PowerManage 3.10

Requirements and Installation Guide

Contents

Contents
About this publication
Who should read this guide
Notices
Support
About PowerManage
Chapter 1 PowerManage requirements 1
Hardware requirements 2
High performance system 2
HPE ProLiant DL380 Gen9 2
Medium performance system 3
HPE ProLiant DL380 Gen9 3
Low cost systems 4
Dell OptiPlex 3050 4
Dell OptiPlex 3040 4
Virtual environment hardware requirements 5
Legacy hardware requirements 5
HAProxy hardware requirements 6
High performance server 6
Medium performance server 6
Rack and power outlet requirements 7
Network and firewall requirements 8
Port number and IP address settings 8
Network diagrams 10
Standalone configuration 10
Two node multisite configuration 11
Four node multisite configuration 11
Software requirements 12
HPE Integrated Lights Out (iLO) 12
Client requirements 12
Chapter 2 PowerManage installation 13
Planning to install PowerManage 14
Prerequisites 14
Preparing the media 14
Creating a PowerManage installation DVD 14
Creating a PowerManage installation USB drive 14
Window system 14
Linux system 15
Installing PowerManage 16
Installing on a HP server 16
Installing on a Dell server 18
Installing on VMware 19
Chapter 3 Post installation administration 33
Completing administration tasks 34

PowerManage console administration tasks 34
Setting the date and time 34
Configuring the network 34
Configure the repository 35
Installing patches 36
Uninstalling patches 36
Backup and restore operations 36
Backing up data to an FTP server 37
Backing up data to an USB drive 37
Restoring data from an FTP server 38
Restoring data from a USB drive 39
Configuring for redundancy 40
Configuring redundancy on a two node system 40
Configuring after a failover event on a two node system 42
Configuring redundancy on a four node system 44
Configuring after a failover event on a four node system 45
Master failover configuration 45
Primary Slave failover configuration 47
SSL certification 48
Creating a certificate request 48
Sending SMS notifications 49
Prerequisites 49
Defining the wake-up modem settings 49
Adding a SMS broker 49
Defining a request 50
Defining a new SMS broker 52
Configuring HAProxy load balancing software 54
Installing HAProxy 54
Installing and configuring CentOS 7 54
Installing HAProxy software 54

About this publication

This publication contains information about the pre-installation requirements at a customer site before and during a Visonic PowerManage V3.10 Professional server installation and configuration.

The installation must be performed by a technical support engineer.

Who should read this guide

This publication must read by the customer before the installation date. You must read the relevant sections in this document and verify to the Visonic point of contact that all the requirements are met before the installation date. A moderate level of server based knowledge and experience is assumed.

This document does not cover in detail all of the installation features.

Notices

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.

© Copyright 2017

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco Security Products. All Rights Reserved.

Trademarks

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Support

EMAIL: info@visonic.com

INTERNET: www.visonic.com

About PowerManage

PowerManage is a web-based host application that can monitor and provision home security and automation services that are provided.

The PowerManage application is built on open standard technologies and an open source Operating System (OS).

Figure 1 shows a typical PowerManage system configuration with the server installed behind a firewall at a service provider's customer site.

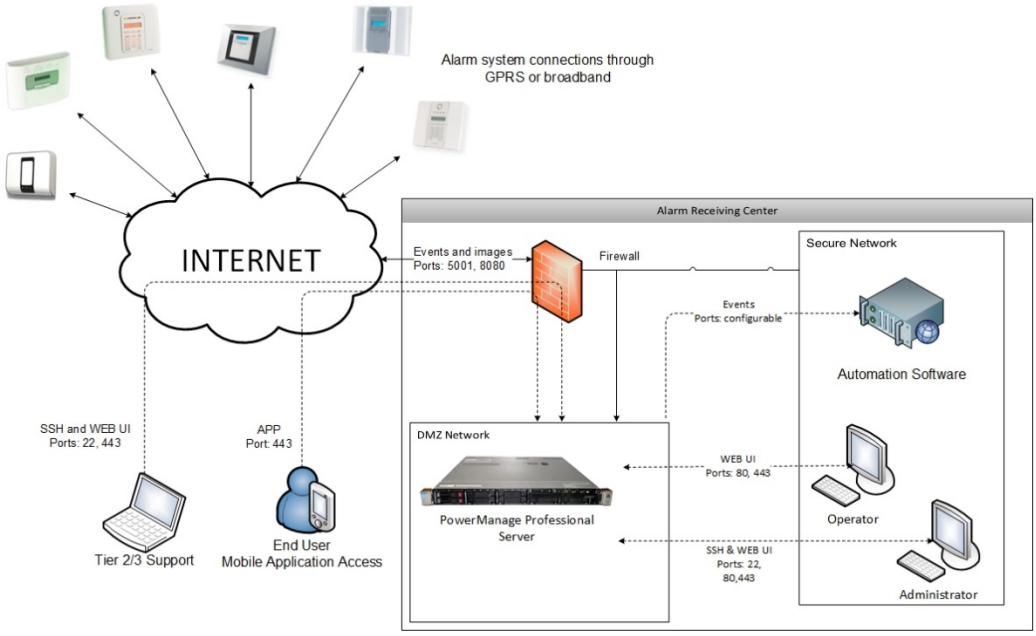


Figure 1: Network topology

A typical network topology might include the following items:

- PowerMaster and PowerMaxPro alarm systems
- Firewall
- PowerManage server
- Automation software such as MASterMind monitoring software

Chapter 1
PowerManage requirements

Hardware requirements

Depending on the installation and the level of performance required you can choose one of the following servers for the installation of the PowerManage web-based host application.

PowerManage V3.10 can be installed on a HPE ProLiant Gen 7 for high to medium performance systems and Dell OptiPlex 3020 and above for low cost systems.

For customers purchasing new platforms we recommend the following hardware configurations.

High performance system

HPE ProLiant DL380 Gen9

Table 1: HPE ProLiant DL380 Gen9 E5-2650v3 2P 32GB-R P440ar 8SFF 2x10Gb 2x800W Perf Server

Component	Description
Form factor	2U rack server
Dimensions (H x W x D)	17.54 in x 28.75 in x 3.44 cm
Processor	Intel® Xeon® E5-2650 v3 (40 core, 2.3 GHz, 25 MB, 105 W)
Memory	64 GB (4 x 16 GB) RDIMM
Storage controller	Dynamic Smart Array B140i and Smart Array P440ar/2GB FBWC
Hard drive	8 SFF Chassis, 440ar/2GB SAS controller
Power supply	(2) 800W Flex Slot Platinum hot plug power supply kit
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL380G9 [752689-B21].

A high performance system solution, supports the following capacity:

- GPRS and Broadband panels, receiver/resolve, with no user or installer applications:
  - 100K panels (50K GPRS panels plus 50K GPRS or broadband panels)
  - GPRS KA 600sec and BB KA 5sec
  - 80 events/second
  - 6 frames/second
  - Daily csv report for all panels, daily pdf report for one panel
  - 4000 RRIs per day
- GPRS and Broadband panels, receiver/resolve, with user or installer applications:
  - 100K panels (50K GPRS panels plus 50K GPRS or broadband panels) with GPRS KA 600sec and BBA KA 5sec
  - 60 events per second
  - 6 frames per second

- 10K simultaneous interactive users with approximately 2700 request per second
- Daily csv report for all panels and daily pdf report for one panel
- 4000 RRIs per day

Medium performance system

HPE ProLiant DL380 Gen9

Table 2: HP ProLiant DL380 Gen9 E5-2620v3 1P 16GB-R P440ar 8SFF 500W PS Base Server hardware specifications

Component	Description
Form factor	2U rack server
Dimensions (H x W x D)	17.54 in x 26.75 in x 3.44 in
Processor x 2	Intel® Xeon® E5-2620 v3 (6 core, 2.4 GHz, 15MB, 85W)
Memory	16GB (1x16 GB) RDIMM
Storage controller	Dynamic Smart Array B140i & Smart Array P440ar/2GB FBWC
Hard drive	8 SFF Chassis, 440ar/2GB SAS controller
Power supply	HPE 500W Flex Slot Platinum Hot Plug Power Supply Kit
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL380G9 [752687-B2]

A medium performance system solution, supports the following capacity:

- GPRS and Broadband panels, receiver/resolve, with no user or installer applications:
  - 40K panels (20K GPRS panels plus 20K GPRS or Broadband panels)
  - GPRS KA 600sec and Broadband KA 5sec
  - 30 events/second
  - 6 frames/second
  - Daily csv report for all panels, daily pdf report for one panel
  - 2000 RRIs per day
- GPRS and Broadband panels, receiver/resolve, with user or installer applications:
  - 25K panels (15K GPRS panels plus 10K GPRS or Broadband panels) with GPRS KA 600sec and Broadband KA 5sec
  - 20 events per second
  - 6 frames per second
  - 5000 simultaneous interactive users with approximately 800 request per second
  - Daily csv report for all panels and daily pdf report for one panel
  - 2000 RRIs per day

Low cost systems

Dell OptiPlex 3050

Table 3: Dell OptiPlex 3050 - Core i5 7500 3.4 GHz - 16 GB hardware specifications

Component	Description
Dimensions (H x W x D)	15.4 cm x 27.4 cm x 35 cm
Processor	Intel® Core i5-7500 (QC, 6 MB, 4 T, 3.4 GHz, 65 W)
Memory	32 GB (maximum) - DDR4-SDRAM
Hard drive	1 x 500 GB - SATA

Dell OptiPlex 3040

Table 4: Dell OptiPlex 3040 - Core i5 6500 3.2 GHz - 16 GB hardware specifications

Component	Description
Dimensions (H x W x D)	15.4 cm x 27.4 cm x 35 cm
Processor	1 x Intel® Core i5 (6th Gen) 6500 / 3.2 GHz (3.6 GHz) (Quad-Core)
Memory	16 GB (maximum) – DDR3L-SDRAM - non-ECC
Hard drive	1 x 500 GB - SATA

Table 5: Dell OptiPlex 3040 - Core i5 4570 3.2 GHz - 8 GB hardware specifications

Component	Description
Dimensions (H x W x D)	15.4 cm x 27.4 cm x 35 cm
Processor	1 x Intel® Core i5 (6th Gen) 4750 / 3.2 GHz (3.6 GHz) (Quad-Core)
Memory	8 GB – DDR3L-SDRAM - non-ECC
Hard drive	1 x 500 GB - SATA

A low cost system solution, supports the following capacity:

- 10K GPRS panels with a KA of 600 seconds and 500 Broadband panels with a KA of 5 seconds
- 5 events/second
- 1 frame/second
- 500 interactive users with approximately 130 requests per second

Virtual environment hardware requirements

The following table describes the minimum hardware requirements to install PowerManage on a VMware vSphere client.

Table 6: vSphere client hardware specifications

Component	Description
CPU	1 CPU
Processor	Intel® Xeon® E5-2650 v3 (40 core, 2.3 GHz, 25 MB, 105 W)
Memory	4 GB RAM
Hard drive	1 x 500 GB SATA

Legacy hardware requirements

The following tables describes the legacy hardware system that are supported.

Table 7: HP ProLiant DL360p G8 Server [670634-S01]

Component	Description
Form factor	1U rack server
Dimensions (H x W x D)	4.32 cm x 42.62 cm x 69.22 cm
Processor x 2	Intel® Xeon® E5-2640 (6 core, 2.5 GHz, 15 MB, 95 W)
Memory	16GB (2 x 8 GB DDR3-1333MHz Low Voltage RDIMMs)
Storage controller	Smart Array P420i and 1GB FBWC (RAID 0/1/1+0/5/5+0)
Hard drive	HP 2 x 600 GB SAS 10k 2,5” SFF
Power supply	(2) HP 460W CS Platinum plus Hot Plug Redundant Power Supply
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL360G8.

Table 8: HP ProLiant DL360p G8 High Performance Server [646904-001]

Component	Description
Form factor	1U rack server
Dimensions (H x W x D)	4.32 cm x 42.62 cm x 69.22 cm
Processor x 2	Intel® Xeon® E5-2650 (8 core, 2 GHz, 20 MB, 95 W)
Memory	32 GB (4 x 8 GB) Registered DIMMs PC3-12800R (1600MHz)
Storage controller	Smart Array P420i and 1GB FBWC (RAID 0/1/1+0/5/5+0/6/6+0)
Hard drive	HP 2 x 600 GB SAS 10k 2,5” SFF
Power supply	(2) HP 750W CS Platinum, plus Hot Plug Redundant Power Supply
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL360G8.

HAProxy hardware requirements

The following tables describe the hardware requirements for a proxy server if required for load balancing and high availability.

High performance server

Table 9: HP ProLiant DL360p G9 Server [670634-S01]

COMPONENT	DESCRIPTION
Form factor	1U rack server
Dimensions (H x W x D)	4.32 cm x 42.62 cm x 69.22 cm
Processor x 2	Intel® Xeon® E5-2640 v3 (6 core, 2.5 GHz, 15 MB, 85 W)
Memory	32 GB (4 x 8 GB) Registered DIMMs PC3-12800R (1600MHz)
Storage controller	Smart Array P420i and 1GB FBWC (RAID 0/1/1+0/5/5+0)
Hard drive	8 SFF Chassis, 440ar/2GB SAS controller
Power supply	(2) HP 460W CS Platinum plus Hot Plug Redundant Power Supply
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL360G9.

Medium performance server

Table 10: HP ProLiant DL360p G8 Server [670634-S01]

Component	Description
Form factor	1U rack server
Dimensions (H x W x D)	4.32 cm x 42.62 cm x 69.22 cm
Processor x 2	Intel® Xeon® E5-2640 (6 core, 2.5 GHz, 15 MB, 95 W)
Memory	16GB (1 x 16 GB) RDIMM
Storage controller	Smart Array P420i and 1GB FBWC (RAID 0/1/1+0/5/5+0)
Hard drive	HP 2 x 600 GB SAS 10k 2,5” SFF
Power supply	(2) HP 460W CS Platinum plus Hot Plug Redundant Power Supply
iLO	Advanced

For details about the HP ProLiant see the Hewlett Packard Enterprise web site, DL360G8.

Rack and power outlet requirements

You must ensure that the following rack and power requirements are met:

- Sufficient room in your designated server rack for a 1U sized server.
- One free power outlet must be present.
  A second power outlet is recommended as the server has two redundant power supplies. More outlets may be required depending on the server configuration, see the remaining document for details.

Network and firewall requirements

You must connect the PowerManage server behind a firewall or Network address translation (NAT) device and use a restrictive access policy.

Port number and IP address settings

You must configure the following network and firewall settings:

- Network settings:
  - Allocate one fixed static IP address.
  - A DNS host name is required for the allocated IP address. You must have an A and PTR record for this address.
  - A symmetric downlink an uplink connection of 10 to 100 Mbit is required at all times. This speed can vary with the system load.
  - The outbound server must have access to the Internet and cannot be blocked.
- Firewall settings:
  - Must support concurrent connections, the number of connetions is based on connections/second = N/2, where N is the number of panels enrolled on the server.
  - Bandwidth for medium performace system must not be less than 10 Mbit /second both for incoming and outgoing traffic For high performance must not be less than 100 Mbit/ seconds.

Table 11 describes the required inbound communication ports that must be open on the internal firewall.

Table 11: Inbound port numbers and protocols used by PowerManage

Port	Protocol	Description
Panel connections		
5001	TCP/UDP	Alarm signals and resolve
8080	TCP/UDP	Alarm images
8443	TCP/UDP	Alarm images secured
5555	TCP/UDP	Offline handler [For GEO redundancy architecture only]
Web interface		
80	HTTP	Resolve web interface
443	HTTPS	Resolve web interface using encrypted SSL
REST API		
443	HTTPS	REST API requests with encrypted SSL
3333	HTTP	REST API requests that are not encrypted if using a HAProxy server
VDCP API		
4444 (configurable)	V-DCP	Script access
Support		

Port	Protocol	Description
22	TCP	SSH only for 91.207.90.0/23
161	SNMP	Nagios or other monitoring platforms
162	SNMP	Nagios or other monitoring 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	SMTP	Email or email relay
587	SMTP	Email or email relay

Network diagrams

The following network diagrams are examples of PowerManage configuration solutions that can be deployed.

The HAProxy server is optional in all configurations. If no HAProxy server is present, you can redirect all SSL traffic https://app_dns from the firewall to the Power Manage server and remove HAProxy server from the schema.

Standalone configuration

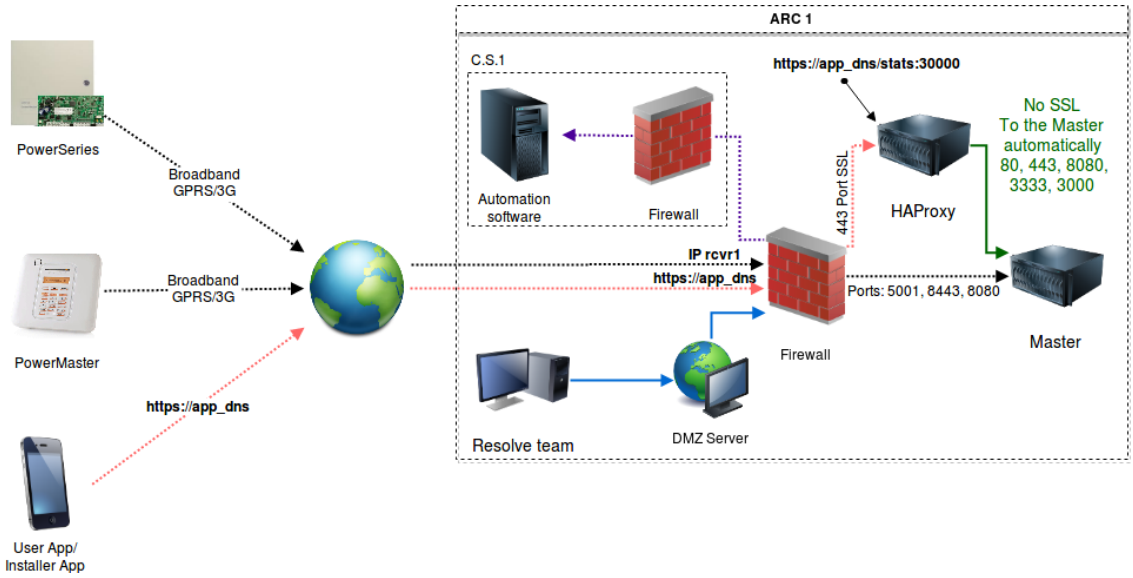


Figure -1 PowerManage standalone configuration

Two node multisite configuration

In a two node configuration the PowerManage server installed at the primary site is replicated on a second PowerManage server installed at a secondary site.

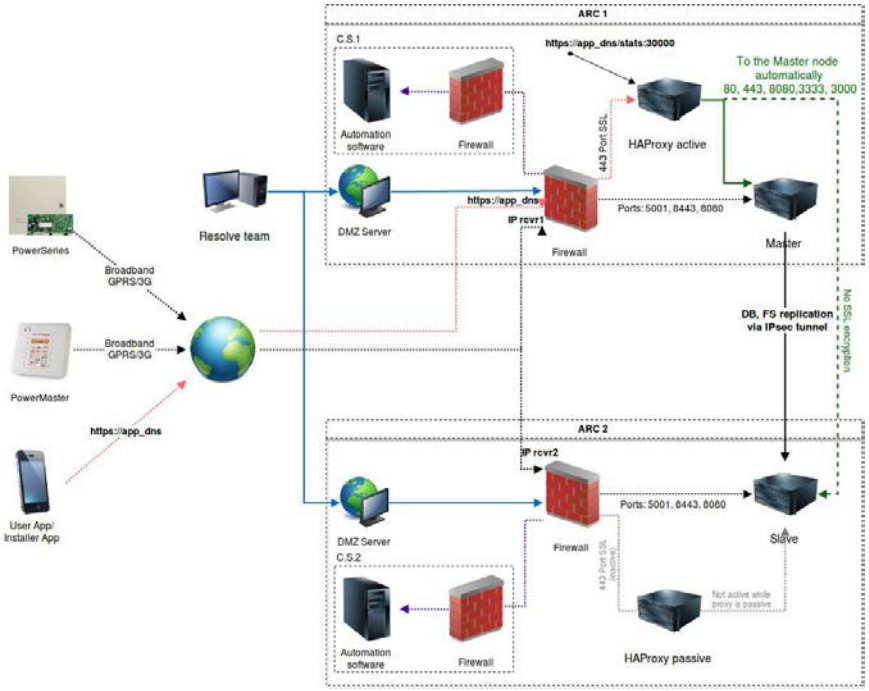


Figure -2 PowerManage two node multisite configuration

Four node multisite configuration

In a four node configuration PowerManage is installed at the primary site and at the secondary site a primary slave manager is configured.

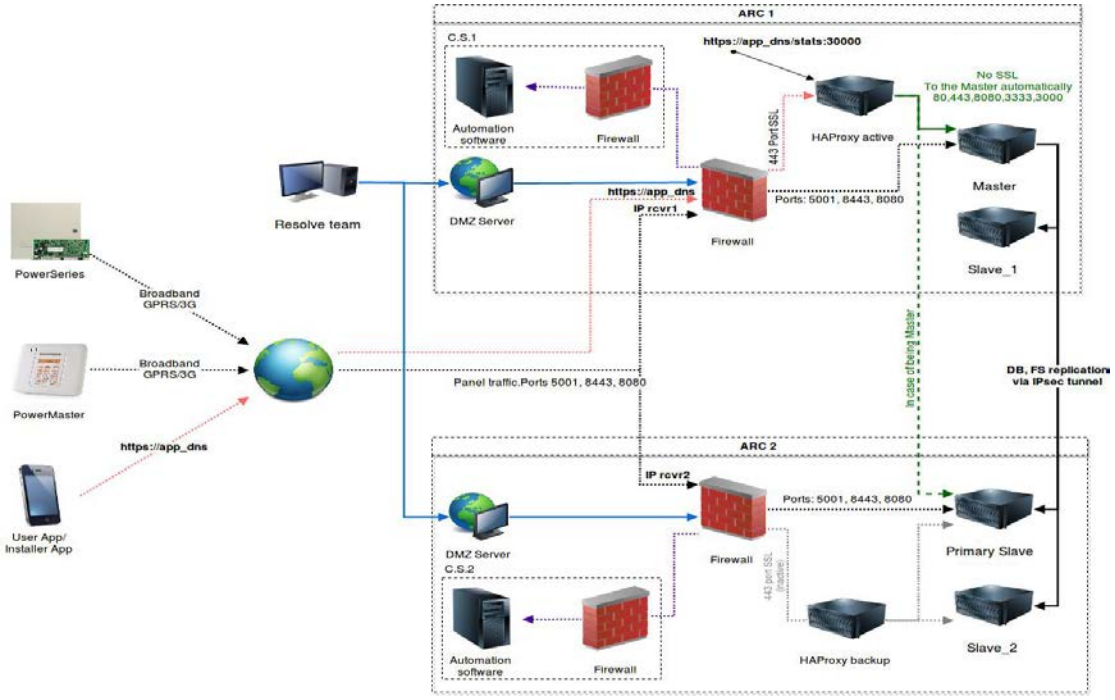


Figure -3 PowerManage four node multisite configuration

Software requirements

HPE Integrated Lights Out (iLO)

The HPE iLO software allows you to manage and monitor servers from a remote machine. The enhanced access and server control provides easier server administration. For further information HPE iLO, see the Hewlett Packard Enterprise website at:

http://h18013.www1.hp.com/products/servers/management/remotemgmt.html?jumpid=servers/lights-out

The iLo interface uses a separate Ethernet port and requires a separate IP address.

Client requirements

The iLo client is 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 2GHz.
- Memory: 4GB RAM.
- Networking: 1Gbit Ethernet connectivity.

Suggested minimum software requirements:

- Operating system:
  - Windows 10, Windows 7, Windows Vista, and Windows XP.
  - Red Hat Linux, Ubuntu Linux, and Fedora.
  - Mac OS
- Browsers:
  - Google Chrome 22+
  - Firefox 6+
  - Safari S5+
  - Internet Explorer 9+ (limited support)
- SSH agent:
  - PuTTy
  - OpenSSH agent
  - SSH agent for Mac

Chapter 2
PowerManage installation

Planning to install PowerManage

Prepare the installation media by creating a PowerManage DVD or USB flash drive.

Prerequisites

A local network engineer or administrator must be available at the time of the installation and ensure that the following equipment is on site:

- USB keyboard
- Console or monitor
- Security panels for testing
- Mobile device for testing

Preparing the media

The PowerManage applicaton is installed from an ISO image file. The file size exceeds 4 GB, you can store the image file on one of the following media types:

- Double layer DVD
- USB flash drive

Creating a PowerManage installation DVD

Use any disk burning software that is capable of burning a disc using an image file. The process is the same for Windows or Linux operating systems.

To burn a disc using an image file, complete the following steps:

1. Place a blank, writeable double layered DVD disc into your computers DVD drive.
2. Start the disc burning program and select the option to burn a DVD from an image file.
3. Browse and select the PowerManage ISO image file.
4. Click **Burn disc image**.

Creating a PowerManage installation USB drive

Several utilities are available for Windows and Linux to create a USB drive.

Window system

To create a PowerManage bootable installation USB drive using the Rufus utility, complete the following steps:

1. Start the Rufus utility and from the **Device** list, select the USB drive.
2. In the **New volume label** field, enter the name for the PowerManage USB drive.

3. In the **Format Options** area, select **Create a bootable disk using: ISO image** and then click the CD-ROM icon and select the PowerManage ISO image file.
4. Click **Start** a confirmation message is displayed, click **Write in DD Image mode**.

Linux system

To create a PowerManage bootable installation USB drive use the Linux **dd** command. The **dd** command 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 are in the directory /dev/.

To write an image file to a bootable media, complete the following steps:

1. Insert the USB media.
2. Format the USB drive.
3. Open a new terminal window, as sudo user and type the following command to find the USB device:

   ```
   fdisk -l
   ```

4. Go to the directory where the PowerManage ISO image is stored and type the following command

   ```
   dd bs=1M if=<image.iso> of=/dev/<device>
   ```

   where <image.iso> is the name of the PowerManage ISO image and <device> is the name of the current device file for the media.

Installing PowerManage

Install the PowerManage application on a server or virtual machine. Depending on the server type the installation process varies.

Installing on a HP server

Complete the following steps to install the PowerManage application on a HP server.

1. Power on the server and insert the PowerManage DVD into the DVD drive or insert the USB drive.
2. Power off and on the server.
3. When the startup screen appears, press **F11** to go to the **Boot Menu**.
4. Select **Legacy BIOS One-Time Boot Menu** and press enter.
5. When the boot menu confirmation message to enter the **Legacy BIOS One Time Boot Menu** appears, press enter.

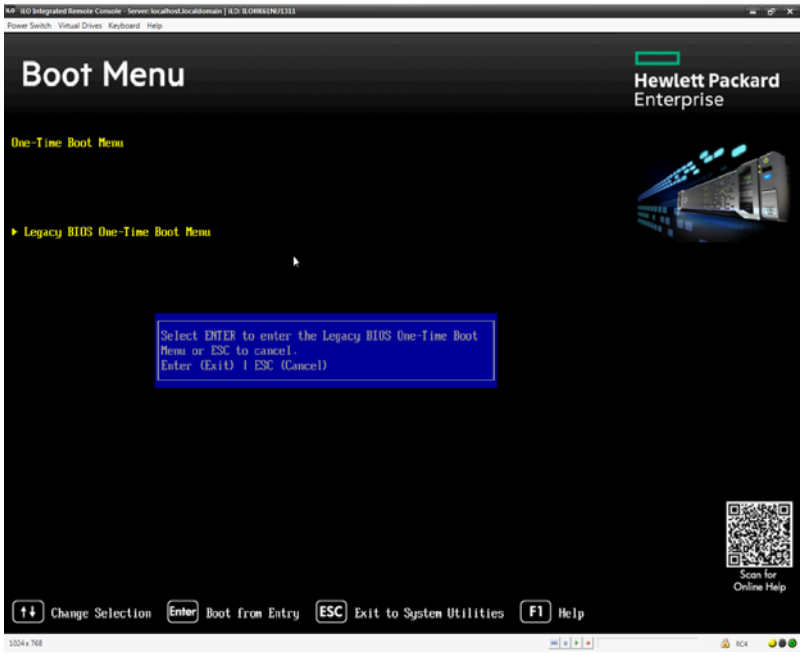


Figure -1 Legacy BIOS One-Time Boot Menu

6. Depending on the installation media, select one of the following options:
    - One Time Boot to CD-ROM (DVD Media installation)
    - One Time Boot to USB DriveKey (USB Media installation)

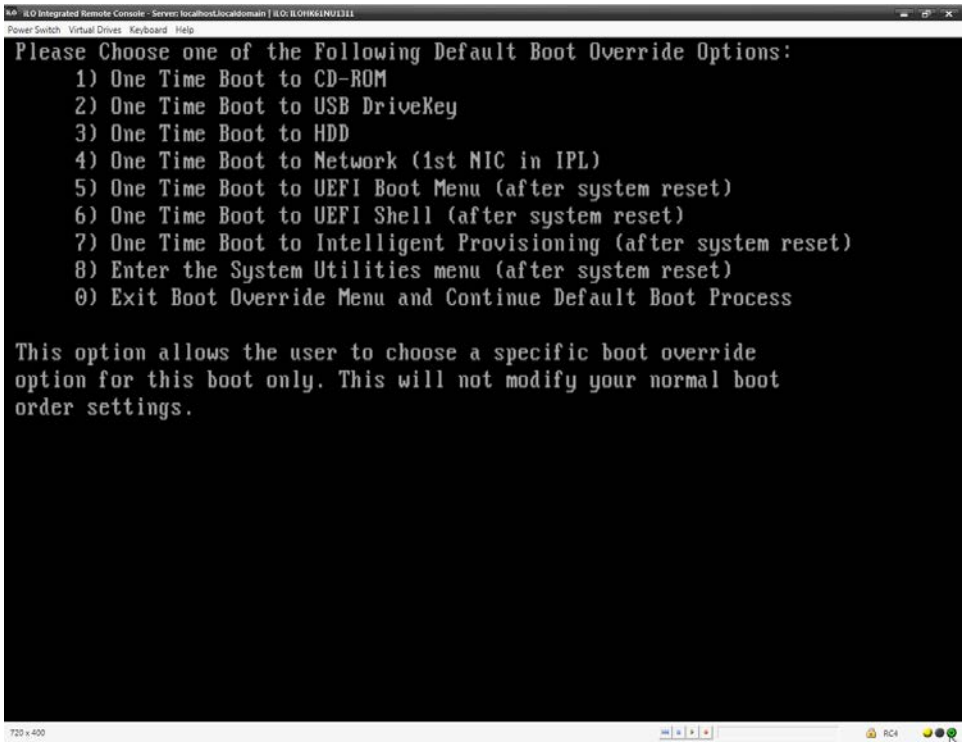


Figure -2 Boot override options

7. Wait until the installation starts, when the **Tyco – PowerManage III Master Disk** boot prompt appears, type one of the following boot options:

   - `usb` (USB Media installation)
   - `cdrom` (DVD Media installation)

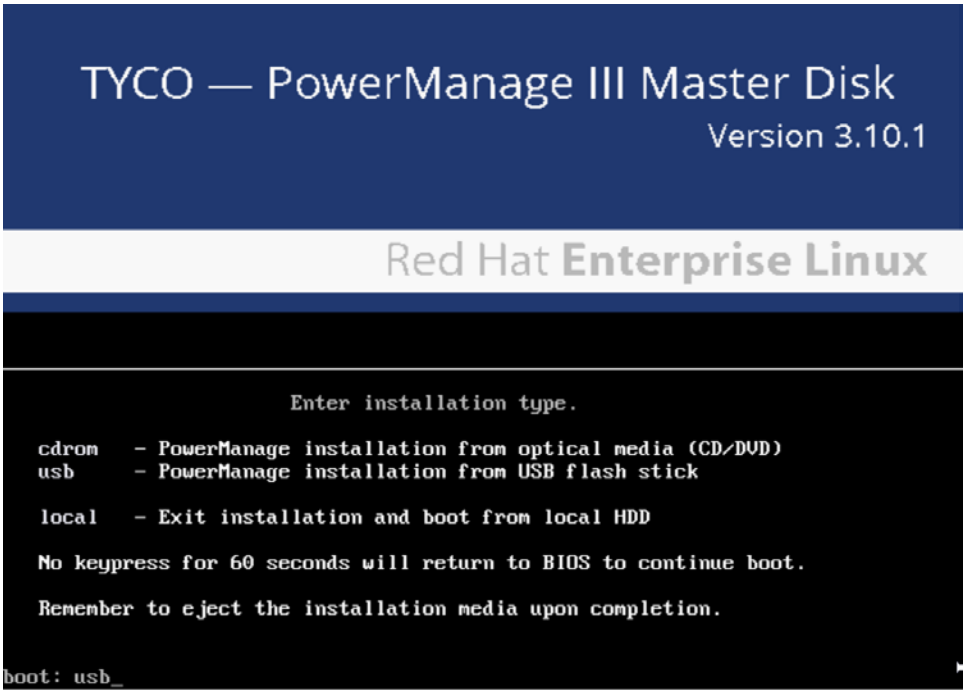


Figure -3 PowerManage boot media options

8. Wait until the installation is complete and the server restarts.

Note: Remove the DVD or the USB after the reboot process.

9. At the l**ocalhost login:** prompt,
    - Enter the user ID: **`root`**
    - Enter the password: **`visonic`**
10. At the **New password:** prompt, enter the new root password twice.

Note: It is recommended not to use the default password.

Result: The PowerManage Man Machine Interface (MMI) appears.

Installing on a Dell server

The PowerManage installation from a DVD is exactly the same as described for the HP server. To install from a USB drive, two identical USB drivers with the same PowerManage images are required.

Complete the following steps to install the PowerManage application on a Dell server.

1. Power on the server, insert the PowerManage DVD into the DVD drive or insert two USB drives.
2. Reboot the server.
3. When the startup screen appears, press **F12** to go to the **One-Time Boot Menu**.
4. From the **One-Time Boot Menu** depending on the media type select one of the following options:
    - One Time Boot to CD-ROM (DVD Media installation)
    - One Time Boot to USB DriveKey (USB Media installation)
5. See Installing on a HP server and complete steps 7 to 10.

Installing on VMware

Complete the following steps to install the PowerManage application on a VMware virtual machine:

1. Log on to VMware vSphere client.

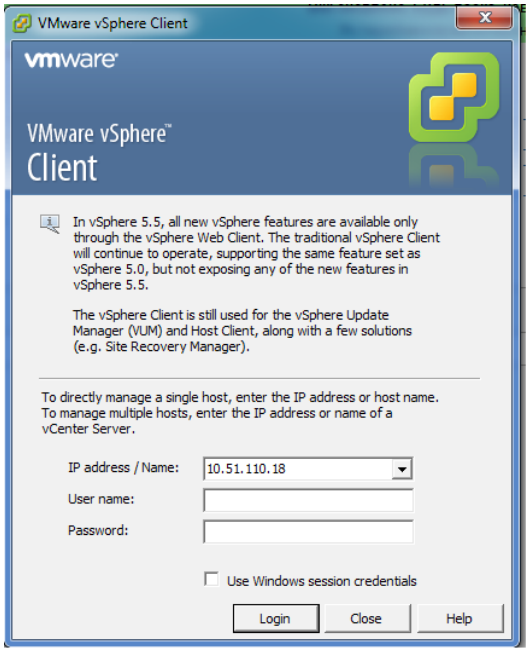


Figure -4 VMware vSphere Client

2. Select the host virtual machine.

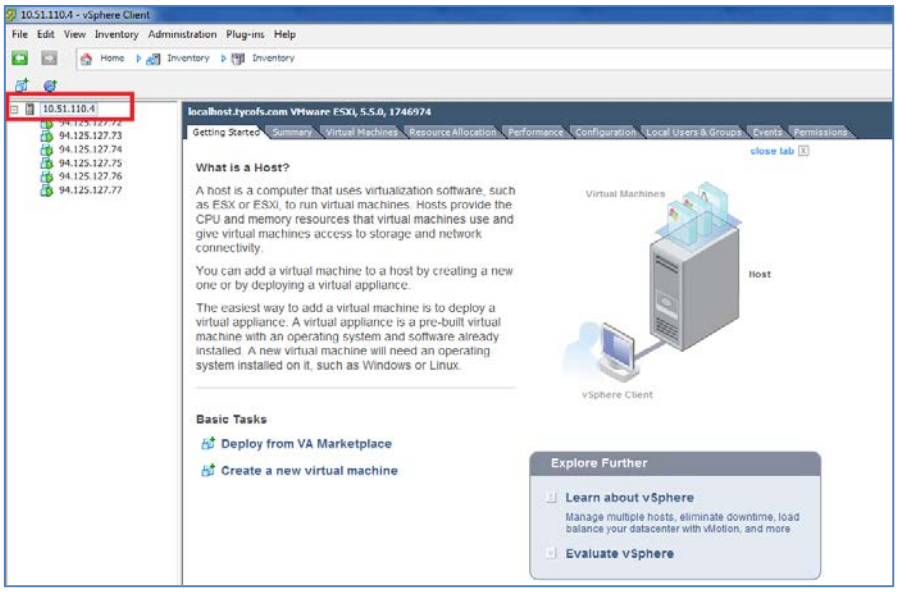


Figure -5 Host selection

3. To add a new adapter complete the following steps:

- Click the **Configuration** tab (action 1).
- In the Hardware pane, select **Networking** (action 2)
- Click **Add Networking** (action 3)

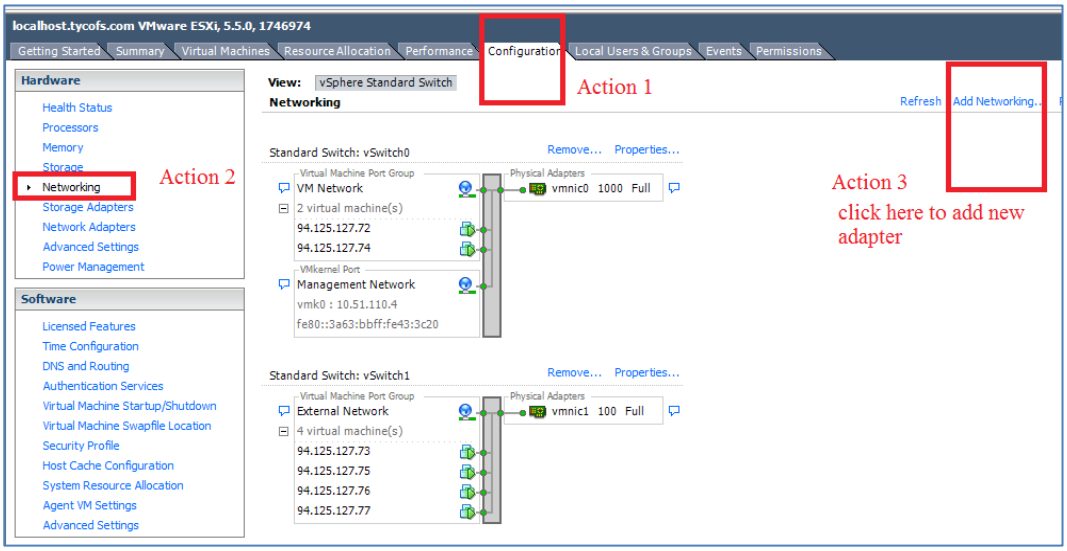


Figure -6 Configuration window

4. On the Connection Type page, click **Virtual Machine** and then click **Next.**

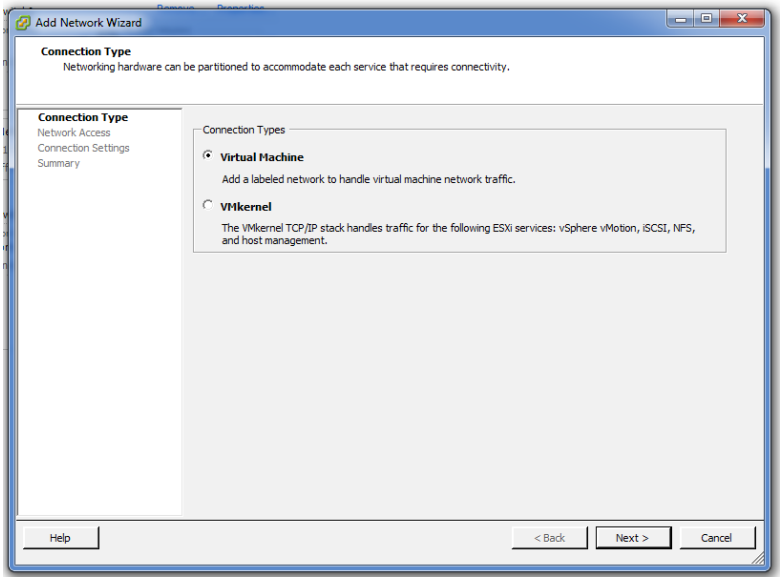


Figure -7 Add Network Wizard – Connection Type page

5. On the Virtual Machines – Network Access page, select the required Ethernet adapter and then click **Next**.

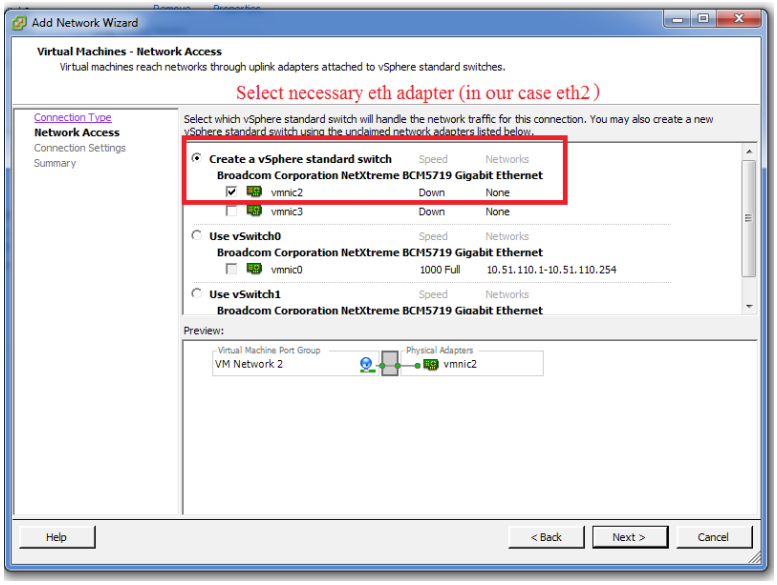


Figure -8 Network Access page

6. On the Virtual Machines – Connection Settings page, in the **Network Label** field enter the name of the adapter and then click **Next**.

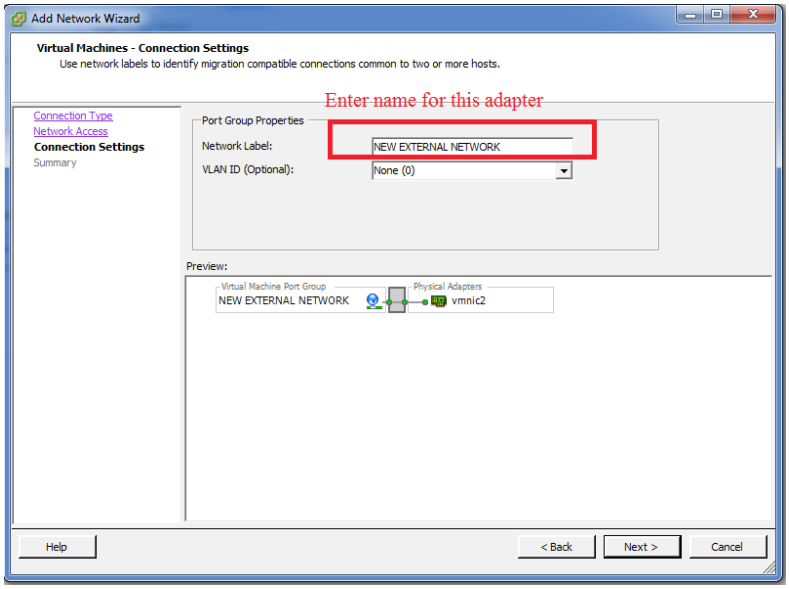


Figure -9 Connection Settings page

7. On the Summary page, review the settings and click **Finish**.

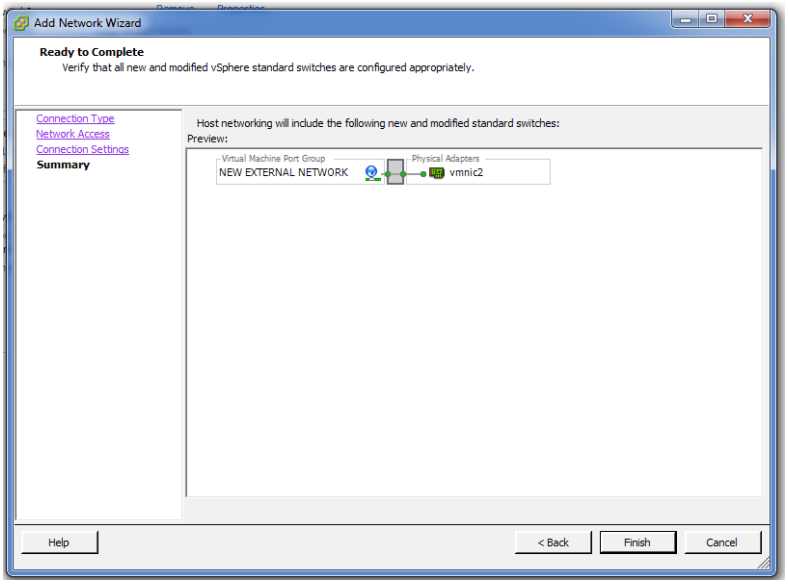


Figure -10 Summary page

8. To upload the PowerManage image file to the VM datastore complete the following steps:

   - Select the host virtual machine (action 1).
   - Click the **Configuration** tab (action 2).
   - In the Hardware pane, select **Storage** (action 3).

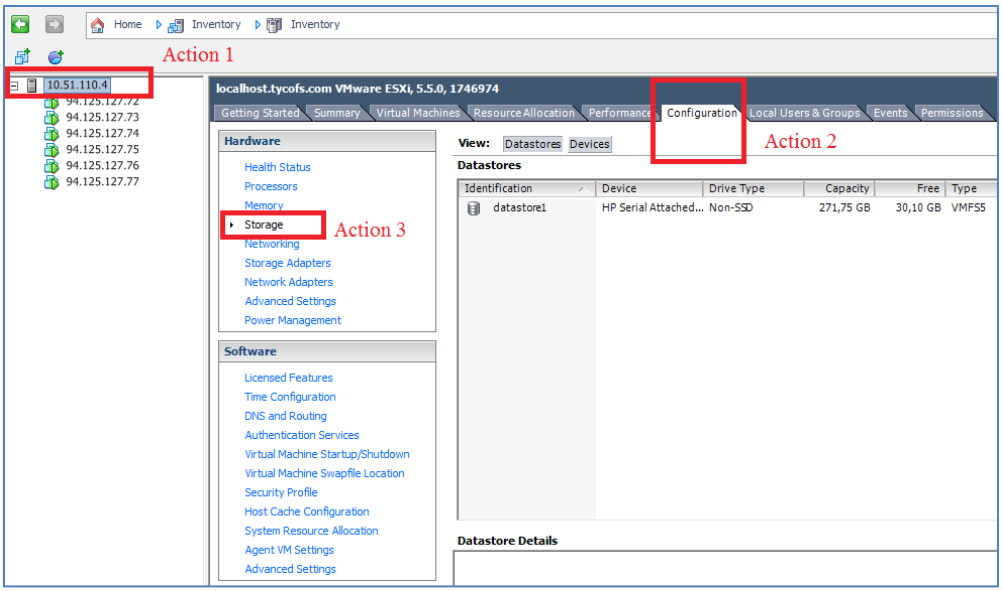


Figure -11 Configuration window

9. In the Datastores pane, right-click the datastore and select **Browse Datastore…**

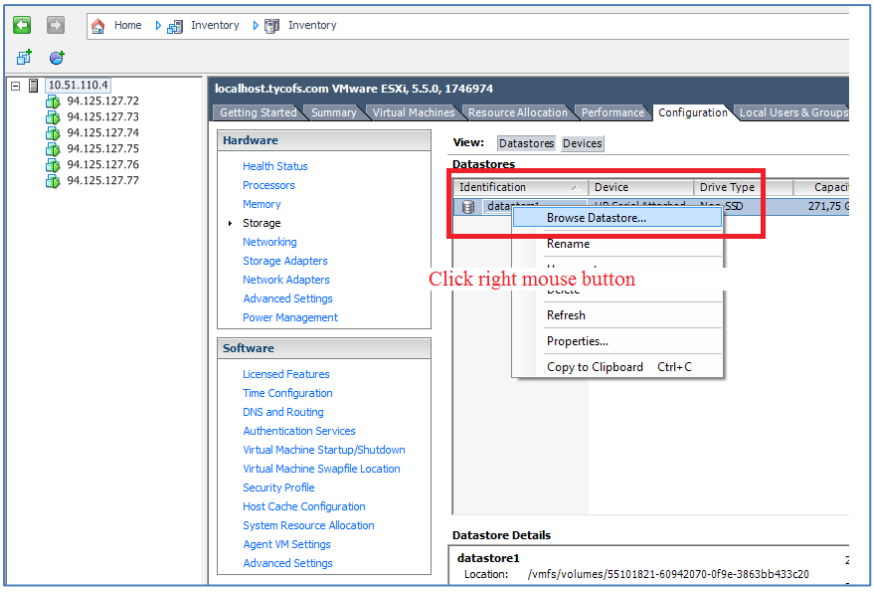


Figure -12 Datastores pane

10. Click the **Upload files to this storage** icon, select **Upload File...** and then select the file to add from the workstation.

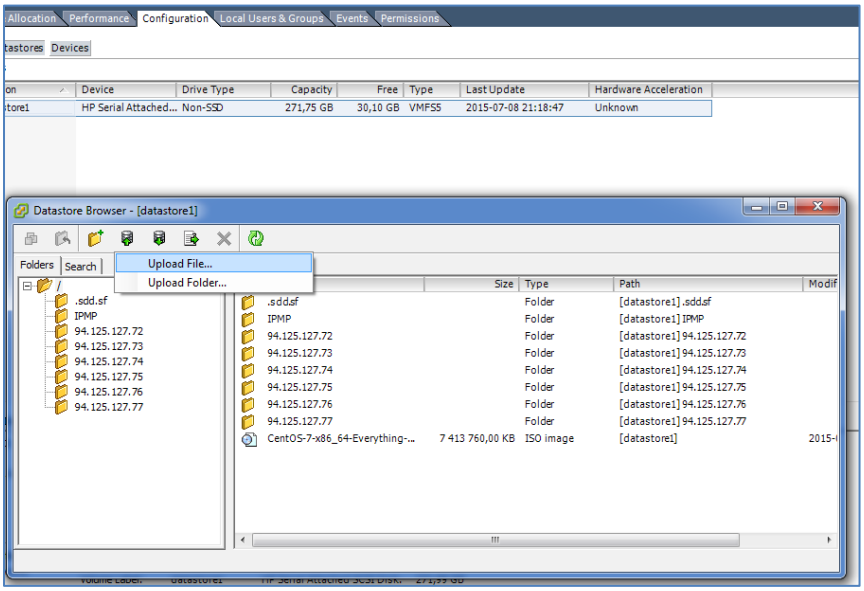


Figure -13 Datastore Browser window

11. Right-click the host virtual machine name, and then click **New Virtual Machine…** on the shortcut menu.

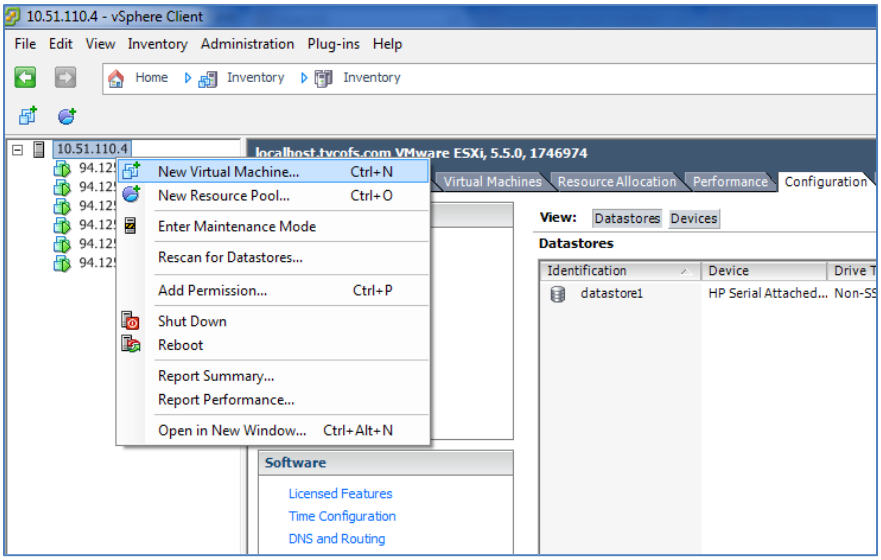


Figure -14 Adding a Virtual Machine

12. On the Configuration page, click **Typical** and then click **Next.**

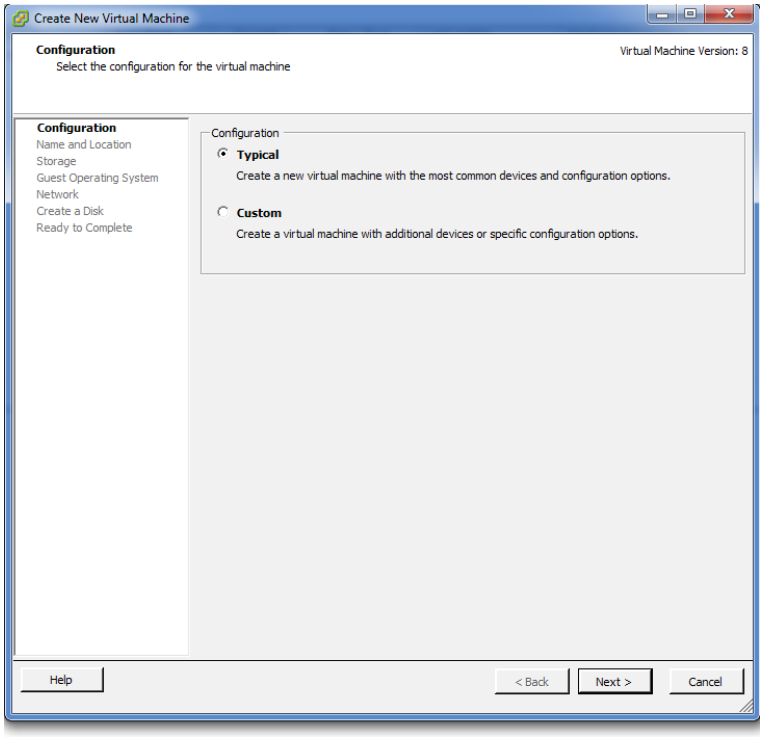


Figure -15 Configuration page

13. On the Name and Location page, in the **Name** field enter the virtual machine name and then click **Next**.

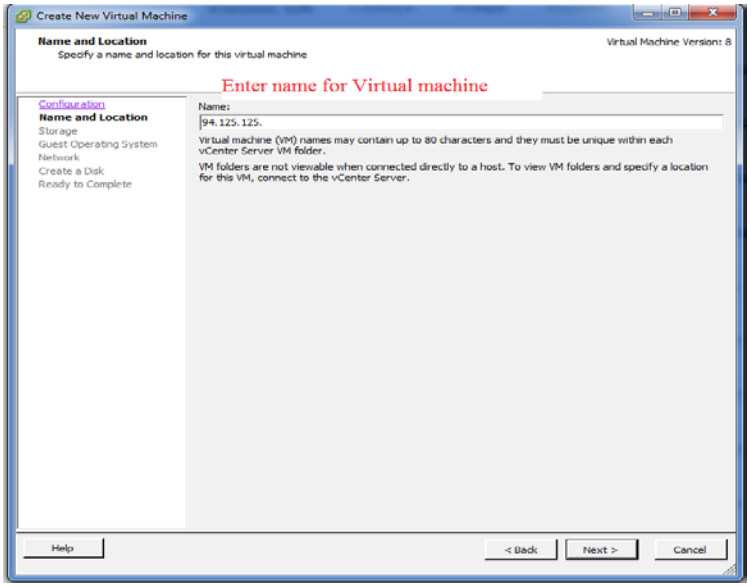


Figure -16 Name and Location page

14. On the Storage page, select a destination storage for the new virtual machines files and then click **Next**.

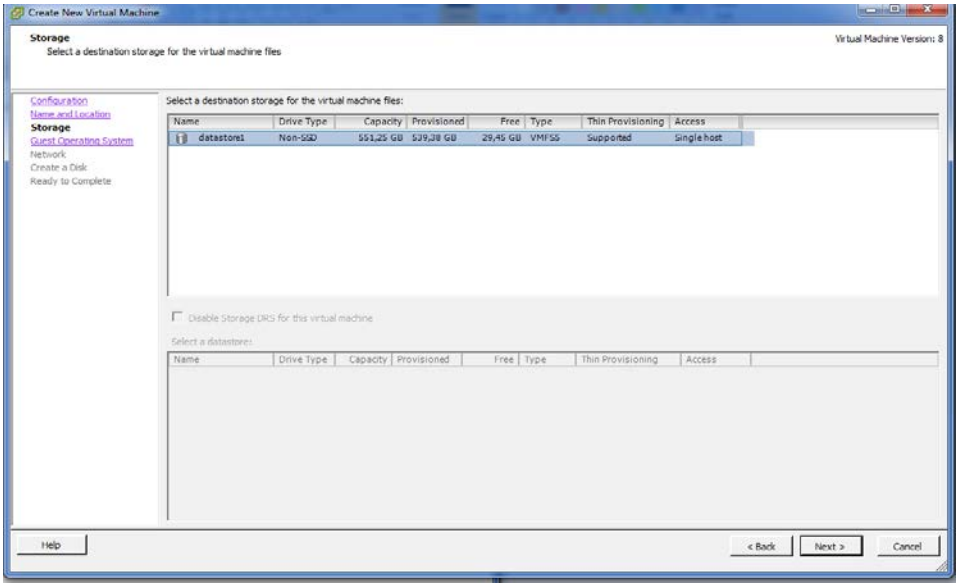


Figure -17 Storage page

15. On the Guest Operating System page:

- Click **Linux**.
- In the Version list, select **Red Hat Enterprise Linux 6 (64-bit)** and then click **Next**.

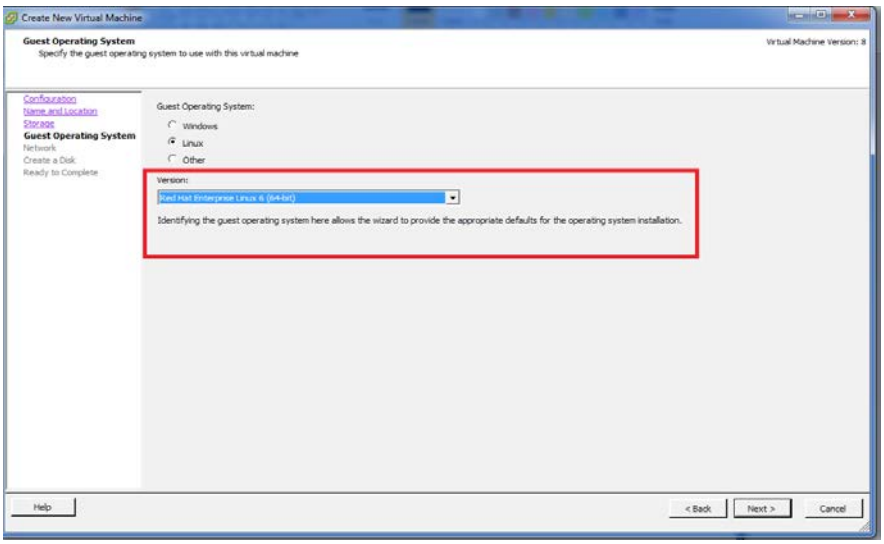


Figure -18 Guest Operating System page

16. On the Network page, select the network and adapter that you have configured:

- From the Network list, select the network connection name.
- From the Adapter list, select the adapter name and then click **Next**.

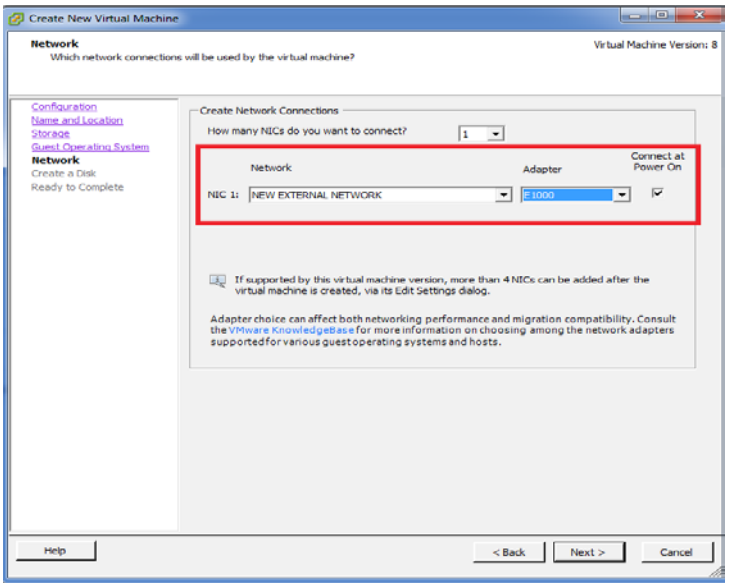


Figure -19 Network page

17. On the Create a Disk page:

- In the Virtual disk size box, select the disk size and measurement type that you want to use.

  Note: This value cannot be less than 120 GB.
- Click Thick Provision Lazy Zeroed and then click Next.

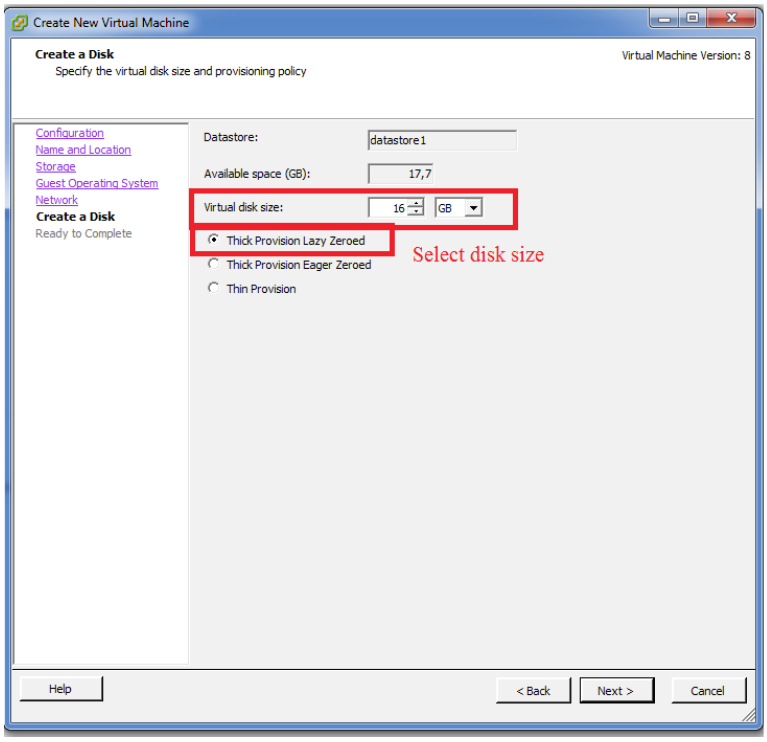


Figure -20 Create a Disk page

18. On the Ready to Complete page, review the settings and click **Finish.**

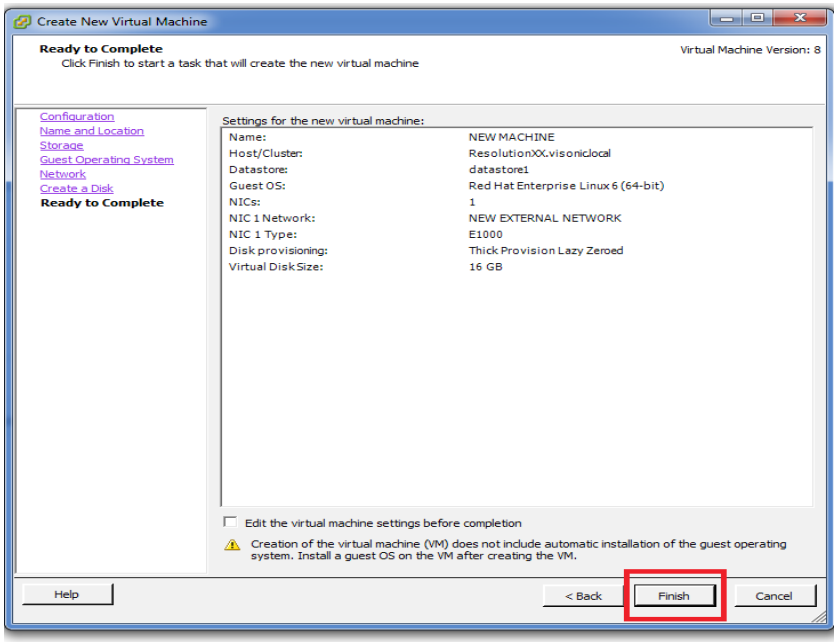


Figure -21 Ready to Complete page

19. Right-click the new virtual machine name, and then click **Edit Settings…** on the shortcut menu.

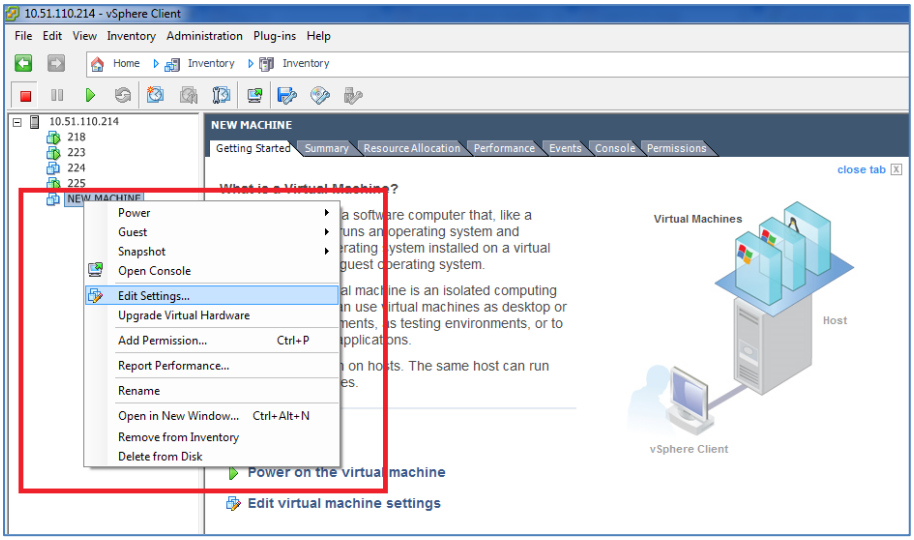


Figure -22 Virtual machine configuration

20. Ensure that the Hardware tab is selected and complete the remaining steps.
21. On the hardware list, click **Memory.** In the Memory Configuration pane, select the size and measurement of the memory size.

Note: A minimum of 4 GB is required.

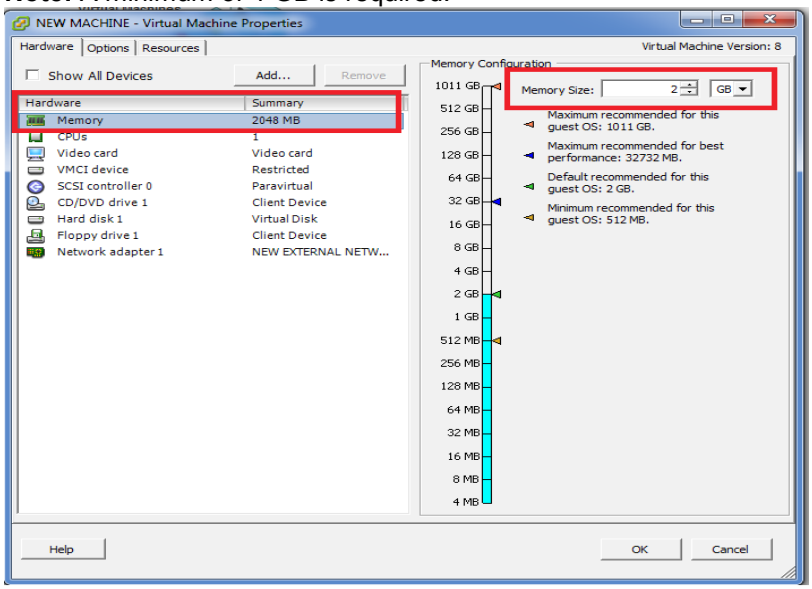


Figure -23 Virtual machine memory configuration

22. On the hardware list, click **CPUs** and select the number of CPUs at least one or more is required.

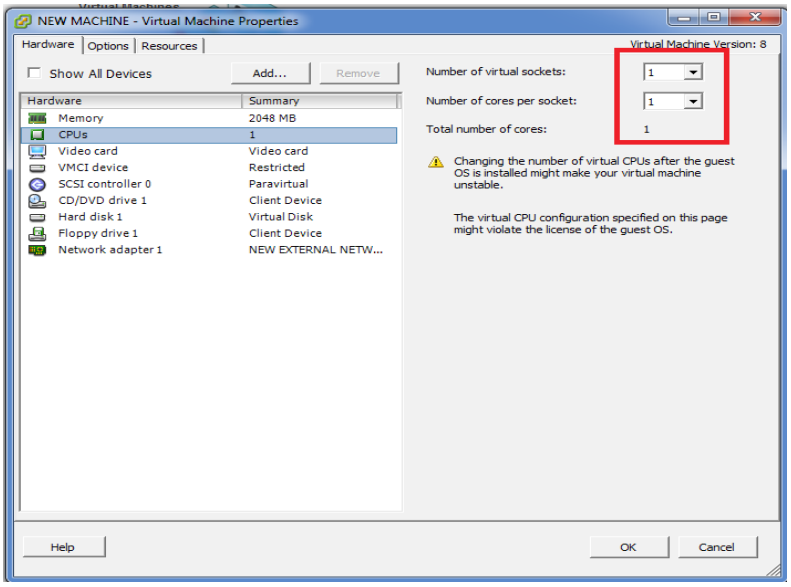


Figure -24 Virtual machine CPU configuration

23. On the hardware list, click **SDSI controller 0**, click **Change Type…**.

    Then from the **SCSI Controller Type** list, click **LSI Logic Parallel**.

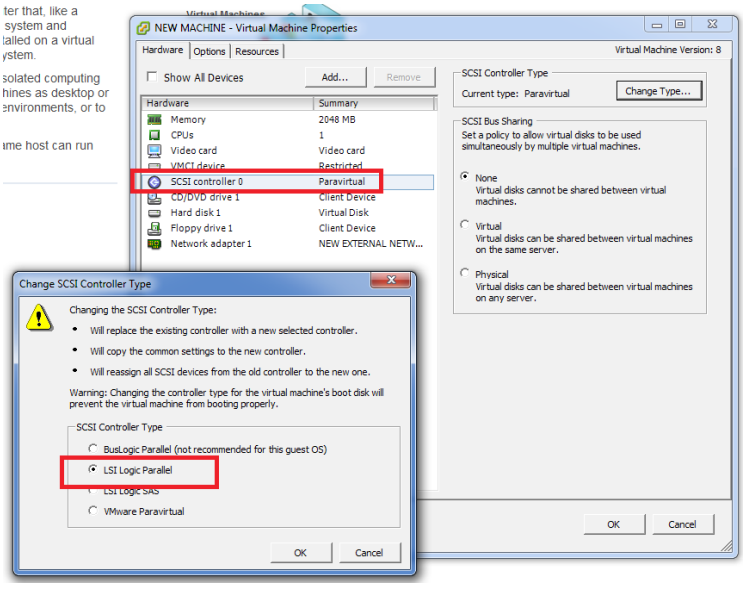


Figure -25 Virtual machine SCSI Controller configuration

24. On the hardware list, click **Network adapter 1**, then from the **Network Connection** list, select the name of the new network connection.

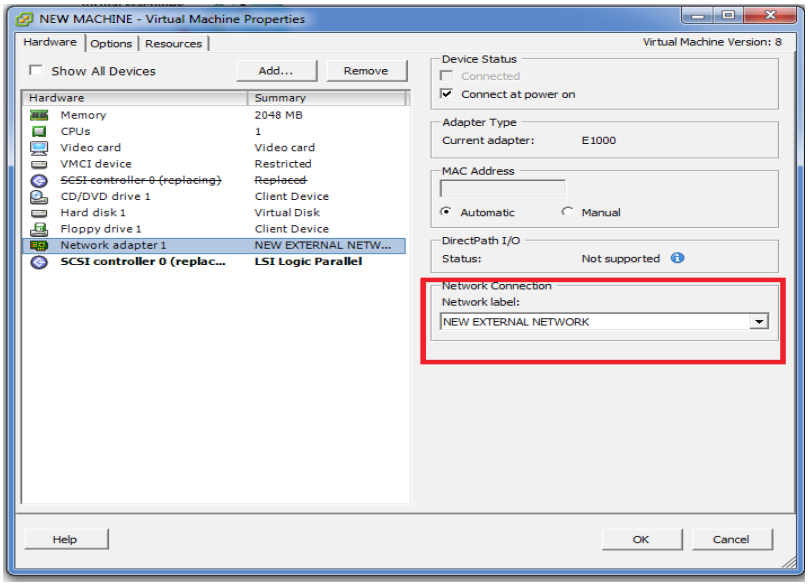


Figure -26 Virtual machine Network adapter configuration

25. On the hardware list, click **CD/DVD drive 1**:

- In the Device Status area, click **Connect at power on**.
- In the Device Type area, click **Datastore ISO File** and then click **Browse**.
  Go to the datastore where the PowerManage ISO file is located and select the image.

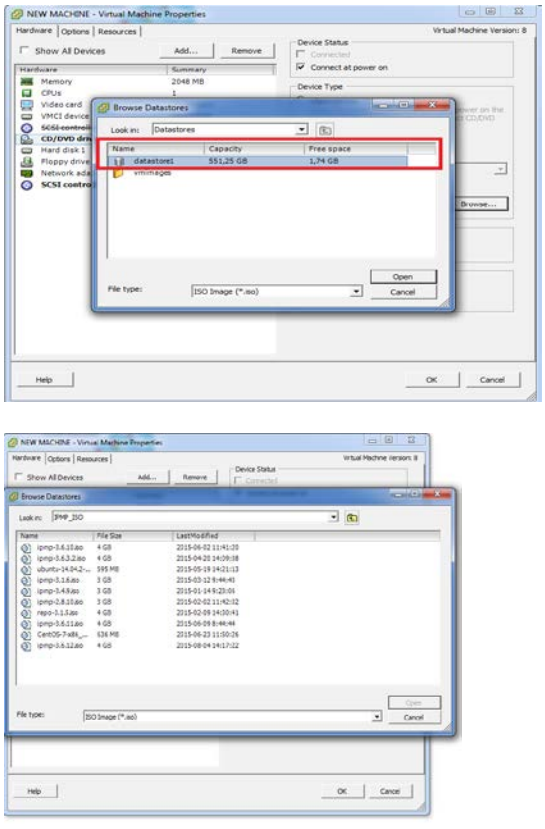


Figure -27 ISO file selection from the datastore

26. Open the virtual machine and connect to the ISO image on the datastore.

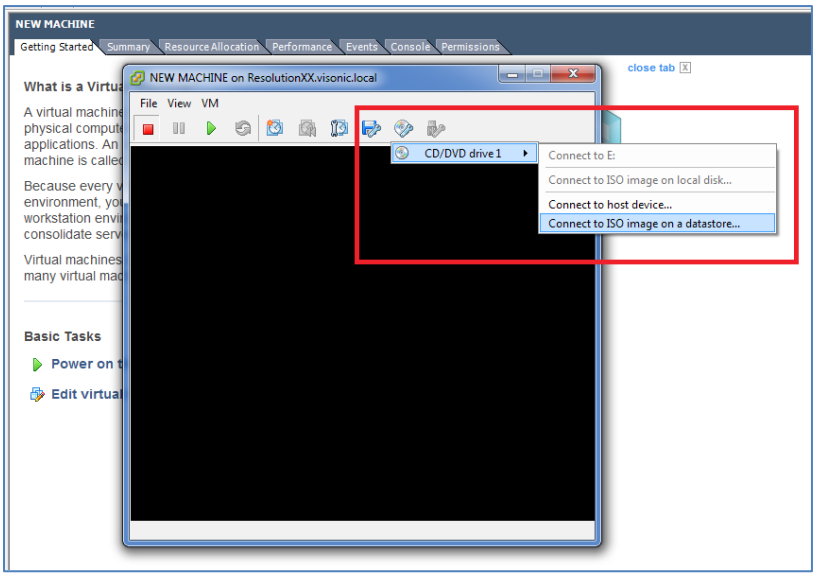
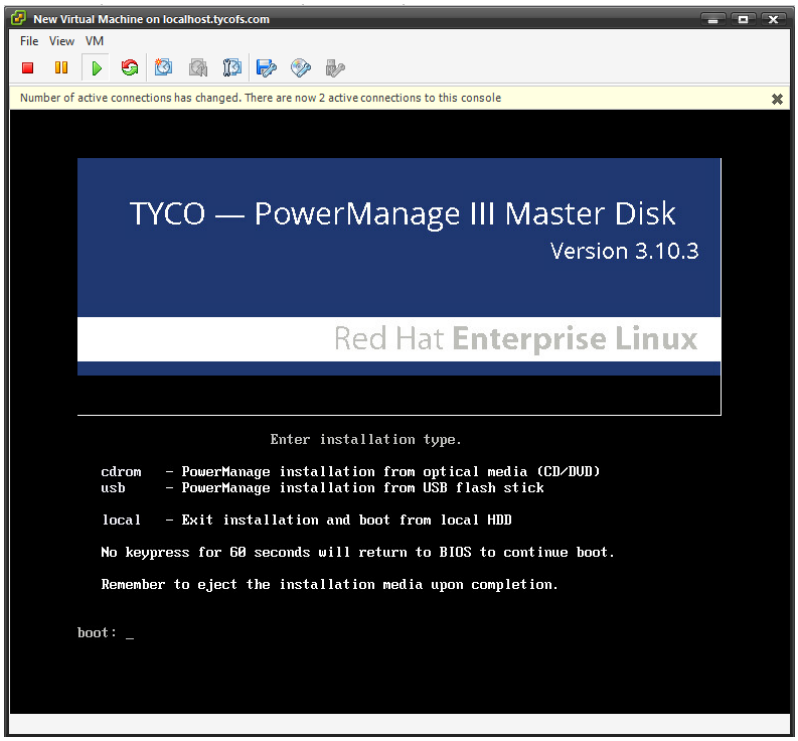


Figure -28 ISO file connection on the datastore

27. Start the virtual machine and type **cdrom** at the boot prompt to install the PowerManage application.



Chapter 3
Post installation administration

Completing administration tasks

After the PowerManage application is installed on the server it is ready for use. However, other administrative tasks not covered during the installation can be necessary depending on your system configuration.

PowerManage console administration tasks

Tasks such as time synchronization, network and repository configuration are performed from the PowerManage console referred to as the MMI console. Log on to the PowerManage console with user ID **root** and password to complete the following tasks.

Setting the date and time

To set the date and time, complete the following steps from the MMI console menu:

1. On the MMI menu, go to **System Configuration > Date/Time settings**.
2. Ensure that the correct time zone is selected and verify that **Sync with Network Time Protocol (NTP)** is enabled.

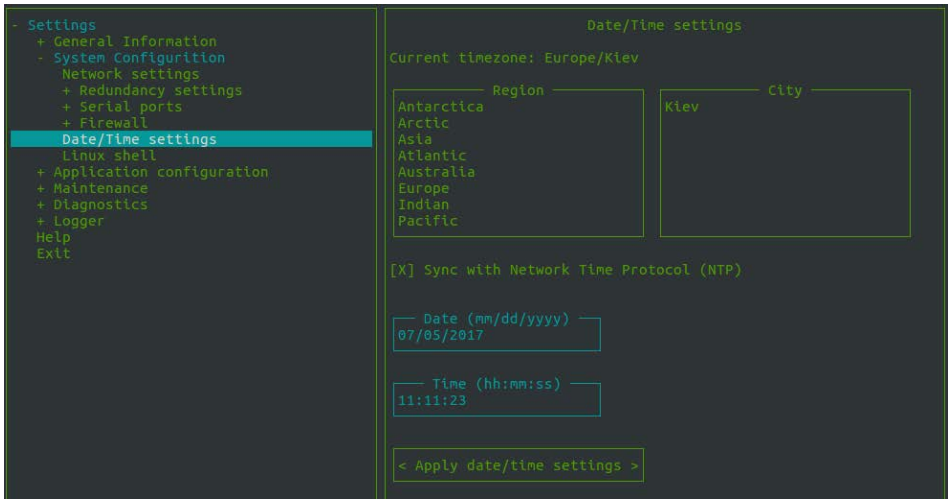


Figure -1 MMI console – Date/Time settings

Configuring the network

To configure the network, complete the following steps from the MMI console:

1. On the MMI menu, go to **System Configuration >Network settings**.
2. In the network configuration pane, in the **Host name** field, enter the host name of the server.
3. In the Primary DNS field, enter the DNS number and if required enter the DNS number for the Secondary and Tertiary DNS.
4. Complete one of the following steps:
    - If the server IP address is configured using DHCP, enable the eth<x> dhcp on/off parameter, where x represents the number of the interface. The enabled field is marked with an X.

- If the server is configured with a static IP address:
    a. Disable the **eth<x> dhcp on/off** parameter, where x is the number of the interface. The disabled field is left blank.
    b. In the **eth<x> IP address**, **eth<x> netmask**, and **eth<x> gateway** fields, type the required values.

5. Select **Apply changes**.

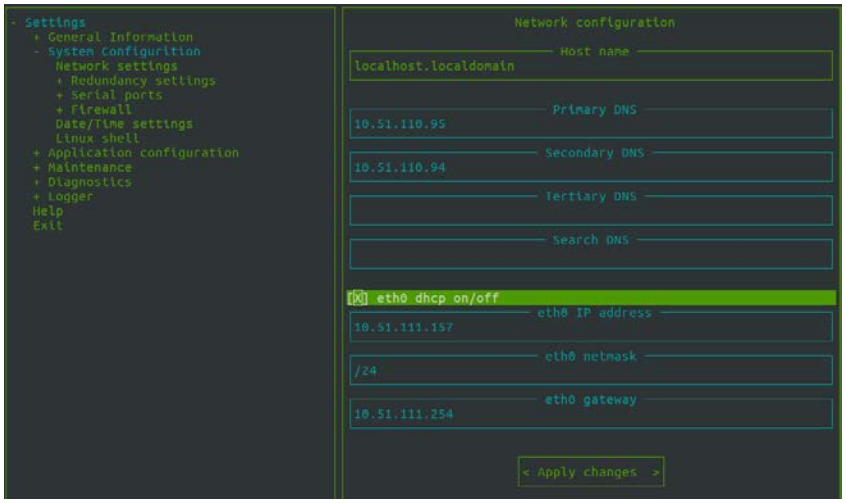


Figure -2 MMI console – Network configuration settings with eth0 selected

Configure the repository

To configure the repository, complete the following steps from the MMI console:

1. On the MMI menu, go to **Maintenance >Repository configuration**.
2. In the repository configuration pane, in the **Server** field, enter the repository IP address.
3. In the **User** field, enter the repository account user name.
4. In the **Password** field, enter the corresponding repository account password.
5. Select **Apply changes**.

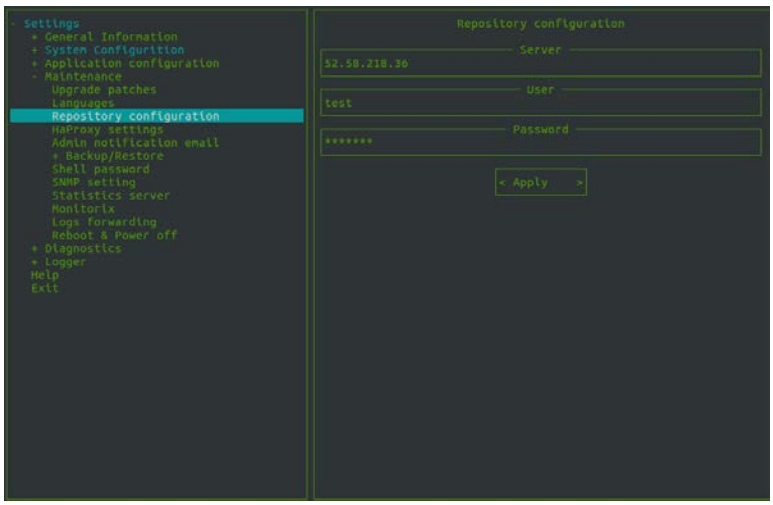


Figure -3 MMI console – Repository configuration settings

Installing patches

PowerManage maintenance updates, which are referred to as patches, bring the server up to the current maintenance software level. You can apply and remove applied patches from the MMI console.

To apply a patch first ensure that you have the repository setting configured on the server.

To install a patch file, complete the following steps from the MMI console:

1. On the MMI menu, go to **Maintenance >Upgrade patches**.
2. In the patches applying configuration pane, in the **Available patches** field, select the required patch file and select **Apply patch**.

After the patch is installed, the name appears in the **Installed patches** field.

Note: To apply multiple patches, you must apply the patches in sequential order. For example, to install `3.6.25.1.tar.gz` and `3.6.25.2.tar.gz`, first install `3.6.25.1.tar.gz` and only after the patch is installed can you install the next patch `3.6.25.2.tar.gz`.

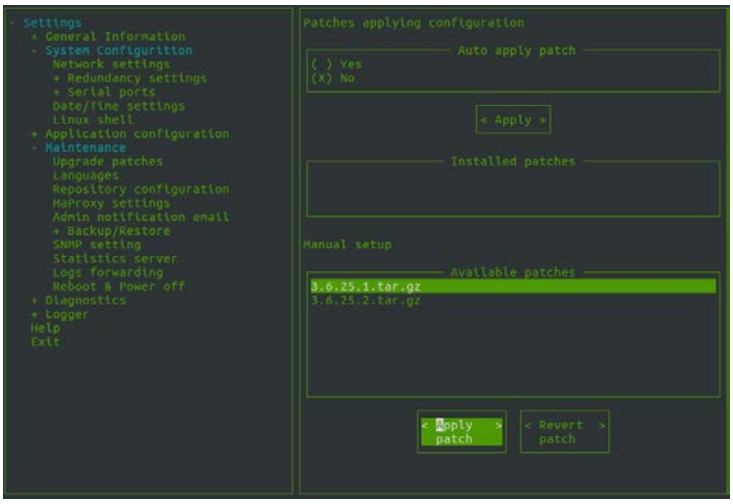


Figure -4 MMI console – Installing patches

Uninstalling patches

To uninstall a patch, complete the following steps from the MMI console:

1. On the MMI menu, go to **Maintenance >Upgrade patches**.
2. In the patches applying configuration pane, in the **Installed patches** field, select the required patch file and select **Revert patch**.

Note: To uninstall multiple patches, you must remove the patches in the reverse order that they were installed.

Backup and restore operations

There are two methods to backup PowerManage data, you can backup data to an FTP server or backup data to a USB drive. Depending on the backup method, you can restore PowerManage data to the server from an FTP server or from a USB drive.

Backing up data to an FTP server

To backup PowerManage data to an FTP server, complete the following steps from the MMI console:

1. On the MMI menu, go to **Maintenance >Backup/Restore >FTP settings**.
2. In the FTP manager pane, complete the following steps:
    - In the FTP IP address field, enter the FTP IP address of the server.
    - In the FTP user field, enter the FTP user name to log on to the server.
    - In the FTP password field, enter the corresponding FTP user password.
3. Select **Save changes**.
4. On the MMI menu, go to **Maintenance >Backup/Restore >Backup**.
5. In the **Backup method** field, select **FTP backup**.
6. In the **Backup variants** field, select the data to include in the backup.
7. In the **Path with name to store on FTP** field, enter the absolute path location to store the backup file and include the file name.

    Note: Select **List dir**, to see a list of backup files that are currently stored in this directory.
8. Select **FTP backup**.
9. A status report is displayed, after the backup is finished, press the **Esc** key on the keyboard to exit the backup mode.

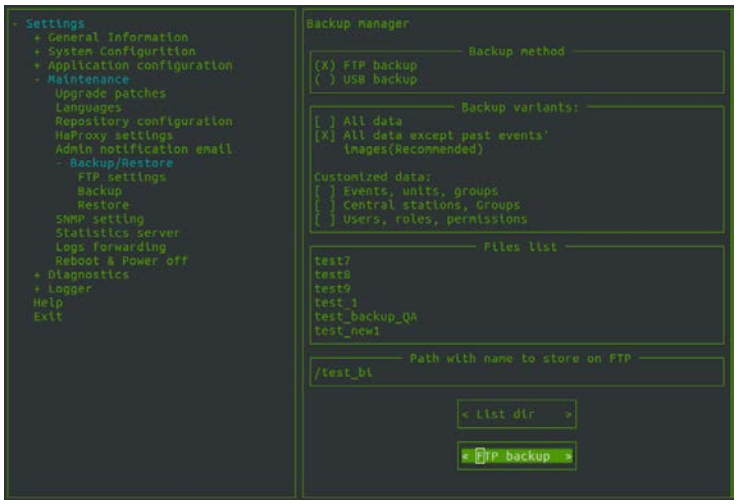


Figure -5 MMI console – FTP backup

Backing up data to an USB drive

To backup PowerManage data to a USB drive, complete the following steps from the MMI console:

1. Connect the USB drive to the server.
2. On the MMI menu, go to **Maintenance >Backup/Restore > Backup**.
3. In the **Backup method** field, select **USB backup**.
4. In the **Backup variants** field, select the data to include in the backup.

5. Select **Check devices** to list available devices and then select the connected USB drive.
6. In the **Path with name to store on USB** field, enter the absolute path to the backup destination and include the file name.

   Note: Select **List dir**, to see a list of backup files that are currently stored in this directory.
7. Select **USB backup**.

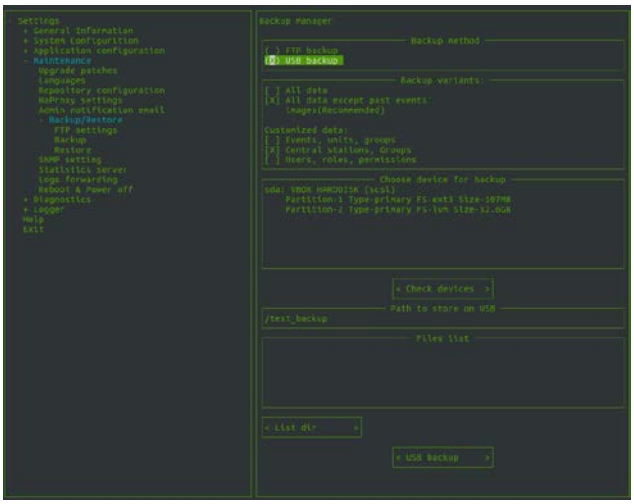


Figure -6 MMI console – USB backup

Restoring data from an FTP server

To restore PowerManage backup data from an FTP server, complete the following steps from the MMI console:

1. On the MMI menu, go to **Maintenance >Backup/Restore >FTP settings**.
2. In the FTP manager pane, complete the following steps:
   - In the FTP IP address field, enter the FTP IP address of the server.
   - In the FTP user field, enter the FTP user name to log on to the server.
   - In the FTP password field, enter the corresponding FTP user password.
3. Select **Save changes**.
4. On the MMI menu, go to **Maintenance >Backup/Restore >Restore**.
5. In the **Restore method** field, select **FTP restore**.
6. In the **Path to restore from FTP** field, enter the absolute path to the directory where the backup file is located.

   Note: Select **List dir**, to see a list of backup files that are currently stored in this directory.
7. In the **Files list** field, select the file to restore and press the **Enter** key on the keyboard.

8. Select **FTP restore**.

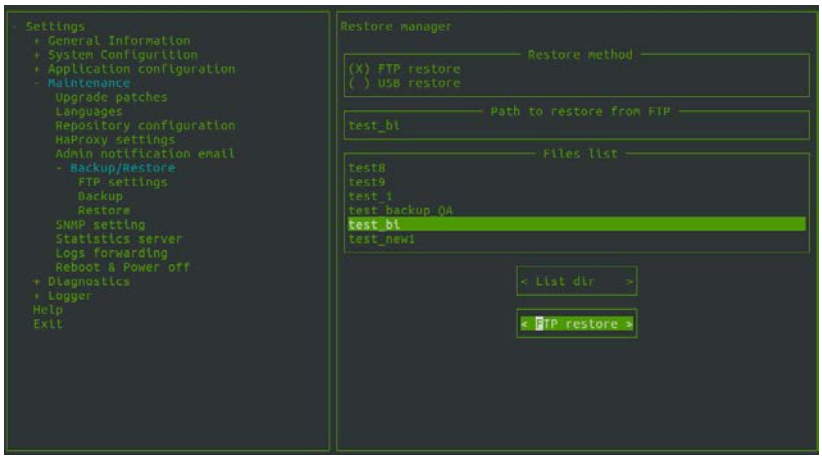


Figure -7 MMI console – Restore from FTP server

Restoring data from a USB drive

To restore PowerManage data from a USB drive, complete the following steps from the MMI console:

1. Connect the USB drive to the server.
2. On the MMI menu, go to **Maintenance >Backup/Restore > Restore**.
3. In the **Restore method** field, select **USB restore**.
4. Select **Check devices** field.
5. In the **Restore from device** field, select the USB connected in step 1.
6. In the **Path to store on USB** field, enter the absolute path to the directory where the backup file is located.

   Note: Select **List dir**, to see a list of backup files that are currently stored in this directory.
7. In the **File list** field, select the required file and press the **Enter** key on the keyboard.
8. Select **USB restore**.

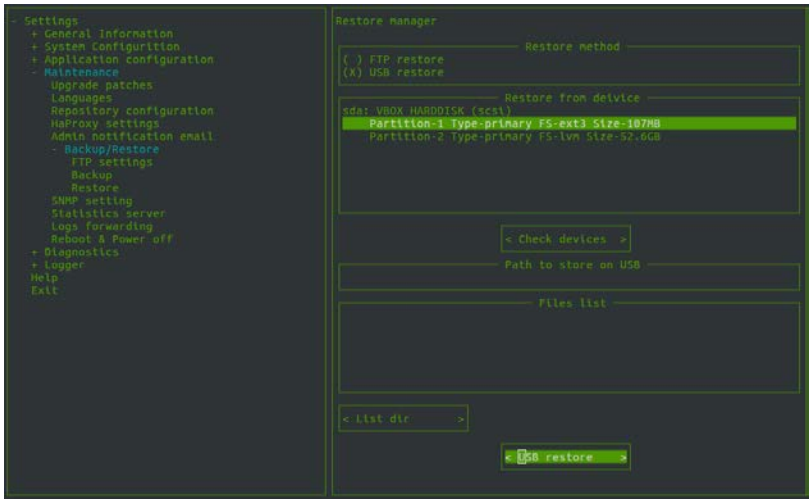


Figure -8 MMI console – Restore from USB device

Configuring for redundancy

Geographical (Geo) redundancy is a remote copy operation between two PowerManage servers at different geographical locations or sites.

You set up a relationship between the two servers, where one server is configured as the primary or master server and the other as the secondary or slave server. Updates on the primary server are synchronized on the secondary server.

Configuring redundancy on a two node system

To configure redundancy for a two node system, complete the following steps:

1. Install servers, see chapter 2 for details.
2. After the installation configure the Central Stations for Master and Slave roles.
3. Log on to the PowerManage MMI console with user ID **root** and password on the primary server (master).
4. On the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy**.
5. In the GeoRedundancy configuration pane, select **Enable Geo Redundancy**.

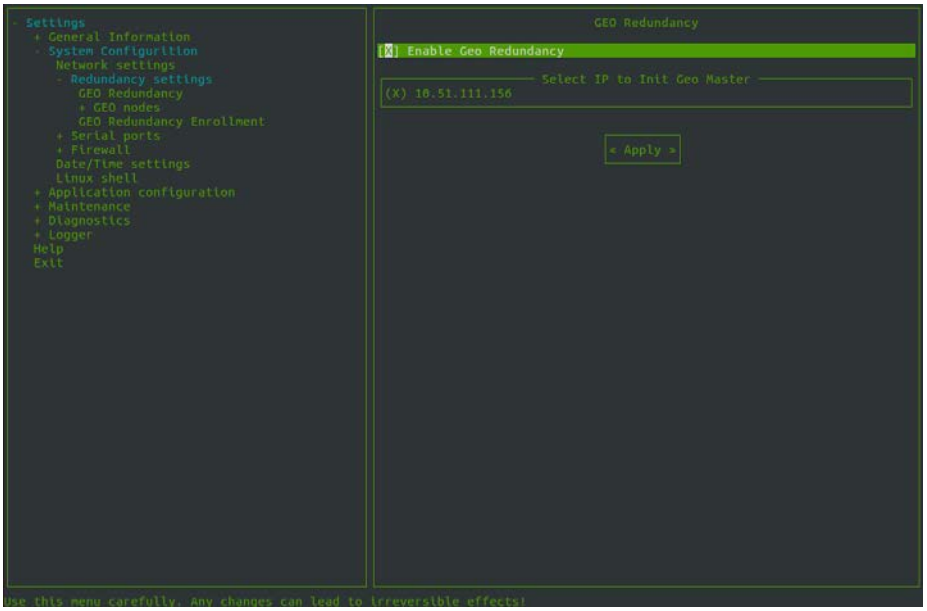


Figure -9 MMI console – Geo Redundancy

6. Select **Apply,** a confirmation dialog box is displayed click **Apply** again.
7. You must wait until the redundancy is enabled. When enabled the mode is Master and displays the Master IP address.

8. Select **Show status** to view the redundancy status and enrolled slaves.

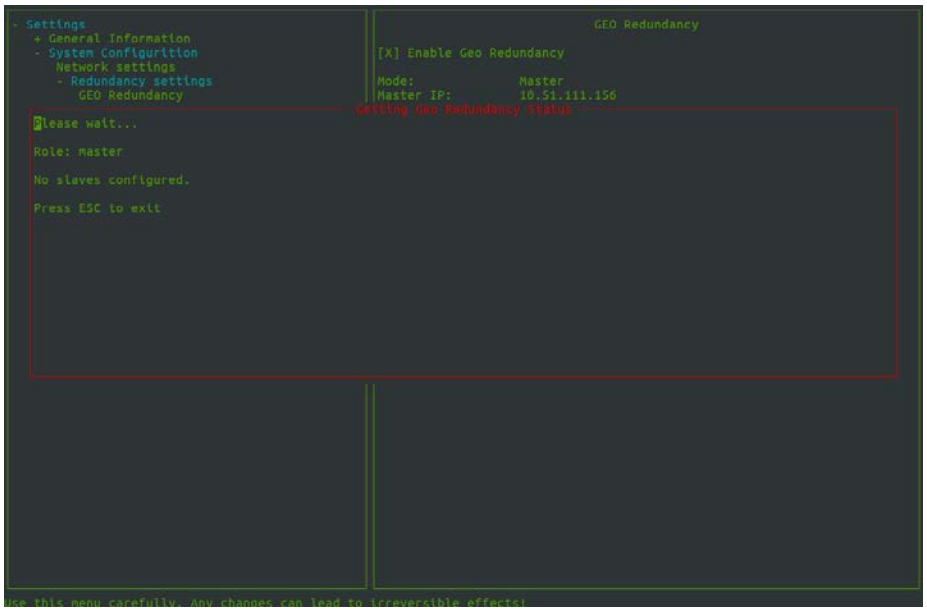


Figure -10 MMI console – Geo Redundancy status

9. On the second server (slave), start the MMI console.
10. Before adding the slave role, verify that **Sync with Network Time Protocol (NTP)** is enabled on both the Slave and Master servers. See Chapter 3, Setting the date and time for details.
11. On the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy Enrolment** and select **Allow enrol this server as slave**.
Note: If not enabled and if the time difference between the master and slave is greater than 10 seconds, the redundancy fails to be created.

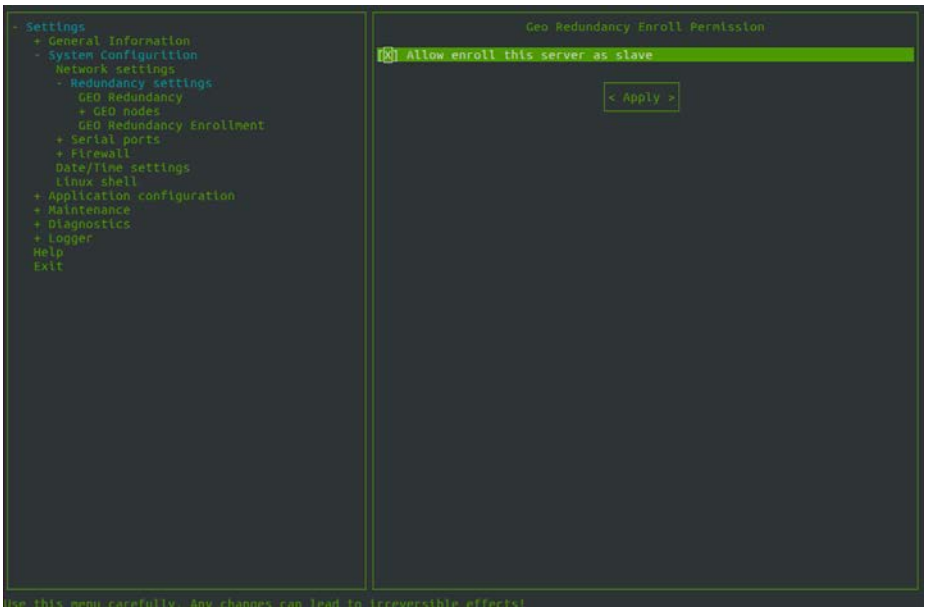


Figure -11 MMI console – Geo Redundancy enrol status

12. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.

13. On the primary servers MMI console menu, go to **System Configuration > Redundancy Settings > GEO Redundancy > GEO nodes > Add GEO slave.**

    - In the Slave IP address field, enter the IP address of the secondary server.
    - In the Slave password field, enter the SSH password that was configured after the installation.

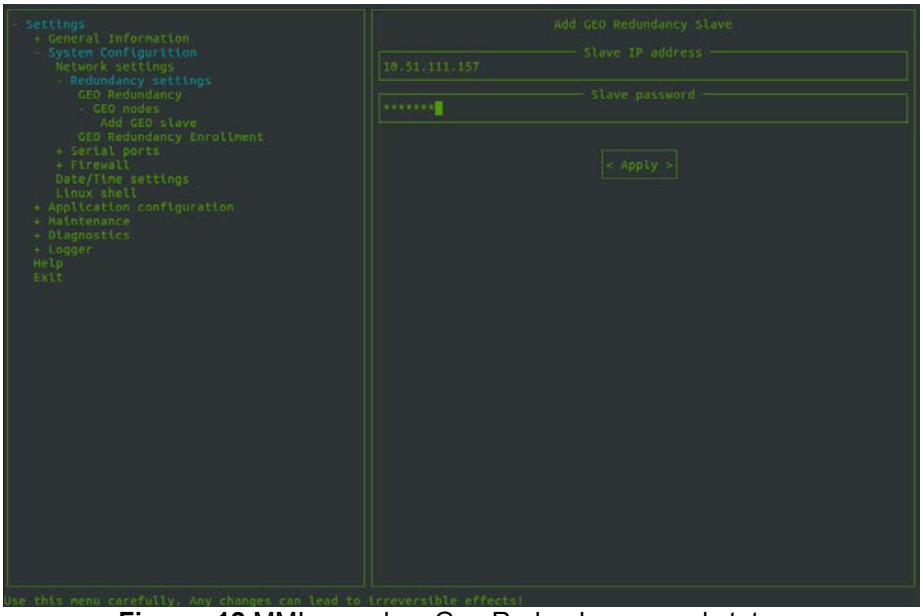


Figure -12 MMI console – Geo Redundancy enrol status

14. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
15. You must wait until the slave is added. When added the redundancy configuration is completed.
16. To see the status of the slave from the primary MMI console menu, go to **System Configuration > Redundancy Settings > GEO Redundancy > GEO nodes** and select **Get slave status**.

Configuring after a failover event on a two node system

When a failover occurs on the primary server, you must reverse the master and slave roles on the servers.

In the event that the primary server fails, complete the following steps:

1. Log on to the primary servers (master) MMI console.
2. On the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy** and deselect **Enable Geo Redundancy** and select **Apply**.
3. Exit the MMI console and log on again.
4. Log on to the secondary servers (slave) MMI console.

5. On the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy** and deselect **Enable Geo Redundancy** and select **Apply**.

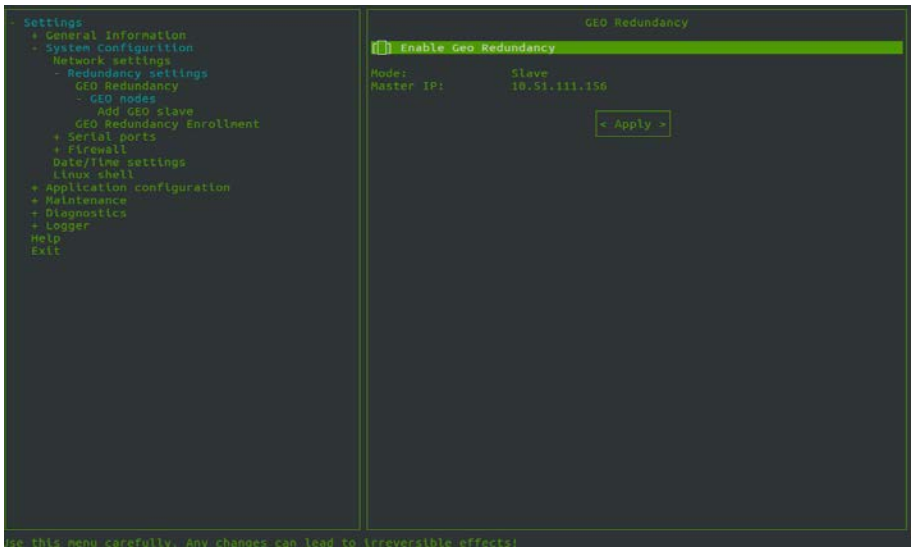


Figure -13 MMI console – Disable Geo Redundancy

6. You must wait until the redundancy is disabled. When disabled the following message is displayed:

```
Important
You should re-establish MMI session to continue.
Press "Exit" and log in again.
<OK>
```

7. Select **OK**. Exit the MMI console and log on again.
8. On the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy** and select **Enable Geo Redundancy.**
9. Select **Apply**. A confirmation dialog box is displayed, select **Apply** again.
10. You must wait until the redundancy is enabled.
11. Start the former primary servers (master) MMI console.

    Note: As a result of the failover the former master is now configured as the slave.
12. On the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy Enrolment** and select **Allow enrol this server as slave**s.
13. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
14. Open the new masters MMI console.
15. On the MMI menu, go to **System Configuration > Redundancy Settings > GEO nodes.**
    - In the **Slave IP address** field, enter the IP address of the former master.
    - In the **Slave password** field, enter the SSH password of the former master.

16. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
17. You must wait until the slave is added.

Configuring redundancy on a four node system

Geographical (Geo) redundancy using a four node system, allows you to add as many slave systems as required. You must configure a Master server at one Geo site and at a second site you must configure a Primary slave role, all other servers can be configured as slave roles.

In the same way as a two node redundancy configuration, the HAProxy server checks which node is the master and redirects REST requests to this node automatically. If no HAProxy server exists, traffic from https://aps_dns must be redirected to the Master node on the firewall.

In the event of a Master Failover, similar to the case of a two node redundancy configuration, the Primary Slave is reconfigured as the Master and a new Primary slave is configured. The primary slave is configured from the MMI console in **System Configuration > Redundancy Settings > GEO Redundancy > GEO nodes > Secondary Node**.

To configure redundancy for a four node system, complete the following steps:

1. Install servers, see chapter 2 for details.
2. After the installation configure the Central Stations for Master and all Slave roles.
3. Log on to the PowerManage MMI console with user ID **root** and password on the primary server (master).
4. On the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy**.
5. In the GeoRedundancy configuration pane, select **Enable Geo Redundancy**.
6. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
7. You must wait until the redundancy is enabled. When enabled the mode shows Master and the Maser IP address is displayed. To view the redundancy status and enrolled slaves, select **Show status**.
8. For each server designated as a slave, complete steps 9 to 10.
9. Start the MMI console and on the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy Enrolment** and select **Allow enrol this server as slave**.
10. Select **Apply,** a confirmation dialog box is displayed click **Apply** again.
11. On the masters MMI console, on the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy > GEO nodes > Add GEO slave.**

    Note: Before adding the slave role, verify that **Sync with Network Time Protocol (NTP)** is enabled on every Slave and Master servers. See Chapter 3, Setting the date and time for details.
12. For each slave node add the IP address and SSH password.

13. To verify that all slaves are added from MMI menu go to **System Configuration > Redundancy settings > GeoRedundancy**

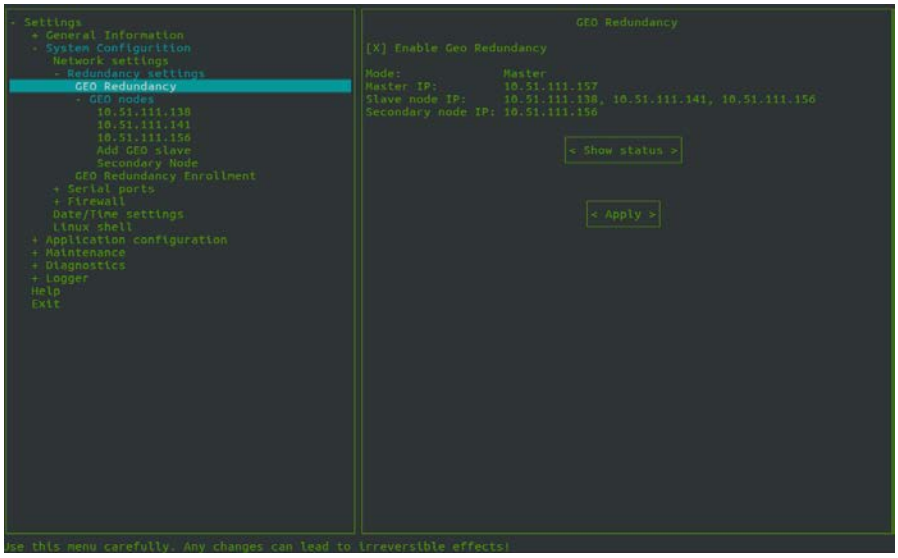


Figure -14 MMI console – Master and slave configuration

14. After enrolling more than one slave, the option **Secondary Node** appears in the menu. Go to **System Configuration > Redundancy settings > GeoRedundancy > Geo nodes > Secondary Node** to assign a primary slave manually.

    Note: By default, the first slave enrolled on the master is the primary slave.

Configuring after a failover event on a four node system

Depending on if the Master or Primary Slave fails different actions are required.

Master failover configuration

In the event that the master fails, you must decide on which server will become the new master server. It can be any of the other servers, for example a primary slave server from the remote site or usually a slave from the same site.

After you manually reconfigure the system, you must change the client firewall and redirect all traffic to the new Master and the primary slave at the remote site if changed.

It is recommended to configure the new master on the same site, otherwise it can be difficult to redirect the traffic from the failed server to the new one. Configuring at the same site, has the advantage of requiring less manual actions and there is no requirement to switch the IP receivers for the panels.

In the event that the primary server fails, complete the following steps:

1. Log on to the primary slave server MMI console. On the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy** and deselect **Enable Geo Redundancy** and select **Apply**.
2. Exit the MMI console and log on again.

3. For each slave and former master, on the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy** and deselect **Enable Geo Redundancy** and select **Apply**.
4. You must wait until the redundancy is disabled.

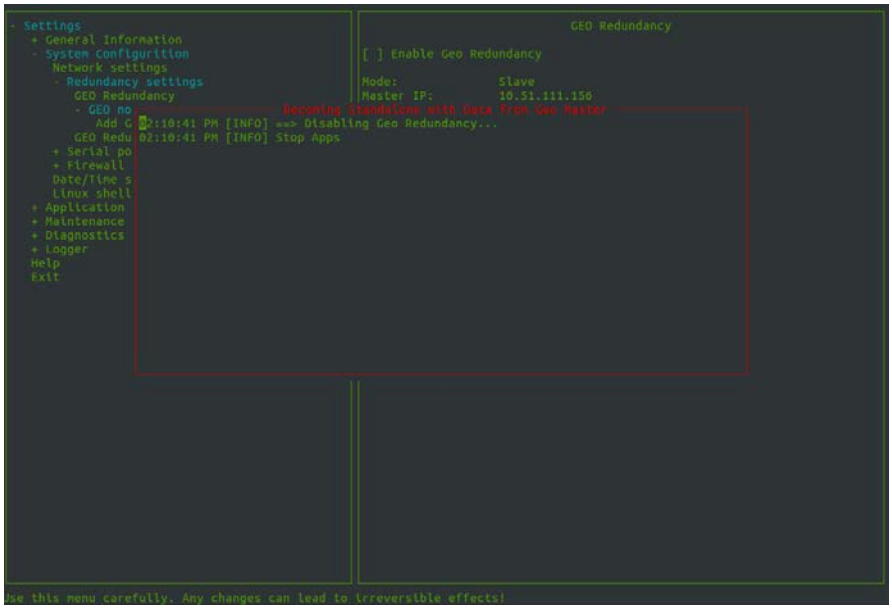


Figure -15 MMI console – Disabling Geo Redundancy

When disabled the following message is displayed:

Important
You should re-establish MMI session to continue.
Press "Exit" and log in again.
<OK>

5. Select **OK**. Exit the MMI console and log on again to each server.
6. In the primary slave MMI menu go to **System Configuration > Redundancy settings > GeoRedundancy** and select **Enable Geo Redundancy**.
7. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
8. You must wait until the redundancy is enabled.
9. For each slave and former master server, complete steps 10 to 11.
10. Start the MMI console and on the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy Enrolment** and select **Allow enrol this server as slave**.
11. Select **Apply,** a confirmation dialog box is displayed click **Apply** again.
12. Start the new master MMI console, on the MMI menu, go to **System Configuration > Redundancy Settings > GEO Redundancy > GEO nodes > Add GEO slave.**
13. For each slave node add the IP address and SSH password of the former Master.
14. Select **Apply,** a confirmation dialog box is displayed select **Apply** again.
15. Wait until the slave is added.

Primary Slave failover configuration

In the event that the primary slave fails, you must reconfigure the new Primary slave on the Master sever.

In the event that the primary slave fails, complete the following steps:

1. Log on to the primary servers (master) MMI console.
2. On the MMI menu, go to **System Configuration > Redundancy settings > GeoRedundancy > GEO nodes > Secondary Node**.
3. In the **Select IP of Secondary node** field, select the new IP address of the new primary slave.

Note: All traffic must be redirected to the new primary slave. It is recommended to select the primary slave on the same site as the one that failed, otherwise problems can be encountered redirecting traffic from the failed node to the new one.

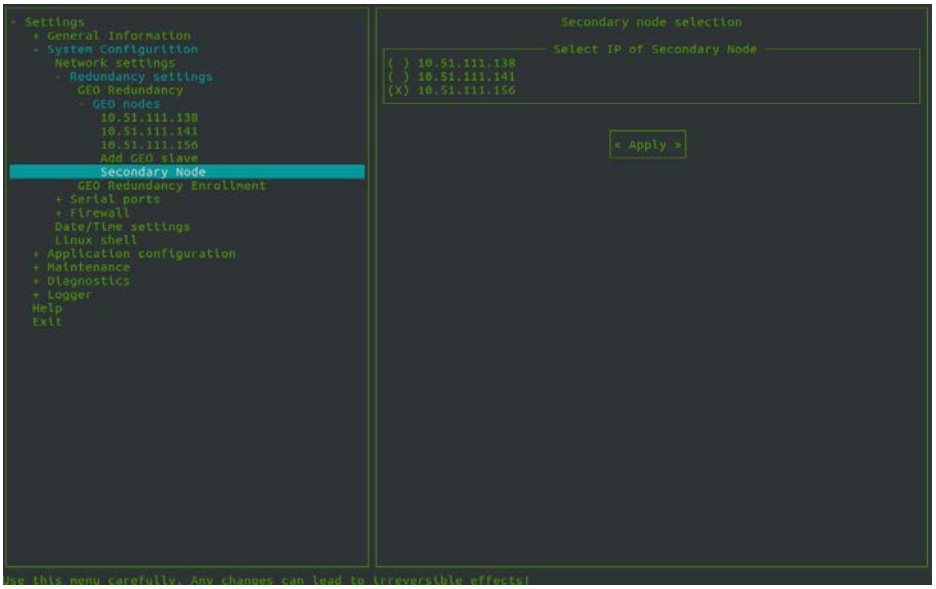


Figure -16 MMI console – Secondary node selection

SSL certification

PowerManage V 3.4.9 and later support HTTPS secure communication. To use this secure communication, you must purchase and install an SSL certificate on the PowerManage server.

Creating a certificate request

To prepare a certificate or SSL request, complete the following steps:

1. Submit a request to the IT department or Internet Service Provider (ISP) to register the PowerMaster server host name for example, *marketing.visonic.com.*
2. Create a file and record the following default 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 host name of the server, for example, *marketing.visonic.com*.
   - Optional: email address.
3. Send the host name of the PowerManage server and the file from step 2 to Visonic. Visonic generates a self-signed certificate request and returns a *public.csr* file and a *private.key* file.
4. Send the *public.*csr *file* and the applicable payment to the certificate authority (CA). The CA returns the signed certificate, such as *.crt file.
5. Send the signed, validated certificate to Visonic and include the original CA email.
6. Visonic uploads the certificate to the repository, which adds HTTPS support to the PowerManage server.

   Note: The certificate consists of a *.csr* and *.key* file, which contains critical security parameters. The *.csr* file is derived from the *.key* file. Therefore, you must keep both files together.
   Ensure that you keep track of the certification expiration and renewal date.

Sending SMS notifications

In order to send SMS notifications you must configure the settings for the SMS broker that you are using. PowerManage is preconfigured for Orange, Cellsynt, TextAnywhere SMS brokers. Also you can configure the modems wake-up settings.

Prerequisites

The GSM modem is connected to the servers configured serial port.

Defining the wake-up modem settings

PowerManage can initiate communications with control panels by sending wake up messages.

To configure the modem settings, complete the following steps:

1. Log on to the PowerManage MMI console. On the MMI menu, go to **Application configuration > Common > SMS Brokers > Add a new broker**.
2. In the **SMS Brokers types** field, select **Modem**.
3. In the **SMS Broker name** field, type the name of the modem.
4. In the **Serial ports** field, select the port to which the modem is connected.
5. In the **SMS Broker description**, type a description or any additional comments.
6. Select Add broker.

Result: The modem is added to SMS Brokers list.

Adding a SMS broker

PowerManage is preconfigured for Orange, Cellsynt, TextAnywhere SMS brokers. To use any of these brokers complete the following steps:

1. Log on to the PowerManage MMI console. On the MMI menu, go to **Application configuration > Common > SMS Brokers**.
2. Select the required broker from the menu list.
3. In the **SMS Brokers sender** field, type the broker's phone number. This number is indicated to the client as the source sender's number for any SMS messages sent by the server.
4. In the **SMS Broker login** and **SMS Broker password** fields, type the user name and password respectively.

5. Select **Add broker**.

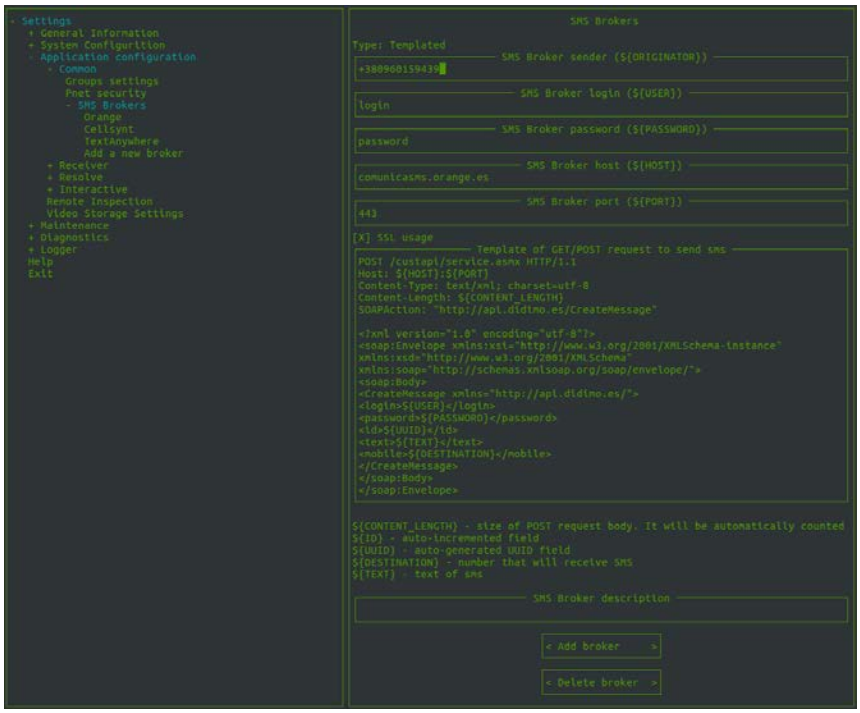


Figure -17 MMI console – SMS brokers

Defining a request

To use a broker other than the preconfigured brokers, you must create an http request that is used to send SMS messages. You must place this request in the brokers configuration file and store the request in the **Template of GET/POST request to send sms** field.

This request syntax can be obtained from the brokers API documentation. There are several parameters but most requests used are generated by PowerManage and can be used as variables inside the request.

To see a list of the PowerManage variables, from the MMI menu, go to **Application configuration > Common > SMS Brokers > Add a new broker**. The variables are listed in the **Template of GET/POST request to send sms** field.

The following list shows the PowerManage variables:

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

When any of the above parameters are used in a request, you just need to store its variable name.

For example, an instance message text is passed into at request as **text=${TEXT}** or **<message>${TEXT}</message>** depending on the brokers API.

The following example shows the text to enter in the **Template of GET/POST request to send sms** field when defining a new broker's configuration file.

The message broker is http://www.vianett.com, see the HTTP GET/POST API documentation at: http://www.vianett.com/en/developers/api-documentation/http-get-post-api.

Request for outgoing message is:

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

For the message broker enter the following text into **Template of GET/POST request to send sms** field:

```
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	Represents the type of method used (GET/POST).
mgsid	Represents the message number and must be a unique ID.
tel	Represents the recipients phone number.
msg	Represents the message text.
campaignid	Represents the parameter specific to the broker, defines your company ID and is specified in the account settings.
HTTP/1.1	Represents the HTTP protocol version.
Host, User-Agent, Connection	Represents the header parameters that are added to the request.

Note: It is important to set the HTTP request line breaks correctly. The requests body should be on one line. Although there are automatic line breaks, all new lines must be created using the **Enter** key.

For example, the following is one line and at the end of the line press the **Enter** key:

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

Type HTTP/1.1 and press **Enter** and so on.

Brokers can use specific parameters in their request, see the brokers API documentation for more details about each parameter. You can use as a reference any of pre-configured message brokers.

Defining a new SMS broker

To add a new message broker, complete the following steps:

1. Log on to the PowerManage MMI console. On the MMI menu, go to **Application configuration > Common > SMS Brokers > Add a new broker**.
2. In the **SMS Brokers types** field, type **Templated**.
3. In the **SMS Brokers name** field, type the broker's name.
4. In the **SMS Broker sender** field, type the broker's phone number. This number is indicated to the client as the source sender's number for all SMS messages sent by the server.
5. In the **SMS Broker login** and **SMS Broker password** fields, type the user name and password respectively.
6. In the **SMS Broker host** field, type the hostname of the broker.
7. In the **SMS Broker port** field, type the port number that is used by the broker.
8. In the **Template of GET/POST request to send sms** field, enter the brokers request to send outgoing SMS messages. See Defining a request for details.
9. Select Add broker.

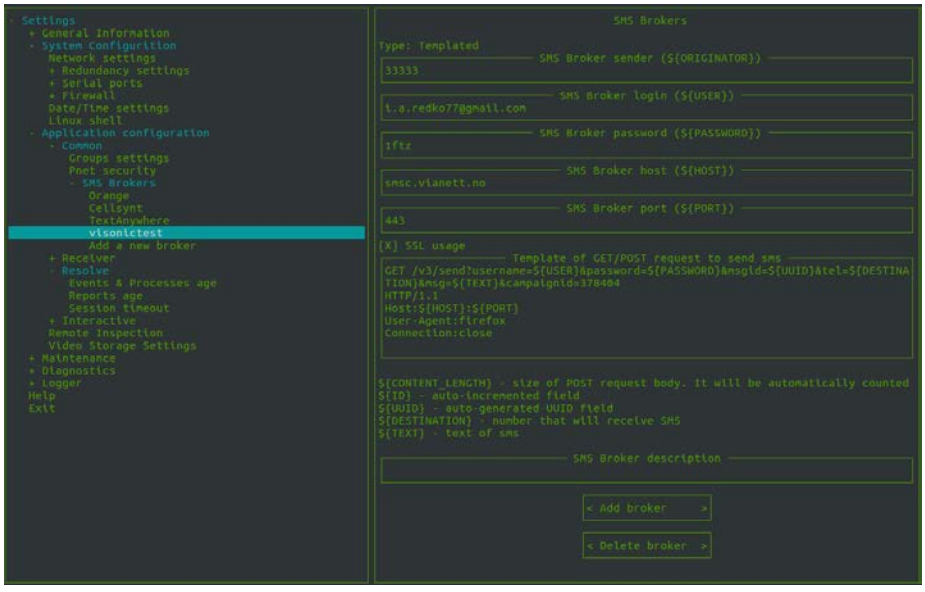


Figure -18 MMI console – Adding a new broker

10. On the MMI menu, go to **Application configuration > Interactive > End user notification > Messaging settings**.
11. Select the **SMS enable** checkbox.
12. In the **Send SMS via** field, select the new broker's name.

13. Select **Apply changes**.

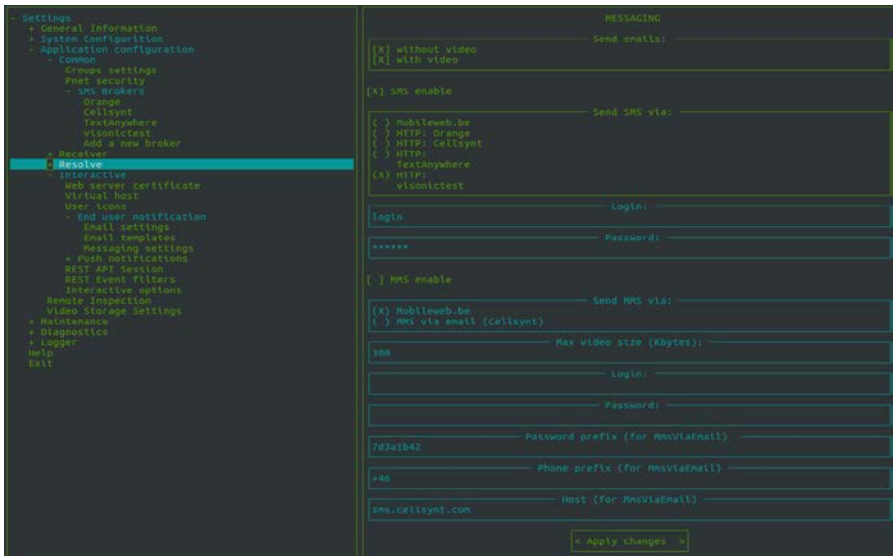


Figure -19 MMI console – Messaging setup

Configuring HAProxy load balancing software

HaProxy (High Availability Proxy) is an open source load balancer software that acts as fast proxy server and provides high availability for TCP and HTTP based applications. It can be implemented and configured for both standalone and Geo redundancy systems.

The PowerManage server uses HAProxy to decrypt SSL traffic. This provides better performance and a more stable and secure system.

The following tasks can be performed by the HAProxy server:

- Decrypts traffic from APP (REST request on 443 HTTPS port) and transmits it directly to PowerManage REST module (3333 HTTP port).
- In the case of a GEO redundancy configuration, the HAProxy checks which node is the master and based on this information REST requests are transmitted to the Master node.

Installing HAProxy

To install HAProxy software you must install Community Enterprise Operation System (CentOS) Linux on the server and configure the network. Then you must install the HAProxy software for PowerManage from an archive.

Installing and configuring CentOS 7

Install CentOS using a minimal or a full ISO image. For instructions and installation files, see the CentOS site at https://www.centos.org/download/.

To configure the network, you can use a graphical interface during the installation or after the installation you can configure from the shell command line.

To configure the network from the shell command line, enter the following commands:

$ nmcli d # identifies all Ethernet cards installed on the server.

$ nmtui # opens graphics terminal for network port configuration

The configuration file is saved to the directory:

/etc/sysconfig/network-scripts/eth_port

To configure the network edit the **eth_port** file manually.

After configuring the network, enter the following command to restart the network service:

$systemctl restart network

Installing HAProxy software

To install the HAProxy software you must download the PowerManage archived version PowerManageProxy_x.x.tar.gz to the CentOS machine.

Use the following command to unpack the archive to any directory, for example the /tmp directory:

$ tar -xzvf PowerManageProxy_x.x.tar.gz -C

D-307302