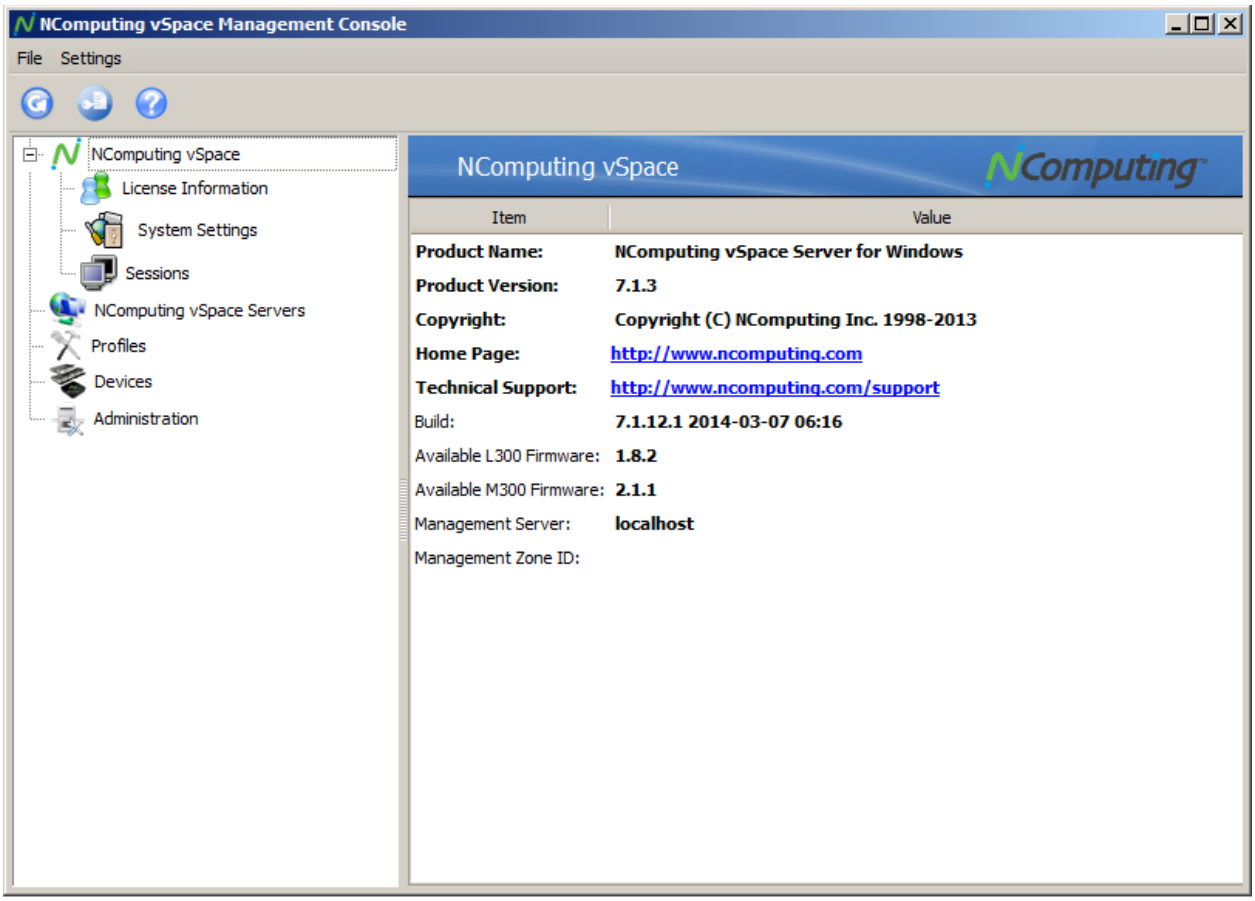
vSpace Server 7.1



User Manual

Important Notices

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

NComputing reserves the right to make improvements and/or changes to this User Manual and to the products, programs and/or specifications described herein at any time without notice. Information contained in this document may have been obtained from internal testing or from a third party. NComputing 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 Manual can be downloaded from the "Documentation" page in the Support section of the NComputing website at: www.ncomputing.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. It is your responsibility to download a copy of the warranty at the time of purchase to keep for your records. The warranty can be downloaded from the "Documentation" page in the Support section of the NComputing website.

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 NComputing 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 high-resolution graphics applications or 3D games that are designed to be supported by stand-alone computers. 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 NComputing systems. Additional software licenses may be required.

Microsoft® Windows® Licenses. You are licensed by NComputing to use the vSpace Server software under the terms of the EULA. You must also acquire the appropriate number of Windows Server licenses and Client Access Licenses for each device or user accessing Windows Server software. You cannot use the vSpace Server software with Windows Client software (i.e., Windows Vista, Windows 7) 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 or as expressly set forth in the "Microsoft Windows Server to Windows XP License Rights" section of the NComputing EULA. In all cases, your rights and obligations with respect to the use of vSpace Server software with Windows Server software and Windows Client software are defined by both the NComputing vSpace Server software EULA and the applicable Microsoft Software License Agreement or EULA. For more information on licensing with Microsoft operating systems see: www.ncomputing.com/mslicensing For single user applications of your L-series product such as remote control, digital signage and 1:1 VDI refer to the same web page for information on client operating systems currently supported.

The NComputing hardware and software products described in this user manual are protected by numerous granted and pending U.S. and international patents. Some components of NComputing products utilize open-source software. Please refer to the GPL Declarations section of this User Manual for more information.

TABLE OF CONTENTS

1.0 Getting Started

Before beginning, make sure you've downloaded the latest version of vSpace for your selected operating system. For the purpose of this document we will be using **vSpace 7.0** in conjunction with the **L300** and **M300** access devices. While certain examples given herein highlight the L-series specifically, it should be noted that the L-series and M-series share nearly identical configuration options.

> **NOTE:** Unless otherwise instructed by an NComputing Support or Engineering representative, it is recommended that vSpace Server 7 be installed using the "clean install" method, meaning that it should not be installed over top of a previous version of vSpace. Any previously existing vSpace software should be uninstalled before proceeding. When possible, we recommend a clean OS install or re-imaging of a system prior to installing vSpace.

1.1 Installing vSpace

Launch the vSpace Server 7 installer, and proceed through the initial screens until you are prompted to select an installation folder. On this screen you will see check-boxes marked "Slave Only", "Enable Discovery", and "Set Remote Management Server".

- **Default Setting (nothing checked):**
  By default, nothing is checked. In this configuration, the vSpace 7 server will assume the role of "master" if no other vSpace 7 server in its subnet has that role. If it discovers a server that is already performing the master role, it will automatically slave to that server.
- **Slave Only:**
  By checking this box, your vSpace 7 server will look for an existing master server to slave to.
- **Enable Discovery:**
  If you have selected "Slave Only" mode, checking Enable Discovery will allow your server to automatically search for and join a master server within its subnet. In the event that no master server exists, the server will function normally except that it will only be able to "see" and manage devices that are connected to it. If a master server is introduced into the subnet at a later time, your server will automatically discover and slave to that server.
- **Set Remote Management Server:**
  If you have selected "Slave Only" mode, checking Set Remote Management Server allows you to specify an existing master server by specifying its IP address. This address can be outside your server's subnet, provided your network routing rules allow for communication to the specified IP.

Once you have selected the options as desired, proceed with the remainder of the installation process. Be sure to reboot your server once the process is complete. The following section provides additional information on the order in which vSpace and vSpace Management Center servers should be installed and configured in relation to one another.

1.2 Server Install Order

vSpace Server 7 introduces several advanced management features and was engineered to work hand-in-hand with vSpace Management Center, NComputing's central management application. The following are recommended installation steps for vSpace-only, and vSpace + vSpace Management Center deployments.

Installing vSpace Management Center and vSpace 7 into a new Management Zone

When logistics allow, it is strongly recommended that your vSpace Management Center servers be installed before your vSpace 7 servers. The following install order represents the "best practice" when creating a new Management Zone under these conditions.

1. Install your master server first, ensuring that you've selected the "Master / Slave" role during install.
2. Install your remaining vSpace Management Center servers using the "Slave Only" role.
3. Install your vSpace 7 servers using the "Slave Only" role.

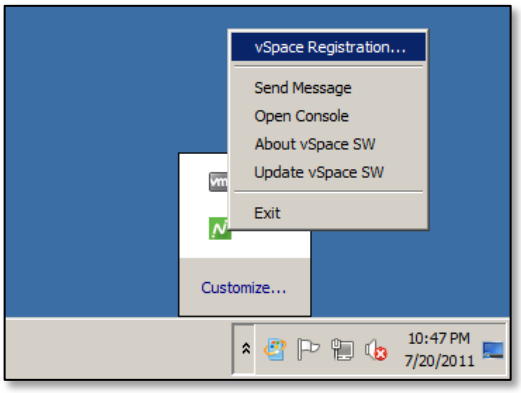
Installing vSpace 7 Only, Adding vSpace Management Center Later

When a deployment is designed to initially use vSpace 7 without vSpace Management Center, the following steps are ideal to ensure that - if vSpace Management Center is introduced at a later date - the transition is as smooth as possible.

1. Install your vSpace 7 master server first, ensuring that you've used the default, "nothing checked" option during install.
2. Install your remaining vSpace 7 servers using the "Slave Only" role.
3. When you are ready to introduce your first vSpace Management Center server into the Zone, Install the server you intend to use as your Master server first using the "Master / Slave" role. This will automatically slave the server to your existing vSpace 7 Master server.
4. Allow 24 hours for the database to propagate between vSpace 7 and vSpace Management Center.
5. Turn off your vSpace 7 Master server. This will cause your vSpace Management Center server to assume the Master role for your Zone.
6. Turn your vSpace 7 Master server back on. The server will now slave to your vSpace Management Center Master server automatically.
7. Install the remainder of your vSpace Management Center servers, using the "Slave Only" role.

1.3 Registering vSpace

Once vSpace is installed, register the host software by right-clicking on the NComputing icon in your system tray and selecting “vSpace Registration,” as shown in the image to the right.



This will launch the Registration Wizard and you will be guided through the remainder of the registration process. You can also access the registration wizard by going to Start -> All Programs -> NComputing vSpace -> vSpace Registration.

1.4 Connecting Your Devices

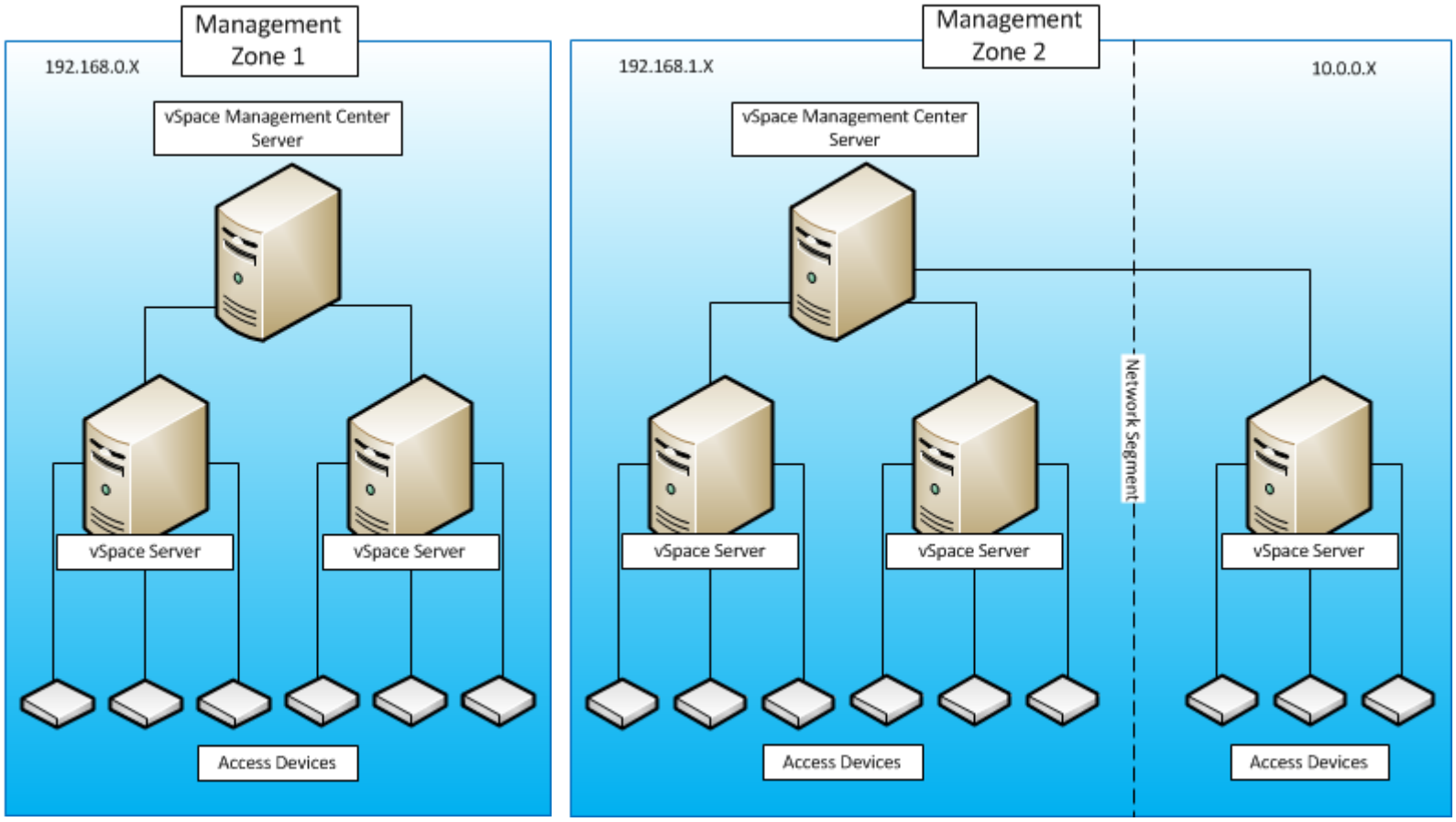
vSpace is now ready to accept connections from L and M-series devices. Keep in mind that, by default, your devices will automatically look for vSpace hosts on their designated subnet. You can alter this behavior from the devices themselves or from within the NC Console **(5.4 Connections Tab)** at any time.

Once they have connected and received a session, you should update the firmware for your access devices as soon as possible. Refer to device configuration in **Section 5.1**. Lastly, ensure that your devices are registered once they’ve accessed the server. By default, the registration process should be completed automatically within 24 hours of a device connecting to a server for the first time. You can verify a device’s registration status by selecting the Devices category of the left navigation tree within the vSpace Server Console. Registration status is displayed under the “Activation State”. You can learn more about reviewing device status in **Section 5** of this manual.

Depending on your selected operating system, further configuration steps may be required for the OS itself (such as adjusting Local Policies or User Groups). Be sure to review our general deployment checklist to ensure that your environment is properly configured to facilitate device sessions.
http://www.ncomputing.com/kb/NComputing-L-series-Deployment-Checklist_309.html

1.5 Management Zones

vSpace 7 organizes vSpace servers and NComputing access devices into Management Zones. Each zone can be comprised of several vSpace 7 servers, vSpace Management Center servers, and devices and exist within a single subnet or span multiple network segments. It is even possible to have a single Management Zone that spans multiple physical locations, provided the network joining those locations allows for communication between the affected segments.

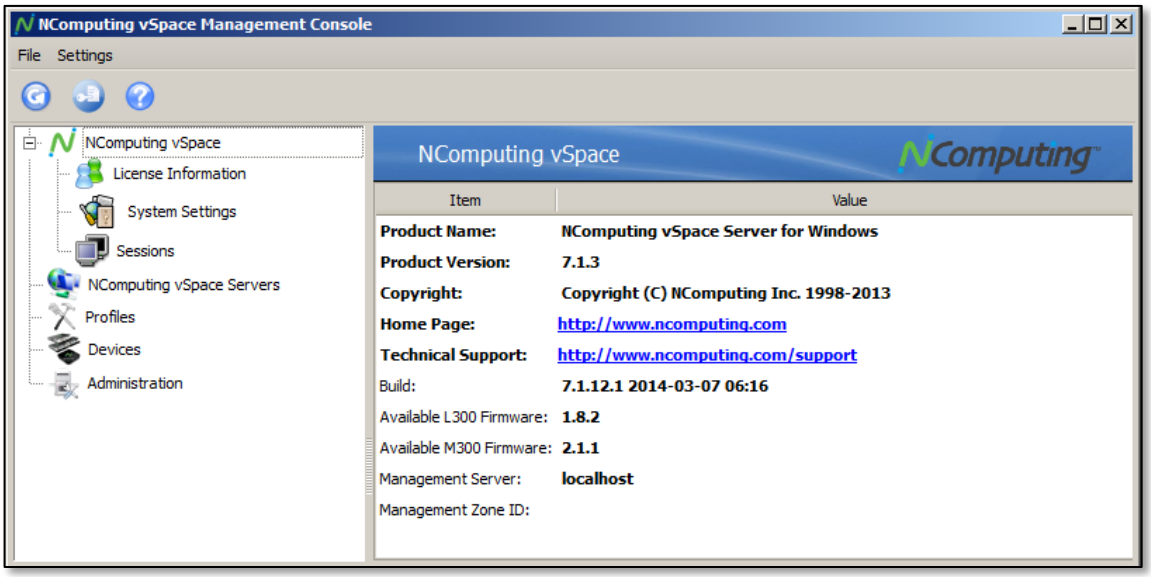


When there are multiple servers within a single Management Zone, one server acts as the master while the other servers are slaved to it. This can be a vSpace 7 server, or a vSpace Management Center server. You can designate a server as the master when it is created, provided there isn't already a master server within that Management Zone. During the installation process you can manually specify which Management Zone you wish a new vSpace Management Center server to join if a Zone already exists. Likewise, you can instruct access devices to automatically join a Zone if one exists within their subnet, or specify a Zone if you wish.

2.0 NComputing vSpace

2.1 vSpace Information

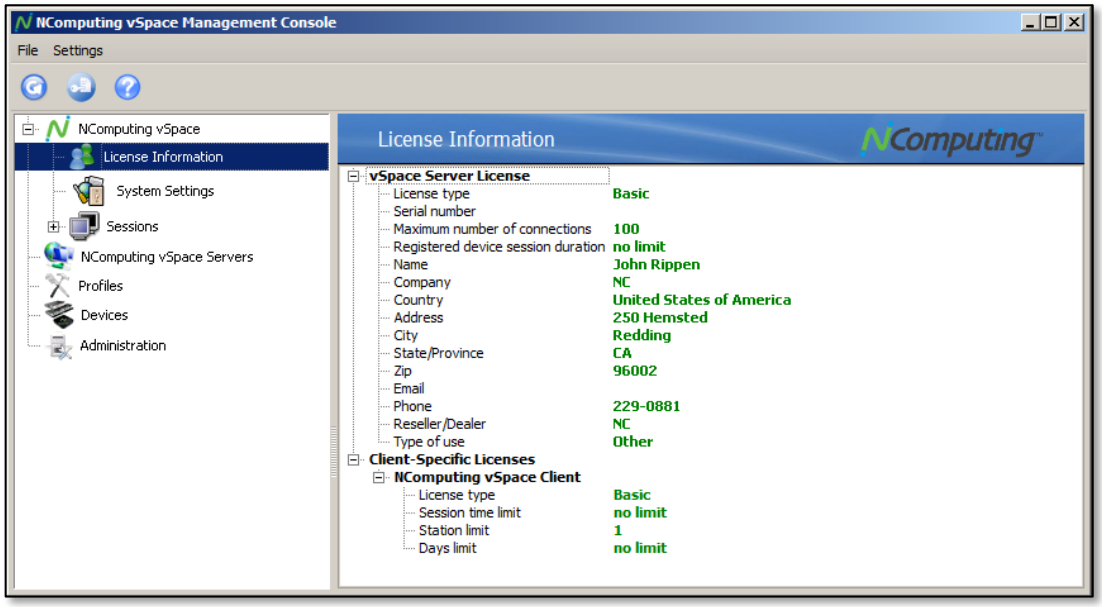
Launch the vSpace Management Console by navigating from the Windows Start button to “NComputing vSpace,” and then click on “NC-Console.” Once the console launches, left-click on the “NComputing vSpace” section of the left navigation tree to display information on the current vSpace build installed on your host. The vSpace Information screen provides the following information:



Product Name	The product name of the current NComputing software installed on the host
Version	The version number of the vSpace build currently installed
Copyright	vSpace Copyright information
Home Page	The official NComputing website URL
Technical Support	The official NComputing Technical Support URL
Build	The version number and build date of the current vSpace Server installation
Available (L300 / M300) Firmware	Indicates the current firmware version available for download from this host
Management Server	Under normal circumstances, this field will list localhost as the Management Server.
Management Zone ID	Displays the ID of the Management Zone to which the vSpace Server currently belongs.

2.2 License Information

Left-click on the “License Information” section of the left navigation tree to display licensing information for the vSpace software on your host. The License Information screen provides the following information:

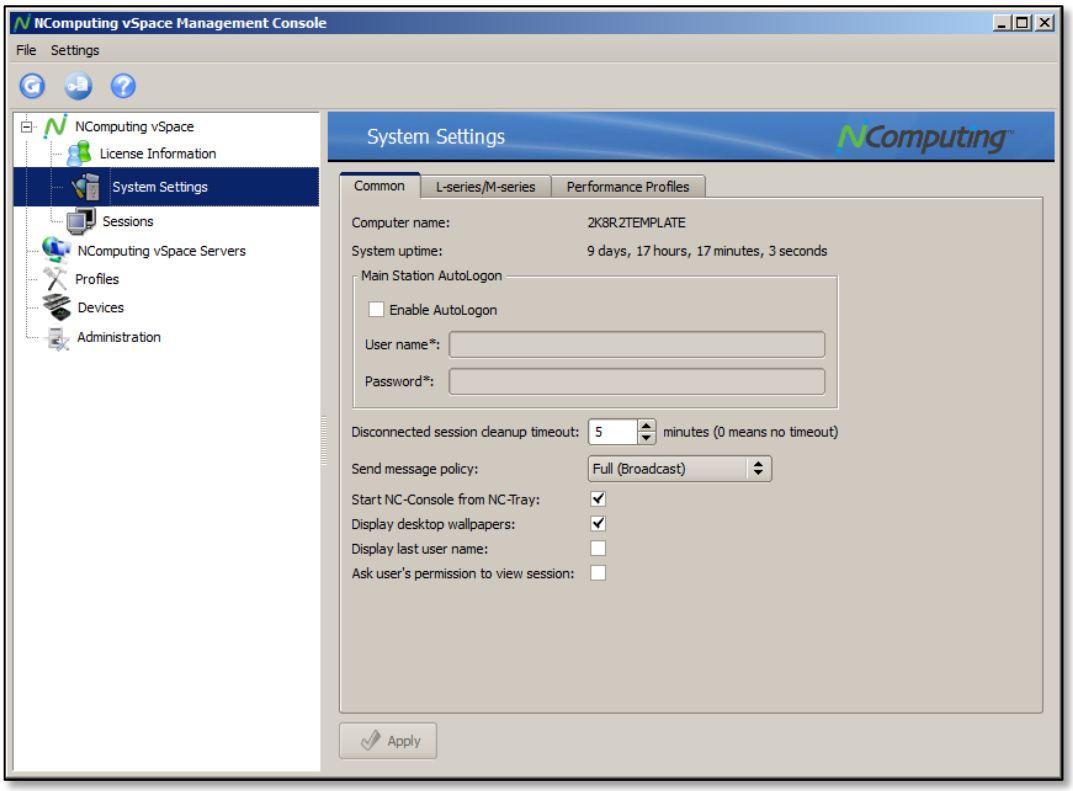


License Type	The type of license associated with the current vSpace install
Serial Number	The vSpace Server Software Serial Number
Maximum Number of Connections	The maximum number of simultaneous NComputing device sessions allowable under the current license
Registered Device Session Duration	The length of time each registered device is allowed to maintain a session
Name, Company, Country, Address, City, State, Zip, Email, Phone	Contact information and other details provided during registration
Reseller / Dealer	The Reseller or Dealer indicated during registration
Type of Use	The use-case indicated during registration
Client-Specific Licenses	Additional Client Device specific licensing information

NOTE: vSpace Server 7 includes a single complimentary vSpace CCU (Concurrent Connected User) license for remote administration and vSpace Client evaluation purposes.

2.3 System Settings - Common

Left-click on the “System Settings” section of the left navigation tree to display settings that affect the host, as well as devices that connect to it. The “Common” tab provides the following options and information:

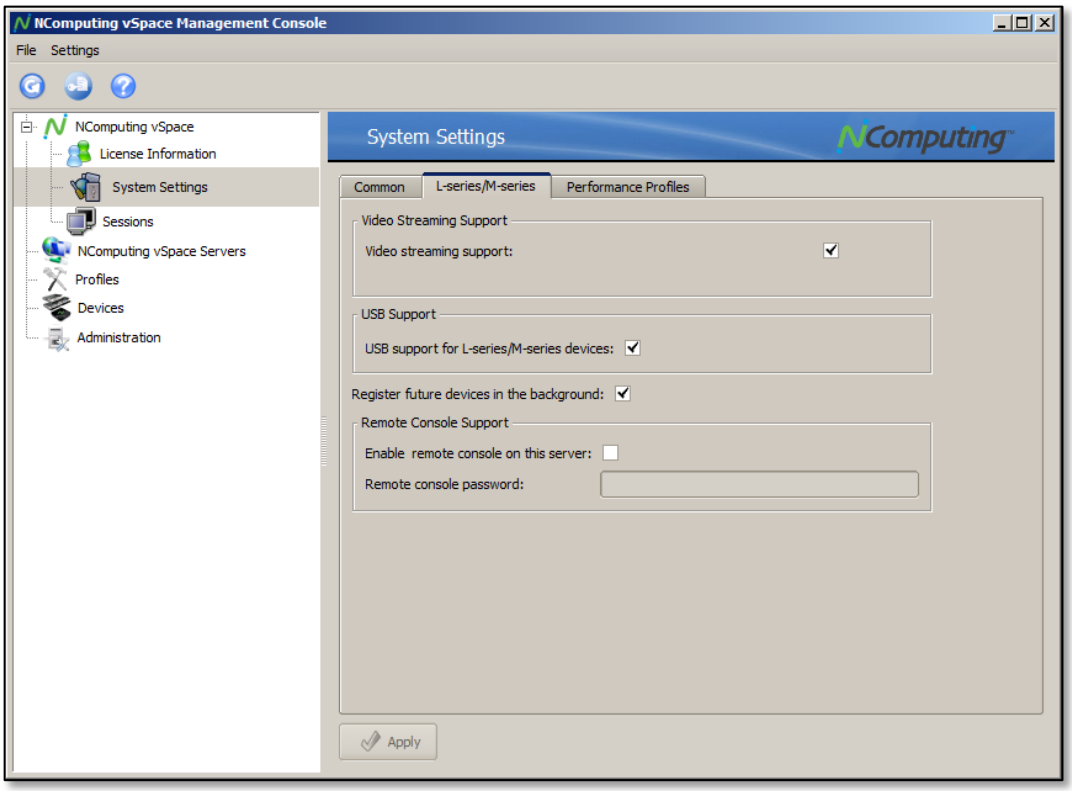


Computer Name	The system name of the vSpace host
System Uptime	Displays the length of time the host has been running without interruption. Reboots and shut-downs will reset this counter.
Main Station Auto Logon	Enabling this feature with a valid user name and password will cause the host to automatically log in to Windows when it boots. Otherwise, a user will need to manually enter a user name and password each time the host starts up.
Disconnected Session Cleanup Timeout	This value determines how long the host will wait before closing a user session after its device disconnects. A larger value provides a longer “grace period” during which users can re-connect their device without losing progress.
Send Message Policy	This setting controls the NC Message feature, which allows devices to send messages to each other. **Full** allows users to send messages to all connected devices. **Point-to-point** restricts messages to a single target device. **Disabled** turns this functionality off entirely.

Start NC Console from NC Tray	This setting determines whether the NC Console can be opened from the NC Tray icon in the task bar.
Display Desktop Wallpapers	Enabling this feature will allow device users to select and display custom Desktop Backgrounds within their Windows sessions.
Display Last User Name	Enabling this feature will auto-populate the user name of the last user to log in when a new user attempts to log in to Windows.
Ask User's Permission to View Session	Enabling this feature will prompt the target user session for permission if someone attempts to view their session through the NC Console.

2.4 System Settings – L-Series/M-series

The "L-Series/M-series" tab provides access to settings that control video streaming, USB support, and remote console support among other features.



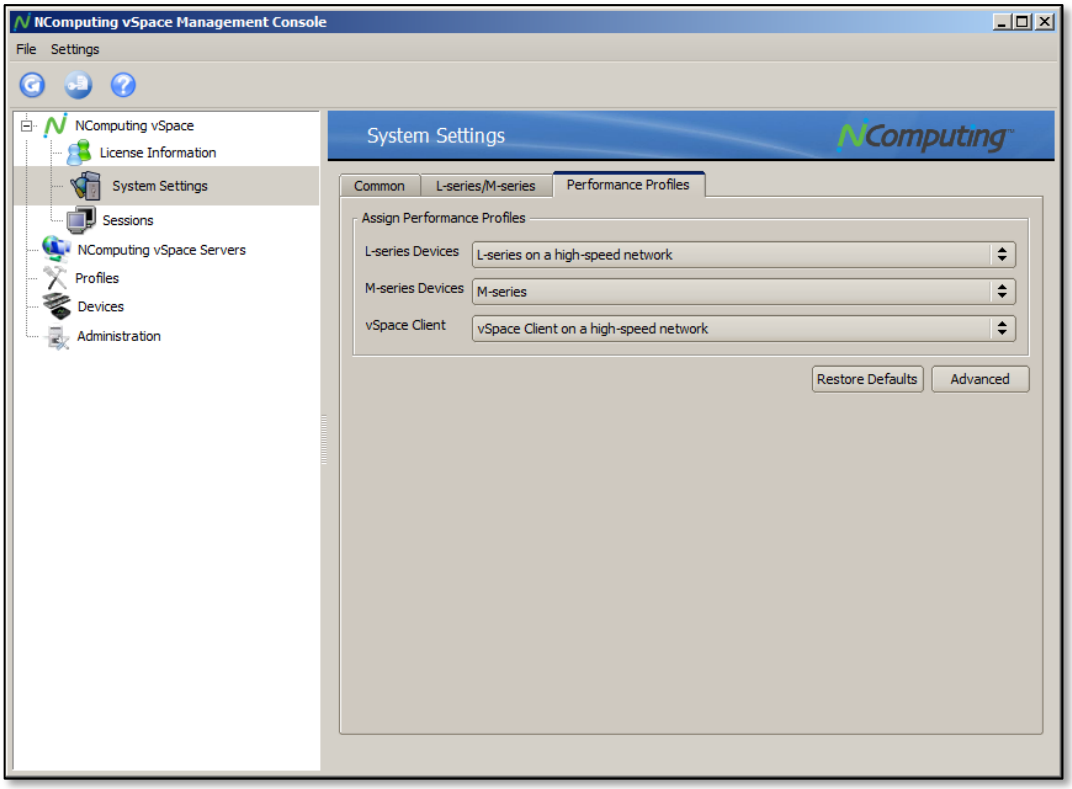
The "L-series/M-series" tab provides the following options and information:

Video Streaming Support	Enables or disables vSpace's proprietary video compression and streaming technology.

USB Support for L-Series/M-series Devices	Enables or disables USB support for L-series and M-series devices. While the feature on this page is a global setting, per-device control is available as pictured in the right-click menu pictured in Section 5.0 of this manual.
Register Future Devices in the Background	Enabling this feature instructs the vSpace host to automatically register and activate L-series and M-series devices that connect in the future. This process will be completed silently in the background and requires no further interaction.
Enable Remote Console on this Server	Enabling this feature will allow other vSpace hosts to view this host's settings, as well as information on active sessions and USB port assignment.
Remote Console Password	Sets the desired password for Remote Console access by other hosts. Hosts attempting to connect remotely to this system will be prompted for this password.

2.5 System Settings – Performance Profiles

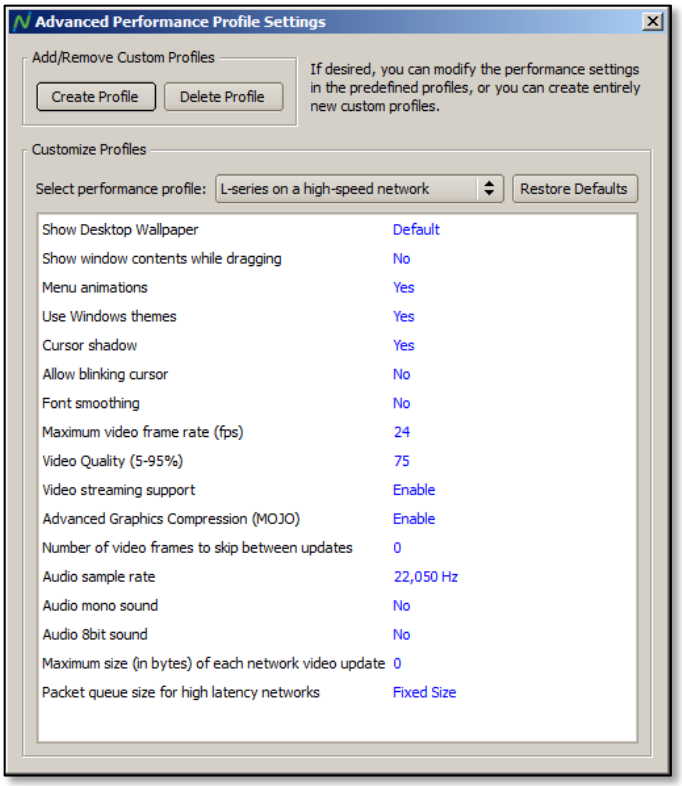
The "Performance Profiles" tab allows administrators to configure and assign separate performance configurations for varying network environments (such as Wireless, Low, and High Speed networks).



Assign Performance Profiles	Allows the administrator to choose from a selection of custom performance profiles to be used in specific network environments.
Advanced	Provides additional advanced configuration options. (see section 2.6)

2.6 System Settings – Performance Profiles ADVANCED

The Advanced menu allow administrators to create, edit, or delete individual performance profiles. The specific settings and their effects are detailed below.



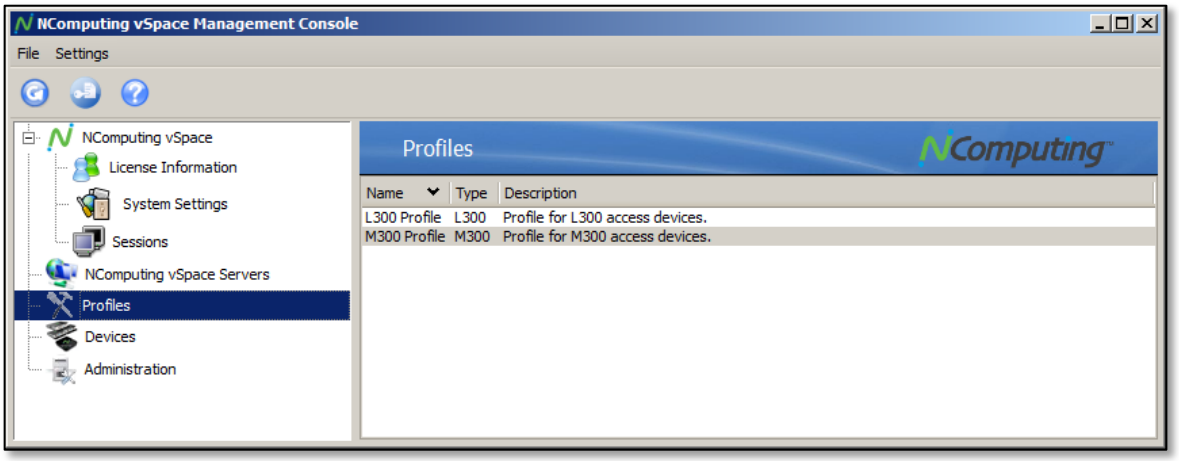
Administrators can add or remove profiles using the “Create Profile” and “Delete Profile” buttons located to the top left of the menu. An existing profile can be selected using the drop down at the top of the “Customize Profiles” section of the menu. Defaults can be restored using the “Restore Defaults” button to the right of the menu.

Show Desktop Wallpaper	Enable the use of desktop wallpapers in user sessions. This can also be set to conform to existing user profile settings (default).
Show window contents while dragging	Enabling this setting shows full window contents when moving a window on the desktop. Disabling this setting will show only the window’s outline while it is moving and can improve the overall performance of the desktop experience.

Menu animations	Enabling this setting enables graphical elements within the OS such as window animations. Disabling this option can improve desktop performance.
Use Windows themes	Setting this to “Yes” enables advanced Windows themes and graphical elements. Disabling this setting can improve desktop performance.
Cursor Shadow	Enables or disables the shadow seen beneath the mouse cursor. (Mouse shadows are not supported)
Allow blinking cursor	Enables or disables the blinking cursor effect.
Font smoothing	Enables or disables smoothing which can improve the appearance of fonts in some situations at the cost of increased resource usage.
Maximum Video frame rate	Enter a value here to limit the frame rate of streaming video to a desired number. Lower numbers will reduce network traffic when streaming videos to client sessions.
Video Quality (5-95%)	Decreasing this percentage will dramatically reduce the amount of network traffic being sent to client sessions at the cost of video quality.
Video streaming support	This setting enables or disables the advanced video streaming capabilities available to L300 and M300 devices.
Advanced Graphics Compression (MOJO)	Allows users to have more than one window open and streaming video at a time per session. Note that video performance may be better when limited to a single stream at a time.
Number of video frames to skip between updates	This value affects the rate at which the session image is updated. Larger values reduce network traffic but create a larger delay between updates.
Audio sample rate	Sets the audio sample rate to be used by sessions.
Audio mono sound	Sets the session to use mono sound.
Audio 8bit sound	Sets the session to use 8-bit sound.
Packet queue size for high latency networks	Increasing this setting can provide a smoother streaming experience in high-latency networks.

3.0 Profiles

Left-click on the “Profiles” section of the left navigation tree to display information on device profiles that have been saved for future use. You can edit or delete these profiles by right-clicking on them in the profile list on the right side of the console.

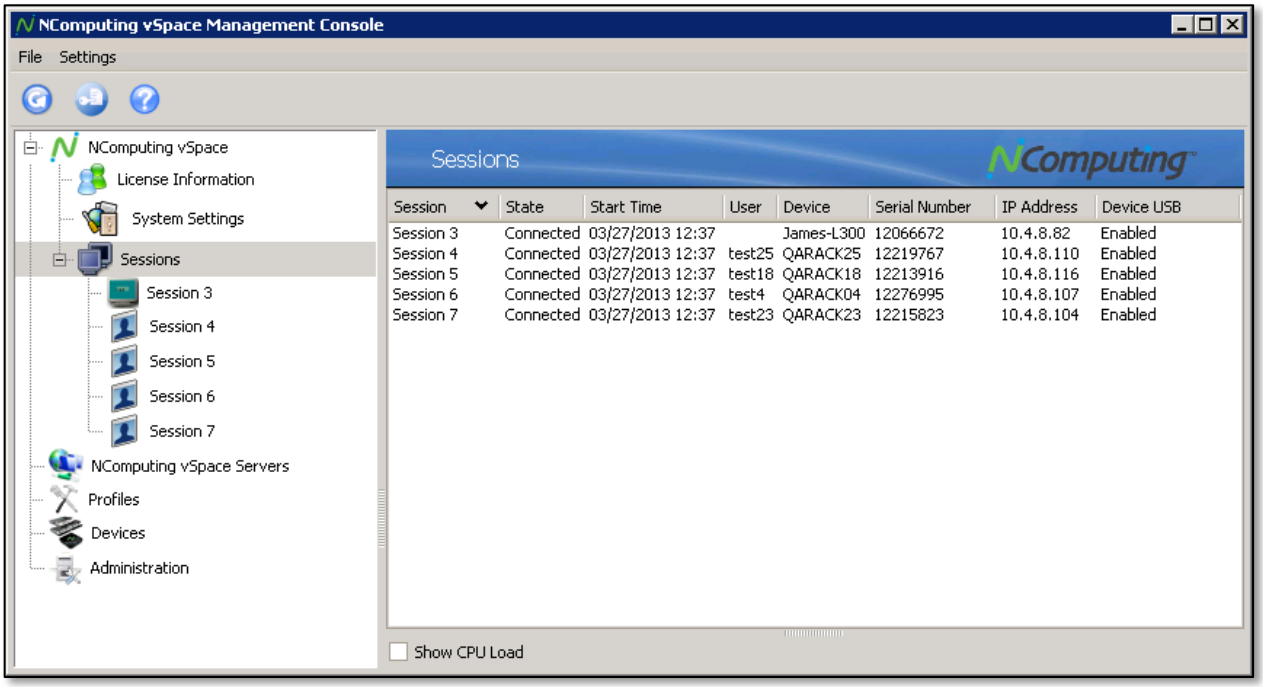


Profiles can be “pulled” from existing devices and then “pushed” to entire groups of devices to simplify the process of configuring several devices at a time. See **5.11 Configuration Profiles** for more information on pushing and pulling profiles.

4.0 Sessions

4.1 Session Overview

When one or more devices connects to your vSpace host, the “Sessions” section of the left navigation tree will be populated with a list of active sessions. Left-click on the “Sessions” section to display an overview of active sessions on the right side of the console.

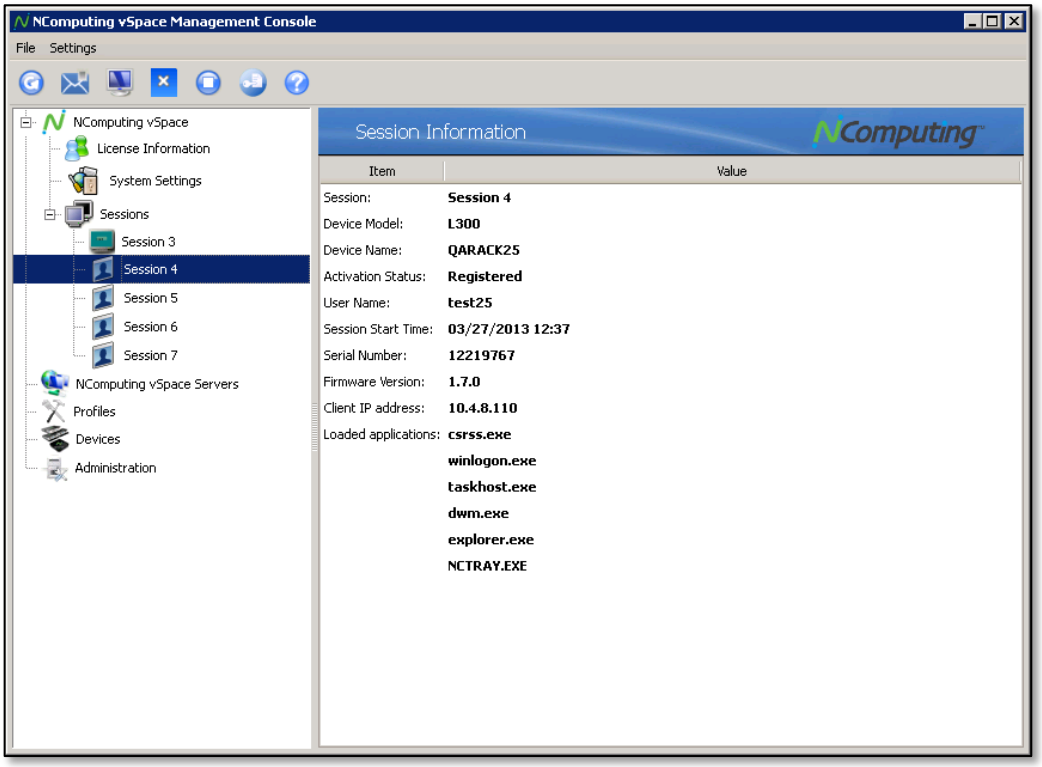


Right-click on any of the active sessions listed on the right side of the console to display the following four options.

View Session	Select this option to allow you to view the desktop of the selected session.
Send Message	Select this option to broadcast a short text message to the selected session.
Disconnect Session	Disconnects the device from the current session, but leaves the session active for a period of time for ease of reconnection.
Stop Session	Logs the user out of the current session.

4.2 Session Information

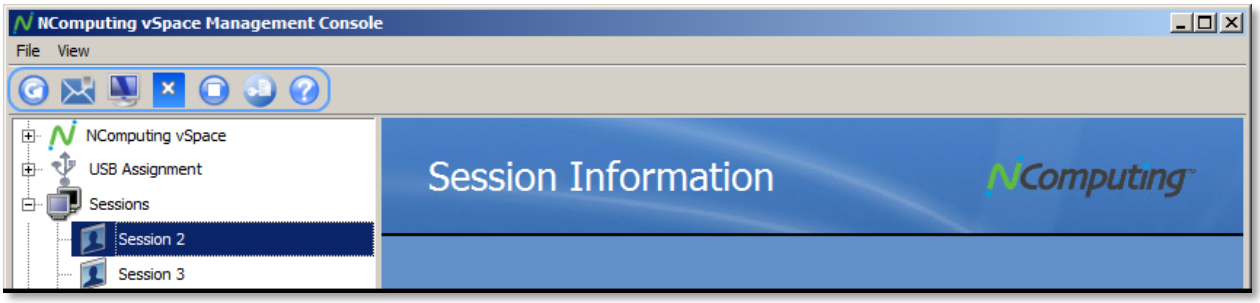
In addition to the session summary, you can expand the “Sessions” section of the left navigation tree to reveal information about individual sessions. Select these sessions to display additional information on the sessions themselves. The Session Information screen provides the following information:



Session	The session’s identifying number
Device Model	The model of device connected to this session
Device Name	The name of the device connected to this session (user configurable)
Activation Status	The device’s activation status, which is dependent on registration
User Name	The Windows User Name associated with this session
Session Start Time	The date and time that the session was created
Serial Number	The serial number of the device associated with this session
Firmware Version	The firmware version being used by the device associated with this session
Client IP Address	The IP address of the device connected to this session
Loaded Applications	The applications currently in use by this session

4.3 Session Controls

A number of controls that provide easy access to some common operations appear at the top of the console. These operations include the ability to remotely view a specific session or to send that session a message.



Refresh – Refreshes Device and Session data within the vSpace console.

Send Message – Sends a private message to the selected session.

View* – Remotely displays the selected session, providing the same desktop view that the user is currently seeing.

Disconnect – Disconnects the device from its associated session.

Stop – Stops the selected session, effectively logging the user out.

Registration –Opens the Registration dialog box.

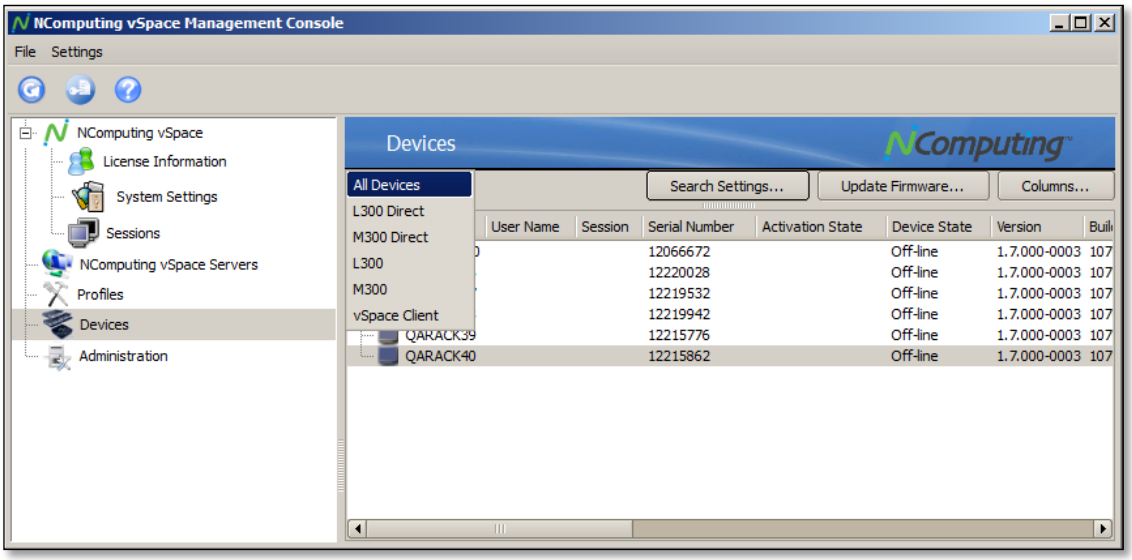
Help – Opens the Ncomputing Support page on an external web browser.

*While using the "View" function on a session, administrators can right-click on the top bar of the view window to take control of that session.

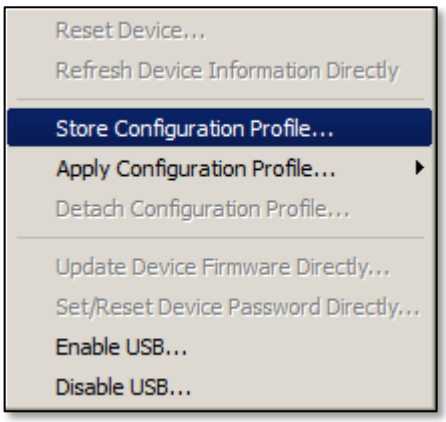
5.0 Device Management

5.1 Device List

Clicking on the Devices category displays a list of devices that can be sorted by device model, using the drop-down menu towards the top of the menu. Basic information for each device, such as Device State, Activation State, and Serial number are displayed in this menu. Right-clicking and double-clicking on specific devices provides additional information and configuration options.



Right-click on a device to display basic maintenance options. Standard left-click "box" selection, shift-click and ctrl-click methods allow for the selection of multiple devices at once.

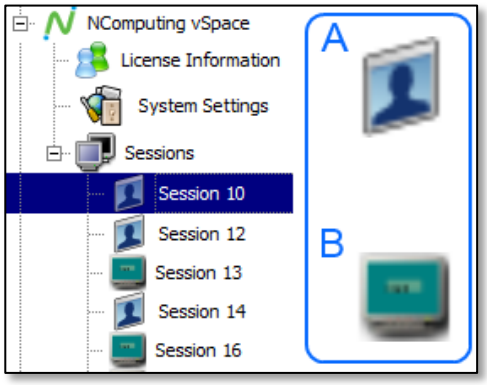


- **Reset Device** – Resets the selected device(s).
- **Refresh Device Information Directly** – Refreshes all information on the selected device within vSpace.
- **Store Configuration Profile*** – Stores a profile of the selected device's settings for future use.
- **Apply Configuration Profile*** – Applies a stored Configuration Profile to the selected device(s).
- **Detach Configuration Profile** – Removes the selected device(s) from the profile they're currently associated with.
- **Update Device Firmware Directly** – Initiates the Firmware Update process on the selected device(s).
- **Set/Reset Device Password Directly** – Opens the Device Password menu for the selected device.
- **Enable USB** – Enables USB support for the selected device(s).
- **Disable USB** – Disables USB support for the selected device(s).

* See **Section 6.11** for more information on storing and applying configuration profiles.

Double-click on any device to open the Device Settings menu. This menu contains the following sub menus, which are explained in detail in the pages that follow. **(**continued in **Section 5.3)**

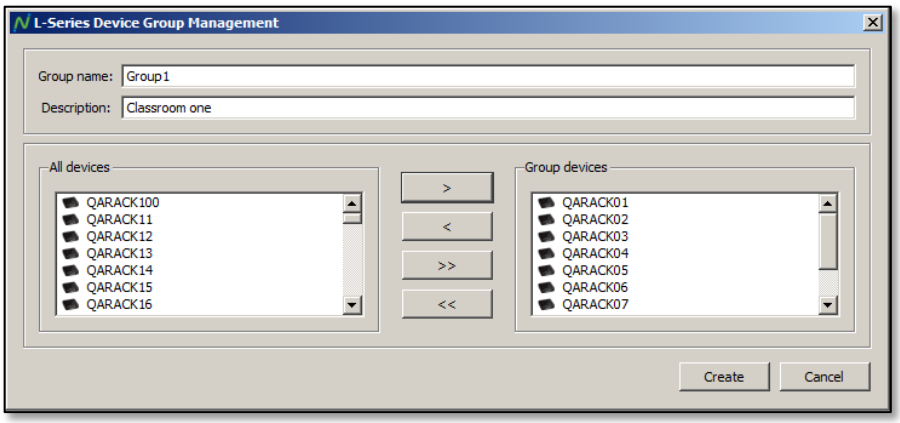
- **Information** – Basic device information
- **Connections** – Connection options
- **Server Groups** – Details on preconfigured Server Groups and their contents
- **Login** – Options for manual and automatic login
- **Network** – Network settings and options
- **Password** – Device password options
- **Update** – Controls for updating device firmware
- **Management** – Allows administrators to configure a primary and secondary management server for the selected device.



Next to each displayed device is an icon, as illustrated to the right. The icon displayed indicates the current state of the device next to it. The silhouette (A) indicates that a user is currently logged into a session on the device. The monitor (B) indicates that the device is currently sitting at a login screen but is not in active use.

5.2 Device Groups

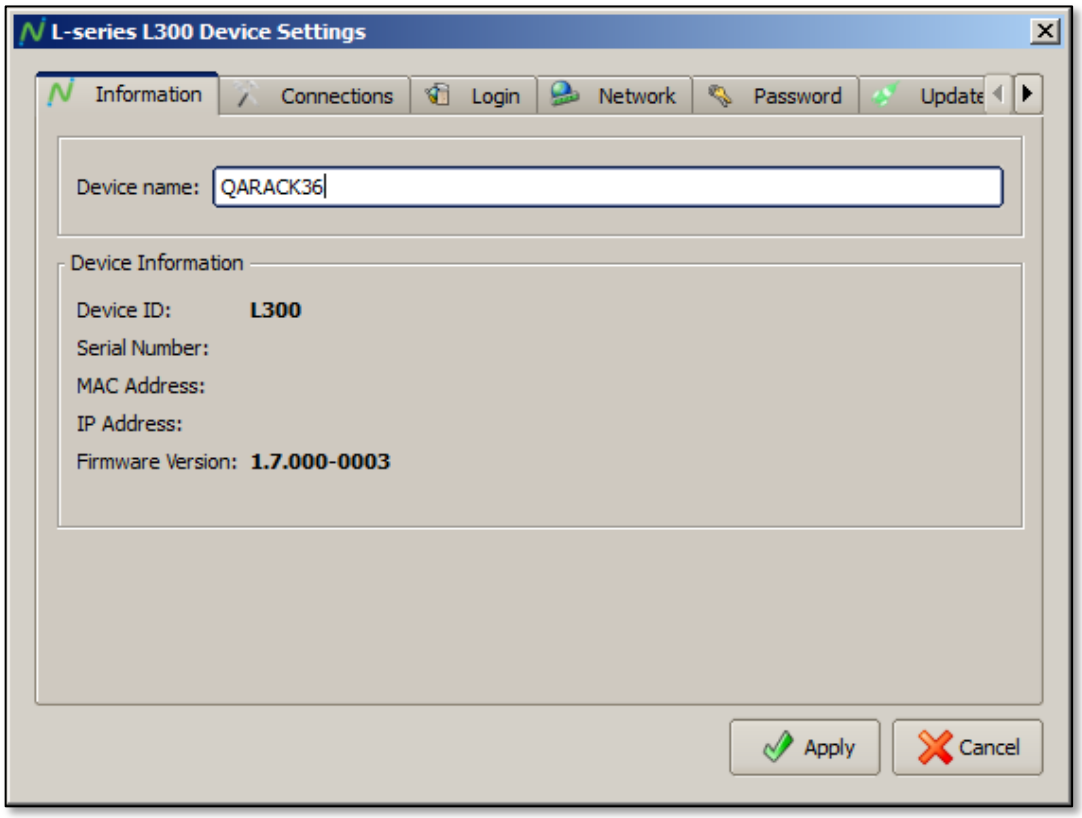
When dealing with large numbers of devices spread throughout several logical or physical groups (for example, deployments across several office floors or classrooms), it can be advantageous to group these devices within the vSpace console itself. This can be accomplished by right-clicking on the "Devices" category along the left navigation tree and selecting "Add Group," which opens the Device Group Management interface, as shown below:



From this interface, devices can be added to a group which can be given a name befitting the nature of your deployment.

5.3 Information Tab

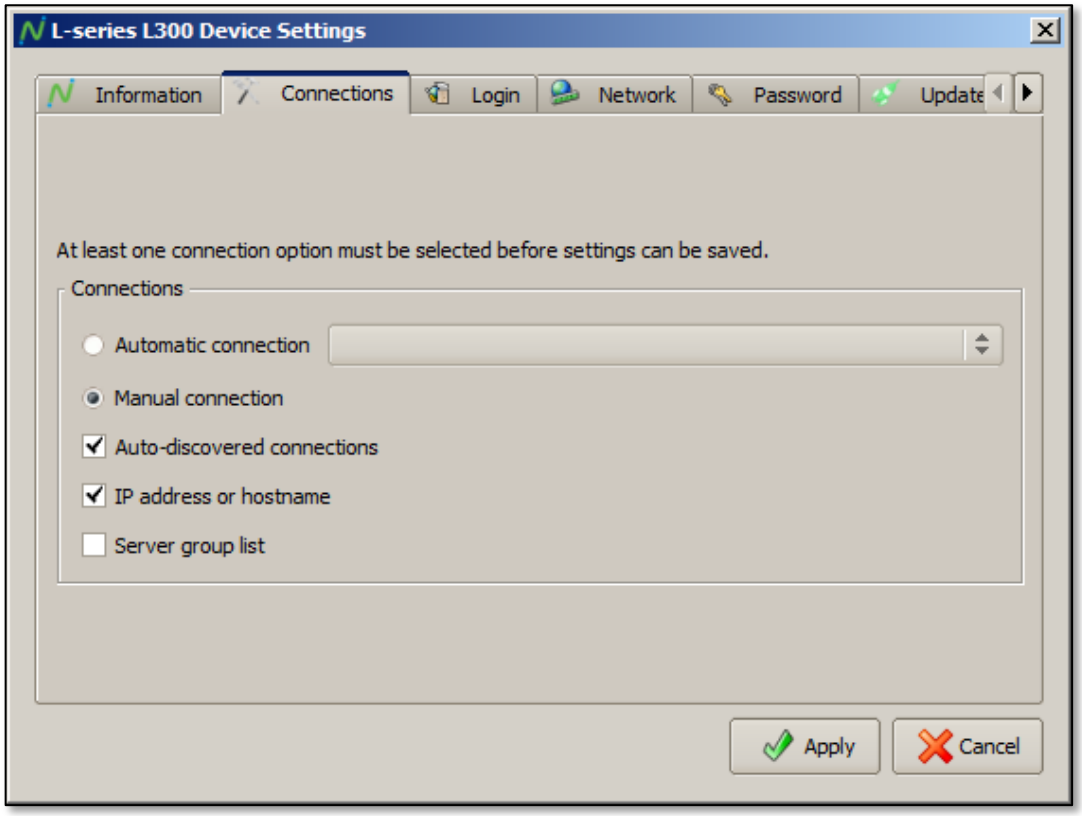
As outlined in section 5.1, double-clicking on a device within the Device category opens a configuration menu which can be used to alter the settings of individual devices. The “Information” tab appears first within this menu, and provides basic information on a selected device, including its network address and serial number. This tab also allows you to rename the device to facilitate identification.



Device Name	Displays the designated device name. This can be edited as desired.
Device ID	The Model ID of the selected device (L300’s have a Device ID of 300)
Serial Number	The serial number of the selected device
MAC Address	The MAC address of the selected device
IP Address	The current IP address of the selected device
Firmware Version	Displays the currently loaded firmware version of the selected device. In this example, the device firmware is out of date, as indicated by the text “Please update firmware.”

5.4 Connections Tab

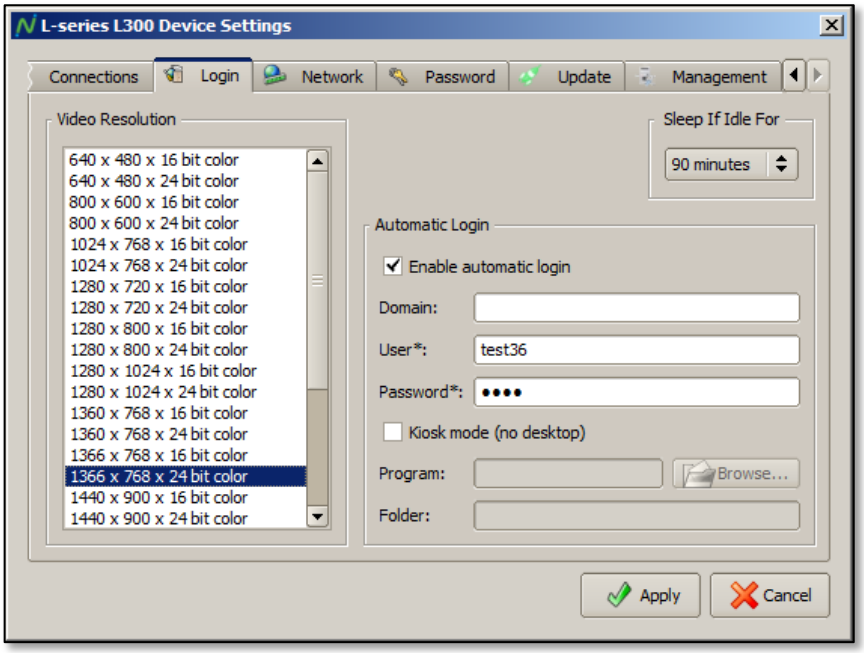
The “Connections” tab provides several host configuration options that determine how the device finds and then connects to available hosts. From here, you can set the device to automatically detect available servers, or instruct the device to connect to specific predetermined hosts or groups of hosts.

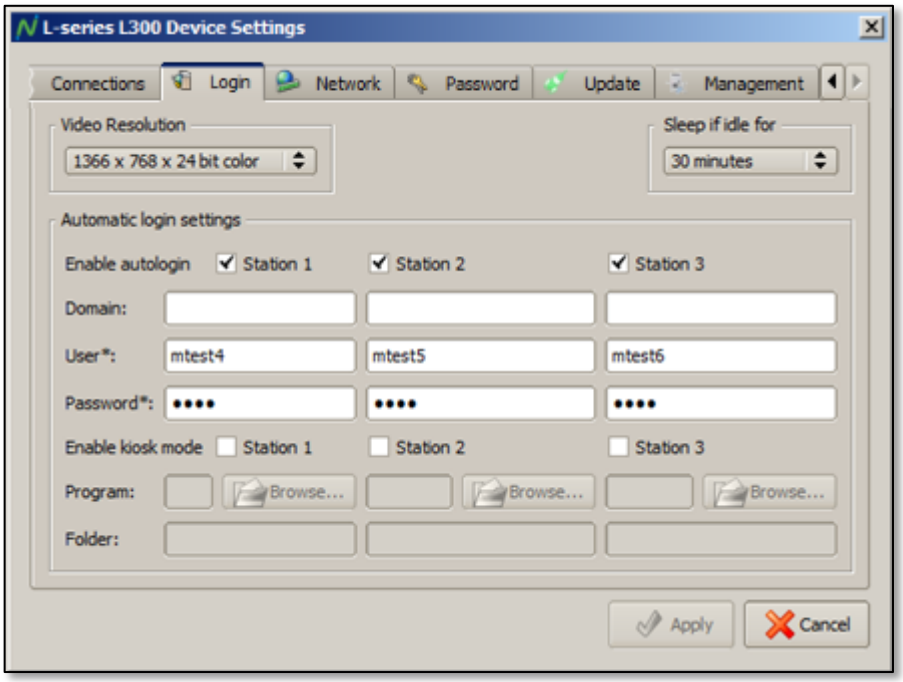


Automatic connection	Configures the device to automatically connect to a predefined server location or server group.
Manual connection	Configures the device so that the user can select a specific host, IP or Server Group each time the device boots.
Auto-discovered connections	Enable to display all available hosts on the device’s subnet.
IP address or hostname	Enable to allow the user to type in a specific IP or host name.
Server group list	Enable to allow the user to select a server group to connect to.

5.5 Login Tab

The “Login” tab provides several configuration choices that determine how the device will behave once it connects to a given host system, including screen resolution and automatic login options. Note that the L-series and M-series Login configuration menus vary slightly as seen below.

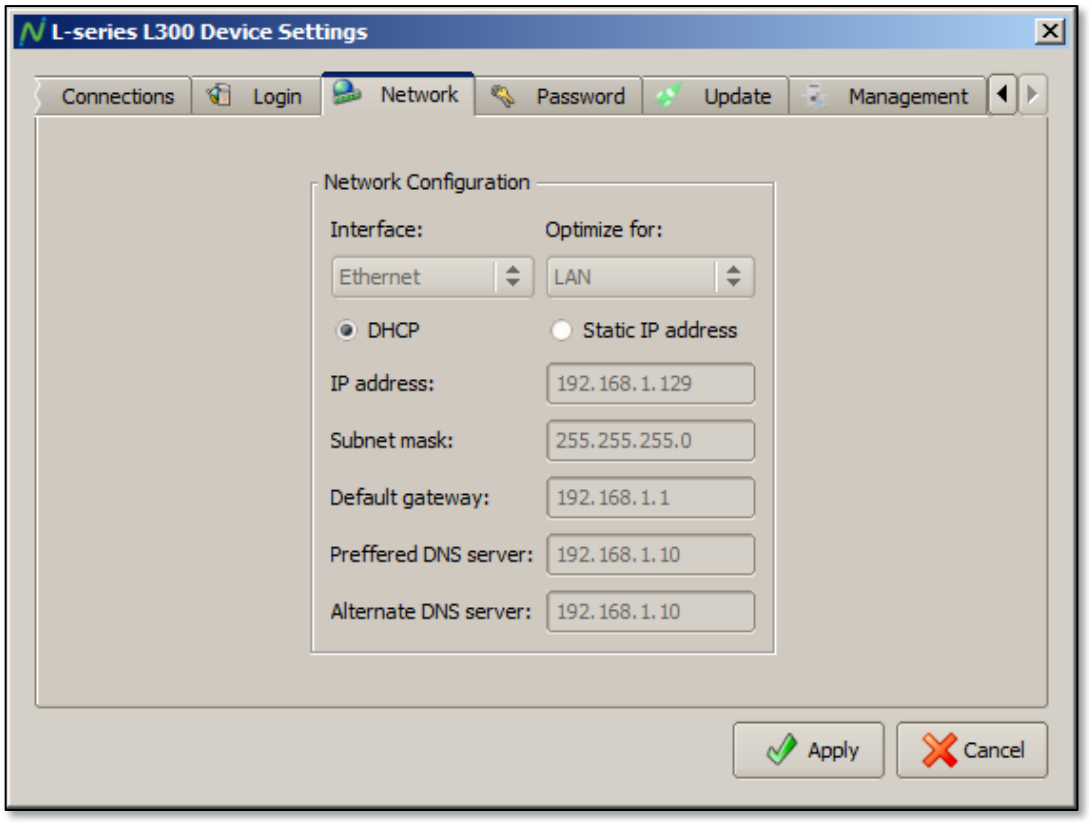




Screen Resolution	Sets the screen resolution and color depth to be used by the device once it connects to a host. Note that for the M-series, all three clients in an M-series kit share the same resolution and color depth settings.
Vertical Refresh Rate	Sets the vertical refresh rate (in Hz) to be used by the device.
Sleep If Idle For	Instructs the device how long to wait before turning off its video signal (thereby allowing the monitor to enter its built-in screen saver mode).
Enable Automatic Login	Instructs the device to use a specific user name and password when it connects to a host. When enabled, the credentials will be entered automatically, allowing for a swift login. Specify the user credentials in the fields below this option.
Kiosk Mode	Instructs the device to immediately launch a specific application on login, instead of providing the standard Windows desktop experience.
Program	The name of the executable or object to be launched on startup
Folder	The path to the file to be executed

5.6 Network Tab

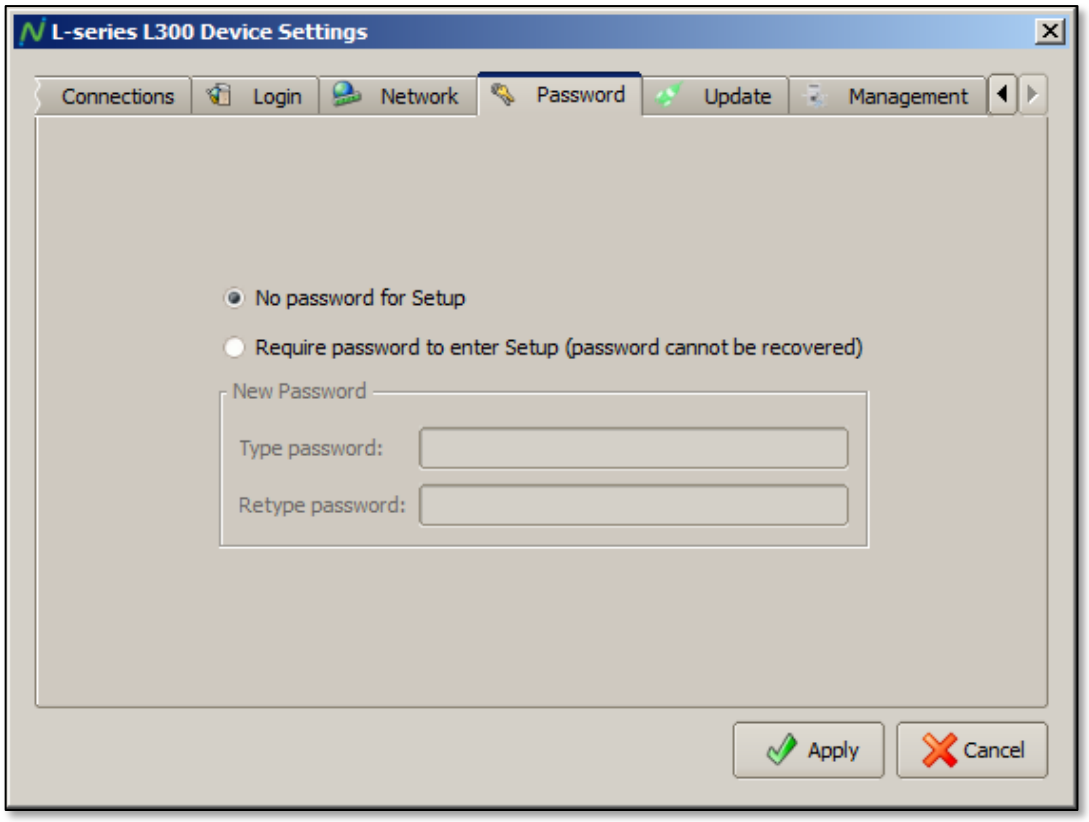
The “Network” tab provides standard network configuration options, including a choice between static and dynamic IP acquisition.



Interface	Indicates the device’s network interface.
Optimize for	Indicates the type of network being used; LAN = Local Area Network.
DHCP	Instructs the device to acquire its network information from a DHCP server.
Static IP Address	Instructs the device to use specific network settings, which can be specified in the fields below this setting.
IP Address, Subnet Mask, Gateway, DNS	Allows administrators to specify network connection information.

5.7 Password Tab

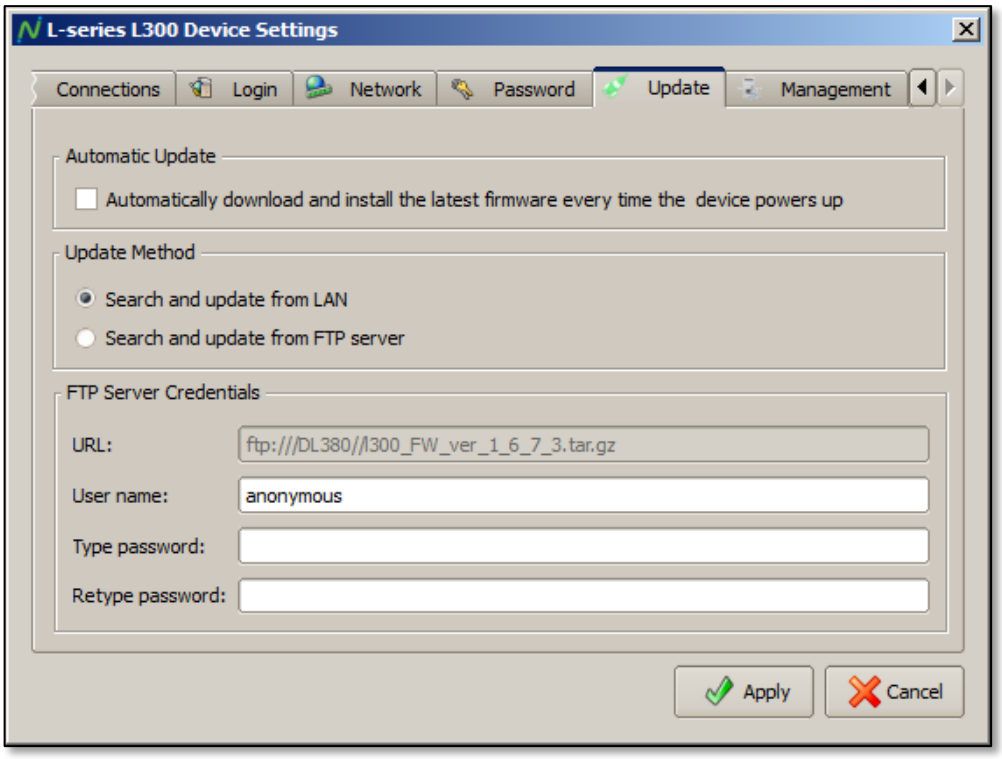
The “Password” tab provides the option of setting a password that will restrict future access to device configuration. Use this tab to enable and disable password protection.



No Password for Setup	Sets the device to be accessible for configuration by any user.
Require Password to Enter Setup	Sets the device to require a password before device settings can be altered. If a password does not currently exist, it can be entered in the fields directly beneath this option.

5.8 Update Tab

The “Update” tab is used to check for and install (if available) firmware updates for the device. This tab allows you to select from several different update methods, and can be set to draw firmware updates from inside your network, or from an external FTP location.



Automatic Update

Enable this option to instruct the device to automatically check for newer firmware that is available on the servers it can see during startup. If found, it will then download and install this firmware automatically.

Search and Update from LAN

This option instructs the device to search for updated firmware within the local area network it resides in.

Search and Update from FTP Server

This option instructs the device to search for updated firmware at a specific FTP location. Enter the full path of a specific firmware file to force the device to use that specific file (which allows for downgrading if needed). Enter the path of a folder that contains multiple firmware versions and a firmware index file to instruct the device to use the most recent firmware version available, according to the index file.

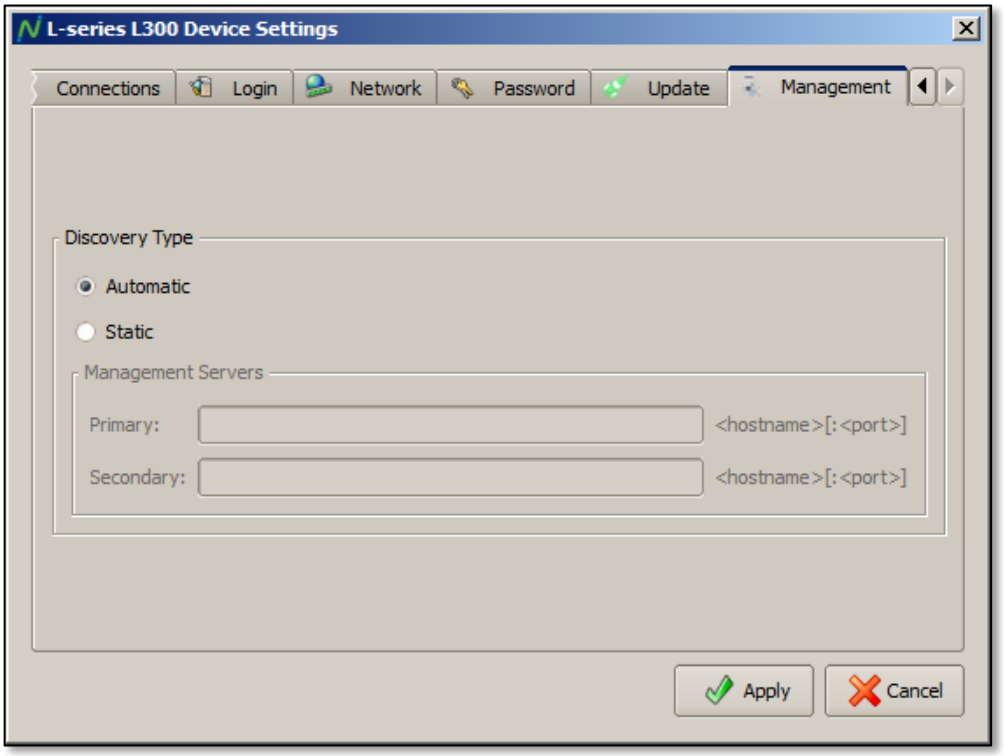
For more information on firmware updates via FTP, visit http://www.ncomputing.com/kb/Using-FTP-to-update-L300-Firmware_308.html

FTP Server Credentials

These fields allow you to enter the URL, user name and password for the FTP server you wish to use (if required).

5.9 Management Tab

The “Management” tab allows administrators to associate devices with specific management servers.

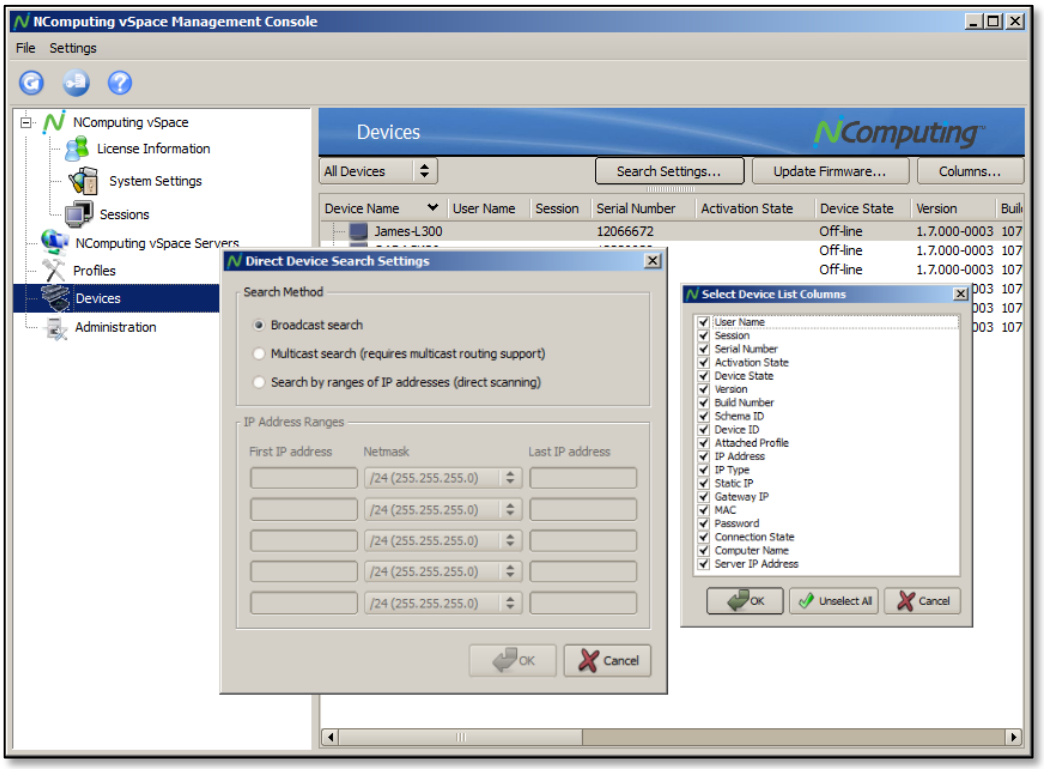


Automatic Enable this option to instruct the device to automatically join any management server it discovers within its network segment.

Static This option allows administrators to manually associate a device with a specific management server, as well as a secondary server.

5.10 Search Settings and Columns

The “Search Settings” and “Columns” features in the upper-right side of the Devices category provide additional tools for locating, sorting and displaying device information.



The “Device Search Settings” dialog box provides administrators with the ability to locate devices anywhere on the network (provided that the connections in question are allowed by the network’s routing rules), as well as the ability to search specific IP ranges, while ignoring others. The dialog box contains the following options:

Broadcast Search	Searches for devices on the same subnet as the host using UDP broadcast.
Multicast Search	Uses the network Multicast functionality of certain high-end routers and switches to more efficiently discover devices. (Must be supported by network hardware.)
Search by Range of IP Addresses	Searches for devices within a specified IP range.
IP Address Range	Provides the necessary fields to specify what range of IP addresses you wish to search within (only applies to “Search by Range of IP Addresses” setting).

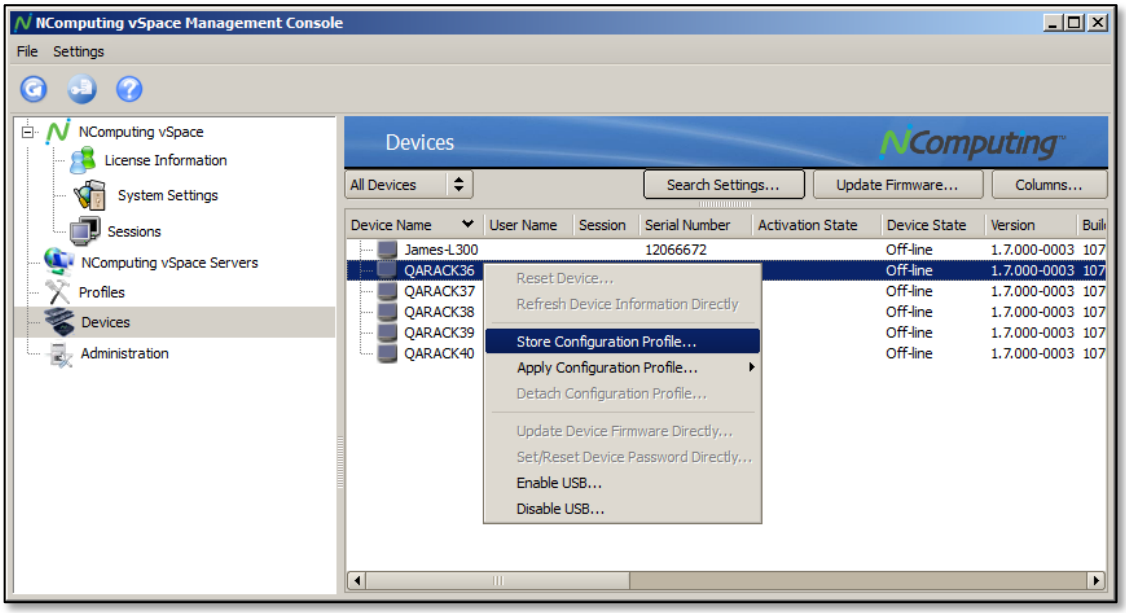
The “Select Device List Columns” dialog box provides an extensive list of device details that can be toggled on or off as desired to create a custom display within the device list. These choices affect which columns are displayed in the device list to the right of the vSpace management console.

5.11 Configuration Profiles

As of vSpace version **L-6.5.1.,** the NComputing vSpace Console includes the ability to save device settings and apply those settings to other devices across the network. While administrators retain the option to fine-tune devices on an individual basis, the Profile Management feature adds the ability to design and then deploy pre-selected configuration profiles to groups of devices in one step.

5.12 Creating Profiles

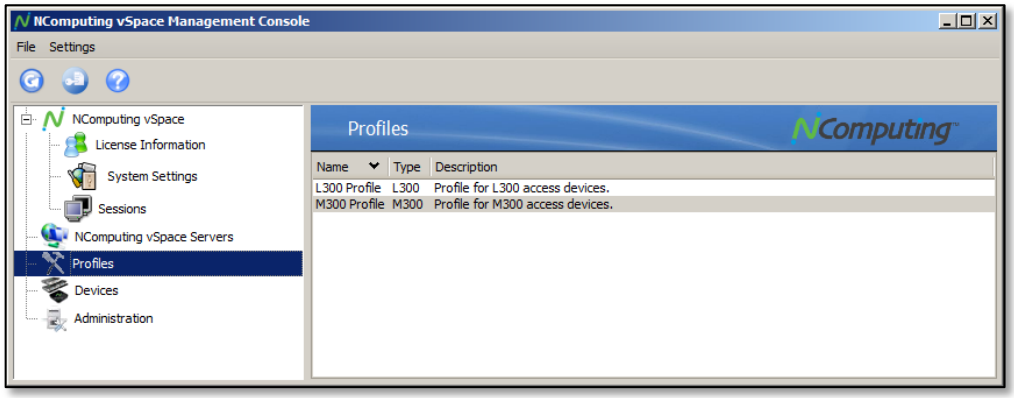
Profiles can be created by right-clicking on a device and selecting the “Store Configuration Profile” option from the pop-up menu that displays, as shown below:



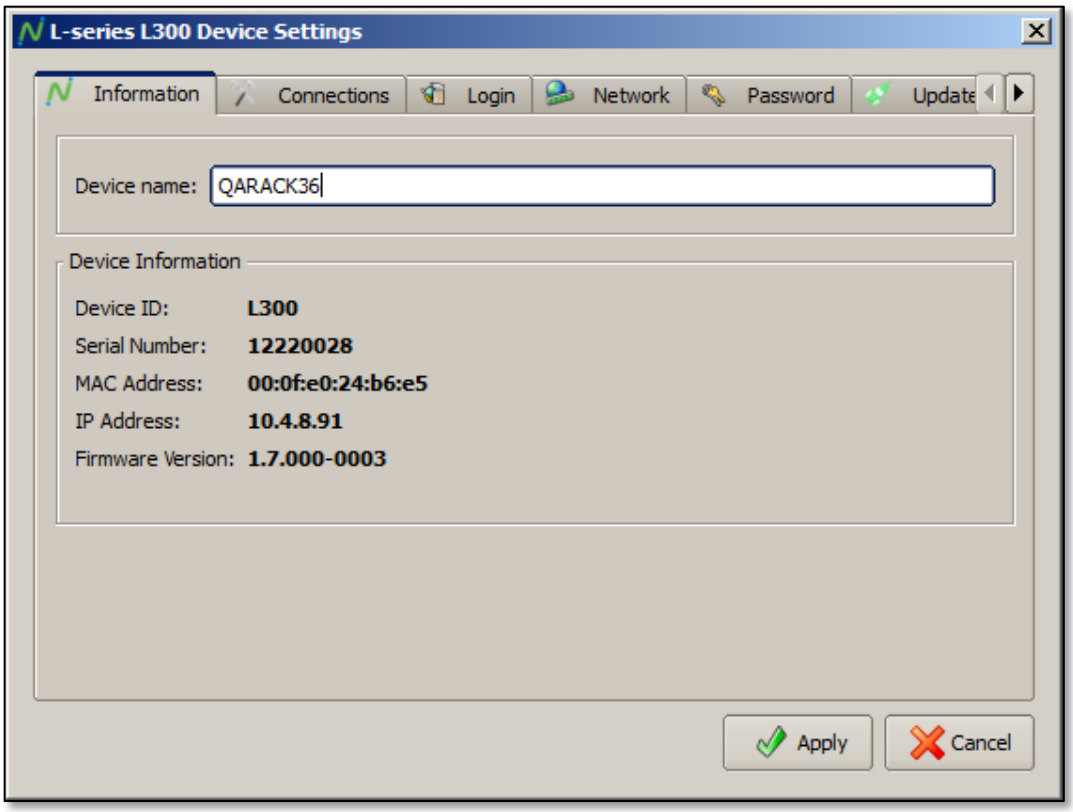
After choosing to store the selected profile, a confirmation will appear. Select “Yes” from the confirmation dialog box to store the profile in the “Profiles” section of the vSpace Management Console. The Management Console can store multiple profiles, and you can edit or remove them at any time.

5.13 Editing Profiles

Once a profile is created, administrators can edit the profile in the same way they would apply changes to the settings of an individual device. To do this, select “Profiles” from the left navigation tree within the Management Console, and then right-click on a profile, as shown below:

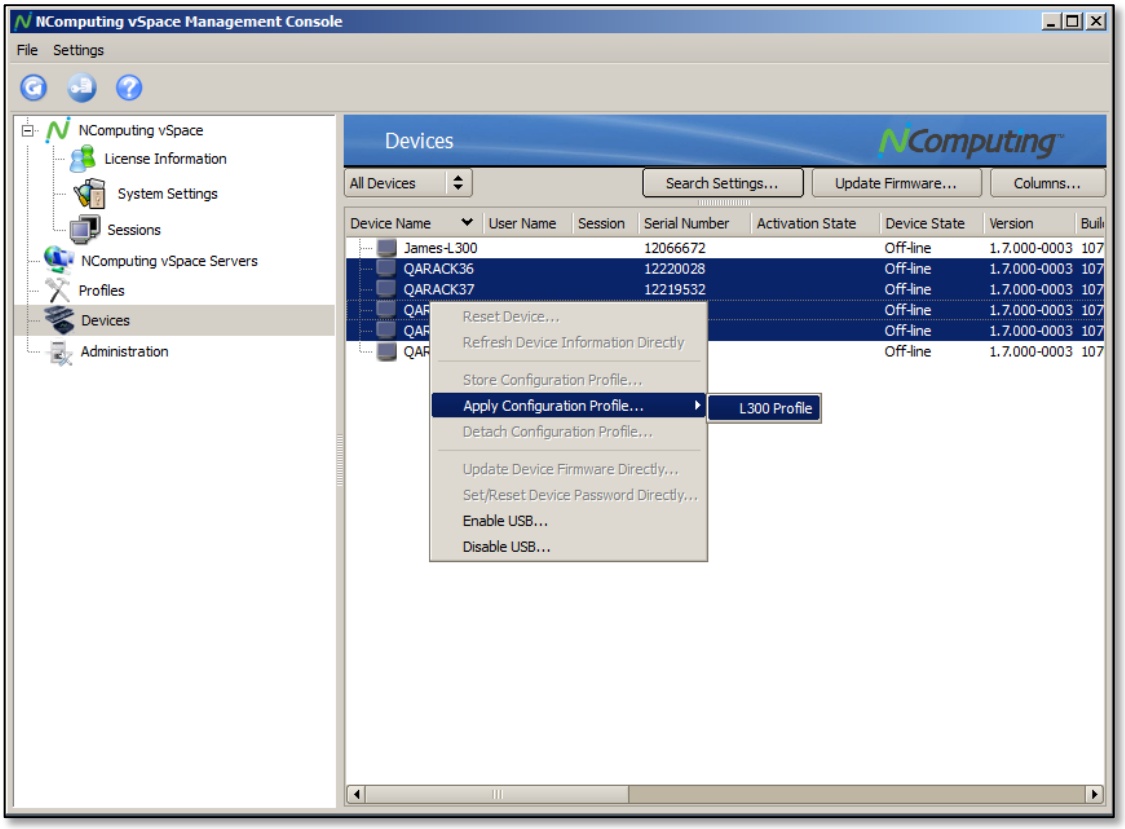


Once you have selected a profile to edit, you will be presented with a multi-tabbed configuration menu that closely resembles the device configuration menu. This menu allows you to rename the selected profile, as well as alter Connection, Server Group, Login, Password and Firmware Update settings. These menus function in the same manor outlined starting in **Section 5.3**.



5.14 Applying Profiles

To apply a saved profile to other devices, select one or more devices within the Device list and then right-click on any of the selected devices. From the pop-up menu that displays, select “Apply Configuration Profile,” as shown below:



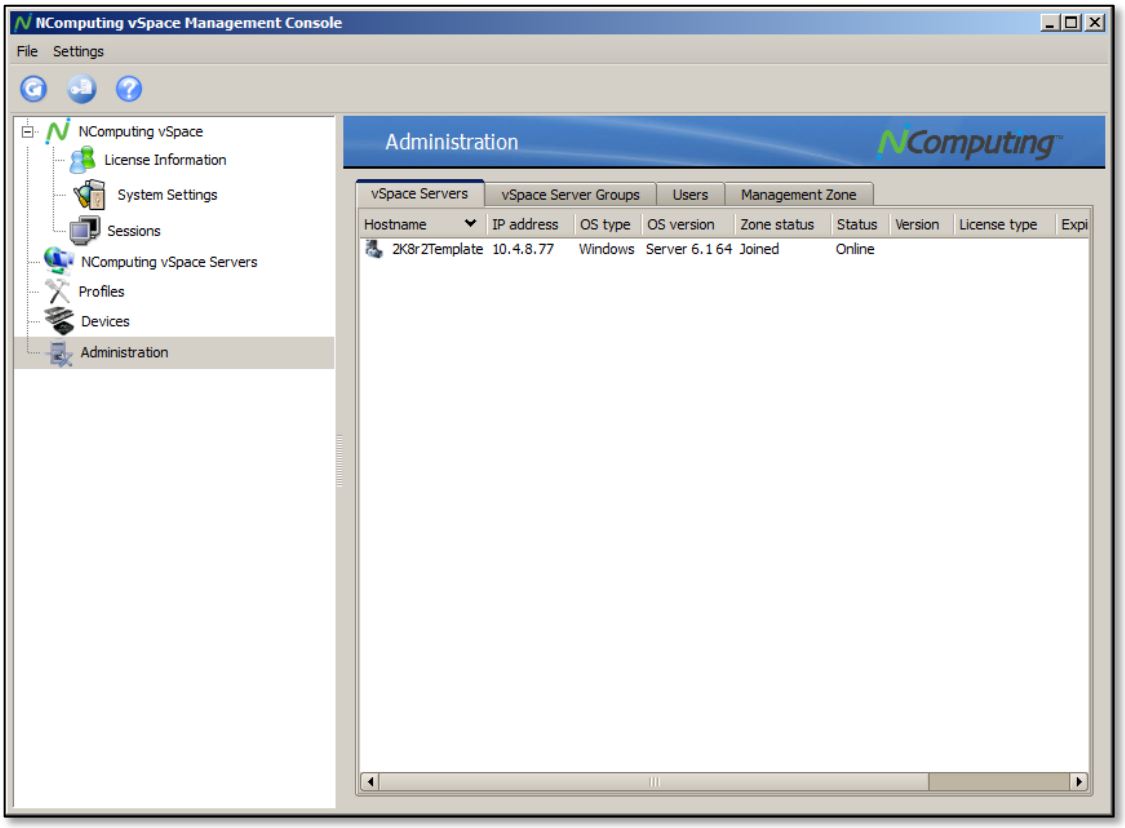
After confirming the action, the Management Console will begin updating the selected devices. This process may take a few moments, depending on the number of devices affected by the update. Once the process is complete, the affected device(s) will reboot automatically.

Keep in mind that L and M-series device profiles are not cross compatible due in part to the fact that the M-series stores information for three separate devices/users per kit as compared to the L-series’ single device/user. For this reason Profiles must be created for and applied to L and M-series devices separately.

> **NOTE:** If a device has a password applied to it, you will be prompted to enter the password when attempting to apply a profile to that device.

6.0 Administration

The Administration category includes additional configuration options for the management zone itself, as well as other administrative options such as user profiles for varying degrees of access as well as vSpace Server Group options.

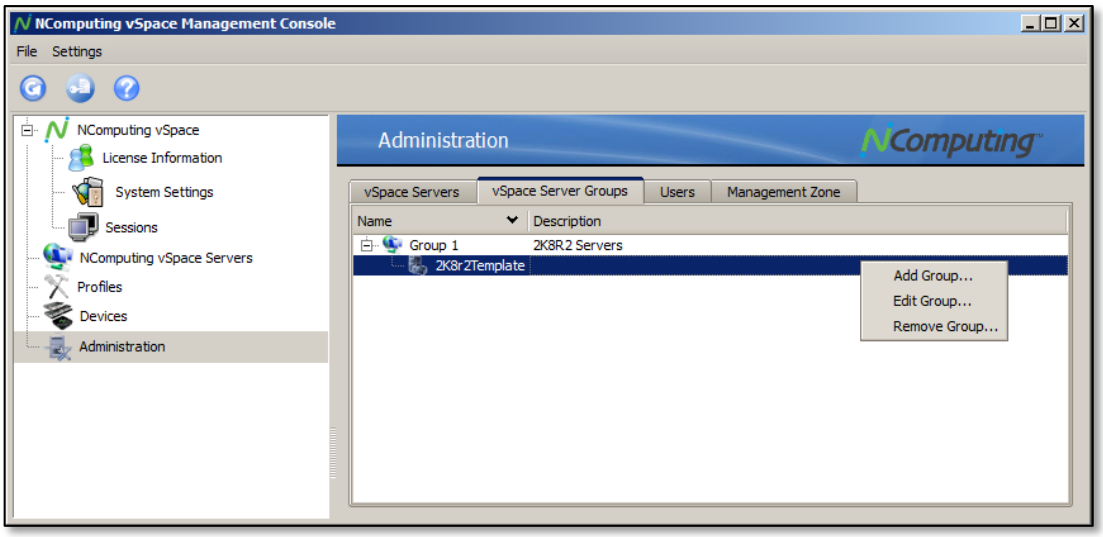


6.1 vSpace Servers

The first tab within the Administration category lists all vSpace and vSpace Management Center servers within the server's management zone. Information such as server IP address, OS type, and zone status are listed in the default view.

6.2 vSpace Server Groups

The second tab within the Administration category allows administrators to create, edit, or remove vSpace Server Groups.

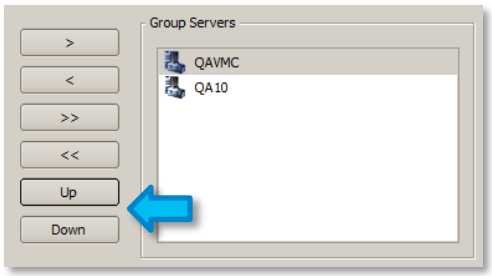


Right clicking within the server groups list allows you to add, edit, remove, and reorder server groups. When editing a group, additional servers can be added to or removed from an existing group.

Server Group Prioritization

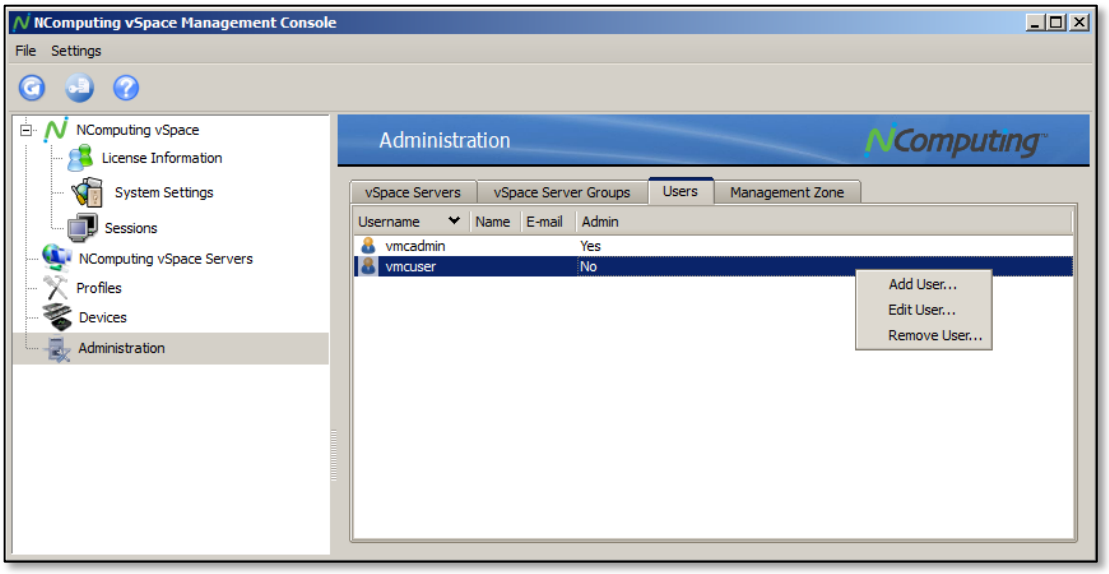
Administrators can prioritize servers within a Server Group by raising or lowering it within the server list. Device connection attempts proceed from the top of the list downward.

Selecting a server and then using the **Up** and **Down** buttons will move that server higher or lower within the server group list.



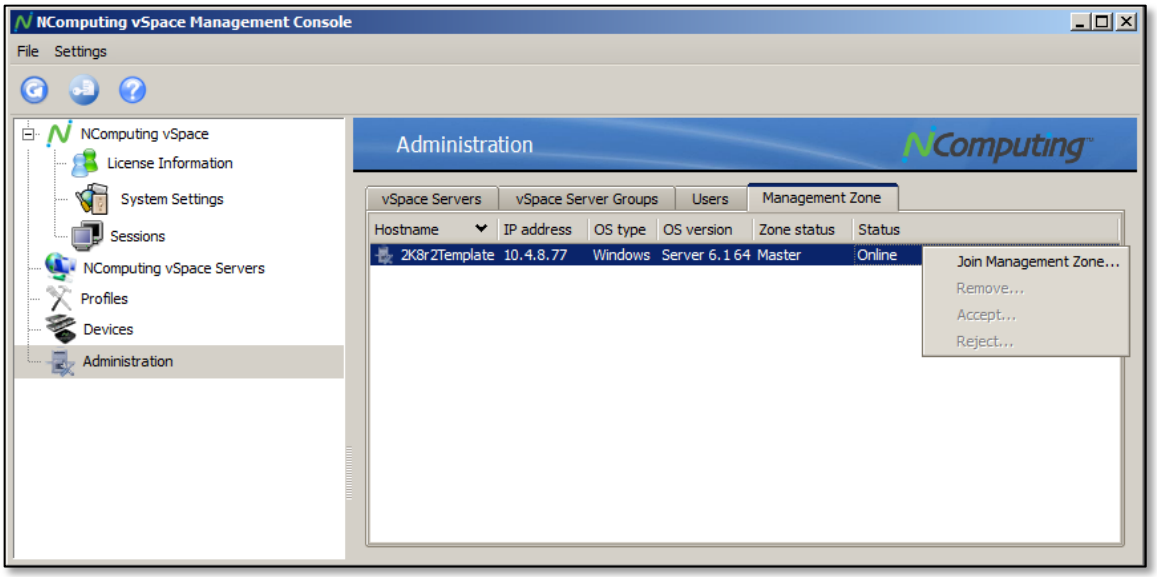
6.3 Users

The Users tab allows administrators to create administrative accounts and provision them with either read-only, or full administrative access. Righ-clicking on a user account provides the option to add, edit, or remove user accounts.



6.4 Management Zone

The Management Zone tab allows administrators to view servers within their management zone, join another management zone, remove servers from a management zone, or accept / reject join requests if the server in question is the Master server within that zone.



7.0 Common Tasks

This section provides some examples of frequently-encountered administrative tasks that utilize many of the features outlined in the previous sections.

7.1 Helpdesk Tasks - Remote Viewing and Controlling a Device Session

For this example, we'll simulate remotely viewing and then controlling an active vSpace session. These actions will demonstrate the following vSpace console features:

- Locating sessions by windows login credentials
- Viewing a session remotely
- Controlling a session remotely

The Scenario:

A device user is having trouble and has called their office helpdesk service to assist them. The nature of the issue suggests that the easiest solution may be to **have a technician take over their session remotely and perform a few troubleshooting tasks**. In this scenario, the user doesn't know what their device name is but provides the Windows Login Name that they used to log in to Windows. They've connected to the **Sales1 server,** which is one of many virtual machines hosted within the office.

Step 1 – Open the vSpace Management Console:

The technician logs into the Sales1 server (using the virtual machine's console application, such as VMWare's vSphere Client). Once logged into the server, the technician launches the NComputing vSpace Management Console. (If this host were on a "bare metal" system, they could just as easily have opened an RDP session or, if the host were located in their part of the office, they could simply go to the host itself and log in to the host using an admin account.)

Step 2 – Determine which session is being used by the device in question:

Under the "L-series" section of the vSpace console, the technician would then locate the device by searching for the Windows Login Name provided under the "User Name" column of the L-series device list (outlined in **5.1** of this guide). Click at the top of any column to allow them to sort by this column to quickly find the user in question. In this scenario, we'll assume it was Session 2.

Step 3 – Use the Session Controls to perform the desired helpdesk tasks:

The technician would then open the "Sessions" section of the console (**4.1 Session Overview and 4.2** Session Information) and left-click on Session 2 in the left navigation tree, revealing several session control options (**4.3 Session Controls**) along the top of the screen. These controls allow them to remotely view and then control the desired user session.

7.2 Maintenance Tasks - Performing a Firmware Update on an Active Device

In this example, we will simulate performing a firmware update on a device that is currently in use. To do this we need to give the current user advanced notice of the impending update before proceeding. This demonstrates the use of the following vSpace console features:

- Locate devices by active session ID
- Send a message to an active session via the console
- Perform a remote firmware update on multiple devices simultaneously

The Scenario:

As the work day winds down in a small office environment, the administrator gets ready to perform firmware updates on L-series devices throughout the building. All of the users have left for the day, with the exception of one. The administrator needs to make sure that the user is aware of the impending device update and restart before proceeding and decides to use the vSpace Management Console to accomplish this task.

Step 1 – Locate the active session and its associated device.

The administrator locates the active session using the "Sessions" section of the Management Console (**4.1 Session Overview** of this guide). If there were more than one user still active, they would all be visible in this list.

Step 2 – Send a message to the active session warning of the impending update.

By selecting the active session(s) found in the "Sessions" list and using the "Send Message" button (**4.3 Session Controls** of this guide), the administrator is able to send a text alert to the remaining user warning the user of the impending firmware update and forced device restart. This gives the user enough time to save their work and log out.

Step 3 – Perform a remote firmware update on all selected devices.

Once the remaining user has closed out their session, the administrator is free to select all of the devices in need of a firmware update in the L-series Devices list and perform a firmware update via the right-click menu (**5.1** of this guide).

7.3 Deployment Tasks – Installing and Configuring a new Computer Lab

For this example, we will go through the steps of initially deploying a series of devices, verifying their connectivity and performing some initial configuration tasks. These actions demonstrate the use of the following vSpace console features:

- Performing a firmware update on multiple devices simultaneously
- Storing and applying a device profile to multiple devices simultaneously

The Scenario:

A school is adding a lab with an additional 20-devices to their existing NComputing deployment. To expedite the deployment process, they will perform as many tasks as they can from the host rather than configuring individual devices.

Step 1 – Connect and Configure the First Device

After creating a host system with sufficient hardware resources for the intended user load and tuning it as outlined in the **Windows Tuning Guide**, vSpace is installed and registered as outlined in **1.1 Installing vSpace** and **1.3 Registering vSpace** of this guide. The administrator connects the first device to the host created for this lab and will use this device as a template for the rest of the devices in the deployment.

Once connected, the administrator locates the device from the host under the L-series Device list (**5.1** of this guide). The administrator right-clicks on the device and then selects "Update Device Firmware" to initiate a firmware update on the selected device. Once that process is complete and the device reboots, the administrator can double-click on the device and configure it as desired (**5.3 Information Tab through 5.8 Update Tab** of this guide).

Step 2 – Store the First Device's Configuration Profile

After completing the configuration process on the selected device, the administrator can then right-click on the device in the L-series Devices list of the console and select "Store Configuration Profile" (**5.12 Creating Profiles** of this guide) to save this configuration for use on the rest of the devices in the lab.

Step 3 – Connect and Configure the Remaining Devices

It is now time to connect the remaining devices. Once the devices are connected, the administrator can perform a firmware update on all of them simultaneously by selecting the group and initiating a firmware update as outlined in **Step 3**.

Once the devices have completed their firmware update, the administrator can then apply the first device's Configuration Profile to the remaining group in one step by again right-clicking on the group and selecting "Apply Configuration Profile" (as described in **5.14 Applying Profiles** of this guide).