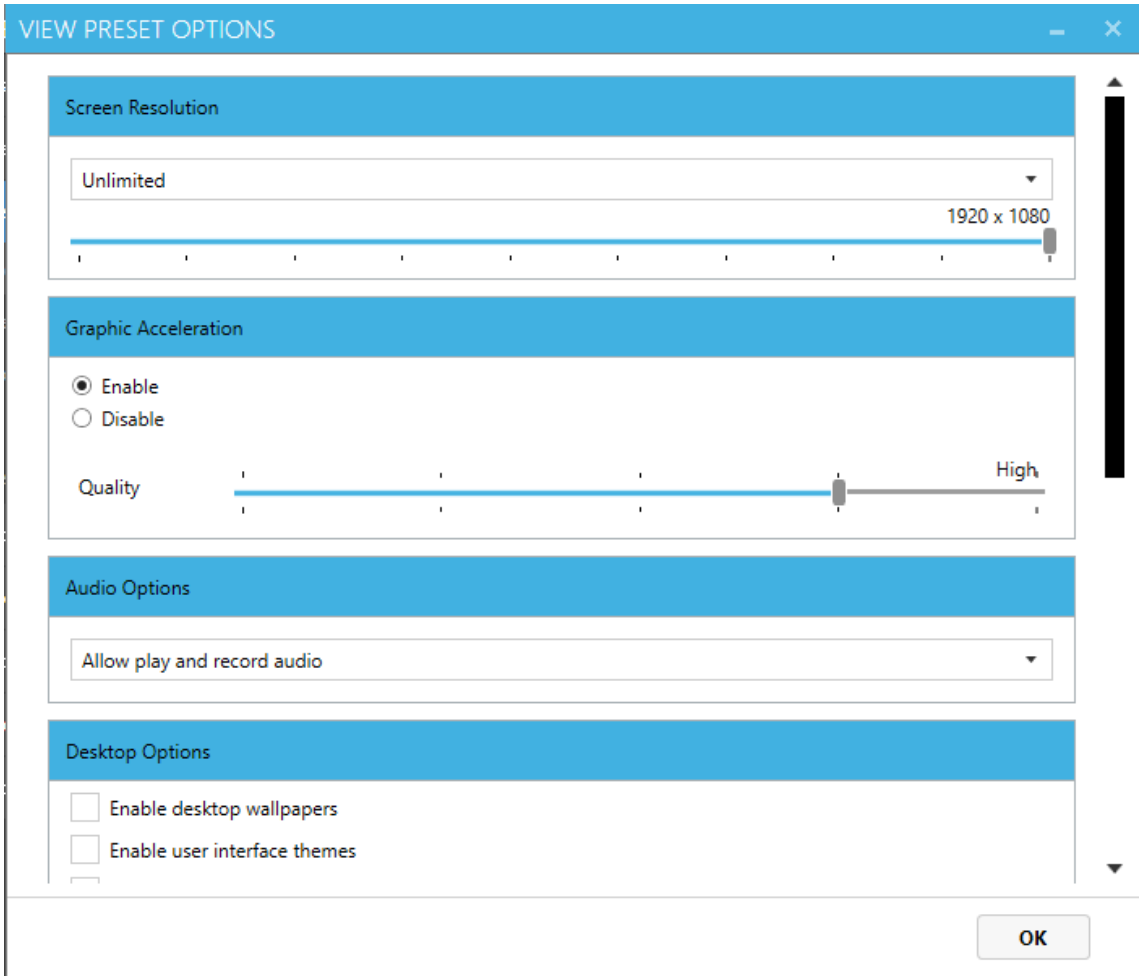


View: View the preset configuration.

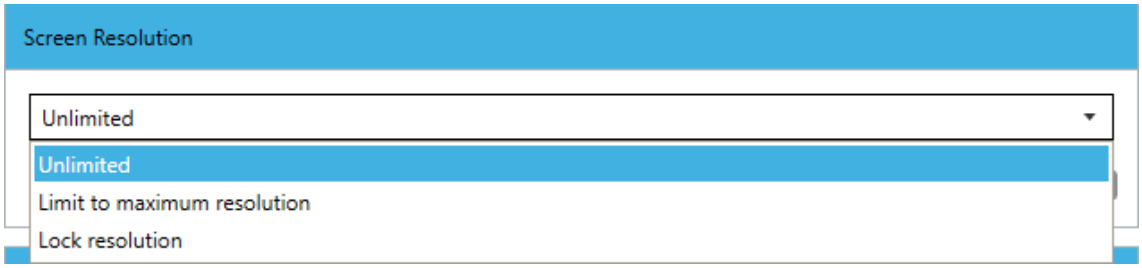
New Copy: Create a new configuration copy based on the preset configuration, and modify the configuration as needed.

Edit: View or modify the configuration copy that has been created.

Delete: Delete the configuration copy.



- **Screen Resolution:**

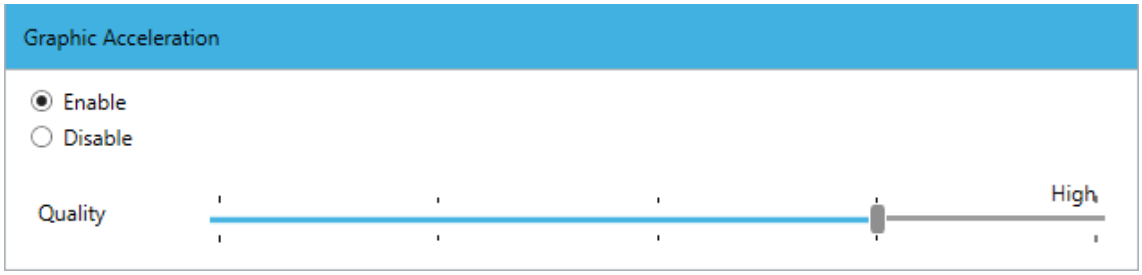


Umlimited: The desktop resolution is synchronized with the display resolution of the terminal login interface.

Limit to maximum resolution: The desktop resolution is synchronized with the display resolution of the terminal login interface, but it will not be higher than the maximum resolution limited here.

Lock resolusion: The desktop resolution is forcibly set to the locked resolution.

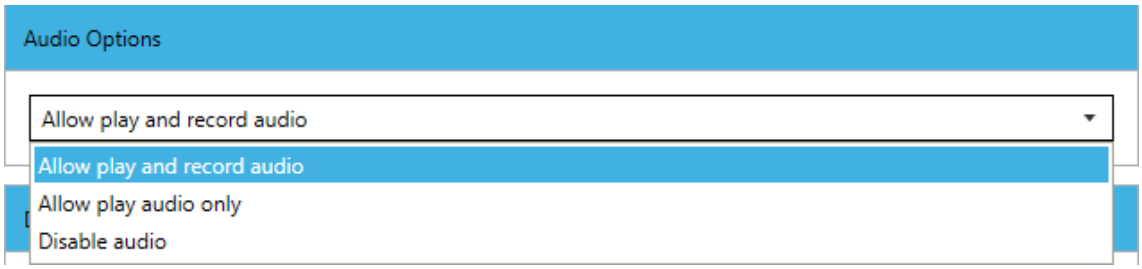
- **Graphic Acceleration:**



Enable (Recommended): Enable the self-developed Dynamic Desktop Protocol (DDP) to reduce the consumption of terminal screen resources and provide a smoother experience. Different image quality has different requirements for the host's CPU and network, and the default is high.

Disable: Turn off the Dynamic Desktop Protocol and use the RDP Protocol that comes with Windows, and some screen flash will appear. It is not recommended to disable Graphic Acceleration.

- **Audio Options:**

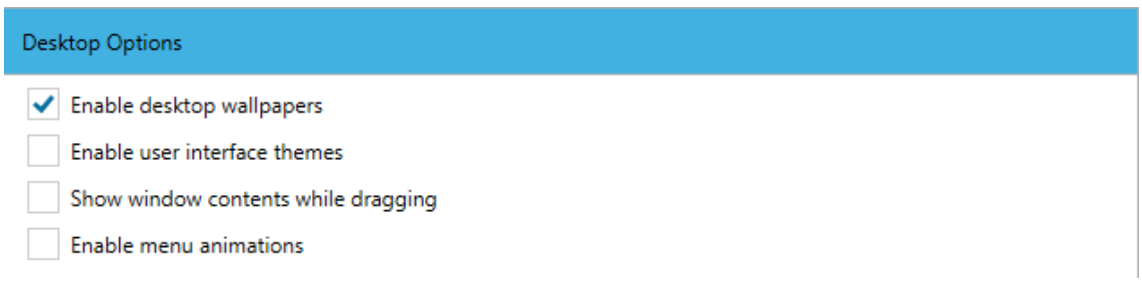


Allow play and record audio: Terminal users can listen to the sound and use the microphone. This option is selected by default.

Allow play audio only: Terminal users can only listen to the sound; the microphone is disabled.

Disable audio: Both the sound and the microphone are disabled.

- **Desktop Options:**



Enable desktop wallpapers: The user can customize the desktop wallpaper. If it is not enabled, it will be a black wallpaper (the server system needs to install the desktop experience component first).

Enable user interface themes: The user can customize the interface theme.

Show window contents while dragging: The contents of the window move along with the drag of the window. When it disables, only the frame of the window moves when the window is dragged.

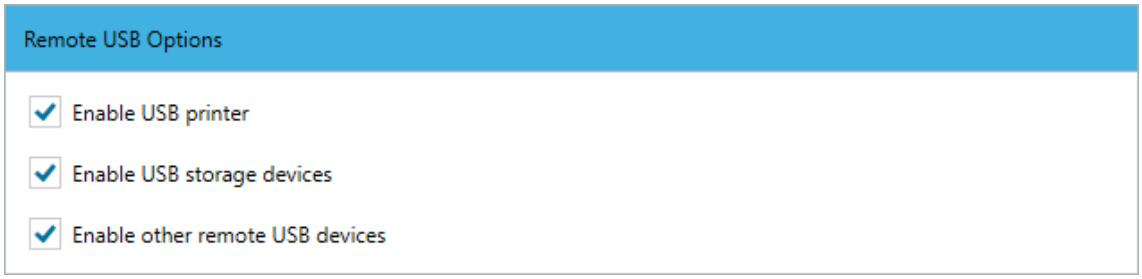
Enable menu animations: The animations will be displayed when you click start or others menu.

Note:

1) All of the desktop options are not checked by default. Enabling the options will consume more system CPU and network resources.

2) After Enable desktop wallpapers is checked, a screen flash will appear when the terminal logs in. This is a normal phenomenon, and it will return to normal after a few seconds.

- **Remote USB Options:** If the option is not checked, only input devices such as mouse and keyboard can be used.

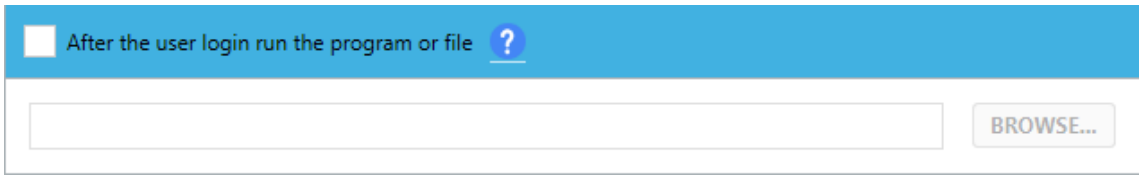


Enable USB printer: Check it to allow the use of USB printer devices on the terminal.

Enable USB storage devices: Check it to allow the use of U disk and mobile hard disk devices on the terminal.

Enable other remote USB devices: Check it to allow the use of other USB devices except U disks, mobile hard disks and USB printer devices on the terminal.

- **After the user login run the program:**



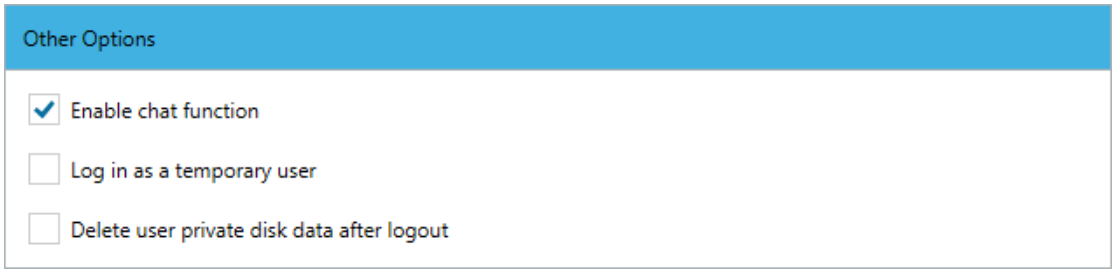
Checked this: After the users log in, the program or file under the path is automatically opened. The users are only allowed to run the currently specified program. After the program or file is closed, the user session is automatically logged out.

If you need to run a file automatically, please follow the format: program under a certain path + space + file under a certain path

E.g., "C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.exe"

"D:\123.doc"

- **Other Options:**



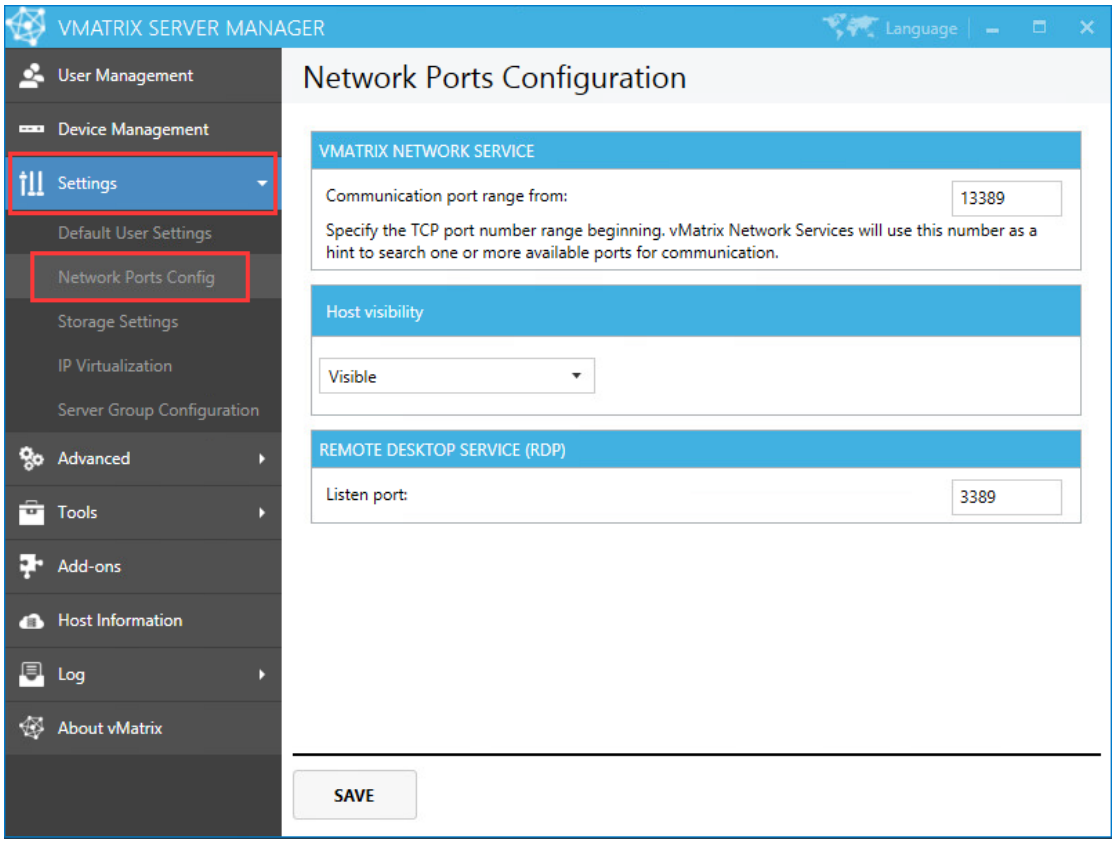
Enable chat function: Check to allow users to use chat tools.

Log in as a temporary user: Checked this, the user will become a temporary user. When a temporary user logs in, a temp folder will be generated to temporarily store the user profile of the user. The temp folder will be automatically deleted after the user logs out. (If you need to revert to a normal user, just uncheck this)

Delete user private disk data after logout: Checked this, the user's private disk data will be cleared every time when the user log out.

5.3.2 Network Ports Configuration

Set the Windows Remote Desktop Services port number, the network communication port number of the vMatrix Server Manager, and whether the host can be automatically discovered by the client users. Using 3389/13389 as default port numbers if without specific reasons.



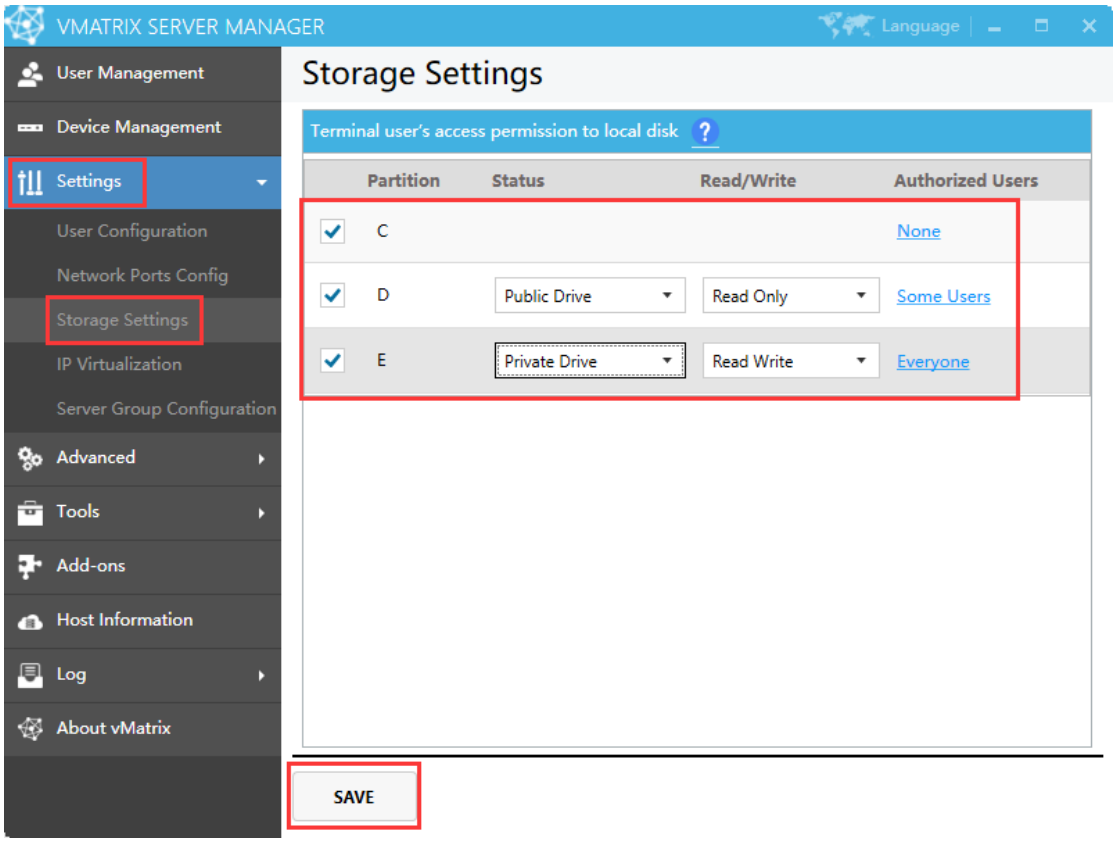
Communication port range from vMatrix Server Suite NETWORK SERVICE: vMatrix Server Manager uses TCP 13389-13393 by default, plus one port for each end user. For example, if 10 users log in to vMatrix host, the ports used are 13389-13403.

Host visibility: Control whether to display vMatrix host to the host list of the terminal. If hidden, you can also search for vMatrix host by manually entering the host's IP address.

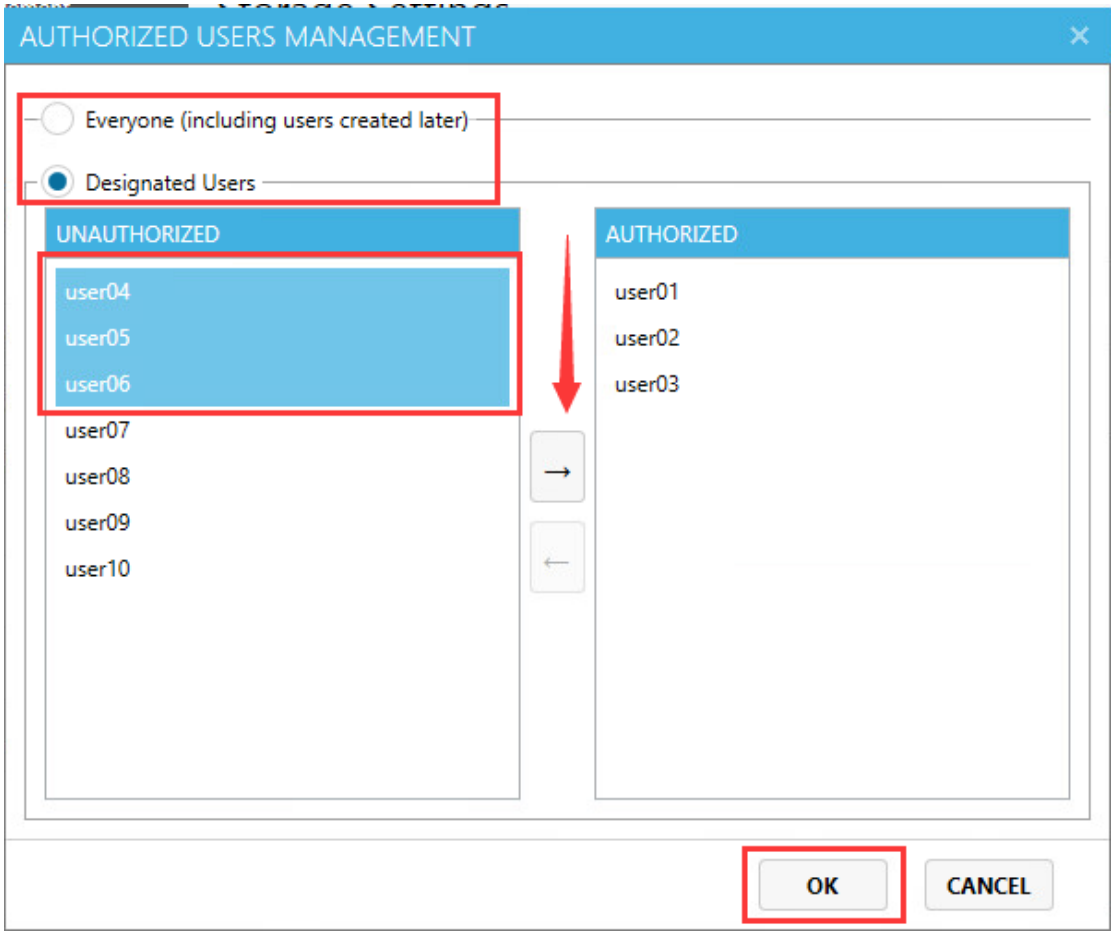
Listen port of REMOTE DESKTOP SERVICE (RDP): The remote desktop service uses TCP port 3389 by default. If there is no special requirement, just keep the default.

5.3.3 Storage Settings

vMatrix allows admins to manage terminal users' access to the local drives including external drives connecting to the host.



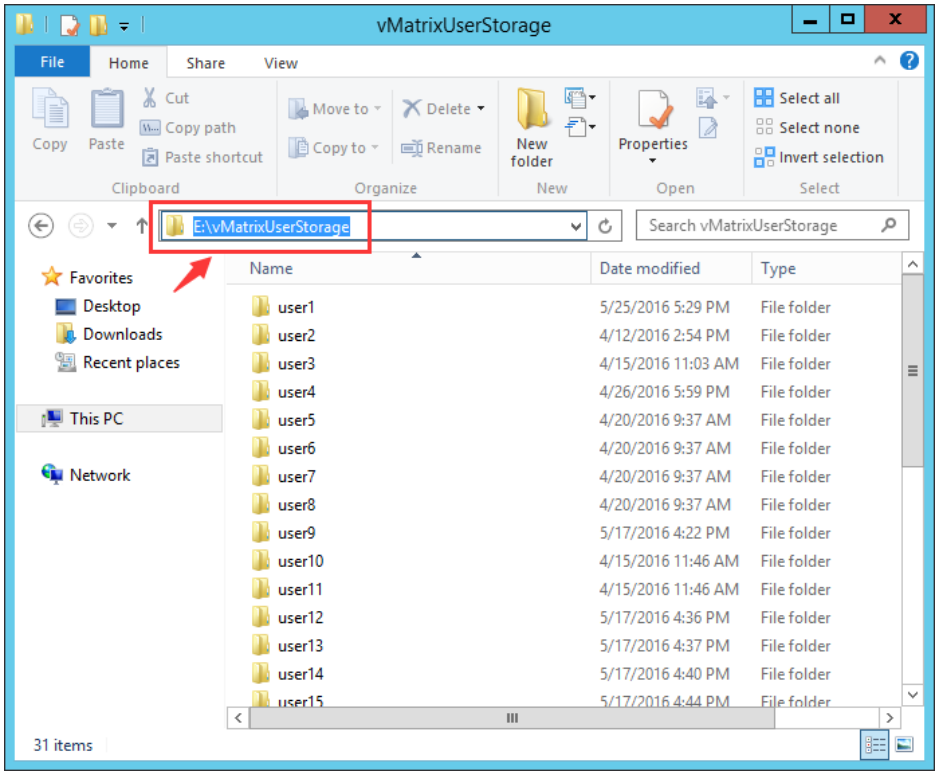
- Status
  - Unchecked (Unmanaged): Do not manage the current disk.
  - Public Drive: files in this drive are accessible to all authorized users.
  - Private Drive: files in this drive are only visible to the owner and the administrators.
  - Read/Write: setting user's read-write permission.
  - Authorized Users: only the authorized users and admin can access the drive.



Notes:

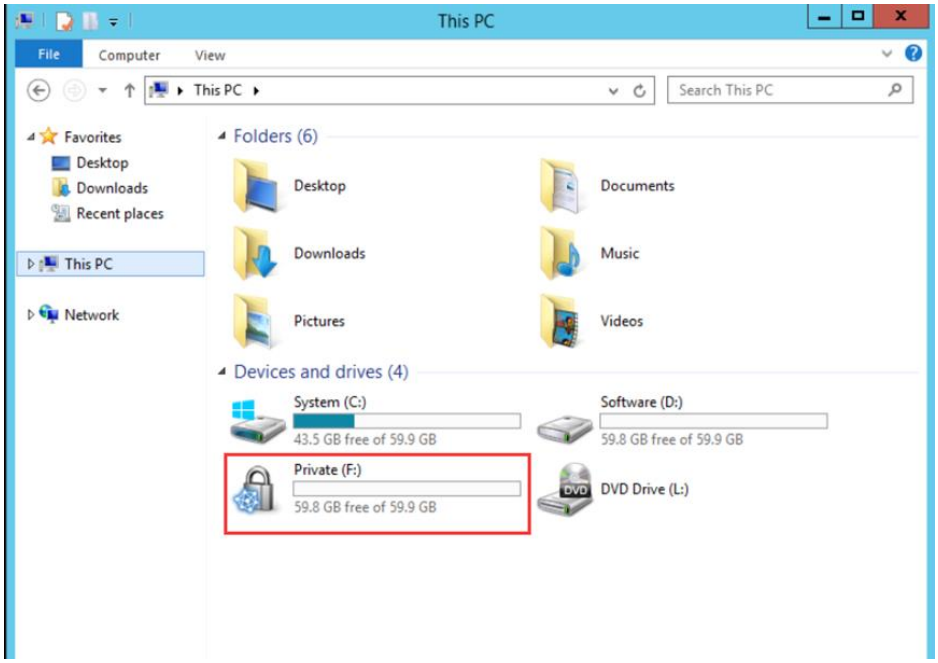
- The storage setting supports multiple private drives, excluding the C drive.
- Disks of non-NTFS and Non-REFS (such as FAT and exFAT) file system do not support read/write control.
- The storage setting works for users only, not for administrators.
- Administrators cannot join the remote desktop users group, otherwise they will not be able to access disks that are set as private disks
- Private drive settings only work for users running on a vCloudPoint zero client. Private drives in the File Explorer viewed by a zero client user are those drives with a lock icon  .
- Settings saved to the system may take longer time for drives with many files.

■ **Administrator's view on a private drive:**



■ **User's view on a private drive:**

Private drives is the drive with a lock icon .



5.3.4 IP Virtualization

Introduction: With Shared Computing solution, multiple users have their own desktop sessions on a single host OS. Because these sessions are on the same OS, they all share the IP address of the host for network communication. The sharing of an IP address for multiple sessions sometimes causes problems in an environment. IP virtualization allows a unique IP address for each user session on the host for its network communication, fixing compatibility problems for use cases where a unique IP address is required for each user session.

Enable IP virtualization: check the "Enable IP virtualization" option and choose the appropriate method(s) to assigned IP addresses. Users who are not assigned a virtual IP will still use the host's IP address.

Use Cases:

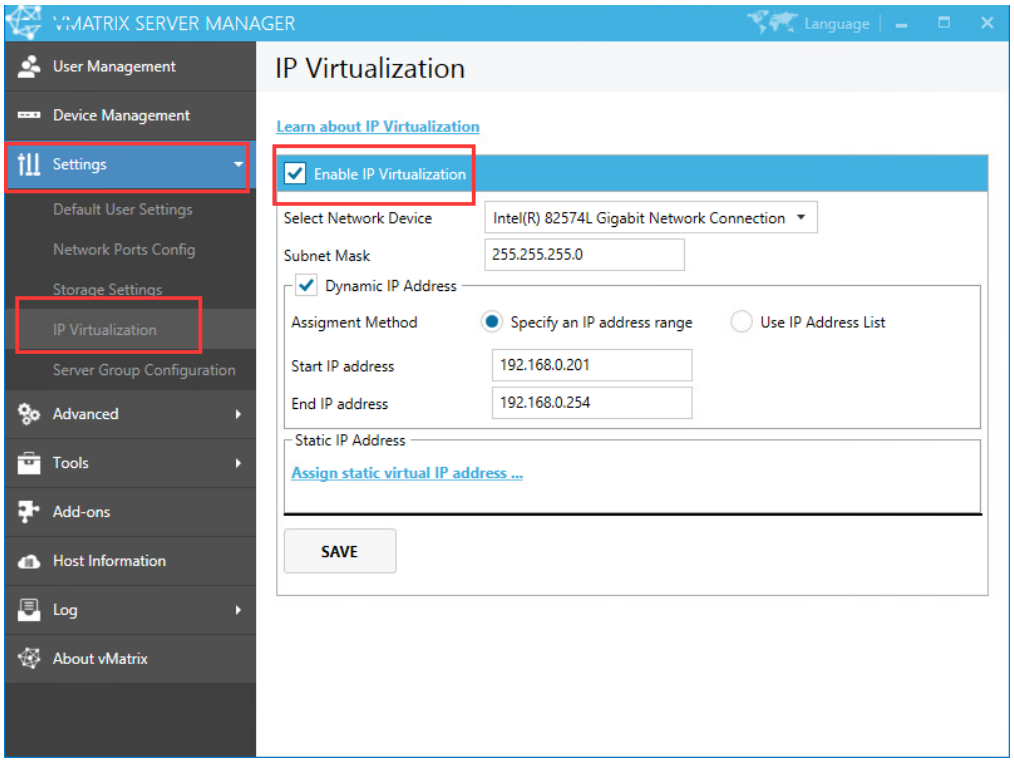
IP virtualization solves the compatibility problem that some users need unique IP addresses in the desktop session based on the environment:

- Certain applications, such as CRM and CTI, require a unique IP address that can't be the same as any other instance of the application.
- Tracking of traffic by IP address.
- Filtering or controlling traffic based on IP address.

Things to know before configuration:

■IP Virtualization configurations require certain network knowledge. Incorrect configurations may cause IP conflict or network failure.

■When IP virtualization is activated, the total number of LAN IP address used by the Shared Computing solution the will be double as before. Besides the IP address used by the client device, each client users will have an additional virtual IP address on the shared host for network communication.

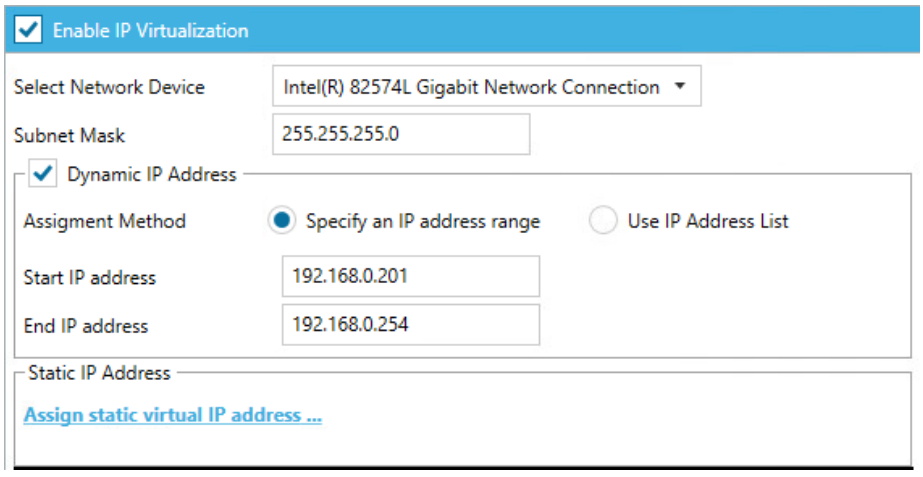


How to configure:

You can allocate a range of list dynamic IP addresses to users or assign a static IP address to each user.

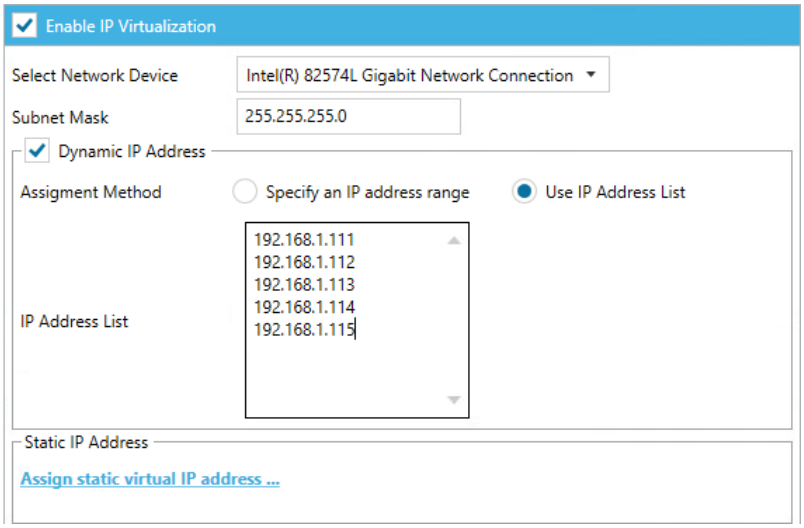
●Dynamic IP addresses

a) IP address range: fill in the range of network segment to be allocated in the starting IP address and ending IP address. The default subnet mask is 255.255.255.0, which can be modified as required.

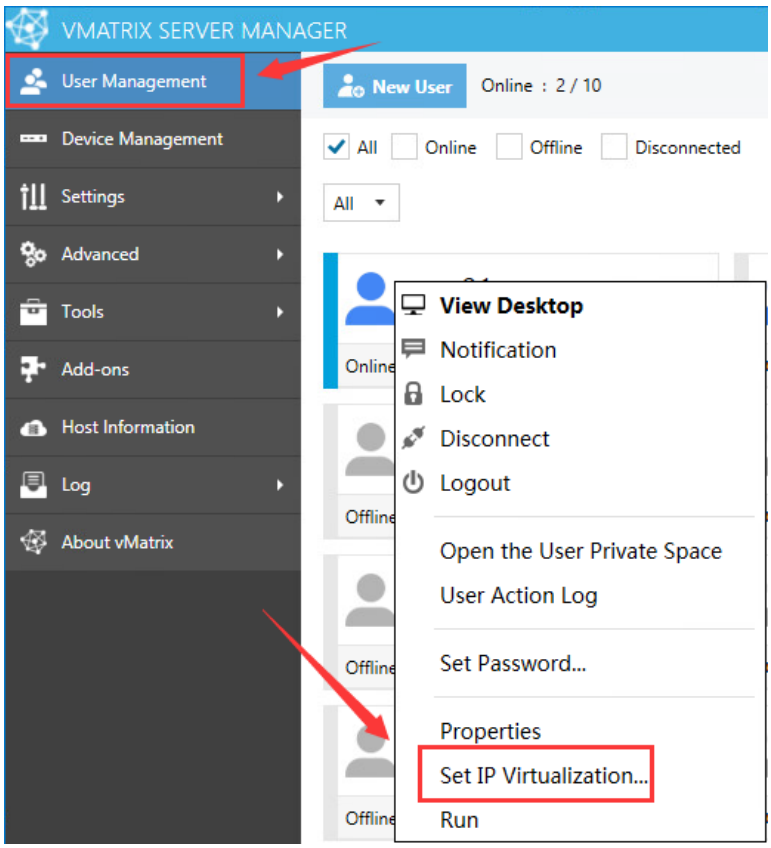


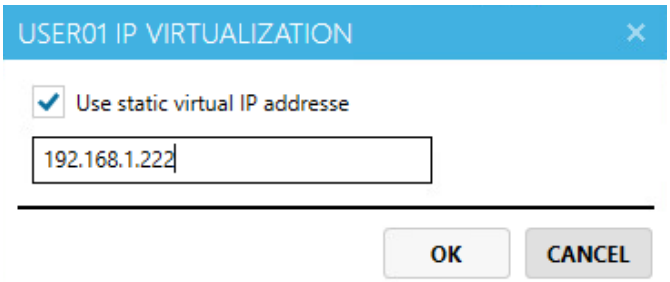
b) IP address list: fill in the IP addresses to be assigned in the IP address list box, one IP

address each line. The default subnet mask is 255.255.255.0, which can be modified as required.

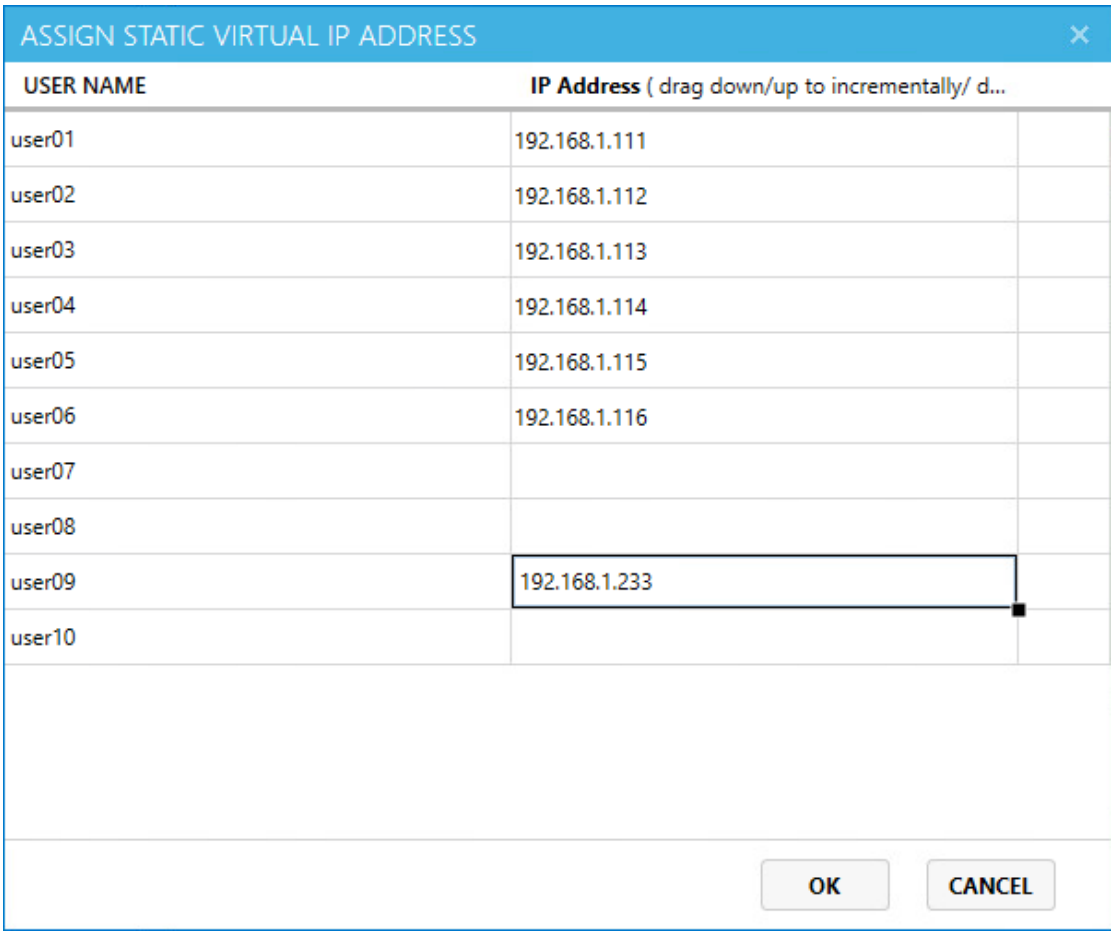


●Static IP addresses: in the User Management page, select the user and right-click to set IP virtualization. In the pop-up window, check " Set IP Virtualization... ", fill in the address and click "OK" to apply.





You can select multiple users to assign static IP addresses at once.



Notes:

- When enabling IP virtualization, please set a static IP address, which do not in the virtualization IP address pool, for the host.
- Dynamic IP addresses and Static IP addresses can be used at the same time.
- IP virtualization can only be set for a single network card. If the server has multiple network cards, the terminal needs to log in to the host through the network card with IP virtualization enabled, otherwise IP virtualization will not take effect.
- If the host has multiple network cards, the virtual IP address range must be in the same network segment as the current network card. Otherwise, client devices will be disconnected when logging in.
- If the allocated virtual IP address has been occupied or the dynamic IP address pool

runs out, the virtual IP address will not be effective on the user session and the user session will continue to use the host's shared IP address.

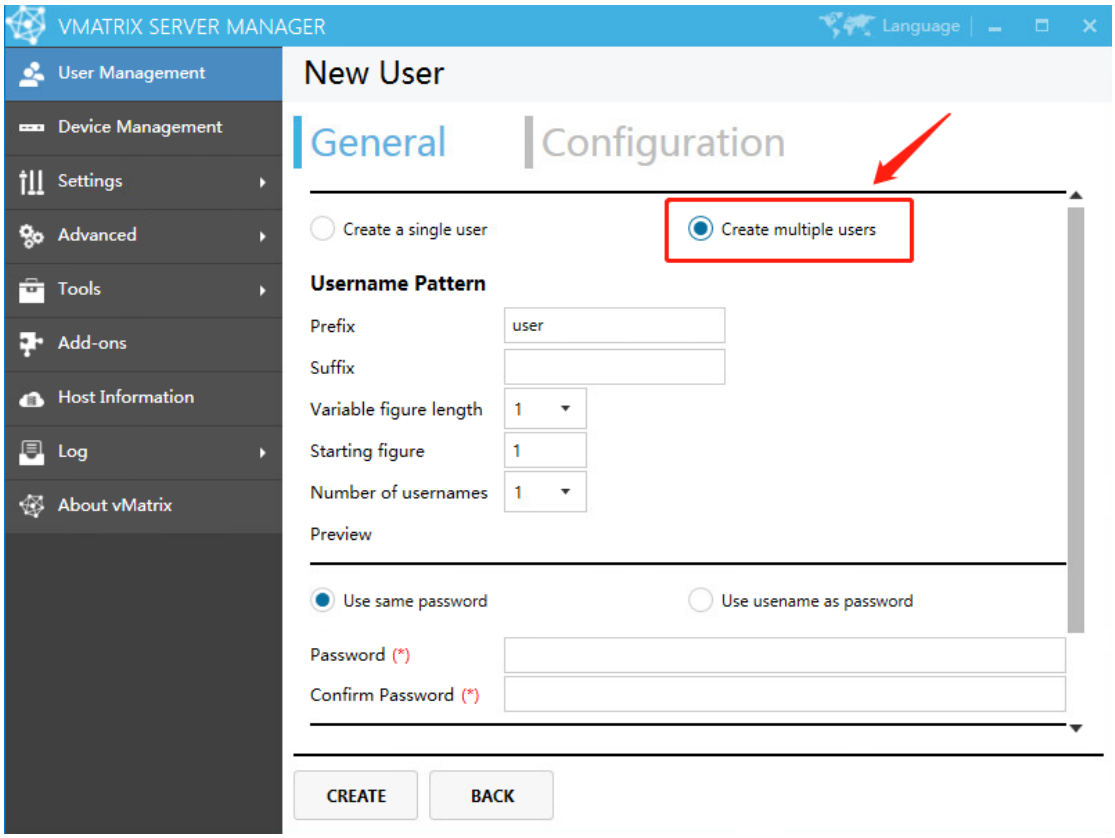
5.3.5 Server Group Configuration

Server group configuration allows the IT admin to set connection polices for hosts within a server group.

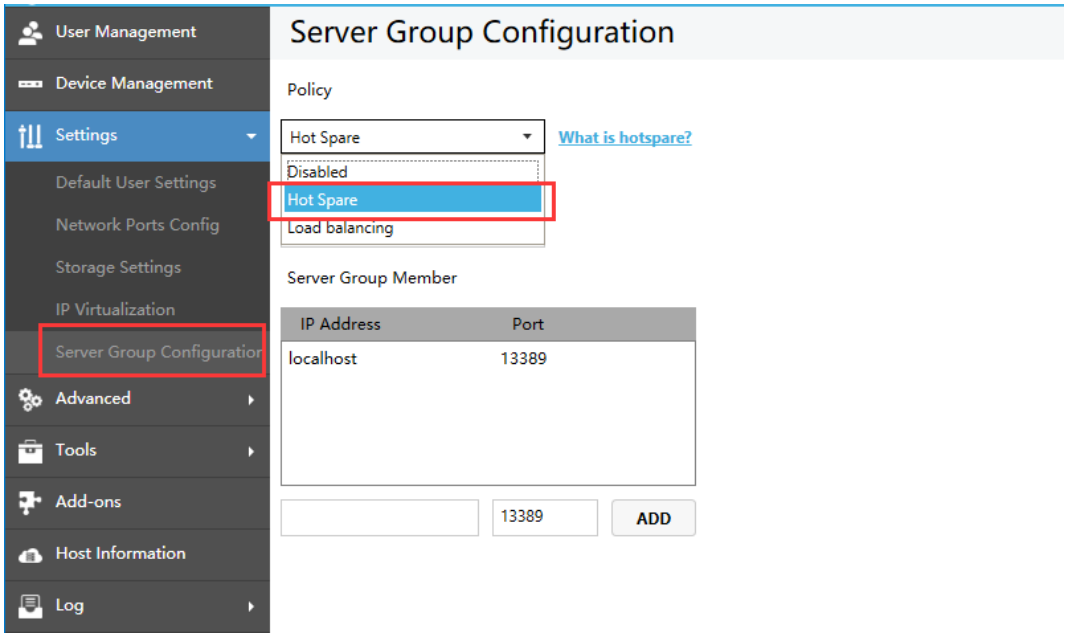
- **Hot Spare:** hot spare is a fail-over policy to ensure business continuity for a server group with multiple running hosts. With hot spare enabled, when the preferred host fails, the users running on it will automatically log into an alternate host in the server group according to a preset priority order.

How to configure:

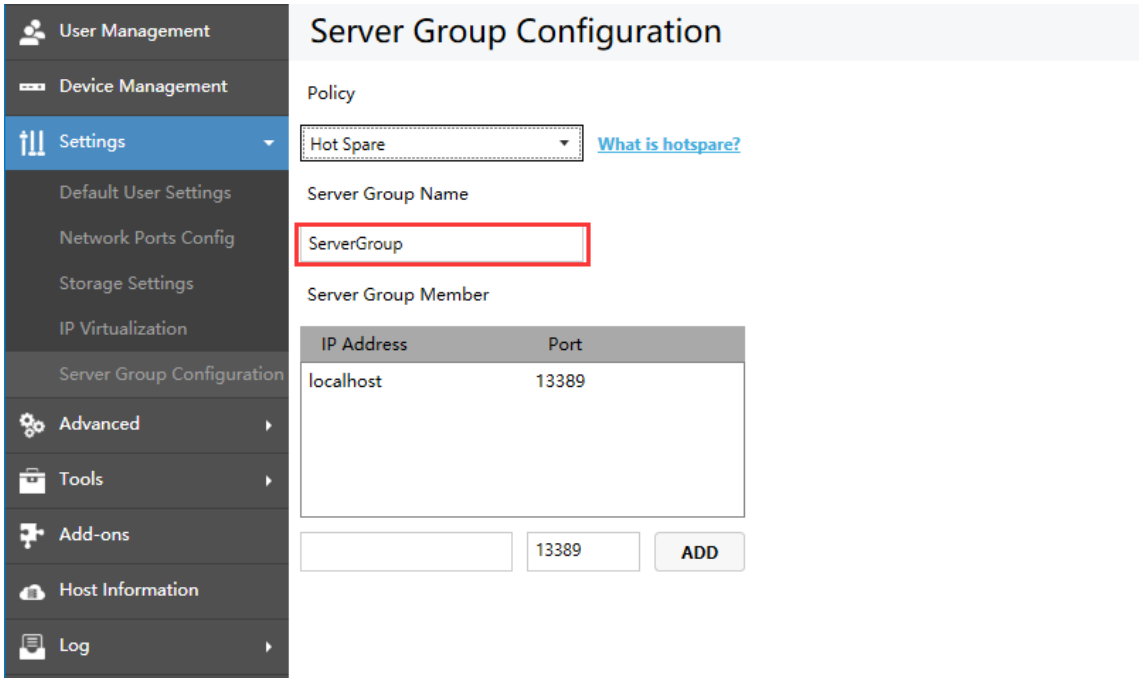
1. Create same user accounts on the shared host.



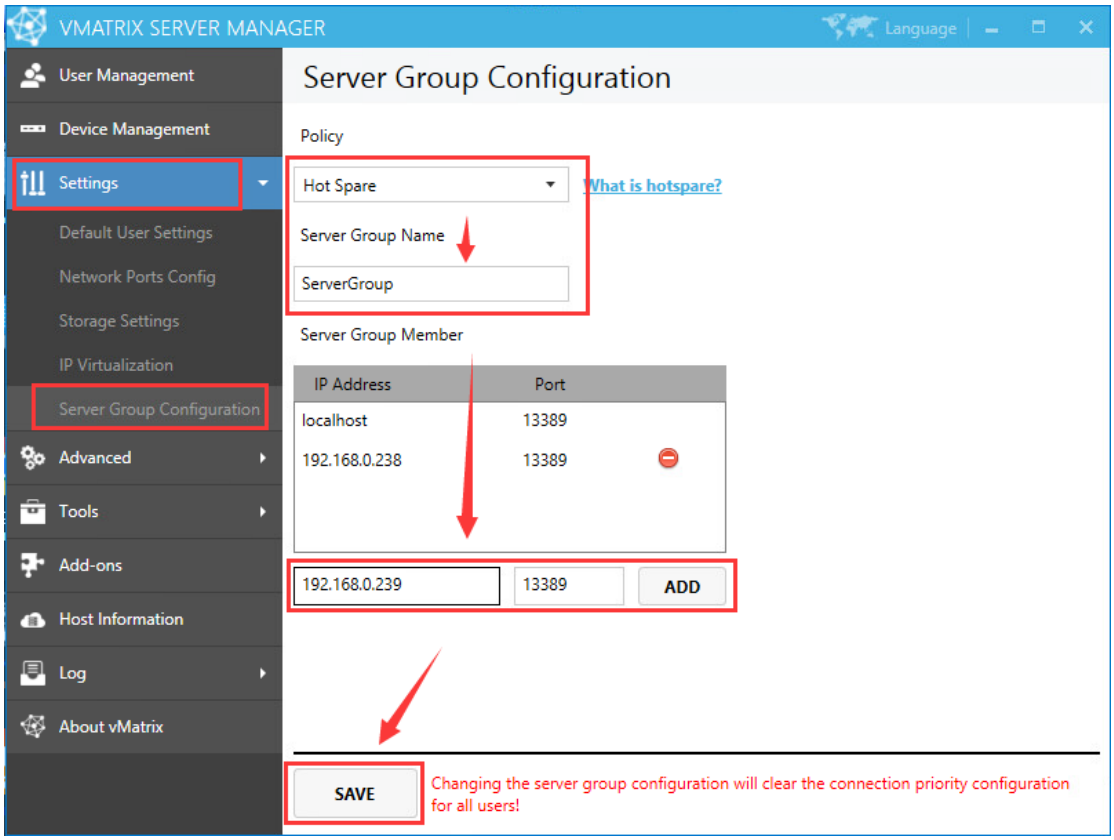
2. At the Settings page of vMatrix Server Manager, enable the "Hot Spare" option.



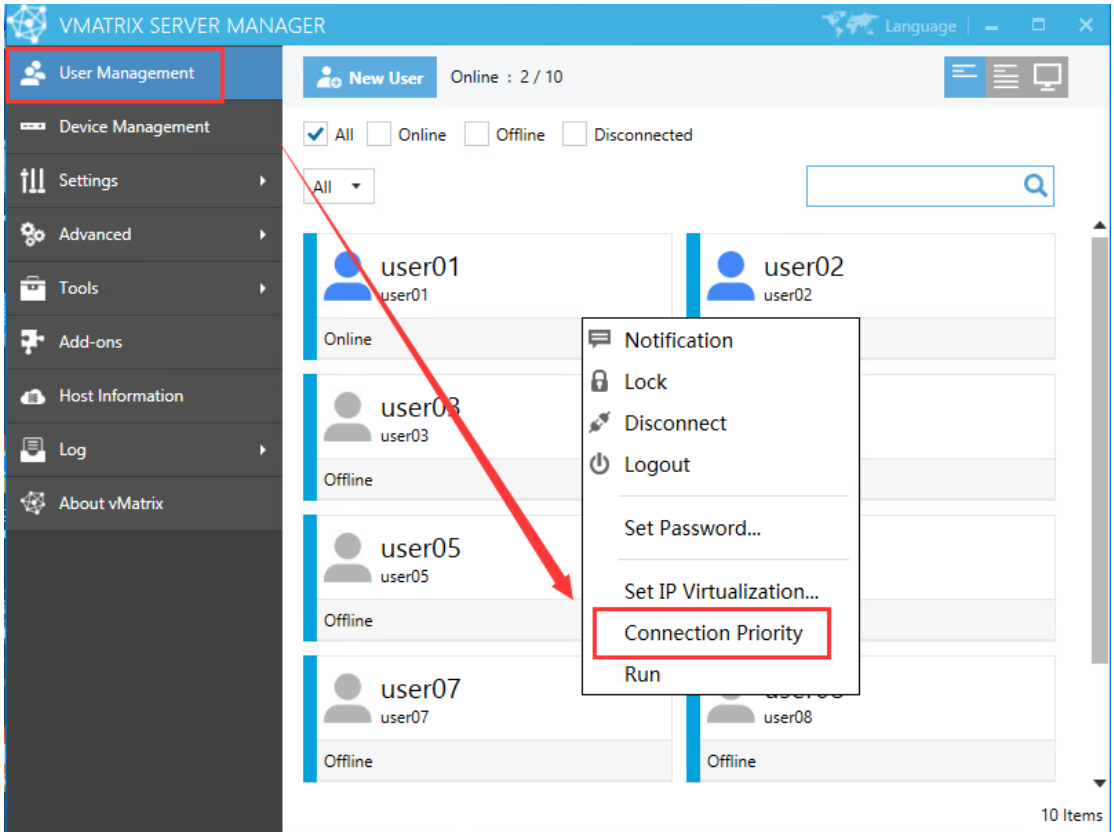
3. Customize a Server Group Name.

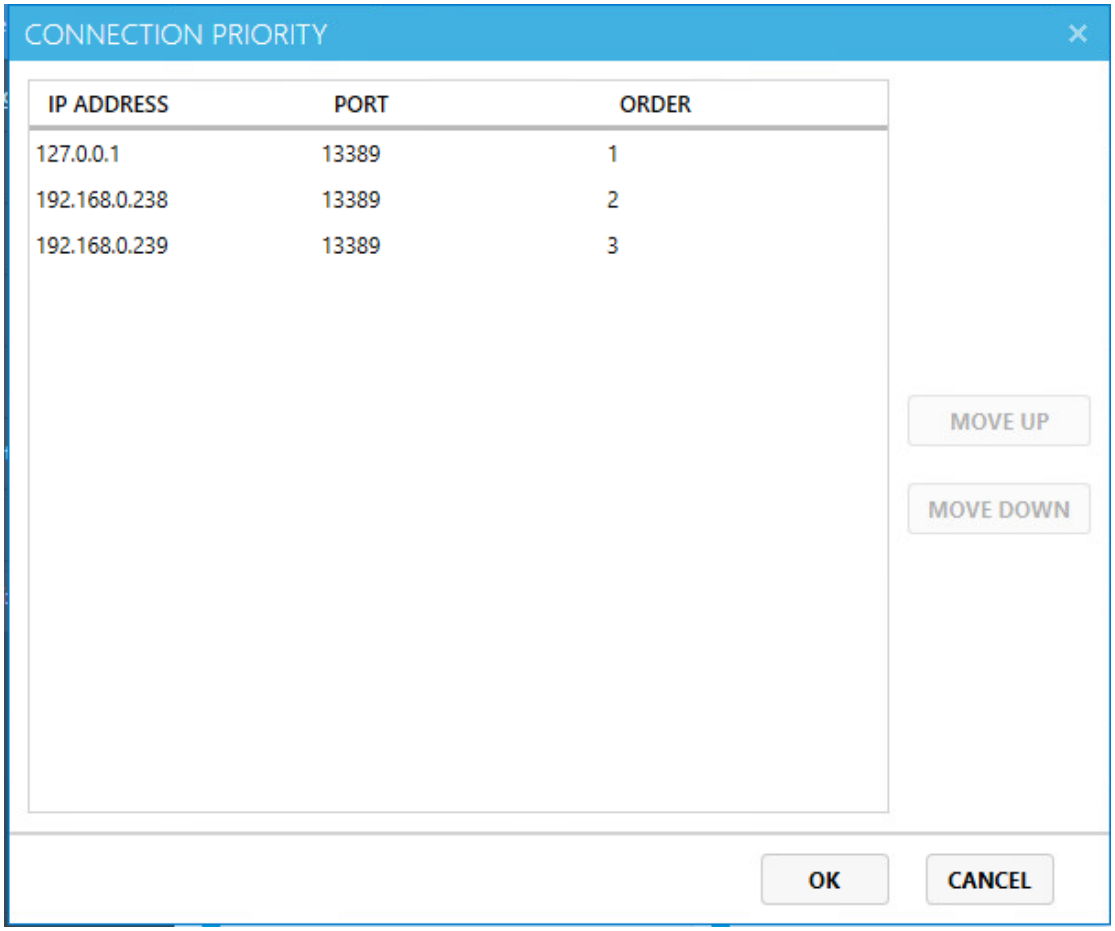


4. Enter the IP addresses that ready add to other hosts of the server group. If the port number of "Settings" - "Network Port Configuration" - "Network Service" has modified, please enter the modified port number. If it has not modified, keep the default, and click the "Save" after adding.



5. At User Management page, select users and set “Connection Priority” for them.





6. Repeat the above steps on other shared host in the server.

Note:

1) The Connection Priority set by the primary and secondary servers for users should be the same.

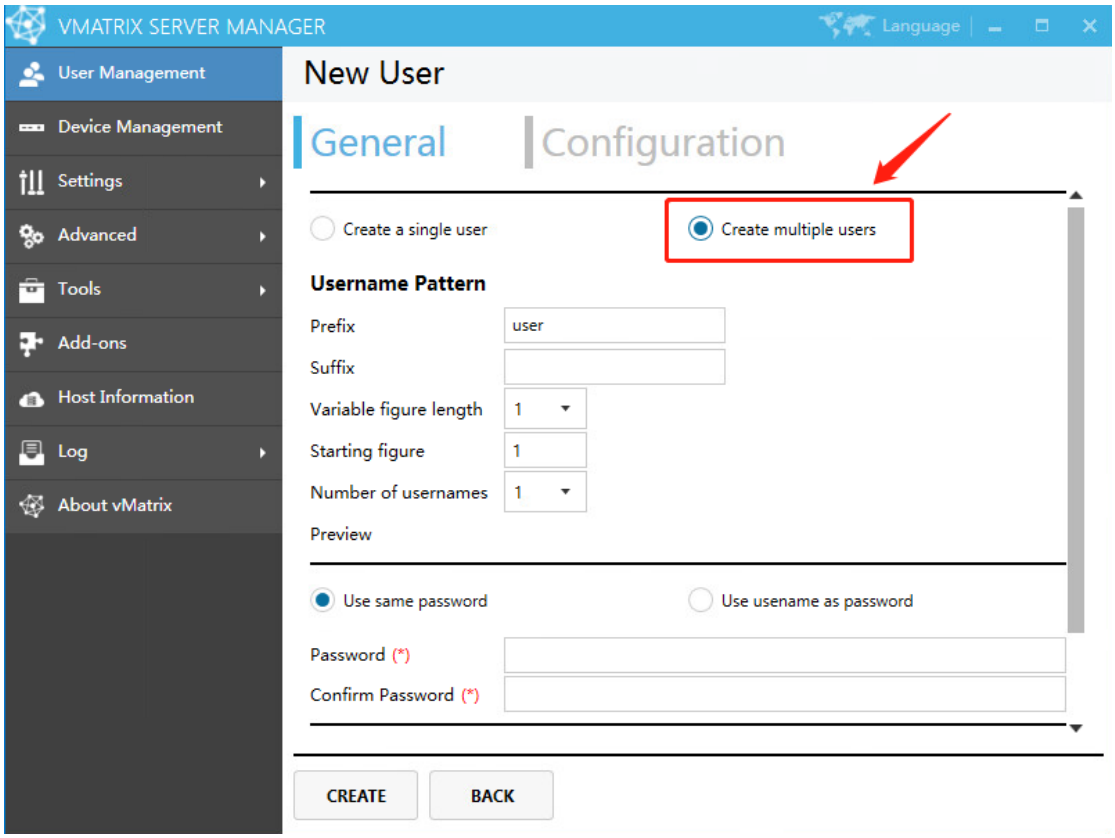
2) When the primary server is down or disconnected from the network, users will reconnect to the secondary server according to the preset Connection Priority.

3) To connect to the primary server when it is back online from a failure, users simply sign their session off from the alternate server and connect again. If there are 2 or more same active sessions in the server group, the last session that the user connects to will be connected, regardless of the connection priority.

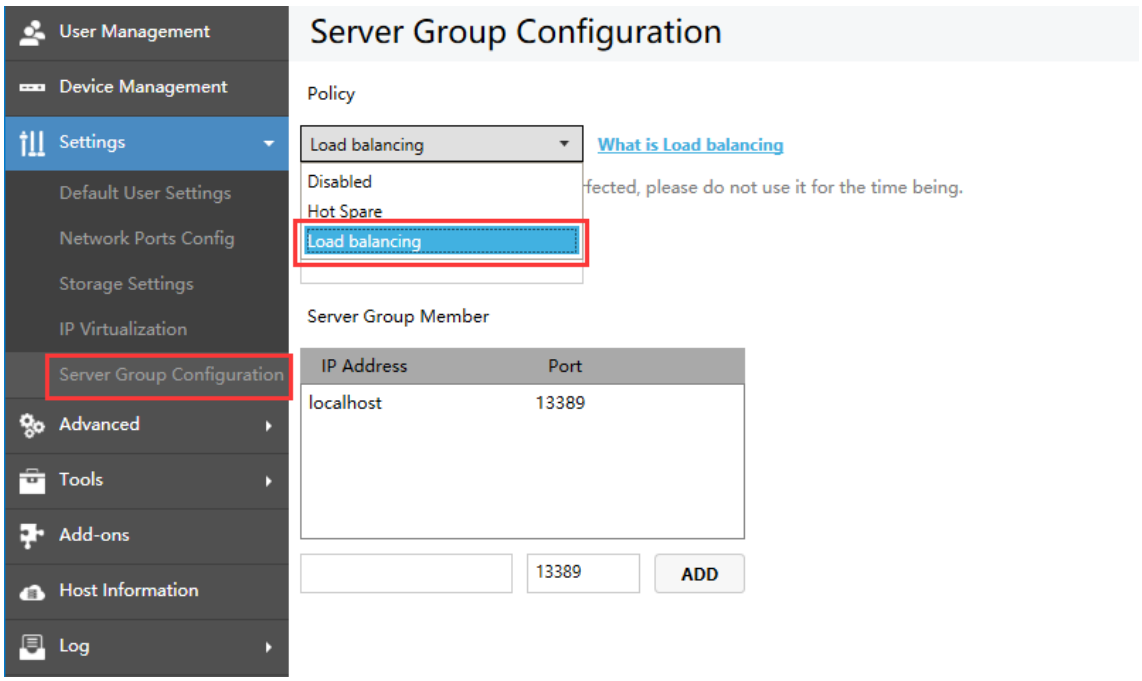
- **Load Balancing:** load balancing is the process of distributing compute resources across multiple hosts. It efficiently distributing incoming user login requests across a group of hosts according to the resources availability. This ensures no single host bears too much workload.

How to configure:

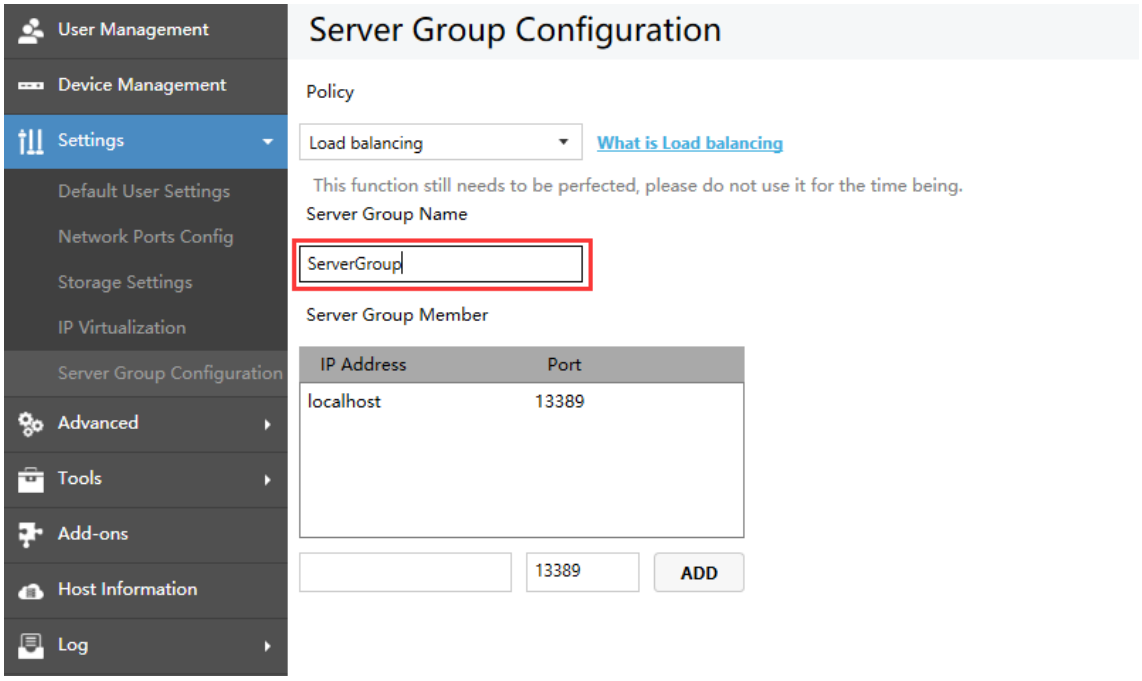
1. Create same user accounts on the shared host.



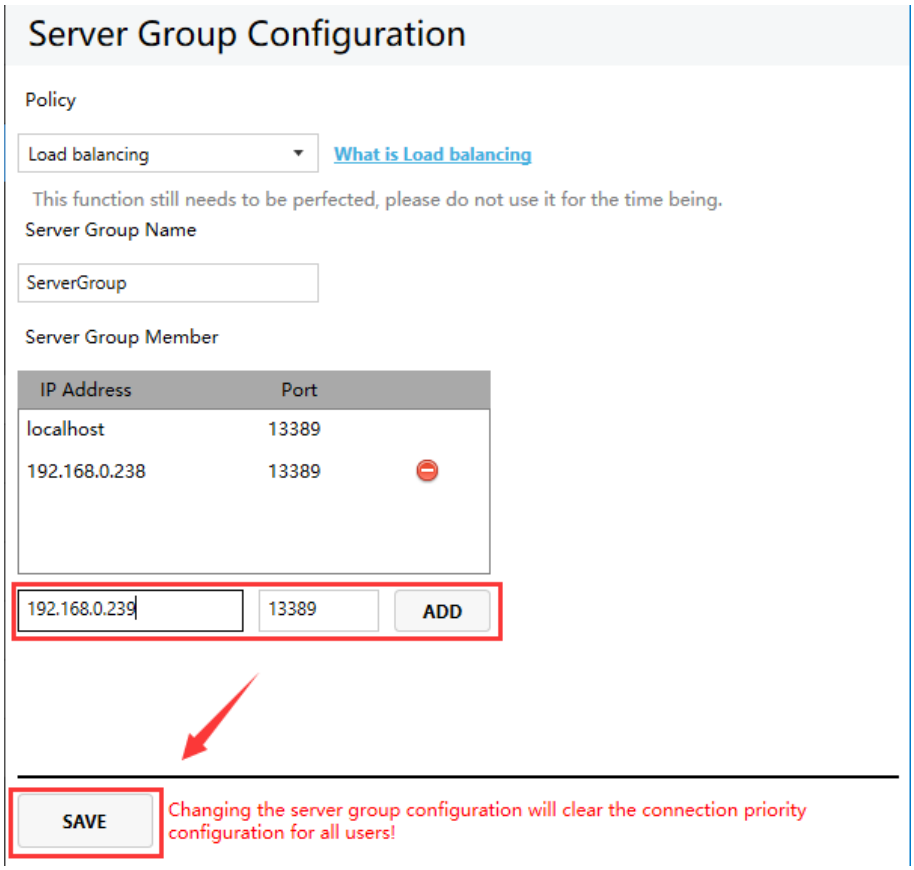
2. At the Settings page of vMatrix Server Manager, enable the “Load Balancing” option.

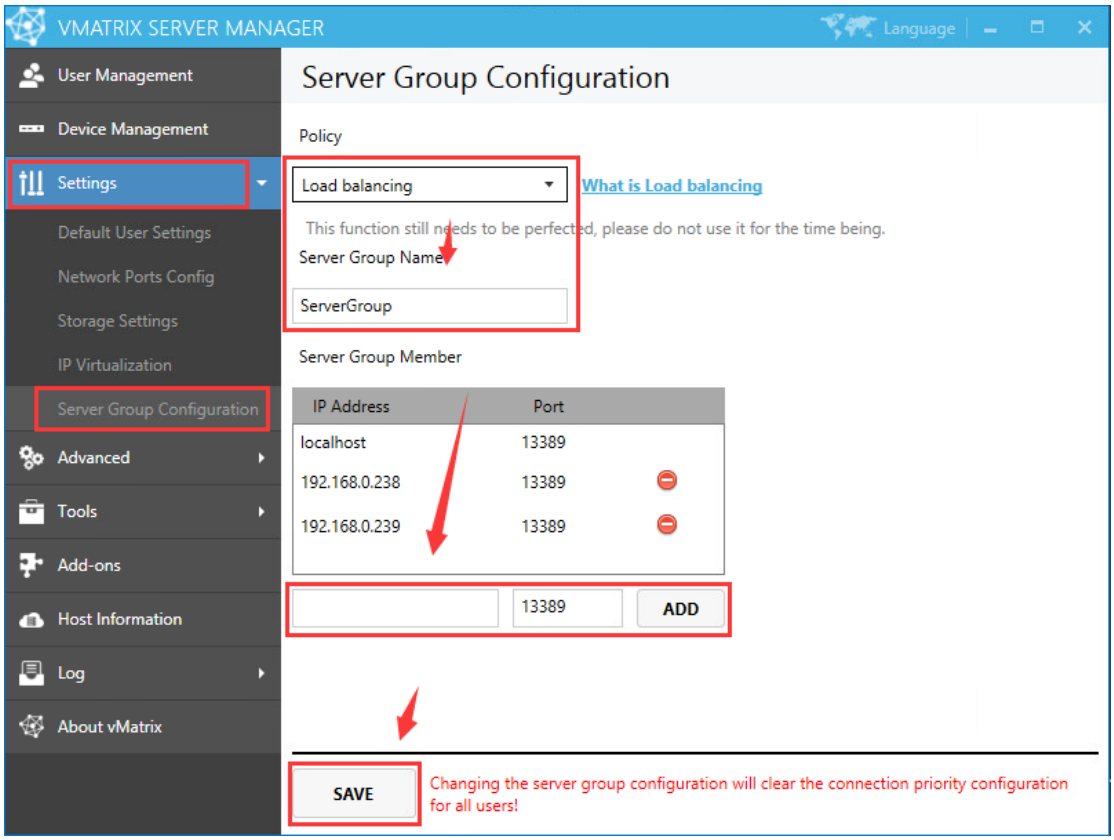


3. Customize a Server Group Name.



4. Enter the IP addresses that ready add to other hosts of the server group. If the port number of "Settings" - "Network Port Configuration" - "Network Service" has modified, please enter the modified port number. If it has not modified, keep the default, and click the "Save" after adding.





5. Repeat the above steps on other shared host to add them to the same server group.

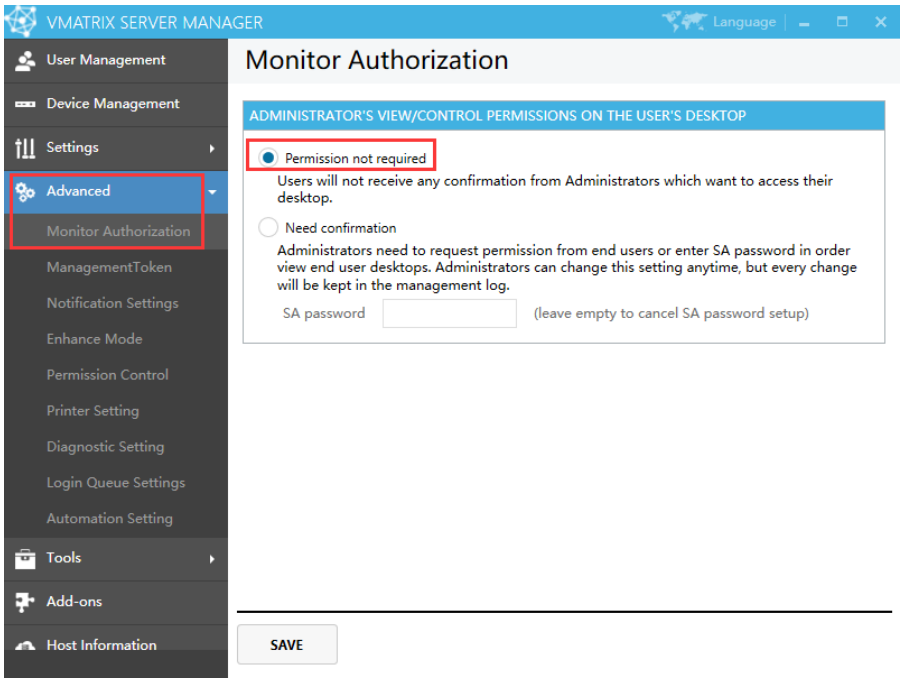
Note: With vMatrix Server Manger version 2.7.0, hosts in the group are assigned to users based on their current memory availability. More available options, such as CPU workload, and number of active users, will be introduced in future released versions.

More about Server Group Configuration:

- The username and password created on the primary and secondary servers must be the same.
- Fill in the correct server group name, group member IP address and port.
- After hosts join a server group, the host name displayed in the host list of the terminal device will be the server group name instead of the host name.

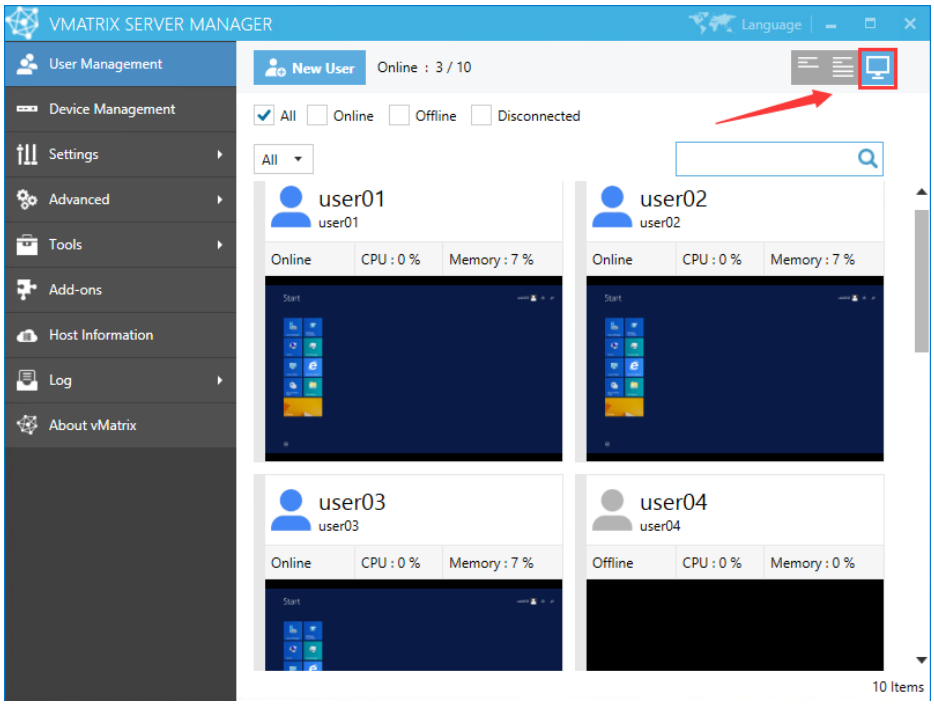
5.4 Advanced

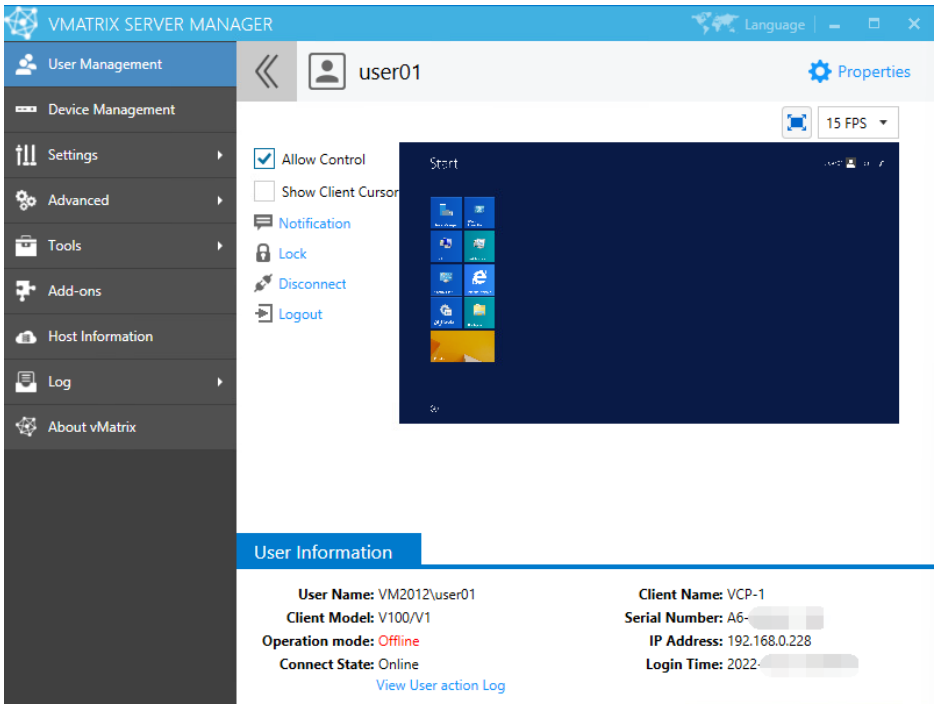
5.4.1 Monitor Authorization



- **Don’t need confirmation:**

Administrators can monitor user desktops without requiring confirmation from the monitored users.

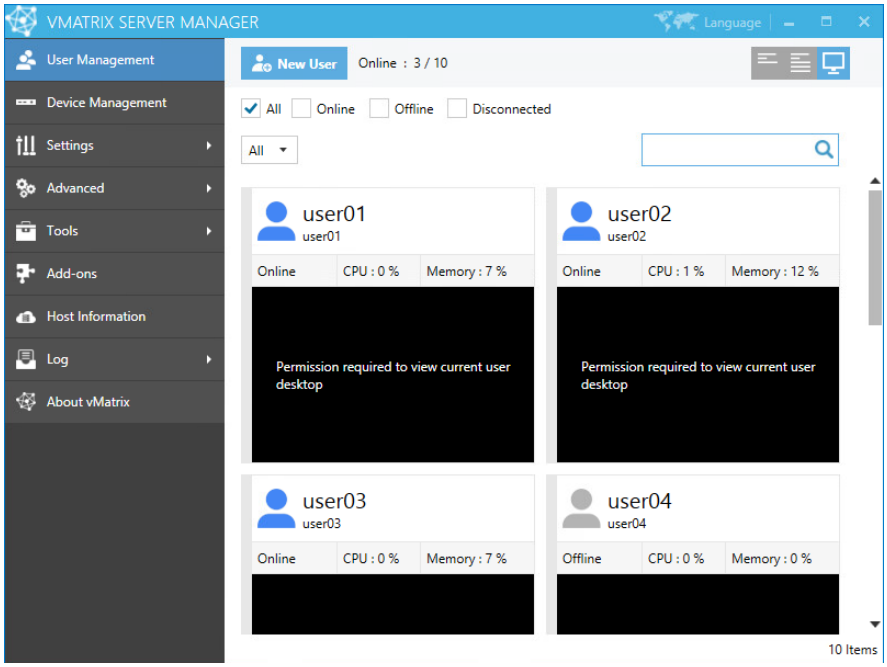


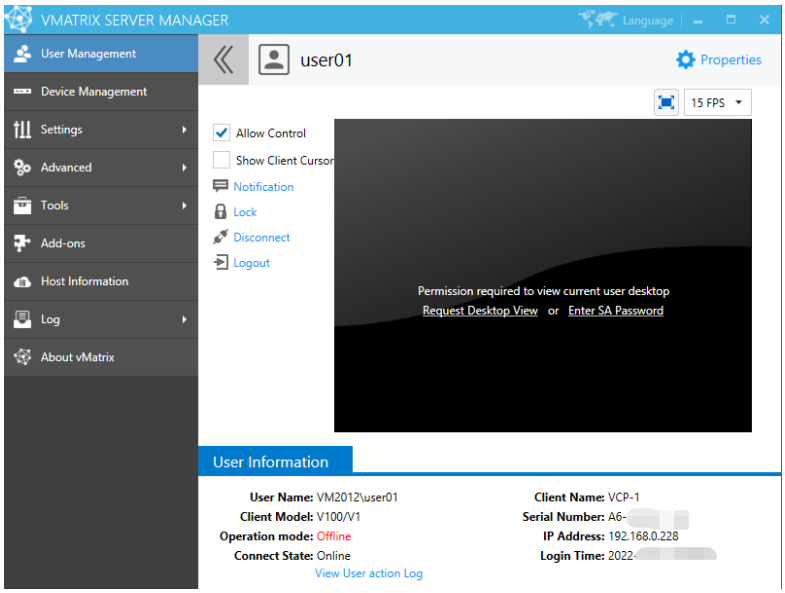


- **Need confirmation:**

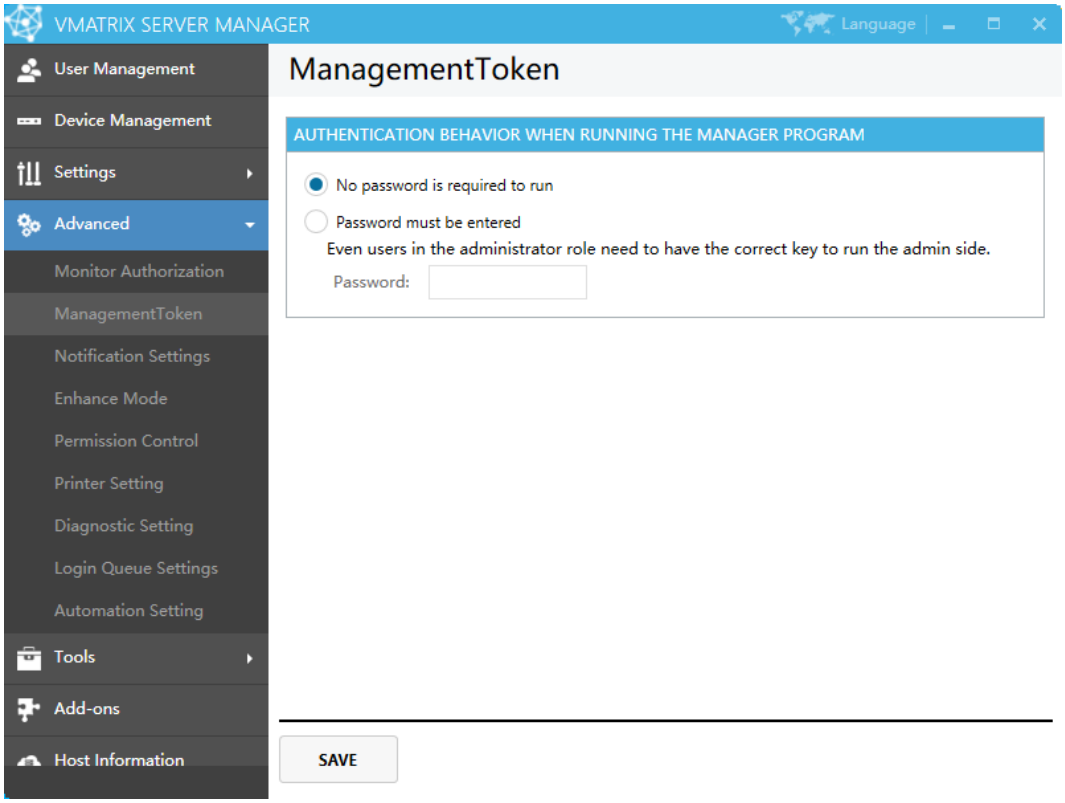
You are required to setup a Super Administrator (SA) password when this option is selected. By selecting this option, administrators need to send request to the user or enter SA password in order to get approval to monitor the user desktop. (Note: as local system administrators have the highest privileges, there is no effective way to prevent local system administrators from changing the settings, administrators can simply cancel monitor

authorization by simply changing the setting to “Don’t need confirmation” or changing the SA password, however, this option allows organization owners to track management logs which is available to view through “Log” -> “Management Log” of this software.





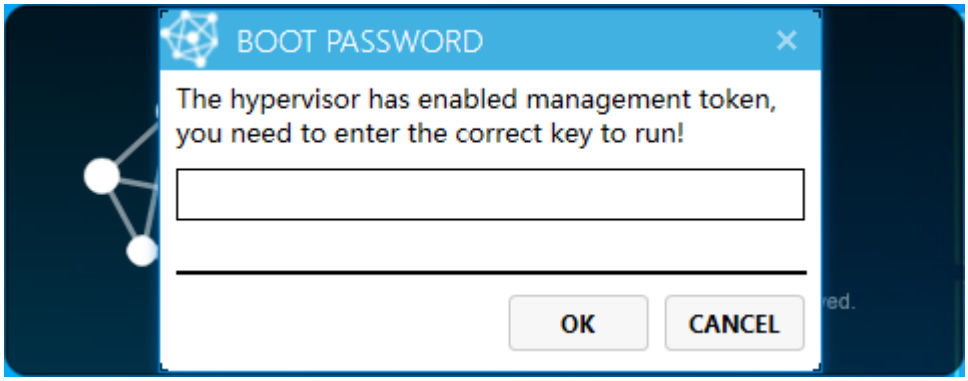
5.4.2 Management Token



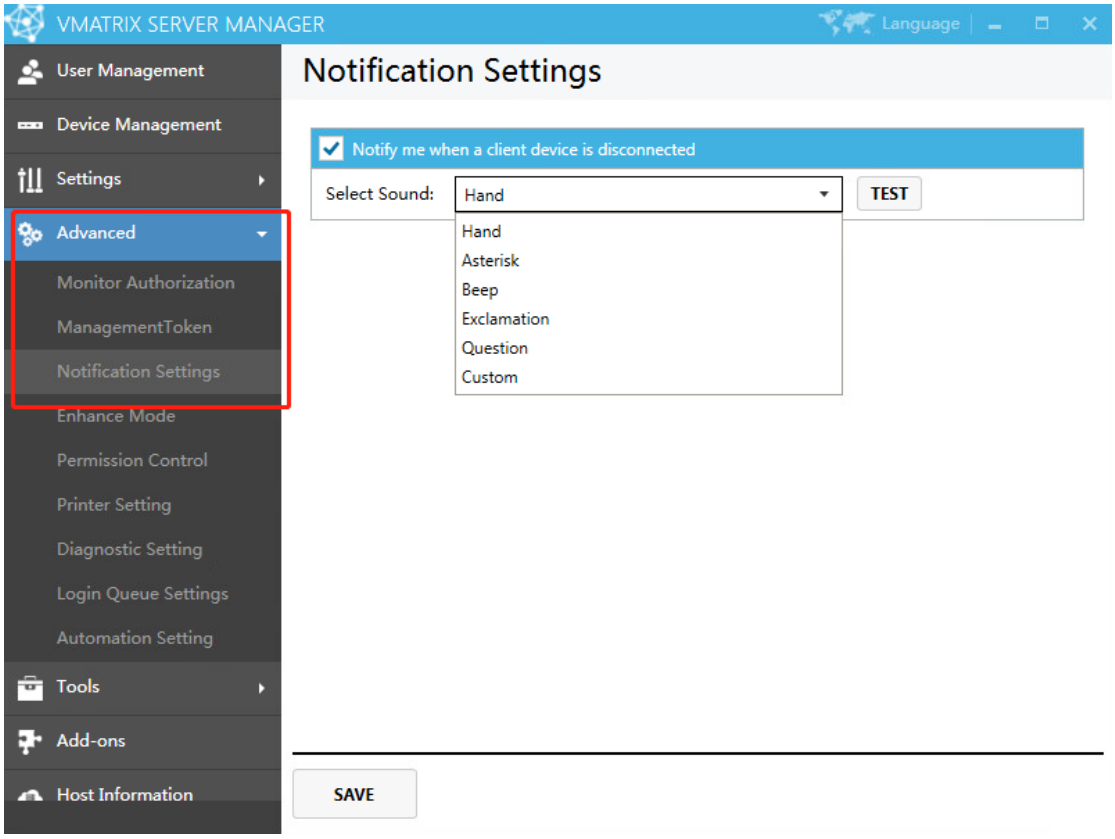
To control whether need a correct key to run the vMatrix server manager.

- **No password is required to run**
- **Password must be entered**

Even users in the administrator role need to have the correct key to run the vMatrix server manager.



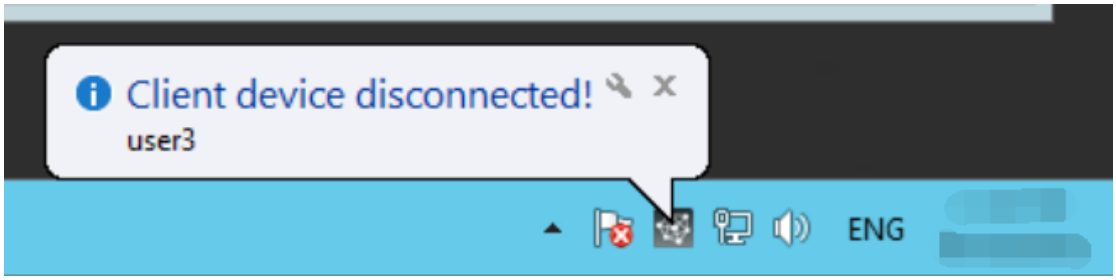
5.4.3 Notification



When notification function is enabled, the administrator will be informed with a bubble prompt if a client device disconnects from the host. This function is often used in unmanned cases to notify the administrator on session disconnections.

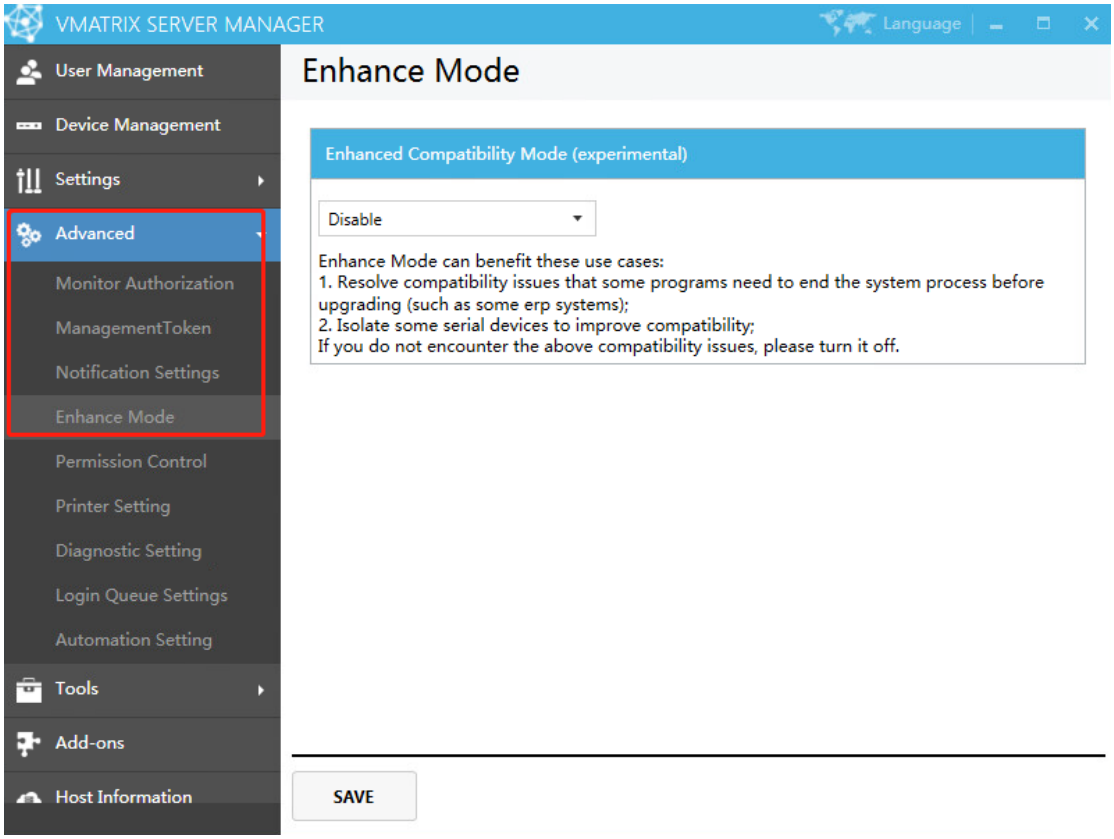
1) Check to enable notification. Select the sound effect. Depending on the system, the default sound effects will be Hand, Asterisk, Beep, Exclamation, Question or muted.

2) You can also use a custom sound file in *.wav format. Click “Save” to complete the setting. When a client device disconnects, the administrator will see a bubble prompt with sound alert.



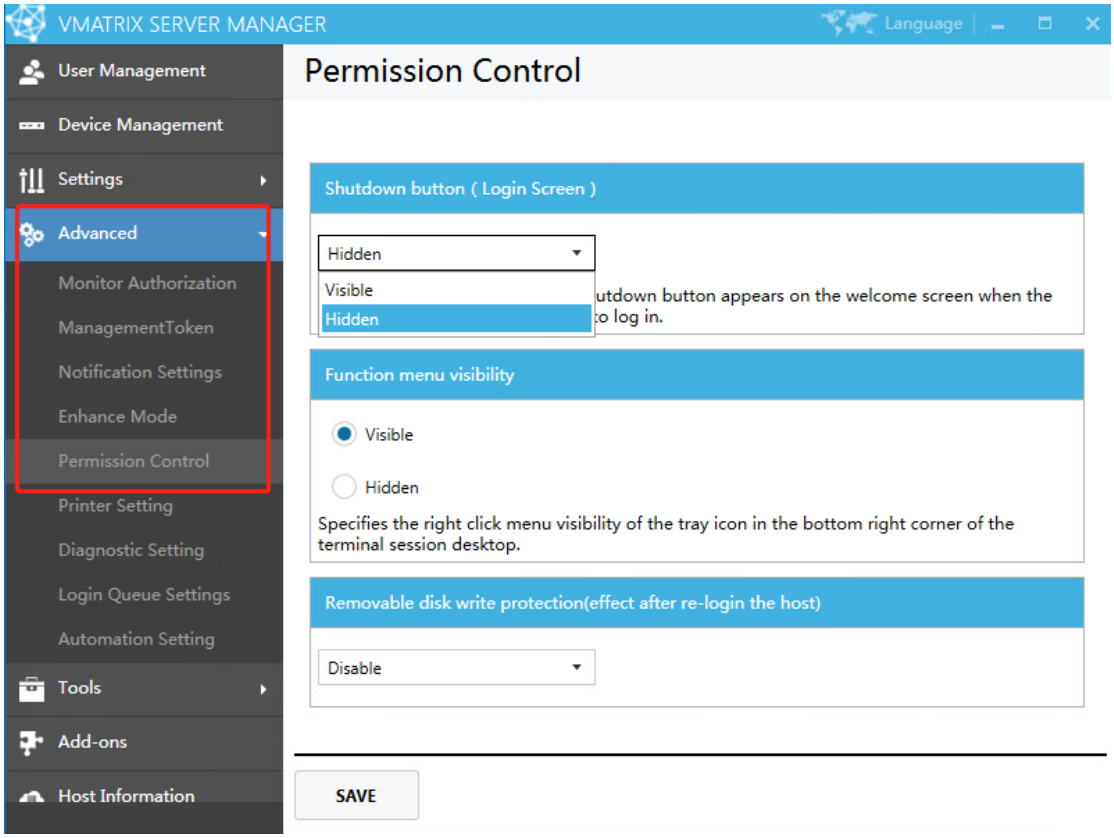
5.4.4 Enhancement Mode

Enhancement Mode may solve compatibility issues that some programs need to end the system process before upgrading (such as some erp systems) or isolate some serial devices(such as Wacom STU 450 Signature Pad) to improve compatibility.

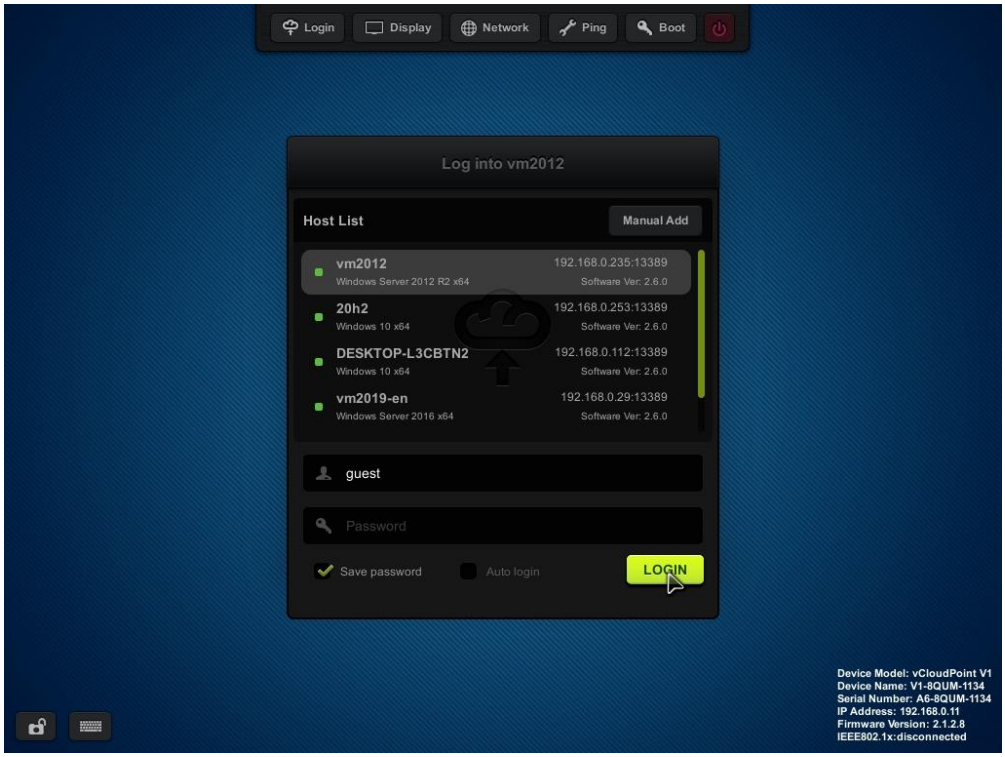


Note: If you do not encounter the above compatibility issues, please turn it off.

5.4.5 Permission Control

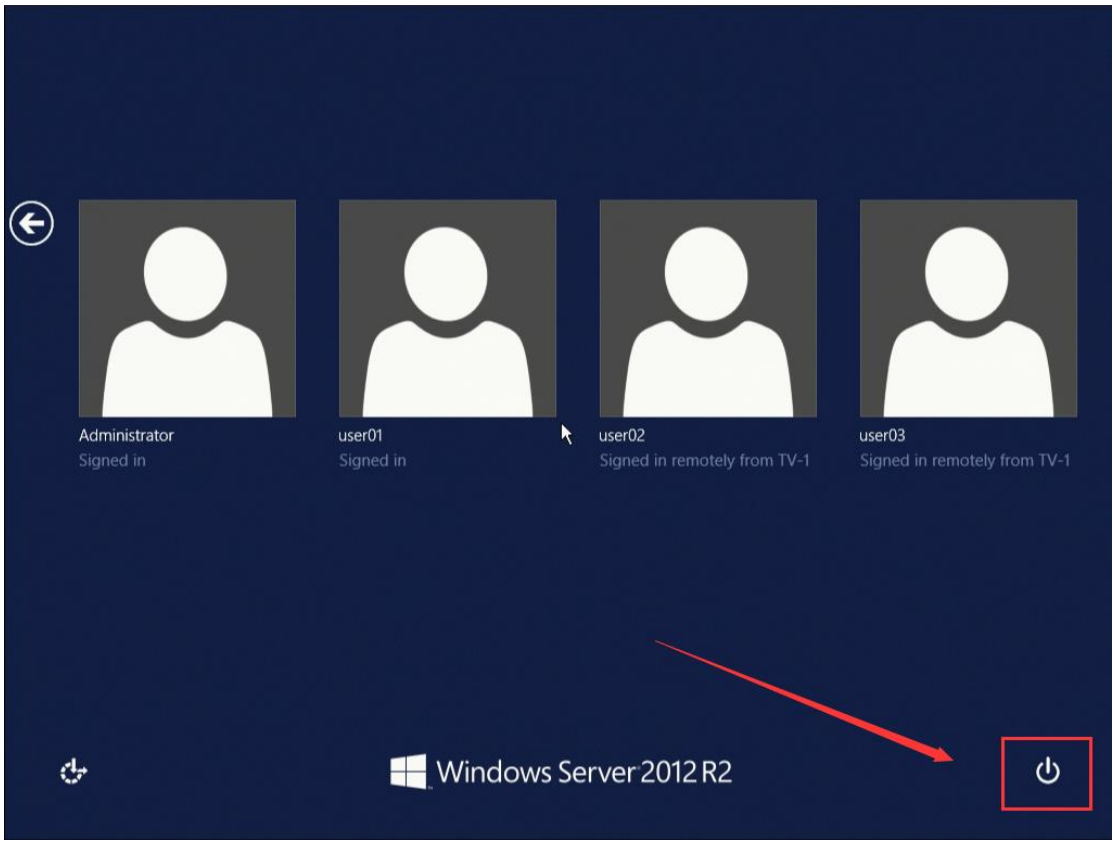


- **Shutdown button (Login Screen):** The switch controls whether the shutdown button appears on the welcome screen when the terminal is logged in anonymously. The terminal can enter the Windows login interface through the guest account.

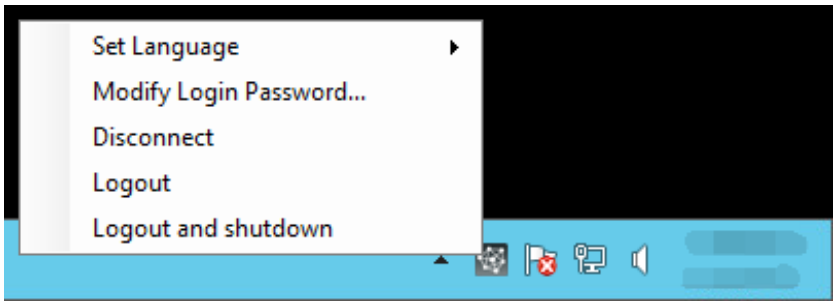


- **Shutdown Button Hidden:**

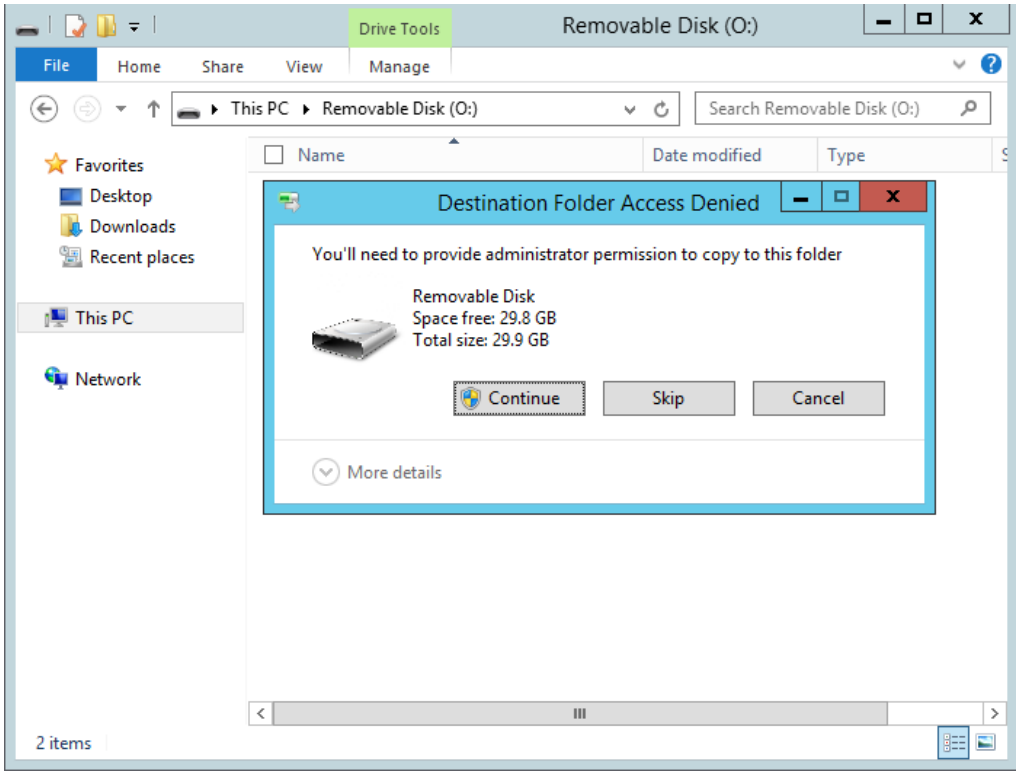
- **Shutdown Button Visible:**



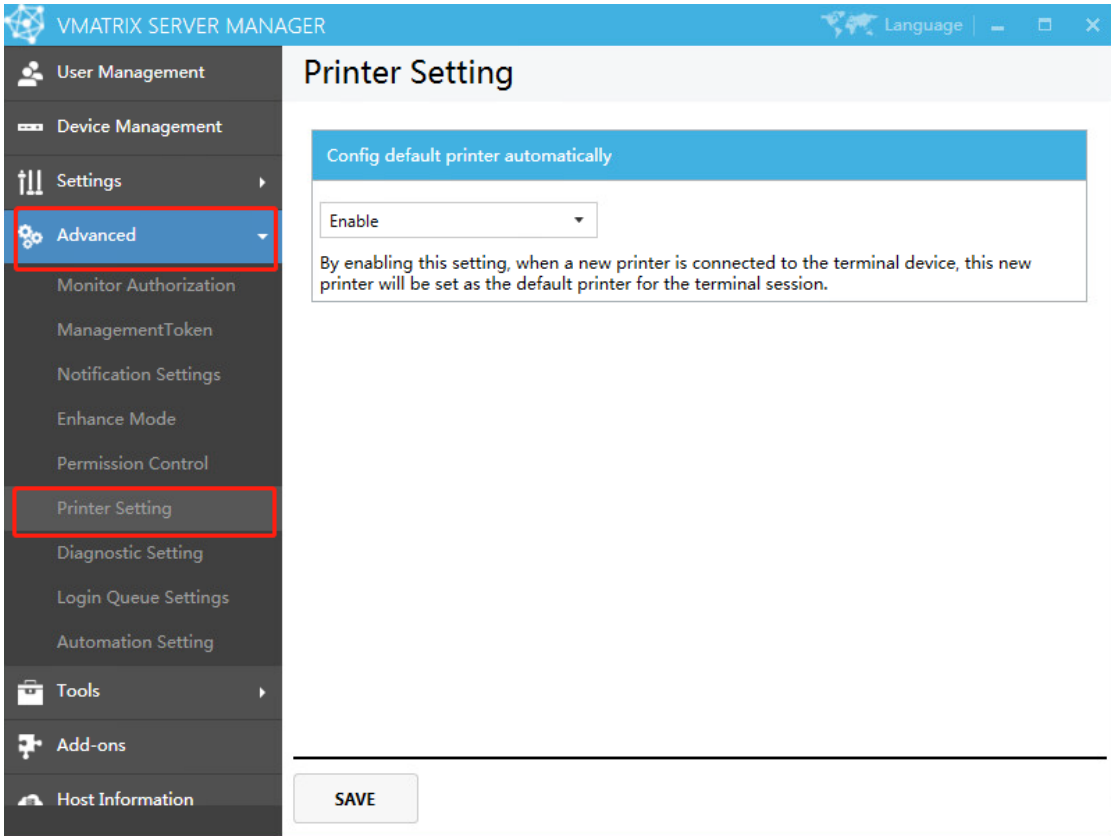
- **Function Menu Visibility:** Control whether the right-click function menu of the tray icon in task tray of the terminal user's desktop is visible.



- **Removable Disk Write Protection:** to control the write permission of removable disk. When Write Protection is enabled, users (including administrators) will not have permission to write data to the removable disk.



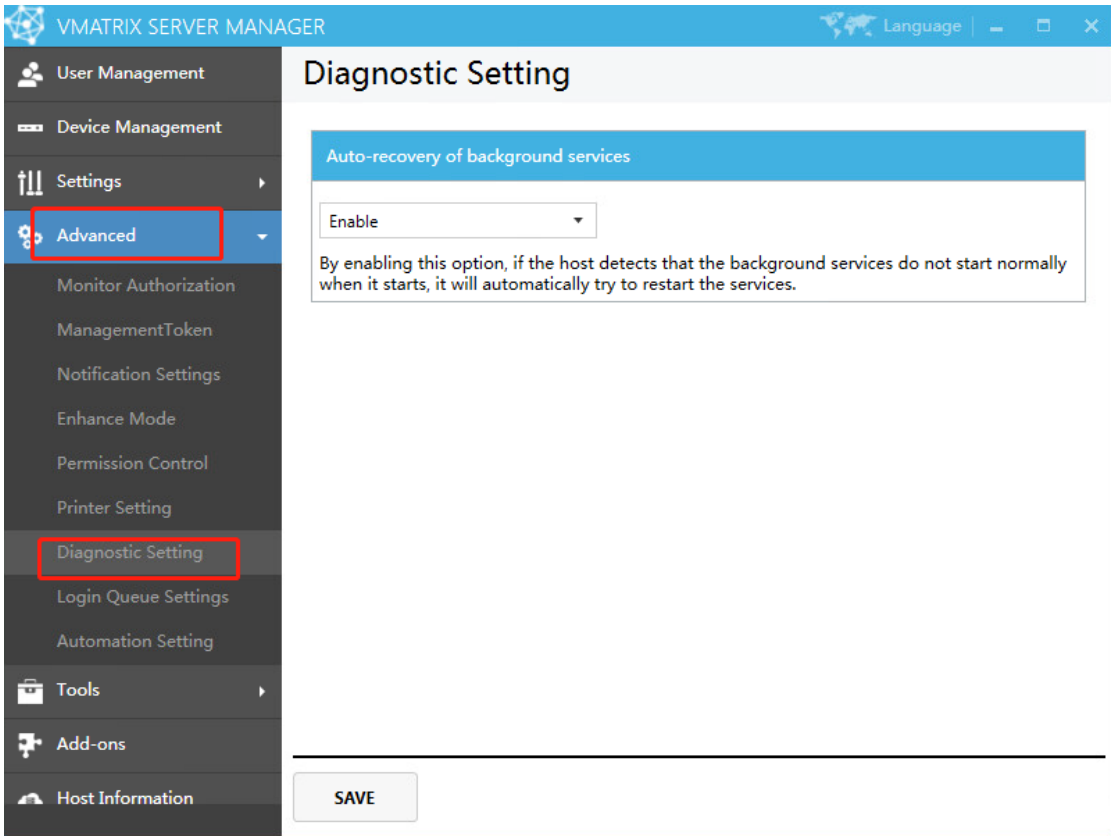
5.4.6 Printer Setting



Config default printer automatically: By enabling this setting, when a new printer is connected to the terminal device this new printer will be set as the default printer for the terminal session.

Note: Not supported for configuring default scanner device automatically. If you use multiple scanner devices at the same time, you need to manually select which device to work.

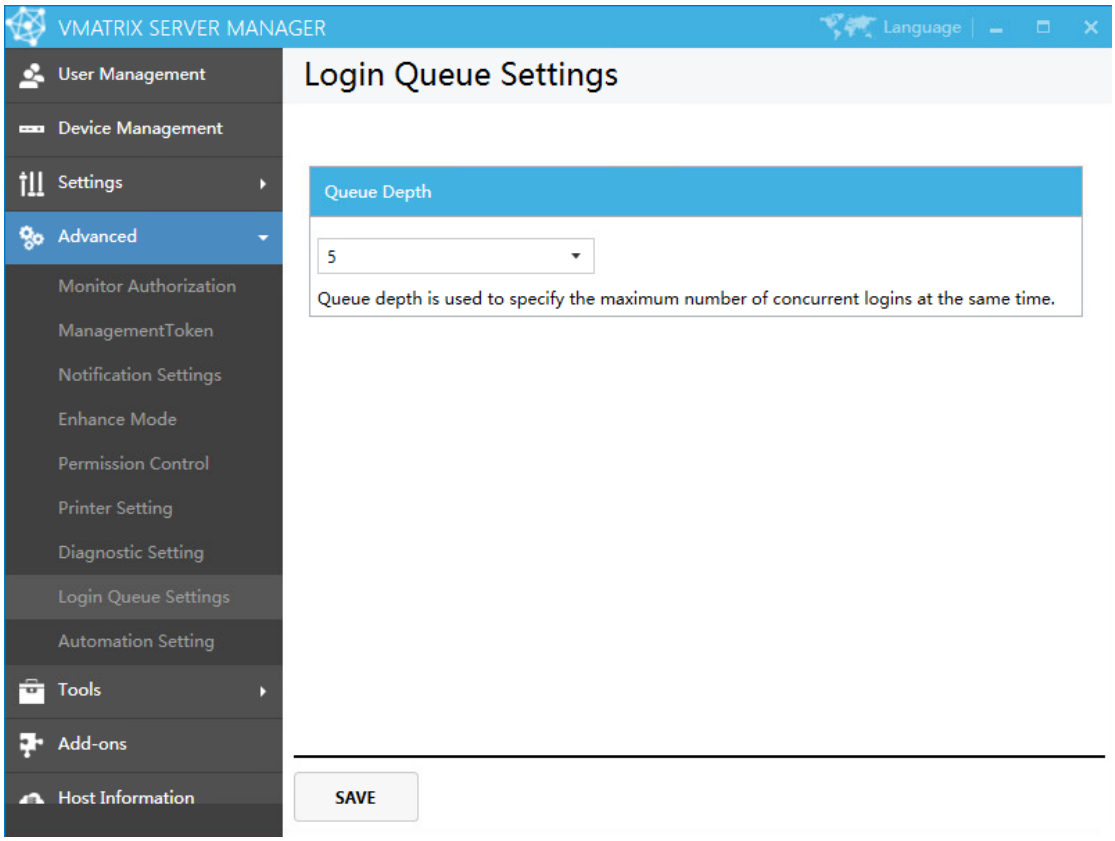
5.4.7 Diagnostic setting



Auto-recovery of background services: By enabling this option, If the host detects that the background services do not start normally when it starts, it will automatically try to restart the services.

Note: This function will only detect and start the service when the host is just turned on. If the background services crash or is discontinued during use, it will not take effect.

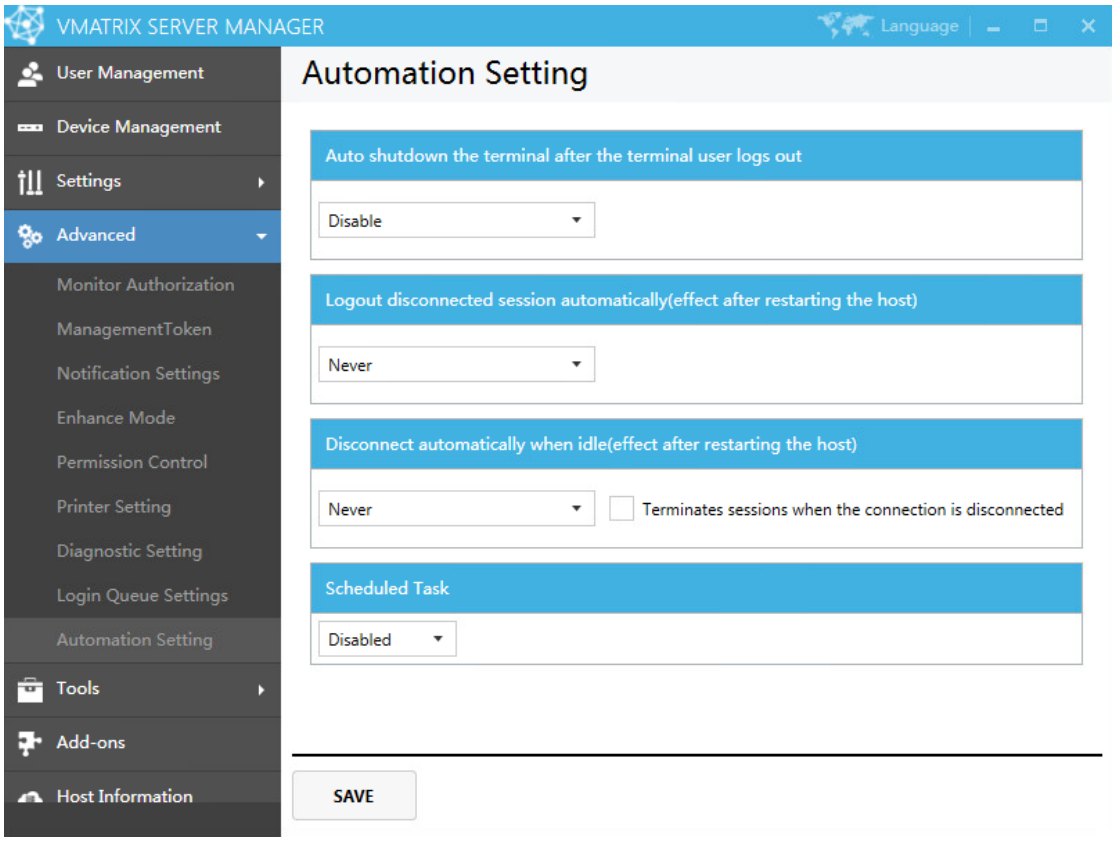
5.4.8 Login Queue Settings



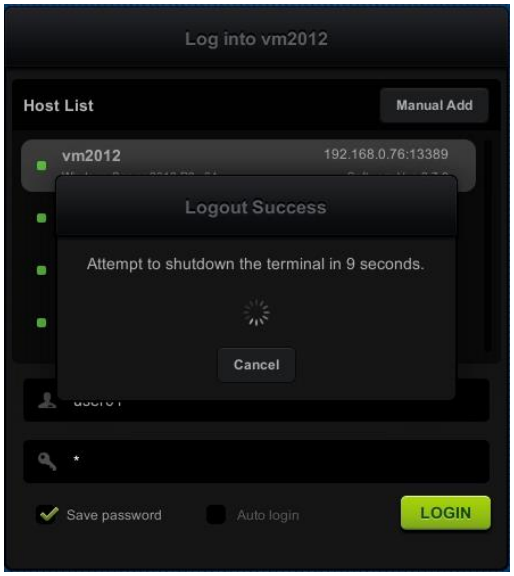
Queue Depth: Queue depth is used to specify the maximum number of concurrent logins at the same time. The number can be adjusted according to the server configuration and the speed of login users.

Note: If the queue depth value is too high, the server may cannot handle excessive user login requests, and cause thread on pause and login timeout.

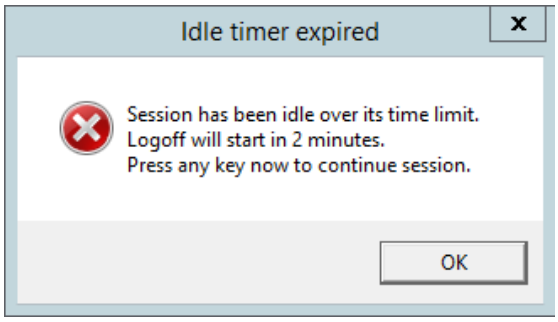
5.4.9 Automation Settings



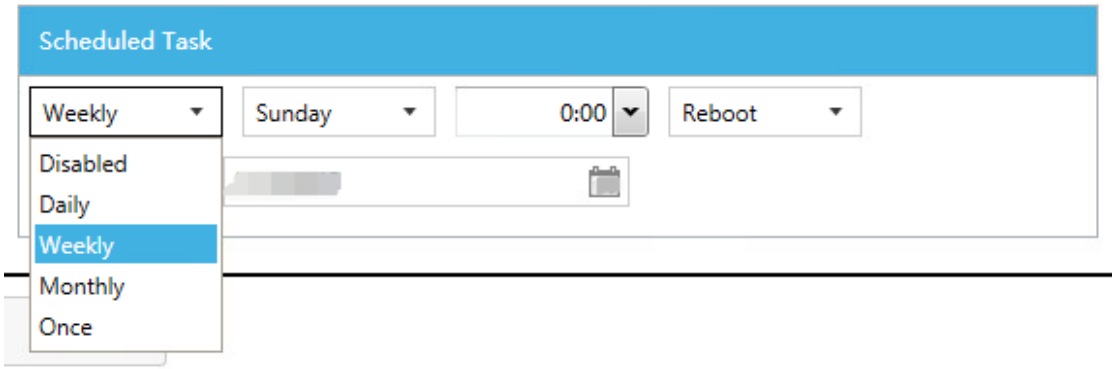
- **Auto shutdown the terminal after the terminal user logs out:** If this function is enabled, every time the terminal user logs out and returns to the login interface, a ten-second countdown prompt will appear. After the countdown is over, the terminal will be automatically powered off. During the countdown, you can manually click to cancel power off the terminal.

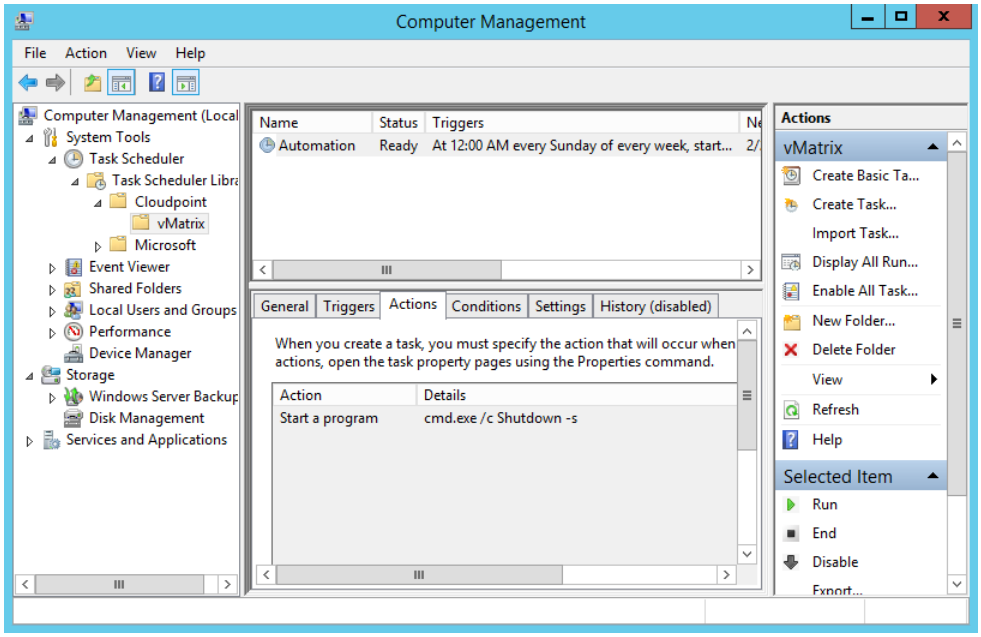


- **Logout disconnected session automatically (effect after restarting the host):** When the specified time is reached, Logout disconnected session automatically from the server.
- **Disconnect automatically when idle (effect after restarting the host):** When the specified time is reached, disconnect automatically the active but idle (no user input) user sessions. The user will receive a warning and be disconnect in 2 minutes. The user can press the key or move the mouse to keep the session active.
  - **Terminates sessions when the connection is disconnected:** when checked, idle sessions that are automatically disconnected will also be logged out.



- **Scheduled Task:** Add a Scheduled Task of “Timing Shutdown”/ “Reboot The Host”.

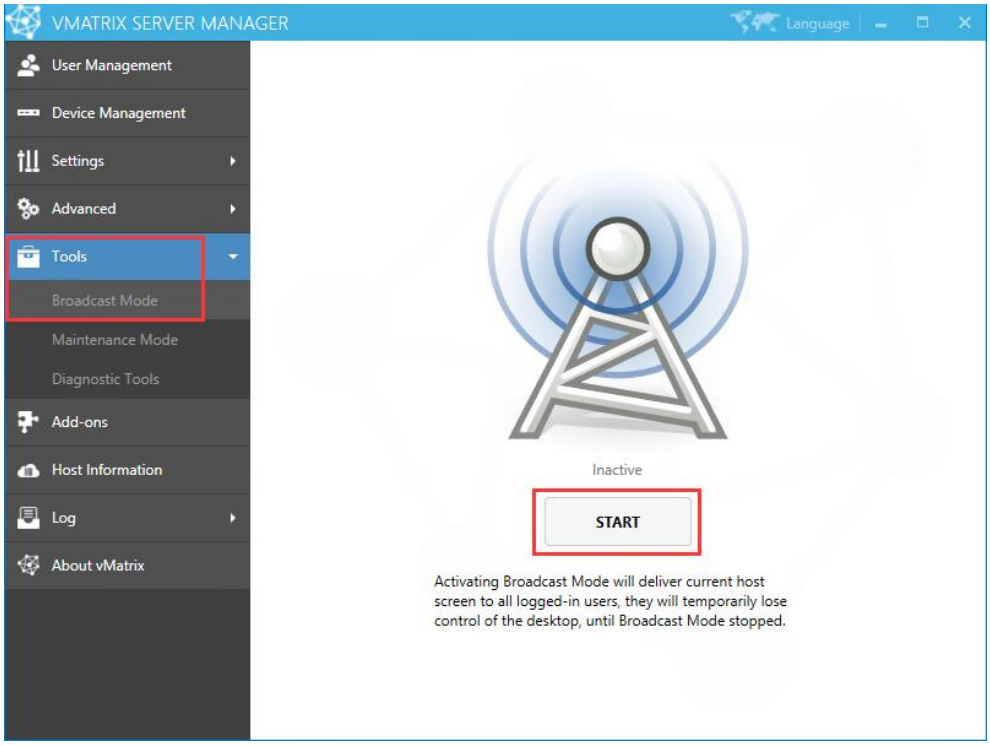




5.5 Tools

5.5.1 Broadcast Mode

Activating this mode will display the entire host screen to the users who are currently connecting to the host. All users will lose control of their desktops when Broadcast Mode is on.



Note:

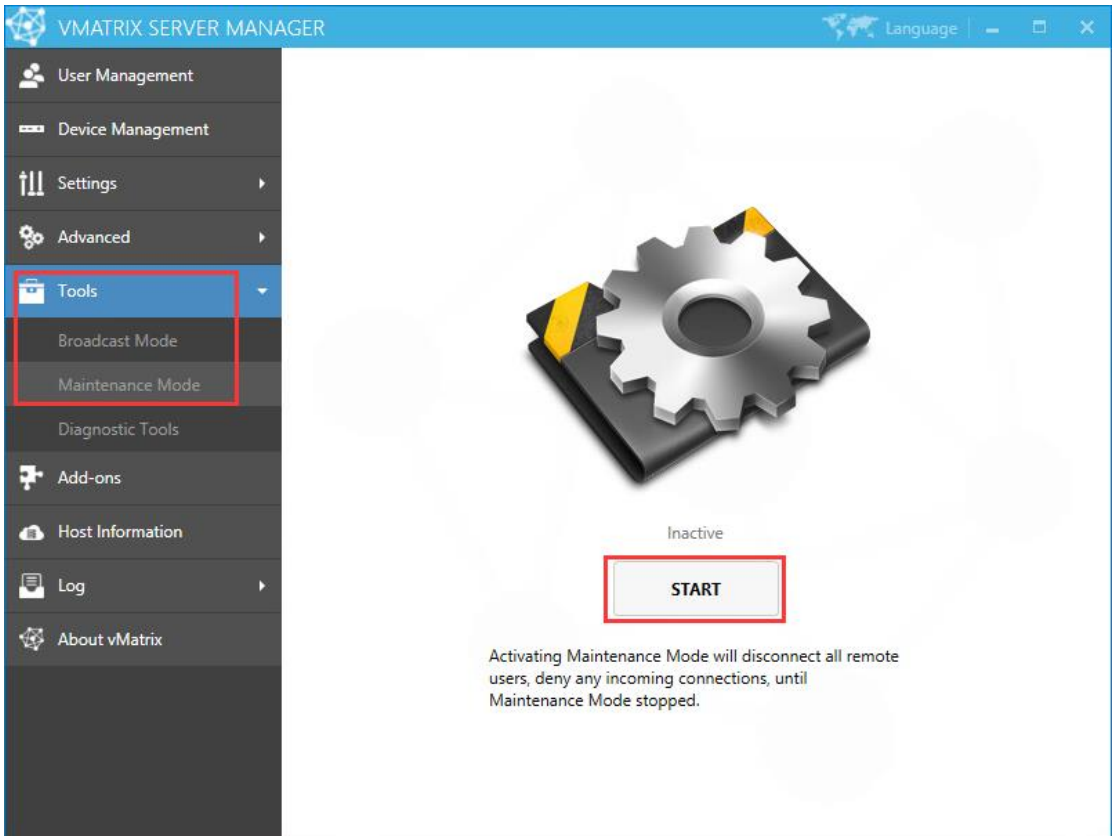
1) Users who latter connect to the host after Broadcast Mode activation will also lose control of their desktops and be given the host screen at the moment they enter their sessions.

2) Broadcast Mode is not effective on users who have logged in but are disconnected (back to the device Login page).

3) When Broadcast Mode is on, desktop resolution of the effected users will be changed to that of the host. Therefore, make sure the host desktop resolution is supported by the effected users' monitor, otherwise, the user monitor will go blank due to desktop resolution out of range.

5.5.2 Maintenance Mode

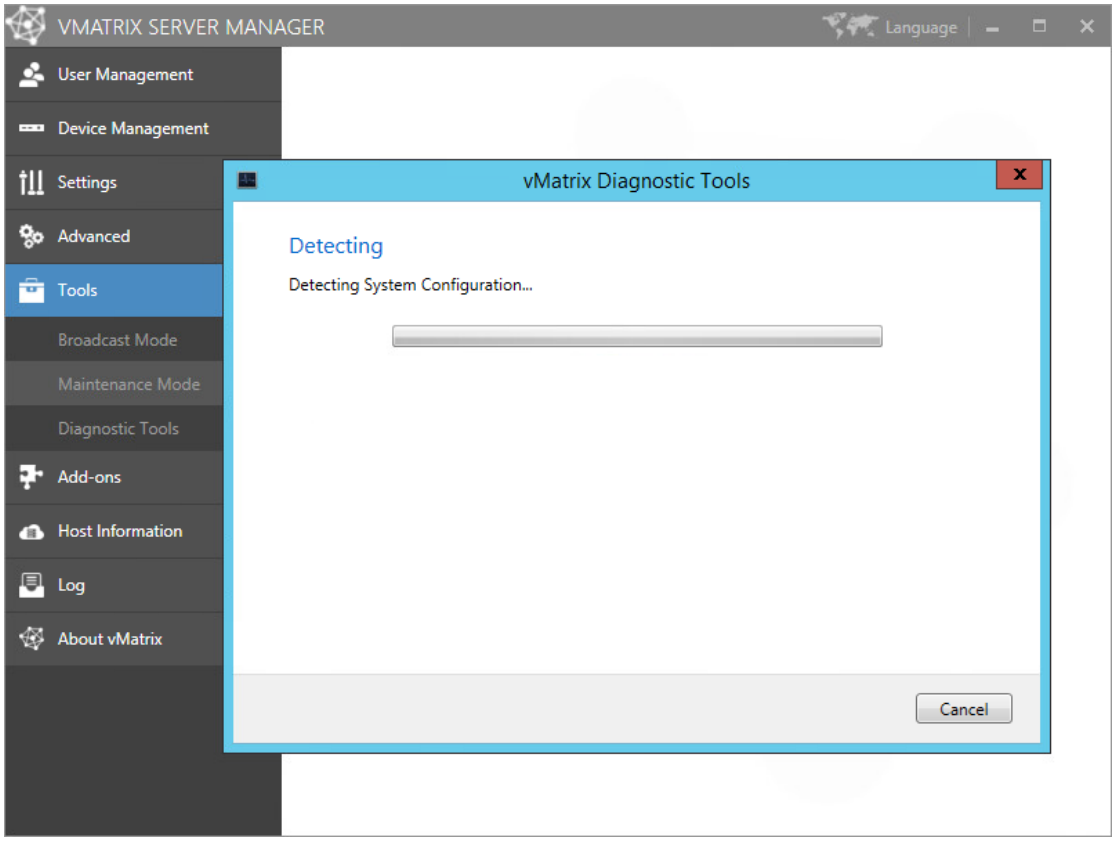
Activating Maintenance Mode will disconnect all connecting users and also deny any incoming connection request from users. This is often used when the host is under maintenance.

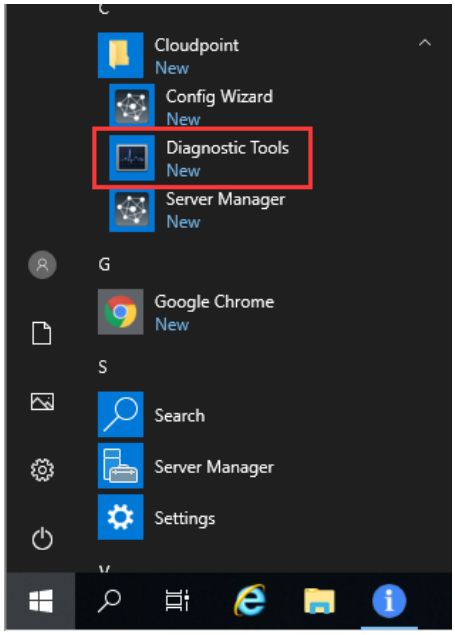


Note: Activating Maintenance Mode just disconnects user sessions, but not logged them out. Users will find their files & applications still in place when Maintenance Mode is off.

5.5.3 Diagnostic Tools

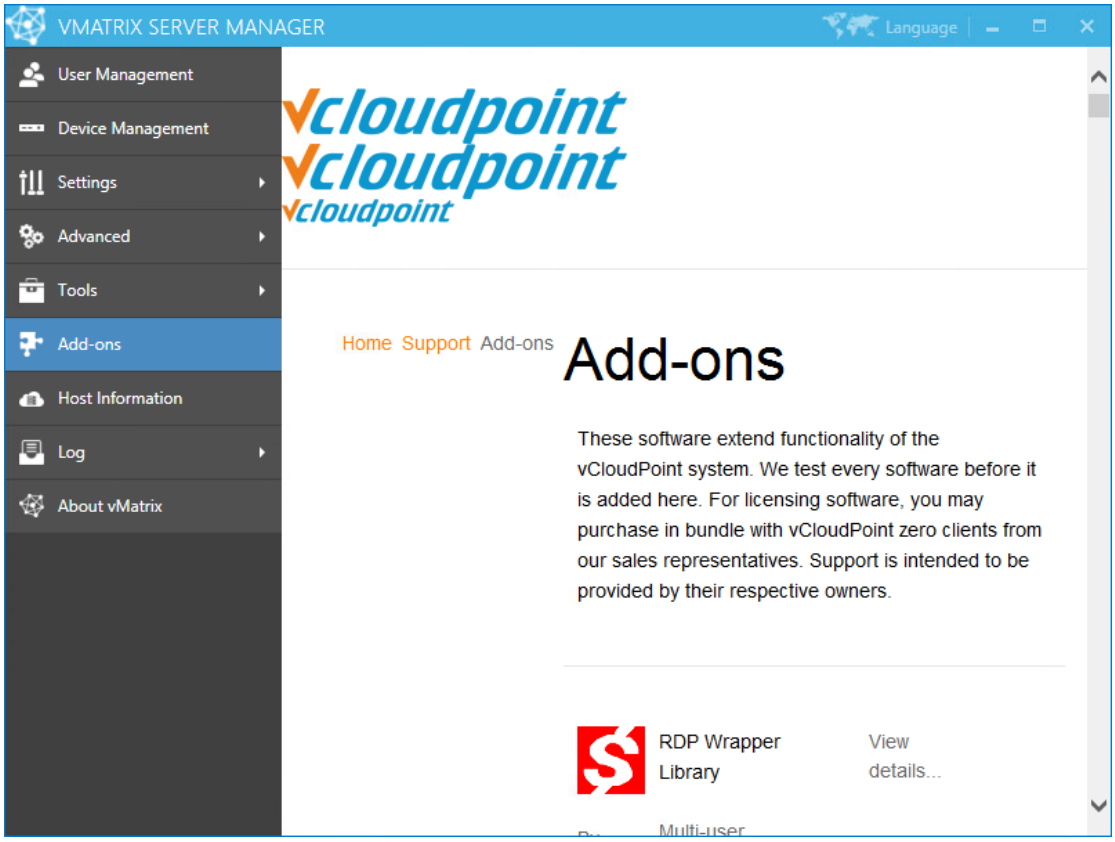
Running Diagnostic Tools will initiate a check on vMatrix Server Manager and prompts you to fix accordingly if any problem is detected. You can also launch the Diagnostic Tools at Programs and Features if vMatrix Server Manager cannot be opened.





5.6 Add-ons

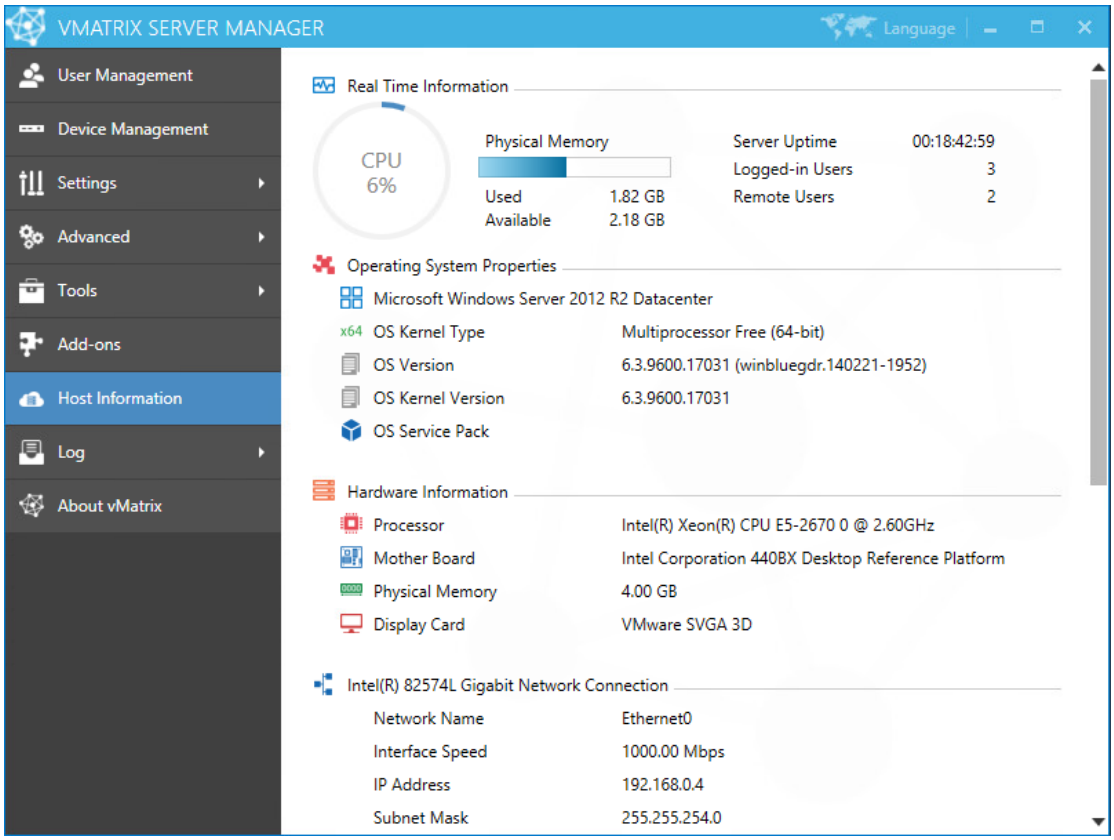
This page contains recommended software that may extend functionality of the vCloudPoint System or are frequently used with vCloudPoint products. The software has been tested compatible with the vCloudPoint system.



Note: this page connects to web page on vCloudPoint website through a web viewer window, thus it requires time when loading contents. If you do not provide internet connection to the host, the page contents will not show.

5.7 Host Information

This page provides an overview of the host information including real time resources consumption, operating system, hardware and network.



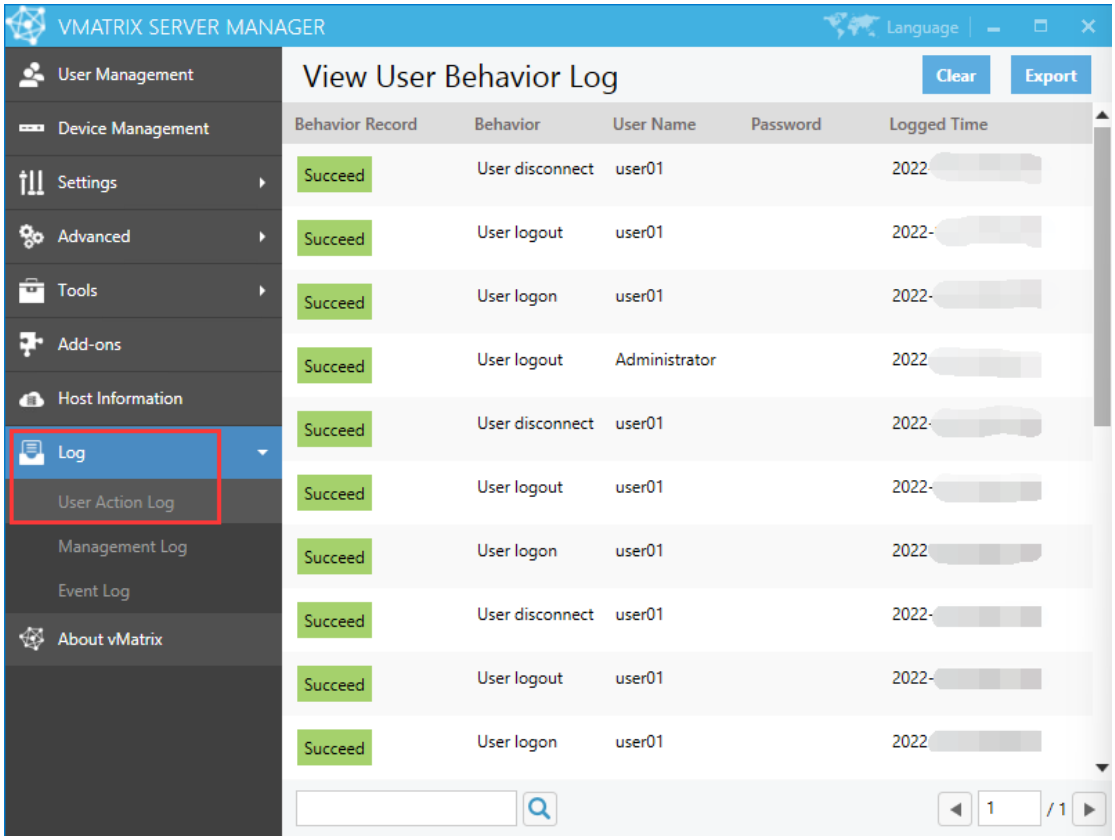
5.8 Log

5.8.1 User Action Log

You can view all user actions since the installation of vMatrix Server Manager.

Clear: clear all User Action Logs.

Export: After confirming the start date and end date, the log can be exported as a csv file or a txt file.

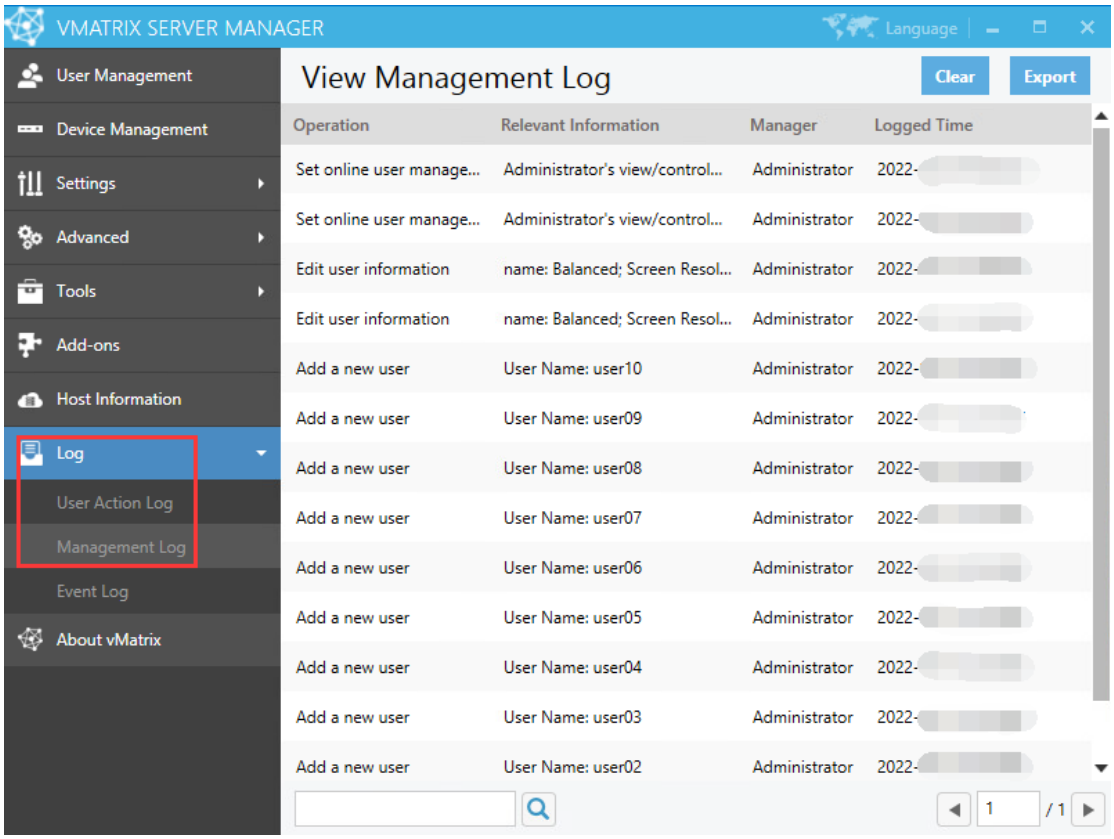


5.8.2 Management Action Log

You can view all management actions since the installation of vMatrix Server Manager.

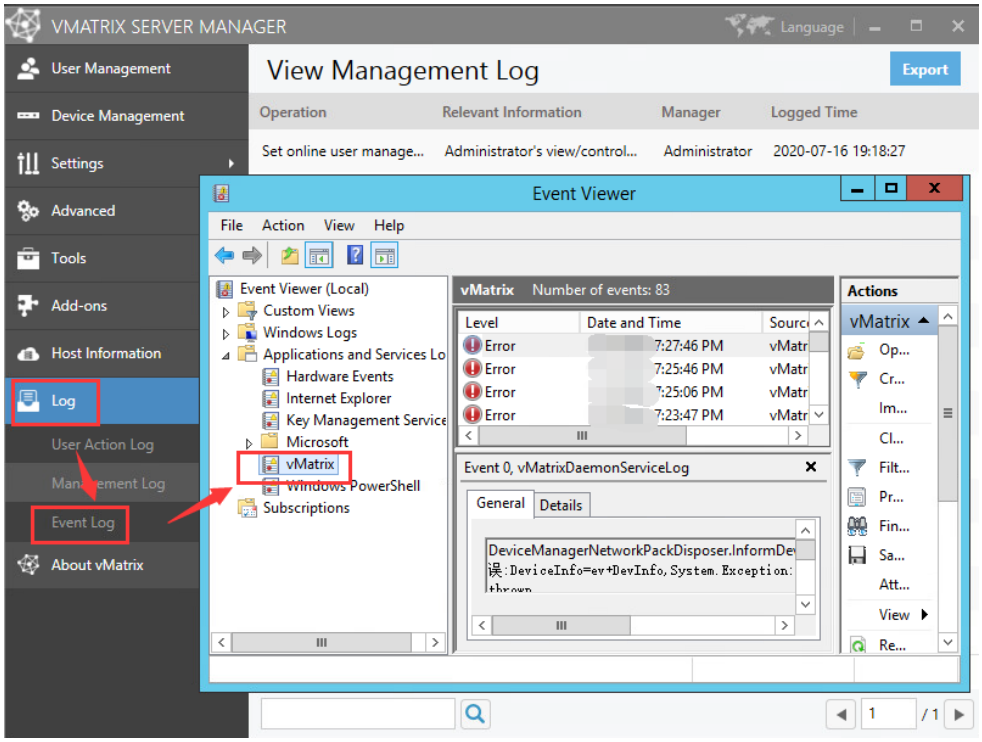
Clear: Clear all Management Log.

Export: After confirming the start date and end date, the log can be exported as a csv file or a txt file.



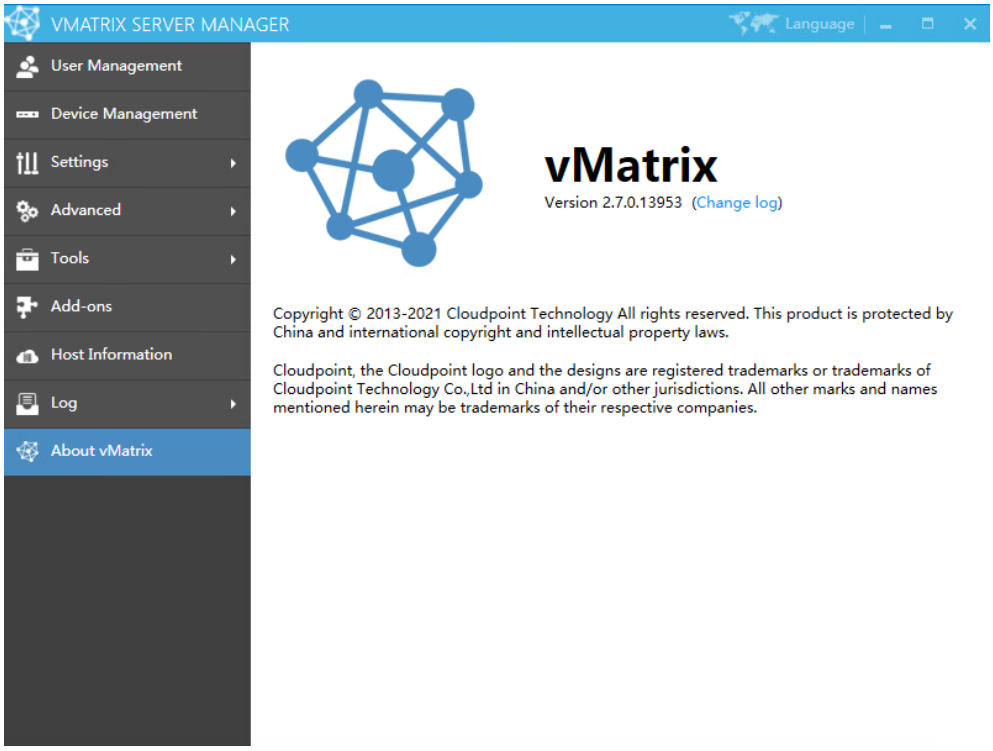
5.8.3 Event Log

Clicking on this menu will open the Windows Event Viewer and locate to the log of vMatrix. When vMatrix Server Manager encounters a problem, the vMatrix error log is helpful for our technical team to analyze and fix problems. As a result, please export and send the vMatrix error log to vCloudPoint technical team when you are reporting a problem. (It requires a few seconds to open the Event Viewer. Besides vMatrix Server Manager, Event Viewer also can be opened through Windows Start Menu.)



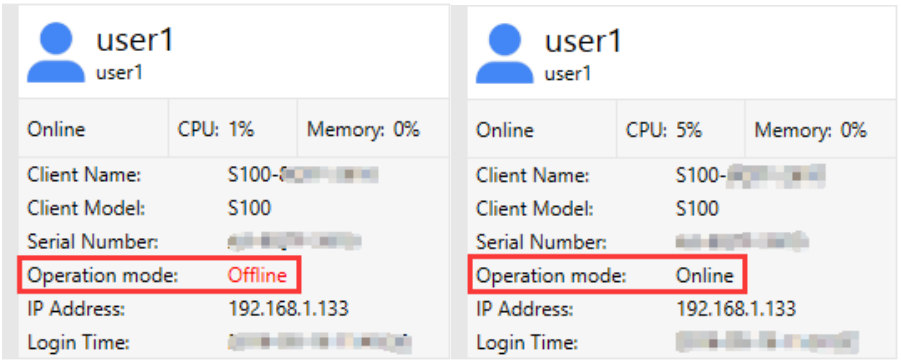
5.9 About vMatrix

This page displays the current version of vMatrix Server Manger and contains a change log describing main changes over the past versions. It also describes the ownership of the software.



5.10 Offline Usage

By factory default, vCloudPoint zero clients and vMatrix Server Manager Software are configured to be used in an internet connected environment (WAN). If your host is provided with internet, no additional configuration is required to be done.



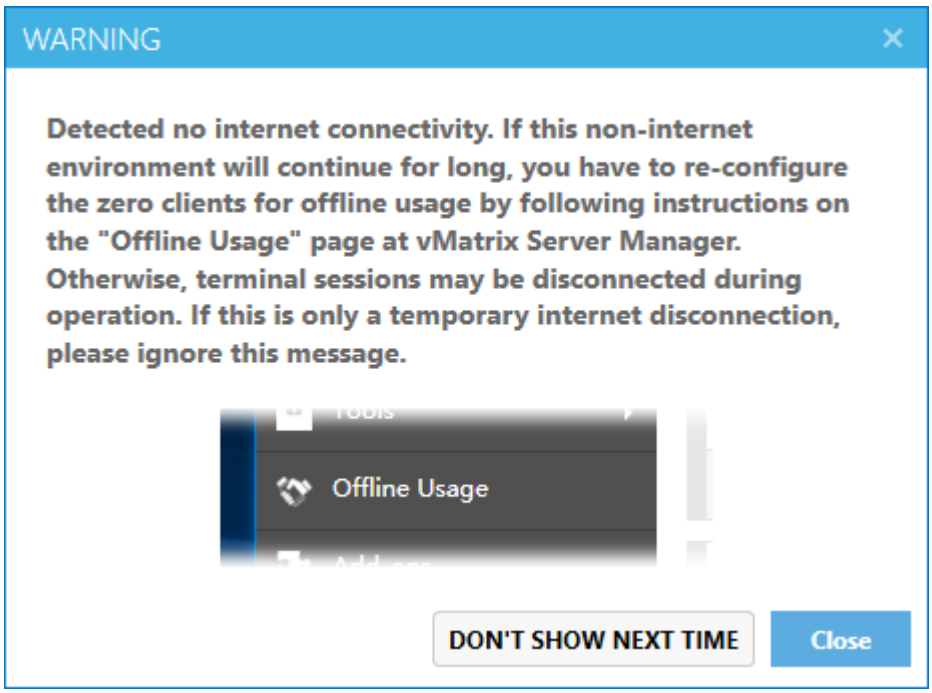
However, if the Operation Mode of the devices connecting to the host stays “Offline” in red all the time, you have to re-configure the devices for offline usage, otherwise the devices may be disconnected in every few minutes during operation.

Use cases where you may encounter this problem and need to apply for “Offline Usage” normally includes the followings:

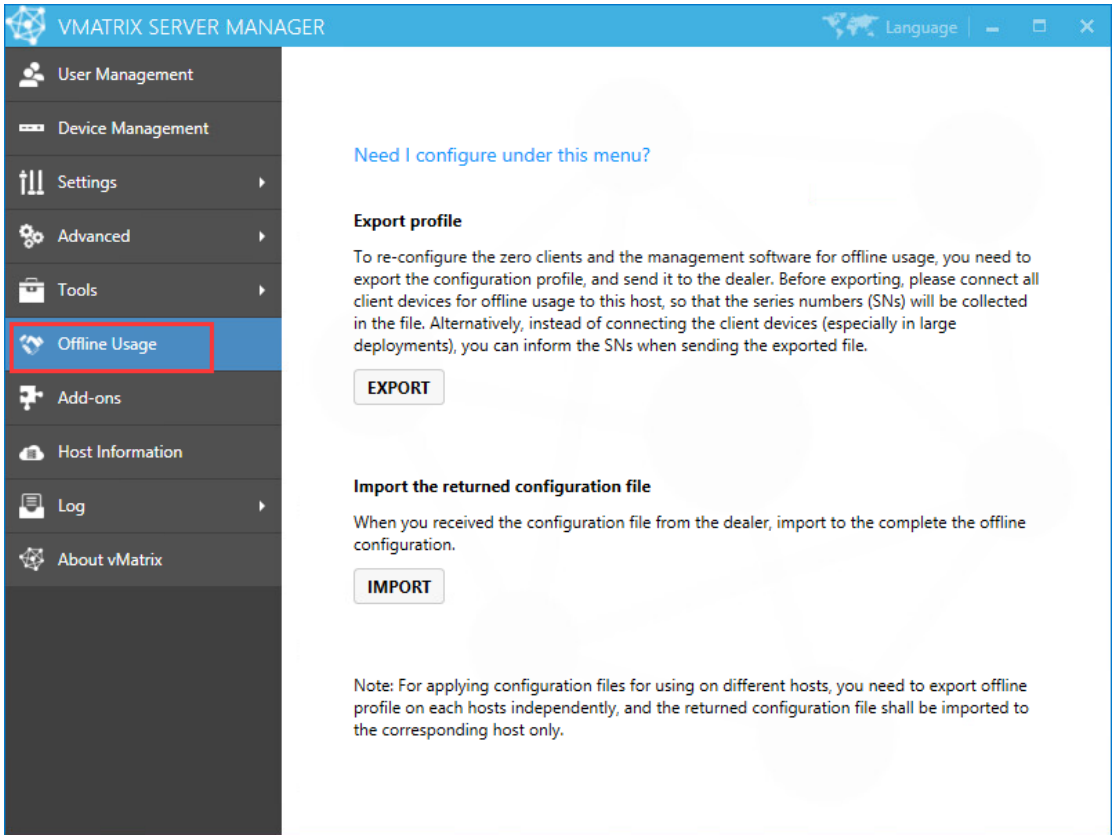
- you do not provide internet connection (WAN) to the host or the internet connection is extremely unreliable;
- you use proxy or VPN or internet control software that the host cannot access our configuration server.

How to re-configure the devices for offline usage:

1) In a non-internet connection environment, vMatrix Server Manager will prompt a message window for offline usage configuration within 5 minutes after host boot.



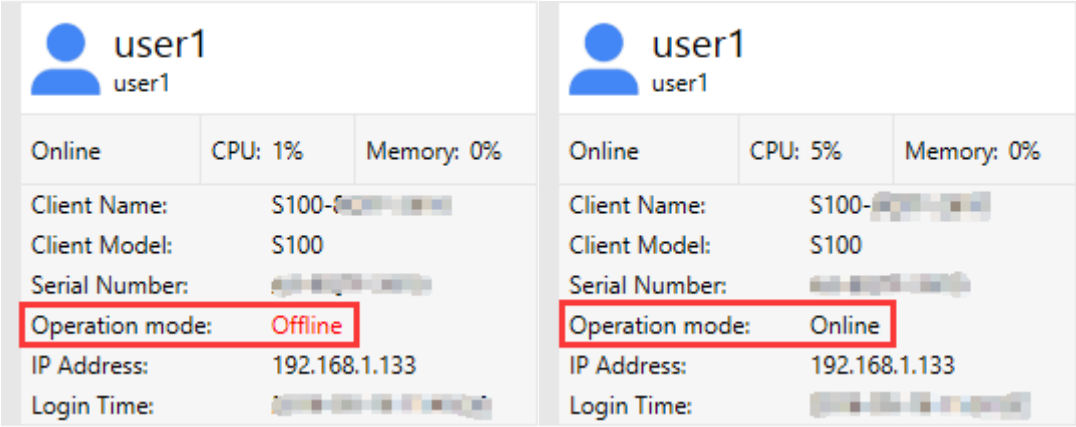
2) Open vMatrix Server Manager, go to Offline Usage page (this page only appears when the host is not provided with internet connection on system boot).



3) Export the configuration profile, and send it to the dealer.

4) The dealer will return you with a configuration file based on your last exported profile. Import the returned file to complete.

5) If your configuration for offline usage is successfully accomplished, the Operation Mode changes from “Offline” in red to “Online” in black.



Note:

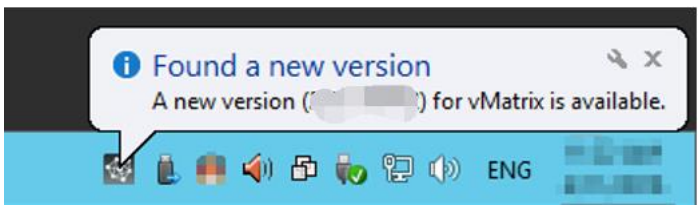
1) Offline usage configuration on vMatrix Server Manager was introduced in the release of vMatirx Server Manager 2.0.2 version, if you are planning to use the vCloudPoint zero clients in a non-internet or unstable internet environment, please use 2.0.2 or a later version of vMatrix Server Manager, and follow the instructions on “Offline Usage” page to process.

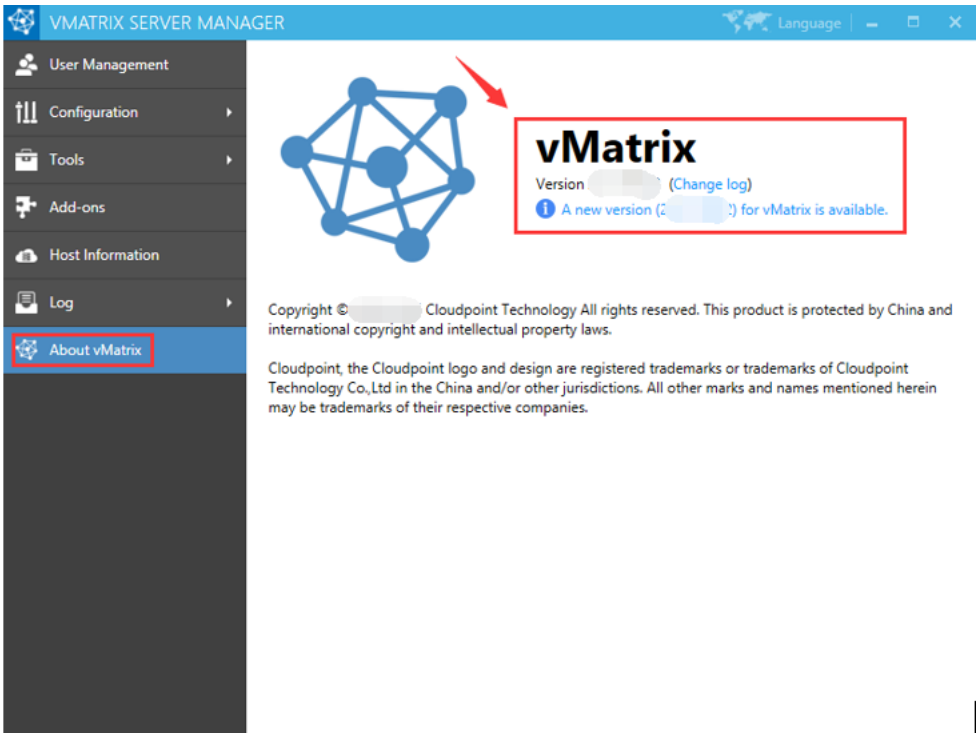
2) Before exporting,
please connect all client devices for offline usage to the host, so that the serials numbers (SNs) will be collected in the file. Alternatively, instead of connecting the client devices (especially in large deployments), you can inform the SNs when sending the exported file.

3) The host hardware when exporting the file should be consistent with the host hardware when it is used offline in the future.

5.11 vMatrix Update

When a new version of vMatrix Server Manager is available, an update message will pop up from the vMatrix icon at the task bar. You will also see the same message with link to download on the “About vMatrix” page on vMatrix Server Manager.





Download the new version by opening the link or visit download center at vCloudPoint website.

After downloading, refer to the first installation steps to install :

1) Log out all users.

2) Disable security software to avoid mistaken report on vMatrix Installation files.

3) Run the installer and process as it is done on initial installation.

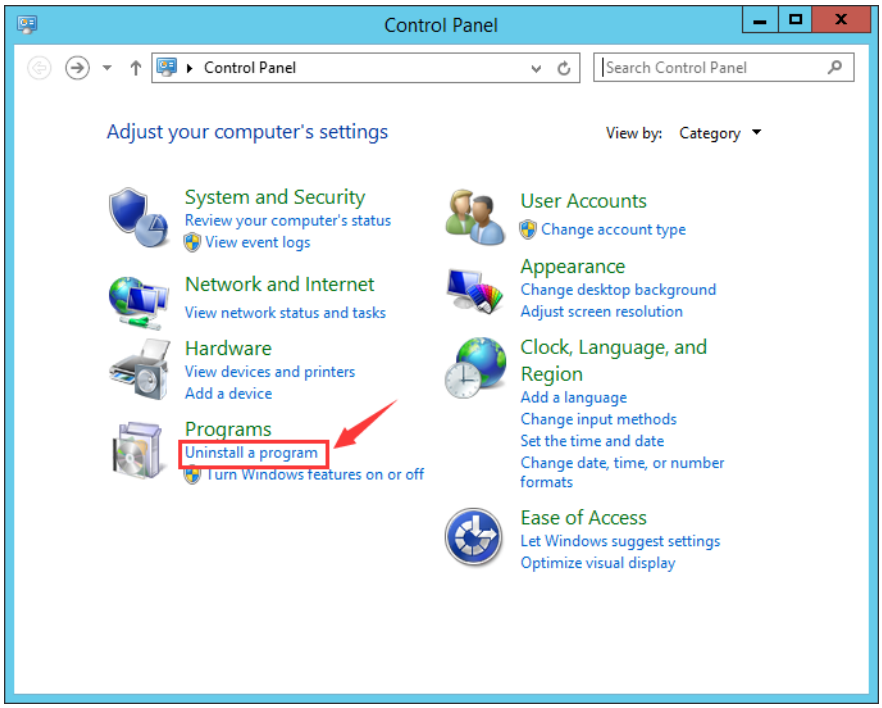
4) Reboot system after installation completes.

5) Check if there is any new device firmware at the device UI. If yes, then update.

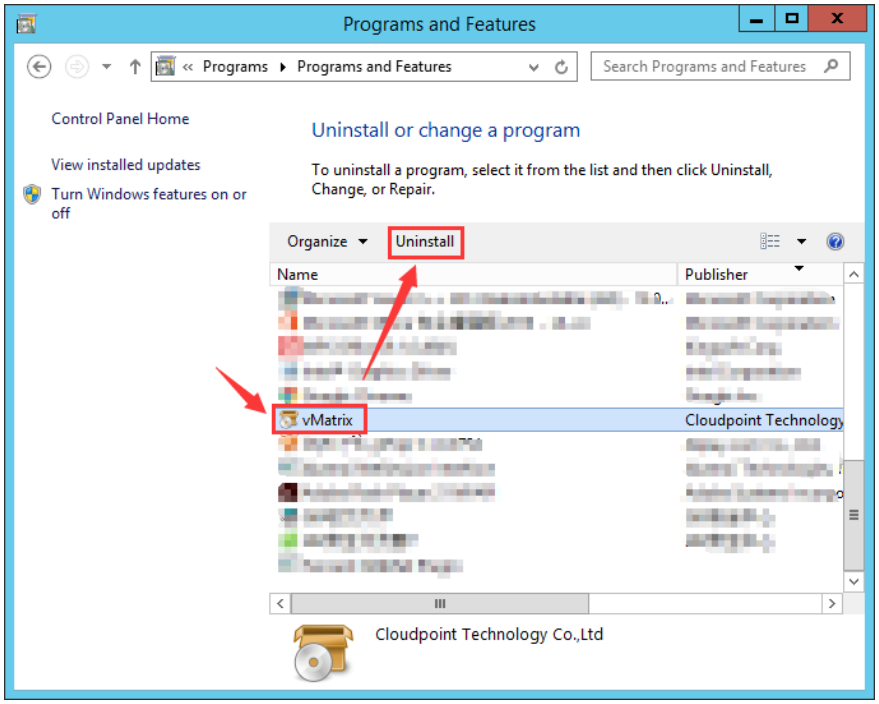
6) The terminal can log in to the host normally.

5.12 vMatrix Uninstall

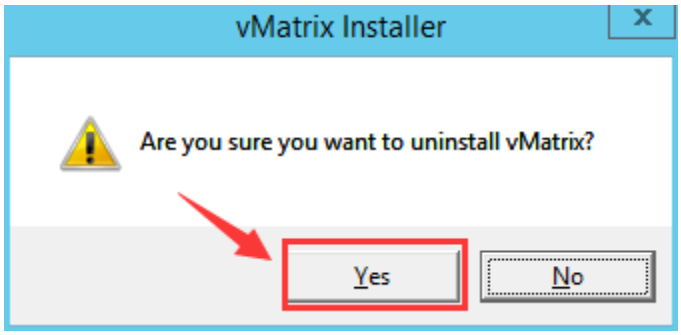
1) Open system control panel, click uninstall a program,



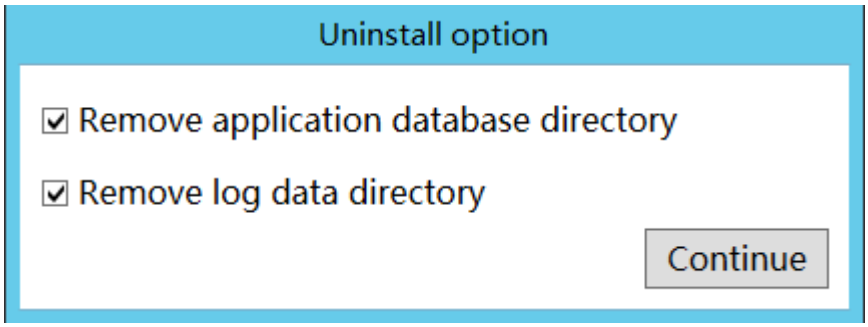
2) Select “vMatrix”, and then click to uninstall.



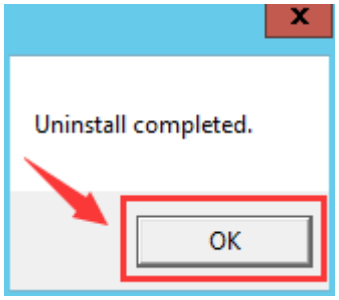
3) Click “Yes” when it prompts if you want to uninstall.



4) Check “Remove application database directory” and “Remove log data directory”, then click “Continue”.



5) Click “OK” when uninstall completes.



Chapter 6. Trouble-shootings

1） Terminal users get disconnected every a few minutes.

You can analyze the problem according to the prompts when disconnected:

- Network is busy. It may be that the host is under high load operation, causing network outages.
- Server-side configuration fail, cannot connect to the Configuration Server. Please check the internet connection of the host.
- Invalid serial number. Please contact the supplier and explain the situation.

2） The host is not shown in host list.

- The list is refreshing. Please wait a moment
- The host list only displays hosts on the same network segment. Please check whether the host and the terminal are on the same network segment.
- Ping the host to see if the host responds to the zero client. If not, that maybe the network problem or vMatrix not working properly.
- The vMatrix Server Manager software is not installed on the host.
- The vMatrix Server Manager software has just been installed, but the host has not been restarted.
- The host has just been powered on, but the vMatrix Server Manager software has not been opened.
- Run the “Diagnostic Tool” to check if the vMatrix Server Manager software working properly.
- If the hidden host function is set in the vMatrix Server Manager software, the terminal needs to manually add the IP of the host.

3） Cannot log into the selected host.

You can analyze the problem according to the prompts:

- Username or password are not available. Reset user's password in "User Management" page of the vMatrix Server Manager software.
- The user are not create by the vMatrix Server Manager software; try to new create an user in vMatrix to log in.
- Go to the vMatrix Server Manager software, in "User Management" page, find the user and right-click, chose "Properties" to check whether the user is disabled.
- Server is busy. Run Task Manager on the host to check if the host CPU is under high load operation, and unable to handle the new login users.
- The vMatrix Server Manager software versions are not paired between the host and zero client.

4） Terminal displays "Waiting to assign IP address ".

- Check whether network devices such as network cables are properly connected.
- Make sure that the network connected to the terminal can automatically obtain an IP address with DHCP, and select "Obtain an IP address automatically" option on the "Network" page to try to obtain an IP address automatically.
- Check whether the network's DHCP address pool is full and unable to assign IP addresses.
- Check whether there are duplicate IP in the network.
- If the network connected to the terminal without DHCP, please go to "network" page to set IP address manually.

5） USB devices do not work, there is no sound or there are lags on scrolling or playing a video.

- Run the vMatrix Server Manager software; open "user management"-"properties"-"Configuration"-"user default settings", check if "Graphic Acceleration", "Audio" and "USB Option" are disable. It is recommend using default configuration.
- Run the diagnostic tool and check if the service is enable normally.

6） private device cannot display in terminal

- Refresh the File Explorer page.
- The user may not create on vMatrix Server Manager.
- Check the permission for Storage Setting on the Vmatrix Server Manager, and re-apply the settings if they are correct.

7） Forget the password for device lock and settings lock.

Reset the device firmware to the factory installed one.

8） The resolution setting of the terminal is wrong, so the display cannot be displayed.

Restore all custom configurations to factory default.

9） If you want to use security software, you need to add the following files of vMatrix Server Manager to the whitelist.

- Disable security software before installing vMatrix to ensure successful installation.
- Add “vMatrix folder” in “C:\Program Files\Cloudpoint\” to the whitelist.
- Add “cphorus.sys, cphost.sys, cprhythm.sys, cptotem.sys” in “C:\Windows\System32\drivers” to the whitelist.