TAKEX

IP INTERFACE MODULE

INT-QUADIP

Instruction Manual

Thank you for purchasing this product. Before using the product, please read this instruction manual to ensure correct operation.

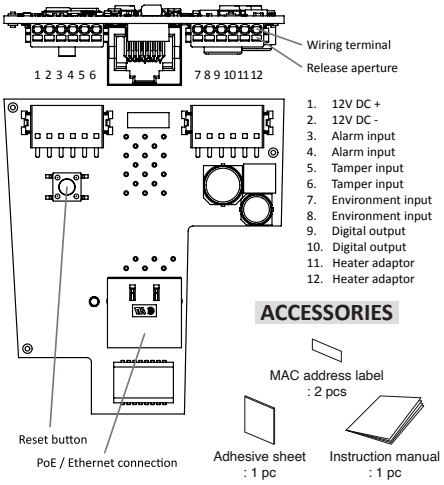
With the Takex IP interface module, our photoelectric beams are as easy as IP cameras to install and integrate with Video Management Systems; start recording when somebody enters the area, move a PTZ to the location of an intrusion, or activate lighting.

The IP module is specifically designed to fit Takex PB-IN-HF/HFA, PB-F/FA, PB-IN-100AT, PB-100ST, PB-KH & PB-IN-75SW series sensors with inputs, outputs and web interface tailored for the product. With the IP module connected your product will function as a true IP device, allowing alarm settings, alarm notification and power supply through the network cable.

The use of the INT-QUADIP as a power supply invalidates the UL listing for PB-IN-HF series sensors.

1 PARTS DESCRIPTION

MAIN UNIT



ACCESSORIES

TABLE OF CONTENTS

2 PRECAUTIONS

- This manual describes precautions by classifying them based on degrees of danger and damage that would be generated if using the unit incorrectly.

- **We categorize these precautions throughout the manual using the following symbols.**

A prohibited action, you must not do.	An action you must do, and should keep in mind.

Warning

- Do not disassemble or modify this device. This may cause fire, electrical shock, or malfunction.
- If the following events occur, turn off the power of the unit immediately, and ask the place of purchase for repair. Failure to follow this may result in fire, electric shock, and/or malfunction.
  - Smoke, abnormal odor, and/or sound are found
  - Liquid, such as water, and/or foreign material has entered the unit
  - The unit has deformed and/or damaged parts
- The Takex INT-QUADIP Module must be connected to a PoE Network structure, installed to the current Networking installation and protocol requirements. All Networking rules apply.
- Only Takex approved devices should be connected to the INT-QUADIP module
- Always ensure the latest Firmware Version is installed
- The INT-QUADIP Interface is designed for use on PoE Class 3 IEEE 802.3af Networks

3 INSTALLATION

You will need 1 x IP module for the beam transmitter (to provide power and monitor the tamper switch, if required), and 1 x IP module for the beam receiver (to provide power and monitor the alarm, tamper, and environmental outputs as required).

1. Insert network cable through the rubber grommet cable entry in the metal backplate of the beam before fixing into position.

   PB-KH series for mounting in beam towers does not have a metal backplate.

2. Pass network cable through the cable entry hole in the beam body and secure beam to backplate.

   The IP module is equipped with a digital output (N.C. 30VAC/DC 100mA Max) which can be controlled from the IP interface. If the digital output is required, install an appropriate cable by repeating steps 1 & 2 above.

3. Fix IP module into position using the adhesive sheet provided, as shown in the diagram.

   Do not connect the network cable before completing step 4!

4. Wire power, alarm, tamper, and environment connections from the IP module to the beam unit as required.
   IP module terminal arrangement is shown in section ***1. PARTS DESCRIPTION***
   IP module Input cable requirements are shown in section ***6. SPECIFICATIONS***

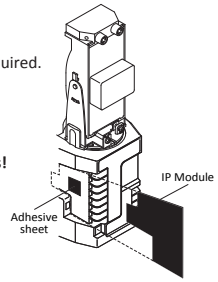
   Wire the digital output cable to the IP module if installed.

   Heater adaptor terminals 11 and 12 are for future use - do not connect to these terminals!

   Tamper/Environment is not supported on all beam series.

5. Connect the network cable into the socket on the IP module. This must be done before the cable is connected to the Power over Ethernet (PoE) Class 3 switch/Injector.

6. When the IP module is powered, align the beam according to the beam installation manual.



4 USER INTERFACE

Settings are made through a web based user interface. All that is required is a device with a modern web browser on the same network as the IP module.

4.1 Factory Default Settings

When using the system for the first time, or if a factory reset has been made, the following settings are used.

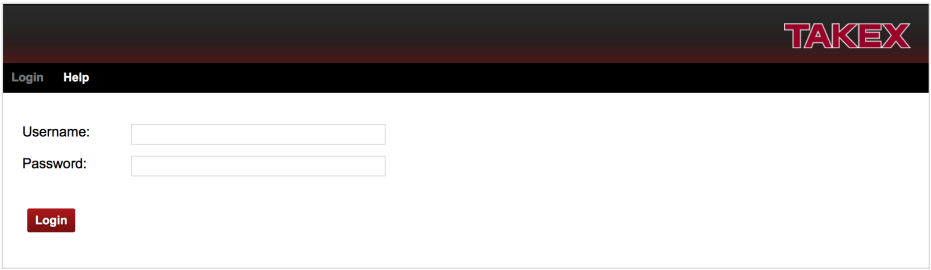
Product IP-address	192.168.0.10
Subnet mask	255.255.255.0
Default router	192.168.0.1
Username	admin
Password	admin

4.2 Login

1. Open a web browser.
2. In the address field, enter the selected product IP-address

   You will automatically log out anybody logged in from another computer!

3. The user interface login page is shown.
4. Login with your username and password.

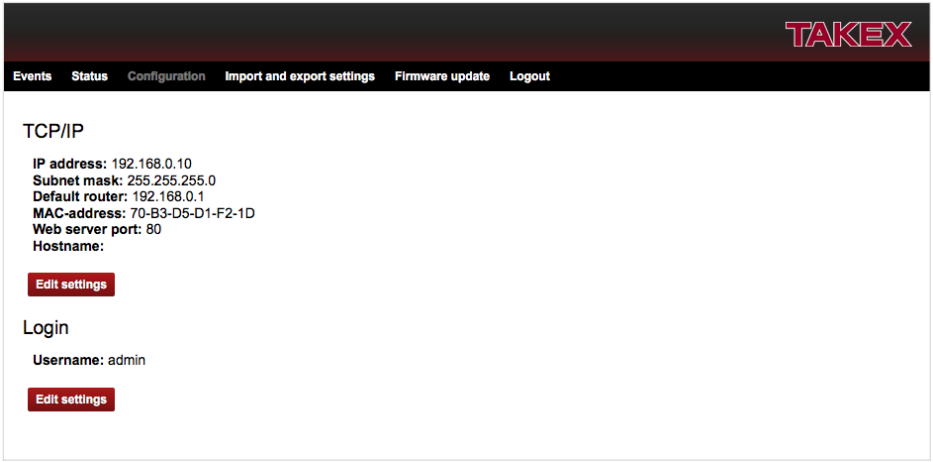


4.3 Installation and configuration

4.3.1 Unit configuration

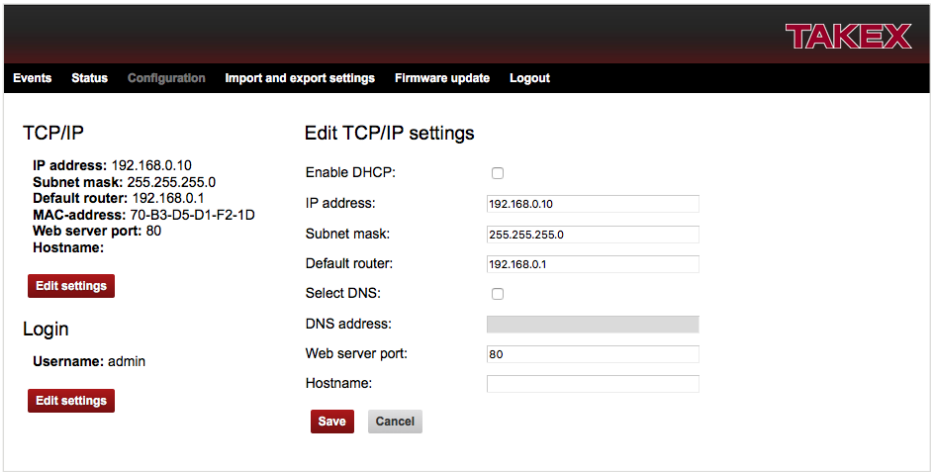
To change TCP/IP settings and Login details

1. Open the *Configuration* tab.

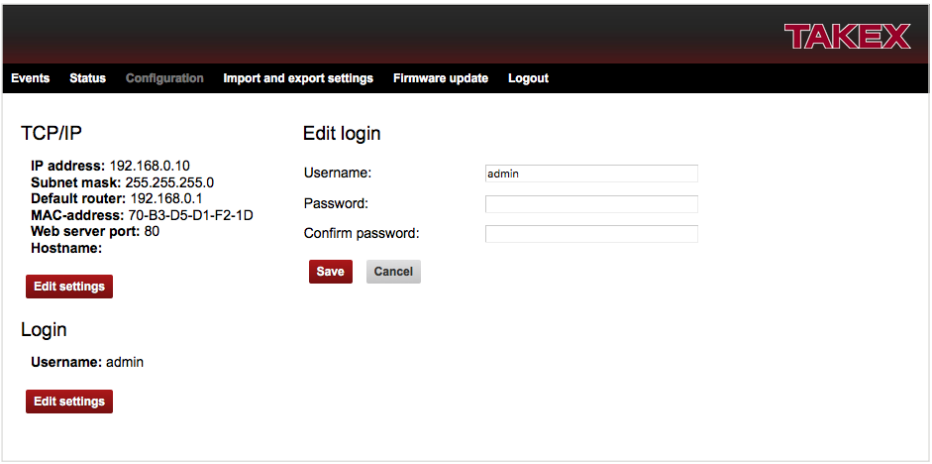


Current settings are shown.

2. To change TCP/IP settings, click *Edit settings*. Input fields appear to the right.



3. Enter desired settings and click the save button.
4. Close browser window and Login using the new TCP/IP Settings.
5. To change Login settings, click *Edit settings*. Input fields appear to the right.

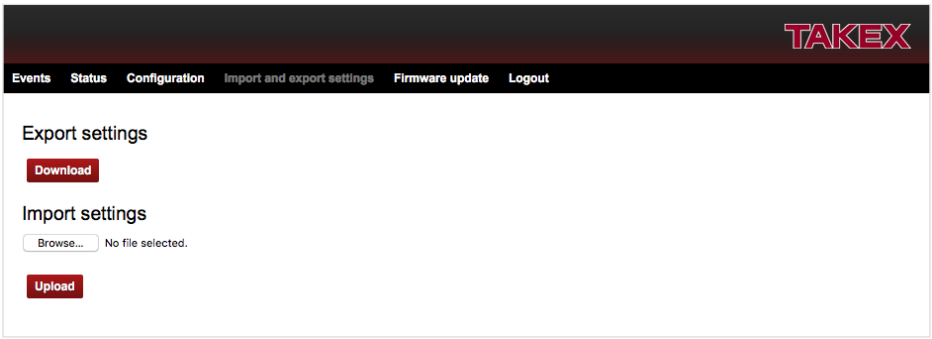


6. Enter a new username and password.
7. Click the save button to confirm.

4.3.2 Import and export settings

Alarm settings can be exported as a file for backup purposes and to copy the settings to other units. IP address and Login settings are not included in this file.

1. Open the *Import and export settings* tab.



2. Export all current alarm settings by clicking the Download button.

> **Pay attention to the file location on your hard drive.**
> **The file name is individual for each unit as it includes the unit MAC-address.**

3. To import a setting file, click *Choose File* button and navigate to the location of the settings file on your hard drive
4. When the file is selected import using the *Upload* button.

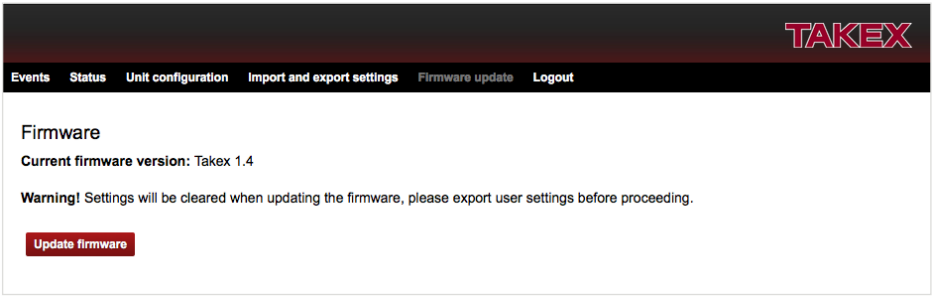
> **Pay attention to the status message next to the button.**
> **Importing a setting file will overwrite all current settings.**

4.3.3 Firmware update

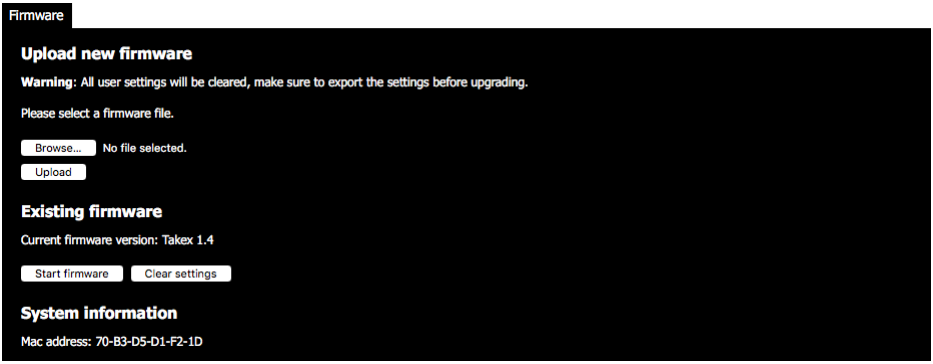
The IP module firmware can be updated to incorporate new versions of Firmware, Clear settings, Restore factory firmware and Restart Firmware.

1. Open the *Firmware* update tab.

Current firmware version is displayed.



2. Click the *Update firmware* button to stop the firmware and enter the system bootloader.



3. To restore factory settings, click *Clear settings* button followed by *Start firmware* to re-start the IP module firmware again.

Password/login will be reset to original default and all event settings cleared. (TCP/IP setting remains unchanged)

4. To upload a new firmware, click Choose File button and navigate to the location of the firmware file on your hard drive. When a file is selected the file name is displayed next to the button.

Uploading a new firmware will erase all alarm and configuration settings excluding Login/password.

5. Click Upload button.

The firmware file will be uploaded to the IP module and over write any previous version and then the IP module will reboot with the new firmware. On completion the new firmware will be displayed.

6. Click *Start firmware* button to restart the IP module with the new firmware. (If IP module does not reset perform a Hardware Reset as outlined in 4.4 below.)

4.4 Hardware reset

A hardware reset is for restarting the IP module after a failed Firmware update, lost login/password, or for returning the module to its factory settings.

All event and configuration will be lost.

Please ensure you have access to Firmware source before attempting a hardware Reset incase the Hardware reset require firmware reloading. factory default IP-address.

1. Disconnect the network cable.
2. Press and hold the reset button, while reconnecting the network cable.
3. The unit will change IP address to Factory default settings (see section 4.1.).
4. Re-open a web browser and enter factory default IP-address.
5. The IP module bootloader screen will be displayed. Please refer to section 4.3.3. step 2.
6. Select *Start firmware* button.
7. If there is any issue with the Hardware reset please upload factory firmware by completing 4.3.3 steps 4 to 6 above.

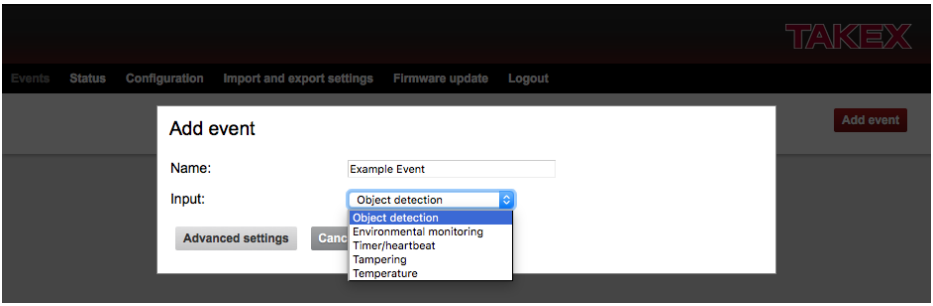
4.5 Alarm settings

All alarm settings are made in the *Events* tab. The IP module works on the principle of "Alarm - Action". This means that alarms are created based on all types of input signals. For each alarm it is possible to create one or more alarm event and action. An action can trigger a network alarm message, or the onboard digital output.

4.5.1 Create an Alarm event

1. Go to the *Events* tab.
2. Click *Add event* button to create an alarm event.
3. Enter a unique name. (i.e. Device/Location)
4. From the *Input* dropdown menu, choose the desired alarm event.

Object detection	Sensor Alarm Output (Normally Closed N/C)
Environmental Monitoring	Sensor Environmental Output (Normally Closed N/C)
Timer/Heartbeat	Creates a periodical alarm event with a time period of between 1 to 99,999 seconds. (Default 60s)
Tampering	Sensor Tamper Output (Normally Closed N/C)
Temperature	Upper/lower temperature alarm event



5. Advanced settings.

These optional settings can be used to change the alarm event behavior depending on the application. Different advanced settings are shown depending on input type.

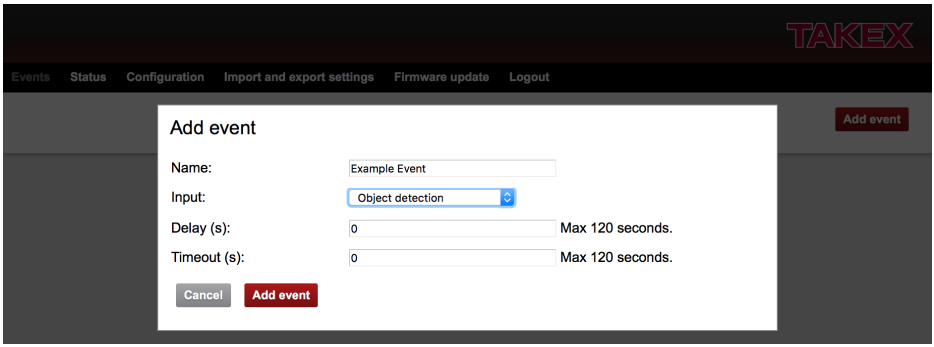
Delay	Alarm delay specifies the time for which the alarm event must be continuously fulfilled before the alarm event is enabled. Default value is 0 seconds, maximum is 120 seconds.
Timeout	Timeout specifies the time before the alarm event is disabled after the alarm conditions are no longer met. Default value is 0 seconds, maximum is 120 seconds.
Timer Period	Timer Period specifies the frequency at which the Timer/Heartbeat signals. Default setting is 60 seconds, adjustable between 1 to 100,000 seconds.

Temperature Upper Limit Temperature Upper Limit specifies the upper temperature for which the alarm event is enabled. Default setting is 35°C.

Temperature Lower Limit Temperature Lower Limit specifies the lower temperature for which the alarm event is enabled. Default setting is 15°C.

The Temperature Upper Limit must be higher than the Temperature Lower Limit.

Hysteresis Hysteresis is used to avoid unstable alarm conditions when the temperature is close to the limit values. The hysteresis specifies the reset value for the upper and lower limits. If no value is set or if the value is set to 0, the default hysteresis value of 1% will be used.



6. Click the *Add Event* button to save the alarm event.
7. Repeat steps 2 to 6 for each alarm event you wish to create.

If multiple actions are desired for an alarm event it is recommended to create multiple alarm events and assign a single action to each.

4.5.2. Edit and Remove Alarm events

1. Edit an alarm event by clicking the *Edit Event* button. An Edit Event window will appear.
2. When the alarm event settings are changed, click the *Save event* button to save the changes.

Clicking any other link will discard all changes.

3. To remove an alarm event click the *Remove Event* button.

Removing an alarm event cannot be undone.

4.5.3. Create an action for an Alarm event

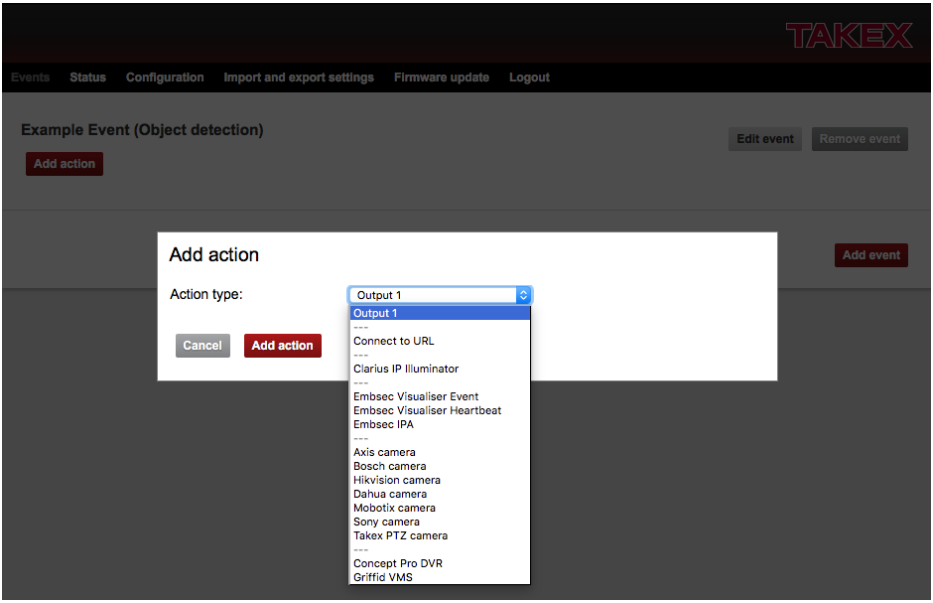
1. Click *Add action* under the desired alarm event.
2. Choose *Action type* from the dropdown menu.

Output 1 This controls the normally closed (N/C) digital output on the IP module. During the alarm event the digital output will change to normally open (N/O).

Connect to URL Connect to URL is used to create any type of network activation. This allows you to have one URL request at alarm start and one URL request at alarm stop.

Partner list On selection of any products listed a built-in wizard will allow you to create a specific URL request needed for the partner product.

Partner list is continuously expanding. Please refer to separate documents regarding integration of these products.



3. Fill in required data fields for the selected action.
4. Click the Add action button to save the action.
5. Repeat step 1-4 for each alarm event.

4.5.4. Test, Remove, and Edit actions

1. To test an action click the *Test* button next to the action.
2. To edit an action click the *Edit* button next to the action.
3. When the action settings are changed, click the *Save action* button to save the changes. Clicking any other link will discard all changes.
4. Remove an action by clicking the *Remove* Button next to the action.

Removing an action cannot be undone.

Digital output actions cannot be edited.

4.5.5. Heartbeat

The heartbeat indicates that the IP module is alive and is working. It is used to detect cable break and product malfunction by periodically sending a short message to the server.

Additional Server software is required for heartbeat monitoring.

4.6 Logout

1. Click the Logout tab in the top menu.

You will automatically be logged out if anybody logs in from another computer to the selected product IP module.

5 SUPPORT

5.1 Support center

For online Service and Support of your IP module

1. Email **EMEASupport@takex.com**

6 SPECIFICATIONS

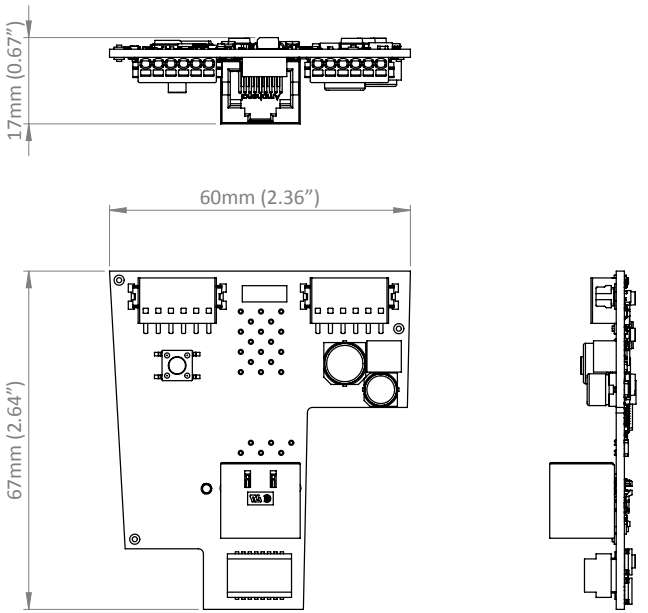
Model	INT-QUADIP
Alarm output	Over IP + Digital output: N.C. 30V (AC/DC) 100mA Max
Alarm input	Alarm Tamper Environmental Heater Adaptor
Input supply voltage	Ethernet IEEE 802.3af/at, TCP/IP
Output supply voltage	Power over Ethernet, class 3 (max 13W)
Supported VMS software	• Axis Camera Companion • Bosch VMS • Embsec Visualiser • Genetec Omnicast • Griffid GMS & GMC • Kentima Ethiris • Milestone Xprotect • Mirasys Carbon VMS • SeeTec Enterprise & Probox
Optional	Heater adaptor
Ambient temperature range	-35°C to +66°C (-31°F to +151°F)
External dimensions	W59mm x H67mm x D16mm (W2.32” x H2.64“ x D0.63”)
Weight	20g (0.7oz)

The IP Module uses push-fit terminal connections for ease of installation, input cable requirements as follows:

Conductor cross section solid min.	0.14 mm²
Conductor cross section solid max.	0.5 mm²
Conductor cross section stranded min.	0.2 mm²
Conductor cross section stranded max.	0.5 mm²
Conductor cross section stranded, with ferrule without plastic sleeve min.	0.25 mm²
Conductor cross section stranded, with ferrule without plastic sleeve max.	0.5 mm²
Conductor cross section AWG/kcmil min.	24
Conductor cross section AWG/kcmil max.	20

NOTES

7 EXTERNAL DIMENSIONS



Limited Warranty :
TAKEX products are warranted to be free from defects in material and workmanship for 12 months from original date of shipment. Our warranty does not cover damage or failure caused by natural disasters, abuse, misuse, abnormal usage, faulty installation, improper maintenance or any repairs other than those provided by TAKEX. All implied warranties with respect to TAKEX, including implied warranties for merchantability and implied warranties for fitness, are limited in duration to 12 months from original date of shipment. During the Warranty Period, TAKEX will repair or replace, at its sole option, free of charge, any defective parts returned prepaid. Please provide the model number of the products, original date of shipment and nature of diffculty being experienced. There will be charges rendered for product repairs made after our Warranty Period has expired.

Maintenance :
• Perform operation checks on a regular basis.

TAKEX

Please note: This device is designed to respond to an intrusion event and to initiate an alarm; it is not a burglary or a crime preventing device. TAKEX is not responsible for damage, injury or losses caused by accident, theft, Acts of God (including inductive surge by lightning), abuse, misuse, abnormal usage, faulty installation or improper maintenance.

In the U.K.
Takex Europe Ltd.
Takex House, Aviary Court, Wade Road,
Basingstoke, Hampshire. RG24 8PE,U.K.
Tel :(+44) 01256-475555
Fax :(+44) 01256-466268
http : // www. takex. com

In the U.S.
Takex America Inc.
151 San Zeno Way
Sunnyvale, CA 94086 U.S.A.
Tel : 408-747-0100
Fax : 408-734-1100
http : // www. takex. com

In Australia
Takex America Inc.
4/15 Howleys Road Notting Hill,
3168 Victoria, Australia
Tel : 03-9546-0533
Fax : 03-9547-9450

In Japan
Takenaka Engineering Co., Ltd.
83-1, Gojo-sotokan, Higashino,
Yamashina-ku, Kyoto 607-8156, Japan
Tel : 81-75-501-6651
Fax : 81-75-593-3816
http : // www. takex-eng. co. jp

TE 6065