



AlarmInstall User Guide

D-307194

Rev. 3

www.jci.com

2020-12

Version 4.8



D-307194



Copyright

2020 Johnson Controls. All rights reserved. JOHNSON CONTROLS, TYCO, VISONIC and DSC are trademarks of Johnson Controls.

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 NOT DOWNLOAD, 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; (vi) 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 Your welcome kit and/or its agreement(s) with Customer's to remind them to keep secure their login and password details and comply with all applicable security policies.
- e. You shall 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

About this guide

- Intended audience

- About the AlarmInstall app

- Support

Configuring the AlarmInstall app

- Supported devices and panels

 - Devices

 - Panels

- Prerequisites

 - Server access approval

 - Configuring PowerManage server approval in the PowerManage web application

 - Configuring installer app access in the PowerManage web application

 - Enabling or disabling the AlarmInstall application for a specific panel in the PowerManage web interface

 - Enabling or disabling the AlarmInstall application for a specific panel on the Panels page

 - Enabling or disabling the AlarmInstall application for a specific panel in the Panel hub

AlarmInstall App configuration

- Running AlarmInstall for the first time

- Remote and direct connections

 - Remote and direct access requirements

- Direct access

 - Connecting to a panel with WiFi in direct mode

- Direct access troubleshooting

 - USB and USB OTG cables connections to an alarm panel (Android devices)

 - Connecting to an alarm panel using cables

- Remote access

 - Remote access panel connections

 - Two factor authentication in Remote Mode

 - Authenticating in remote mode with two factor authentication

 - Logging on to a server

 - Changing and logging on to another server

 - Quick and biometric logon options

 - Changing the app language on the logon screen

- Adding panels

 - Panels list

 - Panel activation for Neo and PSP panels

 - Adding a panel

 - Editing a panel name

 - Removing a panel from the AlarmInstall app

 - Application settings

 - Changing the app language

 - Changing the app theme to light or dark mode

 - Changing your two factor authentication password

 - Enabling or disabling biometric login with face ID or fingerprint

- Changing the temperature scale to Celsius or Fahrenheit

- Viewing the AlarmInstall app version and build number

- Editing user information

- Viewing the EULA and Privacy Notice

- Logging out of the AlarmInstall app

- Managing the security system

 - Approving installer access with homeowner approval with the ConnectAlarm app

 - AlarmInstall app interface

 - General

 - Connection status

 - Running a remote inspection

 - Customer info tab

 - Diagnostics tab

 - Performing a walk test in the Diagnostics tab.

 - Configuration tab

 - Editing the current configuration on the Configuration tab

 - Editing a previous configuration on the Configuration tab

 - Locations tab

 - Log tab

About this guide

Intended audience

This guide is for installers, technicians, and support engineers who configure and troubleshoot alarm security systems using the AlarmInstall app.

About the AlarmInstall app

Use the AlarmInstall app to configure an alarm security system from your mobile device or tablet. Installers can configure a panel on-site or from a remote location. For installers that are on-site, there is no requirement for a wireless keypad if the security panel is hidden. As there are no travel requirements, accessing the panel remotely significantly reduces response and troubleshooting times.

Download the AlarmInstall app from the Apple App Store or from Google Play.

Support

Email: intrusion-support@jci.com

Website:

- EMEA: https://www.tycosecurityproducts.com/TS_ContactDetails.aspx
- APAC: https://www.tycosecurityproducts.com/A_TS_ContactDetails.aspx

Configuring the AlarmInstall app

Supported devices and panels

Devices

You can install the AlarmInstall app on the following devices:

- Apple devices, such as iPads and iPhones, with iOS version 9 or later. Download the AlarmInstall app in the Apple App Store.
- Android version 4.3 devices or later, such as tablets and smartphones. Download the AlarmInstall app in the Google Play Store.

Panels

You can use the AlarmInstall App with the following panels remotely or directly:

Remote access:

- PowerMaster-10
- PowerMaster-30
- PowerMaster-33
- PowerMaster-360
- PowerMaster-360R
- PowerMax
- PowerSeries Pro
- PowerSeries Neo

Direct access:

- PowerMaster-360
- PowerMaster-360R
- PowerSeries Pro
- **Note:** For PowerSeries Pro panels, download the PowerSeries Pro AlarmInstall mobile application.

Prerequisites

Server access approval

Depending on how the server is configured, installers require approval by one of the following methods:

- Server operator approval: The installer can connect to the panel without homeowner permission. To enable this option, disable **APPROVE INSTALLER ACCESS BY USER** in [Configuring PowerManage server approval in the PowerManage web application](#).
- Self-monitoring server: The homeowner approves access to the panel using the ConnectAlarm app every time the installer requests access with the AlarmInstall app. To enable this option, enable **APPROVE INSTALLER ACCESS BY USER** in [Configuring PowerManage server approval in the PowerManage web application](#). For more information on how the user approves access, see [Approving installer access with user approval in the ConnectAlarm app](#).

Configuring PowerManage server approval in the PowerManage web application

Server operators complete the following steps to configure the interactive settings parameters on the PowerManage server:

Note: In the following example, the PowerManage server is version 4.6 and later. For earlier PowerManage versions, refer to the installation guide of the relevant version.

Configuring installer app access in the PowerManage web application

To configure installer app access in the PowerManage web application, complete the following steps:

- From the navigation pane, click **System**, and then click **Settings**.
- From the **INTERACTIVE** tab, click **EDIT** in the **INTERACTIVE SESSIONS** panel and configure the server with one of the following options. For more information, see [Figure 1](#):
 - To enable installer app access to new panels that enroll in the server by default, select the **ENABLE INSTALLER APP FOR NEW INCOMING PANELS** check box.
 - To configure the PowerManage to allow installer access with user approval by the ConnectAlarm user app only, enable **APPROVE INSTALLER ACCESS BY USER**. To configure the PowerManage to allow installer access with user approval, see [Approving installer access with user approval in the ConnectAlarm app](#).
 - To configure the PowerManage to allow installer access with server operator approval only, disable **APPROVE INSTALLER ACCESS BY USER**.

Figure 1: Configuring installer access approval on the INTERACTIVE tab

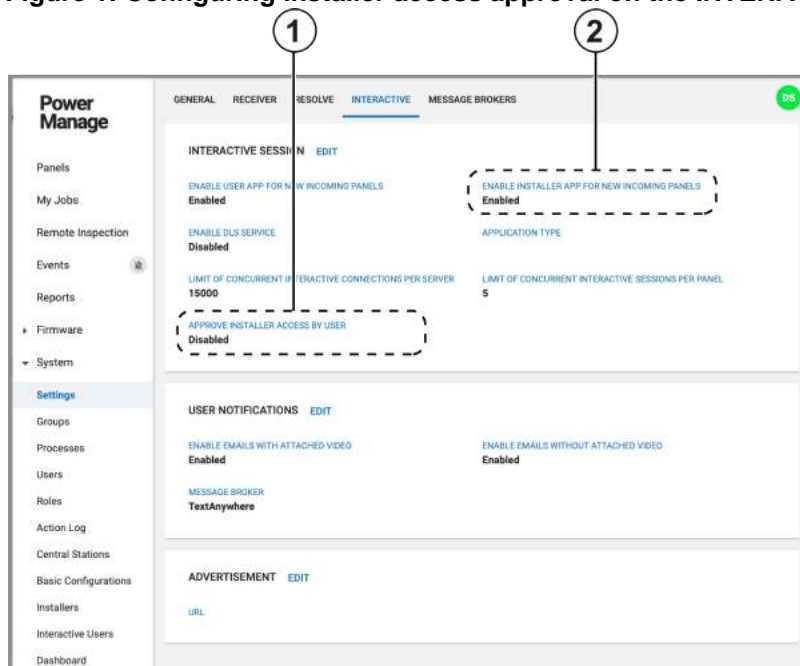


Table 1: Configuring installer access approval on the INTERACTIVE tab

Callout	Name	Description
1	APPROVE INSTALLER ACCESS BY USER	Enable APPROVE INSTALLER ACCESS BY USER to configure the PowerManage to allow installer access only with user approval by the ConnectAlarm user app.
		Disable APPROVE INSTALLER ACCESS BY USER to configure the PowerManage to allow installer access with server operator approval only.
2	ENABLE INSTALLER APP FOR NEW INCOMING PANELS	Enable ENABLE INSTALLER APP FOR NEW INCOMING PANELS to enable the installer app for new panels that enroll by default.

Enabling or disabling the AlarmInstall application for a specific panel in the PowerManage web interface

In the PowerManage web interface, you can enable or disable the AlarmInstall application for a specific panel.

Enabling or disabling the AlarmInstall application for a specific panel on the Panels page

1. From the navigation pane, click **Panels**.
 2. On the Panels page, find the panel you want to configure and click the mobile app icon
 3. Enable **Installer App**. For more information, see Callout 1 and Callout 2 in [Figure 2](#).
- Note:** If you enable ENABLE INSTALLER APP FOR NEW INCOMING PANELS, the installer app enables for new panels that enroll.

Figure 2: Enabling and disabling installer and user access to panels on the Panels page

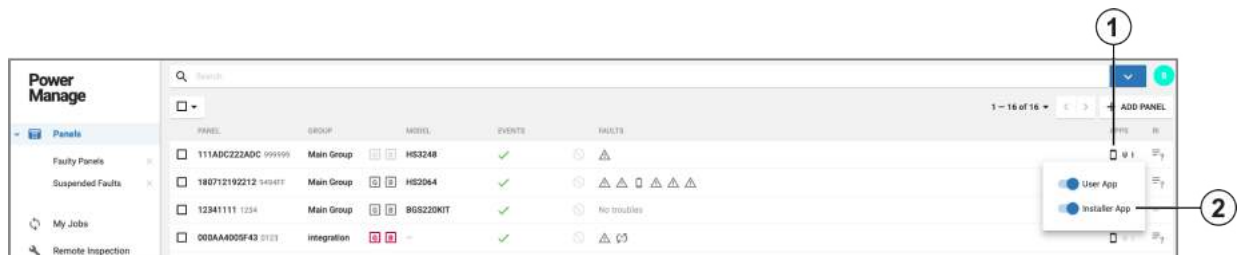


Table 2: Enabling and disabling installer and user access to panels on the Panels page

Callout	Name	Description
1	App icon	Click to use the Installer App and User App toggles.
2	Installer App toggle	Click to enable or disable access to the panel with the installer app.

Enabling or disabling the AlarmInstall application for a specific panel in the Panel hub

1. Go to the panel hub of the panel you want to configure.
2. From the **ACTIONS** drop-down, enable **Installer App**. For more information, see Callout 1 and Callout 2 in [Figure 3](#).

Figure 3: Enabling and disabling installer and user access to panels in the Panel hub

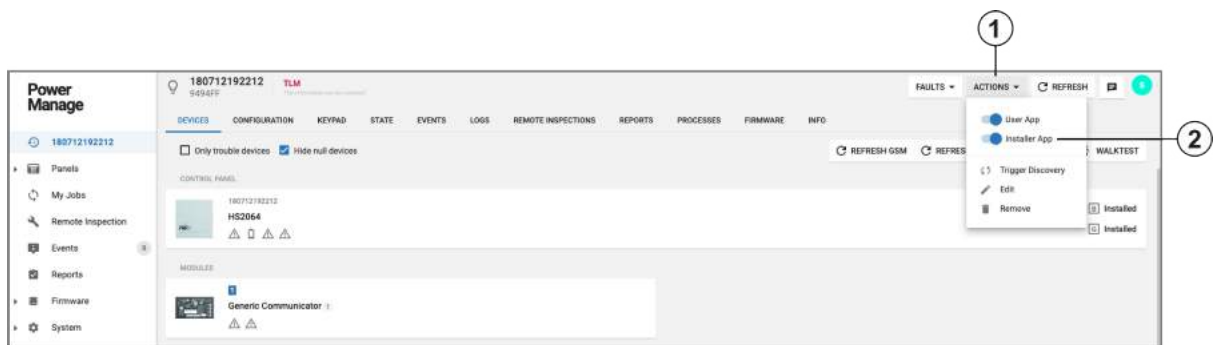


Table 3: Enabling and disabling installer and user access to panels in the Panel hub

Callout	Name	Description
1	ACTION drop down	Click to access actions to perform on a panel.
2	Installer App toggle	Click to enable or disable access to the panel with the installer app.

AlarmInstall App configuration

Running AlarmInstall for the first time

1. Download the application from Apple App Store or Google Play App.
2. Open the app and accept the end user license agreement and privacy notice.
3. To choose the connection type to the panel, select **Direct** or **Remote**. For more information, see [Remote and direct connections](#).

Important: If you connect with remote mode, authenticate your device with two factor authentication. For more information, see [Authenticating in remote mode with two factor authentication](#). If you have already completed two factor authentication, to login, enter your email and password.

4. Add one or more panels. For more information, see [Adding a panel](#).

Remote and direct connections

The AlarmInstall application can work in remote or direct mode.

- Remote mode: The installer can connect to the panel and control it remotely without travelling to the premises of the user. Both the panel and the phone or tablet connect to a server over a wide area network (WAN). For more information, see [Remote access](#).
- Direct mode: The phone connects directly to the panel by local WiFi or a USB cable. The installer must travel on-site to the user's premises. For more information, see [Direct access](#).

Note: Only PowerMaster-360 and PowerMaster-360R panels support direct mode.

Remote and direct access requirements

For remote access, the following prerequisites are required:

- All panels must have cellular or Ethernet connections or a combination of both. You can connect to all alarm panels that are connected to the WAN.
- Before the installer connects to the panel remotely, the server operator, homeowner, or business owner must enroll all panels in the PowerManage server and enable installer app access on the PowerManage server. To enroll panels on the PowerManage server, refer to the relevant *PowerManage User Guide*. For more information on enabling installer app access on the PowerManage server, see [Server access approval](#).

For direct access, the following prerequisites are required:

- A connection to the PowerMaster-360 or PowerMaster-360R alarm panel. This connection can be a WiFi connection to the panel's private local WiFi network. For Android devices, you can connect to the panel using USB and USB OTG cables.
- The mobile device is within range of the panel's WiFi.
- PowerSeries Pro panels require a different app, the PowerSeries Pro AlarmInstall app.

Direct access

Connecting to a panel with WiFi in direct mode

Pre-requisite: Find the panel ID and password on a label on the underside of the panel in the following format:

- Panel ID: XXXXXX
- S/N: XXXXXXXXXX.

The serial number (S/N) is the password.

1. Open the AlarmInstall app.
2. On the connect screen, tap **Direct**.
3. In your device WiFi settings, locate and connect to the panel WiFi. The WiFi ID is the Panel ID. If the panel WiFi ID does not display, complete the following steps:
 - a. Go to the panel's installation menu.
 - b. Follow the following path: 04:COMMUNICATION > 8:WiFi > ACCESS-POINT > A.POINT MODE.
 - c. Select **Enable**.
 - d. Press the +/- buttons on the back of the panel.
4. In the AlarmInstall app, enter the panel ID number as the panel ID and the serial number as the password.
5. Tap **CONNECT**.
6. Enter your configuration code and tap **LOGIN**.
7. Enter the default installer code: 9999.

Direct access troubleshooting

Problem

The following message appears when you try to connect to the panel: Panel is not responding. Please check your WiFi settings.

Solution

There is a problem with the WiFi connection. See the section [Connecting to the alarm panel using direct access](#) and try to connect your device to the panel's local WiFi network.

The following restrictions apply:

- Direct access is only possible when the alarm panel is in a disarmed state.
- Connection time is 15 minutes. Five minutes before the panel disconnects, a beep sounds. To renew the connection press the +/- button on the back of the panel.
- After an hour, the connection automatically terminates and a beep sounds 5 minutes before the panel disconnects.

USB and USB OTG cables connections to an alarm panel (Android devices)

If the AlarmInstall app is installed on an Android device you can access the PowerMaster-360 and PowerMaster-360R panels with micro-USB and USB OTG cables.

Ensure that your device supports a USB OTG cable. To test this, connect an optical mouse to the OTG cable and connect the micro-USB connector to the port on your Android device. If the mouse's optical LED lights and you can move the mouse icon on the Android device, the device supports OTG cable.

Connecting to an alarm panel using cables

Note:

- To connect an Android device to a PowerMaster-360 panel, see [Figure 5](#).
- To connect an Android device to a PowerMaster-360R panel, see [Figure 6](#).
 1. Connect the micro-USB cable and USB OTG cable.
 2. Insert the micro-USB connector of the OTG cable into the micro-USB port on your Android device.
 3. Insert the micro-USB connector cable into the micro-USB port on the panel.

Note: For the PowerMaster-360R, open the panel to access the micro-USB port.
 4. When a dialog box appears in the app, requesting access to the USB port, tap **Yes**.

Figure 4: USB OTG and Micro USB cables



Table 4: USB OTG and Micro USB cables

Callout	Device
1	USB OTG cable
2	Micro USB cable

Figure 5: PowerMaster-360 connections to an Android device

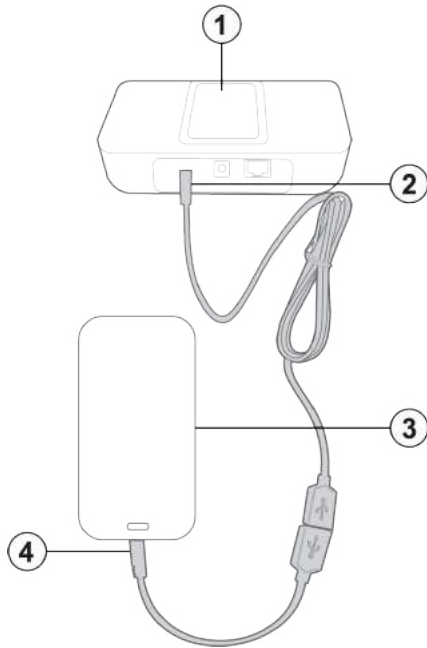


Table 5: PowerMaster-360 connections to an Android device

Callout	Description
1	PowerMaster-360
2	Micro-USB cable connected to panel
3	Android device
4	OTG cable connection

Figure 6: PowerMaster-360R connections to an Android device

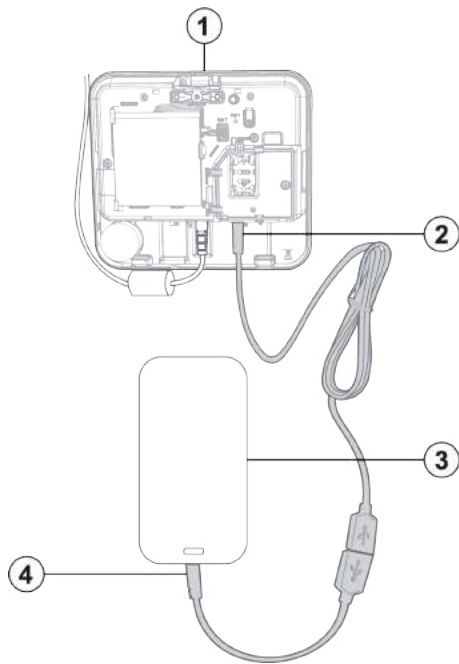


Table 6: PowerMaster-360R connections to an Android device

Callout	Description
1	PowerMaster-360R with base removed
2	Micro-USB cable connected to panel
3	Android device
4	OTG cable connection

Remote access

Remote access panel connections

You can remotely access all panels that are connected to the WAN and are registered on the PowerManage server.

Two factor authentication in Remote Mode

Note: 2FA is supported on PowerManage version 4.6 and later.

Two factor authentication does not rely on only the installer code to connect the installer to the panel. After the two factor authentication, the installer can add panels to the application.

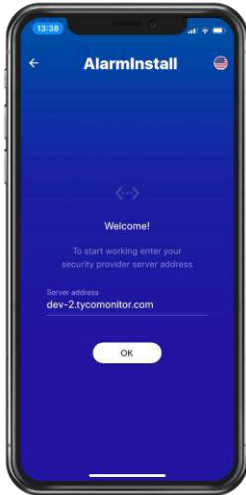
Installers only need to complete two factor authentication once to register in a server in order to access panels but must complete the two factor authentication procedure each time for other servers.

Authenticating in remote mode with two factor authentication

1. Open the AlarmInstall app. First time users must accept the End user license agreement and Privacy Notice.
2. On the connect screen, tap **Remote**.
3. In the Server address field, enter the URL of the PowerManage server you want to connect to and tap **OK**.

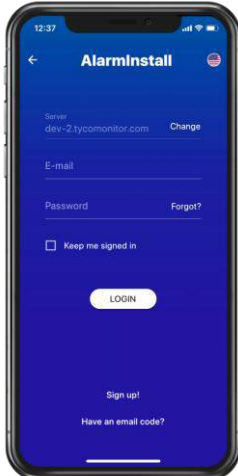
Note: To use the public server, enter: `connect.tycomonitor.com`.

Figure 7: Entering the server address



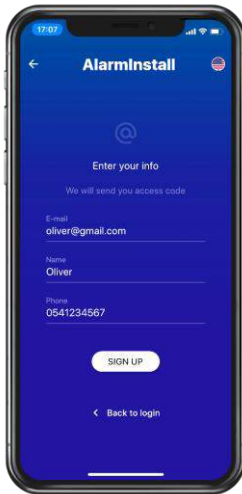
4. Tap **OK**.
5. On the logon screen, tap **Sign up!**.

Figure 8: Signing up to a new server



6. Enter your email address, name, and phone number in the required fields and tap **SIGN UP**.
Note: This information is stored in the PowerManage server. To find the information, open the PowerManage web interface and in the navigation pane, from **System**, select **Installers**.

Figure 9: Entering your logon details



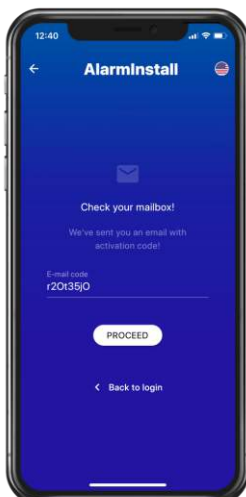
7. An authentication access code is sent to the email address.

Figure 10: Receiving your access code email



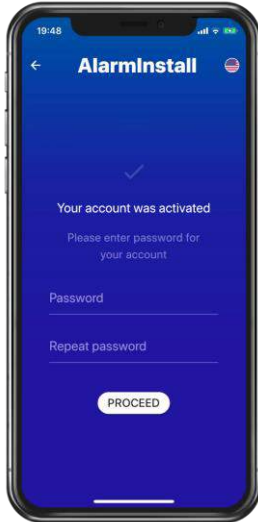
8. Enter your access code in the Email code field and tap **PROCEED**.

Figure 11: Entering your access code



9. Enter a new password in the Password and New password fields and tap **PROCEED**.
Note: If the PowerManage server belongs to a monitoring station, the message **The account has not been approved yet** displays. The central monitoring station must change the installer status from **Pending** to **Accepted** in the PowerManage web interface **Installers** page. For more information, refer to the *PowerManage User Guide*.

Figure 12: Setting a new password



You are now a registered installer with two factor authentication certification. To log on to the server, see [Logging on to a server](#).

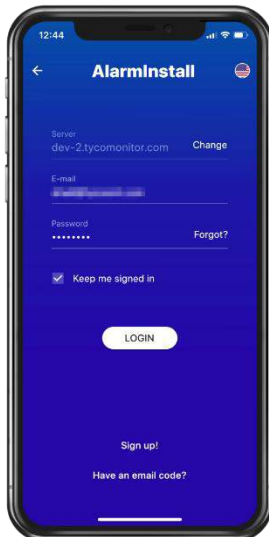
Logging on to a server

Pre-requisite: Complete the two factor authentication procedure in [Authenticating in remote mode with two factor authentication](#).

1. To go to the logon screen, complete one of the following options:
 - Open the AlarmInstall app and on the connect screen, tap **Remote**.
 - If you already enabled 'Keep me signed in', or enabled a biometric log on, you must first log out of the server. In the panels list, tap the menu icon, then tap **Log out**. For more information, see Callout 3 in [Figure 17](#).

Note: To change to a different server, see [Changing and logging on to another server](#).

Figure 13: Logon screen



2. In the Email field, enter the email address. For more information, see [Figure 13](#).
3. In the Password field, enter the password. For more information, see [Figure 13](#).
4. **Optional:** To stay signed in, enable **Keep me signed in**. If your device supports facial recognition or fingerprint scanning, you can also enable the feature at this point. For more information, see [Quick and biometric logon options](#).
5. Tap **LOGIN**.

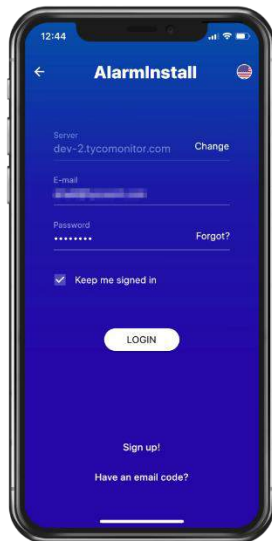
Post-requisite: Add panels to the application. For more information, see [Adding a panel](#).

Note: If an installer tries to log on to a panel that is on a self-monitored server and does not have user permission to access the server, the following message displays: No user permissions. To access the server, see [Approving installer access with homeowner approval with the ConnectAlarm app](#).

Changing and logging on to another server

1. Open the AlarmInstall app and enter the logon screen.
2. To the right of the Server field, tap **Change**.

Figure 14: Changing the server address



3. If you are not registered with the server you want to change to, complete the two factor authentication again. For more information, see [Two factor authentication in Remote Mode](#).

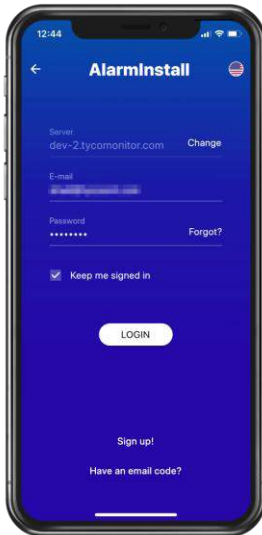
Quick and biometric logon options

To avoid entering a password each time you connect to the app, use a remembered password or biometric options, such as facial recognition and fingerprint scan.

Note: The availability of logon methods depends on the capabilities of your device.

On the logon screen, select the **Keep me signed in** check box.

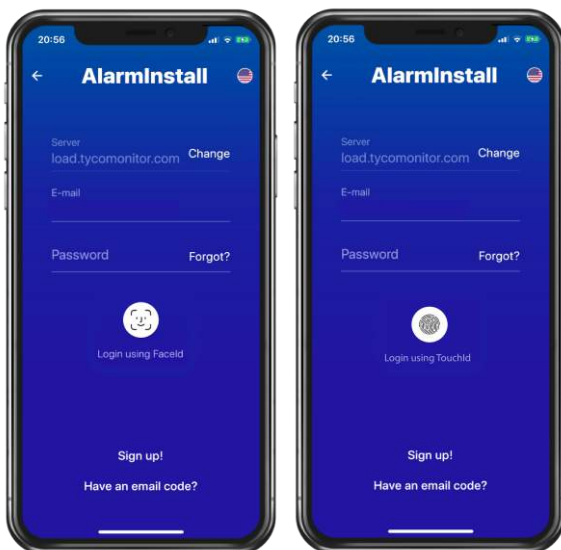
Figure 15: Selecting the Keep me signed in check box



Select one of the following options:

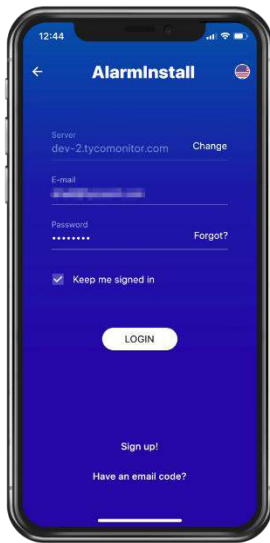
- **Enable FaceId:** Log on to the app with facial recognition.
- **Enable Fingerprint:** Log on to the app with a fingerprint scanner.
- **Remember the password:** Select the checkbox and do not select the other checkboxes.

Figure 16: Biometric logon



Changing the app language on the logon screen

1. Open the AlarmInstall app and enter the logon screen.
2. Tap the US flag to the upper-right of the screen and choose a language.



3. Tap **System default** to use the language of your device, or select the language you want.

Adding panels

Panels list

Installers can add multiple panels to the AlarmInstall app. Panels that you add appear in the panels list.

To edit user information, access the app settings, change your two-factor authentication password and more, see [Panels list menu](#).

Other panel related tasks include the following:

- [Adding a panel](#).
- [Editing a panel name](#).
- [Removing a panel from the AlarmInstall app](#).

Figure 17: Panels list



Table 7: PANELS LIST user interface elements

Callout	Description
1	PANELS LIST. Tap the arrow icon to enter the panel. Note: If an installer tries to log on to a panel that is on a self-monitored server and does not have user permission to access the server, the following message displays: No user permissions. To access the server, see Approving installer access with homeowner approval with the ConnectAlarm app .
2	Edit icon
3	PANELS LIST menu. Tap the menu icon to view a drop-down list. In the list you can perform the following tasks: <ul style="list-style-type: none">• Application settings<ul style="list-style-type: none">○ Changing the app language○ Changing the app theme to light or dark mode○ Changing your two factor authentication password○ Enabling or disabling biometric login with face ID or fingerprint

	<ul style="list-style-type: none">○ Changing the temperature scale to Celsius or Fahrenheit○ Viewing the AlarmInstall app version and build number● Editing user information● Viewing the EULA and Privacy Notice● Logging out of the AlarmInstall app
4	Add panel button

Panel activation for Neo and PSP panels

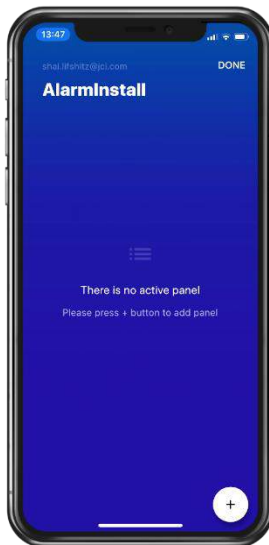
Neo and PSP panels require panel activation with the server but PowerMaster panels do not. The installer code is required for panel activation. If the installer code changes, to activate the panel, in the AlarmInstall app, log in to the panel again with the new installer code. The user app does not work until you activate the panel.

Adding a panel

Pre-requisite: You can only add panels to the AlarmInstall app if the panel is connected to the server.

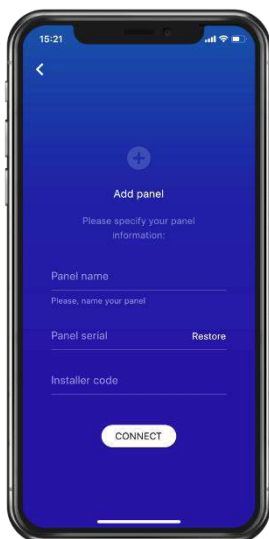
1. Tap the plus button to the bottom-right.

Figure 18: Add panel button



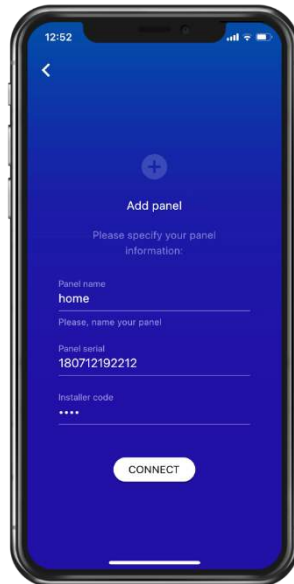
2. **Optional:** If the server is upgraded to PowerManage 4.6, tap **RESTORE** to restore the panels you added previously.

Figure 19: Restoring previously added panels



3. Enter the required information in the following fields:
 - Panel name: Enter a recognizable panel name that appears in the app only.
 - Panel serial: Enter the panel ID. For PowerMaster panels, the six digit ID is on the label on the back of the panel. For Neo and PSP panels, use the integration identification number (installer menu → [851] → [422] twelve digits).
 - Installer code: Enter the installer code.

Figure 19: Entering panel information



4. Tap **CONNECT**.

The panel appears in the panels list.

Note: If you enter incorrect information or if the panel does not connect to the server after three logon attempts, the following message displays: User is temporarily blocked. The application is blocked for 300 seconds. After 300 seconds, you can try to add the panel again.

Editing a panel name

1. On the panels list screen, tap the pencil icon to the upper-right. For more information, see Callout 2 in [Figure 17](#).
2. In the panels list, find the panel and tap the pencil icon next to the panel.
3. Edit the required PANELS LIST information.
4. Tap **OK**.

Removing a panel from the AlarmInstall app

1. On the panels list screen, tap the pencil icon to the upper-right. For more information, see Callout 2 in [Figure 17](#).
2. In the PANELS LIST, find the panel you want to remove.
3. Tap the minus icon next to the panel.
4. Enter your password and tap **REMOVE**.

Application settings

You can view or edit the following settings in the AlarmInstall app:

- Change the app language
- Change the app theme to light or dark mode
- Change your two-factor authentication password
- Enable or disable biometric login with face ID or fingerprint
- Change the temperature scale to Celsius or Fahrenheit
- View the app version number and the build number

Changing the app language

1. **Optional:** If you are completing the two-factor logon process, tap the flag icon to the upper-right and select the language you want.
2. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
3. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
4. Tap **Application settings**.
5. From the Application settings list, tap **Language**.
6. From the Language list, select the desired language.
Note: Select **System default** to use the language of your phone.

Changing the app theme to light or dark mode

1. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
3. Tap **Application settings**.
4. **Optional:** From Theme, enable **Light**.
5. **Optional:** From Theme, enable **Dark**.
6. To exit, tap the back arrow.

Changing your two factor authentication password

1. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
3. Tap **Application settings**.
4. Tap **Change password**.
5. In the Current password field, enter your current password.
6. In the New password and Repeat password fields, enter your new password.
7. Tap **CHANGE**.

Enabling or disabling biometric login with face ID or fingerprint

1. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
3. Tap **Application settings**.
4. **Optional:** To enable biometric login, enable **Use biometric login**.
5. **Optional:** To disable biometric login, disable **Use biometric login**.
6. To exit, tap the back arrow.

Changing the temperature scale to Celsius or Fahrenheit

1. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
3. Tap **Application settings**.
4. **Optional:** To use Celsius, from Temperature scale, enable **Celsius**.
5. **Optional:** To use Fahrenheit, from Temperature scale, disable **Celsius**.
6. To exit, tap the back arrow.

Viewing the AlarmInstall app version and build number

1. **Optional:** If you are on the PANEL LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** If you are connected to a panel, tap the menu icon to the upper-left. For more information, see Callout 1 in in [Figure 21](#).
3. Tap **Application settings**.

4. In DEVELOPER INFORMATION, the application version number and the build number display.
5. To exit, tap the back arrow.

Editing user information

To edit the installer name and phone number as they appear in the **Installers** page in the PowerManage, complete the following steps:

Note: To access the Installers page in the PowerManage web app, from the navigation pane, click the **System** drop down menu, then click **Installers**.

1. In the AlarmInstall app, tap the menu icon to the upper-right.
2. Tap **User information**.
3. **Optional:** In the Name field, enter or edit the installer name.
4. **Optional:** In the Phone field, enter or edit the installer phone number.
5. To save the changes, tap **CHANGE**. To discard the changes, tap the back arrow to the top left.

Viewing the EULA and Privacy Notice

1. From the PANELS LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. **Optional:** Tap **EULA**.
3. **Optional:** Tap **Privacy Notice**.

Logging out of the AlarmInstall app

1. From the PANELS LIST screen, tap the menu icon to the upper-right. For more information, see Callout 3 in in [Figure 17](#).
2. Tap **Logout**.

Managing the security system

Approving installer access with homeowner approval with the ConnectAlarm app

If an installer logs on to a server that is self-monitored, the homeowner must complete the following steps to grant the installer access to the panel:

1. The homeowner opens the ConnectAlarm app.
2. The homeowners taps the menu icon to the upper left. For more information, see Callout 1 in [Figure 20](#).
3. From the menu, the homeowner taps **Installer access**. For more information, see Callout 2 in [Figure 20](#).
4. In the AlarmInstall app, the installer finds the panel that requires installer access and taps the enter icon. For more information, see Callout 3 in [Figure 20](#).
5. The installer enters the installer code and taps **PROCEED**.

Important: For Neo and PSP panels, if the installer code changes, you must enter the new installer code each time or the server will not support the panel. This is called panel activation.

Figure 20: Approving installer access with user approval in the ConnectAlarm app

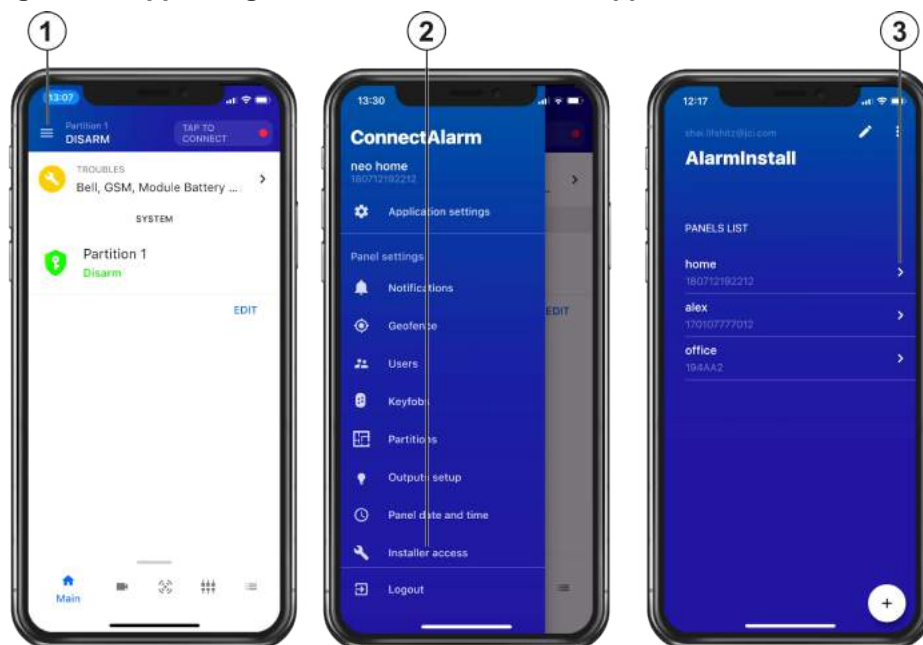


Table 8: Approving installer access with user approval in the ConnectAlarm app

Callout	Description
1	Menu
2	Installer access
3	Panel selection

AlarmInstall app interface

You can configure, monitor, test, and troubleshoot security systems in the AlarmInstall app.

General

Figure 21: General layout

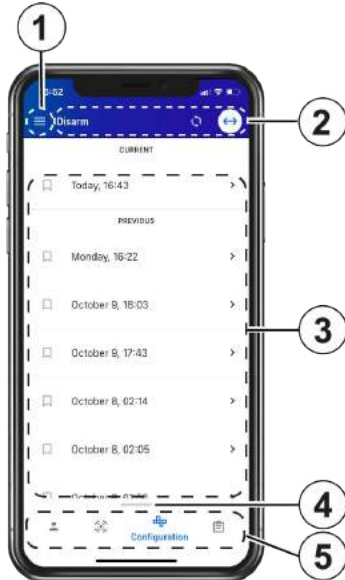








Table 9: General layout of user interface elements

Callout	Name	Description
1	Menu	Tap to access the following: <ul style="list-style-type: none"> Application settings: <ul style="list-style-type: none"> App language Light and dark theme Change two-factor authentication password Biometric login options Temperature measurement standard Remote inspections: Start a remote inspection that checks a panel remotely for any faults that affect the system and its functionality. In the inspection output, a red X indicates a failed test and a green tick indicates a successful test. Tap a test to view more information. Logout
2	Panel and connection status	View the panel arm status and connection status. For more information on the connection status, see Connection status .
3	Tab contents	Displays the information of the tab you open.
4	Process pane	Swipe up the tab bar to view the progress of any ongoing processes.
5	Tab bar	Tap an icon to open the tab. The tab bar contains the following tabs: Customer info, Diagnostics, Configuration, Location, and Log.

Connection status

Use this area to view the panel's connection status. For more information, see Callout 2 in [Figure 21](#). Tap the connection status icon to enlarge it.

Table 10: Connection status user interface elements

Name	Description	
Connected status		The panel and the server are connected.
		
Online status		The panel recently connected to the server but is not actively connected.
		
Offline status		There is no connection between the panel and the server.
		

Running a remote inspection

1. From the PANELS LIST, tap the panel you want to inspect remotely.
2. To the top-left, tap the menu icon.
3. Tap **Remote Inspections**.
4. Tap **INITIATE NOW**.

The remote inspection starts. In the inspection output, a red X indicates a failed test and a green check mark indicates a successful test. Tap a test to view more information.

Customer info tab

The Customer info tab displays information about the customer, such as email address, phone number, and home address. For more information, see Callout 3 in [Figure 22](#).

Note: Customer personal data is used only for security purposes, and is related directly with the panel that is connected to this server.

To edit customer information, tap **Edit** and make the required changes. For more information, see Callout 4 in [Figure 22](#).

The information in this tab synchronizes with the information on the INFO tab in the PowerManage web interface. Personal customer data is used for security purposes only.

Figure 22: Customer info tab

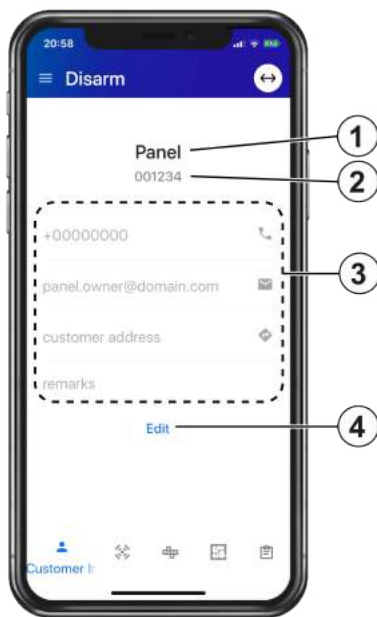


Table 11: Customer info tab user interface elements

Callout	Description
1	Customer panel name
2	Panel account number
3	Customer information
4	Edit customer information

Diagnostics tab

Each device displays basic information such as type, icon, zone, location, troubles, and alarms.

Figure 23: Diagnostics tab

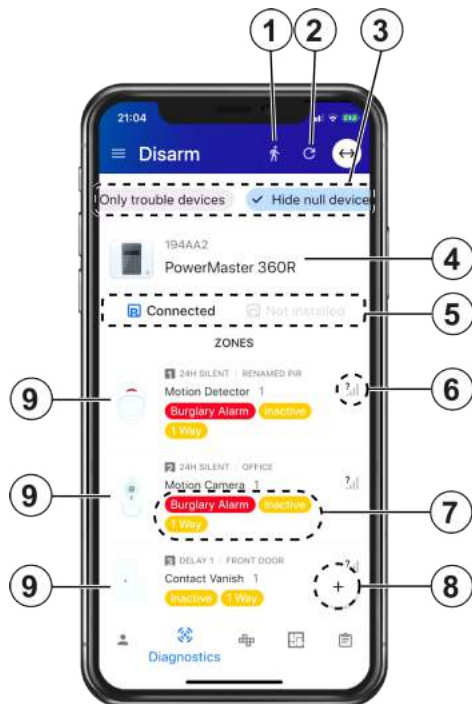


Table 12: Diagnostics tab user interface elements

Callout	Name	Description
1	Walk test	Tap to start a walk test of the panel and devices.
2	Refresh RSSI	Tap to refresh the RSSI readings. For more information, see RSSI.
3	Only trouble devices/Hide null devices	To access the buttons, swipe down from the top of the screen.
		To show devices with troubles only, enable Only trouble devices .
		To hide wired devices that are defined as not existing, enable Hide null devices .
4	Panel	
5	IP and GPRS connection	Displays the connection status of the Internet Protocol. If there is no connection defined, the icon appears greyed.
		Displays the connection status of the GPRS. If there is no connection defined, the icon appears greyed.
6	RSSI	Displays the received signal strength between the device and panel on a scale of one to four bars.
		The question mark in the RSSI icon indicates the RSSI was never read.
7	Alerts and alarms	<ul style="list-style-type: none"> • Yellow color: <ul style="list-style-type: none"> ○ Type ○ Icon ○ Zone ○ Location ○ Troubles

		<ul style="list-style-type: none"> • Red color: <ul style="list-style-type: none"> ○ Alarms
8	Add device	Tap to enroll a new device in the panel. To complete the procedure, enter the device ID or scan the label on the device.
9	Device	<p>To view information about a particular panel or device, tap the device.</p> <p>To change the configuration settings of a panel or device, tap the device, then tap the Configuration tab. For more information about configuration, see Configuration tab.</p> <p>Note:</p> <ul style="list-style-type: none"> • If there is no configuration available, to download the configuration, tap DOWNLOAD. • If the configuration was changed since the last download, to refresh the configuration, tap REFRESH.

Figure 24: Diagnostics tab device inspection

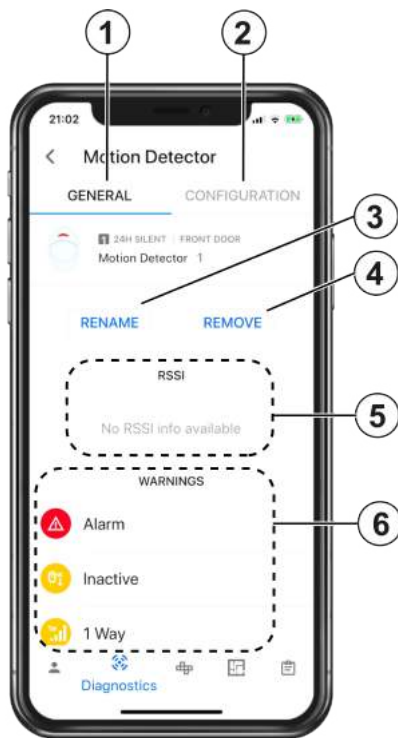


Table 13: Device inspection interface elements

Callout	Name	Description
1	GENERAL tab	Contains general information about the device, such as RSSI and warnings.
2	CONFIGURATION tab	Tap to configure the device
3	RENAME	Tap to rename the device
4	REMOVE	Tap to remove the device Note: For wired zones, DISABLE displays instead of REMOVE. To change the zone type to null zone, tap DISABLE .
5	RSSI	Displays received signal strength indication information
6	WARNINGS	Displays alerts and alarms

Figure 25: Walk test

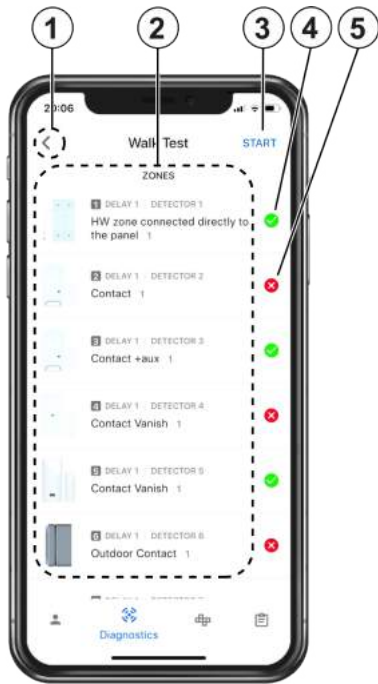


Table 14: Walk test user interface elements

Callout	Name	Description
1	Back	Tap the back icon to return to the Diagnostics tab.
2	Walk Test list	Devices display in the Walk Test list.
3	START	Tap to start the walk test.
4	Success	The device did not fail in the walk test.
5	Failure	The device failed in the walk test.

Performing a walk test in the Diagnostics tab.

1. To enter the walk test screen, tap the walk test icon. The previous walk test displays. For more information, see Callout 1 in [Figure 23](#).
2. To start a walk test, tap **START**. For more information, see Callout 3 in [Figure 25](#).
3. Review the walk test results. The red X symbol signifies device failure and the green check mark signifies success in the walk test. For more information, see Callout 4 and Callout 5 in [Figure 25](#).

Configuration tab

Figure 26: Configuration tab

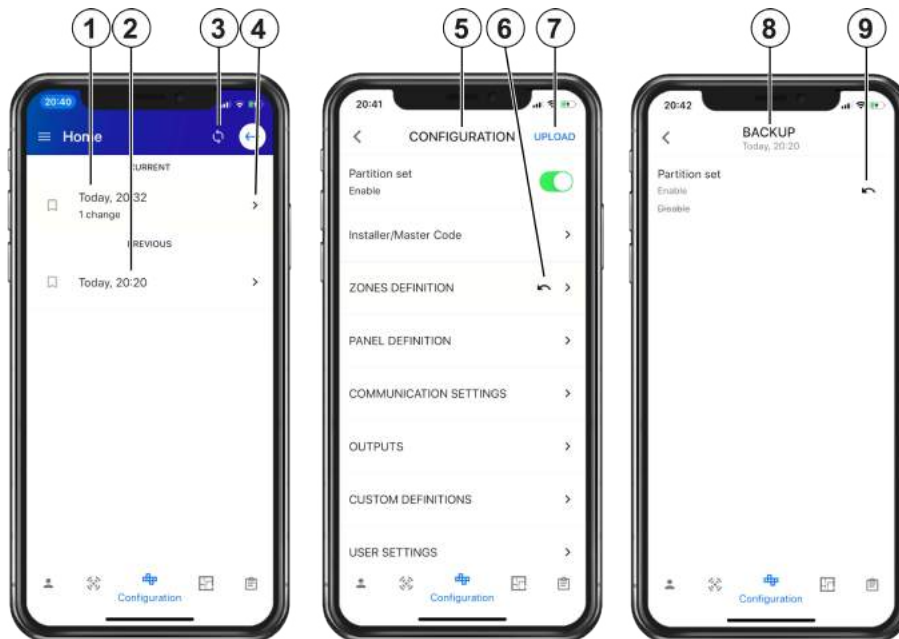


Table 15: Configuration tab user interface elements

Callout	Name	Description
1	CURRENT configuration	Tap to edit the current configuration. For more information about editing a configuration, see Editing the current configuration on the Configuration tab .
2	PREVIOUS configuration list	Previous configurations appear in the PREVIOUS list. Only differences to the current configuration display. For more information about editing a previous configuration, see Editing a previous configuration on the Configuration tab .
3	Refresh	Tap the refresh icon to load the most up-to-date configuration from the panel. Note: A new configuration is created only if there are differences between the configuration in the panel and the current configuration. If a new configuration is created, the current configuration is now a previous configuration and added to the PREVIOUS list.
4	Enter arrow	Tap to open the configuration in the CONFIGURATION page.
5	CONFIGURATION page	View and change the current configuration.
6	Revert	Tap to revert the configuration. Note: The revert icon only appears for configuration parameters that are different from the CURRENT configuration.
7	UPLOAD	Tap to upload your changes to the panel. Note: UPLOAD only appears if you change a configuration parameter.
8	Previous configuration	Tap a previous configuration in the PREVIOUS configuration list to view the parameters that differ from the current configuration.
9	Revert	Tap the revert icon to revert to the previous configuration parameter.

Editing the current configuration on the Configuration tab

1. In the Configuration tab, tap the arrow icon of the CURRENT configuration. For more information on the arrow icon, see Callout 4 in [Figure 26](#).
2. From the CONFIGURATION navigation tree, navigate the tree to find the parameter you want to change.
3. Change the parameter to the value you want.
Note: Tap the revert icon to revert any configuration changes before you upload the new configuration. For more information on the revert icon, see Callout 6 in [Figure 26](#).
4. **Optional:** Continue to make more configuration changes in the navigation tree.
5. To upload the updated configuration to the panel, tap **UPLOAD**. For more information on UPLOAD, see Callout 7 in [Figure 26](#).
Note: If you do not tap UPLOAD, the changed values are stored locally on the phone for 90 days.

Editing a previous configuration on the Configuration tab

1. From the PREVIOUS list, tap a previous configuration.
2. Tap the revert parameter icon to revert the parameter to the previous value. Only parameters that differ from the current configuration display. For more information on the revert icon, see Callout 6 in [Figure 26](#).
3. To upload the change to the panel, tap **UPLOAD**. For more information on UPLOAD, see Callout 7 in [Figure 26](#).

Locations tab

Note: The Locations tab only appears for PowerMaster panels.

The Locations tab displays a list of locations that are under supervision by an alarm system. A location is a familiar name given to a zone.

To change a location name, from the list, tap the location and enter a new name.

Figure 27: Location tab



Log tab

The Log tab displays the panel log.

To download a log file, tap **DOWNLOAD**.

To refresh the log, tap the refresh icon to the upper-right. For more information, see Callout 3 in [Figure 28](#).

Note: PowerMaster panels have two logs: the STANDARD LOG and the LEGACY LOG. The standard log records specific events, such as burglar alarms. It is not possible to delete the standard log and users cannot view it. Visonic panels have a legacy log. Users can view legacy logs and installers can view and delete them.

Neo and PSP panels have one log file that is the same as the Visonic LEGACY LOG. For more information, see Callout 4 in [Figure 28](#).

Figure 28: Standard and legacy logs

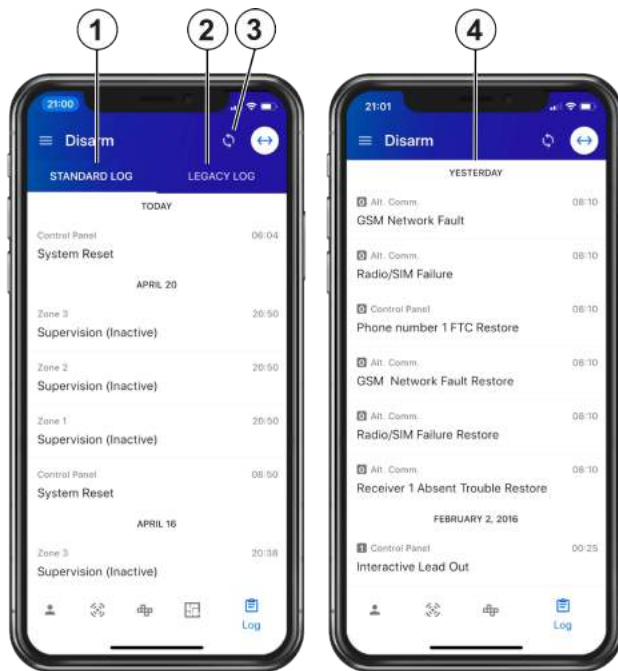


Table 16: Standard and legacy logs

Callout	Description
1	Visonic STANDARD LOG
2	Visonic LEGACY LOG. For more information, see Callout 4.
3	Refresh icon
4	DSC log