Netgenium

ALK3701-IP

Configuration Guide

THE SPECIFICATIONS AND INFORMATION FOR THE HARDWARE AND SOFTWARE PRDUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL INFORMATION AND RECOMMENDATIONS IN THIS MANUAL WERE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

IN NO EVENT SHALL NETGENIUM SYSTEMS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL.

Netgenium ALK3701-IP Manual

Contents

Preface

This preface describes the purpose, audience, organization, and conventions of this guide
The preface covers these topics:

Purpose

The *Netgenium ALK3701-IP Manual* provides information about installing and configuring the Netgenium ALK3701-IP lock controller.

Audience

The *Netgenium ALK3701-IP Manual* is written for network administrators and installers responsible for installing and configuring the Netgenium ALK3701-IP. This guide requires knowledge of IP networking technology.

Conventions

This document uses the following conventions:

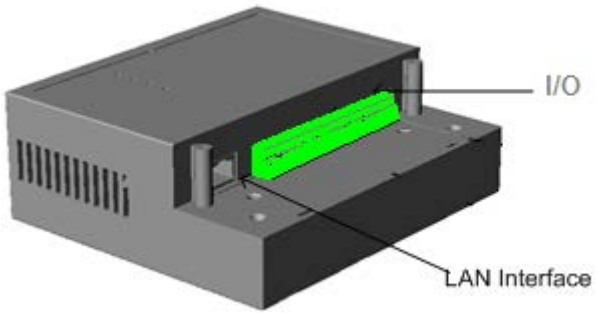
BOLD ORANGE	font is used to show Navigation steps to configure a feature
BOLD RED	font is used to indicate a button or hyperlink
BLUE	font is used to indicate a label on the web page

Chapter 1

Overview

The Netgenium ALK3701-IP Lock Controller is a 802.3af Class 3 POE device. It is capable of onward powering any industry standard 12 Vdc locking hardware and up to 2 card readers (up to a max power budget of 800mA @ 12Vdc).

The controller has 1 RJ 45 style socket for connection to the LAN. The LAN interface is a standard 10/100 network connection. The screw terminals enable connection of locking hardware, readers and a host of I/O devices (RTX, Emergency Breakglass etc.)



The unit is designed to be mounted vertically on a wall or suitable surface above the door to be secured

Powering The Unit

The ALK3701-IP can be powered from any class 3 capable 802.3af power source via the LAN interface.

Resetting the Unit

The ALK3701-IP can be reset by removing power to the unit or pressing the Reset button visible on the front panel or via the software options.

Restore Factory Default Configuration

ALK3701-IP configuration can be restored to factory defaults by pressing the Default button; this will cause the System Status LED to flash Green/Magenta for approximately 30 seconds. If the Reset button is pressed during this time the system will restore the factory default configuration. If the Reset button is not pressed, after 30 seconds the System Status LED will revert to its normal condition.

Chapter 2

Hardware Installation

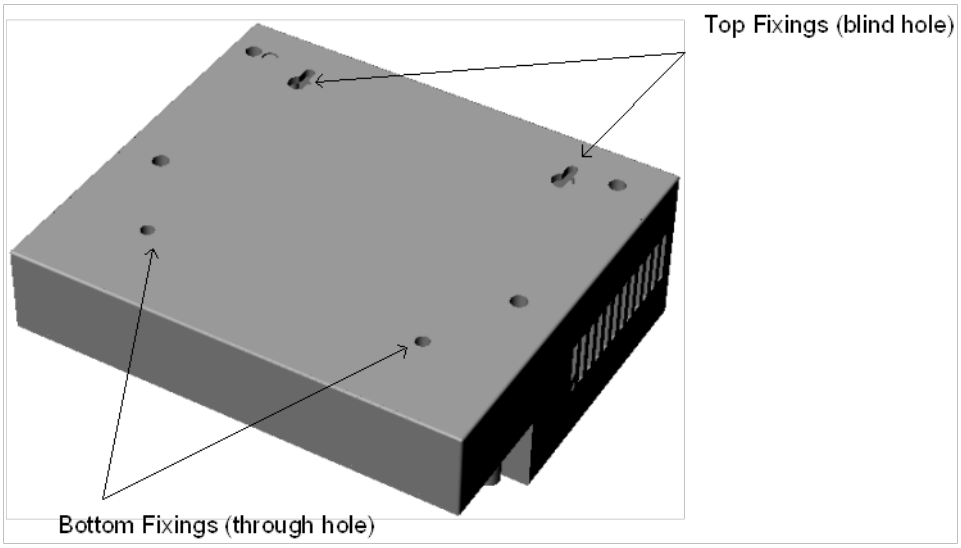
The unit is designed to be mounted vertically on a wall or suitable smooth surface above the door to be protected. Each controller is supplied with a fixing kit containing:

- 4 x wall plugs.
- 2 x 25mm screws (top fixing).
- 2 x 50mm screws (bottom fixing).

To fix the controller to the wall:

- Use the template supplied to drill 4 holes.
- Insert the wall plugs into the holes.
- Using the two 25mm screws. Screw each fixing into the top holes, leave approximately 5mm protruding.

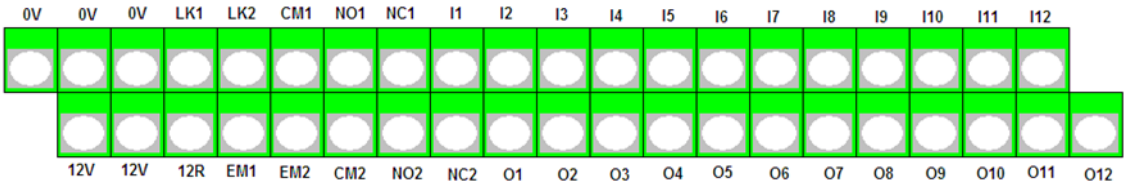
- Locate the unit on the top fixings.
- Use the 50mm screws to secure the unit through the bottom fixings.


Top Fixings (blind hole)
Bottom Fixings (through hole)

CHAPTER 3

INPUTS AND OUTPUTS

All of the I/O devices e.g. locking hardware, card readers, exit switches etc. are connected to the controllers via the screw terminals, shown below.



This chapter will describe the connection of the most common I/O components, the lock hardware, card readers, RTX switch and emergency break glass.

The unit has no support for card readers.

Application notes containing are available for each supported manufacture.

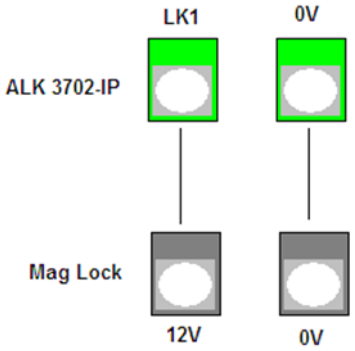
The ALK3701-IP is designed to use POE to power itself and locking mechanism and I/O devices up to a maximum of 800mA @ 12 Vdc.

When designing a solution care should be taken to ensure this budget is not exceeded.

Connecting Lock Hardware

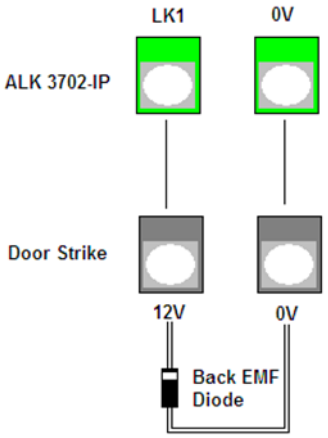
Magnetic Lock

The ALK370x – IP controllers will support any 12Vdc magnetic lock up to a maximum overall load of 800mA. The 12Vdc required to energise the lock is supplied and switched by the controller via the LK1 and 0V terminals.



Ensure the lock mechanism you are connecting has Back EMF Protection – most have. If not a Back EMF Diode of type 1N4001 or equivalent must be fitted.

Door Strike



The ALK370x – IP controllers will support any 12Vdc magnetic lock up to a maximum overall load of 800mA. Door strikes are available as both fail secure and fail safe. Both types require 12Vdc to operate, however a fail secure door strike is locked when no power is present and requires 12Vdc to release the mechanism, a fail-safe door strike is unlocked when no power is present and requires 12Vdc to lock the mechanism.

Both types of mechanism are supported by the controller. The wiring is identical for both types, see Figure 3.3. The lock type is selectable when configuring the controller (see next chapter).

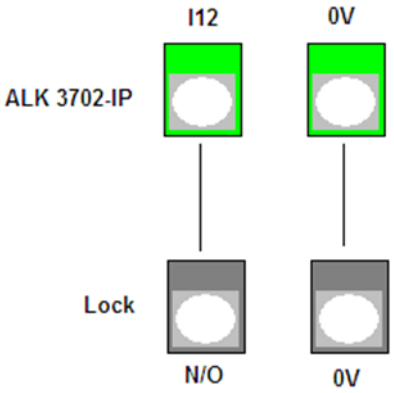
When connecting a door strike to any ALK370x –IP pay special attention to the Back EMF Diode. This must be fitted. Failure to do so could result in the controller being damaged when the lock mechanism is de-energized.

The Back EMF Diode should be of the type 1N4001 or equivalent.

Monitoring The Door Status

If you are using a monitored magnetic lock or door strike it is possible to get an indication of the physical status of the door via relay contacts in the lock mechanism. These are normally presented as C, N/O and N/C.

This feature senses whether the door is open or closed and toggles the relay contacts. The controller can then be configured in software to react to the status of the door.



The door contacts are connected to the lock controller via terminals I12 and 0V as illustrated in Figure 3.3. The illustration shows the N/O contacts connected to I12, this is for illustration purposes only. The lock controller will support both N/O and N/C; this feature is configured in software.

Connecting High Power Locks and Motorized Gates/Barriers

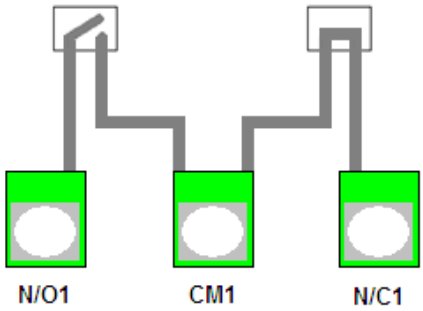
Automatic Gates

As well as supplying 12Vdc to energise locking hardware, the AL3701-IP also provides a clean set of relay contacts. These contacts are controlled by the same logic that switches the 12Vdc to the locking hardware.

Figure 3.5 shows the status of the contacts with the controller powered off.

Most gate mechanisms require a N/O set of relay contacts to close for the gates to open. These contacts are provided across the N/O1 and CM1 terminals of the controller

Alternately if the gate mechanism requires a N/C set of contacts to open for the gates to open. The N/C1 and CM1 terminals should be used.



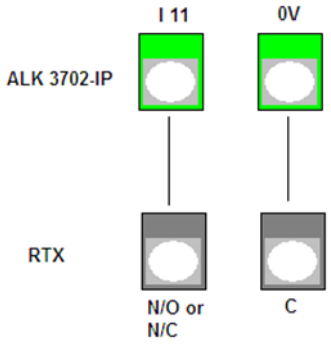
High Power Locks

To control locking hardware that requires a higher voltage and higher power than IEEE802.3af can provide, an external power supply is required. Run one leg of the power supply direct to the lock mechanism and connect the second leg in series with the N/O1 and CM1 and onwardly to the lock mechanism. The relay then acts as a switch and controls the power to the lock.

Connecting Flex I/O

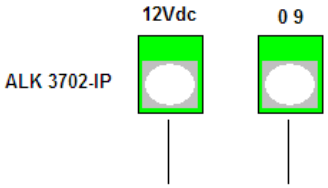
Flex I/O describes a number of general purpose inputs and outputs that can be customized to adopt various functions. The inputs are connected across 0V and one of the Flex I/O pins (I9, I10, I11, I12).

The example below shows a request to exit switch (RTX) wired to I11. (Flex I/O 3).



The RTX switch is connected to the controller via the 0V and any of the Flex I/O connectors, I9 (Flex I/O 1), I10 (Flex I/O 2), I11 (Flex I/O 3) or I12 (Flex I/O 4). The controller will support both N/O (press to make) and N/C (press to break) switch types for each Flex I/O input.

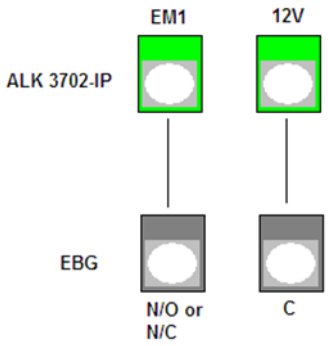
The Flex Outputs provide a negative triggered 12Vdc to each of the four Flex Output terminals (O9, O10, O11, O12).



The illustration on the left shows Flex Output configured on O9. The connection is 2-wire, between 12Vdc and O9. O9 providing a switched 0Vdc.

Connecting The Emergency Break Glass

The supply to the lock controller is connected in series with the EBG. This provides a physical break in the lock supply in the event of an emergency. The connections of the EBG vary depending upon the type used.



The wiring from the ALK3701–IP is as follows:

12V is connected to the common (or equivalent) of the EBG. The N/C (or equivalent) of the EBG is then connected to EM1 of the lock controller, the 12Vdc is then switched to the lock mechanism.

NOTE!!

If no EBG is fitted a hard wired connection must be made between 12V and EM1 to allow the lock to energise.

CHAPTER 4

CONFIGURATION

This chapter describes how to set up the ALK3701-IP for connectivity to the LAN and configure the attached hardware in its environment.

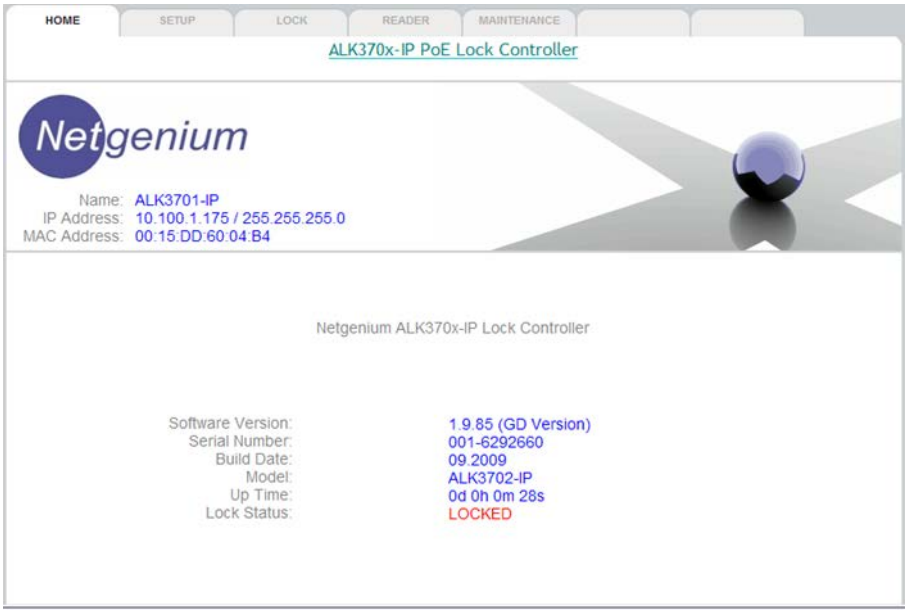
Initial Network Setup

Connect the ALK3071-IP to a POE capable network switch or via a mid-span device.

To logon for the first time, open a web browser and type the IP address of the panel in the address bar. Each unit is pre-configured with a default IP address of 10.100.1.175 when it leaves the factory. The default username and password are as follows:

Username: *Netgenium*
Password: *netgenium*

The home page provides basic information on the controller such as software version serial number etc. Navigation around the menu structure is via the tabs shown at the top of the home page. Each tab redirects the browser to the master page for the configuration section selected. In each section a sub menu is accessible via the links on the left of the page.



To set the controllers IP address:

Navigate to: Setup

Configure the options as described below then click the **Apply** button.

General

Device Name:	*The name for the device (usually a description of the location)*

Network

IP Address:	*IP address of the device*
Network Mask:	*Subnet Mask of the device*
Default Gateway:	*Default Gateway for the device*
Netgenium Primary PolicyServer:	*The IP Address of the primary PolicyServer*
Netgenium Secondary PolicyServer:	*The IP Address of the secondary PolicyServer*
Registration Mode:	*Autonomous or registered with PolicyServer*
Registration Status:	*Current registration status.*

DNS Settings

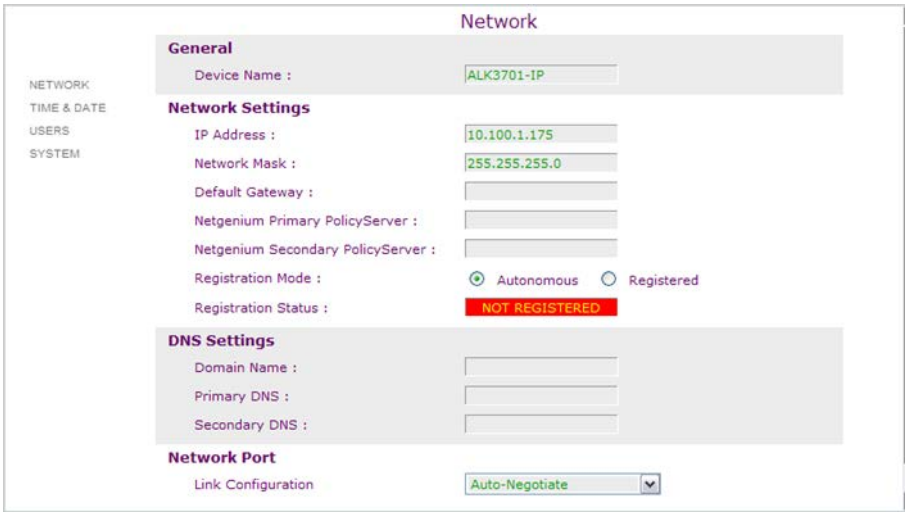
Domain Name:

Primary DNS:

Secondary DNS:

Network Port

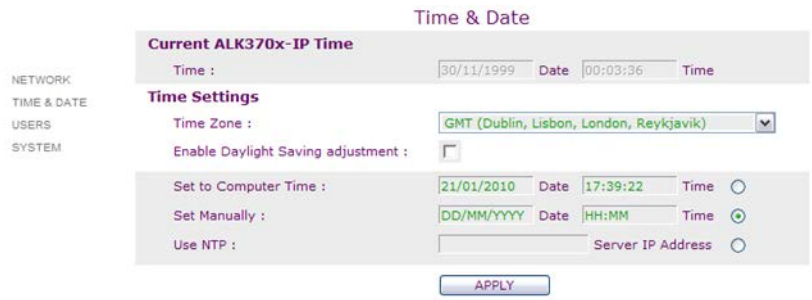
Link Configuration: *Set the speed and duplex settings of the network interface.*



If you have changed the IP address of the controller you will lose the connection to it. Open another browser session and reconnect the new IP address.

Time & Date

Navigate to: Setup>Time&Date



This page enables you to set the system time and date. The options are:

Set to Computer Time

This option sets the time and date to that of your computer when the Apply button is clicked.

Set Manually

Enter the time and date in the textboxes provided and click the Apply button.

Use NTP

With this option enabled the controller will synchronize its time and date with an NTP server every 5 minutes. Enter the IP Address of the NTP server and click the Apply button.

If the controller is configured to register with PolicyServer the unit will automatically be synchronised with PolicyServers date and time.

Users

Navigate to: Setup>Users

Use this page to manage the user accounts used to administer the unit. The default settings are:

Username *netgenium*

Password *netgenium*

To add a new user account, enter the username and password and click the Update button.

To remove an account, highlight the name to delete and click the Delete button.

System

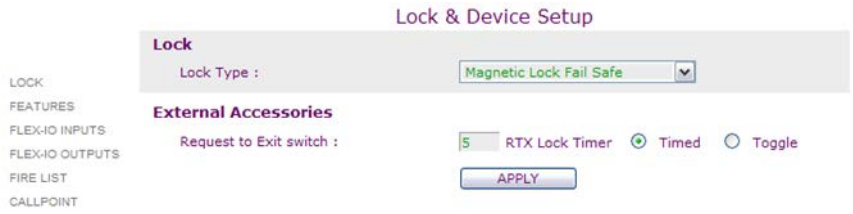
Navigate to: Setup>System

The system password is used to authenticate requests between PolicyServer and the end devices. The default setting is *netgenium*.

Lock

Accessing the Lock tab allows you to configure the type of locking hardware, door furniture inputs and features for the controller.

The initial screen allows you to setup the type of lock hardware connected to the controller.



Select the type of lock being used from the Lock Type dropdown list.

The options are:

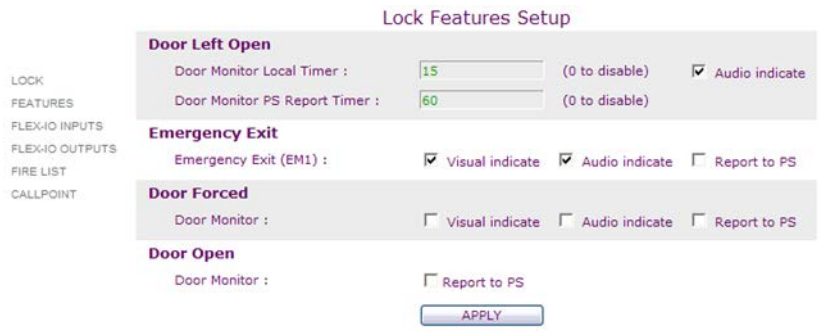
- Magnetic Lock Fail Safe
- Door Strike Fail Safe
- Door Strike Fail Secure
- Clean Relay Contacts

If one or more Request To Exit (RTX) switches are fitted, the behavior of the controller when the switch is pressed is configured here.

The switch can be configured to either toggle the status of the lock or open the lock for a number of seconds. Select the **Toggle** or **Timed** radio button and enter the number of seconds the door is to open during the timed operation. Click the **Apply** button.

Features

Navigate to: Lock>Features



The ALK370x family of lock controllers support a number of audio, visual and report features that can be enabled upon certain events at the door. The features are described below:

Door Left Open.

Providing the state of the door is monitored two events can be used to alert the fact a door has been left open. The audio/visual alert will make the attached card readers flash and beep when the door is open for more than the number of seconds entered in the Open Timer textbox. To disable the audio alert, un-tick the Enable Audio Indication checkbox.

A second option is to send an alert to PolicyServer, this can be configured instead of the audio/visual alert, or as a second stage in the procedure. To enable this alert, enter the number of seconds to elapse before the alert is sent (0 to disable).

Emergency Exit

Three alerts are available when the Emergency Exit switch is activated. Audio (attached reader(s) beep), visual (attached reader(s) flash) or server report.

To enable one or more of these events, place a tick in the appropriate checkbox.

Door Forced

The door forced condition occurs when the door is opened before the lock controller has released the locking mechanism. Therefore this alert is only available when the door state is being monitored.

Three alerts are available, audio (attached reader(s) beep), visual (attached readers flash) or server report.

To enable one or more of these events, place a tick in the appropriate checkbox.

Door Open.

A single alert (report to server) is available when the door is opened. To enable this alert place a tick in the Enable Reports to Server checkbox.

After enabling the features click the **Apply** button to make then active.

Flex IO Inputs

Navigate to: Lock>Flex-IO Inputs

There are 4 Flex I/O inputs available on the ALK3701-IP. Each input can be customized to perform one of seven functions.

These are:

RTX *-request to exit switch*

Callpoint

Fire Alarm Input *- connect to a volts free set of n/o or n/c relay contacts. When the fire alarm is activated the controller can be configured to unlock the door and notify devices on the network or the alert.*

Auxiliary Report *-sends an Auxiliary Report to PolicyServer which can be configured to react upon receipt.*

Door Monitor *- connects to a set of volts free relay contacts (n/o or n/c), monitoring the status of the door (open or closed)*

Door Override (lock) *- when activated, the controller will lock the door and ignore any command received until the condition is reset.*

Door Override (open) *- when activated, the controller will unlock the door and ignore any command received until the condition is reset.*

To configure a Flex I/O input, tick the Enabled checkbox and nominate either normally open (n/o) or normally closed (n/c) depending upon the contacts you are connecting to. Finally select the function the input is to perform from the Operation dropdown list.

When all of the inputs are configured click the **Apply** button.

Fire List

The fire list is used when one of the Flex I/O inputs is connected to a fire alarm. When the alarm is activated and a fire notification is sent to the devices in the Fire List database.

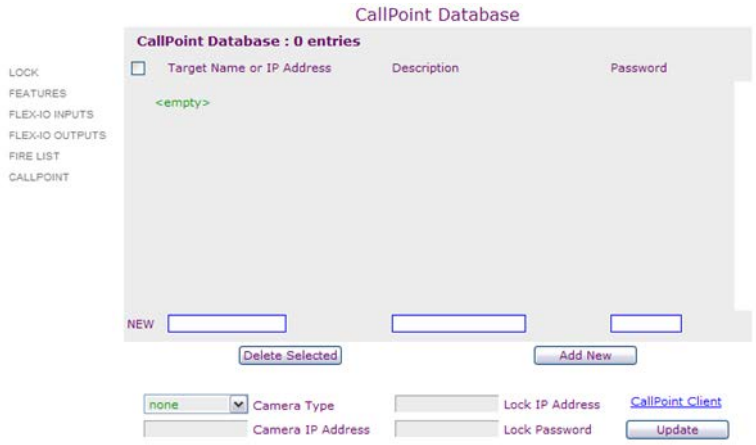
The database contains the IP addresses of the devices to be notified in the event of fire alarm activation. The database must be populated manually.

To add an entry to the Fire Device Database, enter the IP Address, a description and the system password of the device in the textboxes at the bottom of the page. Click the **Add New** button.

To delete an entry, highlight the entry and click the **Delete Selected** button.

CallPoint

The Callpoint list is used when one of the Flex I/O inputs is connected to an input to trigger the Callpoint application on one or more pc.



The database contains the IP addresses of the instances of Callpoint to be notified in the event of Callpoint activation. The database must be populated manually.

To add an entry to the database, enter the IP Address, a description and the system password of the device in the textboxes at the bottom of the page. Click the **Add New** button.

To delete an entry, highlight the entry and click the **Delete Selected** button.

Utilities

The Utilities configuration page allows IP Events to be created and edited . Once configured the events can be invoked in a failover situation, should PolicyServer become unreachable.

This maintains functionality of the system until the server has been restored.

The events target endpoint is identified as an IP address and Layer 4 Port and can in either tcp or udp format.

The packet payload can contain any data, although short cuts exist for commands to Netgenium devices.

Add An Event

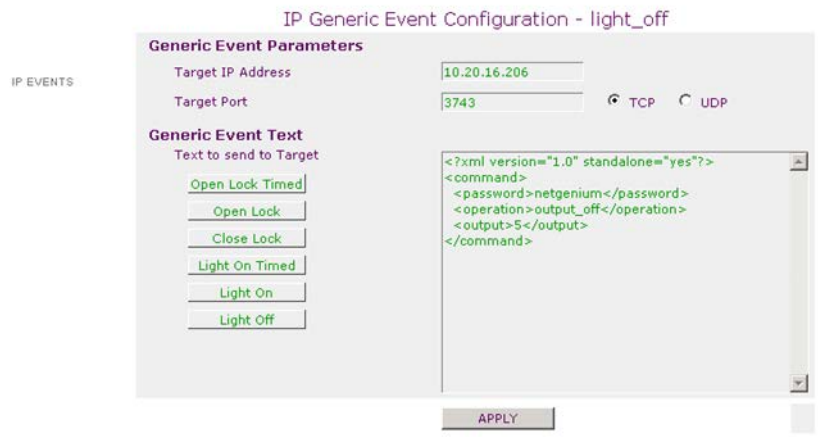
Navigate to: Utilities

1. *Enter the Target IP address, select tcp or udp format and enter the port number you require the event to use.*

2. *Click the **ADD NEW** button.*

The new event is now added to the configuration database. In its current state the event contains no event data. You must edit the event to add the data to be included in the packet.

Edit An Event



Select the Event to be edited from the Select Existing Event: dropdown list and click the **EDIT** button.

Enter the data the event packet is to contain. The data can be typed into the textbox as shown.

The example illustrated shows an event in XML format.

Shortcuts to Netgenium commands can be used by clicking the appropriate button to the left of the textbox.

Click the **APPLY** button.

CHAPTER 5

MAINTENANCE & DIAGNOSTICS

Selecting the Maintenance in the configuration window provides data on the current status of the ALK3701-IP's features, the ability to test each function of the controller remotely and the ability to upgrade the firmware of the controller.

Status

Provides the following data:

Lock Status. *Show the current status of the lock port of the controller (Locked/Unlocked).*

Door Status *Shows the current status of the door, as indicated by the contacts monitoring door status (if connected).*

Emergency Exit Status	*Shows the current status of the Emergency Exit break Glass.*
Request to Exit Status	*Shows the current status of any RTX switches connected to Flex I/O.*
Auxiliary Status	*Shows the current status of any Auxiliary Inputs connected to Flex I/O.*
Fire Status	*Shows the current status of any fire alarm inputs connected to Flex I/O.*
CallPoint Status	*Shows the current status of any callpoint triggers connected to Flex I/O.*
Statistics	*Shows two figures, the number of times the lock hardware has been operated and the number of times the door has been opened.*

Diagnostics

Navigate to: Maintenance>Diagnostics

The diagnostics page allows you to simulate any condition at the door remotely. The following diagnostic functions are available:

Lock Test

Simulate the Timed and Toggle operation of the lock port. Click the appropriate button to use this feature.

RTX

Simulates the Request To Exit button being pressed (if configured).

Callpoint

Simulates Callpoint being triggered (if configured).

Auxiliary

Simulates the Auxiliary input being triggered (if configured).

Fire

Simulates the fire alarm input being triggered (if configured).

Logs

Navigate to: Maintenance>Logs

The controller logs events in a temporary buffer for diagnostic purposes. This buffer is stored in volatile memory and is lost when the unit is powered off.

To clear the buffer manually, click the **Clear Logs** button.

Default

Navigate to: Maintenance>Default

Clicking the **DEFAULT** button will return the controller to factory default settings.
Clicking the **REBOOT** button will reboot the controller.

Update Firmware

Navigate to: Maintenance>Update Firmware

The firmware can be updated via a TFTP server. To update the firmware:

1. A TFTP server must be available on the network.
3. The ALK370x image should be stored in the TFTP root directory.
4. Tick the Enable TFTP Upload check box.
5. Enter the IP address of the TFTP server.
6. Click the Start Upload Process button.

The upload process will begin. The current status of the upload process is displayed in the Live Status window. The correct upload

- Uploading File
- Writing Main Image
- Writing Header
- Rebooting

Ensure the controller is not rebooted and the network connection to the TFTP server remains intact during the upload process.

If you see the message "Problem writing image to flash" in the Live Status window. The upload process has failed

Reboot the controller and start again.

Do not repeat the upload process without a reboot.