IMS**4000**
Infrastructure Monitoring System

USER'S MANUAL

VERSION 5.1

SENSAPHONE®
REMOTE MONITORING SOLUTIONS

Every effort has been made to ensure that the information in this document is complete, accurate and up-to-date. Sensaphone assumes no responsibility for the results of errors beyond its control. Sensaphone also cannot guarantee that changes in equipment made by other manufacturers, and referred to in this manual, will not affect the applicability of the information in this manual.

IMPORTANT SAFETY INSTRUCTIONS

Your IMS-4000E has been carefully designed to give you years of safe, reliable performance. As with all electrical equipment, however, there are a few basic precautions you should take to avoid hurting yourself or damaging the unit:

- Read the installation and operating instructions in this manual carefully. Be sure to save it for future reference.

- Read and follow all warning and instruction labels on the product itself.

- To protect the IMS-4000E from overheating, make sure all openings on the unit are not blocked. Do not place on or near a heat source, such as a radiator or heat register.

- Do not use your IMS-4000E near water, or spill liquid of any kind into it.

- Be certain that your power source matches the rating in the specifications of this manual. If you're not sure of the type of power supply to your facility, consult your dealer or local power company.

- Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.

- Do not overload wall outlets and extension cords, as this can result in the risk of fire or electric shock.

- To reduce the risk of electric shock, the power supply cord for the IMS-4000E Host must have a grounded lug.

- The IMS-4000E Host power supply cord must be used in accordance with applicable UL/CSA/EN/IEC standards, and must meet the conductor size and length terms of the above-mentioned standards.

- All IMS-4000E components (Host, Node, PowerGate and PowerGate2) must be plugged into a grounded outlet.

- Never push objects of any kind into this product through ventilation holes as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock.

- To reduce the risk of electric shock, do not disassemble this product, but return it to Sensaphone Customer Service, or another approved repair facility, when any service or repair work is required. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock when the unit is subsequently used.

- If anything happens that indicates that your IMS-4000E is not working properly or has been damaged, unplug it immediately and follow the procedures in the manual for having it serviced. Return the unit for servicing under the following conditions:

    1. The power cord or plug is frayed or damaged.

    2. Liquid has been spilled into the product or it has been exposed to water.

    3. The unit has been dropped, or the enclosure is damaged.

    4. The unit doesn't function normally when you're following the operating instructions.

- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

- Do not use the telephone to report a gas leak in the vicinity of the leak.

- To reduce the risk of fire or injury to persons, read and follow these instructions:

    1. Use only the specified type and size batteries.

    2. Do not dispose of the batteries in a fire. The cell may explode. Check with local codes for possible special disposal instructions.

    3. Do not open or mutilate batteries. Released electrolyte is corrosive and may cause damage to the eyes or skin. It may be toxic if swallowed.

    4. Exercise care in handling batteries in order not to short the battery with conducting materials such as rings, bracelets, and keys. The battery or conductor may overheat and cause burns.

    5. Remove main power and telephone connections before replacing the battery.

WICHTIGE SICHERHEITSHINWEISE

Ein wesentlicher Aspekt bei der Entwicklung Ihres IMS-4000E war die Gewährleistung eines sicheren und zuverlässigen Betriebs über viele Jahre hinweg. Wie bei allen elektrisch betriebenen Einrichtungen sollten Sie jedoch auch hier einige grundlegende Vorsichtsmaßnahmen beachten, um Schäden am Gerät und Verletzungen zu vermeiden:

- Die Installations- und Betriebsanweisungen in diesem Handbuch aufmerksam und vollständig durchlesen. Das Handbuch für den Fall aufbewahren, dass Sie es in Zukunft noch mal benötigen.

- Alle am Produkt angebrachten Etiketten mit Warnungen und Vorschriften lesen und beachten.

- Um das IMS-4000E vor Überhitzung zu schützen, niemals die Lüftungsöffnungen des Geräts blockieren. Das Gerät nicht auf oder in der Nähe einer Wärmequelle (Heizkörper, Heizschacht) aufstellen.

- Das IMS-4000E nicht in unmittelbarer Umgebung von Wasser verwenden. Keine Flüssigkeiten in das Systemgehäuse gelangen lassen.

- Sicherstellen, dass die verwendete Stromquelle derjenigen entspricht, die in den technischen Daten dieses Handbuchs angegeben ist. Wenn Sie nicht wissen, welche Art von Stromquelle in Ihrer Anlage zum Einsatz kommt, wenden Sie sich an Ihren Händler oder den örtlichen Energieversorger.

- Keine Gegenstände auf dem Netzkabel abstellen. Dieses Produkt nicht so aufstellen, dass Personen auf das Netzkabel treten und es beschädigen können.

- Netzsteckdosen und Verlängerungskabel nicht überlasten. Es besteht Feuer- und Stromschlaggefahr.

- Um das Stromschlagrisiko zu senken, für den IMS-4000E-Host ausschließlich ein Netzkabel mit Schutzkontaktstecker verwenden.

- Das Netzkabel des IMS-4000E-Hosts ist in Übereinstimmung mit den anwendbaren UL-/CSA-/EN-/IEC-Normen bzw. den entsprechenden in Ihrem Land gültigen Normen zu verwenden. Die Vorschriften der genannten Normen in bezug auf die Abmessungen und Längen von Leitern sind einzuhalten.

- Alle IMS-4000E-Komponenten (Host, Knoten, PowerGate und PowerGate2) müssen an eine geerdete Netzsteckdose angeschlossen werden.

- Niemals Gegenstände welcher Art auch immer durch die Lüftungsöffnungen in das Gehäuse des Produkts stecken, da die Gefahr besteht, dass spannungsführende Teile berührt oder Kurzschlüssen verursacht werden, die zu einem Brand oder Stromschlag führen können.

- Um das Stromschlagrisiko zu senken, das Produkt nicht zerlegen, sondern bei erforderlichen Wartungs- oder Reparaturarbeiten zum Sensaphone-Kundendienst oder zu einer anderen zugelassenen Werkstatt geben. Beim Öffnen oder Entfernen von Abdeckungen und Blenden bestehen verschiedene Gefahren, wie etwa die Möglichkeit des Kontakts mit gefährlichen Spannungen. Ferner kann ein unsachgemäßer Zusammenbau zu einem Stromschlag führen, wenn das Gerät anschließend in Betrieb genommen wird.

- Wenn Sie feststellen, dass Ihr IMS-4000E nicht einwandfrei funktioniert oder beschädigt wurde, das Gerät umgehend vom Netz trennen und die im Handbuch stehende Anleitung zur Kontrolle und Reparatur befolgen.

Das Gerät unter folgenden Umständen in Reparatur geben:

1. Netzkabel oder -stecker sind verschlissen oder beschädigt.

2. Flüssigkeit ist in das Gehäuse eingedrungen, oder das Produkt ist mit Wasser in Berührung gekommen.

3. Das Gerät wurde fallengelassen oder das Gehäuse ist beschädigt.

4. Das Gerät funktioniert trotz Beachtung der Betriebsanleitung nicht einwandfrei.

- Während eines Gewitters kein schnurgebundenes Telefon verwenden. Es besteht Stromschlagrisiko durch Blitzeinschlag.

- Gasaustritt niemals telefonisch melden, wenn Sie sich in unmittelbarer Umgebung des Gaslecks befinden.

- Um das Feuer- und Verletzungsrisiko zu verringern, die folgenden Anweisungen lesen und beachte:

1. Nur Akkumulatoren verwenden, die nach Typ und Größe der Herstellerempfehlung entsprechen.

2. Akkumulatoren nie ins Feuer werfen. Es besteht Explosionsgefahr. Gesetzliche Entsorgungsvorschriften beachten.

3. Akkumulatoren nicht öffnen oder beschädigen. Der freigesetzte Elektrolyt ist ätzend und kann Augen- und Hautschäden verursachen. Bei Verschlucken besteht Vergiftungsgefahr.

4. Beim Umgang mit Akkumulatoren mit Sorgfalt vorgehen, damit die Pole nicht durch leitende Materialien wie Ringe, Armbänder oder Schlüssel kurzgeschlossen werden. Es besteht die Gefahr der Erhitzung von Akkumulator oder Leiter und infolgedessen Verbrennungsgefahr.

5. Netz- und Telefonleitungen vor Austausch des Akkumulators trennen.

FCC REQUIREMENTS

Part 68: The Sensaphone IMS-4000E complies with 47 CFR, Part 68 of the rules. On the back of the unit there is a label that contains, among other information, the Certification Number and the Ringer Equivalence Number (REN) for this equipment. You must, upon request, provide this information to your local telephone company.

The REN is useful to determine the quantity of devices that you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN's of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices that you may connect to your line, you may want to contact your local telephone company to determine the maximum REN for your calling area.

The applicable certification jack USOC for this equipment is: RJ11C. The facility interface code (FIC) for this equipment is: 02LS2.

A compliant telephone cord and modular plug are provided with equipment. This equipment is designated to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant. See Installation Instructions for details.

This equipment may not be used on coin service units provided by the telephone company. Connection to party lines is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Should the IMS-4000E cause harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, the telephone company may temporarily discontinue service without notice and you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. The telephone company may make changes in its facilities, equipment, operations, or procedures where such action is reasonably required in the operation of its business and is not inconsistent with the rules and regulations of the FCC that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with the Sensaphone IMS-4000E, or you need information on obtaining service or repairs, please contact:

Sensaphone
901 Tryens Road
Aston, PA 19014

877.373.2700

If the equipment is causing harm to the telephone network, the telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

Part 15: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

TELEPHONE CONSUMER PROTECTION ACT (HOST ONLY)

The FCC Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device, including FAX machines, to send a message unless such message contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business or other entity, or other individual sending the message, and the telephone number of the sending machine or such business, other entity, or individual. (The telephone number provided may not be a 900 number or any other number for which charges exceed local or long-distance transmission charges.)

To comply with this law, you must enter the following information into your IMS-4000E:

- Date and Time as described in the Unit Properties section of the Software Manual.
- Name and telephone number to identify the source of the FAX transmission, as shown in the Unit Properties section of the Software Manual.

GENERAL REQUIREMENTS FOR ALL AUTOMATIC DIALERS (HOST ONLY)

When programming emergency numbers and (or) making test calls to emergency numbers:

1. Remain on the line and briefly explain to the dispatcher the reason for the call.
2. Perform such activities in the off-peak hours, such as early morning or late evenings.

Canadian Department of Communications Statement (Host only)

Notice: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Ringer Equivalence Number (REN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Ringer Equivalence Numbers of all the devices does not exceed 5.0. For IMS-4000E, the Ringer Equivalence Number is 0.0.

The third-party trademarks mentioned below are the property of their respective owners

Licenses and notices for third party software used in this product are listed below:" .

This product contains software provided by NGINX and its contributors.

Copyright (C) 2002-2021 Igor Sysoev

Copyright (C) 2011-2023 Nginx, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

/ zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.13, October 13th, 2022

Copyright (C) 1995-2022 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly   Mark Adler

jloup@gzip.org   madler@alumni.caltech.edu

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: Philip.Hazel

Email domain: gmail.com

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2021 University of Cambridge

All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg

Email local part: hzmester

Email domain: freemail.hu

Copyright(c) 2010-2021 Zoltan Herczeg

All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg

Email local part: hzmester

Email domain: freemail.hu

Copyright(c) 2009-2021 Zoltan Herczeg

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007-2012, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

===

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

3 YEAR LIMITED WARRANTY

PLEASE READ THIS WARRANTY CAREFULLY BEFORE USING THE PRODUCT.

THIS LIMITED WARRANTY CONTAINS SENSAPHONE'S STANDARD TERMS AND CONDITIONS. WHERE PERMITTED BY THE APPLICABLE LAW, BY KEEPING YOUR SENSAPHONE PRODUCT BEYOND THIRTY (30) DAYS AFTER THE DATE OF DELIVERY, YOU FULLY ACCEPT THE TERMS AND CONDITIONS SET FORTH IN THIS LIMITED WARRANTY.
IN ADDITION, WHERE PERMITTED BY THE APPLICABLE LAW, YOUR INSTALLATION AND/OR USE OF THE PRODUCT CONSTITUTES FULL ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS LIMITED WARRANTY (HEREINAFTER REFERRED TO AS "LIMITED WARRANTY OR WARRANTY"). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS WARRANTY, INCLUDING ANY LIMITATIONS OF WARRANTY, INDEMNIFICATION TERMS OR LIMITATION OF LIABILITY, THEN YOU SHOULD NOT USE THE PRODUCT AND SHOULD RETURN IT TO THE SELLER FOR A REFUND OF THE PURCHASE PRICE. THE LAW MAY VARY BY JURISDICTION AS TO THE APPLICABILITY OF YOUR INSTALLATION OR USE ACTUALLY CONSTITUTING ACCEPTANCE OF THE TERMS AND CONDITIONS HEREIN AND AS TO THE APPLICABILITY OF ANY LIMITATION OF WARRANTY, INDEMNIFICATION TERMS OR LIMITATIONS OF LIABILITY.
1. WARRANTOR: In this Warranty, Warrantor shall mean "Dealer, Distributor, and/or Manufacturer."
2. ELEMENTS OF WARRANTY: This Product is warranted to be free from defects in materials and craftsmanship with only the limitations and exclusions set out below.
3. WARRANTY AND REMEDY: Three-Year Warranty — In the event that the Product does not conform to this warranty at any time during the time of three years from original purchase, warrantor will repair the defect and return it to you at no charge.
This warranty shall terminate and be of no further effect at the time the product is: (1) damaged by extraneous cause such as fire, water, lightning, etc. or not maintained as reasonable and necessary; or (2) modified; or (3) improperly installed; or (4) misused; or (5) repaired or serviced by someone other than Warrantors' authorized personnel or someone expressly authorized by Warrantor's to make such service or repairs; (6) used in a manner or purpose for which the product was not intended; or (7) sold by original purchaser.
LIMITED WARRANTY, LIMITATION OF DAMAGES AND DISCLAIMER OF LIABILITY FOR DAMAGES: THE WARRANTOR'S OBLIGATION UNDER THIS WARRANTY IS LIMITED TO REPAIR OR REPLACEMENT OF THE PRODUCT, AT THE WARRANTOR'S OPTION AS TO REPAIR OR REPLACEMENT. IN NO EVENT SHALL WARRANTORS BE LIABLE OR RESPONSIBLE FOR PAYMENT OF ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL AND/OR PUNITIVE DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LABOR COSTS, PRODUCT COSTS, LOST REVENUE, BUSINESS INTERRUTPION LOSSES, LOST PROFITS, LOSS OF BUSINESS, LOSS OF DATA OR INFORMATION, OR FINANCIAL LOSS, FOR CLAIMS OF ANY NATURE, INCLUDING BUT NOT LIMITED TO CLAIMS IN CONTRACT, BREACH OF WARRANTY OR TORT, AND WHETHER OR NOT CAUSED BY WARRANTORS' NEGLIGENCE. IN THE EVENT THAT IT IS DETERMINED IN ANY ADJUDICATION THAT THE LIMITED WARRANTIES OF REPAIR OR REPLACEMENT ARE INAPPLICABLE, THEN THE PURCHASER'S SOLE REMEDY SHALL BE PAYMENT TO THE PURCHASER OF THE ORIGINAL COST OF THE PRODUCT, AND IN NO EVENT SHALL WARRANTORS BE LIABLE OR RESPONSIBLE FOR PAYMENT OF ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL AND/OR PUNITIVE DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST REVENUE, BUSINESS INTERRUTPION LOSSES, LOST PROFITS, LOSS OF BUSINESS, LOSS OF DATA OR INFORMATION, OR FINANCIAL LOSS, FOR CLAIMS OF ANY NATURE, INCLUDING BUT NOT LIMITED TO CLAIMS IN CONTRACT, BREACH OF WARRANTY OR TORT, AND WHETHER OR NOT CAUSED BY WARRANTORS' NEGLIGENCE.
WITHOUT WAIVING ANY PROVISION IN THIS LIMITED WARRANTY, IF A CIRCUMSTANCE ARISES WHERE WARRANTORS ARE FOUND TO BE LIABLE FOR ANY LOSS OR DAMAGE ARISING OUT OF

MISTAKES, NEGLIGENCE, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR DEFECTS IN WAR-RANTORS' PRODUCTS OR SERVICES, SUCH LIABILITY SHALL NOT EXCEED THE TOTAL AMOUNT PAID BY THE CUSTOMER FOR WARRANTORS' PRODUCT AND SERVICES OR $250.00, WHICHEVER IS GREATER. YOU HEREBY RELEASE WARRANTORS FROM ANY AND ALL OBLIGATIONS, LIABILITIES AND CLAIMS IN EXCESS OF THIS LIMITATION.

INDEMNIFICATION AND COVENANT NOT TO SUE: YOU WILL INDEMNIFY, DEFEND AND HOLD HARMLESS WARRANTORS, THEIR OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLI-ERS OR AFFILIATED COMPANIES, AGAINST ANY AND ALL CLAIMS, DEMANDS OR ACTIONS BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIMITED TO DAMAG-ES THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM THE INSTALLATION, OPERATION, USE OF, OR INABILITY TO USE WARRANTORS' PRODUCTS AND SERVICES, OR FROM THE FAILURE OF THE WARRANTORS' SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY WARRANTORS' NEGLIGENCE.

YOU AGREE TO RELEASE, WAIVE, DISCHARGE AND COVENANT NOT TO SUE WARRANTORS, THEIR OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATED COM-PANIES, FOR ANY AND ALL LIABILITIES POTENTIALLY ARISING FROM ANY CLAIM, DEMAND OR ACTION BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIM-ITED TO DAMAGES THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM THE INSTALLA-TION, OPERATION, USE OF, OR INABILITY TO USE WARRANTORS' PRODUCTS AND SERVICES, OR FROM THE FAILURE OF THE WARRANTORS' SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY WARRANTORS' NEGLIGENCE, EXCEPT AS NECESSARY TO ENFORCE THE EXPRESS TERMS OF THIS LIMITED WARRANTY.

EXCLUSIVE WARRANTY: THE LIMITED WARRANTY OR WARRANTIES DESCRIBED HEREIN CONSTI-

TUTE THE SOLE WARRANTY OR WARRANTIES TO THE PURCHASER. ALL IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED, INCLUDING: THE WARRANTY OF MERCHANTIBILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR USE AND THE WARRANTY OF FITNESS FOR A PARTIC-ULAR PURPOSE AND THE WARRANTY OF NON-INFRINGEMENT AND/OR ANY WARRANTY ARIS-ING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

It must be clear that the Warrantors are not insuring your premises or business or guaranteeing that there will not be damage to your person or property or business if you use this Product. You should maintain insurance coverage sufficient to provide compensation for any loss, damage, or expense that may arise in connection with the use of products or services, even if caused by Warrantors' negligence. The warrantors assume no liability for installation of the Product and/or interruptions of the service due to strikes, riots, floods, fire, and/or any cause beyond Seller's control, further subject to the limitations expressed in any License Agreement or other Agreement provided by Warrantors to purchaser.

The agreement between the Warrantors and the Purchaser, including but not limited to the terms and conditions herein shall not be governed by the Convention for the International Sale of Goods. Where applicable, the Uniform Commercial Code as adopted by the State of Delaware shall apply.

4. PROCEDURE FOR OBTAINING PERFORMANCE OF WARRANTY: In the event that the Product does not conform to this warranty, the Product should be shipped or delivered freight prepaid to a Warrantor with evidence of original purchase.

5. LEGAL REMEDIES AND DISCLAIMER: Some jurisdictions may not allow, or may place limits upon, the exclusion and/or limitation of implied warranties, incidental damages and/or consequential damages for some types of goods or products sold to consumers and/or the use of indemnification terms. Thus, the exclusions, indemnification terms and limitations set out above may not apply, or may be limited in their application, to you. If the implied warranties can not be excluded, and the applicable law permits limiting the duration of implied warranties, then the implied warranties herein are to be limited to the same duration as the applicable written warranty or warranties herein. The warranty or warranties herein may give you specific legal rights that will depend upon the applicable law. You may also have other legal rights depending upon the law in your jurisdiction.

6. CHOICE OF FORUM AND CHOICE OF LAW: In the event that a dispute arises out of or in connection with this Limited Warranty, then any claims or suits of any kind concerning such disputes shall only and exclusively be brought in either the Court of Common Pleas of Delaware County, Pennsylvania or the United States District Court for the Eastern District of Pennsylvania.

Regardless of the place of contracting or performance, this Limited Warranty and all questions relating to its validity, interpretation, performance and enforcement shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to the principles of conflicts of law.

Effective date 01/01/2021
SENSAPHONE
901 Tryens Road
Aston, PA 19014
Phone: 610.558.2700
Fax: 610.558.0222
www.sensaphone.com

TABLE OF CONTENTS

CHAPTER 1: INSTALLATION

INTRODUCTION

Congratulations on your purchase of the Sensaphone IMS-4000E Infrastructure Monitoring System. This one-of-a-kind solution will change the way you think about computer room and network monitoring. The system is designed to be a comprehensive method of ensuring 100% up-time of your computer systems. By monitoring all aspects of your computer room, including environmental conditions and network equipment, the system will keep you informed of the status of your infrastructure. Monitored conditions can include temperature levels, humidity levels, line voltage, leak detection, server response, UPS systems, and more. The system allows the computer professional to be notified immediately of any detected problems. Notification can occur via voice telephone call, pager, e-mail. An internal battery backup system insures that the unit will continue to run if main power fails. The system also includes the ability to remotely perform diagnostic tests via Touch-Tone commands or e-mail.

FEATURES

The IMS-4000E series of products includes the following key features:

- Expandable architecture permitting up to thirty-one IMS-4000E Nodes to be used with each IMS-4000E Host.
- Eight sensor inputs per Host to monitor environmental conditions and/or alarm contacts from other computer equipment such as UPS systems.
- 10/100/1000BASE-T Ethernet port for inter-operation with other IMS-4000E equipment and network devices.
- RS-232 serial port for local configuration.
- Internal battery backup for uninterrupted performance.
- Microphone for detecting audible alarms and for listening-in to onsite sounds.
- Compact design allows rack-mount, wall-mount, or tabletop installation.
- ConsoleView software to program and manage your IMS-4000E system.
- Integrated webpage for device configuration and management.
- SNMP v1 & v3 supported.

TECHNICAL SUPPORT

If any questions arise upon installation or operation of the IMS-4000E, please contact the Sensaphone Technical Service Department at 610.558.2700 and have the following information available:

- Date of purchase   _____
- Serial number   _____

Technical support is available from 8:00 AM to 5:00 PM, eastern time.

ABOUT THIS MANUAL

This manual comprises the instructions and commands necessary to install and program the IMS-4000E. Additional summary and application chapters are included to help you speed programming and to understand IMS-4000E's features. You should thoroughly read this manual to establish a basic understanding of the system and keep it as a reference.

HOST INSTALLATION AND CONFIGURATION

PHYSICAL DESCRIPTION

The IMS-4000E Host is housed in a 17"w x 1.75"h x 10"d enclosure, which is 1 EIA rack-mount space high.

FRONT PANEL LAYOUT

The front panel contains connections for eight sensor inputs, microphone input, Ethernet port, serial port, and status LEDs. See figure below:
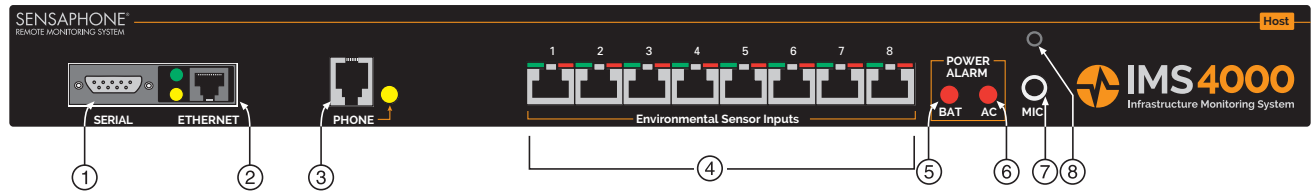
Figure 1: Front Panel Layout of the IMS-4000E Host

1 Serial Port

2 10/100/1000BASE-T

3 Phone line

4 Sensor Inputs (8)

5 Battery Power Alarm LED

6 AC Power Alarm LED

7 External Microphone Input

8 Internal Microphone

SERIAL PORT

The RS-232 serial port can be used to configure network settings. The port operates at 9600 baud, no parity, and 1 stop bit.

RJ-45 10/100/1000BASE-T ETHERNET PORT

This jack is for connecting to your network so that the IMS-4000E Host can communicate with the IMS-4000E Nodes and ping selected network servers and/or services. Two status LEDs are provided. The top LED will light yellow if connected at 1000MB, green if connected at 100MB and off if connected at 10 MB. The bottom LED will blink yellow if there is network activity, it will be OFF there is no network connection.

PHONE JACK

Connect the IMS-4000E's Phone jack to a standard 2-wire analog phone line. The unit dials using touch-tones, with loop start only. The IMS-4000E will recognize ringer frequencies from 16 to 60 Hz and will operate with all standard analog telephone systems that accept tone dialing.

Certain private telephone systems and public switching equipment may not accept the unit's dialing or may generate an unacceptable ring signal. In those cases, a dedicated line may be required for the unit. Consult the supplier of your telephone system if you encounter problems.

CAUTION: Never install telephone wiring during a lightning storm. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface. Use caution when installing or modifying telephone lines.

SENSOR INPUTS

The sensor inputs are designed to interface with IMS-4000E series sensors (See Chapter 6). The use of RJ-45 jacks for sensor inputs allows the use of existing structured cabling to connect remote sensors.

Since the sensor produces an analog signal, it must connect directly to the Host or Node. The path from the sensor to the IMS unit CANNOT pass through a network Hub or Switch.

SENSOR INPUT LEDS

Each sensor input has two LEDs (red and green) to indicate the present status of the input. The key below describes the multiple modes of operation.

Mode 0:   No sensor at input

Green: OFF

Red: OFF

Mode 1:   Sensor present—No alarms

Green: ON

Red: OFF

Mode 2:   Alarm detected but has not exceeded recognition time

Green: FAST BLINK

Red: FAST BLINK

Mode 3:   New alarm exists and not yet acknowledged

Green: SLOW BLINK

Red: SLOW BLINK

Mode 4:   Input is in normal range, but alarm is still unacknowledged

Green: ON

Red: SLOW BLINK

Mode 5:   Alarm has been acknowledged, but input is still out of range

Green: SLOW BLINK

Red: ON

Mode 6:   Sensor in trouble

Green: QUICK FLASH

Red: QUICK FLASH

AC POWER AND BATTERY LEDS

The AC Power and Battery alarm status is indicated by two red LEDs. Their modes of operation are described below.

Mode 1:   No Alarm

LED: OFF

Mode 2:   Alarm detected but has not exceeded recognition time

LED: FAST BLINK

Mode 3:   New Alarm exists and not yet acknowledged

LED: SLOW BLINK

Mode 4:   Alarm has been acknowledged but input is still out of range

LED: ON

MICROPHONE JACK

The Host unit comes with a built-in microphone. Directly below the built-in mic is a separate jack for connecting an optional condenser microphone to sense audible alarms, such as smoke detectors.

When an external microphone is connected, the internal microphone is disabled.

REAR PANEL

The rear panel is where the main power switch is located. The main power cord attaches to the IEC320 connector. The unit can be powered from 100–250VAC 50–60Hz.

IEC 320 connector   Fuse   Power Switch
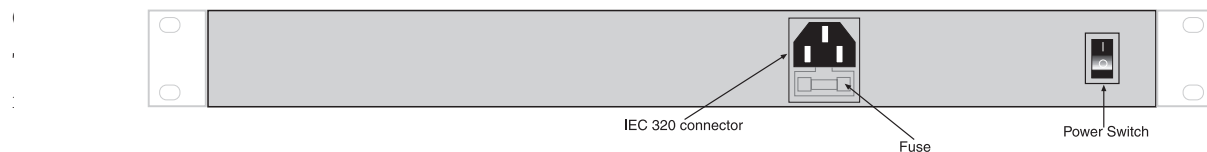
Figure 2: Rear Panel of the IMS Host

INSTALLATION

This section provides information on:

- Operating environment
- Rack, wall, and tabletop installation
- Connecting sensors

Parts Required

Phillips Screwdriver • 9 pin F/F null modem cable • Dumb terminal or PC   w/9 pin com port
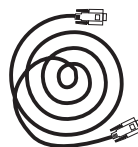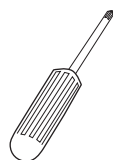
OPERATING ENVIRONMENT

Before you install the IMS-4000E Host be sure that your operating environment meets the physical requirements of the equipment.

Operating Temperature: 32º–122º Fahrenheit (0º–50º C)

Humidity: 5–90 %RH, non-condensing

Power: 100–250VAC 50–60 Hz outlet within 6'

Rack Requirements: Standard 19" equipment rack with supplied mounting bracket hardware. Requires 1.0 EIA rack mount space.

Tabletop requirements: Flat area which can support an enclosure 17" wide by 10" deep by 2" high.

FUSE REPLACEMENT

The IMS-4000E host contains a user replaceable fuse on the main AC power supply, as well as a spare fuse. Both are built into the power connector and can be accessed with a small flat head screwdriver. See figure 2. Before attempting to replace the fuse, turn the power switch off and disconnect the power cable. After you remove the cord you will see a small notch along the bottom edge of the cable entry area of the connector. Insert a small flat-head screwdriver into the notch and force the fuse holder away from the connector body. There will be a visible fuse held in place by a plastic clamp - this is the fuse that is actively protecting the device. There will also be a spare fuse located inside the square plastic cavity below the notch. Use the screwdriver to push out the spare fuse. Replace the blown fuse with the spare and insert the fuse holder back into the power entry connector. Reattach the power cord and turn the power switch on.

Replacement Fuse: 1.6Amp 250VAC Fast acting 5X20 mm (e.g. Littelfuse # 023501.6HXP)

RACK MOUNT INSTALLATION

The IMS-4000E Host can be rack mounted using the included rack mount brackets. Follow the steps below:

1) Attach rack-mount brackets to the sides of the Host unit with a Phillips screwdriver.

2) Attach the unit to the equipment rack using two pan-head screws per side. Tighten the screws with a Phillips screwdriver.

3) Plug the power cord into a 100–250VAC 50/60Hz outlet.
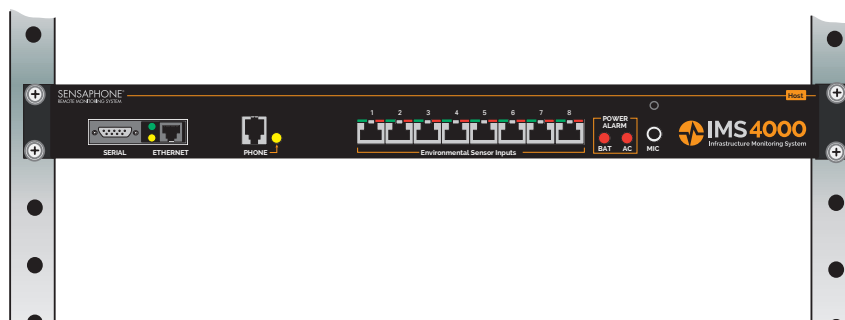
Figure 3: Rack-mounted Host Unit

WALL MOUNT INSTALLATION

The IMS-4000E Host can be wall mounted using the optional wall mount brackets. Follow the steps below:

1) Attach the optional wall mount brackets to the sides of the IMS-4000E using the eight black #6-32 screws. A Phillips screwdriver will be required. (Order part # IMS-4406 Universal Wall Mount Kit)

2) Attach the unit to the wall using two screws per side. Tighten the screws with a Phillips screwdriver.

3) Plug the power cord into a 100–250VAC 50/60Hz outlet.
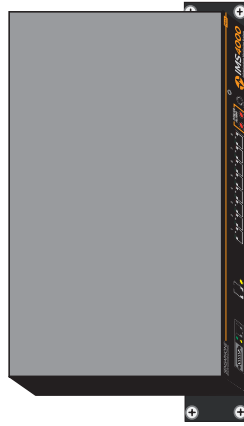
Figure 4: Wall-mounted Host Unit

TABLETOP INSTALLATION

The IMS-4000E Host can be installed on a tabletop or shelf. Follow the steps below:

1) Attach the four self-adhesive rubber feet to the four corners on the bottom of the IMS-4000E.

2) Place the unit on a tabletop or shelf and connect the power cord into a 100-250VAC outlet.
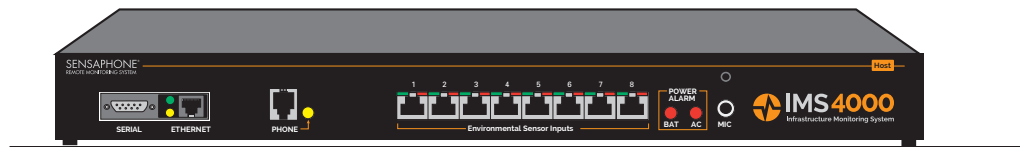
Figure 5: Tabletop-mounted Host Unit

POWER ON SELF TEST (POST)

When the power switch is turned on, the red and green input LEDs will begin a blinking pattern to indicate that the unit is booting up and performing internal diagnostic tests. When the LEDs stop blinking, the unit is fully booted and operational. The boot and Power On Self Test take approximately 1 minute.

CONNECTING SENSORS

The IMS-4000E Host has eight sensor inputs. Each input can accept any sensor type. Sensors are available to monitor the following:

- Temperature
- Humidity
- Water detection
- AC voltage
- Smoke
- Security
- Motion
- Alarm contacts from external equipment

All IMS-4000E sensors connect to the Host using standard RJ-45 cables. This makes it easy to connect sensors directly to the unit. Simply plug one end of the cable into the sensor and the other end into one of the sensor inputs on the Host.

Another benefit of using RJ-45 connectors is that you can easily locate sensors at distant locations within your facility by using your existing structured cabling. For example: Suppose you have an IMS-4000E installed in room A and you want to install a sensor in room B. If your existing cabling infrastructure has an unused cable path between room A and

room B, then you simply use an RJ-45 interconnect cable to connect the IMS-4000E to the patch panel in room A, and an RJ-45 interconnect cable from the wall jack in room B to the sensor.

> **CAUTION:** The sensor produces an analog signal which must connect directly to the Host or Node. The path from the sensor to the IMS unit CANNOT pass through a network Hub or Switch.

NETWORK CONFIGURATION

The IMS-4000E's network settings can be configured through the internal website via DHCP or the device's serial port. If you will be using any IMS-4000E nodes you will need to set the device up with a static IP address. Follow the steps below (using either method) to configure the device's network settings:

Network Setup using the webpage:

1) Download and install the Sensaphone Locator software utility from the Sensaphone.com website (IMS-4000E>Support).

2) Connect the IMS-4000E to a 10/100/1000 switch on your network, turn the unit on, and run the Locator Software on a computer on the same network. The software should identify the IMS-4000E Host and provide the device's IP address.

3) Enter the IP address into your browser and the device web page should appear. Once you get to the Login screen enter the following:

> Username: admin
>
> Password: ims4k

4) Click the 'Settings' gear icon next to the IMS-4000E Host name. Click the Network tab, uncheck the DHCP check box and enter the network settings for the device. Click Save when done. The unit will restart with the new settings. Enter the new IP address into your browser.

Network Setup using the serial port:

The IMS-4000E Host has a serial port on the front panel which is used to configure network settings and security options. A dumb terminal or terminal emulation software is required to get online and set up the configuration. The port is male DTE, so you will need to use a null modem cable. Terminal communication settings must be set to:

- 9600 baud, no parity, 8 data bits, 1 stop bit

To get online with the IMS-4000E, connect your terminal to the serial port and press *<RETURN>*. A menu will appear which will guide you through the setup.

```
Sensaphone IMS-4000E Host Unit V1.0.0.0
Enter Password ()>
{The default password for a New Unit is "ims4k"}
1. Display Enterprise status
2. Display Network and Option configuration
3. Configure Network settings
4. Configure Enterprise Name
5. Configure Web Server
7. Enable Two-Way E-mail Responder
8. Enable Microphone Listen-In
9. Enable default Master Administrator Account (temporarily)
A. Configure SNMP
B. Change Admin Password
C. Reset To Factory Defaults
D. Display Statistics
E. Reboot
F. Logout
Enter option->
```

If you select **Option 1** you will see the IP address and status of the Host and all associated nodes. A sample is shown below:

```
Enterprise Status
Unit                    Type IP         Status
IMS-4000E Monitor    Host 10.1.4.10 Ok
NY_Node Node 10.1.4.17 Ok
Press any key to return to main menu
```

Option 2 will display the network configuration for the Host as well as web server, RAS, and two-way email settings. A sample of Option 2 is shown below:

Network and Option Configuration

```
        Physical Address                00:E0:4B:61:CC:1E
        IP Address (DHCP Enabled)       10.1.4.222
        Sensaphone Locator              Enabled
        Enterprise name                 IMS Enterprise
        Web Server                      Enabled
        Two-Way E-mail Responder        Disabled
        Microphone Listen-in            Enabled
        SNMP RO community               public
        SNMP RW community               private
        SNMP Agent                      Disabled
        Allow remote configuration      Disabled
```

Press any key to return to main menu

Option 3 will allow you to set all pertinent network settings listed under Option 2.

> **NOTE:** You can remotely reconfigure the Host network settings using the IMS-4000E ConsoleView software if the *Allow Remote Configuration* option is set to Y. However, the Host must *initially* be configured via the webpage or serial port.

Option 4 allows you to configure or reconfigure the Enterprise name.

Option 5 allows you to configure the Web server. A sample of the Web configuration menu is shown below:

```
Configure Web Server
1. Enable Web Server
2. Return to main menu
```

Option 7 allows you to Enable or Disable the two-way email feature.

Option 8 allows you to monitor on-site sound through either the built-in or an external microphone.

Option 9 (*Enable default Master Administrator Account (temporarily)*) should only be used in the event that no Master Administrator accounts can be accessed (e.g. the password(s) were forgotten). Enabling this feature will temporarily load the default Master Administrator account (username: admin, password: *ims4k*). This temporary account will unload if any one of the following occurs:

(1) Any of the Master Administrator accounts are edited,

(2) A new Master Administrator account is created, or

(3) The system reboots.

Option A allows you to program the SNMP Read-Only and Read-Write community strings.

```
Configure SNMP
      1. Read-Only community string
      2. Read-Write community string
      3. Enable SNMP Agent
      4. Return to main menu
Enter option ->
Press ENTER to accept new setting or ESC to cancel
Enter SNMP Read-Only community string (public) >
Configure SNMP
```

```
        1. Read-Only community string
        2. Read-Write community string
        3. Enable SNMP Agent
        4. Return to main menuEnter option ->
   Press ENTER to accept new setting or ESC to cancel
   Enter SNMP Read=Write community string (private) >
   Configure SNMP
        1. Read-Only community string
        2. Read-Write community string
        3. Enable SNMP Agent
        4. Return to main menu
   Enter option ->
```

Option B allows you to change the Local Configuration password.

Option C allows you to reset all settings to their default values.

Option D will display statistics.

Option E will save all changes and reboot the system. A reboot is required for changes to take effect.

Option F will save all changes and logout, but the changes will not be activated until the system reboots.

LOCAL CONFIGURATION DEFINITIONS

Password: This is the password which protects access to the local configuration parameters. The default password in a new unit is "ims4k."

IP: This is the IP address assigned to the IMS-4000E on your network. This address is provided by you or your network administrator. It is formatted as a standard dotted decimal number.

Mask: This is the subnet mask which distinguishes the portion of the IP address that is the network ID from the portion that is the station ID.

Gateway: A TCP/IP network must have a gateway to communicate beyond the LAN identified by the network ID. A gateway is a computer or router that is connected to two different networks and can move TCP/IP data from one to the other. If your TCP/IP network has more than one LAN or if you are connecting to the Internet, you will need to know the IP address of the gateway that will transfer TCP/IP data in and out of your LAN. A single LAN that is not connected to other LANs does not require a gateway setting.

DNS: The DNS server is used to translate site names into actual numeric network addresses. Enter the IP address of the DNS server for your network.

Enable Web: Setting this to "**Y**" will enable the web page feature of the IMS-4000E. Set this to "**N**" if you do not want the unit to produce a web page.

Enable Web Password: Setting this to "**Y**" will require a valid user-name and password to be entered in order to view the web page.

Enable 2-Way E-mail: Setting this to "**Y**" will enable the 2-way email feature. With this feature enabled you can send commands to the IMS-4000E via e-mail and receive responses back. Set this to "**N**" to disable this feature.

Enterprise Name: The Enterprise name will appear at the top level of the IMS-4000E ConsoleView software whenever a user logs in to an IMS Host. It provides identification consistency among multiple users and allows for future Enterprise features.

Enable Microphone Listen-In: Enabling this feature will allow users to listen in through the microphone on the front panel of the unit when dialing the unit in Voice mode. Disabling this feature will prevent the microphone from being accessed during a telephone call.

Sensaphone Locator: Software application for Windows that will display the IP address for all Sensaphone IMS4000 Host and Node devices on the local network (if enabled on the device).

BATTERY MAINTENANCE

The IMS-4000E Host includes an internal UPS that automatically switches to battery backup in the event of an AC power failure. The battery in the IMS-4000E Host is a 12V 2.9AH gel cell. This battery will keep the unit operating for approximately 3.5 hours when fully charged and under normal operating conditions.

Service life

Over time and with periodic use, the battery will begin to lose its capacity, resulting in less overall backup time. Under normal operating conditions, three or four years of dependable service life can be expected or between 200 and 1000 charge/discharge cycles, depending on the average depth of discharge. Eventually, battery replacement will be required to maintain a dependable level of service.

Replacing the Battery

The battery in the Host can be replaced by following the instructions listed below. Be sure to read all safety messages and follow the instructions in order as listed. Several tools will be required to change the battery:

• small flathead screwdriver

• needle-nose pliers

> **WARNING: DISCONNECT THE AC POWER CORD FROM THE BACK OF THE UNIT. THERE IS A RISK OF ELECTRICAL SHOCK UNLESS YOU DISCONNECT THE CORD.**
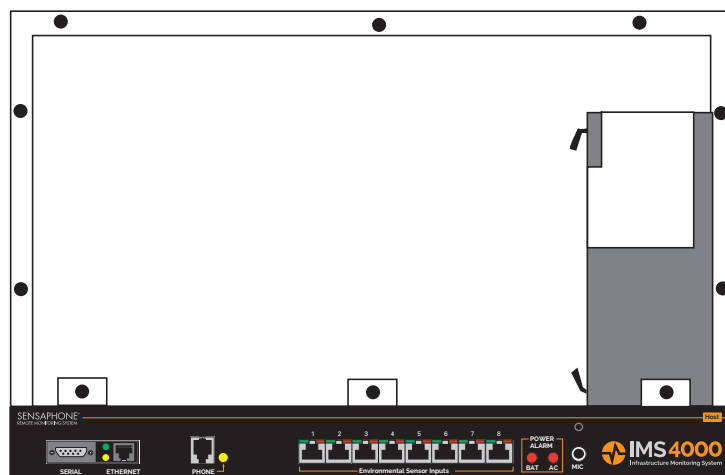
Figure 6: Battery location

Step 1)   Locate the power switch on the rear of the unit and turn the IMS-4000E off.

Step 2)   Disconnect the power cord from the back of the unit.

Step 3)   Disconnect the phone line from the front of the unit.

Step 4)   Remove the IMS-4000E from the rack.

Step 5)   Remove all of the screws in the top cover. Carefully remove the top cover.

Step 6)   Locate the battery on the right side. There will be a red wire (positive)
            and a black wire (negative) connected to the battery. Using needle nose pliers,
            remove the connector with the black wire from the battery first. Gently wiggle it off.

Step 7)   Using needle nose pliers, remove the connector with the red wire from the battery.

Step 8)   Using the nut driver, remove the four nuts which hold down the battery bracket.
            Remove the bracket and battery.

Step 9)   Install the new battery and replace the bracket.

Step 10)   Attach the connector with the red wire to the positive terminal of the battery.

Step 11)   Attach the connector with the black wire to the negative terminal of the battery.

Step 12)   Replace the top IMS-4000E cover and secure with the screws.

Step 13)   Re-install in rack.

Step 14)   Re-attach the power cord.

Step 15)   Re-connect the phone line.

Step 16)   Turn the Power Switch back on.

Akkumulator austauschen

Der Austausch des Akkumulators im Host verläuft gemäß den nachfolgenden Schritten. Lesen Sie alle Sicherheitshinweise aufmerksam durch und folgen Sie den Anweisungen in der angegebenen Reihenfolge. Für den Austausch des Akkumulators sind verschiedene Werkzeuge erforderlich:

• kleiner Schlitzschraubendreher

• Spitzzange

• 1⁄4"-Sechskantschlüssel

ACHTUNG: AKKUMULATOR NUR DURCH EINEN GELZELLENAKKUMULATOR (12 V, 2,9 AH) ERSETZEN.

WARNUNG: VOR AUSTAUSCH DAS NETZKABEL AUF DER RÜCKSEITE DES GERÄTS TRENNEN.

ANDERNFALLS BESTEHT STROMSCHLAGGEFAHR.

Schritt 1)   Das IMS-4000E mit dem Netzschalter auf der Rückseite des Geräts abschalten.

Schritt 2)   Das Netzkabel von der Rückseite des Geräts trennen.

Schritt 3)   Das Telefonkabel von der Vorderseite des Geräts trennen.

Schritt 4)   Das IMS-4000E aus dem Gestell ausbauen.

Schritt 5)   Alle Schrauben auf der Oberseite lösen. Die obere Abdeckung vorsichtig abnehmen.

Schritt 6)   Auf der rechten Seite den Akkumulator ausfindig machen. An den Akkumulator sind ein roter Leiter (+) und ein schwarzer Leiter (–) angeschlossen. Mit der Spitzzange zunächst den Anschluss des schwarzen Leiters vom Akkumulator abtrennen. Dazu den Anschluss vorsichtig mit der Spitzzange hin und her bewegen.

Schritt 7)   Mit der Spitzzange den Anschluss des roten Leiters vom Akkumulator abtrennen.

Schritt 8)   Mit dem Sechskantschlüssel die vier Muttern lösen, mit denen die Akkumulatorhalterung befestigt ist. Halterung und Akkumulator herausnehmen.

Schritt 9)   Neuen Akkumulator einsetzen und die Halterung wieder einbauen.

Schritt 10)   Den Anschluss mit dem roten Leiter am Pluspol des Akkumulators anschließen.

Schritt 11)   Den Anschluss mit dem schwarzen Leiter am Minuspol des Akkumulators anschließen.

Schritt 12)   Die obere Abdeckung des IMS-4000E wieder aufsetzen und mit den Schrauben befestigen.

Schritt 13)   Das IMS-4000E wieder in das Rack einbauen.

Schritt 14)   Das Netzkabel anschließen.

Schritt 15)   Das Telefonkabel wieder anschließen.

Schritt 16)   Den Netzschalter wieder einschalten.

IMS HOST SPECIFICATIONS

OPERATING SPECIFICATIONS

Temperature:	32-122°F
Humidity:	5–90% RH non-condensing
Power Supply:	100–250VAC 50–60Hz
Power Consumption (Typ):	25 Watts
Dimensions:	1.75"h x 9.5"d x 19"w
Backup Battery:	12V 2.9AH Sealed Gel Cell
Backup Time:	3.5 Hours

COMMUNICATION SPECIFICATIONS

Ethernet:	10/100/1000BASE-T
RS-232:	DB9, 9600bps, DTE
Voice Processor:	Yes

ENVIRONMENTAL MONITORING

Internal Monitoring:	AC Power (True RMS Voltage), Backup Battery Level, Sound Level (in dB)
Number of Sensor Ports:	8
Sensor Types:	Temperature, Humidity, Water, Power, Infrared Motion, Smoke, Dry Contacts
Sensor Input Connector:	RJ-45
Sensor Cables:	CAT-5, 568B
Cable Length:	1000'
Visual Indicators:	LEDs, Normal and Alarm
External Microphone:	3.5mm jack, electret condenser

NODE INSTALLATION & CONFIGURATION

PHYSICAL DESCRIPTION

The IMS-4000E Node is housed in a 9.6"w x 1.75"h x 7"d enclosure, which is 1 EIA rack-mount space high.

Front Panel Layout

The front panel contains connections for eight sensor inputs, microphone input, Ethernet port, serial port, and power LED. See figure below:
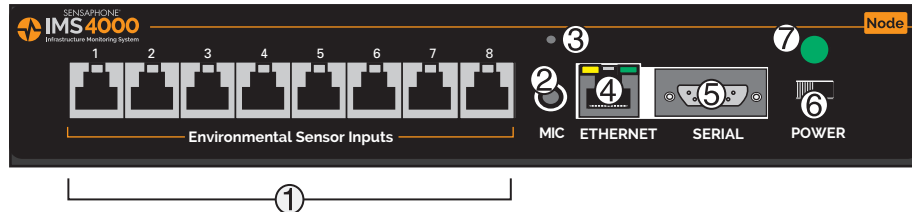
Figure 7: Front Panel Layout of the IMS-4000E Node

    1 Sensor Inputs

    2 Microphone Jack

    3 Internal Microphone

    4 Ethernet Port (10/100BASE-T)

    5 Serial Port

    6 Power Switch

    7 Power LED

SENSOR INPUTS

The sensor inputs are designed to interface with IMS-4000E series sensors (See Chapter 6). The use of RJ-45 jacks for sensor inputs allows the use of existing structured cabling to connect remote sensors.

MICROPHONE

The Node unit comes with a built-in microphone. Directly below the built-in mic is a separate jack for connecting an optional condenser microphone to sense audible alarms, such as smoke detectors.

When an external microphone is connected, the internal microphone is disabled.

10/100BASE-T

This jack is for connecting to your network so that the IMS-4000E Node can communicate with the IMS-4000E Host and ping selected network servers and/or services. Two LEDs indicate Link Status (left) and Receive Date status (right).

SERIAL PORT

The RS-232 serial port is used to configure network settings. The port is DB9 male DTE and operates at 9600 baud, no parity, and 1 stop bit. A DB9 female–female null modem cable is required to configure network settings.

ON/OFF SWITCH

The on/off switch connects main power and battery power to the system. In the event that main power fails, the backup battery system will automatically power the system.

REAR PANEL

The rear panel is where the main power cord exits the unit. A 120VAC/60Hz to 8VAC adapter provides main power to the unit.

BATTERY COMPARTMENT

The battery compartment is located below the top panel. The unit requires (1) 6V 3.4AH rechargeable battery (included). To remove or replace the battery, remove the top cover with a small flat-head screwdriver. {Note: Earlier versions of the node used six (6) C-size 2000mAHr Ni-Cad batteries. These units can be identified by their black network jack or via software—they will be running firmware version 2.xx or earlier.}

INSTALLATION

This section provides information on:

• Operating environment

• Rack, wall, & tabletop installation

• Connecting sensors

• Replacing the battery

Parts Required

Phillips Screwdriver • 9 pin F/F null modem cable • Dumb terminal or PC w/9 pin com port
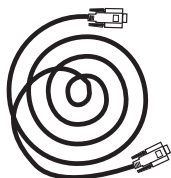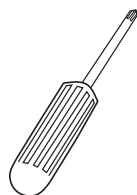
OPERATING ENVIRONMENT

Before you install the IMS-4000E Node be sure that your operating environment meets the physical requirements of the equipment.

Operating Temperature:	32º–122º Fahrenheit (0º–50º C)
Humidity:	5–90 %RH, non-condensing
Power:	120VAC 60 Hz outlet within 6'
Rack Requirements:	Standard 19" equipment rack with supplied mounting bracket hardware. Requires 1.0 EIA rack mount space.
Tabletop requirements:	Flat area which can support an enclosure 10" wide by 8" deep by 2" high.

BATTERY REPLACEMENT

The IMS-4000E Node uses one (1) 6V 3.4AH rechargeable battery (included) for backup power in the event that main power fails. The unit will constantly recharge the battery whenever the power switch is turned on and the unit is plugged into a power supply.

In the event you need to replace the battery, be sure to use battery part # BAT-0006 (see Appendix C: Accessories) to ensure compatibility.

To install the new battery, first slide the power switch to the OFF position and disconnect the power adapter. Next, remove the top cover of the unit by removing the six screws using a small flat-head screwdriver. Remove the wire con-

nectors from the old battery and replace it with the new one. Reconnect the wires to the new battery and reattach the top cover.
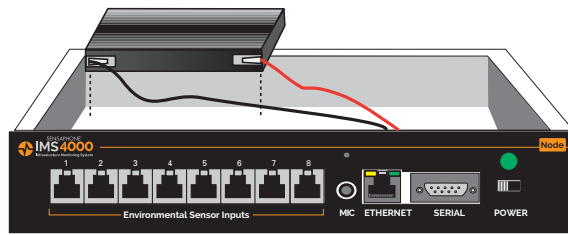
Figure 8: Battery replacement in the Node unit

Austausch des Akkumulators

Der IMS-4000E-Knoten verwendet als Reservestromquelle für Stromausfälle einen (1) wiederaufladbaren Akkumulator (6 V, 3,4 Ah; im Lieferumfang enthalten). Das Gerät lädt diesen Akkumulator auf, sobald es an das Netz angeschlossen und der Netzschalter eingeschaltet ist.

Sofern Sie den Akkumulator austauschen müssen, verwenden Sie aus Kompatibilitätsgründen den Akkumulator mit der Teilenummer BAT-0006 (siehe Anhang C, "Zubehör").

Zum Einbau des neuen Akkumulators zunächst den Netzschalter ausschalten (OFF) und den Netzadapter trennen. Nun die sechs Schrauben, mit der die obere Abdeckung des Geräts befestigt ist, mit einem kleinen Schlitzschraubendreher lösen und die Abdeckung entfernen. Die Leiteranschlüsse vom alten Akkumulator abnehmen und diesen durch den neuen Akkumulator ersetzen. Die Leiter an den neuen Akkumulator anschließen, dann die Abdeckung wieder aufsetzen und befestigen.

Hinweis: Ältere Versionen des Knotens verwenden sechs (6) Nickelkadmium-Akkumulatoren (Größe C, 2000 mAh). Wenn Sie einen solchen Knoten verwenden, müssen Sie die alten Akkumulatoren durch neue Nickelkadmium-Akkumulatoren der Größe C ersetzen.

RACK MOUNT INSTALLATION

The IMS-4000E Node can be rack mounted using the included rack mount brackets. Follow the steps below:

1) Attach rack-mount brackets to the Node with a Phillips screwdriver.
2) Attach the unit to the equipment rack using two pan-head screws per side. Tighten the screws with a Phillips screwdriver.
3) Plug the power adapter into a power outlet.
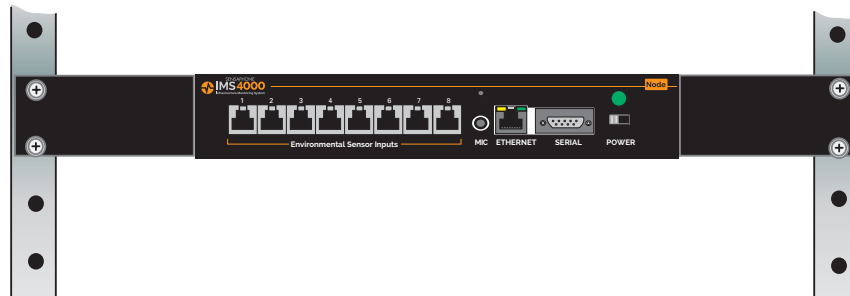
Figure 9: Rack-mounted Node Unit

WALL MOUNT INSTALLATION

The IMS-4000E Node can be wall mounted using the optional wall mount brackets. Follow the steps below:

1) Attach the optional wall mount brackets to the sides of the IMS-4000E using the eight black #6-32 screws. A Phillips screwdriver will be required. (Order part # IMS-4406 Universal Wall Mount Kit)

2) Attach the unit to the wall using two screws per side. Tighten the screws with a Phillips screwdriver.

3) Plug the power cord into a 120VAC 60Hz outlet.

NOTE: An international version is available for 220V 50/60Hz operation. (Order part # IMS-4003.)

Figure 10: Wall-mounted Node Unit

TABLETOP INSTALLATION

The IMS-4000E Node can be installed on a tabletop or shelf. Follow the steps below:

1) Attach the four self-adhesive rubber feet to the four corners on the bottom of the IMS-4000E.

2) Place the unit on a tabletop or shelf and connect the power cord into a 120VAC 60Hz outlet.
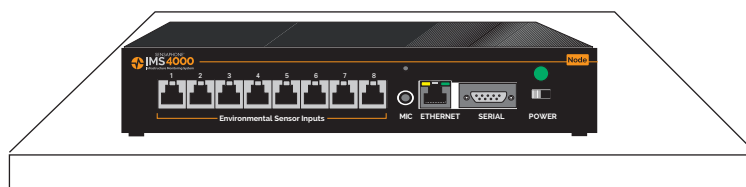
Figure 11: Tabletop-mounted Node Unit

CONNECTING SENSORS

The IMS-4000E Node has eight sensor inputs. Each input can accept any sensor type. Sensors are available to monitor the following:

- Temperature
- Humidity
- Water detection
- AC voltage
- Smoke
- Security
- Motion
- Alarm contacts from external equipment

All IMS-4000E sensors connect to the Node using standard RJ-45 cables. This makes it easy to connect sensors directly to the unit. Simply plug one end of the cable into the sensor and the other end into one of the sensor inputs on the Node.

Another benefit of using RJ-45 connectors is that you can easily locate sensors at distant locations within your facility by using your existing structured cabling. For example: Suppose you have an IMS-4000E Node installed in room A and

you want to install a sensor in room B. If your existing cabling infrastructure has an unused cable path between room A and room B, then you simply use an RJ-45 interconnect cable to connect the IMS-4000E Node to the patch panel in room A, and an RJ-45 interconnect cable from the wall jack in room B to the sensor.

> **Note:** The sensor produces an analog signal which must connect directly to the Host or Node. The path from the sensor to the IMS unit CANNOT pass through a network Hub or Switch.

NETWORK CONFIGURATION

The IMS-4000E Node has an RS232 serial port on the front panel which is used to configure network settings and security options. A dumb terminal or terminal emulation software is required to login and set up the configuration. The node port is male DTE, so a USB-to-DB9 female RS232 adapter cable will be required. Terminal communication settings must be set to:

- 9600 baud, no parity, 8 data bits, 1 stop bit, no flow control

To get online with the IMS-4000E Node, connect your terminal to the serial port and press <*RETURN*>. A menu will appear which will guide you through the setup.

```
Sensaphone IMS-4000 Node Unit   Version: 1.8.0
Main Menu
        1. Display Network configuration
        2. Configure Network settings
        3. Reset to factory defaults
        4. Reboot
        5. Logout

        Enter option->
```

To display the present Network Configuration settings select **Option 1**. To program the Network settings select **Option 2**. Note that the Node must have network visibility of the Host for the IMS-4000E system to function properly. For Network changes to take effect you must reboot the unit (option 4). A typical sample is shown below:

```
Network Configuration
        Physical Address                00:07:F9:00:A2:0C
        Parent Host IP address          173.49.102.229 (Connected)
        Node IP Address                 10.1.4.20
        Subnet Mask                      255.255.255.0
        Default Gateway                 10.1.4.1
        DNS Server                       5.255.255.0
        Node name                        48th Floor Chicago
        Ethernet Mode                    Compatibility Mode
        Allow remote configuration    Y

Press any key to return to main menu
```

NOTE: You can remotely reconfigure the Node network settings using the IMS-4000E ConsoleView software if the Allow Remote Configuration option is set to Y. However, the Node must initially be configured via the serial port before any remote configuration is possible.

```
Press any key to return to main menu
```

Option 2 will allow you to set the Network Configuration parameters. See the list of options below:

```
Configure Network Settings

        1. Set parent IMS-4000 Host IP address
        2. Set IP Address
        3. Set Subnet Mask
        4. Set Default Gateway
        5. Set DNS IP Address
        6. Set Ethernet mode
        7. Set Node name
        8. Remote configuration
        9. Return to main menu
```

Note that the Ethernet Mode contains several options to ensure compatibility with your network equipment. The various Modes are listed below:

```
        1. Compatibility Mode - This mode will automatically select 10MB or 100MB using
           half-duplex.
        2. 10M - This mode will force the unit to only use 10MB half-duplex.
        3. 100M - This mode will force the unit to only use 100MB half-duplex.
        4. Auto - This mode will automatically select 10MB or 100MB full-duplex.
```

Option 3 will reset the Node to factory default settings. All programming and network settings will be deleted.

Option 4 will reboot the system. You must reboot for new Network settings to take effect.

Option 5 will logout without rebooting.

LOCAL CONFIGURATION DEFINITIONS

Parent Host IP Address: This is the IP address of the IMS-4000E Host that this Node is associated with.

Node IP Address: This is the IP address assigned to the IMS-4000E on your network. This address is provided by you or your network administrator. It is formatted as a standard dotted decimal number.

Subnet Mask: This is the subnet mask which distinguishes the portion of the IP address that is the network ID from the portion that is the station ID.

Default Gateway: A TCP/IP network must have a gateway to communicate beyond the LAN identified by the network ID. A gateway is a computer or router that is connected to two different networks and can move TCP/IP data from one to the other. If your TCP/IP network has more than one LAN or if you are connecting to the Internet, you will need to know the IP address of the gateway that will transfer TCP/IP data in and out of your LAN. A single LAN that is not connected to other LANs does not require a gateway setting.

DNS Server: The DNS server is used to translate site names into actual numeric network addresses. Enter the IP address of the DNS server for your network.

Node Name: This name will appear in the IMS-4000E ConsoleView Software. In systems with many Nodes, the Name is useful for identifying one node from another.

IMS NODE SPECIFICATIONS

OPERATING SPECIFICATIONS

Temperature:	32-122°F
Humidity:	5–90% RH non-condensing
Power Supply:	120VAC 60Hz
Power Consumption (Typ):	10 Watts
Dimensions:	1.8"h x 7.0"d x 9.6"w
Backup Battery:	(1) 6V 3.4AH sealed rechargeable
Backup Time:	3.5 Hours

COMMUNICATION SPECIFICATIONS

Ethernet:	10/100 Base-T, 10/100Mbps
RS-232:	DB9, 9600bps, DTE

ENVIRONMENTAL MONITORING

Internal Monitoring:	AC Power, Backup Battery Level, Sound Level (in dB)
Number of Sensor Ports:	8
Sensor Types:	Temperature, Humidity, Water, Power, Infrared Motion, Smoke, Dry Contacts
Sensor Input Connector:	RJ-45
Sensor Cables:	CAT-5, 568B
Cable Length:	1000'
External Microphone:	3.5mm jack, electret condenser

CHAPTER 2: IMS-4000E SOFTWARE

INTRODUCTION

This chapter is designed to help you program and use the IMS-4000E to its fullest potential. The IMS-4000E system helps you maintain, monitor, expedite and control the things that affect your information infrastructure. The ConsoleView Software can be downloaded from the Sensaphone.com website by navigating to Support, then Technical Support, then Sensaphone IMS-4000. Select the Downloads tab and find the link for "IMS-4000 ConsoleView Download.

Help

The IMS-4000E ConsoleView Software provides an extensive Help system to supplement the documentation. Use IMS-4000E Help to access information about commands and dialog boxes. Online help is also available simply by selecting Help from the main menu.

IMS-4000E QUICK START GUIDE

This section presents a useful shorthand guide to configuring your IMS-4000E System for the first time. More detailed information on the processes covered can be found in the sections that follow.

Install Units and Configure Network Settings

Install the IMS-4000E Host and Node(s). Configure the Network settings through the serial port on the front of the units. A terminal or terminal-emulation program can be used. Set the terminal settings for 9600bps (8, N, 1). The default password is "ims4k."

Install Software and Log In to Host

Install the IMS-4000E software from your CD-ROM or other media. Double-click on the IMS-4000E icon on your desktop. The IMS-4000E ConsoleView screen will appear. From the main menu select *Enterprise*, then *Add Enterprise Group*. See below:
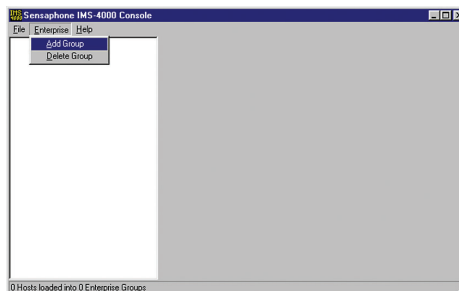
Figure 1: Add Group

Right-click on the words *IP Unknown* below the enterprise name and select *Set IP Address*. Enter the IP address for your IMS-4000E Host and click *OK*. The software will prompt you for a username and password to log in.

DEFAULT USERNAME AND PASSWORD

For new units, the default username is **admin** and the default password is **ims4k**. The software will now attempt to connect to your IMS-4000E Host. A progress bar will show the software retrieving information from the Host.

> **Note:** Do not save the default username and password, because it will be deleted automatically once a Master System Administrator profile is configured.

CONFIGURE THE UNIT PROPERTIES FOR THE HOST AND NODE(S)

Right-click on the word *Host* and select *Unit Properties*. Step through each tabbed page and enter the relevant information for your application. The *Numeric Unit ID* should be set to the Host's telephone number.

The Host can synchronize its clock each night to a time server. To use this feature the IMS-4000E must have network access to a server which supports one of the following: Network Time Protocol - NTP (RFC-1035), Time Protocol - TP (RFC-868), or Daytime Protocol - DP (RFC-867). Enter the IP Address of a Time Server which supports any one of these protocols.

Expand the menus below the Host by clicking the *plus* sign next to the word *Host*. Any nodes associated with the Host should appear. Right-click on the Node names and select *Node Properties*. Configure the Node Properties for each Node.

CONFIGURE INPUT TEMPLATES

Environmental input programming Templates are used to load user specified defaults each time a new sensor is connected to a Host or Node. By properly configuring the Templates before you plug in your sensors, you can minimize the amount of programming required to set up your sensors. To configure the Templates, click the *plus* box next to the word *Settings* to expand the options under this heading. Next, expand the *Input Templates*. This will list all of the different sensor types. Right-click on each of the sensor names to bring up the individual Template programming screens. An example is shown below:
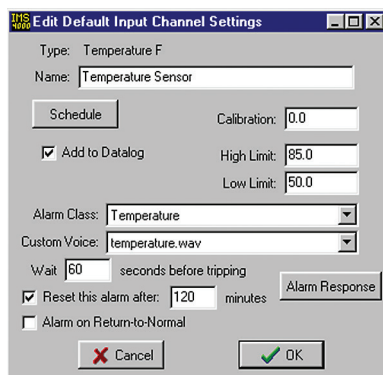
Figure 2: Default Input Channel Settings

CONNECT ENVIRONMENTAL SENSORS TO HOST AND NODE(S)

Once you've configured the Input Templates, connect your sensors. This will automatically load the template programming for each sensor. All sensors connect to the Host and Node via RJ45 connectors. This allows you to use your existing structured cabling for wiring sensors throughout your infrastructure.

 Note: IMS sensors are not IP devices and cannot connect to Hubs or switches.

After connecting your sensors, customize the input alarm parameters for each sensor.

CONFIGURE USER PROFILES AND CONTACTS

Program the User Profiles and Contacts to control who has access to the IMS-4000E and who gets contacted when an alarm occurs. Each user must have a *Username, Password, and User Code*. Right-click on *Profiles* and select *Add New Profile*. Enter information for each user. Click the *Permissions* button and be sure to set up at least one Master System Administrator account. To set up alarm contact information, right-click on the profile name and select *Add New Contact*. You can have up to eight contacts per user. The User Profile screen is shown below:

Figure 3: User Profile

CONFIGURE IP ALARMS

Program the IP addresses for each network device you want to monitor. Expand the Host menu by clicking the plus sign next to the name of your host. Next, right-click on IP Alarms and select Add New IP Alarm. Enter the information to configure the network device you wish to monitor. Be sure to enable the alarm. The IMS unit will ping/connect to the IP address and port you select about once per minute. The IP Alarm programming screen is shown below:

Figure 4: IP Alarm Setup screen

RECORD AND ASSIGN VOICE MESSAGES

Custom voice messages can be used to identify your IMS Hosts/Nodes, PowerGates, Input sensors, IP alarms, and PowerGate outlets. Voice messages must first be recorded on your computer and then uploaded to the IMS Host. Use the CustomVoice Manager screen to record and upload your voice messages. To access the CustomVoice Manager screen, expand the *Host* menu and select *Voice*. Note that Voice messages should be recorded at 8Khz, 8bit, mono, to keep the file size small. See the detailed section on Recording and Uploading Voice Messages later in the manual for more information. Voice messages are assigned to elements of your IMS unit on the respective screens as listed below:

IMS Host Identification message   - Host Unit Properties Screen

IMS Node Identification message   - Node Unit Properties Screen

Input Sensor message   - Input Channel Setup Screen

IP Alarms message   - IP Alarm Setup Screen

PowerGate messages   - PowerGate Setup Screen

SOFTWARE INSTALLATION AND HARDWARE REQUIREMENTS

This section describes how to install and configure the IMS-4000E ConsoleView Software for your enterprise.

HARDWARE AND SOFTWARE REQUIREMENTS

Minimum Requirements:

Intel Pentium processor or equivalent

Intel or AMD 64-bit Processor 2 GHz or greater

100 MB of free disk space

4GB of RAM or more

Microsoft Windows® version 7, 8, 10, or 11.

SOFTWARE INSTALLATION

The IMS-4000E ConsoleView Software can be downloaded from the Sensaphone.com website. Go to the IMS-4000E Host product page, then select the 'Downloads' tab. The IMS-4000E ConsoleView Software setup program makes installation quick and easy. Make sure that all Windows applications are closed before attempting to run setup.

If you encounter problems during installation please contact Sensaphone Technical Support at 610.558.2700 or support@sensaphone.com.

The IMS-4000E ConsoleView Software for Windows will install to a directory named *C:\Program Files\IMS4000*, unless you choose to change the directory name. The installation program will give you three installation choices: Typical, Compact, or Custom. For new installations choose *Typical*.

Figure 5: Installation screen

STARTING THE IMS-4000E CONSOLEVIEW SOFTWARE

Double-click the IMS-4000E icon to start the IMS-4000E ConsoleView Software. The software will automatically try to connect to all IMS-4000E Hosts that have been configured. If this is the first time you are running the software, you will need to create an Enterprise Group and add a Host within each Enterprise. (See *Configuring Hosts and Nodes*)

CONFIGURING HOSTS AND NODES

SETTING UP AN ENTERPRISE

An Enterprise Group comprises an IMS-4000E Host, any IMS-4000E Nodes connected to that Host, and all of the environmental inputs connected to these units, regardless of proximity to the Host.

> **Note:** Before setting up your Enterprise software, you must have locally configured your Host and Node units—which is where you assign the Host its IP address. If you have not done this, the ConsoleView software will not be able to locate your Host. If you are connecting to your Host through a dialup connection, be sure to establish a PPP connection before running the software. (See *Remote Login via Dialup*) See the sections in your Host and Node Manuals on Local Configuration.

To get started, double-click on the IMS-4000E software icon. This will bring up the IMS ConsoleView Screen.
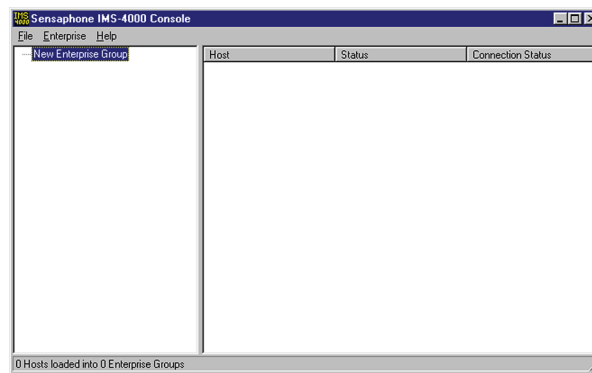
Figure 6: IMS ConsoleView screen

Adding an Enterprise Group

From the ConsoleView menu, click on *Enterprise* and select *Add Enterprise Group*. In the left-hand column, a *New Enterprise Group* will appear. When you connect to the host, the Enterprise Name will update.

Deleting an Enterprise Group

If at any time you wish to delete an Enterprise group, click to highlight the Enterprise Group you would like to delete, select *Enterprise* from the main menu and choose *Delete Enterprise Group*.

ADDING A HOST

Right-click on the words *IP Unknown* below the enterprise name and select *Set IP Address*. Enter the IP address for your IMS-4000E Host and click *OK*. The software will prompt you for a username and password to log in. For new units, the default username is **admin** and the default password is **ims4k**. The software will now attempt to connect to your IMS-4000E Host. A progress bar will show the software retrieving information from the Host.

> **Default Username**: admin

> **Default Password**: ims4k

> **Note:** Do not save the default username and password, because it will be deleted automatically once a Master System Administrator profile is configured.
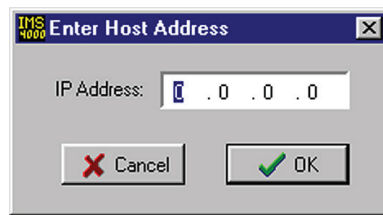
Figure 7: Entering the Host address

To see the programming, inputs, and accessories associated with the host, click in the box beside your enterprise group. The tree hierarchy will appear beneath the Host.

Figure 8: Host Tree

CONNECTING TO A HOST

If you have a Host set up already, you can connect to it in one of two ways: Either right-click on the Host and select *Connect* from the drop down menu, or double-click on the Host in the hierarchy. Both methods will bring up the prompt form where you type in your *username* and *password* to connect to the Host.

DELETING A HOST

To delete a Host, right-click on the Host you would like to delete and select *Delete Host* from the contextual menu.

SETTING THE UNIT PROPERTIES FOR THE IMS HOST

To set the global properties of your IMS-4000E, right-click on the Host name and select *Unit Properties*. On the *System Info* tab, enter the *Unit Name, Description* and *Location*. These parameters will be used when sending alarms to identify the unit. Check the *Auto-Connect on Startup* box if you want the IMS software to connect automatically with the unit at startup. See Figure below.

Figure 9: System Info tab

Next, select the *Phone Settings* tab. Enter the telephone number of the Host in the *Numeric Unit ID* field. The *Numeric Unit ID* will appear on alarm messages delivered to numeric pagers and fax machines.

Figure 10: Phone Settings tab

Select a custom voice message to identify your Host by clicking the arrow in the *Custom Voice* field and selecting a voice file. Custom voice messages can be recorded and uploaded to the Host on the *Custom Voice Manager screen*. The Host Custom Voice message is the first message spoken during a voice call. This message should describe the name and location where the Host is installed.

Enter the number of *Dialout Attempts* you want the IMS to make when an alarm occurs. Dialout attempts is the number of times the IMS will try to call each contact.

If your phone system does not produce a dial tone when you first lift the receiver, uncheck the box marked "*Check for dial tone.*"

Set the "*Rings until Answer*" number. This will determine how many times the line must ring before the IMS-4000E will answer.

Set the "*Intercall Delay.*" This is the time the unit waits between outgoing phone calls. During this period the unit will answer any incoming calls. To acknowledge an alarm via callback you must set this value to at least 1 minute. When set to 0 the unit will dial back-to-back calls without the possibility of calling in to acknowledge an alarm. The Intercall Delay can be set from 0–60 minutes.

Test Dial Tone: The IMS-4000E can be programmed to test periodically for dial tone to ensure that the telephone line is alive in the event that the unit has to dial out for an alarm. If the unit determines that a dial tone is not present, it will send a diagnostic alarm via e-mail and/or SNMP to profiles that are set up to receive diagnostic alarms (i.e. diagnostic class). Check to enable, then enter the test interval, in hours, in the *every X hours* box.

Finally, select the Clock Settings tab. To set the time in the IMS Host, click the button labeled Set to Current PC Time. Next, select the Host's Time Zone according to its location. If you would like the unit to synchronize its time on a daily basis, enter the IP address of a compatible time server.
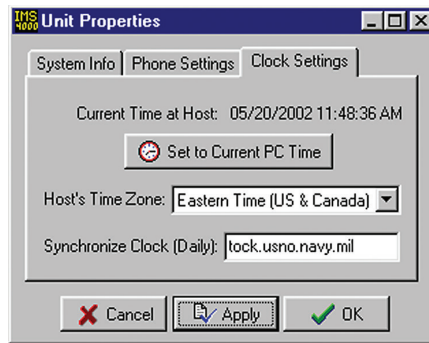
Figure 11: Clock settings tab

The IMS-4000E can be programmed to synchronize its clock to a reference time server every night at midnight. To use this feature the IMS-4000E must have network access to a server which supports one of the following time code protocols:

Network Time Protocol - NTP (RFC-1035)

Time Protocol - TP (RFC-868)

Daytime Protocol - DP (RFC-867)

Click the *Clock Settings* tab. Enter the name or IP address of the time server in the *Synchronize Clock* field. To disable this feature, delete the name or IP address.

> **Note:** After setting the time zone, you must reboot for the new settings to take effect.

ADDING A NODE

Once the node has been connected to the network and the Local Configuration has been performed, it will automatically start communicating with the Host. From the IMS Consoleview the Node will appear within the tree. See figure below.
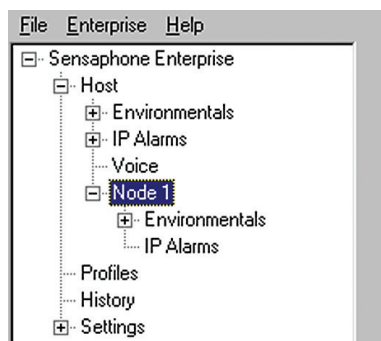
Figure 12: Structure tree with Node

The Node name will appear in green when host-to-node communications are working properly. If a communications problem occurs, the node name will initially turn yellow, to indicate that pending node trouble exists. If the problem persists for several minutes, the node name will turn red and a trouble alarm will be dispatched to Users who are members of the diagnostic class.

DELETING A NODE

To delete a Node, right-click on the Node name in the tree and select *Delete This Node*.

CHANGING HOST NETWORK SETTINGS USING CONSOLEVIEW

You can remotely change the Host network settings using the ConsoleView software if the *Allow Remote Configuration* option is set in the Local Configuration options. However, before doing so consider the following:

If you have any Nodes associated with the Host, they will stop communicating with Host if you change the IP address. So be sure to change the parent Host IP Address in the NODE *before* actually changing it in the Host itself.

To change the network settings in the Host using ConsoleView, right-click on the unit name and select *Network Settings*. The first tab is titled *Ethernet Settings*, click the *Modify* button to bring up the Network Setup screen.
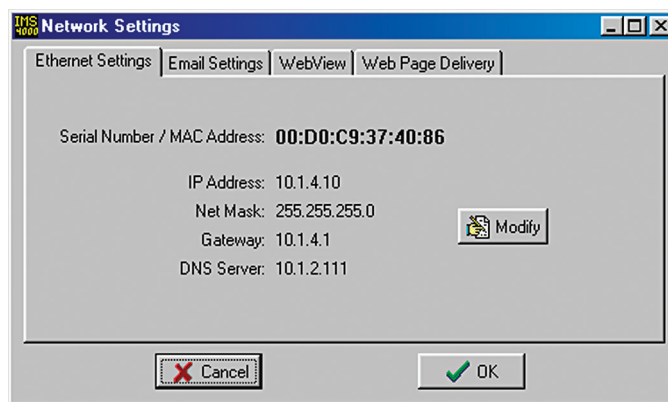

Figure 13: Host Network Settings

> **NOTE:** If the Modify button is grey (inactive) then the unit either does not have the Allow Remote Configuration option set, or the unit's firmware does not support this feature and requires upgrading.

Enter the new network parameters and click *OK*. A warning message will appear telling you that the unit must reboot. Click *OK* to proceed with the change. You will be disconnected while the unit reboots. If you changed the Host's IP address, it will automatically change in ConsoleView as well, so that the software will connect to your host using the new IP address.

SETTING THE UNIT PROPERTIES FOR THE NODE

To set the Properties of your IMS-4000E Node, right-click on the Node name and select *Node Properties*. The Node Name will be copied from the node itself as programmed during the network configuration procedure. Enter the *Location* and *Description* in the fields provided. These parameters will be used to identify the unit when sending alarms. Set the Custom Voice file to identify the Node when speaking over the telephone. (See *Recording and Uploading Voice Messages* for information on creating custom voice messages.)

In normal operation information is periodically passed between the Node and Host. This information mainly consists of current Input values and IP Alarm status. The amount of data transferred during this update is about 700 bytes. You can choose how often information is updated from the Node by selecting either periodic updates (Auto Send) or by selecting Update on a Percent Change basis. This can be used to control network traffic. When you enable the *Auto Send Status Updates* box, the Node will send an update (700 bytes) to the Host based on the *Interval* you program. When you choose the *Send Update on Change* option, the Node will only send an update when a sensor value increases or decreases by x% as programmed. You can even choose to enable both options for more flexibility.

Note that if an alarm is detected, the Node will transmit this information to the Host **immediately**. The Node Properties screen is shown below:
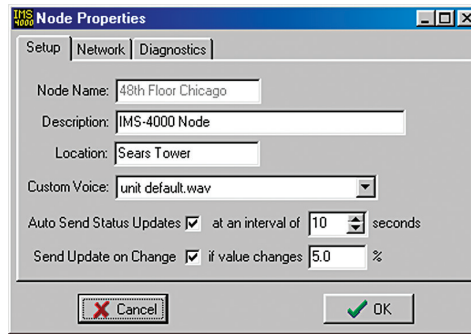
Figure 14: Node Properties Setup Tab

Sample Application:

1) Suppose you are concerned about network traffic generated by Node-to-Host communication but want to view input values that are no more than 20 minutes old.

=>You can enable the *Auto Send* option and enter an interval of 1200 seconds (20 minutes). This will limit Node-to-Host data transfers to no more than 700 bytes every 20 minutes.

2) Suppose that in addition, if the temperature changes by more than 3 degrees Fahrenheit (about 4% at room temperature) you want to see this update immediately.

=> You can enable the *Send Update on Change* option and enter a value of 4%. This will instruct the Node to send an update if the temperature changes by +/- 4% since the last update.

CHANGING NODE NETWORK SETTINGS

You can remotely change the Node network settings using the ConsoleView software if the *Allow Remote Configuration* option is set in the Node Local Configuration options. However, before doing so consider the following:

If you change the parent Host IP address in the Node, then the Node will no longer be in contact with the Host until the Host's IP address also changes.

To change the network settings, right-click on the Node Unit Name and select *Node Properties*. Click on the Network tab. Click on the *Modify* button to bring up the *Network Setup* screen.

Figure 15: Node Network Settings

NOTE: If the *Modify* button is grey (inactive) then the unit either does not have the *Allow Remote Configuration* option set, or the unit's firmware does not support this feature and requires upgrading.

Enter the new network parameters and click *OK*. The Node will reboot and temporarily disconnect from the Host.

CONFIGURING ENVIRONMENTAL INPUTS

Each host or node can have up to 8 external sensors connected. The host or node will automatically identify what sensor type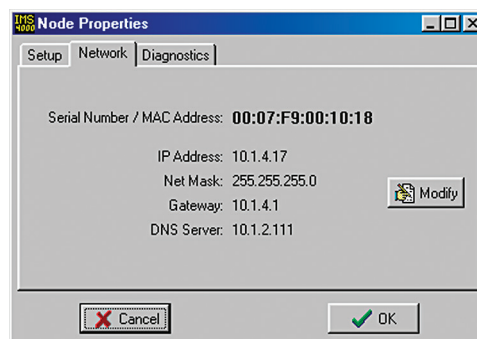 is connected to each input. Note that some newer sensors will require a subtype to be manually programmed. The subtype will appear on the *Channel Setup* screen. This includes the Ultra Low Temperature Sensor, the 15 Amp Current Sensor, and the 20 Amp Current Sensor. To program the environmental input parameters expand the host or node tree by clicking the plus box next to the host/node name.

Channel Setup

Next, click in the plus box beside Environmentals to expand the tree below it. Choose the input you would like to configure and right-click on the sensor name.

Figure 16: Environmental Input Channels

The Channel Setup screen will appear.

Figure 17: Channel Setup screen

Set up the parameters for your environmental input on this screen.

Name: Enter a name which describes what the sensor is monitoring. (ex: Mail Server, Data Center Rack #3, …)

Type: The sensor type is determined automatically when the sensor is plugged into the host or node.

Status: The status indicates if the sensor is presently within alarm limits. For devices such as Water Sensors or Smoke Detectors a Normal condition indicates that there is no water or smoke detected.

In Use: This indicates that a valid sensor is plugged into the channel.

Enabled: This indicates if the channel is currently enabled for alarm monitoring. If it is disabled, the IMS-4000E will not send alarm messages. A channel can be enabled or disabled based on a 7-day + holiday time schedule.

Schedule: Click this button to bring up the Edit Schedule screen. This screen allows you to set times when the channel is enabled or disabled. The blue line indicates days/times when the channel is enabled.
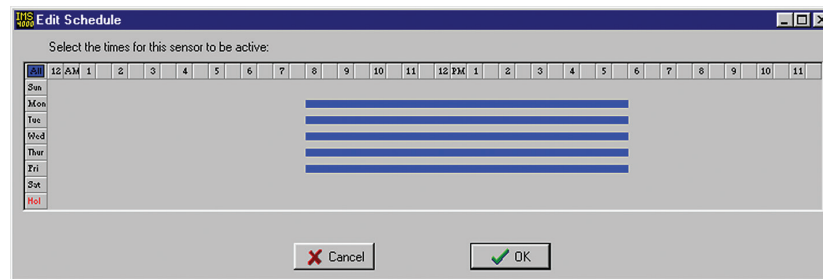
Figure 18: Sensor Schedule screen

The schedule example above enables the sensor Mon-Fri 8AM to 5PM.

Editing the schedule:

• Click on the All button in the top left corner of the grid to enable/disable the entire week.

• Click on the day buttons down the left side of the grid to enable/disable entire days

• Click on the hour buttons across the top of the grid to enable/disable entire hours

• Drag the mouse over portions of the grid to enable/disable specific hours/days

Channel Enabled: This box provides a simple means to enable or disable a sensor channel.

Add to Datalog: Click this box to store the value or status of the channel in the datalogger.

Value: This is the current value of the sensor connected to the channel. (only valid for analog sensor types).

Min: This is the minimum value reached by the sensor since it was connected to the unit.

Max: This is the maximum value reached by the sensor since it was connected to the unit.

Calibration: Enter a positive or negative offset in this field to calibrate the sensor value.

High Limit: Enter the sensor high alarm limit in this field. When the value exceeds this limit for the duration of the recognition time, and if the channel is enabled, an alarm will be tripped.

Low Limit: Enter the sensor low alarm limit in this field. When the value falls below this limit for the duration of the recognition time, and if the channel is enabled, an alarm will be tripped.

Alarm Class: Click the drop down arrow and select the appropriate class for this sensor/channel. If you prefer you can create your own classes on the Class Setup screen.
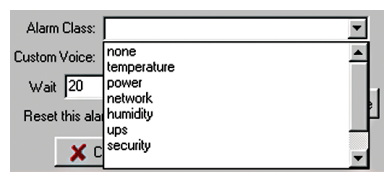
Figure 19: Alarm Class dropdown menu

Custom Voice: Click the drop down arrow and select the custom voice message you would like assigned to this sensor/channel. Voice messages can be recorded on your PC and uploaded into the IMS-4000E on the Custom Voice Manager screen (See Recording and Uploading Voice Messages).
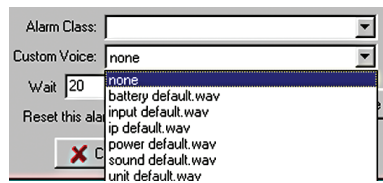
Figure 20: Custom Voice dropdown menu

Wait (Recognition) Time: This is the time required for a fault condition to qualify as an alarm event. The sensor/channel must remain beyond the limits or in a fault condition continuously for this entire period of time in order to become an alarm.

Reset Time: This is the time allowed for an acknowledged alarm's fault condition to be corrected before the IMS-4000E resets (reactivates) the alarm and begins the message delivery process all over again. The minimum reset time is 30 minutes.

Alarm on Return to Normal: This feature makes the unit send a message (or messages) when a condition has moved within its programmed alarm limits or has gone from an alarm state to a Normal state. The person who acknowledged the alarm—in addition to all Inform Only contacts in the alarm class—will receive the message.

SNMP Trap Level: When sending alarm messages via SNMP, this sets the priority of the SNMP trap. The choices are Major or Minor.

ALARM RESPONSE VIA THE POWERGATE, POWERGATE2, OR CAMERA

POWERGATE

When an alarm occurs, you can have PowerGate or PowerGate2 outlets automatically turn ON, turn OFF, or CYCLE power to a device. *Cycling* will switch an outlet OFF for 10 seconds and then switch it back ON. To set up a PowerGate, click the *Alarm Response* button on the Channel Setup Screen. A sample Alarm Response screen is shown below.
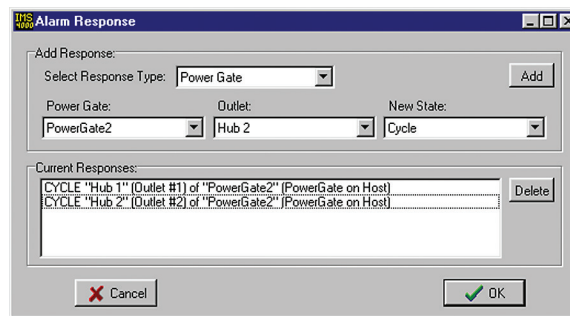
Figure 21: Alarm Response screen for PowerGate

Select Response Type: Choose "PowerGate."

PowerGate: Choose the specific PowerGate you're programming.

Outlet: Choose the PowerGate outlet you want to program for alarm response.

New State: Select the action you want to have occur: On, Off, Cycle.

Click the *Add* button to add this response to the list of current responses; click *Delete* to remove an action. Repeat for as many outlets as you wish to program.

CAMERA SNAPSHOTS ON ALARM

Camera images may be sent to one or more users when an Environmental or IP alarm occurs. Up to four alarm responses (PowerGate or Camera Snapshot) may be programmed per input. To configure this feature choose *Alarm Response* from the *Properties* screen for the chosen input. The following screen will appear.
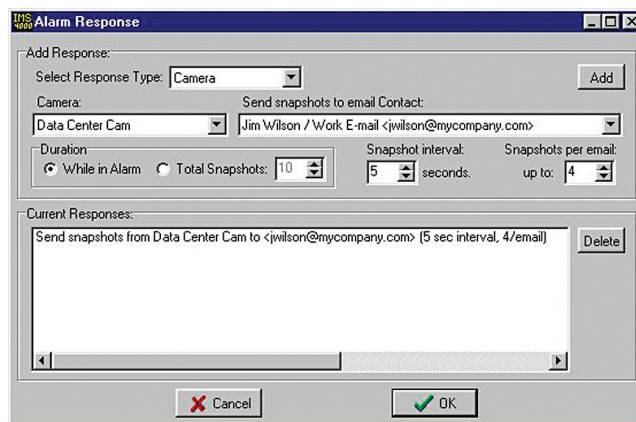
Figure 22: Camera Alarm Response

Click the down arrow in the *Response Type* menu and choose *Camera*. Select the name of the camera from which you would like to receive snapshots. Next, select the E-mail address where you would like the snapshots to be sent. There are two options to determine the *Duration* over which snapshots will be sent. If you choose *While in Alarm* you will receive snapshots continuously until the input goes back to normal. If you choose *Total* you will receive a fixed number of snapshots once the alarm is detected. You can also select the time between snapshots in the Snapshot Interval field, and you can choose the maximum number of *Snapshots Sent per E-mail*. Camera snapshots will not work if a *User Login* is required in the camera.

> **Note:** the E-mail messages sent via Alarm Response operate independent of Profile Class and Contact Schedule.

HIGH SOUND ALARMS

The IMS-4000E measures the sound level with the built-in microphone on the front panel. This can be useful in detecting audible alarms in close proximity to the unit. To detect alarms at a distance from the unit, you can plug an external condenser microphone into the mic jack. Note that the audible alarm must be more than just a periodic beep. Only alarms that produce a loud, steady or pulsing signal (for example, smoke detector alarms) will be recognized by the IMS-4000E.

The unit is programmed to trip an alarm if the sound level increases by a programmed number of decibels. On the High Sound programming screen this parameter is listed as "Change in dB." The default setting is 30db. This means that if the audio level increases more than 30 dB for the duration of the recognition time, an alarm will be tripped.

To verify that your audible alarm is capable of tripping an alarm we recommend that you perform several tests to check the decibel increase at the IMS unit. The test should involve tripping your audible alarm and checking the measured level within the ConsoleView Software. Using the data obtained from your testing, you can then set the *Change in db* parameter appropriately.

If you are not concerned about High Sound alarms or if the unit is installed in a generally noisy environment that could easily trip false alarms, we recommend you disable the High Sound alarm monitoring via the Schedule.

REALTIME STRIP CHART

A realtime Strip Chart will show continuous values for sensors which provide an analog value. Just click on the sensor name and the chart will appear.

The high and low scale of the chart is based on the Min and Max values. To reset Min/Max values, click on the Reset button to the right of the chart.
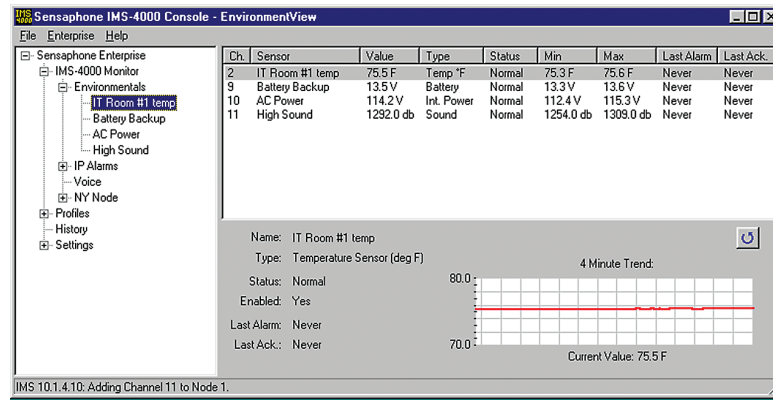
Figure 23: Programmed Environmental Sensors

ENVIRONMENTAL INPUT ALARM LOGIC

Each environmental input will automatically detect the type of sensor connected (temperature, humidity, power, motion...). Analog sensors will include high and low alarm limit programming options while two-state sensors (Normal/Alarm) will simply have a recognition time. In order for an alarm to be dispatched, the sensor must meet the following criteria:

a) It must be Enabled—as configured through the schedule.

b) It must have exceeded the programmed high or limit, continuously, for the duration of the wait (recognition) time. For two-state sensors it must be in the Alarm state, continuously, for the duration of the wait (recognition) time.

c) It must be a member of a Class.

d) There must be one or more User Profiles which include this Class.

Once the alarm is dispatched, the alarm delivery process begins. (See *Alarm Delivery and Acknowledgment* for details.)

Additionally, there is an option to re-trigger the alarm if it remains beyond the High/Low limits (or in an alarm state) too long. This programmable time period is called the Alarm Reset Time. This parameter can be set from 30 to 3600 minutes.

> **Note:** DO NOT set the Alarm Reset Time too short, otherwise you will continue to dispatch the same alarm over and over resulting in numerous phone calls.

TROUBLE ALARMS

The IMS-4000E monitors the presence of all connected sensors to insure the reliability of the system. When a sensor is removed from a Host or Node for more than a minute, a trouble alarm is generated. All trouble alarms are a part of the Diagnostic class, so any User who wishes to receive sensor Trouble Alarm, System Diagnostic or Fault Alarms can do so by including the Diagnostic class in their user Class List.

REMOVING/CHANGING A SENSOR

Since the Host and Node monitor the presence of sensors, you must be careful when removing them to prevent a trouble alarm from occurring. The following procedure is recommended:

a) Disable the sensor you wish to change/remove by clearing its schedule.

b) Disconnect the sensor from the Host or Node.

c) Login to the Host or Node and expand the Environmentals to display all of the inputs. Right click on the sensor to be removed and select Delete.

A new sensor can now be connected to the empty channel.

Special Notes

To reset a Smoke detector alarm, you must momentarily disconnect it from the Host or Node, and then reconnect it. This will silence the alarm and return it to normal operating condition.

CONFIGURING TEMPLATES

Environmental input programming Templates are used to load user-specified defaults each time a new sensor is connected to a Host or Node. By properly configuring the Templates before you plug in your sensors, you can minimize the amount of programming required to set up your sensors. To configure the Templates, click the plus box next to the word Settings to expand the options under this heading. Next, expand the Input Templates. This will list all of the different sensor types.
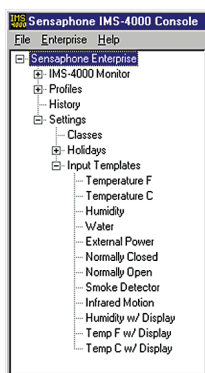

Figure 24: Template Types

Right-click on each of the sensor names to bring up the individual *Template* programming screens. An example is shown below.
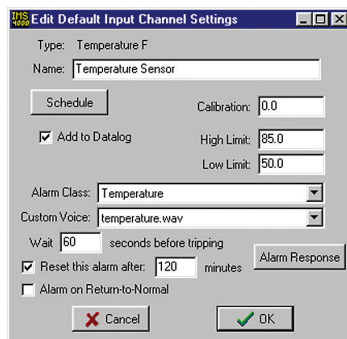

Figure 25: Template

CONFIGURING IP ALARMS

IP ALARM SETUP

Each host or node can monitor up to 64 IP addresses through pinging and port availability. In addition, IP dependencies can be programmed to prevent multiple alarm messages from being sent when common network paths are down.

PROGRAMMING ALARM PARAMETERS

To program the IP Alarm parameters, expand the Host or Node by clicking the plus box next to the host/node name. Next, expand the IP Alarms. To configure a new IP Alarm, right-click on IP Alarms and select *Add New IP Alarm*. Next, right click on the New IP Alarm and select *Setup*. The IP Alarm Setup screen will appear.
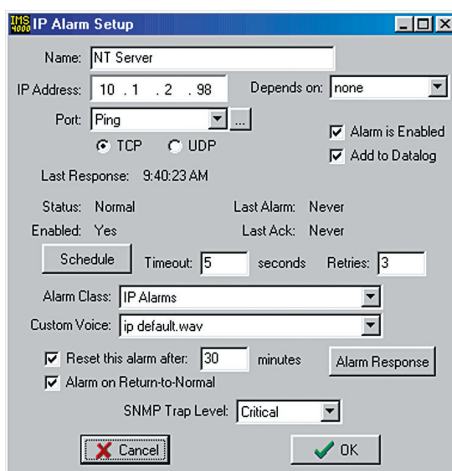
Figure 26: IP Alarm Setup screen

Name: Enter a name which describes the IP address and port to be monitored.

IP Address: Enter the numeric IP address of the device to be monitored.

Port: Enter the port number to be monitored.

Dependency IP: This is the IP address that must be responding for the monitored IP address to have a chance at responding. Or in other words, the monitored IP address is dependent upon the Dependency IP address to function.

Alarm is Enabled: Unchecking this box will disable the IP alarm.

Add to Datalog: Click this box to store the value or status of the channel in the datalogger.

Last Response: This is the date/time that the IP device last responded.

Last Alarm: This is the date/time that the last IP alarm occurred for this IP address.

Last Ack: This is the date/time that the last IP Alarm for this channel was acknowledged.

Status: The status indicates if the IP Address is presently responding or not. A Normal status indicates that the IP device is responding within the limits of the timeout and retry parameters. A Ping Timeout status indicates that the IP device is not responding within the timeout and retry parameters. An IP Route Down status indicates that the dependency IP is not responding and therefore the monitored IP address cannot be reached.

Enabled: This indicates if the IP Address is currently enabled for alarm monitoring. If it is disabled, the IMS-4000E will not send alarm messages. An IP Alarm can be enabled or disabled based on a 7-day + holiday time schedule.

Schedule: Click this button to bring up the Edit Schedule screen. This screen allows you to set times when the IP Alarm is enabled or disabled. The blue line indicates days/times when the channel is enabled.
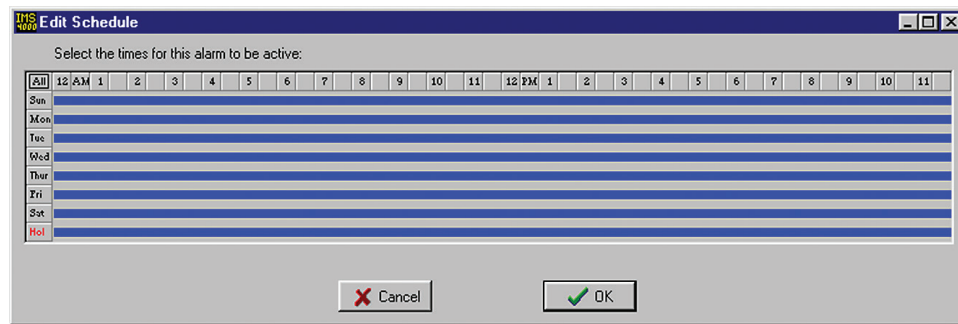
Figure 27: IP Schedule screen

The schedule example above enables the IP alarm 24 hours a day, including holidays.

Editing the schedule:

• Click on the *All* button in the top left corner of the grid to enable/disable the entire week.

• Click on the *day* buttons down the left side of the grid to enable/disable entire days

• Click on the *hour* buttons across the top of the grid to enable/disable entire hours

• Drag the mouse over portions of the grid to enable/disable specific hours/days

Timeout: If the monitored IP address does not respond within this period of time, then the ping is considered a failure. If the number of consecutive failures exceeds the number of Retries then a Ping Timeout alarm is tripped.

Retries: This is the number of times the monitored IP address is pinged after a failure, before a Ping Timeout alarm is tripped.

Alarm Class: Click the drop-down arrow and select the appropriate class for this type of alarm. If you prefer you can create your own classes on the Class Setup screen to group certain types of alarms.

Custom Voice: Click the drop-down arrow and select the custom voice message you would like assigned to this IP Alarm. Voice messages can be recorded on your PC and uploaded into the IMS-4000E on the Voice screen.

Reset Time: This is the time allowed for an acknowledged alarm's fault condition to be corrected before the IMS-4000E resets (reactivates) the alarm and begins the message delivery process all over again. The minimum reset time is 30 minutes.

Alarm on Return-to-Normal: When this feature is enabled, the unit will send a message (or messages) when an IP device goes from a Ping Timeout state to a Responding state. The person who acknowledged the alarm—in addition to all Inform Only contacts in the alarm class—will receive the Return-to-Normal message.

SNMP Trap Level: When sending alarm messages via SNMP, this sets the priority of the SNMP trap. The choices are Major or Minor.

> **Note:** See the previous section, "Alarm Response via the PowerGate, PowerGate2, or Camera" for information on responses to alarms via PowerGates or Cameras.

ALARM LOGIC

Network devices are monitored by the IMS-4000E by pinging/connecting to programmed IP addresses about once a minute. The unit will only attempt to ping/connect to devices which are *Enabled* by the *Schedule*. Each time the network device responds, the IMS-4000E updates the *Last Response* time. A time limit for responding is assigned to each IP Alarm to determine if the device is functioning properly. This time limit is called the ping *Timeout*. If a network device does not respond within this time period, the IMS-4000E will count this as a ping failure. You can program the IMS-4000E to try to ping/connect to the network device several times before tripping an alarm. The ping *Retries* determines how many times the IMS-4000E will try to ping/connect to the device before sending an alarm. An alarm will

only occur if the device fails to respond to consecutive ping attempts. Once a successful response is received, the failure counter will reset. For example: If the ping *Retries* is set to 3, then the IMS-4000E must fail to ping/connect to the device 4 times in a row (initial attempt + 3 retries) to trip an alarm. If the device were to respond after the second attempt, then the failure counter would reset, thus requiring four subsequent successive failures to trip an alarm. Once an alarm is recognized, the *Last Alarm* time will be updated.

A dependency device (IP address) can be programmed for each IP Alarm. This is used to prevent numerous alarms from occurring when common network infrastructure problems arise. If the dependency device fails, then all IP alarms that have this dependency will be temporarily disabled from sending alarms until the dependency device returns to normal (e.g. starts responding to ping/connect requests). When an IP Alarm's dependency is not responding, the status for the IP Alarm will be shown as "IP route down." It is recommended that the dependency device be programmed such that it will go into alarm before any other devices. You can achieve this by setting the number of *Retries* for the dependency device to a lower value than the IP Alarms which rely on this device.

In summary, for an IP Alarm to be dispatched, the following criteria must be met:

   a) The IP Alarm must be enabled—as configured through the schedule.

   b) It must have failed to respond to consecutive ping/connect requests and exceed the number of retries.

   c) It must be a member of a class.

   d) There must be one or more user profiles which include this class.

Once the alarm is dispatched, the alarm delivery process begins. If any of the contacts are programmed as *Until Acknowledged*, then the *Last Ack* time will update when the alarm has been acknowledged. In the case where all contacts are set to *Inform Only*, the Last Ack time will update immediately after the alarm occurs.

Additionally, there is an option to re-dispatch the alarm if it remains in an alarm state too long. This programmable time period is called the *Alarm Reset Time*. This parameter can be set from 30 to 3600 minutes. For example: Suppose the *Alarm Reset Time* is set to 180 minutes. Now suppose an IP device has stopped responding and trips an alarm which results in all programmed users receiving their respective messages. If the IP device continues to remain unresponsive for 180 minutes, then the alarm will be dispatched again and everyone will be contacted once more.

> Note: DO NOT set the *Alarm Reset Time* too short, otherwise you will continue to dispatch the same alarm over and over resulting in numerous phone calls, e-mails, etc.
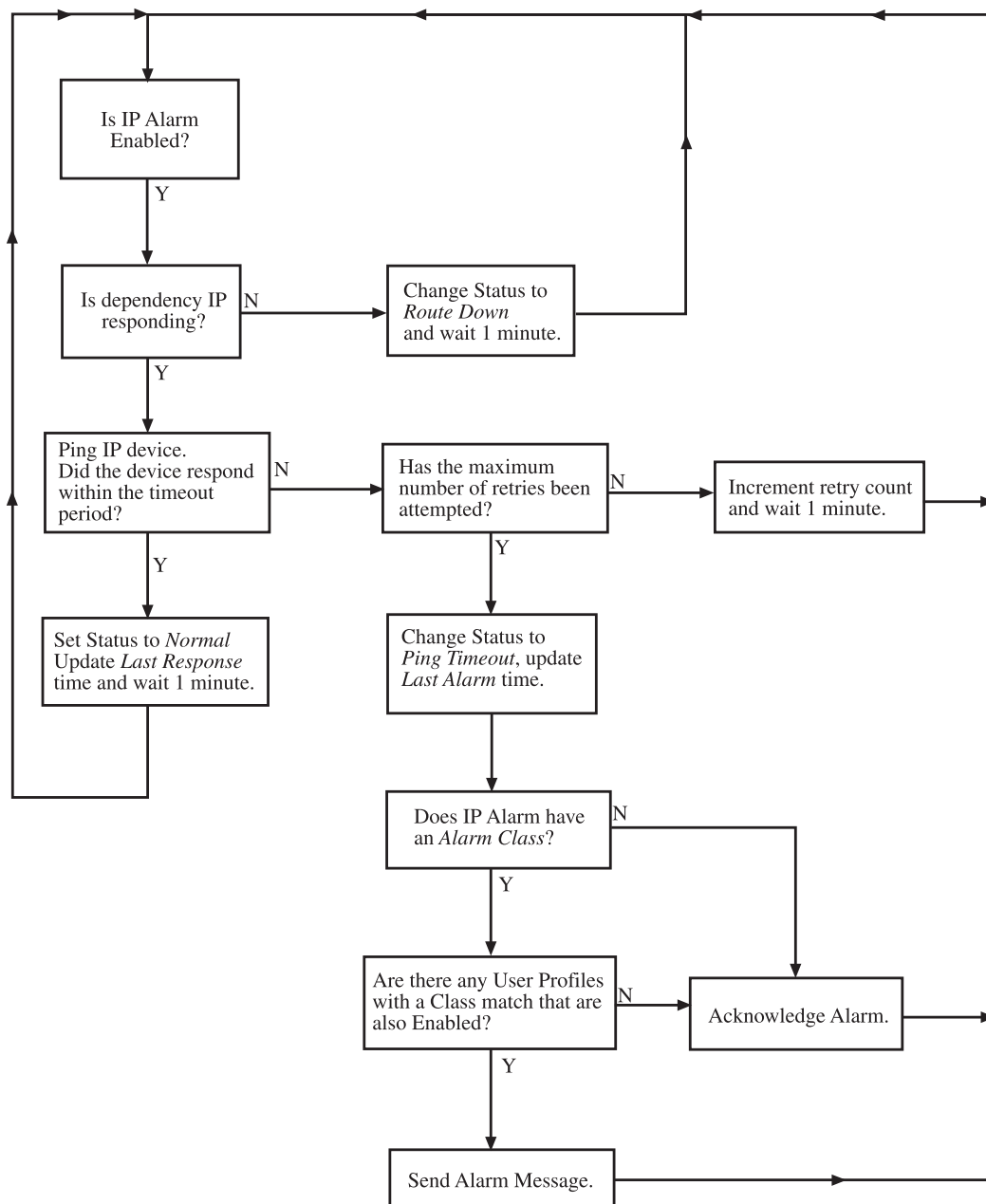
Figure 28: IP Alarm Flowchart

REMOVING AN IP ALARM

Expand the IP Alarms and right-click on the IP Alarm you wish to remove. Choose *Delete this IP Alarm*, and it will be removed.

INPUT/ALARM CLASSES

Classes are used to associate environmental inputs and IP alarms with people. Each input sensor or IP address must be assigned to a *Class*. Each person or *User Profile* selects classes for which they have responsibility. To view the list of Classes, expand the *Settings* menu, then right-click on Classes and select *Properties*. Several classes have been pre-defined in the IMS-4000E to give you a starting point. The default *Classes* are:

- (Diagnostic)

• Temperature	• Humidity	• Water	• High Sound
• Power	• Other	•Smoke	
• Security	• Backup Battery	• IP Alarms	
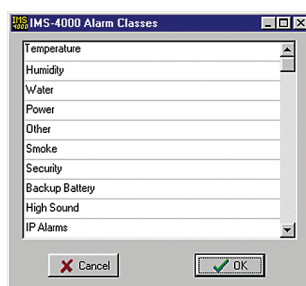
Figure 29: Setup Classes

You can have up to 64 classes in the IMS-4000E. To add Classes, just type in a new class name in the Class table list and click OK. The class programming screen is shown above. Note that the *Diagnostic* Class does not appear in the list shown above. This is because it is a special case, reserved for system faults, trouble alarms, and diagnostic alarms. The *Diagnostic* class cannot be edited or deleted. Any user who wishes to receive these types of alarms should include the *Diagnostic* class in their *Profile Class* list.

CONFIGURING USER PROFILES AND CONTACTS

CONFIGURING USER PROFILES

The User Profile section controls who has access to the IMS-4000E and who gets contacted when an alarm occurs. The User Profile programming screen describes attributes of the user including: name, title, company, dept, username, password, user code, time zone, classes, etc.

When an alarm occurs the IMS-4000E will check the list of User Profiles to see who should be contacted. Users whose class list includes the class of the alarm will be contacted. Each user can have up to 8 contact destinations (phone numbers, e-mail addresses, …). Up to 64 different User Profiles can be created. The IMS-4000E can contact users using 6 different methods: voice, pager, e-mail, and snmp trap.

The order of Profiles contacted can be changed. To move a Profile up or down in the list, click and hold the Profile you wish to move and drag it to its new location, then release the mouse button. The Profile should now display in its new location.

ADDING A PROFILE

Right click on *Profiles* and select *Add New Profile*. The following screen will appear:

Figure 30: User Profile screen

The Name, Company, Department, and Title information are used to identify the user on reports that the unit sends.

The *Username*, *Password*, and *User Code* are used for security purposes.

You must have a Username and Password to:

- Go online with the unit
- Request two-way e-mail features
- Access other features of the unit

The User Code is a four digit number that is required to request a voice status report and to acknowledge alarms. When the IMS-4000E receives a call, it will request the User Code. If a valid User Code is entered, the unit will match this code to the User's Class List and report the status of all Environmental Inputs and IP Alarms which correspond to the selected Classes. Voice Status reports check User permission, and a user can only receive information on items that he has permission to receive. This includes environmental and IP alarm status, PowerGate switching, ping requests, and microphone listen-in. (See "Permissions" section.)

The "Enable This Profile" option provides a convenient way to temporarily enable or disable a User Profile. When a Profile is disabled (unchecked), no alarms or reports will be sent to that user, and the user will not be permitted to log on to the system.

Clicking the *Permissions* button will bring up the Permission screen.

PERMISSIONS

Each user profile has a programmable security level for each device (host/nodes) in the system. To set the Security Access level click the Permissions button. There are three access levels: Master System Administrator, Site Administrator, and User. The restrictions for each security level is as follows …

	Master System Admin	Site Admin	User
Add user profiles	Yes	No	No
Disable user profiles	Yes	No	No
Edit unit properties	Yes	No	No
Edit e-mail settings	Yes	No	No
Edit Node properties	Yes	No	No
Update firmware	Yes	No	No
Configure data logger	Yes	No	No
Add/delete classes	Yes	No	No
Add/delete holidays	Yes	No	No
Edit default input templates	Yes	No	No
Delete sensors	Yes	Yes	No
Disable IP alarms	Yes	Yes	No
Reset min/max	Yes	Yes	No
Other programming changes	Yes	Yes	No
Add camera	Yes	Yes	No
Acknowledge alarms	Yes	Yes	Yes
Switch a PowerGate outlet	Yes	Yes	Yes
Online via local PC	Yes	Yes	Yes
Call in via voice	Yes	Yes	Yes
Call in via modem	Yes	Yes	Yes
Visit password protected Web	Yes	Yes	Yes

To configure a profile as a Master Administrator simply check the box at the top of the screen.
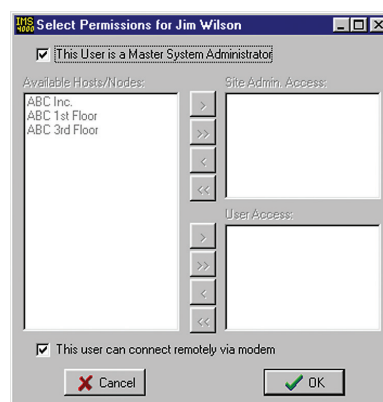

Figure 31: Permissions screen

To configure profiles for Site Administrator or User security levels, select the appropriate Host or Node(s) and click the arrow to copy the Host/Node(s) into the appropriate list. The double arrow >> will copy all units to the list while the single arrow > will copy just the selected unit to the list. Checking the box "*This user can connect remotely via modem*" at the bottom of the screen, allows the user listed at the top of the page to dial in to the system using a modem.

In addition to controlling programming access when using the IMS ConsoleView Software, permissions also have an effect during a telephone call. In voice mode the unit will recite only menus and status information for devices that the user has permission to hear. The associated Classes for each user will also control the content of voice reports. The same applies to two-way e-mail. A user can only receive information or send commands if they have the proper permissions and Class associations.

Examples:

1. If a User that has no Permissions on a particular Node, then the user will not be able to receive any Voice or e-mail reports that contain information about that Node.

2. If a User has permissions on a particular Host/Node unit but none of the environmental sensors are in his class, then he will not receive any information about the environmental sensors.

CLASSES

Clicking the *Classes* button will bring up the Select Classes screen.

Selecting Classes

The User can choose to receive alarm reports from one or more Classes. The list on the left displays all Available Classes. The list on the right shows Selected Classes for this profile. The Arrow Buttons are used to select or deselect classes. See the following Arrow Button definitions and the following figure:

>   Move the highlighted class on the left to the right

>>   Move all classes on the left to the right (select all)

<   Move the highlighted class on the right to the left

<<   Move all classes on the right to the left (deselect all)
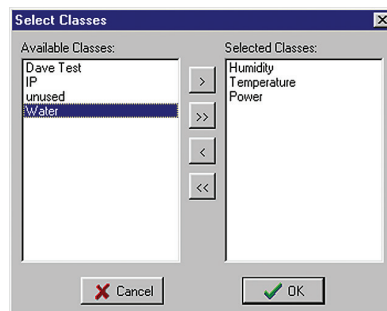

Figure 32: Class Selection screen

DELETING A PROFILE

From the hierarchy on the ConsoleView screen, right-click on the profile you wish to delete and select *Delete This Profile* in the contextual menu.

CONTACTS

The Contacts are the actual telephone numbers, e-mail addresses, pager numbers, etc… that the IMS-4000E will contact when an alarm occurs. You can have up to 8 Contacts per User Profile. Each Contact can have its own Schedule so that you can have certain Contacts be Enabled during daytime hours and others Enabled during nighttime hours. Only Contacts which are Enabled when the alarm occurs, will be contacted.

The order of Contacts can be changed at any time. To move a Contact up or down in the list, click and hold the Contact you wish to move and drag it to its new location, then release the mouse button. The Contact should now display in its new location.

ADDING CONTACTS

To add a Contact, right-click on the User Profile you wish to add a contact to and select *Add New Contact*. An entry called New Contact will appear below the User Profile. Right-click on the New Contact and select *Setup*. The following screen will appear:
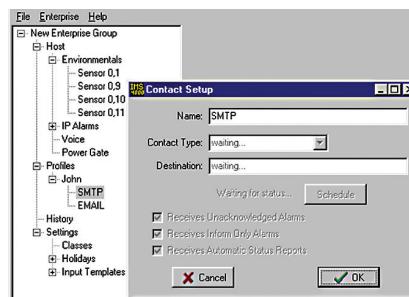
Figure 33: Contact Setup Screen

Enter a Name which describes the contact, like "Jim's Cell," "Acme Inc. e-mail," or "Jim at home."

Select the Contact Type using the drop down arrow. The choices are: Voice, Numeric Pager, Email, and SNMP.

Destination: Enter the Telephone Number, E-mail Address, or Server Name/Address for the contact.

VOICE CALLS

For most voice calls you can simply enter the telephone number of the person you want called. Consider the location of the IMS-4000E Host when entering the number. If an area code is required to call from the Host to your telephone, be sure to include it.

Examples:

No area code required: 555-1234

Area code required: (610)-555-1234

1 + area code required: 1-(610)-555-1234

You can also include additional codes within the telephone number. Listed below are the special code letters and a description of each:

p = 2-second pause

w = wait for answer

b = blind dialing (makes the unit dial and start speaking the message without requesting that a key be pressed)

! = flashes the phone line (momentary hang-up and reconnect, useful in some PBX systems)

These codes can be useful if you want to call an extension within a business. For example, suppose your office was answered by an auto-attendant, but you know that if you dialed the extension the call would be transferred. In this case you can program the telephone number, insert a w to wait for the auto-attendant to answer, and then add the extension you want dialed.

Example: 555-1234-w-170 {Extension 170 will be dialed after the auto-attendant answers}

NUMERIC PAGER CALLS

The IMS-4000E can send alarm messages to numeric pagers. It will automatically send its ID telephone number when dialing to a numeric pager. All you have to do is enter the telephone number of your pager. Be sure to include the (area code) or 1 + (area code), as necessary.

Example: (301)565-2300

If your pager service is answered by a voice-prompted message, or if your pager service allows only a few seconds to enter a number before disconnecting, you will need to enter the telephone number differently. In this case, enter the pager telephone number + two or more pauses + the Host ID telephone number + #.

Example: (301)565-2300-pp-844-1900-#

E-MAIL

Enter the e-mail address.

SNMP

Enter the SNMP server IP address in numeric form (e.g. 192.168.0.1)

SCHEDULE

Click the Schedule button to bring up the Schedule screen for this Contact. Choose the times you want the Contact to be enabled by adjusting the blue bars. Areas where the blue bar appears indicates the day and time the Contact is Enabled.
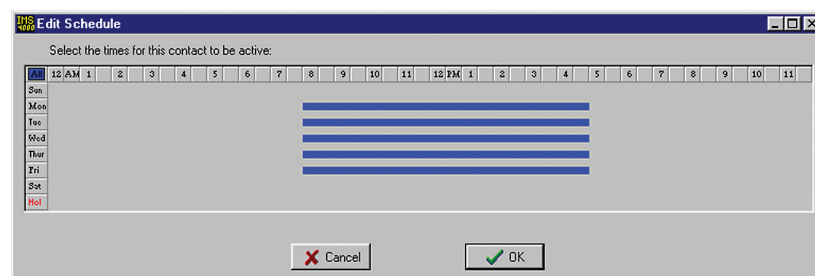
Figure 34: Contact Schedule screen

For example, the schedule above enables the contact Mon-Fri 8AM to 5PM.

Editing the schedule:

- Click on the All button in the top left corner of the grid to enable/disable the entire week.
- Click on the day buttons down the left side of the grid to enable/disable entire days
- Click on the hour buttons across the top of the grid to enable/disable entire hours
- Drag the mouse over portions of the grid to enable/disable specific hours/days

ALARM DELIVERY OPTIONS

There are additional options which appear on the Contact Setup screen depending upon the type of call. For alarm delivery you **must** select either *Receives Unacknowledged Alarms* or *Receives Inform Only Alarms* or both.

<u>Receives Unacknowledged Alarms</u>: This option applies only to voice and pager calls. When selected the IMS-4000E will call this contact until the alarm has been acknowledged or until the number of call attempts has been exhausted. If the alarm is acknowledged by another user, this contact will stop being called.

<u>Receives Inform-only Alarms</u>: This means that the alarm message is for information purposes only. Once the alarm message has been delivered, the IMS will stop calling this contact. This selection is useful for insuring that a record of an alarm is sent. When this option is checked, the IMS-4000E will always send an alarm message to this contact.

> **Note:** If no "Until Acknowledged" contacts are selected to receive an alarm message, the IMS Host will self-acknowledge the alarm.

SAVING AND LOADING PROGRAMMING

The programming in your IMS-4000E can be saved to a file. This gives you the ability to back up your programming or copy the same programming to another IMS-4000E unit. Note that the file you save will not include custom voice files or settings entered through the serial port (network parameters, web settings, two-way e-mail, RAS, etc.). To save your programming to a file, right-click on the name of your host and select *Save Programming*.

To load a programming file into your IMS-4000E, right-click on the name of your host from the menu tree and select *Load Programming*. Select a programming file to load and click the *Load button*. Your unit will have to restart for the new programming to take effect. When the unit restarts, you will be logged off. After 10 or so seconds reconnect to the unit.

RECONNECTING

At times your PC and IMS-4000E Host units may become disconnected. This may happen due to a system restart or other communication-related problem. You can reconnect to an IMS-4000E using the *Reconnect* command. To reconnect to a unit, click on *File* from the main menu and select *Reconnect*. Highlight the IP address of the unit you want to reconnect with and then click the *Reconnect* button.
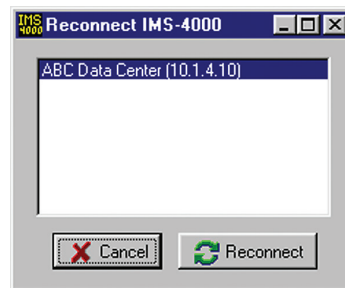

Figure 35: Reconnect Screen

RECORDING AND UPLOADING VOICE MESSAGES

Custom voice messages can be assigned to many aspects of your IMS system. Voice messages are used during call-in status reports and alarm dial-out. This allows the system to identify and describe exactly where the problem is located, which equipment is affected, or which network device is not functioning. You can assign custom voice messages to the following:

IMS-4000E Host {See Host Properties}

IMS-4000E Node {See Node Properties}

Each Environmental Input {See Channel Setup}

Each IP Alarm {See IP Alarm Setup}

Each PowerGate Device {See PowerGate Setup}

Each PowerGate Outlet {See PowerGate Setup}

Voice messages can be recorded using any device that allows you to save messages in the WAV or PCM format. Recordings should be trimmed to remove silence at the beginning and end of each message. Give each recording a file-name that matches the content of the message to make it easier to assign the appropriate message to your devices, sensors and IP alarms.

Once your recordings are completed upload them into the IMS-4000E by clicking the 'Add' button on the IMS-4000E CustomVoice Manager. Select the message you would like to upload then click OK. The new voice message will be loaded into the IMS-4000E and will appear in the list. The window to the right displays all of the voice message file names stored in the IMS-4000E. To change the file name of a voice message click 'Rename'. Enter a new file name and click OK. To delete a voice message, highlight the message and click the 'Delete' button. To listen to a voice message, highlight the message and click the 'Listen' button. Note: You must have a sound card and speakers/headphones to hear the audio. To save voice messages from your IMS-4000E onto your computer, highlight the file name and click the Save button. Select the folder on your computer where you would like the file saved and click OK. This feature is useful to create a backup of the voice messages or to copy voice messages from one IMS-4000E Host to another.

For the voice messages to play back correctly you must set the recording format to PCM, 8KHz, 8 bit, mono. To set these parameters click *File*, then *Properties*. Next, click the *Convert Now* button. In the Format field select "PCM." In the Attributes field select "8,000 Hz, 8 Bit, Mono 8 KB/s." See the following screen.
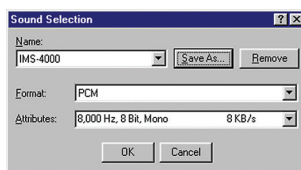

Figure 37: Sound Specifications Screen

HOLIDAY SETUP

The IMS-4000E allows you to program recurring or non-recurring holidays that you can use within your schedule programming. These schedules are used to enable or disable monitoring of Environmental and IP Alarms, and also to enable/disable times when users will receive alarm calls.

To see which holidays are currently programmed, expand the Settings menu by clicking the plus sign next to the word *Settings*, then expand the Holidays menu by clicking the *plus* sign next to the word *Holidays*. See sample below:
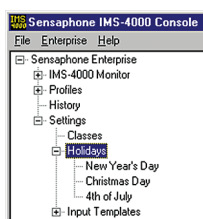

Figure 38: Holiday List

To view the programming of a particular holiday, right-click on the holiday name and select *Properties*.

To program a new Holiday, expand the Settings menu and right-click on the word *Holidays*, then select *Add New Holiday*. The new holiday programming screen will appear as shown below:
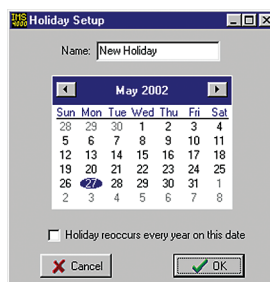
Figure 39: New Holiday

Enter a name for the holiday. Select the month, day, and year for the holiday. Finally, select whether the holiday is recurring. Click *OK* when finished.

ALARM MESSAGE POP-UPS

While online with one or more IMS-4000E units through the ConsoleView Software, you can have an alarm message pop up on your computer screen whenever an alarm occurs. This could be an environmental or IP alarm on any Host or Node. You can configure this feature to display a general message indicating the Unit and Channel names, or you can associate a custom message with each input. The custom message can be displayed as plain text or HTML. The custom messages can be stored either on the local workstation or a drive that is regularly mapped to the workstation.

Activating Alarm Pop-Ups

Click on *File*, then *Options* from the main menu in the ConsoleView Software. The following screen will appear.
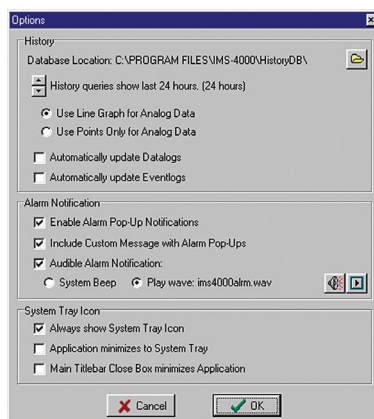
Figure 40: Options Screen

Within the section titled "Alarm Notification" click in the box to *Enable Alarm Pop-Up Notifications*. This will activate the Alarm Message Pop-Up feature. When an alarm occurs, a message will appear that simply displays the Unit and Channel names. If the user has permission to acknowledge the alarm, an Alarm Acknowledgment box will also appear. A sample message is shown below.
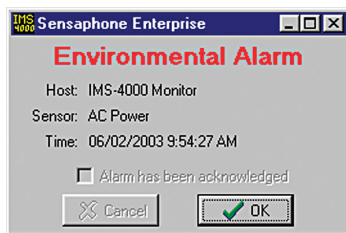
Figure 41: Simple Alarm Popup

Enabling Custom Pop-Up Messages

To have custom messages pop up, you must enable this feature. Select *Options* from the main menu. Click in the box labeled *Include Custom Message with Alarm Pop-Ups*. Next, you must select where your custom messages will be stored (*see below*).

Setting Pop-Up Text Location

When using custom pop-up messages you must specify where these messages will be located. To do this, right-click on the name of your host within the menu tree and select *Alarm Pop-Up Notice Location*. Select the drive and folder where the messages will be stored.

Editing Pop-Up Custom Message

To edit the custom message for a particular environmental input or IP alarm, right-click on the chosen input and select *Edit Alarm Pop-Up Message*. The following screen will appear.

Figure 42: Edit Popup Screen

Messages can be displayed as text or HTML. Select the type of message you want to enter and type your message into the text area. This window will scroll to accommodate lengthy actions. Note that using HTML, you can embed web links in the message for more advanced actions. To test your HTML code, click the *Preview* button. To return to the edit screen click the *Edit* button. See samples below.
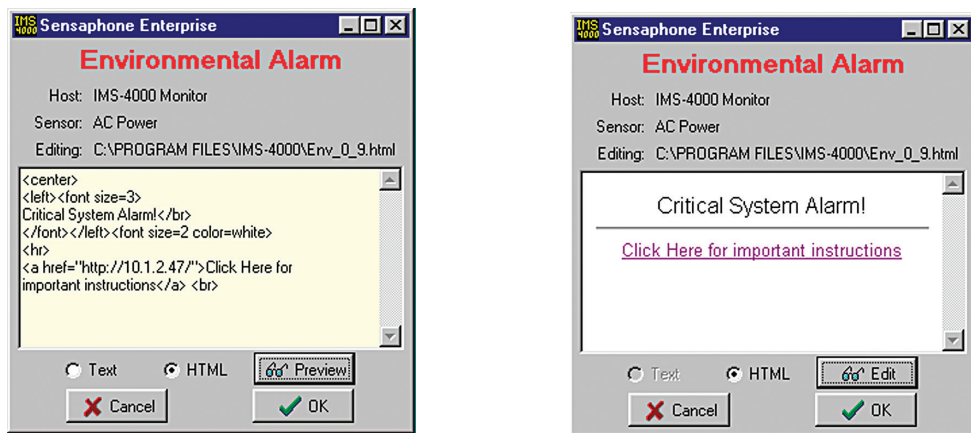
Figure 43: HTML Edit Screen and HTML Preview Screen

Audible Alarm Notification

The ConsoleView Software can optionally beep or play a custom Wave file whenever an alarm is detected. To utilize this feature, click *File*, then *Options* from the main menu. Under the Alarm Notification section select *Audible Alarm Notification*. Next, select either *System Beep* or *Play Wave*. If you selected *Play Wave*, then you must select the Wave file to be played. Click on the speaker button to choose a Wave file. After you've made your choice, you can preview it by clicking the *Play* button. See sample screen below:
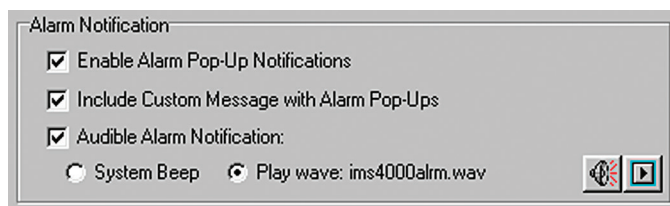
Figure 44: Alarm Notification screen

E-MAIL SETUP AND TWO-WAY E-MAIL COMMANDS

The IMS-4000E can send alarm messages via e-mail using SMTP as well as respond to commands via e-mail. See the Two-Way E-mail section for more information on sending commands.

To set up the e-mail parameters right click on the Host name and select *Network Settings*. Select the Email Settings tab to see the following screen:

Figure 45: E-mail Settings tab

To have the unit send e-mail, you need to set the *SMTP Server* name and the *Return e-mail Address*, *Username* (if required) and *Password* (if required). To have the unit respond to Two-Way e-mail commands you must also set the *POP Server* name, e-mail account *Username* & *Password*, and the *Mail Check Interval*.

SMTP Error messages

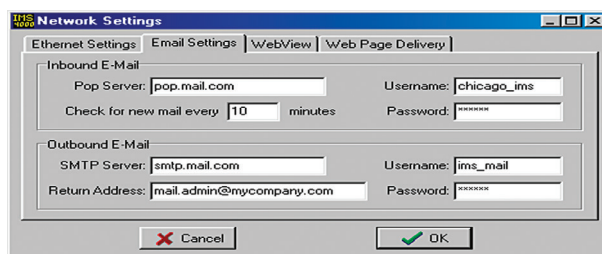If your e-mail settings are incomplete or incorrect there are some messages that will appear in the Event History log which may be helpful.

The "Invalid Configuration" message will appear if you don't have both the SMTP Server name and Return Address programmed. These are the minimum programming requirements to send e-mail. If you have at least these two items programmed and the IMS-4000E is unable to deliver the message, then you will get the message "SMTP Server not Responding," which essentially means that you have one or more of the following problems:

(a) The wrong SMTP server name programmed.

(b) The wrong username programmed.

(c) The wrong password programmed.

(d) A username is programmed but none is required.

(e) A password is programmed but none is required.

(f) All of the e-mail settings are programmed properly but the unit cannot reach your SMTP server for network routing reasons.

(g) The unit cannot reach your DNS server and thus cannot look up the SMTP server IP address.

(h) The DNS server IP address is programmed incorrectly in the IMS Network Configuration settings.

Two Way E-Mail

The IMS-4000E Host has the ability to send and receive standard pop/smtp e-mail. In addition to using e-mail as a method of delivering outbound alarm messages, e-mail can also be used for remote access into the IMS-4000E. A set of commands is available that can be sent to a 4000, within an e-mail, that will cause the 4000 to reply back to the sending e-mail address. Commands are available to inquire status, perform network ping and IP trace-route, and control outlets on a PowerGate.

> **Note:** Two-way e-mail is dependent upon User permissions. This means that the user can only receive information on items for which he has permission. (See "*Permissions*" section)

In order to have the IMS respond to e-mail commands you must first obtain an e-mail address for your IMS-4000E from your internet provider, configure the e-mail settings for your IMS Host (see e-mail setup), and have Two Way E-mail enabled (see Host Local Configuration in the Host Installation Manual).

> **Note:** The username and email address used in two-way e-mail commands must match a Profile Username and Contact. The response will be sent to the specified e-mail address.

Requesting a Status Report

To request a status report, send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: status
```

Requesting an IP Ping

To request an IP ping, send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: ping xxx.xxx.xxx.xxx
```

Requesting a Trace Route

To request an IP trace-route, send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: traceroute xxx.xxx.xxx.xxx
```

Requesting a PowerGate Outlet Command

To request a PowerGate Outlet command, send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: powergate "<PowerGate Name>" "<Outlet Name>" on/off/cycle
```

For example:

```
To: ims4000@mycompany.com
Subject: ims4000
username: jsmith
email: jsmith555@aardvark.net
command: powergate "Gear Rack #1" "Netgear switch #3" cycle
```

Requesting a Picture from a Camera

You can receive an e-mail with an attached picture from any camera configured in the IMS-4000E. The picture will be captured when the IMS-4000E receives the e-mail request.

To receive a picture, send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: camera <camera name>
```

For example:

```
To: ims4000@mycompany.com
Subject: ims4000
username: jsmith
email: jsmith@aardvark.net
command: camera NY Datacenter
```

Requesting Help

You can receive a brief overview of how to use and format two-way e-mail commands, by requesting help.

Send an e-mail message to your IMS-4000E Host with the following information:

```
To: <e-mail address of your IMS-4000E>
Subject: ims4000
username: <valid profile username>
email: <your e-mail address>
command: help
```

For example:

```
To: ims4000@mycompany.com
Subject: ims4000
username: jsmith
email: jsmith@aardvark.net
command: help
```

CONFIGURING A VIDEO CAMERA

The IMS-4000E is compatible with network cameras available from Axis Communications (www.axis.com). By associating a network camera with your IMS-4000E you can create links to the live stream video stream and capture images that can be sent via e-mail when an alarm occurs. The camera connects to your network via an RJ-45 jack. Up to 128 cameras can be associated with each Host or Node. The IMS-4000E ConsoleView Software and web page allow you to click and view live video wherever your camera is installed. You can also capture a still image by right-clicking and choosing Capture Image.

The first step is to get the camera running on your network. This process is independent of the IMS-4000E. Follow the instructions included with the camera to get it set up on your network. Once the camera is properly set up, go into the IMS-4000E ConsoleView Software or web page. Cameras are added to the IMS by expanding the Host menu and right-clicking on the word Cameras. Choose Add Camera. This will bring up the Camera Setup screen (see below). Enter the IP address, port number, and security settings (if required) of the camera according to how it has been configured on your network. See sample screen below:
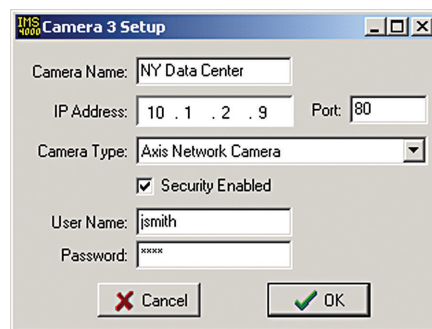
Figure 46: Camera Setup

Select the camera type by clicking on the drop-down arrow and selecting the camera. Click OK when Finished.

Up to 128 cameras can be configured in an IMS system. Once the camera(s) have been configured they can then be associated with a particular Host or Node so that links for these cameras will appear within the menu tree for the chosen unit. You can associate a camera with more than one device if desired. To associate one or more cameras, right-click on Cameras within the menu tree for the selected host or node and choose Associate Cameras. See screen sample below.

Figure 47: Associating Cameras

The window on the left lists all cameras programmed into the system. The window on the right lists cameras associated with the selected Host or Node. To move a single camera to the other window, highlight the camera and click the single left/right arrow. To move all cameras to a new window, simply click the double arrows. This will copy all listed cameras to the other window. If you click on Cameras you will see thumbnails of all associated cameras. To view a large image of a particular camera, simply click on the image.
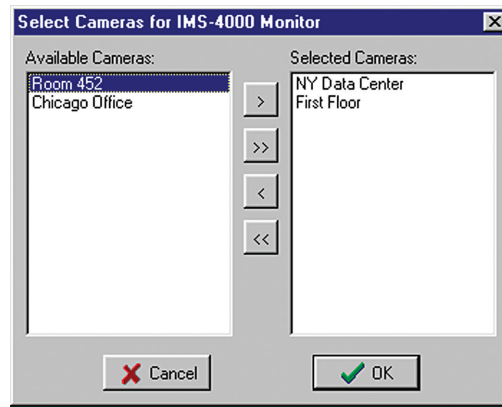
Caution: The Axis network cameras are Ethernet devices. They should only be connected to your Ethernet network. Do not connect them directly to your IMS-4000E Host or Node unit. Connection of any network cameras directly to your IMS-4000E sensor inputs may cause damage to the device.

HISTORY

The IMS-4000E stores both datalog and eventlog history internally. The datalog is a time-stamped collection of input values that can be used to view and graph environmental conditions over time. It can also store the status of IP devices. The user can choose which inputs or IP alarms are stored and specify the overall sampling rate. Care should be taken to select the number of inputs and sampling rate accordingly, since large amounts of data can potentially be logged. The more data being logged, the faster the history log will fill up.

The eventlog contains time-stamped messages that describe activities performed by the unit such as alarm detection, user logins, telephone calls, and alarm acknowledgement. The eventlog history is useful when you want to review the historical events monitored and performed by the IMS-4000E.

When a user goes online, information for both the datalog and eventlog history is automatically retrieved and stored in a database on a user-specified hard disk. This can be a drive on your own computer or a network server. While the program defaults to saving the history database on your local drive, if the system will be used by many users it may be advantageous to store the database on a network drive. To specify the drive for saving History information click *File*, then *Options* from the main menu. A sample screen is shown below:
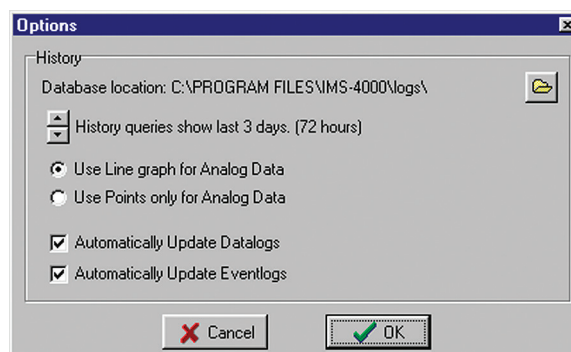

Figure 48: History Options

To change the location for storing the History database, click the folder button on the right side of the screen and choose a new location. The location you select will be displayed to the left.

Use the up or down buttons to select the amount of history to be viewed when accessing the *History* option through the right-click menus in the ConsoleView software. This provides a quick view of the history for a particular Input or Profile. The default time is 24 hours (1 day). Clicking the arrows will increase or decrease the data time by days.

Analog input values will automatically be graphed when viewing *History* through the right-click menus of the ConsoleView software. You can choose to have the graphed data displayed as a line graph or simply show the discrete data points.

You can also deselect the *Automatically Update* buttons if you don't want the Datalog or Eventlog to download each time you connect. If you are using a dialup connection, you may want to disable these functions to speed up the software loading process. (You can manually download the logs as desired by right-clicking on *History* in the menu tree.)

DATALOG HISTORY

The IMS-4000E can log up to 62,500 samples of environmental and IP Alarm history. When the log fills, it will over-write the oldest data first. Environmental data will display the actual value, while IP Alarm data will display either *Normal, Timed Out*, or *IP Down*. All stored history is logged at the same interval as programmed on the History programming screen. To set up the Datalog History, right-click on *History* from the IMS menu tree and select *Properties*. Enter the Interval time and click the *Enable* box. This will start the Datalog feature. The Datalog will store Environmental and IP Alarm values if datalogging is enabled on their respective programming screens.
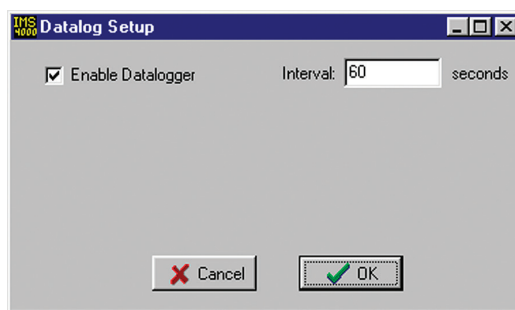
Figure 49: Datalog Setup Screen

Viewing History

Datalog History can be viewed through the ConsoleView software or via the IMS web page. It can be viewed through the ConsoleView software in two ways: There is the quick view which can be displayed by right-clicking on an input or profile and selecting *History*, or you can perform a query on the entire history database using the HistoryView program (right-click on History in the menu tree and select *HistoryView*, or from the main menu select *File*, then *HistoryView*).

History QuickView

You can display a quick view of an input or profile by simply right-clicking on the item and selecting *History*. This will provide an event listing and graph of the input over the last 24 hours (default). You can change the amount of history displayed to several hours or several days by changing the setting on the *Options* screen under the *File* menu. A sample is shown below:

Figure 50: AC Power History

Querying the History Database with HistoryView

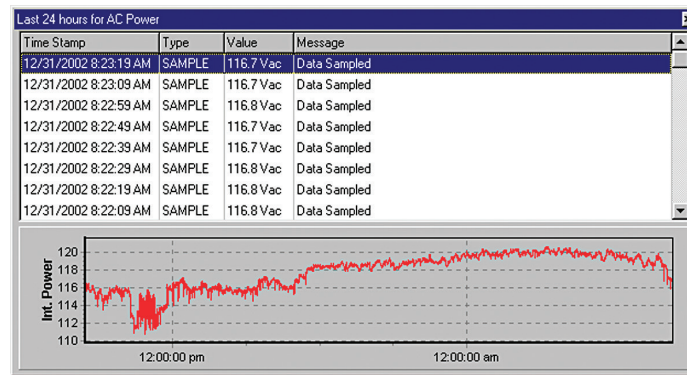The HistoryView program allows you to query the entire History database for all IMS units. There are filters to select Samples, Alarms, System messages, or User Logins. You can view data from an IMS Host and its associated Nodes combined, or individually. You can also graph sampled data.

To begin, run the HistoryView program by right-clicking on *History* in the menu tree and select *HistoryView*, or from the main menu select *File*, then *HistoryView*. The first screen will prompt you to select an IMS Host. Click in the box next the Host you want to Query. The program will then load the associated nodes and input names. In the upper left hand part of the screen is a drop-down box labeled Database. This lets you select between the current database (i.e. History) or a database archive. The default is always the current database, however, if you wish to query data that has been archived you will need to select the appropriate archive database. The archive file names are based on the start and end dates to assist in selecting the proper time frame. Next, select the Host or Nodes that you want to query information on, then select any filters that you want to apply. If you select All you will see all events and data samples for the selected units. If you select *Samples* or *Alarms* you must then choose one or more Environmental Inputs or IP Alarms.

> **Note:** the number that precedes each Environmental and IP description corresponds to the unit number to which they're connected (0 being the Host and 1-31 being the associated Nodes).

If you double-click on an item in the Environmental or IP Alarm box, all of the listed items will become selected and/or deselected. Last, select a time frame to perform the query and click *View*. The selected data will now be displayed. See sample screen below:
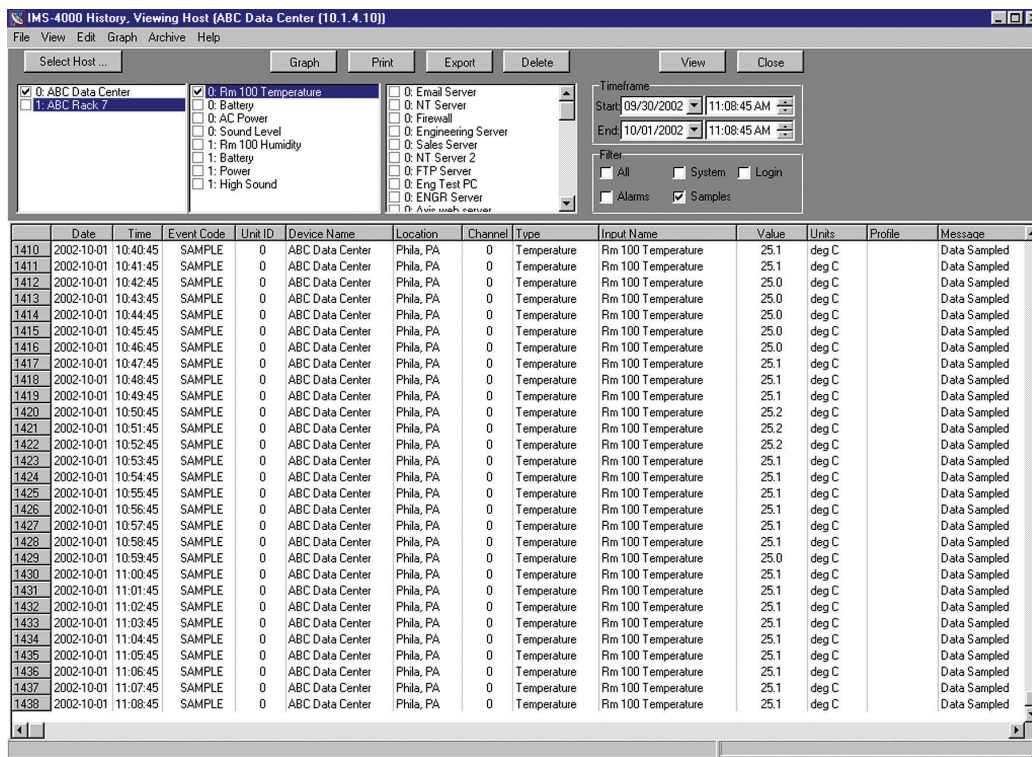

Figure 51: History Viewer

Graphing

Graphing data is possible when the selected query contains only Samples.

If you click on the *Graph* button, all of the points in the query will be displayed as a line graph. There are also options (from the *Graph* menu above) to format and display the data as a bar or area graph. You can have up to eight items displayed on the graph at once. To view different parts of the graph use the arrows on the bottom and sides to adjust the position. A graph can be printed by clicking the *Print* button at the top of the screen. You can copy the graph to the Windows clipboard by clicking the *Copy* button. This allows you to paste the graph into other applications. The *Zoom In* and *Zoom Out* buttons let you view the data with more or less detail. The Reset button restores the original view of the graph. When finished, click the *Close* button to return to the grid.

Printing Data

You can print the data viewed in the grid by clicking the Print button. Printing defaults to an Arial 5 pt. font in order to fit one line of data across one line of an 8.5" x 11" sheet of paper printed in landscape mode. You may choose different fonts and type sizes.

Exporting Data

The *Export* button allows you to save the queried data in the grid to a file format which can be easily imported into other applications. Options include the ability to save the file in CSV format, formatted text (prn), and tab delimited (txt) format. Note: The exported data will represent *only* what you've selected to query.

Click on *File* and select *Export Field Names* from the submenu if you want the field titles (Date, Time, Event Code, etc.) to be included with the data when you export.

Copying to the Clipboard

You can highlight and copy selected cells within the grid to the Windows clipboard. To highlight the data simply click-and-hold the left mouse button and drag the mouse over the cells you wish to highlight, then either right-click and select *Copy*, or click *Edit* from the main menu and select *Copy*. To select all of the data in the grid, right-click within the grid and choose *Select All* from the contextual menu, or click *Edit* from the main menu and choose *Select All* from the submenu. This will highlight all of the data in the grid. You can then perform the Copy function as previously described.

Deleting Data

The *Delete* button will remove the queried data displayed in the grid from the database.

TheViewer Menu offers you other features as well to customize your report.

Archiving

As the history database grows it will begin to take longer to perform a query. It is recommended that the database be periodically archived to keep the size reasonable and to permit satisfactory performance of the HistoryView program. Archiving may be done as often as necessary for performance reasons but it *must* be done when the database reaches its physical limit. To find out how big the database is for a particular unit, select *Database Statistics* under the *Archive* menu. The size of the database and percent full will appear in the status bar along the bottom of the grid. A warning message will appear when the database reaches 80% of its capacity.

To archive the history database you must first disconnect the Host from within ConsoleView. Next, select *Archive* from the main menu and then choose Select *database to archive*. Locate the history.db file for the unit you wish to archive and click *Open*. Next, enter the date range to archive (typically one or more months or a quarter). Click the Archive button. The program will ask if you want to delete archived records from the database. If the database is large then it is recommended that you select yes. The History database will not be reduced in size unless you eventually delete records. The archived data will be stored in a file that includes the "from" and "to" date range in a yr/mn/dy format.

After archiving it's recommended that you Pack the history database (history.db) to free memory and reduce the file size. To do this select *Pack Database* from the *Archive* menu. Note that the *Pack Database* function can only be executed while offline with the IMS unit. To run HistoryView while not connected, click *File*, then *Run* from the ConsoleView main menu.

To view archived data, select the archive database from the drop down menu on the top left part of the screen. Then run a query as usual. You can also restore archived data back into the main "History" database. The archive filename indicates the date range of the data contained in the file. The format is (start date) yr-mn-dy followed by (end date) yr-mn-dy. This will merge the archived data back into the current history database. This may be useful if you need to query across date ranges that span more than one database file. Be careful not to exceed the file size limits when combining an archive database with your current database as this may cause file corruption. To do this, choose Select archive to restore from the Archive menu. Next, choose the archive file you wish to restore and click Open. Next, click the Restore button. The archived data will be copied into the history database and a query can be performed.

Manually Forcing History Downloads

You can manually force full history downloads at any time. As previously stated, if you're on a dialup connection, you may choose to disable auto updates, and need to download the data periodically. To do this, go to your main IMS menu and right-click on History in the tree diagram.

Select *Force Full Eventlog Download* to manually download the Eventlog or Select *Full Datalog Download* to manually download the current datalog.
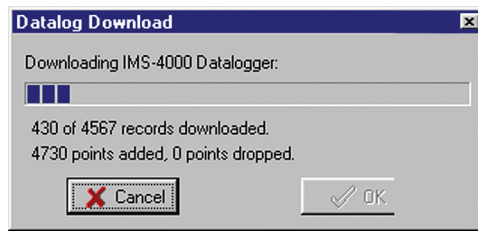

Figure 52: A manual Datalog Download in progress

UPDATING FIRMWARE

From time to time Firmware updates will become available to add features or improve the performance of your IMS-4000E. Most Firmware updates will be included as part of a complete IMS-4000E installation upgrade. Check the IMS-4000E website (www.sensaphone.com/support-4000.html) for the latest information on updates. If you register your unit you will always be informed of the latest features, enhancements, and corrections.

To check the version of Firmware in your IMS-4000E, right-click on the *Hostname* and select *Version Info*. The following screen will appear.
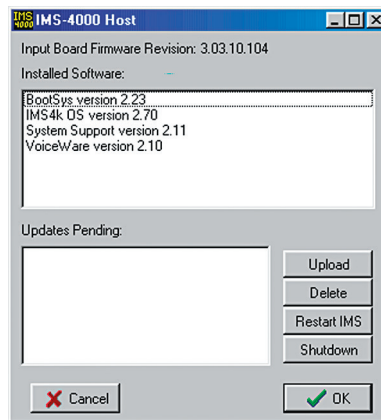
Figure 53: Version Info Screen

The IMS-4000E unit firmware comprises four files: *BootSys version, IMS4k OS version, System Support version*, and *VoiceWare version.* This screen includes functions to upload new firmware and restart the system. Always follow the instructions included with the new firmware files prior to installing any new versions. (Note that the Node firmware is installed separately on the Node Diagnostics screen.)

CHAPTER 3: OPERATION

After installation and programming have been completed, the Sensaphone IMS-4000E is fully operational. This chapter explains how the IMS-4000E operates.

ALARM DELIVERY AND ACKNOWLEDGMENT

The IMS-4000E can be programmed to contact specific users when an alarm occurs. A user may be contacted depending on whether the alarm has already been acknowledged by another user, or regardless of acknowledgement by other users. This allows flexibility in configuring your system for the way you want alarms handled. When a user does not wish to be contacted if someone else has already acknowledged the alarm, then we call this contact type an "Until Acknowledged" contact. "Until Acknowledged" means that a user is on the call list until the alarm is acknowledged, and once acknowledgement is received, this user is removed from the list. If a user always wants to be contacted when an alarm occurs, we call this contact type "Inform Only." This means that this user will always receive notification of the alarm, regardless of acknowledgement by other users.

ALARM ACKNOWLEDGMENT

Alarms can be acknowledged six ways:

1) By entering your Usercode using a touch-tone telephone when prompted during a Voice telephone call.

2) By calling in to the unit and entering your Usercode via touch-tone phone when prompted. Only alarms that are in the User's Class can be acknowledged. Note that the Intercall Delay must be set to a minute or more to allow time to call in to the unit.

3) By logging-in to the IMS-4000E and clicking the Alarm Acknowledgment button on the status screen for the Input in alarm. See sample below:
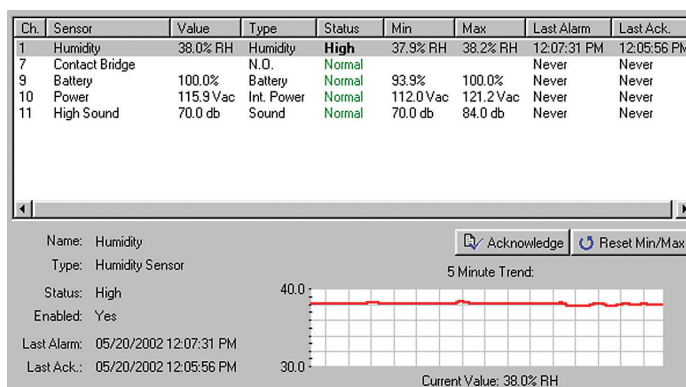

Figure 1: Alarm Acknowledgment button

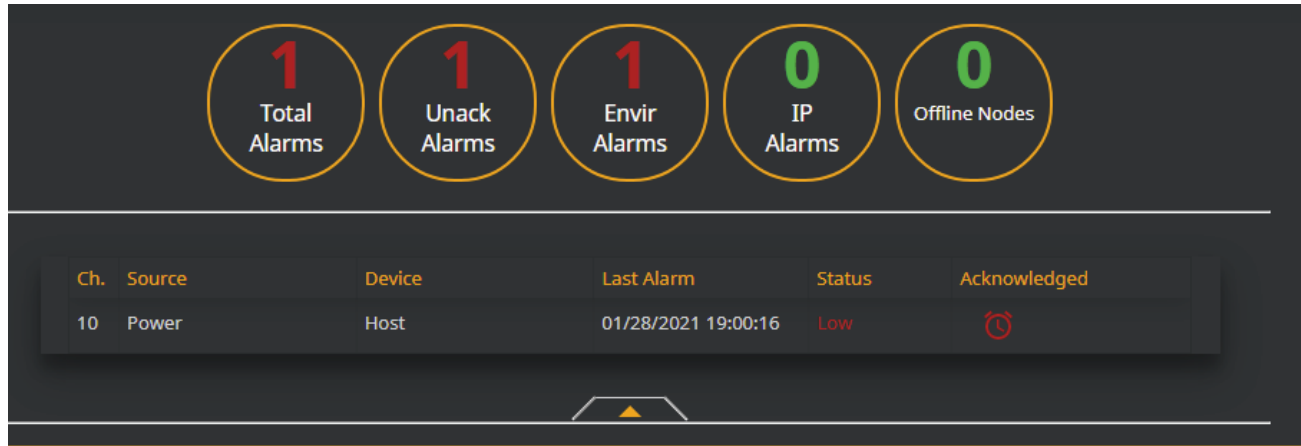4) By clicking the red Alarm clock icon on the IMS webpage.

Figure 2: Web page acknowledgment

5) By SNMP Management software.

6) By the IMS-4000E itself. If there are no Until Acknowledge contacts in the call list or if the maximum number of calling rounds has been exhausted, the IMS-4000E will self-acknowledge the alarm.

ALARM DELIVERY LOGIC

When an alarm occurs, the IMS-4000E will check for Class matches between the input or IP alarm and the User Profiles. When matches are found, the IMS-4000E will then check to see if the associated User Profile is enabled and then check the schedule of each of the Contacts for the profile. Those Contacts that are active at the time will then be called depending on whether they are enabled to receive Inform Only calls or receive Unacknowledged Alarm calls or both. Those contacts enabled for Inform Only will always receive the alarm message, regardless of whether the alarm has been acknowledged or the input or IP alarm returns to Normal. Contacts set to receive Unacknowledged Alarms will only receive calls if the alarm has not been acknowledged. Note that alarms can only be acknowledged during a voice call or by logging in via the IMS Consoleview Software. If there are NO calls of the Unacknowledged type, then the IMS-4000E will acknowledge the alarm immediately after starting the alarm delivery process. It is not recommended that you set pager calls to Unacknowledged unless there are also voice calls being made, the reason being that the only method of acknowledgment in this case will be to log in to the unit via the IMS Consoleview software. Voice Contacts that are enabled for both Inform Only and Unacknowledged will *always* receive the alarm message, but in addition will have the opportunity to acknowledge alarms by entering their Usercode via touch-tones (if the alarm hasn't already been acknowledged).

As long as an alarm remains unacknowledged AND it has Unacknowledged Contacts to be called, the IMS-4000E will continue to call these contacts until an acknowledgment is received OR the maximum dial attempts is reached. Alarms are acknowledged during a voice call by entering the User Code when prompted.

Sample Alarm Messages

Sample E-mail alarm message

```
Subject:              IMS-4000E Alarm
      Date:           Thu, 28 Mar 2002 10:59:47 -0500
      From:           ims4000@abcwidgets.com

FROM:   ABC Widgets Inc.
        IMS-4000E Host
        Boston, MA

ALARM MESSAGE:
High temperature ALARM at ABC Widgets Inc.
CH1: Server room temperature is now 90.3 Deg F
Level crossed limit of 85.0 Deg F
on Thursday 28 March 2002, 10:24:32 AM EST
```

VOICE STATUS REPORT AND TOUCH-TONE COMMANDS

The IMS-4000E is capable of delivering a spoken status report when called via telephone. The status report can provide information on both environmental conditions and IP alarms. In addition, you can ping devices over the telephone and switch PowerGate outlets.

USER SPECIFIC REPORTS

The environmental and IP status report is customized based on your User Code. Only callers with a valid User Code can hear a Status Report. The unit creates a custom report based on the Classes that the User has selected. Only inputs for which there is a Class match between the user Class List and the input Alarm Class will be reported. For example, if a user had selected temperature and humidity in their User Class List, then only inputs assigned to Alarm Class temperature and humidity will be reported.

Sample Status Report

To receive a status report, call the unit. When it answers wait for the beep. Immediately after hearing the beep, press any touch-tone. The unit will begin speaking and request your *User Code*. If the unit receives a valid User Code it will continue with several menu options. A sample of the main menu is shown below:

"Hello, this is the IMS-4000E at the *IT Dept of XYZ Company*"

"Enter your user code:"

To hear the environmental status, press **1**.

To hear the IP status, press **2**.

To ping an IP device press **3**.

To check the status of a PowerGate outlet, press **4**.

To switch an outlet on a PowerGate, press **5**.

To turn on the microphone, press **6**.

To disconnect, press 7.

To repeat this menu, press **8**.

If the caller had selected option 1 they would get a sub-menu asking if they would like to hear an environmental alarm summary report or a full environmental status report. The alarm summary only reports on inputs that are currently beyond their limits, or are in an alarm condition and have a *class* match. The full report provides status on **all** inputs that have a class match. A sample of a full environmental status report is listed below. Items in italics are custom messages recorded by the user.

Environmental sensors at the *IT Dept of XYZ Company*

Channel 1, temperature in the server room, is 76.4 degrees Fahrenheit, OK

Channel 2, temperature in rack B, is 82.7 degrees Fahrenheit, too high

Channel 3, humidity in the server room, is 33.9%, OK

Channel 6, water under server room floor, OK

Channel 7, smoke alarm in the server room, OK

Channel 9, battery, is 100.0%, OK

Channel 10, power, is 116.3 volts, OK

Channel 11, Sound level, OK

> **Note:** The Voice menus are intelligent, such that they will only recite menu options if there is relevant content. For example, if there are no IP Alarms programmed then the IP Alarm menu option will be skipped, or if there is no PowerGate connected, then this menu option will be skipped; or if the User has no Environmental sensors in his class, then these will be skipped.

VOICE ALARM DIALOUT

The IMS-4000E can call and deliver an alarm message in spoken English. After dialing, the unit will begin speaking "IMS-4000E Alarm Message, Press any key to continue." If the unit receives a touch-tone, it will recite the alarm message. When it finishes speaking the message it will request acknowledgement (if the call type is *Until Acknowledged*; if the call type is *Inform*, the unit will just speak the alarm message and disconnect). A sample Voice Alarm call is shown below:

"IMS-4000E Alarm Message, press any key to continue"

"IMS-4000E Alarm Message, press any key to continue" {call is answered and a 5 is pressed}

"IMS-4000E Alarm Message. The temperature is High at the IT Dept of XYZ Company."

"Channel 1, temperature in the server room, is 81.5 Degrees Fahrenheit"

"Level exceeded limit of 80 Degrees Fahrenheit at 7:45PM."

"Enter User Code:" {valid User Code is received}

"Alarm Acknowledged. Goodbye."

PERFORMING AN IP PING VIA TELEPHONE

The IMS-4000E allows you to perform an IP Ping during a voice call-in to the Host. After dialing the unit, press a touch-tone after the beep. The unit will request your *User Code*. Next, listen to the menu choices. Option 3 will allow you to enter an IP address in numeric dot-quad format. Use the * key for a dot. A sample IP Ping is shown below:

"Hello this is the IMS-4000E at the *IT Dept of XYZ Company*."

"Enter your User Code:" {valid User Code is received}

"To hear the environmental status, press 1."

"To hear the IP status, press 2."

"To ping an IP device press 3."   {3 is received}

"Enter IP address, Use the star key for dot. Press pound (#) when finished."

{user enters 10.1.4.17}

"Pinging now..."

"10.1.4.17 is not responding"

CALL-IN ALARM ACKNOWLEDGMENT

If you receive an alarm message on your pager or in your voice mail, you can still acknowledge the alarm by calling the unit back and entering your User Code. Note that the Intercall Delay must be set to at least 1 minute in order for the unit to answer a call.

When you call in to the unit, wait for the beep and then press a button on your touch-tone telephone. If there are unacknowledged alarms in the User's class, the unit will say "Unacknowledged alarms exist. To hear the alarms, press 9." If you press 9, the IMS will announce all unacknowledged alarms that are in the User's class. When the unit finishes announcing all of the alarms, it will say "Enter your user code." If the user code is entered correctly the unit will say "Alarm acknowledged" and it will acknowledge all of the alarms announced, and stop dialing all contacts programmed as "Until Acknowledged" type.

CHAPTER 4: USING THE WEB PAGE

LOGGING-IN VIA THE WEBPAGE

To access the IMS-4000E web page, open your browser and enter the device's IP address.

> **NOTE:** If you didn't assign your unit a static IP address and its using DHCP (default), then install and run the Sensaphone Locator software. This will identify the IP address of the IMS-4000E on your network. Sensaphone Locator software can be downloaded from https://sensaphone.com/service-and-support, then select IMS-4000E.

When the webpage loads for the first time you will be presented with a security warning message. This occurs because the browser can't authorize the default certificate. Click 'Proceed to Secure Connection'.
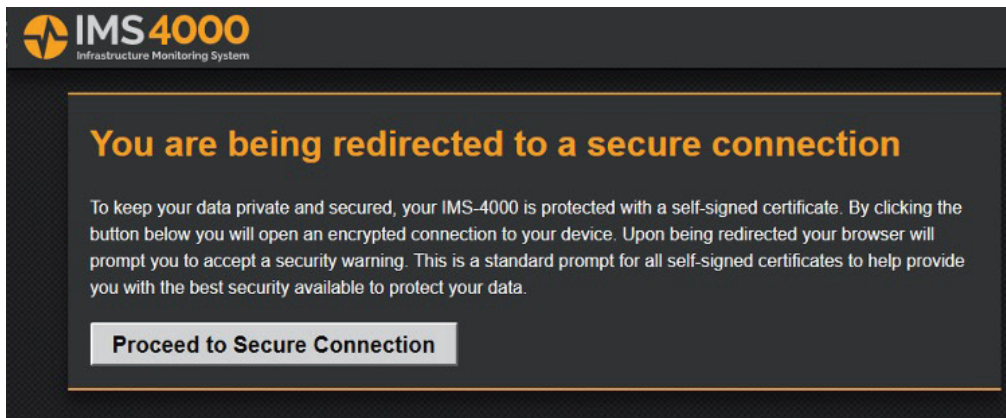
Your browser will then present a security warning, click 'Advanced' or 'Accept the Risk', and then 'Proceed', 'Accept' or 'Continue' to open the login page. These warnings will be eliminated and a secure connection established once you generate and install the security certificate. See 'Using a Security Certificate…' later in this chapter.
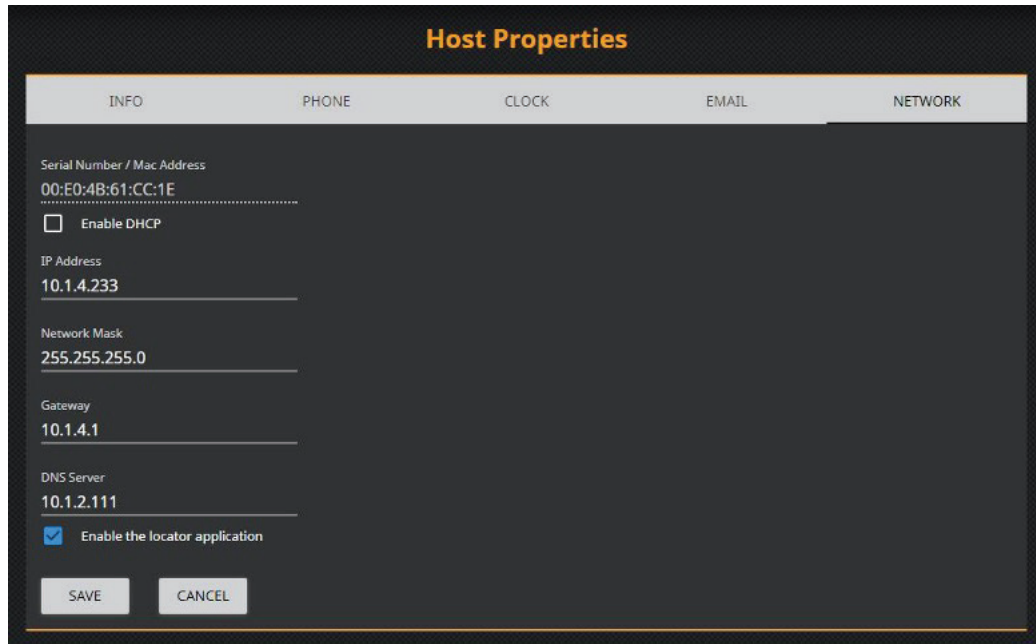
At the login page, enter your username and password (default login u: admin, p: ims4k).
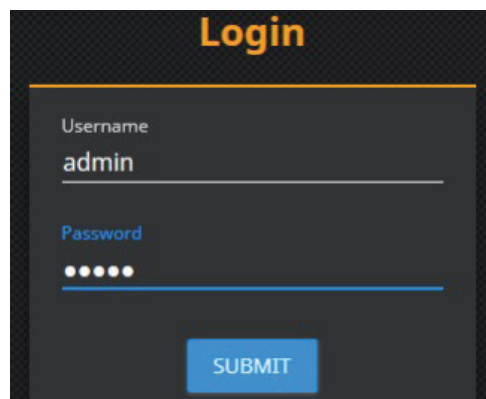
You should now be logged-in to the main page (e.g. the Overview page). The three dashed lines in the top left corner identify the menu button. Click the menu button to navigate to the other pages in the system.

NETWORK SETTINGS

To configure the network settings click the menu button in the top left corner and select 'Overview', then click the gear icon next to the host to open the Host Properties screen. To set a static IP, uncheck the DHCP box and enter the static IP settings for your network, then click 'Save'. Your device will reboot and now be accessible on the new IP address.

HOST PROPERTIES

On the screen above, select 'Info', to configure the Host's name, Location, and Description information. These names will be used on alarm messages to help identify the location of alarm conditions reported by the device. Select 'Phone' to configure parameters specific to the units call-in and call-out features. The 'Numeric ID' is the unit's telephone number. You can assign a custom voice message to identify your host during telephone calls using the 'Custom Voice' selection drop down. See 'Alarm Voice Files' later in this chapter for details on uploading your own voice files to the system.

OVERVIEW

Select 'Overview' from the main menu. This page provides a summary of alarms as well as navigation to the status pages for the Host and Nodes in your system. By clicking the Up/Down arrows for each device you can expand and contract the status page for each device (see below):

You can look at the details for each Environmental Sensor or IP Alarm by clicking the arrow next to each. If the sensor is configured for data logging a graph of the last 24 hours will also appear. See sample below:
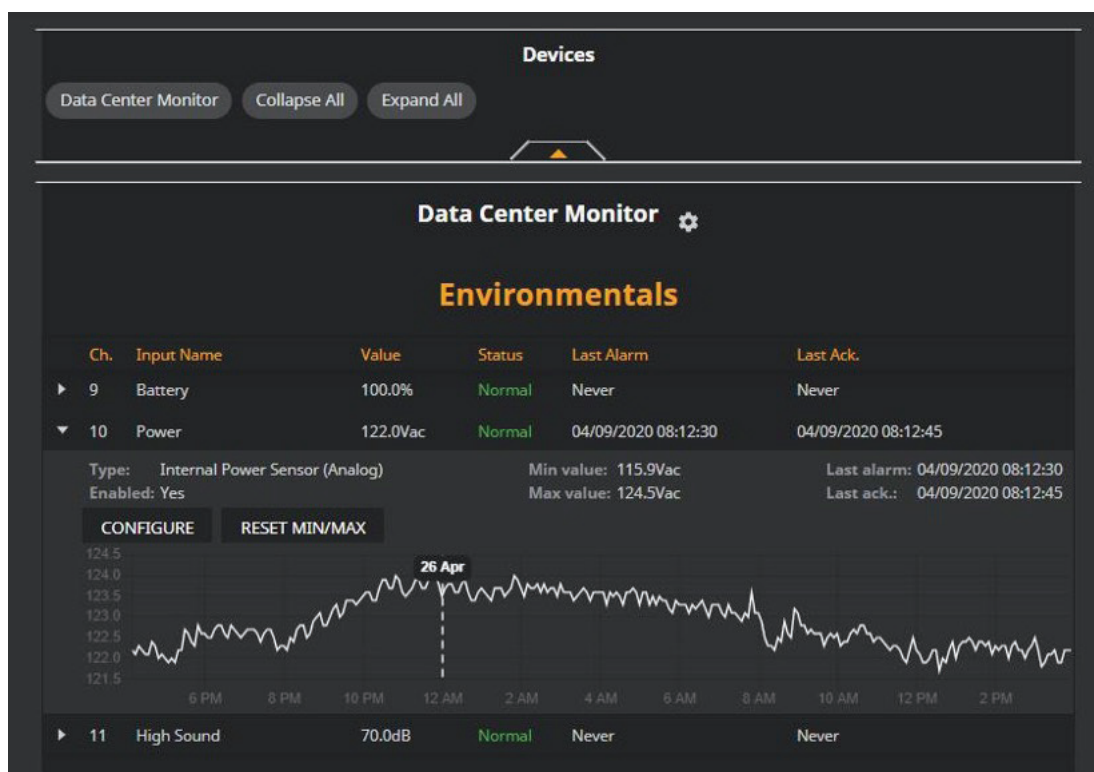
To configure sensor name, alarm limits, and other details click the 'Configure' button. The 'Alarm Response' tab allows you to have camera snapshots sent to an email address when an alarm occurs. One or more cameras must be configured in the system before an alarm response can be added. The 'Schedule' tab allows you to set a weekly schedule when the sensor is enabled or disabled.

EVENT AND DATA LOGS

The system keeps tracks of alarms and other system events in the Event Log. To view the Event Log select 'Logs' from the main menu. On this page you can query for events from a specific device or all devices, as well as the time frame and message type. You can also download the select events in CSV format by clicking the 'Download' button.

The system can also record Sensor values and IP Alarm status on a fixed interval. The recorded data can be viewed on the 'Environmental Data' tab on the Logs page. Use the 'Settings' button at the top of the page to enable the datalog feature and set the recording interval. To query the data select a device, sensor, and start and end times. You can also download the queried data in CSV format.

USER PROFILES

Every user of the system should have a User Profile. To configure or edit User Profiles select 'Profiles' from the main menu. To create a new profile click the 'Create New Profile' button. To edit an existing profile click the gear icon in the Edit column. User's can be configured as Master Administrator to have full access to all devices or they can have limited access to specific devices (e.g. User or Site permission). See chapter 2, Permissions for details. The edit screen is used to enter contact information (email, telephone numbers, etc…) to be notified of alarms. You can also configure your user code to acknowledge alarms during voice calls (see Settings).
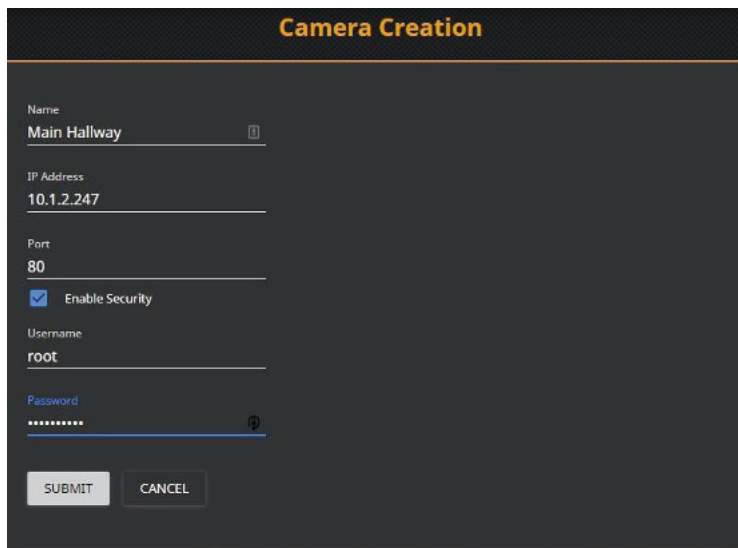
CLASSES

The IMS-4000E allows you to select which users receive which types of alarms. This assignment is configured in the 'Classes' section from the main menu. To see which Users are assigned to a particular sensor class, click the arrow next to the Class name. To assign Users to a particular Class, click the gear icon. The column on the left lists all available Users, the column on the right lists Users assigned to receive this alarm class. You can assign users one at a time by clicking the arrow next to the their name or you can assign all users by clicking the 'Add All' button. Click 'Submit' when done to save your changes.

ALARM VOICE FILES

You can have the IMS-4000E play a custom voice file to identify each host/node, sensor, and IP Alarm in the system when you call-in or when it dials out for an alarm. Voice messages must first be recorded on your computer and then uploaded to the IMS Host. Voice messages should be recorded in WAV or PCM format.. Name each file to match the content of the recorded message. Upload your files to the unit using the 'Alarm Voice Files' page from the main menu. You can click the 'Browse' button to locate files or you can drop files onto the 'Browse' button and they will automatically load into the system. Once your audio files are loaded you can assign them to sensors, IP Alarms, or devices on their respective Configuration or Unit Properties pages.

CAMERAS

The IMS4000 allows you to configure up to 128 network cameras that you can use to view live video or to attach snapshots to emails when alarms occur. The unit works with network cameras from Axis Communications. To configure a camera, select 'Cameras' from the main menu and click 'Add Camera'. Configure the camera settings - see sample below. To attach camera snapshots to emails use the 'Alarm Response' programming screen on the Sensor configure pages.
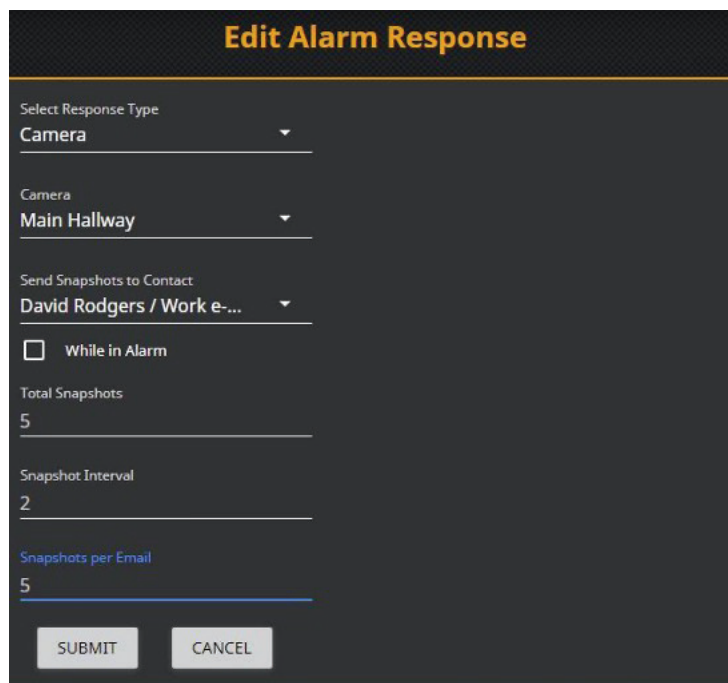
Alarm Response Programming example:

USING A SECURITY CERTIFICATE ON A PRIVATE NETWORK

The following steps describe how to establish a secure connection to the IMS-4000E webpage for devices installed on a private network. A security certificate will need to be installed on each computer that will be accessing the IMS-4000E if a secure connection is required.

1) Click the menu button and select 'Settings'.

2) Click 'Certificates' from the Settings menu.

3) If a certificate has already been generated with the device's current Domain Name or IP Address then don't create a new one. In this case continue to step 4. If you do need to create a certificate then click the button 'Regenerate Certificates', then click 'Okay' to generate a new certificate. The following form will appear. If you have assigned a domain name for your device then enter it in the 'Common Name' field, otherwise leave it at the default setting. You may change the other settings if needed or simply leave them at the default. Click 'Generate' when complete. You should receive an 'Update Successful' message after a minute or so. Click 'Okay'.

Common Name

IMS4000 Device Certificate

Organization

Sensaphone

Organizational Unit

Monitoring

Locality/City

Aston

State/Province

Pennsylvania

Country (ISO Code)

US

Email

.

Days Until Expiration

3650

Key Size

2048

Domain or IP Address

173.49.102.229   ADD ADDRESS

GENERATE   CANCEL

4) Click the 'Download Certificate for Client' button. Your browser may ask if you want to keep or save the file, select 'Yes', 'OK' or 'Keep'. Next, open the 'ims4000CA.crt' file you just downloaded. (If your browser added '.txt' to the end of the filename then rename the file to remove '.txt'). When you open the file Windows will pop up a security warning, click 'Open' or 'OK' to proceed. Next, click 'Install Certificate'. When you are prompted to select the 'Store Location' choose 'Local Machine' then click 'Next'. Windows will ask if you want the certificate location to be selected automatically, do not choose automatic, choose the option that allows you to browse (e.g. 'Place all certificates in the following store'). Click the 'Browse' button, select the folder titled 'Trusted Root Certification Authorities', then click 'OK', then 'Next', and then 'Finish'. Then click 'Yes' to install the certificate. Then click 'OK' to close the import wizard. Close any remaining windows.

5) Close your browser or tab, then re-open the device webpage using the format 'https://ip address. You should now be able to open the web page with no security warnings and a 'lock' symbol in your browser address bar.
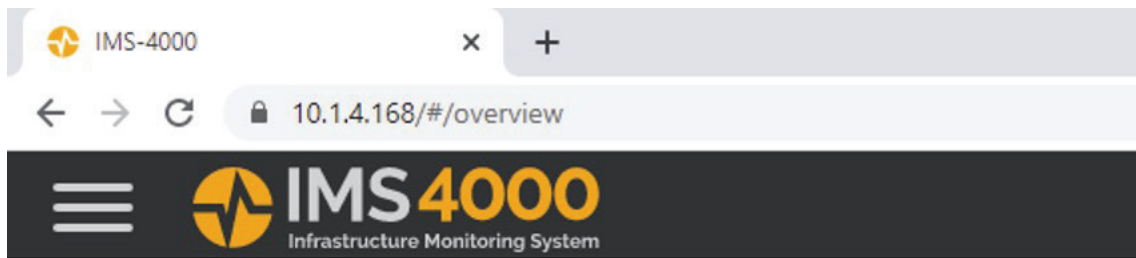
USING A SECURITY CERTIFICATE ON A PUBLIC NETWORK

If you will be using the IMS-4000E on a public network (e.g. the internet) then it would be wise to obtain and install a certificate from a Certificate Authority. The first step would be to obtain a domain name for your device. Once you have a domain name you can obtain a digital certificate and key. The certificate and key must then be installed on the IMS-4000E. Click the Menu button and go to 'Settings', then select the 'Certificates' tab. In the Public Certificate section, click the 'Upload' button and select the digital certificate for the device. Next, in the Private Key section, click the 'Upload' button and select the key file. Then click 'Apply Pending'. You should get an 'Update Successful' message. You will need to logout and restart your browser to have the secure connection take effect.
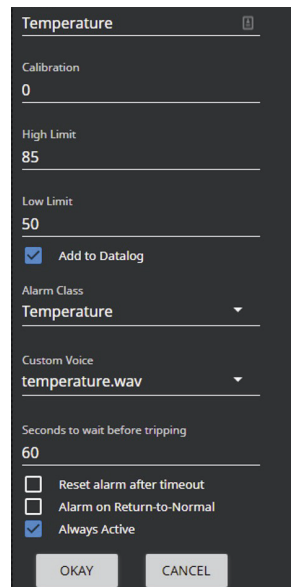
CONFIGURING HOLIDAYS

The IMS-4000E allows you to program recurring or non-recurring holidays that you can use within your schedule programming. These schedules are used to enable or disable monitoring of Environmental and IP Alarms, and also to enable or disable times when users will receive alarm calls. To see which holidays are currently programmed select Holidays from the main menu. If you click the arrow next to each holiday you will see the date assigned to the holiday and whether or not it's configured as a recurring holiday. You can Delete or Edit the holiday by clicking the gear icon. You can also add new holidays by clicking the Create New Holiday button.
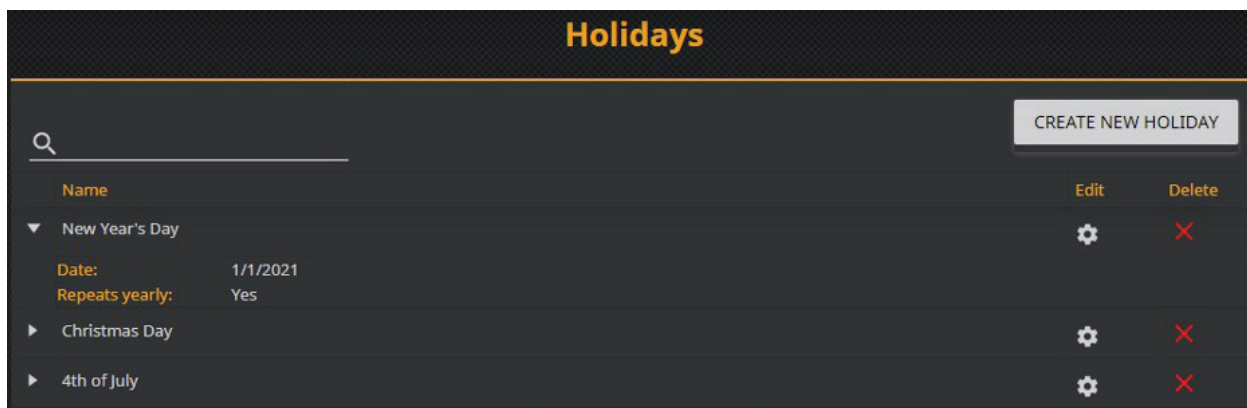
INPUT TEMPLATES

Environmental input programming Templates are used to load user-specified defaults each time a new sensor is connected to a Host or Node. By properly configuring the Templates before you plug in your sensors, you can minimize the amount of programming required to set up your sensors. To configure the Templates, select Input Templates from the main menu. Click the gear icon next to each sensor type to view or change the default settings for that sensor. See sample Template setup screen below:
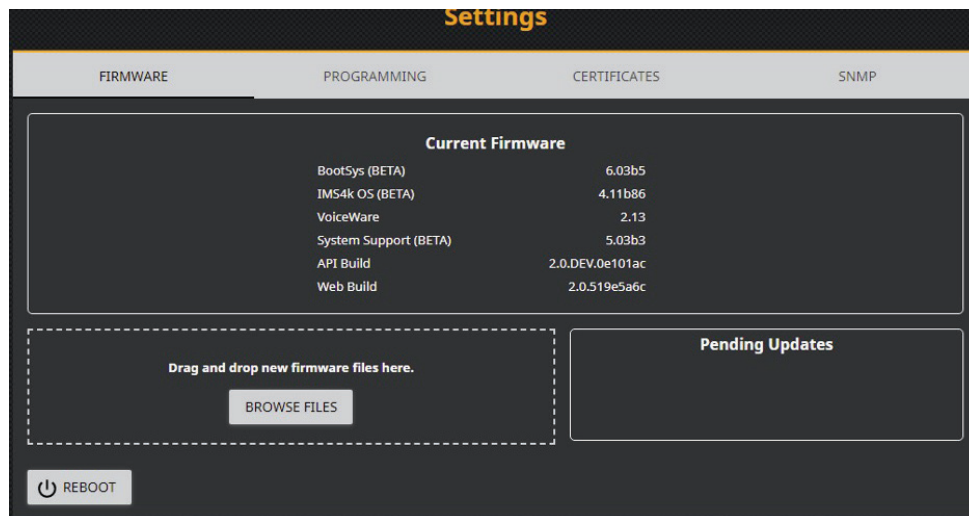
FIRMWARE UPDATES

From time to time Firmware updates will become available to add features or improve the performance of your IMS-4000E. Most Firmware updates will be included as part of a complete IMS-4000E installation upgrade. Check the IMS-4000E downloads page on Sensaphone.com (www.sensaphone.com/support-4000.html) for the latest information on updates. To check the versions of Firmware in your IMS-4000E, select Settings from the main menu. The Firmware versions will be listed in the 'Current Firmware' section. To update the firmware you can drag the new firmware files into the dashed area or just click the browse button and select the files to be installed. The firmware files will then be uploaded to the device. Once the files have been uploaded you can click 'Apply' and the device will install the files and reboot. You will need to login again on the main page after 1-2 minutes.

This screen also gives you the option of simply rebooting the device by clicking the 'Reboot' button at the bottom of the screen.

CHAPTER 5: SNMP

The IMS-4000E Host contains an SNMP agent that supports both SNMP V1 and V3. Through the use of a SNMP network management client, most of the IMS-4000E parameters can be read and written. The IMS-4000E can also send SNMP Traps to SNMP network management clients to indicate an alarm condition. A complete SNMP MIB file is available on the IMS-4000E CD.

Through the SNMP protocol, most of the programming parameters and status information can be accessed. The following is a summary of the IMS-4000E items that can be fully accessed through SNMP:

- Edit Environmental input programming
- Edit IP Alarm programming
- Edit System programming (unit info, e-mail setup, Web FTP setup, phone settings)
- Enable/Disable Datalogging
- Edit the Datalog interval
- Edit/add Classes
- Edit Environmental input template programming
- Edit Camera setup
- Acknowledge alarms
- View Network and Security configuration parameters
- View system diagnostic information

Some parameters of the IMS-4000E involve complex data structures and cannot be accessed through the SNMP protocol.

The following operations cannot be performed through SNMP:

- Add or delete IP alarms
- Add or delete Profiles or Contacts
- Delete a sensor
- Delete a Node
- Configure the system clock
- Modify time schedules
- Edit alarm response programming sequences
- Modify classes on Environmental Inputs, IP Alarms, or Profiles

SNMP can be configured through the "SNMP" and "SNMP Traps" tabs of the IMS-4000E Settings webpage. Additionally the SNMP settings can be configured locally over RS-232.

The IMS-4000E SNMP agent uses UDP port 161 for SNMP reading and writing of parameters. UDP port 162 is used by the IMS-4000E SNMP agent to send SNMP traps.

SNMP SETTINGS:

Enabled: Enables or disables the SNMP agent present in the IMS-4000E. If set to disabled, both read and write access is disabled.

SNMP Version: Specifies the version of SNMP the IMS-4000E SNMP agent will use. SNMP version 1 and version 3 are both supported.

SNMP Version 1 Specific Settings:

Read-Only Community String: Using this community string with your SNMP network management client will grant read-only (GET) access to the IMS-4000E SNMP agent. Write access (SET) is disabled.

Read-Write Community String: Using this community string with your SNMP network management client will grant read and write (GET and SET) access to the IMS-4000E SNMP agent.

SNMP Version 3 Specific Settings:

Read Only Username: Specifies the authorization user name for read only (GET) access. Using this user name in combination with the Read Only Auth Password will grant read-only access to the IMS-4000E SNMP agent.

Read Only Auth Password: Specifies the SNMP V3 authorization password for read-only (GET) access. Use this password with the read only user name to grant read-only access in the IMS-4000E agent. SHA is used by the IMS-4000E to authenticate with SNMP management clients.

Read Write Username: Specifies the authorization user name for read write (GET and SET) access. Using this user name in combination with the Read Write Auth Password will grant read write access to the IMS-4000E SNMP agent.

Read Write Auth Password: Specifies the SNMP V3 authorization password for read write (GET and SET) access. Use this password with the read write user name to grant read write access in the IMS-4000E agent. SHA is used by the IMS-4000E to authenticate with SNMP management clients.

SNMP Privacy: Set SNMP Privacy to enabled to enable AES-128 encryption of SNMP content. If SNMP Privacy is disabled the IMS-4000E SNMP agent will send and receive SNMP content unencrypted.

Read Only Privacy Password: If SNMP privacy is enabled, use this password with the read-only username to grant read only SNMP access with AES-128 encryption.

Read Write Privacy Password: If SNMP privacy is enabled, use this password in combination with the read-write username to grant read-write SNMP access with AES-128 encryption.

SNMP Trap Settings:

The section below describes the settings required to configure the IMS-4000E SNMP agent to successfully communicate with your SNMP network management client. Note that in order for the IMS-4000E SNMP agent to send traps in response to an alarm condition, the following must be configured:

•The IMS-4000E alarm agent must be configured to work with your network management client as described below.

•Your network management agent's IP address must be added as an SNMP contact in your IMS-4000E user profile. Refer to the Contacts section of Chapter 2 for more information.

•Your IMS-4000E profile must belong to a class assigned to the input for which a trap will be sent during an alarm condition. Refer to the Configuring User Profiles and Contacts section of Chapter 2 for more information.

SNMP Trap Version: Set to Version 1 to enable SNMP V1 traps. Set to Version 3 to enable SNMP V3 traps. V3 traps require additional configuration, shown below.

SNMP Trap Version 3 Specific Settings:

SNMP Trap Username: Specifies the SNMP authorization username the IMS-4000E SNMP agent will use to authenticate with your SNMP management software. The SHA authentication function is used by the IMS-4000E SNMP agent.

SNMP Trap Password: Specifies the SNMP authorization password the IMS-4000E SNMP agent will use to authenticate with your SNMP network management client.

SNMP Privacy: Set to Enabled to enable AES-128 encryption of trap content sent by the IMS-4000E SNMP agent. If disabled the content of a trap sent by the IMS-4000E SNMP agent will be unencrypted.

SNMP Privacy Password: Specifies the SNMP privacy password the IMS-4000E SNMP agent will use to authenticate itself with your SNMP management client's encryption engine.

Engine ID: This field indicates the IMS-4000E's SNMP agent engine ID. Configure your SNMP network management client to use this engine ID when receiving traps from an IMS-4000E. The engine ID matches the IMS-4000E's MAC address and is not configurable.

CHAPTER 6: IMS-4000E SENSORS

IMS-4810E ROOM TEMPERATURE SENSOR

Introduction

The IMS-4810E temperature sensor is designed to connect to the IMS-4000E Host or Node and monitor indoor temperatures. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or to a single-gang electrical box.

Package Contents

(1) IMS-4810E Temperature sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(1) 1⁄16" hex key

Cabling

The temperature sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor can be mounted directly on a surface or attached to a single-gang electrical box. Consideration should be given to cable routing before attaching the sensor to the wall. Will the cable go through the wall (cable hidden) or will it run down the wall (cable visible)? Once this has been determined, run the cable to the location where the sensor will be installed.

Electrical box installation

Bring the RJ-45 cable through the electrical box. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and connect the cable to the jack as shown in Figure 1. Attach the sensor to the electrical box using the appropriate screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
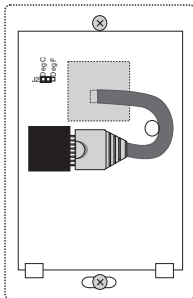

Figure 1: 4810E with Cable exiting through back of enclosure

Hidden cable surface installation

Bring the RJ-45 cable through the wall at the mounting location. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Remove the sensor from the wall. Install the drywall anchors (if necessary) to the wall. Bring the cable through the back of the sensor and connect it to the jack as shown in Figure 1. Attach the sensor to the wall using #6 tapping screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Visible cable surface installation

Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Install the drywall anchors (if necessary) to the wall. Attach the sensor to the wall using #6 tapping screws. Connect the cable to the jack as shown in Figure 2. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Figure 2: 4810E with Cable exiting out enclosure bottom

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

> **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Fahrenheit/Celsius Selection

The IMS-4810E can provide temperature readings in either degrees Fahrenheit or Celsius. To select one or the other, remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Locate the black jumper (see Figure 3) marked J2. Install the jumper in the "Deg F" position for Fahrenheit or the "Deg C" position for Celsius. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
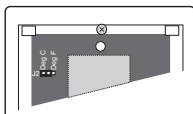
Figure 3: Jumper location (set for Degrees Celsius)

Sensor Template (factory default)		Specifications	
Input Name:	Temperature	Range:	5° to 122°F (-15° to 50°C)
Low Temperature Limit:	50ºF	Humidity:	5–90 %RH
High Temperature Limit:	85ºF	Sensor type:	solid state ic
Recognition Time:	60 Seconds	Accuracy:	+/- 3°F
Reset Time:	0 Seconds	Connector:	RJ-45
Data Logging:	Active	Housing:	white plastic
Voice:	temperature.wav		
Input Class:	Temperature		

IMS-4811E ROOM TEMPERATURE SENSOR W/ DISPLAY ˚F

Introduction

The IMS-4811E temperature sensor is designed to connect to the IMS-4000E Host or Node and monitor indoor temperatures. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or to a single-gang electrical box.

Package Contents

(1) IMS-4811E Temperature sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(1) 1⁄16" hex key

Cabling

The temperature sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor can be mounted directly on a surface or attached to a single-gang electrical box. Consideration should be given to cable routing before attaching the sensor to the wall. Will the cable go through the wall (cable hidden) or will it run down the wall (cable visible)? Once this has been determined, run the cable to the location where the sensor will be installed.

Electrical box installation

Bring the RJ-45 cable through the electrical box. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and connect the cable to the jack as shown in Figure 1. Attach the sensor to the electrical box using the appropriate screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Figure 1: 4811 with Cable exiting through back of enclosure
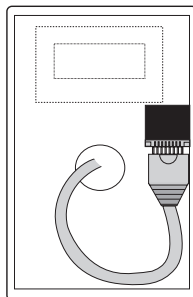
Hidden cable surface installation

Bring the RJ-45 cable through the wall at the mounting location. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Remove the sensor from the wall. Install the drywall anchors (if necessary) to the wall. Bring the cable through the back of the sensor and connect it to the jack as shown in Figure 1. Attach the sensor to the wall using #6 tapping screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Visible cable surface installation

Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Install the drywall anchors (if necessary) to the wall. Attach the sensor to the wall using #6 tapping screws. Connect the cable to the jack as shown in Figure 2. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Figure 2: 4811 with Cable exiting out enclosure bottom

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Temperature	Range:	32° to 95°F
Low Temperature Limit:	50°F	Humidity:	5–90 %RH
High Temperature Limit:	85°F	Sensor type:	solid state ic
Recognition Time:	60 Seconds	Accuracy:	+/- 3 degrees F
Reset Time:	0 Seconds	Connector:	RJ-45
Data Logging:	Active	Housing:	white plastic
Voice:	temperature.wav		
Input Class:	Temperature		

IMS-4812E MINI TEMPERATURE SENSOR

Introduction

The IMS-4812E Mini Temperature Sensor is designed to connect to the IMS-4000E Host or Node and monitor temperatures in tight locations (for example, inside equipment racks). The electrical connection between the sensor and IMS-4000E is made via the attached RJ-45 patch cable. The sensor may be secured inside equipment using double-sided tape (included) or with tie-wraps.

Cabling

The Mini-Temperature Sensor comes with an attached 7' cable with an RJ-45 plug on the end. If the sensor is close to the IMS-4000E Host or Node, you can plug the sensor directly to an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

> **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor may be mounted directly on a surface using double-sided tape (included) or it may be secured to equipment using tie-wraps. The choice depends on your application.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

> **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Temperature	**Range:**	5° to 140°F
Low Temperature Limit:	50°F	**Humidity:**	5–90% RH
High Temperature Limit:	85°F	**Sensor type:**	solid state ic
Recognition Time:	60 Seconds	**Accuracy:**	+/- 3 degrees F
Reset Time:	0 Seconds	**Connector:**	7' cable w/RJ-45 plug
Data Logging:	Active	**Housing:**	black plastic
Voice:	temperature.wav	**Housing dimensions:**	2.13" l x 0.6" d x 1.38" h
Input Class:	Temperature		

IMS-4813E ROOM TEMPERATURE SENSOR W/ DISPLAY ˚C

Introduction

The IMS-4813E temperature sensor is designed to connect to the IMS-4000E Host or Node and monitor indoor temperatures. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or to a single-gang electrical box.

Package Contents

(1) IMS-4813E Temperature sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(1) 1/16" hex key

Cabling

The IMS-4813E temperature sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

> ⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor can be mounted directly on a surface or attached to a single-gang electrical box. Consideration should be given to cable routing before attaching the sensor to the wall. Will the cable go through the wall (cable hidden) or will it run down the wall (cable visible)? Once this has been determined, run the cable to the location where the sensor will be installed.

Electrical box installation

Bring the RJ-45 cable through the electrical box. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and connect the cable to the jack as shown in Figure 1. Attach the sensor to the electrical box using the appropriate screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
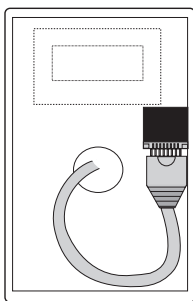

Figure 1: 4813 with Cable exiting through back of enclosure

Hidden cable surface installation

Bring the RJ-45 cable through the wall at the mounting location. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Remove the sensor from the wall. Install the drywall anchors (if necessary) to the wall. Bring the cable through the back of the sensor and connect it to the jack as shown in Figure 1. Attach the sensor to the wall using #6 tapping screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Visible cable surface installation

Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Install the drywall anchors (if necessary) to the wall. Attach the sensor to the wall using #6 tapping screws. Connect the cable to the jack as shown in Figure 2. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
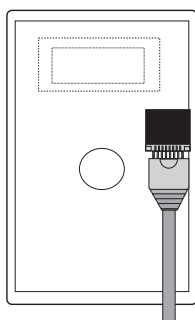
Figure 2: 4813 with Cable exiting out enclosure bottom

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Temperature	Range:	0° to 35°C
Low Temperature Limit:	10º C	Humidity:	5–90 %RH
High Temperature Limit:	27º C	Sensor type:	solid state ic
Recognition Time:	60 Seconds	Accuracy:	+/- 1.7 degrees C
Reset Time:	0 Seconds	Connector:	RJ-45
Data Logging:	Active	Housing:	white plastic
Voice:	temperature.wav		
Input Class:	Temperature		

IMS-4814E ULTRA LOW TEMPERATURE SENSOR

Introduction

The IMS-4814E Ultra Low Temperature Sensor is designed to connect to the IMS-4000E Host or Node and monitor temperatures in refrigerators or freezers. The electrical connection between the sensor and IMS-4000E is made via the attached RJ-45 patch cable. The sensor probe may be secured inside equipment using the included clamp or it may be hung using tie wraps. Do not install the black plastic enclosure inside of a refrigerator or freezer.

Cabling

The Ultra Low Temperature Sensor comes with an attached 7' cable with an RJ-45 plug on the end and a weatherproof probe with 12' of cable. If the sensor installation is close to the IMS-4000E Host or Node, you can plug it directly into an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your struc-tured wiring patch panel directly to the Host or Node environment input.

Caution: The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor housing may be mounted directly on a surface using double-sided tape (included) or it may be secured to equipment using tie-wraps. The choice depends on your application. The sensor probe must be installed in your refrigerator or freezer at a location that is representative of the average temperature. Do not install the probe directly in front of the cold air blower.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. The Ultra Low Temperature Sensor will identify itself as a 4-20mA transducer. On the Properties screen for this sensor you must select the sensor type: either Low Temperature (Deg F) or Low Temperature (Deg C). When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Host and Node Firmware Requirements

The Ultra Low Temperature Sensor requires the following firmware versions in the IMS-4000E Host and updated ConsoleView software for your computer for sensor compatibility:

IMS-4000E Host

• Input board firmware chip version xx.xx.xx.106 or higher

NOTE: Input board firmware is NOT flash upgradeable. A new firmware chip must be installed. For information on obtaining a new firmware chip, please contact Sensaphone Technical Support at 610.558.2700 or via e-mail at support@sensaphone.com.

• ConsoleView version 3.0.15 or higher

- IMS4K OS version 3.00 or higher

- Voice version 2.12 or higher

*Host version information is viewable through the ConsoleView software on the Version Info screen and the Help>About selection from the main menu.

IMS-4000E Node

- Firmware version 2.19 or higher (for 10Mbit/s nodes).

- All firmware versions (for 100Mbit/s nodes).

*Node version information is viewable through the ConsoleView software on the Node Properties>Diagnostics screen.

Sensor Template		Specifications	
Input Name:	Transducer	Temperature Range:	-122° to 53°F (-86 to 12°C)
High Limit:	100	Humidity:	5–90% RH
Low Limit:	0	Sensor type:	sealed thermistor probe
Recognition Time:	3 Seconds	Accuracy:	+/- 3°F
Reset Time:	0 Seconds	Connector:	7' cable w/RJ-45 plug
Data Logging:	Active	Housing:	black plastic
Voice:	None	Housing dimensions:	2.13" l x 0.6" d x 1.38" h
Input Class:	Other	Weight:	3 oz (85 grams)

IMS-4815E ULTRA LOW TEMPERATURE SENSOR IN GLASS BEAD VIAL

Introduction

The IMS-4815E Temperature Sensor is designed to connect to the IMS-4000E Host or Node and monitor temperatures in refrigerators or freezers. The electrical connection between the sensor and IMS-4000E is made via the attached RJ-45 patch cable. The bottle should be secured inside equipment in a central location. Do not install the black plastic enclosure inside of a refrigerator or freezer.

Cabling

The Temperature Sensor comes with an attached 7' cable with an RJ-45 plug on the end and a weatherproof probe with 12' of cable. If the sensor installation is close to the IMS-4000E Host or Node, you can plug it directly into an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor housing may be mounted directly on a surface using double-sided tape (included) or it may be secured to equipment using tie-wraps. The choice depends on your application. The bottle must be installed in your refrigerator or freezer at a location that is representative of the average temperature. Do not install the bottle directly in front of the cold air blower.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. The Temperature Sensor will identify itself as a 4-20mA transducer. On the Properties screen for this sensor you must select the sensor type: either Low Temperature (Deg F) or Low Temperature (Deg C). When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Host and Node Firmware Requirements

The Temperature Sensor requires the following firmware versions in the IMS-4000E Host and updated ConsoleView software for your computer for sensor compatibility:

IMS-4000E Host

- Input board firmware chip version xx.xx.xx.106 or higher

   NOTE: Input board firmware is NOT flash upgradeable. A new firmware chip must be installed. For information on obtaining a new firmware chip, please contact Sensaphone Technical Support at 610.558.2700 or via e-mail at support@sensaphone.com.

- ConsoleView version 3.0.15 or higher

- IMS4K OS version 3.00 or higher

- Voice version 2.12 or higher

*Host version information is viewable through the ConsoleView software on the Version Info screen and the Help>About selection from the main menu.

IMS-4000E Node

- Firmware version 2.19 or higher (for 10Mbit/s nodes).

- All firmware versions (for 100Mbit/s nodes).

*Node version information is viewable through the ConsoleView software on the Node Properties>Diagnostics screen.

Sensor Template		Specifications	
Input Name:	Transducer	Temperature Range:	-122° to 53°F (-86 to 12°C)
High Limit:	100	Humidity:	5–90% RH
Low Limit:	0	Sensor type:	sealed thermistor probe
Recognition Time:	3 Seconds	Accuracy:	+/- 3°F
Reset Time:	0 Seconds	Connector:	7' cable w/RJ-45 plug
Data Logging:	Active	Housing:	HDPE plastic bottle
Voice:	None	Housing dimensions:	3.0" h x 1.6" d
Input Class:	Other		
Weight:	3 oz (85 grams)		

IMS-4816E TEMPERATURE SENSOR W/ EXTERNAL PROBE

Introduction

The IMS-4816E External Probe Temperature Sensor is designed to connect to the IMS-4000E Host or Node and monitor temperatures in difficult environments or in areas where a traditional sensor won't fit. The electrical connection between the sensor and IMS-4000E is made via the attached RJ-45 patch cable. The sensor probe may be secured inside equipment using the included clamp or it may be hung using tie wraps. Do not install the black plastic enclosure inside of a refrigerator, freezer or corrosive environment.

Cabling

The External Probe Temperature Sensor comes with an attached 7' cable with an RJ-45 plug on the end and a weatherproof probe with 12' of cable. If the sensor installation is close to the IMS-4000E Host or Node, you can plug it directly into an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

> **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The temperature sensor housing may be mounted directly on a surface using double-sided tape (included) or it may be secured to equipment using tie-wraps. The choice depends on your application. The sensor probe must be installed at a location that is representative of the average temperature.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. The External Probe Temperature Sensor will identify itself as a 4-20mA transducer. On the Properties screen for this sensor you must select the sensor type: Ext. Temp Probe (°F) or (°C). When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

> **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Host and Node Firmware Requirements

The External Probe Temperature Sensor requires the following firmware versions in the IMS-4000E Host and updated ConsoleView software for your computer for sensor compatibility:

IMS-4000E Host

- Input board firmware chip version xx.xx.xx.106 or higher

    NOTE: Input board firmware is NOT flash upgradeable. A new firmware chip must be installed. For information on obtaining a new firmware chip, please contact Sensaphone Technical Support at 610.558.2700 or via e-mail at support@sensaphone.com.

- ConsoleView version 3.0.22 or higher

- IMS4K OS version 3.13 or higher

- Voice version 2.12 or higher

*Host version information is viewable through the ConsoleView software on the Version Info screen and the Help>About selection from the main menu.

IMS-4000E Node

- Firmware version 2.59 or higher (for 10Mbit/s nodes).

- All firmware versions (for 100Mbit/s nodes).

*Node version information is viewable through the ConsoleView software on the Node Properties>Diagnostics screen.

Sensor Template		Specifications	
Input Name:	Transducer	**Temperature Range:**	32° to 176°F (0° to 80°C)
High Limit: 1	00	**Humidity:**	5–90% RH
Low Limit:	0	**Sensor type:**	sealed thermistor probe
Recognition Time:	3 Seconds	**Accuracy:**	+/- 3°F
Reset Time:	0 Seconds	**Connector:**	7' cable w/RJ-45 plug
Data Logging:	Active	**Housing:**	black plastic
Voice:	None	**Housing dimensions:**	2.13" l x 0.6" d x 1.38" h
Input Class:	Other		

IMS-4820E ROOM HUMIDITY SENSOR

Introduction

The IMS-4820E humidity sensor is designed to connect to the IMS-4000E Host or Node and monitor indoor humidity levels. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or to a single-gang electrical box.

Package Contents

(1) IMS-4820E Humidity sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(1) 1/16" hex key

Cabling

The humidity sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The humidity sensor can be mounted directly on a surface or attached to a single-gang electrical box. Consideration should be given to cable routing before attaching the sensor to the wall. Will the cable go through the wall (cable hidden) or will it run down the wall (cable visible)? Once this has been determined, run the cable to the location where the sensor will be installed.

Electrical box installation

Bring the RJ-45 cable through the electrical box. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and connect the cable to the jack as shown in Figure 1. Attach the sensor to the electrical box using the appropriate screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
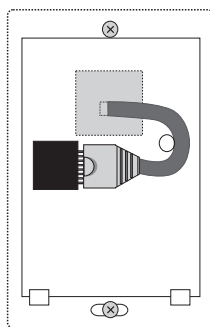

Figure 1: 4820 with Cable exiting through back of enclosure

Hidden cable surface installation

Bring the RJ-45 cable through the wall at the mounting location. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Remove the sensor from the wall. Install the drywall anchors (if necessary) to the wall. Bring the cable through the back of the sensor and connect it to the jack as shown in Figure 1. Attach the sensor to the wall using #6 tapping screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Visible cable surface installation

Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Install the drywall anchors (if necessary) to the wall. Attach the sensor to the wall using #6 tapping screws. Connect the cable to the jack as shown in Figure 2. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Figure 2: 4820E with Cable exiting out enclosure bottom

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Humidity	**Range:**	0–100% RH
Low Limit:	20%	**Temperature:**	32 to 122ºF (0 to 50ºC)
High Limit:	60%	**Accuracy:**	+/- 5%
Recognition Time:	60 Seconds	**Connector:**	RJ-45
Reset Time:	0 Seconds	**Housing:**	white plastic
Data Logging:	Active		
Voice:	humidity.wav		
Input Class:	Humidity		

IMS-4821E ROOM HUMIDITY SENSOR W/ DISPLAY

Installation Instructions

Introduction

The IMS-4821E humidity sensor is designed to connect to the IMS-4000E Host or Node and monitor indoor humidity. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or to a single-gang electrical box.

Package Contents

(1) IMS-4821E Humidity sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(1) 1/16" hex key

Cabling

The humidity sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The humidity sensor can be mounted directly on a surface or attached to a single-gang electrical box. Consideration should be given to cable routing before attaching the sensor to the wall. Will the cable go through the wall (cable hidden) or will it run down the wall (cable visible)? Once this has been determined, run the cable to the location where the sensor will be installed.

Electrical box installation

Bring the RJ-45 cable through the electrical box. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and connect the cable to the jack as shown in Figure 1. Attach the sensor to the electrical box using the appropriate screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.
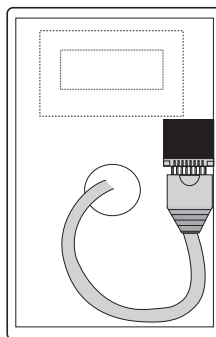

Figure 1: 4821 with Cable exiting through back of enclosure

Hidden cable surface installation

Bring the RJ-45 cable through the wall at the mounting location. Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Bring the cable through the back of the sensor and hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Remove the sensor from the wall. Install the drywall anchors (if necessary) to the wall. Bring the cable through the back of the sensor and connect it to the jack as shown in Figure 1. Attach the sensor to the wall using #6 tapping screws. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Visible cable surface installation

Remove the sensor cover by turning the two hex screws on the bottom of the sensor housing clockwise. Hold the sensor housing against the wall. Use a pencil to mark the hole locations at the top and bottom of the housing. Install the drywall anchors (if necessary) to the wall. Attach the sensor to the wall using #6 tapping screws. Connect the cable to the jack as shown in Figure 2. Secure the sensor cover by turning the two hex screws on the bottom of the cover counterclockwise.

Figure 2: 4821 with Cable exiting out enclosure bottom

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Humidity	**Range:**	5–95%
Low Limit:	20%	**Temperature:**	32° to 158ºF (0° to 70ºC)
High Limit:	60%	**Accuracy:**	+/- 3%
Recognition Time:	60 Seconds	**Connector:**	RJ-45
Reset Time:	0 Seconds	**Housing:**	white plastic
Data Logging:	Active		
Voice:	humidity.wav		
Input Class:	Humidity		

IMS-4830E ZONE WATER DETECTION SENSOR

Introduction

The IMS-4830E Zone Water Detection Sensor protects your server and equipment from damaging water leaks from malfunctioning HVAC systems, cafeteria accidents, or any general plumbing failures in your facilities. The IMS-4830E is powered directly by the IMS-4000E unit.

After mounting the sensor, attach the included WaterRope, and simply lay its orange cable around your equipment: place it on the floor or beneath a raised floor; inside a drop-ceiling or in the rafters between floors; or anywhere you must know about water near your equipment.

You can attach additional Water Detection sensors to each other to expand your water leak detection capabilities throughout your facility; alternatively, IMS WaterRopes are designed to plug into each other to widen your perimeter for any individual sensor.

Package Contents

(1) IMS-4830E Water Detection Sensor

(1) 10' of WaterRope

(5) Adhesive cable clamps

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(4) Rubber feet

Cabling

The water detection sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Extending the WaterRope

You can extend the monitored area by attaching additional pieces of WaterRope. Simply connect the new WaterRope to the end of the first. You can have up to ten (10) pieces of WaterRope (100') connected together from one Water Detection Sensor.

Cascading Water Sensors

You can cascade up to three Water Detection Sensors from a single IMS input channel. This is useful if there is a large distance between each sensor and you don't want to use up additional IMS inputs for individual sensors. Simply connect an RJ-45 cable to the Next Sensor jack on the first sensor to the IMS jack of the second sensor. See Figure below.
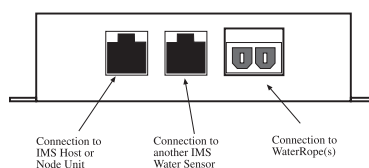

Figure 1: Sensor connections

115

Mounting

The sensor can be mounted to a wall or lie flat on the floor. To maximize the coverage of the WaterRope, install the sensor close to the area to be monitored. For wall mounting, install the Water Detection Sensor close to the floor. Install the two drywall anchors (if necessary) and attach the Water Detection Sensor using the two #6 tapping screws. When installing the sensor on the floor, attach the four rubber feet to the bottom of the enclosure.
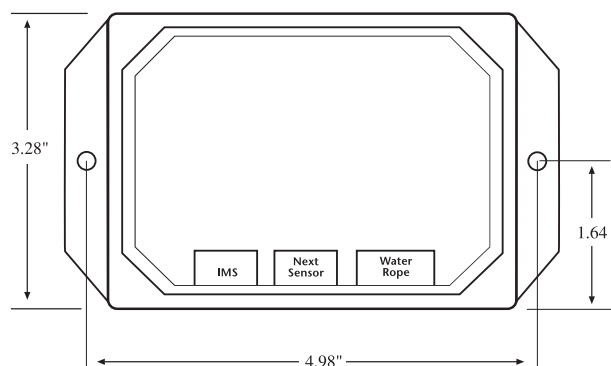

Figure 2: Mounting the sensor

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the config- uration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Water Sensor	Sensing Method:	Conductivity
Recognition Time:	3 Seconds	Sensor:	Polymer core cable with 2 sensing wires
Reset Time:	0 Seconds		
Data Logging:	Active	IMS Connection:	RJ-45
Voice:	water sensor.wav	Housing:	black plastic with mounting ears
Input Class:	Water		

IMS-4840E EXTERNAL POWER FAILURE SENSOR

Introduction

The IMS-4840E External Power Sensor lets you monitor power anywhere within your infrastructure. It reports any loss of power and measures the current voltage in the circuit, allowing you to know the status of each server rack and even of your remote UPS. Any failed generator starts are reported to you immediately. The IMS-4840E can monitor voltage from 0–250VAC 50/60Hz.

Package Contents

(1) IMS-4840E Power Sensor

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(4) Rubber feet

Cabling

The Power Sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠ Caution: The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Connection to
IMS Host or
Node Unit

Power Cord
Connection

Figure 1: Connections to the IMS-4840E

Mounting

The sensor can be mounted to a wall or lie flat on the floor. To mount the sensor to a wall, install the two drywall anchors (if necessary) and attach the Power Sensor using the two #6 tapping screws. When installing the sensor on the floor, attach the four rubber feet to the bottom of the enclosure.
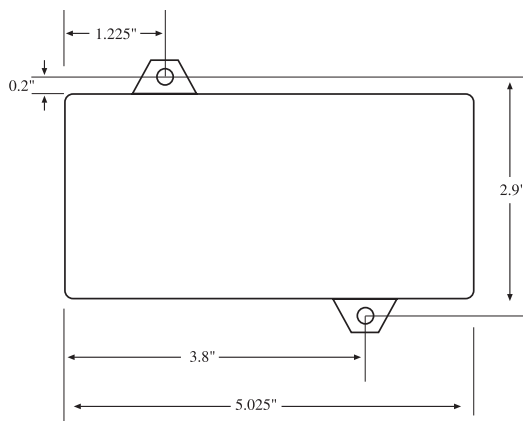
1.225"

0.2"

2.9"

3.8"

5.025"

Figure 2: Mounting the sensor

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Power	Range:	0–250 VAC, 50/60 Hz
Low Limit:	90VAC	Accuracy:	± 2%
High Limit:	130VAC	Power Connection:	universal IEC-320 power inlet
Recognition Time:	60 Seconds	IMS Connection:	RJ-45
Reset Time:	0 Seconds	Housing:	Black plastic with mounting ears
Data Logging:	Active		
Voice:	power default.wav		
Input Class:	Power		

IMS-4850E DRY CONTACT BRIDGE

Introduction

The IMS-4000E Dry Contact Bridge allows you to connect a dry contact alarm from any device to your IMS-4000E Host or Node. The Dry Contact Bridge is compatible with Normally Open and Normally Closed contacts. The electrical connection between the sensor and IMS-4000E is made via RJ-45 patch cable (not included). The sensor may be mounted either on a wall or rest on the floor.

Package Contents

(1) IMS-4850E Dry Contact Bridge

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(4) Rubber feet

Wiring the Contact

Connect your alarm contact to the terminal block labeled Input. Insert 1/2" stripped bare wire into the slot and tighten the screw. The slide switch selects between Normally Open (NO) and Normally Closed NC) dry contacts. Place the switch in the appropriate position for the alarm contact you are monitoring.
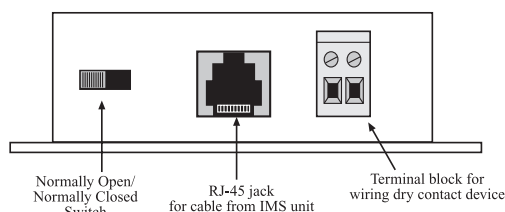
Figure 1: Connections to the IMS-4850E

Cabling

The Dry Contact Bridge connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the bridge to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

> ⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The Dry Contact Bridge can be mounted to a wall or lie flat on the floor. To mount it to a wall, install the two drywall anchors (if necessary) and attach the bridge using the two #6 tapping screws. When installing the sensor on the floor, attach the four rubber feet to the bottom of the enclosure.
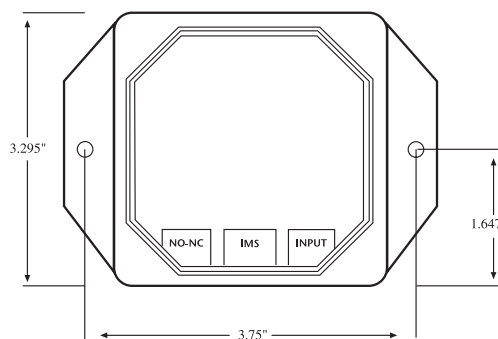

Figure 2: Mounting the sensor

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Contact Bridge	Input:	Normally Open or Normally Closed dry contact
Recognition Time:	3 Seconds	Source/Sense Voltage:	14VDC
Reset Time:	0 Seconds	Source/Sense Current:	10mA
Data Logging:	Active	IMS Connection:	RJ-45
Voice:	dry contact.wav	Operating Temperature Range:	32° to 122°F (0° to 50°C)
Input Class:	Other	Housing:	Black plastic with mounting ears

IMS-4851E 4–20MA BRIDGE

Introduction

The IMS-4000E 4–20mA Bridge allows you to connect a 4–20mA transducer to your IMS-4000E Host or Node. The 4–20mA Bridge features optical isolation between the input and the IMS-4000E, which ensures trouble-free operation and safety. The electrical connection between the bridge and IMS-4000 is made via RJ-45 patch cable (not included). The bridge may be mounted either on a wall or rest on the floor.

Package Contents

(1) IMS-4851E 4–20mA Bridge

(2) Plastic drywall anchors

(2) #6 Metal tapping screws

(4) Rubber feet

Wiring the Transducer

Connect your 4-20mA transducer to the terminal block labeled Input as shown in the figure below. Insert 1/2" stripped bare wire into the slot and tighten the screw. The Current Flow light will glow steadily when current is flowing into the bridge from the transducer. Note that a 4-20mA transducer typically requires you to have an external DC power supply for the transducer. A 24VDC supply is available from Sensaphone (FGD-0053).
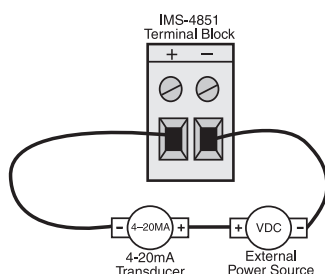
Figure 1: 4–20mA transducer wiring to IMS-4851E Terminal Block

Cabling

The 4-20mA Bridge connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the bridge may be installed in another room or another floor. Connect the bridge to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.
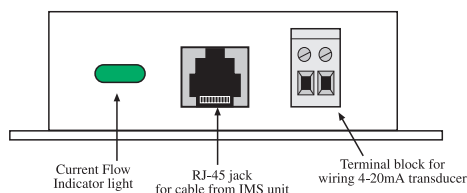
Figure 2: Connections to the IMS-4851E

Caution: The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The 4-20mA Bridge can be mounted to a wall or lie flat on the floor. To mount it to a wall, install the two drywall anchors (if necessary) and attach the bridge using the two #6 tapping screws. When installing the sensor on the floor, attach the four rubber feet to the bottom of the enclosure.
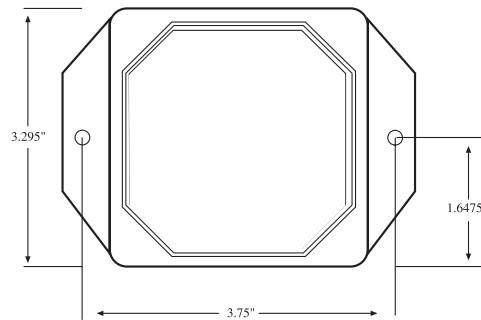

Figure 3: Mounting the sensor

Configuration

The 4-20mA Bridge can display a scaled value to match the calibrated range of your transducer. You must have updated versions of ConsoleView software (v3.0.15) and IMS4k firmware (v3.00) to get this feature. In the ConsoleView Software open the Channel Properties screen and click the SubType drop down menu, then choose Custom Table Limits. Insert the Low (4mA) and High (20mA) values for your transducer into the Table Low and Table High fields. The IMS-4000E will display the scaled value. You may wish to include the units of measure in the Channel Name field.

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sen¬sor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Host and Node Firmware Requirements

The 4-20mA Bridge requires the following firmware versions in the Host and Node(s) for sensor compatibility:

IMS-4000E Host

- Input board firmware chip version xx.xx.xx.103 or higher

   NOTE: Input board firmware is NOT flash upgradeable. A new firmware chip must be installed. For information on obtaining a new firmware chip, please contact Sensaphone Technical Support at 610.558.2700 or via e-mail at support@sensaphone.com.

- ConsoleView version 2.04 or higher

- IMS4K OS version 2.41 or higher

- Voice version 2.09 or higher

*Host version information is viewable through the ConsoleView software on the Version Info screen and the Help>About selection from the main menu.

IMS-4000E Node

- Firmware version 2.19 or higher.

*Node version information is viewable through the ConsoleView software on the Node Properties>Diagnostics screen.

Sensor Template (factory default)		Specifications	
Input Name:	Transducer	Input:	4–20mA DC
Recognition Time:	3 Seconds	Current Limit:	50mA
Reset Time:	0 Seconds	Input Impedance:	Variable (1000W @ 4mA, 260W @ 20mA)
Data Logging:	Active	Accuracy:	± 0.25%
Voice:	None	IMS Connection:	RJ-45
Input Class:	Other	Operating Temperature Range:	32° to 122°F (0° to 50°C)
		Housing:	Black plastic with mounting ears

IMS-4860E MAGNETIC REED DOOR AND WINDOW SWITCH

Introduction

The IMS-4000E Door Switch with bridge enables your IMS-4000E to detect if any unauthorized entry or intrusion has occurred. The bridge may be mounted either on a wall or rest on the floor. The switch is mounted to doors or windows you wish to monitor. The electrical connection between the bridge and IMS-4000E is made via RJ-45 patch cable.

Package Contents

(1) Door Switch with mounting hardware

(1) IMS-4860E bridge

(1) 25' accessory wire

Mounting the Door Switch

The door switch is usually installed to function in a normally closed position when the door (or window or other portal) on which it is mounted is closed. The complete assembly is of two parts: a magnet in a plastic housing, and a sensor switch with screw terminals in another plastic housing.

Mount the switch by fastening it to the non-moving frame surrounding the door or window. Use either mounting screws or the adhesive foam tape attached to the switch segments. Fasten the magnet near the edge of the movable sash or door. Position the magnet housing no more than 1/8" from the switch and tighten mounting screws. Use the spacer bar (included) if needed for alignment.
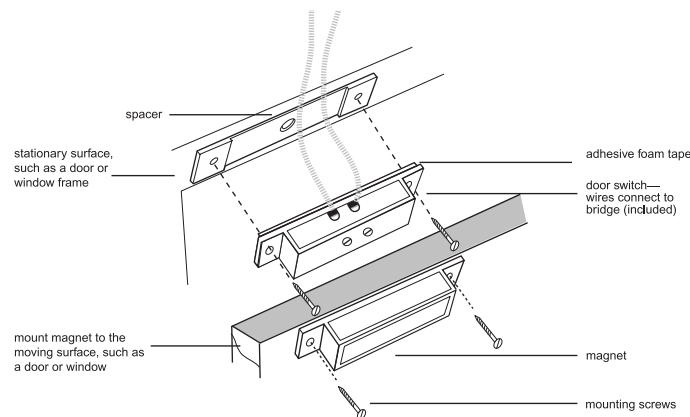
Figure 1: Door switch mounting

Mounting the Bridge

The bridge may be mounted directly on a surface using double-sided foam tape (included) or it may be secured to equipment using tie-wraps. The choice depends on your specific application.

Cabling

The Door Switch connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable) from the bridge. The connection from the bridge to Host or Node can utilize your existing network wiring infrastructure. For example, the switch may be installed in another room or another floor. Connect the bridge to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

Caution: IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)	
Input Name:	Contact Bridge
Recognition Time:	3 Seconds
Reset Time:	0 Seconds
Data Logging:	Active
Voice:	dry contact.wav
Input Class:	Other

Specifications	
Bridge:	
Input:	Normally Open or Normally Closed dry contact
Source/Sense Voltage:	14VDC
Source/Sense Current:	10mA
Cable/Connector:	7' cable with RJ-45 plug
Operating	
Temperature Range:	32° to 122°F (0° to 50°C)
Housing:	Black plastic
Dimensions:	2.13" x 0.6" x 1.38"
Door Switch	
Normality:	Normally Closed
Dimensions:	2.0" x 0.4" x 0.4" (with screw terminals)
Dimensions:	2.0" x 0.4" x 0.4" (part with magnet)

IMS-4861E INFRARED MOTION DETECTION SENSOR

Introduction

The IMS-4861E Infrared Motion Detection Sensor is a dual-element passive infrared intrusion detector for use in electronic security systems. It reduces false alarms by eliminating background noises and nuisance stimuli. The IMS-4861Eemploys variable pulse-count adjustment, thus making it adaptable for use both inside and outside of server/equipment rooms. It is designed to connect to the IMS-4000E Host or Node. Refer to the manufacturer's instruction guide for more information.

Package Contents

(1) IMS-4861E Infrared Motion Detection Sensor

(3) Plastic drywall anchors

(3) #8 Self tapping screws

Cabling

The Passive Infrared Detection Sensor comes with an attached 7' cable with an RJ-45 plug on the end. If the sensor is close to the IMS-4000E Host or Node, you can plug the sensor directly to an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

> **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

You should install the IMS-4861E sensor in a location that is most likely to intercept an intruder. The IMS-4861E monitors motion across a 85º field of vision and can detect motion across the beam as well as motion coming toward the sensor.

> **Note:** Avoid installing the sensor where it faces direct sunlight; faces areas that may change temperature rapidly, or areas where there are air ducts or substantial air flows. All of these can create false reports.

The sensor can also be attached directly to a wall or corner without the bracket. Knockout holes for corner mounting can be accessed by opening the sensor body (see instructions below), taking out the PC board, and then knocking out the appropriate four (angled) holes.

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

> **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Jumper Pin Selections

LED Selection Jumper

Jumper in postion ON (to the right): LED is enabled. The LED will light when the sensor is in alarm condition.

Jumper in position OFF (to the left): LED is disabled.

PULSE/AUTO: Pulse Count Jumper

Jumper in position 2 (to the right): Jumper setting for a stable environment without air drafts.

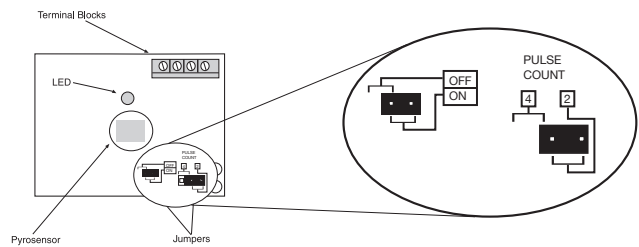Jumper in position 4 (to the left): Setting for a harsh environment.

Figure 2: Sensitivity adjustment and jumper locations

Sensor Template (factory default)

Input Name:	Motion Detector
Recognition Time:	1 Second
Reset Time:	0 Seconds
Data Logging:	Active
Voice:	motion detector.wav
Input Class:	Other

Specifications

Sense Logic:	Quad zone with rodent/pet immunity
Power Input:	9.5-16Vdc
Current Consumption:	8mA @ 12 Vdc
Temperature Compensation:	Yes
Alarm Period:	Approximately 2.5 sec
Alarm Output:	N.C. 200mA @ 28 Vdc (10W in line resistor Form "A")
Operating ambient temperature range:	-4ºF to +122ºF (-20ºC to +60ºC)
Operating humidity range:	Up to 95% (non-condensing)
Storage temperature range:	-40ºF to +176ºF (-40ºC to +80ºC)
RFI protection:	≥20 V/m @ 10-1000 MHz
Dimensions:	3.8" x 2.4" x 1.8" (97mm x 61mm x 46mm)
Weight:	5.6 oz (160 grams)

IMS-4862E SMOKE DETECTION SENSOR

Introduction

The IMS-4862E Smoke Detector Sensor is designed to connect to the IMS-4000E Host or Node and monitor for smoke in indoor environments. The electrical connection between the sensor and IMS-4000E is made via the attached RJ-45 patch cable. The sensor may be secured to a wall or ceiling (hardware not included).

Cabling

The Smoke Detector Sensor comes with an attached 7' cable with an RJ-45 plug on the end. If the sensor is close to the IMS-4000E Host or Node, you can plug the sensor directly to an IMS environmental input. If the cable is too short you can use the included RJ-45 adaptor and a longer patch cable to extend the length. For applications where the sensor may be far from the IMS unit, you may utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input.

⚠️ **Caution:** The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices.

Mounting

The sensor may be mounted directly against a wall or ceiling (hardware not included).

Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. When a new sensor is plugged into the Host or Node, the configuration is set to the factory default via the Sensor Template. If you have modified these templates, the configuration will be set to the modified configuration. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

The smoke alarm is a latching alarm device. To reset the smoke alarm, momentarily disconnect the cable from the front panel of the IMS Host or Node and then reconnect it.

⚠️ **Caution:** Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Sensor Template (factory default)		Specifications	
Input Name:	Smoke Detector	**Sensitivity:**	2.0 ± .37% - .39% /ft.
Recognition Time:	10 Seconds	**Contact Rating:**	2 AMP 28 VDC or 120 VAC resistive
Reset Time:	0 Seconds	**Heat sensor rating:**	Fixed 135º F (57ºC) rate of rise > 15ºF/min. (8.3ºC/min.)
Data Logging:	Active		
Voice:	smoke detector.wav	**Operating voltage:**	8.5–33 VDC, 10% max. ripple
Input Class:	Smoke	**Maximum ambient temperature:**	100ºF (37.8ºC)
		Power-up time:	15 seconds
		Housing:	white plastic
		Housing dimensions:	6.1" d x 1.9" h

IMS-4863E AIR FLOW SENSOR

Introduction

The IMS-4863E Airflow Sensor lets you monitor the movement of air in cooling ducts or inside equipment cabinets. It reports the relative air flow passing the sensor over a range of 0 to 100%, allowing you to monitor the operation of your cooling and ventilation systems.

Cabling

The Airflow Sensor connects to the IMS-4000E Host or Node via an RJ-45 cable (e.g. CAT5 cable). The connection from the sensor to the Host or Node can utilize your existing network wiring infrastructure. For example, the sensor may be installed in another room or another floor. Connect the sensor to your structured wiring network via an RJ-45 jack. At the other end, connect a patch cable from your structured wiring patch panel directly to the Host or Node environment input..

Caution: The IMS sensors are not TCP/IP devices and therefore should not be connected directly to any wiring infrastructure that is connected to network equipment such as a hub, router, or switch. Sensors use RJ-45 plugs and cables similar to those used with Ethernet devices..

Mounting

The sensor can be installed to the wall of a cabinet, inside of a vent, or directly in front of any forced air system. The enclosure can be mounted using the included dual-lock velcro tape, screws, double-sided adhesive foam tape, or with tie wraps. Your specific requirements will dictate the best mounting method for your application. The only installation requirement is that the sensing elements protruding from the side of the enclosure must be in the path of air flow.
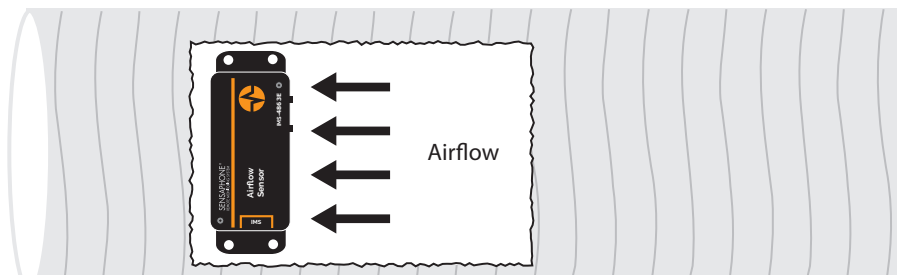
Configuration

All IMS Solution sensors are auto-configured when you plug them into the Host or Node. The Airflow Sensor will identify itself as a 4-20mA transducer. When a sensor is removed, or the connection is disrupted, the configuration data remains intact but the sensor will go into trouble status and generate a trouble alarm. When the sensor is plugged in again, or the connection is re-established, configuration data remains unchanged and the sensor returns to normal operating condition.

Caution: Removing a sensor for less than 60 seconds does not produce a trouble alarm. Removing or unplugging a sensor for more than 60 seconds or plugging in a different sensor at any time will cause a trouble alarm.

Host and Node Firmware Requirements

The Airflow Sensor requires the following firmware versions in the IMS-4000E Host and updated ConsoleView software for your computer for sensor compatibility:

IMS-4000E Host

- Input board firmware chip version xx.xx.xx.106 or higher

  NOTE: Input board firmware is NOT flash upgradeable. A new firmware chip must be installed. For information on obtaining a new firmware chip, please contact Sensaphone Technical Support at 610.558.2700 or via e-mail at support@sensaphone.com.

- ConsoleView version 3.0.22 or higher

- IMS4K OS version 3.13 or higher

• Voice version 2.12 or higher

*Host version information is viewable through the ConsoleView software on the Version Info screen and the Help>About selection from the main menu.

IMS-4000E Node

• Firmware version 2.59 or higher (for 10Mbit/s nodes).

• All firmware versions (for 100Mbit/s nodes).

*Node version information is viewable through the ConsoleView software on the Node Properties>Diagnostics screen.

Sensor Template		Specifications	
Input Name:	Transducer	Range:	0-100 %
High Limit:	100	Operating Temperature:	32 to 80°F (0 to 26.5°C)
Low Limit:	0	Operating Humidity:	0 to 80% RH, non-condensing
Recognition Time:	60 Seconds	IMS Connection:	RJ-45
Reset Time:	0 Seconds	Housing:	Black plastic with mounting ears
Data Logging:	Active	Dimensions:	4.2" x 1.6" x 0.9"
Voice:	none		
Input Class:	Other		

Technical Support for the IMS-4000E Sensors

For questions about installing any of these sensors, please contact your local IMS Solution Reseller or VAR or contact the manufacturer directly at:

SENSAPHONE	Tel:	877.373.2700
901 Tryens Road	Fax:	610.558.0222
Aston, PA 19014	Email:	support@IMS-4000E.com
www.IMS-4000E.com		

APPENDIX A: WEEKLY TESTING PROCEDURE

We recommend that you test your IMS-4000E system weekly to be sure it is functioning properly. This will ensure that when a problem arises the IMS-4000E will be ready to alert the appropriate personnel. A test log template is included at the back of this manual.

There are several tests that can be performed:

1) Call the unit and listen to the Status Report. This will test the unit's ability to answer the phone and speak a message. It will also verify that all of the inputs are reading properly, the alarm conditions are OK, the electricity is on, the microphone is functioning, and the batteries are OK.

2) Create an alarm on each input by tripping all connected sensors.
Temperature sensors: Heat or cool the sensor.
Motion sensors: Have someone walk in front of the sensor.
Door/window sensors: open the door/window.
Water sensors: Apply a small amount of water beneath the sensor or use a wet towel and touch it to the sensor probes.
Humidity sensors: Raise the humidity around the sensor by holding a cup of very hot water beneath the sensor.
Smoke detectors: Hold magnet near test area on smoke detector, or make smoke.

Allow the unit to contact all programmed telephone numbers. This will make sure that the IMS-4000E is programmed properly. It will also prepare personnel to respond appropriately when they receive a call from the Sensaphone.

3) Test the batteries in any IMS unit by unplugging the AC power and making sure that the IMS-4000E continues to function.

4) If you are using your IMS-4000E to listen for a smoke alarm, then be sure to test the smoke alarm to make sure that the IMS-4000E picks up the audible signal and triggers a high-sound-level alarm. Allow the unit to dial all programmed telephone numbers.

5) If you require assistance, call Sensaphone Technical Support at 610.558.2700.

APPENDIX B: TROUBLESHOOTING

SOFTWARE

Why does my IMS-4000E Host begin dialing as soon as I turn it on?

- IMS-4000E will only dial to deliver an alarm message. An unacknowledged alarm exists, and IMS-4000E is trying to deliver an alarm message.

Why can't I connect with my IMS-4000E using my Ethernet network?

- The IMS-4000E's Host or Node's network settings may be incorrect. Verify the IP address, Gateway, DNS, and Subnet mask settings.
- There may be a network IP address conflict. The IMS-4000E Host or Node's IP address may be the same as another device on your network.

Why can't I connect with my IMS-4000E's (Host or Node) serial port?

- A NULL RS-232 serial cable is required to perform the local configuration of an IMS-4000E Host or Node. Verify that you are using a NULL cable. A Null modem serial cable is available for purchase from Phonetics as an accessory (part number IMS-4406).
- Make sure that your cable is connected to a serial (COM) port on your PC, not a parallel (LPT) port.
- Your PC's terminal emulation program settings may be incorrect. The serial Port settings should be as follows:

    Bits per second: 9600

    Data Bits : 8

    Parity: None

    Stop bits: 1

    Flow control: None

Why can't I connect with my IMS-4000E Host using a PPP dial-up connection?

If your modem won't dial at all:

- Make sure that your Windows Dial-up Network connection is properly set up. Check that the telephone number is properly programmed.
- Make sure that your modem is connected to a serial COM port on your PC, not a parallel (LPT) port.

If your modem dials but you can't connect with the IMS-4000E Host:

- Verify the User Name and Password settings on the Windows Dial-Up Network connection match the settings programmed in your IMS-4000E's Profile Setup.
- Make sure that your modem is turned on and plugged into a working telephone line.

Will IMS-4000E retain its programming if there has been a long power failure and the backup battery dies?

Yes. When all power is removed from the IMS-4000E,voice messages and unit programming are retained in a nonvolatile solid-state flash disk.

My IMS-4000E unit got damaged and had to be replaced. Can I use the original unit's saved programming to quickly program the replacement unit?

Yes.

Why won't my IMS-4000E Host dial out?

- Check that you have a Touch-Tone telephone line. The IMS-4000E Host will not be able to dial out if it's on a Pulse telephone line.
- The Contact telephone number may be incorrectly programmed. Verify the telephone numbers. Is a '1 +area code' prefix required? Does your telephone line require a '9' prefix to reach an outside line?

- Each Contact telephone number has a programmable call schedule. It may not be the programmed time of day, or day of week for the IMS-4000E Host to call a particular contact. Verify the call schedule for each contact.

- Recognition time may be set too long for an alarm condition to become a valid alarm. Shorten the Recognition time for the alarm or increase the amount of time that the monitored condition exists.

- The wrong Alarm Class has been assigned. For each environmental or IP alarm, you may specify an Alarm Class. Check the Alarm Class assigned to the environmental or IP channel.

- The user Profile has not been programmed to receive calls for a particular alarm Class. When an alarm occurs, the IMS-4000E checks its list of User Profiles to see who should be contacted. Only users whose class list includes the class of the alarm will be contacted.

- 'Dial Out Attempts' might be set to zero. If this is the case, the IMS-4000E Host will make zero attempts to call the programmed Contacts. Increase 'Dial Out Attempts' to a number greater than zero.

I keep getting a busy signal when I call my IMS-4000E Host.

The IMS-4000E Host may be trying to deliver an alarm message.

Why does IMS-4000E call again with the same alarm after I just acknowledged it?

- The alarm is clearing and quickly re-tripping. If this occurs, and the Alarm Recognition time is very short, the result will be another call for the re-tripped alarm. Increase the Alarm Recognition time to avoid rapid callbacks for the same alarm.

Why won't the IMS-4000E Host communicate with one or more Nodes?

Every IMS-4000E expansion Node is an IP device with a unique address. Check to make sure that the Host IP address is programmed correctly in the Node(s).

APPENDIX C: IMS-4000E ACCESSORIES

The accessories listed below are available from Sensaphone and authorized distributors. Other dry contact sensors, designed for more specialized applications, may also be used. Commercial/industrial electrical supply houses can provide devices to monitor virtually any condition. For further information, contact Sensaphone Customer Service at 610.558.2700.

Part Number	Description
BAT-0006	6V 3AH battery (Node)
BAT-0014	12V 2.9AH battery (Host)
IMS-4002	IMS-4000E Node
IMS-4003	IMS-4000E Node (220VAC 50/60Hz)
IMS-4402	IMS-4000E 7' CAT5 Patch Cable
IMS-4403	IMS-4000E 14' CAT5 Patch Cable
IMS-4404	IMS-4000E 25' CAT5 Patch Cable
IMS-4405	IMS-4000E RJ-45 F/F Coupler Kit (4)
IMS-4406	Wall Mount Kit
IMS-4407	Null Modem Cable
IMS-4408	IMS-4000E Solution Manual (complete)
IMS-4420	Axis Network Camera
IMS-4810E	IMS-4000E Room Temperature Sensor
IMS-4811E	IMS-4000E Room Temperature Sensor w/Display (Fahrenheit)
IMS-4812E	IMS-4000E Mini-Temperature Sensor
IMS-4813E	IMS-4000E Room Temperature Sensor w/Display (Celsius)
IMS-4814E	IMS-4000E Ultra Low Temperature Sensor
IMS-4820E	IMS-4000E Humidity Sensor
IMS-4821E	IMS-4000E Humidity Sensor w/Display
IMS-4830E	IMS-4000E Water Sensor w/10' Water Detection Rope
IMS-4831	IMS-4000E 10' Water Detection Rope
IMS-4840E	IMS-4000E Power Sensor
IMS-4850E	IMS-4000E Dry Contact Bridge
IMS-4851E	IMS-4000E 4–20mA Bridge
IMS-4860E	IMS-4000E Door Switch
IMS-4861E	IMS-4000E Passive Infrared Motion Detector w/7' RJ-45 Cable
IMS-4862E	IMS-4000E Smoke Detector w/7' RJ-45 Cable

APPENDIX D: LICENSE AGREEMENT FOR SENSAPHONE® IMS-4000E CONSOLEVIEW SOFTWARE

PLEASE READ THIS LICENSE AGREEMENT CAREFULLY BEFORE INSTALLATION OF SOFTWARE AND USING THE PRODUCT OR SERVICE.

THIS LICENSE AGREEMENT CONTAINS SENSAPHONE'S STANDARD TERMS AND CONDITIONS.   WHERE PERMITTED BY THE APPLICABLE LAW, BY KEEPING YOUR SENSAPHONE PRODUCT BEYOND THIRTY (30) DAYS AFTER THE DATE OF DELIVERY, YOU FULLY ACCEPT THE TERMS AND CONDITIONS SET FORTH IN THIS LICENSE AGREEMENT.

IN ADDITION, WHERE PERMITTED BY THE APPLICABLE LAW, YOUR INSTALLATION OF THE SOFTWARE AND/OR USE OF THE PRODUCT OR SERVICES CONSTITUTES FULL ACCEPTANCE OF THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CONTAINED HEREIN. THESE INCLUDE WARRANTY DISCLAIMERS, INDEMNIFICATION TERMS AND LIMITATIONS OF LIABILITY.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, INCLUDING ANY WARRANTY DISCLAIMERS, INDEMNIFICATION TERMS OR LIMITATIONS OF LIABILITY, THEN YOU SHOULD NOT USE THE SOFTWARE AND SHOULD RETURN IT TO THE SELLER FOR A REFUND OF THE PURCHASE PRICE.

THE LAW IN YOUR JURISDICTION MAY LIMIT THE EXTENT TO WHICH YOUR RETENTION, INSTALLATION OR USE CONSTITUTES ACCEPTANCE OF THE TERMS AND CONDITIONS HEREIN; AND AS TO THE ENFORCEABILITY OF LIMITATIONS UPON OR EXCLUSIONS OF WARRANTIES, AND UPON INDEMNIFICATION TERMS OR LIMITATIONS OF LIABIILITY, OTHERWISE SET OUT IN THIS AGREEMENT.

This is a License Agreement between Phonetics Incorporated d.b.a. Sensaphone (hereinafter "Sensaphone") and you, the end user. Sensaphone and you accept the terms and conditions set forth herein, a perpetual, limited, non-exclusive License (hereinafter "License").

License Grant

Sensaphone hereby grants you, the end user, a limited, non-exclusive, free to copy, install and use the Sensaphone IMS-4000E ConsoleView software, amendments thereof and its associated files (hereinafter collectively referred to as the "Software") for personal and commercial purposes only. Sensaphone provides the License solely for end-user use. You may not reverse engineer, decompile, or disassemble the software. The software is licensed as a single product. Its component parts may not be separated for use on more than one computer. You may not rent or lease the software individually, separately or independently unless it is used in conjunction with the operation of the Sensaphone IMS-4000E monitoring hardware. You may make copies of the software and transfer your rights under this agreement, provided that each recipient of the software also agrees to the terms of this agreement.

Copyright ©

The copyright of the Software at all times belongs to and remains with Sensaphone. Without prior approval of Sensaphone, no part of the Software may be reproduced, distributed or transmitted in any form or by any means, electronic or mechanical, for any purpose other than stated in the License. All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, text, and applets, incorporated into the Software), and any copies of the Software are owned by Sensaphone (or one or more of its licensors). The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software like any other copyrighted material except that you may make copies of the Software, subject to the limitations set forth herein.

NO WARRANTY—LIMITATION OF LIABILITY—INDEMNIFICATION— COVENANT NOT TO SUE

I. THE SOFTWARE IS PROVIDED "AS IS," AND NEITHER SENSAPHONE NOR ANY OF ITS LICENSORS MAKES ANY EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES TO YOU REGARDING THE USABILITY, CONDITION OR OPERATION THEREOF. NEITHER SENSAPHONE NOR ANY OF ITS LICENSORS WARRANTS THAT THE SOFTWARE WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY AND/OR THAT IT WILL BE FREE FROM VIRUSES OR OTHER DEFECTS. SENSAPHONE AND ITS LICENSORS EXPRESSLY DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, THE WARRANTY OF MERCHANTIBILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR USE AND THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND THE WARRANTY OF NON-INFRINGEMENT AND/OR ANY WARRANTY ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

II. YOUR INSTALLATION AND USE OF THE SOFTWARE IS AT YOUR OWN RISK. YOU ASSUME FULL RESPONSIBILITY AND RISK OF LOSS RESULTING FROM YOUR DOWNLOADING, INSTALLING, AND/OR USE OF FILES OR OTHER MATERIAL. YOU AGREE THAT NEITHER SENSAPHONE NOR ANY OF ITS LICENSORS WILL BE LIABLE FOR DAMAGES (INCLUDING BUT NOT LIMITED TO DIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES) ARISING OUT OF YOUR INSTALLATION OF, USE OF, OR INABILITY TO USE THE SOFTWARE, AND YOU HEREBY WAIVE ANY CLAIMS OF ANY KIND WITH RESPECT THERETO, WHETHER BASED IN CONTRACT, BREACH OF WARRANTY, TORT OR ON ANY OTHER GROUNDS, EVEN IF SENSAPHONE (OR ANY SUCH LICENSOR) HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES, AND WHETHER OR NOT CAUSED BY SENSAPHONE'S OR ITS LICENSORS' NEGLIGENCE. THE SOLE AND ENTIRE LIABILITY OF SENSAPHONE AND ITS LICENSORS, AND YOUR EXCLUSIVE REMEDY WITH RESPECT TO THE USE OF THE SOFTWARE OR ANY BREACH OF THIS AGREEMENT, SHALL BE THE REPLACEMENT OF ANY SOFTWARE FOUND TO BE DEFECTIVE.

III. YOU AGREE TO RELEASE, WAIVE, DISCHARGE AND COVENANT NOT TO SUE SENSAPHONE, ITS LICENSORS, OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATED COMPANIES, FOR ANY AND ALL LIABILITIES ARISING FROM OR POTENTIALLY ARISING FROM ANY CLAIM, DEMAND OR ACTION BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIMITED TO DAMAGES THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM INSTALLATION, OPERATION OF, USE OF, OR THE INABILITY TO USE SENSAPHONE'S SOFTWARE, OR FROM THE FAILURE OF SENSAPHONE'S SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY SENSAPHONE'S NEGLIGENCE, EXCEPT AS NECESSARY TO ENFORCE THE EXPRESS TERMS OF THIS LICENSE AGREEMENT.

IV. YOU WILL INDEMNIFY, DEFEND AND HOLD HARMLESS SENSAPHONE, ITS LICENSORS, OWNERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR AFFILIATED COMPANIES, AGAINST ANY AND ALL CLAIMS, DEMANDS OR ACTIONS BASED UPON ANY LOSSES, LIABILITIES, DAMAGES OR COSTS, INCLUDING BUT NOT LIMITED TO DAMAGE THAT ARE DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL, AND INCLUDING ATTORNEYS FEES AND LEGAL COSTS, THAT MAY RESULT FROM INSTALLATION, OPERATION OF, USE OF, OR THE INABILITY TO USE SENSAPHONE'S SOFTWARE, OR FROM THE FAILURE OF SENSAPHONE'S SYSTEM TO REPORT A GIVEN EVENT OR CONDITION, WHETHER OR NOT CAUSED BY SENSAPHONE'S NEGLIGENCE.

V. WITHOUT WAIVING ANY PROVISION IN THIS LICENSE AGREEMENT, IF A CIRCUMSTANCE ARISES WHERE SENSAPHONE AND/OR ITS LICENSORS ARE FOUND TO BE LIABLE FOR ANY LOSS OR DAMAGE ARISING OUT OF MISTAKES, NEGLIGENCE, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR DEFECTS IN THE SOFTWARE SUBJECT TO THIS AGREEMENT, THEN SUCH LIABILITY SHALL NOT EXCEED THE TOTAL AMOUNT PAID BY THE CUSTOMER UNDER THIS LICENSE AGREEMENT OR $250.00, WHICHEVER IS GREATER. YOU HEREBY RELEASE SENSAPHONE AND ITS LICENSORS FROM ANY AND ALL OBLIGATIONS, LIABILITIES AND CLAIMS IN EXCESS OF THIS LIMITATION.

VI. NEITHER SENSAPHONE NOR ANY OF ITS LICENSORS SHALL BE HELD RESPONSIBLE IN ANY WAY OR BY ANY MEANS, EITHER DIRECTLY OR INDIRECTLY, FOR ANY COMMUNICATIONS DIFFICULTIES OUTSIDE OF

SENSAPHONE'S CONTROL WHICH COULD LEAD TO THE INTERRUPTION OF DATA DELIVERY SERVICE TO YOUR ELECTRONIC MAIL ADDRESS, PAGER, TELEPHONE OR ANY OTHER RECEIVING DEVICES OR THIRD-PARTY DATA STORAGE AND/OR DELIVERY SERVICES.

VII. IN PARTICULAR, YOU WILL NOT RELY ON ANY REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, MADE BY ANY PERSON OTHER THAN AN AUTHORIZED REPRESENTATIVE OF SENSAPHONE, IN EVALUATING THE SOFTWARE.

VIII. THE LAW IN SOME JURISDICTIONS MAY LIMIT OR PRECLUDE WARRANTY EXCLUSIONS OR LIMITATIONS, INDEMNIFICATION TERMS AND/OR LIMITATIONS ON LIABILITY, SO NOT ALL OF THE ABOVE LIMITATIONS MAY APPLY TO YOU.

Disclaimer

Although the Software is scanned for the known viruses, you should scan the Software for viruses or other defects, prior to installation on your system. Sensaphone does not accept any liability for damage or loss as a result of the installation or use of the Software, including but not limited to any damage or loss resulting from any such viruses or defects.

Notwithstanding its efforts Sensaphone reserves the right to change the Software and publish new release versions. Sensaphone assumes no responsibility in notification to the end-user of new release updates or versions of the Application.

Website use

Customer may use services provided by Sensaphone on an Internet web site that could be connected to the use of the Software subject to this Agreement. The use of such web site may only be made by authorized users with a proper identification and pass-word or serial number.

In using such a web site, you are further BOUND BY THE TERMS AND CONDITIONS LOCATED ON THE WEB SITE. YOU MUST READ ALL OF THE TERMS AND CONDITIONS BEFORE PROCEEDING TO USE THE WEB SITE. IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS ON THE WEB SITE, THEN YOU SHOULD CEASE USING THE WEB SITE, AND INFORM SENSAPHONE THAT YOU DO NOT INTEND TO USE AND/OR CONTINUE USING THAT WEB SITE. YOUR USE OF THE WEB SITE IS AN ACKNOWLEDGMENT THAT YOU AGREE TO ALL THE TERMS AND CONDITIONS THEREIN.

Deemed acceptance and applicable law

The installation or use of the Software is deemed acceptance of the terms and conditions contained in the License Agreement. This License Agreement shall be effective and binding upon Sensaphone and you, the end user, upon installation or use of the Software. The term of this Agreement shall commence on the date of installation or use by you and shall continue indefinitely if you remain in compliance with all of the terms and condition set forth herein. If you do not agree to the terms of the License, please do not install or otherwise use the Software.

Choice of Forum and Choice of Law

In the event that a dispute arises out of or in connection with this License Agreement, then any claims or suits of any kind concerning such disputes shall only and exclusively be brought in either the Court of Common Pleas of Delaware County, Pennsylvania or the United States District Court for the Eastern District of Pennsylvania.

Regardless of the place of contracting or performance, this License Agreement and all questions relating to its validity, interpre-tation, performance and enforcement shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to the principles of conflicts of law.

APPENDIX E: RETURNING AN IMS UNIT FOR REPAIR

In the event that any of your Sensaphone IMS-4000E units does not function properly, we suggest that you do the following:

   1) Record your observations regarding the individual unit's malfunction.

   2) Call the Technical Service Department at 610.558.2700 prior to sending the unit to Sensaphone for repair.

   If the unit must be sent to Sensaphone for servicing, please do the following:

   1) Turn the power switch on the rear of the unit Off.

   2) Disconnect all cables, inputs and wiring, and unplug the unit.

   3) Carefully pack the unit to avoid damage in transit. Use the original container (if available) or a sturdy shipping box.

   4) To avoid shipping delays, you must include the following information :

      a) Your name, address and telephone number.

      b) A note explaining the problem.

5) Ship your package to the address below:

      SERVICE DEPARTMENT

      Sensaphone

      901 Tryens Road

      Aston, PA 19014

6) Ship prepaid and insured via UPS or US Mail to ensure a traceable shipment with recourse for damage or replacement.

TEST LOG

Date	Inputs		Dialout		Call-In		Battery				Tested By
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	

Date	Inputs		Dialout		Call-In		Battery				Tested By
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	
	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	Pass ☐	Fail ☐	