PowerManage IV

Requirements and Installation Guide



NOTICE

This document contains proprietary and confidential material of Visonic Ltd. Any unauthorized, reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited. This document is solely for the use of Visonic employees and any authorized customers. Visonic Ltd. reserves the right to make changes in the specifications at any time and without notice.

Preface

This document provides details and defines the requirements needed on the customer side prior and during a Power Manage IV server installation and configuration.

The installation will be performed by the customer IT team with the technical support engineer assistance.

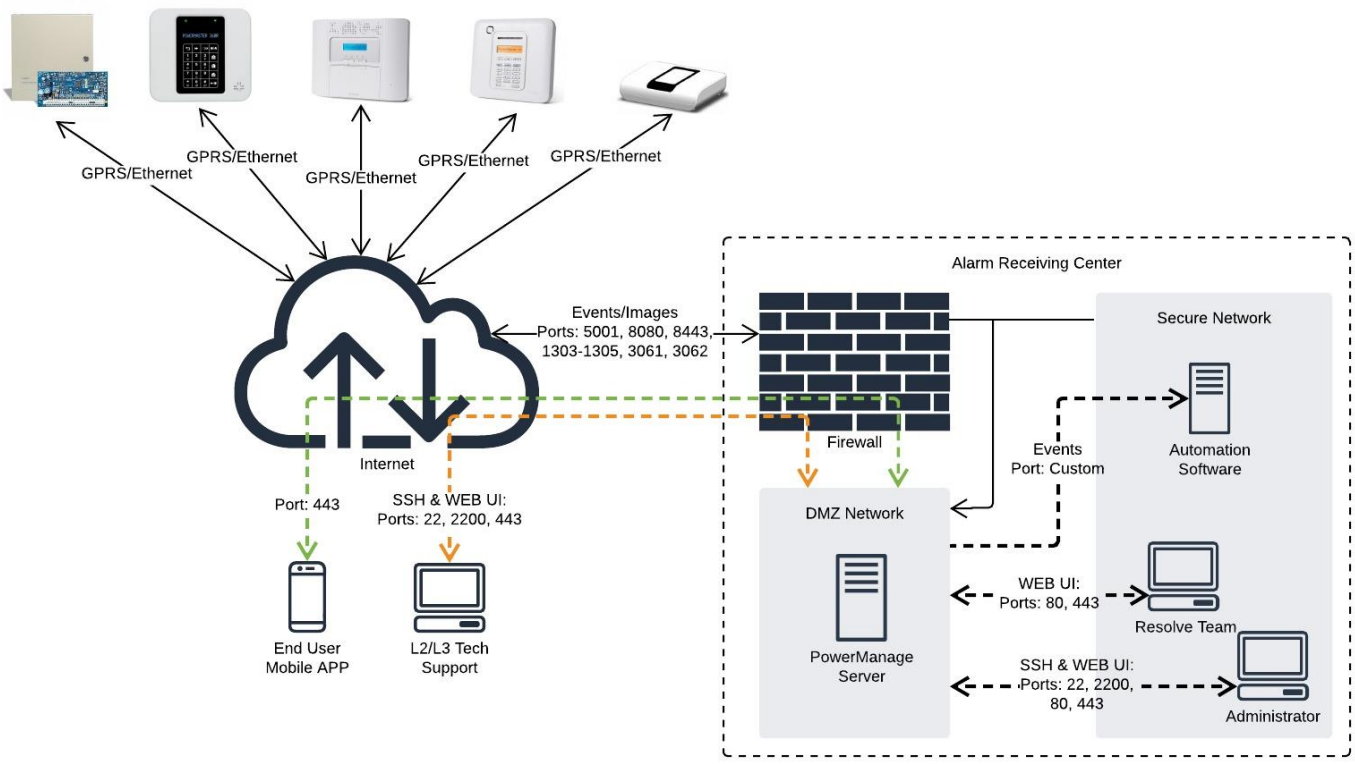
The customer is required to read the relevant sections throughout the entire document and to verify to the point of contact at Tyco/Visonic that all of the requirements will be met on the installation date.
A moderate level of server-based knowledge and experience is assumed**.**

Note: Not all features of the installation system are detailed.

About PowerManage IV

Power Manage IV is a highly efficient web based host platform for provisioning and managing a home security and automation services provided by a security service provider. PowerManage IV elaborates the usage of open standard technologies and open source OS. For more info about PowerManage IV refer to the PowerManage IV Online Help Manual.

The diagram shown below illustrates the typical PowerManage solution installation architecture:



PowerManage - Supported Hardware

➢ *High performance systems hardware:*

HPE ProLiant DL380 Gen10 5118 2P 64GB-R P408i-a 8SFF 2x800W PS

Component	*Description*
Form Factor	2U Rack Server
Dimensions	17.54 x 28.75 x 3.44 in
Processor	Intel® Xeon® 5118 (12 core, 2.3 GHz, 16.5 MB, 105W)
Memory	HPE 64GB (4x16GB) Dual Rank x8 DDR4-2666
Storage Controller	HPE Smart Array P408i-a SR Gen10 12G SAS Modular Controller
Hard Drives	8 SFF (HP 2x600 GB SAS 10k 2,5” SFF recommended)
Power Supply:	(2) 800W Flex Slot Platinum hot plug power supply kit
ILO	Advanced

*For more details follow this link: DL380G10 **[868703-B21]***

HP ProLiant DL380 Gen9 E5-2650v3 2P 32GB-R P440ar 8SFF 2x10Gb 2x800W PS

Component	*Description*
Form Factor	2U Rack Server
Dimensions	17.54 x 26.75 x 3.44 in
Processor	Intel® Xeon® E5-2650 v3 (40 core, 2.3 GHz, 25MB, 105W)
Memory	64GB (4x16GB) RDIMM
Storage Controller	Dynamic Smart Array B140i and Smart Array P440ar/2GB FBWC
Hard Drives	8 SFF Chassis, 440ar/2GB SAS controller
Power Supply:	(2) 800W Flex Slot Platinum hot plug power supply kit

ILO	Advanced

*For more details follow this link: **DL380G9** **[752689-B21]***

➢ *High performance systems load benchmarking:*

High performance system solution handles simultaneously:

- *Monitor and Manage up to 100K panels*
  - *PowerMaster and/or*
  - *PowerSeries Neo/PRO panels*
- *PowerMaster keep-alive*
  - *GPRS = 600sec,*
  - *Broadband = 5sec.*
- *PowerSeries Neo/Pro keep-alive*
  - *GPRS/Broadband = 135sec.*
- *Events/Alarms*
  - *Handling 100 events/sec*
- *Visual Verification*
  - *Support 10 events/sec*
- *Concurrent FW upgrade*
  - *Up to 1K/hour*
- *Concurrent Remote Inspection*
  - *Up to 1K/hour*
- *Concurrent CSV report*
  - *Up to 100K/hour*
- *Concurrent Interactive sessions*
  - *Up to 10K*
- *Event rotation*
  - *1 per month*
- *Process rotation*
  - *1 per month*

Note: These are maximum values for the 100K system with the above keep-alive.

➢ *Mid performance system hardware requirements:*

HPE ProLiant DL380 Gen10 4110 1P 32GB-R P408i-a 8SFF 1x500W PS

Component	*Description*
Form Factor	2U Rack Server
Dimensions	17.54 x 28.75 x 3.44 in
Processor	Intel® Xeon® Scalable 4110 (8 core, 2.1 GHz, 11.00 MB, 85W)
Memory	HPE 32GB (2x16GB) Dual Rank x8 DDR4-2666
Storage Controller	1 HPE Smart Array S100i and 1 HPE Smart Array P408i-a SR Gen10 controller
Hard Drives	HPE 600GB SAS 12G Enterprise 10K SFF
Power Supply:	HPE 500W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit
ILO	Advanced

For more details follow this link: DL380G10 ***[868703-B21]***

HP ProLiant DL380 Gen9 E5-2620v3 1P 32GB-R P440ar 8SFF 500W PS Base Server

Component	*Description*
Form Factor	2U Rack Server
Dimensions	17.54 x 26.75 x 3.44 in
Processor	Intel® Xeon® E5-2620 v3 (6 core, 2.4 GHz, 15MB, 85W)
Memory	32GB (2x16GB) RDIMM
Storage Controller	Dynamic Smart Array B140i & Smart Array P440ar/2GB FBWC
Hard Drives	8 SFF Chassis, 440ar/2GB SAS controller
Power Supply:	500W Flex Slot Platinum hot plug power supply kit
ILO	Advanced

more details: DL380G9 ***[752687-B2]***

➢ *Mid performance systems load benchmarking:*

Mid performance system solution handles simultaneously:

- *Monitor and Manage up to 50K panels*
  - *PowerMaster and/or*
  - *PowerSeries Neo/PRO panels*
- *PowerMaster keep-alive*
  - *GPRS = 600sec,*
  - *Broadband = 5sec.*
- *PowerSeries Neo/Pro keep-alive*
  - *GPRS/Broadband = 135sec.*
- *Events/Alarms*
  - *Handling 50 events/sec*
- *Visual Verification*
  - *Support 5 events/sec*
- *Concurrent FW upgrade*
  - *Up to 1K/hour*
- *Concurrent Remote Inspection*
  - *Up to 1K/hour*
- *Concurrent CSV report*
  - *Up to 50K/hour*
- *Concurrent Interactive sessions*
  - *Up to 5K*
- *Event rotation*
  - *1 per 2 weeks*
- *Process rotation*
  - *1 per 2 weeks*

Note: These are maximum values for the 50K system with the above keep-alive.

➢ *Low cost systems:*

Dell OptiPlex 3060 - Intel Core i5-8500

Component	*Description*
Dimensions	Small form factor
Processor	Intel Core i5-8500 (6 Cores/9MB/6T/up to 4.1GHz/65W)
Memory	8GB 1X8GB DDR4 2666MHz UDIMM Non-ECC
Hard Drives	3.5” 500GB 7200rpm SATA

Dell OptiPlex 3050 - Core i5 7500 3.4 GHz - 16 GB

Component	*Description*
Dimensions	15.4x27.4x35 [HxWxD, cm]
Processor	Intel Core i5-7500 (QC/6MB/4T/3.4GHz/65W)
Memory	32 GB (max) - DDR4 SDRAM
Hard Drives	1 x 500 GB - SATA

➢ *Low cost systems load benchmarking:*

Low cost system solution handles simultaneously:

- *Monitor and Manage up to 10K panels*
  - *PowerMaster and/or*
  - *PowerSeries Neo/PRO panels*
- *PowerMaster keep-alive*
  - *GPRS = 600sec,*
  - *Broadband = 5sec.*
- *PowerSeries Neo/Pro keep-alive*
  - *GPRS/Broadband = 135sec.*
- *Events/Alarms*
  - *Handling 10 events/sec*
- *Visual Verification*
  - *Support 1 events/sec*
- *Concurrent FW upgrade*
  - *Up to 1K/hour*
- *Concurrent Remote Inspection*
  - *Up to 1K/hour*
- *Concurrent CSV report*
  - *Up to 10K/hour*
- *Concurrent Interactive sessions*
  - *Up to 1K*
- *Event rotation*
  - *1 per week*
- *Process rotation*
  - *1 per week*

Note: These are maximum values for the 10K system with the above keep-alive.

➢ *Virtual environment hardware support:*

Minimum hardware requirements for vSphere client installation

Component	Description
CPU	1 CPU
Processor	Intel or AMD processor with two or more logical cores 2GHz each.
Memory	4 GB RAM
Hard Drives	1 x 500 GB - SATA

➢ *Legacy hardware support:*

HP ProLiant DL360p G8 High Performance Server [646904-001]

Component	Description
Form Factor	1U Rack Server
Dimensions	4.32 x 42.62 x 69.22 [HxWxD, cm]
Processor	(2) Intel Xeon E5-2650 (8 core, 2 GHz, 20 Mb, 95W)
Memory	32GB (4 x 8GB) Registered DIMMs PC3-12800R (1600MHz)
Storage Controller	Smart Array P420i/1GB FBWC (RAID 0/1/1+0/5/5+0/6/6+0)
Hard Drives	HP 2 x 600 GB SAS 10k 2,5” SFF
Power Supply	(2) HP 750W CS Platinum Plus Hot Plug Power Supplies
ILO	Advanced

more details: DL360G8

HP ProLiant DL360p G8 Server [670634-S01]

Component	Description

Form Factor	1U Rack Server
Dimensions	4.32 x 42.62 x 69.22 [HxWxD, cm]
Processor	(2) Intel Xeon E5-2640 (6 core, 2.5 GHz, 15Mb, 95W)
Memory	16GB (2 x 8GB DDR3-1333MHz Low Voltage RDIMMs)
Storage Controller	Smart Array P420i/1GB FBWC (RAID 0/1/1+0/5/5+0)
Hard Drives	HP 2 x 600 GB SAS 10k 2,5” SFF
Power Supply	(2) HP 460W CS Platinum Plus Hot Plug Redundant Power Supplies
ILO	Advanced

more details: DL360G8

Dell OptiPlex 3040 - Core i5 6500 3.2 GHz - 16 GB

Component	*Description*
Dimensions	15.4x27.4x35 [HxWxD, cm]
Processor	1 x Intel Core i5 (6th Gen) 6500 / 3.2 GHz (3.6 GHz) (Quad-Core)
Memory	16 GB (max) - DDR3L SDRAM - non-ECC
Hard Drives	1 x 500 GB - SATA

Network & Firewall requirements

PowerManage IV can be deployed in a variety of network configurations. However, a hardware or software firewall and/or NAT between the PowerManage server and the Internet is a must. The firewall should be configured using default-deny policy, allowing only the services listed below.

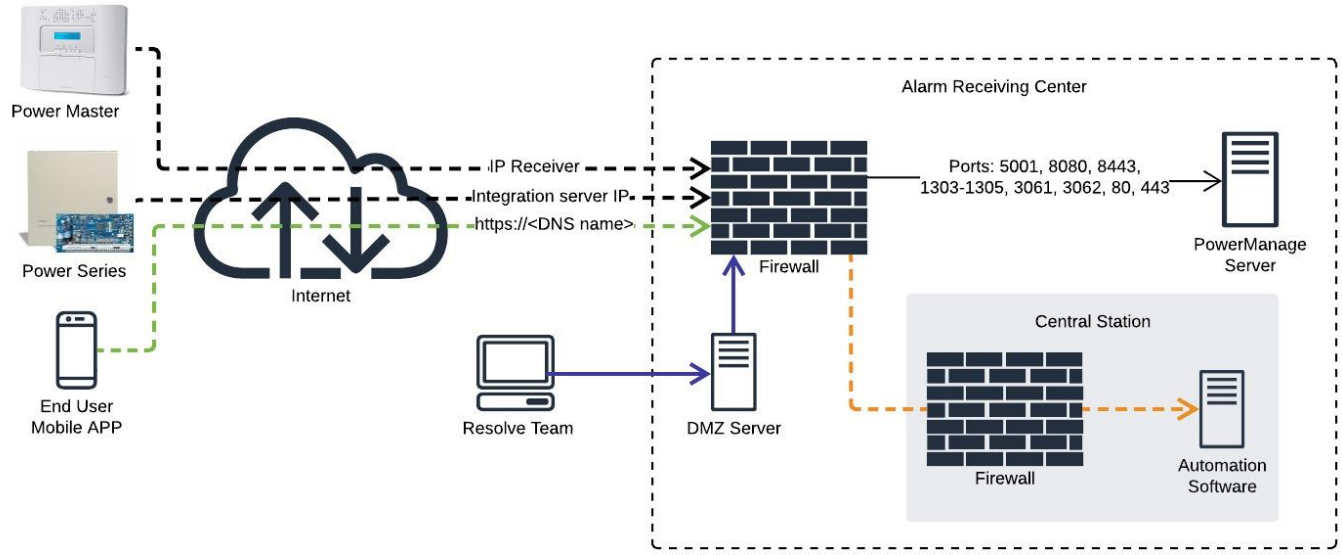
8443	TCP/UDP	Alarm images [secured]
5555	TCP/UDP	Offline handler [in case of GEO only]
NEO Panels ports		
3061-3062	TCP	Fibro Alarms
1303-1304	TCP	ITv2 Alarms/Resolve
1305	TCP	DLS Resolve
Web interface		
80	HTTP	Resolve Web interface
443	HTTPS	Resolve Web interface SSL
2200	HTTPS	Web MMI console
8087	HTTPS	Web Interactive
REST API		
443	HTTPS	REST API requests with SSL
Administrating		
22	TCP	SSH
161	SNMP	Nagios or other platforms
162	SNMP	Nagios or other platforms
Extended support [iLO]		
443	HTTPS	iLO Web interface
17990	TCP/UDP	iLO
17988	TCP/UDP	iLO
Messaging		
25	SMTP	Email or Email relay
465/587	SMTP	Email or Email relay

Rack & Power outlet

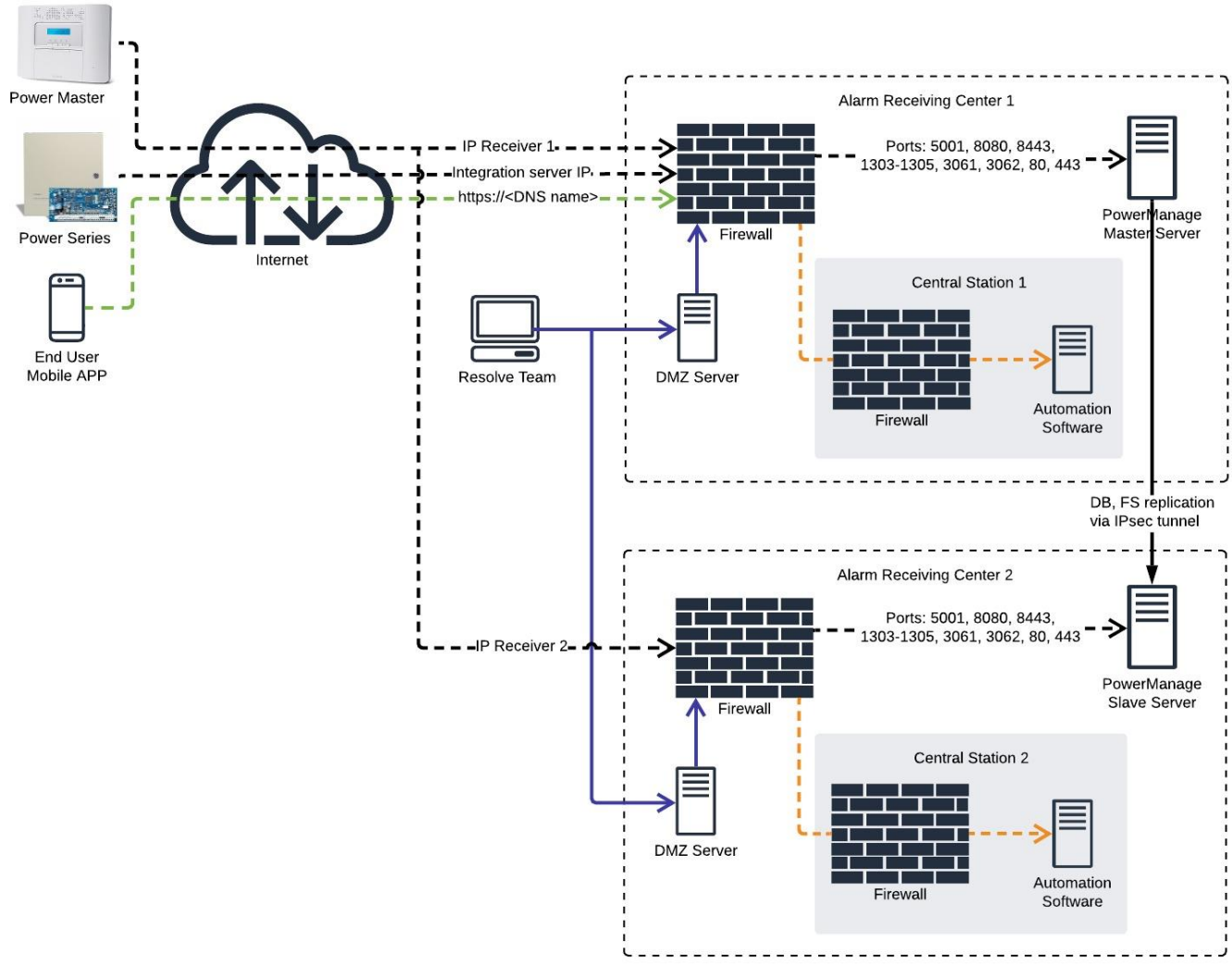
Make sure you have enough room in your designated server rack for a 2U sized server and at least one free power outlet. A second power outlet is recommended as the server has two redundant power supplies. More outlets may be required according to the server configuration that is explained in this document.

Network schematics

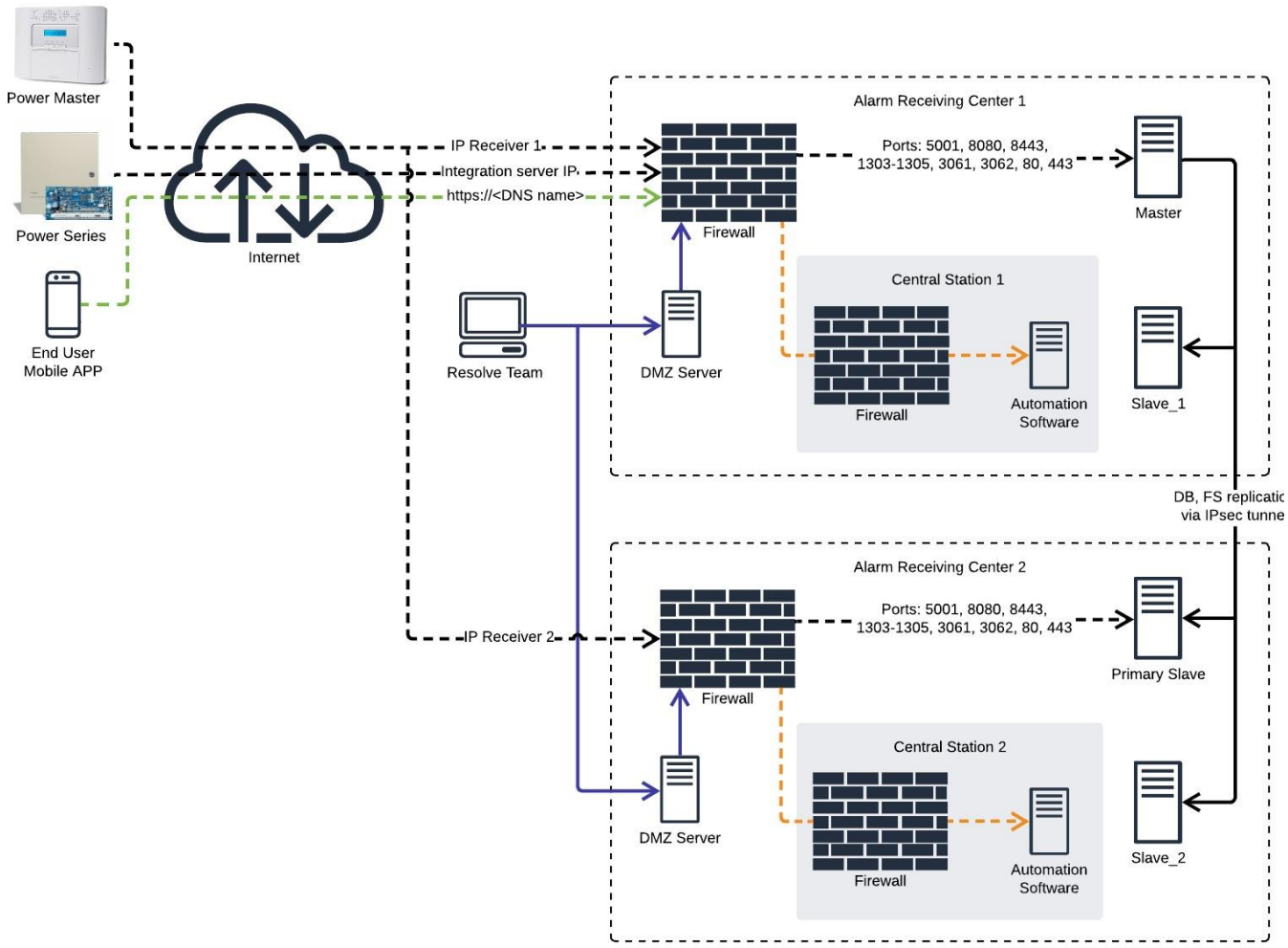
- ***Cost Effective - standalone diagram***



❑ *Hot Backup - two nodes multisites diagram*



❑ *Carrier Grade - 4 nodes multisites diagram*



Software Requirements

❑ *HP Lights-Out Management System*

The HP iLO (Integrated Lights-out) management system provides a better type of access and control of the server from a remote machine making server administration and support easier and more reliable. For more details about iLO:
http://h18013.www1.hp.com/products/servers/management/remotemgmt.html?jumpid=servers/lights-out

The iLO interface uses a separate Ethernet port and thus it needs a separate IP address.

❑ *Client machine requirements. Used for Web and MMI interface access*

Suggested minimum hardware requirements:

- ➢ Processor :Intel or AMD processor with two or more logical cores, each with a speed of 2+GHz
- ➢ Memory: 8GB RAM
- ➢ Networking: 1Gbit Ethernet connectivity

Suggested minimum software requirements:

- ➢ Operating system:
  - ○ Windows 10, Windows 7, Windows Vista, Windows XP, etc
  - ○ Red Hat Linux, Ubuntu Linux, Fedora, etc.
  - ○ Mac OS

- ➢ Browsers:
  - ○ Google Chrome 56+
  - ○ Mozilla Firefox 50+
  - ○ Safari 10+

- ➢ SSH clients
  - ○ PuTTY
  - ○ openssh-client
  - ○ SSH client on MAC

Installation guide

❑ *During the installation process*

A local network engineer/administrator must be available at the time of installation.

In most cases, the following equipment will be on site during the installation:

- ➢ USB keyboard
- ➢ Console or Monitor
- ➢ Security panels for testing
- ➢ Mobile device for testing

❑ *Preparing boot media*

The latest Power Manage versions are installed from the ISO image file. Several media types are available. Choose the one that best suits your requirements.

❖ DVD image

DVD images boot directly into the installation environment.

You can make an installation DVD using the disc burning software on your computer. Make sure that your disc burning software is capable of burning discs from image files.

Burning installation DVD is the same for Windows and Linux systems. The only thing is needed is any burning tool like Nero, ImgBurn, Roxio Creator, Brasero or K3b.

To burn an image file to DVD:

- ➢ Insert a blank, writable DVD disc into your computer's disc burner
- ➢ Launch your disc burning program.
- ➢ In your disc burning program, select the option to burn a DVD from an image file
- ➢ Browse to the ISO image file that you downloaded previously and select it for burning
- ➢ Click the button that starts the burning process

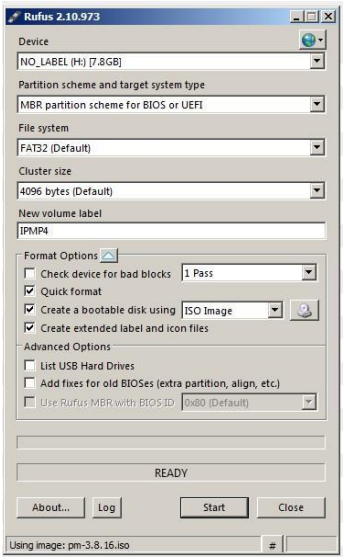
❖ USB image

Several software utilities are available for Windows and Linux that can write image files to a device.

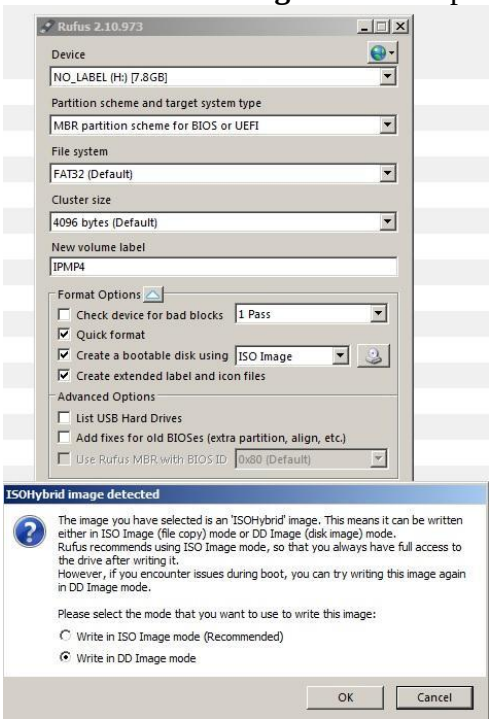
❑ *On Windows:*

To create bootable USB under Windows:

- ➢ Download and launch **Rufus**



- ➢ In Device field select your USB drive
- ➢ In New volume label set the volume name
- ➢ In Format Options set Create a bootable disk using ISO Image and select the location of the image
- ➢ Press start to proceed
- ➢ In appeared dialog select **Write in DD Image mode** and press OK



❑ *On Linux:*

Linux includes the **dd** command for this purpose. The dd utility requires you to specify the device file

that corresponds to the physical media. The name of the device file matches the name assigned to the device by your system. All device files appear in the directory /dev/.

To write an image file to boot media with dd:

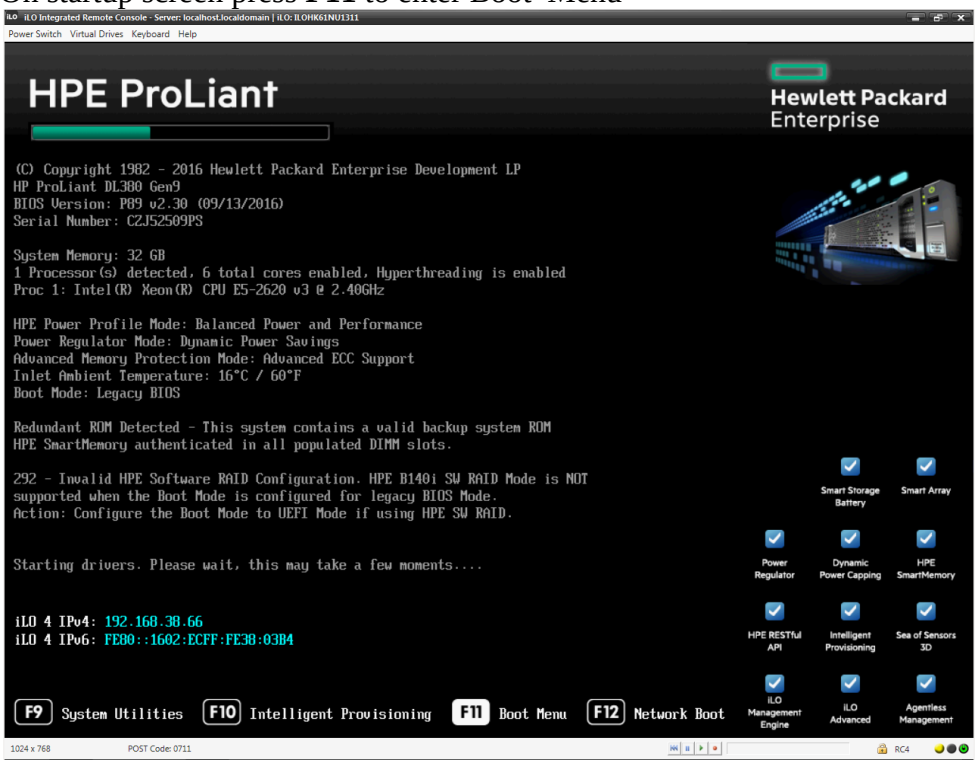
- Attach or insert the USB media
- Open new terminal [all the following might be allowed under sudo user only
- In terminal type the following command: **fdisk -l** to locate your USB device
- Switch to the directory with Power Manage ISO image
- Type the following command: **dd bs=1M if=<image.iso> of=/dev/<device> status=progress**
  Replace <image.iso> with name of the Power Manage IV ISO image, <device> with the name of the current device file for the media

❑ *Booting the installation*

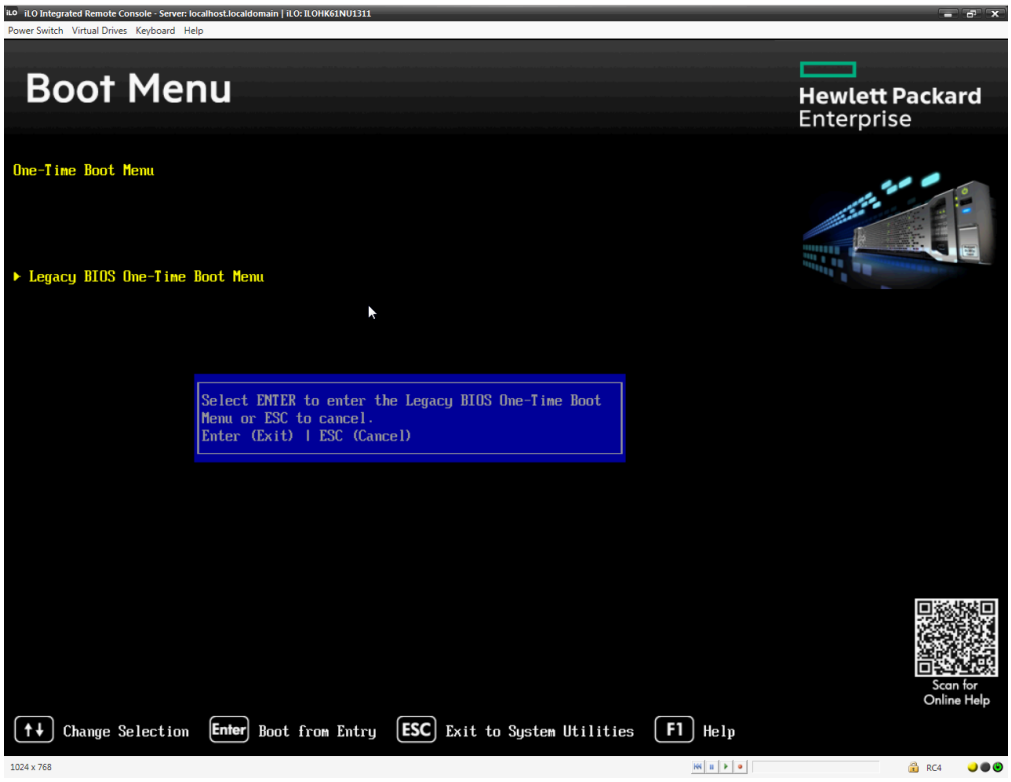
After you have made a bootable USB flash drive or DVD using the steps described in Preparing Boot Media, you are ready to boot the installation

❑ *Power Manage installation on HP equipment*

- Power On HP server.
- Plug in the boot USB drive or insert the boot DVD into your optical disc drive
- Restart the system
- On startup screen press **F11** to enter Boot Menu

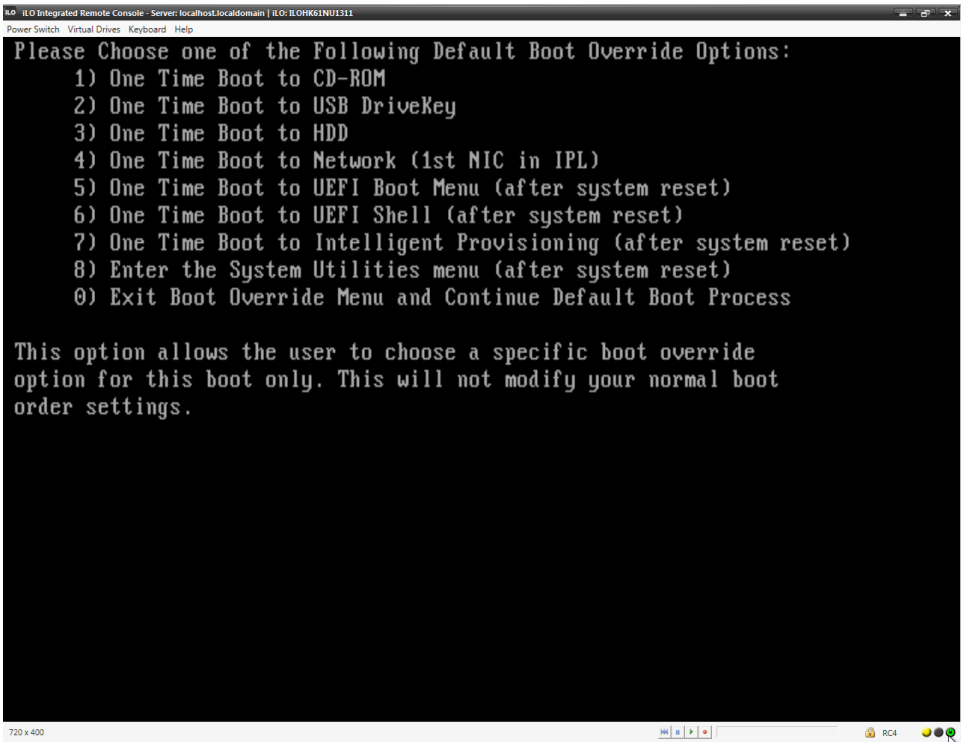


- Select Legacy BIOS One-Time Boot Menu and press Enter
- When dialog appears press Enter.



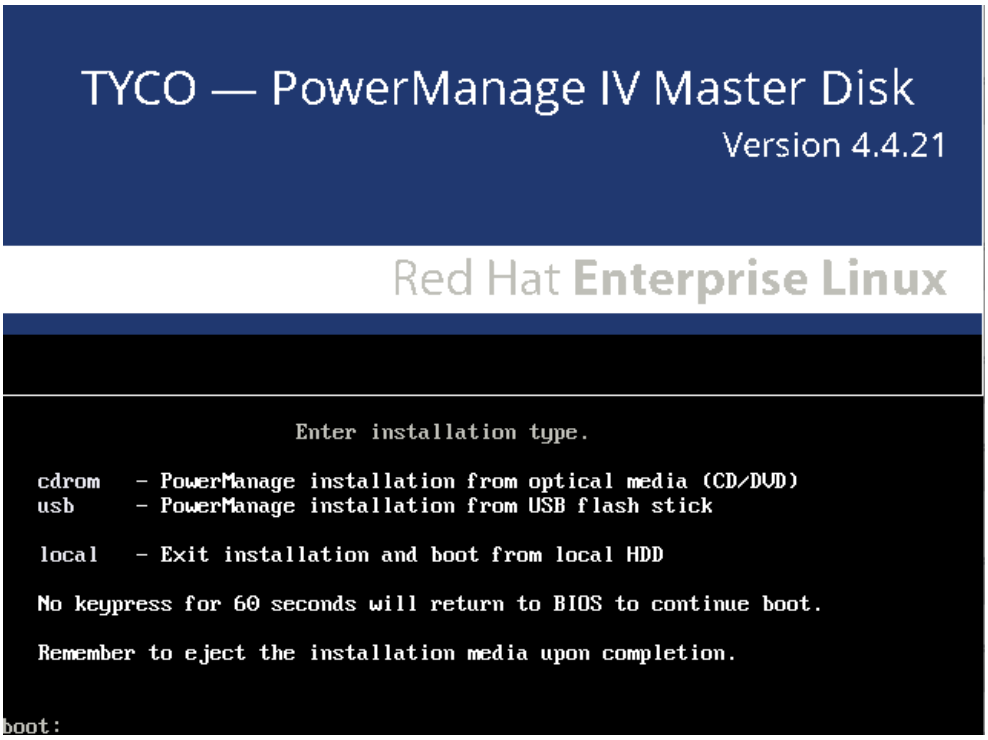
➢ Dependant on installation media DVD/USB select from the list of the options:

- **One Time Boot to CD-ROM**;
- **One Time Boot to USB DriveKey.**



From USB media - choice USB DriveKey, From DVD - choice CD-ROM

➢ Wait until installation starts and type the boot option:
- **usb** - in case of USB installation
- **cdrom** - in case of DVD installation

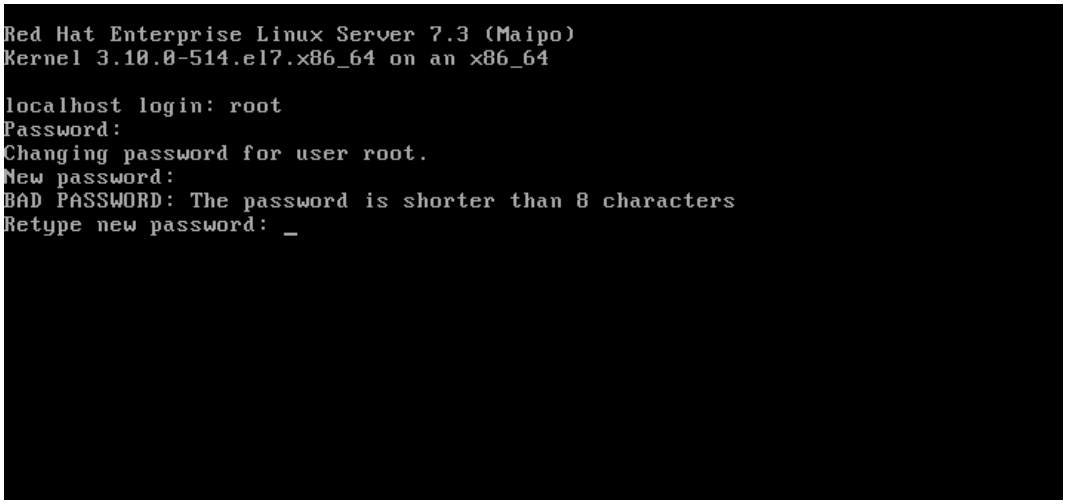


From USB media - choice usb, From DVD media - choice cdrom

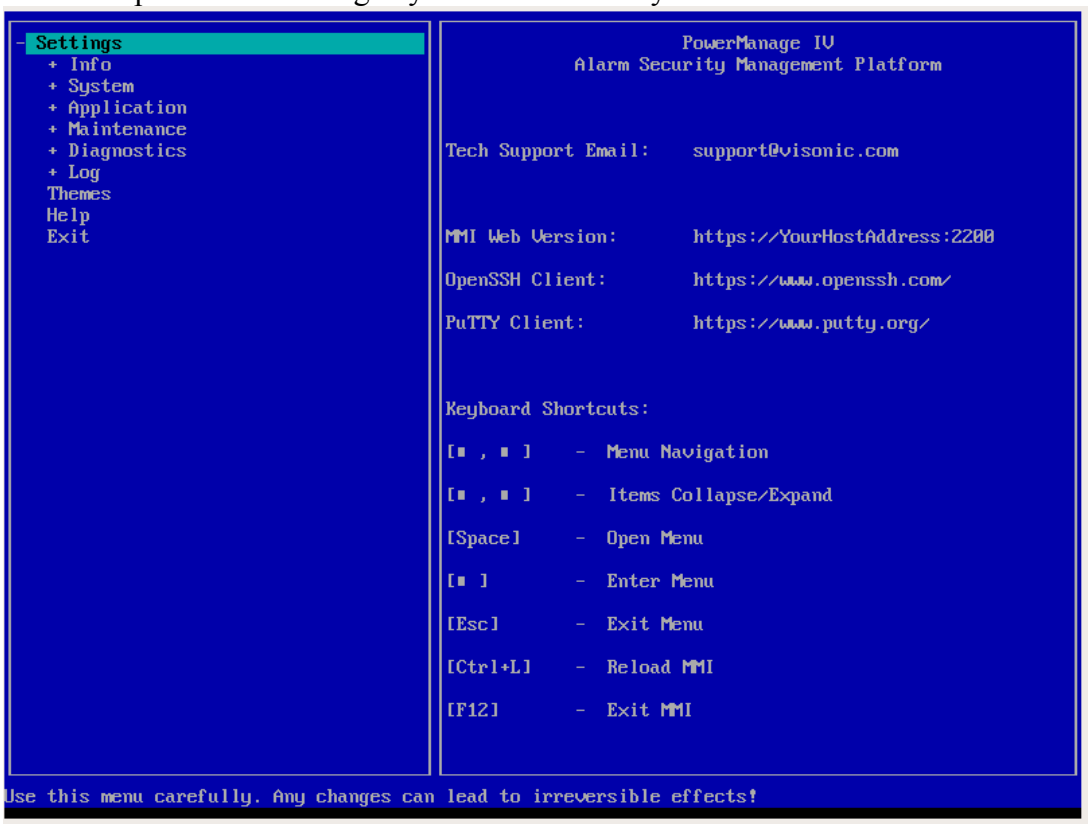
➢ Wait until the installation is completed.
➢ Once installation is completed, server restarts and appears a screen that prompts you to login [login - **root,** password - **visonic.]**
Note: Don't forget to unplug the DVD / USB stack after the reboot process



➢ At this step you are asked to **set a new password** for Unix user root.
Note: Use a combination of letters, numbers, and special characters. The password to include both Uppercase and Lowercase characters.



➢ After password is changed you'll automatically switch to the MMI menu



❑ *Power Manage installation on Dell equipment*

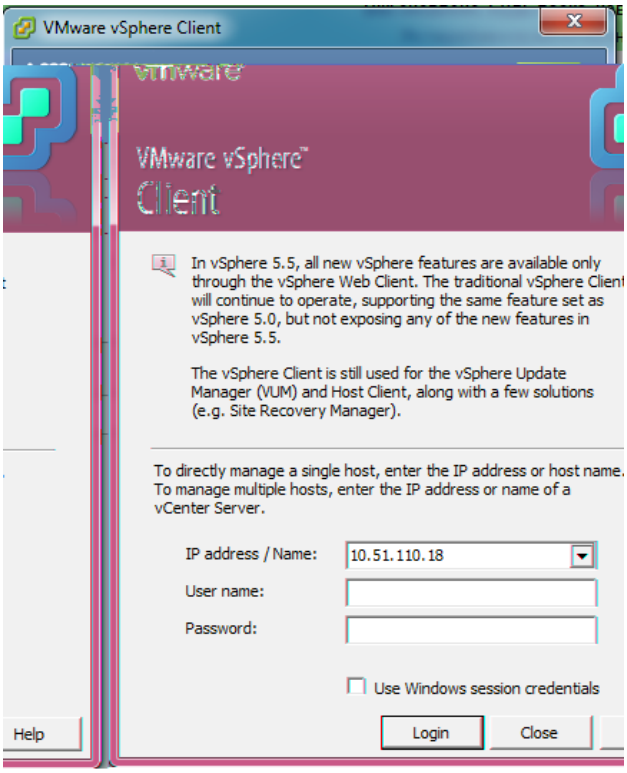
Installation from DVD for Dell equipment is exactly the same as described for HP servers.
USB installation is different. Due to Dells' BIOS configuration peculiar properties two exactly the same USB drivers with the same Power Manage images are needed.

➢ Plug in the boot USB drive or insert the boot DVD into your optical disc drive
➢ Reboot the system
➢ On startup screen press **F12** to enter One-Time Boot menu
➢ Select one time boot option: either USB or CD-ROM
➢ Perform steps 6-11 from the **Installation on HP equipment** instructions

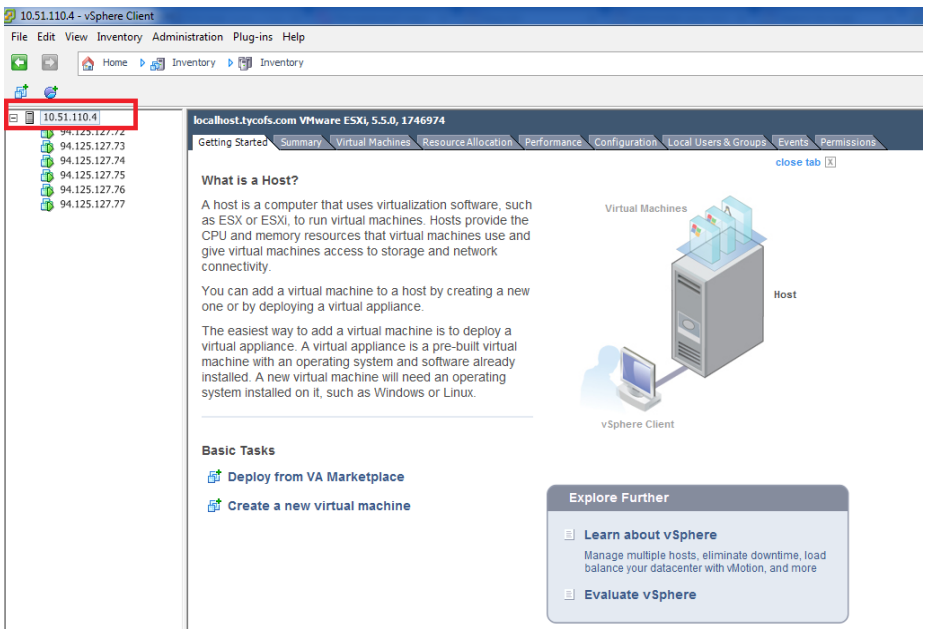
❑ *Power Manage installation on VMWare*

Power Manage installation on VMWare virtual environment requires server with VMWare installed and Power Manage ISO image.

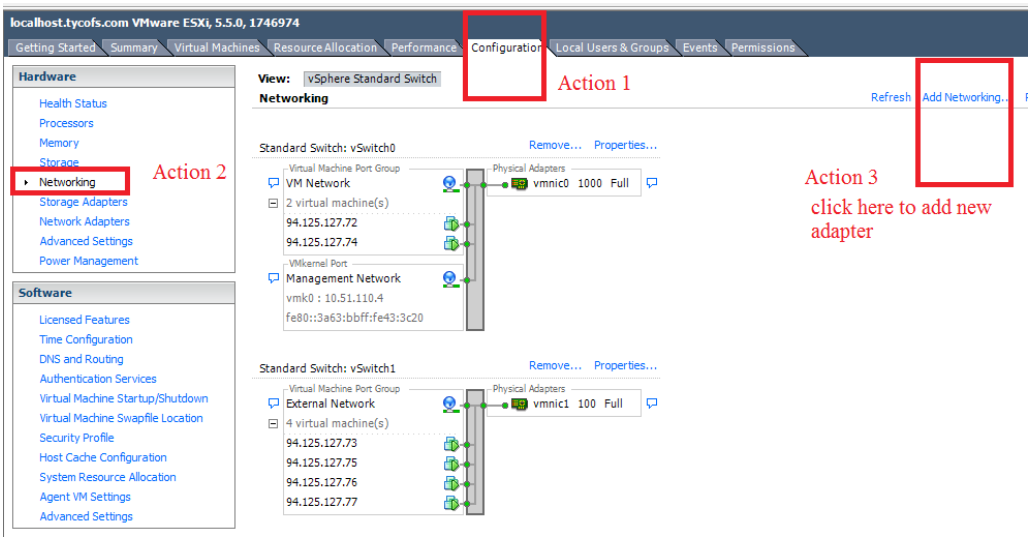
➢ Login to vSphere client



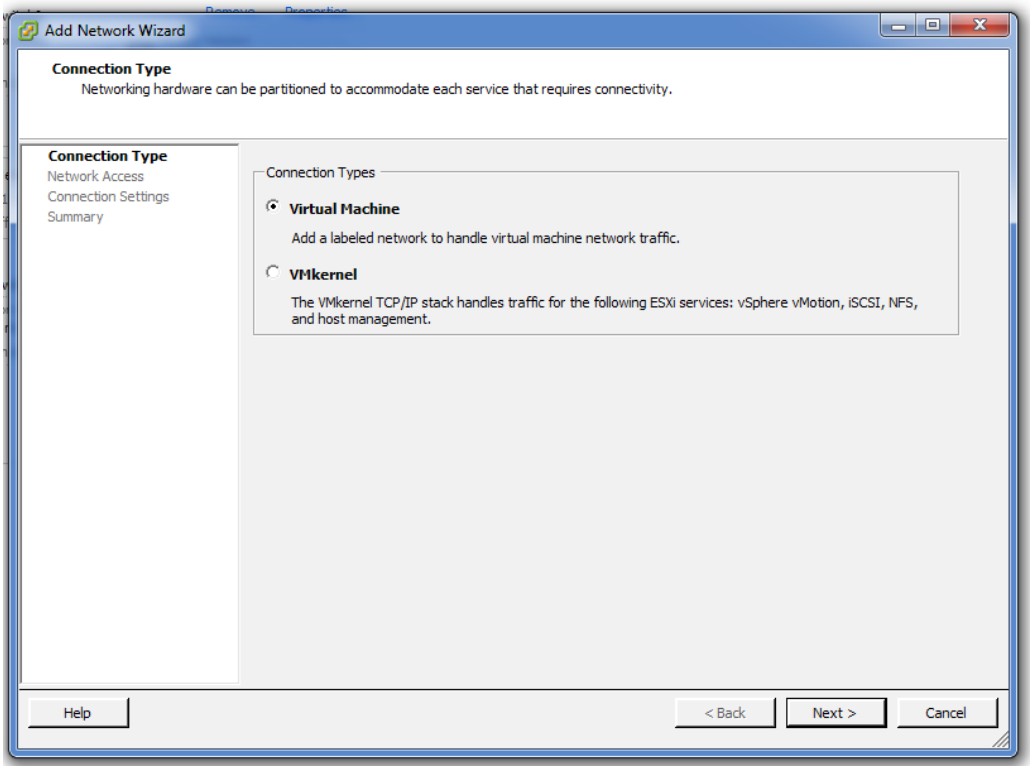
➢ Add new adapter to the virtual machine [should be done once]: click on your virtual host first



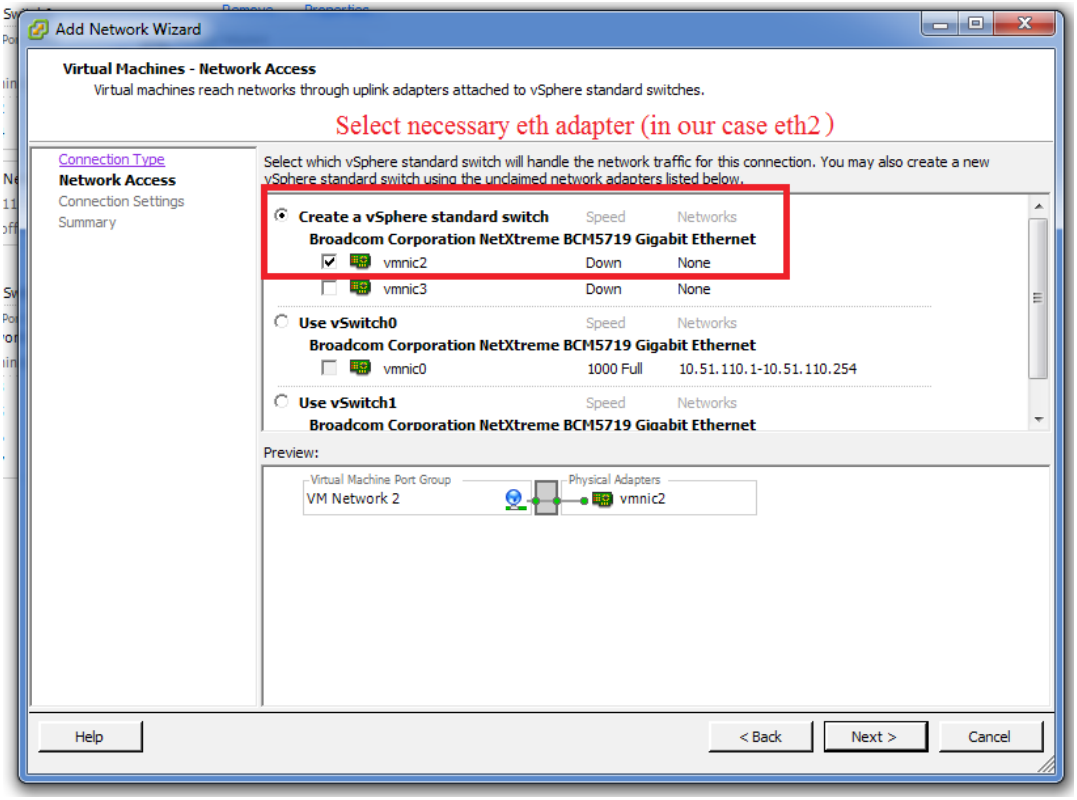
➢ Open ‘Configuration’ tab [Action 1 on the picture below]
➢ In the ‘Hardware’ submenu on the left of the screen select ‘Networking’ menu [Action 2]
➢ Click ‘Add Networking…’ [Action 3]



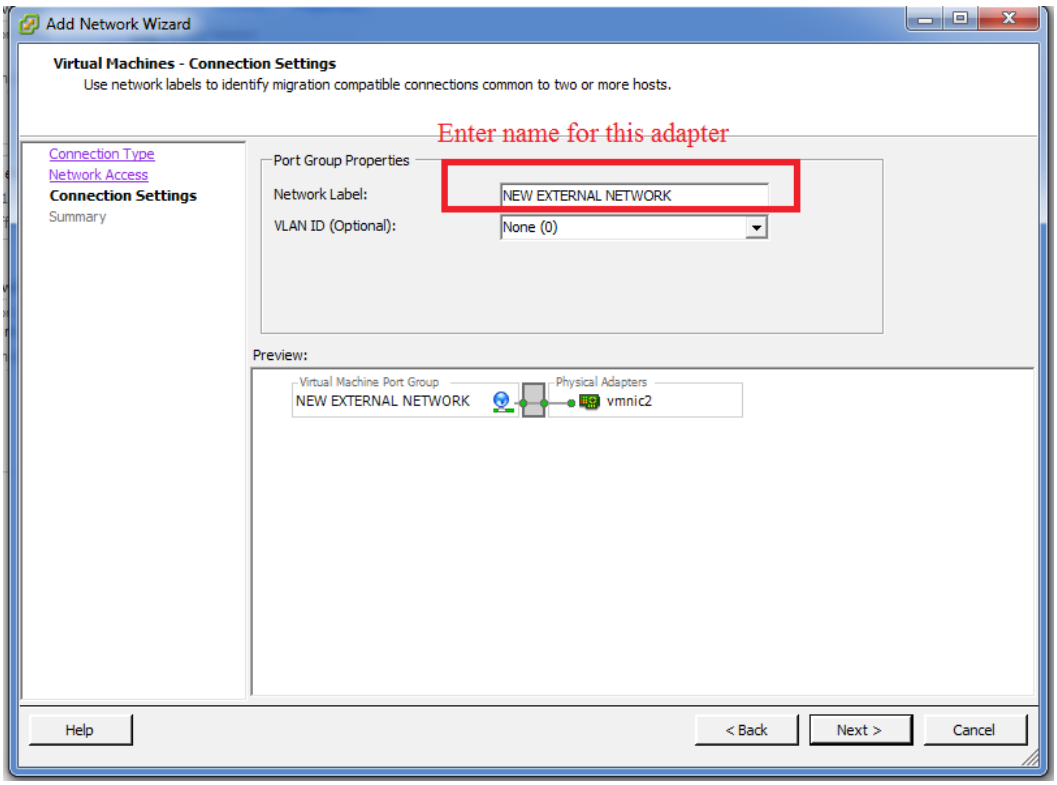
➢ Select ‘Virtual Machine’ connection type and press ‘Next’



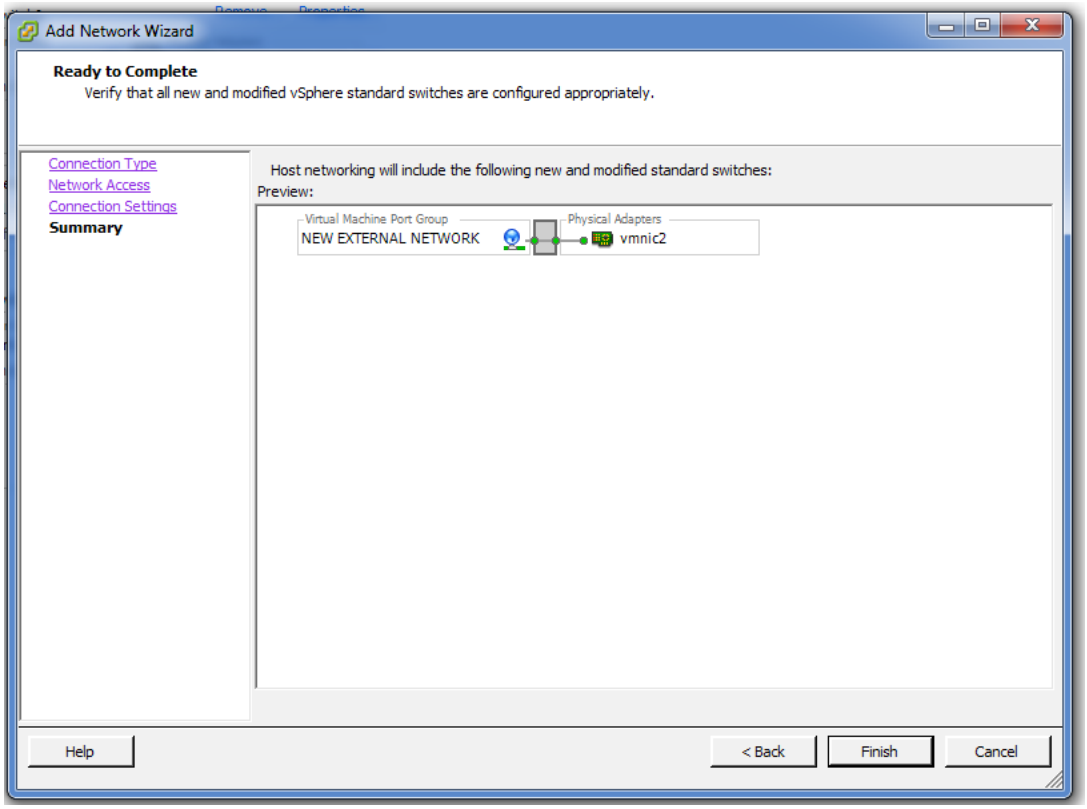
➢ Select necessary Ethernet adapter and press ‘Next’



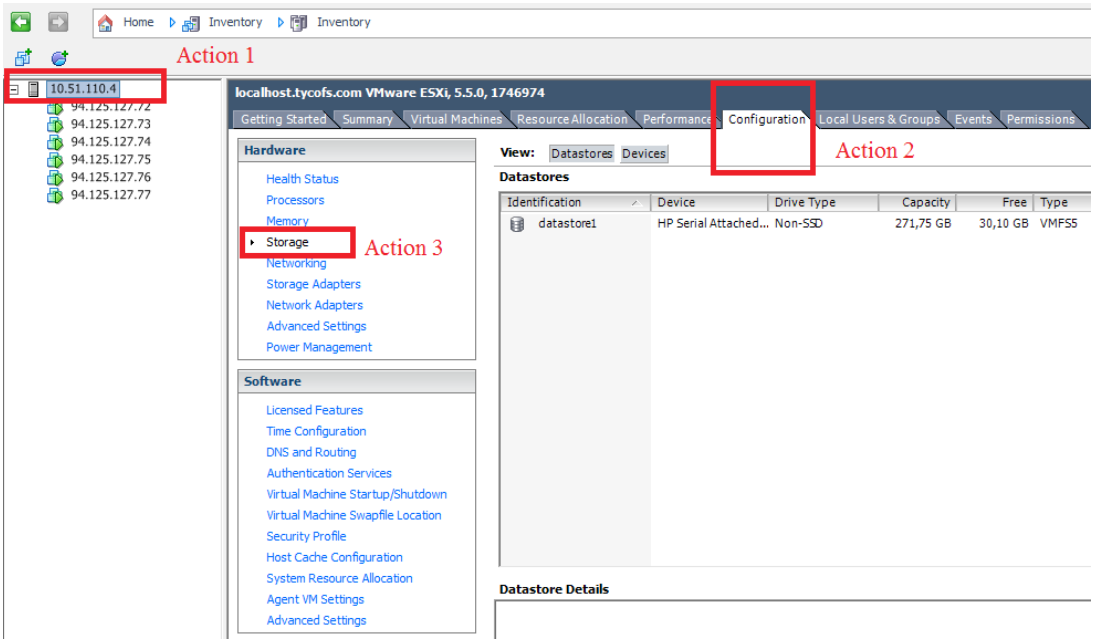
➢ Enter adapter name and press ‘Next’



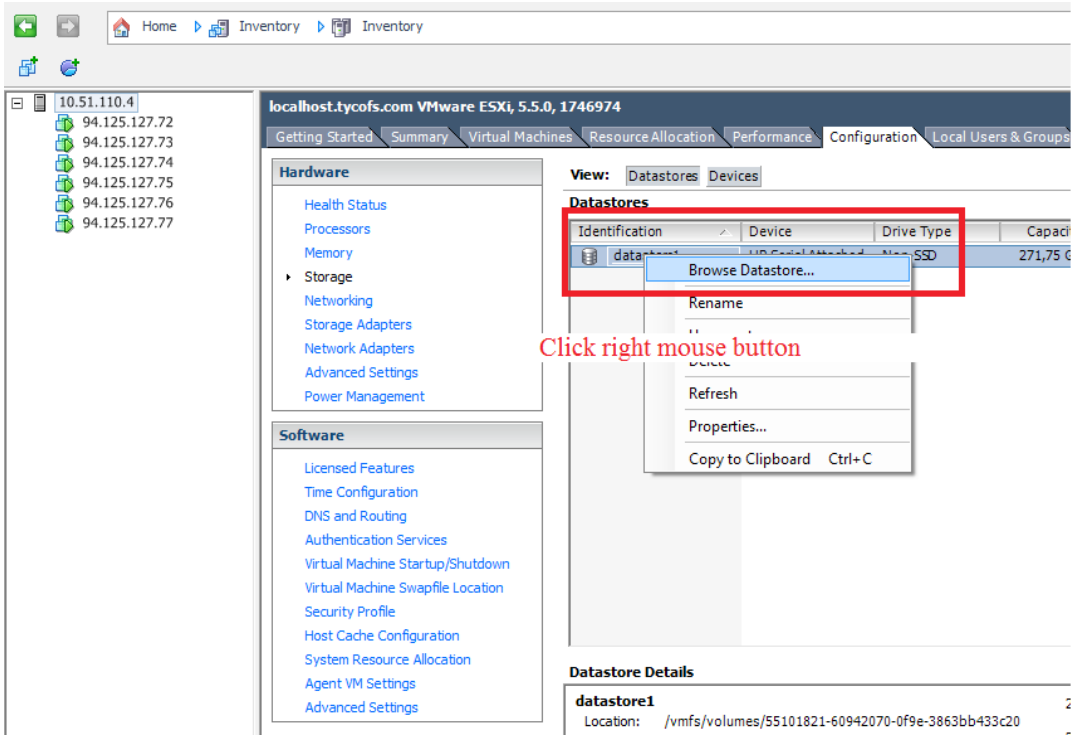
➢ Press ‘Finish’



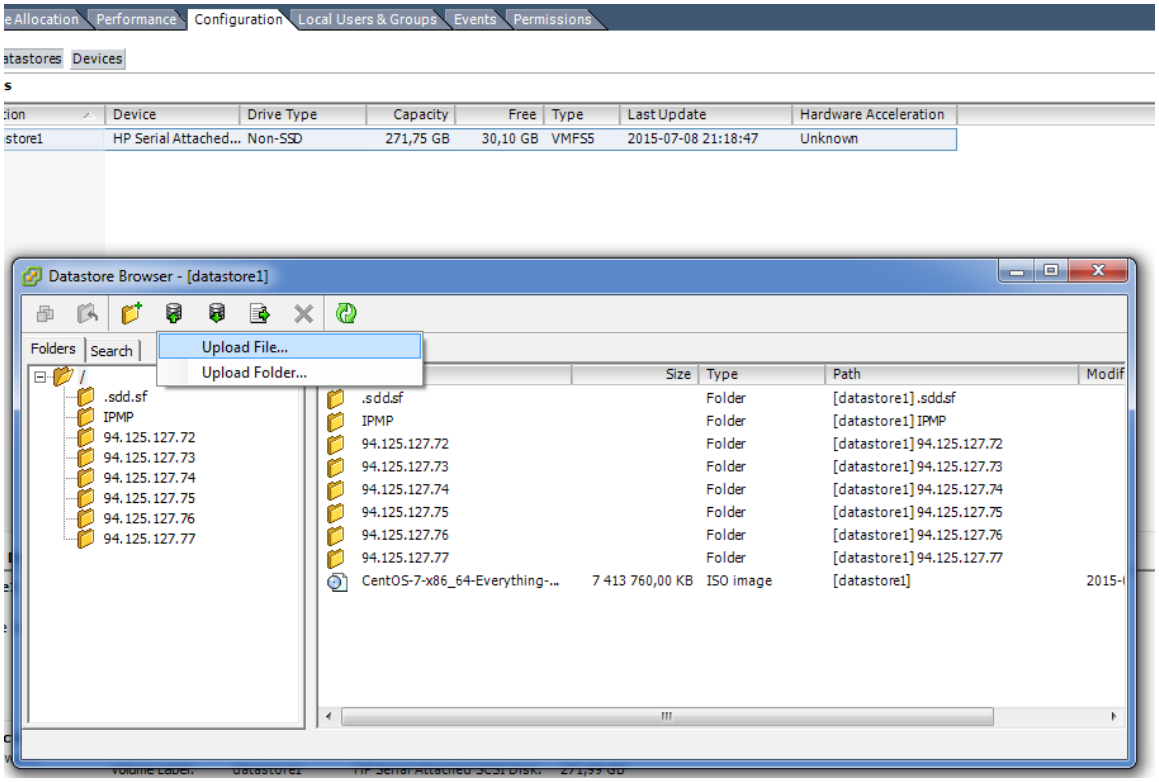
- ➢ Upload Power Manage image file to the VM data store: click on the virtual machine [Action 1 on the picture below]
- ➢ Open 'Configuration' tab [Action 2]
- ➢ In the 'Hardware' submenu on the left of the screen select 'Storage' menu [Action 3]



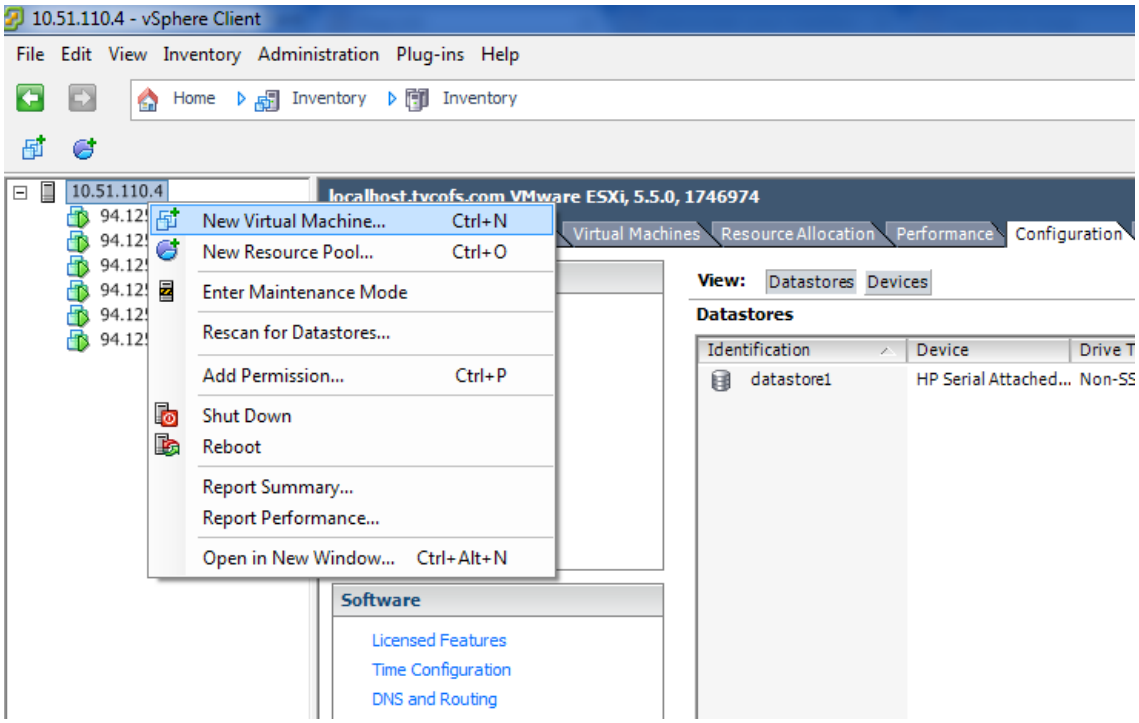
➢ Right click on the data store and select ‘Browse Datastore…’



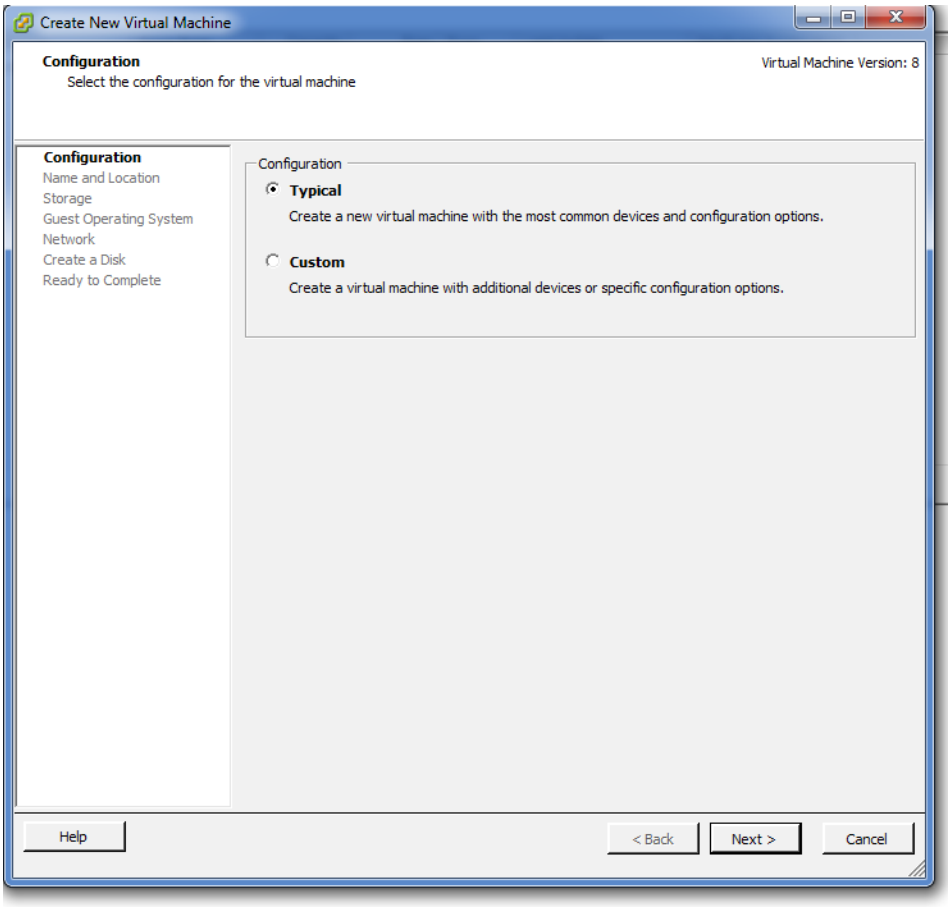
➢ Click ‘Upload files to this storage’ icon, select ‘Upload File…’ and add the file from your workstation



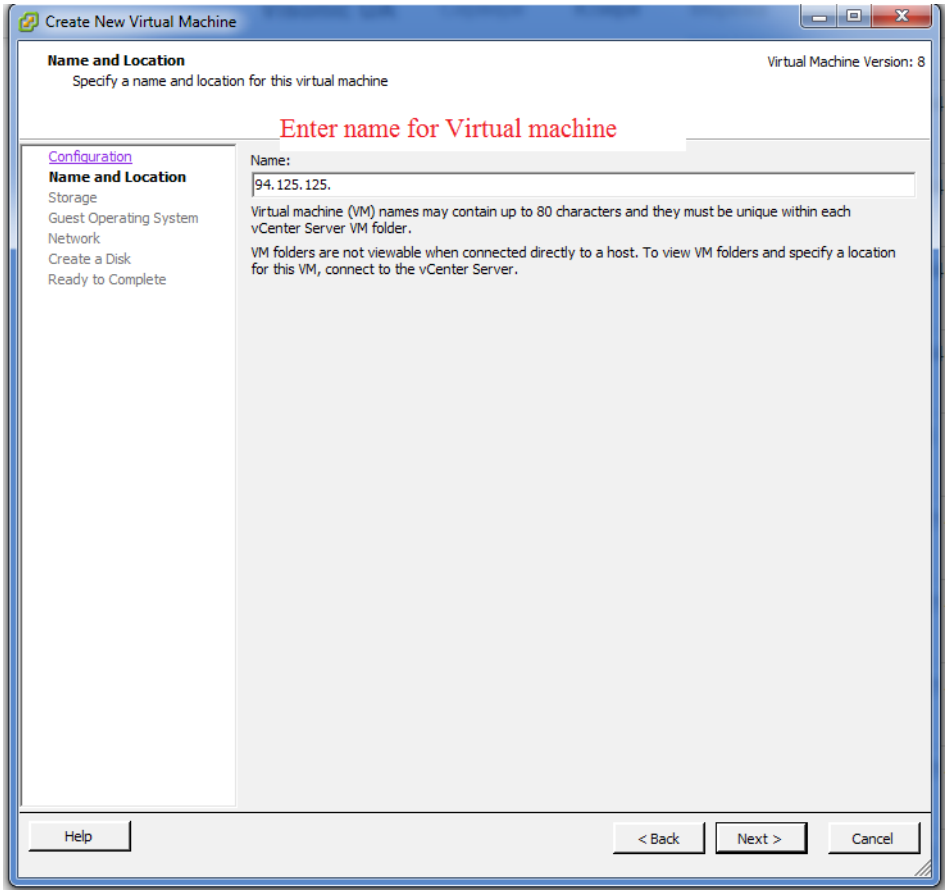
➢ Add new virtual machine: right click on your virtual host and press ‘New Virtual Machine...’



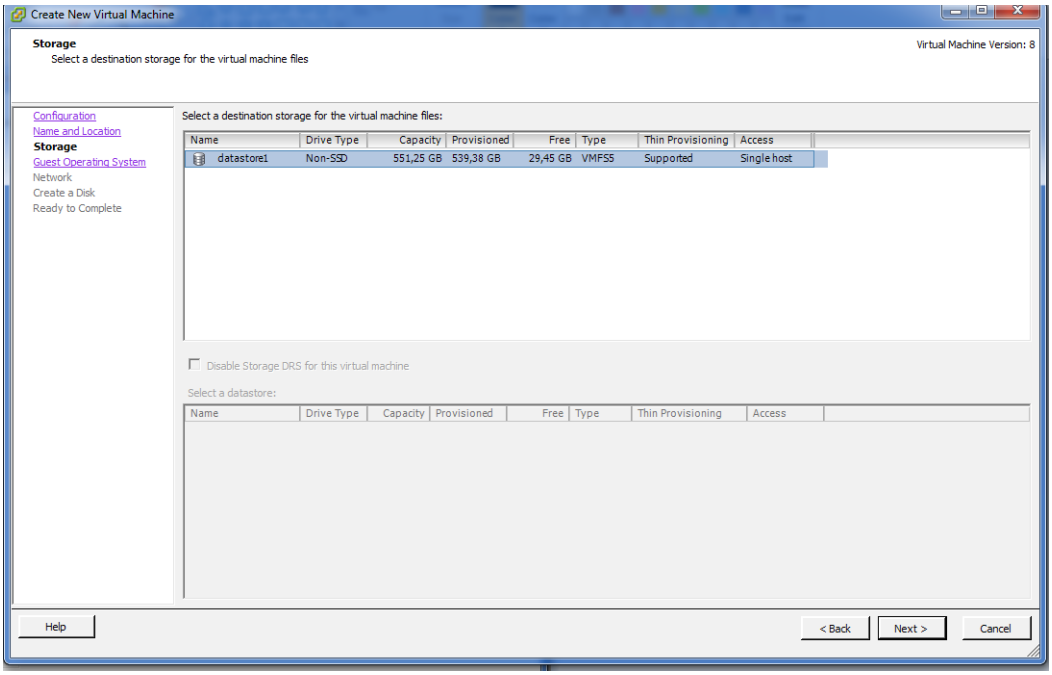
➢ Select ‘Typical’ option in configuration menu, press ‘Next’



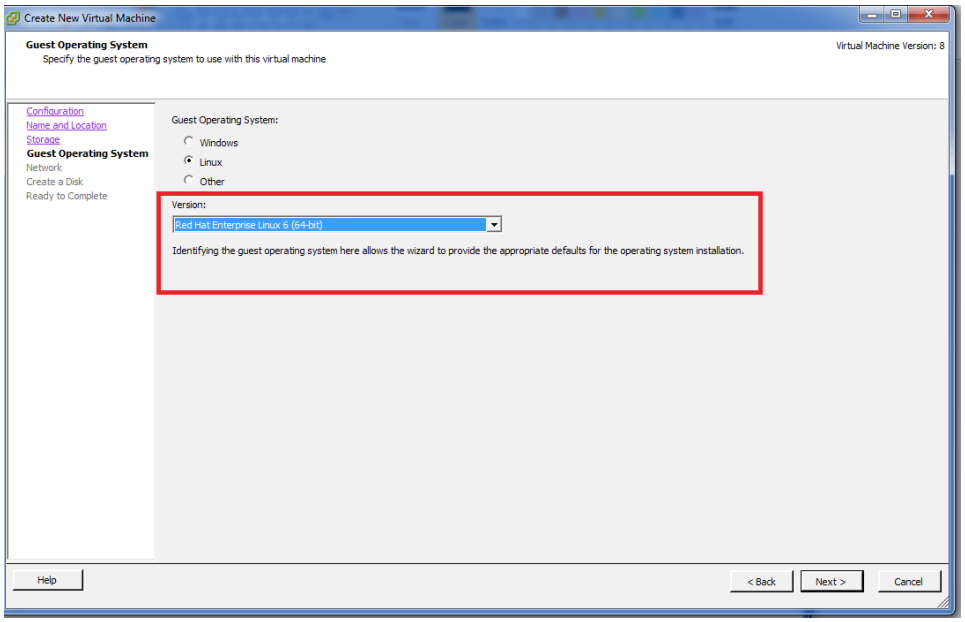
➢ Enter virtual machine name, press ‘Next’



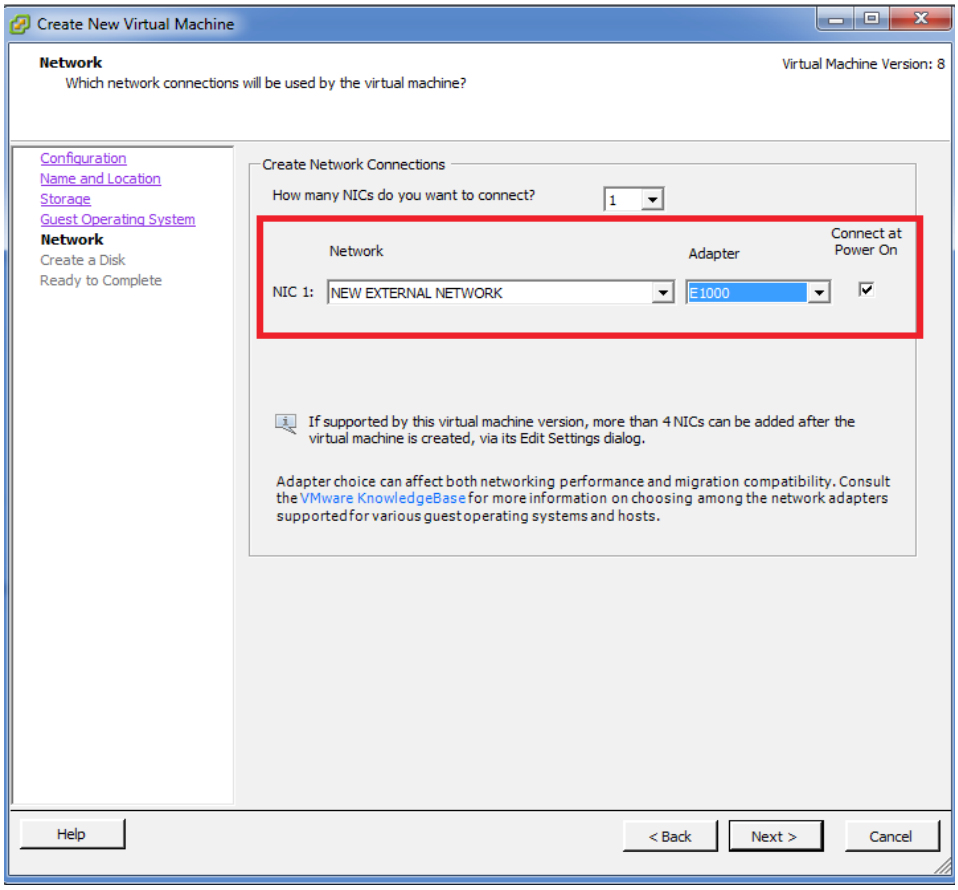
➢ Select a destination data storage for new virtual machine files, press ‘Next’



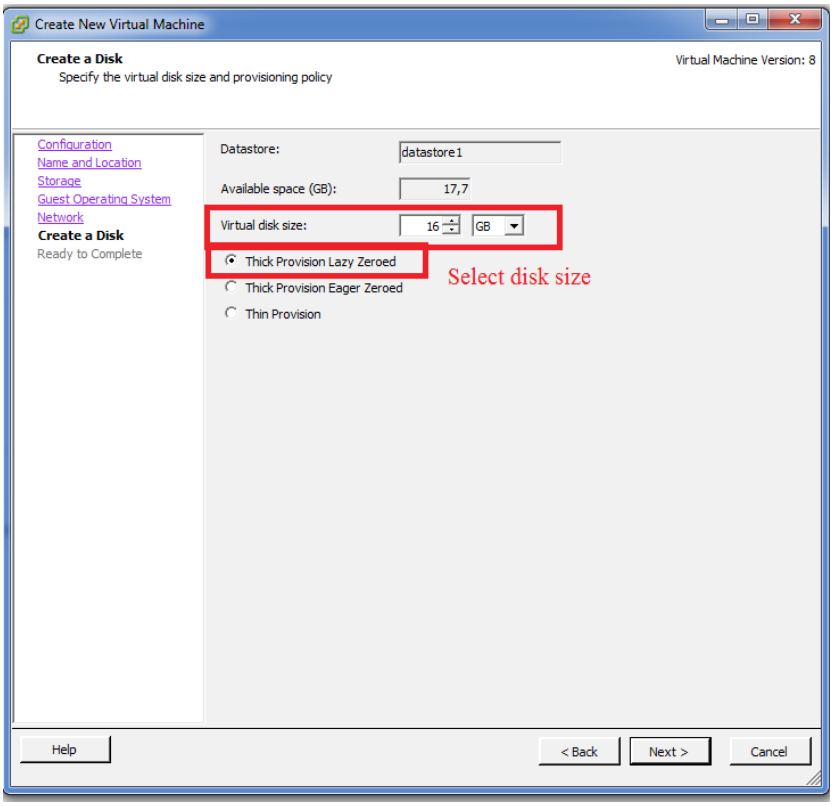
➢ Select Linux Operating System, and set version ‘Red Hat Enterprise Linux 6 (64-bit)’ and press ‘Next’



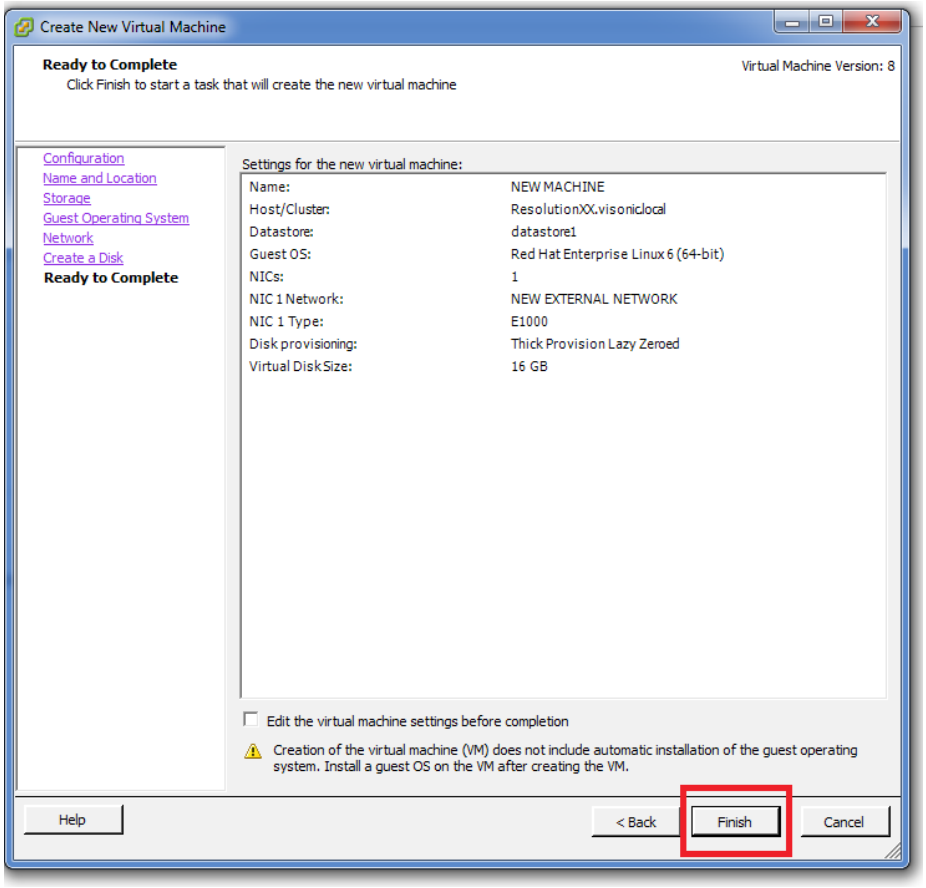
➢ Select Network connection and Adapter to use that you had configured in the beginning of this guide, press ‘Next’



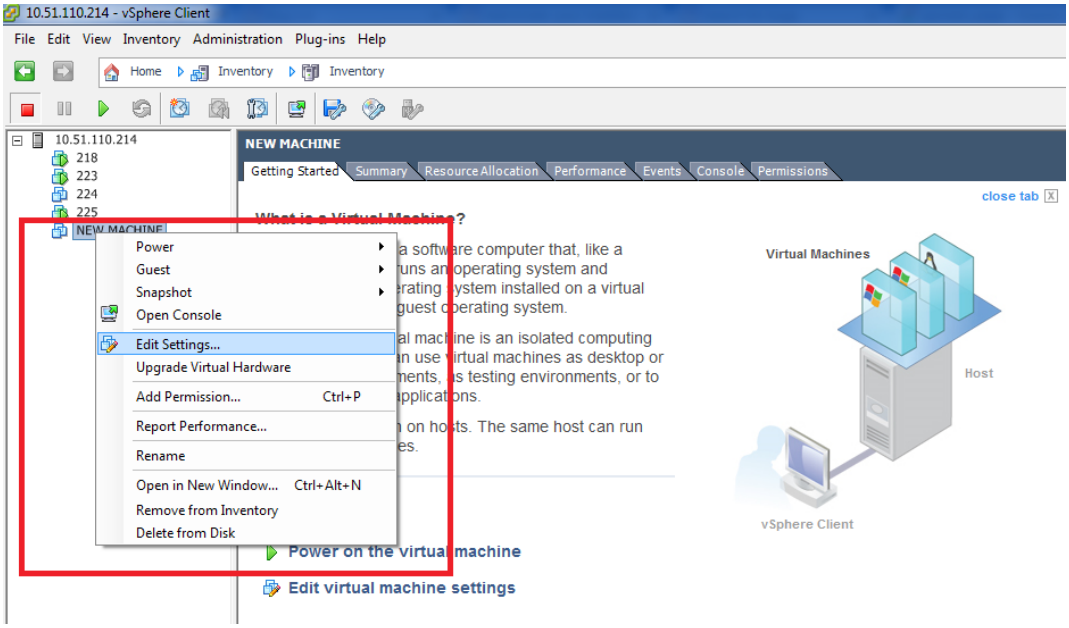
➢ Set virtual disk size: NOT LESS THAN 120 GB, set ‘Thick Provision Lazy Zeroed’ option, press ‘Next’



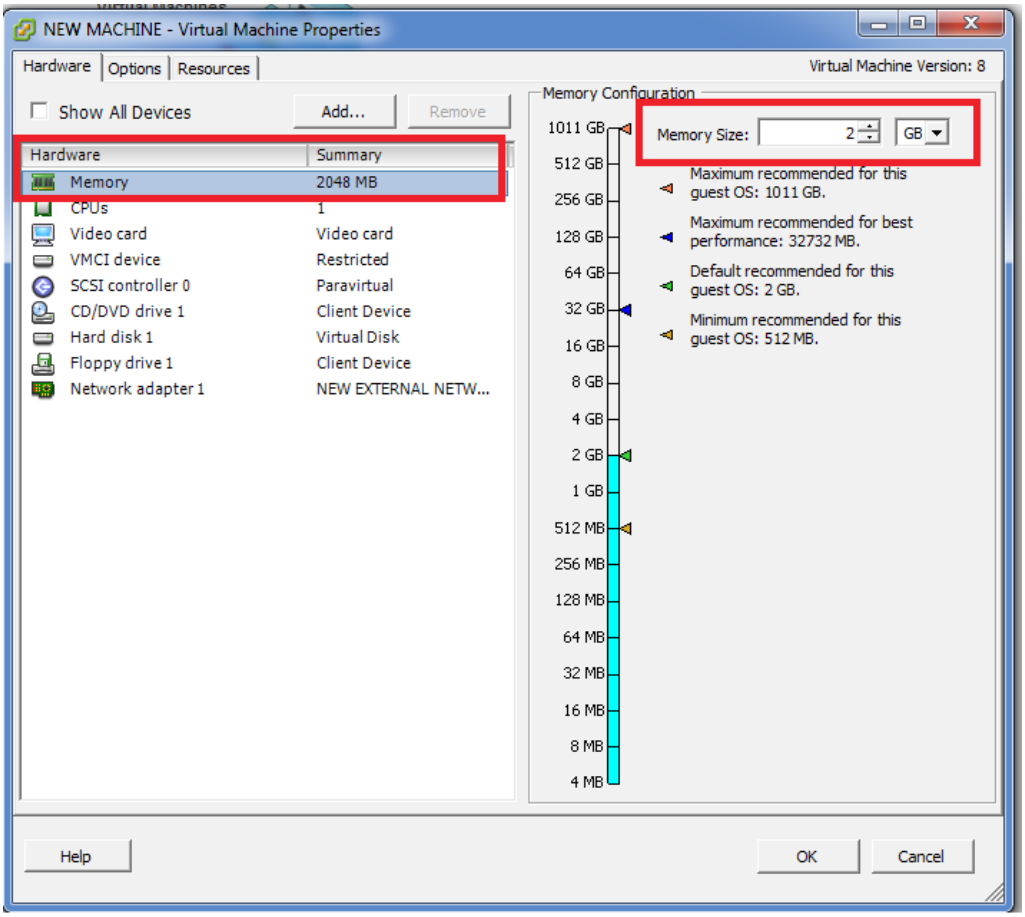
➢ Press ‘Finish’



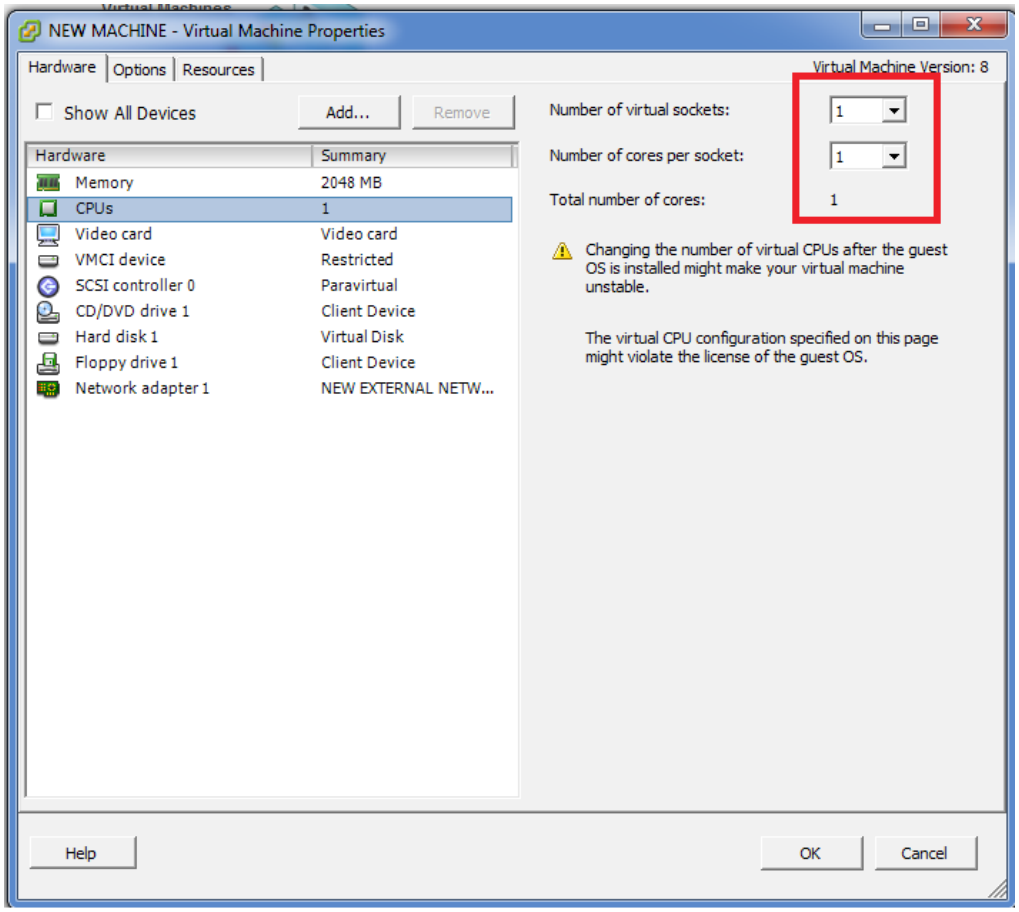
➢ Configure new VM settings: right click VM and press ‘Edit Settings…’



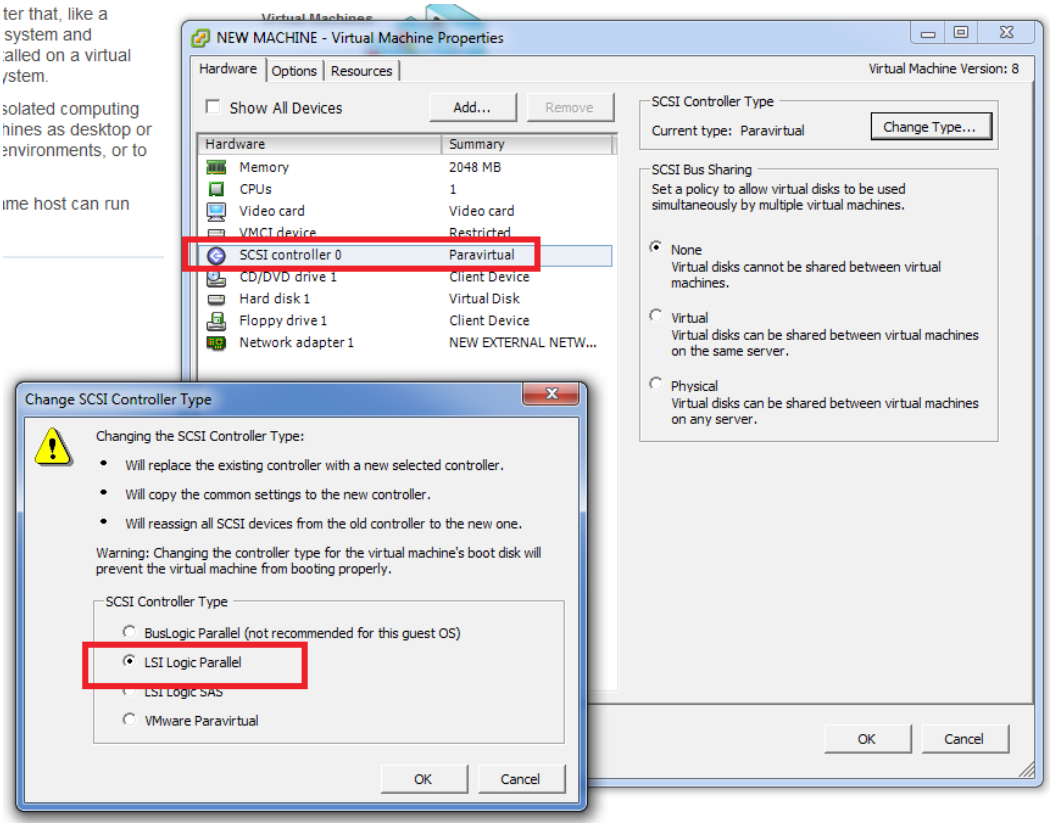
➢ Set Memory Size: at least 4 GB



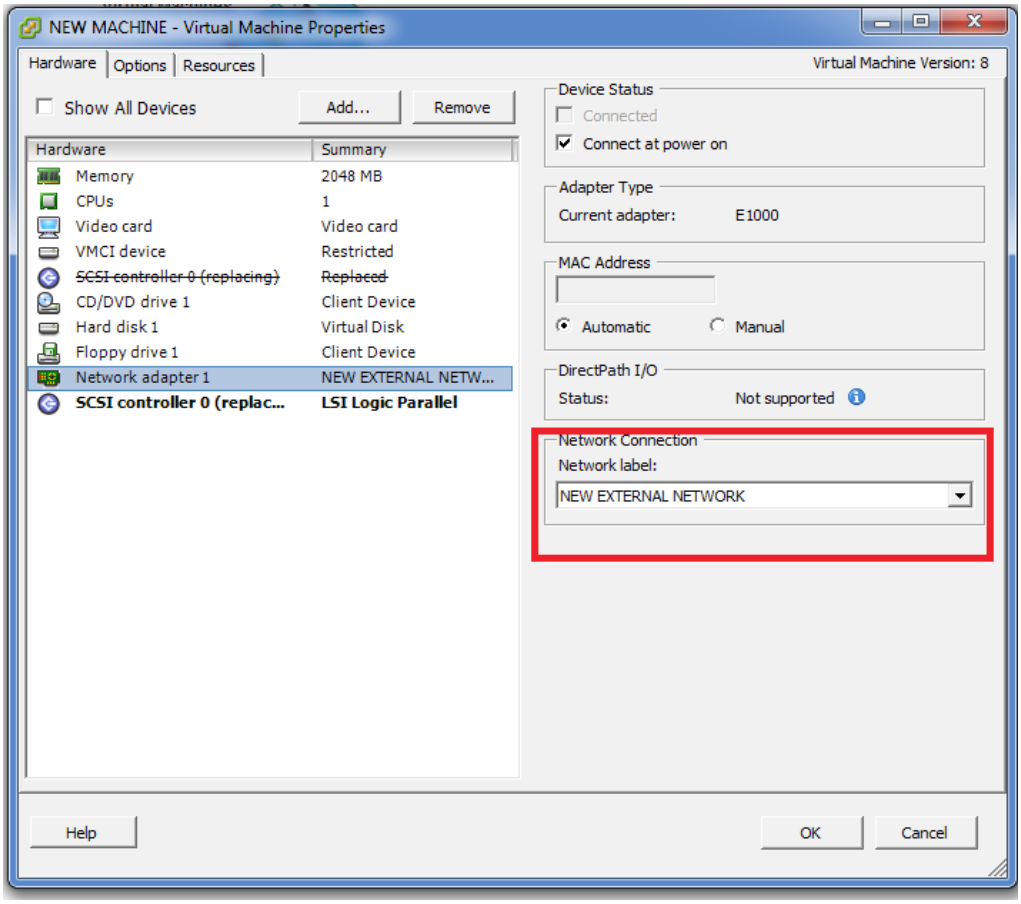
➢ Set CPUs quantity: one or more if required



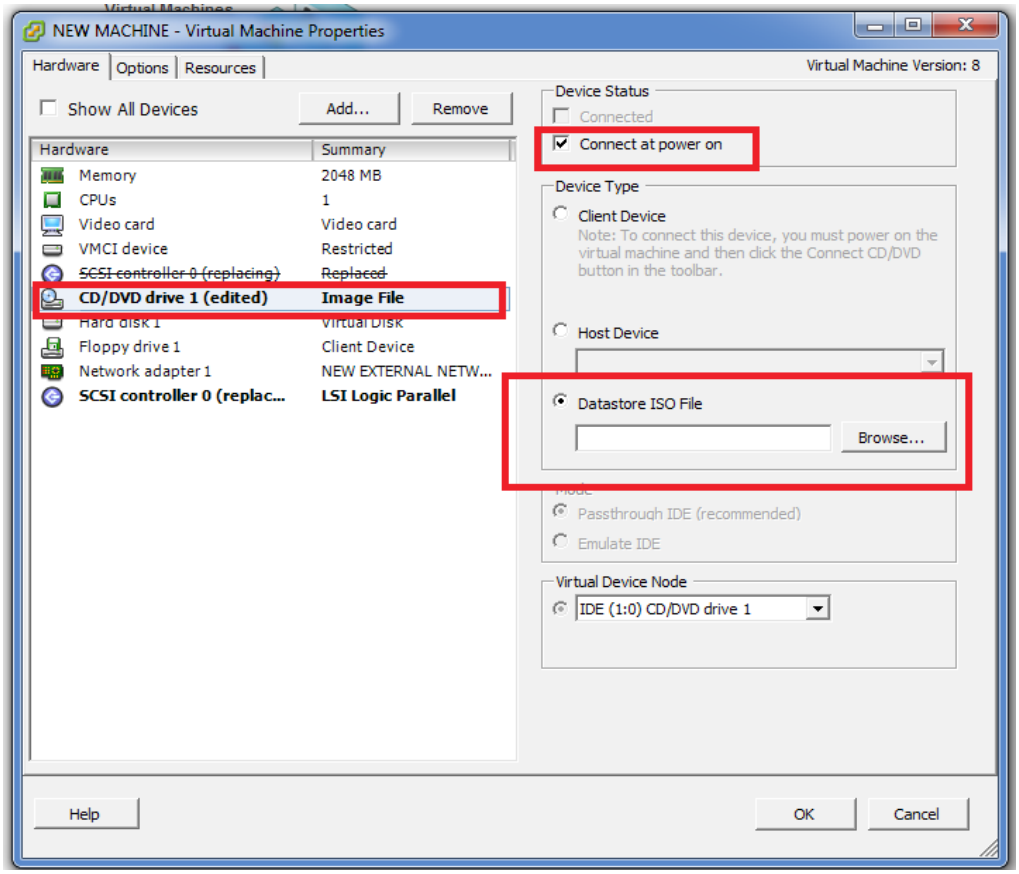
➢ Configure SCSI controller type: press ‘Change type’ and select ‘LSI Logic Parallel’



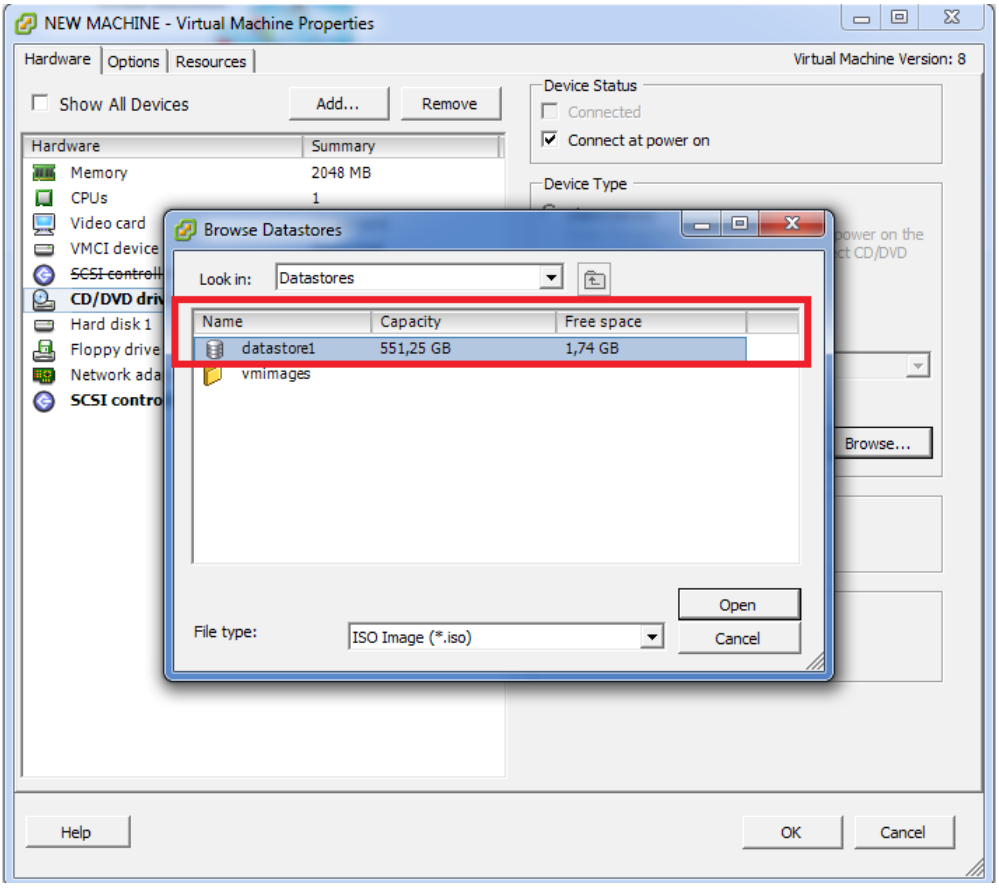
➢ Configure Network adapter

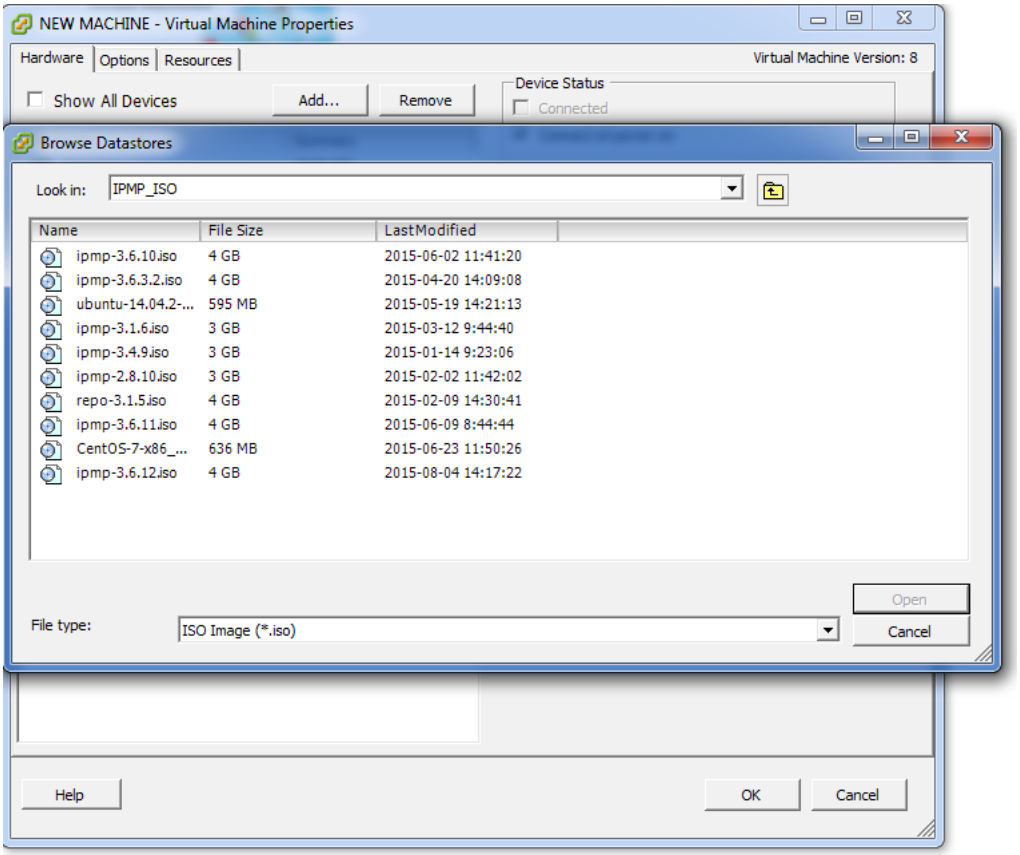


➢ Connect Power Manage image to the VM

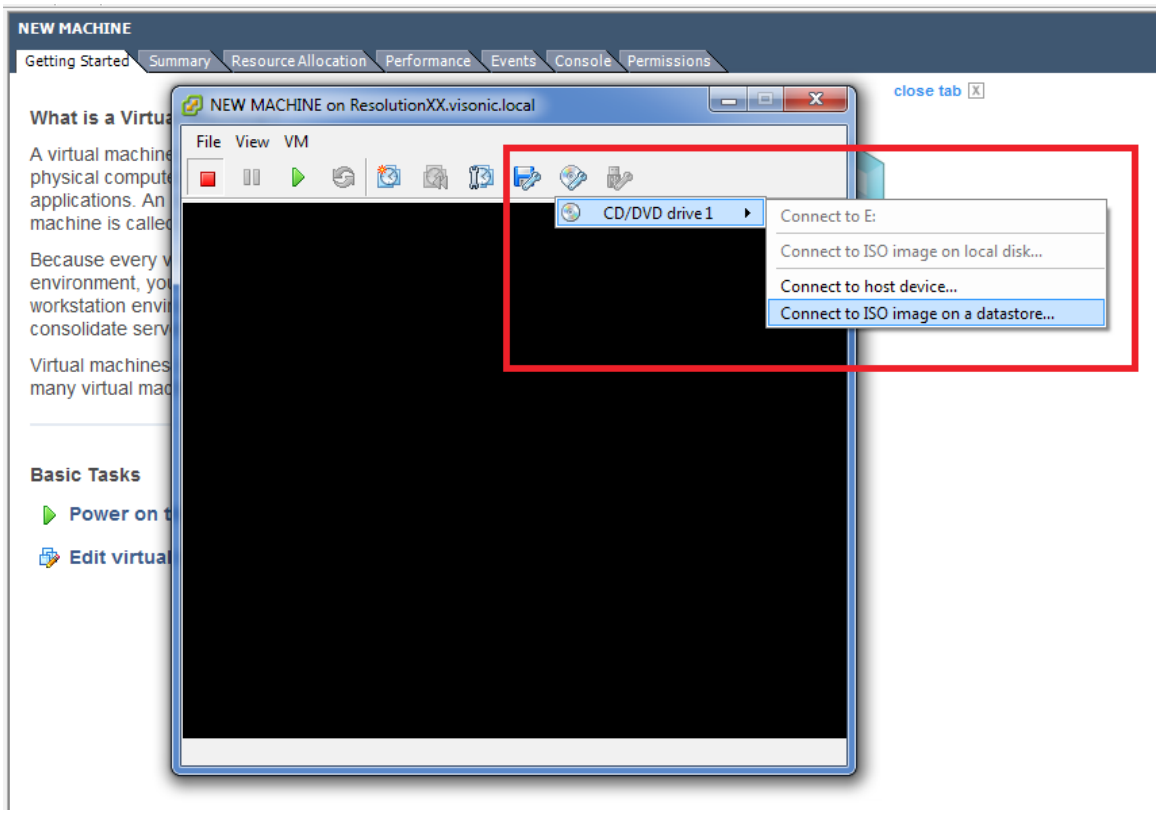


➢ Select Power Manage image file from the data store





➢ Open your virtual machine and connect the image



- Launch virtual machine and proceed with Power Manage installation by typing ‘cdrom’ boot option

Post Installation

After you finish the installation, your system is ready for use. However, other administrative tasks not covered by the installer may still be necessary, depending on how you plan to use your system. The list below describes some of the more common tasks usually performed immediately after a new installation.

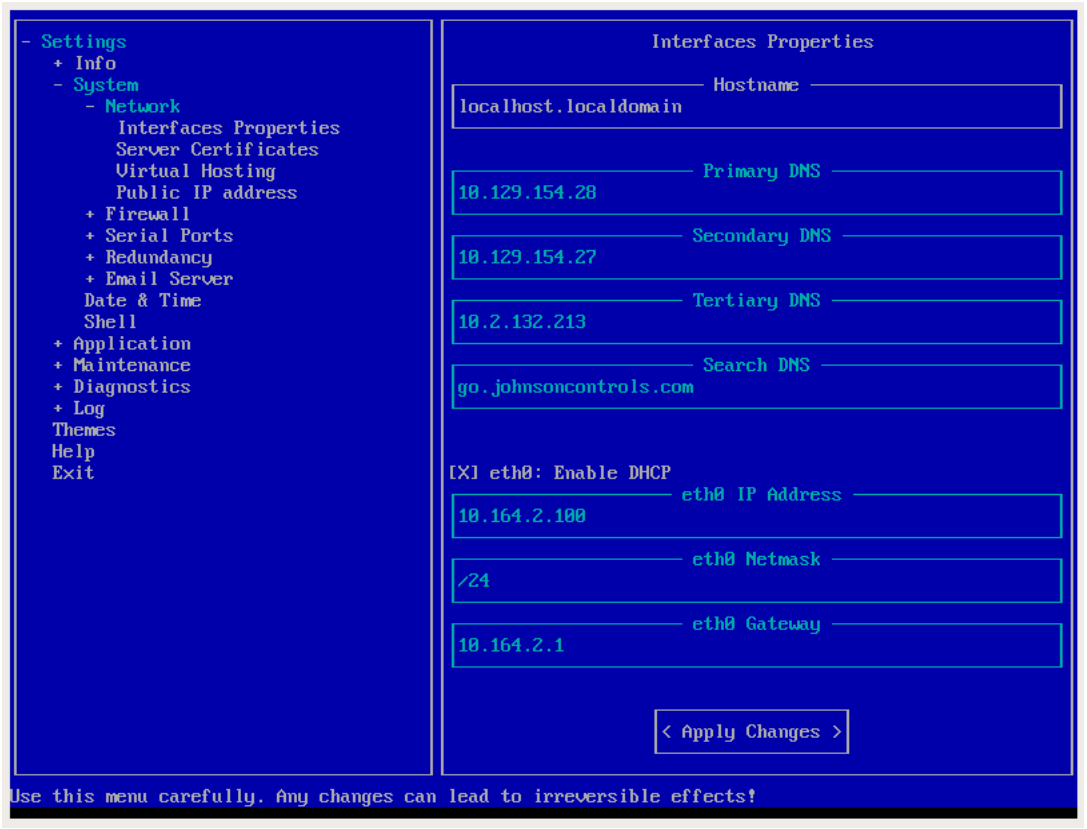
★ Initial Setup

Initial Setup allows you to configure several system settings, necessary to start with the system.

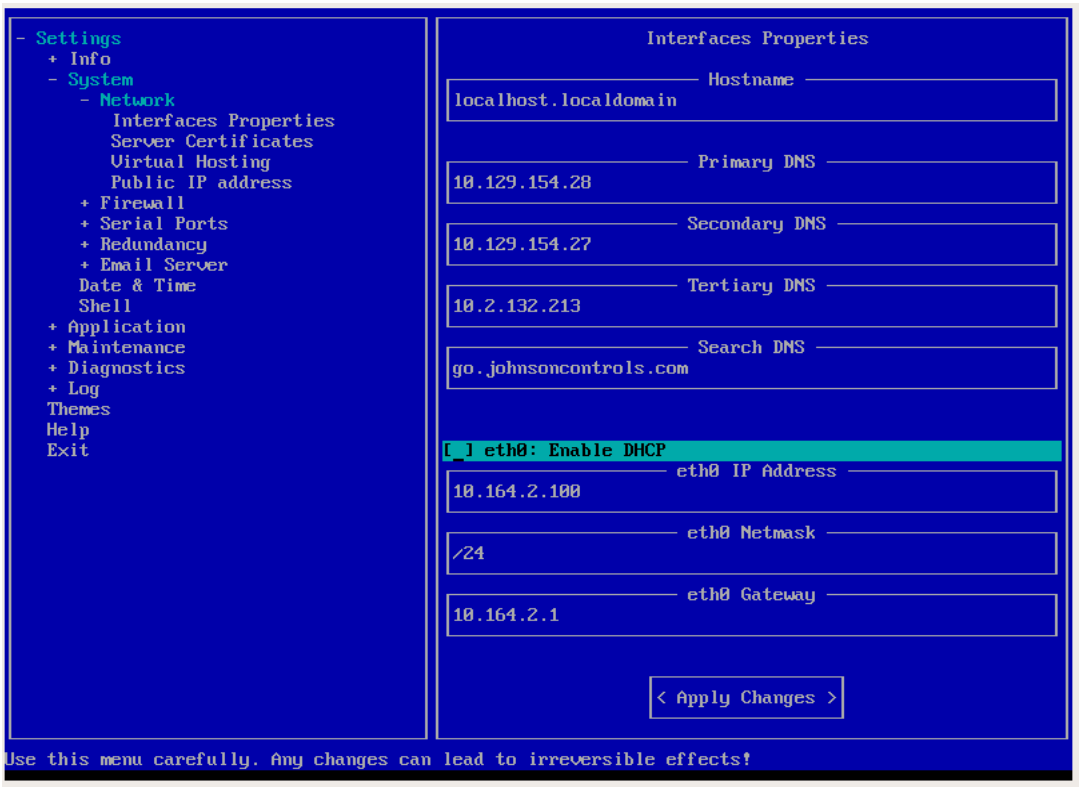
❑ *Configure the Network*

Network configuration settings is the process of setting a network's controls, flow and operation to support the network communication of PowerManage product. This process incorporates multiple configuration and setup processes onnetwork hardware, software and other supporting devices and components.

- In MMI menu go to **System > Network > Interfaces Properties**
- Set your servers’ Hostname
- Set primary DNS [secondary, tertiary if needed]
- Configure servers’ network interface:
  - In case server obtains its IP address by DHCP enable **ethX dhcp on/off** (where x is a number of your interface) option and press **Apply changes**



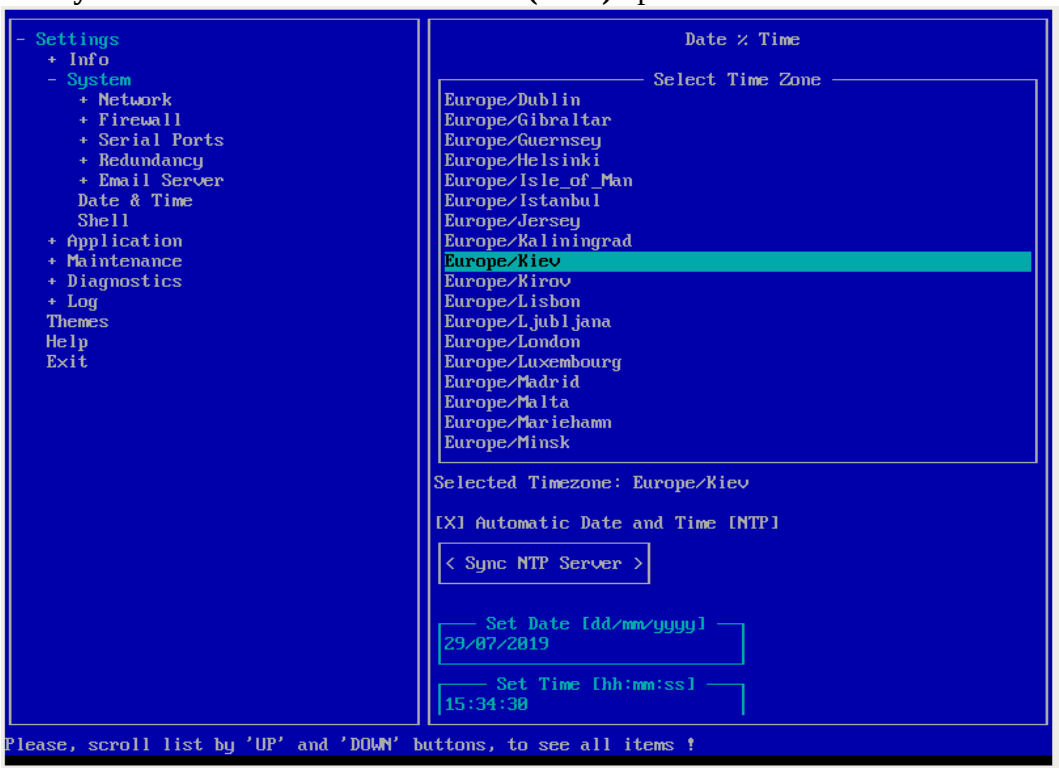
- In case you have to configure static IP address for your server, disable **ethx dhcp on/off** option, set **ethx IP address**, **ethx netmask**, **ethx gateway** and press **Apply changes**



❑ *Configure Time Synchronization*

The Network Time Protocol (NTP) enables the accurate dissemination of time and date information in order to keep the time clocks on networked computer systems synchronized to a common reference over the network or the Internet.

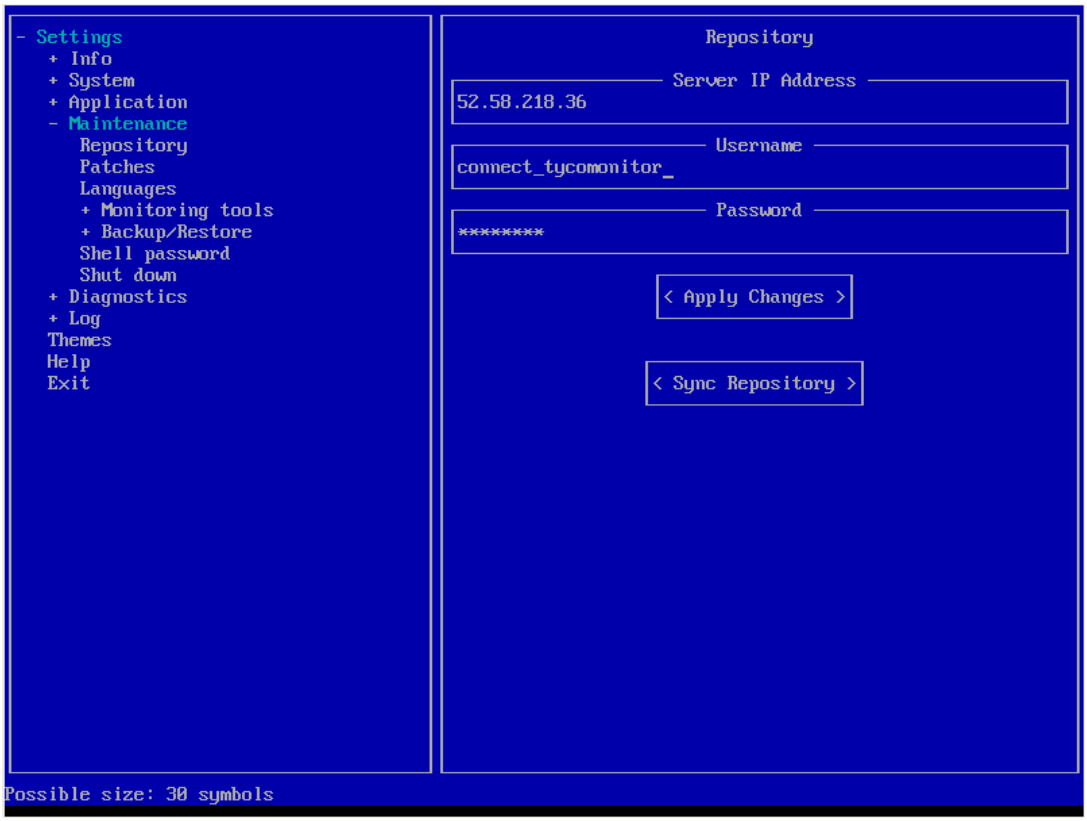
➢ Enter MMI menu, go to **System** > **Date & Time**. Ensure that correct time zone is selected and **Sync with Network Time Protocol (NTP)** option is enabled



❑ *Configure the repository*

A repository, known as a "Repo" for short, is a storage location from which firmware packages, localization, licenses, icons, events mapping, etc may be retrieved and installed on a PowerManage server.

➢ In MMI menu go to **Maintenance > Repository** menu
➢ Set repository IP address in the server field
➢ Set your repository account user
➢ Set your repository account password
➢ Press **Apply Changes**
➢ To synchronize with the repository, press Sync Repository



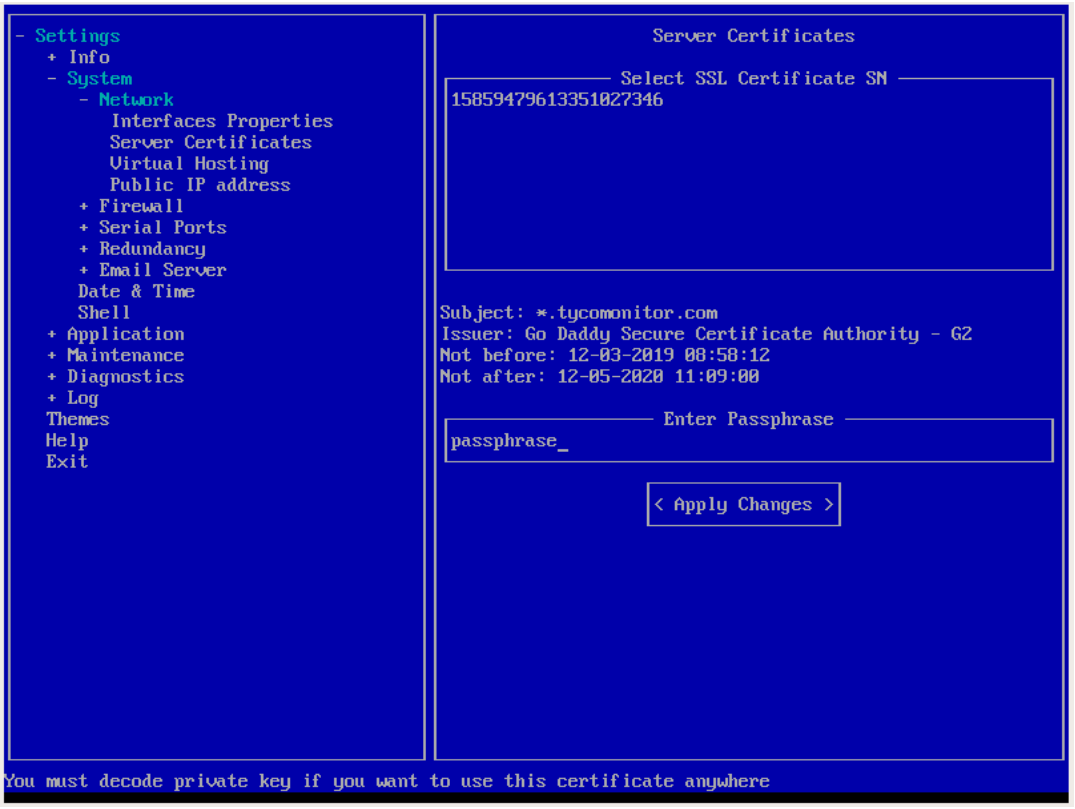
❑ *Assign SSL certificate to the Power Manage*

Pre-request: prior to applying the certificates, make sure your server connected to the repository and SSL certificates are added and assigned to your Repo account. As well, verify server synchronized with the repository. Detailed instruction in Appendix A.

To use HTTPS connections to the PowerManage Web Interface, Web Console and use Web/Mobile interactive services, its required to add and apply SSL certificates to the server.

- ➢ Go to MMI menu **System > Network > Interfaces Properties**
- ➢ Set your server DNS name into the **Hostname** field
- ➢ Go to **System > Network > Server Certificates**

➢ The list of all available SSL certificates is displayed in the **Select SSL Certificate SN** box
➢ Select the required certificate from the list
➢ Enter the key passphrase into the **Enter Passphrase** box
➢ Press **Apply** **Changes**

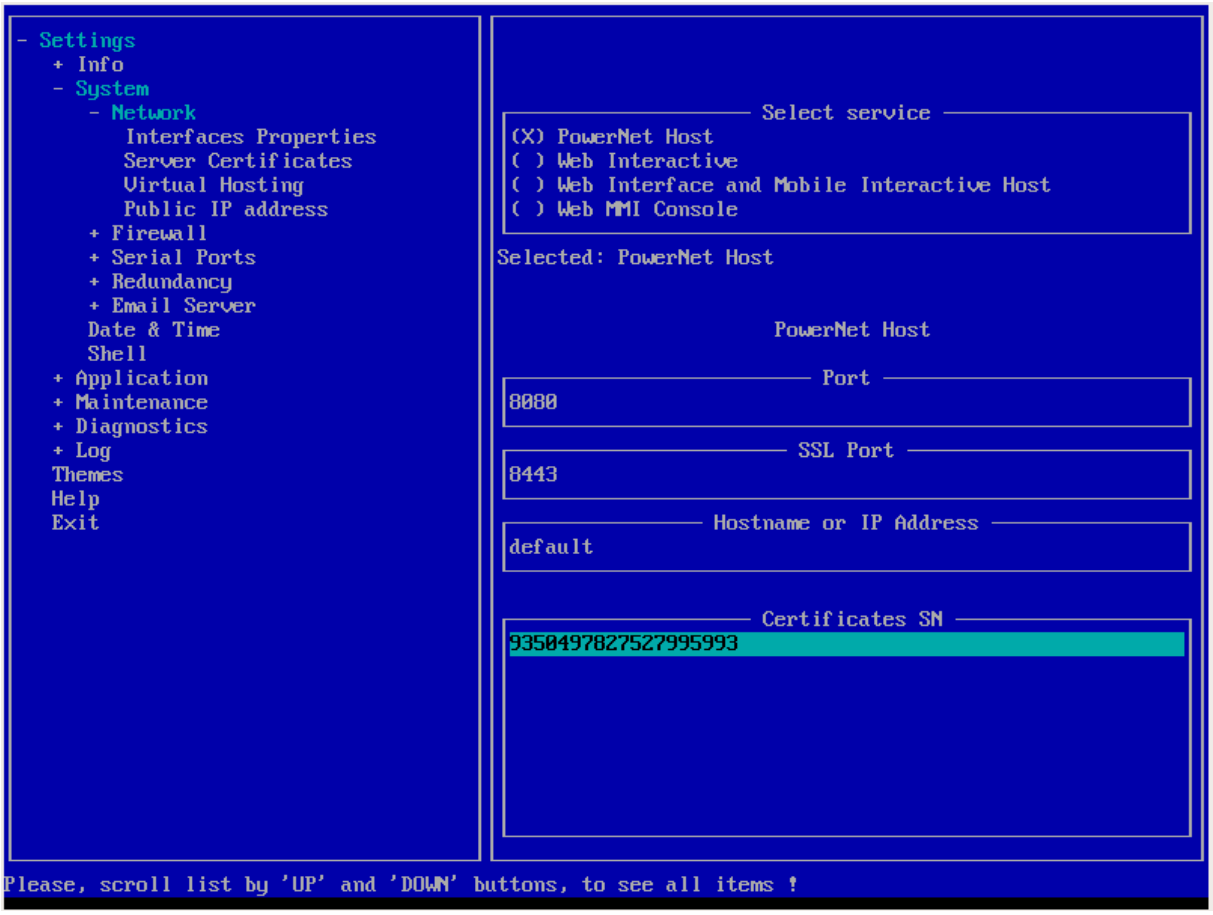


❑ *Configure Virtual Hosting*

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server

➢ In MMI menu go to **System > Network > Virtual Hosting** menu
➢ Select service from the following list:
  - PowerNet host - Communication between Plink & Server
  - Web interactive - Control and monitor panel through the web browser
  - Web Interface and Mobile interactive - Resolve/Maintenance Web interface and Control and monitor panel through mobile app
  - Web MMI console - MMI interface through web browser
➢ Set Ports number [SSL for encrypted connection and not SSL Port for unencrypted]
Note: if a port or SSL port number fields are left empty then the unencrypted or encrypted will not be available.

- ➢ Set the hostname or IP address [IP could be used only with non-encrypted service]
- ➢ Choice the certificate from the list of available certificates
  Note: Different types of SSL keys are listed in the Certificates SN window. Details in windows below.
- ➢ Press "Apply Changes"



To access specific service use the following command in your browser:

- ➢ <server URL>:<port number>

★ Common Post-installation Tasks

After you finish the installation and go through one of the "initial setup" described above, your system is ready for use. However, other administrative tasks not covered by the initial setup utilities may still be necessary, depending on how you plan to use your system. The list below describes some of the more common tasks usually performed immediately after a new installation.

ITv2 protocol is intended for one to one communications between an integration module and a third party integration server or device. The two sides of communication is a peer to peer relationship; both sides can initiate a command/response packet exchange.

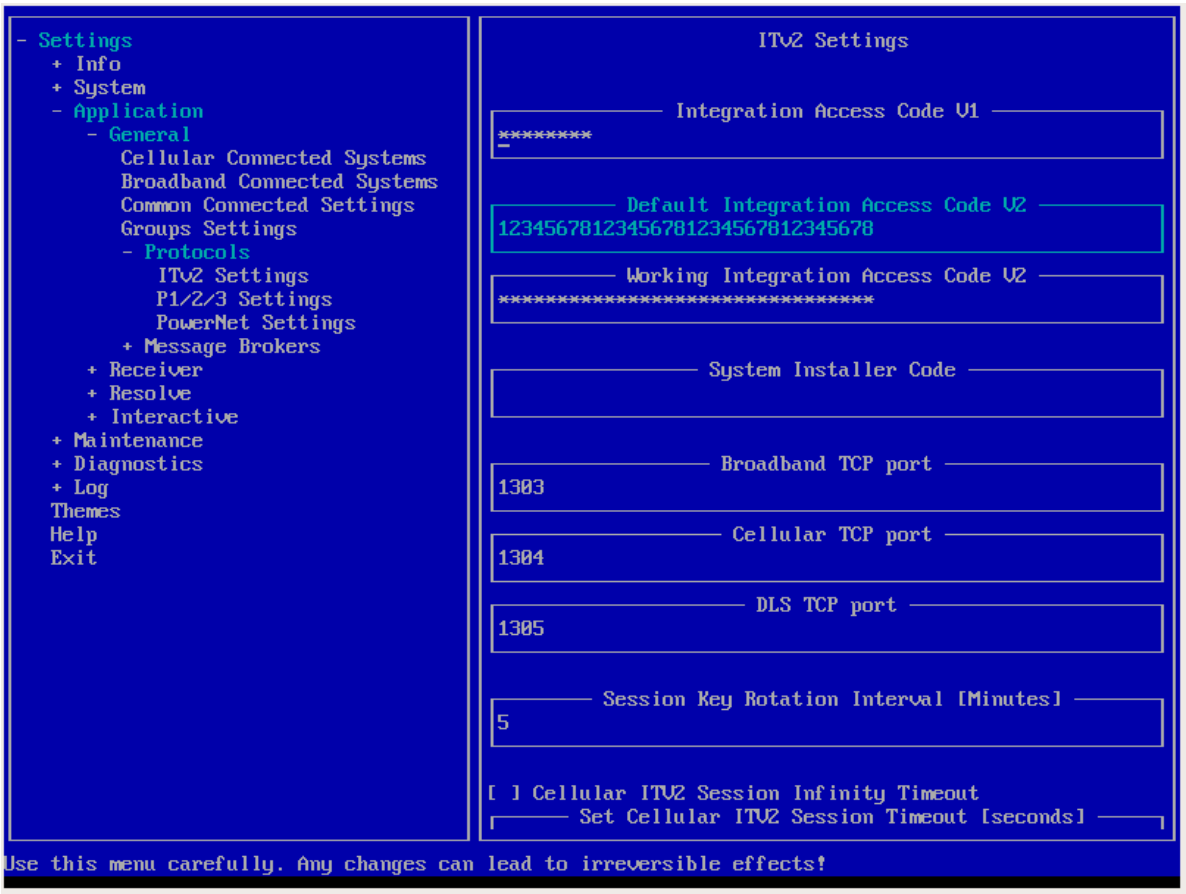
The Neo and PSP (Power Series Pro) panels communicate with the power-manage server via ITv2 protocol that is encrypted with 'Working Integration Access Code'.

The old Neo panels have 8 character integration code which must be identical to the 'Integration

Access Code V1' field (see below screenshot).

The newer Neo panels and PSP panels have 32 character integration code with default value of 12345678123456781234567812345678 (see 'Default Integration Access Code V2' in the below screenshot) and the server automatically changes it to the 'Working Integration Access Code V2' value (see below screenshot).

- ➢ In MMI menu go to **System > Application > General > Protocols > ITv2 Settings**
- ➢ **Default Integration Access Code V2** doesn't change.
- ➢ In **Working Integration Access Code V2** set your access code (this section uses for initialization with applications.



Notes:

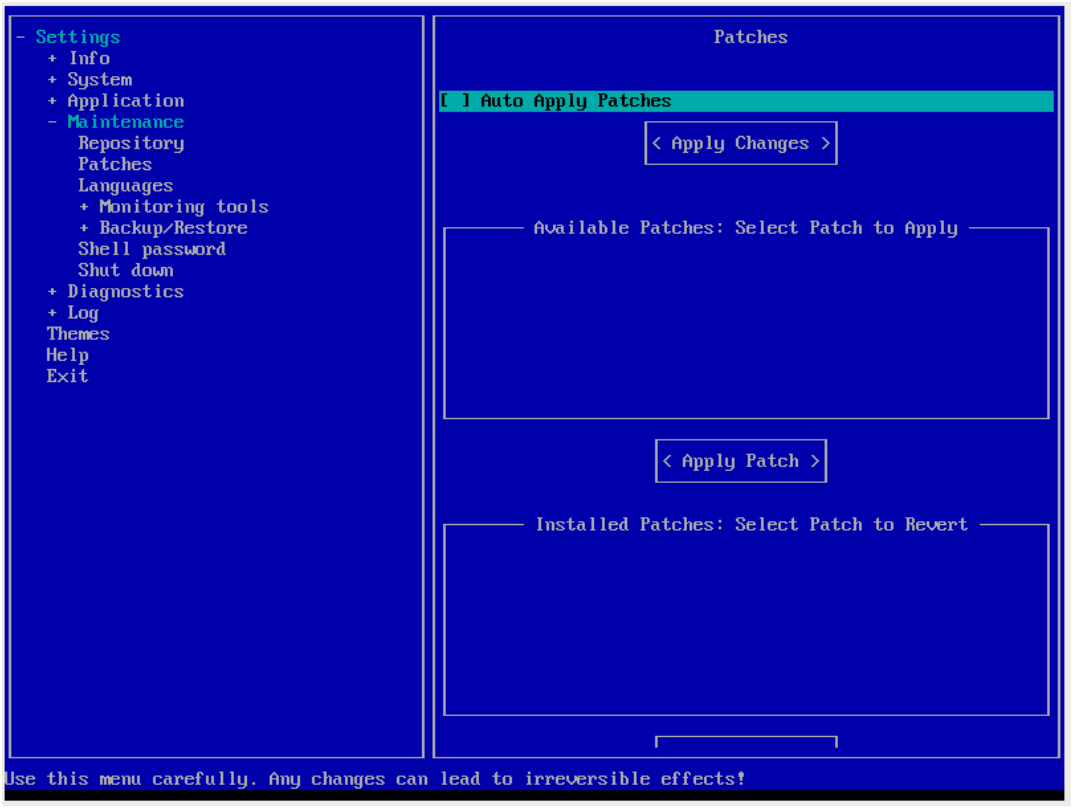
1) The 'Working Integration Access Code V2' value can remain in its default value or changed to any different value prior to any panel enrollment. If value changed after any panel enrollment, all the already enrolled panels will be disconnected.

2) If an enrolled PSP or new Neo panel is reset to factory default, then it must be deleted from the server. Otherwise it will not reconnect to the server.

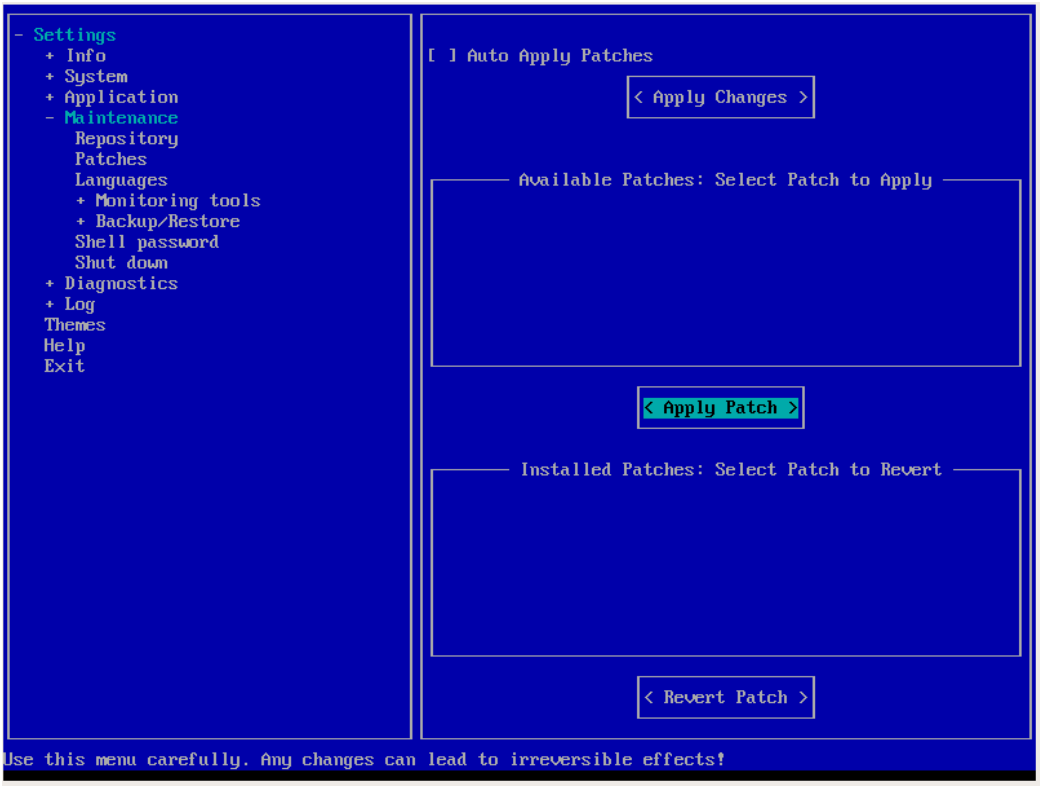
❑ *Applying/Reverting patches*

Verify repository settings configured on your server.

- ➢ In MMI menu go to **System > Maintenance > Patches**
- ➢ All patches available for your server will be displayed
- ➢ Select required patch file from the list and press **Apply Patch**



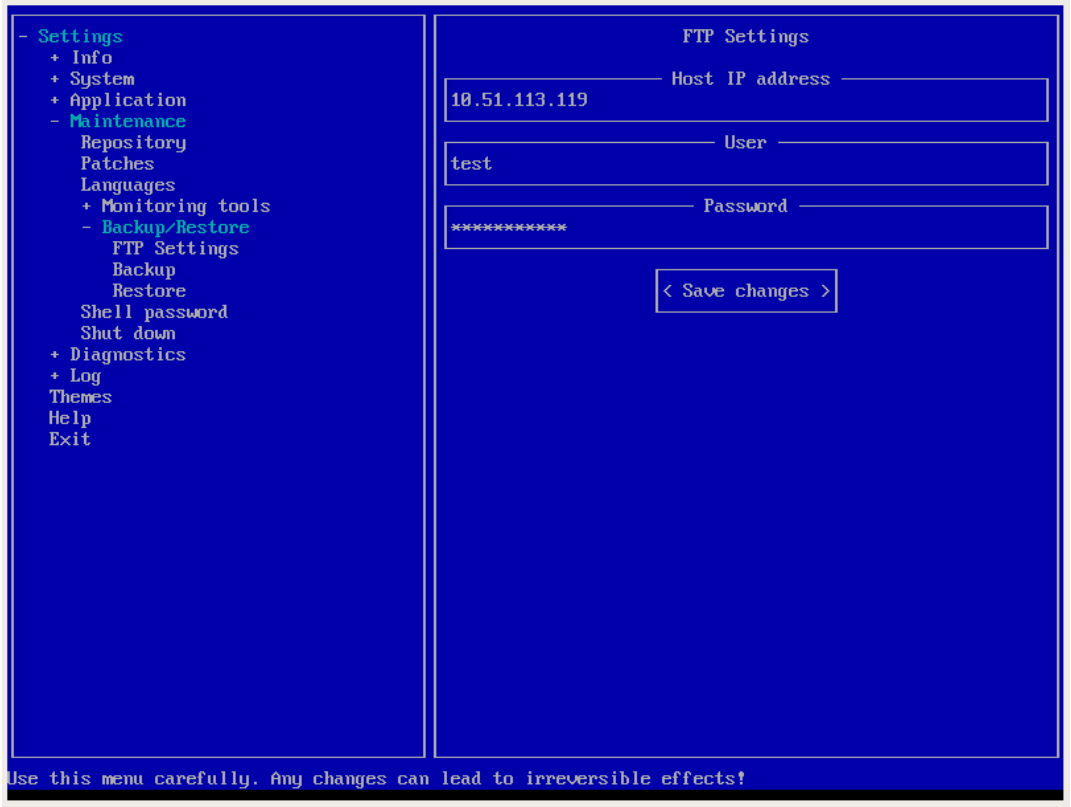
- ➢ Once patch is applied successfully it'll be displayed in **Installed Patches** box
- ➢ In case the patch needs to be removed in the same menu select patch file you need to remove and press **Revert Patch**
- ➢ Patch disappears from **Installed patches** after it's been removed



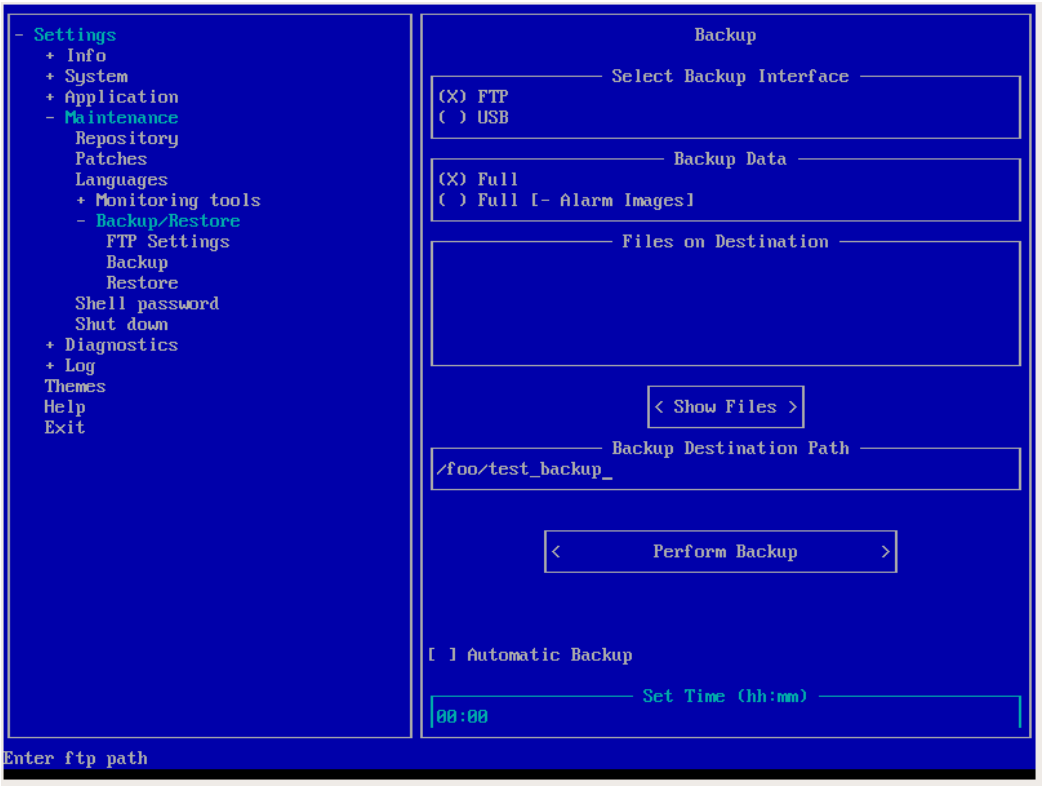
NOTE: If you need to apply multiple patches you need to perform it in direct order. For example: apply patch 1.1.1.1 first, then 1.1.1.2, 1.1.1.3...

❑ *Backup to FTP server*

➢ In MMI menu go to **Maintenance > Backup/Restore > FTP Settings** menu
➢ Set **Host IP address** of your server, **User**, **Password** and press **Apply changes**



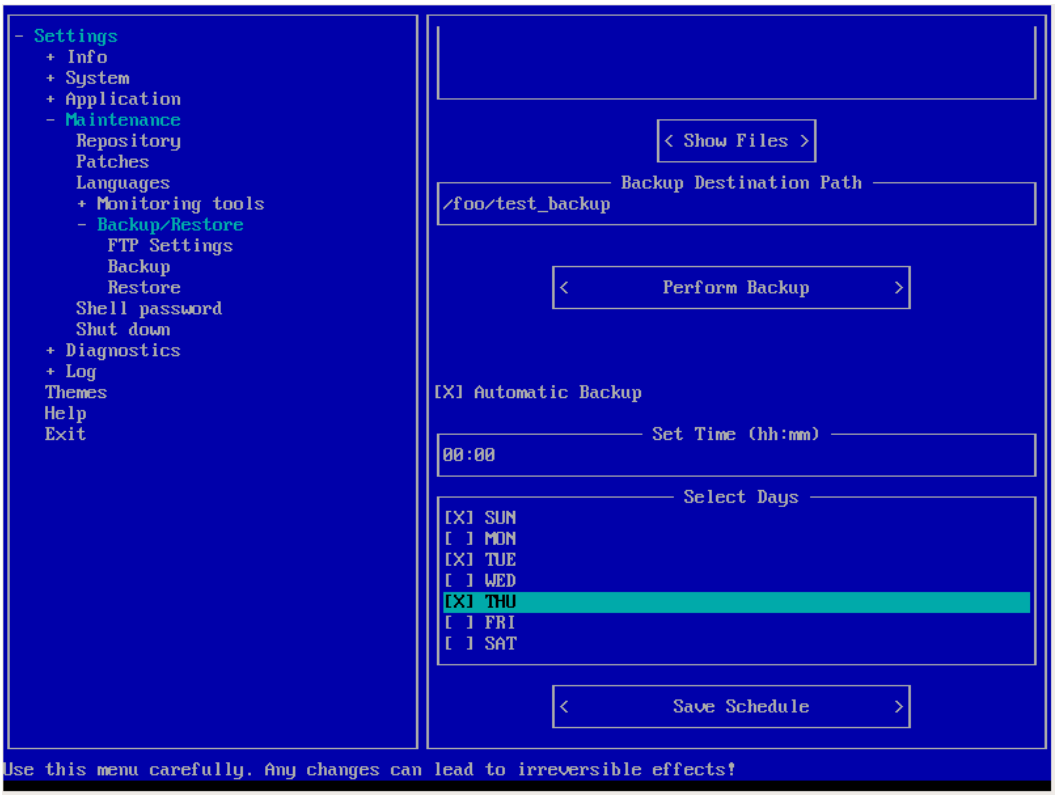
➢ Go to **Maintenance > Backup/Restore > Backup** menu
➢ Set backup method to **FTP backup**
➢ In **Backup Data** define which data do you want to include into backup
➢ In **Backup Destination Path** set absolute path and filename that you're going to create
➢ You can use **Show Files** button to list backup files located in the directory
➢ Press **Perform Backup**



➢ Once the backup is successfully completed, press **ESC** keyboard button

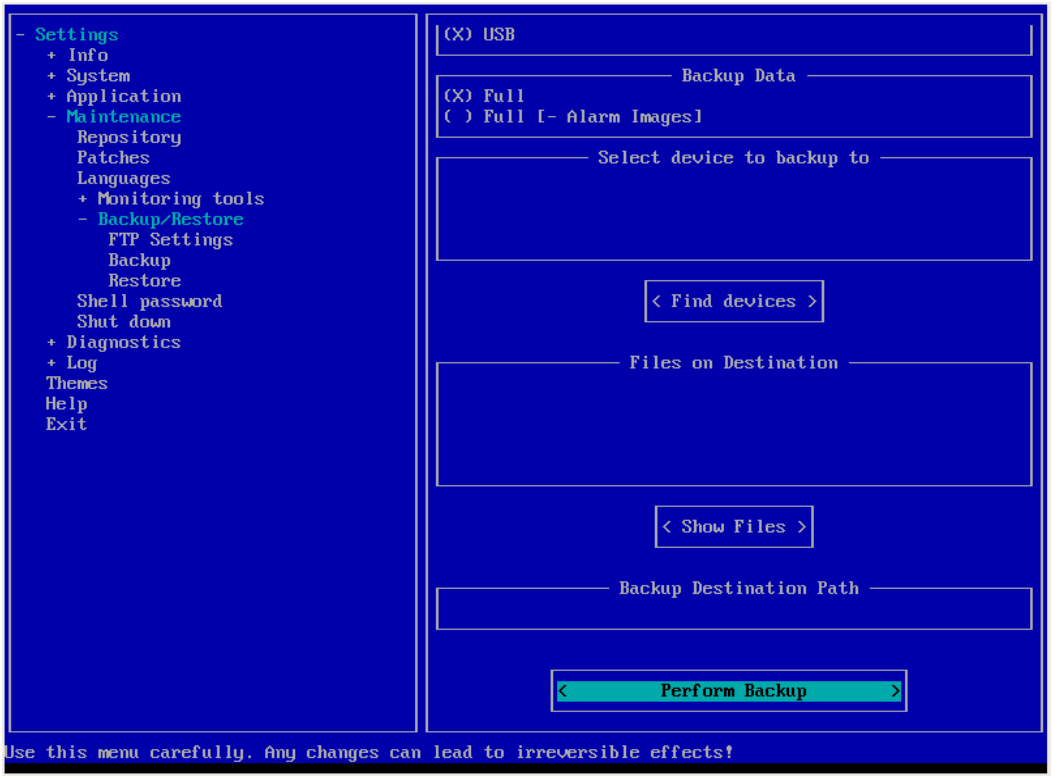
❑ *Backup to FTP server by schedule*

➢ Go to **Maintenance > Backup/Restore > Backup** menu
➢ Set backup method to **FTP**
➢ In **Backup Data** define which data do you want to include into backup
➢ In **Backup Destination Path** set absolute path and filename that you're going to create
➢ Set the **Automatic Backup** checkbox
➢ Set time when to perform the backup
➢ Select the week days at which to perform the backup
➢ Press **Save Schedule**



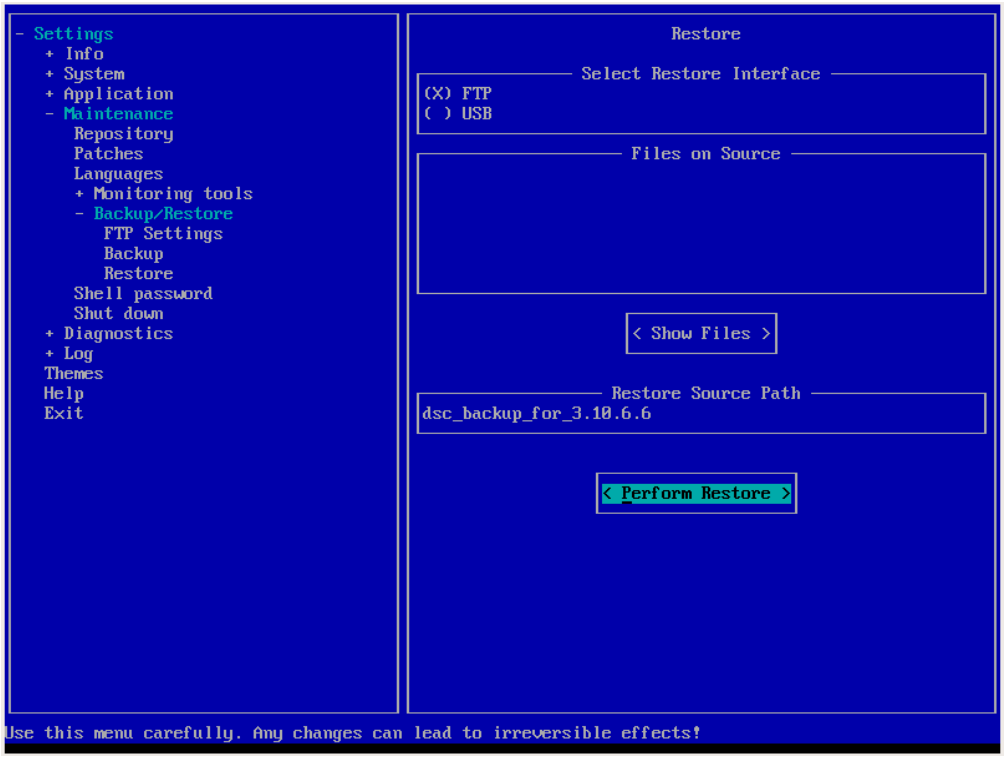
❑ *Backup to USB*

- ➢ Connect USB drive to your server
- ➢ Go to **Maintenance** > **Backup/Restore** > **Backup** menu
- ➢ Set backup method to **USB**
- ➢ In **Backup Data** define which data do you want to include into backup
- ➢ Press **Find devices** to list available devices
- ➢ Select connected USB drive
- ➢ In **Backup Destination Path** set absolute path and filename that you're going to create
- ➢ You can use **List dir** button to list backup files located in the directory
- ➢ Press **Perform Backup**



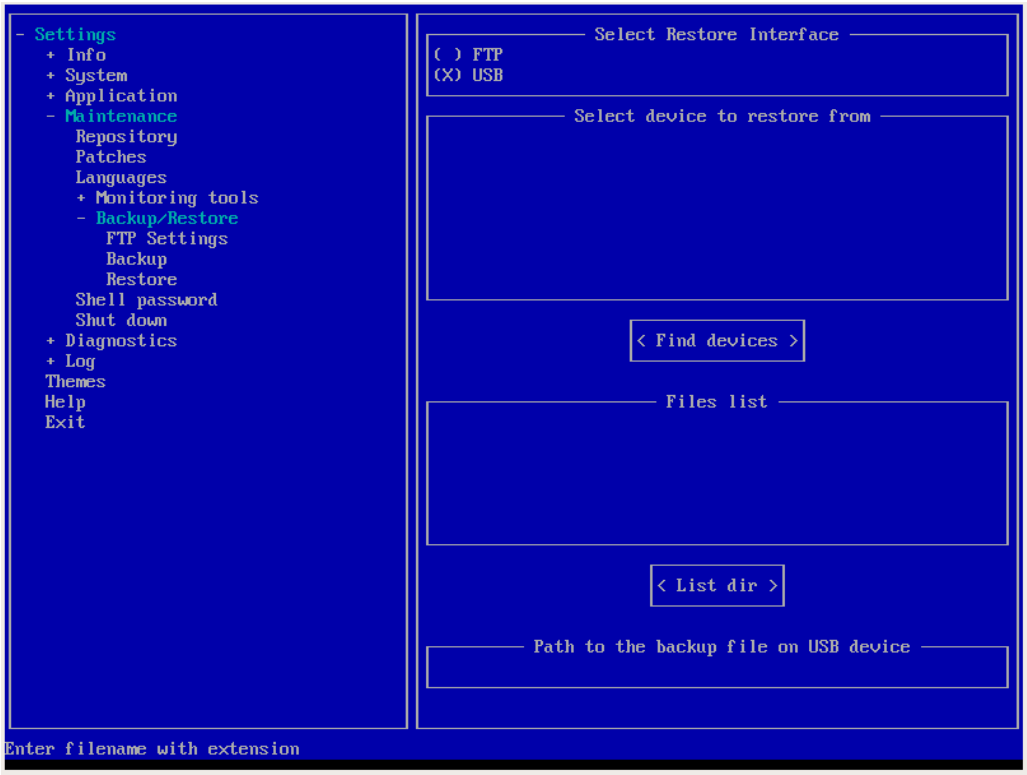
❑ *Restore from FTP server*

- ➢ In MMI menu go to **Maintenance > Backup/Restore > FTP Settings** menu
- ➢ Set **Host IP address** of your server, **User**, **Password** and press **Apply changes**
- ➢ Go to **Maintenance > Backup/Restore > Restore** menu
- ➢ Set restore method to **FTP**
- ➢ In **Path to restore from FTP** set absolute path to directory with backup
- ➢ Press **List dir** button to list available backup files located in the directory
- ➢ In **Files list** select necessary backup file and press **Enter** keyboard button
- ➢ Press **Perform Restore**



❑ *Restore from USB*

- ➢ Connect USB drive to your server
- ➢ In MMI menu go to **Maintenance** > **Backup/Restore** > **Restore** menu
- ➢ Set restore method to **USB**
- ➢ Press **Find devices** to list available devices
- ➢ In **Select device to restore from** select connected USB drive
- ➢ In **Path to the backup file on USB device** set the backup absolute path
- ➢ Press **List dir** button to list backup files located in the directory
- ➢ In **Files list** select necessary backup file and press **Enter** keyboard button
- ➢ Press **Start restore**



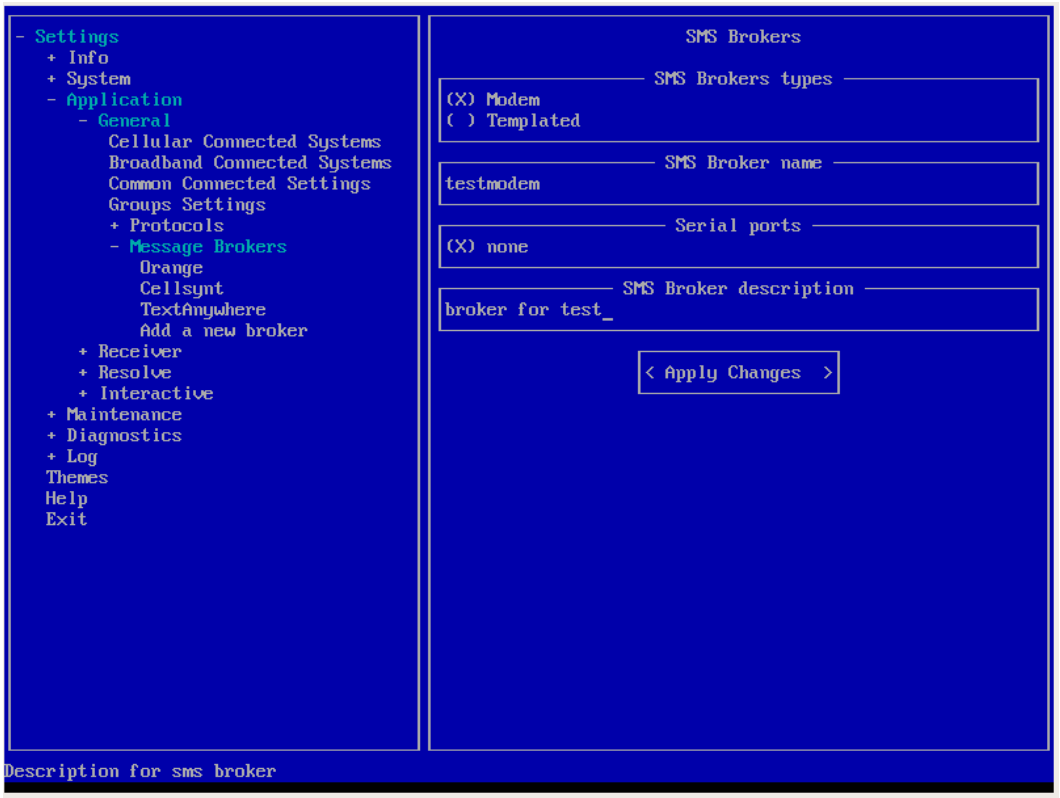
SMS Broker configuration

SMS broker has to be configured in order to send SMS notifications from the server. It's also possible to define Wake-up modem settings.

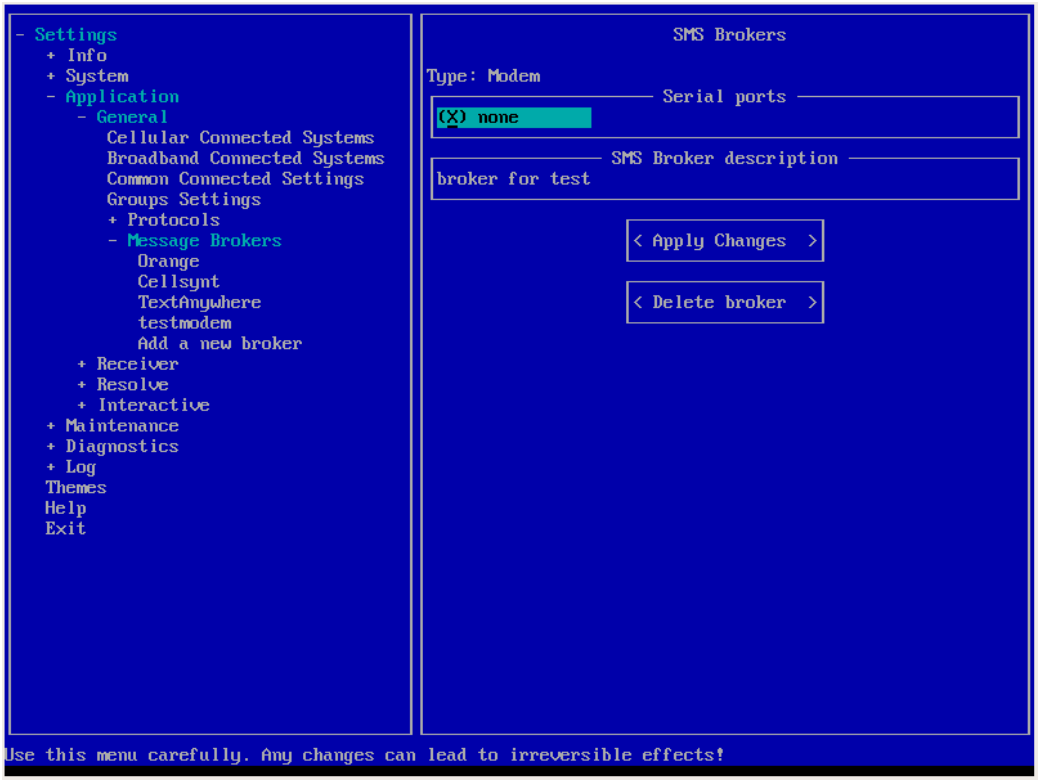
❑ *Defining Wake-up modem settings*

It's meant that GSM modem is already connected to a servers' configured serial port.

- ➢ In MMI menu go to **Application > General > Message Brokers > Add a new broker**
- ➢ In **SMS Brokers types** set type to **Modem**
- ➢ In **SMS Broker name** set name of the modem
- ➢ In **Serial ports** select port to which modem is connected
- ➢ In **SMS Broker description** set modem's description/comments
- ➢ Press **Add broker**



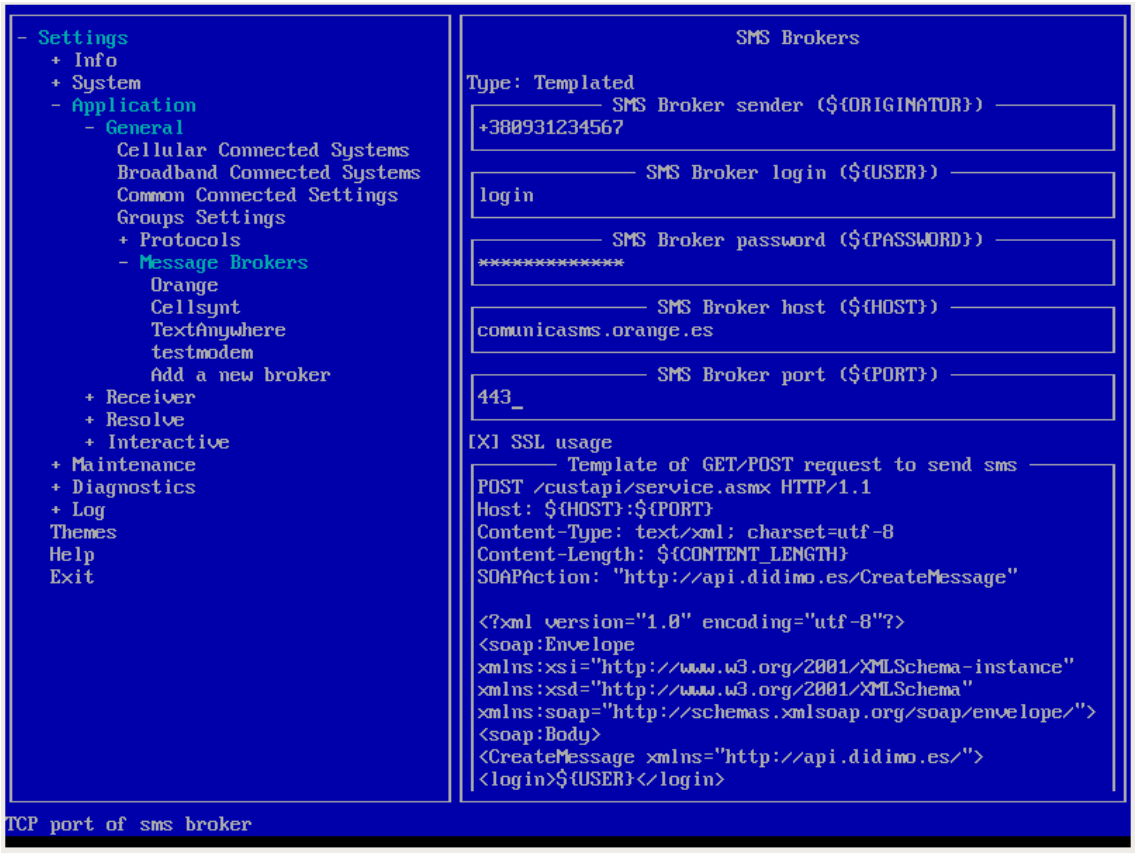
- ➢ After modem is added it'll appear in **Application > General > Message Brokers** list



❑ *Adding SMS broker*

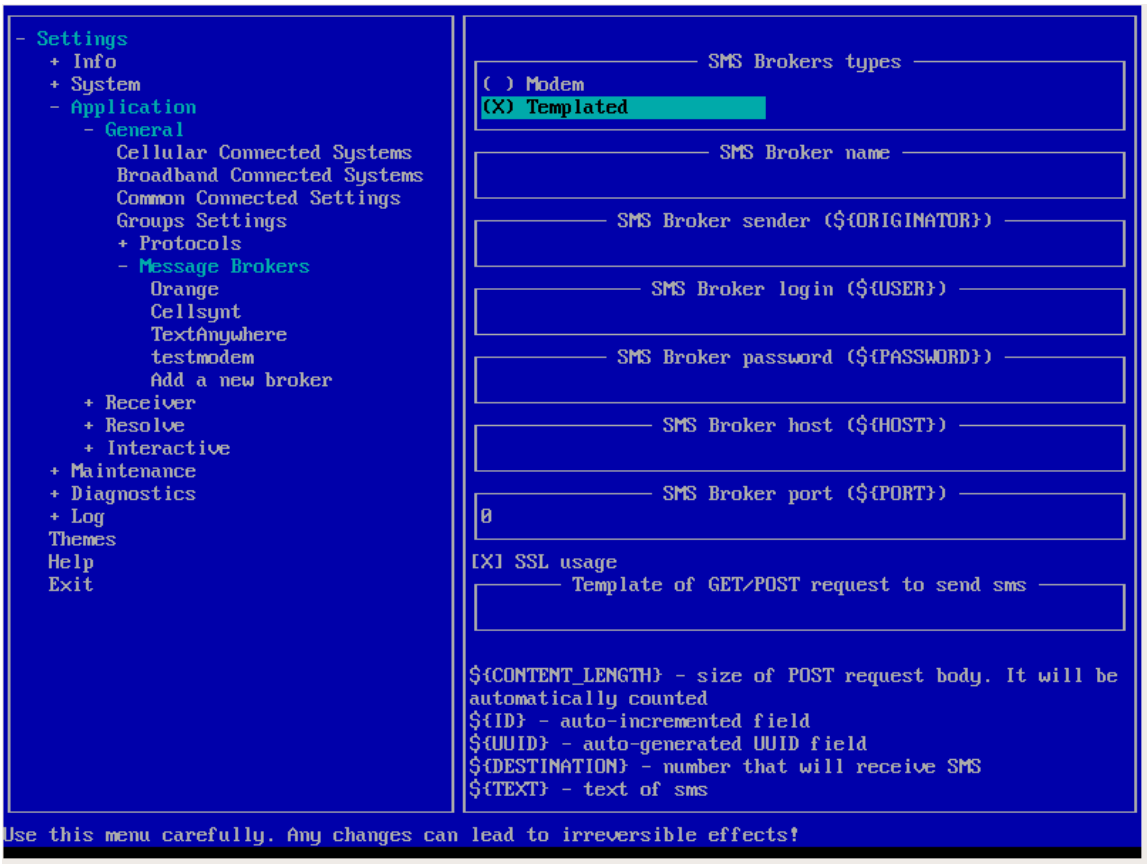
PowerManage has pre-configured settings for Orange, Cellsynt, TextAnywhere SMS brokers. To use any of these brokers:

- ➢ In MMI menu go to **Application > General > Message Brokers**
- ➢ Choose Orange/Cellsynt/TextAnywhere
- ➢ In **SMS Broker sender** set your broker phone number. (This number will be indicated to the client as a source sender number of SMSs sent by your server)
- ➢ In **SMS Broker login** and **SMS Broker password** set login and password respectively
- ➢ Press **Add broker**



To use any other broker it's required to create the HTTP request that will be used to send SMS and place it in the broker's configuration as a **Template of GET/POST request to send sms**.
The request that is used for SMS sending should be obtained from the broker's API.
There are several parameters that most of requests use that are generated by PowerManage itself and can be used as variables inside the request.
These variables are listed in **Application > General > Message Brokers > Add a new broker** under **Template of GET/POST request to send sms** frame:

- ${CONTENT_LENGTH} - size of POST request body. It's counted automatically
- ${ID} - auto-incremented field
- ${UUID} - auto-generated field that is usually used as message ID
- ${DESTINATION_ID} - SMS recipient number
- ${TEXT} - message text



In such way when any of above parameters is used in the request, you just need to store it's variable name. For instance message text will be passed into the request as **'text=${TEXT}'** or **'<message>${TEXT}</message>'** (it depends on broker's API).
Let's consider an example:

Messages broker http://www.vianett.com.

By URL http://www.vianett.com/en/developers/api-documentation/http-get-post-api can be found their HTTP GET/POST API Documentation.

Request for outgoing messages:
https://smsc.vianett.no/v3/send?username=xxxxxx&password=xxxxxx&msgid=xxxx&tel=xxxxxx&msg=Hello+World&pricegroup=300&campaignid=xxxxx

In such way, request that has to be set into the **Template of GET/POST request to send sms** looks this way:

GET /v3/send?username=${USER}&password=${PASSWORD}&msgid=${UUID}
&tel=${DESTINATION}&msg=${TEXT}&campaignid=378404
HTTP/1.1
Host:${HOST}:${PORT}
User-Agent:firefox
Connection:close

where,
GET - type of method that is used (GET/POST)
msgid - message number (must be unique ID)
tel - recipient phone number
msg - message text
campaignid - parameter specific for this exact broker, defines your company ID. Specified in the account settings
HTTP/1.1 - HTTP protocol version
Host, User-Agent, Connection - header parameters that are added to the request

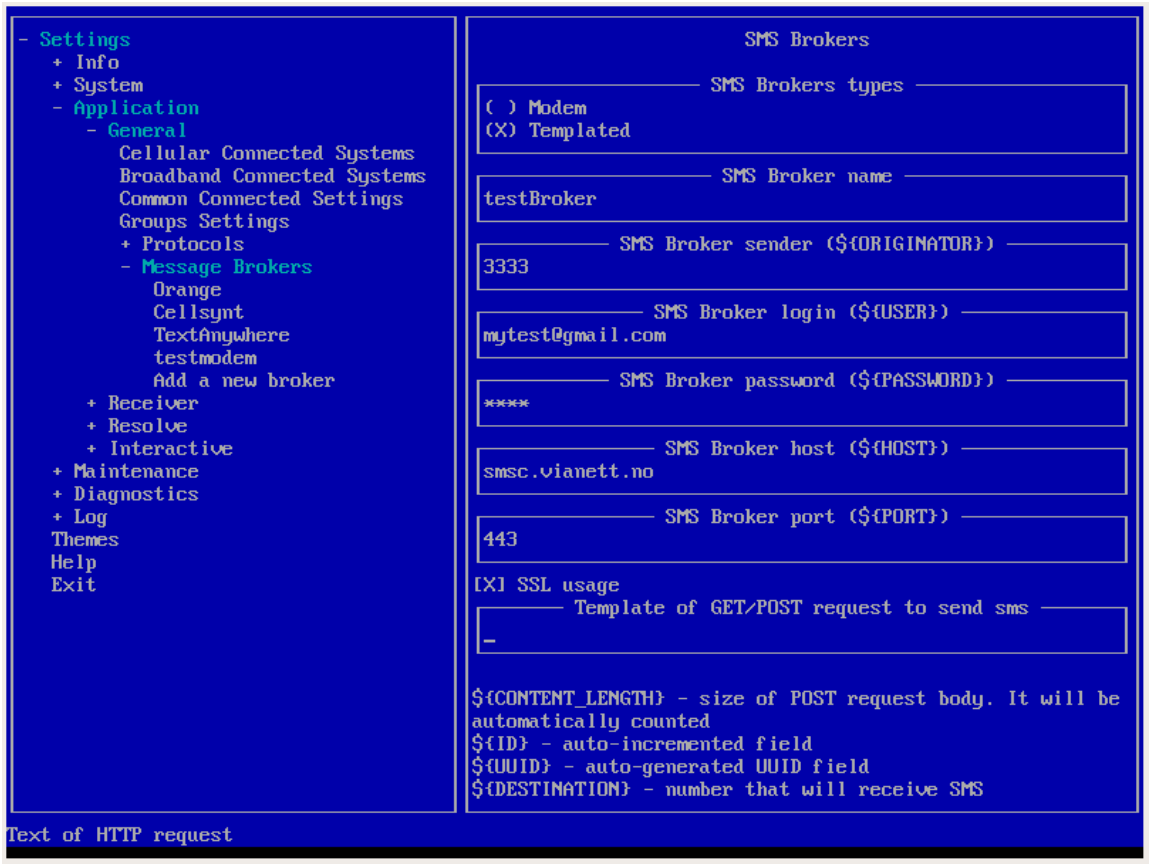
NOTE: It's important to set HTTP request line breaks correctly. Request's body should be one line. Although there are automatic line breaks, all new lines should be created with **Enter**:

GET /v3/send?username=${USER}&password=${PASSWORD}&msgid=${UUID}
&tel=${DESTINATION}&msg=${TEXT}&campaignid=378404

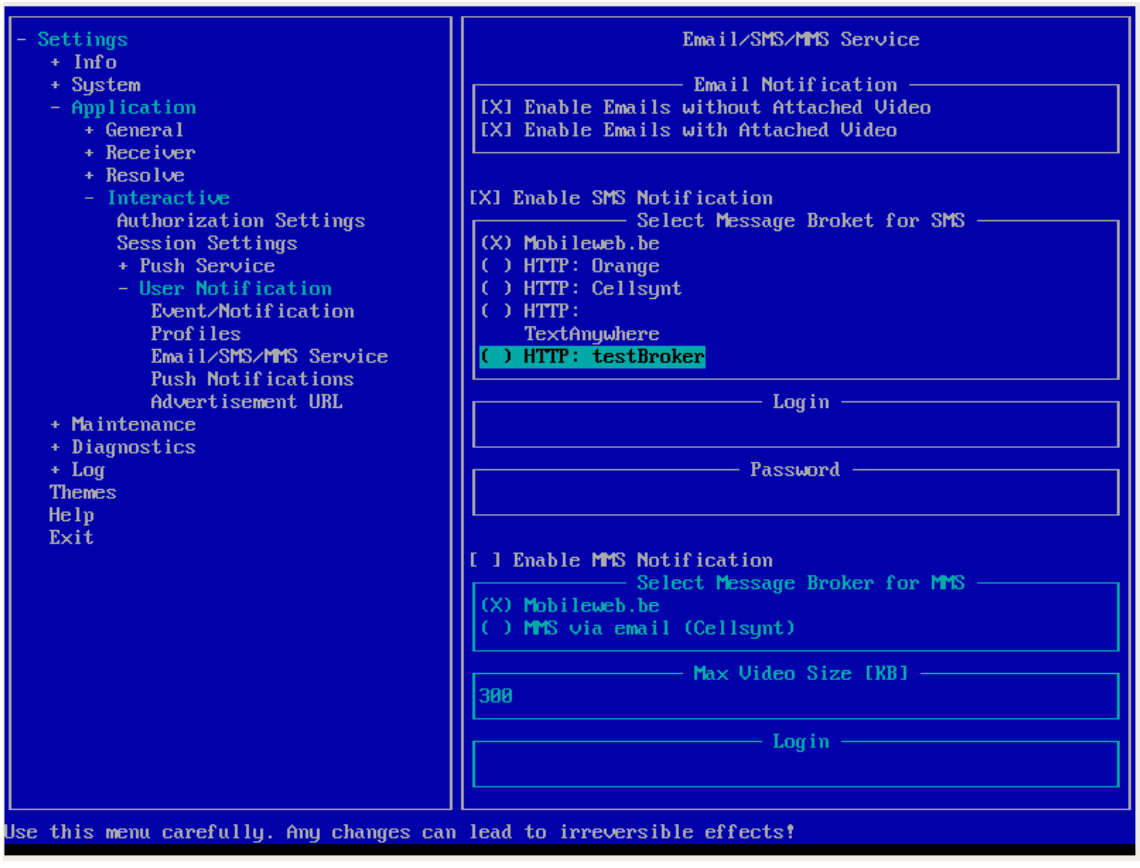
is one line and in the end of it press **Enter**, type **HTTP/1.1** and press **Enter** for new line again, and so on.
With incorrect formatting and unnecessary spaces server will fail to send messages to the broker.

Various brokers may use various specific parameters in their requests, but all of them are explained completely in each broker's HTTP API.
As a reference, any of the pre-configured messages brokers (Orange, Cellsynt, TextAnywhere) can be used.

- In MMI menu go to **Application > General > Message Brokers > Add a new broker**
- In **SMS Brokers types** set **Templated**
- In **SMS Broker name** set your broker's name
- In **SMS Broker sender** set your broker phone number. (This number will be indicated to the client as a source sender number of SMSs sent by your server)
- In **SMS Broker login** and **SMS Broker password** set login and password respectively
- In **SMS Broker host** set a hostname of your broker
- In **SMS Broker port** set a port number that is used by your broker
- In **Template of GET/POST request to send sms** set your broker's request to send outgoing SMS
  (The way how to prepare this request is explained above)
- Press **Add broker**



- ➢ Once the broker is added go to **Application > Interactive > User notification > Email/SMS/MMS Service**
- ➢ Set **Enable SMS Notification** checkbox
- ➢ In **Select Message Broker for SMS** frame select your broker name
- ➢ Press **Apply changes**



Firewall

Internal firewall in PowerManage is an out-of-the-box functionality that is implemented over Iptables Linux utility that is a tool to configure Linux kernel firewall. This functionality covers the following key objectives:

- ➢ Allow incoming connections to some specific ports from some definite networks only.
- ➢ Restrict the number of simultaneous connections to some specific value for a variety of services.

The main purpose of PowerManage firewall is to provide a handy tool that allows configuring a secure network access policies and limit simultaneous connections number to avoid the services overload.

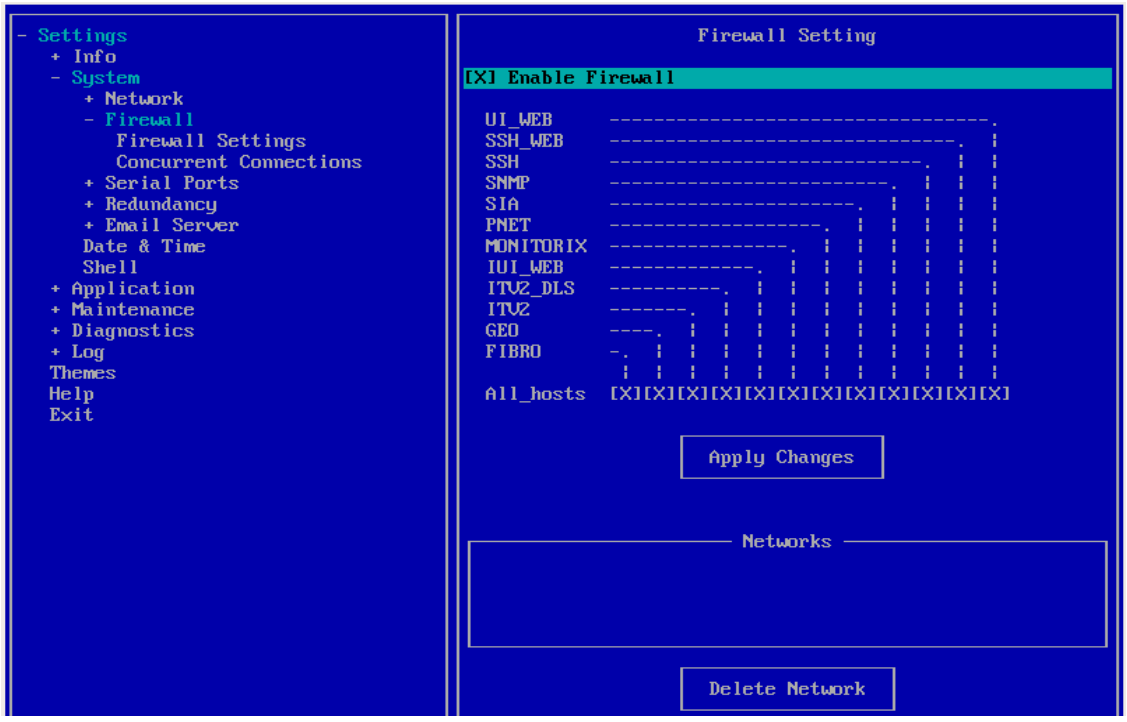
The key point is that the internal firewall is considered as supplementary measure to an external firewall. There is still an advice to use an external firewall on top of PowerManage servers. It should provide more reliable stability and avoid performance issues.

❑ *Restriction of sources for incoming connections*

Firewall is enabled right after the PowerManage installation. By default incoming connections from any IP are allowed to the corresponding TCP/UDP ports of all the services that work with a network. In such a configuration the server is fully operable, but in most of cases this configuration is redundant. It is recommended to limit the allowed source IP addresses and forbid access to services that are not used by customer.

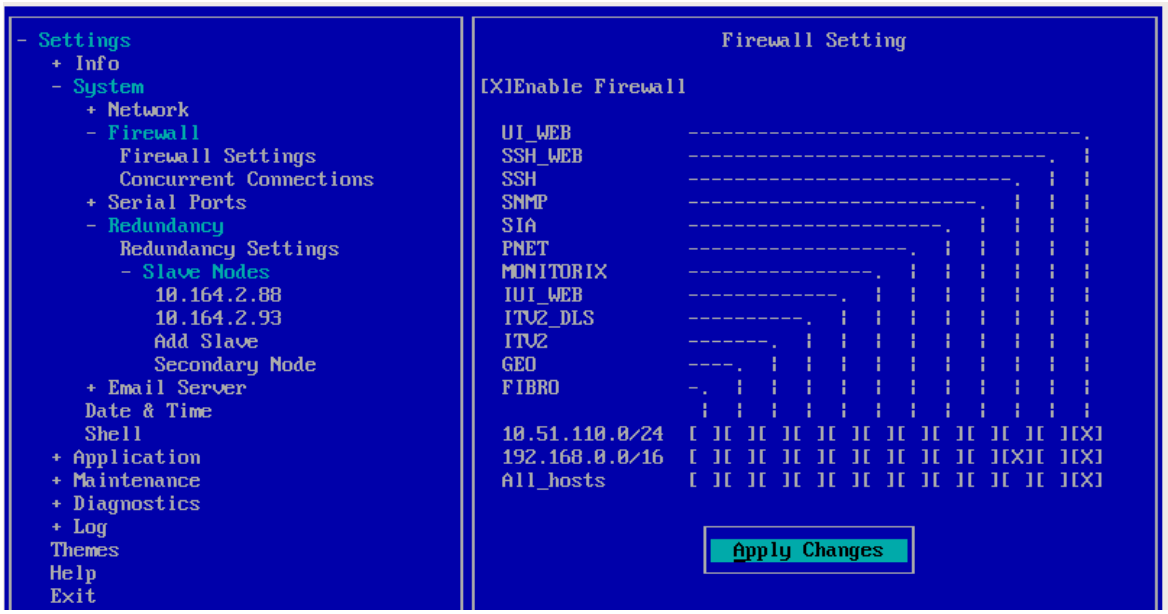
Access can be allowed or denied for services represented by a list of profiles in MMI.
There is an option to add some networks and manage access from them to PowerManage services separately.

- ➢ In MMI menu go to **System > Firewall > Firewall Settings**
- ➢ In the **Add New Network** set the network in the following format: x.x.x.x/y
- ➢ Press **Add Network**



Let's consider the following example:

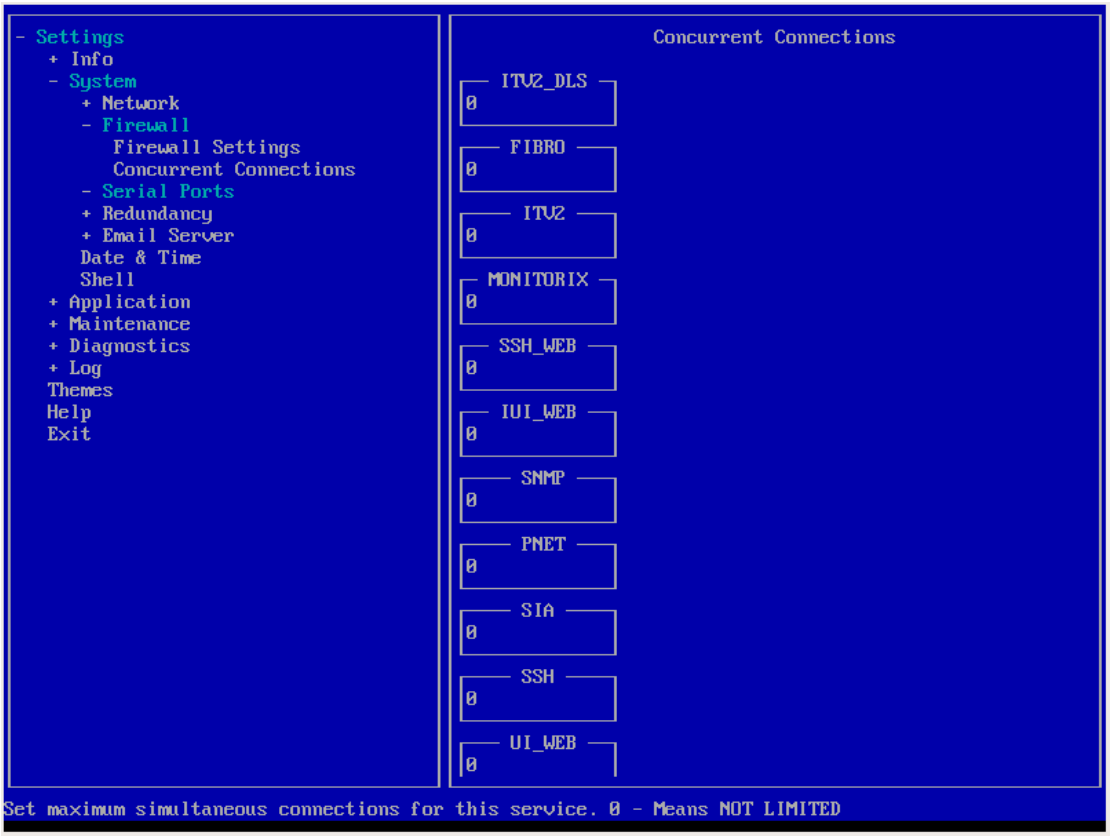
It is seen that all profiles except “GEO”, “HTTP” and “SSH” are enabled for “All_hosts”. It means that an access to the corresponding services is open from any network. “GEO” profile is disabled, it means that the ports that are used for the communication between servers in case GEO redundancy is configured are closed. SSH access is allowed only from the IP within the following networks: 10.51.110.0/24 and 192.168.0.0/16. HTTP (unsecure WEB access) is allowed from 10.51.110.0/24 network only.



- ***Restriction on a number of simultaneous connections***

There is a possibility to restrict a number of simultaneous connections to a list of services represented by the corresponding profiles in MMI. By default it is not limited (corresponds to “0” value in MMI).

It should be noted that in case the number of connections for HTTP is set to 5 it doesn’t refer to a number of opened WEB pages with PowerManage. The only thing it deals with is a number of simultaneous connections via HTTP. Within every single WEB session a few simultaneous connections can be initiated. Therefore, for one WEB session it is required to set the limit above 5 in order to avoid reject of some HTTP queries and thus cause malfunction of established session.


- Settings
+ Info
- System
+ Network
- Firewall
Firewall Settings
Concurrent Connections
- Serial Ports
+ Redundancy
+ Email Server
Date & Time
Shell
+ Application
+ Maintenance
+ Diagnostics
+ Log
Themes
Help
Exit
Concurrent Connections
ITV2_DLS
0
FIBRO
0
ITV2
0
MONITORIX
0
SSH_WEB
0
IUI_WEB
0
SNMP
0
PNET
0
SIA
0
SSH
0
UI_WEB
0
Set maximum simultaneous connections for this service. 0 - Means NOT LIMITED

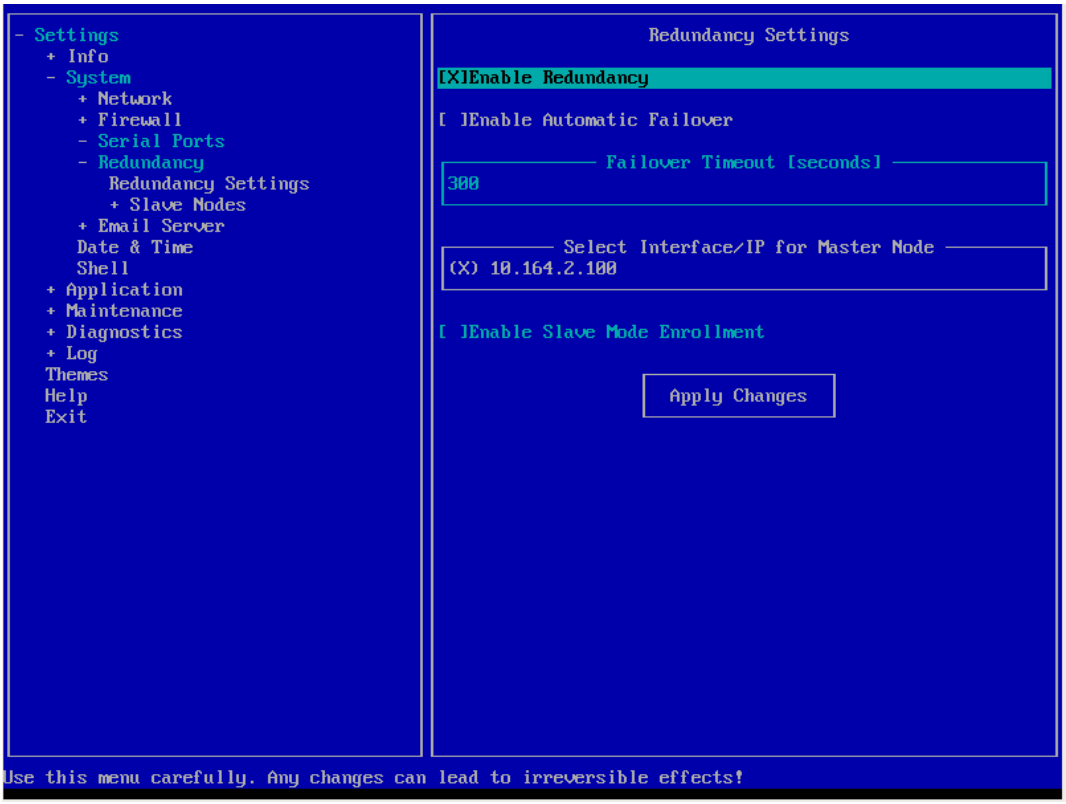
Redundancy configuration

❑ *Redundancy configuration (two nodes system)*

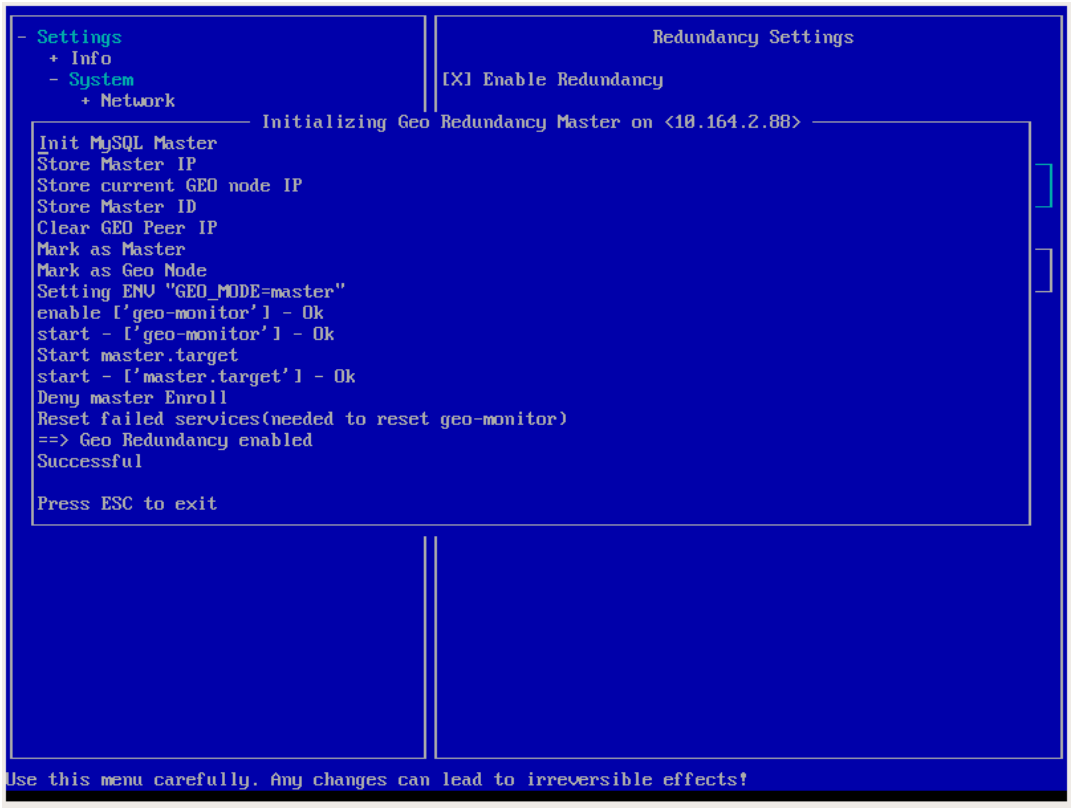
NOTE: in case there is a backup with data that is going to be restored on a new GEO redundant installation, then firstly restore must be performed on a server that is going to be used as Master and only after that GEO redundancy can be configured. It's not needed to perform restore to the Slave servers.

IMPORTANT: in GEO redundancy slave nodes have some services disabled which include WEB GUI and REST API. As far as DSC NEO panel require prior activation before panels will be able to perform a discovery process, and the activation may be done from either the WEB GUI or the user application (requires REST API) the case when the DSC NEO panel is enrolled to the secondary node only of the GEO redundant system, should be avoided. Otherwise it won't be possible to activate the panel.

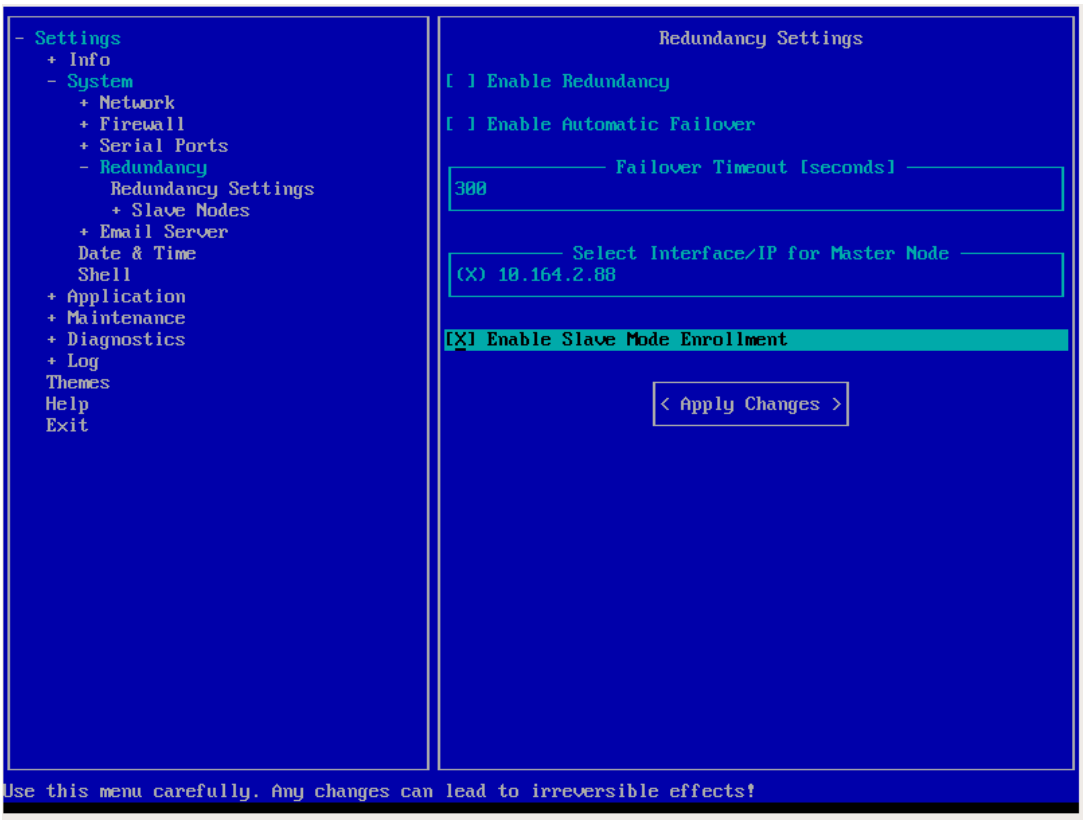
- ➢ Install servers (Check installation guide upper in same doc)
- ➢ After installation configure Central Stations for Master and Slave
- ➢ Enter MMI menu on the Master
- ➢ In **System** > **Redundancy** > **Redundancy** set **Enable Redundancy** option



- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Wait until redundancy is enabled
- ➢ Once redundancy is enabled, you'll see current node mode and Masters' IP. To view redundancy status and enrolled slaves, press **Show status** button

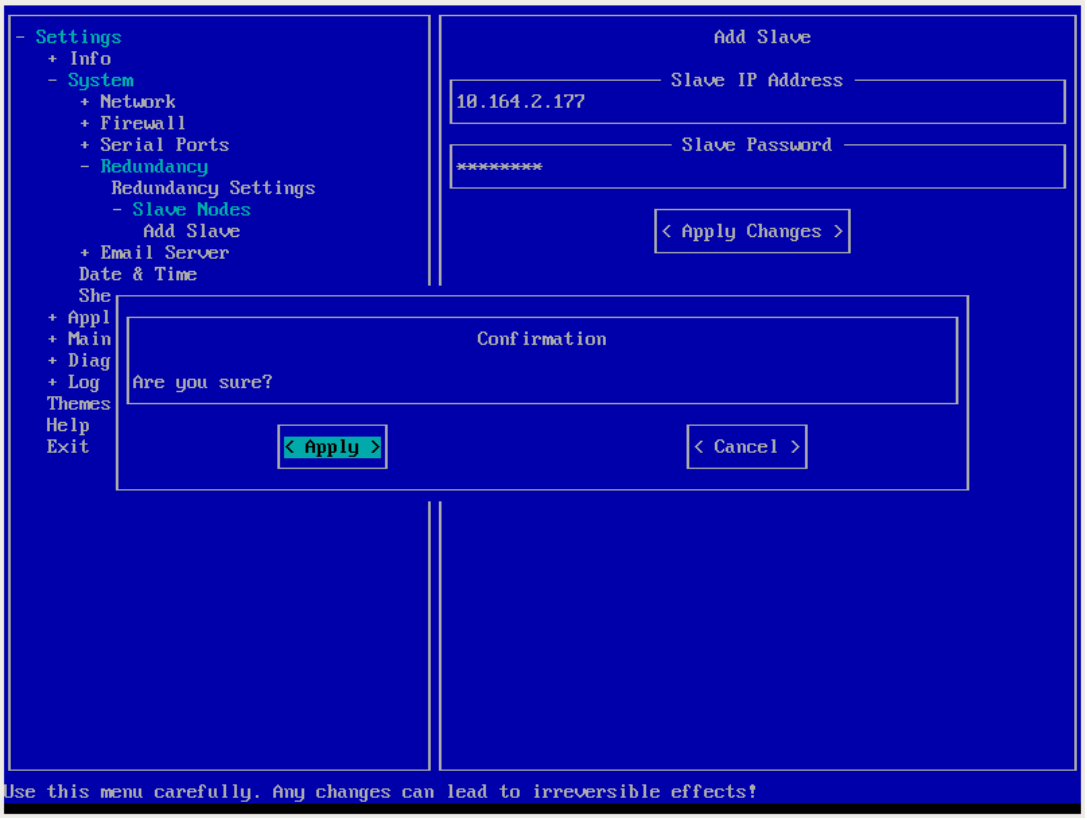


- ➢ Enter MMI menu on the Slave
- ➢ Before adding Slave, enable NTP time synchronization on Slave and Master: in MMI **System > Date & Time** enable **Automatic Date and Time [NTP]** option
- ➢ In **System** > **Redundancy** > **Redundancy Settings** set **Enable Slave Mode Enrollment** option (otherwise in case of time difference between Master and Slave is greater than 10 seconds, redundancy setup will fail)

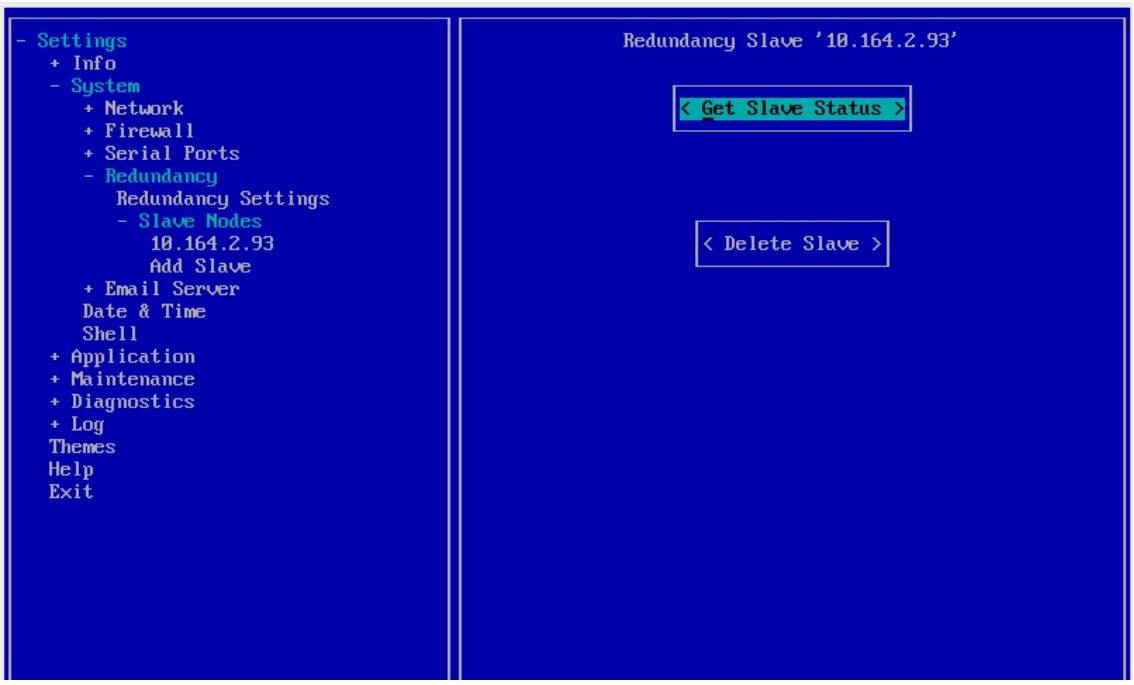


- ➢ Press **Apply Changes** button. In the dialog box press **Ok**

➢ In Masters' MMI menu go to **System** > **Redundancy** > **Slave Nodes** > **Add Slave**
➢ In **Slave IP Address** set the slaves' IP address
➢ In **Slave Password** set slaves' SSH password that was configured after installation



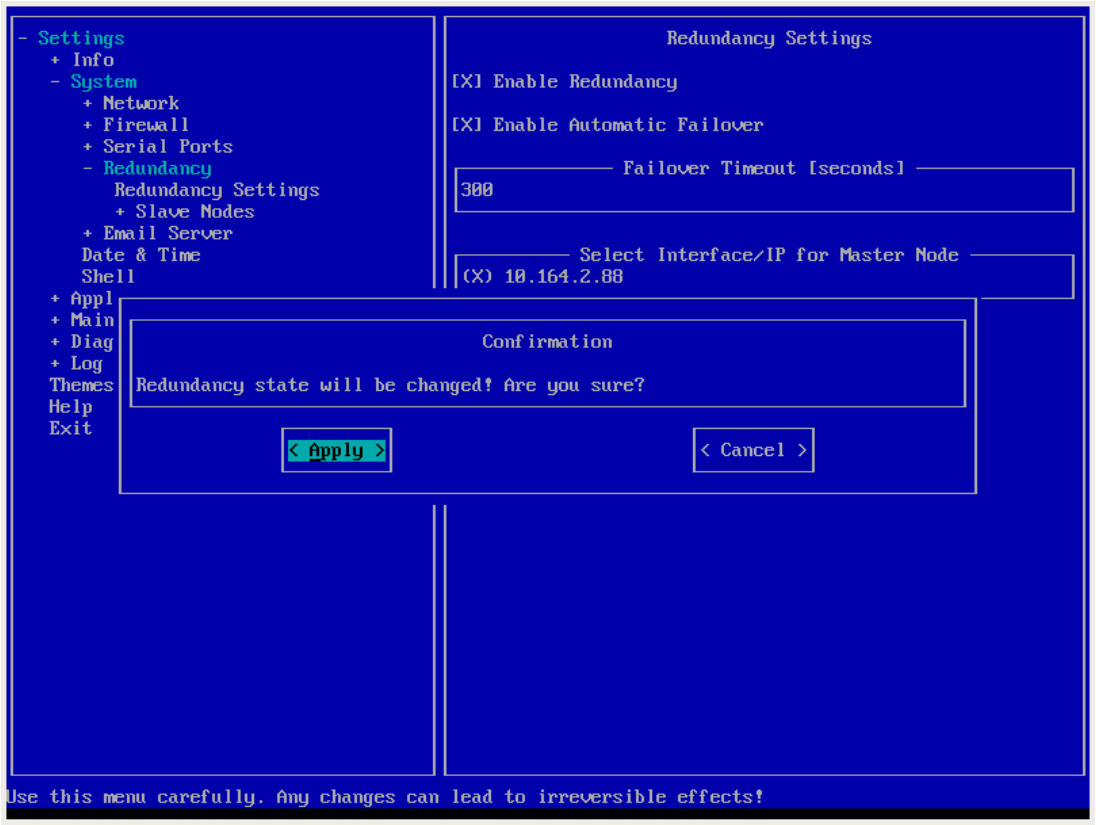
➢ Press **Apply Changes** button. In the dialog box press **Apply** again
➢ Wait until Slave is added
➢ After Slave is added, redundancy configuration is completed. Slave node is displayed in Masters' MMI menu **System** > **Redundancy** > **Redundancy Settings** > **Slave Nodes**
➢ You can view Slave status by pressing **Get Slave Status**



• *Automatic Failover (two nodes system)*

When configuring the redundancy, there is an option to enable the automatic failover in case of Master server fail.
When the redundancy is configured with the automatic failover, there are a health check services enabled on both Master and Primary slave nodes that check availability of the Master server.
In case when Master server fails or becomes unavailable, the Primary slave server disables the redundancy, brings up Masters' database and enables the redundancy again, but configures itself as a Master server.

- In **System** > **Redundancy** > **Redundancy** set **Enable Redundancy** option
- Set Enable Automatic Failover option
- Press **Apply Changes** button. In a dialog box press **Apply** again
- Wait until redundancy is enabled



• *Manual Failover actions*

- Enter Masters' MMI and in **System** > **Redundancy** > **Redundancy Settings** disable **Enable Redundancy** option and press **Apply**
- Exit MMI menu and login again
- Enter MMI menu on the Slave
- In **System** > **Redundancy** > **Redundancy Settings** disable **Enable Redundancy** option and press **Apply**
- Wait until redundancy is disabled
- In the popup press **OK**
- Exit MMI menu and login again
- In **System** > **Redundancy** > **Redundancy Settings** set **Enable Redundancy** option
- Press **Apply Changes** button. In a dialog box press **Apply** again
- Wait until redundancy is enabled
- Enter former Masters' (it's gonna be configured as a slave after it fails) MMI menu
- In **System** > **Redundancy** > **Redundancy Settings** set **Enable Slave Mode Enrollment**

option

- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Open new Masters' MMI menu
- ➢ In **System** > **Redundancy** > **Slave Nodes > Add Slave** add Slave (IP address and ssh password of former Master)
- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Wait until Slave is added

• *Redundancy configuration (4 nodes system)*

NOTE: in case there is a backup with data that is going to be restored on a new GEO redundant installation, then firstly restore must be performed on a server that is going to be used as Master and only after that GEO redundancy can be configured. It's not needed to perform restoration on Slave servers.

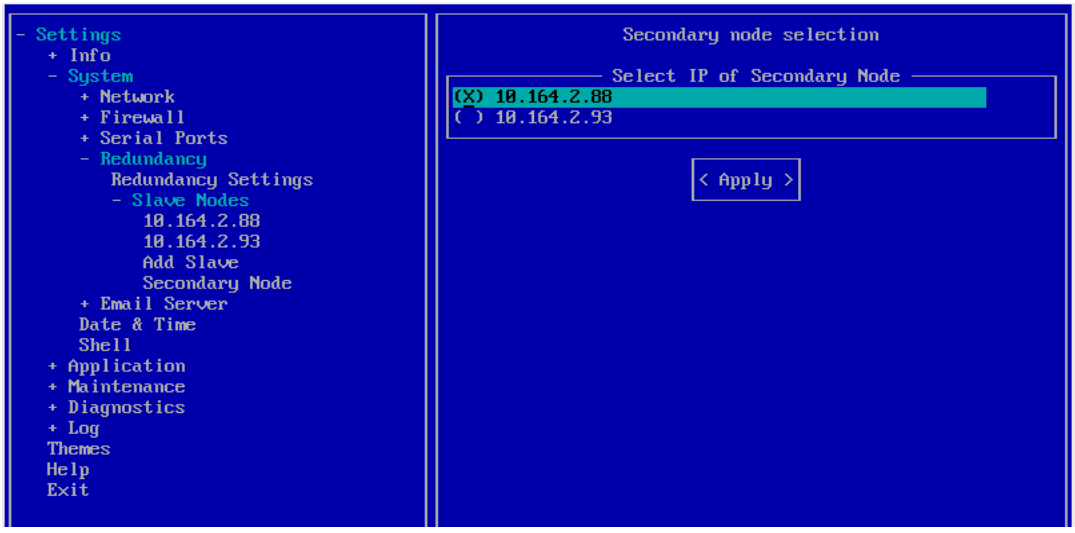
IMPORTANT: in GEO redundancy slave nodes have some services disabled which include WEB GUI and REST API. As far as DSC NEO panel require prior activation before panels will be able to perform a discovery process, and the activation may be done from either the WEB GUI or the user application (requires REST API) the case when the DSC NEO panel is enrolled to the secondary node only of the GEO redundant system, should be avoided. Otherwise it won't be possible to activate the panel.

The redundancy configuration provides ability to add as much Slaves as it's needed. The only necessary thing is that one GEO site must have one Master configured and another site must have Primary Slave designated all other servers will be usual Slaves.

Four nodes configuration is described as far as it's the most prevalent configuration among the clients.

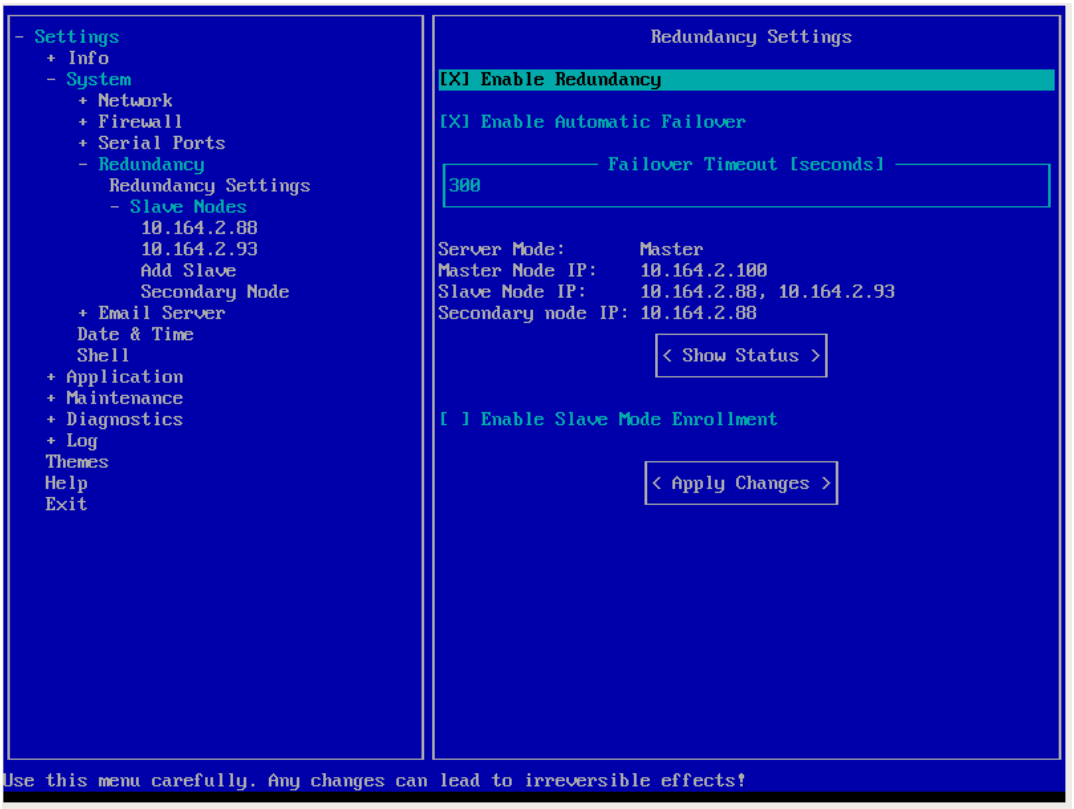
In case of automatic failover was enabled for the redundancy, the Primary slave node disables the redundancy, brings up the former Master database and enables the redundancy, but in this time it sets itself as a Master server. Once the redundancy enabled, new Master server designates new Primary slave among the healthy slave servers and adds it to the redundancy. All the rest of available servers are added as a slave servers.

In case of manual failover configuration, the failover has to be performed in a familiar way as for two nodes redundancy in case of Master fail. Primary Slave should be re-configured as Master and new Primary Slave should be designated. Primary Slave can be configured in **System** > **Redundancy** > **Slave Nodes** > **Secondary Node**.



- ➢ Install servers

- After installation configure Central Stations for Master and all Slaves
- Enter MMI menu on the Master
- In **System** > **Redundancy > Redundancy Settings** set **Enable Redundancy** option
- Press **Apply Changes** button. In a dialog box press **Apply** again
- Wait until redundancy is enabled
- Once redundancy is enabled, you'll see current node mode and Master's' IP. To view redundancy status and enrolled slaves, press **Show status** button
- Enter MMI menu on each Slave
- For each Slave in **System** > **Redundancy > Redundancy Settings** set **Enable Slave Mode Enrollment** option
- Press **Apply Changes** button. In the dialog box press **Apply** again
- In Masters' MMI menu go to **System** > **Redundancy** > **Slave Nodes** > **Add Slave**
- Before adding Slaves, enable NTP time synchronization on every Slave and Master: in MMI **System > Date & Time** enable **Automatic Date and Time [NTP]** option and press **Apply Changes**
- Add every Slave node with its IP and SSH password
- After all Slaves are added you can check them in **System** > **Redundancy Settings** > **Slave Nodes**



- After more than one Slave is enrolled to Master in its MMI menu appear option **System** > **Redundancy** > **Redundancy Settings** > **Slave Nodes** > **Secondary Node** that allows to assign Primary Slave manually (by default the first Slave enrolled to Master is assigned as Primary Slave).

• *Automatic failover (four nodes system):*

In case of automatic failover was enabled for the redundancy, the Primary slave node disables the

redundancy, brings up the former Master database and enables the redundancy, but in this time it sets itself as a Master server. Once the redundancy enabled, new Master server designates new Primary slave among the healthy slave servers and adds it to the redundancy. All the rest of available servers are added as a slave servers.

• *Manual Master failover actions:*

In case of Master failed client able to decide what server will be new Master. It could be any of other 3+ servers (f.e. Primary_slave from remote side or usual Slave from the same side).
After manual reconfiguration of GEO system it is a must to make a change on client firewall and redirect all traffic to the new Master and Primary_slave on another side (if it was changed).
It is highly recommended to configure Master on the same side otherwise it will be difficult to redirect traffic from failed node to the new one also less manual actions need to be performed and IP receivers will not be switched for the panel.

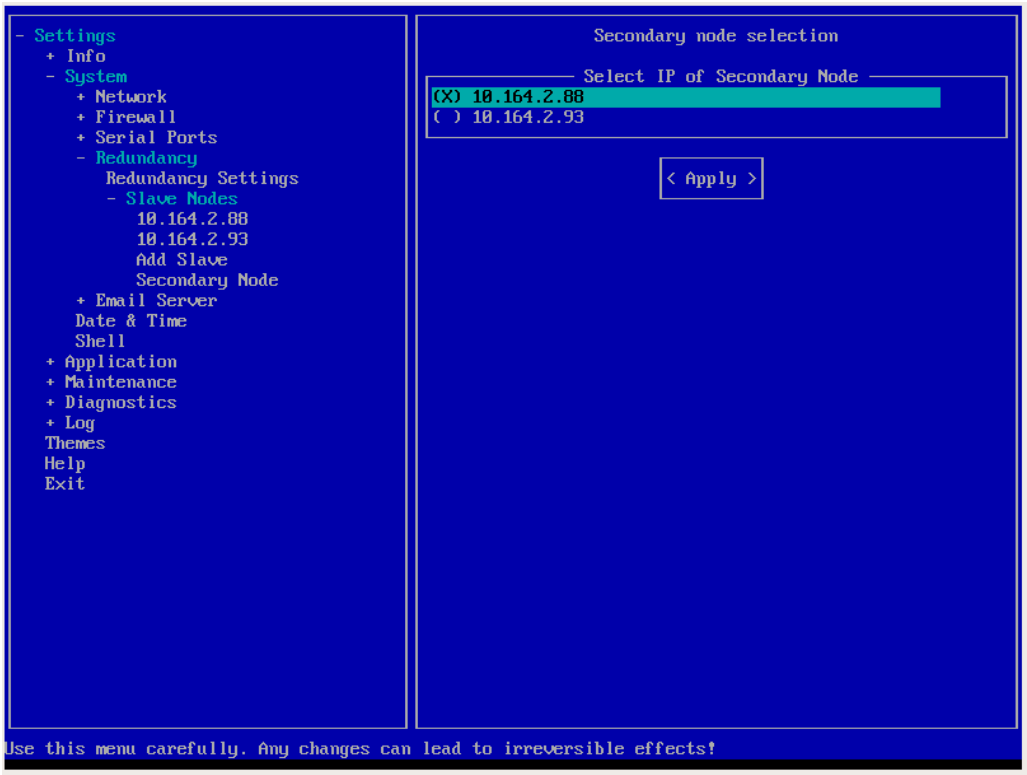
- ➢ Enter Primary Slave ' MMI and in **System** > **Redundancy** > **Redundancy Settings** disable **Enable Redundancy** option and press **Apply Changes**
- ➢ Exit MMI menu and login again
- ➢ For each Slave and former Master disable redundancy in **System** > **Redundancy** > **Redundancy Settings**
- ➢ Wait until redundancy is disabled
- ➢ In the popup press **OK**

- ➢ Exit MMI menu and login again for each node
- ➢ In Primary Slaves' MMI menu go to **System** > **Redundancy** > **Redundancy Settings** set **Enable Redundancy** option
- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Wait until redundancy is enabled
- ➢ For each Slave node and former Master in **System** > **Redundancy** > **Redundancy Settings** set **Enable Slave Mode Enrollment** option
- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Open new Masters' MMI menu
- ➢ In **System** > **Redundancy** > **Redundancy Settings** > **Slave Nodes** add every Slave (IP address and ssh password of former Master)
- ➢ Press **Apply Changes** button. In a dialog box press **Apply** again
- ➢ Wait until Slave is added

• *Manual Primary Slave failover actions:*

In case of Primary_slave fails it is a need to reconfigure new Primary_slave on the Master node in Masters' MMI menu **System** > **Redundancy** > **Redundancy Settings** > **Slave Nodes** > **Secondary Node** (see picture below). And redirect all traffic to the new Primary slave.

It is highly recommended to select new Primary_slave on the same side it was before otherwise it will be difficult to redirect traffic from failed node to the new one.



Appendix-A

SSL certification

Power Manage IV supports HTTPS secure communication. To use this secure communication, a Secure Sockets Layer (SSL) certificate must be purchased and installed on the PowerManage server.

- ➢ Submit a request to the IT department or Internet Service Provider (ISP) to register the PowerManage server host name for example: marketing.visonic.com.

- ➢ Create a file and record the following values:
    - ○ A passphrase or password that is used for encryption. It is best to use a combination of numbers and letters (english alphabet). You can use lowercase letters, uppercase letters or both. The use of special characters is not supported.
    - ○ A two letter country code, for example *UK*.
    - ○ A state or province name. If not applicable you can use the country name.
    - ○ A locality name (region, city), for example *London.*
    - ○ An organization name, for example Visonic
    - ○ Optional: organizational unit name (section or department).
    - ○ Common name, such as company name or the hostname of the server, for example marketing.visonic.com.
    - ○ Optional: email address.
- ➢ Send the hostname of the PowerManage server and the file from step 2 to Visonic. Visonic generates a certification request and returns a public.csr file and a private.key file.
- ➢ Send the public.csr file and the applicable payment to a certification authority (CA). The CA returns the signed certificate such as *.crt file.
- ➢ Send the signed, validated certificate to Visonic and include the original CA email.
- ➢ Visonic uploads the certificate to the repository, which adds HTTPS support to the PowerManage server.

NOTE: The certificate consists of a .crt and .key file, which contains critical security parameters. You should store the .key file in encrypted (passphrase-wrapped) form. You should keep both files together. Ensure that you keep track of the certification expiration and renewal date.