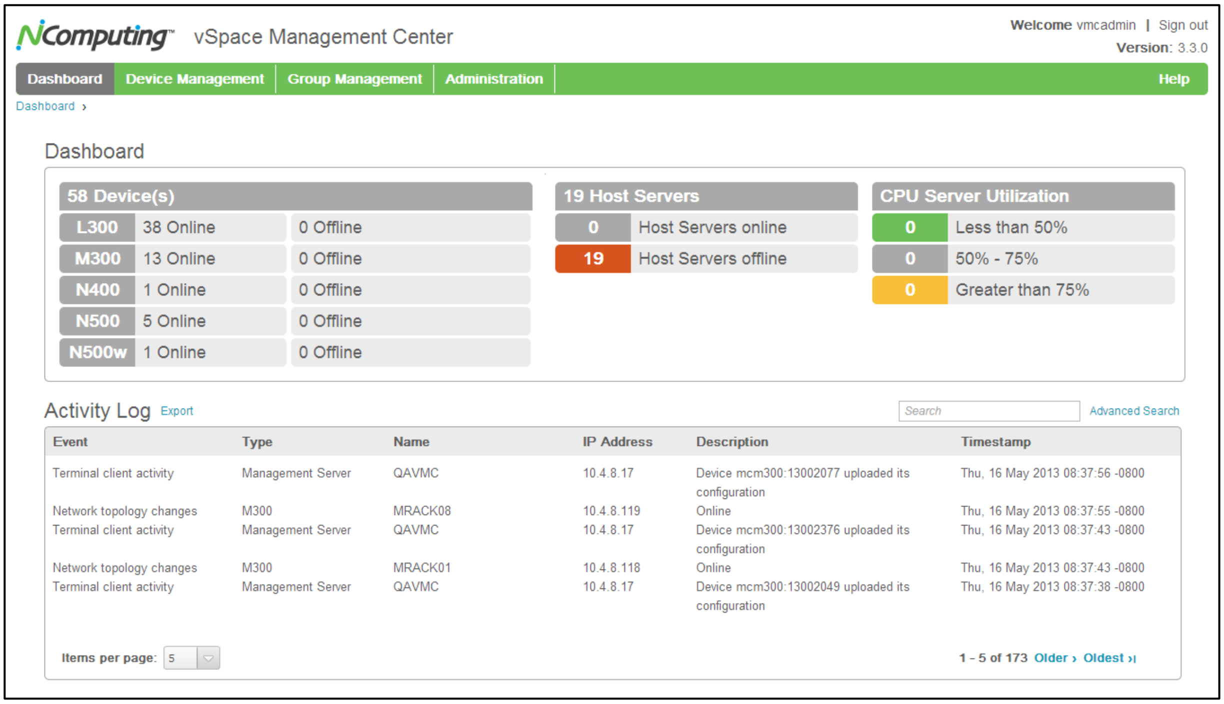
vSpace Management Center 3.3.0 for N-series and vSpace 7.0



Dashboard

58 Device(s)		
L300	38 Online	0 Offline
M300	13 Online	0 Offline
N400	1 Online	0 Offline
N500	5 Online	0 Offline
N500w	1 Online	0 Offline

19 Host Servers	
0	Host Servers online
19	Host Servers offline

CPU Server Utilization	
0	Less than 50%
0	50% - 75%
0	Greater than 75%

Activity Log

Event	Type	Name	IP Address	Description	Timestamp
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002077 uploaded its configuration	Thu, 16 May 2013 08:37:56 -0800
Network topology changes	M300	MRACK08	10.4.8.119	Online	Thu, 16 May 2013 08:37:55 -0800
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002376 uploaded its configuration	Thu, 16 May 2013 08:37:43 -0800
Network topology changes	M300	MRACK01	10.4.8.118	Online	Thu, 16 May 2013 08:37:43 -0800
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002049 uploaded its configuration	Thu, 16 May 2013 08:37:38 -0800

Items per page: 5

1 - 5 of 173

User Manual

Important Notices

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

The NComputing software products described in this user manual are protected by numerous granted and pending U.S. and international patents.

TABLE OF CONTENTS

1.0 vSpace Management Center Overview

For organizations deploying the NComputing N-series thin clients for Citrix HDX, or L300 and M300 access devices for vSpace 7.0, vSpace Management Center provides a highly scalable, flexible and easy to use single point of device management. With its web-based console, IT administrators can manage their NComputing devices from anywhere, anytime. vSpace Management Center helps organize a deployment whether it is a single site or multiple sites – and makes it easy to perform management tasks remotely including firmware updates, configuration changes, device resets and more. By allowing administrators to access and manage their servers and devices from a single location, regardless of the size or number of deployment sites, vSpace Management Center dramatically reduces the administrative overhead needed to maintain and control their environment.

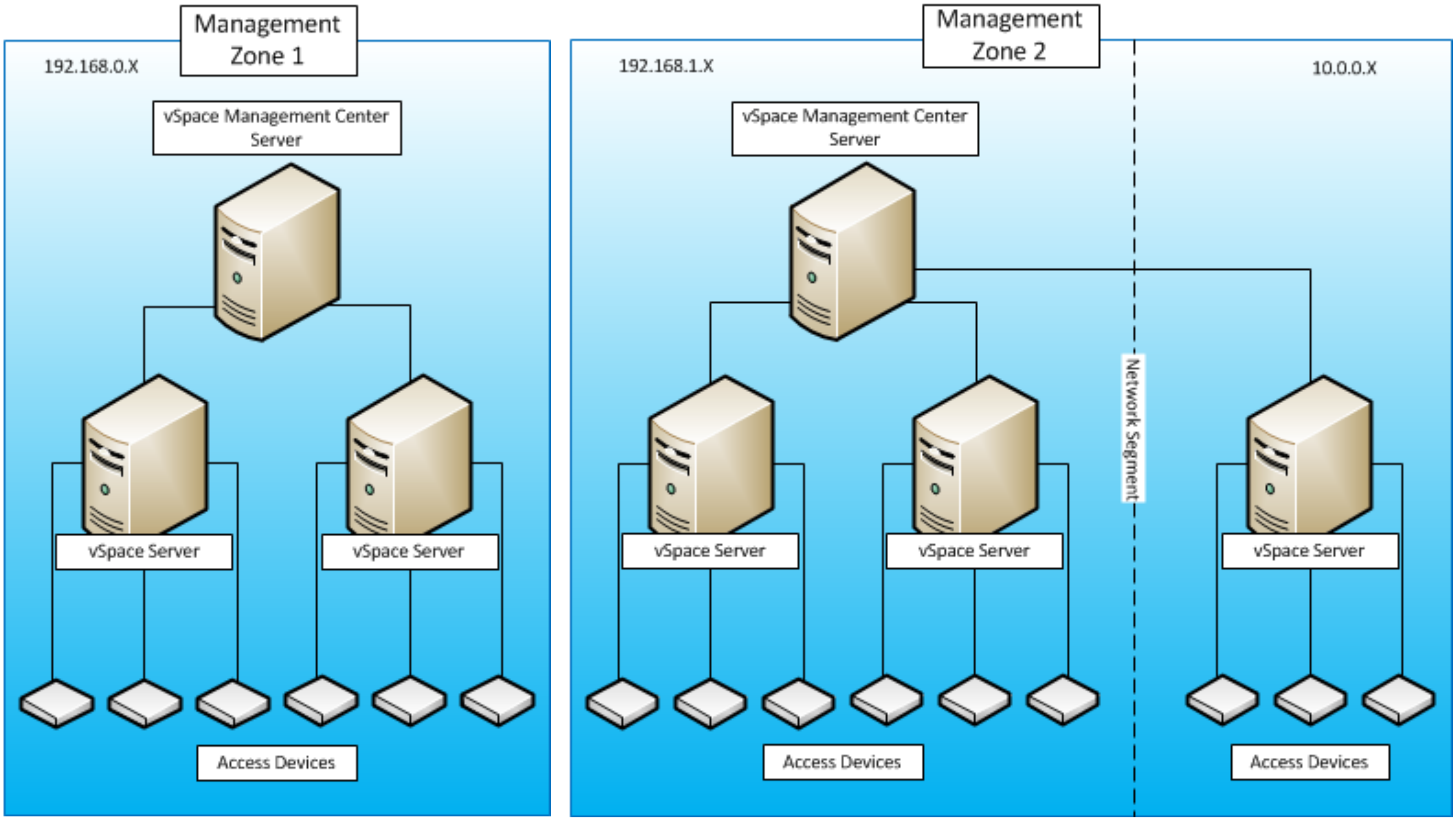
Key Features and Attributes

- **Centralized:** access an entire deployment from a single console
- **Scalable:** manage up to a thousand devices across multiple networks and locations
- **Simple:** easy to install and use with a flexible web-based user interface
- **Profile-based configuration:** assign devices to common profiles for scalable management of device settings
- **1:1 or 1:many management:** use profiles for 1:many management or push settings to an individual device
- **Easy firmware updates:** the firmware update wizard simplifies device updates and scheduling
- **Simple status:** the dashboard with logging and group views enables rapid assessment of your environment's status
- **Consolidated install:** install the complete vSpace Management Center via one installer in under 10 minutes
- **Comprehensive logging:** system events are continually logged to aid in troubleshooting and to confirm actions
- **Delegated Administration:** supports two levels of management for "view-only" and "edit-capable" access and can be easily configured via Active Directory/LDAP

This user manual provides a comprehensive guide to the features offered by vSpace Management Center as well as a detailed explanation of their functions. From remotely updating device firmware to backing up critical information and settings, this document will walk you through each step of using vSpace Management Center's powerful administrative toolset.

1.1 Management Zones

vSpace Management Center organizes vSpace servers and NComputing access devices into Management Zones. Each zone can be comprised of several 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. 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.

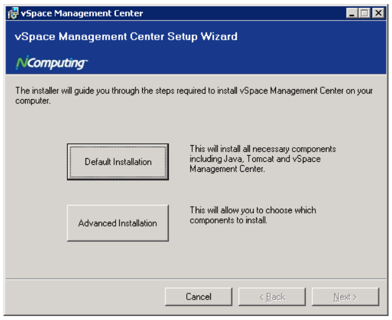
More information on Management Zone configuration is available in **section 6.4** of this manual.

2.0 Installation and Registration

This section of the guide will walk you through the installation and registration process for vSpace Management Center. Keep in mind that this document assumes the user has already acquired both the vSpace Management Center installation software and a number of licenses appropriate for their environment. For the latest NComputing software version please visit the NComputing software download site at http://www.ncomputing.com/downloads

2.1 Software Installation

The begin installation, run the vSpace Management Center installation (vSpace Management Center Installer.msi) and proceed as directed through the installation process.



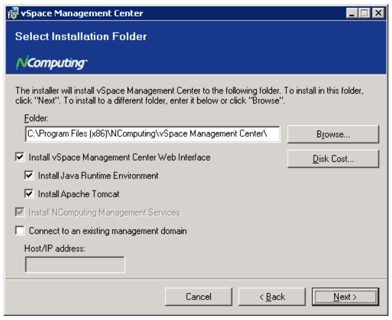
vSpace Management Center Setup Wizard

The installer will guide you through the steps required to install vSpace Management Center on your computer.

This will install all necessary components including Java, Tomcat and vSpace Management Center.

This will allow you to choose which components to install.

You will be given the option to perform a “Default” or “Advanced” installation. The Default method automatically installs all components necessary to run vSpace Management Center. This includes Java and Apache Server.



Select Installation Folder

The installer will install vSpace Management Center to the following folder. To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\NComputing\vSpace Management Center\

☑ Install vSpace Management Center Web Interface

☑ Install Java Runtime Environment

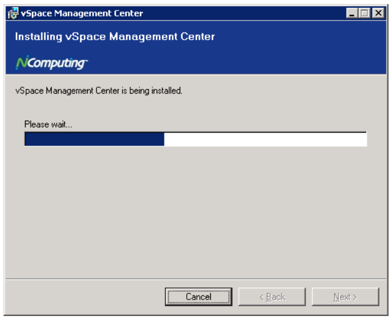
☑ Install Apache Tomcat

☑ Install NComputing Management Services

□ Connect to an existing management domain

Host/IP address:

The Advanced method gives you more control over which components are installed. You will also have the option to automatically join your new server to an existing vSpace Management Center management zone if this is not the first management server you have installed in your environment. For more information on Management Zone integration and Master / Slave server modes, review the following KB article: http://www.ncomputing.com/kb/HOW-TO-Configure-vSpace-Management-Center-Master-Slave-Mode_406.html



Installing vSpace Management Center

vSpace Management Center is being installed.

Please wait...

Once you have selected your installation method, proceed as directed through the installation process until you are notified that the process is complete. At this point a system restart will be required.

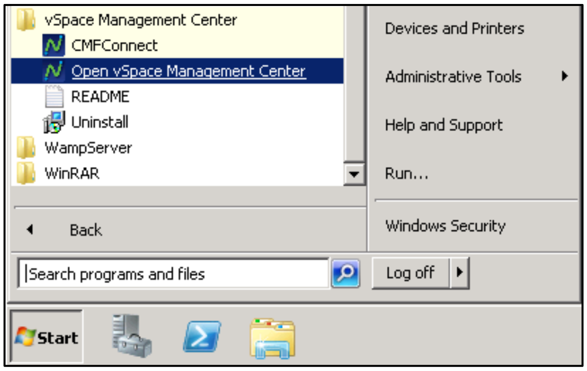
Note: Attempting to complete the installation process or run vSpace Management Center without the presence of Java and Apache Server will result in an error message. See the troubleshooting section for more information.

2.2 Registration

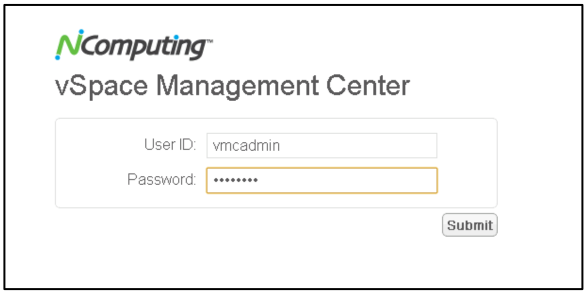
Each new install of vSpace Management Center includes a trial license for 30 days with up to 100 managed devices. For information on adding license keys to your vSpace Management Center server, review the Registration and Licensing section of this user manual.

2.3 Starting vSpace Management Center

Once you have successfully completed the installation process, you can access the vSpace Management Center user interface by opening the vSpace Management Center folder in the Windows Start menu (on the server you installed on). Click “Open vSpace Management Center” to launch the user interface within your default web browser. You can also access the interface from other computers on your network by opening a browser and entering the IP address of your server followed by: “:8080/vmc” For example, if your vSpace Management Center server’s IP address is: 192.168.1.10, then enter: “192.168.1.10:8080/vmc” in your browser.



Opening the vSpace Management Center user interface requires a User ID and Password. When you start vSpace Management Center for the first time, enter the default User ID (“vmcadmin”) and Password (“vmcadmin”) and click “Submit.”



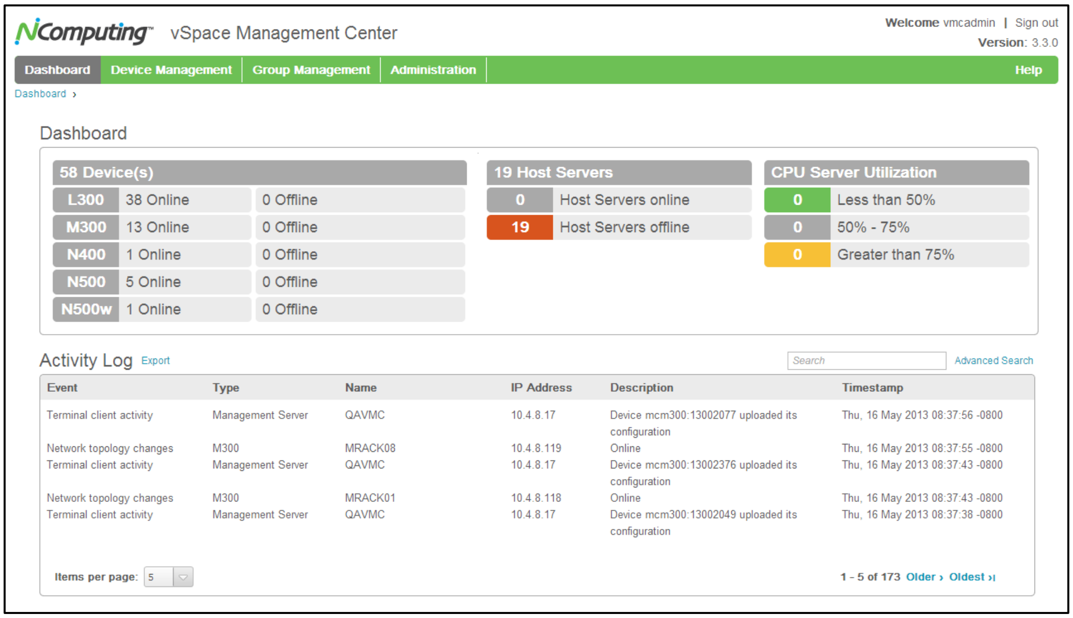
User ID: vmcadmin

Password: ••••••••

Note: It is recommended that you clear your browser’s cache prior to using vSpace Management Center for the first time and between updates.

3.0 vSpace Management Center Dashboard

The dashboard is the first screen you will see when connecting to your vSpace Management Center server. From here, you are presented with a brief summary of device and server status. By using the navigation bar along the top of the screen, you can access each of the management modules. This section will outline each of the functions available to you from this screen.



Dashboard

58 Device(s)		
L300	38 Online	0 Offline
M300	13 Online	0 Offline
N400	1 Online	0 Offline
N500	5 Online	0 Offline
N500w	1 Online	0 Offline

19 Host Servers	
0	Host Servers online
19	Host Servers offline

CPU Server Utilization	
0	Less than 50%
0	50% - 75%
0	Greater than 75%

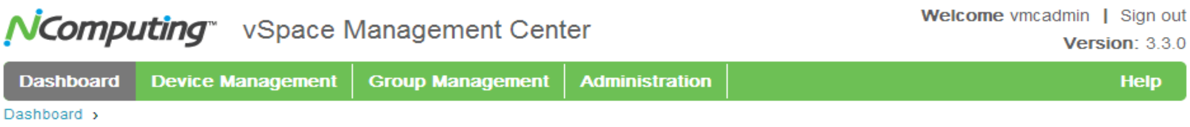
Activity Log Export — Search — Advanced Search

Event	Type	Name	IP Address	Description	Timestamp
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002077 uploaded its configuration	Thu, 16 May 2013 08:37:56 -0800
Network topology changes	M300	MRACK08	10.4.8.119	Online	Thu, 16 May 2013 08:37:55 -0800
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002376 uploaded its configuration	Thu, 16 May 2013 08:37:43 -0800
Network topology changes	M300	MRACK01	10.4.8.118	Online	Thu, 16 May 2013 08:37:43 -0800
Terminal client activity	Management Server	QAVMC	10.4.8.17	Device mcm300:13002049 uploaded its configuration	Thu, 16 May 2013 08:37:38 -0800

Items per page: 5 — 1 - 5 of 173 Older › Oldest ›|

3.1 The Navigation Bar

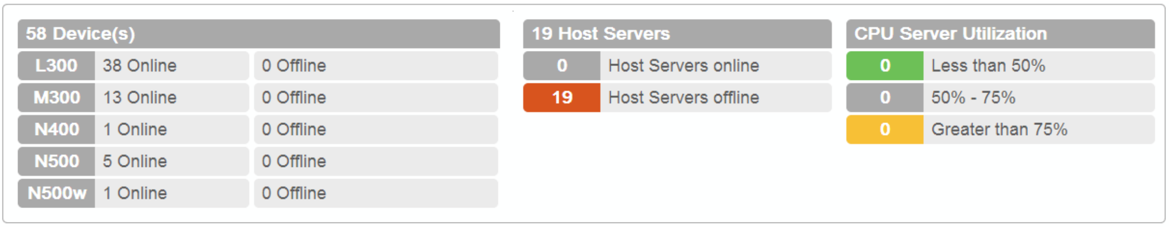
The Navigation Bar is your primary means of navigating between vSpace Management Center's various modules. As seen below, it offers access to Device Management, Group Management, vSpace Management Center Settings, as well as the Help feature.



Note the breadcrumb navigation feature to the bottom left of the Navigation Bar. As you navigate deeper within vSpace Management Center, this will track each step you have taken and give you the ability to step backwards through vSpace Management Center until you have returned to the Dashboard.

3.2 The Dashboard Summary

The Dashboard Summary provides at-a-glance information on the connection status of your access devices, hosts, and CPU utilization.



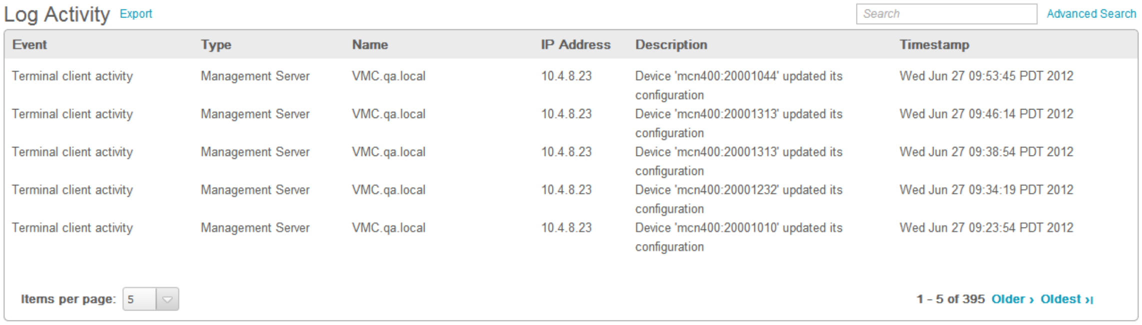
58 Device(s)		
L300	38 Online	0 Offline
M300	13 Online	0 Offline
N400	1 Online	0 Offline
N500	5 Online	0 Offline
N500w	1 Online	0 Offline

19 Host Servers	
0	Host Servers online
19	Host Servers offline

CPU Server Utilization	
0	Less than 50%
0	50% - 75%
0	Greater than 75%

3.3 Log Activity

The Log Activity section of the dashboard presents a detailed breakdown of recent server and device activity. You can search for specific log information through the use of the Advanced Search button located at the top right of the activity list.

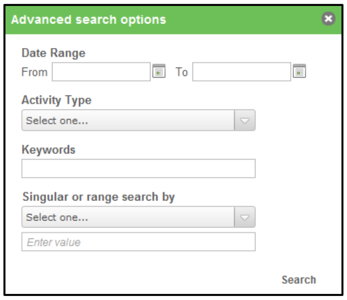


Log Activity Export

Event	Type	Name	IP Address	Description	Timestamp
Terminal client activity	Management Server	VMC.qa.local	10.4.8.23	Device 'mcn400:20001044' updated its configuration	Wed Jun 27 09:53:45 PDT 2012
Terminal client activity	Management Server	VMC.qa.local	10.4.8.23	Device 'mcn400:20001313' updated its configuration	Wed Jun 27 09:46:14 PDT 2012
Terminal client activity	Management Server	VMC.qa.local	10.4.8.23	Device 'mcn400:20001313' updated its configuration	Wed Jun 27 09:38:54 PDT 2012
Terminal client activity	Management Server	VMC.qa.local	10.4.8.23	Device 'mcn400:20001232' updated its configuration	Wed Jun 27 09:34:19 PDT 2012
Terminal client activity	Management Server	VMC.qa.local	10.4.8.23	Device 'mcn400:20001010' updated its configuration	Wed Jun 27 09:23:54 PDT 2012

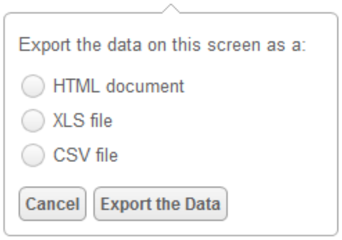
Items per page: 5

1 - 5 of 395 Older › Oldest ›|



The Advanced Search Options menu allows you to search for activities by time and date, activity type, keyword search, and by a singular or range search. Once you have entered the criteria you wish to search by, press the “Search” button to begin your search.

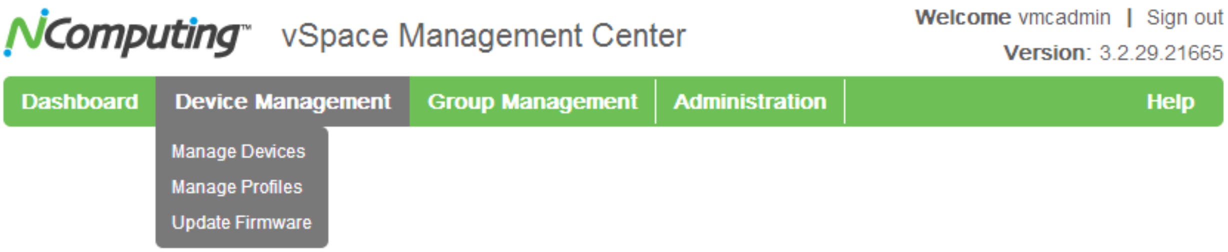
You can export search results to HTML, XLS, or CSV file formats using the “Export” button located to the top left of the Log Activity section.



Export the data on this screen as a:

○ HTML document
○ XLS file
○ CSV file

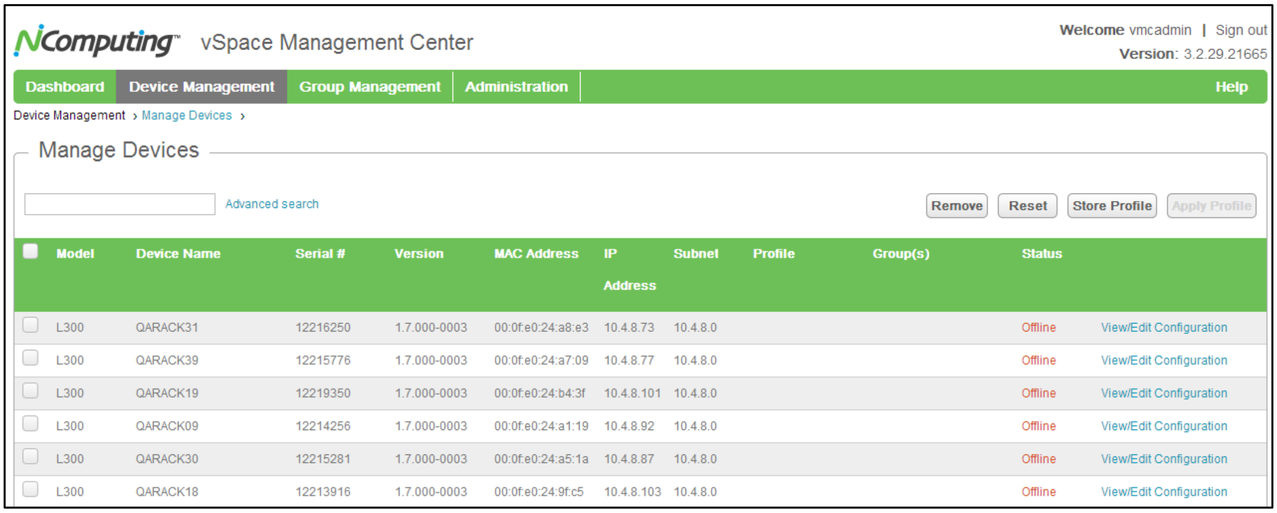
4.0 Device Management



The Device Management module of vSpace Management Center allows administrators to remotely configure their devices, create and manage device profiles, and push firmware updates. This section of the manual will outline each of these functions in detail.

4.1 Manage Devices

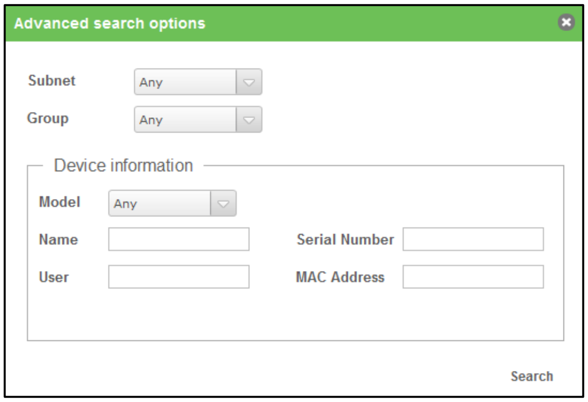
The Manage Devices screen presents the user with a list of the devices that they currently have linked with vSpace Management Center. From this screen you can perform basic administrative tasks such as applying or storing profiles, resetting devices, and verifying device information such as: Device Name, IP address, Serial Numbers, Firmware versions, and Device Model.



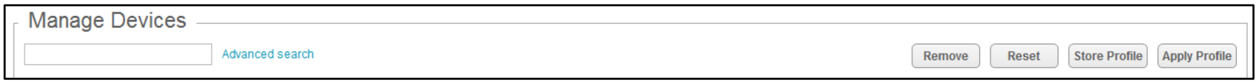
□	Model	Device Name	Serial #	Version	MAC Address	IP Address	Subnet	Profile	Group(s)	Status	
□	L300	QARACK31	12216250	1.7.000-0003	00:0f:e0:24:a8:e3	10.4.8.73	10.4.8.0			Offline	View/Edit Configuration
□	L300	QARACK39	12215776	1.7.000-0003	00:0f:e0:24:a7:09	10.4.8.77	10.4.8.0			Offline	View/Edit Configuration
□	L300	QARACK19	12219350	1.7.000-0003	00:0f:e0:24:b4:3f	10.4.8.101	10.4.8.0			Offline	View/Edit Configuration
□	L300	QARACK09	12214256	1.7.000-0003	00:0f:e0:24:a1:19	10.4.8.92	10.4.8.0			Offline	View/Edit Configuration
□	L300	QARACK30	12215281	1.7.000-0003	00:0f:e0:24:a5:1a	10.4.8.87	10.4.8.0			Offline	View/Edit Configuration
□	L300	QARACK18	12213916	1.7.000-0003	00:0f:e0:24:9f:c5	10.4.8.103	10.4.8.0			Offline	View/Edit Configuration

4.2 Advanced Search

By clicking “Advanced Search” at the top left of the Manage Devices screen, you gain access to the Advanced Search Options menu. From here, you can search for devices by specifying a number of details including Subnet and Device Group, or specific device information such as Device Model, Name, Serial Number, MAC address, or even the name of the user currently logged in to the device.



4.3 Remove, Reset, Store Profile, Apply Profile



Along the top right section of the Manage Devices screen are four buttons that will allow you to perform common management functions. Select one or more devices by clicking the checkbox to the left of the devices in question and then click on the desired function.

Remove

Remove the selected device(s) from vSpace Management Center. See section **Section 7.1 Adding a Device to vSpace Management Center** if you wish to link the device(s) with vSpace Management Center again in the future. Note that you will only be able to remove devices that show up as being “offline.” If no devices are currently offline, the “Remove” button will be grey and inactive.

Reset

Reset the selected device(s). NOTE: Be sure to verify whether the device is currently in use as this will immediately interrupt the user’s session and restart the device (similar to powering off the device and powering it back on).

Store Profile

Store the configuration options currently in use by this device as a profile that can later be applied to any device of the same model.

Apply Profile

Select from a list of currently stored device profiles and apply that profile to the selected device(s). NOTE: Be sure to verify whether the device is currently in use as this will immediately interrupt the user’s session.

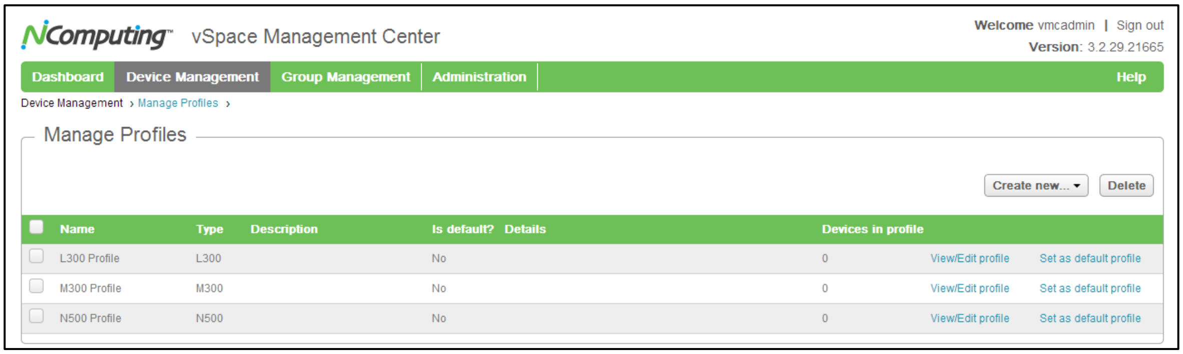
4.4 View/Edit Configuration

To the far right of each device entry you will find a link called “View/Edit Configuration”. Clicking this button will bring up an interface that allows you to view and make changes to the device you selected. These options will vary by device model. The interface for making these changes is similar to the interface for creating and editing profiles per the following section. The only difference is that when you are in the View/Edit Configuration screens, the data in the fields for the specific device will be pre-populated. Specific configuration options are covered in detail in **Section 5.0** and **6.0** of this manual.

4.5 Manage Profiles

The Manage Profiles screen allows you to create, view or edit device profiles. A profile is a common set of configurations for a particular device type in your environment. When you create a profile, you can associate one or more devices to that profile – and from that point on, the devices will continue to be associated with the profile. This means that if you later edit the profile settings, all devices associated with that profile will be updated with the new settings as well. This makes it very easy to manage common settings in a large number of devices simultaneously.

To begin, click either the “Create New” button and select a device type, or click the View/Edit Profile button next to an existing profile in the profile list.



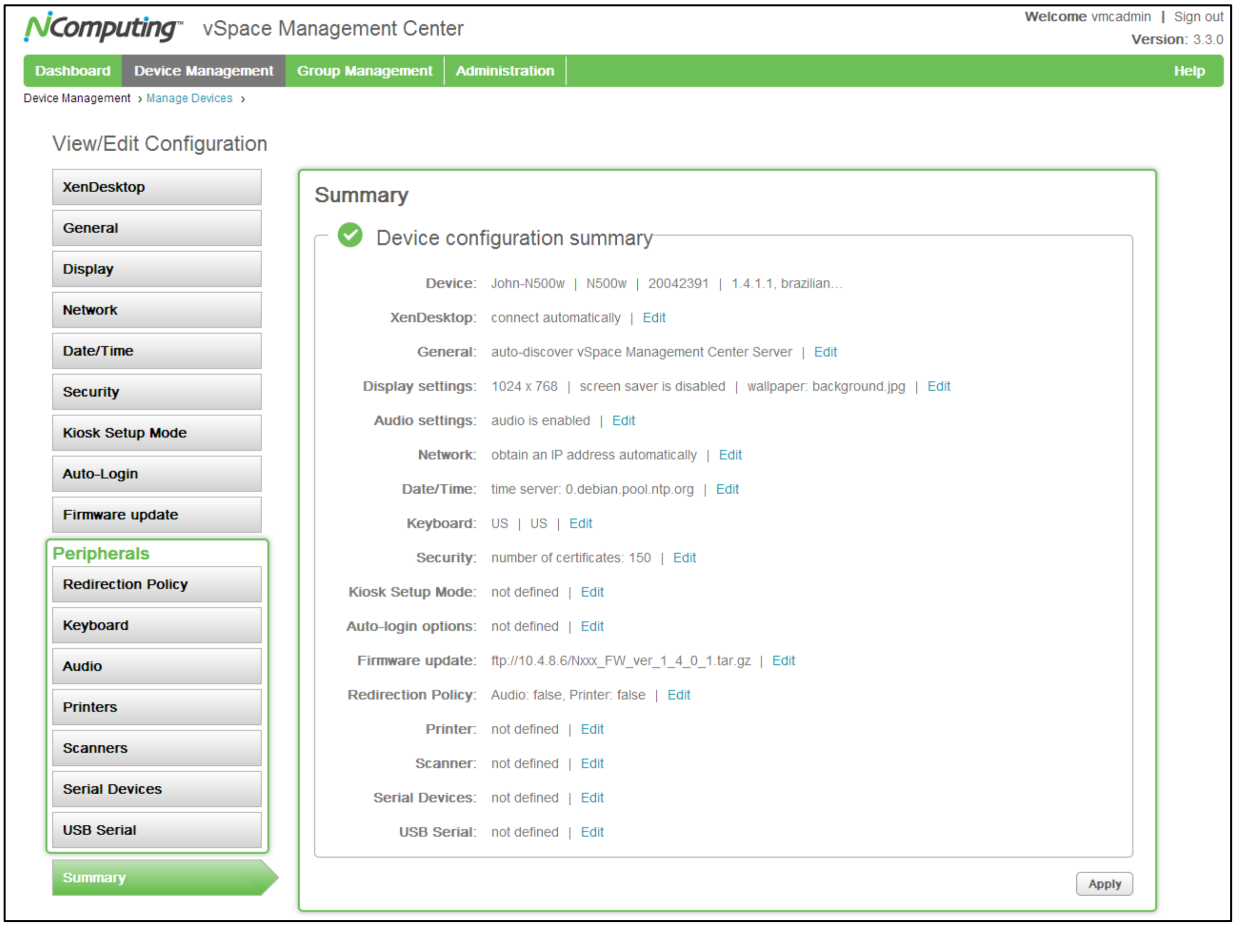
Manage Profiles

□	Name	Type	Description	Is default?	Details	Devices in profile		
□	L300 Profile	L300		No		0	View/Edit profile	Set as default profile
□	M300 Profile	M300		No		0	View/Edit profile	Set as default profile
□	N500 Profile	N500		No		0	View/Edit profile	Set as default profile

Next, you will be taken to the profile wizard where you can name your profile and create a description for future reference. Step through each of the subsequent screens to configuration your profile. Note that a profile does not need to include all the settings of the device. For example, you may wish to have some settings configured uniquely for each device and not set by the common profile. To facilitate this, each component of the profile can be enabled or disabled by checking the box at the top of each section labeled “Edit Settings.” If a section is unchecked for a specific profile, the local data in the device will be preserved and not affected by the profile.

Proceed through the wizard to configure (or skip) each setting screen. The last screen shows a summary of the settings and has the "Apply" button. When you click the "Apply" button the settings in the profile will be pushed to all of the devices that you associated it with. Note that you can also store and apply profiles from the Manage Devices screen, by using an existing device's settings as a template (see section 9.3 Configuring devices using device profiles).

(Below, the configuration tabs for an N-series device can be seen)



Device configuration summary

Device: John-N500w | N500w | 20042391 | 1.4.1.1, brazilian...

XenDesktop: connect automatically | Edit

General: auto-discover vSpace Management Center Server | Edit

Display settings: 1024 x 768 | screen saver is disabled | wallpaper: background.jpg | Edit

Audio settings: audio is enabled | Edit

Network: obtain an IP address automatically | Edit

Date/Time: time server: 0.debian.pool.ntp.org | Edit

Keyboard: US | US | Edit

Security: number of certificates: 150 | Edit

Kiosk Setup Mode: not defined | Edit

Auto-login options: not defined | Edit

Firmware update: ftp://10.4.8.6/Nxxx_FW_ver_1_4_0_1.tar.gz | Edit

Redirection Policy: Audio: false, Printer: false | Edit

Printer: not defined | Edit

Scanner: not defined | Edit

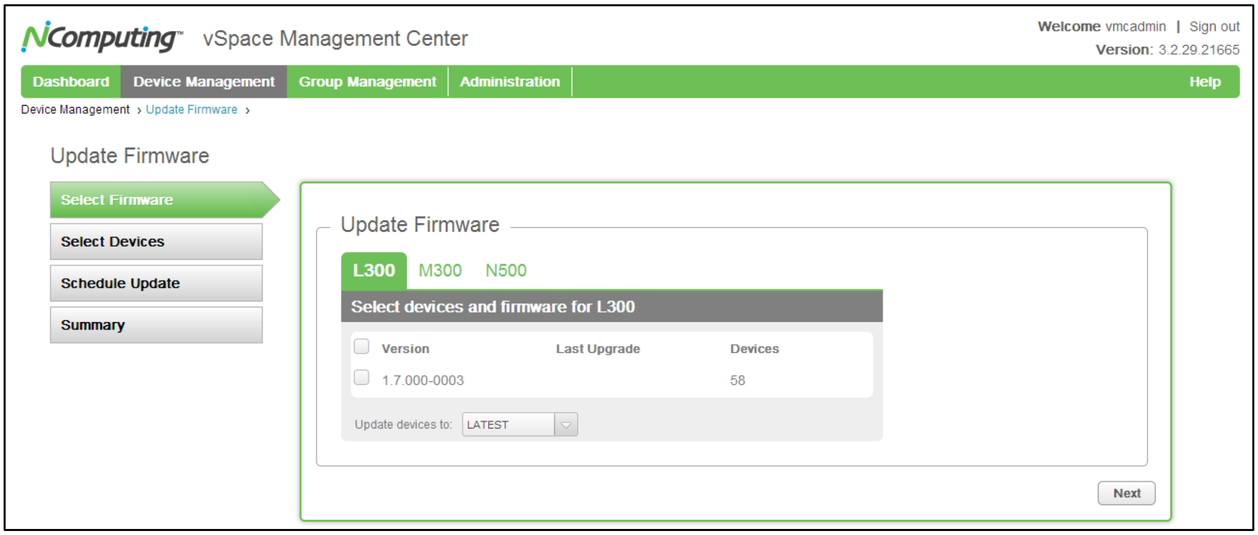
Serial Devices: not defined | Edit

USB Serial: not defined | Edit

IMPORTANT: Note that if, at any time, you overwrite a profile's setting in a particular device by either changing the setting manually via the local user interface on the device or by using the edit configuration function (see 4.1 Manage Devices) then that manually-configured setting will no longer pull from the profile and the device will always use this manually overridden setting. If you wish to revert the device to use the profile for that setting, you must first remove the device from the profile (edit profile, deselect the device, and apply the profile) and then re-attach it (edit profile, select the device, and apply the profile).

4.6 Update Firmware

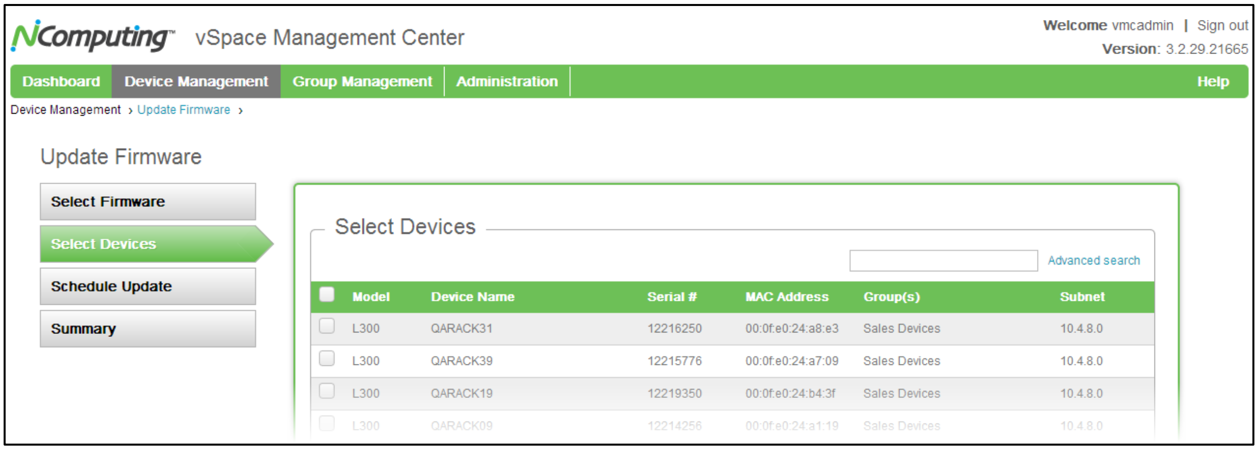
The Update Firmware screen allows you to select from a list of currently available firmware versions and then push a selected version of firmware to one or more devices.



□ Version	Last Upgrade	Devices
□ 1.7.000-0003		58

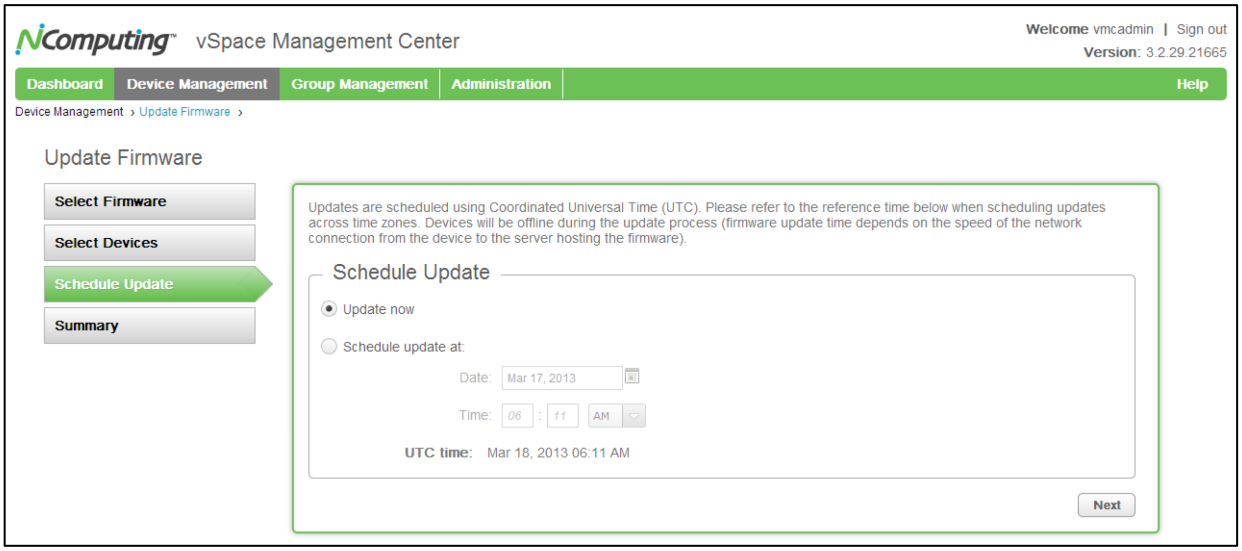
Update devices to: LATEST

To begin a firmware update, select the firmware version from the list provided for the device model in question, and then press "Next". To upload new firmware versions for your devices refer to **6.3 Manage Firmware**.



□ Model	Device Name	Serial #	MAC Address	Group(s)	Subnet
□ L300	QARACK31	12216250	00:0f:e0:24:a8:e3	Sales Devices	10.4.8.0
□ L300	QARACK39	12215776	00:0f:e0:24:a7:09	Sales Devices	10.4.8.0
□ L300	QARACK19	12219350	00:0f:e0:24:b4:3f	Sales Devices	10.4.8.0
□ L300	QARACK09	12214256	00:0f:e0:24:a1:19	Sales Devices	10.4.8.0

Next, select the devices you wish to push this firmware to and press "Next".



Update Firmware

Updates are scheduled using Coordinated Universal Time (UTC). Please refer to the reference time below when scheduling updates across time zones. Devices will be offline during the update process (firmware update time depends on the speed of the network connection from the device to the server hosting the firmware).

Schedule Update

● Update now

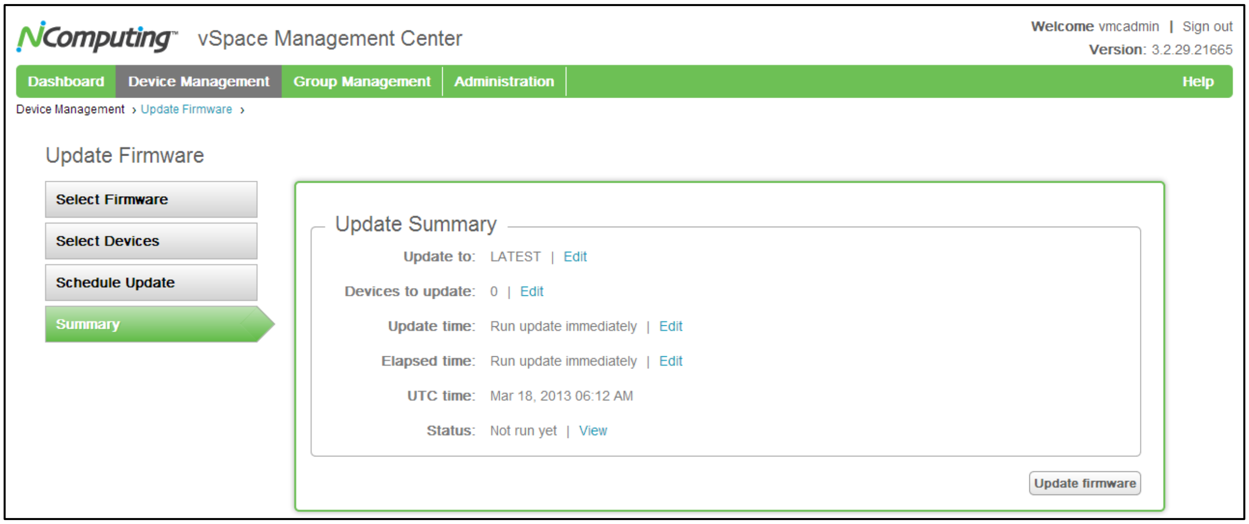
○ Schedule update at:

Date: Mar 17, 2013

Time: 06 : 11 AM

UTC time: Mar 18, 2013 06:11 AM

At this stage, you'll be given the option to push the firmware immediately, or schedule the update for a future date and time. This is especially useful if you wish to perform the update later in the day when usage is at a minimum (firmware updates will cause a device reboot and will disconnect users from their session). Press "Next" when you have selected a time for the update.



Update Firmware

Update Summary

Update to: LATEST | Edit

Devices to update: 0 | Edit

Update time: Run update immediately | Edit

Elapsed time: Run update immediately | Edit

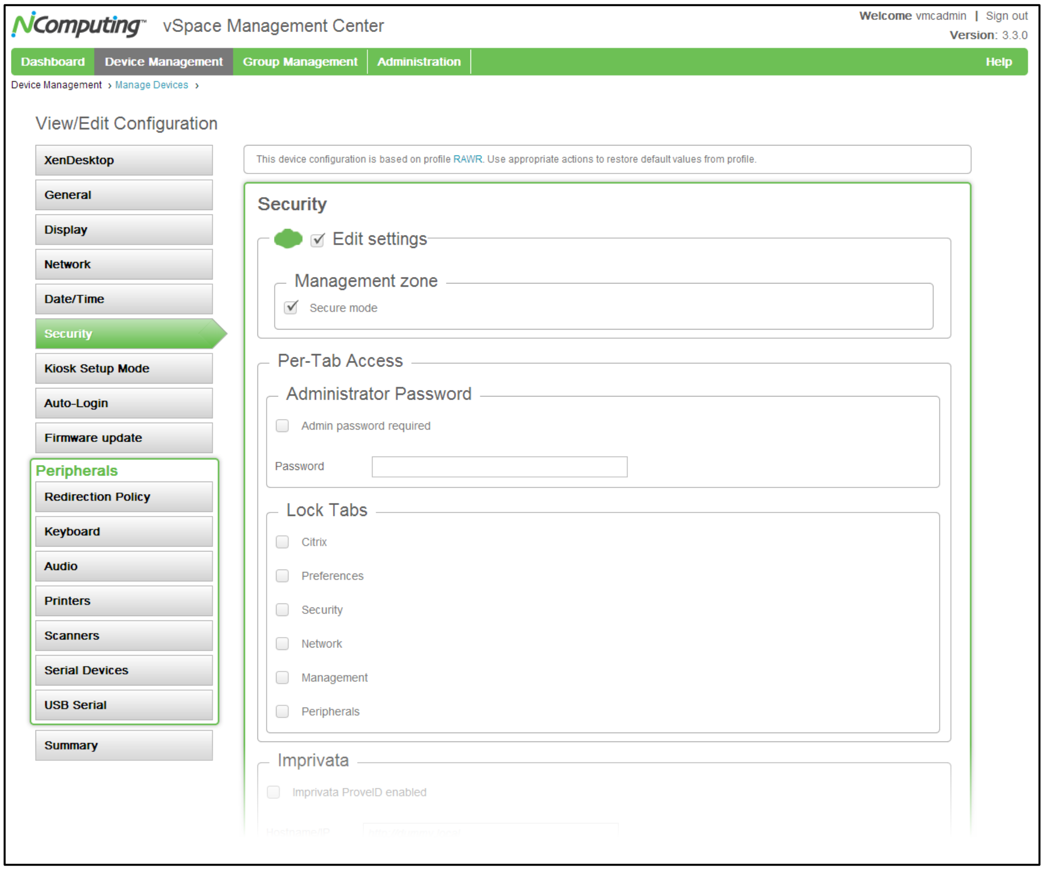
UTC time: Mar 18, 2013 06:12 AM

Status: Not run yet | View

Lastly, you will be presented with a summary of the choices you have made including firmware version, device to be updated, the timing of the update, and other details. Once you are satisfied with the update plan, press "Update firmware" to initiate the update.

4.7 Manage Device Security Settings

The **Security Tab** allows administrators to enable and configure device passwords as well as manage CA Certificates, which are used for establishing and validating SSL connections. This tab can be found by selecting **View/Edit Configuration** next to any device in the **Manage Devices** list or by editing a profile.



View/Edit Configuration

This device configuration is based on profile RAWR. Use appropriate actions to restore default values from profile.

Security

☑ Edit settings

Management zone

☑ Secure mode

Per-Tab Access

Administrator Password

□ Admin password required

Password

Lock Tabs

□ Citrix

□ Preferences

□ Security

□ Network

□ Management

□ Peripherals

Imprivata

□ Imprivata ProveID enabled

Hostname/IP http://dummy.local

Change Password

To protect a device’s settings from unwanted changes, click the checkbox next to “enable password” and then enter the password you wish to associate with the device in question.

Management Zone

Within the Management Zone section, you can elect to enable Secure Mode, which will “lock” the device(s) in question to their current Management Zone. This prevents them from being altered or managed by any other Zones. To move a device configured in this way to another Zone, you must first disable Secure Mode from vSpace Management Center or at the device itself.

For N-series devices, this can be done from the Security Tab. L-series and M-series devices must be “reset” using either the CTRL-SHIFT-END method at the device password screen or the physical reset button on the back of the device.

Add Certificates (N-series only)

Click the “Choose file” button and browse to the location of your .CER and/or .CRT files to add certificates to the selected device(s).

Available Certificates (N-series only)

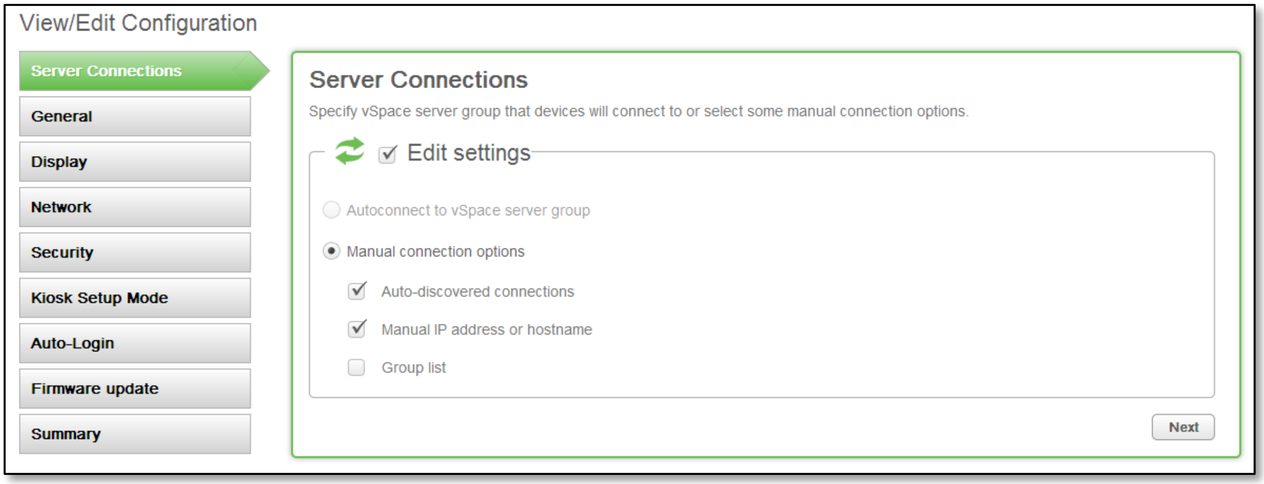
This portion of the security screen provides a list of all certificates currently associated with the device(s). Click the “Details” button to the right of any certificate for more information on that specific certificate.

5.0 L/M-series Configuration

The L300 and M300 product lines share a nearly identical user interface, with the exception of the M300 supporting three sessions per kit while the L300 is a single-user product. The following sections detail each of the configuration tabs found within the View / Edit Configuration menu of L300 and M300 access devices.

5.1 Server Connections Tab

The Server Connections tab allows administrators to determine how a device connects to a vSpace Server. Settings include server discovery modes and the ability to enable connection by server groups.



Server Connections

Specify vSpace server group that devices will connect to or select some manual connection options.

☑ Edit settings

○ Autoconnect to vSpace server group

● Manual connection options

☑ Auto-discovered connections

☑ Manual IP address or hostname

□ Group list

- **<u>Autoconnect to vSpace server group</u>**
  Select to connect to an existing vSpace Server group.

- **<u>Manual connection options</u>**
  Select to manually select a server.

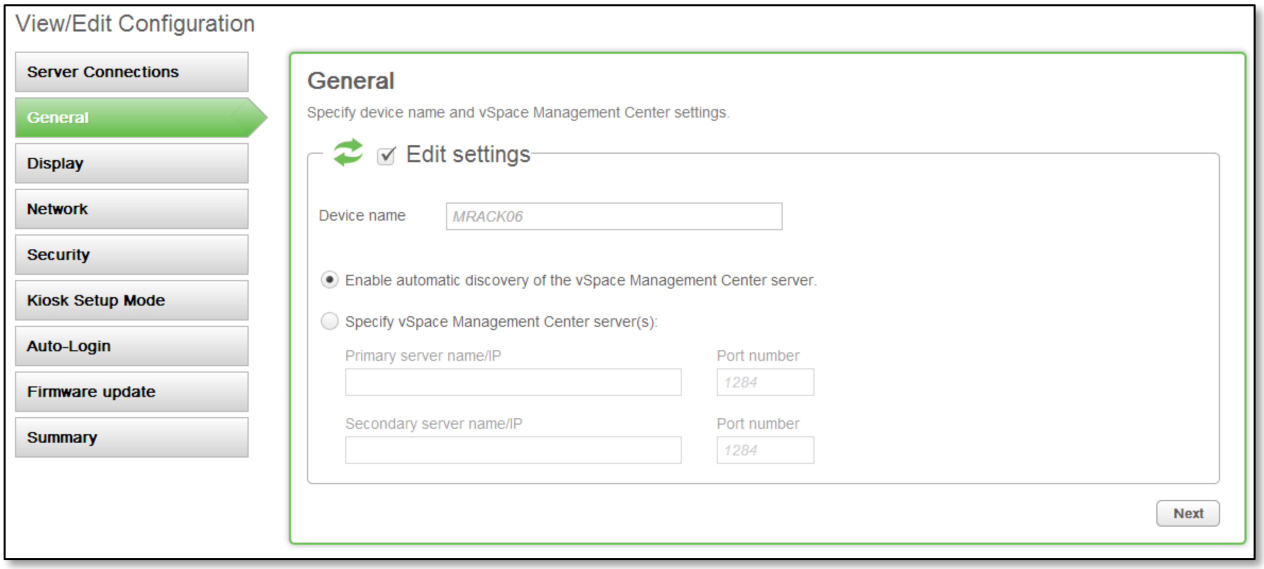
- **<u>Auto-discovered connections</u>**
  When checked, the device will populate the server list with any servers found within its subnet.

- **<u>Manual IP address or hostname</u>**
  When checked, the device will allow the user to discover servers based on their IP address or hostname.

- **<u>Group list</u>**
  When checked, the server list will include any available server groups.

5.2 General Tab

The General Tab allows the administrator to edit general device settings such as Management Zone and device name.



View/Edit Configuration

General

Specify device name and vSpace Management Center settings.

☑ Edit settings

Device name: MRACK06

● Enable automatic discovery of the vSpace Management Center server.

○ Specify vSpace Management Center server(s):

Primary server name/IP:

Port number: 1284

Secondary server name/IP:

Port number: 1284

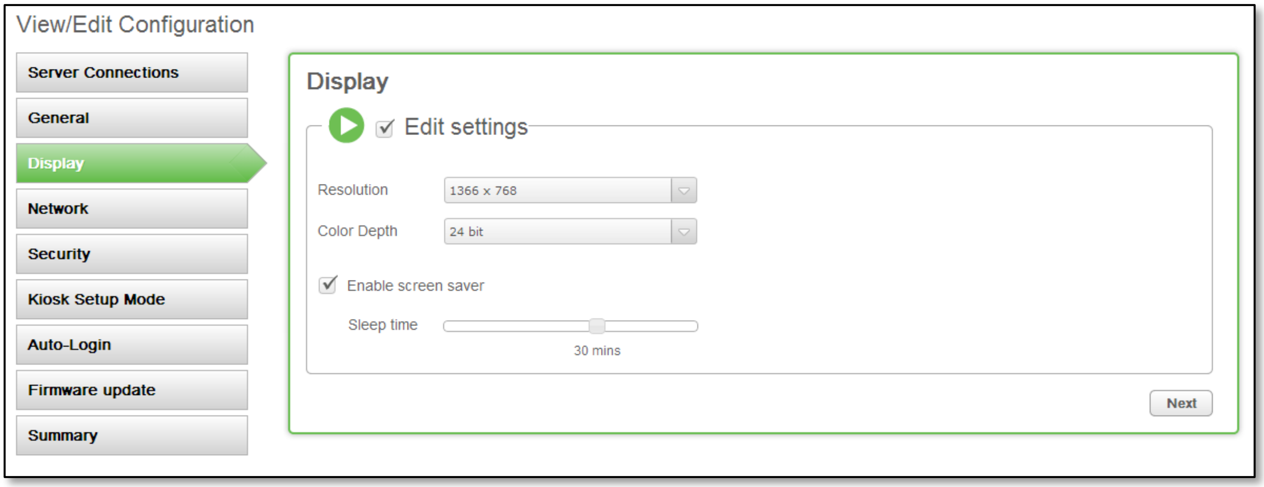
- **Device Name**
  Use this field to alter the L300 or M300 device name. This can be used to help sort devices based on use, location, or user, for example.

- **Enable automatic discovery of the vSpace Management Center server**
  Enabling this feature allows a device to automatically discover a vSpace Management Center server within its subnet or within the Management Zone governing it’s vSpace Server.

- **Specify vSpace Management Center server(s)**
  Selecting this option allows administrators to specify which vSpace Management Center server the device should associate with (and by extension, which Management Zone). A primary and secondary server may be specified for failover purposes.

5.3 Display Tab

The Display Tab contains configuration options related to screen resolution and behavior.



View/Edit Configuration

Display

☑ Edit settings

Resolution: 1366 x 768

Color Depth: 24 bit

☑ Enable screen saver

Sleep time: 30 mins

- **Resolution**
  This dropdown menu contains all monitor resolutions compatible with the device in question.

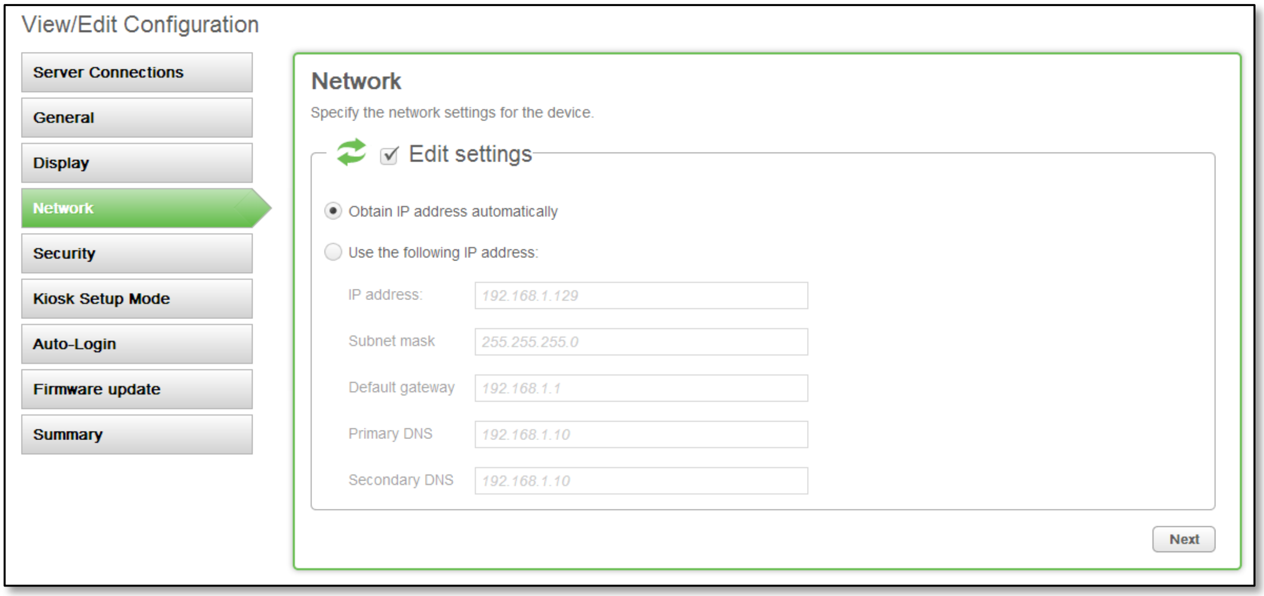
- **Color Depth**
  This dropdown can be used to select display color depth.

- **Enable screen saver**
  Check to enable the device screen saver, which will turn off the display signal and allow the connected monitor to enter its power save mode once idle for a specified period of time.

- **Sleep time**
  This slider allows the administrator to select the amount of idle time a device will wait before entering screen saver mode.

5.4 Network Tab

The network tab contains a full set of common network settings to be used by the selected device.



View/Edit Configuration

Network

Specify the network settings for the device.

☑ Edit settings

● Obtain IP address automatically

○ Use the following IP address:

IP address: 192.168.1.129

Subnet mask 255.255.255.0

Default gateway 192.168.1.1

Primary DNS 192.168.1.10

Secondary DNS 192.168.1.10

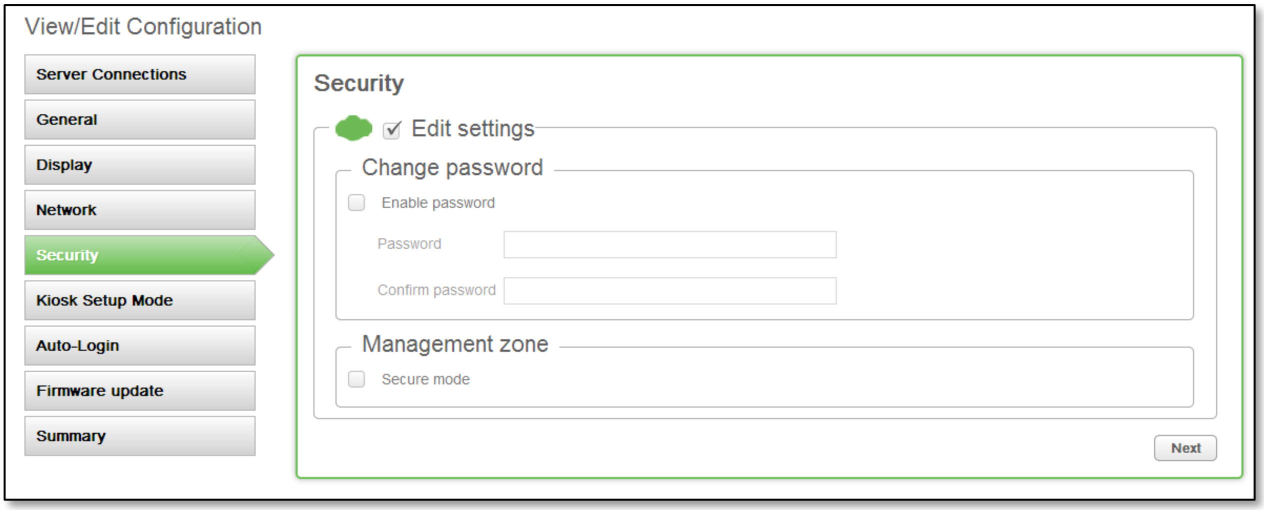
- **Obtain IP address automatically**
  Selecting this option places the device into DHCP mode, causing it to automatically obtain its network settings from the local DHCP server.

- **Use the following IP address**
  Selecting this option allows the administrator to specify their device's network settings.

- **IP address, Subnet mask, Default gateway, Primary DNS, Secondary DNS**
  Standard network settings, including a secondary DNS field for failover purposes.

5.5 Security Tab

The Security Tab contains features designed to help administrators secure their access devices.


View/Edit Configuration

Security

☑ Edit settings

Change password

□ Enable password

Password

Confirm password

Management zone

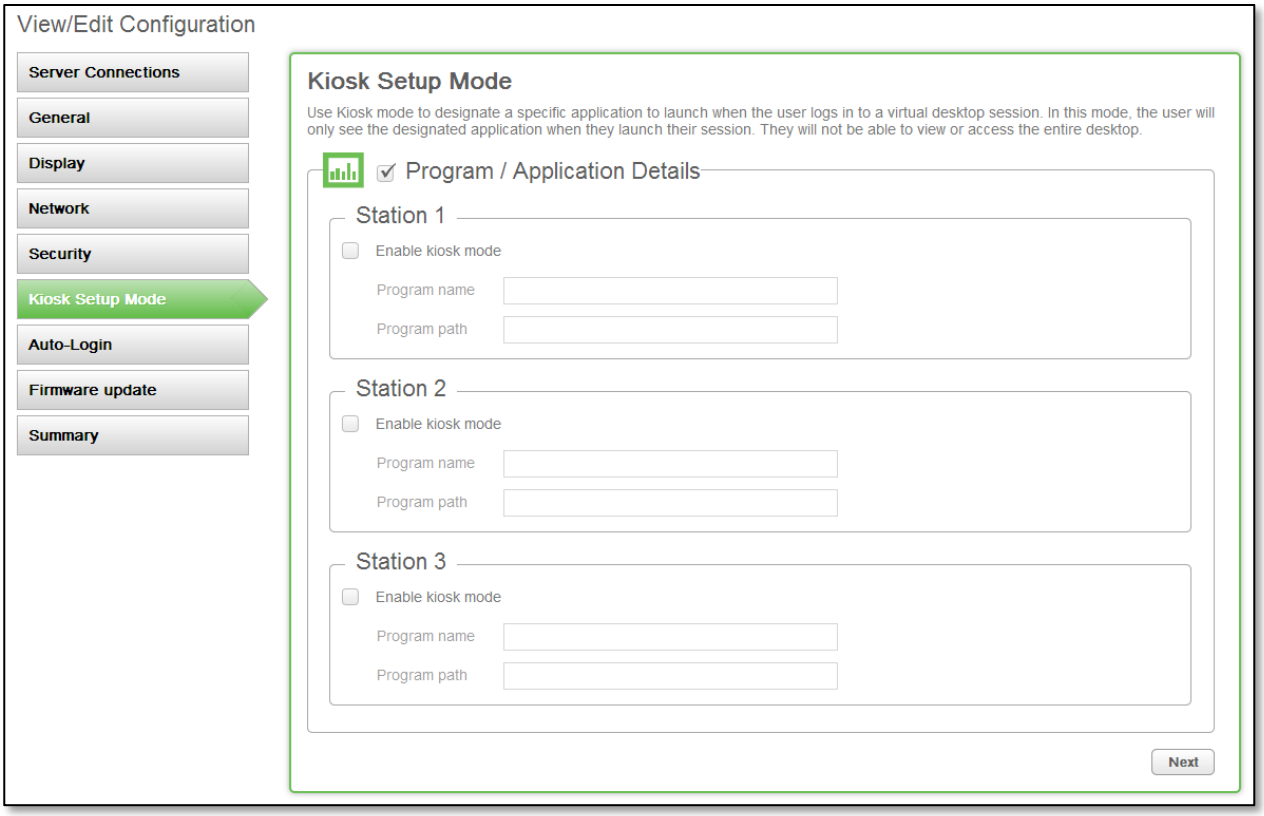
□ Secure mode

- **Enable Password**
  Enabling the password feature on an access device allows administrators to restrict a user's ability to change settings on the device once they're configured. The fields within this setting allow an administrator to enable this feature and set or change a password.

- **Management zone (secure mode)**
  Enabling secure mode for a device prevents it from automatically joining a new Management Zone in the event that it loses connection with its current Zone. Disabling this feature allows the device to automatically connect to another Zone (if one is available).

5.6 Kiosk Setup Mode

The Kiosk Setup Mode Tab can be used to instruct a device to launch a specific application or file when logging into the Windows environment rather than launching the full Windows Explorer interface. This can be used to set up demo booths, displays, or other scenarios where non-standard environments are required.



Kiosk Setup Mode

Use Kiosk mode to designate a specific application to launch when the user logs in to a virtual desktop session. In this mode, the user will only see the designated application when they launch their session. They will not be able to view or access the entire desktop.

☑ Program / Application Details

Station 1

□ Enable kiosk mode

Program name

Program path

Station 2

□ Enable kiosk mode

Program name

Program path

Station 3

□ Enable kiosk mode

Program name

Program path

- **Enable Kiosk Mode***
  This box must be checked to enable Kiosk Mode.

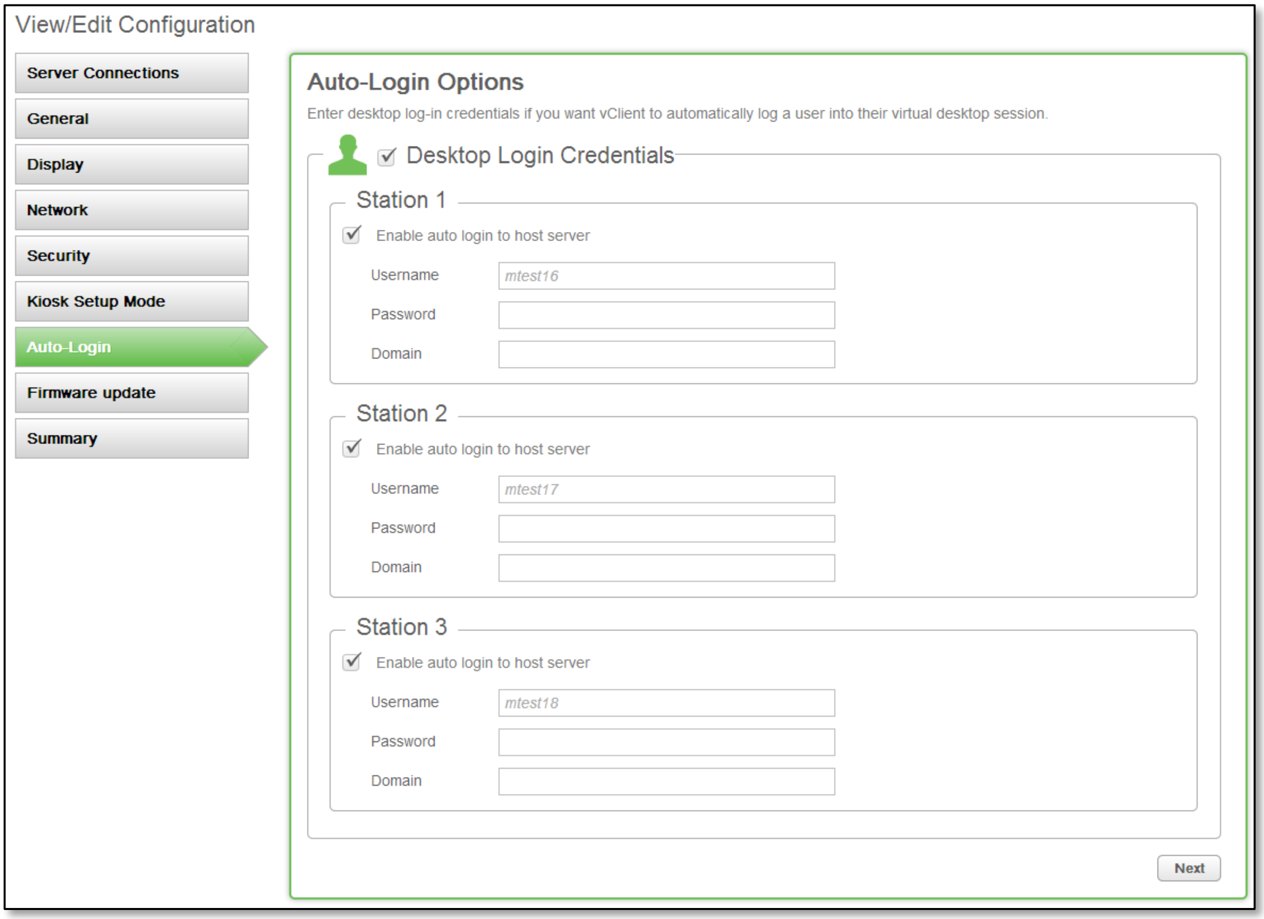
- **Program Name**
  Enter the full name of the application or file (for example: ***DemoVideo.wmv***)

- **Program Path**
  Enter the full file path of the application or file (for example: ***C:\users\public\videos\DemoVideo.wmv***)

*Note that the M300 has three discreet access devices per kit. The L300 lists only one station, as it is a single-user device.

5.7 Auto-Login Options Tab

The Auto-Login Options Tab provides administrators with a means of automatically logging their devices in to a Windows session using pre-specified credentials as soon as they connect to a given server.



Auto-Login Options

Enter desktop log-in credentials if you want vClient to automatically log a user into their virtual desktop session.

☑ Desktop Login Credentials

Station 1

☑ Enable auto login to host server

Username: mtest16

Password:

Domain:

Station 2

☑ Enable auto login to host server

Username: mtest17

Password:

Domain:

Station 3

☑ Enable auto login to host server

Username: mtest18

Password:

Domain:

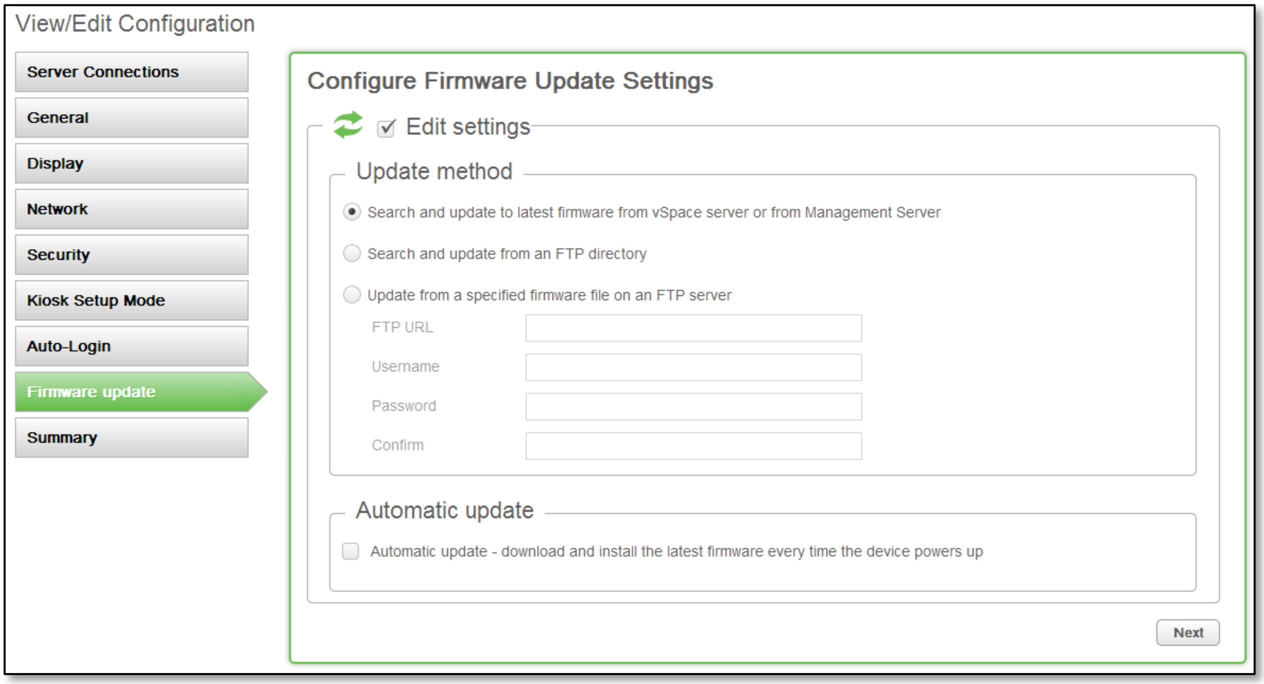
- **<u>Enable auto login to host server</u>**
  Check to enable auto login of the selected station*

- **<u>Username, Password, Domain</u>**
  Enter the desired Windows login credentials and domain information into these fields.

*Note that the M300 has three discreet access devices per kit. The L300 lists only one station, as it is a single-user device.

5.8 Firmware Update Tab

The Firmware Update Tab is used to manage periodic device firmware upgrades and provides multiple avenues of installing files onto the access device.



Configure Firmware Update Settings

☑ Edit settings

Update method

● Search and update to latest firmware from vSpace server or from Management Server

○ Search and update from an FTP directory

○ Update from a specified firmware file on an FTP server

FTP URL
Username
Password
Confirm

Automatic update

□ Automatic update - download and install the latest firmware every time the device powers up

- **<u>Search and update to latest firmware from vSpace Server or from Management Server</u>**
  In this mode, the device will look to its vSpace Server and vSpace Management Center server (if available) for updated firmware if an update is initiated.

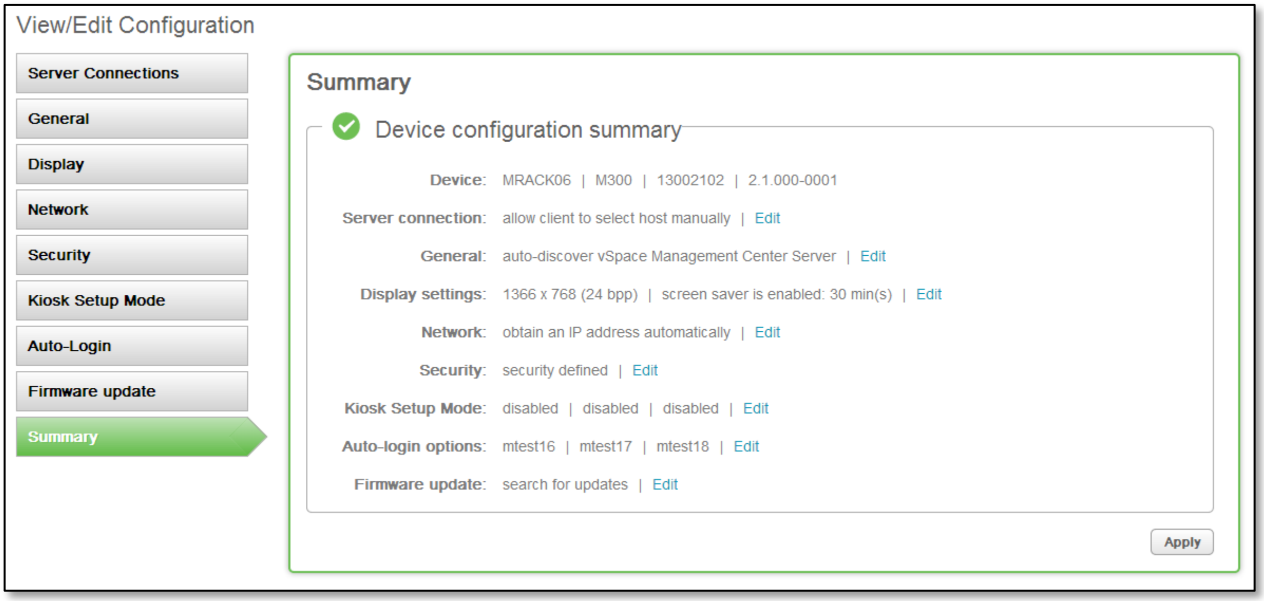
- **<u>Search and update from an FTP directory</u>**
  In this mode, the administrator can specify the URL, user name, and password of an FTP folder containing a firmware index file. The device will download and update it's firmware using the index.txt file to determine which firmware version it should use (favoring the most recent).

- **<u>Update from a specified firmware file on an FTP server</u>**
  In this mode, the administrator can specify the URL, user name, and password of an FTP folder containing a specific firmware file. The device will download and update using that specific file. This can be used to downgrade to a previous firmware version if desired.

- **<u>Automatic update</u>**
  Enabling this feature instructs the device to check its designated source (selected from the options above) each time it boots up. If new firmware is discovered, it will be downloaded and installed automatically.

5.9 Summary Tab

The Summary Tab contains a breakdown of each of the settings selected from the previous tabs and serves as a method of double-checking the full set of settings that are about to be pushed to an access device.



Summary

✓ Device configuration summary

Device:	MRACK06 | M300 | 13002102 | 2.1.000-0001
Server connection:	allow client to select host manually | Edit
General:	auto-discover vSpace Management Center Server | Edit
Display settings:	1366 x 768 (24 bpp) | screen saver is enabled: 30 min(s) | Edit
Network:	obtain an IP address automatically | Edit
Security:	security defined | Edit
Kiosk Setup Mode:	disabled | disabled | disabled | Edit
Auto-login options:	mtest16 | mtest17 | mtest18 | Edit
Firmware update:	search for updates | Edit

- **Edit**
  An Edit button is present to the right of each tab summary. This button can be used to quickly return to a given tab and alter its settings if desired.

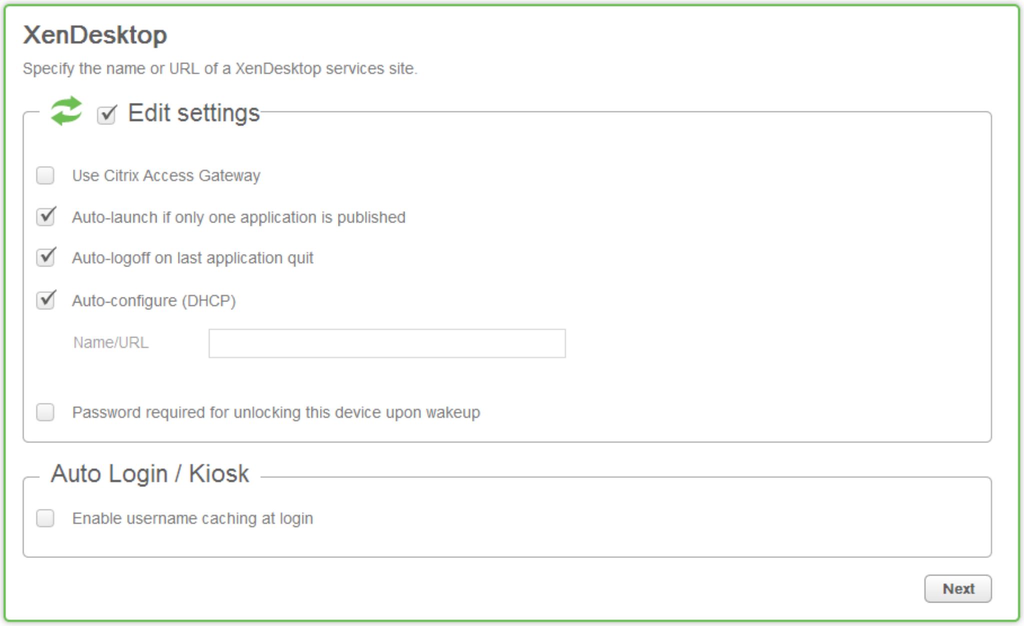
- **Apply**
  The Apply button can be used to finalize the configuration process, rebooting the device in the progress.

6.0 N-series Configuration

The N-series product line, including the N400, N500, and N500w, include features specific to Citrix environments, wireless networking, and advanced peripheral configuration options. The following sections detail each of the configuration tabs found within the View / Edit Configuration menu of an N-series access devices.

6.1 XenDesktop Tab

The XenDesktop Tab is used to configure settings related to the Citrix environment as well as login / logoff behavior.



XenDesktop

Specify the name or URL of a XenDesktop services site.

☑ Edit settings

□ Use Citrix Access Gateway

☑ Auto-launch if only one application is published

☑ Auto-logoff on last application quit

☑ Auto-configure (DHCP)

Name/URL

□ Password required for unlocking this device upon wakeup

Auto Login / Kiosk

□ Enable username caching at login

- **Use Citrix Access Gateway**
  Enabling this feature will allow your N-series device to access your Citrix environment securely from outside your network via the Citrix Access Gateway.

- **Auto-launch if only one application is published**
  If only one application is published to a given user account, that application will automatically be launched on login.

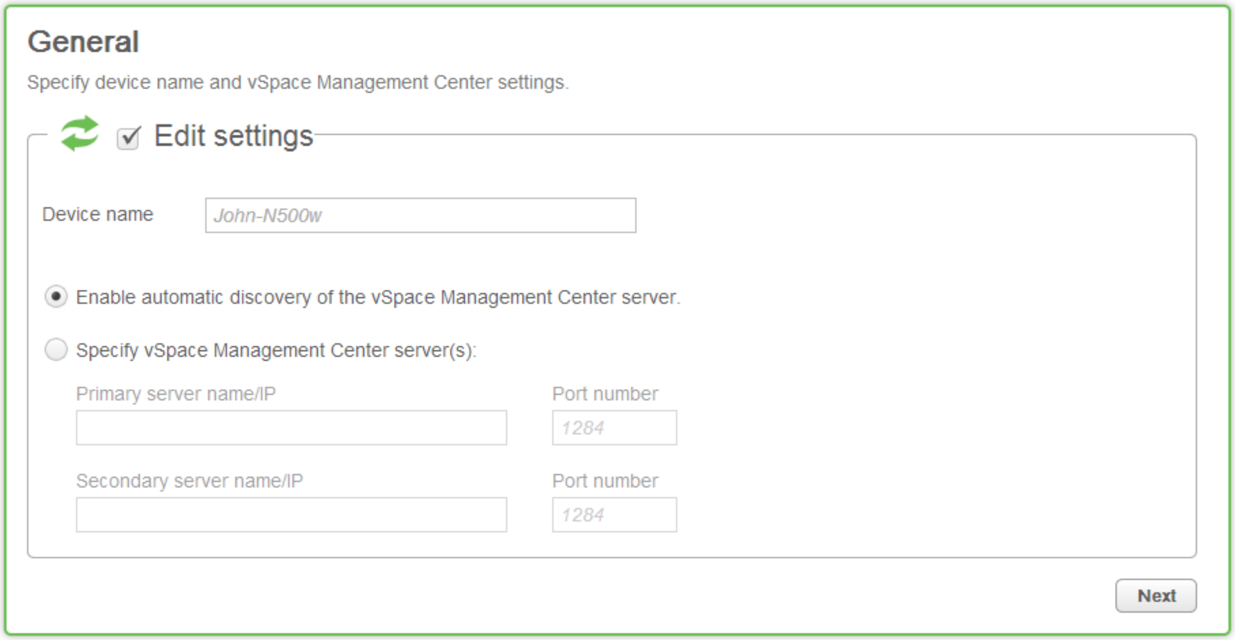
- **Auto-logoff on last application quit**
  When enabled, the device will automatically log out when the last active application is closed.

- **Auto-configure (DHCP)**
  When enabled, the device will use DHCP tags to locate it's XenDesktop Services Site. When disabled, the site can be manually entered.

- **Password required for unlocking this device upon wakeup**
  When enabled, the user will be required to enter a password when waking the device up from standby.

6.2 General Tab

The General Tab allows the administrator to edit general device settings such as Management Zone and device name.



General

Specify device name and vSpace Management Center settings.

☑ Edit settings

Device name: John-N500w

● Enable automatic discovery of the vSpace Management Center server.

○ Specify vSpace Management Center server(s):

Primary server name/IP — Port number: 1284

Secondary server name/IP — Port number: 1284

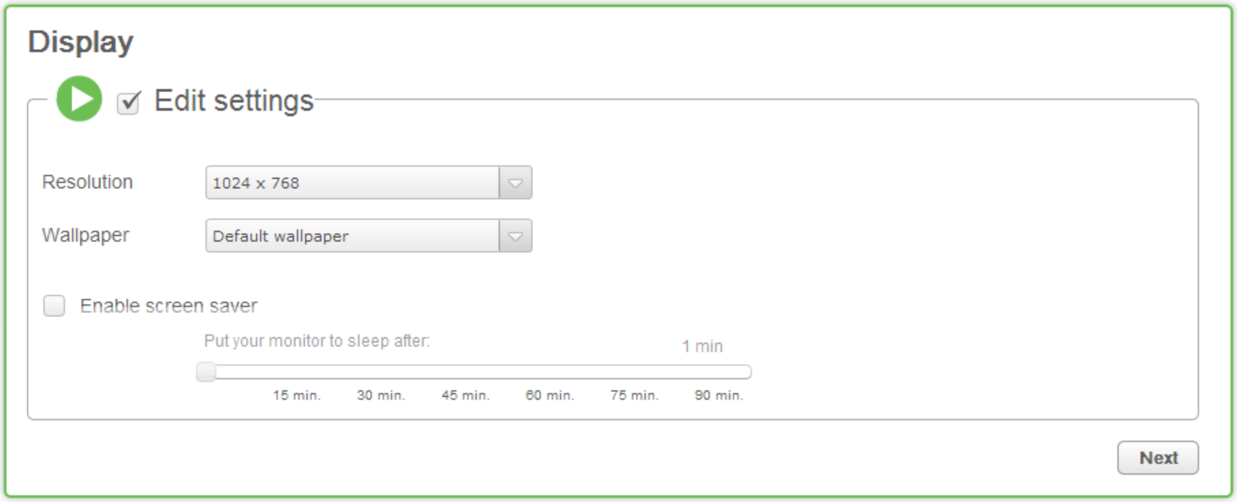
- **Device Name**
  Use this field to alter the L300 or M300 device name. This can be used to help sort devices based on use, location, or user, for example.

- **Enable automatic discovery of the vSpace Management Center server**
  Enabling this feature allows a device to automatically discover a vSpace Management Center server within its subnet or within the Management Zone governing it's vSpace Server.

- **Specify vSpace Management Center server(s)**
  Selecting this option allows administrators to specify which vSpace Management Center server the device should associate with (and by extension, which Management Zone). A primary and secondary server may be specified for failover purposes.

6.3 Display Tab

The Display Tab contains configuration options related to screen resolution and behavior.



Display

☑ Edit settings

Resolution: 1024 x 768

Wallpaper: Default wallpaper

□ Enable screen saver

Put your monitor to sleep after: 1 min

- **Resolution**

  This dropdown menu contains all monitor resolutions compatible with the device in question.

- **Wallpaper**

  Allows the administrator to select a desktop background image for use within the N-series GUI.

- **Enable screen saver**

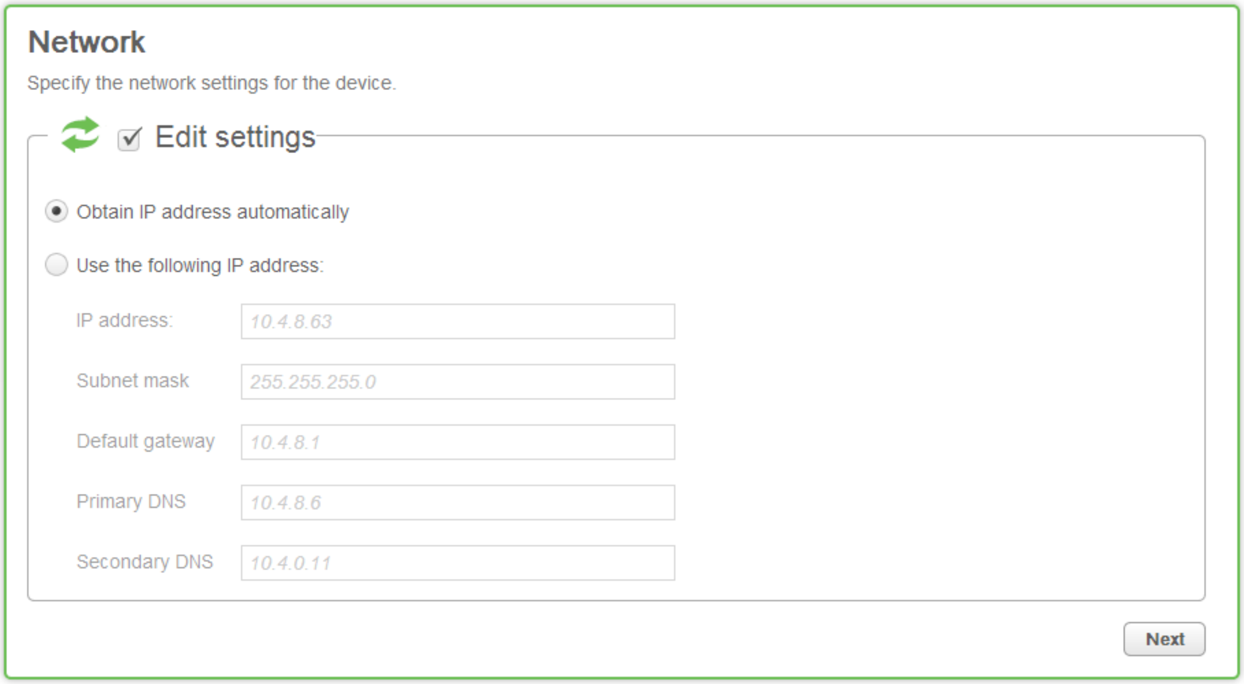
  Check to enable the device screen saver, which will turn off the display signal and allow the connected monitor to enter its power save mode once idle for a specified period of time.

- **Sleep time**

  This slider allows the administrator to select the amount of idle time a device will wait before entering screen saver mode.

6.4 Network Tab

The network tab contains a full set of common network settings to be used by the selected device.



Network

Specify the network settings for the device.

☑ Edit settings

● Obtain IP address automatically

○ Use the following IP address:

IP address: 10.4.8.63

Subnet mask 255.255.255.0

Default gateway 10.4.8.1

Primary DNS 10.4.8.6

Secondary DNS 10.4.0.11

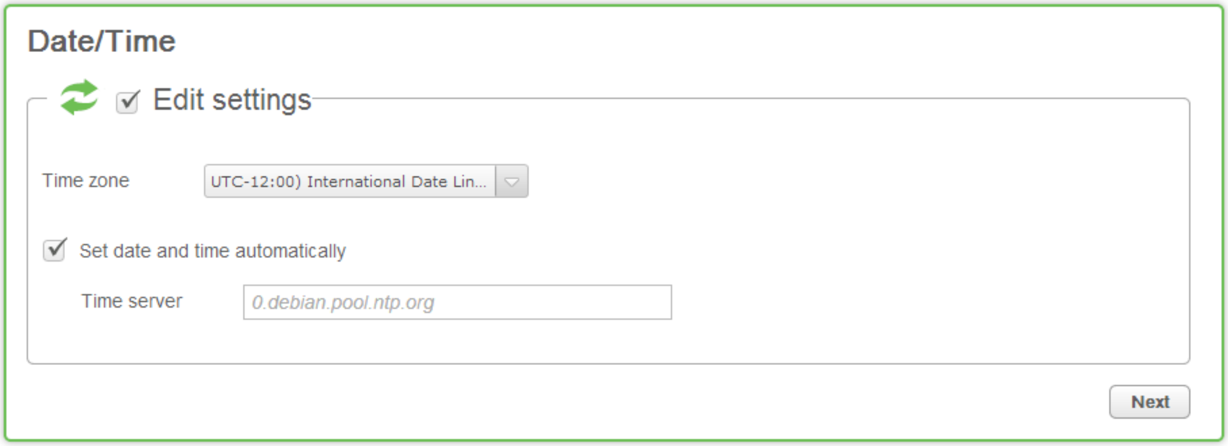
- **<u>Obtain IP address automatically</u>**
  Selecting this option places the device into DHCP mode, causing it to automatically obtain its network settings from the local DHCP server.

- **<u>Use the following IP address</u>**
  Selecting this option allows the administrator to specify their device's network settings.

- **<u>IP address, Subnet mask, Default gateway, Primary DNS, Secondary DNS</u>**
  Standard network settings, including a secondary DNS field for failover purposes.

6.5 Date / Time Tab

The Date / Time Tab allows the administrator to control clock settings within the N-series device.



Date/Time

☑ Edit settings

Time zone: UTC-12:00) International Date Lin...

☑ Set date and time automatically

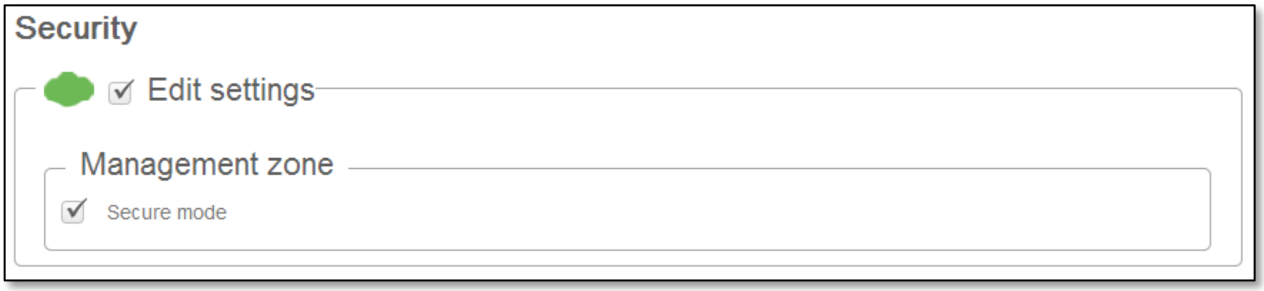
Time server: 0.debian.pool.ntp.org

- **Time Zone**
  This dropdown is used to select the time zone that the device will use.

- **Set date and time automatically**
  Enabling this feature allows the N-series device to independently poll and verify the current time using the time server of your choice. The Time Server field can be used to specify which time server or service the device should use.

6.6 Security Tab

The Security Tab contains several options that help to secure the N-series device, its session, and its connection to the Management Zone.



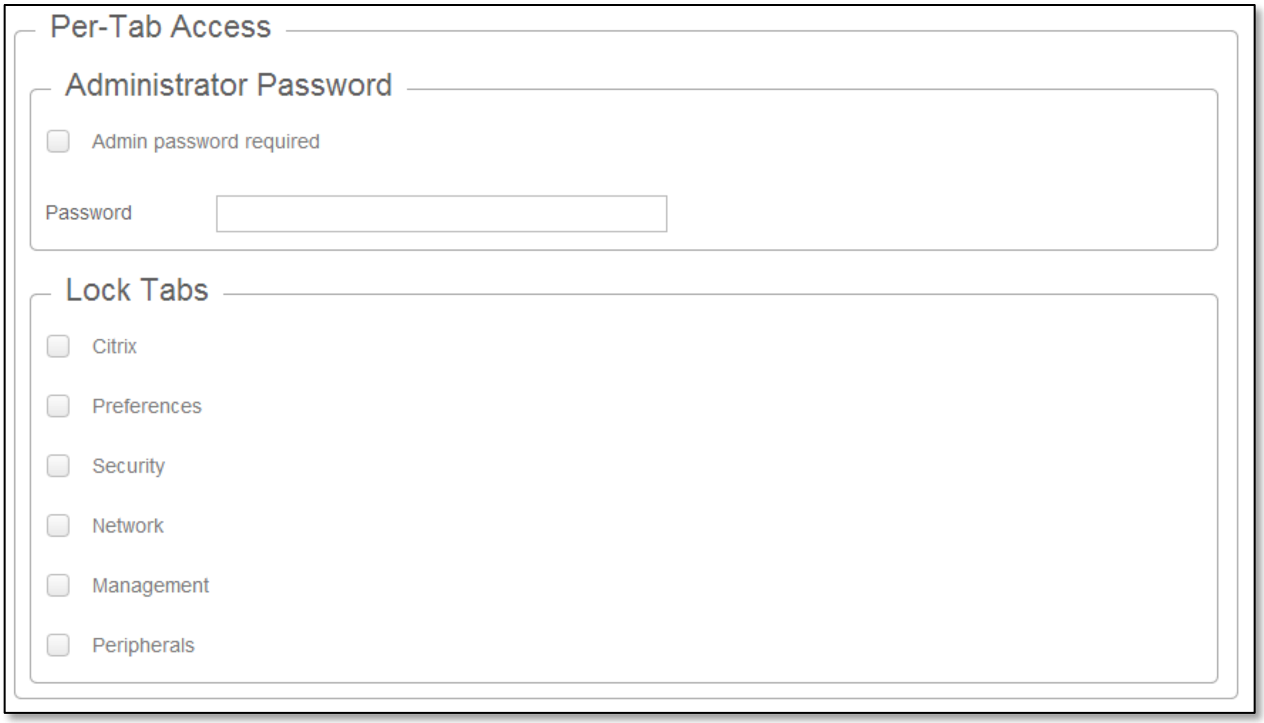
Security

☑ Edit settings

Management zone

☑ Secure mode

- **Management zone (Secure mode)**
  Enabling secure mode for a device prevents it from automatically joining a new Management Zone in the event that it loses connection with its current Zone. Disabling this feature allows the device to automatically connect to another Zone (if one is available).



Per-Tab Access

Administrator Password

□ Admin password required

Password

Lock Tabs

□ Citrix

□ Preferences

□ Security

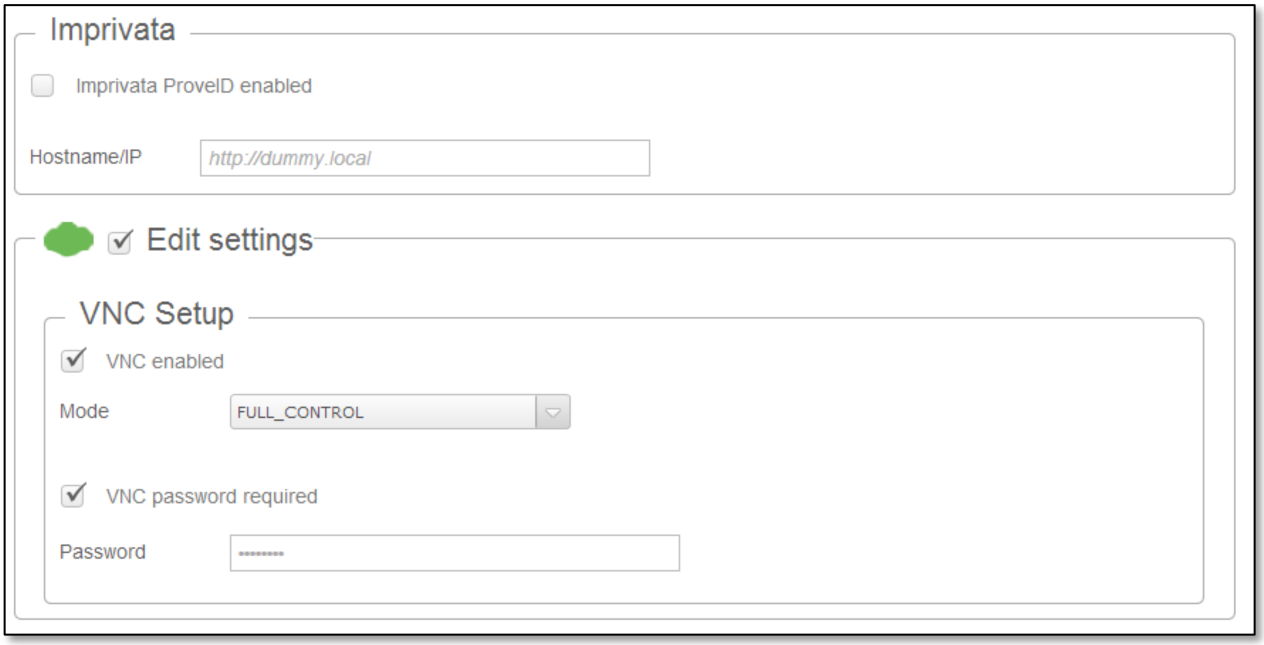
□ Network

□ Management

□ Peripherals

- **Admin password required**
  Enabling this feature causes the device to prompt for a password (specified within the Password field) whenever a user attempts to access the configure menu of an N-series device.

- **Lock Tabs**
  This menu allows the administrator to select which tabs are "locked". Leaving certain tabs unlocked can provide users with varying levels of control over their device and environment.



Imprivata

□ Imprivata ProveID enabled

Hostname/IP: http://dummy.local

☑ Edit settings

VNC Setup

☑ VNC enabled

Mode: FULL_CONTROL

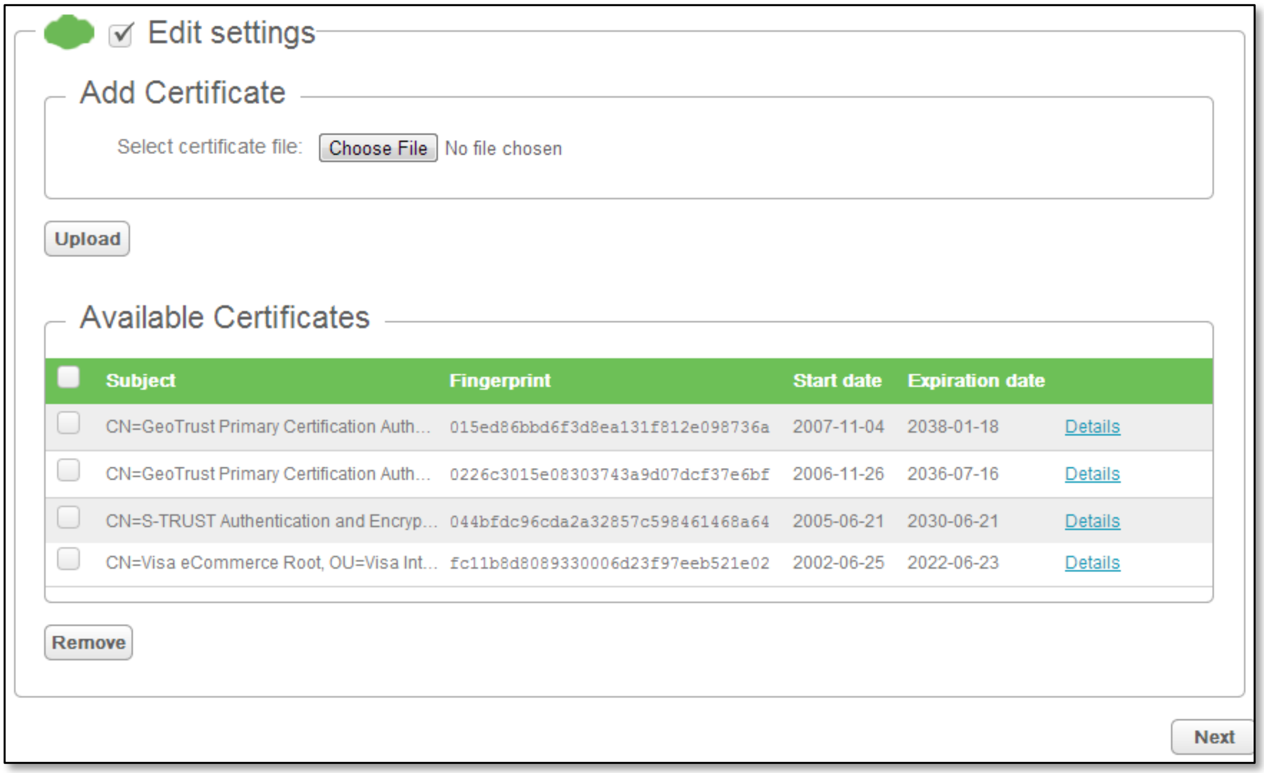
☑ VNC password required

Password: ••••••••

- <u>**Imprivata ProveID enabled**</u>
  Enabling this feature allows the N-series device to make use of Imprivata’s OneSign, RFID card access technology. The Hostname/IP field stores the Imprivata Bootstrap Server. For more information on this feature, visit the following Knowledge Base article:
  http://www.ncomputing.com/kb/HOW-TO-Imprivata-OneSign-Integration_409.html

- <u>**VNC enabled**</u>
  Enabling this feature allows VNC clients to connect to, view, and control the N-series device remotely. The Mode dropdown defines the extent of this control.

- <u>**VNC password required**</u>
  Enabling this feature forces the connecting VNC client to enter a password, specified within the Password field.



Add Certificate

Select certificate file: Choose File No file chosen

Available Certificates

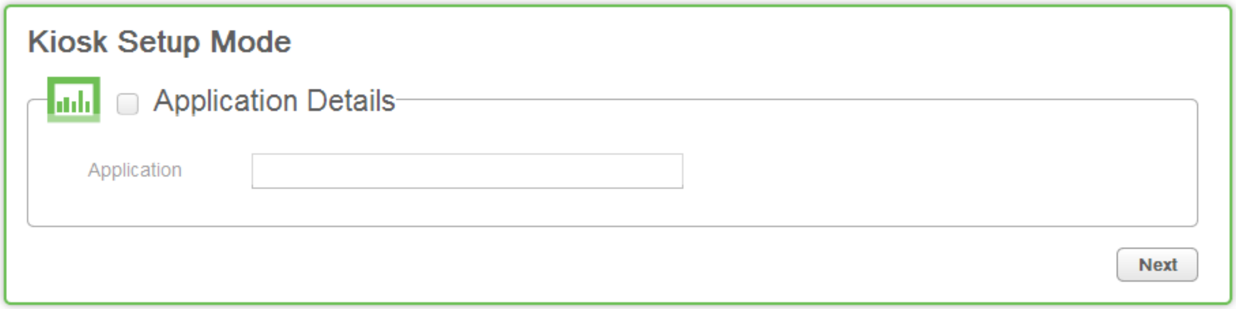
□	Subject	Fingerprint	Start date	Expiration date	
□	CN=GeoTrust Primary Certification Auth...	015ed86bbd6f3d8ea131f812e098736a	2007-11-04	2038-01-18	Details
□	CN=GeoTrust Primary Certification Auth...	0226c3015e08303743a9d07dcf37e6bf	2006-11-26	2036-07-16	Details
□	CN=S-TRUST Authentication and Encryp...	044bfdc96cda2a32857c598461468a64	2005-06-21	2030-06-21	Details
□	CN=Visa eCommerce Root, OU=Visa Int...	fc11b8d8089330006d23f97eeb521e02	2002-06-25	2022-06-23	Details

- **Add Certificate**
  The **Choose File** button within this section allows administrators to manually add security certificates to an N-series device. Once the certificate is located and selected, use the **Upload** button to add it to the device's currently available certificates.

- **Available Certificates**
  This field lists all currently installed security certificates. Certificates can be viewed in detail using the **Details** button to the right of the field, or removed entirely using the **Remove** button at the bottom of the field.

6.7 Kiosk Setup Mode Tab

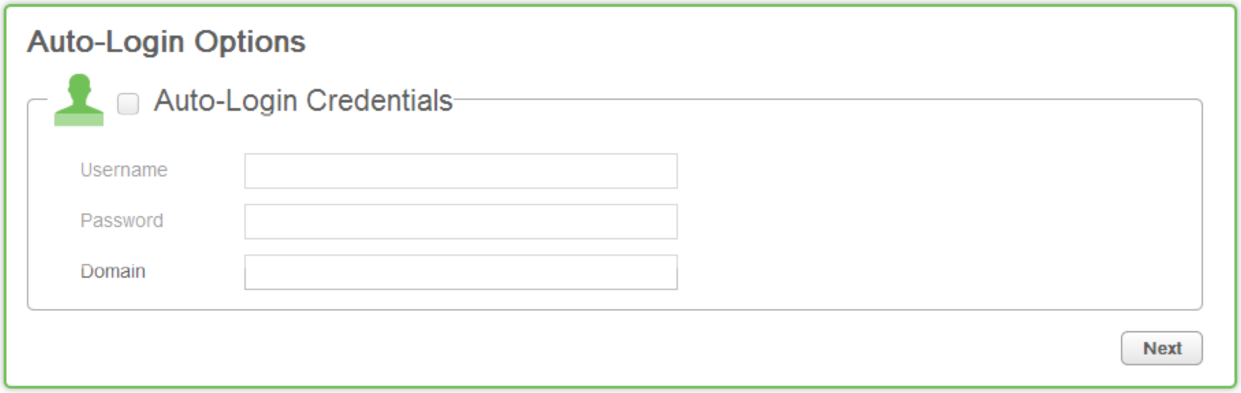
The Kiosk Setup Mode Tab allows administrators to specify an application that they would like to launch in place of the default desktop environment.



- **Application Details**
  Enabling this feature and entering the name of the application (as published within XenApp) causes the specified application to launch automatically on login.

6.8 Auto Login Tab

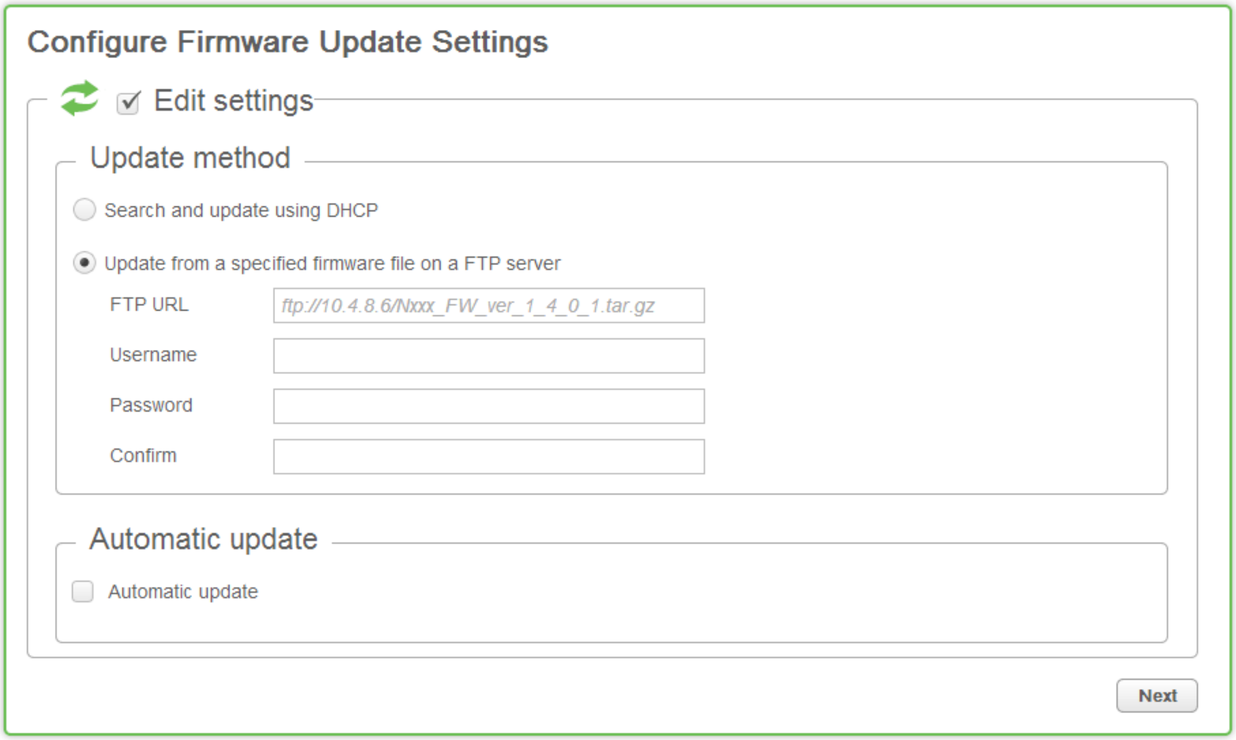
The Auto Login Options Tab allows the administrator to configure auto login functionality.



- **Auto-Login Credentials**
  Enabling this feature and entering the required user credentials and domain information will cause the N-series to automatically log in using the specified information on connection with a Citrix server.

6.9 Firmware Update Tab

The Firmware Update Tab is used to manage periodic device firmware upgrades and provides multiple avenues of installing files onto the access device.



Configure Firmware Update Settings

☑ Edit settings

Update method

○ Search and update using DHCP

● Update from a specified firmware file on a FTP server

FTP URL: ftp://10.4.8.6/Nxxx_FW_ver_1_4_0_1.tar.gz

Username:

Password:

Confirm:

Automatic update

□ Automatic update

- **Search and update using DHCP**
  Instructs the N-series device to check for updated firmware using DHCP tags. For more information on using DHCP tags to automatically configure N-series devices, consult the N-series product user manual.

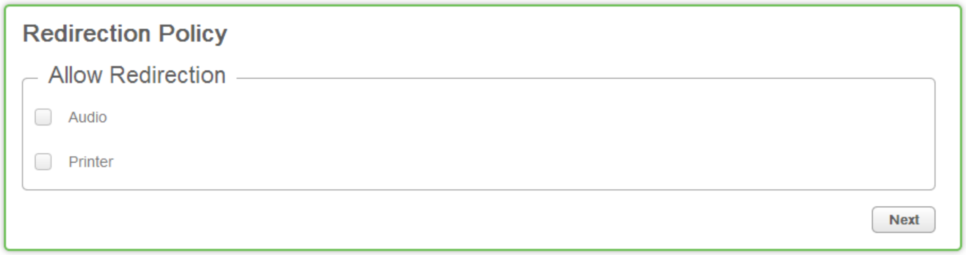
- **Update from a specified firmware file on an FTP server**
  In this mode, the administrator can specify the URL, user name, and password of an FTP folder containing a specific firmware file. The device will download and update using that specific file. This can be used to downgrade to a previous firmware version if desired.

  Note that if a directory is specified instead of a specific firmware file, the N-series will check for a Catalog.txt file and update based on the archive of firmware files located within that directory. This functionality is part of the automatic, sequential update process. Consult the following Knowledge Base article for more information on sequential updates:
  http://www.ncomputing.com/kb/HOW-TO-Sequential-N-series-Firmware-Updates_408.html

- **Automatic update**
  Enabling this feature instructs the device to check its designated source (selected from the options above) each time it boots up. If new firmware is discovered, it will be downloaded and installed automatically.

6.10 Redirection Policy

The Redirection Policy Tab provides administrators the ability to alter how USB audio and printer redirection is handled by the N-series device.



Redirection Policy

Allow Redirection

□ Audio

□ Printer

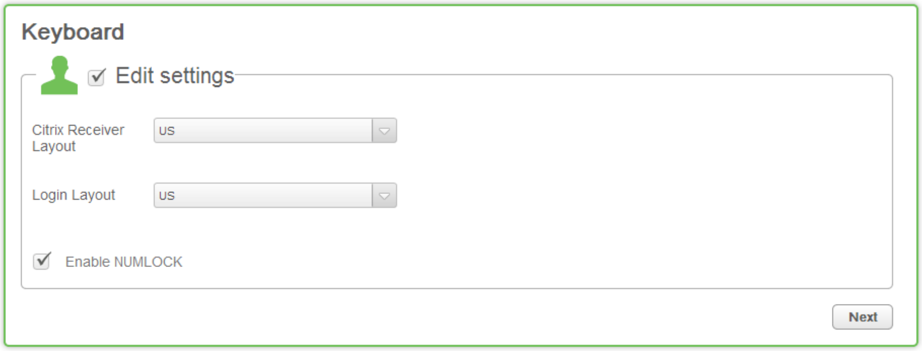
- **Audio**
  A number of specific deployment types, such as those including call centers that rely on USB headsets to deliver microphone input to certain applications, will benefit from enabling Audio redirection. Note that while this alternate method of USB redirection is enabled, users may experience reduced audio playback quality when playing video or browsing multi-media intensive websites.

- **Printer**
  Enabling printer redirection can resolve issues with certain printer specific OEM applications within XenDesktop.

Due to the deployment-specific design of these features, it is recommended that these options be enabled in a test environment prior to deployment into a live environment to ensure that the resulting functionality conforms to the requirements of the deployment.

6.11 Keyboard Tab

The Keyboard Tab allows administrators to configure the regional settings of the N-series' keyboard.



Keyboard

☑ Edit settings

Citrix Receiver Layout: us

Login Layout: us

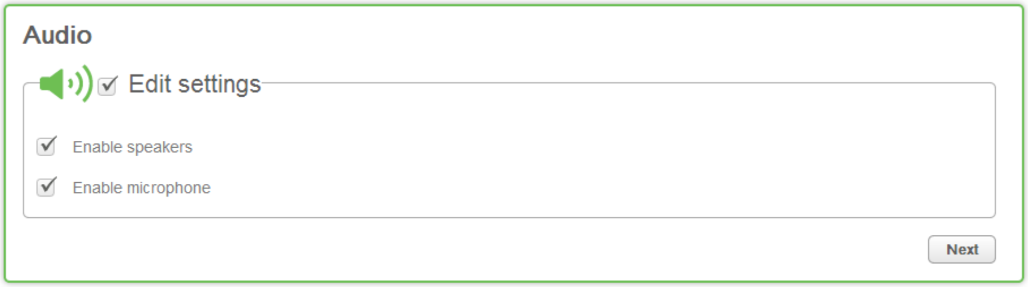
☑ Enable NUMLOCK

- **Citrix Receiver / Login Layout**
  Using the drop down menus, administrators can specify the keyboard localization used for the N-series GUI and the Citrix Receiver environment independently.

- **Enable NUMLOCK**
  Enabling this feature causes the NUMLOCK key to be ON by default when the device is turned on.

6.12 Audio Tab

The Audio Tab allows administrators to enable or disable audio features.



Audio

☑ Edit settings

☑ Enable speakers

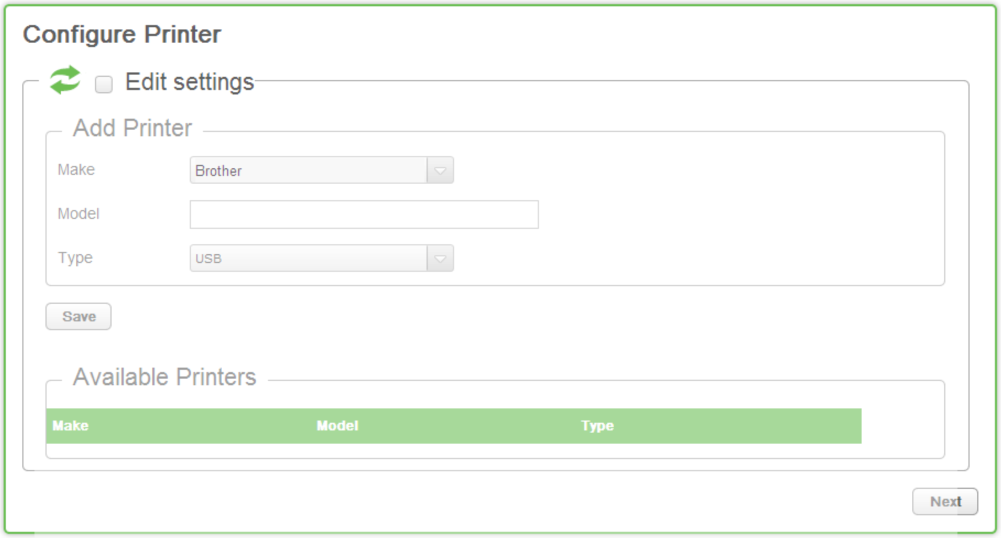
☑ Enable microphone

- <u>**Enable speakers**</u>
  Controls speaker (audio output) functionality.

- <u>**Enable microphone**</u>
  Controls microphone (audio input) functionality.

6.13 Printers Tab

The Printers Tab allows the administrator to associate printers with an N-series device.



Configure Printer

□ Edit settings

Add Printer

Make: Brother

Model:

Type: USB

Available Printers

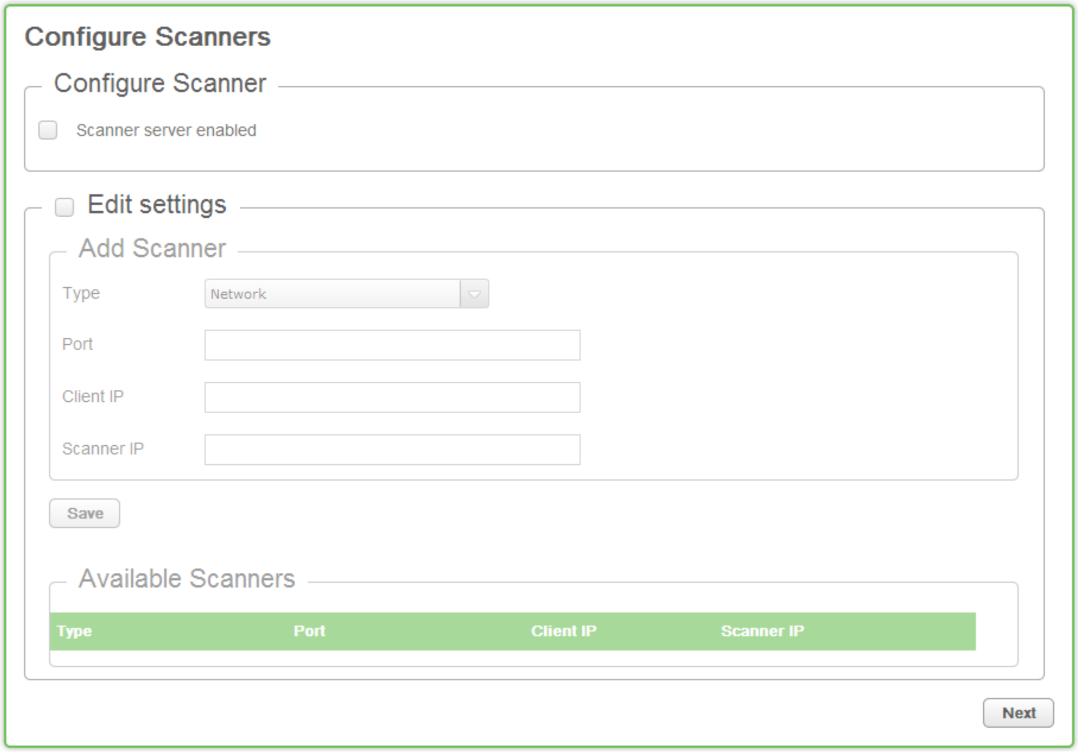
Make	Model	Type

- <u>**Add Printer**</u>
  Using the drop down menus to select printer Type and Make, and the model field to enter the exact model name of the printer (as listed in the device driver name), printers can be added to a device.

- <u>**Available Printers**</u>
  Multiple printers can be associated with a given device, and all associated printers are listed in this field.

6.14 Scanners Tab

The Scanners Tab allows for the association of SANE standard compatible scanners with N-series devices.



Configure Scanners

Configure Scanner

□ Scanner server enabled

□ Edit settings

Add Scanner

Type: Network

Port:

Client IP:

Scanner IP:

Available Scanners

Type	Port	Client IP	Scanner IP

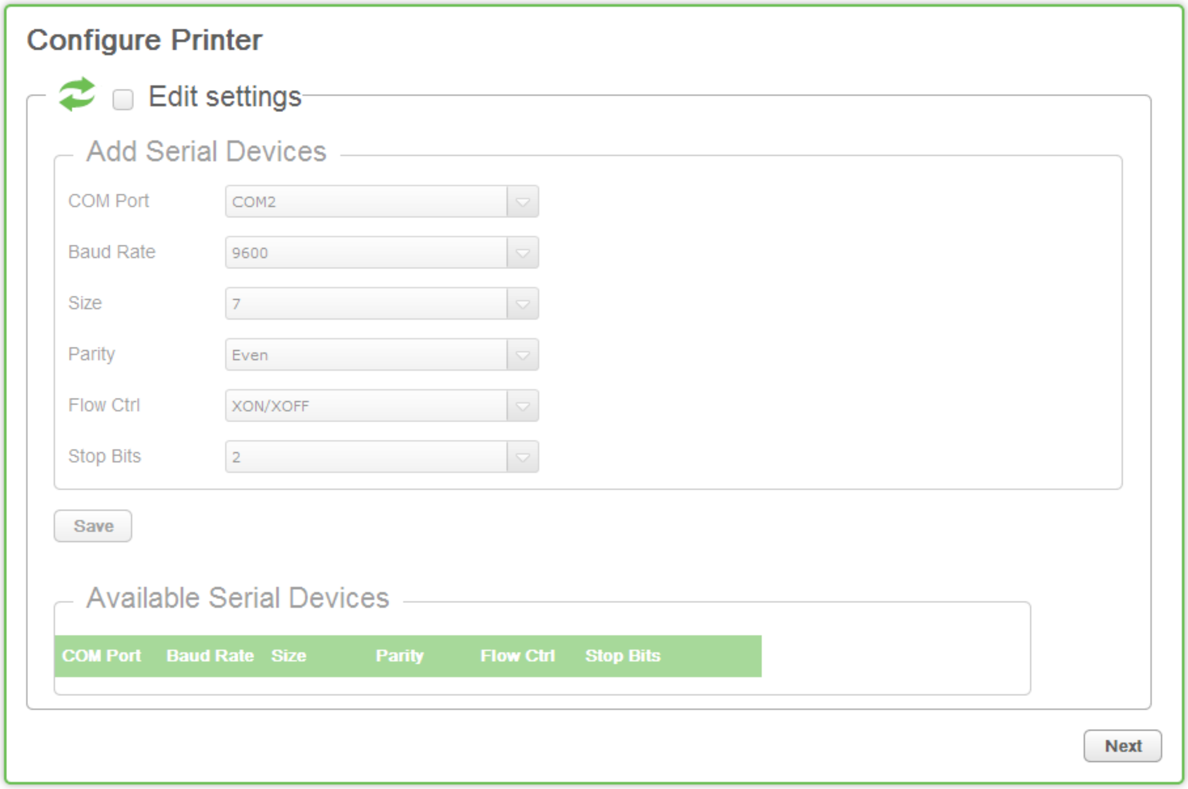
- **Configure Scanner**
  Enabling Scanner server allows the N-series device to access network and USB based scanners.

- **Add Scanner**
  Using the Type dropdown, Port, Client IP, and Scanner IP fields (if applicable) allow the administrator to specify USB and network printers for association with the N-series device.

- **Available Scanners**
  Multiple scanners can be associated with a given device, and all associated scanners are listed in this field.

6.15 Serial Devices Tab

As of firmware 1.4.X, N-series devices support the use of serial devices over USB. This is one of two menus that allow administrators to configure N-series devices for use with serial peripherals.



Configure Printer

□ Edit settings

Add Serial Devices

COM Port	COM2
Baud Rate	9600
Size	7
Parity	Even
Flow Ctrl	XON/XOFF
Stop Bits	2

Available Serial Devices

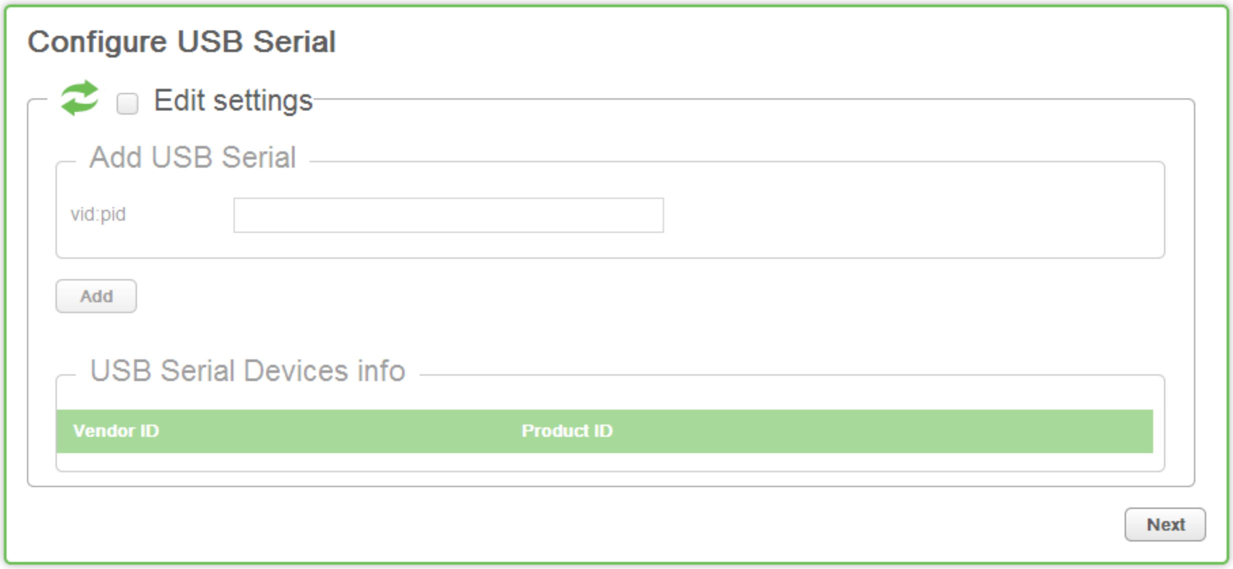
COM Port	Baud Rate	Size	Parity	Flow Ctrl	Stop Bits

- **Add Serial Devices**
  The COM Port, Baud Rate, Size, Parity, Flow Ctrl, and Stop Bits drop down menus are used to configure a given serial device for use with an N-series access device. Consult the peripheral user manual for guidance on the values that should be used. Use the **Save** button to finalize addition of a serial device once the desired values have been set.

- **Available Serial Devices**
  Multiple serial devices can be associated with a given device, and all associated devices are listed in this field.

6.16 USB Serial Tab

The USB Serial Tab is the second of two tabs that allow serial devices to be configured for use with N-series access devices.



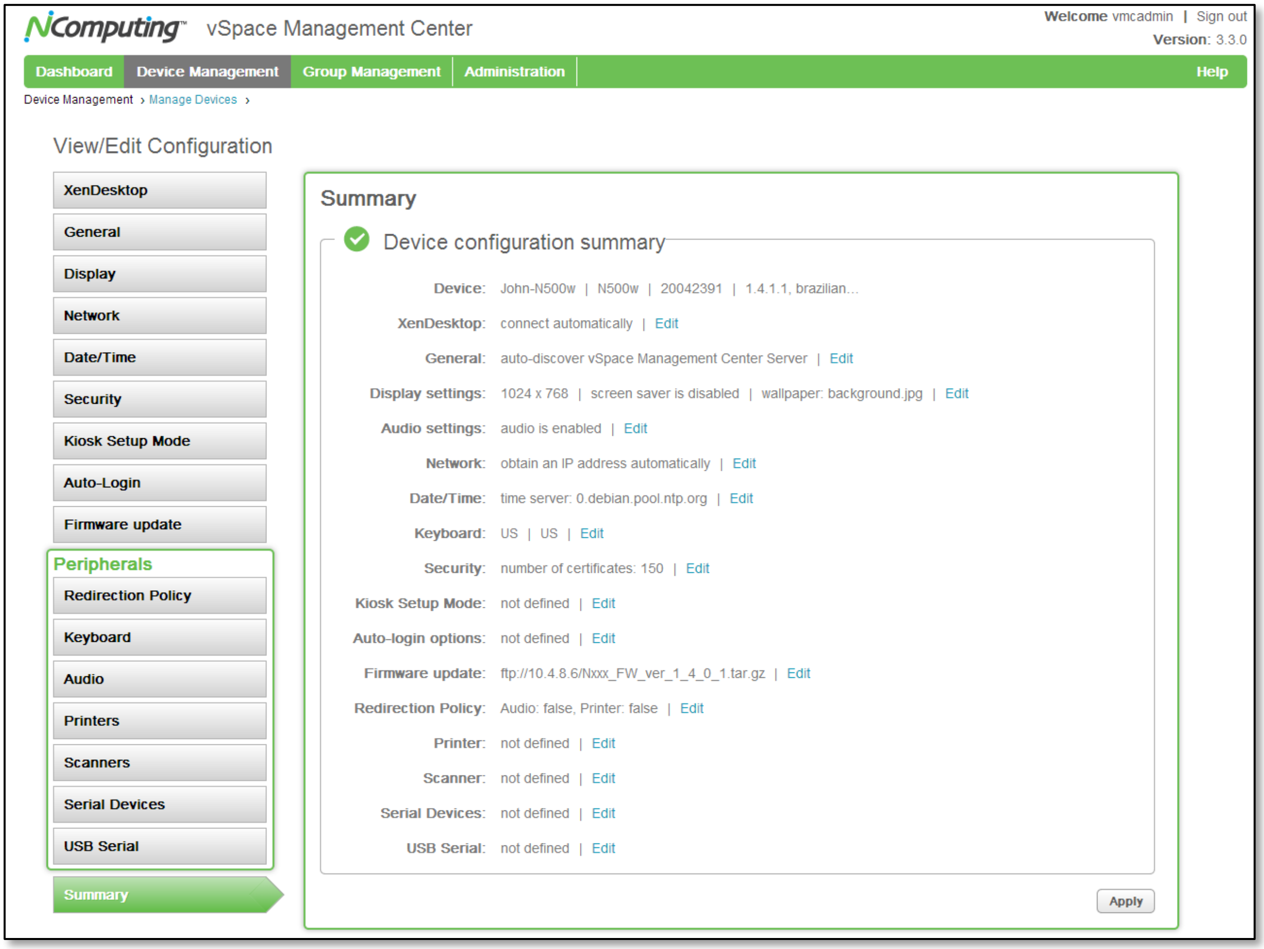
Vendor ID	Product ID

- **<u>Add USB Serial</u>**
  The vid:pid field can be used to add serial devices over USB by specifying the Vendor and Product ID of the device. Consult the peripheral's user manual for guidance on the values that should be used in this field.

- **<u>USB Serial Devices Info</u>**
  Multiple serial devices can be associated with a given device, and all associated devices are listed in this field.

6.17 Summary Tab

The Summary Tab contains a breakdown of each of the settings selected from the previous tabs and serves as a method of double-checking the full set of settings that are about to be pushed to an access device.



Summary

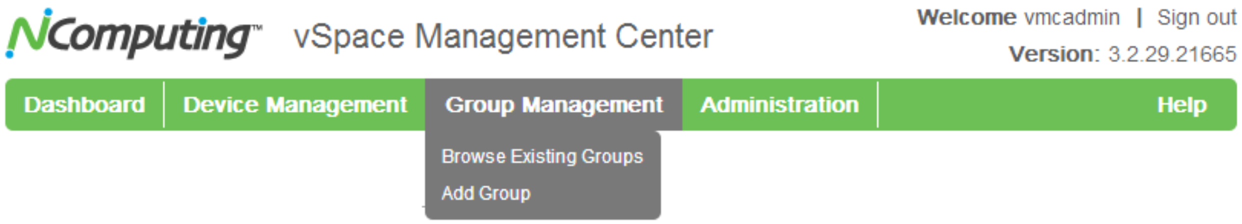
Device configuration summary

Device:	John-N500w | N500w | 20042391 | 1.4.1.1, brazilian...
XenDesktop:	connect automatically | Edit
General:	auto-discover vSpace Management Center Server | Edit
Display settings:	1024 x 768 | screen saver is disabled | wallpaper: background.jpg | Edit
Audio settings:	audio is enabled | Edit
Network:	obtain an IP address automatically | Edit
Date/Time:	time server: 0.debian.pool.ntp.org | Edit
Keyboard:	US | US | Edit
Security:	number of certificates: 150 | Edit
Kiosk Setup Mode:	not defined | Edit
Auto-login options:	not defined | Edit
Firmware update:	ftp://10.4.8.6/Nxxx_FW_ver_1_4_0_1.tar.gz | Edit
Redirection Policy:	Audio: false, Printer: false | Edit
Printer:	not defined | Edit
Scanner:	not defined | Edit
Serial Devices:	not defined | Edit
USB Serial:	not defined | Edit

- **Edit**
  An Edit button is present to the right of each tab summary. This button can be used to quickly return to a given tab and alter its settings if desired.

- **Apply**
  The Apply button can be used to finalize the configuration process, rebooting the device in the progress.

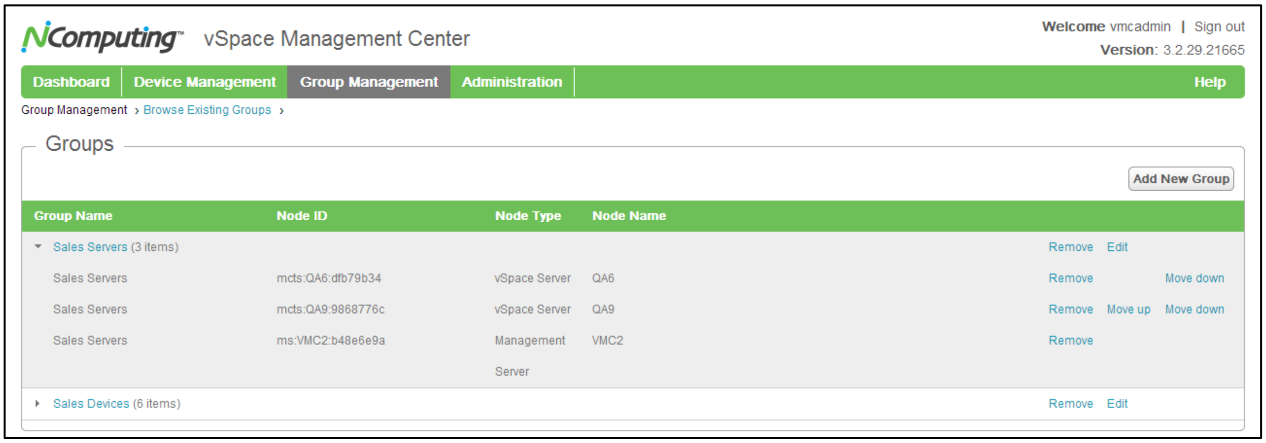
7.0 Group Management



The Group Management module of vSpace Management Center allows administrators to create and maintain Device and Server Groups. This allows administrators to create logical groupings that correspond to device models, geographical locations, or usage needs.

7.1 Browse Existing Groups

You can view all currently existing Groups by selecting “Brows Existing Groups” from the Group Management menu.


NComputing vSpace Management Center
Welcome vmcadmin | Sign out
Version: 3.2.29.21665
Dashboard
Device Management
Group Management
Administration
Help
Group Management › Browse Existing Groups ›
Groups
Add New Group

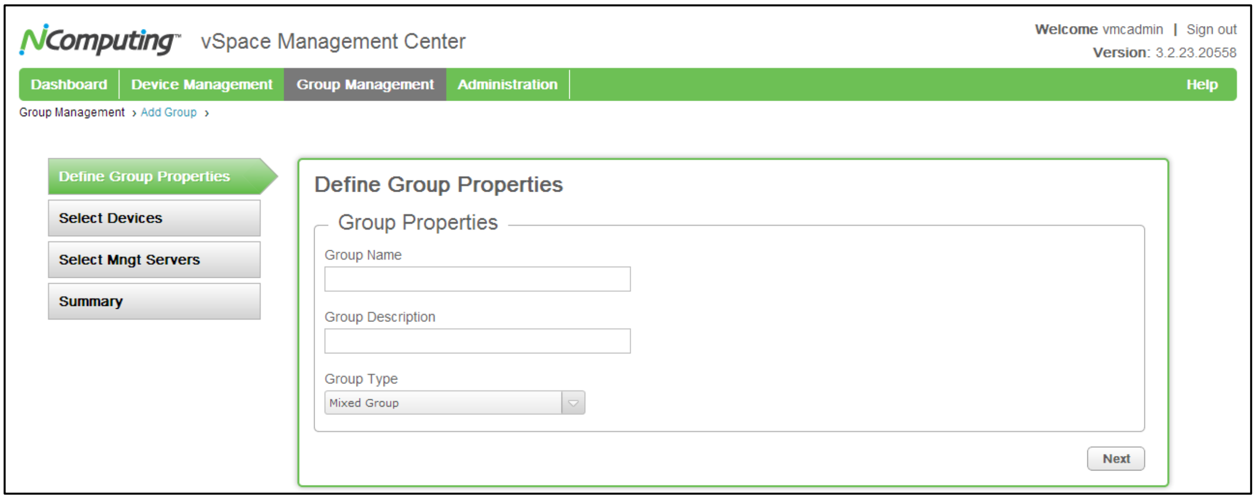
Group Name	Node ID	Node Type	Node Name	
▾ Sales Servers (3 items)				Remove Edit
Sales Servers	mcts:QA6:dfb79b34	vSpace Server	QA6	Remove Move down
Sales Servers	mcts:QA9:9868776c	vSpace Server	QA9	Remove Move up Move down
Sales Servers	ms:VMC2:b48e6e9a	Management Server	VMC2	Remove
▸ Sales Devices (6 items)				Remove Edit

Each group can be expanded to display a list of the individual devices and management servers contained within that group. You can remove individual members of the group by clicking “Remove” to the right of the list. You can also remove or edit the entire group by clicking the “Remove” or “Edit” button to the right of the group name.

To create a new group, click the “Add New Group” button at the top right of the screen.

7.2 Add / Edit Group

To create a new Group, select “Add / Edit Group” from the Group Management menu.



Define Group Properties

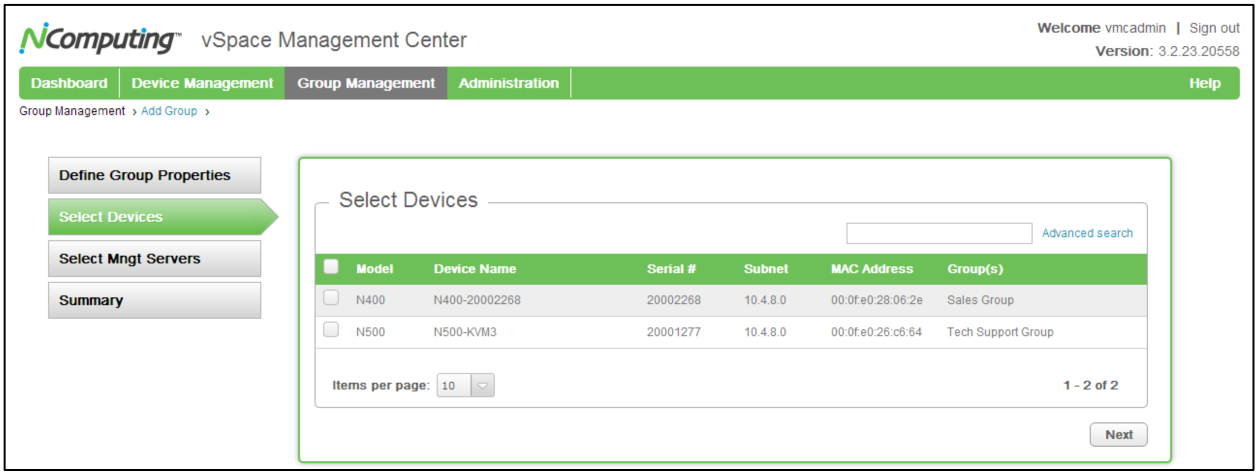
Group Properties

Group Name

Group Description

Group Type: Mixed Group

Begin by defining the group you wish to create by selecting a Group Name and Description. Lastly, select whether the group will contain devices, management servers, or a combination of both (a Mixed Group). Once you click “Next”, you’ll be taken to a list of currently available Devices that you can select for inclusion in your new Group.



Select Devices

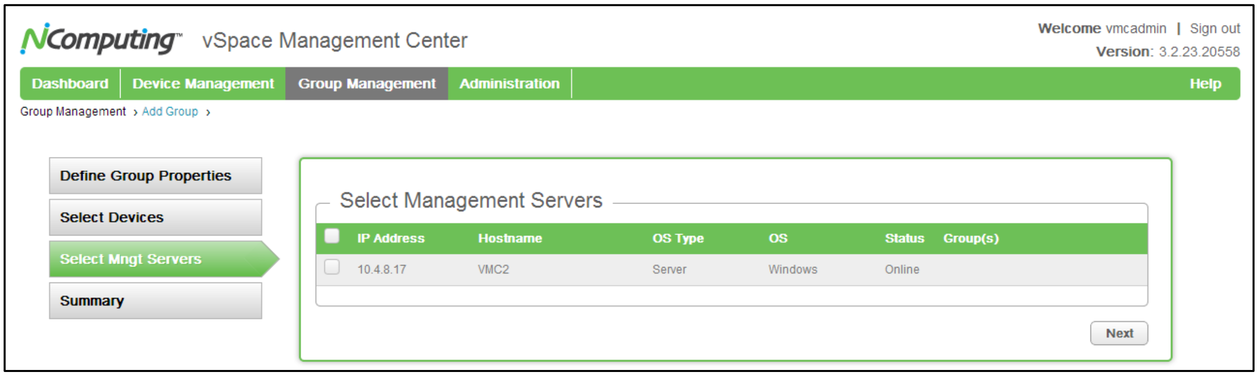
□	Model	Device Name	Serial #	Subnet	MAC Address	Group(s)
□	N400	N400-20002268	20002268	10.4.8.0	00:0f:e0:28:06:2e	Sales Group
□	N500	N500-KVM3	20001277	10.4.8.0	00:0f:e0:26:c6:64	Tech Support Group

Items per page: 10 — 1 - 2 of 2

Next, click the checkbox next to the device(s) you wish to include in your group. Click the “Add Devices” button to the bottom left of the screen to add these to your group. You can view the currently selected Devices by clicking the “Selected Devices” tab at the top of the screen, and return to the “All Virtual Devices” tab to add additional devices if desired.

> **NOTE:** You can search for Devices with specific characteristics by using the Advanced Search function at the top right of the screen.

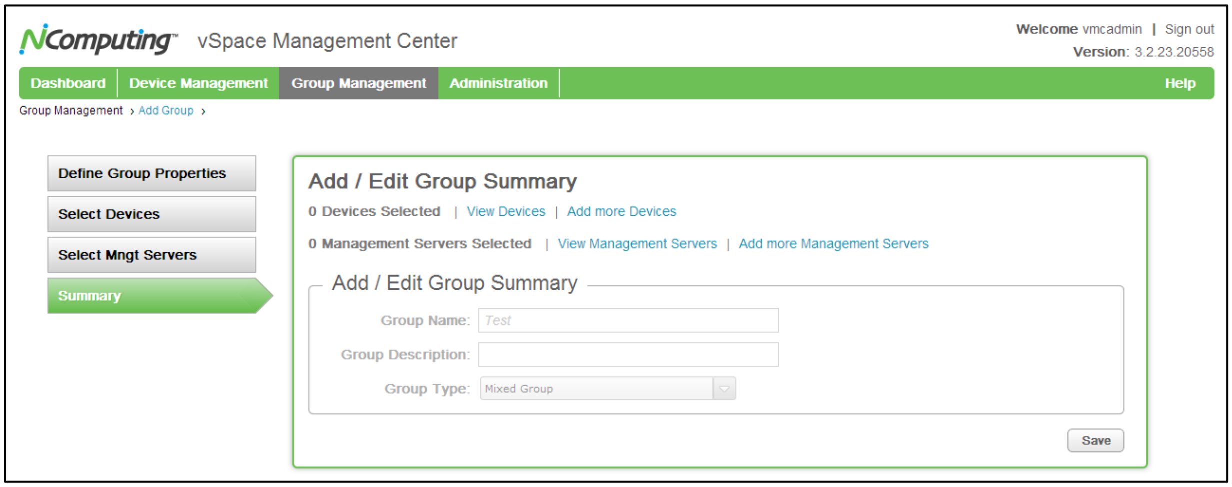
Once you are done selecting devices, click the “Next” button.



Select Management Servers

☐	IP Address	Hostname	OS Type	OS	Status	Group(s)
☐	10.4.8.17	VMC2	Server	Windows	Online	

If you wish to include Management Servers in your Group, you may do so at this stage. Click the check box next to the Server(s) you wish to add and click "Add Management Servers". Click "Next" when you are satisfied with your selections.



Add / Edit Group Summary

0 Devices Selected | View Devices | Add more Devices

0 Management Servers Selected | View Management Servers | Add more Management Servers

Add / Edit Group Summary

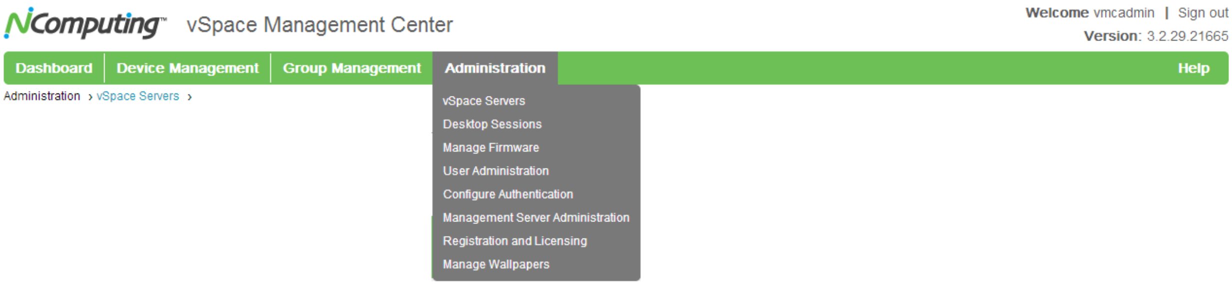
Group Name: Test

Group Description:

Group Type: Mixed Group

Once you have finished selecting Devices and/or Servers for your Group, you will be presented with a summary of the Group. Note that even at this stage in the group creation process, you are still free to go back and add or remove devices and servers as needed. To complete the group creation process, click the "Next" button to the bottom right of the screen.

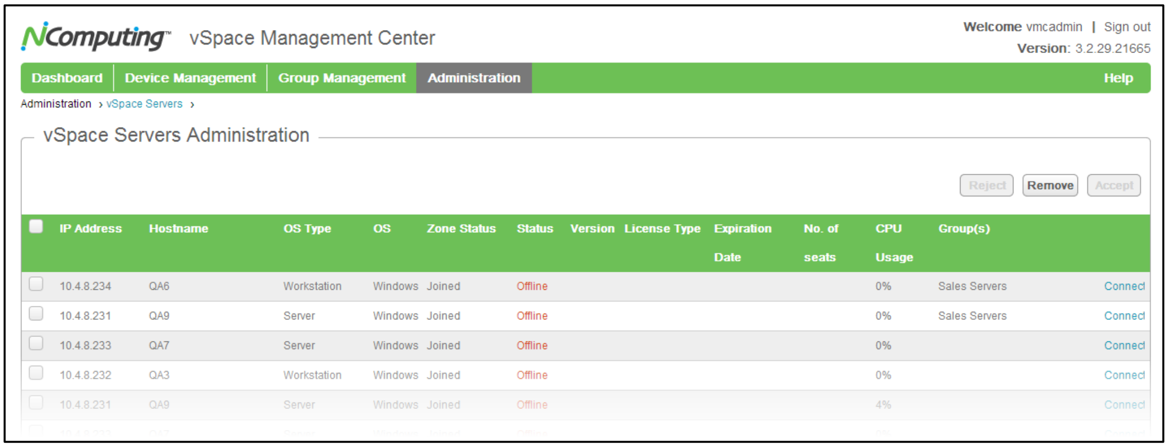
8.0 Settings



The Administration module allows you to configure the vSpace Management Center server itself, configure Authentication Settings, upload firmware and wallpapers to be distributed to devices, as well as other server specific tasks such as registration.

8.1 vSpace Servers

The vSpace Servers section allows you to view each of the vSpace servers within the Management Zone and connect to them for administrative purposes.



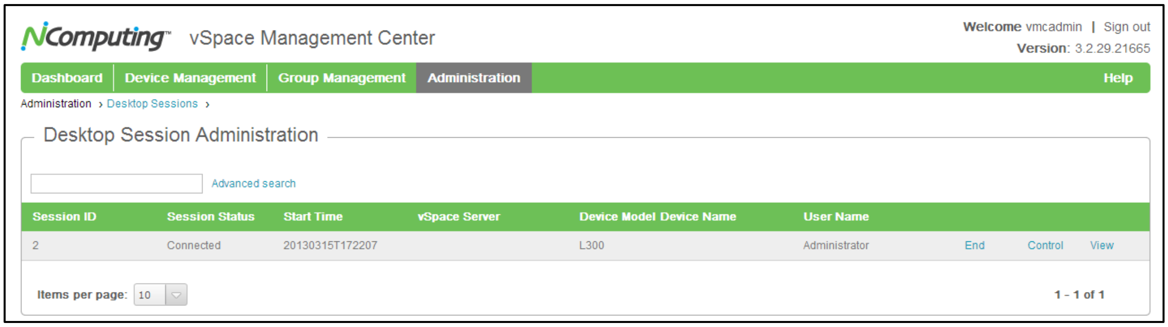
vSpace Servers Administration

☐	IP Address	Hostname	OS Type	OS	Zone Status	Status	Version	License Type	Expiration Date	No. of seats	CPU Usage	Group(s)	
☐	10.4.8.234	QA6	Workstation	Windows	Joined	Offline					0%	Sales Servers	Connect
☐	10.4.8.231	QA9	Server	Windows	Joined	Offline					0%	Sales Servers	Connect
☐	10.4.8.233	QA7	Server	Windows	Joined	Offline					0%		Connect
☐	10.4.8.232	QA3	Workstation	Windows	Joined	Offline					0%		Connect
☐	10.4.8.231	QA9	Server	Windows	Joined	Offline					4%		Connect

Along the top of the server list are key details of each listed server including Host Name, OS Type, and Zone Status. To the right of each row is a Connect button that will open a remote session and allow you to interact with the NComputing vSpace Console for the selected server or make changes to the server itself.

8.2 Desktop Sessions

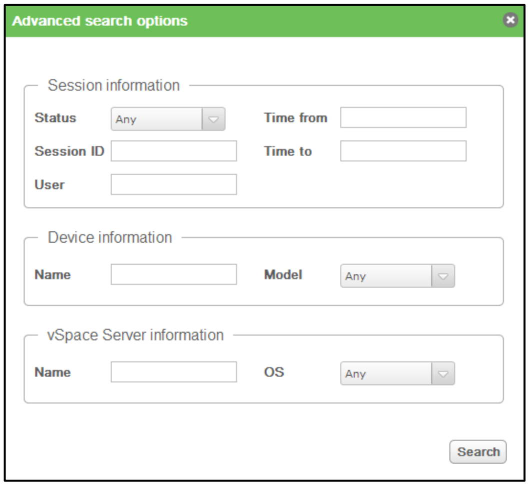
The Desktop Sessions screen allows you to view all active vSpace 7.0 sessions as well as key information such as the model of the device accessing the session and the user name of the user logged in to that session.


NComputing vSpace Management Center
Welcome vmcadmin | Sign out
Version: 3.2.29.21665
Dashboard
Device Management
Group Management
Administration
Help
Administration › Desktop Sessions ›
Desktop Session Administration
Advanced search

Session ID	Session Status	Start Time	vSpace Server	Device Model	Device Name	User Name			
2	Connected	20130315T172207		L300		Administrator	End	Control	View

Items per page: 10

1 - 1 of 1



Status: Any
Session ID:
User:
Time from:
Time to:
Name:
Model: Any
Name:
OS: Any

The Advanced Search feature within this screen allows you to search for sessions within the Management Zone using variables such as Session ID, session creation time, Device Name, Model, or vSpace Server information. This can be especially useful for deployments with hundreds of active devices and sessions.

- **End**
  Clicking End to the right of a session ends the selected session.

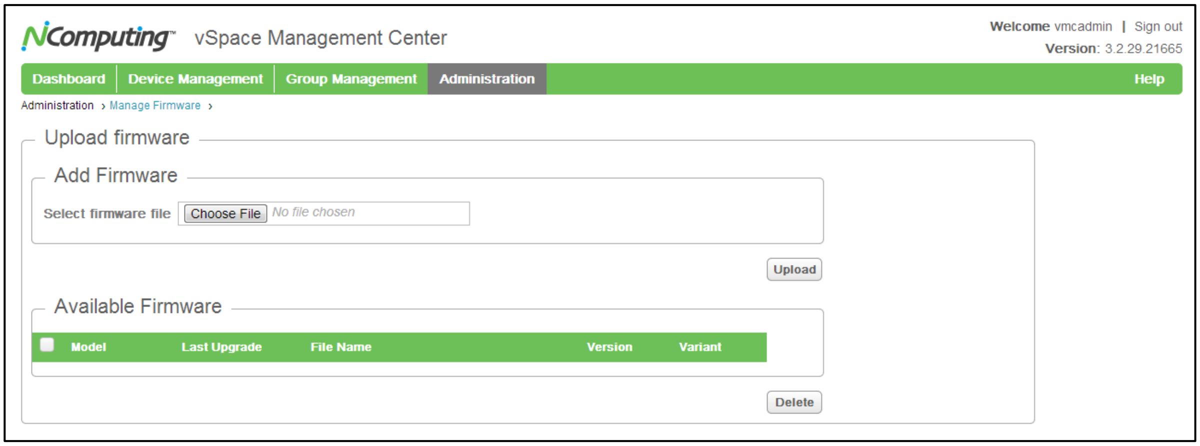
- **Control**
  Clicking Control to the right of a session opens a vSpace Client window allowing the administrator to remotely control the selected session.*

- **View**
  Clicking View to the right of a session opens a vSpace Client window allowing the administrator to remotely view the selected session.*

*Requires that vSpace Client v1.6.2.2 or newer be installed on the system that is accessing vSpace Management Center and initiating the remote view/control session.

8.3 Manage Firmware

The Manage Firmware section allows you to update your inventory of device firmware as new versions become available.

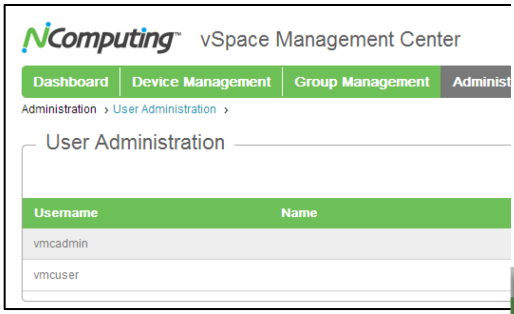


To add a new firmware build, click the "Choose File" button at the top of the screen and navigate to the file's location within Windows. All currently stored firmware builds are displayed in a list at the bottom of the screen.

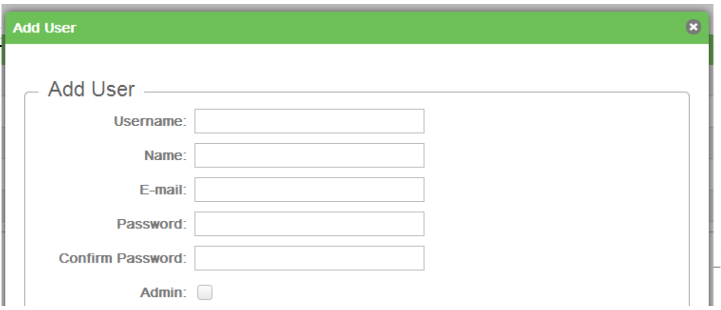
> **NOTE:** In Management Zones with multiple vSpace Management Center servers, uploading firmware files to each of the slave servers is not necessary. Only the master server needs to have the files stored locally in order to push firmware files to access devices. Adding the firmware files to the slave servers does however provide added redundancy in the event that the master server is taken offline and one of the slave servers assumes it's role.

8.4 User Administration

The User Administration screen allows you to create and configure custom user accounts with varying access to vSpace Management Center servers in the event that you do not wish to use Active Directory or a generic LDAP directory service for centralized authentication.


NComputing vSpace Management Center
Dashboard
Device Management
Group Management
Administ
Administration › User Administration ›
User Administration

Username	Name
vmcadmin	
vmcuser	



Existing user accounts are displayed at the bottom of the screen. To add a new user, click the "Add New User" button to the right of the screen.

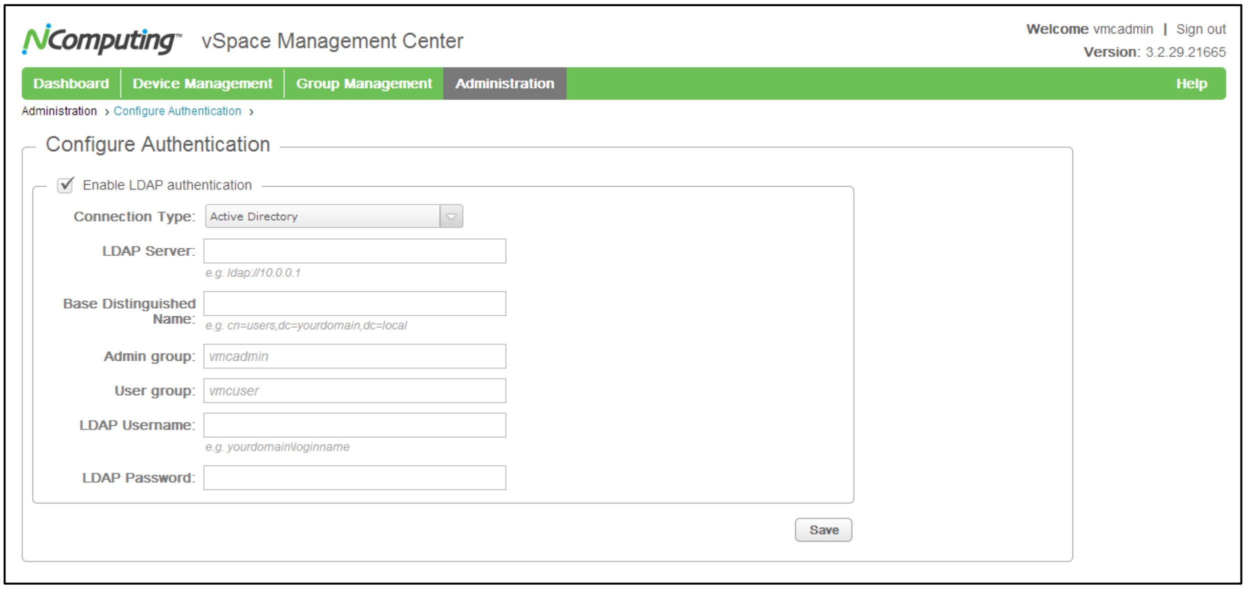
Enter the required account information into the fields provided and select whether the user is to be given admin rights. If enabled, they will have full administrative control over vSpace Management Center servers and their associated devices. If unchecked, they will connect as guests with view-only privileges.

Once you are satisfied with the information entered, press the "Save" button to complete the process. The associated user will then be able access your vSpace Management Center server(s) using these credentials. You can return to the User Administration screen at any time to modify these settings.

> **NOTE:** If authentication to vSpace Management Center is configured for use with Active Directory or a generic LDAP directory, then most of the options within the User Administration screen will be disabled to prevent them from conflicting with domain permissions.
>
> **Best Practice:** Whether creating administrative accounts manually or using existing domain accounts, it is strongly recommended that you create an additional, "backup" administrative account for vSpace Management Center. In the event that the primary administrative account is changed, lost, or for some other reason becomes unusable, the backup account can be used in its place.

8.5 Configure Authentication

The Configure Authentication screen allows administrators to choose how users can authenticate to vSpace Management Center, either through using Active Directory or another vendor's generic LDAP based directory service. This allows multiple levels of administrative access ranging from view-only privileges within vSpace Management Center servers to full editing permissions.


NComputing vSpace Management Center
Welcome vmcadmin | Sign out
Version: 3.2.29.21665
Dashboard
Device Management
Group Management
Administration
Help
Administration › Configure Authentication ›
Save

Configure Authentication

☑ Enable LDAP authentication

Connection Type: Active Directory

LDAP Server: e.g. ldap://10.0.0.1

Base Distinguished Name: e.g. cn=users,dc=yourdomain,dc=local

Admin group: vmcadmin

User group: vmcuser

LDAP Username: e.g. yourdomain\loginname

LDAP Password:

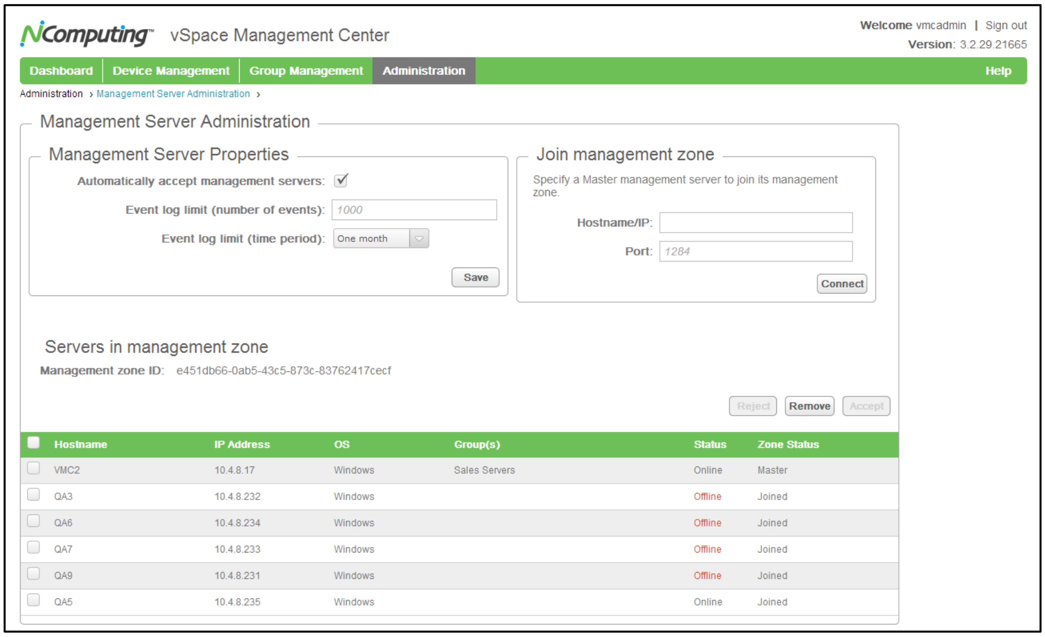
Firstly, select whether or not you wish for vSpace Management Center to use Active Directory or a generic LDAP based directory service. By unchecking the “Enable Authentication” box, vSpace Management Center will rely on the local vSpace Management Center user accounts you create within the User Administration section of the Settings module.

If enabled, you are given the choice between Active Directory integration or LDAP. Use the fields provided to enter the name and location of your domain controller. Then enter the user credentials of a valid domain admin account. Once done, press the “Save” button to the bottom right of the screen.

> **NOTE:** The username and password are only used to verify a successful connection with Active Directory/generic LDAP directory service.

8.6 Management Server Administration

The Management Server Administration screen allows administrators to control how multiple vSpace Management Center servers relate to one another and sets logging parameters.


NComputing vSpace Management Center
Welcome vmcadmin | Sign out
Dashboard
Device Management
Group Management
Administration
Help
Administration › Management Server Administration ›
Save
Connect
Reject
Remove
Accept

Version: 3.2.29.21665

Management Server Administration

Management Server Properties

Automatically accept management servers: ☑

Event log limit (number of events): 1000

Event log limit (time period): One month

Join management zone

Specify a Master management server to join its management zone.

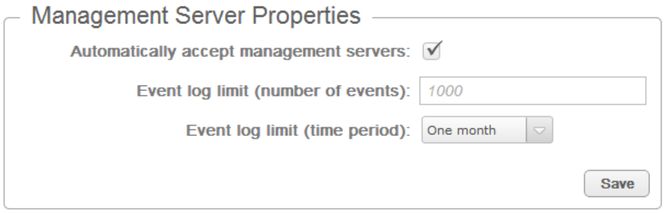
Hostname/IP:

Port: 1284

Servers in management zone

Management zone ID: e451db66-0ab5-43c5-873c-83762417cecf

□	Hostname	IP Address	OS	Group(s)	Status	Zone Status
□	VMC2	10.4.8.17	Windows	Sales Servers	Online	Master
□	QA3	10.4.8.232	Windows		Offline	Joined
□	QA6	10.4.8.234	Windows		Offline	Joined
□	QA7	10.4.8.233	Windows		Offline	Joined
□	QA9	10.4.8.231	Windows		Offline	Joined
□	QA5	10.4.8.235	Windows		Online	Joined



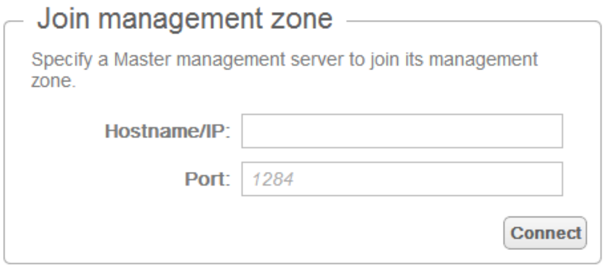
Management Server Properties

Automatically accept management servers: ☑

Event log limit (number of events): 1000

Event log limit (time period): One month

Under the **Management Server Properties** section of this screen, you can decide whether new management servers automatically join your current server's vSpace Management Center zone, or whether they must be allowed to do so via manual acceptance. You can also set the limit for events in your event log within a certain timeframe.



Join management zone

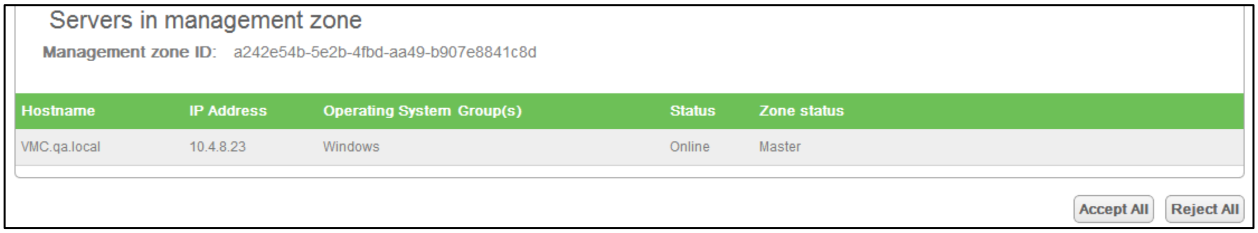
Specify a Master management server to join its management zone.

Hostname/IP:

Port: 1284

The **Join management zone** section of the screen allows you to manually join an existing vSpace Management Center zone by connecting to a server within that zone. If this is the first time a connection between vSpace Management Center servers has occurred within your domain, a new zone will be created automatically and your servers will enter a master / slave relationship based on the order in which they were joined. In a scenario where server B joins server A, server A becomes the master. In other words: the joining server becomes the slave and the server it joins becomes the master.

Lastly, the bottom of the screen displays a list of servers within the current server's zone. This list includes servers that have already been joined and servers that are awaiting approval to join. If this screen is viewed from the master server, you can accept or reject server applications from this list. You can also view the Management Zone ID from this section of the screen, which is unique to each zone.



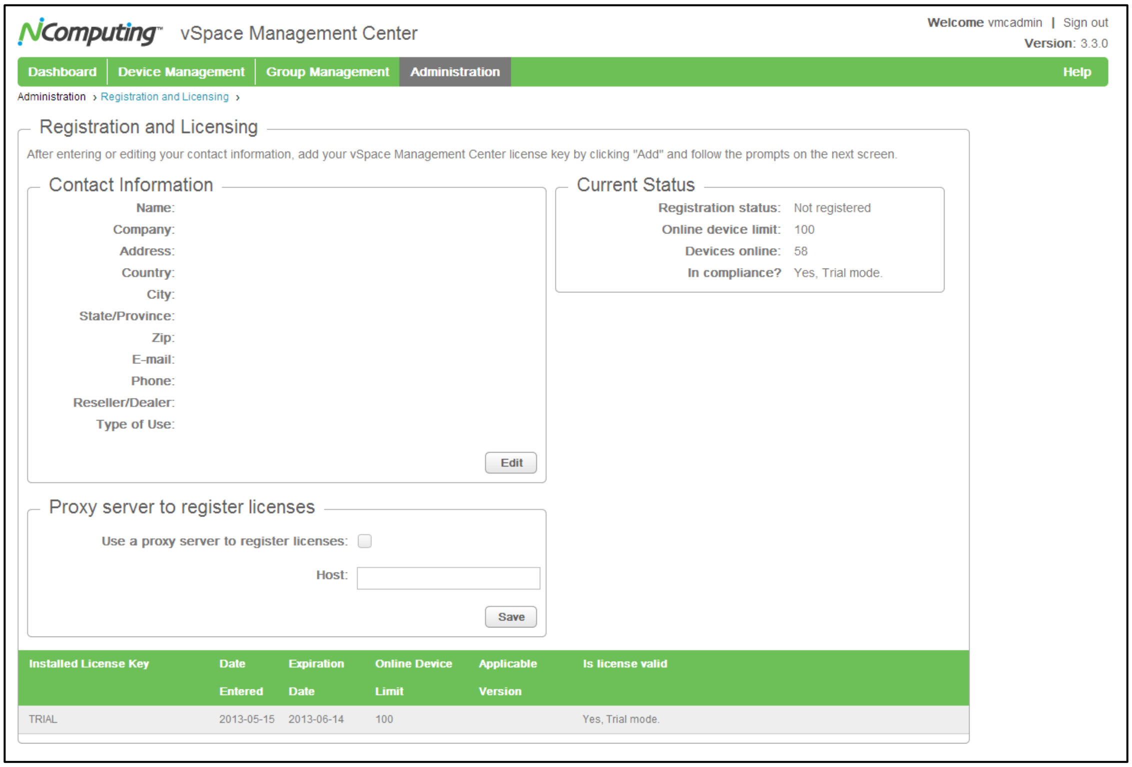
Servers in management zone

Management zone ID: a242e54b-5e2b-4fbd-aa49-b907e8841c8d

Hostname	IP Address	Operating System	Group(s)	Status	Zone status
VMC.qa.local	10.4.8.23	Windows		Online	Master

8.7 Registration and Licensing

The Registration and Licensing screen provides you with a summary of your current vSpace Management Center licensing status and lets you add license keys. The initial registration process consists of filling out the **Contact Information** section of this screen, and then adding a license key as outlined below. The **Proxy server to register licenses** section allows for the use of a Proxy during registration



NComputing vSpace Management Center
Welcome vmcadmin | Sign out
Dashboard
Device Management
Group Management
Administration
Help
Administration › Registration and Licensing ›

Version: 3.3.0

Registration and Licensing

After entering or editing your contact information, add your vSpace Management Center license key by clicking "Add" and follow the prompts on the next screen.

Contact Information

Name:
Company:
Address:
Country:
City:
State/Province:
Zip:
E-mail:
Phone:
Reseller/Dealer:
Type of Use:

Current Status

Registration status:	Not registered
Online device limit:	100
Devices online:	58
In compliance?	Yes, Trial mode.

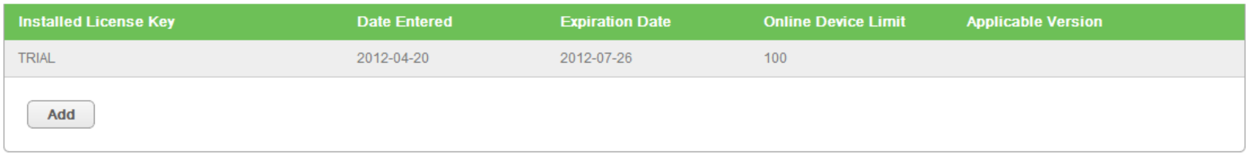
Proxy server to register licenses

Use a proxy server to register licenses: □

Host:

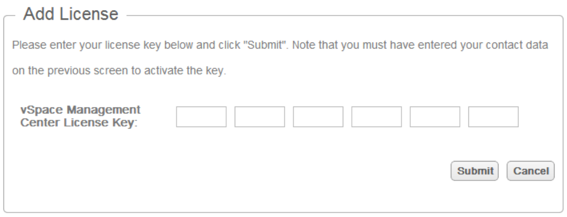
Installed License Key	Date Entered	Expiration Date	Online Device Limit	Applicable Version	Is license valid
TRIAL	2013-05-15	2013-06-14	100		Yes, Trial mode.

The **Current Status** section to the right of the screen displays basic information on your current vSpace Management Center registration status and licensing scheme. The bottom of the screen lists each of your currently installed licenses. Note that licenses can be continually added to vSpace Management Center to accommodate an increase in the volume of managed devices over time as a deployment grows.



Installed License Key	Date Entered	Expiration Date	Online Device Limit	Applicable Version
TRIAL	2012-04-20	2012-07-26	100	

To add licenses to your vSpace Management Center installation, click the **"Add"** button to the bottom left of the Registration and Licensing screen and enter the serial number(s) of the license(s) in question. Note that the Add button will not appear until you have filled out the Contact Information section.



Add License

Please enter your license key below and click "Submit". Note that you must have entered your contact data on the previous screen to activate the key.

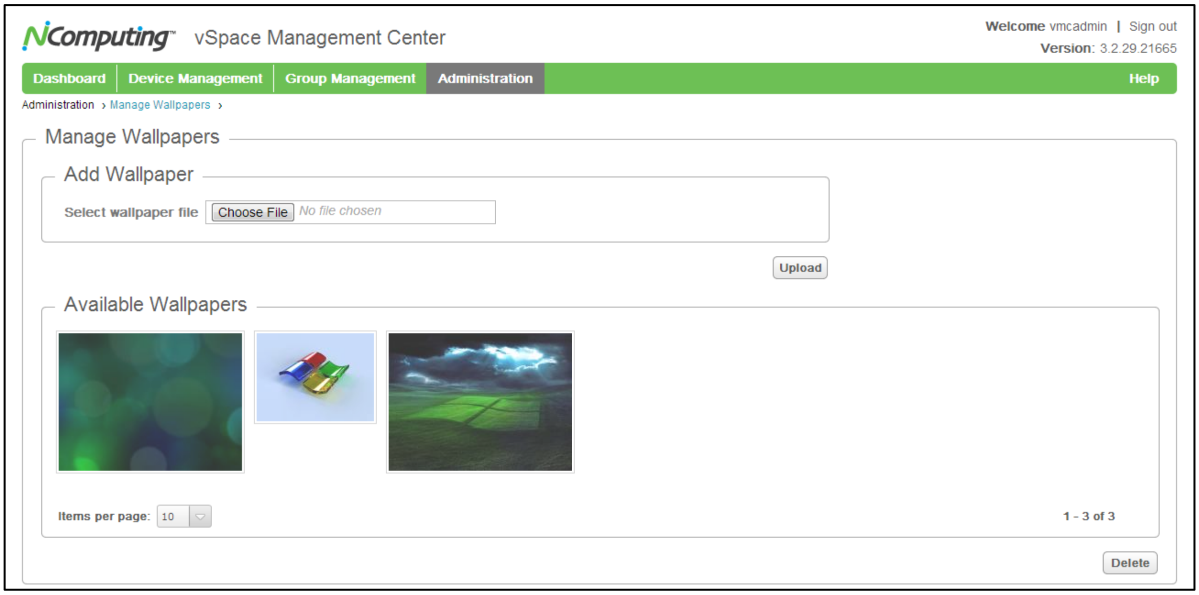
vSpace Management Center License Key:

8.7b N-series and vSpace Management Center Bundled Entitlement

Customers who have purchased N-series devices with vSpace Management Center bundled can obtain their complimentary vSpace Management Center license(s) by visiting the following URL and entering the required purchase information:
http://www.ncomputing.com/enroll
For more information on how to activate bundled vSpace Management Center and Premium Support entitlement, visit the following Knowledge Base article:
http://www.ncomputing.com/kb/N-series-bundled-entitlement-to-vSpace-Management-Center-and-Premium-Support_345.html

8.8 Manage Wallpapers

The Manage Wallpapers screen allows you to upload and manage wallpapers for use with your N-series devices. The screen provides a preview of stored wallpapers and a standard Windows browse feature to locate and add additional wallpapers to the existing inventory.



Page **53** of **65**

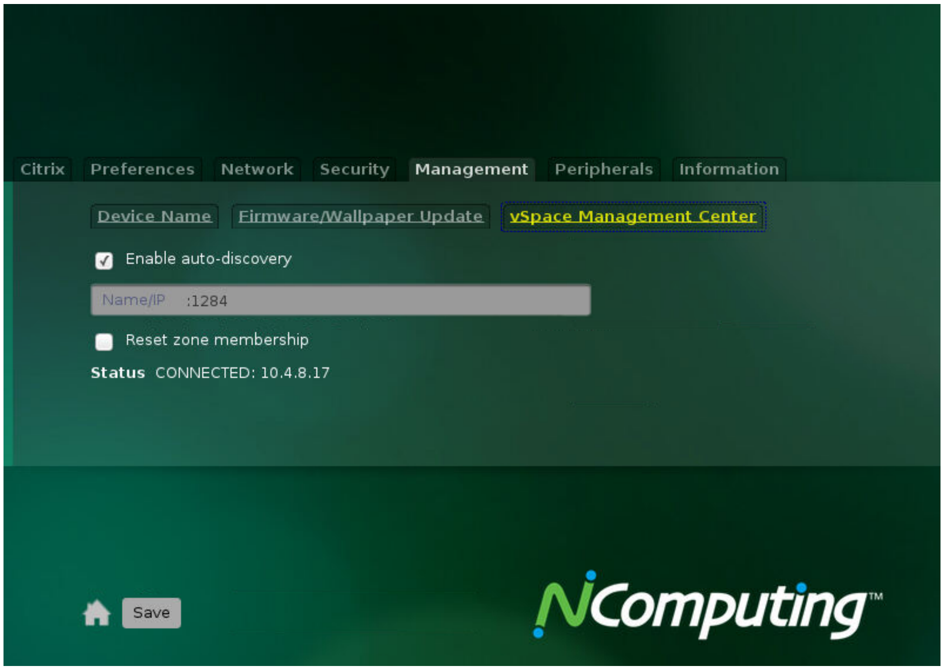
9.0 Common Usage Scenarios

This section of the user manual includes several common usage scenarios that demonstrate the use of vSpace Management Center to perform some common administrative tasks such as selecting and pushing firmware updates to multiple devices simultaneously, configuring devices using profiles, and backing up vSpace Management Center server files.

9.1 Adding an N-series device to vSpace Management Center

In this scenario we'll go over the task of linking NComputing N-series devices to vSpace Management Center so that they can be remotely managed using the vSpace Management Center toolset.

1. Enter the **Settings Menu** from your N-series device and click the **Management Tab**.
2. Select **vSpace Management Center**, as shown below.



☑ Enable auto-discovery

Name/IP :1284

☐ Reset zone membership

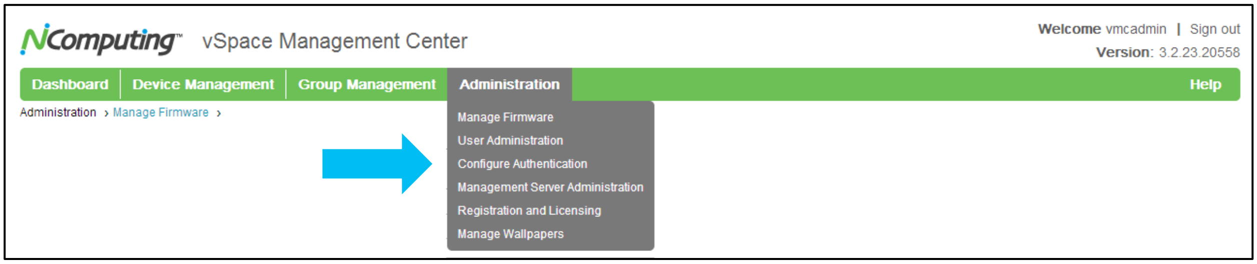
Status CONNECTED: 10.4.8.17

3. By setting **auto-discovery** to Enabled (default setting), your N-series device will automatically join any vSpace Management Center server within its subnet.
4. (Optional): If there is no vSpace Management Center server within your device's subnet, or you wish to manually enter the vSpace Management Center server's location, you may do so by disabling Discovery and entering the IP address or Fully Qualified Domain Name in the **Services** field.

Note: You can also configure your DHCP Server to automatically direct N-series devices to a vSpace Management Center server. Visit http://www.ncomputing.com/kb/Configuring-DHCP-for-Automatic-N-series-Configuration_338.html for more details.

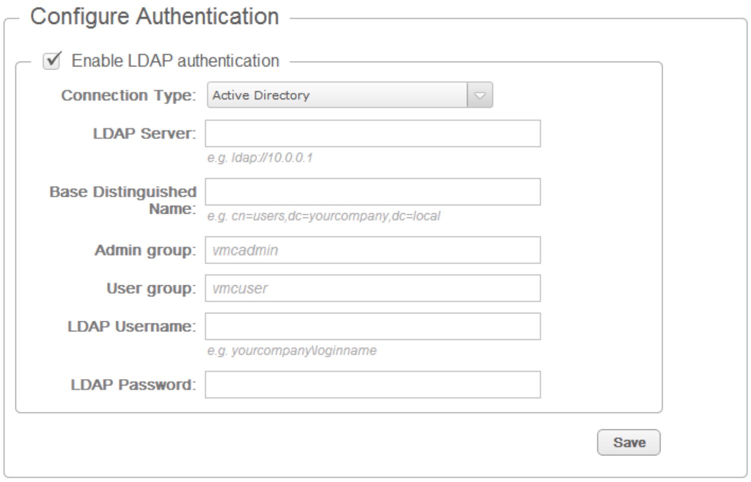
9.2 Configuring vSpace Management Center with Active Directory

To help keep your account management centralized within your environment, vSpace Management Center includes the option for users to authenticate to vSpace Management Center via Active Directory.



1. From the **Settings** module, navigate to the **Configure Authentication** screen.

2. Check the box next to "Enable LDAP Authentication" and then select "Active Directory" from the **Connection Type** dropdown.



3. Enter the URL of your Active Directory server in the **LDAP Server** field.

4. Enter the name of your Domain in the **Base Distinguished Name** field.

5. Enter the admin and user group names you wish to use for vSpace Management Center administrators and users. Default values are provided, but you can use an alternate naming scheme if you desire.

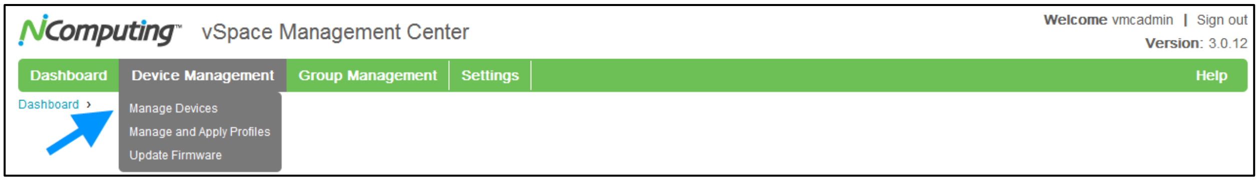
6. Supply the Username and Password of a user account with access to your Active Directory server in the LDAP Username and Password fields, and then press the "Save" button to the bottom right of the screen.

7. Lastly, Using Active Directory Users and Computers on your AD server, create two new user groups with the group names you selected in **step 5**. vSpace Management Center will convey the appropriate privileges to members of these groups. (Users = read only. Admins = read/edit.)

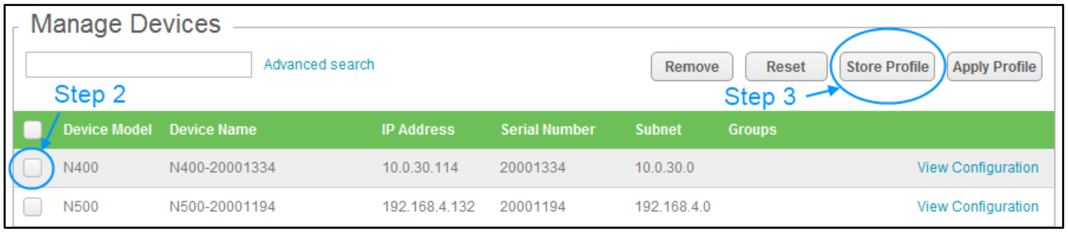
9.3 Configuring devices using device profiles

In this scenario we'll describe the process of creating, managing, and pushing device profiles to your NComputing devices.

A device profile can be created from scratch or imported from any device in your deployment. For the purpose of this scenario, we'll import a profile, save it as a preset, and then push that profile out to additional devices. To do so, follow these steps:

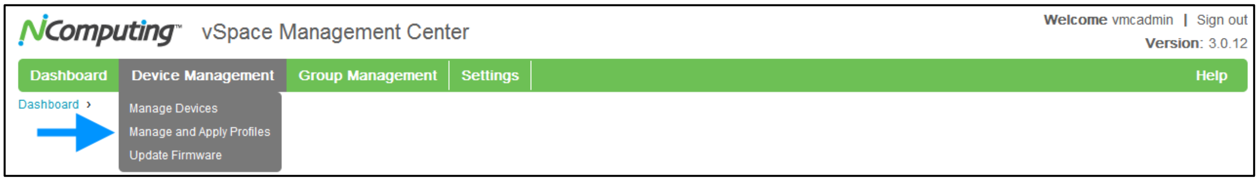


1. From the **Device Management** module within vSpace Management Center, open the **Manage Devices** screen.

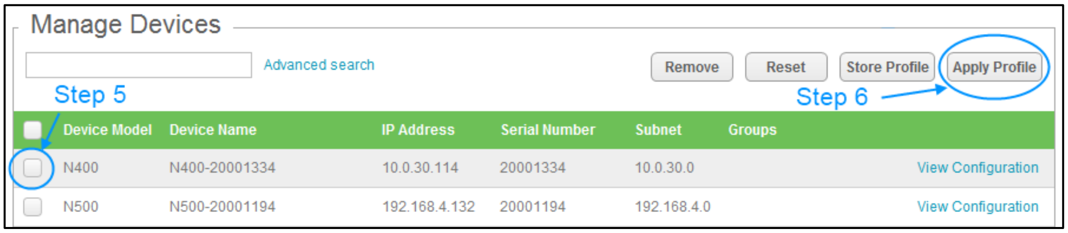


□	Device Model	Device Name	IP Address	Serial Number	Subnet	Groups	
□	N400	N400-20001334	10.0.30.114	20001334	10.0.30.0		View Configuration
□	N500	N500-20001194	192.168.4.132	20001194	192.168.4.0		View Configuration

2. Select the device whose profile you wish to store by checking the checkbox to its left.
3. Click the "Store Profile" button to the top right of the screen to proceed through the profile storing dialog.



4. (Optional): You can review and make alterations to the profile you have just created from the **Manage and Apply Profiles** screen within the **Device Management** module.



□	Device Model	Device Name	IP Address	Serial Number	Subnet	Groups	
□	N400	N400-20001334	10.0.30.114	20001334	10.0.30.0		View Configuration
□	N500	N500-20001194	192.168.4.132	20001194	192.168.4.0		View Configuration

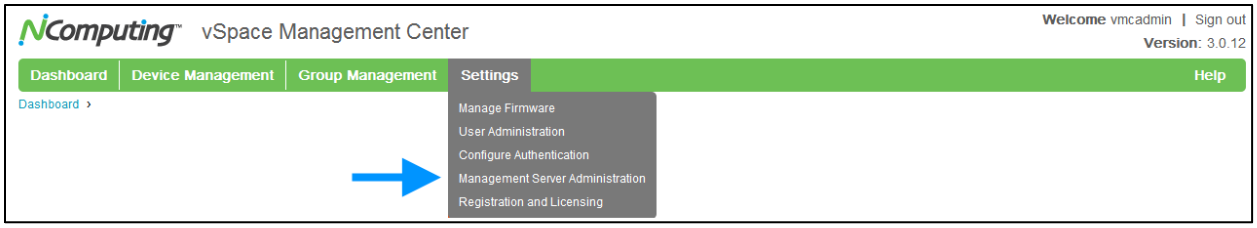
5. From the **Manage Devices** screen, select the device(s) you wish to push your new profile using the checkboxes as in step 2.
6. Once you are satisfied with your selection, click the "Apply Profile" button to apply your new profile to the selected device(s).

9.4 Adding a new vSpace Management Center server to your vSpace Management Center Zone

A group of vSpace Management Center servers working together to manage your NComputing deployment is referred to as a "management zone" or simply "zone." In this scenario we'll discuss the task of adding additional vSpace Management Center servers to your zone as well as outline some of the benefits that multiple servers can offer administrators.

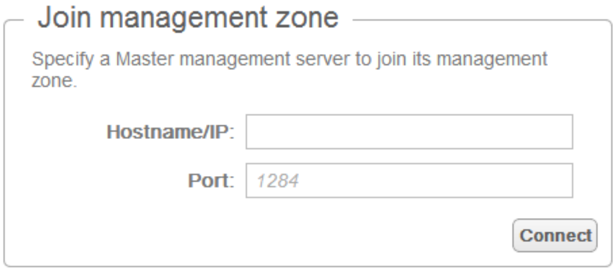
vSpace Management Center servers will automatically join each other to form a management zone if they are within the same subnet and the Management Server Auto-Acceptance feature is enabled. If the Auto-Acceptance feature is not enabled, or differing subnets separate your vSpace Management Center servers, use the following steps to manually join them together:

Joining a Zone from within vSpace Management Center:



1. Open the **Management Server Administration** section of the **Settings** module within vSpace Management Center.

2. In the **Join management zone** field, enter the IP address or fully qualified domain name of the vSpace Management Center server you wish to join in the Host field, with the appropriate port (1284 by default).


Join management zone

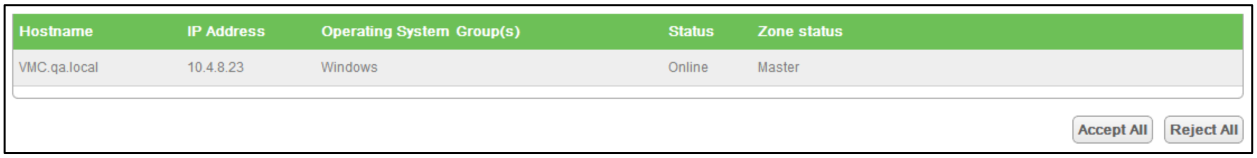
Specify a Master management server to join its management zone.

Hostname/IP:

Port: 1284

NOTE: If you already have a vSpace Management Center Zone comprised of multiple vSpace Management Center servers, you'll need to join the master server within that Zone. The master server is flagged as such in the server list at the bottom of the Management Server Administration screen on all servers within the Zone (as seen below).

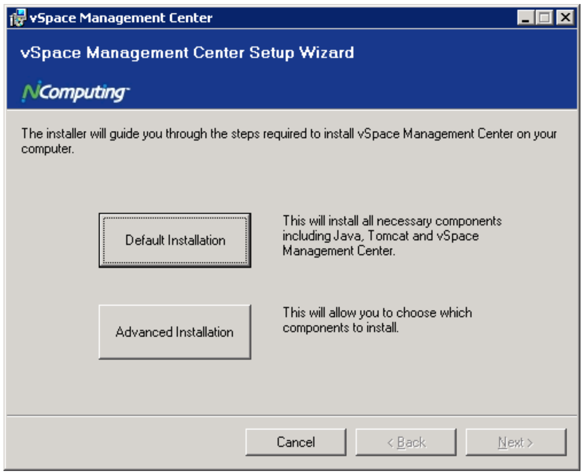
3. From the server you elected to join, accept the join request which should now appear at the bottom of the Management Server Administration screen. This completes the process and creates a vSpace Management Center Zone.



Hostname	IP Address	Operating System	Group(s)	Status	Zone status
VMC.qa.local	10.4.8.23	Windows		Online	Master

Joining a Zone during Installation:

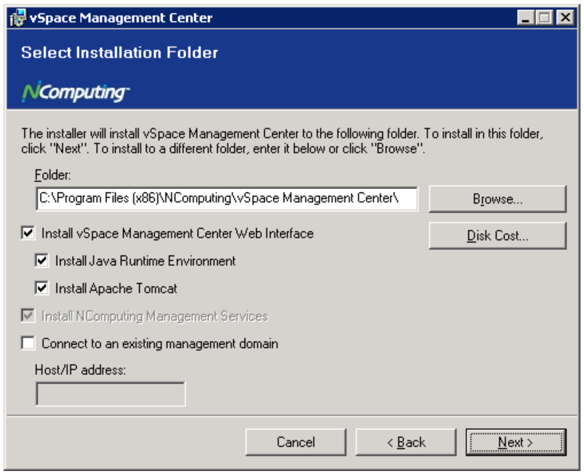
In addition to joining from the Settings module, you can also perform this task automatically when you install vSpace Management Center. This option is available to you as part of the installer.



The installer will guide you through the steps required to install vSpace Management Center on your computer.

This will install all necessary components including Java, Tomcat and vSpace Management Center.

This will allow you to choose which components to install.



The installer will install vSpace Management Center to the following folder. To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\NComputing\vSpace Management Center\

☑ Install vSpace Management Center Web Interface
☑ Install Java Runtime Environment
☑ Install Apache Tomcat
☑ Install NComputing Management Services
□ Connect to an existing management domain

Host/IP address:

During the installation process, select the Advanced Installation option. In the dialog that follows, check the option titled "Connect to an existing management zone". Enter the the IP address of the vSpace Management Center server you wish to join and proceed with installation. Your new vSpace Management Center server will automatically join with your existing Zone once the installation process is complete.

Joining a Zone from Windows:

Lastly, you can use the CMFconnect utility included with vSpace Management Center to join your server to a Zone.

1. From the Windows Start menu, click on vSpace Management Center as you would to launch the management interface.
2. Click the CMFconnect utility to launch the connection dialog and proceed as directed through the utility to join your vSpace Management Center to an existing Zone.

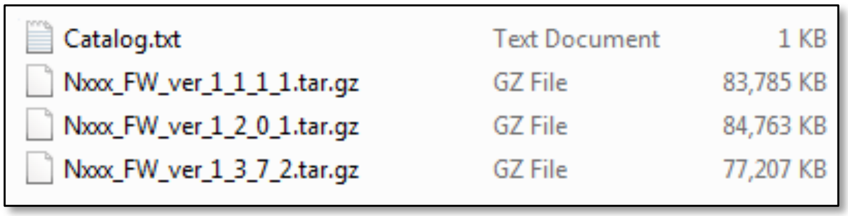
9.5a Automating Sequential Firmware Updates

N-series firmware is designed to be applied sequentially, with each new build applied to the previous build in order of their release. Administrators can manually step a device through sequential firmware updates if desired, or they can configure the devices to perform a sequential update automatically.

> **NOTE:** If a device is updated out of sequence and ends up skipping a firmware build, this can be corrected by downgrading the device and reapplying the firmware update process from beginning to end. Once the device has been updated to firmware version 1.4.1, the remainder of the update process can be automated, as outlined below.

Requirements for Automatic, Sequential Updates

An automatic update requires that the devices be set to either of the “automatic” (DHCP* or URL) update modes (found in **Firmware/Wallpaper Update** section of the **Management Tab** in the N-series GUI) and pointed to a network accessible folder** that contains each of the required firmware builds. The folder should contain the desired firmware files themselves as well as a catalog.txt file, as pictured below:



Catalog.txt	Text Document	1 KB
Nxxx_FW_ver_1_1_1_1.tar.gz	GZ File	83,785 KB
Nxxx_FW_ver_1_2_0_1.tar.gz	GZ File	84,763 KB
Nxxx_FW_ver_1_3_7_2.tar.gz	GZ File	77,207 KB

The catalog.txt file functions as a table of contents for the update service; listing each of the firmware builds in a given archive in the order that they were released. Below is an example of the contents of a catalog.txt file that contains information for three firmware builds, ranging from build 1.1.1 to build 1.3.7.

```
Nxxx_FW_ver_1_1_1_1.tar.gz0 0 0 1 1 1 1 02e90025e8239722e58b62b3a9b92386

Nxxx_FW_ver_1_2_0_1.tar.gz0 0 0 1 2 0 1 945434214db5285596a24404a637471d

Nxxx_FW_ver_1_3_7_2.tar.gz0 0 0 1 3 7 2 a4f5dcdeb8de66aaabfe804fc3a5ee93
```

Each new firmware build is released with a catalog.txt file containing a single line. The above catalog.txt file contains three lines because it was written for an archive that contains three firmware builds. In the event that a new firmware build was released, the archive could be updated by adding the firmware file itself to the folder, and copying the catalog.txt line included with that firmware into the archive’s catalog.txt file. In this case, the next firmware build would add a fourth line.

* Note that using the DHCP setting requires that DHCP tags be configured with the appropriate FTP information. See the N-series User Manual for more information on configuring DHCP tags for automatic updates.

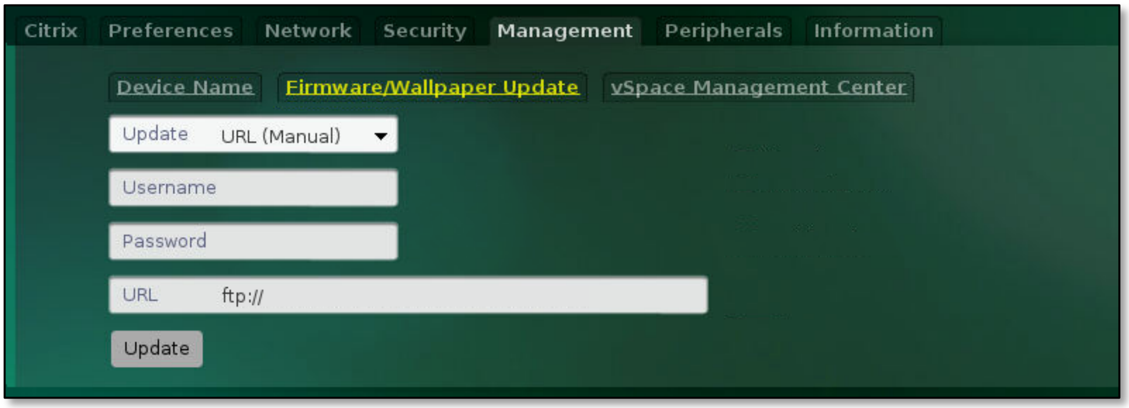
** If a network accessible folder is not available, or assistance is needed to set up such a resource, an example is given using FileZilla at the end of this guide.

9.5b Directing N-series Devices To The Firmware Archive Using the N-series GUI

Once a folder or archive is set up with the above listed requirements, administrators can configure their N-series devices on a per-device basis if desired. This process is outlined in the steps below.

1. From the **Manage Profiles** menu, select the N-series profile you wish to edit. If an N-series profile does not already exist, use the steps outlined in Section 4.5 of this manual to create a new profile for the devices you wish to update.

2. Navigate to the Management Tab, and then select Firmware/Wallpaper Update (pictured below).



Update: URL (Manual)

Username

Password

URL: ftp://

3. Using the **FTP, User, and Password fields**, enter the FTP location of the newest firmware build within the archive you have created. (this will be a file ending in .tar.gz)

4. When finished, click the **Update** button to begin the sequential update.

At this point the device will begin the process of updating to the newest version of firmware available within the archive you have created, proceeding through each of the intervening builds between its current version and the newest version as outlined within the catalog.txt file.

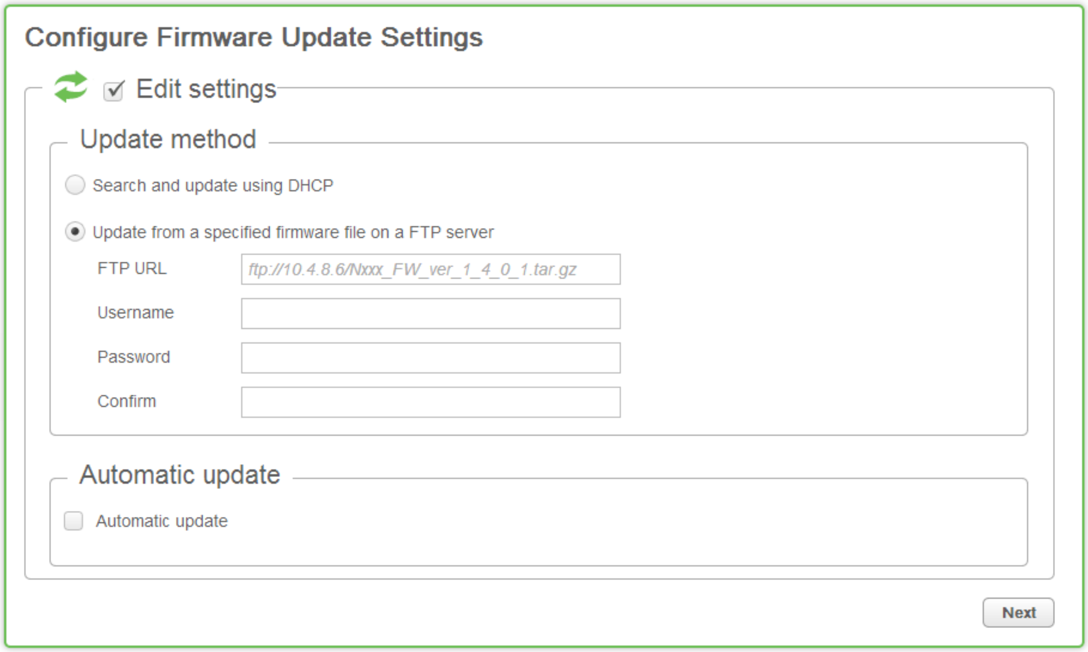
9.5c Directing N-series Devices To The Firmware Archive Using Device Profiles

If a deployment includes vSpace Management Center, administrators can configure all of their N-series devices for automatic updates at the same time through the use of **Device Profiles**. Keep in mind that as with the device GUI method, the FTP folder and firmware archive must be set up prior to initiating the update. The process for initiating the update from vSpace Management Center is outlined in the steps below.

> **IMPORTANT NOTE:** N-series devices must already be running firmware version **1.2.0.1 or newer** to receive a firmware update from vSpace Management Center. If the intended devices are running firmware older than 1.2.0.1, the device GUI method above must be used instead.

1. From the **Manage Profiles** menu, select the N-series profile you wish to edit. If an N-series profile does not already exist, use the steps outlined in Section 4.5 of this manual to create a new profile for the devices you wish to update.

2. Navigate to the Firmware Update Tab (pictured below).



Configure Firmware Update Settings

☑ Edit settings

Update method

○ Search and update using DHCP

● Update from a specified firmware file on a FTP server

FTP URL: ftp://10.4.8.6/Nxxx_FW_ver_1_4_0_1.tar.gz

Username:

Password:

Confirm:

Automatic update

□ Automatic update

3. Check the box next to "**Edit settings**" setting at the top of the menu, then select "**Update from a specified firmware file on a FTP server**".

4. Using the **FTP, User, and Password fields** (making sure to re-enter your password in the Confirm field), enter the FTP location of the newest firmware build within the archive you have created. (this will be a file ending in .tar.gz)

5. Take a moment to verify that all other profile settings are as you desire (including screen resolution, XenDesktop settings, etc), and apply the profile from the **Summary Tab**.

6. If you have not done so already, upload the latest firmware build to your vSpace Management Center server, using the **Manage Firmware** menu under the **Administration Tab**.

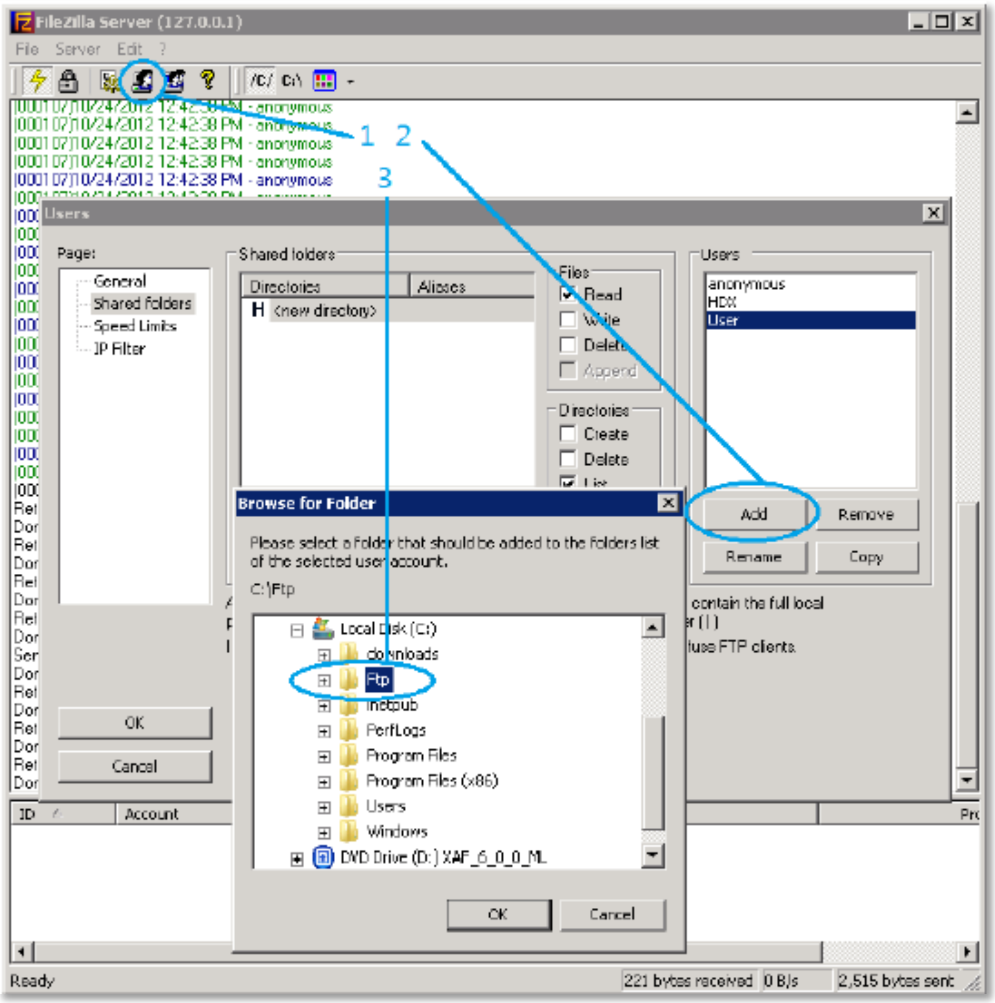
7. Once the above steps have been completed, head to the **Manage Devices** menu under the **Device Management Tab** and initiate a firmware update on the devices of your choice, selecting the most recent firmware version available.

At this point the selected devices will begin pulling updated firmware in the order specified within the catalog.txt with automatic reboots between each firmware version until the process is complete.

9.5d Example of FTP Folder Setup Using FileZilla

In the case of FileZilla, hosting an existing folder on your host system is a simple process. Once installed, open the FileZilla server interface and complete the following steps:

1. Click on the **Users** icon at the top left of the FileZilla Server window.
2. Click the **Add** button under the Users section to the right of the window and create a new user. (This will be the user account you add to your NComputing device later in this guide)
3. **Add a new folder** under the Shared Folders section and select the folder containing your firmware files. This can be the folder mentioned in the previous section, or any other folder if you've decided to host the files elsewhere. (Note the folder's path as it will be important later in this guide)



(000107)10/24/2012 12:42:38 PM - anonymous

Please select a folder that should be added to the folders list of the selected user account.

C:\Ftp

contain the full local

r (|)

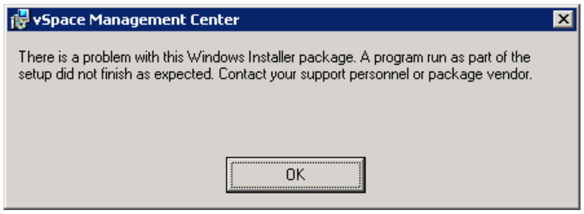
luse FTP clients

Your firmware files are now shared and available for download via FTP by your devices.

10.0 Troubleshooting

Error: There is a problem with this Windows Installer package.

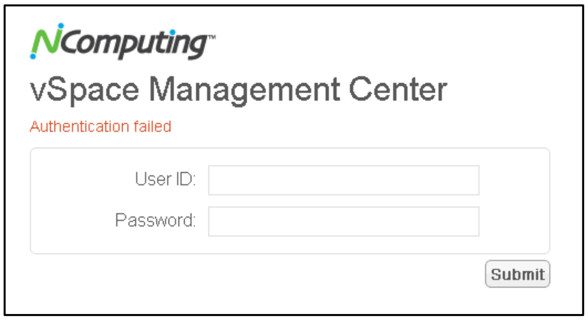
Both Java and Apache Server are required for vSpace Management Center to function properly. If you encounter this error during installation, check to make sure that you have successfully installed both of these components and try again. For your convenience, installers for both of these products are included as part of the "Default" vSpace Management Center installation method.



There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.

Error: Authentication failed

If you receive this error while attempting to log in to the vSpace Management Center user interface, check that you are using the correct credentials and try again. Also check that your caps lock and num lock settings are not interfering with the correct entry of your User ID and Password.



Authentication failed

My device doesn't show up in vSpace Management Center

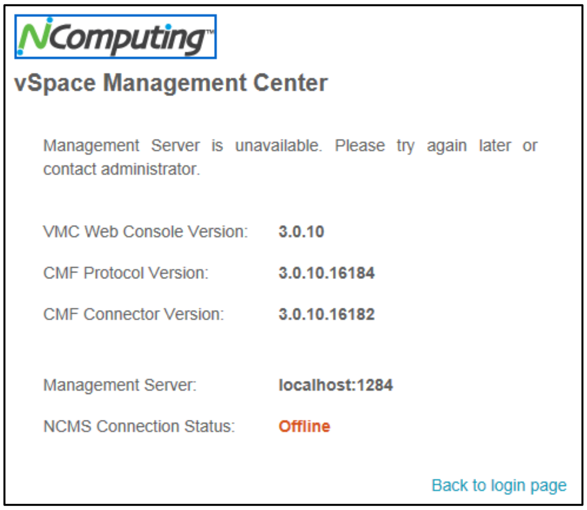
Make sure that you've added the device to vSpace Management Center. Note that this doesn't necessarily happen automatically. Refer to **Section 7.1 Adding a Device to vSpace Management Center** within this document for detailed instructions. For information on configuring your DHCP server to automatically link NComputing devices to vSpace Management Center, review the following Knowledge Base article: http://www.ncomputing.com/kb/Configuring-DHCP-for-Automatic-N-series-Configuration_338.html

Also, be sure that your firewall and network security resources are configured to allow vSpace Management Center to communicate with devices in your environment. For detailed information on Firewall and Antivirus configuration for NComputing products, review the following Knowledge Base article: http://www.ncomputing.com/kb/Configuring-Firewall-and-Antivirus-for-NComputing-Products_63.html

Management Server Connection Status: Offline

An offline status can be an indication that the NC Management Server service is not currently running on the host system.

To check the status of the Management Server service, open the Services window under Start->Administrative Tools on the host system or simply run “services.msc” from the start menu. Once opened, search for “NC Management Server”.



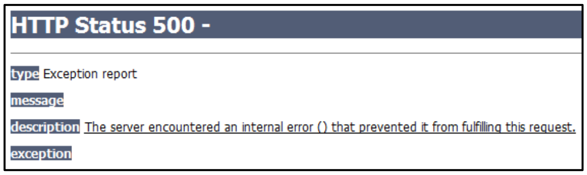
vSpace Management Center

Management Server is unavailable. Please try again later or contact administrator.

VMC Web Console Version:	3.0.10
CMF Protocol Version:	3.0.10.16184
CMF Connector Version:	3.0.10.16182
Management Server:	localhost:1284
NCMS Connection Status:	Offline

HTTP Status 500 Error

An HTTP Status 500 error can usually be resolved by simply clearing your browser’s cache. This error may present itself in certain rare cases including when the browser cache is not cleared after a new version of VMC is installed, as outlined in the installation section of this manual.



HTTP Status 500 -

type Exception report

message

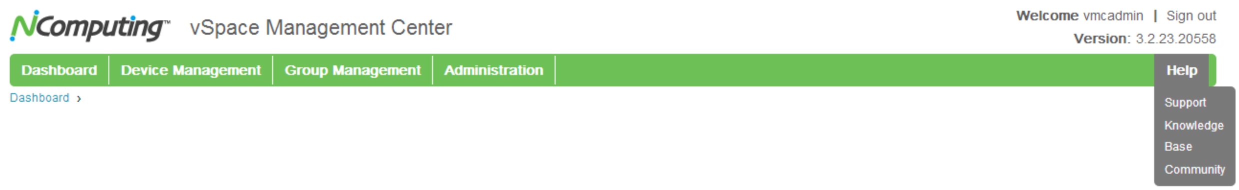
description The server encountered an internal error () that prevented it from fulfilling this request.

exception

The “Enable auto launch” and “Enable auto log off” settings don’t seem to affect my devices

These features have recently been added to vSpace Management Center to give administrators more options for controlling application and session behavior. A future firmware release will enable these settings on the device side.

11.0 Support and Additional Resources



The Help module of the Navigation bar can direct you to several of NComputing's support resources. These resources are outlined below:

NComputing Technical Support

To request Technical Support for NComputing products, please visit the NComputing Support page at http://www.ncomputing.com/support

NComputing Knowledge Base

For additional technical documentation, solutions, and how-toe's, visit http://www.ncomputing.com/kb/

11.1 Disclaimers and Legal Information

Information contained in this document may have been obtained from internal testing or from a third party. This information is for informational purposes only. Information may be changed or updated without notice. NComputing reserves the right to make improvements and/or changes in the products, programs and/or specifications described herein anytime without notice. All NComputing software is subject to NComputing intellectual property rights and may be used only in conjunction with Genuine NComputing hardware and in accordance to the NComputing End User Licensing agreement and Terms of Use.

www.ncomputing.com