



DI-View ***Power and Environmental Monitoring***

User Guide
Version 1.0.1

Conventions Used in this Manual

This manual uses the following typographic conventions:

Table 1-1. Typographic Conventions

<i>italics</i>	Items as seen on screen, field names, menu names, button text etc.
bold	Indicates items that require special emphasis.
fixed	Inputs by the user that must be typed exactly as they appear.
{somevalue}	Italics surrounded by curly braces indicate a user supplied entry that must be input. E.g.: {drive} : \setup
<ctrl+alt+delete>	Text surrounded by angled brackets indicate specific keys to be pressed. Use of the + sign in combination indicate that keys should be pressed together.

Note! *Information of note may be presented like this.*

Warning! *These messages alert you to specific procedures or practices; serious consequences may result including injury if you disregard them.*

About this Manual

This manual is intended to document the DI-View product.

Throughout this document it is assumed that the user has a basic to intermediate knowledge of IT and Networking concepts.

Further information regarding IT and Networking fundamentals may be found in the appendices of this document.

Copyright © 2006-2009 Unite Technologies Ltd.
Unauthorised reproduction prohibited.

Table of Contents

1	Introduction	6
2	DI-View Package.....	7
3	Initial Setup	13
4	Web Management Interface.....	22
5	LDAP	46
6	Troubleshooting	50
7	Appendix A: Technical Details.....	51
8	Appendix B: Hysteresis Demystified	52
9	Appendix C: Networking Reference	54
10	Appendix D: DI-VIEW Sensor Connection Diagramm	55
11	Appendix E: DI-VIEW Sensor Usage Information	56

1 Introduction

Overview

The DI-View is a compact device used to monitor up to 2 power strips within a rack enclosure, along with two input sensors (2x Temp or 2x Humidity or 2x Digital, or a combination of two sensors).

The unit comprises both an SNMP interface and a secure web based interface for monitoring and management.

Some of the main features of the DI-View unit are:

- Secure web management and configuration interface.
- SNMP enabled.
- Two monitoring channels.
- Monitoring of up to two PDUs.
- Optional LCD Status module.

DI-View Applications

Remote Temperature and Humidity Sensing

IT equipment has always demanded high standards of the datacentre environment; temperature and humidity ideally need to be kept within strict limits. However, not all network equipment is situated in an ideal environment. DI-View has the capability to monitor temperature and humidity and raise alarms or take action if a user-configured threshold is crossed.

PDU Monitoring

All IT equipment requires electrical power to function. DI-View via intelligent PDUs allows around-the-clock monitoring of the electrical power environment of the rack.

2 DI-View Package

Package contents

The standard DI-View package contains a DI-View unit with supporting hardware:

Table 2-1. Package contents

1 DI-View Unit.
2 DI-View Sensors incl. Cables
12v power supply with localised mains connector.
Rack mounting kit.

Front of DI-View Unit

The following images show the front panels of the DI-View unit:



Figure 2-1. Front of DI-View.

LEDs

Four LEDs can be found on the front of the DI-View MCU. Their purpose is described below.

Pwr: Illuminates when unit is powered.

Status: Indicates system activity.

Alarm-1: Analogue Alarm (e.g. Temperature, Humidity or Voltage).

Alarm-2: Digital Alarm (e.g. Open / Close contact switch).

Network Link (green):

Embedded in RJ45 ethernet connection. Illuminates when Ethernet link is established.

Network Activity (amber):

Flashes when network activity occurs.

Buttons

Also found on the front of the DI-View MCU are two buttons, their functions are described below.

Reset: Allows the user to reboot the unit.

Mode: The mode select switch is used to reset the unit to factory defaults. See the Troubleshooting section for details.

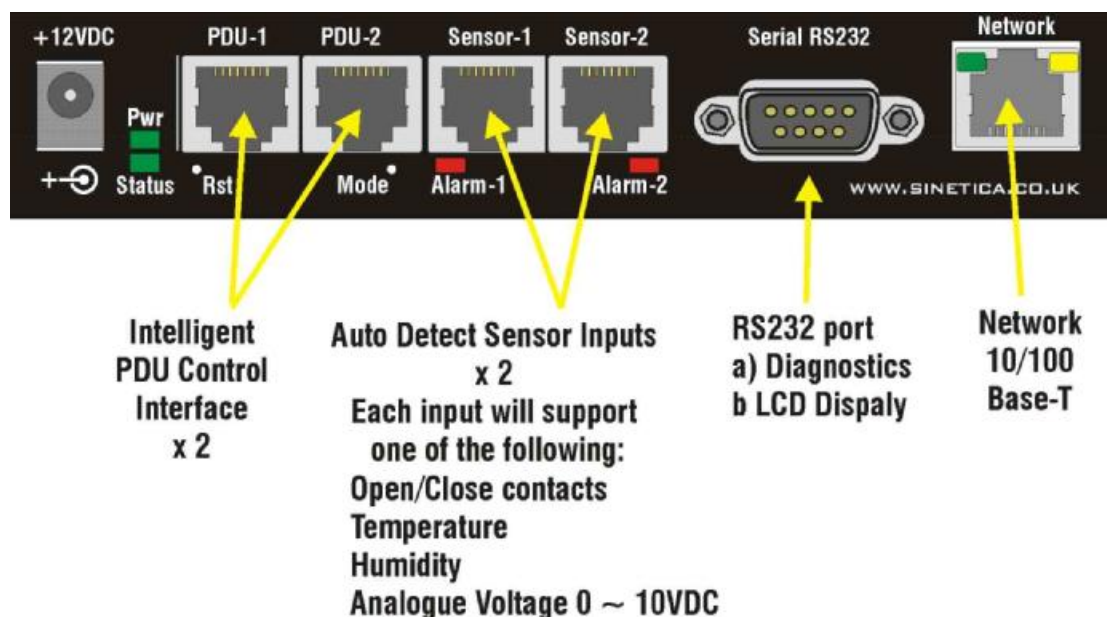


Figure 2-2. Diagram of DI-View MCU.

- +12v:** Connection for 12v power supply unit (supplied).
- PDU-1:** PDU 1 is connected here.
- PDU-2:** PDU 2 is connected here.
- Sensor-1:** Temperature, Humidity, Analogue or Contact sensor 1 is connected here.
- Sensor-2:** Temperature, Humidity, Analogue or Contact sensor 2 is connected here.
- DB-9:** Optional devices such as the LCD Status Monitor unit may be attached here.
- Network**
- Connector:** An RJ-45 connection provides Ethernet and Fast Ethernet connectivity to the DI-View MCU.

Installation Requirements

- DI-View unit.
- 12v DC Power supply (supplied).
- Ethernet or Fast Ethernet network connection.
- Network connected computer system to setup the DI-View MCU.

Rack – Mounting

This section covers the basic 19-inch rack-mounting of the DI-View.

Equipment Required

You need to supply a number-1 and a number-2 Phillips screwdriver to rack-mount the DI-View

Before You Begin

When determining where to install the DI-View, please verify that these guidelines are met:

- Airflow around the DI-View is unrestricted
- Clearance to the front and rear panels meet these conditions:
 - Front-panel LEDs can be easily read
 - Access to ports is sufficient for unrestricted cabling
- AC power cord from the power supply can reach the AC power outlet and that the DC lead can reach the DI-View
- The 10/100 network cabling does not exceed 100 meters from the DI-View to the Network switch
- Temperature around the DI-View does not exceed 40 deg.C
- Humidity around the DI-View does not exceed 90 percent

Installation Warning Statements

This section includes the basic warning statements.

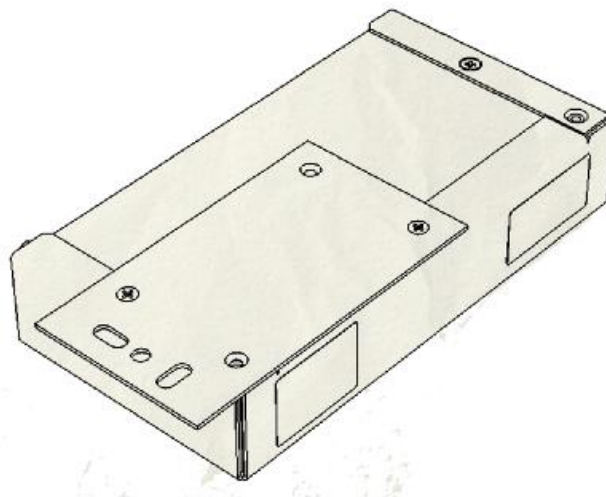
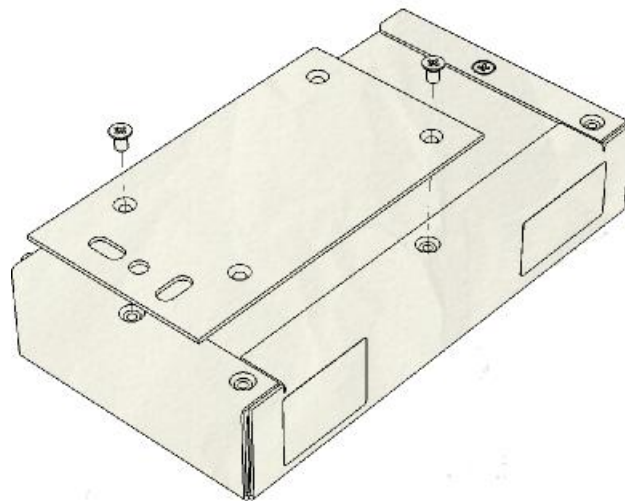
- Only trained and qualified personnel should be allowed to install, replace or service this equipment
- To prevent the DI-View from overheating, do not operate in an area that exceeds the maximum recommended ambient temperature of 40 deg.C
- Installation of the DI-View must comply with local and national electrical codes
- To prevent personal injury when mounting or servicing the DI-View, you must take care to ensure the system remains stable.

- The rack or cabinet should be adequately secured to prevent it from becoming unstable and/or falling over.
- **Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable earthing of rack mounted equipment should be maintained.** Particular attention should be given to supply connections other than direct connections to the branch circuit (i.e. use of power strip etc)

Attaching the Brackets

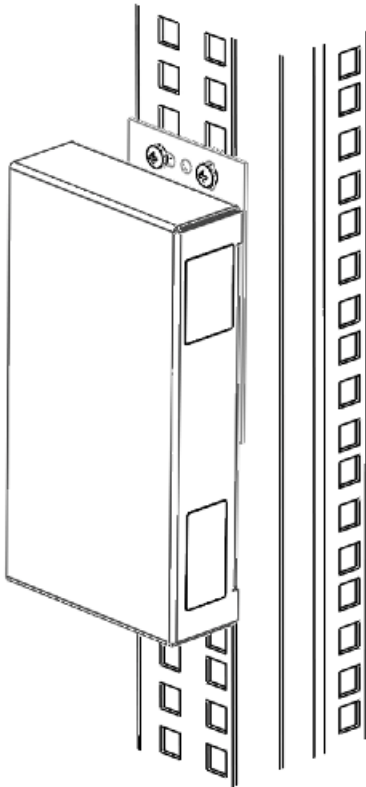
First decide in which orientation the DI-View is to be mounted in the rack or cabinet.

Using a Phillips number-1 screwdriver, remove the two screws from the bottom of the DI-View. Place the mounting bracket on the base of the DI-View and secure using the two screws.



Rack-Mount the DI-View

Hold the DI-View and attached the bracket to rack using two 12-24 screws.



3 Initial Setup

Default Settings

The DI-View unit in factory default condition will have the following network configuration. Advanced users may wish to make use of these settings to access the DI-View units web management interface immediately and proceed with configuration.

Users who do not know how to do this should proceed through this chapter for information on how to configure the DI-View unit.

Table 3-1. DI-View Defaults

IP Address:	192.168.0.253
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Web Management Address:	http://192.168.0.253/
Default username:	admin
Default password	admin

Note! ***Password entries are case sensitive!***

Connecting to the Web Management Interface

The DI-View monitoring solution can be configured entirely using the built in web management interface.

In order to connect to the web management interface for the first time the IP address of the PC to be used may need to be changed.

This section will detail how to connect to change the IP address and connect to the web management interface.

Changing your PCs IP address

Note! *Instructions refer specifically to Windows XP Professional. Please refer to your operating system documentation if you are not using Windows XP Professional.*

- 1) On Windows XP Start menu <**Right Click**> on **My Network Places** then right click on **Properties**. This can be seen in Figure 3-1. My Network Places.

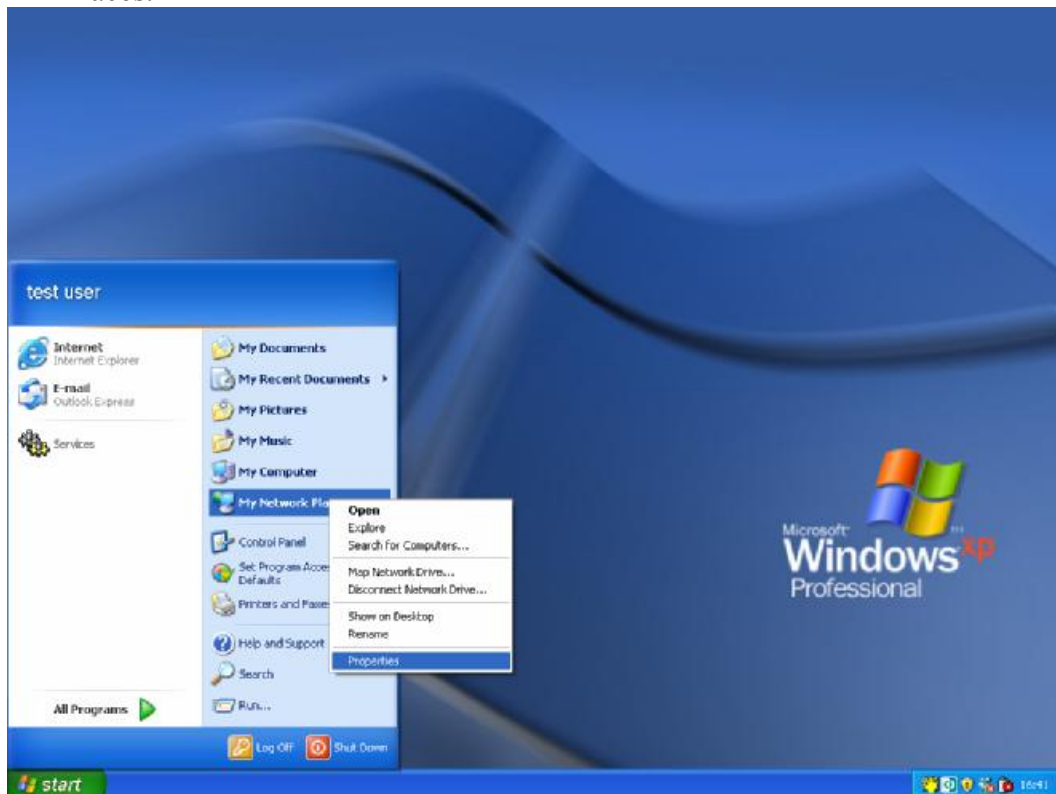


Figure 3-1. My Network Places

- 2) The Network Connections window will appear as shown in Figure 3-2.
Network Connections window

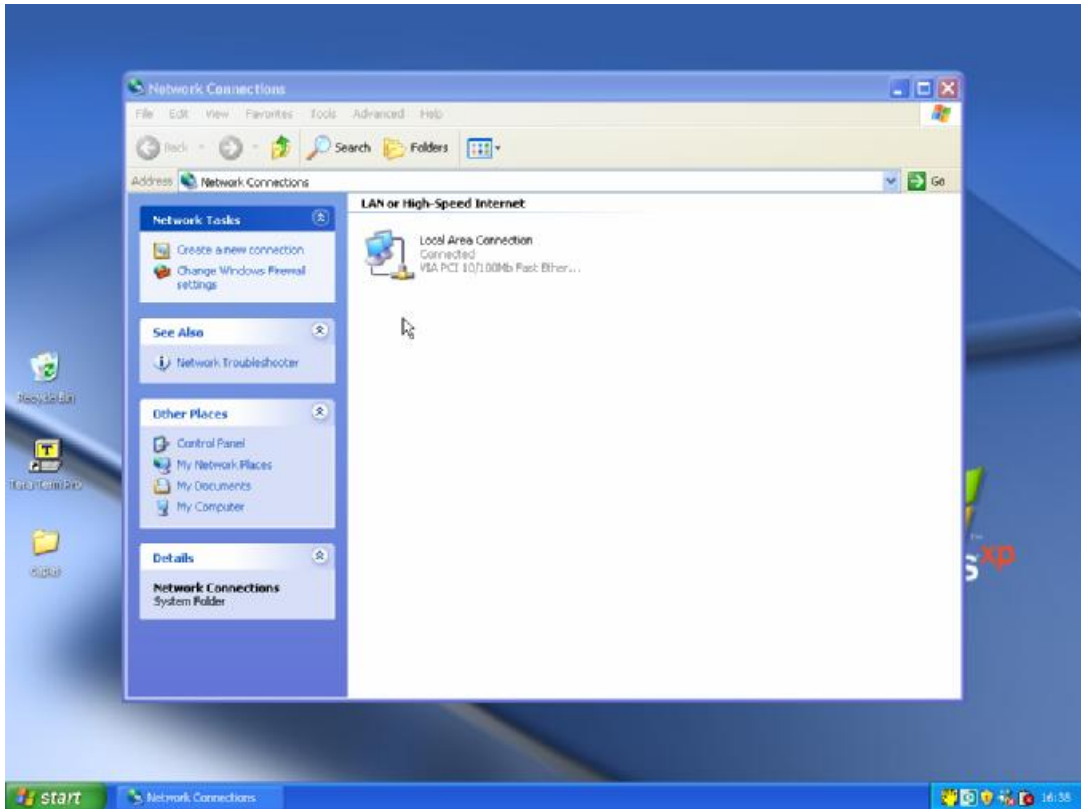


Figure 3-2. Network Connections window

- 3) **<Right Click>** on Local Area Connection and click on **Properties**. This will open the Local Area Connection Properties window as shown in Figure 3-3.
Local Area Connection Properties window.

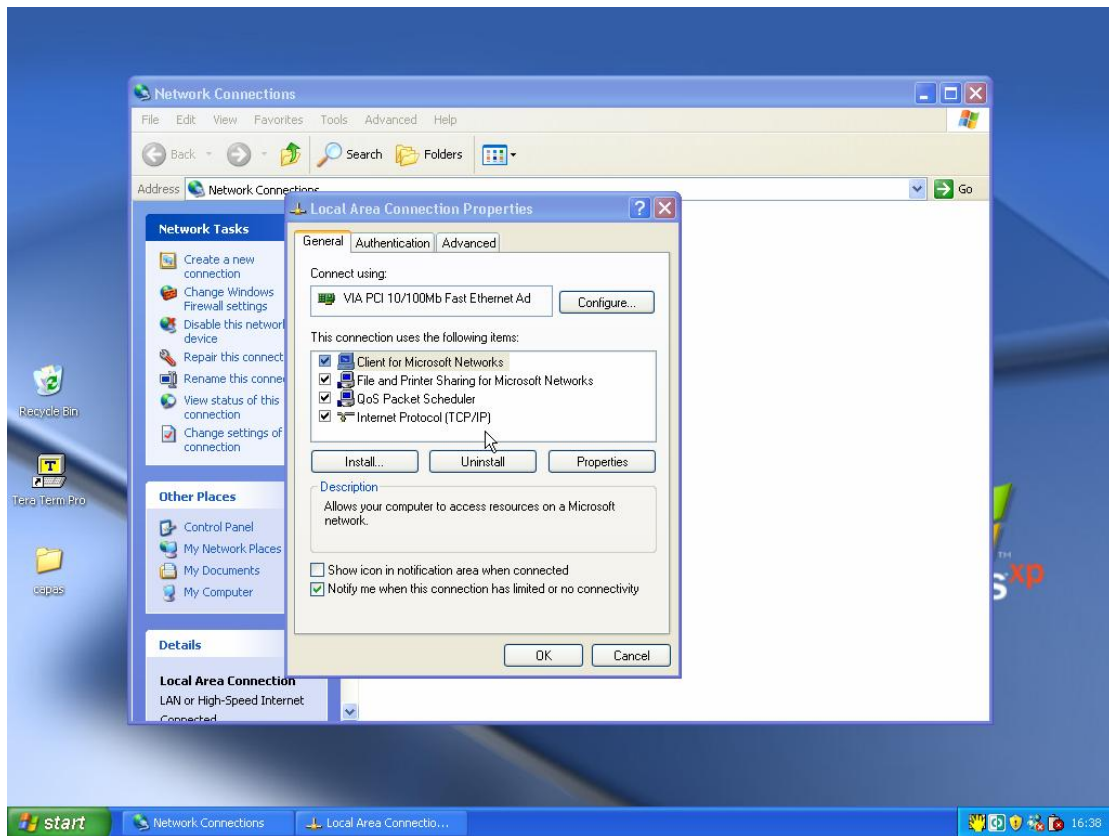


Figure 3-3. Local Area Connection Properties window.

- 4) Select **Internet Protocol (TCP/IP)** (you may need to scroll down). Click the **Properties** button.
- 5) Select **Use the following IP address** and **Use the following DNS server addresses** radio buttons. Proceed to enter the following details into the appropriate boxes. (This can be seen in Figure 3-4. Internet Protocol (TCP/IP) Properties screen)

IP address: 192.168.0.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.0.1

Preferred DNS server: 192.168.0.1

Click **OK** to accept the entries.

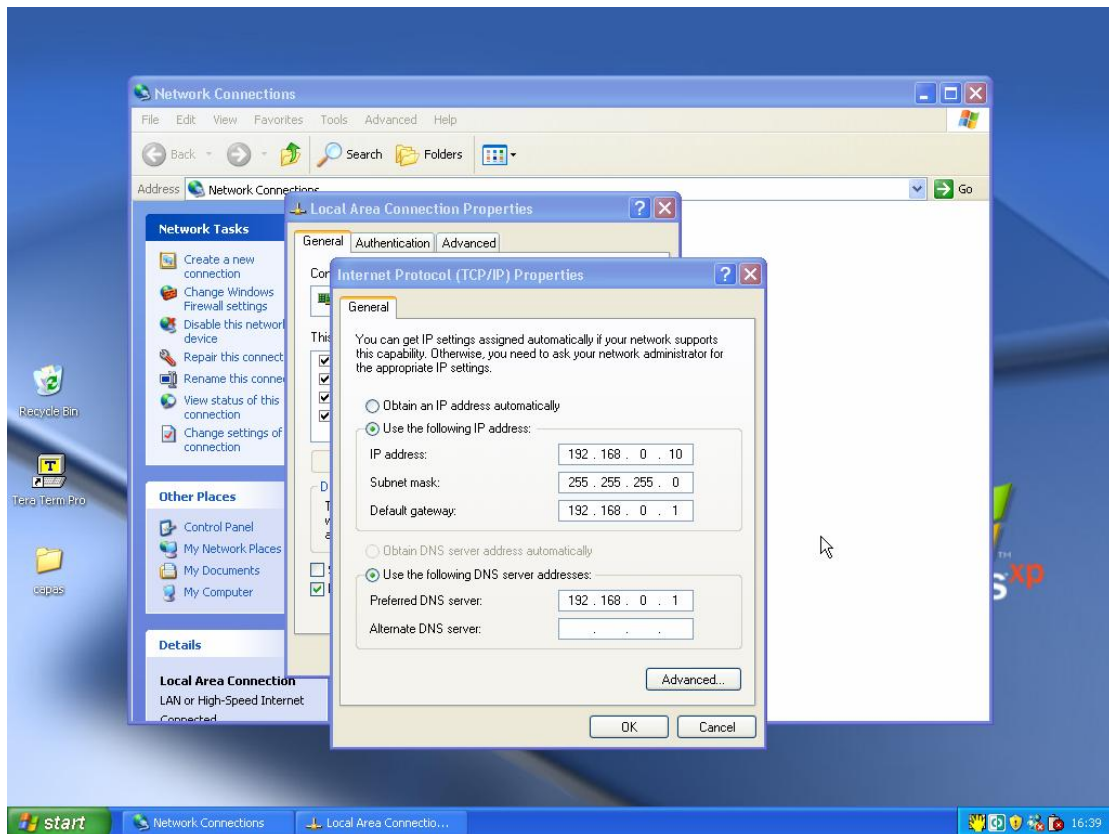


Figure 3-4. Internet Protocol (TCP/IP) Properties screen

- 6) On the Local Area Connection Properties Click **OK** to return to the desktop.

Congratulations you have just changed your IP address and can now proceed with the next stage of the DI-View Rack Monitor setup.

Connecting to the web management interface

- 1) Connect the DI-View MCUs network connection directly to a PCs Ethernet network card using a **crossover cable**.

Note! ***A crossover cable must be used when directly connected the DI-View MCU to a PCs network card.***

- 2) Power the DI-View unit.
- 3) Open a web browser.
- 4) Enter into the address bar `http://192.168.0.253`
- 5) The Web Management Interface will now load.



Figure 3-5. Web Management Interface login screen.

6) Click login and enter the username and password. The unit defaults are:-

Default username:	admin
Default password	admin

Table 3-2. Default Passwords.

Note! Password entries are case sensitive!

Initial network setup

This section provides details on preparing the unit for network access and allowing SNMP network management.

Connection to the web management interface is required.

Entering NMS details

- 1) Click the **Network Setup** tab on the top menu bar then select the **SNMP NMS** button found on the left menu bar.

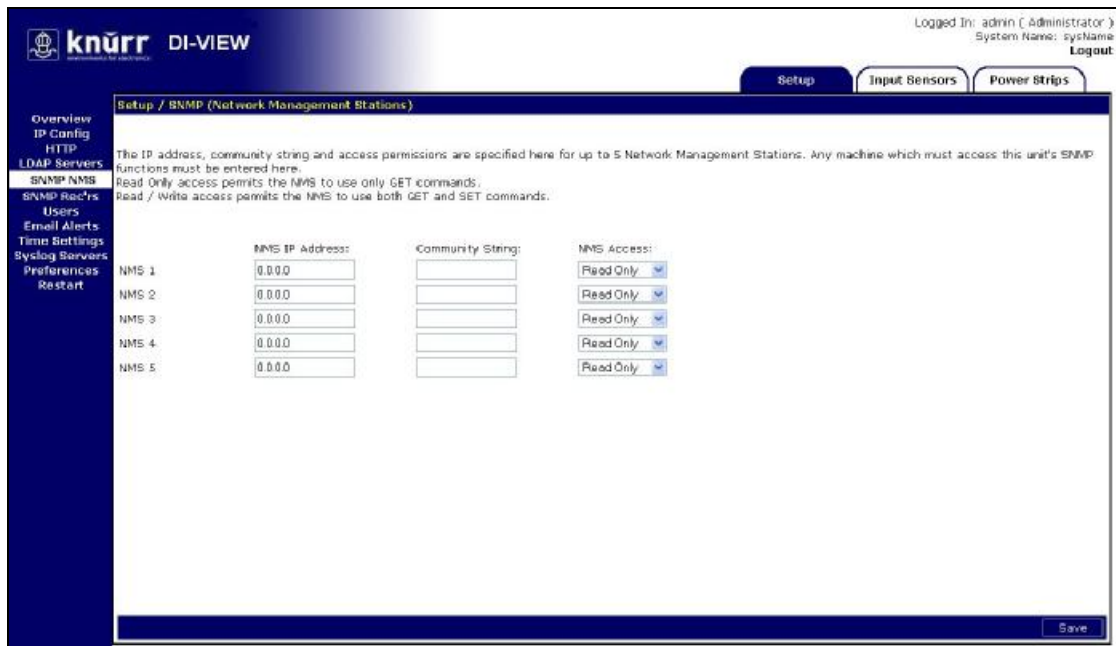


Figure 3-6. SNMP NMS Setup.

- 2) Input the IP address, chosen community string and required NMS access permissions of the Network Management Stations to be used.
- 3) Click **Save** to confirm the changes.
- 4) To disable an NMS the **Disabled** entry should be selected from the **NMS Access** drop down list.

Entering Trap Receiver details

- 1) Click the **Network Setup** tab on the top menu bar then select the **SNMP Rec's** button found on the left menu bar.

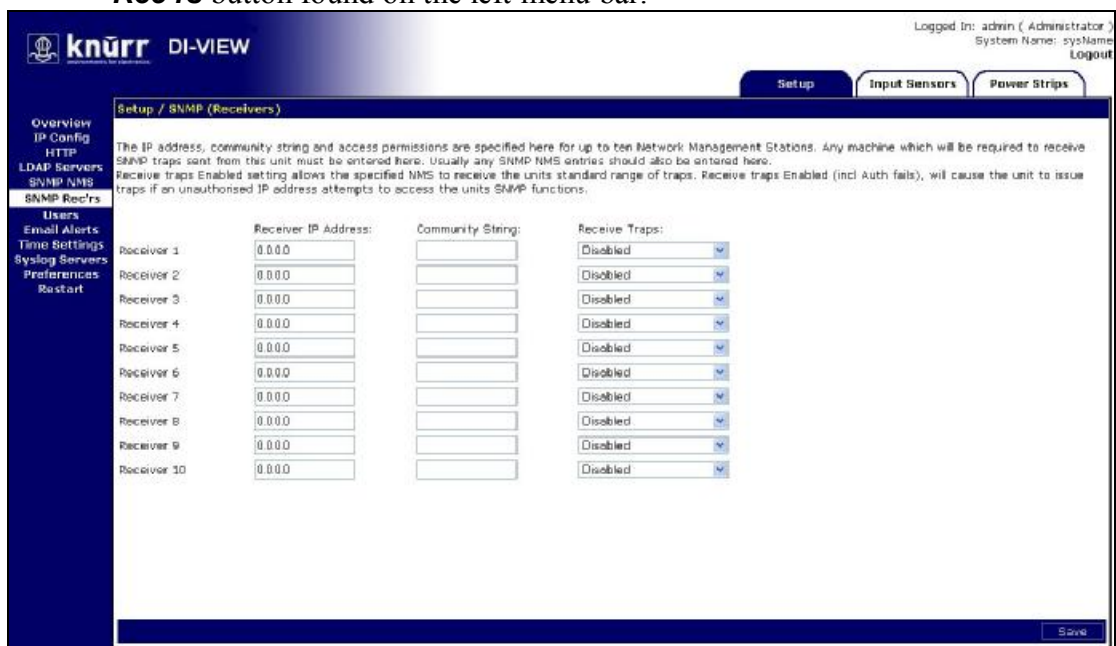


Figure 3-7. Trap Receivers setup

- 2) The IP address, chosen community string and required trap types should be entered for the Network Management Stations to be used.
- 3) Click **Save** to confirm the changes.

Adding users

- 1) Click the **Network Setup** tab on the top menu bar then select the **Users** button found on the left menu bar.

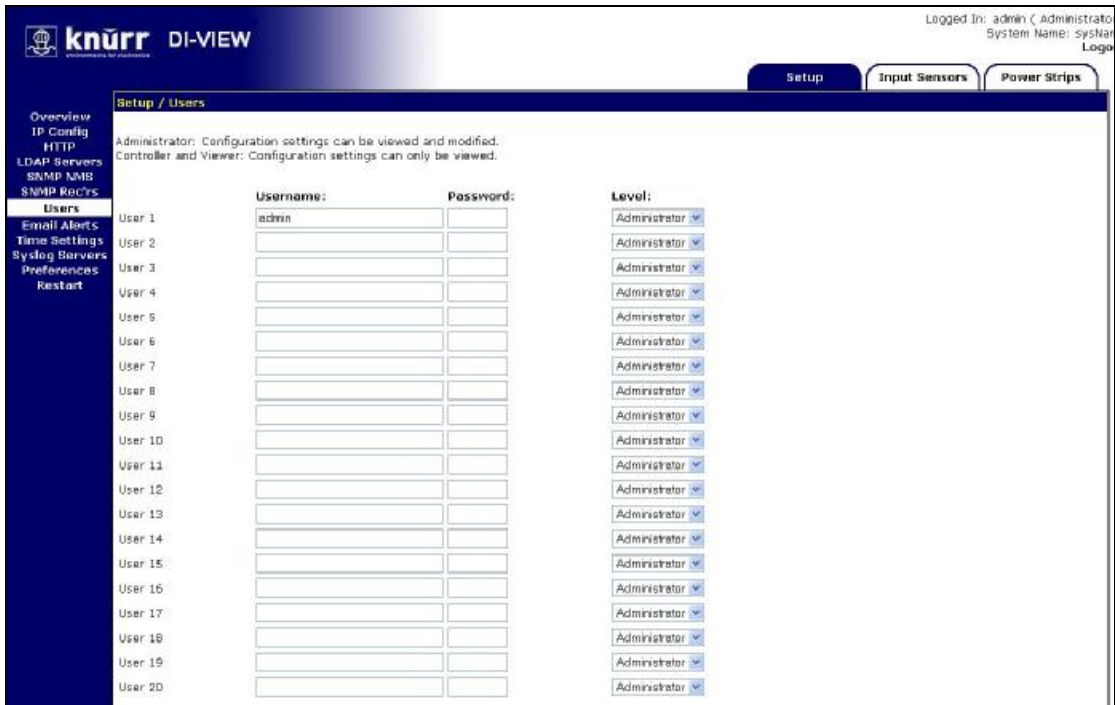


Figure 3-8. User menu

- 2) Usernames, passwords and access levels can be set here. Unique usernames can be set for individuals who require web management access to the DI-View unit.
- 3) Click **Save** to confirm the changes.

Changing the unit IP address

- 1) Click the **Network Setup** tab on the top menu bar then select the **Users** button found on the left menu bar.

knürr DI-VIEW

Logged In: admin (Administrator)
System Name: sysName
LOGOUT

Setup / IP Configuration

Network settings for this unit are set here. This will be the IP address that is used to access the web management interface and by a Network Management Station.

System Name:

IP Address:

Subnet Mask:

Gateway:

Config. Protocol:

Save

Figure 3-9. IP Configuration

- 2) The IP address, subnet mask and gateway that the DI-View will use must be entered here.

Contact your network administrator if you do not know the values that you must enter here.

- 3) Click **Save** to confirm the changes.
- 4) Click **Restart** and select **Restart Now** to reboot the unit and bring the changes into effect.

Note! *Once the IP configuration has changed the DI-View unit will no longer be accessible via the default IP address as the new address will be operational.*

- 5) The DI-View unit should now be connected to the main network and any further required configuration done via the units new IP address.

4 Web Management Interface

The DI-View unit has a built in Web Management interface which can be accessed securely. The interface permits complete configuration and monitoring of the DI-View unit.

Pages where changes can be made have a **Save** button in the lower right hand area. This must be pressed to action and save any changes made.

Network Setup - Overview

The Overview page is the first page displayed and provides the user with an overview of the DI-View units current status.



The screenshot displays the 'Network Setup / Overview' page of the DI-View web management interface. The page features a dark blue header with the 'knürr DI-VIEW' logo and navigation tabs for 'Setup', 'Input Sensors', and 'Power Strips'. A left-hand navigation menu lists various system settings. The main content area displays the following system details:

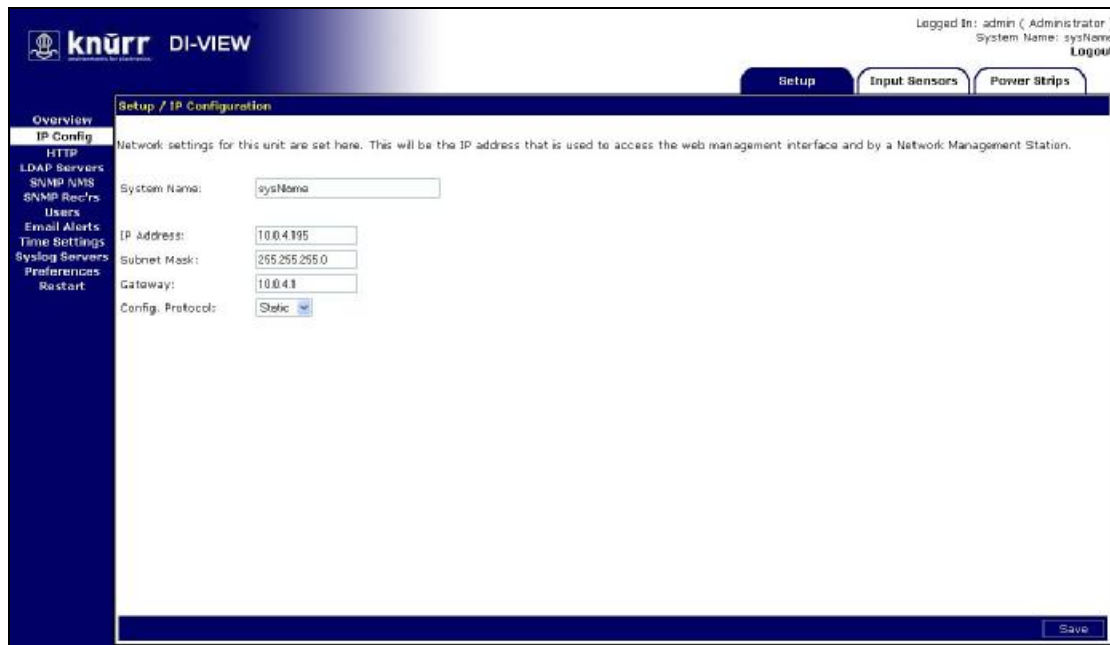
System Name:	sysName
System Location:	sysLocation
System Contact:	sysContact
MAC Address:	00:07:0e:03:01:58
Serial Number:	00344
Firmware Version:	1.05.03
Hardware Revision:	ZBBNC2 Rev 1.01.06
System Uptime:	0 days, 3 hours, 33 mins, 57 secs
IP Address:	10.0.4.195
Subnet Mask:	255.255.255.0
Gateway:	10.0.4.1
Config. Protocol:	Static
Logged In User:	admin
Access Level:	Administrator

Figure 4-1. Overview screen

System name, MAC address, serial number, firmware version and a selection of other system details can be found here.

Network Setup - IP Configuration

The IP Config page permits setting of the DI-View units own management IP address.



The screenshot displays the 'Setup / IP Configuration' page in the Knürr DI-View web interface. The page is titled 'Setup / IP Configuration' and includes a navigation menu on the left with options: Overview, IP Config, HTTP, LDAP Servers, SNMP MIBs, SNMP Reclrs, Users, Email Alerts, Time Settings, Syslog Servers, Preferences, and Restart. The main content area shows the following fields and values:

Field	Value
System Name	sysName
IP Address	10.0.4.195
Subnet Mask	255.255.255.0
Gateway	10.0.4.1
Config. Protocol	Static

A 'Save' button is located at the bottom right of the page.

Figure 4-2. IP Configuration

System Name

System name may be specified here. This would normally be the fully qualified domain name (FQDN) of the device but this is not enforced.

The value specified here can be retrieved by interrogating the 'sysName' node via SNMP.

This allows SNMP management platforms to obtain unique names for units where specified.

This value has no effect on network communications and the unit will function correctly with or without a value.

IP Address

A standard IP address may be entered here. The address is entered in dotted decimal format.

Eg: 192.168.0.44 or 22.10.45.33

The address entered here will be the address by which the DI-View unit is accessed and managed.

Subnet Mask

The subnet mask is used to determine what part of the IP address is the network portion and what part is the host portion.

It is often 255.255.0.0 or 255.255.255.0 however correct setting is essential for correct operation.

The subnet mask is entered in dotted decimal format.

Eg: 255.255.255.0 or 255.255.224.0

Gateway

The gateway setting specifies the IP address of the machine/router which the DI-View unit uses to communicate with different networks.

The gateway address is entered in dotted decimal format.

Eg: 192.168.0.1 or 11.2.24.103

Most networks will have a gateway and correct setting is important for correct network communications.

Note! ***Once IP Configuration options are entered and Save is pressed the changes will take effect. If incorrect entries are made this may result in loss of communication.***

In this event the best course of action is to reset the DI-View units network configuration.

Details of how to do this can be found in the Troubleshooting section.

Network Setup - HTTP

Access method for the web management interface is selected here.

Both HTTP and HTTPS access modes are available by default. Selecting the HTTPS radio button will allow only HTTPS configuration.

Use of HTTPS is recommended for security as connections will be encrypted.

Additionally the TCP port for connection to the Web Management Interface can be specified here.

Note! **Selecting HTTP or HTTPS requires a reboot to take effect.**

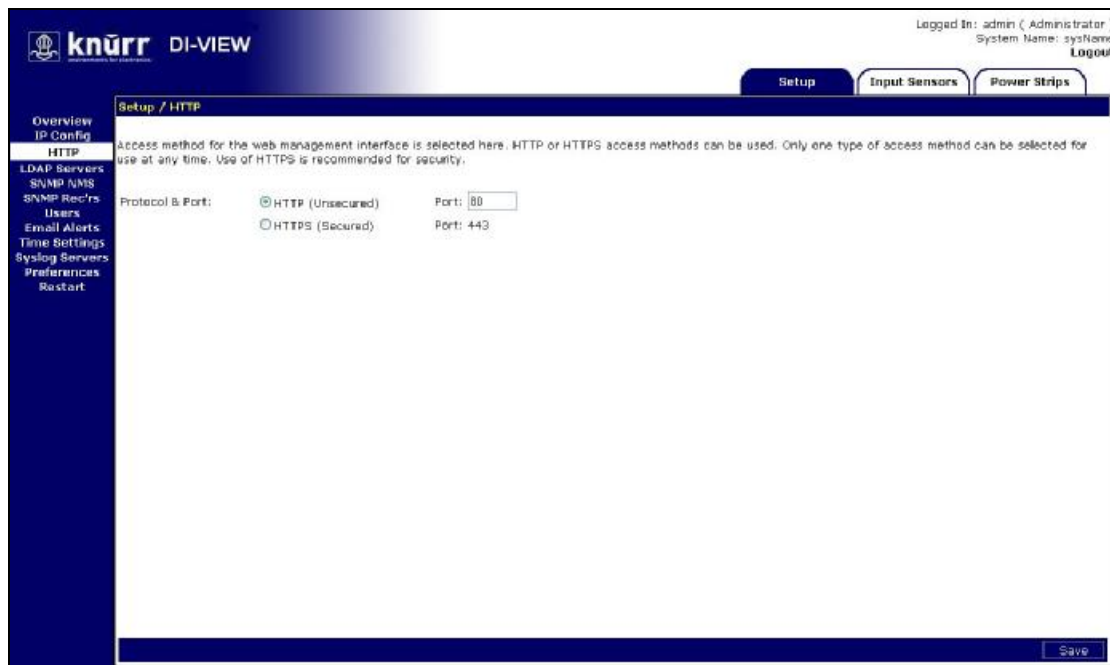


Figure 4-3. HTTP Setup

Network Setup – LDAP Servers

Lightweight Directory Access Protocol (LDAP) configuration options are specified here.

See Section 0
LDAP (Page 46) for configuration details.

The screenshot shows the 'Setup / LDAP Servers' configuration page in the knürr DI-VIEW interface. The page is titled 'Setup / LDAP Servers' and includes a sidebar with navigation options like Overview, IP Config, HTTP, LDAP Servers, and others. The main content area shows configuration fields for 'Enabled' (set to Disabled), 'Credential Cache' (10 Minutes), and sections for 'Primary LDAP Server' and 'Secondary LDAP Server', each with fields for Display Name, IP Address, Unit Base DN, Users Base DN 1, and Users Base DN 2. A 'Save' button is at the bottom right.

Figure 4-4. LDAP Setup

Configuration options for a Primary and Secondary server are provided with identical configuration choices offered.

Enabled

Disabled

No LDAP servers will be queried to verify user login credentials access and privileges. Only internal users will be able to login.

Primary

Only the Primary LDAP Server specified will queried to verify user login credentials access and privileges.

Secondary

Only the Secondary LDAP Server specified will queried to verify user login credentials access and privileges.

Both

Both LDAP Servers specified will queried (with priority given to the Primary) to verify user login credentials access and privileges.

Credential Cache

Specifies how long (in minutes) users successfully authenticated via LDAP will be allowed to access the unit without re-authenticating against LDAP.

Display Name

A display name for the specified LDAP server can be specified here. Display Name is for reference and logging purposes and has no direct affect on LDAP function.

IP Address

The IP address of the LDAP server is specified here.

Unit Base DN

The Distinguished Name (DN) of the directory object containing the DI-View LDAP authentication structure must be provided here. This field is required for LDAP function.

See Section 0

LDAP (Page 46) for configuration details.

Users Base DN 1

The Distinguished Name (DN) of the directory object containing directory users for authentication is specified here.

This field is required for LDAP function.

See Section 0

LDAP (Page 46) for configuration details.

Users Base DN 2

The Distinguished Name (DN) of the directory object containing directory users for authentication is specified here.

This field is optional for LDAP function providing Users Base DN 1 has been specified.

See Section 0

LDAP (Page 46) for configuration details.

Network Setup - SNMP NMS

The IP address, community string and access permissions are specified here for upto 5 Network Management Stations.

Any machine which must access this unit's SNMP functions must be entered here.

Logged In: admin (Administrator)
System Name: sysName
Logout

Setup / SNMP (Network Management Stations)

The IP address, community string and access permissions are specified here for up to 5 Network Management Stations. Any machine which must access this unit's SNMP functions must be entered here.
Read Only access permits the NMS to use only GET commands.
Read / Write access permits the NMS to use both GET and SET commands.

	NMS IP Address:	Community String:	NMS Access:
NMS 1	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="button" value="Read Only"/>
NMS 2	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="button" value="Read Only"/>
NMS 3	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="button" value="Read Only"/>
NMS 4	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="button" value="Read Only"/>
NMS 5	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="button" value="Read Only"/>

Save

Figure 4-5. SNMP NMS

IP Address

The IP address of the NMS machine should be entered here.

Community String

The required community string must be entered here. The default for many devices is **public**.

It is recommended that the community string be changed as it is effectively an access password.

NMS Access

Read Only access permits the NMS to use only GET commands.

Read / Write access permits the NMS to use both GET and SET commands.

Network Setup - SNMP Trap Receivers

The IP address, community string and access permissions are specified here for upto ten Network Management Stations.

Receiver	Receiver IP Address:	Community String:	Receive Traps:
Receiver 1	0.0.0.0		Disabled
Receiver 2	0.0.0.0		Disabled
Receiver 3	0.0.0.0		Disabled
Receiver 4	0.0.0.0		Disabled
Receiver 5	0.0.0.0		Disabled
Receiver 6	0.0.0.0		Disabled
Receiver 7	0.0.0.0		Disabled
Receiver 8	0.0.0.0		Disabled
Receiver 9	0.0.0.0		Disabled
Receiver 10	0.0.0.0		Disabled

Figure 4-6. SNMP Trap Receivers

IP Address

Any machine which will be required to receive SNMP traps sent from this unit must be entered here. Usually any SNMP NMS entries should also be entered here.

Community String

The required community string must be entered here. The default for many devices is **public**.

It is recommended that the community string be changed as it is effectively an access password.

Receive Traps

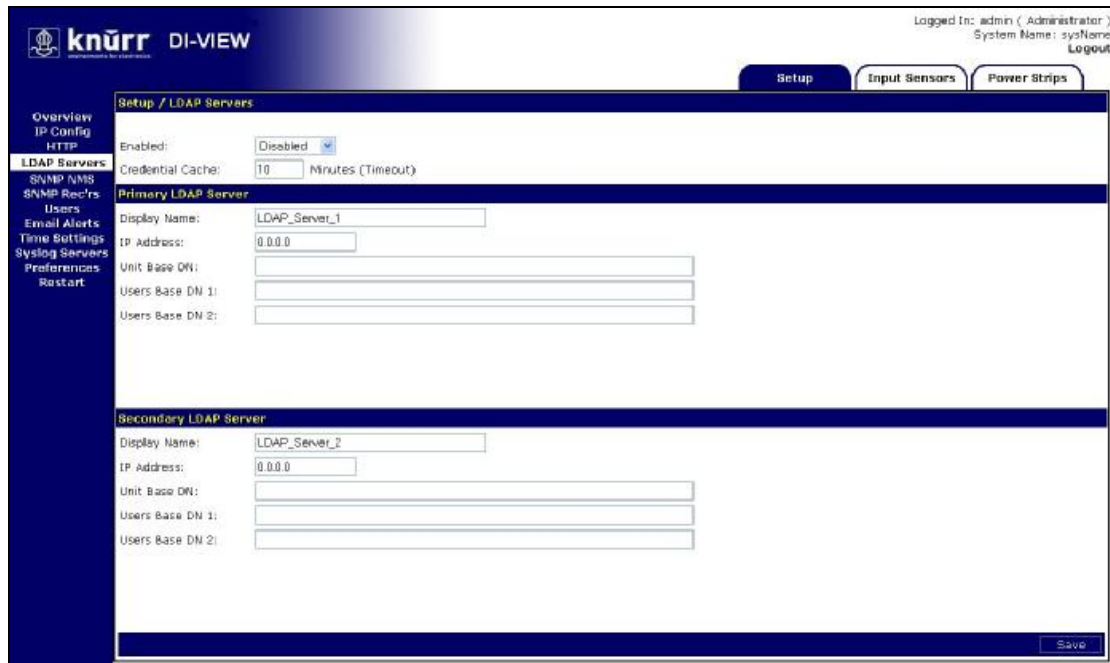
Receive traps **Enabled** setting allows the specified NMS to receive the units standard range of traps.

Receive traps **Enabled (incl Auth fails)**, will cause the unit to issue traps if an unauthorised IP address attempts to access the units SNMP functions.

Receive traps **Disabled** prevents traps from being sent to the specified NMS IP address.

Network Setup - Users

Users with permission to access the Web Management Interface can be added here. Access passwords are also specified along with users access permissions.



The screenshot shows the 'Setup / LDAP Servers' configuration page in the knürr DI-VIEW interface. The page is titled 'Setup / LDAP Servers' and includes a sidebar with navigation options: Overview, IP Config, HTTP, LDAP Servers, SNMP, SNMP Rec'ds, Users, Email Alerts, Time Bottlings, Syslog Servers, Preferences, and Restart. The main content area is divided into sections for 'Primary LDAP Server' and 'Secondary LDAP Server'. Each section contains fields for 'Display Name', 'IP Address', 'Unit Base DN', 'Users Base DN 1', and 'Users Base DN 2'. The 'Enabled' checkbox is currently set to 'Disabled'. The 'Credential Cache' is set to '10 Minutes (Timeout)'. A 'Save' button is located at the bottom right of the page.

Figure 4-7. User Setup

Username

The required username is entered here. This is the username that will be required to login to the Web Management Interface.

Password

Access passwords are entered here on a per user basis.

Level

Three user levels are available for assignment.

Administrator

Administrators have full control of DI-View configuration settings.

Controller

Controllers are able to view configuration settings.

Viewer

Viewers are able to view configuration settings.

Warning! User 1 / admin is the master administrator. It is possible to remove administrator rights from the admin user. Doing this is not recommended as it may leave you without administrator access.

In this situation a reset to factory defaults is the only solution.

Details on how to do this can be found in the Troubleshooting section.

Network Setup – Restart

A unit may be rebooted or reset to factory defaults here.

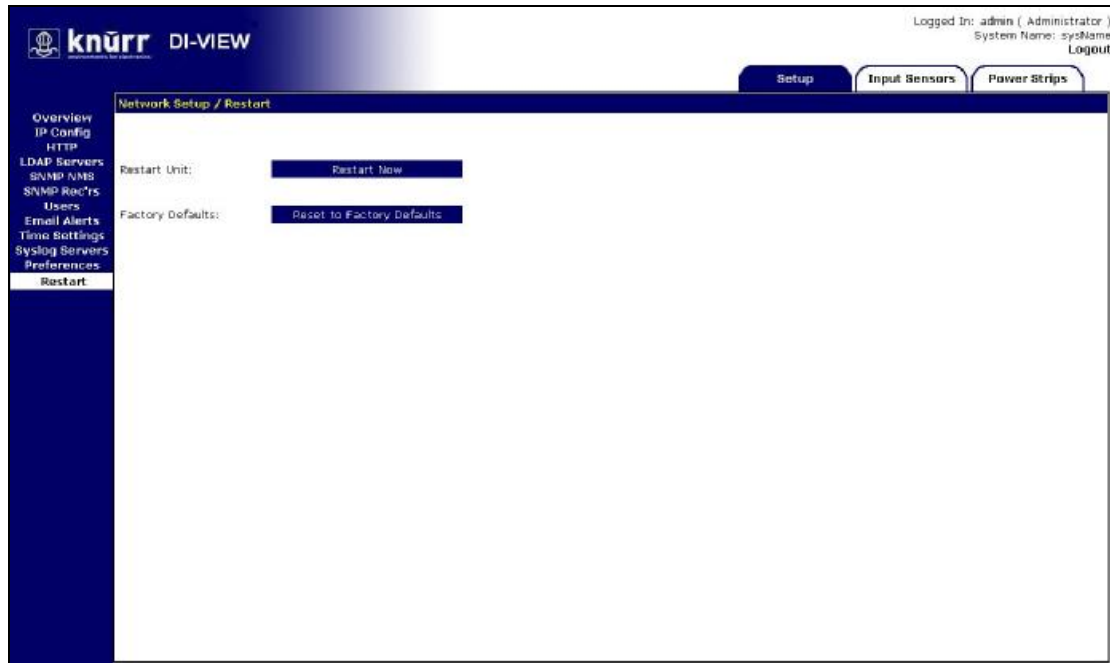


Figure 4-8. Restart

Restart Unit

Restart Now

Selecting '**Restart Now**' commands the unit to reboot. A confirmation prompt is displayed. Rebooting the unit will cause any outstanding configuration changes to come into effect.

Factory Defaults

Reset to Factory Defaults

Selecting 'Reset to Factory Defaults' instructs the unit to restore factory default settings. A prompt appears for confirmation.

Default IP address settings will not come into effect until the unit is rebooted.

This behaviour allows a user to reset a unit to defaults without losing communications. The correct IP address can then be entered on the IP Setup page before the unit is rebooted with the '**Restart Now**' button.

Input Sensors – Status

The Input Sensors status page presents an overview of the DI-View input ports.

Input channel number, name, type of input sensor, status, current readings and thresholds can all be seen at a glance here.

knürr DI-VIEW
 Logged In: admin (. Administrator)
 System Name: sysName
 Logout

Setup Input Sensors Power Strips

Input Sensors / Status

Information from connected input sensors is presented here.

Channel	Type	Detected	Status	Value	Limits			
					UC	UW	LW	LC
1: Input 01	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A
2: Input 02	Auto Detect	None	Fault	---	N/A	N/A	N/A	N/A

Figure 4-9. Input Sensor Status.

Status Indicators

Three status indicators are displayed next to input channels to allow quick determination of normal, warning and critical alarm statuses:-




	All thresholds within limits.
	Upper or lower Warning limit reached/exceeded.
	Upper or lower Warning limit reached/exceeded.

Table 4-1. Input Status Indicators.

Input Sensors – Defaults

The Input Sensor Defaults menu allows configuration parameters which relate to input sensors of specific types to be defined and applied to all inputs of that type.

The types of input sensors are:-

Temperature
Humidity
Analogue (Voltage)
Open/Close Contacts (digital inputs)

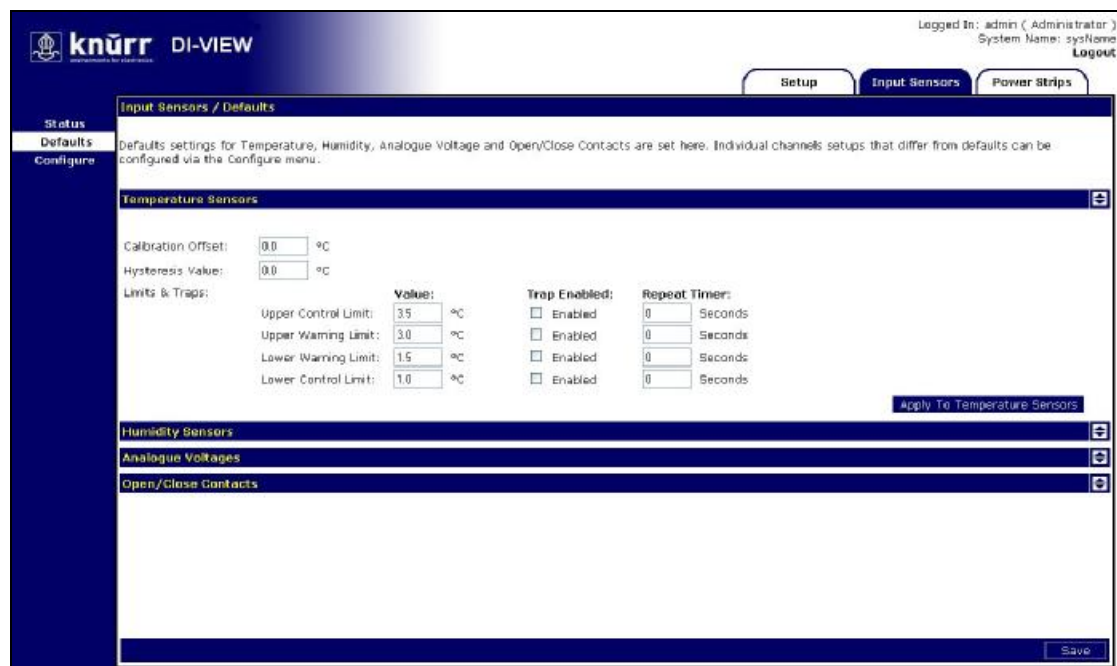


Figure 4-10. Input Sensor Defaults with Temperature and Humidity menus.

The defaults that can be specified are described below.

Calibration Offset

The value entered here alters the actual reading of a sensor by the amount specified.

For example, if a Calibration offset of 6 was used and a sensor's true reading was 36, the indicated reading used for display and alarm purposes would be 42.

This works in an identical way for both temperature and humidity sensors.

Hysteresis Value

The hysteresis default value to be applied to sensors is specified here. The value specified is an offset from a sensor's threshold values.

For example, a hysteresis value of 5 would mean that in the case of an Upper Control Limits alarm the alarm value would have to reduce to 5 below the threshold value before another alarm is issued.

Please see Appendix B: Hysteresis Demystified for detailed information.

Limits and Traps

Default values for sensor alarm thresholds can be specified here. The default settings for alarm threshold traps can also be specified here.

The thresholds that can be set are as follows:-

- Upper Control Limit**
- Upper Warning Limit**
- Lower Warning Limit**
- Lower Control Limit**

Default trap settings can also be applied for all of these thresholds. With the trap box unticked no SNMP alarm traps will be generated even when an alarm condition exists for that threshold.

Repeat Timer

The repeat timer causes alarm traps to be reissued after a specified amount of time if the alarm condition remains present.

Setting the repeat timer to zero (0) will disable the repeat traps.

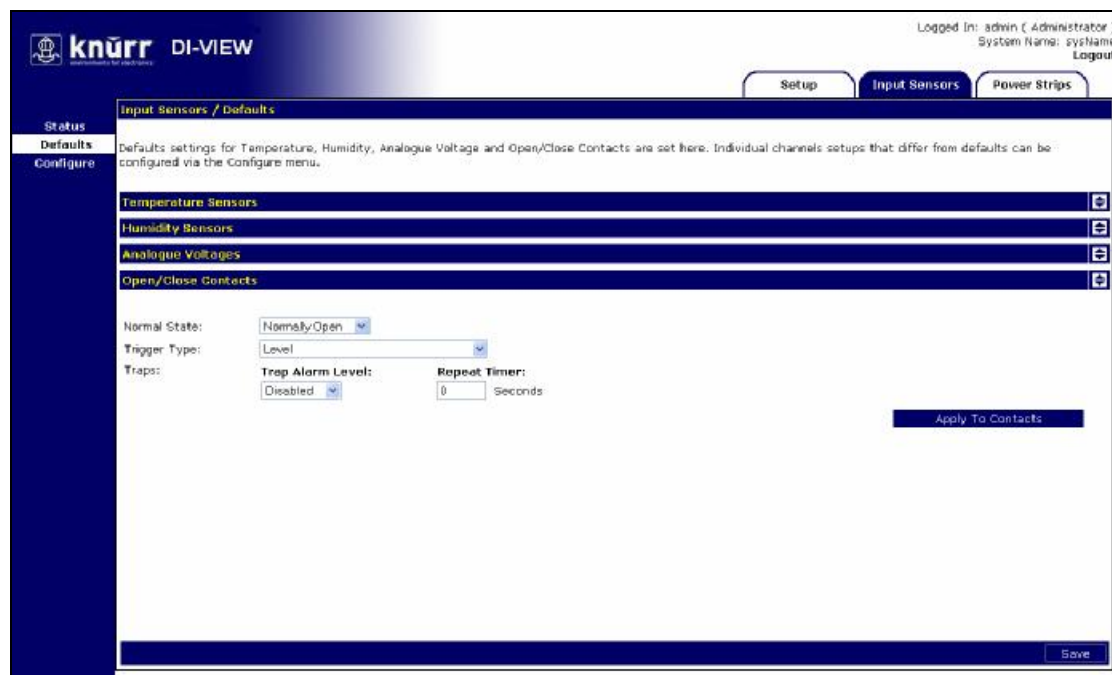


Figure 4-11. Input Sensor Defaults with Open/Close Contacts menu.

The defaults that can be set for Open/Close contacts differ from the Temperature and Humidity settings.

Normal State

Normal state specifies the condition in which a contact is considered to be 'Normal', 'Non-alarmed' state.

Devices such as smoke alarms and air conditioning units often have normally open contacts. In order to receive alarm indications from these types of units setting normally open would cause alarms to be issued when the monitored contact closes.

Setting normally closed in the case of a rack cabinet door would cause an alarm condition when the door was opened.

Trigger Type

Trigger type defaults for Open/Close sensors are specified here.

The three available options for trigger types are:-

Level

Level triggering is the default mode. When an input physically transitions from a Normal to Non-Normal state an alarm will be triggered. However the alarm will only persist whilst the input remains in a Non-Normal state. When the input returns to a normal state the alarm will be cleared.

Normal to Non-Normal (Positive Edge)

This type of triggering may be used in situations where a momentary type input (eg: shock sensor, PIR etc), is used. Since these types of inputs are momentary any alarm condition which occurs no matter how short will persist until manually cleared.

Positive Edge triggering is used when an alarm is required to persist after an input changes from the Normal state to the Non-Normal state.

Non-Normal to Normal (Negative Edge)

This type of triggering may be used in situations where a momentary type input (eg: shock sensor, PIR etc), is used. Since these types of inputs are momentary any alarm condition which occurs no matter how short will persist until manually cleared.

Negative Edge triggering is used when an alarm is required to persist after an input changes from the Non-Normal to Normal state to the state.

Input Sensors - Configure

Configure allows the individual sensor channels to be configured.



Figure 4-12. Input Sensor Configuration

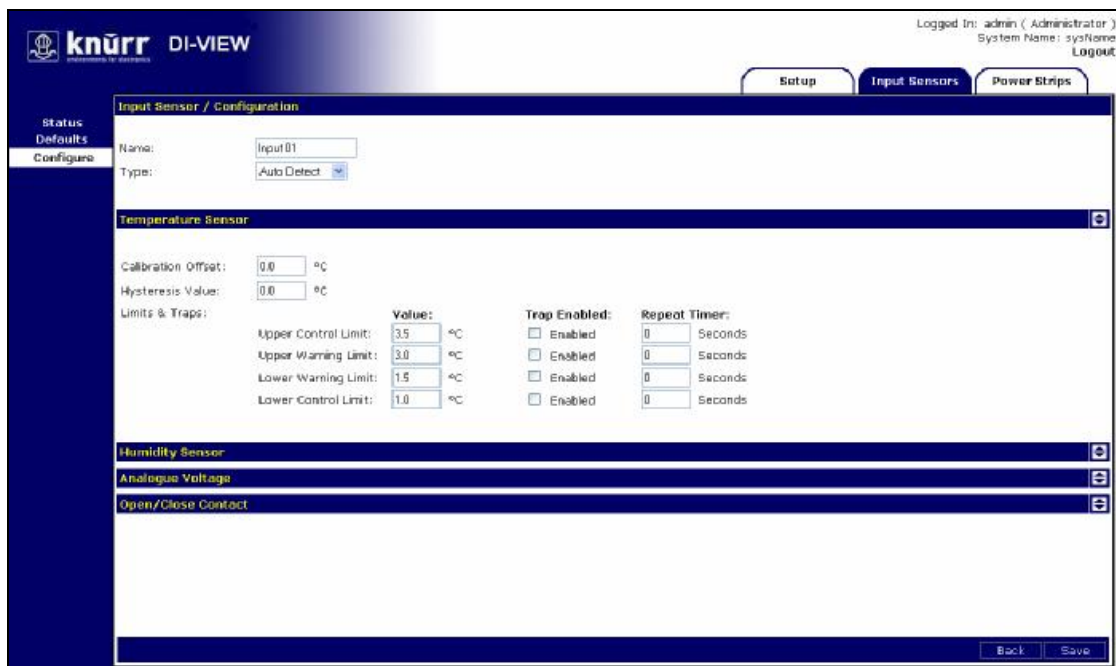


Figure 4-13. Input Sensor Channel Configuration

Selecting the **Config** option will open a detailed configuration page for the selected sensor.

The important difference between the menus presented here and the menus presented on the Defaults page is that settings are applied to individual channels.

The options found in the submenus are identical to those in the Defaults menu, however two additional options can be found.

These are detailed below:-

Name

Sensor channels can be assigned names for ease of identification. Eg: “Server Room Sensor”, “UPS Battery Fail”.

Type

The type of connected sensor is specified here. The sensor channels can be set to auto detect, temperature, humidity, contact or disabled.

Power Strips - Status

The Power Strips status page presents an overview of connected PDUs.

PDU channel number, name, voltage, current thresholds can all be seen at a glance here.

Logged In: admin (Administrator)
System Name: sysName
Logout

Setup Input Sensors Power Strips

Power Strips / Status

Information from connected PDUs is presented here.
View Power: KW-hr KVA

Strip	Outlets	Voltage	Voltage Limits				Current	Current Limits				Power	Power Limits	
			UC	UW	LW	LC		UC	UW	LW	LC		UC	UW
1:	N/A	N/A	0	0	0	0	N/A	0.0	0.0	0.0	0.0	N/A	0.0	0.0
2:	N/A	N/A	0	0	0	0	N/A	0.0	0.0	0.0	0.0	N/A	0.0	0.0
Aggregate							0.0 Amps	0.0	0.0	0.0	0.0	N/A	N/A	N/A

Figure 4-14. Power Strips

Status Indicators

Three status indicators are displayed next to PDU channels to allow quick determination of normal, warning and critical alarm statuses:-




	All thresholds within limits.
	Upper or lower Warning limit reached/exceeded.
	Upper or lower Warning limit reached/exceeded.

Table 4-2. Power Status Indicators.

Power Strips – Configure

The Power strip configuration menu provides the option to proceed to configure individual PDU options.

The two PDU channels can be individually configured by selecting the **Config** option next to channel to be configured.

A summary of several current configuration parameters is displayed on a per PDU channel basis.

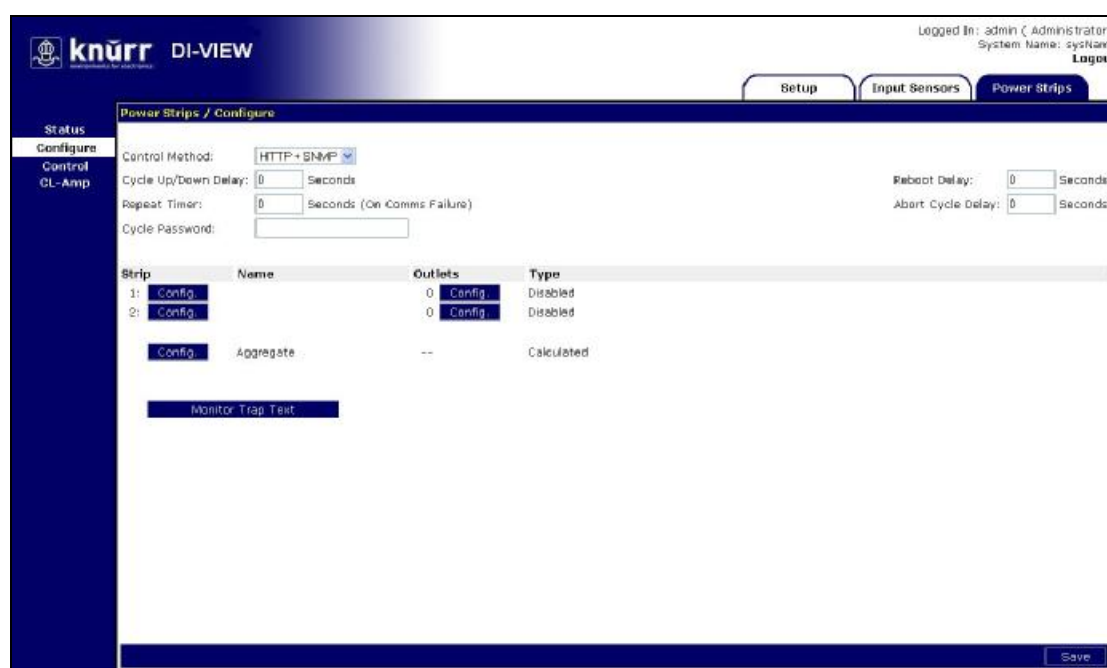


Figure 4-15. Power Strip Configure Menu

Control Method

Control Method specifies which control methods are available to control the outlets on PDUs attached to the unit.

HTTP + SNMP

The Web Management Interface and SNMP can be used to command PDU outlets.

HTTP Only

Only the Web Management Interface may be used to command PDU outlets. This effectively disables SNMP PDU outlet control.

SNMP Only

Only SNMP commands can command PDU outlets. This effectively disables Web Management Interface PDU outlet control.

RS232 Only

Selection allows PDU control commands to be issued directly to a unit via the onboard RS232 port. This option disables Web Management Interface and SNMP control.

Cycle Up/Down Delay

Specifies the interval in seconds between switching on and switching off of outlets when an entire PDU strip is cycled (all outlets commanded on or off).

Repeat Timer (on Comms failure)

Specifies the interval in seconds after an initial PDU comms failure trap is produced that a repeat trap will be issued.

Reboot Delay

Specifies how long (in seconds) an outlet remains off after a reboot before switching back on.

Abort Cycle Delay

Specifies how long in seconds must elapse before a commanded cycle begins on a PDU strip. This allows the user time to reverse the decision to cycle a strip before any outlet states are changed.

This can be set to zero if this functionality is not desired.

Power Strips – Configure - Config

This menu allows all the available options for a specific PDU to be specified.

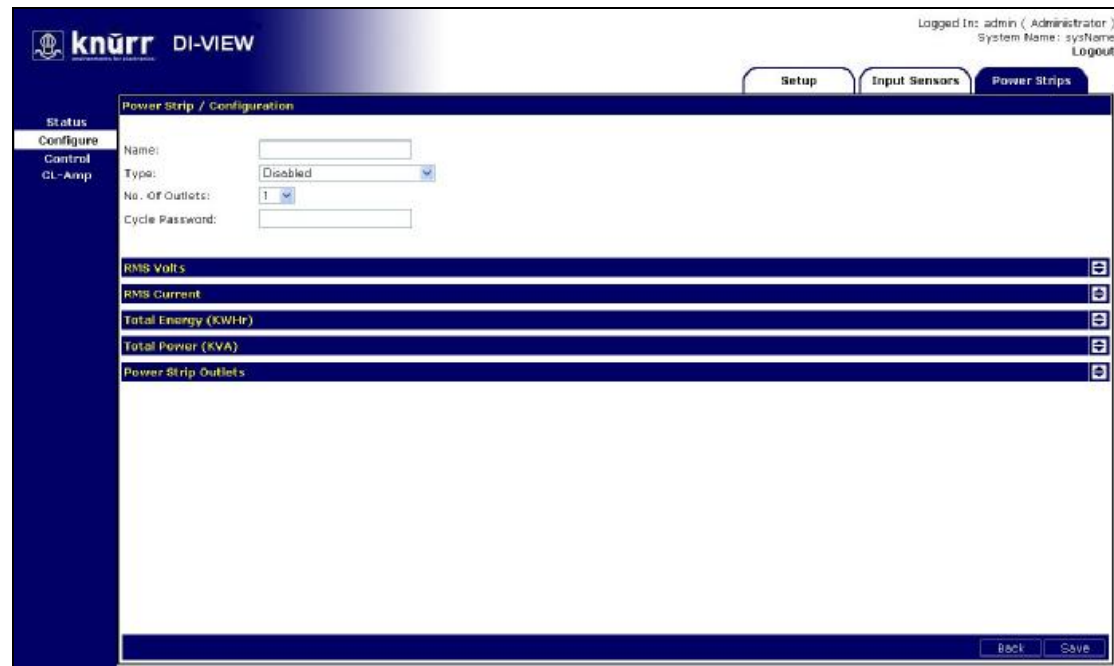


Figure 4-16. Individual Power Strip Config Menu

These options are found on five submenus. The submenus are:-

Configuration

RMS Volts

RMS Current

Total Power

Power Strip Outlets

The functions of the various options will be detailed below:-

Name

Individual PDUs can be assigned names for ease of identification. Eg: “Rack 5 PDU Sensor” or “Comm Room”.

Type

Type of PDU connected to channel is specified here.

Disabled

No monitoring or control will be performed on this PDU channel.

Monitor Only

Monitoring of power values will be performed on this PDU channel.

Control Only

The capability to control individual PDU outlets will be enabled on this PDU channel. No monitoring will be performed.

Monitor and Control

Both outlet control and power monitoring will be enabled on this PDU channel.

Warning! ***It is advised that during unit setup and deployment Control Only or Monitor and Control options be selected before critical loads are connected to outlets.***

Number of Outlets

Specifies the number of **controllable** outlets present on a PDU strip. This is required when **Control Only** or **Monitor and Control** options have been selected.

For example, if you have a PDU consisting of 24 Outlets, one of which is a permanent live (non-switching) outlet, 23 outlets would be specified.

Warning! ***Failure to specify the correct number of outlets can lead to the incorrect outlet being switched on or off.***

Repeat Timer

In the event of a communications failure with a connected PDU this entry in seconds determines how often 'Comm Fail' traps will be generated.

Limits and Traps

Values for voltage, current and total power thresholds can be specified here. Traps for each threshold can also be enabled or disabled here.

The thresholds than can be set are as follows:-

Upper Control Limit
Upper Warning Limit
Lower Warning Limit
Lower Control Limit

Note! ***There are no lower limits for total power as total power consumption can only go up not down.***

Power Strips – Control

Individual outlets or all outlets on a given strip can be switched on and off using this screen.

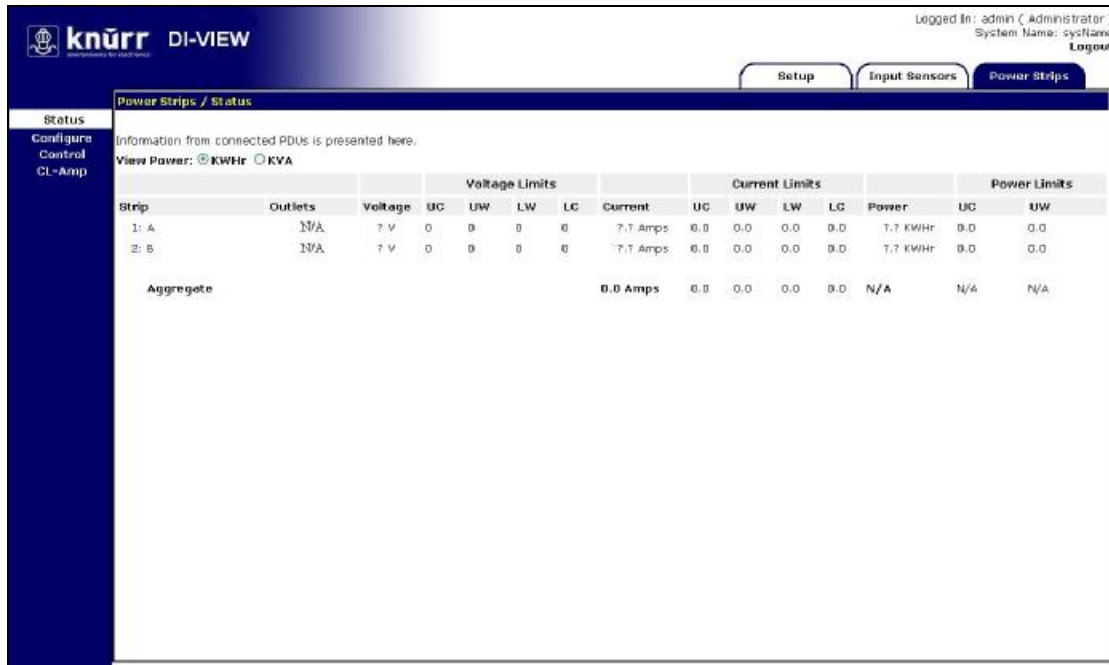


Figure 4-17. Power Strips Control.

The display consists of a visual representation of PDU power strips that have **Control** or **Monitor and Control** enabled on the Configure page.

Strips which are **Disabled** or in **Monitor Only** will not display any outlet graphics and be displayed with appropriate text.

Power Strips inputs are numbered 1 to 6 in ascending order. Power Strip numbers correspond to the physical input ports on the rear of the DI-View MCU.

Switching individual sockets

Any displayed socket can be clicked. This will present a small control menu above the socket which displays further information. Three control options are also presented.

On

Selecting this option commands the selected outlet to switch On. If the outlet is already on this will have no effect.

Off

Selecting this option commands the selected outlet to switch Off. If the outlet is already off this will have no effect.

Reboot

The reboot option commands the selected outlet to switch off. After the time specified by Reboot Delay timer has elapsed the outlet will automatically switch itself back On.

Switching an entire strip

All the outlets on any strip can be commanded to Off or On with a single command.

This can be done by clicking the **Lightning Bolt** symbol on the end of a PDU graphic.

A small dialog will appear offering the following options:-

On

Commands all outlets on a selected Power Strip to switch OFF.

Any outlets already on will remain on, any currently off will be switched on.

Off

Commands all outlets on a selected Power Strip to switch off.

Any outlets already off will remain off, any currently on will be switched off.

Abort!

Once a command has been issued to turn all outlets on a Power Strip on or off, the Abort! Button can be used to cancel or abort the command.

The Abort Cycle delay option on the Power Strips – Configure – Config menu specifies the time allowed in seconds for an abort to be issued.

Strip	Outlets	Voltage	Voltage Limits				Current	Current Limits				Power	Power Limits	
			UC	UW	LW	LG		UC	UW	LW	LG		UC	UW
1: A	N/A	7 V	0	0	0	0	7.7 Amps	0.0	0.0	0.0	0.0	1.7 KWHr	0.0	0.0
2: B	N/A	7 V	0	0	0	0	7.7 Amps	0.0	0.0	0.0	0.0	1.7 KWHr	0.0	0.0
Aggregate							0.0 Amps	0.0	0.0	0.0	0.0	N/A	N/A	N/A

Figure 4-18. Power Strips Control – Switching Dialog.

5 LDAP

DI-View LDAP Overview

The DI-View implements a Lightweight Directory Access Protocol (LDAP) client. This allows the DI-View unit to authenticate user logins to the Web Management Interface (WMI) using an LDAP Directory.

If LDAP is used for authentication it is first consulted when a user attempts a login. If the user is not found or access is denied by LDAP then the credentials are checked against the DI-View internal user list.

Note! ***Configuration of LDAP is an advanced topic and requires existing knowledge of LDAP function and setup (or access to personnel who do).***

DI-View LDAP Structure

In order for a DI-View unit to successfully authenticate a user for WMI login it needs to be ‘pointed’ to a specific structure within a directory.

A unit is ‘pointed’ to this structure within a directory by specifying the **Unit Base DN** on the Network Setup – LDAP page.

The following Organisational Units will need to be created:

DI-View (this can be named anything)
Powerhawk2Administrators
Powerhawk2Controllers
Powerhawk2Viewers

See **Figure 5-1** (Page 47) for hierarchy details.

The following Groups will need to be created:

DI-ViewAdminUsers
DI-ViewControlUsers
DI-ViewViewUsers

Note! ***Groups referred to are groups as found in Active Directory schema. However any implementation which provides a group with a ‘members’ attribute may function.***

The following figure depicts the DI-View LDAP authentication structure:

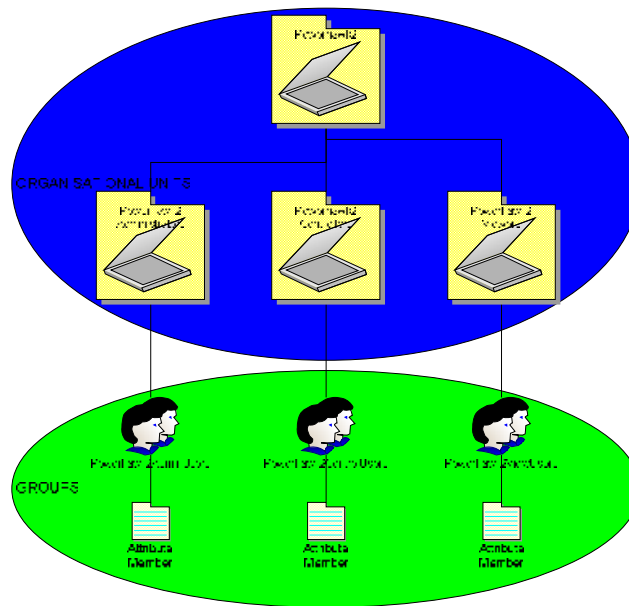


Figure 5-1. LDAP Structure Chart.

Once the required LDAP structure has been created the Distinguished Name (DN) of users should be added to either: Powerhawk2AdminUsers, Powerhawk2ControlUsers, Powerhawk2ViewUsers

Group Membership and Access Level

Membership of these groups grants the following permissions on DI-View units:

Powerhawk2AdminUsers

Users placed into this group will have Admin privileges on DI-View units.

Powerhawk2ControlUsers

Users placed into this group will have Controller privileges on DI-View units.

Powerhawk2ViewUsers

Users placed into this group will have View privileges on DI-View units.

DI-View Unit Configuration

For LDAP authentication to function each DI-View unit requires certain configuration values to be provided.



Figure 5-2. LDAP Setup

The normal steps are listed below:

- 1) If one LDAP server is to be used select **Enabled – Primary**.
- 2) Enter a descriptive name, E.g: AD_Server_1 into **Display Name**.
- 3) Enter the complete DN of the top level OU as seen in **Figure 5-1** above.
- 4) Enter the DN of where users that are members of DI-View access groups can be found in the Directory. These DNs can be entered into **User Base DN 1** and **User Base DN 2**.
- 5) Finally **Save** should be clicked to bring any changes into effect.

6 Troubleshooting

Resetting DI-View to factory default settings

To reset the DI-View unit to factory default perform the following steps:

- 1) Reset the DI-View unit (by pressing the Reset button or removing and reconnecting the power). Wait **5** Seconds.
- 2) After **5** seconds **press and hold** the Mode button until the red **Alarm** until it extinguishes (approx. 10 seconds).
- 3) Wait 90 seconds for the reset to complete.

The factory default settings will have been restored.

Note! ***This process can be aborted by releasing the mode switch before the alarm light has extinguished.***

The NMS Cannot poll the DI-View

- Problem:** The NMS cannot ping or poll the DI-View.
- Solution:** Make sure the network connection to the DI-View is good.
- Solution:** Make sure the cable is in good condition.
- Solution:** Try pinging the DI-View from another computer on the same network segment as the DI-View.
- Solution:** Ensure that the NMS IP Address is in the NMS table of the DI-View.
- Solution:** Ensure that the community string has been set for the NMS via the web management interface.

7 Appendix A: Technical Details

Factory Default Settings

Table 7-1. DI-View Defaults

IP Address:	192.168.0.253
Subnet Mask:	255.255.255.0 (/24)
Default Gateway:	192.168.0.1
Web Management Address:	http://192.168.0.253/
Default username:	admin
Default password	admin

Operating Information

Input Power:	12VDC (300mA ~ 500mA)
Operating Temperature:	0°C to 40°C
Storage Temperature:	-10°C to 70°C
Operating Humidity:	5% to 90% RH
Storage Humidity:	5% to 100% RH

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.

DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

8 Appendix B: Hysteresis Demystified

How Hysteresis works

When a temperature or humidity limit is reached and the relevant limit has its 'OFF to ON Trap' enabled an alarm trap will be issued by the DI-View for this event.

With a zero hysteresis setting the traps will continue to be generated each time the limit is reached.

This may be undesirable in a situation where the temperature or humidity level measure has only reduced by a small amount before rising again and triggering further traps.

The hysteresis function is provided to prevent further alarm traps from being generated until the measured value has fallen to a satisfactory level.

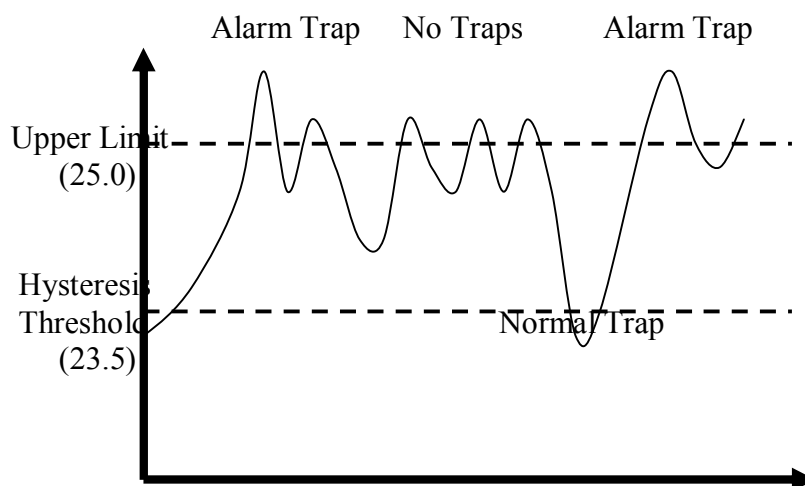


Figure 8-1. Hysteresis chart

As shown in the humidity first rises past its upper warning threshold which generates a trap.

The humidity then reduces slightly but does not reduce to the hysteresis level which is 1.5% RH lower than the alarm (1.5% RH lower as an absolute measured value rather than 1.5% of currently measured value).

Humidity then increases and decreases again. However on the second decrease of humidity the level drops below the hysteresis level. The

Humidity falling below the hysteresis level re-enables alarm traps for the next alarm event. An upper limit of 25 and a hysteresis threshold of 1.5 yield a threshold limit of 23.5.

The humidity level again begins to rise and again exceeds the upper limit, however this time an alarm trap is again generated.

The Hysteresis feature acts on the following Temperature and Humidity thresholds:-

- Upper Control Limit (UCL)
- Lower Control Limit (LCL)
- Upper Warning Limit (UWL)
- Lower Warning Limit (LWL)

The inverse of the above description is true when applied to Temperature and Humidity lower control and warning limits.

As stated above the hysteresis threshold is user configurable using the menu options detailed previously.

9 Appendix C: Networking Reference

This appendix has two sections: *Reference* and *Troubleshooting*.

Reference

This section discusses SNMP communities, IP addressing, subnet masking, routers and gateways.

Communities

A community is a string of printable ASCII characters that identifies a user group with the same access privileges. For example, a common community name is “public”.

For security purposes, the SNMP agent validates requests before responding. The agent can be configured so that only managers that are members of a community can send requests and receive responses from a particular community.

This prevents unauthorized managers from viewing or changing the configuration of a device.

IP Addresses

Every device on an internetwork must be assigned a unique IP (Internet Protocol) address. An IP address is a 32-bit value comprised of a network ID and a host ID.

The network ID identifies the logical network to which a particular device belongs. The host ID identifies the particular device within the logical network.

IP addresses distinguish devices on an internetwork from one another so that IP packets are properly transmitted.

IP addresses appear in dotted decimal (rather than in binary) notation. Dotted decimal notation divides the 32-bit value into four 8-bit groups, or octets, and separates each octet with a period.

For example, 199.217.132.1 is an IP address in dotted decimal notation.

To accommodate networks of different sizes, the IP address has three divisions - Classes A for large, B for medium, and C for small.

The difference among the network classes is the number of octets reserved for the network ID and the number of octets reserved for the host ID:

Class	Value of First Octet	Network ID	Host ID	Number of Hosts
<i>A</i>	<i>1-126</i>	<i>first octet</i>	<i>last three octets</i>	<i>16,387,064</i>
<i>B</i>	<i>128-191</i>	<i>first two octets</i>	<i>last two octets</i>	<i>64,516</i>
<i>C</i>	<i>192-223</i>	<i>first three octets</i>	<i>last octet</i>	<i>254</i>

Any value between 0 and 255 is valid as a host ID octet except for those values reserved by the IPv4 standard for other purposes:

Value	Purpose
<i>0, 255</i>	<i>Network Number & Broadcast</i>
<i>127</i>	<i>Loopback testing and interprocess communication on local devices</i>
<i>224-254</i>	<i>IGMP multicast and other special protocols</i>

Subnetting and Subnet Masks

Subnetting divides a network address into subnetwork addresses to accommodate more than one physical network on a logical network.

For example: A Class B company has 100 LANs (Local Area Networks) with 100 to 200 nodes on each LAN.

To classify the nodes by its LANs on one main network, this company segments the network address into 100 subnetwork addresses (If the Class B network address is 150.1.x.x, the address can be segmented further from 150.1.1.x through 150.1.100.x).

A subnet mask is a 32-bit value that distinguishes the network ID from the host ID for different subnetworks on the same logical network.

Like IP addresses, subnet masks consist of four octets in dotted decimal notation.

You can use subnet masks to route and filter the transmission of IP packets among your subnetworks.

The value “255” is assigned to octets that belong to the network ID, and the value “0” is assigned to octets that belong to the host ID.

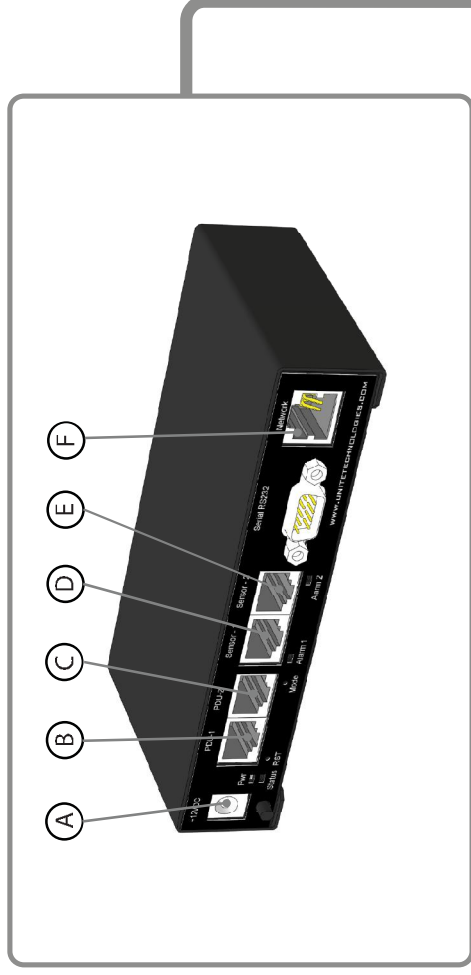
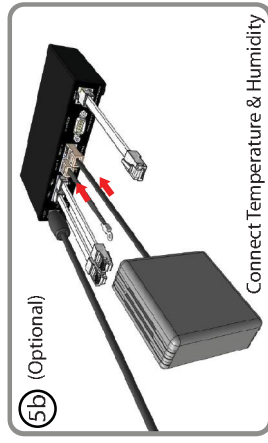
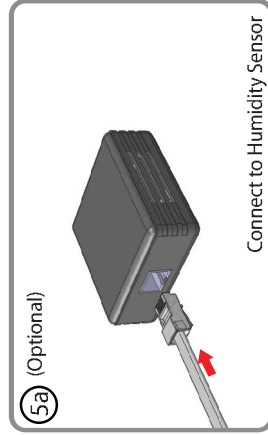
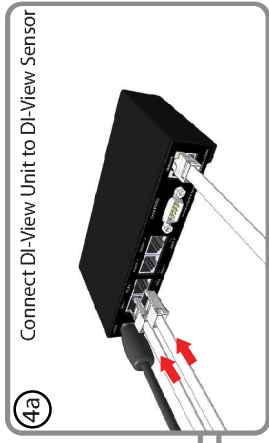
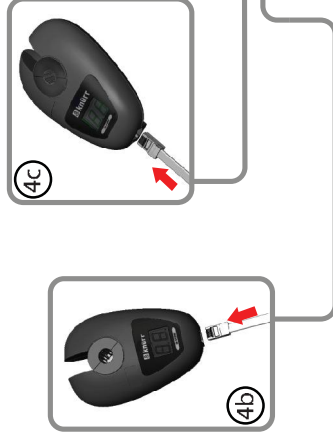
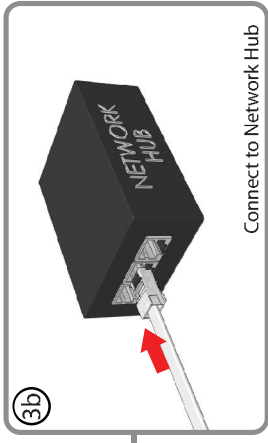
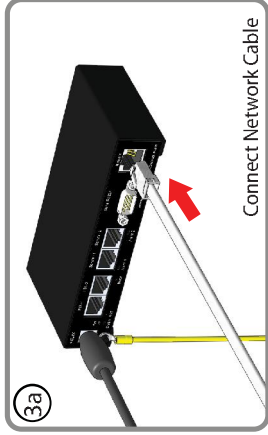
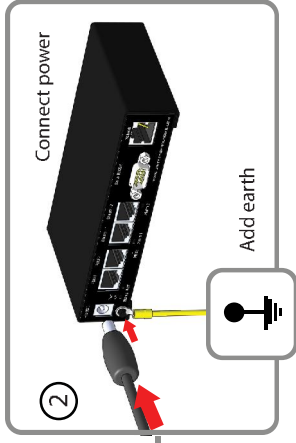
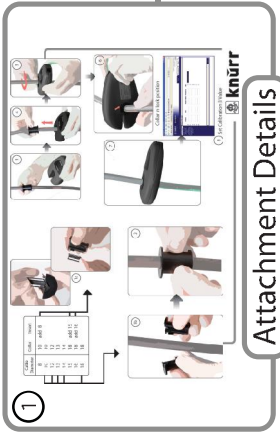
Network Mask	Routing and Filtering
<i>255.0.0.0</i>	<i>Class A network. First octet defines network number. Final three octets define host address. Valid Class A</i>

	<i>network numbers are in the range 1 to 126.</i>
<i>255.255.0.0</i>	<i>Class B network. First 2 octets define network number. Final two octets define host address. Valid class B network numbers are in the range 128.0.x.x to 191.255.x.x</i>
<i>255.255.255.0</i>	<i>Class C network. First 3 octets define network number. Final octet defines host address Valid class C network numbers are in the range. 192.0.0.x 223.255.255.x</i>

Gateways

Gateway, also sometimes referred to as a router, is any device with two or more network adapters connecting to different physical networks.

Gateways allow for transmission of IP packets between different networks on an internetwork.



(A)	12V Power Supply	DC Jack -> DI-View Unit 110~240VAC 50/60Hz Supply
(B) FEED A	RJ45 - RJ45	RJ45 -> DI-View Unit RJ45 -> DI-View Sensor
(C) FEED B		
(D)		RJ45 -> DI-View Unit
(Optional) (E)	RJ45 - RJ45 (Not supplied)	RJ45 -> DI-View Unit Humidity Sensor (Not supplied)
(F)	RJ45 - RJ45 (Not supplied)	RJ45 -> DI-View Unit RJ45 -> Network Hub (Not supplied)

Connection Details



knürr

Calibration B Value	Cable Types
96	- Cable 1 (Schuko cable): 1. DI-STRIP Standard DIN 49440 2. DI-STRIP IEC 320 3. DI-STRIP Standard CEE-7-V (UTE) 3. Serimat Classic 4. Serimat Compact 5. Serimat Black Line
87	- Cable 2 (switzerland cable): 1. DI-STRIP switzerland CH SEV 1011
88	- Cable 3 (USA cable) 1. DI-STRIP Standard USA
93	- Cable 4 (black cable without plug) 1. DI-STRIP BladePower 1ph 2. DI-STRIP PizzaPower 1ph

Please select cable type from above table that is closest match to the cable being monitored.

For maximum accuracy please note the following:-

1. Di-View Sensor should be calibrated to the cable type being used.
2. Di-View Unit should be connected to earth. (use earth stud)
3. Use Di-View Unit Web interface, select **CL-amp** menu option from the **Power Strips** tab and set correct Calibration B Value for cable type in use.
4. 100mm clearance top and bottom with minimum bends.

Type	DI-View Unit - 0:00:00
Model No.	Power & Environmental Monitoring
Input	06.108.310.8
Range	DC 12V 50mA
Frequency	AC 1~30A @ 250V Max 50/60Hz
Unit Dimension	134mm x 89mm x40mm
Weight	14g
Packaging Weight	40g
Packaging size	200mm x 150 x 110
Safety	EN BS 60950
EMC	EN BS 61326-1:2006

WARNING Di-View Unit is designed to be powered by Knurr monitoring units. If external power supply is used it must only be powered from a power source meeting EN60950-1 including clause 2.5 (Limited power sources).



knurr

DI-VIEW

User Guide



For other cable diameter please contact Knurr Technical Support
Knurr AG

Customer Service Center
Mariakirchener Strasse 38
D-94424 Arnstorf
Telefon +49 (0) 87 23-27-100
Telefax +49 (0) 87 23-27-700
E-Mail: knurr.info@knurr.com

