Table of Contents

Copyrights & Warranty

© Copyright 2015 by Visonic Ltd., 24 Habarzel Street, Tel-Aviv 69710, ISRAEL.
All Rights Reserved.

No part of this publication may be reproduced or distributed in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Visonic Ltd.

Microsoft is a registered trademark of Microsoft Corp.

All other products or services referred to in this manual are the trademarks, service marks, or product names of their respective holders.

DISCLAIMER: The information, products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All the statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, and users must take full responsibility for the application of any products specified in this manual.

IN NO EVENT SHALL VISONIC OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF VISONIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

WARRANTY

Visonic Ltd. and/or its subsidiaries and its affiliates ("the Manufacturer") warrants its products hereinafter referred to as "the Product" or "Products" to be in conformance with its own plans and specifications and to be free of defects in materials and workmanship under normal use and service for a period of 12 months from the date of shipment by the Manufacturer. The Manufacturer's obligations shall be limited within the warranty period, at its option, to repair or replace the product or any part thereof.

This warranty does not apply in the following cases: improper installation, misuse, failure to follow installation and operating instructions, alteration, abuse, accident or tampering.

This warranty is exclusive and expressly in lieu of all other warranties, obligations or liabilities, whether written, oral, express or implied, including any warranty of merchantability or fitness for a particular purpose, or otherwise. In no case shall the Manufacturer be liable to anyone for any consequential or incidental damages for breach of this warranty or any other warranties whatsoever, as aforesaid.

This warranty shall not be modified, varied or extended, and the Manufacturer does not authorize any person to act on its behalf in the modification, variation or extension of this warranty. This warranty shall apply to the Product only. All products, accessories or attachments of others used in conjunction with the Product, including batteries, shall be covered solely by their own warranty, if any.

The Manufacturer shall not be liable for any damage or loss whatsoever, whether directly, indirectly, incidentally, consequentially or otherwise, caused by the malfunction of the Product due to products, accessories, or attachments of others, including batteries, used in conjunction with the Products.

The Manufacturer does not represent that its Product may not be compromised and/or circumvented, or that the Product will prevent any death, personal and/or bodily injury and/or damage to property resulting from unauthorized entry, burglary, robbery, or otherwise, or that the Product will in all cases provide adequate warning or protection. User understands that a properly installed and maintained access control system may only reduce the risk of unauthorized entry without warning, but it is not insurance or a guarantee that such will not occur or that there will be no death, personal damage and/or damage to property as a result.

The Manufacturer shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function. However, if the Manufacturer is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regardless of cause or origin, the Manufacturer's maximum liability shall not in any case exceed the purchase price of the Product, which shall be fixed as liquidated damages and not as a penalty, and shall be the complete and exclusive remedy against the Manufacturer.
# Table of Contents

## TABLE OF CONTENTS

1. **INTRODUCTION TO POWERMANAGE**
   - 1.1 This User Guide
   - 1.2 About PowerManage

2. **GETTING STARTED**
   - 2.1 Types of PowerManage Users
   - 2.2 PowerManage Architecture
   - 2.3 Configuration Methods
   - 2.4 Logging in to the PowerManage Platform
     - Forgotten Password
     - Super Administrator Login
     - Logging Out of PowerManage
   - 2.5 The PowerManage Main Screen
   - 2.6 PowerManage User Settings

3. **WORKING WITH PANELS**
   - 3.1 Communication Between PowerManage and Panels
   - 3.2 Working with the All Panels Application
     - Overview
     - Filtering Data On Screen
     - Marking a Panel for Service
     - Adding a Panel
     - Editing Panel Information
     - Deleting a Panel
   - 3.3 Performing Panel Maintenance
     - General
     - Viewing the Panel Location on a Map
     - Diagnostics
     - Performing Actions in the Diagnostics Page
     - PowerLink Interactive Service vs. GPRS Interactive Service
     - Configuring PowerManage Interactive App
   - 3.4 Setting the Panel's Arming State
   - 3.5 Customizing Zone Names
   - 3.6 Viewing the Panel's Event Log
     - Faults Monitoring
     - Suspended Faults
   - 3.7 Remote Inspection
     - Overview
     - Working with the Remote Inspection List
     - Remote Inspection Test Results
   - 3.8 Performing Actions on Multiple Panels
     - Overview
     - P-Master / P-Link FW Upgrade
     - Get Alarm System Configuration
     - Push Basic Configuration
     - Panel Assign New CMS IP Address
     - P-Link2 Password Reset
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Live Log</td>
<td>78</td>
</tr>
<tr>
<td>Application Profiles</td>
<td>79</td>
</tr>
<tr>
<td>Device Logs</td>
<td>80</td>
</tr>
<tr>
<td>Setting up the Information Logging Level</td>
<td>80</td>
</tr>
<tr>
<td>Backup, Restore, Upgrade</td>
<td>81</td>
</tr>
<tr>
<td>Defining PowerManage’s Policy for Alarm Systems</td>
<td>85</td>
</tr>
<tr>
<td>Setting Up Keep-Alive Messages</td>
<td>85</td>
</tr>
<tr>
<td>GPRS-based Alarm Systems</td>
<td>86</td>
</tr>
<tr>
<td>Broadband Alarm Systems</td>
<td>86</td>
</tr>
<tr>
<td>Central Station Reporting</td>
<td>87</td>
</tr>
<tr>
<td>Configuring Repository Settings</td>
<td>89</td>
</tr>
<tr>
<td>License</td>
<td>90</td>
</tr>
<tr>
<td>Defining External API (VDCP) Settings</td>
<td>90</td>
</tr>
<tr>
<td>Interactive Protocol</td>
<td>91</td>
</tr>
<tr>
<td>Using a Customized Icon</td>
<td>91</td>
</tr>
<tr>
<td>Sending Notifications to Mobile Phones</td>
<td>92</td>
</tr>
<tr>
<td>Defining APNS Settings</td>
<td>92</td>
</tr>
<tr>
<td>Defining Session Parameters</td>
<td>93</td>
</tr>
<tr>
<td>Defining the PowerManage Application Display Language</td>
<td>93</td>
</tr>
<tr>
<td>Auto-Enroll Mask</td>
<td>94</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>95</td>
</tr>
<tr>
<td>Panels Activity</td>
<td>95</td>
</tr>
<tr>
<td>Emails Activity</td>
<td>95</td>
</tr>
<tr>
<td>Setting up Visual Alarm Verification</td>
<td>96</td>
</tr>
<tr>
<td>BOLD Manitou</td>
<td>96</td>
</tr>
<tr>
<td>One-click</td>
<td>96</td>
</tr>
<tr>
<td>MASTerMind using One-click:</td>
<td>97</td>
</tr>
<tr>
<td>Visonic’s video protocol (‘Vis-NAP’)</td>
<td>97</td>
</tr>
</tbody>
</table>

A. GUIDELINES FOR INSTALLING SSL CERTIFICATE IN POWERMANAGE 98

B. END USER LICENSE AGREEMENT 99
1. Introduction to PowerManage

1.1 This User Guide

This User Guide provides information on working with the PowerManage service management platform, including how to manage security alarm panels, manage panel configurations, create groups of monitored panels, manage and acknowledge alarms and events, and perform system tasks.

NOTE: This User Guide is intended for use by Monitoring Service Provider operators and IT managers.

1.2 About PowerManage

Visonic's PowerManage is a unique service management platform that offers security service providers a total solution for managing their IP-based services from a Central Monitoring Station (CMS).

PowerManage serves as an IP receiver to both regular and visual events, as a technical support and maintenance system for alarm systems (panels), and enables additional home control and self-monitoring services.

PowerManage supports all Visonic IP security systems (Broadband and GPRS) and may also serve as an event receiver for other monitoring systems based on SIA/IP protocol communication.
2. Getting Started

The PowerManage service management platform centralizes all information on various sets of panels in an easy-to-use web-based interface that allows quickly accessing remote panels and handling events and alarms in real-time.

Initial tasks that should be performed on PowerManage:

- Plan the permission framework:
  - Define groups of panels. Common management functions, such as configuration, arming status, etc., can then be applied on a group
  - Define roles (a role is a set of permissions, to be used by different users)
- Define user hierarchy:
  - Administrator accounts
  - Operator accounts

On-going PowerManage service management platform tasks:

- Adding new Panels (this may be done manually or automatically)
- Viewing and handling security/maintenance events
- Configuring and diagnosing existing Panels.

2.1 Types of PowerManage Users

PowerManage includes the following types of users:

- **Super Admin:** The Super Administrator has the highest level of permissions and capabilities, and is responsible for creating and deleting regular administrators. This user should only be used to manage the system admin accounts. It is not recommended to use the super admin account for managing operators, groups, panels or any other object in the system. Every PowerManage server has a single super admin. The super admin cannot be deleted nor can a super admin be created.
- **Administrator:** Administrators are capable of performing all tasks, except deleting administrators. Administrators can create and edit all operators, define user roles, and access all panels.
- **Operator:** Operators are able to access specific groups of panels to view and/or perform actions (e.g. maintenance, arm/disarm, etc.) based on the access rights.
- **Event interface User:** This user type is relevant for One-Click users (for example, used by the CMS to receive images of an event). It has the same functionality and permissions as an operator.
- **End-user:** In the context of this manual, end-users are home residents, using a Visonic interactive app to access their home security system. The end-user may arm and disarm the panel, view the status of detectors, get alarms, and get image/video verifications.
2.2 *PowerManage Architecture*

PowerManage is an integration platform that incorporates multiple protocols and interfaces (numbers correspond to labels in the figure above):

1. **Receiver**: gets events from the panels via IP or GPRS on standard protocols such as SIA and CID, and transfers them to standard automation receiver and control (AKA ARC) applications such as MLR-2 or FEP, or transfers pictures using Visonic proprietary protocol (VISNAP).
2. **Resolve**: Enables the CMS operator to remotely check, configure and get periodic health reports from the panels.
3. **One-Click**: Opens a browser view displaying the specific panel’s recent events, also with image clips (if any exist).
4. **VDCP**: Enables connection to 3rd party applications through a two way interface based on Pythons. This protocol supports most of the operator’s commands from the PowerManage WEB-GUI on the PowerManage and on the panels.
5. **Interactive application** – Enables homeowners to see the status, arm/disarm, get image verification and view historical logs on his panel from their mobile phones or remote PCs.
6. **PowerManage Management Console**: Administration Console, Linux-based application configuration.

2.3 *Configuration Methods*

The PowerManage uses the following methods to configure the server parameters:

- The PowerManage application’s web site
- The PowerManage Management Console.

**The PowerManage application’s web site**

1. Open a web browser (Google Chrome, Mozilla Firefox - Internet Explorer and Opera are not supported) and go to the IP address (or DNS name if one exists) of your PowerManage server.
2. To log in, enter the general username “admin@visonic.com”, and password "Admin123". It is highly recommended to change the password after entering the web site. Although the web application is used mainly to control users, you can also configure server parameters.

**The PowerManage Management Console**

*Note: The Management Console may also be referred to as "MMI".*

Log into the PowerManage server, using an SSH program such as PuTTY. The management console is used mainly to configure the server parameters. The default user name is "root", and the default password is "visonic".
2.4 Logging in to the PowerManage Platform

In order to access PowerManage, enter the public IP address of the server in the browser’s URL or use the URL directly.
For example: 12.234.210.201.

1. When logging in to the PowerManage web interface, enter your email address and password.

2. After entering the email and password, click Log in. The main page appears.

3. If you want to make additional changes, click the Stay on this page after saving check box.

4. Click the Save Changes button to save the information.
Forgotten Password

If you forgot the password, press the Forgot button; the following window appears:

Type your registered Email Address and press the Remind>> button. The system will send a temporary password, which is valid for one login session, to the specified email. *At this point, use the temporary password to log in. Following this login, you will be prompted to change to a more permanent password.

Super Administrator Login

New accounts for additional PowerManage users can be defined by the administrator in the System page, under Users.

The super-administrator can create new administrators or new operators (if user-roles are defined). Administrators can also create new operators (if user-roles are defined).

The super-administrator "sees" all accounts, while the administrator “sees” all operators but no other administrators.

The super administrator's default username and password are:

- admin@visonic.com
- Admin123

Logging Out of PowerManage

*Note: To log out of the system, click the Logout button in the top right corner of each page.*

2.5 The PowerManage Main Screen

The top menu bar provides the number of events and processes that require attention and shows the name of the currently logged-in user.

From the top bar, you can perform the following actions:

- Click the Audio Notification icon once to disable or enable audio notifications via the local PC speakers.
- Click the Logout button to log out from the system.
- Click the (Profile) button to edit account information of the current user (the user that has just logged in), such as phone number, country or password.
- Select one of the following options that allow performing various tasks:
  - Panels: Allows viewing information on alarm system panels, viewing online/offline/connected panels status (via the GPRS or BBA communication channel), marking panels for service, adding/removing Panels, managing the Panel configuration, viewing faults from alarm systems, performing Remote Inspections, modifying Interactive Features settings, and upgrading the software version of PowerMaster panels and IP Communicator modules. See Working with Panels.
  - Groups: Allows defining groups of panels. See Working with Groups.
  - Events: Provides a list of events per Panel and account, allows defining whether the events were handled and viewing image clips (if any exist). See Viewing and Handling Events.
Getting Started

- **Processes**: Provides a list of all PowerManage executed processes, along with the process status. See Working with Processes.

- **System**: Allows managing PowerManage users, performing troubleshooting, configuring Remote Inspections and performing server maintenance. This page is available to the super-administrator and administrators only. See Performing Administrative Tasks.

**Note:** All pages, except for the SYSTEM page, have a three-level filter on the left side of the page that allows the user to view data based on specific queries.

### 2.6 PowerManage User Settings

These settings are used to change basic user account information, such as the user’s phone number, country in which the PowerManage server is located and the password.

1. Press the **(Profile)** button in the top right side of the screen.

   All PowerManage users have access to this button (unlike the SYSTEM page which is visible to Administrators only).

2. After pressing the **(Profile)** button, make the required changes in the respective boxes.
3. Working with Panels

The Panels page allows you to access the following applications:

- **All Panels**
- **Faults Monitoring**
- **Suspended Faults**
- **Remote Inspection**
- **Reports**

### 3.1 Communication Between PowerManage and Panels

PowerManage communicates with the panels in the following ways:

- **Event PUSH mode**: Panel sends an event to the PowerManage, either on GPRS or on IP communications, via SIA-IP protocol. The PowerManage always listens to the events from the panels.

- **WakeUp Mode**: In this mode, communication is initiated from the server to the panel in order to get information from the panel such as configuration, status etc. The server initiates a GSM call to the panel, which recognizes the voice-call source by the phone number, closes the voice session and opens a GPRS session to the server. If the panel does not respond after several (configurable) retries, the server sends an SMS to the panel. The procedure ends with the panel sending a keep-alive message. The exact behavior described here can also be configured through the server.

- **KeepAlive Mode**: In this mode, the panel is configured to send a “signal” to PowerManage on GPRS and/or IP, at a specific interval. If the signal does not arrive to the server after a number of retries/timeout (configurable), the panel is considered “offline”. This mode’s purpose is to save traffic between the panel and the server.

- **Always on Mode**: When using the panel's GSM/GPRS or IP module for communication, the server is constantly connected to the panel. This mode creates high traffic between the panel and the server.

- **IP Connection Mode**: The panel may include a GPRS module (for cellular connection to the server) and/or a PowerLink module (for IP connection to the server). The server defines which communication channels are active, and notifies 'offline' when keep-alive messages are not received from each of the channels.

### 3.2 Working with the All Panels Application

**Overview**

The **All Panels** application provides a list of all the alarm systems installed at end-users with summary information. The list of panels displayed can be filtered according to specific criteria enabling access to individual panels. This list is accessible from the Panels screen.
Working with Panels

In the list, the following information is displayed per Panel:

- **Left check box**: Select this check box to perform actions on ALL of the listed panels. To select only one or some of the panels, deselect this box.

- **Panel ID**: Displays the Panel’s unique Tyco-Visonic identifier. The Panel ID also appears on a label on the back of the actual Panel.

- **Web name**: Displays the Panel ID which is used by the Visonic application user (e.g., the homeowner). The Web name is identical to the ‘Panel ID’ by default, is not case-sensitive, and can be changed by editing the panel information. See the "Working with PowerManage Interactive " section for further details.

- **Account number**: Displays the account number that is configured in the Panel, and is used to report to the Central Monitoring Station (CMS).

- **Type**: Displays the type of Panel.

- **Group**: Displays the group to which the Panel belongs. Groups are used to manage multiple Panels. For more details on groups see “Working with Groups”.

- **Modules**: Displays the communication module that the Panel uses to communicate (either PowerLink/Broadband or GPRS) and the status of the module:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="B" /></td>
<td>Powerlink Module is offline</td>
</tr>
<tr>
<td><img src="image" alt="B" /></td>
<td>Powerlink Module is online</td>
</tr>
<tr>
<td><img src="image" alt="G" /></td>
<td>GPRS Module is offline</td>
</tr>
<tr>
<td><img src="image" alt="G" /></td>
<td>GPRS Module is online</td>
</tr>
<tr>
<td><img src="image" alt="G" /></td>
<td>GPRS is online, Keep-Alive supervision is disabled</td>
</tr>
</tbody>
</table>

**Note:** When Keep-Alive is disabled, the Panel’s status (online/offline) is saved. If the panel was **online** before the operator disabled Keep-Alive for the group it belongs to, the status appears as ![G](image). If the panel was **offline** before the operator disabled Keep-Alive, it appears as **offline** ![G](image).

- **Events**: Shows the number of unhandled events for the panel. If there are unhandled events, one of the following icons will appear:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="X" /></td>
<td>There are unhandled events, some of which are alarms.</td>
</tr>
<tr>
<td><img src="image" alt="X" /></td>
<td>There are unhandled events, without alarms.</td>
</tr>
</tbody>
</table>

A comprehensive list of icons and their meanings appear in “Description of Icons”.

- **GUI checkbox**: Allows defining whether the end user is allowed to access their Panel via their PowerLink web interface or the interactive application. This is relevant for Panels with the PowerLink broadband add-on module which provides the web interface to the Panel or for Panels with the GPRS module. To completely deny access to the Panel's PowerLink/Interactive web interface, clear the checkbox.

*Notes*: PowerManage can process and display events sent by Panels that are not listed in the Panels-List; these panels were not enrolled to the PowerManage. However, even though events may be processed and displayed in the Events page, PowerManage will not provide management features such as remote arm/disarm, viewing or editing configuration and image on-demand for unenrolled Panels.

The above feature is disabled by default. To enable it, open the Management Console, navigate to the Events before KA option and then press the Apply button, as shown below.
Filtering Data On Screen

When viewing the list of panels you can:

- Click on the column name to sort according to that field.
- Use the **Search** field to search for specific data.
- To do this, enter any part of search value in the **Search** text box and click the **Search** button to search the data. To clear search results click **Clear**.

- Use the **filters** on the left side of the page to view data based on specific queries. Take note that the filter types correspond with the names of the columns in the list.

**To filter data:**

1. Select the filter (e.g. Web name) from the drop-down list to see a list of the values available for that filter.
2. Select a value or click **More values**, and add the exact value to look for in order to see additional options. It is possible to select multiple columns and multiple values. To clear filter results, click **All**.
Marking a Panel for Service

The CMS operators use their own set of maintenance and service procedures on the managed panels. Use one of the following methods to mark a panel for service:

- To assist in the maintenance procedure when viewing a list of panels, mark a panel for service. Select the check box on the left side of the panel row, click the Actions button, and select Mark for service. The panel will be marked as requiring service.

From the drop-down list, select to whom you want to reassign the panel (one of the user roles defined in the SYSTEM page). Explain the reason for service in the Comments box.

After marking the panel for service, the panel will appear in the Faults Monitoring page. The Operator can perform the following tasks on the Faults Monitoring list of panels. Press the Actions button and then select one of the following options. In the dialog box, choose on which faults to implement the action:

- **Reassign faults** Assign the fault handling to another user.
- **Suspend faults** Postpone the handling of these faults. They will then appear in the Suspended Faults page.
- **Resolve faults** Fix the faults.
- **Refresh Panels** Refresh the screen information. Pressing this button uploads updated data from the panels.
Adding a Panel

By default, Panels are added manually to the PowerManage Panels List. However, it is also possible to set up PowerManage to automatically add new panels to the server.

Adding a Panel Manually

Panels can be added manually in the All Panels page.

To add a Panel manually:

1. Click the + Add Unit button at the top of the All Panels page.
2. Enter the following information:

   Panel ID: Enter the Panel’s ID (six digits composed of the alphanumeric characters 0-9 and A-F). The Panel ID appears on the actual Panel, or on the sticker supplied. (Mandatory)
   
   Client type: Select the client type (communication module):
     - GPRS Adapter
     - PowerLink Adapter – PowerLink 2 (broadband) module
     - PL Adapter – PowerLink/PowerLink Pro (broadband) module
   
   Web name: Enter the Panel’s name, which allows end-users to access the Panel’s PowerLink or interactive app module via the web. (Mandatory)
   
   Account number: Enter the account number configured on the Panel, used to report to the CMS. The account number is also automatically obtained from the panel. (Optional)
   
   Group: Select the group to which the Panel belongs. See more details on Adding a group. (Mandatory)
   
   SIM Number: Telephone number of Panel for Wake-Up. (Optional)
   
   Contact Name: Enter a contact name of the end user this panel belongs to. (Optional)
   
   Contact E-mail: Enter a contact e-mail for the Panel. This is used by PowerManage to send 'online/offline' status notifications to the end user. (Optional)
   
   Phone: Enter the contact’s telephone number. This is used by PowerManage to send 'online/offline' status notification to the end user. (Optional)
Working with Panels

Street Address  Enter the contact’s physical location address. This information enables the Map and Satellite View to display the panel’s exact location. (Optional)

Remarks:  Allows adding comments or additional information. (Optional)

3. If you want to add an additional Panel, click the Stay on this page after saving check box. To delete your information changes without saving, click Discard Changes.

4. Click the Save changes button to save the new Panel details.

Adding a Panel Automatically

If the "automatic enrollment" option is enabled for this server in Power Manage console (see Defining PowerManage’s Policy for Alarm Systems), any panel that is configured to the current server will be added following arrival of the first keep-alive message, and will join the "Main" group. The "Automatic enrollment" option in the PowerManage console is available for panels with BBA (BroadBand Adaptor) and GPRS communication, see GPRS-based Alarm Systems and Broadband Alarm Systems

Note: All users in the system can access the "Main" group.

Editing Panel Information

1. While viewing the panel information, click the Panel Actions button at the top of the page and then select Edit Panel.

2. Edit the data as required (for example, enter an email address in the Contact Email field). To delete your information changes without saving, click Discard Changes.

3. Click the Save Changes button to save the changes.

Deleting a Panel

Delete a panel from the Panel List by one of the following procedures:

- In the specific panel page, click the Panel Actions button at the top of the page and then select Remove Panel.
- or-

- In the Panel List, select the panel’s checkbox and click the Remove Unit button at the top of the page. Click Yes to confirm.
3.3 Performing Panel Maintenance

When viewing the list of panels in the PANELS or PROCESSES page, you can click on the panel ID to view information about that panel.

Each panel’s information includes the following:

- General
- Services
- Location
- Diagnostics
- Remote Inspections
- Report Results
- Virtual Keypad
- Set State
- Set/Get Configuration
- Zones Customization
- Standard Log
- Legacy Log

When viewing these pages, the following buttons are available:

- Refresh Panel: Refresh the screen information. Pressing this button uploads updated data from the panel.
- Edit Panel: Edit the panel information.
- Remove Panel: Delete the panel.
- Discard Changes: Delete panel information changes without saving.
- Save Changes: Save panel information changes (only on pages that can be edited).
- Next: View the next panel in the Panel List.
- Previous: View the previous panel in the Panel List.

On each panel page, the left side includes a Menu tab providing links for several relevant options for the panel, and a Remarks tab for writing action item notes about the panel.

Descriptions of these options appear in the sections that follow.

General

Under General, you can view information about the Panel and change parameters.

You can perform the following actions:

- View basic information about the Panel
- Edit information where possible (SIM number, contact name, contact email, street address, phone number and remarks)
- Remove a panel from PowerManage management.

When you finish editing panel information, click the Save Changes button.
Working with Panels

Note: To see to which group this panel belongs, click the Edit Panel button.

The following data is displayed:

- **Status**: The status of the Panel's connection, for example “online”.
- **Panel HW version**: The version of the panel's hardware.
- **Panel SW version**: The version of the panel's software.
- **Panel Default version**: Version of the panel's configuration database.
- **Unit RSU Version**: Version of the Remote Software Upgrade
- **Panel SW last upgraded**: The date of the panel's last software upgrade.
- **PowerLink SW version**: The version of the PowerLink Panel's software.
- **Unit HW Version**: The panel's hardware version.
- **PowerLink Configuration Variant**: Number of PowerLink “PVR’s”
- **PowerLink SW last upgraded**: The date of the PowerLink Panel's last software upgrade.
- **Panel ID**: The panel's identification number.
- **Account number**: The account number the Panel uses to report to the CMS.
- **Web name**: The Panel's given name (defined when you added the panel) which allows end-users to access the Panel's PowerLink module or GPRS module via the web or the interactive app.
- **Panel Type**: The type of the panel, for example “PowerMaster 30”.
- **SIM Number**: Phone number of the Panel's SIM card. PowerManage uses this number to initiate communication with the control panel.
- **Contact Name**: The private name of the contact person for the Panel.
- **Contact Email**: The contact person’s email, which PowerManage uses for the Panel's ‘online/offline’ status notification for Private Report.
- **Street Address**: Enter the contact’s physical location address. PowerManage's Google Maps viewer uses this information to point to and zoom into the panel's exact location (see the following section).
- **Phone**: The contact person’s phone number, which PowerManage uses for the Panel's ‘online/offline’ status for Private notification).
- **Remarks**: Additional notes about the Panel.
Working with Panels

Viewing the Panel Location on a Map

To help the Central Monitoring Station find the location of an alarm or other disturbance that requires a check by security personnel, PowerManage provides a Google Maps viewer on the Panel Info>General page. If the Street Address is specified under Panel Information, the map viewer opens with the panel's location centered and labeled.

1. In the PANELS tab, click the Location link under PANEL INFO. A Google Maps viewer opens, displaying a map of the location.

2. According to your needs, zoom in or out, and display the satellite photograph view of the location.
Working with Panels

Diagnostics

The **Diagnostics** page is used to perform routine panel testing and maintenance. It shows a graphic list of peripherals and allows viewing the status of the panel and the installed modules, and lists the various zones monitored by the panel.

The `<prev | next >` buttons in the upper left side of the page are used for toggling between enrolled panels.

At the top of the **Diagnostics** page, you can see the status/state of the panel and the Panel ID.

The **Diagnostics** page is divided into various sections. A description of each section follows.

- **Control Panel:** Provides details of the selected panel, including the panel name, a graphical presentation of the panel and faults detected for that panel, and the communication channels supported. The following information/options appear:
  - The account number appears next to "Control Panel" in the title bar.
  - Under the title bar, a picture of the panel type appears.
  - In the Status area, each icon represents a fault. Moving the mouse over the icons displays details of the faults (including the comment entered in **Mark for Service**).

<table>
<thead>
<tr>
<th>Fault</th>
<th>Icon</th>
<th>Fault Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low battery</td>
<td>🚭</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Supervision (Missing)</td>
<td>☞️</td>
<td>Fault</td>
</tr>
<tr>
<td>AC fail</td>
<td>☞️</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Line failure (PSTN)</td>
<td>☞️</td>
<td>Fault</td>
</tr>
<tr>
<td>Line failure (GSM)</td>
<td>☞️</td>
<td>Fault</td>
</tr>
<tr>
<td>Keep-alive lost (GPRS)</td>
<td>☞️</td>
<td>Fault</td>
</tr>
<tr>
<td>Keep-alive lost (broadband)</td>
<td>☞️</td>
<td>Fault</td>
</tr>
</tbody>
</table>
Working with Panels

<table>
<thead>
<tr>
<th>Fault</th>
<th>Icon</th>
<th>Fault Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Violated</td>
<td>![Fault Icon]</td>
<td>Alarm</td>
</tr>
<tr>
<td>Tamper open</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>SIM Not Verified</td>
<td>![Maintenance Icon]</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Clean me/Replace from a Smoke/GAS detector</td>
<td>![Maintenance Icon]</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Masking</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Device failed updating configuration</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Memory</td>
<td>![Maintenance Icon]</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Alarm (any kind)</td>
<td>![Alarm Icon]</td>
<td>Alarm</td>
</tr>
<tr>
<td>Jamming</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Current link quality (RSSI) Poor or less</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>1-Way fault</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Last 24-hrs average link quality (RSSI) Poor or less</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Autotest not received</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>User requested service</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
<tr>
<td>Operator marked for service</td>
<td>![Fault Icon]</td>
<td>Fault</td>
</tr>
</tbody>
</table>

- **Communication modules:** The right side of Control Panel window shows available communication modules.

- **Zones:** This window shows the zones defined for the panel.
Working with Panels

A description of the Zones window follows:

The number next to the "Zone" in the title bar represents the number of zones supported by the currently selected partition. Zones typically contain installed sensors. Unused zones are grayed out with diagonal gray lines.

On the right side of the title bar, the total number of faults detected for all zones appears. Faults refer to any type of behavior that deviates from the normal status of the peripheral i.e. low battery, tamper open, one way, AC fail etc. Faults are detected for all zones.

The name of the zone. This name can be changed. The number shows the zone ID.

Allows capturing an on-demand picture from that zone (applies only if a PIR camera sensor is installed in the zone).

To enable the video sent from the panel, the panel needs to be configured to allow sending video-on-demand.

From the panel, select Installer-Mode>Communication>Motion-Camera>View-On-Demand, Enable.

The signal strength indicator represents the strength of the communication signal between the detector in the zone and the panel, as follows:

- **Gray bars**: No communication; this is also represented in the Fault List.
- **Yellow bars**: Communication is only one-way.
- **Green bars**: Two way communication exists. The signal strength is represented as follows:
  - Minimum number of bars (1 bar) = poor communication
  - Medium number of bars (2 bars) = good communication
  - Maximum number of bars (3 bars) = strong communication

Clicking the signal strength's drop-down arrow provides last known (as indicated by "Updated") details on the RF channels: the last time the detector was activated, the most recently used RF channels and repeaters, and the average signal strength for the last 24 hrs.

The **Refresh** button updates statistics for all devices (received from panel).

The **Status** area shows the status of the zone:

- Pre-enrolled means that the definition of the detector/zone exists but there is no actual detector yet. When the detector is installed and enrolled in the panel, this indication will disappear.
- "Bypassed" indicates a zone that remains open while the security system is being armed.
- If faults exist, a list of the faults is shown.

You can move the mouse over the status area to see more details about the faults.

Allows bypassing a zone.

Allow a soak test to run on the unit, checking that nothing triggers false alarms from the sensor installed in this zone (test is successful if zone is not activated).
Working with Panels

- Remove the device from the panel.
- RARELY TRIGGERED zones are marked manually and are not shown in commonly used zones of the Remote Inspection results (enables the zone to appear in reports).

- **Keyfobs, Keypads and Pendants**: The keypad, keyfob, pendants, repeaters, sirens, etc. provides details of devices enrolled in the system other than zones. Details shown per device are similar to zones except they do not have a named location and the device ID shown is numbered separately per keypads, keyfob, repeaters, sirens, etc.

Performing Actions in the Diagnostics Page

The following options are available in the **Diagnostics** page:

- **Filtering devices displayed**: Allows filtering in order to view a smaller device list.

- **Close Service Request**: Allows removing the panel from the **Mark for Service** list.

- **Run Walktest**: The **Run Walk Test** button allows entering the "Walk Test" mode. The security system waits for all devices to be activated, and the button then changes to **Stop Walk Test**.

- **Reassign Device**: Allows reassigning the panel's faults to a different operator (this user role must be defined for the operator in the **SYSTEM** page).

- **Add Device**: When adding a device to the panel, you must enter the device's 7-digit code and (in case of a sensor) a zone number. The new device remains 'pre-enrolled' until the actual device (with the same 7-digit code) is enrolled to the panel, and the device's state then changes from "pre-enrolled" to "enrolled." Then, refresh the panel to see the added device.

The `< prev | next >` buttons in the upper left side of the page are used for browsing to the next or the previous panels in the Panel List.

PowerLink Interactive Service vs. GPRS Interactive Service

PowerManage supports the following panels’ connections:

- PowerMax panel series with PowerLink-2
- PowerMaster panel series with PowerLink-3
- PowerMax panel series with GPRS
- PowerMaster panel series with GPRS
  - Working with the PowerMaster panels series enables the integration of PIR CAM cameras into the system to get series of images and video for video verification, which is not possible to receive from PowerMax panels.
  - Working with PowerLink-2 (on PowerMax panel series), enables the integration of WIFI cameras into the system, which is not possible in GPRS-based solution.
Configuring PowerManage Interactive App

Enable/Disable PowerManage Interactive App for a Panel

In the ALL-Panel list, check the panel’s GUI box to enable PowerManage Interactive app access for its home owner.

Configuring Access to PowerManage Interactive Application

Providing the Web name

The WEB Name is the name used by the home owner to log in to the server. The server will redirect the user’s browser to his PowerLink module’s web interface or GPRS mobile interface.

In the Panel> Edit Panel page, define a unique WEB Name for the home owner.

Using the Web Name to Access the PowerManage Interactive App

For example, you can access a Panel using the web name "John" by entering the following address in a browser:

http://[PowerManage server address]/John

Note: The web name is not case sensitive.

If necessary, the operator can define a new web name in the New Web Name text box.
Event Messages

You can program to send event notifications messages via the **Panel>Services** page. You can send alarm, arming or trouble events to 4 private emails and to 4 private MMS and SMS telephone numbers. Select the event messages to be sent by clicking on the relevant check boxes shown below. After making your selections, click the **Save Messaging** button.

Remote Routine Inspections (RRI)

In the Remote Inspections it is possible to initialize inspection on-demand manually or periodically by schedule, view/filter Remote Inspection results for the panel, mark them as reviewed, add comments by different operators, and configure Remote Inspection setup.

The inspections are performed by uploading the panel log file and analyzing the data (see **Setting up the RRI** below). Following configuration of the test, you can choose one of the following RRI options:

- **Initiate Inspection** immediately
- **Schedule** the inspection periodically (you are prompted to enter the starting time and the cycle length).

**Setting Up the RRI**

The RRI uploads certain values from the panels and checks each of them to see that they are within the correct functionality range, therefore verifying that the installed system is working properly.
Note: Configuring options for the RRI is performed in the SYSTEM page.

1. In the SYSTEM page, under SETTINGS, click Remote Inspection Values to define the scope of the available test options (the "X" value is configurable in the Configuration page):

   - **Check for Reported Faults**: Check for any faults in the last X events. List current faults and tampers.
   - **Total System States**: Check set/unset event within the last X events. Show the last set & unset time.
   - **Check frequently used zones**: Check for zones that have not been activated during the last X weeks. Devices that were defined as "Rarely Triggered" (in the Diagnostics page) will not be reported as "not used".
   - **Treat Adjusted Date/Time as Failure**: If the time difference between the panel and server exceeds X minutes, indicate a "failure."

2. Click the Save Changes button.

   After an inspection ends, the main screen displays the results.
3. To display results from the five most recent RRIs, click the **Show 5 latest** option. To display results during a specific time period, click the **Show from/to** option and specify the beginning and end dates in the **from** and **to** boxes, respectively.

The "Results" and "Range" columns display how many faults occurred during a specific testing period.

4. The "View Info" column specifies the source of the test results. Place the cursor on the "View Info" column of a certain test to display detailed information on the test results (if such information exists).

5. Press the **Mark Reviewed** button (top right of the page) to clear the results.

**Set State**

In the **Set State** page, you can set or view the Armed and Disarmed status of the various zones monitored by the panel:

- **AWAY**: Arm the system when the site is vacated completely.
- **AWAY+instant**: Arm the system when all persons leave the site, without an entry delay, so that any detection will trigger an immediate alarm.
- **AWAY+Latchkey**: Arm the system so that an alert is sent to the homeowners' telephone when their children or other resident have entered the home and disarmed the system.
- **HOME**: Arm the system when persons are present at the site.
- **HOME+instant**: Arm the system when persons are at the site, without an entry delay, so that any detection will trigger an immediate alarm.
- **DISARM**: Disarm the system and stop all alarms.
- **BYPASS**: Select the Bypass checkbox to keep the zone unarmed, and possible to move around in it, while other zones are in an Armed state.
Set/Get Configuration

Under Set/Get, you can download a configuration (pulling the panel's configuration into PowerManage database), edit the configuration, create a basic configuration, compare the configuration with the last known configuration, and save the configuration as the last known.

Setting Panel Configurations

The Panel's configuration is stored on the Panel, not on the PowerManage server. It is possible to download a copy of the configuration of any Panel and then view and edit this copy of the Panel's configuration, and perform remote maintenance.

You can then also upload the new configuration back to one or more Panels.

Downloading a Panel's Configuration

When managing configurations, the operator can download, view and edit a Panel's configuration. It is also possible to perform this action on multiple panels. For more details, see Performing Actions on Multiple Panels.

1. In the Panels list, select a Panel to download the configuration and then select Set/Get Configuration in the left side of the page.

2. Download the panel configuration to the server's database (perform this step only if the server does not yet hold this data).
   Click the Actions drop-down list in the top right corner of the Panels->SetGet Configuration page and select Get Alarm System Configuration.

   ![Actions Drop-down List]

   **Note:** Downloading the configuration from the panel may take a long time, depending on the defined keep-alive period.

When downloading is complete, you can view the panel's configuration.
Editing a Configuration

If a panel’s configuration has been downloaded to the PowerManage server, you can edit it.

1. Click the panel name and select **Edit Configuration** in the **Actions** drop-down list.

2. You can now edit configuration parameters. Use the search query box to find a specific parameter or value.

3. Click **Save Changes** to save the changes to the configuration.

4. Click **Cancel** if you don’t want to save changes to the configuration.

Saving the Last Known Configuration

The PowerManage operator can save a panel’s current configuration, at any point in time. This action creates a “snapshot” of the configuration which can be used for comparison purposes in the future. Changes to the configuration from this point on will not be included in the “last known” configuration (See "Comparing with the Last Saved Configuration" on page 31).

To save the current panel configuration:

- While viewing a Panel’s configuration, click the **Action** drop-down list and select the **Save Configuration** option from the Configuration drop-down menu.
Comparing with the Last Saved Configuration

PowerManage allows you to compare the panel’s current configuration against the panel’s last saved configuration in order to see changes that were made to the configuration.

To compare configurations:

1. Ensure that a configuration for this panel is already saved in the PowerManage database (See "Saving the Last Known Configuration" on page 30). You can upload a modified configuration at a future point in time and compare it to the saved configuration.

2. Click the Action drop-down list and select Compare with Saved Configuration.

3. Use the search text box at the top, or the Show/all/different/changed buttons near the bottom of the screen, to filter the display of the compared configuration values.

4. To update the data from the saved configuration, select the check boxes of the changed fields from the last saved configuration and press the Save Merged button.
Creating a Basic Configuration

The basic configuration is a generic system configuration template created from a particular version or from a specific point in time. You can fine tune the configuration and then upload it to multiple panels (of the same version).

The basic configuration includes all parameters that are not site-specific, excluding parameters such as end-user contact details. You can use any Panel's current configuration to create a basic configuration.

To create a basic configuration:

1. While viewing a Panel’s configuration, select the Make Basic Configuration option from the Actions dropdown list. Select the options you want to base the basic configuration.
2. In the Basic Configuration Name box near the bottom of the screen, enter a name for the configuration.
3. Press the Save Basic button.
3.4 **Setting the Panel’s Arming State**

After the panel has been registered and configured in PowerManage, you can control its arming state (arm/disarm) from the CMS.

1. In the Panel Information page, select **Set State** to change the arming state.

2. Click the status link at the top.

3. Set the required arming state:
   - **Disarm** – Click to disarm the system and stop the transmission of alarms.
   - **Away** – Click to arm the system when nobody is at home. Options are Normal, Instant (no entry delay), and Latchkey (latchkey message alert will be sent).
   - **Home** – Click to arm the system when people are at home. Options are Normal and Instant.
3.5 Customizing Zone Names

You can edit several customized zone-names in the panel (in contrast to the pre-defined zones).

You can use any characters that are associated with the panel's interface language. If you include invalid characters in a zone name, the save process will fail (a red indication, instead of green, will appear in the top right side of the page).

After editing the custom name(s), press the **Save Locations** button.
3.6 **Viewing the Panel’s Event Log**

For each panel, you can view a list of events in one of the following formats: Under Panel Event Log, you can view a standard or legacy log.

From the All Panels List, enter the panel’s information page. In the panel’s menu on the left side of the page, click **Standard log** or **Legacy log**.

- **Standard log**: A list of events that complies with the EN 50131-3 standard’s guideline for listing events (see the figure below).
- **Legacy log**: A list of events that is identical to the event log visible on the panel’s LCD, without filtering.

Click the **Refresh** button in the log page to download events from the control panel. Both logs are cyclic – old events are deleted to allow new events to be logged.
Faults Monitoring

The **Faults Monitoring** application provides a real-time list of panels in need of service and includes details of the fault types and fault severity. In this menu, it is possible to assign faulty-panel service to specific PowerManage operators, suspend (ignore) faults for a certain period of time, and initiate actions on multiple panels in order to fix faults. When you move the mouse pointer over the **Source** column, a list of all active faults appears.

The following information appears in the **Faults Monitoring** page:

- **Panel ID**: The panel's identification number.
- **Account**: The account number the Panel uses to report to the CMS.
- **Web Name**: The Panel's given name (defined when you added the panel) which allows end-users to access the Panel's PowerLink module or GPRS module via the web.
- **Source**: Displays the type of fault and the location e.g. control panel or a specific zone.
- **Time**: Shows when the panel was added to the list.
- **Operator**: Shows to which operator the faulty panel was assigned (See "Defining User Roles" on page 59).
- **New remarks**: Shows the number of new remarks that were added since the last time someone viewed the **Remarks** tab. Moving the pointer over the number of remarks shows information about the last three remarks.

The following options are available at the top of the page:

- **Reassign button**: Allows reassigning a panel to another PowerManage operator.

- **Suspend Faults button**: Allows ignoring one or more faults in a panel to a limited period of time (the fault will be ignored by the Fault-Monitoring application). The panel will be listed in the **Suspended Faults** page. See Suspended Faults for more details on managing suspended faults.
- **Resolve Faults**: This option is available under the **Actions** drop-down menu and allows marking a fault as resolved. It is only relevant for **Marked For Service** panels.

- **Refresh Panels**: Refreshes the screen information by uploading updated data from the panels.

In addition, you can use the filter options on the left side of the page to view specific data.

### Suspended Faults

- The **SuspendedFaults** page allows managing the list of suspended faults by panel by reassigning faults to a different operator or releasing suspended faults.

The following information appears in the **Suspended Faults** page:

- **Panel ID**: The panel’s identification number.
- **Account number**: The account number the Panel uses to report to the CMS.
- **WebName**: The Panel’s given name (defined when you added the panel) which allows end-users to access the Panel’s PowerLink module via the web.
- **Source**: Displays the type of fault and the location e.g. control panel or a specific zone.
- **Until**: Shows until when the fault is suspended.
- **Time**: Shows when the panel was added to the list.
Working with Panels

- **Operator**: Shows to which operator the panel with faults was assigned.

The following options are available at the top of the page:

- **Reassign button**: Allows reassigning a panel. To do this, select the panel and click the **Reassign** button.

- **Resume Faults button**: Allows clearing suspension of a panel, and resumes viewing of any faults.

In addition, you can use the filter options on the left side of the page to view specific data.

### 3.7 Remote Inspection

**Overview**

The **Remote Inspection** page allows scheduling, initiating, and canceling routine remote inspections.

This page provides a list of panels and allows performing the following actions:

- Scheduling, initiating, and canceling routine remote inspections (Remote Inspections)
- Viewing historical Remote Inspection results for a single panel.

At the top of the page, you can use the buttons to perform the following actions:

- **Schedule an inspection**: Allows setting the date for the next remote inspection, and also allows defining whether further inspections will be performed periodically.
- **Initiate an inspection**: Starts an inspection on demand. It is also possible to initiate inspection on an offline panel. In this case, the inspection will start when the panel changes to online.

The **Remote Inspection List** includes the following information:

- **Panel ID**: Displays the Panel's unique Visonic identifier. The Panel ID also appears on a sticker on the back of the actual Panel.
- **Web name**: Displays the Panel's given name which allows end-users to use the server to redirect their browser to their PowerLink module's web interface. This feature does not exist on GPRS based control panels.
Working with Panels
- **Account number**: Displays the account number the Panel uses to report to the Central Monitoring Station (CMS).
- **Result**: Shows the outcome of last test performed on each panel. When a test is in progress, a progress bar appears. "Result" and "Last RI" always refer to the last test that was actually performed on the panel, or, if applicable, the status of the test that is currently in progress.
- **Reviewed**: The "Eye" icon indicates test results have been marked as "handled" by operator. Moving the mouse over this icon shows details of the reviewer. If the user was deleted, "non-existing user" appears instead.
- **Last RI**: Shows the date that the last test performed on the panel was initiated.
- **Next RI**: Shows the next date/time a test will be, or was supposed to be, initiated with the panel. If the details appear in red, the test could not be completed.
  "---" means no further remote inspection is scheduled.
- **Repeat**: Shows whether recurring tests are scheduled beyond what is shown in the Next RI column.

Working with the Remote Inspection List

This section describes the actions that can be performed while viewing the Remote Inspection List.

**Starting a Remote Inspection Auto-Schedule for a Panel**

Allows the operator to set the date for the next remote inspection, and also determine whether further remote inspections will be performed periodically.

It is possible to select multiple panels for scheduling. When an inspection is scheduled, the existing "Next RI" value will be replaced with a dotted line.

The default DATE should be today, unless there is already a schedule for next remote inspection, in which case the date is pre-set to the next remote inspection date.

![Schedule Window](image)

**Stopping a Remote Inspection Auto-Schedule (multiple panels)**

This option allows clearing the schedule of automatic Remote Inspections.

To do this, click the Schedule button. In the Schedule window, select Cancel Scheduled Inspection.

**Rescheduling the Next Remote Inspection Date (multiple panels)**

To re-schedule the next remote inspection, select panels and click the Schedule button. Select a new date from the popup.

**Setting Up the Auto-Schedule Period (multiple panels)**

Select multiple panels and click the Schedule button. In the Schedule window, select Choose Repetition.

**Auto-Adding a New Panel for Remote Inspection**

New panels are added to the Remote Inspection management page when they join the server and they are indicated as new in the Remote Inspection page until the first remote inspection test is performed.

**Perform Remote Inspection now (multiple panels)**

This option starts an inspection on demand. It is also possible to initiate inspection on an offline panel. However, the inspection first starts when the panel changes to online.

To initiate an inspection, select panels and click the Initiate Inspection button.
Remote Inspection Test Results

The results depend on the type of test: some either pass or fail, while others provide information on values checked, such as the number of bypassed zones. In the Report Results page you can see:

- The latest tests per panel in collapsible format. The most recent inspection is open by default.
- The test results include the value, result, range, and additional information.

You can use the Mark reviewed button to indicate that the test result has been reviewed. The system indicates the operator name and time of review.

3.8 Performing Actions on Multiple Panels

Overview

This section provides a summary of the operations that can be performed on multiple panels. You can select panels from the list (e.g. All Panels, Faults Monitoring, etc.) and then select operations to perform in the Actions drop-down menu.

The following table lists the actions that may be executed at the same time on multiple panels and the pages from which you execute them.

<table>
<thead>
<tr>
<th>Action \ Page</th>
<th>Remote Inspection list</th>
<th>All panels list</th>
<th>Faults Monitoring list</th>
<th>Suspended Faults</th>
<th>Event list</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-Master FW Upgrade</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>P-link FW Upgrade</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Get Alarm System</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Push Basic Configuration</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Interactive Features Setting</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Panel Assign New CMS IP Address</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>P-Link Password Reset</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mark for Service</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Do RRI now</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Stop auto-RRI</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Start auto-RRI</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mark panel as reviewed/not-reviewed</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Remove Units</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Service complete (cancel call for service)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resolve Faults</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

P-Master / P-Link FW Upgrade

These options allow you to upgrade the PowerMaster / PowerLink firmware. For details, see Performing PowerMaster / PowerLink FW Upgrade.

Get Alarm System Configuration

This option allows you to download the configuration data of the panels to the PowerManage server. For details on this option, see Downloading a Panel’s Configuration.
Working with Panels

Push Basic Configuration

This option allows you to set several configuration parameters to multiple panels. For details on this option, see Downloading a Basic Configuration.

Panel Assign New CMS IP Address

*Note: This option is applicable only for panels with PowerLink 1 module installed.*

This option allows assigning the monitoring and management of registered panels to a PowerManage application installed on a different computer.

1. In the Panel List, select one or more PowerLink supported panels.
2. In the **Actions** drop-down list in the top right corner of the **Panels** page, select **Panel Assign New CMS IP Address**.
3. In the **Assign New IP** box, type the IP Address of the computer to which you want to switch the panel’s management.
4. Click **Start Process**.
**P-Link2 Password Reset**

From the Panel list you can reset the 'Username' and 'Password' on PowerLink1/PowerLink2 supported panels to access the PowerLink web-page.

**Note:** This is not applicable to PowerLink3-supported panels, because it does not have a web page.

To reset credentials:

1. In the Panel List, select one or more PowerLink2 supported panels.
2. In the Actions drop-down list in the top right corner of the Panels page, select P-Link Password Reset. The Reset Password page opens.
3. Define a new 'username' and 'password' that will be used the next time you access the PowerLink web-page.

**Mark for Service**

PowerManage users (operators and administrators) can "leave a message", for example, make a request for service, and attach the message to one or more panels. This message can be directed to a global list or to a specific operator (user role). See "Marking a Panel for Service" on page 15 for further details.

**Performing PowerMaster / PowerLink FW Upgrade**

You can upgrade the PowerMaster / PowerLink firmware. For PowerMaster, upgrade is possible from one specific version to the other. For PowerLink, upgrade is possible between PowerLink modules of the same family.

To perform upgrade:

1. Click on the Panel / P-Link link in the SYSTEM page
Working with Panels

2. Click the **Synchronize with Repository** button in the top right corner. PowerManage will display the list of available packages.

3. Click on the **Manual** link of the required package.

4. Select the check box of the required PowerMaster panel / PowerLink module to upgrade and then click **OK**.
Working with Panels

5. In the PANELS tab, select the check box of the desired PowerMaster panel / PowerLink module.

6. Select the P-Master FW Upgrade / P-link FW Upgrade option from the Actions drop-down menu.

7. Click the Start process button to begin the PowerMaster / PowerLink firmware upgrade.

8. Click Yes.

9. Click on the PROCESSES tab to view the progress of the firmware upgrade.
3.9 Reports

PowerManage enables you to generate and view reports that include information on panels. Reports can be viewed for all the panels enrolled to the PowerManage or for a single panel.

Generating Reports

1. In the Reports Page, click the + Add Report button.

2. In the Report Name box, assign a name for the report.

3. On the left side, click the + Add Panels link and from the screen that opens, select the panels for reporting.

4. Under Recurrence pattern, select either a one-off report, or a daily, weekly, monthly or yearly report (the displayed options depend on the Recurrence pattern choice).

5. For Daily, Weekly, Monthly or Yearly reports, enter the following information in the screen that opens:
   - The frequency of the recurrence of reports
   - The range of recurrence: select the starting date for the recurrence, and then choose if the meeting will always recur (Recur constantly), or end after a number of occurrences; or recurrence until a specified end date.

6. Under Report generating time, select the Start Right Now check box to generate the report immediately or clear it and enter a specific date.
Working with Panels
7. **Under Contents of the Report**, select at least one of the following types of information to be included in the reports:
   - Events
   - Faults
   - Processes
   - RI Tests
8. **Configurations** provides information from panel configurations for reports. For additional information you can contact Visonic.
9. Select between the **PDF** or **CSV** file format for generating the report.
10. Send the report to a recipient in one of the following ways:
    - By Email: select the **Send an Email** check box and enter the email addresses to send the reports.
    - To an FTP server: select the **Send to FTP Server** check box and enter the address of the FTP server (including FTP username, password, and FTP IP address or URL) to send the reports.
11. Click **Start Process**.

**Viewing Reports**
- **For all panels**: In the **Reports** list, select a panel. Click the PDF or CSV file format button to view the report.
- **For a specific panel**: In the **Panels** list, click on a Panel ID and then select **Report Results** in the left side of the page.
3.10 Virtual Keypad

The PowerManage Virtual Keypad mimics the exact behavior of the PowerMaster panel keypad. It enables viewing system status on the display and provides access to the full USER MODE and INSTALLER MODE panel features. Use this keypad to perform all system setup and programming functions. In addition, it allows the CMS to see the panel keys that are being pressed in real time and provides indication upon every key press on the Control Panel.

*Note:* For additional processes to be run on this panel (such as upload/download configurations, RRI, etc.), it is recommended to exit this page and execute the processes as described in the relevant instructions.

Connecting to the Panel

In the Virtual Keypad page, you can connect to the panel and begin to use the Virtual Keypad.

1. In the **Panels** list, select the Panel and then select Virtual Keypad in the left side of the page.
2. Click the **Start** button; after a few seconds, PowerManage connects to the Panel and “CONNECTED” will appear on the top of the Virtual Keypad.
Notes:

1. When a key is pressed on the Control Panel, it is indicated by a colored outline on the corresponding key of the Virtual Keypad.

2. If Panel connection is by GPRS, there may be a delay when exiting the Installer Mode or User Settings.

In addition to the standard Panel buttons, the Virtual Keypad contains an additional four buttons as follows:

- **Panic** - Click to activate Panic alarm.
- **Up** - Click to move one level up in the menu or to return to the previous setting step.
- **Esc** - Click to jump back to the <OK> TO EXIT screen.
- **Off** - Click to delete the current setting without saving and to reset the previous setting.

On the right side of the screen, the following information is displayed:

- A picture of the Panel is displayed. Click on "+" to the right of the picture to enlarge it. Click on "X" to cancel enlarged view.
- Key press is indicated when performed on the Panel Keypad (blue & →) or on the Virtual Keypad (purple & ←).
- A system log records every key press.
- You can filter data in the system log by entering any of the search values in the Search text box.
- **Save to drive** - click to save the log to the PC's hard drive.
- **Clean log window** - click to erase the log.
4. Working with Groups

A “group” is a collection of panels that are managed together and which allow setting parameters that will apply to all panels in the group, such as reporting settings and messaging language definitions.

When working with groups, take note of the following:

- One group, the "Main" group is always defined, and all automatically added panels join the "Main" group.
- All operators are assigned to user-roles. User-roles are associated with groups by editing the user-role (See "Defining User Roles" on page 59).
- It is possible to associate a panel to a single group.
- It is possible to associate more than one group to a user-role.
- It is possible to associate more than one user-role to a group.

*Note:* To see to which group a specific panel belongs, click the Edit Panel button inside the Panel Information page.

The Groups page provides a list of groups and allows defining new groups and deleting groups. The Groups list includes the following information:

- **Name:** Displays the name of the group.
- **Language:** Displays the language for messages.
- **Country:** Displays the country in which the Panel is located.
- **City:** Displays the city in which the Panel is located.
- **Region:** Displays the region in which the Panel is located.
- **Description:** Displays a description of the group, if defined.
- **Video Format:** Displays the type of video format that is sent by email to the panel's defined contact address. Videos can originate from both GPRS and broadband-based systems. The supported formats are AVI, FLV, MP4, and 3GP.

- Use the icon (“User permission”) to define which type of administrators/operators/user roles have permission to access/edit the group data.
- **Online/Total:** Shows the number of Panels in the group that are currently online out of the total number of panels that are enrolled to the group.
4.1 Adding a Group

Follow the instructions below to add a group.

1. Click the Add Group button at the top of the Groups page.

2. Enter the following information:
   - **Group Name**: Enter a name for the group.
   - **Group Description**: A description of the group.
   - **Country/Region/Province/City**: The panels' location.
   - **Messaging Language**: The language for messages that will be sent to the end-user (by SMS, MMS, or email).
   - **Video format type**: The supported video format.
   - **Interactive Pretend bba**: Enabling/disabling interactive management. For panels with PowerLink3 module installed, with user management through the PowerManage Interactive app, select Enabled. For panels with PowerLink2 module installed, with user management through the PowerLink PC application, select Disabled.
   - **Local Wake Up**: Enabling/disabling WakeUp Mode in which the panel responds when receiving an SMS message from the server.
   - **GPRS KeepAlive**: The interval in seconds in which the system checks that the GPRS connection to the Panel is active. Select to enable or disable the GPRS KeepAlive option.
   - **GPRS KeepAlive, sec**: Allowed values are between 120 seconds and 604,800 seconds.
   - **GPRS Offline Timer, sec**: The interval in seconds that the PowerManage server does not receive keep-alive messages, via the GPRS channel, before the Panel goes offline.
     
     **Note**: This interval must be at least 10 seconds more than the interval set for GPRS KeepAlive, sec.
   - **PL/PL2 KeepAlive, sec**: The interval in seconds at which the panel sends keep-alive messages through the broadband channel to the server. Allowed values are between 5 seconds and 86,400 seconds.
   - **BBA Offline Timer, sec**: The interval in seconds that the PowerManage server does not receive keep-alive messages, via the broadband channel, before the Panel goes offline.
     
     **Note**: This interval must be at least 10 seconds more than the interval set for PL/PL2 KeepAlive, sec.
Working with Groups

- **Panel's time synchronization**: Enabling/disabling synchronization of the Panel's clock with the server's clock.
- **PM upgrade method**: Define whether to use the GPRS or the broadband communication channel to perform software upgrade.

3. Click the Central Station Links tab to define the Central Monitoring Station (CMS) automation software, for example, MASTerMind. These group connections appear in a table on the GROUP page (see Adding an Event Reporting Connection to a Central Monitoring Station):
   - **Connection Name**: Enter the connection name to connect to the CMS for reporting purposes. This must be a unique name that is not be used by any other group.
   - **Central Station**: Enter the name of the CMS after defining the Central Station in the System>Central Station page.
   - **Report Type**: Allows filtering the type of information that is transmitted over this connection to the CMS, such as alert, camera trouble, all, etc.

4. Click the Add Link button to link the group to one or more central stations.
5. To add an additional group, select the stay on this page after saving check box.
6. Click the Save changes button to save the Panel details.

### 4.2 Deleting a Group

Follow the instructions below to delete a group.

1. Select the Group entry in the Group List.
2. Click the Remove Group button at the top of the Groups page.

**Note**: The Main Group cannot be deleted.
Viewing and Handling Events

5. Viewing and Handling Events

The Events page provides a list of events that are received from the Panels. The Event List refreshes itself whenever the CMS receives a new alarm or a new event notice (for example, AC Fail, System Arming) from the monitored panel.

The server stores events for 15 days by default. The number of stored events is pre-defined and affects the server's response time; the larger the number of stored events, the slower the server reacts.

Note: To change the history storage period, enter the Management Console and go to Settings>Application Configuration>Resolve>Events & Processes Age.

The Events list includes the following information:

- **Event ID**: Shows the unique number of the event in the list. The symbol next to the event ID indicates the following:
  - ![Camera trouble, Camera being viewed](icon)
  - ![Alarm](icon)
  - ![Alert](icon)
  - ![Information](icon)
  - ![Open/Closed](icon)
  - ![Offline](icon)
  - ![Online](icon)
  - ![X10 on/off](icon)

- **Type**: Displays the type of alert, for example “control panel low battery”.
- **Pics**: When video is available, the camera icon appears [ ]. Click on the icon to see either live video or playback.
Viewing and Handling Events

- **Device/User**: The source that created the event.
- **Panel ID**: Displays the control panel’s ID.
- **Zone**: The zone number where the event occurred.
- **Raw**: Place the cursor over the icon to view the SIA message data (appears only if the source of the event is an SIA message from the panel)
- **Account**: Displays the account number the Panel uses to report to the CMS.
- **Time**: Shows the date and time at which the event arrived to the server; this time denotes the server time.
  Events are sorted by the time at which they were last updated (an event can be updated with more data, for example a new image, after it first reached PowerManage).

**Notes:**

1. The check box indicates whether or not the event was handled (viewed) by the Administrator or Operator. After selecting this check-box, the status of the event changes from "unhandled" event to "handled" event. On the left side of the page, select filters to allow you to view "handled" and/or "unhandled" events.
2. The envelope icon shows whether an email/SMS/MMS message was sent.
3. When an event is handled, the Events column in the Panels list is updated.
4. After changing the event to "handled," it cannot be changed back to "unhandled."

Viewing Events Received from a Specific Panel

In addition to viewing events from panels, you can also view a list of events that are received from a specific panel.

- In the specific panel's page, click the Events button at the top right of the page. The following list appears.

![Events List](image)

In the bottom left of the opened list, click **Go to events page** to take you to the events list received from all panels.

### 5.1 Searching and Viewing Events Data

When viewing the events page it is possible also to:

- Click on the column name to sort according to that field.
- Use the **Search** field to search for specific data, or use the drop-down lists on the left side of the page, to view data based on specific queries.
- Click **More values** to view additional filtering values.
5.2 **Visual Verification of Alarms and Events**

PowerManage works with various alarm automation programs to display streaming video and event-driven video at the CMS.

If the camera icon [ ] appears in the Pics column, visual event verification is available for the location of the event. For example, if an Alarm notification arrives at the CMS, the operator clicks the camera icon to display the video feed from the monitored area and then confirm whether or not a disturbance or criminal act is currently occurring.

- Select **Live View** tab to view real-time video of the selected location (if applicable). It is possible to define, in PowerMaster panels' configurations, when to activate live view, for example, only during AWAY state.
- Select **PIR Cameras** to view on-demand images that were captured by any PIR cameras installed at the location (if applicable; See “Diagnostics” on page 21).
- Select **Playback** to view video segments that were recorded before the present time. To save a playback image, right-click the image, click **Save Image As**, and specify a file name and folder.
6. Working with Processes

Overview

Some panel related tasks cannot be executed immediately by PowerManage, while other tasks take a long time to perform (for example, contacting a panel). These tasks are handled as background processes. The Processes page provides a list of background processes that were performed by PowerManage, or are still in progress.

A process usually is associated with a user (the creator) and panel (on which the process is executed).

The Processes page is useful if you want to check the status of a background task or cancel it.

The Processes page includes the following information:

- **Process**: Displays the process name.
- **Status**: Shows the status of the process:
  - Succeeded: The process ended successfully.
  - Start: The process has started in the server, but not yet started in the panel.
  - Handled: The process is ongoing in the server and in the panel.
  - Failed: The process failed.
- **Details**: If the process failed, provides a description of the error.
- **Description**: Provides additional information of the process.
- **Panel ID**: Displays the control panel's ID. You can click on the panel ID number to view details on that Panel.
- **User**: Displays the name of the user (operator or administrator) who initiated the process.
- **Started**: Shows the date and time the process started.
- **Duration**: Shows the duration of the process (maximum duration is 1 hour; if this time-period is exceeded, the process failed).
- **Handled check box**: Select this check box if the process was handled.
Working with Processes

Viewing the data

When viewing the data you can:

- Click on the column name to sort according to that field.
- Use the Search field to search for specific data, or use the drop-down lists on the left side of the page, to view data based on specific queries.
- Click More values to view additional filtering values.

Viewing Processes Received from a Specific Panel

In addition to checking background tasks of panels, you can also view processes of a specific panel.

- In the specific panel's page, click the Processes button at the top right of the page. The following list appears.

In the bottom left of the opened list, click Go to processes page to take you to the full list of processes.

6.1 Stopping a Process

To stop a process, select the check-box on the left side of the process line and click the Stop button in the top right corner of the Processes page.

**Note:** Some currently running processes cannot be stopped.
7. Performing Administrative Tasks

Note: The SYSTEM page appears only when an administrator or super administrator logs into the web.

The SYSTEM page allows performing various administrative tasks, including the following actions:

- Managing users including managing user accounts, managing user roles, and viewing user’s action logs
- Performing troubleshooting, including:
  - Initiating software upgrades
  - Managing base configurations

7.1 User Management

Overview

PowerManage includes the following types of users:

- **Super Admin**: The Super Administrator has the highest level of permissions and capabilities, and is responsible for creating and deleting regular administrators. This user should only be used to manage the system admin accounts. It is not recommended to use the super admin account for managing operators, groups, panels or any other object in the system.
  
  Every PowerManage server has a single super admin. The super admin cannot be deleted nor can a super admin be created.

- **Administrator**: Administrators are capable of performing all tasks, except deleting administrators. Administrators can create and edit all operators, define user roles, and access all panels.

- **Groups**: Groups are created to easily manage a set of panels. Each panel can be associated to a single group. Groups are managed in the GROUP tab.

- **User-Roles**: These are access rights granted to groups.

- **Operator**: Operators are able to access specific groups of panels to view and/or perform actions (e.g. maintenance, arm/disarm, etc) based on the access rights. Each operator is assigned to a user-role that defines which groups may be accessed.

- **Event Interface User**: This user type is relevant for On-Click users (for example, used by the CMS to receive images of an event). It has the same functionality and permissions as an operator.

- **End-User**: End-users are home residents, using the Visonic Interactive app to access their home security system. The end-user may arm and disarm the panel, view the status of detectors, get alarms, and get image/video verifications.

The SYSTEM>USERS MANAGEMENT section allows you to create or remove user accounts, define and change user roles, and view a log of user’s actions.
Performing Administrative Tasks

Defining a New User

PowerManage users have the following user management permissions:

- Super-administrator can create administrators and “sees” all users (administrators and operators).
- Administrator can create operators and “see” all operators and himself (but no other administrators).

1. Click on the Users link in the SYSTEM page to view the User List.

2. Click the Add User button in the top right corner of the User List. The Add User page appears.

3. Enter the following information:
   - Full name: Enter the user’s full name (mandatory).
   - Email address: Enter the user’s email address. This is the email address that will be used when logging on to the system (mandatory).
   - Phone: Enter a phone number for the user (mandatory).
   - Country: Select a country for the user (optional).
   - Belongs to role: Select the User Role for this account (See "Defining User Roles" on page 59).
   - Password: Define a password for the user. This is the password that the user will use when logging on to the system. Re-enter the password for confirmation.

4. Click Save Changes to save the new user.
Performing Administrative Tasks

Suspending a User

If necessary, you can suspend a user’s account. To do this, select a user or multiple users, and click the **Toggle Suspend User** button. To release the user, click the **Toggle Suspend User** button again.

The word “suspended” will be visible near the user name when a user is suspended.

Defining User Roles

A Role defines the functional responsibilities and permissions of a user. A role includes the Panel Groups that are assigned to its associated users, and the Administrator who supervises the activity of this role's users.

The **Role List** page provides a list of roles, the creator of the role, the type of user to whom the role is assigned, and a link for modifying the permissions for that role.

To define a role for a user:

1. In the **Role List**, click the **Add Role** button in the top right corner of the page. The **Add Role** page appears.

2. Define a name for the role.

3. In the **Parent Role** list, select the role for this user.

4. In the **User Creator** list, select the user who is the supervisor for this role.
Performing Administrative Tasks

5. Under **Unit Groups**, select any or all groups of Panels to which the role will apply.

6. Click **Save Changes** to save the role. The new role is added to the **Role List**.

7. In the **Role List**, locate the role you added and click **Permissions**.

8. Select “allow” or “deny”, as applicable, to determine the permitted and forbidden actions for this role’s users in the Panels, Groups, Events, and Processes pages.

9. Click **Save Changes** to save the permissions.
Viewing the User Action Log

The User Action Log allows viewing a list of actions per user, the time at which the action occurred, and a description of the action.

- To view the User Action Log, select User Action Log in the System page.

7.2 Adding an Event Reporting Connection to a Central Monitoring Station

You can add a connection to a Central Monitoring Station (CMS)'s alarm receiving center through which PowerManage is able to report events. This is done in the SYSTEM page, or via the Management Console (see Central Station Reporting).

Note: Visual verification (ability of the CMS to view images of an event) is only available for systems using either Vis-NAP protocol or any other monitoring software supporting one-click links.

To add a CMS to the system:

1. In the SYSTEM page, click Central Stations in the Settings column.
2. Click the ADD CENTRAL STATION button.
3. In the **Name** box, enter a name for the station.

4. In the **Type** box, select the suitable protocol depending on the Monitoring Station software.

<table>
<thead>
<tr>
<th>Type:</th>
<th>Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Surgard</strong> if you are using MASterMind or any other Monitoring Station automation software using MLR2 protocol.</td>
<td>• MLR 2 Contact Id</td>
</tr>
<tr>
<td></td>
<td>• MLR 2 SIA L2</td>
</tr>
<tr>
<td></td>
<td>• MLR2 SIA L3 with serial</td>
</tr>
<tr>
<td></td>
<td>• MLR2 MAS SIA L3</td>
</tr>
<tr>
<td>Select <strong>FEP</strong> for integration with BOLD's Manitou software.</td>
<td>• FEP XML/CID</td>
</tr>
<tr>
<td></td>
<td>• FEP XML/SIA</td>
</tr>
<tr>
<td></td>
<td>• FEP XML/SYS</td>
</tr>
<tr>
<td>Select <strong>Vis-NAP</strong> for any monitoring station software vendor that supports Visonic's protocol (e.g. ESI, IBS).</td>
<td>• VIS NAP/Visonic</td>
</tr>
<tr>
<td></td>
<td>• VIS NAP/CID</td>
</tr>
<tr>
<td></td>
<td>• VIS NAP/SIA</td>
</tr>
</tbody>
</table>

5. Define the following settings:

   - **Heart beat**: Defines the rate, in seconds, at which the system will check the status of the connection.
   - **Retry time**: Defines the rate at which the retry will be carried out.
   - **Retry count**: Defines the number of retries that are permitted, if the Heartbeat fails.
   - **Connection type**: Select the type of connection e.g. TCP or serial. Depending on the connection type, either define the IP address (also Host Name, Domain) and port (TCP), or the connection type (serial).
   - **Serial port**: Defines the serial Port that will be used for communication.
Performing Administrative Tasks

6. Click the **Save Changes** button.

The Central Station page lists all CMSs registered with the PowerManage server.

- **Deferred**: Select this option if operator confirmation will be required whenever PowerManage sends alarms or events notification to the CMS. This option is applicable for CMSs that have integrated multiple monitoring/reporting systems (in addition to PowerManage).

---

**To link a group of panels to the CMS:**

1. In the **GROUPS** page, click the name of the relevant panel group.
2. Click the **Central Station Links** tab.
3. Enter the **Connection Name** for easy reference.
4. From the **Central Station** list, choose the CMS name.
5. From the **Report Type** list, choose the type of notifications.

---

6. Click the **Save Changes** button.

**Note**: You can also add CMSs to the system in the PowerManage Management Console (see **Central Station Reporting**).

---

### 7.3 Troubleshooting

The **Troubleshooting** menu allows you to manage PowerManage software versions, upgrades and base configurations.

#### Managing Base Configurations

The **Manage Base Configurations** option in the Troubleshooting menu displays a list of configurations. You can click the **Remove Configurations** button to delete the configuration.

### 7.4 Server Maintenance

This box allows you to do the following actions:

- Define Central Stations (see **Central Station Reporting**).
- Define the default behavior of a remote routine inspection
8. Description of Icons

This section provides a list of the various icons that are used in the PowerManage interface.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>📸</td>
<td>Camera trouble, Camera being viewed</td>
<td></td>
</tr>
<tr>
<td>🔔</td>
<td>Alarm</td>
<td>Panic Alarm, Perimeter Alarm, etc.</td>
</tr>
<tr>
<td>🚨</td>
<td>Alert</td>
<td>Telephone Line Failure, Control Panel Low Battery.</td>
</tr>
<tr>
<td>📩</td>
<td>Information</td>
<td>Perimeter Restore, Cancel Alarm, etc.</td>
</tr>
<tr>
<td>🗑️</td>
<td>Open/Closed</td>
<td>Arm Away, Arm Home, Disarm,</td>
</tr>
<tr>
<td>📡</td>
<td>Offline</td>
<td>Went off-line</td>
</tr>
<tr>
<td>🟢</td>
<td>Online</td>
<td>Has come on-line</td>
</tr>
<tr>
<td>🚪</td>
<td>X10 on/off</td>
<td></td>
</tr>
<tr>
<td>🟧</td>
<td>Module PowerLink offline</td>
<td></td>
</tr>
<tr>
<td>🟧</td>
<td>Module PowerLink online</td>
<td></td>
</tr>
<tr>
<td>🟦</td>
<td>Module GPRS offline</td>
<td></td>
</tr>
<tr>
<td>🟦</td>
<td>Module GPRS online</td>
<td></td>
</tr>
<tr>
<td>🟦</td>
<td>GPRS online, KA disabled</td>
<td></td>
</tr>
<tr>
<td>🟦</td>
<td>GPRS offline, KA disabled</td>
<td></td>
</tr>
<tr>
<td>🔒</td>
<td>Arm Away</td>
<td></td>
</tr>
<tr>
<td>🏠</td>
<td>Arm Home</td>
<td></td>
</tr>
<tr>
<td>🔒</td>
<td>Disarm</td>
<td></td>
</tr>
<tr>
<td>📡</td>
<td>Video on demand, Live View</td>
<td></td>
</tr>
</tbody>
</table>
9. PowerManage Administration Console

9.1 Introduction

The PowerManage Administration Console allows setting up a global (i.e. not related to a specific alarm system) policy for various PowerManage features.

The PowerManage Administration Console is usually used only by the IT manager or person who manages the actual server machine, sets up networking, and defines global configurations.

9.2 Getting Started

Logging in

You can access the administration console using one of the following methods.

Local Access

The console can be accessed locally by connecting a keyboard (USB or PS/2) and a monitor (VGA) directly to the server.

Remote Access

The administration console is accessible via SSH. After configuring the network connection, the PowerManage Management Console will automatically open whenever you initiate the connection in the SSH program.

Visonic recommends use of “PuTTY” – a free SSH client application for Microsoft Windows that can be downloaded over the Internet.

Working with the PowerManage Management Console

When using the PowerManage Management Console, select a menu item (left side) or a parameter (right side) with the mouse:

- Use the up and down arrow keys to move up and down the menus.
- Press Enter or Space to select a menu and display relevant parameters on the left side. Pressing <Enter> also selects or enables an option, displaying an X next to the parameter.
- Press <Tab> to go from the menu tree to the parameter panel or in the opposite direction.
- Press <space> to edit a field.
- Press the left arrow to close a tree branch or to return one menu level.
- Press <F12> to exit the console.
9.3 Setting up Sending of Email

The following setup is required to enable any email related features in the PowerManage server, such as sending email notifications. Obtain this information from either your ISP or your IT department.

- A hostname must be set using DNS records of type A and PTR for the PowerManage server to be used in the email sending. This is the name that will appear in the email notification as the sender's email address.
- DNS server's IP address. This information is usually available from your Internet Service Provider.
- Set up a mail-exchange (MX record) entry. This is usually done by your domain registrar.
- Make sure communication on Port 25 can reach the Internet. This is configured in the networking equipment (e.g. Firewall, gateway) to which PowerManage is connected (it is not configured via the PowerManage administration console).

Note: PowerManage is also able to send emails without any configuration. However, in such a condition, the outgoing emails will have a high chance of being blocked by any anti-spam or other defense mechanisms deployed by the recipient's mail server. Therefore, it is recommended to follow the instructions provided below.

Defining External Email Server Settings

In a typical working environment, PowerManage may send a large number of notification e-mails, which consumes a high amount of available memory in your organization's PowerManage server. Using a different (external) server to send EMail notifications to home-owners makes maintenance easier. In the Email settings, configure PowerManage to send emails through an external SMTP server.

Note: The internal server operates by default and does not require any configurations. If you want to use your own external mail server, you need to configure it as described below.

1. In the Main Menu, select the **Application Configuration>Interactive>End user notification>Email Settings** option.

2. Define the SMTP Relay Authentication.
   - **SMTP server**: Hostname of the external email server.
   - **SMTP login**: User name for logging into the email server.
   - **SMTP password**: Password for logging into the email server (special characters such as "!", "#", "$" may not be allowed).
   - **From**: Address that the email recipient will see.
   - **PowerManage Host Name**: PowerManage’s host server name.

3. Press **Apply**.
Sending Server Alerts to an Administrator by Email

PowerManage has the ability to notify the administrator of specific events for example, services being restarted or high usage of resources. In order to set up email alerts for the system administrator, you must define the email address to which the notifications will be sent.

1. In the **Main Menu**, select **Maintenance>Admin notification email**.

2. Enter the email addresses from which the email notifications originate and the addresses to which email alerts will be sent.

3. Select **Apply** to save the configuration.

### 9.4 Sending SMS and MMS Messages

MMS and SMS are sent by the PowerManage Server using an add-on modem device connected to a serial port of the server.

In order to send SMS messages, make sure that this service is enabled at the message broker. Then, define which serial port (ttyS0, ttyM0, ttyM1, ttyM2, ttyM3) will be used to send messages (**System Configuration>Serial Ports**).

**Note:** Moxa ports correlate with the four black wires connected at the back of the server marked P1 to P4; where: ttyM0 is related to P1, ttyM1 is related to P2, etc.

Configuring settings to enable sending MMS messages is similar to the SMS configuration, with the addition of a maximum video attachment size. In addition, the cellular provider details need to be defined. When defining the MMS modem, make sure that the SMS modem is also connected, is defined and has an operational SIM card.

### Setting Up Messaging Options

In the **Messaging Settings** menu, you can set up PowerManage to send notifications by email, email with video-file attachment, SMS, and/or MMS messaging to the end-user.

For example, the PowerManage server is supplied with a message broker for SMS called “Celtius”. In addition, the server can also interface with other remote message brokers that can deliver the SMS.

1. In the **Main Menu**, select the **Application Configuration>Interactive>End user notification>Messaging Settings** option.
2. The following options are available:
   - **Without video**: Event notification messages are sent without image clips.
   - **With video**: Event notification messages are sent with image clips.
   - **SMS enable**: Defines a message broker to send SMS messages. Enter Login and Password for using this service.
   - **MMS enable**: Defines a message broker to send MMS messages and the maximum video attachment size. Enter Login and Password for using this service.

3. Change the settings as necessary and select **Apply Changes** to save the changes and restart the services.

### Setting Up Modems Configurations

1. In the **Main Menu**, select the **Application Configuration>Interactive>End User Notification>Messaging Settings>Celtius Configuration>Modems configuration**.

2. Select the **SMS Modem** option to define the port name for SMS messages. Press the `<Enter>` or <Space> key to scroll among the options.

3. Select the **MMS Modem** option to define the port name for MMS messages. Press the `<Enter>` or <Space> key to scroll among the options.

4. Select **Apply** to save the settings.

*Note*: Values in the pictures are used as examples only. Each MMS provider will require different settings.

5. In the menu tree, select **MMS sender** and enter the number to dial when sending an MMS.
6. Define the details of the cellular provider responsible for the modem’s SIM card in the **Provider configuration** option (this information is usually available from the cellular provider’s web site.)

7. Select **Apply** to save the settings.

8. Go to **Settings>System Configuration>Serial ports** and select the relevant speed for SMS and MMS ports.

9. Make sure that these settings are the actual physical characteristics.

10. Select **Apply** to save the settings.
9.5 Defining SMS Brokers

In order to send SMS notifications, it is necessary to define SMS Brokers. It is also possible to define GSM Modem Wake-up settings.

Adding an SMS Broker

Follow the steps below to add a new SMS broker.

1. Select **Settings>Application configuration>Common>SMS Brokers>Add a new broker**.

2. Select the broker type: **Orange**, **Modem**, **MTN** or **Text Anywhere**.

3. Define the broker name.

4. Select the serial port that will be used for communication (only if using **Modem**).

5. Fill in the additional broker parameters for authentication.

6. Select **Add broker** or **Delete broker**.

Defining GSM Modem WakeUp Settings

Instead of waiting for panels to periodically send signals to the server, PowerManage can initiate working-state communication with the panel by sending wakeup messages (for example, if you need to change any panel settings).

To define Wakeup settings:

1. In the **Main** menu, select **Settings>Application configuration>Receiver>GPRS/GSM Panels**.

2. In the **SMS receivers** field, define the modem path via which the SMS messages are sent.

3. In this menu, press the up/down arrows to define the **Wakeup Broker**.

4. Define the number of **Wakeup retries** that the server will send.
   - 0 - Server does not send any wakeup messages.
   - 1 - One SMS wakeup message.
   - 2 - One wakeup call attempt and if the call fails, one SMS wakeup message.
   - 3 - Two wakeup call attempts and if the calls fail, one SMS wakeup message.
   - 4 - Three wakeup call attempts and if the calls fail, one SMS wakeup message.
   - 5 - Four wakeup call attempts and if the calls fail, one SMS wakeup message.
5. The **Wakeup timeout** field shows the interval between the moment that the server dials the panel, and the start of the next wakeup attempt. This read-only value is provided by the system.

6. Select **Apply** to save the settings.

### 9.6 Setting up "Always-On" Communication

The PowerManage server can maintain a constantly open (Always-On state) communication channel with PowerMaster and PowerMax-type control panels. This makes it easier to change the configuration, arm and disarm the panel, or view the logs. When this feature is selected the GPRS communication is continuously consumed.

This feature is only required for GPRS-based control panels since broadband-based control panels usually poll the server more frequently.

*Note: Enabling "Always-on" also causes high traffic usage.*

1. In the **Main Menu**, select the **Application Configuration>Resolve>Session timeout**.

2. Select the **Infinite timeout** option, which is then indicated by X. When this option is enabled, the **Session timeout (seconds)** setting is disabled.
9.7 Sending Alerts when Panel Communication Fails

If a panel fails to send “keep-alive” reports to the PowerManage server, PowerManage can notify the operator by email or SMS of a communication failure. Enabling this option applies to all GPRS and broadband based systems connected to the server; instructions for each type of system follows. The contact email address used to send the email alerts is defined in the General Panel Information in the PowerManage web interface.

To set up sending of "panel-is-online/offline" alert messages for GPRS systems:

1. In the Main Menu, select Application configuration>Receiver> Keep Alive Handling.

2. Select the **Send email on online/offline** option, which is then indicated by X, to enable sending email when the panel goes offline and online.

3. Select the **Send SMS on online/offline** option, which is then indicated by X, to enable sending SMS when the panel goes offline and online.

4. Select the **Generate 'SYSTEM OFFLINE/ONLINE' events for one-channel panels** option, which is then indicated by X, to enable sending events when the panel changes to offline or online. GPRS/BBA online/offline events are always sent in any case.

5. Select the **Generate 'SYSTEM OFFLINE/ONLINE' events for two-channel panels** option, which is then indicated by X, to enable sending events when the panel changes to offline or online. GPRS/BBA online/offline events are always sent in any case.

6. Select **Apply Changes** to save the settings.

To setup sending of "panel-is-online/offline" alert messages for Broadband systems:

1. In the Main Menu, select Application configuration> Receiver> Broadband panels.

2. Automatic enrollment: Allows automatic registration of the panel, indicated by X. If this option is not enabled, the panel ID must be defined manually in order to allow working with the server.

3. Select **Apply Changes** to save the settings.
9.8 Setting up Local Redundancy

Overview

Local Redundancy allows synchronizing data between two servers to ensure that, in the event that one of the servers fails, the other will continue providing all services without interruption and almost zero downtime (this switching between servers is called a failover).

Redundancy is configured between two servers with identical hardware configuration. One server is the "Active" server and the other is the "Standby" server (also known as "secondary"). The Standby server also has an identical PowerManage system configuration as the Active one. Each server has its own unique IP address, but they are both connected to a single floating virtual IP address (VIP), which in turn is used to communicate with all the panels. This common connection enables both servers to maintain identical PowerManage databases and separate but identical event log files. Any configuration change in the "Active" server is automatically applied to the "Standby" server. Also, if a software update is installed to the Active server, the update is then automatically applied to the Standby server, too.

Caution! Redundancy should be set upon initial server installation. The server's hardware must support redundancy (see below). After setting up redundancy, it cannot be undone without reinstalling the server. As of this release, PowerManage supports redundancy only in servers manufactured by HP.

To set up redundancy:

1. Ensure that you have the following:
   - Two newly installed servers with identical hardware and software configurations (manufactured by HP), the same root password, and a direct connection between them.
   - Two network connections at each server
   - The network connections are as follows:
     - NIC 1 = eth0/2/3 = use to connect to the Internet (Panels)
     - NIC 2 = eth1 = Connects one server to the other (must be connected during redundancy synchronization).
     - NIC 3 = eth2 = unused
     - *NIC 4 = eth3 = unused
     * Applies to HP G8 server models only.
   2. In the Main Menu, select System Configuration>Network Settings.
3. For each server, define unique Host Names (no upper case letters allowed) and IP addresses for eth0; setting of an IP address for eth1 will occur automatically during redundancy synchronization.

4. In the Main Menu, select System Configuration> Date/Time Settings. Set the Date/Time settings, identical to the minute, on both servers.

**Warning:** Prior to enabling redundancy, do not define any other settings.
To enable and synchronize redundancy:

You need to define the redundancy configuration only on one of the servers. During the subsequent synchronization, the identical settings will be applied to the second server.

1. In the Main Menu, select Settings>System Configuration>Redundancy settings>Local Redundancy.

2. In Redundancy state, select on or off to enable / disable the Redundancy option, which is then indicated by X.

   If on is selected, additional options appear.

3. In WAN interface, select the port that is connected to the WAN (panels).
4. In Cross link interface, select the port that physically connects between the primary and secondary servers.

5. Enter the Virtual IP Address, which will be used for communication with the panels.

6. Enter the second server's IP address and password.

7. Select Apply to start redundancy synchronization. The time required for synchronization depends on the size of the servers' hard drives - typically, it will take over 1 hour.

Note: If the synchronization process fails before completion, you must reinstall PowerManage on both servers, in order to prevent system corruption.

By the end of the synchronization, one of the servers is defined as "Active" and the other one is defined as "Standby". The Active server's Management Console displays the complete configuration menu and options, and the Standby server's Management Console displays only minimal, basic configuration settings. Any configuration change in the Active server is automatically applied to the Standby server (even if the changed parameters are not visible in the Standby server's Management Console).

9.9 Setting up Geographical Redundancy

Overview

Geographical Redundancy further increases the reliability of the Power Manage system by providing a remote system to serve as an operational backup for the local system.

Geo-redundancy feature answers the following requirements:

- Operates on sites with a stand-alone system
- Operates on sites with local redundancy system
- Both Active and Standby sites work as receivers all the time
- Master / Slave modes defined manually by system administrator
- Synchronization is done once a night at 4:30 AM local time
- Synchronization is done automatically
- Both the database and the file system are synchronized (*).

(*) File system is synchronized using rsync tool with add-on internal logic, to decrease time and traffic needed for synchronization. (for more info please see: http://rsync.samba.org)

Configuration Process

1. Configure the Standby server.

   a. Select Enable Geo Redundancy.
   b. Select the Secondary node.
   c. In the Peer IP Address box, enter the IP address of the Active server.
2. Configure the Active server.
   - Select Enable Geo Redundancy
   - Select the Primary node.
   - In the Peer IP Address box, enter IP address of the Standby server.
   - In the Peer Password box, enter the SSH password of the Standby server.

3. To run an initial synchronization, press ‘Apply’.

Note:
- The connection between the two sites uses the Virtual IP address that is known to the panels. There is no need to add a dedicated IP address.
- Synchronization is done once a day. In case of failover, the maximum lost data is from the last 24 hours only.
- Geo master and slave roles are defined manually by the administrator.
- The Slave site has a short downtime during synchronization process time.
- For proper installation, all 4 nodes should be online during initial Geo Redundancy setup.
9.10 Viewing Logs

Overview

The following types of logs can be viewed for debugging purposes:

- **Live View**: Allows viewing unfiltered event logs, as they happen.
- **Service Logs**: Allows viewing logs for a specific service/module.
- **Device Logs**: Allow viewing logs per device.
- **Syslog level**: Allows viewing logs per type of event.

View Live Log

- To view live event logs, select **Settings>Logger>Live log** and then press **OK**.
- To stop viewing the live log, press **<Esc>**.
PowerManage Administration Console

Application Profiles

In the Application Profiles page, you can choose the types of messages that will appear in the various types of logs (event, video, msg, etc.).

1. To view logs for a specific service or module, select Settings>Logger>Application profiles.

2. To select the types of messages that appear in the various service logs, navigate in this page by pressing the arrow keys.
   - To enable a message type for a specific log, press <Space> when the cursor is inside the relevant box.
   - To enable a message type to appear in all service logs, navigate to the top of the specific column and press <Space>.
   - To enable a service log to display all message types, navigate to the start of the specific row and press <Space>.

   The following service logs are available:
   - **pic_sender**: Picture dispatcher for MMS and email.
   - **pir_film**: Receiving images from PIR cameras.
   - **sia_server**: GPRS communication.
   - **evt_sender**: Forward of events to the CMS.
   - **msg_sender**: Texting dispatcher for SMS and email.
   - **ipmp_xmlrpc**: Web GUI
   - **pnet_update**: PowerLink Keep-alive messages.
   - **pnet_server**: General PowerLink communication.
   - **repo_sync**: Synchronization of PowerManage with the Repository server.
   - **pnet_notify**: PowerLink events.

3. Select the module for which you want to view logs and then select Apply.

A service from the above list can be started and stopped using a shell command to start service / stop service. The following items can be synchronized with the Repository-Server: XML, PO, Panel-software-upgrade.

Once a day, PowerManage accesses the repository and pulls the files to be updated.
Device Logs

To view logs for a specific device:

1. Select Settings>Logger>Device Log.
2. Enter the ID of the control panel.
3. Select Apply to save the settings.

Setting up the Information Logging Level

To configure which type of events will be logged by the PowerManage server:

1. Select Settings>Logger>Syslog level.
2. Select the log level, e.g. alert, error, or information.
3. Select Apply to save the settings.

Note: For regular use it is recommended to select “Info” option to prevent messages overflow.
PowerManage Administration Console

9.11 Backup, Restore, Upgrade

PowerManage allows you to back up, and restore the configuration file, events, and panel information to/from an external FTP server or a USB drive.

When upgrading to a new version of PowerManage, perform a backup process to save the current system data for restoring after completing the upgrade.

Before starting the upgrade, check the FTP site to verify that your language is supported in the new version (open the **Important. Read before installation.txt** file”). Otherwise, your PowerManage will install and display in the default English language.

**To set up an FTP location**

1. In the **Main** menu, select **Settings>Maintenance>Backup/Restore>FTP Settings**.

![FTP Settings](image)

2. Enter the FTP server’s IP address, the FTP user name and the FTP password.

3. Press **Save Changes**.
To back up PowerManage data to an FTP server:

1. In the Main menu, select Settings>Maintenance>Backup/Restore>Backup.

2. In the Backup method box, select FTP Backup.

3. In the Backup Variants choose the type of data to be backed up. Default application data will always be included in the stored data. It is recommended to not back up all past event images.
   - All data: All application data and configurations, in addition to the default data, will be included in the backup files.
   - All data except past events images: All data except image clips of past events will be included in the backup files.
   - Events, units, groups: All panel data, including panel configurations, groups, and recorded events will be included in the backup files.
   - Central stations, groups: Central stations data is included in the backup files.
   - Users, roles, permissions: User data is included in the backup files.

4. Files list will show the existing files under this directory. Select List dir to choose the relevant directory.

5. In the Path With name to store on FTP box, enter the full path and location on the FTP server for storing the backed up data.


   The backup operation will pack the application data and will send it to the FTP remote site.

Note: The PowerManage services will be shut down while in the backup session and will be up again automatically when the backup operation ends.

To back up PowerManage data to a USB drive:

1. In the Main menu, select Settings>Maintenance>Backup/Restore>Backup.

2. In the Backup method box, select USB Backup.
3. In the Backup Variants choose the type of data to be backed up. Default application data will always be included in the stored data. It is recommended to not back up all past event images.

- **All data**: All application data and configurations, in addition to the default data, will be included in the backup files.

- **All data except past events images**: All data except image clips of past events will be included in the backup files.

- **Events, units, groups**: All panel data, including panel configurations, groups, and recorded events will be included in the backup files.

- **Central stations, groups**: Central stations data is included in the backup files.

- **Users, roles, permissions**: User data is included in the backup files.

4. In the **Choose Device for Backup** list, select the relevant USB device. Press the **Check Device** button to display any drives connected to a server port.

5. In the **Path to store on USB** box, enter the full path and location on the USB drive for storing the backed up data.

6. **Files list** will show the existing files under this directory. Select **List dir** to choose the relevant directory.

7. Press **USB Backup**.

   The backup operation will pack the application data and will send it to the USB drive location.

*Note:* The PowerManage services will be shut down while in the backup session and will be up again automatically when the backup operation ends.
To restore PowerManage data from an FTP server:

1. In the Main menu, select Settings>Maintenance>Backup/Restore>Restore.

2. In the Restore Method box, select FTP Restore.

3. In the Path to restore from FTP box, enter the full path and location on the FTP server of the backed up data.

4. Files list will show the existing files under this directory. Select List dir to choose the relevant directory.

5. Press FTP Restore.

To restore PowerManage data from a USB drive:

1. In the Main menu, select Settings>Maintenance>Backup/Restore>Restore.

2. In the Restore Method box, select USB Restore.

3. In the Restore from device list, select the relevant USB device. Press the Check Device button to display any drives connected to a server port.

4. In the Path to store on USB box, enter the full path and location on the USB drive that contains the backed up data.

5. Files list will show the existing files under this directory. Select List dir to choose the relevant directory.

6. Press USB Restore.
9.12 **Defining PowerManage's Policy for Alarm Systems**

PowerManage allows defining how alarm systems connected to the PowerManage server will be treated/handled. Separate policies exist for GPRS-based systems and Broadband based systems.

**Setting Up Keep-Alive Messages**

When Keep-Alive messaging is enabled, the panel will send a periodic notification to the server, in GPRS protocol, that it is “alive” (it is online and operating normally). If the panel is disconnected, the server will not receive keep-alive messages from that panel.

**To set up Keep-Alive messaging:**

1. In the **Main** menu, select **Settings>Application Configuration>Common>Groups Settings**.

2. Select **GPRS Keep Alive enabled**, indicated by X.

   **Note:** Disabling this option will prevent modifications of panel settings from the CMS via PowerManage; panel setting modifications would only be possible after sending wake-up signals to the target panels (requiring deployment of a modem).

3. For the applicable communication type (GPRS or Broadband):
   - In the **GPRS Keep Alive period** or **BBA Keep Alive period** box, enter the interval, in seconds, at which the Keep-Alive notification will be sent from the panel.

4. For the applicable communication type (GPRS or Broadband):
   - In the **GPRS offline timer** or **BBA offline timer** box, enter the interval in seconds that must elapse for non-reception of keep-alive messages via the GPRS or Broadband channel before the Panel goes offline.

5. Press **Save changes**.
GPRS-based Alarm Systems

To define the GPRS/GSM Mode policy:

1. In the Main menu, select Settings>Application Configuration>Receiver>GPRS/GSM panels.

2. Define relevant options:
   - Automatic enrollment: Allows automatic registration of the panel, indicated by X. If this option is not enabled, the panel ID must be defined manually in order to allow working with the server.
   - SMS receivers: Modem path via which the SMS messages are sent. Also used for sending a wake up notification.

3. Press Apply Changes to save the settings.

Broadband Alarm Systems

To define the Broadband-based policy:

1. In the Main menu, select Settings>Application Configuration>Broadband panels.

2. Define the following option:
   - Automatic enrollment: Allows automatic registration of the panel, which is then indicated by X. If not enabled, the panel ID must be defined manually in order to allow working with the server.

3. Select Apply Changes to save the settings.
9.13 Central Station Reporting

PowerManage can be connected to multiple alarm receiving centers, each with its own event handling system. Defining a central station (CS) requires definition of the actual communication channel that is established between the remote stations (PowerManage) and the central station (CMS). Each physical channel must be defined in PowerManage.

To define a central station communication channel:

1. In the Main menu, select Settings>Application Configuration>Receiver>CMS settings>Add a new CS to define a new central station.

2. In the CS Name box, enter the central station name.

3. In the Type box, select the suitable protocol depending on the Monitoring Station software:

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Surgard if you are using the MasterMind solution or any other Monitoring Station automation software using MLR2 protocol.</td>
<td>MLR 2 Contact Id&lt;br&gt;MLR 2 SIA L2&lt;br&gt;MLR2 SIA L3 with serial&lt;br&gt;MLR2 MAS SIA L3</td>
</tr>
<tr>
<td>Select FEP for integration with BOLD's Manitou software or any FEP-compliant solution.</td>
<td>FEP XML/CID&lt;br&gt;FEP XML/SIA&lt;br&gt;FEP XML/SYS</td>
</tr>
<tr>
<td>Select Vis-NAP for any monitoring station software vendor that supports Visonic's protocol (e.g. ESI).</td>
<td>VIS NAP/Visonic&lt;br&gt;VIS NAP/CID&lt;br&gt;VIS NAP/SIA</td>
</tr>
</tbody>
</table>

Note: Support for images for visual verification will only be available using the One-click method.
4. Define the following settings:
   o **Deferred** – This is an additional central station option that allows sending only events approved by the client. In this case, the client receives an event and decides to send or not to send this event to the central station. If the client decides to send the event, they must approve the event.
   o **Heartbeat enabled**: If enabled (indicated by an X), the system will check the status of the connection at the specified Heartbeat rate
   o **Retry time**: Defines the rate at which the system retries to send the event.
   o **Retry count**: Defines the number of retries that are permitted, if the event wasn’t handled by the central station.
   o **Connection type**: Select the type of connection e.g. TCP or serial. Depending on the connection type, either define the IP address (also Host Name, Domain) and port (TCP) or the connection type (serial).

5. Select **Apply** to save the settings. The new central station name now appears as a station in the CMS Settings branch on the left panel.

6. In the Main menu, select **Settings>Application Configuration>CMS Settings>[new CS branch]**.

7. Press <Enter>, select **Add a new link** and press <Enter> again.

8. In the **Add a New Link** screen, define the following:
   o **Link name**: The central station menu is the system configuration of the central station and links the events rules which include protocol (CID, SIA, etc.), and filter for events (alarms, alerts, restore) which should be sent to central station. A Link uses the CS configuration.
   o **Protocol**: Define which internal protocols will be used (For example, MLR-2 can contain many types of internal protocols).
   o **Profile**: Define for which events visual alarm verification will be allowed (All, alert, alarm, restore, security open close, camera being viewed, camera trouble, home device on off, home device trouble, online, offline, notice).

9. Select **Apply** to save the settings.
### 9.14 Configuring Repository Settings

The Repository provides a central location for commonly used files that can be downloaded by various PowerManage devices, for example: License, XML files for specific panel defaults, PO files for translations, Panel-software-upgrade. Once a day, PowerManage accesses the repository and downloads the files to be updated, based on the profile defined at the server.

**To define repository connection settings:**

1. In the **Main** menu, select **Settings>Maintenance>Repository configuration**.

2. Under **Server**, define the repository IP address.

3. Define the username and password to access the server.

4. Select **Apply** to save the settings.
9.15 License

Since PowerManage version 3.1, the user license is provisioned through the cloud-provisioning server AKA repository.

The number of maximum allowed panels on the server is viewed through the About menu, under the “Limits” section. In this case the server is limited to maximum 50,000 panels to be enrolled.

9.16 Defining External API (VDCP) Settings

This option allows PowerManage to integrate with third party Telco billing applications via a North-Bound API (i.e. VDCP).

To define external API parameters:

1. In the Main menu, select Settings>Application Configuration>Receiver>External API.

2. Define the TCP Port that will be used to communicate with the external API.

3. Define the Login username and Password.

4. Select Apply to save the settings.
Interactive Protocol

The Secured http (https) protocol is used to connect the user to the PowerManage for Interactive services by entering a password.

To enter the password:

1. In the **Main** menu, select **Settings>Application Configuration>Interactive>Web server certificate**.

   ![Web server certificate settings](image)

   - **Pass phrase**: Enter a password to be used for the SSL Certificate. The password should consist of a combination of alphanumeric characters.

   **Note**: Refer to Appendix B for the procedure on how to install the SSL Certificate in PowerManage.

2. In **Pass phrase**, enter a password to be used for the SSL Certificate. The password should consist of a combination of alphanumeric characters.

3. Select **Apply** to save the settings.

Using a Customized Icon

You can change the Visonic logo in the login screen of the Visonic2Go application with an icon of your choice. The icon must first be added to the Repository. After the Repository is synchronized with the server, you can select the customized icon.

To add the customized icon:

1. In the **Main** menu, select **Settings>Application Configuration>Interactive>User Icons**.

   ![User icons settings](image)

   - **Current icon**: Default

2. From the list of icons, select an icon. Note that the icon must be available in the Repository.

3. Select **Apply** to save the settings.
Sending Notifications to Mobile Phones

This feature enables sending Push Notifications to the Visonic2Go app even when the app is closed or not activated.

**Note:** Notifications must be enabled in the management console and in the mobile phone's settings.

**To send notifications to mobile phones**

1. In the Main menu, select **Settings>Application Configuration>Interactive>Push notifications>Common settings**.

   - Select the **Enable push notifications sending** option, which is then indicated by X.
   - In **Select event profiles for push notifications**, select the types of event notifications to be sent.
   - Select **Apply Changes** to save the settings.

**Defining APNS Settings**

You can define whether mobile apps are to be compiled for release (Distribution) or for development and which protocol versions to use for authentication when encrypting messages.

**To define APNS Settings**

1. In the **Main** menu, select **Settings>Application Configuration>Interactive>Push notifications>APNS settings**.

   - In **APNS type**, unless otherwise specified, select **Distribution APNS**, which is then indicated by X.
   - In **SSL/TLS version**, select the protocol version to use for encrypting messages.
Defining Session Parameters

You can define the session parameters for using the mobile phone applications.

To define session parameters

1. In the **Main** menu, select **Settings>Application Configuration>Interactive>REST API Session**.

   - **Max interactive users per panel**: enter the maximum number of mobile phone users per panel.
   - **Max login attempts per device**: enter the maximum number of attempts to log in to the mobile phone application after which login is blocked.
   - **Time to block user if number of login attempts exceeded (seconds)**: enter the period of time in seconds to block unauthorized user login.
   - **Mobile session timeout (seconds)**: enter the timeout period in seconds, following unsuccessful login attempts, before the user can attempt to log in again to the mobile phone application.
   - **Select Apply changes** to save the settings.

9.17 Defining the PowerManage Application Display Language

In this menu, select the display language of the PowerManage application.

1. In the **Main** menu, select **Settings>Maintenance>Languages**.

   - **Use the up/down arrows to select the language**.
   - **Select Apply**.
   - **Restart the application**.
9.18 Auto-Enroll Mask

Auto-Enroll Mask allows the enrollment of only a defined and limited set of panels to PowerManage. Only panels with a Panel-ID that corresponds to the regular expression in the mask are enrolled.

To define an enrollment mask:

1. In the Main menu, select Settings>Application Configuration>Receiver>Autoenroll Mask.

Examples for regular expressions include the following:

- ^$ symbols match the starting/ending position within the string. For example:
  - ^A - only panel-IDs that start with A (A3232C, A22300 etc.) are enrolled.
  - A$ - only Panel-IDs that end with A (32676A, DD323A, etc.) are enrolled.

- . (dot) matches any single character. For example:
  - a.c matches "abc", "a1c", etc.,
    (as opposed to [a.c], which matches only the exact characters "a", ",", or "c").

- (asterisk) matches the preceding element zero or more times. For example:
  - ab*c matches "ac", "abc", "abbc", etc.

- [xyz]* matches any combination of the enclosed characters, such as "", "x", "y", "z", "zx", "zyx", "xyzzy", and so on.

- .* (dot asterisk) matches any symbol.

- [^…] is a NOT expression (include all but…). Any panel with a specified character is NOT enrolled. A hyphen indicates a character set, running from first to last. For example:
  - [^ 7-9] will allow enrollment of any panel ID that does not include 7, 8, or 9.
9.19 Diagnostics

Panels Activity
Enter a specific panel-ID to get more information on the panel status and events.
In the Main menu, select Settings>Diagnostics>Panels Activity.

Emails Activity
Enter a specific email-address to check which emails were sent to this address.
In the Main menu, select Settings>Diagnostics>_emails Activity.
9.20 Setting up Visual Alarm Verification

PowerManage supports the use of the following systems for Visual alarm verification:

BOLD Manitou

PowerManage supports the protocol used by BOLD's Manitou. The protocol is selected and configured from the dialog menus of PowerManage during installation. The integration allows monitoring providers to view images (clips) related to events embedded in the Manitou application.

One-click

Any automation software that allows a web-link (hyper-link) in the event information can be used with PowerManage. In this case the MLR2 protocol is used to relay the event information without the visual information. When the event is processed by the monitoring provider, the operator clicks once on a web-link to view the visual images (clips) from the protected site (link to event-interface-user which allows to see only last 15 events for last 5 minutes or initialize video on demand for specified panel and user). The operator can then view the most recent events on their screen or adjoining screen, along with the images associated with them on-demand.

To configure the one-click option in PowerManage, select MLR2 and add a new user with the "Event Interface User" role in the System page of the PowerManage web page (see 7.1.3).

This method requires adding a simple link to every account on the automation software, in the following format (make sure to write or copy/paste this URL as one line, with no spaces; also, the brackets are placeholders for user-specific information and must not be typed):

http://[powermanage-IP-address]/extern/login/in/el/[user]/p/[password]?page=/event/video/account/[account number]

Where:

- [Powermanage IP address] is the address of PowerManage server.
- [user] and [password] are used to enable the event-user login to PowerManage with the "event-user" role in PowerManage.
- [account number] represents the account number as recorded against that account in the PowerManage event log.

The One-Click method is widely used by several monitoring providers, including those using MASterMind.
MAsterMind using One-click:

The hyperlink is usually added in Mastermind as part of defining the site and client information in a Procedure or a General Dispatch instruction (see the General Dispatch example in the following figure).

In the General Dispatch Instruction example above, the link to the monitoring user account is entered in the Dispatch Instructions box, using the following syntax (remember to include the "<" and ">"; also, replace the text between the brackets with the relevant user-specific information - the brackets are placeholders and must not be typed):

```html
<http://[Powermanage-IP-address]/extern/login/in/e/[user]/p/[password]?page=/event/video/account/[account number]>
```

Where:

- `[powermanage IP address]` is the address of PowerManage server.
- `[user]` and `[password]` are used to log in the user with the "event-user" role in PowerMaster.
- `[account number]` represents the account number as recorded against that account in the PowerManage event log.

Please refer to the example in the figure above.

Visonic's video protocol ("Vis-NAP")

Visonic specific protocol that allows CMS vendors to integrate with PowerManage.
A. Guidelines for Installing SSL Certificate in PowerManage

**Note:** This section applies to PowerManage v3.4.9 and higher.

To increase the security level of PowerManage, Visonic has added support for secure http communication (https) to version 3.4.9 and up. To use this secure communication, a Secure Sockets Layer (SSL) certificate must be purchased and installed in PowerManage, following the below process:

1. The end-customer’s IT department and/or ISP must register its PowerManage server with a host name (for example: marketing.visonic.com).

2. The end-customer should fill in the following details:
   - **Passphrase:** This is the password that will be used for encryption; there are no requirements, but it is recommended that it be a complex combination of numbers, letters and special characters
   - **Country Name** (two-letter code): e.g. UK
   - **State or Province Name** (full name; if not applicable, write the country name): e.g. UK
   - **Locality Name** (region, city): e.g. London
   - **Organization Name** (e.g. company): e.g. Visonic
   - **Organizational Unit Name** (e.g. section, department): This detail is optional
   - **Common Name** (the company name or the server’s host name): e.g. marketing.visonic.com
   - **Email Address:** This detail is optional

The end-customer’s IT department should send the above information to Visonic. After steps 1 and 2 have been completed, Visonic will complete the process.

1. Visonic will send the end-customer a file named "public.csr". This file is the self-signed certificate.

2. The end-customer’s IT department should contact a Certificate Authority (CA) to receive the valid SSL certificate. The customer should send the self-signed certificate ("public.csr") and the applicable payment to the CA. The CA will return the signed certificate.

3. The end-customer should then send Visonic the signed, validated certificate (including the original email that was sent from the CA).

4. Visonic will upload the certificate to the repository, adding HTTPS support to the PowerManage server.
End User License Agreement

B. End User License Agreement

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND VISONIC LTD. ("TYCO") AND GOVERNS YOUR USE OF THE SOFTWARE ACCOMPANYING THIS EULA, WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright or other international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2. GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a. General. This EULA permits you to use the Software for which you have purchased this EULA. Once you have purchased licenses for the number of copies of the Software that you require, you may use the Software and accompanying material provided that you install and use no more than the licensed number of copies at one time. The Software is only licensed for use with specified Licensor-supplied Systems. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b. Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

d. Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to any portion of the Software, or create any derivative works without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. A copy of each applicable third party license can be found in the file README.TXT or other documentation accompanying the Software. Such open source software and other third party software is not subject to any warranty and indemnity set forth in this EULA. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you have a right to receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. A copy of such source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.
End User License Agreement

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

b. Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

8. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY. VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. EXCLUSION OF OTHER DAMAGES. OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, BUSINESS INCOME OR SAVINGS OR THE AVAILABILITY OF ANY DATA OR RECORDS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW
End User License Agreement

LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of Israel, without giving effect to any choice or conflict of law provision or rule that would cause the application of the laws of any jurisdiction other than Israel. Each of the Parties submits to the exclusive jurisdiction of any court sitting in Tel Aviv, Israel for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

9. SPECIAL PROVISIONS FOR POWERMANAGE SOFTWARE. If the Software consists of Tyco’s PowerManage IP/GPRS-based Security Management Platform, then the following additional provisions shall apply to your use of the Software:

a. You may use the PowerManage Software to provide services to your, and your dealer customer’s, end user customers (“Customers”) to remotely access and use the end user functionality of the PowerManage Software, as installed on your hardware, for the sole purpose of remotely configuring, managing and monitoring their intrusion systems, provided that you comply with all applicable privacy and other laws governing your providing such services and access to Customers.

b. License Limitations. You will not, and will not permit any dealer, Customer or other person reasonably within your control to, rent, lease, sub-license, loan, copy, modify, adapt, merge, translate, reverse engineer, decompile, disassemble or create derivative works based on the whole or any part of the Software.

c. You may establish terms and conditions for the engagement of your dealers and the provision of services using the Software to Customers, provided that all such agreements are consistent with the terms of this EULA. You will be solely liable to your dealers and Customers under the terms and conditions of such agreements. Tyco will not be bound by, and you will indemnify and hold harmless Tyco and its affiliates from any claims or demands of any third party arising out of or related to, the grant of any warranties, indemnities, or other terms and conditions greater in scope than those set forth in this EULA.

d. You shall include statements in your welcome kit and/or its agreement(s) with Customer’s to remind them to keep secure their login and password details and comply with all applicable security policies.

e. You shall provide each of your dealers and Customers, and shall cause your dealers to provide each of their Customers, with a written agreement with respect to their access and use of the Software that contains at least the following minimum terms: (i) prohibition against distribution and copying of the Software, (ii) prohibition against making modifications and derivative works of the Software; (iii) prohibition against decompiling, reverse engineering, disassembling, and otherwise reducing the Software to a human-perceivable form; (iv) provision indicating ownership of Software by your Suppliers; (v) disclaimer by Tyco of all applicable statutory warranties, to the full extent allowed by law; (vi) industry standard limitation of liability for Tyco limited to fees paid for the service, including a disclaimer of indirect, special, incidental, punitive, and consequential damages, to the full extent allowed by law; and (vii) all privacy and other end user disclosures required by applicable law. You shall not, and shall ensure that your dealers do not, make any warranty, express or implied, on behalf of Tyco.

f. You shall be solely responsible for:

i. all services you offers and supply to your dealers and Customers;

ii. all of your, your dealer and Customer content, posted, printed, stored, received, routed or created through the use of the Software, including both its content and accuracy;

iii. managing the provision of the service offered by you to your Customers using the Software; and

iv. compliance with all privacy and other laws applicable to your use of the Software and provision of services.

g. You agree that you will comply with applicable all laws and regulations relating to the protection and privacy of the Personal Information of Customers and will utilize appropriate security, technical and organizational measures to protect against unauthorized or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information, in connection with your use of the Software. Personal Information means any information concerning an identifiable individual (including an End User), including information obtained from an End User through the use of Software, such as photos and video.

h. You agree to indemnify Tyco and its affiliates for any claims, damages and expenses (including reasonable attorney’s fees) related to your or your dealer’s failure to comply with this section 9.