VANDERBILT INDUSTRIES

lite blue® Manual

VANDERBILT

Vanderbilt Industries Copyright Notice

CONTACT INFORMATION

Vanderbilt Industries
Phone: 855-316-3900
Fax: 973-316-3999
www.vanderbiltindustries.com

Contents

VBB-NRI G2 92

VRI-1 111

UL Listing Summary

Compatible UL evaluated equipment

Vanderbilt Equipment

- Vanderbilt AP02 *(pending)*
- VBB-RI
- VBB-NRI
- VBB-NRI G2
- SBB-RI (Legacy)

XCEED-ID Equipment

- XF1050

Supported Proximity Cards

- Standard 26-bit Wiegand Format
- Vanderbilt 34-bit Wiegand Format
- HID Corporate 1000 35-bit
- HID Corporate 1000 48-bit
- HID/ProxIF 37-bit
- XceedID 40-bit
- XceedID 35-bit

Note: All interconnected devices (panic hardware, REX, alarm devices, door contacts, computers, wiring, etc.) must be UL Listed.

Hardware Not UL Evaluated

Schlage VIP Locks

Schlage AD-300 Locks

Schlage Wireless Locks

- PIM400-485-VBB
- AD-400 locks
- PIM-SBB (Legacy)
- WA Series locks
- WRI Series locks
- GWE – ENGAGE Gateway (RS-485)
- NDE Series Wireless Locks w/ ENGAGE Technology

Firmware Designation

VBB Firmware: lite blue v. Y.X.X

- Y – Represents the embedded firmware version (matching the software application version)
- X.X – Sequential numbers representing the embedded firmware feature upgrades

VBB-RI Firmware: g1_0.XX

- XX – Sequential numbers representing the embedded firmware feature upgrades

VBB-NRI Firmware: g4_0.XX

- XX – Sequential numbers representing the embedded firmware feature upgrades

VRI-1 Firmware: vri1_appl_X_XX_XX.aax

- X_XX_XX – X.XX.XX firmware feature version

VRI-1 Firmware: vri2_appl_X_XX_XX.aax

- X_XX_XX – X.XX.XX firmware feature version

UL Evaluated Firmware

- UL is evaluating firmware v5.0.0 Build 28 in the VLB
- UL has evaluated firmware g1_0.05 in the SBB-RI (Legacy)
- UL has evaluated firmware FV11 in the VBB-RI
- UL has evaluated firmware g4_0.08 in the VBB-NRI
- UL has evaluated firmware v6.31 in the VBB-NRI G2

The following should be incorporated into the system:

- The UL 294 requires the **lite blue** controller enclosure and the VBB-RI enclosure to have a tamper switch that will generate an alarm whenever the enclosure is opened. Connect the tamper switch flying leads to a UL Listed burglar alarm system or UL Listed local siren/annunciator.

Note: UL has only evaluated the system for stand-alone operation. The connection to a PC/Web browser is to be employed as a local programming/downloading/monitoring tool only.

Operation Testing and Maintenance

Operation Testing

Once **lite blue** and system components are installed, log into the system and set up a cardholder with a credential and access. Present that credential at read head to test. A green LED indicates system is working.

Maintenance

No regular maintenance is required; **lite blue** and system components are self-supporting.

Declaration of Conformity

Below is the Declaration of Conformity for the VLB, VBB-NRI and VBB-RI.

We Of	Vanderbilt Industries 2 Cranberry Road Parsippany, NJ 07054 USA
Certify that the equipment described below conforms with the essential requirements of the following European Directive: Electromagnetic Compatibility (EMC) 2004/108/EC	
Conforming Apparatus	VBB Vanderbilt lite blue Reader Controller VBB-NRI Vanderbilt lite blue Network Reader Interface VBB-RI Vanderbilt lite blue Reader Interface
Serial Numbers	Serial Number Starting with BB100,000
Harmonized Standards Referenced or Applied	EN 55011:2009/A1:2010 EN 61000-6-2:2005/AC:2005
Authorized Representative	Elie Moneuse, Production Manager Vanderbilt Industries Parsippany, NJ USA Tel: 973-316-3926 E-mail: eliemoneuse@vanderbiltindustries.com
Date of Issue	March 15, 2009
Signed	Elie Moneuse

Preface

This manual describes the installation and wiring procedures for the **lite blue** controller and peripheral devices.

Who should use this book

This installation manual provides guidelines for installing and configuring the **lite blue** controller and the hardware that interfaces with it. This guide is intended to be read by installation technicians and service personnel only. It is not intended for end users of the system.

How this book is organized

Before Installation: Describes the processes and steps necessary before installing the **lite blue** system.

Chapter 1 lite blue: Describes how to correctly configure the **lite blue** controller along with its features and specifications.

Chapter 2 VBB-RI Reader Interface: Describes how to connect the VBB-RI to **lite blue** and peripheral devices.

Chapter 3 VBB-OBRI Onboard Reader Interface: Describes how to connect the **lite blue** VBB-OBRI to peripheral devices.

Chapter 4 SBB-RI (Legacy) Reader Interface: Describes how to connect the Legacy SBB-RI to **lite blue** and peripheral devices.

Chapter 5 VBB-NRI Networked Reader Interface: Describes how to connect the VBB-NRI to **lite blue** and peripheral devices.

Chapter 6 VRI-1 Single Reader Interface: Describes how to connect the new VRI-1 to **lite blue** and peripheral devices.

Chapter 7 VRI-2 Dual Reader Interface: Describes how to connect the new VRI-2 to **lite blue** and peripheral devices.

Chapter 8 Schlage Adaptable AD-300 Series Locks: Describes the integration of Schlage AD-300 Locks to **lite blue**.

Chapter 9 Schlage VIP Locks: Describes the integration of Schlage VIP Locks to **lite blue**.

Chapter 10 Schlage Adaptable AD-400 Series Wireless Locks: Describes the integration of Schlage AD-400 Series Wireless devices with **lite blue**.

Chapter 11 Schlage NDE Series Wireless Locks with ENGAGE: Describes the integration of Schlage NDE Series Wireless locks with **lite blue**.

Chapter 12 Schlage Wireless Readers: Describes the integration of Schlage wireless devices to **lite blue**.

Chapter 13 VEVMS-VBB Video Server Integration: Describes in brief the integration of the VEVMS-VBB video server with **lite blue**.

Chapter 14 Troubleshooting: Tips and suggestions on how to more effectively use **lite blue**.

Symbols and conventions

The following are the documentation conventions used in this manual:

Note: A note provides information which should be considered by the user.

Warning: Provides important information about procedures and events. If not considered by the user, it may cause damage to hardware or system data.

Bold: Text in bold letters are used for window names, button names etc.

Disclaimer: Disclaimers provide information that should be considered by the technician.

U.S./International Technical Support

If any problems are encountered while installing or operating **lite blue**, please contact our technical support team for assistance.

U.S. Vanderbilt Technical Support: Phone: 855-316-3900

International Vanderbilt Technical Support: Phone: 973-316-3900

Vanderbilt Technical Support: E-mail: techsupport@vanderbiltindustries.com

Hours of Technical Support

Standard technical support is available during Vanderbilt normal business hours, Monday through Friday, excluding Vanderbilt Industries observed holidays.

Before Installation

This section provides information on what should be considered before installing the **lite blue** hardware.

Requirements

- Check to see that all the equipment necessary for the installation is on hand. Make sure all the necessary tools to properly install the equipment, i.e. screwdrivers, wire cutters, digital meter, etc., are available.
- Mount all the enclosures in a secure and accessible location.
- It is optimal to mount all enclosures on fire rated plywood which is affixed to a solid wall covering i.e. sheetrock or bare cinder block.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4" x 1" lag bolts.

Electrical Wiring Considerations

- Wiring methods shall be in accordance with the National Electrical Code (ANSI/NFPA70), local codes, and the authorities having jurisdiction.
- The use of unshielded or ungrounded cable may cause problems. Ground shields must be grounded only at one end. If the shield is connected in both ends a ground loop will be created which will introduce more noise into the system.
- Before installing the system, verify that the correct UL Listed Power-limited Power supplies capable of 4 hours standby power are available.
- Remember to turn off all power before connecting any equipment.
- Make sure the correct wire type and gauges are being used as indicated on the cable requirement chart, please refer to the Cable Requirement Chart for details.
- All back-up batteries should be replaced with the same type and rating as the original power supply.
- A licensed electrician will need to supply 120VAC for connection to a UL294 Listed Power Limited, Power Supply capable of 4 hours standby power for the **lite blue** controller.

Before Powering System

- Mount and connect all readers in accordance with manufacturer's specification.
- Mount and connect all door contacts in accordance with manufacturer's specification.
- Mount and connect all exit requests and annunciators in accordance with manufacturer's specification.
- Mount and connect all peripheral equipment in accordance with manufacturer's specification.
- Mount and connect all lock devices in accordance with manufacturer's specification.
- Verify that the micro SD Card is firmly seated to **lite blue** and has not been loosened in shipping.

Environmental Consideration

- **lite blue** (VLB), the VBB-NRI and the VBB-RI must be installed indoors within the protected premises in a clean and a dust free environment.
- Ambient temperature: 32F to 120F (0 C to 49C)
- Relative Humidity: 85%, +/- 5%

Cable Requirement Chart

The chart below gives the recommended distance between the **lite blue** controller and the devices it connects to. All cabling and wire should be UL Listed and/or Recognized wire suitable for the application.

- Power supply input line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.
- RS-485 communication line(s) must have signal line transient protection complying with the Standard for Protectors for Data Communications & Fire Alarm Circuits, UL 497B, with a standard marked rating of 50 V.

Connection	Max Distance Power (ft)	Max Distance Communication (ft)	Cable Requirement
lite blue to VBB-RI	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
VBB-OBRI to Magstripe Reader Head	200	200	22 AWG/5 Condr, Strd, Shld
VBB-OBRI to Proximity Reader Head	500	500	22 AWG/5 Condr, Strd, Shld
lite blue to VRI-1	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to VRI-2	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
VBB-NRI to Power Supply	4000	N/A	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to AD-300	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to Schlage VIP			
At 12 Volts DC	1000	4000	18 AWG/2 Pair, Strd, Twst, Shld
At 24 Volts DC	3000	4000	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to PIM400-485-VBB	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to GWE – ENGAGE	4000	4000	18 AWG/2 Pair, Strd, Twst, Shld
lite blue to PIM-SBB (Legacy)	1000	1000	18 AWG/2 Pair, Strd, Twst, Shld

Abbreviations:

- Strd. = Stranded
- Shld. = Shielded
- Twst. = Twisted

Web Browser Requirements

Internet Explorer 11

lite blue has been tested on IE 11 running on the Windows 10 operating system. Any machine with the recommended amount of memory for Windows 10 will meet the memory requirements for Internet Explorer 11.

Firefox v80.0

lite blue has been tested on Firefox running on the Windows 10 operating system. Any computer running with the recommended amount of memory for Windows 10 will meet the memory requirements for Firefox. Firefox has not been tested on the Mac OS X operating system.

Apple Safari v13.1 (OS X)

lite blue has been tested on Apple Safari v13.1 running on the MacOS Catalina v10.15.4 operating system. Any Apple Mac system with the recommended amount of memory for MacOS Catalina v10.15.4 will meet the memory requirements for Safari.

Apple Safari Mobile

lite blue has been testing on Apple Safari v14 mobile running on Apple iPadOS v14.0 operating system.

Google Chrome v85.0

lite blue has been tested on Google Chrome running on the Windows 10 and Apple iPadOS v14.0 operating systems. Any system running with the recommended amount of memory for the underlying operating system will meet the memory requirements for Chrome. Chrome has not been tested on the Mac OS X operating system.

Note: lite blue uses ports 80 and 443 to communicate; these ports cannot be blocked by any firewall.

Device Power Requirements

The **lite blue** controller is designed to provide power from a power supply to itself and the 2 onboard reader interfaces. Additional devices may be powered separately using the same power supply (*i.e. not routed through the **lite blue***). The power supply(s) must be large enough to power the **lite blue** controller and all peripheral devices. Make sure that the total power requirements of all devices do not exceed the output of the power supply(s) in use. If not enough power is being supplied, the devices and the **lite blue** controller will not work correctly.

Description	Model #	Amps	Volts
Vanderbilt **lite blue**	VLB	485mA	12 to 24VDC
Reader Interface	VBB-RI	300mA	12 to 24VDC
Reader Interface	VRI-1	150mA	12 to 24VDC
Reader Interface	VRI-2	450mA	12 to 24VDC
Reader Interface (Legacy)	SBB-RI	300mA	12 to 24VDC
Network Reader Interface	VBB-NRI (Powered Locally)	300mA	20 to 32VDC
Network Reader Interface	VBB-NRI G2 (Powered Locally)	485mA	12 to 24VDC
AD-300 Hardwired Lock	AD-300	300mA	12 to 24VDC
AD-400 Wireless PIM	PIM400-485-VBB	300mA	12 to 24VDC
AD-400 Wireless Lock	AD-400 External Power Supply	300mA	12 to 24VDC
ENGAGE Gateway	GWE – ENGAGE Gateway (RS-485)	330mA	12 to 24VDC
Schlage VIP Lock	VIP Lock	1.1A	12 to 24VDC
Wireless PIM (Legacy)	PIM-SBB	250mA	7.5 to 14VDC

Example 1: One power supply is going to be used to power 4 Schlage VIP locks and 5 VBB-RIs:

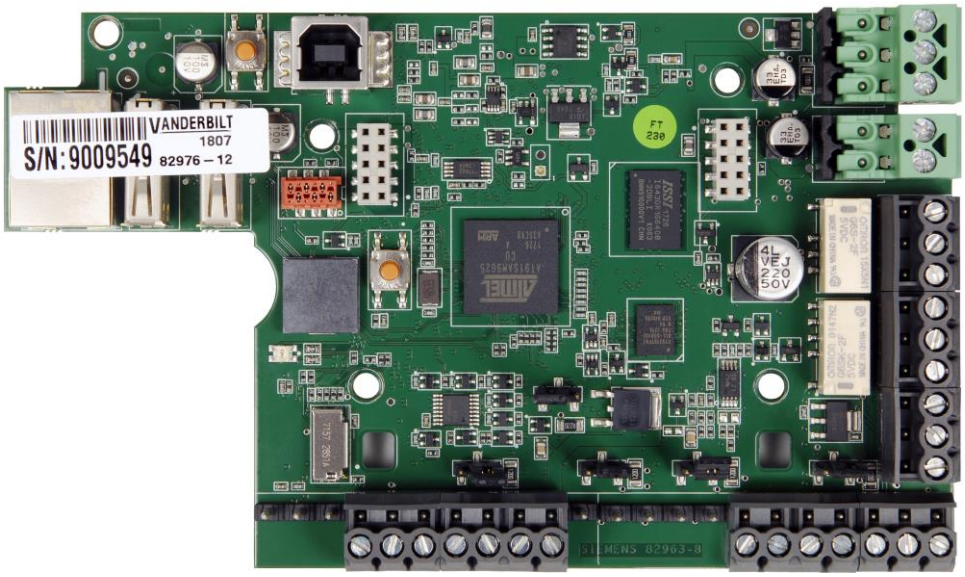
- VIP locks require 600mA @ 12 VDC and VBB-RIs require 300mA
- 600mA x 4 = 2400mA (for the VIPs)
- 300mA x 5 = 1500mA (for the VBB-RIs)
- Total is 2400mA + 1500mA = 3900mA
- 3900 mA = 3.9A
- A 5Amp power supply would be used in this situation.

Example 2: One power supply is going to be used to power 7 Schlage VIP locks, 2 VBB-RIs and **lite blue**:

- VIP locks require 600mA @ 12 VDC, VBB-RIs require 300mA, **lite blue** requires 250mA
- 600mA x 7 = 4200mA (for the VIPs)
- 300mA x 2 = 600mA (for the VBB-RIs)
- 250mA x 1 = 250mA (for **lite blue**)
- Total is 4200mA + 600mA + 250mA = 5050mA
- 5050 mA = 5.05A
- A 5Amp power supply is NOT recommended in this situation. A 10Amp power supply should be used to insure the system does not lose power.

lite blue

CHAPTER 1



Vanderbilt **lite blue** *Embedded Controller*

Overview

The **lite blue** system is based on the Vanderbilt AP02 controller and is equipped with 10 / 100 Base-T Ethernet connection with two RS-485 serial ports and two onboard reader interfaces capable of Wiegand or Magstripe input. It is a Linux application utilizing an atmel ARM926EJ-S 32-bit processor with 400MHz CPU clock, it also has 256 KB SRAM, 256MB NAND Flash and 128MB SDRAM. User access is via a network connection using any supported browser that allows a remote connection to manage the system. **lite blue** communicates with a series of devices such as the Vanderbilt VBB-RI, VBB-OBRI, VRI-1, VRI-2, VBB-NRI, Schlage AD-300, VIP, AD-400, NDE Wireless Locks and Wireless readers.

Highlights

- 8 card reader maximum configuration
  - 8 per RS-485 data channel maximum
  - 2 per onboard Wiegand channels maximum
- Lockable tamper proof enclosure
- 256MB NAND Flash and 128MB SDRAM with 5,000 ID capability
- Dynamically allocated memory
- 16 Gb memory Class 10, UHS I miniSD Card
- 10/100 Base-T Ethernet Connection
- Linux Kernel operating system

Dimensions

- **lite blue controller:** 151mm H x 201mm W x 53mm D
- **Enclosure:** 8-1/4" H x 7-1/2" W x 3-1/2" D
- **Power:** 12 / 24 VDC
- **Power Consumption:** 260mA maximum without Onboard Readers
- **Max. Device Output:** 12-24VDC @ 485mA
- **Ambient Temperature:** -40° to 55 °C
- **Humidity:** Humidity: 25° C @ 80% to 55° C @ 93% (III, IEC 60839-11-1)

Power Supply Requirements

- UL294 Listed Power-Limited Power Supply capable of 4 hours standby power providing 12VDC or 24VDC

Note: The LED on the cover of the VLB is a power indicator. However, it is not an AC indicator as the UL Listed power-limited power supply capable of 4 hour standby power could be providing the VLB with power even if AC power has been removed.

The **lite blue** controller is designed to only provide power the power supply to readers attached to the two onboard reader interfaces. Additional devices must be powered independently from the **lite blue** controller. If a single power supply is used, it must be large enough to power the **lite blue** controller and all attached devices. Make sure that the total power requirements for all devices does not exceed the output of the power supply(s) in use (see specific device chapters for power requirements). If not enough power is being supplied, the devices and the **lite blue** controller will not work correctly.

Power method 1 - Single Power Supply

Utilize a single UL Listed Power Limited power supply:

- Connect power cables from the power supply to TB1 GND and VIN in order to power **lite blue**
- Connect additional cables from the same power supply to the peripheral devices as needed

Power method 2 - Multiple Power Supplies

Utilize multiple UL Listed Power Limited power supplies:

- Connect one power supply to TB1 GND and VIN to power **lite blue**
- Connect additional power supplies to power peripheral devices as needed

Configuration Guidelines

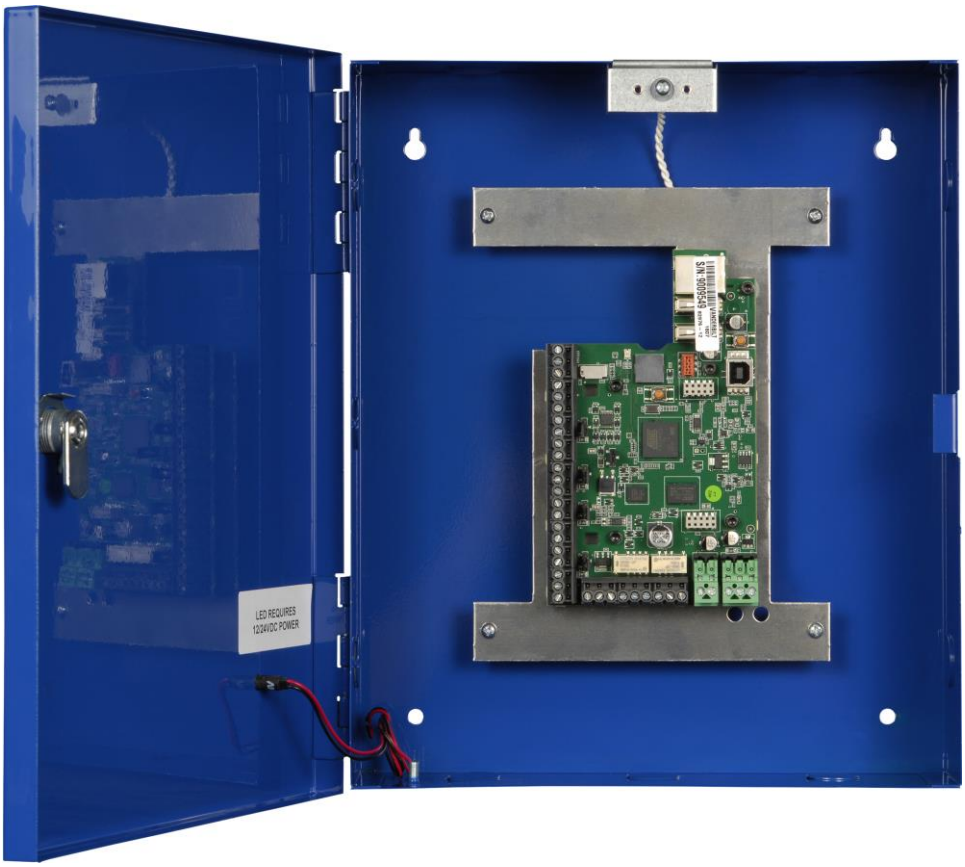
- The **lite blue** controller has 2 data channels to connect devices via an RS-485 communication protocol and 2 reader interfaces (Channel 0) supporting Wiegand or Magstripe reader heads. Each RS-485 data channel port can support up to 8 devices. A total of 8 devices for all channels can be connected to **lite blue**.
- **lite blue** on board reader interfaces will provide power to the connected reader devices. RS-485 devices must be powered independently.
- **lite blue** allows different types of RS-485 devices (VBB-RI, AD-300, VIP, AD-400 Wireless) to use the same data channel.
- The data connections for every device on the same channel must be properly connected in a daisy chain and then back to RS458-1 or RS485-2 TR+ and TR-.
- A UL Listed Power Limited, Power Supply capable of 4 hours standby power will be needed to provide power to the external devices.
- Please refer to power requirements for each device connecting to **lite blue**.
- Devices must be powered independently of **lite blue** with a local power source.

Installation and Configuration Steps

1. Mount **lite blue** controller to wall.
2. Connect all peripheral devices (VBB-RI, VBB-NRI, Wiegand Readers, AD-300, VIP, PIM or PIM-400). See specific device chapters for details.
3. Connect 12 VDC or 24VDC power supply to TB1 GND and VIN of the **lite blue** controller.
4. Connect power to all external devices independently as needed.
5. Turn on the power supply to **lite blue** and any additional power supplies.
6. Configure the **lite blue** IP address, date and time. See the **lite blue** IP Configuration and **lite blue** Date and Time setup section for details.

Enclosure Installation

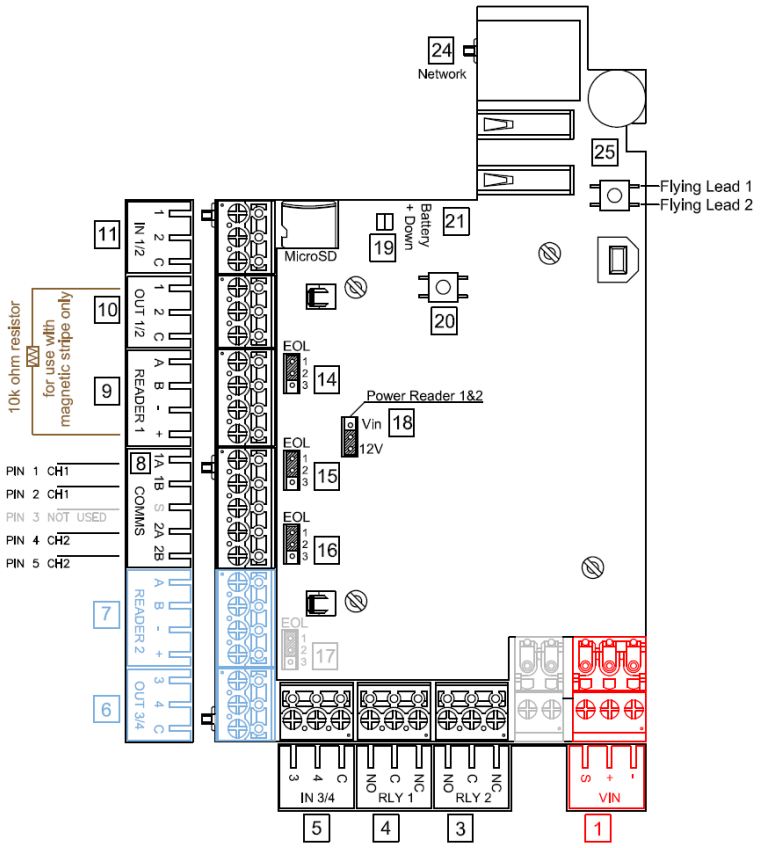
lite blue Enclosure - An enclosure with a hinged door and a lock is included with each **lite blue** system. The flying leads of the tamper switch should be attached to a UL Listed burglar alarm system or Listed local siren/annunciator. Do not connect the flying leads to the tamper switch on **lite blue**.



Features

- Metal enclosure with hinged door
- The enclosure is provided with a lock and key
- The enclosure is outfitted with a tamper switch
- Enclosure Dimensions: 12" x 10" x 2.75"

lite blue Pin Layout



lite blue Pin Functions

IMPORTANT WARNING

Incorrect wiring to the power connector [1] (VIN) will cause serious damage to the equipment.
Please check all wiring connections prior to turning the system on.

1 - POWER (VIN)

VIN	-	GROUND
VIN	+	VOLTAGE IN
VIN	S	SHIELD (CONNECT TO CHASSIS GROUND)

Power Requirements: 12-24VDC @ 560mA
Current Consumption: 260mA maximum without onboard readers connected. All connected devices must be UL Listed
Use a Class 2 power Limited UL294 Listed access control power supply
Use UL Listed and/or recognized wire suitable for the application

RESET

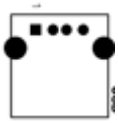
Press and Hold the AP02 controller Reset Button 20 until the short beeps begin and for nine (9) short beeps or less. The controller will shut down and reboot. The configured Network Settings (IP Address, etc.) will be retained on reboot

SHUTDOWN

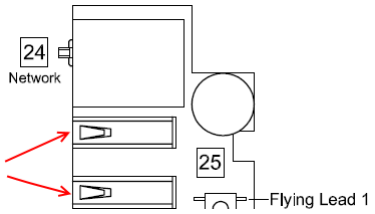
Press and Hold the AP02 controller Reset Button 20 until the short beeps begin and continue to hold until after 10 short beeps followed by 2 long beeps. The controller will power down. The configured Network Settings (IP Address, etc.) will be retained on restart. Disconnect and reconnect power to restart the controller

Functions On AP02 Controller

microSD card slot.



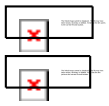
USB Ports (*reserved for future use*).



15 RS485 Termination (*default* = *Off*)

16 RS485 Termination (*default* = *Off*)

18 PASS 12V = Reader Power Select



12 V Available to Reader Ports (min 20 V in)

Input Power "Passed Through" to Reader Ports

Verify Manufacturer Specifications for Reader Head Voltage Maximum

25 **Tmp / Gnd** - Tamper. Connect to flying leads. Transaction when enclosure door is opened or closed.

24 **ETHERNET** - Ethernet cable to network connects here.

Onboard Reader Interfaces

See VBB-OBRI.

lite blue LED Indicators

The following AP02 controller onboard LED indicators are available for indicating the **lite blue** system status.

24 **Network States** *(software controlled)*

- Green: Communicating with host
- Orange: Acknowledgments

19 **Communications**

- Green: Outbound
- Red: Inbound
- Amber Flashing: lite blue

All Vanderbilt AP02 controller onboard LED indicators will be turned OFF once the **lite blue** system has been safely powered down.
Refer to **lite blue** PIN Functions above or the User Manual for proper Restart / Shutdown instructions.

lite blue IP Configuration

The IP address of **lite blue** has to be configured so that it can communicate with a web browser. Configuration should occur after the controller is fully installed. There are two methods to configure the IP address: Static IP and DHCP which are detailed below.

Static IP Configuration (Recommended)

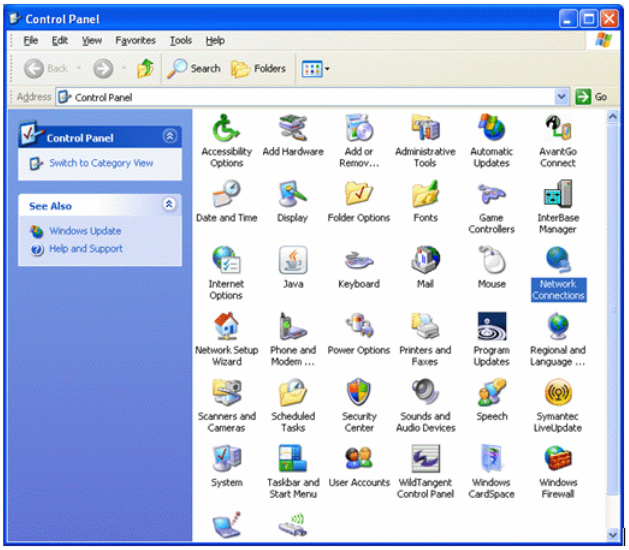
1 Connect a PC with a web browser to the **lite blue** controller.

- Direct Connection - Using a cross-over cable, the controller can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the controller can be connected to a hub or switch that is on the same network as the PC.

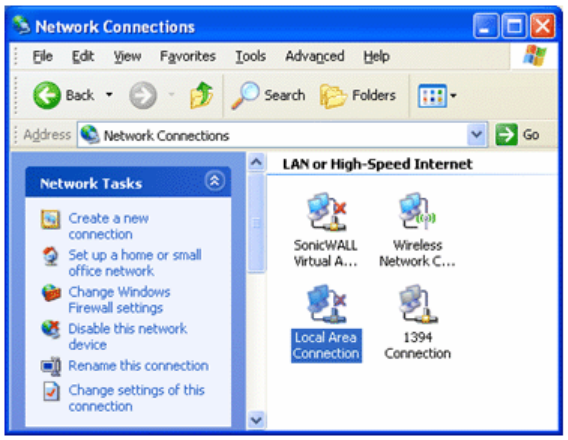
2 Configure the PC's network settings to communicate with **lite blue**.

a) Click on the **Start** button.

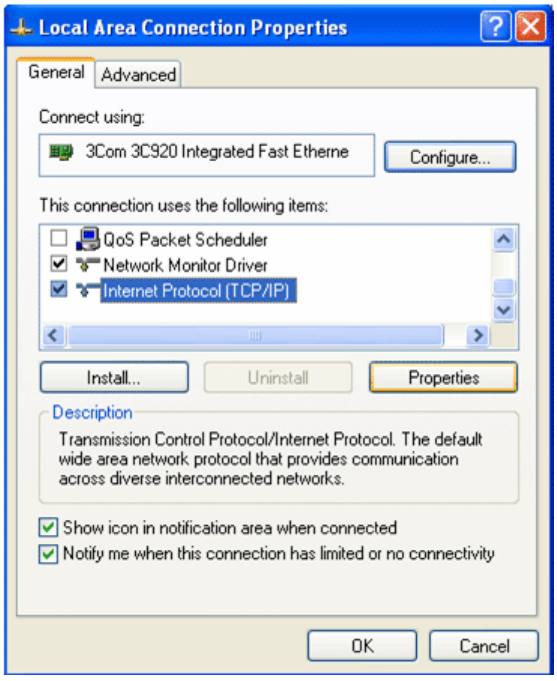
b) Click on **Control Panel**. The Control Panel window will open.



c) Click on **Network Connections**. The Network Connections window will open.



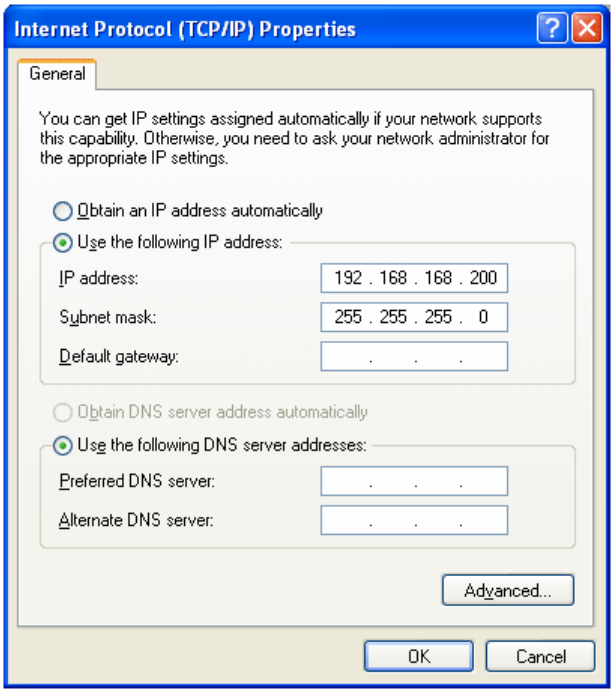
d) Click on **Local Area Connection**. The Local Area Connection Properties window will open.



e) Scroll down and select **Internet Protocol (TCP/IP)**.

f) Click the **Properties** button. The Internet Protocol (TCP/IP) Properties window will open.

g) Make a note of the existing settings. These will need to be restored at the end of the lite blue configuration process to return the PC to its usual settings.



h) Click on the **Use the following IP address** button.

i) Enter 192.168.168.200 into the **IP address** field.

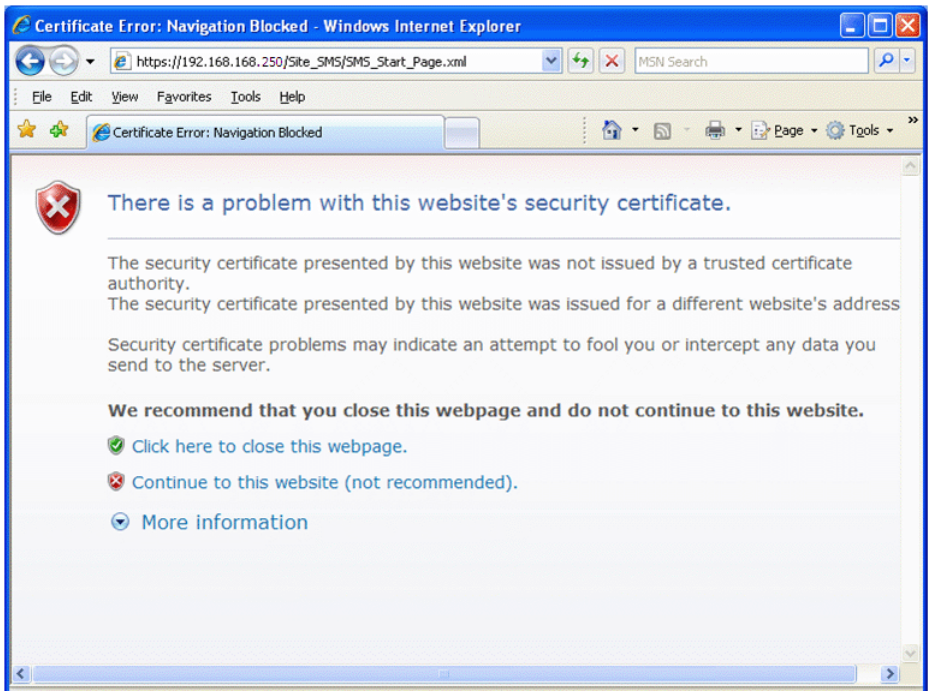
j) Enter 255.255.255.0 into the **Subnet mask** field.

k) Click on the **OK** button. The window will close. The PC's network settings are now compatible with lite blue.

3 Open a web browser.

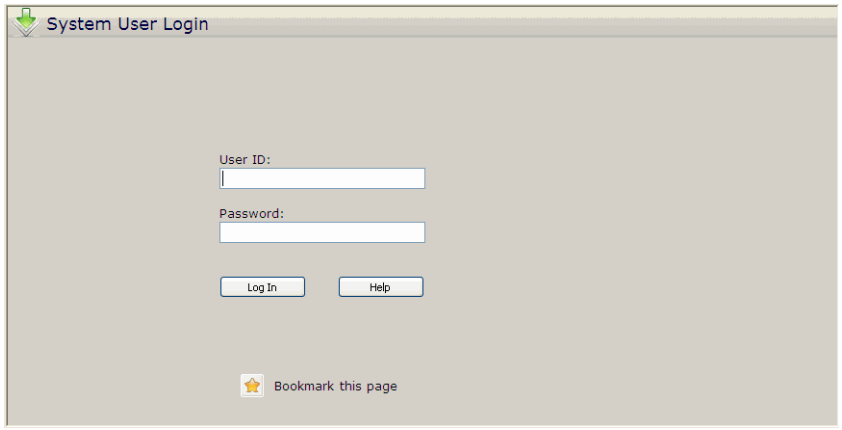
4 Go to http://192.168.168.250

a) If dip switch 1 of S1 on the lite blue controller is in the "ON" position this window will open:



b) This message is not an error and should be bypassed. Click on **Continue to this website (not recommended)**.

c) The **lite blue** home page will open. Wait a moment for it to redirect to the log in screen.



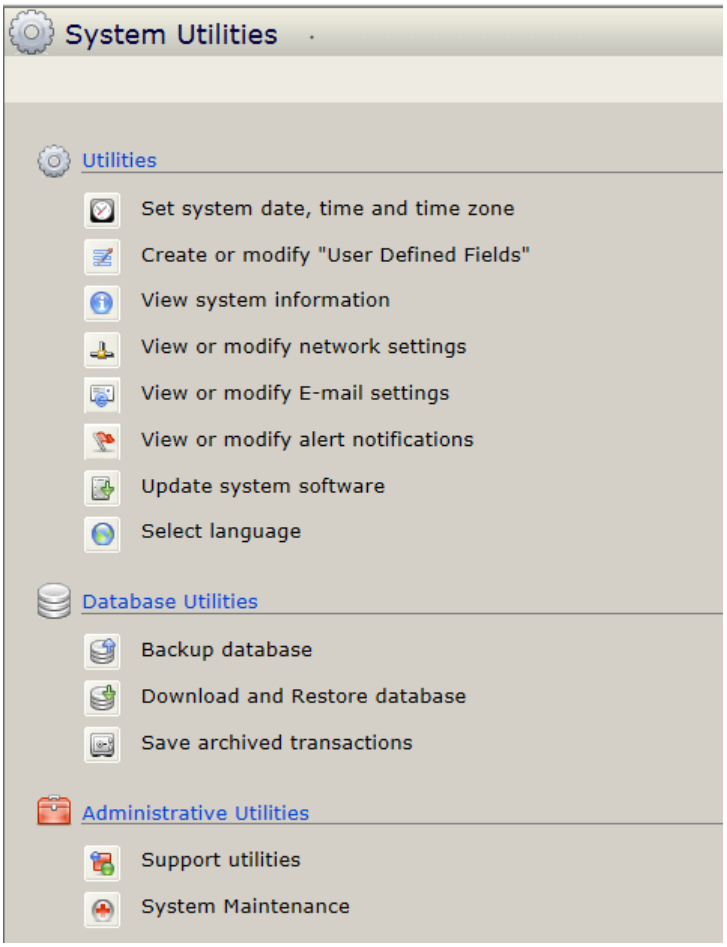
5 Log in.

a) Enter User ID. Default User ID is usr.

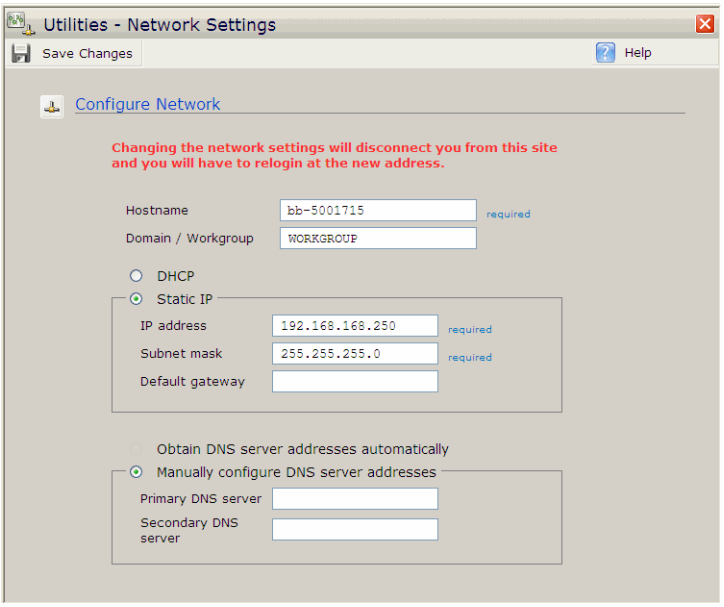
b) Enter Password. The default password is "password".

c) Click on the **Log In** button. The **lite blue** main window will open.

6 Click on the **Utilities** button on the left side of the screen. The System Utilities window will open.



7 Click on the **View or modify network settings button**. The Network Settings window will open.



8 Click on the **Static IP** button.

a) Enter new IP address into the IP address field. Consult with network technicians to get an address that is compatible with the existing network.

b) Enter new Subnet mask into the Subnet mask field. Consult with network technicians to get an address that is compatible with the existing network.

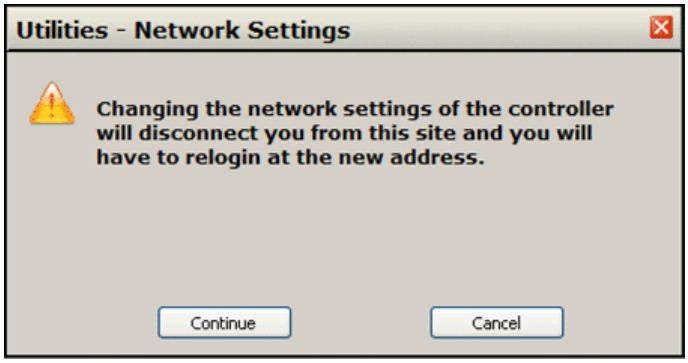
c) Enter new Default gateway into the Default gateway field. Consult with network technicians to get an address that is compatible with the existing network.

9 Click on the **Manually configure DNS server addresses** button.

a) Enter a primary DNS server address into the Primary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

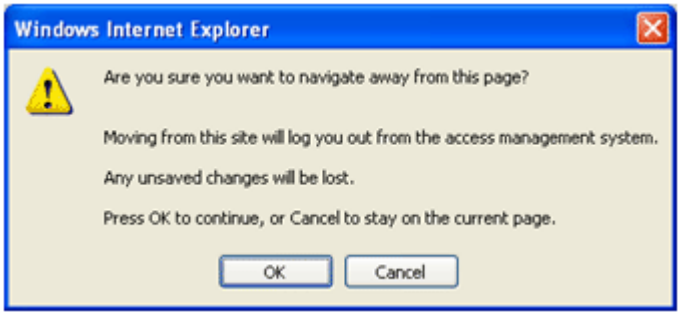
b) Enter a Secondary DNS server into the Secondary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

10 Click on the **Save Changes** button. The Utilities - Network Settings pop-up window will open.



11 Click on the **Continue** button. The connection to **lite blue** will be lost as the network settings are updated.

12 Close the browser window. A pop-up window will open.



13 Click on the **OK** button. The pop-up and the browser window will close.

14 Restore the network settings on the PC (follow step 2 above to access the network settings of the PC).

15 Open a web browser.

16 Enter http:// followed by the new IP address into the browser. The **lite blue** home page will open and **lite blue**'s IP address is successfully configured.

DHCP Configuration

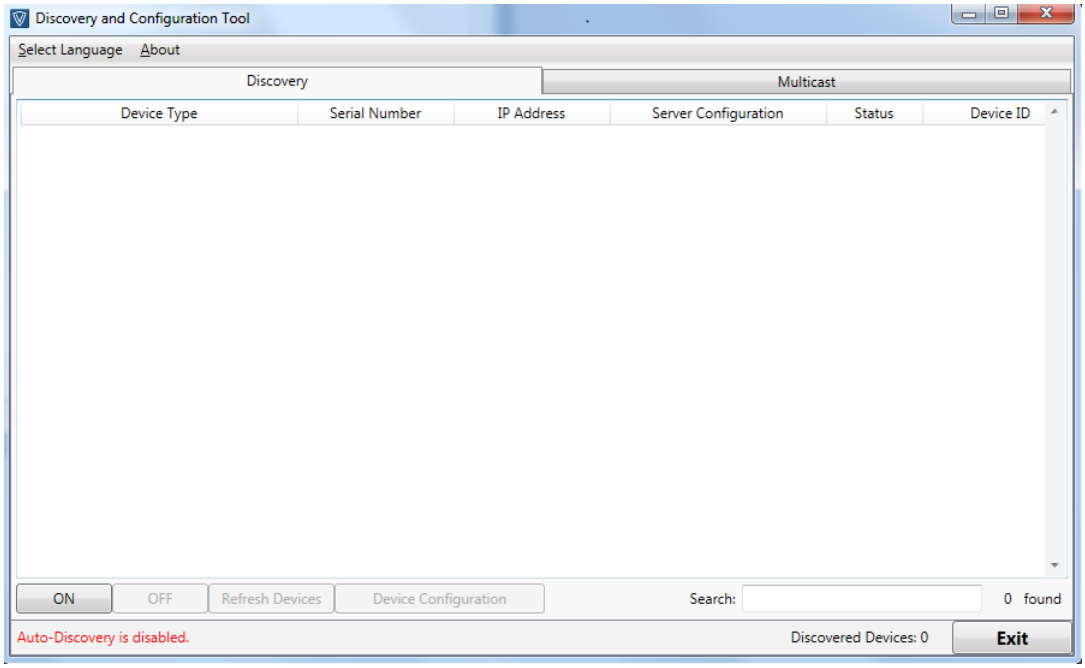
Configuring the **lite blue** controller to DHCP requires the Discovery and Configuration program. This program is located on the CD that is included with **lite blue**.

To configure the **lite blue** controller with the Discovery and Configuration tool:

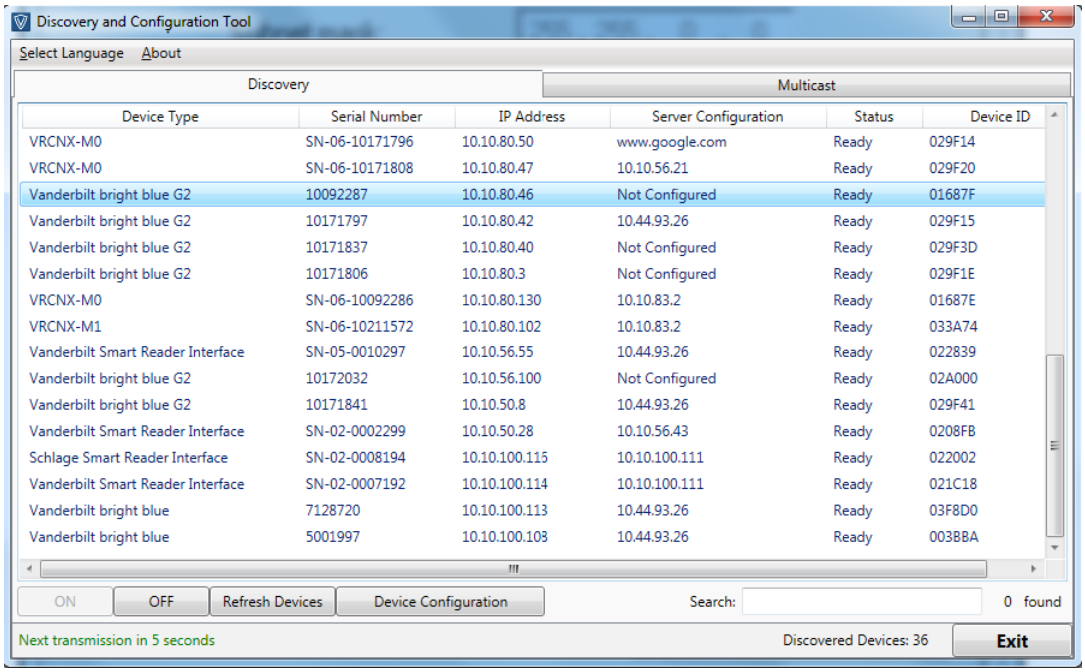
1 Connect the PC running the Discovery and Configuration tool to the **lite blue** controller.

- Direct Connection - Using a cross-over cable, the controller can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the controller can be connected to a hub or switch that is on the same network as the PC.

2 Run the Discovery and Configuration tool.



3 Click on the **On** button to search for **lite blue** controllers.

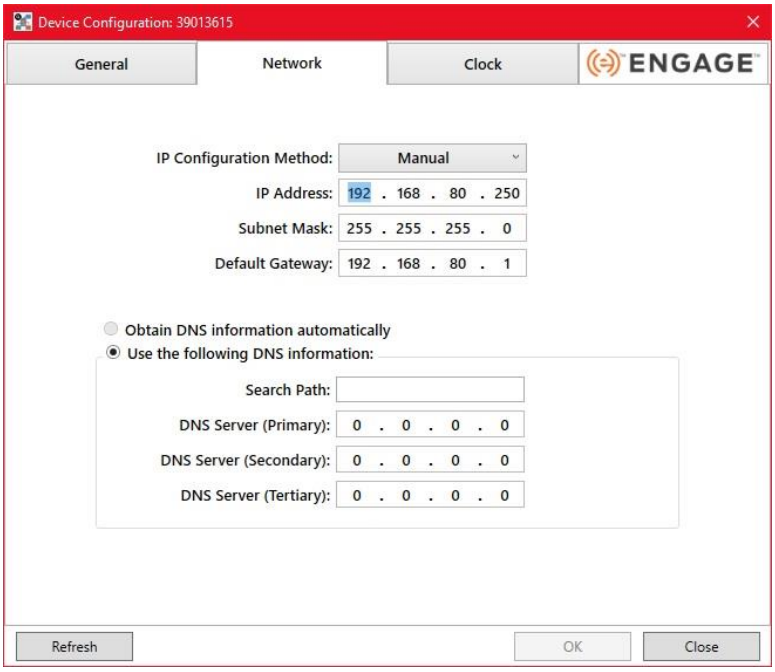


4 Edit the default values.

a) Select which controller to configure.

b) Click on the **Device Configuration** button. The Device Configuration window will open.

c) Click on the **Network** tab.



d) Using the drop-down box, change the IP configuration method to DHCP.

e) Click on the **OK** button to apply the change.

f) Make a note of the IP Address. Enter the IP address into a web browser to connect to the **lite blue** software. It may take a few seconds for the new IP address to be generated.

5 Exit the Discovery and Configuration program.

Note: DHCP is not recommended for **lite blue**. If the dynamic IP address is changed then the Discovery and Configuration tool will need to be run to find the new IP address and any bookmarks for **lite blue** will be invalidated. Static IP is recommended for **lite blue**.

lite blue Date and Time Setup

The date and time for **lite blue** has to be set up for the system to work properly. The date and time can be entered in two ways: 1) Through the **lite blue** software. 2) Using the Discovery and Configuration Tool as described below.

Using the lite blue software to set date and time

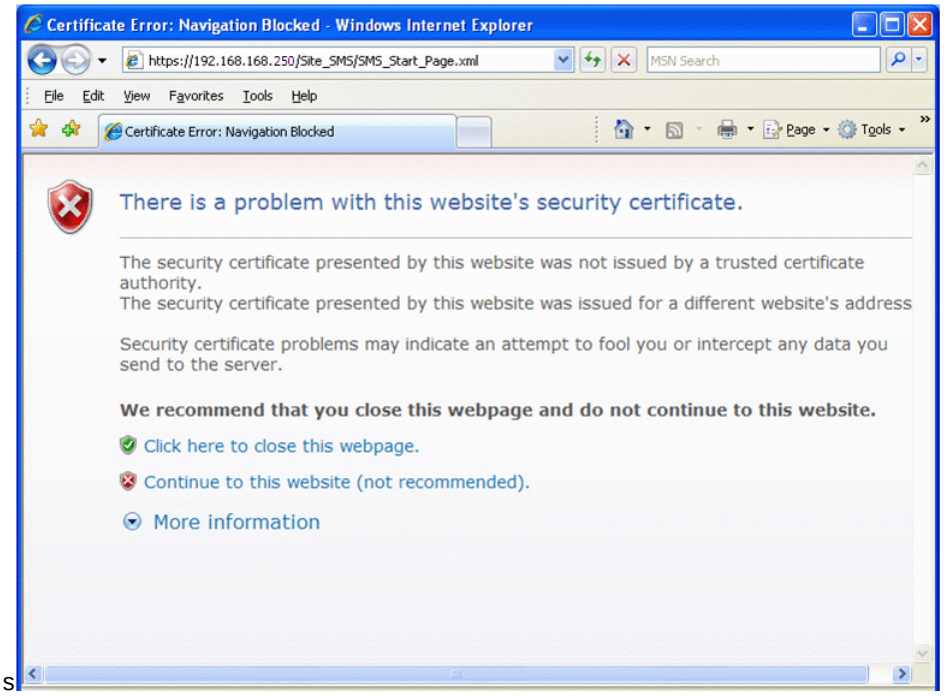
1 Connect a PC with a web browser to the **lite blue** controller.

- Direct Connection - Using a cross-over cable, the controller can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the controller can be connected to a hub or switch that is on the same network as the PC.

2 Open a web browser.

3 Enter the IP address of the **lite blue** controller into the web browser, see the **lite blue IP Configuration** chapter for details.

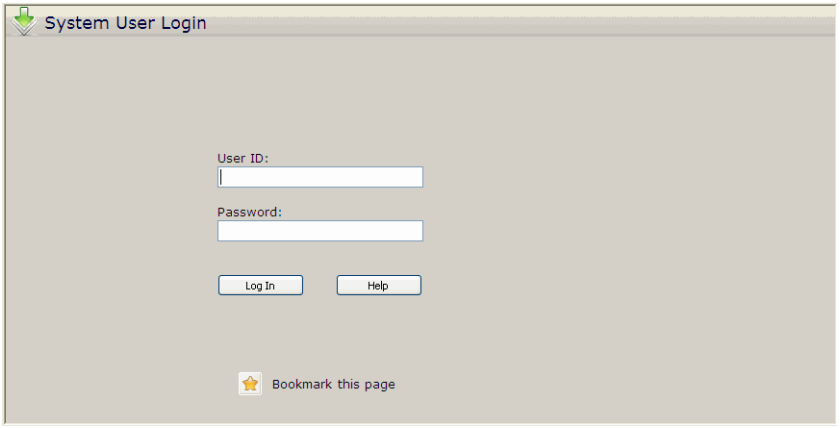
a) If dip switch 1 of S1 on the lite blue controller is in the "ON" position then this window will open:



s

b) This message is not an error and should be bypassed. Click on **Continue to this website (not recommended)**.

c) The **lite blue** home page will open. Wait a moment for it to redirect to the log in screen.



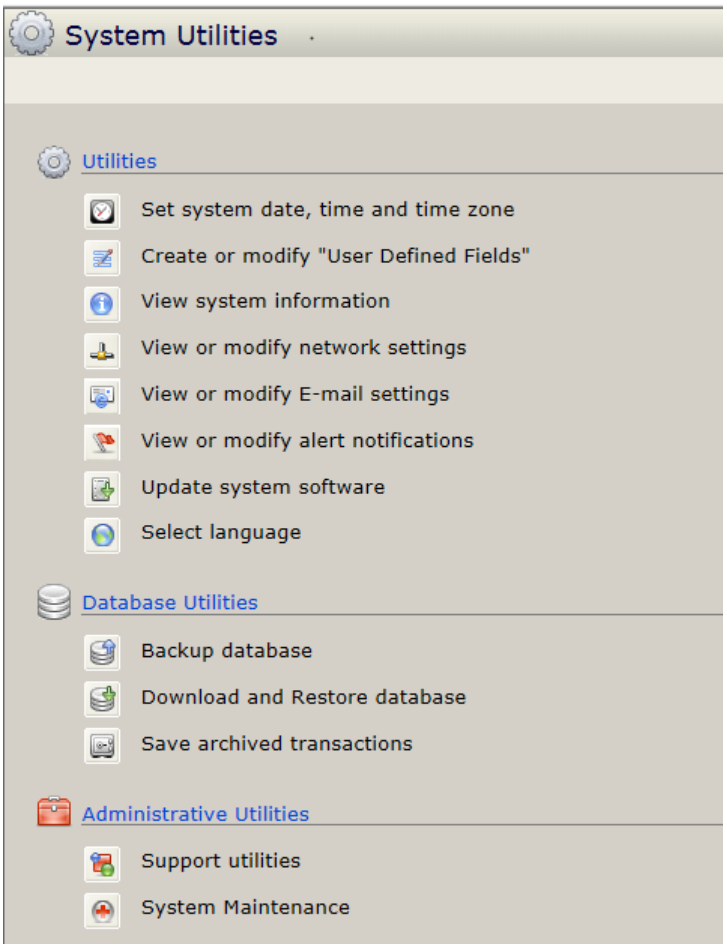
4 Log in.

a) Enter User ID. Default User ID is usr

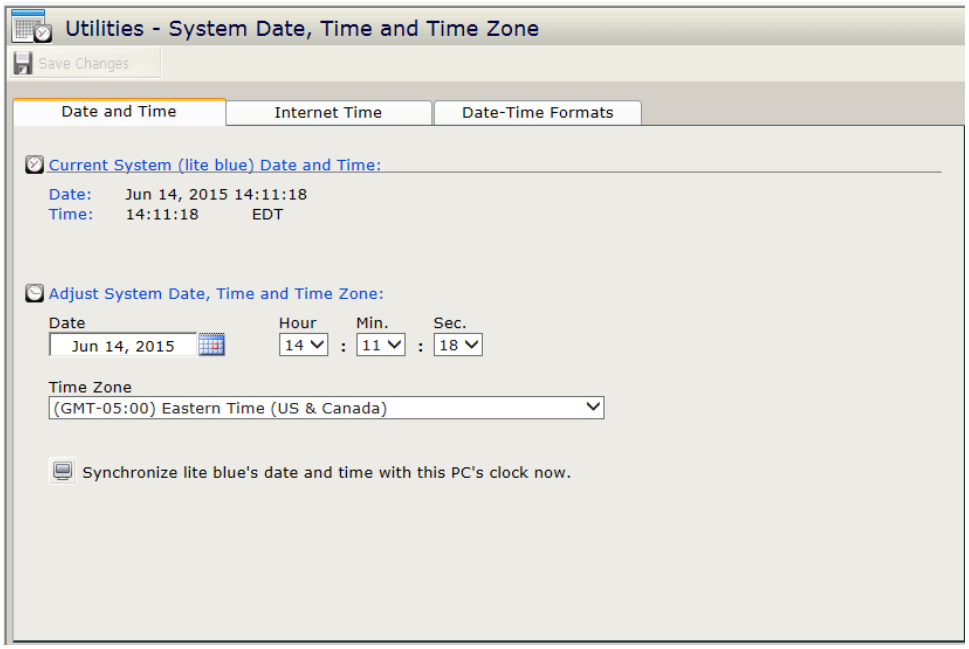
b) Enter Password. Default Password is password

c) Click on the **Log In** button. The **lite blue** main window will open.

5 Click on the **Utilities** button on the left of the main screen. The System Utilities window will open.



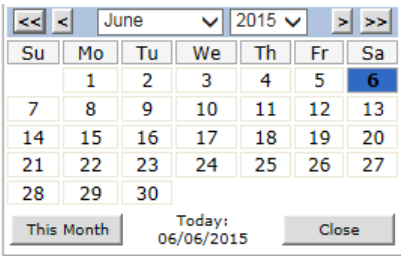
6 Click on the **Set system date, time and time zone** button. The Utilities - System Date, Time, and Time Zone window will open.



7 Set the date, time, and time zone:

a) Using the **Time** drop down boxes, specify the time.

b) Click on the calendar button to the right of the **Date** field. The calendar pop-up will open.



c) Select the date. The calendar pop-up will close.

d) Select the time zone from the **Regional Time Zone** list.

e) **Optional**: Instead of setting the time and date manually the **Sync time with local PC** button can be used. Select the time zone from the **Regional Time Zone** list and click **Save Changes**. Then click on the **Sync time with local PC** button and the date and time will be synchronized with that of the PC.

Note: The regional time zone is set to Eastern Time by default.

8 Click on the **Apply** button. The system time, date, and time zone will be updated.

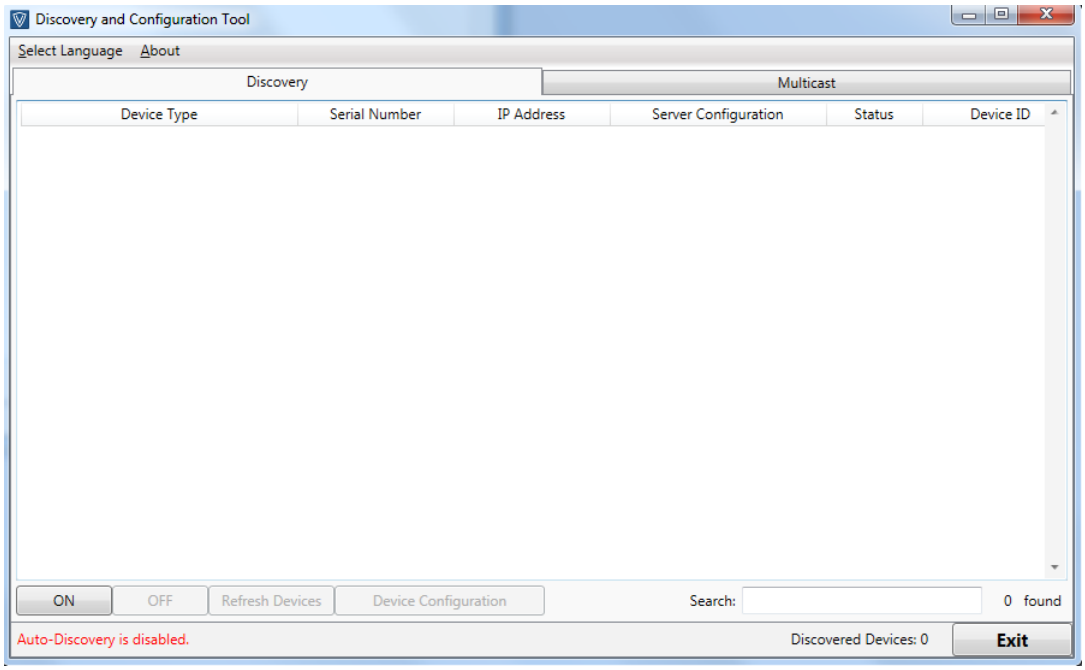
Using the Discovery and Configuration Tool to set date and time

1 Connect the PC running the Discovery and Configuration tool to the **lite blue** controller.

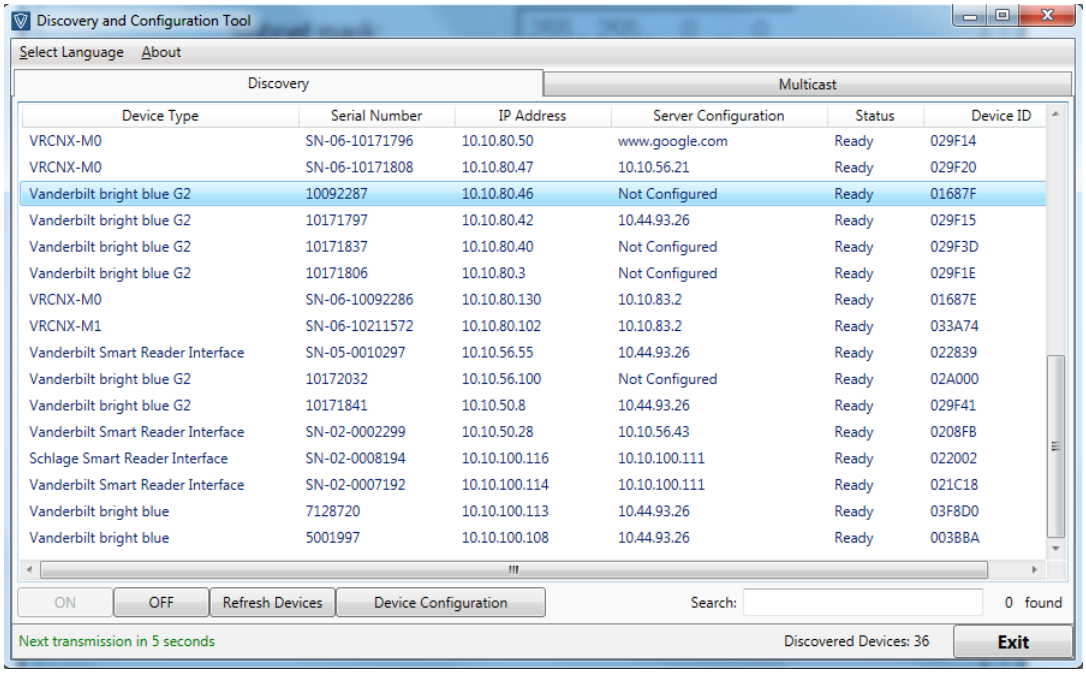
- Direct Connection - Using a cross-over cable, the controller can be connected directly to the network card of the PC.

- Network Connection - Using a regular network cable, the controller can be connected to a hub or switch that is on the same network as the PC.

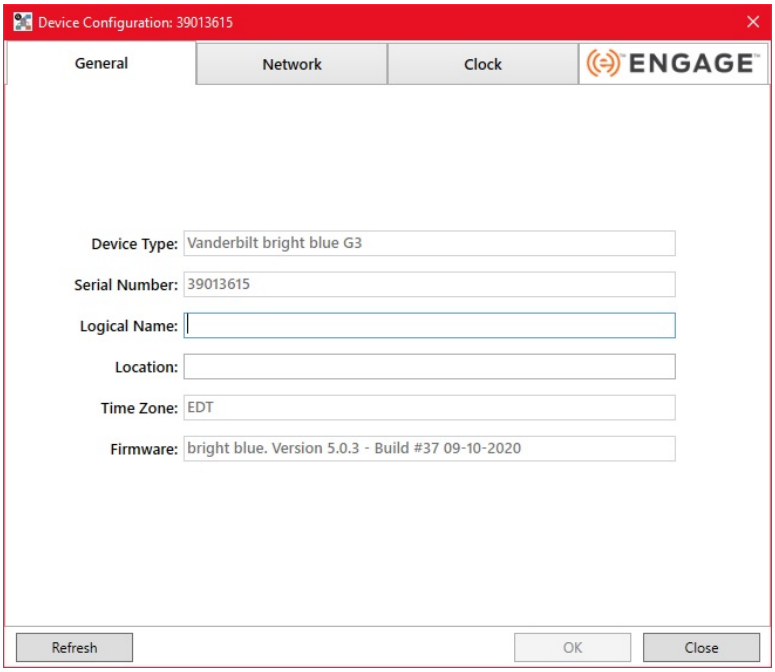
2 Run the Discovery and Configuration tool.



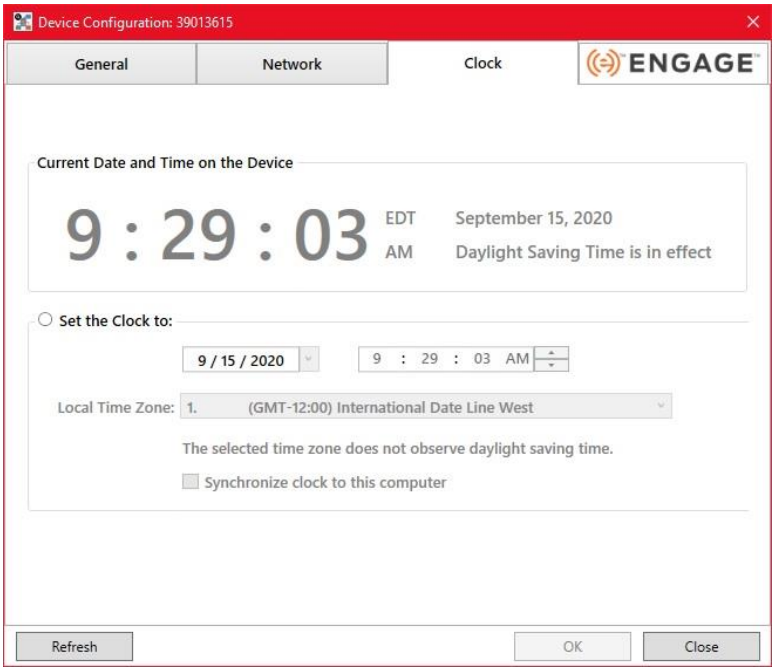
3 Click on the **On** button to search for **lite blue** controllers.



4 Select the **lite blue** controller and click on the **Device Configuration** button. The Device Configuration window will open.



5 Click on the Clock tab.



6 Click on the Set the Clock To button.

7 Click on the Synchronize clock to this computer check box to select it.

8 Click OK to synchronize **lite blue** with the PC clock.

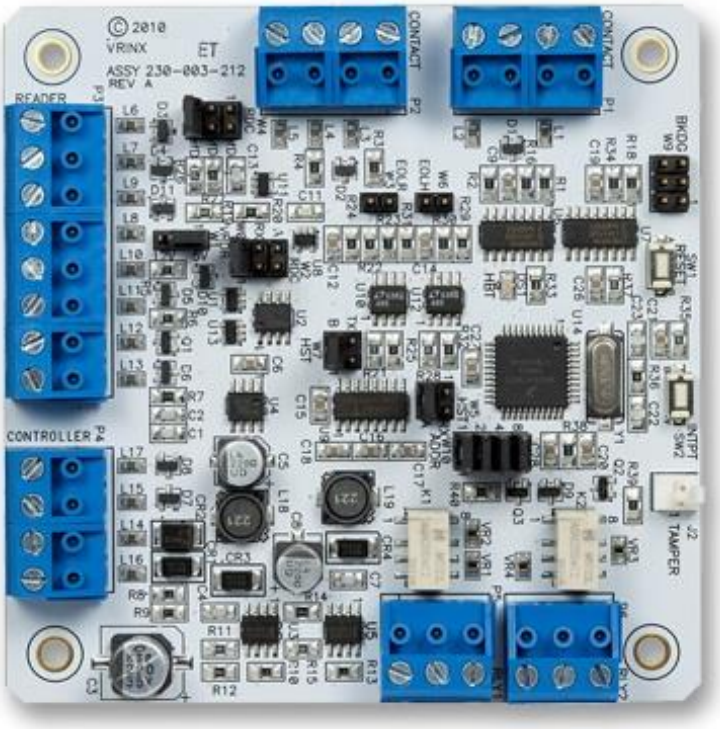
9 Close the Discovery and Configuration Tool.

Battery Replacement

The **lite blue** controller uses a UL Listed CR2032 or equivalent 3V Lithium Coin Cell battery. The battery should be replaced every year by a trained technician. Battery can be replaced **without** powering down controller.

VBB-RI

CHAPTER 2



Reader Interface

Overview

The VBB-RI is a Reader Interface between **lite blue** and card readers. The VBB-RI offers a cost-effective, modular approach to access control system design. Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)
  - HID Corporate 1000 48-bit (not evaluated by UL)
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Communicates via RS-485 protocol
- Powered directly from **lite blue**
- **OPTIONAL -** can be powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.

Features

- Supports one read-head credential
- Connects directly to the communication channels on the **lite blue** controller via RS-485 protocol
- Includes Two 2 amp, form C, single pole/double throw, mechanically latching relay
- Connection for one multi-color LED for access granted or access denied indication
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc.

Specifications

- Board Dimensions - 3-13/16” x 3-13/16” x 3/4” D
- Enclosure Dimensions - 8-1/4”H x 7-1/2W” x 3-1/2” D
- Power requirements - 14 to 24 VDC (usually supplied by **lite blue** Controller)
- Power consumption - 300mA max. (with reader)
- Ambient temperature - 0º to 49º C or 32º to 120º F

VBB-RI Enclosure

VBB-RI Enclosure - An enclosure with a hinged door is included for each VBB-RI. The flying leads of the tamper switch should be attached to a UL Listed burglar alarm system or Listed local siren/annunicator.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8.25” x 7.5” x 3.5”

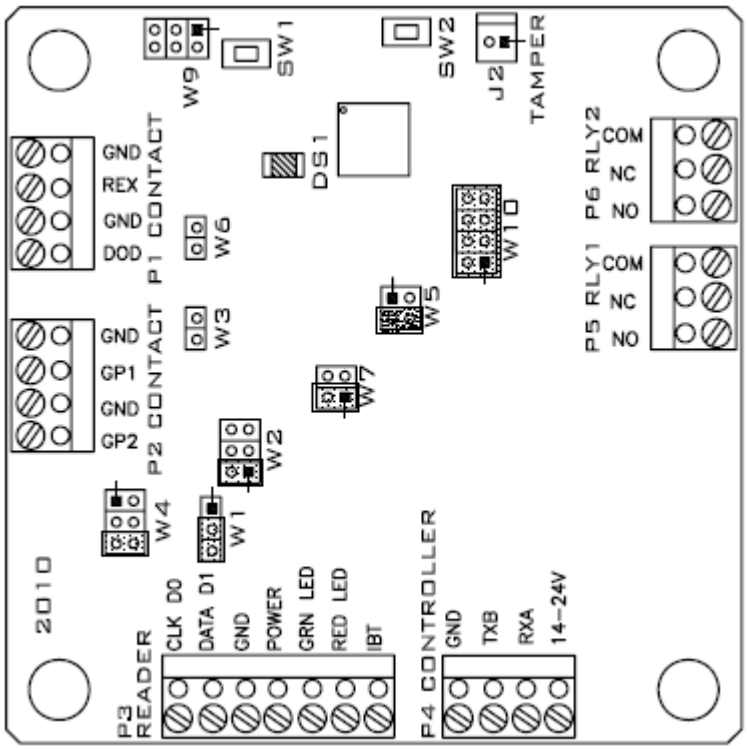
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting the enclosure

- Field Wiring - It is recommended that you drill holes or punch the knockouts in the metal enclosure for field wiring before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4” x 1” lag bolts.
- To secure the VBB-RI enclosure use two screws through the openings provided on the cover. Alternately a lock can be added using the provided punch out section on the cover.

VBB-RI Pin Layout



VBB-RI Pin Functions

P4 - Power source and communication wiring. Used to connect **lite blue** to the VBB-RI.

- Pin 1 is Ground (GND)
- Pin 2 is Data B (TXB)
- Pin 3 is Data A (RXA)
- Pin 4 is Power (14-24V)

P1/P2 - The VBB-RI has four contact points, two at P1 and two at P2. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

P5/P6 - Relay outputs. The VBB-RI comes with two relay outputs. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. P5 is for the Door Held Open relay. P6 is for the door unlock relay.

W1 - Read head voltage selector. The read-head voltage selector provides 5VDC or 12VDC to the various types of read-heads.

- No jumper will provide no power
- A jumper across Pins 1 and 2 will also provide 5VDC
- A jumper across Pins 2 and 3 will provide 12VDC

Note: Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read-head voltage requirements.

W10 - VBB-RI Reader Interface Addressing. The address of the VBB-RI is dependent on the position of jumpers on these pins. Please see the section on Addressing VBB-RI for more details.

J2 - On Board Tamper Connection. The enclosure tamper switch will be wired to the supplied tamper connector flying leads. Polarity is not a concern.

DS1 - LED Description.

- Slow Blink -- Power, but no data communication
- Fast Blink -- Power and data communication

SW1 - Hardware Reset Switch. The Reset Switch clears all the memory on the VBB-RI. Press the reset switch for 3 seconds to clear the memory.

SW2 - Software Reset Switch. Recommended for factory use only.

Note: Make sure that there is power on VBB-RI (P4)

Warning: Do not press switch unless instructed by the factory representative.

Pins Left at Default

The below Pins/Jumpers should be left at their default settings:

- W2 - Determines the configuration of the second pin (RXAW1) at P3.
  Default: Jumper on pins 1&2

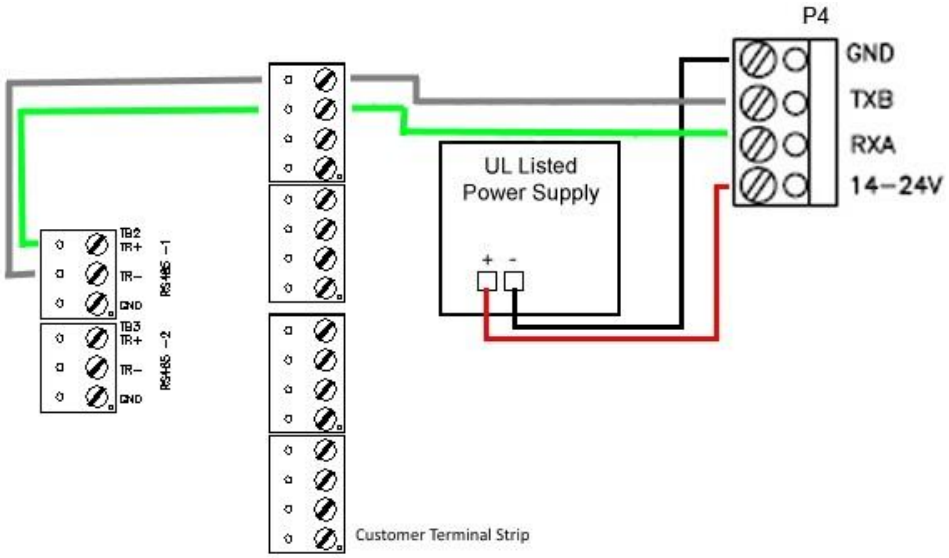
- W3 - P3 Pin1/Pin2 RS485 Communication Line Terminator.
  Default: No Jumper
- W4 - Determines the configuration of the first pin (TXBW0) at P3.
  Default: Jumper on pins 5&6
- W5 - Determines the configuration of the third pin (RXA) at P4.
  Default: Jumper on pins 3&4
- W6 - P4 Pin2/Pin3 RS485 Communication Line Terminator.
- Default: No Jumper
- W7 - Determines the configuration of the second pin (TXB) at P4.
  Default: Jumper on pins 1&2

Pins Not Used

W9 - BKDG: No jumper required for normal operation.

Connecting to lite blue

Data communication between the **lite blue** controller and a VBB-RI reader interface is via RS-485 protocol. Either RS-485 channel on the **lite blue** controller can be used to communicate with P4 on a VBB-RI. The below example is using RS485-1 on the **lite blue** controller and P4 on the VBB-RI.



Data Communication between lite blue and VBB-RI

lite blue	VBB-RI	Power Supply
RS-485-1 TR+	Pin 3 - RXA (Data A)	
RS-485-1 TR-	Pin 2 - TXB (Data B)	
	Pin 4 - PWR (Power)	+ (Power)
	Pin 1 - GND (Ground)	- (Ground)

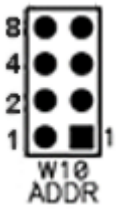
Powering the VBB-RI

The VBB-RI should receive power directly from a UL 294 Listed Power Limited power supply. Power will be supplied independently from the **lite blue** controller.

Addressing the VBB-RI

W10 on the VBB-RI consists of four jumpers that can be combined to set the address for the device. Each VBB-RI on a **lite blue** controller RS-485 data channel must have a unique address (1 – 8).

Make a note of the address of the VBB-RI and which channel it is connected to. This information will be required to set up the lock in the software.



VBB-RI Address Chart

VBB-RI Address	Jumper Locations
1	1 2 4 8
2	2 4 8
3	1 4 8
4	4 8
5	1 2 8
6	2 8
7	1 8
8	8

Connecting to Read Head

The VBB-RI reader interface can communicate to many different read heads. Provided here are the pin outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

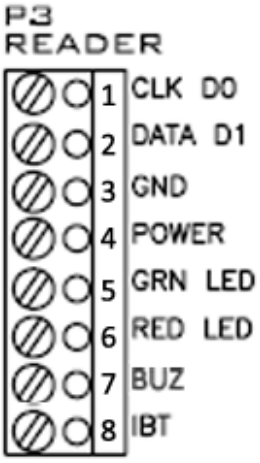
Recommended Wire Chart: VBB-RI to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VBB-RI to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VBB-RI to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VBB-RI to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VBB-RI to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

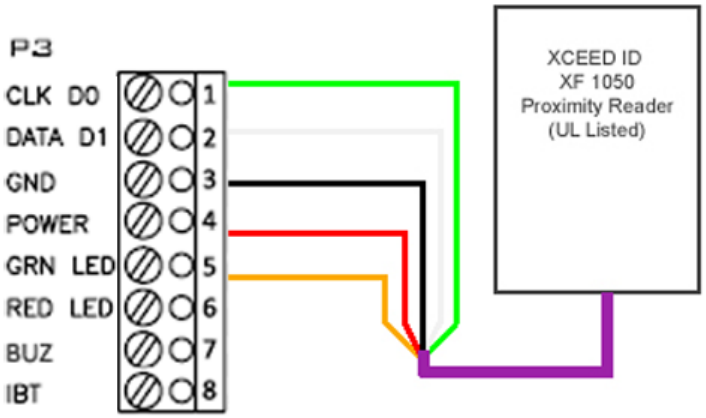
Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

P3 - VBB-RI Pin Connections



XCEED ID XF 1050 Proximity Reader



Proximity Read Head Pin Connections

VBB-RI	Proximity Reader
PIN 1 (CLK)	DATA 0 (GREEN)
Pin 2 (DAT)	DATA 1 (WHITE)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED
Pin 7 (BUZ)	NOT USED
Pin 8 (IBT)	NOT USED

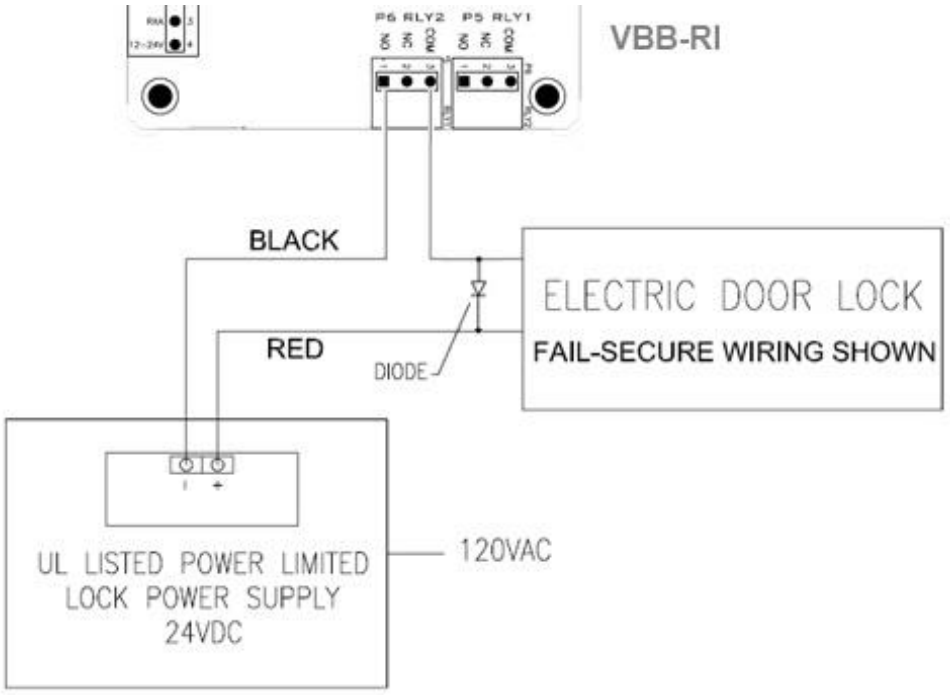
Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VBB-RI	Magnetic Stripe Reader
PIN 1 (CLK)	DATA 0 (WHITE)
Pin 2 (DAT)	DATA 1 (GREEN)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED
Pin 7 (BUZ)	NOT USED
Pin 8 (IBT)	NOT USED

Installing Diode for Lock Wiring - Relay

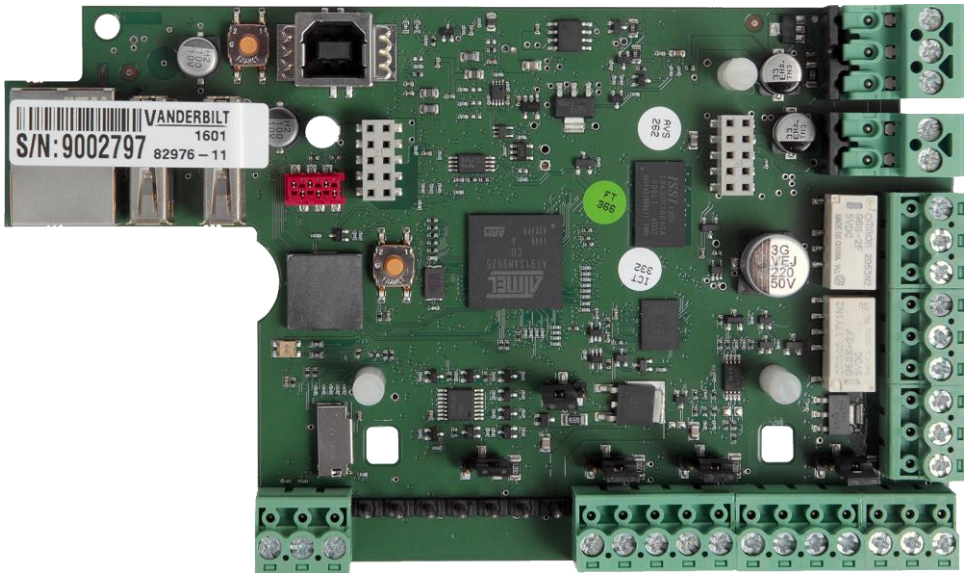
A diode is supplied with the VBB-RI which should be fitted across 12V and COM to protect the relay contacts.



The lock is wired across 12V and COM. A 0V link to COM is then required to complete the circuit. This will be wired to NO or NC depending on lock type: Fail Open / Fail Closed (diagram above shows Fail Open).

VBB-OBRI

CHAPTER 3



Onboard Reader Interface

Overview

The VBB-OBRI is an onboard Reader Interface between **lite blue** and card readers. These 2 included Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)
  - HID Corporate 1000 48-bit (not evaluated by UL)
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Embedded directly on **lite blue** Vanderbilt AP02 Controller
- Powered directly from **lite blue**

Features

- Supports one read-head attached to each reader interface
- Mounted directly on the **lite blue** Vanderbilt AP02 Controller
- Includes Two 2 amp, form C, single pole/double throw, mechanically latching relays **total**
- Connection for one multi-color LED for access granted or access denied indication
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc. **total**

Specifications

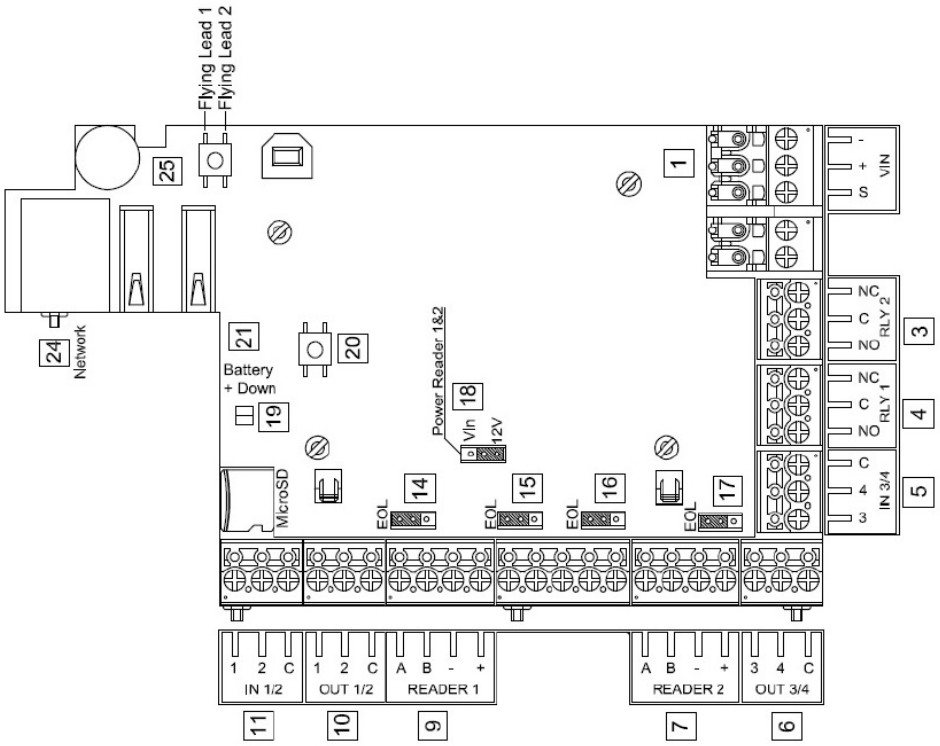
- Power requirements: supplied by **lite blue** Controller
- Power consumption: 485mA @ 12 – 24 VDC, 260 mA Max without Onboard Readers
- Ambient temperature: -40º to 55º C

VBB-OBRI Supports 2 Configurations:

VBB-OBRI Single Reader Interface = 4 Contacts and 2 Relays / Reader (Max 1 Door)
VBB-OBRI Dual Reader Interface = 2 Contacts and 1 Relay / Reader (Max 2 Doors)

See VBB-OBRI PIN Functions Below

PIN Layout



Onboard Reader Interface Connections:

- *Reader 1 (OUT1, IN1, IN2) or alternately (OUT1, OUT2, IN1, IN2, IN3 IN4)*
- *Reader 2 (OUT2, IN3, IN4) or alternately **not used***

PIN Functions

1 Power / VIN

- + is Power
- - is Ground
- S is Chassis Ground

4 Relay 1 – Max 30 VDC @ 2 A

- NC is Normally Closed
- C is Common
- NO is Normally Open

3 Relay 2 – Max 30 VDC @ 2 A

- NC is Normally Closed
- C is Common
- NO is Normally Open

The VBB-OBRI has four unsupervised contact points.
Unsupervised door contacts have maximum wire length of 2,000 feet.

6 Contact Inputs 1 & 2

- 1 – N/O
- 2 – N/C
- C is Ground

5 Contact Inputs 3 & 4

- 3 – N/O
- 4 – N/C
- C is Ground

9 & 10 Read Head 1 Connection

- 1 is LED
- 2 is Not Used
- C is Not Used
- A is CLK (Data 0)
- B is DAT (Data 1)
- - is Ground
- + is Power

6 & 7 Read Head 2 Connection

- 3 is LED
- 4 is Not Used
- C is Not Used
- A is CLK (Data 0)
- B is DAT (Data 1)
- - is Ground
- + is Power

14 Not Used

15 Not Used

16 Not Used

17 Not Used

18 Read Head Voltage Selector. The VBB-OBRI A read head voltage selector provides wither 12 VDC or passes VIN to the read head depending on jumper location.

- A jumper across PINs 2 and 3 (12V) will provide 12 VDC (default setting)
- A jumper across PINs 1 (Vin) and 2 will pass VIN
- No jumper will provide 0 VDC

Warning: Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read head voltage requirements.

24 lite blue Network Connection

Reader and I/O Assignment

The VBB-OBRI Supports 2 Door Configurations:

- Single Door Control (2 Relays and 4 Contacts per door)
- Dual Independent Door Control (1 Relay and 2 Contacts per door)

VBB-OBRI Reader Inputs and I/O is associated to one of the configurations above depending on the Reader Template applied in Door Setup as indicated below.

Device Selection	Reader Used	Relay Assignment	Contacts Assignment
Single Door Control			
VBB-OBRI Single Reader Interface	Reader 1	Relay 1 Relay 2	Contact 1 – REX Contact 2 – DOD Contact 3 – Push Button Contact 4 – Aux Input
	Reader 2 Unused		
Dual Independent Door Control			
VBB-OBRI Dual Reader Interface	Reader 1	Relay 1	Contact 1 – REX Contact 2 – DOD
	Reader 2	Relay 2	Contact 3 – REX Contact 4 – DOD

Connecting to lite blue

The VBB-OBRI are mounted onboard the VBB Vanderbilt AP02 Controller. No additional connection to **lite blue** is required.

Addressing

The two VBB-OBRI readers are addressed using the lite blue software. Please refer to the lite blue User Manual under Door Setup.

Connecting to Read Head

The VBB-OBRI reader interface can communicate to many different read heads. Provided here are the pin outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

Recommended Wire Chart

Connection	Maximum Distance (ft)	Cable Recommendation
VBB-OBRI to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VBB-OBRI to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VBB-OBRI to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VBB-OBRI to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

PIN Connections

Reader 1 Shown for Example

Proximity Reader

Proximity Read Head Pin Connections

VSRC-A	Proximity Reader
9 PIN A (CLK)	DATA 0 (GREEN)
9 PIN B (DAT)	DATA 1 (WHITE)
9 PIN - (GND)	GROUND (BLACK)
9 PIN + (GND)	POWER (RED)
10 PIN 1 (LED)	LED (ORANGE)
10 PIN 2 (NA)	NOT USED
10 PIN C (NA)	NOT USED

Magnetic Stripe Reader

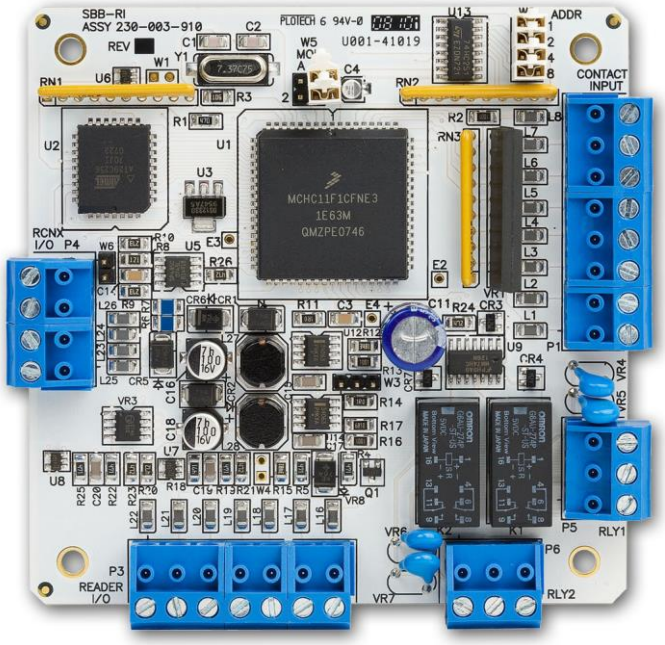
Magnetic Stripe Read Head Pin Connections

VSRC-A	Magnetic Stripe Reader
9 PIN A (CLK)	DATA 0 (WHITE)
9 PIN B (DAT)	DATA 1 (GREEN)
9 PIN - (GND)	GROUND (BLACK)
9 PIN + (GND)	POWER (RED)
10 PIN 1 (LED)	LED (ORANGE)
10 PIN 2 (NA)	NOT USED
10 PIN C (NA)	NOT USED

Note: Colors may vary slightly depending on the read head manufacturer. Use this chart as a model.

SBB-RI (Legacy)

CHAPTER 4



lite blue *Reader Interface (SBB-RI Legacy)*

Overview

The Legacy SBB-RI is a Reader Interface between **lite blue** and card readers. The SBB-RI offers a cost-effective, modular approach to access control system design. Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)
  - HID Corporate 1000 48-bit (not evaluated by UL)
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Communicates via RS-485 protocol
- Powered directly from **lite blue**
- **OPTIONAL -** can be powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.

Standard Features

- Supports one read-head credential
- Connects directly to the communication channels on the **lite blue** controller via RS-485 protocol
- Includes Two 2 amp, form C, single pole/double throw, mechanically latching relay
- Connection for one multi-color LED for access granted or access denied indication
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc.

Specifications

- Board Dimensions - 3-13/16” x 3-13/16” x 1-3/4”D
- Enclosure Dimensions - 8-1/4”H x 7-1/2W” x 3-1/2”D
- Power requirements - 12 to 24 VDC (supplied by **lite blue** controller)
- Power consumption - 300mA max. (with reader)
- Ambient temperature - 0º to 49º C or 32º to 120º F

SBB-RI Enclosure

SBB-RI Enclosure - An enclosure with a hinged door is included for each SBB-RI. The flying leads of the tamper switch should be attached to a UL Listed burglar alarm system or Listed local siren/annunicator.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8.25” x 7.5” x 3.5”

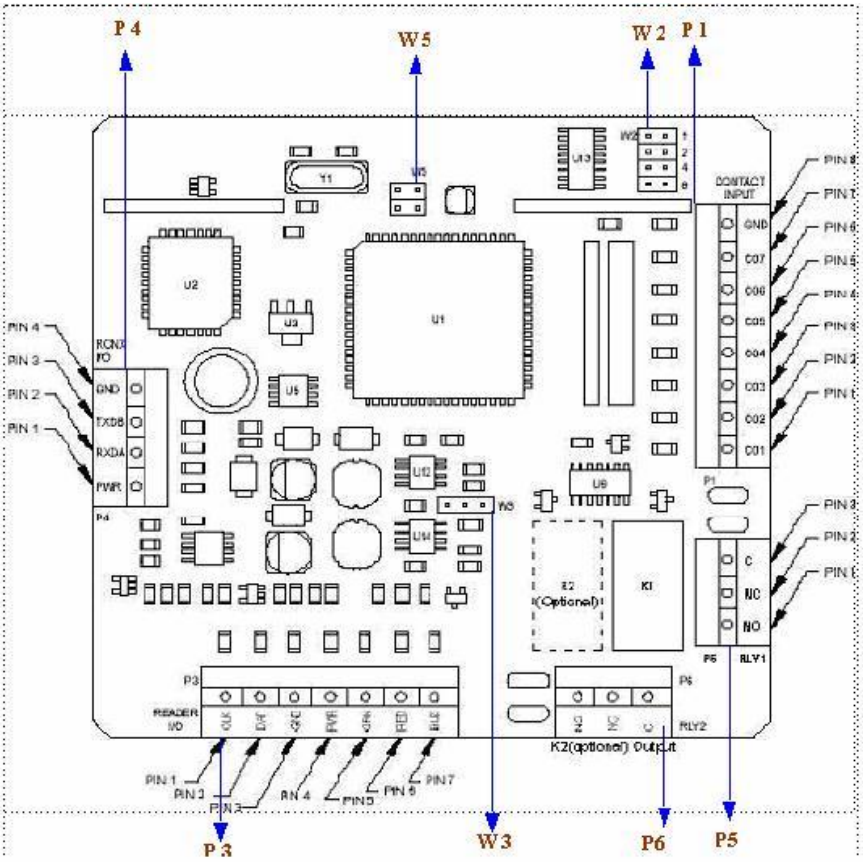
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting

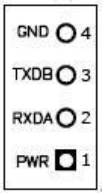
- Field Wiring - It is necessary to punch the knockouts in the metal enclosure for field wiring. It is recommended that this is done before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4" x 1" lag bolts.
- To secure the SBB-RI enclosure use two screws through the openings provided on the cover. Alternately a lock can be added using the provided punch out section on the cover.

SBB-RI Pin Layout



SBB-RI Pin Functions

P4 - Power source and communication wiring. Used to connect **lite blue** to the SBB-RI.



- Pin 4 is Ground
- Pin 3 is Data B
- Pin 2 is Data A
- Pin 1 is Power

P1 - Contact Inputs. The SBB-RI has four unsupervised contact points. When connecting more than two contact inputs to Pin 8 (GND), a terminal strip to connect the common ground wires needs to be installed. Unsupervised door contacts have maximum wire length of 2,000 feet.

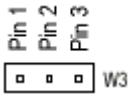
- Pin 1 is Exit Request (REX) - Normally Open
- Pin 2 is Door Position Switch (DOD) - Normally Closed
- Pin 3 is Push Button Override - Normally Open
- Pin 4 is Auxiliary Input - Normally Closed
- Pin 5 is Not Used
- Pin 5 is Not Used
- Pin 6 is Not Used
- Pin 7 is Not Used
- Pin 8 is Ground

P5/P6 - Relay outputs. The SBB-RI comes with two relay output. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp.

- Pin 1 - Normally Open
- Pin 2 - Normally Closed
- Pin 3 - Common

W5 - Factory use only. Do not add a jumper under normal operating conditions.

W3 - Read head voltage selector. The SBB-RI read-head voltage selector provides 5VDC or 12VDC to the various types of read-heads depending on jumper location.



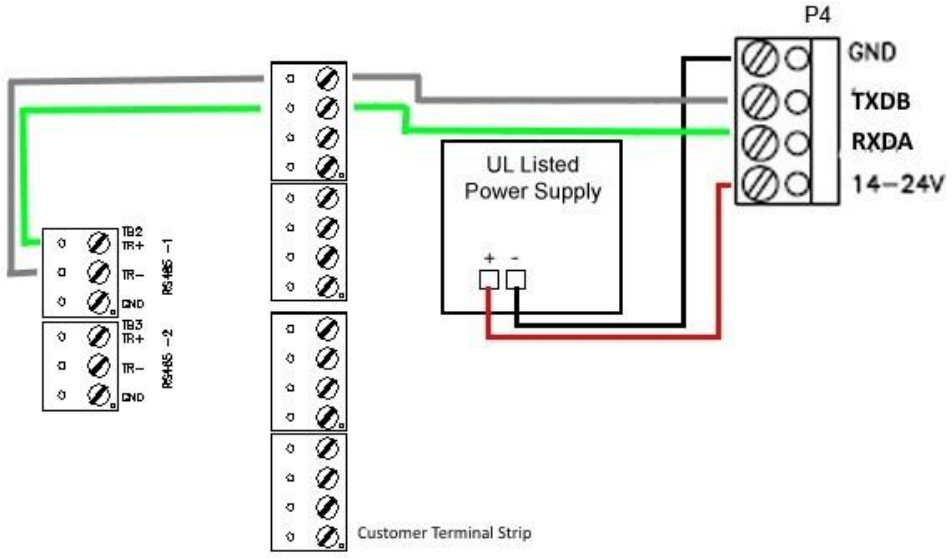
- No jumper will provide 5VDC
- A jumper across Pins 1 and 2 will also provide 5VDC
- A jumper across Pins 2 and 3 will provide 12VDC

Warning: Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read-head voltage requirements.

W2 - SBB-RI addressing. The address of the SBB-RI is dependent on the position of jumpers on these pins. Please see the section on Addressing SBB-RI for more details.

Connecting to lite blue

Data communication between the **lite blue** controller and a VBB-RI reader interface is via RS-485 protocol. Either RS-485 channel on the **lite blue** controller can be used to communicate with P4 on a VBB-RI. The below example is using RS485-1 on the **lite blue** controller and P4 on the VBB-RI.



Data Communication between lite blue and SBB-RI

lite blue	SBB-RI	Power Supply
RS-485-1 TR+	Pin 2 - RXDA (Data A)	
RS-485-1 TR-	Pin 3 - TXDB (Data B)	
	Pin 1 - PWR (Power)	+ (Power)
	Pin 4 - GND (Ground)	- (Ground)

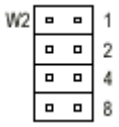
Powering the SBB-RI

The SBB-RI should receive power directly from a UL 294 Listed Power Limited power supply. Power will be supplied independently from the **lite blue** controller.

Addressing the SBB-RI

W2 on the SBB-RI consists of four jumpers that can be combined to set the address for the device. It is recommended that the set address correspond to the slot on the **lite blue** controller it is connected to. For example, if the SBB-RI is connected to the **lite blue** controller at Device 1-15 (Channel 1, Address 15) then the jumpers on the SBB-RI should equal 15. If the SBB-RI is connected to Device 2-7 (Channel 2 Address 7) then the jumpers should equal 7.

Make a note of the address of the SBB-RI and which channel it is connected to. This information will be required to set up the lock in the software.



SBB-RI Address Chart

SBB-RI Address	Jumper Locations	SBB-RI Address	Jumper Locations
1	1 2 4 8	9	1 2 4
2	2 4 8	10	2 4
3	1 4 8	11	1 4
4	4 8	12	4
5	1 2 8	13	1 2
6	2 8	14	2
7	1 8	15	1
8	8	16	None

Connecting to Read Head

The SBB-RI reader interface can communicate to many different read heads. Provided here are the pin outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

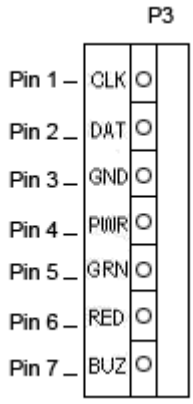
Recommended Wire Chart: SBB-RI to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
SBB-RI to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
SBB-RI to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
SBB-RI to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
SBB-RI to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

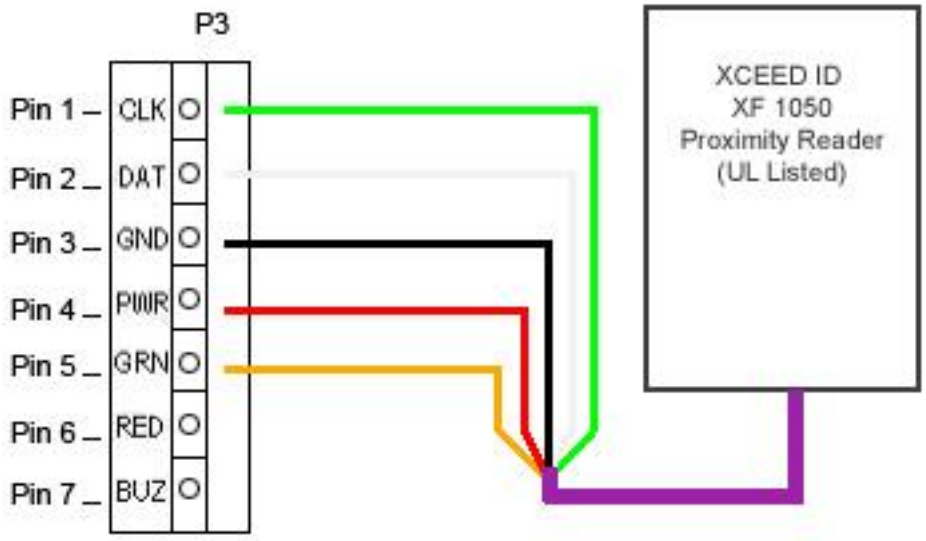
Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

P3 - SBB-RI pin connections



XCEED ID XF 1050 Proximity Reader



Proximity Read Head Pin Connections

SBB-RI	Proximity Reader
PIN 1 (CLK)	DATA 0 (GREEN)
Pin 2 (DAT)	DATA 1 (WHITE)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED
Pin 7 (BUZ)	NOT USED

Magnetic Stripe Reader

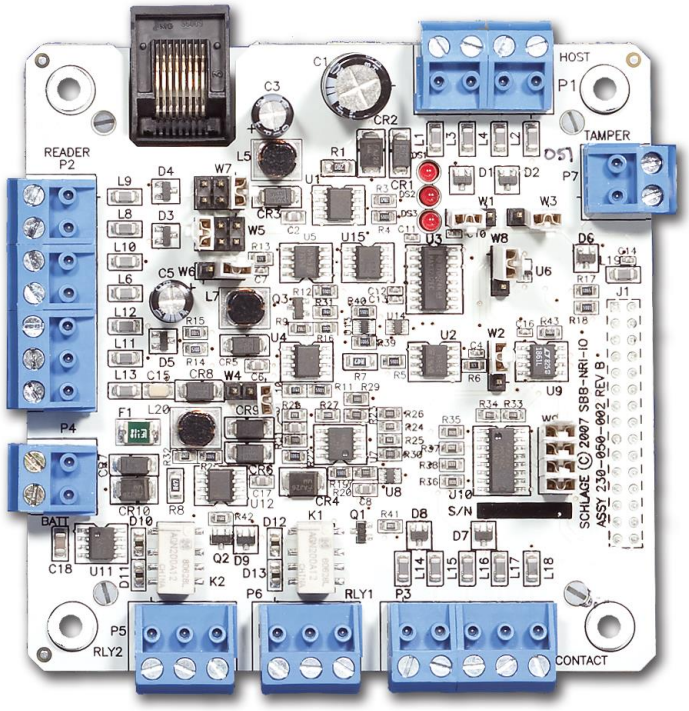
Magnetic Stripe Read Head Pin Connections

SBB-RI	Magnetic Stripe Reader
PIN 1 (CLK)	DATA 0 (WHITE)
Pin 2 (DAT)	DATA 1 (GREEN)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED

SBB-RI	Magnetic Stripe Reader
Pin 7 (BUZ)	NOT USED

VBB-NRI

CHAPTER 5



Vanderbilt **lite blue** *Network Reader Interface (VBB-NRI)*

Overview

The VBB-NRI is a Networked Reader Interface that communicates with **lite blue** via a network connection. The VBB-NRI offers a cost-effective, modular approach to access control system design. Networked Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-Bit (not evaluated by UL)
  - HID Corporate 1000 48-Bit (not evaluated by UL)
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Communicates via network protocol at 10Base-T
- Powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.
- **OPTIONAL -** can be powered directly from **lite blue**. (See Cable Requirement Chart for details)

Standard Features

- Supports one read-head credential
- Communicates with **lite blue** via network protocol at 10/100 Base-T
- Connection for one multi-color LED for access granted or access denied indication
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc.

Specifications

- Board Dimensions - 3-13/16” x 3-13/16” x 2-1/4”D
- Enclosure Dimensions - 8-1/4”H x 7-1/2W” x 3-1/2”D
- Power requirements - 20VDC to 32VDC
- Power consumption - 300mA max. with reader
- Ambient temperature - 0º to 49º C or 32º to 120º F

VBB-NRI Enclosure

VBB-NRI Enclosure - An enclosure with a hinged door is included for each VBB-NRI.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8.25” x 7.5” x 3.5”

Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting

- Field Wiring - It is necessary to punch the knockouts in the metal enclosure for field wiring. It is recommended that this is done before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4" x 1" lag bolts.
- To secure the VBB-NRI enclosure use two screws through the openings provided on the cover. Alternately a lock can be added using the provided punch out section on the cover.

VBB-NRI IP Configuration

The IP address of the VBB-NRI has to be configured so that it can communicate with **lite blue**. Configuration should occur after the reader interface is fully installed. There are two methods to configure the IP address: Static IP and DHCP which are detailed below.

Note: Communication is at 10Base-T

Static IP Configuration (Recommended)

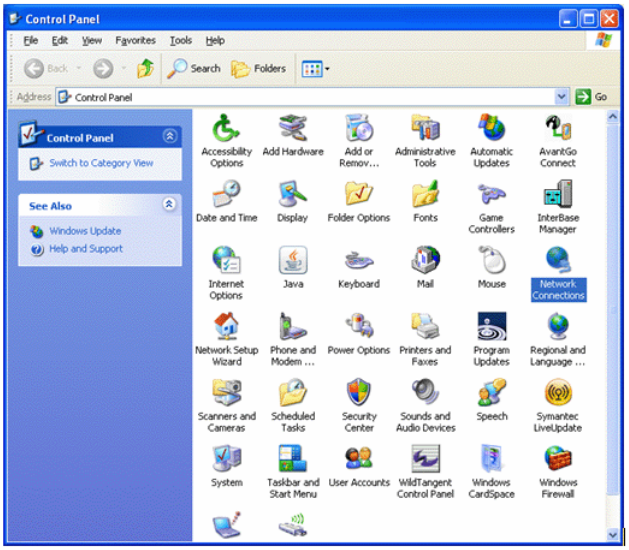
1 Connect a PC with a web browser to the VBB-NRI.

- Direct Connection - Using a cross-over cable, the reader interface can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the reader interface can be connected to a hub or switch that is on the same network as the PC.

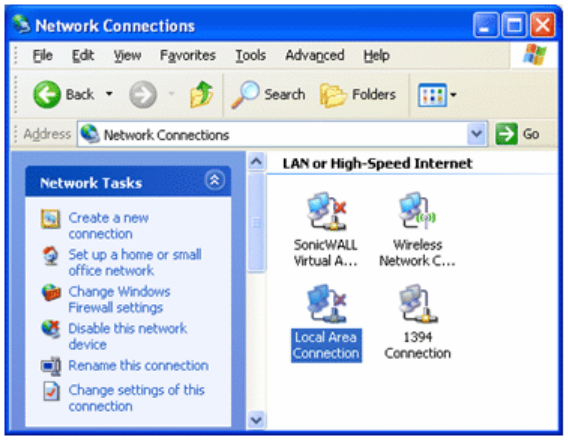
2 Configure the PC's network settings to communicate with the VBB-NRI

a) Click on the **Start** button.

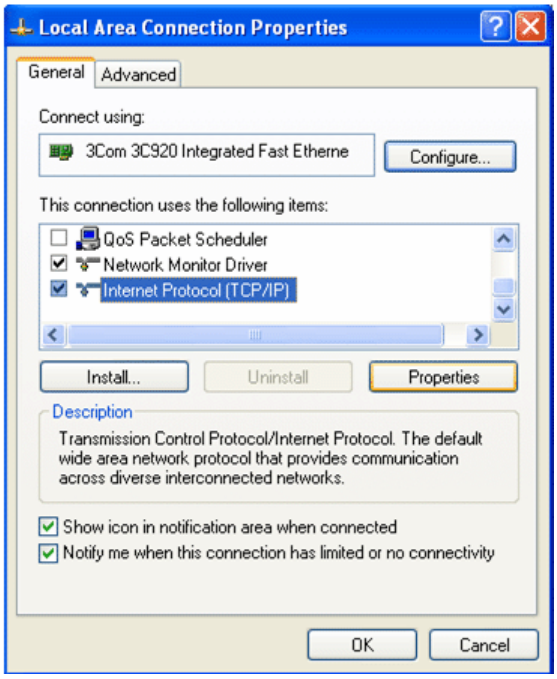
b) Click on **Control Panel**. The Control Panel window will open.



c) Click on **Network Connections**. The Network Connections window will open.



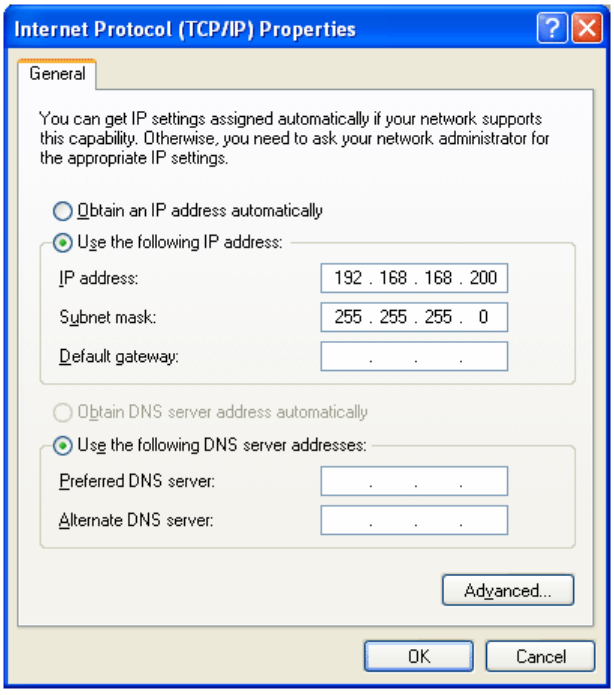
d) Click on **Local Area Connection**. The Local Area Connection Properties window will open.



e) Scroll down and select **Internet Protocol (TCP/IP)**.

f) Click the **Properties** button. The Internet Protocol (TCP/IP) Properties window will open.

g) Make a note of the existing settings. These will need to be restored at the end of the VBB-NRI configuration process to return the PC to its usual settings.



h) Click on the **Use the following IP address** button.

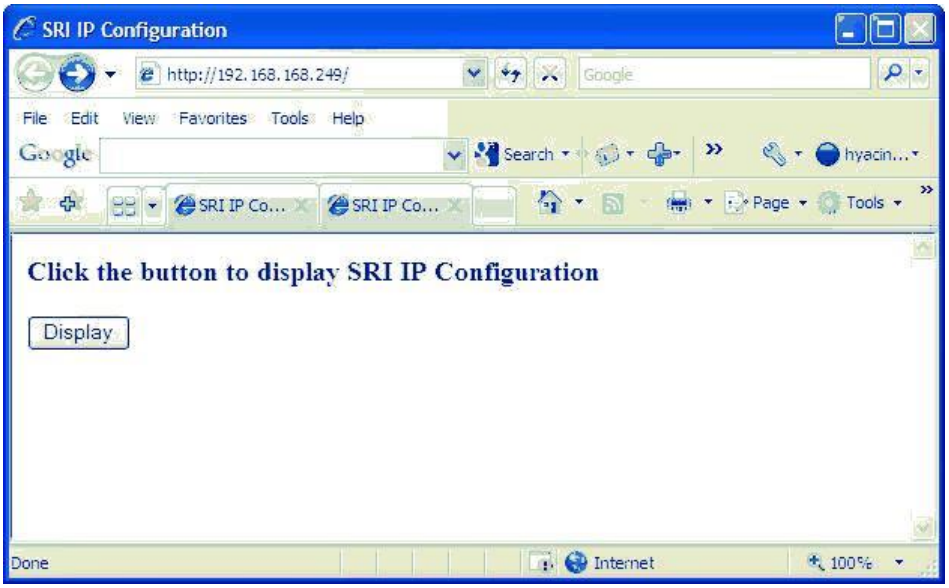
i) Enter 192.168.168.200 into the **IP address** field.

j) Enter 255.255.255.0 into the **Subnet mask** field.

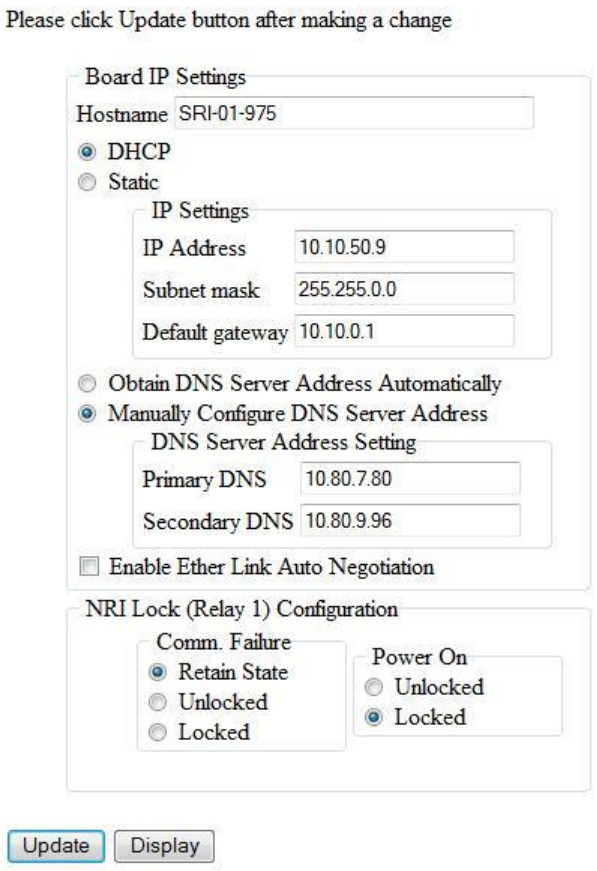
k) Click on the **OK** button. The PC's network settings are now compatible with the default VBB-NRI.

3 Open a web browser.

4 Go to http://192.168.168.249; the SRI IP Configuration window will open.



5 Click on the **Display** button, the VBB-NRI IP Configuration GUI window will open. See the **Configuration GUI** section for additional details.



6 Click on the **Static IP** button.

a) Enter new IP address into the IP address field. Consult with network technicians to get an address that is compatible with the existing network.

b) Enter new Subnet mask into the Subnet mask field. Consult with network technicians to get an address that is compatible with the existing network.

c) Enter new Default gateway into the Default gateway field. Consult with network technicians to get an address that is compatible with the existing network.

7 Click on the **Manually configure DNS server addresses** button.

a) Enter a primary DNS server address into the Primary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

b) Enter a Secondary DNS server into the Secondary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

8 Click on the **Update** button. Make a note of the IP address as it will be used in the **lite blue** Door Setup section.

9 Restore the network settings on the PC (follow step 2 above to access the network settings of the PC).

The Static IP address of the VBB-NRI has been set.

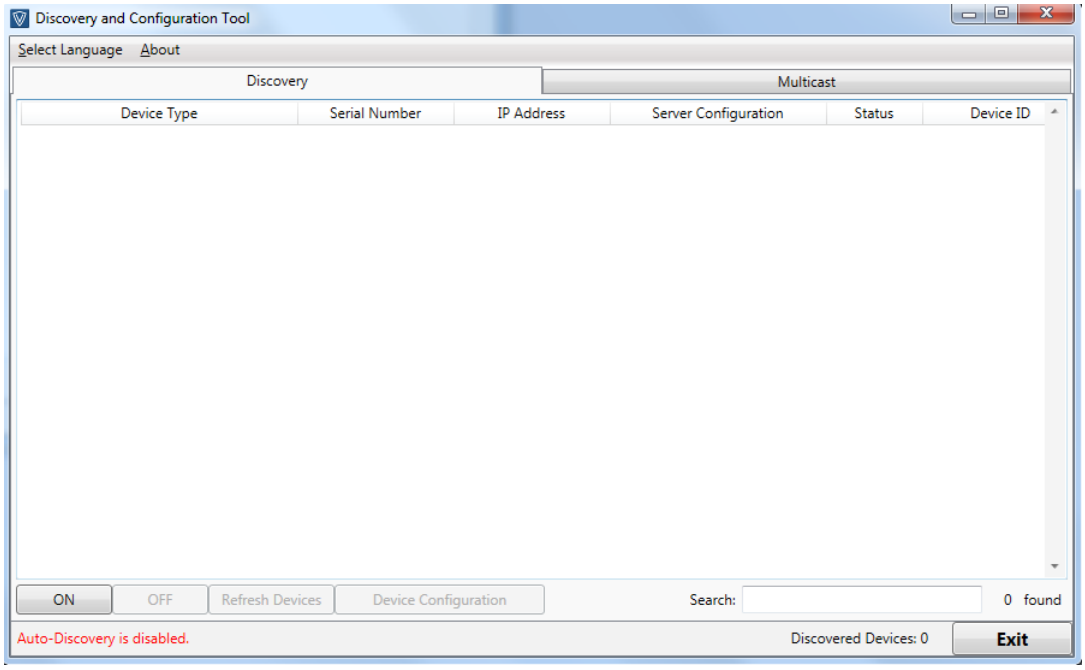
Note: The Static IP address can also be set using the Discovery and Configuration Tool. Follow the directions below for DHCP but select the Static IP configuration option and manually enter the IP address and Subnet mask.

DHCP Configuration

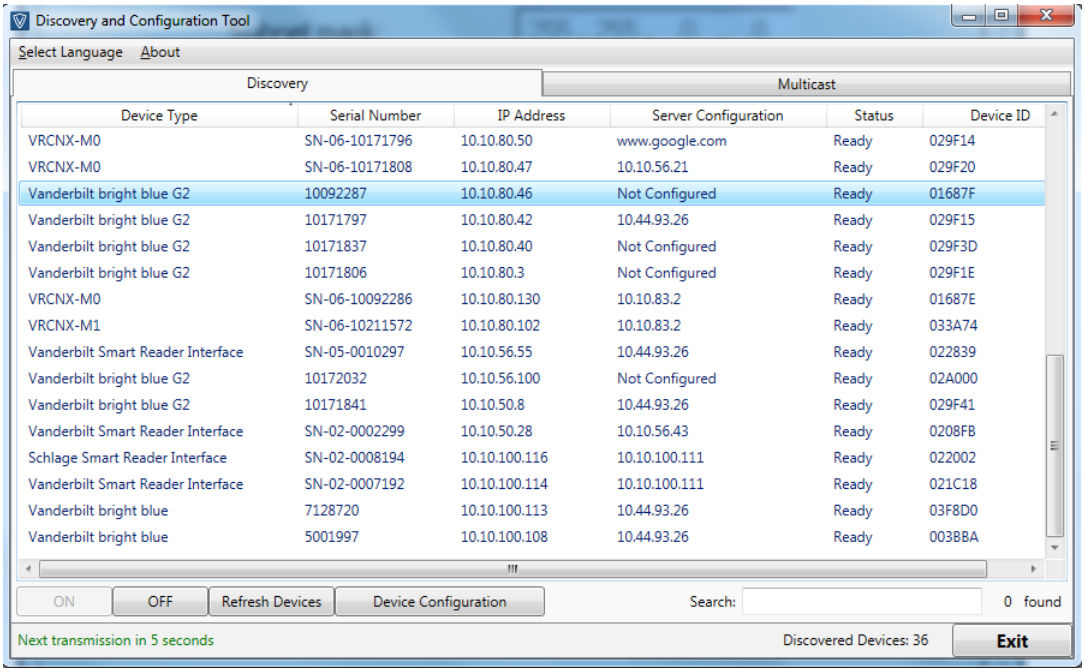
Configuring the VBB-NRI to DHCP requires the Discovery and Configuration program (located on the CD that is included with **lite blue**).

To configure the VBB-NRI with the Discovery and Configuration tool:

1. Connect the PC running the Discovery and Configuration tool to the VBB-NRI.
   - Direct Connection - Using a cross-over cable, the VBB-NRI can be connected directly to the network card of the PC.
   - Network Connection - Using a regular network cable, the VBB-NRI can be connected to a hub or switch that is on the same network as the PC.
2. Run the Discovery and Configuration tool.



3 Click on the **On** button to search for VBB-NRI.

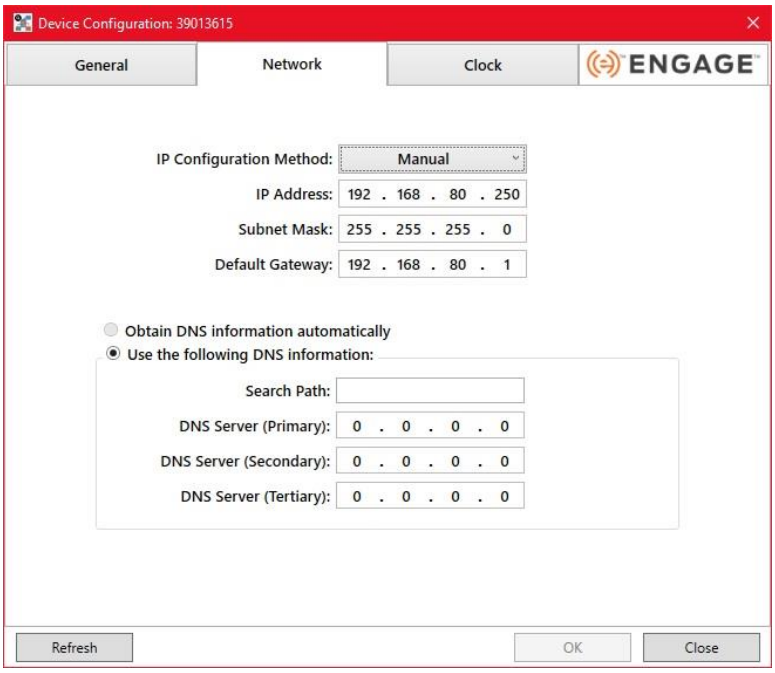


4 Edit the default values.

a) Select which VBB-NRI to configure. If multiple VBB-NRIs are discovered, use the Serial Number to determine which to configure.

b) Click on the **Device Configuration** button to open the Device Configuration window.

c) Click on the **Network** tab.



d) Using the drop-down box, change the IP configuration method to DHCP.

e) Click on the **OK** button to apply the change.

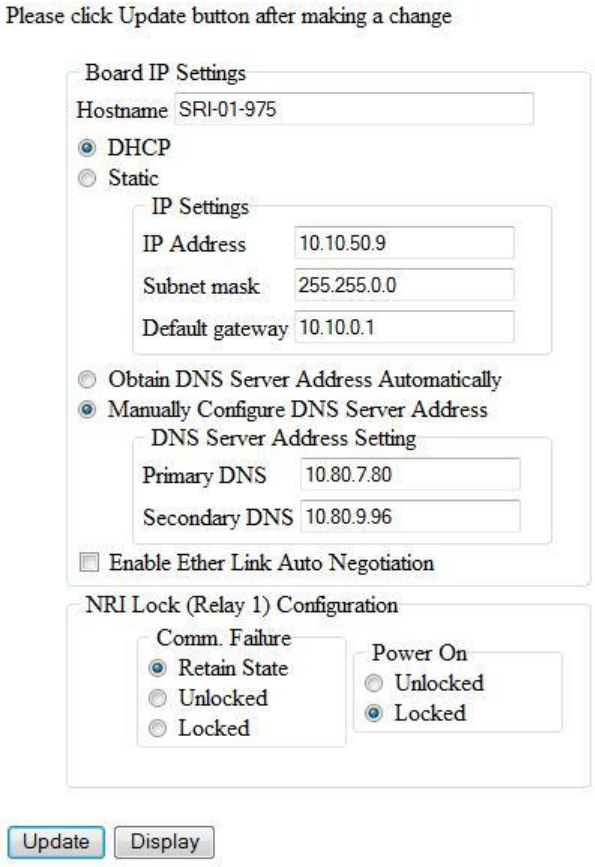
f) Make a note of the IP Address, it will be used by the **lite blue** interface to configure the VBB-NRI.

5 Exit the Discovery and Configuration program.

The DHCP address of the VBB-NRI has been set.

Note: The DHCP address can also be set using the Configuration GUI. Follow the directions above for Static IP but select the DHCP configuration option and then use the Discovery and Configuration tool to find the IP address.

Configuration GUI (Graphic User Interface)



Hostname - This displays the name of the specific VBB-NRI board. The default name should not be changed. The name is in a standard format of SRI-01-XXX.

- SRI - Smart Reader Interface
- 01 - The designation for an VBB-NRI
- XXX - The serial number of the specific VBB-NRI (in the above example the serial number is 975).

The Host Name is used to access and setup the VBB-NRI using Dynamic DNS in conjunction with DHCP. Consult with network technicians for details on setting up your network in this manner.

DHCP - This setting sets up the VBB-NRI to use a DHCP server on your network (use only if you have a DHCP server on the network).

Static - This setting forces the VBB-NRI to use a static IP address.

IP Address

- When in Static mode, this is where you set the NRI's IP address.
- When in DHCP mode, displays the IP address configured by the DHCP server.

Subnet Mask

- When in Static mode, this is where you set the NRI's subnet mask.
- When in DHCP mode, displays the subnet mask configured by the DHCP server.

Default Gateway

- When in Static mode, this is where you set the default gateway.
- When in DHCP mode, displays the default gateway configured by the DHCP server.

Obtain DNS Server Address Automatically - When chosen, your DHCP server will assign your DNS Server IP addresses.

Manually Configure DNS Server Address - When chosen you will assign your DNS server IP addresses.

Primary DNS

- When Automatically obtained, displays the Primary DNS chosen by the DHCP server.
- When Manually entered, this is where you enter the Primary DNS address.

Secondary DNS

- When Automatically obtained, displays the Secondary DNS chosen by the DHCP server.
- When Manually entered, this is where you enter the Secondary DNS address.

Enable Ether Link Auto Negotiation - The VBB-NRI is capable of communication speeds of either 10 or 100 Base-T and, with this option enabled, can switch between the two speeds if necessary. Enabled this option to allow the VBB-NRI to automatically detect and use the communication speed of the switch it is connected to.

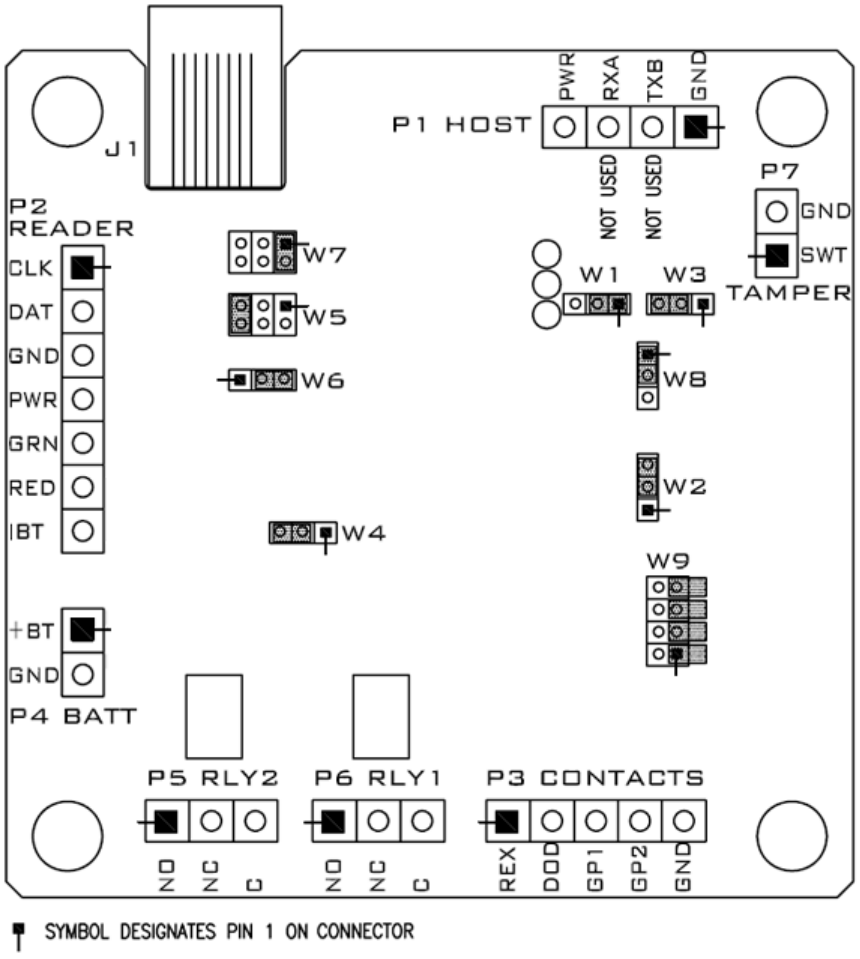
NRI Lock (Relay 1) Configuration - This section is used to define the state of Relay 1 on the VBB-NRI in case of network communication failure during MRO Override state or power restored without network communications restoration.

Note: Whether the lock connected to the VBB-NRI is Fail Safe or Fail Secure will ultimately determine what effect the state of Relay 1 will have on the lock. The examples below are assuming a Fail Secure installation.

- **Comm Failure** - Choose one of the options to define the behaviour of Relay 1 in the event of communication failure. Once communication is returned Relay 1 will resume its Normal Operation state.
  - **Retain State** - The lock will stay in whatever state it was in (activated or deactivated) when communication was lost.
  - **Unlocked** - The relay will be activated when communication is lost. In most installations this will mean that the door will become unsecured.
  - **Locked** - The relay will be deactivated when communication is lost. In most installations this will mean that the door will become secured.

- **Power On** - This section is used to define the behaviour of Relay 1 while **lite blue** is reloading the VBB-NRI after a power loss. In the case of a power failure Relay 1 will become deactivated. When power and communication are returned, **lite blue** will need to reload the VBB-NRI. During this time the Power On option determines what state Relay 1 will be in. Once the VBB-NRI has been fully restored it will resume its Normal Operation state.
  - **Unlocked** - The relay will be activated when the VBB-NRI receives power and is being reloaded. In most installations, this will mean that the door will become unsecured.
  - **Locked** - The relay will be deactivated when the VBB-NRI receives power and is being reloaded. In most installations, this will mean that the door will become secured.

VBB-NRI Pin Layout



VBB-NRI Pin Functions

P1 - Power source wiring. Used to supply power to the VBB-NRI.

- Pin 1 is Ground
- Pin 2 is RXA and is not used with **lite blue**
- Pin 3 is TXB and is not used with **lite blue**
- Pin 4 is Power

P2 - Read head connection.

- Pin 1 through 5 are used to connect to a read head. See the **Connecting to Read Head** section for details.
- Pin 6 is RED and is not used with **lite blue**
- Pin 7 is IBT and is not used with **lite blue**

P3 - Contact Inputs. The VBB-NRI has four unsupervised contact points. When connecting more than two contact inputs to Pin 5 (GND), a terminal strip to connect the common ground wires needs to be installed. Unsupervised door contacts have maximum wire length of 2,000 feet.

- Pin 1 is Exit Request (REX) - Normally Open
- Pin 2 is Door Position Switch (DOD) - Normally Closed
- Pin 3 is Push Button Override - Normally Open
- Pin 4 is Auxiliary Input - Normally Closed
- Pin 5 is Ground

P5/P6 - Relay outputs. The VBB-NRI comes with two relay output.

- Pin 1 - Normally Open
- Pin 2 - Normally Closed
- Pin 3 - Common

W4 - Read head voltage selector. The VBB-NRI read-head voltage selector provides 5VDC or 12VDC to the various types of read-heads depending on jumper location.

- A jumper across Pins 1 and 2 will provide 12VDC (Default Setting)
- A jumper across Pins 2 and 3 will provide 5VDC
- No jumper will also provide 5VDC

Warning: Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read-head voltage requirements.

W9 - Used to disable network functionality. This pin functions differently depending on which version of the VBB-NRI is in use. See the **Verifying Upgrade/Checking Version Number** section at the end of this chapter if you need to determine which version of the VBB-NRI is in use.

VBB-NRI versions 11 and below:

- Pins 1&2 - Enable/Disable onboard web server (Configuration GUI). Enabled by default. If jumpered together, the onboard web server is disabled.
- Pins 3&4 - Enable/Disable Telnet. Enabled by default. If jumpered together, Telnet is disabled

- Pins 5&6 - Enable/Disable Discovery protocol. Enabled by default. If jumpered together, the Discovery protocol is disabled, meaning that the Discovery tool will NOT find the unit.
- Pins 7&8 - reserved for future use.

VBB-NRI version 12 and above:

- Pins 1 & 2 - Enable/Disable: Onboard web server (Configuration GUI), Telnet, Ping and Discovery protocol. Enabled by default. If jumpered together, the onboard web server (GUI), Telnet, Ping and Discovery protocol are disabled. If disabled then the VBB-NRI cannot be reached via the GUI, Telnet, Ping or the Discovery and Configuration Tool.
- Pins 3 & 4 - Not used at this time.
- Pins 5 & 6 - Not used at this time.
- Pins 7 & 8 - Not used at this time.

Warning: After installation, it is recommended that both the onboard web server and telnet be disabled. Leaving them enabled could allow unauthorized access to the VBB-NRI.

Pins Left at Default

The below pins should be left at their default settings:

- W1/W3 - Used to set the Host communication protocol. Default W1: 1&2 Default W3: 2&3
- W2 - Used for RS485 termination (Reader Interface Termination). Default: 2&3
- W5/W7 - Sets communication protocol. Default W5: 5&6 Default W7 1&2
- W6 - Used for RS485 termination (Controller Board Termination). Default 2&3
- W8 - Used to set Magstripe data signal for negative or positive. Default 1&2

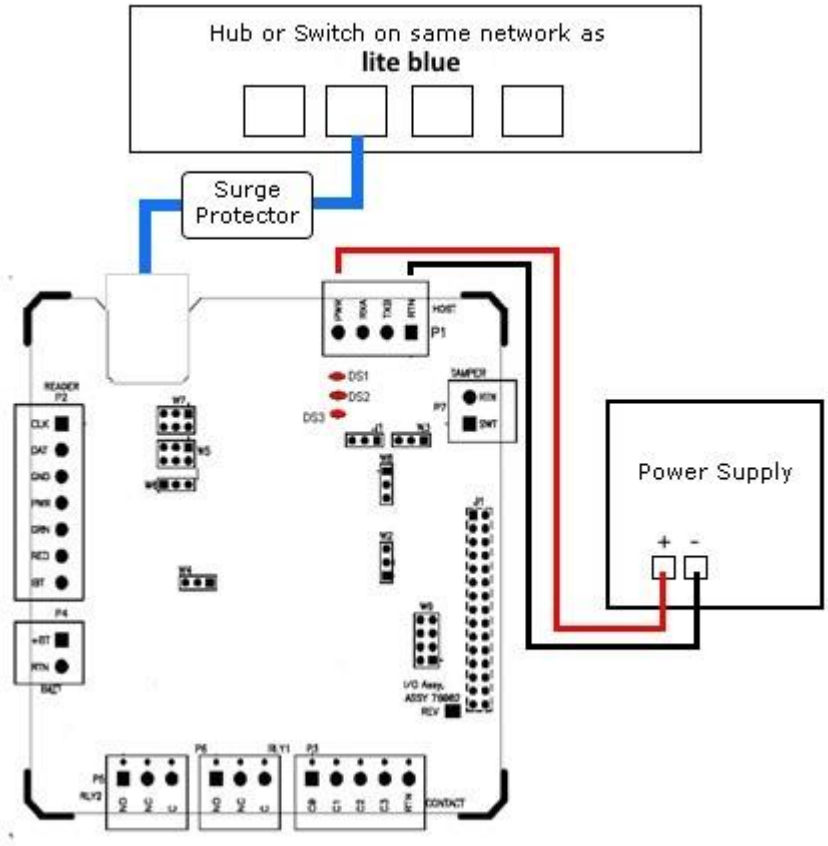
Pins Not Used

The below pins are not used on the VBB-NRI:

- P4
- P7

Connecting to lite blue

There is no direct connection between the VBB-NRI and **lite blue**. They need to be on the same network and the proper IP address of the VBB-NRI needs to be entered when setting up the door (see the VBB-NRI IP Configuration section for details) for them to communicate. In addition, a data surge protector needs to be installed between **lite blue** and the hub or switch. Install the supplied data surge protector (DITEK-DTK-MRJ45C5E) or an equivalent UL Listed unit. Power is supplied independently from a power supply connecting to P1 on the VBB-NRI.



Data Communication between lite blue and VBB-NRI

lite blue	VBB-NRI	Power Supply
Ethernet To Network	Ethernet to Network	
	Pin 1 - PWR (Power)	+ (Power)
	Pin 4 - GND (Ground)	- (Ground)

Connecting to Read Head

The VBB-NRI reader interface can communicate to many different read heads. Provided here are the pin outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

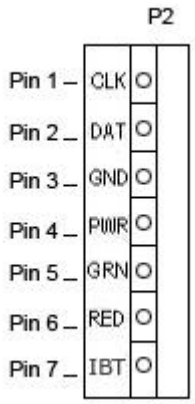
Recommended Wire Chart: VBB-NRI to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VBB-NRI to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VBB-NRI to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VBB-NRI to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VBB-NRI to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

P2 - VBB-NRI pin connections



Proximity Reader

Proximity Read Head Pin Connections

VBB-NRI	Proximity Reader
PIN 1 (CLK)	DATA 0 (GREEN)
Pin 2 (DAT)	DATA 1 (WHITE)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED
Pin 7 (IBT)	NOT USED

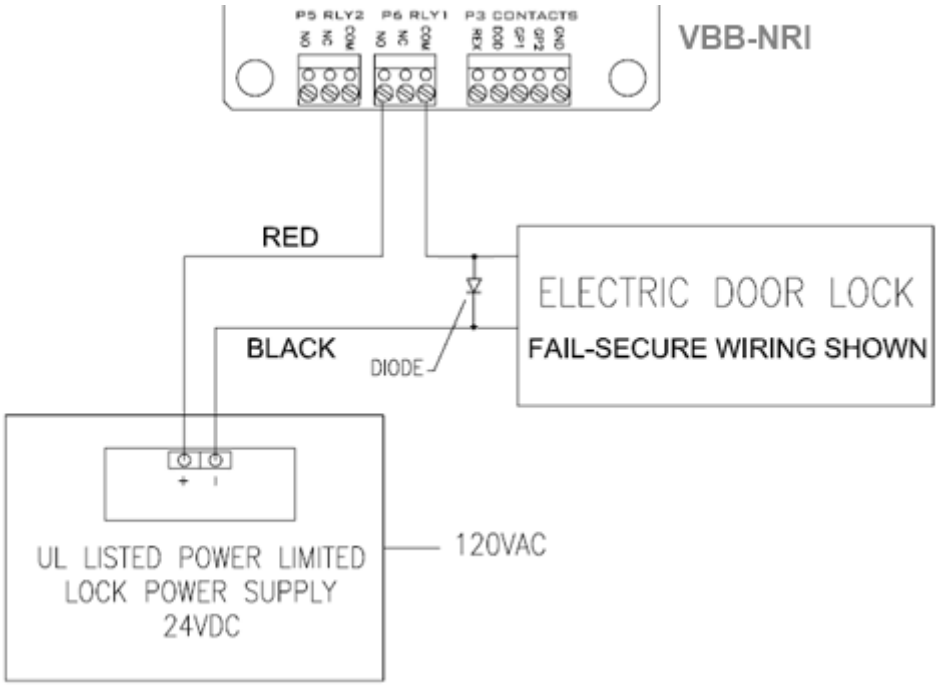
Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VBB-NRI	Magnetic Stripe Reader
PIN 1 (CLK)	DATA 0 (WHITE)
Pin 2 (DAT)	DATA 1 (GREEN)
Pin 3 (GND)	GROUND (BLACK)
Pin 4 (PWR)	POWER (RED)
Pin 5 (GRN)	LED (ORANGE)
Pin 6 (RED)	NOT USED
Pin 7 (IBT)	NOT USED

Installing Diode for Lock Wiring - Relay

A diode is supplied with the VBB-NRI which should be fitted across 12V and COM to protect the relay contacts.



The lock is wired across 12V and COM. A 0V link to COM is then required to complete the circuit. This will be wired to NO or NC depending on lock type: Fail Open / Fail Closed (diagram above shows Fail Open).

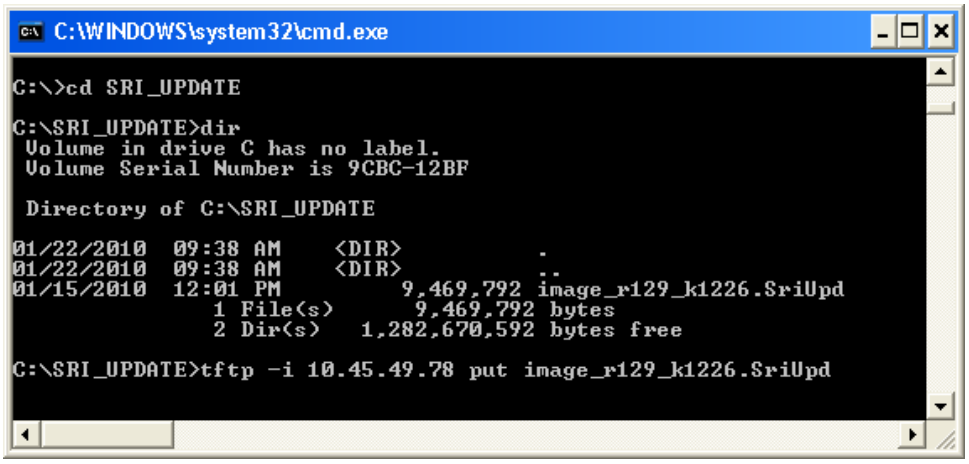
Upgrading Firmware

With v10 and higher of the VBB-NRI it is possible for the user to update the firmware using the TFTP update through a telnet session.

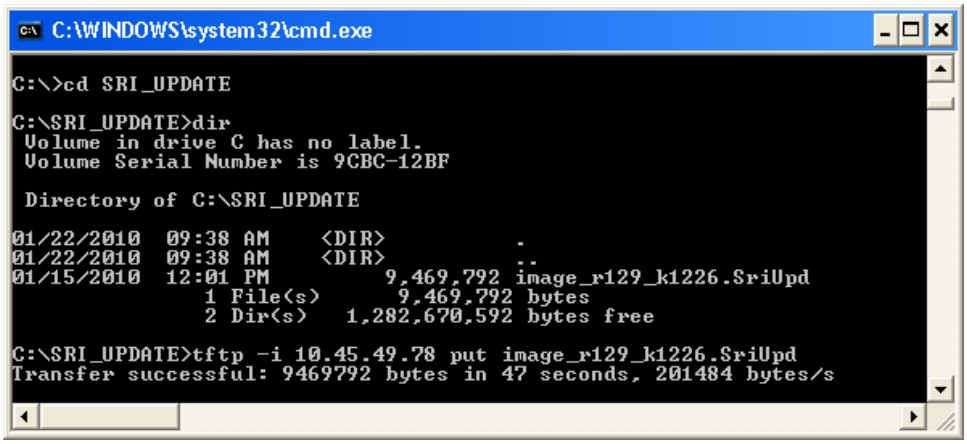
To update the firmware:

1. Open the command line.
2. Navigate to the location of the update file.
3. Enter **tftp –i "VBB-NRI IP Address" put "filename"**;

Example: tftp -I 10.45.49.78 put image_r129_k1226.SriUpd (the name of the image will vary depending on the release of the firmware).



4 You will receive the following message when the file is sent to the VBB-NRI. It may take a few minutes for the board to update to the latest firmware after the message is received.



Verifying Upgrade/Checking Version Number

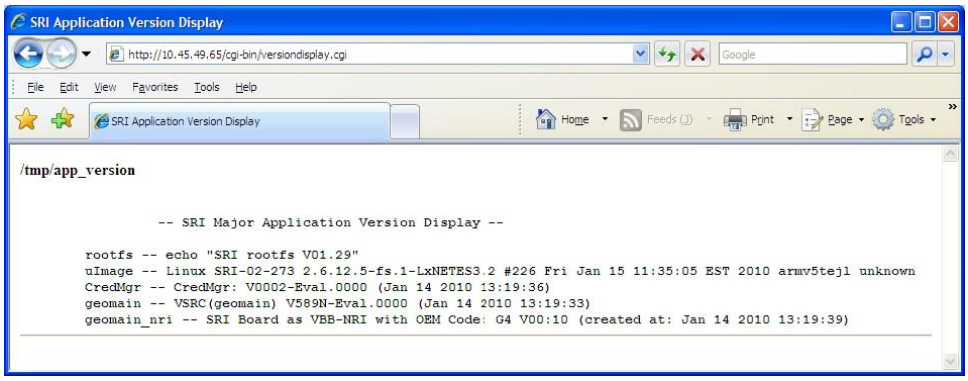
Once the file has been successfully uploaded the user can verify the upgrade by checking the version number of the VBB-NRI. Please allow 5 minutes after the file has been successfully uploaded to the VBB-NRI before verifying the upgrade.

To check the version number:

1 Go to **http://vbb-ri_address/index_ver.html** to load the SRI Application Version Display.

Example: http://10.45.49.65/index_ver.html

2 Click on the **Version Display** button. The full SRI Application Version Display window will open.



3 Check the Geomain_ nri field which displays what revision of firmware was loaded to the VBB-NRI during the upgrade. If the data in this field corresponds to the version upgrade, your upgrade is successful.

Example: If you've just upgraded the VBB-NRI to VBB-NRI v10, it will read: **SRI Board as VBB-NRI with OEM Code: G4 V00:10 (created at: Jan 14, 2010 13:19:39)** The "G4 V00:10" section states that this is an VBB-NRI v10.

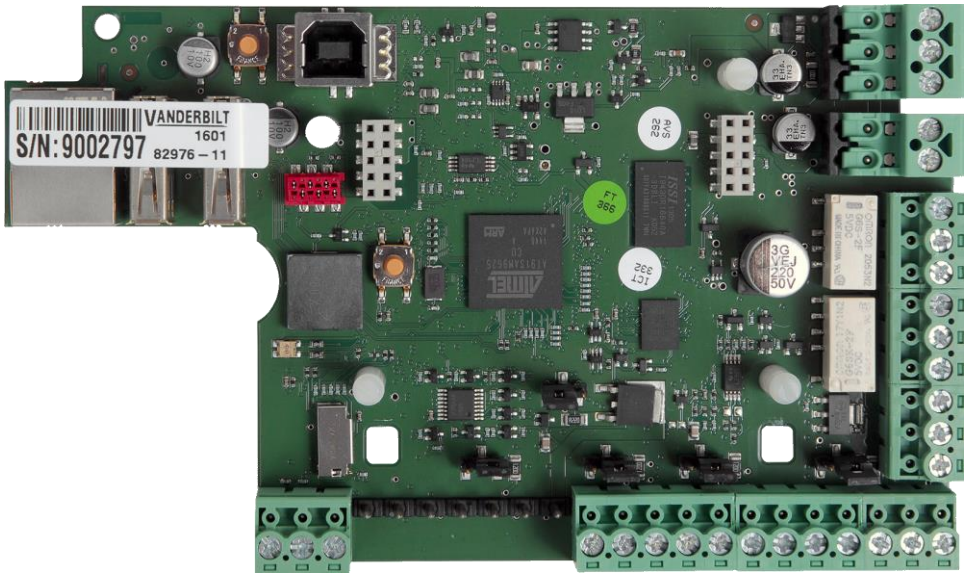
Additional Information

The following information will vary depending on the version of the firmware that has been uploaded to the SRI. For our example with this upgrade, we are showing the following information:

- Rootfs - Usually not updated during the upgrade
- Uimage - Usually not updated during the upgrade
- CredMgr - These values may change depending on if the firmware that has been loaded to the VBB-NRI has been developed especially for a customer evaluation
- Geomain - These values may change depending on if the firmware that has been loaded to the VBB-NRI has been developed especially for a customer evaluation
- Geomain_ nri – Displays the current firmware version of the board.

VBB-NRI G2

CHAPTER 6



Vanderbilt **lite blue** *Network Reader Interface (VBB-NRI Generation 2)*

Overview

The VBB-NRI G2 is a Networked Reader Interface that communicates with **lite blue** via a network connection exactly like the previous generation VBB-NRI. The VBB-NRI G2 offers a cost-effective, modular approach to access control system design. Networked Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-Bit (not evaluated by UL)
  - HID Corporate 1000 48-Bit (not evaluated by UL)
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Communicates via network protocol at 10Base-T
- Powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours' standby power.
- **OPTIONAL -** can be powered directly from **lite blue** (see Cable Requirement Chart for details).

Standard Features

- Supports one read-head credential
- Communicates with **lite blue** via network protocol at 10/100 Base-T
- Connection for one multi-color LED for access granted or access denied indication
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc.

Specifications

- Board Dimensions: 151mm H x 201mm W x 53mm D
- Enclosure Dimensions: 8-1/4" H x 7-1/2" W x 3-1/2" D
- Power requirements: 9.5 VDC to 29.5 VDC
- Power consumption: 600 mA @ 12 VDC
- Ambient temperature: -40º to 55º C

VBB-NRI G2 Enclosure

VBB-NRI G2 Enclosure - An enclosure with a hinged door is included for each VBB-NRI G2.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8.25" x 7.5" x 3.5"

Environmental conditions

- Ambient Temperature: -40º to 55º C
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting

- Field Wiring - It is necessary to punch the knockouts in the metal enclosure for field wiring. It is recommended that this is done before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4" x 1" lag bolts.
- To secure the VBB-NRI G2 enclosure use two screws through the openings provided on the cover. Alternately a lock can be added using the provided punch out section on the cover.

VBB-NRI G2 IP Configuration

The IP address of the VBB-NRI G2 has to be configured so that it can communicate with **lite blue**. Configuration should occur after the reader interface is fully installed. There are two methods to configure the IP address: Static IP and DHCP which are detailed below.

Note: Communication is auto negotiated to 10 or 100 Base-T

Static IP Configuration (Recommended)

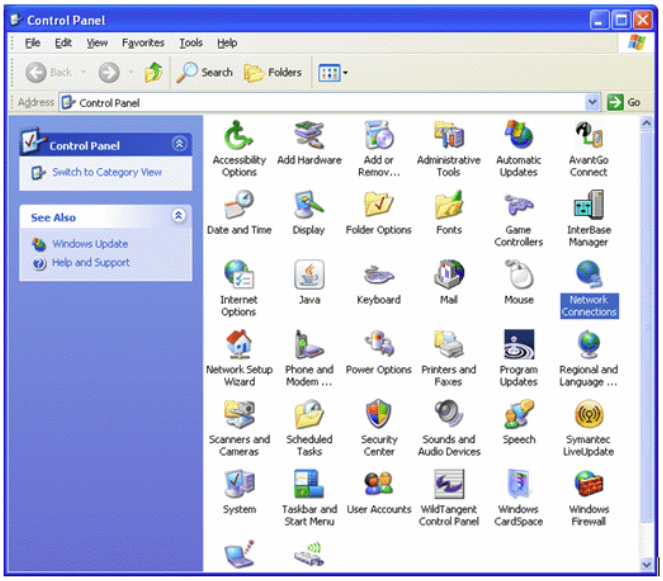
4 Connect a PC with a web browser to the VBB-NRI G2.

- Direct Connection - Using a cross-over cable, the reader interface can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the reader interface can be connected to a hub or switch that is on the same network as the PC.

5 Configure the PC's network settings to communicate with the VBB-NRI G2

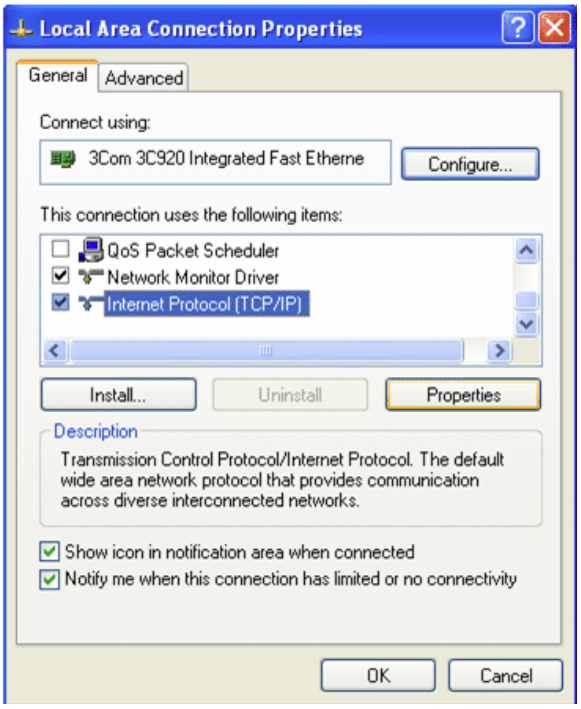
g) Click on the **Start** button.

h) Click on **Control Panel**. The Control Panel window will open.



i) Click on **Network Connections**. The Network Connections window will open.

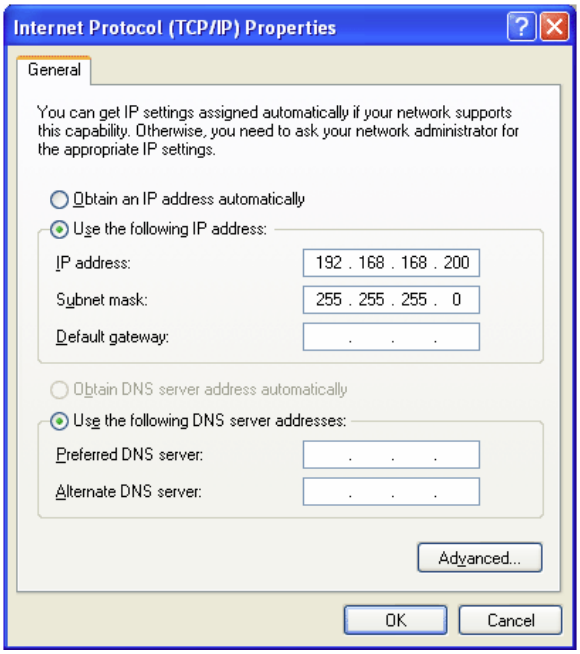
j) Click on **Local Area Connection**. The Local Area Connection Properties window will open.



k) Scroll down and select **Internet Protocol (TCP/IP)**.

l) Click the **Properties** button. The Internet Protocol (TCP/IP) Properties window will open.

m) Make a note of the existing settings. These will need to be restored at the end of the VBB-NRI G2 configuration process to return the PC to its usual settings.



n) Click on the **Use the following IP address** button.

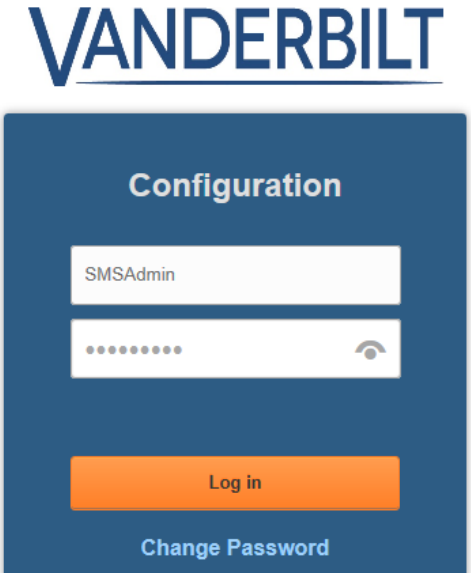
o) Enter 192.168.168.200 into the **IP address** field.

p) Enter 255.255.255.0 into the **Subnet mask** field.

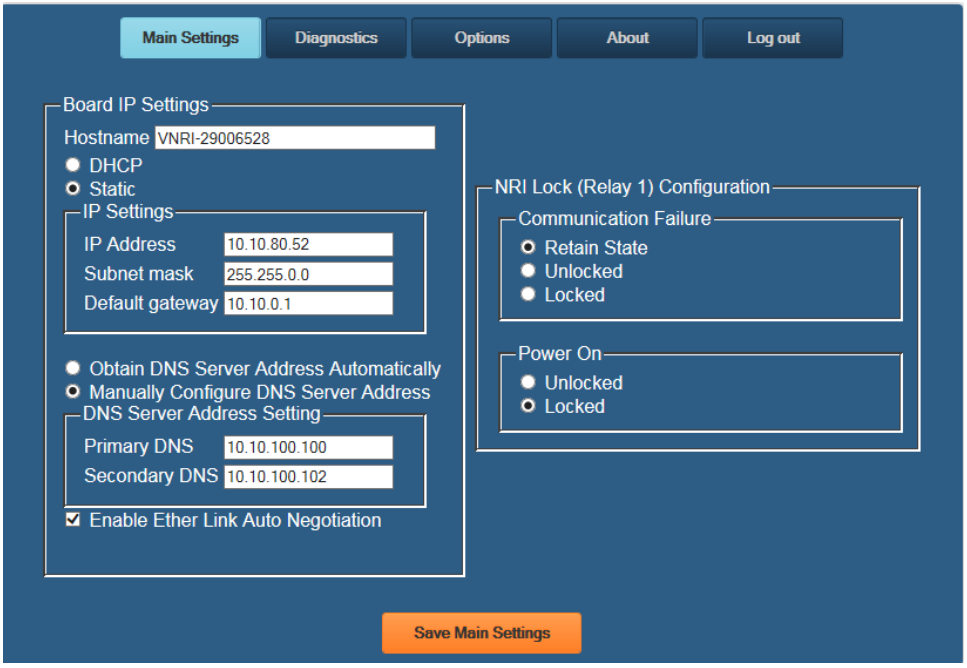
q) Click on the **OK** button. The PC's network settings are now compatible with the default VBB-NRI G2.

6 Open a web browser.

7 Go to https://192.168.168.249 to load the Configuration Application (PW = “SECAdmin1”).



8 Click on the **Main Settings Tab**, the VBB-NRI G2 IP Configuration GUI window will open. See the **Configuration GUI** section for additional details.



9 Click on the **Static IP** button.

r) Enter new IP address into the IP address field. Consult with network technicians to get an address that is compatible with the existing network.

s) Enter new Subnet mask into the Subnet mask field. Consult with network technicians to get an address that is compatible with the existing network.

t) Enter new Default gateway into the Default gateway field. Consult with network technicians to get an address that is compatible with the existing network.

10 Click on the **Manually configure DNS server addresses** button.

u) Enter a primary DNS server address into the Primary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

v) Enter a Secondary DNS server into the Secondary DNS server field. Consult with network technicians to get an address that is compatible with the existing network.

11 Click on the **Update** button. Make a note of the IP address as it will be used in the **lite blue** Door Setup section.

12 Restore the network settings on the PC (follow step 2 above to access the network settings of the PC).

The Static IP address of the VBB-NRI G2 has been set.

Note: The Static IP address can also be set using the Discovery and Configuration Tool. Follow the directions below for DHCP but select the Static IP configuration option and manually enter the IP address and Subnet mask.

DHCP Configuration

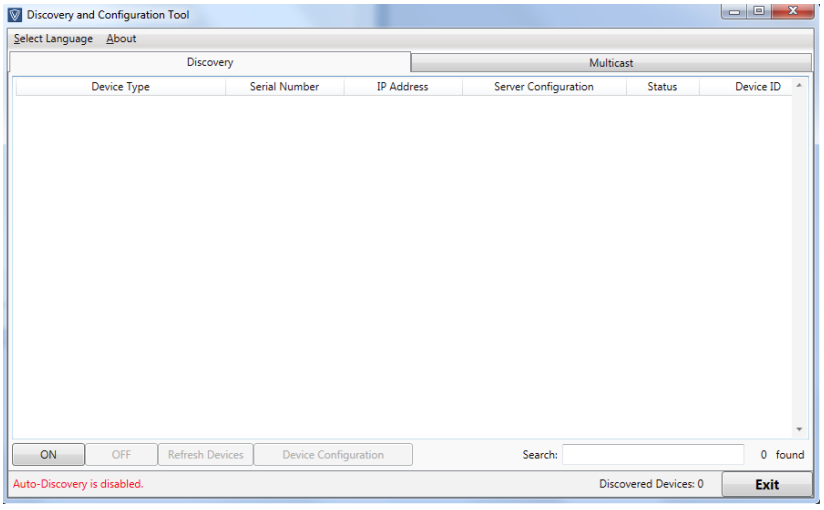
Configuring the VBB-NRI G2 to DHCP requires the Discovery and Configuration program (located on the CD that is included with **lite blue**).

To configure the VBB-NRI G2 with the Discovery and Configuration tool:

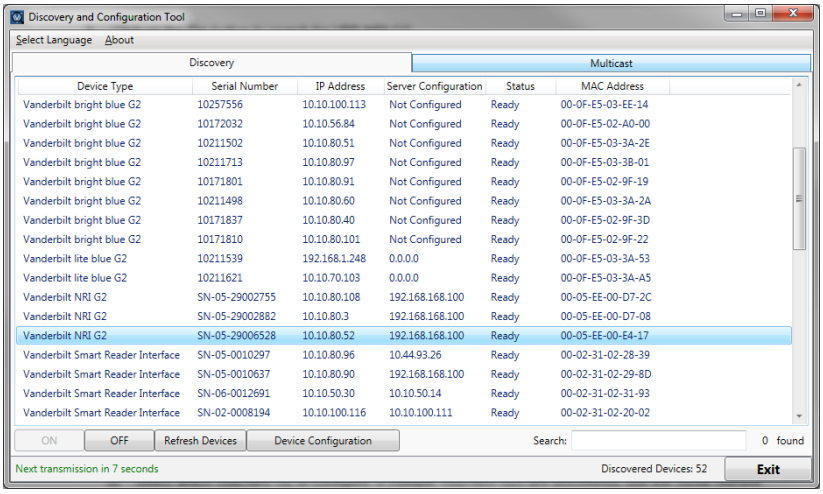
13 Connect the PC running the Discovery and Configuration tool to the VBB-NRI G2.

- Direct Connection - Using a cross-over cable, the VBB-NRI G2 can be connected directly to the network card of the PC.
- Network Connection - Using a regular network cable, the VBB-NRI G2 can be connected to a hub or switch that is on the same network as the PC.

14 Run the Discovery and Configuration tool.



15 Click on the **On** button to search for VBB-NRI G2.

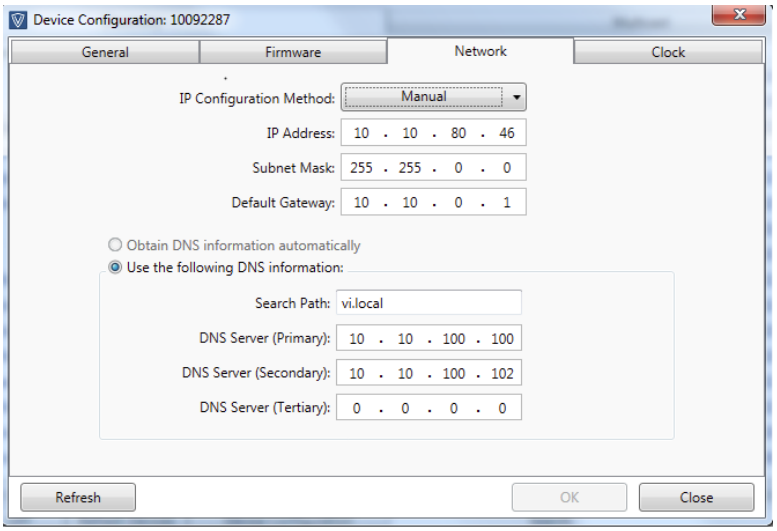


16 Edit the default values.

a) Select which VBB-NRI G2 to configure. If multiple VBB-NRI G2s are discovered, use the Serial Number to determine which to configure.

b) Click on the **Device Configuration** button to open the Device Configuration window.

c) Click on the **Network** tab.



d) Using the drop-down box, change the IP configuration method to DHCP.

e) Click on the **OK** button to apply the change.

f) Make a note of the IP Address, it will be used in **lite blue** to configure the VBB-NRI G2.

17 Exit the Discovery and Configuration program.

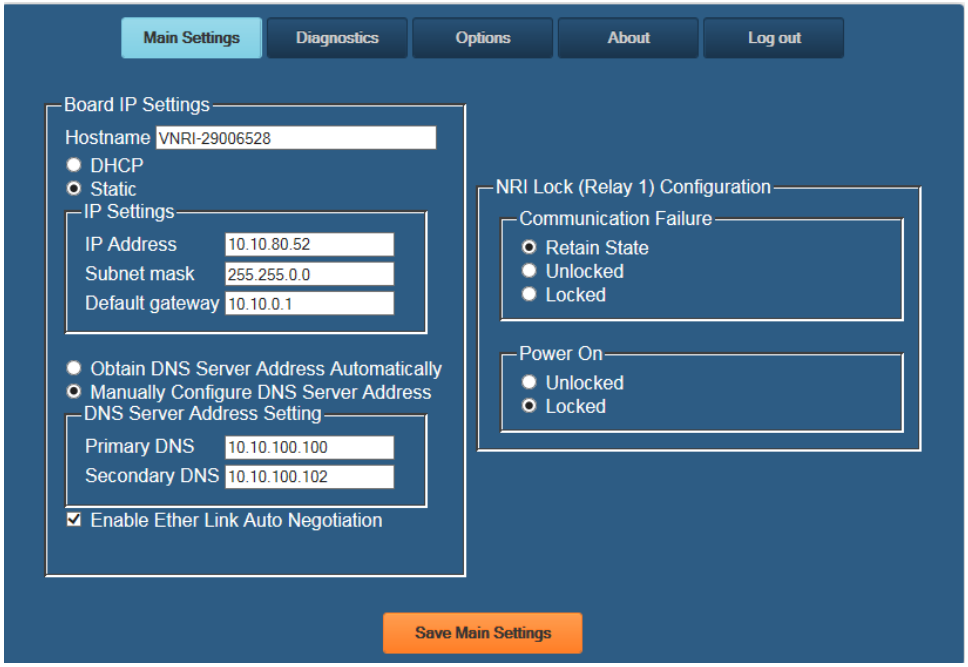
The DHCP address of the VBB-NRI G2 has been set.

Note: The DHCP address can also be set using the Configuration GUI. Follow the directions above for Static IP but select the DHCP configuration option and then use the Discovery and Configuration tool to find the IP address.

Configuration GUI (Graphic User Interface)

Go to https://VBB-NRI_G2_IP_Address to access the Configuration Application (PW = “SECAdmin1”).

Main Settings



Hostname - This displays the name of the specific VBB-NRI G2 board. The default name should not be changed. The name is in a standard format of VNRI-XXXXXXXX

- VNRI – Vanderbilt Network Reader Interface
- XXXXXXXX – Serial number of the specific VBB-NRI G2 (*29006528 in the example above*)

The Host Name is used to access and setup the VBB-NRI G2 using Dynamic DNS in conjunction with DHCP. Consult with network technicians for details on setting up your network in this manner.

DHCP - This setting sets up the VBB-NRI G2 to use a DHCP server on your network (use only if you have a DHCP server on the network).

Static - This setting forces the VBB-NRI G2 to use a static IP address.

IP Address

- When in Static mode, this is where you set the NRI's IP address.
- When in DHCP mode, displays the IP address configured by the DHCP server.

Subnet Mask

- When in Static mode, this is where you set the NRI's subnet mask.

- When in DHCP mode, displays the subnet mask configured by the DHCP server.

Default Gateway

- When in Static mode, this is where you set the default gateway.
- When in DHCP mode, displays the default gateway configured by the DHCP server.

Obtain DNS Server Address Automatically - When chosen, your DHCP server will assign your DNS Server IP addresses.

Manually Configure DNS Server Address - When chosen you will assign your DNS server IP addresses.

Primary DNS

- When Automatically obtained, displays the Primary DNS chosen by the DHCP server.
- When Manually entered, this is where you enter the Primary DNS address.

Secondary DNS

- When Automatically obtained, displays the Secondary DNS chosen by the DHCP server.
- When Manually entered, this is where you enter the Secondary DNS address.

Enable Ether Link Auto Negotiation - The VBB-NRI G2 is capable of communication speeds of either 10 or 100 Base-T and, with this option enabled, can switch between the two speeds if necessary. Enabled this option to allow the VBB-NRI G2 to automatically detect and use the communication speed of the switch.

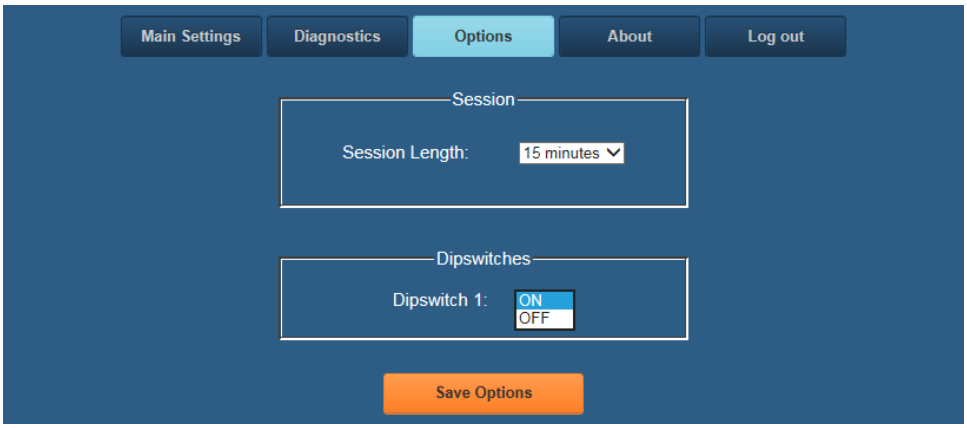
NRI Lock 1 Relay Configuration – Define the state of Relay 1 on the VBB-NRI G2 in case of network communication failure during MRO Override state or power restored without network communications restoration.

Note: Whether the lock connected to the VBB-NRI G2 is Fail Safe or Fail Secure will ultimately determine what effect the state of Relay 1 will have on the lock. The examples below are assuming a Fail Secure installation.

- **Communication Failure** - Choose one of the options to define the behavior of Relay 1 in the event of communication failure. Once communication is returned Relay 1 will resume its Normal Operation state.
  - **Retain State** - The lock will stay in whatever state it was in (activated or deactivated) when communication was lost.
  - **Unlocked** - The relay will be activated when communication is lost. In most installations, this will mean that the door will become unsecured.
  - **Locked** - The relay will be deactivated when communication is lost. In most installations, this will mean that the door will become secured.
- **Power On** - This section is used to define the behavior of Relay 1 while **lite blue** is reloading the VBB-NRI G2 after a power loss. In the case of a power failure Relay 1 will become deactivated. When power and communication are returned, **lite blue** will need to reload the VBB-NRI G2. During this time the Power On option determines what state Relay 1 will be in. Once the VBB-NRI G2 has been fully restored it will resume its Normal Operation state.
  - **Unlocked** - The relay will be activated when the VBB-NRI G2 receives power and is being reloaded. In most installations, this will mean that the door will become unsecured.
  - **Locked** - The relay will be deactivated when the VBB-NRI G2 receives power and is being reloaded. In most installations, this will mean that the door will become secured.

Options

Settings on the Options tab can be used to secure the VBB-NRI G2 configuration application.



The Session Length drop down can be used to adjust the Configuration Application session inactivity timer.

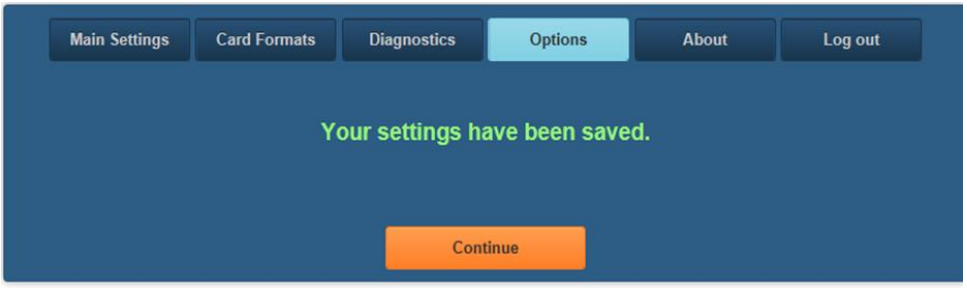
Vanderbilt ships VBB-NRI G2 with Dipswitch 1 = ON which allows access to the Configuration application.

Set Dipswitch 1 = OFF to disable Configuration access. PING and Auto-discovery will also be disabled (i.e. the Discovery and Configuration Tool will not be able to locate the VBB-NRI G2).

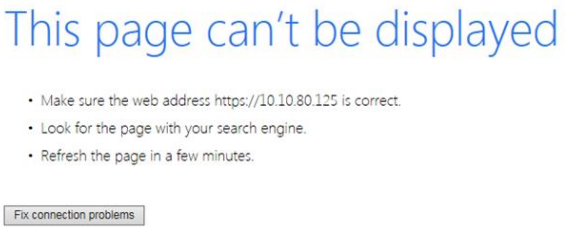
The VBB-NRI G2 can still be accessed via SSH (WinSCP or PuTTy).

Click the “Save Options” button to commit any changes.

Warning: After installation, it is recommended that the Configuration Application is disabled. Leaving it enabled could allow unauthorized access to the VBB-NRI G2.



Subsequent attempts to access the Configuration Application will be denied.

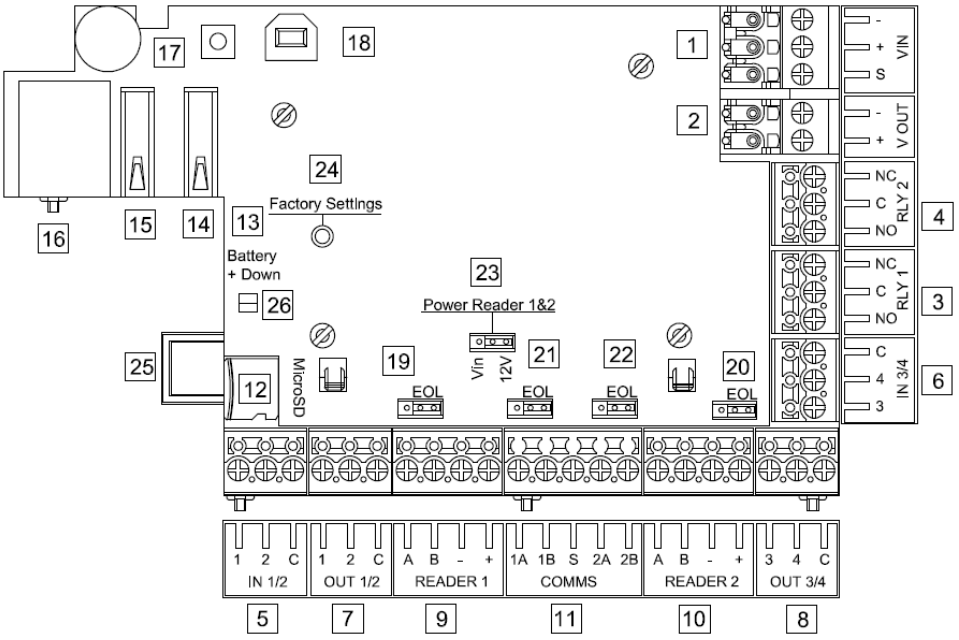


Physical access to the VBB-NRI G2 is required to re-enable the Configuration Application.

Press and Hold the Tamper Switch 17 AND Press and Release the Reset Button 24 three (3) times in succession. Release the Tamper Switch 17. A one (1) second beep will be heard on the 2nd and 3rd Reset Button activations. Releasing the Tamper Switch will generate a two (2) second beep.

Access and log into the Configuration Application within ten (10) minutes, select Options, and reset Dipswitch 1 = ON and click “Save Options”.

VBB-NRI G2 Pin Layout



VBB-NRI G2 Pin Functions

1 Power / VIN

- + is Power
- - is Ground
- S is Chassis Ground

2 Not Used

3 Relay 1 – Max 30 VDC @ 2 A

- NC is Normally Closed
- C is Common
- NO is Normally Open

4 Relay 2 – Max 30 VDC @ 2 A

- NC is Normally Closed

- C is Common
- NO is Normally Open

The VBB-NRI G2 has four unsupervised contact points. Unsupervised door contacts have maximum wire length of 2,000 feet.

5 Contact Inputs 1 & 2

- 1 is Exit Request (REX) – N/O
- 2 is Door Position Switch (DOD) – N/C
- C is Ground

6 Contact Inputs 3 & 4

- 3 is Push Button Override – N/O
- 4 is Auxiliary Input – N/C
- C is Ground

7 & 9 Read Head Connection

- 1 is LED
- 2 is Not Used
- C is Not Used
- A is CLK (Data 0)
- B is DAT (Data 1)
- - is Ground
- + is Power

8 & 10 Not Used

11 Not Used

19 Not Used

20 Not Used

21 Not Used

22 Not Used

23 Read Head Voltage Selector. The VBB-NRI G2 read head voltage selector provides wither 12 VDC or passes VIN to the read head depending on jumper location.

- A jumper across PINs 2 and 3 (12V) will provide 12 VDC (default setting)
- A jumper across PINs 1 (Vin) and 2 will pass VIN
- No jumper will provide 0 VDC

Warning: Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read head voltage requirements.

16 Configure network functionality.

Refer to Configure GUI section above.

Factory Reset and Power down

Reboot

Press and Hold the VBB-NRI G2 Reset Button 24 for five (5) to nine (9) seconds. The buzzer will beep once after four (4) seconds. The buzzer will begin to beep rapidly after five (5) seconds – release the Reset Button and the board will reboot. The configured Network Settings (IP Address, etc.) will be retained on reboot.

Power Down

Press and Hold the VBB-NRI G2 Reset Button 24 for ten (10) seconds. The buzzer will beep once after four (4) seconds. The buzzer will begin to beep rapidly after five (5) seconds and then board will power down after ten (10 seconds). The configured Network Settings (IP Address, etc.) will be retained on reboot.

Reboot and Reset to Default IP Address

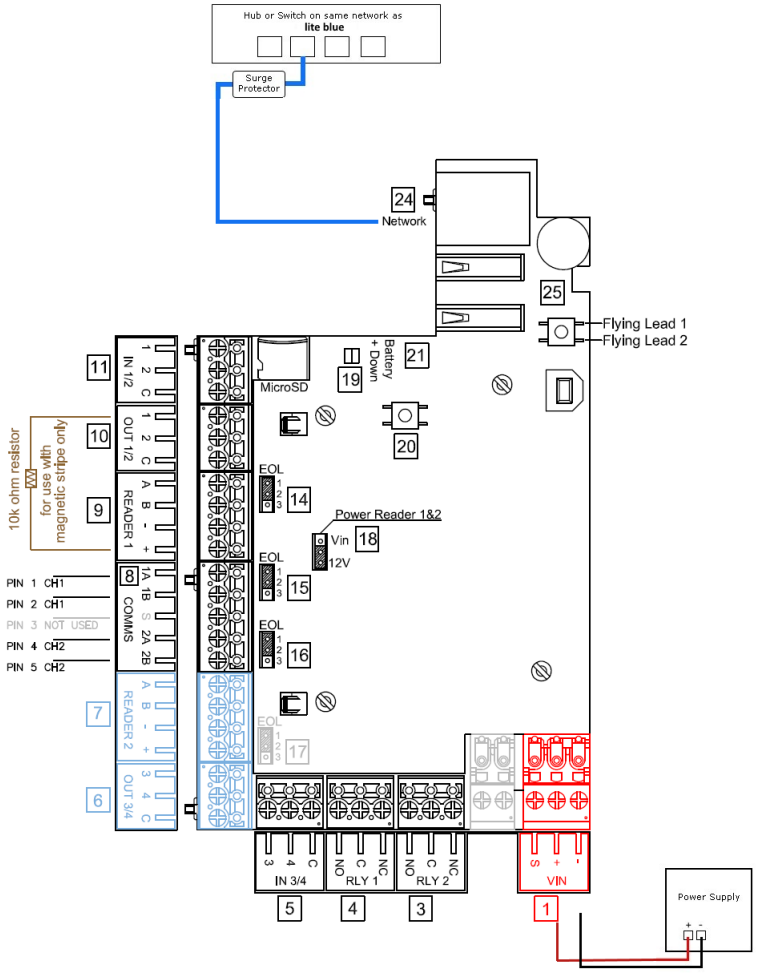
Press and Hold the VBB-NRI G2 Reset Button 24 AND Tamper Switch 17 for five (5) to nine (9) seconds. The buzzer will beep once after four (4) seconds. The buzzer will begin to beep rapidly after five (5) seconds – release the Reset Button and the board will reboot. The Network Settings will reset to the Vanderbilt Defaults on reboot.

Power Down and Reset to Default IP Address

Press and Hold the VBB-NRI G2 Reset Button 24 AND Tamper Switch 17 for ten (10) seconds. The buzzer will beep once after four (4) seconds. The buzzer will begin to beep rapidly after five (5) seconds and then board will power down after ten (10 seconds). The Network Settings will be reset to the Vanderbilt Defaults when the VBB-NRI G2 is repowered.

Connecting to lite blue

There is no direct connection between the VBB-NRI G2 and **lite blue**. They need to be on the same network and the proper IP address of the VBB-NRI G2 needs to be entered when setting up the door (see the VBB-NRI G2 IP Configuration section for details) for them to communicate. In addition, a data surge protector needs to be installed between **lite blue** and the hub or switch. Install the supplied data surge protector (DITEK-DTK-MRJ45C5E) or an equivalent UL Listed unit. Power is supplied independently from a power supply connecting to P1 on the VBB-NRI G2.



Data Communication between lite blue and VBB-NRI G2

lite blue	VBB-NRI G2	Power Supply
Ethernet To Network	Ethernet to Network	
	1 VIN + (Power)	+ (Power)
	1 VIN - (Ground)	- (Ground)

Connecting to Read Head

The VBB-NRI G2 reader interface can communicate to many different read heads. Provided here are the pin outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

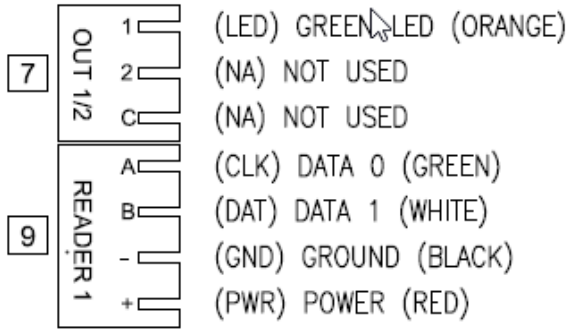
Recommended Wire Chart: VBB-NRI G2 to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VBB-NRI G2 to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VBB-NRI G2 to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VBB-NRI G2 to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VBB-NRI G2 to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

7 & 9 VBB-NRI G2 PIN Connections



Proximity Reader

Proximity Read Head Pin Connections

VBB-NRI G2	Proximity Reader
9 PIN A (CLK)	DATA 0 (GREEN)
9 PIN B (DAT)	DATA 1 (WHITE)
9 PIN - (GND)	GROUND (BLACK)
9 PIN + (GND)	POWER (RED)
7 PIN 1 (LED)	LED (ORANGE)
7 PIN 2 (NA)	NOT USED
7 PIN C (NA)	NOT USED

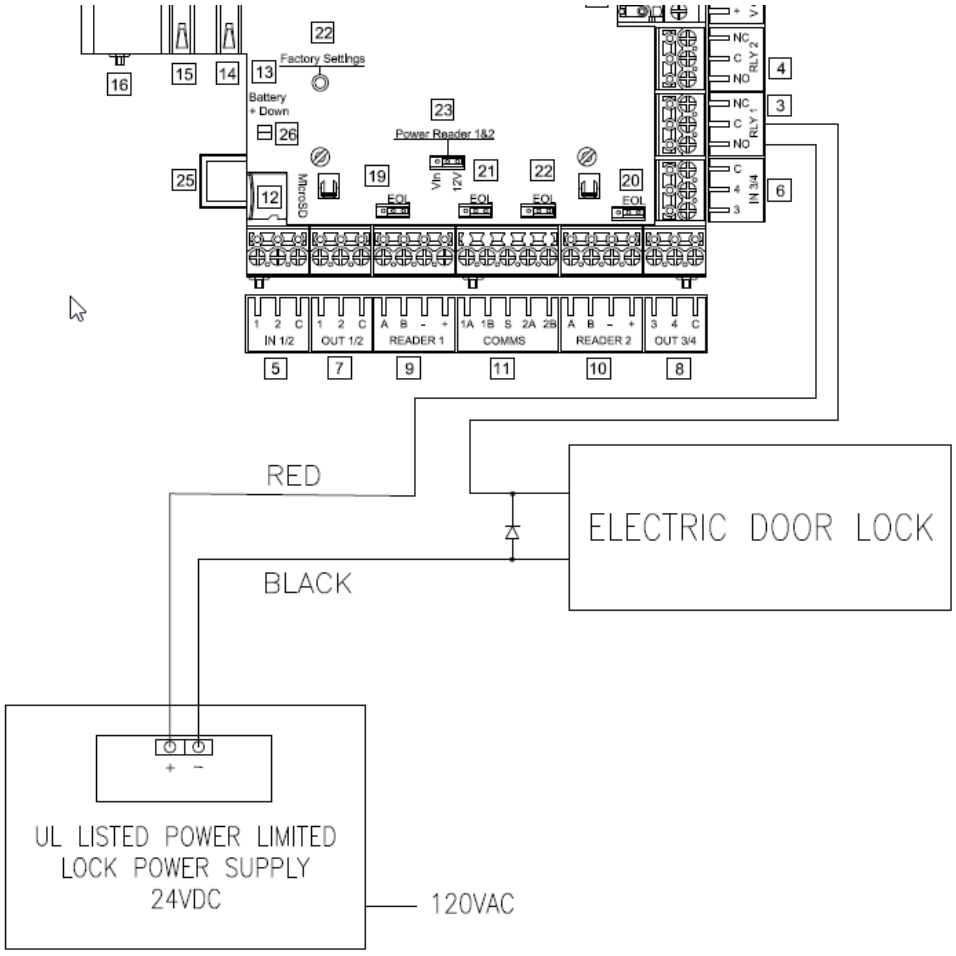
Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VBB-NRI G2	Magnetic Stripe Reader
9 PIN A (CLK)	DATA 0 (WHITE)
9 PIN B (DAT)	DATA 1 (GREEN)
9 PIN - (GND)	GROUND (BLACK)
9 PIN + (GND)	POWER (RED)
7 PIN 1 (LED)	LED (ORANGE)
7 PIN 2 (NA)	NOT USED
7 PIN C (NA)	NOT USED

Installing Diode for Lock Wiring - Relay

A diode is supplied with the VBB-NRI G2 which should be fitted across 24V and COM to protect the relay contacts.



The lock is wired across 24V and COM. A 0V link to COM is then required to complete the circuit. This will be wired to NO or NC depending on lock type: Fail Open / Fail Closed (diagram above shows Fail Open).

Upgrading Firmware

The VBB-NRI G2 firmware can only be updated via SSH. Vanderbilt recommends using WinSCP. The instructions provided below assume WinSCP is used to make the SSH connection to the VBB-NRI G2.

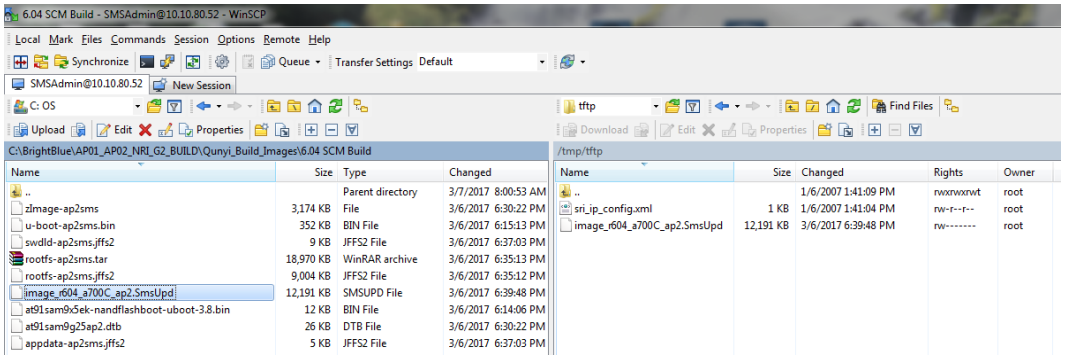
18 Launch WinSCP on a computer on the same network with the VBB-NRI G2.

19 Connect to the VBB-NRI G2.

20 Navigate to the location of the update file in the right pane of WinSCP.

21 Copy the image file *.SMSUpd file provided by Vanderbilt into the tmp/tftp folder in the left pane of WinSCP.

22 Close WinSCP and the update will be applied automatically.



Verifying Upgrade/Checking Version Number

Once the file has been successfully uploaded the user can verify the upgrade by checking the version number of the VBB-NRI G2. Please allow 5 minutes after the file has been successfully uploaded to the VBB-NRI G2 before verifying the upgrade.

To check the version number:

23 Launch the web configuration for the VBB-NRI G2 (https://IPAddress) and select Diagnostics after login.

24 Select the About tab.

25 Review the **smsc** and **vnri** lines which display the revision of firmware loaded to the VBB-NRI G2 during the upgrade. If the data in this field corresponds to the version upgrade, your upgrade is successful.

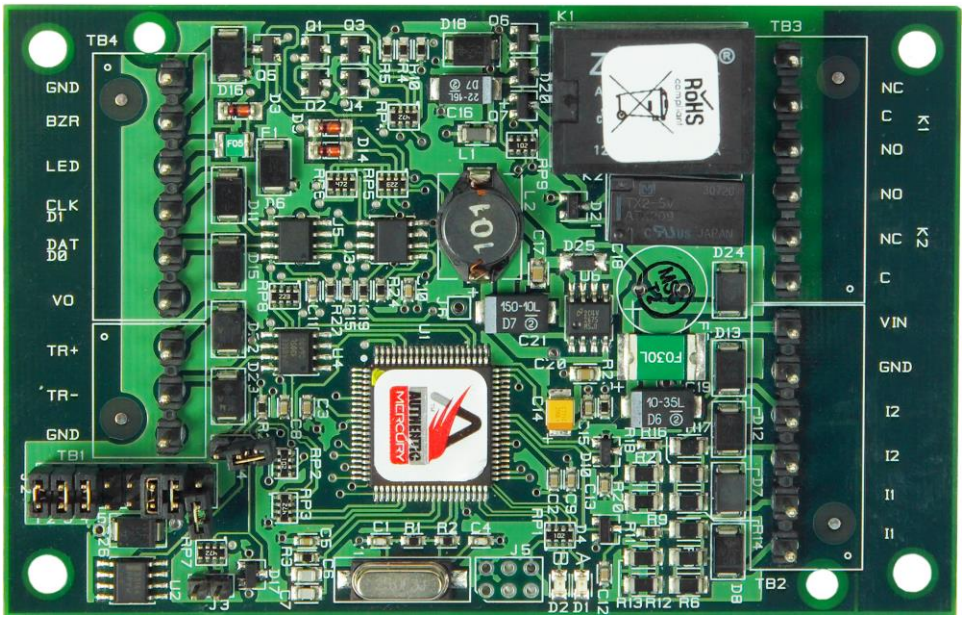
Additional Information

The following information will vary depending on the version of the firmware that has been uploaded to the VBB-NRI G2:

- Rootfs – Usually not updated during the upgrade
- uImage – Usually not updated during the upgrade
- autodscv – Usually not updated during the upgrade
- smsc – Usually not updated during the upgrade
- vnri – Displays the current firmware version of the board

VRI-1

CHAPTER 7



Single Reader Interface

Overview

The new VRI-1 is a Reader Interface between the **lite blue** and card readers. The VBB-RI offers a cost-effective, modular approach to access control system design. The new VRI-1 works similarly to the VRINX but utilizes a new SMS-M protocol. Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)
  - HID Corporate 1000 48-bit (not evaluated by UL)

  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - Vanderbilt 35-bit (including EV1)
  - MiFare 32-Bit Serial Number
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and **lite blue**
- Can be powered directly from **lite blue**
- **OPTIONAL -** can be powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.

Features

- Supports one read-head credential
- Connects directly to the communication channels on the **lite blue** controller via RS-485 protocol
- Two form C, single pole/double throw, 30 VDC mechanically latching relays:
  K1 rated @ 5A; K2 rated @ 1A
- Two supervised or unsupervised contact inputs with the ability to support a wide range of end-of-line resistor values
- Connection for one multi-color LED for access granted or access denied indication
- Connector for one buzzer/annunciator

Specifications

- Board Dimensions: 4.25” W x 2.75” L x 1” H (108mm x 70 mm x 24.6mm)
- Enclosure Dimensions: 8-1/4”H x 7-1/2W” x 3-1/2” D
- Power requirements: 12 – 24 VDC (supplied from **lite blue** or external Power Supply)

> **Warning:** Input Power is passed directly to the Reader Head Terminal.
> If the Reader Head Terminal is used to power the reader head, verify that the VRI-1 input voltage is within the allowable range for the specific reader head connected.

- Power consumption: 50 - 150mA max (depending on input voltage)
- Ambient temperature: 0º to 49º C or 32º to 120º F

VRI-1 Enclosure

VRI-1 Enclosure – An enclosure with a hinged, screw-down door is included for each VRINX board. Tamper switch, lock and key are available options.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8 1/4” x 7 1/2” x 3 1/2”

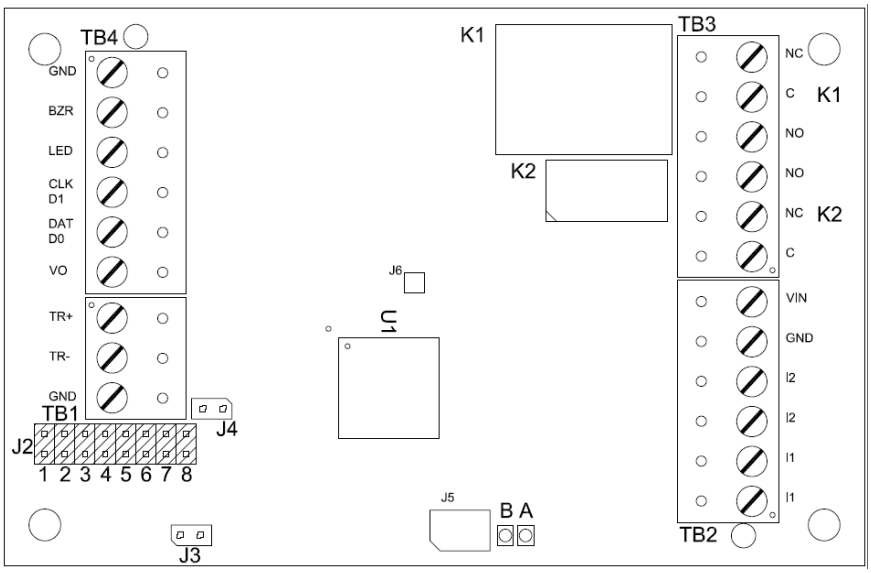
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting the enclosure

- Field Wiring – It is recommended that you drill holes or punch the knockouts in the metal enclosure for field wiring before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4” x 1” lag bolts.

VRI-1 Pin Layout



VRI-1 Configuration

The VRI-1 will be connected to the **lite blue** via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one **lite blue** data channel. Wire runs are limited to 4,000 feet (Data Only) from the **lite blue** to a VRI-1 (*see Recommended Wire Chart*). Data communication between **lite blue** and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration, each VRI-1 board is connected to any one of the Device connectors (Device 1-1 through 2-16) on the **lite blue** controller with TB1 for RS-485 communications and TB2 for power on a VRI-1 in parallel. A maximum of 16 VRI-1 boards can be connected to each channel in this manner.

Note: Only identical protocol devices can be connected on the same channel on the **lite blue**. VRI-1 devices cannot be wired on the same data channel with any older Vanderbilt or Schlage devices.

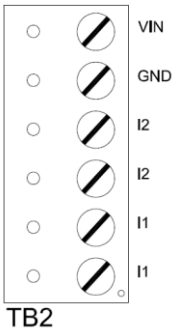
Daisy chain configuration

In a daisy chain configuration, the VRI-1 reader interfaces are connected to one another in series. A maximum of 16 devices can be connected to a **lite blue** data channel. This configuration is not recommended by Vanderbilt; if a wire is broken in the loop, downstream devices will not communicate with **lite blue**.

VRI-1 Pin Functions

TB2 – Power source and contact inputs

Provides power to the VRI-1 from the power supply. 12 – 24 VDC 10% filtered power required. Two supervised or unsupervised contact inputs are provided, typically for DOD and REX monitoring. Contact inputs have individual grounds. Supervised door contacts support a maximum wire length of 1,000 ft. Unsupervised door contacts support a wire length of 2,000 ft.



TB2

- PIN 1 is Power (VIN)
- PIN 2 is Ground (GND)
- PIN 3 is Door Contact 2 (Normally Closed)
- PIN 4 is Door Contact 2 (Normally Closed)
- PIN 5 is Door Contact 1 (Normally Closed)
- PIN 6 is Door Contact 1 (Normally Closed)

J2 – VRI-1 Reader Interface Addressing

The address of the VR-1 is dependent on the position of jumpers on these pins. Please see the section on Addressing VRI-1 for more details.

J3 – On Board Tamper Connection

The enclosure tamper switch will be wired to the supplied tamper connector flying leads. Polarity is not a concern.

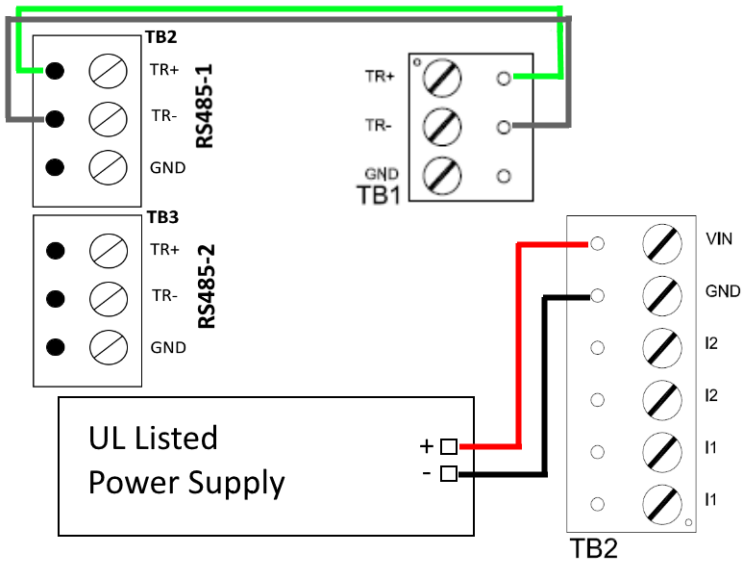
J4 – RS485 Communication Line Terminator

D1 (A) / D2 (B) – Status LEDs

- Powered Up: All LEDs OFF
- Initialization: LED A ON at start if initialization
- Runtime: LED A heartbeat and on-line status after successful initialization
  Offline: 1 Hz (20% ON)
  Online – Unencrypted: 1 Hz (80% ON)
  Online – Encrypted: 3X 0.1s ON, 0.1s OFF followed by 0.1s ON, 0.3s OFF
- Waiting for Firmware Download: LED A = 0.1s ON, 0.1s OFF
- Communication Status: LED B indicates RS485 communications activity.

Connecting to lite blue

Data communication between the **lite blue** controller and a VRI-1 reader interface is via RS-485 protocol. Either RS-485 channel on the **lite blue** controller can be used to communicate with TB1 for RS-485 communications. Use TB2 to supply power from the power supply to the VRI-1. The example below shows connections between TB2 (RS485-1) on the **lite blue** controller and TB1, TB2 on the VRI-1.

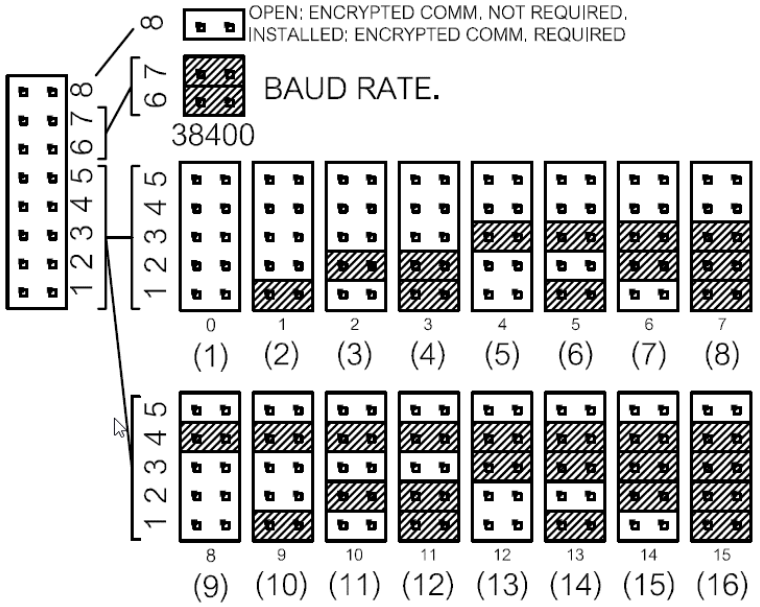


Data Communication between lite blue and VRI-1

lite blue	VRI-1	Power Supply
TB2 – TR+	TB1 PIN 1 – TR+	
TB2 – TR-	TB1 PIN 2 – TR-	
	TB2 PIN1 – VIN	+ (Power)
	TB2 PIN2 – GND	- (Ground)

Addressing the VRI-1

J2 on the VRI-1 consists of eight sets of jumpers that can be combined to set the address for the device, RS-485 communications baud rate and enable encryption. Record the jumper configured address of the VRI-1 and which channel it is connected to on the **lite blue** controller. This information will be required to set up the reader in **lite blue**.



Connecting to Read Head

The VRI-1 reader interface can communicate to many different read heads. Provided here are the PIN outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

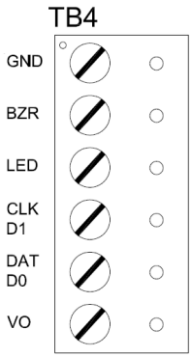
Recommended Wire Chart: VRI-1 to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VRI-1 to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VRI-1 to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VRI-1 to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VRI-1 to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

TB4 – Reader Head Connections



Ground (Black)

Buzzer (Not Used)

LED (Orange)

Clock / D1 (White)

Data / D0 (Green)

V0 (Red)

XCEED ID XF 1050 Proximity Reader

Proximity Read Head Pin Connections

VRI-1	Proximity Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (BZR)	NOT USED
PIN 3 (LED)	LED (ORANGE)
PIN 4 (CLK D1)	DATA 1 (WHITE)
PIN 5 (DAT D0)	DATA 0 (GREEN)
PIN 6 (V0)	POWER (RED)

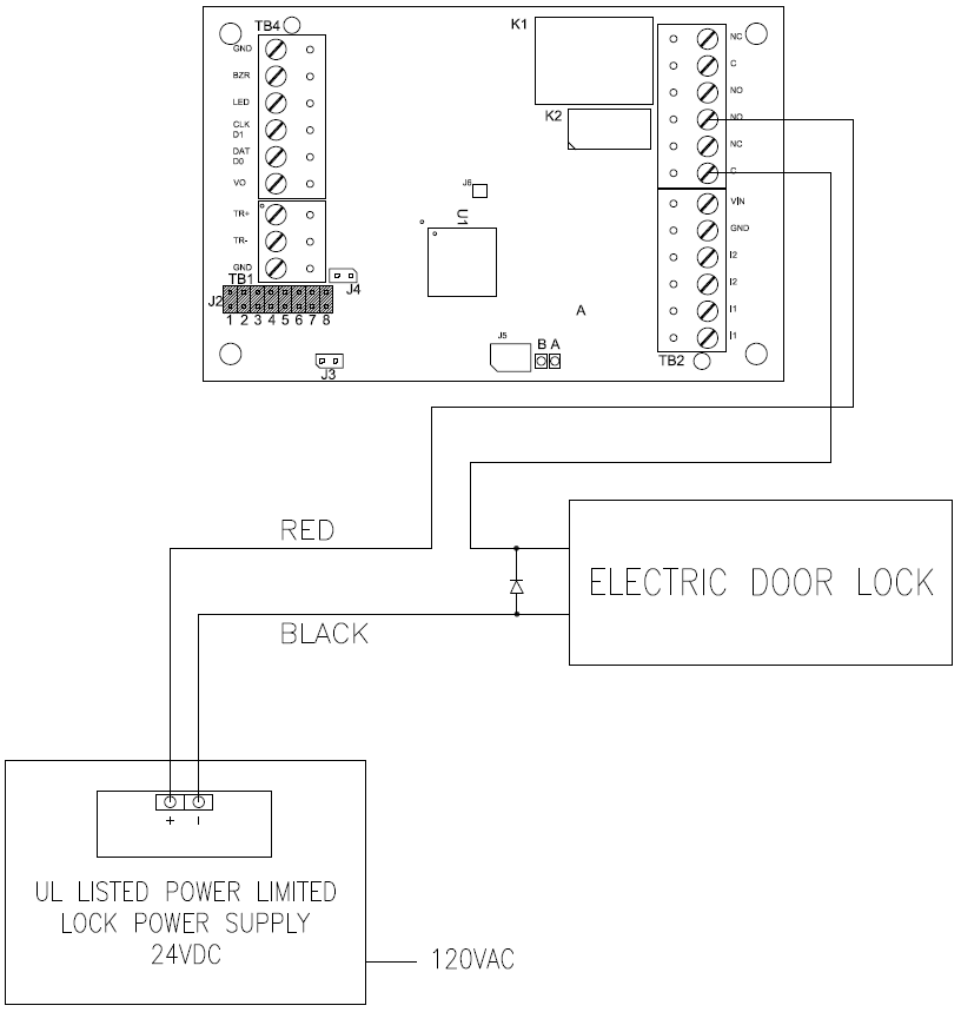
Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VRI-1	Magnetic Stripe Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (BZR)	NOT USED
PIN 3 (LED)	LED (ORANGE)
PIN 4 (CLK D1)	DATA 1 (GREEN)
PIN 5 (DAT D0)	DATA 0 (WHITE)
PIN 6 (V0)	POWER (RED)

Installing Diode for Lock Wiring - Relay

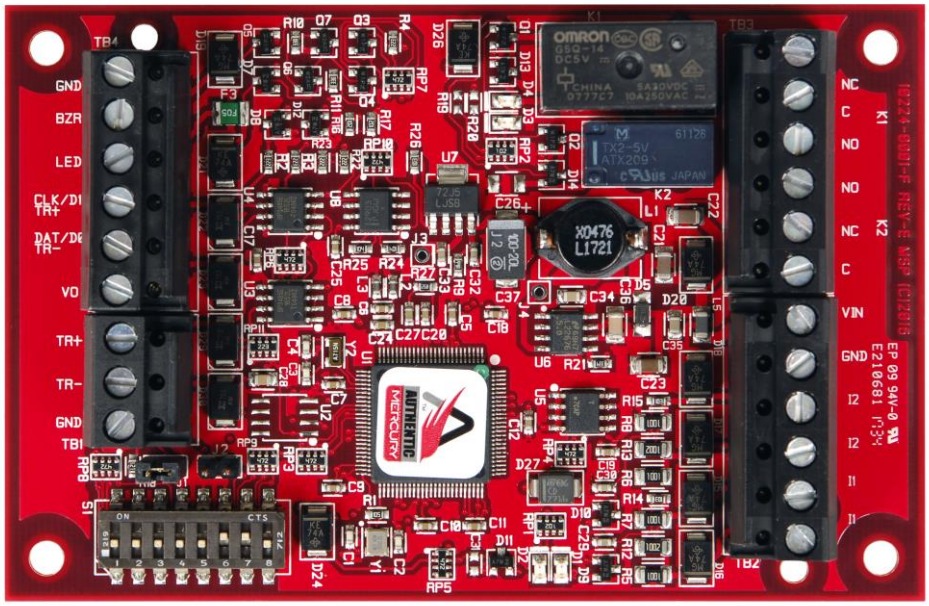
A diode is supplied with the VRI-1 which should be fitted across 12V / 24V and COM to protect the relay contacts.



A diode is used to eliminate the voltage spike seen across an inductive load when supply voltage is suddenly removed. This spike can damage the reader interface if not suppressed.

VRI-1S3

CHAPTER 8



Single Reader Interface – Series 3

Overview

The new VRI-1S3 is a Reader Interface between the **lite blue** and card readers. The VRI-1S3 works identically to the VRI-1, utilizing the SMS-M protocol. Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)
  - HID Corporate 1000 48-bit (not evaluated by UL)

- HID/ProxIF 37-Bit
- XceedID 40-Bit
- Vanderbilt 35-bit (including EV1)
- MiFare 32-Bit Serial Number

- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and **lite blue**
- Can be powered directly from **lite blue**
- **OPTIONAL -** can be powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.

Features

- Supports one read-head credential
- Connects directly to the communication channels on the **lite blue** controller via RS-485 protocol
- Two form C, single pole/double throw, 30 VDC mechanically latching relays:
  K1 rated @ 5A; K2 rated @ 1A
- Two supervised or unsupervised contact inputs with the ability to support a wide range of end-of-line resistor values
- Connection for one multi-color LED for access granted or access denied indication
- Connector for one buzzer/annunciator

Specifications

- Board Dimensions: 4.25” W x 2.75” L x 1” H (108mm x 70 mm x 24.6mm)
- Enclosure Dimensions: 8-1/4”H x 7-1/2W” x 3-1/2” D
- Power requirements: 12 – 24 VDC (supplied from **lite blue** or external Power Supply)

> **Warning:** Input Power is passed directly to the Reader Head Terminal.
> If the Reader Head Terminal is used to power the reader head, verify that the VRI-1 input voltage is within the allowable range for the specific reader head connected.

- Power consumption: 50 - 150mA max (depending on input voltage)
- Ambient temperature: 0º to 49º C or 32º to 120º F

Enclosure

VRI-1S3 Enclosure – An enclosure with a hinged, screw-down door is included for each VRI-1S3 board. Tamper switch, lock and key are available options.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 8 1/4” x 7 1/2” x 3 1/2”

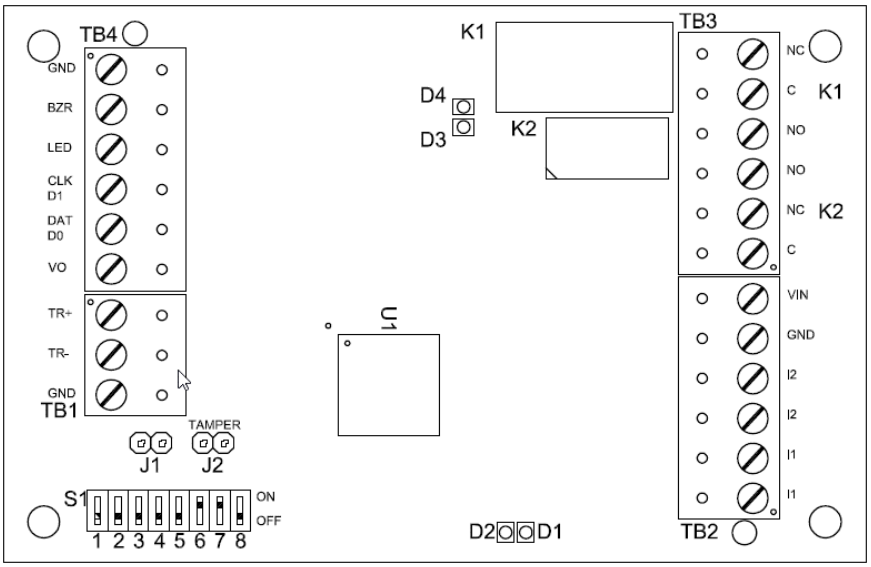
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting the enclosure

- Field Wiring – It is recommended that you drill holes or punch the knockouts in the metal enclosure for field wiring before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4” x 1” lag bolts.

PIN Layout



Configuration

The VRI-1S3 will be connected to the **lite blue** via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one **lite blue** data channel. Wire runs are limited to 4,000 feet (Data Only) from the **lite blue** to a VRI-1S3 (*see Recommended Wire Chart*). Data communication between **lite blue** and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration, each VRI-1S3 board is connected to any one of the Device connectors (Device 1-1 through 2-16) on the **lite blue** controller with TB1 for RS-485 communications and TB2 for power on a VRI-1S3 in parallel. A maximum of 16 VRI-1S3 boards can be connected to each channel in this manner.

Note: Only identical protocol devices can be connected on the same channel on the **lite blue**. VRI-1S3 devices cannot be wired on the same data channel with any older Vanderbilt or Schlage devices.

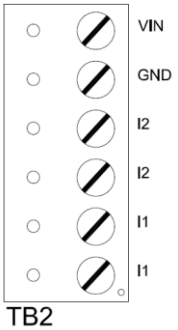
Daisy chain configuration

In a daisy chain configuration, the VRI-1S3 reader interfaces are connected to one another in series. A maximum of 16 devices can be connected to a **lite blue** data channel. This configuration is not recommended by Vanderbilt; if a wire is broken in the loop, downstream devices will not communicate with **lite blue**.

PIN Functions

TB2 – Power source and contact inputs

Provides power to the VRI-1S3 from the **lite blue**. 12 – 24 VDC 10% filtered power required. Two supervised or unsupervised contact inputs are provided, typically for DOD and REX monitoring. Contact inputs have individual grounds. Supervised door contacts support a maximum wire length of 1,000 ft. Unsupervised door contacts support a wire length of 2,000 ft.



TB2

- PIN 1 is Power (VIN)
- PIN 2 is Ground (GND)
- PIN 3 is Door Contact 2 (Normally Closed)
- PIN 4 is Door Contact 2 (Normally Closed)
- PIN 5 is Door Contact 1 (Normally Closed)
- PIN 6 is Door Contact 1 (Normally Closed)

J2 – Reader Interface Addressing

The address of the VR-1S3 is dependent on the position of jumpers on these pins. Please see the section on Addressing VRI-1S3 for more details.

J3 – On Board Tamper Connection

The enclosure tamper switch will be wired to the supplied tamper connector flying leads. Polarity is not a concern.

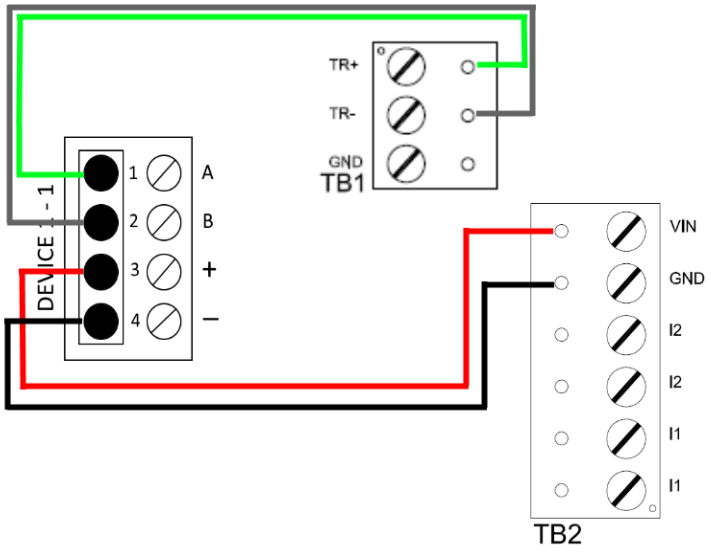
J4 – RS485 Communication Line Terminator

D1 (A) / D2 (B) – Status LEDs

- Powered Up: All LEDs OFF
- Initialization: LED A ON at start if initialization
- Runtime: LED A heartbeat and on-line status after successful initialization
  Offline: 1 Hz (20% ON)
  Online – Unencrypted: 1 Hz (80% ON)
  Online – Encrypted: 3X 0.1s ON, 0.1s OFF followed by 0.1s ON, 0.3s OFF
- Waiting for Firmware Download: LED A = 0.1s ON, 0.1s OFF
- Communication Status: LED B indicates RS485 communications activity.

Connecting to lite blue

Communication between the **lite blue** controller and a VRI-1S3 reader interface is via RS-485 protocol. Any one of the Device connectors (Device 1-1 through 2-16) on the **lite blue** controller can be used to communicate with TB1 for RS-485 communications and TB2 for power on a VRI-1S3. The example below shows connections between Device 1-1 on the **lite blue** controller and TB1, TB2 on the VRI-1S3.

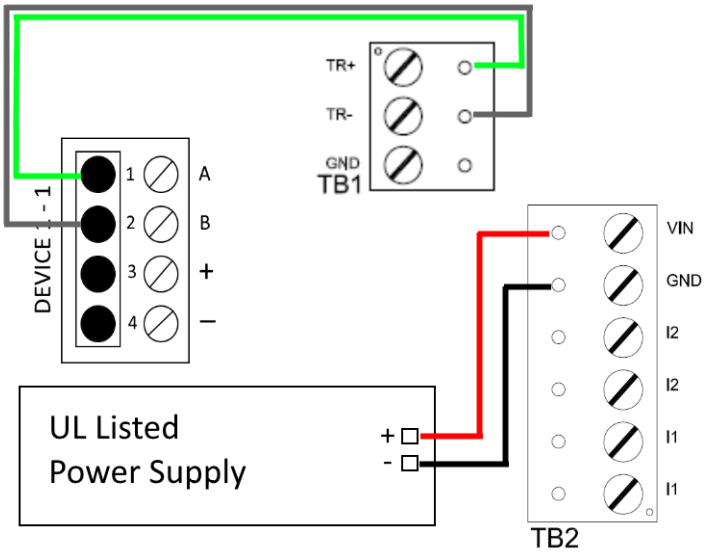


Data Communication between lite blue and VRI-1S3

lite blue	VRI-1S3
PIN 1 – A (Data A)	TB1 PIN 1 – TR+
PIN 2 – B (Data B)	TB1 PIN 2 – TR-
PIN 3 – + (Power)	TB2 PIN1 – VIN
PIN 4 – - (Ground)	TB2 PIN2 – GND

Optional - Powering Directly From a Power Supply

If desired, the VRI-1S3 can receive power directly from a UL 294 Listed Power Limited power supply. Communication between the **lite blue** controller and the VRI-1S3 remains via RS-485 protocol. Any one of the Device connectors (Device 1-1 through 2-16) on the **lite blue** controller can be used to communicate with TB1 on a VRI-1S3. Power will be supplied independently from the power supply to TB2 on the VRI-1S3.



Data Communication between lite blue and VRI-1S3

lite blue	VRI-1S3	Power Supply
PIN 1 – A (Data A)	TB1 PIN 1 – TR+	
PIN 2 – B (Data B)	TB1 PIN 2 – TR-	
	TB2 PIN1 – VIN	+ (Power)
	TB2 PIN2 – GND	- (Ground)

Addressing

S1 on the VRI-1S3 consists of eight slide switches that can be combined to set the address for the device, RS-485 communications baud rate and enable encryption. Record the switch configured address of the VRI-1S3 and which channel it is connected to on the **lite blue** controller. This information will be required to set up the reader in **lite blue**. The numbers in parenthesis are the **lite blue** device addresses.

	8	7	6	5	4	3	2	1
0 (1)	OFF	ON	ON	OFF	OFF	OFF	OFF	OFF
1 (2)	OFF	ON	ON	OFF	OFF	OFF	OFF	ON
2 (3)	OFF	ON	ON	OFF	OFF	OFF	ON	OFF
3 (4)	OFF	ON	ON	OFF	OFF	OFF	ON	ON
4 (5)	OFF	ON	ON	OFF	OFF	ON	OFF	OFF
5 (6)	OFF	ON	ON	OFF	OFF	ON	OFF	ON
6 (7)	OFF	ON	ON	OFF	OFF	ON	ON	OFF
7 (8)	OFF	ON	ON	OFF	OFF	ON	ON	ON
8 (9)	OFF	ON	ON	OFF	ON	OFF	OFF	OFF
9 (10)	OFF	ON	ON	OFF	ON	OFF	OFF	ON
10 (11)	OFF	ON	ON	OFF	ON	OFF	ON	OFF
11 (12)	OFF	ON	ON	OFF	ON	OFF	ON	ON
12 (13)	OFF	ON	ON	OFF	ON	ON	OFF	OFF
13 (14)	OFF	ON	ON	OFF	ON	ON	OFF	ON
14 (15)	OFF	ON	ON	OFF	ON	ON	ON	OFF
15 (16)	OFF	ON	ON	OFF	ON	ON	ON	ON

SWITCHES 6 & 7 DETERMINE THE BAUD RATE 38,400, DEFAULT: ON
SWITCH 8 DETERMINES ENCRYPTION, DEFAULT: OFF

Connecting to Read Head

The VRI-1S3 reader interface can communicate to many different read heads. Provided here are the PIN outs for the most commonly used read-heads. The connection is different for each reader type. See the Recommended Wire Chart below for the proper wire type and lengths.

.

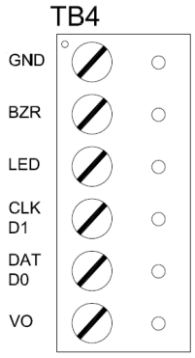
Recommended Wire Chart: VRI-1S3 to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VRI-1 to Magstripe Reader Head	200	22 AWG/5 Cond, Strd, Shld
VRI-1 to Proximity Reader Head	500	22 AWG/5 Cond, Strd, Shld
VRI-1 to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VRI-1 to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

- Cond. = Conductor
- Strd. = Stranded
- Shld. = Shielded

TB4 – Reader Head Connections



Ground (Black)

Buzzer (Not Used)

LED (Orange)

Clock / D1 (White)

Data / D0 (Green)

V0 (Red)

XCEED ID XF 1050 Proximity Reader

Proximity Read Head Pin Connections

VRI-1	Proximity Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (BZR)	NOT USED
PIN 3 (LED)	LED (ORANGE)
PIN 4 (CLK D1)	DATA 1 (WHITE)
PIN 5 (DAT D0)	DATA 0 (GREEN)
PIN 6 (V0)	POWER (RED)

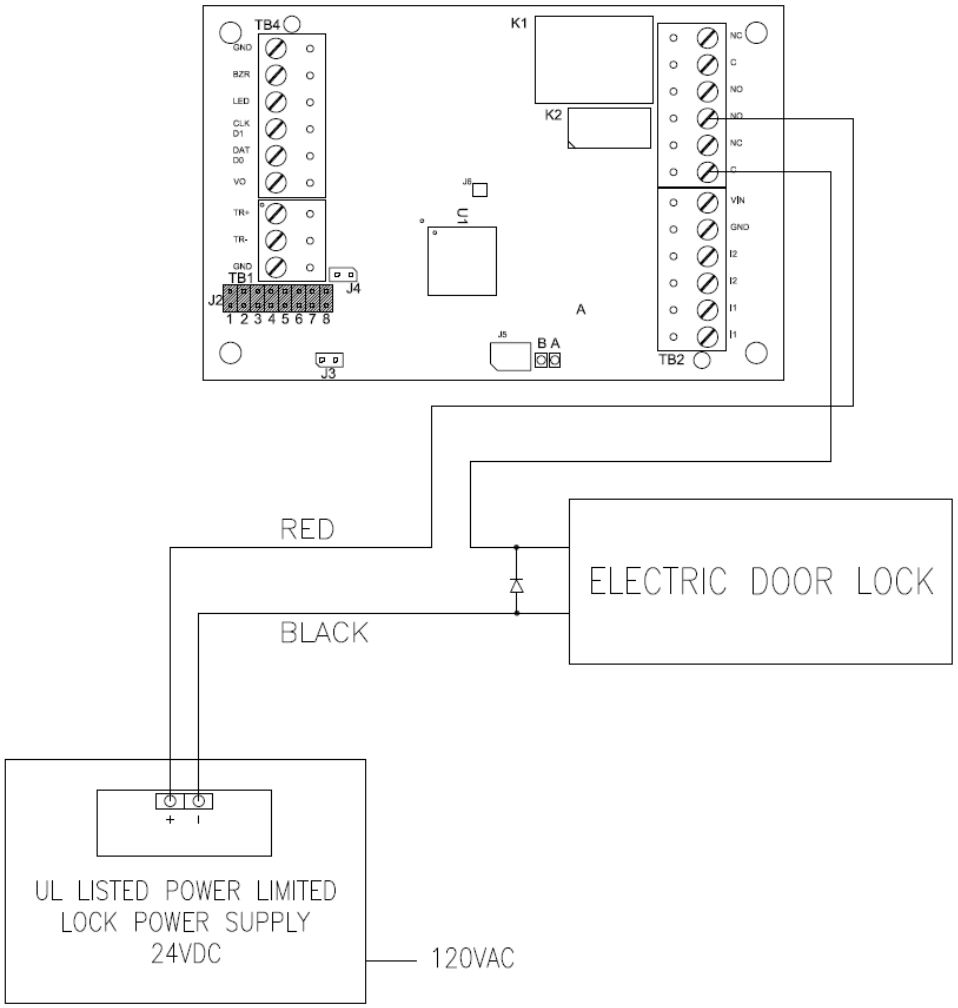
Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VRI-1	Magnetic Stripe Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (BZR)	NOT USED
PIN 3 (LED)	LED (ORANGE)
PIN 4 (CLK D1)	DATA 1 (GREEN)
PIN 5 (DAT D0)	DATA 0 (WHITE)
PIN 6 (V0)	POWER (RED)

Installing Diode for Lock Wiring - Relay

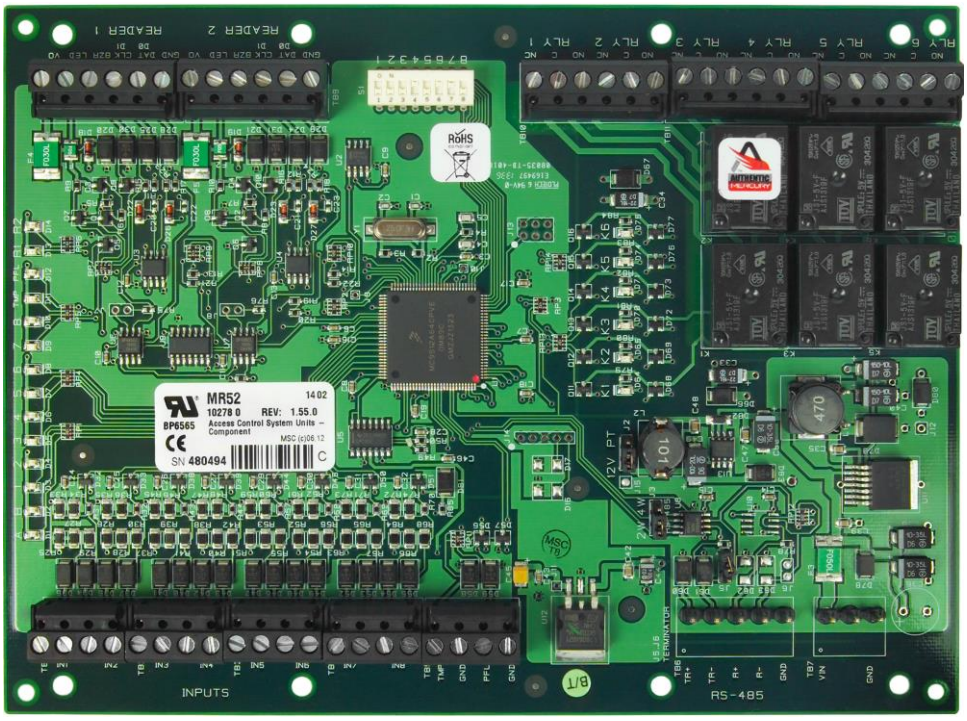
A diode is supplied with the VRI-1S3 which should be fitted across 12V / 24V and COM to protect the relay contacts.



A diode is used to eliminate the voltage spike seen across an inductive load when supply voltage is suddenly removed. This spike can damage the reader interface if not suppressed.

VRI-2 / VRI-2S3

CHAPTER 9



Dual Reader Interface

Overview

The VRI-2 (green) and VRI-2S3 (red – series 3) are Reader Interfaces between the **lite blue** and card readers. The VRI-2 and VRI-2S3 function identically and will be referred to as VRI-2. The VRI-2 works similarly to the VRINX but utilizes a new SMS-M protocol and supports 2 card reader connections. Reader Interfaces can connect to a variety of different read head technologies supported by **lite blue**. These include both Magnetic Stripe (not evaluated by UL) and Proximity readers.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format) and Magnetic Stripe (not evaluated by UL)
  - Standard 26-bit
  - Vanderbilt 34-bit
  - Xceed-ID XF1050 Reader
  - HID Corporate 1000 35-bit (not evaluated by UL)

- HID Corporate 1000 48-bit (not evaluated by UL)
- HID/ProxIF 37-Bit
- XceedID 40-Bit
- Vanderbilt 35-bit (including EV1)
- MiFare 32-Bit Serial Number

- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and **lite blue**
- Can be powered directly from **lite blue**
- **OPTIONAL -** can be powered locally by a UL294 Listed Power-Limited, Power Supply capable of 4 hours standby power.

Features

- Supports two read-head connections
- Connects directly to the communication channels on the **lite blue**
- Includes six 5 amp, form C, single pole/double throw, mechanically latching relays
- Eight supervised or unsupervised contact inputs with the ability to support a wide range of end-of-line resistor values when supervision is being used.
- Connection for one multi-color LED for access granted or access denied indication
- Connector for one buzzer/annunciator

Specifications

- Board Dimensions: 6” W x 8” L x 1” D (152 mm x 203 mm x 25 mm)
- Enclosure Dimensions: 10” H x 12” W x 3-1/2” D
- Power requirements: 12 – 24 VDC (supplied from the **lite blue** or external power supply)
- Power consumption: 270 – 450mA (depending on input voltage plus nominal reader current to 550 mA)
- Ambient temperature: 0º to 70º C or 32º to 158º F

Enclosure

VRI-2 Enclosure – An enclosure with a hinged, screw-down door is included for each VRI-2 board. Tamper switch, lock and key are available options.

Features

- Metal enclosure with hinged door
- Enclosure Dimensions: 10” H x 12” W x 3-1/2” D

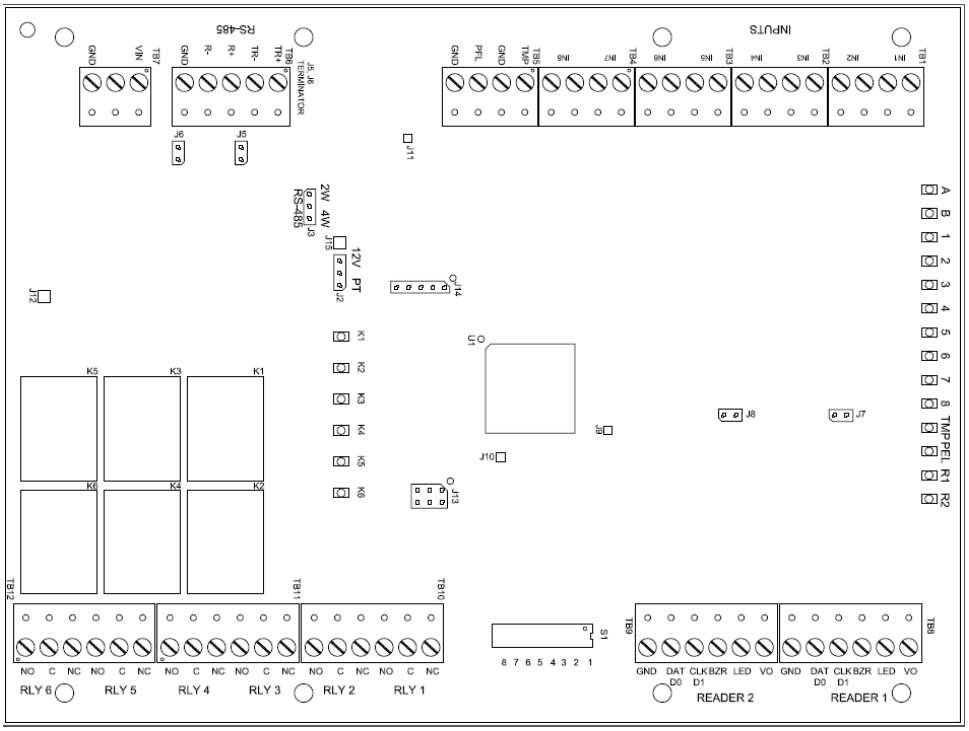
Environmental conditions

- Ambient Temperature: 0º to 70º C or 32º to 158º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting the enclosure

- Field Wiring – It is recommended that you drill holes or punch the knockouts in the metal enclosure for field wiring before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4” x 1” lag bolts.

PIN layout



Configuration

The VRI-2 will be connected to the **lite blue** via RS-485 protocol. A maximum of 8 **reader interfaces** can be connected to one **lite blue** data channel. Wire runs are limited to 4,000 feet (Data Only) from the **lite blue** to a VRI-2 (*see Recommended Wire Chart*). Data communication between the **lite blue** and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration, a VRI-2 board is connected to either of the RS-485 connectors (TB2 Device 1-1 through 2-16) on the **lite blue** controller with TB6 for RS-485 communications and TB7 for power on a VRI-2 in parallel. A maximum of 8 **reader interfaces** (*4 VRI-2 boards if using both reader interfaces*) can be connected in this manner.

Note: Only identical protocol devices can be connected on the same channel on the **lite blue**. VRI-2 devices cannot be wired on the same data channel with any older Vanderbilt or Schlage devices.

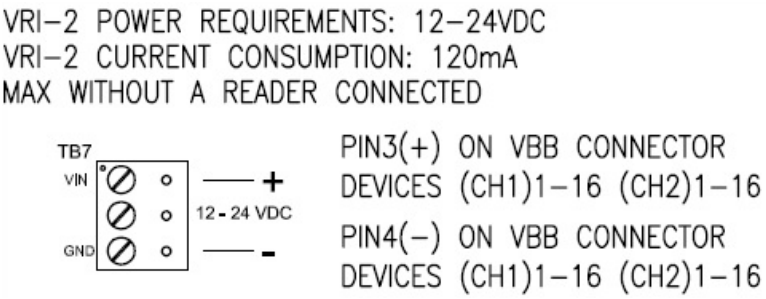
Daisy chain configuration

In a daisy chain configuration, the VRI-2 reader interfaces are connected to one another in series. A maximum of 8 ***reader interfaces*** (*4 VRI-2 boards if using both reader interfaces*) can be connected to a **lite blue**. This configuration is not recommended by Vanderbilt; if a wire is broken in the loop, downstream devices will not communicate with **lite blue**.

PIN Functions

TB7 - Power source

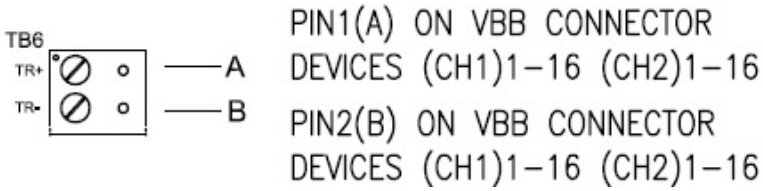
Provides power to the VRI-2 from the **lite blue**.



- PIN 1 is Power (VIN), 12 – 24 VDC
- PIN 2 unused
- PIN 3 is Ground (GND)

TB6 - Communications

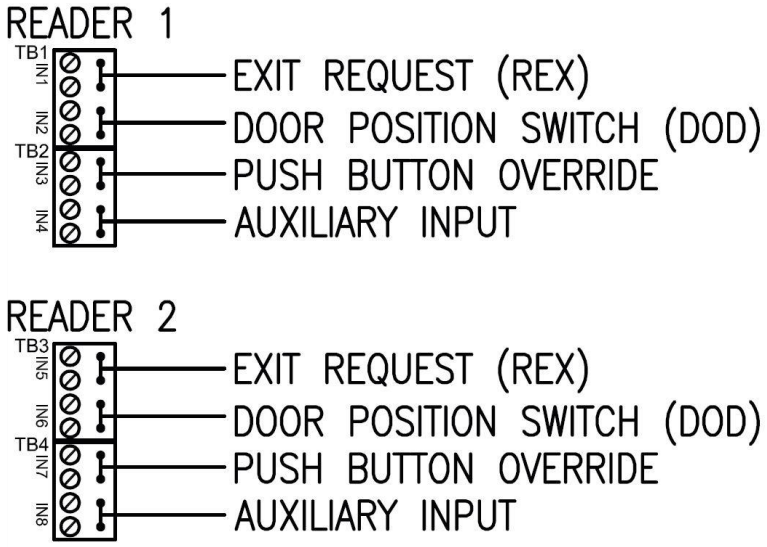
Provides RS-485 communications between the VRI-2 and the **lite blue**.



- PIN 1 is Data A (TR+)
- PIN 2 is Data B (TR-)

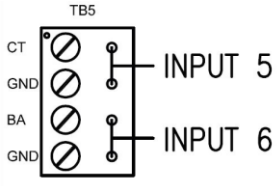
TB1 – TB5 Contact inputs

The VRI-2 has eight supervised or unsupervised contact points plus cabinet Tamper and UPS Fault Monitoring contact inputs (TB5).



Device Type:

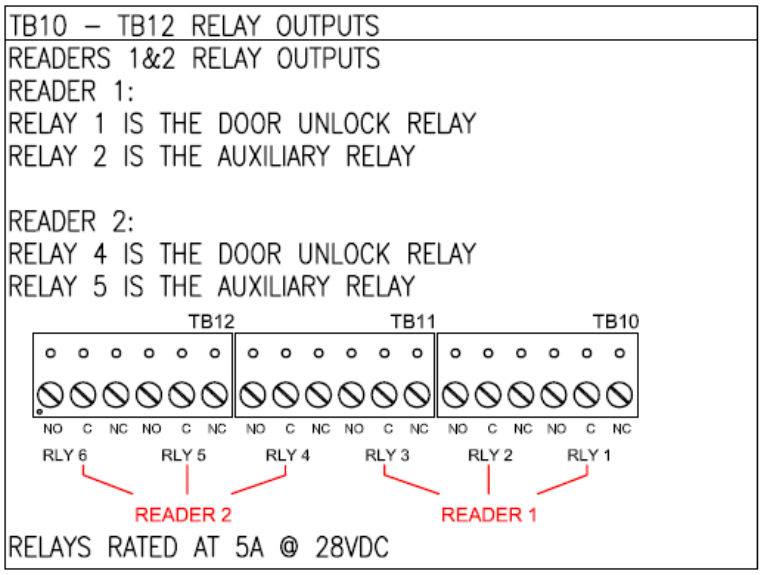
- DOD (supervised): max distance = 1,000 ft
- DOD (unsupervised): max distance = 2,000 ft



- Input 5 – Onboard Cabinet Tamper
- Input 6 – UPS Fault Monitoring

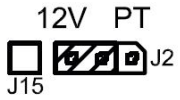
TB10 – TB12 Relay Outputs

The VRI-2 has six relay outputs.

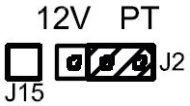


J15 – Read head voltage selector

12 VDC is available on Reader Ports (VIN >= 20 VDC):



VIN “Passed Through” to Reader Ports:



Serious damage may occur to the read-head if this jumper is set incorrectly. Please check the read-head voltage requirements.

S1 – VRI-2 Reader Interface Addressing

The address of the VRI-2 is dependent on the position of the DIP switches in S1.

The hardware address for each physical VRI-2 must be set to address 1 – 16 for use with **lite blue**. The first reader is assigned "A" and the second reader is assigned "B" *(i.e. 1A & 1B or 5A & 5B)*.

SMS Address	DIP Switch Position							
	8	7	6	5	4	3	2	1
(1)	OFF	ON	ON	OFF	OFF	OFF	OFF	OFF
(2)	OFF	ON	ON	OFF	OFF	OFF	OFF	ON
(3)	OFF	ON	ON	OFF	OFF	OFF	ON	OFF
(4)	OFF	ON	ON	OFF	OFF	OFF	ON	ON
(5)	OFF	ON	ON	OFF	OFF	ON	OFF	OFF
(6)	OFF	ON	ON	OFF	OFF	ON	OFF	ON
(7)	OFF	ON	ON	OFF	OFF	ON	ON	OFF
(8)	OFF	ON	ON	OFF	OFF	ON	ON	ON
(9)	OFF	ON	ON	OFF	ON	OFF	OFF	OFF
(10)	OFF	ON	ON	OFF	ON	OFF	OFF	ON
(11)	OFF	ON	ON	OFF	ON	OFF	ON	OFF
(12)	OFF	ON	ON	OFF	ON	OFF	ON	ON
(13)	OFF	ON	ON	OFF	ON	ON	OFF	OFF
(14)	OFF	ON	ON	OFF	ON	ON	OFF	ON
(15)	OFF	ON	ON	OFF	ON	ON	ON	OFF
(16)	OFF	ON	ON	OFF	ON	ON	ON	ON

S1 DIP Switch 6 & 7 determine RS-485 communications baud rate: default = 38,400

S1 DIP Switch 8 determines RS-485 encryption: default = OFF

A – R2 Status LEDs

- Powered Up: All LEDs OFF
- Initialization: LEDs A – R2 Sequenced ON then OFF at completion of initialization
- Runtime: LED A heartbeat and on-line status after successful initialization
  Offline: 1 Hz (20% ON)
  Online – Unencrypted: 1 Hz (80% on)
  Online – Encrypted: 3X 0.1s ON, 0.1s OFF followed by 0.1s ON, 0.3s OFF
- Waiting for Firmware Download: LED A = 0.1s ON, 0.1s OFF
- Communication Status: LED B indicates RS485 communications activity

- LED 1: IN1 Status
- LED 2: IN2 Status
- LED 3: IN3 Status
- LED 4: IN4 Status

SMS VR-2 Template Applied:

- LED 5: IN5 Status = Request to Exit
- LED 6: IN6 Status = Door Status Monitor
- LED 7: IN7 Status = Push Button Override
- LED 8: IN8 Status = Auxiliary Input (Report Status of Lockdown/Toggle)

- LED TMP: Cabinet Tamper
- LED PFL: Power Fault
- LED R1: Reader 1 Activity
- LED R2: Reader 2 Activity
- LED K1: Relay 1 Energized
- LED K2: Relay 2 Energized
- LED K3: Relay 3 Energized
- LED K4: Relay 4 Energized
- LED K5: Relay 5 Energized
- LED K6: Relay 6 Energized

LEDs A – R2 are continually pulsed to their opposite state for 0.1s under normal operation

Schlage Adaptable AD-300 Series Locks

CHAPTER 10

Schlage Adaptable AD-300 Series Lock

Overview

The AD-300 Lock is an integrated, modular lock that includes all the standard peripheral devices at a secured door opening. AD-300 Locks can be integrated directly into the **lite blue** controller. The communication protocol is RS-485 to any of the communication channels on the **lite blue** controller.

Features

- Connects directly to the **lite blue** controller via RS-485 protocol to one of the communication channels.
- Available with mortise, cylindrical lock and exit device trim.
- Available with (HID) proximity or magnetic stripe credential technologies.
- Integrated PIN pad allows for PIN+Credential access.

Specifications

- Power is received from the **lite blue** controller.
- Power Requirements - 12VDC or 24VDC
- Power Consumption - 300mA max.

Contacts and Pin Functions

A set of input contacts and output relays are provided on the Schlage Adaptable AD-300 Series locks.

Input Contacts

- Request to Exit (REX), normally open, non-supervised
- Door Open Detect (DOD), normally open, non-supervised
- Clutch Position, normally closed, non-supervised
- Key Switch, normally closed, non-supervised
- Interior Push Button, normally open, non-supervised
- Lithium Battery

Credential Reader Technologies

- HID Proximity Credential
- Magnetic Stripe Credential

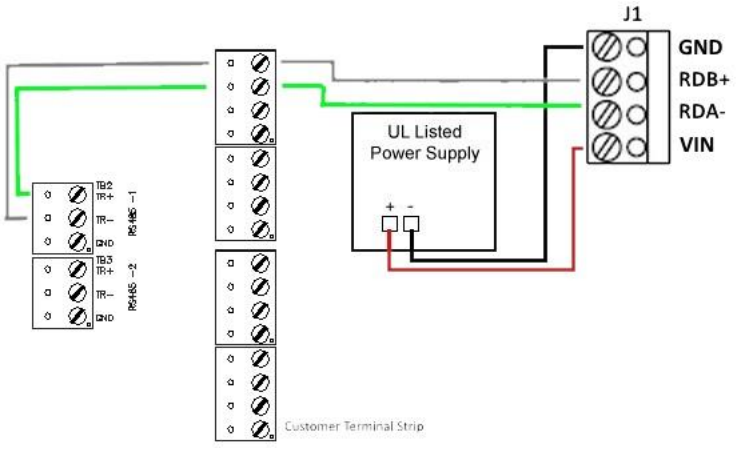
J3 & J4 - RS-485 termination. This jumper must be in place to enable communication between the AD300 lock and **lite blue**.

J1 - Power source and communication. Used to connect **lite blue** to the AD300 lock.

SW1 - Tamper Switch

Connecting to lite blue

Communication between the **lite blue** controller and an AD-300 lock is via RS-485 protocol. Either RS-485 channel on the **lite blue** controller can be used to communicate with J1 on an AD-300 lock. The below example is using RS485-1 on the **lite blue** controller and J1 on the AD-300 lock.



Data Communication and Power between lite blue and AD-300

lite blue	AD-300	Power Supply
RS-485-1 TR+	RDA- (Data A)	
RS-485-1 TR-	RDB+ (Data B)	
	VIN (Power)	+ (Power)
	GND (Ground)	- (Ground)

Addressing the AD-300 Lock

The AD-300 lock is addressed using the Schlage Utility Software (SUS), which is run from the Pideon PDA. The address used by the AD-300 locks go from 0 to 15. **lite blue** uses an address list of 1 through 16. When addressing an AD-300 lock it is important to remember this. An address of 0 for the AD-300 lock equals an address of 1 in **lite blue**. It is recommended that the set address correspond to the slot on the **lite blue** controller that the AD-300 lock is connected to, minus one number. The Channel number is not affected by this.

Example: The AD-300 lock is connected to the **lite blue** controller at Device 1-2 (Channel 1, Address 2) then the address of the AD-300 lock should be set to 1. If the AD-300 is connected to Device 2-10 (Channel 2 Address 10) then the address should be set to 9.

lite blue Address	SUS Address
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

lite blue Address	SUS Address
9	8
10	9
11	10
12	11
13	12
14	13
15	14
16	15

After the AD-300 has been connected to the **lite blue** controller, make a note of the channel and address. This information will be required to set up the lock in the software.

For additional information on the Schlage Utility Software see the **Schlage Utility Software User's Guide**.

To address the AD-300 lock:

1. Click **Start** on the PDA. A Menu will open with a list of programs.
2. Select the **Schlage Utility Software** option to open **SUS**.
3. Select **Manager** from the **Log on as** drop down menu.
4. Enter the password into the **Password** field. Default password is **123456**

5 Click the **Login** button. The SUS program will open. The bottom of the screen will say **No Device Connected.**

6 Connect the PDA to the AD-300 lock using the supplied USB cable.

7 Press the **Schlage** button twice on the AD-300 keypad. The bottom of the PDA screen will now display AD300.

8 Click on the **Options** button at the bottom of the PDA screen. A list of options will open.

9 Put the AD-300 lock into **Pairing Mode** (this is necessary for the PDA to be able to make changes to the lock's settings).

10 Hold down the **Internal Push Button** on the AD-300 lock.

11 While holding down the **Internal Push Button**, click the **Tamper Switch (SW1)** three times on the AD-300 lock. The red LEDs in the Schlage button will flash.

12 On the PDA click the **Pair PDA to Device** option. A pop-up will display when the pairing process is complete.

13 Click on the **Lock Properties** option.The Lock Properties window will open.

14 Click on the **Edit** tab.

15 Click on the **RS485 Address** field. A touch-keyboard will open at the bottom of the screen.

16 Using the touch-keyboard, enter in the address of the lock.

17 Click on the **Save** button at the bottom of the screen. After a moment the **Properties Saved Successfully** pop-up will open.

18 Either click **OK** on the pop-up, or wait a moment and it will close on its own. The lock has been addressed.

19 Make a note of the address, it will be required to set up the lock in the software.

Schlage VIP Locks

CHAPTER 11

VIP Lock

Overview

The Schlage VIP Lock is an integrated, modular lock that includes all the standard peripheral devices at a secured door opening. VIP Locks can be integrated directly into the **lite blue** controller. The communication protocol is RS-485 to any of the communication channels on the **lite blue** controller.

Features

- Connects directly to the **lite blue** controller via RS-485 protocol to one of the communication channels.
- Available with mortise, cylindrical lock and exit device trim.
- Available with (HID) proximity or magnetic stripe credential technologies in a variety of finishes and lever styles.

Specifications

- Power is received from the **lite blue** controller.
- Power Requirements - 12VDC or 24VDC
- Power Consumption - 1.1A @ 12VDC or 600mA @ 24VDC

Contacts, Relays, and Pin Functions

A set of input contacts and output relays are provided on the Schlage VIP Lock. The locks can be ordered with integrated credential readers.

Input Contacts

- Request to Exit (REX), normally open, non-supervised
- Door Open Detect (DOD), normally open, non-supervised
- Latch bolt monitor (LBM), normally closed, non-supervised
- Key position, normally closed, non-supervised
- Spare

Output Relays

- Solenoid for door strike
- Red Led Control
- Green Led Control
- Beeper Control

Credential Reader Technologies

- HID Proximity Credential
- Magnetic Stripe Credential

JP1 - RS-485 termination. This jumper must be removed to enable communication between VIP and **lite blue**.

J3 - Power source and communication. Used to connect **lite blue** to the VIP.

J6 - Not used.

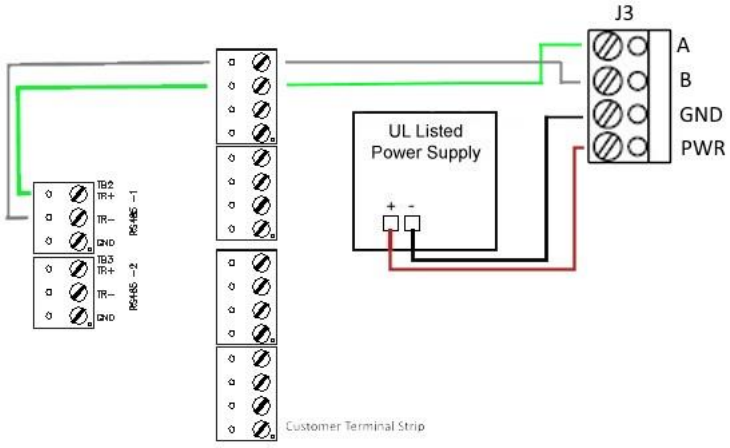
Dip Switches

- **1-4** - Used for addressing the VIP. See the Addressing the VIP section for details.
- **5** - Used to choose between Fail Secure and Fail Safe
  - OFF - Fail Secure (FSE)
  - ON - Fail Safe (FSA)
- **6** - Used to choose between magstripe and proximity reader.
  - OFF - Magstripe Reader
  - ON - Proximity Reader
- **7** - Used to set protocol type. To communicate with lite blue this must be switched to ON.
  - OFF - VIP protocol
  - ON - 'F' series protocol

Note: Dip Switch 7 MUST be switched to the ON position for the VIP lock to work with **lite blue**.

Connecting to lite blue

Communication between the **lite blue** controller and a VIP lock is via RS-485 protocol. Either RS-485 channel on the **lite blue** controller can be used to communicate with J3 on a VIP lock. The below example is using RS485-1 on the **lite blue** controller and J3 on the VIP lock.



Data Communication and Power between lite blue and VIP

lite blue	VIP	Power Supply
RS-485-1 TR+	Pin 4 – A (Data A)	
RS-485-1 TR-	Pin 3 – B (Data B)	
	Pin 1 – PWR (Power)	+ (Power)
	Pin 2 – GND (Ground)	- (Ground)

Note: For **lite blue** to communicate with a Schlage VIP Lock, the jumper at JP1 on the VIP lock must be removed and dip switch 7 must be switched to ON.

Addressing the VIP Lock

There are a set of 12 dip switches on the VIP lock, the first four of which are used to set the address for the device. It is recommended that the set address correspond to the slot on the **lite blue** controller it is connected to. For example, if the VIP is connected to the **lite blue** controller at Device 1-2 (Channel 1, Address 2) then the switches on the VIP should equal 2. If the VIP is connected to Device 2-10 (Channel 2 Address 10) then the dip switches should equal 10.

After the VIP has been connected to the **lite blue** controller, make a note of the address. This information will be required to set up the lock in the software.

Note: Only the first 4 switches are used for addressing.

VIP Address Chart

VIP Address	Switch 1	Switch 2	Switch 3	Switch 4
1	Off	Off	Off	Off
2	On	Off	Off	Off
3	Off	On	Off	Off
4	On	On	Off	Off
5	Off	Off	On	Off
6	On	Off	On	Off
7	Off	On	On	Off
8	On	On	On	Off
9	Off	Off	Off	On
10	On	Off	Off	On
11	Off	On	Off	On
12	On	On	Off	On
13	Off	Off	On	On
14	On	Off	On	On
15	Off	On	On	On
16	On	On	On	On

Schlage Adaptable AD-400 Series

CHAPTER 12

Schlage Adaptable AD-400 Series Lock

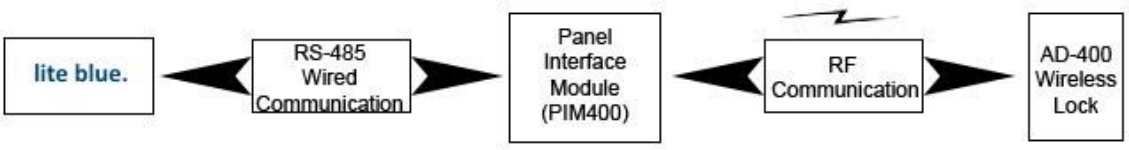
Overview

Schlage wireless devices can be seamlessly integrated to your lite blue system. The PIM400-485-VBB communicates directly to the lite blue controller via RS-485 protocol and can support up to 16 Schlage AD-400 Series locks. Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Schlage AD-400 Components

The Schlage AD-400 Series wireless system contains two different types of modules:

- One wireless panel interface module (PIM400)
- One wireless lock (AD-400)



The PIM400 (PIM400-485-VBB) is hard wired to the **lite blue** communication channels via RS-485 protocol. The PIM400 installation location is determined by the location of the AD-400 lock with which it will communicate via radio frequency (RF).

The AD-400 lock is installed at the access point where access will be controlled and/or monitored.

Schlage AD-400 Series Wireless modules

The two components of the AD-400 Series locks, the PIM400 and the AD-400 lock, are detailed in the following sections.

Panel Interface Module (PIM400-485-VBB)

The PIM400-485-VBB can be integrated with the **lite blue** system, it works in conjunction with the AD-400 Locks. The PIM400-485-VBB module is hard wired directly to lite blue communication channels and communicates via RS-485 protocol. The PIM400-485-VBB can support up to 16 AD-400 locks (8 locks on **lite blue**).

NOTE: When accessing the PIM400-485-VBB with the SUS the device may be labeled as "PIM400-485-SBB" which does not affect programming of the device and should be ignored.

The PIM400 is capable of configuring, via the Schlage Utility Software (SUS), the following items:

- Heartbeat interval
- Relock time
- Card format type
- Extended unlock
- Polarity of status signals
- Latch type
- Query intervals and quantity for unlock requests
- Cache mode
- Lock state in case of RF communication loss
- Relock action (timer only, door open or timer or door closed or timer card code conversions)
- Frequency agility for increased interference immunity
- Addressing

Card formats

- The PIM400-485-VBB accepts card formats up to 255 bits.

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 20% RH to 95% RH (non-condensing)
- Operating Voltage: 12 to 24 VDC (Powered from **lite blue** or locally)
- Power consumption: 300mA max.

Radio frequency (RF) - The PIM400 includes an RF Transceiver

- Spread spectrum
- Direct sequencing spread spectrum
- Frequency: 902-928 MHz
- Data Rate: 62.5 kbps (half duplex)
- Modulo 256 error detection
- Selectable channels: 1 of 15 standard; 5 groups of 3 increased interference immunity (configurable)
- Approvals: FCC and RSS-210 (Canada)
- Transmitter Power: Up to 300mW
- Receiver Sensitivity: 90dBM typical

Specifications for the PIM400-485-VBB

- RS-485 Communication to **lite blue** controller
- Supports 16 Wireless Devices
- No SRINX is required
- **lite blue** can support multiple PIM400-485-VBB

AD-400 Series Wireless Locks

Schlage AD-400 Series locks contain all of the elements needed to electronically control and monitor access through a door via an RF link. The lock includes a lockset, a Request-to-Exit sensor/switch, a Request-to-Enter sensor/ switch, a power supply (battery pack), and terminals for monitoring a clutch position switch/sensor, a card reader, and an RF transceiver for communicating with another RF transceiver in a Panel Interface Module (PIM400) which then interfaces to **lite blue**.

Performance

- Verification Time: Typically 0.2 seconds including lock actuation time but not including access panel delays
- Communications (Heartbeat)
- Wake Up on Radio - Allows the PIM400 to alert the AD-400 locks in case of a Lockdown event.
- Addressing

Card reader - Magnetic Stripe Card Reader

- ANSI/BHMA A156.25 compliant Track 2 Clock & Data Output (Some card code conversions available)
- Read Rate - 3 – 50 inches per second
- Card Thickness - 0.030 inches thick
- ANSI/ISO Standards 7810, 7811 1/51 7812, and 7813

Card Reader - Proximity Reader

- ANSI/BHMA A156.25 compliant
- Compatible with HID proximity cards
- Wiegand output
- Card Read Range: up to 4 inches
- Compliance to FCC Part 15, RSS-210 of Industry Canada
- ESD Protection: 12KV

Card formats -Can read all card formats up to 255 bits.

Request-to-exit - The sensor/switch is built-in and will be triggered from the activation of the door lever on the protected side of the door.

Request-to-enter - The sensor/switch is built-in as a momentary switch on the lock.

Clutch Position - Schlage AD-400 locks provide a way to lock or unlock a door and monitor access from a remote location. Schlage AD-400 locks are fail-safe from the protected side of the door.

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 20% RH to 95% RH (non-condensing)

Power source

The Schlage AD-400 lock uses 4 or 8 AA alkaline battery packs. Optionally can be powered by 12VDC or 24VDC.

Operating voltage

- Power Requirements (Battery): 4 AA batteries that will supply 6.2 volts.
  - The locks will continue to operate down to 4.5 volts before reaching a Low Battery state.
  - At 4.0 volts the lock reaches a battery critical state and will shut down and go into a failsafe or fail lock mode depending on what the operations in the SUS have been set to.
- Power Requirements (wired): 12 to 24VDC
- Current Requirements: Standby: 55 micro Amps typical (Proximity version)
- Power consumption: 300mA max.
- Battery Life - Up to 2 years with 4AA (8AA option available for extended battery life)

Range - The Schlage AD-400 Lock can have a range up to 200 feet on one floor when used in normal office interior construction and up to 1000 feet line of sight.

- Transmitter Power - Up to 200 mW
- Receiver Sensitivity - 90dBm typical
- Wiegand technology to external reader

WRI400

The WRI400 is a networked access point controller that communicates with **lite blue** via RF through a mating Panel Interface Module (PIM400-485-VBB). It is designed to provide wireless connectivity to electronic access control components including credential readers, door position and request to exit switches.

Performance

- Verification Time - Less than 0.10 second (not including panel delays)
- Communications (Heartbeat) Interval - Configurable in 1 second increments from 1 second to 18 hours. Heart Beat can be set to 1 second for override operation
- Features - Tamper Switch, Door Status Monitoring, Door Strike Relay, Aux Relay, and 2 Reader Head operation.
- Inputs - Request-to-Enter, Request-to-Exit, Door Position Switch, Reader Tamper 1, Reader Tamper 2
- Addressing

Card formats

- Accepts card formats up to 255 bits.

Operational environment

- Temperature - -31ºF (-35ºC) to 151ºF (66ºC)
- Humidity - 0 - 100% condensing

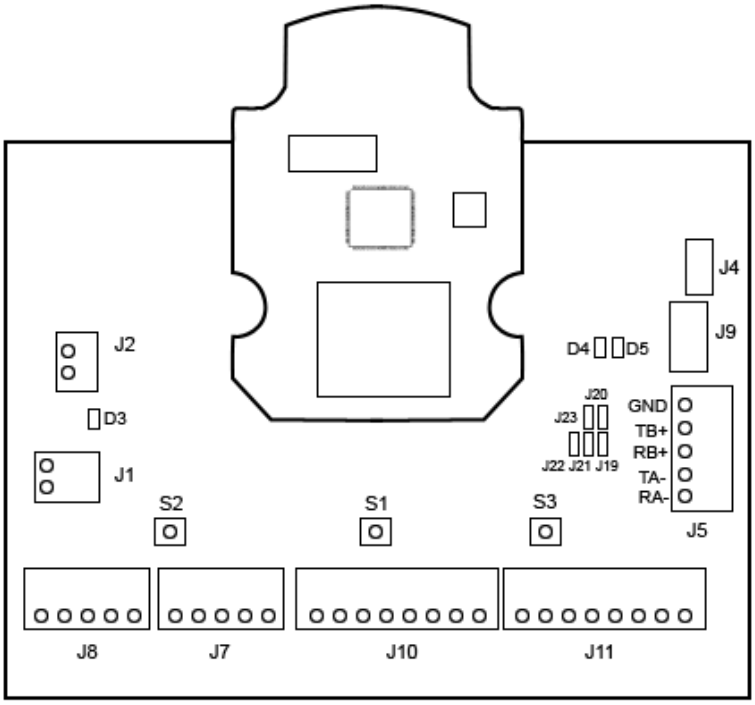
Power source

- Power Requirements - 12 VDC or 24 VDC; 500 mA maximum current

Radio Frequency (RF) - The PIM includes an RF Transceiver.

- Optional Dynamic Channel Switching
- 900 MHz spread spectrum, direct sequence, 10 channels
- Frequency - 902-928 MHz
- Data Rate - RF: 40 kbps
- Modulo 256 error detection
- Encryption: AES-128 bit keys
- Approvals - FCC and RSS-210 (Canada)
- Transmitter Power - Up to 300mW
- Receiver Sensitivity - 90dBM typical
- Remote antenna modules - The PIM modules are capable of accommodating Remote Antenna Modules.

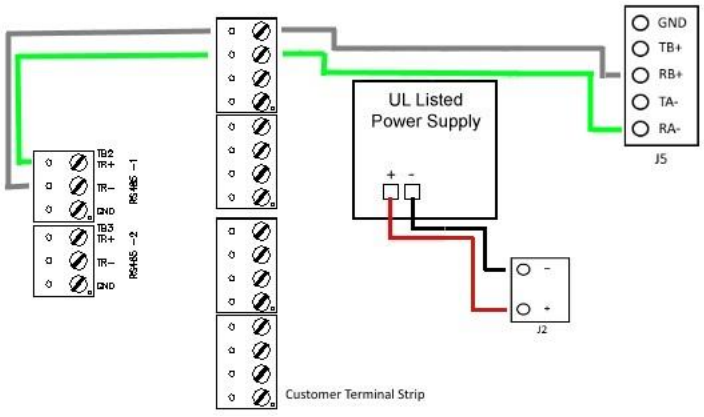
Wiring Instructions



The PIM400 must be powered separately from a local power supply. **lite blue** and the PIM400 communicate via RS-485 protocol.

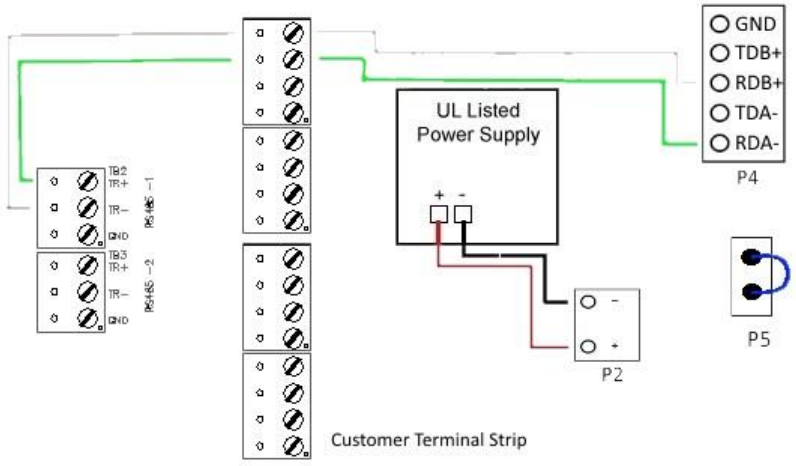
Wiring between lite blue and PIM400 (legacy)

The PIM receives power at J2 (powered locally) and data at J5. J5 has two pins for Data A and two pins for Data B. A jumper must be at J20 to combine the Data A pins and at J19 to combine the Data B pins. The below example is using RS485-1 on the **lite blue** board to J5 and J2 on the PIM400.



Wiring between lite blue and PIM400 (new)

The new, smaller form factor PIM400 receives power at P2 (powered locally) and data at P4. There is a 2/4 wire RS-485 communications jumper, P5 which must be ON (jumper installed) for 2-wire RS-485 communication on P4. The below example is using RS485-1 on the **lite blue** board to P4 and P2 on the PIM400.



Data Communication and Power between lite blue and PIM400

lite blue	PIM400 (legacy)	Power Supply
RS-485-1 TR+	J5 RA- (jumpered at J19)	
RS-485-1 TR-	J5 RB+ (jumpered at J20)	
	J2 Pin 2 - PWR (Power)	+ (Power)
	J2 Pin 1 - GND (Ground)	- (Ground)
lite blue	**PIM400 (new)**	**Power Supply**
RS-485-1 TR+	P4 RDA- (P5 Jumper ON)	
RS-485-1 TR-	P4 RDB+ (P5 Jumper ON)	
	P2 Pin 2 - PWR (Power)	+ (Power)
	P2 Pin 1 - GND (Ground)	- (Ground)

PIM400 Configuration

The Schlage Utility Software (SUS) located on the included PDA must be used to configure each PIM400-495-VBB. It is used to set the PIM400's address and the HIGH/LOW address range of the AD-400 locks that will be communicating with it.

NOTE: When accessing the PIM400-485-VBB with the SUS the device may be labeled as "PIM400-485-SBB" which does not affect programming of the device and should be ignored.

Initial set up of the PIM400 requires the following:

- Login to SUS
- Pair to PDA
- Set PIM400 Address

Log In to SUS

You must log in to the Schlage Utility Software (SUS) located on the included PDA. Follow the steps below to log in:

1. Click **Start** on the PDA. A Menu will open with a list of programs.
2. Select the **Schlage Utility Software** option to open **SUS**.
3. Select **Manager** from the **Log on as** drop down menu.
4. Enter the password into the **Password** field. Default password is **123456**.
5. Click the **Login** button. The SUS program will open. The bottom of the screen will say **No Device Connected.**

Pair to PDA

The PIM400 must be paired to the PDA the first time it is connected. Follow the steps bellow to pair the PDA to the PIM400:

1. Log in to SUS (see steps above).
2. Connect the PDA to the PIM400 using the supplied USB cable.
3. Click on the **Options** button at the bottom of the PDA screen. A list of options will open.
4. Put the PIM400 into **Pairing Mode** (this is necessary for the PDA to be able to make changes to the PIM's settings).
   a) On the PIM400, hold down the **Link 1 (S2)** button.
   b) Press the **Link 2 (S3)** button three times while continuing to hold down the Link 1 button. The red LEDs in the Schlage button will flash. The lock is now in pairing mode.
5. On the PDA click the **Pair PDA to Device** option. A pop-up will display when the pairing process is complete.

Note: You only need to pair the PIM400 to the PDA once. After pairing the PIM400 and PDA will communicate whenever connected.

Set PIM400 Address

The SUS is used to set the address of the PIM400. The address of the PIM should be set to the lowest number available, from 0 to 15. A maximum of sixteen (16) AD-400 Locks can communicate with a PIM400 module on the same channel, with all reader types. The address used by the PIM400 and AD-400 locks go from 0 to 15 in the SUS and in the **lite blue** interface. However, the rest of the locks in **lite blue** use an address list of 1 through 16. When addressing a PIM400 or AD-400 lock, it is important to remember this. An address of 0 for the PIM400 or AD-400 lock, in SUS, equals an address of 1 for the rest of the locks in **lite blue**. The PIM400 will have the same address as the AD-400 lock with the lowest address.

When setting the address of the PIM400 you must also designate the range of addresses being used by the AD-400 locks that will communicate with this PIM400, designating both a low and a high address for the doors. This allows the system to know which addresses to keep open for the AD-400 locks.

Example: A PIM400 is being added to the system, and it will have 8 AD-400 locks communicating with it. These are the only devices on this channel, so there are no other device addresses to worry about. The PIM400 will be set at address 0, with a Low value of 0 and a High Value of 7 (meaning the AD-400 locks will be addressed from 0 to 7). In the **lite blue** interface, the PIM400 will be addressed as 0 and the AD-400 locks will be addressed as 0 through 7.

When adding multiple PIM400s to the same channel, the second PIM should have the next available address and its LOW/HIGH range for the AD-400 locks communicating with it should start at that number.

Example: A second PIM400 is being added to the system, on the same channel as the first above. There will be 6 AD-400 Locks communicating with this PIM400. The addresses of the original PIM400 and AD-400 locks has already been set (see above example) so the new PIM400 will have to take this into account. The PIM400 address will be set to 8 (the next available number) and the Low value will be set to 8 and the high value will be set to 13. In **lite blue**, this PIM400 will be addressed at 8 and the AD-400 locks communicating with it will be addressed from 8 through 13.

When adding wired locks to the same channel as a PIM400, you have to take into account the difference in addressing.

Example: An VBB-RI is being added to the system, as the same channel as the PIM400s above. The address of the two PIM400s and their locks has already been set (see the above examples) so the VBB-RI will have to take this into account. The first PIM400 and its locks are taking up addresses 0 through 7 and the second PIM400 and its locks are taking addresses 8 through 13, so addresses 0 through 13 are taken. This counts as addresses 1 through 14 (0+1=1 and 13+1=14) for the hardwired locks. So the VBB-RI will be put on the next available address, which is address 15.

Wired Address	Wireless Address
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Wired Address	Wireless Address
9	8
10	9
11	10
12	11
13	12
14	13
15	14
16	15

Follow the steps below to Address the PIM and to set its LOW/HIGH range for AD-400 locks.

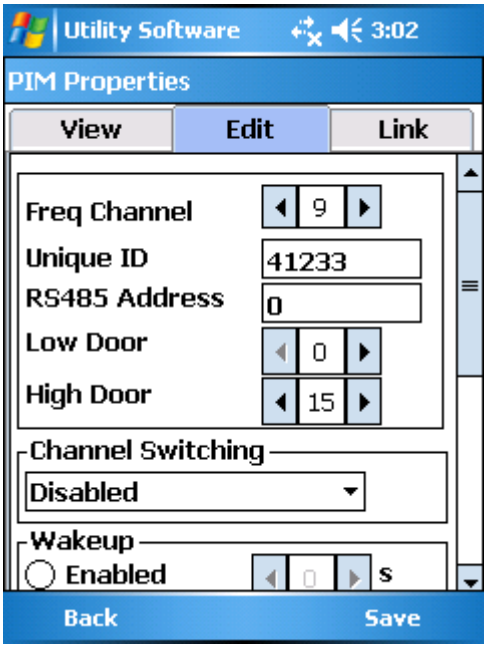
1 Log in to SUS (see steps above).

2 Connect the PDA to the PIM400 using the supplied USB cable.

3 Click on the **Device Options** button.

4 Click on the **PIM Properties** option.

5 Click the **Edit** tab.



6 Define the PIM400's address by clicking on the **RS485** field; this is where the PIM400's address is set. A numerical keypad will open at the bottom of the screen.

7 Using the keypad, set the address of the PIM400.

8 On the **Low Door** option, use the up and down arrows to define the low address of the AD-400s that will communicate with this PIM400.

9 On the **High Door** option, use the up and down arrows to define the high address of the AD-400s that will communicate with this PIM400.

10 Click **Save**. The address of the PIM400 and the address range of the AD-400s have been set.

AD-400 Series Lock Configuration

Configuration of the AD-400 Series locks is accomplished by the SUS while the PDA is connected to the PIM400. After the PIM400 has been configured you can Link AD-400 Locks to it and address them. Once the lock has been addressed the user can test the connection using the Diagnostics section.

Linking/Addressing

Follow the steps bellow to link/address an AD-400 lock:

1 Click **Start** on the PDA. A Menu will open with a list of programs.

2 Select the **Schlage Utility Software** option to open **SUS**.

3 Select **Manager** from the **Log on as** drop down menu.

4 Enter the password into the **Password** field. Default password is **123456**

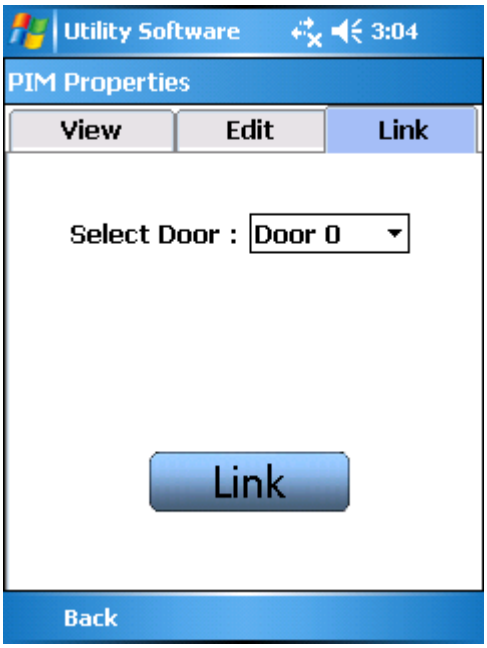
5 Click the **Login** button. The SUS program will open. The bottom of the screen will say **No Device Connected.**

6 Connect the PDA to the PIM400 using the supplied USB cable.

7 Click on the **Device Options** button.

8 Click on the **PIM Properties** option.

9 Go to the **Link** tab.



10 Use the **Select Door** drop down menu to Set the address of the AD-400. This number will be the AD-400's address.

11 Click **Link**.

12 Put the AD-400 Lock into **Linking Mode**:

a) Hold down the **Exit Request Lever**.

b) While holding down the lever, present a **credential**.

c) The **Schlage** button will blink as will the **Internal Push Button**. The lock is now in **Linking Mode**.

d) Release **Exit Request Lever**.

13 Once the **Stop** option is enabled, the AD-400 is now linked to this PIM400 with the specified address.

Diagnostics

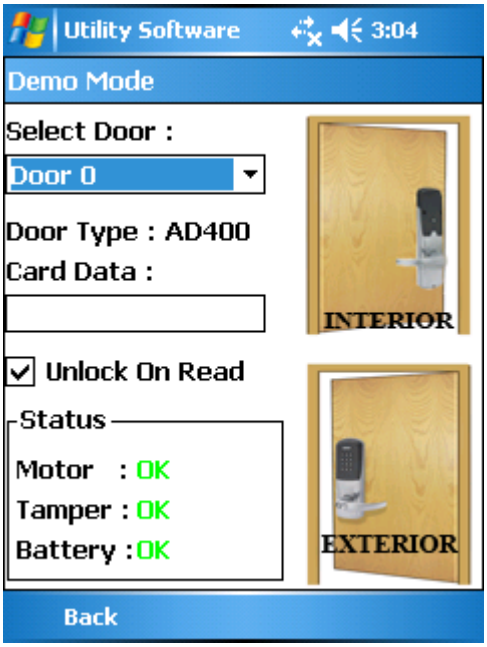
Follow the steps below to determine if you have correctly Linked your AD-400 lock to your PIM400:

1 Log in to SUS (see steps above).

2 Connect the PDA to the PIM400 using the supplied USB cable.

3 Click on the **Device Options** button.

4 Click on the **Diagnostics** option. The **Demo Mode** window will open.



5 Using the **Select Door** drop down, select the door you wish to test.

If the **Status** section shows **OK**, then you have successfully linked the AD-400.

Now, to perform a complete operational test of the AD-400:

1 Present your credential to the AD-400. If the door is functioning correctly the card data will appear in the **Card Data** field.

2 Depress the Internal Lever. If the door is functioning correctly the **Interior image** will show an open door.

3 Depress the External Lever. If the door is functioning correctly the **Exterior image** will show an open door.

WRI400 Configuration

Configuration of the WRI400 is accomplished by the SUS while the HHD is connected to the PIM400. After the PIM400 has been configured you can Link the WRI400 to the PIM400 and address it.

Connecting to HHD/Coupling/Linking

The HHD is used to configure the WRI400. Follow the steps below to connect to the HHD, couple with the HHD, and Link to the PIM400. For information about the HHD and WRI400 settings, see the Schlage Utility Software (SUS) User Guide at www.schlage.com/support.

Connecting to the HHD

To connect the HHD to the WRI400:

1 Verify power is connected to the WRI400.

2 Loosen the 4 screws and remove the WRI400 cover. The Power LED should blink when the cover is off.

Note: The WRI400 will send a tamper signal while the cover is off.

3 Log in to the SUS software (refer to the SUS User Guide for log-in procedure).

Note: Make sure the HHD connection type is set to **USB Connection**.

4 Connect the HHD to the WRI400 USB port (J5). The WRI400's USB LED (2) will blink green.

- The WRI400 is communicating with the HHD when the USB LED blinks green and the HHD display indicates **WRI400** at the bottom of the main screen. The SUS is now ready to view the WRI400 settings.

5 To Edit Settings or Update Firmware on the WRI400, the SUS software and the WRI400 must be coupled. Follow the steps below to couple the WRI400 and the HHD.

Coupling with the HHD

1 Connect the WRI400 to the HHD (see section above for details).

2 On the WRI400, press and hold the **SCHLAGE** button while pressing the **LINK** button three (3) times within 5 seconds. The USB LED will blink red and green.

3 On the SUS, select the option **Couple HHD to Device**. The SUS will report when coupling is successful.

- Successful coupling will be indicated on the WRI400 with a blinking green USB LED.

Linking to a PIM400

1 Click **Start** on the HHD. A Menu will open with a list of programs.

2 Select the **Schlage Utility Software** option to open **SUS**.

3 Select **Manager** from the **Log on as** drop down menu.

4 Enter the password into the **Password** field. Default password is **123456**

5 Click the **Login** button. The SUS program will open. The bottom of the screen will say **No Device Connected.**

6 Connect the HHD to the WRI400 using the supplied USB cable (see instruction above for details on connecting the WRI400 to the HHD).

7 Click on the **Device Options** button.

8 Click on the **PIM Properties** option.

9 Go to the **Link** tab.

10 Use the **Select Door** drop down menu to Set the address of the WRI400. This number will be the WRI400's address.

11 Click **Link**.

12 Make sure power is connected to the WRI400.

13 Remove the WRI400 cover.

14 Press and hold the WRI400's **LINK** button until the RX/TX LED blinks red and green.

15 When linking is successful, the RX/TX LED will blink to indicate the quality of the RF link.

- Solid green, fast green blinks, or green with very few red blinks = Good link
- Solid red or fast red blinks = Poor or no link

Note: The WRI400 will fail to link if it is not in RF range of the PIM400.

Additional Configuration

Once the WRI400 has been linked and addressed the Heartbeat, Request to Exit, and Door Position Switch options need to be configured. Follow the steps below to finish the configuration:

Connect the WRI400 to the HHD

1 Using the USB cable, connect the HHD to **J5** on the WRI400.

2 Start the SUS application.

3 Log into the SUS (default password is 123456). **WRI400** will be displayed at the bottom of the screen after a short delay.

4 You are now ready to configure the WRI400.

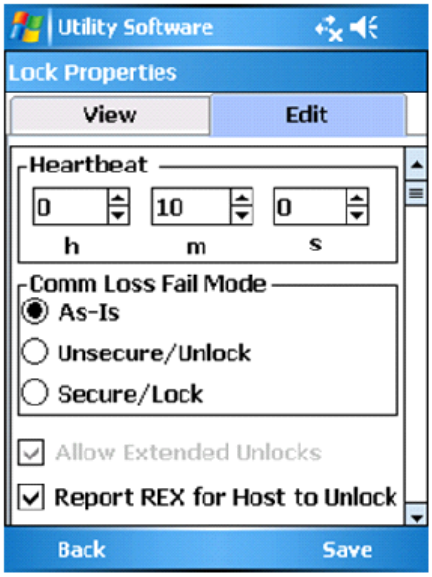
Configure Heartbeat

1 Click on **Device Options** once the connection steps above have been followed and **WRI400** is displayed at the bottom of the SUS screen.

2 Click on **Lock Properties**.

3 Click on the **Edit tab**.

4 Scroll down to the **Heartbeat** section of the Edit Tab.



5 Change the default setting (10 Minutes) to 1 second to allow for a Door Forced or Door Held Open transaction to be read by **lite blue** and activate the auxiliary relay.

6 Click **Save**.

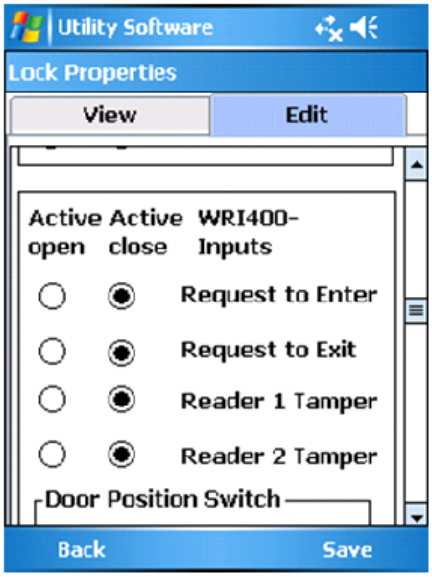
Configure Request to Exit

1 Click on **Device Options** once the connection steps above have been followed and **WRI400** is displayed at the bottom of the SUS screen.

2 Click on **Lock Properties**.

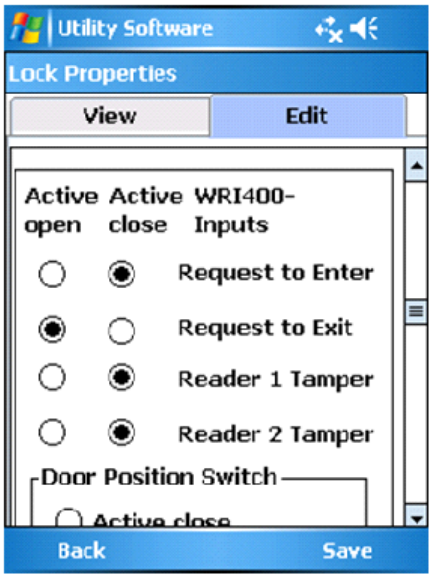
3 Click on the **Edit tab**.

4 Scroll down to the **WRI400-Inputs** section of the Edit Tab.



Default Configuration

5 Change the default setting of the Request to Exit option to **Active open**. When done the screen should look like the following image:



Correct Configuration

6 Click **Save**.

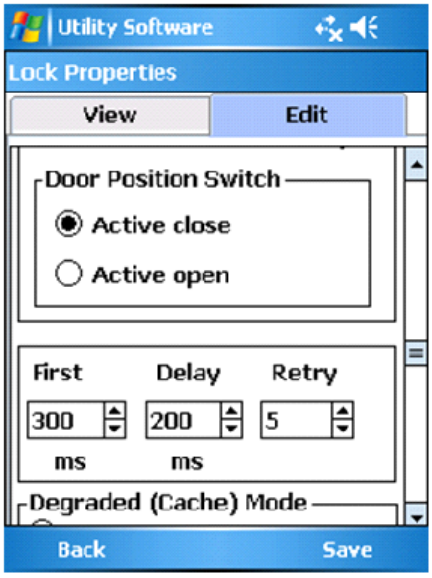
Configure Door Position Switch

1 Click on **Device Options** once the connection steps above have been followed and **WRI400** is displayed at the bottom of the SUS screen.

2 Click on **Lock Properties**.

3 Click on the **Edit tab**.

4 Scroll down to the **Door Position Switch** section of the Edit Tab.

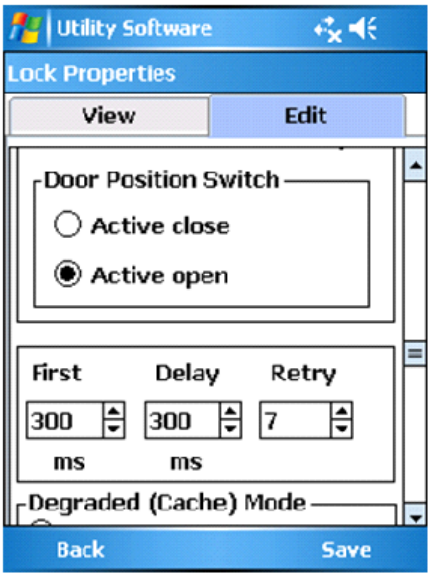


Default Configuration

5 Change the default setting of the Door Position Switch option to **Active open**.

6 Change the **Delay** option to **300**.

7 Change the **Retry** option to **7**. When done the screen should look like the following image:



Correct Configuration

8 Click **Save**.

Schlage NDE Series
Wireless Locks with ENGAGE

CHAPTER 13

Schlage NDE Series Wireless Lock with ENGAGE Technology

Overview

Schlage NDE Series wireless devices can be seamlessly integrated with the lite blue system. The GWE – ENGAGE Gateway communicates directly to the lite blue controller over RS-485 via RSI protocol and can support up to 10 Schlage NDE Series wireless locks with ENGAGE technology (8 when used with **lite blue**). Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Note: For the GWE – ENGAGE Gateway to communicate with the lite blue, v4.2.0 or higher must be installed.

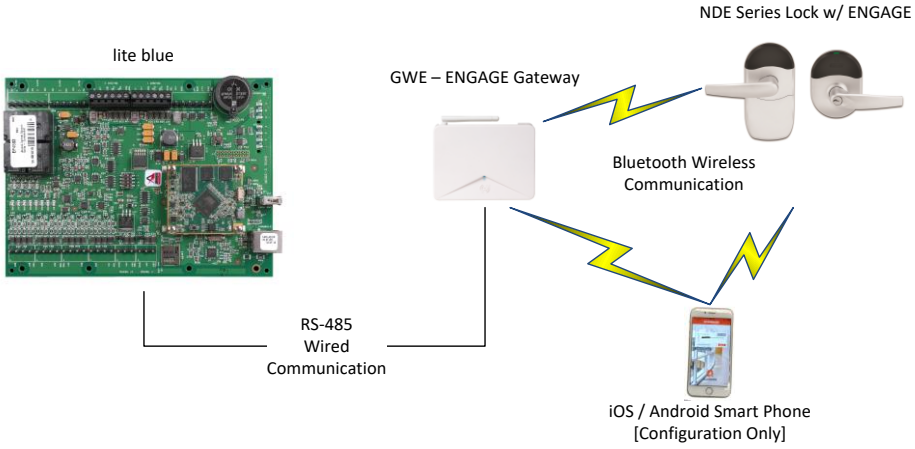
NDEB Series Wireless locks are also supported. Select the NDE Series Wireless Lock.

Bluetooth credentials are not supported. NDEB IPB is not supported.

Schlage NDE Series Components

The Schlage NDE Series Lock system with ENGAGE technology consists of the following components:

- One or more GWE – ENGAGE Gateways
- One or more NDE Series wireless locks (maximum 10 per gateway)
- Android or iOS Smartphone with ENGAGE app for configuration



The GWE – ENGAGE Gateway is hard wired to the lite blue controller communication channels via RS-485 protocol. The Gateway installation location is determined by the location of the NDE series locks (maximum distance between Gateway and NDE series locks is 100 feet) with which it will communicate wirelessly via Bluetooth.

Schlage NDE Series Wireless Modules

Gateway (GWE - ENGAGE)

The GWE – ENGAGE works in conjunction with the NDE Series Locks. The GWE – ENGAGE Gateway is hard wired directly to the lite blue controller communication channels and communicates via RS-485 protocol. The GWE – ENGAGE can support up to 10 NDE locks.

The GWE – ENGAGE is capable of configuring, via the ENGAGE Android or iOS app under Lock settings, the following items:

- Relock
- parameters
- Card data format conversion
- Extended unlock
- Fail safe / fail secure / fail as-is
- Door held pre-alarm
- Cache memory parameters
- Reader configuration
- User interface configuration

Operational environment

- Temperature: 32 – 120 °F (0 – 49 °C)
- Humidity: 0 – 100% (non-condensing)
- Power: 12 VDC @ 330 mA; 24 VDC @ 100 mA or 802.3af/at PoE @ 60 mA (*cannot be powered from VRCNX-M/R*)

Specifications for the GWE – ENGAGE Gateway

- 2.4 GHz Bluetooth v4.0
- Spread spectrum
- Dynamic channel switching (40 channels)
- Range: Up to 100' with obstructions (normal building construction), up to 200' clear line of site
- Gateway to Lock Encryption: AES 256-bit
- Certifications: UL294, FCC Part 15, Industry Canada (IC), RoHS
- RS-485 Communication to VRCNX-M or VRCNX-R
- Supports 10 NDE Wireless Devices
- VRCNX-M/R can support multiple GWE - ENGAGE

NDE Series Wireless Locks

Schlage NDE Series locks with ENGAGE technology contain all of the elements needed to electronically control and monitor access through a door wirelessly. The lock includes a lockset, a Request-to-Exit sensor/switch, a power supply (battery pack), terminals for monitoring a clutch position switch/sensor, a card reader and a RF transceiver for communicating with a GWE – ENGAGE Gateway or smart phone (for configuration only). The GWE – ENGAGE Gateway interfaces to the lite blue reader controller via wired RS-485.

Performance

- Credential verification time: <= 1 second including lock actuation time but not including latency time of host when paired with a GWE – ENGAGE Gateway
- Wake Up on Radio - Allows the GWE - ENGAGE to alert the NDE locks in case of a Lock-out event. Responds to command from SMS within 5 seconds when lined to GWE – ENGAGE Gateway.
- Addressing
- Bluetooth Low Energy v4.0 when used with GWE – ENGAGE Gateway
- Range: up to 100 feet on one floor when used in normal office interior construction

Mechanical Specifications

- ANSI / BHMA A156.25-2013 (Indoor / Outdoor)
- ANSI / BHMA A156.2-2011, Series 4000, Grade 1
- Power: 4 AA alkaline batteries
- Battery Life: up to 2 years (*indoor application, 13.56 MHz CSN credential, 100 actuations daily*)

Operating voltage

- The 4 AA batteries will supply 6.2 volts.
  - The locks will continue to operate down to 4.5 volts when Low Battery will be reported.
  - The locks will report Critical Batter at 4.0 volts and into a fail-safe, fail secure or fail as-is mode depending on lock configuration via ENGAGE mobile app.

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 0% to 100% non-condensing

Card Reader - Proximity Reader

- 125 kHz and 12.56 MHz smart credentials
- ISO standard 15693 and ISO 14443
- Card Read Range: up to 1.25” on 125 kHz proximity credentials
  up to 0.75” on 13.56 MHz smart credentials
- 125 kHz proximity credentials compatibility:
  Schlage, XceedID, HID, GE/CASE PRoxLite, AWID and LenelProx
- 13.56 MHz smart credential compatibility:
  Secure Sector: Schlage MIFARE, aptiQ MIFARE Classic, XceedID, aptiQ MIFARE DESFire EV1 with PACSA, aptiQ mobile
  CDN Only: DESFire, HID iClasss, Inside Contactless Pico Tag, MIFARE, MIFARE DESFire EV1, ST Microelectronics, Texas Instruments Tag-It, Phillips I-Code
- Wiegand output
- Certifications: UL 294, UL10C, FCC Part 15, ADA, RoHS, Industry Canada (IC)
- ESD Protection: 12KV

Card formats: Above specified card formats up to 255-bit

Request-to-exit: built-in switch will be triggered from the activation of the door lever on the protected side of the door.

Clutch position: Schlage NDE locks provide a way to lock or unlock a door and monitor access from a remote location. Schlage NDE locks are fail-safe from the protected side of the door. These locksets are controlled by the lite blue system.

Door position: built-in magnetic Door Position Switch (DPS) used to report Door Open, Door Forced or Door Held events. Must be calibrated via ENGAGE mobile app during lock commissioning. Will report out of calibration.

GWE – ENGAGE Gateway Wiring Instructions

Power

- lite blue 12 – 24 VDC
- GWE – ENGAGE Gateway powered by external 24 VDC power supply

lite blue to GWE – ENGAGE Gateway

- Controller to Gateway via RS-485 wiring max 4000’

lite blue	GWE – ENGAGE Gateway
RS-485-1 TR+ or RS-485-2 TR+	TX-
RS-485-1 TR- or RS-485-2 TR-	TX+

GWE – ENGAGE Gateway, NDE Lock and SMS Addressing

The address of the GWE - ENGAGE Gateway (RS-485) should be set to the lowest number available, from 0 to 9. A maximum of ten (10) NDE Series wireless locks with ENGAGE can communicate with a Gateway on the same channel (8 on **lite blue**). The address defined in the Gateway and **lite blue** for the NDE locks ranges from 0 to 7.

lite blue addresses will always be identical to the value displayed in the ENGAGE iOS or Android app. The ENGAGE Gateway will have the same address as the NDE lock with the lowest address.

Setting the address of the Gateway requires designation of the range of addresses being used by the NDE Locks that will communicate with the Gateway: designate both a Low and a High address for the NDE locks to allow the Gateway to maintain the correct open addresses for the NDE locks.

Example: A Gateway is defined which will be supporting 5 NDE locks. These are the only devices on this controller channel, so there are no other device addresses to consider. Set the Gateway to address 0, with a Low value of 0 and a High value of 4 (i.e. the NDE locks will be addressed from 0 to 4).

Additional Gateways on the same controller channel, should be addressed with the next available address and its Low / High range for the NDE locks should start at that number.

Example: A second Gateway is added to the system, on the same channel as the example above. There will be 2 NDE Locks communicating with the 2nd Gateway. Addresses of the 1st Gateway and NDE locks have already been set (see above example). These addresses must be considered when addressing the 2nd Gateway and additional NDE locks. The 2nd Gateway should be configured to address 5 (the next available address) and the Low value will be set to 5 and the high value will be set to 6.

Configure lite blue to communicate with the 2nd Gateway at address 5 and the NDE locks communicating with it will be addressed from 5 through 6.

Configuring GWE – ENGAGE Gateway and NDE Locks

Allegion ENGAGE Account

Schlage GWE – ENGAGE Gateways and NDE Series locks with ENGAGE technology are commissioned (initialized for use) and configured using an iOS or Android smart phone app which requires login to an Allegion ENGAGE account.

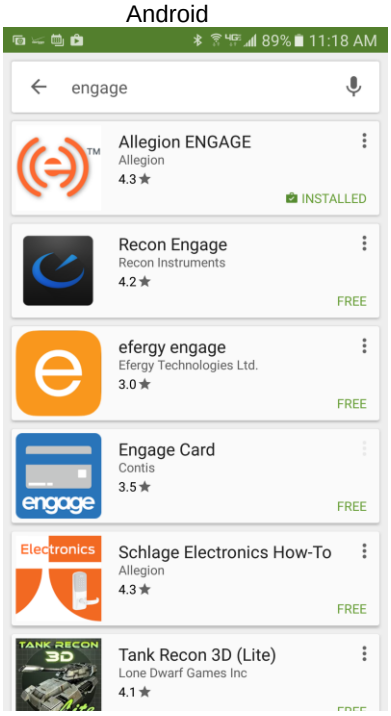
The commissioning will download an encryption key to the Gateway and Locks which is shared by all ENGAGE devices assigned to the ENGAGE Account Site so that only ENGAGE devices within the same site can communicate with each other and with the ENGAGE app login to the site.

Vanderbilt will create an ENGAGE Site and forward an Invite via email which must be accepted prior to lock commissioning and configuration. Use the Vanderbilt provided ENGAGE account username (email address) and password in the ENGAGE Android or iOS mobile app as indicated below.

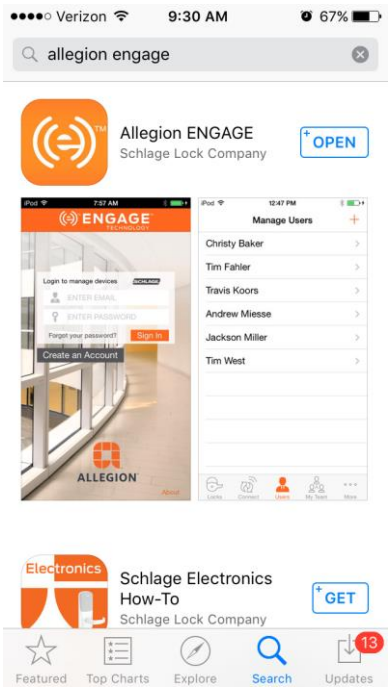
Download ENAGE app

- Open the Google Play store or Apple App store on the mobile device
- Search for “Allegion ENGAGE”

Android



iOS



- Click on the Allegion ENGAGE application
- Click Install

Allegion updates the ENGAGE application frequently so screen shots for the examples below are not provided to avoid confusion. Please refer to the latest Allegion ENGAGE documentation for sample screens.

Commission / Configure GWE – ENGAGE Gateway

- Open the ENGAGE app on the mobile device
- Login to the unique site using the credentials provided by Vanderbilt
- The initial “Manage Devices” screen will be empty until the first lock or gateway is added to the site
- Select Connect to devices / Add Device
- Verify that 24 VDC external power is applied to the GWE – Engage Gateway.
- Gateway initial power-on self-test will sequence various LED colors.
- Gateway LED will indicate solid red when ready to be commissioned.
- Click the “+” / “Add Device” in the ENAGE app to find the Gateway.
- Select the Gateway. The Gateway LED will flash blue.
- Click “Yes”.
- Configure Device will open
- Name the Gateway and click Save / Next
- The next screen is used to configure the RS-485 address of the Gateway and the settings for the Low Door address & High Door address (see addressing section above).
- Set the Gateway, Low Door and High Door Addresses
- Click “Save” – Commissioning is completed
- Click “Disconnect”
- The Gateway will now be displayed in the Connect to Device / Site screen

If the GWE – Gateway is not successfully commissioned and defined via the Android or iOS mobile device, the Gateway will have to be reverted to the Schlage Factory Default settings prior to a 2nd attempt to commission. See the Schlage GWE – Gateway Installation Instruction Guide for Factory Default Reset instructions.

Commission NDE Locks w/ ENGAGE Technology

Schlage NDE Locks must be fully assembled, batteries installed with the battery cover in place and a Factory Default Reset (FDR) performed prior to commissioning.

Deviation from the commissioning procedure outlined below may prevent lock commissioning and require an FDR prior to repeating the process.

Do Not Modify Settings Other Than Those Specified Below During the Commissioning Process

- Open the ENGAGE app on the mobile device
- Login to the unique site using the credentials provided by Vanderbilt
- Open the “Connect Devices” / “Site Name” screen
- Select the “+” sign to initiate lock commissioning
- The Commission Device screen should display as indicated below
- Turn and release the NDE lock inside lever as indicated
- Click “OK”
- The NDE lock should now display in the ENGAGE app
- Select “Add”
- The NDE lock should start flashing red
- Select “Yes”
- Enter a Name for the NDE lock and click “→” / “Next”
- The ENGAGE app will prompt for magnetic Door Position Switch (DPS) calibration
- Close the door
- Click “OK” / “Calibrate” to initiate DPS calibration
- The ENGAGE app will prompt for Wi-Fi configuration

Schlage NDE Lock Wi-Fi is Not Used when the Locks Are Connected to the GWE – ENGAGE Gateway

The NDE Locks Communicate with the GWE – Gateway via Bluetooth

- Turn Wi-Fi OFF
- Click “✓” / “Finish” to complete commissioning

The NDE Lock Firmware Version Will Be Interrogated and the ENGAGE app Will Prompt for a Mandatory Firmware Update for Locks with Outdated Firmware

- Follow the ENGAGE app prompts to update the firmware if required

The Firmware Update Process Differs Between Android and iOS Devices

Due to the Bandwidth Required to Transfer the Firmware Update File, the NDE Lock Wi-Fi will be Temporarily Enabled by the ENGAGE app and the Mobile Device must be Connected to the NDE Lock Wi-Fi Access Point

This Process is Automated Under Android Devices but Requires Manually Intervention for iOS Devices

- The NDE lock should now appear in the Connect to Devices / Site screen

Configure Communications Delay and Retry Timing

- Select “Connect” and “Configure Device”
- Select “Advanced”
- Select “Advanced RSI”
- Acknowledge the Warning by Clicking “Continue”
- Acknowledge the Warning by Clicking “Continue”
- Set the following Credential Inquiry Timing parameters:
    - Set First Delay (ms) = 300
    - Set Subsequent Delay (ms) = 300
- Set Retry Times = 7
- Select Save
- Repeat the above process for each Schlage NDE lock to be utilized with **lite blue**
- Logout of the ENGAGE Mobile app

If the Schlage NDE lock(s) are not successfully commissioned and configured via the Android or iOS mobile device, the lock(s) will have to be reverted to the Schlage Factory Default settings prior to a 2nd attempt to commission. See the Schlage NDE Wireless Lock Installation Instruction Guide for Factory Default Reset instructions.

Define ENGAGE Devices in lite blue

The GWE – ENGAGE Gateway (RS-485) must be connected and defined in **lite blue** prior to configuring any NDE Wireless locks.

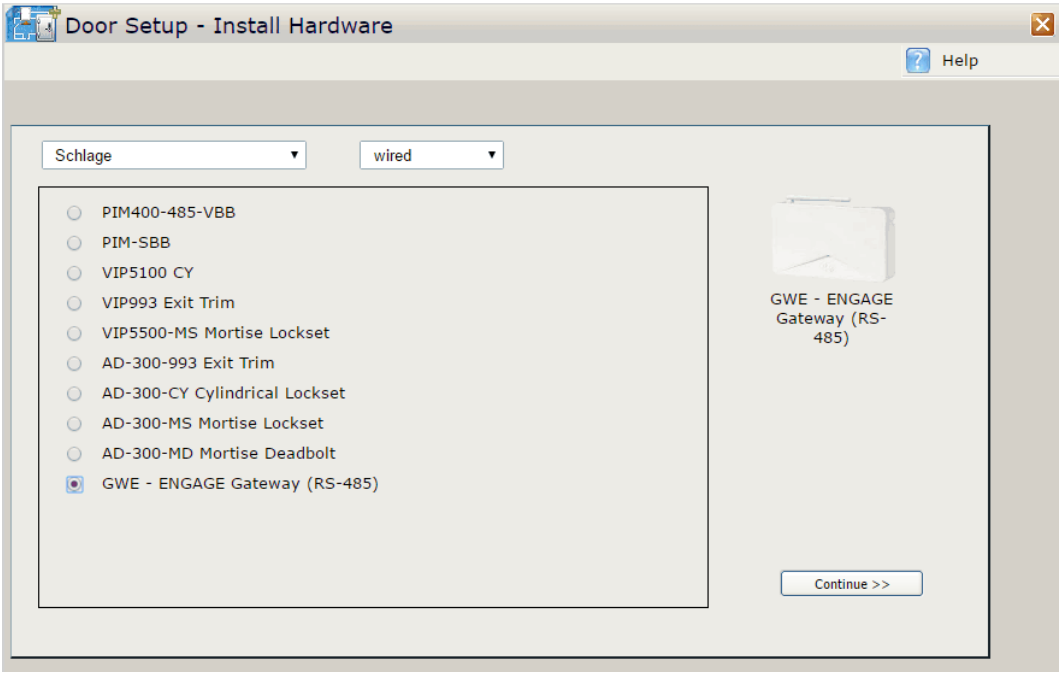
- Connect to lite blue and login with USR or another administrator account

Define Gateway

1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left side of the main screen.

2 Click the **Add doors and hardware** button in the Installation and Configuration Tasks section. The Door Setup - Install Hardware window will open.

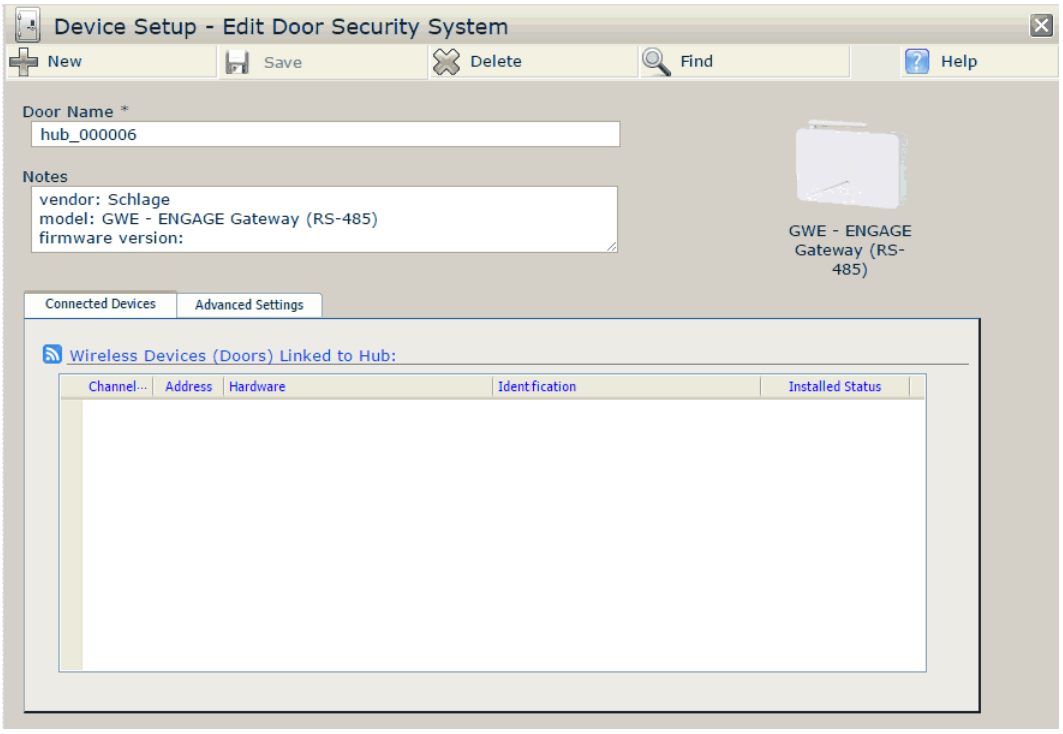
3 Select **Schlage** and **Wired** from the drop-down menus at the top.



4 Click on the radio button to the left of GWE - ENGAGE Gateway (RS-485)

5 Click on the **Continue** button. The **Installation** pop-up window will open asking you to Confirm Hub Record Creation.

6 Click **OK** to set up a Gateway. The **Device Setup - Edit Door Security System** window will open.



7 Complete the **Door Name** and **Notes** fields.

8 Select the **Advanced Settings** tab in the bottom half of the screen.

9 Define the following options:

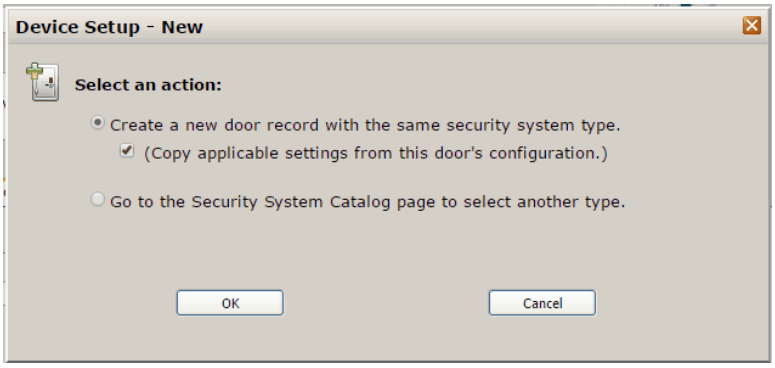
e) Select the **Channel Number** corresponding to the channel on the lite blue to which the Gateway is wired.

f) Set the **Gateway Address** to match the address that is specified by the Allegion ENGAGE Mobile App. Please see the GWE - ENGAGE Gateway (RS-485) section of the installation guide for more details.

g) **Installed**. Click this box if this Gateway is currently installed on the system.

10 Click the **Save** button at the top of the screen. The screen will refresh and the door profile will be saved.

11 Click the **New** button at the top of the screen to add additional Gateways. **The Device Setup - New** pop-up window will open.



12 Select from the following options:

- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Device Setup - Edit Door Security System** window will reopen. Repeat the configuration steps above.
- **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. The new lock will have all the same settings as the previous lock. Rename the lock and complete any **Notes** (if desired), define the **Channel** and **Address** of the new lock and make any other changes necessary. Click **Save Door** once the lock is configured as desired.
- **Go to the Security System Catalog page to select another type.** Select this to set up a door type different from the previous door type. The pop-up window will close and the **Device Setup - Install Electronic Security System Hardware** window will open. Follow the steps for the lock type selected.

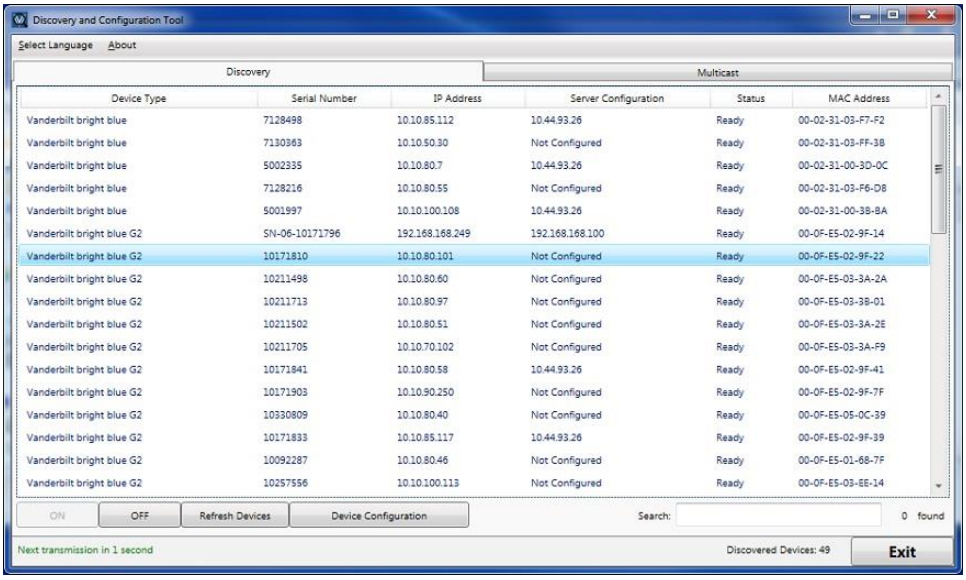
Link NDE Locks to GWE – ENGAGE Gateway

Linking the GWE – ENGAGE Gateway and NDE Wireless Locks with ENGAGE Technology is accomplished using the Vanderbilt Discovery Tool provided with lite blue.

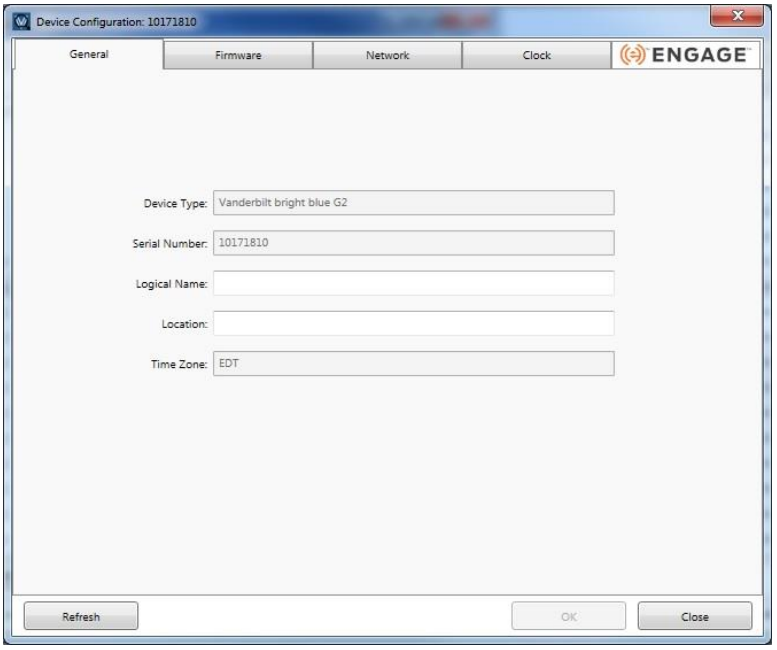
Discovery Tool v1.4.7 or newer is required.

lite blue v4.2.0 or newer is required.

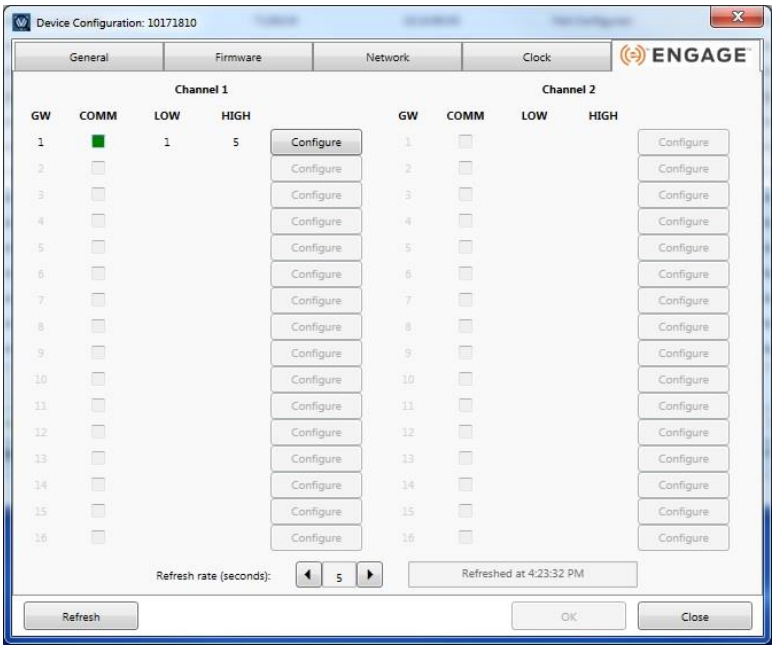
- Launch the Discovery Tool and click “ON” to enable auto-discovery



- Locate the lite blue Controller to which the GWE – ENGAGE Gateway is wired and double-click to open the Device Configuration dialog.



- Select the “ENGAGE” tab once displayed



- Any connected GWE – ENGAGE Gateways should display at the appropriate RS-485 Address
- The configured Low and High NDE Lock Address will be retrieved from the Gateway and displayed

The Discovery Tool will display all Addressing as required by lite blue. ENGAGE Device Addressing is 0-based while Diagnostics Addressing is 1-based. See *GWE – ENGAGE Gateway, NDE Lock and lite blue Addressing* above.

Discovery Tool ENGAGE dialogs auto-refresh. The Default auto-refresh is 5 seconds and is user configurable.

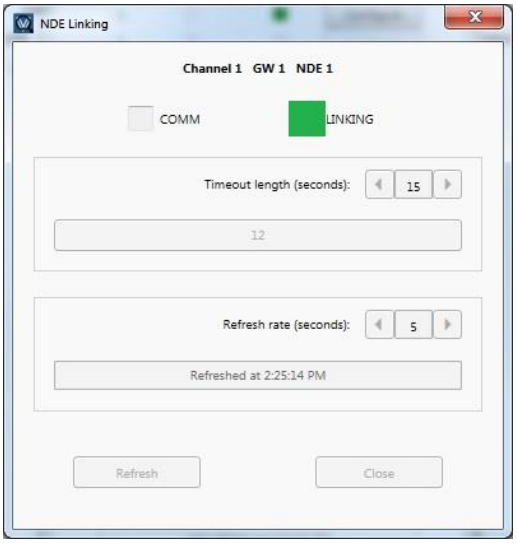
- Click “Configure” to display NDE ***commissioned and configured*** locks available for linking.

- Click “Configure” on the NDE Lock to Link

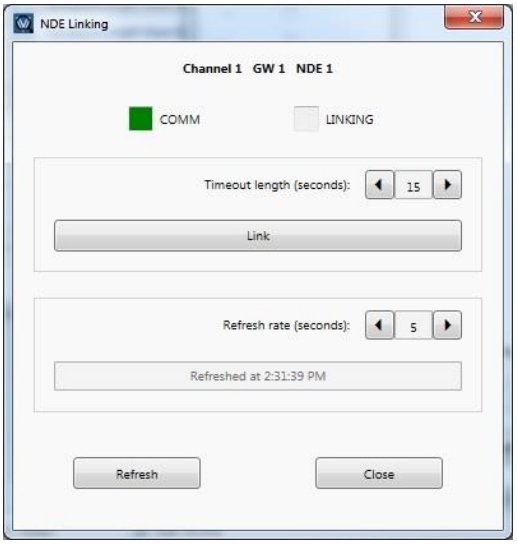
- Click “Link” to initiate the linking process

All dialog buttons will be disabled during the linking process for a timeout period of 15 seconds which is user configurable up to 30 seconds. The Link button will become a counter for the Timeout period. Once the timeout period expires, the Link button will become Abort.

- The Linking indicator will indicate green once the Gateway is placing in Linking Mode
- Turn the NDE Lock inside lever and present a credential to start put the Lock into Linking Mode

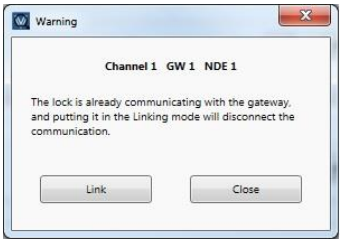


- The COMM indicator will turn green once the Lock is successfully linked to the Gateway and the Lock will exit Linking Mode (Linking indicator gray)



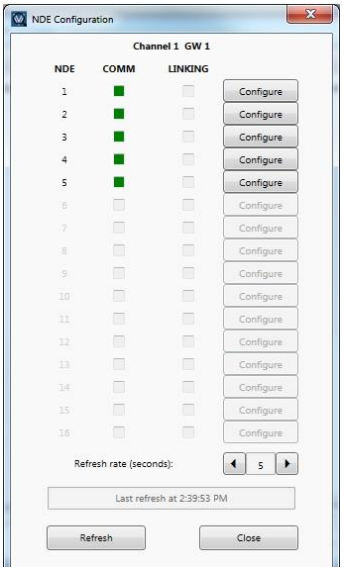
- Click “Close” once the COMM indicator displays green

Clicking the Link button on a Lock that is already Linked and communicating with an GWE – ENAGE Gateway will unlink the Lock and cancel communication with the Gateway. If this was not intentional, click the Close button in the warning dialog presented.

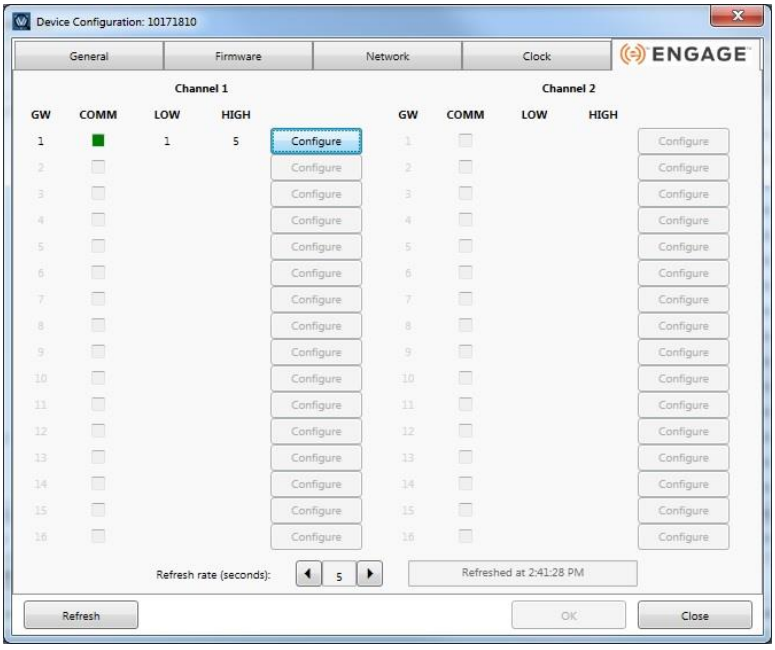


- The Lock will display communicating in the Available Locks dialog.

- Repeat the above process to link additional NDE Locks to the selected Gateway



- Close the dialog once all desired NDE Locks are linked to the Gateway



- Repeat for additional GWE – ENGAGE Gateways and NDE Wireless Locks as required.
- Close the Device Configuration dialog when complete
- Exit the Discovery Tool

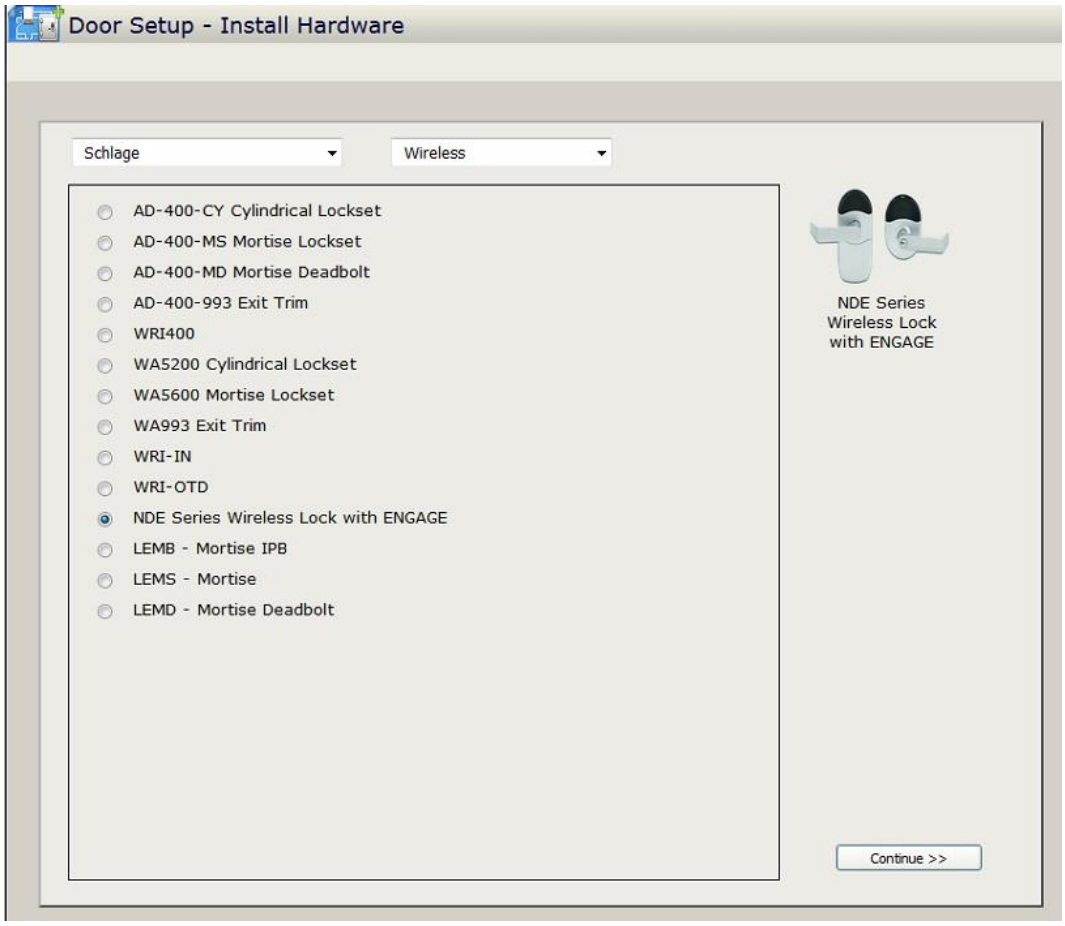
Define NDE Lock

Note: If using a Schlage NDE Wireless lock, a GWE - ENGAGE Gateway (RS-485) must be programmed before continuing. Please see the GWE - ENGAGE Gateway (RS-485) section above for more details.

1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left.

2 Click the **Add doors hardware** button in the Installation Tasks section. The **Door Setup - Install Hardware** window will open.

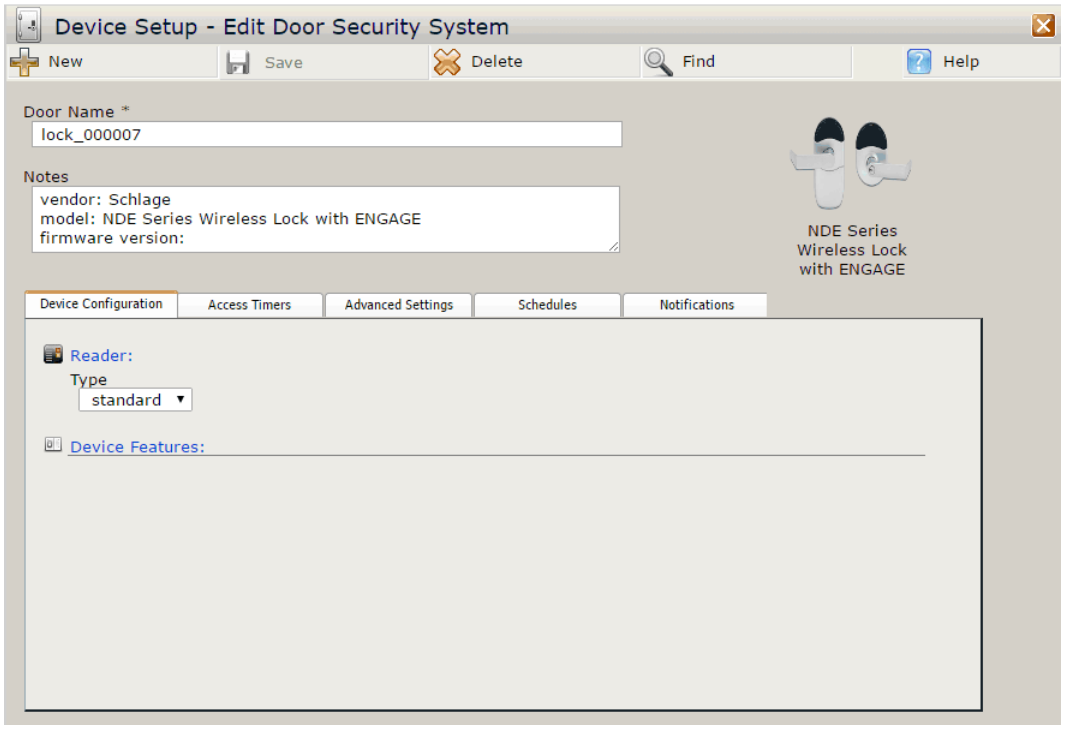
3 Select **Schlage** and **Wireless** from the drop-down menus at the top.



4 Click on the radio button to the left of the type of NDE Series Wireless Lock with ENGAGE lock to be set up.

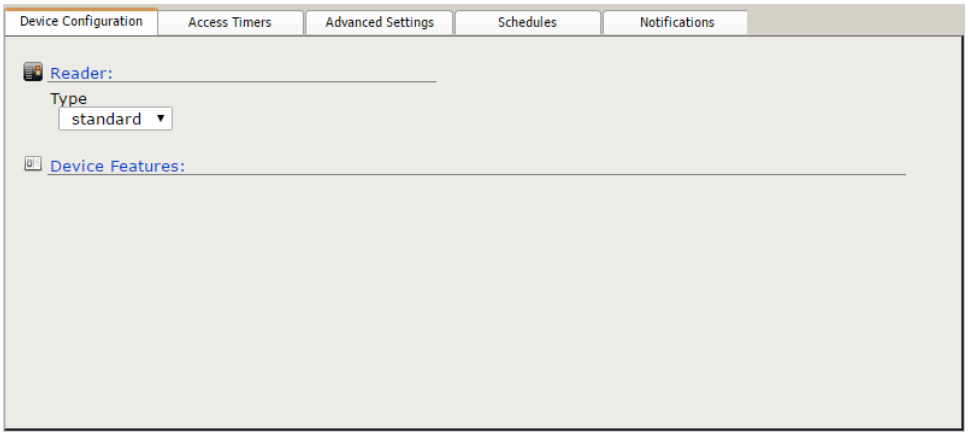
5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.

6 Click **Ok** to confirm the correct lock. The **Door Setup - Edit Door Security System** window will open.



7 Complete the **Door Name** and **Notes** fields.

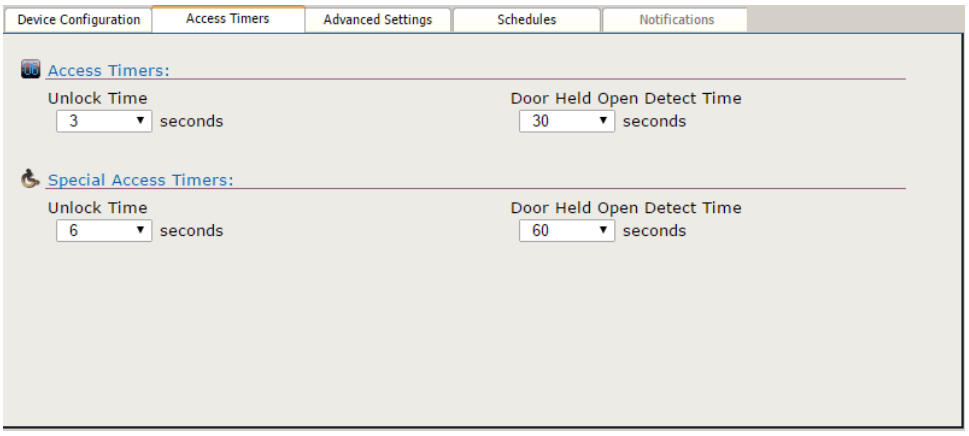
8 Select the **Device Configuration** tab in the bottom half of the screen.



9 Define the following **Reader Type** options:

- **Standard** - Readers for any location not using antipassback.
- **Entry** - Readers that are defined as entry readers for antipassback purposes.
- **Exit** - Readers that are defined as exit readers for antipassback purposes.

10 Now select the **Access Timers** tab.



11 Define the following **Timers** options:

h) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.

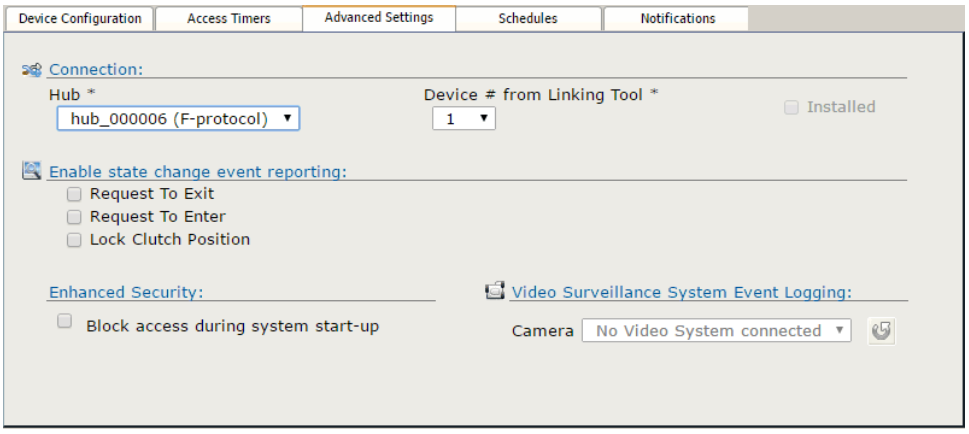
i) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.

12 Define following **Special Access Timers** options:

j) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.

k) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

13 Select the **Advanced Settings** tab in the bottom half of the screen.



14 Define the following options in the **Connection** section:

l) Select the Gateway that the lock is connected to from the **Hub** drop down box.

m) Set the **Device # from Linking Tool** to the exact number specified by the Allegion ENGAGE Mobile App. Please see the NDE Wireless Lock w/ ENGAGE section of the installation guide for more details.

n) **Installed**. Click this box if this lock is currently installed on the system.

15 Select the desired options in the **Enable state change event reporting** section:

o) Check the **Request To Enter** box for the ability to generate reports and see activity based on when the Request to Enter is activated.

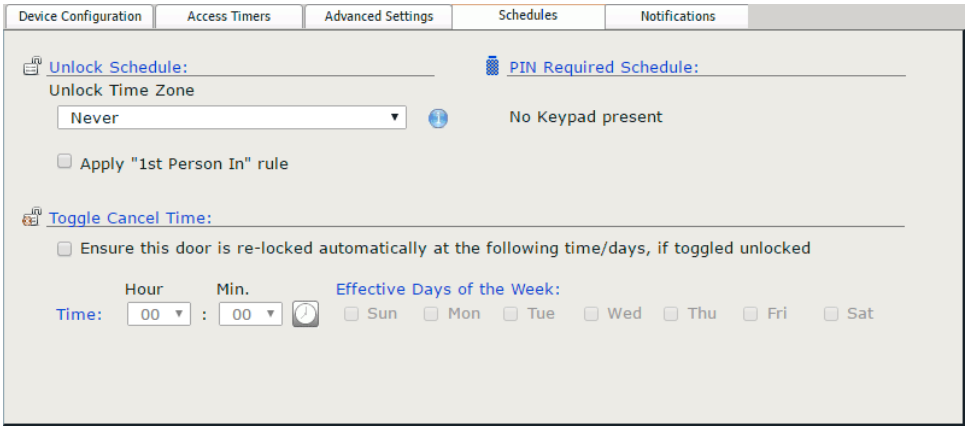
p) Check the **Request To Exit** box for the ability to generate reports and see activity based on when the REX is activated.

q) Check the **Lock Clutch Position** box for the ability to generate reports and see activity based on when the lock's clutch is engaged/disengaged.

16 Check the **Block access during system start-up** option under **Enhanced Security** if you wish to disable access to this door any time the system restarts.

17 If the **lite blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.

18 Select the **Schedules** tab in the bottom half of the screen.



19 Select the desired options in the **Unlock Schedule** section:

r) Select the time zone for the door using the **Unlock Time Zone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button with the mouse. An information window will open showing the schedule of the selected time zone.

s) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. If a door has an **Unlock Time Zone** and this rule is selected, the door will not automatically unlock unless a valid credential is presented within the specified time zone. A credential holder must also have this feature enabled for a credential to activate the 1st Person In feature (see the Adding Personnel section for details on adding this feature to a person).

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked until a person with this feature is in the building. Select the 7:00am to 5:00pm Time Zone and check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after a person who also has this feature enabled has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

20 **PIN Required Schedule** will not present any options. A **Keypad o**ption is not currently available for the NDE Wireless Locks.

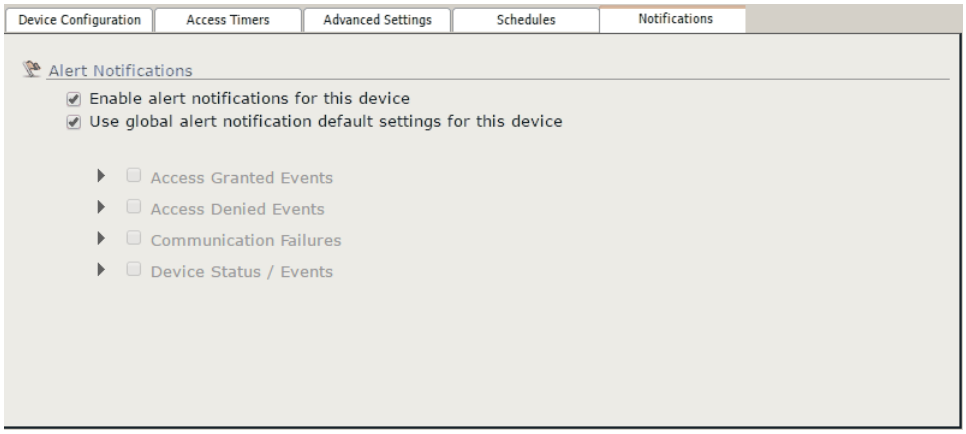
21 Define the following options in the **Toggle Cancel Time** section:

t) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:** box to enable this feature. This will lock this door automatically at the specified time.

u) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.

v) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.

22 Select the Notifications tab in the bottom half of the screen.



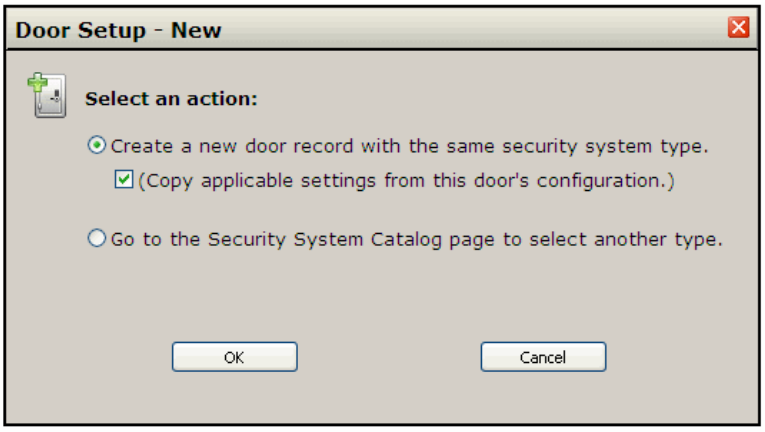
23 Select the desired alert notifications for the device:

w) Check the **Enable alert notifications for this device** box to enable email alerts for this door.

x) Check the **Use global alert notification default settings for this device** box to use the global alert settings for this door (see Utilities - View of modify alert notifications). Uncheck this box to override the global default settings and customize the alert notifications for this door.

24 Click the **Save** button at the top of the screen. The screen will refresh and the door will be saved.

25 To add additional locks, click the **New Door** button at the top of the screen. **The Door Setup - New** pop-up window will open.



26 Select from the following options:

- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat the steps above.

- **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat the steps above.
- **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Hardware** window will open. Follow the steps for the lock type selected.

Schlage LE Series Wireless Locks

CHAPTER 14

Schlage LE Series Wireless Lock

Overview

Schlage LE Series wireless devices can be seamlessly integrated with the lite blue system similarly to Schlage NDE Locks. The GWE – ENGAGE Gateway communicates directly to the lite blue controller over RS-485 via RSI protocol and can support up to 10 Schlage NDE or LE Series wireless locks (8 when used with **lite blue**). Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Note: For the GWE – ENGAGE Gateway to communicate with the lite blue, v4.2.0 or higher must be installed.

LEB Series Wireless locks are also supported. Select the equivalent model LE Series Wireless Lock.

Bluetooth credentials are not supported.

Schlage LE Series Components

The Schlage LE Series consists of the following components:

- One or more GWE – ENGAGE Gateways
- One or more LE Series wireless locks (maximum 10 per gateway)
- Android or iOS Smartphone with ENGAGE app for configuration

The GWE – ENGAGE Gateway is hard wired to the lite blue controller communication channels via RS-485 protocol. The Gateway installation location is determined by the location of the LE series locks (maximum distance between Gateway and NDE series locks is 100 feet) with which it will communicate wirelessly via Bluetooth.

Schlage LE Series Wireless Modules

Gateway (GWE - ENGAGE)

The GWE – ENGAGE works in conjunction with the NDE and LE Series Locks. The GWE – ENGAGE Gateway is hard wired directly to the lite blue controller communication channels and communicates via RS-485 protocol. The GWE – ENGAGE can support up to 10 NDE locks.

The GWE – ENGAGE is capable of configuring, via the ENGAGE Android or iOS app under Lock settings, the following items:

- Relock
- parameters
- Card data format conversion
- Extended unlock
- Fail safe / fail secure / fail as-is
- Door held pre-alarm
- Cache memory parameters
- Reader configuration
- User interface configuration

Operational environment

- Temperature: 32 – 120 °F (0 – 49 °C)
- Humidity: 0 – 100% (non-condensing)
- Power: 12 VDC @ 330 mA; 24 VDC @ 100 mA or 802.3af/at PoE @ 60 mA (*cannot be powered from VRCNX-M/R*)

Specifications for the GWE – ENGAGE Gateway

- 2.4 GHz Bluetooth v4.0
- Spread spectrum
- Dynamic channel switching (40 channels)
- Range: Up to 100' with obstructions (normal building construction), up to 200' clear line of site
- Gateway to Lock Encryption: AES 256-bit
- Certifications: UL294, FCC Part 15, Industry Canada (IC), RoHS
- RS-485 Communication to VRCNX-M or VRCNX-R
- Supports 10 NDE Wireless Devices
- VRCNX-M/R can support multiple GWE - ENGAGE

LE Series Wireless Locks

Schlage LE Series locks contain all of the elements needed to electronically control and monitor access through a door wirelessly. The lock includes a lockset, a Request-to-Exit sensor/switch, a power supply (battery pack), terminals for monitoring a clutch position switch/sensor, a card reader and a RF transceiver for communicating with a GWE – ENGAGE Gateway or smart phone (for configuration only). The GWE – ENGAGE Gateway interfaces to the lite blue reader controller via wired RS-485.

Performance

- Credential verification time: <= 1 second including lock actuation time but not including latency time of host when paired with a GWE – ENGAGE Gateway
- Wake Up on Radio - Allows the GWE - ENGAGE to alert the NDE locks in case of a Lock-out event. Responds to command from SMS within 5 seconds when lined to GWE – ENGAGE Gateway.
- Addressing
- Bluetooth Low Energy v4.0 when used with GWE – ENGAGE Gateway
- Range: up to 100 feet on one floor when used in normal office interior construction

Mechanical Specifications

- ANSI / BHMA A156.25-2013 (Indoor / Outdoor)
- ANSI / BHMA A156.2-2011, Series 4000, Grade 1
- Power: 4 AA alkaline batteries
- Battery Life: up to 2 years (*indoor application, 13.56 MHz CSN credential, 100 actuations daily*)

Operating voltage

- The 4 AA batteries will supply 6.2 volts.
  - The locks will continue to operate down to 4.5 volts when Low Battery will be reported.
  - The locks will report Critical Batter at 4.0 volts and into a fail-safe, fail secure or fail as-is mode depending on lock configuration via ENGAGE mobile app.

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 0% to 100% non-condensing

Card Reader - Proximity Reader

- 125 kHz and 12.56 MHz smart credentials
- ISO standard 15693 and ISO 14443
- Card Read Range: up to 1.25” on 125 kHz proximity credentials
  up to 0.75” on 13.56 MHz smart credentials
- 125 kHz proximity credentials compatibility:
  Schlage, XceedID, HID, GE/CASE PRoxLite, AWID and LenelProx
- 13.56 MHz smart credential compatibility:
  Secure Sector: Schlage MIFARE, aptiQ MIFARE Classic, XceedID, aptiQ MIFARE DESFire EV1 with PACSA, aptiQ mobile
  CDN Only: DESFire, HID iClasss, Inside Contactless Pico Tag, MIFARE, MIFARE DESFire EV1, ST Microelectronics, Texas Instruments Tag-It, Phillips I-Code
- Wiegand output
- Certifications: UL 294, UL10C, FCC Part 15, ADA, RoHS, Industry Canada (IC)
- ESD Protection: 12KV

Card formats: Above specified card formats up to 255-bit

Request-to-exit: built-in switch will be triggered from the activation of the door lever on the protected side of the door.

Clutch position: Schlage NDE locks provide a way to lock or unlock a door and monitor access from a remote location. Schlage NDE locks are fail-safe from the protected side of the door. These locksets are controlled by the lite blue system.

Door position: built-in magnetic Door Position Switch (DPS) used to report Door Open, Door Forced or Door Held events. Must be calibrated via ENGAGE mobile app during lock commissioning. Will report out of calibration.

GWE – ENGAGE Gateway Wiring Instructions

See Chapter 13 – NDE Series Wireless Locks

GWE – ENGAGE Gateway, LE Lock and SMS Addressing

The address of the GWE - ENGAGE Gateway (RS-485) should be set to the lowest number available, from 0 to 9. A maximum of ten (10) LE or NDE Series wireless locks can communicate with a Gateway on the same channel. The address defined in the Gateway and **lite blue** for the LE or NDE locks ranges from 0 to 9.

lite blue addresses will always be identical to the value displayed in the ENGAGE iOS or Android app. The ENGAGE Gateway will have the same address as the LE or NDE lock with the lowest address.

Setting the address of the Gateway requires designation of the range of addresses being used by the LE or NDE Locks that will communicate with the Gateway: designate both a Low and a High address for the LE or NDE locks to allow the Gateway to maintain the correct open addresses for the LE or NDE locks.

Example: A Gateway is defined which will be supporting 5 LE locks. These are the only devices on this controller channel, so there are no other device addresses to consider. Set the Gateway to address 0, with a Low value of 0 and a High value of 4 (i.e. the LE locks will be addressed from 0 to 4).

Additional Gateways on the same controller channel, should be addressed with the next available address and its Low / High range for the LE locks should start at that number.

Example: A second Gateway is added to the system, on the same channel as the example above. There will be 5 LE Locks communicating with the 2nd Gateway. Addresses of the 1st Gateway and LE locks have already been set (see above example). These addresses must be considered when addressing the 2nd Gateway and additional LE locks. The 2nd Gateway should be configured to address 5 (the next available address) and the Low value will be set to 5 and the high value will be set to 9.

Configure lite blue to communicate with the 2nd Gateway at address 5 and the LE locks communicating with it will be addressed from 5 through 9.

Configuring GWE – ENGAGE Gateway and LE Locks

Allegion ENGAGE Account

Schlage GWE – ENGAGE Gateways and LE Series locks with ENGAGE technology are commissioned (initialized for use) and configured using an iOS or Android smart phone app which requires login to an Allegion ENGAGE account.

The commissioning will download an encryption key to the Gateway and Locks which is shared by all ENGAGE devices assigned to the ENGAGE Account Site so that only ENGAGE devices within the same site can communicate with each other and with the ENGAGE app login to the site.

Vanderbilt will create an ENGAGE Site and forward an Invite via email which must be accepted prior to lock commissioning and configuration. Use the Vanderbilt provided ENGAGE account username (email address) and password in the ENGAGE Android or iOS mobile app as indicated below.

Download ENAGE app

See Chapter 13 – NDE Locks

Commission / Configure GWE – ENGAGE Gateway

See Chapter 13 – NDE Locks

Commission LE Series Locks

See Chapter 13 – NDE Locks … *the process is the same*

Define ENGAGE Devices in lite blue

The GWE – ENGAGE Gateway (RS-485) must be connected and defined in lite blue prior to configuring any NDE Wireless locks.

- Connect to lite blue and login with USR or another administrator account

Define Gateway

See Chapter 13 – NDE Locks

Link LE Locks to GWE – ENGAGE Gateway

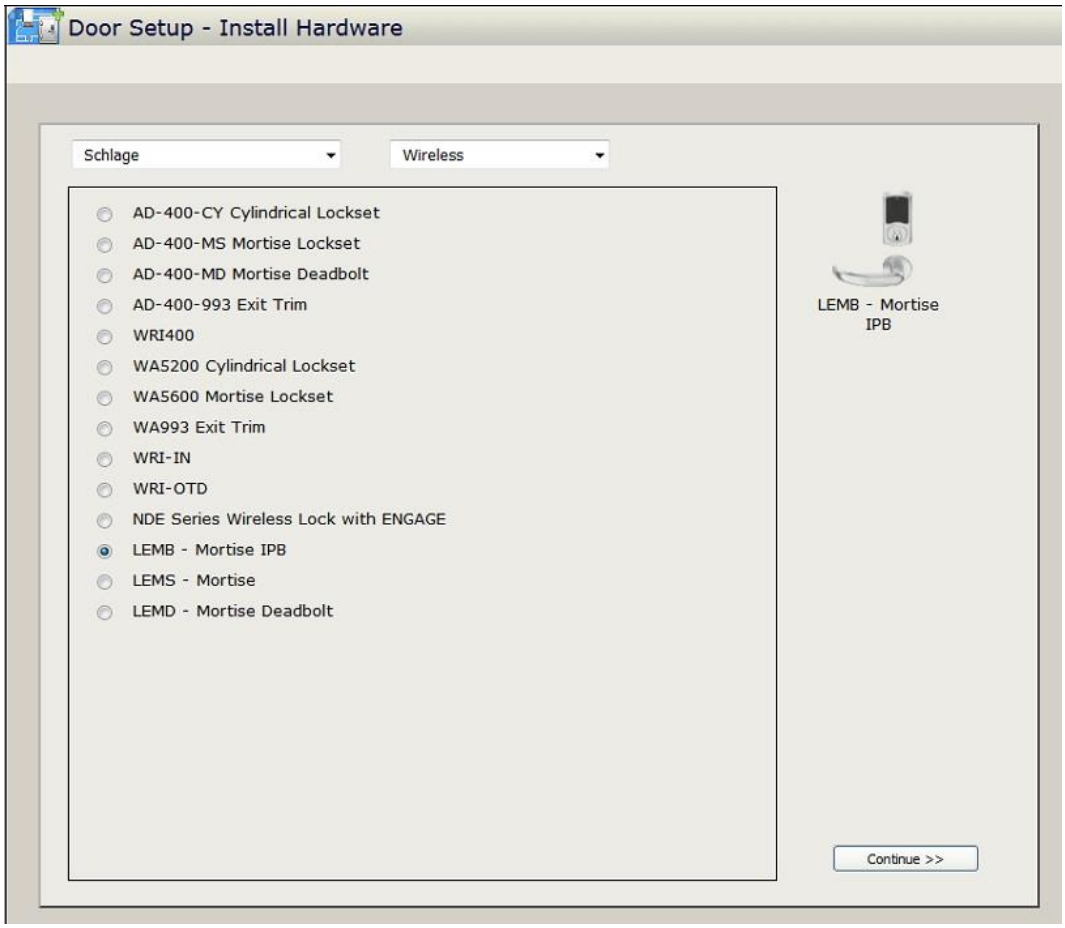
See Chapter 13 – NDE Locks … *the process is the same*

Define LE Lock

Note: If using a Schlage LE Wireless lock, a GWE - ENGAGE Gateway (RS-485) must be programmed before continuing. Please see the GWE - ENGAGE Gateway (RS-485) section above for more details.

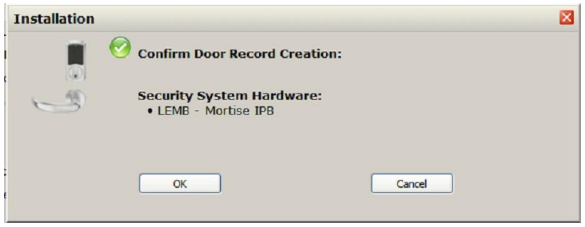
1. Open the **Door Setup** section by clicking on the Door Setup navigation button on the left.
2. Click the **Add doors hardware** button in the Installation Tasks section. The **Door Setup - Install Hardware** window will open.

3 Select **Schlage** and **Wireless** from the drop-down menus at the top.

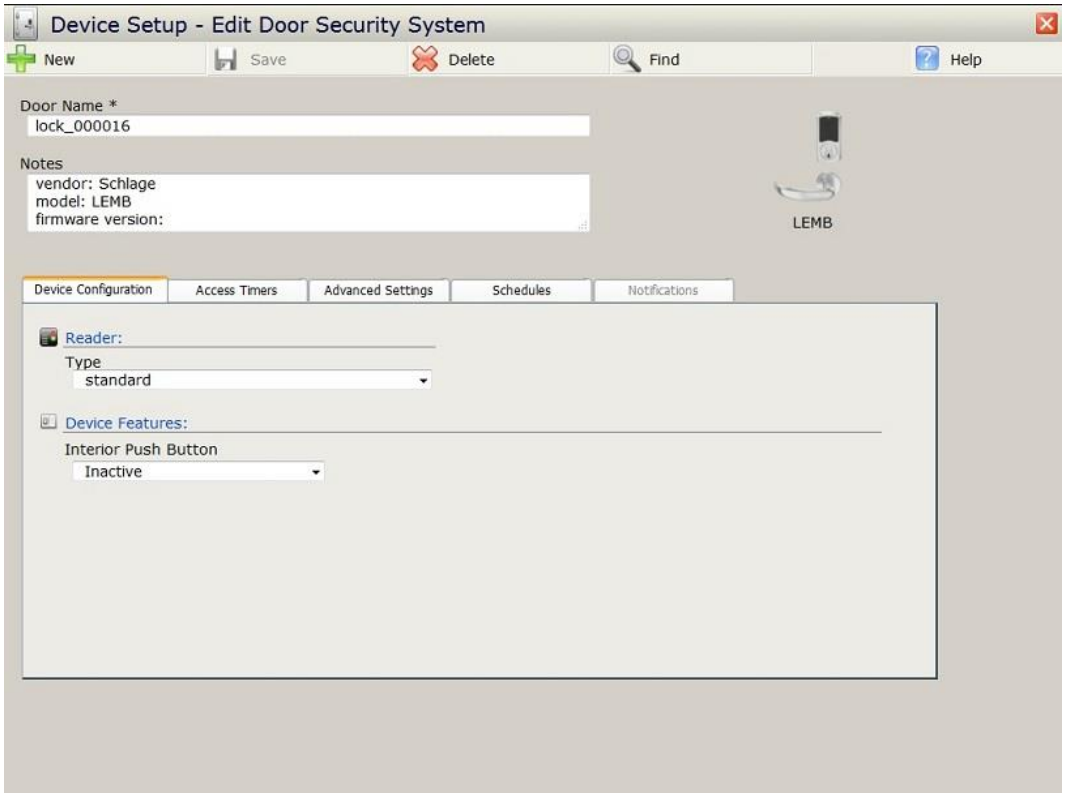


4 Click on the radio button to the left of the type of LE Series Wireless Lock to be set up.

5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.

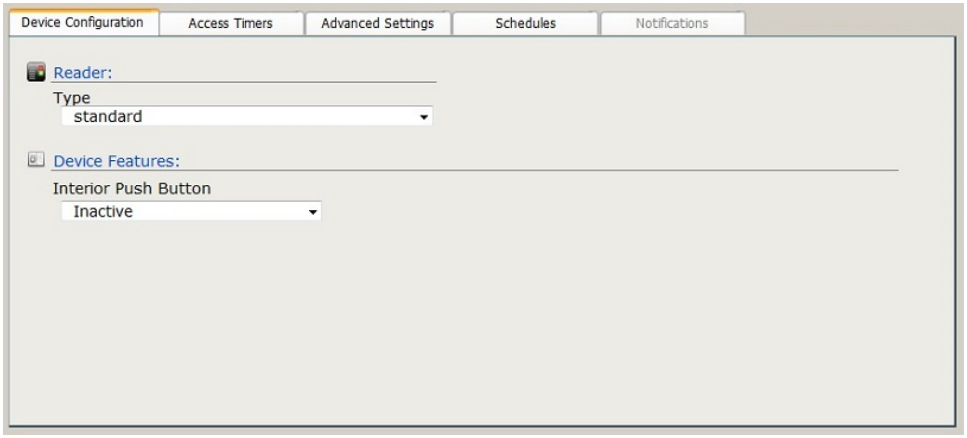


6 Click **Ok** to confirm the correct lock. The **Door Setup - Edit Door Security System** window will open.



7 Complete the **Door Name** and **Notes** fields.

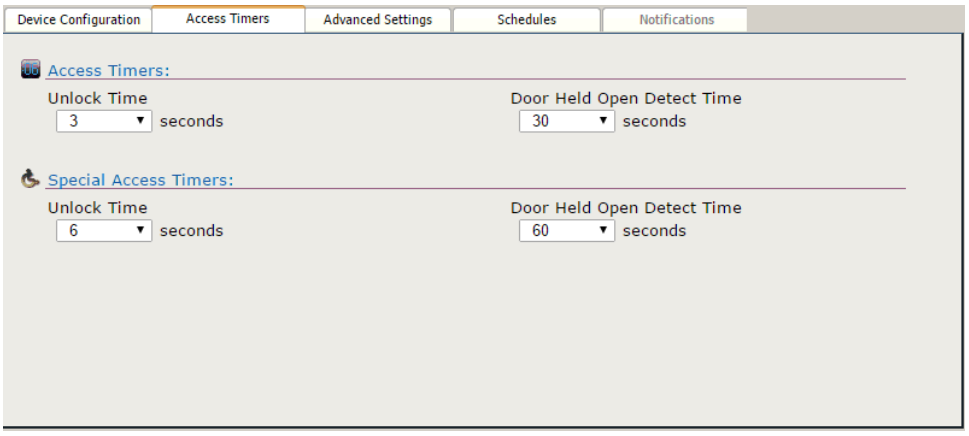
8 Select the **Device Configuration** tab in the bottom half of the screen.



9 Define the following **Reader Type** options:

- **Standard** - Readers for any location not using antipassback.
- **Entry** - Readers that are defined as entry readers for antipassback purposes.
- **Exit** - Readers that are defined as exit readers for antipassback purposes.

10 Now select the **Access Timers** tab.



11 Define the following **Timers** options:

a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.

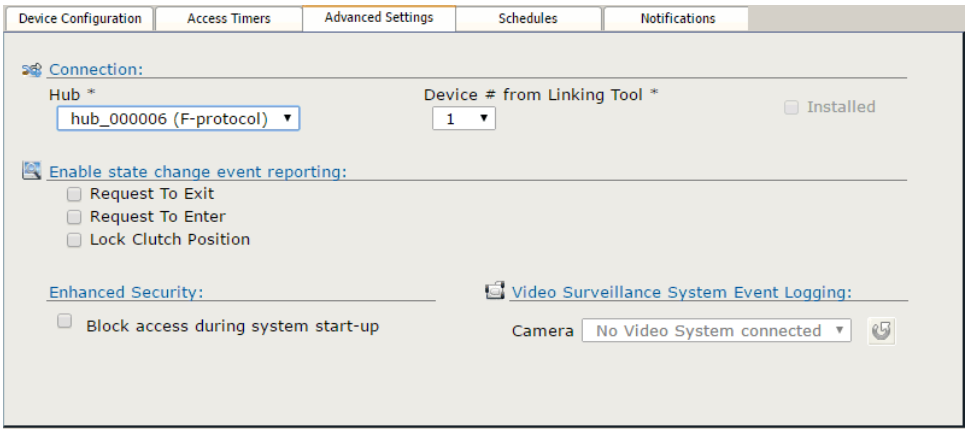
b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.

12 Define following **Special Access Timers** options:

a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.

b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

13 Select the **Advanced Settings** tab in the bottom half of the screen.



14 Define the following options in the **Connection** section:

a) Select the Gateway that the lock is connected to from the **Hub** drop down box.

b) Set the **Device # from Linking Tool** to the exact number specified by the Allegion ENGAGE Mobile App. Please see the LE Wireless Lock section of the installation guide for more details.

c) **Installed**. Click this box if this lock is currently installed on the system.

15 Select the desired options in the **Enable state change event reporting** section:

a) Check the **Request To Enter** box for the ability to generate reports and see activity based on when the Request to Enter is activated.

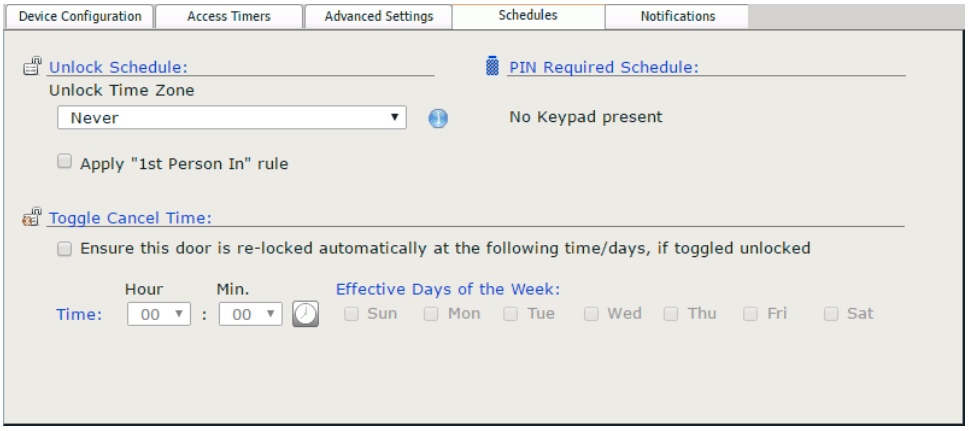
b) Check the **Request To Exit** box for the ability to generate reports and see activity based on when the REX is activated.

c) Check the **Lock Clutch Position** box for the ability to generate reports and see activity based on when the lock's clutch is engaged/disengaged.

16 Check the **Block access during system start-up** option under **Enhanced Security** if you wish to disable access to this door any time the system restarts.

17 If the **lite blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.

18 Select the **Schedules** tab in the bottom half of the screen.



19 Select the desired options in the **Unlock Schedule** section:

a) Select the time zone for the door using the **Unlock Time Zone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button with the mouse. An information window will open showing the schedule of the selected time zone.

b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. If a door has an **Unlock Time Zone** and this rule is selected, the door will not automatically unlock unless a valid credential is presented within the specified time zone. A credential holder must also have this feature enabled for a credential to activate the 1st Person In feature (see the Adding Personnel section for details on adding this feature to a person).

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked until a person with this feature is in the building. Select the 7:00am to 5:00pm Time Zone and check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after a person who also has this feature enabled has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

20 **PIN Required Schedule** will not present any options. A **Keypad o**ption is not currently available for the NDE Wireless Locks.

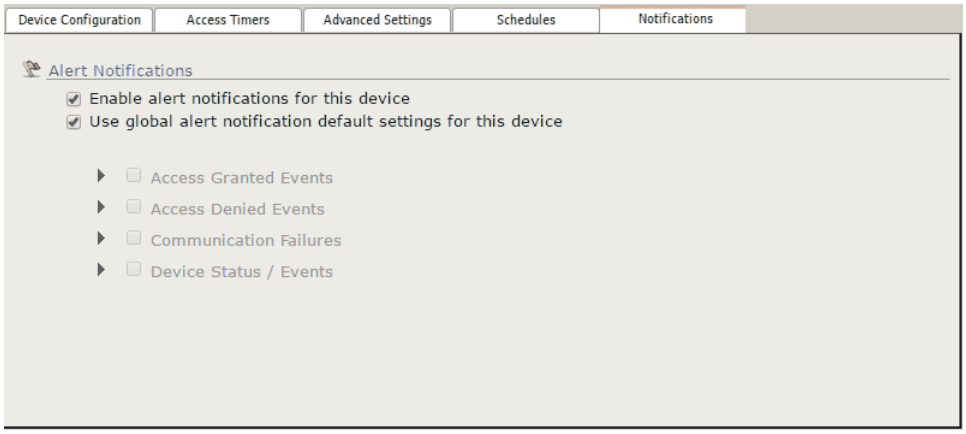
21 Define the following options in the **Toggle Cancel Time** section:

a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:** box to enable this feature. This will lock this door automatically at the specified time.

b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.

c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.

22 Select the Notifications tab in the bottom half of the screen.



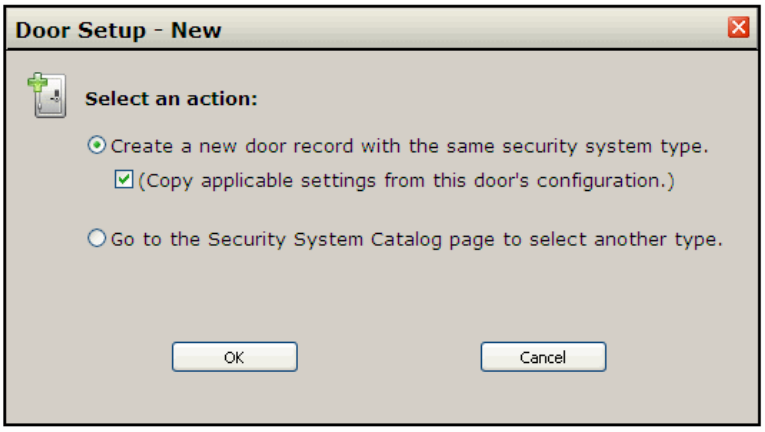
23 Select the desired alert notifications for the device:

a) Check the **Enable alert notifications for this device** box to enable email alerts for this door.

b) Check the **Use global alert notification default settings for this device** box to use the global alert settings for this door (see Utilities - View of modify alert notifications). Uncheck this box to override the global default settings and customize the alert notifications for this door.

24 Click the **Save** button at the top of the screen. The screen will refresh and the door will be saved.

25 To add additional locks, click the **New Door** button at the top of the screen. **The Door Setup - New** pop-up window will open.



26 Select from the following options:

- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat the steps above.

- **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat the steps above.
- **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Hardware** window will open. Follow the steps for the lock type selected.

Schlage Wireless Readers

CHAPTER 15

Wireless reader

Overview

Schlage wireless devices can be seamlessly integrated with the **lite blue** system. The PIM-SBB (Legacy) communicates directly to **lite blue** via RS-485 protocol and can support up to 16 Schlage wireless devices.

Abbreviations

Terms and description

Term	Description
PIM	Panel Interface Module
WAPM	Wireless Access Point Module
WRI	Wireless Reader Interface

The Schlage Wireless Access product line contains several variations of the same module.

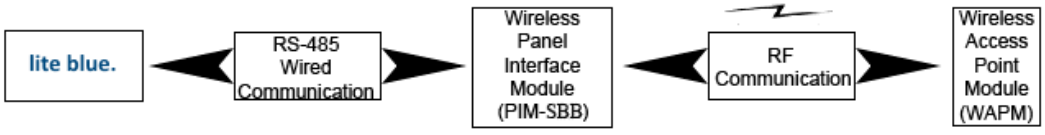
Wireless Access Modules

Name	Acronym	Type
Panel Interface Module	PIM	PIM
Wireless Access	WA	WAPM
Wireless Reader Interface	WRI	WAPM

Schlage Wireless System Components

There are various wireless devices that are used to integrate with **lite blue**. The Schlage wireless system contains two different types of modules:

- One wireless panel interface module (PIM)
- Up to 16 wireless access point modules (WAPM)



Wireless system block diagram

The PIM (PIM-SBB Legacy) is hard wired to the **lite blue** power and communication channels via RS-485 protocol. The PIM installation location is determined by the location of the WAPM with which it will communicate via radio frequency (RF).

The WAPM is installed at the access point where access will be controlled and/or monitored. Some wiring at the access control point may be required, depending on the application being applied to the WAPM .

Regardless of which WAPM is used, the communication link is always RF.

Wireless Panel Interface Module - PIM-SBB (Legacy)

The PIM-SBB (Legacy) works in conjunction with several types of wireless peripherals devices. The PIM-SBB module is hard wired directly to the **lite blue** power and communication channels via RS-485 protocol. The PIM-SBB can support up to 16 wireless devices (8 on **lite blue**).

Note: Only PIMs with firmware version 3.13 or higher are compatible with **lite blue**. Check the firmware version by holding down the Reset button (S3) until the LEDs (CR6-10) start blinking. The red LEDs will blink first and display the first part of the firmware version, then the green LEDs will blink displaying the second part of the firmware version. Example: the reset button is pushed and the red LEDs blink 3 times then the green LEDs blink 13 times to indicate firmware version 3.13.

The PIM is capable of configuring (via laptop) the following items:

- Heartbeat interval
- Relock time
- Card format type
- Extended unlock
- Polarity of status signals
- Latch type
- Query intervals and quantity for unlock requests
- Cache mode
- Lock state in case of RF communication loss
- Relock action (timer only, door open or timer or door closed or timer card code conversions)
- Frequency agility for increased interference immunity
- Addressing - Automatic during Linking

Card formats

- The PIM-SBB accepts card formats up to 255 bits

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 20% RH to 95% RH (non-condensing)
- Operating Voltage: 7.5 to 14.0 VDC. Powered from any data channel on the **lite blue** controller that is supplying 12VDC or separately from UL listed power supply.
- Power consumption: 300mA max.

Radio frequency (RF) - The PIM includes an RF Transceiver

- Spread spectrum
- Direct sequencing spread spectrum
- Frequency: 902-928 MHz
- Data Rate: 62.5 kbps (half duplex)
- Modulo 256 error detection
- Approvals: FCC and RSS-210 (Canada)
- Transmitter Power: Up to 300mA
- Receiver Sensitivity: 90dBM typical
- Remote antenna modules - The PIM-SBB is capable of accommodating Remote Antenna Modules

Specifications for the PIM-SBB

- RS-485 Communication to **lite blue** controller
- Supports 16 Wireless Devices (8 on **lite blue**)
- No VBB-RI is required
- **lite blue** can support multiple PIM-SBB

Schlage Wireless Modules

There are several types of WAPM modules such as the WA series of locks and the WRI. The following sections detail each one of these modules.

WA Series Locks (WA)

The WA series locks are products in the Schlage Wireless Access Point Module (WAPM) category. They contain all of the elements needed to electronically control and monitor access through a door via an RF link. The lock includes a lockset, a Request-to-Exit sensor/switch, an optional Request-to-Enter sensor/ switch, a power supply (battery pack), and terminals for monitoring a door position switch/sensor, a card reader, and an RF transceiver for communicating with another RF transceiver in a Panel Interface Module (PIM) which interfaces with **lite blue**.

Performance

- Verification Time: Typically 0.2 seconds including lock actuation time but not including access panel delays
- Communications (Heartbeat) Interval - Configurable in 15 second increments from 15 seconds to 273 hours
- Addressing - Automatic during Linking

Card reader - Magnetic Stripe Card Reader

- ANSI/BHMA A156.25 compliant Track 2 Clock & Data Output (Some card code conversions available)
- Read Rate - 3 – 50 inches per second
- Card Thickness - 0.030 inches thick
- ANSI/ISO Standards 7810, 7811 1/51 7812, and 7813
- Indoor only

Card Reader - Proximity Reader

- ANSI/BHMA A156.25 compliant
- Compatible with HID proximity cards
- Wiegand output
- Weatherproof bezel and gasket provide protection for outdoor use.
- Card Read Range: up to 4 inches
- Compliance to FCC Part 15, RSS-210 of Industry Canada
- ESD Protection: 12KV

Card formats -The card reader can read all card formats up to 255 bits.

Request-to-exit - The sensor/switch is built-in and will be triggered from the activation of the door lever on the protected side of the door.

Request-to-enter (optional) - The optional sensor/switch is built-in as a momentary switch on the reader.

Strike/Lock - Schlage WA Series Locks provide a way to lock or unlock a door and monitor access from a remote location. They are fail-safe from the protected side of the door. These locks are controlled by **lite blue**.

Cylindrical Type WA5200 Series

- ANSI Grade 1
- Lever Handles
- Fits 2 1/8" diameter hole in door
- Backset: 2 ¾" standard (2 3/8" available)
- Weight: 5.75 lbs.
- Door Thickness: For doors 1-3/8" to 2-1/8"
- 1.2.9.1.1 Latchbolt
- A ½" or ¾" with 2 ¾" backset, or ½" with 2-3/8" backset.
- Door Position - It monitors an external reed type of switch, a magnetically operated switch provided with the lockset to determine door position.

Mortise Type WA5600 Series

- ANSI Grade 1
- Lever Handles
- Weight: 8 lbs.
- Door Thickness: For doors 1-3/4" to 2-3/4"
- Latchbolt - Available with either a ¾" latchbolt or 1" autobolt.
- Door Position - A door position monitoring circuit is available. It monitors a integral reed type of switch, a magnetically operated switch to determine door position.

Operational environment

- Temperature: -35°C to +66°C
- Humidity: 20% RH to 95% RH (non-condensing)

Power source

The Schlage WA Series Locks uses 8 no-button AA alkaline cells welded together into a battery pack insulated with a shrink-wrap wrapper. It has two wire leads and a polarized connector compatible with connector from the WA5200 Series and WA5600 Series PCB.

Operating voltage

- Power Requirements: 5.5 to 13.2 VDC
- Current Requirements: Standby: 55 micro Amps typical (Proximity version)
- Maximum: 400mA peak (transmitting)
- Battery Life - The battery pack is capable of providing power for two years with 40,000 card swipes/presentations per year with a ten-minute heartbeat period. It will provide power for four years at 10,000 card swipes/presentation per year with a 10-minute heartbeat interval or one and a half years at 25,000 card swipes/presentation per year with a one-minute heartbeat interval.

Radio Frequency (RF) - The PIM includes an RF Transceiver.

- Spread spectrum

- Direct sequencing spread spectrum
- Frequency: 902-928 MHz
- Data Rate: 62.5 kbps (half duplex)
- Modulo 256 error detection
- Selectable channels: 1 of 15 standard; 5 groups of 3 increased interference immunity (configurable)
- Approvals: FCC and RSS-210 (Canada)
- Transmitter Power: Up to 300mW
- Receiver Sensitivity: 90dBM typical
- Remote antenna modules - The PIM is capable of accommodating Remote Antenna Modules.

Range - 200 feet on one floor when used in normal office interior construction and up to 600 feet line of sight.

- Transmitter Power - Up to 200 mW
- Receiver Sensitivity - 90dBm typical

Wireless Reader Interface (WRI – Indoor or Outdoor)

The WRI-IN/OUT-12VDC acts as a remote card reading device that communicates via RF with **lite blue** through a mating Panel Interface Module (PIM). The Schlage wireless modules are powered locally with 12 VDC power supply. The modules will transfer a bit stream up to 255 bits from one card reader with any Wiegand, ABA or custom formatted outputs. The WRI-IN/OUT-12VDC acts as a control interface for third party electric locking mechanisms such as electric strikes and magnetic locks. The WRI-IN-12VDC communicates to its mating PIM up to 200' on the same floor in typical office construction and up to 1000' line of site.

Performance

- Verification Time - Less than 0.10 second (not including panel delays)
- Communications (Heartbeat) Interval - Configurable in 1 second increments from 1 second to 18 hours. Heart Beat can be set to 10 seconds for ARO and MRO operation
- Features - Tamper Switch, Door Status Monitoring, Door Strike Relay, Aux Relay, and 2 Reader Head operation.
- Gate Control - WRI /OTD with Optional Long Range Antenna
- Addressing - Automatic during RF Linking

Card formats

- The WRI-IN/OUT-12VDC accepts card formats up to 255 bits.

Operational environment

- Temperature - -35°C to +66°C
- Humidity - 20% RH to 95% RH (non-condensing)

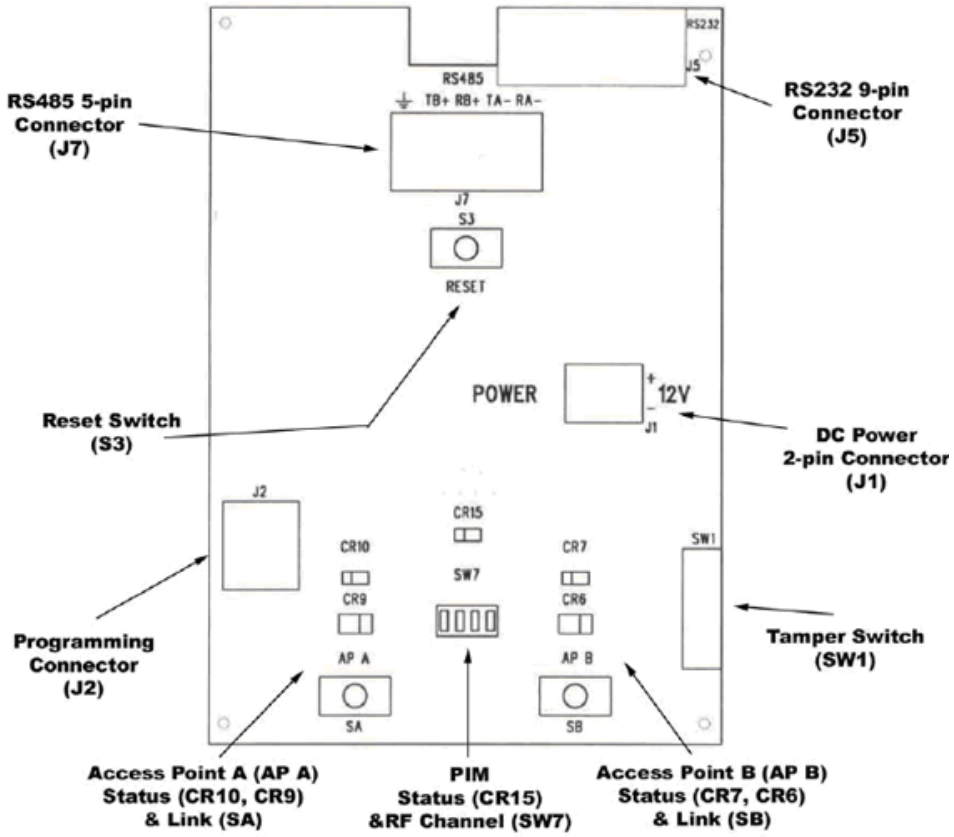
Power source

- Power Requirements - 12VDC power supply (593PI-12VDC recommended)
- Operating Voltage - 7.5 to 14.0 VDC

Radio Frequency (RF) - The PIM includes an RF Transceiver.

- Spread spectrum
- Direct sequencing spread spectrum
- Frequency - 902-928 MHz
- Data Rate - 62.5 kbps (half duplex)
- Modulo 256 error detection
- Selectable channels - 1 of 15 standard; 5 groups of 3 increased interference immunity (configurable)
- Approvals - FCC and RSS-210 (Canada)
- Transmitter Power - Up to 300mW
- Receiver Sensitivity - 90dBM typical
- Remote antenna modules - The PIM modules are capable of accommodating Remote Antenna Modules.

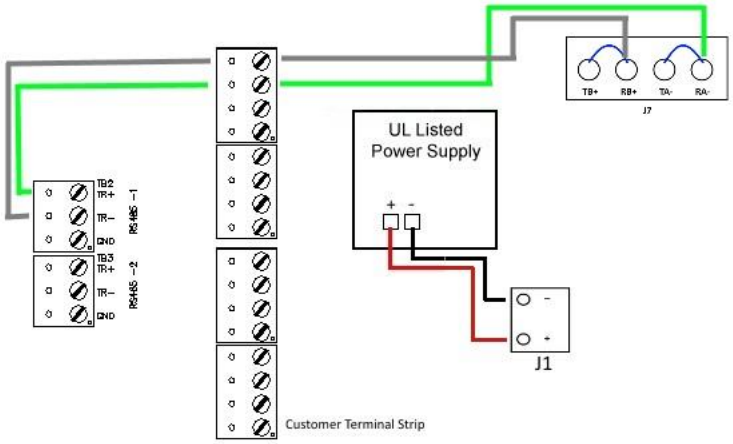
Wiring instructions



All Schlage wireless devices should be powered with a 12VDC power supply. The PIM-SBB (Legacy) can be powered directly from any data channel of the **lite blue** controller that is supplying 12VDC or separately from a local power supply. **lite blue** and the PIM-SBB communicate via RS-485 protocol.

Wiring between lite blue and PIM Module

The PIM receives power at J1 and data at J7. J7 has two pins for Data A and two pins for Data B. The Data A pins (TA- and RA-) must be jumpered together. The Data B pins (TB+ and RB+) must also be jumpered together. The below example is using RS485-1 on the **lite blue** board to J7 and J1 on the PIM.



Data Communication and Power between lite blue and PIM-SBB

lite blue	PIM-SBB J7
RS-485-1 TR+	TA- RA- (jumpered)
RS-485-1 TR-	TB+ RB+ (jumpered)
lite blue	**PIM-SBB J1**
	Pin 1 - PWR (Power)
	Pin 2 - GND (Ground)

Wireless reader modules configuration

The Schlage Wireless Configuration & Demonstration Tool (CDT) must be used to assign each PIM-SBB an address and to address each WAPM connected to it.

A maximum of sixteen (16) wireless readers can communicate with a PIM module on the same channel, with all reader types. Address can be 0 through 15 (panel number 0 to 15 in the CDT). Example - if a WAPM is configured as Panel 5 (door 5) using the CDT, then its corresponding address in **lite blue** is five (5).

Note: All other devices use address 1 through 16. Do not allow the device addresses to overlap when using non-wireless devices in tandem with wireless devices. Example: wireless devices using addresses 0 through 10 require any non-wireless devices to start their addressing at 12.

Device capacities

PIM-SBB (Legacy) modules

- Contact 1 - PIM module
- Tamper state - NC

WAPM modules

- Relay 1 for the lock
- Relay 1 state will be reported back to **lite blue**
- Contact 1 for REX – Normally Open, Non-supervised
- Contact 2 for DOD – Normally Open, Non-supervised
- Contact 3 for Tamper – NC, Non-supervised
- Contact 4 for Battery – NC, Non-supervised
- Contact 5 for Motor – NC, Non-supervised (Currently not applicable)
- Contact 6 for Request to Enter - NC, Non-supervised

WRI

- Relay 1 for the lock
- Relay 1 state will be reported back to **lite blue**
- Relay 2 for Aux Relay
- Relay 2 state will not be reported to the **lite blue**
- Contact 1 for REX – Normally Open, Non-supervised
- Contact 2 for DOD – Normally Open, Non-supervised
- Contact 3 for Tamper – NC, Non-supervised

Linking and addressing locks to the PIM

Requirements - PIM CDT RS-232 cable to the serial port on the PC running the CDT program.

Installing the CDT software

CDT Requirements:

- Microsoft Windows XP or higher
- Microsoft Internet Explorer 5.0 or higher
- Sun Java Runtime Environment (tested with JRE version 6 update 12 or lower, automatically loaded on most computers)

To install the CDT software:

1. go to http://www.wyrelessaccess.com/
2. Go to the Support Icon.
3. Click on **Configuration & Demonstration Tool**.
4. Download and save CDT executable.

Run wireless software

1. A folder will be created called WirelessDemo.
2. Select WirelessDemo.HTML and double click to open.

If the screen looks like the one shown above, the CDT software has been successfully installed. Proceed to configure the PIM. If the screen does appear to be the one shown it is required to install Microsoft Java Virtual machine (MSJVM).

Installing Microsoft Java Virtual Machine

1. Go to http - //realtime.barchart.com/javaprobs.htm
2. Click the link Download Microsoft VM .
3. Download and save old version of the MJVM MSJAVX86.EXE.
4. Execute the file to install the application.

5 This will check for the basic VM and install an older version onto your PC.

Note: Once you have installed the older version of the Java VM, it is recommend that the file be renamed. This will prevent the file being overwritten when the newer version of the application is downloaded.

6 The next step is to download the updates by obtaining the newer version of the Microsoft Java VM from http - //java-virtual-machine.net/download.html.

7 Once the file is on downloaded, execute it and load the Virtual Machine.

8 Re-boot the computer.

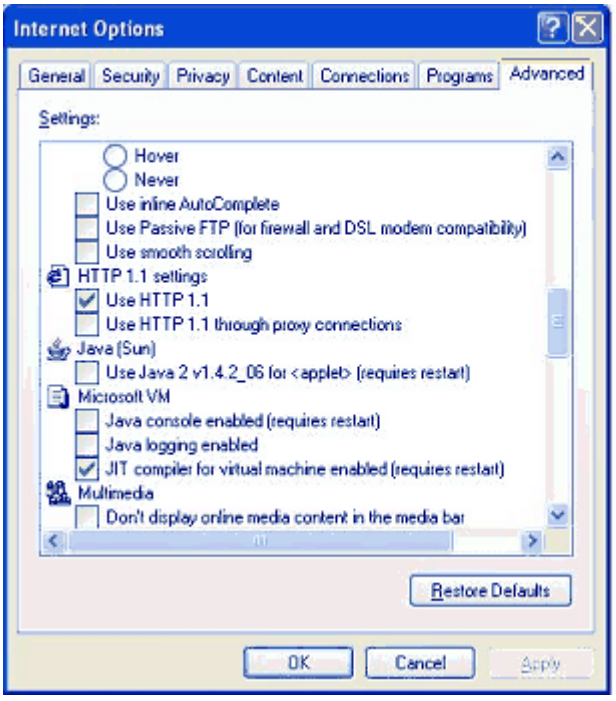
Internet Options

You may now have to setup Java properly in Internet options for the CDT.

1 Open WirelessDemo.HTML.

2 Select **Tools>Internet Options**.

3 Go to the **Advanced** tab.



4 Uncheck the option **Use Java 2x1.4.2-06 for <applet> (requires to start)**.

5 Click **OK**.

6 If there are any problems, restart the CDT application.

Configuring PIM

The next step is defining the PIM address by placing the **PIM** in to **Link Mode**. Follow these instructions.

1 After the CDT software has been installed, execute **WirelessDemo.html** from the Wireless Demo folder.

2 For **PIM Status**, select the proper com port from the drop down menu.

3 Connect the PIM to the PC using a DB9 female to DB9 male that is connected to the PIM RS232 port.

4 After this connection is made, hold down one of the PIM link switches (SA or SB).

a) Continue to hold the link switch and press the reset button (S3). Do not stop pressing the link switch.

b) The LED's (CR6 – 10) on the PIM begin flashing, displaying the firmware version of the PIM. When completed, (CR7 and 10) will continue to flash RED and CR15 will be continue to blink GREEN. At this point, the PIM will be in the CDT link mode as long as the CDT program on the PC remains running and connected to the PIM.

c) Release the link switch.

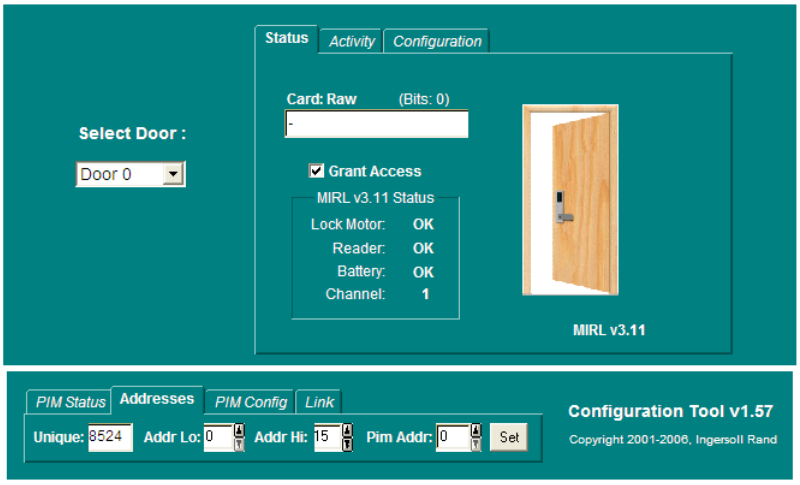
d) On the CDT screen, under PIM Status you should now see the "PIM Connected on Proper Com Port" message.

5 Using the Addresses tab, set the address of the PIM.

a) If one PIM is being used per channel set the **PIM Addr** to 0.

b) If more than one PIM is being used per channel set the PIM Addr of each PIM to the lowest number in the address range. (See the next step for details on address range.)
Example: Channel 1 of **lite blue** will have two PIMs. One PIM will be interfacing with 5 WAPMs and the other will be interfacing with 6. The first PIM will have an Addr Lo of 0 and an Addr Hi of 4. The PIM Addr for this PIM will be 0. The second PIM, when configured, will have an Addr Lo of 5 and an Addr Hi of 10. The PIM Addr for this PIM will be 5.

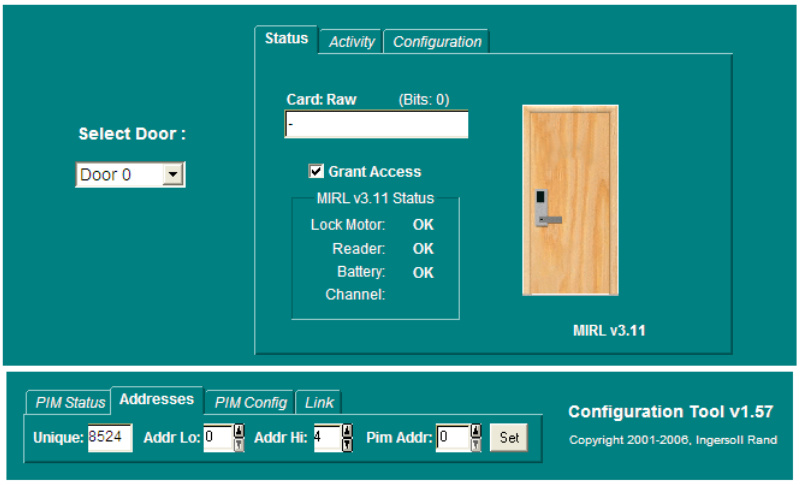
Note: The PIM Addr setting should always be equal to the Addr Lo setting.



Example address settings for a single PIM on a channel

6 Using the Addresses tab, set the range of address for the WAPMs interfacing with the PIM.

a) If one PIM is being used per channel set the **Addr Lo** to 0 and the **Addr Hi** to 15.



Example address settings for the first of two PIMs on one channel

b) If more than one PIM is being used per channel determine how many WAPMs will interface with each PIM and address accordingly.
Example: Channel 1 of **lite blue** will have two PIMs. One PIM will be interfacing with 5 WAPMs and the other will be interfacing with 6. The first PIM will have an Addr Lo of 0 and an Addr Hi of 4. The second PIM, when configured, will have an Addr Lo of 5 and an Addr Hi of 10.

Example address settings for the second of two PIMs on one channel

Note: If multiple PIMs are being used on the same channel it is recommended that room be left in the addressing range for later expansion. Example: Channel 1 of **lite blue** will have two PIMs. At time of installation one PIM will be interfacing with 5 WAPMs and the other will be interfacing with 6. However there may be a time when more WAPMs will be added to these PIMs. The first PIM will have an Addr Lo of 0 and an Addr Hi of 6. This leaves room for an additional two WAPMs to be added to this PIM at a later date. The second PIM, when configured, will have an Addr Lo of 7 and an Addr Hi of 15. This leaves room for an additional 3 WAPMS to be added to this PIM at a later date.

Disconnecting PIM from the link mode

1 To disconnect PIM from the link mode, close the CDT application.

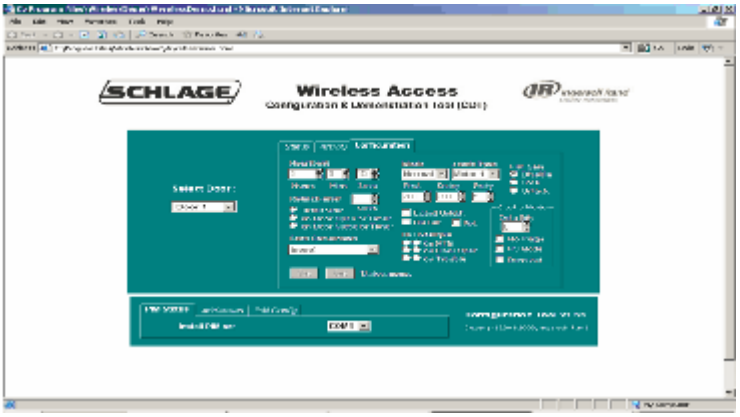
Configuring the WRI

Follow these steps to place the WRI into the Link Mode in order to setup proper panel address. There are two WRI models; WRI -OTD and WRI - IN.

1. Make sure the PIM is already in link mode. See the Configuring PIM section for details.
2. Place the WRI-OTD into the link mode by pressing the reset switch.
3. Place the WRI-IN into the link mode by recycling power.
4. Go to the Link tab on the CDT screen.
5. Using the Panel drop down box select the Address (panel) of the WRI.
6. Click on the Start button. On the WRI the (LED2) will start blinking.
7. Generate a transaction by presenting any card to the reader or by pushing the tamper button. The transactions will display on the CDT software screen. This indicates that the WRI reader has been addressed.
8. Click on the Configuration tab. This tab is used to set the Heartbeat / First / Delay / Retry / FC Mode or Card Number Mode.
   a) The Heart Beat is used to determine how often the WRI communicates with the PIM. Leave this at default.
   b) Set the First / Delay to 300. This is required for proper operation.
   c) Set the Retry to 7. This is required for proper operation.
9. Click on the Set button at the bottom of the CDT screen.

Note: A transaction may need to be produced in order for these settings to be sent to the WRI.

10. Make a note of the address as this will be used by the **lite blue** user interface to configure the lock.
11. Configuration of the WRI is complete. To set up another WRI follow steps 1 through 10 above.



Disconnecting WRI from the link mode

1. To disconnect WRI from the link mode, close the CDT application.

Configuring WA Series Locks

Follow these steps to place the WA Series Lock into the Link Mode in order to setup proper address

1. Make sure the PIM is already in link mode. See the Configuring PIM section for details.
2. Go to the Link tab on the CDT screen.
3. Using the Panel drop down box select the Address (panel) of the lock.
4. On the CDT screen, click on the Start button.
5. To put the lock in link mode, activate the Exit Request handle and hold it down while presenting a card to the reader.
   a) Continue holding down the Exit Request for approximately 15 seconds.
   b) The LED on the lock will begin blinking Green very rapidly.
   c) Release the Exit Request Handle.
   d) The Green LED will continue to blink while the Linking process takes place. When the Link process is completed, the LED will stop and then blink Green slowly and a tone will be heard for a number of repetitions.
6. Generate a transaction by presenting any card to the reader or by pushing the tamper button. The transaction will display on the CDT software screen. This indicates that the lock has been addressed (see figure below).

7. Click on the Configuration tab. This tab is used to set the Heartbeat / First / Delay / Retry / FC Mode or Card Number Mode.
   a) The Heart Beat is used to determine how often the lock communicates with the PIM. Leave this at default.
   b) Set the First / Delay to 300. This is required for proper operation.
   c) Set the Retry to 7. This is required for proper operation.
8. Click on the Set button at the bottom of the CDT screen.

Note: A transaction may need to be produced in order for these settings to be sent to the lock.

9. Make a note of the address as this will be used by the **lite blue** user interface to configure the lock.

10 Configuration of the lock is complete. To set up another WA series lock, follow steps 1 through 9 above.

Disconnecting WA Series Locks from the link mode

1 To disconnect lock from the link mode, close the CDT application.

VEVMS-VBB Video Server Integration

CHAPTER 16

VEVMS-VBB

Overview

Integrating a **lite blue** access control panel with the **VEVMS DVR/NVR** will provide the ability to view and search video based on **lite blue** transactions. After configuring **lite blue** to communicate with an VEVMS DVR/NVR, alarms can be shown in **Video Control** or **MultiVideo Remote** based on transactions. In addition, recorded video can be displayed based on transaction searches in the **Playback** application.

For smaller VEVMS systems, such as a system with only one **VEVMS-VBB DVR/NVR** installed, it is recommended to use the **Central Security Remote** application to manage **VEVMS Remote Client** users. Central Security Remote is used in place of the **Enterprise Management System** (i.e. **Video System Security** and the **Video Launcher**), and is much simpler to setup and configure. See the VEVMS Manual for details on the full VEVMS system.

Note: The VEVMS-VBB video recorder will only support a maximum of (4) **MJPEG** IP cameras at any time. Exceeding the limit of MJPEG IP cameras can cause the system to be unstable. The VEVMS-VBB **will** however, support all cameras using **MPEG4.**

Cameras

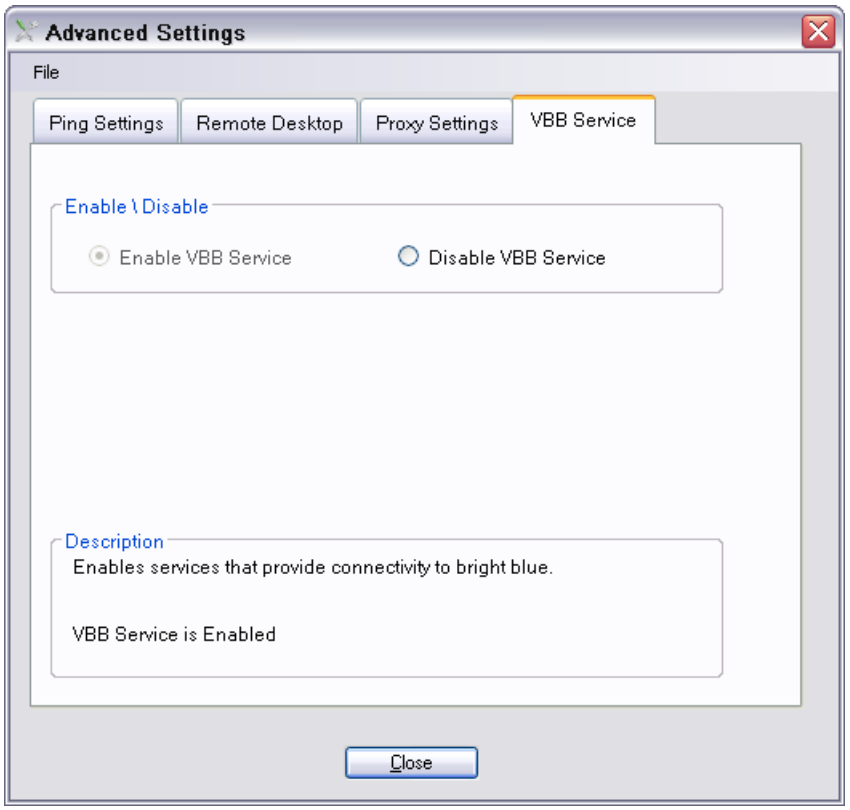
The following cameras are compatible with the VEVMS-VBB Video Server:

Coax/Serial PTZ Cameras and Switches	IP CAMERAS
MIGVAN	JVC VN-C11U
Phillips Camera	JVC VN-C20U
ULTrak	Panasonic WV-NM100 (PTZ)
Phillips Control (switch)	Panasonic WV-NS324 (PTZ)
AD: AN001	Panasonic WV-NS202 (PTZ)
AD: 168 & MP48	AXIS 2xx (PTZ)
Panasonic WV-CS850A (new)	Sony IP (PTZ)
Panasonic WV-CS850A	Sony IP (Fixed)
Pelco "D"	Mobotix M10
AD SpeedDome Ultra VII	VCS_VIP-10/1000
Pelco Matrix Switcher	Toshiba IK-WB02A
Kaletel-RS422	Toshiba IK-WB
Panasonic WV-CS950	UDP IPC PTZ
Panasonic WV-CS850B	Analog to Digital IP Encoders
Panasonic WV-CW860A	Mango (CGI)
Pelco G	Mango DSP
If connecting cameras directly to VEVMS then the following converter is needed: **RS232/485 or RS232/422**	UDP NVE
	Mango IPD-552

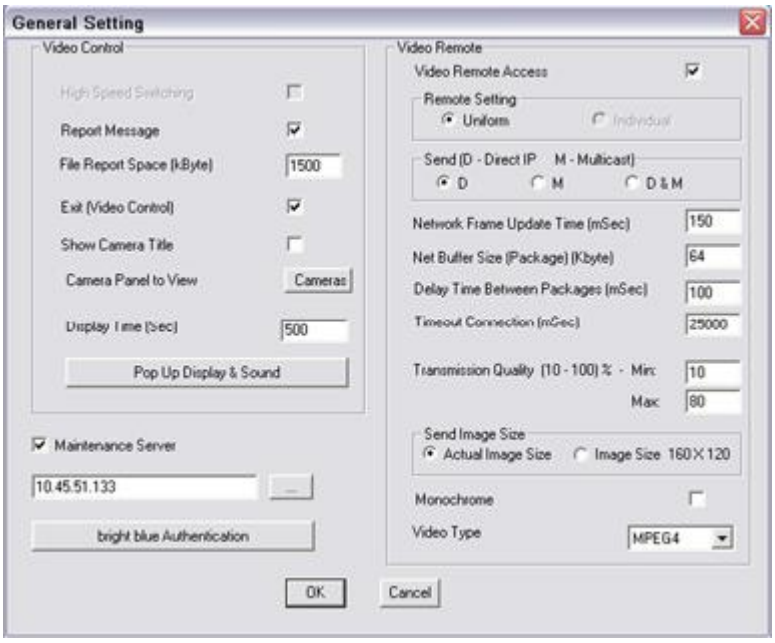
Configuration

To configure **lite blue** to work with an **VEVMS DVR/NVR**, follow these steps:

1 On the **VEVMS DVR/NVR**, go to **System Tools --> Advanced Settings**. Click the **VBB Service** tab, and then click **Enable VBB Service**.



2 Go to **Video Server Settings --> General Settings**. The General Settings window will open.



3 Click on the **lite blue Authentication** button. The lite blue Authentication window will open.

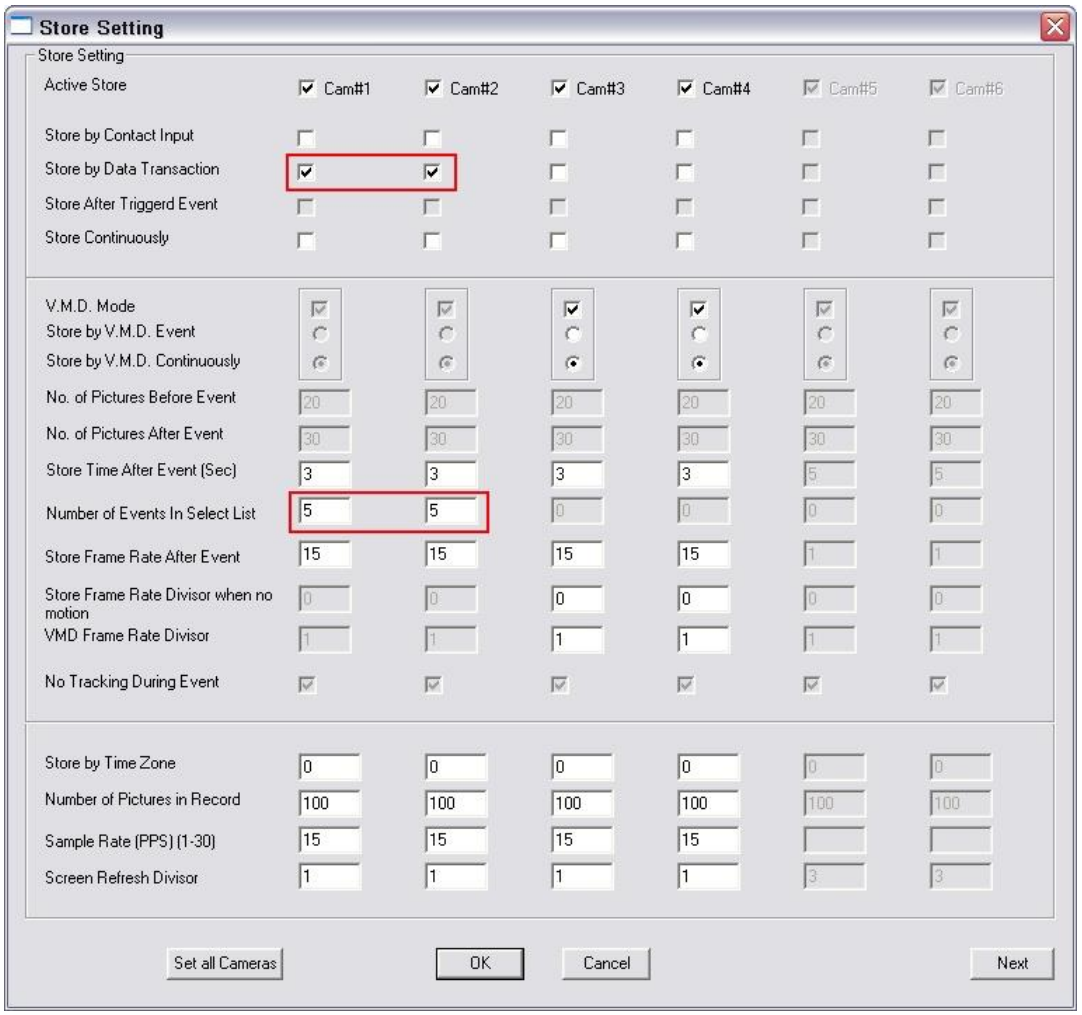
a) Enter **vanderbilt** into the User Name field.

b) Enter **vanderbilt** into the Password field.

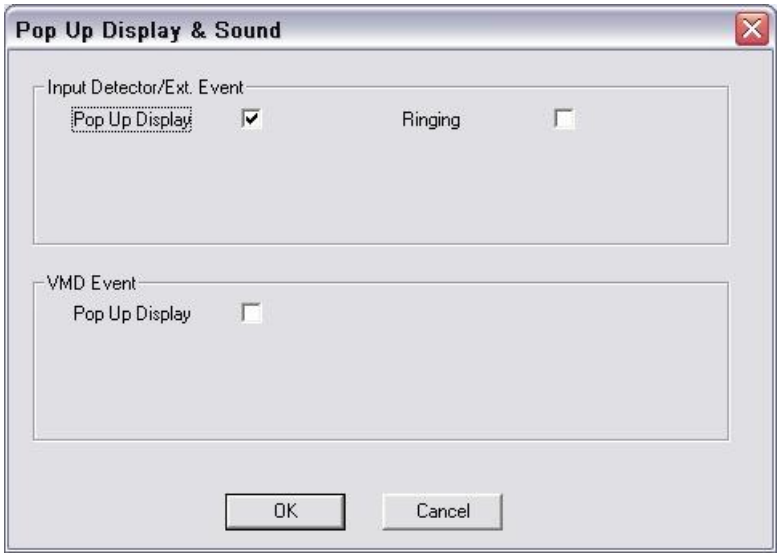
c) Enter **vanderbilt** into the Password Confirm field.

d) Click the **OK** button. The window will close; lite blue Authentication is complete.

4 Go to **Video Server Settings --> Store Settings**. Enable "**Store by Data Transaction**" for any cameras that will be recording based on **lite blue** transactions. Also configure the **No. of Pictures Before Event** and **No. of Pictures After Event** fields, as well as the **Number of Events in Select List** (if **Shift + Right Click** in Video Control is desired). Cameras configured to record based on lite blue transactions can also be configured to record by **VMD Continuously** (in addition to lite blue transactions). VMD Event, Store by Contact Input, and Store Continuously cannot be used in addition to lite blue transactions.

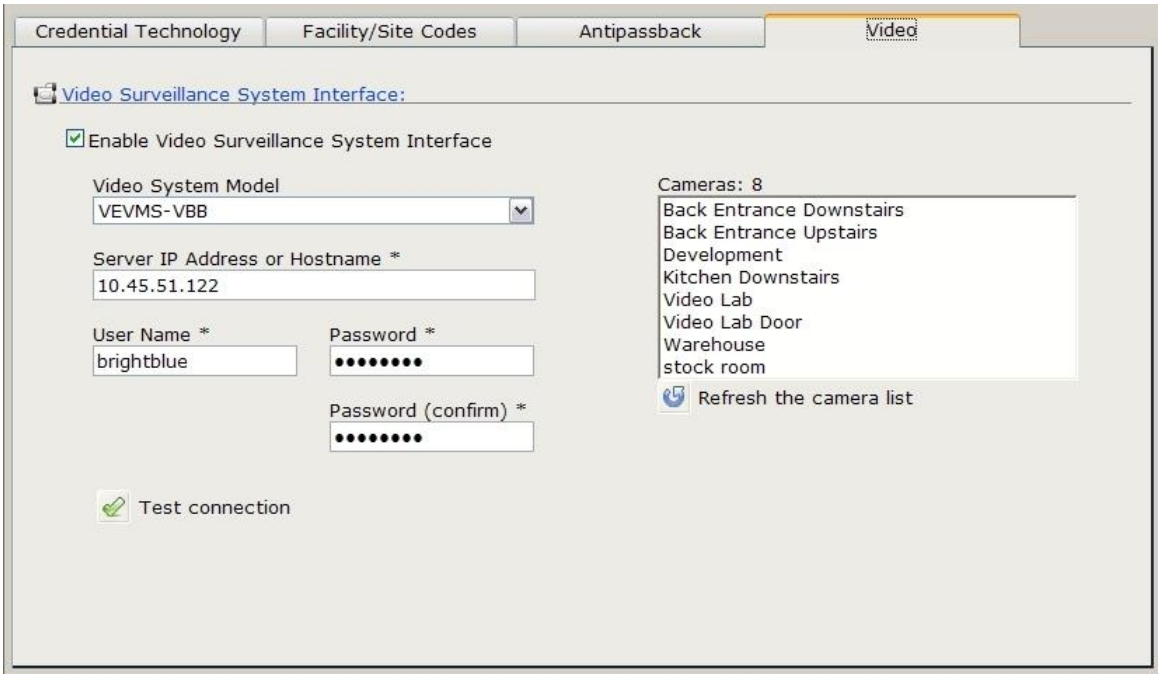


5 Go to **Video Server Settings --> General Settings** and click "**Pop Up Display and Sound**" to enable alarm notification in **Video Control**. Enabling **Pop Up Display** will maximize Video Control and show a red border around the camera when a **lite blue** transaction occurs. This also enables the **Shift + Right Click** feature in Video Control, which will display a list of the last few lite blue transactions. The number of transactions displayed using **Shift + Right Click** is defined in Step 2.



Note: Step 4 through **Step 6** must be completed within the **lite blue** interface from an external PC. These steps cannot be accomplished from the VEVMS DVR/NVR itself.

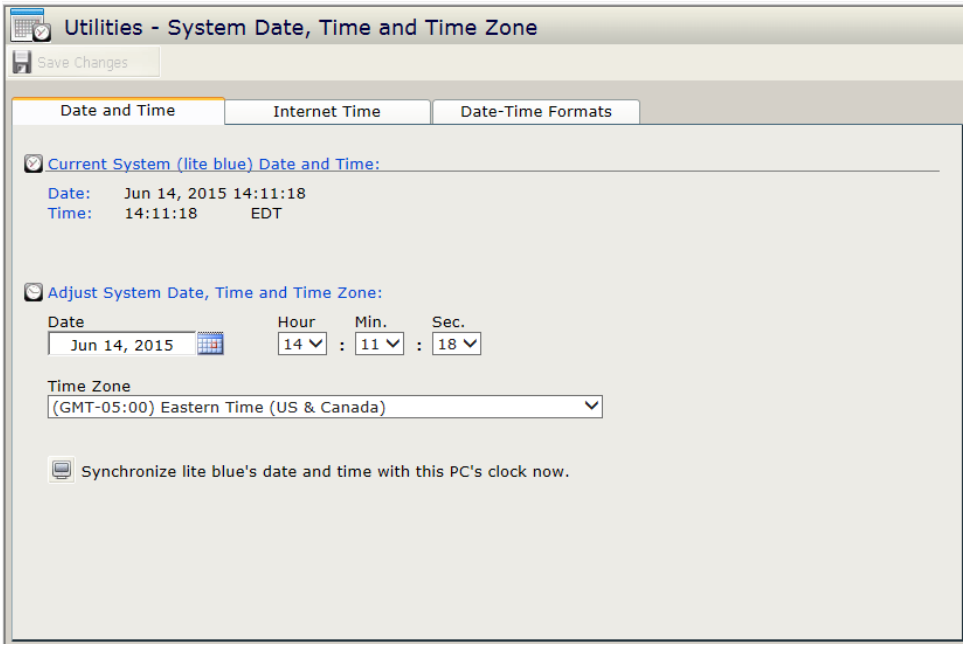
6 Once the **VEVMS DVR/NVR** has been setup properly, the **lite blue** video settings will need to be configured. In the **lite blue** software, go to **Door Setup --> View or Modify Global Settings** and switch to the **Video** tab. Check off "**Enable Video Surveillance System Interface**" and enter the IP address, user name (vanderbilt) and password (vanderbilt). Click **Save Changes** to establish a connection. If successful, the camera list will appear on the right hand side.



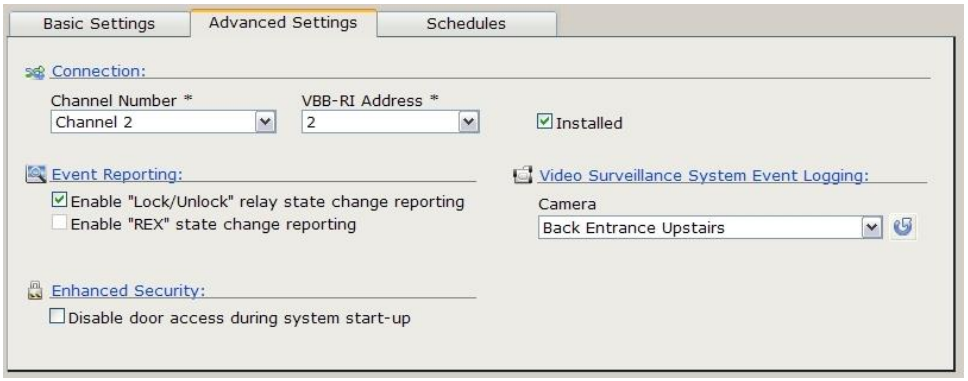
7 After making the initial connection, the **Time Zone** and **Date / Time settings** must be synchronized between **lite blue** and the **VEVMS DVR/NVR**. Go to **Utilities --> Set System Date, Time and Time Zone** and then configure the Time Zone (if necessary). Click **Save Changes** before attempting to synchronize the date and time.

Note: The **Time Zone** in **lite blue MUST** match the Time Zone configured on the VEVMS DVR/NVR. Please ensure that the VEVMS DVR/NVR has the correct Time Zone configured before completing **Step 5**. The VEVMS DVR/NVRs Time Zone is displayed on the Date and Time tab in **lite blue**.

After saving the updated Time Zone, click "**Synchronize lite blue's date and time with the Video Surveillance System now.**" The time will continue to be synchronized regularly between lite blue and the VEVMS DVR/NVR.



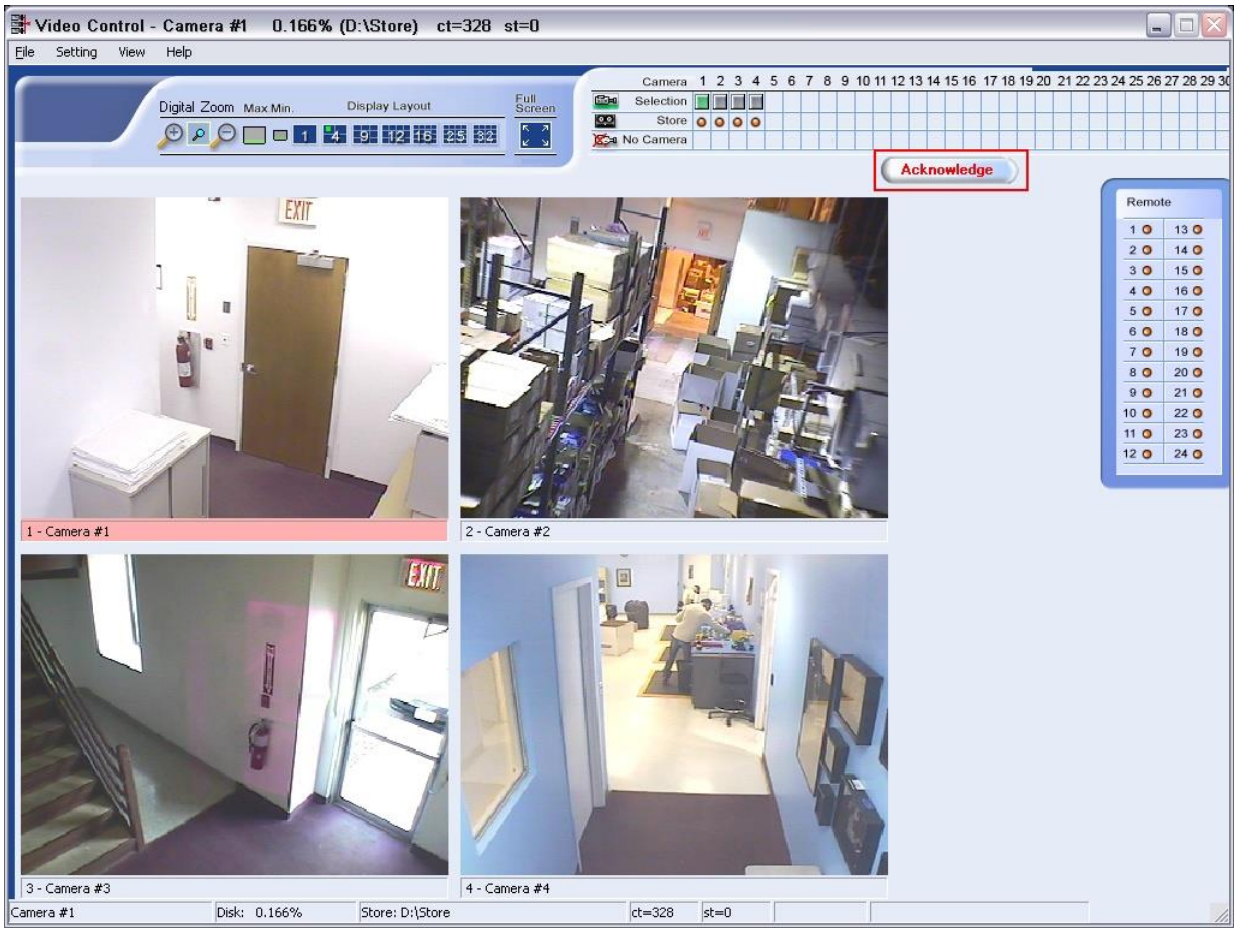
8 The doors in **lite blue** must be linked with cameras on the VEVMS DVR/NVR. Go to **Door Setup --> View or Modify Door Configuration** and select the Door that is to be linked with camera. Switch to the **Advanced Settings** tab, and select the desired camera from the drop down list. Click **Save Changes** to complete the **lite blue** configuration.



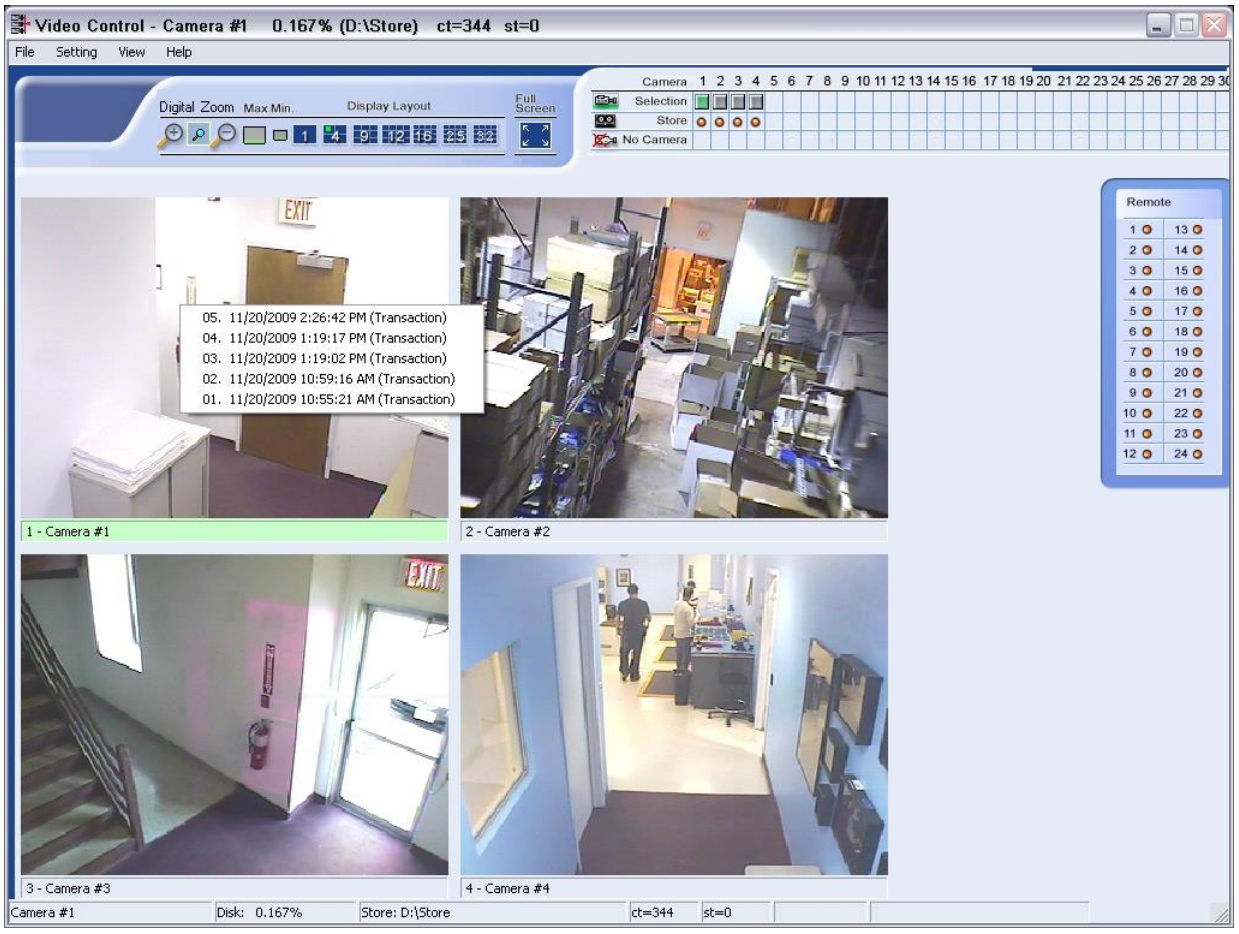
Viewing lite blue Transaction Alarms

If **Pop Up Display** is configured, incoming transactions from **lite blue** will create alarms in **Video Control**. For details on Pop Up Display see the VEVMS Manual.

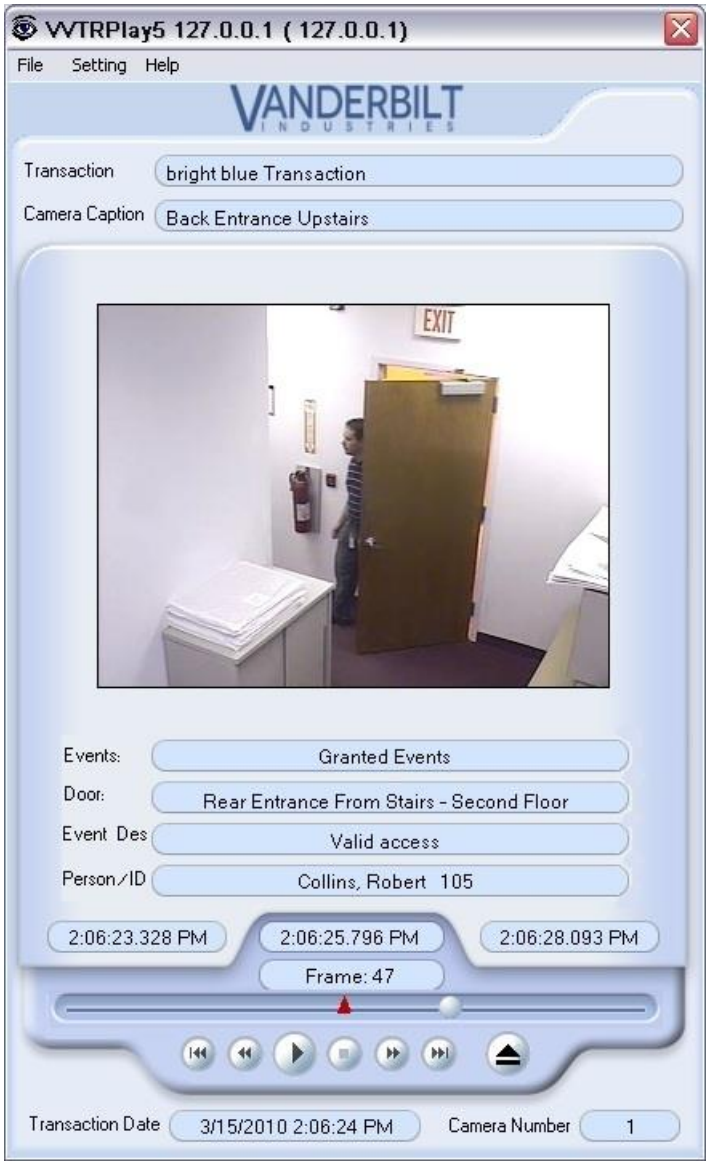
View Video from the Current Alarm - When an alarm comes in, the camera title bar will turn red, and an **Alarm Silence** / **Acknowledge** button will also appear in the upper right hand corner. To view the most recent alarm, hold down the **Shift** key and then **right click** the camera's picture. Click "View Recorded Video for this Event" on the drop-down menu to view the video from the current alarm.



View Video from a Recent Alarm - Once the Alarm Silence / Acknowledge button is clicked, holding down **Shift** and **right clicking** on a lite blue linked camera will display a drop-down list of recent alarms. The number of alarms shown in this list is defined in **Video Server Settings --> Store Settings** in the "**Number of Events in Select List**" field. Click on an alarm to view the video associated with that transaction.



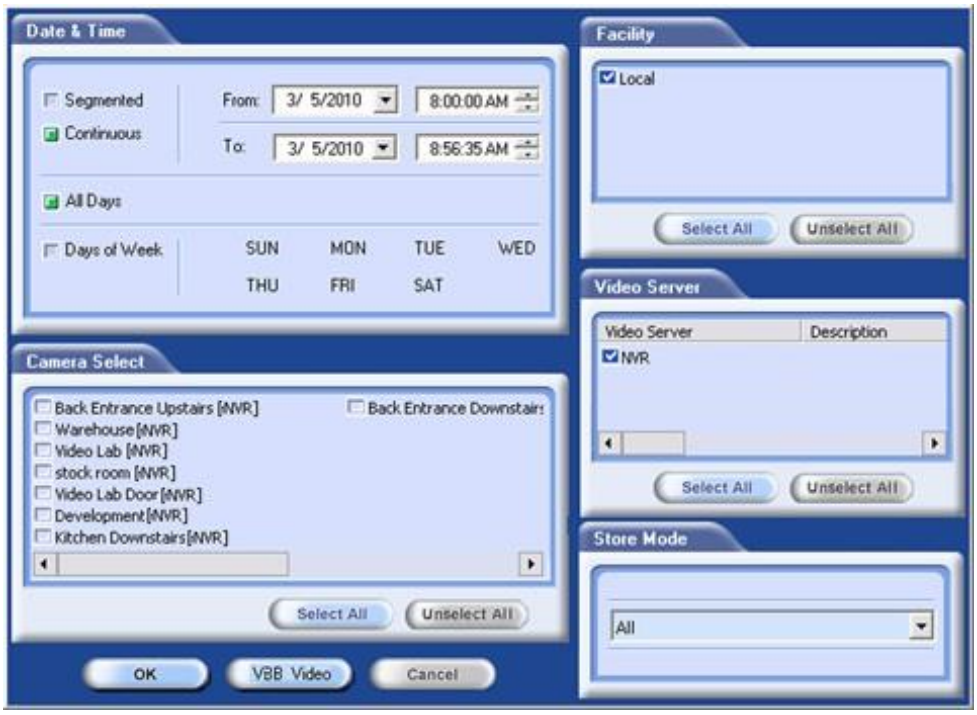
VVTRPlay5 - When an alarm is selected using either of the previous two methods, the **VVTRPlay5** window will appear. The video associated with the transaction will play automatically. VVTRPlay5 includes standard controls to Pause, Fast Forward, and Rewind the video transaction. Any **Meta Data** associated with the transaction is also displayed, such as **Event Type**, **Door Name**, **Event Description** and **Person Name / Encoded ID**.



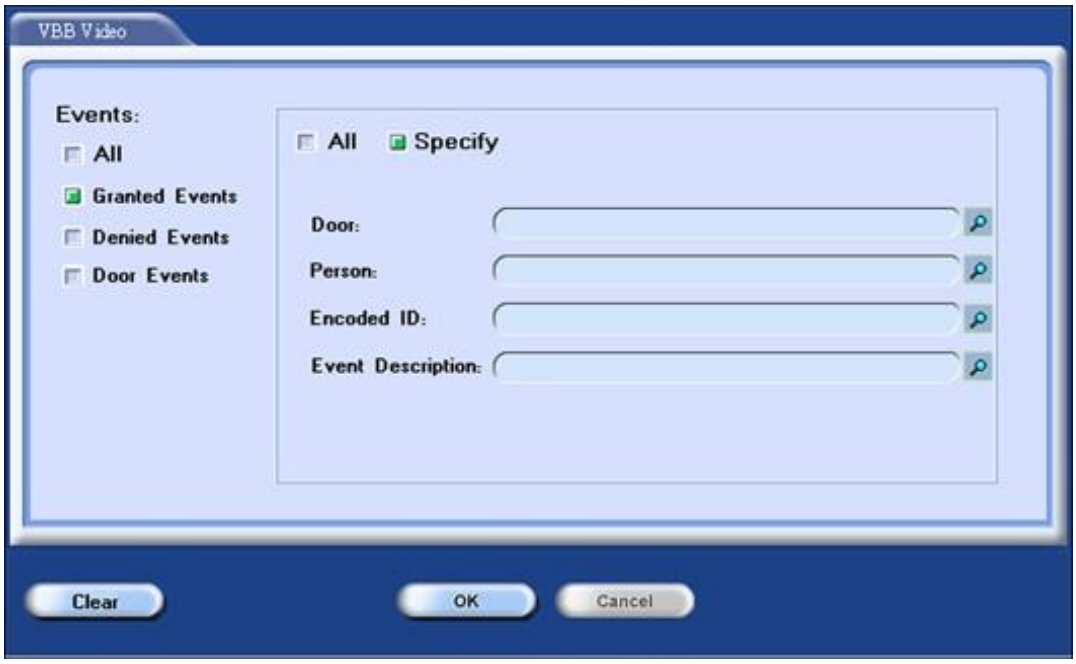
Searching for lite blue Transaction Alarms

Video can also be searched through based on **lite blue** transactions. This is done through the standard Find utility in the **Playback** application by following these steps.

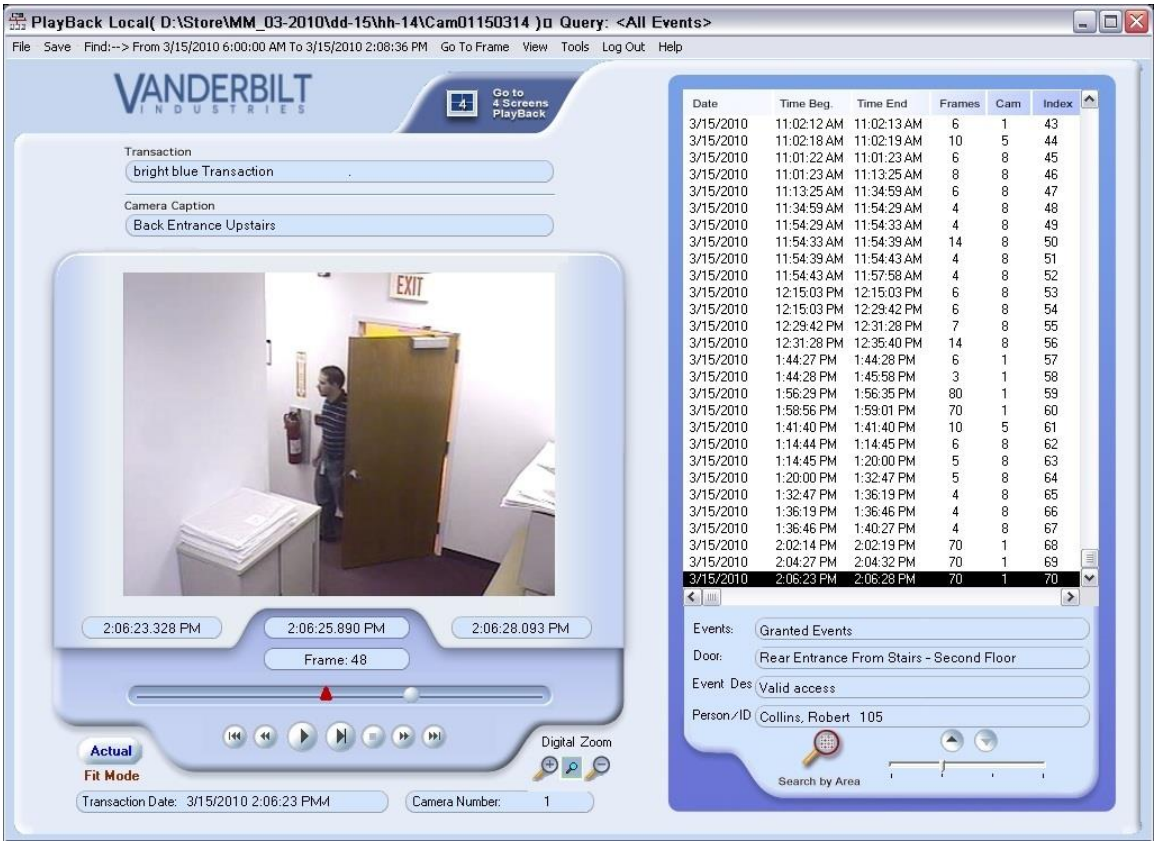
1 Select the desired Date / Time range, Facility, VEVMS DVR/NVR and Camera(s), then click the **VBB Video** button.



2 Specify the **Event Type** or keep the default of **All Event Types** and click OK.



3 View the associated video in **Playback.** It will appear like any other video event type (VMD, Contact Input, etc.), except extra fields will appear listing any **Meta Data** associated with the transaction, such as **Event Type**, **Door Name**, **Event Description** and **Person Name / Encoded ID**.



Troubleshooting

CHAPTER 17

Overview

This chapter details how to troubleshoot and fix various issues with lite blue. If your system is not functioning properly, check this chapter for possible fixes. If you do not find your problem here, or if the recommended fix does not solve the problem, contact technical support for assistance.

Device Communication

If devices are not communicating, there may be:

- Device addressing Issues
- Wiring problems

Device Addressing Issues

If multiple RS-495 devices are given the same address on installation all or some of the devices will not work or will only work intermittently. To correct, disconnect all of the devices and reconnect one at a time to diagnose the problem. Re-address the duplicate device to a unique address.

Wiring Problems

If the communication wiring to a device is reversed, communication to all other devices on that channel may go down. To correct, disconnect all of the devices and reconnect one at a time to diagnose the problem. Once the reversed device is found, wire correctly.

Upgrading Software

Manually Unlock Doors for Upgrade

When finishing an upgrade of the **lite blue** software, the system will briefly lose communication, causing the doors to lock. It is recommended that you use the Door Status and Control section of **lite blue** to manually unlock any commonly used doors before running the upgrade. The doors will stay in the unlock state until system communication is restored, at which point they will revert to their normal function.

Disable Encryption

If upgrading to 2.0 or above it is necessary to turn off SSL encryption. See the lite blue Pin Functions section for details on disabling SSL.

File Not Authorized Warning While Upgrading

Check the date that lite blue is set to. This error occurs if lite blue's date is out of synch with the current date. If the date will not reset the battery needs to be changed. See the Battery Replacement section for details.

System Reboot

When the system is rebooted (as in the case of a power outage) it takes a little time for the personnel database to reload. During the reloading process the doors of the system will function normally, however activity will not be logged until the reloading process is finished. This means that the Activity Monitor and the Door Status and Control sections will not show activity or status until the system has reloaded.

Discovery and Configuration Tool

If either **lite blue** or an VBB-NRI cannot be found by the Discovery and Configuration Tool:

- Check to make sure any local Firewall software is turned off
- Make sure they are on the same local network as the computer running the Discover and Configuration Tool

Errors When Logging In or Saving Records to the Database

If you receive an error message when logging in or when attempting to save data to the database:

1. Hold the **lite blue** RESET/SHUTDOWN Switch located behind the top left corner of the Vanderbilt AP02 Controller for at least 10 seconds.
2. After 10 seconds LED D7 will stay on sold and the **lite blue** will power down within 1 second.
3. Remove power from *MAIN POWER IN VBB* and reconnect to power up **lite blue**.
4. If operation is not restored contact Vanderbilt Technical Support.

Date and Time

Incorrect Date/Time

If the system is working properly, but the date and time are not correct, then the Lithium battery on the **lite blue** board needs to be replaced. See the Battery Replacement section for details.

Slowly Losing/Gaining Time

If the time is either gaining or losing minutes (as in, becomes 10 minutes fast or 10 minutes slow over the course of a day or week) then the Lithium battery on the **lite blue** board needs to be replaced. See the Battery Replacement section for details.

Index

P

R

S

T

U

V

W

X

VANDERBILT

vanderbiltindustries.com

Vanderbilt Industries
2 Cranberry Road
Parsippany, NJ 07054
973 316 3900
@VanderbiltInd
Vanderbilt Industries

an ACRE company

04002-1219