PowerManage 4.16

Requirements and Installation Guide



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.

2024-09 Rev. 1

Table of contents

- Preface
  - About PowerManage IV
- PowerManage - Supported Hardware
  - High-performance systems hardware (bare-metal server):
    - HPE ProLiant DL380 Gen10
    - High-performance systems load benchmark:
  - High-performance systems hardware (AWS cloud instance):
    - c5d.9xlarge AWS instance
    - High-performance systems load benchmark:
  - Mid-performance systems hardware:
    - HPE ProLiant DL380 Gen10
    - Mid-performance systems load benchmark:
  - Low-cost systems hardware (bare-metal server):
    - Dell OptiPlex 7060
    - Low-cost systems load benchmark:
  - Low-cost systems hardware (AWS cloud instance):
    - m4.xlarge AWS instance
    - Low-cost systems load benchmark:
  - Virtual environment hardware support:
    - Minimum hardware requirements for vSphere client installation
- Network and Firewall requirements
  - Table-1.1 - The list of outbound and inbound ports that should be opened for iLO interface:
  - Table-1.2 - The complete list of inbound ports to be forwarded from the firewall to the server:
  - Table-1.3 - The complete list of outgoing ports to be forwarded from the firewall to the server:
  - Table-1.4 - The list of outbound and inbound ports that should be opened for Geo Redundancy:
- Rack and Power outlet
- Network schematics
- Software Requirements
  - HP Lights-Out Management System
  - Client machine requirements. Used for Web and MMI interface access
- Installation guide
  - During the installation process
  - Preparing boot media
    - DVD image
    - USB image
      - On Windows:
      - On Linux:
  - Booting the installation
    - PowerManage installation on HP equipment
    - PowerManage installation on Dell equipment
    - PowerManage installation on Virtual machines
    - PowerManage installation on VMWare
- Post Installation
  - Initial Setup
    - Configure Network
    - Configure Time Synchronization
    - Configure Repository
    - Configure SSL certificates
    - Configure Public IP address

        - Configure Mail server
    - Common Post-installation Tasks
        - Restoring a backup from version 4.12.46 to version 4.16
        - Configure ITv2 Settings
        - Backup to FTP server
        - Backup to FTP server by schedule
        - Backup to USB
        - Restore from FTP server
        - Restore from USB
        - Setup Email notifications
        - Default Super Admin account settings setup
        - Admin Multi-factor Authentication
        - Configure Antivirus
        - Add an already enrolled NEO/PSP panel without removing it
    - Incremental upgrade
- Firewall
    - Restriction of sources for incoming connections
    - Restriction on the number of simultaneous connections
- Redundancy configuration
    - Two-node system. Local mode
    - Disable redundancy on the Secondary node
    - Two-node system. Geo mode
    - Automatic Failover (two-node system)
    - Manual Failover actions
    - Redundancy configuration (4 nodes system)
    - Automatic failover (four nodes system)
    - Manual Master failover actions
    - Manual Primary Secondary failover actions
- Appendix-A
    - SSL certification

Preface

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

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

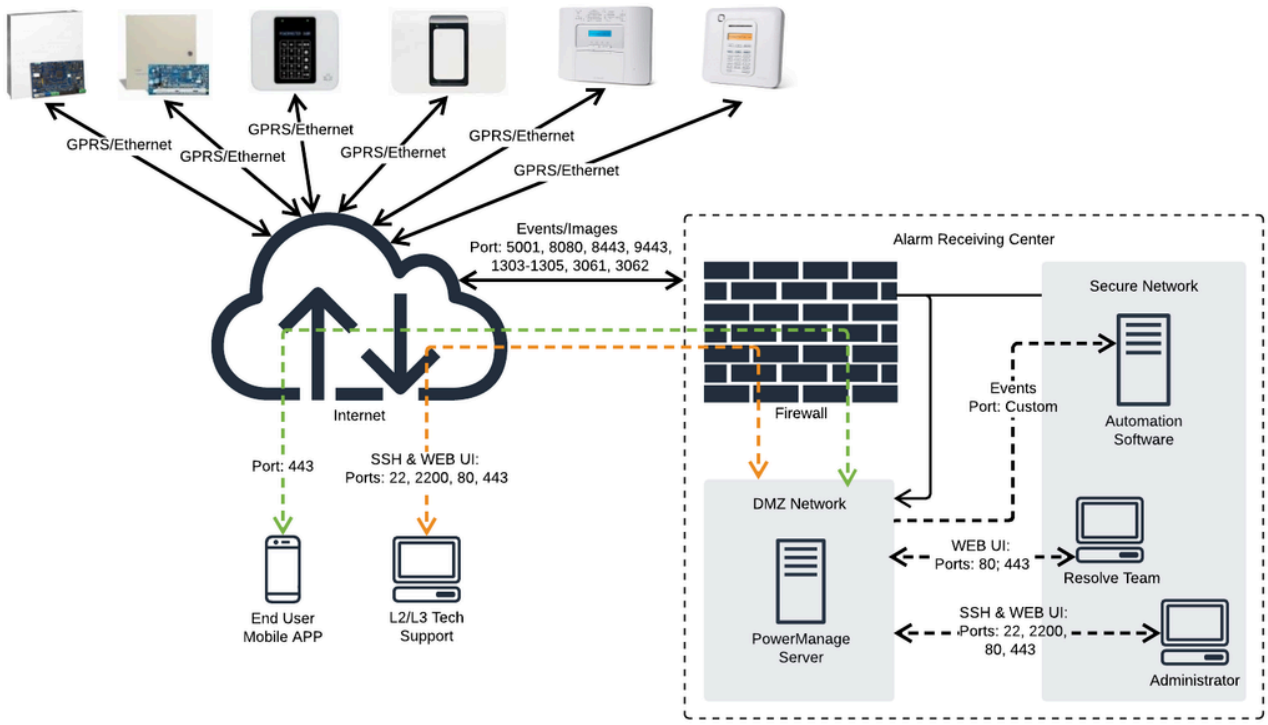
A moderate level of server-based knowledge and experience is assumed**.**

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

About PowerManage IV

PowerManage IV is a highly efficient web-based host platform for provisioning and managing home security and automation services provided by a security service provider. PowerManage IV elaborates on 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 (bare-metal server):

HPE ProLiant DL380 Gen10

Component	Description
Processor	2 CPU Intel® Xeon® Gold 5118 (24 cores, 48 threads, 2.3 GHz, 16.5 MB)
Memory	HPE 96GB Dual Rank x8 DDR4-2666
Storage Controller	HPE Smart Array P408i-a SR Gen10 12G SAS Modular Controller
Storage	RAID 10 (HP 4x600 GB (we recommend HP 4x1 TB) SAS 10k 2,5” SFF recommended)

For more details follow this link: **DL380G10**

High-performance systems load benchmark:

High-performance system solution handles simultaneously:

- Monitor and manage up to 101000 panels
  - PowerMaster BBA - 20K
  - PowerMaster GPRS - 60K
  - DSC BBA - 5K
  - DSC GPRS - 5K
  - DualPath BBA - 1K
  - IQ BBA - 10K
- Supervision periods
  - PowerMaster BBA - 5 sec
  - PowerMaster GPRS - 600 sec
  - DSC BBA - 135 sec
  - DSC GPRS - 135 sec
  - IQ BBA - 135 sec
- ITv2 sessions
  - Handling 1K notifications/sec
- LWM2M
  - Handling 1K notifications/sec
- Events/Alarms
  - Handling 30 events/sec
- Visual Verification/Video on demand
  - Handling 1 frame/sec
- Push notifications
  - Android pushes - Handling – 17 pushes/sec
    Iphone pushes - Handling 17 pushes/sec

- Concurrent Interactive sessions
  - User REST - Handling 500 requests/sec, 250 users
  - Installer REST - Handling 50 requests/sec, 50 users
- Concurrent operators at PowerManage GUI
  - Handling 80 requests/sec, 50 operators
- Billing
  - 3K IQ panels with enabled billing plan
- Concurrent Remote Inspection
  - Up to 1K/hour
- Reports
  - 1 CSV report for each panel per day
  - 1 PDF report for each panel per day

Notes:

These are the maximum values for the 101K system with the above keep-alive.

Overall search on the server affects performance.

High-performance systems hardware (AWS cloud instance):

c5d.9xlarge AWS instance

Component	Description
Instance type	c5d.9xlarge
vCPU	Virtual 36 cores (36 threads) - Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
Memory	72GB
Storage	HDD 1000Gb, volume type gp2, 3000 IOPS, no RAID

Notes:

Amazon EC2 instances support multithreading, which enables multiple threads to run concurrently on a single CPU core. Each thread is represented as a virtual CPU (vCPU) on the instance. An instance has a default number of CPU cores, which varies according to instance type. For example, an m5.xlarge instance type has two CPU cores and two threads per core by default—four vCPUs in total.

Amazon EC2 C5 instances deliver cost-effective high performance at a low price per compute ratio for running advanced compute-intensive workloads. More information you can find in the official AWS documents.

High-performance systems load benchmark:

High-performance system solution handles simultaneously:

- Monitor and manage up to 120000 panels
  - PowerMaster BBA - 5K
  - PowerMaster GPRS - 15K
  - DSC BBA - 70K

    - DSC GPRS - 30K
- Supervision periods
    - PowerMaster BBA - 5 sec
    - PowerMaster GPRS - 600 sec
    - DSC BBA - 135 sec
    - DSC GPRS - 135 sec
- ITv2 sessions
    - Handling 6K notifications/sec
- Events/Alarms
    - Handling 30 events/sec
- Visual Verification/Video on demand
    - Handling 1 frame/sec
- Push notifications
    - Android pushes - Handling – 10 pushes/sec
    - Iphone pushes - Handling 10 pushes/sec
- Concurrent Remote Inspection
    - Up to 1K/hour
- Reports
    - 1 CSV report for each panel per day
    - 1 PDF report for each panel per day
- Concurrent Interactive sessions
    - User REST - Handling 250 requests/sec, 500 users
    - Installer REST - Handling 50 requests/sec, 50 users
- Concurrent operators at PowerManage GUI
    - Handling 40 requests/sec, 25 operators

Notes:

These are the maximum values for the 120K system with the above keep-alive.

Overall search on the server affects performance.

Mid-performance systems hardware:

HPE ProLiant DL380 Gen10

Component	Description
Processor	Intel® Xeon® Gold 5118 (12 cores, 24 threads, 2.3 GHz, 16.5 MB)
Memory	HPE 32 GB Dual Rank x8 DDR4-2666
Storage Controller	1 HPE Smart Array S100i and 1 HPE Smart Array P408i-a SR Gen10 controller
Storage	HPE 600GB SAS 12G Enterprise 10K SFF

For more details follow this link: **DL380G10**

Mid-performance systems load benchmark:

Mid-performance system solution handles simultaneously:

- Monitor and manage up to 50000 panels
  - PowerMaster BBA - 20K
  - PowerMaster GPRS - 50K
- Supervision periods
  - PowerMaster BBA - 5 sec
  - PowerMaster GPRS - 600 sec
- ITv2 sessions
  - Handling 500 notifications/sec
- Events/Alarms
  - Handling 15 events/sec
- Visual Verification/Video on demand
  - Handling 0.5 frame/sec
- Push notifications
  - Android pushes - Handling – 5 pushes/sec
  - Iphone pushes - Handling 5 pushes/sec
- Concurrent Remote Inspection
  - Up to 500/hour
- Reports
  - 1 CSV report for each panel per day
  - 1 PDF report for each panel per day
- Concurrent Interactive sessions
  - User REST - Handling 250 requests/sec, 125 users
  - Installer REST - Handling 25 requests/sec, 25 users
- Concurrent operators at PowerManage GUI
  - Handling 40 requests/sec, 25 operators

Notes:

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

Overall search on the server affects performance.

Low-cost systems hardware (bare-metal server):

Dell OptiPlex 7060

Component	Description
Processor	Intel(R) Core(TM) i5-8500 (6 Cores, 6 threads, 3,00 GHz)
Memory	16GB 2X8GB DDR4 2400MHz DIMM
Storage	1 x NVMe 256GB

Low-cost systems load benchmark:

Low-cost system solution handles simultaneously:

- Monitor and manage up to 10000 panels
  - PowerMaster BBA - 2K
  - PowerMaster GPRS - 6K
  - DSC BBA - 500
  - DSC GPRS - 500
  - IQ BBA - 1K
- Supervision periods
  - PowerMaster BBA - 5 sec
  - PowerMaster GPRS - 600 sec
  - DSC BBA - 135 sec
  - DSC GPRS - 135 sec
  - IQ BBA - 135
- ITv2 sessions
  - Handling 100 notifications/sec
- LWM2M sessions
  - Handling 200 notifications/sec
- Events/Alarms
  - Handling 20 events/sec
- Visual Verification/Video on demand
  - Handling 0.1 frame/sec
- Concurrent Remote Inspection
  - Up to 200/hour
- Reports
  - 1 CSV report for each panel per day
  - 1 PDF report for each panel per day
- Concurrent Interactive sessions
  - User REST - Handling 200 requests/sec, 100 users
  - Installer REST - Handling 10 requests/sec, 10 users
- Concurrent operators at PowerManage GUI
  - Handling 15 requests/sec, 10 operators

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

Low-cost systems hardware (AWS cloud instance):

m4.xlarge AWS instance

Component	Description
Instance type	m4.xlarge
vCPU	Virtual 4 cores (4 threads) - Intel(R) Xeon(R) Scalable Processor (Broadwell E5-2686 v4 or Haswell E5-2676 v3) up to 2.4GHz
Memory	16GB
Storage	HDD 300Gb, volume type gp2, 3000 IOPS, no RAID

Notes:

Amazon EC2 instances support multithreading, which enables multiple threads to run concurrently on a single CPU core. Each thread is represented as a virtual CPU (vCPU) on the instance. An instance has a default number of CPU cores, which varies according to instance type. For example, an m5.xlarge instance type has two CPU cores and two threads per core by default—four vCPUs in total.

Amazon EC2 M4 instances provide a balance of compute, memory, and network resources. More information you can find in the official AWS documents.

Low-cost systems load benchmark:

High-performance system solution handles simultaneously:

- Monitor and manage up to 3000 panels
  - PowerMaster BBA - 1000
  - PowerMaster GPRS - 1000
  - DSC BBA - 500
  - DSC GPRS - 500
- Supervision periods
  - PowerMaster BBA - 5 sec
  - PowerMaster GPRS - 600 sec
  - DSC BBA - 135 sec
  - DSC GPRS - 135 sec
- ITv2 sessions
  - Handling 70 notifications/sec
- Events/Alarms
  - Handling 3 events/sec
- Visual Verification/Video on demand
  - Handling 1 event/sec
- Concurrent Remote Inspection
  - Up to 100/hour
- Reports
  - 1 CSV report for each panel per day
  - 1 PDF report for each panel per day
- Concurrent Interactive sessions

- User REST - Handling 80 requests/sec, 40 users
- Installer REST - Handling 1 request/sec, 2 users

- Concurrent operators at PowerManage GUI
  - Handling 2 requests/sec, 5 operators

Notes:

These are the maximum values for the 3000 system with the above keep-alive.

Overall search on the server affects performance.

Virtual environment hardware support:

Minimum hardware requirements for vSphere client installation

Component	Description
CPU	2 CPU
Processor	Intel or AMD processor with two or more logical cores 2GHz each.
Memory	8 GB RAM
Storage	1 x 300 GB - SATA or 1 x NVMe 256GB

Network and 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 a default-deny policy, allowing only the services listed below.

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

$$R \approx (N_{GPRS} + N_{BBA})*5,$$

where

N_{GPRS} - number of GPRS panels enrolled to the server,

N_{BBA} - number of BBA panels.

Note: The highest concurrent connections number is reached in a 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 slower 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 are 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 the needed connections. For more information check Table-1.3.

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.

IMPORTANT: In case when the issue is required to be investigated by the PowerManage team, SSH access from specific IP addresses must be provided to the support team. Otherwise, the support team performs any troubleshooting on the server. The exact IP addresses can be provided upon your request to PowerManage-Support@jci.com.

Table-1.1 - The list of outbound and inbound ports that should be opened for iLO interface:

Port	Protocol	Description
Extended support [iLO]		
443	TCP	iLO Web interface
17988	TCP/UDP	iLO
17990	TCP/UDP	iLO

Table-1.2 - The complete list of inbound ports to be forwarded from the firewall to the server:

Port	Protocol	Description
Panel ports		
5001	TCP/UDP	Alarm signals/Resolve
8080	TCP/UDP	Alarm images
8443	TCP/UDP	Alarm images [secured]
9443	TCP/UDP	LTE upgrade
3061-3062	UDP	Fibro Alarms and images
1303-1304	TCP	ITv2 Alarms/Resolve
1305	TCP	DLS Resolve
5685	UDP	LwM2M Bootstrap port
5684	UDP	LwM2M main port
Web interface		
443	TCP	Resolve Web interface and REST API
2200	TCP	Web MMI console
Administrating		
161	TCP/UDP	SNMP
22	TCP	SSH and MMI console

Table-1.3 - The complete list of outgoing ports to be forwarded from the firewall to the server:

Port	Protocol	Description
Temporary ports		
27000-65333	TCP/UDP	Ephemeral port range
Push notifications		
443	TCP	Android and iOS push notifications
Email sending		
25	TCP	SMTP port
465, 587	TCP	SMTP port with SSL
Repo synchronization		
443	TCP	Updating certificates and keys
5443	TCP	Updating license

Table-1.4 - The list of outbound and inbound ports that should be opened for Geo Redundancy:

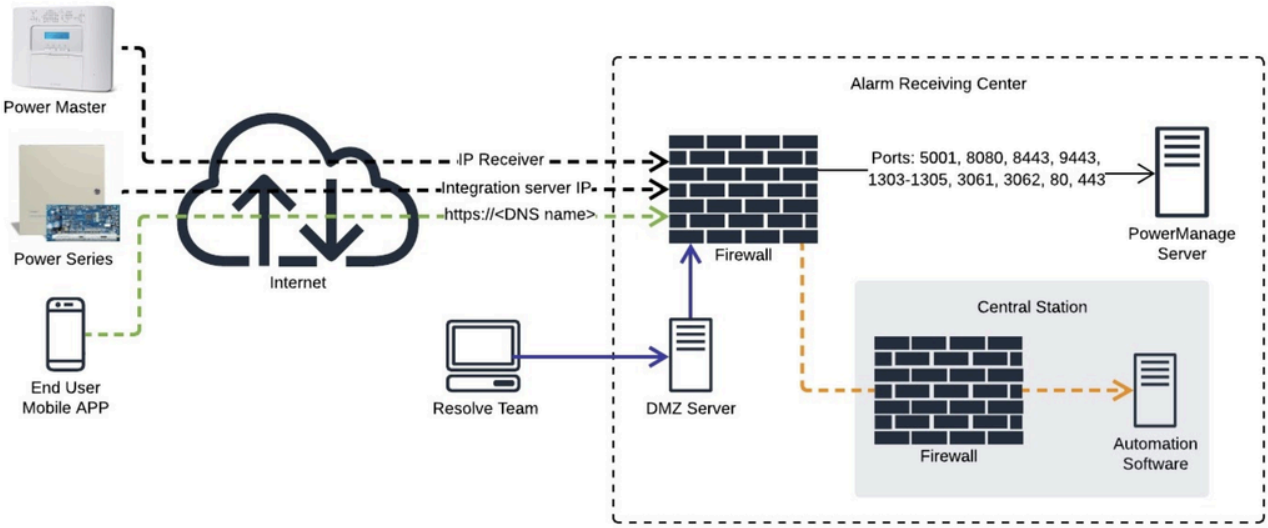
Port	Protocol	Description
Redundancy		
22	TCP	SSH connection between nodes
500	UDP	IPSEC. For IKE, to manage encryption keys
4500	UDP	IPSEC NAT-Traversal mode

Rack and Power outlet

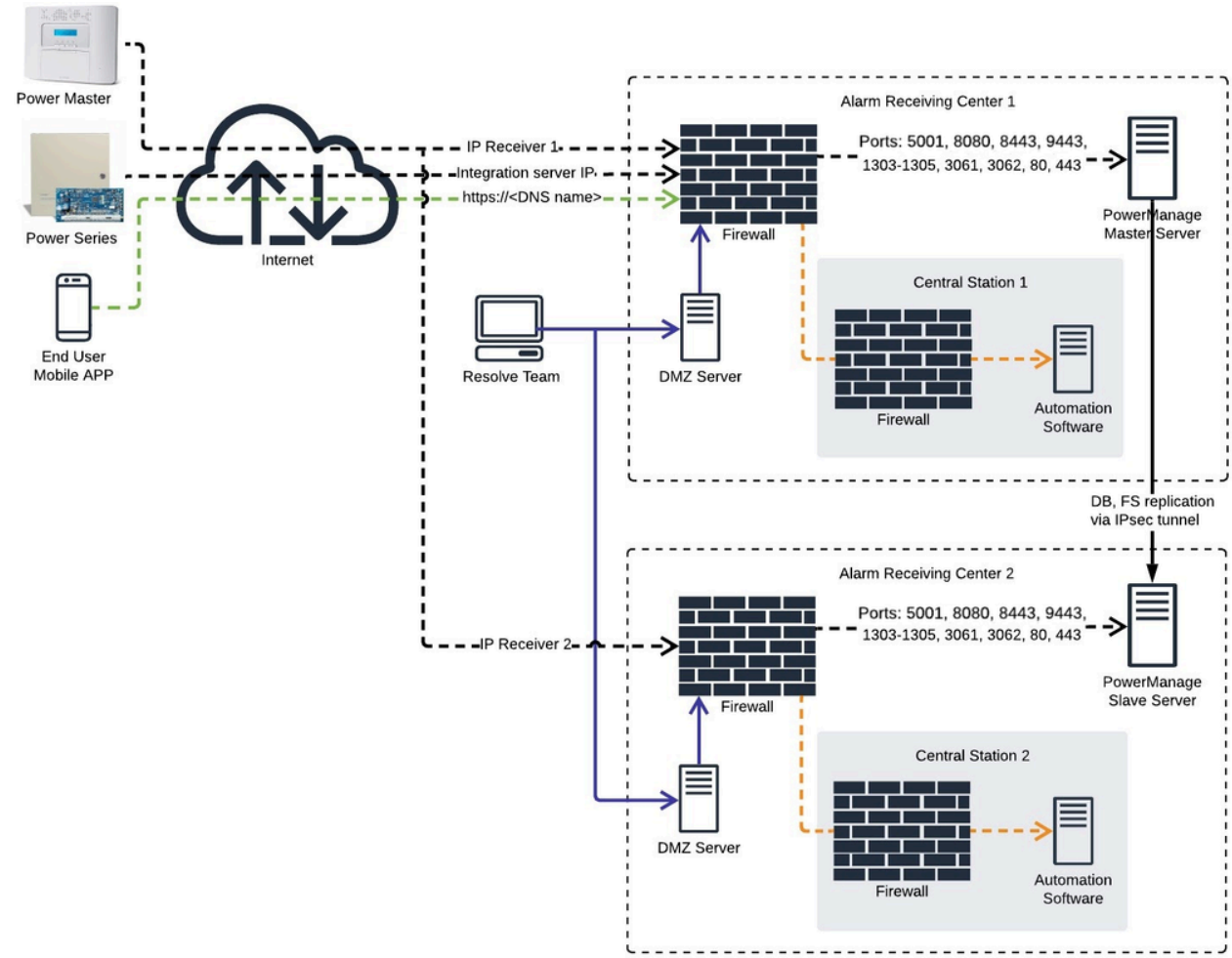
Make sure you have enough room in your designated server rack for a 2U-sized server and at least one free power outlet. A second power outlet is recommended as the server has two redundant power supplies. More outlets may be required according to the server configuration that is explained in this document.

Network schematics

Cost-Effective - standalone diagram



Hot Backup - two nodes multisite 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 supports easier and more reliable. For more details about iLO use this link.

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 11.
  - Red Hat Linux, Ubuntu Linux, Fedora, etc.
  - Mac OS
- Browsers:
  - Google Chrome 110+
  - Mozilla Firefox 102+
- 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 PowerManage 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 that 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

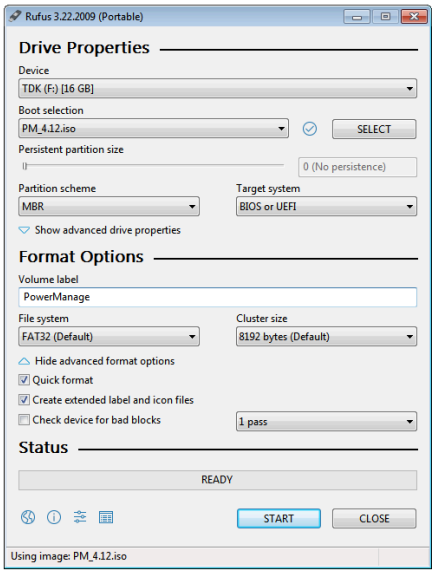
USB image

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

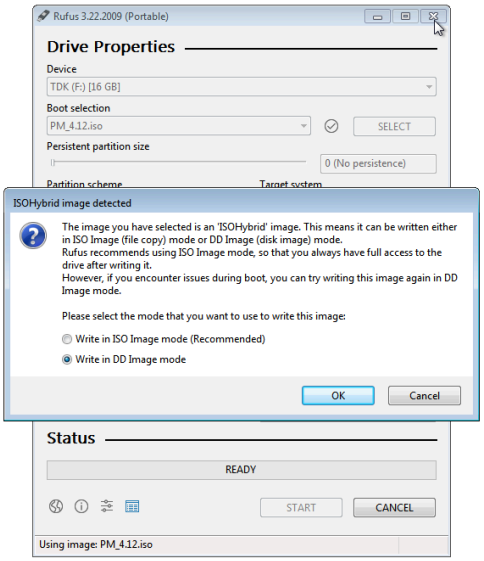
On Windows:

To create a bootable USB under Windows:

- Download and launch **Rufus**



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



On Linux:

Linux includes the **dd** command for this purpose. The dd utility requires you to specify the device file that corresponds to the physical media. The name of the device file matches the name assigned to the device by your system. All device files appear in the directory /dev/.

To write an image file to boot media with dd:

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

> **IMPORTANT**: **The default root user must not be changed.** The PowerManage is an entirely completed product that has been tested and validated with the exact environment and configuration that are provided by the original PowerManage distribution. In case of any additional packages are installed and configuration changes are made by the customers, support will not be provided.

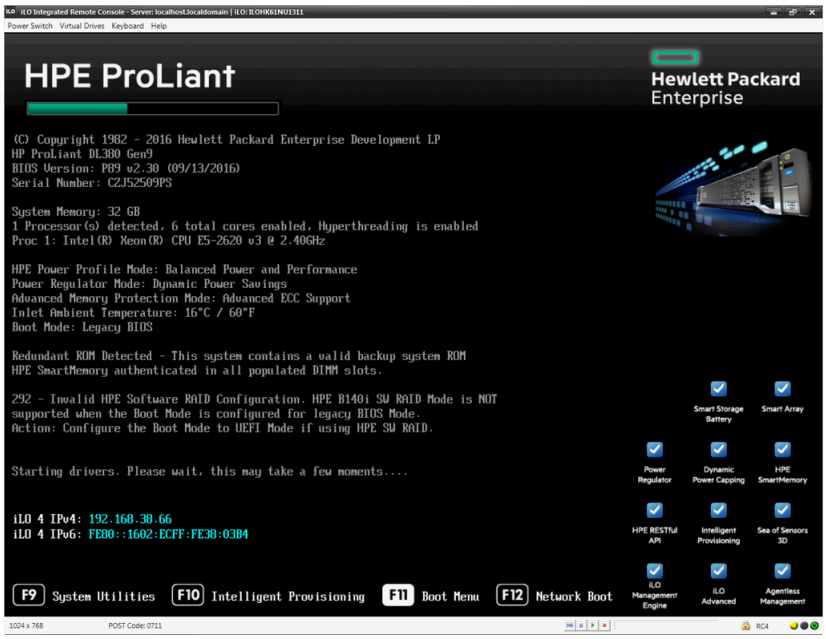
- The default user for the MMI is **mmi**, the default password is **visonic**.
- The **Secure Boot** option must be disabled before starting the installation.
- An Internet connection and a DHCP server on the network are required during the installation.
- Remove previous installations from UEFI boot records.

PowerManage installation on HP equipment

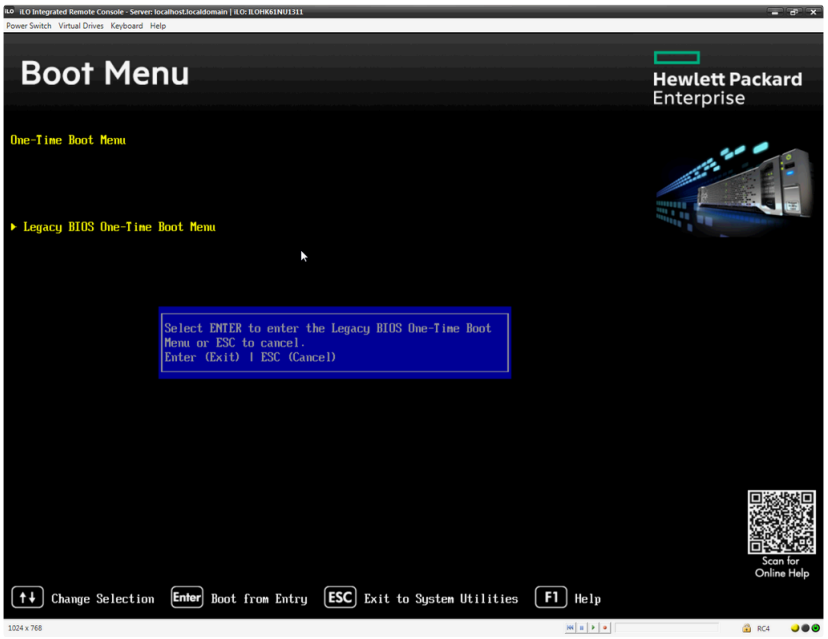
- Power On HP server.
- Plugin the boot USB drive or insert the boot DVD into your optical disc drive

> **Note:** During the PowerManage installation only one type of bootable drive (USB or DVD) must be inserted into the server.

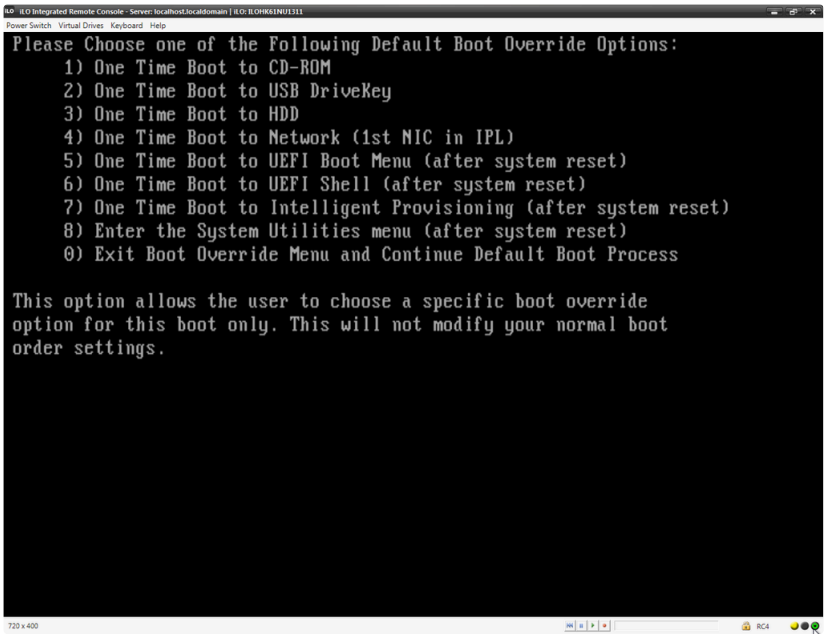
- Restart the system
- On the startup screen, press **F11** to enter the Boot Menu



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

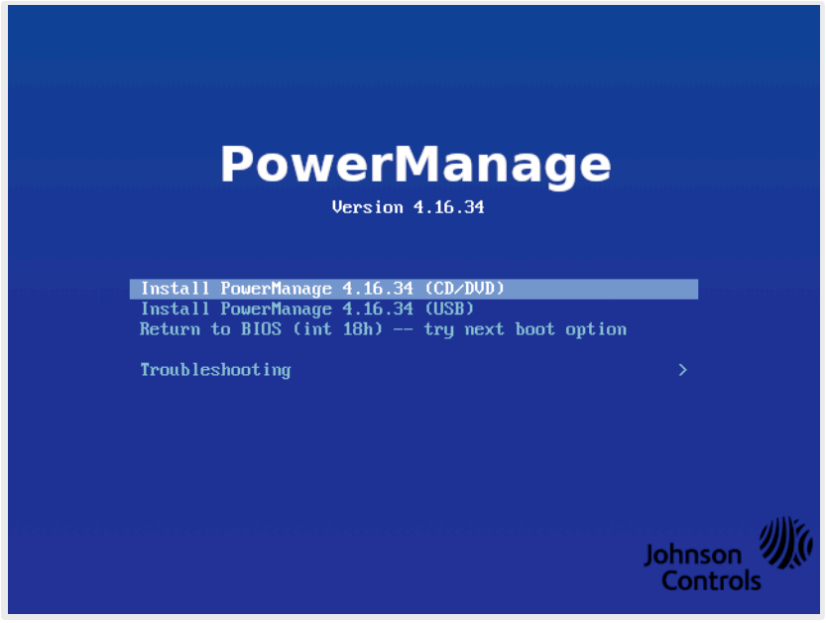


- Depending on the installation media DVD/USB select from the list of options:
  - **One Time Boot to CD-ROM**;
  - **One Time Boot to USB DriveKey.**



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

- Wait until installation starts and type the boot option:
  - **USB** - in case of a USB installation
  - **CD/DVD** - in case of DVD installation

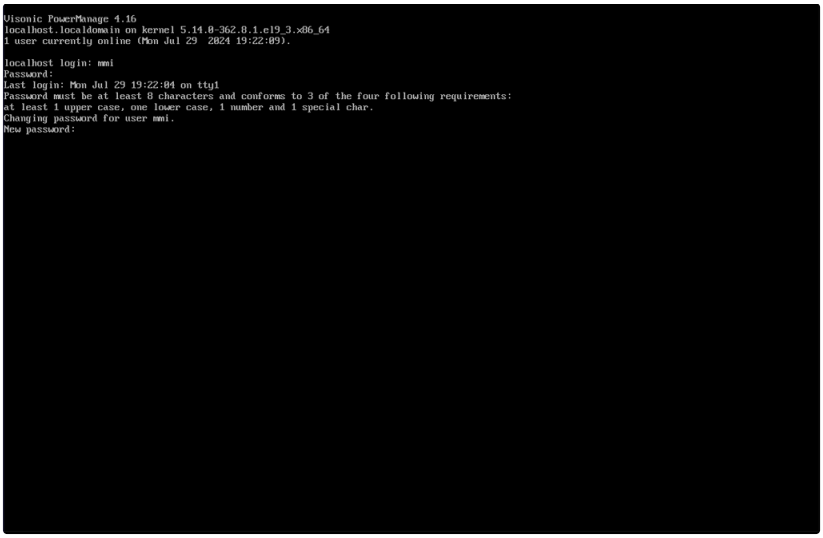


- Wait until the installation is completed.
- Once the installation is completed, the server restarts and appears on a screen that prompts you to login [user - **mmi,** password - **visonic**].

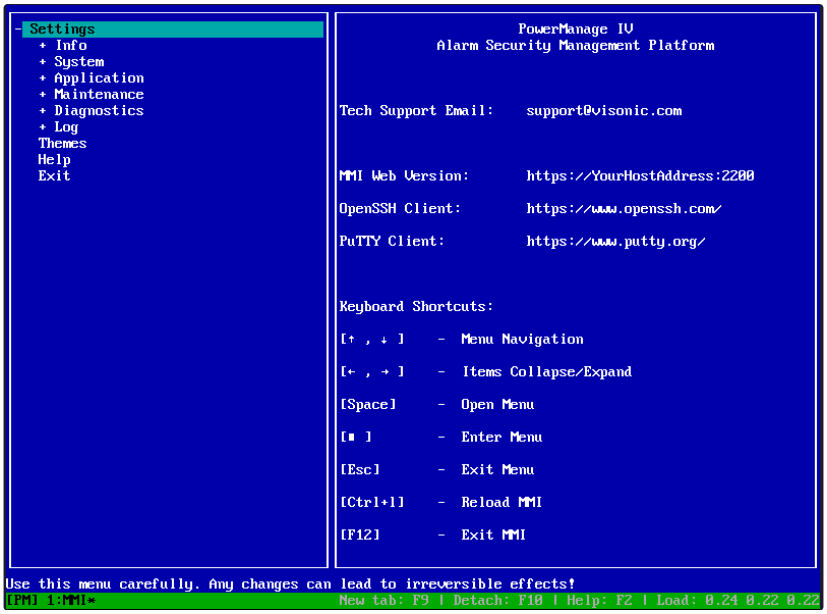
> **Note**: Don't forget to unplug the DVD / USB stack after the reboot process.

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

> **Note**: Use a combination of letters, numbers, and special characters. The password to include both uppercase and lowercase characters.



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



PowerManage 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 Dell's BIOS configuration peculiar properties, two exactly the same USB drivers with the same PowerManage images are needed.

- Plugin the boot USB drive or insert the boot DVD into your optical disc drive

> **Note:** During the PowerManage installation only one type of bootable drive (USB or DVD) must be inserted into the server

- Reboot the system
- On the startup screen, press **F12** to enter the One-Time Boot Menu
- Select a one-time boot option: either USB or CD-ROM
- Perform steps 6-11 from the **Installation on HP equipment** instructions

PowerManage installation on Virtual machines

Installation of the PowerManage on the Virtual Machines can be installed on the following platforms:

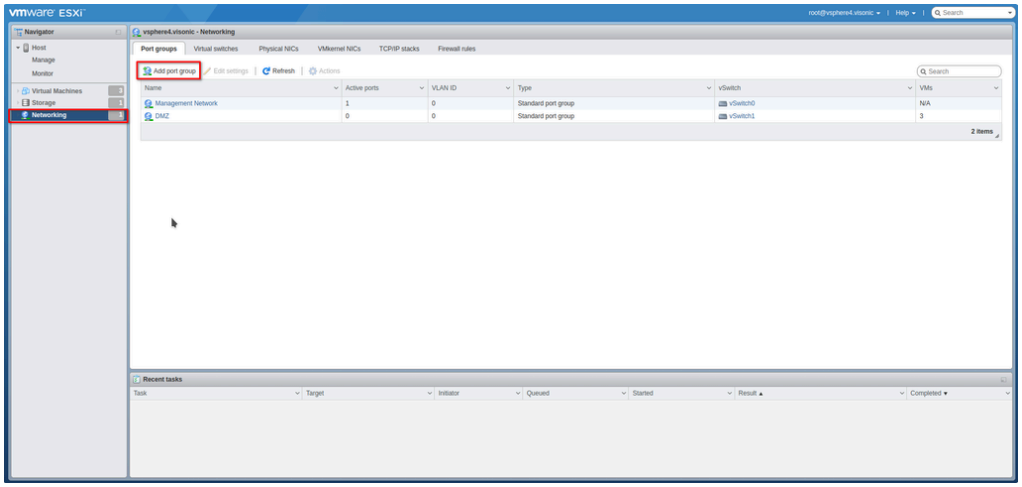
- Proxmox
- VMware

For the installation overview on the VMWare platform, please refer to the PowerManage installation on VMWare paragraph.

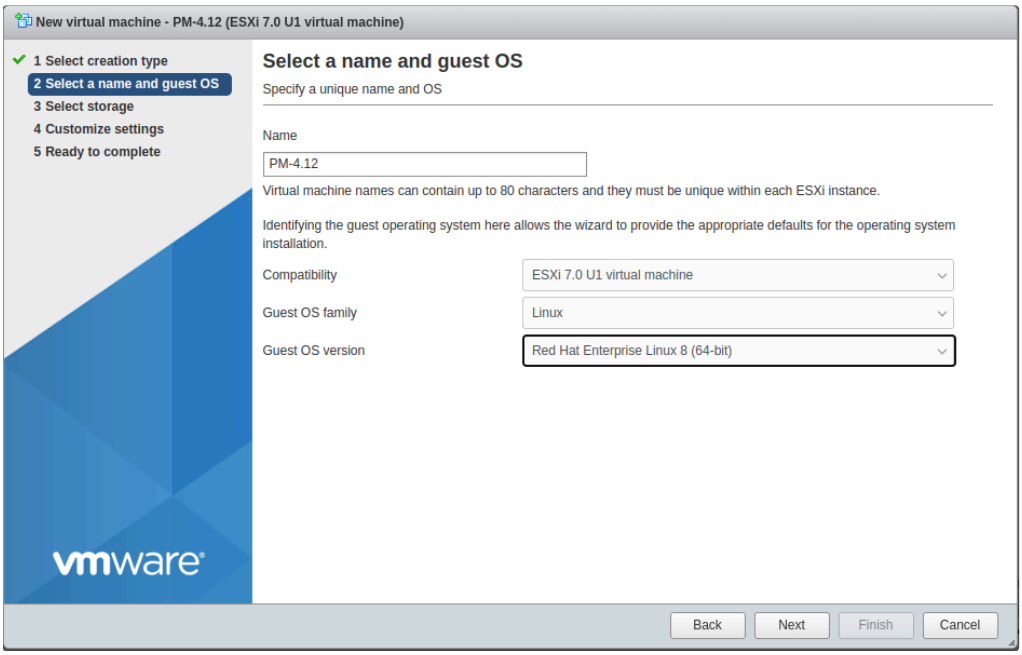
PowerManage installation on VMWare

PowerManage installation on the VMWare virtual environment requires a server with VMWare installed and a PowerManage ISO image.

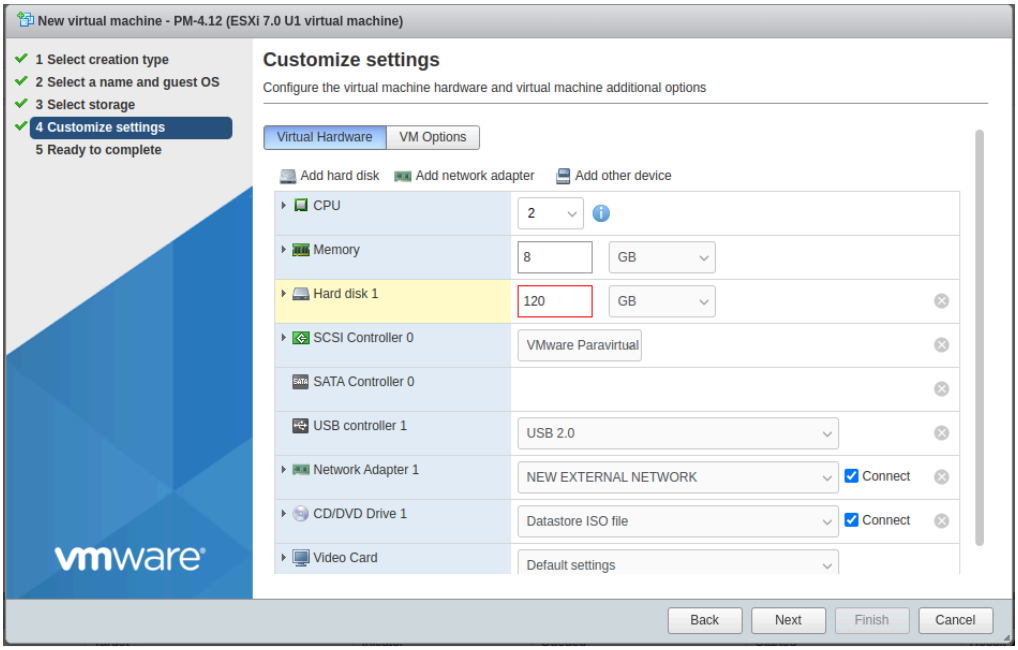
- Login to vSphere client.
- Add a new adapter to the virtual machine [should be done once]: go to the "Networking" page.



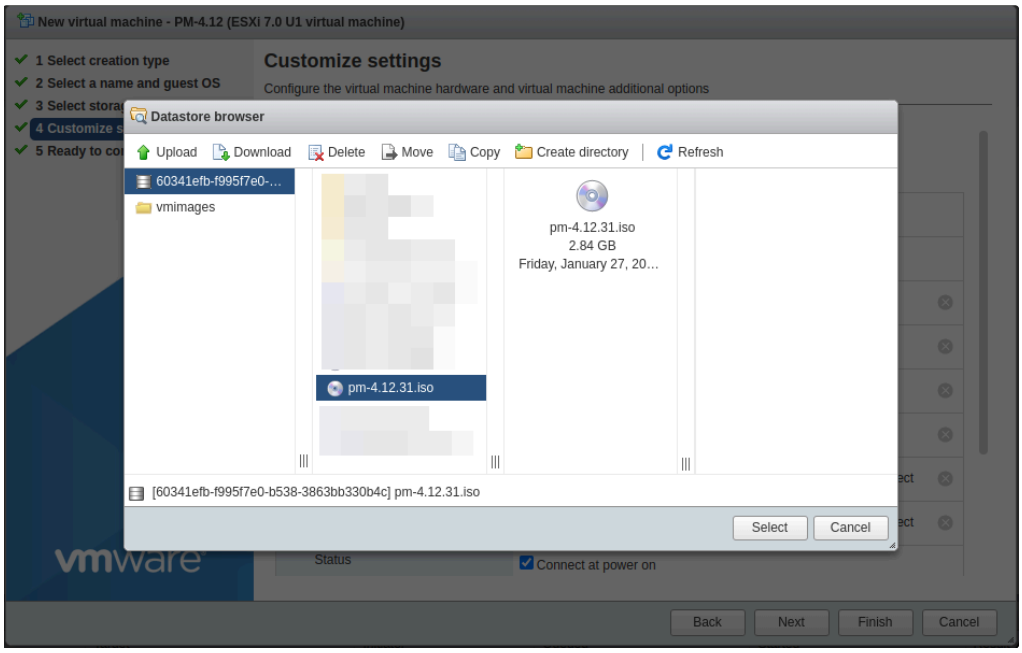
- Press ‘Add port group’.
- Enter the adapter name.
- Select the relevant Virtual switch and press “Add”.
- Upload the PowerManage image file to the VM datastore: go to the ‘Storage’ tab, select the relevant Datastore, and press Datastore browser.
- Press upload and select PowerManage iso file from your workstation.
- Add a new virtual machine: go to the Virtual Machines and press ‘Create / Register VM’.
- Select the ‘Create a new virtual machine option in the configuration menu, and press ‘Next’.
- Enter the virtual machine name, set ‘Guest OS family’ as ‘Linux’ and ‘Guest OS version’ as ‘Red Hat Enterprise Linux 8’, and press ‘Next’.



- Select a destination data storage for new virtual machine files, and press ‘Next’.
- Select the Network connection and Adapter to use that you had configured at the beginning of this guide, and press ‘Next’.
- Set virtual disk size: not less than 120 GB, set the ‘Thick Provision Lazy Zeroed’ option, and press ‘Next’.
- Set Memory Size: at least 8 GB.
- Set CPU quantity: two or more if required.
- Configure Network adapter.



- Select ‘Datastore ISO file’ as a CD/DVD drive and select the ISO file of PowerManage



- Press ‘Next’ and ‘Finish’
- Launch the virtual machine and proceed with PowerManage installation.

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.

Changes in PowerManage 4.16

- Antivirus configuration in MMI
- Default Support Admin customization
- Refactored Mail server configuration. SMTP supports TLS
- Patch deprecation in favor of Incremental upgrade

Initial Setup

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

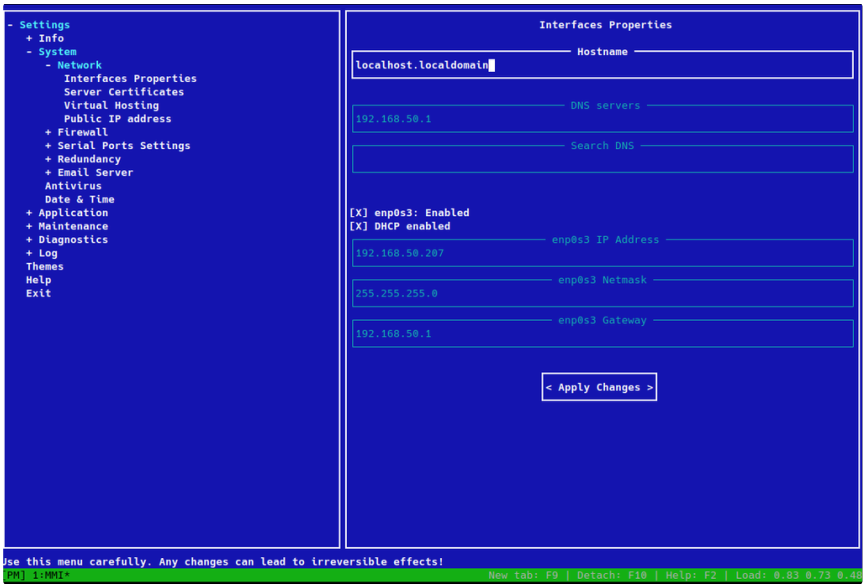
Configure Network

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

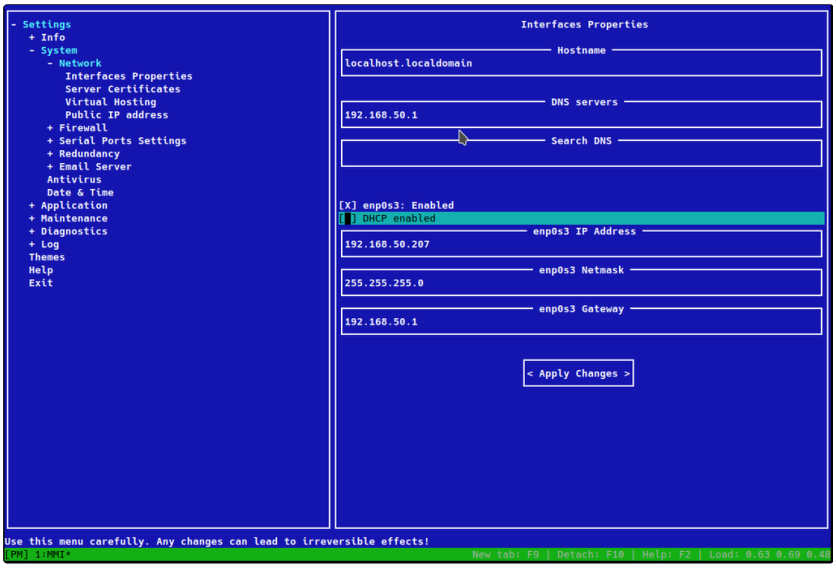
- In the MMI menu go to **System > Network > Interfaces Properties**
- Set your servers' Hostname
- Enable network interface **ethX on/off**

> **Note**: The 'ethX' is the example name of the interface. And 'X' in ethX is the example number of the interface. Network names also can be like 'enoX', 'ensX', 'enp0sX', etc.

- Configure the servers' network interface if the server obtains its IP address by DHCP enable **DHCP on/off** option and press **Apply Changes.**



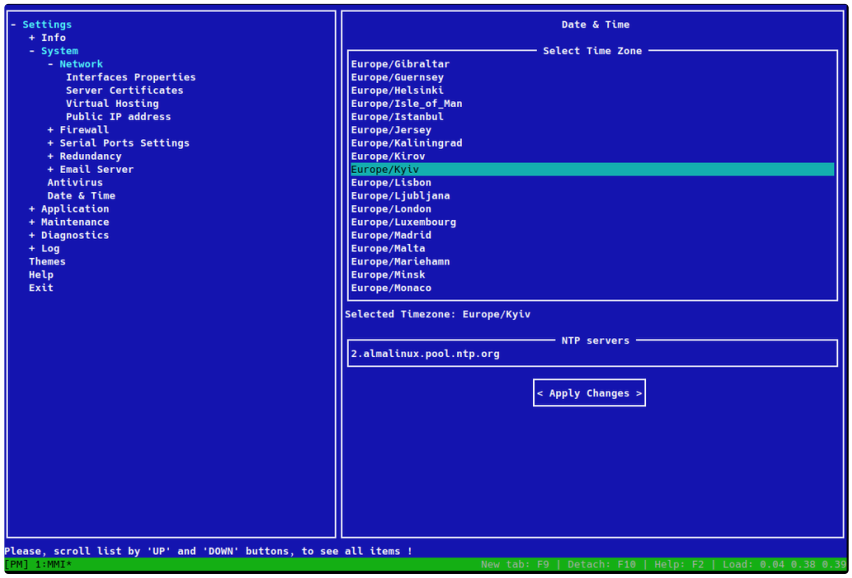
- In case you have to configure a static IP address for your server, disable **DHCP on/off** option, set **ethX IP address**, **ethX netmask**, **ethX gateway,** and press **Apply changes.**



Configure Time Synchronization

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

Enter the MMI menu, and go to **System** > **Date & Time**. Ensure that the correct time zone is selected, set **NTP servers** and press **Apply changes.**

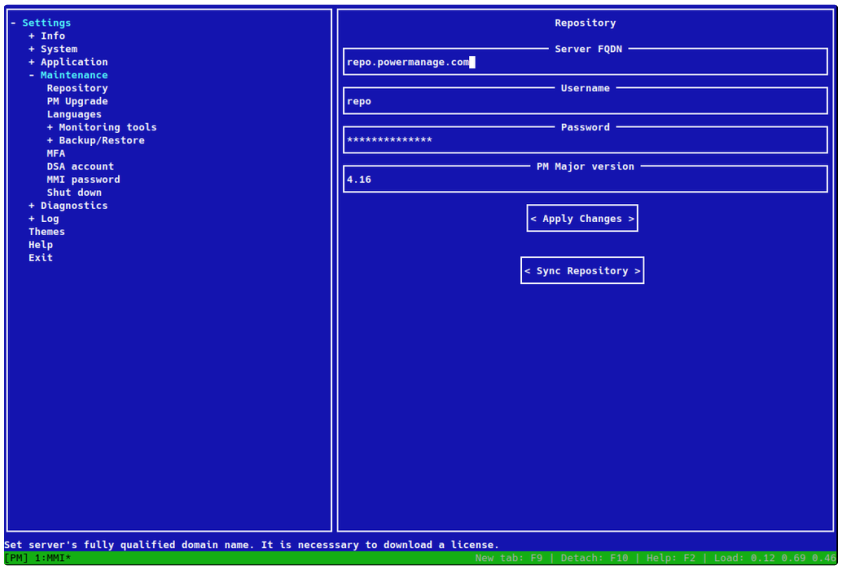


Configure Repository

> **Note:** If you are performing incremental upgrade or restoring from 4.12 to 4.16 - change repository after process finish. Please contact support to provide new credentials.

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. The repository for PowerManage 4.16 has an IP address **54.227.244.122** and a Fully Qualified Domain Name **repo.powermanage.com.**

- In the MMI menu go to **Maintenance > Repository** menu.
- Set your repository account user.
- Set your repository account password.
- Set the PM Major version as 4.16.
- Press **Apply Changes.**
- To synchronize with the repository, press **Sync Repository.**

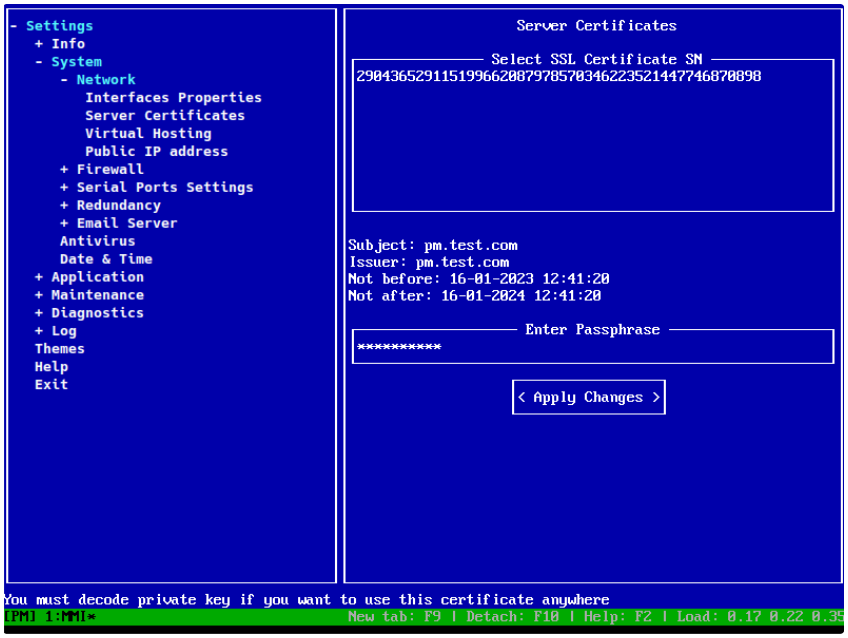


Configure SSL certificates

Before applying certificates, make sure your server is connected to the repository and SSL certificates are added and assigned to your Repo account. Also, make sure that your server is synchronized with the repository. Detailed instructions are in Appendix A.

To use HTTPS connections to the PowerManage Web Interface, and Web Console, it's required to add and apply SSL certificates to the server.

- Go to the 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**



After that, the decrypted SSL certificate should appear in the **Virtual hosting** menu. The virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server. To access a specific service use the following command in your browser: https://<server URL>:<port number>

- In the MMI menu go to **System > Network > Virtual Hosting** menu
- Select a service from the following list:
  - LTE upgrade host - Communication between the LTE Modem & Server during LTE Modem upgrading process
  - PowerNet host - Communication between Plink & Server
  - Web Interface and Mobile Interactive - Resolve/Maintenance Web interface and Control and monitor panel through the mobile app
  - Web MMI console - MMI interface through a web browser

> **Note**: The field Hostname is required for LTE upgrade host and should correspond to the public PowerManage DNS name

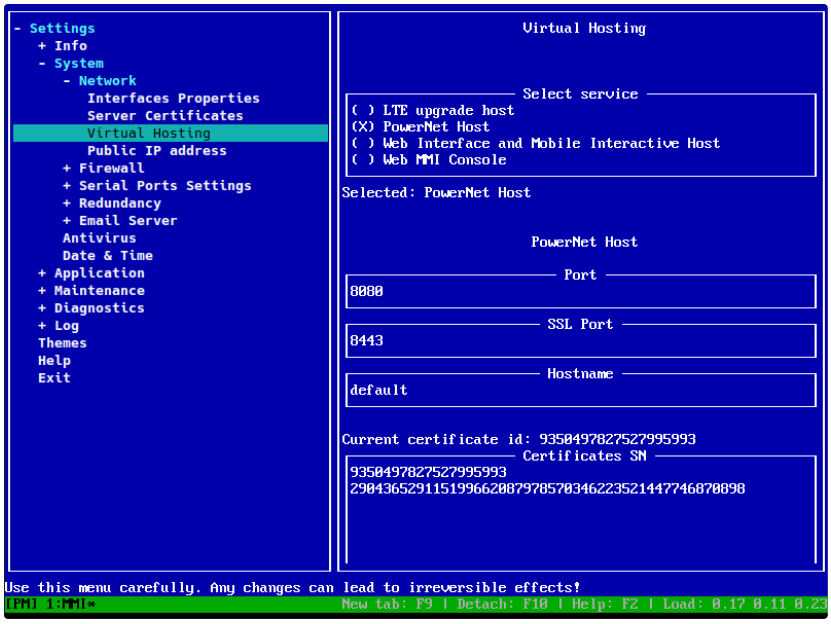
- Set Ports number [SSL for encrypted connection and not SSL Port for unencrypted]

> **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**



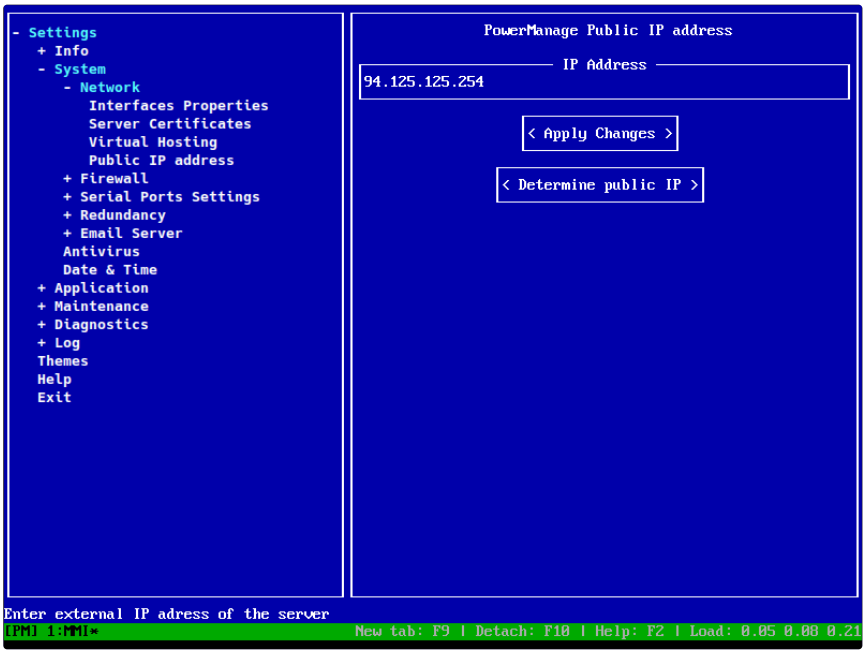
Configure Public IP address

Public IP address must be defined as its real public IP address, it can be the public IP address of the Firewall on which the panels are configured.

> ⚠ **IMPORTANT**: Public IP address is an essential option for the correct displaying of KA of the panels, for the SMS wakeup feature.

- In the MMI menu go to **System > Network > Public IP address**
- **Option 1**: Set **IP address** manually and press **Apply Changes**
- **Option 2**: Press **Determinate public IP** to detect the IP address automatically and press **Apply Changes**

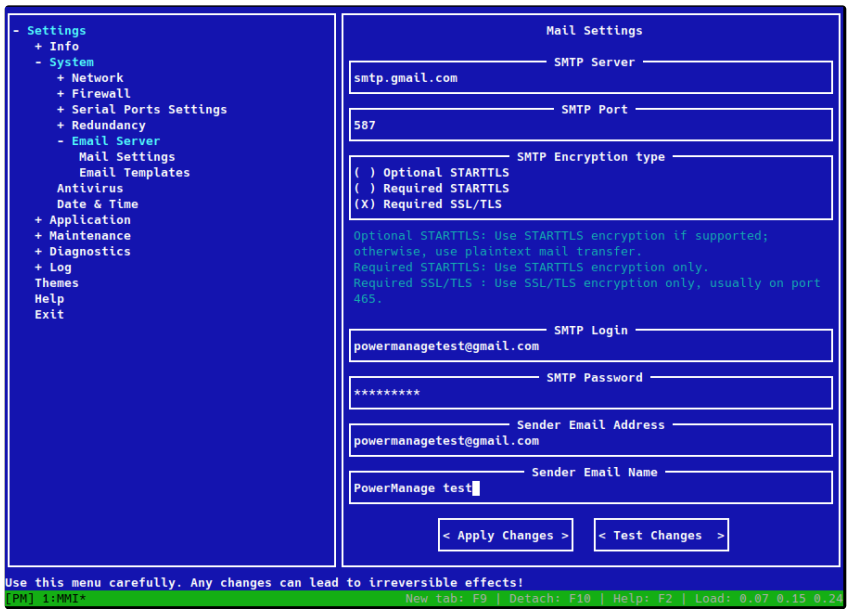
> ℹ **Note**: **Determinate public IP** button automatically detects the IP address and fills in the IP address field, be sure to check the IP address after it is determined.



Configure Mail server

PowerManage uses Postfix email relay for 2FA, end-user email notifications, MFA, and admin notifications.

- In the MMI menu go to the **System > Mail server**
- Set **SMTP server**.
- Set **SMTP port**.
- Select **SMTP Encryption type**.
- Set **SMTP Login** and **SMTP Password**.
- Set **Sender Email Address** and **Sender Email Name**.
- Press **Apply Changes**



To test email settings press **Test Changes**. Fill in the email address and press **Ok**.

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.

Restoring a backup from version 4.12.46 to version 4.16

> ⚠ **IMPORTANT**: Restoring a backup to 4.16 must be performed from version 4.12.46.1 or higher.
>
> Change repository after restore. Please contact support to provide new credentials.
>
> After restoring a backup all users should clear the cache in their web browser

- Make a backup of the server 4.12.46.1 or higher.
  (For more information, see Backing up files to the FTP server or Backing up files to a USB drive.)
- Restore the backup on a new clean PM server version 4.16.
  (For more information see Restoring data from an FTP server or Restoring data from a USB flash drive.)
- Apply all available patches if any. For more information, see **Incremental upgrade**.
- Configure **Mail server** and select the appropriate email template in **Email Templates** menu. If you do not have customized templates for 4.16, use the default template.

Configure ITv2 Settings

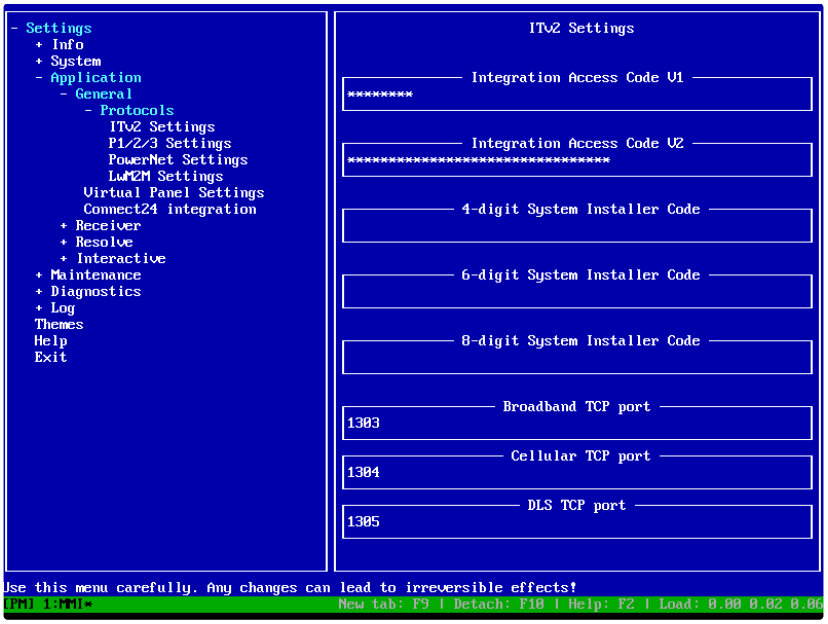
ITv2 protocol is intended for one-to-one communications between an integration module and a third-party integration server or device. The two sides of communication are peer-to-peer relationships; both sides can initiate a command/response packet exchange.

> **Note**: The PowerManage server supports only one simultaneous ITv2 session for NEO and PSP panels.

The old Neo panels have 8 characters of an integration code that must be identical to the **Integration Access Code V1** field (see the below screenshot). The newer Neo panels and PSP (Power Series Pro) panels communicate with the PowerManage server via ITv2 protocol that is encrypted with **Integration Access Code V2**.

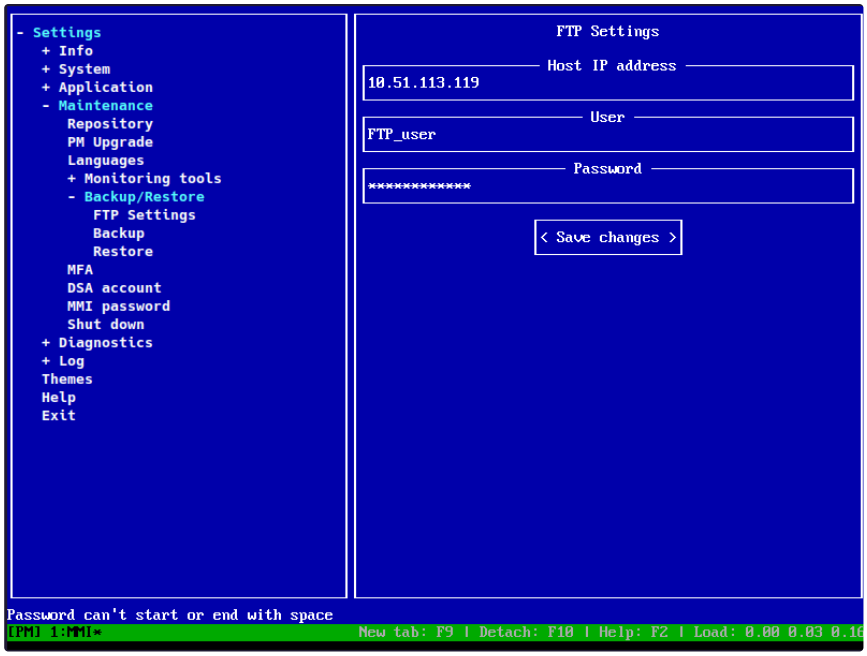
The newer Neo panels and PSP panels have 32 character integration code with the default value of 12345678123456781234567812345678 and the server automatically changes it to a unique Integration Access Code during the panel activation.

- In the MMI menu go to **System > Application > General > Protocols > ITv2 Settings**
- In **Integration Access Code V2** set your access code



Backup to FTP server

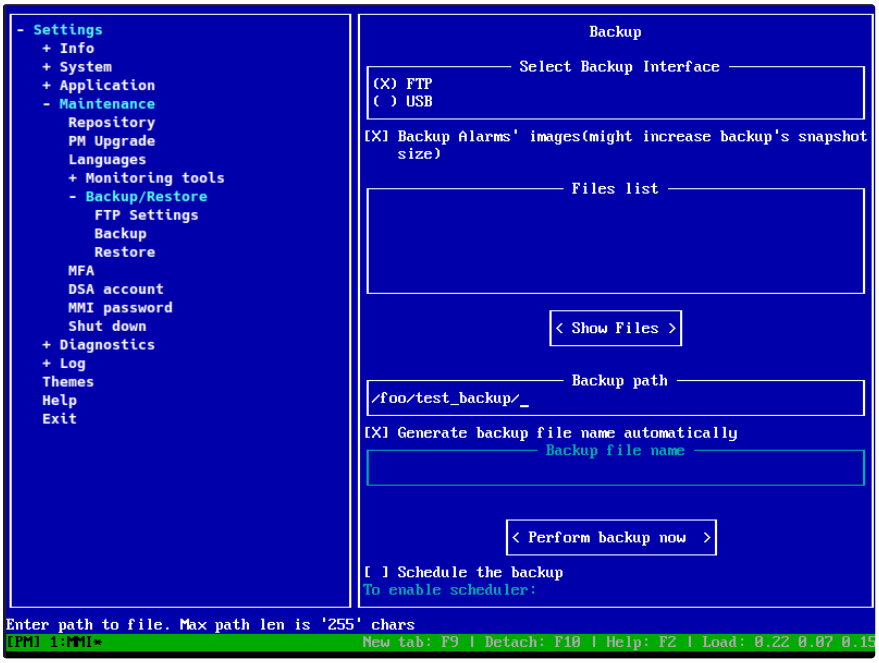
- In the MMI menu go to **Maintenance > Backup/Restore > FTP Settings** menu
- Set **Host IP address** of your server, **User**, **Password** and press **Save changes**



- Go to **Maintenance > Backup/Restore > Backup** menu.
- Set the backup method to **FTP.**
- You can check the **Backup Alarms images** checkbox to include alarm images in the backup file.

> **Note:** We recommend performing a backup without images if the number of images is more than 1.5 million, it may take 2 hours to perform a backup. And in this case, some information will be outdated.

- In **Backup Path** set the absolute path to the directory where the backup will be saved.
- You can uncheck **Generate backup file name automatically** and set the backup name in the **Backup file name.**
- You can use the **Show Files** button to list backup files located in the directory.
- Press **Perform backup now.**

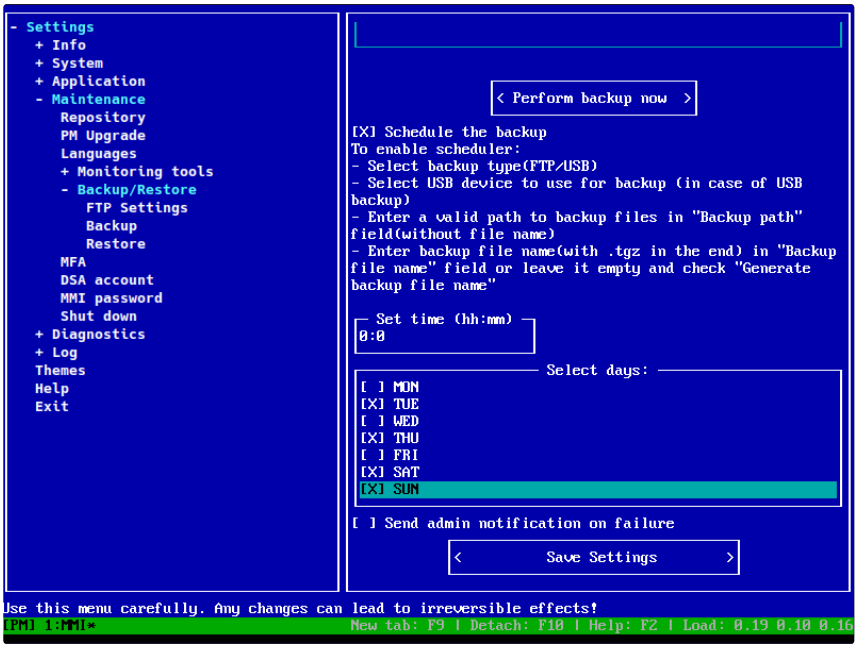


Backup to FTP server by schedule

- Go to **Maintenance > Backup/Restore > Backup** menu.
- Set a backup method to **FTP.**
- You can check the **Backup Alarms images** checkbox to include alarm images in the backup file.

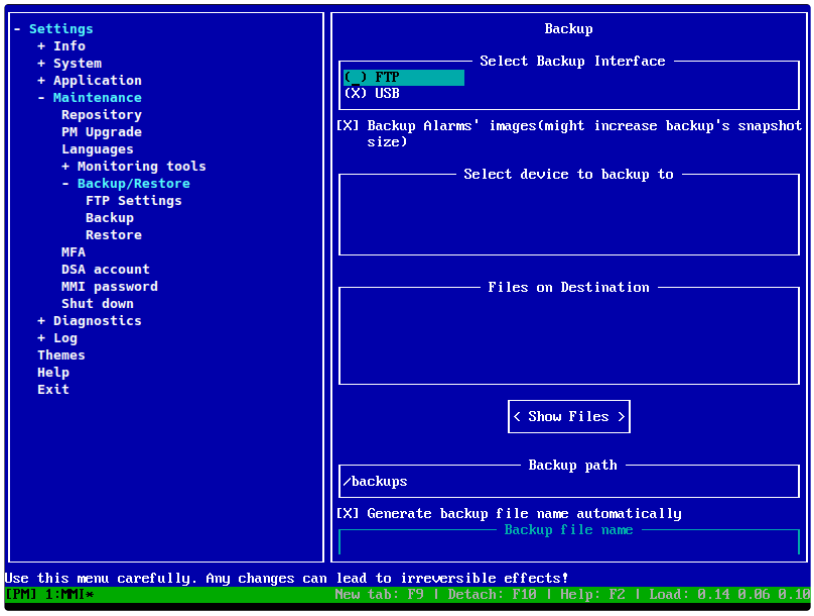
> **Note:** We recommend performing a backup without images if the number of images is more than 1.5 million, it may take 2 hours to perform a backup. And in this case, some information will be outdated.

- In **Backup Path** set the absolute path to the directory where the backup will be saved.
- You can uncheck **Generate backup file name automatically** and set the backup name in the **Backup file name.**
- Set the **Schedule the backup** checkbox.
- Set the time to perform the backup.
- Select the weekdays on which to perform the backup.
- Press **Save Schedule.**



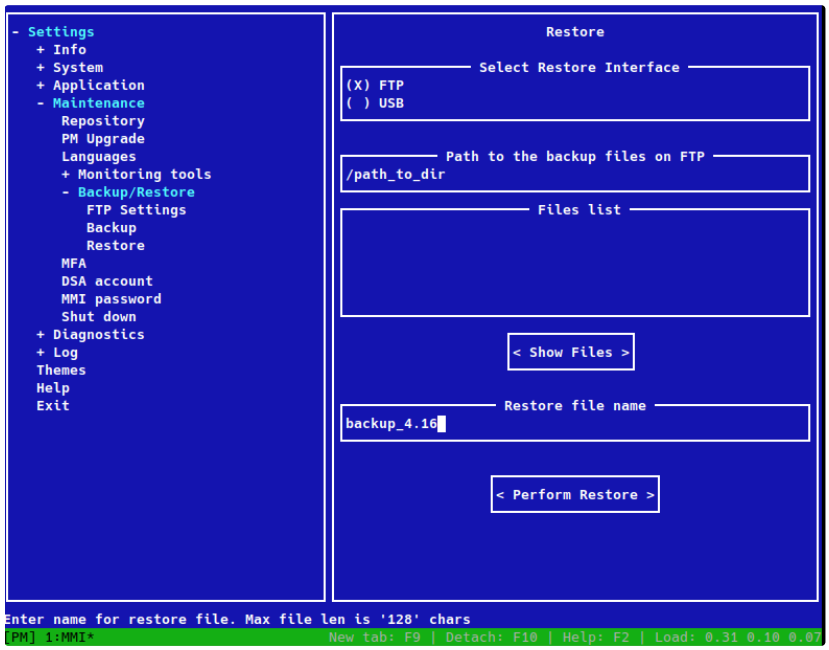
Backup to USB

- Connect the USB drive to your server. The USB drive must have at least 1 partition formatted as EXT3, EXT4, FAT32
- Go to **Maintenance > Backup/Restore > Backup** menu
- Set a backup method to **USB.** The system will automatically show all available USB devices that can be used for backups.
- You can check the **Backup Alarms images** checkbox to include alarms images to the backup file
- Select the connected USB drive
- In **Backup Path** set the absolute path to the directory where the backup will be saved
- You can uncheck **Generate backup file name automatically** and set the backup name in the **Backup file name**
- You can use the **Show Files** button to list backup files located in the directory
- Press **Perform Backup**



Restore from FTP server

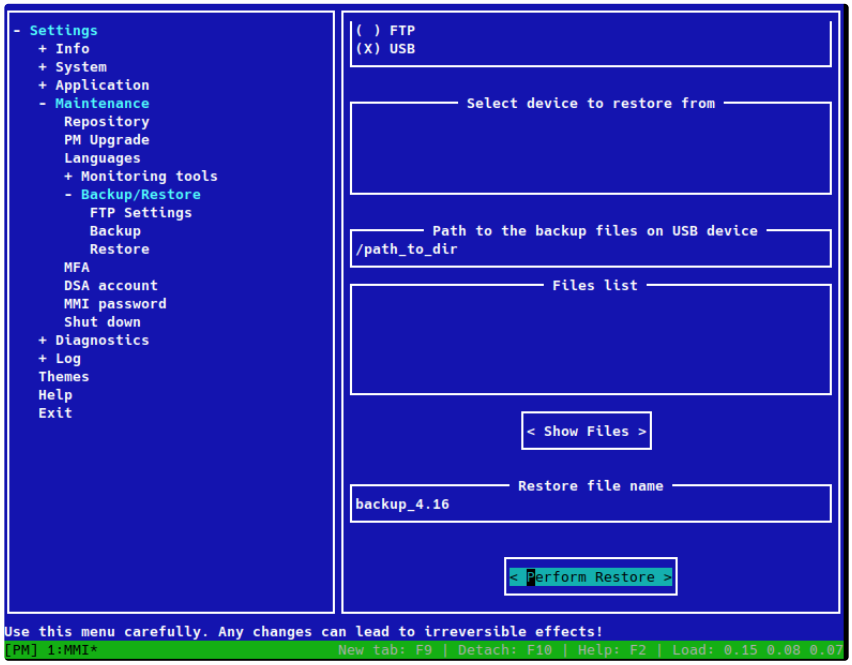
- In the MMI menu go to **Maintenance > Backup/Restore > FTP Settings** menu
- Set **Host IP address** of your server, **User**, **Password** and press **Save changes**
- Go to **Maintenance > Backup/Restore > Restore** menu
- Set the restore method to **FTP**
- In **Restore Source Path** set an absolute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



Restore from USB

- Connect the USB drive to your server.

- In the MMI menu go to **Maintenance > Backup/Restore > Restore** menu.
- Set the restore method to **USB.** The system will automatically show all available USB devices that are connected to a server.
- Select the connected USB drive in **Select device to restore from**.
- In **Path to the backup file on the USB device** set the backup absolute path.
- Press the **List dir** button to list backup files located in the directory.
- In the **Files list** select the necessary backup file and press the **Enter** keyboard button.
- Press **Start restore.**



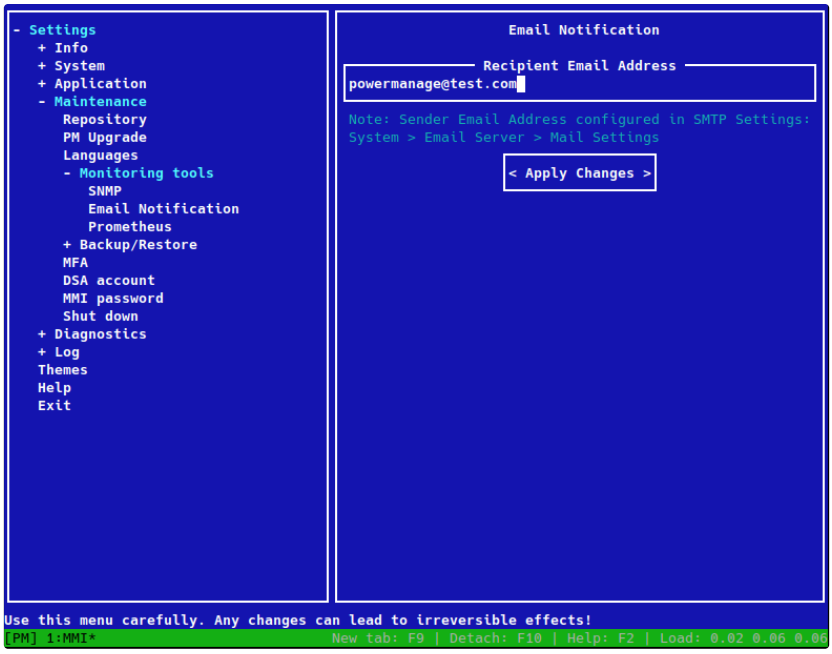
Setup Email notifications

Email notification is a feature for monitoring the following things:

- SSL certificate expiration
- Monitoring redundancy status
- License expiration
- License downloading problems
- Automatic backup fail notification

> **Note**: Configure **Mail settings** to allow the server to send emails. In the MMI menu go to **System > Email server > Mail settings**.

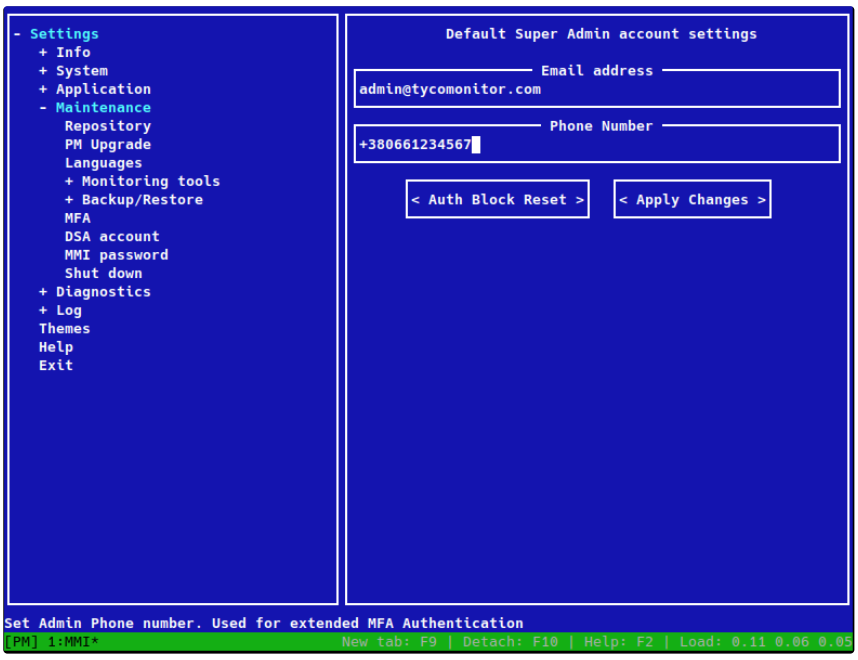
- In the MMI menu go to **Maintenance > Monitoring tools > Email notifications** menu setup the recipient email address.



Default Super Admin account settings setup

Default Super Admin user account email and phone be altered in the DSA account.

If the **Default Super Admin** user fails to log in three times consecutively, the login will be blocked for a duration of 5 minutes. To reset authentication attempts, you can utilize **Auth Block Reset**.



Admin Multi-factor Authentication

Notes:

Default Super Admin phone is being set in new **DSA Account** frame.

You can disable MFA by pressing the **Disable MFA** button.

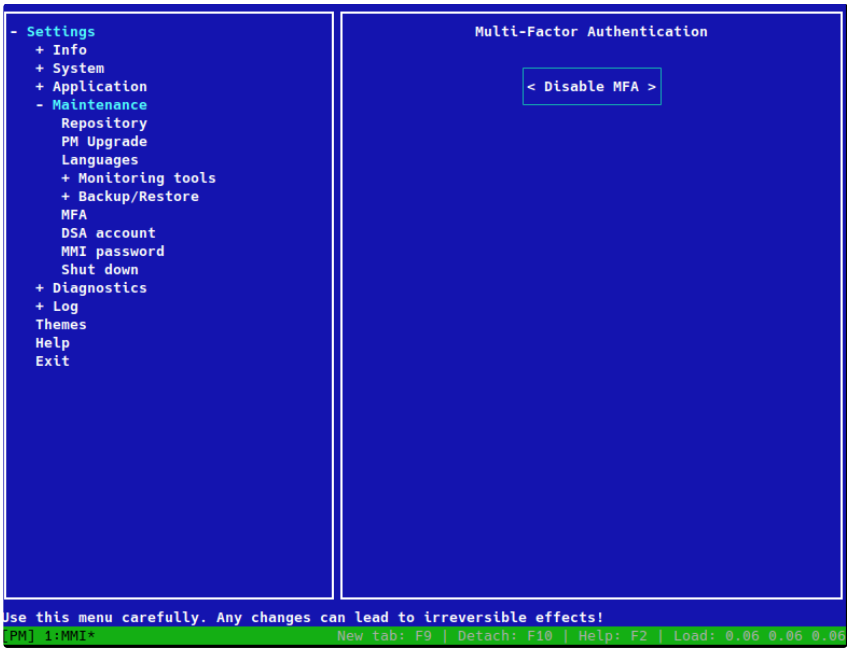
Configure an SMS broker to allow the server to send SMS and Enable MFA in the WEB GUI.

Multi-factor authentication (MFA) can be applied for **Default Super Admin** user.
MFA STATUS is enabled (default status is Disabled) the GUI login is composed of two stages:

- Entering the user's email + password.
- Entering OTP (One Time Password) code that is sent from the PowerManage server to the operator's phone via SMS.

In this case, we are setting up a backup mobile number for **Default Super Admin**. To set up MFA for specific users you can go to menu **System** > **Users** > ***specific user*** > **Phone number**

- In the MMI menu go to **Maintenance > Admin MFA Phone number** set number for Multi-factor authentication
- Press **Apply Changes**

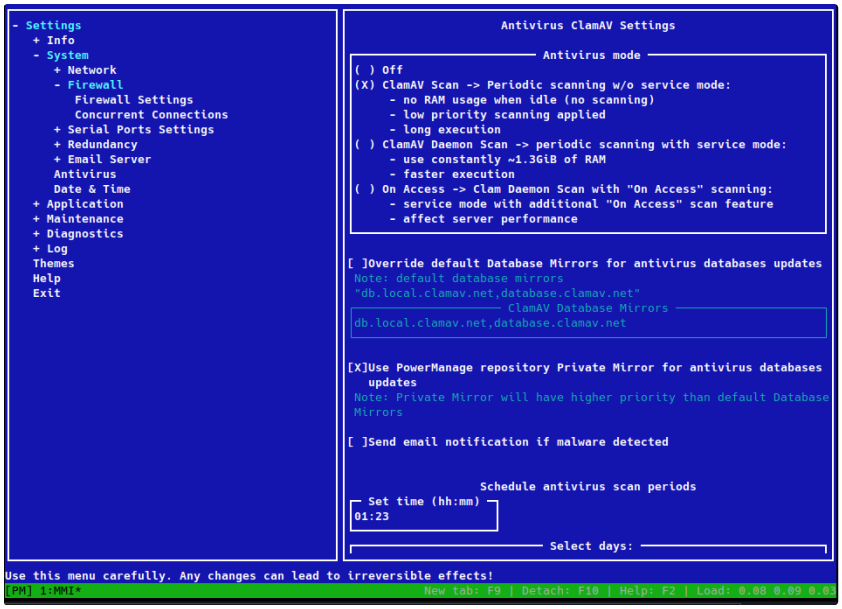


Configure Antivirus

In 4.16 we introduce ClamAV for PowerManage 4.16. ClamAV® is an open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

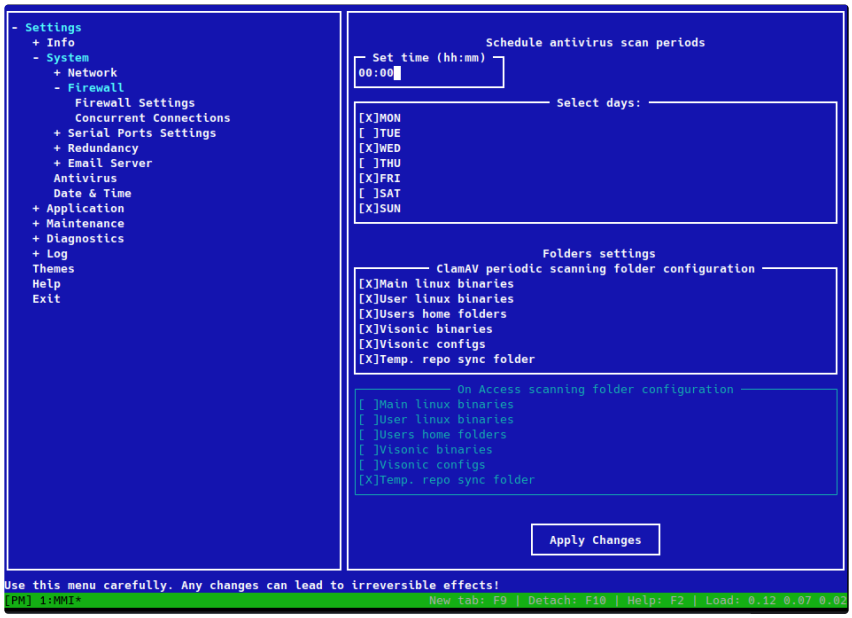
> ClamAV gets the Database mirror from the PowerManage repository by default. Therefore, you must configure the repository before setting up the antivirus.

- In the MMI menu go to **System > Antivirus** menu.
- There are multiple options for periodic antivirus scans:
  - Periodic scan without service mode - scan runs when scheduled and does not use any resources when idle. Execution takes longer.
  - Periodic scan with service mode - scan runs when scheduled and executes a bit faster but uses RAM when idle.
  - On Access scan. In addition to the previous one, the scan runs in "On Access" mode - scans files for viruses in real time when they are opened, saved, and run. Affects server performance.



- Enable “Send notifications if malware detected” (Optional)
- Set time of scheduled scan
- Select days for scan
- Select folders for periodic scan (by schedule time)

  Select folders for “On Access” scan (available if “On Access” mode enabled)
- Press **Apply Changes**



Add an already enrolled NEO/PSP panel without removing it

> **Note**: This is only relevant for panels that are using Type 2 encryption. To add a previously enrolled panel (e.g. after factory default reset) a user must disable the encryption for the panel.

- Set the same panel Integration Access Code as it is set in **Integration Access Code V2**.

> **Note**: **Integration Access Code V2** is 12345678123456781234567812345678 by default.

- The panel will require new activation if it comes with a different installer code. To avoid it, the installer code should be set the same as before.
- In the WEB GUI go to panel > ACTIONS > BBA/GPRS Encryption > disable toggle.

Note: The panel must be in a disconnected state.

- Initialize the panel connection to the PowerManage server. E.g. power up the panel.

After the actions, the panel should pass the ITv2 encryption and become online without removing from the server.

Incremental upgrade

The incremental upgrade is a well-known way of distributing software packages to the end user. It is usually implemented using small packages, where one package contains one single tool, accessing through the internet to a remote software repository.

The idea of implementing an incremental upgrade is to upgrade major and minor PowerManage versions without restoring from a backup of the previous version.

IMPORTANT: The upgrade to 4.16.34 must be performed from 4.12.46.1 or higher.

Before you start the upgrade, you need to contact technical support to get new credentials to access the **repo.powermanage.com** repository.

The **Secure Boot** option must be disabled on PowerManage 4.12.46.1 (or higher) before starting the installation or incremental upgrade. If the option was enabled during the installation, you should contact the Support team.

Notes:

Make a backup of the server before making the incremental upgrade.

Pictures related to receiving events are lost when events are received during the incremental upgrade.

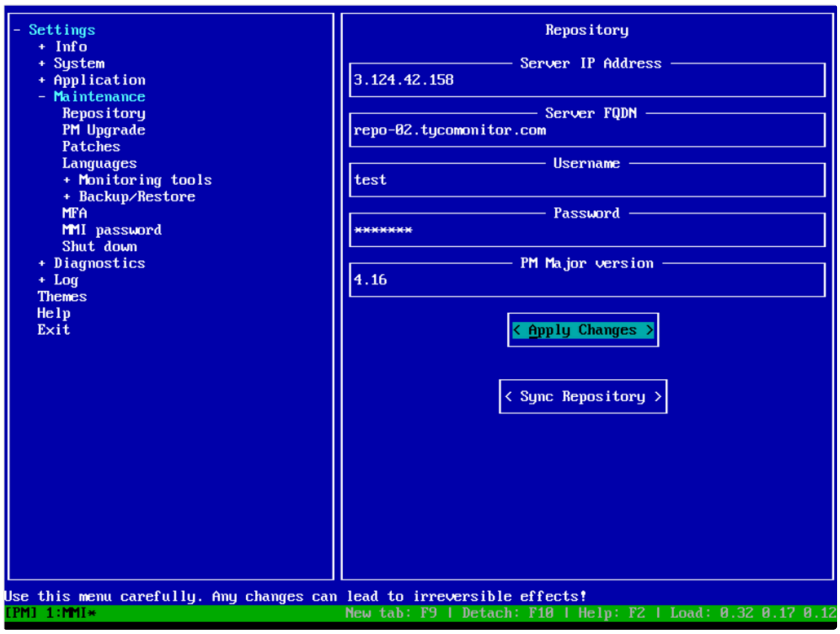
After the incremental upgrade, all users should clear the cache in their web browsers.

PowerManage server must be rebooted after an incremental upgrade from a major server version to a higher major server version (e.g., upgrade from 4.12.X to 4.16.X).

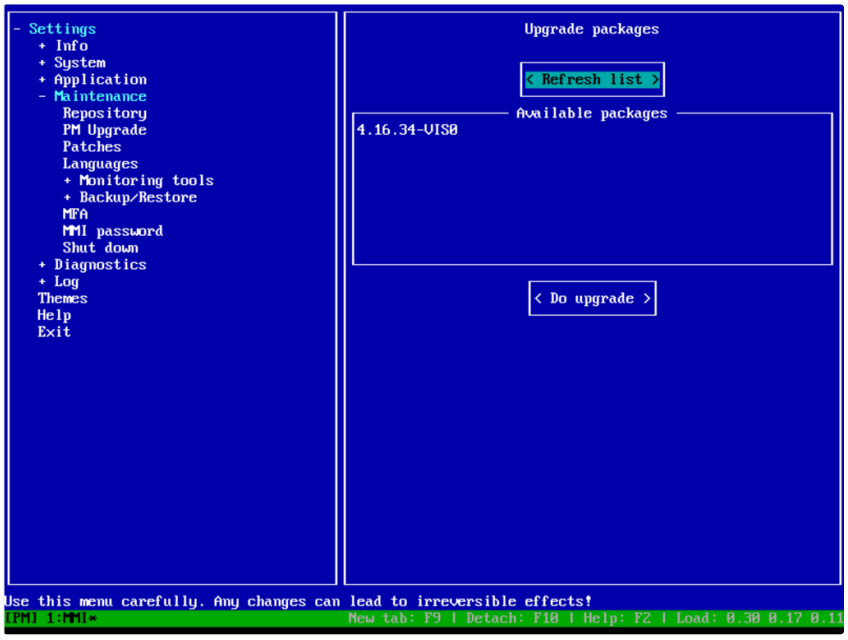
Each Redundancy Node must be standalone in the case of the incremental upgrade. After the upgrade and rebooting, Redundancy can be configured again. For details on how to configure, see Redundancy configuration.

After the upgrade, configure **Mail server** and select the appropriate email template in **Email Templates** menu. If you do not have customized templates for 4.16, use the **default** template.

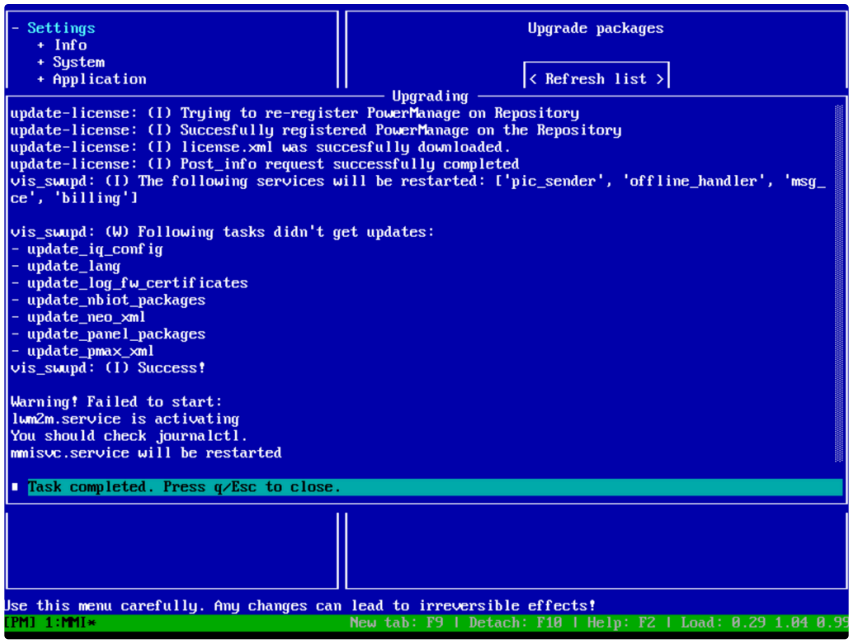
- In the MMI menu go to **Settings** > **Maintenance** > **Repository**
- Set 4.16 in **PM Major version**
- Press **Apply Changes**



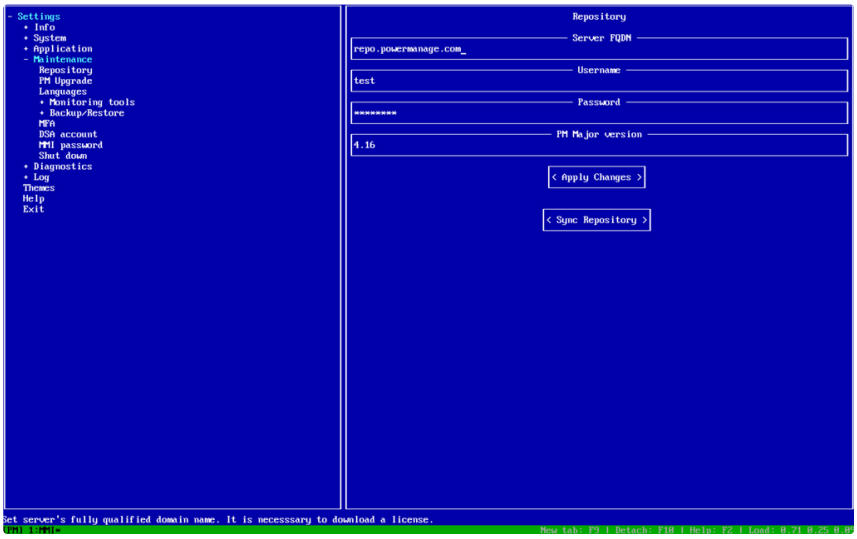
- In the MMI menu go to **Settings** > **Maintenance** > **PM Upgrade**
- Press **Refresh list**
- After the message “Task completed” select package from **Available Packages**



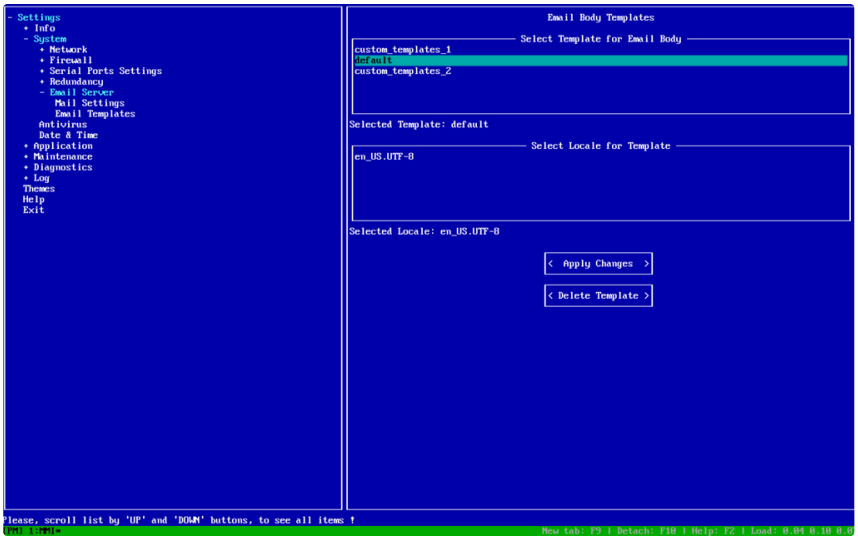
- Read release notes and press ESC
- Press **Do upgrade**



- After the upgrade is done set the new credentials in **Repository** settings
- Go to **Settings** > **Maintenance** > **Repository**
- **Repository** menu is changed and the **Server FQDN** is changed to **repo.powermanage.com.**



- Make sure that the Repository account is correct and the PowerManage server can connect and sync with the new repository.
- Configure **Mail server** and select the appropriate email template in **Email Templates** menu. If you do not have customized templates for 4.16, use the **default** templates.


- Settings
+ Info
- System
+ Network
+ Firewall
+ Serial Ports Settings
+ Redundancy
- Email Server
Mail Settings
Email Templates
Antivirus
Date & Time
+ Application
+ Maintenance
+ Diagnostics
+ Log
Themes
Help
Exit
Email Body Templates
Select Template for Email Body
custom_templates_1
default
custom_templates_2
Selected Template: default
Select Locale for Template
en_US.UTF-8
Selected Locale: en_US.UTF-8
< Apply Changes >
< Delete Template >
Please, scroll list by 'UP' and 'DOWN' buttons, to see all items !
[TM] 1:TM*
New tab: F9 | Detach: F10 | Help: F2 | Load: 0.04 0.10 0.0

Firewall

The internal firewall in PowerManage is an out-of-the-box functionality that is implemented over the Iptables Linux utility which is a tool to configure the 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 the PowerManage firewall is to provide a handy tool that allows configuring secure network access policies and limiting simultaneous connections number to avoid service overload.

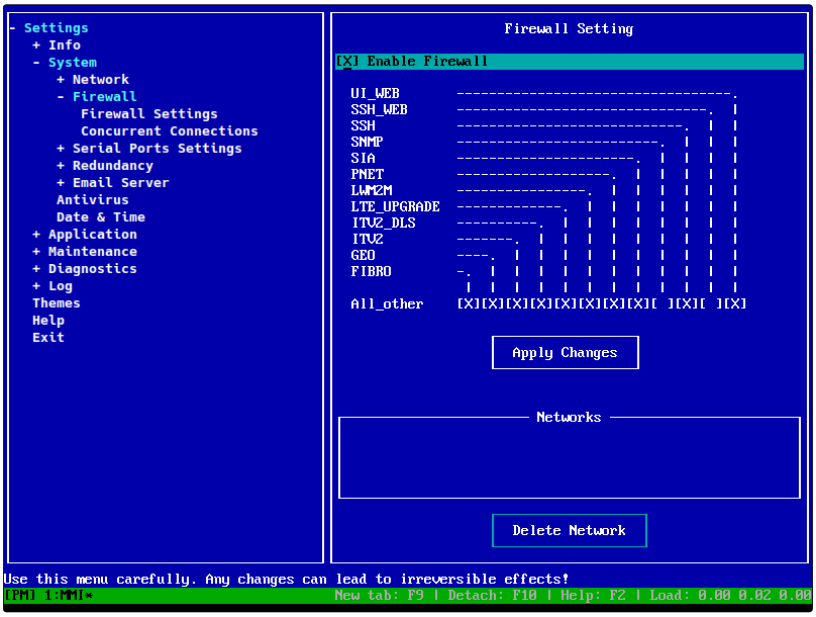
The key point is that the internal firewall is considered a supplementary measure to an external firewall. It is still advisable to use an external firewall on top of PowerManage servers. It should provide more reliable stability and avoid performance issues.

Restriction of sources for incoming connections

The 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 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 customers.

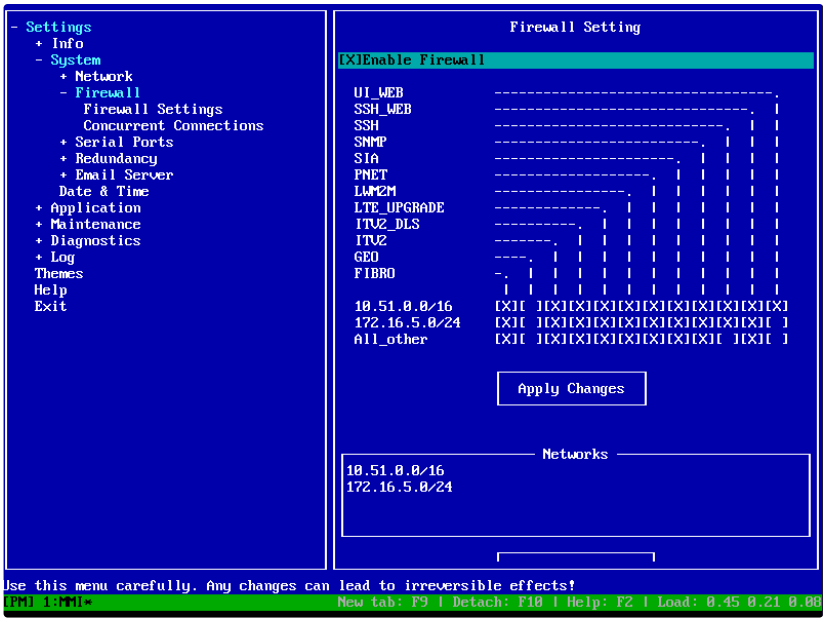
Access can be allowed or denied for services represented by a list of profiles in MMI. There is an option to add some networks and manage access from them to PowerManage services separately.

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



Let's consider the following example:

It is seen that all profiles except “GEO”, “HTTP/HTTPS”, and “SSH” are enabled for “All_hosts”. It means that access to the corresponding services is open from any network. “GEO” profile is disabled, which 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: 10.51.0.0/16 and 172.16.5.0/24. HTTP/HTTPS (WEB access) is allowed from the 10.51.0.0/16 network only.



Restriction on the number of simultaneous connections

There is a possibility to restrict the number of simultaneous connections to a list of services represented by the corresponding profiles in MMI. By default, it is not limited (corresponds to the “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 rejection of some HTTP queries and thus cause malfunction of established sessions.

Redundancy configuration

The redundancy feature works in two modes: Geo and Local.

Notes:

Pictures and reports received within five minutes might be lost on the new master node in case of switching the secondary node to master after failover.

Reconfiguring the redundancy feature on PowerManage servers leads to a restart of services. Some services may not work during the restart, as a result of which some panels may become disabled for some time.

Disassemble the redundancy in case some node or all nodes need to be shut down.

Email notification should be configured on the master server to inform about failure (Settings > Maintenance > Monitoring Tools > Email notification).

After reconfiguring master or slave nodes, as well as after switching off master or slave nodes, all users should clear the cache in their web browser.

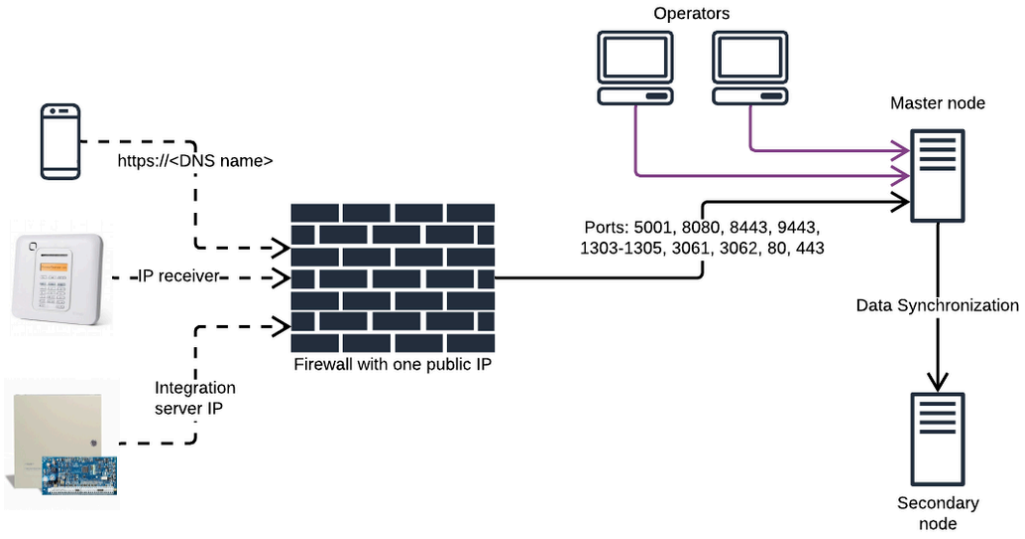
In case there is a backup of data that is going to be restored on a new redundant installation, you must first perform the restore to the server that is going to be used as Master, and only then you can configure the redundancy. You do not need to perform the restore to the secondary node servers.

For the redundancy setup, we recommend using an uninterruptible power supply (UPS) for the master and all secondary nodes to prevent corruption of the database on the nodes in case of an unexpected AC power failure. In case the AC power will soon be gone and the nodes without UPS, we recommend shutting down the server. Also if the AC current is already gone and the UPS will soon run out, we recommend shutting down the server.

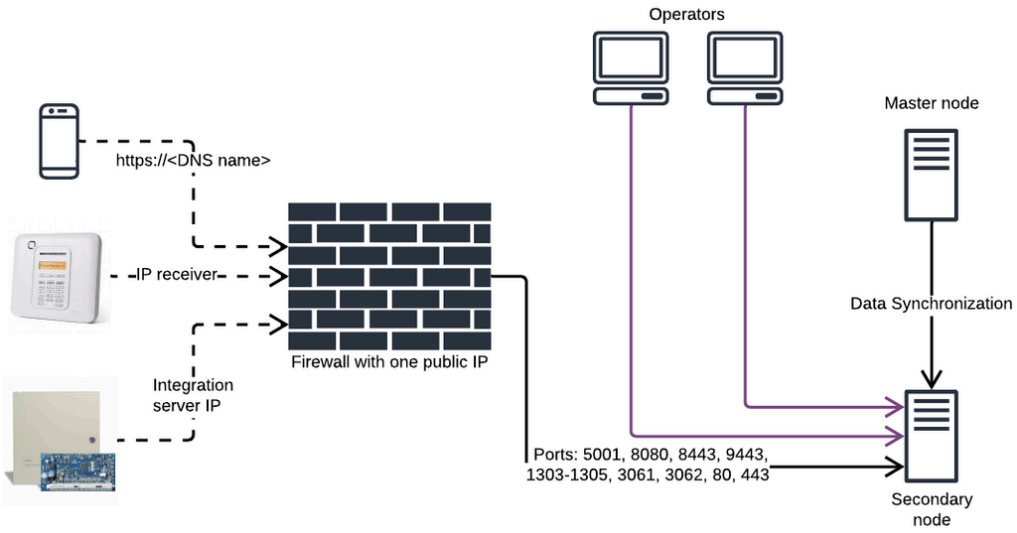
Two-node system. Local mode

Local redundancy mode was designed for clients who don't want to use two-channel communication between security panels and PM servers but do want to have redundancy for their bare metal PM servers.

In Local mode, all security panels access only the Master PM server via one public IP address and can't access the Secondary node at all.



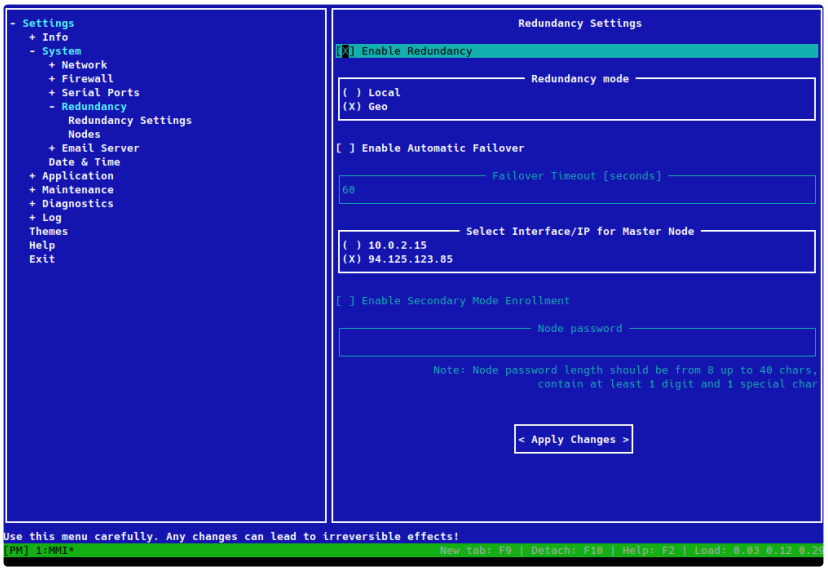
In Local redundancy, the option **Automatic switchover feature is not available**. If the Master server becomes not available or part of its services are not available, clients should manually disable redundancy on the Secondary node and then **reconfigure their Firewall** to redirect all traffic to the secondary node.



Disable redundancy on the Secondary node

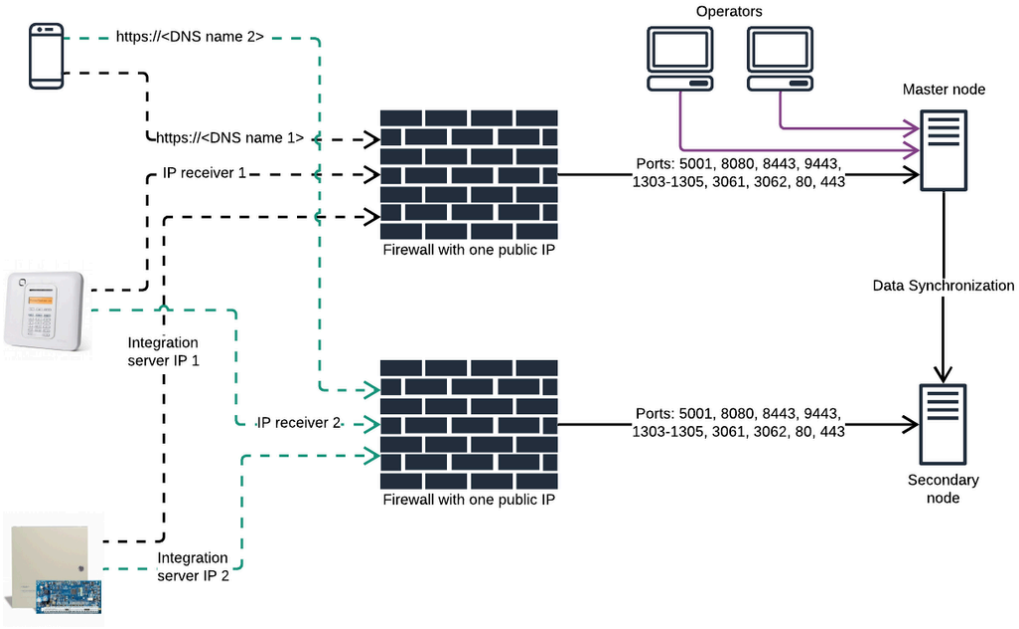
> **IMPORTANT**: Master and Secondary must have the same **Public IP address** and it must correspond to the public IP address of their Firewall. For more information, see Configure Public IP address.
>
> In Local mode the client must be sure that both PM servers have the same **Integration Access Code V2**. For more information, see Configure ITv2 Settings. It is important because after the Secondary node becomes a Standalone or Master server and the client reconfigures their Firewall to redirect all the traffic to this server, all DSC panels will start to communicate with this server using **Integration Access Code V2**. from the old Master node. Otherwise the DSC panels will not be able to connect to the new Master node.

- Ensure the secondary node has the same **public IP address** as the external firewall. In the navigation tree, select **Settings**, select **System**, then select **Network**.
- In the **IP Address**, enter the same IP address as the firewall IP.
- In the navigation tree, select **Settings** and select **System**.
- From **System**, select **Redundancy**, then select **Redundancy Settings**.
- Disable **Enable Redundancy**.



Two-node system. Geo mode

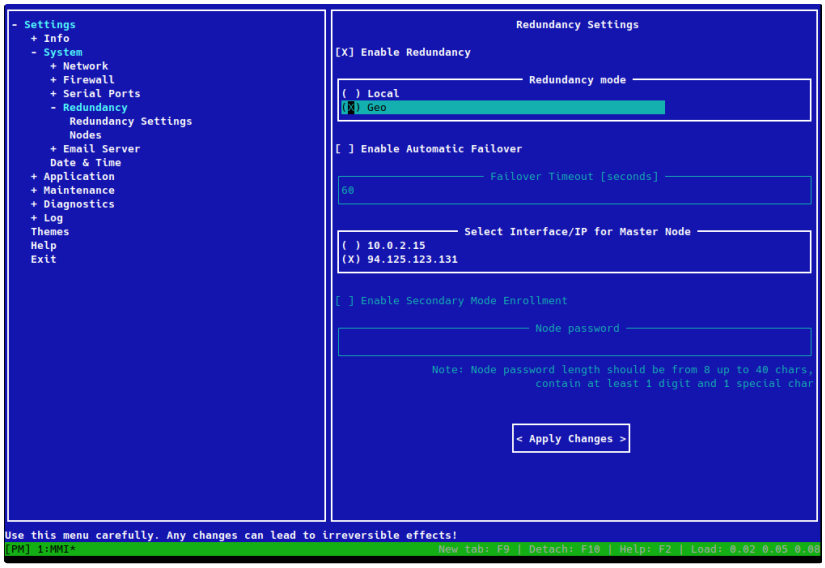
Geo redundancy mode was designed to get maximum availability of the services by receiving events on both redundancy nodes. In Geo mode security panels communicate to both redundancy nodes.



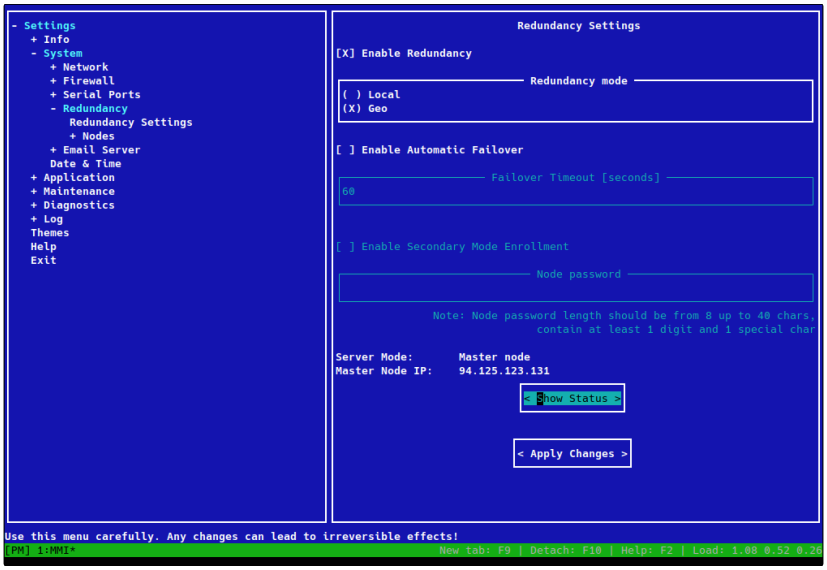
In geo-redundancy mode **is available Automatic switchover feature**. If a Master server becomes not available or part of its services are not available, the Secondary node automatically becomes Master and starts operating as a normal Master node. Clients **should not reconfigure their Firewalls** to redirect all traffic to the secondary node. All panels just continue working with the new Master node.

> ⚠ **IMPORTANT**: Master and Secondary must have different **Public IP address**. Both PM servers must be defined as its real public IP address, it should be the public IP address of its Firewall. For more information, see Configure Public IP address.
>
> In Redundancy Secondary 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, should be avoided. Otherwise, it won't be possible to activate the panel.

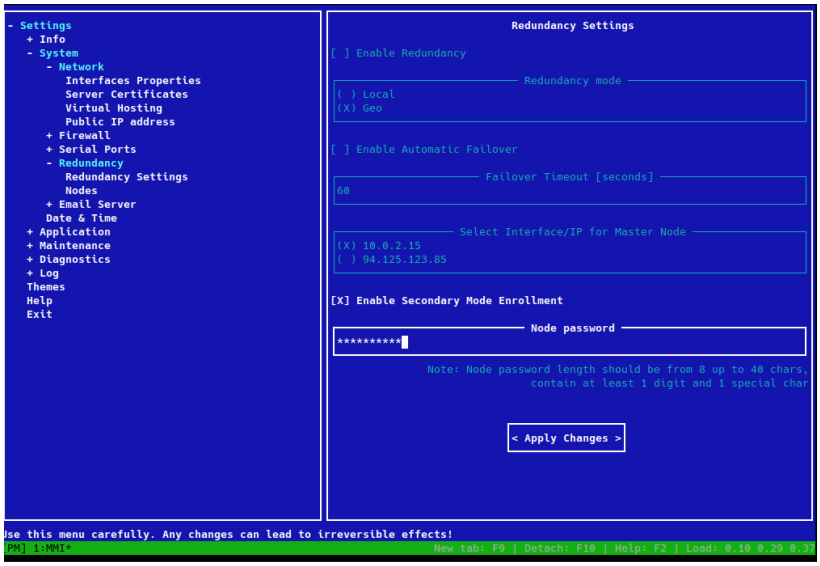
- Configure Central Stations for Master and Secondary.
- Enter the MMI menu on the Master.
- In **System** > **Redundancy** > **Redundancy Settings** set **Enable Redundancy** option.



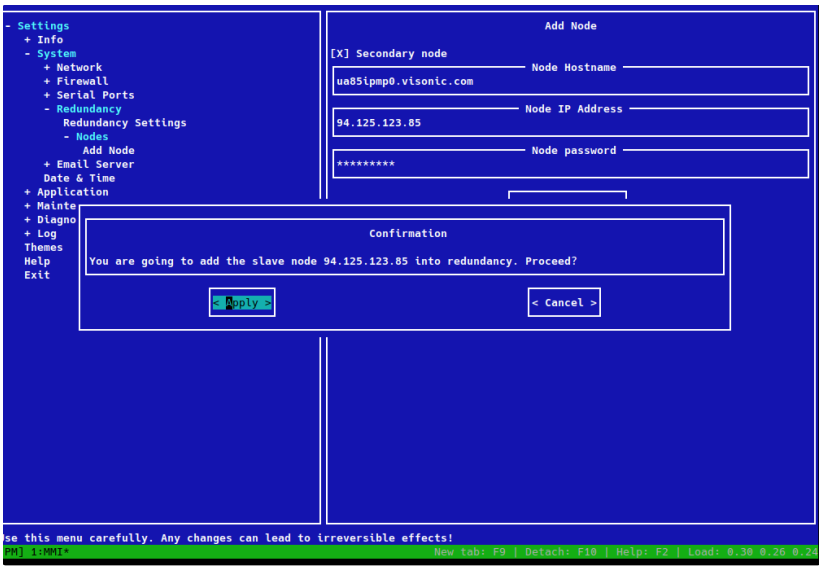
- Press **Apply Changes** button. In a dialog, box press **Apply** again.
- Wait until redundancy is enabled.
- Once redundancy is enabled, you will see the current node mode and Masters' IP. To view redundancy status and enrolled Secondaries, press the **Show status** button.



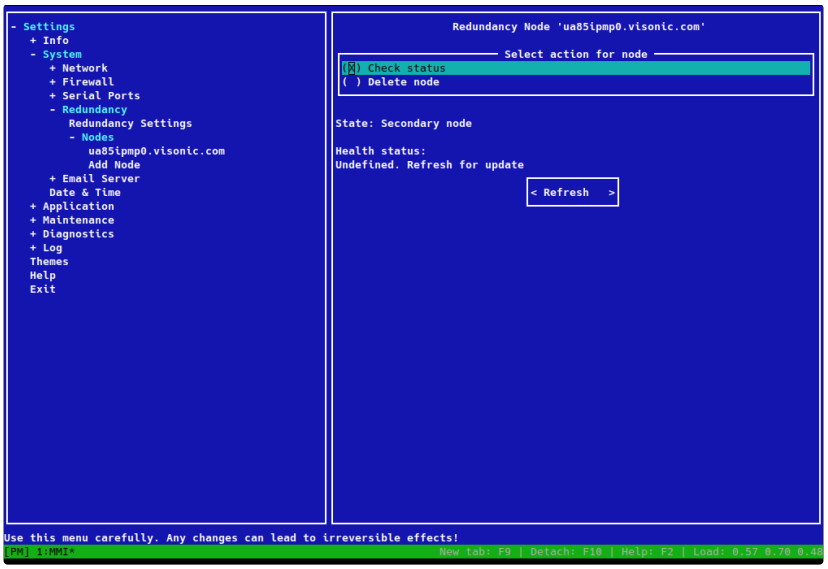
- Enter the MMI menu on the Secondary.
- Before adding Secondary, enable NTP time synchronization on Secondary and Master: in MMI **System > Date & Time** enable **Automatic Date and Time [NTP]** option.
- In **System** > **Redundancy** > **Redundancy Settings** set **Enable Secondary Mode Enrollment** option (otherwise in case the time difference between Master and Secondary is greater than 10 seconds, redundancy setup will fail).
- Enter **Node password**. Node password length should be from 8 up to 40 chars, contain at least 1 digit and 1 special char.



- Press **Apply Changes** button. In a dialog window, after the option is enabled, press **ESC.**
- In the Master's MMI menu go to **System** > **Redundancy** > **Nodes** > **Add Node.**
- In **Node Hostname** set the Secondary node hostname.
- In **Node IP Address** set the Secondary node IP address.
- In **Node Password** set the password that was configured on the secondary node.



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

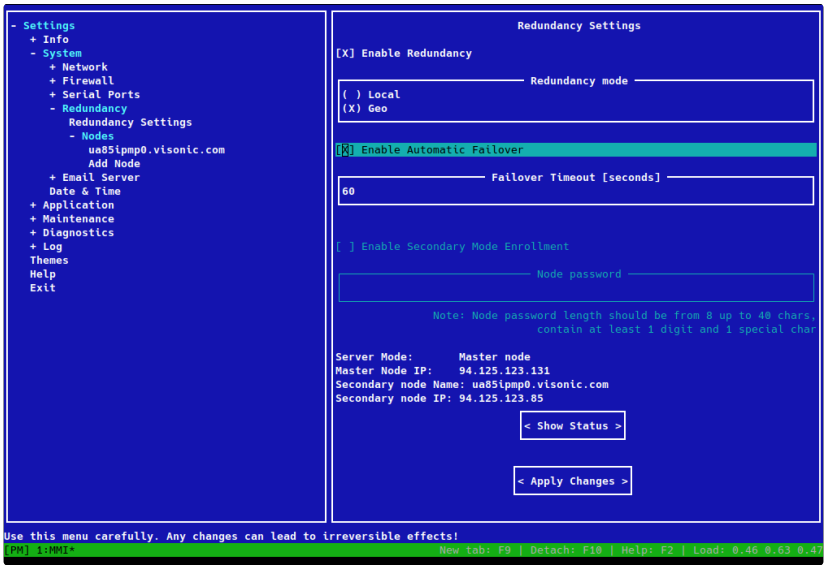


Automatic Failover (two-node system)

When configuring the redundancy, there is an option to enable the automatic failover in case the Master server fails. When the redundancy is configured with the automatic failover, there are health check services enabled on both Master and Primary Secondary nodes that check the availability of the Master server.

In case the Master server fails or becomes unavailable, the Primary Secondary server disables the redundancy, brings up the Master database, and enables the redundancy again, but configures itself as a Master server.

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



Manual Failover actions

- Enter Masters' MMI and in **System** > **Redundancy** > **Redundancy Settings** disable **Enable Redundancy** option and press **Apply.**
- Exit MMI menu.
- Enter the MMI menu on the Secondary node that you want to make the master node.
- In **System** > **Redundancy** > **Redundancy Settings** disable the **Secondary Mode Enrollment** option and press **Apply.**

- Wait until redundancy is disabled.
- In the popup press **OK.**
- Exit the MMI menu and log in again.
- In **System** > **Redundancy** > **Redundancy Settings** and enable **Enable Redundancy**.
- 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 Secondary after it fails) MMI menu.
- In **System** > **Redundancy** > **Redundancy Settings** set **Enable Secondary Mode Enrollment** option.
- Set **Node password.**
- Press **Apply Changes** button. In a dialog window, after the option is enabled, press **ESC.**
- Open new Masters' MMI menu.
- In **System** > **Redundancy** > **Nodes > Add Nodes** add Secondary (IP address and Node password of former Master).
- Press **Apply Changes** button. In a dialog box press **Apply** again.
- Wait until the Secondary is added.

Redundancy configuration (4 nodes system)

The redundancy configuration provides the ability to add as many Secondaries as it's needed. The only important thing in such a setup with 4 nodes is that as in a simple setup one node remains master, and from the other three nodes one should be indicated as Primary Secondary designated all other 2 as Usual Secondaries.

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

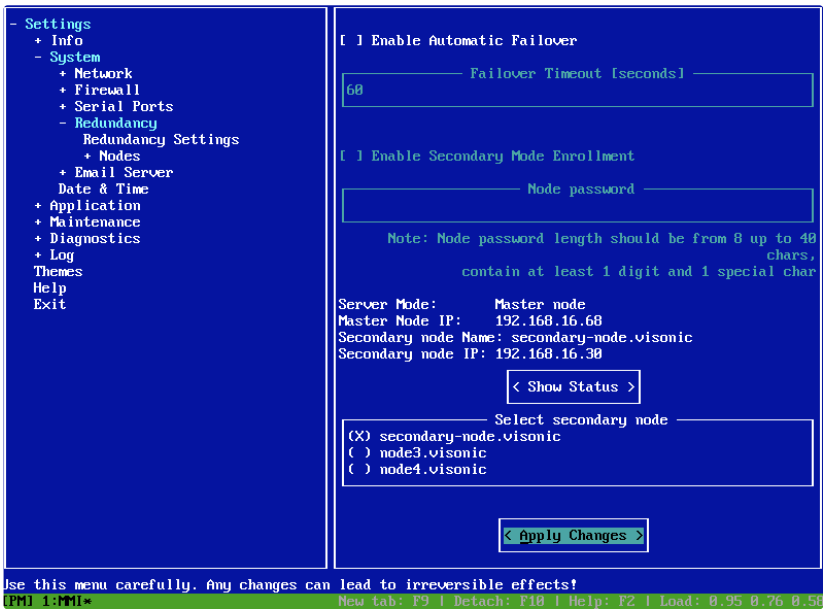
In case of automatic failover was enabled for the redundancy, the Primary Secondary node disables the redundancy, brings up the former Master database, and enables the redundancy, but in this time it sets itself as a Master server. Once the redundancy is enabled, the new Master server designates a new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

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

> ⚠ **IMPORTANT**: Master and Secondary must have different **Public IP address**. Both PM servers must be defined as its real public IP address, it should be the public IP address of its Firewall. For more information, see Configure Public IP address.
>
> In Redundancy Secondary 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, should be avoided. Otherwise, it won't be possible to activate the panel.

- Install servers.
- After installation configure Central Stations for the Master and all Secondaries.
- Enter the MMI menu on the Master.
- In **System** > **Redundancy > Redundancy Settings** set **Enable Redundancy** option.
- **Select Interface for Master Node.**
- Press **Apply Changes** button. In a dialog box press **Apply** again.
- Wait until redundancy is enabled.
- Once redundancy is enabled, you'll see the current node mode and Master's IP. To view redundancy status and enrolled Secondaries, press the **Show status** button.
- Enter the MMI menu on each Secondary.
- For each Secondary in **System** > **Redundancy > Redundancy Settings** set enable **Enable Secondary Mode Enrollment** option.

- Press **Apply Changes** button. In a dialog window, after the option is enabled, press **ESC.**
- Before adding Secondaries, enable NTP time synchronization on every Secondary and Master: in MMI **System > Date & Time** enable **Automatic Date and Time [NTP]** option and press **Apply Changes.**
- In Masters' MMI menu go to **System** > **Redundancy** > **Secondary Nodes** > **Add Node.**
- Add every Secondary node with its IP and password.
- Once all Secondaries are added you can check them in **System** > **Redundancy Settings** > **Nodes.**



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

Automatic failover (four nodes system)

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

Manual Master failover actions

In case of a Master fails the client is able to decide what server will be the new Master. It could be any of the other 3+ servers (f.e. Primary_secondary from the remote side or usual Secondary from the same side).

After the manual reconfiguration of the GEO system, it is a must to make a change on the client firewall and redirect all traffic to the new Master and Primary secondary 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 the failed node to the new one also less manual actions need to be performed and IP receivers will not be switched for the panel.

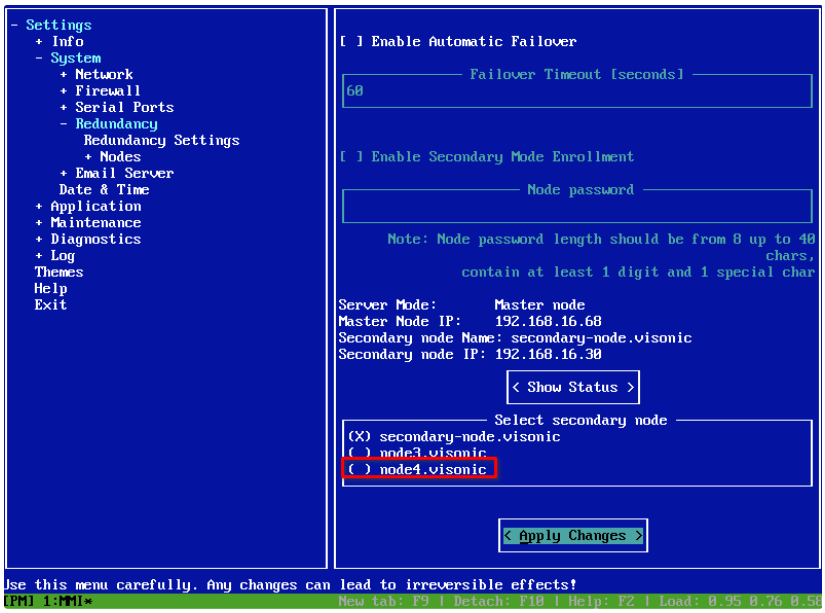
- Enter Primary Secondary' MMI and in **System** > **Redundancy** > **Redundancy Settings** disable the **Secondary Mode Enrollment** option and press **Apply Changes.**
- Exit MMI menu.
- For each Secondary and former Master disable redundancy in **System** > **Redundancy** > **Redundancy Settings**.
- Disable **Enable Redundancy** on the former master and disable **Secondary Mode Enrollment** on each secondary node.
- Wait until redundancy is disabled.

- In the popup press **OK.**
- Exit MMI menu.
- In the Primary Secondary MMI menu go to **System** > **Redundancy** > **Redundancy Settings** to enable **Enable Redundancy** option.
- Press **Apply Changes** button. In a dialog box press **Apply** again.
- Wait until redundancy is enabled.
- For each Secondary node and former Master in **System** > **Redundancy** > **Redundancy Settings** set **Enable Secondary Mode Enrollment** option.
- Set **Node password.**
- Press **Apply Changes** button. In a dialog box press **Apply** again.
- Open new Masters' MMI menu.
- In **System** > **Redundancy** > **Redundancy Settings** > **Nodes** add every Secondary node: -enter the **Node Hostname, Node IP Address**, and **Node password** fields. The IP address is the same as the former master and **Node password** that was set.
- Press **Apply Changes** button. In a dialog box press **Apply** again.
- Wait until the Secondary is added.

Manual Primary Secondary failover actions

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

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



Appendix-A

SSL certification

PowerManage 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 hostname for example marketing.visonic.com.

Note: Server supports following certificate algorithms RSA/ECDH/ECDSA and RSA key algorithm (4096 bits key size).

- Create a file and record the following values:
  - A passphrase or password is used for encryption. It is best to use a combination of numbers and letters (the 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).
  - The common name, such as the 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 an encrypted (passphrase-wrapped) form. You should keep both files together. Ensure that you keep track of the certification expiration and renewal date.