

AcceptNet

QUICKSTART INFORMATION MANUAL

Revision 2.2

By Michael Lekias

Copyright © 2003
Professional Software Design

TABLE OF CONTENTS

1. INTRODUCTION	5
1.1. MIMIMUM SYSTEM REQUIREMENTS.....	5
1.1.1. <i>ACCEPTNET SERVER</i>	5
1.1.2. <i>Other Requirements</i>	6
1.1.3. <i>ACCEPTNET CLIENT</i>	6
1.2. A NOTE ABOUT REQUIREMENTS.....	7
1.3. SYSTEM PERFORMANCE:.....	7
1.4. ABOUT WINDOWS [®] AND THIS DOCUMENT.....	8
1.5. ON LINE HELP.....	8
1.6. RECOMMENDED TIME AND DATE FORMAT.....	8
2. INSTALLATION	10
2.1. FROM FLOPPY DISKS.....	10
2.2. FROM CD.....	10
2.3. INSTALLING AND SETTING UP.....	10
2.3.1. <i>AcceptNet Server</i>	10
2.3.2. <i>AcceptNet Client</i>	11
2.3.3. <i>TCPtoSerial Utility</i>	11
2.4. INVOKING THE SOFTWARE.....	12
2.4.1. <i>Invoking AcceptNet Server software</i>	12
2.4.2. <i>Invoking AcceptNet Client software</i>	12
3. THE TOPOGRAPHY OF AN ACCEPTNET SYSTEM	13
4. RUNNING ACCEPTNET SERVER FOR THE FIRST TIME	15
4.1. NETWORK CONFIGURATION.....	15
4.2. HARDWARE KEY.....	15
4.2.1. <i>USB Keys</i>	16
4.2.2. <i>Parallel Port (DB25) Key</i>	16
4.2.3. <i>Registering To Upgrade Features</i>	16
4.3. PANEL CONNECTIONS.....	16
4.3.1. <i>Direct Serial Connection</i>	17
4.3.2. <i>TCP/IP to Serial Connection</i>	17
4.3.3. <i>Generic Serial (CCTV) Panels</i>	18
4.3.4. <i>Lantronix UDS10</i>	18
4.3.5. <i>Modem Connection</i>	23
4.3.6. <i>Modem Schedules</i>	24
4.3.7. <i>Connection Security</i>	25
4.4. CLIENT CONNECTIONS.....	26

- 4.4.1. *Terminal Services* 27
- 4.5. SERVER LOGIN 27
 - 4.5.1. *Operator Password* 27
 - 4.5.2. *Uploading Panel Configuration* 28
- 5. RUNNING ACCEPTNET CLIENT FOR THE FIRST TIME..... 29**
 - 5.1. CONTROLLING THE SERVER 30
 - 5.2. TENANCY 30
 - 5.2.1. *Sections* 31
 - 5.2.2. *Tenant Specific Review* 32
 - 5.2.3. *Default Tenancy While Logged Out* 32
 - 5.3. PERMISSIONS..... 33
 - 5.4. OPERATORS..... 33
- 6. TROUBLE SHOOTING..... 34**
- 7. GETTING STARTED WITH THE ACCEPTNET SYSTEM..... 36**
 - 7.1. GETTING STARTED WITH THE ACTPNET CLIENT 36
 - 7.2. CHANGING THE OPERATOR PASSWORD 36
 - 7.3. THE REVIEW LOG 37
 - 7.3.1. *Automatic Archiving of Review* 37
 - 7.3.2. *Queryable fields*..... 38
 - 7.3.3. *Searching the Archive*..... 38
 - 7.4. SETTING UP APPLICATION PREFERENCES 38
 - 7.4.1. *AcceptNet Server Comms Preferences*..... 38
 - 7.4.2. *AcceptNet Client Login/Logout Settings*..... 39
 - 7.5. SECURING ACCEPTNET 41
 - 7.6. DEFINING PERMISSION SETS 42
 - 7.6.1. *Default/Installer Permissions*..... 42
 - 7.7. DEFINING OPERATORS 42
 - 7.8. OPERATOR LOG 43
- 8. USING THE ACCEPTNET SYSTEM 44**
 - 8.1. MONITORING 44
 - 8.1.1. *Mimic (Annunciation) Panel* 44
 - 8.1.2. *Review Event Log* 45
 - 8.1.3. *Review Filters* 46
 - 8.1.4. *Searching for Review*..... 49
 - 8.1.5. *Preparing and Printing Event Reports* 49
 - 8.1.6. *Alarm Event Log*..... 50
 - 8.1.7. *Alarm Acknowledgment* 51
 - 8.2. GRAPHICAL SECURITY (LOCALE) MONITORING 53

8.3.	CONTROL OF PERIPHERALS	53
8.4.	DATABASE NAVIGATOR.....	54
8.4.1.	<i>Editing</i>	54
8.4.2.	<i>Switching Between Panels</i>	55
8.4.3.	<i>Copying Records Between Panels</i>	55
8.4.4.	<i>Preparing and Printing</i>	55
8.4.5.	<i>Changing User Editor Labels</i>	56
8.5.	ACCEPTNET SERVER REVIEW MANAGER	56
8.5.1.	<i>Setting up Panel Inputs and Areas</i>	57
8.5.2.	<i>Processing Review</i>	57
9.	MAINTAINING ACCEPTNET.....	62
9.1.	BACKING UP THE DATABASE.....	62
9.2.	RESTORING THE DATABASE.....	62
INDEX.....		64

1. INTRODUCTION

This document summarises the installation requirements for the AcceptNet Network software as well as some information about some of the features of the application.

For additional detailed information on any parts of the application, use the on-line help.

1.1. MINIMUM SYSTEM REQUIREMENTS

1.1.1. ACCEPTNET SERVER

The *minimum* system requirements of the PC running the AcceptNet Server will vary depending on the number of panels and clients that the application must serve. The more panels and clients connected to the AcceptNet system the higher the performance requirements. The following is *not a recommendation* and will change depending on the number of other applications, services and devices running on the PC at the same time. Also consider any operating system configuration or personal requirements as well as the number of clients, the number of tenants, the panel memory configurations, network performance and panel serial connections required.

- Pentium III® 350MHz Processor.
- Windows 98, NT, 2000, XP Pro® Operating System – “Plain Vanilla” as supplied by Microsoft®.
- Latest Service Pack/updates for Windows®
- “Plain Vanilla” Windows® compliant BIOS.
- 256Mb RAM for Windows NT, 2000, XP Pro, 128Mb RAM Windows 98®
- TCP/IP compliant Network Card 10Mb/s, Windows® TCP/IP drivers and Winsock installed
- Standard Windows® TCP/IP network configuration.
- 50Mb free HDD space per panel. More if storing archived review to HDD @ 6Mb / 40000 review events.
- 800 x 600 resolution display 256 colours. Small (standard) Fonts
- Concept Access 3000 Revision 3 firmware or later. Concept Access 4000 panel Firmware - Revision 2.0 or later.
- Suitable windows compliant A4 printer.
- 1 Parallel port or 1 USB port.

1.1.2. Other Requirements

- Maximum 150 panels at 512Kb assuming access configuration and 26,000 users per panel (subject to change without notice). This requires approx > 6000 GB HDD space.
- Alloy (www.alloy.com.au) multiport serial adapter card for installations involving more than 2 serially connected panels or use default Windows® Serial Port devices, COM1/COM2 for up to 2 panels.
- External 3 Com US Robotics modem for modem connected panels.
- Word Pad installed, with rich text fonts loaded.
- Hardware key (printer or USB port) to enable the software.
- Uninterruptible Power Supply (UPS).
- Watchdog facility on unmaintained systems
- Lantronix UDS10 for TCP/IP to serial conversion for remote panels where required.
- PC running TCPTOSERIAL utility. To provide TCP/IP to serial conversion for remote panel where required and PC is convenient. Minimum Pentium 120Mhz, 16Mb RAM, 5Mb free HDD, UPS, W98, TCP/IP network card and connection.

1.1.3. ACCEPTNET CLIENT

The following *minimum* system requirements are suggested for an AcceptNet Client running alone on a standard Windows installation. This is *not a recommendation* and will change depending on the number of other applications, services and devices running on the PC at the same time. Also consider any operating system configuration or personal requirements as well as panel configuration, number of tenants configured and network performance.

- Pentium II® 233 MHz Processor.
- Windows 98, NT, 2000, XP Pro® Operating System installed – “Plain Vanilla” as supplied by Microsoft®.
- “Plain Vanilla” Windows® compliant BIOS.
- TCP/IP compliant Network Card minimum 1Mb/s, Windows® TCP/IP drivers and Winsock installed.
- Standard Windows® TCP/IP network configuration.
- 128Mb RAM for Windows NT, 2000 Pro, XP Pro, 64Mb RAM Windows 98®
- 50Mb free HDD space.
- 800 x 600 resolution display 256 colours. Small (standard) Fonts.
- Word Pad installed, with rich text fonts loaded.
- Suitable windows compliant ID card or standard A4 printer.

1.2. A NOTE ABOUT REQUIREMENTS

The specifications listed above are only *minimum* requirements. The amount of memory actually required may increase depending on the number and demands of other applications running simultaneously (ie. their combined individual memory/HDD requirements). Stability and performance can be improved by increasing memory size, freeing disk space, increasing virtual memory limits, reducing the number of open applications or increasing processor speed, improving network bandwidth or performance.

Contact the System Administrator at the installation site or a knowledgeable PC supplier for help in determining an appropriate or recommended system requirement based on the minimum requirements above for each security system installation.

Epson® printers with greater than 64 page types are currently not supported.

1.3. SYSTEM PERFORMANCE:

Windows NT4.0/2000/XP® systems will require more memory and likely a faster microprocessor than Windows 95/98® systems to meet an equivalent level of performance

Where the greatest operating system stability is required especially in high end, high risk security installations, system administrators/installers should consider using Windows NT/2000/XP-Pro. Also limit the number of third party hardware/software “add-ons” (eg. scanner hardware, video accelerator/input cards etc...). Drivers and hardware that are supported intrinsically by Windows (ie. no hardware manufacturer’s disk required) are preferred.

System administrators should also consider applying any software fixes for any hardware devices supported by the relevant manufacturer of any peripheral hardware as well as any OS service packs distributed and updated by Microsoft, in PC systems that exhibit problems.

Use of large bitmap images for locales and or user graphics can be very RAM intensive. Speed will be dependent on the amount of free RAM available and the number and size of the graphics screens loaded.

Large review/archive logs (for example, greater than 5000 events) will also place greater demands on the system resources and affect performance. Make an effort to ensure the amount of review visible at any one time is kept to a minimum.


Older S3 video card drivers may exhibit problems if hardware acceleration is enabled. In which case obtain and install an update of the S3 video drivers. If problems persist try setting the hardware acceleration level to “NONE” from the advanced settings in the display applet of the control panel.

1.4. ABOUT WINDOWS® AND THIS DOCUMENT

- Sub menu items are separated from parent menu items by ‘|’. **For example:** The Exit sub-menu item in the File menu is referred to by “File | Exit”.
- The underscore under letters in button captions or field labels in the application indicate that a keyboard short cut can be applied to activate the item. **For example:** The File menu can be activated by hitting the “Alt” key together with the “F” on the keyboard. This action is equivalent to left mouse clicking the File menu item.
- A dialog (dialogue) is a window requiring user input or acknowledgment.
- Tab will move the focus on an item in a window to the next item in sequence, usually the next item to the left or down from the current one. For convenience when using the database editor, use TAB to move from input field to field.

1.5. ON LINE HELP

There is on-line help associated with almost all dialogs in the AcceptNet client and server applications. You can activate help specific to the dialog you are using or the operation you are trying to perform by:

1. Hitting the F1 function key on the keyboard, after opening or accessing a dialog,
2. Clicking on the  help button of the current dialog.

1.6. RECOMMENDED TIME AND DATE FORMAT

The Time and Date format is maintained by the operating system through the “Control panel”. Operators must be aware of the current date/time format being used as this will determine the format any dates/times entered into the system. Entering the date/time in an **incorrect** format may result in incorrect values being interpreted by the system – this may adversely affect timezone programming and user expiry.

The recommended settings are as follows:

1. Invoke the “Regional Settings” screen from the Start menu. Select “Settings | Control Panel | Regional Settings”.
2. Select the “Time” tab, and from the “Time Style” drop-down menu, select the option “H:mm:ss” – (24 hour clock). If the option is not available simply type in the time format displayed here.
3. Now select the “Date” tab, and from the “Short Date Style” drop-down menu, select the option, “d/M/yyyy”. (day, month year – 4 digit year) If the option is not available simply type in the date format displayed here.

2. INSTALLATION

2.1. FROM FLOPPY DISKS

To install either AcceptNet Server or AcceptNet Client software place Disk 1 of the installation set into drive 'A:'. Select **Run** from the **Start** menu under Windows 95/NT4/2000/XP® and type:

```
A:\install
```

Then select 'OK'. You will be prompted for the remaining disks in the installation set as they are required.

2.2. FROM CD

Insert the CD into drive 'D:' (assuming the CDROM drive is drive D:), if the CD does not automatically produce a PSD installation dialog then from the **Start** button on the desktop select **Run** and 'Browse' for the setup.exe file in the root of the CD directory. The PSD installer will appear.

When using the PSD product installer, select the AcceptNet product from the explorer list on the left of the application or click on the AcceptNet logo on the right. Then click on the appropriate installation buttons in the product window to the right. Always install the AcceptNet Server first.

2.3. INSTALLING AND SETTING UP

2.3.1. AcceptNet Server

As the installation proceeds you will be prompted to indicate the hardware key (dongle) type.

- If your PC does not support a USB card or outlets then select "Only use parallel port".
- If you have received a USB hardware key or you do not know what key type you have received select "Don't know"

As the installation script proceeds a DOS shell window will appear and display the message

```
#####
#                                     #
#  HARDWARE KEY DRIVER              #
#  INSTALLED SUCCESSFULLY          #
#                                     #
#####
```

This indicates that the system has successfully installed the hardware key drivers required to access and verify the hardware key (plugged into the printer port). Unless these drivers are installed you will not be able to run the server application.

If the following message appears.

```
#####
#                                     #
#  UNABLE TO INSTALL HARDWARE KEY DRIVER #
#  YOU WILL BE UNABLE TO USE THE SERVER #
#                                     #
#  CONTACT: Accept@psdesignn.com.au      #
#                                     #
#####
```

The hardware drivers were NOT installed properly and the server hardware key will not work. You may proceed with the installation of the software however the server will (likely) not run. Contact your software vendor for help regarding this error.

If the window does not close automatically click on the 'X' in the top right corner of the window's drag bar. The installation will continue.

2.3.2. AcceptNet Client

Enter the location of the AcptClient application and wait for the script to complete.

2.3.3. TCPtoSerial Utility

You can install and use this utility whenever direct serial connection to a panel is not available but where a TCP/IP network connection is available to a PC located

near the panel. The “nearby” PC running this utility therefore can be used to provide the serial connection to the panel and transfer this serial information via TCP/IP to the AcceptNet Server. Refer to **Panel Connections** on page 16

There is no installation script available with the TCPtoSerial utility. To install this tool simply copy the file TCPtoSerial.exe from the source installation disk or CD to a suitable directory location on the PC to which the panel is going to be serially (directly) connected.

The PC to which the panel is serially connected is expected to remain active as long as the AcceptNet Server is active. A UPS is therefore recommended. It is also a good idea to add a shortcut to the TCPtoSerial utility in the PROGRAMS | STARTUP sub-folder of the START menu to ensure the utility is started again should the system be shutdown and restarted.

2.4. INVOKING THE SOFTWARE

2.4.1. Invoking AcceptNet Server software.

Once the AcceptNet Server application and related files have been installed run the server application for the first time by:

1. Activating the AcceptNet Server ICON from the desktop
2. Activating the AcceptNet Server ICON from the main Start Menu.
3. Activating the AcceptNet Server ICON from the AcptServer folder under the Programs Folder in the Start Menu.

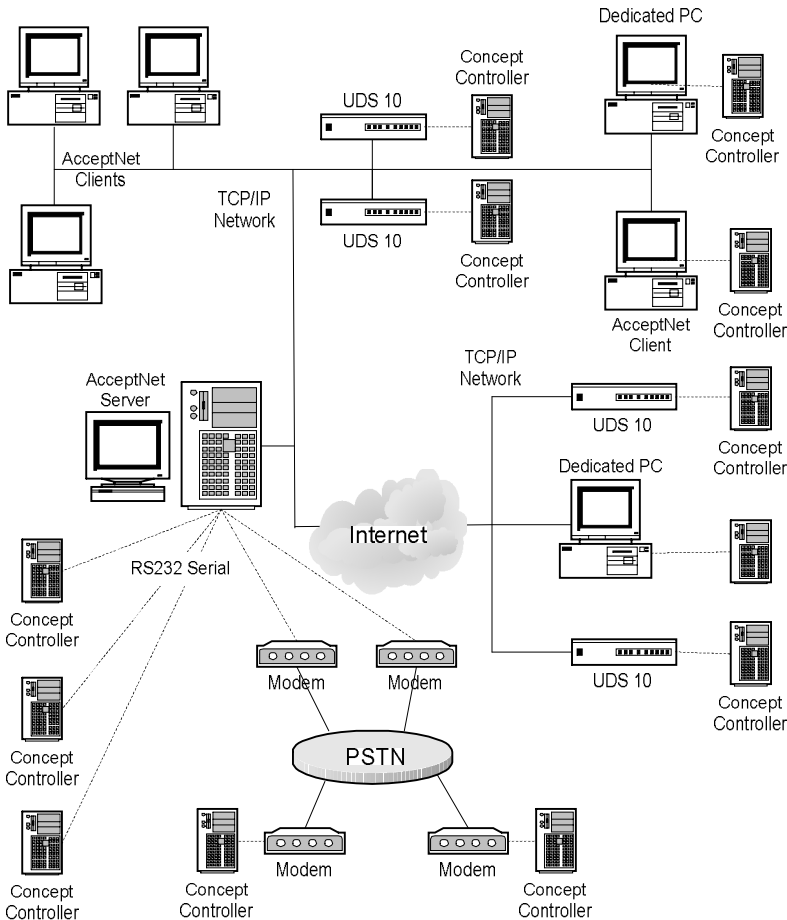
2.4.2. Invoking AcceptNet Client software.

Once the AcceptNet Client application and related files have been installed run the client application for the first time by:

1. Activating the AcceptNet Client ICON from the desktop
2. Activating the AcceptNet Client ICON from the main Start Menu.
3. Activating the AcceptNet Client ICON from the AcptClient folder under the Programs Folder in the Start Menu.

3. THE TOPOGRAPHY OF AN ACCEPTNET SYSTEM

The following diagram illustrates an example of the complicated layout of panels and clients that can be supported with the AcceptNet software.



In the diagram three panels are connected directly to the AcceptNet server via serial (RS232) connections. Further panel connections are achieved via the local TCP/IP network or via the Internet to a remote network. In addition PSTN access via modems to panels can also be managed by scheduled or permanent dial-in connection.

Some AcceptNet client PC's can be used to additionally support the TCPtoSerial utility and so provide the serial to TCP/IP conversion of data sent between the AcceptNet server and those remote panels. Other PC's (dedicated PC's) do not have the AcceptNet Client installed however still use the TCPtoSerial converter to connect a panel to the TCP/IP network.

Still further panels are shown connected to the server by the dedicated TCP/IP to serial Lantronix devices (UDS10).

Only TCP/IP connections are permitted across the Internet to panels. Later versions of AcceptNet lower bandwidth TCP/IP only based connections. Therefore a client connection across a *high speed* Internet connection is possible and Microsoft Network support (file sharing) is not required. For practical purposes however the bandwidth of such a connection should be greater than 1Mbps. Though lower bandwidths and modem connections are possible the performance of the application will suffer substantially from the reduced bandwidth allowable.

Where AcceptNet software version permits, connections to remote panels by PSTN can be established manually or scheduled to each panel. These connections will be permanent provided the number of modems at the AcceptNet Server is greater than or equal to the number of remote panels, otherwise the connections can be scheduled and limited according to the scheduler settings. For best performance high speed (19200 or better) external modems are recommended for the connection. For best results the panel(s) should be configured to use the External Modem comms task.

NOTE: Dial-up connections to panels require the use of the PC-direct protocol. Unlike the direct serial and TCP/IP connection access to the panel cannot be limited to the installed version of the AcceptNet server. Any PC-direct/Win-direct or AcceptNet access is permitted from any source where the INSTALLER PIN is known. For this reason PSD recommends the use of PIN's with 6 or more digits. Also the installer PIN should be hidden through suitable permission set programming from within the AcceptNet client user editors. Refer to section 4.3 below for information on setting up panel connections.

4. RUNNING ACCEPTNET SERVER FOR THE FIRST TIME

4.1. NETWORK CONFIGURATION

The AcceptNet system requires Microsoft TCP/IP support.

Prior to running AcceptNet software you should make sure that a suitable Windows compliant network card or dial-up modem is installed and a TCP/IP driver for that card/connection has been installed using the appropriate network applet under Windows. This must be done for both the AcceptNet Server and each AcceptNet Client. Make sure a valid TCP/IP address is or can be assigned for each machine that is unique on the network joining the two PC's.

Under Windows 98/95/NT and for a stand-alone installation of AcceptNet (server and client on the same machine – no network) a standard or compact Windows install is recommended, this *must* include dial up networking.

Under Windows 2000/XP, the default installation should at least include dial up networking and should be sufficient for a stand-alone configuration.

If the network you are using is not a registered IP sub-network (no IP numbers have been allocated to your locale domain) then you should assign IP addresses in the range 192.168.0.0 to 192.168.255.255. These addresses are usually assigned to local networks that are isolated from the Internet or other registered IP sub-networks.

Each client and server should must have a valid unique computer name and this name should have an associated IP address defined by a WINS server (where available), allocated by DHCP or entered in the HOSTS file under the WINDOWS directory or under WINNT\system32\drivers\etc.

4.2. HARDWARE KEY

Before you run the server application, make sure the DB25 or USB hardware key provided is plugged into the *printer* or USB port of the Accept Server PC respectively.

If the key is not installed properly (or the driver failed to be loaded during the installation procedure above) the following message will be shown:

“Invalid or missing hardware key”.

In which case you should make sure the hardware key is installed securely (make sure the printer port works – try a test print) and/or reinstall the software.

4.2.1. USB Keys

Under Windows XP/2000/98 a USB token should be installed automatically as soon as the item is inserted in a free USB socket. Therefore if supplied with a USB key ensure the key is inserted correctly and restart Windows before running AcceptNet Server to ensure the USB token hardware has been detected and Windows drivers installed properly. Once the USB drivers are installed log into Windows and start the AcceptNet Server.

4.2.2. Parallel Port (DB25) Key

If supplied with a parallel port key make sure the key is plugged into the parallel (printer) port *not one of the 25 pin serial ports*.

4.2.3. Registering To Upgrade Features

The AcceptNet Server access limits and feature list can be extended by entering an unlock code, purchased from Professional Software Design P/L, and using or entering code values in the registration dialog. To invoke the registration dialog, login to the server and select “Register|Upgrade” from the main menu. Once displayed you may enter the new unlock code supplied by PSD to extend various licenses in your system.

Before applying for your new unlock code you will need to carefully note, on a registration form, the **Key** and **Current Code** shown in the registration dialog, as well as a list of required new features and/or the additional access.

4.3. PANEL CONNECTIONS

When the server application is run for the first time, you will be asked to define at least 1 panel connection. Click ‘OK’ to proceed to the panel setup dialog and create a panel record by typing in a valid description/name for the panel. This name will be used throughout AcceptNet to reference the panel, choose a name

therefore that will help the operators/installers recognise the panel's purpose and/or location.

You can invoke the panel setup dialog at any time after first execution by logging in; "Login | Disable Clients", then selecting "Setup | Panels" from the main menu. Refer to the section **Server Login** on page 27.

4.3.1. Direct Serial Connection

Click on "Setup Comm..." button in the panel setup dialog to associate a direct serial port connection and configure the com-port number, BAUD, stop bits etc... 1 stop bit, 9600 BAUD, **no** flow control and **no** parity is recommended for each panel. The must match the relevant Concept comms task settings.

Ensure you know which com-port number is associated with each physical DB9/DB25 output plug of the PC, especially where multiple panels must be supported. Verify these serial ports are functioning correctly, if required (using Hyper-terminal to another PC for example), before you proceed.

In addition you may specify the communications protocol that will be used to communicate with the panel. Use "Accept" where-ever possible, only use PC-Direct to connect to panels that do not support the Accept comms task or when using modems to make connections. Review throughput is limited to < 11 review events per second when using PC direct protocol.

4.3.2. TCP/IP to Serial Connection

It is possible to connect to a panel via a TCP/IP network. A TCP/IP to serial converter must be attached at the panel to convert the panel's normal serial output to TCP/IP. You can use a PC located near the panel and the TCPtoSerial utility that ships with AcceptNet or you can use a hardware device (Lantronix UDS10, for example) to convert serial to TCP/IP.

When setting up the panel connection tick the "Use TCP/IP" option to enter the computer or host name of the TCP/IP device to which a panel is serially connected. Choose a TCP-port number that matches the TCP-port number of the host TCP/IP to serial device – usually 10001 in the UDS10. If you are using the TCPtoSerial utility then ensure the port numbers are the same at the AcptServer panel setup dialog and in the main screen of the TCPtoSerial utility. The computer or hostname of the TCPtoSerial utility will be the computer name of the PC running the AcceptNet Server. The serial port settings should be identical to

those values that would be entered in the AcptServer panel setup dialog if connecting the AcceptNet Server directly to a panel via a serial port, as above.

The TCPtoSerial utility or other TCP to serial device should have been installed/connected and configured prior to the setting up the connection in the AcptServer.

4.3.3. Generic Serial (CCTV) Panels

AcceptNet supports two panel types, the Concept panel by Innerrange and a Generic Serial panel for use with CCTV equipment, non-concept panels and possibly fire alarm systems. The generic input panel allows input sequences (log events) to be “captured” and processed in a similar way that review would be processed from a Concept system, producing an acknowledgeable alarm and state changes on locale diagrams etc... In addition control sequences can be sent to the serial device to control cameras etc...

AcceptNet cannot support devices that require intelligent hand shaking. However simple send/ack protocols can usually be supported but there are no facilities to handle error correction or intelligent recovery-handshaking. CCTV devices that require unsolicited unacknowledged ASCII key sequences (say devices that support a serial keyboard input) can usually be supported.

4.3.4. Lantronix UDS10

Checking Factory Defaults

To ensure that the UDS10 hasn't been pre-configured connect a UDS10 serially to a PC and run a suitable serial comms package (hyper-terminal). A “straight through” cable must be used to connect the device to a serial port of the PC – you do not need a null modem (cross-over) connector. The serial port settings should be 9600, 8 bits, 1 stop and no parity.

Once the comms package is started, power the UDS10 off then on, when the red LED flashes type a series of lower-case **x** characters on the keyboard. The welcome screen should be displayed. Press enter (<cr>) to reveal the main menu.

Make a note of the “*** basic parameters”. Make sure the IP address reads “0.0.0.0/DHCP”. If it does not then see the section below “**Resetting the IP address**” or “**Setting A Fixed IP Address**” to change the IP address to a suitable value.

1. Select item 7 from the menu to set the device to factory defaults.
2. Select item 9 from the main menu to save and exit.
3. Shutdown the communications session.

Resetting the IP address

Connect to the UDS10 via the serial port as described above and invoke the UDS10 welcome screen and main menu.

1. At the main menu type 0 (Server Configuration) then follow the prompts as follows:

```
IP address:  0 <cr><cr><cr>
Set Gateway IP address: N
Netmask...:  0
Change Telnet config...: N
```
2. When the main menu is redisplayed the “*** basic parameters” should read 0.0.0.0/DHCP.
3. Select item 9 from the main menu to save and exit.

NOTE: If a DHCP server exists on the network then after saving and exiting the UDS10 the device may receive an IP address from the DHCP server. You may need to reconnect “serially” to the UDS10 to read the new IP address from the “*** basic parameters” section. Make a note of this IP address for the purposes of testing the physical connection below.

Select item 8 from the main menu to exit without saving any changes.

Physical and Logical Connection

A suitable TCP/IP connection via a fixed network to the UDS 10 must be provided between the AcceptNet server and UDS10.

The UDS10 by default will have no IP address and will support DHCP however AcceptNet can only resolve connection details provided the UDS10 can be assigned a constant NAME (via WINS) or a fixed IP address. Consult your system-administrator for information about setting up Windows to dynamically allocate IP addresses and host names.

For the purposes of this guide we will use/assign an IP address of 192.168.0.99 for the UDS10 and a host name of “MYUDS10” which resolves to the above IP address.

If the *IP address of the UDS10 is known* (has been assigned by DHCP or a fixed IP address has been configured) then:

1. From a DOS shell: C:\> PING 192.168.0.99
2. Otherwise, where a valid host name (eg. MYUDS10) exists for the UDS10, from a DOS shell try:
C:\> PING MYUDS10
3. If the physical connection is OK you will receive several of the following.
Reply from 192.168.0.99 bytes=32 time<10ms TTL=64

Note the returned “time” value may change and may give some indication of the quality of the connection.

If you do not receive the packet confirmation information of step 2 then the physical connection or IP routing to the device is invalid – at which point you should contact the network administrator to fix the problem.

If the *IP address has not been assigned* to the UDS10 and not DHCP is available then:

1. Make sure there are no other devices on the network that have *not* received an IP address.
2. From a DOS shell:
C:\> ARP -s 192.168.0.99 00-20-4A-??-??-??
Look at the product information label on the UDS10 to get the three missing two digit (??) number used above.

C:\> TELNET 192.168.0.99 1

3. The above connection attempt will fail – shutdown the telnet session, the UDS 10 device will now assume an IP address of 192.168.0.99.
4. From a DOS shell:
C:\> TELNET 192.168.0.99 9999
5. If the physical connection is valid a successful telnet session will be established and the UDS10 welcome message will be displayed.

Alternative Test

Follow steps 1 to 3 of the above then start a web browser (Internet Explorer/Netscape) specifying an URL of `http://192.168.0.99`

You should (eventually) see the UDS10 configuration form in HTML format. Exit the browser: Setting up the UDS10 using this HTML form is *not* documented in this guide.

Setting A Fixed IP Address

Set a fixed IP address if you do not wish to use dynamic IP address allocation by DHCP. Connect to the UDS10 serially as mention in the above section “**Checking Factory Defaults**”.

After the welcome screen is displayed hit <enter> (carriage return <cr>) to invoke the main menu.

1. Select item 0 to configure the IP address.
2. At the main menu type 0 (Server Configuration) then follow the prompts as follows:

```
IP address:  192 . 168 . 0 . 99
Set Gateway IP address: N
Netmask...: 0
Change Telnet config...: N
```
3. Select item 9 to save and exit the UDS10.
4. Shutdown the telnet/comms session.

The UDS10 should now have a fixed IP address of 192.168.0.99 (or the IP address of your preference). Verify the IP address by following the steps in the section above, “**Physical and Logical Connection**”.

General Programming of the UDS10

Connect to the UDS10 serially as mention in the above section “**Checking Factory Defaults**”. Or by starting a Telnet session from a DOS prompt by:

```
C:\> TELNET 192.168.0.99 9999
```

OR

```
C:\> TELNET MYUDS10 9999
```

1. Once the welcome screen is displayed hit enter (<cr>) to invoke the main menu.
2. Select item 1 (Channel 1 configuration) from the main menu.

3. If factory defaults have been imposed then you should not need to change any of the displayed default parameters, thus ensure the following values are given:
Baudrate: 9600
I/F Mode: 4C
Flow: 00
Port No.: 10001 // This is the TCP port number you *must* use in the panel setup dialog
// under AcceptNet to connect to this UDS10 at IP address 192.168.0.99.
Connect mode: C0
Remote IP address: 000 . 000 . 000 . 000
Remote Port: 00000
DisConnMode: 00
FlushMode: 00
DisConTime: 00:00
SendChar 1: 00
SendChar 2: 00
4. You may change the port number above to another value (do NOT use 2149 however). You must select a TCP port number that is not used by *any* operating system or other application services on the AcceptNet server machine.
5. The Remote PORT and Remote IP address are *not used* since the UDS10 is configured (as above) to automatically *listen* for remote connections. The remote address information therefore is determined from the connection request issued by the AcceptNet server.
6. Select Item 9 (save and exit) from the main menu.
7. Disconnect from the device, shutdown the Telnet/comms session etc...

Connecting the UDS10 to the Panel

Once the UDS10 has been configured, you must connect the UART port to the UDS10 DB25 pin interface using a suitable cable. *The PC-direct or Printer cable will NOT work.* See the note about cables below.

Cables

If you are using a standard PC-direct cable or Accept cable from the panel then you *will* need a NULL modem (cross-over) connector to the UDS10.

Otherwise a standard external modem cable as supplied for the Concept panel is **recommended** to connect directly from the UDS10 to the panel UART port. This requires **no** rewiring or converters.

Port Configuration

As per the usual com-task programming at the Concept panel, you should ensure that no other Concept panel comms tasks are assigned to the same UART port number.

1. Use the default Accept/Commpass comms-task settings.
2. Ensure the baud rate is set to 9600 on the correct UART port number.
3. Ensure the client code is set to 0001.
4. If the server has never communicated with the panel before then you will need to set the K option to Y in the final sub-menu of the Commpass/Accept comms task.
5. Once a connection is established to the panel (via TCP/IP) through the UDS10, communication with the panel is the same as for a local/direct serial connection.
6. You may need to login to the server and **Re-establish Session Keys** from the **Admin** menu under the AcceptNet server before you can successfully initialise panel communications. Refer to the on-line help under AcceptNet server for more information.

AcceptNet Server Panel Setup

If you are using DHCP to dynamically allocate an IP address to the UDS10 then make sure when you program the panel settings in the panel setup dialog that only a HOSTNAME is shown. Enable (tick) the “IP addresses dynamically allocated” option in the COMMS page of the preferences dialog in the AcceptNet Server application to disable entering/use of IP address values when setting up panel connections.

If you have assigned a fixed IP address to the UDS10, untick the “IP addresses dynamically allocated” option in the COMMS page of the preferences dialog in the AcceptNet Server application to disable entering/use of IP address values when setting up panel connections. You may now enter an IP address or resolve an IP address when setting up a panel connection.

4.3.5. Modem Connection

It is possible to connect to a panel using a modem. A valid modem device must have been installed under Windows in order to be able to use this option.

The modem connection uses the PC-Direct protocol only. You must enter a phone-number and a valid TAPI device for the panel connection record to be

accepted. . More than one panel can share the same modem, however the connection to each panel will be shared depending on the type of schedule running and the connection/schedule timing of any applied timer scheduling.

4.3.6. Modem Schedules

There are three types of modem connection schedules.

1. Manual
2. Update
3. Timed

The **Manual** schedule is only available when the timed schedule is deactivated. This schedule assumes all manually initiated modem connections are permanent until manually disconnected. If a panel update is triggered, any existing manual modem connections will be reset.

NOTE: A manual connection initiated while a timed schedule is active simply pre-empts connection to the selected panel. Thus the schedule will re-order itself to connect the selected panel immediately but the modem schedule will still be active. Thus after the selected panels scheduled connection time is expired the scheduler will connect the next panel in the current schedule list for that modem.

The **Update** schedule is triggered from a client (where permissions allow) and allow an operator to initiate a modem-connection to off-line panels for download of any outstanding database changes. The update schedule overrides any other schedule type. Once changes have been downloaded to the required panels, the update schedule is cancelled. The system returns to the timer schedule if enabled. Once an update is initiated it will attempt to download changes to the panel forever !! You must therefore make sure that a reliable connection to the panel(s) can be made by modem as required if giving users access (permissions) to this feature in the AcptClient. You can reset the scheduler by selecting the “reset the modem schedule” option in the Admin menu of either the AcptServer or AcptClient (after controlling the server where permissions allow).

The **Timer** schedule includes a start time, repeat count, connection time and modem control time. A unique timer schedule can be applied to each modem available. Once a modem schedule has been configured, all modem connected panels of a particular common modem device will be dialled according to the connection and total periods. By using a timer schedule more than one panel can share the same server modem. The modem timer scheduler is invoked from either

the panel setup dialog or from the panel status dialog once logged into the AcptServer.

The “**Start Time**” is the time at which the panel connection list is executed. That is the first panel in the schedule list will be dialled at or just after the start time. If the start time is not ticked the scheduler will start immediately the dialog is closed.

The “**Repeat Every**” time is the time the schedule process will allocate to a particular list of panels. Thus the connection list is executed to completion once then repeated according to the repeat settings. Once a connection list is executed to completion any “start time” will be incremented by the value of the repeat interval. For example if the start time is 10am on 15 Jan 2003, once the connection list is executed to completion the start time will automatically be set to 10am 16 Jan 2003 where the “repeat every” value is set to 1 days.

The **Duration** of a panel connection is the amount of time a modem will remain connected or attempt to connect to a panel. During this time AcceptNet will be able to “talk” to the panel.

The **Total Time** is the total time allocated to the panel item in the schedule list. The scheduler will wait the “total time” before dialling the next panel in the connection list. If the duration is smaller than the total time then there will be a period of time after the duration time during which the modem will be inactive (disconnected) before the next panel in the connection list is dialled.

4.3.7. Connection Security

AcceptNet server supports additional security features which prevent access to panels, intended for a particular installation, from being accessed by another version of the software located elsewhere. This security only applies to panel connections that employ the Accept or Commpass comms task protocol.

The panel connection is “locked” by AcceptNet Server when it first communicates with a panel. Thereafter only that instance of the AcceptNet Server will be able to communicate with a panel using the Accept comms task.

To reset the connection to a panel the INSTALLER must login to the panel, via a terminal and reset the Accept comms Task by:

1. Deactivating the Accept comms task at the panel via a terminal
2. Re-setting the K option to Y.

3. Re-activating the Accept comms-task.
4. Recover session keys (Admin | Recover keys...) at the AcceptNet Server. This will redefine a unique key for the connection and “lock” communications to that instance of the server software. This may take some time depending on the configured comms. timeouts in the preferences.

If the AcceptNet server dongle is replaced or software was re-installed on a new PC. you may skip the first few steps and just try the procedure in step 4 above.

4.4. CLIENT CONNECTIONS

When the server application is run for the first time, you will be asked whether the AcptClient is or will be installed and connected to on the same machine as the AcptServer. If you select “No” you will need to enter a client connection definition in the ensuing client setup dialog.

Whether you select to install a local client or manually enter a remote client definition, you can still invoke the client setup dialog to modify client connection details at any time after logging in “Login | Disable Clients” then selecting “Setup | Clients” from the main menu when available.

When using the client setup dialog you must enter a description of the client machine for reference only as well as the PC (Computer) name of the client machine running AcptClient. If setting up a local client activate the “local client” button to setup the connection parameters automatically.

Make sure the TCP port number is 2149 for each connection, you can only run 1 AcceptNet Client on each client machine on the network. If the port number is not correct you may need to open the “Setup | Preferences” menu item and change the port number in the Clients page of the ensuing dialog – see below.

NOTE: The port number, 2149, has been reserved by IANA for use exclusively by the AcceptNet software therefore you should not need to change it. If it is already being used by another application (other than an AcceptNet application) then that software should be configured to use a different port number for its network services.

Once the client and panel details have been correctly entered the server will initialise connections and the main menu will be enabled.

As soon as a valid AcptClient to AcptServer connection is established, it will be locked. Once locked only the PC whose computer name is entered in the

appropriate client connection record in the “setup clients” dialog will be allowed to connect to the server. All AcptClient PC’s *must* have unique computer names. In order to allow AcptServer to accept a new connection from another PC with the same name the connection record in the “setup clients” dialog must be unlocked by activating the “unlock” button. Changing a PC’s hardware configuration, upgrading the operating system or installing new fixed drives may require the AcceptNet client/server connection record to be “unlocked” before communications will be allowed.

4.4.1. Terminal Services

AcceptNet does not support terminal services. If Microsoft terminal services are used connection to the AcptServer and or use of either the AcptClient/AcptServer may be problematic. You must apply for extra client licenses to run more than 1 AcptClient

4.5. SERVER LOGIN

To extend the menu, for access to the Admin and Setup functions you will need to login. Open the “Login | Disable Clients” menu item to invoke the login screen.

The default login password is “Accept” (case sensitive, do not include the quotes). You should change this password (Select “Setup | Change Password”) as soon as possible.

Entering the password incorrectly three times will result in a delay being imposed before an attempt to login again is accepted. The delay is configurable in the preferences once logged into the server.

4.5.1. Operator Password

The login dialog now requires a genuine operator password. That is the same password an operator would enter when logging into an AcceptNet Client.

The AcceptNet server expects the password to be either the INSTALLER’s password or the password of an *additional* operator. The “*additional*” operator is defined in the preferences dialog (client page) and cannot be the INSTALLER. When the additional operator is specified the AcceptNet server login dialog will accept either the INSTALLER’s password or the “additional” operators password. The password therefore will determine whose name appears in the server event

log for the login event. If no operator accounts have been created (other than the INSTALLER) then no “additional” operator will be allowed.

The default case sensitive INSTALLER password in the AcceptNet system is “Accept”.

4.5.2. Uploading Panel Configuration

Proceed to the Admin menu and select “Upload All Panels” to upload all information relevant to the panels you have configured previously. Once the upload has completed you should open the “Update States All Panels” item to synchronise state information in the server database according to the current state of inputs, auxiliaries etc... at the panels.

Once the panel data has been uploaded and states updated, you can proceed to use AcceptNet to manage your security. Click on the “Login | Disable Clients” to enable client access to the server. The Admin and Setup menus will be hidden and the “tick” next to the “Disable clients” item will no longer be shown.

The database is deemed invalid until all specified panel connections have been uploaded correctly. Most front-end features will be disabled while the database is deemed “invalid”.

5. RUNNING ACCEPTNET CLIENT FOR THE FIRST TIME

Before running the client for the first time you should ensure the server has been installed as above and is running. Also make sure the server has not “Disabled Clients” under the Login menu of the AcceptNet Server – the server should only show 4 menu items when “logged out”.

The default login password for the AcceptNet Client INSTALLER account is “Accept” (case sensitive, do not include the quotes). You should change this password (Select “Setup | Change Password”) as soon as possible.

Provided a valid TCP/IP network connection exists between the client and the server application you should be able to start the application and receive a login dialog. You should also see “LOGGED OUT” in the operator status box at the bottom right of the client application screen. If the application fails to run or “NO SERVER” is displayed you will need to do one or all of the following.

1. Ensure the AcceptNet Server application is running
2. Ensure the AcceptNet Server host machine is accessible from this workstation – that is, you can ping or telnet into the AcceptNet Server PC across the network.
3. Check the server connection parameters by clicking on the “Server” button of the login dialog, the “Find Server” dialog is displayed. Set the “Server Name” to the IP host name (usually the computer name) of the machine running the AcceptNet Server or set the IP address to that host machine if the hostname/computer name is not known or doesn’t work and cannot be resolved. Ensure the TCP port number is 2149, ie. the port number configured at the AcceptNet Server above.

Ensure the database Service is also set to 12005. This port number is reserved for use with AcceptNet by IANA. The DB server properties in the AcptServer Preference should be set to mirror this service/port number. *The administration port in the DB Server preferences should always be 1 more than the data port.*

If a connection cannot be established within a few seconds, restart the AcceptNet Server and AcceptNet Client. If a connection to the AcceptNet Server still fails to proceed then check your network settings and AcceptNet server network accessibility.

5.1. CONTROLLING THE SERVER

In order to access any features which affect the total AcceptNet installation (eg, full upload/download, tenancy, panel preferences, review management, graphics etc...) the server must be controlled exclusively. When AcceptNet is under “server control” only one operator can administer the system at any one time.

To control the server from the AcceptNet Server application you must disable any connected clients. If you select “Login | Disable Clients” and login successfully, all connected clients will be ungracefully disconnected. You can warn the clients that you intend to “disconnect” them by using the “Broadcast Message” feature and typing in an appropriate message string. Then activating “OK” sends the message to all connected clients.

Once the “Disable Client” item has been invoked and all clients have been forcibly disconnected/logged-out, the Admin and Setup menu’s will become visible. When finished administering the system don’t forget to “Enable Clients” so that the clients can regain access to the AcceptNet system. The idle logout feature in the AcptServer, if configured in the AcptServer preferences, will automatically enable the clients once a specified idle time is exceeded.

You can also control the server from an AcceptNet Client (“Admin | Control Server”) however no broadcast message system is supported. Again once exclusive access is granted the server will forcibly log out all other AcceptNet clients in the system. When finished administering the system don’t forget to “Admin | Relinquish server” at the AcceptNet Client to give up exclusive access and allow the other clients to regain access. Ensure that this option is generally NOT enabled in an operators permission set (“Admin | Permissions” in the AcceptNet Client).

5.2. TENANCY

A tenant in the AcceptNet system consists of a group of AcceptNet clients that belong to an isolated section of a secure building or buildings. Specific areas, doors, lifts, users and user types can therefore be reserved for use by specific tenants and be hidden from other tenants in the building(s). An operator is associated with a particular tenant via the permission set, in which a tenancy ID is defined. Every time that operator logs into an AcceptNet Client the tenancy associated with his/her permission set is applied.

You can only create and modify a tenancy from the AcceptNet Server application or modify an existing one from the AcceptNet Client provided Server Control (see section 5.1 above) is established.

The MAIN(1) tenant is the initial system default tenancy. It contains no sections and so allows full access to all panel entities. Operators in single tenancy installations should use this default tenancy.

An operator limited by a tenancy other than MAIN(1) will likely have restricted access to some panel entities. That means only those entities reserved to an operator's tenancy or any unrestricted entities will be visible from the user editor by that operator. For example only a subset of a panel's total areas will be controllable or editable from within the AcptClient by operator X of tenancy 1 while operator Y of tenancy 2 is unable to see areas reserved to tenancy 1 and will see a different subset of areas. Both operators can see unrestricted (usually unassigned) areas.

5.2.1. Sections

A list of sections defines a tenancy. Sections are allocated to panel entities from within each of the appropriate DB editors. An operator of a tenancy can only access, control or edit entities whose sections are also members of the operator's tenancy or whose sections are set to <unrestricted>. Sections are created, renamed or removed from tenancies using the tenancy editor.

A section represents a sub-group within a tenancy. When an entity is placed in that sub-group it is effectively reserved for use only by the tenant to which the section belongs.

For example: Assume that every tenancy contains 1 unique section. Assigning a section to an entity in an entity editor (user, door, area, list editor etc...) therefore reserves that entity to the specific tenant.

In reality however it is likely that certain entities within the panel(s) configuration will be common to more than one tenant. For example the front door to the building in which several tenants reside. Thus the front door needs to be allocated a section which will allow it to be used by all tenants. In such a case an additional "common" section would need to be created and elements like the front door assigned with that section. That special common section can then be added to all relevant tenants' section lists thereby allowing access to that common element by operators from each those tenancies.

5.2.2. Tenant Specific Review

Review is logged for each tenant separately. Thus only events that are relevant to a tenancy are logged in the tenants current or archived review logs. Events for which no tenancy association can be determined (eg. system events) are sent to all tenants. All review is logged by the “MAIN (1)” – default – tenancy. It is possible however that while one part of the review is specific to a tenant and another part is specific to all tenants (eg. the area of an “xmit alarm in area” review event might have a section while the input doesn’t or has a different section). In that case the event will be logged for *all* relevant tenants’.

Each new (non-default) tenant must define a review log ID string that will uniquely identify the current review log associated with that tenant at the AcceptNet Server. As well the archive directory to which review will be archived from the tenant’s current review log and the frequency of the archive in days must be entered. Choose an archive directory that is writable only from the AcceptNet server. Care should be taken to ensure that the archive directory is unique for each tenant, so that other tenant’s review is not archived to the same directory.

For a single, MAIN(1), tenant system there may still be a need to customise the archive review parameters using the tenancy editor. The review log ID should *not* be modified however. By default all review in the single default tenancy system is archived to the “Archived Review” subdirectory under the directory where the AcceptNet server is installed

5.2.3. Default Tenancy While Logged Out

Each AcceptNet Client must be associated with a default tenancy. This therefore determines the tenancy that will be applied to alarm processing while the client application is **not** logged in, that is there is no operator or permission set in effect. Generally a client machine will belong to a particular tenant in which case that machine’s default tenancy will be the same as the tenancy of the permission sets of the operators that uses that machine.

Change the default tenancy in the “Login/Out” page of the “Setup | Preferences” dialog at the AcptClient.

For a single tenancy system using the default tenancy, the logged out tenancy will be the first tenant “MAIN (1)”.

5.3. PERMISSIONS

When a client has exclusive (server) control of the AcceptNet system the permission set editor can be used to define/modify permission sets throughout the AcceptNet network, regardless of the current operator's tenancy. An operator however cannot modify the tenancy of their own permission set nor that of the INSTALLER.

When a client does not have exclusive control of the server the permission set editor will only grant access to permission sets of the same tenancy. Therefore, an operator cannot modify the permission set of another tenant unless they control the server exclusively.

Refer to section 7.6 on page 42 for general information about permission sets.

5.4. OPERATORS

When a client has exclusive (server) control of the AcceptNet system the operator editor can be used to define/modify operator information throughout the AcceptNet network, regardless of the current operator's tenancy. An operator however cannot modify their own account nor that of the INSTALLER.

When a client does not have exclusive control of the server the operator editor will only grant access to operators of the same tenancy. Therefore, an operator cannot modify the account of another tenant's operator unless they control the server exclusively.

Refer to section 7.7 on page 42 for general information about operator definitions

6. TROUBLE SHOOTING

Invalid or Missing Hardware Key.

You must ensure the hardware key (the DB25 pin male to female plug) is plugged into the printer (parallel) port *not the serial port* of the PC. If supplied with a USB key you must install the USB key into a free USB port. Insert the USB key before running the AcceptNet Server. If running W2000/XP/9X an “installing new hardware” dialog should appear. Wait for the system to recognise the hardware then restart the PC. Once restarted run the AcceptNet Server.

Exception Running “Setup|Alarm Handling Messages”

When installing AcceptNet onto systems running NT 4.0, AcceptNet relies on certain Microsoft DLLs that are normally present in a standard NT 4.0 installation. It may be necessary to install WordPad for NT, this will additionally install the shared DLL’s that the alarm handling editor requires.

Difficulties Communicating With the Panel

The most common cause of problems are

1. Invalid port settings, check stop bits and BAUD rate, ensure **no** flow control **nor** parity is selected in the panels communications setup dialog invoked from the AcceptNet Server: “Setup | Panels | Setup Comms...”
2. Cable not connected because of:
 - ◆ Trying to use the wrong PC COM port or trying to use the COM port connected to the serial mouse.
 - ◆ Physical disconnection, external cable fault or cable not plugged in
 - ◆ Internal cable connection fault – check with your PC supplier.
 - ◆ Cable length exceeds RS232 specification.

NOTE: You can verify correct functioning of the PC port by connecting two PC’s together through a null modem connecting the serial ports you wish to test. Run and configure HyperTerminal on each to see if you can transmit and receive characters across the connection.

3. Incorrect configuration of port/baud or options in the panel. Refer to your Concept Panel documentation for more information. The comms task settings are entered as follows:
 - ◆ Deactivate the Accept comms task
 - ◆ Set baud rate to 9600

- ◆ Set UART port to 1,2, 3 or 4. Connect the PC direct cable at the same UART port as programmed.
- ◆ Set the client code to 0001
- ◆ Reporting options are normally all set to ‘n’
- ◆ Set the extra options as follows:

```

Extra Opts.          . . . S P C K D
                       n n n Y n n Y n
  
```

NOTE: The K setting automatically resets to “n” when successful communication to the server ensues.

- ◆ If communications still fails, try “Admin | Recover keys..” from the AcceptNet server.
4. Incorrect Baud Rate
 - ◆ Does not match Comms Task “Compass”/“AcceptNet” settings in panel.
 - ◆ Rate too fast for line quality, try a slower baud rate. For example: 4800 instead of 9600.
 5. AcceptNet can not access the required COM port. Because another windows application (eg. HyperTerminal, the mouse driver etc...) is using it. Close all other applications - restart Windows to be sure or chose another comms port.
 6. Check the event log in the AcceptNet Server for exception notifications.
 7. Re-set the K option to Y in the Accept Comms task in the panel and from the Admin menu in the AcceptNet Server choose “Recover All Session Keys” or “Recover Session Key...”. This operation may take some time to complete.

If you are still having trouble and you are sure that all the links and settings are correct, then shutdown AcceptNet Server, restart Windows then the restart the server application and try again.

7. GETTING STARTED WITH THE ACCEPTNET SYSTEM

You first things you should do (as INSTALLER) are:

1. Using the AcceptNet Server: Upload all panels, then update states from all panels.
2. Plan your tenancies if more than 1 tenant exists in the installation. That is: define the likely common and unique sections. Work out what doors, areas, lifts, time-zones, menu-groups etc... should belong to which tenants and apply the appropriate sections to these using the panel entity editors.
3. Setup each tenant's operators and permission set. Make sure the "Server Control" option is *disable* for all but the most trusted operators.

7.1. GETTING STARTED WITH THE ACTPNET CLIENT

The first things you should do after you login to the AcceptNet Client are:

- Change your default password, create operator accounts, and setup the permissions for operators specific to the tenant responsible for the client machine.
- If you have logged in as INSTALLER and are using the default password, the application will warn you that this is not a secure password. It is not secure because it is a documented default – so is well known.

7.2. CHANGING THE OPERATOR PASSWORD

To change the current operator's password, once logged in, choose "Setup | Change Password" from the main menu. Alternatively use the operator setup dialog (Admin | Operators) to modify the password for an account which is *not* the current operator's.

You can only change the password if you know the old one. Enter the current password where it reads 'Old'. Enter the preferred new password where it reads "New" and verify it – retype the new password where it reads "Verify" (to make sure you haven't mistyped the "new" password)

Once modified an operator password applies to all AcceptNet Clients in the AcceptNet network. *Changing the INSTALLER or "additional operator" password changes the relevant login passwords on the AcceptNet Server (post V2.7.0).*

7.3. THE REVIEW LOG

The review log is a dynamic log of events sent by a panel to the AcceptNet server. The review log viewed at any one time may be a subset of the total information stored by the AcceptNet System depending on the constraints of any custom review filter applied. However once a valid database is uploaded and subject to the integrity of communications with the panel AcceptNet will store *all* review received by the panel in the dynamic review log file in the AcceptNet installation directory.

This log can become unwieldy if it is not archived regularly – this could result in system failures due to lack of resources (memory etc...) and will be slow to process, open and update. There is no need to store large amounts of review in the dynamic (active) review log since a report of past review can be simply achieved using the “review | search archive“ feature. In addition the review log should be archived and preserved in case of file system error should the dynamic review log get damaged.

Entity names should be chosen (for doors, areas, inputs etc...) that reflect the panel, building or section they belong to so that the review is more meaningful.

NOTE: In a multi-panel system it is imperative that the amount of review produced by the panels be limited to only the most necessary events – specifically those events that deal with user access and or alarm notification. Be careful however *not* to turn off necessary auxiliary logging at the panel. Auxiliary events are used to identify door locks on/off activity and keep track of the door state. Use the review process editor to further reduce the events that are logged. “Tick” the “Do not log” option in the general or specific criteria page for relevant review event groups to reduce the amount of unnecessary review.

7.3.1. Automatic Archiving of Review

Review Archive timing is defined per tenant in the tenancy dialog discussed above (section 5.2 **Tenancy** on page 30).

Ensure that the number of days is set such that the total review accumulated does not exceed 10,000 events between archives. The created archive files are stored in alpha-date order and can be concatenated into one large review log as required. Setup an archive time such that as few operators as possible will be inconvenienced when the AcceptNet server archives review – all review log windows are closed on the AcceptNet Client when review is archived.

There should be no need to generate complicated reports on the current review, instead restore multiple archive files and apply filters thereafter.

7.3.2. Queryable fields

Custom review filters may contain “queryable conditions” a queryable condition will appear in the condition list with a value of “???”. A queryable field is resolved at the time the filter is applied. When a filter is executed or applied AcceptNet looks for any queryable conditions and if found will prompt the operator for suitable search values. If no values are entered then the queryable conditions are ignored and the filter is applied as if those queryable conditions were removed from the filter definition.

For example: A queryable user access filter might contain a “user=???” query and a “door=???” query. When executed the filter allows a number of reports to be generated for each just by changing the value of user ID when requested and without having to edit and save the review filter each time.

7.3.3. Searching the Archive

Select “Review | Search Archive” to search through the review archive for the current operator’s tenancy. Enter a date range over which you wish to conduct the search, choose a date range that will result in a suitable number of events, if the result set of events is too large AcceptNet will display nothing and indicate an error. Specify an additional custom review filter to further limit the result set to the required “type” of review. If the filter contains queryable condition you will be asked to enter the desired values (eg the user ID, the door ID) to be applied in the search

7.4. SETTING UP APPLICATION PREFERENCES

Select “Setup | Preferences” from the main menu to adjust application defaults.

7.4.1. AcceptNet Server Comms Preferences

Panel Communication Polling and Integrity

The physical connection between the panel and the front end should be tested periodically. The value entered in the “Poll/Test communications” input box determines the delay period before communication with the panel is tested whenever the application is idle. The actual time it takes to determine a comms

failure may be longer (an additional 10 seconds) than this value due to grace timeouts in the communications protocol with the panel.

For busy systems running poor quality connections increase the Packet Wait Timeout, Character Wait Timeout and Maximum packet retries.

If the “Notify on comms errors” is ticked, then any communications failures as a result of the poll testing above will be reported in the AcceptNet event log.

To view activity between the AcceptNet Server and the panel enable the “Show Rx/Tx lights” options. Two EIA coloured squares will appear in the bottom left of the server main screen. Red indicates data received/transmitted from/to any panel and green indicates no-activity. The timing of these status lights is not in “real time” so merely reflects activity in the line.

Panel Clock Synchronisation

The “Synchronise Panel Clock” option will configure the AcceptNet Server to update all panels’ clocks to reflect the PC system time whenever AcceptNet is restarted. In general this is not recommended as PC system time can be changed through the operating system too easily thus resulting in potentially inaccurate review time-stamping and or panel time-zone related security failures.

7.4.2. AcceptNet Client Login/Logout Settings

Automatic Logout

Idle operators can be logged out automatically. Thus if an AcceptNet Client has not been used for some time the system can automatically log out the current operator, so protecting the system from unauthorised access. If you do not want idle operators to be logged out, *ever*, then **un**check the “Logout Idle Operator” checkbox.

If automatic logout is enabled, (i.e. the “Logout Idle Operator” checkbox is checked) then choose an appropriate idle time in seconds (60 = 1min, 300 = 5 minutes etc..). The idle time is the period of time during which no keyboard or mouse activity is detected in the AcceptNet client application. Thus if there is no keyboard or mouse activity within the AcceptNet application for more than the idle period, the auto-logout process will be initiated and the grace period commenced.

If automatic logout is enabled, ie. the “Logout Idle Operator” checkbox is checked, then choose an appropriate “Logout Grace Period” in seconds (60 = 1min, 300 = 5 minutes etc..). The grace period is the amount of time AcceptNet will tolerate the idle operator condition once detected, before completely logging out the operator from the application.

NOTE: *In certain circumstances (during critical processing like panel upload/download) the auto-logout feature will be suspended. This means that while “idleness” is still timed and the grace period checked the current operator will not be automatically logged out. For example auto-logout is suspended during uploads and downloads to the panel, this prevents the upload/download process from being interrupted should the time taken to complete be larger than the operator idle-time. Once the critical process is completed however and/or the underlying dialog closed, if the idle and grace periods have been exceeded the current operator will be logged out immediately and without grace.*

Minimum Password Size

Set the minimum password size on an AcceptNet Client to ensure that operators are assigned passwords greater than a minimum length of characters. This prevents the use of null passwords (0 length passwords) which undermine the login integrity. The greater the number of characters the greater the number of permutations possible and the harder it is for an unauthorised user to guess a password.

Password Retry Limit

The password retry limit determines the maximum number of attempts an operator is permitted when entering their password before the login process is deemed failed. Once the retry limit is exceeded the application will be closed. This helps to make random access hacking more difficult. This option is only applicable where the “login to exit” preference is disabled.

Login To Exit

When set this option disables the shutting down of AcceptNet Client from the login screen. Hence a record of the operator that closes the application is ensured if this option is on (ticked). When this option is disabled (un-ticked) no record of who shut down AcceptNet Client is recorded in the login log.

NOTE: A program termination from the operating system, power failure or other system failure will most likely *not* result in a valid login log entry regardless of the value of this option.

7.5. SECURING ACCEPTNET

The AcceptNet software, the underlying operating system, file system and network security where applicable as well as the physical security (location) of the PC must all be considered in systems that require an uninterrupted and unadulterated stream of review, operator logging and alarm handling.

Access to the software or its information can be controlled in several ways:

1. Operator permission sets – to control access to various parts of the AcceptNet System.
2. Change login preferences:
 - ◆ Login to exit application - option enabled or disabled to help prevent unauthorised termination of the AcceptNet application from the login screen
 - ◆ Minimum password size - to make it more difficult to guess an operator's password
 - ◆ Logout idle operators - to prevent unauthorised access when AcceptNet is unattended but logged in.
 - ◆ Password retry limit – to slow down password guessing.
3. Choice of appropriate (non-obvious) passwords.
4. Limit file access and increase network security and limit file sharing – to protect against public access to files used by AcceptNet from a remote system or from the Internet via FTP, Telnet etc..
5. Limiting access to various PC control functions (like the task manager), registry, system clock, shutdown/restart and control panel – to prevent the application being uninstalled, terminated or its run-time parameters modified illegally.
6. Regular backups conducted. Auto-backup enabled in the AcceptNet Server. Backups to be stored securely so that log and other information can be stored permanently in a format and location that cannot be easily breached.
7. Limiting physical access to the PC's running AcceptNet, power supply of the PC's or cabling thereto.

It is not sufficient to rely on AcceptNet security settings or permission sets to control security if at any time a user can access modify and/or delete the login and review logs after a theft or security breach has occurred by using tools available to a Windows literate user.

7.6. DEFINING PERMISSION SETS

A permission set can be applied to every operator or a number of operators. They can be likened to panel menu groups and simply control which features in AcceptNet are available to an operator and which will be hidden or disabled.

7.6.1. Default/Installer Permissions

The installer permission set – the default set created when the software is installed for the first time (called “Full Access” or “INSTALLER”) cannot be deleted, nor modified by any operator other than the Installer.

The permission set of the default operator (INSTALLER) after installation allows access to all features of the application.

Permission Sub-Setting

Only the installer has access to the permission sub-setting option in the permission setup dialog.

Once sub-setting is enabled (by the installer), any permission sets created by any operator (other than the installer) can never be “better” than the INSTALLER permission set. Thus if the installer modifies the INSTALLER permission set such that the installer database editors are disabled, when other operators log-in they will not be able to change the installers permission set nor tick the features that the installer has disabled through sub-setting. Thus the permission options un-ticked in the installer permission set will be unavailable (greyed out) to other operators. Other operators will not be able to create a new permission set that will allow them to enable any of those unavailable features. Those features disabled in the installers permission set will be permanently unavailable until the *installer* logs in and re-enables them (ticks them) in the installers permission set.

7.7. DEFINING OPERATORS

In an application being accessed by different operators (security guards, office staff etc...) it is a good idea to define unique operator accounts to each of these persons. By defining a unique account, the administrator (or a person with high authority), can control which features each operator may access when logged in to the AcceptNet application.

For example:

The personnel manager may need access to the user database editor but should be denied access to the timezone editor. All non-administrative users should be denied access to the preferences and permissions setup.

Select “Admin | Operators” from the main menu to invoke the operator setup dialog. Operators cannot change their own permissions. The current operator will be warned of this before they try to edit their own details.

To define a new operator, activate the “New” button and enter the operator’s details.

Finally:

- Enter a “Login Name” for the operator. This is the *case-sensitive* name the operator will need to enter in the “Name” field of the login dialog when logging in.
- Type in a unique password. A password is required that at least meets or exceeds the minimum password length as specified in the Preferences dialog – explained in the section **Minimum Password Size** on page 40. Verify the password by retyping it in the “Verify” field. The password will be checked for correctness once the “Done” button is activated.

Remember: The passwords and login names are case sensitive.

- To clear the selected operator’s password, click on the button marked with a red cross next to the “Password” field of the dialog. If the minimum password length is non-zero then you will need to enter and verify a password for this operator before AcceptNet will accept any changes.
- Specify the permission set you wish this operator to use. Modify the permission set or create one in the permission setup dialog invoked by clicking on the + button next to the permission set drop down list box.

Refer to the section **Defining Permissions** on page 42.

7.8. OPERATOR LOG

A record is kept of all logins and logouts as well as DB edits and entity (door, input, area etc..) control attempts, so an audit trail is available to show operator activity and prove responsibility. Operator events are either stored in the review log, according to the “Setup | Preferences | Client | Log Operator Activity To Review” option in the AcceptNet Server or locally on the client machine in an operator log file if this server preference is *not* ticked.

8. USING THE ACCEPTNET SYSTEM

AcceptNet supports the following features:

- Review Monitoring and Alarm Processing
- Graphical Security (Locale) Monitoring
- Control of Concept Peripherals
- Full Panel Programming
- Customised Review Management

8.1. MONITORING

Monitor alarms and events or state changes using either or all of the review logs, mimic panel or locale diagrams

8.1.1. Mimic (Annunciation) Panel

The area grid displays the on/off or Alarm State of selected areas, all or *assigned* areas in the system. All concept inputs should be placed in closed areas in order to make full use of the mimic panel system. When an area changes state, the colour of the relevant grid element changes according to the colour-key in the bottom left corner of the window.

An assigned area is one that has been programmed from AcceptNet or used within an area list or when uploaded from the panel is not “empty”- that is, it contains some non-default configuration information – eg a non-default name has been given, an exit aux is defined etc... You may define a custom area display list for the mimic panel, by selecting any areas of interest from the custom area setup dialog invoked after activating the “custom” radio button in the bottom of the mimic panel dialog.

When an alarm is received in an area, the relevant area grid square will display the alarm state according to the colour of the alarm state key.

Try the following:

- Double click on the coloured squares of the colour key to customise colours.
- Right mouse click on the grid to receive a pop-up menu. Select a menu item to:
 - ◆ Acknowledge area alarms,
 - ◆ View relevant locales,
 - ◆ Open or close the area or invoke the feedback control dialog for the area.

- Double click on an area grid square to invoke the locale diagram (graphical security monitor) that contains the selected area, if one exists.
- Select (single click) an area grid square that is showing an alarm condition and activate the “Ack” button in the toolbar to acknowledge all alarms in that area. Refer to the section **Alarm Acknowledgment** on page 51 for a discussion on acknowledging alarms.
- Click on the “Show Assigned” radio button at the bottom of the window. The grid should show a reduced number of areas. Note however that if the panel configuration includes an area list with all areas in it then all areas in the system will be assigned and hence the “Show assigned” option will give the same result as “Show All”
- Click on the custom radio button to display only the areas selected in the custom display list.

8.1.2. Review Event Log

The review event log is a text based “printer-review-like” log of events generated by the Concept panel to which AcceptNet is connected. These security events indicate user access or changes in entity (area, auxiliary etc...) states or input/zone changes throughout the Concept security network.

If you cannot receive review or certain review events are not being shown in the “All Events” review log then there is likely to be a communications problem with the relevant panel or the panel is not logging the review to its internal review buffers as expected.

If the event is an access event right mouse click and select “Show User” to reveal a user information dialog for that event. Once server control is established, right mouse click on any review event and select “Show Review Manager” to go directly to the review process/criterion that was applied for that event.

IMPORTANT NOTE: If all review events generated by the Concept panel are to be recorded by the AcceptNet active review log, it is important to ensure that the AcceptNet Comms Task at the panel is NEVER set to “Idle”, even when the AcceptNet application is not running.

This ensures that if the AcceptNet application is shutdown, the activity that occurs at the panel is still buffered internally to the panel while AcceptNet is off-line and will be automatically uploaded to the AcceptNet when AcceptNet is re-started. Be aware that AcceptNet will require a few seconds or minutes to “catch” up to the panel where the panel’s internal review buffer is almost full, also the panel internal buffer is not unlimited so the oldest review will be lost if communications

with AcceptNet cannot be established in an appropriate time depending on the amount of review generated in the security alarm system.

Also ensure the **Do not log** option in the review manager is un-ticked for all review criteria or processes that apply to review events that must be logged.

Organising the Review Log

Customize the visualisation of a review log by:

1. Resizing columns by clicking on and dragging the column lines.
2. Defining and/or applying a filter to limit the visible review to a particular type or which contain a specific sub-set of event information. **For example:** limit review to alarm events, user accesses, zone-input changes or a combination of all three. Review filters are described in more detail below.
3. Display the relevant panel ID (name or number) for each event according to the preferences.

8.1.3. Review Filters

The review filters can be applied to active review or when a search through archived review is initiated.

To view all events select “Review | All Events”, when requesting a filtered (reduced set) review log select the “Review | Custom” sub menu a list of existing, predefined filters will be displayed. Select the desired item to open a new review log with the selected filter applied.

Filter Example

Filters are created using the Review Filter Editor. In the example below we wish to generate a report on the following circumstances: All user accesses between 10am and 3pm on 16 July 1999 to the Store Room Area (which is available through door "Store Door" (door ID 2)). We therefore would generate a filter to trap the above event(s) in an active review log or archived review as follows:

The conditions that determine a user access event are grouped within the first BEGIN END statements. Thus the condition list is equivalent to:

All events where the event timestamp is between 10am and 3pm on 16/07/1999

AND

is a "user access" event

AND

the store room door ("Store Door") is accessed.

The conditions that determine a "user access event" are therefore:

Any events that are trapped by the "user access door" to "user access module" review processes (see Review Manager)

OR

Any event that contains the words "Illegal PIN" - like an illegal PIN, module message.

OR

Any event where the floor number is not 0 (like a user access floor event).

These user access conditions must be grouped with BEGIN and END to force the filter processing to treat the group separately from the rest of the condition list. Without the BEGIN and END the filter would match any "Illegal PIN" event and any floor access events (regardless of date range), all other user access type review events matched would be suitably limited by the applied date range.

Getting Technical

Someone with a sound understanding of the concept review system might ask: "Why stipulate 'illegal PIN' or 'floor <> NULL' when these two conditions can NEVER occur together with door information in a single review event". Therefore a more efficient definition for the required filter above would therefore be:

All events where the event timestamp is between 10am and 3pm on 16/07/1999

AND

any event involving a user (user ID defined, ie. a non-zero value)

AND

the store room door is accessed.

Which would be entered in the condition list exactly as:

Date+Time>=16/7/99 10:00:00

Date+Time<= 16/7/99 15:00:00

User<>NULL
Door=Store Door

Dynamic Filters

Dynamic filters are filters that contain queryable conditions. To define a filter to request the user ID and/or door ID for a filter dynamically, ie when the filter is applied, rather than be locked into a particular constant value condition, use queryable conditions. Tick the “query” option in the statement setup dialog when adding a condition.

When displayed in the filter definition editor query conditions appear as “user=???” and “door=???” for example, in the condition list for a filter. These query conditions might be added to the user access filter for example. The presence of these queryable conditions will force the application to request values from the operator when the "user access" filter example above is executed. Once values are assigned the filter behaves as if the ??? values were replaced with the actual specific ID chosen. If no values are chosen the whole queryable condition is ignored.

Condition List Processing

The condition list is processed using standard boolean-logic rules where BEGIN and END are equivalent to brackets in a boolean statement.

For example:

$w = b$ and $(x > d$ or $x \leq g)$ and $y = h$

is the same as

```
w = b
BEGIN
  x > d
  OR
  x <= g
END
y = h
```

Remember:

$w = b$ and $(x > d$ or $x \leq g)$ and $y = h$ does not necessarily give the same results as: $w = b$ and $x > d$ or $x \leq g$ and $y = h$. Placing the BEGIN, END around statements forces those statements to be calculated first.

The latter would be processed by Accept as:

$((w = b$ and $x > d)$ or $(x \leq g))$ and $y = h$.

8.1.4. Searching for Review

The active review log only contains review since the system last archived and removed old events from it. An archive is therefore maintained by AcceptNet of all events ever received by the application, until the archive files are moved to another storage medium manually by an appropriately informed system administrator. It is possible to search these archives for events between a certain date range and using any of the custom review filters defined by selecting "Review | Search Archive". Choose a suitably short date range or apply a custom filter that will produce a suitably sized sub-set of review events. If the result set is too large AcceptNet will not display any results.

8.1.5. Preparing and Printing Event Reports

Once the active or archived review log data is opened in the review log dialog, preview the printer output (hard-copy) by activating the "Preview" buttons in the review log toolbar, this may take some time depending on the number of events in the result set of review log being viewed.

If necessary return to the review log dialog and adjust the column widths, setup the page orientation or margins using the page setup button so that the required columns and their content fit neatly in the width of the default paper size. Preview to confirm then close and activate the "Print" button from the review log dialog to begin printing the table. Select the appropriate printer and enter the desired page range in the ensuing system print dialog and activate the OK button to start printing.

To limit the print-out to a selection of events, highlight the events required then click on the print button and select "Selection" in the print range section of the ensuing system print dialog - only those highlighted events will be printed.

Filter the review (select a predefined filter) to limit the review to a particular subset of information. The current review filter can be accessed directly and edited from the archived review log window while viewing archived review by clicking on the "Edit filter" button.

If generating a lot of reports for different individual users, for example, it would be logical to create a review filter with one “queryable” user condition. A queryable user condition will be a filter condition where the user ID is not specified (is ???). Thus when the filter is executed (a filtered review log or archive search initiated) the system will automatically request the appropriate user ID of the user for which a log/report is required. Enter the ID in the ensuing “specify value” dialog or select clear to generate an access report for all users.

You may save the review as it is displayed in the archived or active review log windows to text, import into MS Excel (for example) and sort, search and process as required.

8.1.6. Alarm Event Log

The alarm event log displays a summary of review events belonging to the current tenancy. Specifically it contains the review events that AcceptNet has been configured to process as alarms – ie. their priority is not NONE as defined for the event’s criterion or review process in the review manager. Right mouse click on the event and select “Show Review Manager” to go directly to the review process/criterion for that event.

An alarm event message is only displayed once. A count of the number of times the alarm has occurred (before being acknowledged at AcceptNet) is indicated in the event count column. The date/time of the *last received* alarm is indicated in the event time/date column.

Alarms are displayed in priority and time/date order. That is top to bottom from highest to lowest priority and oldest to newest event

Any and all alarms specific to the operators tenancy can be acknowledged from this dialog.

Concept Access 4000 Panel Pogramming

The Compass “Comms Task” in the panel only logs relevant alarm events if they are programmed to be reported (or transmitted) to the Comms Task within the panel.

To enable an input/zone to report an alarm to a Comms Task, the **Process Group** assigned to the Input (in the panel) must have the relevant Comms flags set for **Isolate**, **Tamper**, **Alarm**, and **Restore** messages. You will note that some of the

default Process Groups such as “Burglary”, “Fire”, “Syst. Tamper”, “Syst. Silent” and “Access Silent” already have the appropriate flags set.

Any inputs to be handled as alarms by AcceptNet but not the dialler comms task (or another comms task eg securitel, SIA etc..) should be assigned a separate area. An area-list filter should be used within the dialler/monitoring comms task that excludes the special area used to hold AcceptNet alarms

For example:

Door forced and Door held alarms may not be commonly monitored by a remote Central Station. These inputs should be placed in their own area and assigned a process group that must have the “A” flag set to Yes in the “Input Type” options; and the “A” and “R” flags set to Yes in the “Reporting Options”.

In addition the comms task programmed for “Contact ID” for example, should have an area list filter assigned and that area list should NOT contain the area that contains the door forced/held alarms.

8.1.7. Alarm Acknowledgment

A security guard operator using AcceptNet may be expected to monitor the security of an installation under the control of a concept panel. In such a capacity an operator maintains security by watching the AcceptNet screen. An operator is therefore notified of important alarm conditions by either:

- Flashing of the Alarm button and/or changes in alarm statistics in the main too bar.
- Changes in the alarm log window.
- Changes in grid colour on the mimic panel.
- Changes in entity graphics/colours in the graphical locale monitor dialogs
- Most commonly by audible alarms configured and sounded by AcceptNet in response to processing of specific review events.

In response to alarms, the security guard operator is expected to take some form of action. Initially this may be to acknowledge the alarm by:

- Selecting (single click) an alarmed area grid square from the annunciation panel and selecting “Ack” from the right mouse pop-up menu or click on the “Ack” button in the mimic panel tool bar.
- Selecting multiple alarm events in the alarm log by clicking on the alarms of interest while holding the <Ctrl> or <Shift> key down.

- Selecting an entity (area or zone/input) from a locale diagram and selecting “Ack Alarms” from the right mouse pop-up menu.

As well as the default (installed) acknowledgment messages, a tenant may define their own acknowledgment messages. These messages are thereafter not available for use by other tenants.

NOTE: When acknowledging alarms in a multi-tenanted system if an alarm is common to two or more tenants then it only need be acknowledged by one of the tenants to be acknowledged in all tenancies. A suitable review log entry (alarm acknowledgment) will be added to all of the “common” tenants’ logs.

Alarm Handling

Alarm handling messages are the same for all tenants in the AcceptNet system. Modifications or additions to the alarm handling affect all tenants equally.

If alarm-handling instructions exist for the selected alarm event, it will be displayed toward the front of the screen as the alarm is being acknowledged or when “Show handling” is selected from the events right mouse pop-up menu. If multiple alarms are selected each with different handling instructions, no handling instructions will be offered if the selection is acknowledged together.

Handling instructions can be provided for each alarm type (review process or criterion) and assigned to review events using the review manager discussed in the section **AcceptNet Server Review Manager** on page 56. Setup these alarm handling instructions using the word processor like features of the Alarm Handling editor invoked by selecting “Setup | Alarm Handling Messages” from the main menu.

Alarm handling messages can be used to instruct the operator as to their responsibilities to the alarm condition.

Entering A Response

Once the alarm has been resolved, by physical inspection of the cause for example, an operator may be required to enter a written acknowledgment response into the ensuing Acknowledgment Response dialog according to the “Get Operator Ack” option in the review manager setting for that event process or criterion – see **AcceptNet Server Review Manager** on page 56. This would normally be a single sentence describing the operator’s assessment and actions to the alarm.

8.2. GRAPHICAL SECURITY (LOCALE) MONITORING

A locale is used in AcceptNet to refer to a specific security plan displayed by the Locale Monitor or Locale Graphic editor. These diagrams are the grouping of Concept security entities (areas, inputs, doors etc...) on to a background plan or bitmap image. The locale can therefore be a house, several rooms within a large complex, a suburb or part thereof. Each locale most likely contains many Concept security areas and several input/zone detectors and is accessible by many doors.

Invoke the Locale Monitor by selecting “Security | Monitor Locale” from the main menu or by activating the “Monitor Locale” button of the main toolbar.

The Locale Monitor provides an immediate view of the states of security entities within a Concept security network as well as any unacknowledged area/input AcceptNet alarms. Use the locale monitor to observe movement, pin-point and acknowledge alarm conditions as well as control access and security.

Invoke the locale editor by selecting “Security | Locale Editor” from the main menu or by activating the “Diagram Editor” button in the main toolbar or by right mouse clicking on the background of the locale monitor and selecting “Edit Diagram”. Refer to the on-line help for more information on using the locale diagram dialog. Monitor the locale just created by clicking on the background and selecting “Monitor”, the diagram is locked, the toolbar hidden and entity states are displayed according to the state implied by the latest review events.

Controlling Entities

Double (left) click on an entity in the locale monitor to invoke the control feedback dialog for that item. Alternatively control the entity directly or from a feedback control dialogue by selecting the control state item or “Control” item from the right mouse click pop-up menu.

8.3. CONTROL OF PERIPHERALS

The control of peripherals for access or security, allows an operator to manage the state of various entities throughout the Concept security network. These entities include Zones/Input, Auxiliaries, Auxiliary Lists, Home Auxiliaries, Doors, Areas, Door Lists, Area Lists, Lifts and Floors. Use this facility to isolate zones, de-activate areas or open and close doors.

The control feedback dialog can be invoked from within the Mimic (annunciation) Panel dialog or locale Monitor dialog.

The control list dialog is invoked by selecting the relevant entity type to control from the Control menu. Activating the “Control” button of the main toolbar invokes the last entity list opened previously. The item to be controlled is then selected from the ensuing control list. To find a particular name quickly, type the first few letters of the entity name into the incremental search box above the entity list. The list pointer will move to the entity that matches the incremental text as closely as possible.

Select the entity to be controlled click on the done button (green tick). If the selected entity can be controlled the control feedback dialog will be invoked. Simply select the required on/off options and activate the “Go” button to attempt the control change.

Alternatively the state of the entity is displayed in the right most column of the entity list – no state is displayed for lists or entities that do not have a singular state. Right mouse click on the list item to control and select the required state of the entity from the ensuing pop-up menu. The state information in the dialog will change to indicate success or failure of the control.

If controlling a list type entity in this manner the feedback dialog will be displayed automatically to display the results of the change of state command.

8.4. DATABASE NAVIGATOR

Invoke the database navigator by selecting “Security | Edit Database” from the main menu or by activating the “Data” button of the main toolbar.

Click on the + of a navigator node to open the underlying list of editors or sub-nodes. Click on the list item under a node in the navigator to open the relevant database editor.

8.4.1. Editing

Select the required record of interest from the name or ID list box associated with each field in the editor (where applicable). Alternatively “scroll” through all the visible editor records by activating the left and right arrow buttons in the editors toolbar. Only the records that have been reserved to the current operator’s tenancy or remain unrestricted will be visible.

Edit a record as required and save your changes by activating the “Save” button in the dialog’s toolbar. Alternatively, once any changes have been made, you will be

prompted to save or ignore changes if you close the dialog or attempt to move to a different record.

Any time a record is saved at the AcceptNet client, an update request is sent to the AcceptNet Server. A notification message will be displayed at the AcceptNet client once those changes have been downloaded to the relevant panel by the server application.

An operator is warned if an attempt is made to modify a record in an editor that is currently being edited simultaneously by another operator at another AcceptNet Client. The “blocked” operator must simply wait for the other operator to finish incorporating his/her specific changes before trying again.

The operator may also be blocked from editing a record if the AcptServer is currently downloading the contents of the current record or parts of the table to any panel. Check the panel status to determine the download state of panels connected to the system.

8.4.2. Switching Between Panels

Click on the Select panel button in the DB navigator at any time to invoke the panel selection dialog, select a different panel to invoke the same editor as was currently open for the panel selected. The record displayed in the refreshed editor will be the last record modified in that editor for the newly selected panel.

8.4.3. Copying Records Between Panels

Click on the “copy to other panel” button in an editor to invoke the panel copy dialog specific to the current editor. Select the records in the top list that you would like to copy and select the panels in the bottom list to which you would like the selected records to be copied. If successful the records overwrite the records of the same ID number in the destination panels. Thus AL003 from panel 1 copied to panel 3 and 4 will overwrite AL003 in panels 3 and 4.

8.4.4. Preparing and Printing

To view the data in a tabulated form, activate the “Preview/Prepare” button of a dialog editor. The ensuing dialog displays the assigned records for the data underlying the current editor.

Organise the table column widths, visibility and titles by activating the “table format” button or change column widths by clicking and dragging the column lines.

Once formatted, print and preview the table by activating the “Print” or “Preview” buttons in the toolbar of the data preview dialog.

Order data by entering the column titles of the columns required to sort the table information. The ordering is performed from left to right according to the columns chosen. Each column title in the “order-by” string must be separated by a semi-colon.

8.4.5. Changing User Editor Labels

The Address, State, Country, ZIP, Info1, Info2 labels of the user editor may be changed from within the editor to some other caption. These changes affect the editor and are subsequently the same for all user records. Label changes are applied to all clients in the operator’s tenancy.

Extra fields in the user editor are arranged as follows: The first top most 8 fields are tested for uniqueness. These fields should be used to contain information unique to each user, eg address, license number etc... The fields have an index associated with them so they can be searched. The next top 8 fields are indexed but not tested for uniqueness and could be used for example to hold group information like department for example.

Right mouse click on the label and select “Change Label” from the pop-up menu or double click on the label to invoke the caption editor. An ampersand (&) next to a caption letter forces that letter to be underlined. The underlined character then provides the hot key for that edit field. A double ampersand (&&) together gives ‘&’ in the caption. Two labels cannot share the same hot key.

8.5. ACCEPTNET SERVER REVIEW MANAGER

Changes to the review manager affect the way a review event is processed by the AcceptNet Server and subsequently how those events are displayed at an AcceptNet Client. It does not however affect the review to tenant relationship of the event. Changes made to the review process therefore affect *all* AcceptNet Clients and tenants equally. Consensus must be reached between all tenants as to how alarms are to be presented at each AcceptNet Client.

8.5.1. Setting up Panel Inputs and Areas

Ensure all inputs are in closed areas for inputs that are to be displayed in locale diagrams. Ensure those areas are closed when updating states. Zones in open areas may not return their correct current-state value.

It is a good idea to create a special area called (for example) “AcceptNet Area” and place all diagram related inputs in that area. Create an additional process group called (for example) “AcceptNet PG” that can be used to tailor the reporting of inputs within the AcceptNet area.

Filter out AcceptNet Area related review events from any monitoring comms tasks (securitel, earthnet, SIA etc..) by stipulating an area list in the filter options that *excludes* the AcceptNet area.

Do not use raw input change events for complicated alarm or review processing. Instead rely on Input Comms trigger type events.

8.5.2. Processing Review

Alarm Options:

- **Priority.** If set to any value other than “None” the review event associated with the current process is an “alarm” and therefore will be logged in the alarm log, can have a sound, alarm handling and may require acknowledgment.
- **Sound WAV File.** When a valid file name is entered the event that fits this review process will make the selected sound. Ensure that a valid WAV file is selected. For no sound, delete the file name from the input field.
- **Continuous Sound.** If set, the alarm sound specified in the “Sound WAV File” option is repeated continuously approximately once a second until the alarm is acknowledged or the flashing alarm activity button in the main toolbar is activated.
- **Get Operator Ack.** If set, then the alarm event when acknowledged will require report input (an account of what was done to administer the alarm etc...) by the operator before the alarm will be cleared from the alarm log.
- **Help Procedure.** The alarm handling (help/instructions) message that will be displayed as the user acknowledges the alarm event.

Process Options:

- **Do not log.** If set the review is not logged in the review log. It will still be processed internally and related entity states displayed correctly by AcceptNet.

- **Msg Box.** The review text for the event will be displayed in a small message dialog as the event is received.
- **Locale.** If set, the locale monitor dialog that contains the entity or area indicated by the review event will be invoked.
- **No State Update:** If set entity states implied in the review events applicable to this review process are ignored.
- **User Info.** An user summary dialog will be displayed (complete with user graphic and extra information) when the event is received.
- **Relay Msg:** If set review events applicable to this review process will be relayed to the paging system by PSD messenger. PSD Messenger must be installed and configured appropriately.
- **Maximise.** If AcceptNet is minimised or does not have focus, setting this option will force AcceptNet to be maximised (fill the whole screen) and be repainted at the front of the screen, becoming the active application on the desktop.
- **Mimic Panel.** If set, the mimic (annunciation) panel dialog will be invoked as the review event is received.
- **Trig Ctrl:** If set you can assign a control list to review events that match the current review process. The control list is a list of actions (entity on/off/isolate/lock/secure etc...) that will be performed when an appropriate review event is received.
- **Ctrl Dialog.** The feedback control dialog is displayed once the event is received and provided the event contains an affected entity value that can be controlled.
- **Review Log.** The All events review log is displayed when the review event is received.

How to Use a Review Process

The review process for a particular review event type or group is configured using the review manager.

Event Groups or Event Types

Every binary review event (10 bytes) sent by the panel belongs to a group. Each group implies a fixed byte format. The information in the raw bytes of a review event are broken down into information items according to the byte format rules for each group. Those information items are then filtered and acted upon according to the specifications of a review process. There is only one review process per review event group and this process tells Front-End how to process the review event. The assignment of the review process to each review event group is fixed and cannot be changed.

For example: When a user accesses a door by a card at a reader an event will be sent by the panel to Front-End. The type and format of the bytes of the review sent belong to a user-door-access review group. Hence the "User access door" default review process will be used to process the event, as that is the process assigned permanently to this type of review.

The review process therefore allows a priority and text to be assigned to all events belonging to the underlying review event group, as well as sound and actions. Remember however that the review process applies to a group of review events hence in the example for user-door-access events all card user access through any door will be process identically. That is the format of the output text, any sound and the priority will be same. Note however that the text strings may change slightly if variables are used in the review process string.

As discussed above an event in an event group contains several information items. These items can be different for each review event in the same group, hence a review message like "User accessed a door" in the review text part of the review manager dialog would not be suitable for every door and user in the installation. Thus variables are permitted in the review text to tell the front-end software to insert the appropriate information. Now a user access door event contains, panel ID, door (affected entity), user ID, access information (access by card/pin etc...) and error value and an action (denied, granted), thus only 6 variables will be recognised. The variables can be inserted by using the add/modify button when editing text. Each variable is delimited by a % to help distinguish them from the static parts of the message.

Specific Events

While processing of a review event according to its group is efficient it does not allow for tailoring of the system to a specific review event. A specific review event might be one that occurs at a particular door or by a particular user.

For a specific event the generalised event-group review process may not be adequate to describe the actions to take or apply an alarm priority appropriately.

For example: A user accesses the stationery cupboard via a card reader. Under the applicable event-group review process the system assigns no priority (it is not an alarm event) and the derived review event text is black on white (window text on window background) - depending on your desktop's colour scheme.

Now a company may decide that there have been a number of excessive "withdrawals" from that cupboard and would like to monitor accesses to this

cupboard as a low priority alarm. Thus the guard who is positioned appropriately knows when the cupboard is being accessed and can watch it more closely during those times.

Obviously setting the priority on the "User access door" process would not be a solution as every door being accessed through-out the day would result in an alarm which the security guard must eventually acknowledge and discard. The solution therefore is to leave the user-access door review process as it is but set up *specific review criterion* under the "User access door" review process that defines the door being accessed. Like a review filter the values assigned in the review criterion must match the review event being sought.

For the above example therefore under the "User access door" review process go to the **Specific Criteria** page in the review manager and click on the **Define** button. The ensuing criterion setup dialog shows several information field names in two columns. As discussed above a user access door event contains, panel ID, door (affected entity), user ID, access information (access by card/pin etc...), an error value and an action (denied, granted). By selecting the appropriate values for these fields we can specify exactly which review event (or events) we wish to "trap" and process it separately according to the process settings defined in the specific criteria page.

In the case of the stationery cupboard scenario, the affected entity ID field is set to the door ID for the stationery cupboard (check the **Affected Ent.ID** check box to enable selection), and the action value to "granted" (check the **Action** check box to enable selection).

Once the criterion is defined and upon returning to the **Specific Criteria** page of the review manager, the process options will be visible. These process options will apply to the criterion just defined - and *only* that criterion. Now set the priority to "Low" and the "Sound WAV file" to a suitable file name. Set the review text to "User %user% has accessed the stationery cupboard" and choose an appropriate text colour.

Thus whenever a user successfully accesses the stationery cupboard a low priority alarm will sound and coloured text will appear as defined in the review manager. Only that review event will be processed in this way. Unsuccessful accesses to the stationery cupboard would be processed according to the more general event-group process - because the criteria requires successful access.

Further modify the specific criteria to trap access to the cupboard by a particular user by activating the user field of the criteria definition dialog and selecting a

specific user. Set the subsequent review text to "Suspect has opened stationery cupboard" - no variables required.

9. MAINTAINING ACCEPTNET

9.1. BACKING UP THE DATABASE

To maintain the integrity of the system, the database should be backed up (a copy made) and stored safely on external media (floppy disk) or internally at another location on the hard disk. The database being a collection of file-system controlled files is at the mercy of operating system foibles. While a good database attempts to preserve its integrity against power failure and operating system crashes it cannot guarantee its integrity under all circumstances (particularly HDD crash) or an inappropriately timed system failure. Hence some other mechanism is required to recover the database – usually by copying data to some form of compressed archive or ZIP.

Data including user details (address, photos/graphics and miscellaneous setting information), passwords, operators and operator details, locales and **review** are not recoverable from the panel (via an upload). For this reason, a procedure of regular backing up will ensure that as little database information as possible is lost in the unlikely event of a severe or untimely system failure.

To backup the complete AcceptNet database, including review select “Admin | Backup Front End Data to ZIP” from the main menu and follow the prompts. The single backup ZIP file created employs standard PK-ZIP compatible compression and concatenation algorithms.

9.2. RESTORING THE DATABASE

To restore the database from a previous backup, select “Admin | Restore Data from ZIP” from the main menu. Locate the file that was created from a previous backup and open it in the ensuing file search dialog.

NOTE: *Once the database is restored you should update the panel by performing a complete download to the panel - select “Admin | Restore Panel”. This will ensure that the panel and the database use the same database configuration. This is particularly important if the restored data is significantly different from the current panel configuration (for example if restoring to an old default or test configuration).*

IMPORTANT: *If you are unsure as to the age of the data you have restored and do not wish to disturb the current panel configuration then synchronise databases*

by **UPLOADING** from the panel – be aware however that restored user information and some entity names may be modified according to the more current contents of the panel.

INDEX

A

- AcceptNet Client
 - ICONS, 12
- AcceptNet Security, 41
- AcceptNet Server
 - ICONS, 12
- Alarms
 - Acknowledge from mimic panel, 51
 - Acknowledgment Response, 52
 - Concept panel programming, 50
 - Event Log, 50
 - Handling Instructions, 52
 - Multiple Selection, 51
 - Operators Responsibility, 51
- Annuciator Panel. *See* Mimic Panel
- Assigned Areas, 44
- Auto Logout
 - Grace Period, 40
 - Idle Period, 39
 - Suspended, 40
- Automatic Review Archiving, 37

B

- Backing Up Data, 62

C

- Client Connections, 26
- Communications
 - Preferences, 38
 - Troubleshooting, 34
- Control
 - Feedback, 53
 - Feedback, using, 54
 - List dialog, 54
 - Peripherals, 53
- Control Lists, 58
- Control Peripherals
 - From locale diagram, 53

D

- Database Editor
 - Copying Panel Info., 55
 - Printing data, 55
 - Save, Cancel, Done and Exit, 54
 - Switching Panels, 55
 - Using, 54
- Database Navigator
 - Selecting an editor, 54
- Date Time Formats, 8
- Dialog
 - Definition, 8

G

- Generic Serial (CCTV) Panels, 18
- Getting Started, 36

H

- Hotkeys, 8

I

- Installation
 - CD, 10
 - Client, 11
 - Floppy Disk, 10
 - Server, 11
- INVOKING THE SOFTWARE
 - Client, 12
 - Server, 12

L

- Locale Monitor
 - Construct using locale editor, 53
 - Controlling Entities, 53
 - Security Monitoring, 53

M

- Mimic Panel

Acknowledging alarms, 45
 Customising Colours, 44
 Described, 44
 Invoking Locale from, 45
 Show Assigned, 45
 Monitoring, 44
 Moving in a Window, 8

N

Network Configuration, 15

O

Online Help, 8
 Operator Log, 43
 Operators
 Configuring, 43
 Defining, 42
 Example, 43

P

Panel Connections, 16
 Direct Serial, 17
 Modem Connection, 23
 TCP/IP to Serial Connection, 17
 Password
 Changing default, 36
 Minimum Size, 40
 Retry limit, 40
 Permissions
 Default, 42
 Defining, 42
 Preferences
 Auto-logout, 39
 Communications, 38
 Password Retry Limit, 40
 Synchronise Panel Clock, 39

R

Restoring Data, 62

Review Filter Example, 46
 Review Filters, 46
 Review Log, 37
 Description, 45
 Organising, 46
 Printing Reports, 49
 Queryable fields, 38
 Searching, 49
 Searching for events, 38
 Review Manager
 Alarm and process options, 57
 Putting inputs in areas, 57
 Specific events criteria, 59
 Using a review process, 58
 Running the Client for the first time, 29
 Running THE Server for the first time,
 15

S

Server Control, 30
 Server Login, 27
 Additional Operator, 27
 Synchronising Panel Clock, 39
 System Requirements, 5
 A Note About..., 7
 Client, 6
 Other, 6
 Performance, 7
 Server, 5

T

TCPToSerial Utility, 11
 Tenancy Defined, 30

U

Uploading Panel Config., 28

Z

ZIP file, 62