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.

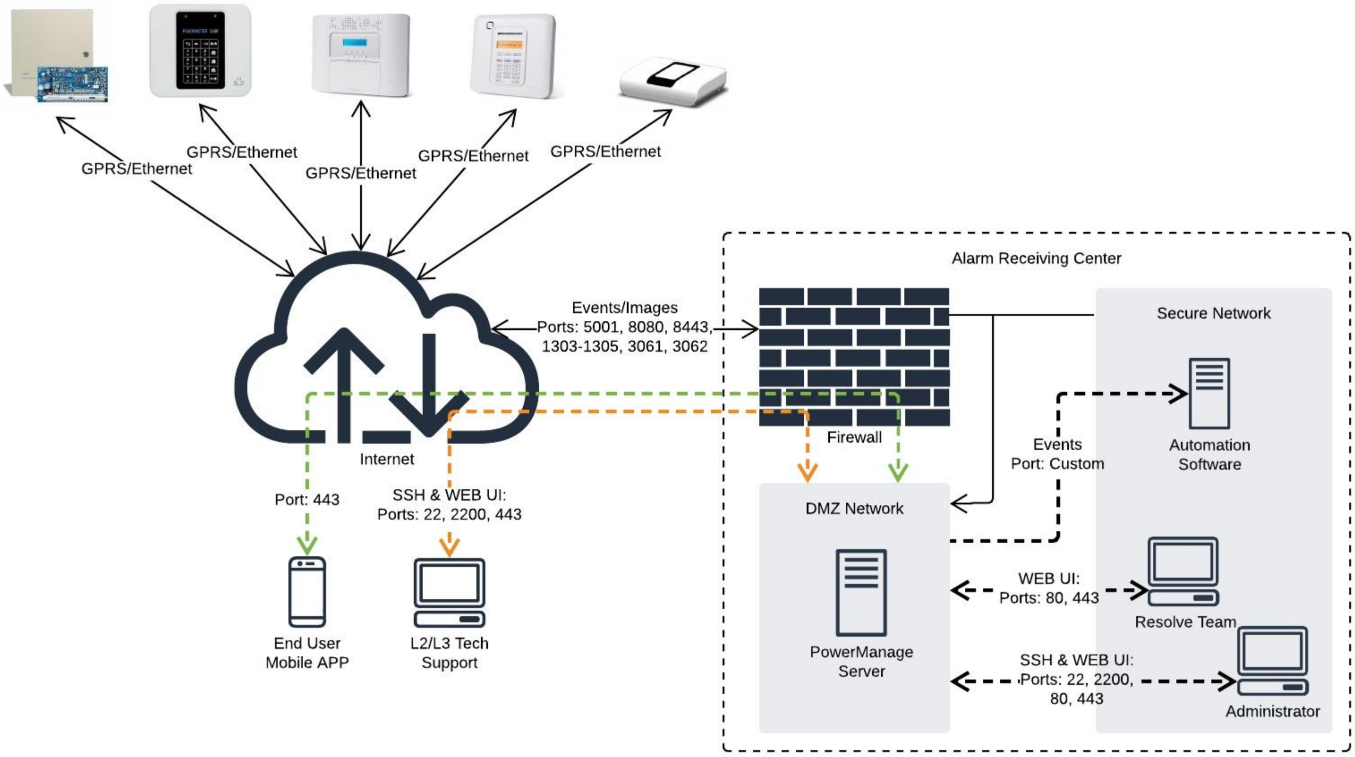
The customer is required to read the relevant sections throughout the entire document and to verify to the point of contact at Tyco/Visonic that all of the requirements will be met on the installation date.
A moderate level of server-based knowledge and experience is assumed**.**

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.

The firewall must support required connections limit **R** [in new connections per second], which depends on panels KA configuration. **R** can be estimated by the following equation:

$$\mathbf{R} \approx (\mathbf{N}_{\mathbf{GPRS}} + \mathbf{N}_{\mathbf{BBA}})*5,$$

where
$\mathbf{N}_{\mathbf{GPRS}}$ - number of GPRS panels enrolled to the server,
$\mathbf{N}_{\mathbf{BBA}}$ - number of BBA panels.

NOTE: The highest concurrent connections number is reached in case when all panels are switched to a new server and, therefore, the discovery process starts on all of them simultaneously. At the same time during normal operation this value is a few times lower than the aforementioned limit.

A DNS hostname with A and PTR records is required to reach the PowerManage instance from e.g. mobile clients.

There is a number of services on PowerManage that initiate outbound connections. This includes public services like NTP, DNS, FTP, SMTP, etc; configurable external services like SMS brokers, Central Stations, Push Notification providers, etc. All outbound connections are initiated from source port range **27000-65333**. It is required to allow all egress traffic to avoid blocking of the needed connections.

Bandwidth requirement:

- Minimum 5 Mbit/sec incoming/outcoming for low cost systems;
- Minimum 10 Mbit/sec incoming/outcoming for mid performance systems;
- Minimum 100 Mbit/sec incoming/outcoming for high performance systems.

NOTE: PowerManage requires a dedicated link. Any third-party services shouldn’t use this link.

Table-1.1 - the complete list of inbound ports to be forwarded from the firewall to the server:

Port	Protocol	Description
PM Panels ports		
5001	TCP/UDP	Alarm signals/Resolve
8080	TCP/UDP	Alarm images

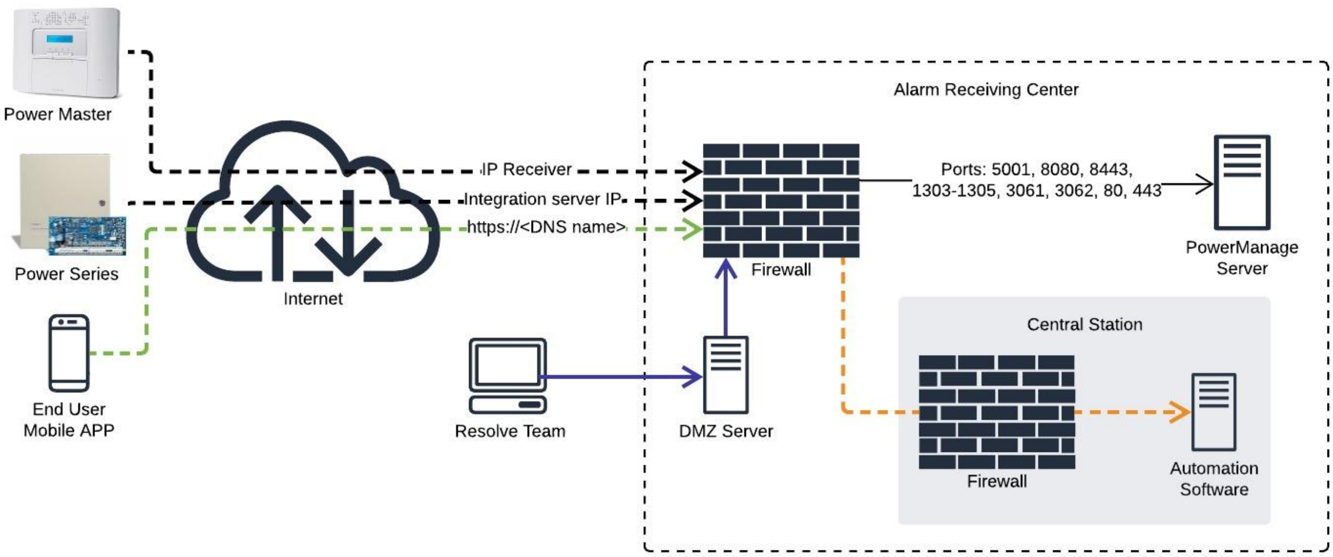
8443	TCP/UDP	Alarm images [secured]
5555	TCP/UDP	Offline handler [in case of GEO only]
NEO Panels ports		
3061-3062	TCP	Fibro Alarms
1303-1304	TCP	ITv2 Alarms/Resolve
1305	TCP	DLS Resolve
Web interface		
80	HTTP	Resolve Web interface
443	HTTPS	Resolve Web interface SSL
2200	HTTPS	Web MMI console
8087	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

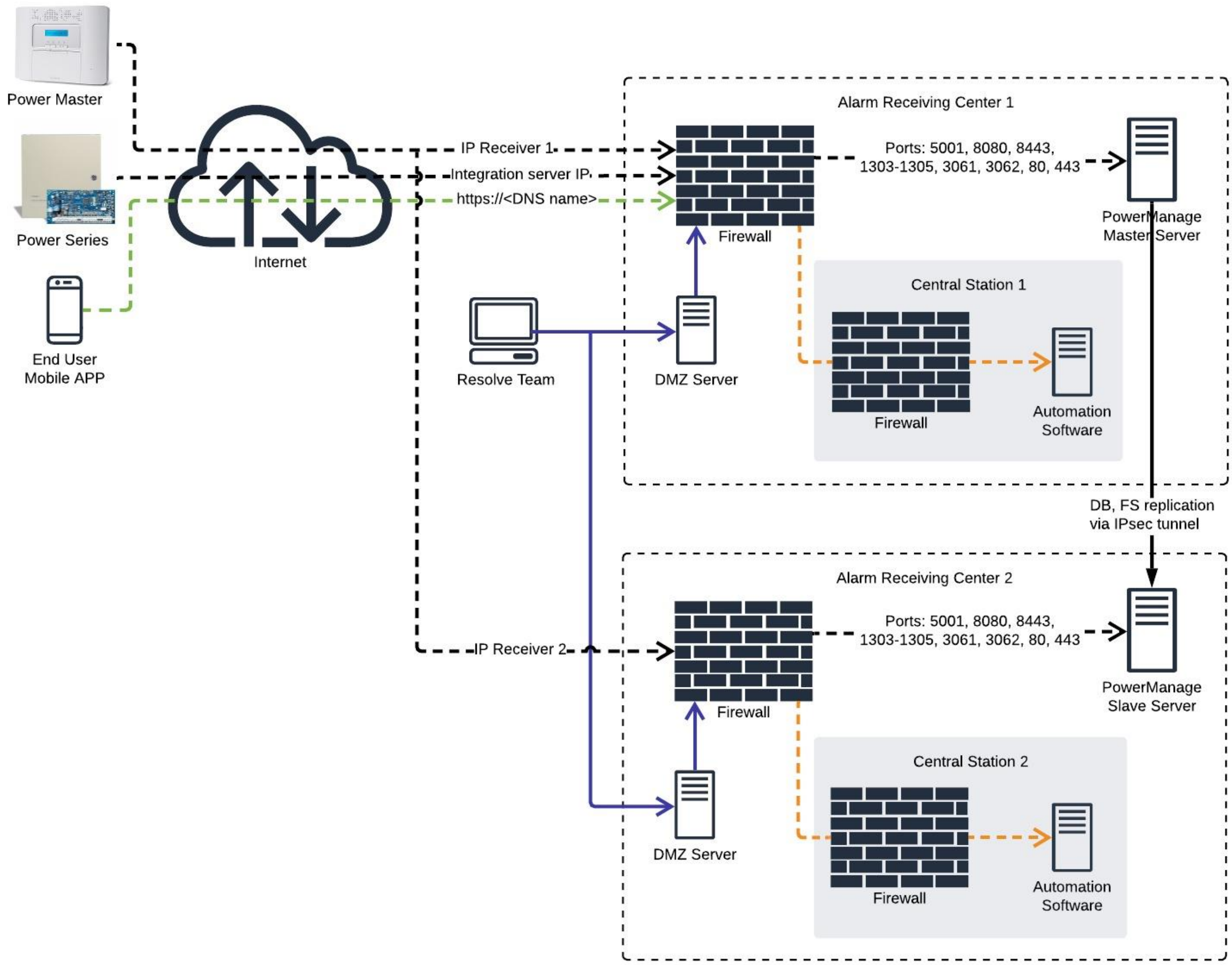
Make sure you have enough room in your designated server rack for a 2U sized server and at least one free power outlet. A second power outlet is recommended as the server has two redundant power supplies. More outlets may be required according to the server configuration that is explained in this document.

Network schematics

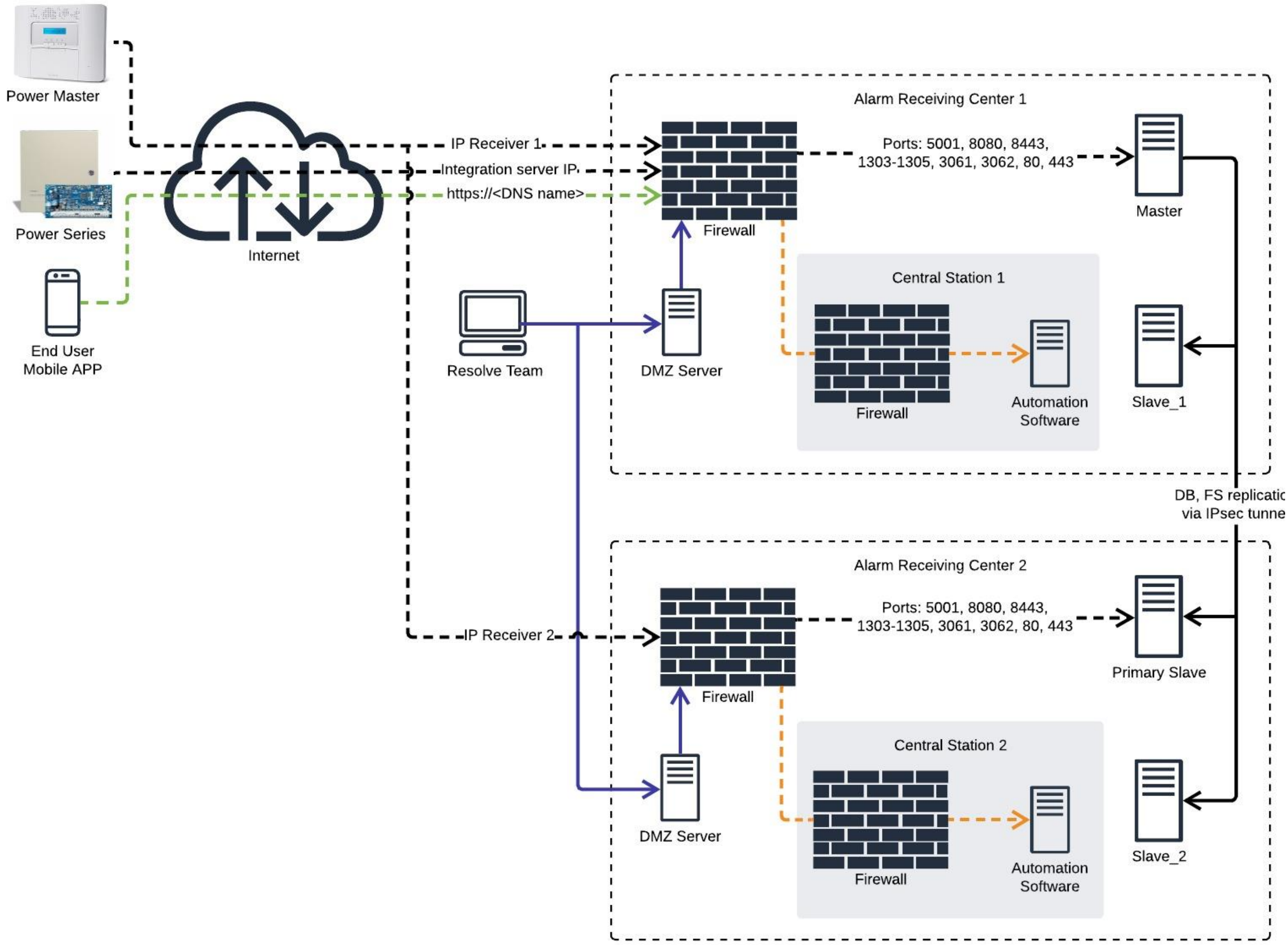
❑ ***Cost Effective - standalone diagram***



❑ *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

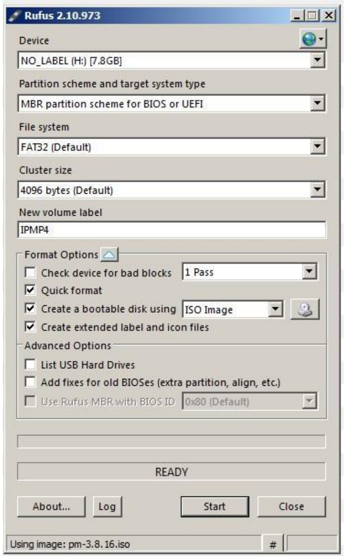
❖ USB image

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**



Rufus 2.10.973

Device: NO_LABEL (H:) [7.8GB]

Partition scheme and target system type: MBR partition scheme for BIOS or UEFI

File system: FAT32 (Default)

Cluster size: 4096 bytes (Default)

New volume label: IPMP4

Format Options

- ☐ Check device for bad blocks: 1 Pass
- ☑ Quick format
- ☑ Create a bootable disk using: ISO Image
- ☑ Create extended label and icon files

Advanced Options

- ☐ List USB Hard Drives
- ☐ Add fixes for old BIOSes (extra partition, align, etc.)
- ☐ Use Rufus MBR with BIOS ID: 0x80 (Default)

READY

Using image: pm-3.8.16.iso

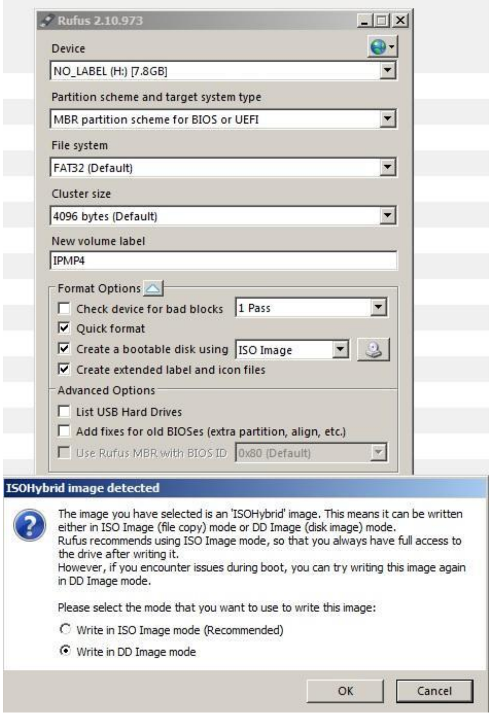
➢ In Device field select your USB drive

➢ 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



Rufus 2.10.973

Device: NO_LABEL (H:) [7.8GB]

Partition scheme and target system type: MBR partition scheme for BIOS or UEFI

File system: FAT32 (Default)

Cluster size: 4096 bytes (Default)

New volume label: IPMP4

Format Options

- ☐ Check device for bad blocks: 1 Pass
- ☑ Quick format
- ☑ Create a bootable disk using: ISO Image
- ☑ Create extended label and icon files

Advanced Options

- ☐ List USB Hard Drives
- ☐ Add fixes for old BIOSes (extra partition, align, etc.)
- ☐ Use Rufus MBR with BIOS ID: 0x80 (Default)

ISOHybrid image detected

The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode.
Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it.
However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

- ○ Write in ISO Image mode (Recommended)
- ● Write in DD Image mode

❑ *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:

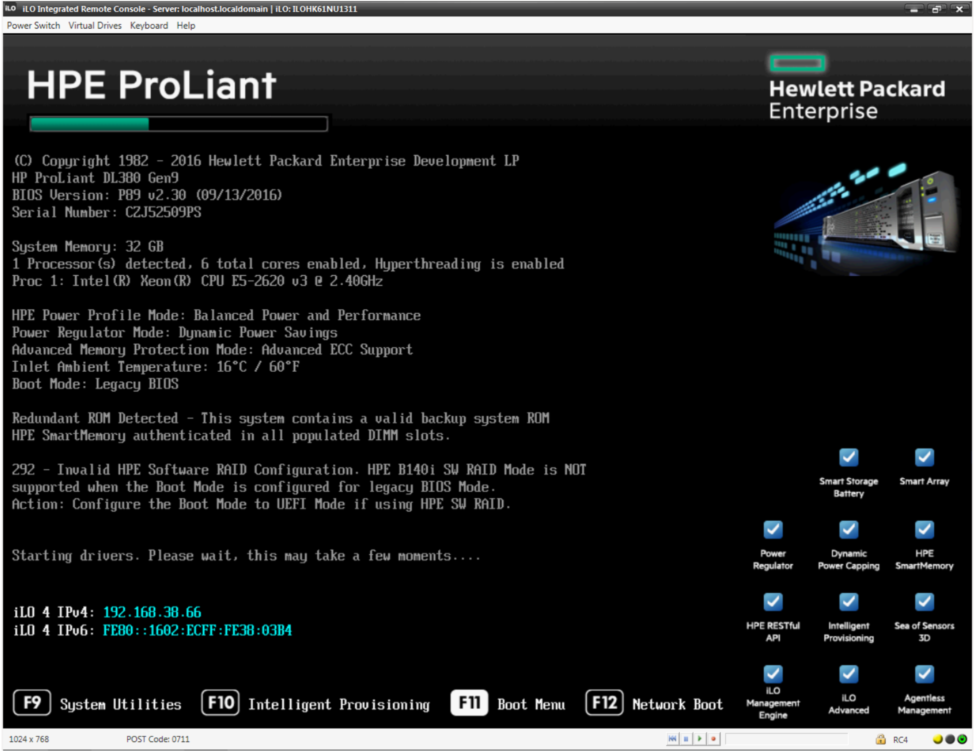
- Attach or insert the USB media
- Open new terminal [all the following might be allowed under sudo user only
- In terminal type the following command: **fdisk -l** to locate your USB device
- Switch to the directory with Power Manage ISO image
- Type the following command: **dd bs=1M if=<image.iso>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

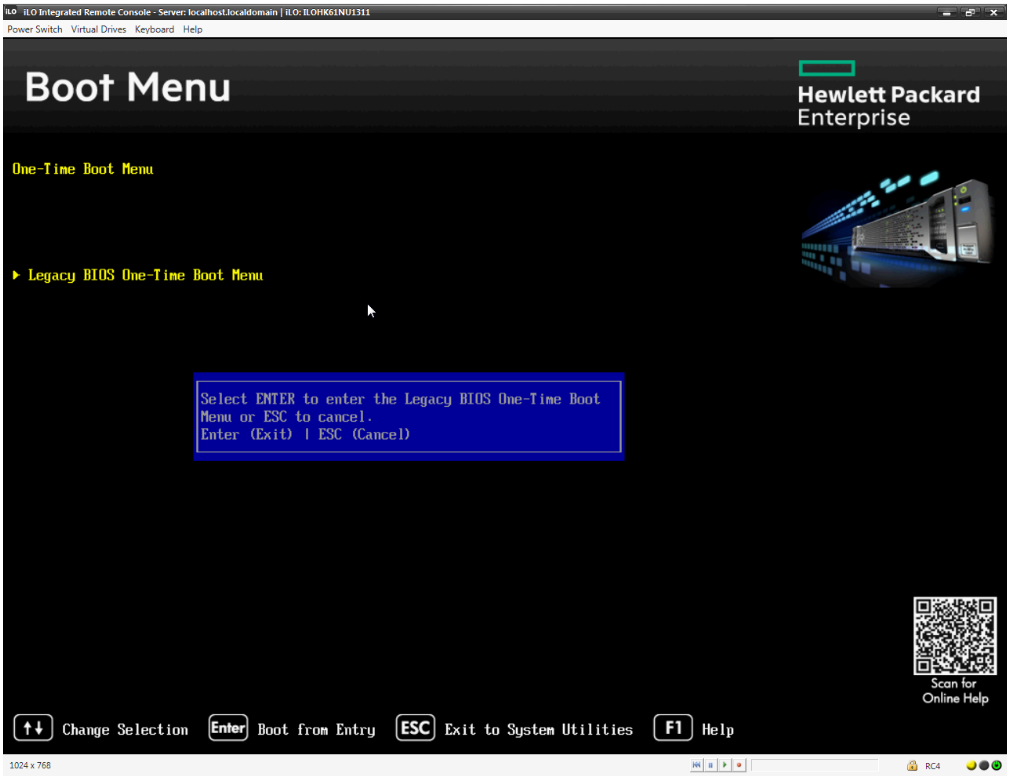
❑ *Power Manage installation on HP equipment*

- 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



```
(C) Copyright 1982 - 2016 Hewlett Packard Enterprise Development LP
HP ProLiant DL380 Gen9
BIOS Version: P89 v2.30 (09/13/2016)
Serial Number: CZJ52509PS

System Memory: 32 GB
1 Processor(s) detected, 6 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz

HPE Power Profile Mode: Balanced Power and Performance
Power Regulator Mode: Dynamic Power Savings
Advanced Memory Protection Mode: Advanced ECC Support
Inlet Ambient Temperature: 16°C / 60°F
Boot Mode: Legacy BIOS

Redundant ROM Detected - This system contains a valid backup system ROM
HPE SmartMemory authenticated in all populated DIMM slots.

292 - Invalid HPE Software RAID Configuration. HPE B140i SW RAID Mode is NOT
supported when the Boot Mode is configured for legacy BIOS Mode.
Action: Configure the Boot Mode to UEFI Mode if using HPE SW RAID.


Starting drivers. Please wait, this may take a few moments....


iLO 4 IPv4: 192.168.38.66
iLO 4 IPv6: FE80::1602:ECFF:FE38:03B4

F9 System Utilities   F10 Intelligent Provisioning   F11 Boot Menu   F12 Network Boot
```

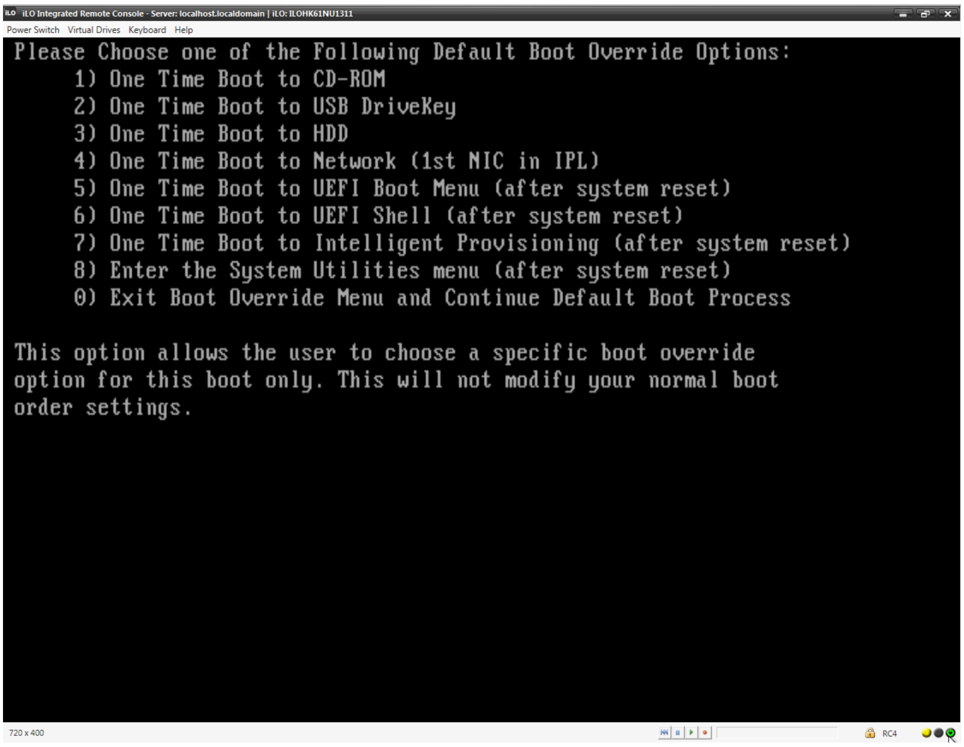
- Select Legacy BIOS One-Time Boot Menu and press Enter
- When dialog appears press Enter.


iLO Integrated Remote Console - Server: localhost.localdomain | iLO: ILOHK61NU1311
Power Switch Virtual Drives Keyboard Help
Hewlett Packard Enterprise
Scan for Online Help
↑↓ Change Selection
Enter Boot from Entry
ESC Exit to System Utilities
F1 Help
1024 x 768
RC4

```
Boot Menu

One-Time Boot Menu

▸ Legacy BIOS One-Time Boot Menu

Select ENTER to enter the Legacy BIOS One-Time Boot
Menu or ESC to cancel.
Enter (Exit) | ESC (Cancel)
```

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

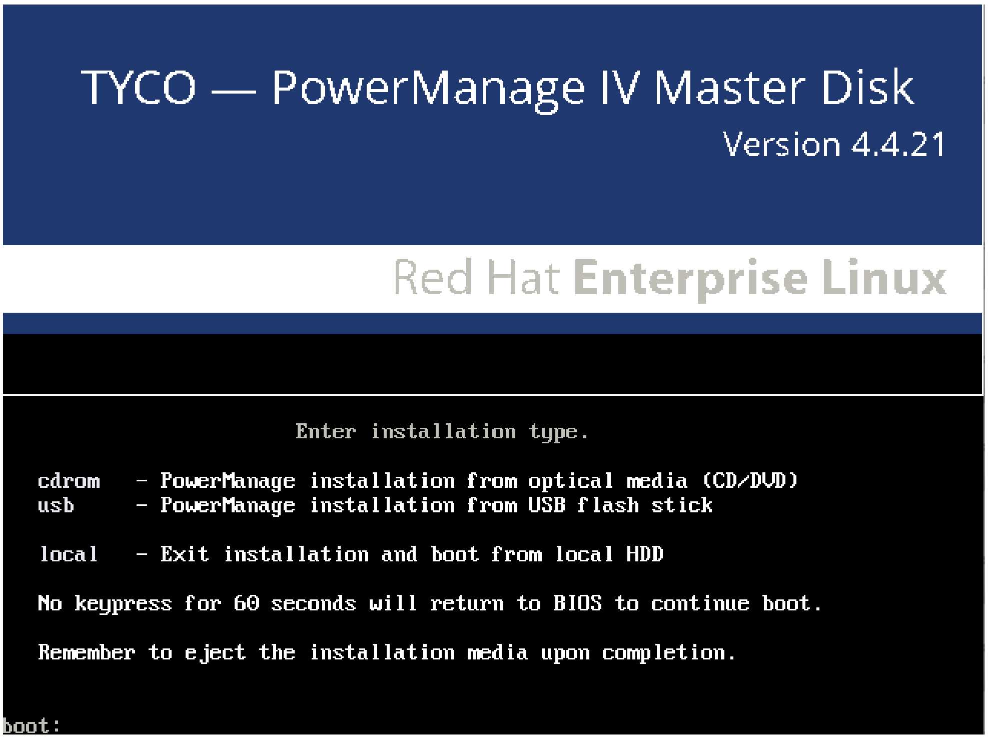
- **One Time Boot to CD-ROM**;
- **One Time Boot to USB DriveKey.**


iLO Integrated Remote Console - Server: localhost.localdomain | iLO: ILOHK61NU1311
Power Switch Virtual Drives Keyboard Help
720 x 400
RC4

```
Please Choose one of the Following Default Boot Override Options:
     1) One Time Boot to CD-ROM
     2) One Time Boot to USB DriveKey
     3) One Time Boot to HDD
     4) One Time Boot to Network (1st NIC in IPL)
     5) One Time Boot to UEFI Boot Menu (after system reset)
     6) One Time Boot to UEFI Shell (after system reset)
     7) One Time Boot to Intelligent Provisioning (after system reset)
     8) Enter the System Utilities menu (after system reset)
     0) Exit Boot Override Menu and Continue Default Boot Process

This option allows the user to choose a specific boot override
option for this boot only. This will not modify your normal boot
order settings.
```

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

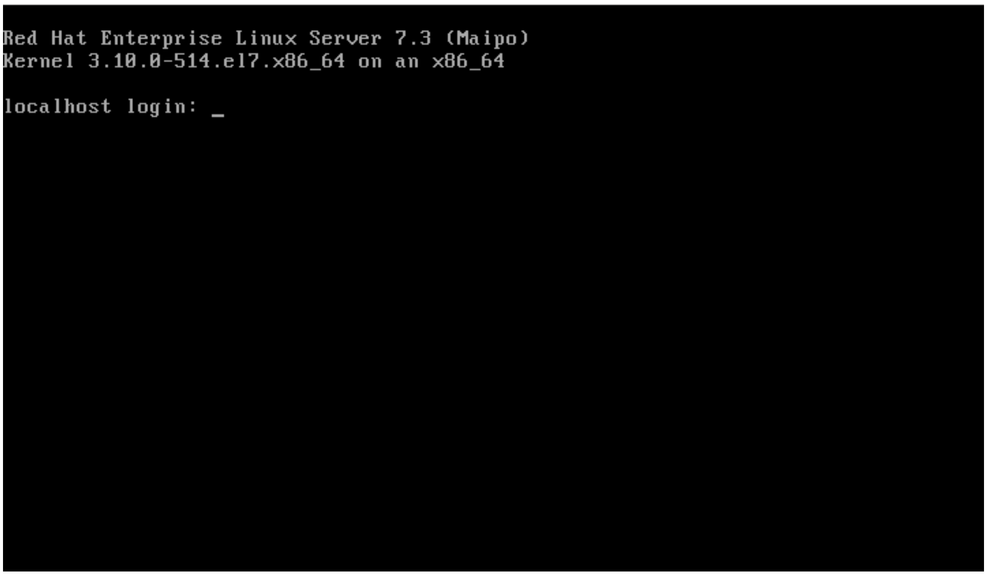


TYCO — PowerManage IV Master Disk
Version 4.4.21
Red Hat **Enterprise Linux**

```
                        Enter installation type.

  cdrom    - PowerManage installation from optical media (CD/DVD)
  usb      - PowerManage installation from USB flash stick

  local    - Exit installation and boot from local HDD

  No keypress for 60 seconds will return to BIOS to continue boot.

  Remember to eject the installation media upon completion.


boot:
```

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

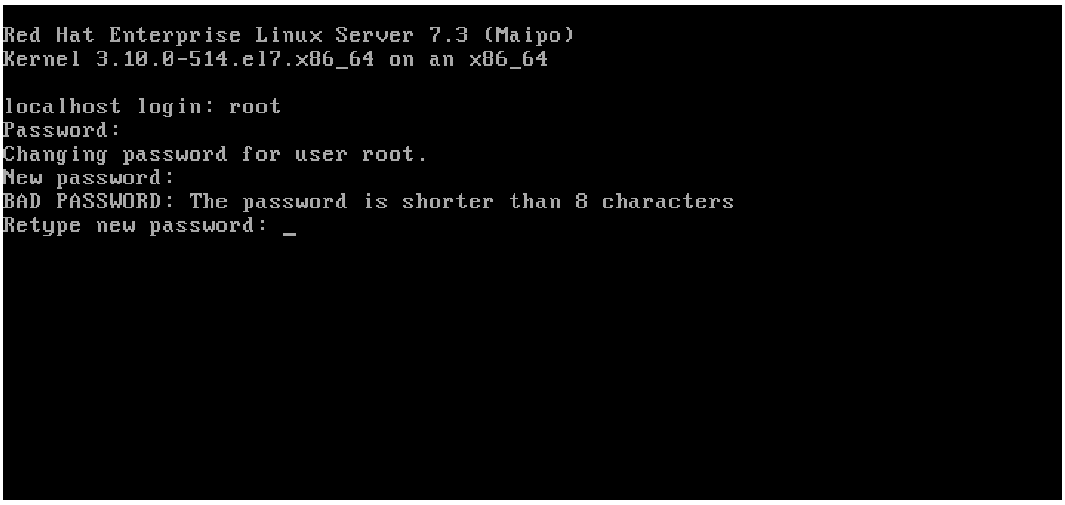
- Wait until the installation is completed.
- Once installation is completed, server restarts and appears a screen that prompts you to login [login - **root,** password - **visonic.]**
  Note: Don’t forget to unplug the DVD / USB stack after the reboot process



```
Red Hat Enterprise Linux Server 7.3 (Maipo)
Kernel 3.10.0-514.el7.x86_64 on an x86_64

localhost login: _
```

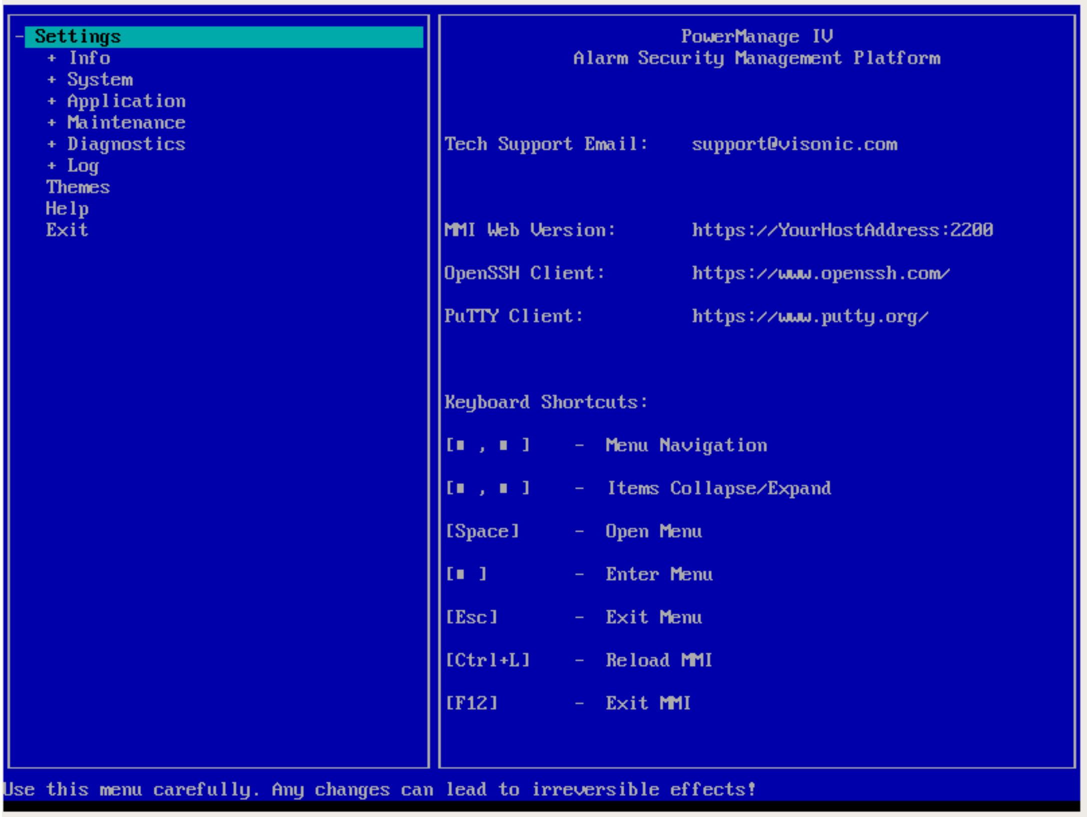
- ➢ At this step you are asked to **set a new password** for Unix user root.

  Note: Use a combination of letters, numbers, and special characters. The password to include both Uppercase and Lowercase characters.



```
Red Hat Enterprise Linux Server 7.3 (Maipo)
Kernel 3.10.0-514.el7.x86_64 on an x86_64

localhost login: root
Password:
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: _
```

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



```
- Settings                                     PowerManage IV
   + Info                          Alarm Security Management Platform
   + System
   + Application
   + Maintenance
   + Diagnostics                Tech Support Email:    support@visonic.com
   + Log
   Themes
   Help
   Exit                         MMI Web Version:       https://YourHostAddress:2200

                                OpenSSH Client:        https://www.openssh.com/

                                PuTTY Client:          https://www.putty.org/


                                Keyboard Shortcuts:

                                [■ , ■ ]      -   Menu Navigation

                                [■ , ■ ]      -   Items Collapse/Expand

                                [Space]       -   Open Menu

                                [■ ]          -   Enter Menu

                                [Esc]         -   Exit Menu

                                [Ctrl+L]      -   Reload MMI

                                [F12]         -   Exit MMI

Use this menu carefully. Any changes can lead to irreversible effects!
```

❑ *Power Manage installation on Dell equipment*

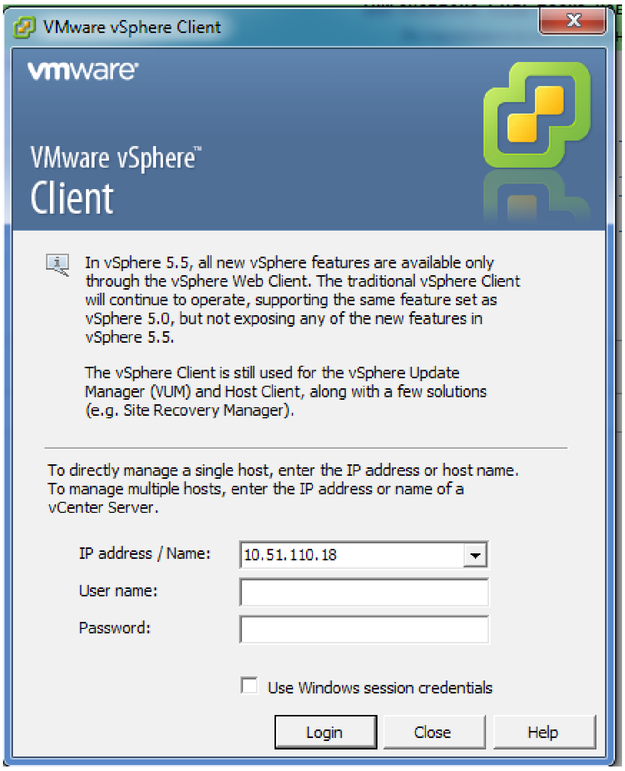
Installation from DVD for Dell equipment is exactly the same as described for HP servers.
USB installation is different. Due to Dells’ BIOS configuration peculiar properties two exactly the same USB drivers with the same Power Manage images are needed.

- ➢ 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



VMware vSphere Client

VMware vSphere™ Client

In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

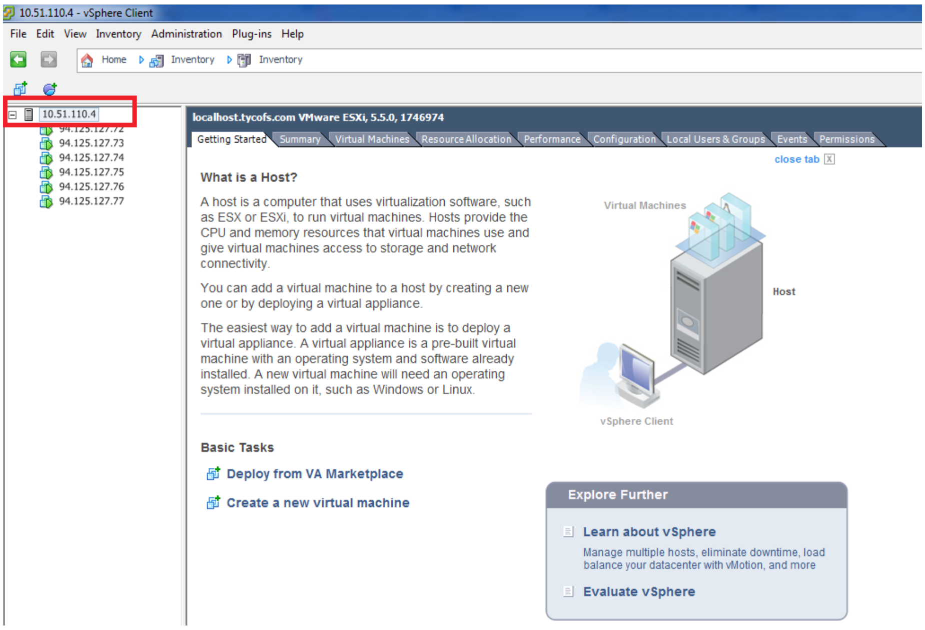
IP address / Name: 10.51.110.18

User name:

Password:

□ Use Windows session credentials

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



10.51.110.4 - vSphere Client

10.51.110.4
94.125.127.72
94.125.127.73
94.125.127.74
94.125.127.75
94.125.127.76
94.125.127.77

localhost.tycofs.com VMware ESXi, 5.5.0, 1746974

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

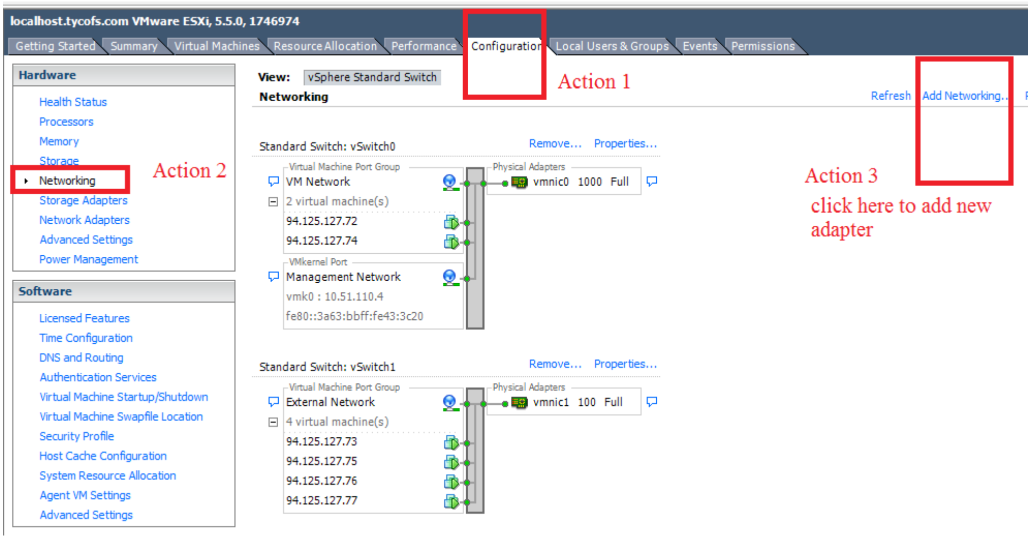
You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

- ➢ 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]



localhost.tycofs.com VMware ESXi, 5.5.0, 1746974

View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group
VM Network
2 virtual machine(s)
94.125.127.72
94.125.127.74

Physical Adapters
vmnic0 1000 Full

VMkernel Port
Management Network
vmk0 : 10.51.110.4
fe80::3a63:bbff:fe43:3c20

Standard Switch: vSwitch1

Virtual Machine Port Group
External Network
4 virtual machine(s)
94.125.127.73
94.125.127.75
94.125.127.76
94.125.127.77

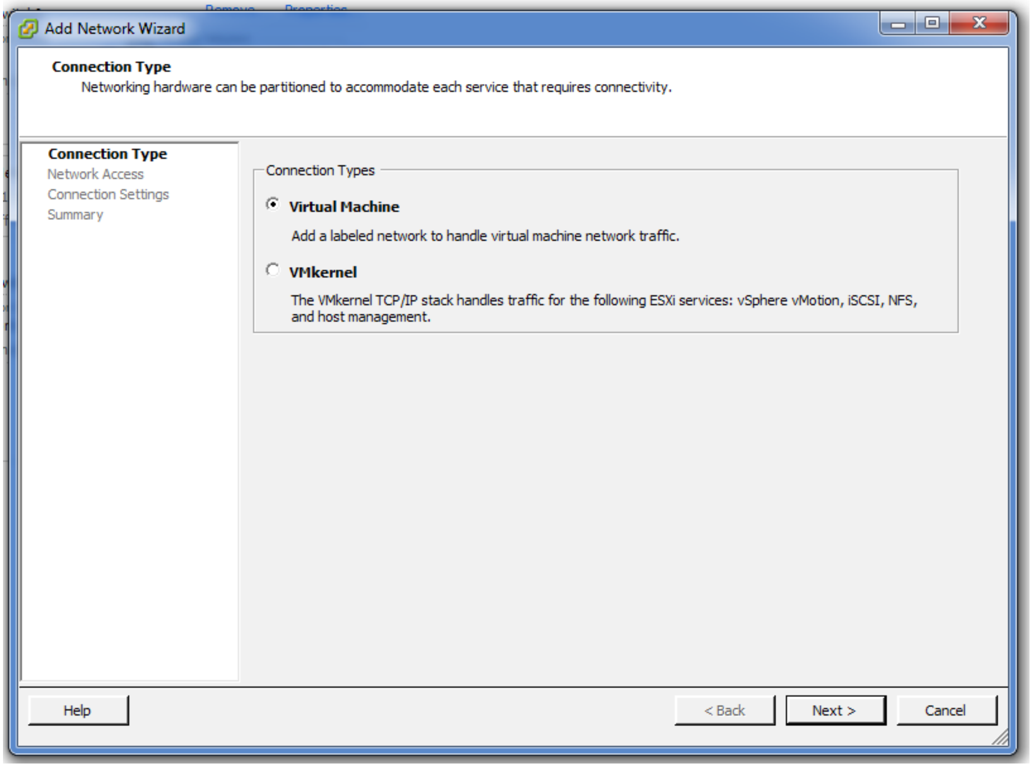
Physical Adapters
vmnic1 100 Full

Action 1

Action 2

Action 3
click here to add new adapter

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



Add Network Wizard

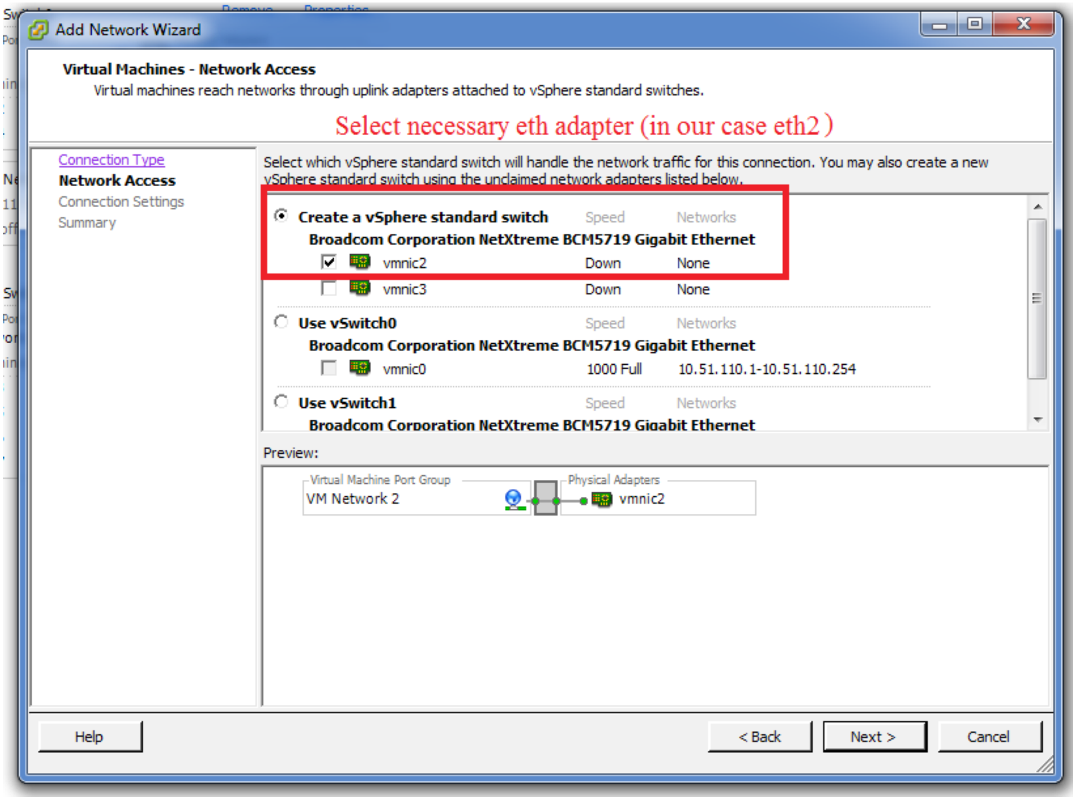
Connection Type
Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Types

● **Virtual Machine**
Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**
The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

- ➢ Select necessary Ethernet adapter and press ‘Next’



Add Network Wizard

Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Select necessary eth adapter (in our case eth2)

Select which vSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.

● Create a vSphere standard switch — Speed — Networks

Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet

		Speed	Networks
☑	vmnic2	Down	None
□	vmnic3	Down	None

○ Use vSwitch0 — Speed — Networks

Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet

		Speed	Networks
□	vmnic0	1000 Full	10.51.110.1-10.51.110.254

○ Use vSwitch1 — Speed — Networks

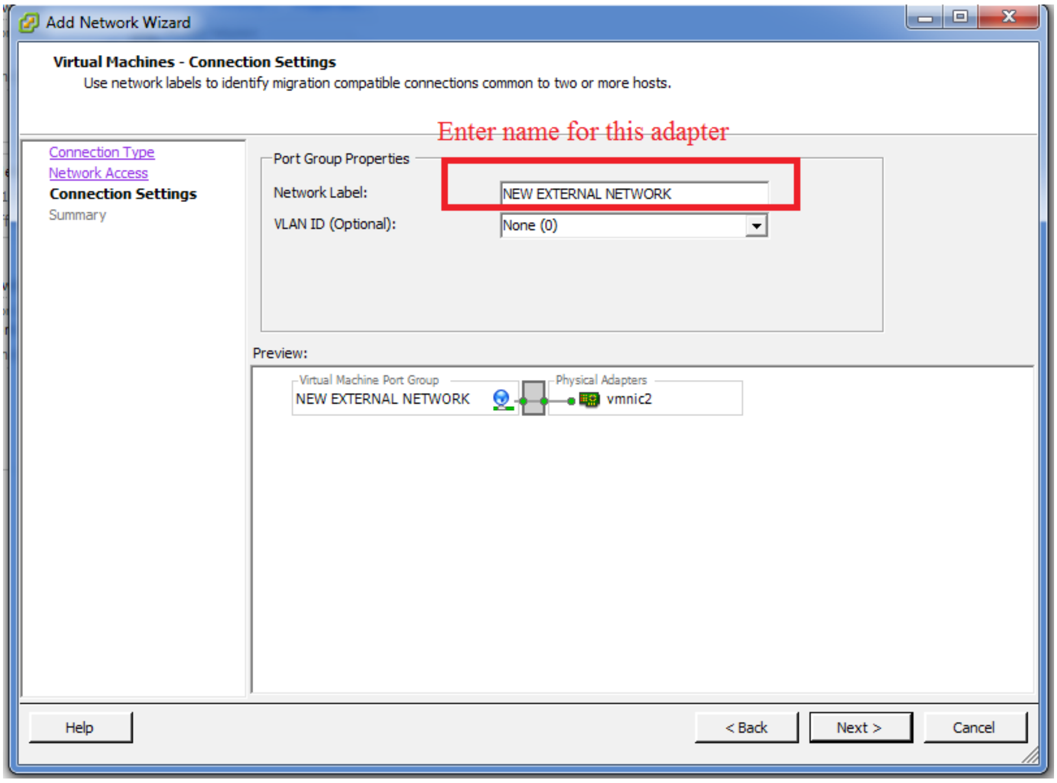
Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet

Preview:

Virtual Machine Port Group: VM Network 2

Physical Adapters: vmnic2

➢ Enter adapter name and press ‘Next’



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

Enter name for this adapter

Port Group Properties

Network Label: NEW EXTERNAL NETWORK

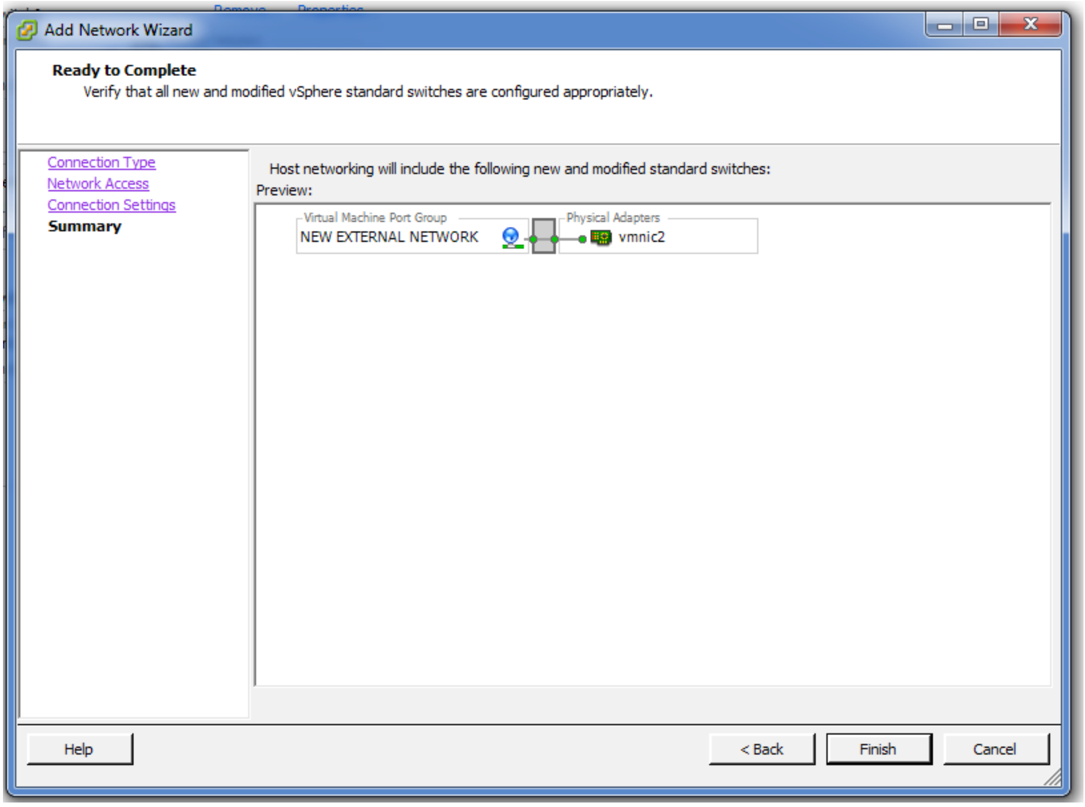
VLAN ID (Optional): None (0)

Preview:

Virtual Machine Port Group: NEW EXTERNAL NETWORK

Physical Adapters: vmnic2

➢ Press ‘Finish’



Ready to Complete

Verify that all new and modified vSphere standard switches are configured appropriately.

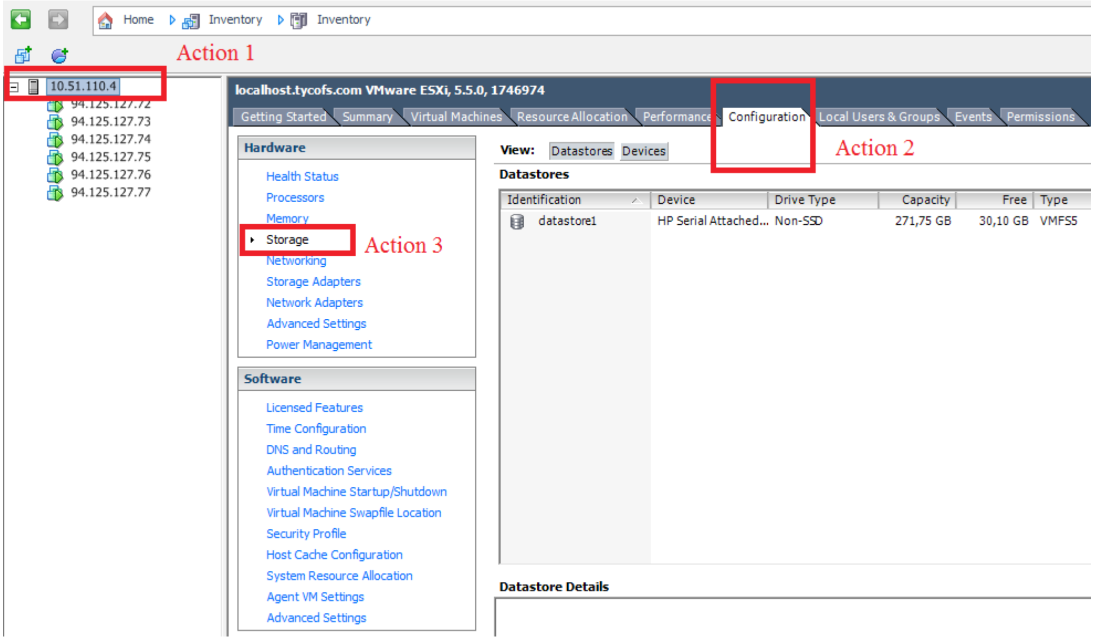
Host networking will include the following new and modified standard switches:

Preview:

Virtual Machine Port Group: NEW EXTERNAL NETWORK

Physical Adapters: vmnic2

- ➢ 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]

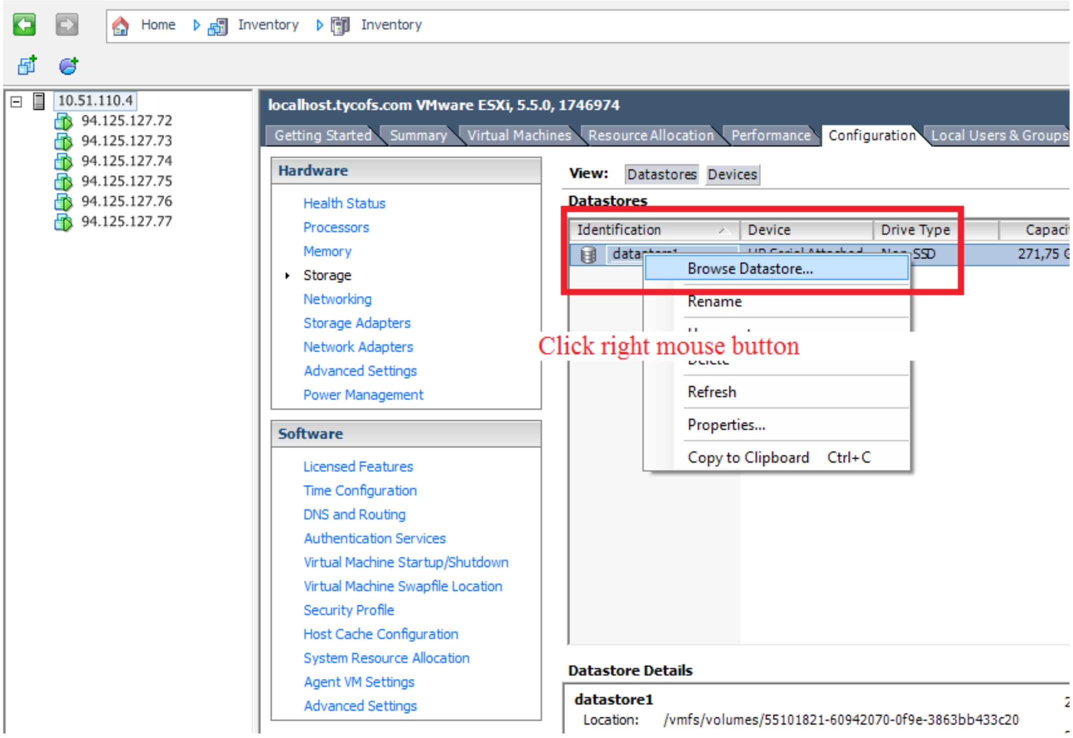


localhost.tycofs.com VMware ESXi, 5.5.0, 1746974

Datastores

Identification	Device	Drive Type	Capacity	Free	Type
datastore1	HP Serial Attached...	Non-SSD	271,75 GB	30,10 GB	VMFS5

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

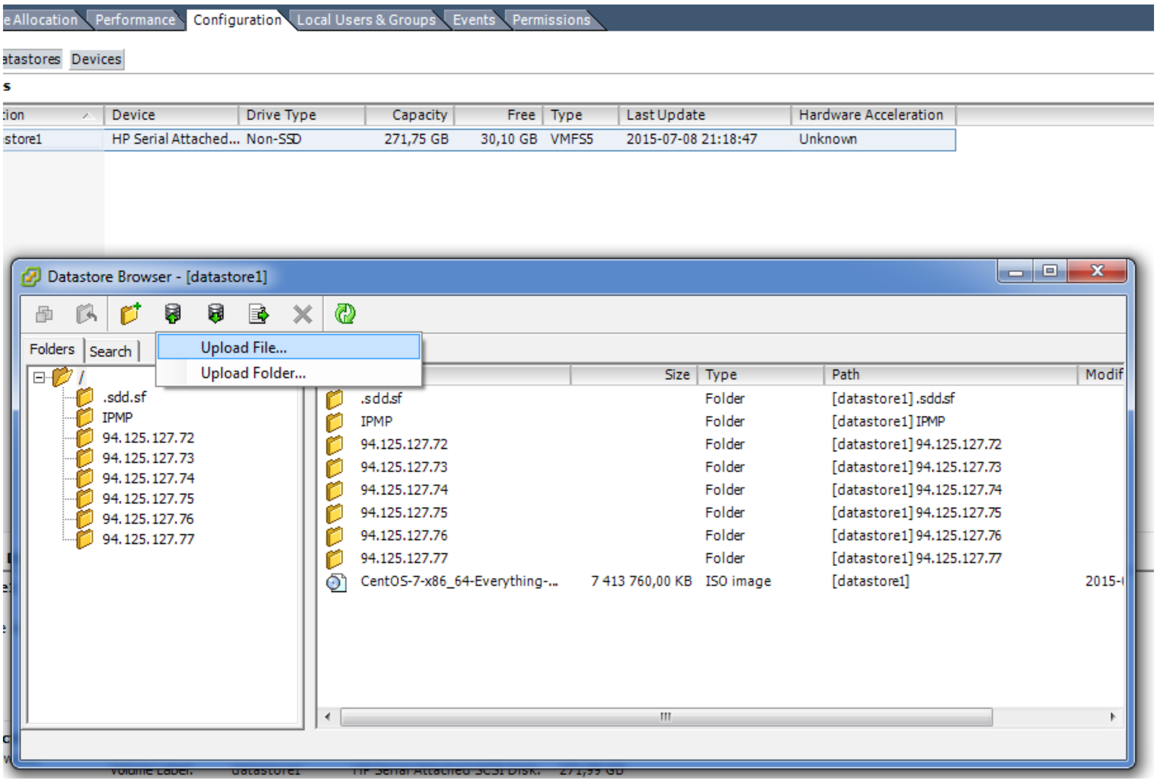


Click right mouse button

Datastore Details

datastore1
Location: /vmfs/volumes/55101821-60942070-0f9e-3863bb433c20

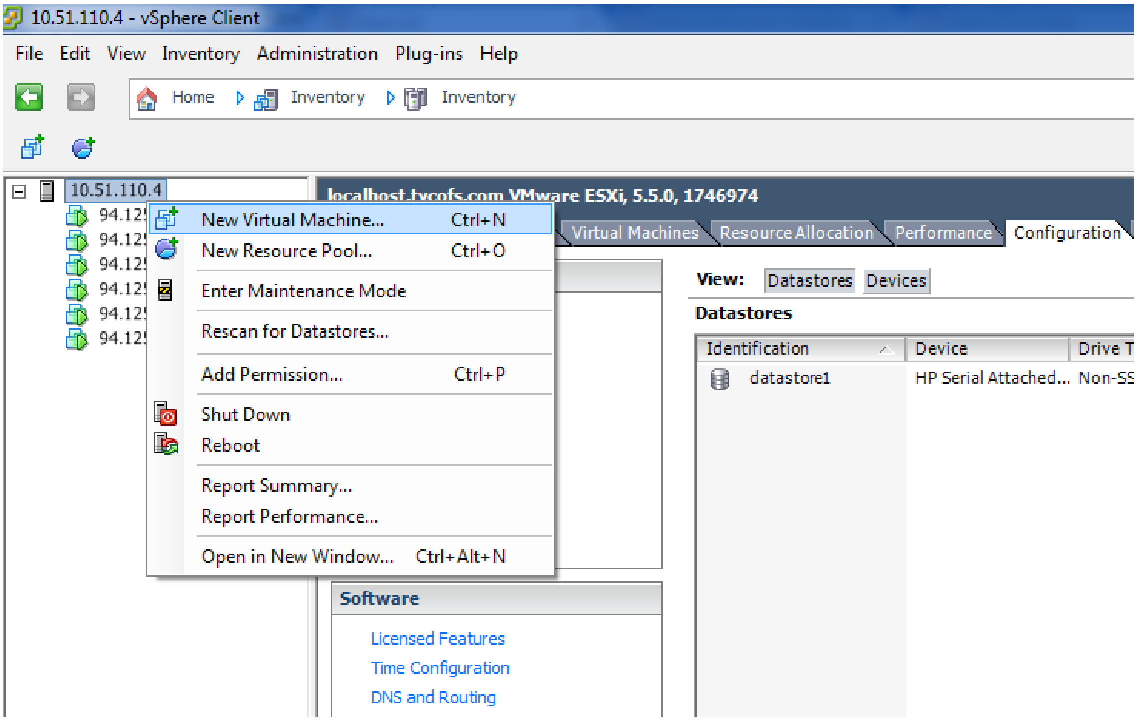
- Click ‘Upload files to this storage’ icon, select ‘Upload File…’ and add the file from your workstation



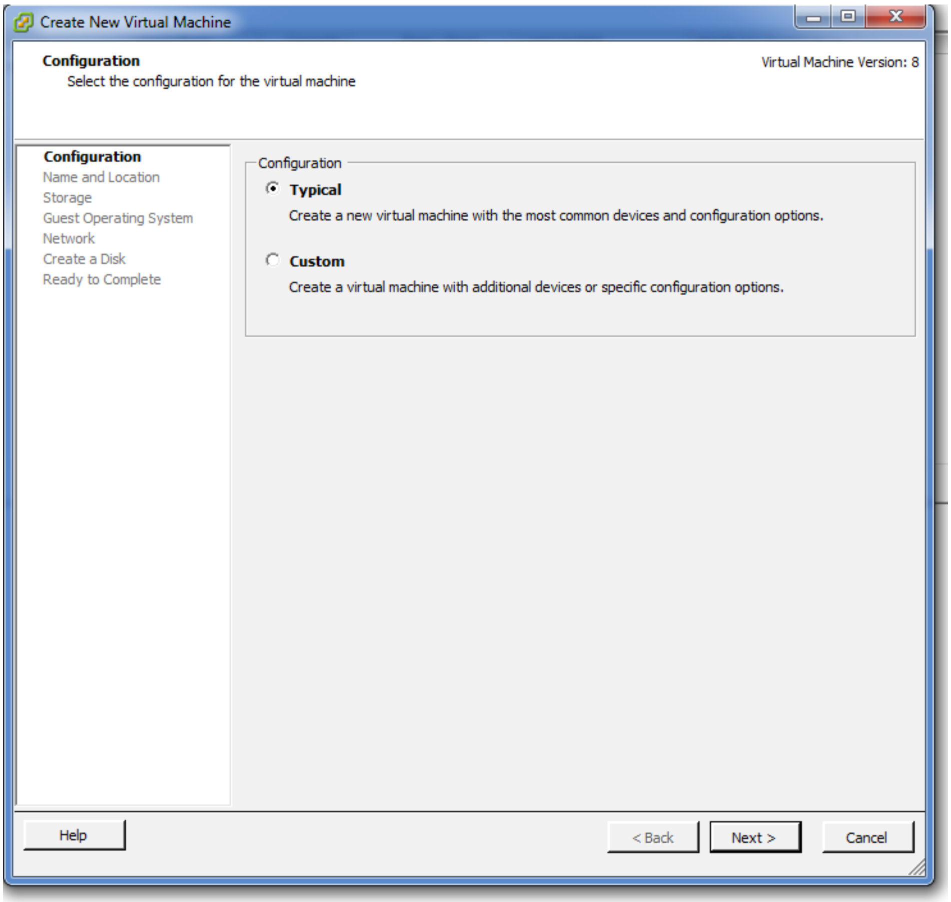
ion	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Acceleration
store1	HP Serial Attached...	Non-SSD	271,75 GB	30,10 GB	VMFS5	2015-07-08 21:18:47	Unknown

	Size	Type	Path	Modif
.sdd.sf		Folder	[datastore1] .sdd.sf	
IPMP		Folder	[datastore1] IPMP	
94.125.127.72		Folder	[datastore1] 94.125.127.72	
94.125.127.73		Folder	[datastore1] 94.125.127.73	
94.125.127.74		Folder	[datastore1] 94.125.127.74	
94.125.127.75		Folder	[datastore1] 94.125.127.75	
94.125.127.76		Folder	[datastore1] 94.125.127.76	
94.125.127.77		Folder	[datastore1] 94.125.127.77	
CentOS-7-x86_64-Everything-...	7 413 760,00 KB	ISO image	[datastore1]	2015-I

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



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



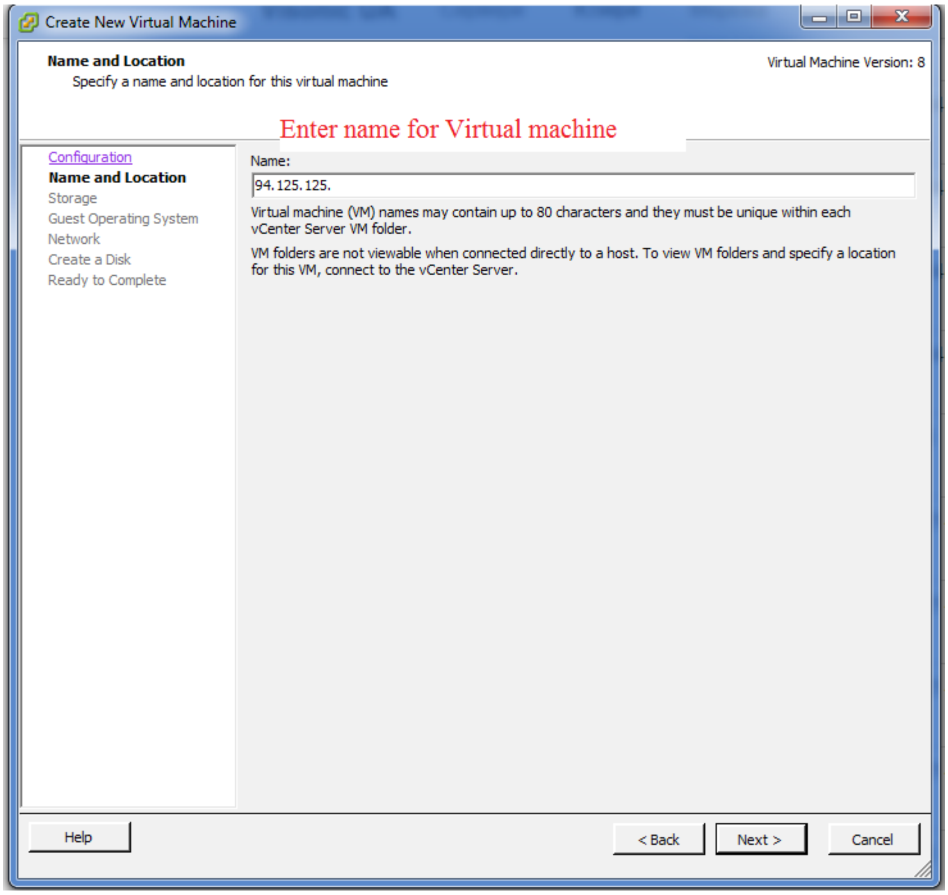
Configuration
Select the configuration for the virtual machine

Configuration

● **Typical**
Create a new virtual machine with the most common devices and configuration options.

○ **Custom**
Create a virtual machine with additional devices or specific configuration options.

- Enter virtual machine name, press ‘Next’



Name and Location

Specify a name and location for this virtual machine

Virtual Machine Version: 8

Enter name for Virtual machine

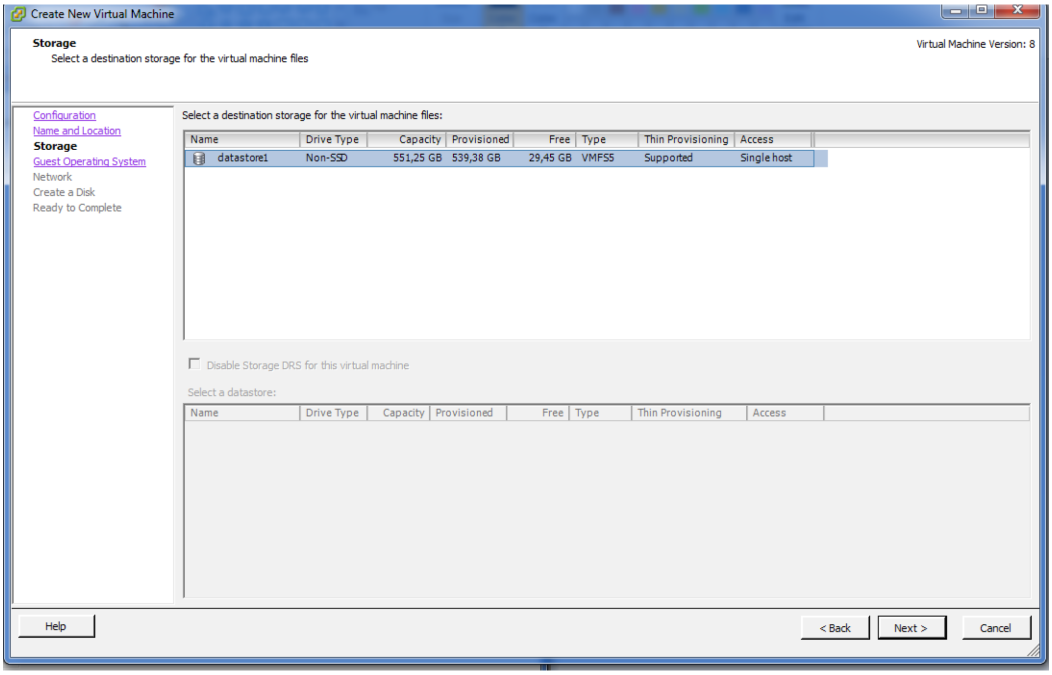
Name:

94.125.125.

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

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



Storage

Select a destination storage for the virtual machine files

Virtual Machine Version: 8

Select a destination storage for the virtual machine files:

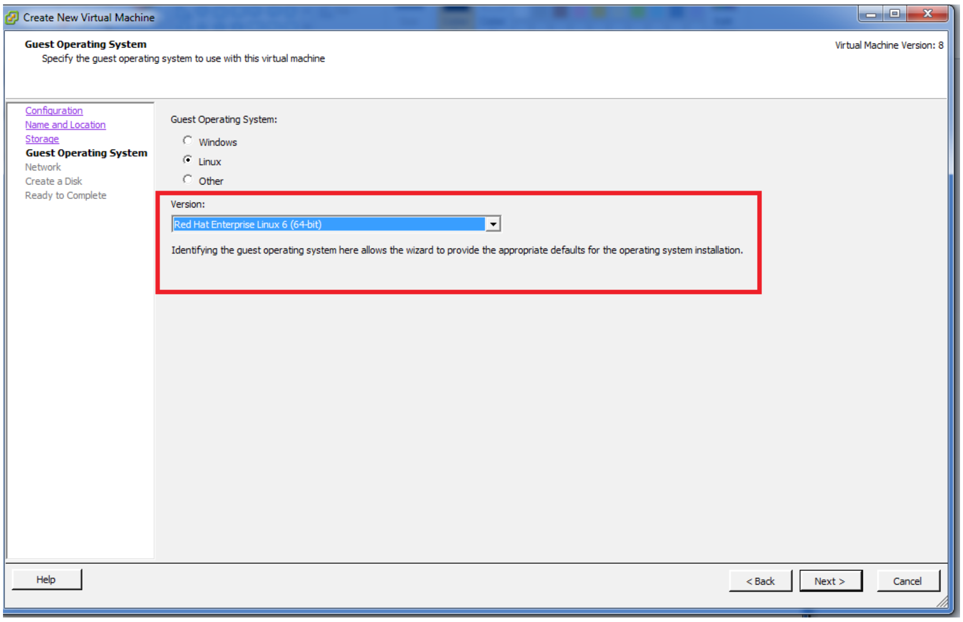
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
datastore1	Non-SSD	551,25 GB	539,38 GB	29,45 GB	VMFS5	Supported	Single host

□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning	Access

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



Create New Virtual Machine

Guest Operating System

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 8

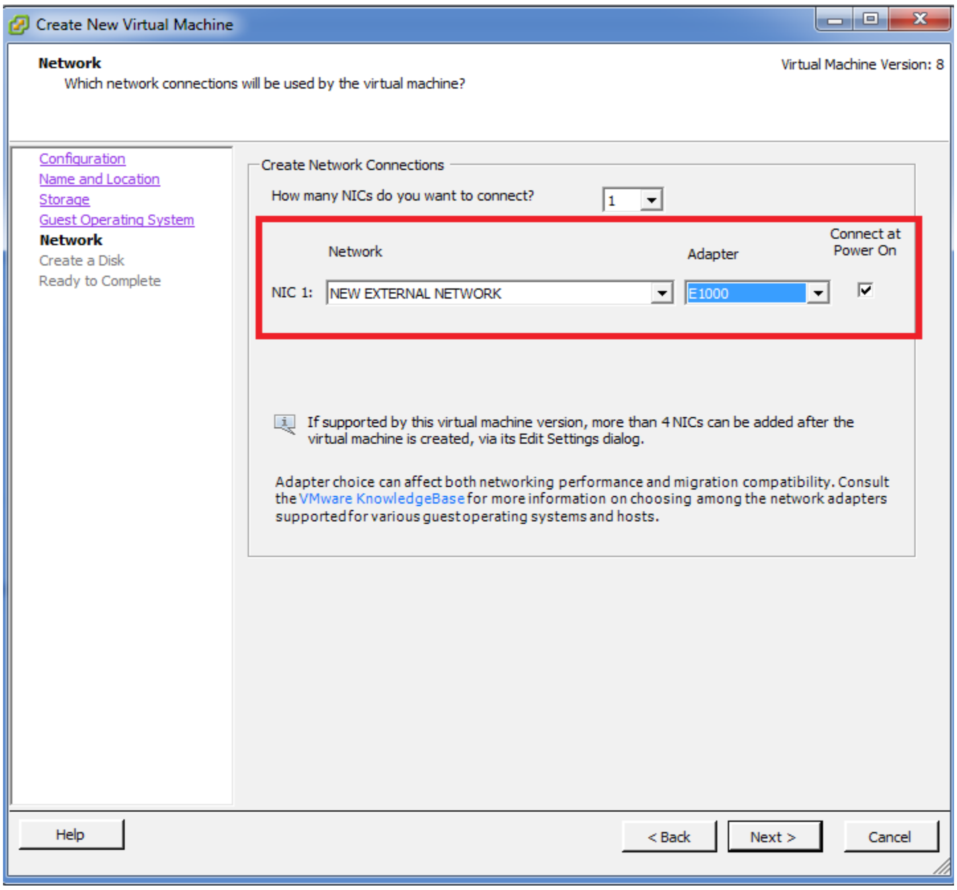
Guest Operating System:

○ Windows
● Linux
○ Other

Version: Red Hat Enterprise Linux 6 (64-bit)

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

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



Create New Virtual Machine

Network

Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

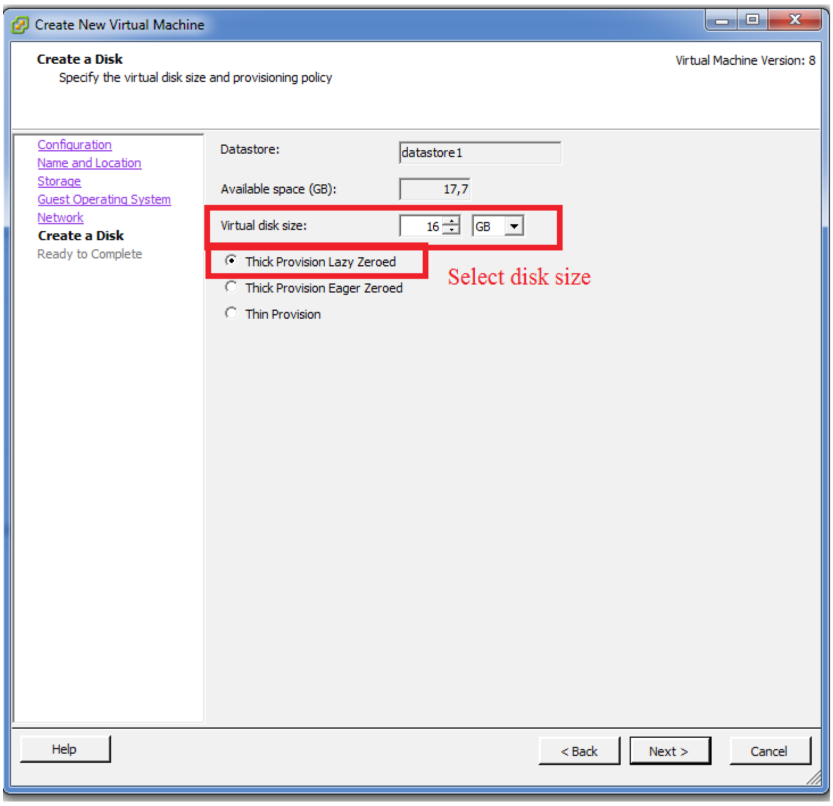
How many NICs do you want to connect? 1

	Network	Adapter	Connect at Power On
NIC 1:	NEW EXTERNAL NETWORK	E1000	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

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



Create New Virtual Machine

Create a Disk
Specify the virtual disk size and provisioning policy

Virtual Machine Version: 8

Datastore: datastore1

Available space (GB): 17,7

Virtual disk size: 16 GB

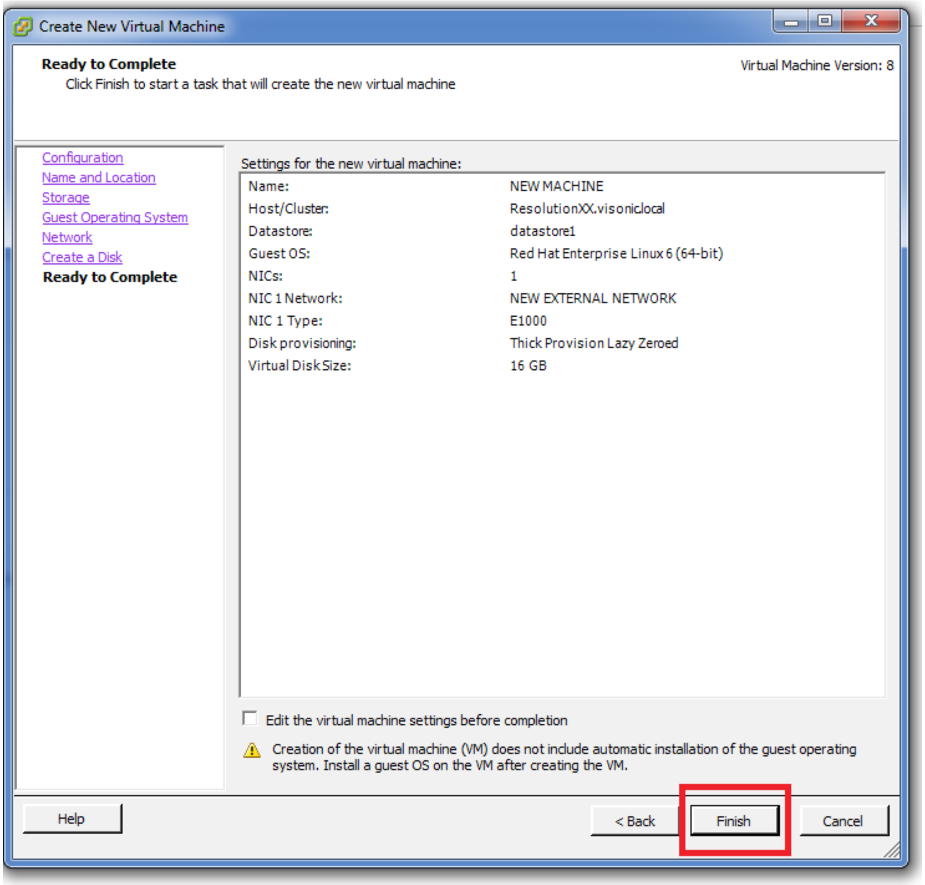
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

Select disk size

- Press ‘Finish’



Create New Virtual Machine

Ready to Complete
Click Finish to start a task that will create the new virtual machine

Virtual Machine Version: 8

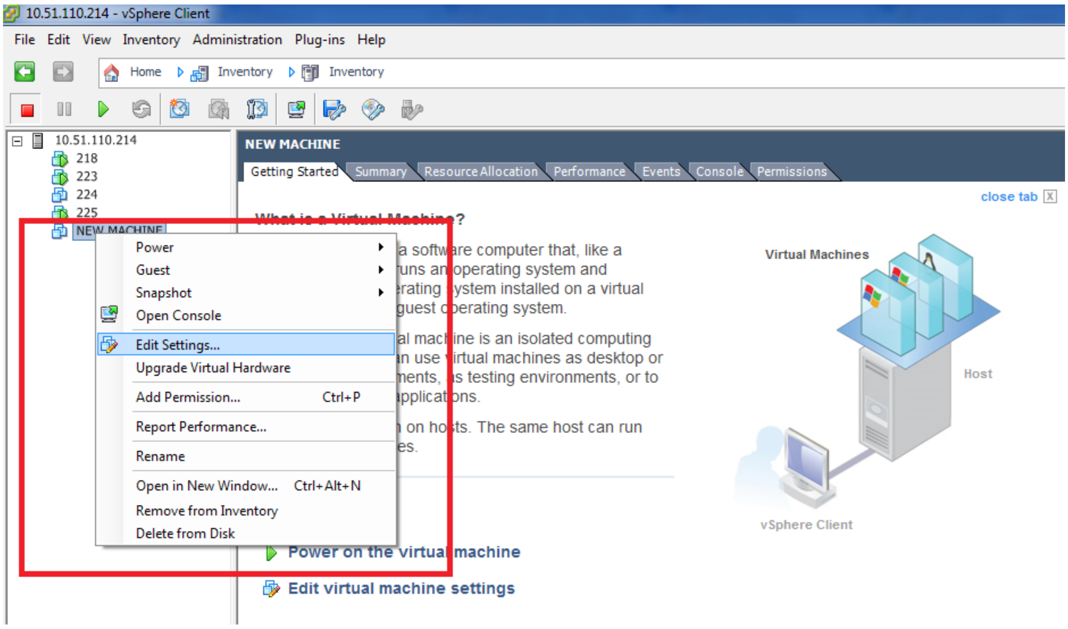
Settings for the new virtual machine:

Name:	NEW MACHINE
Host/Cluster:	ResolutionXX.visonic.local
Datastore:	datastore1
Guest OS:	Red Hat Enterprise Linux 6 (64-bit)
NICs:	1
NIC 1 Network:	NEW EXTERNAL NETWORK
NIC 1 Type:	E1000
Disk provisioning:	Thick Provision Lazy Zeroed
Virtual Disk Size:	16 GB

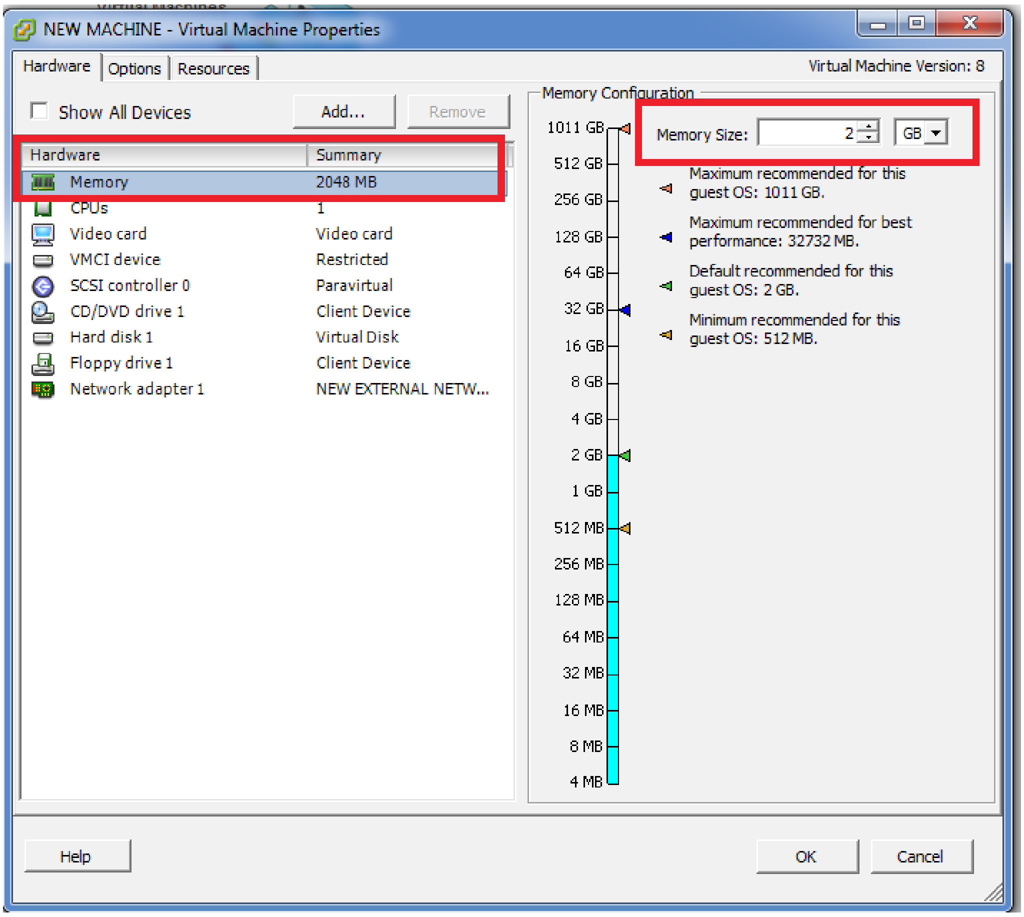
□ Edit the virtual machine settings before completion

Creation of the virtual machine (VM) does not include automatic installation of the guest operating system. Install a guest OS on the VM after creating the VM.

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



➢ Set Memory Size: at least 4 GB



Hardware	Summary
Memory	2048 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	Paravirtual
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	NEW EXTERNAL NETW...

Memory Size: 2 GB

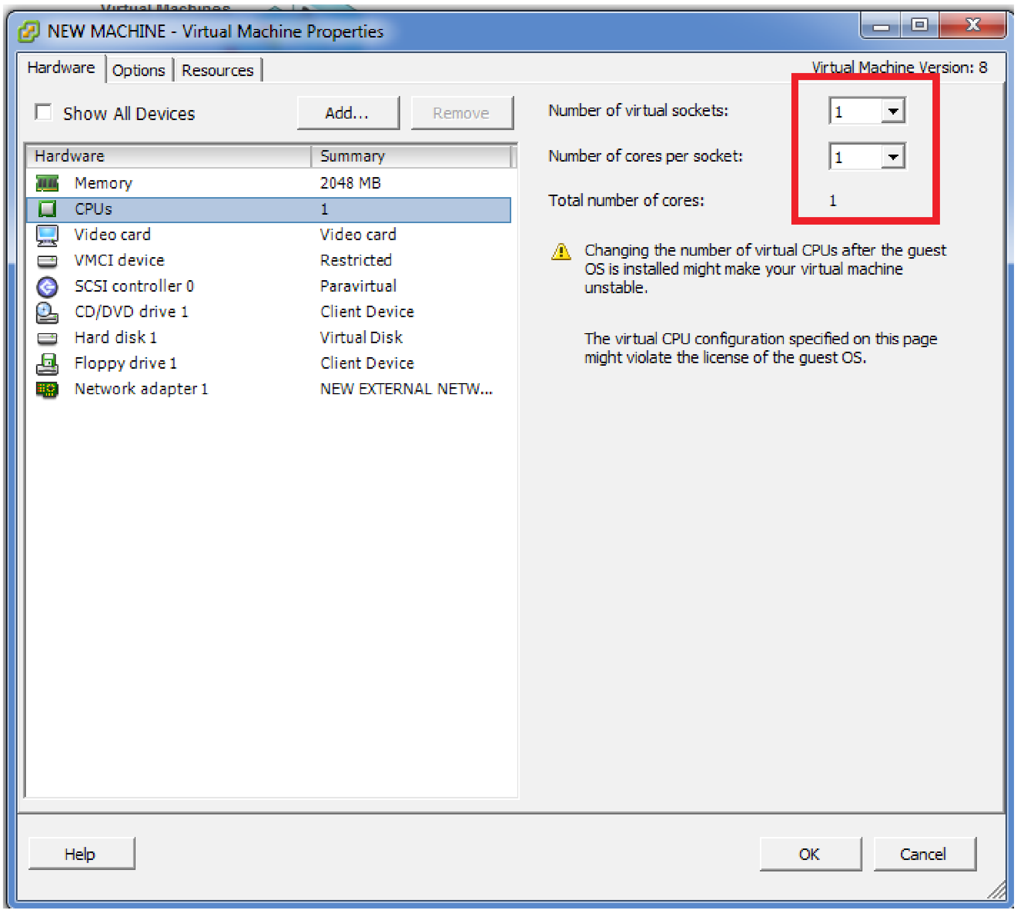
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 32732 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 512 MB.

- Set CPUs quantity: one or more if required



NEW MACHINE - Virtual Machine Properties

Hardware | Options | Resources

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	Paravirtual
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	NEW EXTERNAL NETW...

Number of virtual sockets: 1

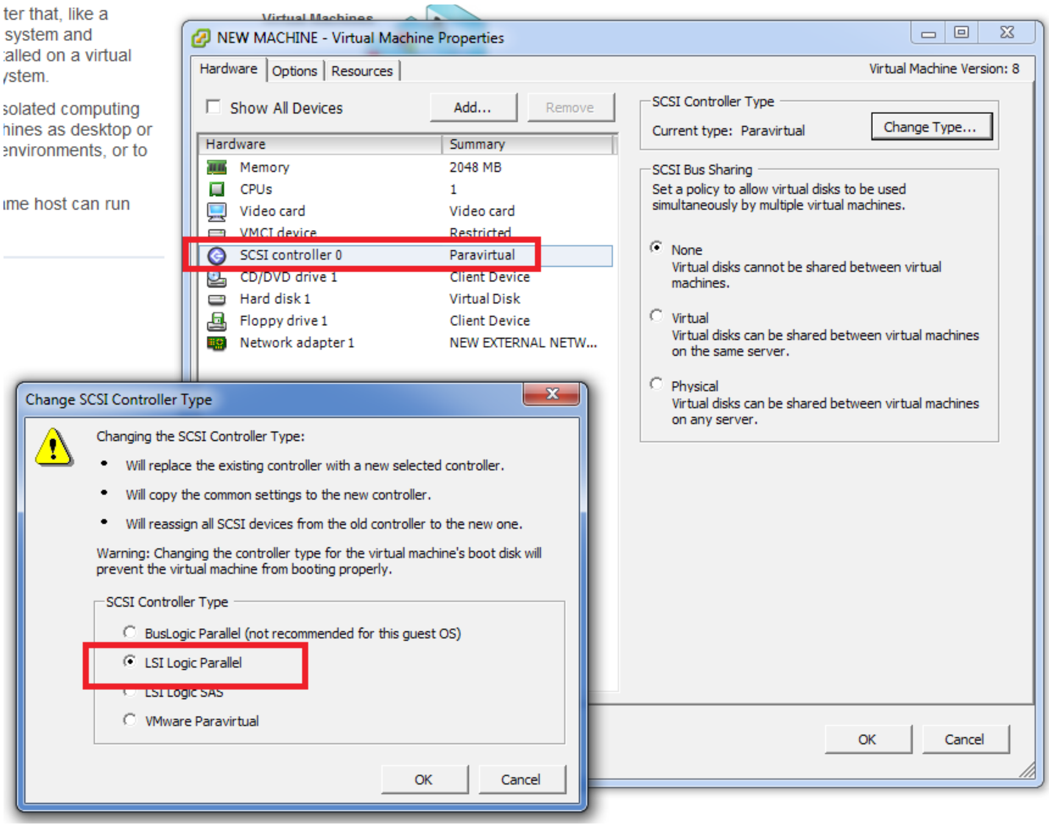
Number of cores per socket: 1

Total number of cores: 1

Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

- Configure SCSI controller type: press 'Change type' and select 'LSI Logic Parallel'



ter that, like a
system and
alled on a virtual
ystem.

solated computing
hines as desktop or
environments, or to

ime host can run

NEW MACHINE - Virtual Machine Properties

Hardware | Options | Resources

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
SCSI controller 0	Paravirtual
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	NEW EXTERNAL NETW...

SCSI Controller Type

Current type: Paravirtual

SCSI Bus Sharing

Set a policy to allow virtual disks to be used simultaneously by multiple virtual machines.

● None
Virtual disks cannot be shared between virtual machines.

○ Virtual
Virtual disks can be shared between virtual machines on the same server.

○ Physical
Virtual disks can be shared between virtual machines on any server.

Change SCSI Controller Type

Changing the SCSI Controller Type:

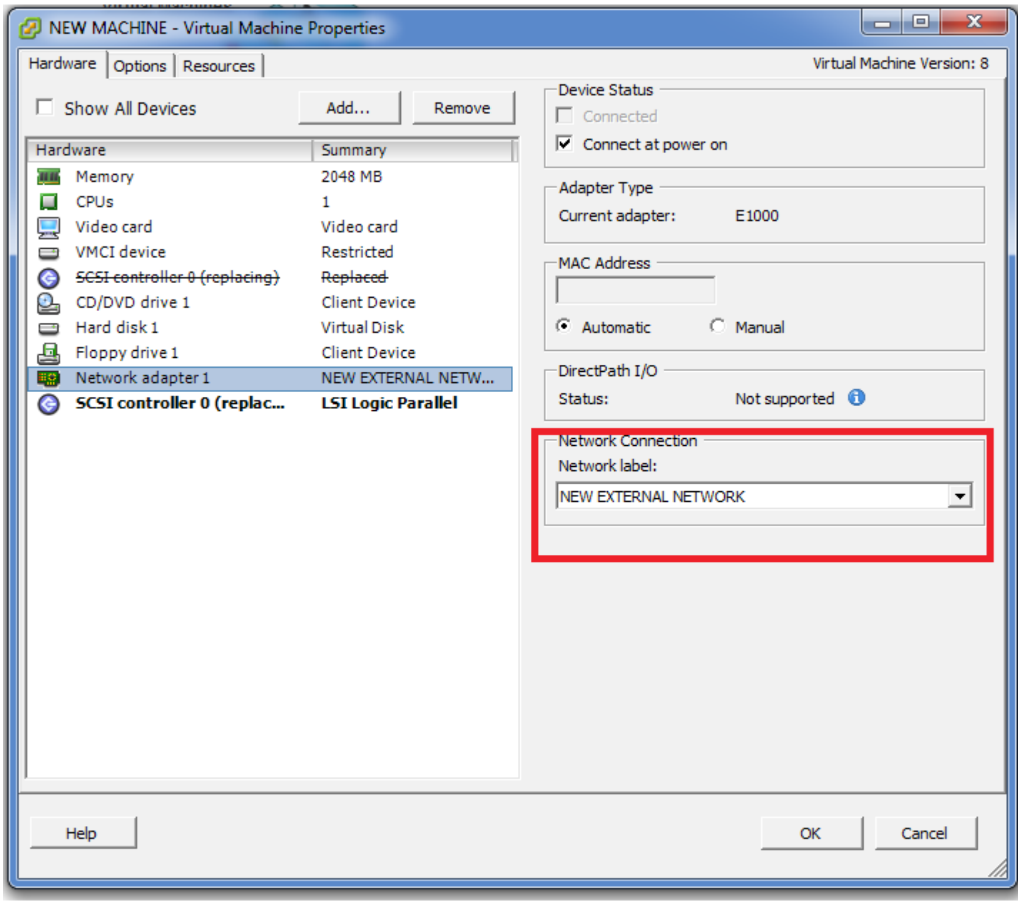
- Will replace the existing controller with a new selected controller.
- Will copy the common settings to the new controller.
- Will reassign all SCSI devices from the old controller to the new one.

Warning: Changing the controller type for the virtual machine's boot disk will prevent the virtual machine from booting properly.

SCSI Controller Type

○ BusLogic Parallel (not recommended for this guest OS)
● LSI Logic Parallel
○ LSI Logic SAS
○ VMware Paravirtual

- ➢ Configure Network adapter



NEW MACHINE - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	2048 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
~~SCSI controller 0 (replacing)~~	~~Replaced~~
CD/DVD drive 1	Client Device
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	NEW EXTERNAL NETW...
SCSI controller 0 (replac...	**LSI Logic Parallel**

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: E1000

MAC Address

● Automatic ○ Manual

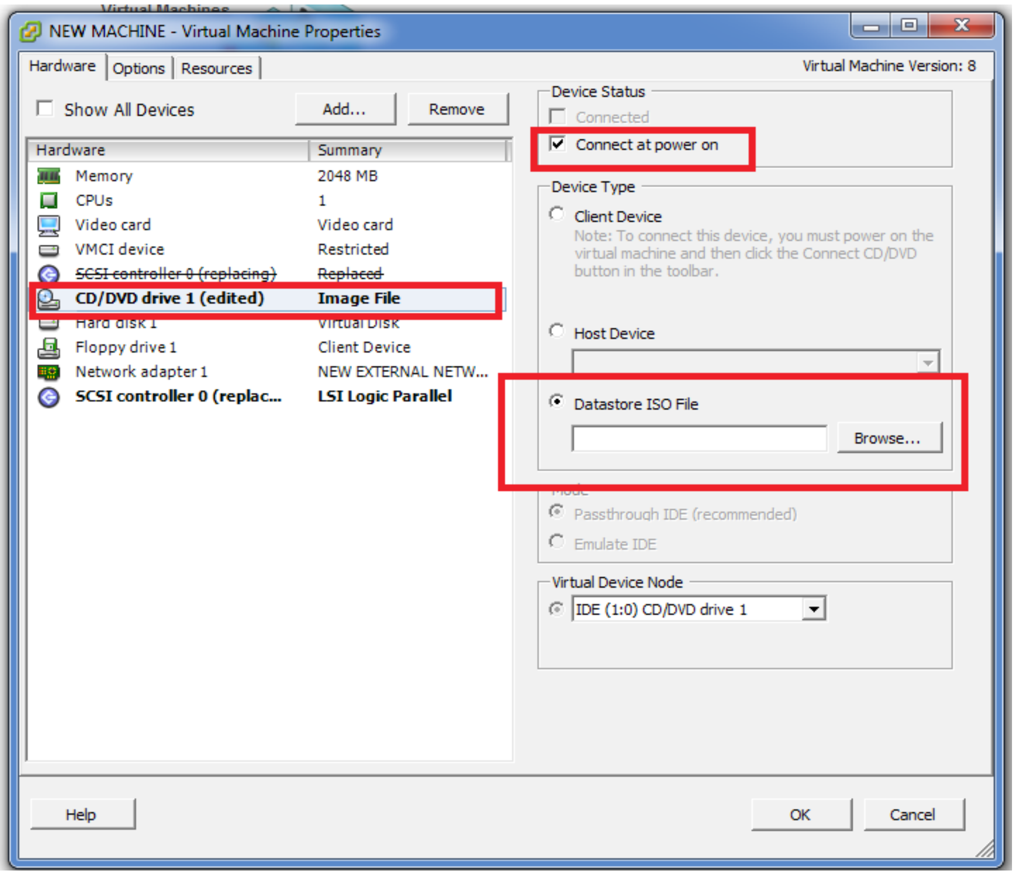
DirectPath I/O

Status: Not supported

Network Connection

Network label: NEW EXTERNAL NETWORK

- ➢ Connect Power Manage image to the VM



NEW MACHINE - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	2048 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
~~SCSI controller 0 (replacing)~~	~~Replaced~~
CD/DVD drive 1 (edited)	**Image File**
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	NEW EXTERNAL NETW...
SCSI controller 0 (replac...	**LSI Logic Parallel**

Device Status

□ Connected

☑ Connect at power on

Device Type

○ Client Device

Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.

○ Host Device

● Datastore ISO File — Browse...

Mode

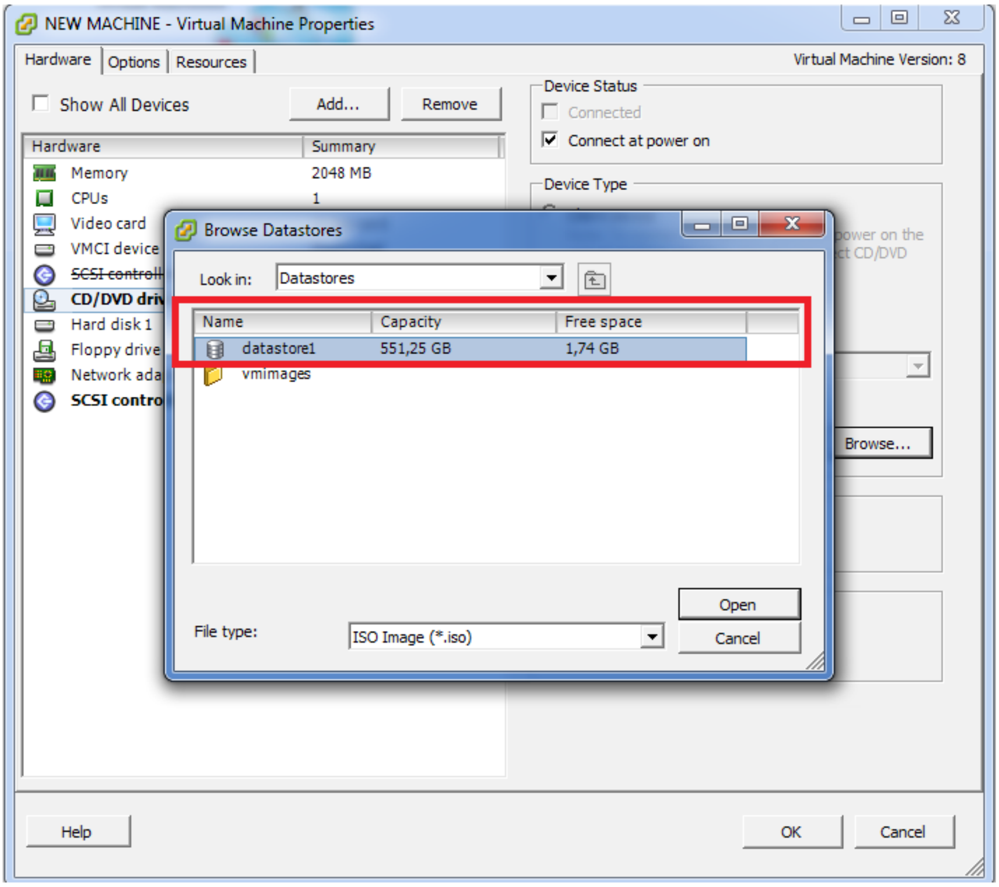
● Passthrough IDE (recommended)

○ Emulate IDE

Virtual Device Node

IDE (1:0) CD/DVD drive 1

➢ Select Power Manage image file from the data store



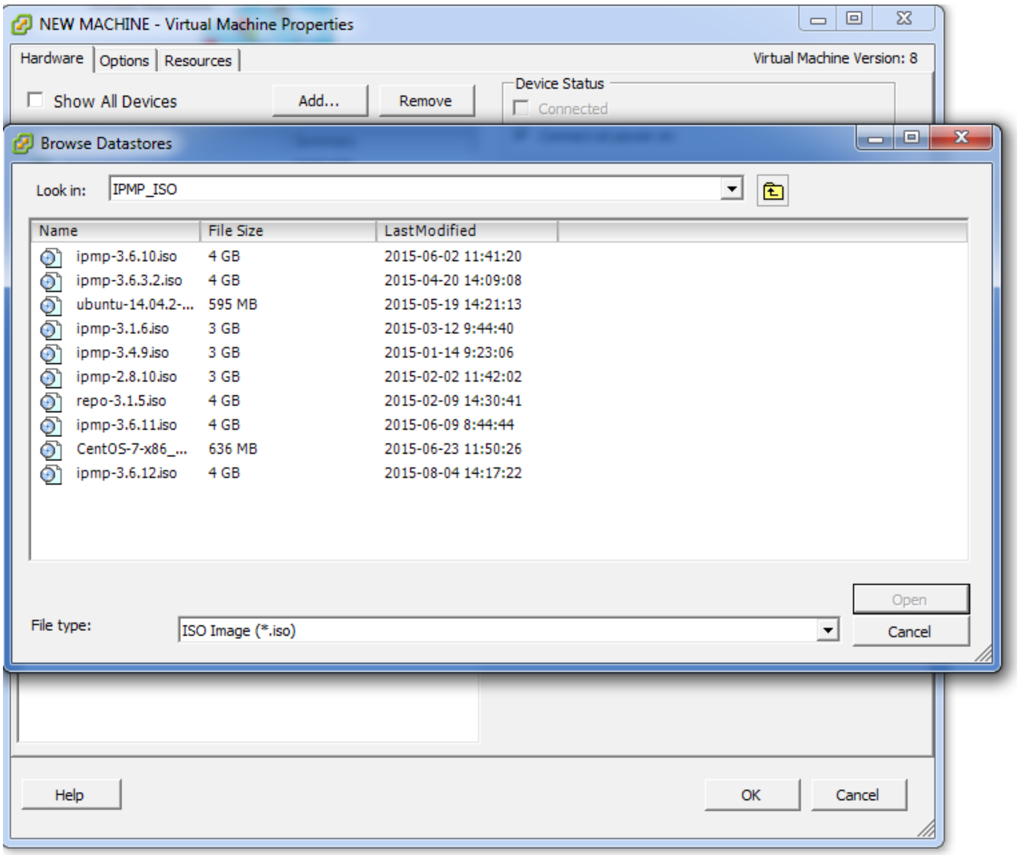
NEW MACHINE - Virtual Machine Properties

Browse Datastores

Look in: Datastores

Name	Capacity	Free space
datastore1	551,25 GB	1,74 GB
vmimages		

File type: ISO Image (*.iso)

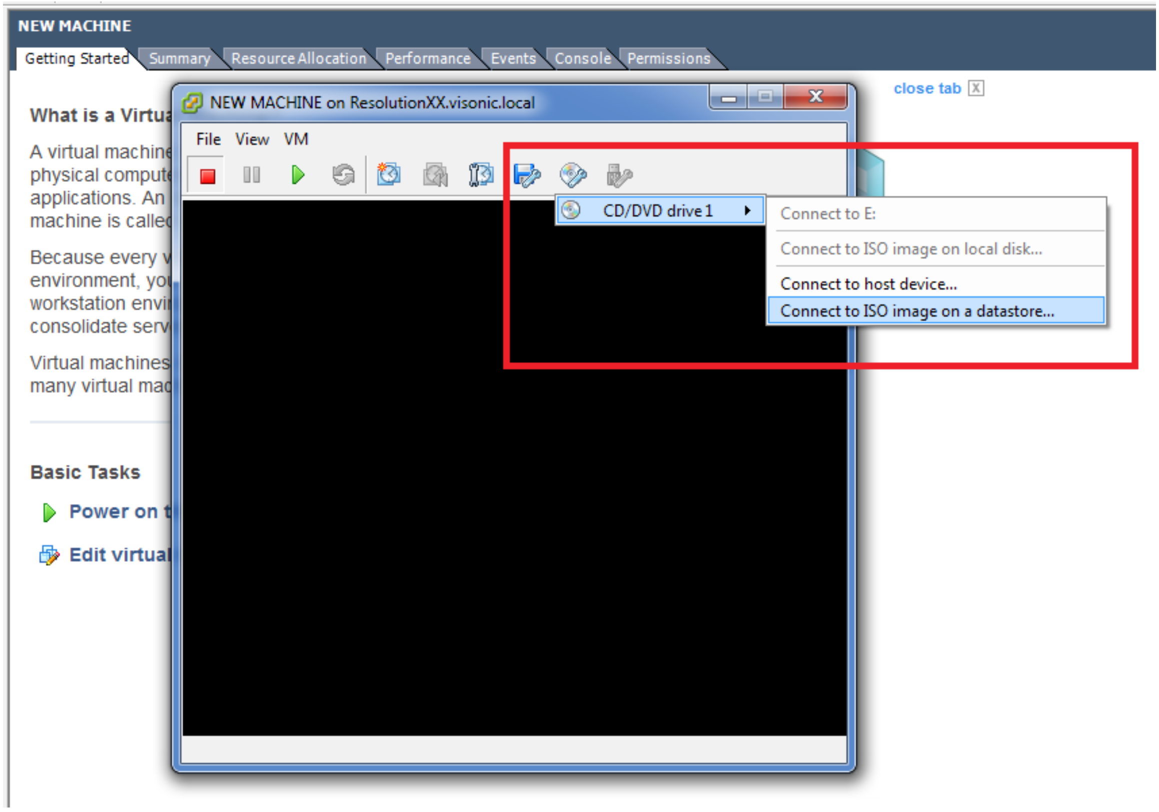


Look in: IPMP_ISO

Name	File Size	LastModified
ipmp-3.6.10.iso	4 GB	2015-06-02 11:41:20
ipmp-3.6.3.2.iso	4 GB	2015-04-20 14:09:08
ubuntu-14.04.2-...	595 MB	2015-05-19 14:21:13
ipmp-3.1.6.iso	3 GB	2015-03-12 9:44:40
ipmp-3.4.9.iso	3 GB	2015-01-14 9:23:06
ipmp-2.8.10.iso	3 GB	2015-02-02 11:42:02
repo-3.1.5.iso	4 GB	2015-02-09 14:30:41
ipmp-3.6.11.iso	4 GB	2015-06-09 8:44:44
CentOS-7-x86_...	636 MB	2015-06-23 11:50:26
ipmp-3.6.12.iso	4 GB	2015-08-04 14:17:22

File type: ISO Image (*.iso)

- ➢ 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.

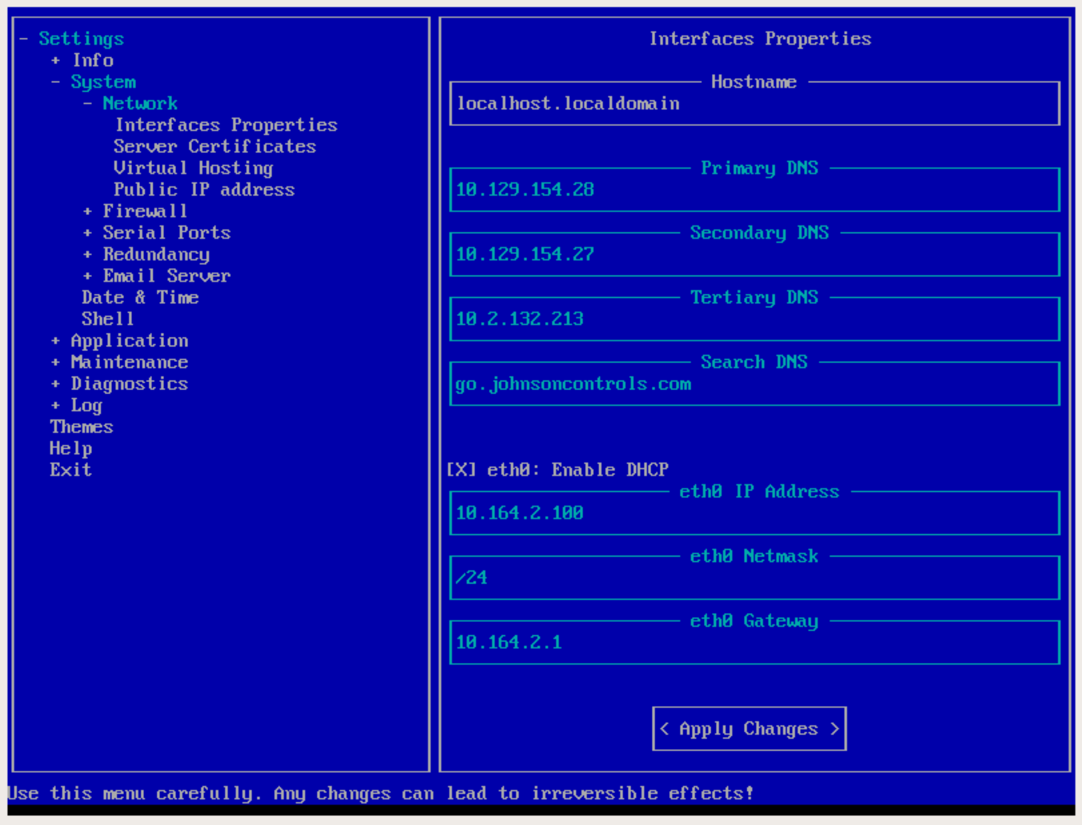
★ Initial Setup

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**



Interfaces Properties

Hostname: localhost.localdomain

Primary DNS: 10.129.154.28

Secondary DNS: 10.129.154.27

Tertiary DNS: 10.2.132.213

Search DNS: go.johnsoncontrols.com

[X] eth0: Enable DHCP

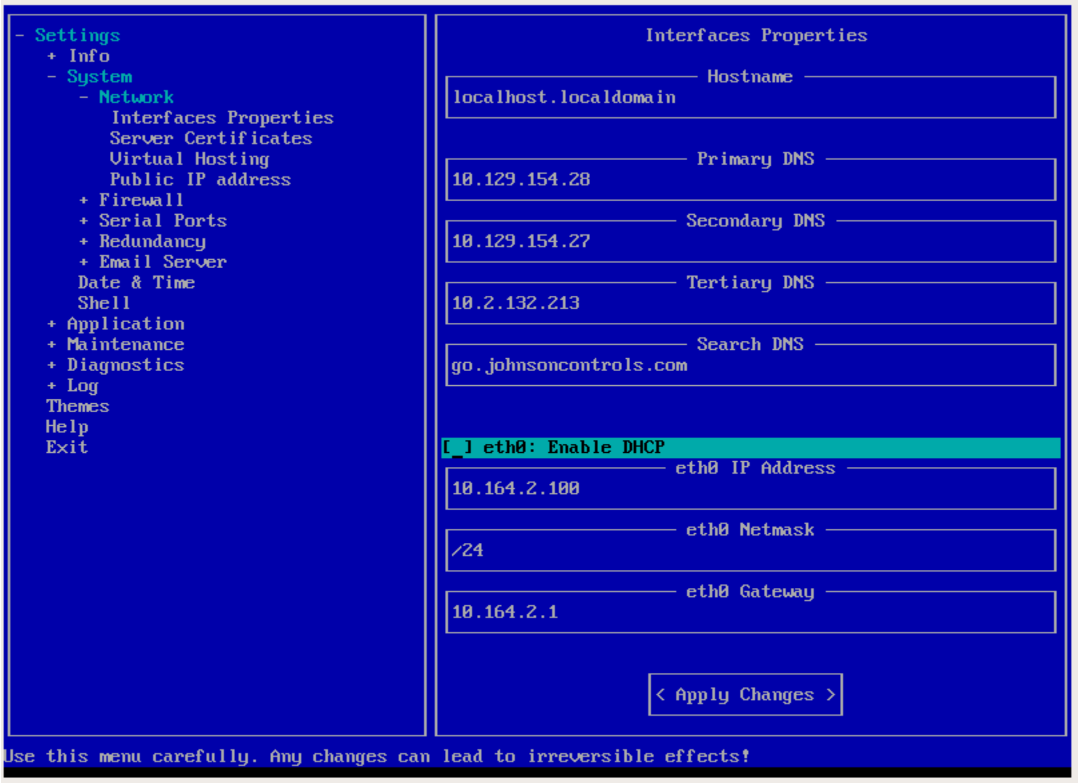
eth0 IP Address: 10.164.2.100

eth0 Netmask: /24

eth0 Gateway: 10.164.2.1

Use this menu carefully. Any changes can lead to irreversible effects!

- 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**



Interfaces Properties

Hostname: localhost.localdomain

Primary DNS: 10.129.154.28

Secondary DNS: 10.129.154.27

Tertiary DNS: 10.2.132.213

Search DNS: go.johnsoncontrols.com

[_] eth0: Enable DHCP

eth0 IP Address: 10.164.2.100

eth0 Netmask: /24

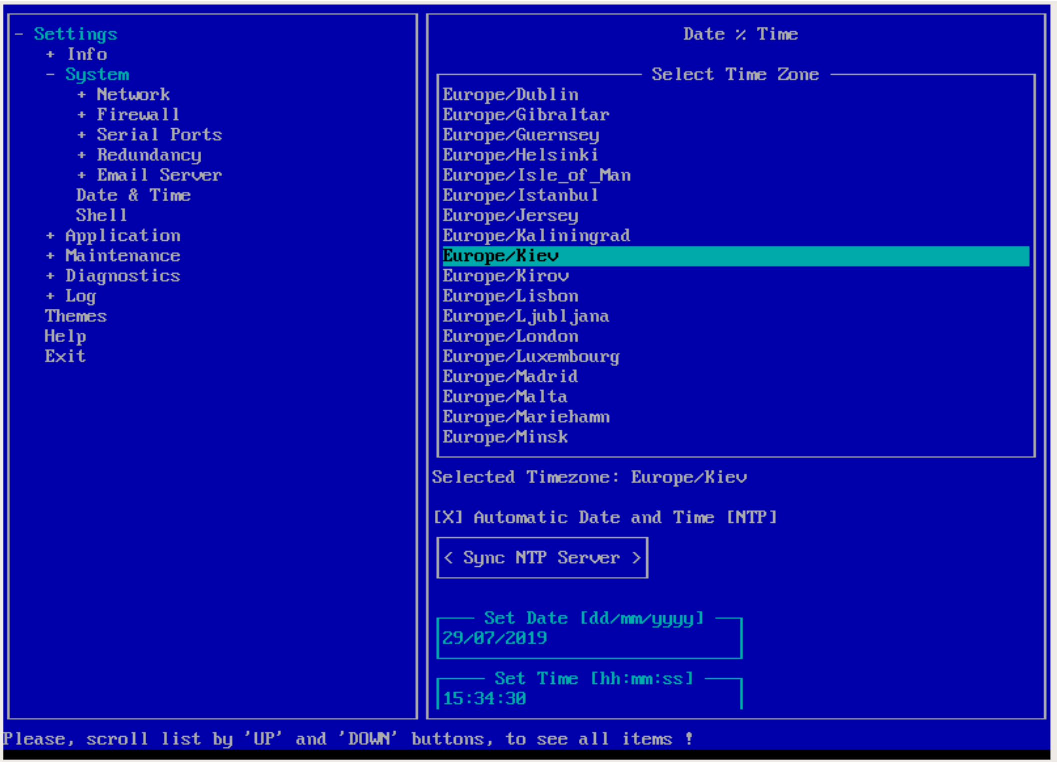
eth0 Gateway: 10.164.2.1

Use this menu carefully. Any changes can lead to irreversible effects!

❑ *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

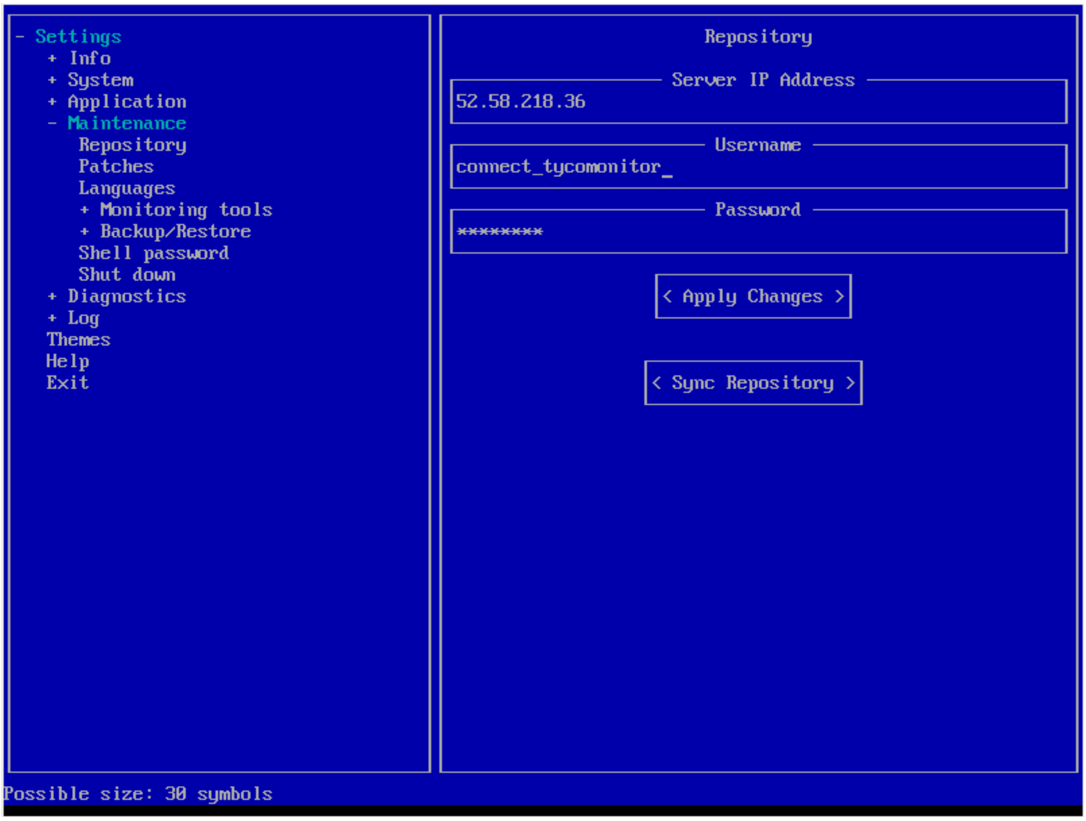


```
Selected Timezone: Europe/Kiev

[X] Automatic Date and Time [NTP]

Set Date [dd/mm/yyyy]
29/07/2019

Set Time [hh:mm:ss]
15:34:30

Please, scroll list by 'UP' and 'DOWN' buttons, to see all items !
```

❑ *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



Repository

Server IP Address: 52.58.218.36

Username: connect_tycomonitor_

Password: *********

Possible size: 30 symbols

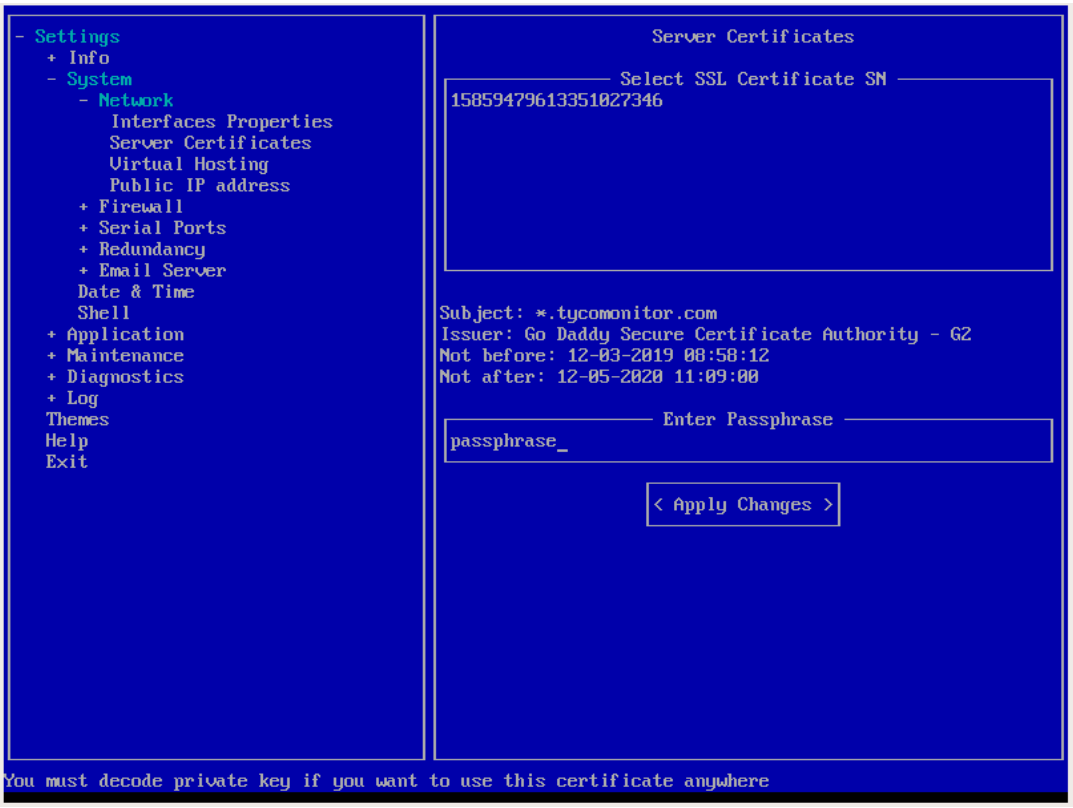
❑ *Assign SSL certificate to the Power Manage*

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**



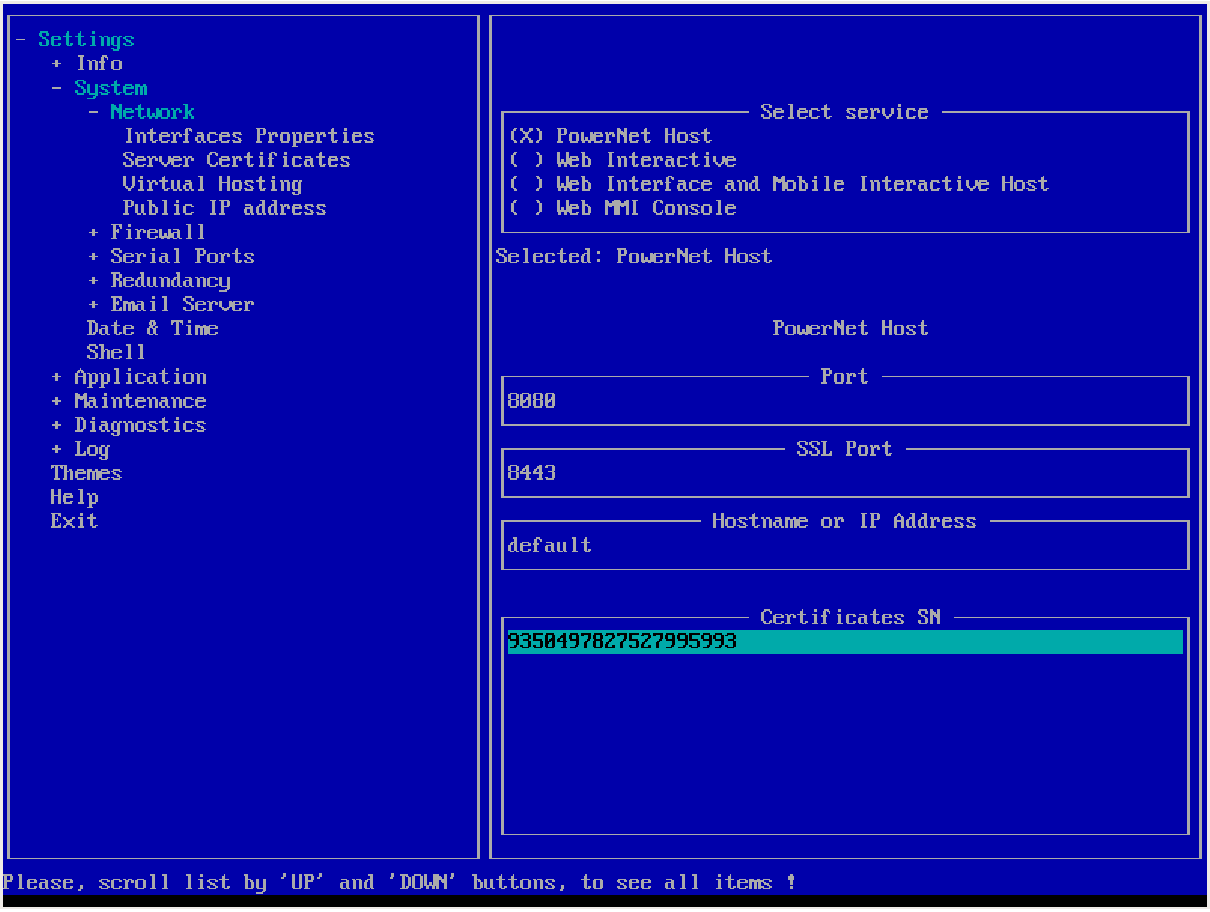
```
1585947961335l027346

Subject: *.tycomonitor.com
Issuer: Go Daddy Secure Certificate Authority - G2
Not before: 12-03-2019 08:58:12
Not after: 12-05-2020 11:09:00

passphrase_

You must decode private key if you want to use this certificate anywhere
```

❑ *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”



```
- Settings                                    
    + Info                                    
    - System                                  
        - Network                                      Select service
            Interfaces Properties           (X) PowerNet Host
            Server Certificates             ( ) Web Interactive
            Virtual Hosting                 ( ) Web Interface and Mobile Interactive Host
            Public IP address               ( ) Web MMI Console
        + Firewall
        + Serial Ports                     Selected: PowerNet Host
        + Redundancy
        + Email Server
        Date & Time                                    PowerNet Host
        Shell
    + Application                                          Port
    + Maintenance                           8080
    + Diagnostics
    + Log                                                SSL Port
    Themes                                  8443
    Help
    Exit                                           Hostname or IP Address
                                            default

                                                     Certificates SN
                                            9350497827527995993

Please, scroll list by 'UP' and 'DOWN' buttons, to see all items !
```

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.

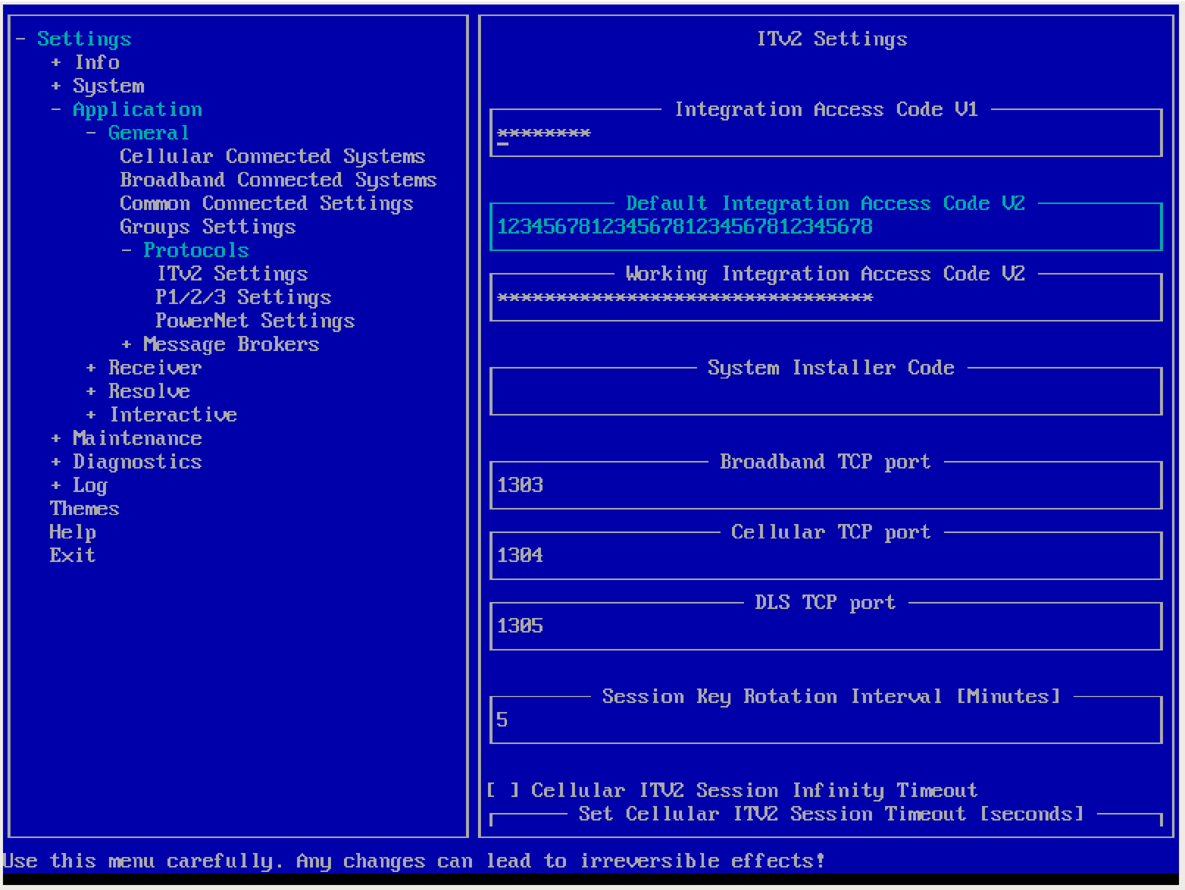
The Neo and PSP (Power Series Pro) panels communicate with the power-manage server via ITv2 protocol that is encrypted with ‘Working Integration Access Code’.

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.



```
- Settings
   + Info
   + System
   - Application
      - General
         Cellular Connected Systems
         Broadband Connected Systems
         Common Connected Settings
         Groups Settings
         - Protocols
            ITv2 Settings
            P1/2/3 Settings
            PowerNet Settings
         + Message Brokers
      + Receiver
      + Resolve
      + Interactive
   + Maintenance
   + Diagnostics
   + Log
   Themes
   Help
   Exit
```

```
                        ITv2 Settings

          Integration Access Code V1
*********

          Default Integration Access Code V2
12345678123456781234567812345678

          Working Integration Access Code V2
********************************

          System Installer Code


          Broadband TCP port
1303

          Cellular TCP port
1304

          DLS TCP port
1305

          Session Key Rotation Interval [Minutes]
5

[ ] Cellular ITV2 Session Infinity Timeout
          Set Cellular ITV2 Session Timeout [seconds]
```

```
Use this menu carefully. Any changes can lead to irreversible effects!
```

Notes:

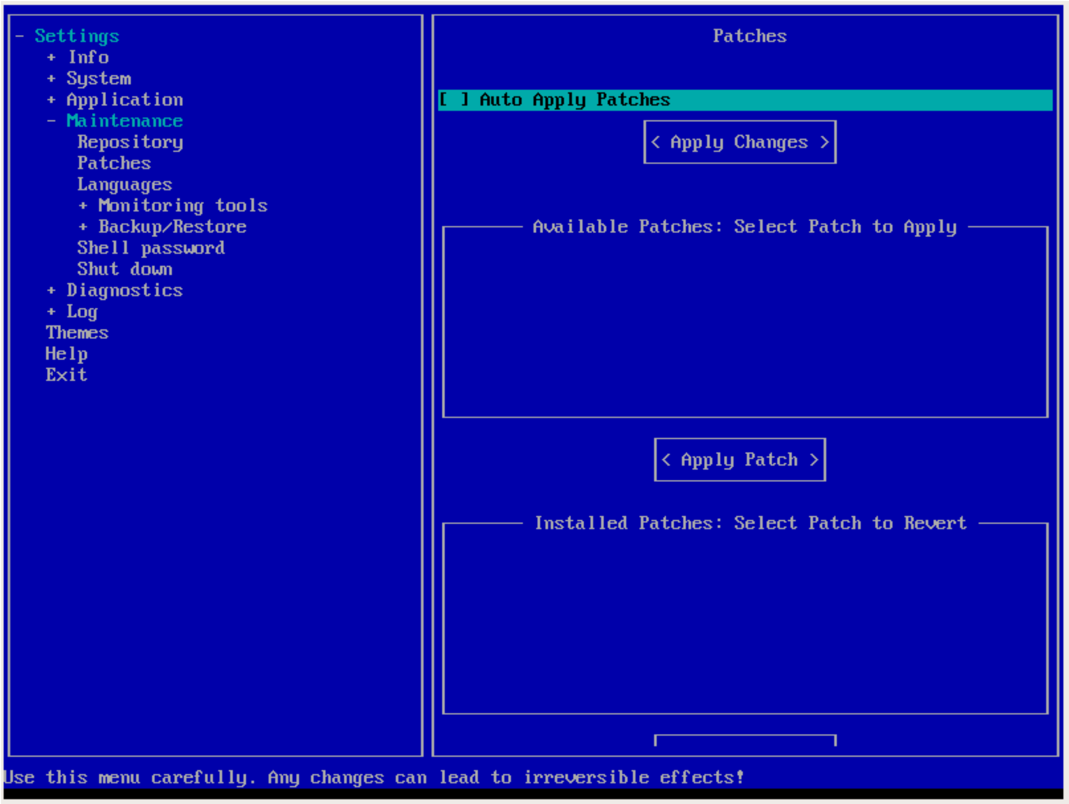
1) The 'Working Integration Access Code V2' value can remain in its default value or changed to any different value prior to any panel enrollment. If value changed after any panel enrollment, all the already enrolled panels will be disconnected.

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*

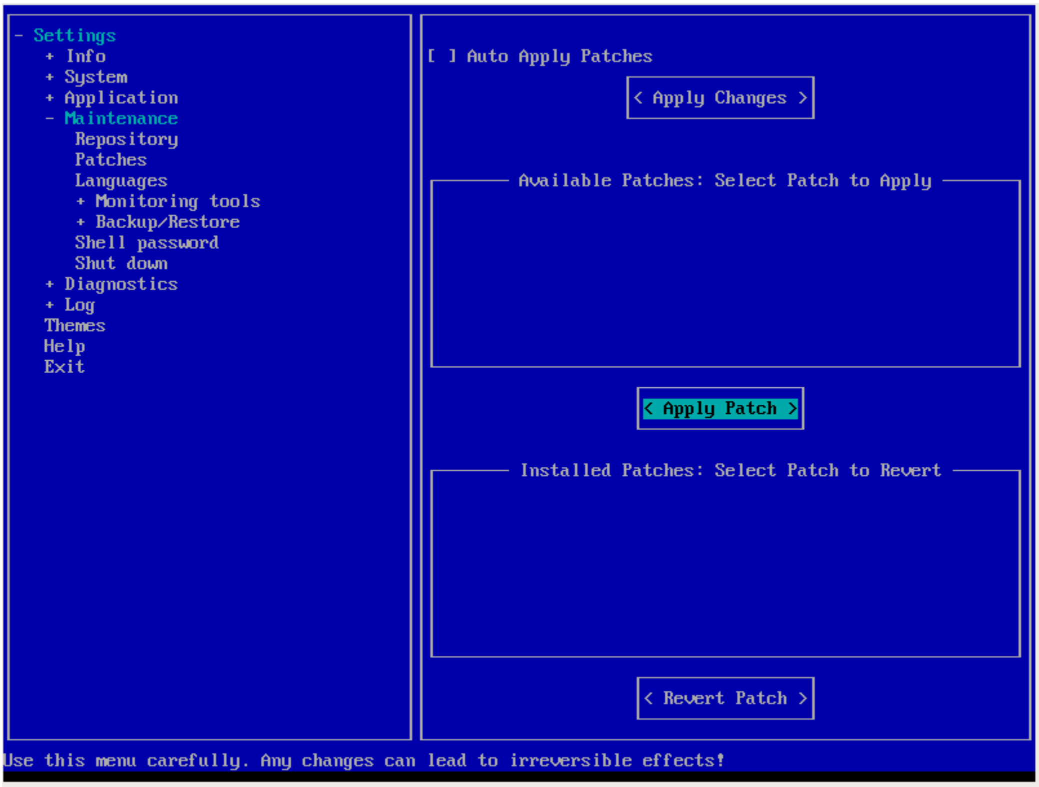
Verify repository settings configured on your server.

- ➢ 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**



Use this menu carefully. Any changes can lead to irreversible effects!

- ➢ 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

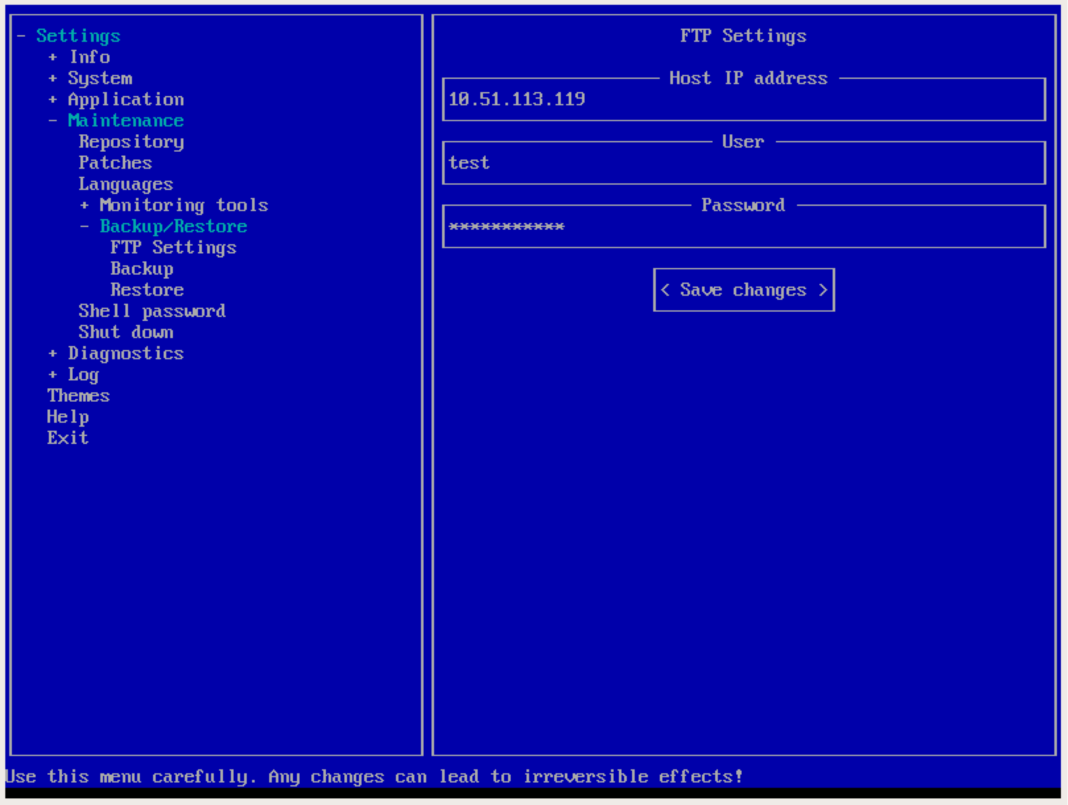


Use this menu carefully. Any changes can lead to irreversible effects!

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**



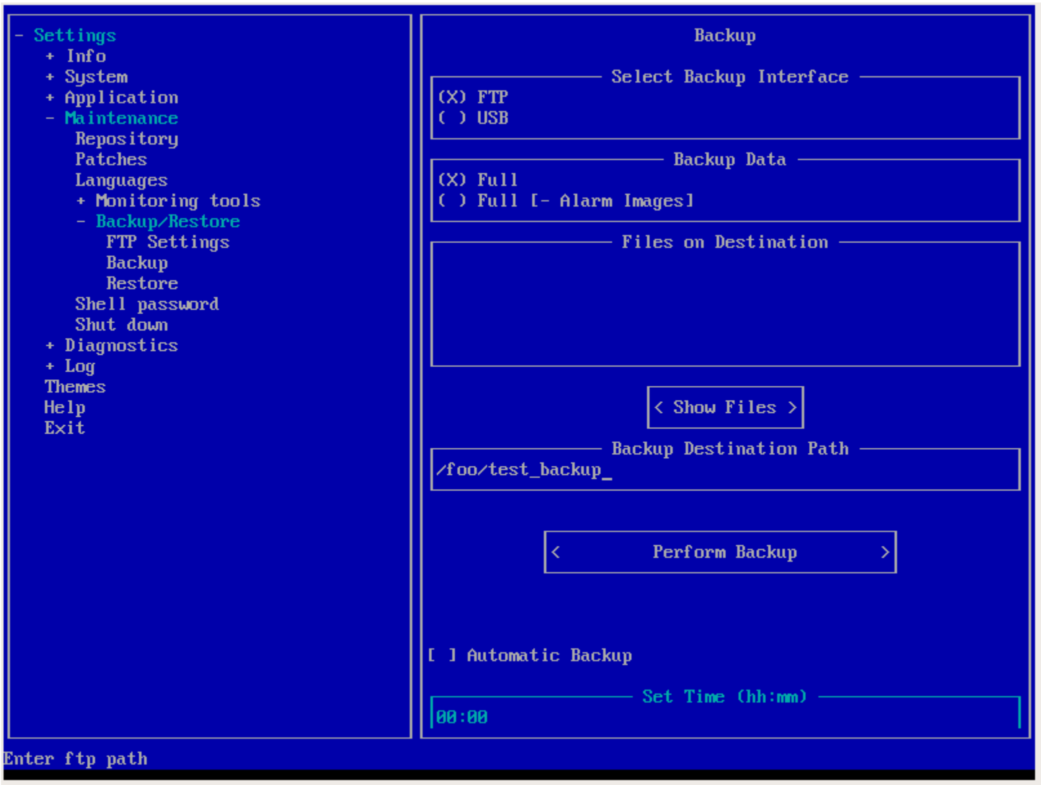
Host IP address
10.51.113.119

User
test

Password
****

Use this menu carefully. Any changes can lead to irreversible effects!

- 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**

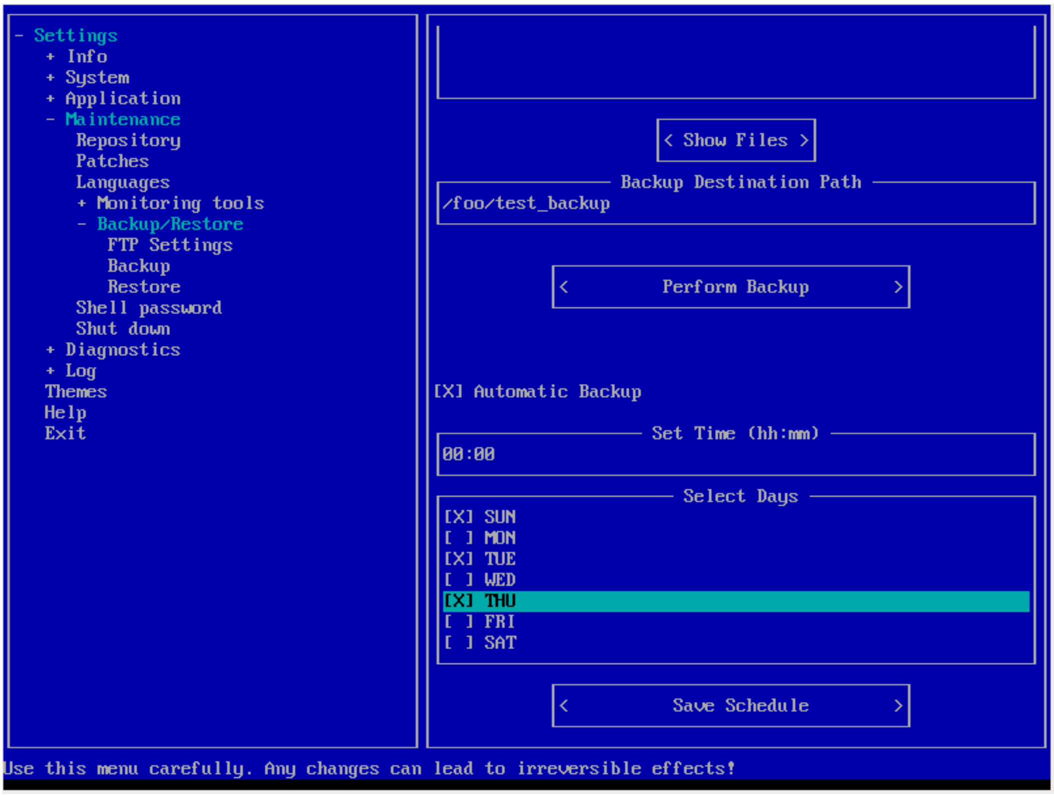


```
- Settings                              Backup
   + Info                  ──────── Select Backup Interface ────────
   + System                (X) FTP
   + Application           ( ) USB
   - Maintenance
      Repository           ──────────── Backup Data ────────────
      Patches              (X) Full
      Languages            ( ) Full [- Alarm Images]
      + Monitoring tools
      - Backup/Restore     ──────── Files on Destination ────────
         FTP Settings
         Backup
         Restore
      Shell password
      Shut down
   + Diagnostics
   + Log
   Themes                          < Show Files >
   Help
   Exit                    ────── Backup Destination Path ──────
                           /foo/test_backup_

                           <         Perform Backup         >


                           [ ] Automatic Backup

                           ────────── Set Time (hh:mm) ──────────
                           00:00
Enter ftp path
```

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

❑ *Backup to FTP server by schedule*

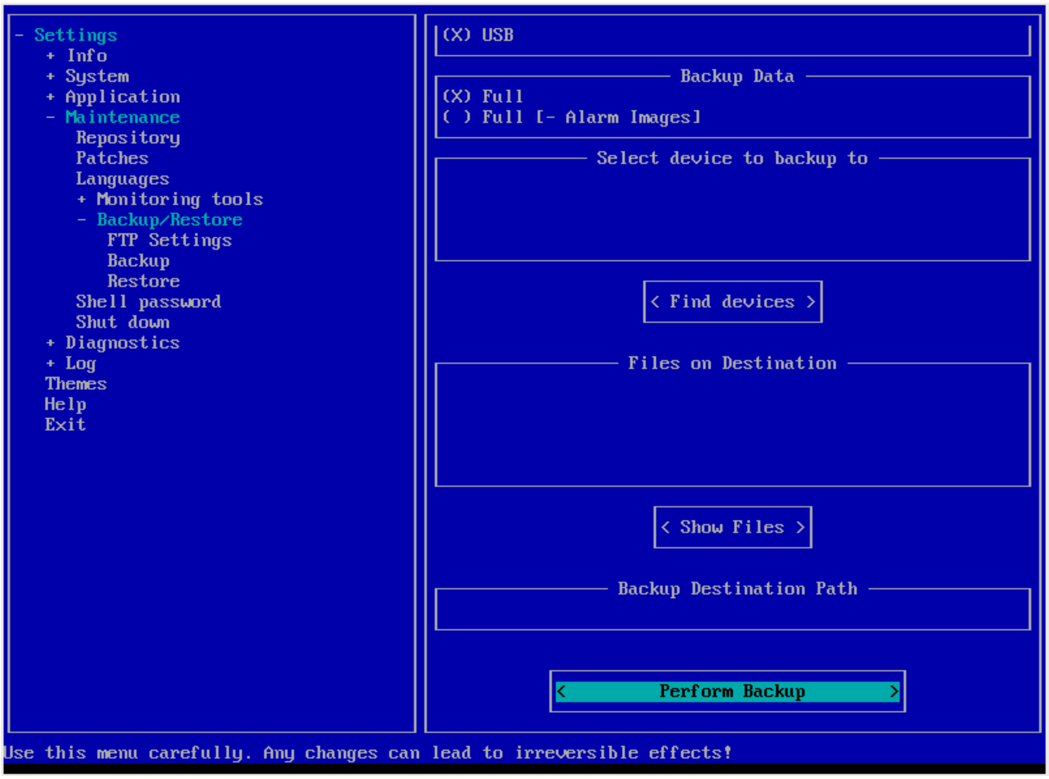
- ➢ Go to **Maintenance** > **Backup/Restore** > **Backup** menu
- ➢ Set backup method to **FTP**
- ➢ In **Backup Data** define which data do you want to include into backup
- ➢ In **Backup Destination Path** set absolute path and filename that you’re going to create
- ➢ Set the **Automatic Backup**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



```
- Settings
   + Info
   + System
   + Application
   - Maintenance
      Repository
      Patches
      Languages
      + Monitoring tools
      - Backup/Restore
         FTP Settings
         Backup
         Restore
      Shell password
      Shut down
   + Diagnostics
   + Log
   Themes
   Help
   Exit

                 < Show Files >

 Backup Destination Path
 /foo/test_backup

             <   Perform Backup   >

[X] Automatic Backup

 Set Time (hh:mm)
 00:00

 Select Days
 [X] SUN
 [ ] MON
 [X] TUE
 [ ] WED
 [X] THU
 [ ] FRI
 [ ] SAT

             <   Save Schedule   >

Use this menu carefully. Any changes can lead to irreversible effects!
```

❑ *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**

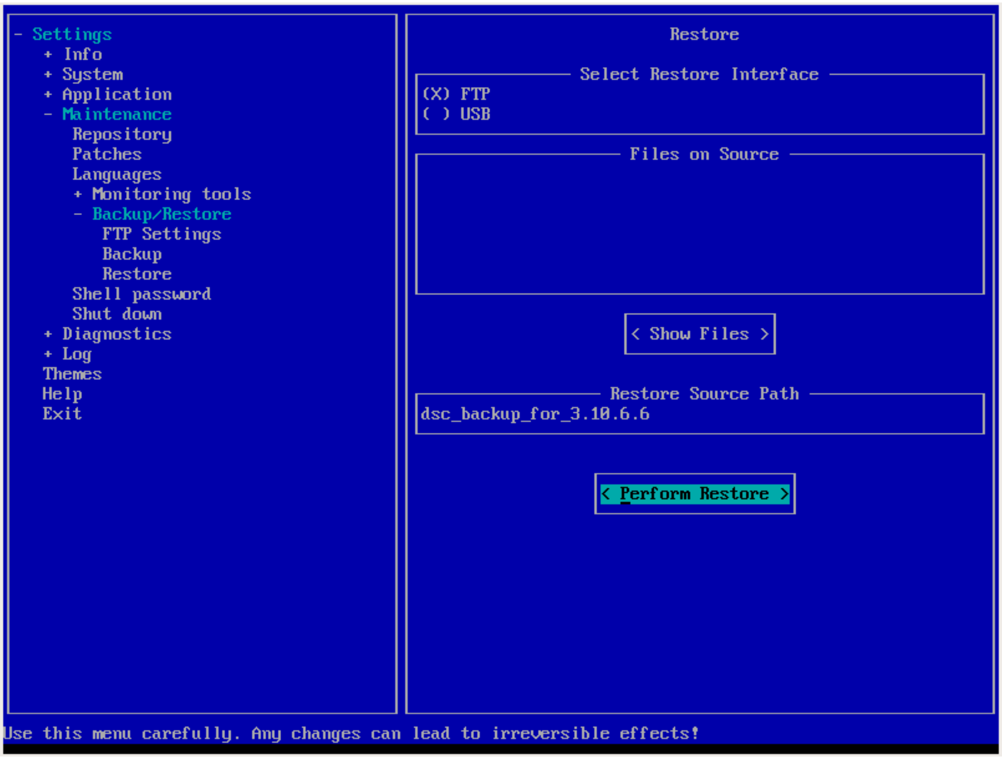


```
(X) USB

Backup Data
(X) Full
( ) Full [- Alarm Images]
```

Use this menu carefully. Any changes can lead to irreversible effects!

❑ *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**



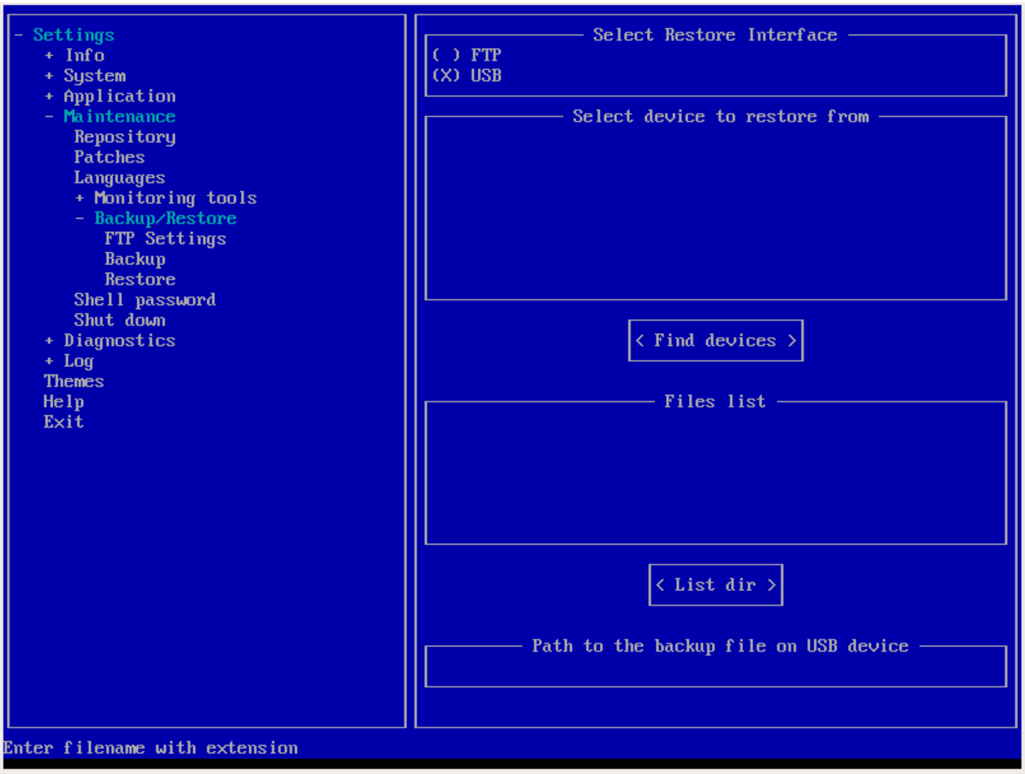
Select Restore Interface
(X) FTP
( ) USB

Restore Source Path
dsc_backup_for_3.10.6.6

Use this menu carefully. Any changes can lead to irreversible effects!

❑ *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**



Select Restore Interface
( ) FTP
(X) USB

Enter filename with extension

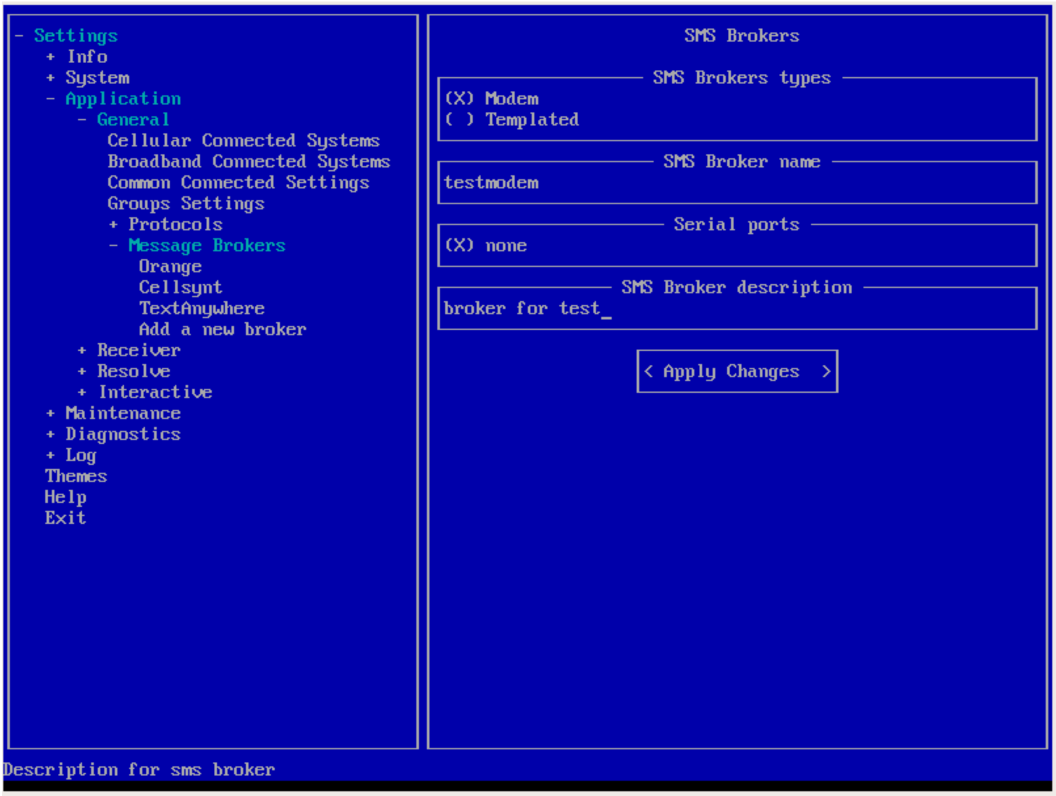
SMS Broker configuration

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*

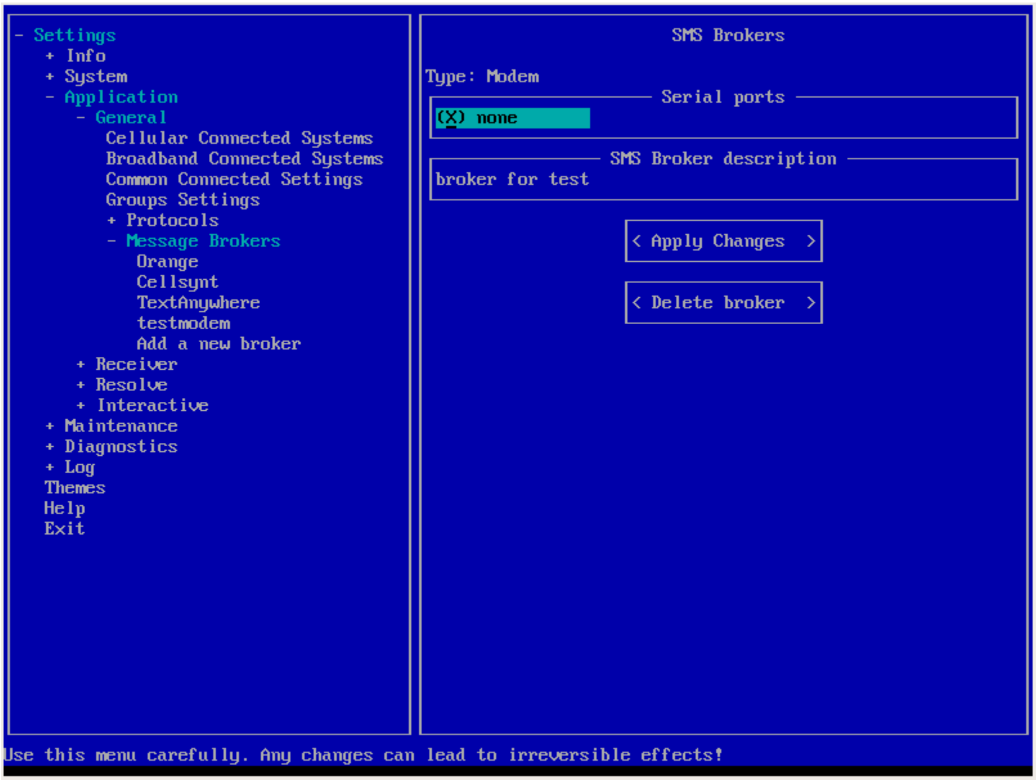
It’s meant that GSM modem is already connected to a servers’ configured serial port.

- ➢ 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**



```
- Settings                                        SMS Brokers
   + Info
   + System                          ─────────── SMS Brokers types ───────────
   - Application                     (X) Modem
      - General                      ( ) Templated
         Cellular Connected Systems
         Broadband Connected Systems ─────────── SMS Broker name ─────────────
         Common Connected Settings   testmodem
         Groups Settings
         + Protocols                 ─────────── Serial ports ────────────────
         - Message Brokers           (X) none
            Orange
            Cellsynt                 ─────────── SMS Broker description ──────
            TextAnywhere             broker for test_
            Add a new broker
      + Receiver                            < Apply Changes >
      + Resolve
      + Interactive
   + Maintenance
   + Diagnostics
   + Log
   Themes
   Help
   Exit

Description for sms broker
```

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

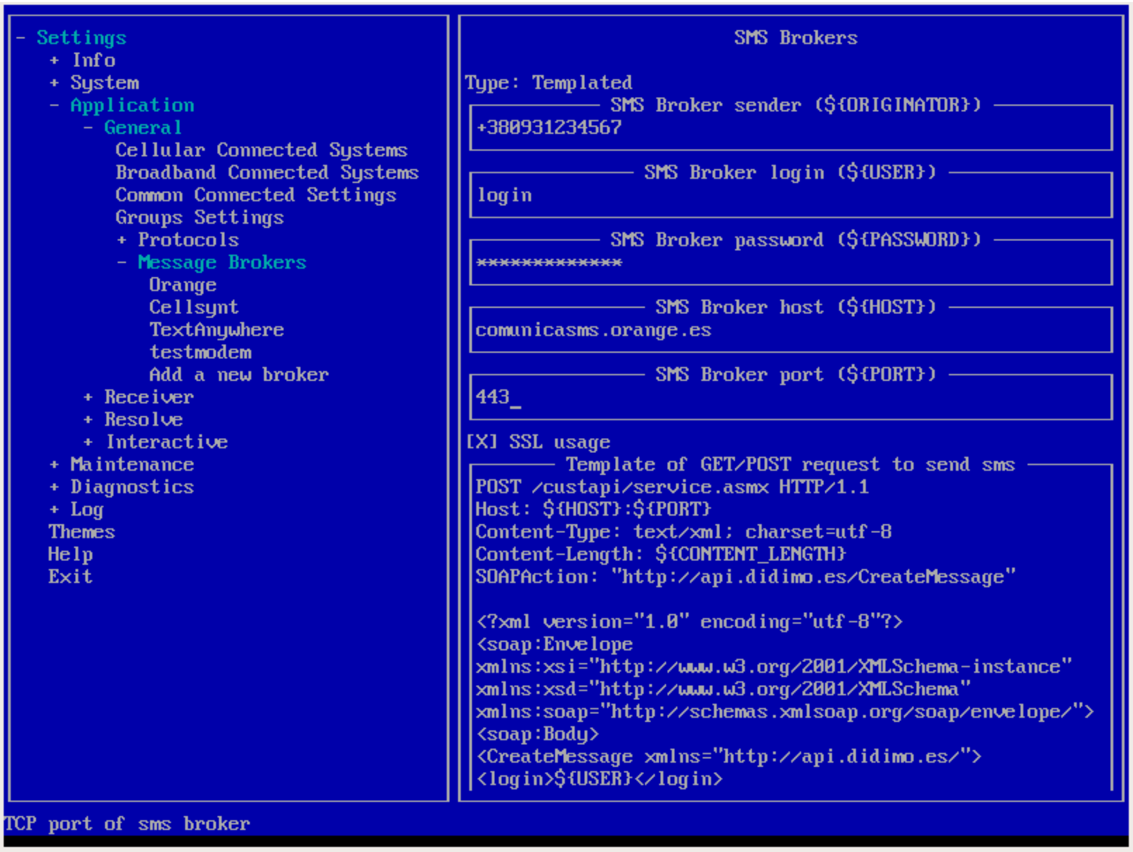


```
- Settings                                          SMS Brokers
   + Info
   + System                              Type: Modem
   - Application                          ─────────── Serial ports ───────────
      - General                           (X) none
         Cellular Connected Systems
         Broadband Connected Systems      ──────── SMS Broker description ────────
         Common Connected Settings        broker for test
         Groups Settings
         + Protocols                               < Apply Changes  >
         - Message Brokers
            Orange                                 < Delete broker  >
            Cellsynt
            TextAnywhere
            testmodem
            Add a new broker
      + Receiver
      + Resolve
      + Interactive
   + Maintenance
   + Diagnostics
   + Log
   Themes
   Help
   Exit
Use this menu carefully. Any changes can lead to irreversible effects!
```

❑ *Adding SMS broker*

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

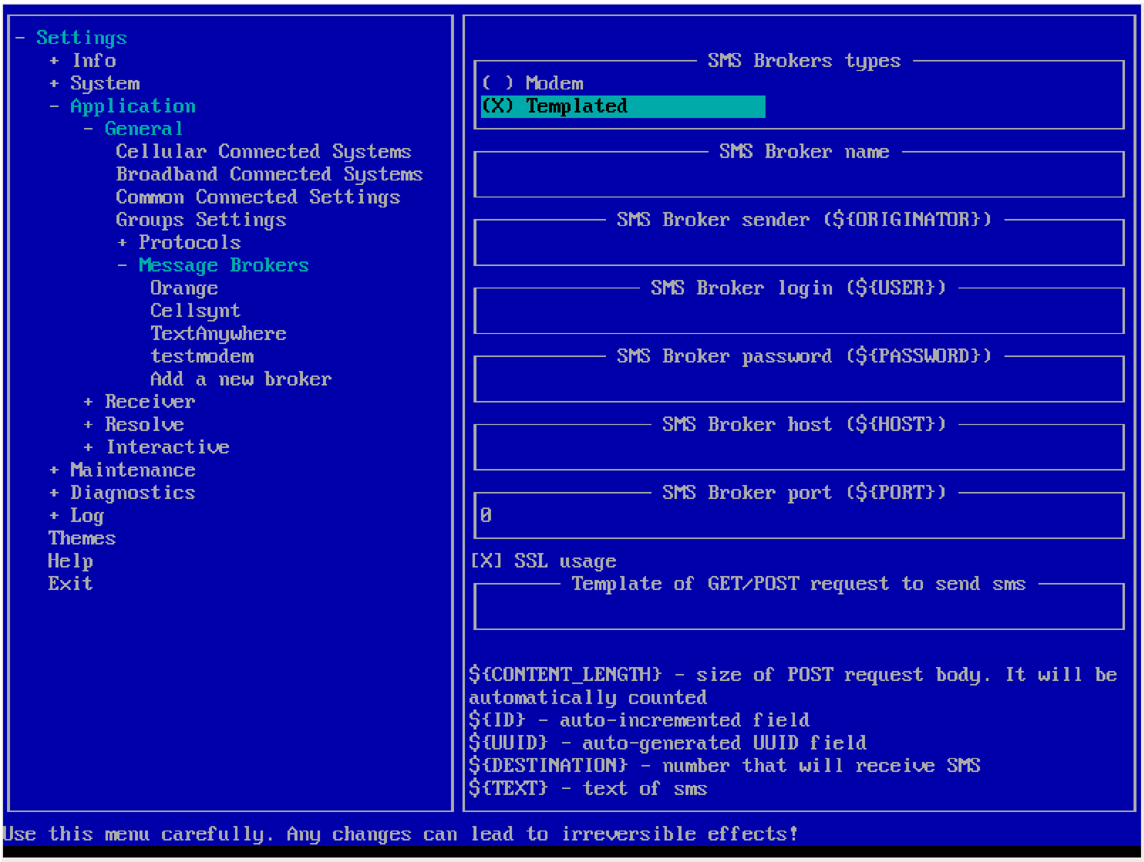
- ➢ In MMI menu go to **Application** > **General** > **Message Brokers**
- ➢ Choose Orange/Cellsynt/TextAnywhere
- ➢ In **SMS Broker sender** set your broker phone number. (This number will be indicated to the client as a source sender number of SMSs sent by your server)
- ➢ In **SMS Broker login**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



```
SMS Brokers

Type: Templated
SMS Broker sender (${ORIGINATOR})
+380931234567
SMS Broker login (${USER})
login
SMS Broker password (${PASSWORD})
*************
SMS Broker host (${HOST})
comunicasms.orange.es
SMS Broker port (${PORT})
443_
[X] SSL usage
Template of GET/POST request to send sms
POST /custapi/service.asmx HTTP/1.1
Host: ${HOST}:${PORT}
Content-Type: text/xml; charset=utf-8
Content-Length: ${CONTENT_LENGTH}
SOAPAction: "http://api.didimo.es/CreateMessage"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<CreateMessage xmlns="http://api.didimo.es/">
<login>${USER}</login>

TCP port of sms 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



```
SMS Brokers types
( ) Modem
(X) Templated
SMS Broker name

SMS Broker sender (${ORIGINATOR})

SMS Broker login (${USER})

SMS Broker password (${PASSWORD})

SMS Broker host (${HOST})

SMS Broker port (${PORT})
0
[X] SSL usage
Template of GET/POST request to send sms


${CONTENT_LENGTH} - size of POST request body. It will be
automatically counted
${ID} - auto-incremented field
${UUID} - auto-generated UUID field
${DESTINATION} - number that will receive SMS
${TEXT} - text of sms
Use this menu carefully. Any changes can lead to irreversible effects!
```

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

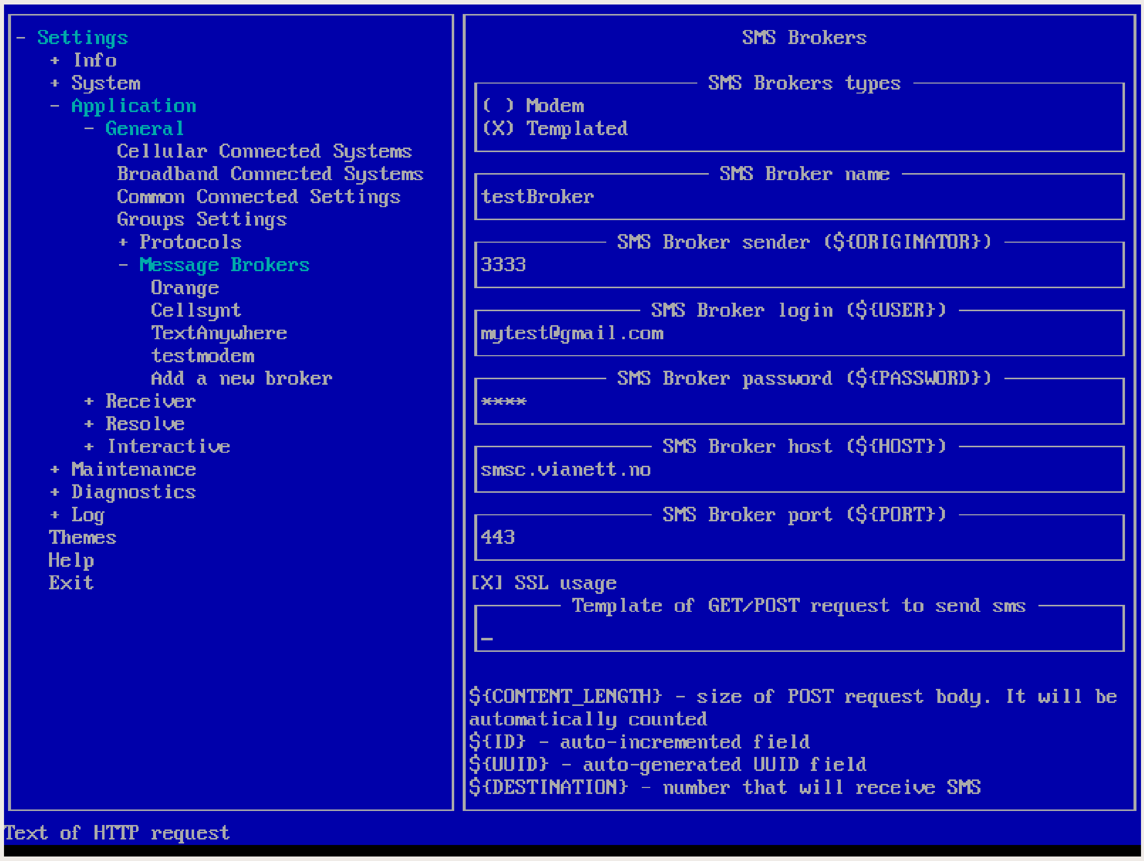
NOTE: It's important to set HTTP request line breaks correctly. Request's body should be one line. Although there are automatic line breaks, all new lines should be created with **Enter**:

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**

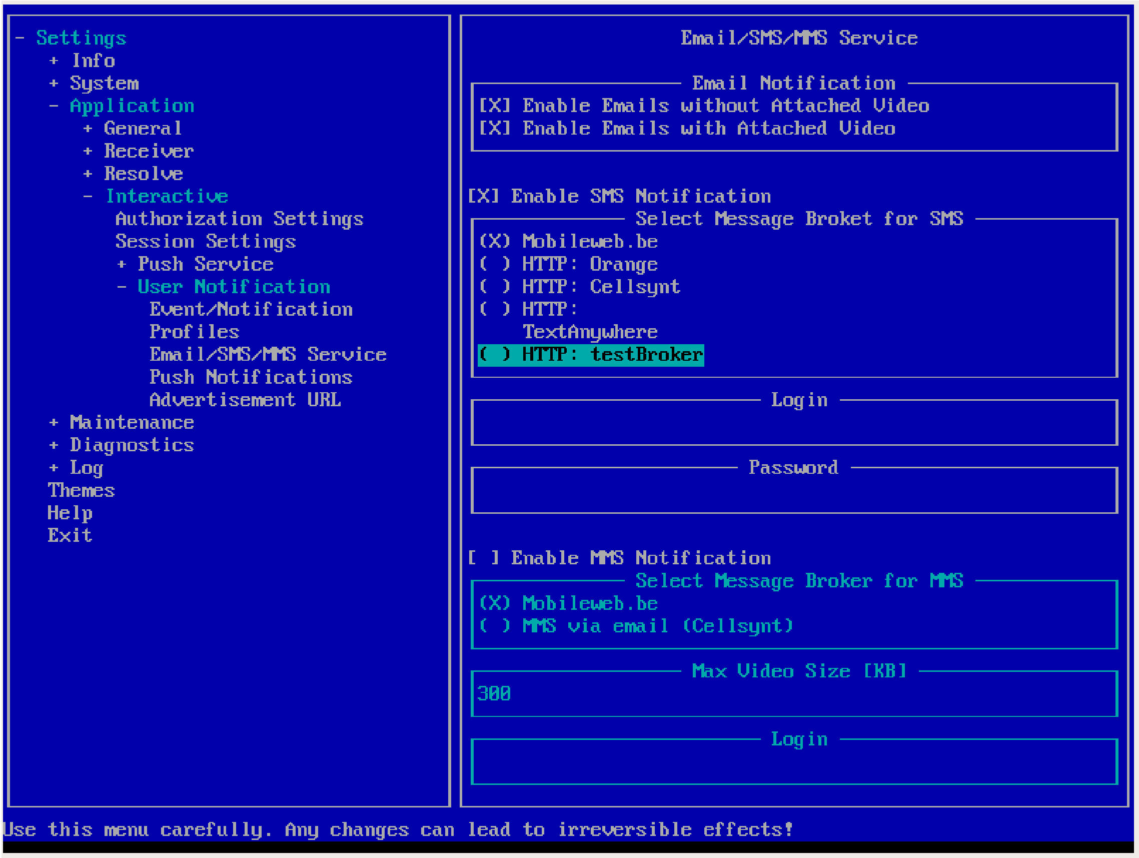


```
- Settings
   + Info
   + System
   - Application
      - General
         Cellular Connected Systems
         Broadband Connected Systems
         Common Connected Settings
         Groups Settings
         + Protocols
         - Message Brokers
            Orange
            Cellsynt
            TextAnywhere
            testmodem
            Add a new broker
      + Receiver
      + Resolve
      + Interactive
   + Maintenance
   + Diagnostics
   + Log
   Themes
   Help
   Exit
```

```
                         SMS Brokers

 ------------------ SMS Brokers types ------------------
 ( ) Modem
 (X) Templated

 ------------------- SMS Broker name -------------------
 testBroker

 ------------ SMS Broker sender (${ORIGINATOR}) ---------
 3333

 -------------- SMS Broker login (${USER}) --------------
 mytest@gmail.com

 ----------- SMS Broker password (${PASSWORD}) ----------
 ****

 --------------- SMS Broker host (${HOST}) --------------
 smsc.vianett.no

 --------------- SMS Broker port (${PORT}) --------------
 443

[X] SSL usage
 --------- Template of GET/POST request to send sms -----
 _

${CONTENT_LENGTH} - size of POST request body. It will be
automatically counted
${ID} - auto-incremented field
${UUID} - auto-generated UUID field
${DESTINATION} - number that will receive SMS
```

```
Text of HTTP request
```

- ➢ 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**



```
- Settings
   + Info
   + System
   - Application
      + General
      + Receiver
      + Resolve
      - Interactive
         Authorization Settings
         Session Settings
         + Push Service
         - User Notification
            Event/Notification
            Profiles
            Email/SMS/MMS Service
            Push Notifications
            Advertisement URL
   + Maintenance
   + Diagnostics
   + Log
   Themes
   Help
   Exit
```

```
                    Email/SMS/MMS Service

 ------------------ Email Notification -----------------
 [X] Enable Emails without Attached Video
 [X] Enable Emails with Attached Video

[X] Enable SMS Notification
 -------------- Select Message Broket for SMS -----------
 (X) Mobileweb.be
 ( ) HTTP: Orange
 ( ) HTTP: Cellsynt
 ( ) HTTP:
     TextAnywhere
 ( ) HTTP: testBroker

 ------------------------ Login ------------------------


 ----------------------- Password ----------------------


[ ] Enable MMS Notification
 -------------- Select Message Broker for MMS -----------
 (X) Mobileweb.be
 ( ) MMS via email (Cellsynt)

 ------------------ Max Video Size [KB] -----------------
 300

 ------------------------ Login ------------------------
```

```
Use this menu carefully. Any changes can lead to irreversible effects!
```

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.

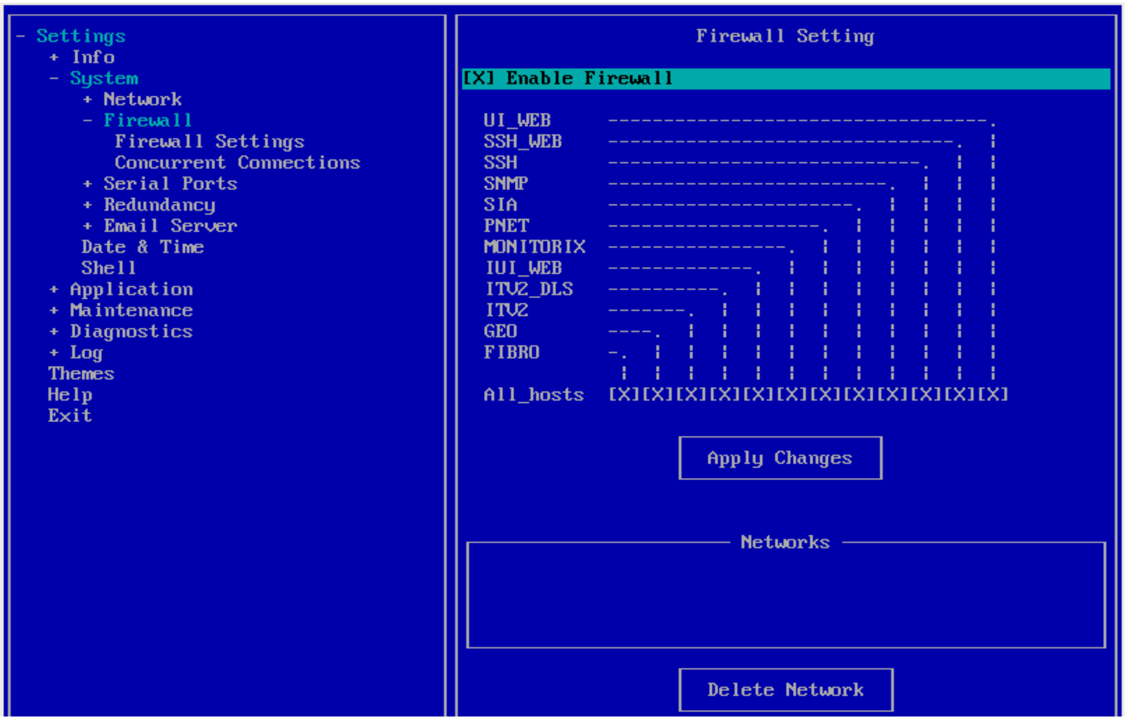
The key point is that the internal firewall is considered as supplementary measure to an external firewall. There is still an advice to use an external firewall on top of PowerManage servers. It should provide more reliable stability and avoid performance issues.

❑ *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.

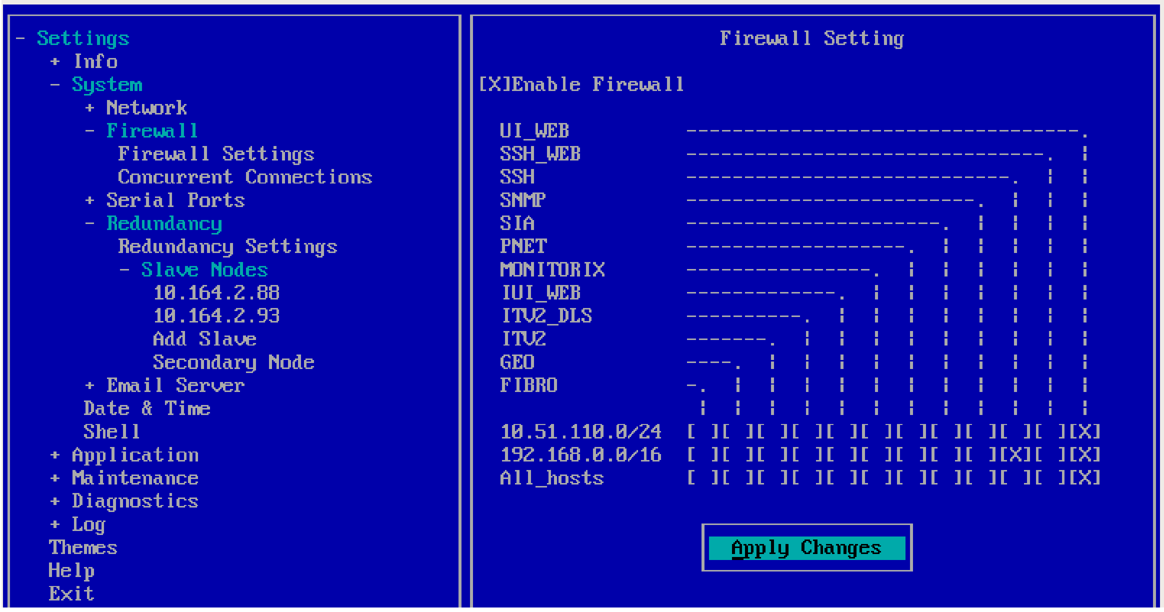
- In MMI menu go to **System** > **Firewall** > **Firewall Settings**
- In the **Add New Network** set the network in the following format: x.x.x.x/y
- Press **Add Network**



```
[X] Enable Firewall

UI_WEB
SSH_WEB
SSH
SNMP
SIA
PNET
MONITORIX
IUI_WEB
ITV2_DLS
ITV2
GEO
FIBRO

All_hosts   [X][X][X][X][X][X][X][X][X][X][X][X]
```

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.

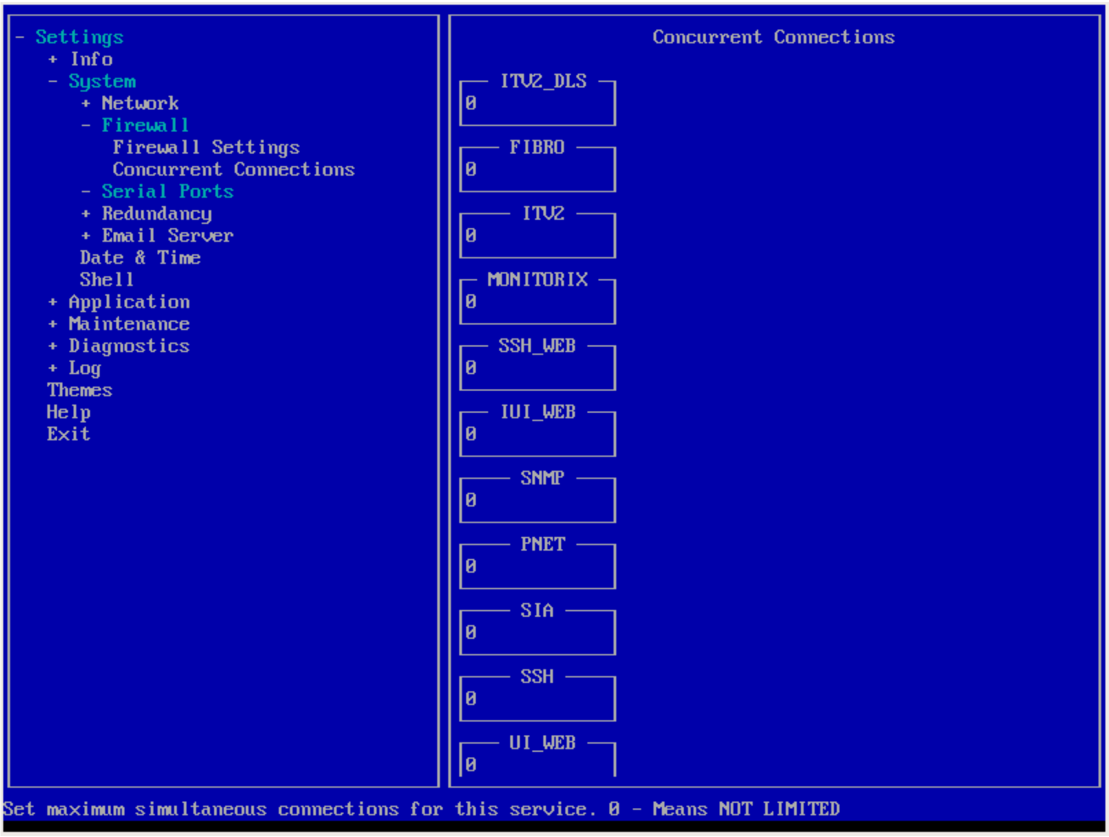


```
                    Firewall Setting

[X]Enable Firewall

  UI_WEB          ----------------------------------.
  SSH_WEB         -------------------------------.  ¦
  SSH             ----------------------------.  ¦  ¦
  SNMP            -------------------------.  ¦  ¦  ¦
  SIA             ----------------------.  ¦  ¦  ¦  ¦
  PNET            -------------------.  ¦  ¦  ¦  ¦  ¦
  MONITORIX       ----------------.  ¦  ¦  ¦  ¦  ¦  ¦
  IUI_WEB         -------------.  ¦  ¦  ¦  ¦  ¦  ¦  ¦
  ITV2_DLS        ----------.  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦
  ITV2            -------.  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦
  GEO             ----.  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦
  FIBRO           -.  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦
                   ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦  ¦
  10.51.110.0/24  [ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][X]
  192.168.0.0/16  [ ][ ][ ][ ][ ][ ][ ][ ][ ][X][ ][X]
  All_hosts       [ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][ ][X]

                  Apply Changes
```

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.



```
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
```

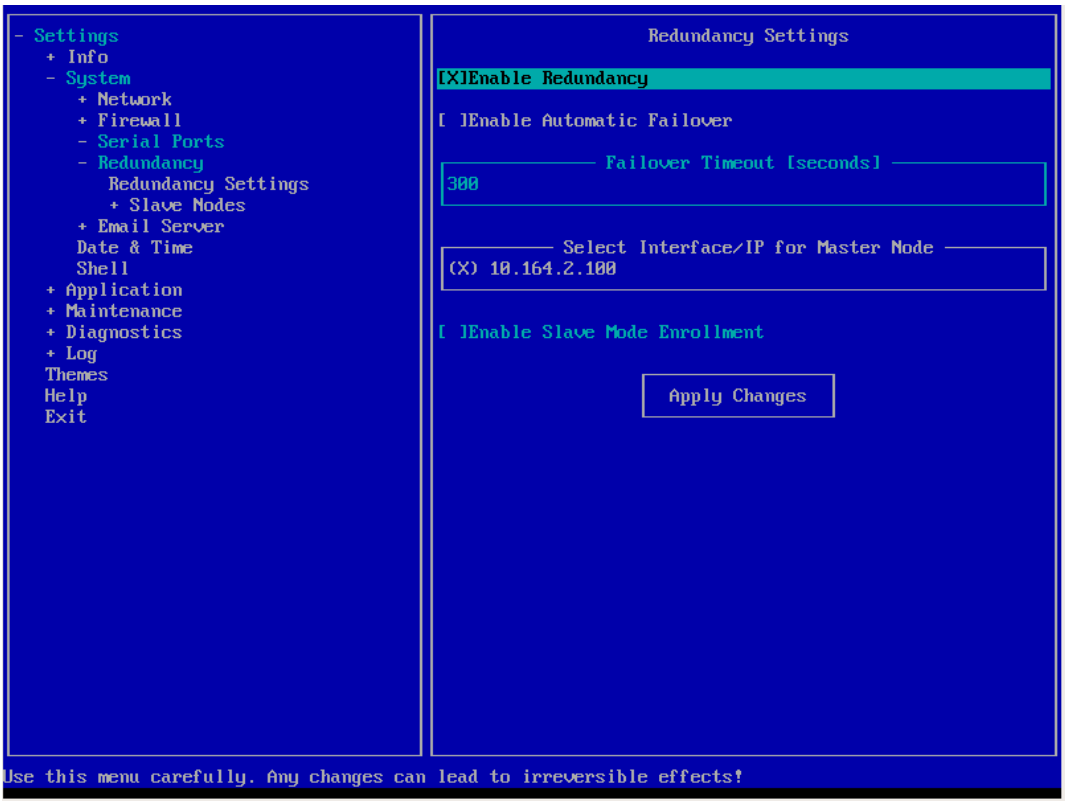
Redundancy configuration

❑ *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



Redundancy Settings

[X]Enable Redundancy

[ ]Enable Automatic Failover

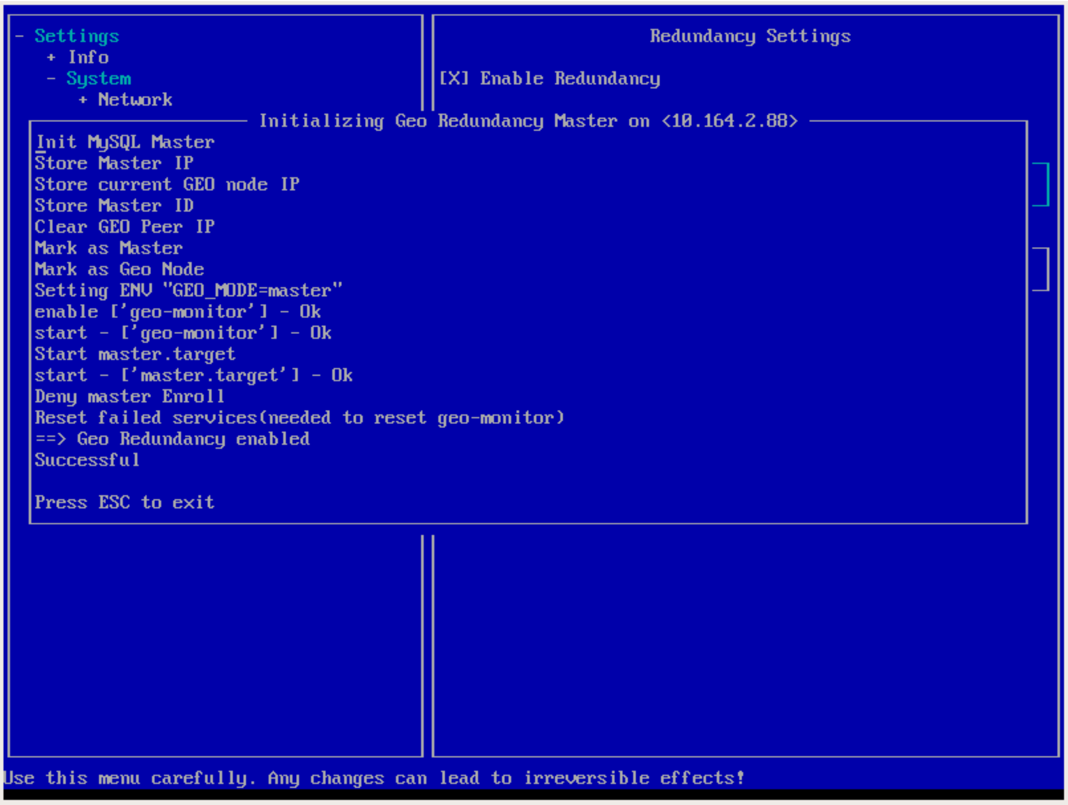
Failover Timeout [seconds]: 300

Select Interface/IP for Master Node: (X) 10.164.2.100

[ ]Enable Slave Mode Enrollment

Use this menu carefully. Any changes can lead to irreversible effects!

- ➢ 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



Redundancy Settings

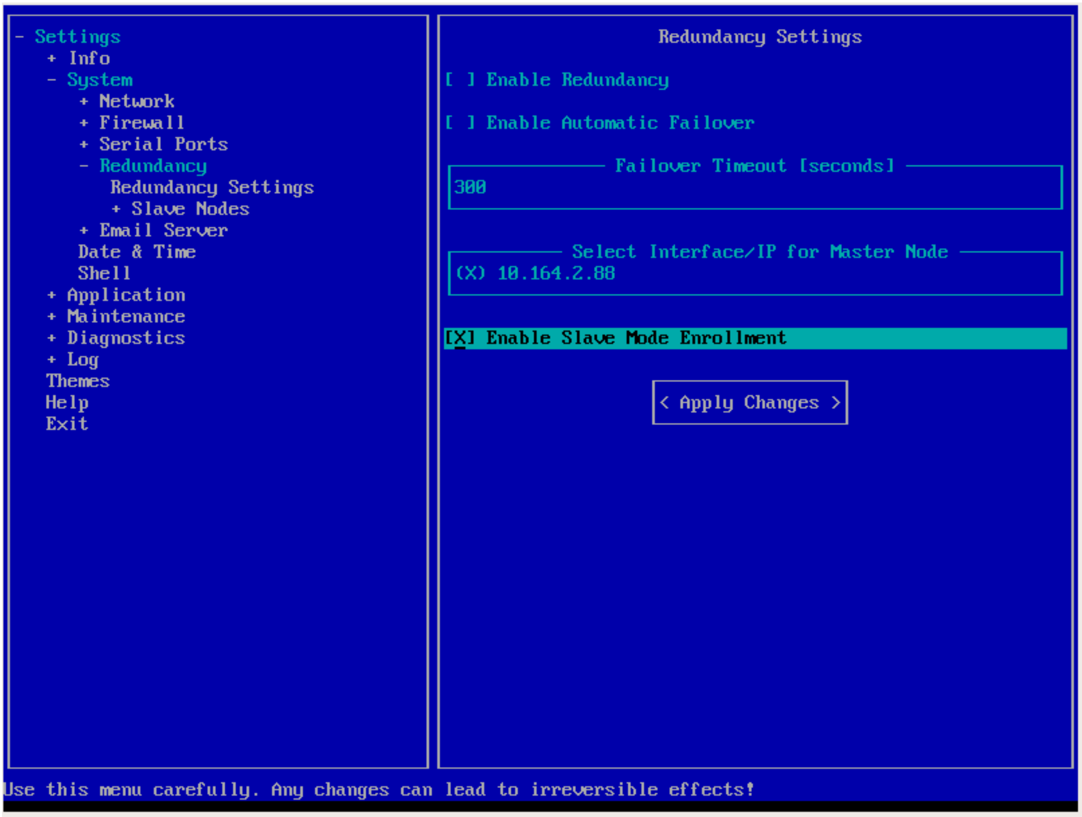
[X] Enable Redundancy

Initializing Geo Redundancy Master on <10.164.2.88>

```
Init MySQL Master
Store Master IP
Store current GEO node IP
Store Master ID
Clear GEO Peer IP
Mark as Master
Mark as Geo Node
Setting ENV "GEO_MODE=master"
enable ['geo-monitor'] - Ok
start - ['geo-monitor'] - Ok
Start master.target
start - ['master.target'] - Ok
Deny master Enroll
Reset failed services(needed to reset geo-monitor)
==> Geo Redundancy enabled
Successful

Press ESC to exit
```

Use this menu carefully. Any changes can lead to irreversible effects!

- ➢ 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)



Redundancy Settings

[ ] Enable Redundancy

[ ] Enable Automatic Failover

Failover Timeout [seconds]: 300

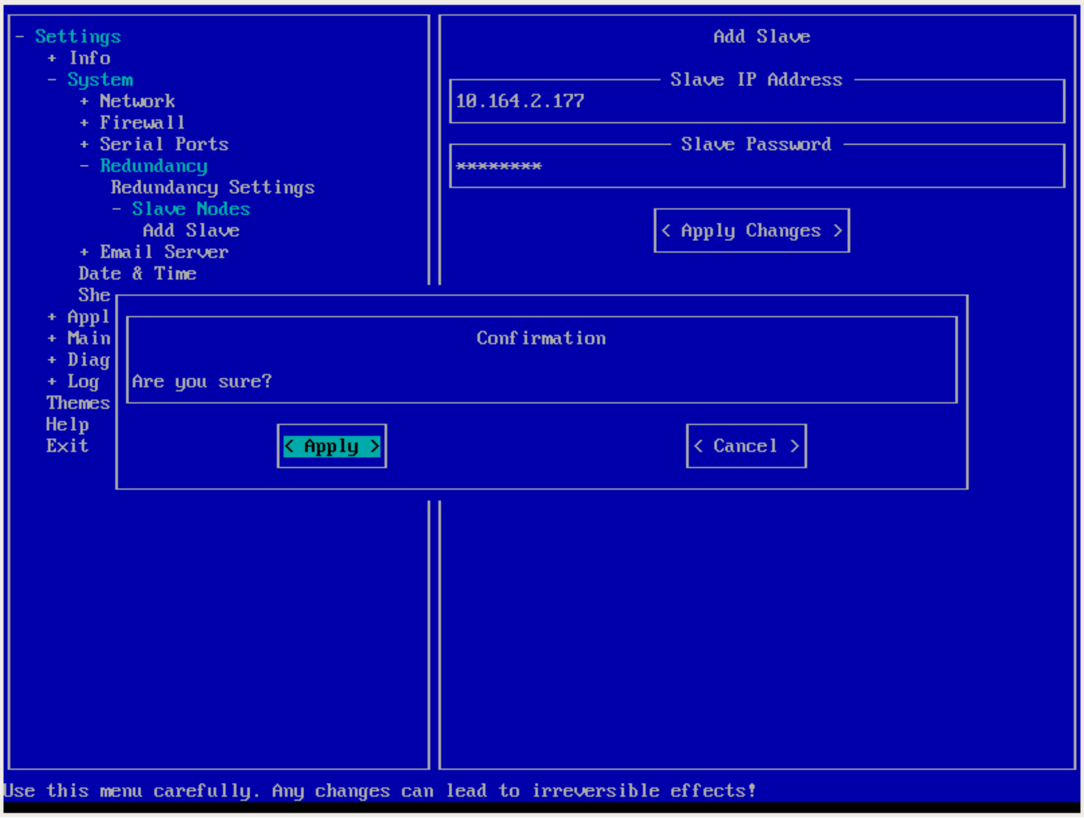
Select Interface/IP for Master Node: (X) 10.164.2.88

[X] Enable Slave Mode Enrollment

Use this menu carefully. Any changes can lead to irreversible effects!

- ➢ 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



Slave IP Address: 10.164.2.177

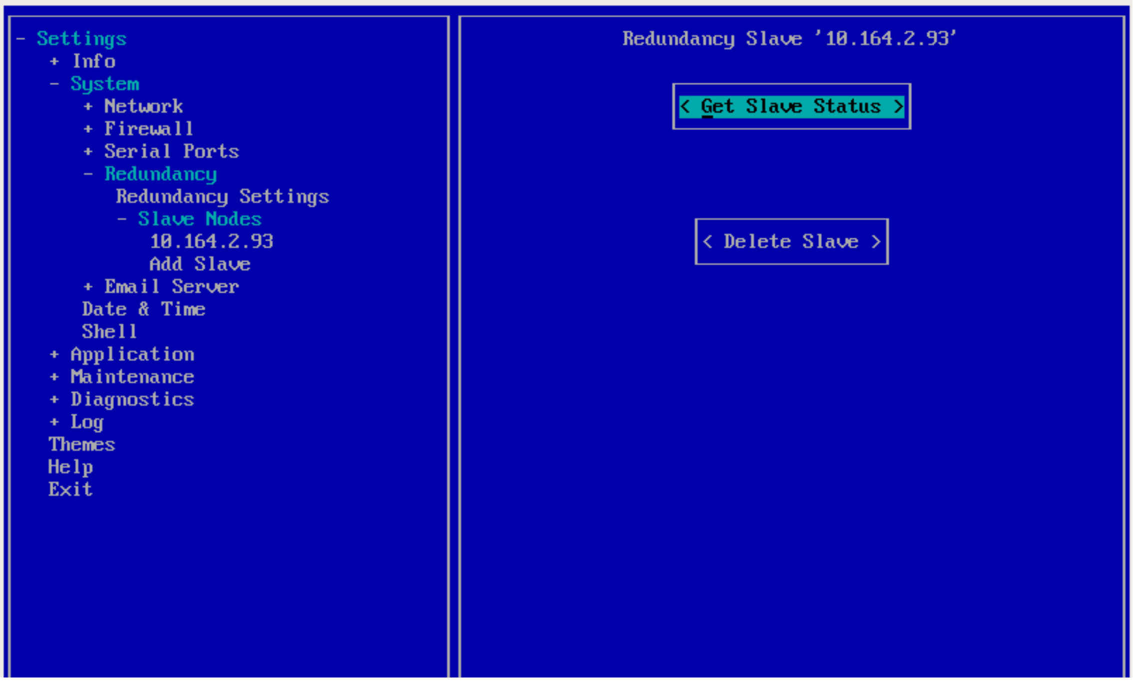
Slave Password: *********

Confirmation

Are you sure?

Use this menu carefully. Any changes can lead to irreversible effects!

- 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**

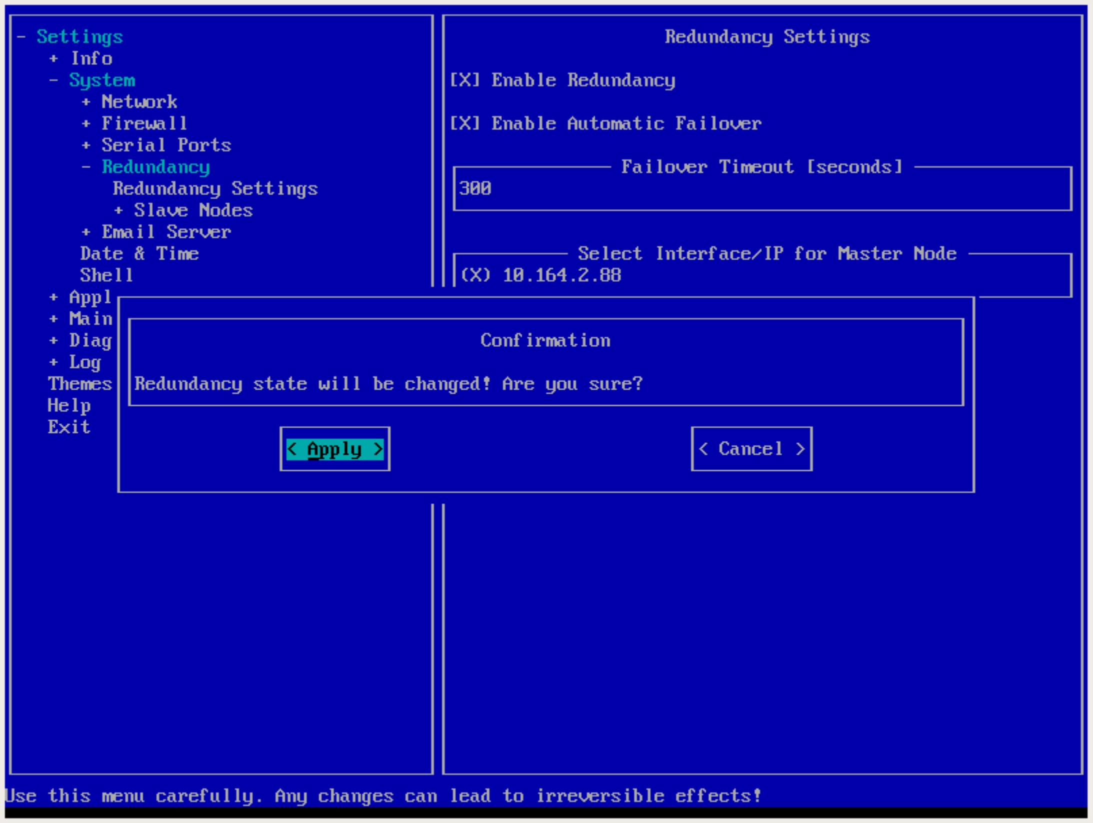


Redundancy Slave ’10.164.2.93’

• *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



```
- Settings                                        Redundancy Settings
   + Info
   - System                             [X] Enable Redundancy
      + Network
      + Firewall                        [X] Enable Automatic Failover
      + Serial Ports
      - Redundancy                       ------- Failover Timeout [seconds] -------
         Redundancy Settings            300
         + Slave Nodes
      + Email Server
      Date & Time                        ------- Select Interface/IP for Master Node -------
      Shell                             (X) 10.164.2.88
   + Appl
   + Main                                   Confirmation
   + Diag
   + Log
   Themes   Redundancy state will be changed! Are you sure?
   Help
   Exit             < Apply >                         < Cancel >

Use this menu carefully. Any changes can lead to irreversible effects!
```

• *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.

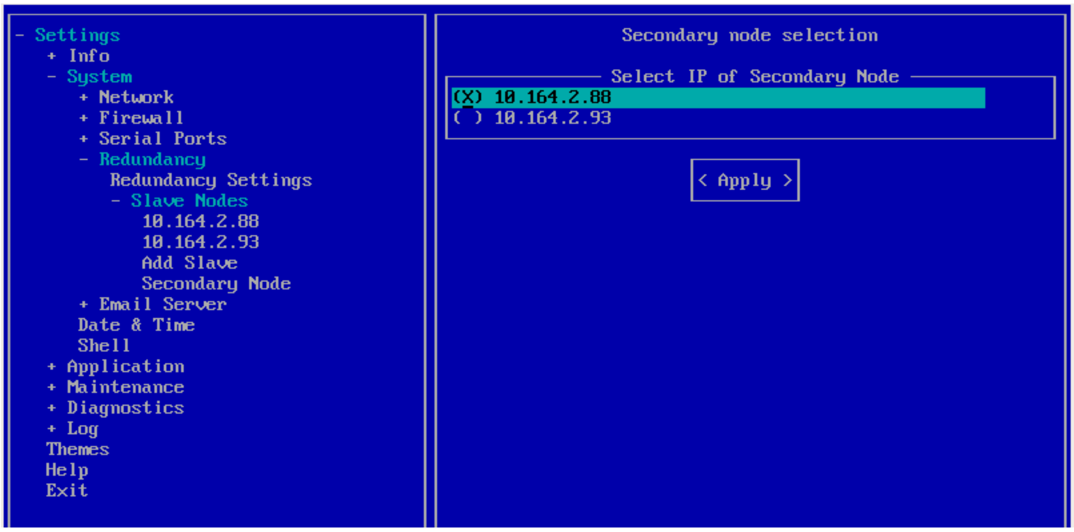
IMPORTANT: in GEO redundancy slave nodes have some services disabled which include WEB GUI and REST API. As far as DSC NEO panel require prior activation before panels will be able to perform a discovery process, and the activation may be done from either the WEB GUI or the user application (requires 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.

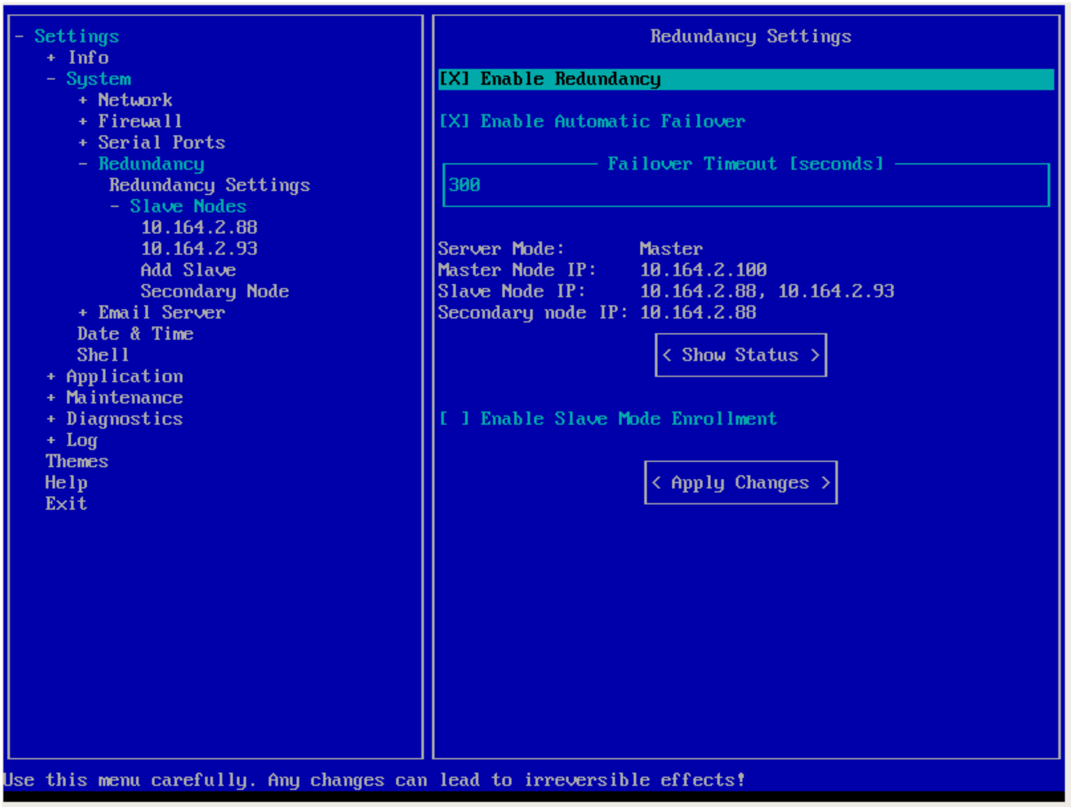
In case of manual failover configuration, the failover has to be performed in a familiar way as for two nodes redundancy in case of Master fail. Primary Slave should be re-configured as Master and new Primary Slave should be designated. Primary Slave can be configured in **System** > **Redundancy** >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



```
Secondary node selection

Select IP of Secondary Node
(X) 10.164.2.88
( ) 10.164.2.93
```

- ➢ 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**



```
[X] Enable Redundancy

[X] Enable Automatic Failover

Failover Timeout [seconds]
300

Server Mode:        Master
Master Node IP:     10.164.2.100
Slave Node IP:      10.164.2.88, 10.164.2.93
Secondary node IP:  10.164.2.88

[ ] Enable Slave Mode Enrollment

Use this menu carefully. Any changes can lead to irreversible effects!
```

- 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.

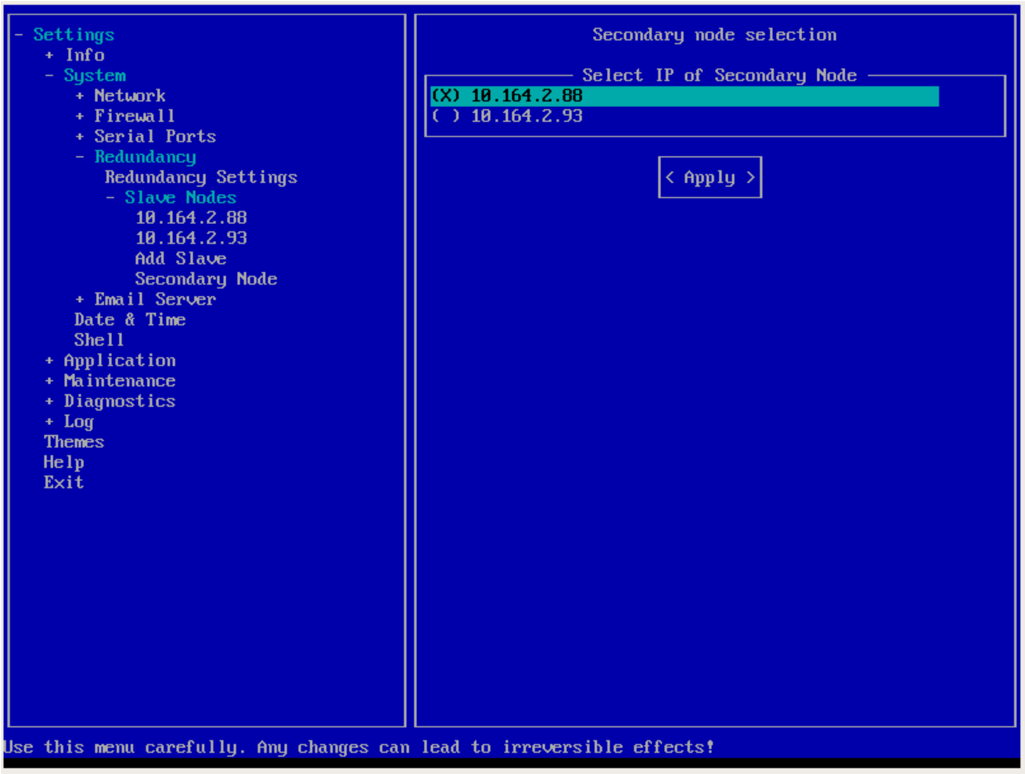
- ➢ Enter Primary Slave ' MMI and in **System** > **Redundancy** > **Redundancy Settings** disable **Enable Redundancy** option and press **Apply Changes**
- ➢ Exit MMI menu and login again
- ➢ For each Slave and former Master disable redundancy in **System** > **Redundancy** > **Redundancy Settings**
- ➢ 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.



```
Secondary node selection

Select IP of Secondary Node
(X) 10.164.2.88
( ) 10.164.2.93
```

```
Use this menu carefully. Any changes can lead to irreversible effects!
```

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.