PowerManage Installation Guide

Building Technologies & Solutions

www.jci.com

2021-01

D-308291

Rev. 1

Version 4.8

D-308291

End User License Agreement

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

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND TYCO FIRE & SECURITY GMBH ("***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, ACCESSING 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 NOTDOWNLOAD, INSTALL, ACCESS, OR OTHERWISE USE THE SOFTWARE. If this EULA is being agreed to by a corporation or other legal entity, then the person agreeing to this EULA on behalf of that corporation or entity represents and warrants that he or she is authorized and lawfully able to bind that corporation or entity to this EULA. You should print and retain a copy of this EULA for Your records.

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 on a stand-alone basis or 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 laws and 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.

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

a. General. During the term of this EULA, this EULA grants You and Your individual employees a revocable, non-transferable, non-sublicensable, nonexclusive license to use the object code version of the Software and any Documentation for Your internal use only, subject to all Scope Restrictions. The order document under which You have licensed the Software may contain additional terms limiting the scope of Your license, including, but not limited to, a specified number of users or specific systems, licensed facilities, geographic areas, etc. (collectively, "***Scope Restrictions***"). 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. In the event the Software is furnished for use in connection with a particular Tyco (or a Tyco affiliate's) system or hardware product, it may only be used in conjunction with that Tyco(or Tyco affiliate's) system or hardware product. If the Software is furnished embedded in a Tyco (or a Tyco affiliate's) system or hardware product, the Software may not be extracted or used separately from that system or product. "***Documentation***" means Tyco's then-current generally available documentation for use and operation of the Software. Documentation is deemed included in the definition of Software for purposes of this EULA. The term "Software" will be deemed to include any updates, bug fixes, and new versions (collectively, "***Enhancements***") that Tyco may, in its discretion, make available to You. You are responsible for ensuring Your employees comply with all relevant terms of this EULA and any failure to comply will constitute a breach by You. The Software is licensed, not sold. Except for the limited license granted above, Tyco and its licensors retain all right, title and interest in the Software, all copies thereof, and all proprietary rights in the Software, including copyrights, patents, trademarks and trade secret rights.

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 (or a Tyco affiliate) 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. Restrictions. Your use of the Software must be in accordance with the Documentation. You will be solely responsible for ensuring Your use of the Software is in compliance with all applicable foreign, federal, state and local laws, rules and regulations. You may not (i) copy or distribute the Software except to the extent that copying is necessary to use the Software for purposes set forth herein; provided You may make a single copy of the Software for backup and archival purposes; (ii) modify or create derivative works of the Software; (iii) decompile, disassemble, reverse engineer, or otherwise attempt to derive the trade secrets embodied in the Software, except and only to the extent that such activity may be expressly permitted, notwithstanding this limitation or another limitation contained in this EULA, either by applicable law or, in the case of open source software, the applicable open source license; (iv) use the Software for purposes of developing a competing product or service; (v) remove any copyright, trademark, proprietary rights, disclaimer, or warning notice included on or embedded in any part of the Documentation and Software; (v) assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Software, or directly or indirectly permit any third party to use or copy the Software. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA. Under no circumstances will Tyco be liable or responsible for any use, or any results obtained by the use, of the services in conjunction with any services, software, or hardware that are not provided by Tyco. All such use will be at Your sole risk and liability.

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. 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.

e. Trademarks. This EULA does not grant You any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

f. Software Keys. The hardware/software key, where applicable, is Your proof of license to exercise the rights granted herein and must be retained by You. Lost or stolen keys will not be replaced.

g. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

h. Registration of Software. The Software may require registration with Tyco prior to use. If You do not register the Software, this EULA is automatically terminated and You may not use the Software.

i. Compliance with Laws. The use of the Software may require your compliance with local and national laws and regulations,. You are solely responsible for compliance with all applicable laws and regulations relating to the use of the Software, including but not limited to those laws and regulations pertaining to personal data protection, privacy and security.

j. Enhancements. To the extent Tyco makes them available to You, Software Enhancements may only be used to replace all or part of the original Software that You are licensed to use. Software Enhancements do not increase the number of copies licensed to You. If the Software is an upgrade of a component of a package of Software programs that You licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software Enhancements downloaded via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that You are licensed to use the original Software on those Systems.

k. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4. THIRD PARTY SOFTWARE. To the extent any software licensed from third parties, including open source software, (collectively, "***Third Party Software***") is provided with or incorporated into the Software, You will comply with the terms and conditions of the applicable third party licenses associated with the Third Party Software, in addition to the terms and restrictions contained in this EULA. All relevant licenses for the Third Party Software are provided in the Documentation or product files accompanying the Software. 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 may have a right to reverse engineer such open source software or receive open source code for such open source 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. If applicable, a copy of such open source code may be obtained free of charge by contacting your Johnson Controls representative. TYCO MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, WITH REGARD TO ANY THIRD PARTY SOFTWARE. ALL THIRD PARTY SOFTWARE IS PROVIDED "AS-IS," WITHOUT WARRANTIES OF ANY KIND. IN NO EVENT WILL TYCO BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE THIRD PARTY SOFTWARE, EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

5. METERING DEVICES. The Software may contain technology based metering devices and passive restraints to regulate usage. For example, the Software may contain a license file limiting use to the licensed number of concurrent users/devices or named users/devices or may temporarily restrict usage until license and other fees have been paid in full. You acknowledge that such restraints and metering devices are a reasonable method to ensure compliance with the license and have been factored into the license and other fees and the EULA as a whole. You agree that You will not directly or indirectly circumvent, override, or otherwise bypass such metering devices and restraints that regulate the use of the Software.

6. TERM AND TERMINATION. Unless provided otherwise in an accompanying order document, this EULA will commence on the earlier of the date You first download, install, access or use the Software (the "**Effective Date**") and continue in effect for the term specified in the order document or, if no term is specified, until it is terminated (the "**Term**") as provided in this Section. Either party may terminate this EULA on written notice to the other party if the other party is in material breach of its obligations hereunder and fails to cure the breach within thirty (30) days of such written notice. In addition, either party may, in its sole discretion, elect to terminate this EULA on written notice to the other party upon the bankruptcy or insolvency of the other party or upon the bankruptcy or insolvency of the other party upon the commencement of any voluntary or involuntary winding up, or upon the filing of any petition seeking the winding up of the other party. In the event of any claim of intellectual property infringement relating to the Software, Tyco may terminate this EULA on written notice to You and, as Your sole and exclusive remedy, refund the license fees paid, if any, hereunder (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to You). Sections 9 and 10 shall remain unaffected. Upon any termination or expiration of this EULA, the license granted in Section 2 will automatically terminate and You will have no further right to possess or use the Software. On Tyco's request, You will provide Tyco with a signed written statement confirming that the Software has been permanently removed from Your systems.

7. FEES; TAXES. You will pay the fees, if any, associated with the Software. All amounts due hereunder shall be paid within thirty (30) days of the date of the invoice. Payments not made within such time period shall be subject to late charges equal to the lesser of (i) one and one-half percent (1.5%) per month of the overdue amount or (ii) the maximum amount permitted under applicable law. All taxes, duties, fees and other governmental charges of any kind (including sales and use taxes, but excluding taxes based on the gross revenues or net income of Tyco) that are imposed by or under the authority of any government or any political subdivision thereof on the fees for the Software shall be borne solely by You, unless You can evidence tax exemption and shall not be considered a part of a deduction from or an offset against such fees. If You lose tax exempt status, You will pay any taxes due as part of any renewal or payment. You will promptly notify Tyco if Your tax status changes. You will pay all court costs, fees, expenses and reasonable attorneys' fees incurred by Tyco in collecting delinquent fees.

8. LIMITED WARRANTY.

a. Warranty. Tyco warrants that (i) for a period of thirty (30) days from delivery initial delivery of the Software to you (the "***Warranty Period***"), the Software will operate in substantial conformity with its Documentation. If, during the Warranty Period, you notify Tyco of any non-compliance with the foregoing warranty, Tyco will, in its discretion: (a) use commercially reasonable efforts to provide the programming services necessary to correct any verifiable non-compliance with the foregoing warranties; or (b) replace any non-conforming Software; or if neither of foregoing options is reasonably available to Tyco, (c) terminate this Agreement in whole or in part, and refund to You the fees, if any, paid for the non-conforming Software (less depreciation calculated on a three (3)-year straight-line basis commencing on the date of initial delivery to you). Tyco shall not be liable for failures caused by third party hardware and software (including your own systems), misuse of the Software, or Your negligence or willful misconduct. EXCEPT AS PROVIDED IN THIS SECTION, THE SOFTWARE IS PROVIDED ON AN "AS AVAILABLE," "AS IS" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, TYCO AND ITS AFFILIATES, AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, QUIET ENJOYMENT, QUALITY OF INFORMATION, AND FITNESS FOR A PARTICULAR PURPOSE. TYCO AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS DO NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY TYCO OR ANY OF ITS PERSONNEL OR AGENTS SHALL CREATE ANY ADDITIONAL Tyco WARRANTIES OR IN ANY WAY INCREASE THE SCOPE OF Tyco'S OBLIGATIONS HEREUNDER.

b. Exclusive Remedy. Tyco's entire liability and Your exclusive remedy under the warranty set forth in this Section 8 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.

9. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL TYCO AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR INDIRECT DAMAGES, WHICH SHALL INCLUDE, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOST PROFITS, LOST DATA AND BUSINESS INTERRUPTION, ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE ENTIRE AGGREGATE LIABILITY OF TYCO AND ITS AFFILIATES AND THEIR RESPECTIVE SUPPLIERS AND VENDORS UNDER THIS AGREEMENT FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE) SHALL BE LIMITED TO FEES PAID BY YOU FOR THE SOFTWARE, IF ANY, DURING THE THREE (3) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

10. CONFIDENTIALITY. You acknowledge that the ideas, methods, techniques, and expressions thereof contained in the Software (collectively, "***Tyco Confidential Information***") constitute confidential and proprietary information of Tyco, the unauthorized use or disclosure of which would be damaging to Tyco. You agree to hold the Software and Tyco Confidential Information in strictest confidence, disclosing information only to permitted individual employees who are required to have access in order to perform under this Agreement and to use such information only for the purposes authorized by this Agreement. You are responsible for and agree to take all reasonable precautions, by instruction, agreement or otherwise, to ensure that Your employees who are required to have access to such information in order to perform under this Agreement, are informed that the Software and Tyco Confidential Information are confidential proprietary information belonging to Tyco and to ensure that they make no unauthorized use or disclosure of such information. You may disclose Tyco Confidential Information if You are required to do so pursuant to a governmental agency, a court of law or to any other competent authority so long as You provide Tyco with written notice of such request prior to such disclosure and cooperate with Tyco to obtain a protective order. Prior to disposing of any media reflecting or on which is stored or placed any Software, You will ensure any Software contained on the media has been securely erased or otherwise destroyed. You recognize and agree a remedy at law for damages will not be adequate to fully compensate Tyco for the breach of Sections 1, 2, or 10. Therefore, Tyco will be entitled to temporary injunctive relief against You without the necessity of proving actual damages and without posting bond or other security. Injunctive relief will in no way limit any other remedies Tyco may have as a result of breach by You of the foregoing Sections or any other provision of this Agreement.

11. DATA COLLECTION AND USE. You acknowledge and agree that the Software and/or hardware used in connection with the Software may collect data resulting from or otherwise relating to Your use of the Software and/or hardware ("***Data***") for purposes of providing You with service/product recommendations, benchmarking, energy monitoring, and maintenance and support. Tyco shall be the exclusive owner of all Data. Tyco shall have the right to de-identify Your Data so that it does not identify You directly or by inference (the "***De-Identified Data***"). Tyco shall have the right and ability to use the De-Identified Data for its business purposes, including improvement of the Software, research, product development, product improvement and provision of products and services to Tyco's other customers (collectively, "***Tyco's Business Purposes***"). In the event Tyco does not own or is unable to own the De-Identified Data as a result of applicable law, or contractual commitments or obligations, You grant Tyco a non-exclusive, perpetual, irrevocable, fully-paid-up, royalty free license to use, copy, distribute, and otherwise exploit statistical and other data derived from Your use of the De-Identified Data for Tyco's Business Purposes.

12. FEEDBACK. You may provide suggestions, comments, or other feedback (collectively, "***Feedback***") to Tyco and its affiliates with respect to their products and services, including the Software. Feedback is voluntary and Tyco is not required to hold it in confidence. Tyco may use Feedback for any purpose without obligation of any kind. To the extent a license is required under Your intellectual property rights to make use of the Feedback, You grant Tyco and its affiliates an irrevocable, non-exclusive, perpetual, world-wide, royalty-free license to use the Feedback in connection with Tyco's and its affiliates' businesses, including enhancement of the Software, and the provision of products and services to Tyco's customers.

13. GOVERNING LAW AND JURISDICTION.

a. This EULA is governed by and construed in accordance with the laws of the State of Wisconsin, as applied to agreements entered into and wholly performed within Wisconsin between Wisconsin residents. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this EULA, the parties agree to the application of the laws of the country in which You entered into this EULA to govern, interpret, and enforce all of Your and Tyco's respective rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this EULA, without regard to conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply to any such action or proceeding.

b. Jurisdiction. Any action or proceeding brought by either party hereto shall be brought only in a state or federal court of competent jurisdiction located in Milwaukee, Wisconsin and the parties submit to the in personam jurisdiction of such courts for purposes of any action or proceeding. In the event the foregoing sentence is determined by a court of competent jurisdiction to not be enforceable or applicable to an action or proceeding brought by either party relating to or under this EULA, the parties agree all rights, duties, and obligations of the parties are subject to the courts of the country in which You entered into this EULA.

14. GENERAL. This EULA constitutes the entire understanding and agreement between the parties with respect to the transactions contemplated in this EULA and supersedes all prior or contemporaneous oral or written communications with respect to the subject matter of this EULA, all of which are merged in this EULA. This EULA shall not be modified, amended or in any way altered except by an instrument in writing signed by authorized representatives of both parties. In the event that any provision of this EULA is found invalid or unenforceable pursuant to judicial decree, the remainder of this EULA shall remain valid and enforceable according to its terms. Any failure by Tyco to strictly enforce any provision of this EULA will not operate as a waiver of that provision or any subsequent breach of that provision. The following provisions shall survive any termination or expiration of this EULA: Sections 3.a (Restrictions), 3.i (Compliance with laws). 4 (Third Party Software), 6 (Term and Termination), 7 (Fees and Taxes) (to the extent of any fees accrued prior to the date of termination), 9 (Limitation of Liability), 10 (Confidentiality), 11 (Data Collection and Use), 12 (Feedback), 13 (Governing Law and Jurisdiction), 14 (General), 15 (Export/Import), and 16 (U.S. Government Rights). Tyco may assign any of its rights or obligations hereunder as it deems appropriate. **IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT IN THE EVENT ANY REMEDY HEREUNDER IS DETERMINED TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, ALL LIMITATIONS OF LIABILITY AND EXCLUSIONS OF DAMAGES SET FORTH HEREIN SHALL REMAIN IN EFFECT.**

15. EXPORT/IMPORT. The Software is licensed for use in the specific country authorized by Tyco. You may not export or import the Software to another country without Tyco's written permission and payment of any applicable country specific surcharges. You agree to comply fully with all relevant and applicable export and import laws and regulations of the United States and foreign nations in which the Software will be used ("***Export/Import Laws***") to ensure that neither the Software nor any direct product thereof are (a) exported or imported, directly or indirectly, in violation of any Export/Import Laws; or (b) are intended to be used for any purposes prohibited by the Export/Import Laws. Without limiting the foregoing, You will not export or re-export or import the Software: (a) to any country to which the United States or European Union has embargoed or restricted the export of goods or services or to any national of any such country, wherever located, who intends to transmit or transport the Software back to such country; (b) to any user who You know or have reason to know will utilize the Software in the design, development or production of nuclear, chemical or biological weapons; or (c) to any user who has been prohibited from participating in export transactions by any federal or national agency of the U.S. government or European Union. You will defend, indemnify, and hold harmless Tyco and its affiliates and their respective licensors and suppliers from and against any and all damages, fines, penalties, assessments, liabilities, costs and expenses (including attorneys' fees and expenses) arising out of any Your breach of this Section.

16. U.S. GOVERNMENT RIGHTS. The Software is a "commercial item" as that term is defined at 48 CFR 2.101 (October 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 CFR 12.212 (September 1995), and is provided to the U.S. Government only as a commercial end item. Consistent with 48 CFR 12.212 and 48 CFR 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the Software with only those rights set forth herein.

17. SPECIAL PROVISIONS FOR POWERMANAGE SOFTWARE. If the Software consists of or includes Tyco's PowerManage IP/GPRS-based Security Management Platform software, then the following additional provisions shall apply to Your use of the Software:

a. Subject to purchasing the requisite number of licenses, You may use the Software to provide services to Your, and Your authorized dealer'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. 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 You 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 be solely responsible for: (i) all services You offer 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.

f. 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.

g. 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 17.

Contents

Preface

This manual describes the minimum initial configuration, setup, and running of the server. Use this installation guide for the following purposes:

Note: For more information about the configuration, refer to PowerManage 4.8 User Guide.

- To ensure you have the hardware and software requirements to install PowerManage 4.8.
- To install PowerManage 4.8
- To configure PowerManage 4.8

This document is intended for a customer IT team-member with a moderate level of knowledge of servers, and the Technical Support engineer who assists in the process.

The customer must complete the following tasks:

1. Read the relevant sections of the installation guide.
2. Confirm with the Johnson Controls International (JCI) point of contact that all of the pre-installation requirements will be completed by the installation date.

About PowerManage 4.8

PowerManage 4.8 is an efficient web-based host platform that you use to provision and manage home security and automation services supplied by a security service provider. PowerManage 4.8 uses open standard technologies and operating systems. For more information about PowerManage 4.8, refer to the *PowerManage 4.8 User Guide*.

PowerManage installation architecture

Figure 1: Typical PowerManage solution installation architecture

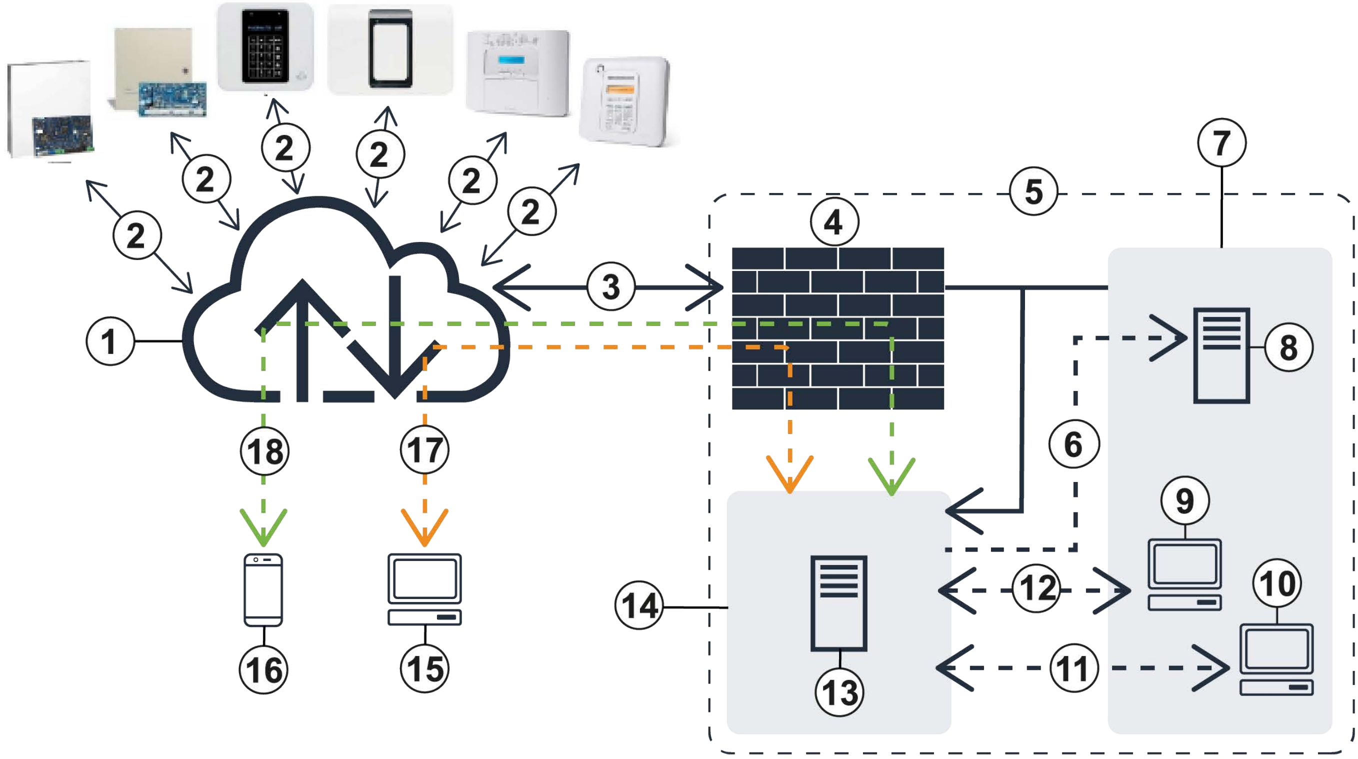


Table 1: Typical PowerManage solution installation architecture

Callout	Description
1	Internet
2	GPRS/Ethernet
3	Events/images Ports: 5001, 8080, 8443, 1303-1305, 3061, and 3062.
4	Firewall
5	Alarm receiving center
6	Events port custom
7	Secure network
8	Automation software
9	Resolve team
10	Administrator
11	SSH and web user interface Ports: 22, 2200, 80, 443
12	Web user interface Ports: 80, 443
13	PowerManage master server node
14	DMZ network
15	L2/L3 tech support
16	End user mobile app
17	SSH and web user interface Ports: 22, 2200, 80, 443
18	Port: 443

Supported hardware for PowerManage 4.8

Hardware requirements for high-performance systems

Table 2: HPE ProLiant DL380 Gen10 5118 2P 64 GB-R P408i-a 8SFF 2 x 800 W PS hardware specifications

Component	Description
Form factor	2U Rack Server
Dimensions (H x W x D)	17.54 in. x 28.75 in. x 3.44 in.
Processor	Intel® Xeon® 5118 (12 core, 2.3 GHz, 16.5 MB, 105 W)
Memory	HPE 64 GB (4 GB x16 GB) Dual Rank x8 DDR4-2666
Storage controller	HPE Smart Array P408i-a SR Gen10 12G SAS Modular Controller
Hard drives	RAID 10 with HP 4 x 1 TB hard drives or a minimum of HP 4 x 600 GB hard drives, SAS 10k 2.5 in. SFF is recommended.
Power supply	(2) 800 W Flex Slot Platinum hot plug power supply kit
ILO	Advanced

Table 3: HP ProLiant DL380 Gen9 E5-2650v3 2P 32 GB-R P440ar 8SFF 2 x 10 GB 2 x 800 W PS hardware specifications

Component	Description
Form factor	2U Rack Server
Dimensions (H x W x D)	17.54 in. x 26.75 in. x 3.44 in.
Processor	Intel® Xeon® E5-2650 v3 (40 core, 2.3 GHz, 25 MB, 105 W)
Memory	64 GB (4 x16 GB) RDIMM
Storage controller	Dynamic Smart Array B140i and Smart Array P440ar/2 GB FBWC
Hard drives	RAID 10 with HP 4 x 1 TB hard drives or a minimum of HP 4 x 600 GB hard drives, SAS 10k 2.5 in. SFF is recommended.
Power supply	(2) 800 W Flex Slot Platinum hot plug power supply kit
ILO	Advanced

For more information on DL380 Gen10 server, refer to the DL380 Gen9 Server manual.

Load benchmarking for high performance systems

Table 4: Maximum simultaneous processes for the 100K system

Process	**Maximum values**
Panel monitoring and management	Up to 100,000 PowerMaster, PowerSeries Neo, and PowerSeries PRO panels in the same system
PowerMaster keep-alive time	GPRS: 600 s
	Broadband: 5 s
PowerSeries Neo and PowerSeries Pro keep-alive time	GPRS: 135 s
	Broadband: 135 s
ITv2 sessions	6,000 notifications a second
Events and alarms	100 events a second
Visual verification	10 events a second
Concurrent FW upgrades	Up to 1,000 upgrades an hour
Concurrent remote inspections	Up to 1,000 an hour
Concurrent CSV reports	Up to 100,000 an hour
Concurrent interactive sessions	2,000 requests a second
Concurrent operators on the PowerManage GUI	100
Event rotation	One rotation every month
Process rotation	One rotation every month

Minimum hardware requirements for mid-performance systems

For more information on the HPE ProLiant DL380 Gen10 server, refer to the HPE ProLiant DL380 Gen10 server manual.

Table 5: HPE ProLiant DL380 Gen10 4110 1P 32GB-R P408i-a 8SFF 1x500W PS hardware specifications

Component	**Description**
Form factor	2U Rack Server
Dimensions (H x W x D)	17.54 in. x 28.75 in. x 3.44 in.
Processor	Intel® Xeon® Scalable 4110 (8 core, 2.1 GHz, 11.00 MB, 85 W)
Memory	HPE 32 GB (2 x 16 GB) Dual Rank x 8 DDR4-2666
Storage controller	1 HPE Smart Array S100i and 1 HPE Smart Array P408i-a SR Gen10 controller
Hard drives	HPE 600 GB SAS 12G Enterprise 10K SFF
Power supply	HPE 500 W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit
ILO	Advanced

For more information on the HPE ProLiant DL380 Gen9 server, refer to the HPE ProLiant DL380 Gen9 server manual.

Table 6: HP ProLiant DL380 Gen9 E5-2620v3 1P 32GB-R P440ar 8SFF 500W PS Base Server hardware specifications

Component	**Description**
Form factor	2U Rack Server
Dimensions (H x W x D)	17.54 in. x 26.75 in. x 3.44 in.
Processor	Intel® Xeon® E5-2620 v3 (6 core, 2.4 GHz, 15 MB, 85 W)
Memory	32 GB (2 GB x 16 GB) RDIMM
Storage controller	Dynamic Smart Array B140i & Smart Array P440ar/2 GB FBWC
Hard drives	8 SFF Chassis, 440ar/2 GB SAS controller
Power supply	500 W Flex Slot Platinum hot plug power supply kit
ILO	Advanced

Load benchmarking for mid-performance systems

Table 7: Maximum simultaneous processes for the 50K system

Process	Maximum values
Panel monitoring and management	Up to 50,000 PowerMaster, PowerSeries Neo, and PowerSeries PRO panels in the same system
PowerMaster keep-alive time	GPRS: 600 s
	Broadband: 5 s
PowerSeries Neo and PowerSeries Pro keep-alive time	GPRS: 135 s
	Broadband: 135 s
Events and alarms	50 events a second
Visual verification	5 events a second
Concurrent FW upgrades	Up to 1,000 upgrades an hour
Concurrent remote inspections	Up to 1,000 an hour
Concurrent CSV reports	Up to 50,000 an hour
Concurrent interactive sessions	Up to 2,000 requests a second
Concurrent operators on the PowerManage GUI	100
Event rotation	One every two weeks
Process rotation	One every two weeks

Hardware requirements for low-cost systems

Table 8: Dell OptiPlex 7060 - Intel Core i5-7500 3.4 GHz - 16 GB

Component	Description
Dimensions	Tower (13.8 in. x 6.1 in. x 10.8 in.)
Processor	Intel Core i5-7500 (6 Cores)
Memory	16 GB 2 X 8 GB DDR4 2400 MHz DIMM
Hard drives	1 x 500 GB SATA

Load benchmarking for low-cost systems

Table 9: Maximum simultaneous processes for the 10K system

Process	Maximum values
Panel monitoring and management	Up to 10,000 PowerMaster, PowerSeries Neo, and PowerSeries PRO panels in the same system
PowerMaster keep-alive time	GPRS: 600 s
	Broadband: 5 s
PowerSeries Neo and PowerSeries Pro keep-alive time	GPRS: 135 s
	Broadband: 135 s
ITv2 sessions	40 notifications a second
Events and alarms	10 events a second
Visual verification	One event a second
Concurrent FW upgrades	Up to 1,000 upgrades an hour
Concurrent remote inspections	Up to 1,000 an hour
Concurrent CSV reports	Up to 10,000 an hour
Concurrent interactive sessions	500 requests a second
Concurrent operators on the PowerManage GUI	Up to 10
Event rotation	One per week
Process rotation	One per week

vSphere virtual machine client requirements

Table 10: Minimum hardware requirements for vSphere client installation hardware specifications

Component	Description
CPU	1 CPU
Processor	Intel or AMD processor with two or more logical cores 2 GHz each.
Memory	4 GB RAM
Hard drives	1 x 500 GB Serial ATA (SATA)

Legacy hardware support

For more information on the HPE ProLiant DL360p G8 server, refer to the [HPE ProLiant DL360p G8 server manual].

Table 11: HP ProLiant DL360p G8 High Performance Server [646904-001] hardware specifications

Component	Description
Form factor	1U Rack Server
Dimensions (H x W x D)	4.32 in. x 42.62 in. x 69.22 in.
Processor	(2) Intel Xeon E5-2650 (8 core, 2 GHz, 20 MB, 95 W)
Memory	32 GB (4 x 8 GB) Registered DIMMs PC3-12800R (1600MHz)
Storage controller	Smart Array P420i/1 GB FBWC (RAID 0/1/1+0/5/5+0/6/6+0)
Hard drives	RAID 10 with HP 4 x 600 GB hard drives SAS 10k 2.5 in. SFF
Power supply	(2) HP 750 W CS Platinum Plus Hot Plug Power Supplies
ILO	Advanced

For more information on the HPE ProLiant DL360p G8 server, refer to the [HPE ProLiant DL360p G8 server].

Table 12: HP ProLiant DL360p G8 Server [670634-S01] hardware specifications

Component	Description
Form factor	1U Rack server
Dimensions (H x W x D)	4.32 in. x 42.62 in. x 69.22 in.
Processor	(2) Intel Xeon E5-2640 (6 core, 2.5 GHz, 15 MB, 95 W)
Memory	16 GB (2 x 8 GB DDR3-1333MHz Low Voltage RDIMMs)
Storage controller	Smart Array P420i/1 GB FBWC (RAID 0/1/1+0/5/5+0)
Hard drives	RAID 10 with HP 4 x 600 GB hard drives SAS 10k 2.5 in. SFF
Power supply	(2) HP 460 W CS Platinum Plus Hot Plug Redundant Power Supplies
ILO	Advanced

Table 13: Dell OptiPlex 3060 - Intel Core i5-8500 hardware specifications

Component	Description
Dimensions (H x W x D)	Small form factor (11.5 in. x 3.7 in. x 11.4 in.)
Processor	Intel Core i5-8500 (6 Cores/9 MB/6 T/4.1 GHz/65 W) Note: The processor base frequency is 3.00 GHz
Memory	8 GB 1 x 8 GB DDR4 2666 MHz UDIMM Non-ECC
Hard drives	3.5 in. 500 GB 7200 rpm SATA

Table 14: Dell OptiPlex 3050 - Core i5 7500 3.4 GHz - 16 GB hardware specifications

Component	Description
Dimensions (H x W x D)	15.4 in. x 27.4 in. x 35 in.
Processor	Intel Core i5-7500 (QC/6 MB/4 T/3.8 GHz/65 W)
Memory	32 GB (max) - DDR4 SDRAM
Hard drives	1 x 500 GB - SATA

Table 15: Dell OptiPlex 3040 - Core i5 6500 3.2 GHz - 16 GB hardware specifications

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

Network and firewall requirements

You can deploy PowerManage 4.8 in a variety of network configurations. You must use a software or hardware firewall between the PowerManage server and the internet. You can use a NAT with or instead of the firewall.
Configure the firewall to use default-deny policy, to allow only the following listed services:

- Estimating the required connection limit
- DNS requirements
- Bandwidth requirements

Estimating the required connection limit

The firewall must support the required connection limit. The highest concurrent connections number is reached in a case when all panels are switched to a new server. During this switch, the discovery process starts for each panel simultaneously. During normal operation, this value is a number of times lower than the limit.

You can estimate the number of new connections per second with the following equation:
R ≈ (NGPRS + NBBA)*5

- R is the number of new connections per second, which depends on the panel's KA configuration.
- NGPRS is the number of GPRS panels enrolled in the server.
- NBBA is the number of BBA panels enrolled in the server.

DNS requirements

To reach the PowerManage instance, you require a DNS hostname with A and PTR records. This a maximum specification to cater for mobile clients.
There are a number of services on PowerManage that initiate outbound connections. This includes public services, such as NTP, DNS, FTP, SMTP; configurable external services, such as SMS brokers, central stations, push notification providers. All outbound connections are initiated from source port range 27000-65333. To avoid blocking the required connections, you must allow all egress traffic.

Bandwidth requirements

The following bandwidth specifications are required, depending on your system:

- For low cost systems, a minimum of 5 Mbit a second for both incoming and outgoing traffic is required.
- For mid-performance systems, a minimum of 10 Mbit a second for both incoming and outgoing traffic is required.
- For high performance systems, a minimum of 100 Mbit a second for both incoming and outgoing traffic is required.

PowerManage 4.8 requires a dedicated link that is not shared with third-party services.

Table 16: List of inbound ports to be forwarded from the firewall to the server

Description	Port	Protocol	Description
PowerMaster Panels	5001	TCP/UDP	Alarm signals/resolve
	8080	TCP/UDP	Alarm images
	8443	TCP/UDP	Alarm images for an encrypted TLS connection
	5555	TCP/UDP	This port is used by the offline handler between the master and primary secondary nodes in GEO redundancy mode.
	9443	TCP/UDP	LTE upgrade
NEO Panels	3061 and 3062	UDP	Fibro alarms and images
	1303 and 1304	TCP	ITv2 alarms/resolve
	1305	TCP	DLS resolve
Web interface	80	HTTP	Resolve web interface
	443	HTTPS	Resolve web interface SSL
	2200	HTTPS	Web MMI console
	8087	HTTPS	Web Interactive
REST API	443	HTTPS	REST API requests with SSL
Administrating	22	TCP	SSH
	161	SNMP	Nagios or other platforms
	162	SNMP	Nagios or other platforms
Extended support (iLO)	443	HTTPS	iLO Web interface
	17990	TCP/UDP	iLO
	17988	TCP/UDP	iLO
Messaging	25	SMTP	Email or email relay
	465 and 587	SMTP	Email or email relay

Rack and power outlet

Ensure you have enough space in your designated server rack to fit a 2U sized server and that there is at least one free power outlet. A second power outlet is recommended because the server has two redundant power supplies. More outlets may be required according to the server configuration described in Supported hardware for PowerManage 4.8.

Network schematics

Figure 2: Standalone diagram for cost effective solutions

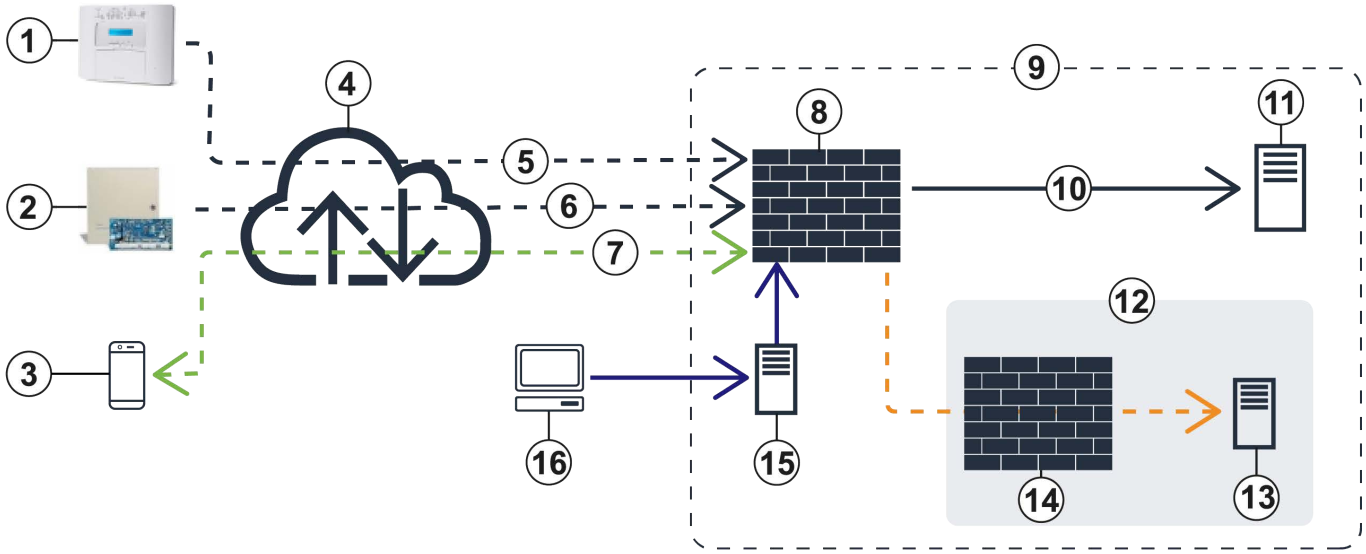


Table 17: Standalone diagram for cost effective solutions

Callout	Description
1	PowerMaster
2	PowerSeries
3	User app
4	Internet
5	IP receiver
6	Integration server IP
7	https://<DNS name>
8	Firewall
9	Alarm receiving center
10	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
11	PowerManage master server node
12	Central station 1
13	Automation server
14	Firewall
15	DMZ server
16	Resolve team

Figure 3: Two node multi-site diagram for hot backup

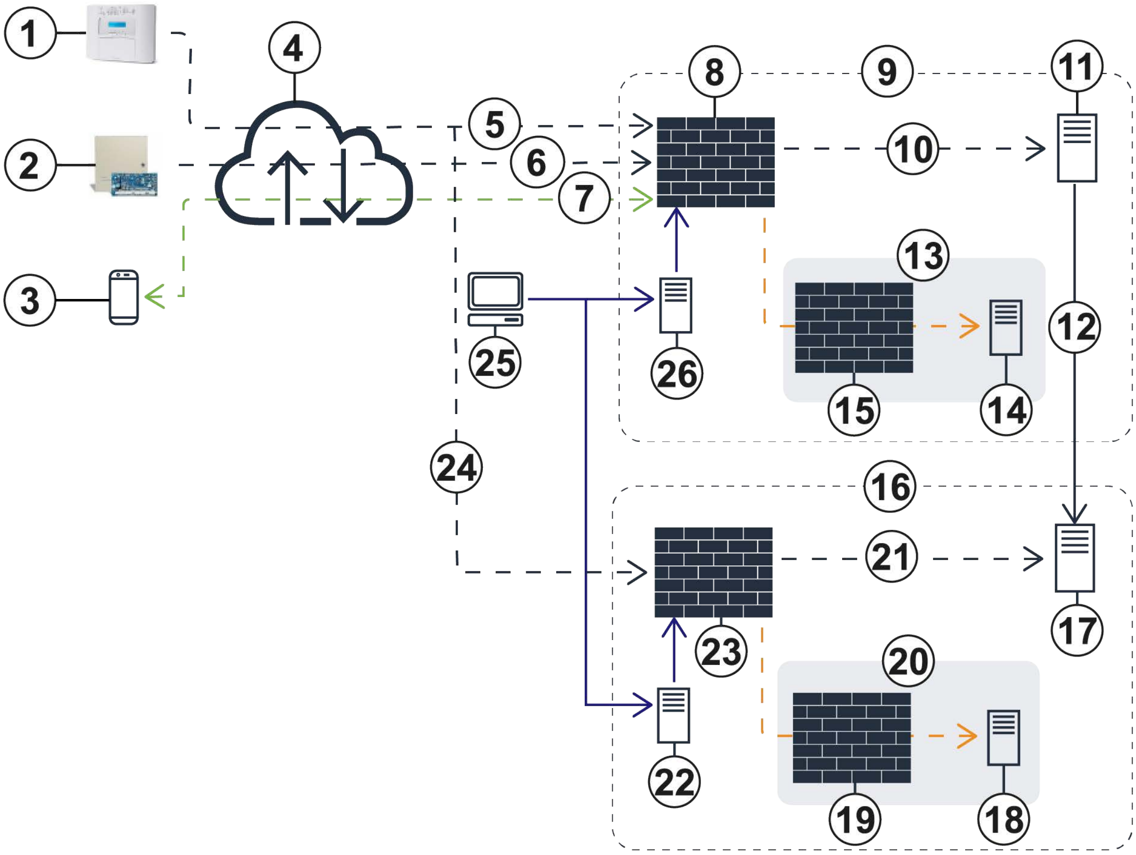


Table 18: Two node multi-site diagram for hot backup

Callout	Description
1	PowerMaster
2	PowerSeries
3	User app
4	Internet
5	IP receiver 1
6	Integration server IP
7	https://<DNS name>
8	Firewall
9	Alarm receiving center 1
10	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
11	PowerManage master server node
12	DB, FS republication via IPsec tunnel
13	Central station 1
14	Automation software
15	Firewall
16	Alarm receiving center 2
17	PowerManage secondary server node
18	Automation software
19	Firewall
20	Central station 2
21	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
22	DMZ server
23	Firewall
24	IP receiver 2
25	Resolve team
26	DMZ server

Figure 4: Four node multi-site diagram for carrier grade

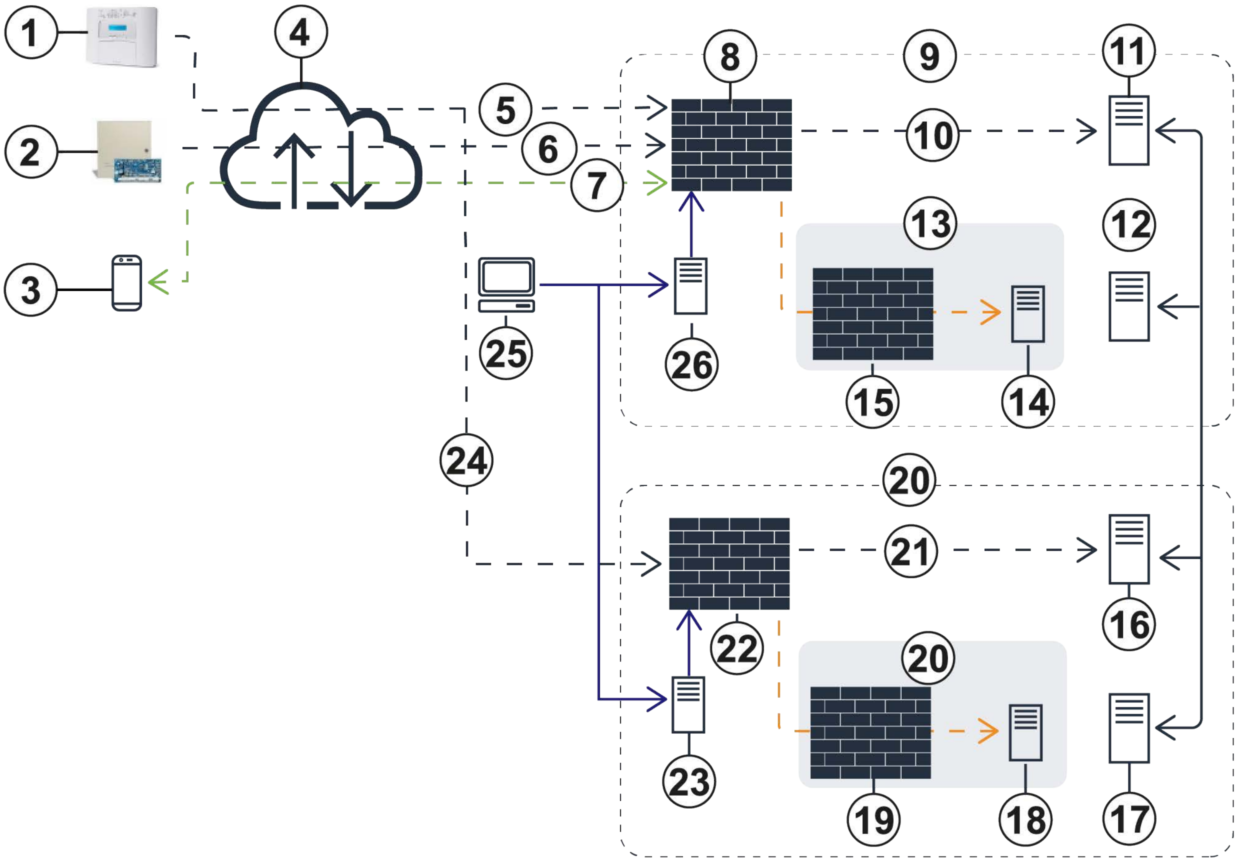


Table 19: Four node multi-site diagram for carrier grade

Callout	Description
1	PowerMaster
2	PowerSeries
3	User app
4	Internet
5	IP receiver 1
6	Integration server IP
7	https://<DNS name>
8	Firewall
9	Alarm receiving center 1
10	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
11	PowerManage master server node
12	DB, FS republication via IPsec tunnel
13	Central station 1
14	Automation software
15	Firewall
16	Primary secondary server node
17	Secondary server node
18	Automation software
19	Firewall
20	Central station 2
21	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
22	Firewall
23	DMZ server
24	IP receiver 2
25	Resolve team
26	DMZ server

Software Requirements

HP Lights-Out Management System

To improve server administration and support, you can use the HP iLO (Integrated Lights-Out) management system to remotely access and control the server. For more about about iLO, refer to the HP website: http://h10032.www1.hp.com/ctg/Manual/c00254396.pdf

The iLO interface requires a separate IP address because it uses a separate Ethernet port.

Client machine requirements for Web and MMI interface access

Table 20: Web and MMI interface access hardware requirements

Processor	Use an Intel or AMD processor with two or more logical cores. The logical cores require a speed of 2 GHz or more
Memory	8GB RAM
Networking	1 GB Ethernet connectivity

Table 21: Web and MMI interface access minimum software requirements

Operating system	Windows 10, Windows 8.1, and Windows 7
	Red Hat Linux, Ubuntu Linux, Linux Mint, Fedora, and Debian
	Mac OS
Browsers	Google Chrome 56+
	Mozilla Firefox 50+
SSH clients	PuTTY
	openssh-client
	SSH client on MAC

Installing PowerManage

Resource requirements

A local network engineer or administrator must be available at the time of installation.
You require the following equipment on site during the installation:

- A USB keyboard
- A console or monitor
- Security panels for testing
- A mobile device to test app functionality

Boot media preparation

You can install the latest versions of PowerManage from the ISO image file with DVD image or USB image media. Choose the medium that best suits your requirements.
Request access to the PowerManage ISO image from your JCI sales representative.

DVD image

DVD images boot directly into the installation environment.
Use the disc burning software on your computer to make an installation DVD. Ensure that the disc burning software is capable of burning discs from image files.

For Windows and Linux systems, use burning tools, such as Nero, ImgBurn, Roxio Creator, Brasero, or K3b to complete the DVD image installation.

Burning an image file to DVD

To burn an image file to DVD, complete the following steps:

1. Insert a blank, writable DVD disc into the computer's disc burner.
2. Launch the disc burning program.
3. In the disc burning program, select the option to burn a DVD from an image file.
4. Browse to and select the ISO image file and select it.
5. Start the burn process.

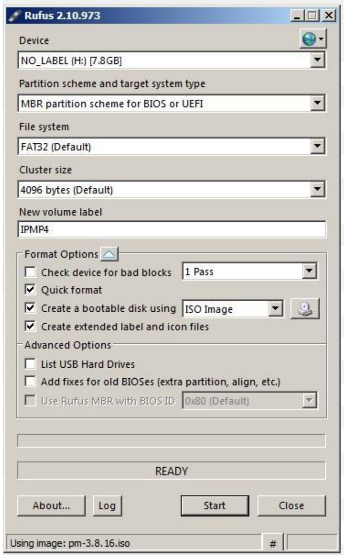
USB image

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

Writing image files to a USB device on Windows

1. Download and launch Rufus.
2. From the **Device** drop-down menu, select the USB drive.
3. In the **New volume label** field, enter the volume name.
4. In the **Format Options** pane, select the **Create a bootable disk using** check box and from the drop-down menu, select **ISO Image**. To select the location of the image, click the disk and find the image path.
5. Click **Start**.
6. In the **Write in DD Image mode** dialog box, click **OK**.

Figure 5: Rufus image writing



Writing image files to a USB device on Linux

Pre-requisite: Sudo user permission is required for this procedure.

1. Insert the USB drive.
2. Open new shell.
3. To locate your USB device, in the shell, type the following command: `fdisk -l`
   Note: Sudo user permission is required for this step and the following steps.
4. Use the `cd` command to change to the directory that contains the PowerManage ISO image.
5. Type the following command: `dd bs=1M if=`<image.iso> `of=/dev/`<device> `status=progress`
   Note:
   - Replace <image.iso> with name of the PowerManage ISO image and replace <device> with the USB drive path.
   - The dd utility requires you to specify the device file that corresponds to the physical media. The name of the device file matches the name assigned to the device by your system. All device files appear in the directory /dev/.

Starting the installation

After you create a bootable USB flash drive or DVD, you can boot the installation.
Use the following default username and password:

- The default username for the MMI is `mmi`.
- The default password is `visonic`.

Important:

- Do not change the default root user. PowerManage is a complete product that is tested and validated with the exact environment and configuration that is provided by your PowerManage distributor. If the installer or the customer installs any additional packages or makes changes to the configuration, you cannot avail of PowerManage support.
- To successfully install the PowerManage, you require a stable internet connection and a DHCP server on the network.

For more information on how to create a bootable DVD, see Burning an image file to DVD.

For more information on how to create a bootable USB flash drive on Windows operating systems, see Writing image files to a USB device on Windows.

For more information on how to create a bootable USB flash drive on Linux operating systems, see Writing image files to a USB device on Linux.

Installing the PowerManage on HP equipment

1. Launch the HP server.
2. Insert the boot USB drive or DVD.
3. Restart the system.
4. To enter the boot menu, on the startup screen, press **F11**. For more information, see Figure 5.
5. Select **Legacy BIOS One-Time Boot** Menu and press Enter.
6. When a dialog box appears, press the Enter key.
7. **Optional**: Choose from one of the following options:
    - For DVD installations, from the list, select **One Time Boot to CD-ROM.**
    - For USB installations, from the list, select **One Time Boot to USB DriveKey**.
8. When the PowerManage installation starts, type one of the following options, depending on your boot media type:
    - For a USB installation: `usb`
    - For a CD or DVD installation: `CD/DVD`
9. When the installation finishes, the server restarts. To log on, enter the following credentials:
    - Login: `mmi`
    - Password: `visonic`
10. To enter a new password and access the MMI menu, when prompted, enter the new password for the Unix user mmi. The password must contain at least eight characters and contain three of the four following character requirements:
    - At least one upper case letter
    - At least one lower case letter
    - At least one number
    - At least one special character

PowerManage installation on Dell equipment

To install the PowerManage with a DVD boot, follow the procedure outlined in Installing the PowerManage on HP equipment.

To install PowerManage with USB on Dell equipment, you need two identical USB drives that contain the same PowerManage image to meet Dell’s BIOS configuration properties. For more information, see Installing the PowerManage on Dell equipment.

Installing the PowerManage on Dell equipment

Pre-requisite: To install PowerManage with USB on Dell equipment, you need two identical USB drives that contain the same PowerManage image to meet Dell's BIOS configuration properties.

1. Insert both boot USB drives or insert the boot DVD into the optical disc drive.
2. Reboot the system.
3. To enter One-Time Boot menu, on the startup window, press F12.
4. From the **One-Time Boot** menu, select one of the following options:
    - For USB installation, select **USB**.
    - For DVD installation, select **CD-ROM**.
5. Complete Step 6 to Step 11 outlined in Installing the PowerManage on HP equipment.

Installing PowerManage on VMWare

Pre-requisite: To install PowerManage on VMWare, the virtual environment requires a server with VMWare and PowerManage ISO image installed.

Adding a network to your VM

1. Login to vSphere client.
2. To add a new adapter to the virtual machine, in the navigation tree, click the virtual host.
   Note: You must add at least one adapter to the virtual machine.
3. On the **Configuration** tab, from the **Hardware** navigation tree, select **Networking**.
4. To the top-right, click **Add Networking**.
5. In the **Add Network Wizard** dialog box, from **Connection Types**, enable **Virtual machine** and click **Next**.
6. In **Network Access**, enable **Create a vSphere standard switch** and select the check box of the Ethernet adapter you want. Click **Next**.
7. In **Connection Settings**, from the **Port Group Properties** pane, enter the adapter name in the **Network Label** field.
8. Click **Next**, then **Finish**.

Uploading the Power Manage image file to the VM data store

1. From the navigation tree, click on your virtual machine.
2. On the **Configuration** tab, from the **Hardware** pane, select **Storage**.
3. From the **Datastores** pane, right click the datastore that you want, and click **Browse Datastore**.
4. In the **Datastore Browser** window, click the datastore upload icon and click **Upload file**.

Adding a new virtual machine

1. From the navigation tree, right click your virtual host and click **New Virtual Machine**.
2. In the **Create New Virtual Machine** window, from the **Configuration** pane, enable **Typical**. Click **Next**.
3. From the navigation tree, click **Name and Location**. In the **Name** field, enter your virtual machine name, and click **Next**.
4. From the navigation tree, click **Storage**. From the **Select a destination storage for the virtual machine files** pane, select the data storage destination you want. Click **Next**.
5. From the navigation tree, click **Guest Operating System**. From the **Guest Operating System**, enable **Linux**.
6. From the **Version** drop-down, select **Red Hat Enterprise Linux 6 (64-bit)** and click **Next**.
7. From the navigation tree, click **Network**. In the **Create Network Connections** pane, from the **Network** drop-down, select the network connection you configured previously.
8. From the **Adapter** drop-down, select the adapter you configured previously. Enable **Connect at Power On** and click **Next**.
9. From the navigation tree, click **Create a Disk**. From **Virtual disk size**, select the virtual disc size. The minimum requirement is 120 GB. Enable **Thick Provision Lazy Zeroed.** Click **Next**, then click **Finish**.

Configuring a new virtual machine

1. In the **vSphere Client**, from the navigation tree, right-click the new VM and click **Edit Settings**.
2. In the **Virtual Machine Properties** window, complete the following steps:
3. From the **Hardware** pane, click **Memory**.
4. From **Memory Size**, select a memory size of at least 4 GB.
5. From the **Hardware** pane, click **CPU**.
6. Select the number of virtual sockets and cores per socket from **Number of virtual sockets** and **Number of cores per socket** drop-down menus.
7. From the **Hardware** pane, click **SCSI controller 0**.
8. From **SCSI Controller Type**, click **Change Type...**.
9. In the **Change SCSI** dialog box, from **SCSI Controller Type**, enable **LSI Logic Parallel** and click **OK**. Select a memory size of at least 4 GB.
10. From the **Hardware** pane, click **Network adapter 1**.
11. In **Network Connection**, from the **Network label** drop-down, select your network adapter.
12. From the **Hardware** pane, click **CD/DVD drive 1 (edited)**.
13. In **Device Status**, select the **Connect at power on** check box.
14. From the **Network label** drop-down, select your network adapter.
15. To connect the PowerManage image to the VM, in **Device Type**, enable **Datastore ISO File** and click **Browse**.
16. In the **Browse Datastores** window, select the image file that you want and click **Open**.
17. In the new virtual machine window, click the DVD settings icon, and select your CD/DVD drive.
18. Click **Connect to ISO image on a datastore**.
19. To boot the PowerManage installation, launch the virtual machine and input `cdrom`.

Post installation

When you finish the installation, the system is ready to use. Other administrative tasks may still be necessary, depending on how you plan to use your system. This section describes some of the common tasks to perform immediately after a new installation.

Changes in PowerManage 4.8

LTE upgrade

For more info about LTE Upgrade refer to the PowerManage 4.8 User Guide.

Initial setup

Complete the initial setup procedure to configure several system parameters that are required for the system to operate.

Network configuration

Configure the network settings to set the network's controls, flow, and operation to support the network communication of PowerManage products. This process involves multiple configuration and setup processes on network hardware, software, and other supporting devices and components.

Configuring the network

1. Open the MMI menu.
2. From the navigation tree, select **System**, and from the **System** list, select **Network**.
3. From the **Network** list, select **Interface Properties**.
4. In the **Interfaces Properties** pane, in **Hostname**, enter your servers' hostname. For more information, see Figure 6.
5. In the **DNS servers** field, enter your DNS. If required, you can enter a secondary or tertiary DNS in the **DNS servers** field.
6. Complete one or more of the following options. For more information, see Figure 7:
   Note: The 'X' in **ethX** is the number of your interface.
   - If your server obtains its IP address by DHCP, enable **network interface ethX on/off** and enable **ethX dhpc on/off**.
   - If you want to configure a static IP address for your server, disable ethx dhcp on/off and enter the IP address, Netmask, and Gateway in the **ethx IP address**, **ethx Netmask**, **ethx Gateway** fields.
7. Click **Apply changes**.

Figure 6: Interface properties DNS configuration

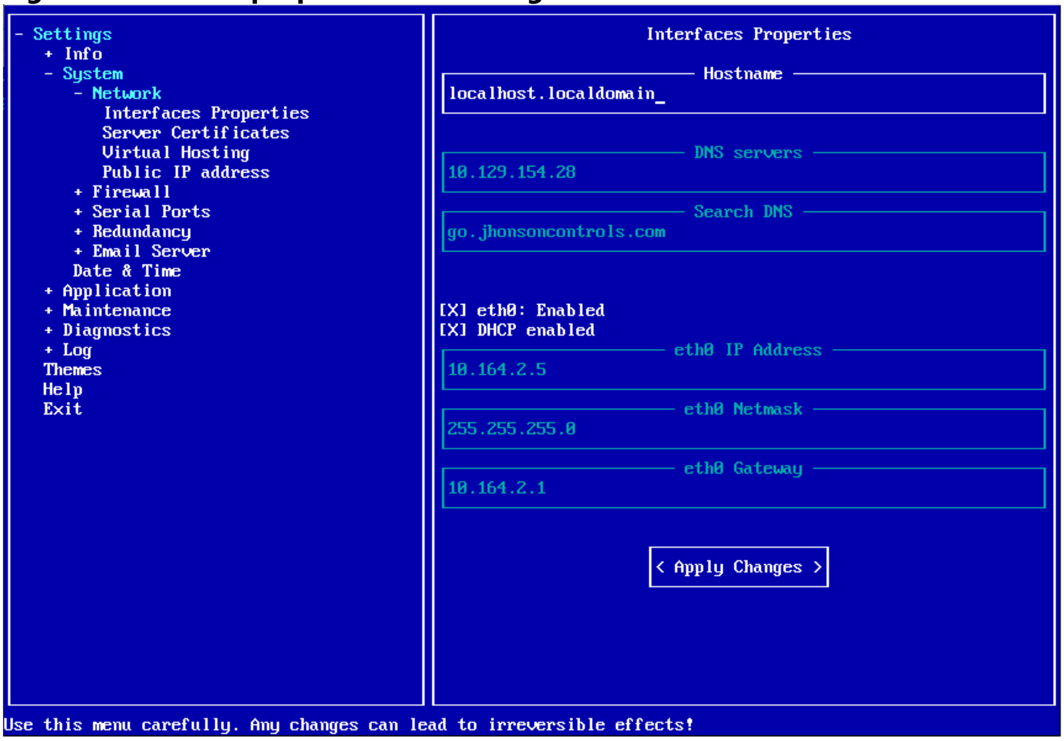
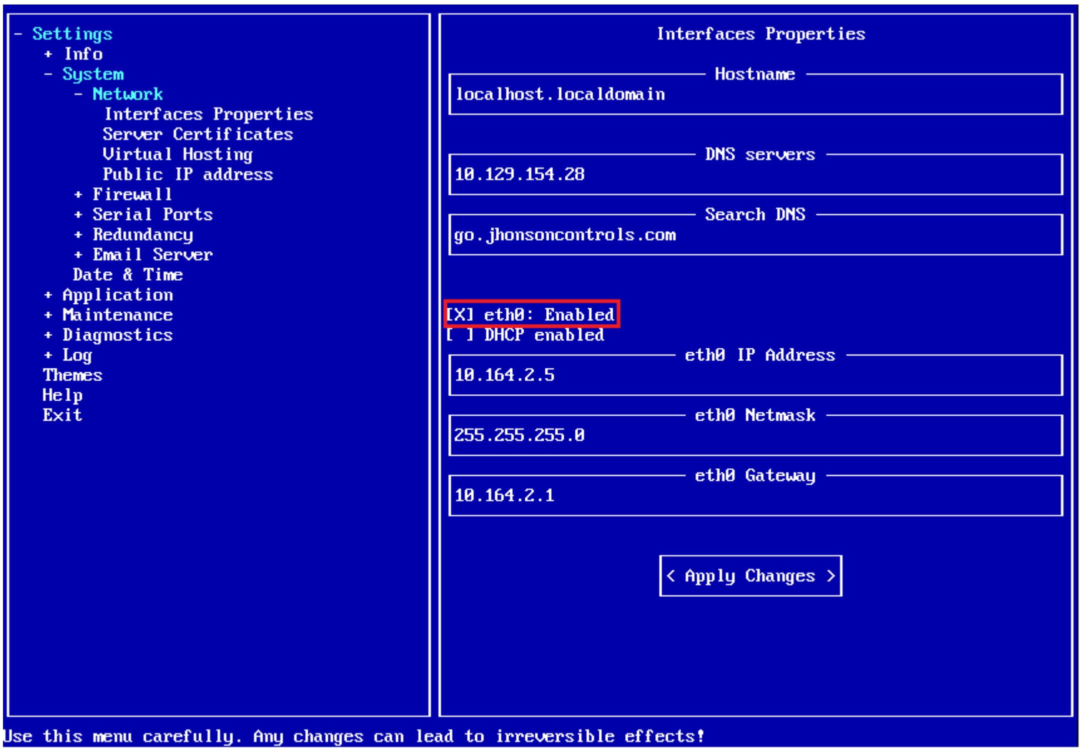


Figure 7: Ethx configuration



Configuring time synchronization

Network Time Protocol (NTP) synchronizes date and time information on networked computer systems with a common internet reference.

1. Open the MMI menu.
2. In the navigation tree, from the **System** list, select **Date & Time**.
3. From the **Select Time Zone** list, select your time zone.
4. Enter **NTP servers.**
5. Press **Apply changes.**

Configuring the repository

Use a repository to store firmware packages, localization, licenses, icons, events mapping, and more. You can retrieve and install repositories on a PowerManage server.

1. Open the MMI menu.
2. In the navigation tree, from the **Settings** list, select **Maintenance**, then select **Repository**.
3. Enter the repository IP address in the **Server IP Address** field.
4. Enter the domain name in the **Server FQDN** field.
5. In the **Username** field, enter a new repository account username.
6. In the **Password** field enter a new repository account password.
7. Click **Apply Changes**.
8. To synchronize with the repository, click **Sync Repository**.

Assigning SSL certificate to the Power Manage

To use HTTPS connections to the PowerManage Web Interface, Web Console and use Web/Mobile interactive services, it is required to add and apply SSL certificates to the server. For more information, see Appendix A.

Pre-requesite: Connect your server to the repository and add and assign the required SSL certificates to your Repo account. Verify that the server is synchronized with the repository. For more information, see Appendix A.

1. Open the MMI menu.
2. In the navigation tree, from **Settings**, select **Network**, then select **Interface Properties**.
3. In the **Hostname** field, enter your DNS name.
4. In the navigation tree, from **Network**, select **Server Certificates**.
5. From the **Select SSL Certificate SN** list, select the required certificate.
6. In the **Enter Passphrase** field, enter a new passphrase.
7. Click **Apply Changes**.

Configuring virtual hosting

Use virtual hosting to host multiple domain names on a single server. Each domain name is handled separately.

1. Open the MMI menu.
2. In the navigation tree, from **Settings**, select **Network**, then select **Virtual Hosting**.
3. From the **Select service** list, select one of the following services:
    - **LTE upgrade host**: Communicates between the LTE Modem and the server during the LTE Modem upgrade process.
      Note: You must enter a hostname in the **Hostname** field.
    - **PowerNet Host**: Enables communication between the plink and the server.
    - **Web Interactive**: Control and monitor panels using a web browser.
    - **Web Interface and Mobile Interactive Host**: Resolve alarms and alerts, and perform maintenance using the web browser and control and monitor panels using mobile app.
    - **Web MMI Console**: Use the MMI interface using a web browser.
4. Choose one of the following port numbers:
    - To add an unencrypted port, in **Port**, enter `80`.
    - To add two unencrypted ports, in **Port**, type `8080`.
    - To add an encrypted port, in **SSL Port**, type `443`.

    Note: If the **Port** or **SSL Port** fields are empty, the PowerManage cannot connect to the network with `https://` or `http://`
5. In the **Hostname or IP Address** field, enter a hostname or IP address. Configure hostname for encrypted connections.
6. From the **Certificates SN** list, select a certificate. All keys that are available are in the **Certificates SN** list.
7. Click **Apply Changes.**

To access a specific service, from your browser, enter the following command: *<server URL>*:*<port number>*

Common post-installation tasks

After you finish the installation and go through one of the methods described in Initial setup, your system is ready for use. However, other administrative tasks not covered by the initial setup utilities may still be necessary, depending on how you plan to use your system.

The following list describes some common tasks that you can perform after a new installation:

- Applying a patch.
- Reverting a patch.
- Backing up files to the FTP server.
- Scheduling backups to the FTP server.
- Backing up files to a USB drive.
- Scheduling backups to the FTP server.
- Restoring data from an FTP server.
- Restoring data from a USB flash drive.

ITv2 protocol

ITv2 protocol is used for one-to-one communication between an integration module and a third party integration server or device. It is a peer to peer relationship: both sides can initiate a command or response packet exchange.

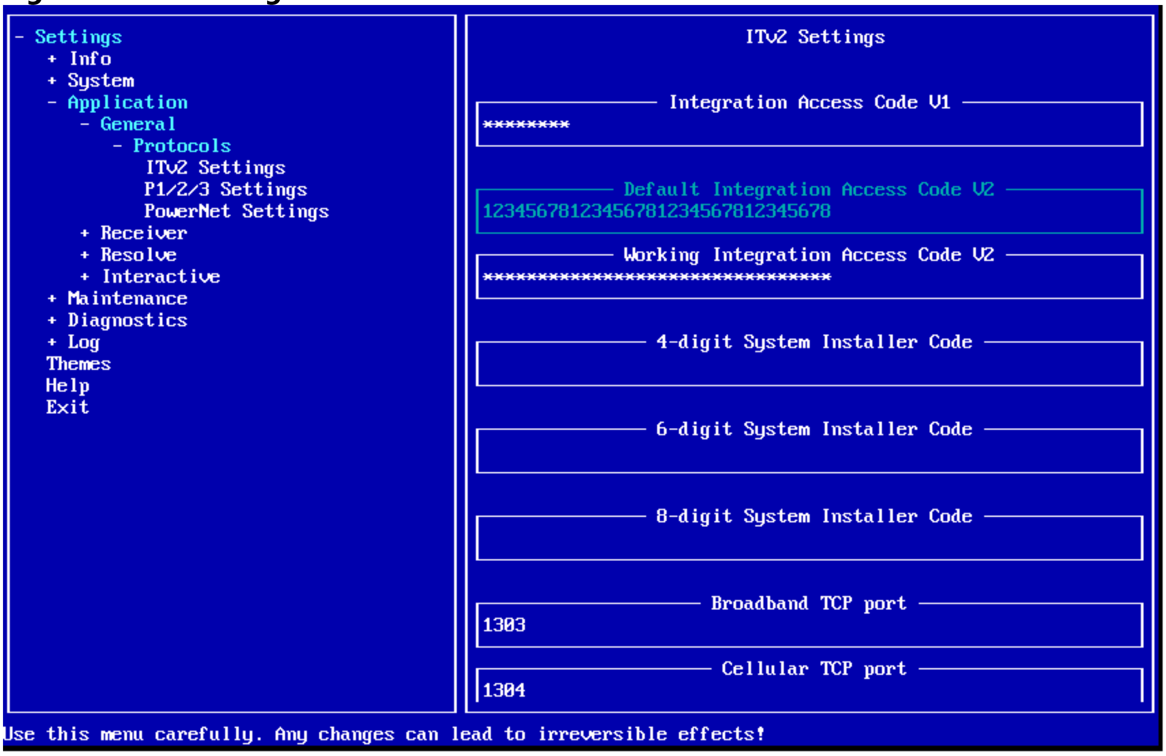
ITv2 protocol for Neo and PSP panels

The Neo and PSP (Power Series Pro) panels communicate with the power-manage server via ITv2 protocol that is encrypted with a working integration access code.

Earlier Neo panel versions have an eight-character integration code which must be identical to the Integration Access Code V1 field. For more information, see Changing the working integration access code.

Newer Neo and PSP panels have a 32-character integration code with a default value of `12345678123456781234567812345678`. For more information, see Default Integration Access Code V2 in Figure 8. The server automatically changes the default code to the Working Integration Access Code V2 value. For more information, see Working Integration Access Code V2 in Figure 8.

Figure 8: ITv2 settings



Changing the working integration access code

The working integration process starts various applications. Complete the following steps to change or enter a new working integration access code:

Note: You do not need change the default value for Working Integration Access Code V2. If you want to change the value for Working Integration Access Code V2, complete the following procedure before you enrol panels in the server. Panels that are already enrolled in the server disconnect when the access code changes.

1. In the MMI menu, select **System**, and then **Application**.
2. Select **General**, then **Protocols**, and **ITv2 Settings**.
   Note: You cannot change the **Default Integration Access Code V2** value.
3. In the **Working Integration Access Code V2** field, enter a new access code.

Note: To connect a new Neo panel enrolled in the server, or an enrolled PSP panel that you reset to the factory default, complete the procedure in Connecting a new Neo panel or a PSP panel that you reset to default.

Connecting a new Neo panel or a PSP panel that you reset to default

1. Complete the procedure in Changing the working integration access code.
2. In the panel menu, select **panel**, then select **ACTIONS**.
3. To reset the panel encryption, select **BBA/GPRS Encryption**, then select **BBA/GPRS Encryption**, and **disable**.
   Step result: The server automatically changes the access code in the panel and sets **BBA/GPRS encryption** to **enable**.

Applying a patch

1. Open the MMI menu, in the navigation tree, from **Settings**, select **Maintenance**, then select **Patches**.
2. From the **Patches** list, select the patch file you want.
   Note: The **Patches** list contains only patches that are available for your server.
3. Click **Apply Changes**.

Note:

- Apply patches manually.
- To apply multiple patches, complete this procedure for each patch in order and with one patch at a time. For example, apply patch 1.1.1.1 first, then apply 1.1.1.2, and 1.1.1.3, until all patches are applied.
- Patches that you apply successfully appear in the **Installed Patches: Select Patch to Revert** list. To revert a patch, see Reverting a patch. Some auto applied patches may not display in the **Installed Patches: Select Patch to Revert** list.

Reverting a patch

1. Open the MMI menu, in the navigation tree, from **Settings**, select **Maintenance**, then select **Patches**.
2. From the **Installed Patches: Select Patch to Revert** list, select the patch you want to revert.

The patch is removed from the **Installed Patches: Select Patch to Revert** list.

Backing up files to the FTP server

1. In the MMI menu, in the navigation tree, from **Maintenance**, select **Backup/Restore**, then select **FTP Settings**.
2. In the **Host IP address** field, enter your host IP address.
3. In the **User** field, enter your username.
4. In the **Password** field, enter your password and click **Save changes**.
5. In the navigation tree, from **Backup/Restore**, select **Backup**.
6. In the **Select Backup Interface** field, enable **FTP**.
7. In the **Backup path** field, enter the absolute path and filename that you want to create.
8. **Optional:** To include alarm images in the backup file, enable the **Backup Alarms' images** checkbox.
   Note: If there are more than 1.5 million image files, do not include images in the backup. It may take up to 2 hours to perform a backup, which can render some information out of date.
9. **Optional:** To list backup files in the directory, click **Show Files**.
10. Click **Perform backup now**.
11. When the backup completes successfully, press the escape key on the keyboard.

Scheduling backups to the FTP server

1. In the MMI menu, in the navigation tree, select **Maintenance**, then select **Backup/Restore**.
2. From **Backup/Restore**, select **Backup**.
3. In **Select Backup Interface**, enable **FTP**.
4. To include alarm images in the backup file, enable the **Backup Alarms' images** checkbox.
   Note: If there are more than 1.5 million image files, do not include images in the backup. It may take up to 2 hours to perform a backup, which can render some information out of date.
5. **Optional:** Click **Show Files** to browse any available drives.
6. In the **Backup path** field, enter the absolute path and filename that you want to create.
7. Select the **Schedule the backup** checkbox.
8. In the **Set time (hh:mm)** field, enter the time for when you want the backup to occur.
9. In the **Select days** pane, select one or more days when you want the backup to occur.
10. Click **Save Schedule**.

Backing up files to a USB drive

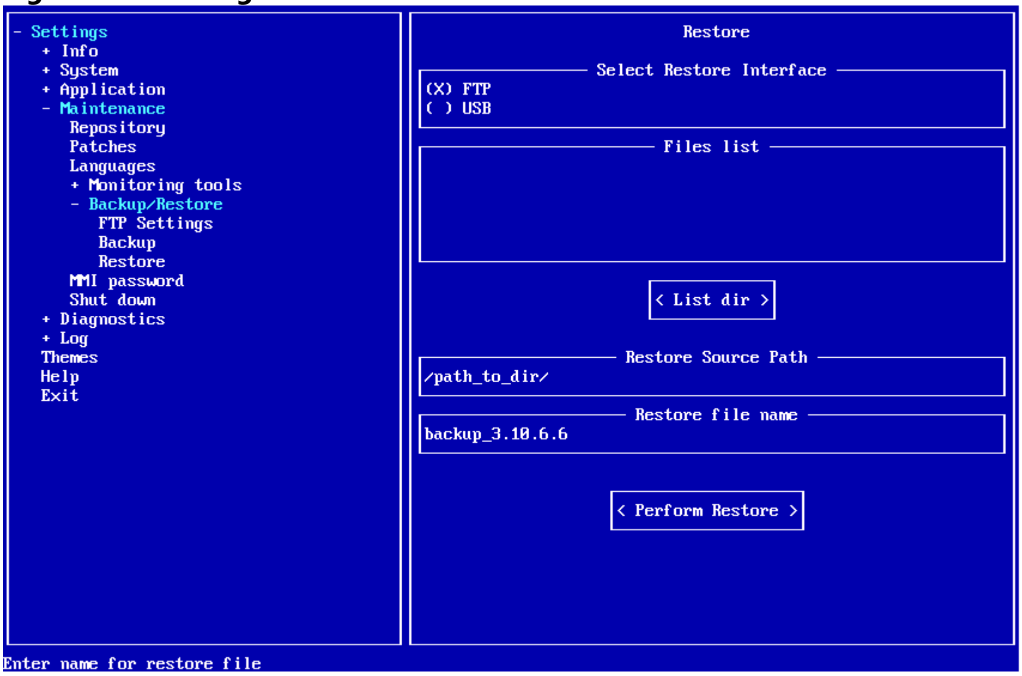
Important: Format at least one partition as EXT2, EXT3, EXT4, or FAT32 in the USB drive.

1. Insert a USB drive into your server.
2. In the MMI menu, from **Settings**, select **Maintenance.**
3. From **Backup/Restore**, select **Backup.**
4. From **Select Backup Interface**, enable **USB**.
5. In **Select device to backup to**, select your USB device.
6. In the **Backup path** field**,** enter the absolute path and filename that you want to create.
7. **Optional:** To view a list of backup files in the directory, click **Show Files**.
8. Click **Perform Backup**.

Restoring data from an FTP server

1. In MMI menu, from **Settings**, select **Maintenance**, then **Backup restore**.
2. From **Backup/Restore**, select **FTP Settings**.
3. Enter the host IP address, username, and password in the **Host IP address**, **User**, and **Password** fields, and click **Apply changes**.
4. In the navigation tree, from **Backup/Restore**, select **Restore**.
5. In the **Select Restore Interface** area, select **FTP**. For more information, see Figure 9.
6. In the **Restore Source Path** area, enter the absolute path to the directory with the backup.
7. Click **List dir** to list available backup files located in the directory
8. In **Files list** select the necessary backup file and press the **Enter** button on your keyboard.
9. Press **Perform Restore**.

Figure 9: Restoring data from an FTP server



Restoring data from a USB flash drive

1. Connect the USB drive to your server.
2. In the MMI menu, from **Settings**, select **Maintenance**, then **Backup/Restore**. From **Backup/Restore**, select **Restore**.
3. In **Select Restore Interface**, select **USB**. The system automatically displays all available USB devices that connect to the server.
4. In **Select device to restore from**, select the USB drive you want to use.
5. In **Path to the backup file on USB device**, enter the absolute path of the backup.
6. Click **List dir** to list backup files located in the directory.
7. From **Files list**, select the backup file that you want to use and press the enter key.
8. Click **Perform restore**.

Firewall

The main purpose of the PowerManage firewall is to provide an easy-to-use tool to configure secure network access policies and limit the number of simultaneous connections to avoid an overload.

The internal firewall in PowerManage works immediately after the installation process and does not require configuration. It is implemented with the Iptables Linux utility, which is a Linux kernel firewall configuration tool. This function performs the following tasks:

- Permits incoming connections only to specified ports from defined networks.
- Restricts the number of simultaneous connections to a specified value for a variety of services.

The internal firewall is intended to be supplementary to an external firewall and not a replacement. The internal firewall provides more stability and reliable performance.

Source restriction for incoming connections

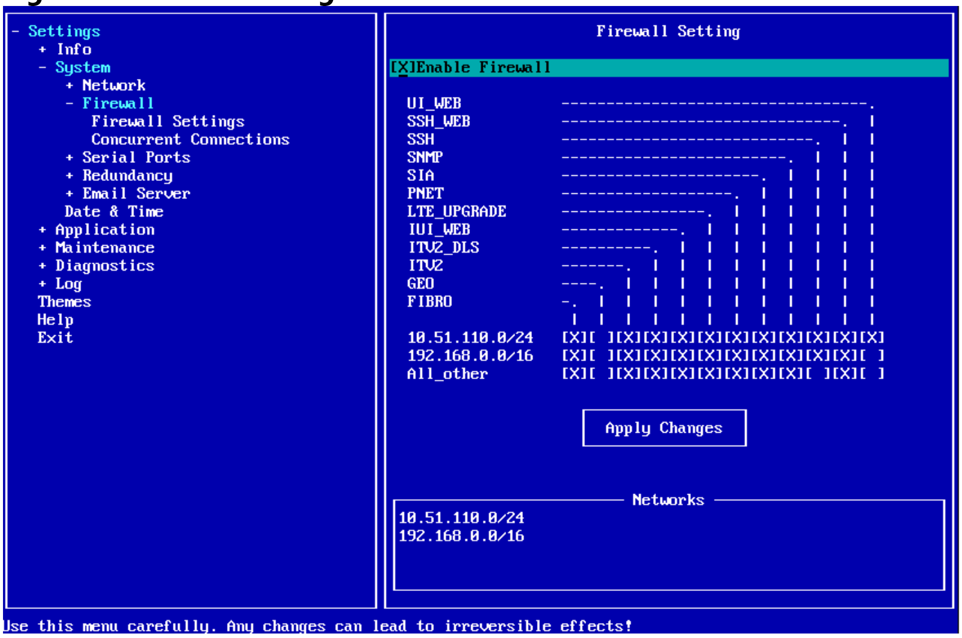
The firewall turns on immediately after you install the PowerManage. By default, an incoming connection from any IP is permitted to connect to the corresponding TCP/UDP ports of all services that work with a network. In this configuration the server is fully operable, but in most cases this configuration is redundant. Limit the allowed source IP addresses and forbid access to services that that customers don't use.

You can allow or deny access for services. The MMI provides a list of profiles.
There is an option to add some networks and manage access from them to PowerManage services separately.

Source restriction example

Consider the following example in Figure 10:
All_other is enabled for all profiles except **GEO**, **HTTP/HTTPS** and **SSH**. Enable **All_hosts** to allow access to the service from any network.
GEO is disabled. This means that if you configure GEO redundancy, you close the ports for the communication between servers.
SSH access allows only IPs within the following networks: 10.51.110.0/24 and 192.168.0.0/16.
Unsecure web access with HTTP/HTTPS is only allowed on the 10.51.110.0/24 network.

Figure 10: Firewall configuration



Restricting sources for incoming connections

1. In the MMI menu, click **System**.
2. From **System**, select **Firewall**, and then **Firewall Settings**.
3. In **Add New Network**, enter the network in the following format: `x.x.x.x/y`
4. Click **Add Network**.

Restriction on a number of simultaneous connections

You can restrict the number of simultaneous connections to a list of services represented by the corresponding profiles in MMI. By default it is not limited. It corresponds to a value of 0 in MMI.

If the number of connections for http is set to 5, the value refers to the number of simultaneous connections with http and not the number of opened web pages on the PowerManage GUI. Within each web session, a few simultaneous connections can initiate. To avoid rejecting some http queries and causing the established session to malfunction, set the limit of a single web session to a value of 5 or more.

For more information on editing the firewall concurrent connections, see Editing the firewall concurrent connections.
For more information on source restriciton, see Source restriction for incoming connections and Source restriction example.

Editing the firewall concurrent connections

1. Enter the MMI menu.
2. From **System**, select **Firewall**.
3. Select **Concurrent Connections**.
4. Enter the maximum simultaneous connections for each service.
5. Click **Apply Changes**.

Redundancy configuration

The redundancy feature works in the two following modes: geo and local.

If you want to restore a data backup on a new redundant installation, first perform a restore on the server that you want to use as the master server, then configure the redundancy server. You do not need to perform the restore on the secondary node servers.

Note:

- If you reconfigure the redundancy feature for PowerManage servers, the service restarts. Some services may not work during the restart process and panels may disable for a period of time.
- In the redundancy setup, to prevent node database corruption in the case of an unexpected AC power failure, use an uninterruptible power supply (UPS) for the master node and all secondary nodes. If you do not have a UPS and are about to lose AC power, shut down the server. Similarly, if you lose AC power and the UPS will soon run out of power, shut down the server.

Two-node system in local mode

Local redundancy mode is designed for clients who do not want to use two-channel communication between security panels and PowerManage servers, but do want redundancy for their bare metal PowerManage servers.

In local mode, only panels can access the master PowerManage server with one public IP address and cannot access the secondary node.

Figure 11: Two-node system architecture in local mode

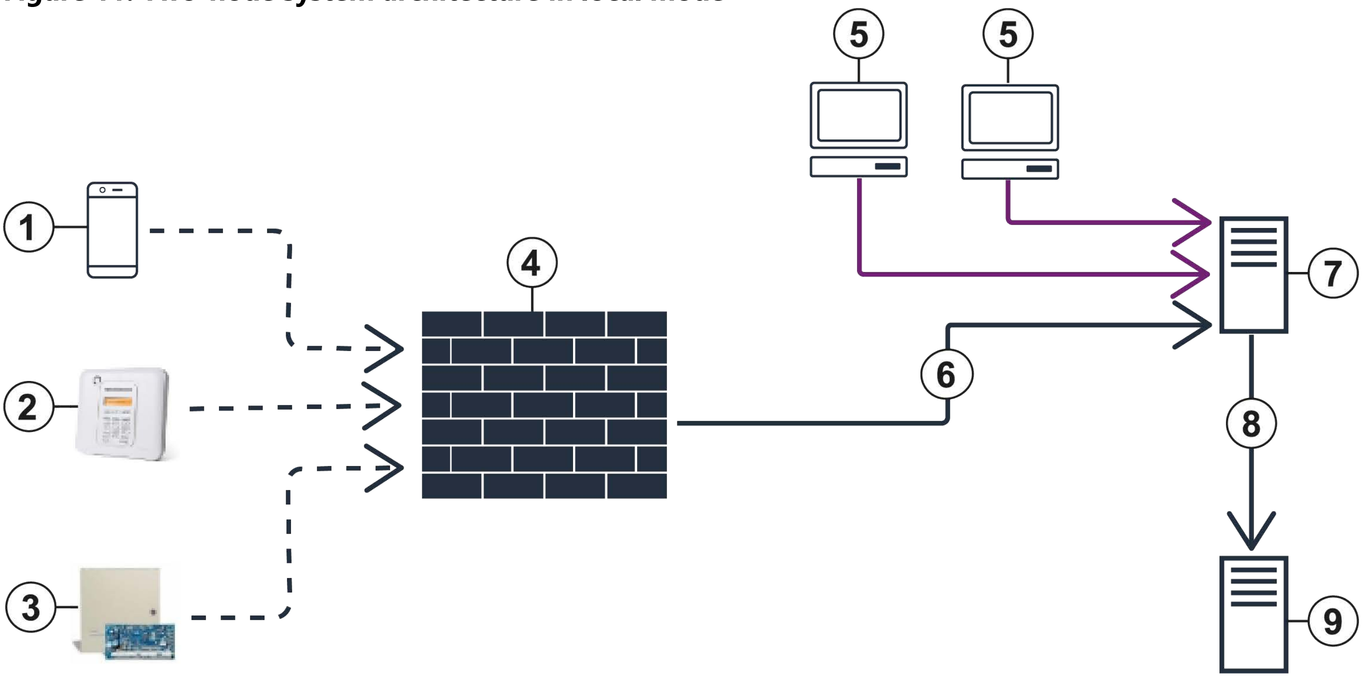


Table 22: Two-node system architecture in local mode

Callout	Description
1	https://<DNS name>
2	IP receiver
3	Integration server IP
4	Firewall with one public IP address
5	Operator
6	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
7	PowerManage master server node
8	Data synchronization
9	PowerManage secondary server node

In local redundancy mode, the automatic switchover option is not available. If the master server or part of its services is not available, you can manually disable the redundancy on the secondary node and then reconfigure your firewall to redirect all traffic to the secondary node.

For an example of redundancy modes, see Figure 13.

Figure 12: Diverting to the secondary node in a two-node system local mode architecture

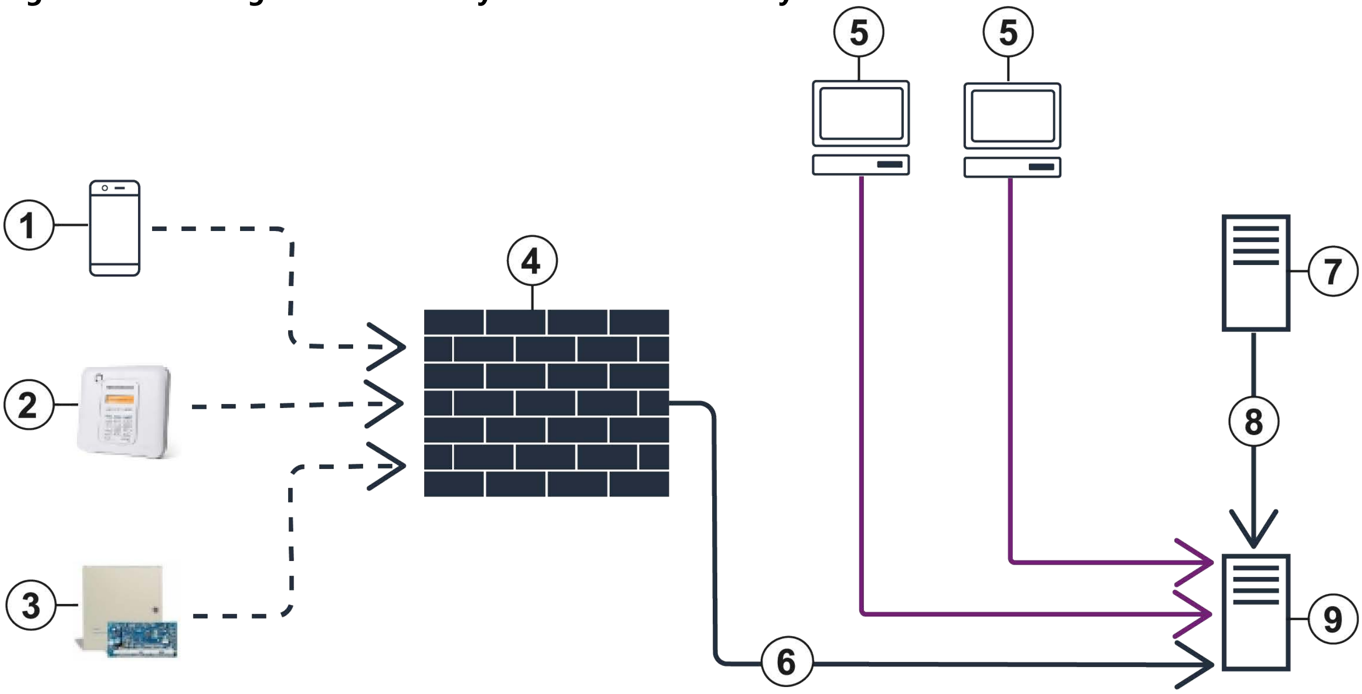


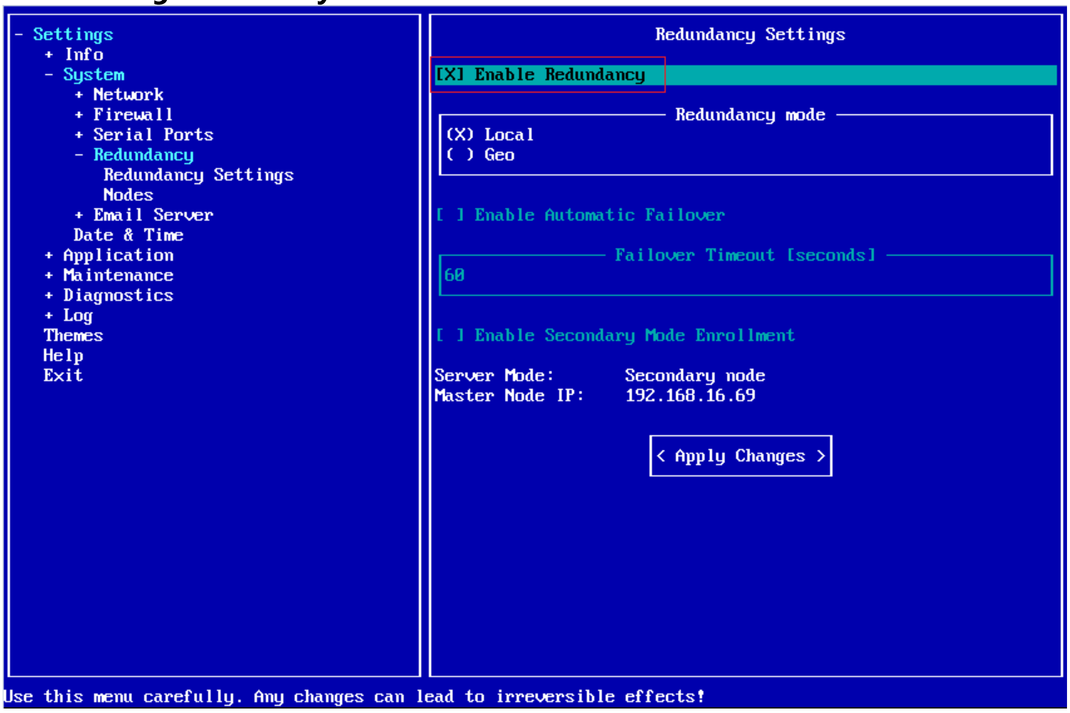
Table 23: Diverting to the secondary node in two-node system local mode architecture

Callout	Description
1	https://<DNS name>
2	IP receiver
3	Integration server IP
4	Firewall with one public IP address
5	Operator
6	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, and 443
7	PowerManage master server node
8	Data synchronization
9	PowerManage secondary server node

Disabling redundancy on the secondary node

1. Ensure that the master and the secondary servers have the same working integration access code. For more information, see Changing the working integration access code.
2. To ensure the master and secondary nodes have the same public IP address for the firewall, in the navigation tree, from **Settings**, select **System**, then select **Network**.
3. In **IP Address**, enter the same IP address as the other node.
4. In the navigation tree, from **Settings** select **System**.
5. From **System**, select **Redundancy**, then select **Redundancy Settings**.
6. Enable **Enable Redundancy**. For more information, see Figure 13.

Figure 13: Disabling redundancy on the second node



Two-node system in Geo mode

Geo redundancy mode is designed to achieve maximum availability for the services by receiving events on both redundancy nodes. In Geo mode, security panels communicate to both redundancy nodes.
The automatic switchover feature is available in Geo redundancy mode. If the master server or part of its services is not available, the secondary node automatically becomes the master.

Note: Do not reconfigure your firewalls to redirect all traffic to the secondary node. The panels continue to work with the new master node.

To restore a new GEO redundant installation with backup data, complete the following steps in order:

1. Perform a restore on the server that you want to use as the main node.
2. Perform the restore on the secondary node.
3. Configure the GEO redundancy.

Figure 14: Two-node system architecture in Geo mode

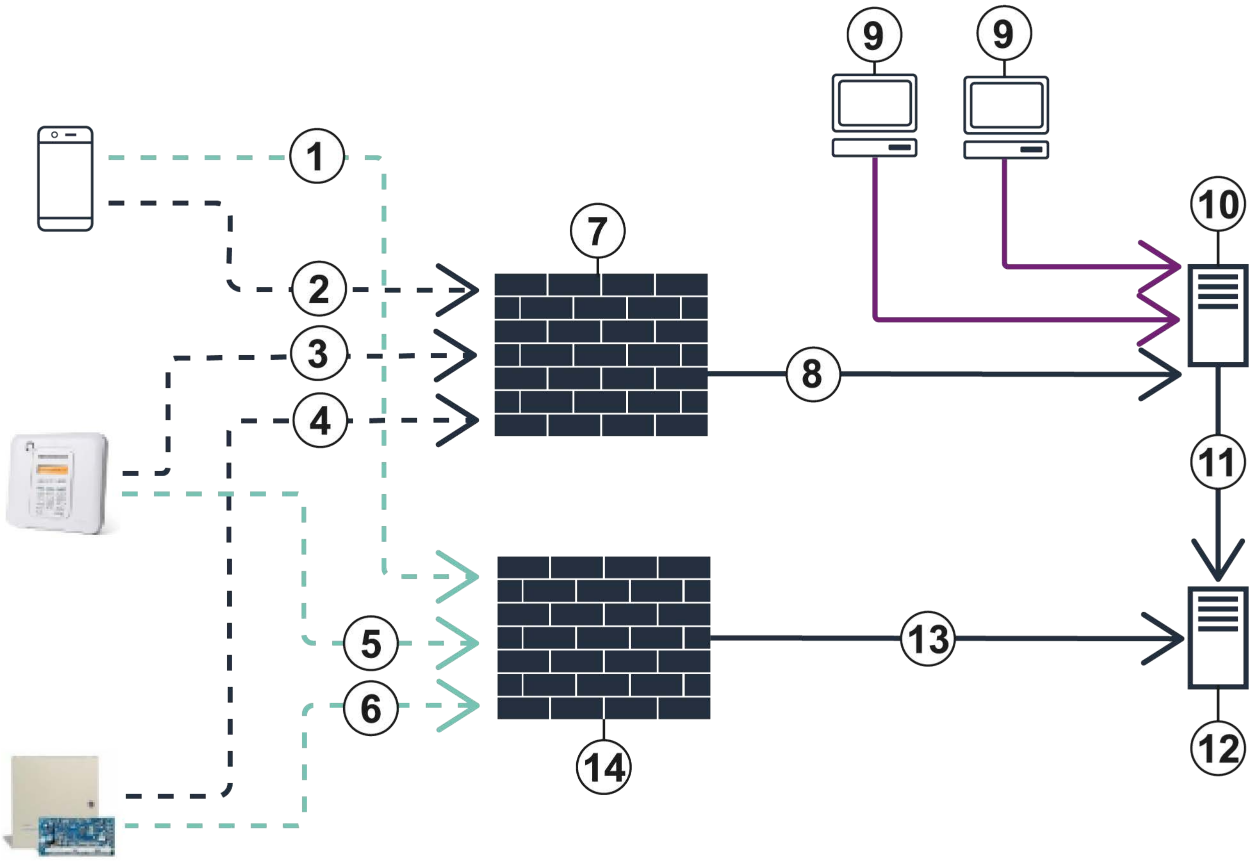


Table 24: Two-node system architecture in Geo mode

Callout	Description
1	https://<DNS name 2>
2	https://<DNS name 1>
3	IP receiver 1
4	Integration server IP 1
5	IP receiver 2
6	Integration server IP 2
7	Firewall with one public IP address
8	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, 443
9	Operator
10	PowerManage master server node

11	Data synchronization
12	PowerManage secondary server node
13	Port: 5001, 8080, 8443, 1303-1305, 3061, 3062, 80, and 443
14	Firewall with one public IP address

Assigning different public IP addresses to the master and secondary node

Ensure that the master and secondary servers have a different public IP address. Each node server must be defined as its public IP address or the public IP address of its firewall.

To configure this in the MMI menu, complete the following for each node:

1. In the navigation tree, from **Settings**, select **System**, then **Network**.
2. In **IP Address**, enter the IP address.

Note:

- In redundancy mode, some services, such as the web interface and REST API, are disabled in the secondary node.
- With DSC NEO panels, you must activate the panels before you perform the discovery process. Perform the activation by using the web interface or the user application. The user application requires REST API. If the DSC NEO panel is only enrolled in the secondary node, it is not possible to activate the panel.

Enabling redundancy in GEO mode

1. Configure the central stations for the master and secondary nodes. For more information, refer to the *PowerManage 4.8 User Guide*.
2. Enter MMI menu on the master node and complete the following steps:
    a. In the navigation tree, from **System**, select **Redundancy.**
    b. Enable **Enable Redundancy**. For more information, see Figure 15.
    c. Click **Apply Changes**.
    d. When a dialog box appears, click **Apply** and wait until the redundancy mode enables.
    Step result: Once redundancy mode enables, you can see the mode of the current node and the IP address of its master. To view the redundancy status and the enrolled secondary nodes, click **Show status**.
3. Enter MMI menu on the secondary node and complete the following steps:
    a. To enable NTP time synchronization for the secondary and master node, in the MMI menu, from **Settings**, select **System**.
    b. Select **Date & Time**, and then enable **Automatic Date and Time[NTP]**.
    c. From **System**, select **Redundancy**, then select **Redundancy Settings.**
    d. Enable **Enable Secondary Mode Enrollment**. For more information, see Figure 16.
    Note: A time difference greater than 10 seconds between the master and secondary node redundancy setup will fail
    e. Click **Apply Changes**. When a dialog box appears, click **OK**.
4. In the master node MMI, complete the following steps:
    a. In the navigation tree, from **Settings**, select **Redundancy.**
    b. Select **Nodes**, and then select **Add Node**.
    c. In **Node Hostname**, enter the name of the node.
    d. In **Node IP Address**, enter the node IP address.
    e. In **Node SSH Password,** enter the SSH root password of the secondary node.
    f. Click **Apply Change**. When a dialog box appears, click **Apply** and wait until the secondary node is added.

To check the secondary node status in the master node MMI menu, see Checking the secondary node status in the master node MMI menu.

Figure 15: Configuring the master node

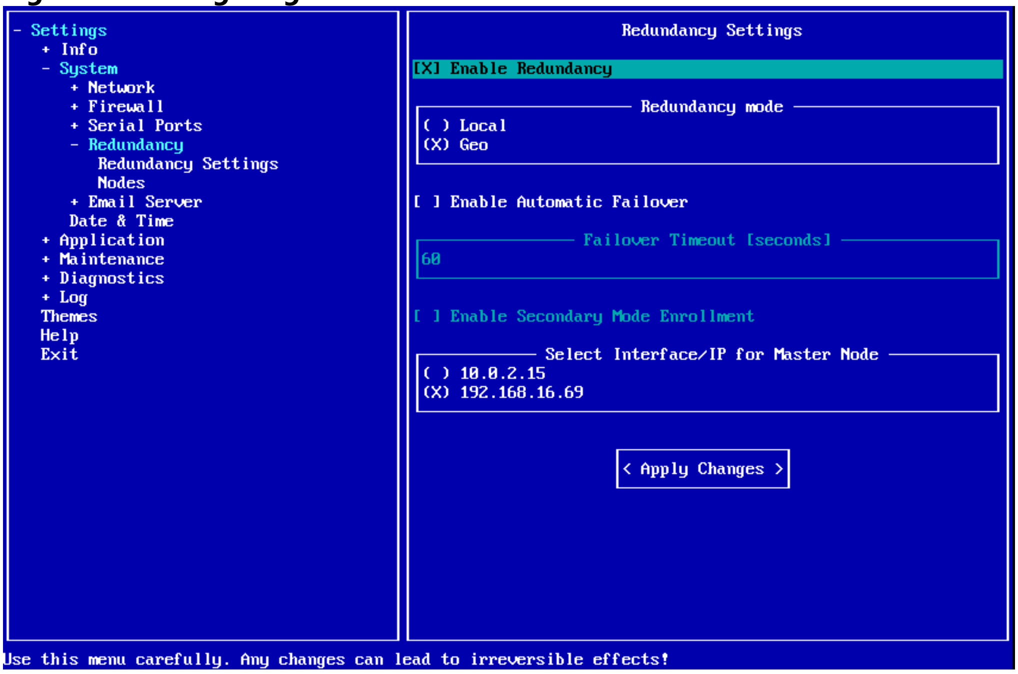


Figure 16: Enabling secondary mode enrollment

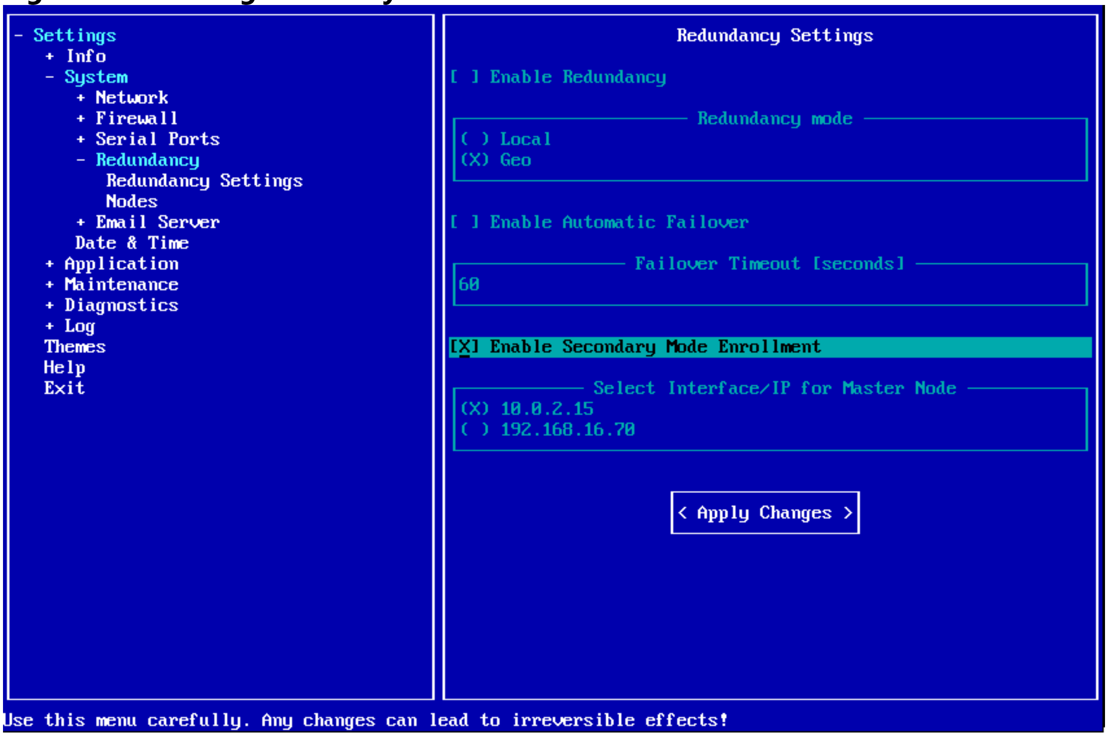
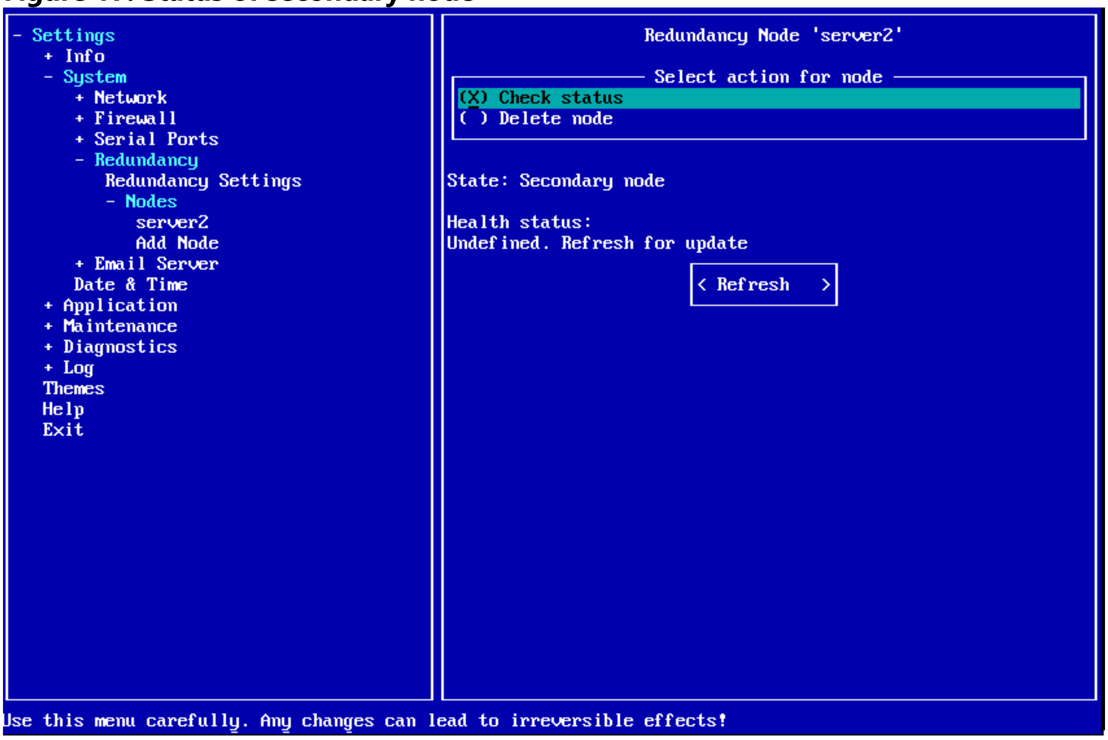


Figure 17: Status of secondary node



Checking the secondary node status in the master node MMI menu

The secondary node now displays in the masters node's MMI menu. To view the node status, complete the following steps:

1. In the navigation tree, from **System**, select **Redundancy**.
2. Select **Redundancy Settings**, and then select **Node**.
3. To view the node status, click **Check Status**. For more information, see Figure 17.

Automatic failover for two-node systems

When you configure the redundancy, you can enable automatic failover in the event that the master server fails. When automatic failover is enabled, there are health check services enabled on both master and primary secondary nodes that check for the availability of the master server.

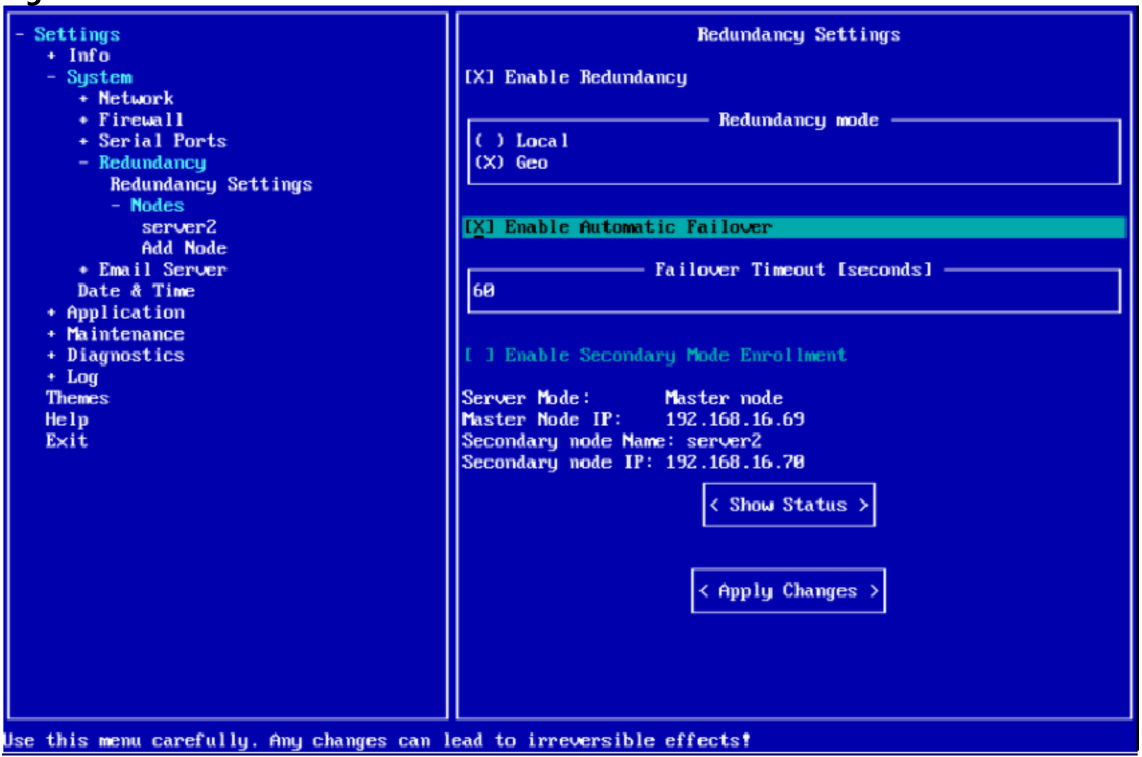
If the master server fails or becomes unavailable, the primary secondary completes the following tasks:

1. Disables the redundancy
2. Inspects the master database
3. Configures itself as the master server
4. Enables the redundancy again.

Enabling automatic failover for two-node systems

1. In the Settings navigation tree, from **System,** select **Redundancy**, and then select **Redundancy Settings**.
2. Enable **Enable Redundancy**.
3. Enable **Enable Automatic Failover**. For more information, see Figure 18.
4. Click **Apply Changes**.
5. When a dialog box appears, click **Apply** and wait until the redundancy enables.

Figure 18: Enable automatic failover



Configuring manual failover actions for two-node systems

1. Enter the MMI menu of the master node and complete the following steps:
    a) From **System**, select **Redundancy**, then **Redundancy Settings**.
    b) Disable **Enable Redundancy** and click **Apply.**
    c) Exit the MMI menu.
2. Enter the MMI menu on the secondary node and complete the following steps:
    a) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    b) Disable **Enable Redundancy** and click **Apply Changes**. When the redundancy disables a dialog box appears. Click **OK**.
    c) Exit MMI menu and log on to the secondary node again.
    d) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    e) Enable **Enable Redundancy** and click **Apply Changes**. When the redundancy enables, a dialog box appears. Click **Apply**.
3. Enter the master node MMI menu and complete the following steps:
    a) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    b) Enable **Enable Secondary Mode** and click **Apply Changes.** When the redundancy enables, a dialog box appears. Click **Apply**.
4. Enter MMI menu for the secondary node that you want to make the master node and complete the following steps:
    a) From **System**, and then select **Redundancy**.
    b) Select **Nodes**, and then select **Add Nodes**.
    c) Enter the former master node IP address and SSH root password.
    d) Click **Apply Changes**. When a dialog box appears, click **Apply** and wait for the secondary node to be added.

Redundancy configuration for four-node systems

To restore a new GEO redundant installation with backup data, complete the following steps in order:

1. Perform a restore on the server that you want to use as the main node.
2. Perform a restore on the secondary nodes.
3. Configure the GEO redundancy.

With GEO redundancy, some services are disabled for secondary nodes, such as the web interface and REST API.

With DSC NEO panels, you must activate the panels before you perform the discovery process. Perform the activation by using the web interface or the user application, which requires REST API.
Note: You cannot activate a DSC NEO panel if you only enroll the panel in the secondary node.

In the redundancy configuration, you can add as many secondary nodes as you require but one GEO site must have one master node configured and another site must have a primary secondary node. The other servers are the secondary nodes.

If you enable automatic failover for the redundancy, the following processes occur:

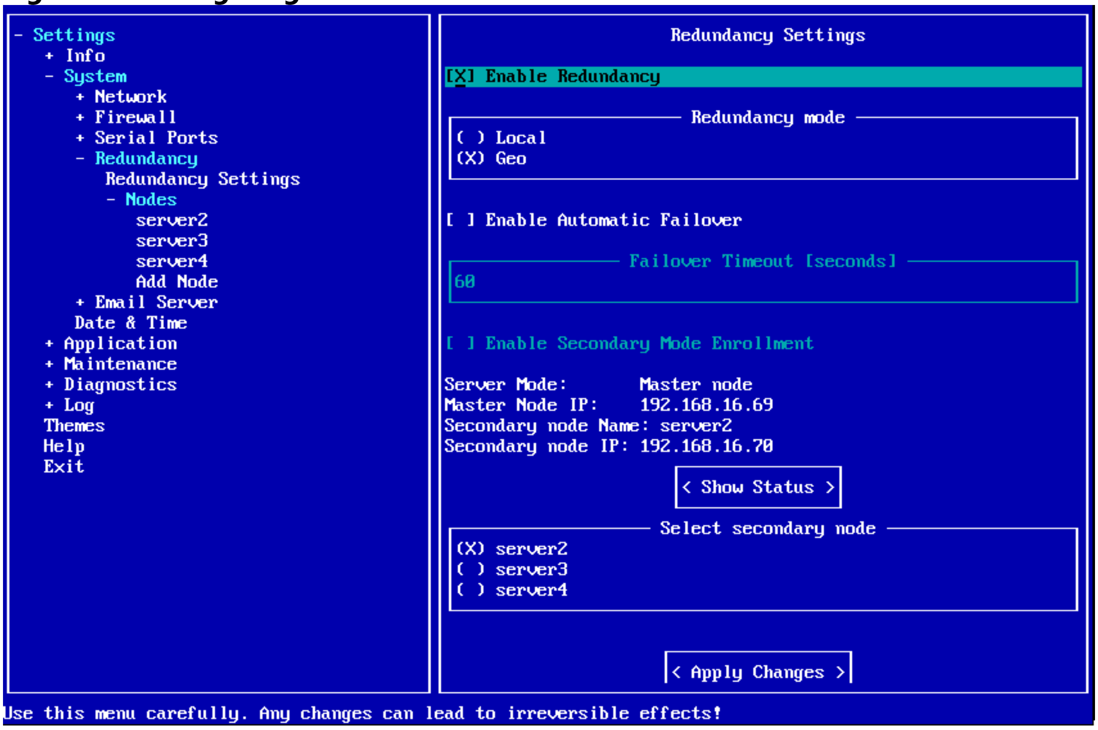
1. The primary secondary node disables the redundancy.
2. The primary secondary node retrieves the former master node database
3. The primary secondary node enables the redundancy and sets itself as the master server.
4. When the redundancy enables, the new master node designates the new primary secondary node from the healthy secondary nodes and adds it to the redundancy.
5. The remaining available servers are added as secondary servers.

For a manual failover configuration, as a precaution to the master node failing, perform a failover similar to the two-node redundancy. Reconfigure the primary secondary node as the master and designate the new primary secondary node. You can configure the primary secondary node in **System** > **Redundancy** > **Nodes** > **Secondary Node**.

Configuring manual failover actions for four-node systems

1. Install the nodes.
2. Configure the central stations for the master and secondary nodes.
3. In the master node, complete the following steps:
    a) Enter the MMI menu
    b) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    c) Enable **Enable Redundancy** and click **Apply Changes**. When a dialog box appears, click **Apply**. For more information, see Figure 19.
    d) When the redundancy enables, you can see the current node mode and the master servers' IP address.
    e) **Optional:** To view the redundancy status and the enrolled secondary nodes, click **Show status**.
4. For each secondary node, complete the following steps:
    a) Enter the MMI menu.
    b) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    c) Enable **Secondary Mode Enrollment**.
    d) Click **Apply Changes**. When a dialog box appears, click **Apply**.
    e) Disable **Enable Redundancy** and click **Apply Changes**.
    f) When the redundancy disables, a dialog box appears. Click **OK**.
5. In the master node, complete the following steps:
    a) Enter the MMI menu.
    b) From **System**, select **Redundancy**, and then select **Redundancy Settings**.
    c) Enable **Enable Secondary Mode** and click **Apply Changes.** When the redundancy enables, a dialog box appears. Click **Apply**.
6. Before you add any nodes, complete the following steps to enable NTP time synchronization for the master node and each secondary node:
    a) In the navigation tree, from **System**, select **Date & Time**.
    b) Enable **Automatic Date and Time [NTP]**.
    c) Click **Apply Changes**.
7. In the secondary node that you want to make the master node, complete the following steps:
    a) Enter MMI menu.
    b) From **System**, and then select **Redundancy**.
    c) Select **Nodes**, and then select **Add Node**.
    d) To add each secondary node, enter the node hostname, node IP address and node SSH root user in the **Node Hostname**, **Node IP Address**, and **Node SSH User** fields.
8. If you enrol more than one secondary node, by default, the first secondary node you enrol is the primary secondary. To manually designate the primary secondary, in the master node, complete the following steps:
    a) Enter the MMI menu.
    b) From **System**, select **Redundancy**, then **Redundancy Settings**.
    c) From **Redundancy Settings**, select **Nodes**.
    d) Select the secondary node you want as the primary secondary.
    e) Enable **Enable Secondary Mode Enrollment**.
    f) Click **Apply Changes.** When the redundancy enables, a dialog box appears. Click **Apply**.

Figure 19: Configuring manual failover actions



Automatic failover for a four-node system

If you enable automatic failover for the redundancy, the following processes occur:

1. The primary secondary node disables the redundancy.
2. The primary secondary node inspects the former master database, and enables the redundancy.
3. The primary secondary node designates itself as the master.
4. When the redundancy enables, the new master server designates the new primary secondary among the healthy secondary servers and adds it to the redundancy.
5. The remaining available servers are added as secondary servers.

Manual master failover actions

Decide which server is the new master if the current master server fails. The new master can be any of the other three or more servers. For example, you can make a node on a remote site the master, or make the secondary node from the same site the master.

After you manually reconfigure the GEO system, you must make a change on client firewall and redirect all traffic to the new master and primary secondary on the remote site.
Configure the master on the same site so that is not difficult to redirect traffic from the failed node to the new one. If the master server is on the same side, less manual action is required and the IP receiver doesn't need to be changed for the panel's IP.

Manually configuring the master failover actions

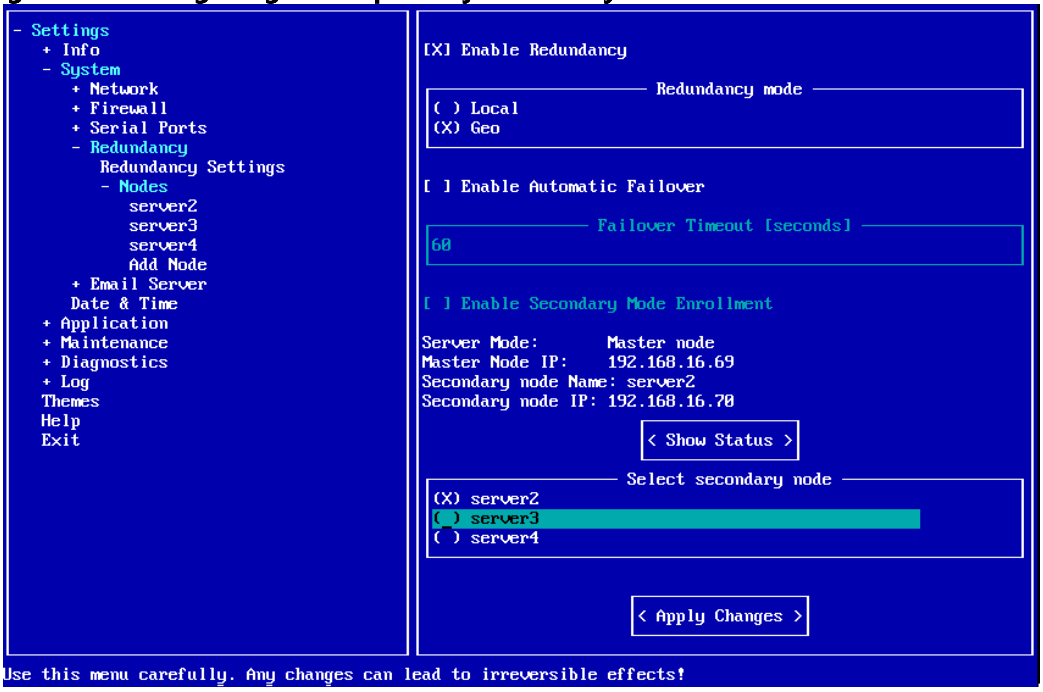
1. Enter the primary secondary MMI menu and complete the following steps:
    a) From **System**, select **Redundancy**, then **Redundancy Settings.**
    b) Disable **Enable Redundancy** and click **Apply Changes**.
    c) Exit the MMI menu and log on again.
2. For each secondary node and the former master node, complete the following steps:
    a) From **System**, select **Redundancy**, then **Redundancy Settings.**
    b) Disable **Enable Redundancy** and click **Apply Changes**.
    c) Wait until the redundancy is disabled. When a dialog box appears, click **OK**.
    d) Exit the MMI menu.
3. Complete the following steps for the primary secondary node:
    a) From **System**, select **Redundancy**, then **Redundancy Settings.**
    b) Enable **Enable Redundancy** and click **Apply Changes**.
    c) Wait until the redundancy is disabled. When a dialog box appears, click **OK**.
    d) Exit the MMI menu.
4. For each secondary node and the former master node, complete the following steps:
    a) From **System**, select **Redundancy**, then **Redundancy Settings.**
    b) Enable **Enable Secondary Mode Enrollment**.
    c) Click **Apply Changes**. When a dialog box appears, click **OK**.
    d) Exit the MMI menu.
5. Open the master node MMI menu and complete the following steps:
    a) From **System**, select **Redundancy**, then **Redundancy Settings.**
    b) From **Redundancy Settings**, select **Nodes**.
    c) To add each secondary node, enter the node hostname, node IP address and node SSH root user in the **Node Hostname**, **Node IP Address**, and **Node SSH User** fields. The IP address and SSH root password are the same as the form master values.
    d) Click **Apply Changes**. When a dialog box appears, click **OK**.
    e) Wait until the secondary node is added and complete the procedure for the remaining nodes.

Configuring a new primary secondary node

If the primary secondary node fails, you must configure a new primary secondary. To make it easier to redirect traffic from a failed node to the new node, select a new primary secondary node on the same site as the failed node.

1. Enter the master node MMI menu
2. From **System**, select **Redundancy**, then select **Redundancy Settings**.
3. To redirect all traffic to the new primary secondary, in **Select secondary node**, enable the node you want as the primary secondary. For more information, see Figure 20.

Figure 20: Configuring a new primary secondary node



Appendix A

SSL certification

Power Manage IV supports HTTPS secure communication. To use HTTPS, purchase a Secure Sockets Layer (SSL) certificate and install it on the PowerManage server.

1. Submit a request to the IT department or Internet Service Provider (ISP) to register the PowerManage server host name.
2. Create a file and enter the following values in order:
    a) A passphrase or password that is used for encryption. It is best to use a combination of numbers and letters from the English alphabet. You can use lowercase letters, uppercase letters or both. The use of special characters is not supported.
    b) A two letter country code, such as *UK*.
    c) A state or province name. If not applicable you can use the country name.
    d) A locality name (region, city), such as *London*.
    e) An organization name, such as Visonic.
    f) **Optional:** An organizational unit name, such as a section or department.
    g) A common name, such as company name or the hostname of the server.
    h) **Optional:** An email address.
3. Send the hostname of the PowerManage server and the file in Step 2 to Visonic. Visonic generates a certification request and returns a `public.csr` file and a `private.key` file.
4. Send the public.csr file and the applicable payment to a certification authority (CA). The CA returns the signed certificate such as a .crt file.
5. Send the signed, validated certificate to Visonic and include the original CA email.

Visonic uploads the certificate to the repository, which adds https support to the PowerManage server.

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