220 Software

QUICK START GUIDE

Scope of Document

This document gives a brief overview of the 220 System.

Document Conventions

We use the following conventions in this document:

	*Note – points out extra information*
	*Tip – points out alternative methods to perform a task*
	*Important – points out important information*
	***Warning – points out potential danger to you or the product***

Before You Begin

Have the following available:

- An active Ethernet connection (using a standard Ethernet Cable) to the 220 Controller and IP Terminals.
- The 220 Software Suite.
- The MAC Address and Fixed Address of each 220 Controller – on a label bundled with the Controller.

1 Installation

220 Software Installation Procedure

Install the 220 Software Suite on a single Host PC as follows:

1. Insert the 220 Installation CD into the CD-ROM drive.
2. Select the **Install 220 Suite** option.

If the CD does not start up automatically, browse the CD in Windows® Explorer and double-click Setup.exe.

3. Select **English** as the language option.
4. Click the **OK** button.

If no Database Server is present, one is installed. Follow the onscreen instructions for this.

5. At the Introduction screen, click **Next**.
6. At the Licence Agreement screen, select the **I Accept the Terms of the Licence Agreement** radio button.
7. Click the **Next** button.
8. At the Choose Install Folder screen, click **Next**.

*If you change the installation directory file path, ensure that you enter **text only, NO spaces**.*

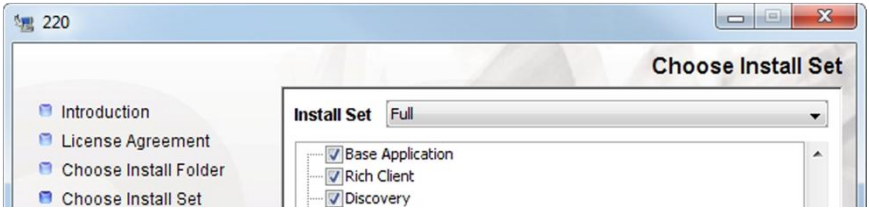


Figure 1 – Install Set Menu

9. At the Choose Install Set screen, from the **Install Set** drop-down list, make your preferred installation type selection.

An Install Set is a collection of pre-selected applications suitable for specific scenarios. Customize an Install Set option by selecting or de-selecting applications from the list.

10. Click the **Next** button.
11. Click the **Install** button.
12. At the Install Complete dialog, click the **Done** button.

By default Windows® XP (SP2 and SP3) installs a firewall. To keep this Firewall, unblock the TCP Ports thereby allowing functionality of the 220 Software. Continue as follows:

1. *Select **Start**>**Control Panel**.*
2. *Select the **Windows Firewall** icon.*
3. *In the Windows Firewall Settings dialog, select the **Exceptions** tab.*
4. *Click on the **Add Port** button.*
5. ***Unblock the TCP Port** in the Add a Port dialog, by completing the **Name** and **Port Number** (Ethernet Controllers use **10005**) text boxes.*
6. *Select the **TCP** radio button.*
7. *Close the Add a Port dialog, by clicking the **OK** button.*
8. *At the Windows Firewall Settings dialog, again click on the **Add Port** button.*
9. ***Set the Ethernet Firebird Port** by completing the **Name** (for example Firebird Service) and **Port Number** (Ethernet communication uses **3050**).*
10. *Select the **TCP** radio button.*
11. *Close the Add a Port dialog, by clicking the **OK** button.*
12. *Close the Windows Firewall Settings dialog, by clicking the **OK** button.*

Installing the Firebird 2.1 Database Server

A Database Server is required to host the 220 Database. If the 220 Suite is installed on to a single PC, the Database Server installs automatically. However, if more than one PC is used to host the 220 Software, you must install the Database Server manually.

Firebird automatically prompts to install, if a previous version is not detected.

1. As any PC on the network can host the Database Server, select a PC to host the Database Server.
2. Insert the 220 Installation CD in the PC's CD-ROM drive.
3. Browse to the **\database\firebird** directory on the 220 Installation CD.
4. Double-click **Firebird.exe**.
5. In the Select Language Setup dialog, from the drop-down menu, select your preferred **language**.
6. Click the **OK** button.

Firebird Installation Wizard

1. At the Welcome dialog, review and follow the on-screen instructions.
2. Click the **Next** button.
3. At the Licence Agreement dialog, select the **I Accept the Agreement** radio button.
4. Click the **Next** button.
5. Review the Information dialog, and then click the **Next** button.
6. In the Select Destination Location dialog, select the **Destination Directory**—we recommend that you use the default location of **C:\Program Files\Firebird\Firebird_2_1**.
7. Click the **Next** button.
8. From the drop-down menu, select the **Full Installation of Super Server and Development Tools** option.
9. At the Select Start Menu Folder screen click **Next**.

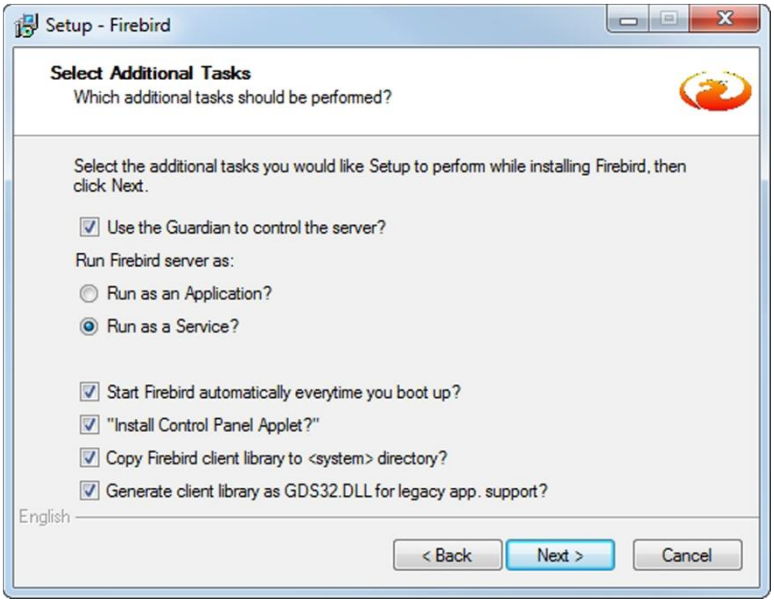


Figure 2 – Firebird Select Additional Tasks

10. On the Select Additional Tasks screen:
    - Select the **Use the Guardian to Control the Server?** option.
    - Select the **Run as a Service?** option.
    - Select the **Start Firebird Automatically Everytime You Boot Up?** option.
    - Select the **"Install Control Panel Applet?"** option.
    - Select the **Copy Firebird Client Library to <System> Directory?** option.
    - Select the **Generate Client Library as GDS32.DLL for Legacy app. Support?** option.
11. Click the **Next** button.
12. Click the **Install** button.
13. Review the Information dialog and then click the **Next** button.
14. Click the **Finish** button.

Installing the USB Registration Interface's USB Driver

220 uses a USB Registration Reader Interface to read Tags. Some Interface versions also provide an RS485 communication link to the Controllers. To install the driver, proceed as follows:

*If there are old USB Drivers on the PC, delete them **before** installing the provided driver.*

*On some PC's, the **New Hardware Found** wizard displays every time you plug in a **USB Registration Reader Interface** with a new USB Serial Number (Fixed Address). If this happens, choose the option to automatically install the unit. The **New Hardware Found** wizard will not display again.*

1. Plug the **USB Registration Interface** into a USB port on the PC. The **Found New Hardware Wizard** displays.
2. Select the **Locate and Install Driver Software (Recommended)** option.
3. Select **I don't have the Disk. Show me Other Options**.
4. Select the **Browse My Computer for Driver Software (Advanced)** option.
5. Click the **Browse** button.
6. In the Browse for Folder dialog, select the **220\USB_Device _Driver** folder.
7. Click the **OK** button.
8. Click the **Next** button.
9. At the Windows Security dialog, select the **Install this Driver Software Anyway** option.
10. Click the **Close** button.

You will notice that the Wizard pops up twice, installing two drivers; one for the **USB Registration Reader** and one for the **COM Port to USB Bridge**.

2 Pre-configuration Procedure

When *all* 220 Software components are installed, you need to perform the **Pre-configuration Procedure**. This procedure determines if the hardware communication infrastructure is functioning correctly.

RS485 Communications Infrastructure

1. Using the supplied USB Cable, connect the RS to the PC.
2. Using the 220 Controller's RS485 Controller Port, connect the 220 Controller to the RS Registration Interface.

USB Communications Infrastructure

1. Plug the **220 Controller** into a USB port on the PC. The **Found New Hardware Wizard** displays.
2. Select the **Locate and Install Driver Software (Recommended)** option.
3. Select **I don't have the Disk. Show me Other Options**.
4. Select the **Browse My Computer for Driver Software (Advanced)** option.
5. Click the **Browse** button.
6. In the Browse for Folder dialog, select the **220\USB_Device _Driver** folder.
7. Click the **OK** button.
8. Click the **Next** button.
9. At the Windows Security dialog, select the **Install this Driver Software Anyway** option.

Take note of the COM Port number displayed by the Driver Software Installation dialog.

10. Click the **Close** button.

TCP/IP Communications Infrastructure

If your installation includes IP Terminals, review the section ***Guidelines for Setup of IP Terminals (iTT or iTRT)*** *on page 43 before proceeding further.*

For ***220 Controllers or Terminals installed on the LAN*** *(that is the local Subnet of the Host PC),* ***make use of the Discovery Utility integrated with the 220 Base Application****.* ***For 220 Controllers or Terminals installed on a WAN*** *(that is the non-local Subnet of the Host PC),* ***make use of the stand-alone Discovery Utility*** *(local to the Controller)* ***and export the configuration settings to the Host PC****. The Host PC runs the 220 Base Application.*

View ALL Available 220 Controllers or Terminals on the Local Subnet

Ensure the PC running Discovery is on the SAME subnet as the 220 Controllers or Terminals for viewing.

1. Using your chosen method, open the Discovery Utility:
   - From the *220 Base Application*, from the Menu Bar, select **Hardware**>**Unit Discovery**.
   - Alternatively, start the *stand-alone Discovery Utility* from Windows® by going to **Start**>**All Programs**>**220**>**Utils**>**Discovery Utility**.
2. On the Menu Bar, go to **Network**>**Search Local Subnet**.
3. If the Utility fails to find any Devices, at the **Device Not Found** dialog, click the **OK** button.
4. On the Menu Bar, go to **Network**>**Advanced Local Search**.

By selecting **Advanced Local Search**, you may select the correct **Network Interface** (only displayed where more than one exists) and enter the correct **Subnet Mask**. If the search returns Controller or

Terminal details, the Utility (while running) retains the Network Interface and Subnet Mask information for further searches. You may however, use Advanced Local Search again during the session for further searches using different search criteria.

5. Select the relevant Network Interface, if more than one displays.
6. Click the **OK** button.
7. In the Input dialog, in the textbox, enter the **Subnet Mask** for your network.
8. Click on the button. Wait for the Controllers and Terminals to display.

Sort the information displayed in either ascending or descending order by selecting the column header.

View a SPECIFIC Controller or Terminal

1. On the Menu Bar, go to **Network**>**Search IP**.
2. In the **Enter IP Address** dialog, enter the **IP Address** of the Controller or Terminal you're searching for.
3. Click on the button. Wait for the Controller or Terminal to display.

Secure Logon

1. In the **Device Password** dialog, enter your **password**. The default password is **masterkey**, for improved security we recommend that you change this password.
2. Click on the button.

Change the Secure Logon

1. From the Menu Bar, select **Configuration**>**Change Password**.
2. **Logon** if requested.
3. In the **Enter New Password** textbox enter a new password (not exceeding 16 characters) for the selected Controller or Terminal.

4. In the **Confirm New Password** textbox re-enter your chosen password.
5. Click on the button.

Grouping Controllers and Terminals

On display of Controllers and Terminals, the following icons appear: the icon represents unlinked Controllers. The icon represents Terminals and the icon represents Controllers with linked Terminals. On expanding the Controller tree, the icon displays, with the linked Terminals displaying below.

Creating the Group and Adding Controllers

There is no need to give a group name to a Controller if it has no IP Terminals.

1. Select the **Controller** and the **Terminal's** it should control.
2. On the Menu Bar, select **Configuration**>**Add to Group**.

*Alternatively, right-click and select **Add to Group** from the pop-up menu.*

3. In the **Enter Group Name** dialog, enter a suitable group name for the selected units.
4. **Logon** if requested (see page 9). A password is required for each Controller and Terminal being added to the Group.
5. Click the button.

Adding Terminals to Existing Controller Groups

1. Select the **Terminal(s)** to be added to the Group.
2. On the Menu Bar, select **Configuration**>**Add to Group**.

*Alternatively, right-click and select **Add to Group** from the pop-up menu.*

3. In the **Select the Group Name** dialog, double-click on your chosen group name row.
4. **Logon** if requested (see page 9). A password is required for each Controller and Terminal being added to the Group.
5. Click the button.

Communication Configuration – Case Local

Configure the Controller or Terminal's Static IP Address (Ethernet)

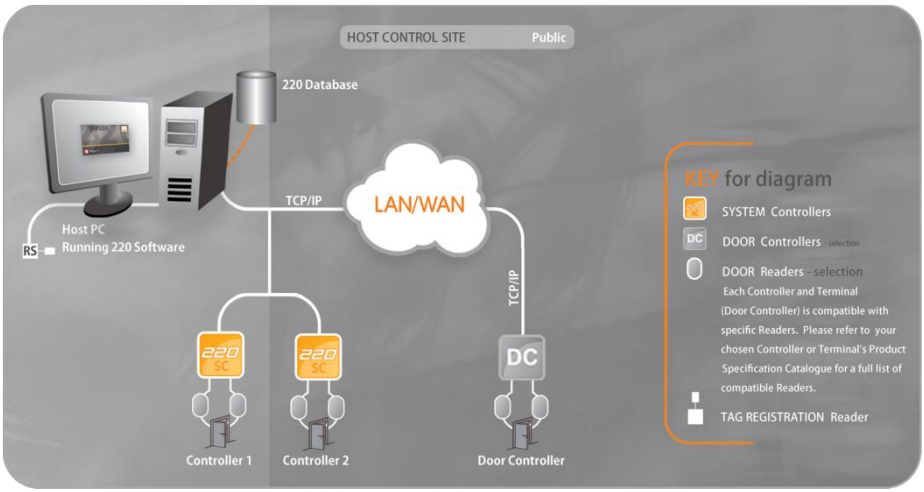


Figure 3 – Case Local—Configure the Controller or Terminal's Static IP Address (Ethernet)

If a DHCP server is present, IP Addresses are dynamically assigned initially. Obtain a suitable IP Address from your Network Administrator. A private static IP Address is essential for the Controller or Terminal because a DHCP Server may assign a new IP Address resulting in the Software losing communications. If the Controller or Terminal is NOT on the DHCP Server, ensure the PC is on the same IP Range as that of the Controller or Terminal. If the PC's IP Range differs, you cannot change the Controller or Terminal's settings.

1. From the 220 Base Application, from the Menu Bar, select **Hardware**>**Unit Discovery**.
2. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
3. From the Menu Bar, select **Network**>**Configure IP**.
4. **Logon** if requested (see page 9).

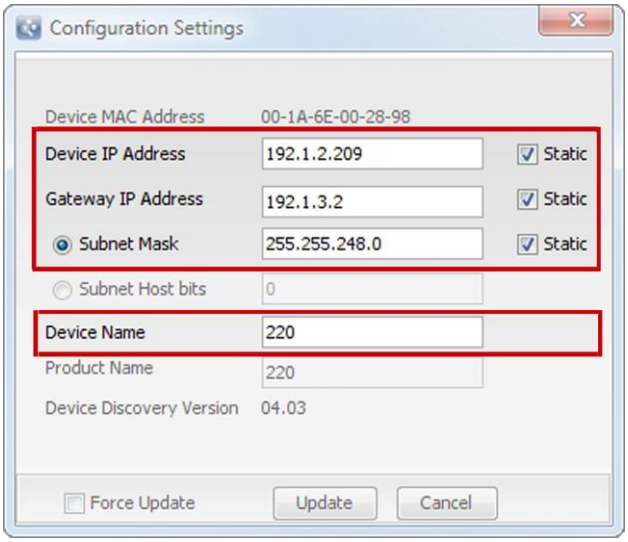


Figure 4 – Configuration Settings Dialog

By assigning an invalid IP Address, the Controller or Terminal may no longer communicate. Refer to the Hardware Installation Manual for information on restoring factory defaults.

5. In the Device IP Address textbox, enter a **Device IP Address**.
6. Tick the checkbox to set the IP Address to **Static**.
7. In the Gateway IP Address textbox, enter a **Gateway IP Address**.
8. Tick the checkbox to set the Gateway IP Address to **Static**.
9. Continue with ONE of the procedures (Subnet Mask or Subnet Host Bits) that follow:

Subnet Mask

a. Select the **Subnet Mask** radio button.
b. In the textbox, alongside, enter the **Subnet's Address**.
c. Tick the checkbox to set the Subnet Mask to **Static**.

Subnet Host Bits

a. Select the **Subnet Host Bits** radio button.
b. Enter the number of bits in the textbox.

10. If necessary, amend the supplied **Device Name**. Use the same site prefix to name devices belonging to the same site. For example: "Site_1–Factory", "Site_1–Testing" and so on.
    Changes to the IP Configuration result in the Controller or Terminal rebooting on acceptance of the change. The Configuration Settings dialog remains open while allowing the Controller or Terminal to reboot. On closure of the dialog, the Utility again searches for the Controller or Terminal and if successful, displays the updated details.
11. Ensure the **Force Update** checkbox is **UNCHECKED**. If the Force Update checkbox remains unchecked, the Controller or Terminal changes the IP Address testing communication on the new Address. If successful, the update becomes final; if not, the Controller or Terminal reverts to its old settings.
12. Click the **Update** button.

After detection and configuration it's not necessary to assign a Logical Address, as the 220 Auto-ID process does this. It is not necessary to export the settings to a file.

Communication Configuration – Case Remote

Option 1: Configure the Controller or Terminal's Static IP Address (Ethernet)

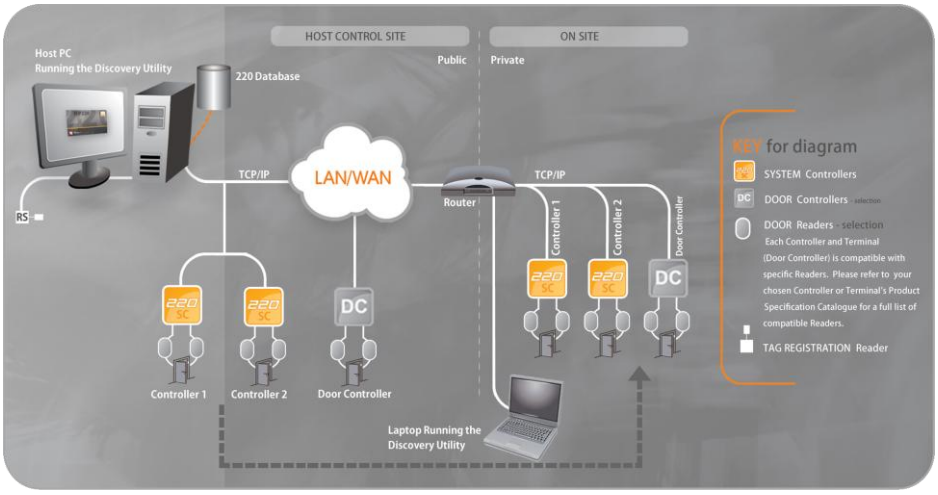


Figure 5 – Case Remote—Configure the Controller or Terminal's Static IP Address (Ethernet)

Use the stand-alone Discovery Utility on the same local Subnet as the 220 Controllers or Terminals for configuration. You may temporarily install and pre-configure the Controllers or Terminals on any convenient Subnet, local to the PC running the Discovery Utility. After configuration, move the Controllers or Terminals to the remote location. Alternatively Install the Discovery Utility on a PC on the remote Subnet. Export the settings to a file for manual entry into the 220 Base Application.

If a DHCP Server is present, IP Addresses are dynamically assigned initially. If the Controller or Terminal is NOT on the DHCP Server, ensure the PC is on the same IP Range as that of the Controller or Terminal. If the PC's IP Range differs, you cannot change the Controller or Terminal's settings. A public static IP Address is essential for the Controller or Terminal because the Controller or Terminal is destined for a WAN.

1. In Windows®, go to **Start**>**All Programs**>**220**>**Utils>Discovery Utility**.
2. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
3. From the Menu Bar, select **Network**>**Configure IP**.
4. **Logon** if requested (see page 9).

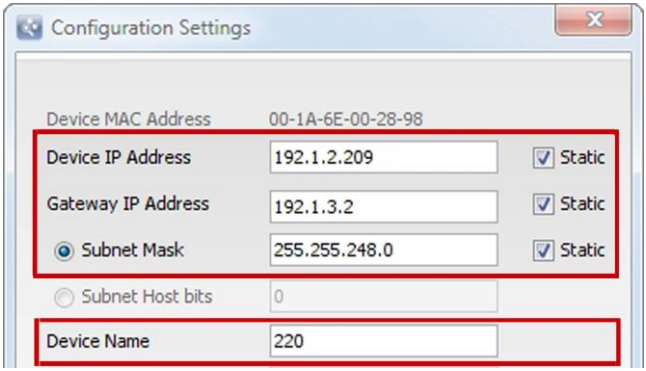


Figure 6 – Configuration Settings Dialog

By assigning an invalid IP Address, the Controller or Terminal may no longer communicate. Refer to the Hardware Installation Manual for information on restoring factory defaults.

5. In the Device IP Address textbox, enter a **Device IP Address**.
6. Tick the checkbox to set the IP Address to **Static**.
7. In the Gateway IP Address textbox, enter a **Gateway IP Address**.
8. Tick the checkbox to set the Gateway IP Address to **Static**.
9. Continue with ONE of the procedures (Subnet Mask or Subnet Host Bits) that follow:

Subnet Mask

a. Select the **Subnet Mask** radio button.
b. In the textbox, alongside, enter the **Subnet's Address**.
c. Tick the checkbox to set the Subnet Mask to **Static**.

Subnet Host Bits

a. Select the **Subnet Host Bits** radio button.
b. Enter the number of bits in the textbox.

10. If necessary, amend the supplied **Device Name**. Use the same site prefix to name devices belonging to the same site. For example: “Site_1–Factory”, “Site_1–Testing” and so on.

If the Force Update checkbox remains UNCHECKED, the Controller or Terminal changes the IP Address testing communication on the new Address. If successful, the update becomes final; if not, the Controller or Terminal reverts to its old settings.

Changes to the IP Configuration result in the Controller or Terminal rebooting on acceptance of the change. The Configuration Settings dialog remains open while allowing the Controller or Terminal to reboot. On closure of the dialog, the Utility again searches for the Controller or Terminal and if successful, displays the updated details.

11. Ensure the **Force Update** checkbox is **CHECKED** when assigning an Address on an external subnet. The Controller or Terminal changes the IP Address and reboots. If the Address points outside the Local Subnet, the Controller or Terminal is not found until it’s physically moved to the new location.
12. Click the **Update** button.
13. From the Menu Bar, select **File**>**Export IP Config**.
14. In the Save dialog, click the **Save** button (by default this file is named **discovery.txt**, you may however change this file name).
15. Exit the Discovery Utility.
16. Send a copy of the exported Discovery file (**discovery.txt**) to the Host Location.
17. If locally pre-configured, move the Controller or Terminal to its remote location.

*After installing the Controller or Terminal in its new location, you can find it by going to **Network**>**Search IP**.*

Option 2: Configure the Controller or Terminal's Public Host Name (Ethernet)

Use this option where you install your 220 Controller or Terminal behind a Router with a public hostname resolved to an IP Address. In this scenario, the Router is setup (by your Network Administrator) to route data to the separate Controllers or Terminals via the port numbers uniquely associated with them. Detection of Controllers or Terminals using the Discovery Utility is only done locally, that is on the Local Subnet, behind the Router. To address the Controller or Terminal from the world beyond the Router, the local IP Address of the Controller or Terminal must change to the Router's public hostname.

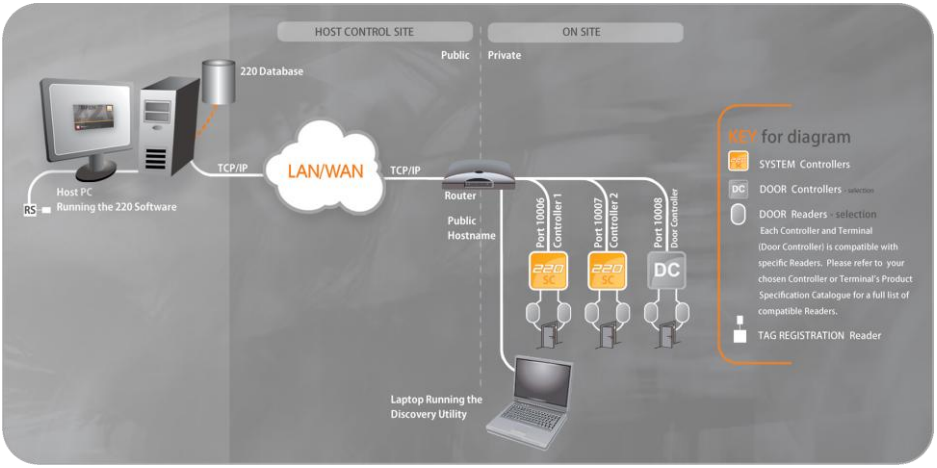


Figure 7 – Case Remote—Configure the Controller or Terminal's Public Host Name (Ethernet)

1. Select a UNIQUE **Communication Port Number** for the 220 Controller or Terminal.
2. Program the Router to direct all data destined for that port to the Controller or Terminal.

3. In Windows®, go to **Start**>**All Programs**>**220**>**Utils**>**Discovery Utility**.
4. In the **Discovery Utility** window, select the Controller or Terminal for configuration.
5. From the Menu Bar, select **Network**>**Configure IP**.
6. **Logon** if requested (see page 9).
7. Allow the DHCP assigned addresses to remain and set as static or obtain a static address from your network administrator.
8. If necessary, amend the supplied **Device Name**.

Change the Secure Logon and Clear the Controller or Terminal's memory as required.

9. Change the Communication Port Number to the unique port number set up on the Router.
10. From the Menu Bar, select **File**>**Export IP Config**.
11. In the Save dialog, click the **Save** button (by default this file is named **discovery.txt**, you may however change this file name according to your needs).
12. Exit the Discovery Utility.
13. Send a copy of the exported Discovery file (**discovery.txt**) to the Host Location.

In the 220 Software now add a new communication channel to your selected Site, either manually or by importing the file you exported earlier (**discovery.txt**). If the file is imported, the Port Number is correct and you need only change the IP Address to the Router's public Hostname. Auto-ID continues as normal.

Option 3A: Configure the Controller's Mobile Settings (GPRS) for GPRS and SMS

This connection option is not supported where you have Controllers connected (by RS485) to the GPRS enabled Controller.

When configuring the GSM Module for GPRS and SMS ensure that you obtain a PUBLIC Access Point Name (APN) from your Mobile Service Provider.

When using a Hostname instead of an IP Address, ensure that you have access to a PC with an active Internet connection.

This option only applies to the 220 Controller fitted with a GSM Module.

Pre-configure the Controller with the Controller connected to the local LAN. After pre-configuration, remove the network connection from the Controller.

Pre-configuration, get the following from your Mobile Service Provider:

- Buy a **SIM Card** (you will need the **PIN** and **PUK** numbers for this SIM Card).
- Get a public **Access Point Name** (**APN**).
- Confirm details for the **SMS Service Centre**.
- Have the **Username** and **Password** for the Access Point Name (APN) available (only needed in some instances).

And from a Dynamic Domain Name Service Provider, get the following:

- Select one of the supported Providers, namely **changeip.org**, **dyndns.com** or **no-ip.com**.
- Register a **Hostname for your 220 Controller** with your chosen Provider.
- Register a **Username** and **Password** for your 220 Controller.
- Register a **Hostname for the PC hosting the 220 Software**, or use a public static IP Address.

Both Hostnames must resolve to a public IP Address, they cannot remain blank.

1. In Windows®, go to **Start**>**All Programs**>**220**>**Utils**>**Discovery Utility**.
2. In the **220 Discovery Utility** window, select the Controller for configuration.
3. From the Menu Bar, select **Network**>**Configure Mobile Settings**.
4. **Logon** if requested (see page 9).

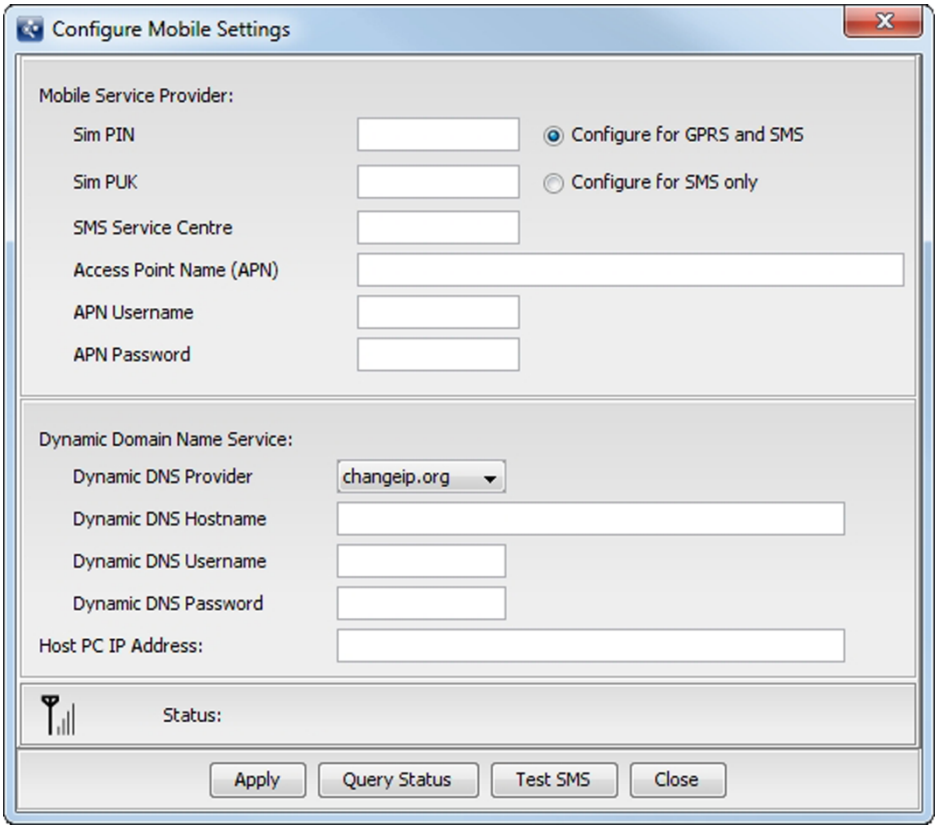


Figure 8 – Configure Mobile Settings Dialog

*The **Signal Strength** icon on the Status bar indicates the signal strength being experienced by the Controller's GSM Module. 5 Bars indicates maximum signal strength.*

5. Complete the fields under the header **Mobile Service Provider**:
   - **SIM PIN—**this is the Personal Identification Number (PIN), a numerical combination of up to 5 digits, supplied with your SIM Card. Wrong entry of the PIN (more than 3 times) locks the SIM Card.
   - **SIM PUK—**this is the PIN Unlock Key. This number offers protection of the device and SIM Card with the PIN. Entry of the wrong PUK (more than 10 times) permanently blocks the device, a new SIM Card is then required.
   - **SMS Service Centre—**the contact number for the repository that stores messages for delivery to the destination user when they are available. Stored on the SIM Card, this number may not come into sight until you activate your mobile settings. If you wish to use the service and the number does not finally appear, contact your service provider for assistance
   - **Access Point Name (APN)—**this is the name used to identify a public (free) GPRS bearer service in the GSM mobile network. The Access Point Name (APN) defines the type of service provided in the packet data connection.
   - **APN Username—**possibly needed for the Access Point Name (APN).
   - **APN Password—**possibly needed for the Access Point Name (APN).
6. Ensure the **Configure for GPRS and SMS** radio button is selected (default).
7. Under the header **Dynamic Domain Name Service**, From the **Dynamic DNS Provider** drop-down list, select one of the supported Providers.
8. In the Dynamic **DNS Hostname** textbox, enter the registered 220 Controller's Hostname.
9. In the **Dynamic DNS Username** textbox and **Dynamic DNS Password** textbox, enter the registered Username and Password respectively for your 220 Controller.
10. In the **Host PC IP Address** textbox, enter the public static IP Address.

When using a SIM Card with a single static IP Address, enter the public static IP Address of the Host PC, not the Hostname. Contact your Mobile Service Provider for more information on your SIM Card.

11. Click the **Apply** button.

The Discovery Utility captures the configuration information and forwards the information on to the Controller for activation. The Controller starts the process of establishing a GPRS connection. The Discovery Utility queries the Controller for status until the Utility gets a result. During the verification process there is an approximately 60-second time-out.

The Discovery Utility decides on the success of the configuration. At the end of the verification process, the Status bar at the bottom of the Configure Mobile Settings dialog, displays the status of the configuration. Possible status messages include:

- **Listening**—this is the desired status message.
- **GSM Module Not Present**—indicates the GSM Module is removed or uninstalled.
- **GSM Module Present**—Controller is aware the GSM Module is connected, however the Controller is busy going through the connection process.
- **SIM PIN or PUK Error**—indicates you have captured the wrong PIN or PUK number.
- **GPRS Network Error**—indicates the GSM Module cannot connect to the Network.
- **APN Error**—indicates the wrong APN Name was captured. This message also appears however, where you have exceeded your data cap or you have no available airtime on your SIM Card.
- **DDNS Error**—indicates there is an error with the captured

DDNS parameters.

- **Connected—**connected status only occurs if a Controller was already configured and currently connected by GPRS to the 220 Software while still connected by Ethernet.

*If the connection is not established, the Controller may begin the verification process again. In an instance where the verification process times out, click the **Query Status** button manually requesting the status.*

*If you do NOT get the status **Listening**, correct any errors and then press the **Apply** button again.*

On acceptance of the settings, the GPRS parameters are written to the **DiscoveryGSM.txt** file. The 220 Software automatically imports this file for permanent storage in the Database (in case of Hardware replacement).

12. On achieving the Listening status, close the Configure Mobile Settings dialog.
13. Export the configuration file, from the Menu Bar, select **File**>**Export IP Config**.
14. Click the **Save** button.
15. Exit the 220 Discovery Utility.
16. Send both the **DiscoveryGSM.txt** and **Discovery.txt** files to the Host PC (ensuring you place both files in the same destination folder) before beginning the Auto-ID process.
17. Disconnect the 220 Controller from the LAN.
18. Reboot the Controller.
19. Continue with the Auto-ID process (see page 27 for assistance).

Option 3B: Configure the Controller's Mobile Settings (GPRS) for SMS Only

A public Access Point Name (APN) is NOT required for SMS only.

In instances where your Controller connects by Ethernet, but you still require SMS capability, continue as follows:

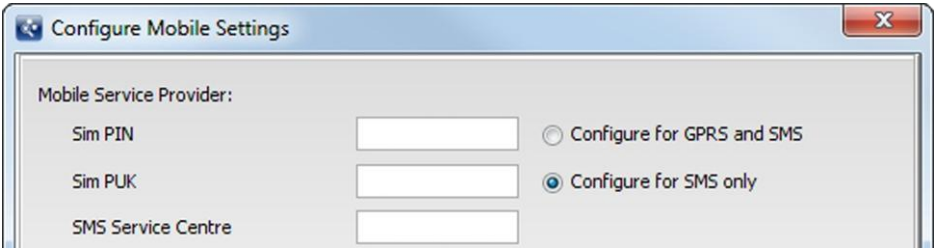


Figure 9 – Configure Mobile Settings Dialog

*The **Signal Strength** icon on the Status bar indicates the signal strength being experienced by the Controller's GSM Module. 5 Bars indicates maximum signal strength.*

1. In Windows®, go to **Start**>**All Programs**>**220**>**Utils**>**Discovery Utility**.
2. In the **220 Discovery Utility** window, select the Controller for configuration.
3. From the Menu Bar, select **Network**>**Configure Mobile Settings**.
4. **Logon** if requested (see page 9).
5. Ensure the Configure **for SMS Only** radio button is selected.
6. Complete the fields under the header **Mobile Service Provider**:
   - **SIM PIN**
   - **SIM PUK**
   - **SMS Service Centre**
7. Click the **Apply** button.

*Your setup is complete and working correctly when you receive the Status message **SMS Configuration Completed**. We recommend that you test the connection by clicking the **Test SMS** button. Where called for by your country and or your service provider, precede the recipient's mobile number with the country code.*

Configure the Port Number

This is an advanced feature; use the feature only if required.

After making changes to one or more Controller or Terminal's Configuration Settings, ensure that you export the configuration file for entry into the 220 Base Application.

Using the **Discovery Utility,** view or configure the **Port Number** of the Controller or Terminal as follows:

1. Select the **Controller** or **Terminal** for configuration.
2. From the Menu Bar, select **Configuration**>**Set Configuration**.
3. **Logon** if requested (see page 9).
4. In the **Communication Port Number** textbox, change the Port Number. The default Port Number is **10005** for Controllers and **10008** for Terminals. Only change the default Port Number if it clashes with other devices or services on your network.
5. In the **Terminal Listener Port** textbox, change the Port Number (Controller listens to Terminals on this Port). The default Port Number is **10008**. Only change the default Port Number if it clashes with other devices or services on your network or if you communicate with the Terminal over a WAN using Port Fowarding.
6. Tick the **Safe IP** checkbox, thus ensuring that the Controller only responds to the Host PC.
7. Click the button to confirm.
8. Wait while the Controller or Terminal re-boots (about 15 seconds).

3 Site Configuration Procedure

Open the Software

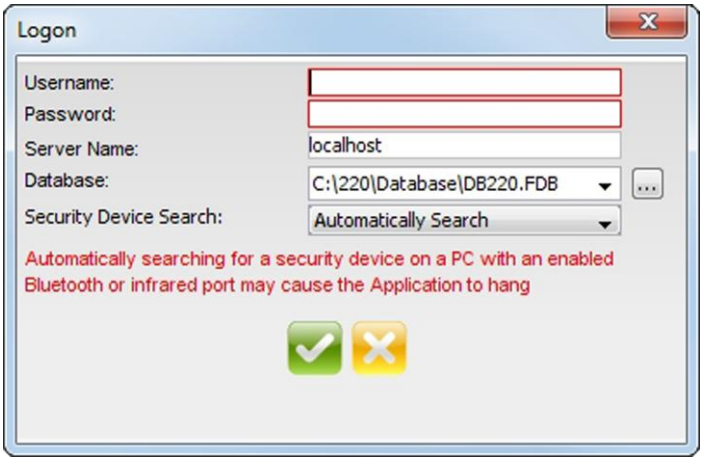


Figure 10 – Login Dialog

1. In Windows®, click **Start**>**All Programs**>**220**>**220**.
2. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).
3. From the **Security Device Search** drop-down list, make your selection from the following choices:
   - **Automatically Search—**for *220-3* and *220-4* installations where an RS Registration Interface is connected but you are unsure of the COM Port number in use by the RS Registration Interface. Automatically searching on a computer that has an enabled Bluetooth or Infrared Port may result in the 220 application freezing.
   - **Enter the COM Port Name—**for *220-3* and *220-4* installations where an RS Registration Interface is connected and you know the COM Port number in use by the RS Registration Interface. *Recommended when you have an enabled Bluetooth or Infrared*

Port. If you select this choice, enter the COM Port number in the supplied textbox. If your installation does NOT use the default Database Server Port of 3050, enter the server name and port number (that is *server:port*). An example could include *localhost:3051*, that is with *3051* being the port used.

- **I do NOT Have One**—for *220-1* and *220-2* installations with no RS Registration Interface.

4. Click the button.

Do NOT disconnect the RS Registration Interface while still connected to the 220 Software. Should you unintentionally disconnect the RS while the Software's running, close the 220 Software, reconnect the RS and then restart the Software.

Database Version Check

After completing the login action, the **Automatic Database Upgrade Utility** checks the database version. If the Utility confirms the Database is older than that needed by the Software, a Warning dialog tells you an upgrade is needed. Perform the upgrade as follows:

1. At the Warning dialog, click the **OK** button.
2. In the Database Updater dialog, click the **Upgrade** button.
3. At the Message dialog, click the **OK** button.

If you do not upgrade the Database immediately, the 220 Software closes.

Hardware Auto-ID

Hardware detected for the first time receives a Logical Address. This Logical Address does not change, thus ensuring continuity in the Database.

During an Auto-ID, the Base Application searches for and configures hardware for use with the 220 System. Perform an Auto-ID after physically connecting and powering up the Hardware. The Auto-ID process differs across the different communication mediums; therefore continue with one of the following:

Controller Connected to Host PC using RS485 (RS Registration Interface)

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. From the Auto-ID Communications Configuration dialog, select the appropriate **Com Port** record.
4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected to the Host PC using TCP/IP

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. If your Controller does NOT appear in the **Auto-ID Communications Configuration** dialog continue as follows:

When using IP Terminals, do not use the button. Instead, make use of the button

   a. Click the button.
   b. In the **Channel** column, replace the default IP Address details with the IP Address of your Controller.
   c. Press **Enter**.

   Or alternatively continue as follows:

a. Click the button.
b. In the Input dialog, enter the **Subnet Mask** details for your Network.
c. Click the button.

*The **IP Door Controllers (Advanced)** tab provides a list of the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the button.*
2. *In the Input dialog, enter the **Subnet Mask** details for your network.*
3. *Click the button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*
7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 4 following).*

4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected over a Wide Area Network (WAN)

Controllers connected using a GSM Module do NOT support IP Terminals.

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. In the Auto-ID Communications Configuration dialog, click the **Import Channels** button.
4. Select the **Discovery.txt** file (originally exported from the Discovery Utility).
5. Click the **Open** button.

*The **IP Door Controllers (Advanced)** tab provides a list of the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the **Import Channels** button.*
2. *Select the **Discovery.txt** file (originally exported from the Discovery Utility).*
3. *Click the **Open** button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*

7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 6 below)*

6. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
7. Click the button.
8. At the Firmware Revision dialog, click the button.

*You may carry out the Auto-ID process at any stage, by selecting **Hardware**>**Auto ID Units**.*

Connecting Controller A via the network and Controller B (connected to Controller A) by RS485, lets you configure both Controllers at the same time.

*After performing Auto-ID, review the log of identified units by selecting **Hardware**>**Latest Auto ID Log** from the Menu Bar. This feature lets you check whether Auto-ID has missed any terminals, possibly because of a wrong DIP-switch setting or faulty communications.*

Firmware Version Confirmation

After physically connecting, powering up and identifying the Hardware, confirm whether a Firmware upgrade is required.

The Firmware Revisions dialog indicates the Unit Type along with the Latest Firmware revision available and the Current Firmware version in use by the unit. Access the Firmware Revisions dialog by selecting **Hardware**>**Firmware Version Check** from the Menu Bar.

*See the Software Installers Guide, **Part 7 – Utilities** for more information on the **Firmware Upgrade Utility**.*

Standard Site Configuration

1. If not already selected, select the  Page Tab.
2. In the Configuration Pane, complete the **Site Name** textbox.
3. Complete the **Site Street/Physical Address** text area.

Advanced Site Configuration

Communications Group Options

1. If you wish to communicate only with the selected site, select the **Communicate Exclusively** checkbox.
2. From the **Communication Schedule** drop-down list select a Communication Schedule.
3. In the final drop-down list in the **Communications** group, select from the following options:
   - **Inter-controller**—this allows for communication to take place across Controllers. Inter-controller Communications is beneficial when used with Building Management and in maintaining Anti-passback (APB) status across Controllers.
   - **Fall-back**—this allows for configuration where TCP/IP is the default communications channel and RS485 being the secondary channel. Where your TCP/IP connection fails, the 220 Software falls back on RS485 and operations continue as normal (slightly slower than TCP/IP). When the TCP/IP connection restores, the Software automatically resumes communication on the primary TCP/IP connection. *This configuration does NOT support inter-controller or pass-through communications.*

The selection you make above, determines the options available to you on the Controller Configuration Pane.

*Click the **Synchronize** button to write IP Mapping files to the 220 directory. These files are used on selection of **UDP Multi Controller** as the **communications type**.*

Region Group Options

1. From the **Time Zone** drop-down list, make your selection.
2. Set the Apply Daylight Saving option as follows:
   a. Alongside **Apply Daylight Saving**, click the **Yes** radio button.
   b. Click on the **Set Daylight Saving** button.
   c. In the Set Daylight Saving dialog, set the **Time Offset**, **Start Date**, **Start Time**, **End Date** and **End Time**.
   d. Click the button.

Miscellaneous Group Options

Door Status Polling

1. Click the **Set Parameters** button.
   - Set the **Polling Frequency** (seconds)—how often Doors (Locations) get polled for their status.
   - Set the **Door Open Time Limit** (seconds)—normal duration Doors (Locations) remain open.
2. Click the button.

Valid Site Codes

1. Click the **Configure** button.

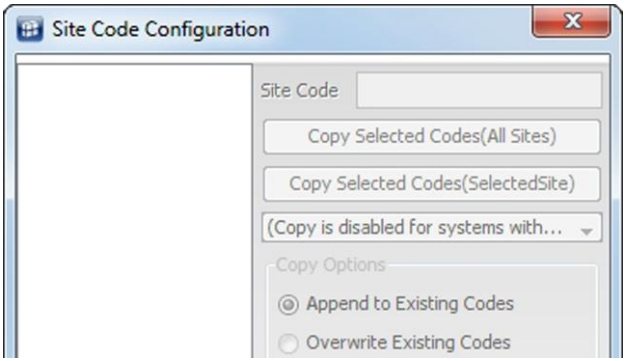


Figure 11 – Site Code Configuration

2. Click the button.
3. In the **Site Code** textbox, enter a suitable code.

4. Select either the **Append to Exiting Codes** or **Overwrite Existing Codes** radio button.
5. Click the button.

After updating the Site Configuration Pane, click the button.

Controller Configuration

1. Select the Page Tab.
2. In the **Controller Name** textbox, assign your Controller a suitable name.
3. From the **Mode Configuration** drop-down list, make your selection.

> *The instructions that follow continue as for an Advanced Configuration. For a Standard Configuration ignore references made to fields that appear greyed out.*

4. Enable or disable Controllers as per your requirements, by selecting or de-selecting the **Controller Enabled** checkbox.
5. From the **APB Configuration** group, adjust the following settings:
   - Set the **APB Lockout Delay on Entry** (minutes)—the same Tagholder may not pass the same anti-passback (APB) entry access point within the specified time period.
   - Set the **APB Lockout Delay on Exit** (minutes)—the same Tagholder may not pass the same anti-passback (APB) exit access point within the specified time period.

Site Configuration Set to Inter-controller Communications
With your site setup to use inter-controller communications, continue with the following Controller configuration options:

1. From the **Primary Communications** drop-down list, make your selection.

2. From the **Communications Mode** drop-down list, make your selection from the following choices:
   - **Standard Controller**—this is the default choice. This configuration associates to Controller configurations preceding V1.82, including all configuration choices offered in 220 Software V1.80. In addition, support includes inter-controller communications (for IP Controllers only).
   - **Controller Forwards Communications for RS485 Controllers**—this allows for inter-controller communications for Controllers daisy-chained from an IP Controller. For example, Controller A has a network cable connected to it and has Controller B and Controller C connected to its RS485 Controller bus. A Tagholder enters a Door (Location) on Controller A, Controller A will update the anti-passback status of the Tagholder on Controller B and Controller C. This option DOES NOT affect pass through communications. The Software still communicates with the daisy-chained Controllers via Controller A.

Activate the Controller Forwards Communications for RS485 Controllers option as follows:

1. *In the Controller Configuration Pane, click the **Communications** button.*
2. *Click the*  *button.*
3. *In the **Address** column of the new record, enter the Communication Port details for your RS.*
4. *Click the*  *button.*
5. *From the **Communications Mode** drop-down, select the **Controller Forwards Communications for RS485 Controllers** option.*
6. *From the **Primary Communications** drop-down list, select the newly added Communication Port number.*

Site Configuration Set to Fall-back Communications

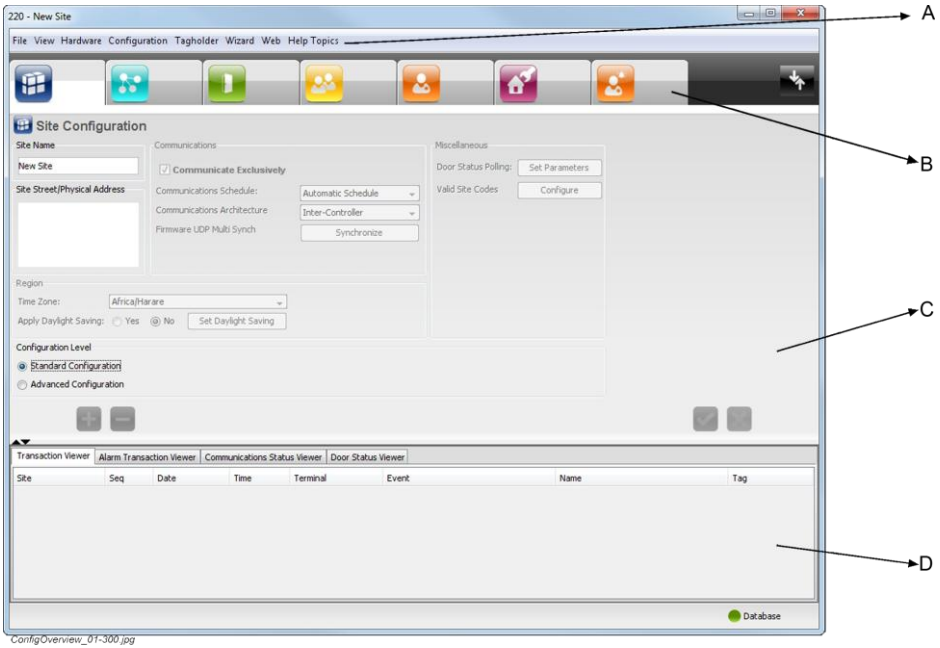
Fall-back Communications allows for configuration using TCP/IP as the primary communications channel and RS485 as the secondary channel. Where your TCP/IP connection fails, the 220 Software falls back on RS485 and operations continue as normal (slightly slower than TCP/IP). When the TCP/IP connection restores, the Software automatically resumes communication on the primary TCP/IP connection. *This configuration does NOT support inter-controller or pass-through communications.* With your site setup to use fall-back communications, continue with the following Controller configuration options:

1. From the **Primary Communications** drop-down list, make your selection.
2. From the **Secondary Communications** drop-down list, make your selection.

After updating the Controller Configuration Pane, click the  button.

4 Using the 220 Software

220 User Interface



ConfigOverview_01-300.jpg

Figure 12 – 220 Base Application User Interface

The 220 Base Application only displays as shown in Figure 12 where you select the standard Windows® 7 (Professional, Enterprise or Ultimate), Windows® Vista (Business or Ultimate) and XP Professional themes. Using other non-standard themes results in 220 displaying incorrectly.

The following parts comprise the 220 Base Application's interface:

A—Menu Bar
Contains drop-down menus that let you navigate between different operations in the 220 Base Application. These menus include: File, Hardware, Configuration, Tagholder, Web and Help Topics.

B—Page Tabs
Switches between the different configuration settings, for example:

- Site Configuration
- Controller Configuration
- Door Configuration
- Access Group Configuration
- Tagholder Configuration
- Building Management Configuration
- Notification Configuration

C—Configuration Pane
Lets you adjust various settings based on your selection from the Page Tabs or Menu Bar.

D—Viewer Pane
The Viewer Pane consists of Tabs showing the following information:

- **Transaction Viewer**—gives a live real-time view of all types of transactions in the System. It displays the names of the Doors (Locations) and details of Tagholders who have entered or exited these Doors (Locations).
- **Alarm Transaction Viewer**—gives a live real-time view of all *alarm* transactions in the System. It displays the names of the Doors (Locations) and details of Tagholders who have entered or exited these Doors (Locations).

- **Communications Status Viewer**—indicates the status of the 220 Controllers communicating with the 220 System.
- **Door Status Viewer**—indicates the status of the Doors (Locations) forming part of the Site. You may physically unlock Doors (Locations) displayed here, using the 220 Software.

Click the  button (placed alongside the Page Tabs) to adjust the Base Applications layout:

- ***First Click**—closes the Viewer Pane, opening the Configuration Pane in Full Screen Mode.*
- ***Second Click**—opens the Viewer Pane in Full Screen Mode.*
- ***Third Click**—returns the Base Application to Split-screen Mode, showing both the Configuration Pane and the Viewer Pane.*

Alternatively, adjust the layout as follows:

1. *From the Main Menu, select **View**.*
2. *Make your selection from the following:*
   - ***Split View**—shows both the Configuration Pane and the Viewer Pane.*
   - ***Configuration View**—closes the Viewer Pane, opening the Configuration Pane in Full Screen Mode.*
   - ***Monitoring View**—opens the Viewer Pane in Full Screen Mode.*

Using Help

*The **Context Sensitive WebHelp provided with the 220 Software works with your positioned Mouse Pointer (or cursor) on your screen**. For example if you place your Mouse Pointer in the Viewer Pane, WebHelp opens Context Sensitive WebHelp specific to the Viewer Pane. If, however, you want WebHelp specific to the active Configuration Pane, continue as follows:*

1. *Move your Mouse Pointer into the Configuration Pane.*
2. *Anchor your Mouse Pointer by clicking the left-hand button on your mouse, thus ensuring the Pane has focus.*
3. *Press the **F1** key on your keyboard.*

The 220 System has integrated **context sensitive** WebHelp. Information not covered here is covered in detail in the WebHelp. Activate the WebHelp as follows:

1. In Windows®, go to **Start**>**Programs**>**220**>**220**.
2. From the Menu Bar select **Help Topics**>**Online Help**.

Key Assist

Selecting the **Key Assist** option opens an area on the right-hand side of the Base Application's desktop. This area displays a list of keyboard shortcuts that let you quickly move between the Page Tabs.

The final option listed in the Key Assist Area (**System Navigation**) opens the System Navigation dialog. This dialog allows quick navigation through System related functions.

Support Diagnostics

The Support Diagnostics Bundle assists you by supplying Technical Support Staff with information about your System. This helps them to

solve your problems quickly and efficiently.

Create a Support Diagnostic Bundle as follows:

1. From the Main Menu, select **Help Topics**>**Support Diagnostics**.
2. Select the **Included in Bundle** tab.
3. The Diagnostics Bundle includes the following information by default. Customize the information sent by deselecting the checkbox alongside:
   - **Transactions (Last 500)**—selecting this sends the last 500 transactions in the System including access, status and alarm transactions.
   - **System Log Files**—sends the System Log files.
   - **Firebird Log (Database Server)**—sends the Database server log if the Database is installed on the default directory.
   - **Site Summary**—includes information such as the number of Tagholders with access and the number of Doors configured on a Site. Also provides hardware configuration data like how the Base Application communicates to the Controller as well as information about connected terminals and their configuration.
   - **Holiday Data**—sends information about Holiday configuration.
   - **Host PC Information**—includes information such as PC specifications, processes running on the PC and results from a netstat (a command-line tool providing information on network connections, routing and other network interface statistics).
4. Select the **Contact Information** tab.
5. Fill in your contact information as necessary.
6. Create the Diagnostic Bundle using one of the following methods:

Sites WITH Pre-configured Notifications

For e-mail setup information please refer to Part 3 - Preference Configuration (System Notification Tab).

1. Click the **Generate Bundle** button.

2. If you have an existing reference number, complete the **Reference No.** textbox.
3. Complete the **Support E-mail** address textbox.
4. Click the **E-mail Bundle** button.
5. Click the  button.

Sites WITHOUT Pre-configured Notifications

1. Click the **Generate Bundle** button.
2. Click the  button.
3. Browse to **C:\220**.
4. Locate the zip file **diagnosticBundle_(date generated)_(time generated)**.
5. Attach the zip file to an e-mail.
6. Send the e-mail to the Technical Support Staff.

Site Setup

Perform Site setup in the following order:

1. Site Configuration
2. Controller Configuration
3. Door Configuration
4. Access Group Configuration
5. Tagholder Configuration
6. Holiday Configuration
7. Full Upload

For detailed information on Site setup, please refer to Part 3 of the 220 Software Manual. Or alternatively, refer to the WebHelp included with the 220 Software.

Advanced Options

Guidelines for the Setup of IP Terminals (iTT or iTRT)

Support for IP Terminals (iTT and iTRT) is only available on Controllers with firmware V4.00 and above.

DO NOT connect RS485 Terminals to IP Terminals on the RS485 connector. This is an unsupported configuration.

Use the Discovery Utility for discovering, configuring and grouping IP Terminals with their parent Controller.

Controllers must know which Terminal they should communicate with. In an RS485 environment a Logical Address, assigned during Auto-ID achieved this. 220 however, calls for extra steps when using an Ethernet configuration. In an Ethernet configuration, group IP Terminals with a parent Controller before configuration. Then Auto-ID the hardware and finally, perform a Full Upload. Only then can you access the hardware with the Firmware Upgrade Utility.

Where you have more than one Site, repeat the procedure for each Site.

Steps to Discover, Group and Configure Controller and IP Terminal Settings

1. Display Controllers and IP Terminals by performing a network search. Refer to page 8 for more information. On display of the Controllers and Terminals, the following icons appear: the  icon represents unlinked Controllers. The  icon represents Terminals.

2. Configure the IP Address for each Controller and IP Terminal. Refer to page 11 for more information.
3. Group one or more IP Terminal with a single Controller. Refer to page 10 for more information.
4. Configure the application settings (that is the Port Number) for each Controller and IP Terminal. Defaults should meet most installations needs.

DO NOT set Safe IP at this stage.

5. Set the password for each Controller and IP Terminal, ensuring that you keep the same password for all units. The default password is **masterkey**. Change this password to a string of not more than 16 characters.
6. If you are connecting over a WAN, export the selected units to a text file (discovery.txt). Refer to page 15 for information on this process.

Steps Required in the 220 Base Application

1. Perform and Auto-ID. Refer to page 27 for more information.
2. Perform a Full Upload to all units. Refer to Part 3 – General Configuration for more information on this process.

Steps Required in the Firmware Upgrade Utility

Perform a Full Upload BEFORE trying to Ping your IP Terminals.

3. Start the Firmware Upgrade Utility and set the Protocol to **UDP Multi Controller**.
4. Check that all hardware is connected and working as specified by using the **Ping** tool.
5. Carry out a Firmware Upgrade if required.

Refer to Part 7 – Utilities for detailed instructions on using the Firmware Upgrade Utility.

Additional Options

- Carry out **Safe IP** by going back to the Discovery Utility. Search for the units and then **carry out Safe IP on each unit individually**. Refer to Part 7 – Utilities for more information.
- Move an IP Terminal from one Controller to another, in the Base Application, uninstall the IP Terminal first. Then perform a Full Upload. This releases the IP Terminal from its parent Controller and prevents network diagnostic problems. Refer to Part 3 – General Configuration for more information.

Extra Information

Further information is available at the following resources:

- **220 Software Manual** (ISW303-0-0-GB-XX).
- **220 WebHelp** (ISW391-0-0-GB-XX).
- **220 Controller Installation Manual** (ISC301-0-0-GB-XX).

User Notes