Zero Client with vMatrix Server Manager

User Manual

Rev4: 07-28-2020

This guide applies to Windows Server 2019 and earlier versions. All screen shots shown were captured from Windows Server 2012 and 2019 installations. The installation, configuration and login screens are based on vMatrix Server Manager 2.5.2. 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....1
Safety Information....2
Regulatory Compliance.... 2
Chapter 1. Product Overview.... 4
1.1 Brief Introduction.... 4
1.2 Package Contents....4
1.3 Device Connections....5
Chapter 2. Panning for Deployment.... 6
2.1 Host Configurations & Networking.... 6
2.1.1 Configurations by number of users and workloads....6
2.1.2 Networking....7
2.2 Software Requirements.... 8
2.2.1 vMatrix Server Manager....8
2.2.2 Windows Operating System....8
2.2.3 Multi-User Application....9
2.2.4 VLC Media Player....14
Chapter 3. Installation & Connection....15
3.1 vMatrix Installation.... 15
3.2 User Creation.... 19
3.3 Device Connection.... 21
3.4 Device Login.... 22
Chapter 4. Using The Zero Client.... 25
4.1 Menu Settings.... 25
4.1.1 Login....25
4.1.2 Display.... 27
4.1.3 Network....28
4.1.4 Ping....32
4.1.5 Boot.... 33
4.1.6 Shutdown Button.... 34
4.2 Settings Lock.... 35
4.3 Keyboard Layout Settings....36
4.4 Notification Log.... 37
4.5 Device Information.... 38
4.6 Firmware Update.... 39
4.7 Reset....42

4.8 Disconnect & Sign off..... 43
4.9 Use USB Devices.....43
4.10 More Tools & Settings..... 44
4.10.1 vChat Internal Messenger.....44
4.10.2 Set Password.....44
4.10.3 Set Language.....45
4.10.4 Set Hotkeys 45
4.10.5 Private Drive.....46
Chapter 5. Using vMatrix Server Manager.....47
5.1 User Management..... 47
5.1.1 New User Creation.....47
5.1.2 User Status View.....49
5.1.3 User Information View..... 50
5.1.4 User Desktop View.....51
5.1.5 Right Click Menu.....52
5.1.6 Personal Monitoring & Controlling..... 57
5.1.7 Personal User Settings.....59
5.2 Device Management.....70
5.2.1 Device Information View.....70
5.2.2 Right Click Menu.....71
5.2.3 Connect Setting..... 83
5.3 Configuration..... 84
5.3.1 Default User Settings.....84
5.3.2 Network Ports Config..... 85
5.3.3 Storage Settings.....86
5.3.4 IP Virtualization.....89
5.3.5 Server Group Configuration.....93
5.4.1 Monitor Authorization.....97
5.4.2 Notification..... 99
5.4.3 Enhancement Mode..... 100
5.4.4 Permission Control..... 101
5.5 Tools.....103
5.5.1 Broadcast Mode..... 103 5.5.2
Maintenance Mode.....104
5.5.3 Diagnostic Tools..... 105
5.6 Add-ons..... 106
5.7 Host Information.....107

5.8 Log.....108
5.8.1 User Action Log..... 108
5.8.2 Management Action Log..... 109
5.8.3 Event Log..... 110
5.9 About vMatrix..... 111
5.10 Offline Usage..... 112
5.11 More Tools & Settings.....115
5.11.1 Chat Tool.....115
5.11.2 Set Password..... 116
5.11.3 Set Language..... 117
5.11.4 Set Hotkeys 118
5.12 vMatrix Update..... 119
5.13 vMatrix Uninstall.....120
Chapter 6. Trouble-shootings.....122

Important Notices

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

BlackBox 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. BlackBox 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 BlackBox website at: www.BlackBox.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 BlackBox 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 BlackBox system. Additional software licenses may be required.

The BlackBox hardware and software products described in this user manual are protected by numerous granted and pending ISLAMIC REPUBLIC OF PAKISTAN and international patents.

© 2020 by Informatica Tecnologia (informatica.com.pk). All rights reserved. BlackBox and vMatrix are registered Trademark of Informatica Tecnologia (informatica.com.pk). – ISLAMIC REPUBLIC OF PAKISTAN. 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

BlackBox 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. BlackBox 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. BlackBox 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 BlackBox box, you will find the following items:

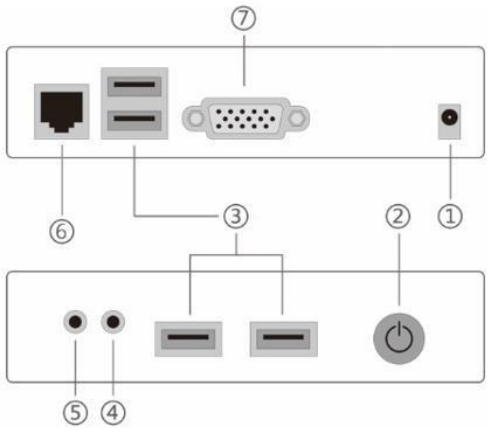
- A zero client terminal device
- A base/mounting bracket
- Two screws
- A 5V power adapter

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

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

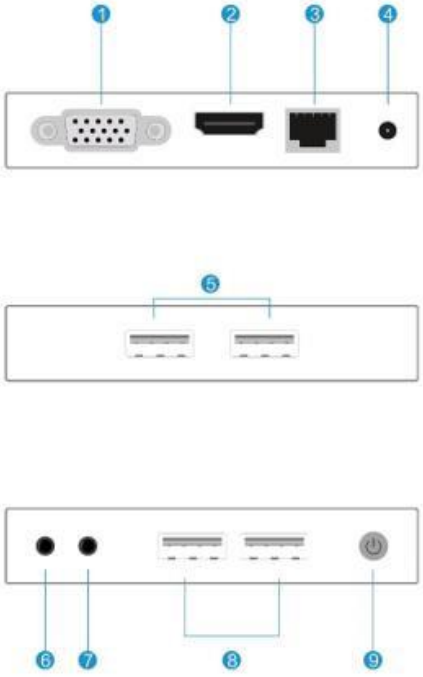
1.3 Device Connections

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



①VGA 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 Host Configurations & Networking

The preliminary guideline below provides an estimated starting point from which administrators can test and, if needed, adjust the hardware specifications of their chosen host systems. BlackBox recommends that you always test your environment in advance of deployment to ensure it meets your expectations.

2.1.1 Configurations by number of users and workloads

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.					

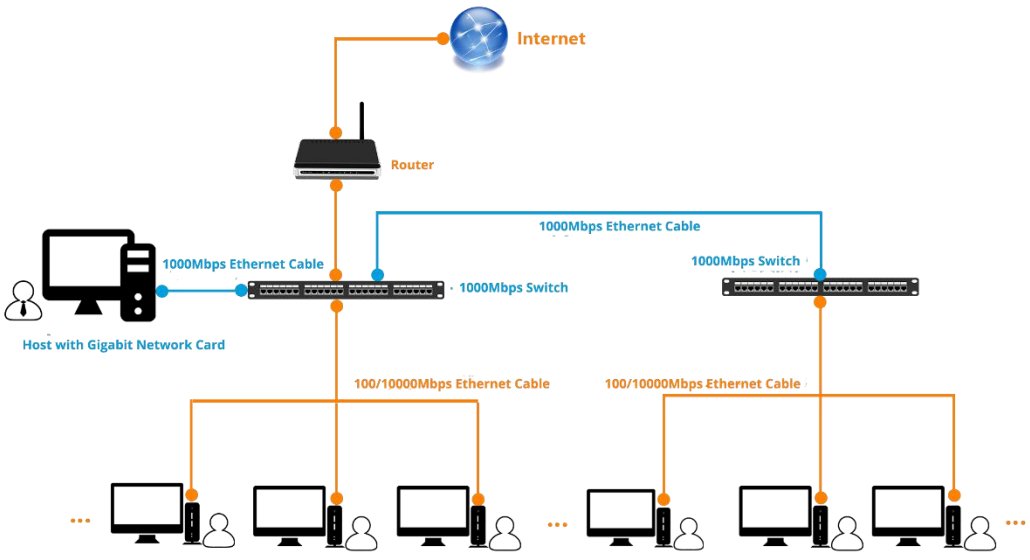
Note:

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) vMatrix Server Manager permits up to 99 users per host. The number of users a customer's installation will support depends upon the host's configuration and performance expectations of the customer.

3) You are recommended to 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, and 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



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

2.2 Software Requirements

2.2.1 vMatrix Server Manager per shared host

The latest version of vMatrix Server Manager is obtainable at

https://www.BlackBox.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 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 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

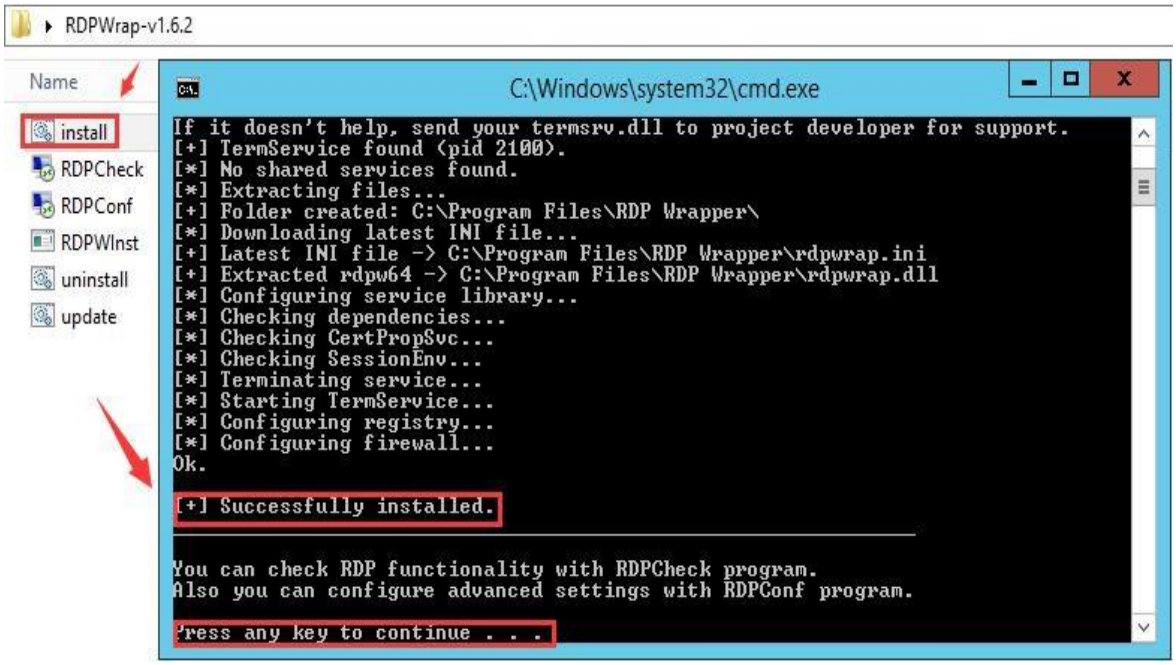
vMatrix doesn't contain a component or application to allow multiple users to access the host simultaneously. To allow a simultaneous multi-user login, you need to install RDP Wrapper (download and learn more at www.BlackBox.com/support/add-ons) or obtain Microsoft RDS CALs. To properly license BlackBox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

- **RDPwrapper**

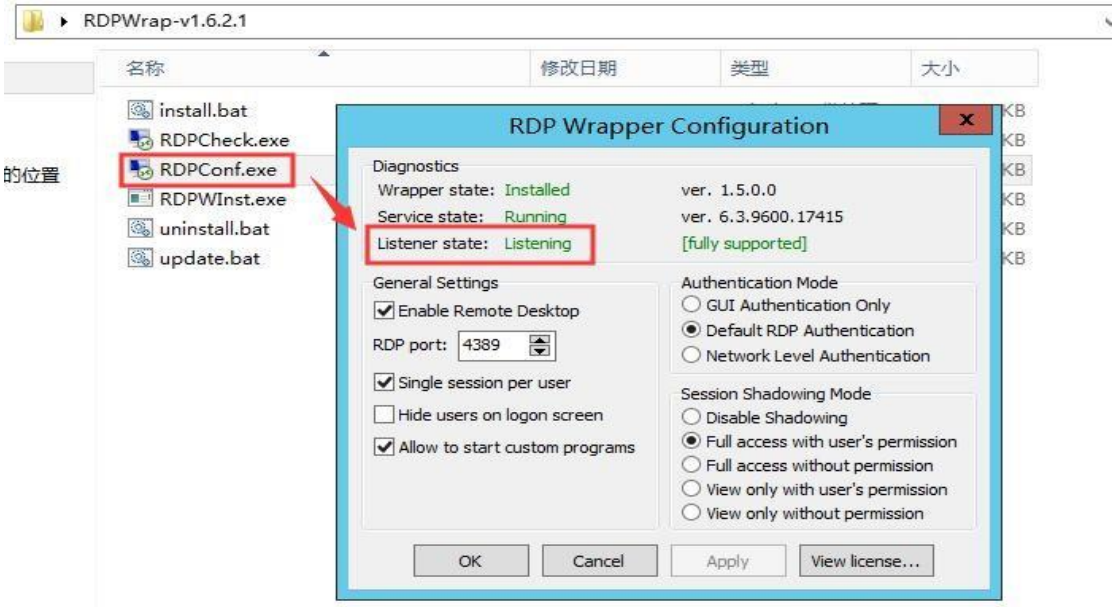
RDP Wrapper is a free open source project to enable Remote Desktop Host support. RDP Wrapper is obtainable at https://github.com/DrDrrae/rdpwrap/releases

Instructions:

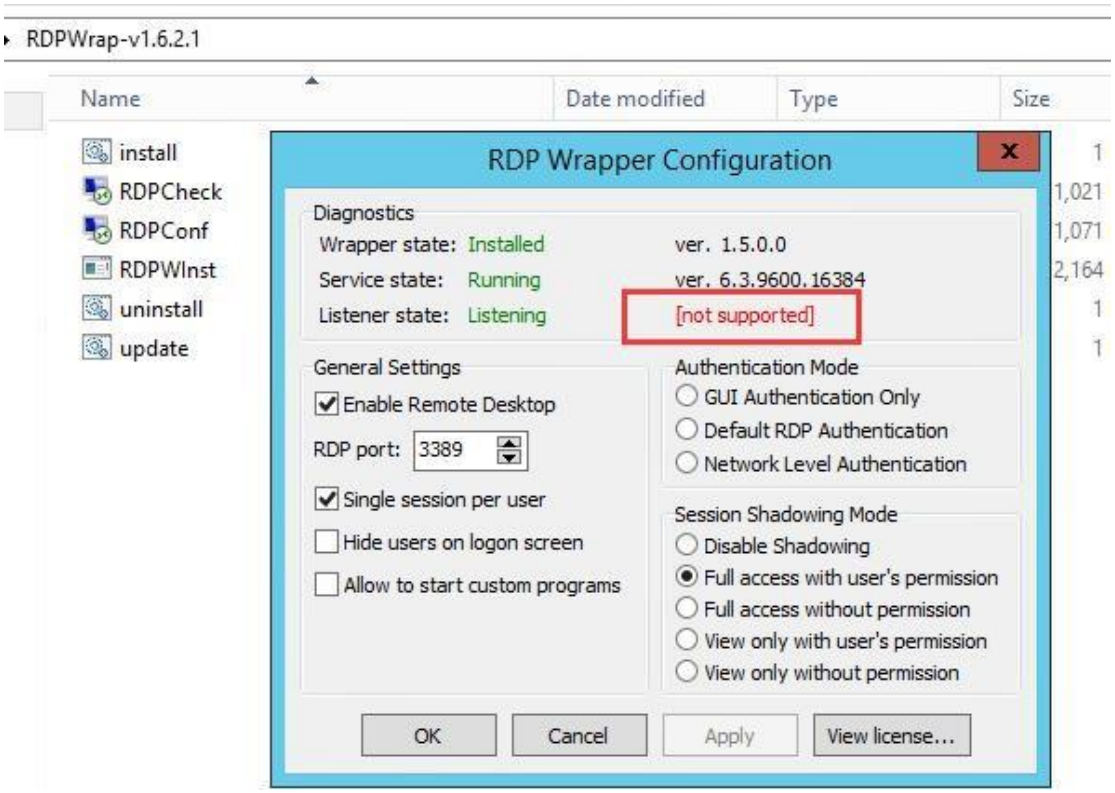
1) Download the RDPWrap.zip file and then unzip it. Simply run the insall.bat file and press any key when finished but make sure to disabled anti-virus software during installation.



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



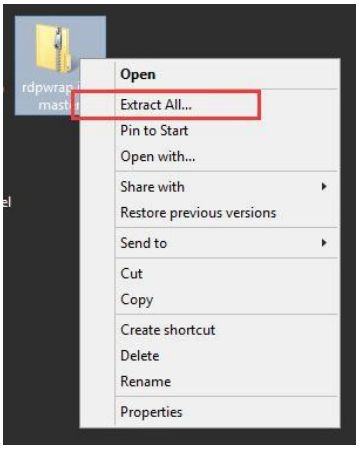
Reminder: update the "rdpwrap.ini" file if the configuration tool shows "[not supported]" in red.



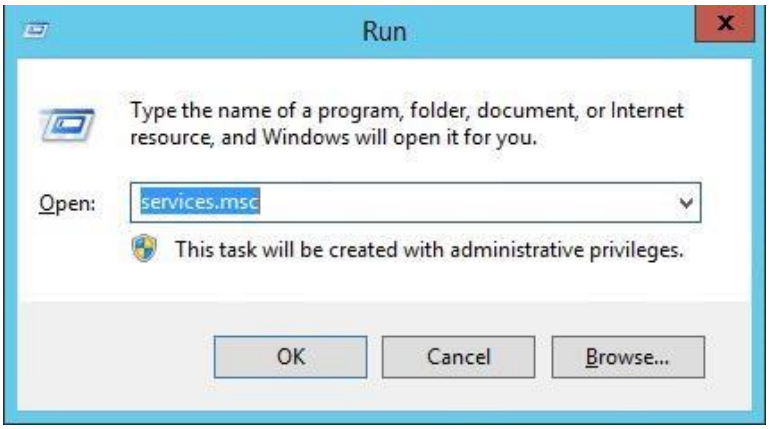
①

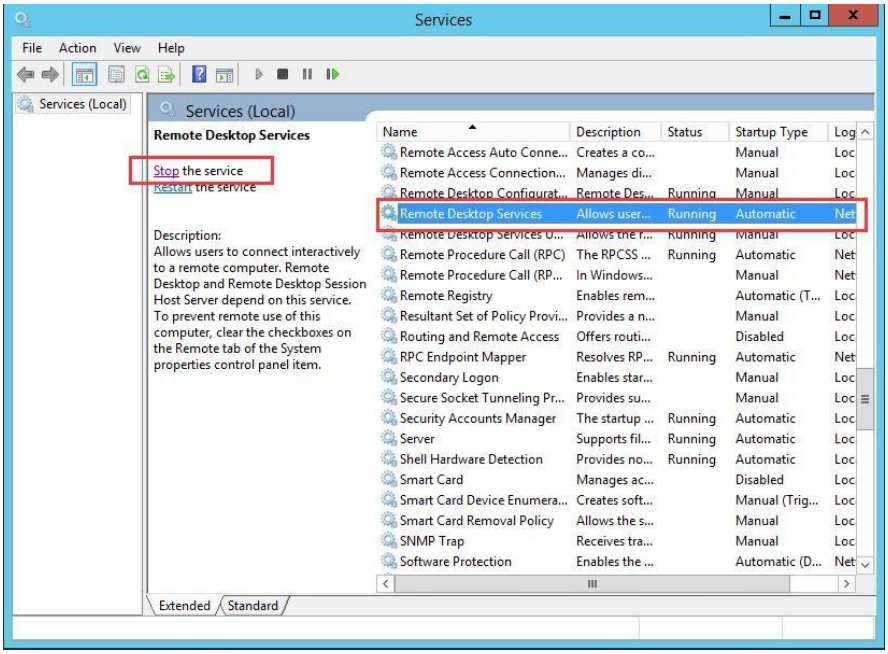
Download the latest "rdpwrap.ini" compressed file and extract the files.

Download Url: https://codeload.github.com/sebaxakerhtc/rdpwrap.ini/zip/master.

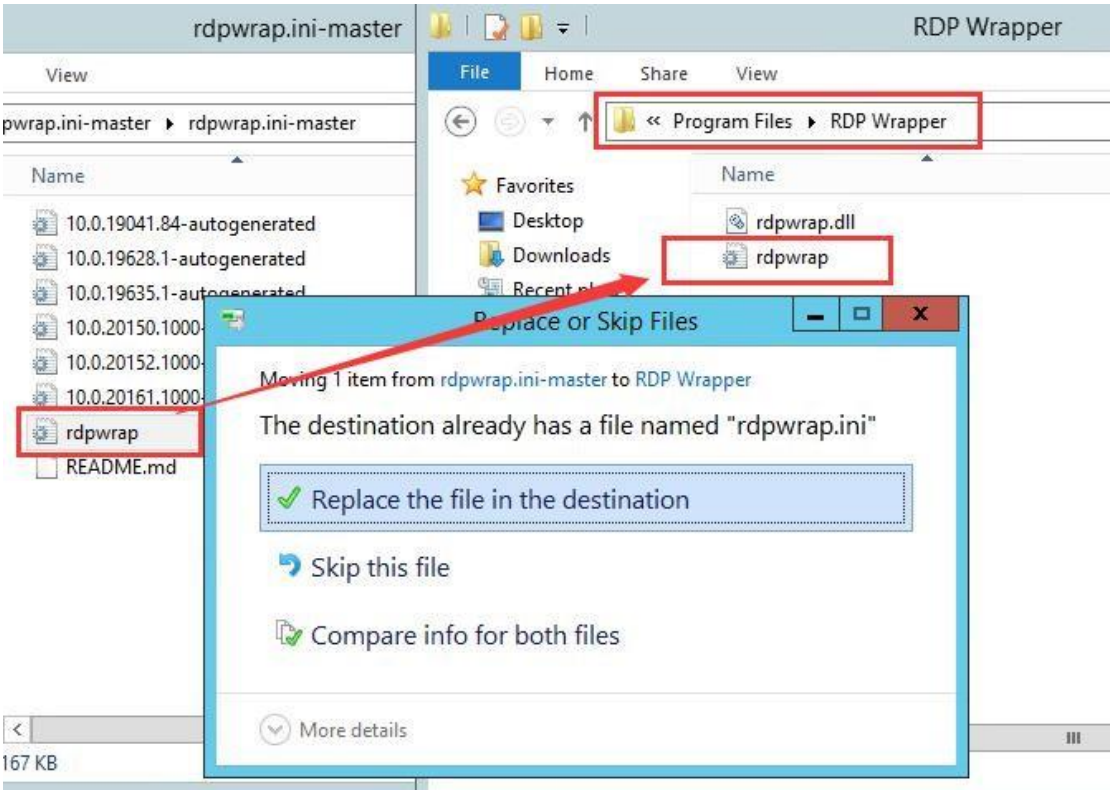


② Presss “Win”+“R” to run “services.msc”, and stop the “Remote Desktop Services”.

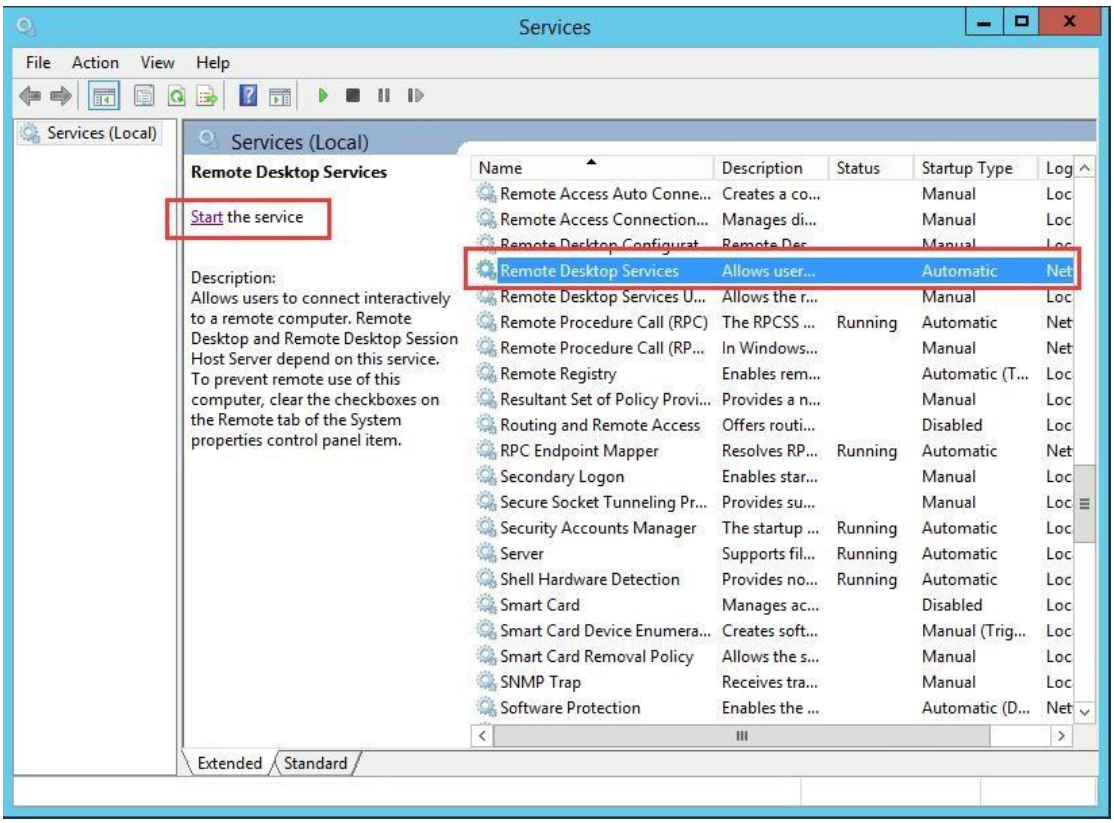




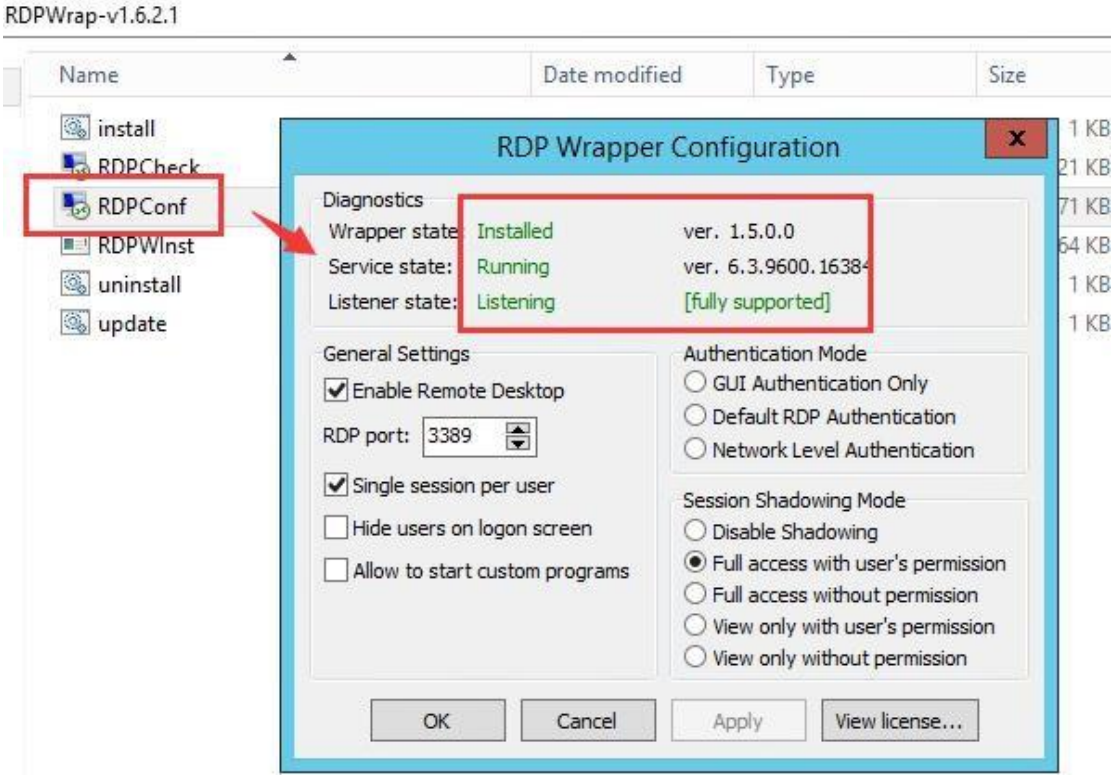
③ Replace the “rdpwrap.ini” file in the path of C:\Program Files\RDP Wrapper with the downloaded one.



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. You are licensed by BlackBox to use the vMatrix Server Manager software under the terms of the EULA. You cannot use the vMatrix Server Manager software with Windows Client software (i.e., Windows XP, Windows 7, Windows 8/8.1, Windows 10) unless a single user and no other user accesses the same Windows Client software at any one time, or you are authorized to do so under an applicable license from Microsoft. In all cases, your rights and obligations with respect to the use of vMatrix Server Manager software with Windows Server software and Windows Client software are defined by both the BlackBox vMatrix Server Manager software EULA and the applicable Microsoft Software License Agreement or EULA.

2) Run the RDP Wrapper files after extracting them to your local disk. Do not run them in the compress file. 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, BlackBox 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. This feature is supported by VLC player of 2.1.5 or newer versions and works automatically after the installation of vMatrix 2.x. Just make sure you are using the correct versions of vMatrix and VLC player and VLC player is selected to play the video, then you are ready to "save".

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

Note:

1) 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.

2) 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.

3) vDirect 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

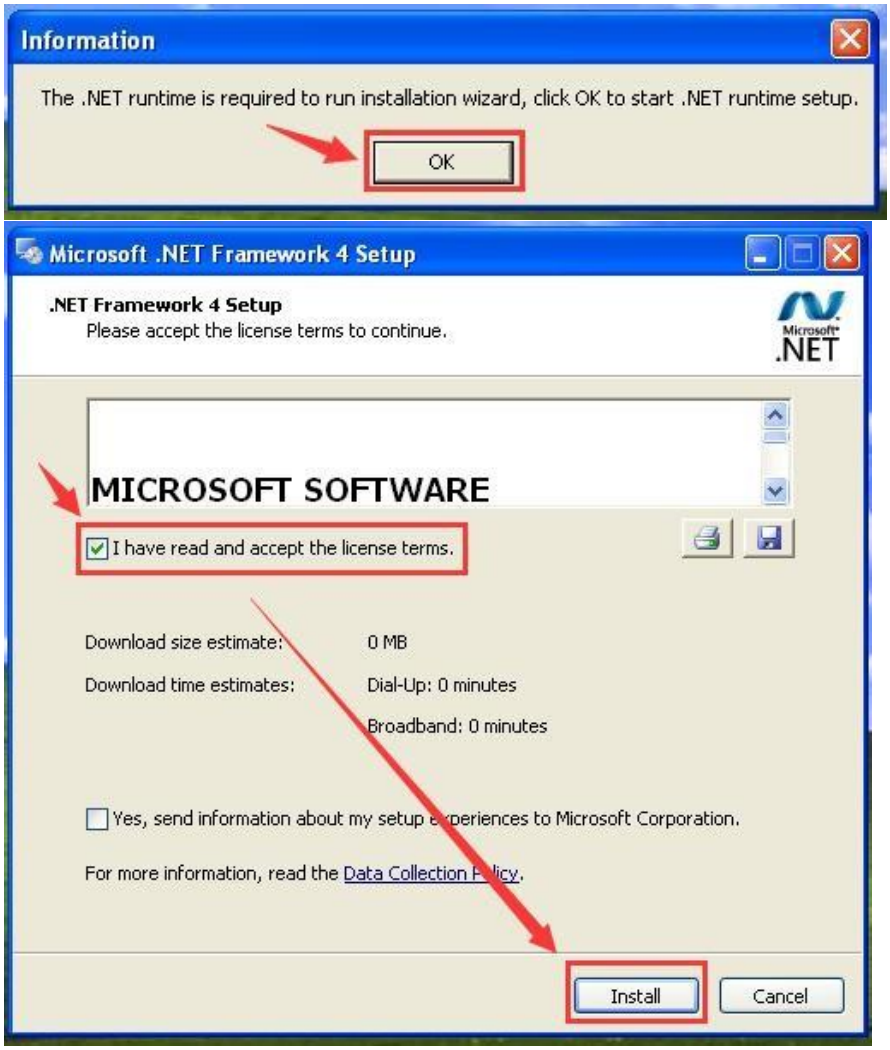
- It is recommended to use the new original operating system to avoid problems such as installation failure or use error due to file corruption or loss of the old system. Please download the original Windows system image on the official website of Microsoft to ensure system security and functional integrity.

- Please make sure to DISABLE secure boot 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.

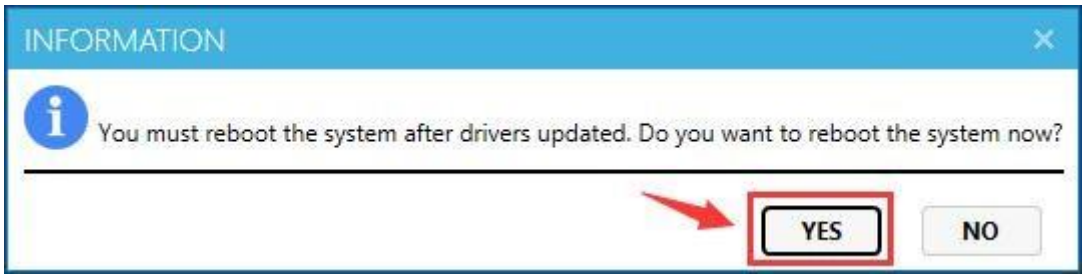
2) On initial installation, vMatrix Installer will detect if some required components are installed on the host. Allow installing required components if it prompts. For the Windows XP operating system, you have to manually install the components as shown below:



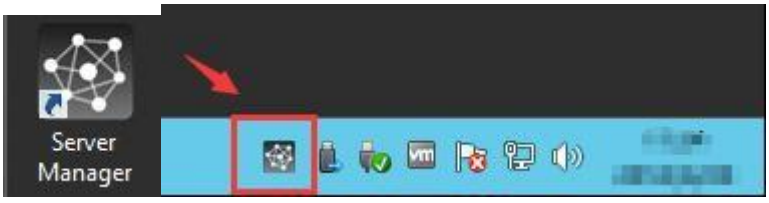
3) During installation, your will be prompted to install drivers, click “Install”.

4) Click “Completed” and finish installation.

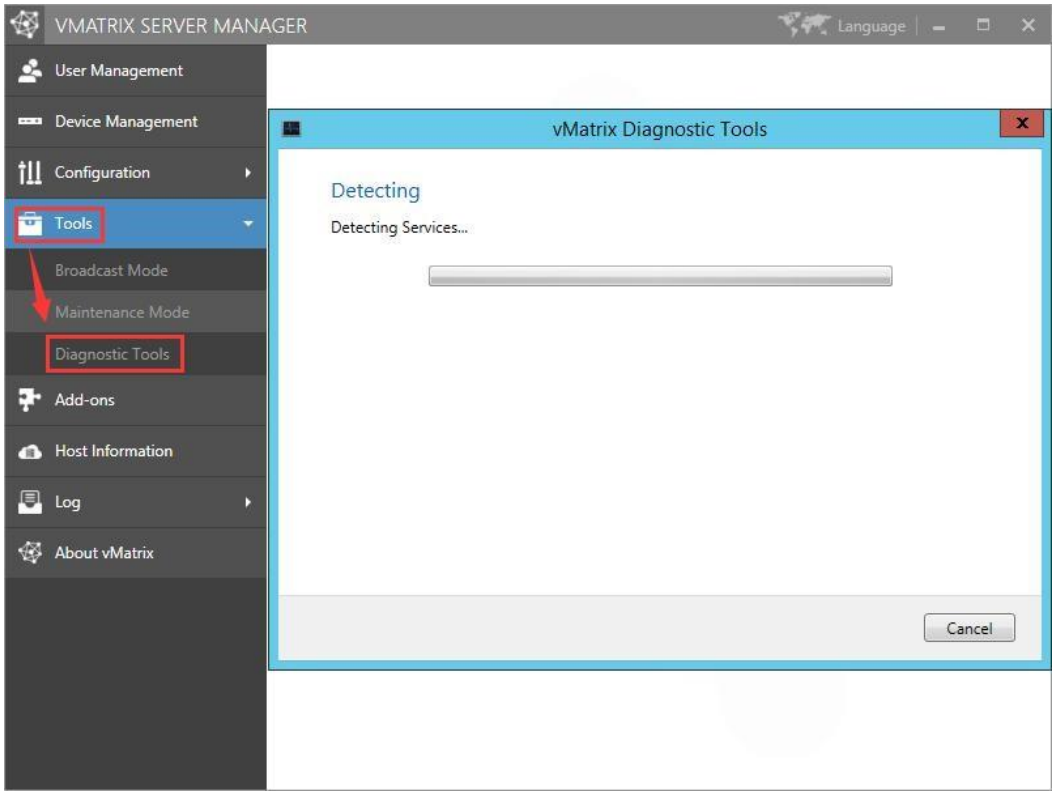
5) You will be asked to reboot the system. Click “yes”.



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.

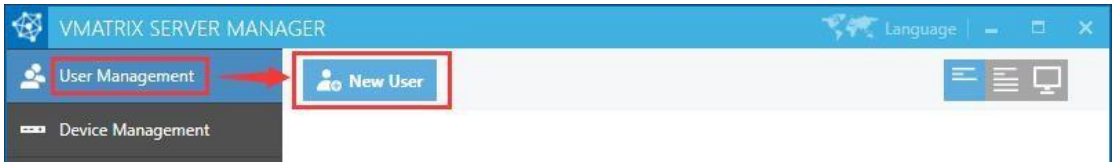


8) After vMatrix Server Manager is running properly, install Microsoft RDS CALs or RDP wrapper to support multi-user login.

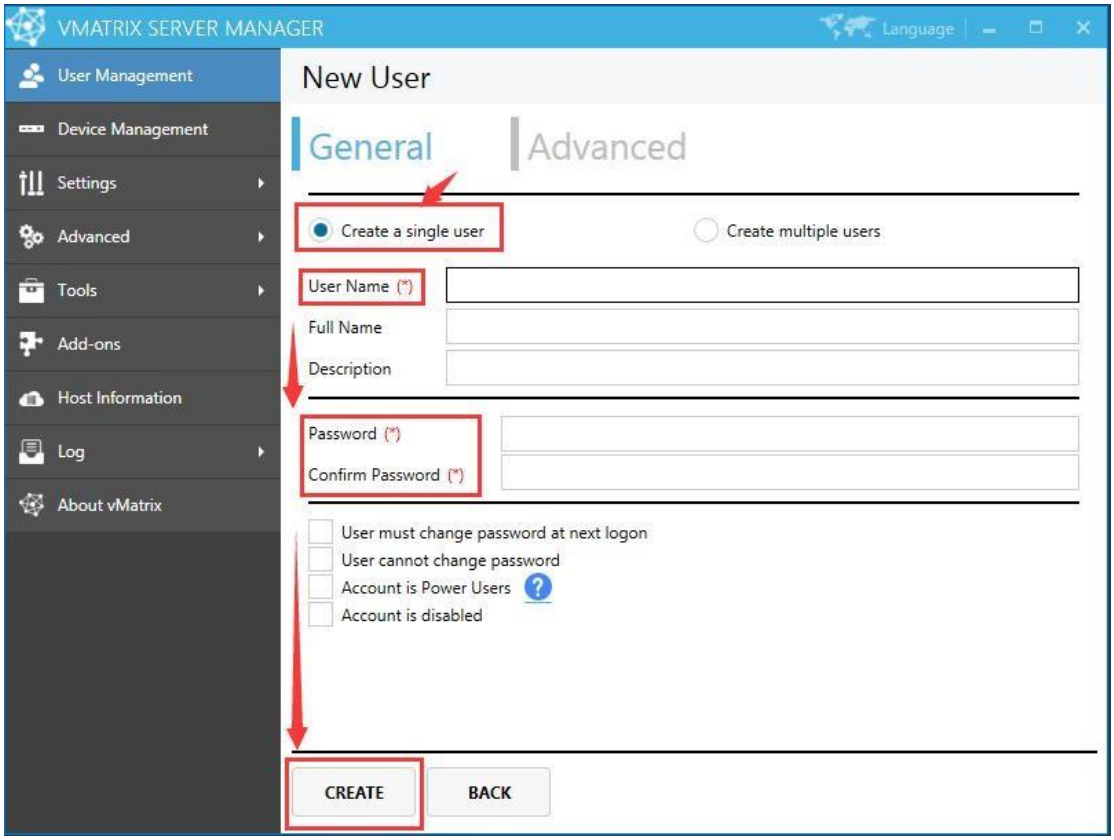
3.2 User Creation

1) Open vMatrix Server Manager console.

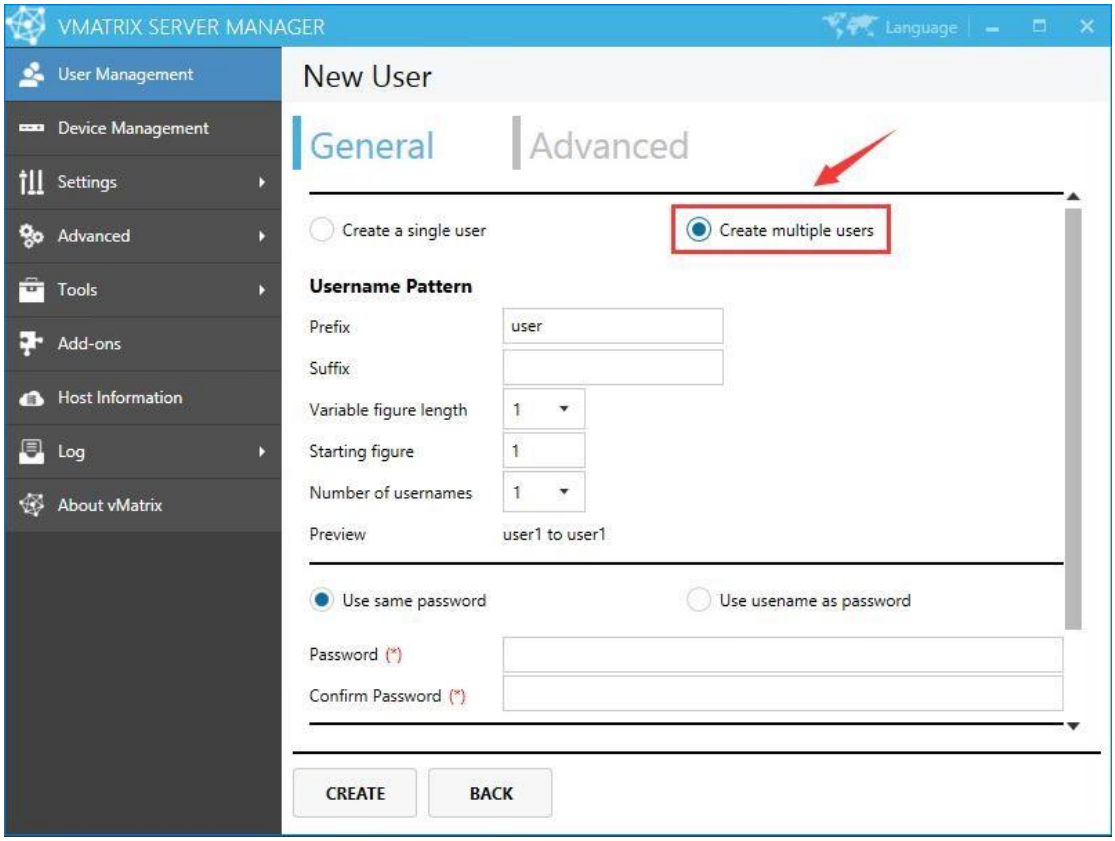
2) Go to “User Management” page, click “New User” to create user accounts.



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



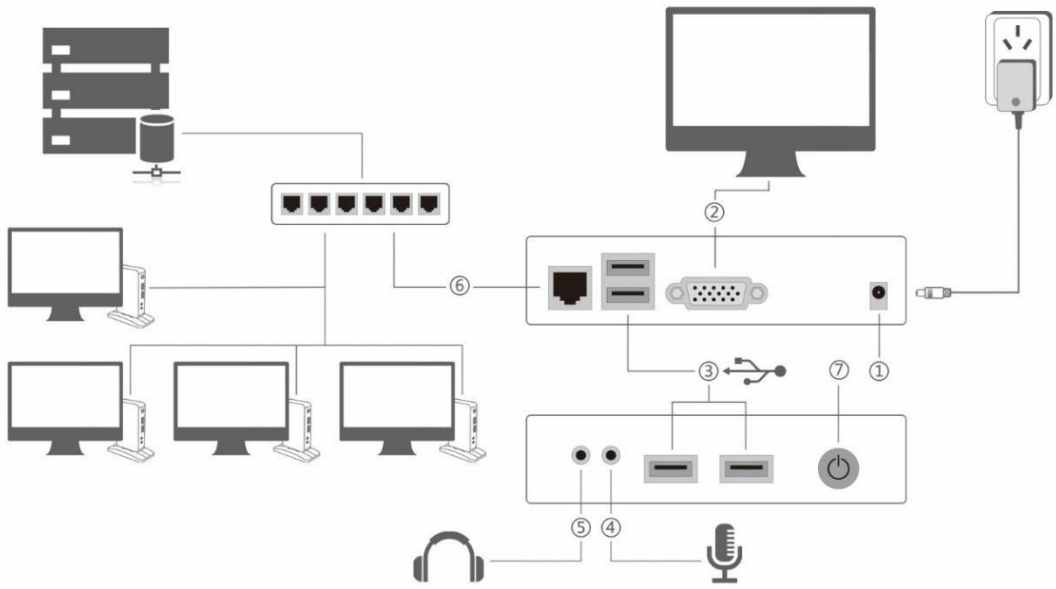
To create multiple users at a time, select “Create multiple users”, and then select the number of users and enter passwords or select to use user name as password for all users.


VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Add-ons
Host Information
Log
About vMatrix
New User
General
Advanced
Create a single user
Create multiple users
Username Pattern
Prefix
user
Suffix
Variable figure length
1
Starting figure
1
Number of usernames
1
Preview
user1 to user1
Use same password
Use username as password
Password (*)
Confirm Password (*)
CREATE
BACK

3.3 Device Connection

Connect the zero client to other peripherals as shown below.

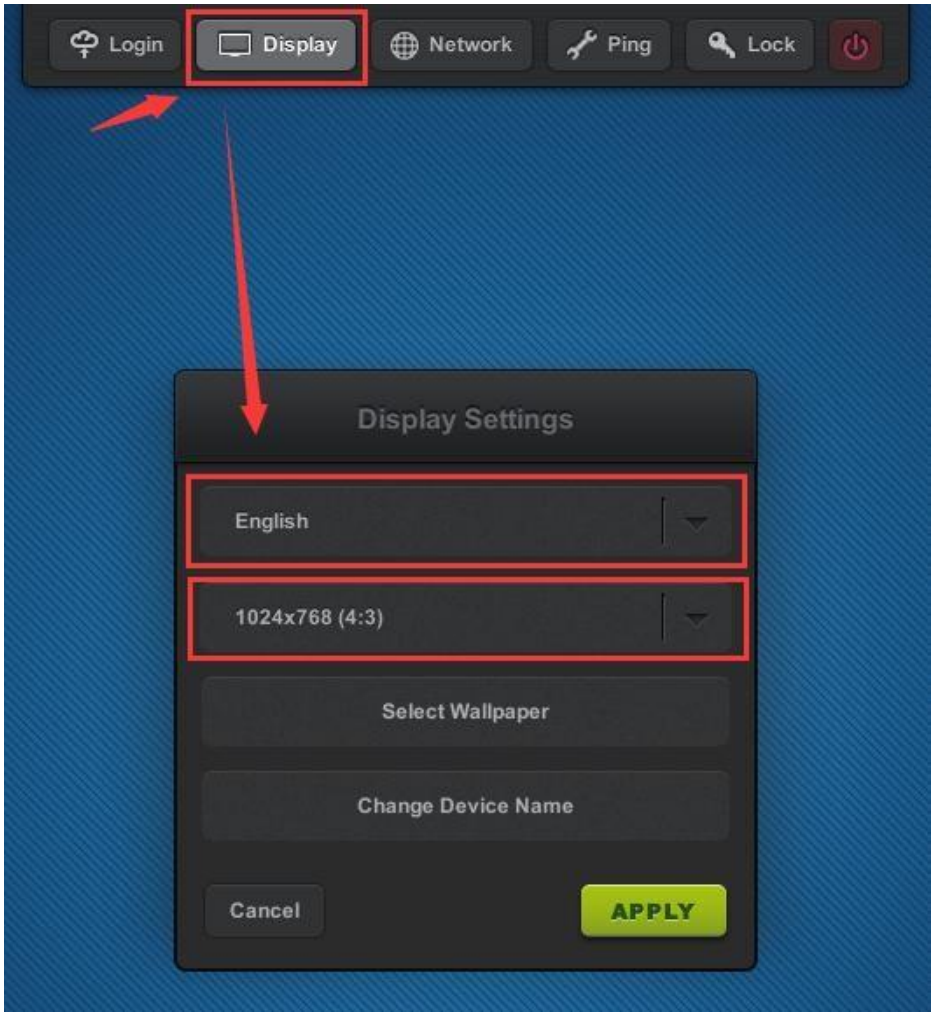
- Connect the zero client to the power adapter of 5V, 2A. Do not use power adapter of other specifications to avoid damage to the zero client.
- Connect the S100 zero client to a monitor with VGA port and V1 zero client to a monitor with VGA or HDMI port.
- Connect the zero client to USB keyboard and 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.



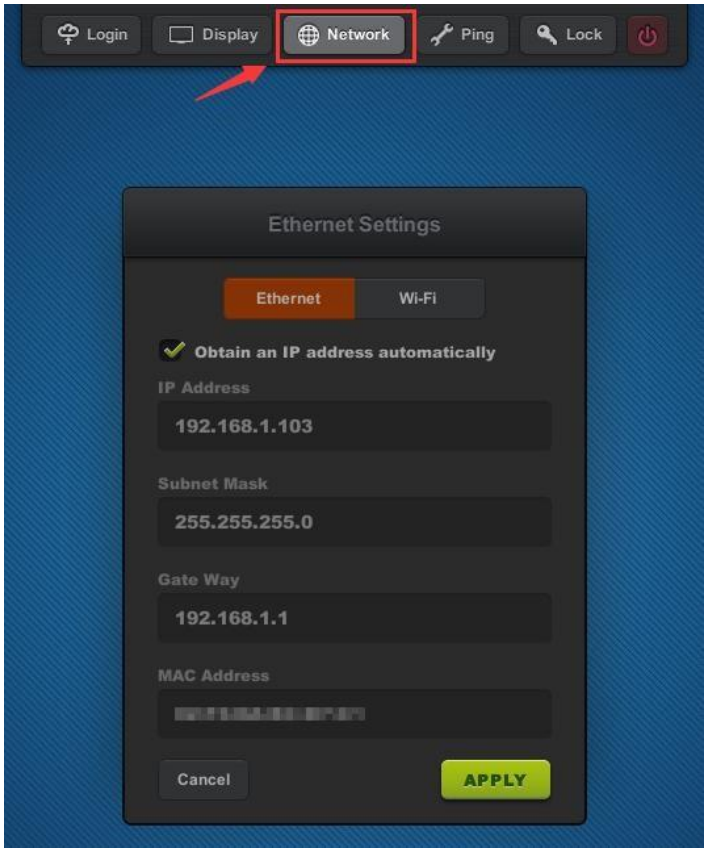
3.4 Device Login

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

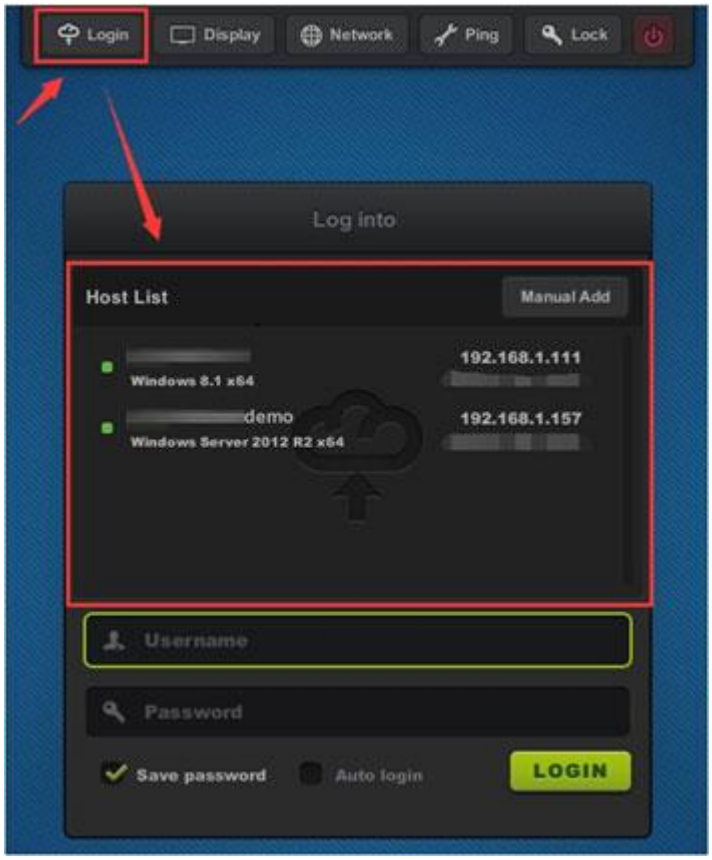
2) After system boot, go the display page, select your correct language and desktop resolution; factory default language is “English” and desktop resolution is “1024x768”.



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.

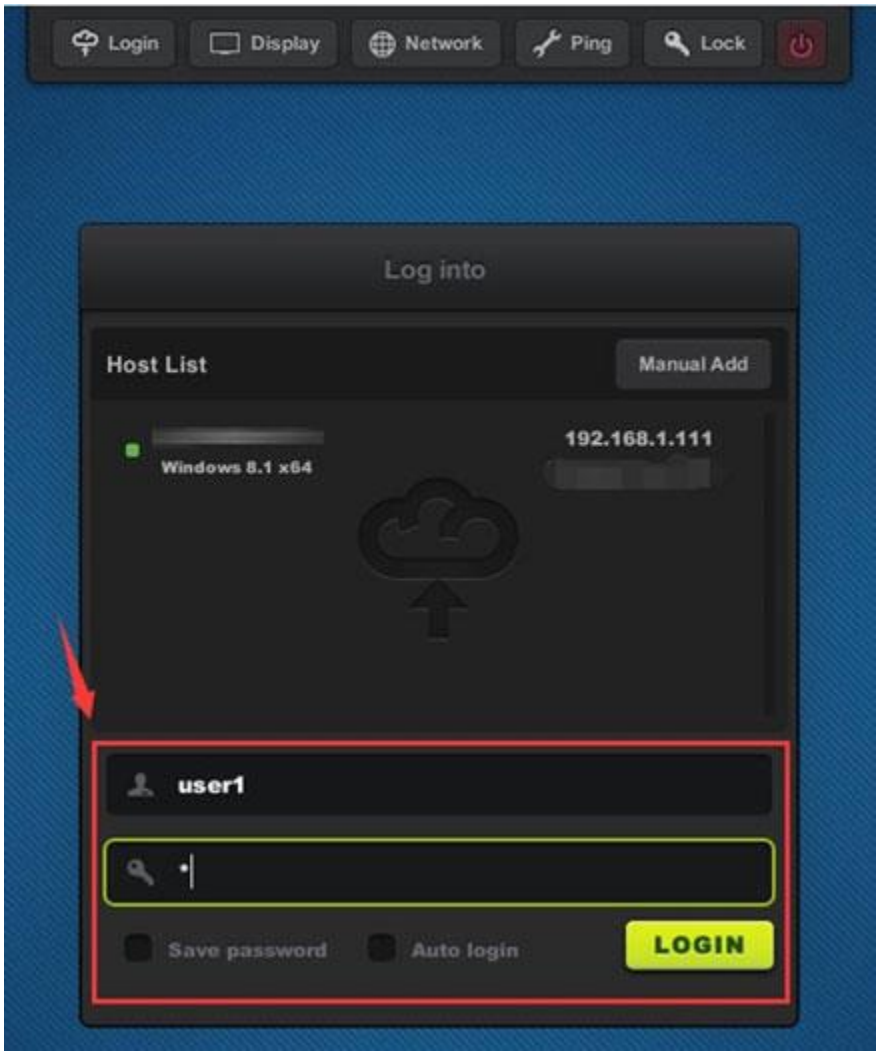


4) Go back to the “Login” page, select the host available in your network for connection.



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.



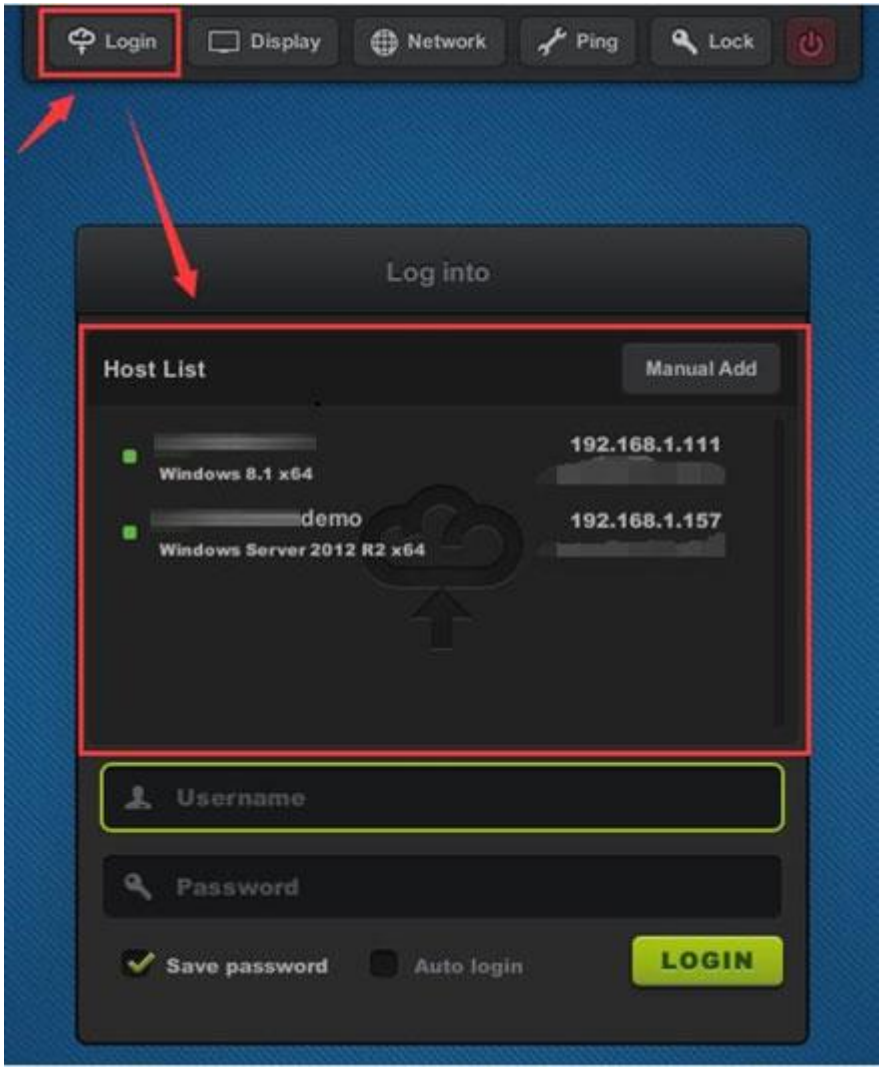
Chapter 4. Using The Zero Client

4.1 Menu Settings

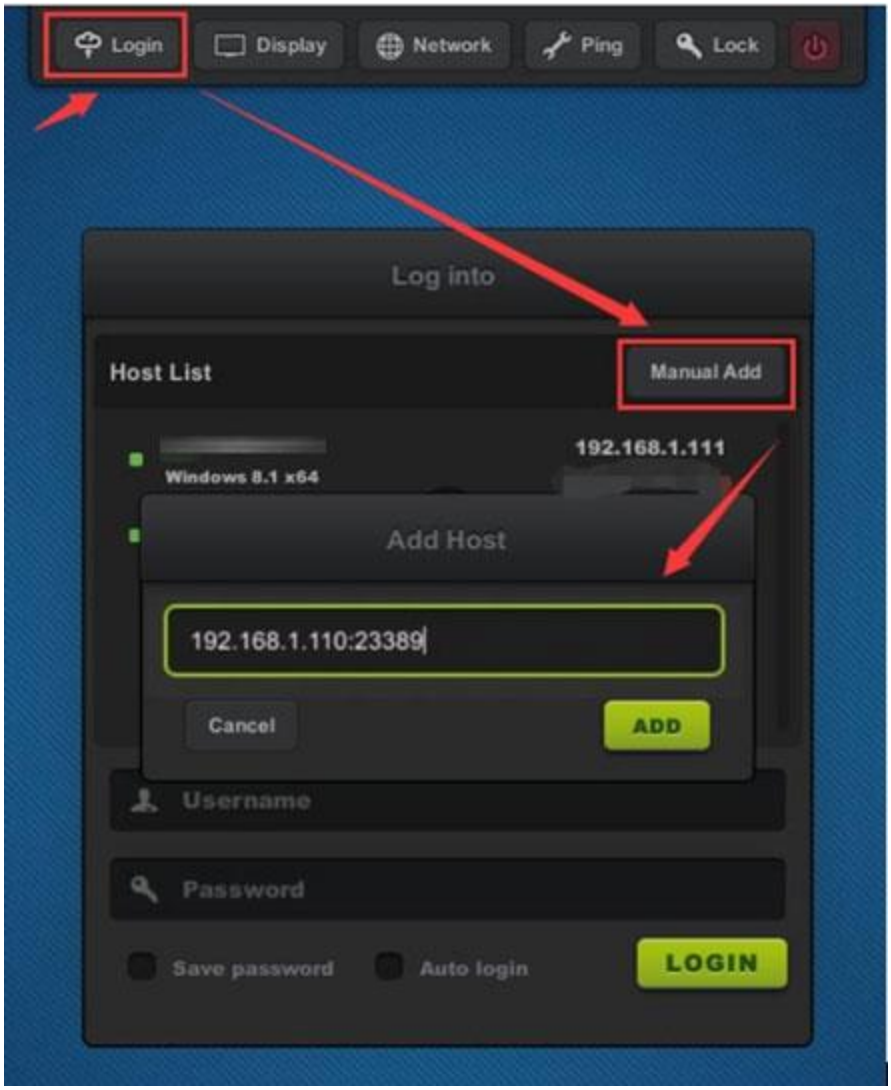
4.1.1 Login

- 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.
3) hosts that the device ever connected to even it is not in the same network segment.

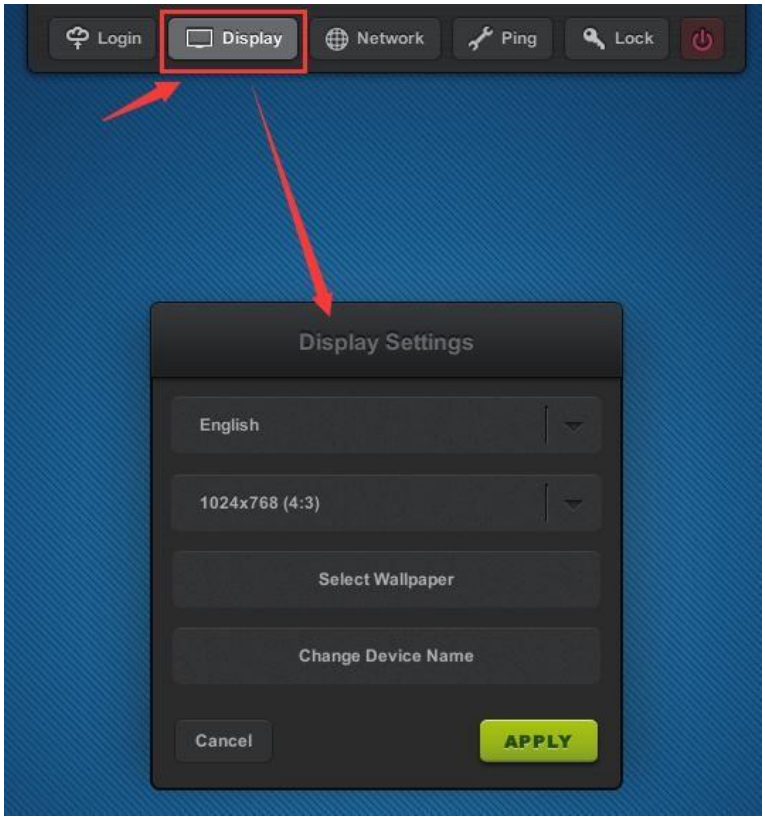


- To connect to an available host not shown in the list, you can manually add the host IP through the “Manual Add” button ((vMatrix default network port is 13389, if you have manually changed the port, add the port number when you manually add the host).



- Password field is case-sensitive while user name field is not.
- Save password: to remember the user name and password of this login so you won't have to enter user name and password again on next login. Changes will take effect on next login.
- Auto login: enabling auto login will skip the device login page and directly enter the system of the last login host with saved user name and password on device boot. Auto login will automatically enable "Save password". Changes will take effect on next login. To cancel Auto login (go back to the device login page) after entering the host system, disconnect or sign out user session.

4.1.2 Display

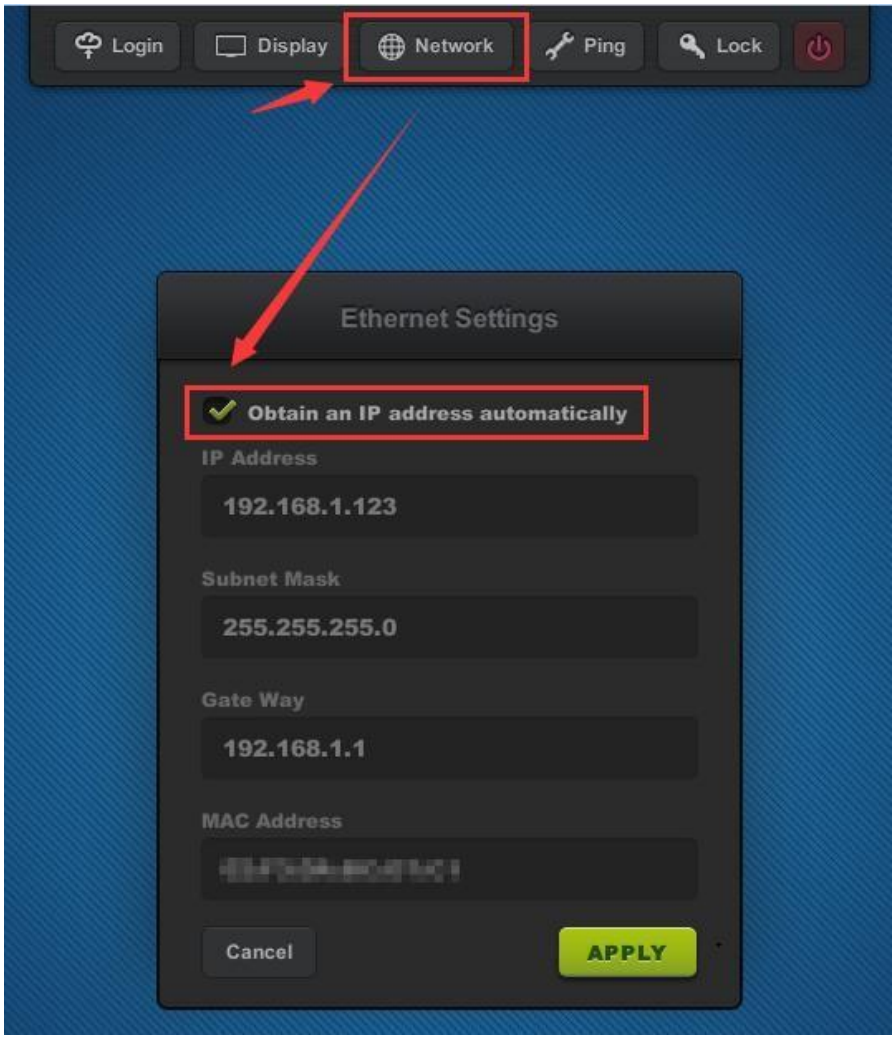


- **Language:** to change the device language; available languages: English Chinese, Russian, default: English.
- **Resolution:** to change the resolution for the device interface and user desktop; default: 1024x768 (4:3), maximum: 1920x1080.
- **Wallpaper:** to change wallpaper for the device interface.
- **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.



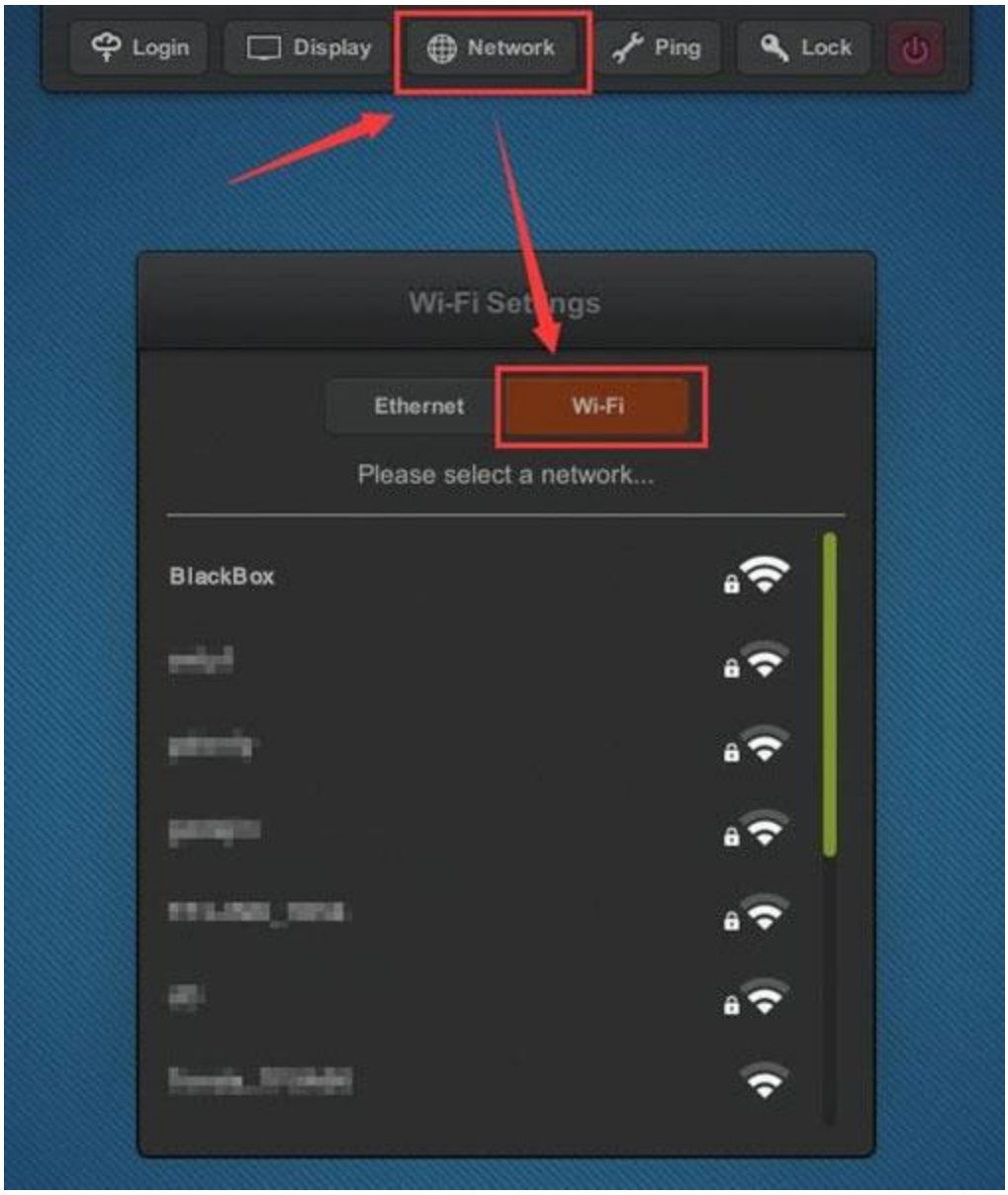
Note: IP address of the client device is for communication in LAN with vMatrix Server Manager only (for device management). After connecting to the host, the user desktop session will share the IP address of the host for network communication (for session management). If you want each user desktop session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

- **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.



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

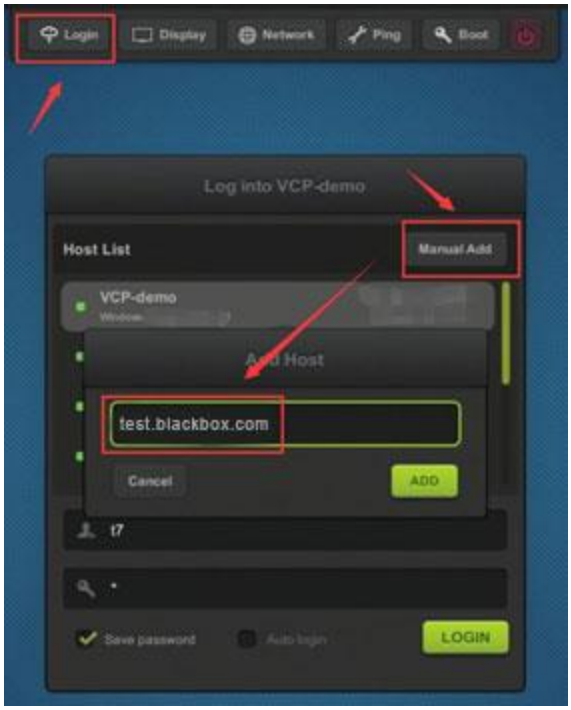
3) When the WIFI network you selected is displayed above the line divider, the WIFI connection is established.

Note:

1) Any antenna that is built with RTL8188EUS chip and connects with USB 2.0 standard is supported by BlackBox zero clients.
2) Please connect the WIFI antenna before the zero client is powered on.
3) Only one WIFI connection can be 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 which you are connecting the zero client to.
5) Although the BlackBox 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.
6) When the Wi-Fi password is entered incorrectly, there will no prompt, the device will keep connecting. You need to click the right button to enter the detail page, click "Ignore this network", and then reselect Wi-Fi network and enter the correct password.

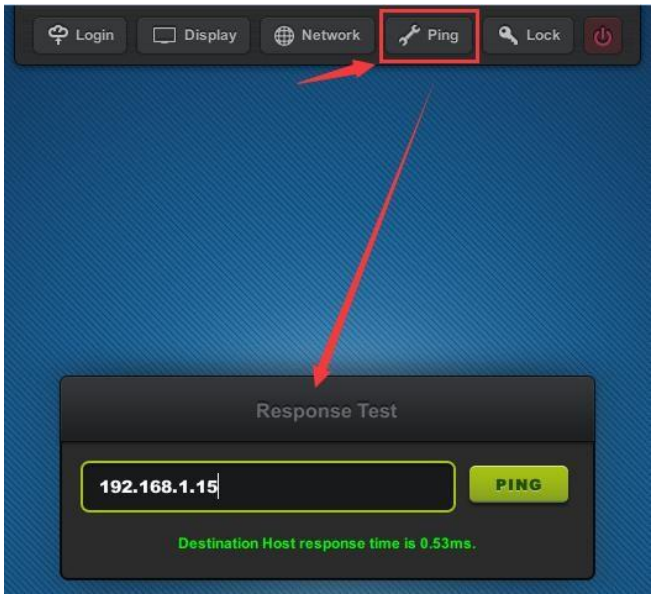
- **DNS Settings**

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.



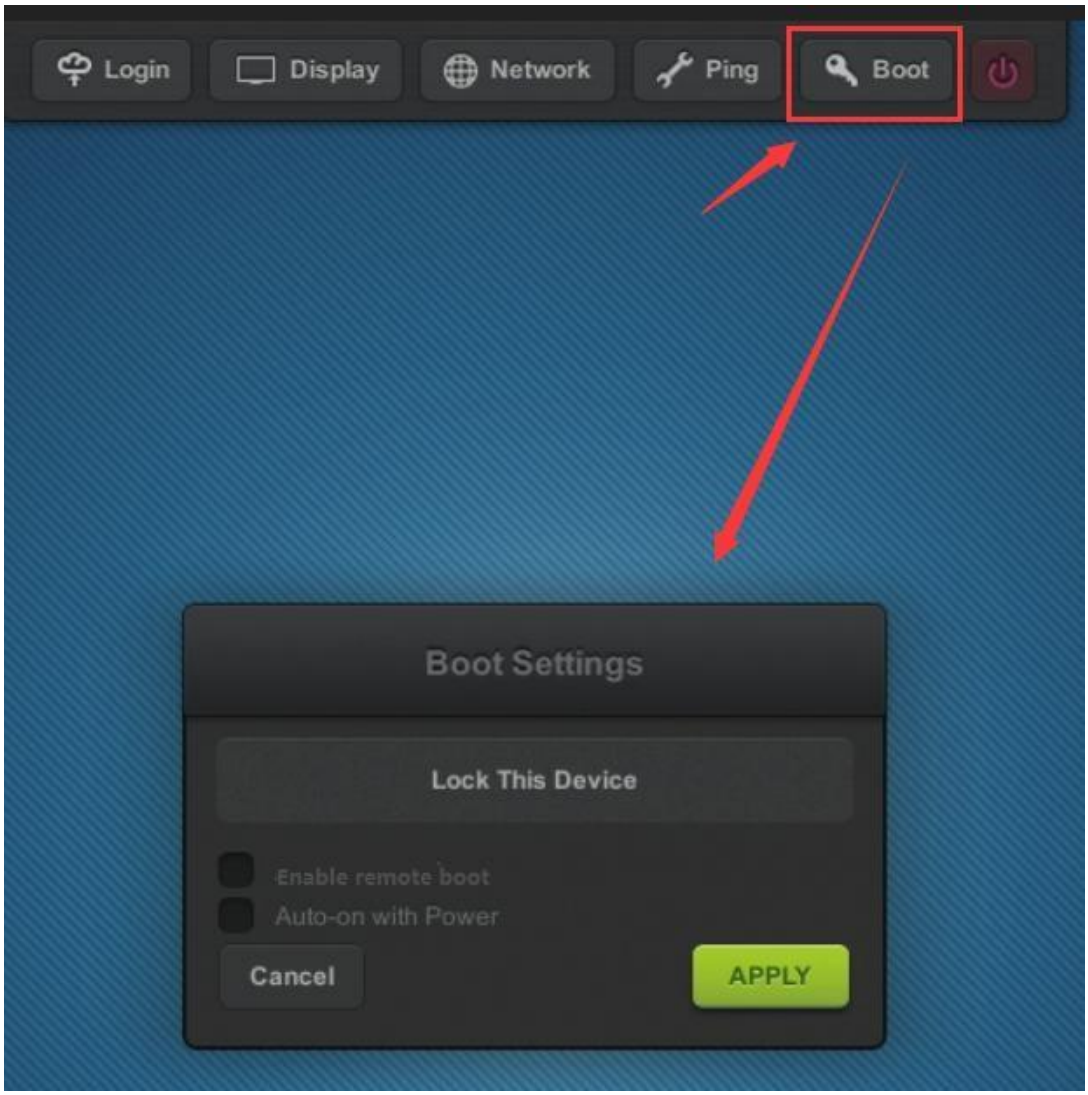
4.1.4 Ping

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 is connected fine. The shorter the response time, the better the connection.



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.



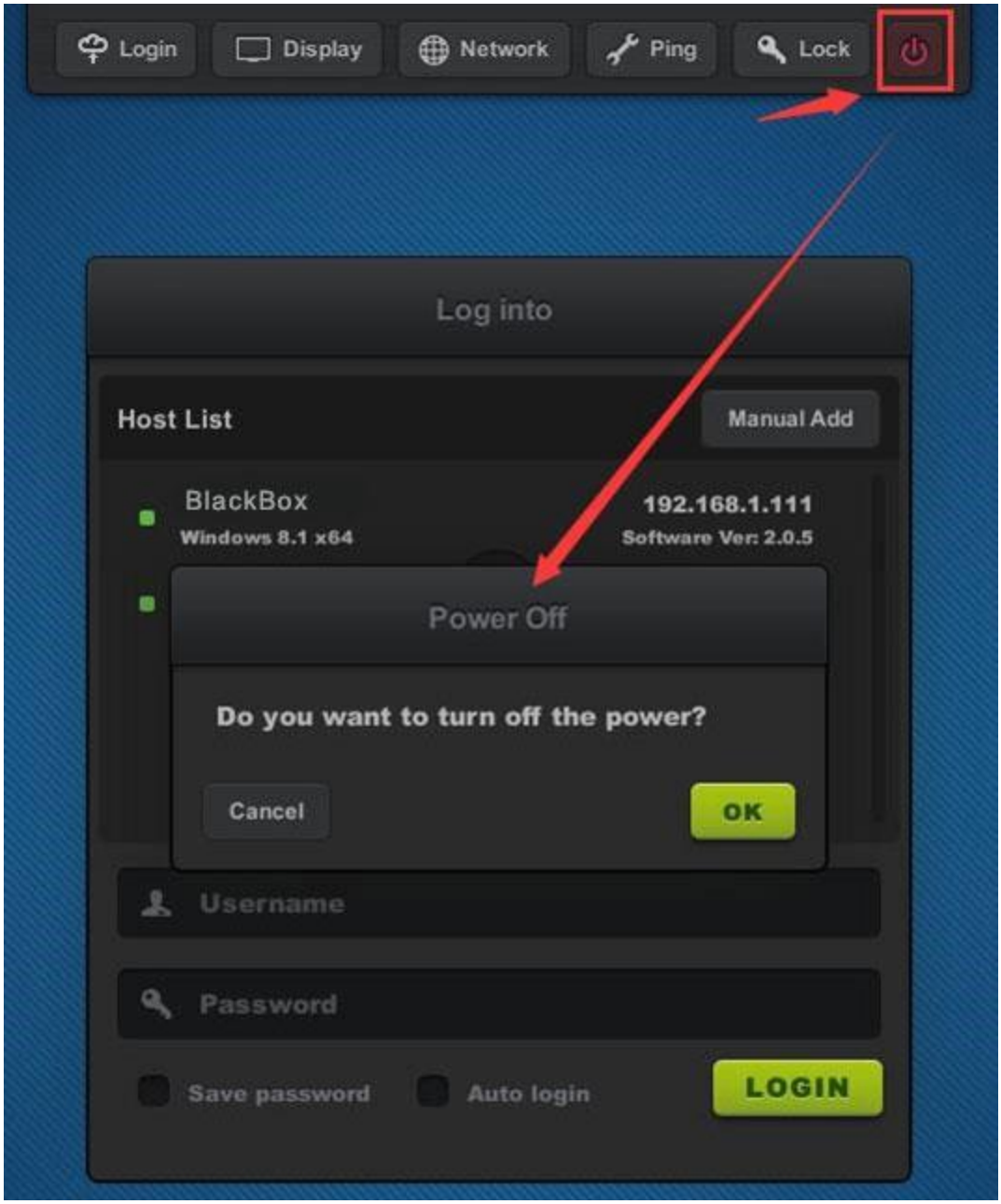
Note:

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

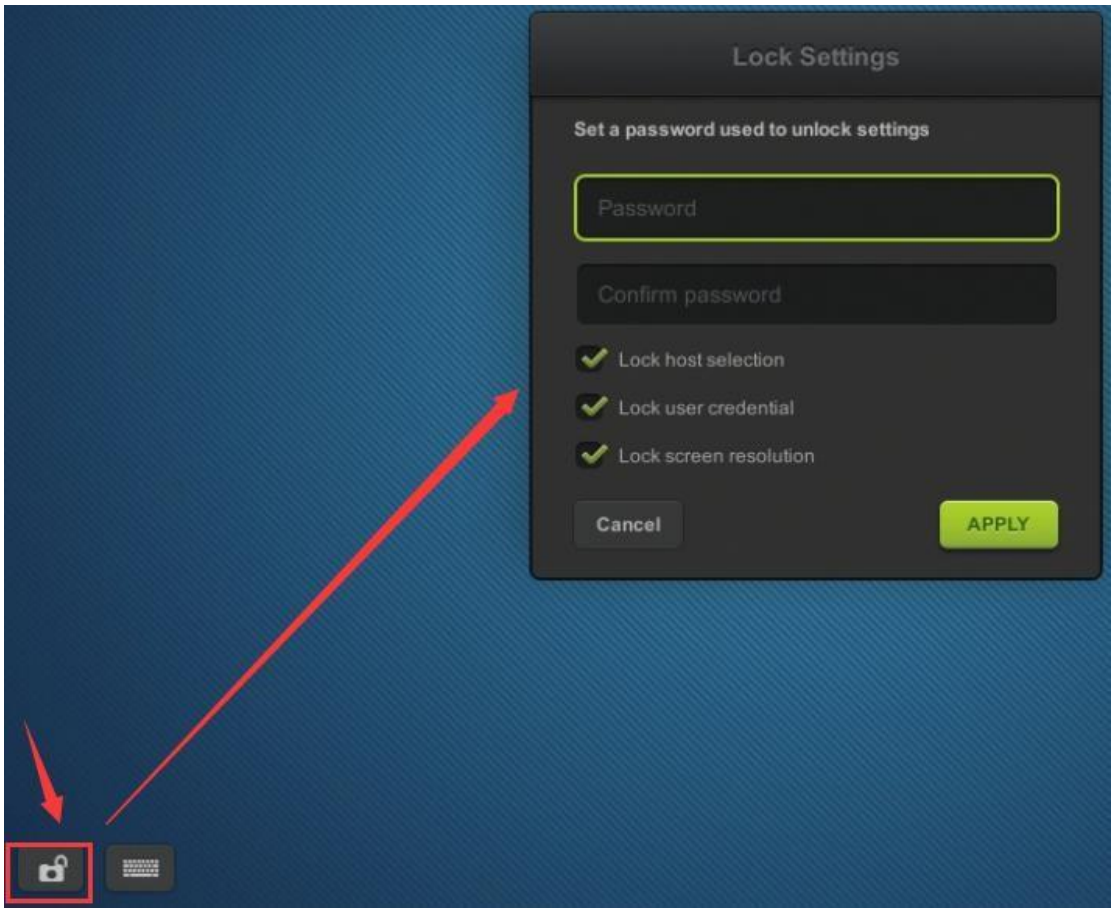
This button allows you to turn off the device without pressing the physical button on the device. This is helpful when the device is mounted at the back of the monitor.



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 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.



Note:

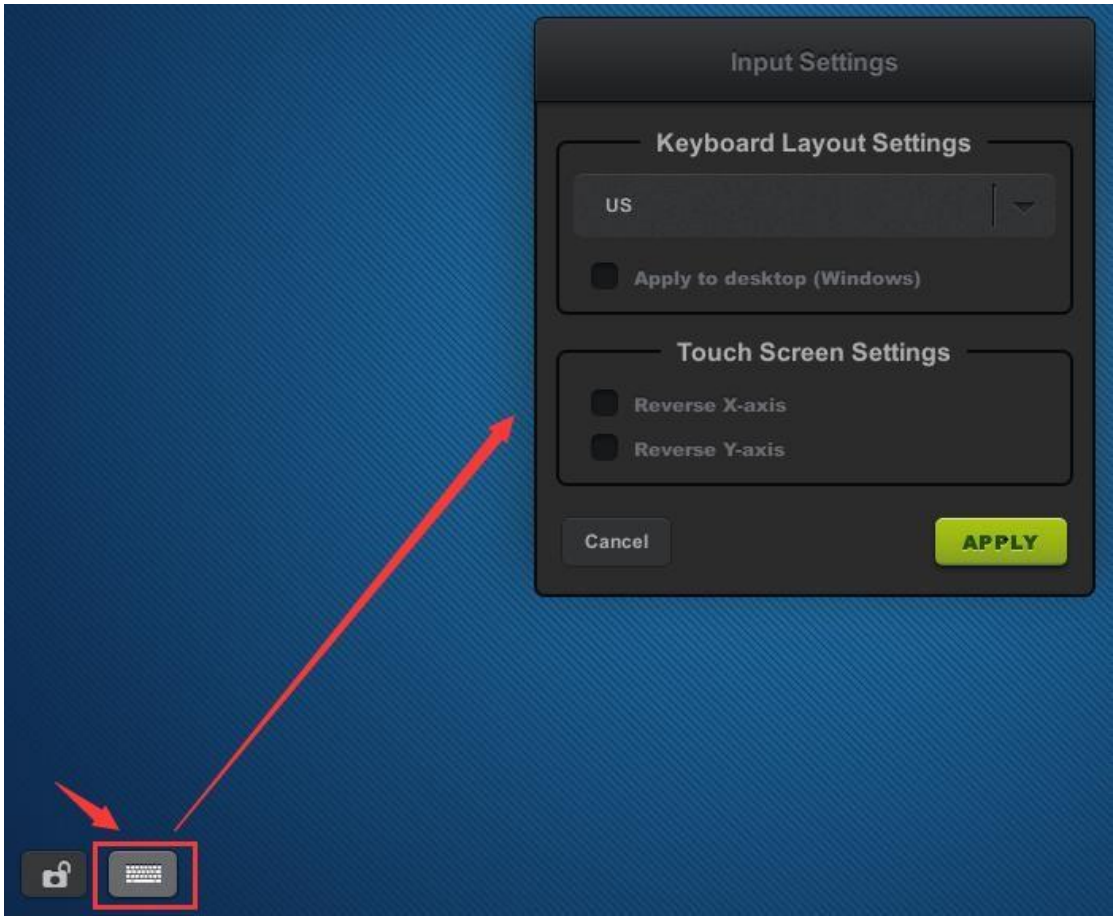
1) To unlock the device, just clear the password and apply.

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

4.3 Keyboard Layout Settings

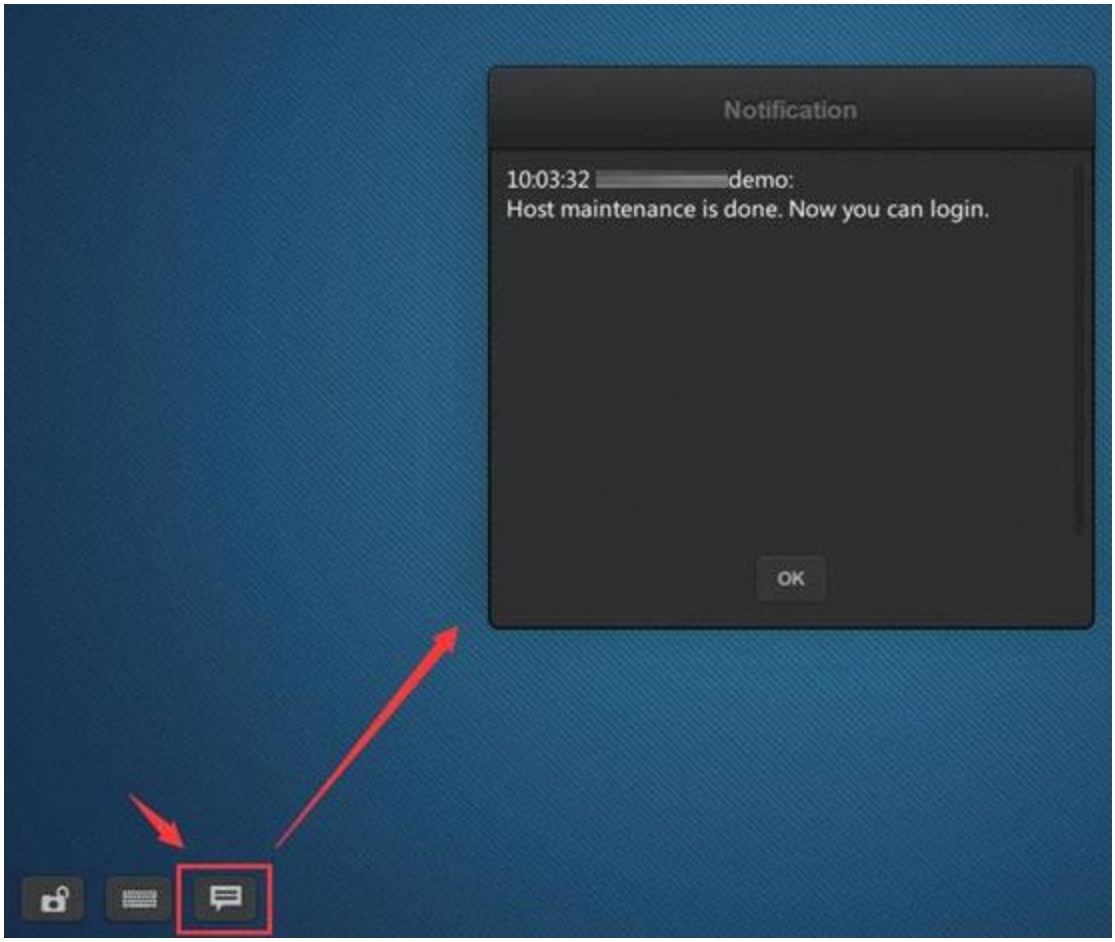
- **Keyboard Layout Settings:** to set up the language of the keyboard input; 111 languages are available, defaulted US; if the option “Apply to desktop (Windows)” is not selected, the setting applies to input on the device interface only.

- **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.



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.
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, e.g.: BlackBox S100;
- **Device Name:** the name of the device; default name is S100 - (last 8 serials number); 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.
- **Upgradable to:** the latest version of device firmware that is available in the network. Click the download button to update.

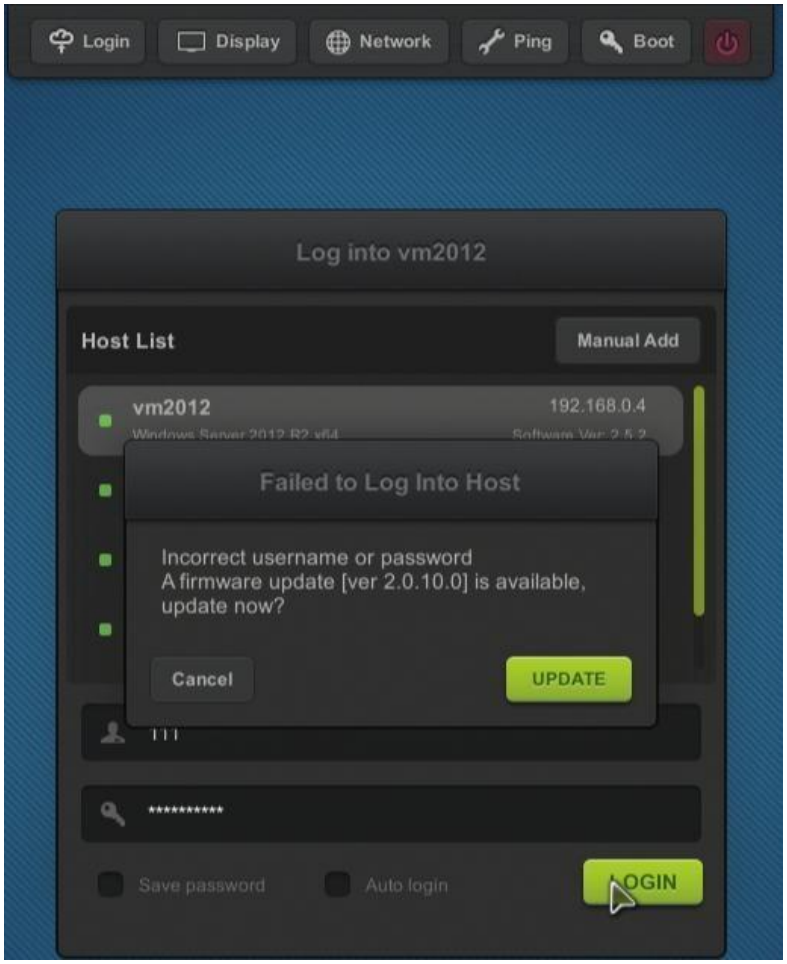
4.6 Firmware Update

It is always recommended to use the latest available version of firmware on your BlackBox 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.

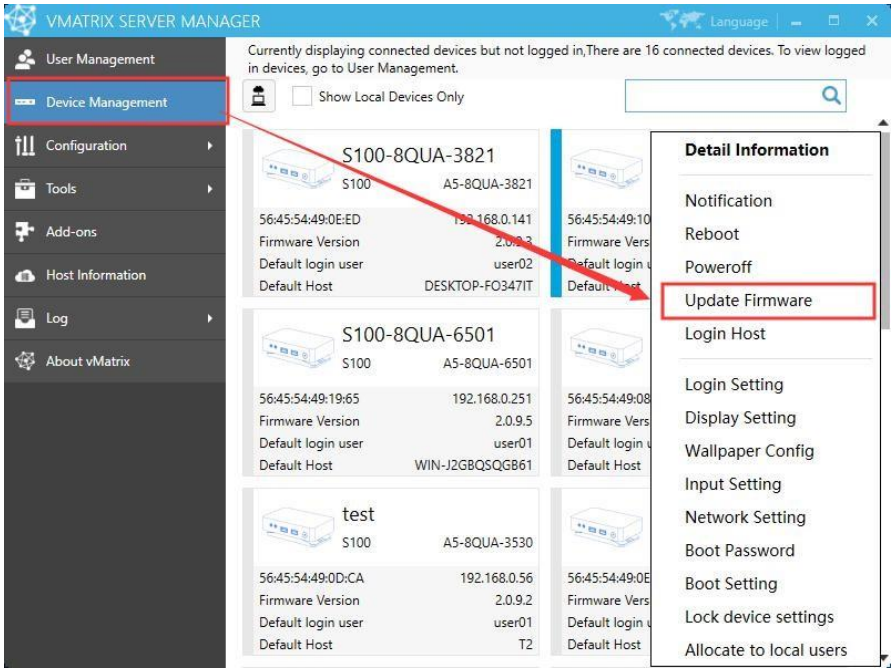
There are three ways for you to update the firmware:

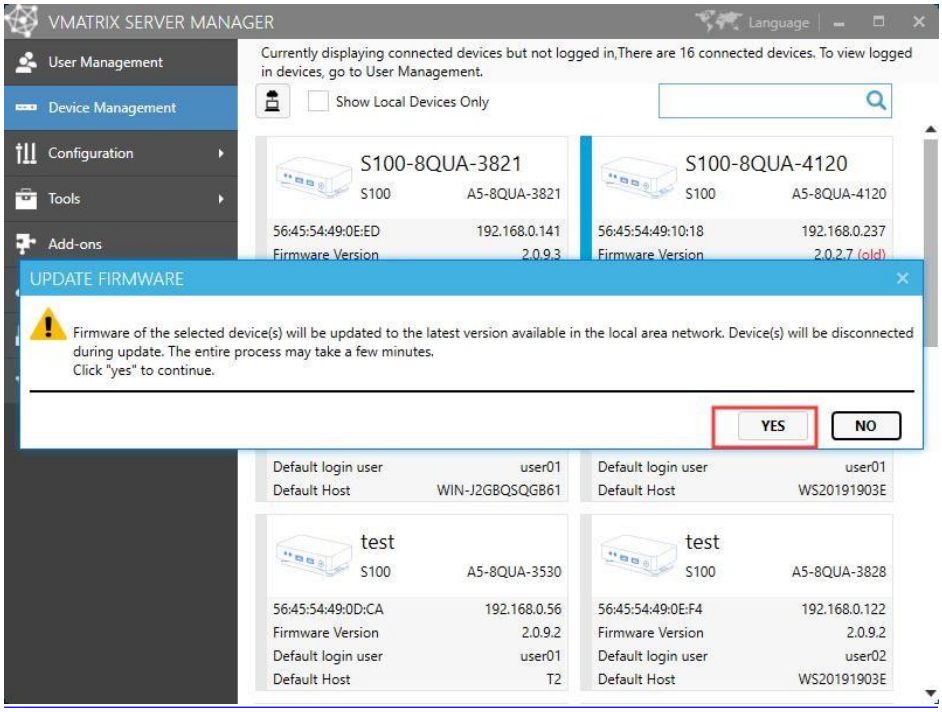
1) Click the download icon at the right bottom screen to update to the latest version available in the network.

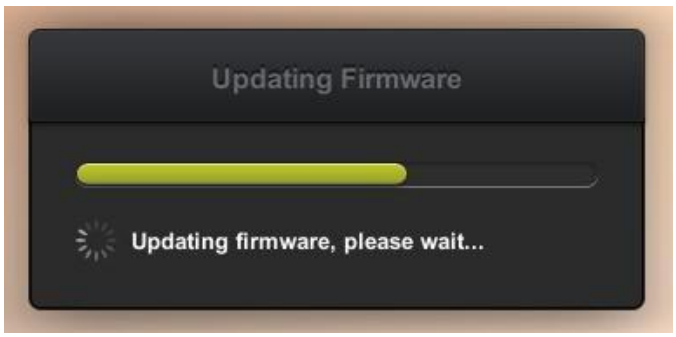
2) Select a host and purposely enter incorrect user name and password. Simply click the “UPDATE” button on the pop-up window to update with the new firmware (if there is) included in the vMatrix Server Manager on the host.



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
Configuration
Tools
Add-ons
Host Information
Log
About vMatrix
Currently displaying connected devices but not logged in,There are 16 connected devices. To view logged in devices, go to User Management.
Show Local Devices Only
S100-8QUA-3821
S100
A5-8QUA-3821
56:45:54:49:0E:ED
Firmware Version
Default login user
user02
Default Host
DESKTOP-FO347IT
S100-8QUA-6501
S100
A5-8QUA-6501
56:45:54:49:19:65
192.168.0.251
Firmware Version
2.0.9.5
Default login user
user01
Default Host
WIN-J2GBQSQGB61
test
S100
A5-8QUA-3530
56:45:54:49:0D:CA
192.168.0.56
Firmware Version
2.0.9.2
Default login user
user01
Default Host
T2
Detail Information
Notification
Reboot
Poweroff
Update Firmware
Login Host
Login Setting
Display Setting
Wallpaper Config
Input Setting
Network Setting
Boot Password
Boot Setting
Lock device settings
Allocate to local users





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. 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.

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: there is no "shutdown" option for terminal users to shut down the host system. 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.

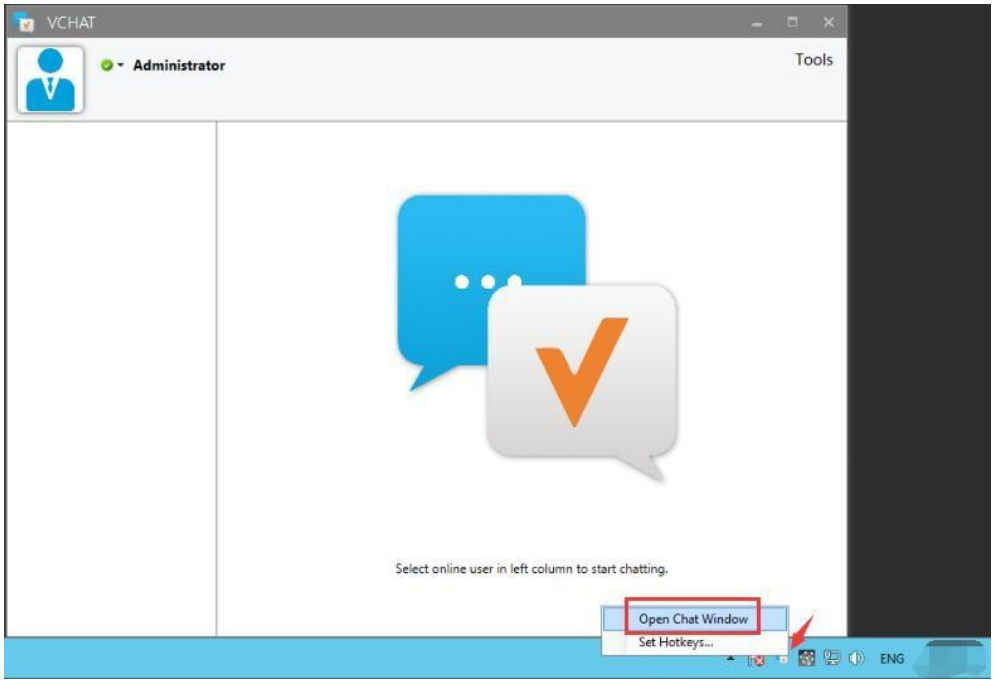
4.9 Use USB Devices

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

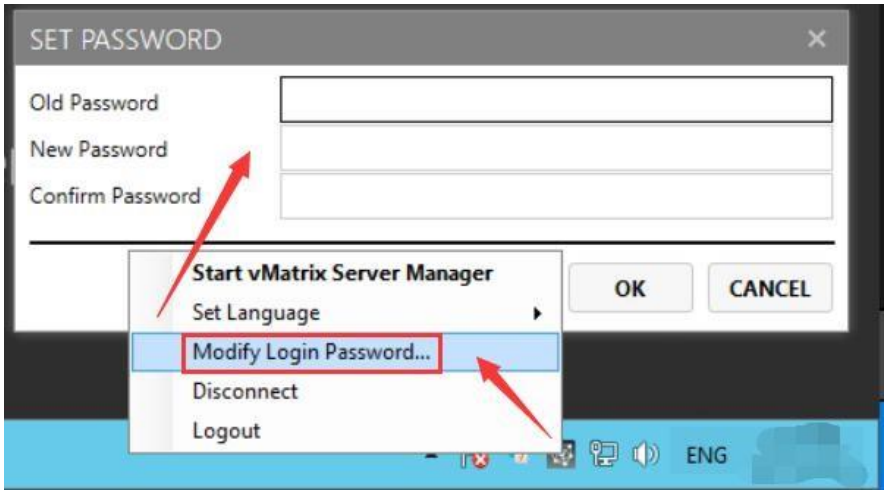
4.10.1 vChat Internal Messenger

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".



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.

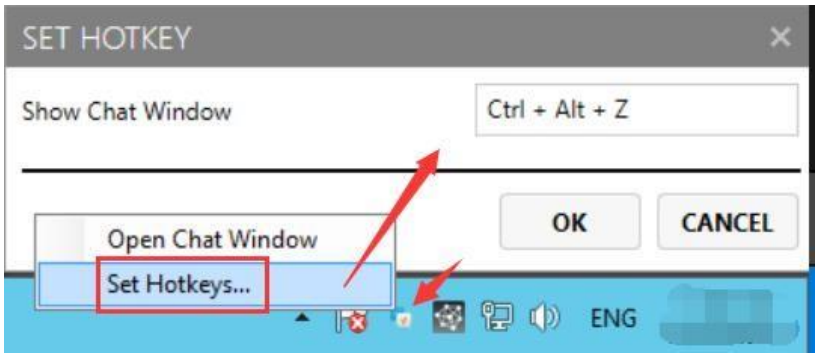


4.10.3 Set Language

This is to set language for displaying messages of the BlackBox 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.

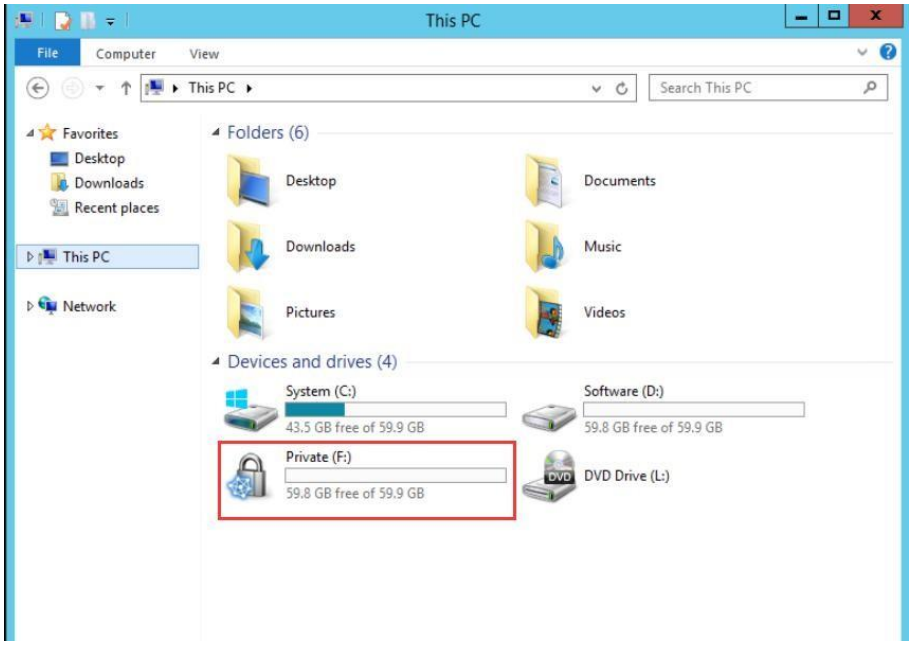
4.10.4 Set Hotkeys ...

This is to set hotkey to open chat window. To ensure the hotkey works, do not use the same combination of keys for other applications.



4.10.5 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.



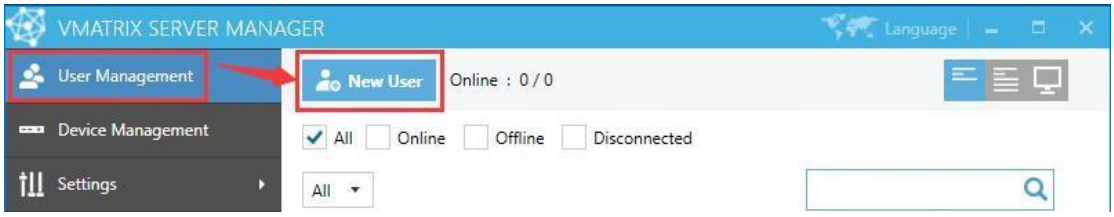
Note: By default, the files on the user's desktop are stored in the C drive. It is recommended that users store personal files in Private Drive to prevent the issue of insufficient space of the C drive.

Chapter 5. Using vMatrix Server Manager

5.1 User Management

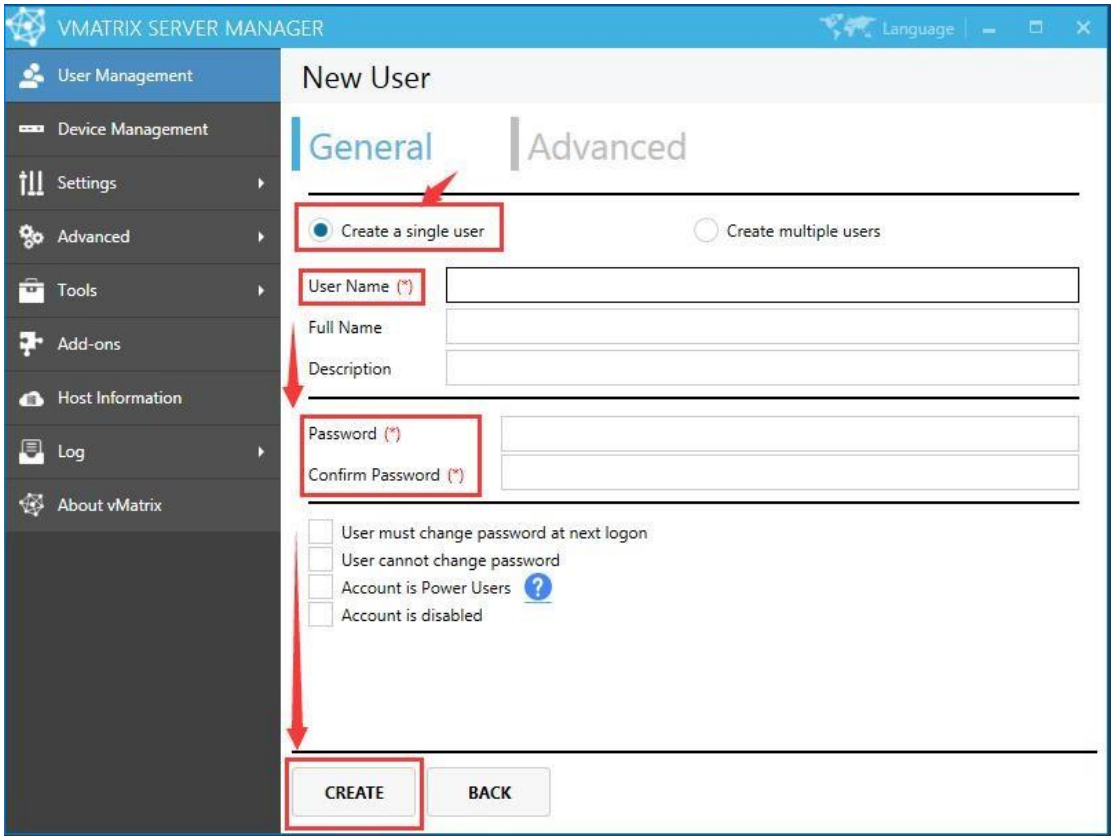
5.1.1 New User Creation

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



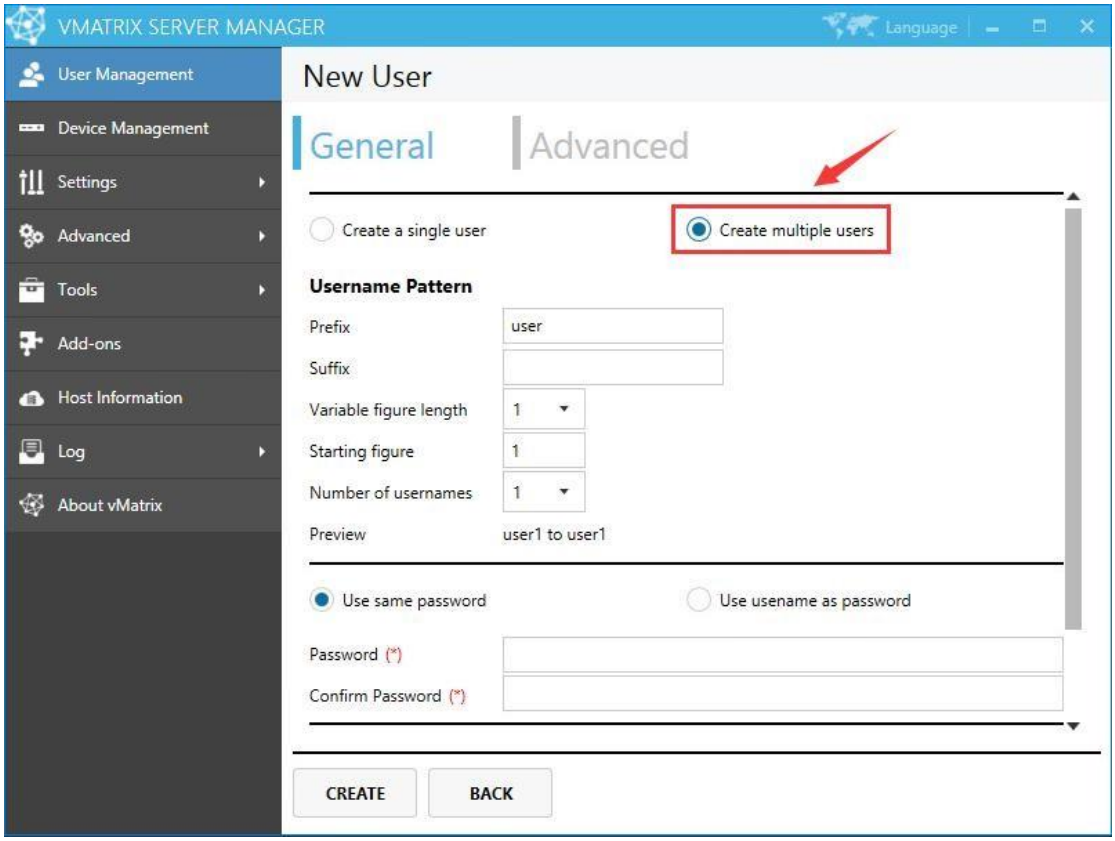
- Single user creation (defaulted)

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



- Multiple user creation

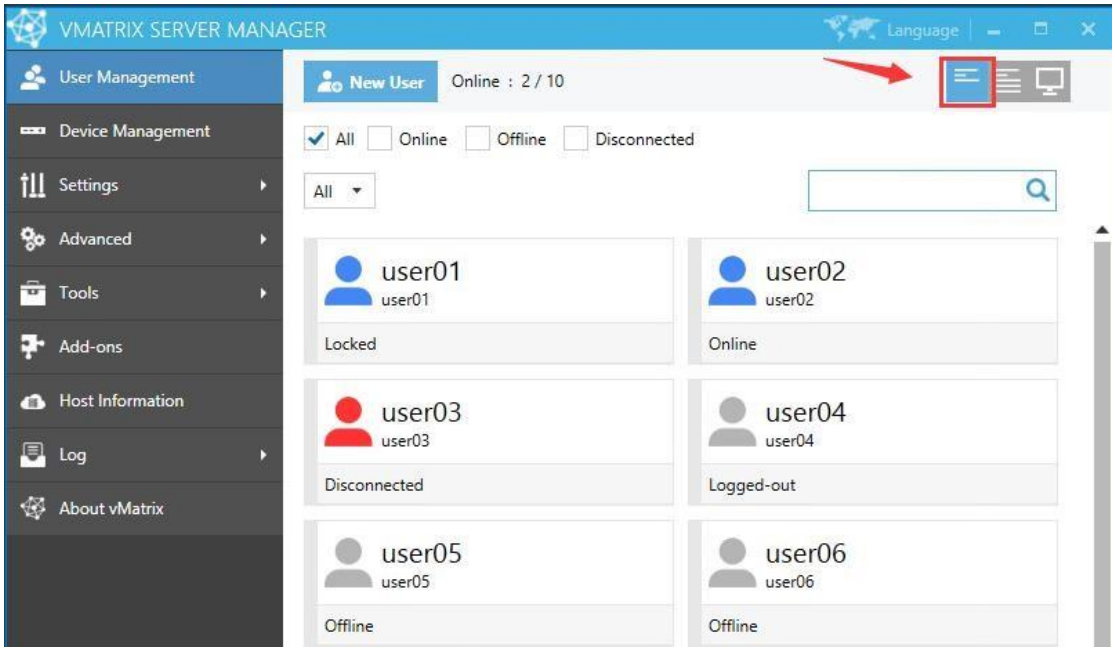
To create multiple users at a time, select “Create multiple users” and then you will be given a few more fields.



- **Prefix:** prefix that all user names start with; defaulted "user"; e.g.: user1, sales1, *student*1, *teacher*1…
- **Suffix:** suffix that all user names end with; defaulted empty; e.g.: user1fl1, user1fl2, user1fl3…
- **Variable figure length:** the number of the variable figure; defaulted "1"; e.g.: user1fl, user01fl1, user001fl1…
- **Starting figure:** the number that the variable figure start with; defaulted "1"; e.g.: user4fl1, user5fl1, user6fl1…
- **Number of usernames:** the number of users to be created; defaulted "1"; e.g.: user1fl1; user1fl1, user2fl1; user1, user2fl1, user3fl1…
- **Use the same password:** all users use the same password; defaulted; e.g.: user1, user1, user1.
- **Use username as password:** all users use their use name as the password; e.g.: user1, user2, user3.

User

5.1.2 Status View

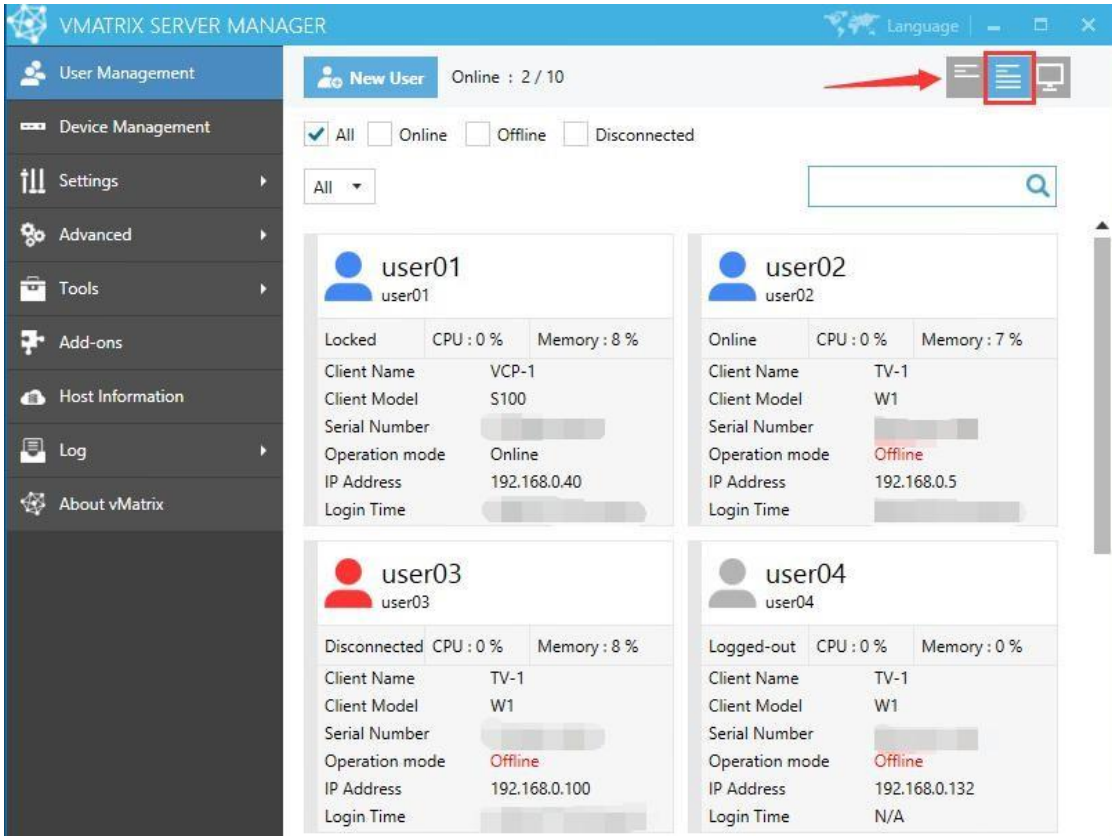


On this selection, you can view CPU and Memory consumption for each user and their status including:

- **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.

User

5.1.3 Information View



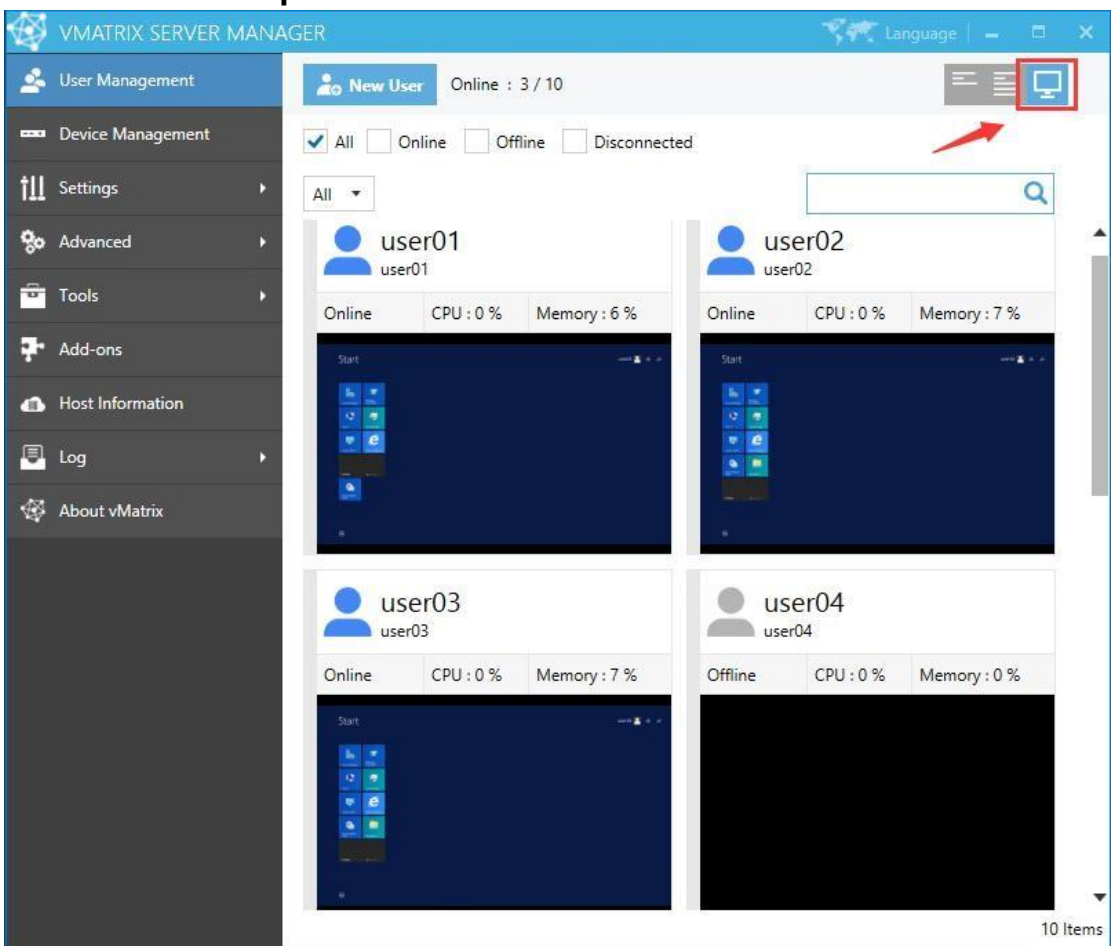
On this selection, you can view CPU & Memory consumption and status for each user and their device information including:

- **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.

User

- **Login Time:** the time when the user logged into this host.

5.1.4 Desktop View

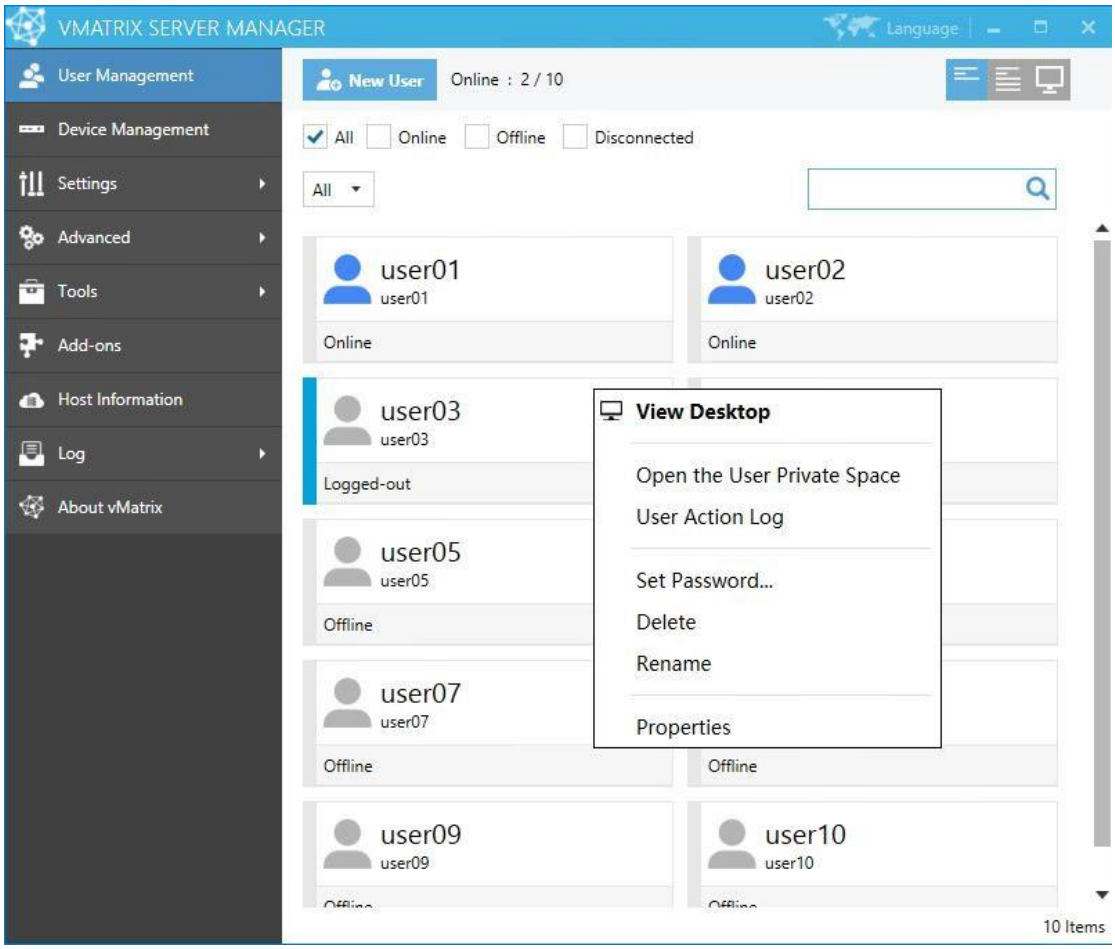


On this selection, you can view user's real time desktops in tiles.

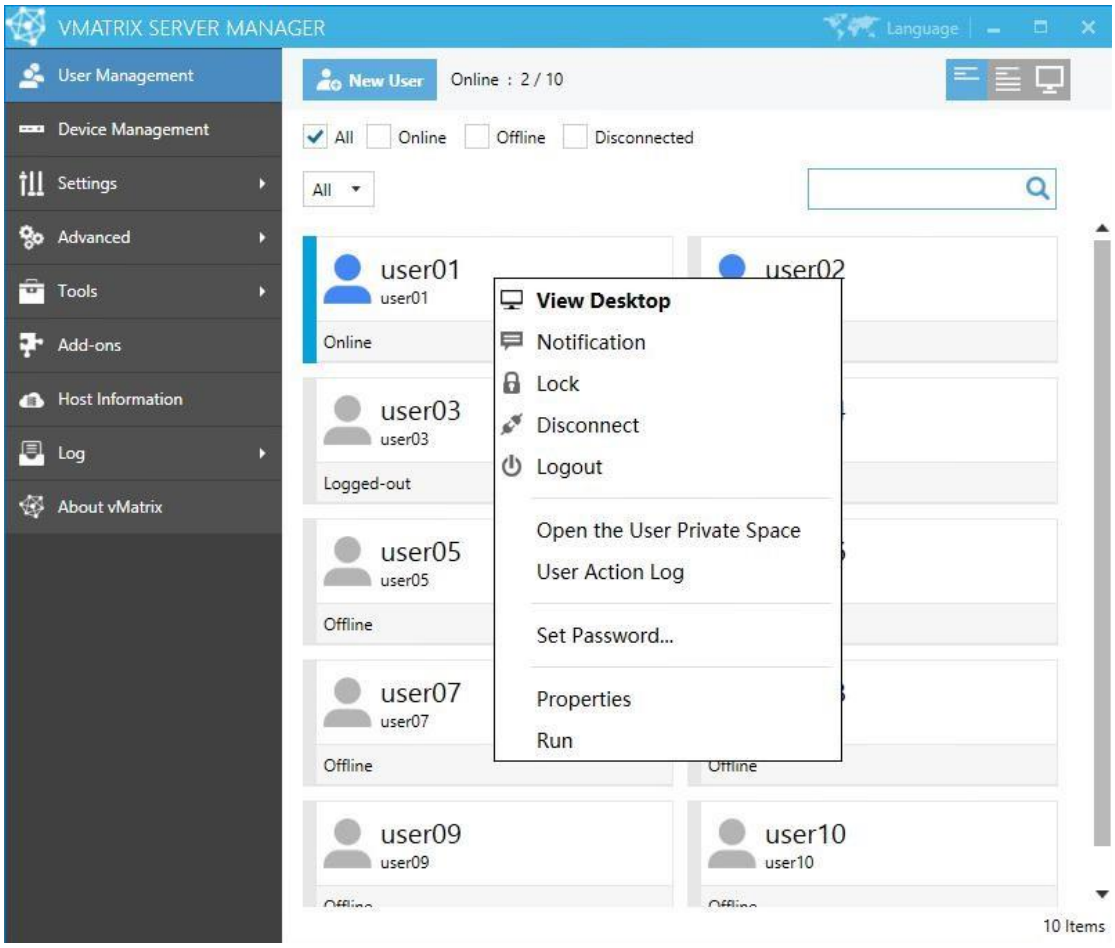
5.1.5 Right Click Menu

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.

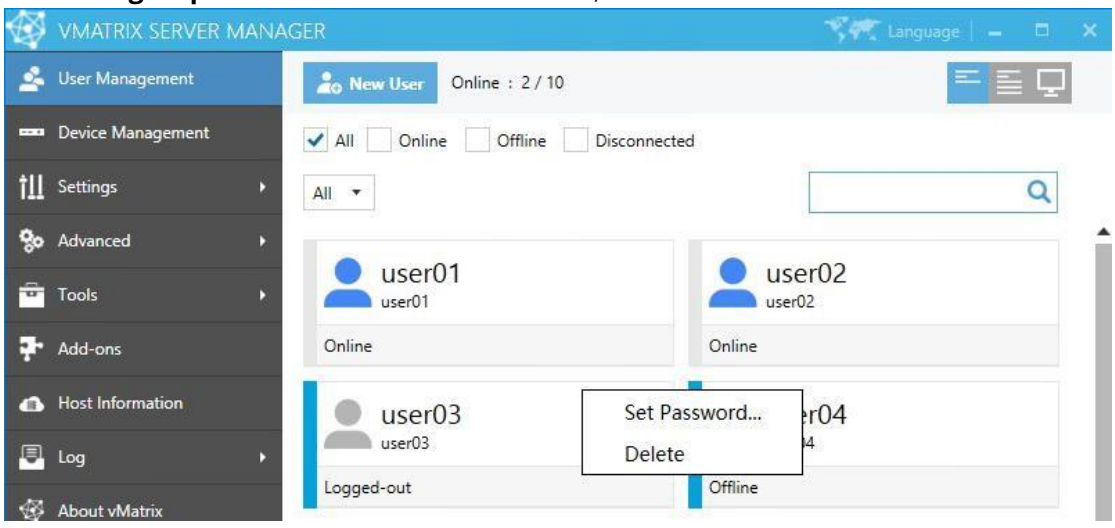
- **On a single offline user:** View Desktop,Open the User Private Space, User Action Log, Set Password..., Delete, Rename, Properties.



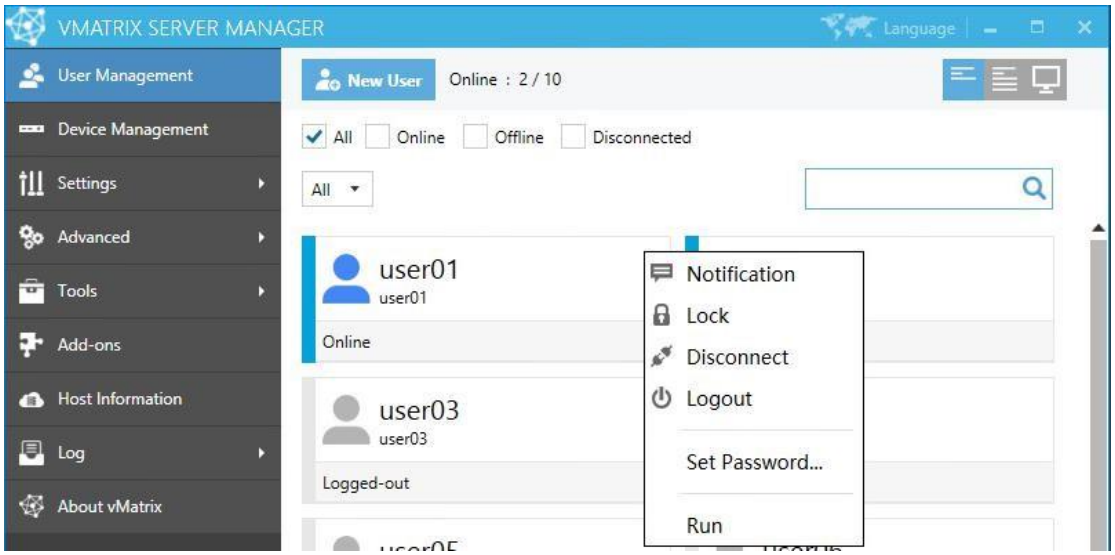
- **On a single online user: View Desktop,**Notification, Lock, Disconnect, Logout, Open the User Private Space, User Action Log, Set Password..., Rename, Properties.



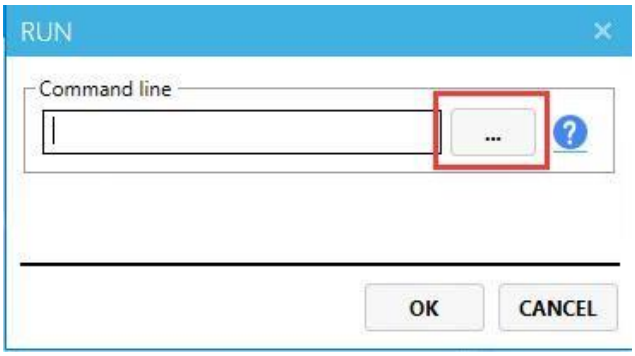
- **On a group of offline users:** Set Password, Delete.



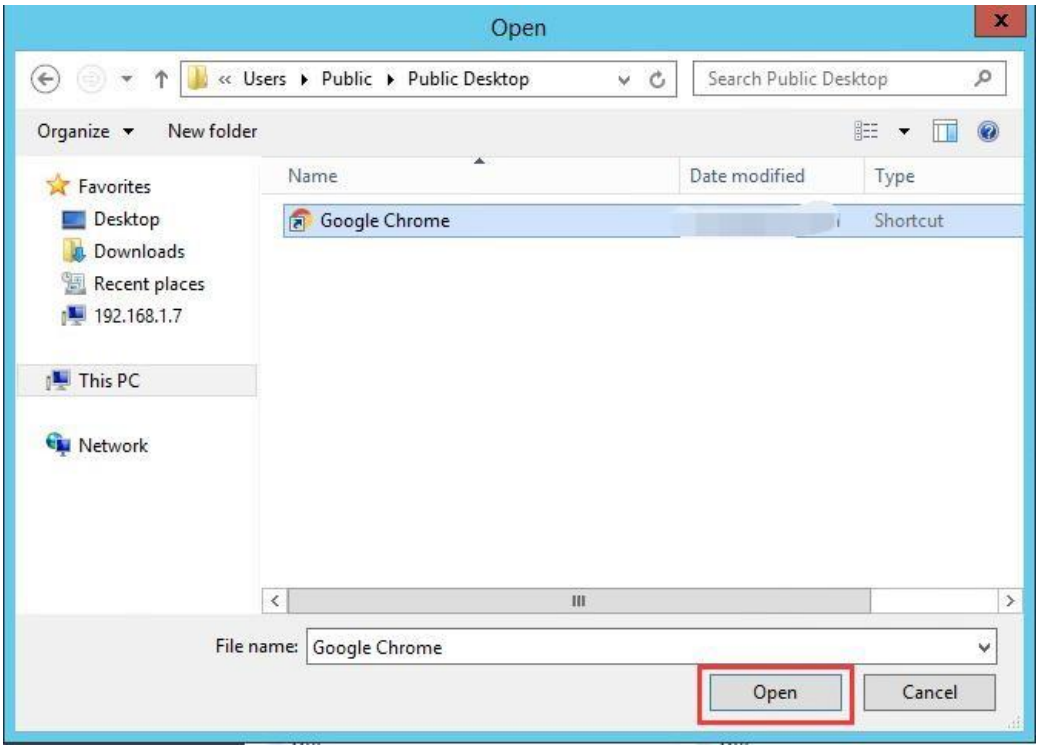
- **On a group of online users:** Notification, Lock, Disconnect, Logout, Set Password...



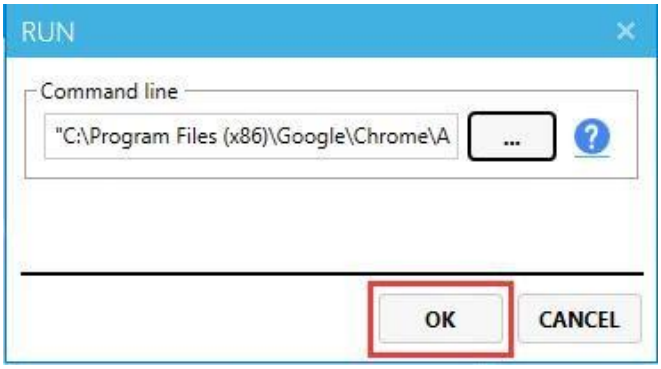
- **View Desktop:** Enter detailed information page of the user.
- **Notification:** to send a notification to the selected user in a small pop-up windows.
- **Lock:** to lock the selected user's desktop; the user's screen goes to system login page where password is required for re-login.
- **Disconnect:** to disconnect the selected user's session; the user session is till 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.
- **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.



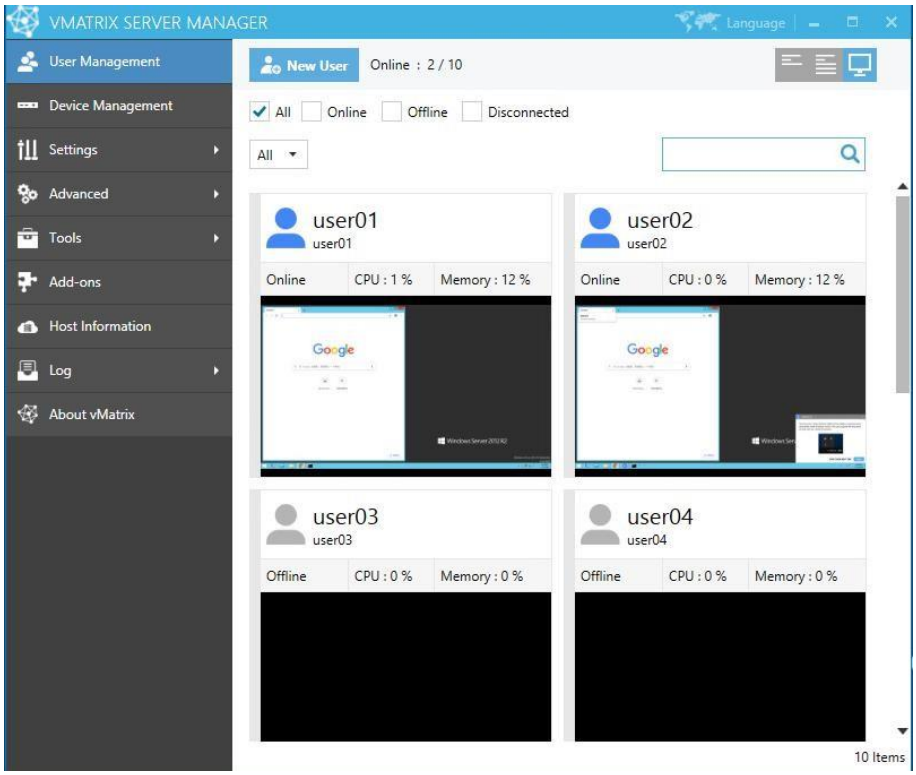
1) Select the program you want to run and click "Open".



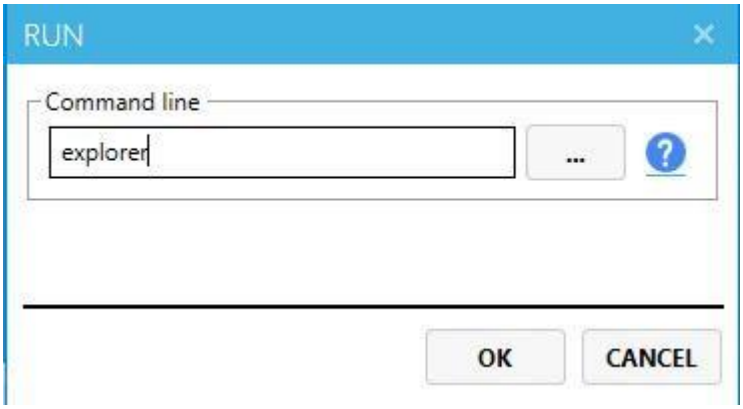
2) Click “OK”.



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



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

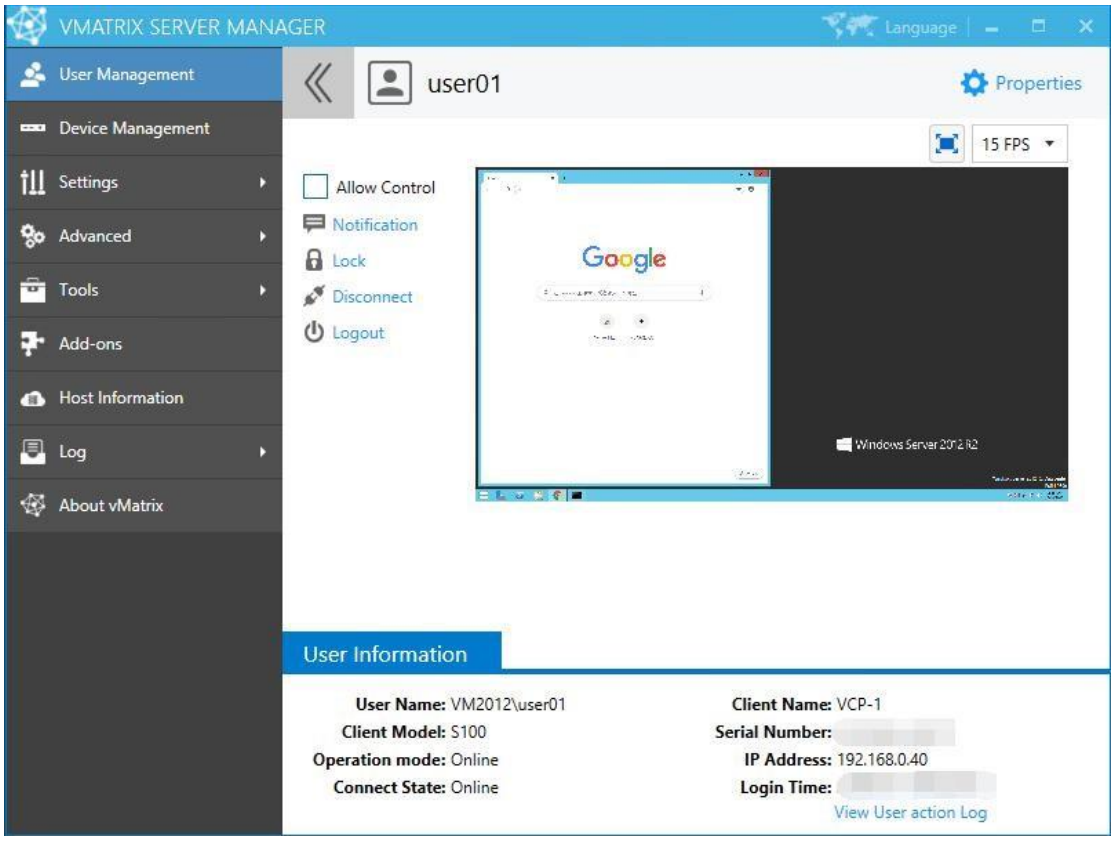


Notes:

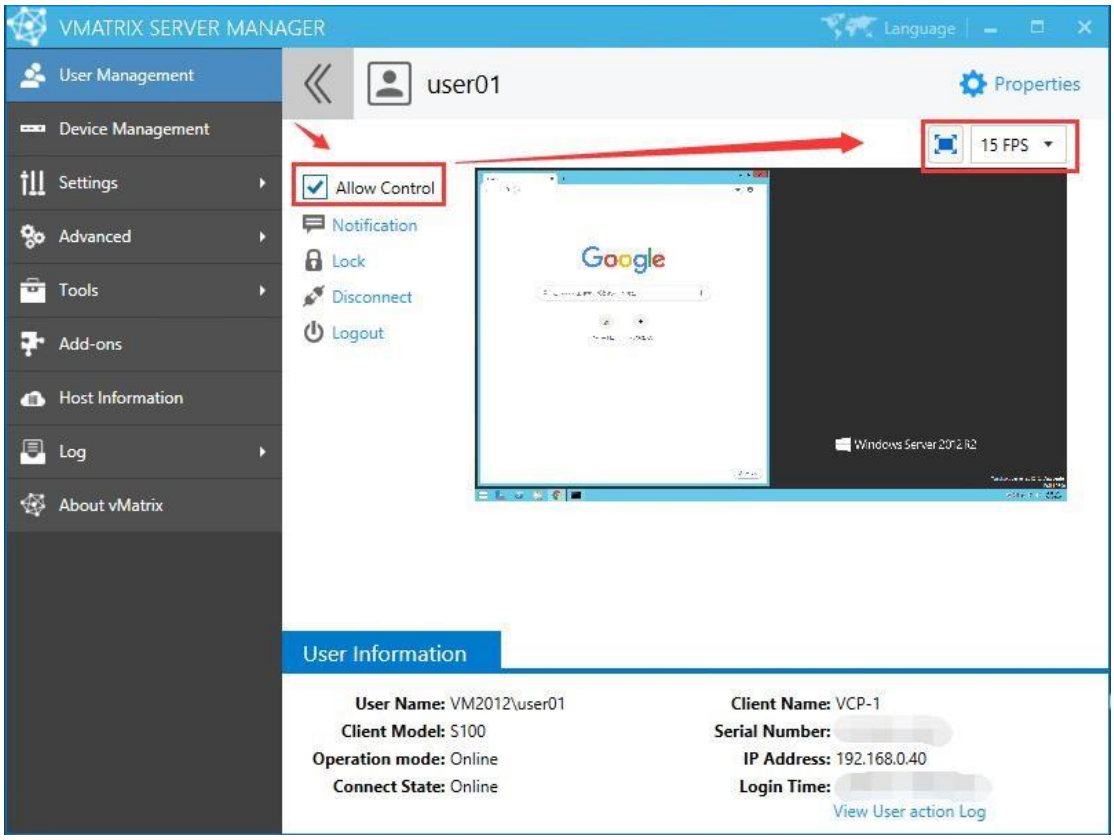
- Example of system command with parameters ping localhost -t
- Example of running a file in default program: C:\test.mp4
- Example of running a file in specific program: notepad.exe C:\test.txt
- If the path contains spaces, the path string must be enclosed in double quotes, example: "C:\Program Files\test.exe"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

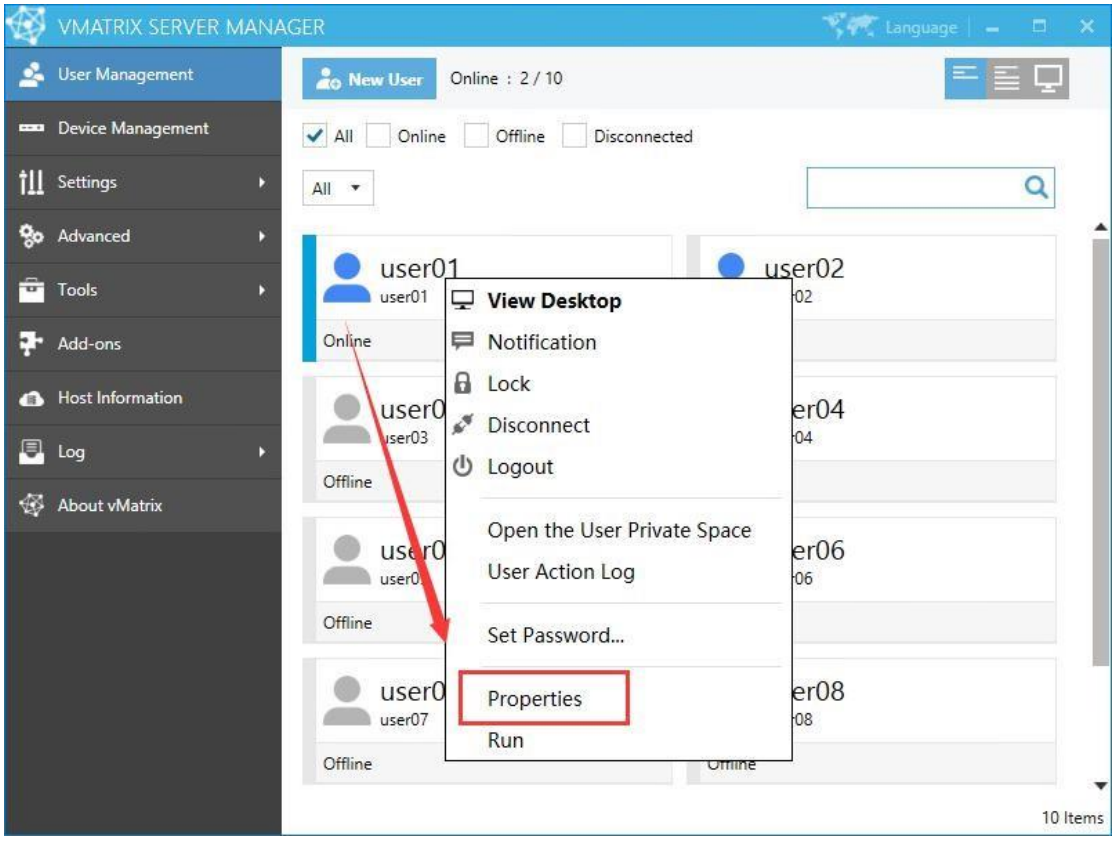


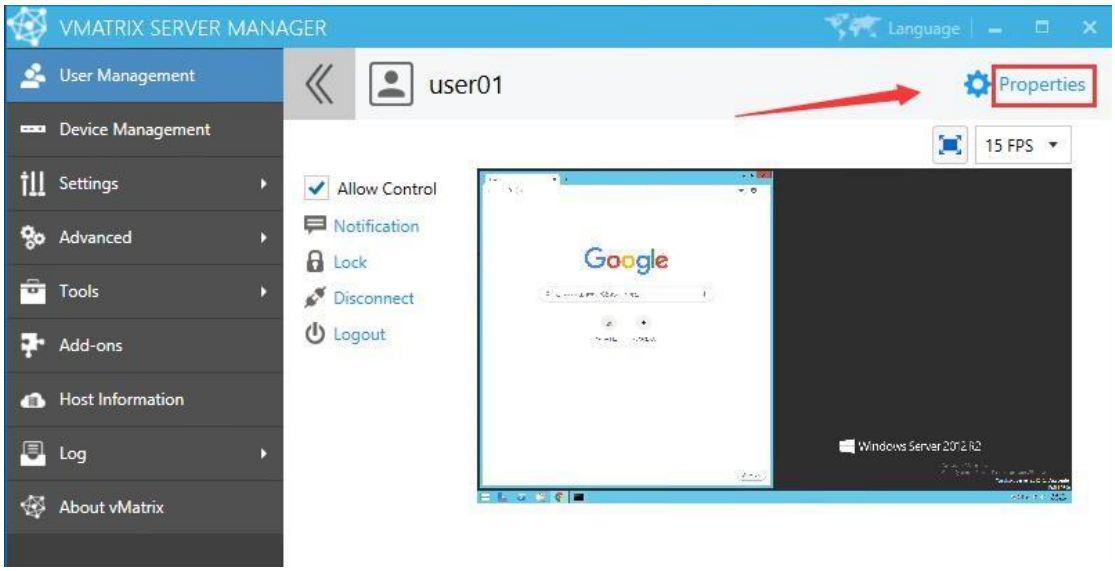
- **Allow Control:** if this option is selected, you can take control over the user's desktop.
- **Extend Icon:** click on this icon to extend the view the user's desktop in full screen. When entering full screen view, you can move the cursor to the right top corner to exit full screen view.
- **15FPS:** select the refresh rate from 5- 30FPS when you are viewing the desktop.
- **Properties:** to change the selected user's personal settings.


VMATRIX SERVER MANAGER
Language
User Management
Device Management
Settings
Advanced
Tools
Add-ons
Host Information
Log
About vMatrix
user01
Properties
15 FPS
Allow Control
Notification
Lock
Disconnect
Logout
Google
Windows Server 2012 R2
User Information
User Name: VM2012\user01
Client Model: S100
Operation mode: Online
Connect State: Online
Client Name: VCP-1
Serial Number:
IP Address: 192.168.0.40
Login Time:
View User action Log

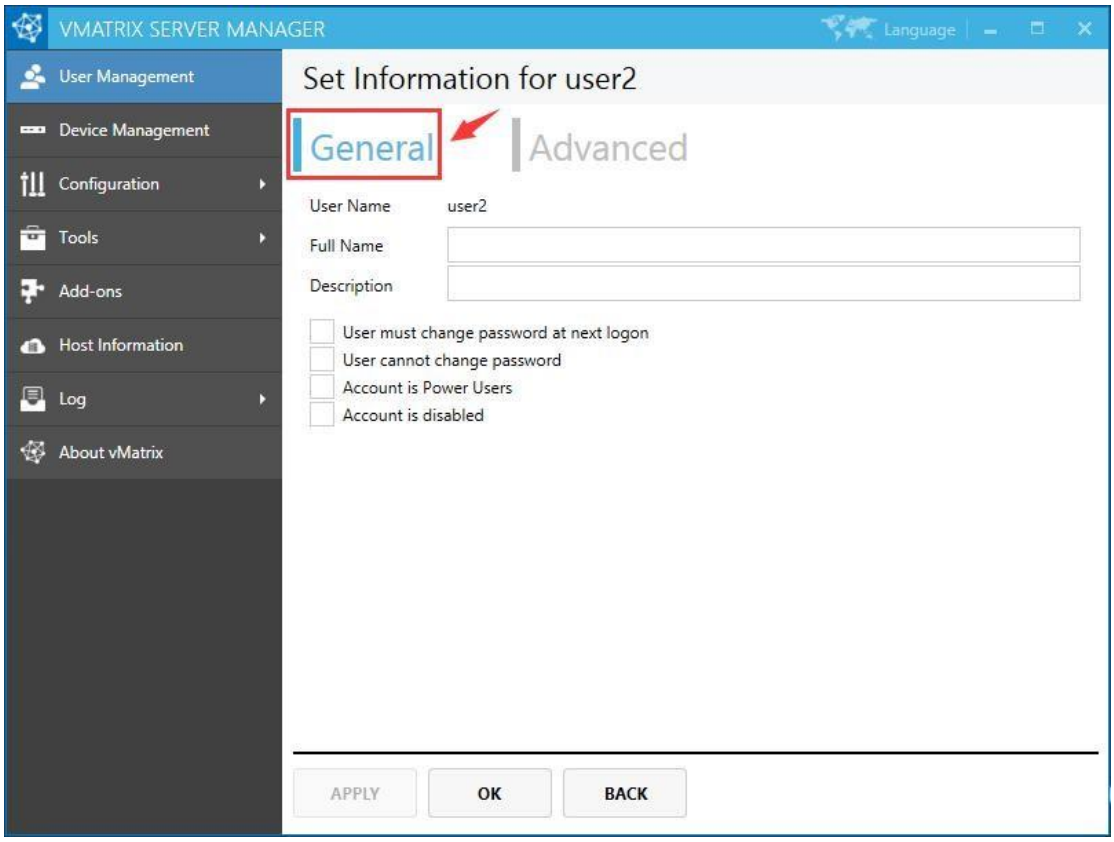
5.1.7 Personal User Settings

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.



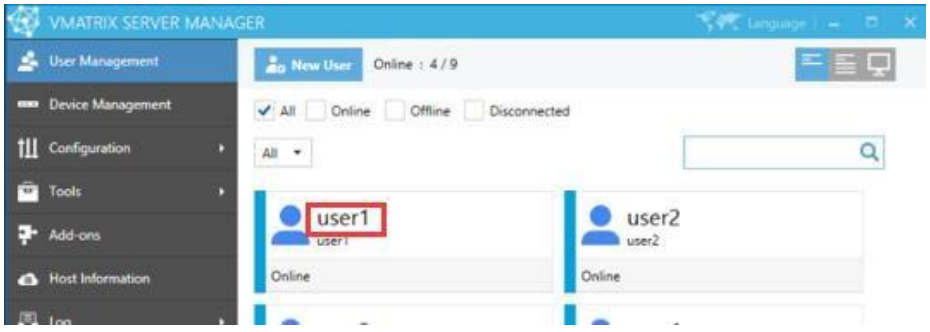


❖ **General Settings:**



- **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.

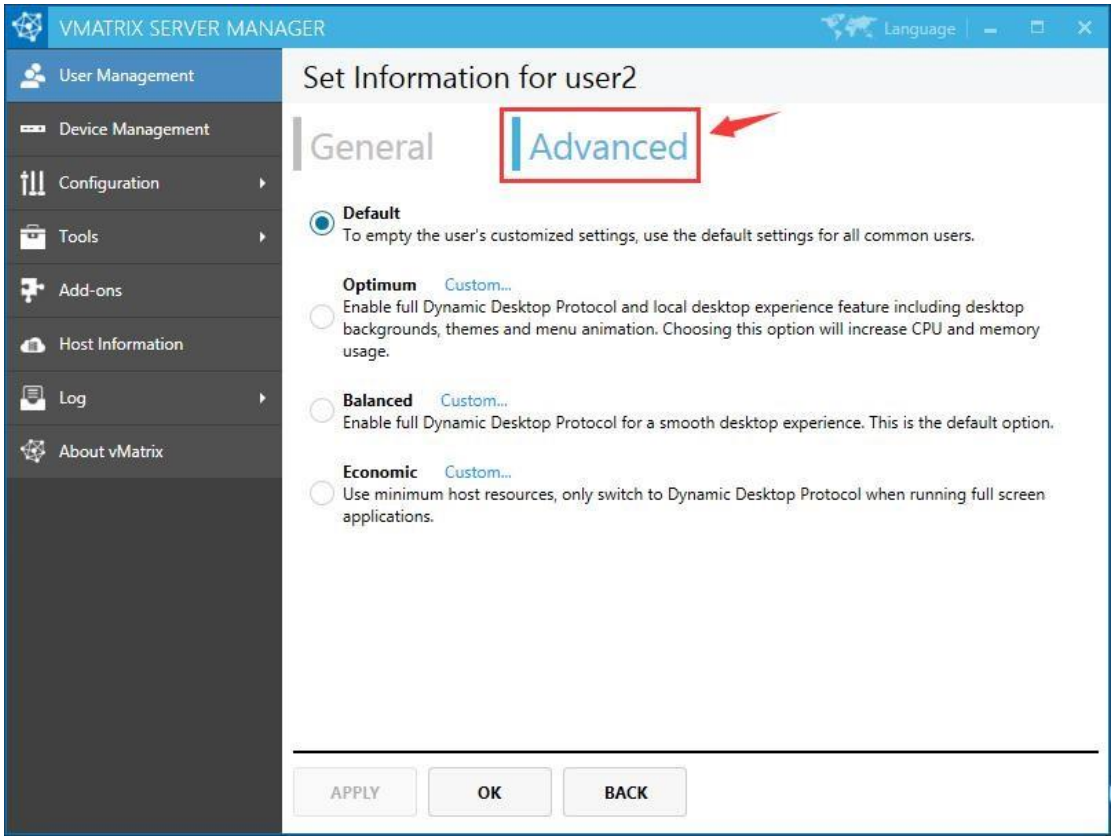
- **User must change password at next logon:** selecting this option will force the user to change password at next logon.

- **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.

❖ Advanced Settings:



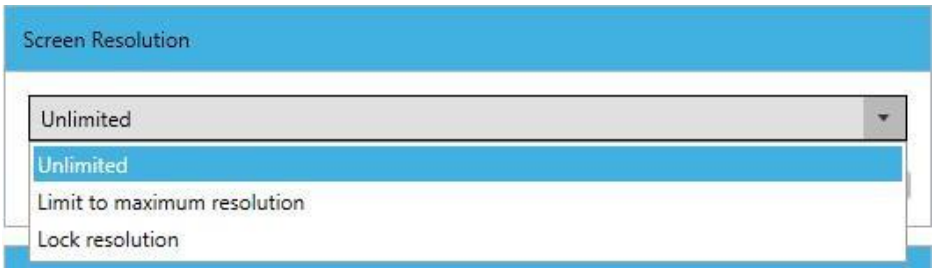
Advanced settings allows you customize user settings. Changes will take effect at user's next login. Advance settings include:

- **Desktop Resolution:**

- **Unlimited:** the user can use all device supported resolution.

- **Limit to maximum resolution:** limit user to use a selected resolution or resolutions below.

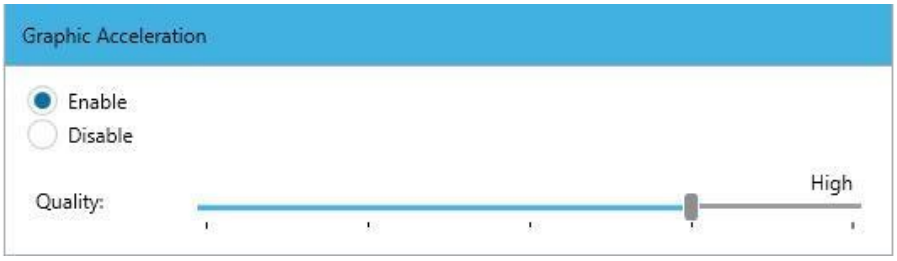
- **Lock resolution:** lock resolution to the only selected resolution.



- **Graphic Acceleration:**

  - **Enable:** (defaulted and recommended) to enable the use of BlackBox Dynamic Desktop Protocol (DDP) for a smoother desktop experience. Enabling this option will also allow you to select display quality from lowest, low, medium, high, to highest. Default display quality is high. The higher display quality is selected, the higher CPU and network bandwidth will be consumed.

  - **Disable:** to disable the use of DDP and use the system built-in Remote Desktop Protocol (RDP) for image transmission. If this option is selected, the user will be given a less desktop responsive experience and video play in full screen or large window is not watchable.

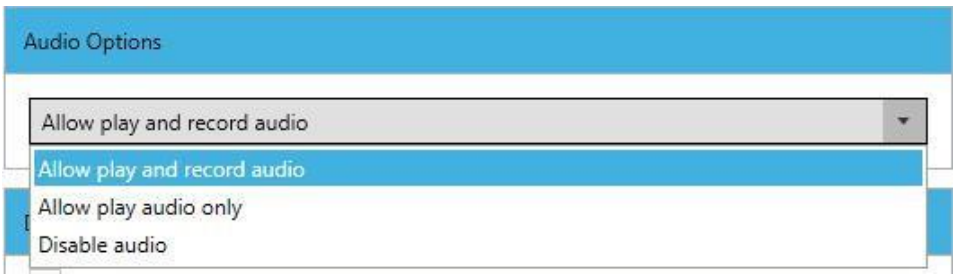


- **Audio:**

  - **Allow play and record audio:** to enable the user to play and record audio on the device. (default)

  - **Allow play audio only:** to enable the user to play but not record audio on the device.

  - **Disable audio:** to disable the user to play or record audio on the device.



- **Desktop Options:**

- **Enable desktop wallpapers:** to enable the user to change background desktop wallpapers.
- **Enable user interface themes:** to enable the user to switch interface themes.
- **Show window contents while dragging:** to enable the user to see contents within window while dragging.
- **Enable menu animations:** to enable the user to see menu animation while opening a menu.

Note: Desktop Options are defaulted disabled. Enabling these options will cause higher CPU and network bandwidth consumption.

- **USB Options:** enabled (checked) by default; when disabled (unchecked), only input devices such as mouse and keyboard are allowed.
- **Enable USB Printers:** check to allow the user to use USB printers.
- **Enable USB Storage Devices:** check to allow the user to use USB storage devices like U disk and portable hard drive.
- **Enable other remote USB devices:** check to allow the user to use USB devices except printers and storage devices.

- **After the user login run the program:**
- **checked:** to enable this user session to auto run a specific installed program after user login without manual operation. When this option is enabled, the user is only allowed to run the designated program rather than the entire desktop session. If the

user close the program, the session will be terminated as well. This function is often used when the terminal device by this user is configured to be auto login after powered on. To enable this function, check the option and then enter the directory or click “BROWSE...” to specify an installed program by following this format: program path+ space+ file path, e.g. “C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.exe D:\123.doc”.

- **Unchecked:** (defaulted) to go to the user’s desktop after login.

- **Other Options (Chat Function):**

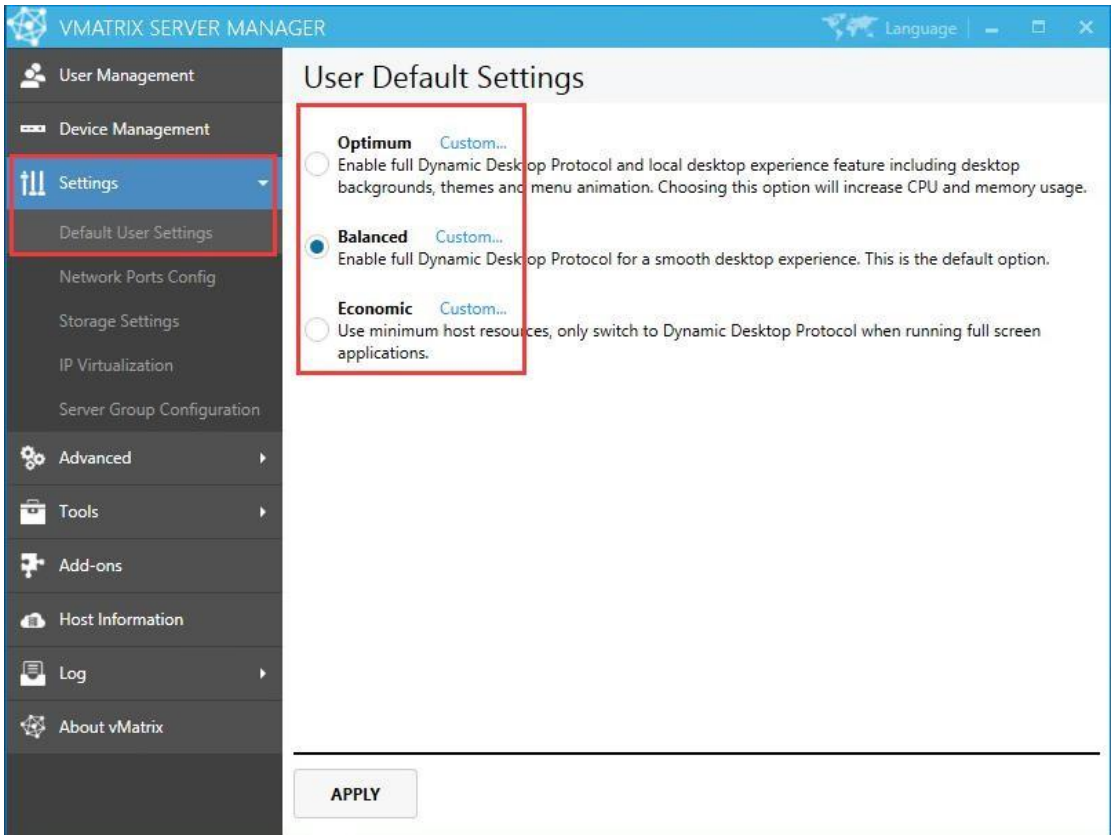
- **checked:** (defaulted) to enable the user to use the Chat Tool for communication with other login users.

- **Unchecked:** to disable the user to use the Chat Tool.

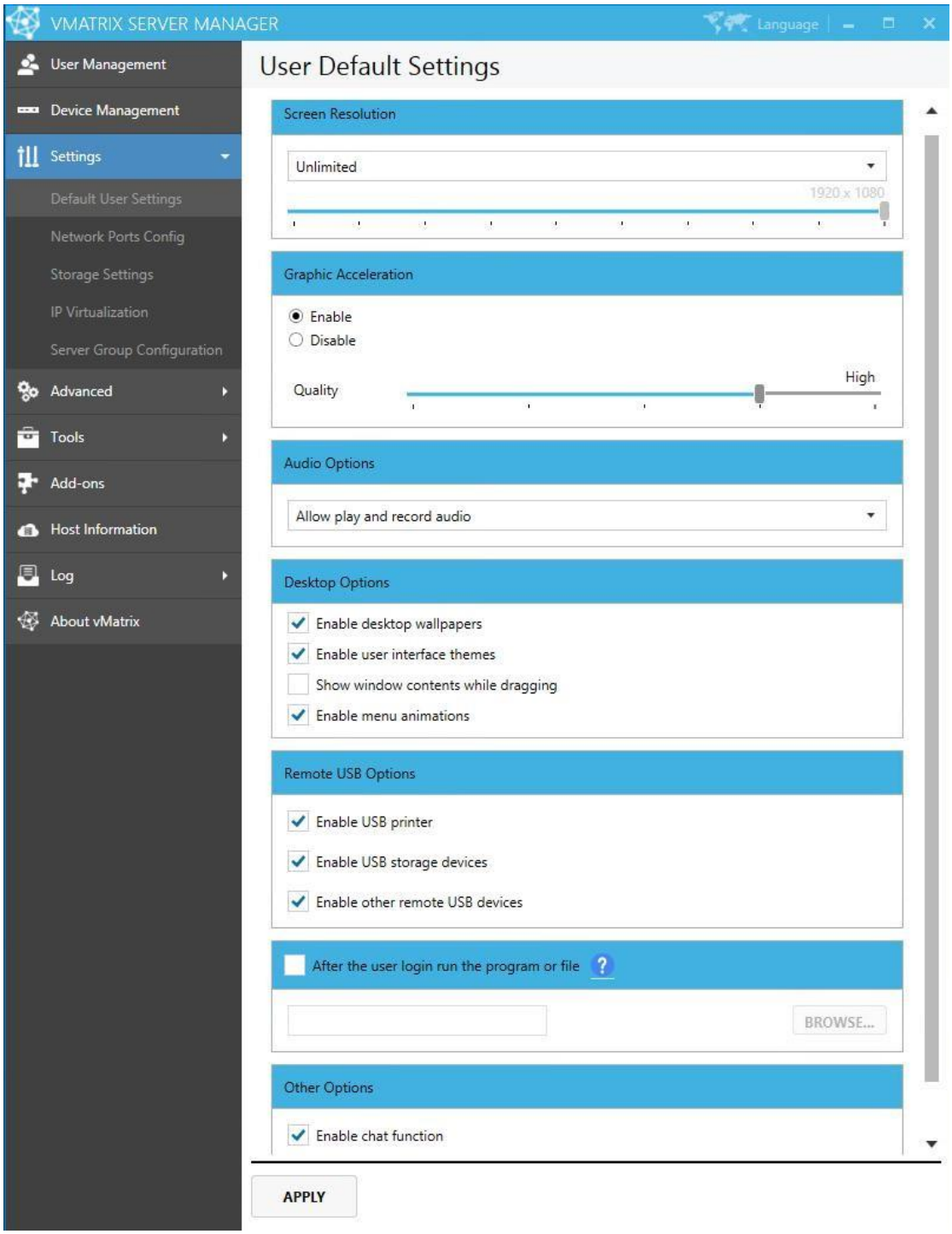
RESET TO DEFAULT SETTINGS: click to reset the current settings to default.

- **Default:**

This option uses the global settings for all users which can be configured at Configuration -> Default User Settings.



- **Optimum:**
  - **Desktop Resolution:** Unlimited
  - **Graphic Acceleration:** Enable, High
  - **Audio:** Allow play and record audio
  - **Desktop Options:** 1st, 2nd and 4th options checked
  - **USB Options**: checked
  - **After the user login run the program:** unchecked
  - **Other Options (Chat Function):** checked



- **Balanced:**

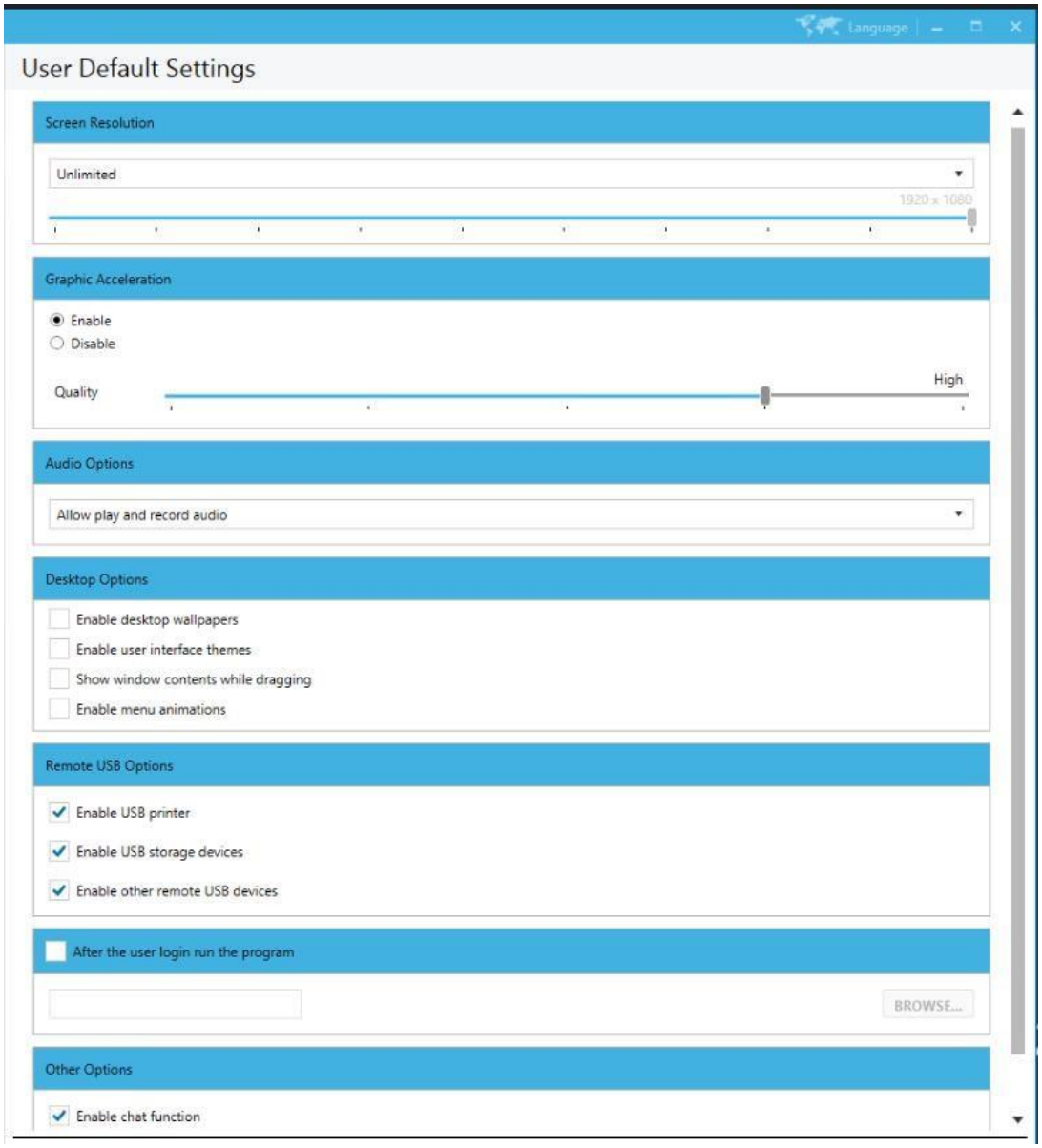
■ **Desktop Resolution:** Unlimited

■ **Graphic Acceleration:** Enable, High

■ **Audio:** Allow play and record audio

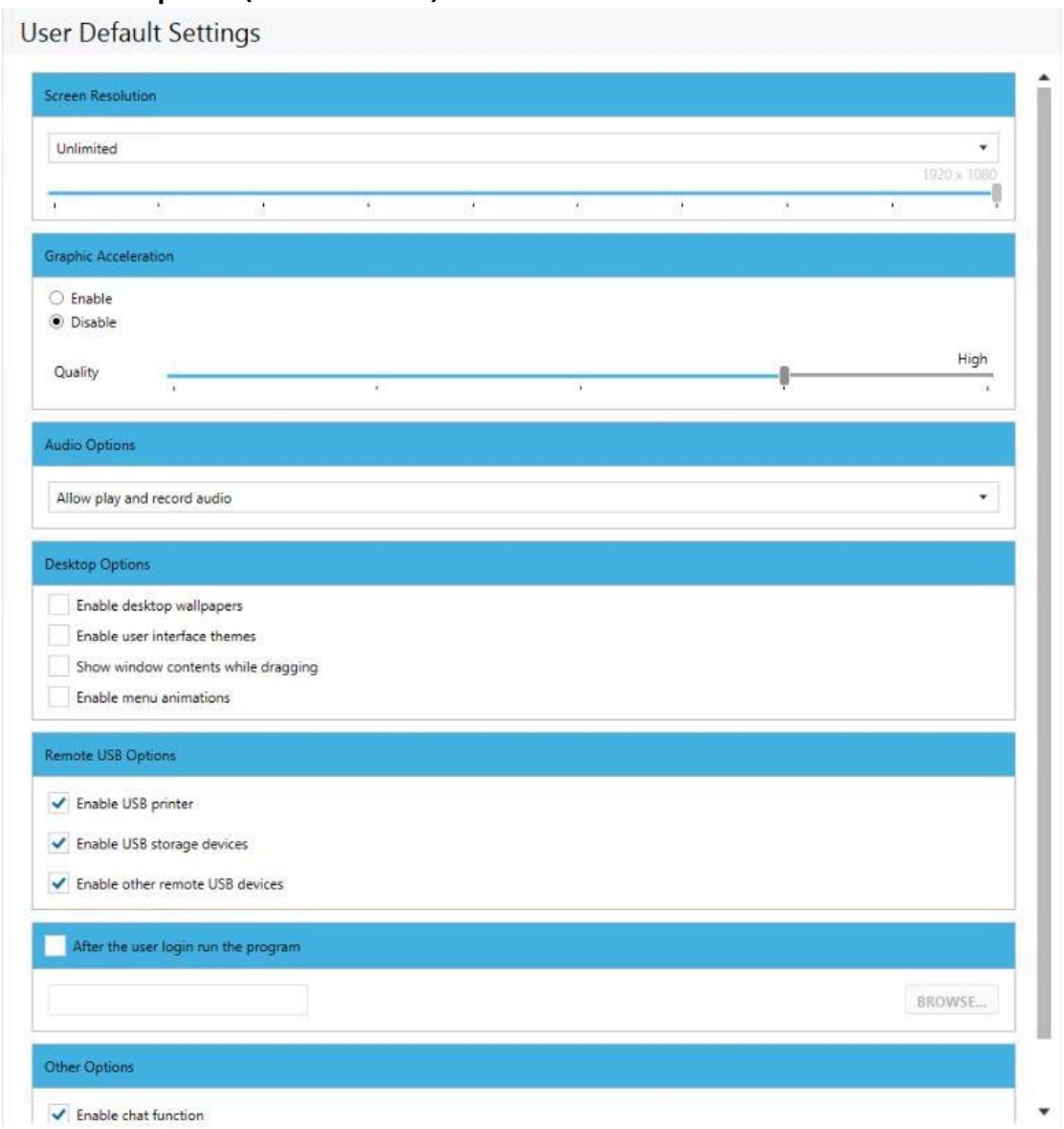
■ **Desktop Options:** all options unchecked ■ **USB Options:** checked

- **After the user login run the program:** unchecked
- **Other Options (Chat Function):** checked



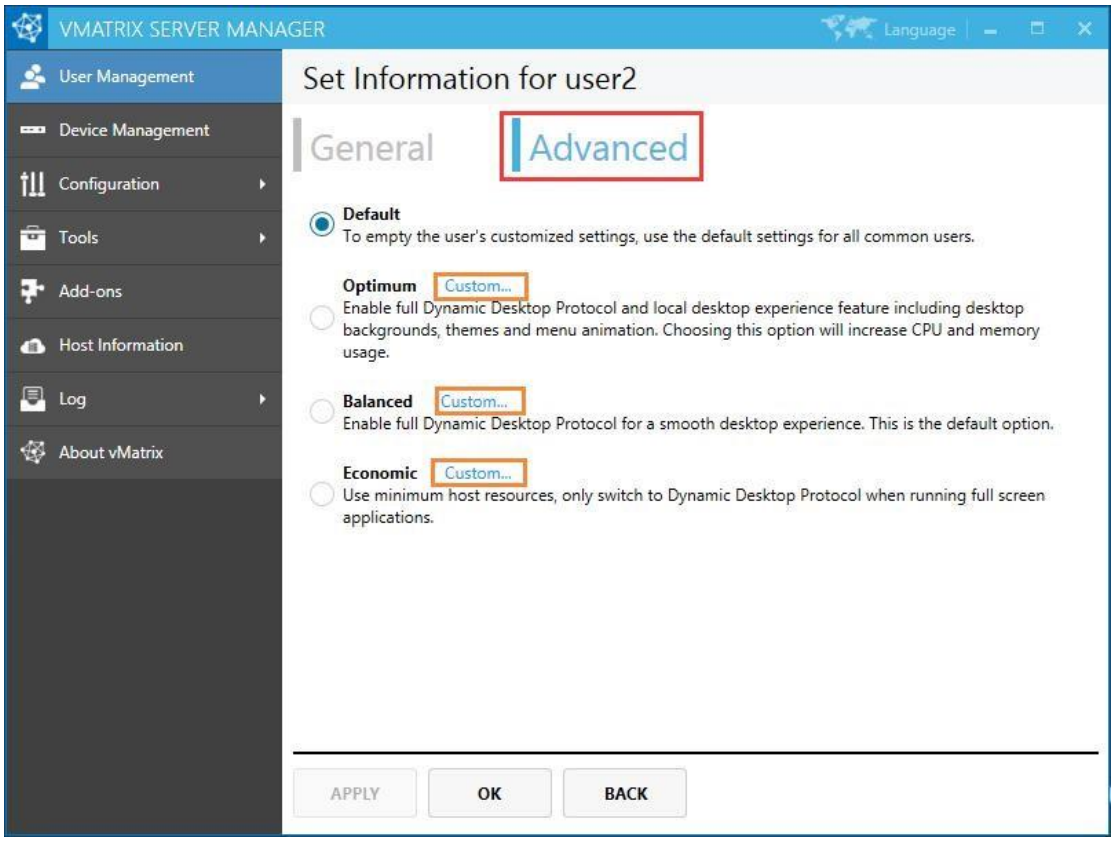
- **Economic:**
- **Desktop Resolution:** Unlimited
- **Graphic Acceleration:** Disable
- **Audio:** Allow play and record audio
- **Desktop Options:** all options unchecked
- **USB Options:** checked

- **After the user login run the program:** unchecked
- **Other Options (Chat Function):** checked



- **Custom...:**

This option allows you to customize user settings based on the 3 most used types of Optimum, Balanced, and Economic.

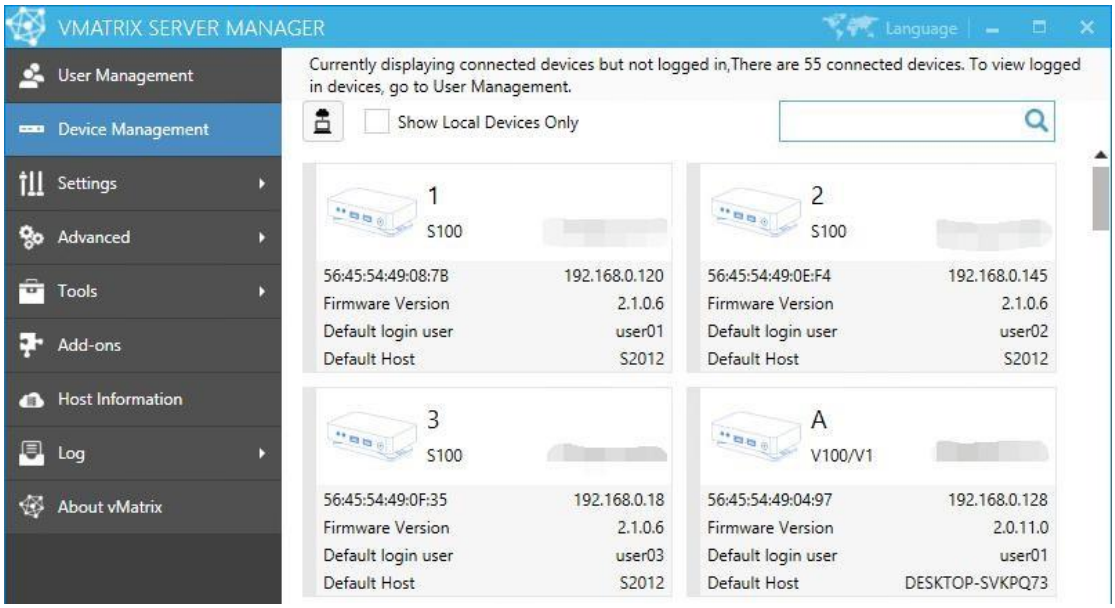

VMATRIX SERVER MANAGER
Language
User Management
Device Management
Configuration
Tools
Add-ons
Host Information
Log
About vMatrix
Set Information for user2
General
Advanced
Default
To empty the user's customized settings, use the default settings for all common users.
Optimum
Custom...
Enable full Dynamic Desktop Protocol and local desktop experience feature including desktop backgrounds, themes and menu animation. Choosing this option will increase CPU and memory usage.
Balanced
Custom...
Enable full Dynamic Desktop Protocol for a smooth desktop experience. This is the default option.
Economic
Custom...
Use minimum host resources, only switch to Dynamic Desktop Protocol when running full screen applications.
APPLY
OK
BACK

5.2 Device Management

5.2.1 Device Information View

On this page, you can view device information including:

- Device name: name of the device; defaulted model name + last 8 serial numbers.
- Device model: model of the device.
- Serial number：serial number of the device.
- Mac address: physical Mac address of the device.
- IP address: the IP address of the device in the LAN.
- Firmware version: firmware version that the device is using.
- Default login user: the saved user name for next login; it is the last login user name or the one customized at the Login Settings.



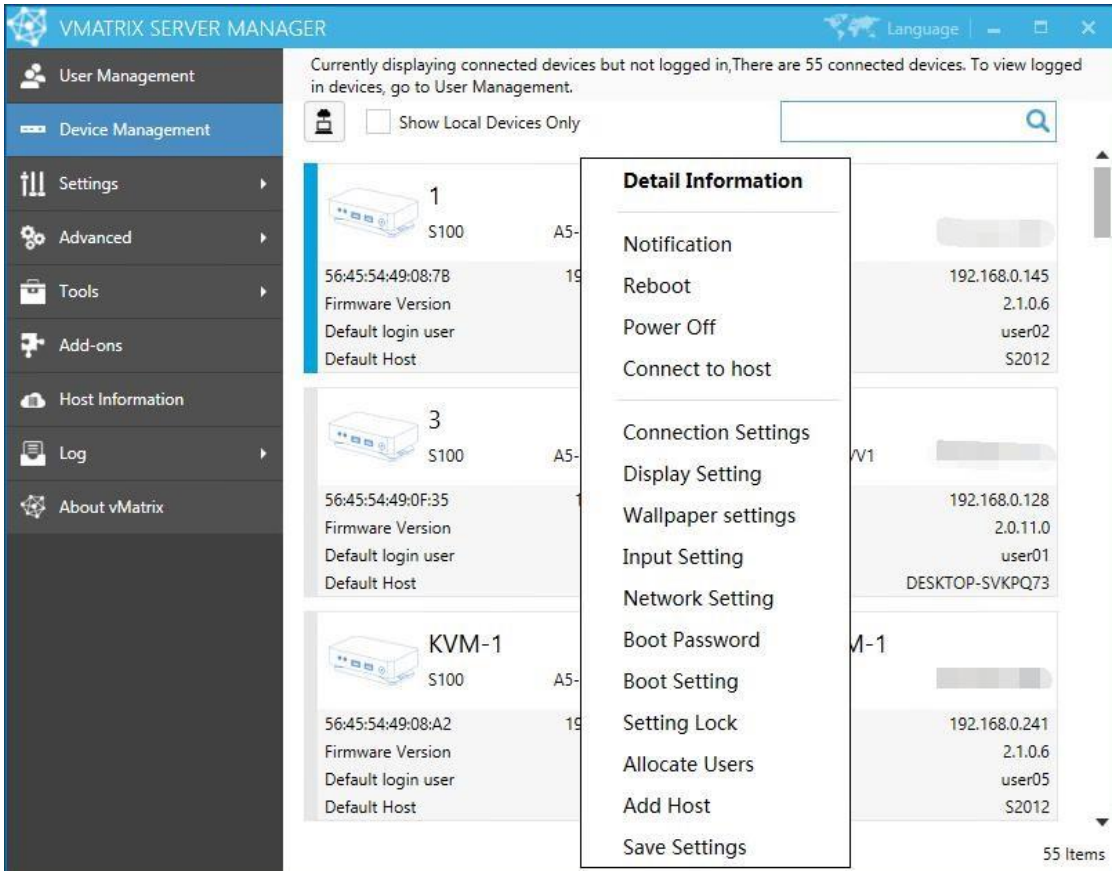
Note: This page displays connected devices (powered on devices in the same LAN as the host or powered on devices that has ever logged into the host) but not logged in. To view logged in devices, go to User Management.

5.2.2 Right Click Menu

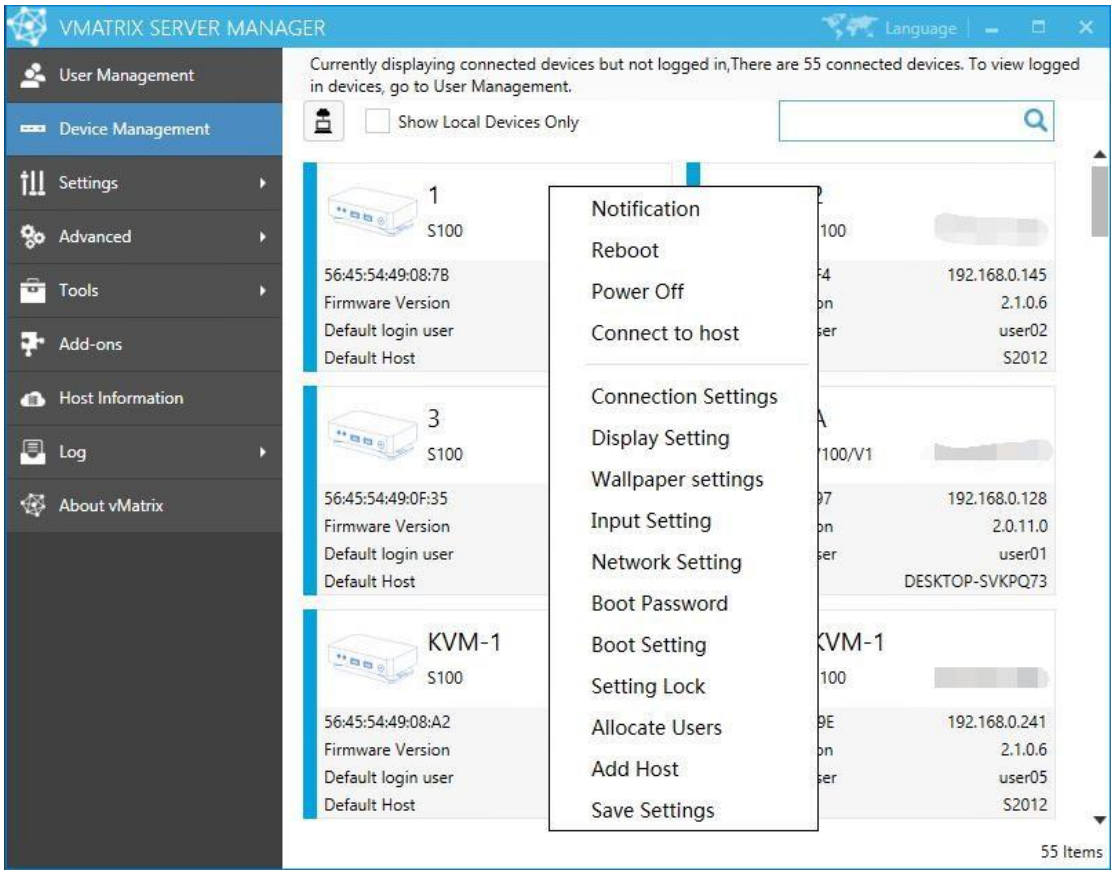
Right click on a single or multiple device modules to open the device management menu. Each of displayed options (except Notification) performs a function which can be found on

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.

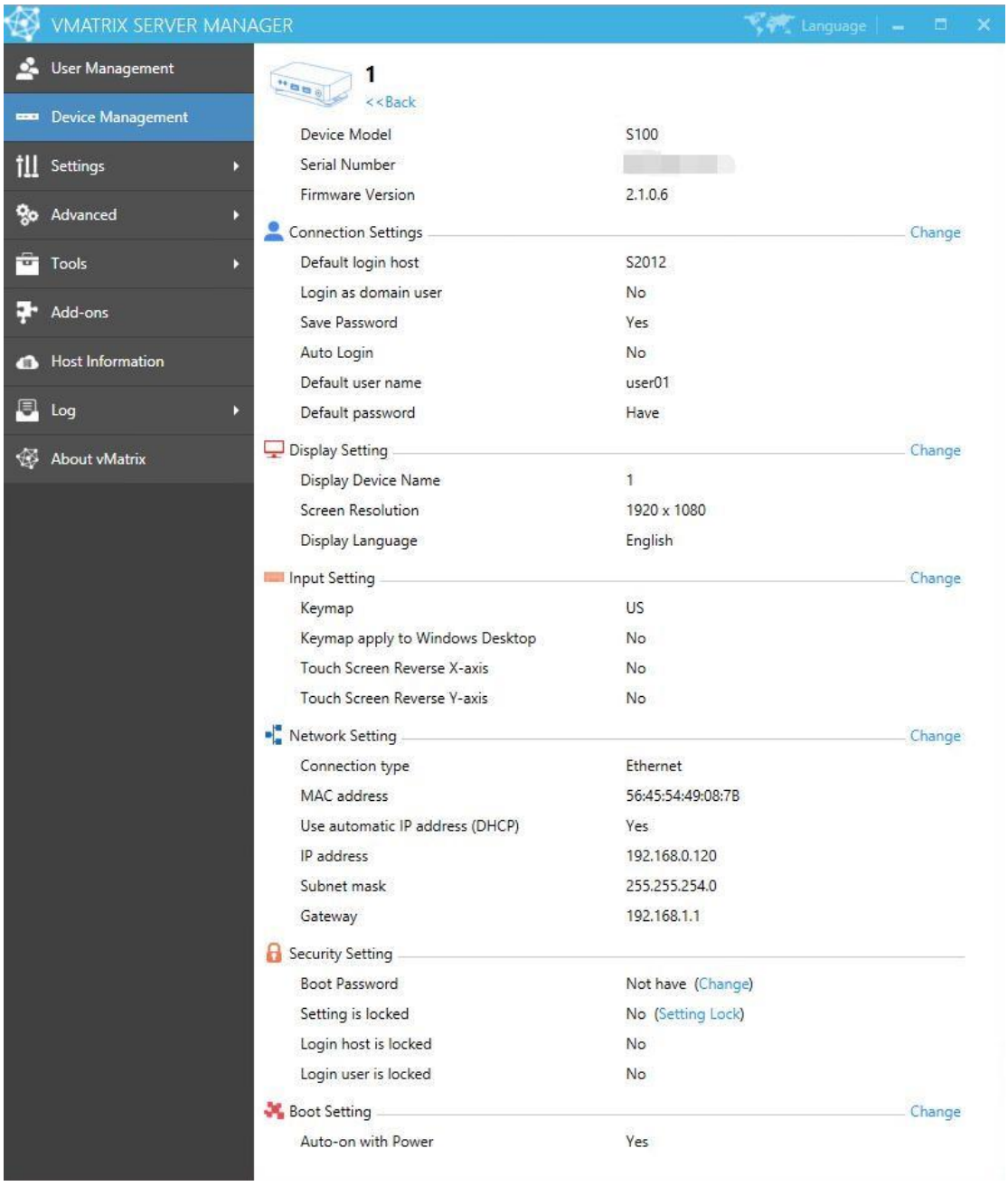
- **On a single device:** Detail Information, Notification, Reboot, Poweroff, Update Firmware, Login Host, Login Setting, Display Setting, Wallpaper Config,Input Setting, Network Setting, Boot Password, Lock Device Settings, Allocate to local users.



- **On multiple devices:** Detail Information, Notification, Reboot, Poweroff, Update Firmware, Login Host, Login Setting, Display Setting, Wallpaper Config,Input Setting, Network Setting, Boot Password, Lock (Unlock) Device Settings, Allocate to local users.

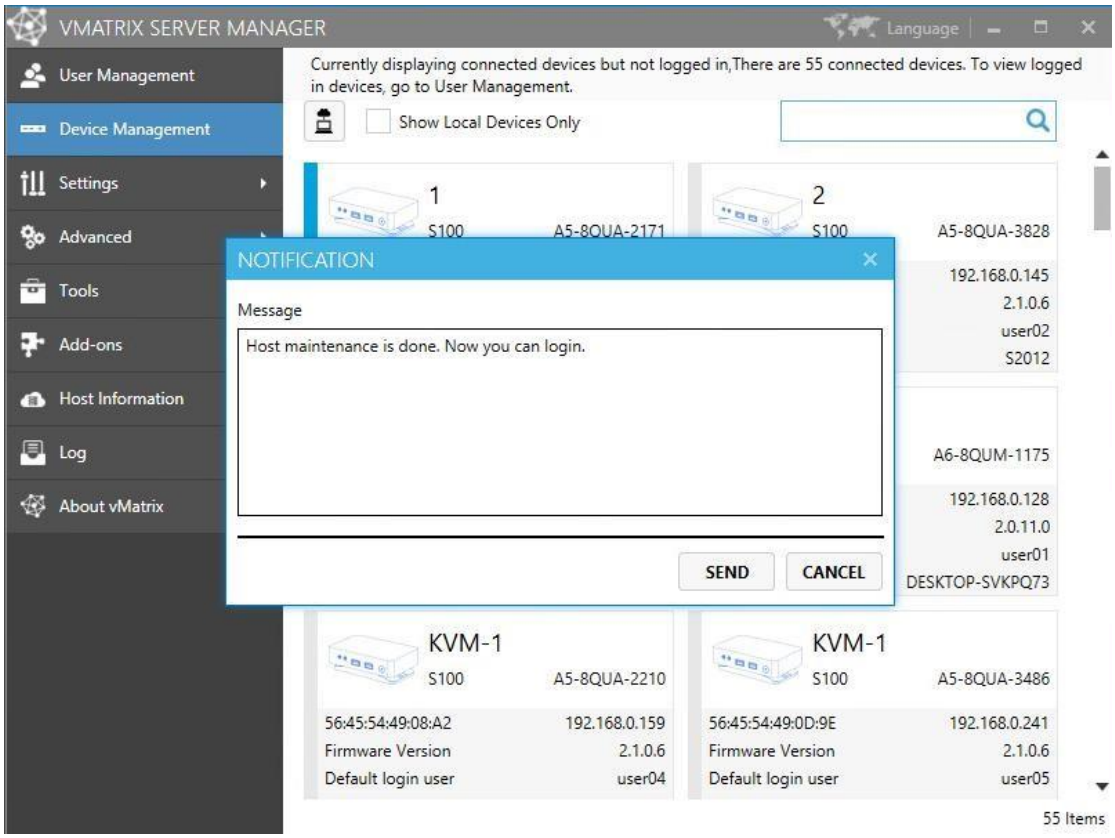


- **Detail Information:** to view the detail information of the selected device. To enter this page, you can either double click the device module or right click to select the option. To change any setting on this page, click “Change”.

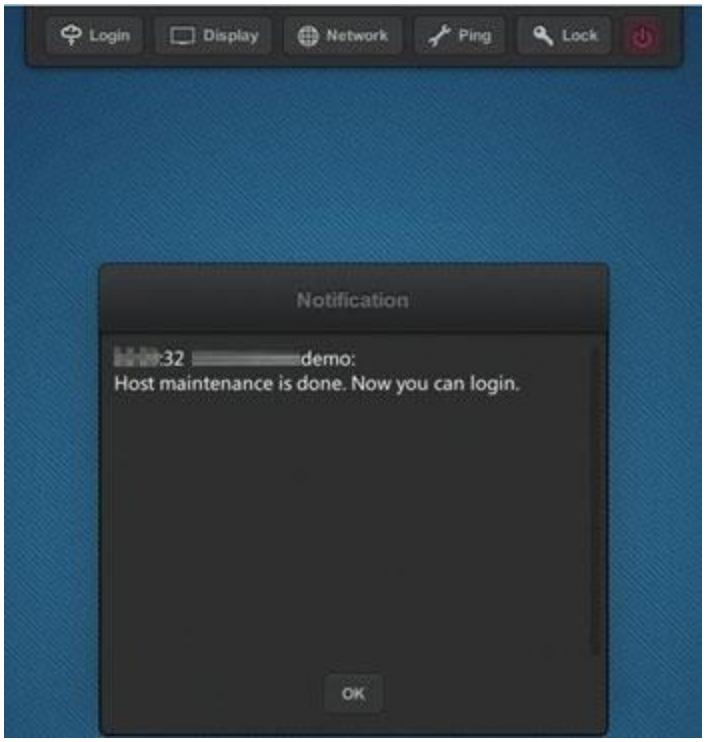


- **Notification:** to send a notification to the selected user.

Notification sent from host:

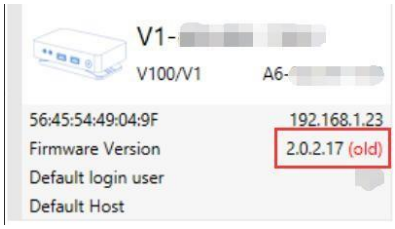


Notification to the device:



- **Reboot:** to reboot the selected devices. ■ **Poweroff** : to shut down the selected devices.

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



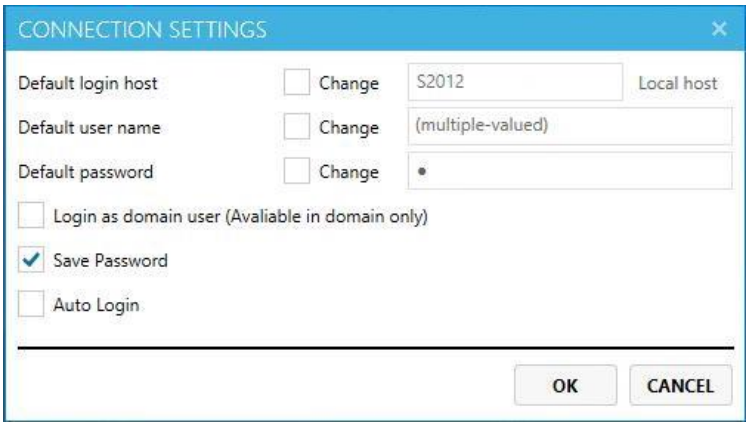
Notes:

1. Keep the vMatrix Server software of all hosts to the same version.

2. 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.

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

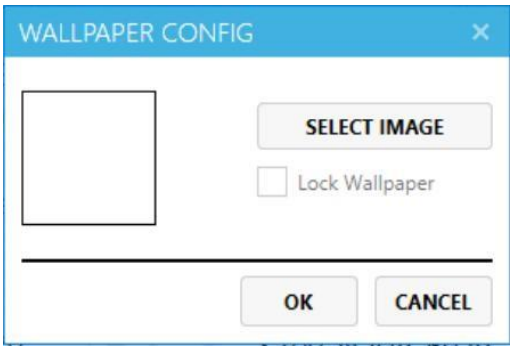
- **Login Setting:** to change the selected devices login settings including default login host, default user name, default password, domain selection, password saving selection and auto login selection which will be used for the devices next login. When multiple devices are selected, click "Local host" to set the device as default login host, the Default User Name field is disabled and password change only works when the same password is used by all users. 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).



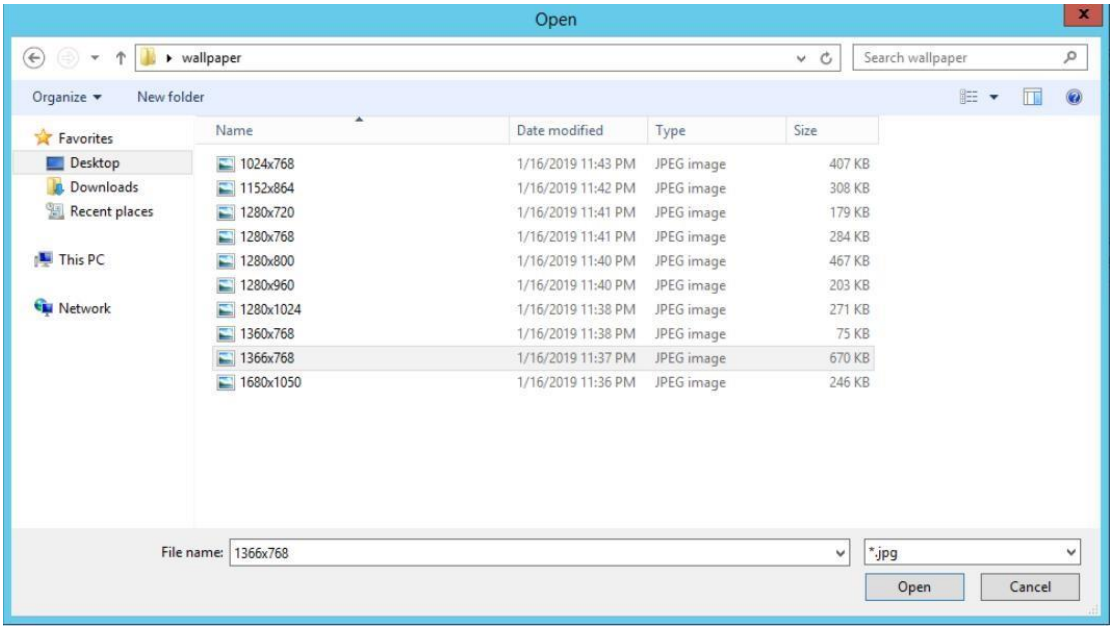
Display Setting: to change the display settings of the selected devices including device name, screen resolution and language; if you leave the device name field empty, the default name with serial number will be used.

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

1. Click “SELECT IMAGE”;

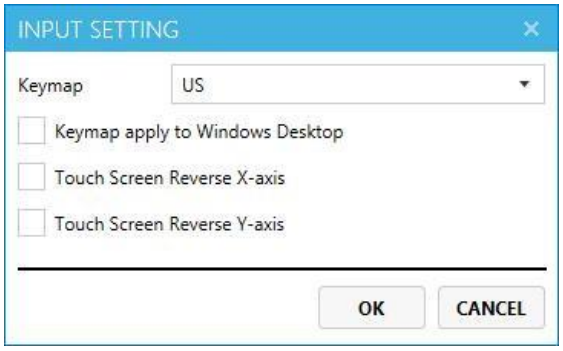


2. Select an image, only JPG image is supported;

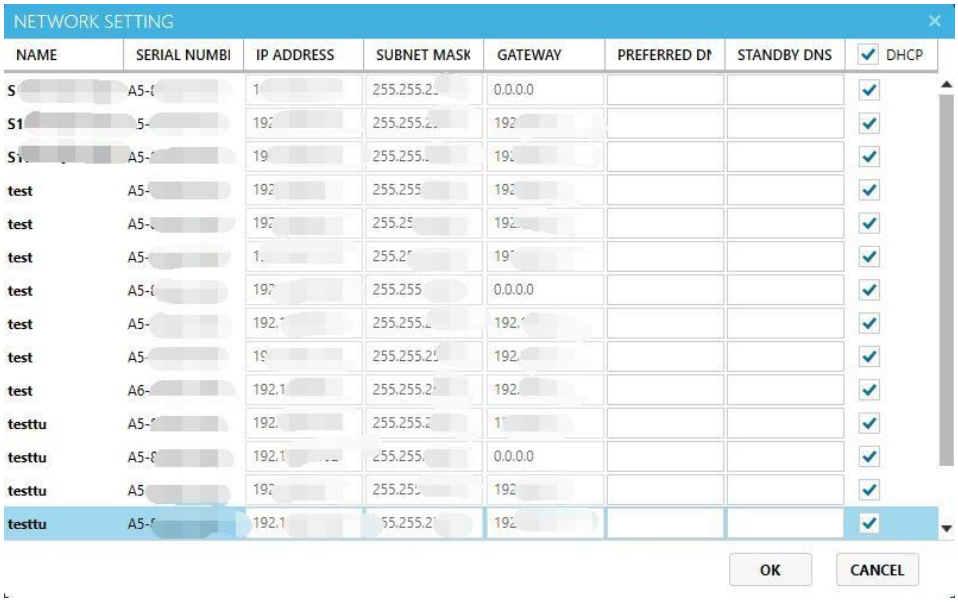


3. Then click "OK" to apply the configuration (if you lock down the wallpaper, users cannot change wallpaper on the client device.

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



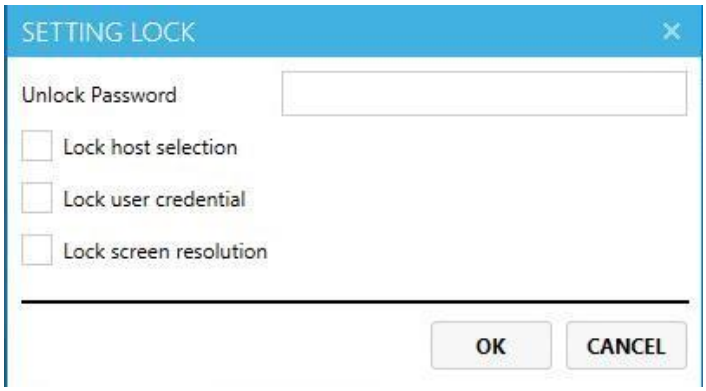
- **Network Setting:** to change the network settings of the selected device to using DHCP automatic or customized IP address; this option is available only when a single device is selected and WIFI setting is not available on remote control through network.



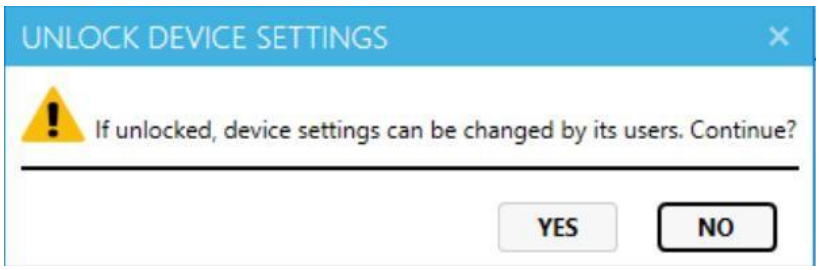
Boot Password: to set up a password on device boot so that the user is required to enter password to use the device.

- **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.

- **Lock Device Settings:** 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 is to disable the host selection and restrict the user to login to the selected host. A host must be selected before this option is selected. Lock user credential is to disable the user to change user name and password and restrict 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. After you set up a password for the device, this option will be replaced by “Unlock Device Settings” on its right click menu.

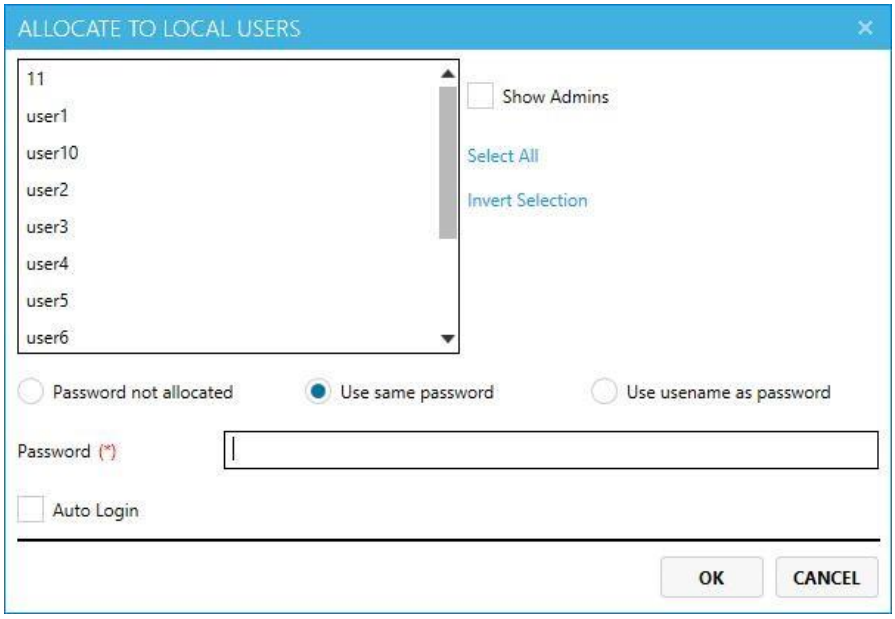


Unlock Device Settings：To unlock the device settings. The lock-down password will be clear on clicking this option will immediately clear the earlier lock password without the need to enter the password. After you unlock the settings for the device, this option will be replaced by “Lock Device Settings” on its right click menu.

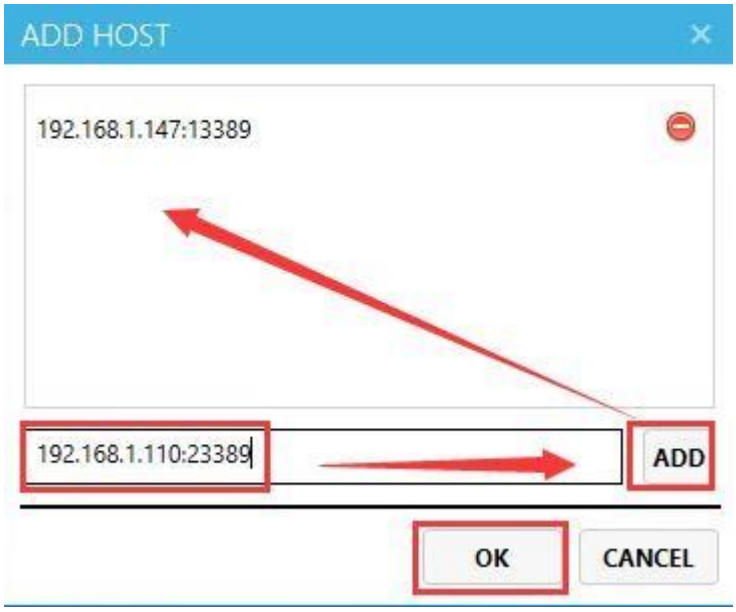


- **Boot Setting**：When the option of “Enable remote boot” is checked, the client device can be booted from the server manager. When the option of “Auto-on with Power ” is checked, the client device will be automatically powered on with power supply.

- **Allocate to local users:** randomly allocate the selected devices to local users. Note: if the number of devices exceeds the number of existing user, some devices will not be collocated. If password is not allocated, auto login cannot be selected.



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).



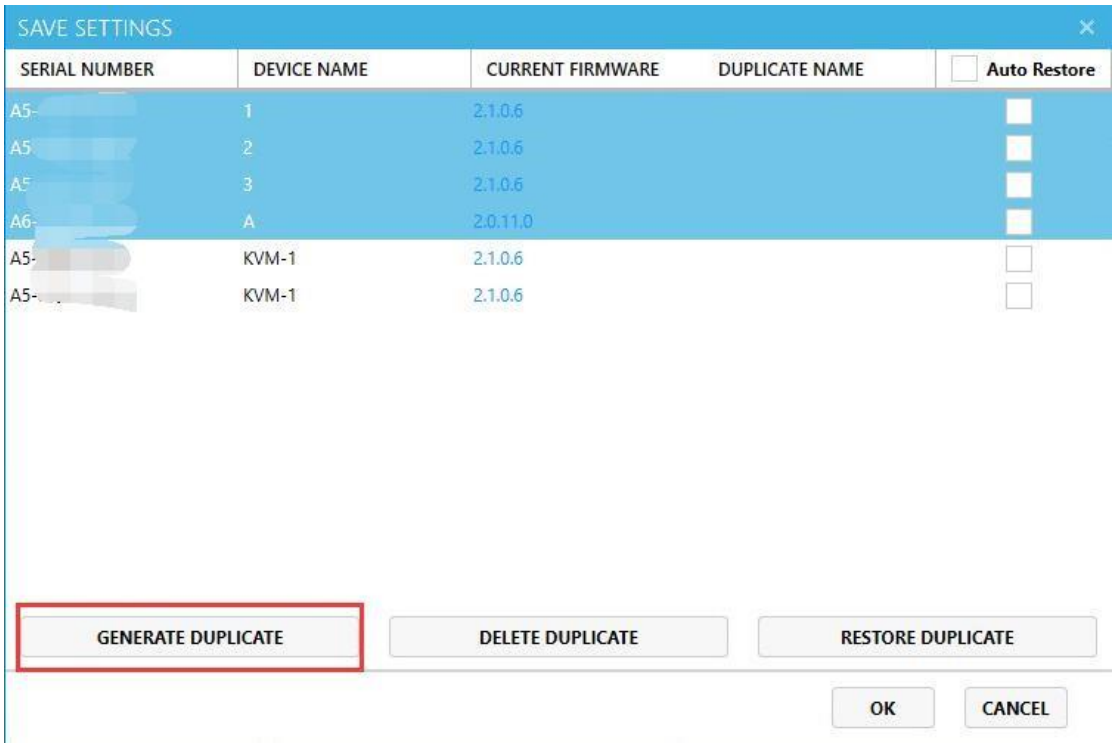
Notes:

- 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.

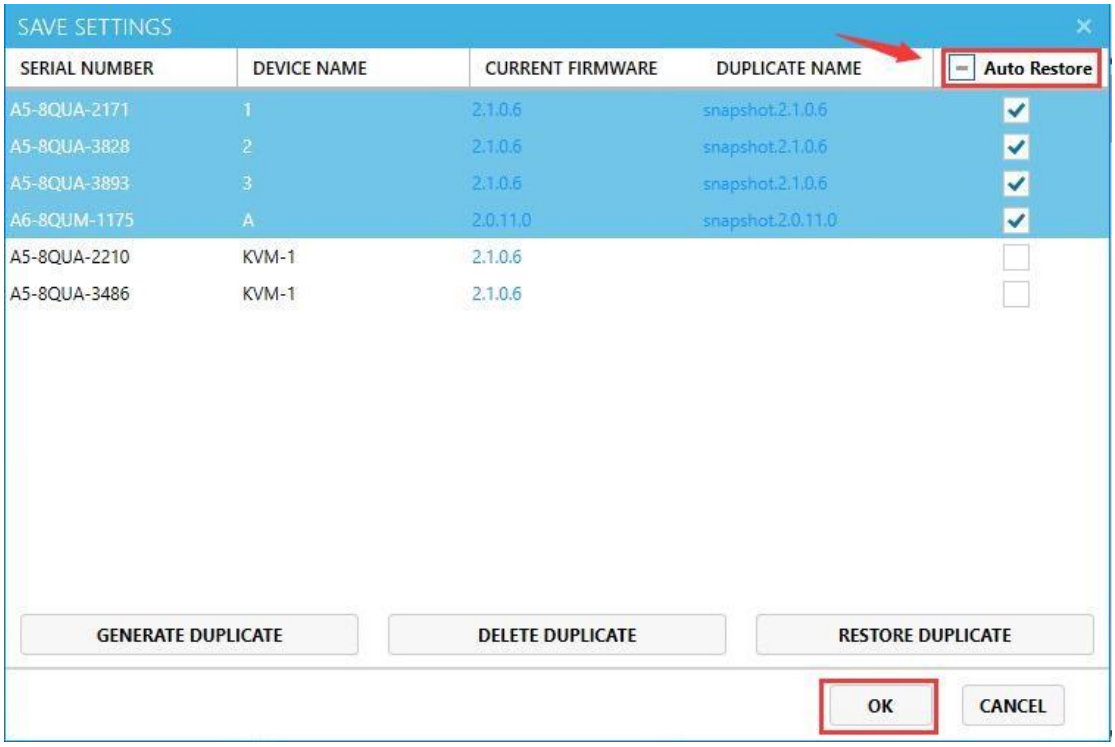
■ **Save Settings:** save device settings to the host for restoration in case of settings lost by resetting.

1. Select the devices to generate duplicates.

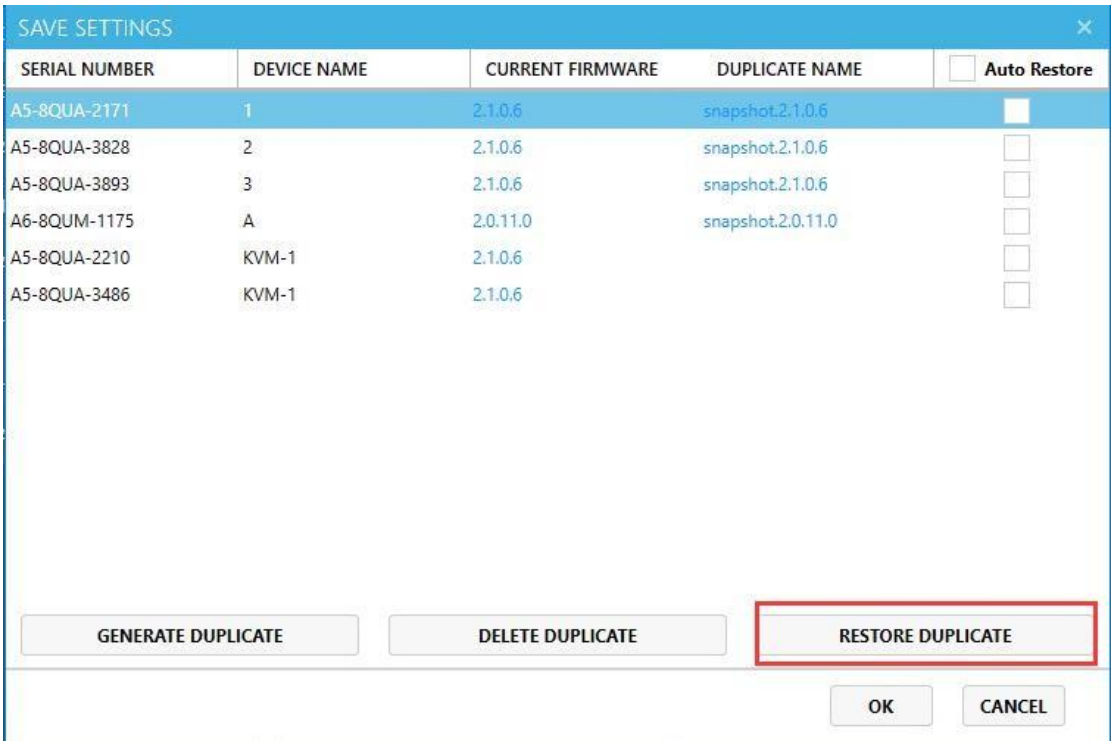
■



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



3. Uncheck the “Auto Restore” option if you want to manually restore the settings.

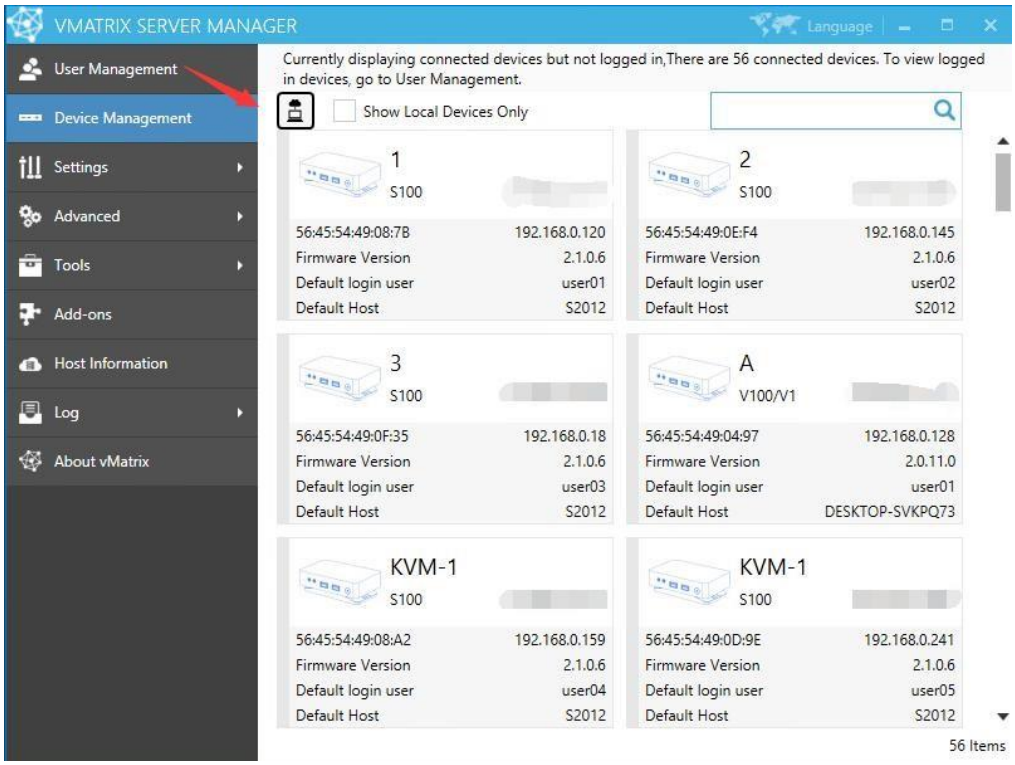


Notes:

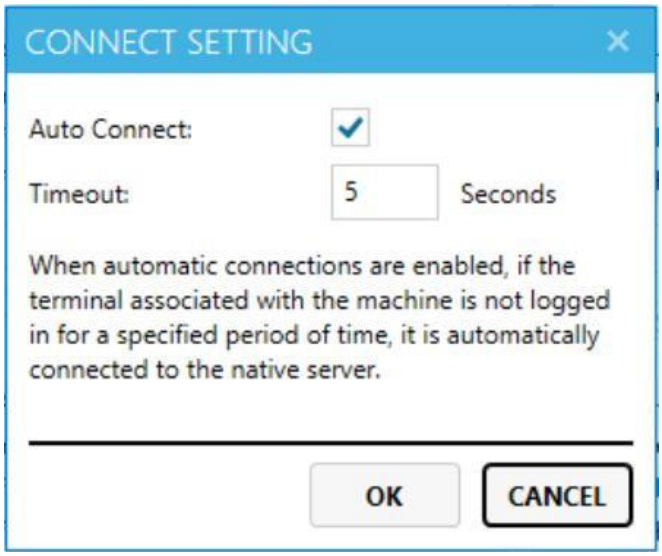
- The client devices shall be connected to the host for generating or restore from a saved setting duplicate.
- A setting duplicate must be saved before the device settings being manually or automatically restored.
- When a client device is configured with auto restoration on settings, any changes to 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, a firmware update will be executed first before recovering the settings.

5.2.3 Connect Setting

When automatic connection is enabled, if the terminals associated with the machine is not logged in for the specified time you have set, it will be automatically connected to the native server.



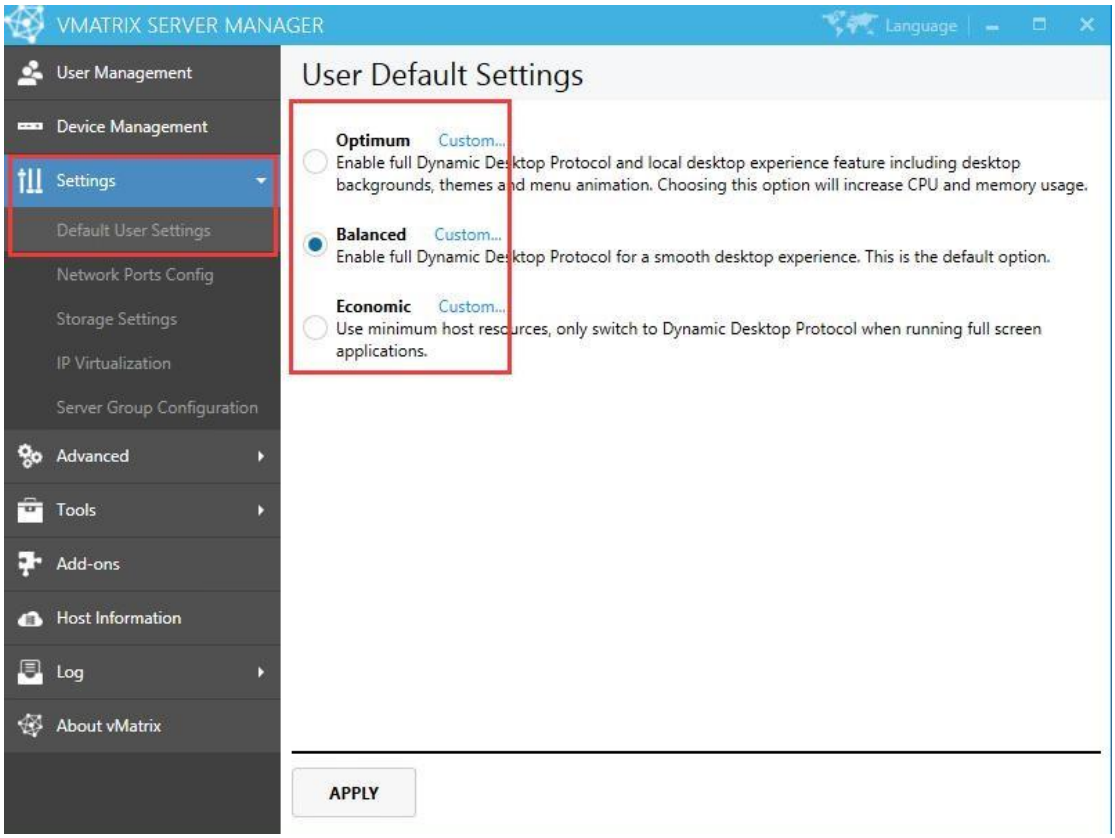
Check the “Auto Connect” option and enter the appropriate down-count time, and then click “OK” to save the configuration.



5.3 Configuration

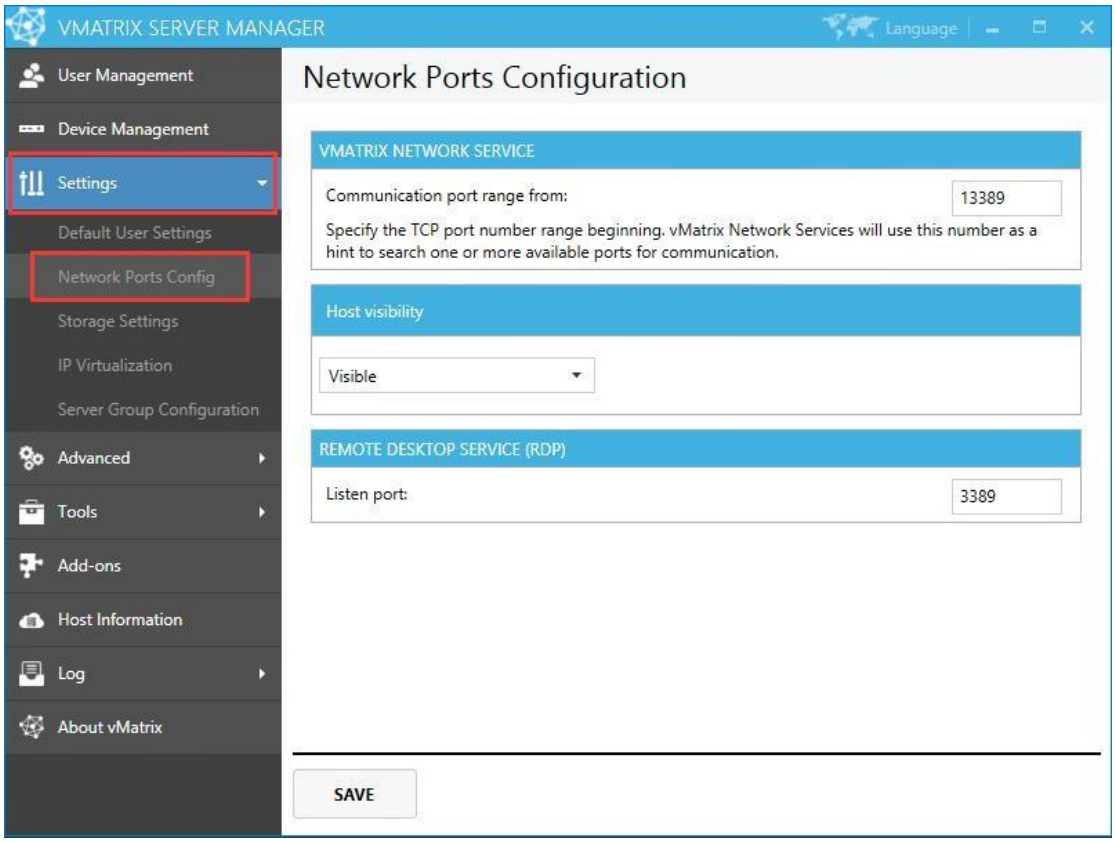
5.3.1 Default User Settings

Default settings will apply for those users using “Default” as their advance settings. Changes will take effect at user’s next login.



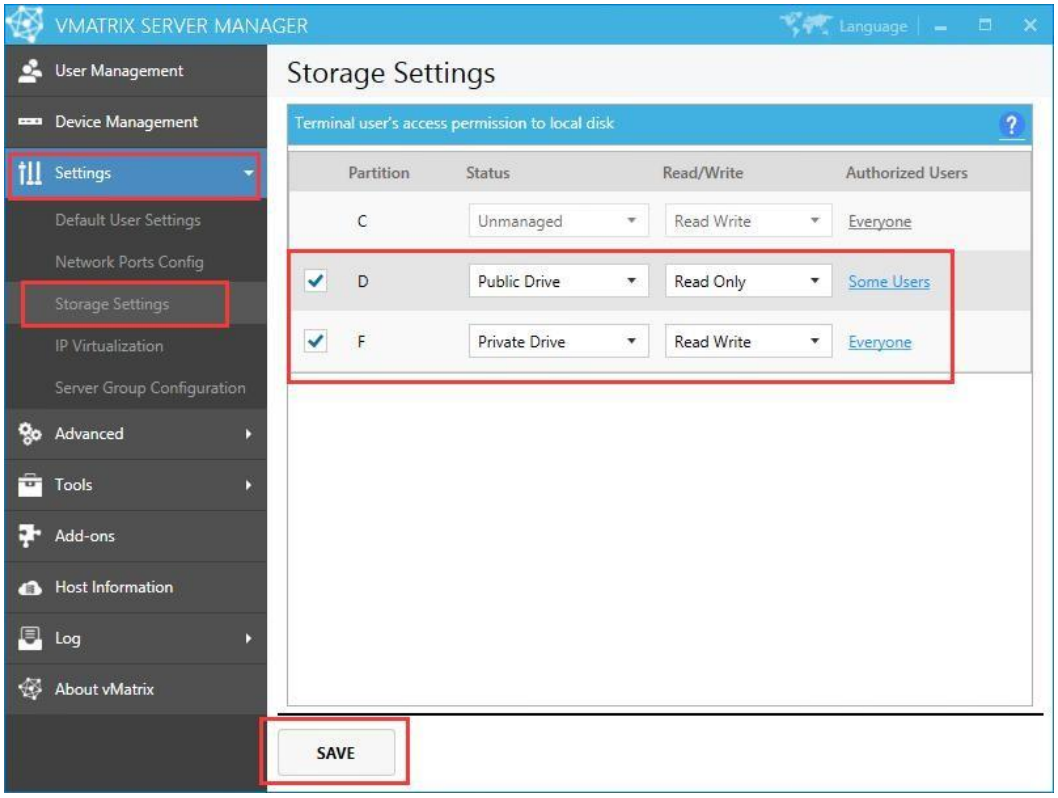
5.3.2 Network Ports Config

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. Default port numbers are 3389/13389.

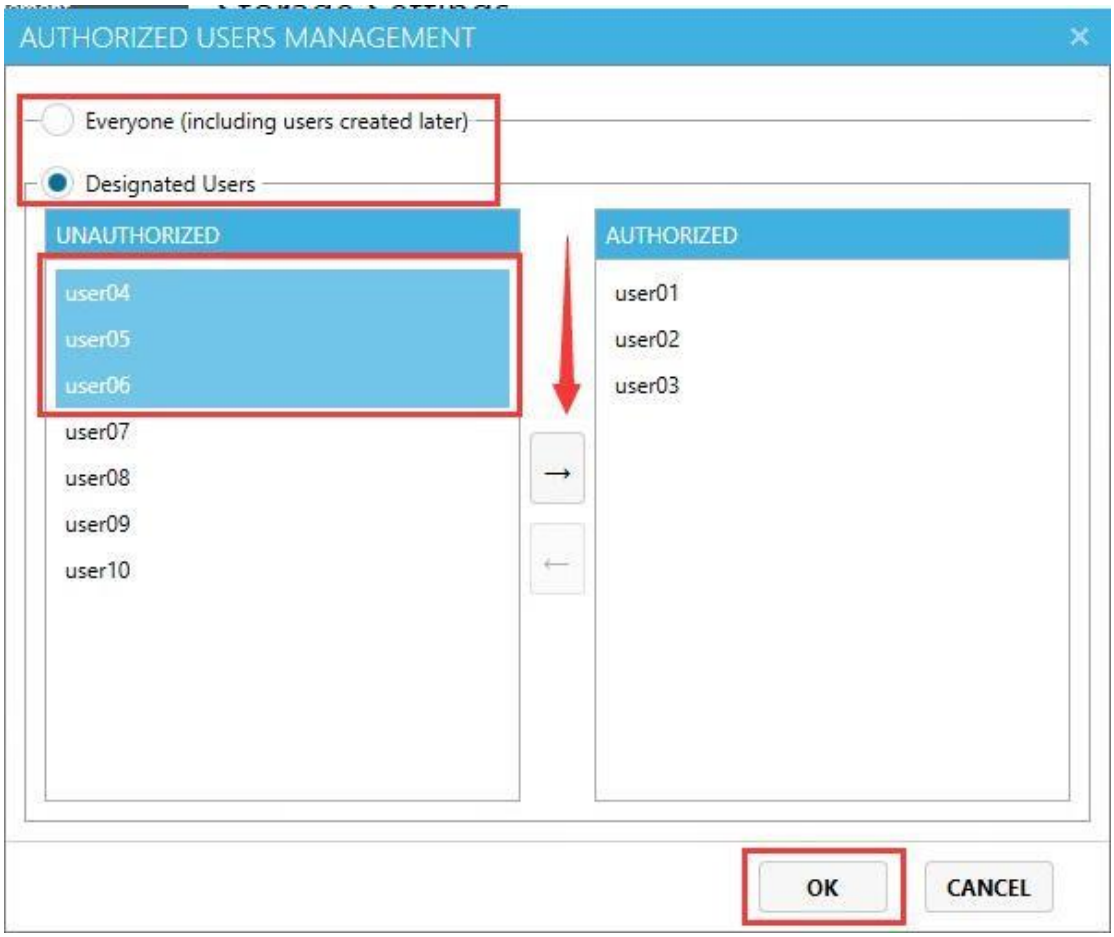


5.3.3 Storage Settings

vMatrix allows admins to manage terminal users' access to the local drives (except the C drive) including external drives connecting to the host.



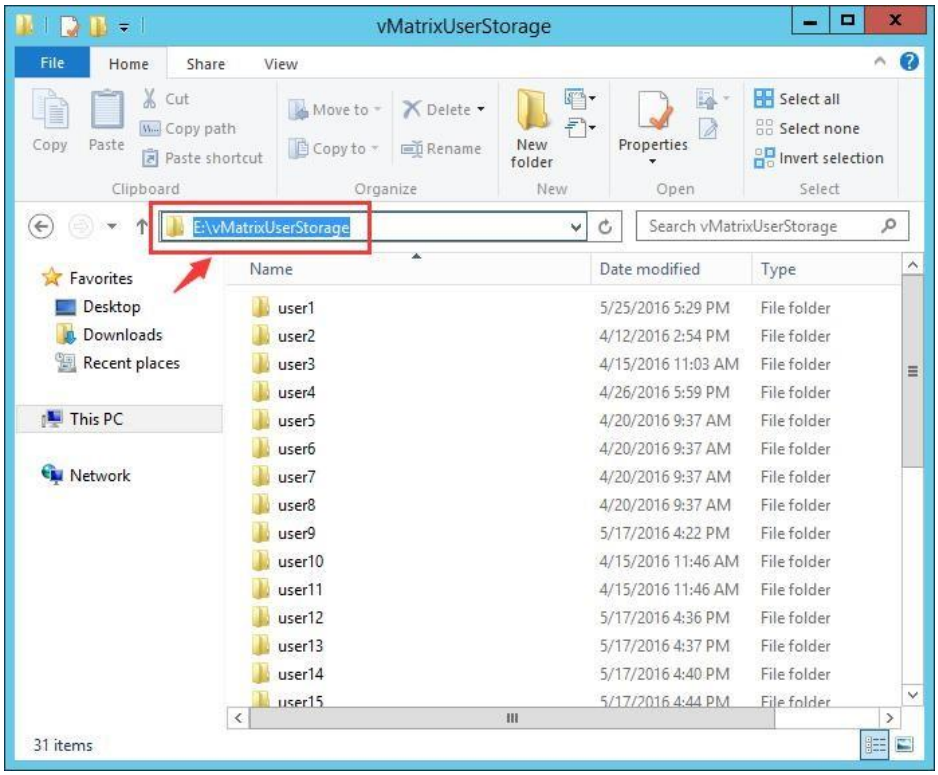
- Status
  - Public Drive: files in this drive are accessible to all authorized users.
  - Private Drive: files in this drive are only visible to the owner and the administrators.
  - Unmanaged: if you have personalized authorization settings for this drive and do not want vMatrix to overwrite these settings, leave it unmanaged.
- Read/Write
  - Read only: authorized users can read files in this drive or copy them to other drives but cannot create, modify or delete files in this drive.
  - Read Write: authorized users can read, create, copy, modify, and delete files in this drive.
- Authorized Users
  - Everyone: all terminal users, included later created users are authorized to access the drive.
  - Some Users: only the selected terminal users are authorized to access the drive.
  - None: no terminal users can access this drive.
  - Unauthorized users: drives are hidden to unauthorized users



Notes:

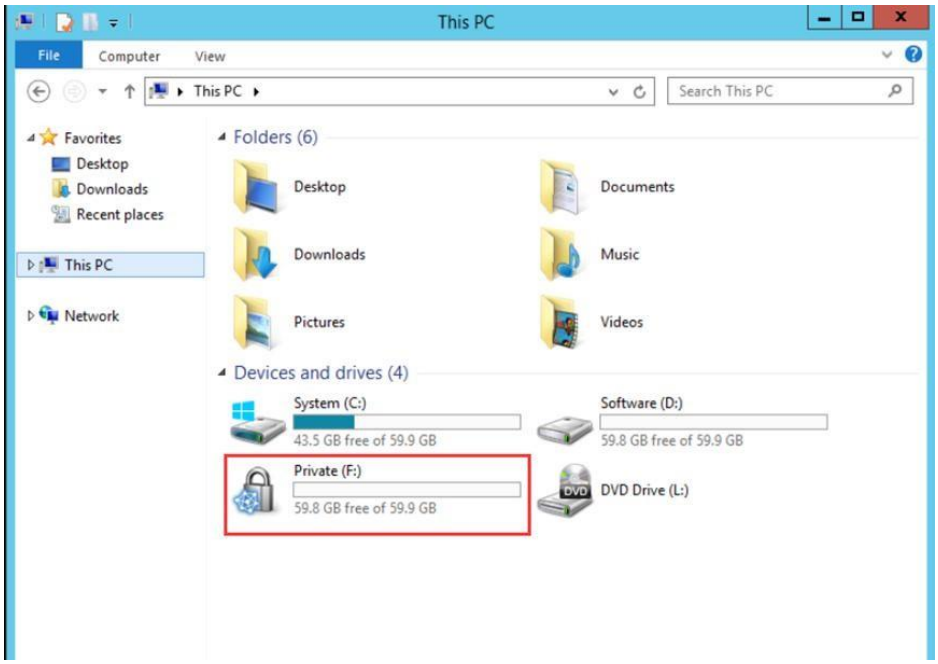
- The storage setting supports multiple private drives, excluding the C drive.
- Disks of non-NTFS and Non-REFS (such as FAT and exFAT) file system do not support read/write control and are hidden to unauthorized users in the File Explorer view, they can still access the drive by entering the directory like “H:/”in the File Explorer.
- The storage setting works for users only, not for administrators.
- Private drive settings only work for users running on a BlackBox 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:

The root folder of the User Private Space viewed by common users is the third-level subfolder beneath the root folder viewed by administrators (Root-> Folder: vMatrixUserStroage -> Folder: %name of the user%). The partition letter of the User Private Space falls to a latter letter of that viewed by administrators.



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.

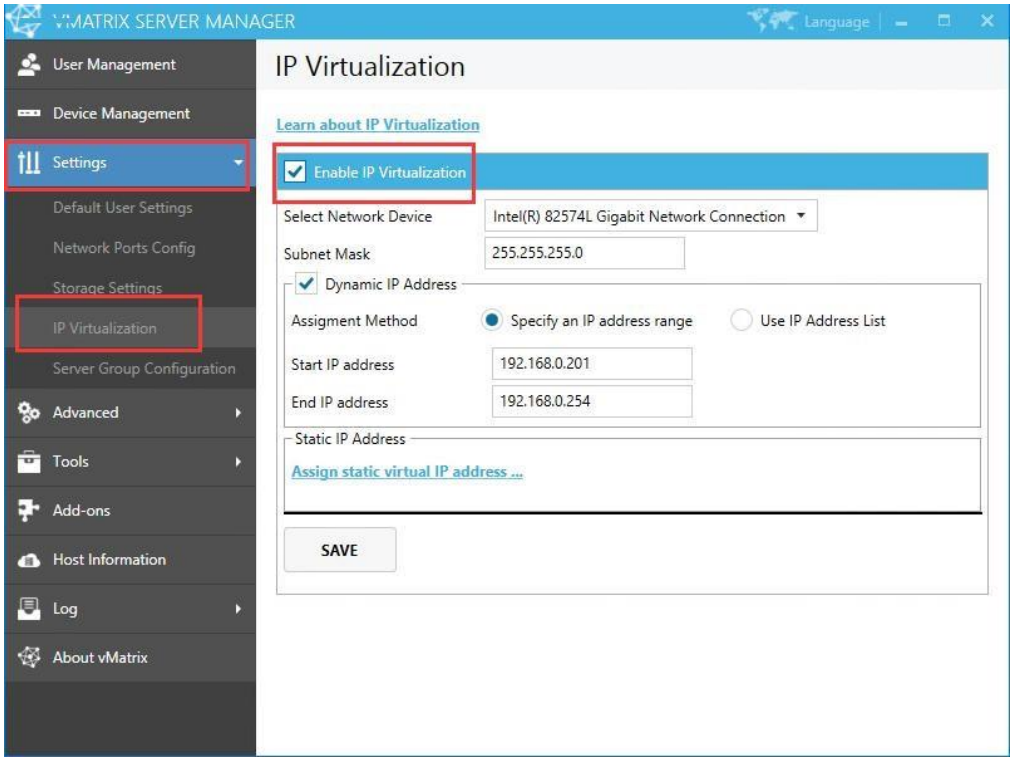
Use Cases:

- 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 charging 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.

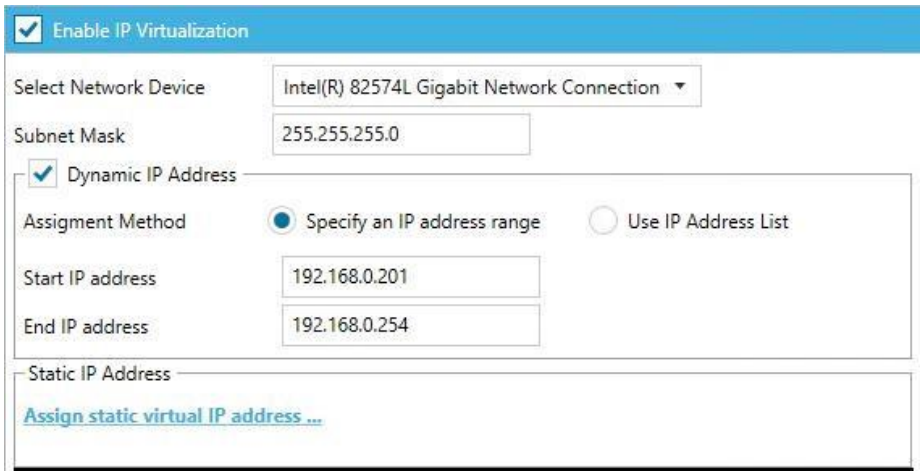
■ When IP virtualization is activated, the total number of LAN IP address used by the Shared Computing solution the will be double as before. Besides the IP address used by the client device, each client users will have an additional virtual IP address on the shared host for network communication.



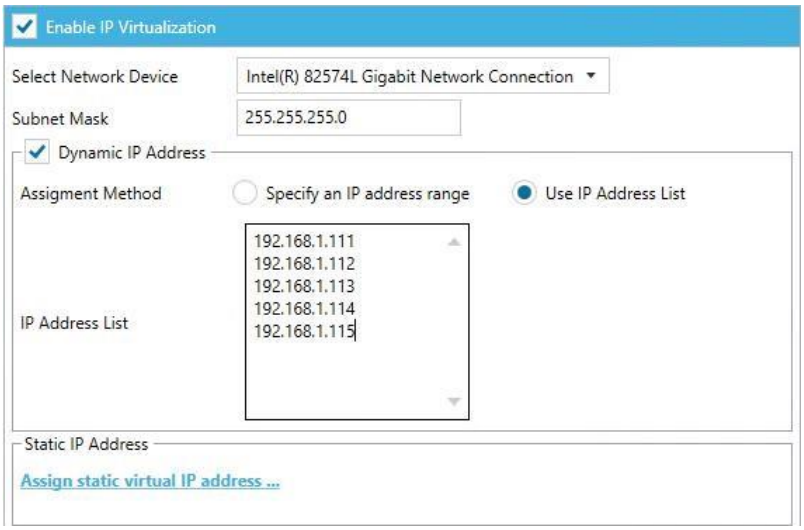
How to configure:

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

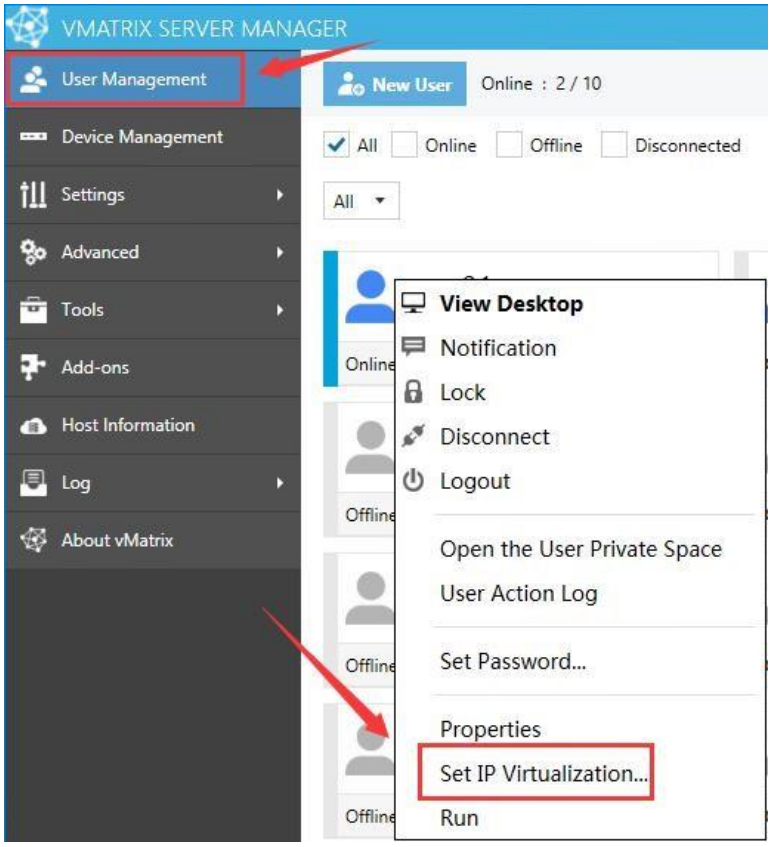
a) IP address range: fill in the range of network segment to be allocated in the starting IP address and ending IP address. The default subnet mask is 255.255.255.0, which can be modified as required.



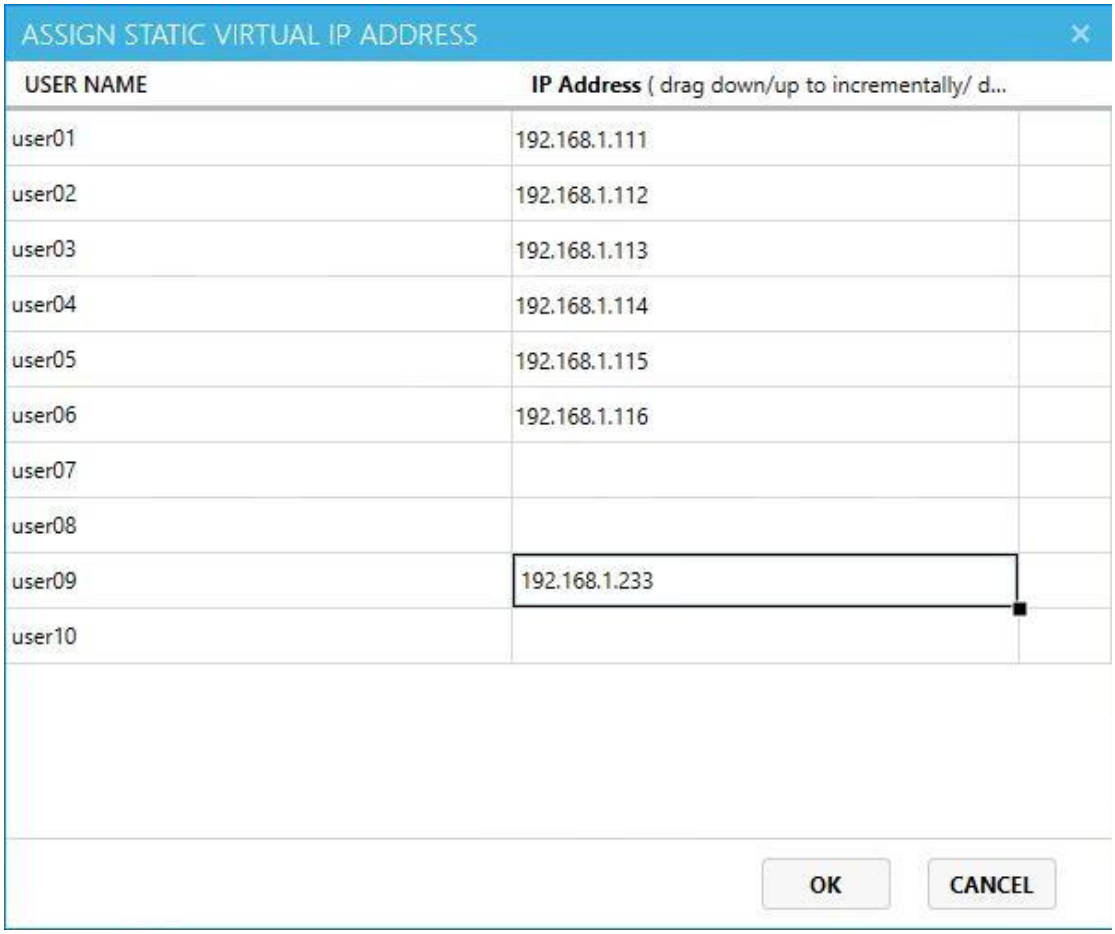
b) IP address list: fill in the IP addresses to be assigned in the IP address list box, one IP address each line. The default subnet mask is 255.255.255.0, which can be modified as required.



● 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 a time.



Notes:

- When enabling IP virtualization, please set a static IP address for the host.
- 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.

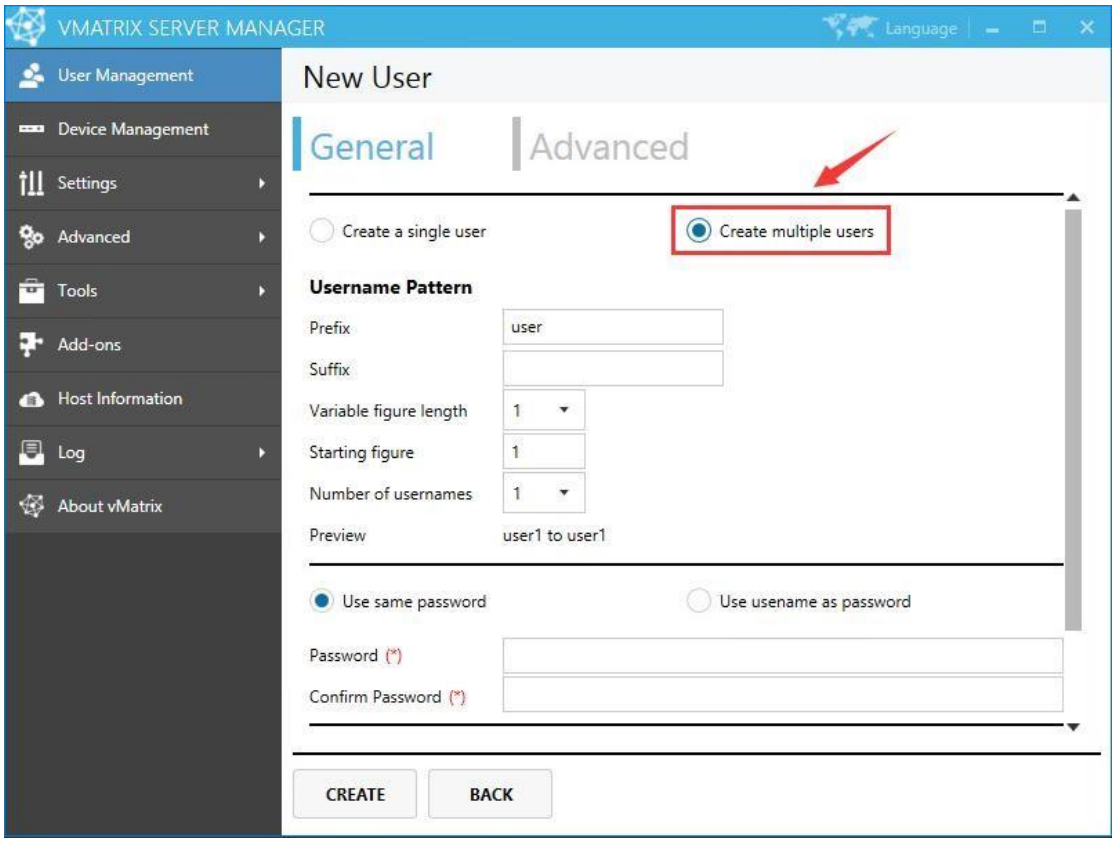
5.3.5 Server Group Configuration

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

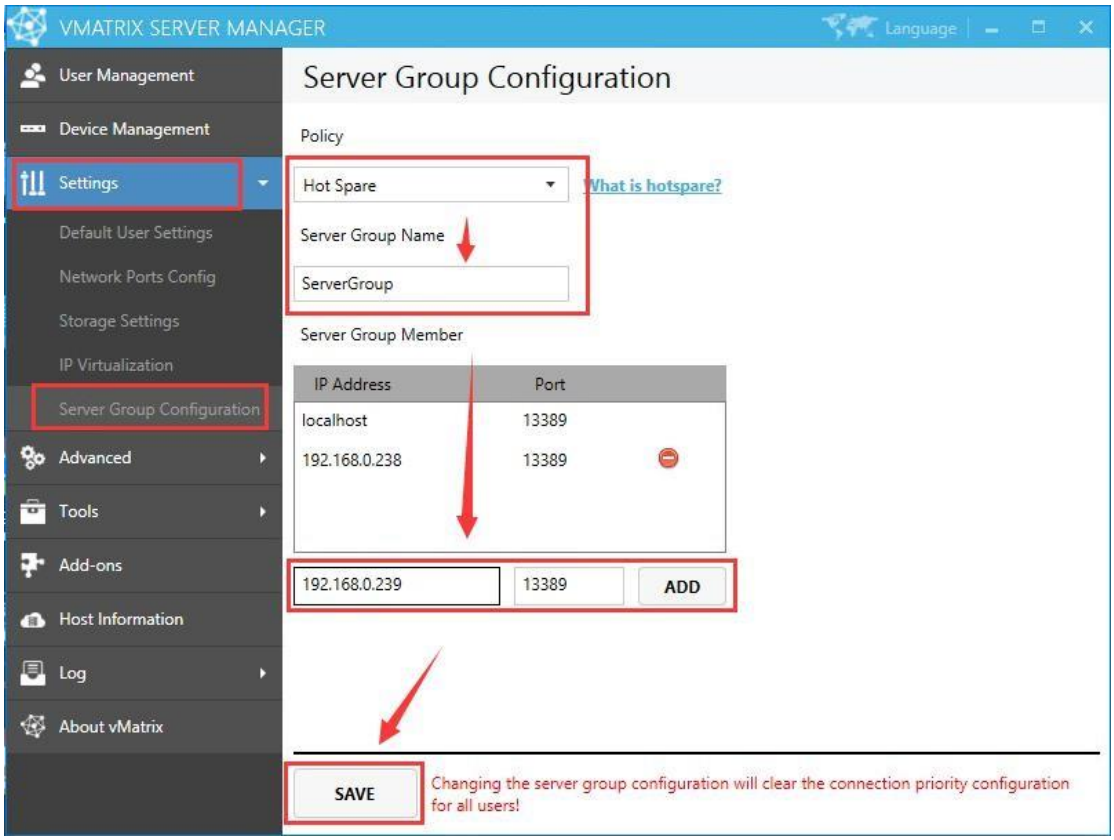
- **Hot Spare:** hot spare is a fail-over policy to ensure business continuity for a server group with multiple running hosts. With hot spare enabled, when the preferred host fails, the users running on it will automatically log into an alternate host in the server group according to a preset priority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

How to configure

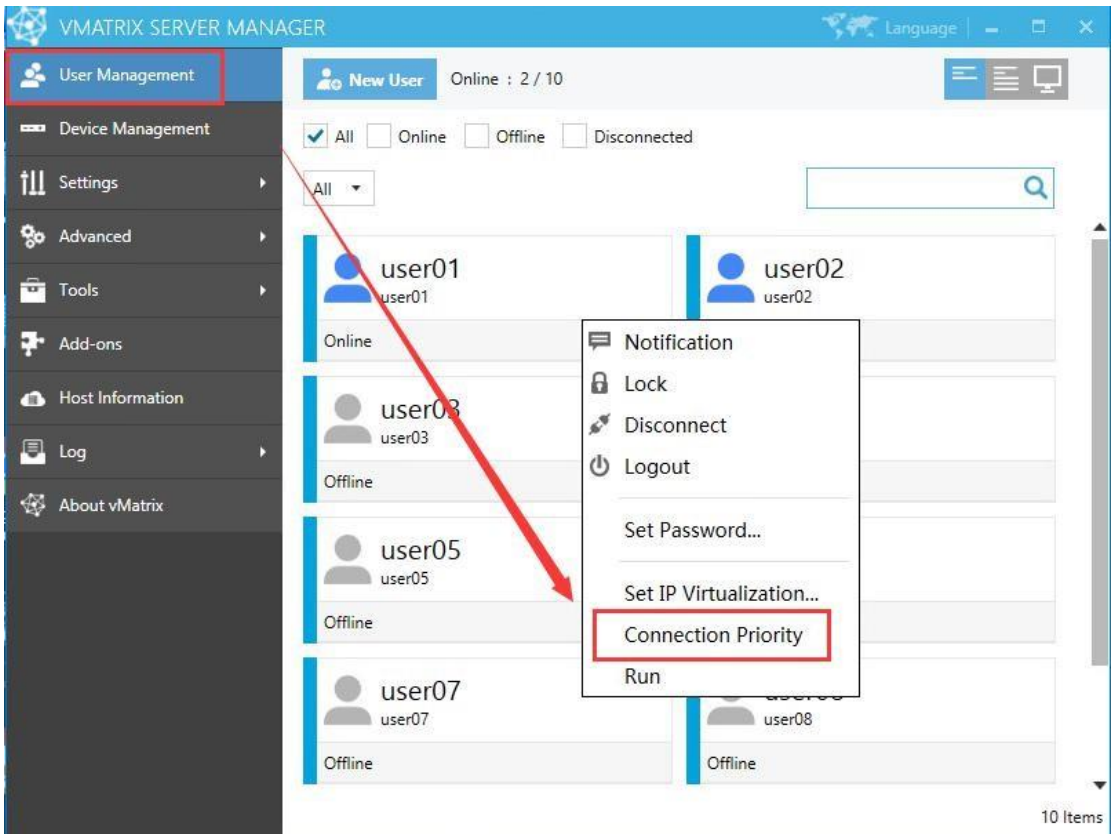
1. Create same user accounts on the shared host.

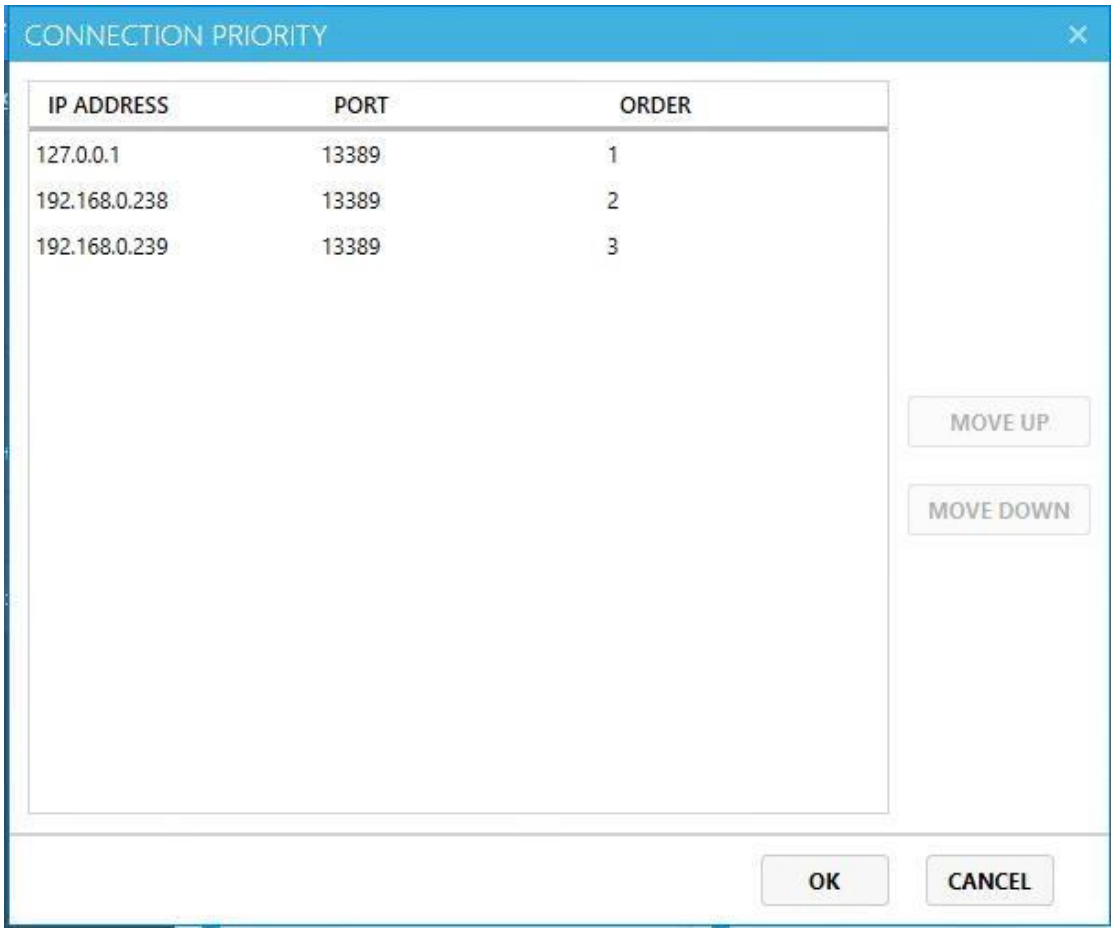


2. At the Settings page of vMatrix Server Manager, enable the hot spare option, create a server group and add multiple shared hosts into the server group.



3. At the User Management page, set connection priority for the users.





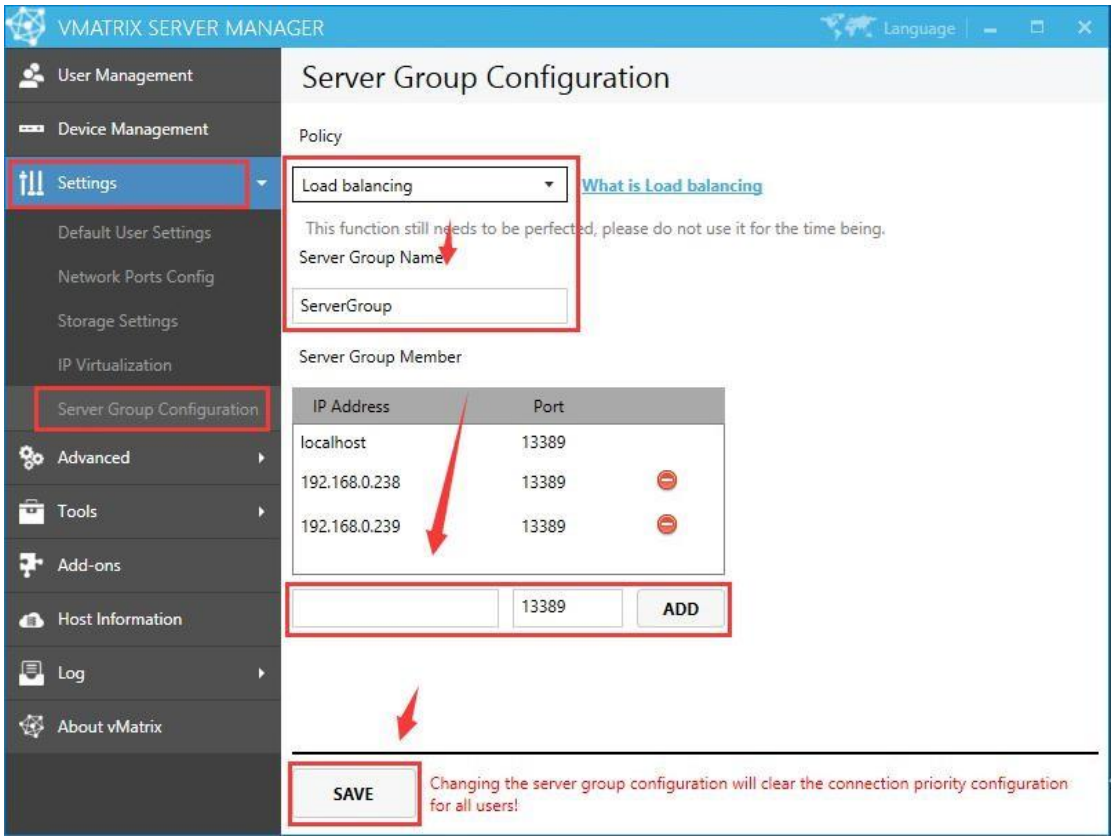
4. Repeat the 2nd and 3rd server grouping and connection priority configuration steps on other shared host within the server group.

Note: 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. At the Settings page of vMatrix Server Manager, enable the load balancing option, create a server group and add multiple shared hosts into the server group.



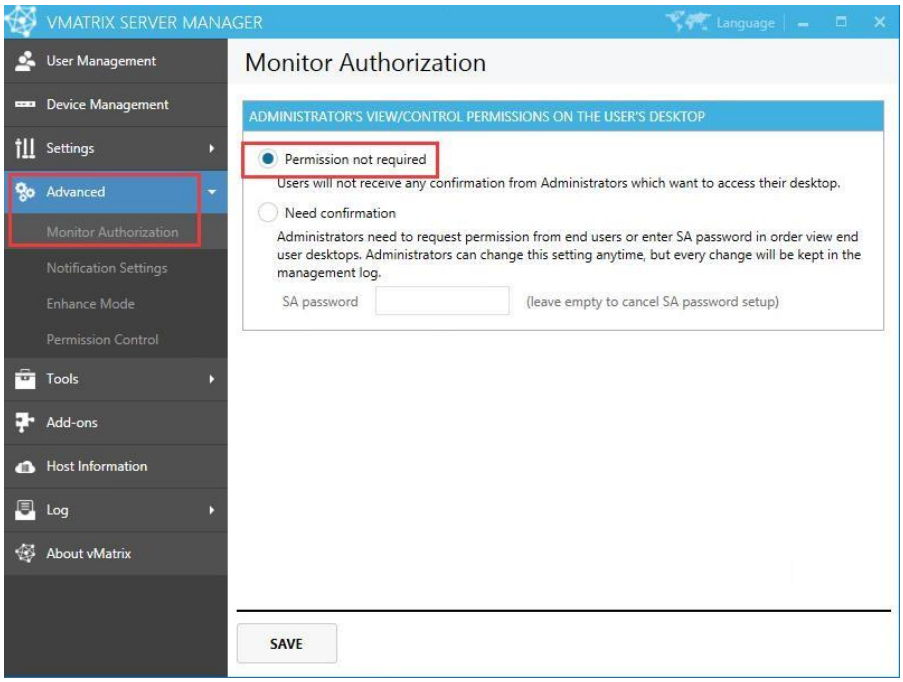
2. Repeat the above steps on other shared host to add them to the same server group.

Note: With vMatrix Server Manger version 2.5.2, 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:

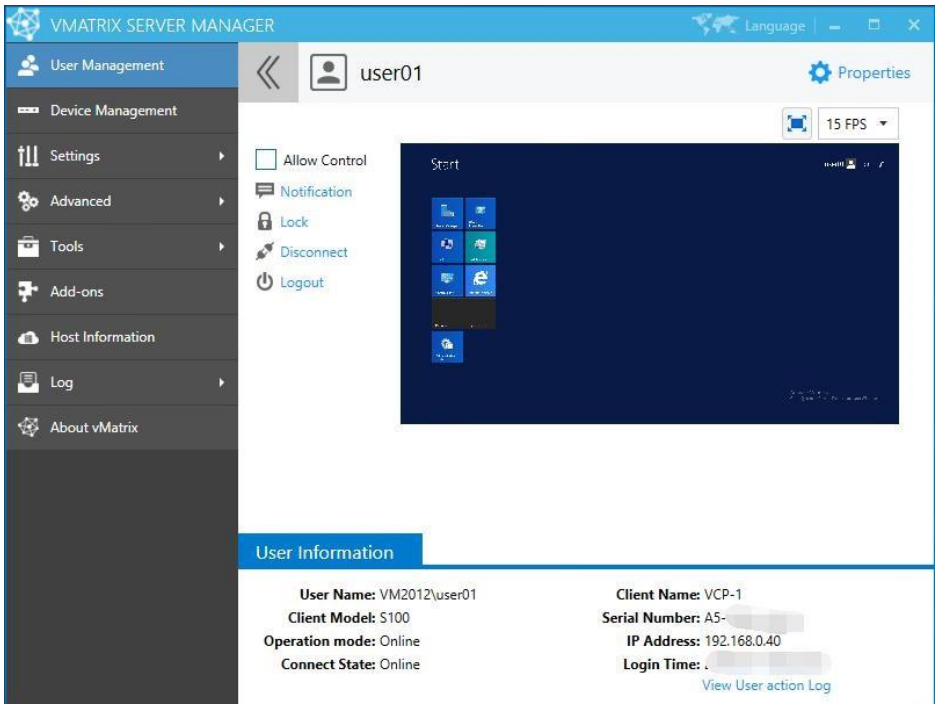
- After hosts join a server group, the host name displayed in the host list of the terminal device will be the server group name instead of the host name.
- Server group name and IP address shall be the same among all server members in the server group.
- A shared storage system is recommended to allow the staff to get back to their work documents when they switch to another server. You can also set up folder redirection and roaming user profiles in a Windows domain to ensure integrity and consistency of user data across multiple hosts.

5.4.1 Monitor Authorization



- **Don't need confirmation:**

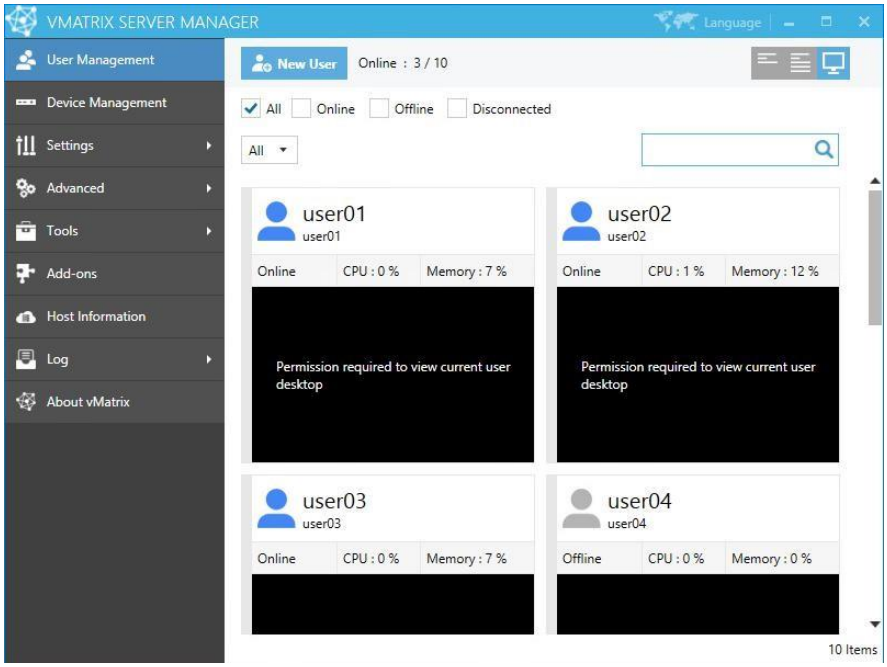
administrators can monitor user desktops without requiring confirmation from the monitored users.

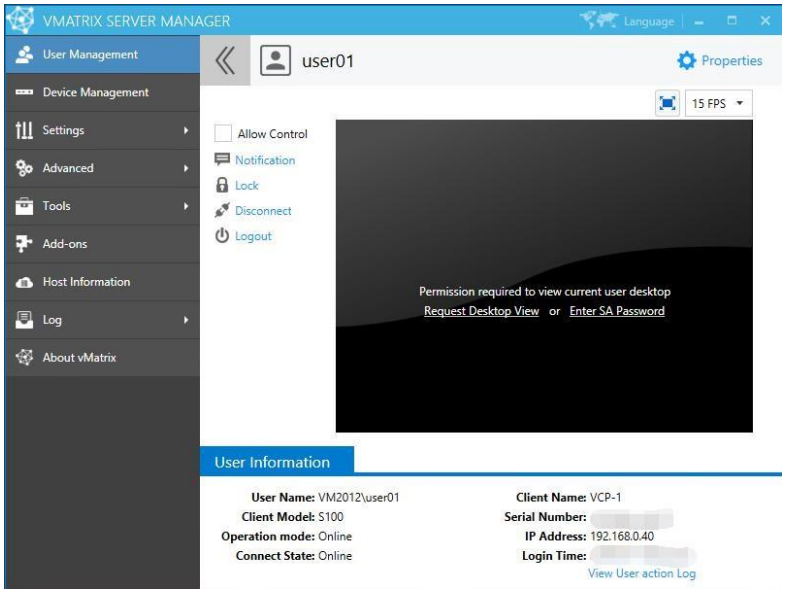


- **Need confirmation:**

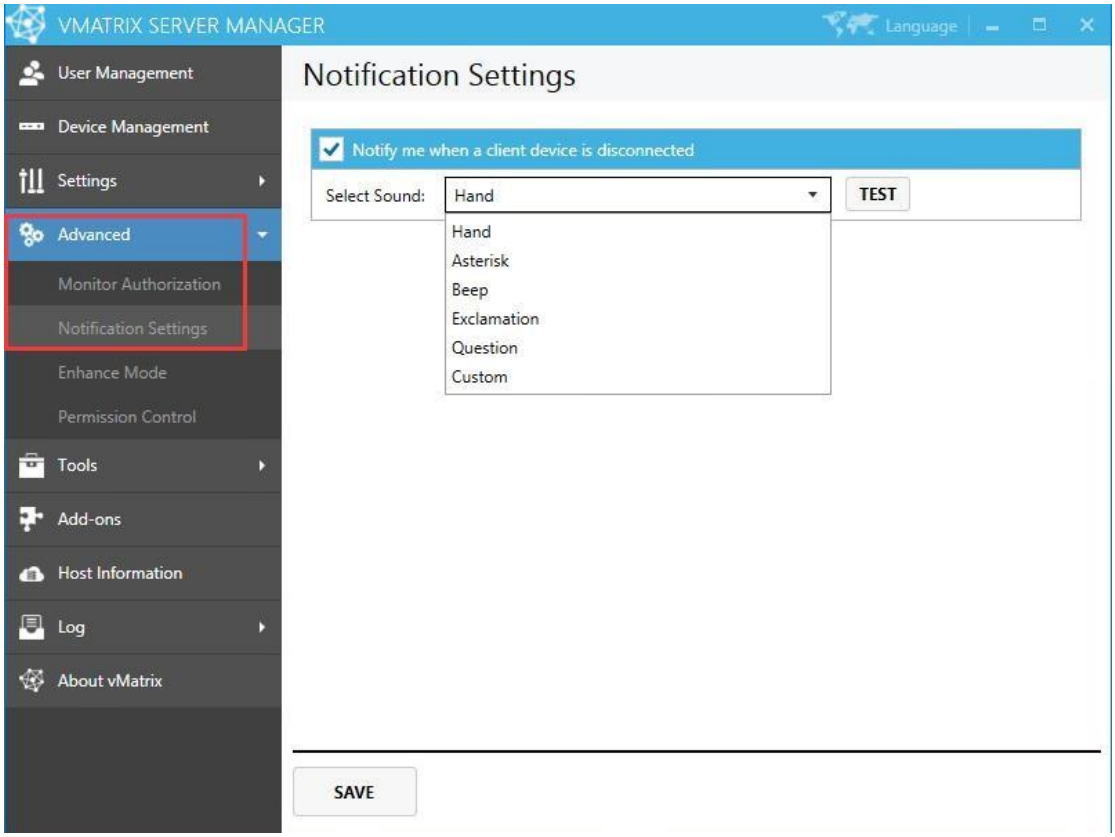
you are required to setup a Super Administrator (SA) password when this option is selected. By selecting this option, administrators need to send request to the user or enter SA

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.





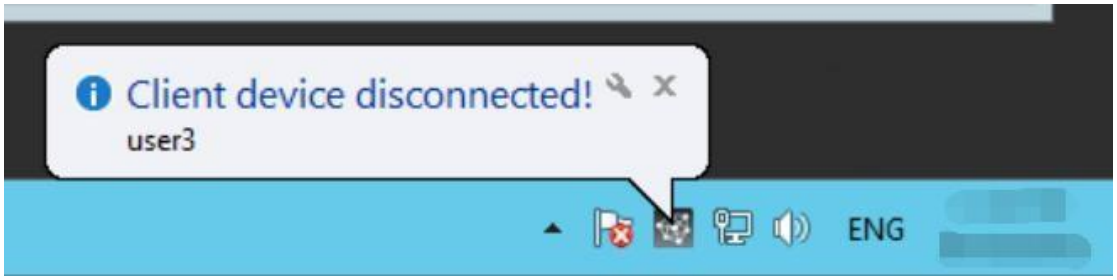
5.4.2 Notification



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.

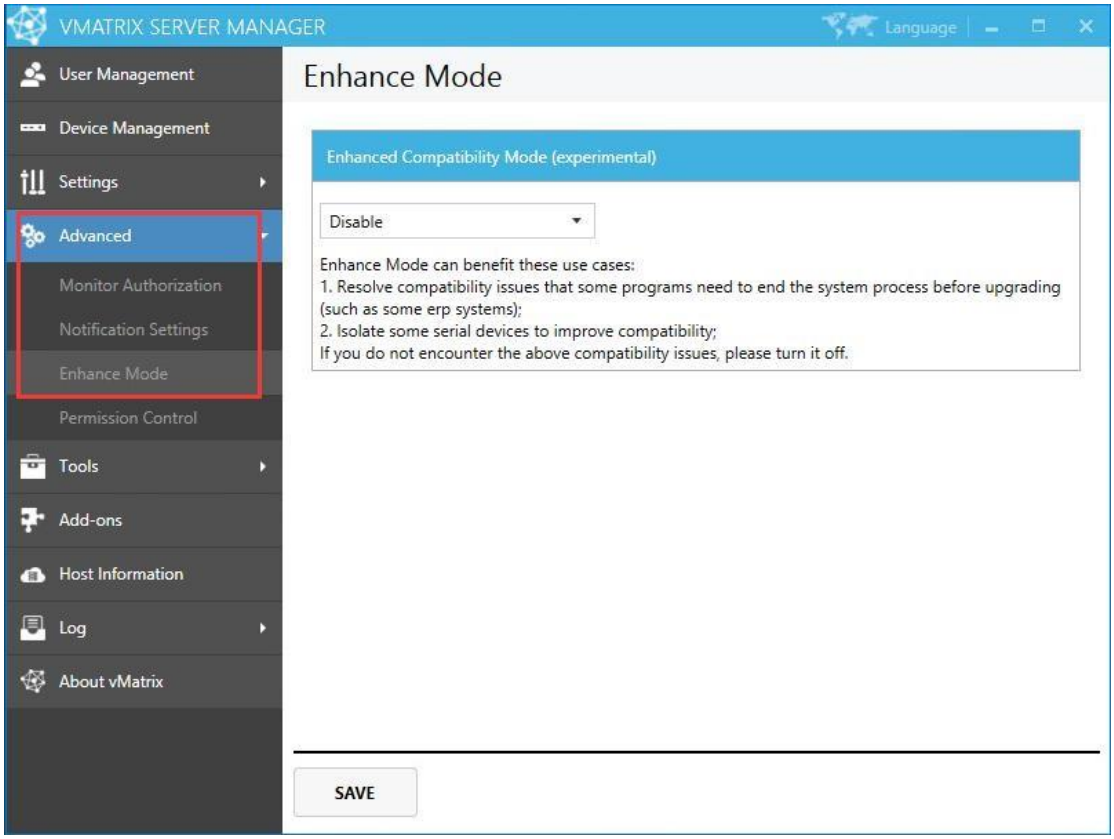
2) Select the sound effect. Depending on the system, the default sound effects will be Hand, Asterisk, Beep, Exclamation, Question or muted. You can also use a custom sound file in *.wav format. Click “Save” to complete the setting. When a client device disconnects, the administrator will see a bubble prompt with sound alert.



5.4.3 Enhancement Mode

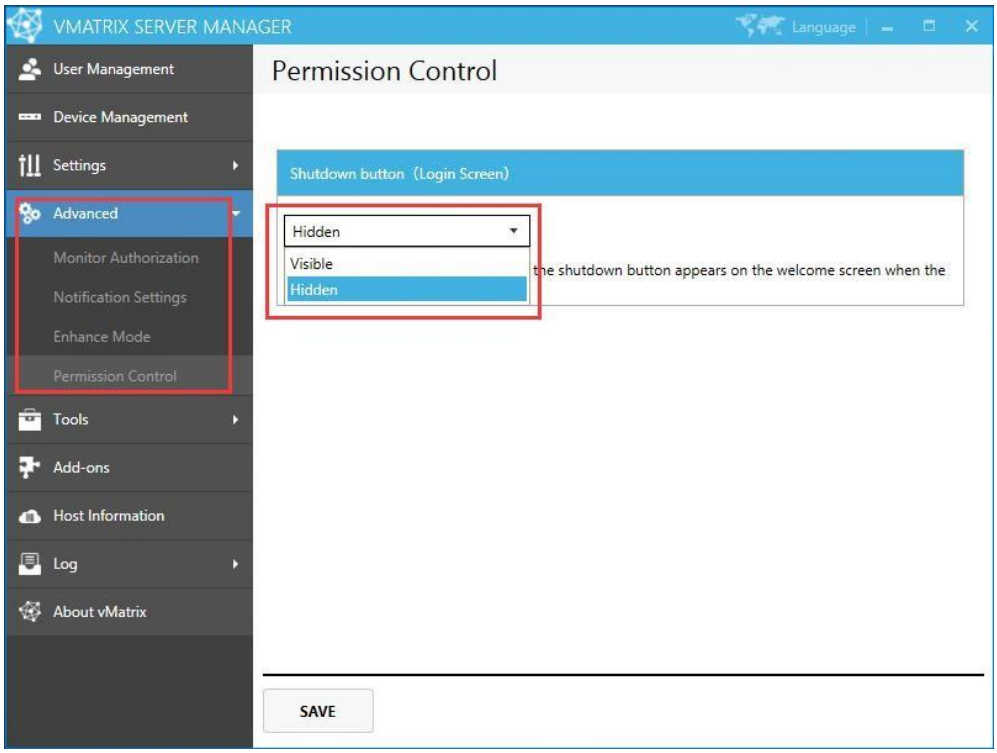
Enhancement Mode may solve compatibility issues that some programs need to end the system process before upgrading (such as some erp systems) or isolate some serial devices

to improve compatibility. If you do not encounter the above compatibility issues, please turn it off.



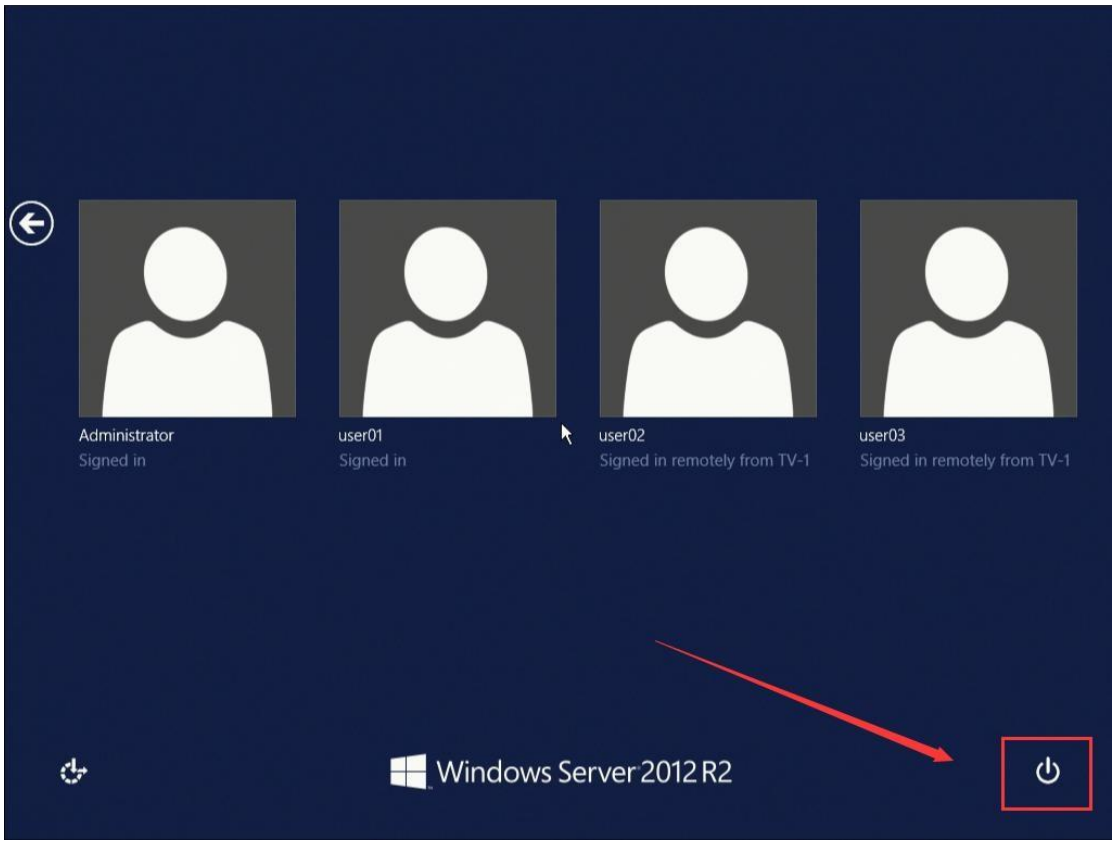
5.4.4 Permission Control

The switch controls whether the shutdown button appears on the welcome screen when the terminal is logged in anonymously.



- **Hidden:**

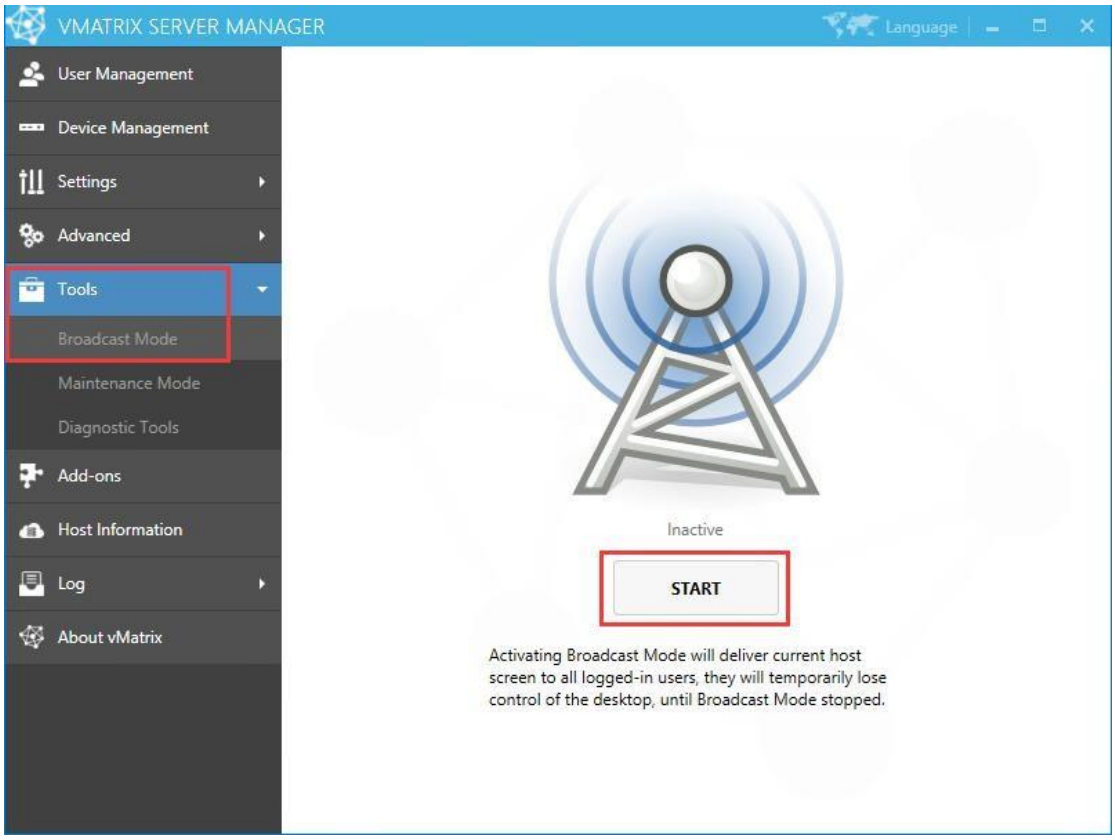
- **Visible:**



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:

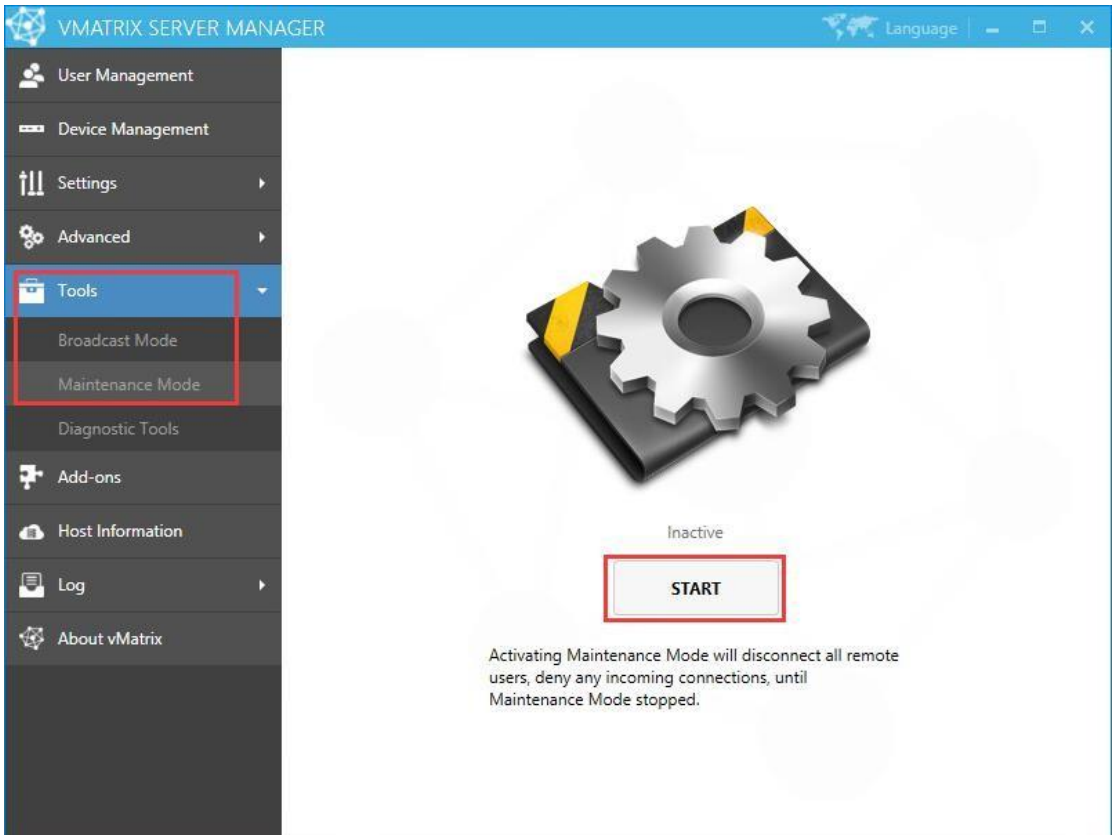
1) Users who latter connect to the host after Broadcast Mode activation will also lose control of their desktops and be given the host screen at the moment they enter their sessions.

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

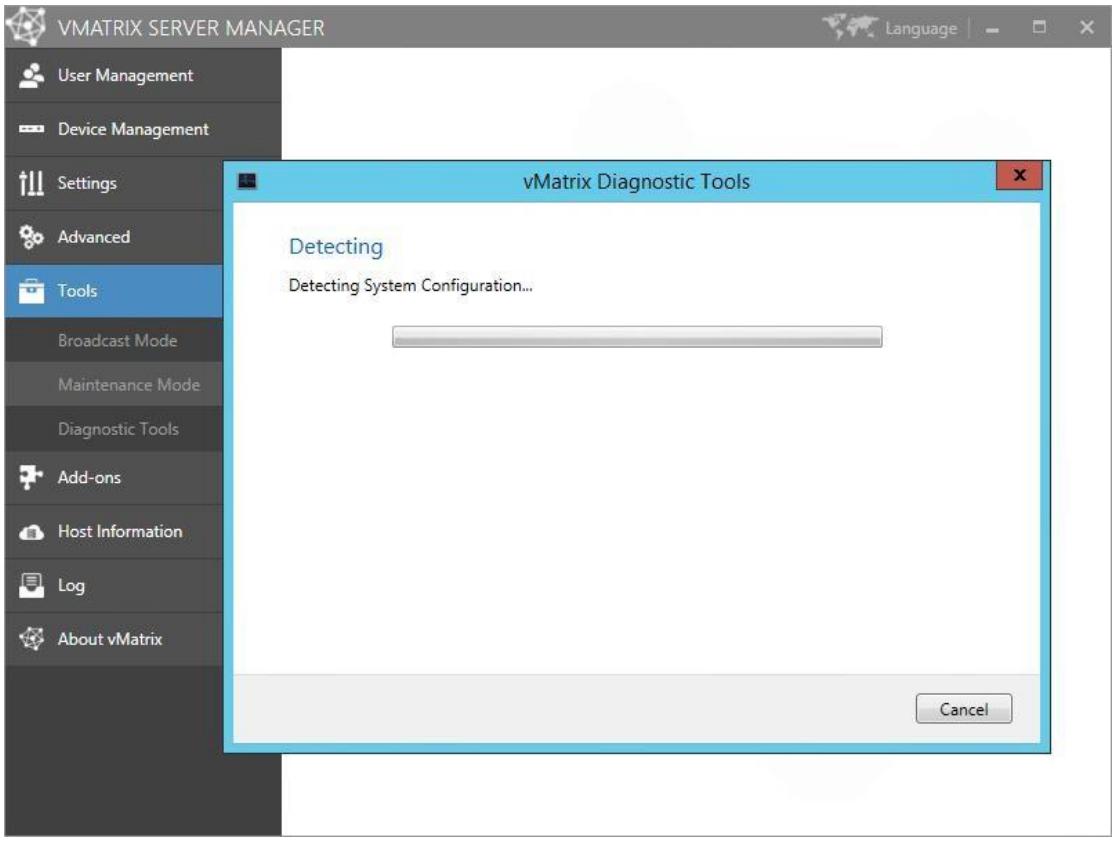
Activating Maintenance Mode will disconnect all connecting users and also deny any incoming connection requestfrom users. This is often used when the host is under maintenance.



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.

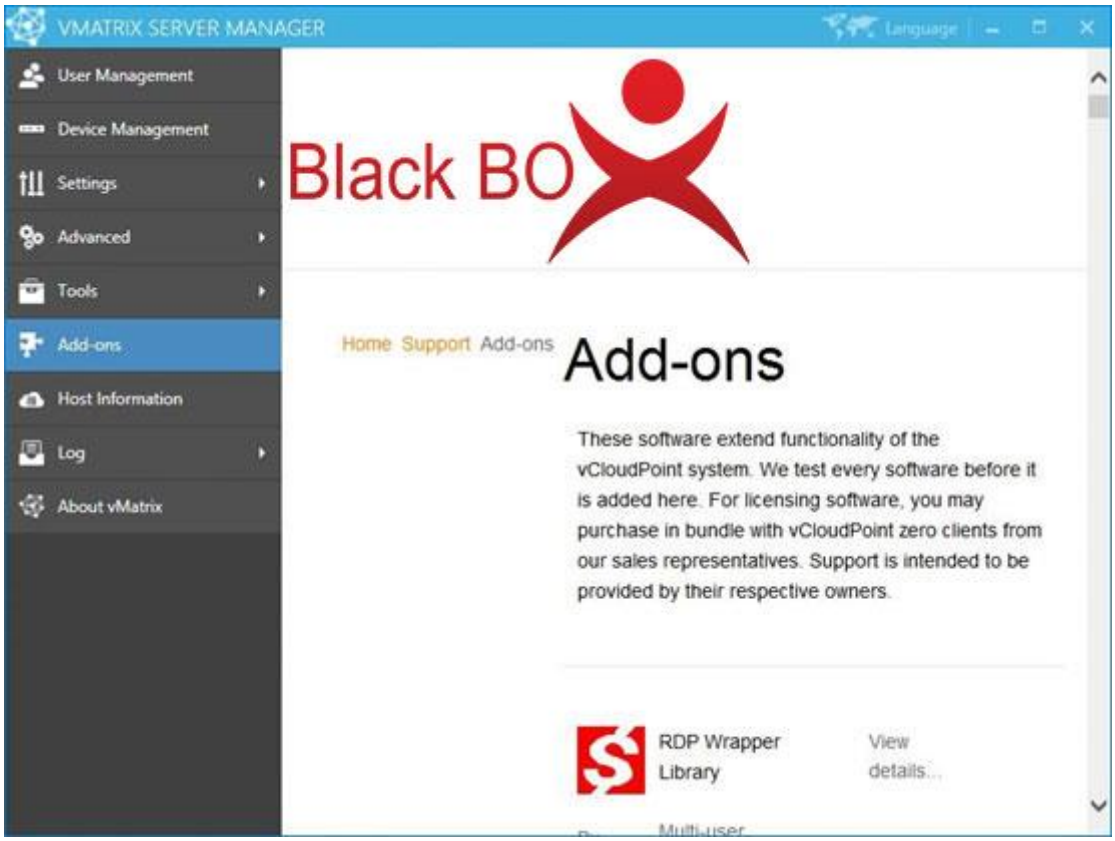
5.5.3 Diagnostic Tools

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

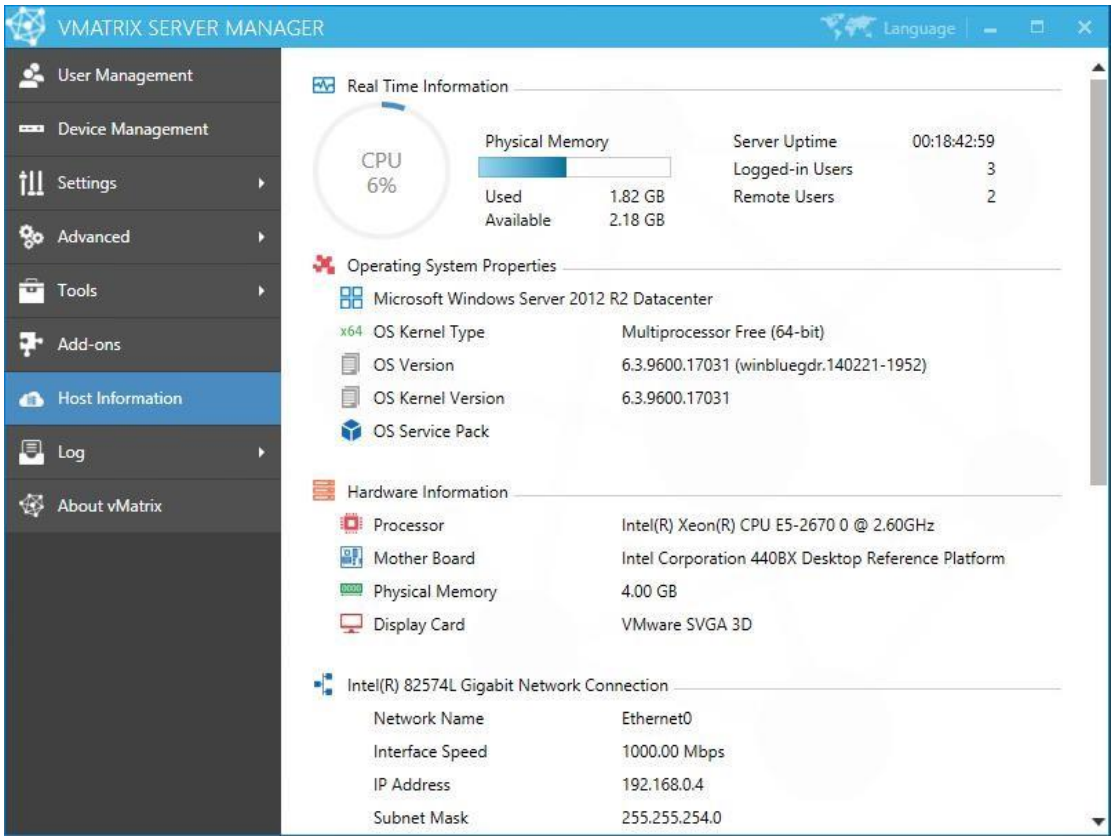
This page contains recommended software that may extend functionality of the BlackBox System or are frequently used with BlackBox products. The software has been tested compatible with the BlackBox system.



Note: this page connects to web page on BlackBox 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

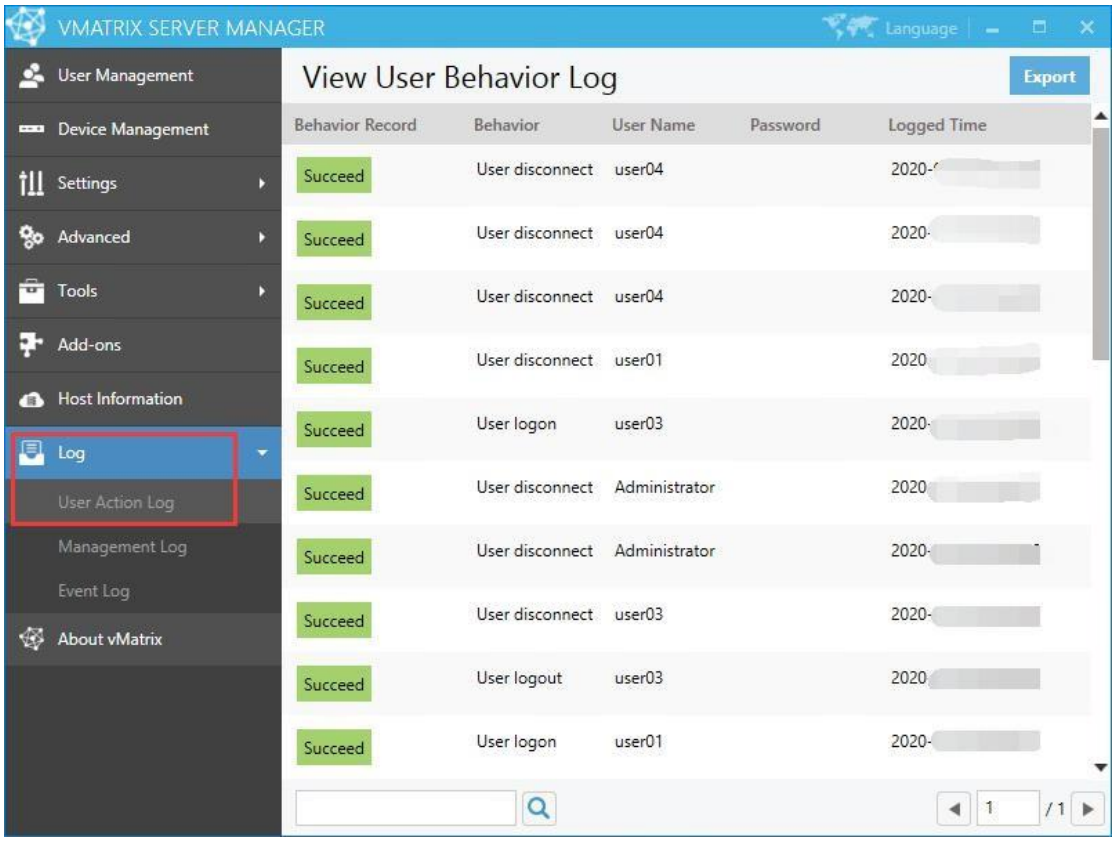
This page provides an overview of the host information including real time resources consumption, operating system, hardware and network.



5.8 Log

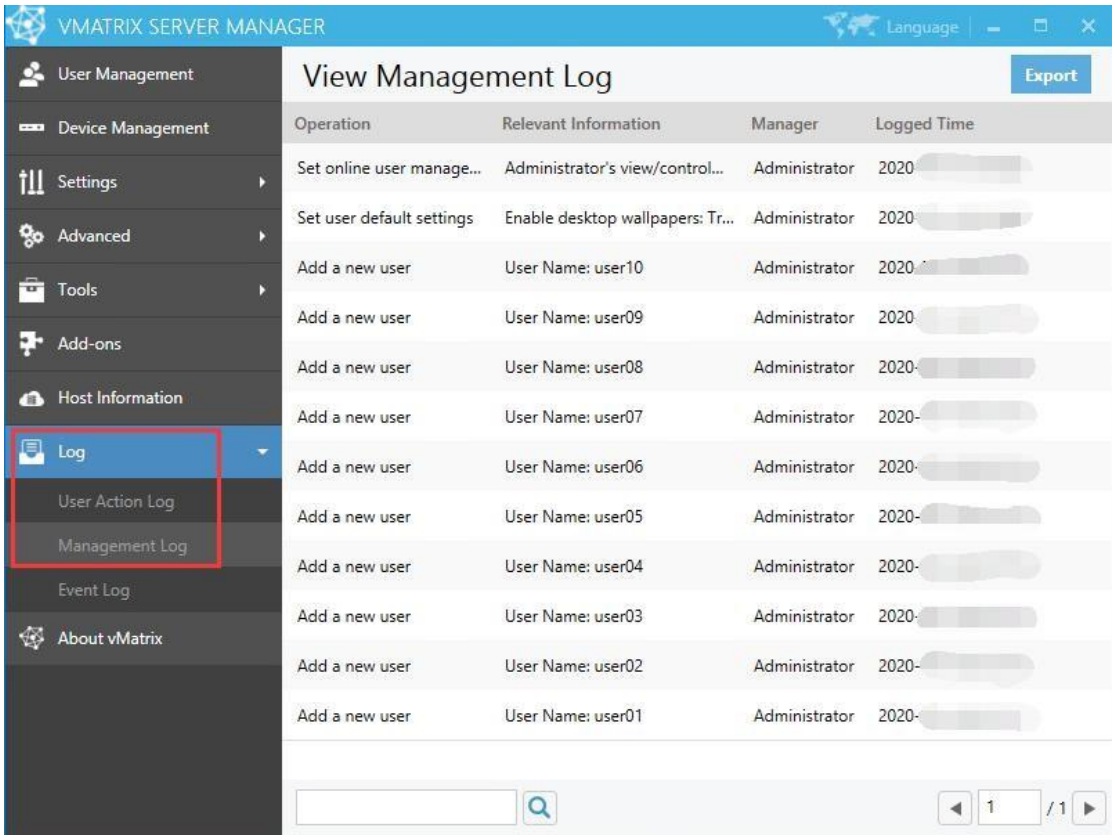
5.8.1 User Action Log

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



5.8.2 Management Action Log

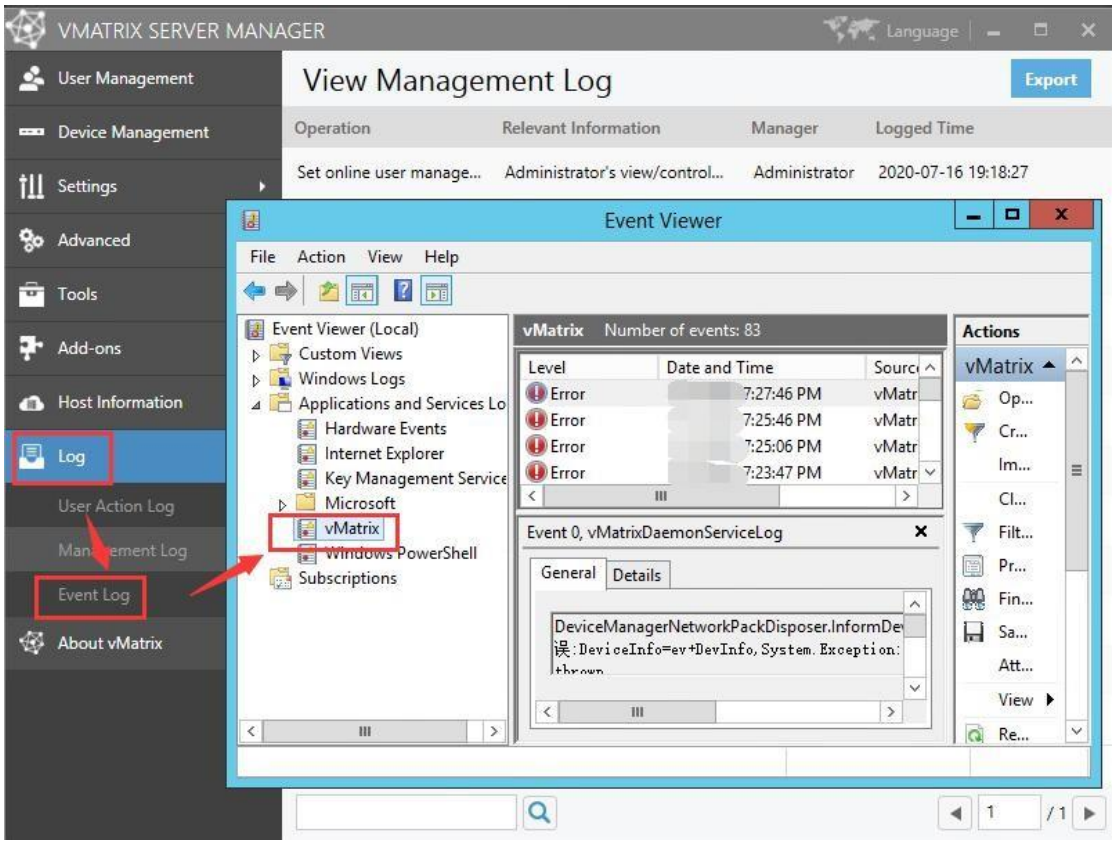
You can view all management actions since the installation of vMatrix Server Manager.



Note: This is where you can view the setting history of Monitor Authorization to avoid administrators overuse of monitoring over user desktops.

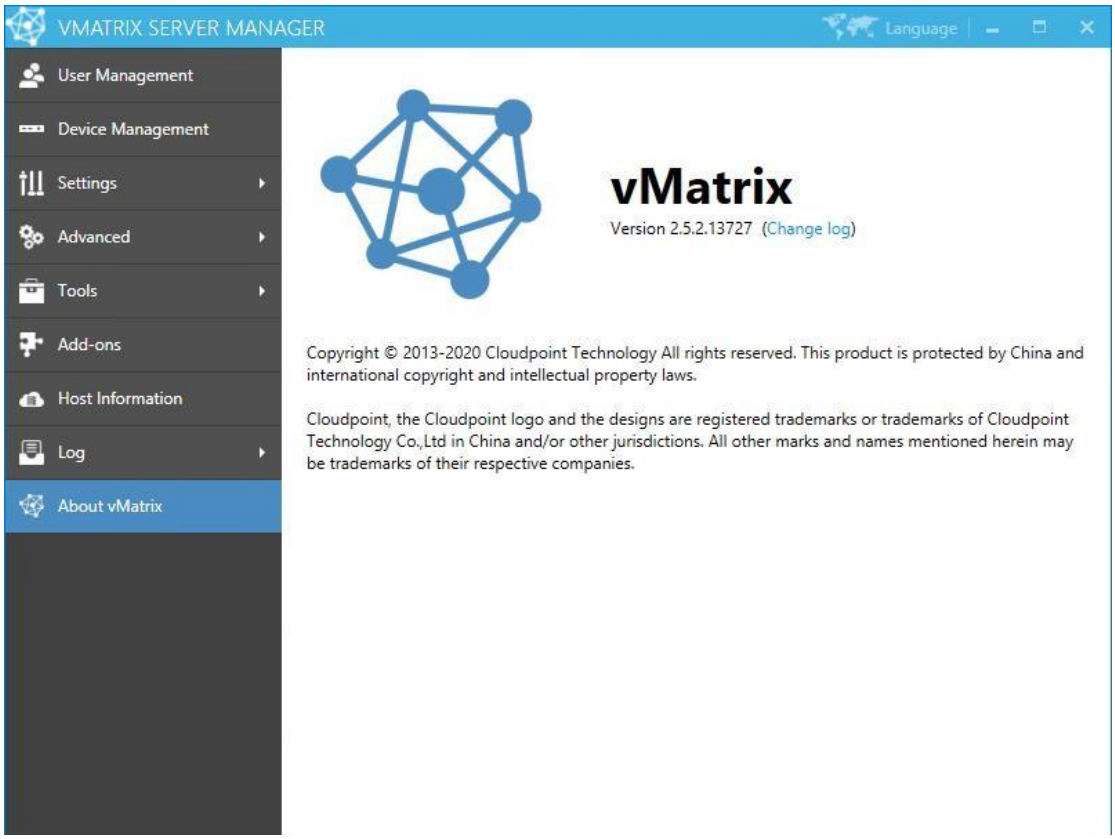
5.8.3 Event Log

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 BlackBox 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.)



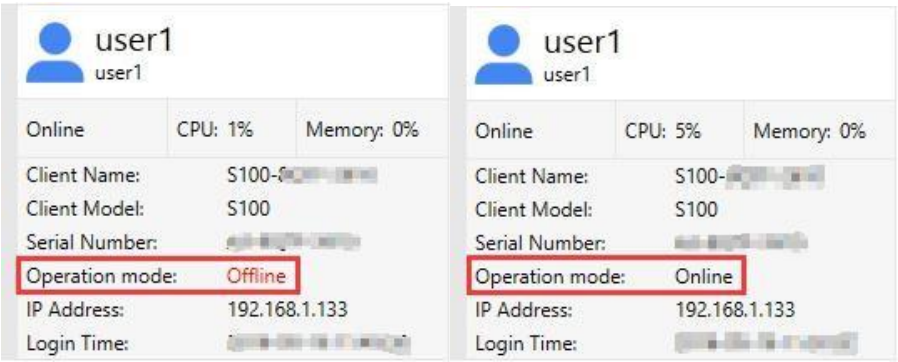
5.9 About vMatrix

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, BlackBox 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. The Operation Mode displayed on the User Management page of any device connecting to the host will automatically change from “Offline” in red to “Online” in black, meaning the device is properly working in an internet provided environment.



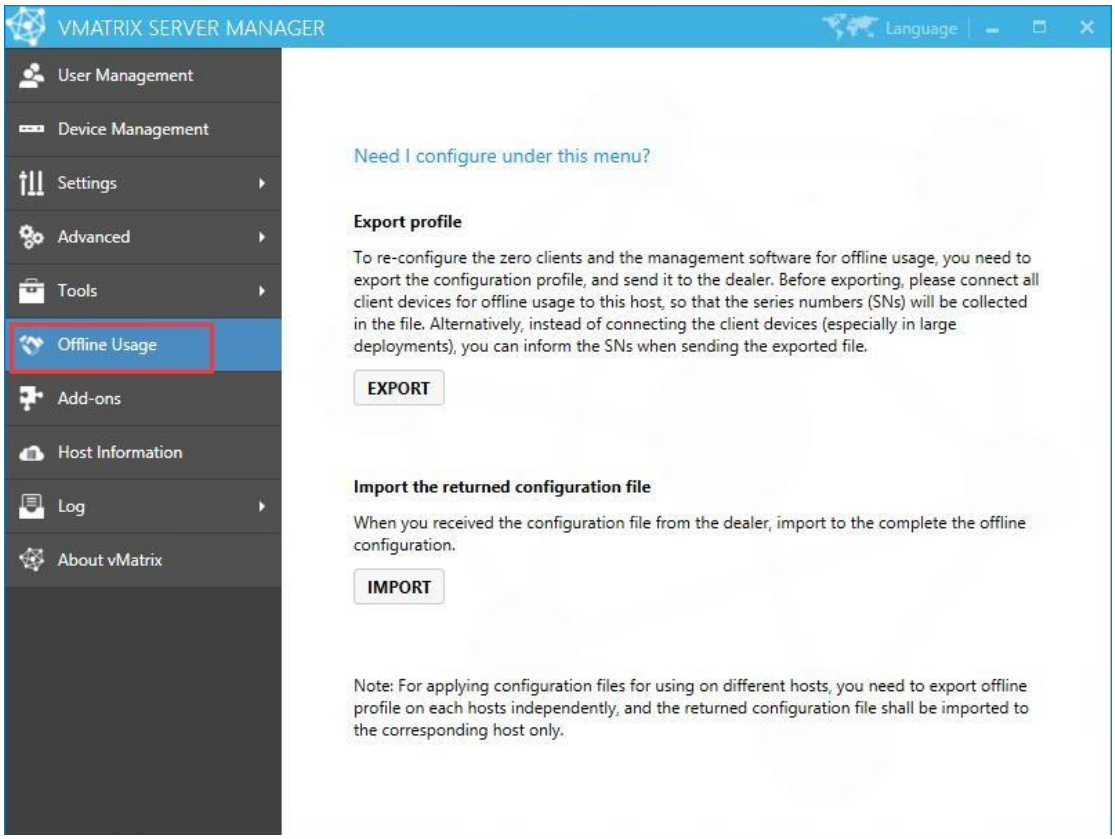
However, if the Operation Mode of the devices connecting to the host stays “Offline” in red all the time, you have to re-configure the devices for offline usage, otherwise the devices may be disconnected in every few minutes during operation. Use cases where you may encounter this problem and need to 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: api.cpterm.com.

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.

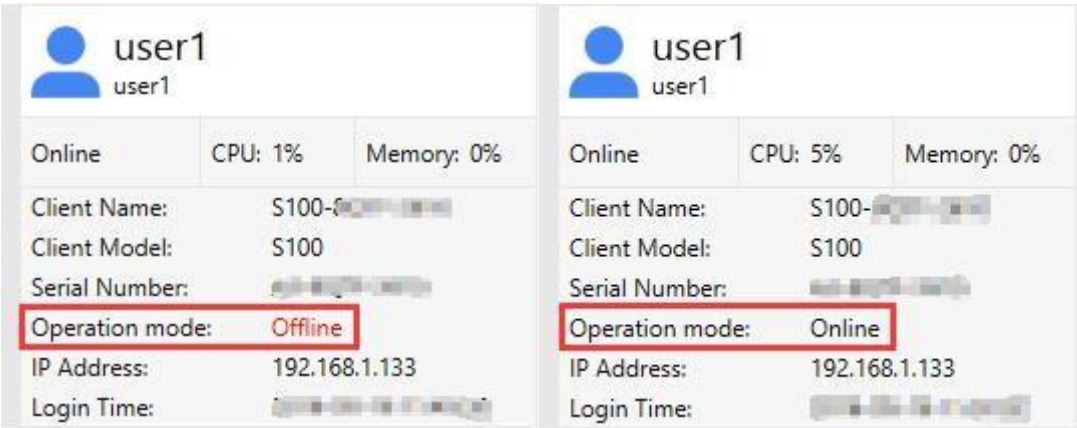
2) Open vMatrix Server Manager, go to Offline Usage page (this page only appears when the host is not provided with internet connection on system boot).



3) Export the configuration profile, and send it to the dealer. 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 (es pecially in large deployments), you can inform the SNs when sending the exported file.

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.

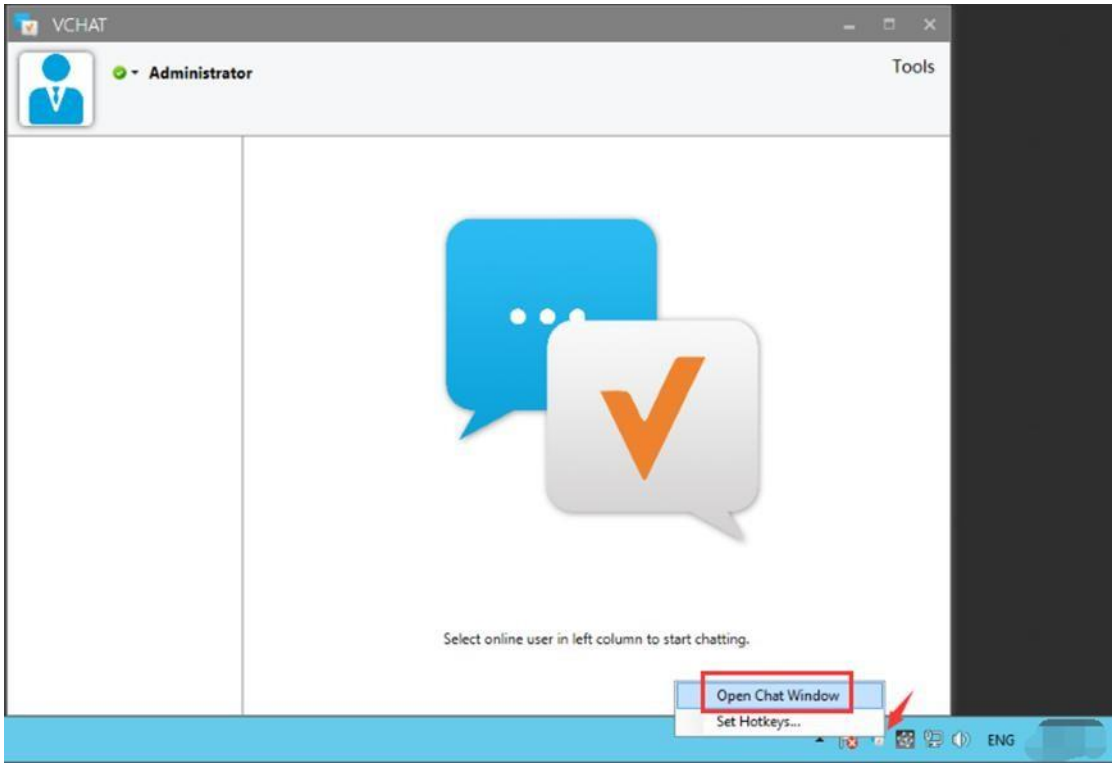


Note: Offline usage configuration on vMatrix Server Manager was introduced in the release of vMatirx Server Manager 2.0.2 version, if you are planning to use the BlackBox zero clients in a non-internet or unstable internet environment, please use 2.0.2 or a later version of vMatrix Server Manager, and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

5.11 More Tools & Settings

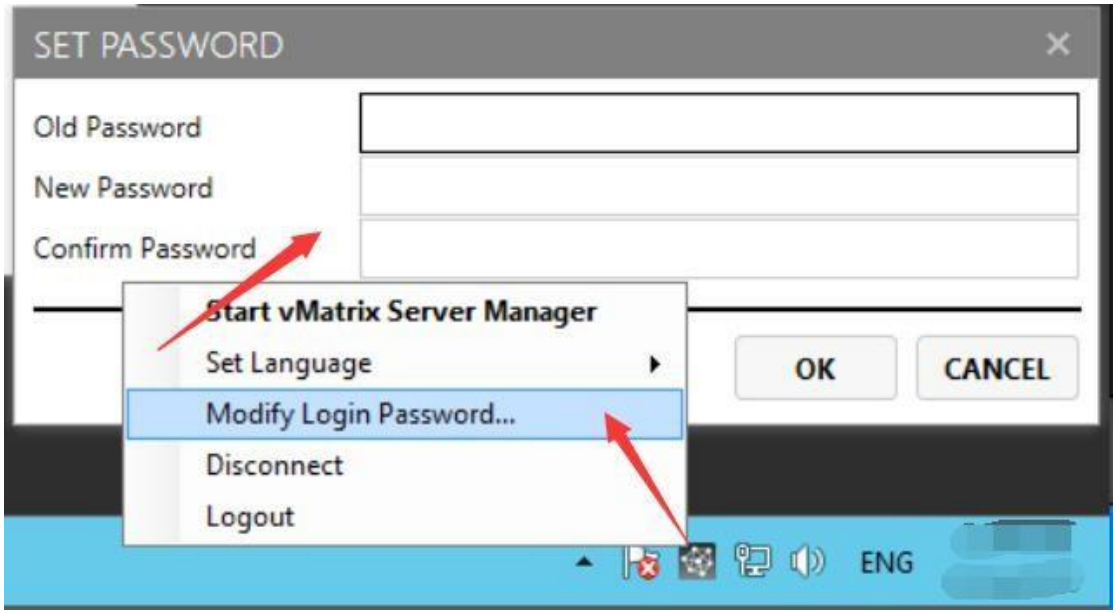
5.11.1 Chat Tool

The Chat Tool allows users to talk with other users connecting to the same host. To run the Chat Tool, right click on the vMatrx icon at the task bar and then click “Open Chat Window”.



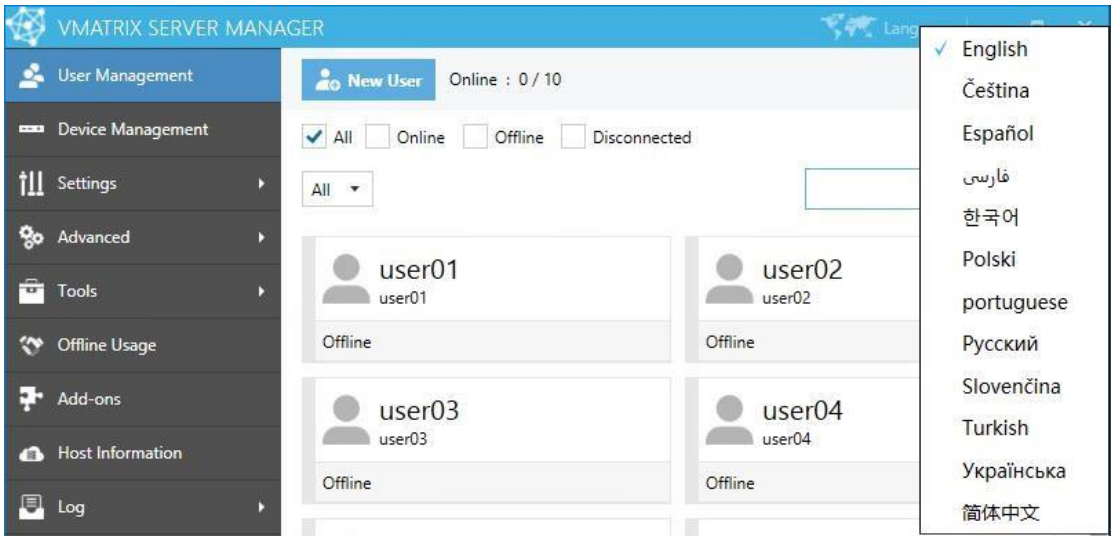
5.11.2 Password

This allows the current user to reset their login password without doing it 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 in the required fields.



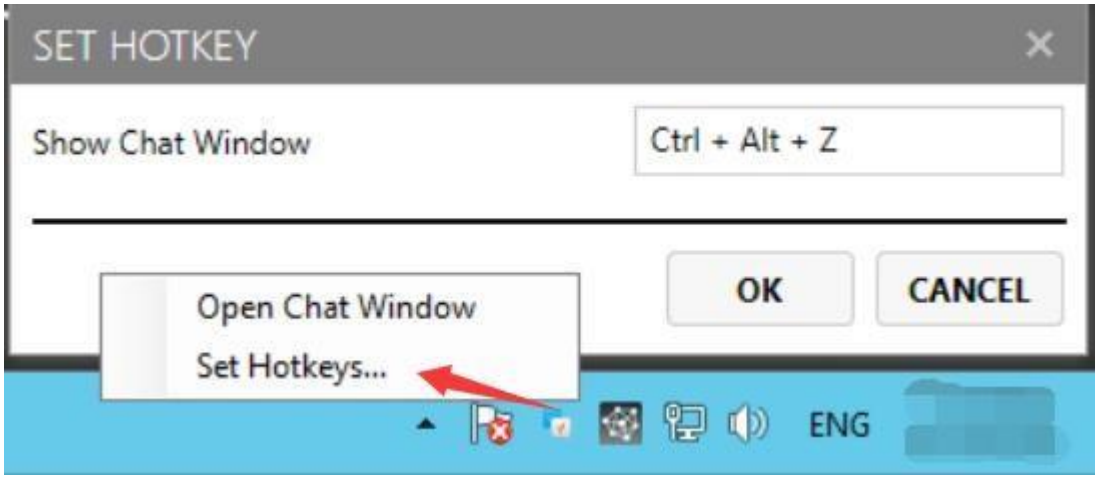
5.11.3 Language

This is to set language used by vMatrix Server Manager. Right click on the vMatrx icon at the task bar, click on “Set Language” and then available languages will be shown on the right. You can also change language at the right top bar on vMatrix Server Manager.



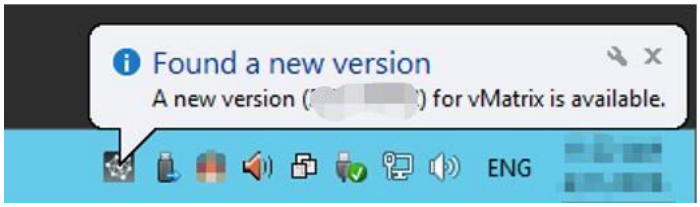
5.11.4 Hotkeys ...

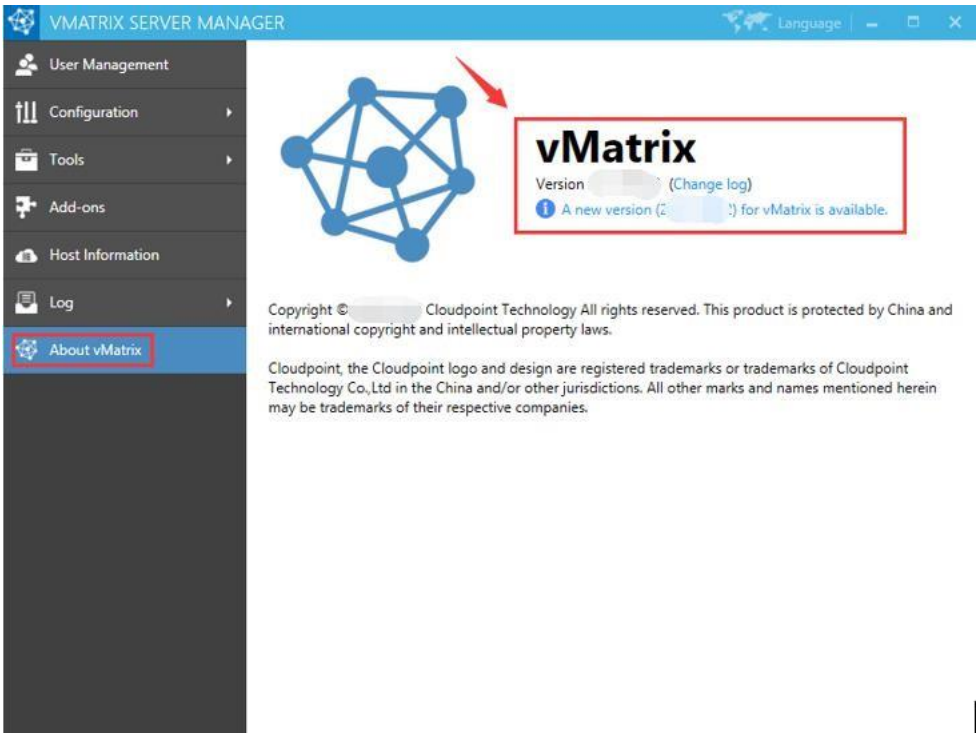
This is to set hotkey to open the vChat window. To ensure the hotkey works, do not use the same combination of keys for other applications.


SET HOTKEY
Show Chat Window
Ctrl + Alt + Z
OK
CANCEL
Open Chat Window
Set Hotkeys...
ENG

5.12 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 BlackBox website.

After downloading, follow the steps below to update:

1) Log out all users and disable security software to avoid mistaken report on vMatrix Installation files.

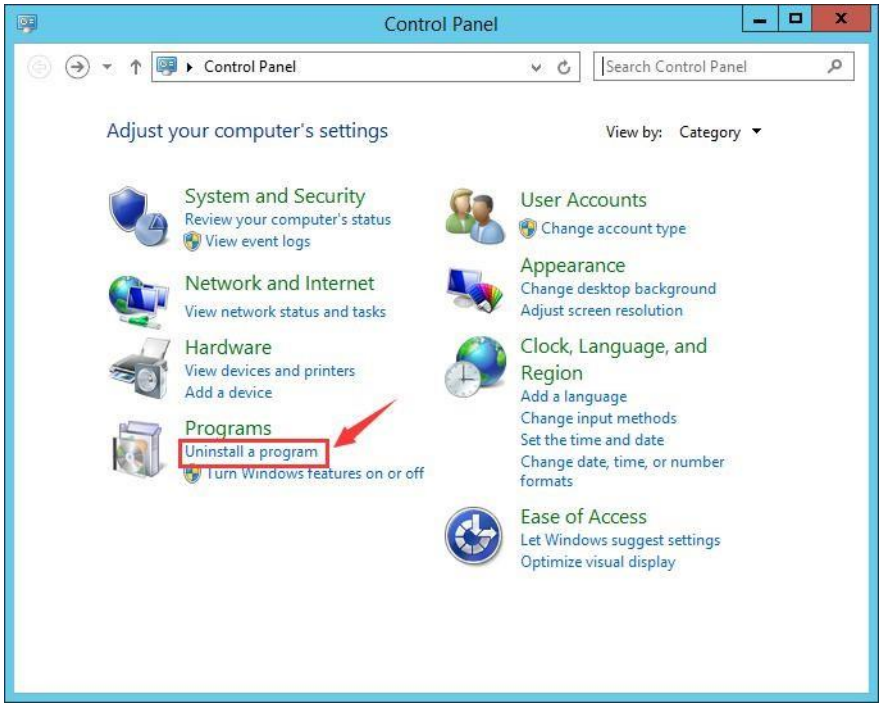
2) Run the installer and process as it is done on initial installation.

3) Reboot system after installation completes.

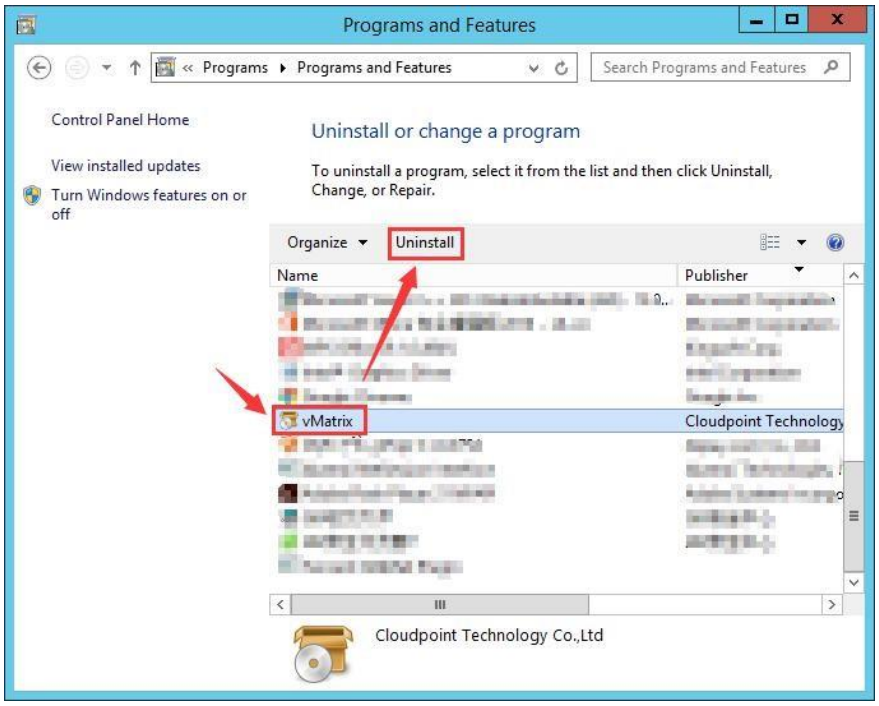
4) Check if there is any new device firmware at the device UI. If yes, then update.

5.13 vMatrix Uninstall

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

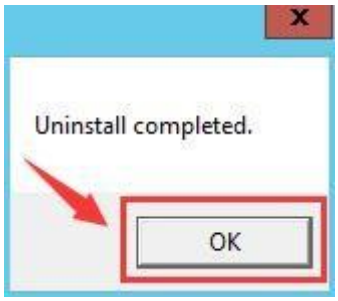


2) Select “vMatrix”, and then click to uninstall.



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

4) Click “OK” when uninstall completes.



Chapter 6. Trouble-shootings

Q1, My zero clients get disconnected every a few minutes.

By factory default, the BlackBox zero clients and the management software are configured to be used in an internet connected environment (WAN). If you are using them in a non-internet environment, you have to re-configure the zero clients and management software by simply following the guides at the Offline Usage menu on vMatrix Server Manager, otherwise, sessions will time out (disconnected) during operation.

Offline configuration is required if your actual use case meets any of the following conditions:

- 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: api.cpterm.com.

Q2, The host is not shown in host list.

1) The vMatrix Server Manager software is not installed on the host or not working properly.

Solution: Install or re-install vMatrix Server Manager.

2) There is network problem between the host and the zero client.

Solution: Ping the host to see if the host responds to the zero client. If not, check the network connection of the zero client and the host.

3) The zero client is with a new firmware version while the vMatrix Server Manager version on the host is out of date.

Solution: Upgrade the vMatrix Server Manager.

4) IP Addresses in the DHCP pool have been used up so that new connected zero clients cannot find hosts in the LAN while the old connected zero clients do not have the problem.

Solution: Go to the DHCP setting page and enable more IP addresses or shorten the time of IP address tenancy.

Q3, Cannot log into the selected host.

1) A pop-up window says that the device's serial number is invalid.

Solution: Contact our technical support team with the device's serial number.

2) Unstable Local Area Network (LAN).

Solution: Examine cable and switch and make sure the zero clients are connected to the host in the same LAN.

3) IP address pool is full that new devices cannot login.

Solution: Lease more IP addresses, and recommend shorten IP address tenancy time in case there is a plenty of mobile devices connecting to the same network.

4) IP address conflict that the sign-in of one user may log the other out.

Solution: Make sure all devices use different IP address from the others in the same LAN. Recommend using default DHCP instead static IP addresses.

Q4, USB devices do not work, there is no sound or there are lags on scrolling or playing a video.

If you have one or all of the above problems, you may probably see "cpaccel.exe" (Cloudpoint Multimedia Accelerator) error message from Windows or by running vMatrix Diagnostic Tool. This is due to some file missing of vMatrix Server Manager, mainly caused by mistaken removal or block of fire-wall or anti-virus software. The best and quickest way to fix this problem is to re-install vMatrix Server Manager (make sure you have disabled security software before installation). If you still have this problem in use, you may have to add vMatrix files or ports to exception list of security software. Also refer to How to Configure Firewall and Antivirus software for BlackBox Products on this page.

P5, Forget the password for device lock.

Press F2 on device boot to clear device configurations.

Q6, Forget the password for settings lock.

Long press the switch button until you see the resetting window.

Q7, Monitor displays “out of range” message or turns blank when connecting to a zero client or the user session entering Broadcast Mode.

1) the zero client is preset a desktop resolution (e.g.: 1920x1080) that is not supported by the monitor (e.g.: maximum resolution support of the monitor is 1440x900).

Solution: press F2 on device boot to restore desktop resolution to default 1024x768.

2) the desktop resolution on the host is not supported by the monitor connecting to the zero client. (When entering Broadcast Mode, the user session will switch the desktop resolution to that used by the host.)

Solution: lower desktop resolution used by the host to the one supported by the monitor connecting to the zero client.