SECURITY MANAGEMENT SYSTEM (SMS)

Manual

VANDERBILT

Vanderbilt Industries Copyright Notice

CONTACT INFORMATION

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

Contents

Preface 28

Before Installation 29

Discovery and Configuration Utility 35

VRCNX-R 40

VSRC 103

VMRC-1 171

VMRC-2 189

VRI-1S3 248

VRI-2 / VRI-2S3 256

SRINX (Legacy) 267

Schlage Adaptable AD-300 Series Locks 333

Schlage VIP Locks 339

Assa Abloy Aperio Series Wireless Locks 344

Assa Abloy IP-Enabled Locks 375

Schlage NDE Series Wireless Locks with ENGAGE 426

Von Duprin ENGAGE RM / RU Exit Devices 453

Schlage LE Series Wireless Locks with ENGAGE 461

Schlage Wireless Readers 468

Contact Supervision 490

Index 493

UL Listing Summary

Compatible UL Evaluated Equipment

Vanderbilt Equipment

- VSRC-A / VRCNX-A
- VRINX
- VIONX-8
- VRI-1 / VRI-1S3
- VRI-2 / VRI-2S3
- VI-16IN / VI-16INS3
- VI-16O / VI-16OS3

Legacy Vanderbilt Equipment

- VSRC / VRCNX-R
- SRCNX (Legacy)
- SRINX (Legacy)
- SIONX (Legacy)
- SIONX-24 (Legacy)

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

Hardware Not UL Evaluated

- IP Addressable Module: SIPNX-100 (Legacy)
- Dial-up Modem: SMODNX (Legacy)
- VSRC-M / VRCNX-M

The following devices should be incorporated into your system:

- 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.
- The UL 294 requires that the VRCNX-R, VSRC, SRCNX-R (Legacy) and VRINX/SRINX (Legacy) enclosures have tamper switches that will activate an alarm or trouble signal.

Firmware Designations

VRCNX-R / VSRC Firmware

- **Firmware Upgrade (Flash) File** = "image_rXXX_k1253_aYYYC.SriUpd"

  XXX = Vanderbilt Root File System version of the embedded Linux operating system.
  YYY = Firmware Version
- **Controller Diagnostics Display** = "SRI rootfs vX.XX"

  X.XX = Vanderbilt Root File System version of the embedded Linux operating system.
- **CIM Firmware Display** = "YYY"

  YYY = Firmware Version

VRCNX-M / VSRC-M Firmware

- **Firmware Upgrade (Flash) File** = "image_rXXX_aYYYG_ep4502.SmsUpd"

  XXX = Vanderbilt Root File System version of the embedded Linux operating system.
  YYY = Firmware Version
- **Controller Diagnostics Display** = "SMS-M rootfs vX.XX"

  X.XX = Vanderbilt Root File System version of the embedded Linux operating system.
- **CIM Firmware Display** = "YYY"

  YYY = Firmware Version

VRCNX-A / VSRC-A Firmware

- **Firmware Upgrade (Flash) File** = "image_rXXX_aYYYG_ap2.SmsUpd"

  XXX = Vanderbilt Root File System version of the embedded Linux operating system.
  YYY = Firmware Version
- **Controller Diagnostics Display** = "SMS-A rootfs vX.XX"

  X.XX = Vanderbilt Root File System version of the embedded Linux operating system.
- **CIM Firmware Display** = "YYY"

  YYY = Firmware Version

SRCNX (Legacy) Firmware

- **Firmware Upgrade (Flash) File** = "rcnxXXX.u27"

  XXX = Firmware Version
- **CIM Firmware Display** = "XXX"

  XXX = Firmware Version

SRINX (Legacy)

- **Firmware Upgrade (Flash) File** = "FSMSA_XX.HEX"

  XX = Firmware Version

VRINX

- **Firmware Upgrade (Flash) File** = "SRINX_G_VXXA-FL.s19"

  XX = Firmware Version

VRI-1

- **Firmware Upgrade (Flash) File** = "vri1_appl_X_XX_XX.aax"

  X_XX_XX = X.XX.XX Firmware Version

VRI-1S3

- **Firmware Upgrade (Flash) File** = "vri1s3_appl_X_XX_XX_enc.aax"

  X_XX_XX = X.XX.XX Firmware Version

VRI-2

- **Firmware Upgrade (Flash) File** = "vri2_appl_X_XX_XX.aax"

  X_XX_XX = X.XX.XX Firmware Version

VRI-2S3

- **Firmware Upgrade (Flash) File** = "vri2s3_appl_X_XX_XX_enc.aax"

X_XX_XX = X.XX.XX Firmware Version

VI-16IN

- **Firmware Upgrade (Flash) File** = "vi16in_appl_X_XX_XX.aax"

  X_XX_XX = X.XX.XX Firmware Version

VI-16INS3

- **Firmware Upgrade (Flash) File** = "vi16ins3_appl_X_XX_XX_enc.aax"

  X_XX_XX = X.XX.XX Firmware Version

VI-16O

- **Firmware Upgrade (Flash) File** = "vi16o_appl_X_XX_XX.aax"

  X_XX_XX = X.XX.XX Firmware Version

VI-16OS3

- **Firmware Upgrade (Flash) File** = "vi16os3_appl_X_XX_XX_enc.aax"

  X_XX_XX = X.XX.XX Firmware Version

VMRC-1

- **Firmware Upgrade (Flash) File** = "vmrc-1_X_XX_XX_XXXX.crc"

  X_XX_XX_XXXX = X.XX.XX.XXXX Firmware Version

VMRC-2

- **Firmware Upgrade (Flash) File** = "vmrc-2_X_XX_XX_XXXX.crc"

  X_XX_XX_XXXX = X.XX.XX.XXXX Firmware Version

VMRC-1L

- **Firmware Upgrade (Flash) File** = "vmrc-1l_X_XX_XX_XXXX_fs_X_XX.crc"

  X_XX_XX_XXXX = X.XX.XX.XXXX Firmware Version

  fs_X_XX = File System Version

VMRC-2L

- **Firmware Upgrade (Flash) File** = "vmrc-2l_X_XX_XX_XXXX_fs_X_XX.crc"

  X_XX_XX_XXXX = X.XX.XX.XXXX Firmware Version

  fs_X_XX = File System Version

VMRC-4

- **Firmware Upgrade (Flash) File** = "vmrc-4_X_XX_XX_XXXX_fs_X_XX.crc"

  X_XX_XX_XXXX = X.XX.XX.XXXX Firmware Version

  fs_X_XX = File System Version

Operation Testing and Maintenance

Operation Testing

Once the SMS system components are installed, log into the SMS 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; the SMS system components are self-supporting.

Preface

The Vanderbilt Security Management System (**SMS**) is manufactured with high quality control standards. This manual describes the installation and wiring procedures for the online **Vanderbilt SMS** hardware.

Who should use this book

This hardware manual provides guidelines for configuring and customizing **Vanderbilt SMS** based on your unique company needs. This guide is intended to be read by installation engineers and service personnel only. It is not intended for end users of the system.

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.

Vanderbilt SMS Technical Support

If you encounter any problems while installing or operating the Vanderbilt SMS, please contact our technical support team for assistance.

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

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

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

Hours of Technical Support

Our standard technical support hours are from 8:00 a.m to 6:00 p.m. Eastern Standard Time, Monday through Friday, excluding Vanderbilt Industries observed holidays.

Before Installation

This section provides information on what should be considered before installing **Vanderbilt SMS** hardware.

Requirements

- Check to see that you have all the equipment necessary for the installation. Make sure you have all the necessary tools to properly install the equipment such as screwdrivers, wire cutters and digital meter, etc.
- All field wiring must comply with NFPA 70 (NEC) and local wiring codes. The use of unshielded or ungrounded cable will may cause problems. Make sure the correct wire type and gauges are being used for the proper wire lengths (refer to the Recommended Wire Chart).
- 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.
- Ground all wires where necessary.
- A licensed electrician will need to supply 120VAC for the Vanderbilt SMS.

Electrical wiring considerations

- All field wiring must comply with NFPA 70 (NEC) and local wiring codes.
- The use of unshielded or ungrounded cable will may cause problems. Ground shields must be grounded only at one end. If you connect the shields at both ends you will create a ground loop which will introduce more noise into the system.
- Before you install the system, verify that the correct power supplies are available.
- Remember to turn off all power before you connect any equipment.
- Always use the recommended wire type and gauge for all your connections (refer to Recommended Wire Chart).

Warning: To reduce risk of fire, all fuses should be replaced with the same type and rating as the original supplied with the **Vanderbilt** products.

- All back-up batteries should be replaced with the same type and ratings as the original supplied with the Vanderbilt products.
- A licensed electrician will need to supply 120VAC where necessary.

Before powering system

- Mount and connect all readers in accordance with manufacture’s specifications.
- Mount and connect all door contacts in accordance with manufacture’s specifications.
- Mount and connect all exit requests and annunciators in accordance with manufacture’s specifications.
- Mount and connect all peripheral equipment in accordance with manufacture’s specifications.
- Mount and connect all lock devices in accordance with manufacture’s specifications.
- Make all Vanderbilt controller channel connections for additional VRINXs, VIONX-8s and other SMS supported access control devices.

For Legacy Devices

- Connect dial-up modem (SMODNX) and/or IP addressable module (SIPNX-100).
- Connect any memory expansion modules (SMEMNX-3 or SMEMNX-7)
- Make all SRCNX channel connections for additional SRCNX, VRINX/SRINX, VIONX-8, SIONX-24, and other SMS supported access control devices.

Environmental conditions

- **SMS** hardware must be installed in a clean and a dust free environment.
- Ambient temperature - 32º F to 120º F (0º C to 49º C)
- Relative Humidity - 10% to 85%
- All head end equipment should be mounted in a secure area.

Recommended wire chart

The chart below indicates recommended wire distances and wire gauges for your **SMS** hardware connections.

Connection	Maximum Distance (ft)	Cable Recommendation
SRCNX (Legacy) Reader Controller to PC/ CIM via RS-232 protocol	50	22 AWG/3 Cond., Strd.,Shld
SRCNX Reader Controller to Contact Inputs	2,000	22 AWG/2 Cond., Strd., Twst., Shld
SRCNX Reader Controller Data connection to another SRCNX, VRINX, VIONX-8, SIONX-24, PIM-485, or Schlage VIP Locks via RS-485 protocol	4,000	18 AWG/2 Cond., Strd., Twst., Shld
VRCNX-R/M/A Reader Controller Data connection to a VRINX, VIONX-8, SIONX-24, PIM-485, VRI-1, VRI-2, VI-16IN, VI-16O, Aperio AH-30 Hub or Schlage VIP Locks via RS-485 protocol	4,000	18 AWG/2 Cond., Strd., Twst., Shld
SRCNX Reader Controller Power connection to another SRCNX, VRINX, VIONX-8, SIONX-24 PIM-485, or Schlage VIP Locks. (Over 500' should be powered locally)	250 500	22 AWG/2 Cond., Strd., Shld 18 AWG/2 Cond., Strd., Shld
VRCNX-R/M/A Reader Controller Power connection to a VRINX, VIONX-8, SIONX-24 PIM-485, VRI-1, VRI-2, VI-16In, VI-16O, Aperio AH-30 Hub or Schlage VIP Locks. (Over 500' should be powered locally)	250 500	22 AWG/2 Cond., Strd., Shld 18 AWG/2 Cond., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Magnetic Stripe read head	500	18 AWG/5 Cond., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Wiegand read head	500	22 AWG/5 Cond., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Proximity read head	500	18 AWG/5 Cond., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Bar Code read head	20	22 AWG/5 Cond., Strd., Shld
VRINX Reader Interface to Barium Ferrite read head	500	22 AWG/5 Cond., Twst., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Contact Inputs (*supervised)*	1,000	22 AWG/2 Cond., Twst., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Contact Inputs (*unsupervised)*	2,000	22 AWG/2 Cond., Twst., Strd., Shld
VRINX, VRI-1 or VRI-2 Reader Interface to Exit Button	2,000	22 AWG/2 Cond., Twst., Strd., Shld

Abbreviations: Cond. = Conductor; Strd.=Stranded; Shld.=Shielded; Twst. - Twisted

System Requirements

Minimum System Requirements

Single User / Client Workstation

- Processor: Intel Core i5
- Memory: 8 Gb Ram
- Disk Space: 120 Gb
- USB Port for SMS Distribution Media
- 10/100/1000 Base-T network card (NIC) - *must be active for SMS licensing*

SMS does NOT support hosting a CIM or the SP on a multi-homed system (more than one active NIC).

CIM – SP – Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

- Mouse, Keyboard & Monitor
- Operating System:
  - 64-bit Windows 8 Professional (except Home Edition)
  - 64-bit Windows 8.1 Professional (except Home Edition)
  - 64-bit Windows 10 Professional (except Home Edition)
  - MS OLE DB Driver for SQL v18.3 (will be installed if necessary)
  - MS ODBC Driver for SQL v17 (will be installed if necessary)
    - 32-bit System DSN for ODBC Driver (will be created)
  - .NET v4.8 (will be installed if necessary)
- Database Engine:
  - SQL Server 2012 Express SP2 or newer
  - SQL Server 2014 Express SP1 or newer
  - SQL Server 2016 Express SP1 or newer
  - SQL Server 2017 Express
  - SQL Server 2019 Express CU10 or newer

SMS does NOT support installation in a SQL cluster environment.

The SMS Install Media Includes 64-bit SQL 2014 Express SP2.

SQL Server Express installation will be to a Named Instance called “SMS”.

Multiuser Server

- Processor: Intel Core i7 or Xeon
- Memory: 8 Gb Ram
- Disk Space: 500 Gb
- USB Port for SMS Distribution Media
- 10/100/1000 Base-T network card (NIC) - *must be active for SMS licensing*

SMS does NOT support hosting a CIM or the SP on a multi-homed system (more than one active NIC).

CIM – SP – Controller communications may be unpredictable on multi-homed systems.

If NIC redundancy is required. Vanderbilt recommends teaming multiple NICs in the same system.

- Mouse, Keyboard & Monitor
- Operating System:
  - 64-bit Windows 8 Professional (except Home Edition)
  - 64-bit Windows 8.1 Professional (except Home Edition)
  - 64-bit Windows 10 Professional (except Home Edition)
  - 64-bit Windows 2012 Essentials, Standard or Datacenter
  - 64-bit Windows 2012 R2 Essentials, Standard or Datacenter
  - 64-bit Windows 2016 Essentials, Standard or Datacenter
  - 64-bit Windows 2019 Essentials, Standard or Datacenter
  - MS OLE DB Driver for SQL v18.3 (will be installed if necessary)
    - MS ODBC Driver for SQL v17 (will be installed if necessary)
  - 32-bit System DSN for ODBC Driver (will be created)
  - .NET v4.8 (will be installed if necessary)
- Database Engine:
  - SQL Server 2012 Standard or Enterprise SP2 or newer
  - SQL Server 2014 Standard or Enterprise SP1 or newer
  - SQL Server 2016 Standard or Enterprise SP1 or newer
  - SQL Server 2017 Standard or Enterprise
  - SQL Server 2019 Standard or Enterprise

SMS does NOT support installation in a SQL cluster environment.

ASSA ABLOY IP-Enabled WiFi or PoE Locks Support

- ASSA ABLOY Door Service Router (DSR) host meeting ASSA ABLOY current minimum specs
  - Up to 128 Locks: 2 CPU Cores; 4 Gb RAM; 20 Gb HD
    - 64-bit Windows 7, Windows 10, Windows Server 2008 R2, 2012, 2016 or 2019
  - Up to 1,024 Locks: 4 CPU Cores; 8 Gb RAM; 20 Gb HD
    - 64-bit Windows Server 2008 R2, 2012, 2016 or 2019
  - Up to 2,048 Locks: 8 CPU Cores; 16 Gb RAM; 20 Gb HD
    - 64-bit Windows Server 2008 R2, 2012, 2016 or 2019

  (SMS is certified for a maximum of 750 locks per DSR)
- ASSA ABLOY DSR v8.0.15 installed ***on a stand-alone host from SMS***

Optional SMS Web / Guest Pass Web Registration Support

- Multiuser Server Processor / Memory Specifications
- SMS Enterprise
- IIS Server v7.5 or newer ***on a stand-alone host from SMS***
- .NET Framework 2.0
- .NET Framework 4.0 / 4.8
- Installation assistance available via paid Vanderbilt Technical Support
- *SMS Web v7.0.0 release expected approximately 2-months after SMS v7.0.0 release*
- *DNS Reverse Lookup must be enabled across network to utilize SMS Web Portrait Monitor*

Virtual Server Support

- VMware ESX v4.1 through ESX v6.7
- Microsoft Hyper-V on Windows Server 2012 R2 or newer
- Guests Running an SMS Supported Operating System
- Guests Meeting the same Minimum Requirements defined above

The SMS license binds to the SP host system hardware properties.

The SP host system virtual guest must be configured for static NIC and hard drive properties.

SMS does NOT support vMotion or Live Migration for the SP host virtual system.

SMS does NOT support installation in a Citrix or any terminal server environment.

CHAPTER 1

Discovery and Configuration Utility

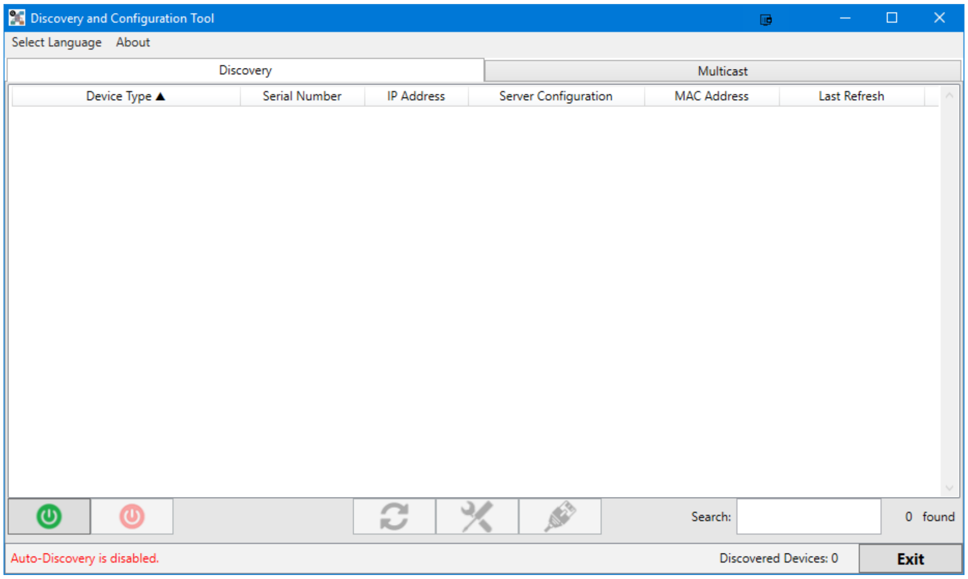
The multilingual Vanderbilt Discovery and Configuration Utility (DCT) is a separate application that, once installed, provides an alternate method for configuring the Network properties of the Vanderbilt VSRC, VSRC-M, VSRC-A, VRCNX-R, VRCNX-M and VRCNX-A controllers than the methods described in the specific controller sections that follow.

1 Run the DCT.exe program

- Direct Connection - the controller may be connected to the network port on the system
- Network Connection - the controller may be connected to the same network subnet as the system

> The DCT uses multicast to locate compatible Vanderbilt controllers and must be run from a system on the same subnet as the controllers requiring configuration and no routers can be located on the network between the system running the DCT and the controllers to configure.

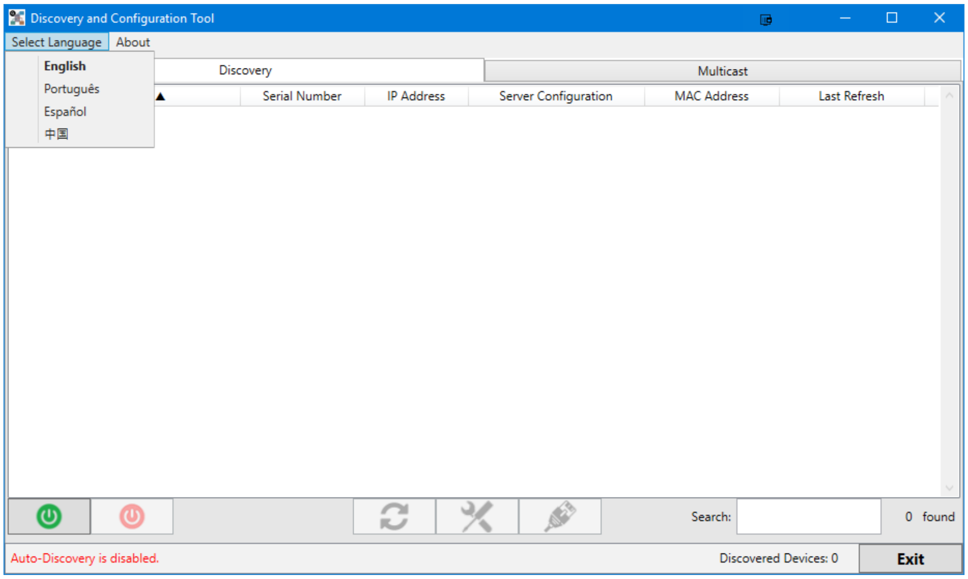
2 The DCT will open in the disabled state and the default language is English:



Auto-Discovery is disabled.

3 Click on "Select Language" to change the display language if desired. The following options are available:

- English
- Portuguese
- Spanish
- Simplified Chinese



0 found

Auto-Discovery is disabled.

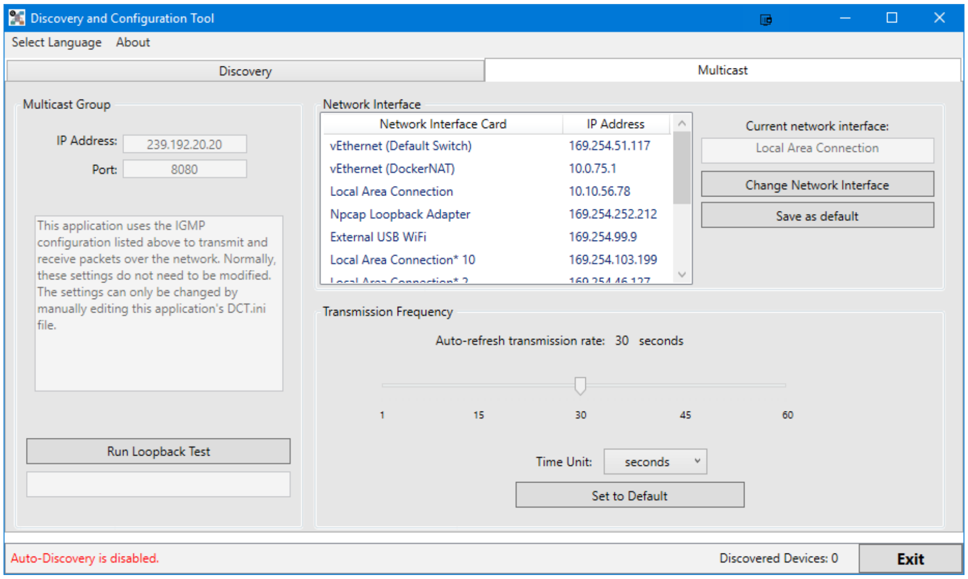
Discovered Devices: 0

4 Select the **Multicast** tab.

If the system has more than one network card (NIC) installed, you may need to select the appropriate network card attached either directly to the controller to configure or connected to the network segment on which the controllers are connected.

---

1. Highlight the NIC under the Network Interface list as desired.
2. Click **Change Network Interface** to activate this NIC for DCT operations.
3. *Optionally* click **Save as default** to make this NIC the default for future DCT sessions on this system.



IP Address: 239.192.20.20

Port: 8080

This application uses the IGMP configuration listed above to transmit and receive packets over the network. Normally, these settings do not need to be modified. The settings can only be changed by manually editing this application's DCT.ini file.

Network Interface Card	IP Address
vEthernet (Default Switch)	169.254.51.117
vEthernet (DockerNAT)	10.0.75.1
Local Area Connection	10.10.56.78
Npcap Loopback Adapter	169.254.252.212
External USB WiFi	169.254.99.9
Local Area Connection* 10	169.254.103.199
Local Area Connection* 2	169.254.46.127

Current network interface: Local Area Connection

Auto-refresh transmission rate: 30 seconds

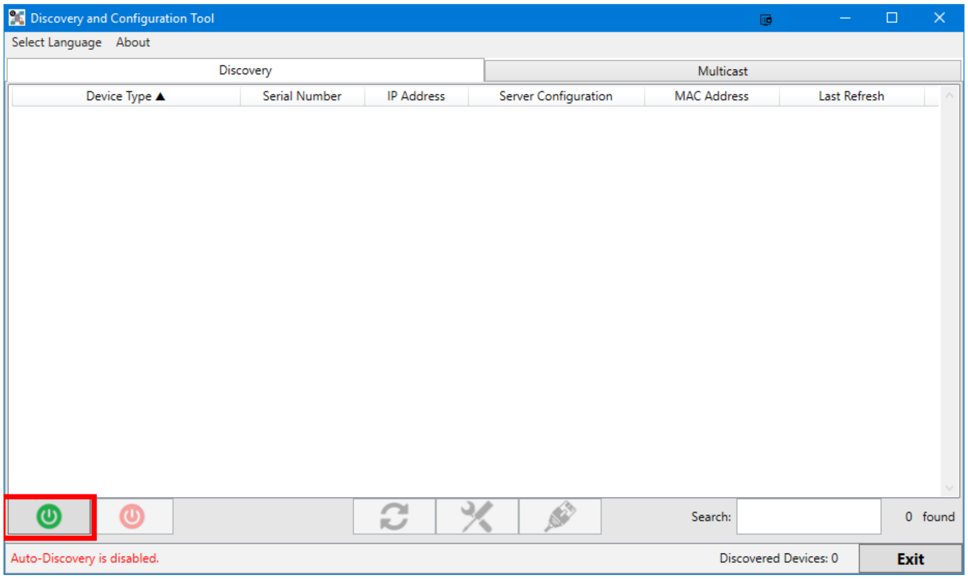
Time Unit: seconds

Auto-Discovery is disabled.

Discovered Devices: 0

4. Click on the **Discovery** tab once Multicast settings have been set.

5 Click ON to begin a search for VSRC, VSRC-M, VSRC-A, VRCNX-R, VRCNX-M and VRCNX-A controllers attached to the selected NIC / network segment.



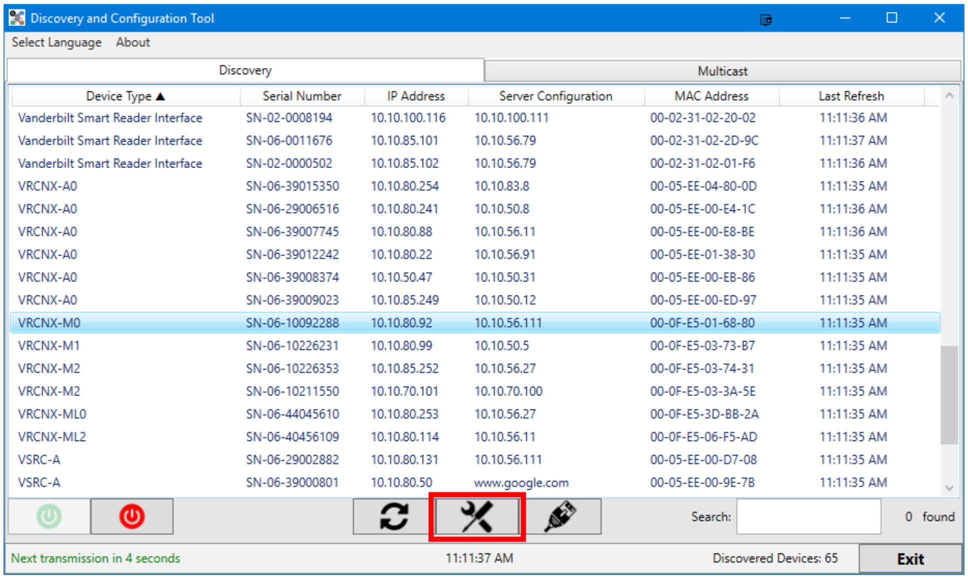
Auto-Discovery is disabled.

Discovered Devices: 0

6 The DCT **Discovery** tab will be populated with controllers responding to the multicast on the selected NIC / network segment.

Controllers with Auto Discovery Disabled via jumper / switch will NOT Respond and CANNOT be Configured via the DCT.

7 Select desired controller to configure and click **Device Configuration** (*VRCNX-M0 in the example below*).



Device Type ▲	Serial Number	IP Address	Server Configuration	MAC Address	Last Refresh
Vanderbilt Smart Reader Interface	SN-02-0008194	10.10.100.116	10.10.100.111	00-02-31-02-20-02	11:11:36 AM
Vanderbilt Smart Reader Interface	SN-06-0011676	10.10.85.101	10.10.56.79	00-02-31-02-2D-9C	11:11:37 AM
Vanderbilt Smart Reader Interface	SN-02-0000502	10.10.85.102	10.10.56.79	00-02-31-02-01-F6	11:11:36 AM
VRCNX-A0	SN-06-39015350	10.10.80.254	10.10.83.8	00-05-EE-04-80-0D	11:11:35 AM
VRCNX-A0	SN-06-29006516	10.10.80.241	10.10.50.8	00-05-EE-00-E4-1C	11:11:36 AM
VRCNX-A0	SN-06-39007745	10.10.80.88	10.10.56.11	00-05-EE-00-E8-BE	11:11:36 AM
VRCNX-A0	SN-06-39012242	10.10.80.22	10.10.56.91	00-05-EE-01-38-30	11:11:35 AM
VRCNX-A0	SN-06-39008374	10.10.50.47	10.10.50.31	00-05-EE-00-EB-86	11:11:35 AM
VRCNX-A0	SN-06-39009023	10.10.85.249	10.10.50.12	00-05-EE-00-ED-97	11:11:35 AM
VRCNX-M0	SN-06-10092288	10.10.80.92	10.10.56.111	00-0F-E5-01-68-80	11:11:35 AM
VRCNX-M1	SN-06-10226231	10.10.80.99	10.10.50.5	00-0F-E5-03-73-B7	11:11:35 AM
VRCNX-M2	SN-06-10226353	10.10.85.252	10.10.56.27	00-0F-E5-03-74-31	11:11:35 AM
VRCNX-M2	SN-06-10211550	10.10.70.101	10.10.70.100	00-0F-E5-03-3A-5E	11:11:35 AM
VRCNX-ML0	SN-06-44045610	10.10.80.253	10.10.56.27	00-0F-E5-3D-BB-2A	11:11:35 AM
VRCNX-ML2	SN-06-40456109	10.10.80.114	10.10.56.11	00-0F-E5-06-F5-AD	11:11:35 AM
VSRC-A	SN-06-29002882	10.10.80.131	10.10.56.111	00-05-EE-00-D7-08	11:11:35 AM
VSRC-A	SN-06-39000801	10.10.80.50	www.google.com	00-05-EE-00-9E-7B	11:11:35 AM

Next transmission in 4 seconds

11:11:37 AM

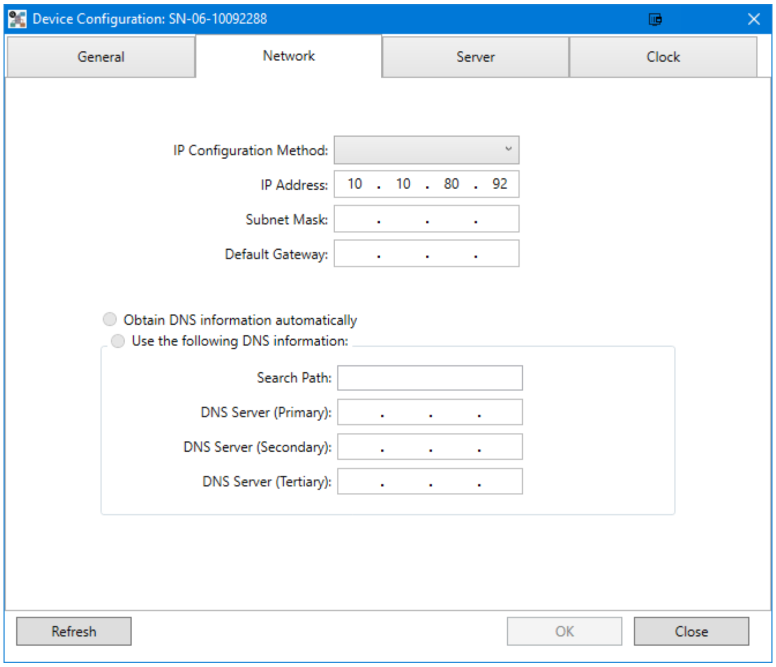
Discovered Devices: 65

8 Configure the controller as required for SMS operation.

1. Select the **Network** tab and set the following options as desired:

Consult with IT regarding the correct network settings for SMS controllers

- IP Configuration Method
- IP Address
- Subnet Mask
- Default Gateway
- DNS automatic (DHCP) or Manual configuration
- DNS Search Path
- DNS Server (Primary)
- DNS Server (Secondary)
- DNS Server (Tertiary)



Device Configuration: SN-06-10092288

IP Configuration Method:

IP Address: 10 . 10 . 80 . 92

Subnet Mask: . . .

Default Gateway: . . .

○ Obtain DNS information automatically

○ Use the following DNS information:

Search Path:

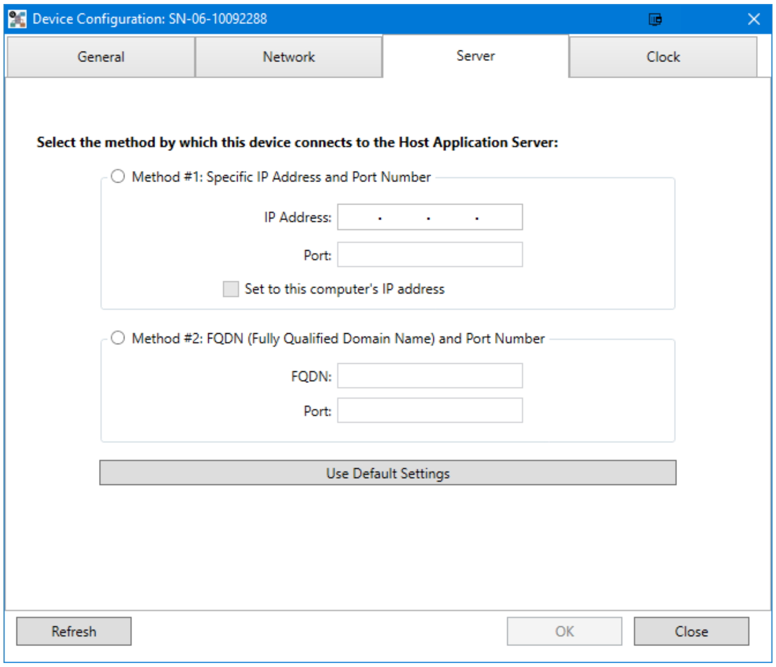
DNS Server (Primary): . . .

DNS Server (Secondary): . . .

DNS Server (Tertiary): . . .

2. Select the **Server** tab and set the following options for connection to the Host Application Server (SMS CIM) as desired:

   - Method #1: Specific IP Address and Port Number
     - Enter the SMS CIM IP Address
     - Enter the SMS CIM Port Number. The CIM normally communicates to the controllers on Port 3001 unless changed by IT requirements.
   - Method #2: FQDN (Fully Qualified Domain Name) and Port Number
     - Enter the FQDN of the SMS CIM.
     - Enter the SMS CIM Port Number. The CIM normally communicates to the controllers on Port 3001 unless changed by IT requirements.



Select the method by which this device connects to the Host Application Server:

○ Method #1: Specific IP Address and Port Number

IP Address: . . .

Port:

□ Set to this computer's IP address

○ Method #2: FQDN (Fully Qualified Domain Name) and Port Number

FQDN:

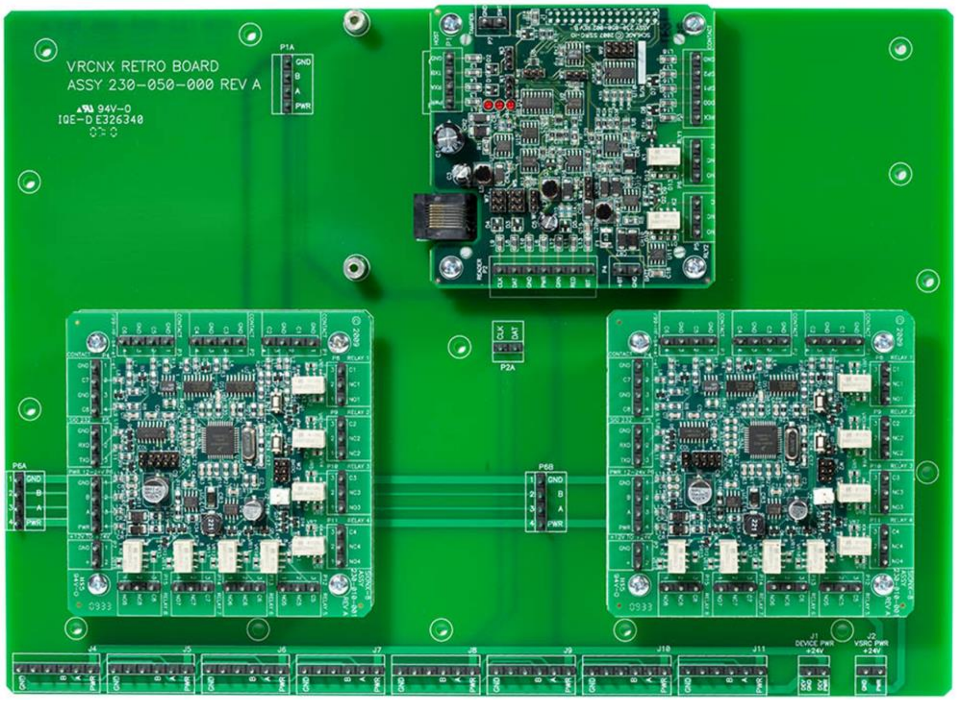
Port:

   - Click **Close** to complete controller configuration.

9 Select and configure additional controllers as desired following the steps above.

CHAPTER 2

VRCNX-R



Reader Controller

Overview

The VRCNX-R Reader Controller is an intelligent device that can be paired with the **Vanderbilt Security Management System** (SMS) Enterprise software package. The VRCNX-R can have up to two VIONX-8 devices attached to it if contacts and/or relays are required; these onboard VIONX-8 devices do not contribute to the total number of devices that can be connected to the VRCNX-R. The VRCNX-R is an independently programmable device which is capable of making decisions and storing history at the local level if communication is lost.

The VRCNX-R has three different software defined types depending on the number of contacts and relays associated with the board: VRCNX-R0, VRCNX-R1 and VRCNX-R2.

- VRCNX-R0: No contacts or relays
- VRCNX-R1: One VIONX-8 is onboard providing up to 8 contacts and 8 relays
- VRCNX-R2: Two VIONX-8s are onboard providing up to 16 contacts and 16 relays

Note: In this chapter VRCNX-R refers to all three model types. The specific model will be referenced only when the model type affects set up or configuration. If either a VRCNX-R1 or a VRCNX-R2 will work in the configuration, then it will be referred to as VRCNX-R1/R2.

Highlights

- Communicates to the server (installed with Vanderbilt SMS software) via network protocol at 10/100 Base-T
- Powered locally by a 24VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power
- Flashable firmware
- Capable of running in degraded mode, allowing local decision making if communication fails between the VRCNX-R and the network
- Can be used with a multitude of **Vanderbilt SMS** communication devices including the Vanderbilt reader interface modules (VRINX, VRI-1 and VRI-2) which support read head technologies including Proximity, Magnetic Stripe, Wiegand, Barium Ferrite, bar code, smart card, biometric, keypad and other SMS compatible access control devices

Features

For all VRCNX-R varieties:

- 16 device capacity (compatible devices include: VRINX, VRI-1, VRI-2, VIONX-8, VRI-16IN, VRI-16O, SIONX-24 and other SMS compatible access control devices)
- Approximately 45 Mb available for storage after Linux and Kernel applications have been loaded
- Communicates with CIM via network protocol at 10/100 Base-T
- DNS Compatible

For VRCNX-R1:

- 8 supervised or unsupervised Contact Inputs
- 8 Relay Outputs

For VRCNX-R2:

- 16 supervised or unsupervised Contact Inputs
- 16 Relay Outputs

Configuration Guidelines

- All VRCNX-R Reader Controllers have 2 communication channels (channels 2 and 3). Each channel will support 8 devices for a total of 16 devices. Only devices of the same protocol (either SMS protocol, SMS-M protocol, F-series protocol or Aperio Protocol) may be connected to an individual channel.
  - **The VRCNX-R1 and the VRCNX-R2 can only have SMS protocol devices connected to channel 3.**
- Vanderbilt devices that may be connected to a VRCNX-R: VRINX, VIONX-8, and SIONX-24 (SMS protocol); VRI-1, VRI-2, VI-16IN and VI-16O (SMS-M protocol).
- Other devices that may be connected to a VRCNX-R: Schlage wireless PIM-485, PIM-400, AD-300 and Schlage VIP Locks (with F-series protocol); Aperio AH-30 hub (Aperio Protocol) with up to 16 supported Aperio Wireless Locks (up to 8 Aperio wireless locks per AH-30 hub).
- The number after the VRCNX-RX designates how many VIONX-8 boards are attached to the VRCNX-R. The VRCNX-R0 has none, the VRCNX-R1 has one and the VRCNX-R2 has two. These VIONX-8s do not count toward the total number of devices that can be connected to the VRCNX-R.
- There is no Main/Satellite configuration for the VRCNX-R. Each VRCNX-R is a stand-alone board.

Specifications

- Board Dimensions - 9-3/4” H x 13-1/2” W x 1-1/2” D (board only)
- Power Requirements - 20VDC to 32VDC
- Power Consumption - (excluding peripheral devices) 300 mA
- Ambient Temperature - 0º to 49º C or 32º to 120º F
- Humidity - 10% to 85%

VRCNX-R Enclosure

VRCNX-R Enclosure - An enclosure with a hinged door is included for each VRCNX-R.

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: 20” x 20” x 4”

Environmental conditions

- Ambient Temperature - 0º to 49º C or 32º to 120º F
- The room must be dust free and clean
- 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.

VRCNX-R IP Configuration

The IP address of the VRCNX-R has to be configured so that it can communicate with the CIM. Configuration should occur after the VRCNX-R has been fully installed. Below are detailed instructions on how to configure the VRCNX-R with a Static IP address. DHCP configuration is possible, but not recommended.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

DNS Configuration

With firmware v2.61 VRCNX-R is now DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. For DHCP setup see the DHCP Configuration section.

Follow the steps below to configure the static IP of the VRCNX-R.

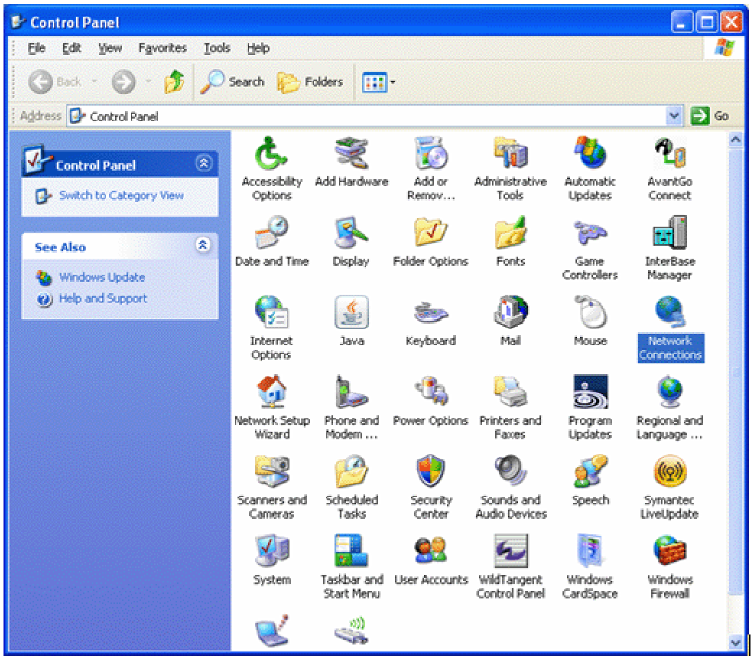
1 Connect a PC with a web browser to the VRCNX-R.

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

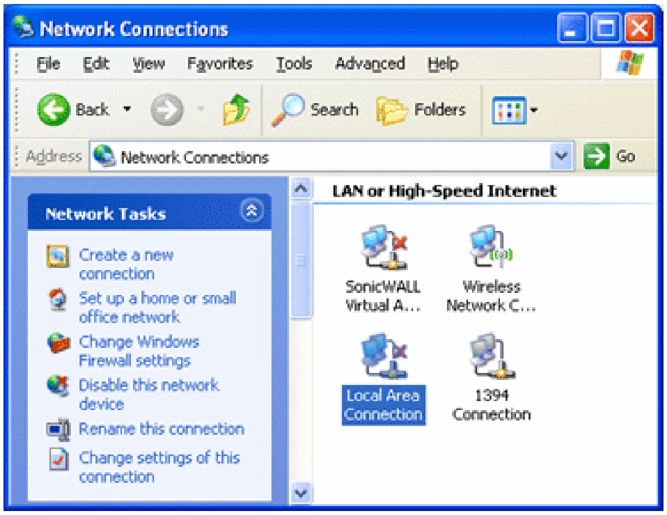
2 Configure the PC's network settings to communicate with the VRCNX-R:

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

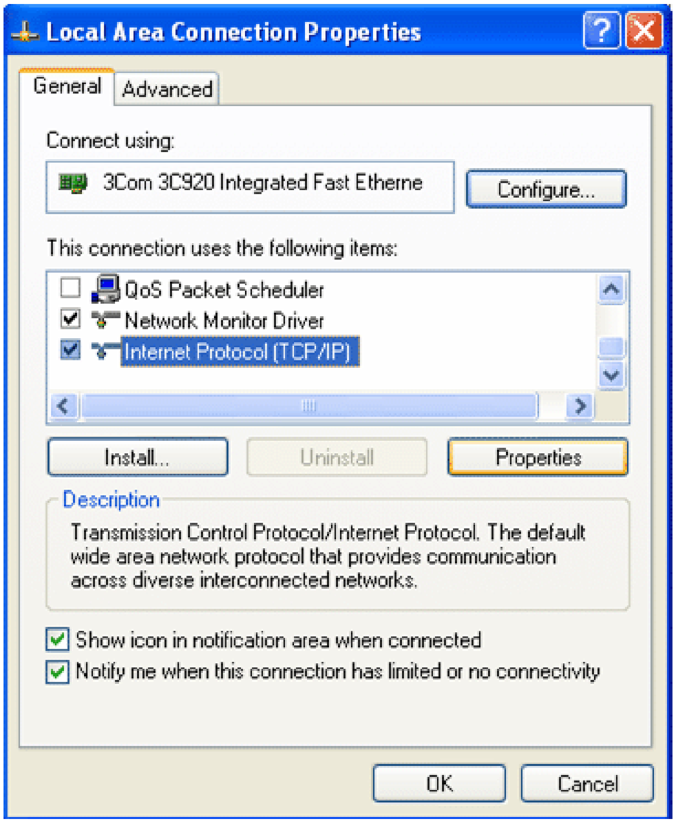
b) Click on **Control Panel**. The Control Panel window will open.



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.



Connect using:

3Com 3C920 Integrated Fast Etherne

This connection uses the following items:

□ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description

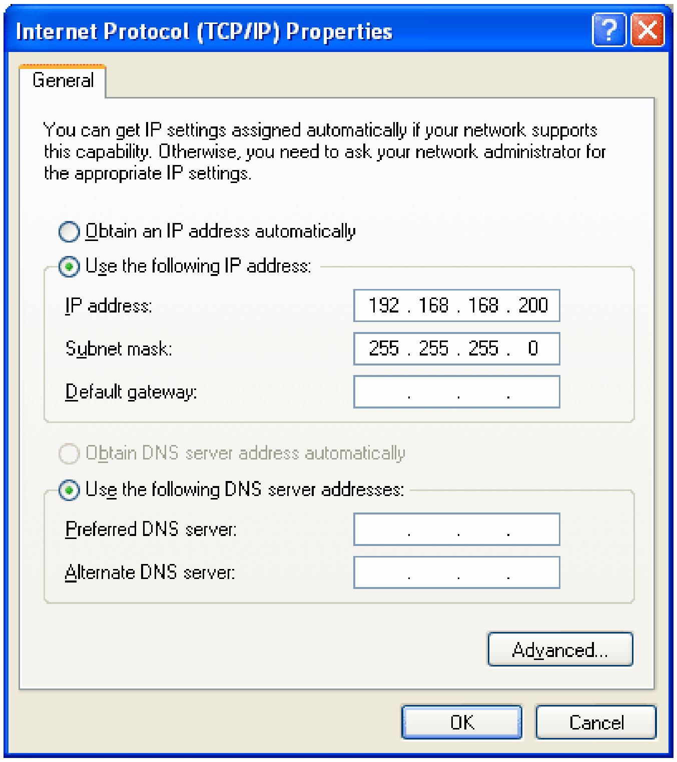
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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 VRCNX-R configuration process to return the PC to its usual settings.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 168 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

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

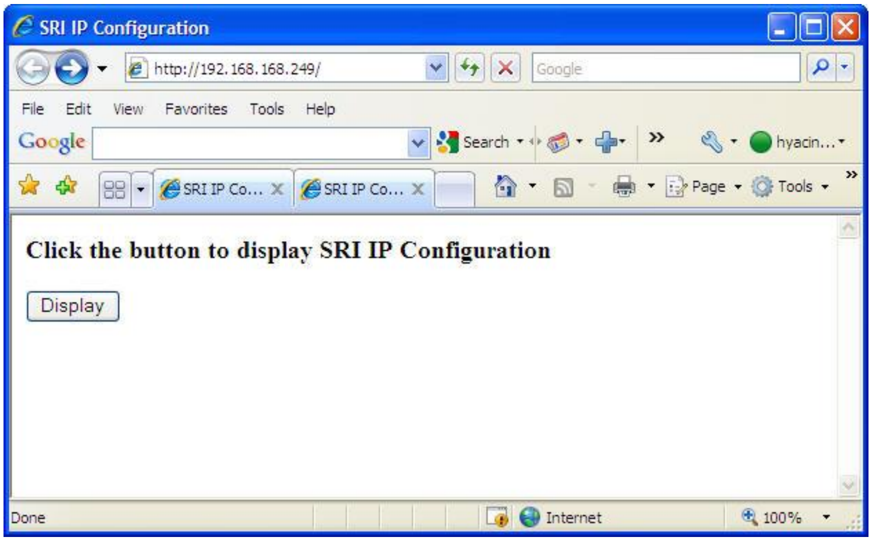
i) Enter 192.168.168.200 into the **IP address** field.

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 the default VRCNX-R IP address (Default IP address is 192.168.168.249).

3 Open a web browser.

4 Go to http://192.168.168.249 -- the **IP Configuration** window will open.

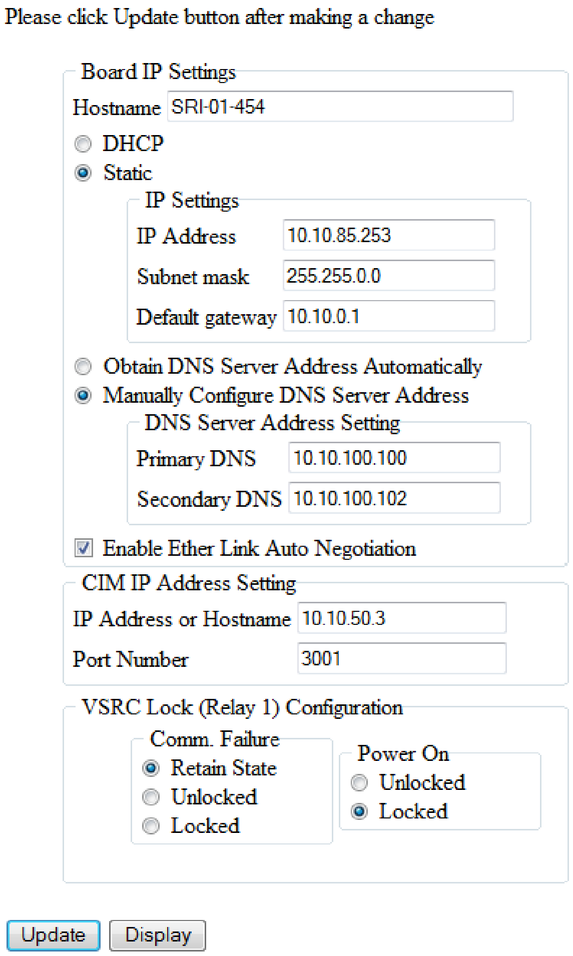


SRI IP Configuration

http://192.168.168.249/

Click the button to display SRI IP Configuration

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



Please click Update button after making a change

Board IP Settings

Hostname SRI-01-454

○ DHCP

● Static

IP Settings

IP Address 10.10.85.253

Subnet mask 255.255.0.0

Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically

● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100

Secondary DNS 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname 10.10.50.3

Port Number 3001

VSRC Lock (Relay 1) Configuration

Comm. Failure

● Retain State

○ Unlocked

○ Locked

Power On

○ Unlocked

● Locked

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 (Optional, for DNS configuration).

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 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or
- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

9 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered in this screen.

10 Click on the **Update** button. Make a note of the IP address as it will be used by SMS to communicate with the VRCNX-R.

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

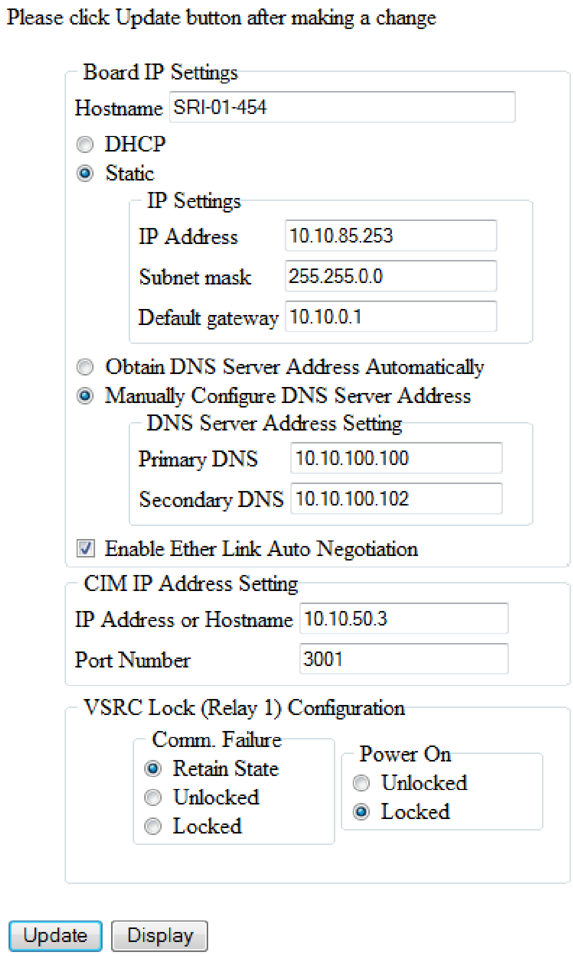
The IP address of the VRCNX-R has been set.

DHCP Configuration

Configuring the VRCNX-R to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

WARNING: If Controller IP addresses change, the system will not be aware of it until the DNS cache refreshes. Also, the CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may run incorrectly.

GUI (Graphic User Interface)



Please click Update button after making a change

Board IP Settings

Hostname SRI-01-454

○ DHCP
● Static

IP Settings

IP Address 10.10.85.253
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname 10.10.50.3
Port Number 3001

VSRC Lock (Relay 1) Configuration

Comm. Failure
● Retain State
○ Unlocked
○ Locked

Power On
○ Unlocked
● Locked

Hostname - This displays the name of the specific VRCNX-R. The name is in a standard format of SRI-02-XXX.

- SRI - Smart Reader Interface
- 02 - The designation for an VSRC/VRCNX-R
- XXX - The serial number of the specific VRCNX-R (in the above example the serial number is 454).

The Host Name is used to access and setup the VRCNX-R 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 VRCNX-R to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes there will be a loss of controller communications until the new IP address is recognized by the CIM.

Static - This setting forces the VRCNX-R to use a static IP address.

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VRCNX-R'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 VRCNX-R'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.

DNS Server Address Setting

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

Enable Ether Link Auto Negotiation - The VRCNX-R 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 VRCNX-R to automatically detect and use the communication speed of the switch it is connected to.

Note: This option is not available on older model VRCNX-Rs. If this option does not show in the GUI then the VRCNX-R will only communicate at 10Base-T.

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS the Fully Qualified Domain Name (FQDN) of the CIM should be entered here
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definitions matches the port entered on this screen.

VSRC Lock (Relay 1) Configuration – Not used with VRCNX-R. Only used when configuring VSRC.

VRCNX-R Device Configuration

The VRCNX-R has 2 channels for devices and can support up to 16 devices (8 devices of the same protocol per channel). Each channel on the VRCNX-R can only support devices of the same protocol.

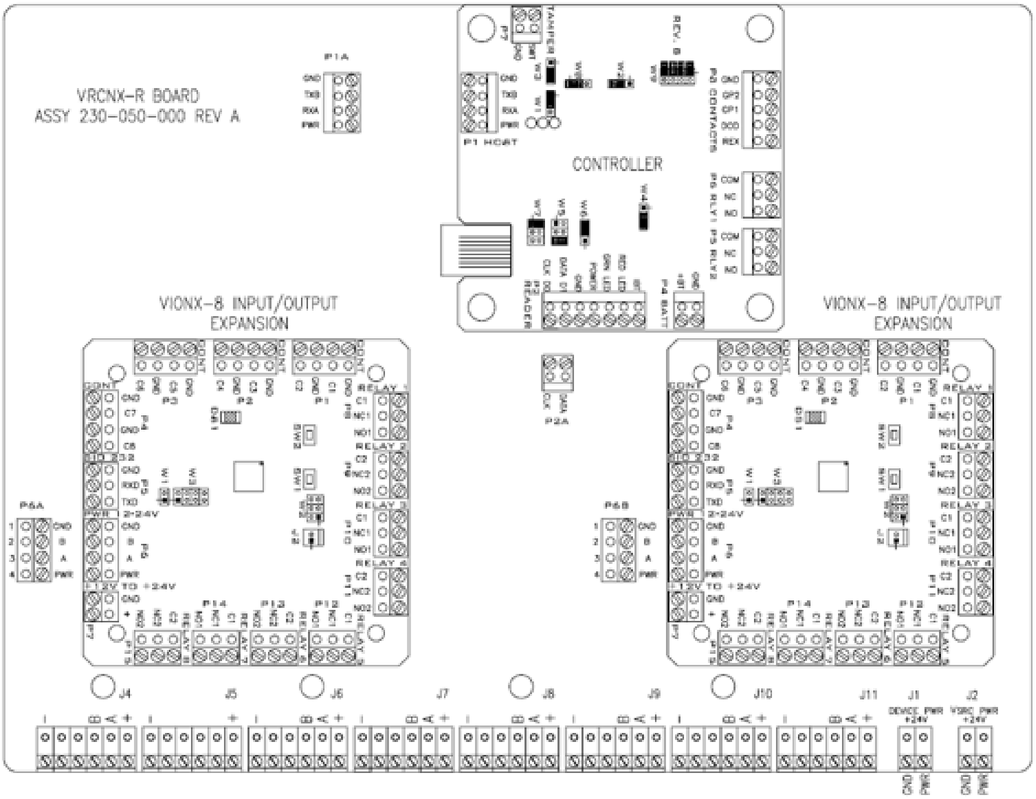
There are four types of protocol being used by devices:

- **SMS Protocol** - VRINX, VIONX-8, HC11 Reader Interface, SRINX (Legacy) and SIONX-24 (Legacy)
- **SMS-M Protocol** – VRI-1, VRI-2, VI-16IN and VI-16O
- **Aperio Protocol** - Assa Abloy Aperio AH30 RS-485 hub; IN100, K100, KS100, M100 and PR100 wireless locks
- **F-Series Protocol** - Schlage AD-Series Locks, Schlage VIP with F-protocol (old VIP Protocol not supported) and Schlage WAPM

When connecting devices to the VRCNX-R it is important to make sure that only devices of the same protocol are put on the same channel.

- Channel 2 on the VRCNX-R (J4 through J7) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-R0 (J8 through J11) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-R1 (J8 through J11) can be used to connect SMS protocol devices only.
- Channel 3 on the VRCNX-R2 (J8 through J11) can be used to connect SMS protocol devices only.

VRCNX-R Pin Layout



The VRCNX-R is made of up of a Controller Board and the VRCNX-R back-board. In addition, the VRCNX-R1 has one VIONX-8 board and an VRCNX-R2 has two VIONX-8 boards. Each of these components has a different pin layout which is described below.

VRCNX-R Pin Functions

J1 - Power source wiring for connected devices. This is where the power supply is connected to the VRCNX-R to supply power to devices connected to J4 through J11. (This is optional as the devices can be powered locally.)

- Dev Gnd is Ground
- Dev PWR is Power

J2 - Power source wiring for on board VSRC and VIONX-8(s). This is where the power supply is connected to the VRCNX-R to supply power to the on board VSRC and VIONX-8 (if included).

- Gnd is Ground
- PWR is Power

J4 through J7 - Communication and power for channel 2 devices. Receives power from J1.

- Pin 1 is Ground
- Pin 2 is not used
- Pin 3 is not used

- Pin 4 is B
- Pin 5 is A
- Pin 6 is Power

J8 through J11 - Communication and power for channel 3 devices. Receives power from J1.

- Pin 1 is Ground
- Pin 2 is not used
- Pin 3 is not used
- Pin 4 is B
- Pin 5 is A
- Pin 6 is Power

P1A - Power source connection and data connection for channel 2 to the VSRC. This is where the onboard VSRC receives power and channel 2 communication from the VRCNX-R.

- GND connects to GND on P1 of the VSRC
- B connects to TXB on P1 of the VSRC
- A connects to RXA on P1 of the VSRC
- PWR connects to PWR on P1 of the VSRC

P2A - Data connection for channel 3 to the VSRC. This is where the onboard VSRC receives channel 3 communication from the VRCNX-R.

- CLK connects to CLK on P2 of the VSRC
- DAT connects to DAT on P2 of the VSRC

P6A - Power source and data connection to the first VIONX-8. This is where the first onboard VIONX-8 receives power and communication from the VRCNX-R.

- GND connects to GND on P6 of the VIONX-8
- B connects to B on P6 of the VIONX-8
- A connects to A on P6 of the VIONX-8
- PWR connects to PWR on P6 of the VIONX-8

P6B - Power source and data connection to the second VIONX-8. This is where the second onboard VIONX-8 receives power and communication from the VRCNX-R.

- GND connects to GND on P6 of the VIONX-8
- B connects to B on P6 of the VIONX-8
- A connects to A on P6 of the VIONX-8
- PWR connects to PWR on P6 of the VIONX-8

Controller Pin Functions

P1 - Power source connection and data connection for channel 2 to the VRCNX-R. This is where the onboard VSRC receives power and channel 2 communication from the VRCNX-R.

- GND connects to GND on P1A of the VRCNX-R
- B connects to TXB on P1A of the VRCNX-R
- A connects to RXA on P1A of the VRCNX-R
- PWR connects to PWR P1A of the VRCNX-R

P2 - Data connection for channel 3 to the VRCNX-R. This is where the onboard VSRC receives channel 3 communication from the VRCNX-R.

- CLK connects to CLK on P2A of the VRCNX-R
- DAT connects to DAT on P2A of the VRCNX-R

P7 - Tamper switch. This is where a tamper switch is connected to the VSRC (for the whole VRCNX-R).

- Pin 1 (GND) is Ground
- Pin 2 (SWT) - Normally Closed

W9 - Used to determine the type of VRCNX-R (R0, R1 or R2) and to disable network communication. .

- 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 VSRC cannot be reached via the GUI, Telnet, Ping or the Discovery and Configuration Tool.
- Pins 3 & 4 - Not used at this time.
- Pin 5 & 6 and 7 & 8 - Different jumper configurations determine what type of VRCNX-R this is (R0, R1 or R2). See the chart below for details.

VRCNX-R Type	Pins 5&6	Pins 7&8
R0	On	On
R1	Off	On
R2	On	Off

Warning: Vanderbilt recommends Jumpering W9 Pins 1 & Pin 2 together to DISABLE the onboard web server, telnet, ping, and discovery protocol after installation and configuration. Leaving them enabled could allow unauthorized access to the controller.

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: 2&3 Default W3: 1&2
- W2 - Used for RS485 termination (Reader Interface Termination). Default: 2&3
- W5/W7 - Sets communication protocol. Default W5: 3&4 Default W7 3&4
- 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 VSRC (when connected to an VRCNX-R):

- P4
- P3
- P5/P6
- W4

VIONX-8 Pin Functions

Note: There can be up to two VIONX-8 boards onboard the VRCNX-R. The below pin functions are broken up into first and second VIONX-8s for clarity.

First VIONX-8 (left side)

P6 - Power source and data connection to the VRCNX-R. This is where the onboard VIONX-8 receives power and communication from the VRCNX-R.

- GND connects to GND on P6A of the VRCNX-R
- B connects to B on P6A of the VRCNX-R
- A connects to A on P6A of the VRCNX-R
- PWR connects to PWR P6A of the VRCNX-R

P1 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 1
- Pin 3 is Ground
- Pin 4 is Contact 2

P2 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 3
- Pin 3 is Ground
- Pin 4 is Contact 4

P3 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 5
- Pin 3 is Ground
- Pin 4 is Contact 6

P4 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 7
- Pin 3 is Ground
- Pin 4 is Contact 8

P8 - Relay Output 1. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P9 - Relay Output 2. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P10 - Relay Output 3. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P11 - Relay Output 4. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P12 - Relay Output 5. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P13 - Relay Output 6. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P14 - Relay Output 7. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P15 - Relay Output 8. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

SW1 - Hardware Reset Switch. The Reset Switch clears all the memory on the VIONX-8. 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 VIONX-8 (P6 or P7) when pressing reset switches.

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

W3 - VIONX-8 Addressing. The address is preset and should not be altered.
Default is address 15 -- Jumpers on 1 & 2.

Second VIONX-8 (right side)

P6 - Power source and data connection to the VRCNX-R. This is where the onboard VIONX-8 receives power and communication from the VRCNX-R.

- GND connects to GND on P6B of the VRCNX-R
- B connects to B on P6B of the VRCNX-R
- A connects to A on P6B of the VRCNX-R
- PWR connects to PWR P6B of the VRCNX-R

P1 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 9
- Pin 3 is Ground
- Pin 4 is Contact 10

P2 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 11
- Pin 3 is Ground
- Pin 4 is Contact 12

P3 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 13
- Pin 3 is Ground
- Pin 4 is Contact 14

P4 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 15
- Pin 3 is Ground
- Pin 4 is Contact 16

P8 - Relay Output 9. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P9 - Relay Output 10. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P10 - Relay Output 11. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P11 - Relay Output 12. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P12 - Relay Output 13. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P13 - Relay Output 14. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P14 - Relay Output 15. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P15 - Relay Output 16. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

SW1 - Hardware Reset Switch. The Reset Switch clears all the memory on the VIONX-8. 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 VIONX-8 (P6 or P7) when pressing reset switches.

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

W3 - VIONX-8 Addressing. The address is preset and should not be altered.
Default is address 16 - Jumpers on: None.

Pins Not Used

P7

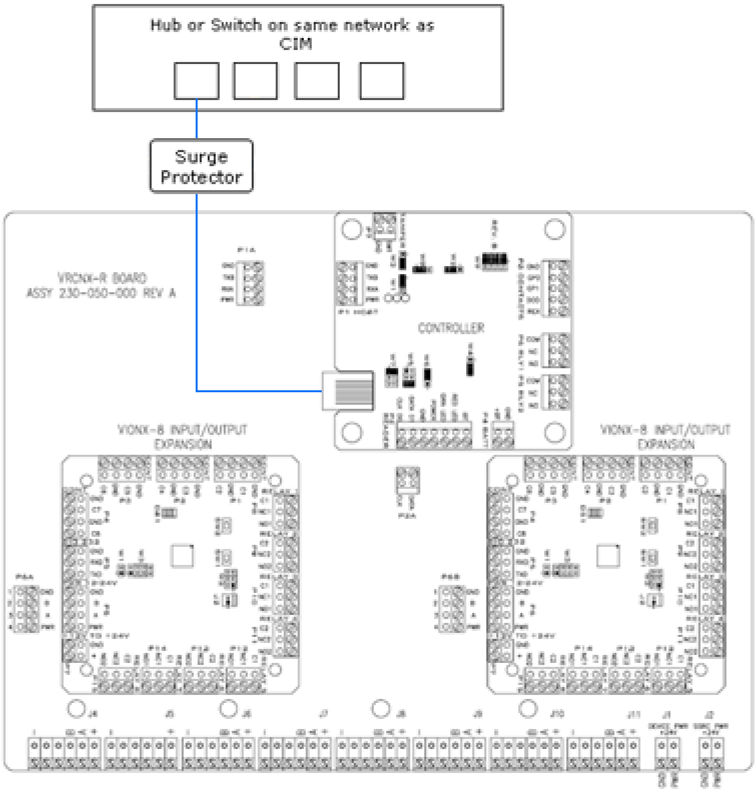
P5

W1

J2

Connecting to CIM

There is no direct connection between the VRCNX-R and the CIM. To connect, they need to be on the same network and the proper IP address of the VRCNX-R needs to be entered when setting up the VRCNX-R in SMS. In addition, a data surge protector needs to be installed between the VRCNX-R 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 J2 on the VRCNX-R.

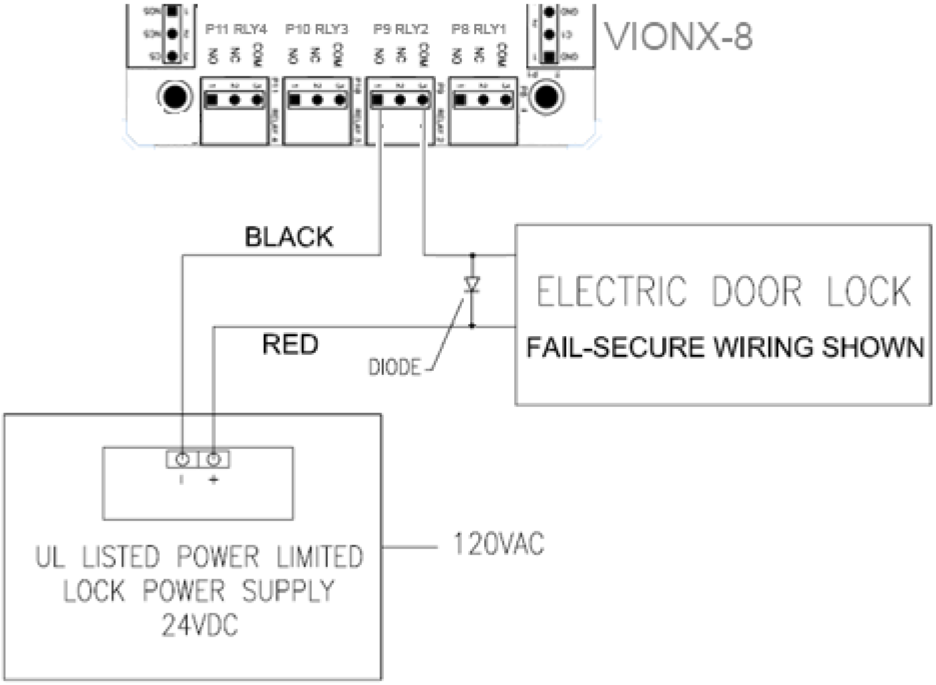

Hub or Switch on same network as CIM
Surge Protector
VRCNX-R BOARD
ASSY 230-050-000 REV A
CONTROLLER
VIONX-8 INPUT/OUTPUT EXPANSION
VIONX-8 INPUT/OUTPUT EXPANSION

Data Communication between CIM and VRCNX-R

CIM	VRCNX-R
Ethernet To Network	Ethernet to Network

Installing Diode for Lock Wiring - Relay

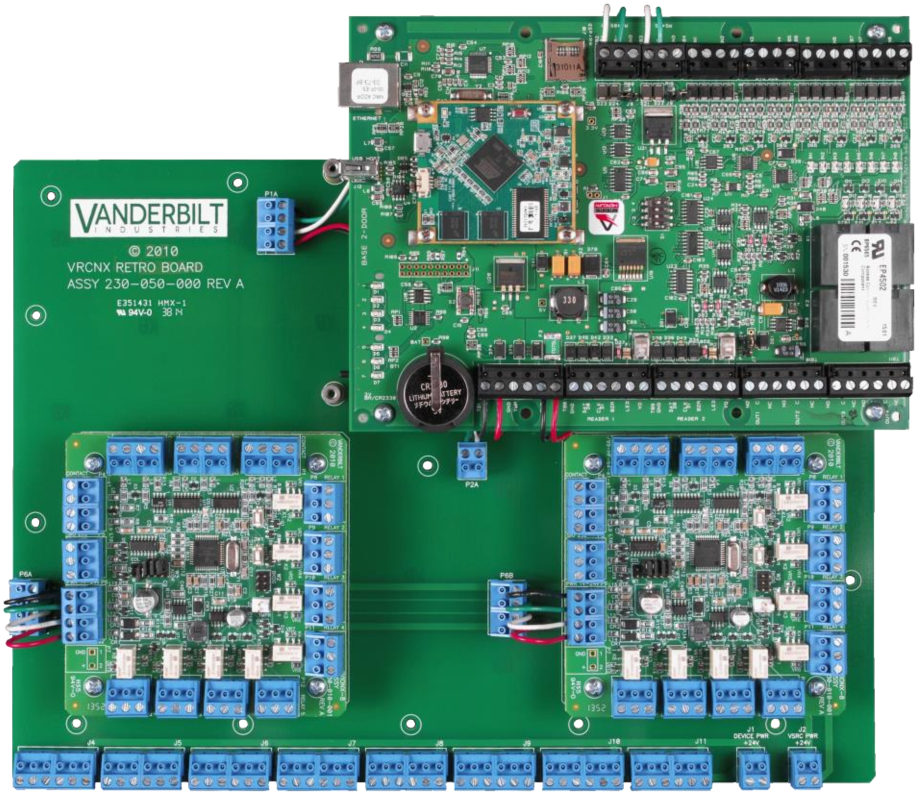
If installing an VRCNX-R1/2 a diode is supplied with the system which should be fitted across 12VDC or 24VDC and COM of the VIONX-8 to protect the relay contacts.



The lock is wired across 12VDC or 24VDC 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 Safe / Fail Secure. (Above diagram is of Fail Secure).

CHAPTER 3

VRCNX-M



Reader Controller

Overview

The VRCNX-M Reader Controller is an intelligent device based on a Mercury EP4502 controller that can be paired with v6.0.2 and newer **Vanderbilt Security Management System** (SMS) Enterprise software installations. The VRCNX-M can have up to two VIONX-8 devices attached to it if contacts and/or relays are required; these onboard VIONX-8 devices do not contribute to the total number of devices that can be connected to the VRCNX-M. Alternately, the VRCNX-M can also have 1 x VI-16IN and 1 x VI-16O I/O modules connected to provide onboard contacts and relays which do not contribute to the total number of connected devices. The VRCNX-M is an independently programmable device which is capable of making decisions and storing history at the local level (*Enhanced Offline Mode*) if communication is lost.

The VRCNX-M has four different **software** defined types depending on the contacts and relays devices associated with the board: VRCNX-M0, VRCNX-M1, VRCNX-M2 and VRCNX-M3.

- VRCNX-M0: no contacts or relays
- VRCNX-M1: one VIONX-8 mounted onboard providing up to 8 contacts and 8 relays
- VRCNX-M2: two VIONX-8s mounted onboard providing up to 16 contacts and 16 relays
- VRCNX-M3: 1 x VI-16IN and 1 x VI-16O connected to Channel 3 providing up to 16 contacts and 16 relays

Note: In this chapter VRCNX-M refers to all four model types. The specific model will be referenced only when the model type affects set up or configuration. If either a VRCNX-M1 or a VRCNX-M2 will work in the configuration, then it will be referred to as VRCNX-M1/M2.

Highlights

- Communicates to the server (installed with Vanderbilt SMS software) via network protocol at 10/100 Base-T
- Powered locally by a 12VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power
- Flashable firmware
- Capable of running in Enhanced Offline Mode, allowing local decision making if communication fails between the VRCNX-M and the network

Can be used with a multitude of **Vanderbilt SMS** communication devices including the Vanderbilt reader interface modules (VRINX, VRI-1 and VRI-2) which support read head technologies including Proximity, Magnetic Stripe, Wiegand, Barium Ferrite, bar code, smart card, biometric, keypad and other SMS compatible access control devices

Features

For all VRCNX-M varieties:

- 16 device capacity (compatible devices include: VRINX, VRI-1, VRI-2, VIONX-8, VI-16IN, VI-16O, SIONX-24 and other SMS compatible access control devices)
- Enhanced Offline Mode provides persistent copy of downloaded Access Records used for local Access decisions during loss of network connection
- Enhanced Offline Mode storage of up to 20,000 Transactions and 5,000 Alarms to nonvolatile memory (*survives power cycle*)
- Communicates with CIM via network protocol at 10/100 Base-T
- DNS Compatible

For VRCNX-M1:

- 8 supervised or unsupervised Contact Inputs
- 8 Relay Outputs

For VRCNX-M2/M3:

- 16 supervised or unsupervised Contact Inputs
- 16 Relay Outputs

Configuration Guidelines

- All VRCNX-M Reader Controllers have 2 communication channels (channels 2 and 3). Each channel will support 8 devices for a total of 16 devices. Only devices of the same protocol (either SMS protocol, SMS-M protocol, F-series protocol or Aperio Protocol) may be connected to an individual channel.
  - **The VRCNX-M1 and the VRCNX-M2 can only have SMS protocol devices connected to channel 3.**
  - **The VRCNX-M3 can only have SMS-M protocol devices connected to channel 3.**

- Vanderbilt devices that may be connected to a VRCNX-M: VRINX, VIONX-8 and SIONX-24 (SMS protocol); VI-1, VI-2, VI-16IN and VI-16O (SMS-M protocol).
- Other devices that may be connected to a VRCNX-M: Schlage wireless PIM-485, PIM-400, AD-300 and Schlage VIP Locks (with F-series protocol); Aperio AH-30 hub (Aperio Protocol) with up to 16 supported Aperio Wireless Locks (up to 8 Aperio wireless locks per AH-30 hub).
- The number after the VRCNX-RX designates I/O modulus connected to the VRCNX-M. The VRCNX-M0 has none, the VRCNX-M1 has one VIONX-8 onboard, VRCNX-M2 has two VIONX-8 onboard and the VRCNX-M3 has one VI-16IN and one VI-16O connected. These I/O modules do not count toward the total number of devices that can be connected to the VRCNX-M.
- There is no Main/Satellite configuration for the VRCNX-M. Each VRCNX-M is a stand-alone controller.

The 2 Wiegand readers mounted onboard the Mercury EP4502 controller are not currently supported.

Specifications

- Board Dimensions - 9-3/4” H x 13-1/2” W x 1-1/2” D (board only)
- Power Requirements - 12VDC to 24VDC
- Power Consumption - (excluding peripheral devices) 300 mA
- Ambient Temperature - 0º to 49º C or 32º to 120º F
- Humidity - 10% to 85%

VRCNX-M Enclosure

VRCNX-M Enclosure - An enclosure with a hinged door is included for each VRCNX-M.

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: 17” x 17” x 2-3/4"

Environmental Conditions

- Ambient Temperature - 0º to 49º C or 32º to 120º F
- The room must be dust free and clean
- 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.

VRCNX-M IP Configuration

The IP address of the VRCNX-M has to be configured so that it can communicate with the CIM. Configuration should occur after the VRCNX-M has been fully installed. Below are detailed instructions on how to configure the VRCNX-M with a Static IP address. DHCP configuration is possible, but not recommended.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

DNS Configuration

VRCNX-M controllers are DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section for DHCP setup.

Follow the steps below to configure the static IP of the VRCNX-M.

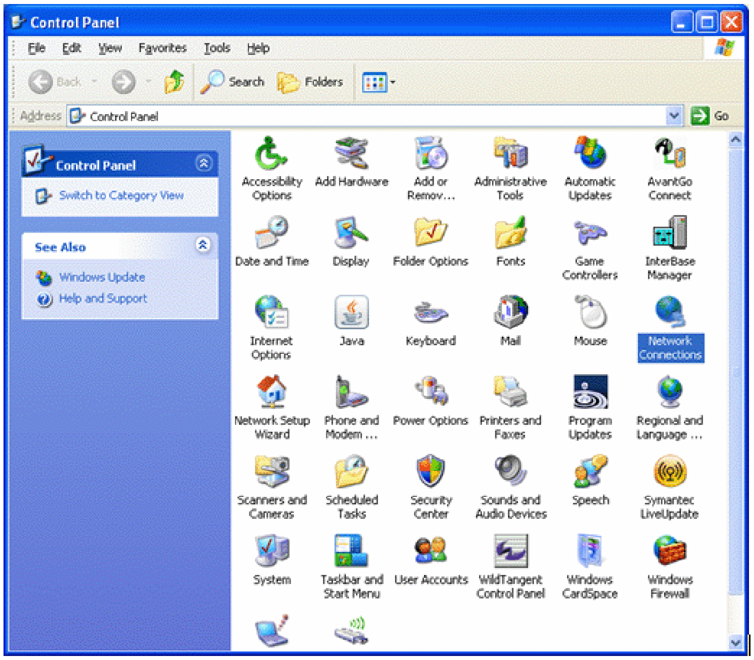
1 Connect a PC with a web browser to the VRCNX-M.

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

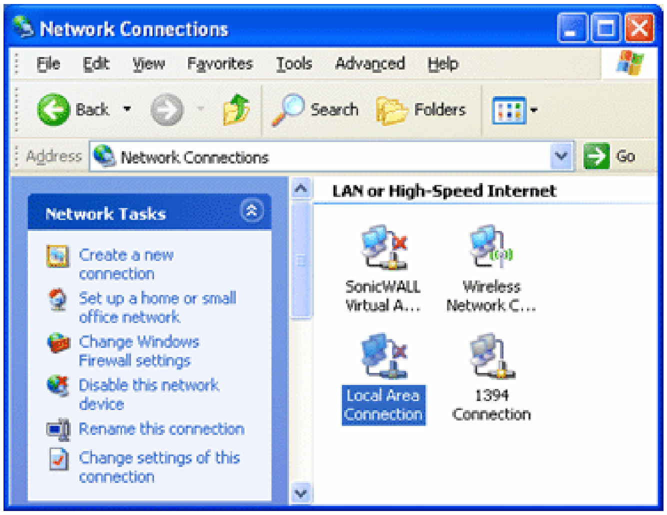
2 Configure the PC's network settings to communicate with the VRCNX-M

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

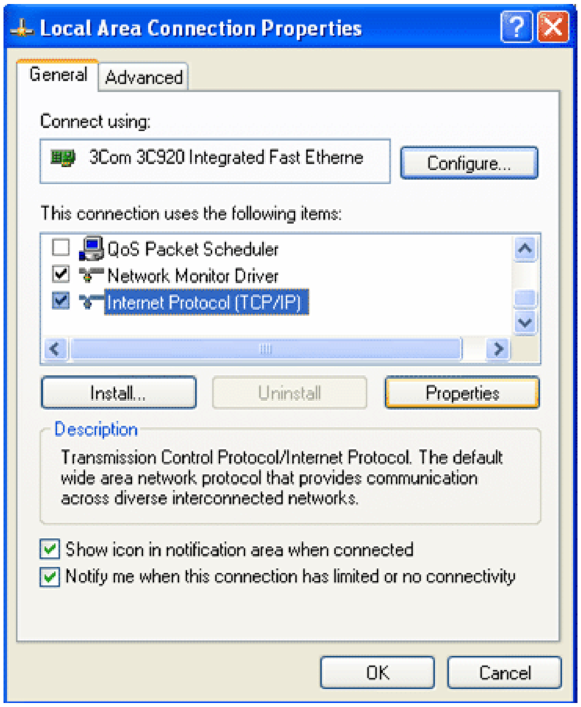
b) Click on **Control Panel**. The Control Panel window will open.



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.



Connect using:

3Com 3C920 Integrated Fast Etherne

This connection uses the following items:

□ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description

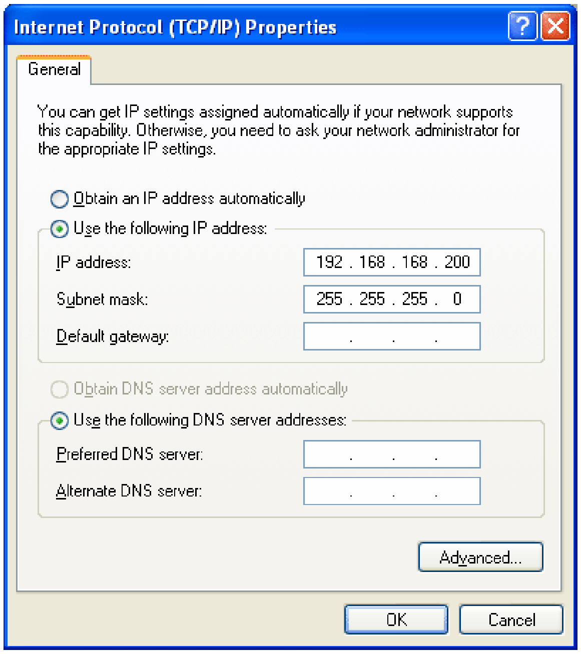
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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 VRCNX-M configuration process to return the PC to its usual settings.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

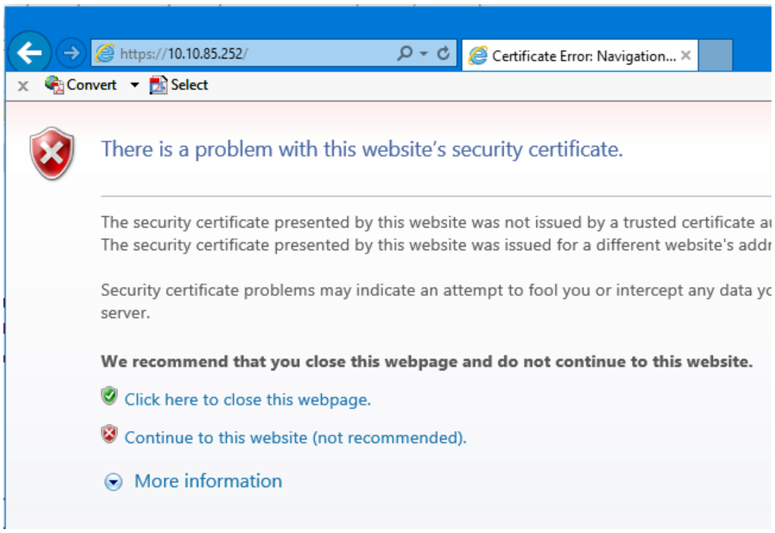
i) Enter 192.168.168.200 into the **IP address** field.

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 the default VRCNX-M IP address (Default IP address is 192.168.168.249).

3 Open a web browser.

4 Navigate to https://192.168.168.249 – the VRCNX-M controllers use a self-signed certificate for SSL communications, so you may see the warning below. Click “Continue to this website” to access the controller login page.



https://10.10.85.252/

Certificate Error: Navigation...

There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate a

The security certificate presented by this website was issued for a different website's addr

Security certificate problems may indicate an attempt to fool you or intercept any data yc server.

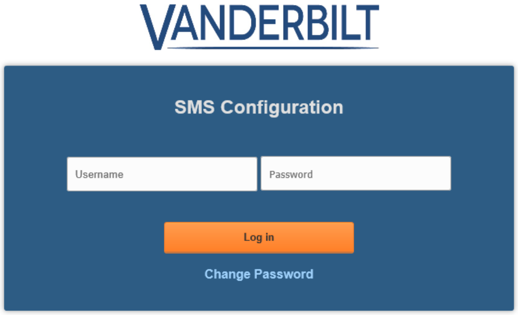
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

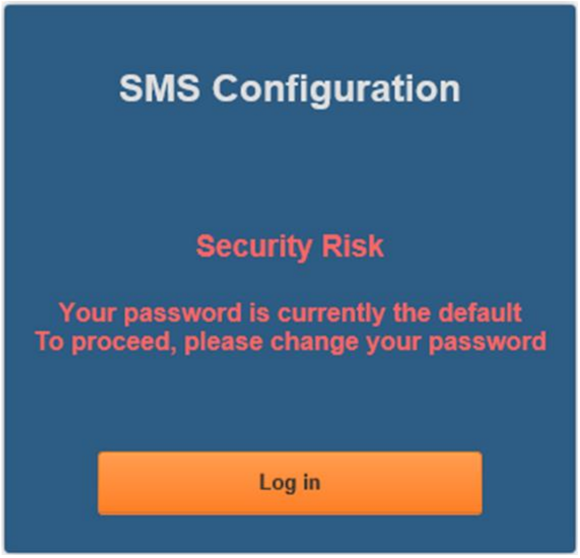
More information

5 Enter “SMSAdmin” for the user name and “SECAdmin1” for the password and click **Log in**.



a) The “SECAdmin1” password is only valid on the first login for after updating to FW v7.02M or new shipments from Vanderbilt after 7/8/2020.

b) On initial login the following message will be displayed:



Security Risk

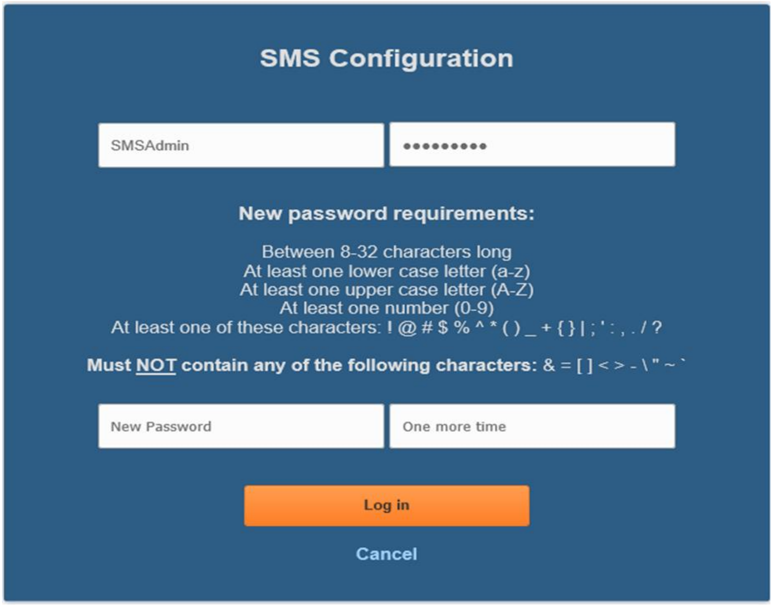
Your password is currently the default
To proceed, please change your password

c) You are required to enter a new, complex password.

d) Click **Log in** and provide the default credentials again.

e) Click **Change Password**.

f) Enter and confirm the new password at the dialog below.



SMS Configuration

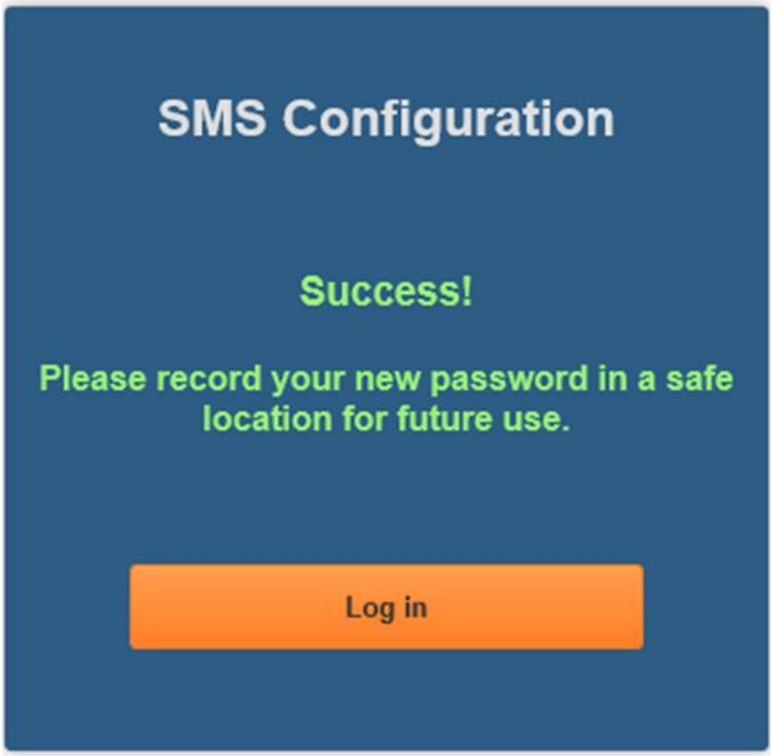
SMSAdmin ●●●●●●●●●●

New password requirements:

Between 8-32 characters long
At least one lower case letter (a-z)
At least one upper case letter (A-Z)
At least one number (0-9)
At least one of these characters: ! @ # $ % ^ * ( ) _ + { } | ; ' : , . / ?

Must NOT contain any of the following characters: & = [ ] < > - \ " ~ `

g) Select **Log in** to continue.



SMS Configuration

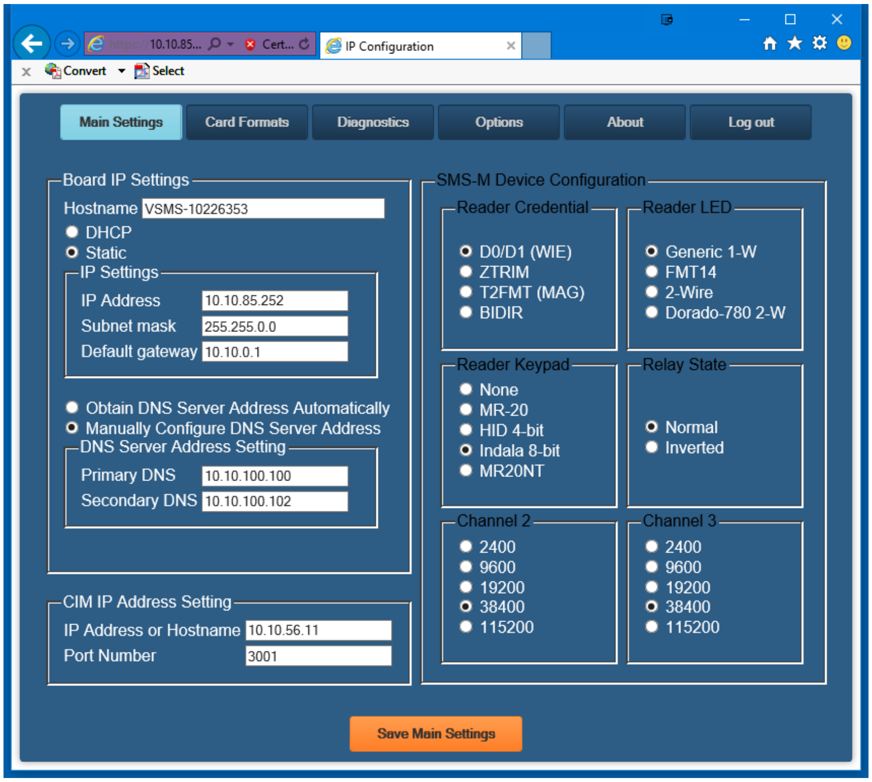
Success!

Please record your new password in a safe location for future use.

h) Select **Log in** again to continue after successful password reset.

Forgotten Password Recovery Will Require Contacting Vanderbilt Technical Support

6 The Main Settings screen will display.



Board IP Settings

Hostname VSMS-10226353

○ DHCP
◉ Static

IP Settings

IP Address 10.10.85.252
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
◉ Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

CIM IP Address Setting

IP Address or Hostname 10.10.56.11
Port Number 3001

SMS-M Device Configuration

Reader Credential
◉ D0/D1 (WIE)
○ ZTRIM
○ T2FMT (MAG)
○ BIDIR

Reader LED
◉ Generic 1-W
○ FMT14
○ 2-Wire
○ Dorado-780 2-W

Reader Keypad
○ None
○ MR-20
○ HID 4-bit
◉ Indala 8-bit
○ MR20NT

Relay State
◉ Normal
○ Inverted

Channel 2
○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

Channel 3
○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

7 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.

8 Click on the **Manually configure DNS server addresses** button (Optional, for DNS configuration).

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.

9 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or
- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

10 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered in this screen.

11 Click **Save Main Settings**. Make a note of the IP address as it will be used by SMS to communicate with the VRCNX-M.

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

The IP address of the VRCNX-M has been set.

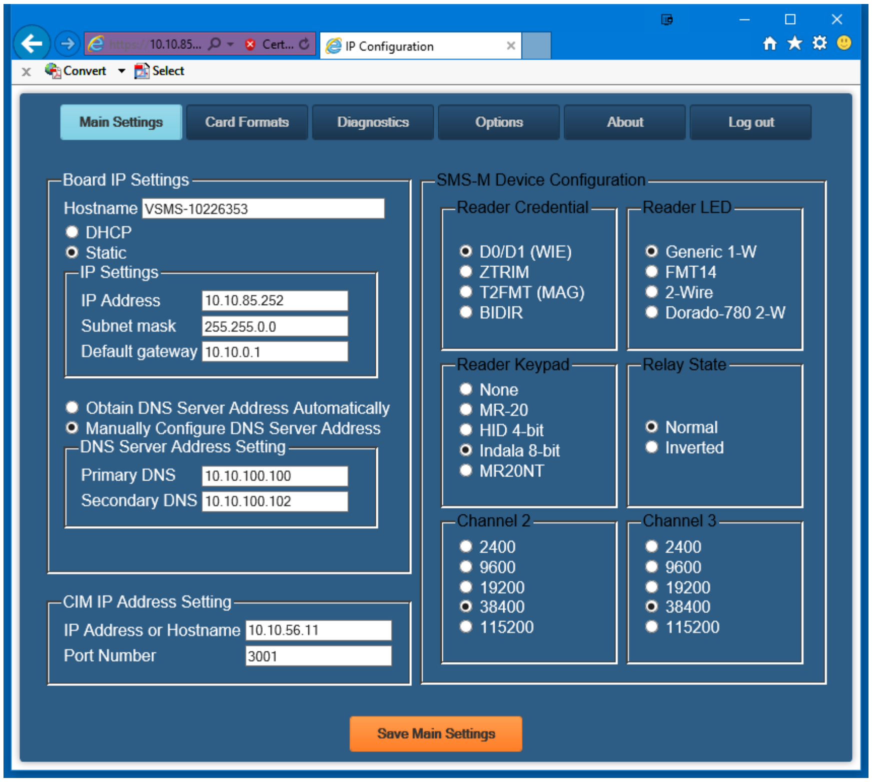
DHCP Configuration

Configuring the VRCNX-M to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

WARNING: If Controller IP address changes, the system will not be aware of it until the DNS cache refreshes. The CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may not operate correctly.

GUI (Graphical User Interface)

Main Settings



Board IP Settings

Hostname VSMS-10226353

○ DHCP
● Static

IP Settings

IP Address 10.10.85.252
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

CIM IP Address Setting

IP Address or Hostname 10.10.56.11
Port Number 3001

SMS-M Device Configuration

Reader Credential

● D0/D1 (WIE)
○ ZTRIM
○ T2FMT (MAG)
○ BIDIR

Reader LED

● Generic 1-W
○ FMT14
○ 2-Wire
○ Dorado-780 2-W

Reader Keypad

○ None
○ MR-20
○ HID 4-bit
● Indala 8-bit
○ MR20NT

Relay State

● Normal
○ Inverted

Channel 2

○ 2400
○ 9600
○ 19200
● 38400
○ 115200

Channel 3

○ 2400
○ 9600
○ 19200
● 38400
○ 115200

Hostname - This displays the name of the specific VRCNX-M. The name is in a standard format of VSMS-XXXXXXXX.

- VSMS - Mercury EP4502 Based Reader Controller
- XXXXXXXX - The serial number of the specific VRCNX-M (in the above example the serial number is 10226353).

The Host Name is used to access and setup the VRCNX-M 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 VRCNX-M to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes, there will be a loss of controller communications until the new IP address is recognized by the CIM.

Static - This setting forces the VRCNX-M to use a static IP address.

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VRCNX-M'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 VRCNX-M'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.

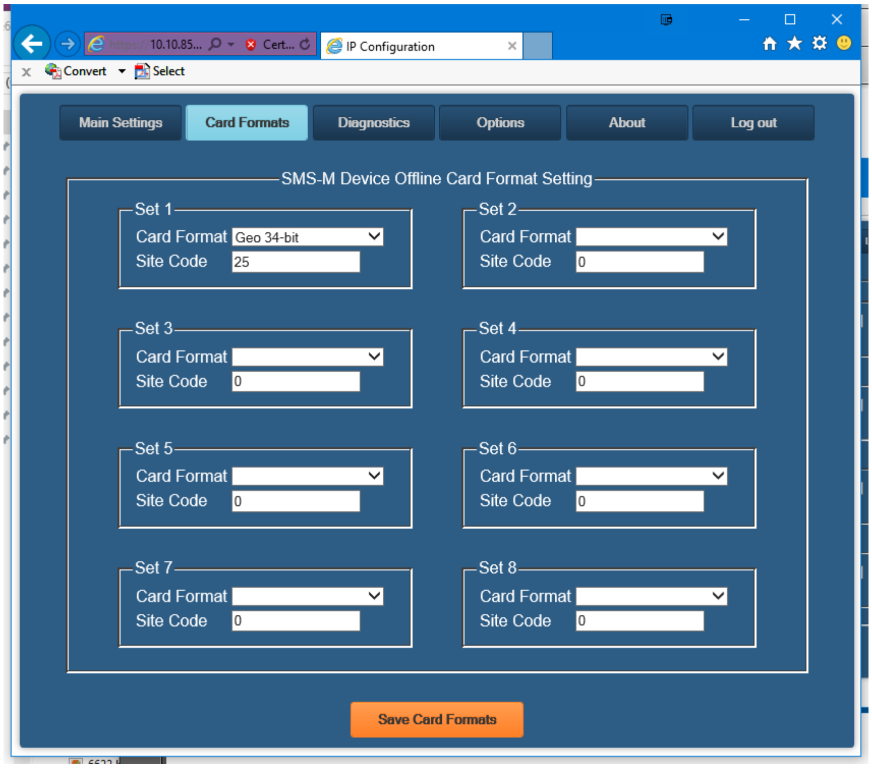
DNS Server Address Setting

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

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS the Fully Qualified Domain Name (FQDN) of the CIM should be entered here
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definitions match the port entered on this screen.

Card Formats



SMS-M Device Offline Card Format Setting

Set 1
Card Format Geo 34-bit
Site Code 25

Set 2
Card Format
Site Code 0

Set 3
Card Format
Site Code 0

Set 4
Card Format
Site Code 0

Set 5
Card Format
Site Code 0

Set 6
Card Format
Site Code 0

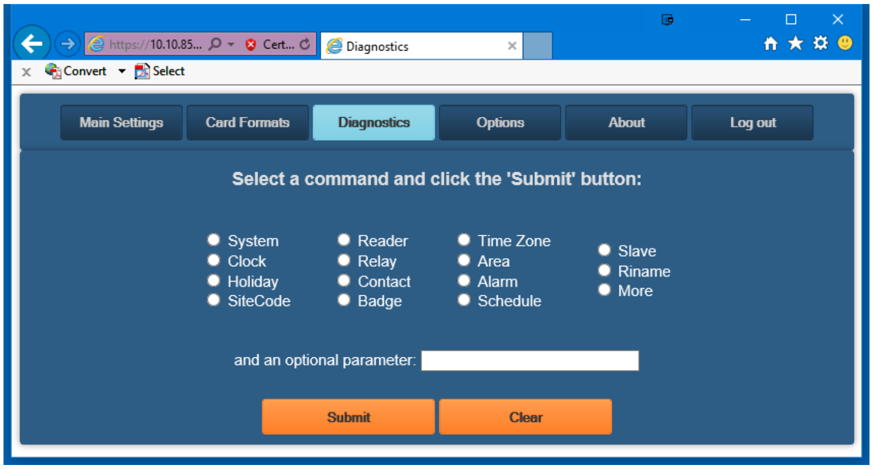
Set 7
Card Format
Site Code 0

Set 8
Card Format
Site Code 0

Set 1 – Set 8

Use this page to configure up to 8 Card Formats and Site Codes that will be active during Degraded Mode (the VRCNX-M has lost communication to the CIM and is loading the Enhanced Offline Access database from the last CIM connection).

Diagnostics



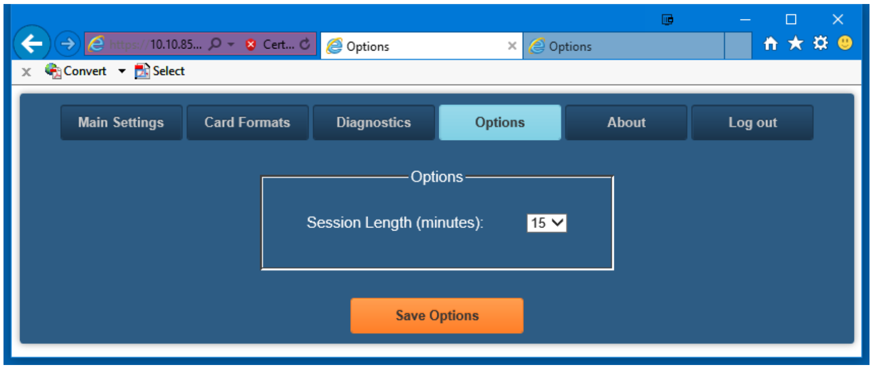
Select a command and click the 'Submit' button:

○ System ○ Reader ○ Time Zone ○ Slave
○ Clock ○ Relay ○ Area ○ Riname
○ Holiday ○ Contact ○ Alarm ○ More
○ SiteCode ○ Badge ○ Schedule

and an optional parameter:

Use this page to display additional detailed information regarding the VRCNX-M and data currently residing in memory. Use this page as directed by Vanderbilt Technical Support.

Options

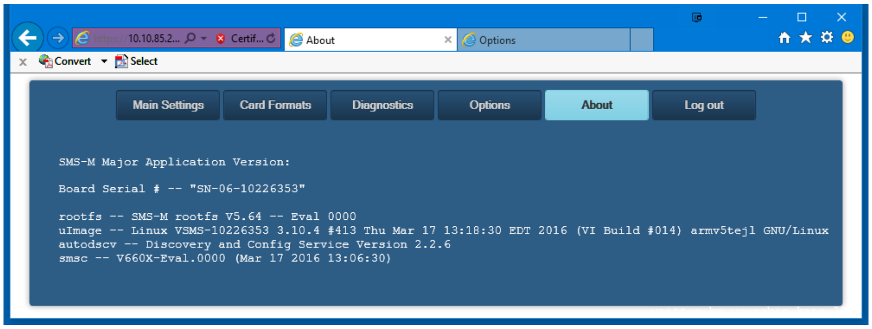


Options

Session Length (minutes): 15

Use to set the session inactivity timeout.

About



```
SMS-M Major Application Version:

Board Serial # -- "SN-06-10226353"

rootfs -- SMS-M rootfs V5.64 -- Eval 0000
uImage -- Linux VSMS-10226353 3.10.4 #413 Thu Mar 17 13:18:30 EDT 2016 (VI Build #014) armv5tejl GNU/Linux
autodscv -- Discovery and Config Service Version 2.2.6
smsc -- V660X-Eval.0000 (Mar 17 2016 13:06:30)
```

This page displays detailed information regarding the firmware loaded on the controller.

VRCNX-M Device Configuration

The VRCNX-M has 2 channels for devices and can support up to 16 devices (8 devices of the same protocol per channel). Each channel on the VRCNX-M can only support devices of the same protocol.

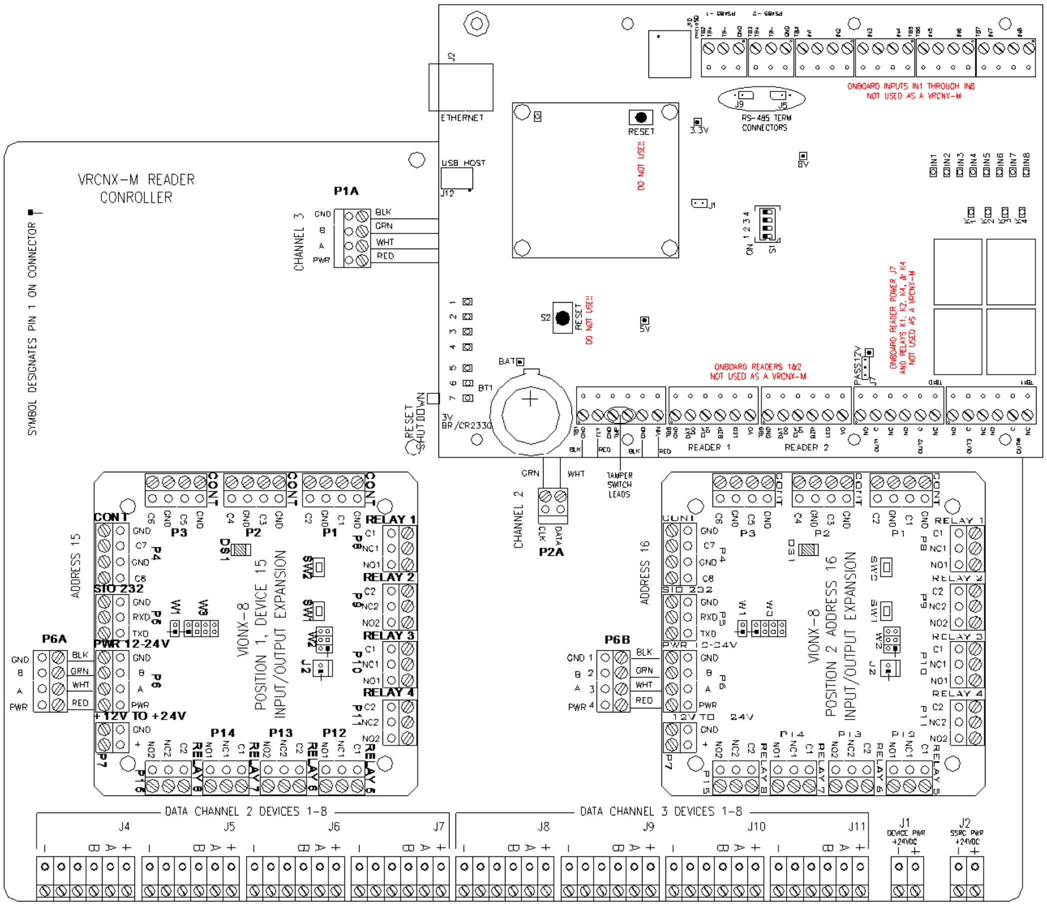
There are four types of protocol being used by devices:

- **SMS Protocol** – VRINX, VIONX-8, SRINX (Legacy) and SIONX-24 (Legacy)
- **SMS-M Protocol** – VR-1, VRI-2, VI-16IN and VI-16O
- **Aperio Protocol** – Assa Abloy Aperio AH30 RS-485 hub; A100 Narrow, IN100, K100, KS100, M100 and PR100 wireless locks
- **F-Series Protocol** – Schlage AD-Series Locks, Schlage VIP with F-protocol (*old VIP Protocol not supported*), Schlage WAPM

When connecting devices to the VRCNX-M it is important to make sure that only devices of the same protocol are put on the same channel.

- Channel 2 on the VRCNX-M (J4 through J7) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-M0 (J8 through J11) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-M1 (J8 through J11) can be used to connect SMS protocol devices only.
- Channel 3 on the VRCNX-M2 (J8 through J11) can be used to connect SMS protocol devices only.
- Channel 3 on the VRCNX-M3 (J8 through J11) can be used to connect SMS-M protocol devices only.

VRCNX-M Pin Layout



The VRCNX-M is made of up of a Controller Board and the VRCNX-R back-board. In addition, the VRCNX-M1 software configuration has one VIONX-8 board and an VRCNX-M2 has two VIONX-8 boards. The VRCNX-M3 has one VRI-16IN and one VRI-16O connected. Each of these configurations has a different pin layout which is described below.

VRCNX-M Pin Functions

J1 - Power source wiring for connected devices. This is where the power supply is connected to the VRCNX-M to supply power to devices connected to J4 through J11 (*optional as the devices can be powered locally*).

- Dev Gnd is Ground
- Dev PWR is Power

J2 - Power source wiring for the backplane mounted VSRC-M and VIONX-8(s). This is where the power supply is connected to the VRCNX-M to supply power to the backplane mounted VSRC-M and VIONX-8 (if included).

- Gnd is Ground
- PWR is Power

J4 through J7 - Communication and power for channel 2 devices. Receives power from J1.

- Pin 1 is Ground
- Pin 2 is not used
- Pin 3 is not used
- Pin 4 is B
- Pin 5 is A
- Pin 6 is Power

J8 through J11 - Communication and power for channel 3 devices. Receives power from J1.

- Pin 1 is Ground
- Pin 2 is not used
- Pin 3 is not used
- Pin 4 is B
- Pin 5 is A
- Pin 6 is Power

P1A - Power source connection and data connection for channel 2 to the VRCNX-M. Provides power to backplane mounted VSRC-M and data from RS-485-1 to channel 2 on the backplane for up to 8 devices.

- GND connects to GND (PIN 5) on TB1 on the backplane mounted VSRC-M
- B connects to TR- on TB3 (RS-485-2) on the backplane mounted VSRC-M
- A connects to TR+ on TB3 (RS-485-2) on the backplane mounted VSRC-M
- PWR connects to VIN (PIN 6) on TB1 on the backplane mounted VSRC-M

P2A - Data connection for channel 3 to the VRCNX-M. This is where the backplane mounted VSRC-M receives channel 3 communication from the VRCNX-M.

- CLK connects to TR- on TB2 (RS-485-1) on the backplane mounted VSRC-M
- DAT connects to TR+ on TB2 (RS-485-1) on the backplane mounted VSRC-M

P6A - Power source and data connection to the first VIONX-8. Provides power for the first VIONX-8 from the VRCNX-M backplane and communication to the backplane mounted VSRC-M.

- GND connects to GND on P6 of the VIONX-8
- B connects to B on P6 of the VIONX-8
- A connects to A on P6 of the VIONX-8
- PWR connects to PWR on P6 of the VIONX-8

P6B - Power source and data connection to the second VIONX-8. Provides power for the first VIONX-8 from the VRCNX-M backplane and communication to the backplane mounted VSRC-M.

- GND connects to GND on P6 of the VIONX-8
- B connects to B on P6 of the VIONX-8
- A connects to A on P6 of the VIONX-8
- PWR connects to PWR on P6 of the VIONX-8

P7 - Tamper Switch. Connection for a tamper switch for the whole VRCNX-M.

Leads from the enclosure mounted tamper switch are connected to TB1 PINs 3 & 4 on the backplane mounted VSRC-M.

S1 - Used to determine the type of VRCNX-M (M0, M1 or M2/M3) and to disable network communication.

- Switch 1 - Enable/Disable: Onboard web server (Configuration GUI), Ping and Discovery protocol. Enabled by default. If OFF, the onboard web server (GUI), Ping and Discovery protocol are disabled. If disabled the VRCNX-M cannot be reached via the GUI, Ping or the Discovery and Configuration Tool.
- Switch 2 - Reserved for Future Use
- Switch 3 - Used in Conjunction with Switch 4 to determine type of VRCNX-M (M0, M1, M2/M3). See chart below for details.
- Switch 4 - Used in Conjunction with Switch 3 to determine type of VRCNX-M (M0, M1, M2/M3). See chart below for details. VRCNX-M2 and VRCNX-M3 switch settings are identical, the types are differentiated in SMS software configuration.

VRCNX-M Type	Switch 3	Switch 4
M0	On	On
M1	Off	On
M2 / M3	On	Off

Warning: Vanderbilt recommends Setting S1-Switch 1 OFF to DISABLE the onboard web server, ping, and discovery protocol after installation and configuration. Leaving these features enabled could allow unauthorized access to the controller.

Pins Left at Default

The below pins should be left at their default settings:

- J9 - Used for RS485 Channel 2 termination (Reader Interface Termination).
  Default: PINs 1 & 2 Jumper Removed.
- J5 - Used for RS485 Channel 3 termination (Reader Interface Termination).
  Default: PINs 1 & 2 Jumper Removed.

VIONX-8 Pin Functions

Note: There can be up to two VIONX-8 boards onboard the VRCNX-M. The below pin functions are broken up into first and second VIONX-8s for clarity.

First VIONX-8 (left side)

P6 - Power source and data connection to the VRCNX-M. This is where the onboard VIONX-8 receives power and communication from the VRCNX-M.

- GND connects to GND on P6A of the VRCNX-M backplane
- B connects to B on P6A of the VRCNX-M backplane
- A connects to A on P6A of the VRCNX-M backplane
- PWR connects to PWR P6A of the VRCNX-M backplane

P1 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 1
- Pin 3 is Ground
- Pin 4 is Contact 2

P2 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 3
- Pin 3 is Ground
- Pin 4 is Contact 4

P3 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 5
- Pin 3 is Ground
- Pin 4 is Contact 6

P4 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 7
- Pin 3 is Ground
- Pin 4 is Contact 8

P8 - Relay Output 1. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P9 - Relay Output 2. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P10 - Relay Output 3. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P11 - Relay Output 4. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P12 - Relay Output 5. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P13 - Relay Output 6. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P14 - Relay Output 7. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P15 - Relay Output 8. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

SW1 - Hardware Reset Switch. The Reset Switch clears all the memory on the VIONX-8. 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 VIONX-8 (P6 or P7) when pressing reset switches.

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

W3 - VIONX-8 Addressing. The address is preset and should not be altered.
Default is address 15 -- Jumpers on 1 & 2.

Second VIONX-8 (right side)

P6 - Power source and data connection to the VRCNX-M. This is where the onboard VIONX-8 receives power and communication from the VRCNX-M.

- GND connects to GND on P6B of the VRCNX-M backplane
- B connects to B on P6B of the VRCNX-M backplane
- A connects to A on P6B of the VRCNX-M backplane
- PWR connects to PWR P6B of the VRCNX-M backplane

P1 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 9
- Pin 3 is Ground
- Pin 4 is Contact 10

P2 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 11
- Pin 3 is Ground
- Pin 4 is Contact 12

P3 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 13
- Pin 3 is Ground
- Pin 4 is Contact 14

P4 - Contact inputs. Each contact input can support two contacts, each with its own ground.

- Pin 1 is Ground
- Pin 2 is Contact 15
- Pin 3 is Ground
- Pin 4 is Contact 16

P8 - Relay Output 9. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P9 - Relay Output 10. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P10 - Relay Output 11. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P11 - Relay Output 12. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P12 - Relay Output 13. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P13 - Relay Output 14. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P14 - Relay Output 15. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

P15 - Relay Output 16. Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

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

SW1 - Hardware Reset Switch. The Reset Switch clears all the memory on the VIONX-8. 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 VIONX-8 (P6 or P7) when pressing reset switches.

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

W3 - VIONX-8 Addressing. The address is preset and should not be altered.
Default is address 16 - Jumpers on: None.

Pins Not Used

P7

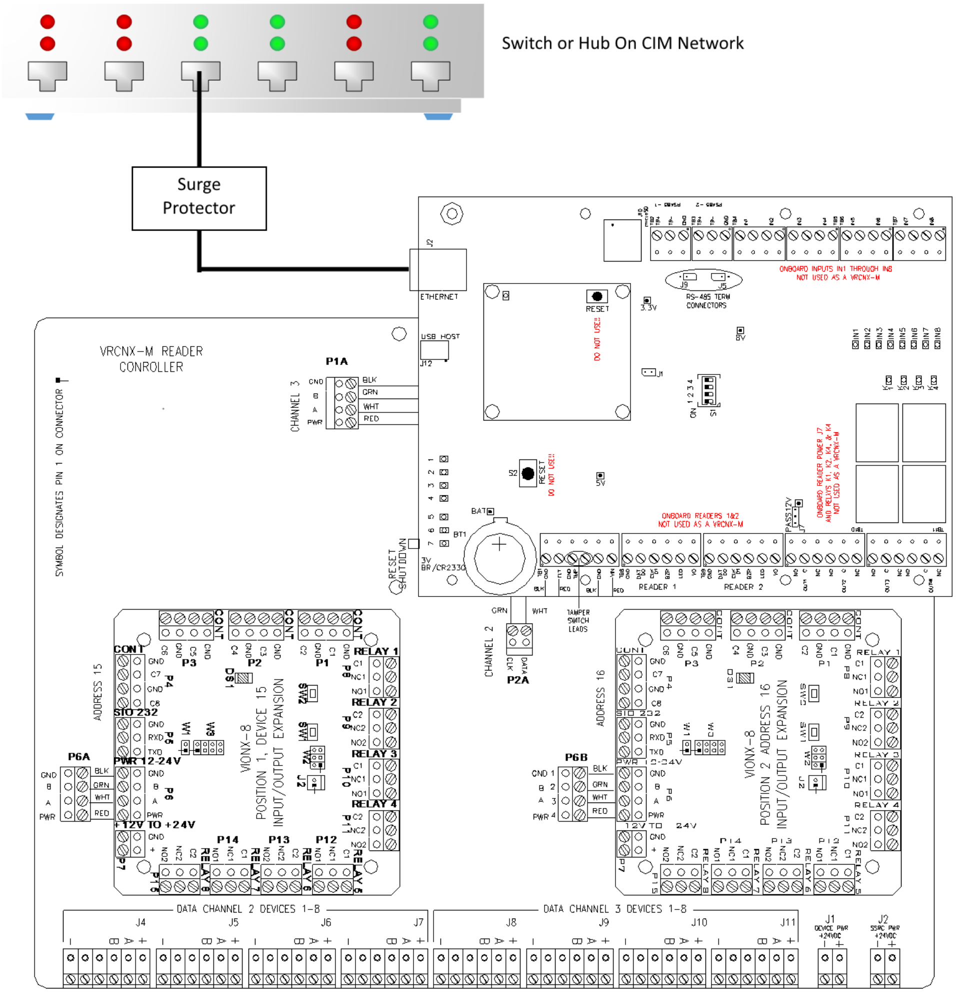
P5

W1

J2

Connecting to CIM

There is no direct connection between the VRCNX-M and the CIM. To connect, they need to be on the same network and the proper IP address of the VRCNX-M needs to be entered when setting up the VRCNX-M in SMS. In addition, a data surge protector needs to be installed between the VRCNX-M 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 J2 on the VRCNX-M.

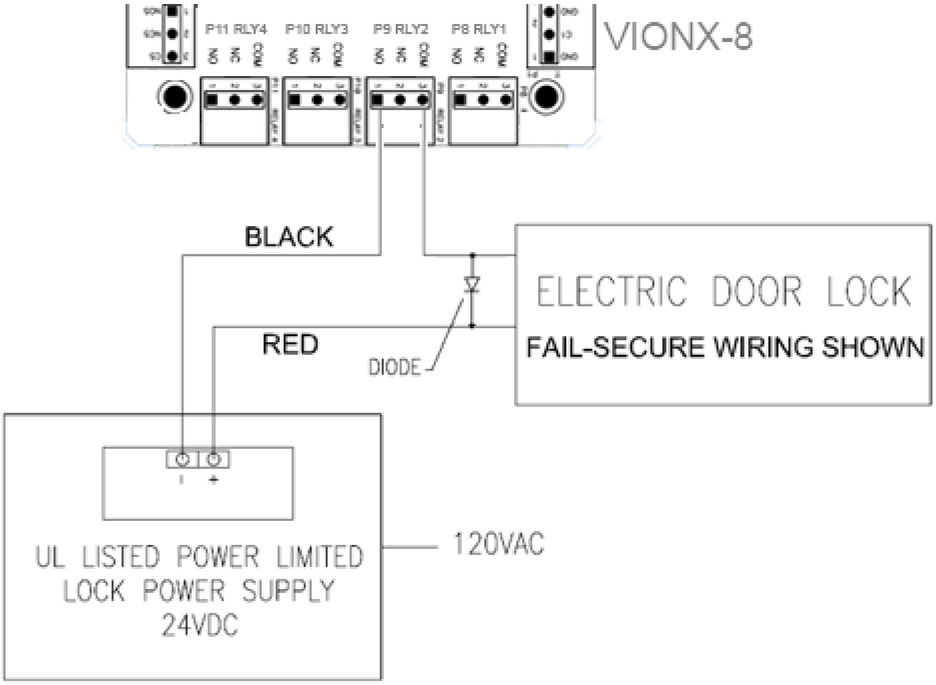

Switch or Hub On CIM Network
Surge Protector
ETHERNET
RESET
USB HOST
J12
VRCNX-M READER CONROLLER
SYMBOL DESIGNATES PIN 1 ON CONNECTOR
P1A
CHANNEL 3
GND
B
A
PWR
BLK
GRN
WHT
RED
RS-485 TERM CONNECTORS
ONBOARD INPUTS IN1 THROUGH IN8 NOT USED AS A VRCNX-M
DO NOT USE!!
ONBOARD READERS 1&2 NOT USED AS A VRCNX-M
ONBOARD READER POWER J7 AND RELAYS K1, K2, K4, & K4 NOT USED AS A VRCNX-M
READER 1
READER 2
3V BR/CR2330
BT1
BAT
RESET SHUTDOWN
CHANNEL 2
P2A
TAMPER SWITCH LEADS
ADDRESS 15
VIONX-8 POSITION 1, DEVICE 15 INPUT/OUTPUT EXPANSION
ADDRESS 16
VIONX-8 POSITION 2 ADDRESS 16 INPUT/OUTPUT EXPANSION
P6A
P6B
DATA CHANNEL 2 DEVICES 1-8
DATA CHANNEL 3 DEVICES 1-8
J4
J5
J6
J7
J8
J9
J10
J11
J1 DEVICE PWR +24VDC
J2 SSRC PWR +24VDC

Data Communication between CIM and VRCNX-M

CIM	VRCNX-M
Ethernet To Network	Ethernet to Network

Installing Diode for Lock Wiring - Relay

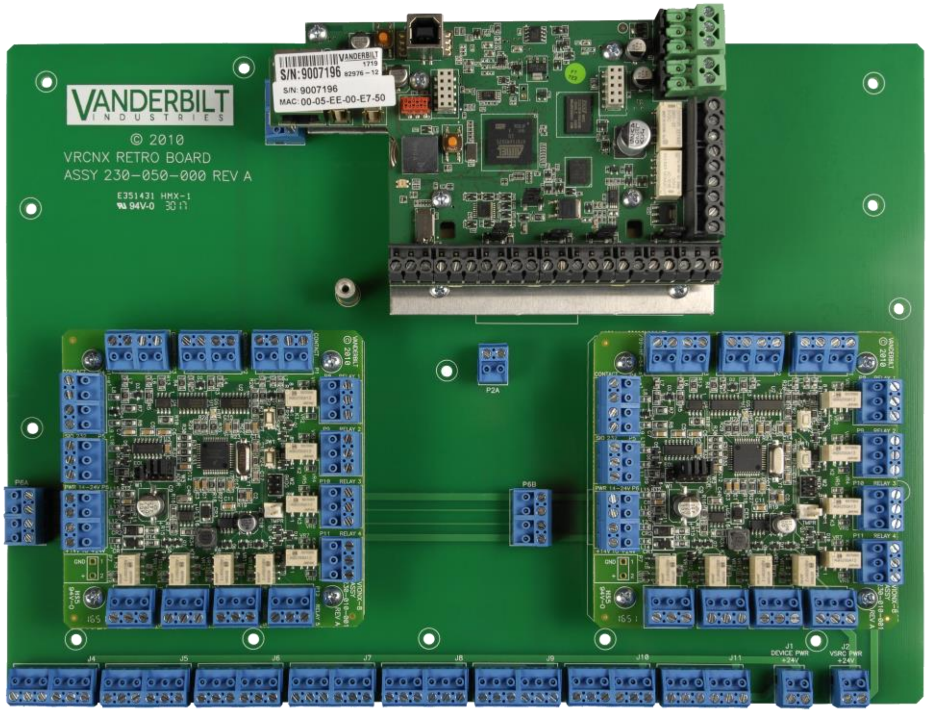
If installing an VRCNX-M1/2 a diode is supplied with the system which should be fitted across 12VDC or 24VDC and COM of the VIONX-8 to protect the relay contacts.



The lock is wired across 12VDC or 24VDC 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 Safe / Fail Secure. (Above diagram is of Fail Secure).

CHAPTER 4

VRCNX-A



Reader Controller with 2 x VIONX-8

Overview

The VRCNX-A Reader Controller is an intelligent device that can be paired with v6.4.1 and newer **Vanderbilt Security Management System** (SMS) Enterprise software installations. The VRCNX-A can have up to two VIONX-8 I/O modules mounted onboard the back plane or 1 x VI-16IN and 1 x VI-16O I/O modules connected externally which can be configured as “onboard” to provide “onboard” contacts and relays which do not contribute to the total number of connected devices. The VRCNX-A is an independently programmable device which is capable of making decisions and storing history at the local level (*Enhanced Offline Mode*) if communication is lost.

The VRCNX-A has three different **software** defined types depending on the contacts and relays devices associated with the board: VRCNX-A0, VRCNX-A1, VRCNX-A2 and VRCNX-A3. ***VRCNX-A I/O configuration, set in the controller web configuration, must exactly match the software defined type for communications to work properly***.

- VRCNX-A0: no contacts or relays
- VRCNX-A1: 1 x VIONX8 mounted onboard, wired to Channel 3, providing 8 contacts and 8 Relays
- VRCNX-A2: 2 x VIONX8 mounted onboard, wired to Channel 3, providing 16 contacts and 16 Relays
- VRCNX-A3: 1 x VI-16IN and 1 x VI-16O mounted externally, wired to Channel 3 providing 16 contacts and 16 relays

Note: In this chapter VRCNX-A refers to all model types. The specific model will be referenced only when the model type affects set up or configuration. If either a VRCNX-A1 or a VRCNX-A will work in the configuration, then it will be referred to as VRCNX-A1/A2.

Highlights

- Communicates to the server (installed with Vanderbilt SMS software) via network protocol at 10/100 Base-T
- Powered locally by a 12 – 24 VDC @ 2A Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power
- Field Flashable firmware
- Capable of running in Enhanced Offline Mode, allowing local decision making if communication fails between the VRCNX-A and the network

Can be used with a multitude of **Vanderbilt SMS** communication devices including the Vanderbilt reader interface modules (VRINX, VRI-1 and VRI-2) which support read head technologies including Proximity, Magnetic Stripe, Wiegand, Barium Ferrite, bar code, smart card, biometric, keypad and other SMS compatible access control devices.

Features

For all VRCNX-A varieties:

- 16 external device capacity (compatible devices include: VRINX, VRI-1, VRI-2, VIONX-8, VI-16IN, VI-16O, SIONX-24 and other SMS compatible access control devices)
- Enhanced Offline Mode provides persistent copy of downloaded Access Records used for local Access decisions during loss of network connection
- Enhanced Offline Mode storage of up to 5,000 Transactions and 1,250 Alarms to nonvolatile memory (*survives power cycle*)
- Communicates with CIM via network protocol at 10/100 Base-T
- DNS Compatible

For VRCNX-A1:

- 8 supervised or unsupervised Contact Inputs
- 8 Relay Outputs

For VRCNX-A2/A3:

- 16 supervised or unsupervised Contact Inputs
- 16 Relay Outputs

Configuration Guidelines

- All VRCNX-A Reader Controllers have 2 communication channels (channels 2 and 3). Each channel supports 8 RS-485 (wired) devices for a total of 16 devices. Only devices of the same protocol (either SMS protocol, SMS-M protocol, F-series protocol or Aperio Protocol) may be connected to an individual channel.
  - **The VRCNX-A1 and the VRCNX-A2 can only have SMS protocol devices connected to channel 3.**
  - **The VRCNX-A3 can only have SMS-M protocol devices connected to channel 3.**
- Vanderbilt devices that may be connected to a VRCNX-A: VRINX, VIONX-8 and SIONX-24 (SMS protocol); VI-1, VI-2, VI-16IN and VI-16O (SMS-M protocol).

- Other devices that may be connected to a VRCNX-A:
  - Schlage NDE Gateway with NDE linked with to up to 16 NDE wireless locks (up to 10 per NDE Gateway)
  - Schlage wireless PIM-485 or PIM-400 linked with up to 16 AD-400 wireless locks (16 per PIM)
  - AD-300 and Schlage VIP Locks (with F-series protocol);
  - Aperio AH-30 hub (Aperio Protocol) with up to 16 supported Aperio Wireless Locks (up to 8 Aperio wireless locks per AH-30 hub).
- The number after the VRCNX-A designates I/O modules connected to the VRCNX-A. The VRCNX-A0 has none, the VRCNX-A1 has one VIONX-8 onboard, VRCNX-A2 has two VIONX-8 onboard and the VRCNX-A3 has one VI-16IN and one VI-16O connected. These I/O modules do not count toward the total number of 16 devices that can be connected to the VRCNX-A.
- There is no Parent / Child configuration for the VRCNX-A; each VRCNX-A is a stand-alone controller.

The 2 Wiegand readers and associate I/O mounted onboard the controller are not supported.

Specifications

Board Dimensions:	9-3/4” H x 13-1/2” W x 1-1/2” D (board only)
Power Requirements:	12 – 24 VDC
Power Consumption:	360 mA @ 12 VDC (excluding peripheral devices)
Ambient Temperature:	-40º to 55º C
Humidity:	-10% to 85%

VRCNX-A Enclosure

VRCNX-A Enclosure - An enclosure with a hinged door is included for each VRCNX-A.

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: 17” x 17” x 2-3/4"

Environmental Conditions

- Ambient Temperature - 0º to 49º C or 32º to 120º F
- The room must be dust free and clean
- Mount the enclosure on fire rated plywood which is affixed to a cinder block wall or finished wall covering
- 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.

VRCNX-A IP Configuration

The IP address of the VRCNX-A has to be configured so that it can communicate with the CIM. Configuration should occur after the VRCNX-A has been fully installed. Below are detailed instructions on how to configure the VRCNX-A with a Static IP address. DHCP configuration is possible, but not recommended.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

DNS Configuration

VRCNX-A controllers are DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section for DHCP setup.

Follow the steps below to configure the static IP of the VRCNX-A.

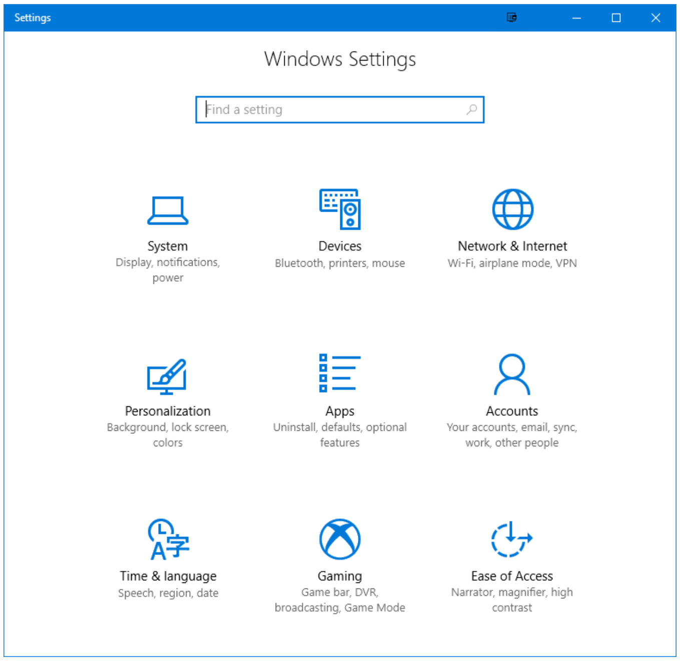
1 Connect a PC with a web browser to the VRCNX-A.

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

c) Click the **Start** button.

d) Click **Settings**.



Settings

Windows Settings

Find a setting

System
Display, notifications, power

Devices
Bluetooth, printers, mouse

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

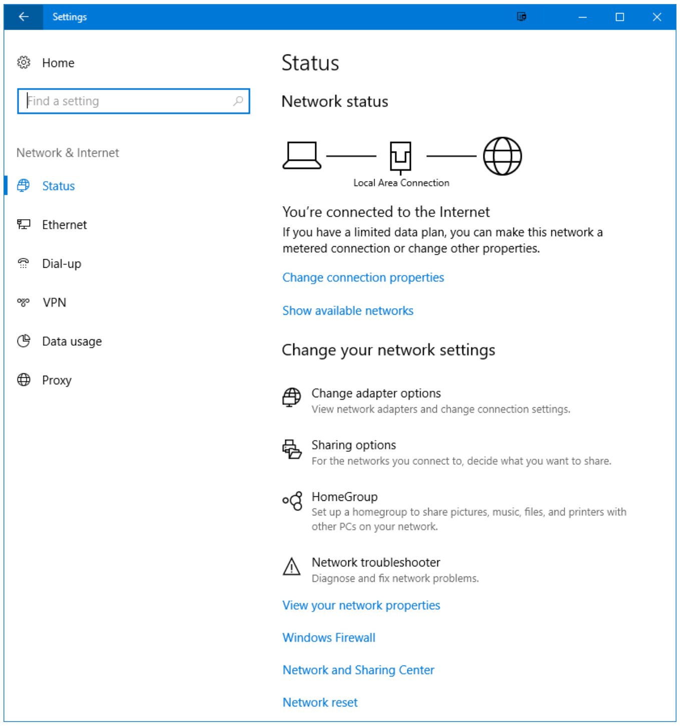
Accounts
Your accounts, email, sync, work, other people

Time & language
Speech, region, date

Gaming
Game bar, DVR, broadcasting, Game Mode

Ease of Access
Narrator, magnifier, high contrast

e) Click **Network & Internet**.



Settings

Home

Find a setting

Network & Internet

- Status
- Ethernet
- Dial-up
- VPN
- Data usage
- Proxy

Status

Network status

Local Area Connection

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

HomeGroup
Set up a homegroup to share pictures, music, files, and printers with other PCs on your network.

Network troubleshooter
Diagnose and fix network problems.

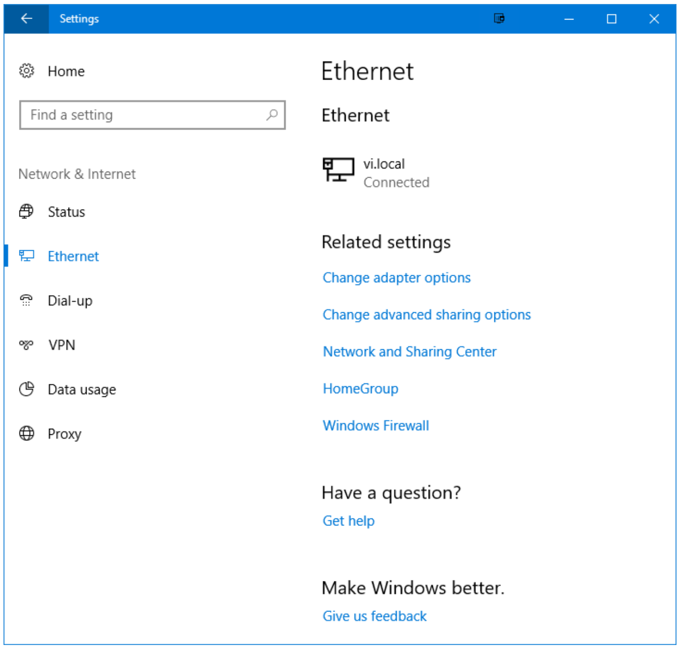
View your network properties

Windows Firewall

Network and Sharing Center

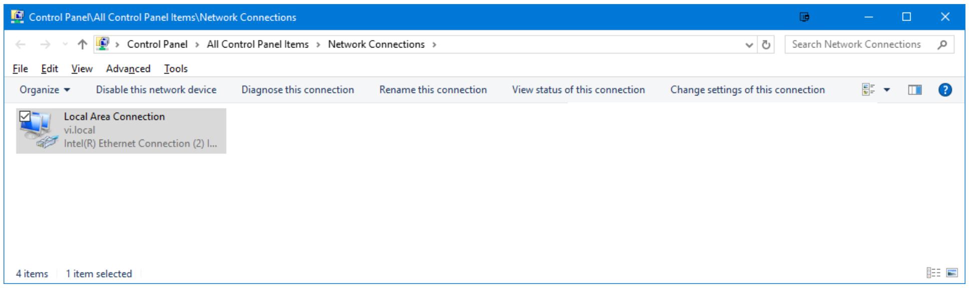
Network reset

f) Click **Ethernet**.



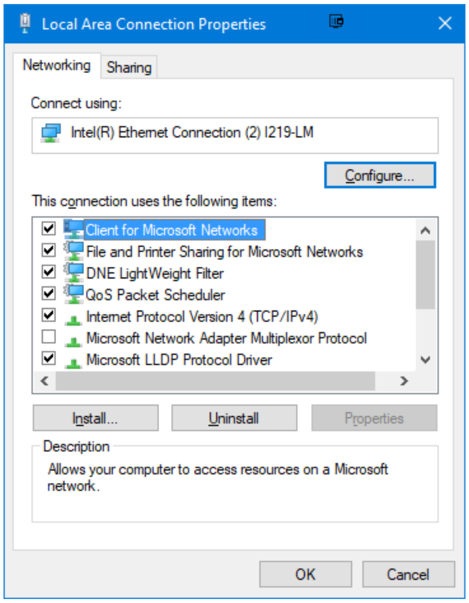
vi.local
Connected

g) Click **Change adapter options**


Control Panel\All Control Panel Items\Network Connections
Control Panel › All Control Panel Items › Network Connections ›
Search Network Connections
File Edit View Advanced Tools
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
4 items
1 item selected

Local Area Connection
vi.local
Intel(R) Ethernet Connection (2) I...

h) Highlight the NIC connected to the VRCNX-A and click **Change settings of this connection**.



Connect using:

Intel(R) Ethernet Connection (2) I219-LM

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ DNE LightWeight Filter
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

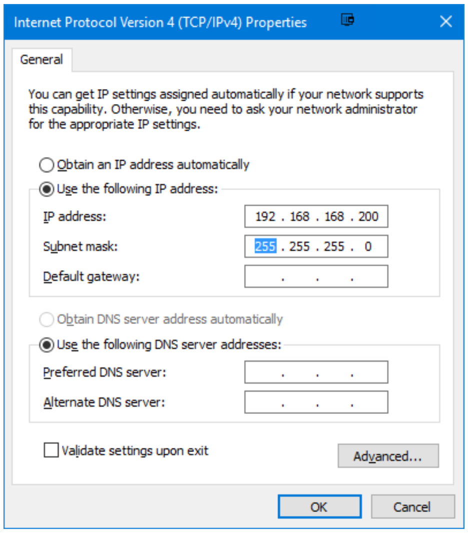
Description

Allows your computer to access resources on a Microsoft network.

i) Scroll down and select **Internet Protocol (TCP/IP v4)**.

j) Click the **Properties** button.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 168 . 200
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

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

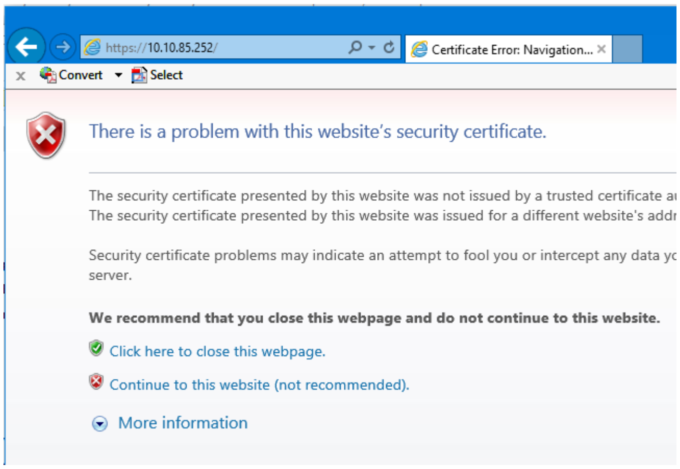
m) Enter 192.168.168.200 into the **IP address** field.

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

o) Click on the **OK** button. The window will close. The PC's network settings are now compatible with the default VRCNX-A IP default address (default IP address = 192.168.168.249).

3 Open a web browser.

4 Navigate to https://192.168.168.249 – the VRCNX-A controllers use a self-signed certificate for SSL communications, so you may see the warning below. Click "Continue to this website" to access the controller login page.



https://10.10.85.252/

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate au
The security certificate presented by this website was issued for a different website's addr

Security certificate problems may indicate an attempt to fool you or intercept any data yc server.

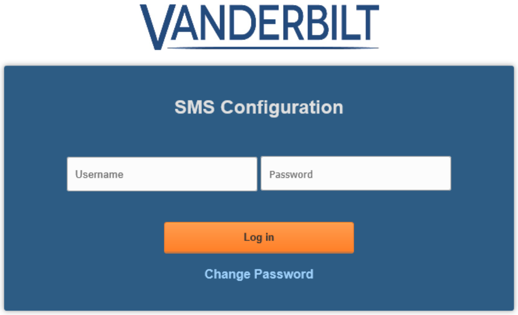
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

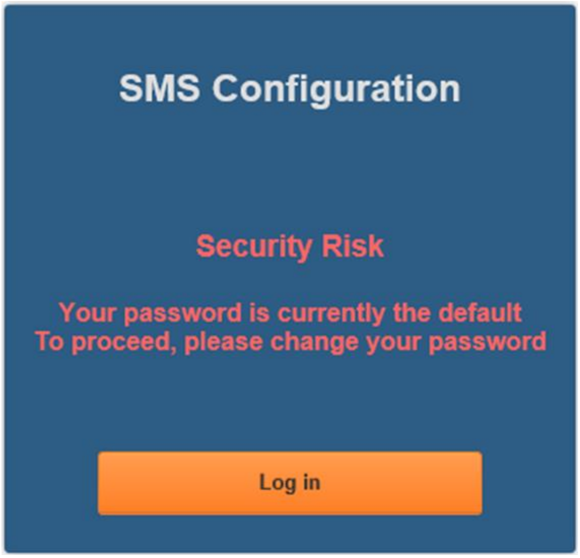
More information

5 Enter “SMSAdmin” for the user name and “SECAdmin1” for the password and click **Log in**.



a) The “SECAdmin1” password is only valid on the first login for after updating to FW v7.41A or new shipments from Vanderbilt after 7/8/2020.

b) On initial login the following message will be displayed:



Security Risk

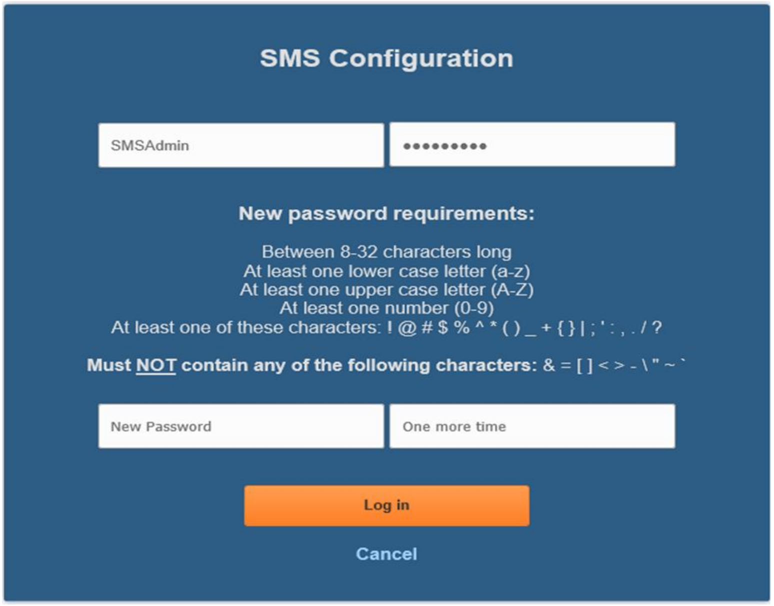
Your password is currently the default
To proceed, please change your password

c) You are required to enter a new, complex password.

d) Click **Log in** and provide the default credentials again.

e) Click **Change Password**.

f) Enter and confirm the new password at the dialog below.



SMS Configuration

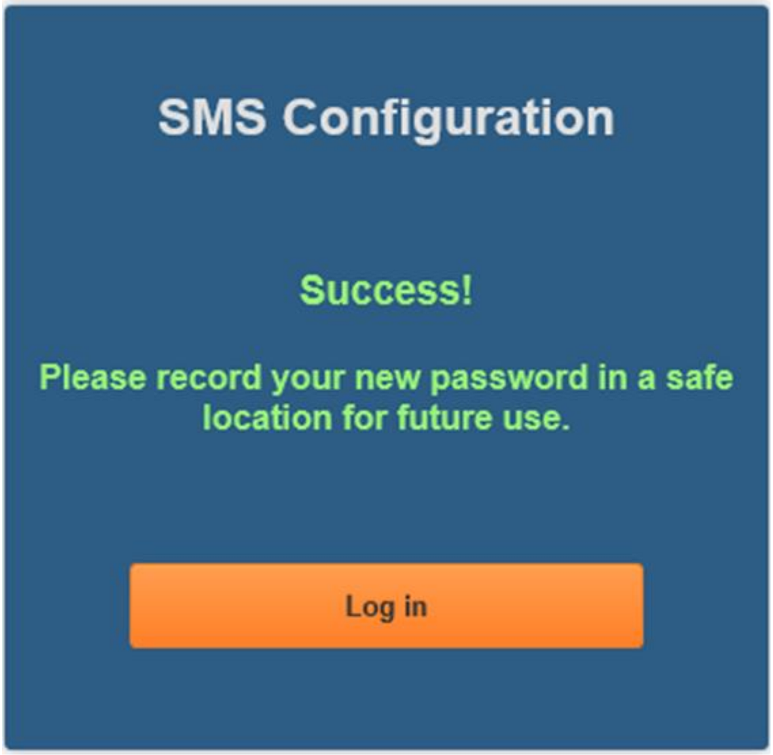
SMSAdmin
●●●●●●●●●

New password requirements:

Between 8-32 characters long
At least one lower case letter (a-z)
At least one upper case letter (A-Z)
At least one number (0-9)
At least one of these characters: ! @ # $ % ^ * ( ) _ + { } | ; ' : , . / ?

Must NOT contain any of the following characters: & = [ ] < > - \ " ~ `

g) Select **Log in** to continue.



SMS Configuration

Success!

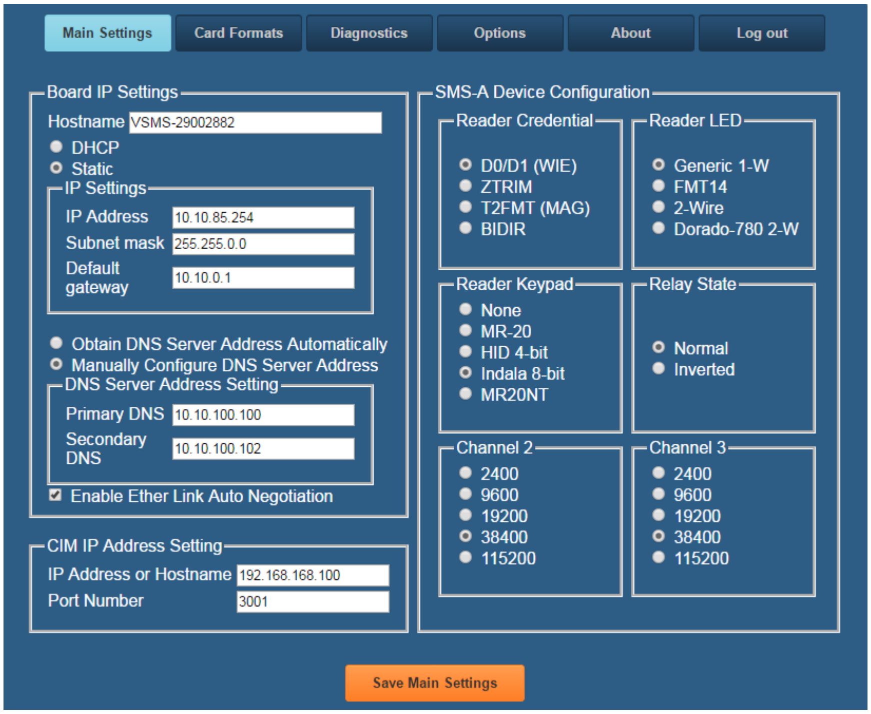
Please record your new password in a safe location for future use.

h) Select **Log in** again to continue after successful password reset.

Forgotten Password Recovery Will Require Contacting Vanderbilt Technical Support

6 The Main Settings screen will display.

NOTICE: The controller configuration password may be changed at this screen. Vanderbilt recommends that the controller configuration password is changed from the Vanderbilt default on initial controller configuration.



Board IP Settings

Hostname VSMS-29002882

○ DHCP
◉ Static

IP Settings

IP Address 10.10.85.254
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
◉ Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname 192.168.168.100
Port Number 3001

SMS-A Device Configuration

Reader Credential
◉ D0/D1 (WIE)
○ ZTRIM
○ T2FMT (MAG)
○ BIDIR

Reader LED
◉ Generic 1-W
○ FMT14
○ 2-Wire
○ Dorado-780 2-W

Reader Keypad
○ None
○ MR-20
○ HID 4-bit
◉ Indala 8-bit
○ MR20NT

Relay State
◉ Normal
○ Inverted

Channel 2
○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

Channel 3
○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

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

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

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

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

8 Click on the **Manually configure DNS server addresses** button (Optional, for DNS configuration).

l) 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.

m) 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.

9 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or
- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

10 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered in this screen.

11 Click **Save Main Settings**. Make a note of the IP address as it will be used by SMS to communicate with the VRCNX-A.

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

The IP address of the VRCNX-A has been set.

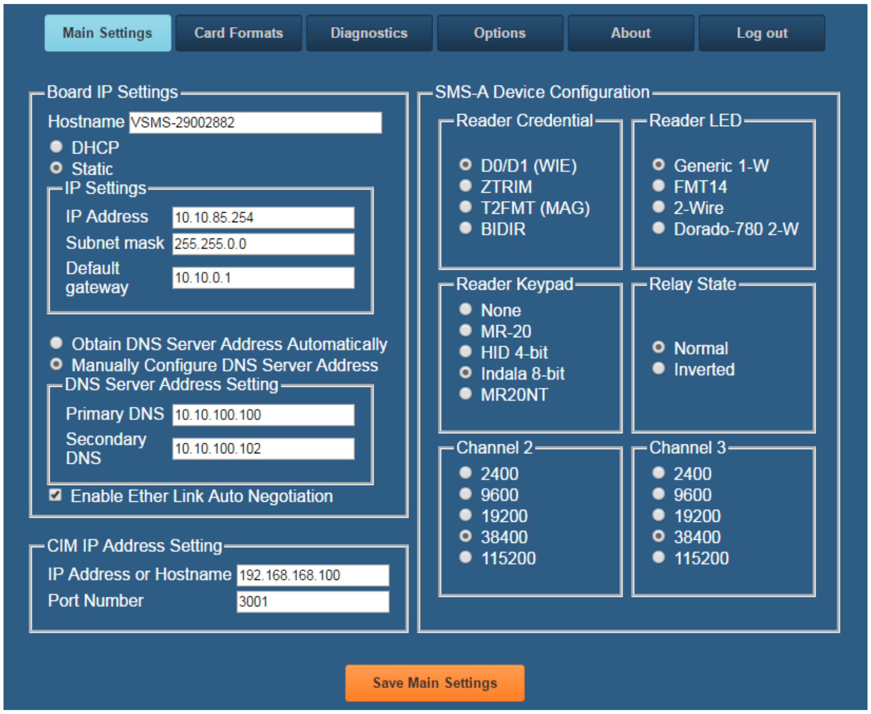
DHCP Configuration

Configuring the VRCNX-A to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

WARNING: If Controller IP address changes, the system will not be aware of it until the DNS cache refreshes. The CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may not operate correctly.

GUI (Graphical User Interface)

Main Settings



Board IP Settings

Hostname VSMS-29002882

○ DHCP
◉ Static

IP Settings

IP Address 10.10.85.254
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
◉ Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname 192.168.168.100
Port Number 3001

SMS-A Device Configuration

Reader Credential

◉ D0/D1 (WIE)
○ ZTRIM
○ T2FMT (MAG)
○ BIDIR

Reader LED

◉ Generic 1-W
○ FMT14
○ 2-Wire
○ Dorado-780 2-W

Reader Keypad

○ None
○ MR-20
○ HID 4-bit
◉ Indala 8-bit
○ MR20NT

Relay State

◉ Normal
○ Inverted

Channel 2

○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

Channel 3

○ 2400
○ 9600
○ 19200
◉ 38400
○ 115200

Hostname - This displays the name of the specific VRCNX-A. The name is in a standard format of VSMS-XXXXXXXX.

- VSMS: Vanderbilt SMS Reader Controller
- XXXXXXXX: The serial number of the specific VRCNX-A
  (in the above example the serial number is 29002882).

The Host Name is used to access and setup the VRCNX-A 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 VRCNX-A to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes, there will be a loss of controller communications until the new IP address is recognized by the CIM.

Static - This setting forces the VRCNX-A to use a static IP address.

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VRCNX-A'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 VRCNX-A'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.

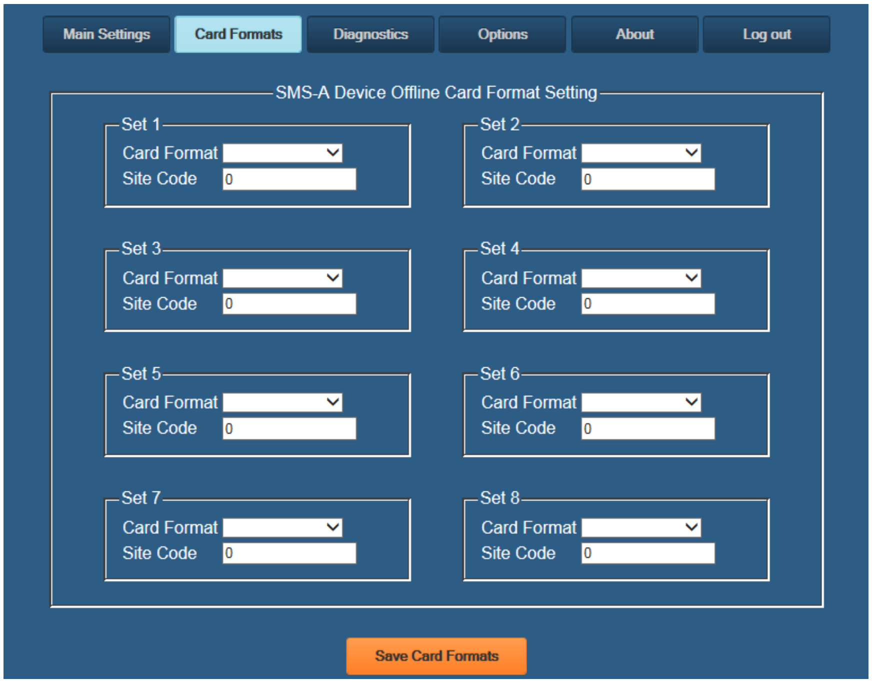
DNS Server Address Setting

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

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS the Fully Qualified Domain Name (FQDN) of the CIM should be entered here
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definitions match the port entered on this screen.

Card Formats



SMS-A Device Offline Card Format Setting

Set 1
Card Format
Site Code 0

Set 2
Card Format
Site Code 0

Set 3
Card Format
Site Code 0

Set 4
Card Format
Site Code 0

Set 5
Card Format
Site Code 0

Set 6
Card Format
Site Code 0

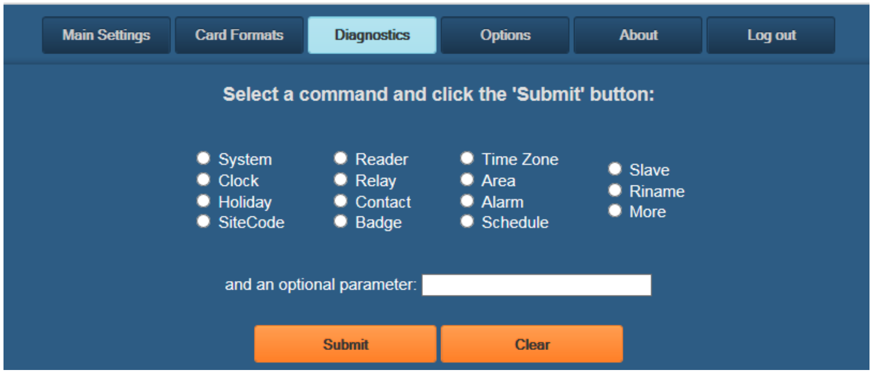
Set 7
Card Format
Site Code 0

Set 8
Card Format
Site Code 0

Set 1 – Set 8

Use this page to configure up to 8 Card Formats and Site Codes that will be active during Degraded Mode (when configured as VSRC-A only and the VSRC-A has lost communication to the CIM and is in the process of loading the Enhanced Offline Access database from the last CIM connection).

Diagnostics



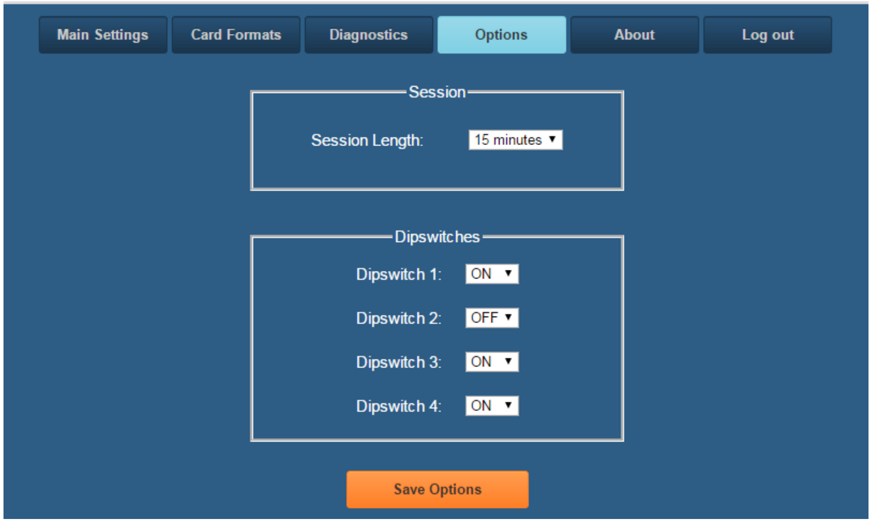
Select a command and click the 'Submit' button:

○ System ○ Reader ○ Time Zone ○ Slave
○ Clock ○ Relay ○ Area ○ Riname
○ Holiday ○ Contact ○ Alarm ○ More
○ SiteCode ○ Badge ○ Schedule

and an optional parameter:

Use this page to display additional detailed information regarding the VRCNX-A and data currently residing in memory. Use this page only as directed by Vanderbilt Technical Support.

Options



Session

Session Length: 15 minutes

Dipswitches

Dipswitch 1: ON

Dipswitch 2: OFF

Dipswitch 3: ON

Dipswitch 4: ON

- Session Length: Use to set the session inactivity timeout.
- Dipswitch 1: Enable/Disable Onboard web server (Configuration GUI), Ping and Discovery protocol. Enabled by default. If OFF, the onboard web server (GUI), Ping and Discovery protocol are disabled.
  If disabled then the VRCNX-A cannot be reached via the GUI, Ping or the Discovery and Configuration Tool.

Physical Access to the VRCNX-A is required to re-enable the Configuration Application.

Press and Hold the Tamper Switch 25 AND Press and Release the Reset Button 20 three (3) times in succession. Release the Tamper Switch 25. 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”.

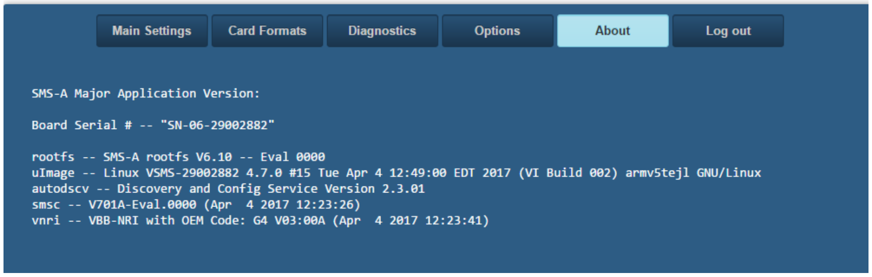
- Dipswitch 2: Reserved for Future Use
- Dipswitch 3: Used in Conjunction with Dipswitch 4 to configure as VRCNX-A0 or VRCNX-A3
- Dipswitch 4: Used in Conjunction with Dipswitch 3 to configure as VRCNX-A0 or VRCNX-A3

Type	Dipswitch 3	Dipswitch 4
VSRC-A	Off	Off
VRCNX-A0	On	On
VRCNX-A1	Off	On
VRCNX-A2/A3	On	Off

Warning: SMS software configuration of the VRCNX-A as either VRCNX-A0 / A1 / A2 / A3 **MUST** match the GUI Configuration settings or the VRCNX-A will not communicate correctly to connected devices.

Warning: Vanderbilt recommends Setting Dipswitch 1 OFF to DISABLE the onboard web server, ping, and discovery protocol after installation and configuration. Leaving these features enabled could allow unauthorized access to the controller.

About



```
SMS-A Major Application Version:

Board Serial # -- "SN-06-29002882"

rootfs -- SMS-A rootfs V6.10 -- Eval 0000
uImage -- Linux VSMS-29002882 4.7.0 #15 Tue Apr 4 12:49:00 EDT 2017 (VI Build 002) armv5tejl GNU/Linux
autodscv -- Discovery and Config Service Version 2.3.01
smsc -- V701A-Eval.0000 (Apr  4 2017 12:23:26)
vnri -- VBB-NRI with OEM Code: G4 V03:00A (Apr  4 2017 12:23:41)
```

This page displays detailed information regarding the firmware loaded on the controller.

VRCNX-A Device Configuration

The VRCNX-A has 2 channels for devices and can support up to 16 devices (8 devices of the same protocol per channel). Each channel on the VRCNX-A can only support devices of the same protocol.

There are four types of protocol being used by devices:

- **SMS Protocol** – VRINX, VIONX-8, SRINX (Legacy) and SIONX-24 (Legacy)
- **SMS-M Protocol** – VR-1, VRI-2, VI-16IN and VI-16O
- **Aperio Protocol** – Assa Abloy Aperio AH30 RS-485 hub; A100 Narrow, IN100, K100, KS100, M100 and PR100 wireless locks
- **F-Series Protocol** – Schlage ENGAGE with NDE Gateway and NDE series wireless locks, Schlage AD-Series Locks, Schlage VIP with F-protocol (*old VIP Protocol not supported*), Schlage WAPM

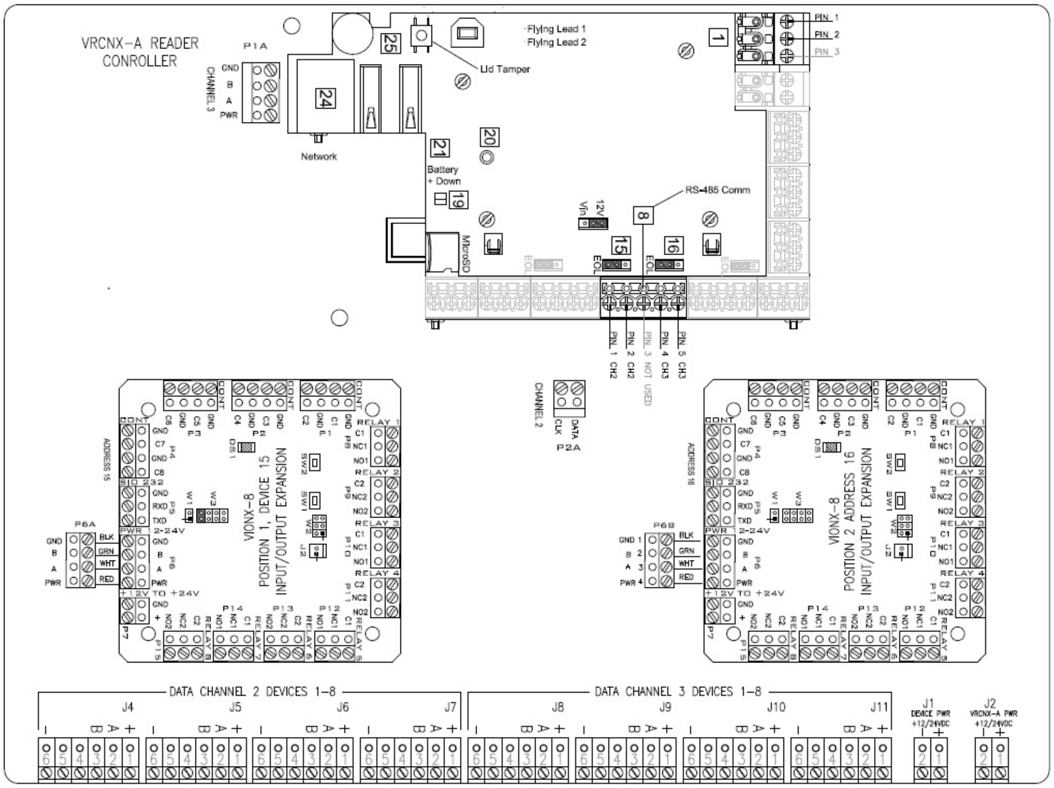
When connecting devices to the VRCNX-A it is important to make sure that only devices of the same protocol are put on the same channel.

- Channel 2 on the VRCNX-A0 (COMMS 1A & 1B) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-A0 (COMMS 2A & 2B) can be used to connect F protocol devices, SMS protocol devices, SMS-M protocol devices or Aperio protocol devices. Only one type can be used per channel, mixing protocols on one channel causes conflicts with the devices.
- Channel 3 on the VRCNX-A3 (COMMS 2A & 2B) can be used to connect SMS-M protocol devices only.

The VRCNX-A is configured through the GUI Configuration (see previous section) as a VRCNX-A0 / A1 / A2 / A3, to indicate the presence of onboard connected I/O devices.

WARNING: SMS software configuration of the VRCNX-A as either VRCNX-A0 / A1 / A2 / A3 **MUST** match the GUI Configuration settings or the VRCNX-A will not communicate correctly to connected devices.

VRCNX-A PIN Layout



The VRCNX-A is made of up of a Controller Board and the VRCNX-A back-board. In addition, the VRCNX-A3 has one VRI-16IN and one VRI-16O connected. Each of these configurations has a different PIN layout which is described below.

VRCNX-A PIN Functions

NOTICE: Connections 3, 4, 5, 6, 7, 8, 9 & 10 on the backplane mounted VSRC-A are not used when the controller is configured as a VRCNX-A (*refer to VSRC-A PIN Payout*).

J1 - Power source wiring for connected devices. This is where the power supply is connected to the VRCNX-A to supply power to devices connected to J4 through J11 (*optional if the devices are powered locally*).

- Dev Gnd is Ground
- Dev PWR is Power

J4 through J7 - Communication and power for channel 2 devices. Receives power from J1.

- PIN 6 is Ground
- PIN 5 is not used
- PIN 4 is not used
- PIN 3 is B
- PIN 2 is A
- PIN 1 is Power

J8 through J11 - Communication and power for channel 3 devices. Receives power from J1.

- PIN 6 is Ground
- PIN 5 is not used
- PIN 4 is not used
- PIN 3 is B
- PIN 2 is A
- PIN 1 is Power

P1A - Power source connection and data connection for channel 2 to the VRCNX-A. Provides power to backplane mounted VSRC-A and data from COMMS 1A & 1B to channel 3 on the backplane for up to 8 devices.

- GND connects to $\boxed{1}$ PIN 1 – on the backplane mounted VSRC-A
- B connects to $\boxed{8}$ PIN 5 – on the backplane mounted VSRC-A
- A connects to $\boxed{8}$ PIN 4 – on the backplane mounted VSRC-A
- PWR connects to $\boxed{1}$ PIN 2 – on the backplane mounted VSRC-A

P2A - Data connection for channel 3 to the VRCNX-A. This is where the backplane mounted VSRC-A receives channel 3 communication from the VRCNX-A.

- CLK connects to $\boxed{8}$ PIN 2 – on the backplane mounted VSRC-A
- DAT connects to $\boxed{8}$ PIN 1 – on the backplane mounted VSRC-A

Leads from the enclosure mounted tamper switch are connected to the leads from $\boxed{25}$ on the backplane mounted VSRC-A.

Factory Reset and Power down

The Reset Button labeled 20 on the onboard mounted VSRC-A is used for Rebooting, Powering Down and Resetting, in conjunction with the Tamper Button 25, the VRCNX-A as indicated below.

The controller will produce 3 long beeps followed by a series of shorter beeps at a faster interval when depressed.

Reboot

Press and Hold the backplane mounted VSRC-A 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.

Power Down

Press and Hold the backplane mounted VSRC-A 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.

Reboot and Reset to Default IP Address

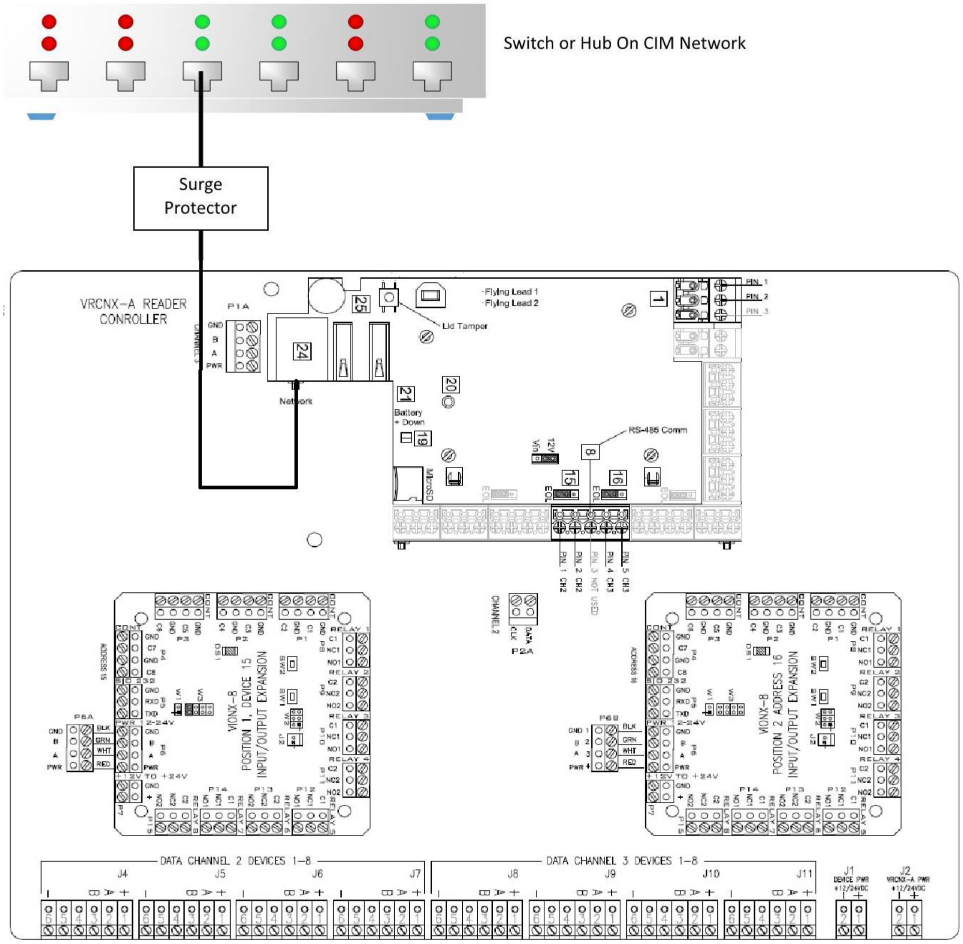
Press and Hold the backplane mounted VSRC-A Reset Button 20 **and** Tamper Button 25 until the short beeps begin and for nine (9) short beeps or less. The controller will shut down and reboot. The configured Network Settings (IP Address, etc.) will be reset to the factory default (192.168.168.249) on reboot.

Power Down and Reset to Default IP Address

Press and Hold the backplane mounted VSRC-A Reset Button 20 **and** Tamper Button 25 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 reset to factory default (192.168.1686.249) on restart. Disconnect and reconnect power to restart the controller.

Connecting to CIM

There is no direct connection between the VRCNX-A and the CIM. To connect, they need to be on the same network and the proper IP address of the VRCNX-A needs to be entered when setting up the VRCNX-A in SMS. In addition, a data surge protector needs to be installed between the VRCNX-A 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 J2 on the VRCNX-A.

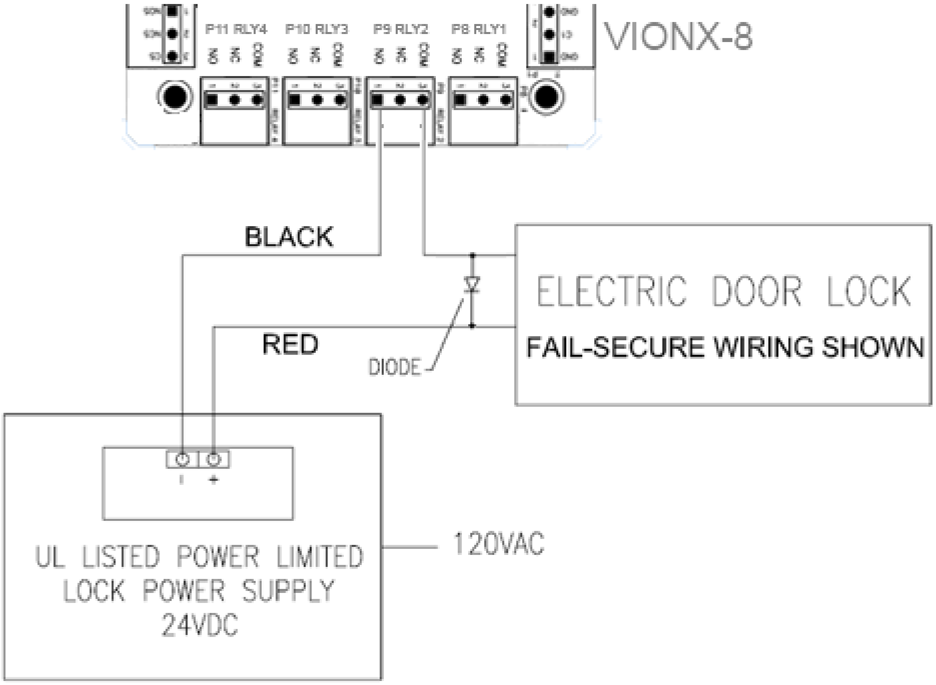


Data Communication between CIM and VRCNX-A

CIM	VRCNX-A
Ethernet To Network	Ethernet to Network

Installing Diode for Lock Wiring - Relay

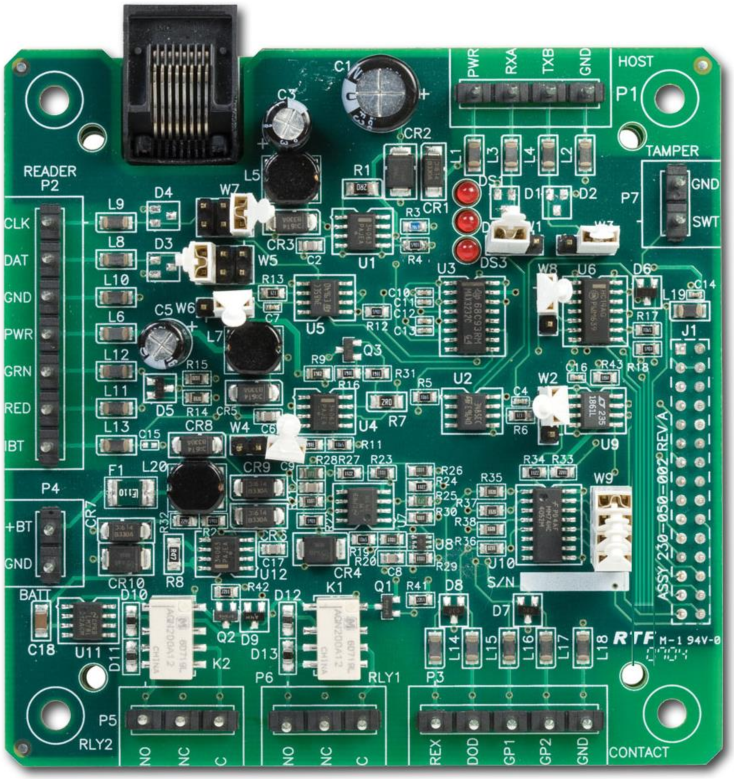
If installing an VRCNX-A1/2 a diode is supplied with the system which should be fitted across 12VDC or 24VDC and COM of the VIONX-8 to protect the relay contacts.



The lock is wired across 12VDC or 24VDC 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 Safe / Fail Secure. (Above diagram is of Fail Secure).

CHAPTER 5

VSRC



Vanderbilt Single Reader Controller (VSRC)

Overview

The Vanderbilt Single Door Controller (VSRC) is an intelligent device with a modular approach. The VSRC is an independently programmable device which is capable of making decisions and storing history at the local level if communication is lost with the server. It communicates with the CIM via TCP/IP protocol and can be connected to a variety of different read head technologies supported by SMS.

Highlights

- Supports various read head technologies; Proximity, (Wiegand Format), Magnetic Stripe, barcode, iButton, smartcard, biometric, and more.

  Proximity Cards

  - Standard 26-bit
  - Vanderbilt 34-bit

- HID Corporate 1000 35-Bit
- HID Corporate 1000 48-Bit
- HID/ProxIF 37-Bit
- XceedID 40-Bit
- XceedID 35-bit (including EV1)
- MiFare 32-Bit Serial Number (With HID read-head ONLY)

Magstripe Cards

- Geoffrey encoded magcard 14-D
- Geo-Image magcard 11-D
- Locknetic 18-D magcard

- Communicates via network protocol at 10/100 Base-T
- Powered locally by a 24VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power.
- Capable of running in degraded mode, allowing local decision making if communication fails between the VSRC and the network.

Standard Features

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

Specifications

- Board Dimensions - 3-13/16” x 3-13/16” x 1-1/4” D
- Enclosure Dimensions - 8-1/4”H x 7-1/2W” x 3-1/2” D
- Power requirements - 20VDC to 32VDC
- Power consumption - 200mA (500mA max. with read head)
- Ambient temperature - 0º to 49º C or 32º to 120º F

VSRC Enclosure

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

Features

- Metal enclosure with hinged door, tamper switch, lock & key
- 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

- 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.

VSRC IP Configuration

The IP address of the VSRC has to be configured so that it can communicate with the CIM. Configuration should occur after the VSRC has been fully installed. Detailed instructions on how to configure the VSRC with a Static IP address are listed below. DHCP configuration, while not recommended by Vanderbilt, is also possible with DHCP reservations. Please review the DHCP Configuration section before configuration.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

VSRC running firmware V2.61 or newer is DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section before configuration DHCP.

Follow the steps below to configure the static IP of the VSRC.

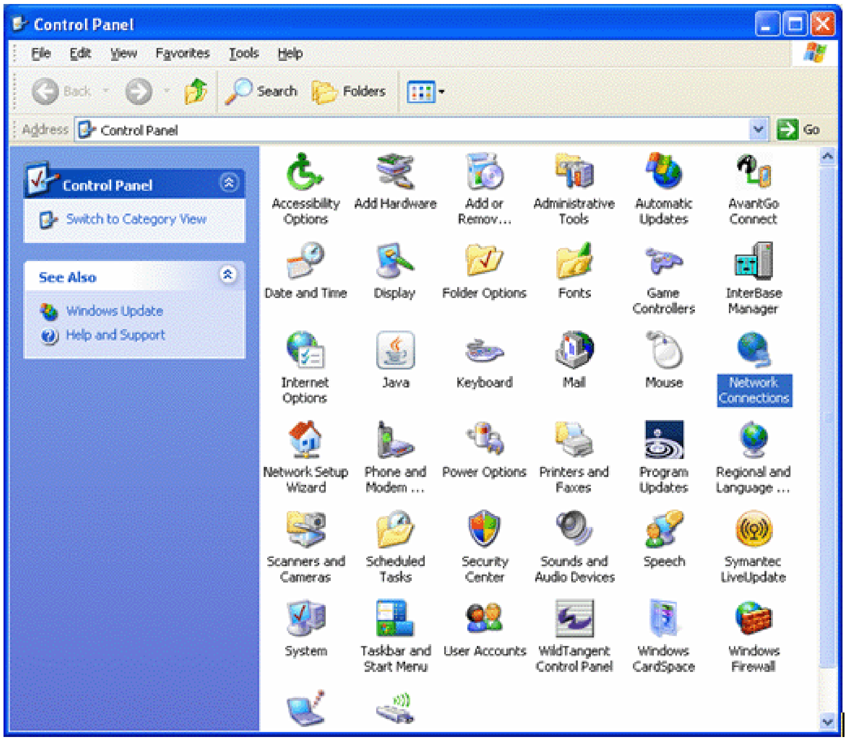
1 Connect a PC with a web browser to the VSRC.

- 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.

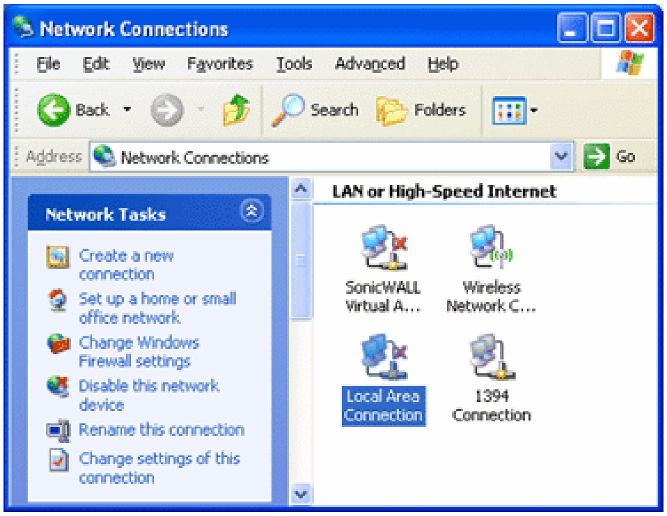
2 Configure the PC's network settings to communicate with the VSRC

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

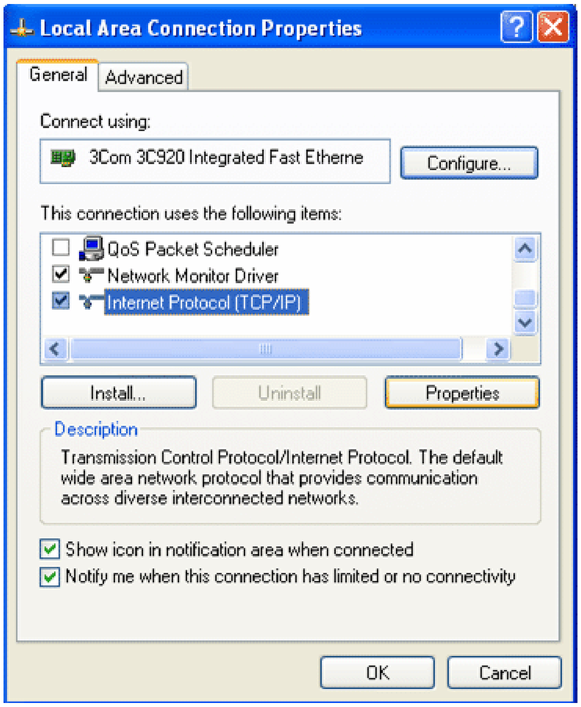
b) Click on **Control Panel**. The Control Panel window will open.



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


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Rename this connection
Change settings of this connection
LAN or High-Speed Internet
SonicWALL Virtual A...
Wireless Network C...
Local Area Connection
1394 Connection

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



Local Area Connection Properties

General | Advanced

Connect using:

3Com 3C920 Integrated Fast Etherne

This connection uses the following items:

□ QoS Packet Scheduler

☑ Network Monitor Driver

☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

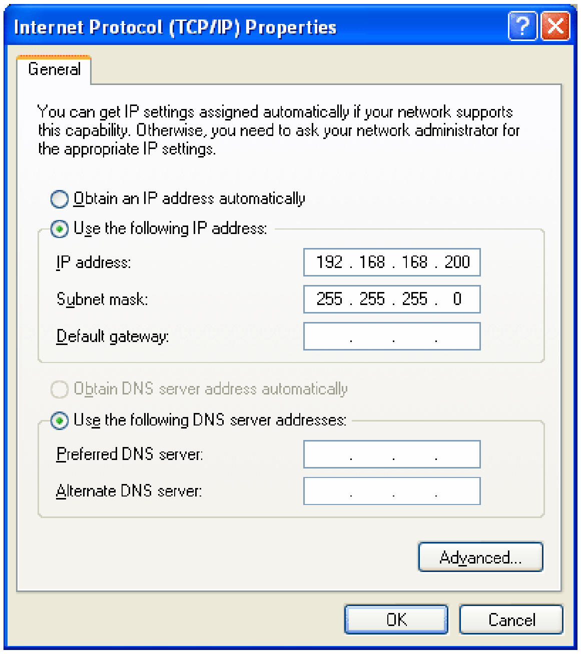
☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

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 VSRC configuration process to return the PC to its usual settings.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

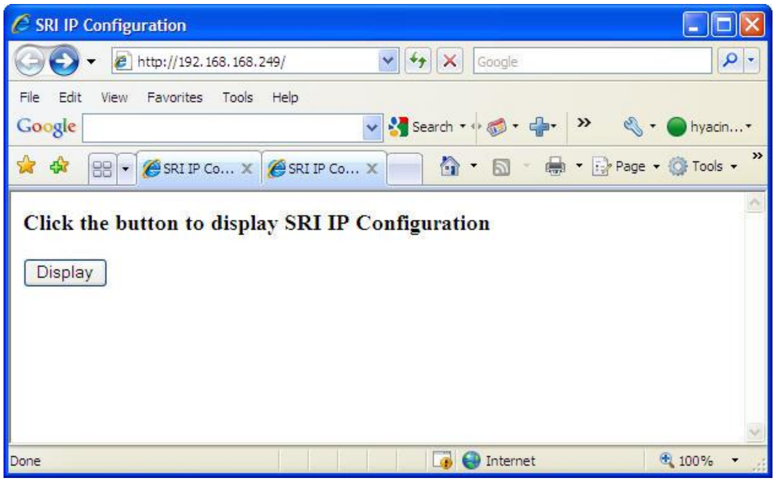
i) Enter 192.168.168.200 into the **IP address** field.

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 the default VSRC IP address (Default IP address is 192.168.168.249).

3 Open a web browser.

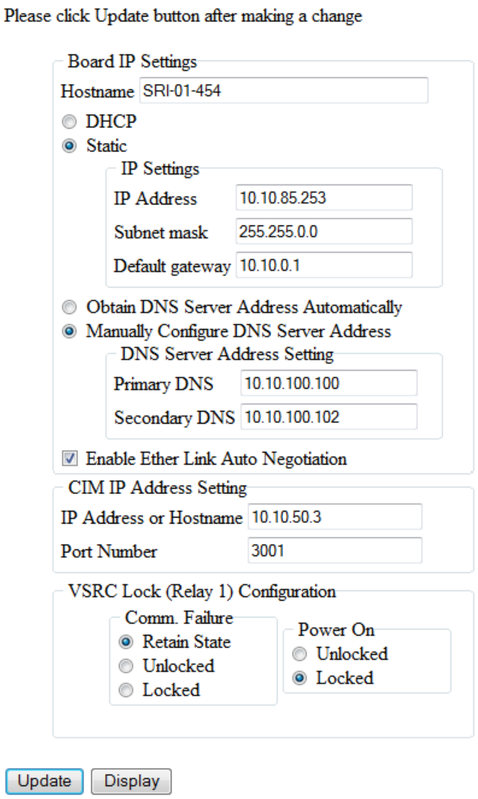
4 Go to http://192.168.168.249 -- the **IP Configuration** window will open.



Click the button to display SRI IP Configuration

Display

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



Please click Update button after making a change

Board IP Settings

Hostname SRI-01-454

○ DHCP

● Static

IP Settings

IP Address 10.10.85.253

Subnet mask 255.255.0.0

Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically

● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100

Secondary DNS 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname 10.10.50.3

Port Number 3001

VSRC Lock (Relay 1) Configuration

Comm. Failure

● Retain State

○ Unlocked

○ Locked

Power On

○ Unlocked

● Locked

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 (Optional, for DNS configuration).

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 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or
- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

9 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered on this screen.

10 Click on the **Update** button. Make a note of the IP address or the Hostname as it will be used by SMS to communicate with the VSRC.

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

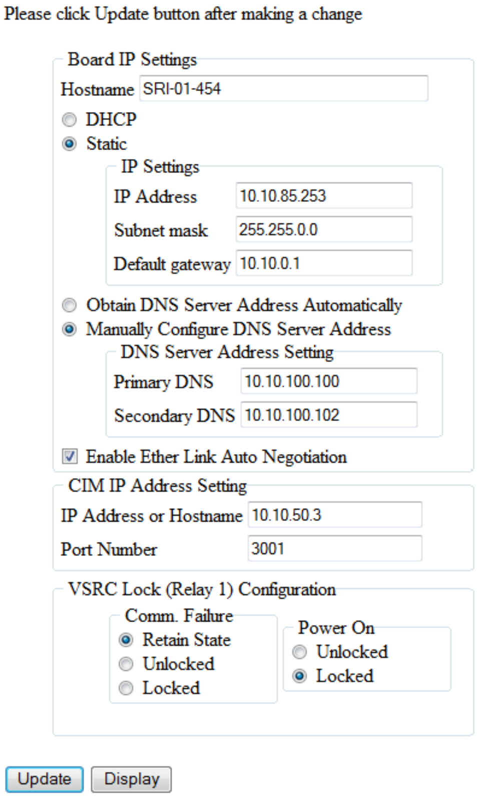
12 The IP address of the VSRC has been set.

DHCP Configuration

Configuring the VSRC to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

WARNING: If Controller IP addresses change, the system will not be aware of it until the DNS cache refreshes. Also, the CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may run incorrectly.

GUI (Graphic User Interface)



Please click Update button after making a change

Board IP Settings

Hostname: SRI-01-454

○ DHCP
● Static

IP Settings

IP Address: 10.10.85.253
Subnet mask: 255.255.0.0
Default gateway: 10.10.0.1

○ Obtain DNS Server Address Automatically
● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS: 10.10.100.100
Secondary DNS: 10.10.100.102

☑ Enable Ether Link Auto Negotiation

CIM IP Address Setting

IP Address or Hostname: 10.10.50.3
Port Number: 3001

VSRC Lock (Relay 1) Configuration

Comm. Failure
● Retain State
○ Unlocked
○ Locked

Power On
○ Unlocked
● Locked

Hostname - This displays the name of the specific VSRC. The name is in a standard format of SRI-02-XXX.

- SRI - Smart Reader Interface
- 02 - The designation for an VSRC
- XXX - The serial number of the specific VSRC (in the above example the serial number is 210).

The Host Name is used to access and setup the VSRC 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 VSRC to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes there will be a loss of controller communications until the new IP address is recognized by the CIM.

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

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VSRC'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 VSRC'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.

DNS Server Address Setting

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

Enable Ether Link Auto Negotiation - The VSRC 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. Enable this option to allow the VSRC to automatically detect and use the communication speed of the switch to which it is is connected.

Note: This option is not available on older model VSRCs. If this option does not show in the GUI then the VSRC will only communicate at 10Base-T.

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS the Fully Qualified Domain Name (FQDN) of the CIM should be entered here.
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definition matches the port entered on this screen.

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

Note: Whether the lock connected to the VSRC 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.

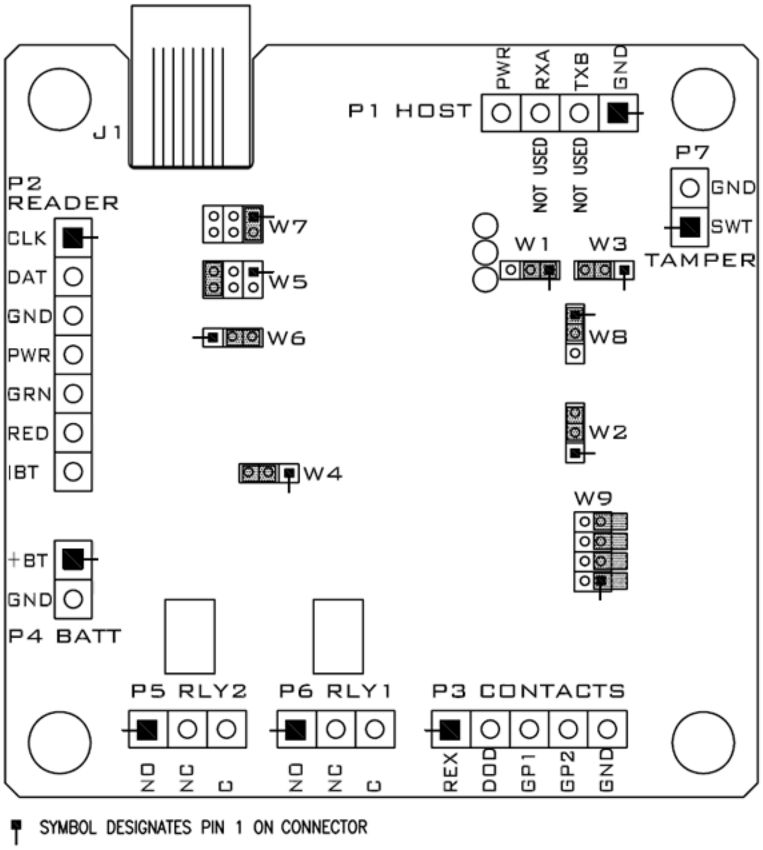
- **Comm Failure** - Choose one of the options to define the behaviour of Relay 1 in the event of communication failure. Once communication is returned Relay 1 will resume its Normal Operation state.
    - **Retain State** - The lock will stay in whatever state it was in (activated or deactivated) when 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.

Example: VSRC Lock (Relay 1) Configuration - Comm. Failure During MRO = Unlock

```
  Unlock Command (MRO) sent to VSRC:
        Green LED Activated
        Relay 1 Activated
        DOD Shunted
  Communications Failure to VSRC:
        Previous MRO Cleared
                  Cancel Reader Toggle
        Set Lock Based on Comm. Failure During MRO Setting (e.g. Unlock)
                  Energize Relay 1
                  Energize Green LED
  Communications Restored to VSRC:
        Restore Normal Operation
                  Reset Relay 1
                  Reset Reader
```

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

VSRC Pin Layout



VSRC Pin Functions

P1 - Power source wiring. This is where the VSRC receives power.

- Pin 1 is Ground
- Pin 2 is not used
- Pin 3 is not used
- Pin 4 is Power

P3 - Contact Inputs. The VSRC has four supervised or 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)
- Pin 2 is Door Position Switch (DOD)
- Pin 3 is Push Button Override
- Pin 4 is Auxiliary Input (If the IPB function is in use then Pin 4 is for the IPB)
- Pin 5 is Ground

P5/P6 - Relay outputs. The VSRC comes with two relay outputs.

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

P7 - Tamper switch. This is where a tamper switch is connected to the VSRC.

- Pin 1 (GND) is Ground
- Pin 2 (SWT) - Normally Closed

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

- A jumper across Pins 2 and 3 will provide 12VDC (Default Setting)
- A jumper across Pins 1 and 2 will 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 communication.

- 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 VSRC 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 in a standard VSRC configuration.
- Pins 7 & 8 - Not used in a standard VSRC configuration.

Warning: After installation it is recommended that Pins 1 & 2 be disabled. Leaving them enabled could allow unauthorized access to the VSRC.

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

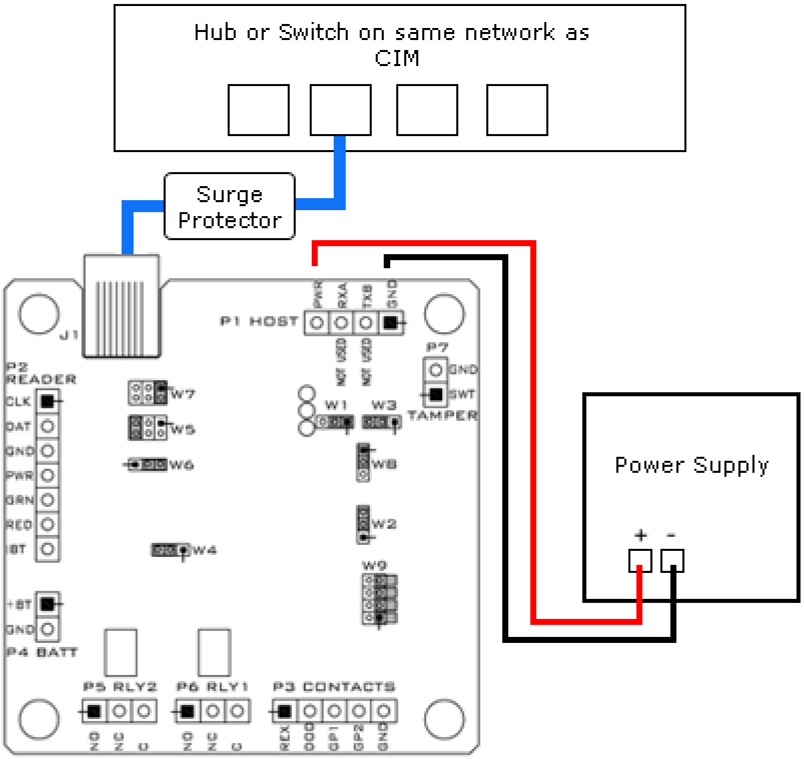
Pins Not Used

The below pins are not used on the VSRC:

- P4

Connecting to CIM

There is no direct connection between the VSRC and the CIM. To connect, they need to be on the same network and the proper IP address of the VSRC needs to be entered when setting up the VSRC in SMS. In addition, a data surge protector needs to be installed between the VSRC 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 VSRC.



Data Communication between CIM and VSRC

CIM	VSRC	Power Supply
Ethernet To Network	Ethernet to Network	
	Pin 1 - PWR (Power)	+ (Power)
	Pin 4 - GND (Ground)	- (Ground)

Connecting to Read Head

The VSRC 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.

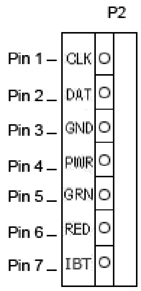
Recommended Wire Chart: VSRC to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VSRC to Magstripe Reader Head	500	18 AWG/5 Cond, Strd, Shld
VSRC to Proximity Reader Head	500	18 AWG/5 Cond, Strd, Shld
VSRC to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VSRC to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

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

P2 - VSRC pin connections



Proximity Reader

Proximity Read Head Pin Connections

VSRC	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

Wiegand Reader

Wiegand Read Head Pin Connections

VSRC	Wiegand 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 (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (IBT)	NOT USED

Magnetic Stripe Reader

Magnetic Stripe Read Head Pin Connections

VSRC	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

VMR - 5 Magnetic Stripe - LED 1 wire configuration

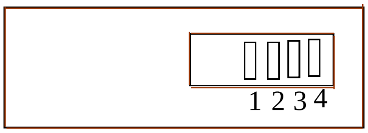
VMR - 5 Magnetic Stripe - LED 1 Pin Connections

VSRC	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (IBT)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off



VMR - 5 Magnetic Stripe - LED 2 wire configuration

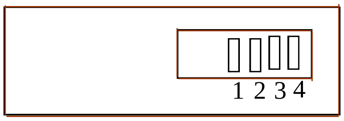
VMR - 5 Magnetic Stripe - -LED 2 Pin Connections

VSRC	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (IBT)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = Off S4 = Off



VMR-10 and VMR-20 Magnetic Stripe

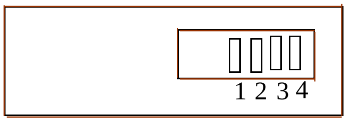
VMR-10 and VMR-20 Magnetic Stripe Pin Connections

VSRC	VMR-10 and VMR-20
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (IBT)	NOT USED

VMR-10 and VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On



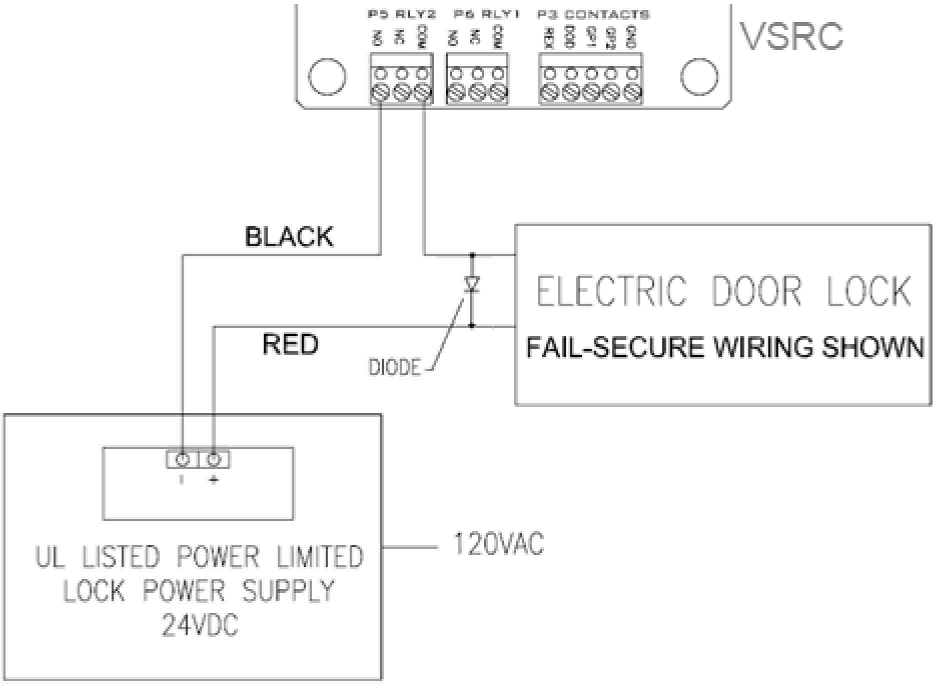
Touch Reader

Touch Reader Pin Connections

VSRC	Touch 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 (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (BUZ)	NOT USED

Installing Diode for Lock Wiring - Relay

A diode is supplied with the VSRC 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 is Fail Open*).

VSRC-300

Overview

The VSRC-300 is a software defined variant of the VSRC. It communicates with the CIM in the same manner as the VSRC but instead of connecting to one read-head, the VSRC-300 connects to Schlage AD-300 Series locks. Up to 8 AD-300 locks can be connected in series and then connected to the VSRC-300, allowing it to be the controller for up to 8 AD-300 locks.

VSRC-300 Pin Functions

Below are the PIN and Jumper values of the VSRC-300 that differ from the standard VSRC values.

P2 - Connection to AD-300 Series lock

- Pin 1 (CLK) - Data B
- Pin 2 (DAT) - Data A
- Pin 3 (GND) - Ground
- Pin 4 (PWR) - Power
- Pin 5 (GRN) - Not Used
- Pin 6 (RED) - Not Used
- Pin 7 (IBT) - Not Used

Note: All AD-300 locks connected to a VSRC-300 must be powered locally.

W5 - Sets communication protocol.

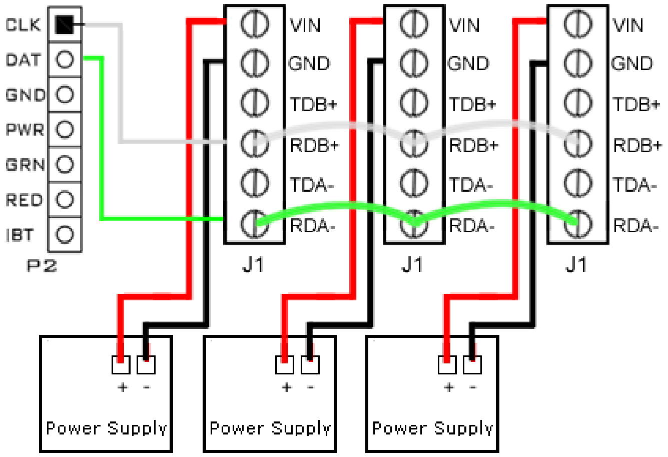
- Pins 3&4 - Need to be Jumpered together for the VSRC-300 to communicate with an AD-300 Series lock.

W7 - Sets communication protocol.

- Pins 3&4 - Need to be Jumpered together for the VSRC-300 to communicate with an AD-300 Series lock.

Note: All locks connected to an VSRC-300 will be on Channel 2 when configured in SMS.

Wiring between VSRC-300 and AD-300 Series



The above example shows an VSRC-300 connecting to three AD-300 locks. Up to eight AD-300 locks can be connected in series.

VSRC-300 -- AD-300 Series

VSRC-300 P2	AD-300 J1
Pin 1 (CLK) = Data B	RDB+
Pin2 (DAT) = Data A	RDA-

Jumper between (TA-RA-) and (TB+RB+)

VSRC - 400

Overview

The VSRC-400 is a software defined variant of the VSRC. It communicates with the CIM in the same manner as the VSRC but instead of connecting to one read-head, the VSRC-400 connects to the Schlage PIM400-485-SMS. The PIM400-485-SMS then connects wirelessly to up to 16 Schlage AD-400 Wireless locks. This allows the VSRC-400 to be the controller for up to 16 wireless locks.

VSRC-400 Pin Functions

Below are the PIN and Jumper values of the VSRC-400 that differ from the standard VSRC values.

P2 - Connection to PIM400-485-SMS

- Pin 1 (CLK) - Data B
- Pin 2 (DAT) - Data A
- Pin 3 (GND) - Ground
- Pin 4 (PWR) - Power
- Pin 5 (GRN) - Not Used
- Pin 6 (RED) - Not Used
- Pin 7 (IBT) - Not Used

Note: It is recommended that the PIM be powered locally.

W5 - Sets communication protocol.

- Pins 3 & 4 - Need to be Jumpered together for the VSRC-400 to communicate with the PIM400.

W7 - Sets communication protocol.

- Pins 3 & 4 - Need to be Jumpered together for the VSRC-400 to communicate with the PIM400.

Note: All locks connected to an VSRC-400 will be on Channel 2 when configured in SMS.

Wiring between VSRC-400 and PIM400-485-SMS

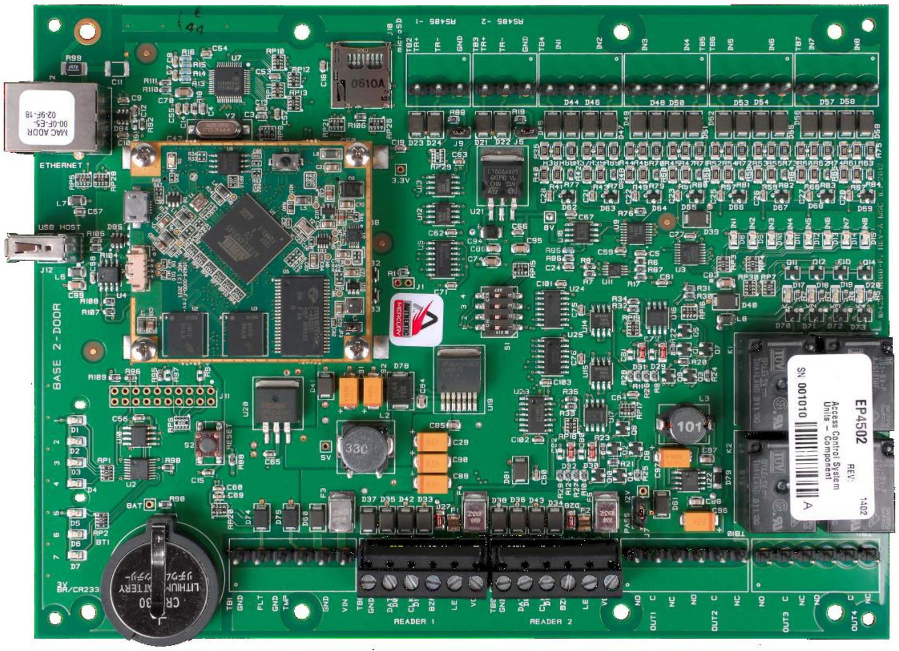
VSRC-400 -- PIM400-485-SMS

VSRC-400 P2	PIM400-485-SMS J5
Pin 1 (CLK) = Data B	TB+ jumpered to RB+
Pin 2 (DAT) = Data A	TA- jumpered to RA-

Jumper between (TA-RA-) and (TB+RB+)

CHAPTER 6

VSRC-M



Vanderbilt Mercury EP4502 based Dual Reader Controller (VSRC-M)

Overview

The Vanderbilt Dual Reader Controller (VSRC-M) is an intelligent device based on a Mercury EP4502 controller that can be paired with v6.2.0 and newer **Vanderbilt Security Management System** (SMS) Enterprise software installations. The VSRC-M contains 2 onboard Wiegand / Magstripe readers and associated relays and contacts. The VSRC-M is an independently programmable device capable of making decisions and storing history at the local level (*Enhanced Offline Mode*) if communication is lost.

VSRC-M Highlights

- Supports read head technologies utilizing Wiegand (D0/D1) or Magstripe (clock/data) signals.

  Proximity Cards

  - Standard 26-bit
  - Vanderbilt 34-bit
  - HID Corporate 1000 35-Bit
  - HID Corporate 1000 48-Bit

- HID/ProxIF 37-Bit
- XceedID 40-Bit
- XceedID 35-bit (including EV1)
- MiFare 32-Bit Serial Number (With HID read-head ONLY)

Magstripe Cards

- Geoffrey encoded magcard 14-D
- Geo-Image magcard 11-D
- Locknetic 18-D magcard

- Communicates via network protocol at 10/100 Base-T
- Powered locally by a 12VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power.
- Capable of running in *Enhanced Offline Mode*, allowing local decision making if communication fails between the VSRC-M and the network.

VSRC-M Standard Features

- Supports two read-head credentials
- Communicates with CIM via network protocol at 10/100 Base-T
- Connection for two multi-color LEDs for access granted or access denied indication
- Connector for two buzzer/annunciators
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc. *for each Read Head*
- Connector for tamper switch

VSRC-M Specifications

- Board Dimensions - 8"H x 6"W
- Enclosure Dimensions - 10"H x 12W" x 2-3/4" D
- Power requirements - 12VDC to 24VDC
- Power consumption - 200mA (500mA max. with read head)
- Ambient temperature - 0º to 49º C or 32º to 120º F

VSRC-M Enclosure

VSRC-M Enclosure Features

- Metal enclosure with hinged door, tamper switch, lock & key
- Enclosure Dimensions: 10" x 12" x 2-3/4"

VSRC-M Enclosure 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

VSRC-M Enclosure 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.

VSRC-M IP Configuration

The IP address of the VSRC-M has to be configured so that it can communicate with the CIM. Configuration should occur after the VSRC-M has been fully installed. Detailed instructions on how to configure the VSRC-M with a Static IP address are listed below. DHCP configuration, while not recommended by Vanderbilt, is also possible with DHCP reservations. Please review the DHCP Configuration section before configuration.

Note: Communication is at 10/100 Base-T

VSRC-M Static IP and DNS Configuration

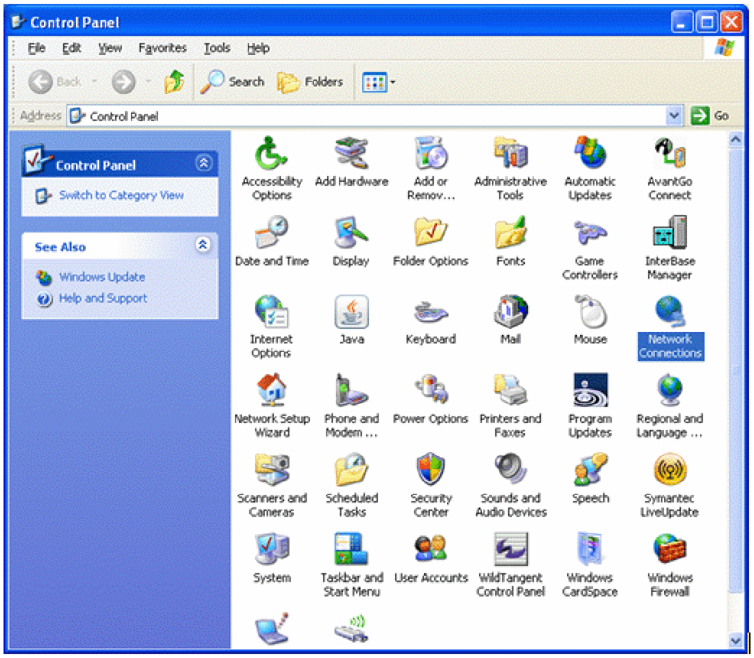
The VSRC-M is DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section before configuration DHCP.

Follow the steps below to configure the static IP of the VSRC-M.

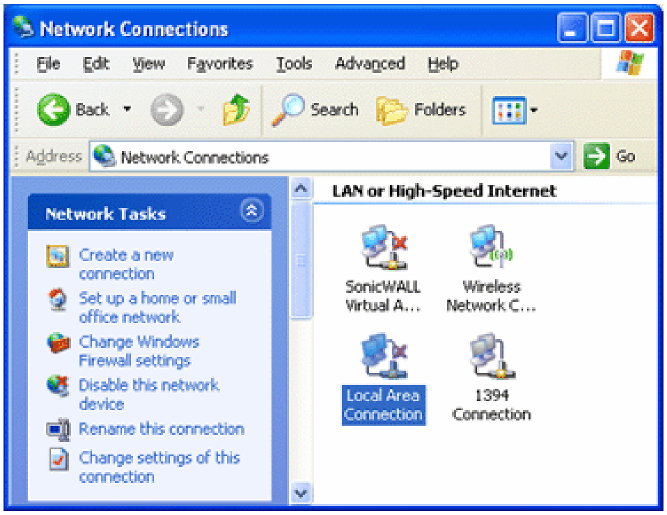
1. Connect a PC with a web browser to the VSRC-M.
   - Direct Connection - Using a cross-over cable, the reader interface can be connected directly to the network card of the PC.
   - Network Connection - Using a regular network cable, the reader interface can be connected to a hub or switch that is on the same network as the PC.
2. Configure the PC's network settings to communicate with the VSRC-M.

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

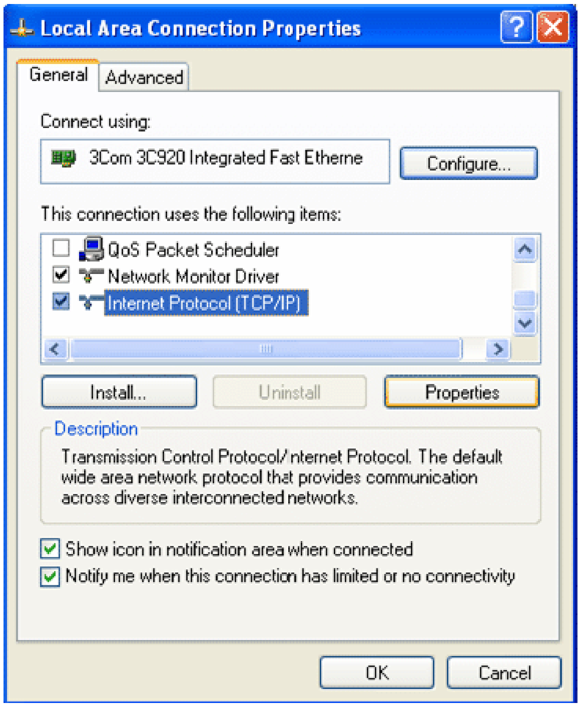
b) Click on **Control Panel**. The Control Panel window will open.



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


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Rename this connection
Change settings of this connection
LAN or High-Speed Internet
SonicWALL Virtual A...
Wireless Network C...
Local Area Connection
1394 Connection

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



Local Area Connection Properties

Connect using:

3Com 3C920 Integrated Fast Etherne

This connection uses the following items:

- □ QoS Packet Scheduler
- ☑ Network Monitor Driver
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

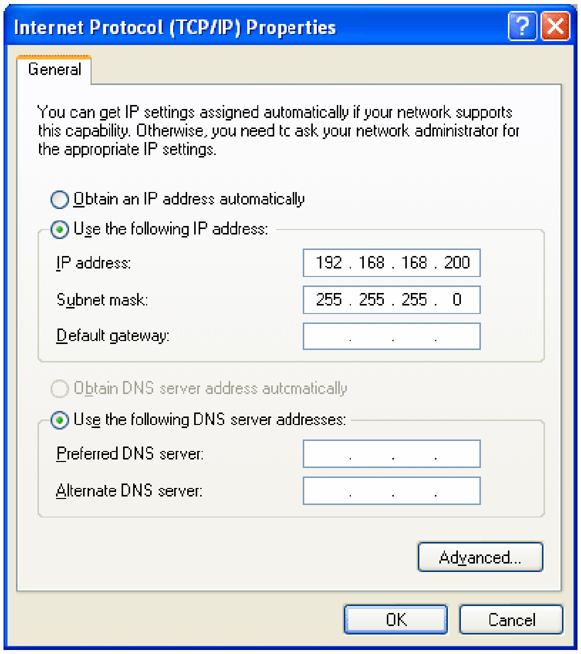
☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

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 VSRC-M configuration process to return the PC to its usual settings.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

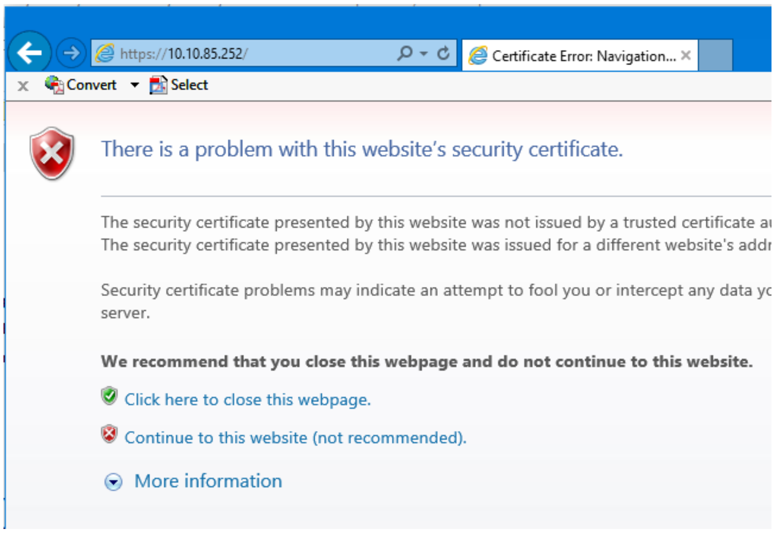
i) Enter 192.168.168.200 into the **IP address** field.

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 the default VSRC-M IP address (the Default IP address is 192.168.168.249).

3 Open a web browser.

4 Navigate to https://192.168.168.249 – the VSRC-M controllers use a self-signed certificate for SSL communications, so you may see the warning below. Click “Continue to this website” to access the controller login page.



There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate a
The security certificate presented by this website was issued for a different website's addr

Security certificate problems may indicate an attempt to fool you or intercept any data yc server.

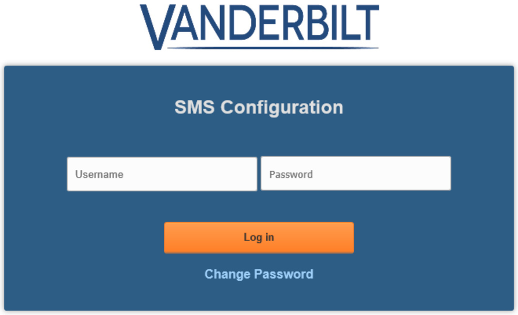
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

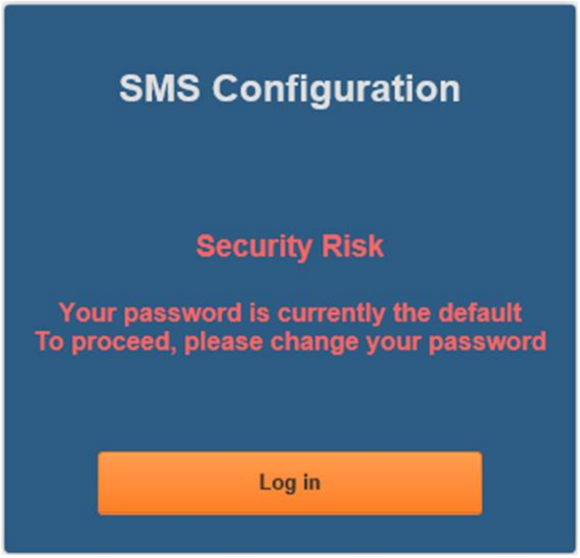
More information

5 Enter “SMSAdmin” for the user name and “SECAdmin1” for the password and click **Log in**.



a) The “SECAdmin1” password is only valid on the first login for after updating to FW v7.02M or new shipments from Vanderbilt after 7/8/2020.

b) On initial login the following message will be displayed:



SMS Configuration

Security Risk

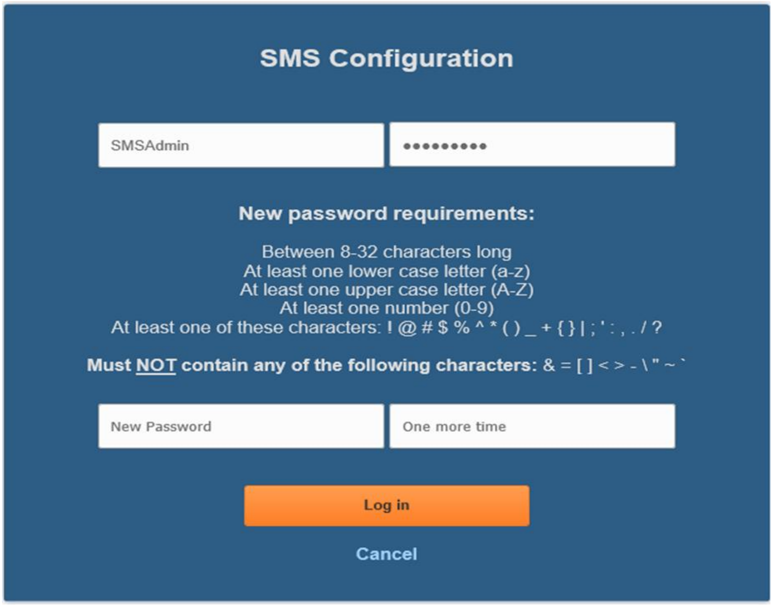
Your password is currently the default
To proceed, please change your password

c) You are required to enter a new, complex password.

d) Click **Log in** and provide the default credentials again.

e) Click **Change Password**.

f) Enter and confirm the new password at the dialog below.



SMS Configuration

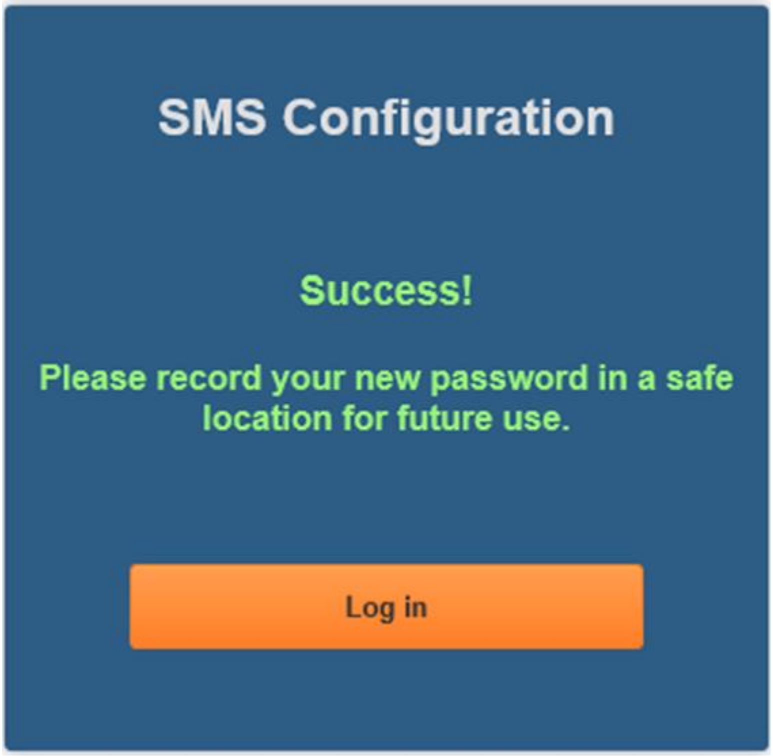
SMSAdmin ●●●●●●●●●

New password requirements:

Between 8-32 characters long
At least one lower case letter (a-z)
At least one upper case letter (A-Z)
At least one number (0-9)
At least one of these characters: ! @ # $ % ^ * ( ) _ + { } | ; ' : , . / ?

Must NOT contain any of the following characters: & = [ ] < > - \ " ~ `

g) Select **Log in** to continue.



SMS Configuration

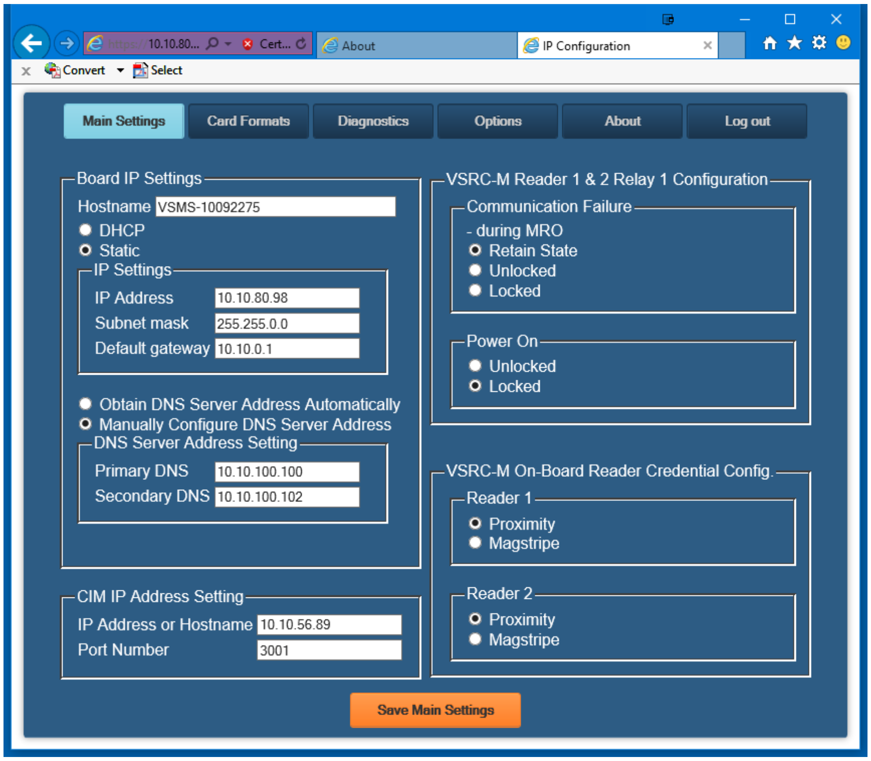
Success!

Please record your new password in a safe location for future use.

h) Select **Log in** again to continue after successful password reset.

Forgotten Password Recovery Will Require Contacting Vanderbilt Technical Support

6 The Main Settings screen will display.



Board IP Settings

Hostname VSMS-10092275

○ DHCP

● Static

IP Settings

IP Address 10.10.80.98

Subnet mask 255.255.0.0

Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically

● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100

Secondary DNS 10.10.100.102

CIM IP Address Setting

IP Address or Hostname 10.10.56.89

Port Number 3001

VSRC-M Reader 1 & 2 Relay 1 Configuration

Communication Failure

- during MRO

● Retain State

○ Unlocked

○ Locked

Power On

○ Unlocked

● Locked

VSRC-M On-Board Reader Credential Config.

Reader 1

● Proximity

○ Magstripe

Reader 2

● Proximity

○ Magstripe

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

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

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

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

8 Click on the **Manually configure DNS server addresses** button (Optional, for DNS configuration).

l) 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.

m) 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.

9 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or

- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

10 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered in this screen.

11 Click **Save Main Settings**. Make a note of the IP address as it will be used by SMS to communicate with the VSRC-M.

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

13 The IP address of the VSRC-M has been set.

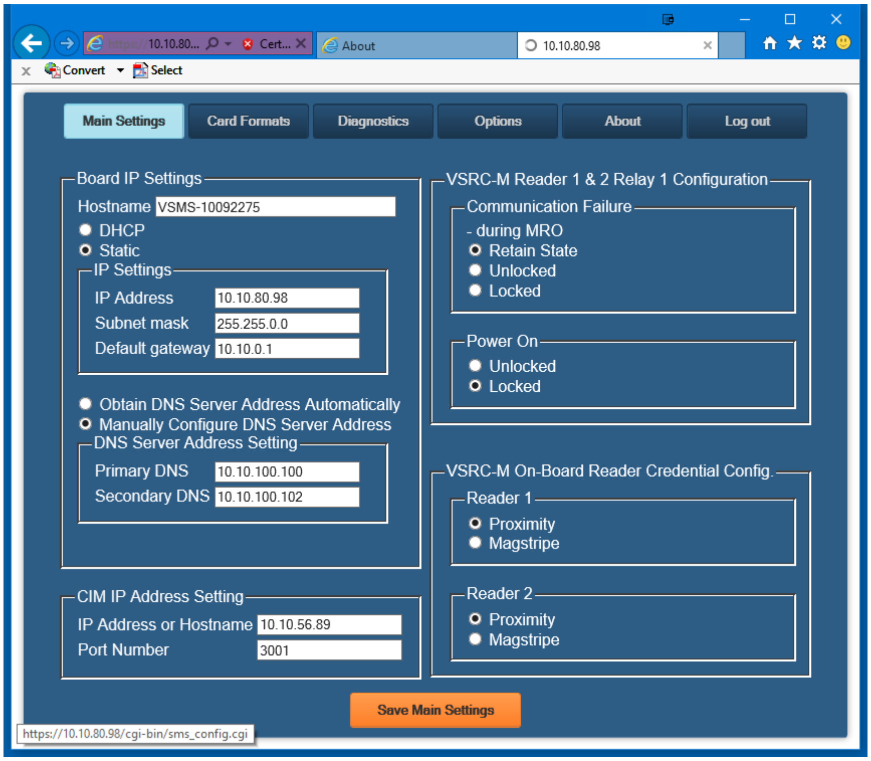
VSRC-M DHCP Configuration

Configuring the VSRC-M to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

WARNING: If Controller IP address changes, the system will not be aware of it until the DNS cache refreshes. The CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may not operate correctly.

VSRC-M GUI (Graphical User Interface)

Main Settings



Board IP Settings

Hostname VSMS-10092275

○ DHCP
● Static

IP Settings

IP Address 10.10.80.98
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 10.10.100.100
Secondary DNS 10.10.100.102

CIM IP Address Setting

IP Address or Hostname 10.10.56.89
Port Number 3001

VSRC-M Reader 1 & 2 Relay 1 Configuration

Communication Failure
- during MRO
● Retain State
○ Unlocked
○ Locked

Power On
○ Unlocked
● Locked

VSRC-M On-Board Reader Credential Config.

Reader 1
● Proximity
○ Magstripe

Reader 2
● Proximity
○ Magstripe

Hostname - This displays the name of the specific VSRC-M. The name is in a standard format of VSMS-XXXXXXXX.

- VSMS - Mercury EP4502 Based Reader Controller
- XXXXXXXX - The serial number of the specific VSRC-M (in the above example the serial number is 10092275).

The Host Name is used to access and setup the VSRC-M 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 VRCNX-M to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes, there will be a loss of controller communications until the new IP address is recognized by the CIM.

Static - This setting forces the VRCNX-M to use a static IP address.

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VRCNX-M'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 VRCNX-M'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.

DNS Server Address Setting

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

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS the Fully Qualified Domain Name (FQDN) of the CIM should be entered here
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definitions match the port entered on this screen.

VSRC Reader 1 & 2 Relay 1 Configuration - This section is used to define the state of Relay 1 associated with each VSRC-M reader in case of network communication failure during MRO Override state or power restored without network communications restoration.

Note: Whether the lock connected to the VSRC 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 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.

Example: VSRC Lock (Relay 1) Configuration - Comm. Failure During MRO = Unlock

Unlock Command (MRO) sent to VSRC:

Green LED Activated

Relay 1 Activated

DOD Shunted

Communications Failure to VSRC:

Previous MRO Cleared

Cancel Reader Toggle

Set Lock Based on Comm. Failure During MRO Setting (e.g. Unlock)

Energize Relay 1

Energize Green LED

Communications Restored to VSRC:

Restore Normal Operation

Reset Relay 1

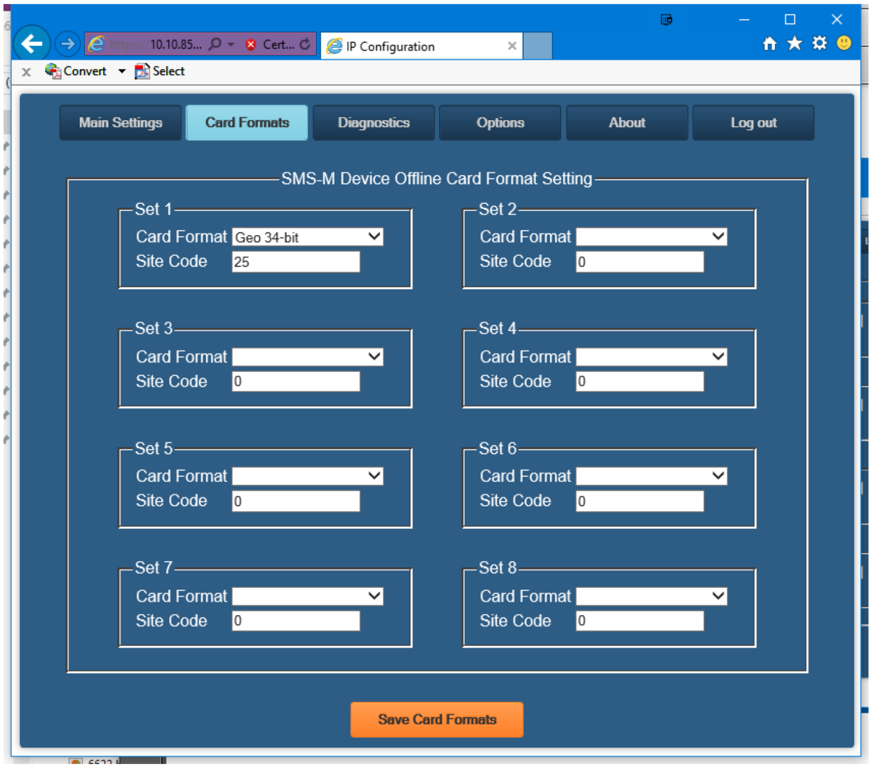
Reset Reader

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

VSRC-M On-Board Reader Credential Configuration - Two on-board Reader Interfaces can be configured on the VSRC-M. Use the settings below to specify the Credential Technology for each on-board Reader Interface.

- **Reader 1** - Choose the Credential Technology
  - Proximity
  - Magstripe
- **Reader 2** - Choose the Credential Technology
  - Proximity
- Magstripe

Card Formats



SMS-M Device Offline Card Format Setting

Set 1
Card Format Geo 34-bit
Site Code 25

Set 2
Card Format
Site Code 0

Set 3
Card Format
Site Code 0

Set 4
Card Format
Site Code 0

Set 5
Card Format
Site Code 0

Set 6
Card Format
Site Code 0

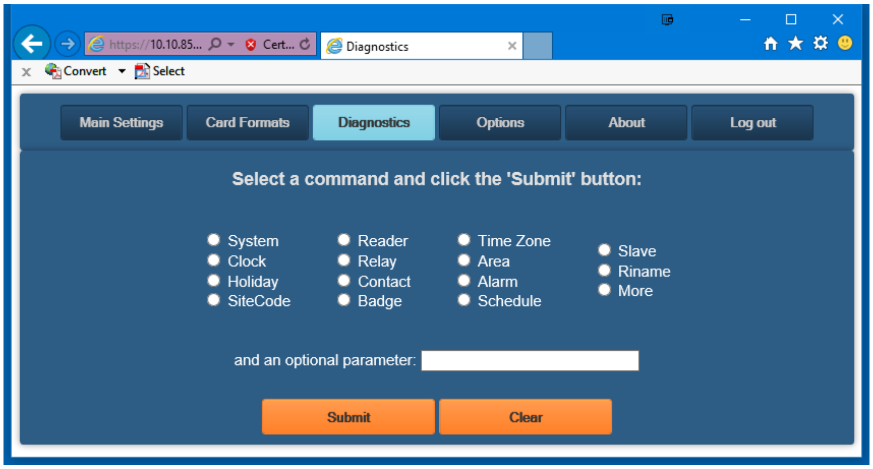
Set 7
Card Format
Site Code 0

Set 8
Card Format
Site Code 0

Set 1 – Set 8

Use this page to configure up to 8 Card Formats and Site Codes that will be active during Degraded Mode (the VSRC-M has lost communication to the CIM and is loading the Enhanced Offline Access database from the last CIM connection).

Diagnostics



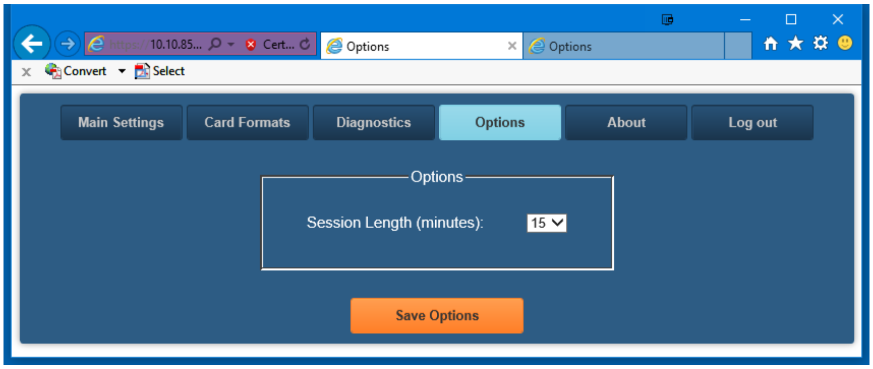
Select a command and click the 'Submit' button:

○ System ○ Reader ○ Time Zone ○ Slave
○ Clock ○ Relay ○ Area ○ Riname
○ Holiday ○ Contact ○ Alarm ○ More
○ SiteCode ○ Badge ○ Schedule

and an optional parameter:

Use this page to display additional detailed information regarding the VRCNX-M and data currently residing in memory. Use this page as directed by Vanderbilt Technical Support.

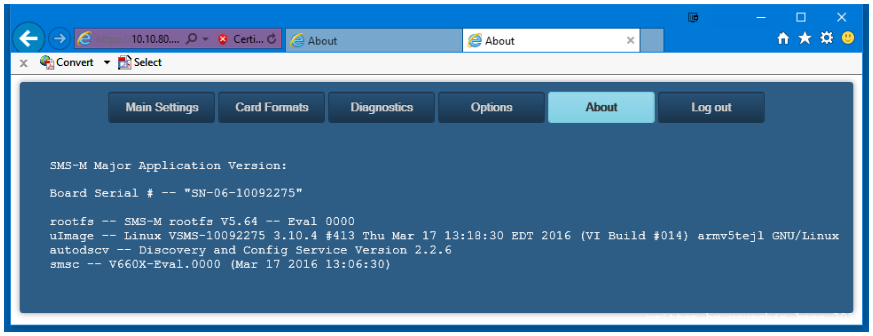
Options



Session Length (minutes): 15

Use to set the session inactivity timeout.

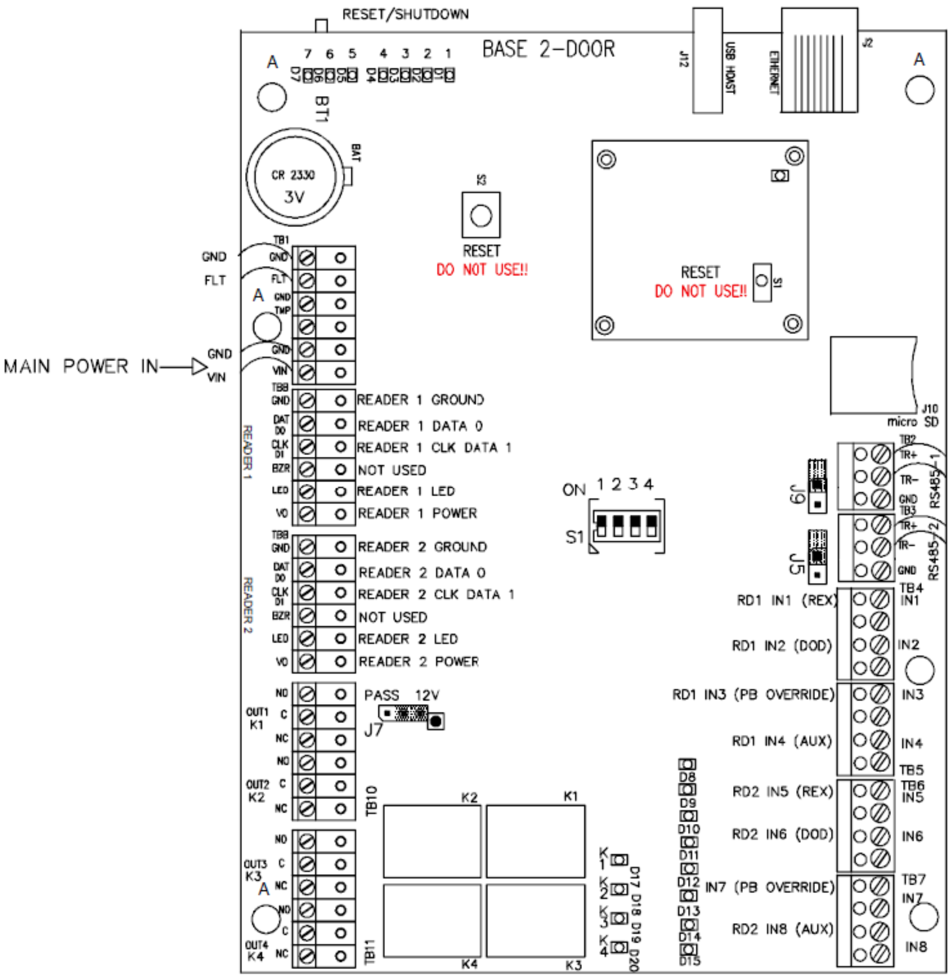
About



```
SMS-M Major Application Version:

Board Serial # -- "SN-06-10092275"

rootfs -- SMS-M rootfs V5.64 -- Eval 0000
uImage -- Linux VSMS-10092275 3.10.4 #413 Thu Mar 17 13:18:30 EDT 2016 (VI Build #014) armv5tejl GNU/Linux
autodscv -- Discovery and Config Service Version 2.2.6
smsc -- V660X-Eval.0000 (Mar 17 2016 13:06:30)
```

This page displays detailed information regarding the firmware loaded on the controller

VSRC-M Pin Layout



Pin Functions

TB1 - Power input for the VSRC-M. 12VDC or 24VDC.

- GND (-) ' Shutdown / Restart
- FLT (+) ' Shutdown / Restart
- GND (-) ' Tamper
- TMP (+) ' Tamper
- GND is (-) ' VSRC-M Main Power
- VIN is (+) ' VSRC-M Main Power

RESET / SHUTDOWN - Hold for 5 - 9 seconds and release for Reboot.

Hold for 10 seconds for Power Down. Refer to LED Indicators.

J10 - micro SD connection for flash memory.

J12 - USB HOST (reserved for future use).

S1 - Used to disable network communications.

- Switch 1 - Enable/Disable: Onboard web server (Configuration GUI), Ping and Discovery protocol. Enabled by default. If OFF, the onboard web server (GUI), Ping and Discovery protocol are disabled. If disabled then the VSRC-M cannot be reached via the GUI, Ping or the Discovery and Configuration Tool.
- Switch 2 - Reserved for Future Use
- Switch 3 - Off
- Switch 4 - Off

J5 - RS485 Termination (default = Off)

J9 - RS485 Termination (default = Off)

J7 - PASS 12V = Reader Power Select

- Jumper PINs 2 & 3 = 12 V Available to Reader Ports (min 20 V in)
- Jumper PINs 1 & 2 = Input Power "Passed Through" to Reader Ports

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

S2 - RESET -- DO NOT USE.

JP3 [CPU Daughter Board] - DO NOT REMOVE.

J4 [CPU Daughter Board] - RS-232

S1 [CPU Daughter Board] - RESET -- DO NOT USE.

Never Depress the S2 RESET button on the main controller or S1 RESET button on the CPU daughter board.

These buttons will interrupt power to the VSRC-M without shutting down critical software processes and may render the VSRC-M inoperable.

READER 1 - Onboard Reader Interface (Wiegand / Magstripe)

GND	Ground
DAT D0	Data / Data 0
CLK D1	Clock / Data 1
BZR	Reader Buzzer
LED	Reader LED
VO	Reader Power

READER 2 - Onboard Reader Interface (Wiegand / Magstripe)

GND	Ground
DAT D0	Data / Data 0
CLK D1	Clock / Data 1
BZR	Reader Buzzer
LED	Reader LED
VO	Reader Power

OUT 1 - Relay Output 1 for Reader 1

NO	Normally Open
C	Common
NC	Normally Closed

OUT 2 - Relay Output 2 for Reader 1

NO	Normally Open
C	Common
NC	Normally Closed

OUT 3 - Relay Output 1 for Reader 2

NO	Normally Open
C	Common
NC	Normally Closed

OUT 4 - Relay Output 2 for Reader 2

NO	Normally Open
C	Common
NC	Normally Closed

IN 1 - Contact Input 1 for Reader 1

- 2 wires used for Request to Exit (REX)

IN 2 - Contact Input 2 for Reader 1

- 2 wires used for Door Open Detect (DOD)

IN 3 - Contact Input 3 for Reader 1

- 2 wires used for Push Button Override

IN 4 - Contact Input 4 for Reader 1

- 2 wires used for Auxiliary Input

IN 5 - Contact Input 1 for Reader 2

- 2 wires used for Request to Exit (REX)

IN 6 - Contact Input 2 for Reader 2

- 2 wires used for Door Open Detect (DOD)

IN 7 - Contact Input 3 for Reader 2

- 2 wires used for Push Button Override

IN 8 - Contact Input 4 for Reader 2

- 2 wires used for Auxiliary Input

ETHERNET - Ethernet cable to network connects here.

> **Warning:** Vanderbilt recommends Setting S1-Switch 1 OFF to DISABLE the onboard web server, ping, and discovery protocol after installation and configuration. Leaving these features enabled could allow unauthorized access to the VSRC-M.

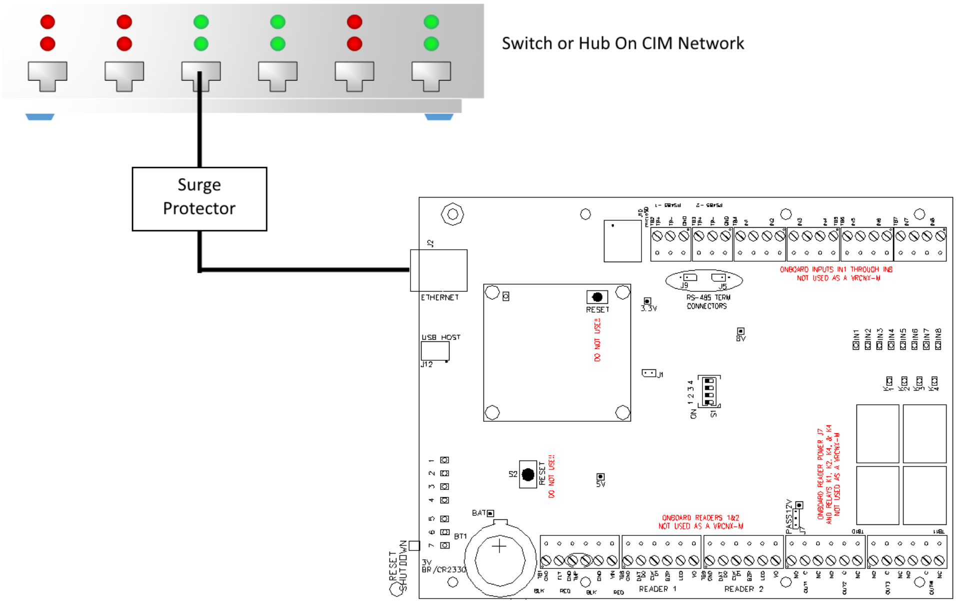
Pins Left at Default

The below pins should be left at their default settings:

- J9 - Used for RS485 Channel 2 termination (Reader Interface Termination).
  Default: PINs 1 & 2 Jumper Removed.
- J5 - Used for RS485 Channel 3 termination (Reader Interface Termination).
  Default: PINs 1 & 2 Jumper Removed.

Connecting VSRC-M to CIM

There is no direct connection between the VSRC-M and the CIM. To connect, they need to be on the same network and the proper IP address of the VSRC-M needs to be entered when setting up the VSRC-M in SMS. In addition, a data surge protector needs to be installed between the VSRC-M 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 TB1 on the VSRC-M.


Switch or Hub On CIM Network
Surge Protector
ETHERNET
USB HOST
J12
RESET
DO NOT USE!!
RS-485 TERM CONNECTORS
ONBOARD INPUTS IN1 THROUGH IN8 NOT USED AS A VRCNX-M
ONBOARD READER POWER J7 AND RELAYS K1, K2, K4, & K4 NOT USED AS A VRCNX-M
ONBOARD READERS 1&2 NOT USED AS A VRCNX-M
READER 1
READER 2
RESET SHUTDOWN
3V BR/CR2330
BT1
BAT
S2
S1
ON
PASS12V
3.3V
5V
8V

Data Communication between CIM and VSRC-M

CIM	VSRC-M
Ethernet To Network	Ethernet to Network

Connecting to Read Heads

The following sections how to install various credential read heads to the VSRC-M reader interfaces.

The VSRC-M 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.

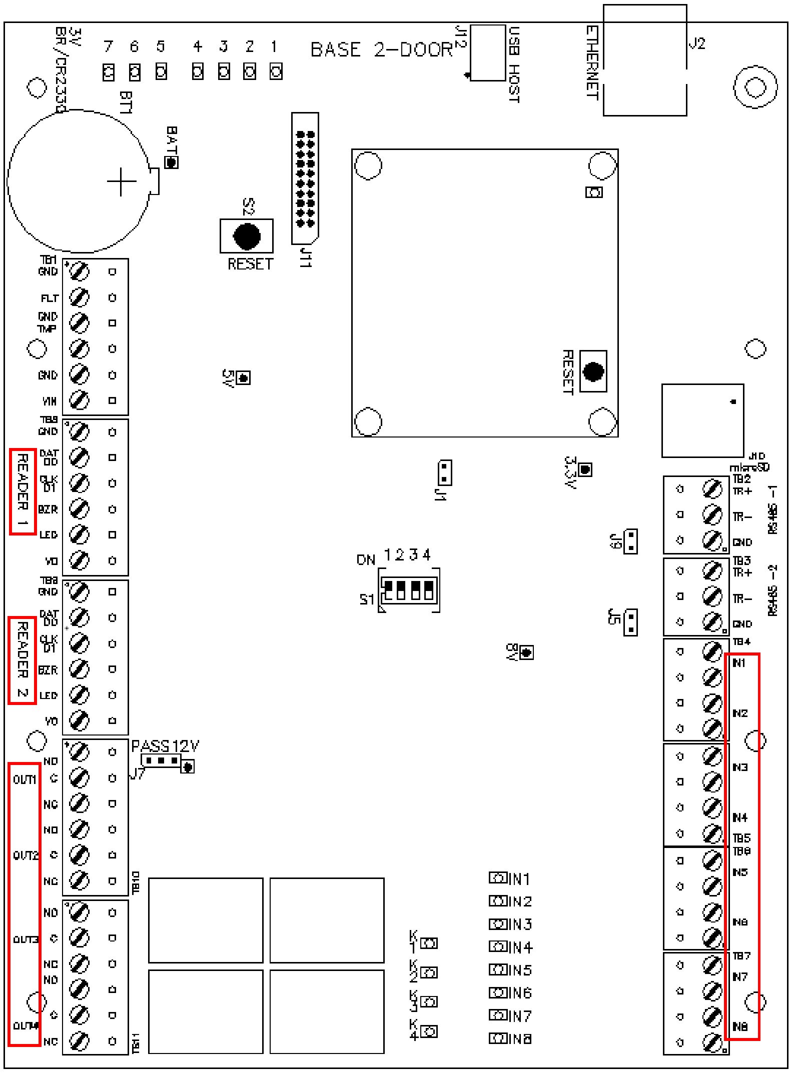
Recommended Wire Chart: VSRC-M to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VSRC-M to Magstripe Reader Head	200	18 AWG/5 Cond, Strd, Shld
VSRC-M to Proximity Reader Head	500	18 AWG/5 Cond, Strd, Shld
VSRC-M to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VSRC-M to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

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

VSRC-M RI Pin Connections



Reader 1

Reader 1 can be used to connect 1 card-reader to the VSRC-M:

- Pin 1 is Ground (GND)
- Pin 2 is DAT/D0 (Data 0)
- Pin 3 is CLK/D1 (Data 1)
- Pin 4 is Buzzer (14-24V)
- Pin 5 is LED
- Pin 6 is Power (V0)

Reader 1 has four contact points at TB4 - IN1 and TB4 - IN2 and TB5- IN3 and TB5 - IN4. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

Reader 1 has two relay outputs at TB10 - OUT1 and TB10 - OUT2. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. OUT1 is for the Door Unlock relay. OUT2 is for the Door Held Open relay.

Reader 2

Reader 2 can be used to connect 1 card-reader to the VSRC-M.

- Pin 1 is Ground (GND)
- Pin 2 is DAT/D0 (Data 0)
- Pin 3 is CLK/D1 (Data 1)
- Pin 4 is Buzzer (14-24V)
- Pin 5 is LED
- Pin 6 is Power (V0)

Reader 2 has four contact points at TB6 - IN5 and TB6 - IN6 and TB7- IN7 and TB7 - IN8. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

Reader 2 has two relay outputs at TB11 - OUT3 and TB11 - OUT4. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. OUT3 is for the Door Unlock relay. OUT4 is for the Door Held Open relay.

J7 - Read head voltage selector. The read-head voltage selector provides pass-through or 12VDC to the various types of read-heads for both Reader 1 and Reader 2.

- No jumper will provide no power
- A jumper across Pass and the center Pin will pass-through VSRC-M main input voltage
- A jumper across the center Pin and 12V 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.

Proximity Reader

Wiegand / Proximity Read Head Pin Connections

VSRC-M	Proximity Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	BEEPER (YELLOW); 12-24V
PIN 5 (LED)	LED (ORANGE)
PIN 6 (PWR)	POWER (RED)

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

VSRC-M VMR-5 Magnetic Strip - LED 1 Wire Configuration

VMR - 5 Magnetic Stripe - LED 1 Pin Connections

VSRC-M	VMR-5
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	NOT USED
PIN 5 (LED)	LED (BROWN)
PIN 6 (PWR)	POWER (RED)

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off

VSRC-M VMR-10 and VMR-20 Magnetic Stripe

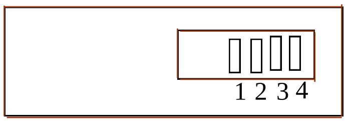
VMR-10 and VMR-20 Magnetic Stripe Pin Connections

VSRC-M	VMR-10 and VMR-20
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	NOT USED
PIN 5 (LED)	LED (BROWN)
PIN 6 (PWR)	POWER (RED)

VMR-10 and VMR-20 Switch Settings

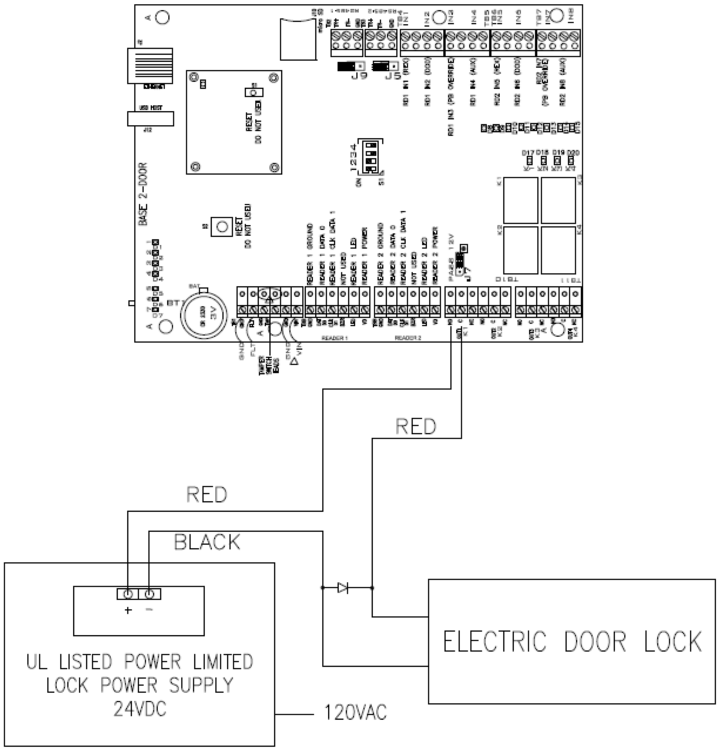
Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On



Installing Diodes for Lock Wiring - Relay

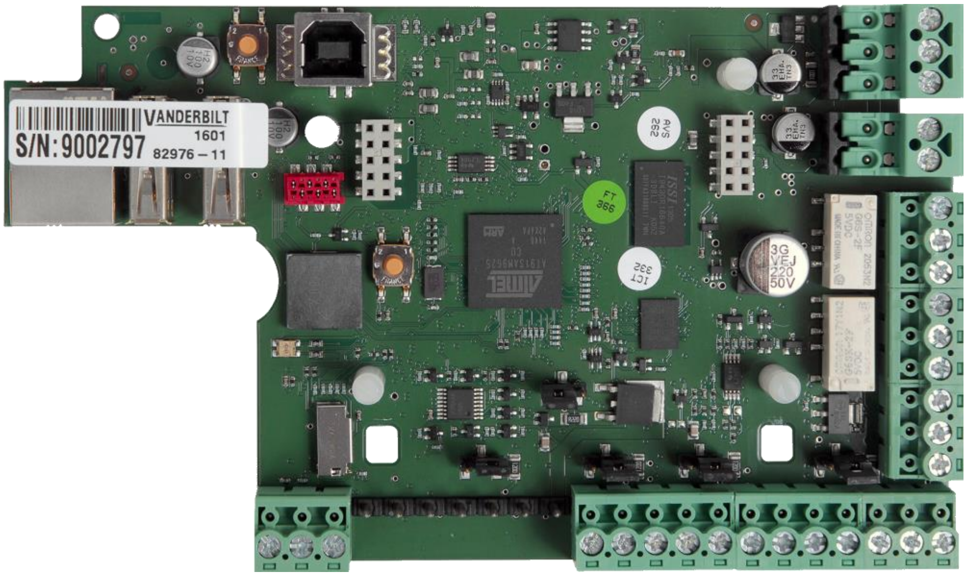
Diodes are supplied with the VSRC-M which should be fitted across 12V and COM on each Reader Interface to protect the relay contacts.



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 relay K1 and K3 NO or NC depending on lock type: Fail Open / Fail Closed (*the diagram above is Fail Open*).

CHAPTER 7

VSRC-A



Vanderbilt Dual Reader Controller (VSRC-A)

Overview

The Vanderbilt Dual Reader Controller (VSRC-A) is an intelligent device that can be paired with v6.4.5 and newer **Vanderbilt Security Management System** (SMS) Enterprise software installations. The VSRC-A contains 2 onboard Wiegand / Magstripe readers and associated relays and contacts. The VSRC-A is an independently programmable device capable of making decisions and storing history at the local level (*Enhanced Offline Mode*) if communication is lost.

VSRC-A Highlights

- Supports read head technologies utilizing Wiegand (D0/D1) or Magstripe (clock/data) signals.

Proximity Cards

- Standard 26-bit
- Vanderbilt 34-bit
- HID Corporate 1000 35-Bit
- HID Corporate 1000 48-Bit
- HID/ProxIF 37-Bit
- XceedID 40-Bit
- XceedID 35-bit (including EV1)

- MiFare 32-Bit Serial Number (With HID read-head ONLY)

Magstripe Cards

- Geoffrey encoded magcard 14-D
- Geo-Image magcard 11-D
- Locknetic 18-D magcard

- Communicates via network protocol at 10/100 Base-T
- Powered locally by a 12VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power.
- Capable of running in *Enhanced Offline Mode*, allowing local decision making if communication fails between the VSRC-A and the network.

VSRC-A Standard Features

- Supports two read-head credentials
- Communicates with CIM via network protocol at 10/100 Base-T
- Connection for two multi-color LEDs for access granted or access denied indication
- Connector for two buzzer/annunciators
- SMS software configuration as VSRC-A2 includes 2 input contacts for exit request (REX) and door position switch (DOD) *for each read head*
- Alternate SMS software configuration as VSRC-A1 includes 4 input contacts for exit request (REX), door position switch (DOD), exterior push button (EPB) and auxiliary input *for a single read dead*
- Connector for tamper switch

VSRC-A 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

VSRC-A Enclosure

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.

IP Configuration

The IP address of the VSRC-A has to be configured so that it can communicate with the CIM. Configuration should occur after the VSRC-A has been fully installed. Detailed instructions on how to configure the VSRC-A with a Static IP address are listed below. DHCP configuration, while not recommended by Vanderbilt, is also possible with DHCP reservations. Please review the DHCP Configuration section before configuration.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

The VSRC-A is DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section before configuration DHCP.

Follow the steps below to configure the static IP of the VSRC-A.

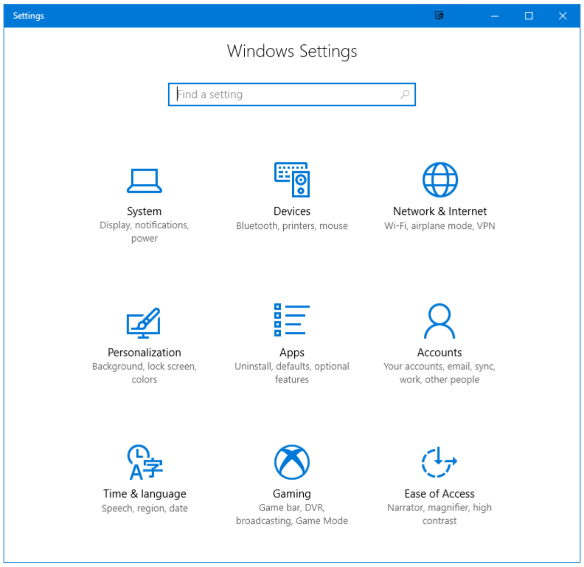
1 Connect a PC with a web browser to the VSRC-A.

- 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.

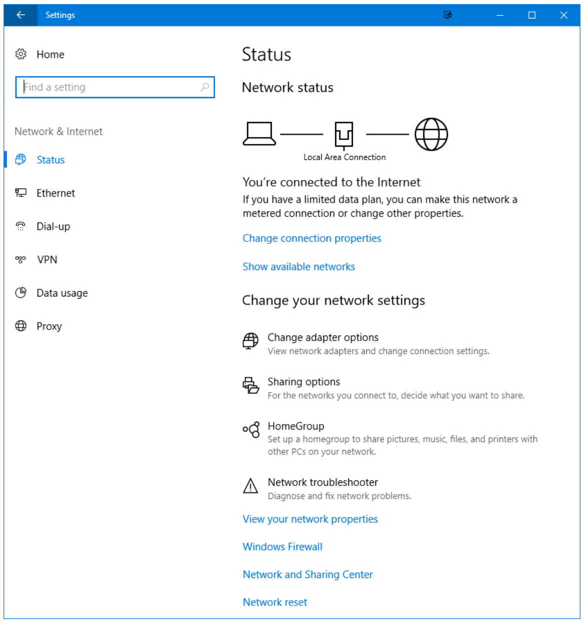
2 Configure the PC's network settings to communicate with the VSRC-A.

a) Click the **Start** button.

b) Click **Settings**.


Settings
Windows Settings
Find a setting
System
Display, notifications, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast

c) Click **Network & Internet**.



Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Data usage

Proxy

Status

Network status

Local Area Connection

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

HomeGroup
Set up a homegroup to share pictures, music, files, and printers with other PCs on your network.

Network troubleshooter
Diagnose and fix network problems.

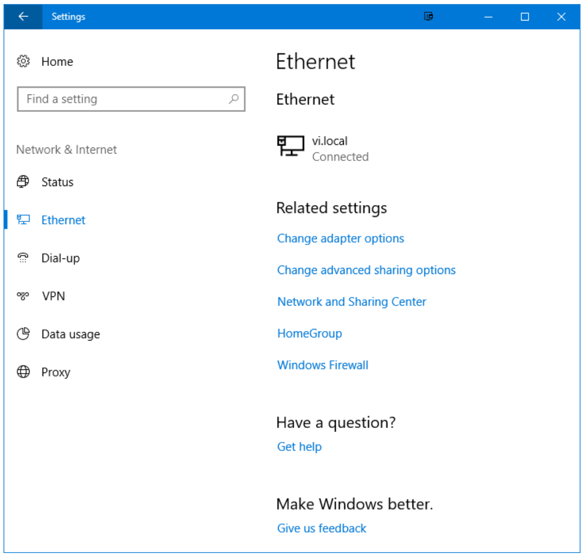
View your network properties

Windows Firewall

Network and Sharing Center

Network reset

d) Click **Ethernet**.



Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Data usage

Proxy

Ethernet

Ethernet

vi.local
Connected

Related settings

Change adapter options

Change advanced sharing options

Network and Sharing Center

HomeGroup

Windows Firewall

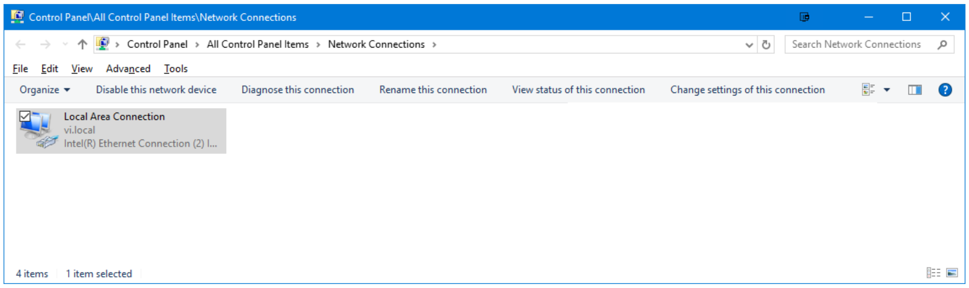
Have a question?

Get help

Make Windows better.

Give us feedback

e) Click **Change adapter options**



Control Panel\All Control Panel Items\Network Connections

Control Panel › All Control Panel Items › Network Connections ›

Search Network Connections

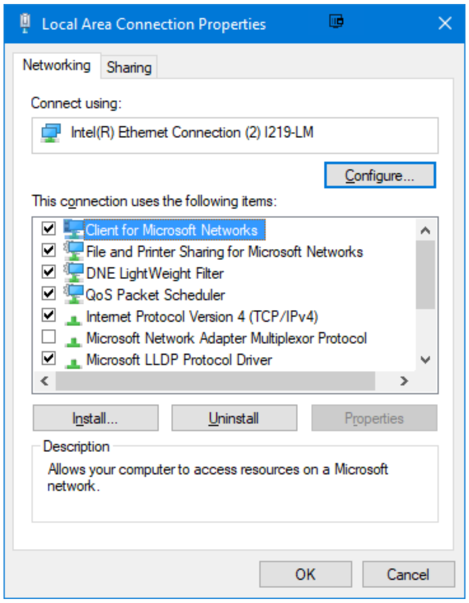
File Edit View Advanced Tools

Organize ▾ Disable this network device Diagnose this connection Rename this connection View status of this connection Change settings of this connection

☑ Local Area Connection
vi.local
Intel(R) Ethernet Connection (2) I...

4 items 1 item selected

f) Highlight the NIC connected to the VRCNX-A and click **Change settings of this connection**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) Ethernet Connection (2) I219-LM

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ DNE LightWeight Filter
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Install... | Uninstall | Properties

Description

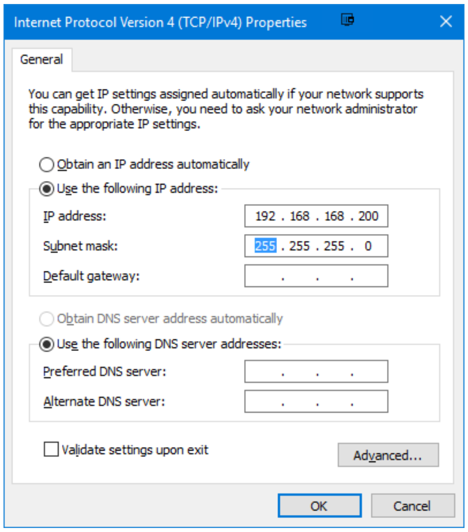
Allows your computer to access resources on a Microsoft network.

OK | Cancel

g) Scroll down and select **Internet Protocol (TCP/IP v4)**.

h) Click the **Properties** button.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 168 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK | Cancel

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

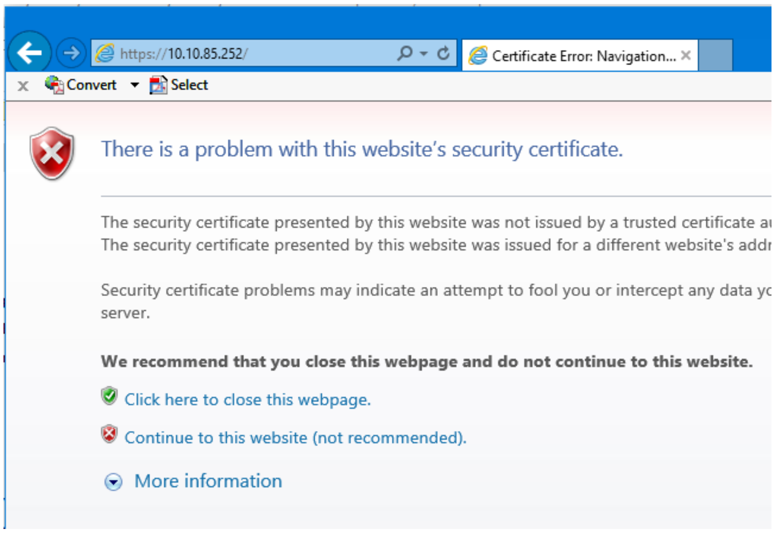
k) Enter 192.168.168.200 into the **IP address** field.

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

m) Click on the **OK** button. The window will close. The PC's network settings are now compatible with the default VSRC-A IP address (the Default IP address is 192.168.168.249).

3 Open a web browser.

4 Navigate to https://192.168.168.249 – the VSRC-A controllers use a self-signed certificate for SSL communications, so you may see the warning below. Click “Continue to this website” to access the controller login page.



There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate a
The security certificate presented by this website was issued for a different website's addr

Security certificate problems may indicate an attempt to fool you or intercept any data yo
server.

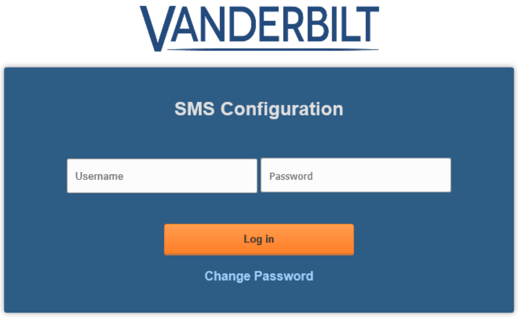
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

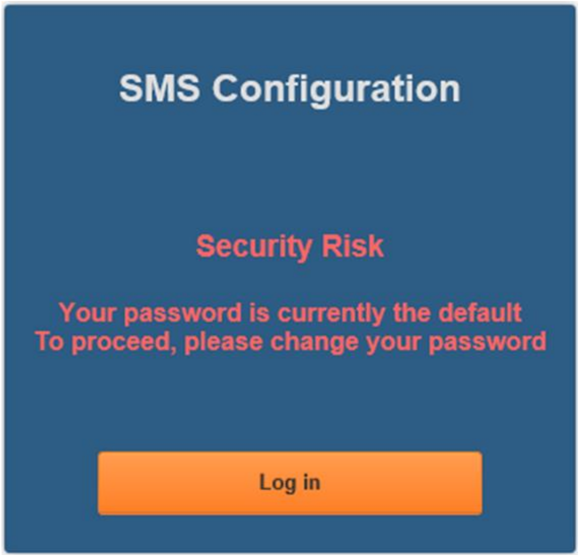
More information

5 Enter “SMSAdmin” for the user name and “SECAdmin1” for the password and click **Log in**.



a) The “SECAdmin1” password is only valid on the first login for after updating to FW v7.41A or new shipments from Vanderbilt after 7/8/2020.

b) On initial login the following message will be displayed:



SMS Configuration

Security Risk

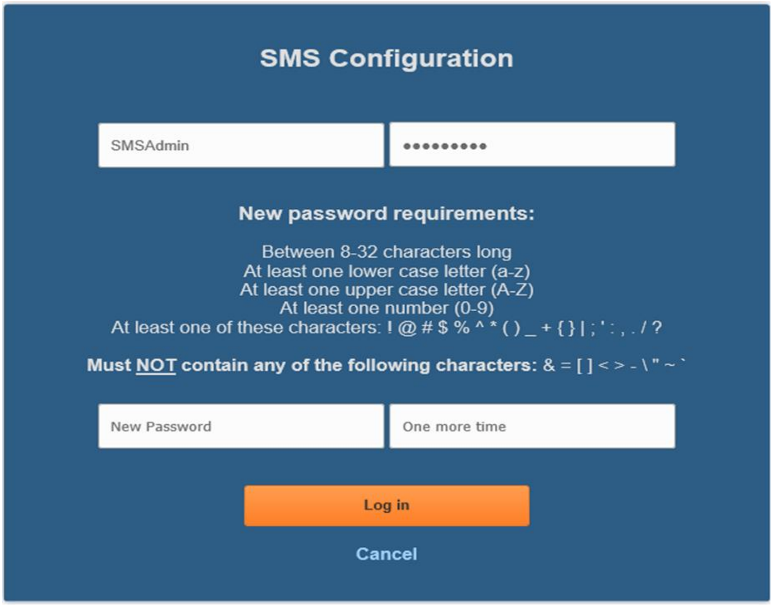
Your password is currently the default
To proceed, please change your password

c) You are required to enter a new, complex password.

d) Click **Log in** and provide the default credentials again.

e) Click **Change Password**.

f) Enter and confirm the new password at the dialog below.



SMS Configuration

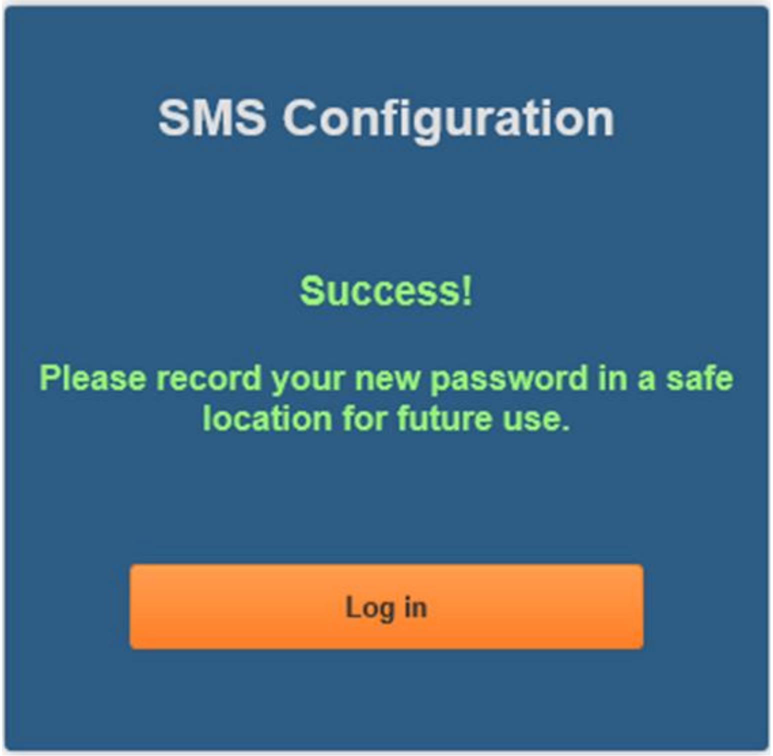
SMSAdmin ●●●●●●●●●●

New password requirements:

Between 8-32 characters long
At least one lower case letter (a-z)
At least one upper case letter (A-Z)
At least one number (0-9)
At least one of these characters: ! @ # $ % ^ * ( ) _ + { } | ; ' : , . / ?

Must NOT contain any of the following characters: & = [ ] < > - \ " ~ `

g) Select **Log in** to continue.



SMS Configuration

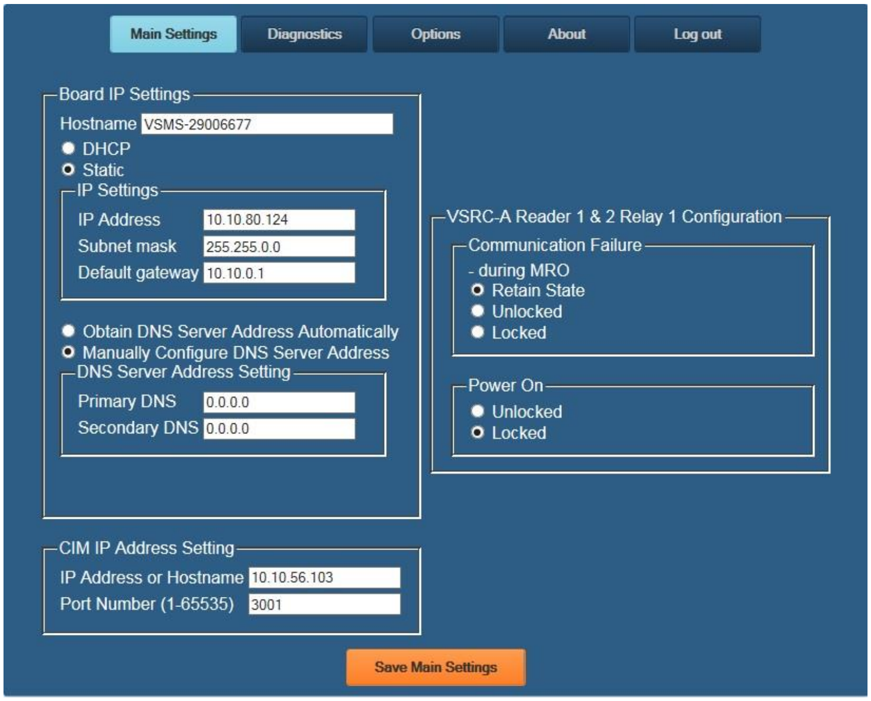
Success!

Please record your new password in a safe location for future use.

h) Select **Log in** again to continue after successful password reset.

Forgotten Password Recovery Will Require Contacting Vanderbilt Technical Support

6 The Main Settings screen will display.



Board IP Settings

Hostname VSMS-29006677

○ DHCP

● Static

IP Settings

IP Address 10.10.80.124

Subnet mask 255.255.0.0

Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically

● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 0.0.0.0

Secondary DNS 0.0.0.0

VSRC-A Reader 1 & 2 Relay 1 Configuration

Communication Failure

- during MRO

● Retain State

○ Unlocked

○ Locked

Power On

○ Unlocked

● Locked

CIM IP Address Setting

IP Address or Hostname 10.10.56.103

Port Number (1-65535) 3001

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

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

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

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

8 Click on the **Manually configure DNS server addresses** button (Optional, for DNS configuration).

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.

9 In the **CIM IP Address Setting** section at the IP Address or Hostname field either:

- Enter the IP address of the CIM
  or
- If using DNS, enter the Fully Qualified Domain Name (FQDN) of the CIM.

10 Enter the Port Number of the CIM into the **Port Number** field in the **CIM IP Address Setting** section. The number should be 3001 unless IT technicians specify otherwise. Verify that the controller definition matches the port entered in this screen.

11 Click **Save Main Settings**. Make a note of the IP address as it will be used by SMS to communicate with the VSRC-A.

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

13 The IP address of the VSRC-A has been set.

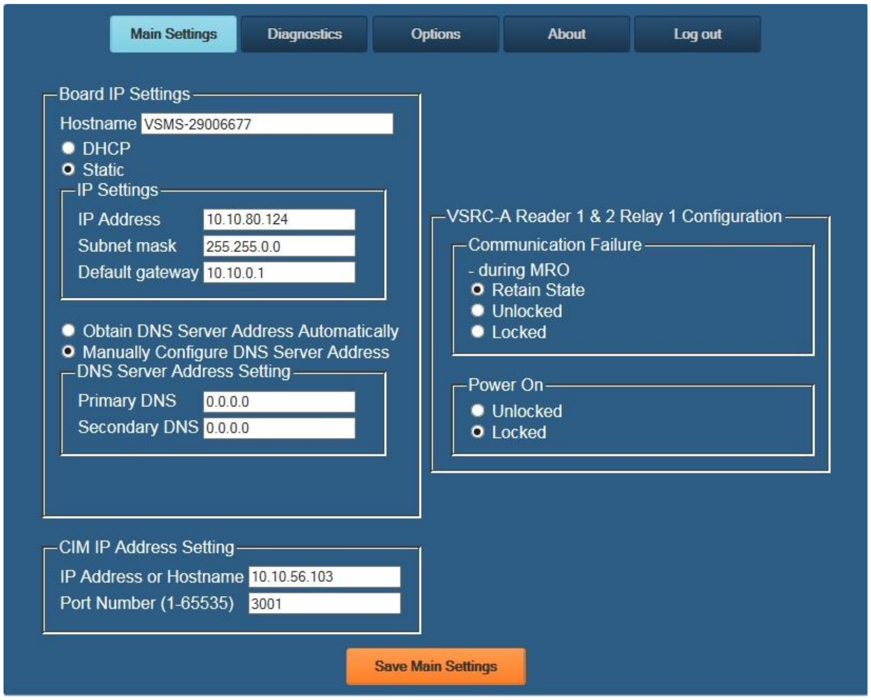
DHCP Configuration

Configuring the VSRC-A to DHCP is possible but the different methods required, depending on network architecture, are beyond the scope of this manual. Contact Technical Support for help with DHCP configuration.

> **WARNING:** If Controller IP address changes, the system will not be aware of it until the DNS cache refreshes. The CIM will need to be restarted in order for it to resolve the new IP address. During the time that the cache has not refreshed and the CIM has not been restarted, the system may not operate correctly.

GUI (Graphical User Interface)

Main Settings



Board IP Settings

Hostname VSMS-29006677

○ DHCP
● Static

IP Settings

IP Address 10.10.80.124
Subnet mask 255.255.0.0
Default gateway 10.10.0.1

○ Obtain DNS Server Address Automatically
● Manually Configure DNS Server Address

DNS Server Address Setting

Primary DNS 0.0.0.0
Secondary DNS 0.0.0.0

VSRC-A Reader 1 & 2 Relay 1 Configuration

Communication Failure

- during MRO
● Retain State
○ Unlocked
○ Locked

Power On

○ Unlocked
● Locked

CIM IP Address Setting

IP Address or Hostname 10.10.56.103
Port Number (1-65535) 3001

Hostname - This displays the name of the specific VSCR-A. The name is in a standard format of VSMS-XXXXXXXX.

- VSMS: Vanderbilt SMS Reader Controller
- XXXXXXXX: The serial number of the specific VSRC-A
  (in the above example the serial number is 29006677).

The Host Name is used to access and setup the VSRC-A 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 VSRC-A to use a DHCP server on your network (use only if you have a DHCP server on the network). Vanderbilt recommends utilizing static IP addressing or DHCP reservations for controllers. If the controller IP address changes, there will be a loss of controller communications until the new IP address is recognized by the CIM.

Static - This setting forces the VSRC-A to use a static IP address.

IP Settings

- **IP Address**
  - When in Static mode, this is where you set the VSRC-A'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 VSRC-A'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.

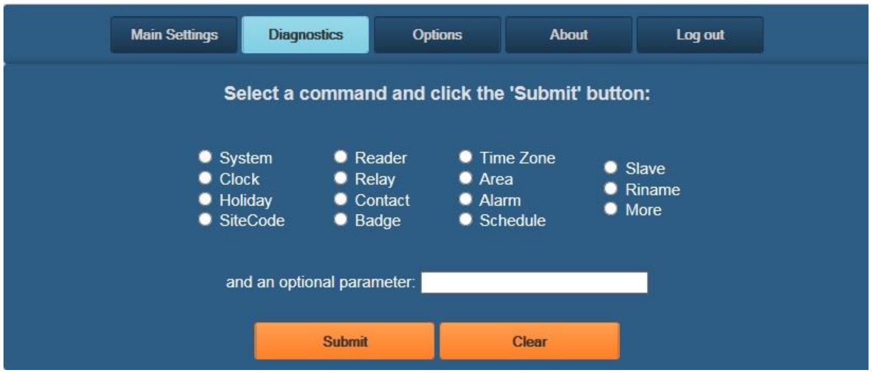
DNS Server Address Setting

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

CIM IP Address Setting

- **IP Address or Hostname -** Displays the IP Address or Hostname of the computer running the CIM; if using DNS, the Fully Qualified Domain Name (FQDN) of the CIM should be entered here
- **Port Number -** Displays the Port Number of the CIM: Use port 3001 unless otherwise specified by IT technician. Verify that the controller definitions match the port entered on this screen.

Diagnostics



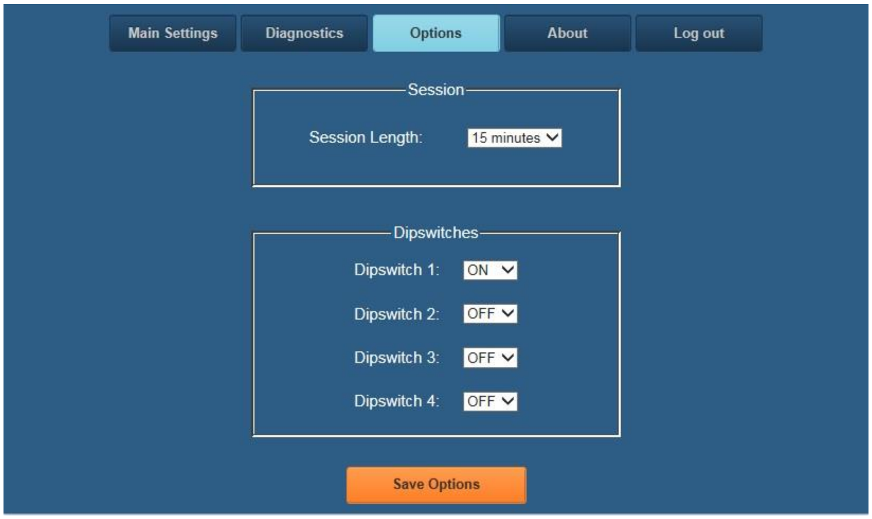
Select a command and click the 'Submit' button:

○ System
○ Clock
○ Holiday
○ SiteCode
○ Reader
○ Relay
○ Contact
○ Badge
○ Time Zone
○ Area
○ Alarm
○ Schedule
○ Slave
○ Riname
○ More

and an optional parameter:

Use this page to display additional detailed information regarding the VSRC-A and data currently residing in memory. Use this page only as directed by Vanderbilt Technical Support.

Options



Session

Session Length: 15 minutes

Dipswitches

Dipswitch 1: ON

Dipswitch 2: OFF

Dipswitch 3: OFF

Dipswitch 4: OFF

- Session Length: Use to set the session inactivity timeout.
- Dipswitch 1: Enable/Disable Onboard web server (Configuration GUI), Ping and Discovery protocol. Enabled by default. If OFF, the onboard web server (GUI), Ping and Discovery protocol are disabled.
  If disabled then the VSRC-A cannot be reached via the GUI, Ping or the Discovery and Configuration Tool.

Physical Access to the VSRC-A is required to re-enable the Configuration Application.

Press and Hold the Tamper Switch 25 AND Press and Release the Reset Button 20 three (3) times in succession. Release the Tamper Switch 25. 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”.

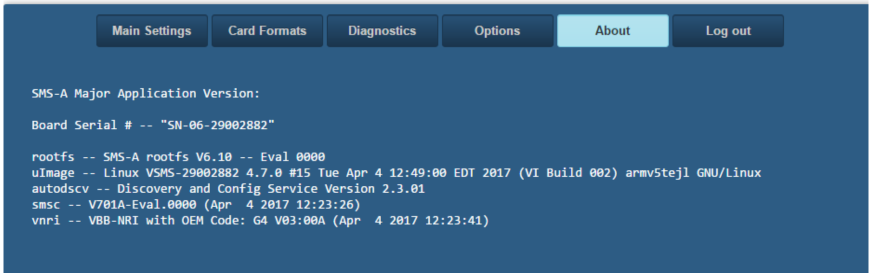
- Dipswitch 2: Reserved for Future Use
- Dipswitch 3: Used in Conjunction with Dipswitch 4 to configure as VSRC-A or VRCNX-A

- Dipswitch 4: Used in Conjunction with Dipswitch 3 to configure as VSRC-A or VRCNX-A

Type	Dipswitch 3	Dipswitch 4
VSRC-A	Off	Off
VRCNX-A0	On	On
VRCNX-A1	Off	On
VRCNX-A2/A3	On	Off

Warning: Vanderbilt recommends Setting Dipswitch 1 OFF to DISABLE the onboard web server, ping, and discovery protocol after installation and configuration. Leaving these features enabled could allow unauthorized access to the controller.

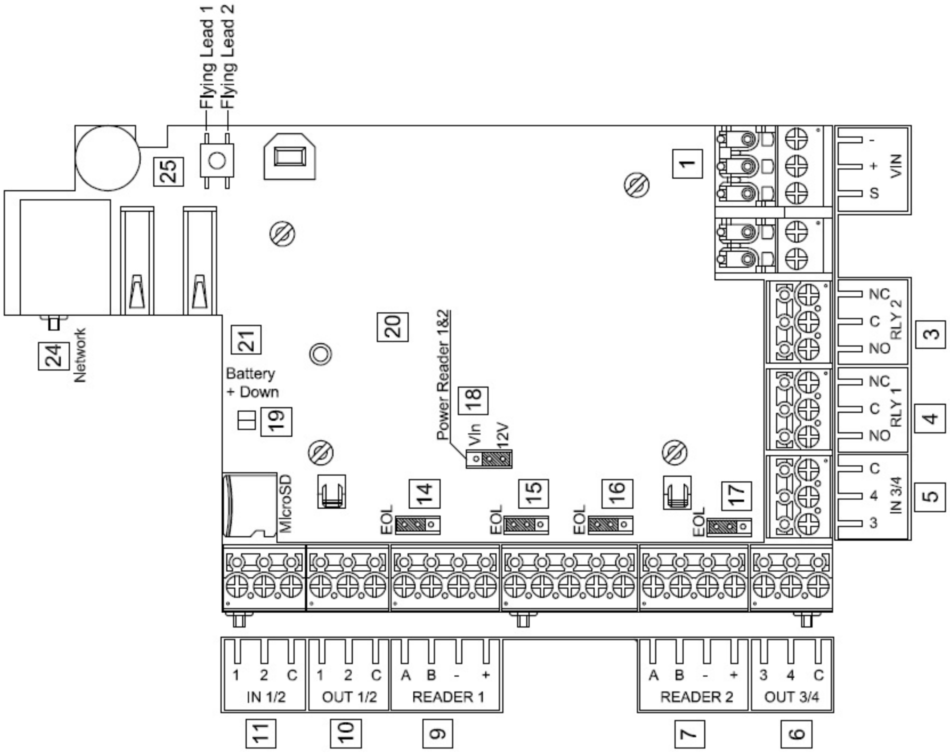
About



```
SMS-A Major Application Version:

Board Serial # -- "SN-06-29002882"

rootfs -- SMS-A rootfs V6.10 -- Eval 0000
uImage -- Linux VSMS-29002882 4.7.0 #15 Tue Apr 4 12:49:00 EDT 2017 (VI Build 002) armv5tejl GNU/Linux
autodscv -- Discovery and Config Service Version 2.3.01
smsc -- V701A-Eval.0000 (Apr  4 2017 12:23:26)
vnri -- VBB-NRI with OEM Code: G4 V03:00A (Apr  4 2017 12:23:41)
```

This page displays detailed information regarding the firmware loaded on the controller.

VSRC-A PIN Layout



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 VSRC-A 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 VSRC-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 Configure network functionality:

Refer to Configuration GUI section above.

Reader and I/O Assignment

The VSRC-A Supports 3 Door Configurations:

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

VSRC-A Reader Inputs and I/O is associated to one of the configurations above depending on the Reader Template applied in System Manager as indicated below.

Template	Reader Used	Relay Assignment	Contacts Assignment
Single Door Control			
VSRC Reader Template	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			
VSRC-A Dual Reader Template	Reader 1	Relay 1	Contact 1 – REX Contact 2 – DOD
	Reader 2	Relay 2	Contact 3 – REX Contact 4 – DOD
Single Door Control IN / OUT Readers – ***SMS v6.4.5 or newer***			
VSRC-A IN Reader Template	Reader 1 / Reader 2	Relay 1 Relay 2	Contact 1 – REX Contact 2 – DOD Contact 3 – Push Button Contact 4 – Aux Input
VSRC-A OUT Reader Template	Reader 2 / Reader 1		

Factory Reset and Power down

The Reset Button labeled 20 on the onboard mounted VSRC-A is used for Rebooting, Powering Down and Resetting, in conjunction with the Tamper Button 25, the VRCNX-A as indicated below.

The controller will produce 3 long beeps followed by a series of shorter beeps at a faster interval when depressed.

Reboot

Press and Hold the backplane mounted VSRC-A 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.

Power Down

Press and Hold the backplane mounted VSRC-A 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.

Reboot and Reset to Default IP Address

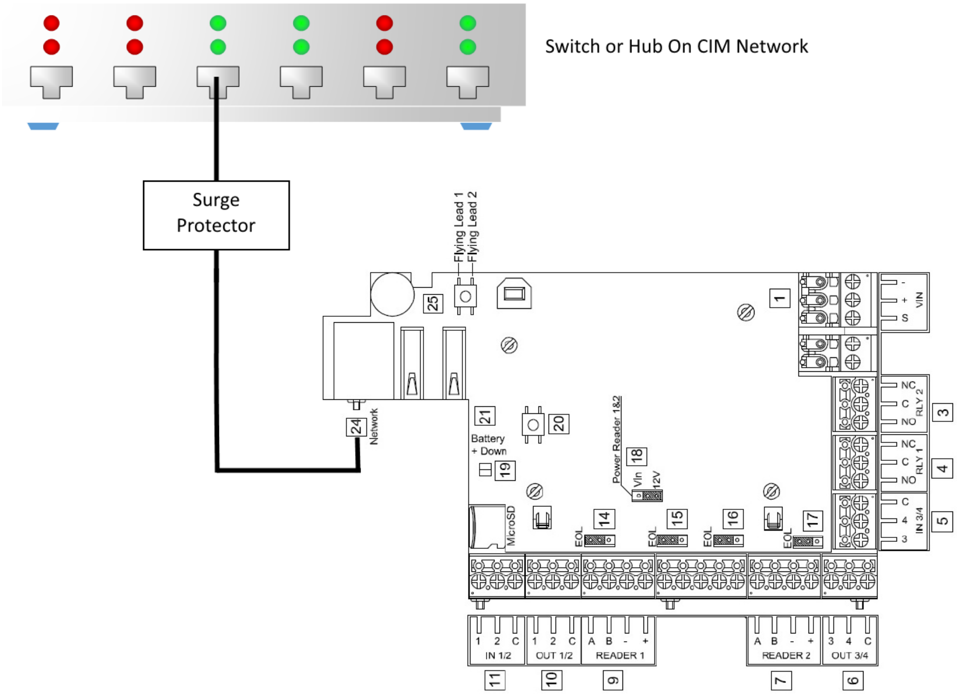
Press and Hold the backplane mounted VSRC-A Reset Button 20 **and** Tamper Button 25 until the short beeps begin and for nine (9) short beeps or less. The controller will shut down and reboot. The configured Network Settings (IP Address, etc.) will be reset to the factory default (192.168.168.249) on reboot.

Power Down and Reset to Default IP Address

Press and Hold the backplane mounted VSRC-A Reset Button 20 **and** Tamper Button 25 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 reset to factory default (192.168.1686.249) on restart. Disconnect and reconnect power to restart the controller.

Connecting to CIM

There is no direct connection between the VSRC-A and the CIM. To connect, they need to be on the same network and the proper IP address of the VSRC-A needs to be entered when setting up the VSRC-A in SMS. In addition, a data surge protector needs to be installed between the VSRC-A 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 TB1 on the VSRC-A.



Data Communication between CIM and VSRC-A

CIM	VSRC-A
Ethernet To Network	Ethernet to Network

Connecting to Read Heads

The following sections how to install various credential read heads to the VSRC-A reader interfaces.

The VSRC-A 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: VSRC-A to Reader Head

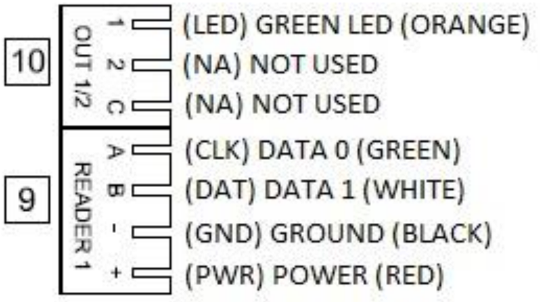
Connection	Maximum Distance (ft)	Cable Recommendation
VSRC-A to Magstripe Reader Head	200	18 AWG/5 Cond, Strd, Shld
VSRC-A to Proximity Reader Head	500	18 AWG/5 Cond, Strd, Shld
VSRC-A to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VSRC-A to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

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

Reader 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.

VMR-5 Magnetic Strip – LED 1 Wire Configuration

VSRC-A	VMR-5
9 PIN A (CLK)	DATA 1 (WHITE)
9 PIN B (DAT)	DATA 0 (GREEN)
9 PIN - (GND)	GROUND (BLACK)
9 PIN + (GND)	POWER (RED)
10 PIN 1 (LED)	LED (BROWN)
10 PIN 2 (NA)	NOT USED
10 PIN C (NA)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

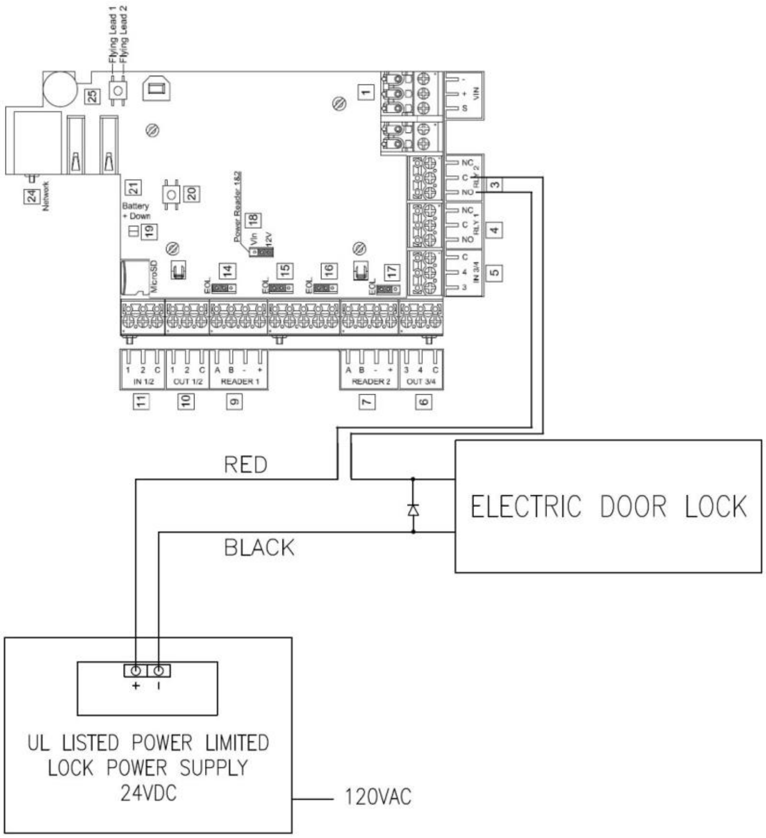
S1 = Off S2 = Off S3 = Off S4 = Off

VMR-10 and VMR-20 Magnetic Stripe

VSRC-A	VMR-5
$\boxed{9}$ PIN A (CLK)	DATA 1 (WHITE)
$\boxed{9}$ PIN B (DAT)	DATA 0 (GREEN)
$\boxed{9}$ PIN - (GND)	GROUND (BLACK)
$\boxed{9}$ PIN + (GND)	POWER (RED)
$\boxed{10}$ PIN 1 (LED)	LED (BROWN)
$\boxed{10}$ PIN 2 (NA)	NOT USED
$\boxed{10}$ PIN C (NA)	NOT USED

Installing Diodes for Lock Wiring - Relay

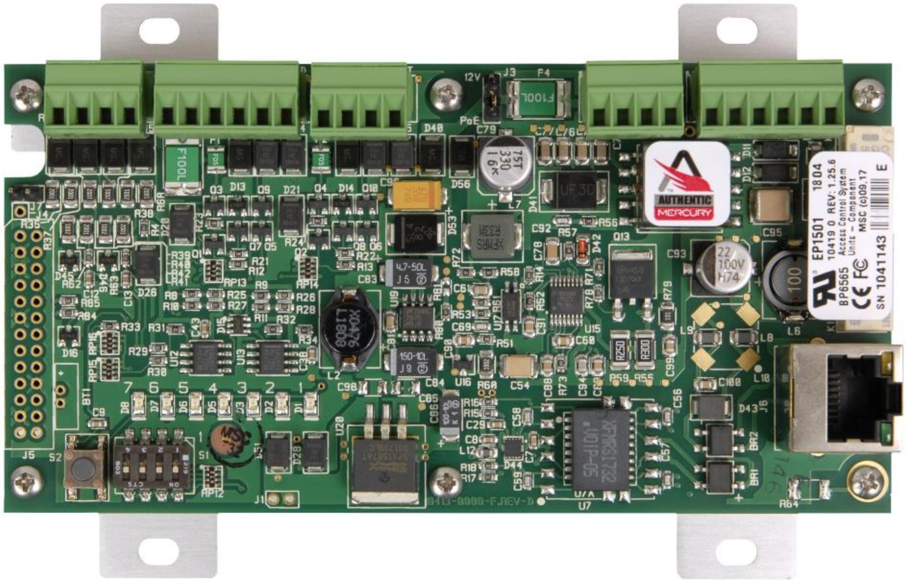
Diodes are supplied with the VSRC-A which should be fitted across 12V and COM on each Reader Interface to protect the relay contacts.



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 relay K1 and K3 NO or NC depending on lock type: Fail Open / Fail Closed (*the diagram above is Fail Open*).

VMRC-1

CHAPTER 8



VMRC-1 Single Reader Controller – Authentic Mercury Protocol

Overview

The Vanderbilt VMRC-1 is a PoE capable Single Reader Controller capable of supporting 1 to 17 total readers. The VMRC-1 supports 1 reader directly via an onboard reader interface and up to additional 8 ***physical*** devices may be connected via a single RS-485 channel. Using 8 RS-485 connected VRI-2 Dual Reader Interfaces, a total of 17 readers may be connected to the VMRC-1 (including the onboard reader interface which may be used in conjunction with RS-485 connected devices) or up to total 9 readers if 8 VRI-1 Single Reader Interfaces are used with the onboard reader. VI-16IN or VI-16O devices may also be connected and will reduce the total number of readers supported. Built on the Authentic Mercury platform (Mercury Hardware and Firmware), the VMRC-1 communicates with the SMS Mercury CIM (mCIM) via TCP/IP and can be connected to a variety of different read head technologies.

The VMRC-1 includes 2 general purpose contact inputs, assigned to the onboard reader interface; 2 Form-C relay outputs assigned to the onboard reader interface and 1 dedicated cabinet tamper contact input.

Highlights

- Supports read head technologies utilizing Wiegand (D0/D1) or Magstripe (clock/data) signals.

  Proximity Cards

  - Standard 26-bit
  - Vanderbilt 34-bit
  - HID Corporate 1000 35-Bit
  - HID Corporate 1000 48-Bit
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - XceedID 35-bit (including EV1)
  - MiFare 32-Bit Serial Number (With HID read-head ONLY)

  Magstripe Cards

  - Geoffrey encoded magcard 14-D
  - Geo-Image magcard 11-D
  - Locknetic 18-D magcard
- Communicates via network protocol at 10/100 Base-T
- Powered either via PoE or locally by a 12VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power.
- Capable of running in *Enhanced Offline Mode*, allowing local decision making if communication fails between the VMRC-1 and the network.

Standard Features

- Supports a single read-head credentials
- Communicates with mCIM via network protocol at 10/100 Base-T
- Connection for one multi-color LEDs for access granted or access denied indication
- Connector for one buzzer/annunciators
- Includes 2 input contacts for exit request (REX) and door position switch (DOD) *for the onboard Reader Interface*
- Connector for dedicated Cabinet Tamper

Specifications

▪ Board Dimensions:	5.40” H x2.75” W
▪ Enclosure Dimensions:	8 ¼” x 7 ½” x 3 ½”
▪ Power requirements:	PoE @ 12.95 W or 12 VDC @ 200 mA minimum, 900 mA maximum *180 mA Max Provided to the read head*
▪ Power consumption:	650 mA max. including read head
▪ Ambient temperature:	0º to 70º C

Enclosure

Enclosure Features

- Metal enclosure with hinged door, tamper switch, lock & key
- Enclosure Dimensions: 8 ¼" x 7 ½" x 3 ½"

Enclosure Environmental Conditions

- Ambient Temperature: 0º to 70º C
- Humidity: 5 to 95% RHNC
- 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

Enclosure 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.

IP Configuration

The VMRC-1 connects to the SMS host network via TCP/IP and communicates over the network to the SMS Mercury Communication Interface Module (**mCIM**) via Authentic Mercury protocol.

The **mCIM** is a Windows Service which supports communications with up to 256 Authentic Mercury Controllers, *depending on traffic*.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

The VMRC-1 is DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section before configuration DHCP.

Follow the steps below to configure the static IP of the VMRC-1.

The VMRC-1 controller ships with a default IP address = 192.168.0.251 and subnet mask = 255.255.255.0.

1. Change the IP address of your computer to a non-conflicting IP address on the same subnet as the controller (e.g. 192.168.0.252 / 255.255.255.0).

2. Connect the VMRC-1 directly to your computer with a network cable.

3. Verify that VMRC-1 S1 DIP switches 1 – 4 are all OFF.

4. Apply 12 VDC power to the controller.

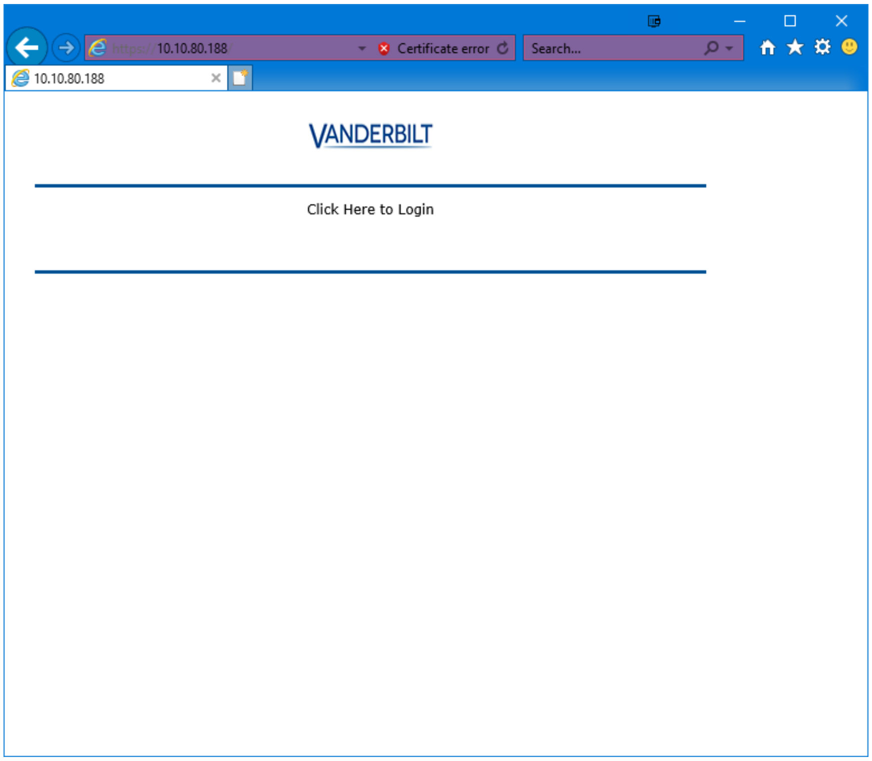
5. Set DIP Switch #1 from OFF to ON to enable the build-in default admin account.

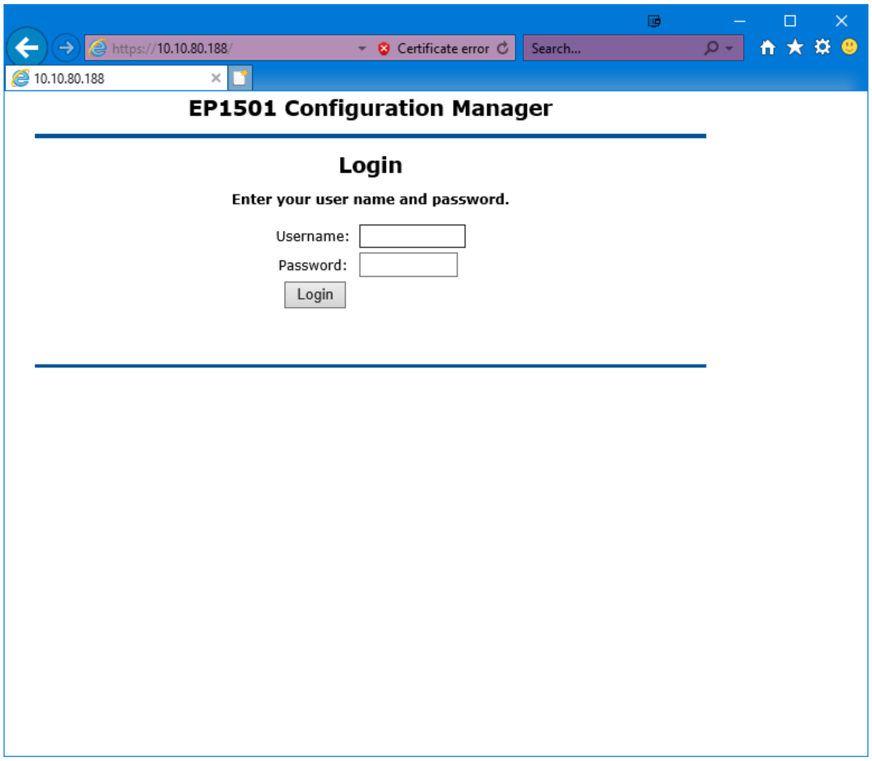
> *Setting DIP Switch #1 ON enables a 5-minute window to login with the default admin account*
>
> *Reenable the login window by Setting DIP Switch #1 OFF for at least 10 seconds*

6. Open a web browser and navigate to the following URL: http://192.168.0.251

7. A certificate warning will appear which varies by browser and browser settings. Allow the connection.

8. Click the link below the Vanderbilt logo to proceed to the login page.





EP1501 Configuration Manager

Login

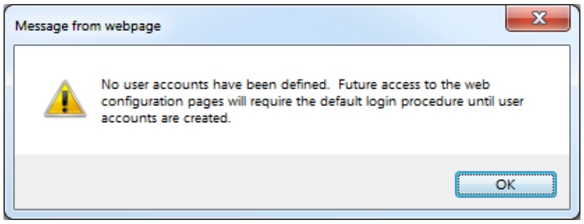
Enter your user name and password.

Username:

Password:

9. Enter the default Username and Password (*both case sensitive*):
    - Username = “admin”
    - Password = “password”

10. The following dialog may appear once the **Home** page loads.



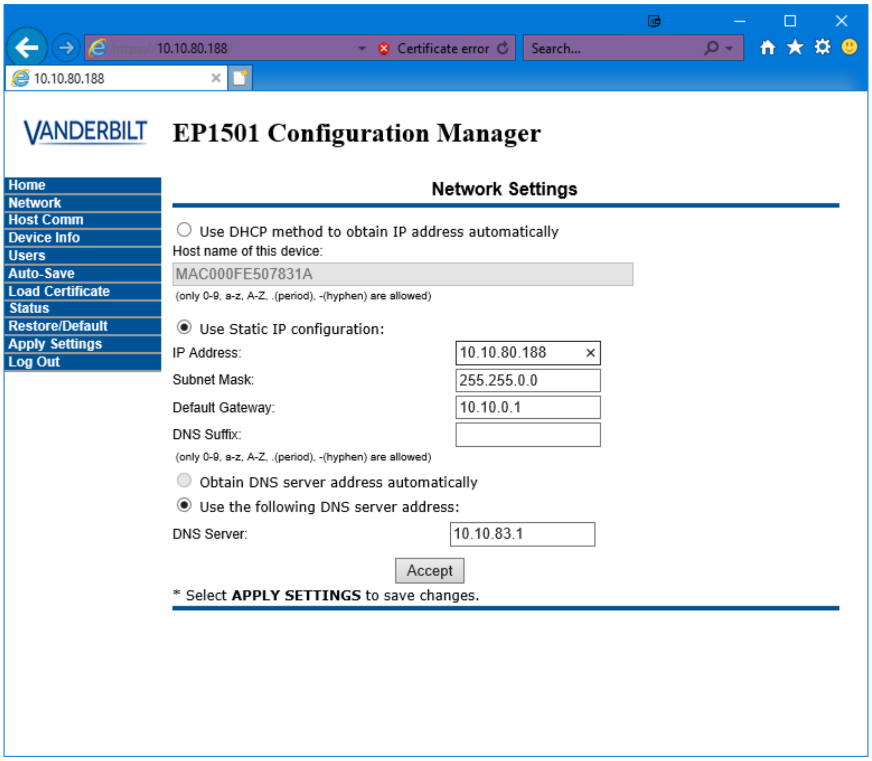
Message from webpage

No user accounts have been defined. Future access to the web configuration pages will require the default login procedure until user accounts are created.

11. Vanderbilt recommends creating a user account for providing access to the controller configuration without requiring physical access to the controller DIP Switch #1.

12. Click “OK”.

13. Select the **Network** option from the menu to access the Network Settings page.



EP1501 Configuration Manager

Network Settings

○ Use DHCP method to obtain IP address automatically

Host name of this device:

MAC000FE507831A

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

● Use Static IP configuration:

IP Address:	10.10.80.188
Subnet Mask:	255.255.0.0
Default Gateway:	10.10.0.1
DNS Suffix:	

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

○ Obtain DNS server address automatically

● Use the following DNS server address:

DNS Server: 10.10.83.1

* Select **APPLY SETTINGS** to save changes.

14. Vanderbilt recommends assigning a static IP address, so the controller can always be easily accessed.
    - Select “Use Static IP configuration”.
    - Enter the appropriate SMS host network **IP Address** for the controller as specified by IT.
    - Enter the appropriate SMS host network **Subnet Mask** for the controller as specified by IT.
    - Enter the appropriate SMS host network **Default Gateway** for the controller as specified by IT.
    - Enter the appropriate SMS host network **DNS Server** as specified by IT or enter 0.0.0.0.
15. Click “Accept”.

DHCP Configuration

The VMRC-1 initiates communications to the **mCIM** so configuring the VMRC-1 for DHCP will not affect SMS communications or operability and can be selected via the Network Settings menu as shown above.

> ***WARNING:*** *While using DHCP will not affect the ability of the controller to function with SMS, it might not be easy to determine the current IP address of a controller configured for DHCP without IT support. The controller IP address must be known to access the controller web configuration. Vanderbilt recommends using reservations if using DHCP.*

SMS Communications Configuration

The VMRC-1 controller ships with default Host Communications configured for IP Server. The Host Communications settings must be changed for the controller to communicate to the SMS **mCIM**.

1. Select **Host Comm** from the menu to load the Host Communications configuration page.

2. Change Primary Host Port **Connection Type** to “IP Client”.

3. Change Primary Host Port **Data Security** to “TLS Required” if encryption communication is desired.

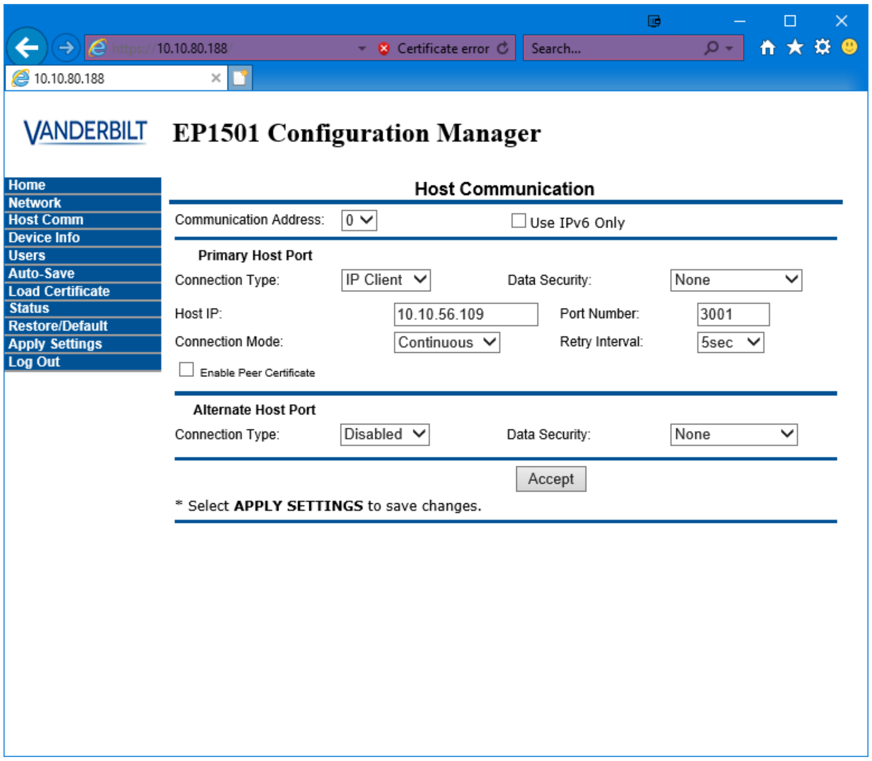
> *SMS Authentic Mercury protocol TLS encryption can only be enabled **per mCIM***

4. Change the Primary Host Port **Host IP** to the IP Address of the computer hosting the **mCIM**.

> *Vanderbilt recommends a dedicated **mCIM** host*
>
> *The **mCIM** Port defined in SMS **must match** the VMRC-1 Host Port setting*

5. Change the Primary Host Port **Port Number** to 5001, ***only if required***.

6. Do not change any other settings. SMS does not support the Alternate Host Port.



EP1501 Configuration Manager

Host Communication

Communication Address: 0 □ Use IPv6 Only

Primary Host Port

Connection Type: IP Client Data Security: None

Host IP: 10.10.56.109 Port Number: 3001

Connection Mode: Continuous Retry Interval: 5sec

□ Enable Peer Certificate

Alternate Host Port

Connection Type: Disabled Data Security: None

* Select **APPLY SETTINGS** to save changes.

7. Click “Accept”.

Create User Account

Vanderbilt recommends creating at least 1 user account so that physical access to the controller for setting DIP Switch #1 is not required for accessing the controller configuration.

1. Select **Users** from the Menu.

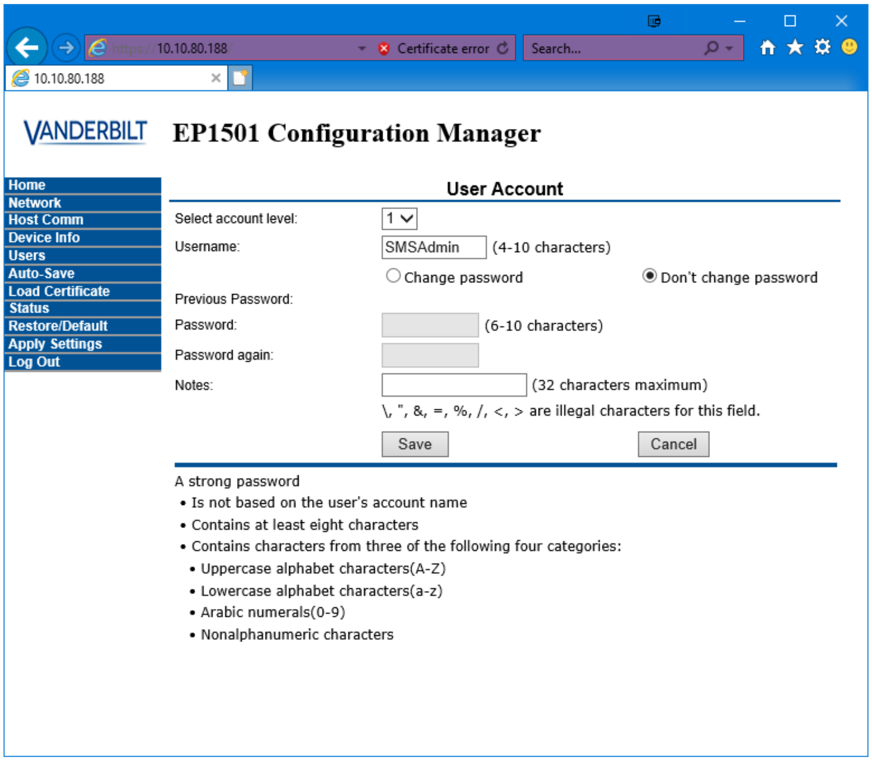
2. Click “New User”.

3. Leave “Select account level” = 1 (*administrator*)

4. Enter desired **Username**. Vanderbilt recommends SMSAdmin.

5. Enter desired **Password** and confirm.

6. Enter **Notes** if desired.



EP1501 Configuration Manager

User Account

Select account level: 1

Username: SMSAdmin (4-10 characters)

○ Change password ● Don't change password

Previous Password:

Password: (6-10 characters)

Password again:

Notes: (32 characters maximum)

\, ", &, =, %, /, <, > are illegal characters for this field.

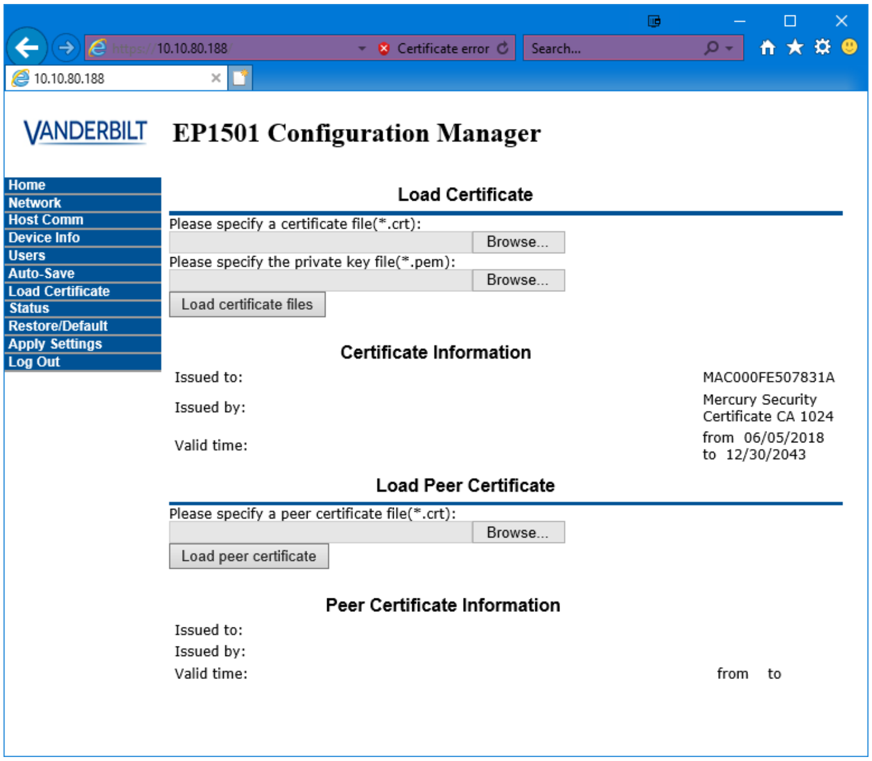
A strong password
- Is not based on the user's account name
- Contains at least eight characters
- Contains characters from three of the following four categories:
  - Uppercase alphabet characters(A-Z)
  - Lowercase alphabet characters(a-z)
  - Arabic numerals(0-9)
  - Nonalphanumeric characters

7. Click “Save”.

Upload Certificate

If TLS encryption will be enabled, a custom certificate may be downloaded to the controller which will be used in place of the Mercury provided self-signed certificate.

1. Select **Load Certificate** from the Menu.



EP1501 Configuration Manager

Load Certificate

Please specify a certificate file(*.crt):

Please specify the private key file(*.pem):

Certificate Information

Issued to:	MAC000FE507831A
Issued by:	Mercury Security Certificate CA 1024
Valid time:	from 06/05/2018 to 12/30/2043

Load Peer Certificate

Please specify a peer certificate file(*.crt):

Peer Certificate Information

Issued to:	
Issued by:	
Valid time:	from to

2. Click “Choose File” under “Please specify a certificate file” to specify the Certificate .crt file.

3. Click “Choose File” under “Please specify the private key file” to specify the Certificate Key .pem file.

4. Click “Load certificate files”.

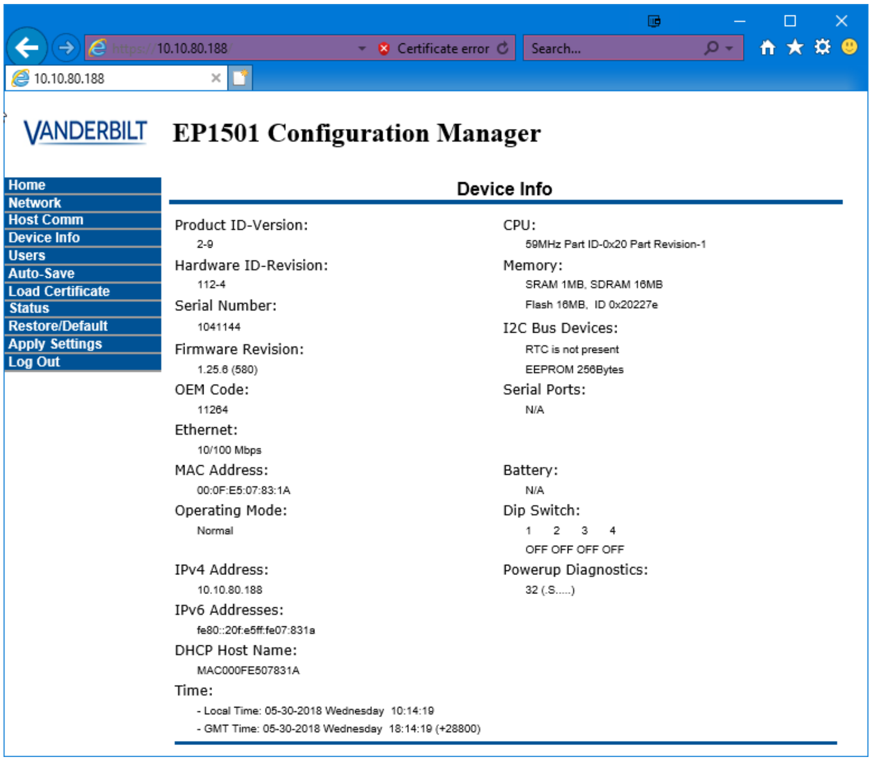
Document and Commit Configuration Changes

Once all desired configuration changes have been Accepted, they must be committed, and the controller rebooted to enable the new settings.

Prior to committing changes and rebooting the controller, Vanderbilt recommends saving a screen shot of the controller configuration and device specific information for documentation.

Record the controller Serial Number – it is required for SMS configuration.

1. Select Device Info from the Menu.



EP1501 Configuration Manager

Device Info

Product ID-Version:
2-9

Hardware ID-Revision:
112-4

Serial Number:
1041144

Firmware Revision:
1.25.6 (580)

OEM Code:
11264

Ethernet:
10/100 Mbps

MAC Address:
00:0F:E5:07:83:1A

Operating Mode:
Normal

IPv4 Address:
10.10.80.188

IPv6 Addresses:
fe80::20f:e5ff:fe07:831a

DHCP Host Name:
MAC000FE507831A

Time:
- Local Time: 05-30-2018 Wednesday 10:14:19
- GMT Time: 05-30-2018 Wednesday 18:14:19 (+28800)

CPU:
59MHz Part ID-0x20 Part Revision-1

Memory:
SRAM 1MB, SDRAM 16MB
Flash 16MB, ID 0x20227e

I2C Bus Devices:
RTC is not present
EEPROM 256Bytes

Serial Ports:
N/A

Battery:
N/A

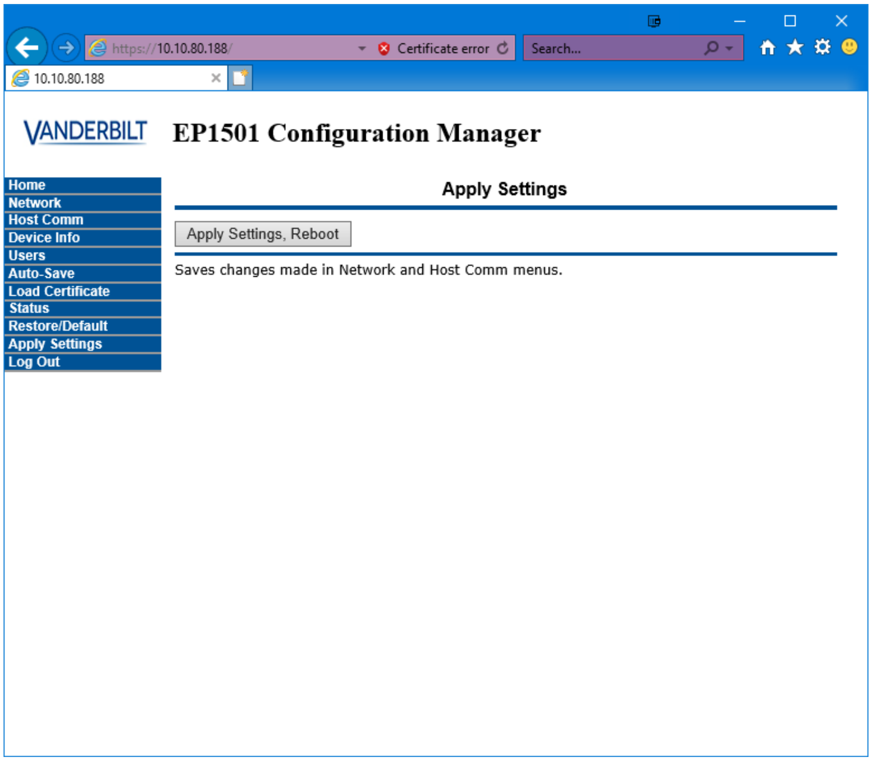
Dip Switch:
1 2 3 4
OFF OFF OFF OFF

Powerup Diagnostics:
32 (.S.....)

2. Save a screen shot or at least note IP Address and Serial Number.

3. Click “Apply Settings” in the menu.

4. Click “Apply Settings, Reboot”.



EP1501 Configuration Manager

Apply Settings

Saves changes made in Network and Host Comm menus.

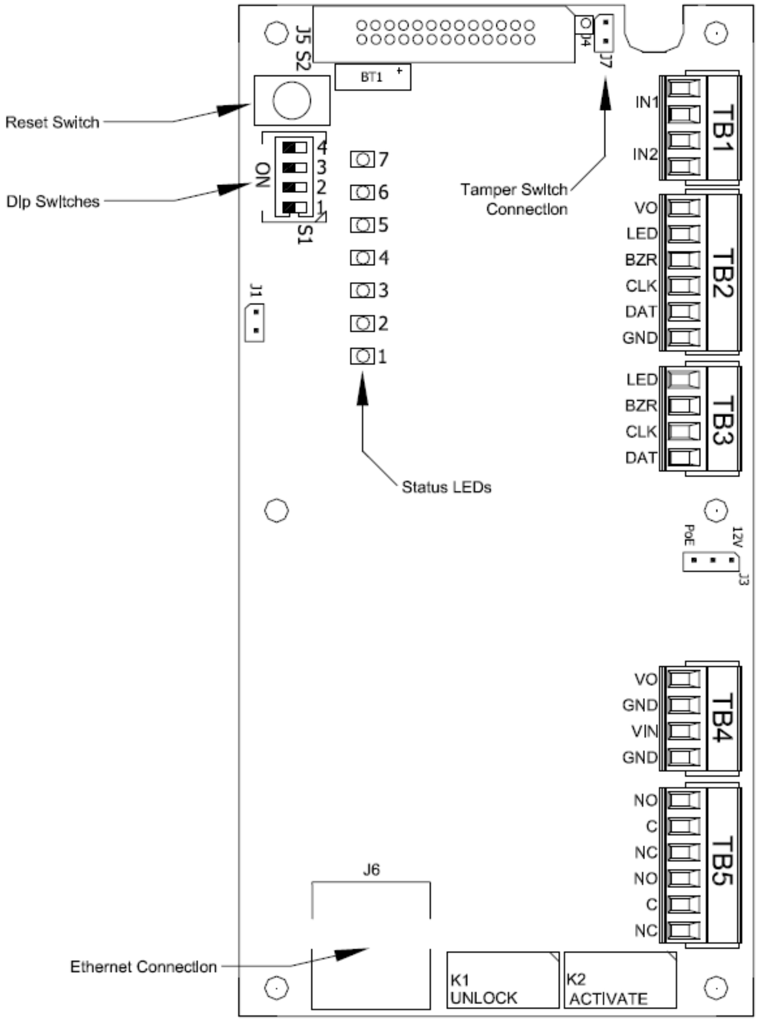
5. A page might display stating that the DIP Switches are not set for normal operation or no user accounts have been created. Select each checkbox and click “Yes”.

6. Controller configuration for SMS has been completed.

> *Ensure that SMS configuration for Data Security and Host Port Number are configured identically in SMS or the controller will not communication with the **mCIM***

7. Set all DIP Switches to OFF (normal operating mode).

Pin Layout


J5 S2
BT1
+
J4
J7
Reset Switch
Dip Switches
ON
4
3
2
1
S1
7
6
5
4
3
2
1
Tamper Switch Connection
IN1
IN2
TB1
VO
LED
BZR
CLK
DAT
GND
TB2
LED
BZR
CLK
DAT
TB3
J1
Status LEDs
PoE
12V
J3
VO
GND
VIN
GND
TB4
NO
C
NC
NO
C
NC
TB5
J6
Ethernet Connection
K1
UNLOCK
K2
ACTIVATE

Pin Functions

CONNECTION		
TB1-1	Input 1	IN1
TB1-2		IN1
TB1-3	Input 2	IN2
TB1-4		IN2
TB2-1	Reader 1	VO: Reader Power
TB2-2		LED: Reader LED
TB2-3		BZR: Reader Buzzer
TB2-4		CLK/D1: Clock/Data 1 or RS-485 TR+
TB2-5		DAT/D0: Data/Data 0 or RS-485 TR-
TB2-6		GND: Ground
TB3-1	Reader 2	LED: Reader LED
TB3-2		BZR: Reader Buzzer
TB3-3		CLK/D1: Clock/Data 1
TB3-4		DAT/D0: Data/Data 0
TB4-1	Auxiliary Power Out	VO: Power Out – 12 Vdc
TB4-2		GND: Ground
TB4-3	Power Input	VIN: 12 Vdc
TB4-4		GND
TB5-1	Out 1	NO: Normally Open Contact
TB5-2		C: Common
TB5-3		NC: Normally Closed Contact
TB5-4	Out 2	NO: Normally Open Contact
TB5-5		C: Common
TB5-6		NC: Normally Closed Contact

Jumpers

JUMPERS	SET AT	DESCRIPTION
J1	N/A	Factory Use Only
J2	N/A	Factory Use Only
J3	PoE	VMRC-1 powered from Ethernet Connection
	12V	VMRC-1 powered from local 12 Vdc to TB4-3 (VIN) and TB4-3 (GND)
J4	N/A	Factory Use Only
J5	N/A	Factory Use Only
J6	N/A	10Base-T / 100Base-TX Ethernet Connection
J7		Cabinet Tamper Switch Input: short = tamper secure

DIP Switches

The four switches on S1 DIP switch configure the operating mode of the VMRC-1 processor. DIP switches are read on power-up except where noted. Pressing switch S2 causes the VMRC-1 to reboot.

1	2	3	4	Definition
OFF	OFF	OFF	OFF	Normal operating mode.
ON	X	X	X	After initialization, enable default User Name (admin) and Password (password). The switch is read on the fly, no need to re-boot. See IT Security section for additional information.
OFF	ON	X	OFF	Use factory default communication parameters.
ON	ON	X	OFF	Use OEM default communication parameters. Contact system manufacture for details. See Bulk Erase below.
X	X	ON	X	Disable TLS secure link. Switch is read only when logging on.
ON	ON	OFF	OFF	Bulk Erase prompt mode at power up. See Bulk Erase below.

All other switch settings for unassigned and are reserved for future use. X = don't care.
In the factory or OEM default modes, downloaded configuration/database is not saved to flash memory.

Cabinet Tamper

There is one dedicated input for cabinet tamper. Normal (safe) condition is a closed contact. If this input is not used, install a jumper wire.

Factory Reset

Follow the steps below to Bulk Erase Configuration memory for the VMRC-1.

This procedure should be attempted to performed to accomplish the following:

- Erase all configuration and cardholder database data (sanitize the controller)
- Recover from controller database corruption causing VMRC-1 to continuously reboot

If the procedure below does not correct the initialization issue, contact Vanderbilt Technical Support.

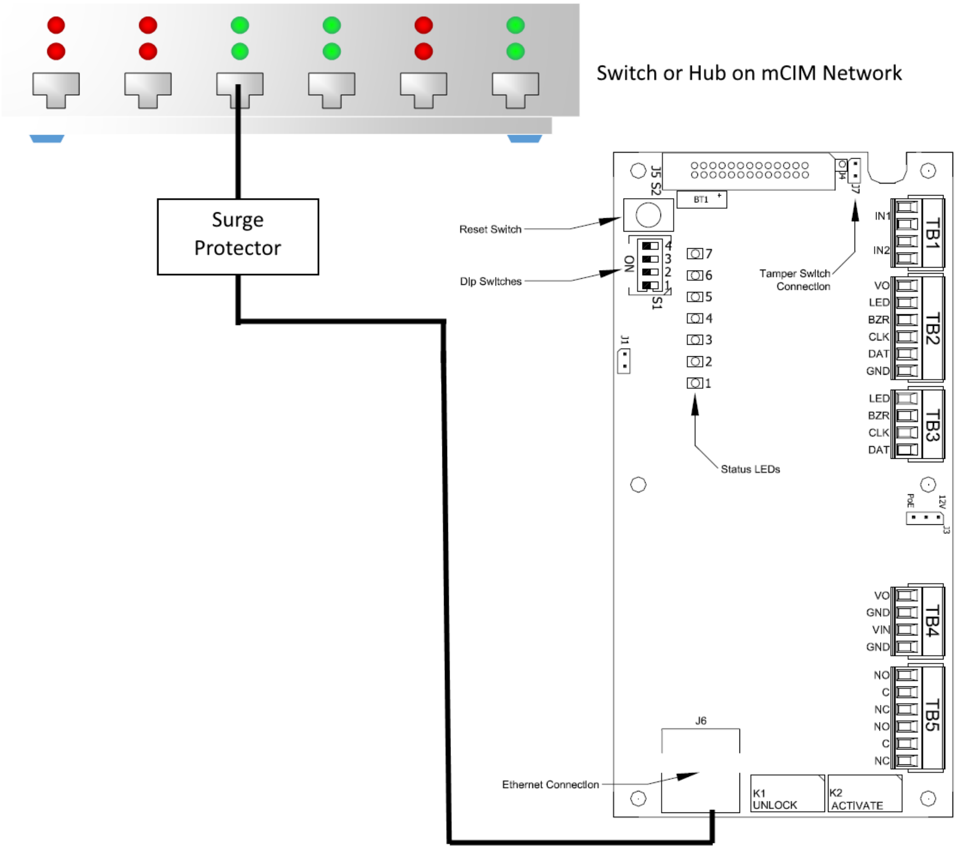
Do Not Remove Power During Steps 2 – 8 Below

1. Set S1 DIP switches to: 1 & 2 "ON", 3 & 4 "OFF".
2. Apply power to the VMRC-1.
3. Watch for LEDs 1 & 2 and 3 & 4 to alternately flash at a 0.5 second rate.

4. Within 10 seconds of powering up, change switches 1 or 2 to "OFF". If these switches are not changed, the VMRC-1 board will power up using the OEM default communication parameters.
5. LED 2 will flash indicating that the configuration memory is being erased.
6. Full memory erase takes up to 60 seconds.
7. When complete, only LEDs 1 & 4 will flash for 8 seconds.
8. The VMRC-1 will reboot 8 seconds after LEDs 1 & 4 stop flashing (no LEDs are on during this time).

Connecting VMRC-1 to mCIM

There is no direct connection between the VMRC-1 and the **mCIM**. To connect, they need to be on the same network and the proper IP address of the **mCIM** needs to be entered when setting up the VMRC-1. In addition, a data surge protector should be installed between the VMRC-1 and the hub or switch. Install the supplied data surge protector (DITEK-DTK-MRJ45C5E) or an equivalent UL Listed unit. Power is supplied via PoE or independently from a power supply connected the VMRC-1.



Data Communication between mCIM and VMRC-1

mCIM	VMRC-1
Ethernet To Network	Ethernet to Network

Connecting to Read Heads

The following sections how to install various credential read heads to the VMRC-1 reader interfaces.

The VMRC-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: VMRC-1 to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VMRC-1 to Magstripe Reader Head	200	18 AWG/5 Cond, Strd, Shld
VMRC-1 to Proximity Reader Head	500	18 AWG/5 Cond, Strd, Shld
VMRC-1 to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VMRC-1 to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

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

VMRC-1 RI Pin Connections

Reader 1

Reader 1 is used for RS-485 peripheral device connections (VRI-1, VRI-2, VI-16IN or VI-16O) to the VMRC-1:

- TB2-4 is RS-485 TR+
- TB2-5 is RS-485 TR-

Reader 2

Reader 2 can be used to connect 1 card-reader to the VMRC-1:

- TB3-1 is LED
- TB3-2 is Buzzer
- TB3-3 is CLK/D1 (Data 1)
- TB3-4 is DAT/D0 (Data 0)
- TB4-1 is Power (V0)
- TB4-2 is Ground (GND)

Reader 2 has two contact points at TB1: 1 – 4. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

Reader 2 has two relay outputs at TB5: 1 – 6. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. TB5 1 – 3 are for the Door Unlock relay. TB5: 4 – 6 are for the Door Held Open relay.

Proximity Reader

Wiegand / Proximity Read Head Pin Connections

VMRC-1	Proximity Reader
TB3-1 (LED)	LED (ORANGE)
TB3-2 (BUZZER)	BEEPER (YELLOW)
TB3-3 (CLK/D1)	DATA 1 (WHITE)
TB3-4 (DAT/D0)	DATA 0 (GREEN)
TB4-1 (PWR)	POWER (RED)
TB4-2 (GND)	GROUND (BLACK)

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

VMR-10 and VMR-20 Magnetic Stripe

VMR-10 and VMR-20 Magnetic Stripe Pin Connections

VSRC-M	VMR-10 and VMR-20
TB3-1 (LED)	LED (BROWN)
TB3-2 (BUZZER)	NOT USED
TB3-3 (CLK/D1)	DATA 1 (WHITE)
TB3-4 (DAT/D0)	DATA 0 (GREEN)
TB4-1 (PWR)	POWER (RED)
TB4-2 (GND)	GROUND (BLACK)

VMR-10 and VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On

VMRC-1 Device Configuration

The VMRC-1 also has 1 RS-485 channel for devices and can support up to 8 **physical** Authentic Mercury serial I/O devices (SIOs).

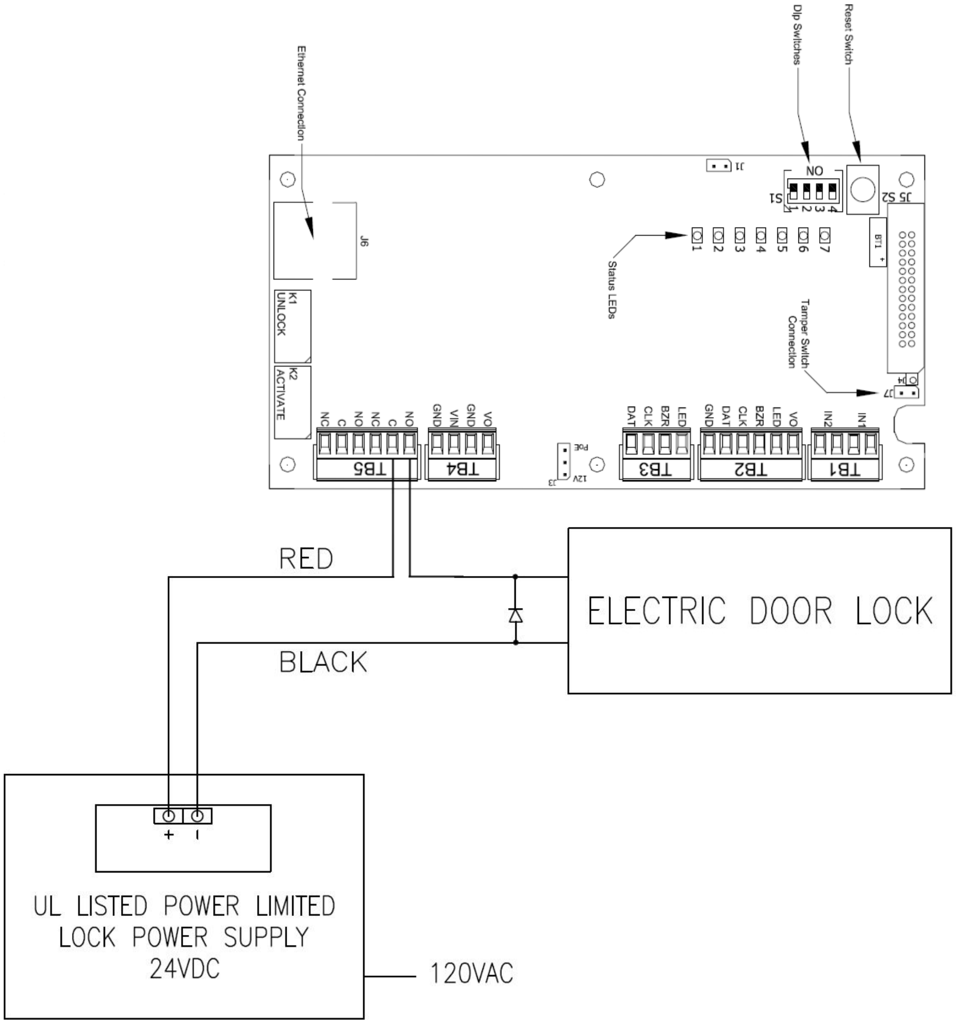
The SIO communication port (TB2) is a 2-wire RS-485 interface which can be used to connect additional I/O panels. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,219 m). Use twisted pairs (minimum 24 AWG) with drain wire and shield for communication.

- TB2-4 is RS-485 TR+
- TB2-5 is RS-485 TR-

Do not terminate any of the devices on the RS-485 bus.

Installing Diodes for Lock Wiring - Relay

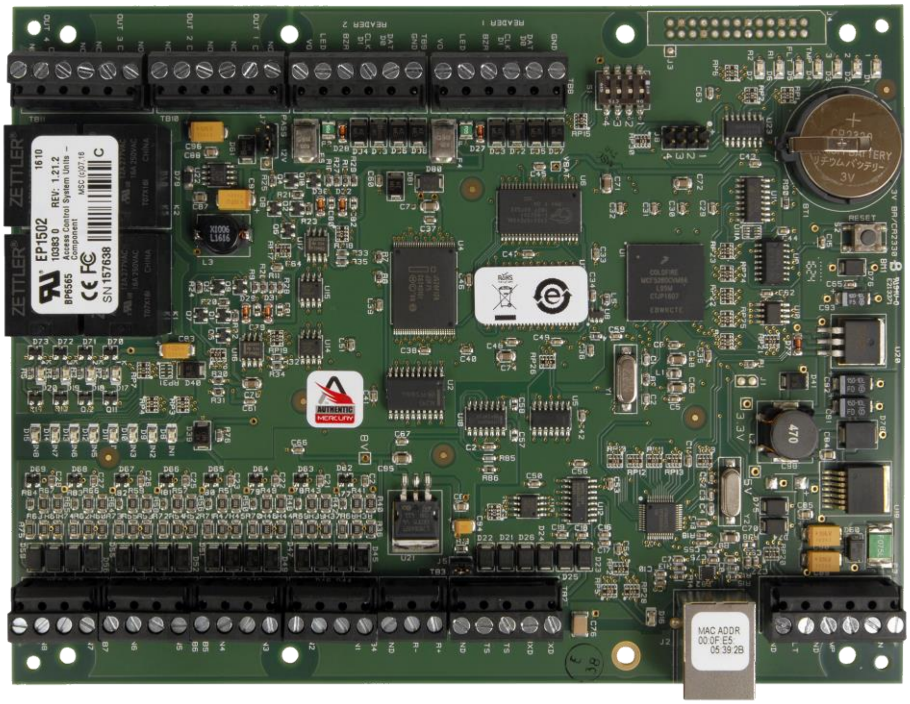
Diodes are supplied with the VMRC-1 which should be fitted across 12V and COM on the Reader Interface to protect the relay contacts.



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 relay K1 NO or NC depending on lock type: Fail Open / Fail Closed (*the diagram above is Fail Open to Relay 1*).

VMRC-2

CHAPTER 9



VMRC-2 Dual Reader Controller – Authentic Mercury Protocol

Overview

The Vanderbilt VMRC-2 is a Dual Reader Controller capable of supporting up to 32 total devices. The VMRC-2 supports 2 devices directly via onboard reader interfaces and an additional 30 devices via a single RS-485 channel (or 32 RS-485 connected devices). Built on the Authentic Mercury platform (Mercury Hardware and Firmware), the VMRC-2 communicates with the SMS Mercury CIM (mCIM) via TCP/IP and can be connected to a variety of different read head technologies.

The VMRC-2 includes 8 general purpose contact inputs, 4 each assigned to each onboard reader interface; 4 Form-C relay outputs, 2 each assigned to each onboard reader interface; 1 dedicated cabinet tamper contact input and 1 dedicated power fault contact input connection.

Highlights

- Supports read head technologies utilizing Wiegand (D0/D1) or Magstripe (clock/data) signals.

  Proximity Cards

  - Standard 26-bit
  - Vanderbilt 34-bit
  - HID Corporate 1000 35-Bit
  - HID Corporate 1000 48-Bit
  - HID/ProxIF 37-Bit
  - XceedID 40-Bit
  - XceedID 35-bit (including EV1)
  - MiFare 32-Bit Serial Number (With HID read-head ONLY)

  Magstripe Cards

  - Geoffrey encoded magcard 14-D
  - Geo-Image magcard 11-D
  - Locknetic 18-D magcard
- Communicates via network protocol at 10/100 Base-T
- Powered locally by a 12VDC Rated UL294 Listed Power-Limited Power Supply, capable of 4 hours standby power.
- Capable of running in *Enhanced Offline Mode*, allowing local decision making if communication fails between the VSRC-M and the network.

Standard Features

- Supports two read-head credentials
- Communicates with mCIM via network protocol at 10/100 Base-T
- Connection for two multi-color LEDs for access granted or access denied indication
- Connector for two buzzer/annunciators
- Includes 4 input contacts for devices such as exit request (REX), door position switch (DOD), etc. *for each Read Head*
- Connector for dedicated Cabinet Tamper
- Connector for dedicated Power Fault Interrupt

Specifications

- Board Dimensions: 8” H x 6” W
- Enclosure Dimensions: 10” H x 12 W” x 2-3/4” D
- Power requirements: 12VDC to 24VDC
  - *180 mA Max Provided to Each Reader Head if VIN > 20 VDC*
- Power consumption: 500mA max. without read head
- Ambient temperature: 0º to 70º C

Enclosure

Enclosure Features

- Metal enclosure with hinged door, tamper switch, lock & key
- Enclosure Dimensions: 10” x 12” x 2-3/4”

Enclosure Environmental Conditions

- Ambient Temperature: 0º to 70º C
- Humidity: 5 to 95% RHNC
- 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

Enclosure 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.

IP Configuration

The VMRC-2 connects to the SMS host network via TCP/IP and communicates over the network to the SMS Mercury Communication Interface Module (**mCIM**) via Authentic Mercury protocol.

The **mCIM** is a Windows Service which supports communications with up to 256 Authentic Mercury Controllers, *depending on traffic*.

Note: Communication is at 10/100 Base-T

Static IP and DNS Configuration

The VMRC-2 is DNS Compatible. Configuring a DNS Server is beyond the scope of this manual; a network technician should be contacted to set up the DNS Server. The directions below give details for Static IP setup with and without DNS. See the DHCP Configuration section before configuration DHCP.

Follow the steps below to configure the static IP of the VMRC-2.

The VMRC-2 controller ships with a default IP address = 192.168.0.251 and subnet mask = 255.255.255.0.

1. Change the IP address of your computer to a non-conflicting IP address on the same subnet as the controller (e.g. 192.168.0.252 / 255.255.255.0).

2. Connect the VMRC-2 directly to your computer with a network cable.

3. Verify that VMRC-2 S1 DIP switches 1 – 4 are all OFF.

4. Apply 12 – 24 VDC power to the controller.

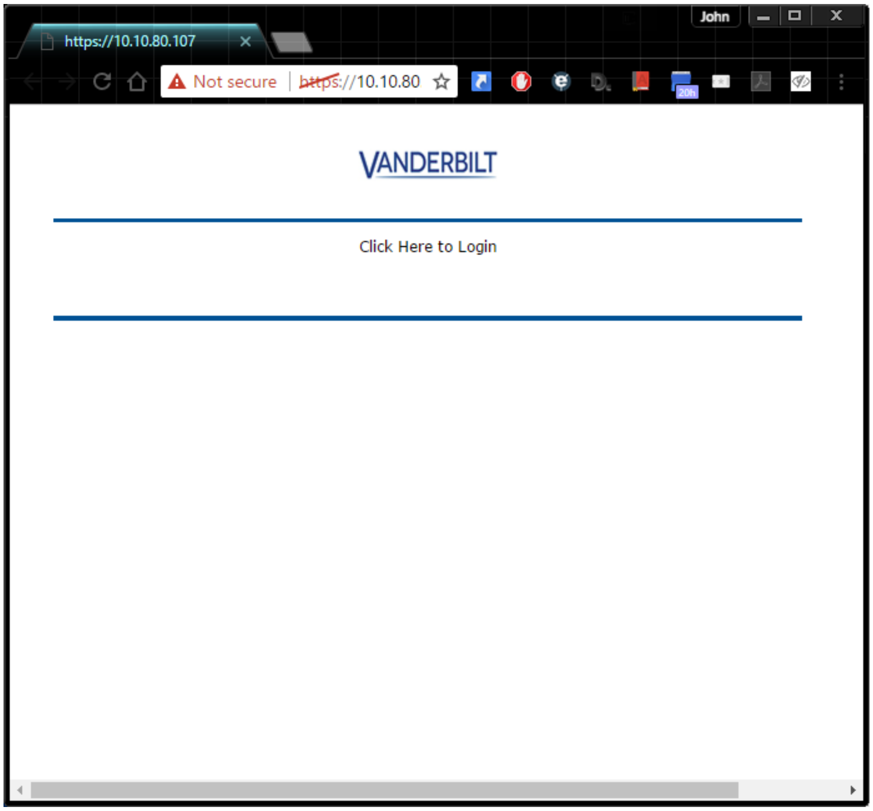
5. Set DIP Switch #1 from OFF to ON to enable the build-in default admin account.

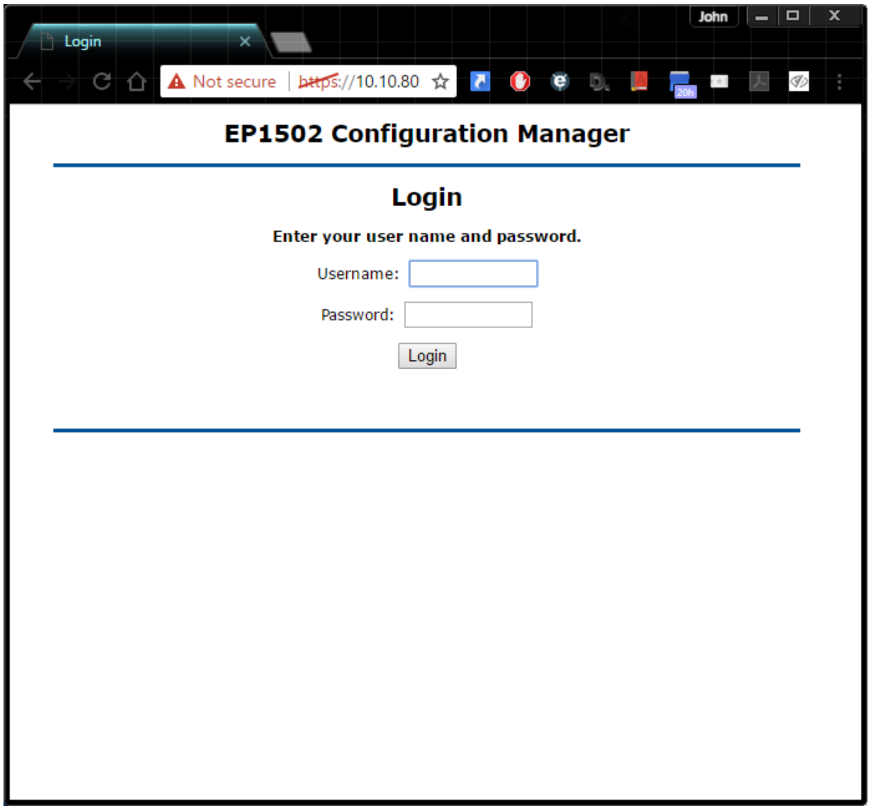
> *Setting DIP Switch #1 ON enables a 5-minute window to login with the default admin account*
>
> *Reenable the login window by Setting DIP Switch #1 OFF for at least 10 seconds*

6. Open a web browser and navigate to the following URL: http://192.168.0.251

7. A certificate warning will appear which varies by browser and browser settings. Allow the connection.

8. Click the link below the Vanderbilt logo to proceed to the login page.





EP1502 Configuration Manager

Login

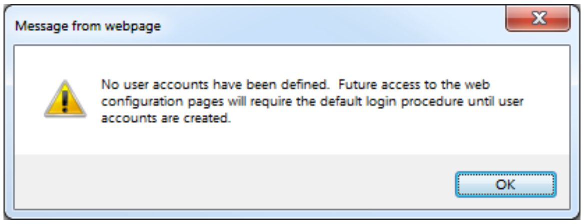
Enter your user name and password.

Username:

Password:

9. Enter the default Username and Password (*both case sensitive*):
   - Username = “admin”
   - Password = “password”

10. The following dialog may appear once the **Home** page loads.

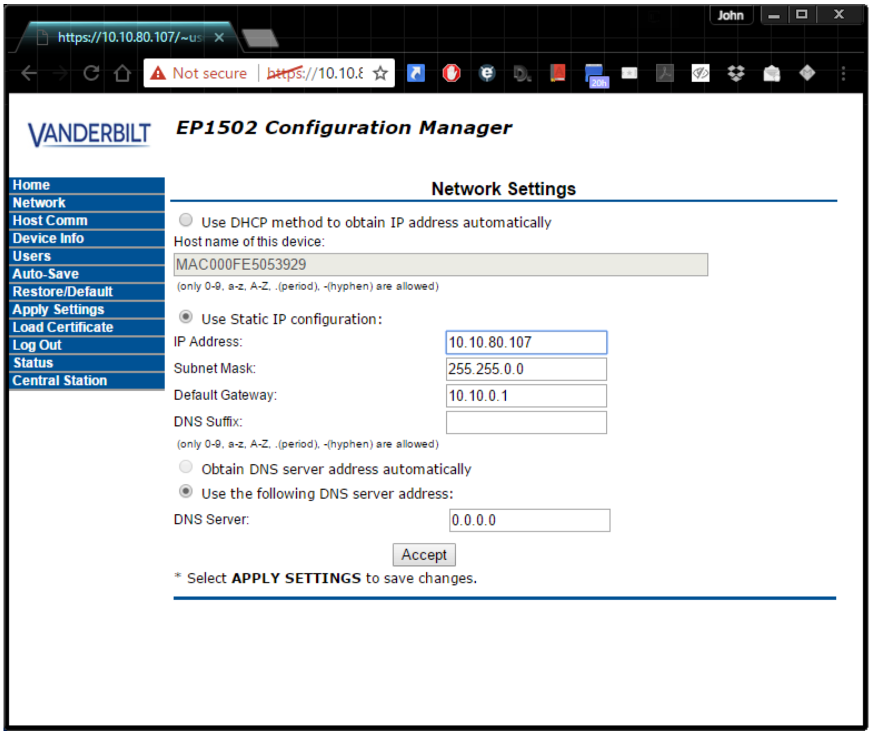

Message from webpage

No user accounts have been defined. Future access to the web configuration pages will require the default login procedure until user accounts are created.

11. Vanderbilt recommends creating a user account for providing access to the controller configuration without requiring physical access to the controller DIP Switch #1.

12. Click “OK”.

13. Select the **Network** option from the menu to access the Network Settings page.



EP1502 Configuration Manager

Network Settings

○ Use DHCP method to obtain IP address automatically

Host name of this device: MAC000FE5053929

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

● Use Static IP configuration:

IP Address: 10.10.80.107

Subnet Mask: 255.255.0.0

Default Gateway: 10.10.0.1

DNS Suffix:

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

○ Obtain DNS server address automatically

● Use the following DNS server address:

DNS Server: 0.0.0.0

* Select **APPLY SETTINGS** to save changes.

14. Vanderbilt recommends assigning a static IP address, so the controller can always be easily accessed.
    - Select “Use Static IP configuration”.
    - Enter the appropriate SMS host network **IP Address** for the controller as specified by IT.
    - Enter the appropriate SMS host network **Subnet Mask** for the controller as specified by IT.
    - Enter the appropriate SMS host network **Default Gateway** for the controller as specified by IT.
    - Enter the appropriate SMS host network **DNS Server** as specified by IT or enter 0.0.0.0.
15. Click “Accept”.

DHCP Configuration

The VMRC-2 initiates communications to the **mCIM** so configuring the VMRC-2 for DHCP will not affect SMS communications or operability and can be selected via the Network Settings menu as shown above.

> ***WARNING:*** *While using DHCP will not affect the ability of the controller to function with SMS, it might not be easy to determine the current IP address of a controller configured for DHCP without IT support. The controller IP address must be known to access the controller web configuration. Vanderbilt recommends using Reservations if using DHCP.*

SMS Communications Configuration

The VMRC-2 controller ships with default Host Communications configured for IP Server. The Host Communications settings must be changed for the controller to communicate to the SMS **mCIM**.

1. Select **Host Comm** from the menu to load the Host Communications configuration page.

2. Change Primary Host Port **Connection Type** to “IP Client”.

3. Change Primary Host Port **Data Security** to “TLS Required” if encryption communication is desired.

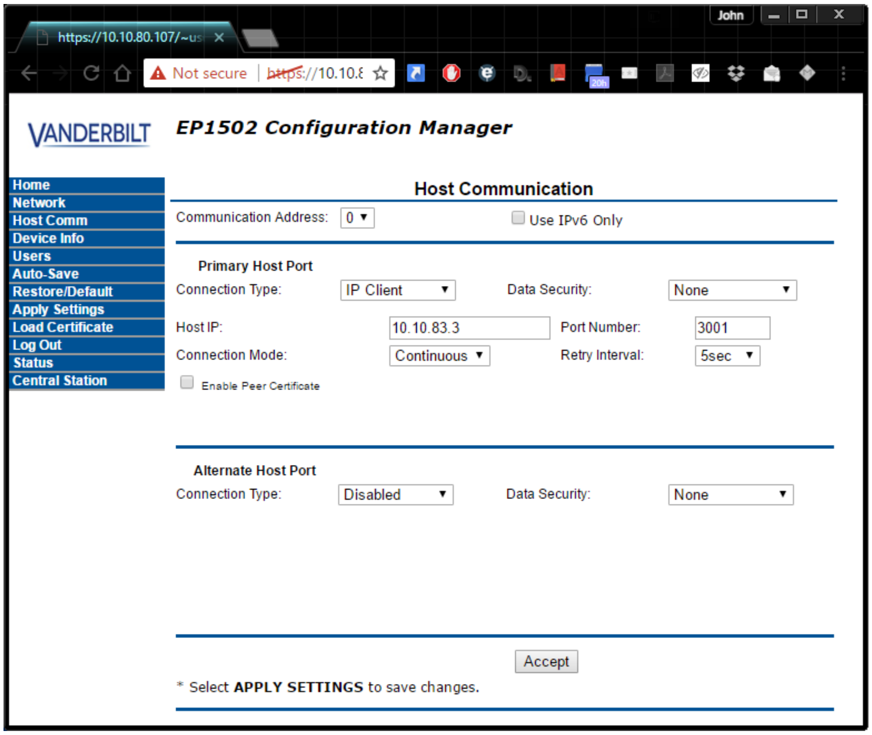
> *SMS Authentic Mercury protocol TLS encryption can only be enabled **per mCIM***

4. Change the Primary Host Port **Host IP** to the IP Address of the computer hosting the **mCIM**.

> *Vanderbilt recommends a dedicate **mCIM** host*
>
> *The **mCIM** Port defined in SMS **must match** the VMRC-2 Host Port setting*

5. Change the Primary Host Port **Port Number** to 5001, ***only if required***.

6. Do not change any other settings. SMS does not support the Alternate Host Port.



EP1502 Configuration Manager

Host Communication

Communication Address: 0 ▾ □ Use IPv6 Only

Primary Host Port

Connection Type: IP Client ▾ Data Security: None ▾

Host IP: 10.10.83.3 Port Number: 3001

Connection Mode: Continuous ▾ Retry Interval: 5sec ▾

□ Enable Peer Certificate

Alternate Host Port

Connection Type: Disabled ▾ Data Security: None ▾

* Select **APPLY SETTINGS** to save changes.

7. Click “Accept”.

Create User Account

Vanderbilt recommends creating at least 1 user account so that physical access to the controller for setting DIP Switch #1 is not required for accessing the controller configuration.

1. Select **Users** from the Menu.

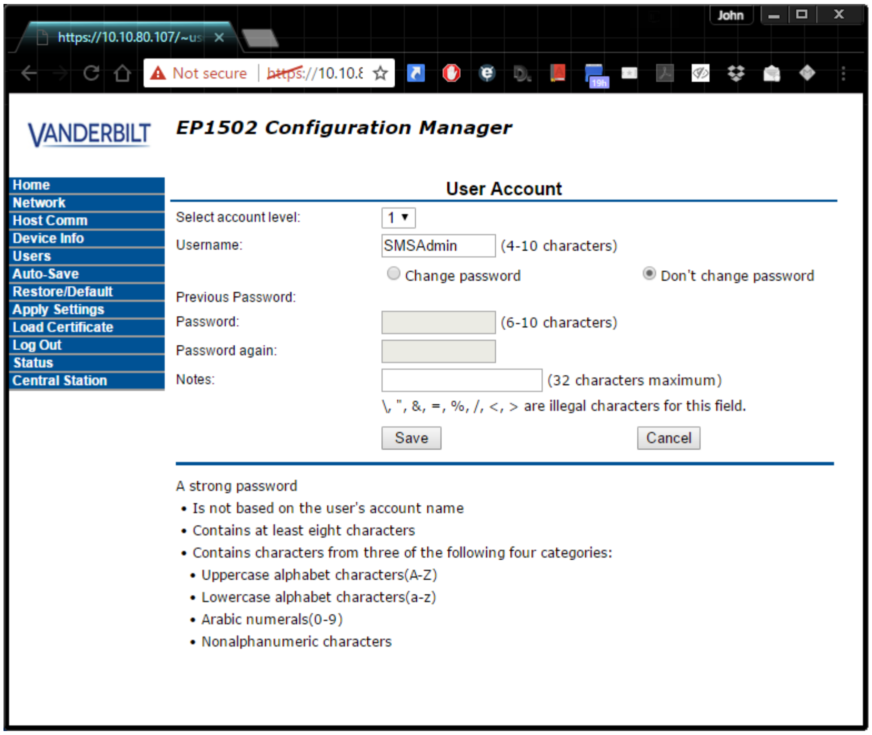
2. Click “New User”.

3. Leave “Select account level” = 1 (*administrator*)

4. Enter desired **Username**. Vanderbilt recommends SMSAdmin.

5. Enter desired **Password** and confirm.

6. Enter **Notes** if desired.



EP1502 Configuration Manager

User Account

Select account level: 1

Username: SMSAdmin (4-10 characters)

○ Change password ● Don't change password

Previous Password:

Password: (6-10 characters)

Password again:

Notes: (32 characters maximum)

\, ", &, =, %, /, <, > are illegal characters for this field.

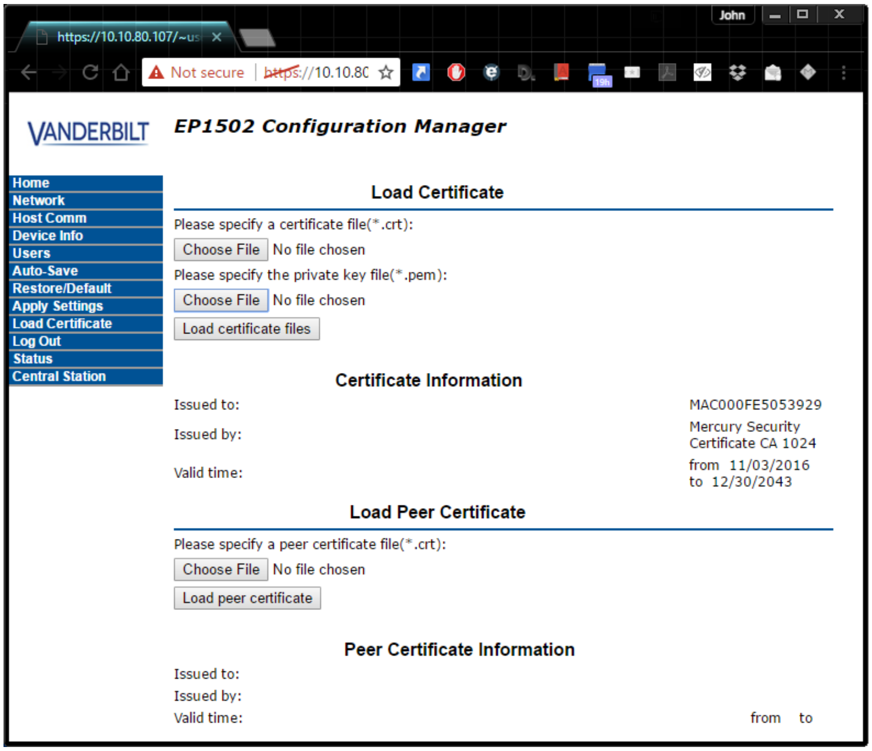
A strong password
- Is not based on the user's account name
- Contains at least eight characters
- Contains characters from three of the following four categories:
  - Uppercase alphabet characters(A-Z)
  - Lowercase alphabet characters(a-z)
  - Arabic numerals(0-9)
  - Nonalphanumeric characters

7. Click “Save”.

Upload Certificate

If TLS encryption will be enabled, a custom certificate may be downloaded to the controller which will be used in place of the Mercury provided self-signed certificate.

1. Select **Load Certificate** from the Menu.



EP1502 Configuration Manager

Load Certificate

Please specify a certificate file(*.crt):

Choose File No file chosen

Please specify the private key file(*.pem):

Choose File No file chosen

Certificate Information

Issued to:	MAC000FE5053929
Issued by:	Mercury Security Certificate CA 1024
Valid time:	from 11/03/2016 to 12/30/2043

Load Peer Certificate

Please specify a peer certificate file(*.crt):

Choose File No file chosen

Peer Certificate Information

Issued to:	
Issued by:	
Valid time:	from to

2. Click “Choose File” under “Please specify a certificate file” to specify the Certificate .crt file.

3. Click “Choose File” under “Please specify the private key file” to specify the Certificate Key .pem file.

4. Click “Load certificate files”.

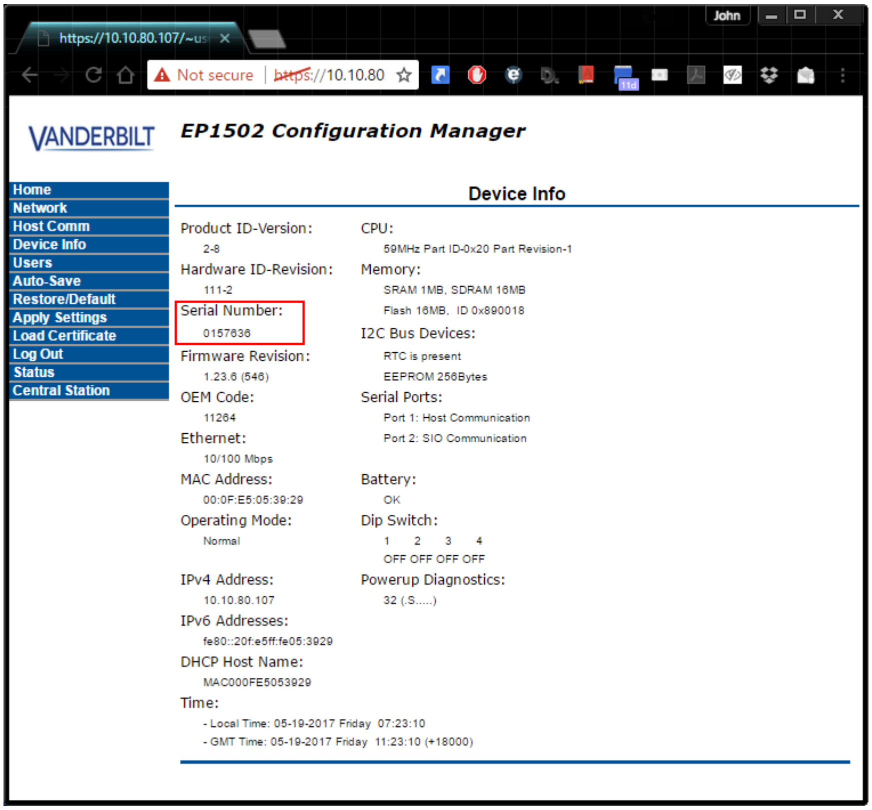
Document and Commit Configuration Changes

Once all desired configuration changes have been Accepted, they must be committed, and the controller rebooted to enable the new settings.

Prior to committing changes and rebooting the controller, Vanderbilt recommends saving a screen shot of the controller configuration and device specific information for documentation.

The controller Serial Number should be recorded – it is required for SMS configuration.

1. Select Device Info from the Menu.



EP1502 Configuration Manager

Device Info

Product ID-Version:
2-8

Hardware ID-Revision:
111-2

Serial Number:
0157636

Firmware Revision:
1.23.6 (546)

OEM Code:
11264

Ethernet:
10/100 Mbps

MAC Address:
00:0F:E5:05:39:29

Operating Mode:
Normal

IPv4 Address:
10.10.80.107

IPv6 Addresses:
fe80::20f:e5ff:fe05:3929

DHCP Host Name:
MAC000FE5053929

Time:
- Local Time: 05-19-2017 Friday 07:23:10
- GMT Time: 05-19-2017 Friday 11:23:10 (+18000)

CPU:
59MHz Part ID-0x20 Part Revision-1

Memory:
SRAM 1MB, SDRAM 16MB
Flash 16MB, ID 0x890018

I2C Bus Devices:
RTC is present
EEPROM 256Bytes

Serial Ports:
Port 1: Host Communication
Port 2: SIO Communication

Battery:
OK

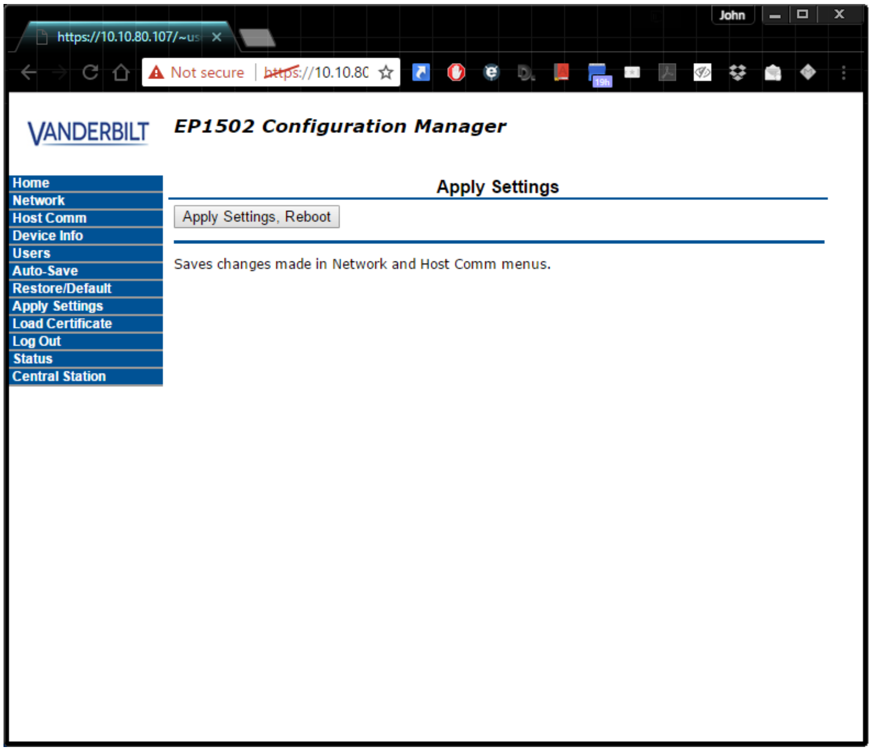
Dip Switch:
1 2 3 4
OFF OFF OFF OFF

Powerup Diagnostics:
32 (.S.....)

2. Save a screen shot or at least note the IP Address and Serial Number.

3. Click “Apply Settings” in the menu.

4. Click “Apply Settings, Reboot”.



EP1502 Configuration Manager

Apply Settings

Saves changes made in Network and Host Comm menus.

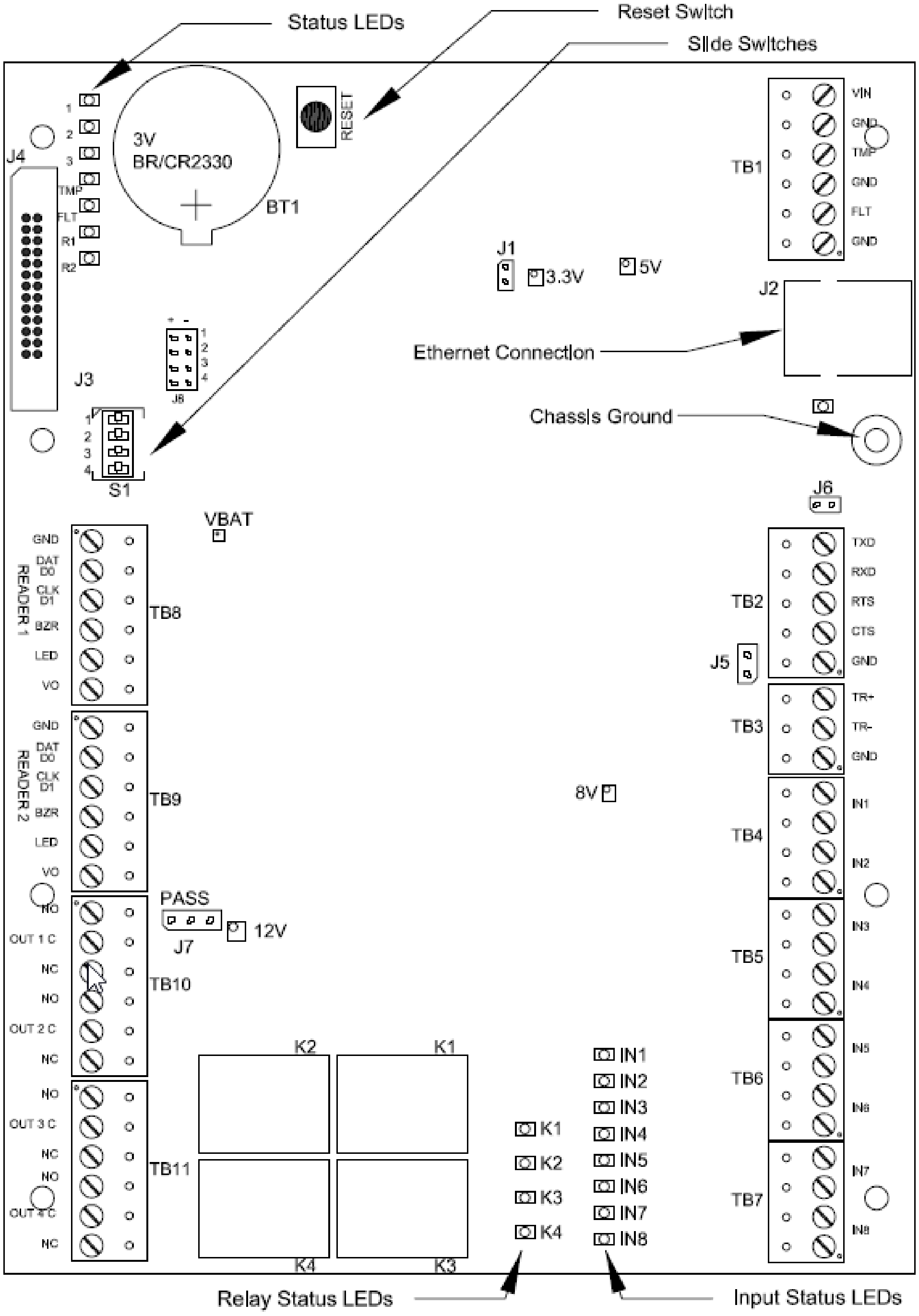
5. A page might display stating that the DIP Switches are not set for normal operation or no user accounts have been created. Select each checkbox and click “Yes”.

6. Controller configuration for SMS has been completed.

> *Ensure that SMS configuration for Data Security and Host Port Number are configured identically in SMS or the controller will not communication with the **mCIM***

7. Set all DIP Switches to OFF (normal operating mode).

Pin Layout


Status LEDs
Reset Switch
Slide Switches
1
2
3
TMP
FLT
R1
R2
J4
3V
BR/CR2330
BT1
RESET
TB1
VIN
GND
TMP
GND
FLT
GND
J1
3.3V
5V
J2
Ethernet Connection
+ -
1
2
3
4
J8
J3
1
2
3
4
S1
Chassis Ground
J6
VBAT
READER 1
GND
DAT D0
CLK D1
BZR
LED
VO
TB8
TB2
TXD
RXD
RTS
CTS
GND
J5
TB3
TR+
TR-
GND
READER 2
GND
DAT D0
CLK D1
BZR
LED
VO
TB9
8V
TB4
IN1
IN2
PASS
J7
12V
NO
OUT 1 C
NC
NO
OUT 2 C
NC
TB10
TB5
IN3
IN4
K2
K1
TB6
IN5
IN6
NO
OUT 3 C
NC
NO
OUT 4 C
NC
TB11
K1
K2
K3
K4
IN1
IN2
IN3
IN4
IN5
IN6
IN7
IN8
TB7
IN7
IN8
K4
K3
Relay Status LEDs
Input Status LEDs

Pin Functions

CONNECTION		
TB1-1	Power Fault Input	GND
TB1-2		FLT
TB1-3	Cabinet Tamper Input	GND
TB1-4		TMP
TB1-5	Power Input	GND
TB1-6		VIN: 12 to 24 VDC
TB3-1	SIO Port	GND
TB3-2	(2-wire RS-485)	TR-
TB3-3		TR+
TB4-1	Input 2	IN2
TB4-2		IN2
TB4-3	Input 1	IN1
TB4-4		IN1
TB5-1	Input 4	IN4
TB5-2		IN4
TB5-3	Input 3	IN3
TB5-4		IN3
TB6-1	Input 6	IN6
TB6-2		IN6
TB6-3	Input 5	IN5
TB6-4		IN5
TB7-1	Input 8	IN8
TB7-2		IN8
TB7-3	Input 7	IN7
TB7-4		IN7

CONNECTION		
TB8-1	Reader 1	GND: Ground
TB8-2		DAT/D0: Data/Data 0/TR-
TB8-3		CLK/D1: Clock/Data 1/TR+
TB8-4		BZR: Reader Buzzer
TB8-5		LED: Reader LED
TB8-6		VO: Reader Power
TB9-1	Reader 2	GND: Ground
TB9-2		DAT/D0: Data/Data 0/TR-
TB9-3		CLK/D1: Clock/Data 1/TR+
TB9-4		BZR: Reader Buzzer
TB9-5		LED: Reader LED
TB9-6		VO: Reader Power
TB10-1	Out 1	NO: Normally Open Contact
TB10-2		C: Common
TB10-3		NC: Normally Closed Contact
TB10-4	Out 2	NO: Normally Open Contact
TB10-5		C: Common
TB10-6		NC: Normally Closed Contact
TB11-1	Out 3	NO: Normally Open Contact
TB11-2		C: Common
TB11-3		NC: Normally Closed Contact
TB11-4	Out 4	NO: Normally Open Contact
TB11-5		C: Common
TB11-6		NC: Normally Closed Contact

Jumpers

JUMPERS	SET AT	DESCRIPTION
J1	N/A	Factory Use Only
J2	N/A	10-Base-T/100Base-Tx Ethernet Connection (Port 0)
J3	N/A	Factory Use Only
J4	N/A	Factory Use Only
J5	OFF	Port 2 RS-485 EOL Terminator is OFF
	ON	Port 2 RS-485 EOL Terminator is ON
J6	N/A	Factory Use Only
J7	Reader Power Select. **See Note 1**	
	12V	12 VDC at Reader Ports
	PASS	VIN "Pass Through" to Reader Ports
J8-1	N/A	Remote Status LED #1. See Note 2
J8-2	N/A	Remote Status LED #2. See Note 2
J8-3	N/A	Remote Status LED #3. See Note 2
J8-4	N/A	Remote Status LED #4. See Note 2

Note 1: The input power (VIN) must be 20 VDC minimum if the 12V selection is to be used.

Note 2: Observe POLARITY connection to LED. External current limiting is not required.

DIP Switches

The four switches on S1 DIP switch configure the operating mode of the VMRC-2 processor. DIP switches are read on power-up except where noted. Pressing switch S2 causes the VMRC-2 to reboot.

1	2	3	4	Definition
OFF	OFF	OFF	OFF	Normal operating mode.
ON	X	X	X	After initialization, enable default User Name (admin) and Password (password). The switch is read on the fly, no need to re-boot. See IT Security section for additional information.
OFF	ON	X	OFF	Use factory default communication parameters.
ON	ON	X	OFF	Use OEM default communication parameters. Contact system manufacture for details. See Bulk Erase below.
X	X	ON	X	Disable TLS secure link. Switch is read only when logging on.
ON	ON	OFF	OFF	Bulk Erase prompt mode at power up. See Bulk Erase below.

All other switch settings for unassigned and are reserved for future use. X = don't care.
In the factory or OEM default modes, downloaded configuration/database is not saved to flash memory.

Pins Not Used

CONNECTION		
TB2-1	Host Port 1 (RS-232)	GND
TB2-2		CTS
TB2-3		RTS
TB2-4		RXD
TB2-5		TXD

Cabinet Tamper and UPS Fault Input

There are two dedicated inputs for cabinet tamper and UPS fault monitoring. Normal (safe) condition is a closed contact. If these inputs are not used, install a jumper wire

Factory Reset

Follow the steps below to Bulk Erase Configuration memory for the VMRC-2.

This procedure should be attempted to performed to accomplish the following:

- Erase all configuration and cardholder database data (sanitize the controller)
- Recover from controller database corruption causing VMRC-2 to continuously reboot

If the procedure below does not correct the initialization issue, contact Vanderbilt Technical Support.

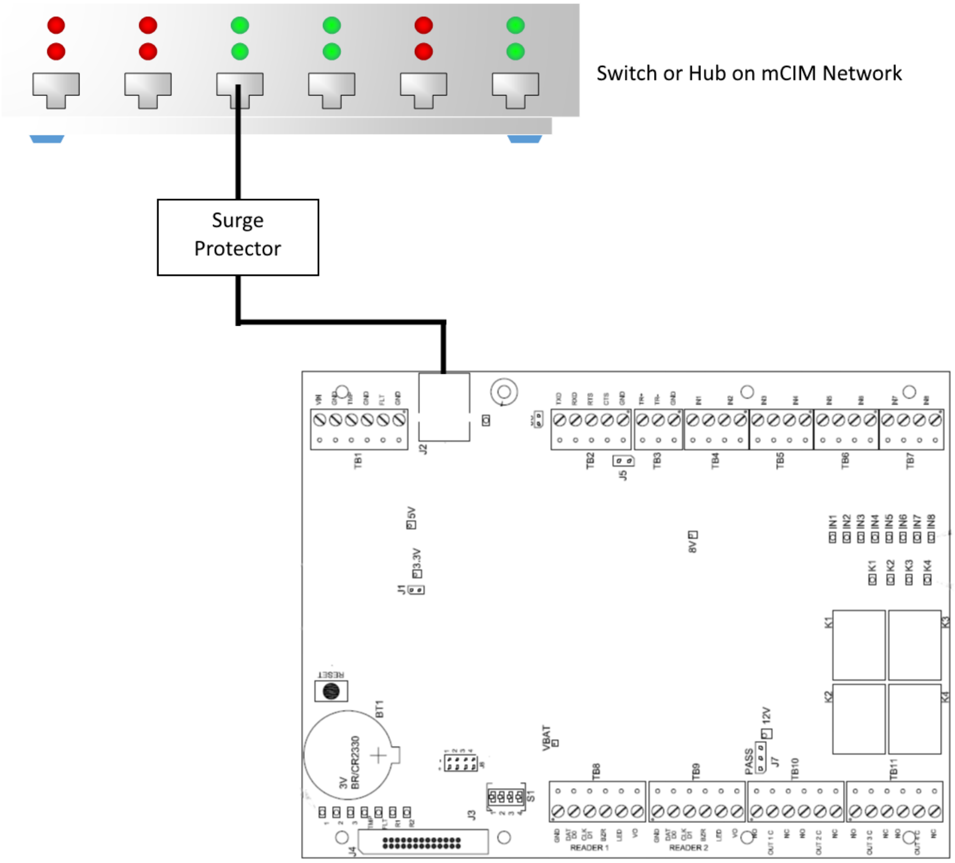
Do Not Remove Power During Steps 1 – 8 Below

9. Set S1 DIP switches to: 1 & 2 "ON", 3 & 4 "OFF".
10. Apply power to the VMRC-2.
11. Watch for LEDs 1 & 2 and 3 & 4 to alternately flash at a 0.5 second rate.
12. Within 10 seconds of powering up, change switches 1 or 2 to "OFF". If these switches are not changed, the VMRC-2 board will power up using the OEM default communication parameters.
13. LED 2 will flash indicating that the configuration memory is being erased.

14. Full memory erase takes up to 60 seconds.
15. When complete, only LEDs 1 & 4 will flash for 8 seconds.
16. The VMRC-2 will reboot 8 seconds after LEDs 1 & 4 stop flashing (no LEDs are on during this time).

Connecting VMRC-2 to mCIM

There is no direct connection between the VMRC-2 and the **mCIM**. To connect, they need to be on the same network and the proper IP address of the **mCIM** needs to be entered when setting up the VMRC-2. In addition, a data surge protector should be installed between the VMRC-2 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 connected the VMRC-2.



Data Communication between mCIM and VMRC-2

mCIM	VMRC-2
Ethernet To Network	Ethernet to Network

Connecting to Read Heads

The following sections how to install various credential read heads to the VMRC-2 reader interfaces.

The VMRC-2 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: VMRC-2 to Reader Head

Connection	Maximum Distance (ft)	Cable Recommendation
VMRC-2 to Magstripe Reader Head	200	18 AWG/5 Cond, Strd, Shld
VMRC-2 to Proximity Reader Head	500	18 AWG/5 Cond, Strd, Shld
VMRC-2 to Door Contact	2000	22 AWG/2 Cond, Strd, Shld
VMRC-2 to Exit Button	2000	22 AWG/2 Cond, Strd, Shld

Abbreviations:

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

PIN Connections

Reader 1

Reader 1 can be used to connect 1 card-reader to the VMRC-2:

- TB8-1 is Ground (GND)
- TB8-2 is DAT/D0 (Data 0)
- TB8-3 is CLK/D1 (Data 1)
- TB8-4 is Buzzer (14-24V)
- TB8-5 is LED
- TB8-6 is Power (V0)

Reader 1 has four contact points at TB4: 1 – 4 and TB5: 1 – 4. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

Reader 1 has two relay outputs at TB10: 1 – 6. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. TB10: 1 – 3 are for the Door Unlock relay. TB10: 4 – 6 are for the Door Held Open relay.

Reader 2

Reader 1 can be used to connect 1 card-reader to the VMRC-2:

- TB9-1 is Ground (GND)
- TB9-2 is DAT/D0 (Data 0)
- TB9-3 is CLK/D1 (Data 1)
- TB9-4 is Buzzer (14-24V)
- TB9-5 is LED
- TB9-6 is Power (V0)

Reader 1 has four contact points at TB6: 1 – 4 and TB7: 1 – 4. Each contact point has its own ground. Unsupervised door contacts have maximum wire length of 2,000 feet.

Reader 1 has two relay outputs at TB11: 1 – 6. The relays are single pole/double throw and are rated at 30 VDC @ 2 amp. TB11: 1 – 3 are for the Door Unlock relay. TB11: 4 – 6 are for the Door Held Open relay.

Proximity Reader

Wiegand / Proximity Read Head Pin Connections

VMRC-2	Proximity Reader
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	BEEPER (YELLOW); 12-24V
PIN 5 (LED)	LED (ORANGE)
PIN 6 (PWR)	POWER (RED)

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

VMR-5 Magnetic Strip - LED 1 Wire Configuration

VMR - 5 Magnetic Stripe - LED 1 Pin Connections

VMRC-2	VMR-5
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	NOT USED
PIN 5 (LED)	LED (BROWN)
PIN 6 (PWR)	POWER (RED)

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off

VMR-10 and VMR-20 Magnetic Stripe

VMR-10 and VMR-20 Magnetic Stripe Pin Connections

VSRC-M	VMR-10 and VMR-20
PIN 1 (GND)	GROUND (BLACK)
PIN 2 (DAT/D0)	DATA 0 (GREEN)
PIN 3 (CLK/D1)	DATA 1 (WHITE)
PIN 4 (BUZZER)	NOT USED
PIN 5 (LED)	LED (BROWN)
PIN 6 (PWR)	POWER (RED)

VMR-10 and VMR-20 Switch Settings

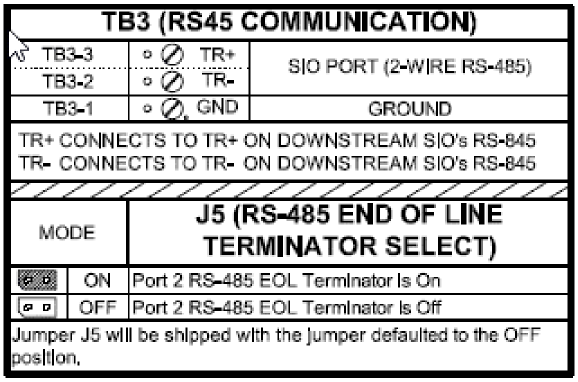
Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On

VMRC-2 Device Configuration

The VMRC-2 also has 1 RS-485 channel for devices and can support up to 32 Authentic Mercury serial I/O devices (SIOs).

The SIO communication port (TB3) is a 2-wire RS-485 interface which can be used to connect additional I/O panels. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,219 m). Use twisted pairs (minimum 24 AWG) with drain wire and shield for communication.



TB3 (RS45 COMMUNICATION)

TB3-3	TR+	SIO PORT (2-WIRE RS-485)
TB3-2	TR-	
TB3-1	GND	GROUND

TR+ CONNECTS TO TR+ ON DOWNSTREAM SIO's RS-845
TR- CONNECTS TO TR- ON DOWNSTREAM SIO's RS-845

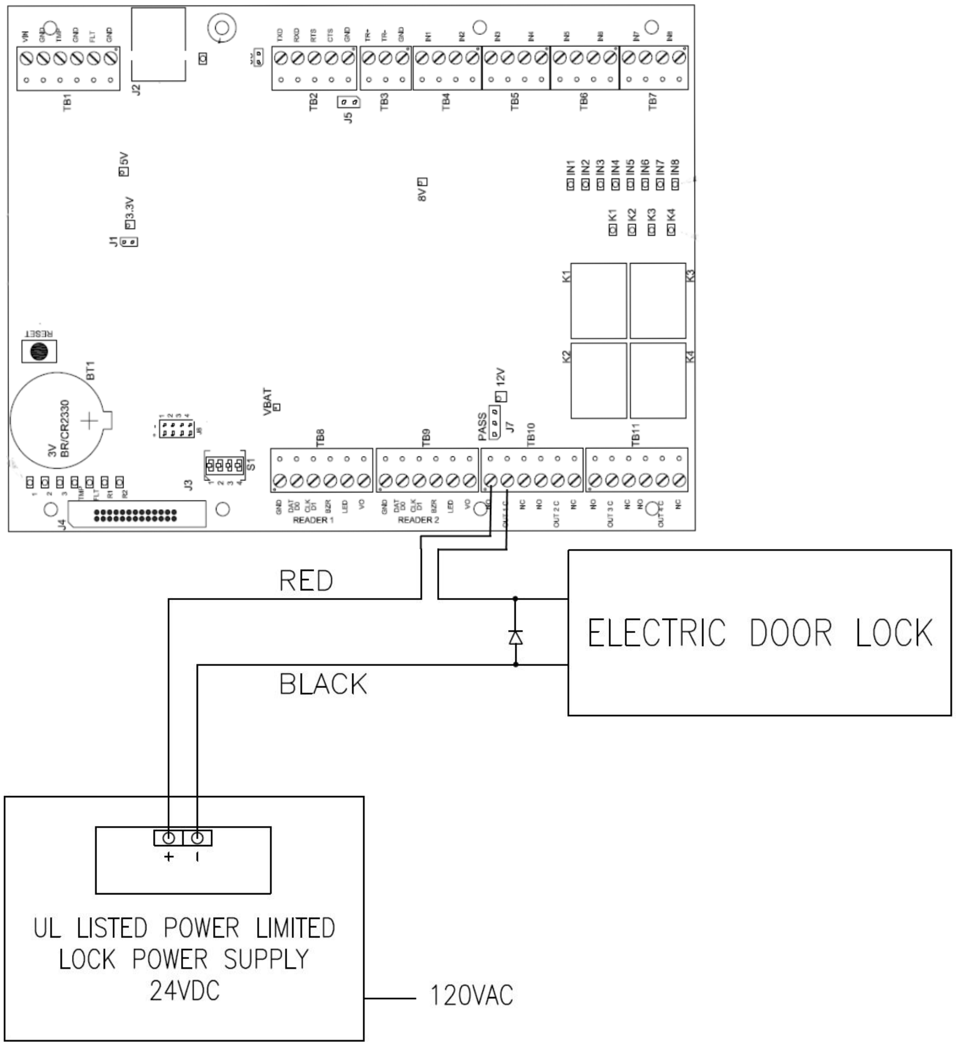
MODE		J5 (RS-485 END OF LINE TERMINATOR SELECT)
▨	ON	Port 2 RS-485 EOL Terminator Is On
□	OFF	Port 2 RS-485 EOL Terminator Is Off

Jumper J5 will be shipped with the jumper defaulted to the OFF position.

Install the termination jumper ONLY on the device at each end of the RS-485 bus. Failure to do so will compromise proper operation of the communications channel.

Installing Diodes for Lock Wiring - Relay

Diodes are supplied with the VMRC-2 which should be fitted across 12V and COM on each Reader Interface 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 relay K1 and K3 NO or NC depending on lock type: Fail Open / Fail Closed (*the diagram above is Fail Open to Relay K1 for Reader 1*).

CHAPTER 10

SRCNX (Legacy)

Reader Controller

Overview

The Vanderbilt legacy series of Reader Controllers -- SRCNX (Legacy) -- are intelligent devices that can be paired with any of the **Vanderbilt Security Management System** (SMS) software packages. The number of controllers and downstream devices are unlimited. The SRCNX (Legacy) Reader Controller is an independently programmable device which is capable of making decisions and storing history at the local level if communication is lost with the server. The SRCNX (Legacy) series include the SRCNX-2, SRCNX-8, and the SRCNX-16.

Highlights

- Communication between the SRCNX (Legacy) and the server (installed with **Vanderbilt SMS** software) can be directly wired to the serial port, an optional dial up modem, or an optional IP addressable module
- Dynamically allocated memory
- Firmware that can be flashed
- Enabled with a super cap to keep on board memory intact in case of a power failure
- Capable of adding a secondary dial-up alarm path when an IP configuration is used for added security (The SRCNX, in a dial up modem configuration, will dial the PC back before receiving any data)
- Communicates to the server when there is an alarm or when the transaction buffer is 75% full
- Can be used with a multitude of **Vanderbilt SMS** communication devices including the Vanderbilt reader interface modules (VRINX) which support read head technologies including Proximity, Magnetic Stripe, Wiegand, Barium Ferrite, bar code, smart card, biometric, keypad and other SMS compatible access control devices.

Standard on-board features

- 16 device capacity (devices include: SRCNX (Legacy), VRINX, VIONX-8, SIONX-24 and other SMS compatible access control devices.)
- Two 2 Amp output relays SP/DT and mechanically latching
- Eight supervised or unsupervised contact inputs
- 1MB RAM
- Full duplex RS-232 connection

SRCNX (Legacy) configuration guidelines

1 All SRCNX (Legacy) Reader Controllers have 8 communication channels. Each channel will support two Vanderbilt devices for a total of 16 devices. Only two identical devices may be connected to an individual channel.

2 Vanderbilt devices that may be connected directly to a SRCNX communication channel: SRCNX, VRINX, VIONX-8 and SIONX-24.

3 Other devices that may be connected directly to a SRCNX communication channel: Schlage wireless PIM400, Schlage wireless PIM-485, Schlage AD-300 Series Locks and Schlage VIP Locks.

4 The number after the SRCNX- X designates how many Vanderbilt 'NX' devices (SRCNX, VRINX, VIONX-8, or SIONX-24) can be connected to the reader controller. All channels are available for Schlage wireless PIM-485 devices and Schlage VIP Locks on any panel (as long as the channels have identical devices).

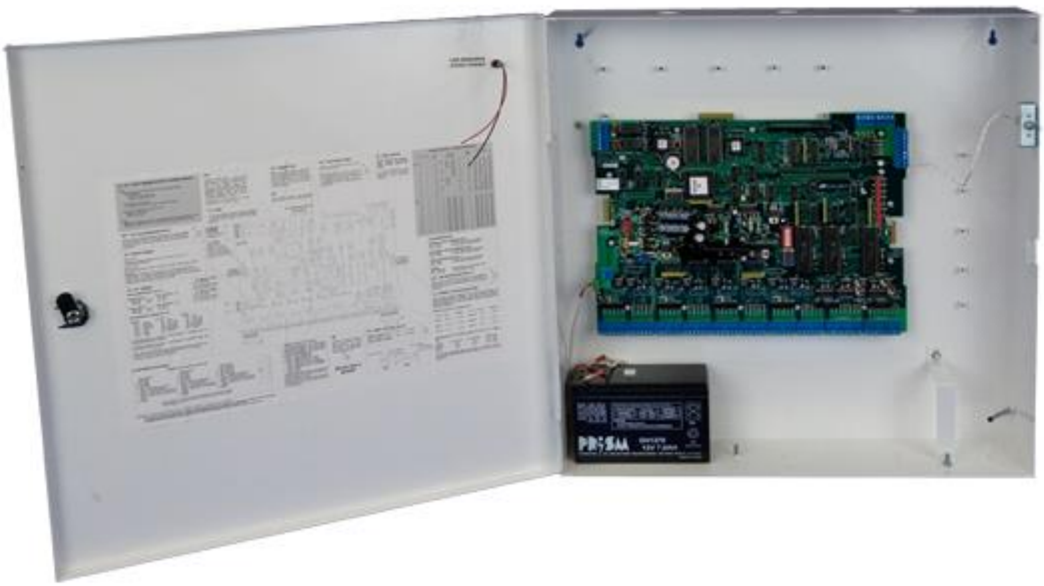
5 When Schlage wireless PIM400, Schlage wireless PIM-485, Schlage AD-300 Series or Schlage VIP devices are configured on a reader controller, you may not connect a satellite SRCNX to the main SRCNX.

Specifications

- Board Dimensions - 9-3/4" H x 13-1/2" W x 1-1/2" D (board only)
- Enclosure Dimensions - 20" x 20" x 4"
- Power Requirements - 16VAC, 4 amps (S16H-NX sold separately) or 24 VDC 4 amp power supply (sold separately)
- Power Consumption - (excluding peripheral devices) 600 mA
- Ambient Temperature - 0º to 49º C or 32º to 120º F
- Humidity - 10% to 85%
- Maximum Distance to PC - 50 feet via RS-232 data communication (see Recommended Wire Chart)
- SRCNX (Legacy) Fuse Replacement - 5 amps @ 250V slow blow 5 mm x 22 mm. Warning to reduce risk of fire, replace only with same type and rating fuse.

Standard Enclosure installation

SRCNX (Legacy) Standard Enclosure - An enclosure with a hinged door and a lock is included with your system for each SRCNX (Legacy) board. The tamper proof switch enables the system to send an alarm whenever someone opens the enclosure.



SRCNX (Legacy) Standard Enclosure

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: 20” x 20” x 4”
- One 12VDC - 7-amp hour gel cell battery for battery back-up is included

Environmental conditions

- Ambient Temperature - 0º to 49º C or 32º to 120º F
- The room must be dust free and clean
- 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 1-1/2” lag bolts

Optional equipment

Power Supply

Use a UL294 Power Limited Power Supply capable of four hours of standby battery power to supply power to the SRCNX (Legacy) reader controller. All peripheral devices: locks, PIR’s, local annunciators, etc. must be powered separately.

VRINX reader interface

The reader interface units communicate the data between the read-head and the SRCNX (Legacy) reader controller via RS-485 protocol. The VRINX connects to one of the communication channels on the SRCNX. See VRINX chapter for addition information and features.

Features

- One read-head communication port
- Four supervised or unsupervised contact inputs
- On board Tamper Connection
- 2 Form ‘C’ single pole/double throw 1 amp relay output
- Can be power from the SRCNX (refer to Recommended Wire Chart)
- Enclosure Dimensions: 8-1/4” x 7-1/2” x 3-1/2”
- Metal enclosure with hinged door, and dual screw closure
- Tamper Switch, lock & key option available

VIONX-8 expansion module

This module provides additional contact inputs and relay outputs. The VIONX-8 connects to one of the communication channels on the SRCNX (Legacy). The VIONX-8 can be powered from the SRCNX reader controller. See the VIONX-8 chapter for more details.

Features

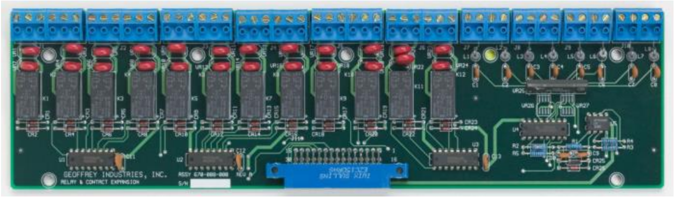
- 8 output relays - 1-amp SP/DT relays (single pole/double throw)
- 8 Contact inputs supervised or unsupervised
- Enclosure Dimensions - 8 1/4" x 7 1/2" x 3 1/2"
- Metal enclosure with hinged door and dual screw closure
- Tamper switch, lock & key option available

SIONX (Legacy) expansion module

This module provides additional contact inputs and relay outputs. This board snaps onto the SRCNX (Legacy) reader controller. Only one SIONX can be attached to a SRCNX board.

Features

- 12 output relays - 2-amp SP/DT (single pole/double throw)
- Eight input contacts supervised or unsupervised
- Dimensions - 11”W x 3”D



SIONX-24 (Legacy) expansion module

This module provides additional contact inputs and relay outputs. The SIONX-24 connects to one of the communication channels on the SRCNX (Legacy). The SIONX-24 can be powered from the SRCNX reader controller. See SIONX-24 chapter for more details.

Features

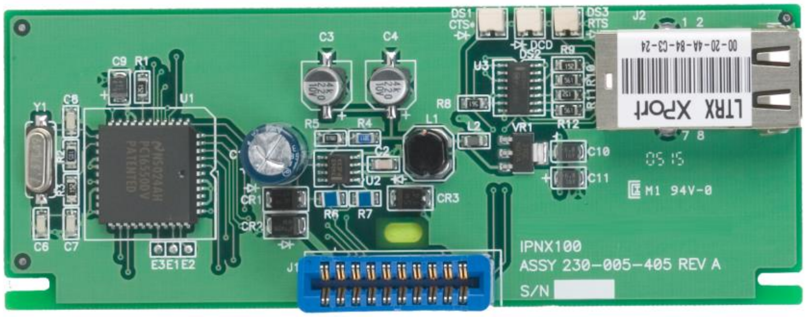
- 24 output relays - 2-amp SP/DT relays (single pole/double throw)
- 24 Contact inputs supervised or unsupervised
- Enclosure Dimensions - 12” x 12” x 4”
- Metal enclosure with hinged door, tamper switch, lock and key

SMODNX (Legacy) dial-up modem

Provides communication through a standard telephone line. This board snaps onto the SRCNX (Legacy) reader controller. Only one SMODNX module per SRCNX. Dimensions: 5 1/4” W x 2” D

SIPNX-100 (Legacy) IP addressable module

Provides communication through an ethernet LAN. This board snaps onto the SRCNX (Legacy) reader controller. Only one SIPNX-100 module can be attached to one SRCNX. Dimensions: 5 1/4” W x 2” D



SMEMNX-3 (Legacy) and SMEMNX-7 (Legacy) memory expansion modules

Provides expanded memory on the SRCNX (Legacy) for additional card holders and areas. These boards snap onto the SRCNX reader controller. Only one memory module per SRCNX. Dimensions: 2 1/2” H x 5 1/2” W x 3/8” D

- SMEMNX-3 provides an additional 3 MB memory
- SMEMNX-7 provides an additional 7 MB memory

System overview

Vanderbilt SMS is modular and extremely versatile. There are many combinations to correctly configure your Security Management System.

Vanderbilt SMS delivers four levels of powerful software packages that will integrate access control, digital video and alarm monitoring.

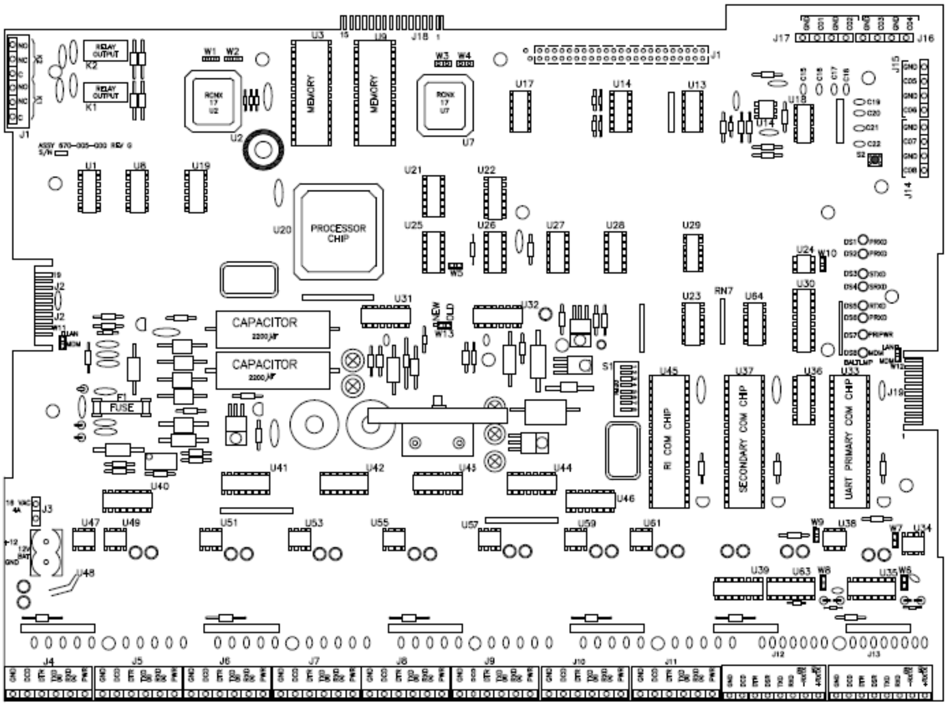
The Communication Interface Module (CIM) is a program designed to issue all database changes and gather information from the Reader Controller (VRCNX-R, VSRC, and SRCNX-Legacy). The CIM stores the information in the proper history files. Communication between CIM and the Reader Controller is via TCP/IP protocol, RS-232 protocol or a legacy dial up modem.

If your system has multiple PC’s and multiple Reader Controllers, the system can be configured using a TCP/IP network connection between devices.

The legacy Reader Controller (SRCNX) can be configured for redundant communication back to the server/ CIM, using a network connection module and a dial up modem as a back-up.

The legacy Reader Controller (SRCNX) can be designed to use a multiplex or daisy chain configuration if a network is not available. Configure the SRCNX that communicates (through RS-232) with the CIM as a Main Controller (MC). This MC will provide information to the other satellite SRCNX boards in the system. The communication between the MC and other satellite SRCNX boards is via RS-485 protocol.

SRCNX (Legacy) reader controller pin layout



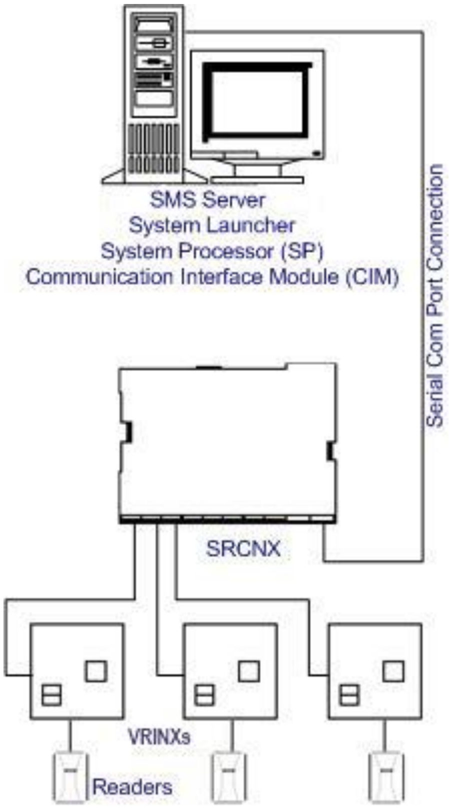
System communication options

Communication between the SRCNX (Legacy) and the CIM can be established in various ways.

1. SRCNX direct connection to the server/CIM via RS-232 protocol.
2. SIPNX-100 network connection via TCP/IP communication protocol
3. SMODNX dial-up modem connection via telephone lines
4. Network Communication with Redundant Alarm Back-up

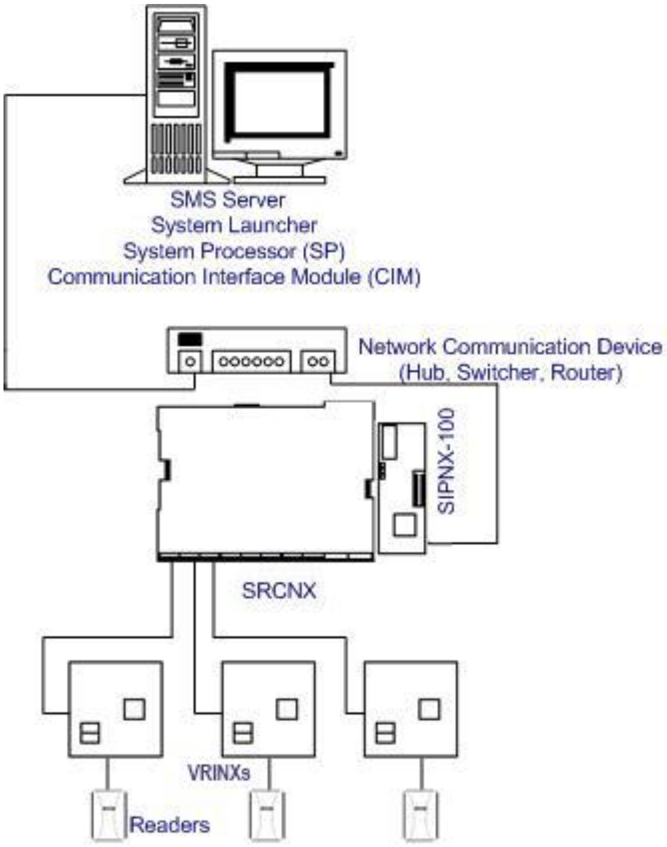
RS-232 direct connection to the server (CIM)

One SRCNX (Legacy) board can be connected directly to a serial port (COM) on the server via a cable for RS-232 communication protocol (see Recommended Wire Chart). This cable has an 8-pin connector on one end which should be connected to J13 on the SRCNX board. The DB-25 or DB-9 connector at the other end should be plugged into the server serial port. The maximum distance between the SRCNX and the PC is 50 feet.



SIPNX-100 network communication

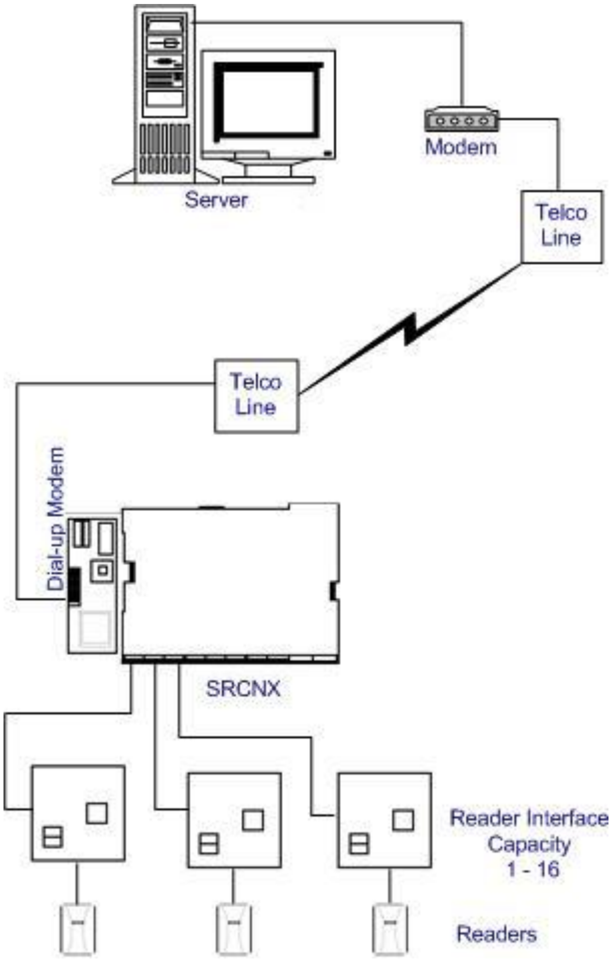
The SRCNX (Legacy) can communicate to the server via an IP addressable module (SIPNX-100) using a network cable. The SIPNX-100 module is connected to J19 on the SRCNX board. One end of the network cable should be inserted to the SIPNX-100 module and the other end of the cable should be plugged into the network or network device. The diagram below illustrates this type of configuration.



SMODNX - dial-up modem communication

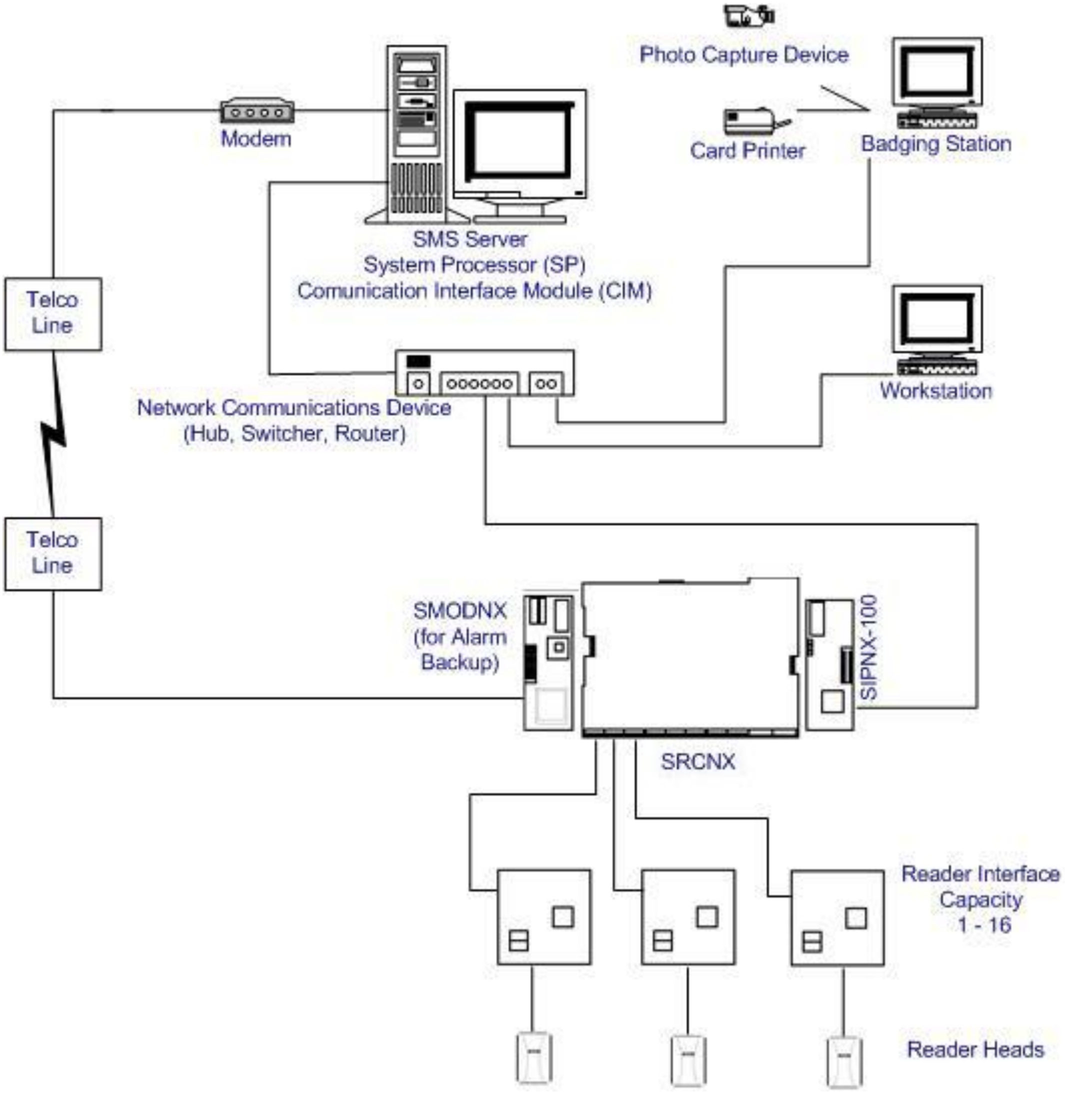
When using the SMODNX modem for data communication, be sure to purchase high quality proprietary cable (22 AWG /5 Cond) for connecting to the modem of your server. Connect the SMODNX modem to J2 of the SRCNX (Legacy) board. One end of the cable into the SMODNX and the other into a standard telephone jack for 2400 baud communication.

The PC can use an internal or external modem. If an external modem is used at the server, use a DB-25 modem cable for connecting modem and the PC serial (COM) port. The maximum distance between the modem and the server should be 50 feet.



Network communication with redundant alarm back-up

It is possible that your system communication can be affected by various network interruptions. If a redundant means of communication is installed, interruptions can be avoided, alarms will be received through dial-up modem communication.



Main Controller (SRCNX - Legacy) configuration

The SRCNX (Legacy) can be configured as a Main Controller that can control a maximum of 16 additional SRCNX reader controllers.

Data communication between main and a satellite SRCNX's can be a multiplex or a daisy chain configuration.

Main and satellite SRCNX's are connected to each other via an RS-485 communication protocol. Wire runs are limited to 4,000 feet (Data Only) from the main controller to satellite SRCNX. (see Recommended Wire Chart).

A reader controller that has Schlage VIP Lock or Schlage wireless devices cannot be configured as a main controller. These Schlage devices must be connected to a satellite SRCNX reader controller.

Multiplex configuration

In a multiplex configuration the SRCNX (Legacy) reader controllers are connected to the communication channels J 4 to J 11 on the main SRCNX board in parallel. A maximum of 16 devices can be connected in this manner.

Note: Identical devices must be connected on the same channel. You cannot mix devices on the same channel.

Daisy chain configuration

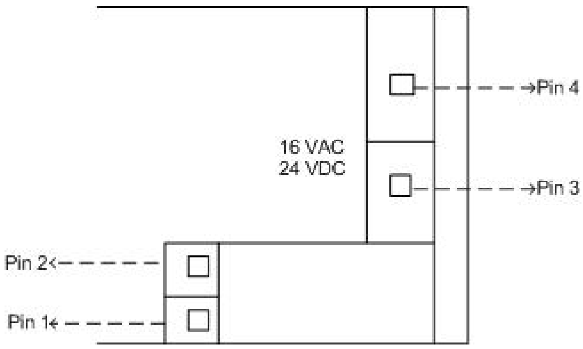
In a daisy chain configuration, the SRCNX (Legacy) reader controllers are connected to one another in series. Up to 16 devices can be connected to a main SRCNX controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the SRCNX.

SRCNX (Legacy) reader controller pin functions

J3 - Power source

Provides power to the SRCNX (Legacy) and battery back-up. Pins 1 & 2 are for the battery charging circuit (12VDC) only. Pin 1 is (-) and Pin 2 is (+); be polarity conscious.

Pins 3 & 4 are for power input (16VAC or 24VDC @ 4 amps). Polarity does not affect these Pins 3 & 4.



F1- Fuse

F1 fuse provides current limiting protection in the event of overloading the SRCNX (Legacy) power supply.

SRCNX Fuse Replacement: 5 amp @ 250V slow blow 5mm x 22mm.

Warning: To reduce risk of fire, replace only with same type and rating fuse.

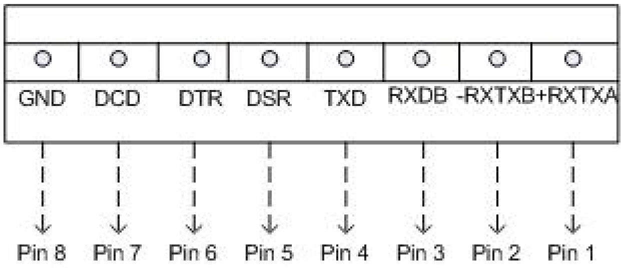
S2- Reset switch

The Reset Switch clears all the memory on the SRCNX (Legacy) reader controller. Press the reset switch for 3 seconds to clear the memory.

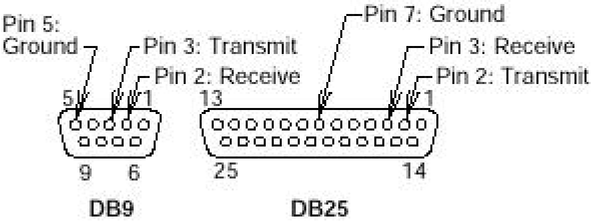
Note: Make sure that there is power to SRCNX reader controller. (J3)

J13 - Primary data communication port

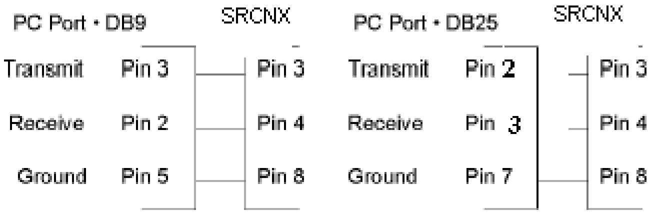
Communication between SRCNX (Legacy) board and the server (CIM) is via RS232 protocol.



J13 Primary Communication Port on the SRCNX



Pin assignments for cable connected to J13

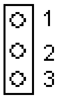


PC Port - DB9		SRCNX	PC Port - DB25		SRCNX
Transmit	Pin 3	Pin 3	Transmit	Pin 2	Pin 3
Receive	Pin 2	Pin 4	Receive	Pin 3	Pin 4
Ground	Pin 5	Pin 8	Ground	Pin 7	Pin 8

Pin assignments for cable connected to J13

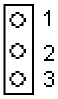
W7 - Communication protocol on J13

To configure a main controller the jumper should be on Pins 2 & 3 for RS-232 communication protocol. The satellite SRCNX (Legacy) jumper should be on Pins 1 & 2 for RS-485 communication protocol.



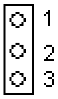
W9 - Secondary communication port protocol on J12

The secondary communication port is for diagnostics and troubleshooting. To configure the secondary communication port (J12) the jumper should be on Pins 2 & 3 for RS-232 communication protocol.



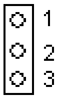
W 10 - Watchdog timer

Under normal conditions the jumper should be on Pins 2 and 3. When the jumper is on Pins 1 and 2, the debugging mode is activated. This mode is recommended for troubleshooting only. When the jumper is on Pins 1 and 2, the watchdog timer is disabled, the SRCNX (Legacy) board cannot reset itself.



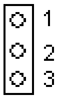
W11 - Voltage selector for J2 (Dial-up Modem)

When using the SMODNX dial-up modem module the jumper must be across Pins 2 & 3 to supply 5 VDC to connector J2. Serious damage could result if this jumper is placed incorrectly.



W12 - Voltage selector for J19 (IP Module)

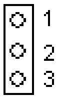
When using the SIPNX-100 IP addressable module the jumper must be across Pins 2 & 3 to supply 12VDC to connector J19. Serious damage could result if this jumper is placed incorrectly.



W13 - Voltage selector for Reader Interfaces (VRINX)

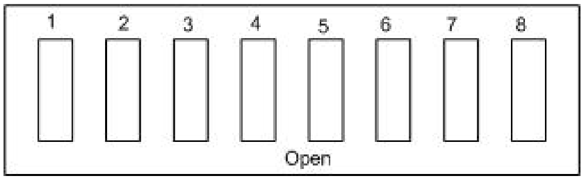
When using the VRINX reader interfaces the jumper must be across Pins 1 & 2 to supply 24VDC, and Pins 2 & 3 to supply 12 VDC.

Note: Older HC11 reader interfaces the jumpers need to be across Pins 2 & 3. The VRINX and the HC11 reader interfaces can be mixed on the same SRCNX (Legacy) reader controller but must be on separate channels and the jumper must be across Pins 1 & 2.



S1 Dip switch setting

Pins 1 through 4 are not applicable on the main controller.



S1 Dip Switch Settings for the Main Controller

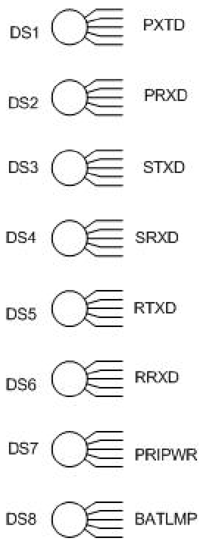
	1	2	3	4	5	6	7	8
MC	N/A	N/A	N/A	N/A	**Open** - Global Antipassback and Global Relay Control. **Closed** - Local Antipassback	**Open** - 38,400 baud comm. to SRCNX **Closed** - 9600 baud comm. to VRINX satellite SRCNX	**Open** - 38400 Baud comm. to CIM/MC **Closed -** 9600 baud comm. to CIM/MC	**Closed -**MC **Open** -SRCNX

Note: Switch 6 on the main controller should match with switch 7 on the satellite SRCNX.

S1 Dip Switch Settings for a satellite SRCNX Connected to a Main Controller

Conn	Chan	Addr. A	S1 Dip Switch Settings	Addr. B	S1 Switches (1 2 3 4)
J 4	1	1 2	CL CL CL CL OP CL CL CL	1	CL CL CL CL
J5	2	1 2	CL CL CL CL OP CL CL CL	2	OP CL CL CL
J6	3	1 2	CL CL CL CL OP CL CL CL	3	CL OP CL CL
J7	4	1 2	CL CL CL CL OP CL CL CL	4	OP OP CL CL
J8	5	1 2	CL CL CL CL OP CL CL CL	5	CL CL OP CL
J9	6	1 2	CL CL CL CL OP CL CL CL	6	OP CL OP CL
J10	7	1 2	CL CL CL CL OP CL CL CL	7	CL OP OP CL
J11	8	1 2	CL CL CL CL OP CL CL CL	8	OP OP OP CL

LED Description



Main Controller SRCNX Communication

DS1 – PTXD On when data is being transmitted

DS2 – PRXD On when data is being received

Reserved for Secondary Communication Port

DS3 – STXD Reserved for diagnostic communication

DS4 – SRXD Reserved for diagnostic communication

VRINX (Reader Interface) Communication

DS5 – RTXD On when data is being transmitted

DS6 – RRXD On when data is being received

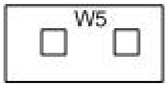
Power

DS7 – PRIPWR Primary Power – should always be on

DS8 – BATLMP Indicates battery power

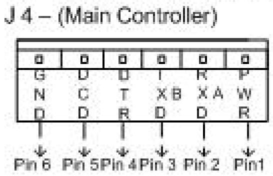
W 5 - EEPROM Flash Enable

The jumper on W5 enables the EEPROM flash chips U2 & U7 to be programmed on site.

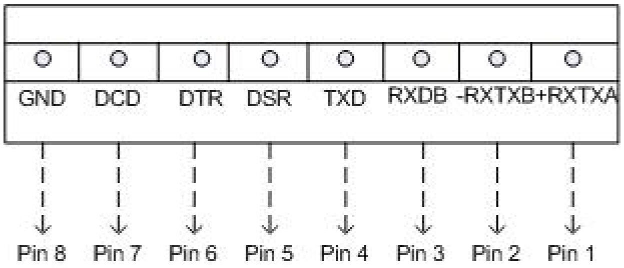


J 4 - J 11 - Data communication channels (satellite SRCNX)

Communication between a main SRCNX controller and a satellite SRCNX controller.



MC (J 13) - Satellite SRCNX



Data Communication between main controller and satellite SRCNX

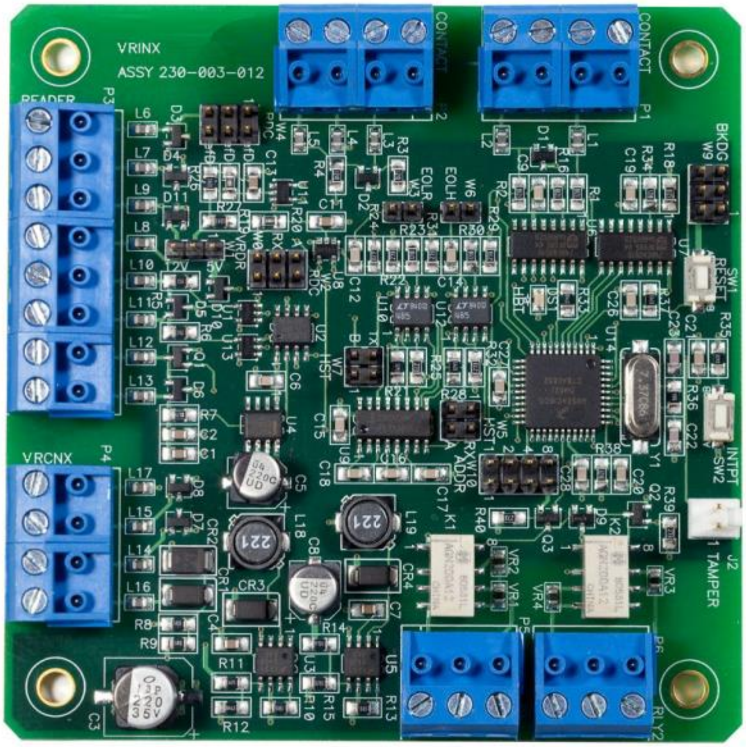
Main Controller (MC)	Satellite SRCNX
Pin 1 PWR - N/A	
Pin 2 RXD (A)	Pin 1 RXTX (A)
Pin 3 TXD (B)	Pin 2 RXTX (B)

Note: Other pins are not applicable.

Disclaimer: Pins J4 to J11 are rated at 240 mA per channel. The devices that are connected to pins J4 to J11 that exceed 240 mA per channel are not UL evaluated.

CHAPTER 11

VRINX



Reader Interface

Overview

The VRINX is a Reader Interface between the Reader Controllers and Card Readers. The VRINX works similarly to the legacy version, with only some minor changes to pin layout. The VRINX offers a cost-effective, modular approach to access control system design. Reader Interfaces can be used in small systems with one reader and large systems with thousands of readers. The VRINX Reader Interface is supported by the entire family of Vanderbilt reader controllers.

Highlights

- Supports various read head technologies; Proximity, Magnetic Stripe, barcode, Wiegand, iButton, barium ferrite, smart card, biometric and more
- Supported by the entire family of Vanderbilt Reader Controllers
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and the Reader Controller
- Can be powered directly from the VRCNX-R or separately (depending on type and length of wire, refer the Recommended Wire Chart) by a 24VDC Rated 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 VRCNX-R, VRCNX-M or VRCNX-A Reader Controllers
- Includes Two 1 amp, form C, single pole/double throw, mechanically latching relays
- Four 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 - 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 - 14VDC - 24 VDC (usually supplied from the VRCNX-R/M/A Reader Controller)
- Power consumption - 120mA max (without reader)
- Ambient temperature - 0º to 49º C or 32º to 120º F

VRINX Enclosure

VRINX 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”

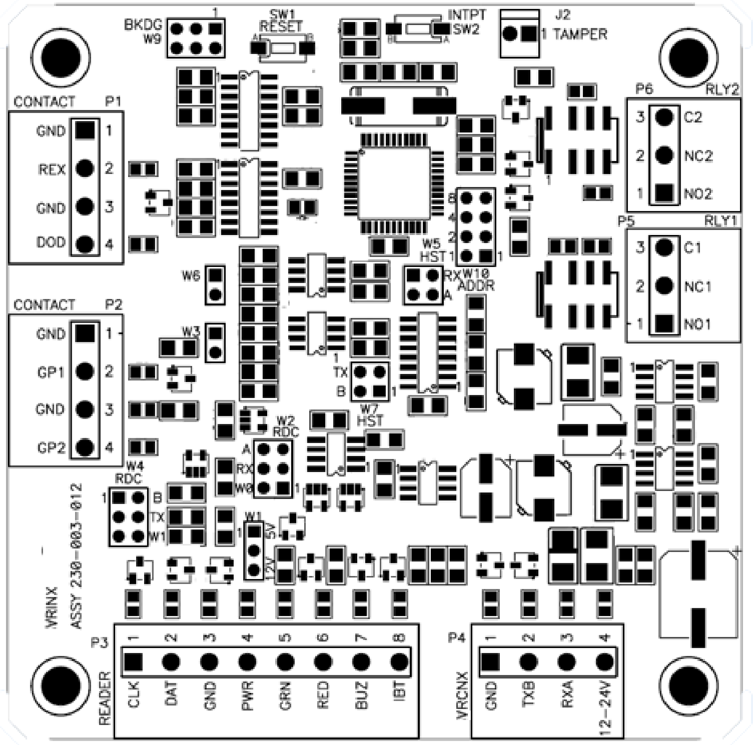
Environmental conditions

- 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.

VRINX pin layout



VRINX configuration

The VRINX will be connected to the Reader Controller VRCNX-R via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one VRCNX-R reader controller. Wire runs are limited to 4,000 feet (Data Only) from the main controller to a VRINX. (see Recommended Wire Chart). Data communication between reader controller and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration the VRINX boards are connected to channels J 4 to J 11 on the VRCNX-R board in parallel. A maximum of 16 VRINX boards can be connected in this manner.

Note: Only identical devices can be connected on the same channel on the VRCNX-R.

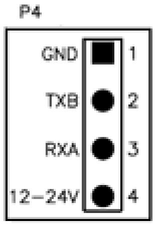
Daisy chain configuration

In a daisy chain configuration, the VRINX reader interfaces are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R/M/A.

VRINX pin functions

P 4 - Power source and communication wiring

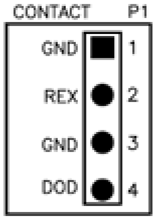
Provides power and communication to the VRINX from the VRCNX-R.

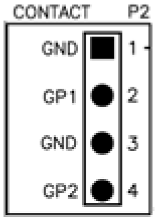


- Pin 1 is Ground (GND)
- Pin 2 is Data B (TXB)
- Pin 3 is Data A (RXA)
- Pin 4 is Power (12-24V)

P1/P2 - Contact inputs

The VRINX has four supervised or unsupervised contact points, two at P1 and two at P2. Each contact point has its own ground. Supervised door contacts have maximum wire length of 1,000 ft. Unsupervised door contacts have maximum wire length of 2,000 feet.





P1

- Pin 1 is Ground
- Pin 2 is Request to Exit (REX)
- Pin 3 is Ground
- Pin 4 is Door Open Detect (DOD)

P2

- Pin 1 is Ground
- Pin 2 is Auxiliary Input (GP1)
- Pin 3 is Ground
- Pin 4 is Auxiliary Input (GP2) (If the IPB function is in use then Pin 4 is for the IPB)

W 1 - 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

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

W2/W4 - P3 Communication Configuration

W2 and W4 determine whether P3 is for Credential, RS232, or RS485 communication. Default setting is for Credential communication. See the table below for details.

Communication Type	Jumpers on W2	Jumpers on W4
Credential (default)	1 & 2	5 & 6
RS232	3 & 4	3 & 4
RS485	1 & 2	1 & 2

W5/W7 - P4 Communication Configuration

W5 and W7 determine whether P4 is for RS232 or RS485 communication. Default setting is for RS485 communication. See the table below for details.

Communication Type	Jumpers on W5	Jumpers on W7
RS485 (default)	3 & 4	1 & 2
RS232	1 & 2	3 & 4

W 10 - VRINX Reader Interface Addressing

The address of the VRINX is dependent on the position of jumpers on these pins. Please see the section on Addressing VRINX for more details.

W3 - RS485 Communication Line Terminator

W3 is the P3 Pin1/Pin2 RS485 Communication Line Terminator.

W6 - RS485 Communication Line Terminator

W6 is the P4 Pin2/Pin3 RS485 Communication Line Terminator.

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 VRINX. Press the reset switch for 3 seconds to clear the memory.

Note: Make sure that there is power on VRINX (P4)

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

SW2 - Software Reset Switch

Recommended for factory use only.

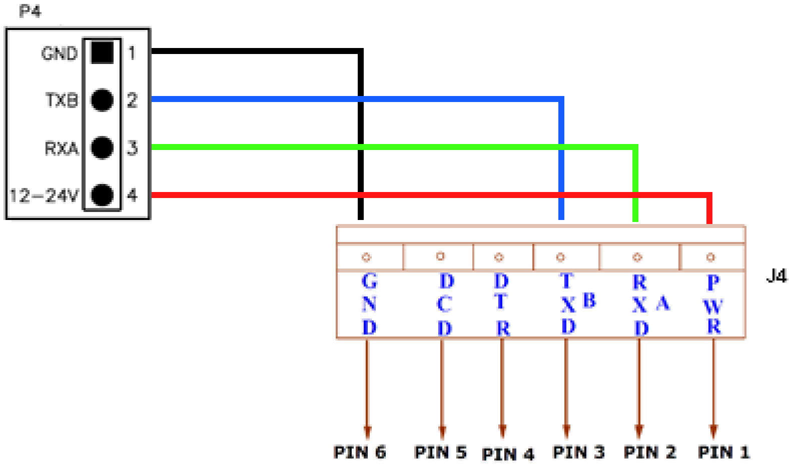
Pins not Used

W9 - BKDG: No jumper required for normal operation.

Connecting to VRCNX-R

Communication between a VRCNX-R reader controller and a VRINX reader interface is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R board and P4 on VRINX. In the following example we have selected J4 on the VRCNX-R board.

Note: Only identical devices are allowed on same channels.

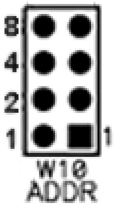


Data communication between VRINX and VRCNX-R

VRINX P4	VRCNX-R J4
Pin 1 - GND	Pin 6 - GND
Pin 3 - RXA	Pin 2 - RXD (A)
Pin 2 - TXB	Pin 3 - TXD B
Pin 4 - Power	Pin 1 - Power
No connection	Pin 4 - DTR
No connection	Pin 5 - DCD

Addressing the VRINX

W10 on the VRINX consists of four jumpers that can be combined to set the address for the device. Make a note of the address of the VRINX and which channel it is connected to. This information will be required to set up the lock in the software.



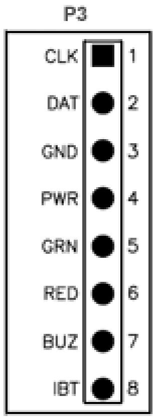
VRINX Address Chart

VRINX Address	Jumper Locations	VRINX 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

Read head wiring instructions

The VRINX reader interface can communicate to many different read heads. We have provided the pin outs for the most commonly used read-heads. The connection is different for each reader type. Please refer to the Recommended Wire Chart for the proper wire and lengths.

P 3 - VRINX pin connections



Proximity Reader

Proximity Read Head Pin Connections

VRINX	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

Wiegand Reader

Wiegand Read Head Pin Connections

VRINX	Wiegand 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 (BROWN)
Pin 6 (RED)	NOT USED
Pin 7 (IBT)	NOT USED

VMR - 5 Magnetic Stripe - LED 1 wire configuration

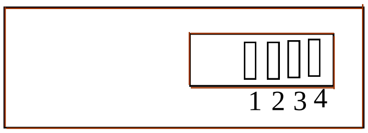
VMR - 5 Magnetic Stripe - LED 1 Pin Connections

VRINX	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (IBT)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off



VMR - 5 Magnetic Stripe - LED 2 wire configuration

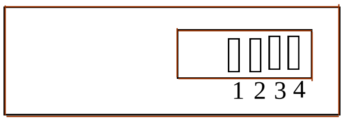
VMR - 5 Magnetic Stripe - -LED 2 Pin Connections

VRINX	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (IBT)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = Off S4 = Off



VMR-10 and VMR-20 Magnetic Stripe

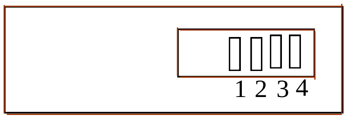
VMR-10 and VMR-20 Magnetic Stripe Pin Connections

VRINX	VMR-10 and VMR-20
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (IBT)	NOT USED

VMR-10 and VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On



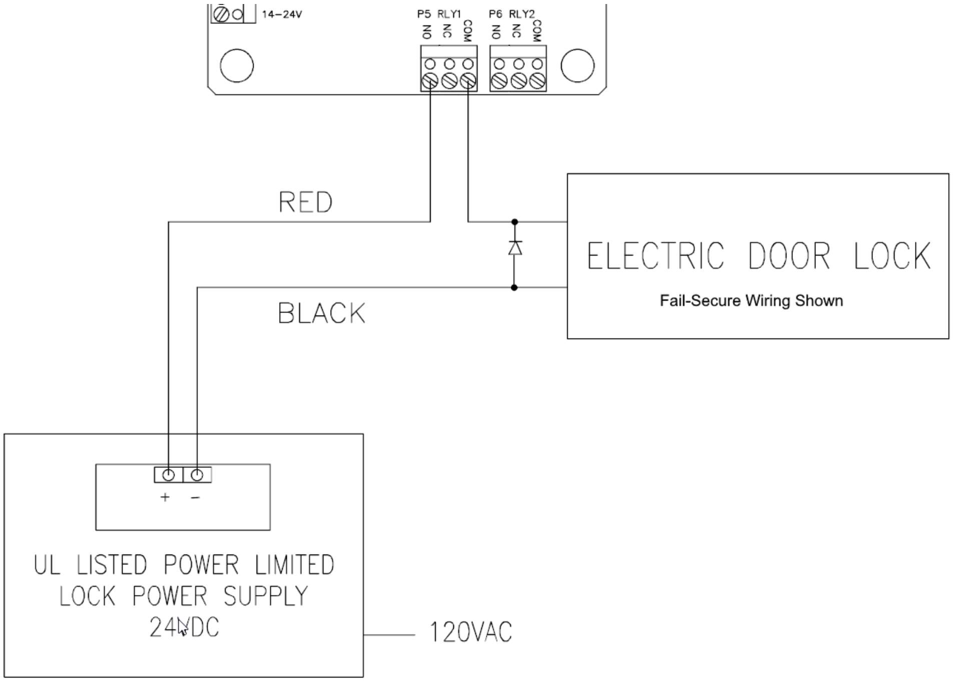
Touch Reader

Touch Reader Pin Connections

VRINX	Touch 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 (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (IBT)	NOT USED

Installing Diode for Lock Wiring - Relay

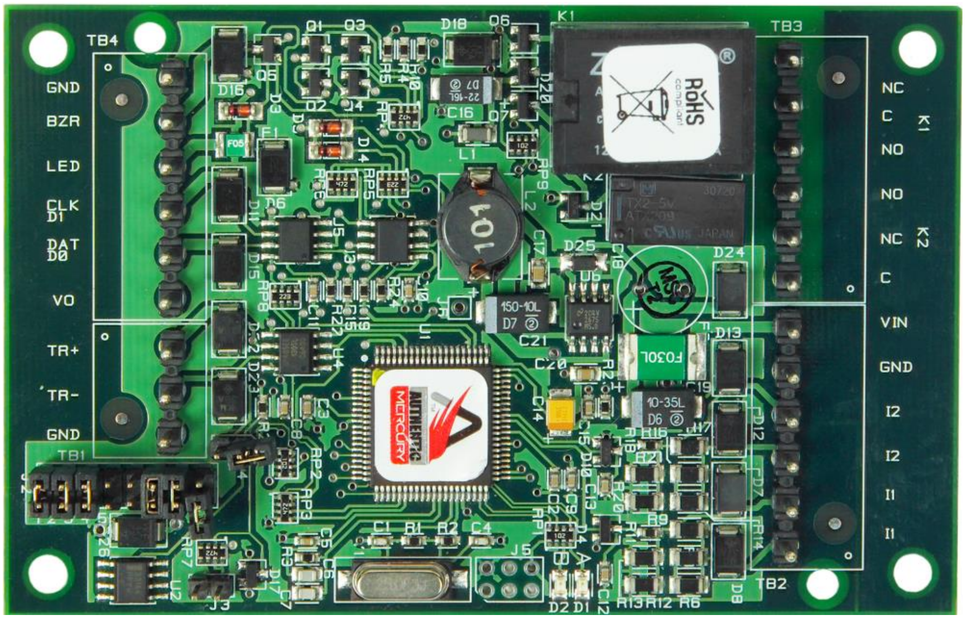
A diode is supplied with the VRINX which should be fitted across 12V and COM to protect the relay contacts.



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. (Above diagram is of Fail Open).

VRI-1

CHAPTER 12



Single Reader Interface

Overview

The VRI-1 is a Reader Interface between the Reader Controllers and Card Readers. The VRI-1 works similarly to the VRINX but utilizes a new SMS-M protocol. Reader Interfaces can be used in small systems with one reader and large systems with thousands of readers. The VRI-1 Reader Interface is supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt reader controllers.

Highlights

- Supports various read head technologies; Proximity, Magnetic Stripe, barcode, Wiegand, iButton, barium ferrite, smart card, biometric and more
- Supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt Reader Controllers
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and the Reader Controller
- Can be powered directly from the VRCNX-R/M/A or separately (depending on type and length of wire, refer the Recommended Wire Chart) by a 12VDC Rated 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 VRCNX-R/M/A Reader Controllers
- 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 VRCNX-R/M 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”

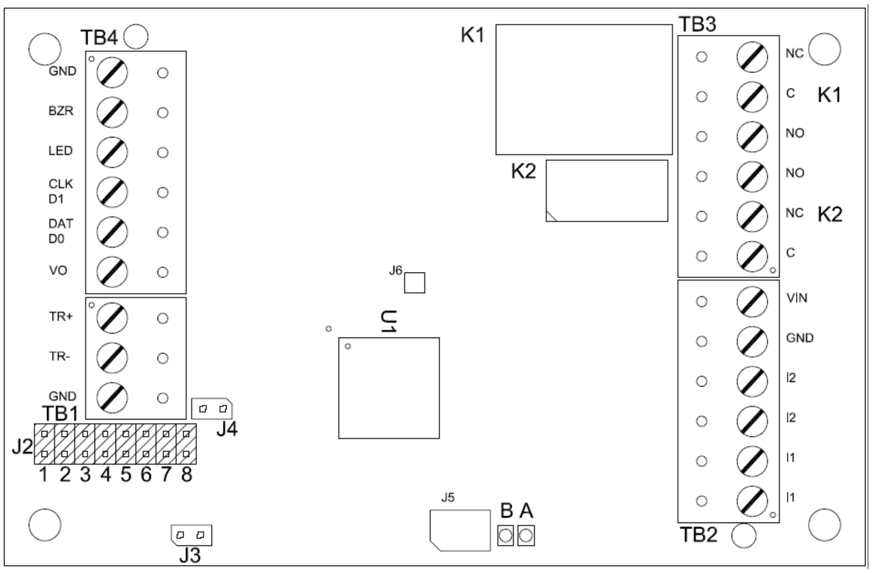
Environmental conditions

- 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 Reader Controller VRCNX-R/M/A via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one VRCNX-R/M/A reader controller. Wire runs are limited to 4,000 feet (Data Only) from the main controller to a VRI-1 (*see Recommended Wire Chart*). Data communication between reader controller and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration the VRI-1 boards are connected to channels J4 to J11 on the VRCNX-R/M/A board in parallel. A maximum of 16 VRI-1 boards can be connected in this manner.

Note: Only identical protocol devices can be connected on the same channel on the VRCNX-R/M/A.

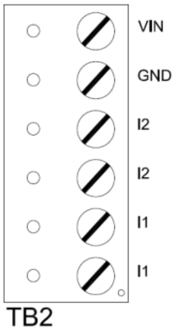
Daisy chain configuration

In a daisy chain configuration, the VRI-1 reader interfaces are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R/M/A.

VRI-1 PIN functions

TB2 – Power source and contact inputs

Provides power to the VRI-1 from the VRCNX-R/M/A. 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.



- 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

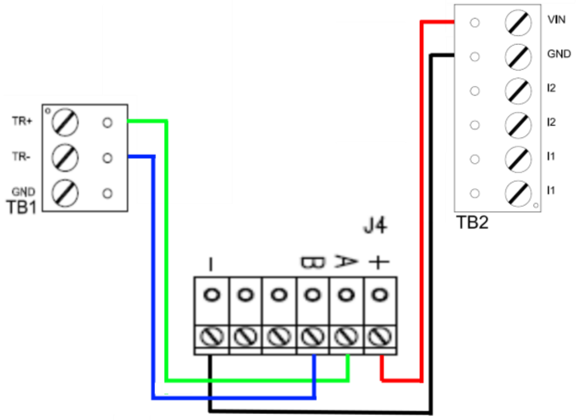
D1 (A) / D2 (B) – Status LEDs

- 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 VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VRI-1 reader interface is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and TB1 for RS-485 communications and TB2 for power on the VRI-1. In the following example we have selected J4 on the VRCNX-R/M/A board.

Note: Only identical protocol devices are allowed on same channels.

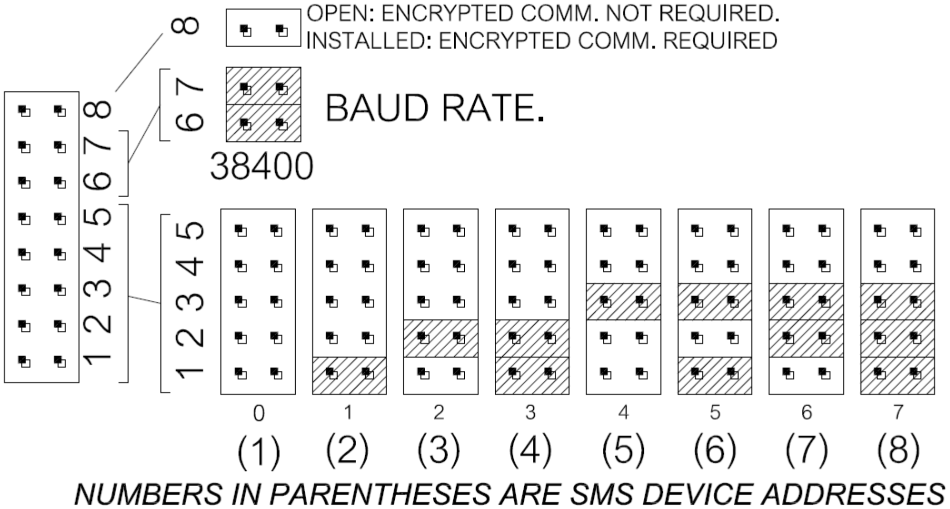


Data & Power connections between VRI-1and VRCNX-R/M/A

VRI-1	VRCNX-R/M/A J4
TB2 PIN 1 – VIN	PIN 1 – Power
TB2 PIN 2 - GND	PIN 6 – GND
TB1 PIN 1 – TR+	PIN 2 – RXD (A)
TB1 PIN 2 – TR-	PIN 3 – TXD (B)
No connection	PIN 4 - DTR
No connection	PIN 5 - DCD

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 VRCNX-R/M/A. This information will be required to set up the reader in SMS.

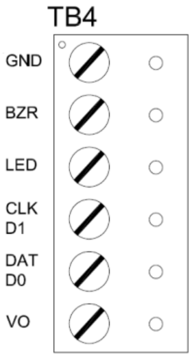


NUMBERS IN PARENTHESES ARE SMS DEVICE ADDRESSES

Read head wiring instructions

The VRI-1 reader interface can communicate to many different read heads. The connection is different for each reader type, please refer to the reader head documentation for wiring instructions.

TB4 – Reader Head Connections



Ground (Black)

Buzzer (Not Used)

LED (Orange)

Clock / D1 (White)

Data / D0 (Green)

V0 (Red)

Supported Readers

Proximity

Vanderbilt / XCeedID / Standard Wiegand

VMR-5 Magnetic Stripe

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off

VMR-10 and VMR-20 Magnetic Stripe

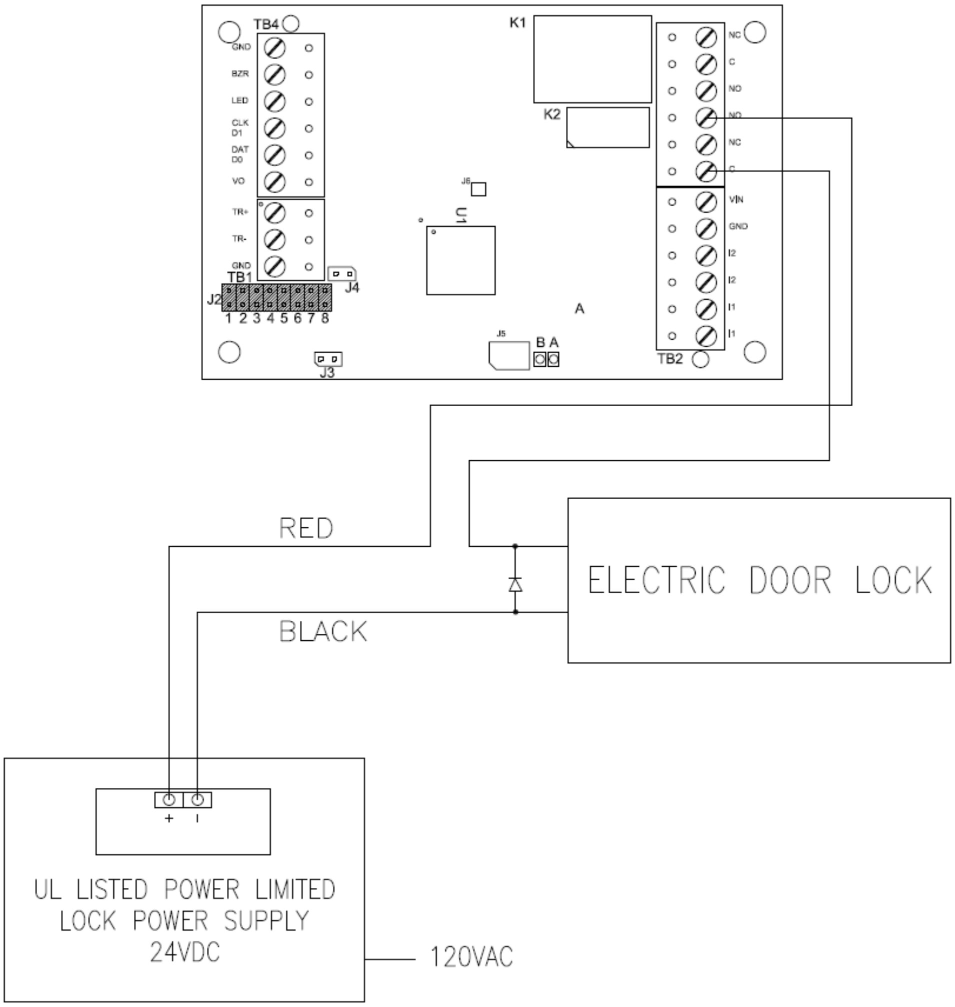
VMR-10 / VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On

Installing Diode for Lock Wiring - Relay

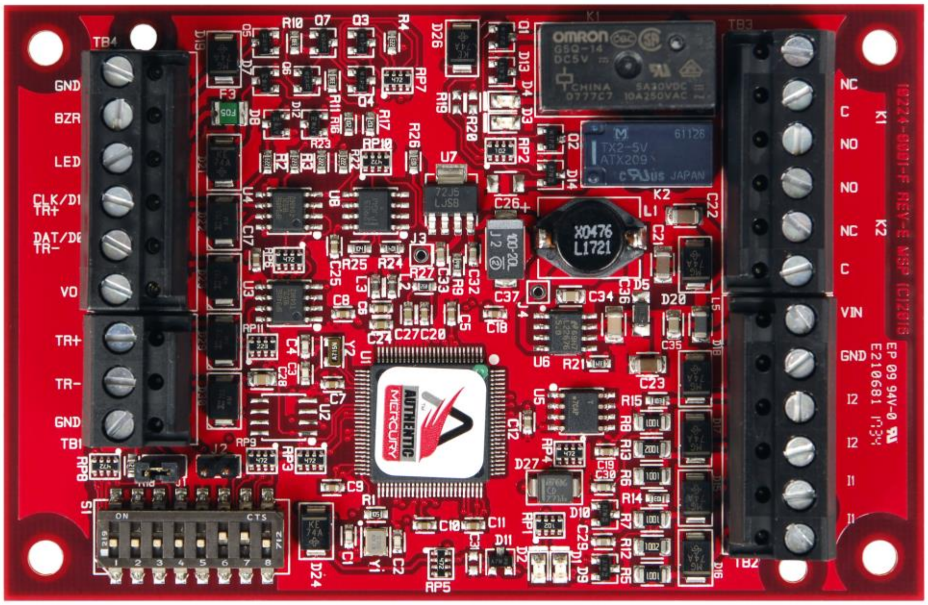
A diode is supplied with the VRI-1 which should be fitted across 12V / 24V and COM to protect the relay contacts.



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 13



Single Reader Interface – Series 3

Overview

The VRI-1S3 is a Series 3 Reader Interface between the Reader Controllers and Card Readers. The VRI-1S3 works identically to the VRI-1 and utilizes the SMS-M protocol. Reader Interfaces can be used in small systems with one reader and large systems with thousands of readers. The VRI-1S3 Reader Interface is supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt reader controllers.

Highlights

- Supports various read head technologies; Proximity, Magnetic Stripe, barcode, Wiegand, iButton, barium ferrite, smart card, biometric and more
- Supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt Reader Controllers
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and the Reader Controller
- Can be powered directly from the VRCNX-R/M/A or separately (depending on type and length of wire, refer the Recommended Wire Chart) by a 12VDC Rated 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 VRCNX-R/M/A Reader Controllers
- 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 VRCNX-R/M 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"

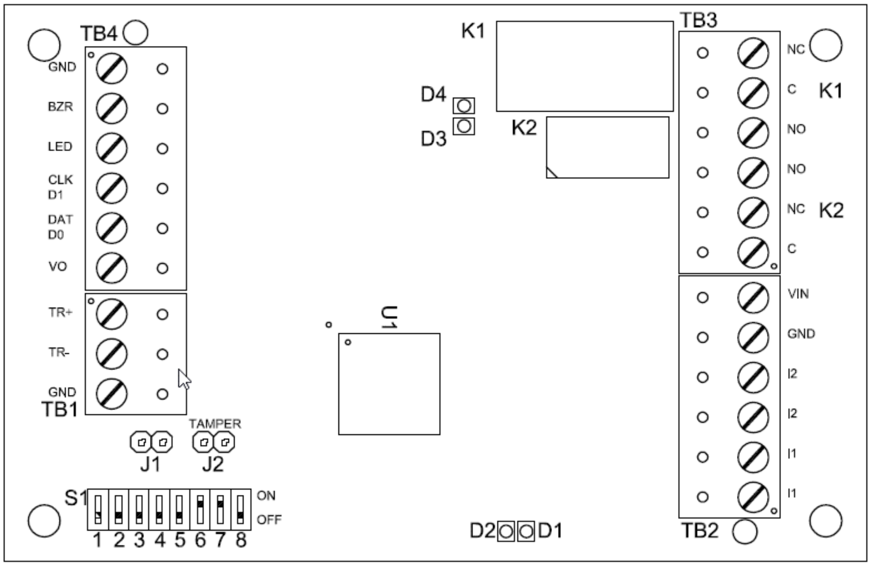
Environmental conditions

- 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 Reader Controller VRCNX-R/M/A via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one VRCNX-R/M/A reader controller. Wire runs are limited to 4,000 feet (Data Only) from the main controller to a VRI-1S3 (*see Recommended Wire Chart*). Data communication between reader controller and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration the VRI-1S3 boards are connected to channels J4 to J11 on the VRCNX-R/M/A board in parallel. A maximum of 16 VRI-1S3 boards can be connected in this manner.

Note: Only identical protocol devices can be connected on the same channel on the VRCNX-R/M/A.

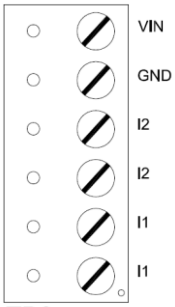
Daisy chain configuration

In a daisy chain configuration, the VRI-1S3 reader interfaces are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R/M/A.

PIN Functions

TB2 – Power source and contact inputs

Provides power to the VRI-1S3 from the VRCNX-R/M. 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-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

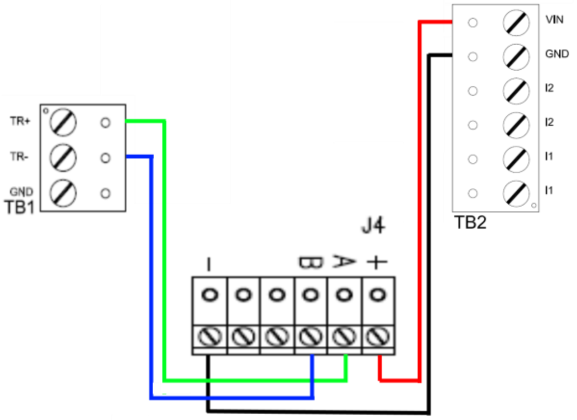
D1 (A) / D2 (B) – Status LEDs

- 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 VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VRI-1S3 reader interface is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and TB1 for RS-485 communications and TB2 for power on the VRI-1S3. In the following example we have selected J4 on the VRCNX-R/M/A board.

Note: Only identical protocol devices are allowed on same channels.

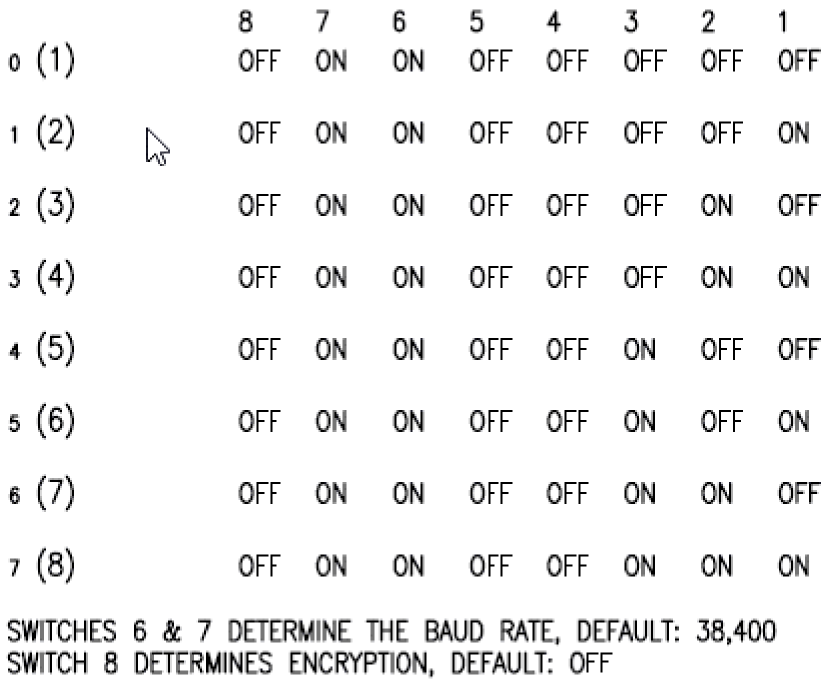


Data & Power connections between VRI-1S3 and VRCNX-R/M/A

VRI-1S3	VRCNX-R/M/A J4
TB2 PIN 1 – VIN	PIN 1 – Power
TB2 PIN 2 - GND	PIN 6 – GND
TB1 PIN 1 – TR+	PIN 2 – RXD (A)
TB1 PIN 2 – TR-	PIN 3 – TXD (B)
No connection	PIN 4 – DTR
No connection	PIN 5 – DCD

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 VRCNX-R/M/A. This information will be required to set up the reader in SMS. The numbers in parenthesis are the SMS device addresses.



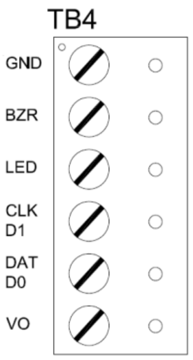
	8	7	6	5	4	3	2	1
0 (1)	OFF	ON	ON	OFF	OFF	OFF	OFF	OFF
1 (2)	OFF	ON	ON	OFF	OFF	OFF	OFF	ON
2 (3)	OFF	ON	ON	OFF	OFF	OFF	ON	OFF
3 (4)	OFF	ON	ON	OFF	OFF	OFF	ON	ON
4 (5)	OFF	ON	ON	OFF	OFF	ON	OFF	OFF
5 (6)	OFF	ON	ON	OFF	OFF	ON	OFF	ON
6 (7)	OFF	ON	ON	OFF	OFF	ON	ON	OFF
7 (8)	OFF	ON	ON	OFF	OFF	ON	ON	ON

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

Read head wiring instructions

The VRI-1S3 reader interface can communicate to many different read heads. The connection is different for each reader type, please refer to the reader head documentation for wiring instructions.

TB4 – Reader Head Connections



Ground (Black)

Buzzer (Not Used)

LED (Orange)

Clock / D1 (White)

Data / D0 (Green)

V0 (Red)

Supported Readers

Proximity

Vanderbilt / XCeedID / Standard Wiegand

VMR-5 Magnetic Stripe

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off

VMR-10 and VMR-20 Magnetic Stripe

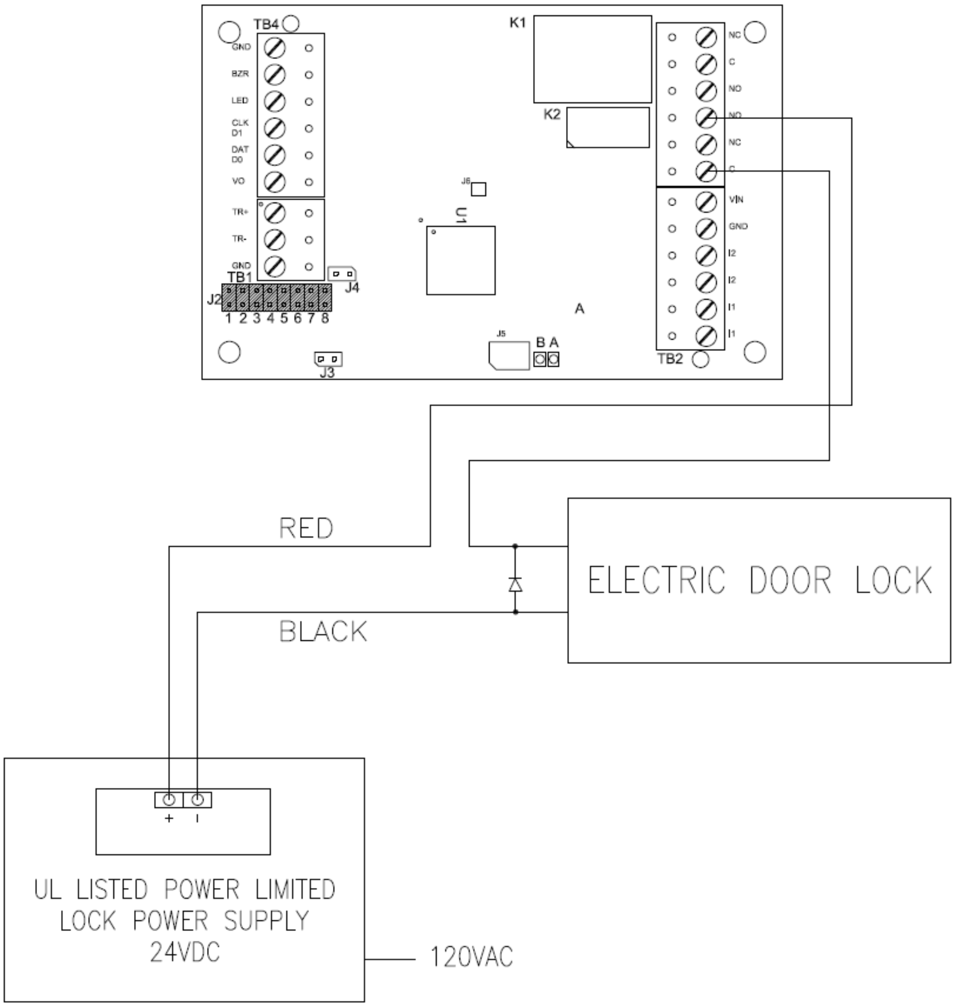
VMR-10 / VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On

Installing Diode for Lock Wiring - Relay

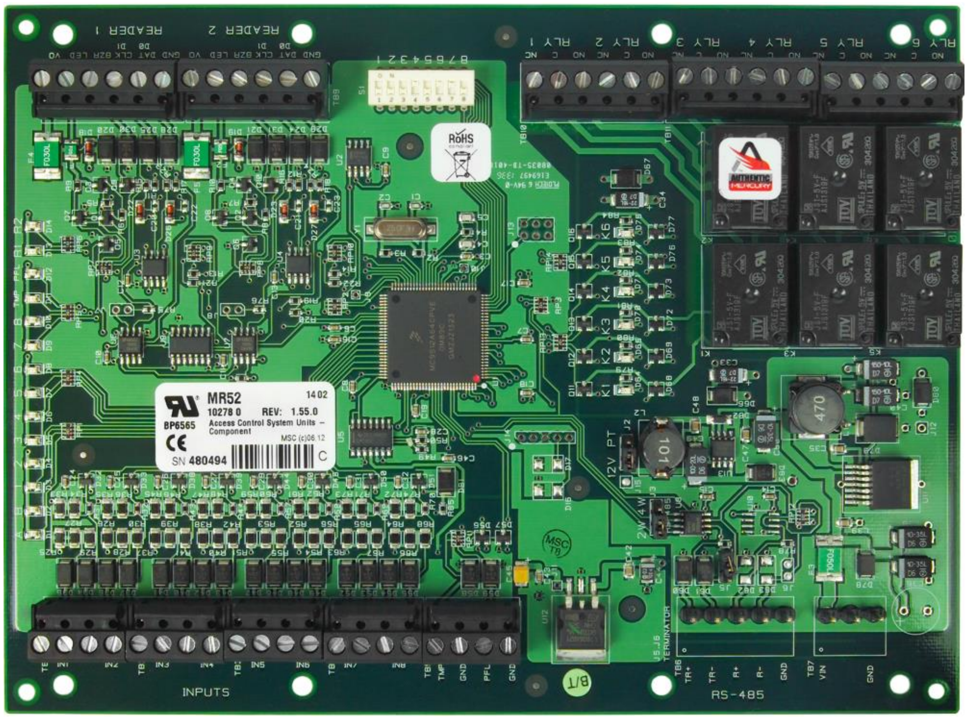
A diode is supplied with the VRI-1S3 which should be fitted across 12V / 24V and COM to protect the relay contacts.



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 14



Dual Reader Interface

Overview

The VRI-2 (green) and VRI-2S3 (red – series 3) are Reader Interfaces between the Reader Controllers 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 the SMS-M protocol. Reader Interfaces can be used in small systems with one reader and large systems with thousands of readers. The VRI-2 Reader Interface is supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt reader controllers.

Highlights

- Supports various read head technologies; Proximity, Magnetic Stripe, barcode, Wiegand, iButton, barium ferrite, smart card, biometric and more
- Supported by the VRCNX-R, VRCNX-M and VRCNX-A Vanderbilt Reader Controllers
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and the Reader Controller
- Can be powered directly from the VRCNX-R/M/A or separately (depending on type and length of wire, refer the Recommended Wire Chart) by a 12 – 24 VDC Rated 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 VRCNX-R/M/A Reader Controllers
- 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 VRCNX-R/M/A 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

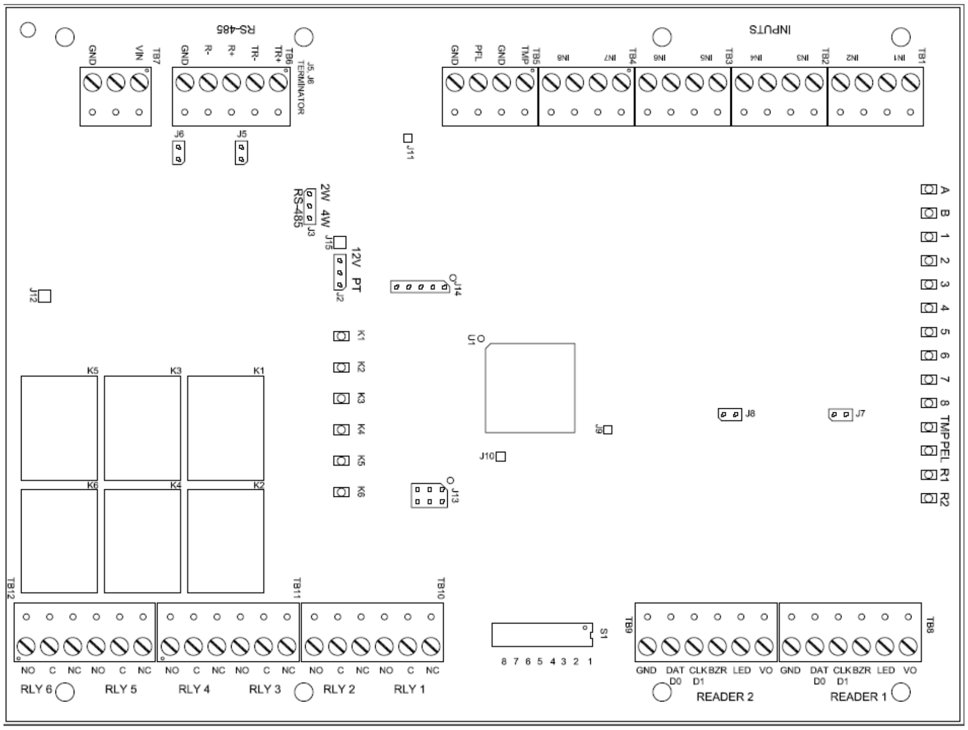
Environmental conditions

- 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 Reader Controller VRCNX-R/M/A via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one VRCNX-R/M/A reader controller. Wire runs are limited to 4,000 feet (Data Only) from the main controller to a VRI-2 (*see Recommended Wire Chart*). Data communication between reader controller and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration the VRI-2 boards are connected to channels J4 to J11 on the VRCNX-R/M/A board in parallel. A maximum of 8 VRI-2 boards can be connected in this manner (4 per channel).

Note: Only identical protocol devices can be connected on the same channel on the VRCNX-R/M/A.

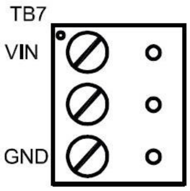
Daisy chain configuration

In a daisy chain configuration, the VRI-2 reader interfaces are connected to one another in series. Up to 8 VRI-2 devices can be connected to a reader controller (4 per channel). This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R/M/A.

PIN Functions

TB7 - Power source

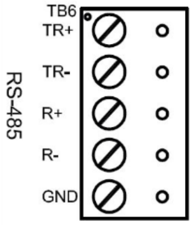
Provides power to the VRI-2 from the VRCNX-R/M/A.



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

TB6 - Communications

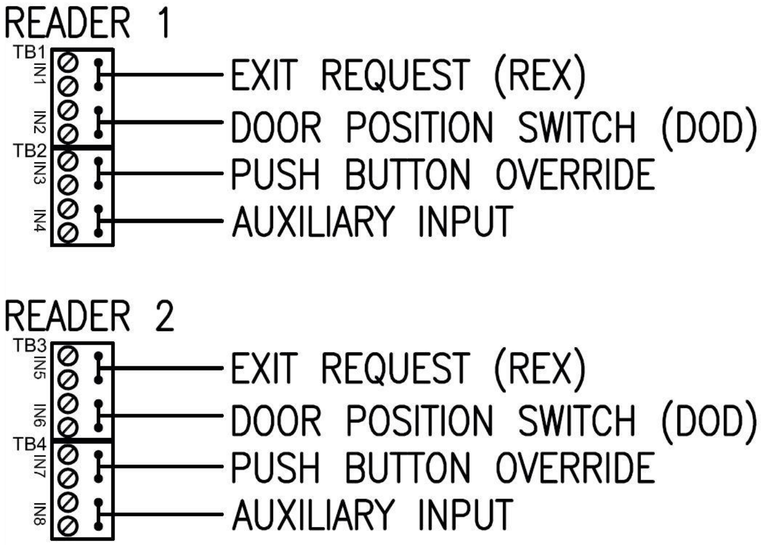
Provides RS-485 communications between the VRI-2 and the VRCNX-R/M.



- PIN 1 is Data A (TR+)
- PIN 2 is Data B (TR-)
- PIN 3 unused
- PIN 4 unused
- PIN 5 unused

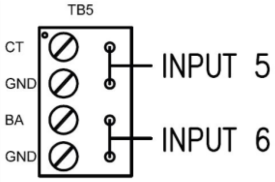
TB1 – TB5 Contact inputs

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



Device Type:

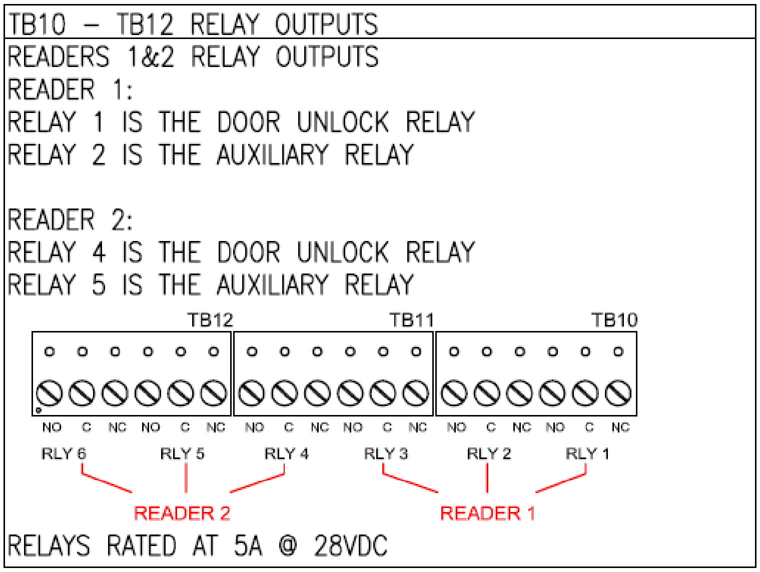
DOD (supervised):	max distance = 1,000 ft
DOD (unsupervised):	max distance = 2,000 ft



- Input 5 – Onboard Cabinet Tamper with SMS VRI-2 reader template
- Input 6 – UPS Fault Monitoring = user definable with SMS custom label

TB10 – TB12 Relay Outputs

The VRI-2 has six relay outputs.



TB10 – TB12 RELAY OUTPUTS

READERS 1&2 RELAY OUTPUTS

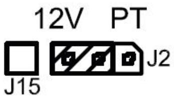
READER 1:
RELAY 1 IS THE DOOR UNLOCK RELAY
RELAY 2 IS THE AUXILIARY RELAY

READER 2:
RELAY 4 IS THE DOOR UNLOCK RELAY
RELAY 5 IS THE AUXILIARY RELAY

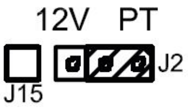
RELAYS RATED AT 5A @ 28VDC

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 –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 an odd address for use with SMS

SMS	DIP Switch Position							
Address	8	7	6	5	4	3	2	1
(1)	OFF	ON	ON	OFF	OFF	OFF	OFF	OFF
(3)	OFF	ON	ON	OFF	OFF	OFF	ON	OFF
(5)	OFF	ON	ON	OFF	OFF	ON	OFF	OFF
(7)	OFF	ON	ON	OFF	OFF	ON	ON	OFF

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

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

SMS Software Programming
VRI-2 Reader 1 = Odd Address
VRI-2 Reader 2 = Next Sequential Even Address

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)

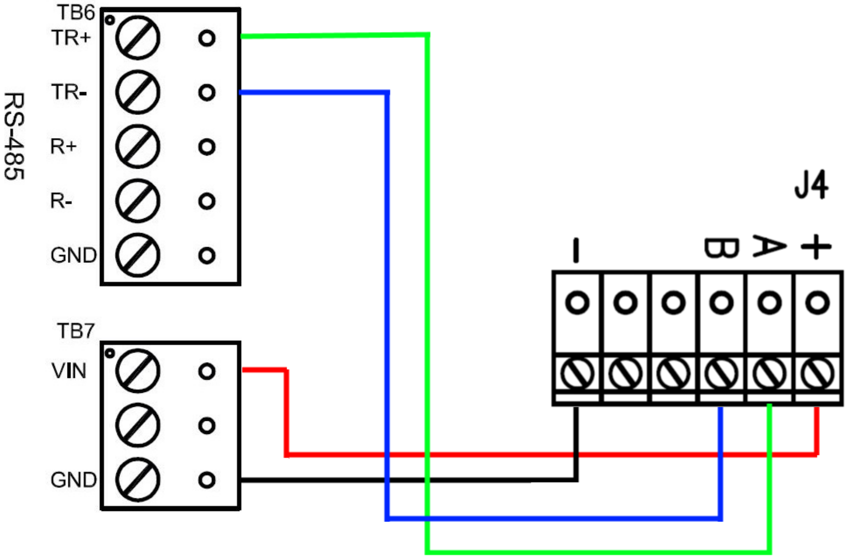
LED TMP:	Cabinet Tamper
LED PFL:	Power Fault
LED R1:	Reader 1 Activity
LED R2:	Reader 2 Activity
LED K1:	Relay 1 Energized
LED K2:	Relay 2 Energized
LED K3:	Relay 3 Energized
LED K4:	Relay 4 Energized
LED K5:	Relay 5 Energized
LED K6:	Relay 6 Energized

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

Connecting to VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VRI-2 reader interface is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and TB6 on VRI-2. In the following example we have selected J4 on the VRCNX-R/M/A board.

Note: Only identical protocol devices are allowed on same channels.



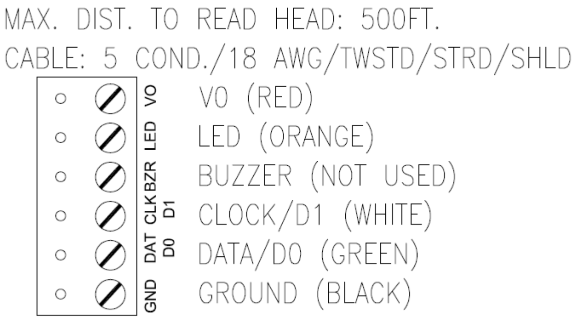
Data & Power connections between VRI-1and VRCNX-R/M/A

VRI-2	VRCNX-R/M/A J4
TB7 PIN 1 – VIN	PIN 1 – Power
TB7 PIN 3 - GND	PIN 6 – GND
TB6 PIN 1 – TR+	PIN 2 – RXD (A)
TB6 PIN 2 – TR-	PIN 3 – TXD (B)
No connection	PIN 4 - DTR
No connection	PIN 5 - DCD

Read head wiring instructions

The VRI-2 reader interfaces can communicate to many different read heads. The connection is different for each reader type, please refer to the reader head documentation for wiring instructions.

TB8 – TB9 Reader Head Connections



Supported Readers

Proximity

Vanderbilt / XCeedID / Standard Wiegand

VMR-5 Magnetic Stripe

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off

VMR-10 and VMR-20 Magnetic Stripe

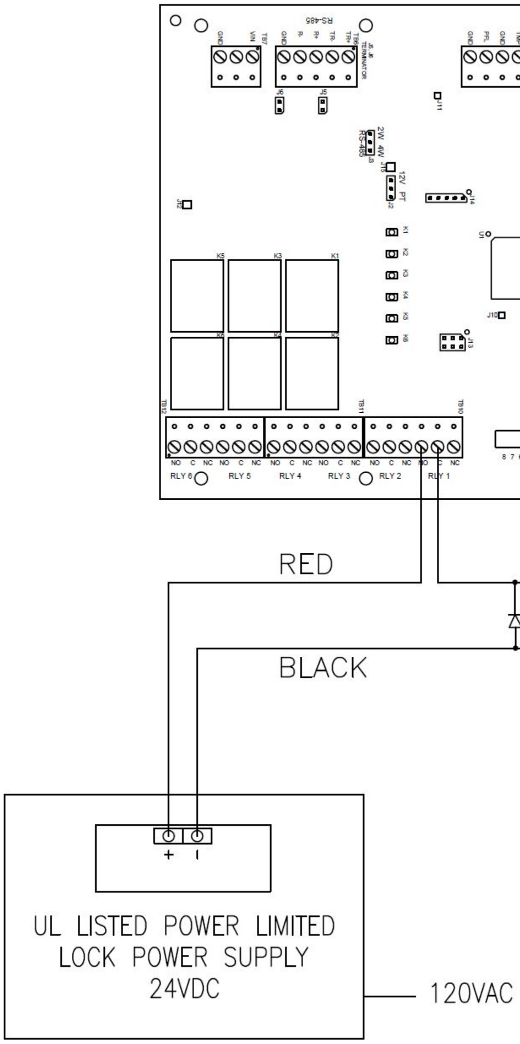
VMR-10 / VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On

Installing Diode for Lock Wiring - Relay

A diode is supplied with the VRI-2 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.

CHAPTER 15

SRINX (Legacy)

Reader Interface

Overview

The legacy SRINX (Legacy) is a Reader Interface between Reader Controllers and Card Readers. The SRINX offers a cost-effective, modular approach to access control system design. Reader Interfaces can be used in small systems with one reader and large systems with thousands of readers. The SRINX Reader Interface is supported by the entire family of Vanderbilt reader controllers.

Highlights

- Supports various read head technologies; Proximity, Magnetic Stripe, barcode, Wiegand, barium ferrite, smart card, biometric and more
- Supported by the entire family of Vanderbilt Reader Controllers
- Communicates via RS-485 protocol
- Capable of running in degraded mode, allowing local decision making, if communication fails between the Reader Interface and the Reader Controller
- Can be powered directly from the VRCNX-R or separately (depending on type and length of wire, refer the Recommended Wire Chart)

Standard features

- Supports one read-head credential
- Connects directly to the communication channels on the VRCNX-R Reader Controllers
- Includes One 2-amp, form C, single pole/double throw, mechanically latching relay
- Includes Two 2-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
- Connection for one multi-color LED for GO or NO/GO indication
- Connector for one buzzer/annunciator

Specifications

- Board Dimensions - 3-13/16” H x 3-13/16” W x 1-3/4” D
- Enclosure Dimensions - 8-1/4” H x 7-1/2” W x 3-1/2” D
- Power requirements - 12VDC - 24 VDC (usually supplied from the VRCNX-R Reader Controller)
- Power consumption - 23mA (without read heads)
- Ambient temperature - 0º to 70º C or -14º to 185º F

SRINX (Legacy) standard enclosure

SRINX (Legacy) Standard Enclosure - An enclosure with a hinged door and a lock is included for each SRINX board. The tamper proof switch enables the system to send an alarm whenever someone opens the enclosure.

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: 8.25” x 7.5” x 3.5”

Standard enclosure installation

Environmental conditions

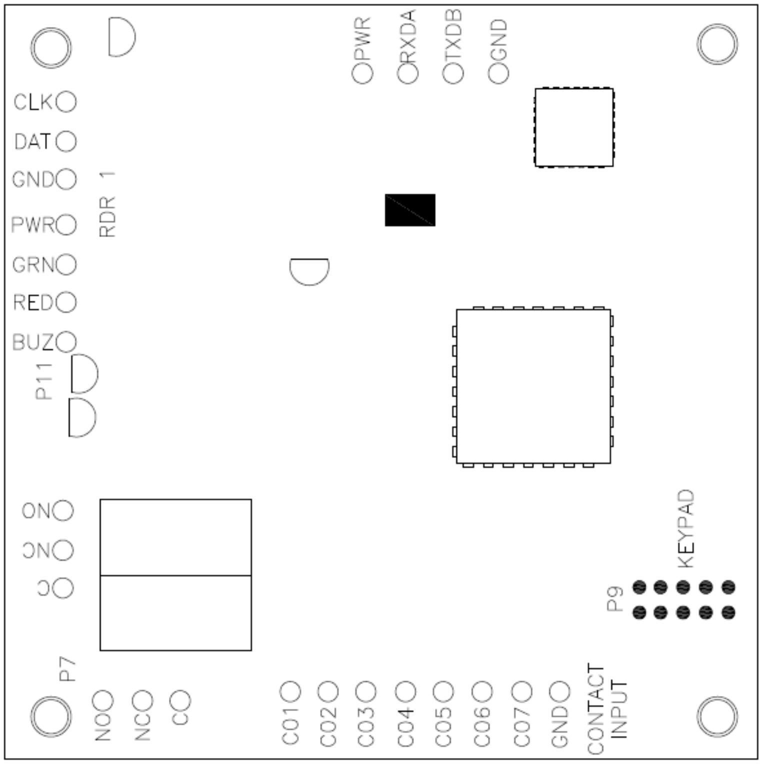
- Ambient Temperature: 0º to 49º C or 32º to 120º F
- The room must be dust free and clean.
- It is optimal to mount the enclosure on fire rated plywood which is affixed to a cinder block wall or a wall covering i.e. sheetrock
- Mount the cabinet in a secure, but generally accessible location

Mounting the enclosure

1. 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.
2. A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.

3 Mount the enclosure to the wall using the provided mounting holes. Recommended mounting hardware: Four 1/4” x 1” lag bolts.

SRINX (Legacy) pin layout



SRINX (Legacy) configuration

The SRINX (Legacy) will be connected to the Reader Controller VRCNX-R via RS-485 protocol. A maximum of 16 reader interfaces can be connected to one VRCNX-R reader controller. Wire runs are limited to 4,000 feet from the main controller to a SRINX. (see Recommended Wire Chart). Data communication between reader controller and the reader interfaces can be a multiplex or a daisy chain configuration.

Multiplex configuration

In a multiplex configuration the SRINX boards are connected to channels J 4 to J 11 on the VRCNX-R board in parallel. A maximum of 16 SRINX boards can be connected in this manner.

Note: Only identical devices can be connected on the same channel on the VRCNX-R.

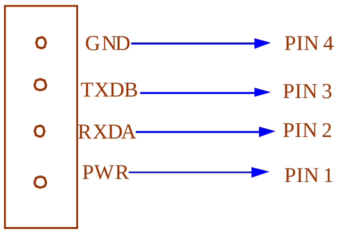
Daisy chain configuration

In a daisy chain configuration, the SRINX reader interfaces are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R.

SRINX (Legacy) pin functions

P 4 - Power source and communication wiring

Provides power to the SRINX. Pins 1 (+) and 4 (-) are polarity conscious. Power requirements are 12VDC or 24VDC only, minimum 350 mA. The SRINX can be powered from the VRCNX-R (refer to Table 1 for wire type and lengths). Pins 2 and 3 are for data transmission to the VRCNX-R (refer to Table 2). The VRCNX-R and SRINX communication is via RS-485 protocol at 9600 baud rate (refer to the Recommended Wire Chart for wire type and length). Maximum distance between SRINX and Reader Controller is 4,000 feet.



P4 power source and communication between VRCNX-R & SRINX

Distance (Ft.)	Gauge
250	22 AWG-Strd,Twst, Shld
500	18 AWG-Strd,Twst, Shld
1000	14 AWG-Strd,Twst, Shld
2000	12 AWG-Strd,Twst, Shld

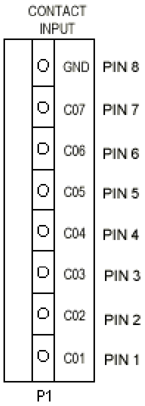
Data communication between SRINX and Reader Controllers

SRINX P4	VRCNX-R J4 - J 11
Pin 2 - RXDA	Pin 2 - RXD (A)
Pin 3 - TXDB	Pin 3 TXD B

Pin 1 - Contact inputs

The SRINX has eight supervised or unsupervised contact points. When connecting more than two contact inputs to Pin 8 (GND), you should install a terminal strip to connect the common ground wires. Supervised door contacts have maximum wire length of 1,000 ft. Unsupervised door contacts have maximum wire length of 2,000 feet.

Note: In a UL listed system Pin 8 (CO8) is used for SRINX enclosure tamper switch only.
Pin 1 (CO1) is used for Request to Exit (REX) device.



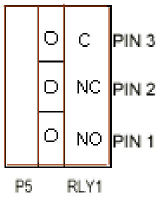
PIN 1 Contact Input Layout

SRINX P1	
Pin 1 C01	1st Contact Input
Pin 2 C02	2nd Contact Input
Pin 3 C03	3rd Contact Input
Pin 4 C04	4th Contact Input
Pin 5 C05	5th Contact Input
Pin 6 C06	6th Contact Input
Pin 7 C07	7th Contact Input
Pin 8 GND	Ground

P5 / P6 - Relay outputs

The SRINX-1 comes with one relay output (P5). The SRINX-2 comes with two relay outputs (P5 & P6). 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



W 5 - Factory use only

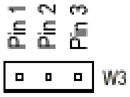
W 5 is for factory use only. Do not add a jumper under normal operating conditions.

W 3 - Read head voltage selector

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

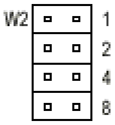
- No jumper will provide 5VDC
- A jumper across Pins 1 and 2 will also provide 5VDC
- A jumper across Pins 2 and 3 will provide 12VDC

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



W 2 - SRINX reader interface addressing

The VRCNX-R reader controller will individually recognize the SRINX modules when they are addressed individually. The data communication ports on the VRCNX-R are Pins J 4 through J11. These pins will be directly connected to the SRINX reader interfaces (refer to Recommended Wire Chart).

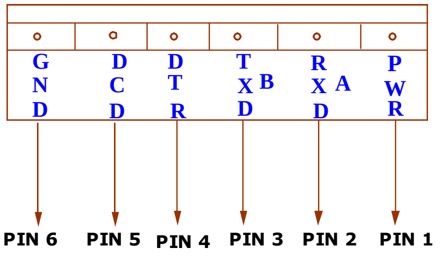


SRINX Address Chart

SRINX Addr. A	Jumper Locations	SRINX Addr. B	Jumper Locations
1	1 2 4 8	1	1 2 4 8
1	1 2 4 8	2	2 4 8
1	1 2 4 8	3	1 4 8
1	1 2 4 8	4	4 8
1	1 2 4 8	5	1 2 8
1	1 2 4 8	6	2 8
1	1 2 4 8	7	1 8
1	1 2 4 8	8	8
2	2 4 8	9	1 2 4
2	2 4 8	10	2 4
2	2 4 8	11	1 4
2	2 4 8	12	4
2	2 4 8	13	1 2
2	2 4 8	14	2
2	2 4 8	15	1
2	2 4 8	16	

J4 - J11 Data communication channels

Communication between a VRCNX-R reader controller and a SRINX reader interface is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R board and P3 on SRINX. In the following example we have selected J4 on the VRCNX-R board.



Note: Only identical devices are allowed on same channels.

Data communication between VRCNX-R and SRINX

VRCNX-R (J4)	SRINX
Pin 1 - Power	Pin 1- Power
Pin 2 -RXD (A)	Pin 2- RXD (A)

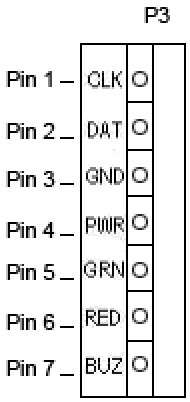
VRCNX-R (J4)	SRINX
Pin 3- TXD (B)	Pin 3 - TXD (B)
Pin 4 - DTR	No connection
Pin 5 - DCD	No connection
Pin 6 - GND	Pin 4 -GND

Read head wiring instructions

The SRINX (Legacy) reader interface can communicate to many different read heads. We have provided the pin outs for the most commonly used read-heads. The connection is different for each reader type. Please refer to the Recommended Wire Chart for the proper wire and lengths.

Note: The shield must be connected to Pin 3 on the SRINX.

P 3 - SRINX pin connections



Proximity Reader

Proximity Read Head Pin Connections

SRINX	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

Wiegand Reader

Wiegand Read Head Pin Connections

SRINX	Wiegand 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 (BROWN)
Pin 6 (RED)	NOT USED
Pin 7 (BUZ)	NOT USED

MAGTEK Magnetic Stripe

Magtek Magnetic Stripe Pin Connections

SRINX	Magtek Mag Stripe
PIN 1 (CLK)	DATA 0 (GREEN)
PIN 2 (DAT)	DATA 1 (YELLOW)
PIN 3 (GND)	GROUND (BROWN)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (BLACK)
PIN 6 (RED)	LED (WHITE)
PIN 7 (BUZ)	NOT USED

VMR - 5 Magnetic Stripe - LED 1 wire configuration

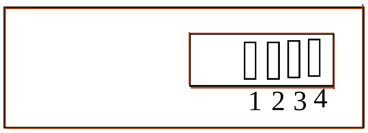
VMR - 5 Magnetic Stripe - LED 1 Pin Connections

SRINX	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (BUZ)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = Off S3 = Off S4 = Off



VMR - 5 Magnetic Stripe - LED 2 wire configuration

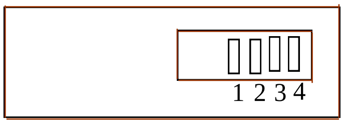
VMR - 5 Magnetic Stripe - LED 2 Pin Connections

SRINX	VMR-5
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (BUZ)	NOT USED

VMR-5 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = Off S4 = Off



VMR-10 and VMR-20 Magnetic Stripe

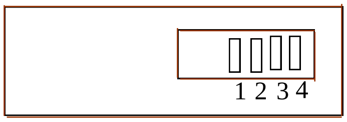
VMR-10 and VMR-20 Magnetic Stripe Pin Connections

SRINX	VMR-10 and VMR-20
PIN 1 (CLK)	DATA 1 (WHITE)
PIN 2 (DAT)	DATA 0 (GREEN)
PIN 3 (GND)	GROUND (BLACK)
PIN 4 (PWR)	POWER (RED)
PIN 5 (GRN)	LED (ORANGE)
PIN 6 (RED)	LED (BROWN)
PIN 7 (BUZ)	NOT USED

VMR-10 and VMR-20 Switch Settings

Remove the top mounting bracket to access the DIP switches.

S1 = Off S2 = On S3 = On S4 =On



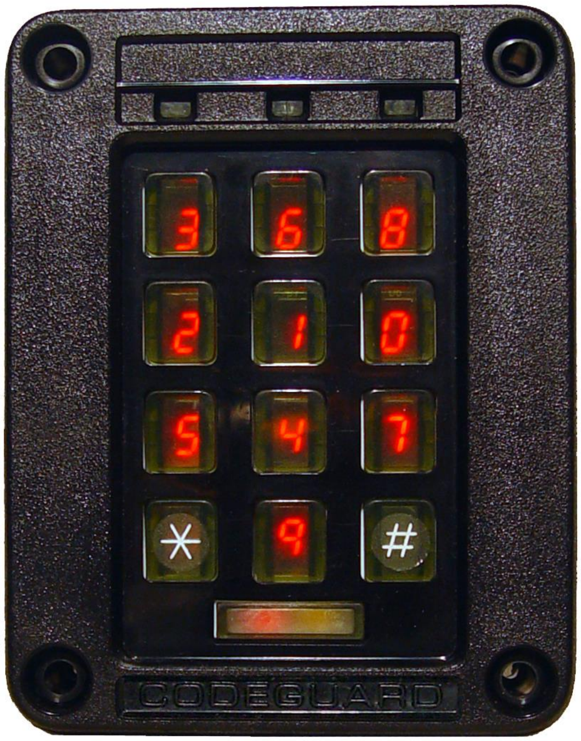
Touch Reader

Touch Reader Pin Connections

SRINX	Touch 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 (BROWN)
PIN 6 (RED)	NOT USED
PIN 7 (BUZ)	NOT USED

CHAPTER 16

Scramble Keypad Reader



Scramble Keypad Reader

Overview

The SERIII Scramble Keypad is a keypad reader designed to prevent onlookers from detecting the PIN code being entered. The LEDs display a randomly allocated set of numbers from 0 to 9. The position of the numbers change every time the keypad is activated. Only the user standing directly in front of the keypad can see the scrambled digits.

Electrical connections to the installation are made to a screw terminal connector which plugs into the rear of the Vanderbilt Scramble Keypad Reader. Full details of the signals and pin numbering can be found later in this section.

Features and benefits

- Very narrow viewing angle of the lighted, scrambled digits
- Extremely durable membrane keypad
- Random allocation of digits ensures even wear to the keys
- Individual PIN codes can be up to 9 digits in length
- The SERIII has a weatherproof rating of IP65
- An audible alarm signals when a button is depressed
- Robust polycarbonate enclosure
- Equipped with power-up diagnostics and self-test routine
- Wiegand communication protocol
- Over 3.6 million unique permutations are available
- Terminal connection on the rear of the unit

Connecting the keypad to SMS

The keypad connects to the **Vanderbilt SMS** through the **User Connector** lines. Prior to installation the keypad operating mode is selected using the factory set internal rotary code switch. Disconnect power from the keypad before altering this switch.

Driving the Buzzer

If the BUZZER input is driven to a logic LO (Ground), then the buzzer will sound. Internal operation at keypresses cannot be disabled; the internal and external functions share the buzzer in a logical OR.

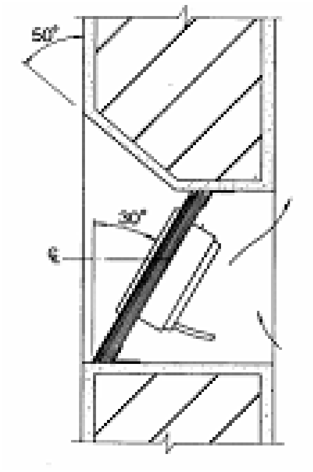
Note: The buzzer is not intended for long continuous operation. Such operation may shorten the life of the part.

Installation information

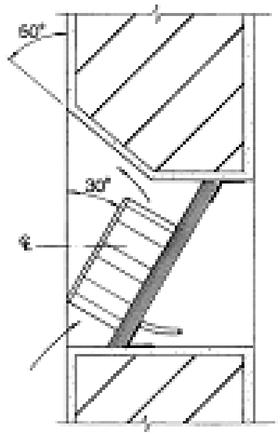
1. The Vanderbilt Scramble Keypad Reader can be flush mounted in a panel of up to 1.75 thickness (2.25 with rear access) or surface mounted in accessory SERIII. Full details of the various types of installation are given later in this section.
2. Installation at eye level with Vanderbilt Scramble Keypad Reader mounted parallel to the vertical plane of a wall, door or panel, results in the eye level range of height being restricted to 6.3ins (160mm) at a distance of 17.7ins (450mm) from the keyboard. This corresponds to an angular accommodation of + /- 10 degs. which is necessary to prevent “over-the-head” viewing of the display.
3. The head of the viewer exceeds the space within the boundaries of display visibility.
4. If Vanderbilt Scramble Keypad Reader is mounted at a low level of 45ins and tilted backwards at an angle of 3Odegs, the vertical viewing accommodation is greatly increased. As an example, to accommodate varying heights, people with an eye level at 50ins can move close to the keyboard and people with an eye level of 67.7ins can stand further back at a distance of approximately 17.7ins. The vertical accommodation range increases from 6.2ins to 17.7ins.
5. The body of the viewer exceeds the space within the boundaries of display visibility.

Vanderbilt Scramble Keypad Reader recessed on 30 degree sloping panel

Flush Panel Mounting



Surface Mounting Accessory

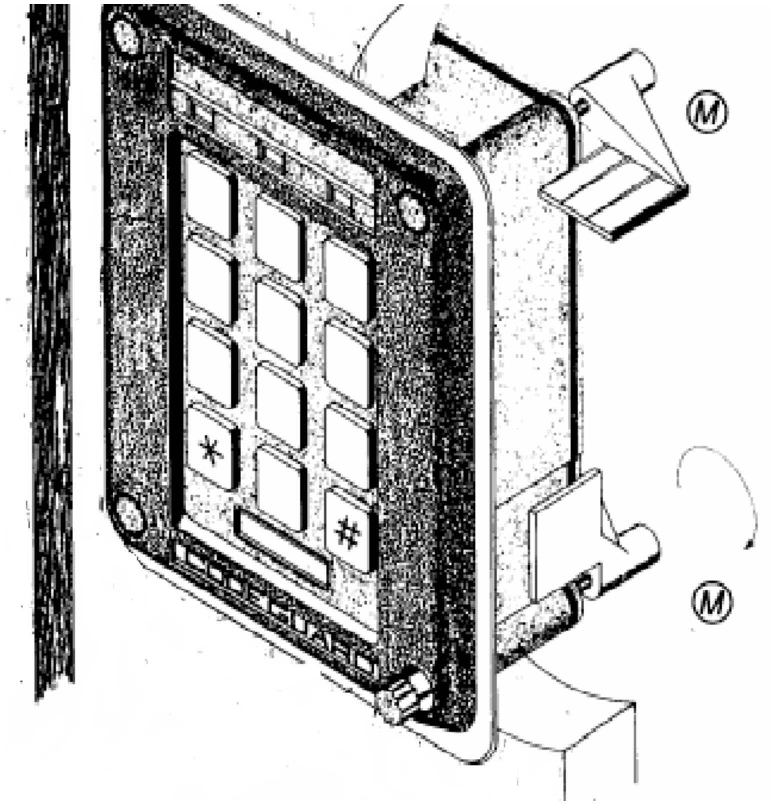


Caution: Do not restrict air circulation.

Both angled configurations provide a typical (eye level) viewing accommodation of 17.7".

If the C/L is at 45ins, the eye level range is: - 50ins to 67.7ins (1720mm).

Flush mounting of Vanderbilt Scramble Keypad Reader



Extended travelling lugs

Compress the front flange against the face of the panel or mounting plate

Retracted

Extend and travel to close

Caution: Ensure that air is free to circulate behind the rear cover

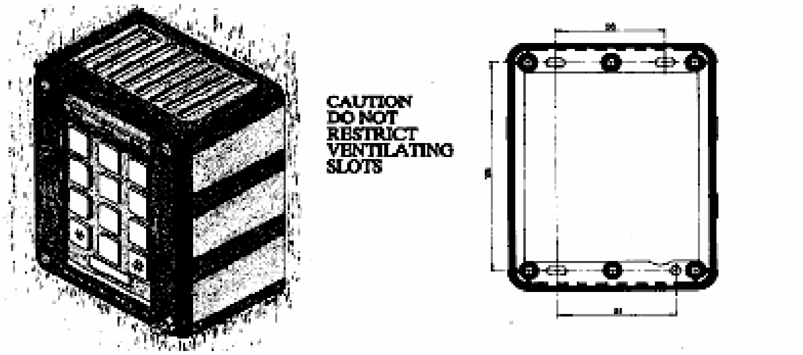
1. Cut out an accurate mounting hole for Vanderbilt Scramble Keypad Reader using a template.

   *Usable only where rear access is available to hold lugs in position while tightening. In all other cases the body of the Vanderbilt Scramble Keypad Reader stops the lugs in the correct position while the screw is rotated clockwise to tighten.

2. Fit the screws through the Vanderbilt Scramble Keypad Reader enclosure and, using tool Part no. 118-1, drive them into the Lugs. Rotate the screw counter-clockwise to set the Lugs to the retracted position.

3. Enter the Vanderbilt Scramble Keypad Reader through the mounting hole, then tighten the screws using tool Part no. 118-1. This rotates the Lugs to the engaged position due to friction between the thread and the lug. If the thread becomes lose with use, apply a suitable thread locking compound to restore the friction

Surface mounting using accessory SMK-2



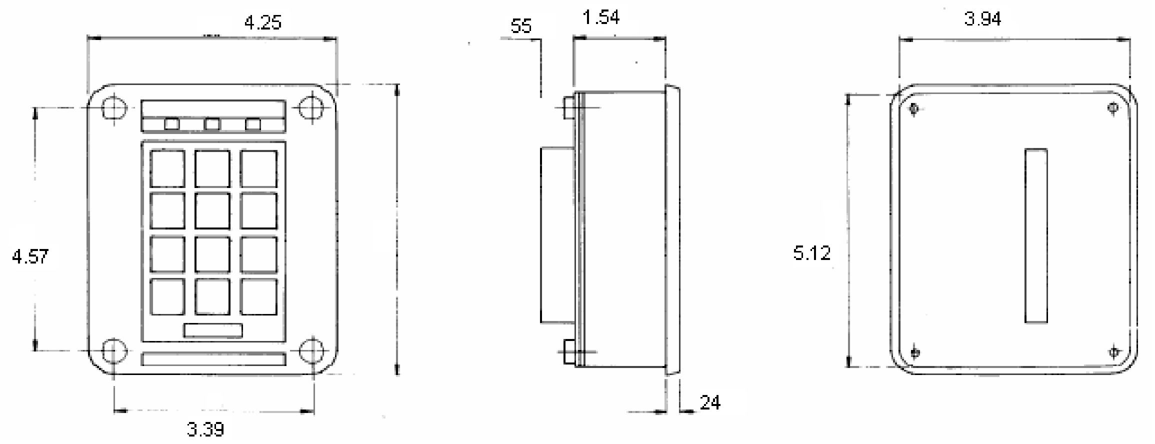
1 Mount Vanderbilt Scramble Keypad at the required height; usually about 66ins (1676mm) unless the low level 30 deg. Tilted position is required as described at the beginning of this section.

2 Mount the surface accessory using hardware appropriate to the situation and make the necessary hole for the connecting cables.

3 Attach the plug to the cable, plug this into the Vanderbilt Scramble Keypad Reader, and assemble it into the surface mount accessory.

4 Mount the Vanderbilt Scramble Keypad Reader by fitting the tamper resistant screws (provided).

Outline dimensions



Pin descriptions (Wiegand version)

Keypad PIN	Description	VRINX P3
1 +5V	Power for interface	
2 GND		3 GND
3 POWER IN	+8 to +12V DC Unreg	4 PWR
4 YELLOW	UserLED low=ON	5 GRN LED
5 D1	Data output	2 DATA 1
6 BUZZER	low-ON	6 BUZ
7 D0	Data output	1 DATA 2 (CLK)
8 RED	User LED low-ON	8 RED LED

Keypad self-test

When power is first applied to the keypad it performs a self-test and displays its firmware version number and operating mode.

The display format is:

- Top row - firmware version number
- Second row - blank
- Third row - Wiegand versions
  Err if mode switch incorrectly set
- Bottom row - mode switch setting

If the display is filled with “F”s on power-up this indicates that the instrument has failed its self-test.

If “Err” is displayed in the third row of the display this indicates that the setting of the mode switch is not compatible with this version of the Vanderbilt Scramble Keypad Reader. Check these settings against the table for the appropriate mode version.

Pulse output specifications

The output pulses on the data transmission lines DO and DI are of approximately 100 microseconds duration at a repetition rate of approximately five milliseconds.

Electrical specifications

- Operating Temperature Range - -15 to + 50 degrees C
- Input Voltage - + 8V to + 12V DC unregulated
- Input Current:
  - Display off - l00mA (TYP) l80mA (MAX)
  - Display on - 280mA (TYP) 350mA (MAX)
  - User LED current - 20mA per LED
- INPUT 0-3 - LSTTL input (MATRIX, ENCODED modes)
- INPUT 0-3 - (RS232 mode) Maximum input voltage+ / - 30V
- INPUT 0-3 (RS422 mode) Maximum input voltage+ / - 7V (differential)
- OUTPUT 0-3 (LTTL output) (MATRIX, ENCODED modes)
- OUTPUT 0-3 (RS232 mode)
  - Minimum output voltage + / - 5V
  - Maximum output voltage + / - 1OV
- OUTPUT 0-3 (RS422 mode)
  - Minimum output voltage + / - 2V (differential)
  - Maximum output voltage + 5V
- External Buzzer, RED, - LSTTL input
  - Yellow, Output Enable,
  - Remote Disable
- Data Available - LSTTL output

Note: Operating the keypad from input voltages greater than + 8V will increase its power dissipation. For maximum reliability the keypad should be operated as near as possible to + 8V

The rear panel of the unit acts as a heat sink. Where possible the unit should be mounted so as to maximize air circulation around the rear panel.

Operating the keypad

Follow these instructions to operate the keypad.

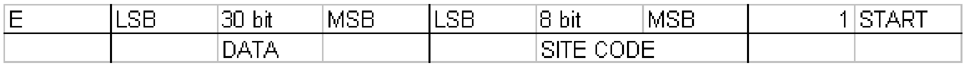
1. Press the "*" key to enable the display.
2. Enter the encoded ID. If the length of the ID is less than nine (9), press the "#" key to disable the display, and transmit the code (this is done automatically if the maximum number of digits are entered). Each keystroke causes a beep from the buzzer and a LED at the top of the keyboard to flash to confirm to the user that the entry has been received by the Vanderbilt Scramble Keypad Reader.
3. The entered code digits are accumulated, and then converted to a binary number before transmission. The block of data transmitted includes a site code set at the factory.
4. Pressing the "*" key during entry (i.e. before the "#" key is pressed) will re-scramble the digits. If no key is pressed within a period of eight (8) seconds, the display is automatically turned off.
5. The yellow and red user LED’s on the keypad are not driven by the keypad but may be driven by the Vanderbilt SMS. See the wiring diagram.
6. Pressing the "#" key while the "*" key is held pressed (and vice versa) results in a unique code being output to the Vanderbilt SMS, and a continuous tone at the keypad. This may be decoded as a doorbell, panic etc.

Operating mode

Mode 0

Code length - 1 to 9 digits.

The transmitted block length is 40 bits.



E	LSB	30 bit	MSB	LSB	8 bit	MSB	1	START
		DATA			SITE CODE			

BIT 1 is a start bit and is always “1”.

The last bit (bit 40) is an EVEN parity bit for the 30 data bits.

Setting the site code

The site code is set using the upper two rotary switches located behind the rubber grommet in the rear cover of the unit. The default factory set site code is 0 (zero). Select the required site code by rotating the switches until the arrow on the actuator points to the correct number. Each switch is numbered 0 to F, allowing 256 different site codes to be selected (from 00 to FF). The switch on the left sets the most-significant digit (MSD) of the site code, the switch on the right sets the least-significant digit (LSD) of the code. Disconnect power from the unit when altering the setting of these switches. The site code must match the site code defined in the Vanderbilt SMS software. The site code is defined using **System Manager>Site Code Sets** and **Site Codes** option.

Driving the user LEDs

Driving the YELLOW input to a logic LO (Ground) will light the yellow LED. Driving the RED input to a logic LO (Ground) will light the red LED. If not required these inputs may be left open circuit.

Firmware Information

The firmware Fcgs9_09.hex is designated for Vanderbilt Scramble Keypad Reader with card formats set for Vanderbilt Scramble Keypad III Mode 0: 40 Wiegand bits output, you can enter up to nine (9) digits as keypad ID. If the keypad ID is less than nine (9) digits, enter the code, and press "#" to transmit the code.

Enabled card formats in the firmware

- Magcard - Vanderbilt SMS encoded card
- Wiegand - Standard 26-bit
- HID 35-bit
- HID/ProxIF 37-bit
- Scramble keypad 40-bit

CHAPTER 17

Custom Enclosures

SRCNX (Legacy)-ENCL

Overview

This product has been designed to make large **Vanderbilt SMS** easier to install and service. The **Vanderbilt Custom Enclosures** are pre-wired, pre-assembled and pre-tested at the factory.

The SRCNX (Legacy)-ENCL and the VRINX-ENCL enclosures include a removable sub-panel, necessary power supplies, fuses, and wiring harness for a complete access control system and peripheral devices. The terminal blocks for landing all field wiring are clearly labeled. The SRCNX (Legacy) Reader Controller and VRINX Reader Interfaces are sold separately to allow customization. Please order the SRCNX (Legacy) and the VRINX with the designation NB (No Box). The Reader Controller is only installed in the SRCNX (Legacy)-ENCL and cannot be installed in the VRINX-ENCL. The Reader Interfaces are available with one (VRINX-1) or two (VRINX-2) output relays. When you place the order, specify if the Reader Interfaces should have one or two relays. All the SRCNX (Legacy) channels are available for Wireless (PIM-485) devices and VIP Locks on any SRCNX (Legacy) Reader Controller.

The SRCNX (Legacy)-ENCL enclosure can house one SRCNX-8 or one SRCNX-16 Reader Controller and up to (8) VRINX Reader Interfaces. The enclosure is 31" x 31" x 8" with a removable sub-panel, fuses, and wiring harness. The enclosure is supplied with one 24V 10-amp power supply for lock power and peripheral devices, and two 12VDC 12-amp hour gel cell batteries for battery backup. The enclosure also comes with one 24V 4-amp power supply for the SRCNX Reader Controller, and two 12VDC 12-amp hour gel cell batteries for battery backup. The terminal blocks for landing all field wiring are clearly labeled.

The VRINX-ENCL unit is used in conjunction with the SRCNX (Legacy)-ENCL to expand reader capacity from 8 to 16 VRINXs. The VRINX-ENCL must be tied to the SRCNX (Legacy)-ENCL unit containing the SRCNX (Legacy) board; the VRINX-ENCL does not include a Reader Controller. The expansion enclosure will house up to (8) VRINX Reader Interfaces. All Reader Interfaces are sold separately, to order devices without the small enclosures specify NB. This expansion enclosure will be connected to the SRCNX (Legacy)-ENCL with 1" conduit nipples. The expansion enclosure is 31" x 31" x 8" with removable sub-panel, fuses, and wiring harness. The enclosure is supplied with one 24V 10-amp power supply for lock power and peripheral devices, and two 12VDC 12 amp hour gel cell batteries for battery backup. The terminal blocks for landing all field wiring are clearly labeled.

Features

- Pre-wired and pre-tested enclosures with on-board power supplies have clearly marked quick connectors that greatly reduces setup times
- Design allows for easy replacement of all components
- Plug-and-use design that powers and supports all lock mechanisms, read-heads, contact inputs, PIR motion detectors and local annunciators
- Meets the rigorous requirements of nationwide installation and service
- Significantly reduces manpower requirements during installation and decreases disruption in client’s daily business
- Makes service and maintenance easy, the enclosure gives consistency to every site and reduces the training curve for personnel
- Clearly marked components within the custom enclosures allow a service technician to enter any site and be immediately familiar with the equipment
- All fail secure locks will stay functional after fire panel cuts power to all fail safe locks

Specifications

Electrical rating

- SRCNX (Legacy)-ENCL & VRINX-ENCL Input - 120VAC / 60Hz, 6 amp
- SRCNX (Legacy)-ENCL & VRINX-ENCL Output - 24VDC output - Output power is all power limited.
- Reader Maximum Output - 120mA @ 12VDC per reader (total readers shall not exceed 1.92 amps @ 12VDC)
- Lock Maximum Output - 1 Amp @ 24VDC per lock (total locks shall not exceed 6.5 amps @ 24VDC).
- PIR Maximum Output - 50mA @ 24VDC per PIR (total PIR units shall not exceed 1.15 amps @ 24VDC).
- Annunciator Maximum Output - 50mA @ 24VDC per Annunciator
(total Annunciator units shall not exceed 1.15 amps @ 24VDC)
- Cooling Fans maximum output - 18A @ 24VDC per cooling fan (two cooling fans per enclosure)
- The AL1024UL power supply (peripheral devices) shall not exceed a continuous load of 8 amps.
- Operating Temperature - 32 - 120 F (0 - 49 C)

Battery back-up

- SRCNX (Legacy) Battery Back-up - Two (2) 12VDC 12-amp hour gel cell batteries @ 8 amp continuous (not included with VRINX-ENCL). Located on the right-hand side of the enclosure
- Locks and Peripheral Devices -Two (2) 12VDC 12-amp hour gel cell batteries @ 2 amp continuous. Located on the left-hand side of the enclosure
- Automatic switch over to stand-by battery when AC fails
- Zero voltage drop when switched over to battery back-up
- A minimum of 4 hours of back-up is provided

Visual indicators (outside the enclosures)

AC Power LED is provided on the door of the enclosures (SRCNX-ENCL and the VRINX-ENCL). The LED on the SRCNX-ENCL is connected in series to the AC Power terminals on the AL-400ULXB and the AL-1024ULXB power supplies. The LED on the VRINX-ENCL is connected to the AC Power terminal on the AL-1024ULXB power supply. Wiring the LED in this manner avoids the back-up batteries from keeping the LED on.

Fuse ratings

- SRCNX Fuse Replacement - replace with a 5 amp @ 250V slow blow 5x22 mm fuse only
- Diode Block Fuse Plug Replacement - must be replaced with exact replacement, 5.6mA @ 24VDC, please contact Vanderbilt factory

Reference material

1. Vanderbilt SMS Software Manual
2. Drawings:
   - ENCLTB 8-24-06 Rev. 1 (Terminal Block Layout-affixed to the inside of the enclosure door)
   - ENCLDL 8-24-06 Rev. 1 (Device Layout-affixed to the inside of the enclosure door)

Product markings

- Numbered side terminal strips label to determine the inputs for field wiring
- Drawing ENCLTB is displayed on the inside of the door to indicate the terminal blocks numbers, their functions, and location of the LED lights
- Drawing ENCLDL is displayed on the inside of the door to indicate the general layout of the devices in the enclosure and to hand label the field devices for future service reference
- A label is displayed to indicate the date of manufacture, electrical ratings and rating of fuse replacements.
- Labels are placed near fuses for specific replacement ratings

Installation Instructions

Environmental conditions

- Room temperatures must be 32 - 120F (0 - 49C)
- Dust free, clean, and secured area
- Mount enclosures on fire rated plywood which is affixed to a solid wall covering i.e. sheetrock or bare cinder block.
- A minimum of 6" spacing between units and other equipment for free airflow of the internal fans

Mounting

1 The SRCNX-ENCL must be mounted or fastened to studs that are part of the building structure, which can support the weight of the enclosure.

2 We recommend two people to hang the enclosure. The sub panel can be removed to reduce the weight of the units.

3 The doors can be removed to reduce the weight of the unit. When removing doors from the panel: separate the quick disconnect for the AC fail indicator LED, separate the bonding straps using the quick disconnects. Lift the door slowly to free the hinge pins and remove the doors.

4 Mount white enclosure to the wall using provided mounting holes.

5 Recommended hardware to use - four ¼” x 3" lag bolts.

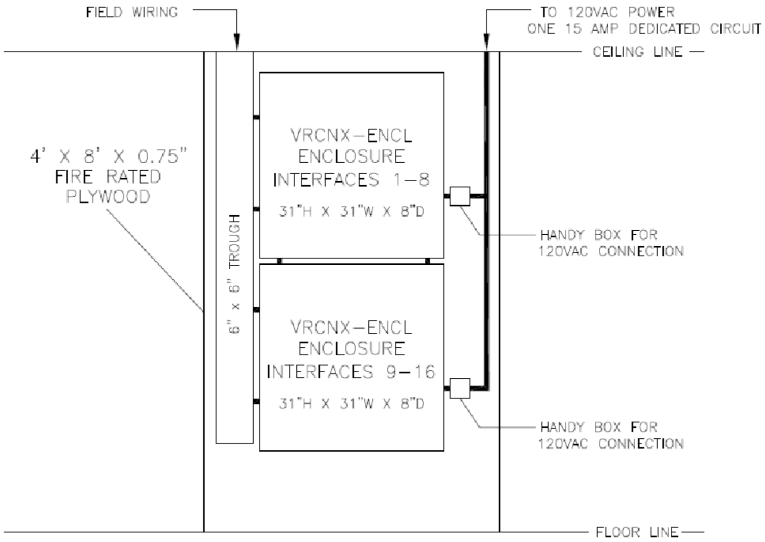
6 When using the VRINX-ENCL expansion model with the SRCNX-ENCL enclosure attach the expansion unit using 1" nipple connectors. The wire needed to connect the enclosures together is four 8 conductor - 18 AWG Stranded, Shielded and Twisted wire.

7 The wires will come from terminal strip 1 & 2 in the VRINX-ENCL and will be landed on expansion terminal strip numbers 1 & 2 in the SRCNX-ENCL, number for number on the terminal strips.

8 Batteries are included with the custom enclosures. Please refer to Figure 2 for recommended battery placement inside the enclosure.

9 The following is one example of a Wallfield Layout for a typical enclosure setup

Note: The SRCNX-ENCL and the VRINX-ENCL are shipped from the factory pre-assembled with the Reader Controller (SRCNX) and the Reader Interfaces (VRINX) boards. In the event of a board replacement or project upgrades, installation instructions have been provided.



Example of a Wallfield Layout

General information

- All field wiring must comply with NFPA 70 (NEC) and local wiring codes.
- All output wiring is power limited except the battery leads. Keep the battery leads separated from the field wiring by a minimum of ¼ inch spacing.
- All interconnecting devices must be UL Listed.
- All locks shall be 24VDC. Lock Maximum Output: 1 amp @ 24VDC per lock. Total lock power for SRCNX-ENCL shall not exceed 6.5 amps @ 24VDC. Total lock power for VRINX-ENCL shall not exceed 6.5 amps @ 24VDC.
- Grills are placed over internal fans for the technician's safety - do not remove.
- All internal wiring has been provided for your convenience - do not change internal wiring harness, unless instructed from authorized Vanderbilt personnel.
- When connecting two wires in any of the terminal block insertion plugs, the wire must be twisted together and then inserted for proper connectivity.
- Do not remove the High Voltage cover unless instructed by authorized Vanderbilt personnel.
- Use back-up batteries provided with the system and replace the batteries with the same voltage and amperage rating.
- The service on/off switch located in the middle of the high voltage shield is the main shut off for the primary power for the entire enclosure including the peripheral devices. The service on/off switch should be in the off position while any internal wiring is being performed.
- Two tamper switches have been mounted on the middle rails for the enclosure doors. Please be sure to close both the doors properly for the tamper switches to be effective and not send an alarm.

Electrical requirements

- A licensed electrician will need to supply 120VAC with one, 15 amp dedicated circuit per two enclosure boxes.
- All wiring must comply NFPA 70 (NEC) and local wiring codes.
- The electrician will install a handy box outside the enclosure and make all high voltage electrical connections in this handy box.

Installation

When the enclosures have been securely mounted to the wall, you can begin the installation process.

1. The sub panel must be mounted back into the enclosure using the provided stand-offs and hardware.
2. The doors must be re-installed with the bonding straps and the AC-fail LED reconnected to the chassis/enclosure. The AC-fail terminals on the power supplies have been wired in series to avoid the LED from staying on during the use of battery backup (SRCNX-ENCL only).
3. A BX pigtail has been provided at the right side of the enclosure for the electrical (120VAC) power connection. The provided pigtail has been punched through the enclosure and fastened with a BX clamp on the outside of the enclosure.

Distribution of 24VDC power in the enclosure

- The power for the SRCNX is supplied from the 24VDC 4-amp power supply in the enclosure; located under the high voltage metal shield.
- The power for the peripheral devices is supplied from the 24VDC 10-amp power supply in the enclosure; located under the high voltage metal shield. All locks must be 24VDC.

Wiring the access control locks

- **Lock power distribution** - The power for the locks is routed from the power supply through the RT-2 fire relay coil. The power is then passed through N/O (RT-2) to the Power Distribution Modules (PDM). The PDM unit will limit the power leaving the power supply and isolate the power to individual 2.5 amp output channels on the PDM. The individual outputs of the PDM are wired to the reader interface relays, then to the field device terminal strips. The wiring configuration for locks in non-fire alarm and fire alarm conditions are explained in more detail below.
- **Setting fail-safe and fail-secure Locks** - The enclosures are shipped from the factory in the fail-safe position (switch is open - up position). It is recommended that all fail-safe locks be installed in the same enclosure, if using multiple enclosures. Set the Fire Alarm Function Block (FAFB) switches to fit your application, open/up fail-safe or closed/down fail-secure. The FAFB sets the state of the lock condition in a fire alarm situation, determining fail-safe or fail-secure locks.
- **Fire alarm Condition** - In a fire alarm condition the 24VDC will pass through the RT-2 fire alarm N/C relay and will be distributed to the PDM #2. The output channels then go to the Fire Alarm Function Block (FAFB) and distribute power to the common side of the reader interface relays and distribute power to the fail-secure locks only. In a fire alarm condition the LED status on the RT-2 will be off, the PDM #1 will be off, and the PDM #2 will be off. Refer to drawing ENCLTB for block names and numbers, located on the door of the enclosure.
- **Non-fire alarm condition** - In a non-fire alarm condition the 24VDC will pass through the RT-2 fire alarm N/O relay and will be distributed to the PDM #1. The output channels then go to the diode terminal block. The diode terminal block will supply power to the common side of the reader interface relays. The diode terminal block will keep the voltage from back feeding through the diodes. In a non-fire alarm condition the LED status on the RT-2 will be on and the PDM #1 will be on. The PDM #2 LED will only be lit if there are fail-secure locks on the system. Any switch on the FAFB block in the closed position will cause the PDM #2 LED to be on. Refer to drawing ENCLTB for block names and numbers, located on the door of the enclosure.

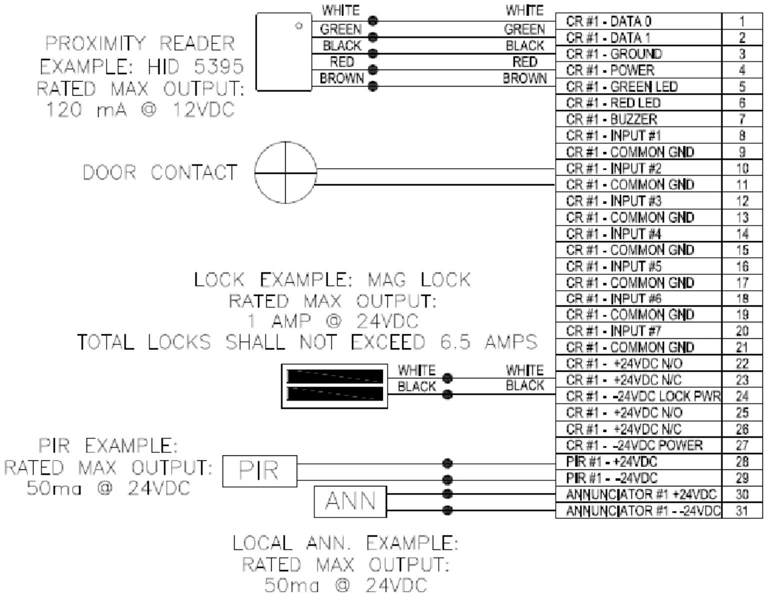
- **Fire panel tie-in** - Each enclosure will require one N/C dry contact relay from the building Fire Alarm Panel (FAPL). The internal wiring harness has been pre-wired to the side terminal strip for the fire tie-in. Use terminal numbers 249 (fire tie-in +) and 250 (fire tie-in -) for this function.

Peripheral device power distribution

The enclosures also provide 24VDC power for peripheral devices such as request to exit PIR's and local annunciators. The power is distributed through the PDM #3 to the numbered field device terminal blocks. The PDM unit will limit the power leaving the power supply and isolate the power to individual 2.5-amp output channels on the PDM. PDM #3 is located under the high voltage metal shield.

Wiring the access control door devices

- **Card readers** - The card readers will be wired to the field wiring terminal strips. The internal wiring to the VRINX units has been completed for you in the internal wiring harness. The terminal strips have been sectioned into wiring group blocks or door locations CR1 (Card Reader number one). The wire colors have been coordinated for HID card readers. The labels also let you know the function of each terminal if other card readers are used with the system.
- **Input devices** - The field wiring terminal strips also have the reader interface inputs and relays represented on them. The internal wiring to the VRINX units has been completed for you in the internal wiring harness. The inputs are labeled one through seven. Input one should always be used for the exit button, if applicable. If an exit button is not used in your application start with input number two. Inputs such as door contacts will be used on terminals two through seven. The motion detector PIR's and local annunciators have designated terminals that are powered from the peripheral power supply, so please use these marked terminals.



CR #1 - DATA 0	1
CR #1 - DATA 1	2
CR #1 - GROUND	3
CR #1 - POWER	4
CR #1 - GREEN LED	5
CR #1 - RED LED	6
CR #1 - BUZZER	7
CR #1 - INPUT #1	8
CR #1 - COMMON GND	9
CR #1 - INPUT #2	10
CR #1 - COMMON GND	11
CR #1 - INPUT #3	12
CR #1 - COMMON GND	13
CR #1 - INPUT #4	14
CR #1 - COMMON GND	15
CR #1 - INPUT #5	16
CR #1 - COMMON GND	17
CR #1 - INPUT #6	18
CR #1 - COMMON GND	19
CR #1 - INPUT #7	20
CR #1 - COMMON GND	21
CR #1 - +24VDC N/O	22
CR #1 - +24VDC N/C	23
CR #1 - -24VDC LOCK PWR	24
CR #1 - +24VDC N/O	25
CR #1 - +24VDC N/C	26
CR #1 - -24VDC POWER	27
PIR #1 - +24VDC	28
PIR #1 - -24VDC	29
ANNUNCIATOR #1 +24VDC	30
ANNUNCIATOR #1 - -24VDC	31

SRCNX (Legacy) reader controller replacement

1. Power down the entire enclosure using the service switch.
2. Unplug all of the blue connectors, channels 1 through 8 (reader interface connections).
3. Unplug the blue power connector (left side of the SRCNX board).
4. Unplug the green battery back-up connector (left side of the SRCNX board).
5. Remove 14 SRCNX mounting screws.
6. Replace with the new SRCNX using 14 mounting screws.

7. Connect all blue connectors channels 1 through 8 (reader interfaces).
8. Connect the blue power connector (left side of the SRCNX board).
9. Connect the green battery back-up connector (left side of the SRCNX board).

VRINX reader interface replacement

1. Power down the entire enclosure using the service switch.
2. Unplug all of the blue connectors.
3. Remove 4 VRINX mounting screws.
4. Replace with the new VRINX using 4 mounting screws.
5. Connect all blue connectors.

Battery replacement

- All output wiring is power limited except the battery leads.
- Keep the battery leads separated from the field wiring by a minimum of ¼ inch spacing.
- Do not block airflow for the fan.

Recommended maintenance

The Custom Enclosures should be properly maintained for longevity of the product. The recommended testing should be performed semi-annually.

Visual inspection

- A visual inspection should be made of that the wall the units are mounted on for water stains or damage. The ceiling above the units should be checked for water stains or damage.
- A visual inspection of the outside of the units for tampering or damage. Make sure the lock is intact and functional.
- The AC Fail indicator LED should not be on.

Inside the custom enclosures

- When the doors are opened, make sure the tamper switches are working and sending an alarm.
- Make sure the fans are functional and the safety grills are still screwed in place.
- A physical inspection should be performed to look for any loose or disconnected wires.
- The back-up batteries should be inspected for corrosion and then checked for the proper voltage. The batteries should be replaced every 3 years or earlier if necessary.
- The SRCNX fuse should not be blown.
- Check the LED status. Follow the LED on/off conditions for fail-safe or fail-secure locks in a non fire alarm condition.

IP addressable module installation (not evaluated by UL)

- The IP addressable module provides 10/100 Base T ethernet connectivity for the SRCNX reader controllers. The IP addressable module snaps onto the SRCNX board on the right-hand side of the board. The jumper setting (W12) must be on 2 and 3 (LAN).
- See your network administrator for the static IP address that will be assigned to your IP addressable module (SIPNX-100).
- Check the network IP address of the default gateway used by the IP module to see if it reaches the CIM (if applicable).
- Check the net mask for the connection.
- Check the node address / MAC address of the IP module.
- The format for the node address / MAC address is displayed as: 00-02-4a-64-45-b3. This is located on the white sticker on the IP module (SIPNX-100) itself.
- The IP address of the CIM workstation will be communicating to the IP module.

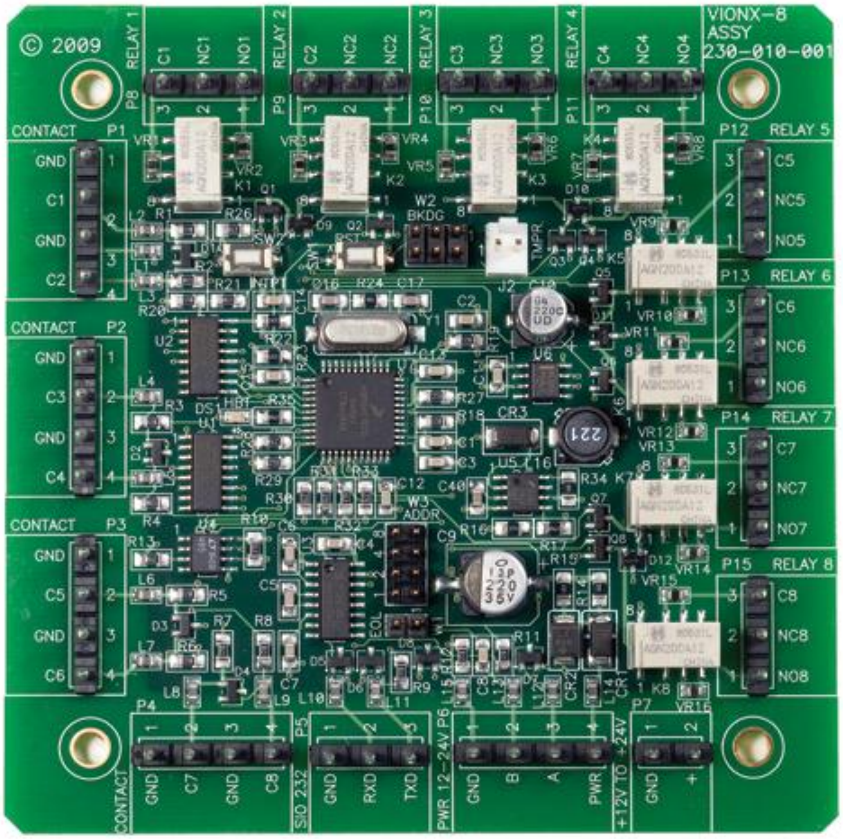
Dial-up modem installation (not evaluated by UL)

- The dial-up modem provides data communication via a telephone line.
- The dial-up modem snaps onto the SRCNX on the left-hand side of the board and then to a standard telephone jack for a 2400 baud communication.

Note: Please refer to Vanderbilt Security Management System User Manual Form UM 8-24-06 Rev. 1 for programming your Vanderbilt Security Management System.

CHAPTER 18

VIONX-8



VIONX-8

Overview

The **VIONX-8** provides 8 supervised or unsupervised input contacts and 8 SP/DT mechanical latching output relays. The VIONX-8 is an input/output expansion module for the VRCNX-R. Any input can be associated with any output response or a multitude of output responses within the same VRCNX-R network. The VIONX-8 can be utilized to provide alarm control and/or elevator floor control.

Note: For the VIONX-8 to communicate with the VRCNX-R, the VRCNX-R must have firmware v5.92 or higher installed.

Features

- 8 one-amp SP/DT output relays
- 8 supervised or unsupervised input contacts, normally open or normally closed
- Contacts can be defined as alarms, door status, egress or other environmental conditions
- Provides alarm control and elevator control
- Connects to the communication channels on the VRCNX-R
- Can be powered from the VRCNX-R or via a 24VDC Rated UL 294 Listed Power Limited external power supply
- One or more VIONX-8 modules can be used to provide floor control with each VIONX-8 module being capable of controlling up to 8 floors (1 contact per floor - subject to the VRCNX-R memory requirements)

Specification

- Dimensions - 4 3/16" x 4 3/16” x 2 1/2” D
- Power Requirements - 14 to 24 VDC
- Ambient temperature - 0º to 49º C or 32º to 120º F
- Data communication between the VIONX-8 and the VRCNX-R is RS-485 protocol
- Maximum distance between VIONX-8 and VRCNX-R is 4000 feet (Data Only) (refer to Recommended Wire Chart)

VIONX-8 enclosure

VIONX-8 standard enclosure - An enclosure with a hinged, screw-down door is included with your system for each VIONX-8 board. Tamper switch, lock & key options available.

Features

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

Standard enclosure installation

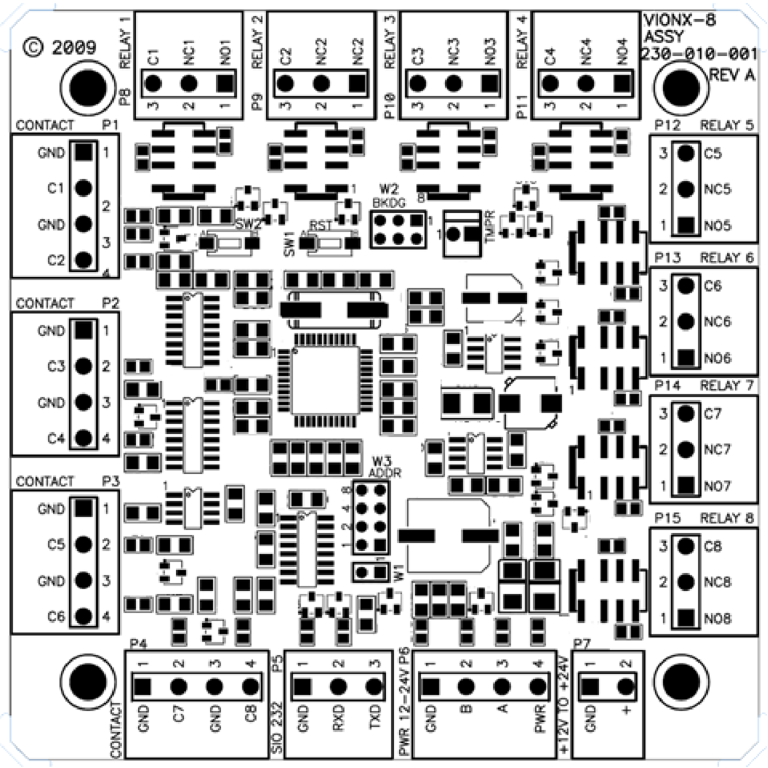
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- Clean and dust free room
- 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 knock-outs 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 1-1/2” lag bolts

VIONX-8 I/O expansion pin layout



VIONX-8 I/O expansion pin functions

P6 - Power source and communication wiring

The VIONX-8 can be powered directly from the VRCNX-R (refer to Recommended Wire Chart). When the VIONX-8 is being powered from the VRCNX-R the power source can be either 14VDC or 24VDC.

- Pin 1 is Ground (GND)
- Pin 2 is Data B (B)
- Pin 3 is Data A (A)
- Pin 4 is Power (PWR)

P7 - External Power Source

The VIONX-8 can be powered from a 24VDC Rated UL 294 Listed Power Limited external power supply if distances are too great from the VRCNX-R. Power can be 14VDC or 24VDC.

- Pin 1 is Ground (GND)
- Pin 2 is Power (+)

P 1 - P 4 - Contact inputs

The VIONX-8 has 8 supervised or unsupervised contact points (P1-P4). Each contact point has an individual ground. Supervised door contacts have maximum wire length of 1,000 feet. Unsupervised door contacts have maximum wire length of 2,000 feet.

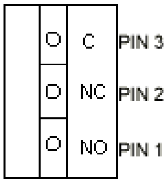
P8 to P15 - Relays outputs

The VIONX-8 comes with 8 relay outputs (P8 through P15). Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 1 amp. Inductive loads require noise suppression kit.

Pin 1 - Normally Open

Pin 2 - Normally Closed

Pin 3 - Common



SW1 - Hardware Reset Switch

The Reset Switch clears all the memory on the VIONX-8. Press the reset switch for 3 seconds to clear the memory.

Note: Make sure that there is power on VIONX-8 (P6 or P7)

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

SW2 - Software Reset Switch

Recommended for factory use only.

W2 - Factory use only

W2 is for factory use only. Do not add a jumper under normal operating conditions.

W 1 - RS-485 Communication Line Terminal

W1 is the P6 Pin2/Pin 3 RS 485 communication line terminator.

In a daisy chain configuration, the VIONX-8 are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices are not communicating.

W3 - VIONX-8 addressing

The address is dependent on the position of jumpers on these pins. See the section on Addressing the VIONX-8 for details.

DS1 LED Description

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

J2 - On Board Tamper Connection

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

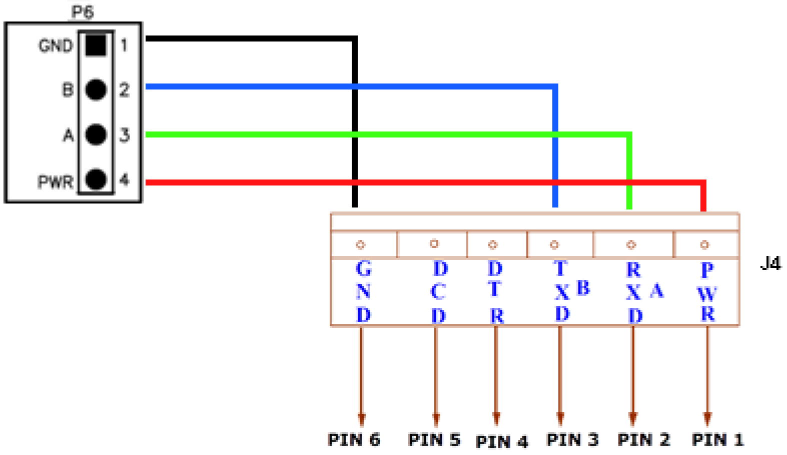
Pins Not Used

W2 - BKDG: No jumper required for normal operation.

Connecting to VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VIONX-8 is via RS-485 protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and P6 on the VIONX-8. In the following example we have selected J4 on the VRCNX-R/M/A board.

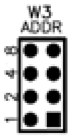
Note: Only identical devices are allowed on same channels.



Data communication between the VIONX 8 and the VRCNX-R/M/A

VIONX 8 - P6	VRCNX-R/M/A - J4
Pin 1 (GND)	Pin 6 GND
Pin 2 (B)	Pin 3 TXDB
Pin 3 (A)	Pin 2 RXDA
Pin 4 (PWR)	Pin 1 PWR

Addressing the VIONX-8

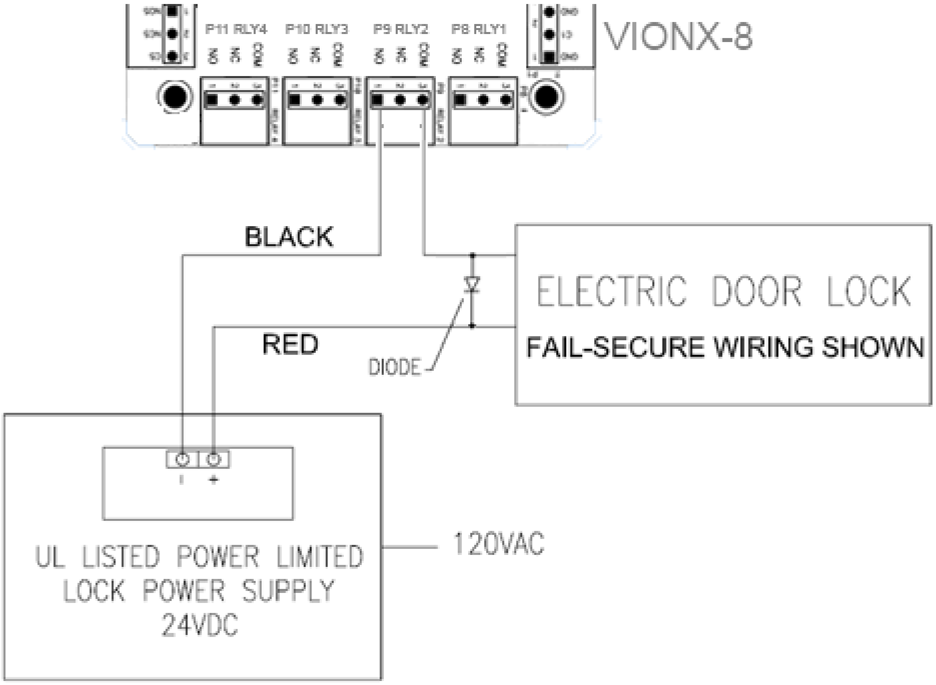


VIONX-8 Addressing jumpers

VIONX-8 Addr. A	Jumper Locations	VIONX-8 Addr. B	Jumper Locations
1	1 2 4 8	1	1 2 4 8
1	1 2 4 8	2	2 4 8
1	1 2 4 8	3	1 4 8
1	1 2 4 8	4	4 8
1	1 2 4 8	5	1 2 8
1	1 2 4 8	6	2 8
1	1 2 4 8	7	1 8
1	1 2 4 8	8	8
2	2 4 8	9	1 2 4
2	2 4 8	10	2 4
2	2 4 8	11	1 4
2	2 4 8	12	4
2	2 4 8	13	1 2
2	2 4 8	14	2
2	2 4 8	15	1
2	2 4 8	16	No Jumpers

Installing Diode for Lock Wiring - Relay

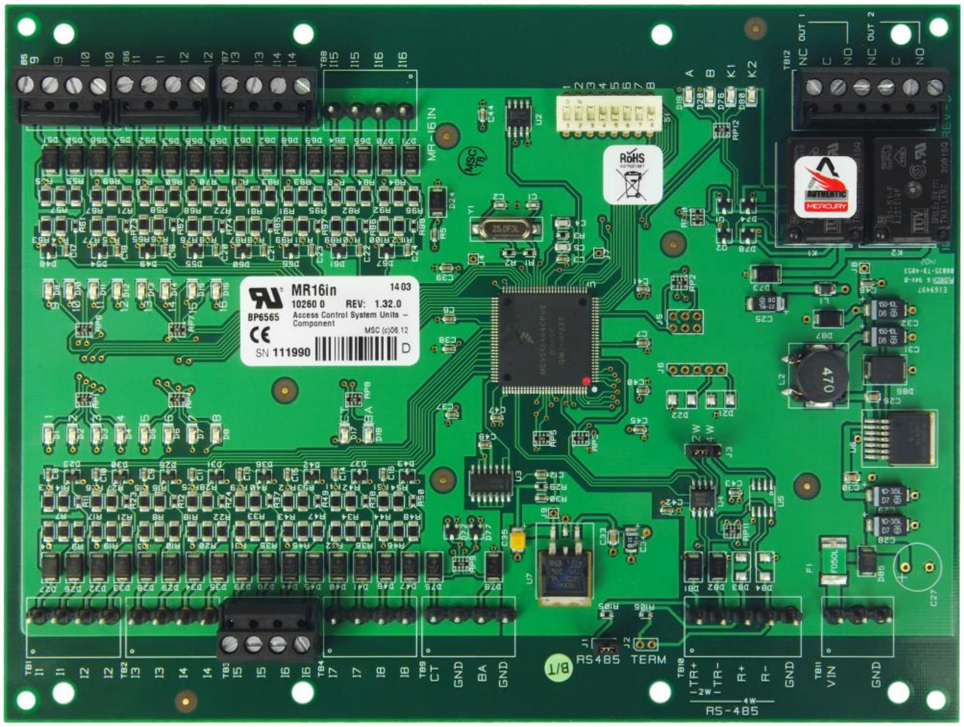
A diode is supplied with the VIONX-8 which should be fitted across 12V and COM to protect the relay contacts.



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. (Above diagram is of Fail Open).

CHAPTER 19

VI-16IN / VI-16INS3



16 Contact Input Module

Overview

The **VI-16IN** provides 16 supervised or unsupervised input contacts. The VI-16IN is an input expansion module for the VRCNX-R/M/A. Any input can be associated with an output response on a VI-16O output expansion module, VIONX-8 input-output expansion module or a multitude of output responses within the same VRCNX-R/M/A network. The VI-16IN can be utilized to provide alarm control and/or elevator floor control.

Note: VRCNX-R/M firmware v6.60 or higher is required for the VI-16IN to communicate with the VRCNX-R/M.

Features

- 16 supervised or unsupervised input contacts, normally open or normally closed
- Contacts can be defined as alarms, door status, egress or other environmental conditions
- Provides alarm control and elevator control
- Connects to the communication channels on the VRCNX-R/M/A using SMS-M protocol
- Can be powered from the VRCNX-R/M/A or via a 12 or 24 VDC Rated UL 294 Listed Power Limited external power supply
- One or more VI-16N modules can be used to provide floor control with each VI-16IN module being capable of controlling up to 16 floors (1 contact per floor - subject to the VRCNX-R/M/A memory requirements) in conjunction with a VI-16O (1 relay output per floor).

Specification

- Dimensions: 6” W x 8” H x 1” D (152mm x 203mm x 25.4mm)
- Power Requirements: 12 to 24 VDC
- Ambient temperature: 0º to 70º C or 32º to 158º F
- Data communication between the VI-16IN and the VRCNX-R/M/A is over RS-485 using SMS-M protocol
- Maximum distance between VI-16IN and VRCNX-R/M/A is 4000 feet (Data Only) (refer to Recommended Wire Chart)

VI-16IN enclosure

VI-16IN standard enclosure – An enclosure with a hinged, screw-down door is included with your system for each VI-16IN board. Tamper switch, lock & key options available.

Features

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

Standard enclosure installation

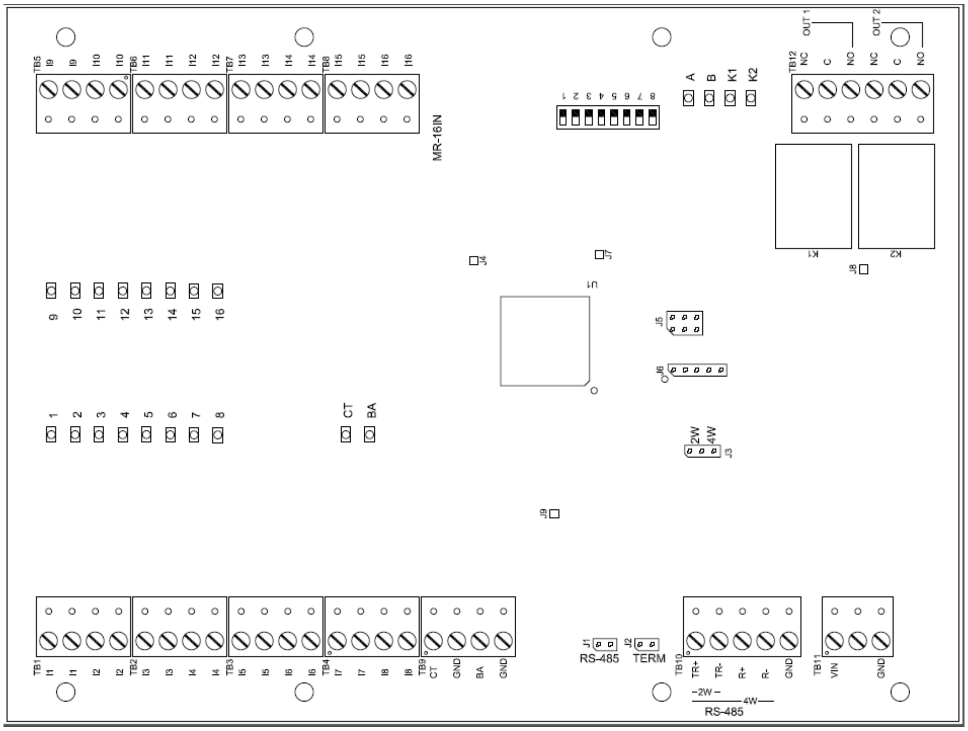
Environmental conditions

- Ambient Temperature: 0º to 70º C or 32º to 158º F
- Clean and dust free room
- 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 knock-outs 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 1-1/2” lag bolts

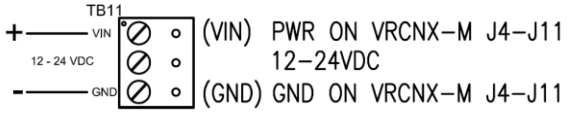
VI-16IN Input Expansion pin layout



VI-16IN Input Expansion pin functions

TB11 – Power source

VI–16IN POWER REQUIREMENTS: 12–24VDC
VI–16IN CURRENT CONSUMPTION: 120mA MAX

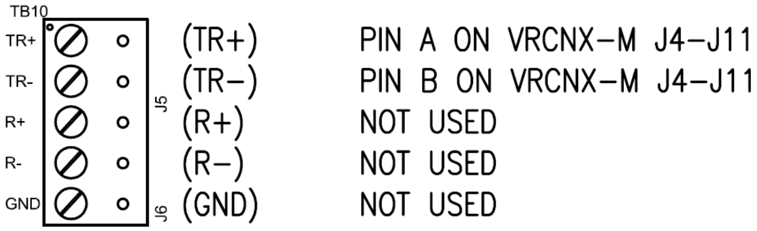


TB11 – External Power Source

The VI-16IN can be powered from 12 – 24 VDC Rated UL 294 Listed Power Limited external power supply if distances are too great from the VRCNX-R/M. Power can be 12 or 24VDC.

- PIN 1 is Power (VIN)
- PIN 3 is Ground (GND)

TB10 – RS485 Data Communications


TB10
TR+ (TR+) PIN A ON VRCNX-M J4-J11
TR- (TR-) PIN B ON VRCNX-M J4-J11
R+ (R+) NOT USED
R- (R-) NOT USED
GND (GND) NOT USED
J5
J6

TB1 – TB 8 Contact inputs

The VI-16IN has 16 **SMS software controlled** supervised or unsupervised contact points (TB1 – TB8). Each contact point has an individual ground. Supervised door contacts have maximum wire length of 1,000 feet. Unsupervised door contacts have maximum wire length of 2,000 feet.

J1 - RS485 Communication Line Terminator

In a daisy chain configuration, the VI-16IN are connected to one another in series. Up to 16 devices can be connected to a reader controller (8 each on 2 channels). This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices are not communicating.

J3 – RS485 Communication 2 or 4-Wire Selection

SMS support 2-wire configuration only.

S1 – VI-16IN addressing

The address of the VI-16IN is dependent on the position of the DIP switches in S1.

VI-16IN Address (SMS Address)	DIP Switch Position							
	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
VI-16IN as VRCNX-M3/A3 Onboard Inputs								
14 (15)	OFF	ON	ON	OFF	ON	ON	ON	OFF

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

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

VI-16IN as VRCNX-M3/A3 Onboard Inputs
Requires VRCNX-M/A Switch Configuration as VRCNX-M2/A2 and
SMS Software Configuration as VRCNX-M3/A3

A – BA Status LEDs

- Powered Up: All LEDs OFF
- Initialization: LEDs 1 – 16, CT, BA, A & B 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
- LED 5: IN5 Status
- LED 6: IN6 Status
- LED 7: IN7 Status
- LED 8: IN8 Status
- LED 9: IN9 Status
- LED 10: IN10 Status
- LED 11: IN11 Status
- LED 12: IN12 Status
- LED 13: IN13 Status
- LED 14: IN14 Status
- LED 15: IN15 Status
- LED 16: IN16 Status
- LED CT: Cabinet Tamper
- LED BA: Power Fault
- LED K1: Relay 1 Energized
- LED K2: Relay 2 Energized

TB9 – On Board Tamper Connection

Two unsupervised on-board dedicated contacts are provided for environmental monitoring. Contact configuration is configured via SMS.

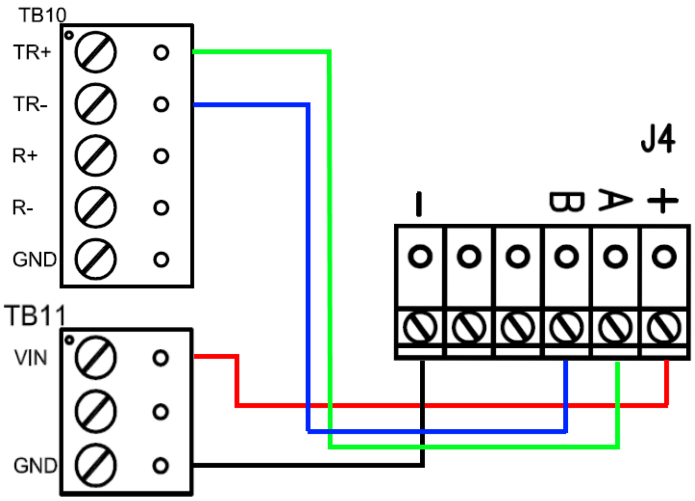
Input 17 is user definable for onboard Cabinet Tamper monitoring and custom labeling can be defined in SMS.

Input 18 is user definable for UPS Fault monitoring and custom labeling can be defined in SMS.

Connecting to VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VI-16IN is via RS-485 using SMS-M protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and TB10 on the VI-16IN. In the following example we have selected J4 on the VRCNX-R/M/A board.

Note: Only identical protocol devices are allowed on same channels.

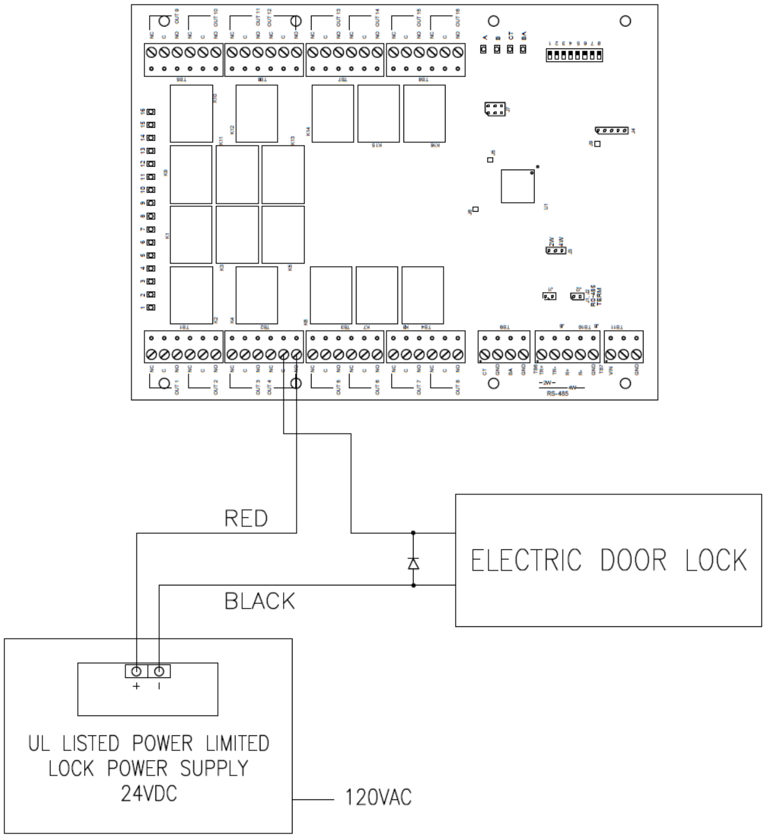


Data & Power connections between VI-16O and VRCNX-R/M/A

VI-16IN	VRCNX-R/M/A J4
TB11 PIN 1 – VIN	PIN 1 – Power
TB11 PIN 3 - GND	PIN 6 – GND
TB10 PIN 1 – TR+	PIN 2 – RXD (A)
TB10 PIN 2 – TR-	PIN 3 – TXD (B)
No connection	PIN 4 - DTR
No connection	PIN 5 - DCD

Installing Diode for Lock Wiring - Relay

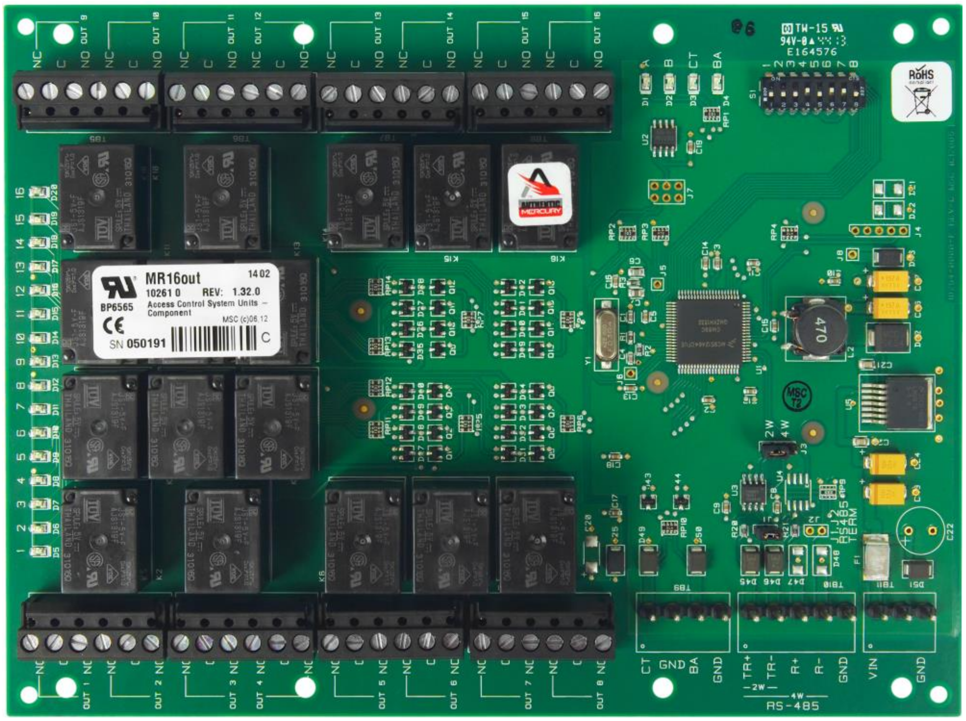
A diode is supplied with the VI-16IN which should be fitted across 12V / 24V and COM to protect the relay contacts.



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.

CHAPTER 20

VI-16O / VI-16OS3



16 Relay Output Module

Overview

The **VI-16O** provides 16 SP/DT mechanical latching output relays. The VI-16O is a relay output expansion module for the VRCNX-R/M/A. The relay outputs can be associated with any inputs on a VI-16IN input expansion module, VIONX-8 input-output expansion module or a multitude of input responses within the same VRCNX-R/M/A network.

Note: VRCNX-R/M firmware v6.60 or higher is required for the VI-16O to communicate with the VRCNX-R/M.

Features

- 16 one-amp SP/DT output relays
- Connects to the communication channels on the VRCNX-R/M/A using SMS-M protocol
- Can be powered from the VRCNX-R/M/A or via a 12 – 24 VDC Rated UL 294 Listed Power Limited external power supply

Specification

- Dimensions: 6” H x 8” W x 1” D (152mm x 203mm x 24.4mm)
- Power Requirements: 12 to 24 VDC
- Ambient temperature: 0º to 70º C or 32º to 158º F
- Data communication between the VI-16O and the VRCNX-R/M/A is over RS-485 using SMS-M protocol
- Maximum distance between VI-16O and VRCNX-R/M/A is 4000 feet (Data Only) (refer to Recommended Wire Chart)

VI-16O enclosure

VI-16O standard enclosure – An enclosure with a hinged, screw-down door is included with your system for each VI-16O board. Tamper switch, lock & key options available.

Features

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

Standard enclosure installation

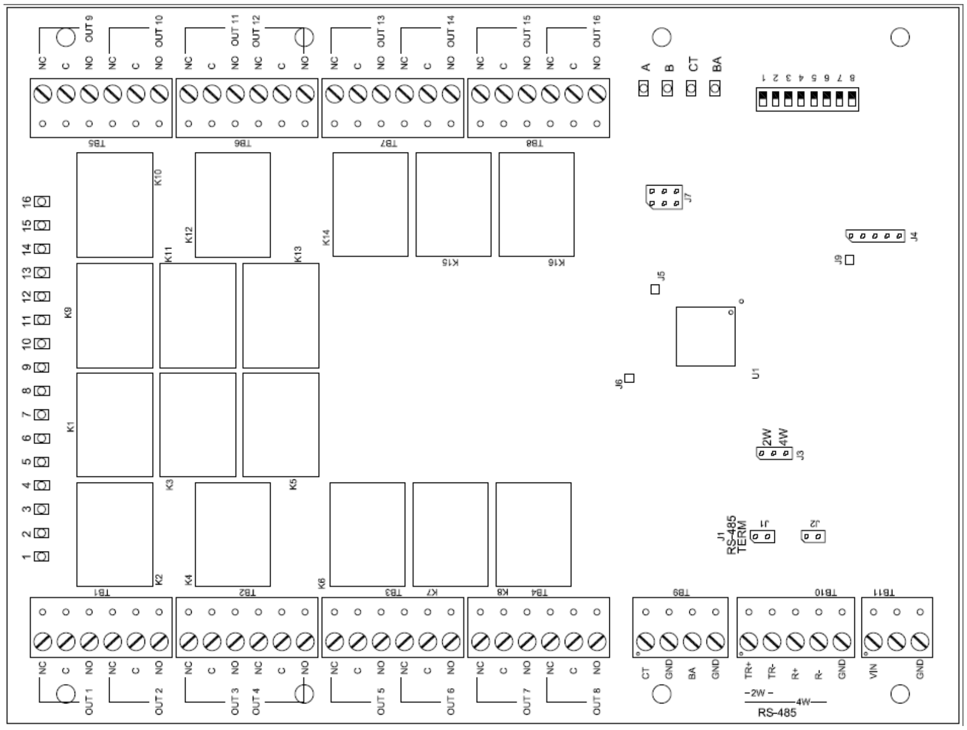
Environmental conditions

- Ambient Temperature: 0º to 70º C or 32º to 158º F
- Clean and dust free room
- 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

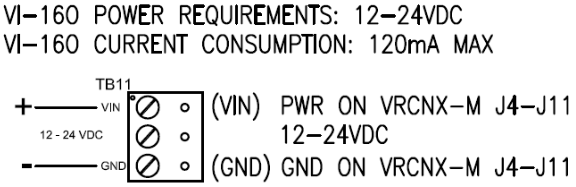
- Field Wiring - It is recommended that you drill holes or punch the knock-outs in the metal enclosure for field wiring before mounting the enclosure to the wall.
- A non-metallic sleeve is recommended to protect the wiring where it enters the cabinet.
- Mount the enclosure to the wall using the provided mounting holes.
- Recommended mounting hardware: Four 1/4” x 1-1/2” lag bolts

VI-16O Output Expansion pin layout



VI-16O Output Expansion pin functions

TB11 – Power source

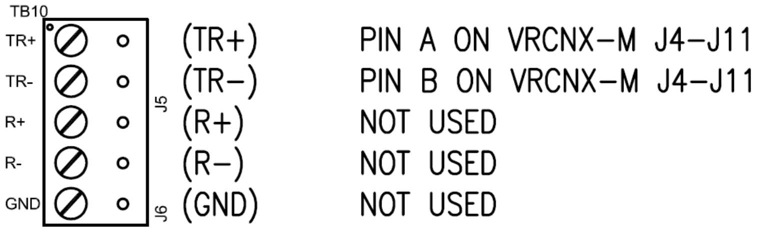

VI–16O POWER REQUIREMENTS: 12–24VDC
VI–16O CURRENT CONSUMPTION: 120mA MAX

TB11 – External Power Source

The VI-16O can be powered from 12 – 24 VDC Rated UL 294 Listed Power Limited external power supply if distances are too great from the VRCNX-R/M/A. Power can be 12 or 24VDC.

- PIN 1 is Power (VIN)
- PIN 3 is Ground (GND)

TB10 – RS485 Data Communications



TB1 – TB 8 Relay outputs

The VI-16O has 16 **SMS software controlled** relay outputs (TB1 – TB8). Each relay is rated at 5A @ 30 VDC.

J1 - RS485 Communication Line Terminator

In a daisy chain configuration, the VI-16O are connected to one another in series. Up to 16 devices can be connected to a reader controller (8 each on 2 channels). This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices are not communicating.

J3 – RS485 Communication 2 or 4-Wire Selection

SMS support 2-wire configuration only.

S1 – VI-16O addressing

The address of the VI-16O is dependent on the position of the DIP switches in S1.

VI-16O Address (SMS Address)	DIP Switch Position							
	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
VI-16O as VRCNX-M3/A3 Onboard Inputs								
15 (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

VI-16O as VRCNX-M3/A3 Onboard Inputs
Requires VRCNX-M/A Switch Configuration as VRCNX-M2/A2
and SMS Software Configuration as VRCNX-M3/A3

A – BA Status LEDs

- Powered Up: All LEDs OFF
- Initialization: LEDs 1 – 16, CT, BA, A & B 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: OUT1 Status
- LED 2: OUT2 Status
- LED 3: OUT3 Status
- LED 4: OUT4 Status
- LED 5: OUT5 Status
- LED 6: OUT6 Status
- LED 7: OUT7 Status
- LED 8: OUT8 Status
- LED 9: OUT9 Status
- LED 10: OUT10 Status
- LED 11: OUT11 Status
- LED 12: OUT12 Status
- LED 13: OUT13 Status
- LED 14: OUT14 Status
- LED 15: OUT15 Status
- LED 16: OUT16 Status
- LED CT: Cabinet Tamper
- LED BA: Power Fault

TB9 – On Board Tamper Connection

Two unsupervised on-board dedicated contacts are provided for environmental monitoring. Contact configuration is configured via SMS.

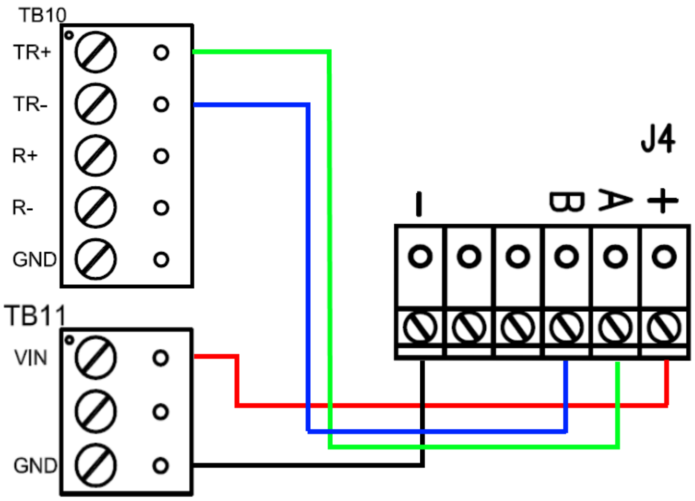
Input 17 is user definable for onboard Cabinet Tamper monitoring and custom labeling can be defined in SMS.

Input 18 is user definable for UPS Fault monitoring and custom labeling can be defined in SMS.

Connecting to VRCNX-R/M/A

Communication between a VRCNX-R/M/A reader controller and a VI-16O is via RS-485 using SMS-M protocol. Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board and TB10 on the VI-16O. In the following example we have selected J4 on the VRCNX-R/M/A board.

Note: Only identical protocol devices are allowed on same channels.

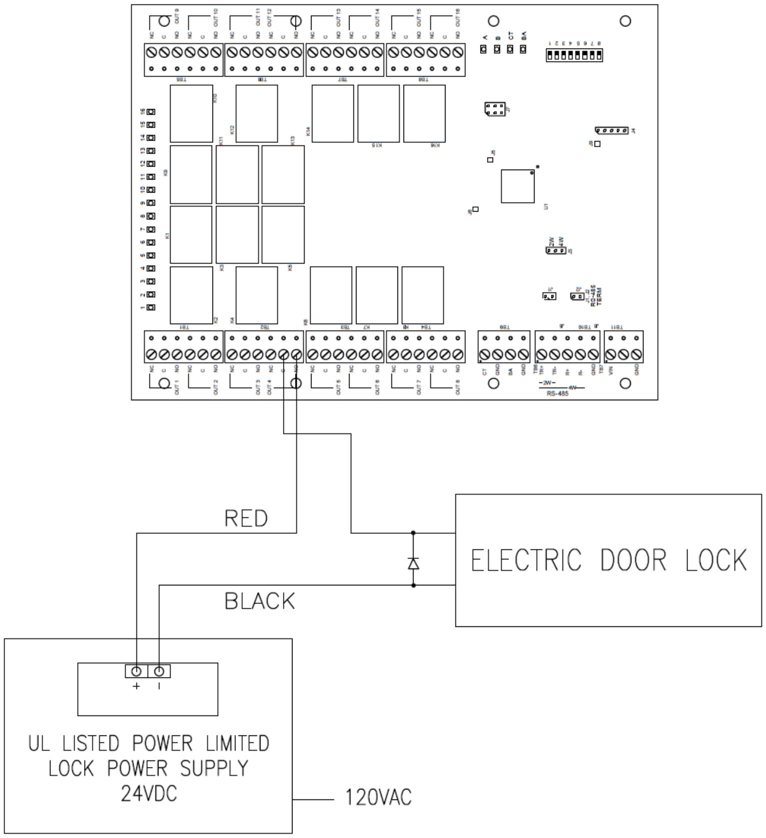


Data & Power connections between VI-16O and VRCNX-R/M/A

VI-16O	VRCNX-R/M/A J4
TB11 PIN 1 – VIN	PIN 1 – Power
TB11 PIN 3 - GND	PIN 6 – GND
TB10 PIN 1 – TR+	PIN 2 – RXD (A)
TB10 PIN 2 – TR-	PIN 3 – TXD (B)
No connection	PIN 4 - DTR
No connection	PIN 5 - DCD

Installing Diode for Lock Wiring - Relay

A diode is supplied with the VI-16IN 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.

CHAPTER 21

SIONX-24 (Legacy)

Input/Output Expansion Module

Overview

The **SIONX-24 (Legacy)** provides 24 supervised or unsupervised input contacts and 24 SP/DT mechanical latching output relays. The SIONX-24 (Legacy) is an input/output expansion module for the SRCNX (Legacy). Any input can be associated with any output response or a multitude of output responses within the same SRCNX (Legacy) network. The SIONX-24 can be utilized to provide alarm control and/or elevator floor control.

Features

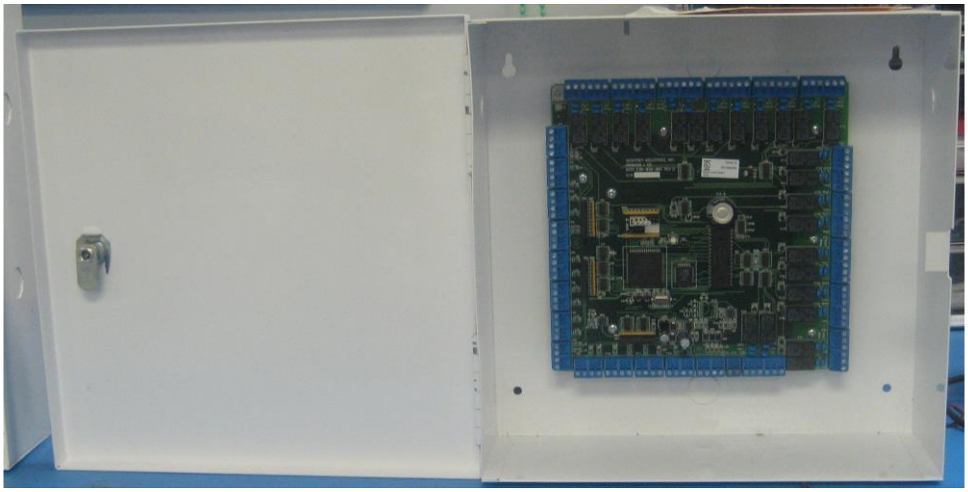
- 24 two-amp SP/DT output relays
- 24 supervised or unsupervised input contacts, normally open or normally closed
- Contacts can be defined as alarms, door status, egress or other environmental conditions
- Provides alarm control and elevator control
- Connects to the communication channels on the SRCNX (Legacy)
- Can be powered from the SRCNX (Legacy) or via an external power supply
- One or more SIONX-24 modules can be used to provide floor control
- Each SIONX-24 module is capable of up to 24 floors (1 contact per floor - subject to the SRCNX (Legacy) memory requirements)

Specification

- Dimensions - 8” x 8”
- Enclosure - 12” x 12” x 4”
- Power Requirements - 12 to 24 VDC; 120 mA at 12 VDC
- Ambient temperature - 0º to 49º C or 32º to 120º F
- Data communication between the SIONX-24 (Legacy) and the SRCNX (Legacy) is RS-485 protocol
- Maximum distance between SIONX-24 (Legacy) and SRCNX (Legacy) is 4000 feet (refer to Recommended Wire Chart)

SIONX-24 (Legacy) standard enclosure

SIONX-24 (Legacy) standard enclosure - An enclosure with a hinged door and a lock is included with your system for each SIONX-24 board. The tamper proof switch enables the system to send an alarm whenever someone opens the enclosure.



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 12” x 4”

Standard enclosure installation

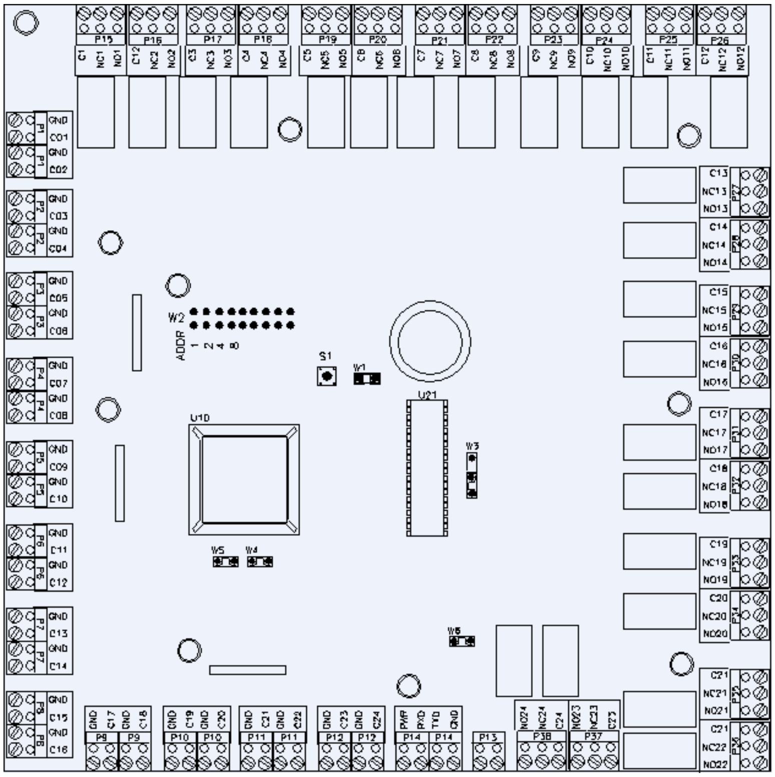
Environmental conditions

- Ambient Temperature: 0º to 49º C or 32º to 120º F
- Clean and dust free room
- 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 knock-outs 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 1-1/2” lag bolts

SIONX-24 I/O expansion pin layout



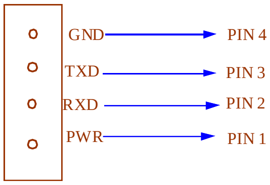
SIONX-24 I/O expansion pin functions

P13 - External power source

The SIONX-24 can be power from an external power supply if distances are too great from the SRCNX (Legacy). The SIONX-24 will accept 16VAC. The recommended optional power supply is the S16H-NX. Be polarity conscious.

P14 - Power source and communication wiring

The SIONX-24 can be powered directly from the SRCNX (Legacy) (refer to Recommended Wire Chart). When the SIONX-24 is being powered from the SRCNX (Legacy) the power source can be either 12VDC or 24VDC (polarity is not a concern).



Data communication between the VIONX 24 and the SRCNX (Legacy)

VIONX 24 - P14	SRCNX (Legacy) - J4
Pin 1 (PWR)	Pin 1 PWR
Pin 2 (RXD)	Pin 2 RXDA
Pin 3 (TXD)	Pin 3 TXDB
Pin 4 (GND)	Pin 6 GND

P 1 - P 12 - Contact inputs

The SIONX-24 has 24 supervised or unsupervised contact points (P1-P24). Each contact point has an individual ground. Supervised door contacts have maximum wire length of 1,000 feet. Unsupervised door contacts have maximum wire length of 2,000 feet.

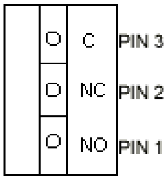
K1 to K24 - Relays outputs

The SIONX-24 comes with 24 relay outputs (K1 through K24). Relays are single pole/ double throw, mechanically latching and are rated at 30 VDC @ 2 amp. Inductive loads require noise suppression kit.

Pin 1 - Normally Open

Pin 2 - Normally Closed

Pin 3 - Common



S 1 - Reset switch

The Reset Switch clears all the memory on the SIONX-24 I/O Expansion Module. Press the reset switch for 3 seconds to clear the memory.

Note: Make sure that there is power on SIONX-24 (P13 or P14)

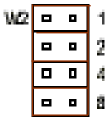
W4 and W5 - Factory use only

W4 & W5 are for factory use only. Do not add a jumper under normal operating conditions.

W 6 - RS-485 line terminal

In a daisy chain configuration, the SIONX-24 are connected to one another in series. Up to 16 devices can be connected to a reader controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices are not communicating with the SRCNX (Legacy).

W2 - SIONX-24 addressing



SIONX-24 Addressing jumpers

SIONX-24 Addr. A	Jumper Locations	SIONX-24 Addr. B	Jumper Locations
1	1 2 4 8	1	1 2 4 8
1	1 2 4 8	2	2 4 8
1	1 2 4 8	3	4 8
1	1 2 4 8	4	1 4 8
1	1 2 4 8	5	1 2 8
1	1 2 4 8	6	2 8
1	1 2 4 8	7	1 8
1	1 2 4 8	8	8
2	2 4 8	9	1 2 4
2	2 4 8	10	2 4
2	2 4 8	11	1 4
2	2 4 8	12	4
2	2 4 8	13	1 2
2	2 4 8	14	2
2	2 4 8	15	1
2	2 4 8	16	

Addressing jumpers

Jumper 5 and 6: No jumpers (Not used)

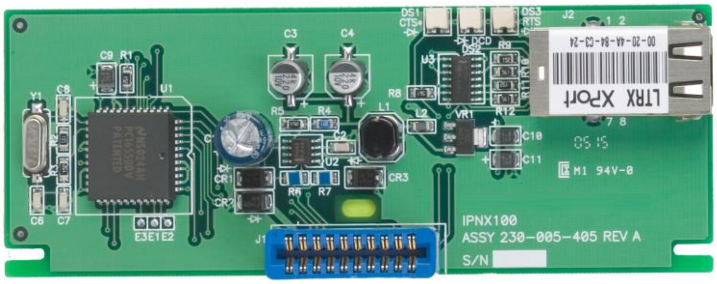
Jumper 7: No jumper (For future use)

Jumper 8: For diagnostic use only.

If communication is lost with the SRCNX (Legacy) and the jumper is on, by closing contact input X, it will energize relay output X.

CHAPTER 22

SIPNX-100 (Legacy)



IP addressable module

Overview

The SIPNX-100 (Legacy) module provides TCP/IP ethernet connectivity for the SRCNX (Legacy) series of reader controllers. This device will operate with the SRCNX-2, SRCNX-8 and the SRCNX-16.

Specifications

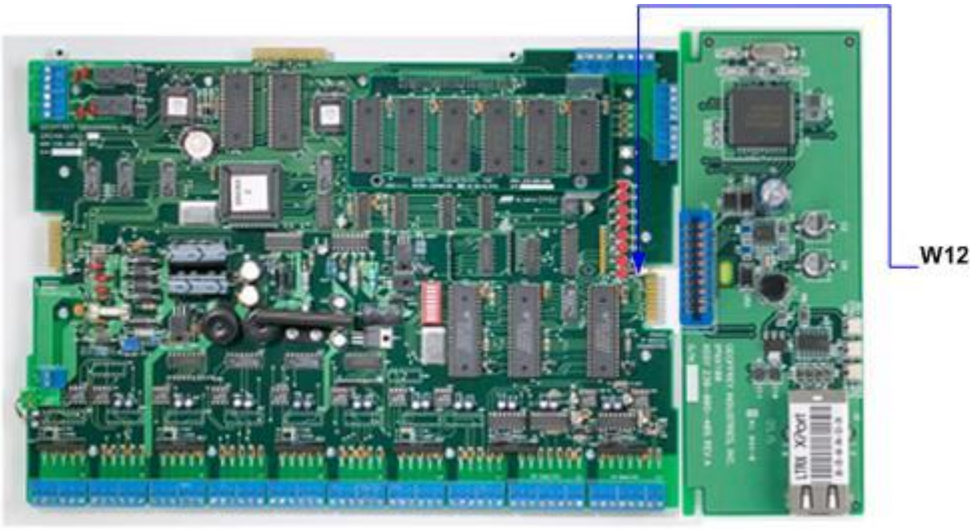
- Dimensions - 5-1/4” x 2”
- Power Requirements - 12VDC
- Ambient Temperature - 0º to 49º C or 32º to 120º F
- Allows the SRCNX (Legacy) to communicate via TCP/IP ethernet

Warning: Failure to follow these directions may lead to malfunctioning of the devices and also void the warranty.

Installing the SIPNX-100 (Legacy)

The power to the SRCNX (Legacy) must be off. You will blow the IP module if the SRCNX is not powered down.

Orient your SRCNX board as shown; the SIPNX-100 module is installed on the right-hand side of the SRCNX reader controller J19.



Note: Do not remove jumpers or modules with the SRCNX powered on. The board must be powered off before any changes or swapping of components.

W12 - voltage selector for SRCNX (Legacy) J19

The W12 jumper setting must be on Pins 2 and 3 (LAN).

Before you begin

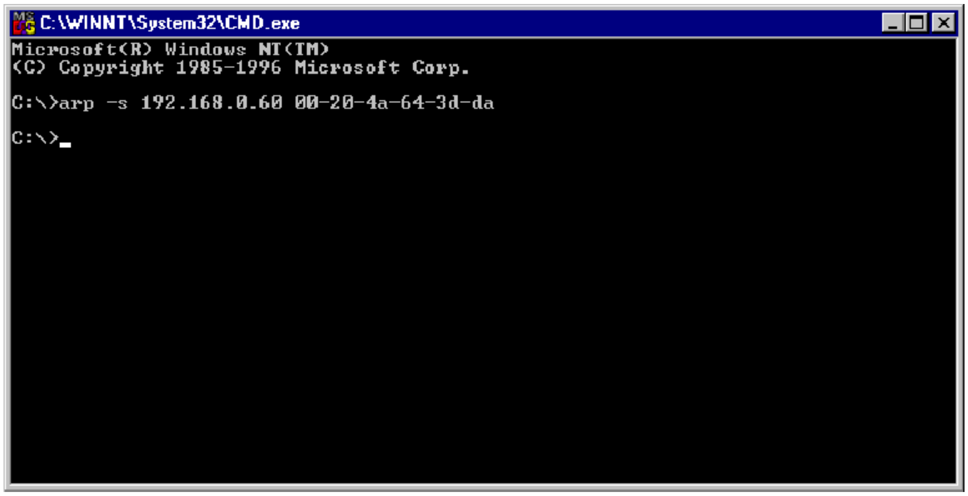
Before you begin configuring the IP module you must find out the following things:

- The network IP address that will be assigned to the SIPNX-100 (Legacy) module (See your network administrator for the static IP address)
- The network IP address of the default gateway used by the SIPNX-100 to reach the server/CIM if applicable
- The net mask for the connection
- The node address / MAC address of the IP module
- The format for the node address / MAC address is displayed as: 00-20-4a-64-45-b3. This is located on the white sticker on the IP module itself
- The IP address of the CIM workstation that will be communicating to the SIPNX-100

SIPNX-100 (Legacy) module configuration

1. Click on the Start button and click Run from the start menu. Type “CMD” into the Open field on the window. This brings the DOS prompt. Press <Enter>.
2. Type “ARP – s <IP Address for SRCNX> <Node Address of card on SRCNX>”. (Please note that there are spaces between characters) Press <Enter>.

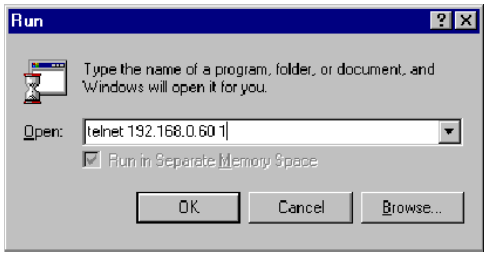
Example: C:arp –s 192.168.0.60 00-20-4a-64-3d-da



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>arp -s 192.168.0.60 00-20-4a-64-3d-da

C:\>_
```

3 Click on the **Start** button and click Run from the start menu. Type, “telnet <IP Address for SRCNX> 1” into the Open field. (Please note that there are spaces between characters). Click OK.

Example: telnet 192.168.0.60 1

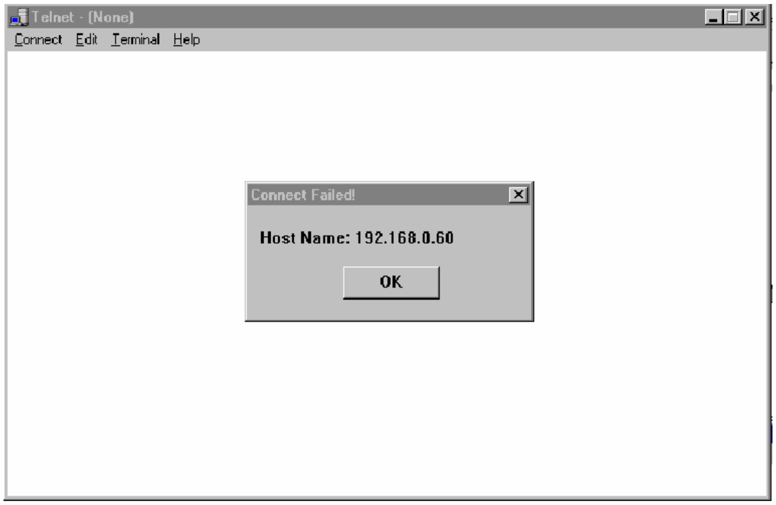


Type the name of a program, folder, or document, and Windows will open it for you.

Open: telnet 192.168.0.60 1

☑ Run in Separate Memory Space

4 If the operating system on your machine is Windows NT, the Telnet window will open, and the connection will FAIL, as shown in the example below.



Connect Failed!

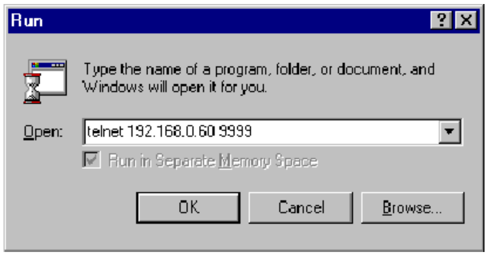
Host Name: 192.168.0.60

5 Leave the window open and continue with the following instructions.

Note: If you are using Windows 2000, the Telnet window will open, and pause for a few moments and then will be cleared from your screen. Continue with the following instructions.

6 Click on the Start button on your windows status bar. Click **Run**. Type, “telnet <IP Address for SRCNX> 9999” into the window. (*Please note that there are spaces between characters*)

Example: telnet 192.168.0.60 9999



Type the name of a program, folder, or document, and Windows will open it for you.

Open: telnet 192.168.0.60 9999

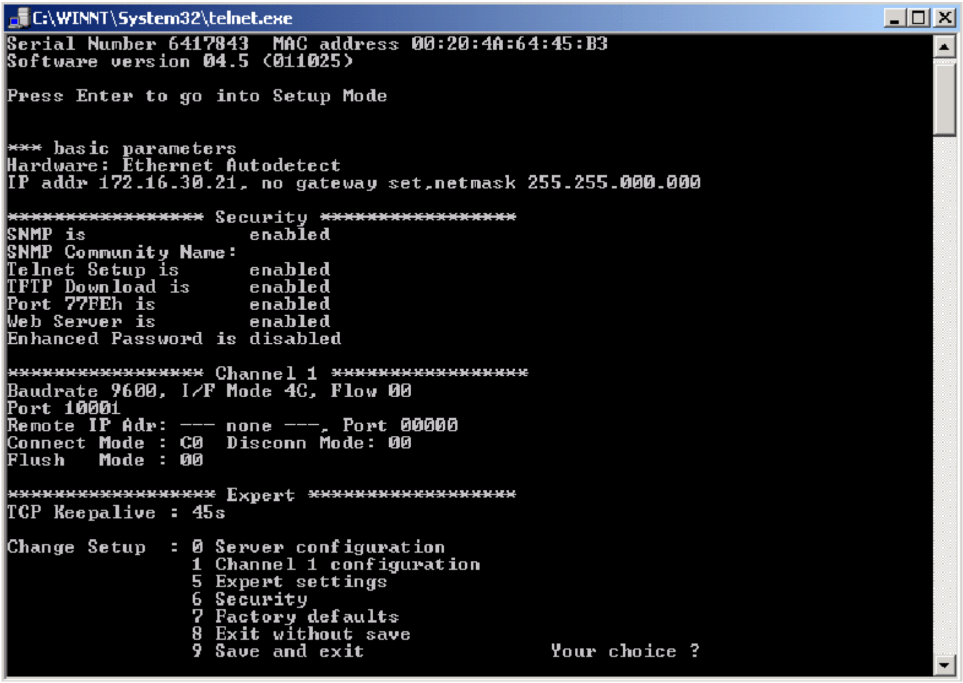
☑ Run in Separate Memory Space

a) You will establish a connection to the IP module.

b) You will be instructed to press <Enter> to connect.

Note: Press < Enter> quickly or the connection will time out.

7 This brings you to the Telnet session (C:\Winnt\System32\Telnet.exe).



```
Serial Number 6417843  MAC address 00:20:4A:64:45:B3
Software version 04.5 (011025)

Press Enter to go into Setup Mode


*** basic parameters
Hardware: Ethernet Autodetect
IP addr 172.16.30.21, no gateway set,netmask 255.255.000.000

***************** Security *****************
SNMP is              enabled
SNMP Community Name:
Telnet Setup is      enabled
TFTP Download is     enabled
Port 77FEh is        enabled
Web Server is        enabled
Enhanced Password is disabled

***************** Channel 1 *****************
Baudrate 9600, I/F Mode 4C, Flow 00
Port 10001
Remote IP Adr: --- none ---, Port 00000
Connect Mode : C0  Disconn Mode: 00
Flush   Mode : 00

****************** Expert ******************
TCP Keepalive : 45s

Change Setup   : 0 Server configuration
                 1 Channel 1 configuration
                 5 Expert settings
                 6 Security
                 7 Factory defaults
                 8 Exit without save
                 9 Save and exit             Your choice ?
```

8 You may be required to enter a password to enter the set up mode. Enter password “geof”. Press **<Enter>**.

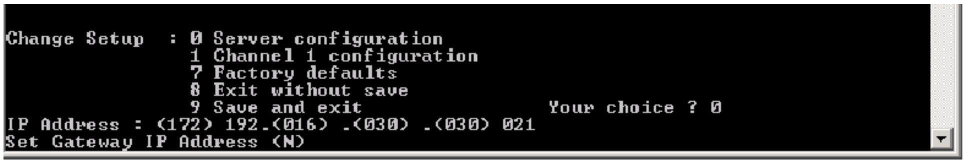
9 Press 0 (zero) for server configuration then press **<Enter>**.

Note: For the following instructions, pressing enter will confirm the listed option value. To change the value listed, type in the correct value.

10 **IP Address:**

Enter each Octet of the IP address, or press **<Enter>** to confirm the Octet as it appears.

Example:



```
Change Setup  : 0 Server configuration
                1 Channel 1 configuration
                7 Factory defaults
                8 Exit without save
                9 Save and exit              Your choice ? 0
IP Address : (172) 192.(016) .(030) .(030) 021
Set Gateway IP Address (N)
```

The above example shows the original Octet of the IP address as (172). To make a change we typed **192** and pressed **<Enter>** key to accept this value. Now the next Octet of the IP address is displayed. Value was **(016)**. To accept the value, we pressed the **<Enter>** key. The next value was **(030)**. Again, we accepted the value by pressing the **<Enter>** key. The last Octet value was **(030**). We typed in **021** and pressed the **<Enter>** key to accept the change.

11 Set Gateway IP Address **"N**". Press **<Enter>.** If you have a gateway press "**Y**". If you do not, press **<Enter>** or type "**N**" to continue.

Note: This is the gateway of the IP module, not the CIM.

12 **Net mask:** Number of Bits for host part = 8. Local net mask 8 will be displayed. To accept the value press **<Enter>**. To change the value type in the number and press **<Enter>**.

A brief description about subnet mask:

A net mask defines the number of bits taken from the IP address that are assigned for the host section.

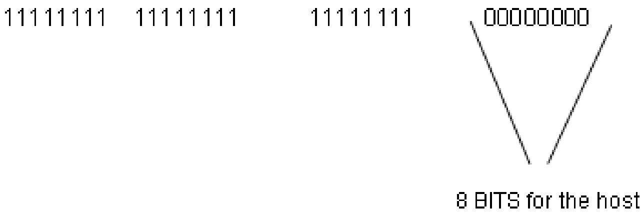
Note: Class A: 24 bits; Class B: 16 bits; Class C: 8 bits.

The Device Server prompts for the number of host bits to be entered, then calculates the net mask, which is displayed in standard decimal-dot notation when the saved parameters are displayed (for example, 255.255.255.0).

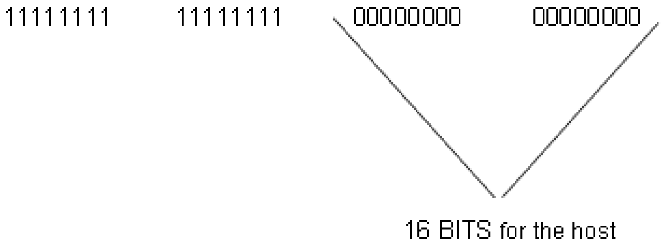
Example:

Just count the number of zero's in the subnet mask to get the number of host bits.

would equate in binary to:



255.255.0.0 would equate in binary to:



If you were to have a "nonstandard" subnet mask like:

255.255.255.248

11111111 11111111 11111111 11111000

3 BITS for the host

This is how you determine the host bits for the SIPNX-100 IP module subnet mask.

Another way of determining the Subnet Mask host bits would be to use the Scientific Calculator and convert from the Decimal notation to Binary notation. For the Example above: 255.255.255.248

Using the Scientific Calculator, select the Dec option and enter in the number 248. Then select the Bin option and you will now see the converted Decimal number as Binary number 11111000. Again, this would be 3 BITS for the host. After entering the net mask continue with step 13.

13 Change Telnet config password **<N>**. Press **<Enter>**.

14 Press"1" for Channel 1 configuration. Press **<Enter>**.

Enter channel information

Note: The following items should use the values listed. If the values you see during this setup is different, change the values to match this document. Start with 38400 as the baud rate, this may have to be adjusted later if there are communication problems.

1 Baud Rate= 38400 Press <Enter>

2 I/F Mode= <4C> Press <Enter>.

3 Flow= <00> Press <Enter>

4 Port No. <10001> Press <Enter>

5 Connect Mode= 05 Press <Enter>

6 Remote IP Address= IP Address for the CIM. Press <Enter>. This is the IP address of the computer, where the CIM resides on.

7 Remote Port= 3001 Press <Enter>.

Note: The value entered here must be the same value entered to the controller definition IP Port Number edit control.

8 DisConn Mode <00> Press <Enter>.

9 Flush Mode <00> Press <Enter>.

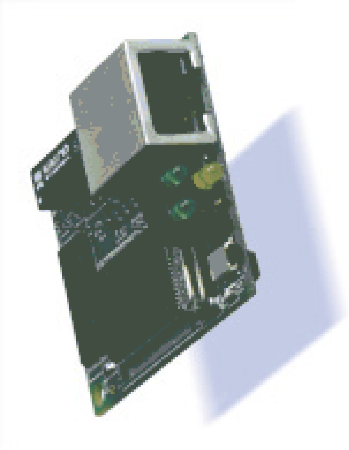
10 Disconn Time <00:00> Press <Enter> twice.

11 SendChar1 <00> Press <Enter>.

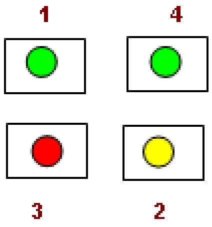
12 SendChar2 <00> Press <Enter>.

13 Press 9 to save & exit. Press <Enter>.

Diagnostic LED explanation



The SIPNX-100 (Legacy) has four status LEDs: serial port (Channel) 1 status, serial port (Channel) 2 status, diagnostics, and network link status. See the following table for a complete description of status LED pin out location and function.



LED Description

LED	Description	Location	LED Functions
1	Serial Port (Channel 1) Status	Con 4, Pin 4	Lights solid green to indicate Channel 1 is *idle*. Blinks green to indicate Channel 1 is connected to the network and *active*.
2	Serial Port (Channel 2) Status	CON 4, Pin 7	Lights solid yellow to indicate Channel 2 is *idle*. Blinks yellow to indicate Channel 2 is connected to the network and *active*.

LED	Description	Location	LED Functions
3	Diagnostics	CON 4, Pin 3	Blinks or lights solid red in combination with the green(Channel1) LED to indicate diagnostics and error detection. Red solid, green (Channel 1) blinking: 1x: EPROM checksum error 2x: RAM error 3x: Network controller error 4x: EEPROM checksum error 5x: Duplicated IP address on the network* 6x: Software does not match hardware* Red blinking, green (Channel 1) blinking: 4x: Faulty network connection* 5x: No DHCP response received* Lights solid green to indicate network port is connected to the network.
4	Network Link Status	CON 4, Pin 8	Lights solid green to indicate network port is connected to the network.
5	*Non-fatal error		

CHAPTER 23

Schlage Adaptable AD-300 Series Locks

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 Vanderbilt VRCNX-R/M/A, VSRC-300 or VMRC-1/VMRC-2 controllers. The communication protocol is via RS-485 to the connected controller.

Note: For the AD-300 lock to communicate with the VRCNX-R, the VRCNX-R must have firmware v5.92 or higher installed.

Features

- Connects directly to the VRCNX-R/M/A, VSRC-300 or VMRC-1/VMRC-2 controller via RS-485 protocol to one of the communication channels.
- Available with mortise, cylindrical lock and exit device trim.
- 16 Schlage AD-300 Series locks can be directly connected to a VRCNX-R/M/A reader controller.
- Available with (HID) proximity or magnetic stripe credential technologies.
- Integrated PIN pad allows for PIN+Credential access.

Specifications

- A separate power supply is required (The VRCNX-R/M/A does not supply power to the Schlage AD-300 locks)
- Power Requirements - 12VDC or 24VDC
- Power Consumption - 1.1 amp @ 12VDC or .6 amp @ 24VDC

Contacts, Relays, 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
- Deadbolt Position
- Low Lithium battery

Internal Push Button (IPB) - If the AD-300 lock is defined in SMS as having an IPB function (either LockDown or Toggle) this button activates that option (see the SMS Software Manual for details).

Toggle LED - When the IPB is used as a Toggle switch the LED will illuminate depending on the state of the lock. (Only if running firmware V2.1.7 or higher. Lower firmware versions will have full IPB functionality but the LED will not respond.)

- In Toggle - green light
- Out of Toggle - red light

LockDown LED - When the IPB is used as a LockDown switch the LED will illuminate depending on the state of the lock. (Only if running firmware V2.1.7 or higher. Lower firmware versions will have full IPB functionality but the LED will not respond.)

- In Lockdown - red light
- Out of Lockdown - green light

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 AD-300 lock and the VRCNX-R/M/A controller.

J1 - Power source and communication. This is where the VRCNX-R/M/A connects to the AD-300 lock.

SW1 - Tamper Switch

Schlage Adaptable AD-300 Series Lock Configuration

VRCNX-R/M/A configuration guidelines

1. The VRCNX-R/M/A or VMRC-1 can control a maximum of 16 Schlage AD-300 Locks.
2. The VMRC-2 can control a maximum of 32-devices AD-300 Locks.
3. A VSRC-300 can control a maximum of 8 Schlage AD-300 Locks.
4. Data communication between Schlage AD-300 Locks and the VRCNX-R/M/A or VMRC-1/VMRC-2 reader controller can be a multiplex or a daisy chain configuration. Communication with the VSRC-300 is via daisy chain only.
5. The Schlage AD-300 Locks and the reader controllers are connected to each other via an RS-485 communication protocol. Wire runs are limited to 4,000 feet (Data Only -- see Recommended Wire Chart).
6. A SRCNX (Legacy) reader controller that has a Schlage AD-300 Lock connected to it cannot be configured as a main controller. These Schlage devices must be connected to a satellite SRCNX (Legacy) reader controller.

Multiplex configuration

In a multiplex configuration the Schlage AD-300 Locks are connected to the controller RS-485 PINs in parallel:

VRCNX-R/M/A:	J4 to J11
VMRC-1/1L:	TB2-4 and TB2-5
VMRC-2/2L:	TB3-2 and TB3-3

A maximum of 16 AD-300 Locks can be connected in this manner.

Note: Only identical devices can be on the same channel.

Daisy chain configuration

In a daisy chain configuration, the Schlage AD-300 Locks are connected to one another in series. Up to 16 devices can be connected to the VRCNX-R/M/A controller. This configuration is not the preferred method when connecting to other controllers; if the chain/wire is broken in the loop, the last devices will not communicate with the controller. However, this is the method used when connecting to a VSRC-300. See the VSRC chapter for details.

Connecting to VRCNX-R/M/A

Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board.

VRCNX-R/M/A - AD-300 Lock

VRCNX-R/M/A J4-J11	AD-300 Lock
Pin 2 (A)	RDA- (Data A)
Pin 3 (B)	RDB+ (Data B)

Connecting to VMRC-1/2

Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board.

VMRC-1/2 to AD-300 Lock

VMRC-1 / 1L	VMRC-2 / 2L	AD-300 Lock
TB2-4 (TR+)	TB3-3 (TR+)	RDB+ (Data B)
TB2-5 (TR-)	TB3-2 (TR-)	RDB- (Data A)

Addressing the AD-300 Lock

The AD-300 lock is addressed using the Schlage Utility Software (SUS), which is run from the Pideon HHD (Hand Held Device). The address used by the AD-300 locks go from 0 to 15. SMS 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 SMS. The Channel number is not affected by this.

Example: The AD-300 lock is connected to the VRCNX-R/M/A on channel 1 and addressed in SMS as Address 2 then the address of the AD-300 lock should be set to 1. If the AD-300 is connected to channel 2 and addressed in SMS as Address 10 then the address should be set to 9.

SMS Address	SUS Address
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

SMS 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 VRCNX-R/M/A controller, make a note of the channel, this information will be required to set up the lock in SMS.

Note: All AD-300 locks connecting to an VSRC-300 default to Channel 2.

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 HHD. A Menu will open with a list of programs.
2. Select the **Schlage Utility Software** option. **SUS** will open.
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 AD-300 lock using the supplied USB cable.
7. Press the **Schlage** button twice on the AD-300 keypad. The bottom of the HHD screen will now display AD300.
8. Click on the **Options** button at the bottom of the HHD screen. A list of options will open.
9. Put the AD-300 lock into **Pairing Mode** (this is necessary for the HHD 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 HHD 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 SMS.

CHAPTER 24

Schlage VIP Locks

VIP Lock

Overview

The Schlage VIP Lock is an integrated, modular lock that includes all the standard peripheral devices at a secured door opening. Complete door monitoring is provided by the Schlage VIP locks. The Schlage VIP Locks can be integrated directly into the Vanderbilt VRCNX-R/M/A Reader Controller. The communication protocol is RS-485 to one of the communication channels on the VRCNX-R/M/A. For additional Schlage VIP Lock information, please visit www.schlage.com.

Features

- Connects directly to the VRCNX-R/M/A reader controller via RS-485 protocol to one of the communication channels.
- 16 Schlage VIP Locks can be directly connected to a VRCNX-R/M/A reader controller.
- 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

- A separate power supply is required (The VRCNX-R/M/A does not supply power to the Schlage VIP Locks)
- Power Requirements -12VDC or 24VDC
- Power Consumption - 1.1 amp @ 12VDC or .6 amp @ 24VDC

Provided devices on the Schlage VIP Lock

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), non-supervised
- Door Open Detect (DOD), non-supervised
- Latch bolt monitor (LBM), non-supervised
- Key position, 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

Schlage VIP Lock Configuration

Controller configuration guidelines

1. All VRCNX-R/M/A Reader Controllers have 2 communication channels; each channel will support 8 Schlage devices for a total of 16 devices. Only devices with the same communication protocol may be connected to an individual channel.
2. When Schlage wireless PIM-485 or Schlage VIP Locks devices are configured on a SRCNX (Legacy), you may not connect a satellite SRCNX (Legacy) to the main SRCNX (Legacy).

Note: Only two identical devices may be connected to each of the 8 channels on the SRCNX (Legacy).

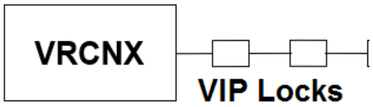
3 The VRCNX-R/M/A can control a maximum of 16 Schlage VIP Locks.

4 Data communication between Schlage VIP Locks and the reader controller can be a multiplex or a daisy chain configuration.

5 The Schlage VIP Locks and the reader controllers are connected to each other via an RS-485 communication protocol. Wire runs are limited to 4,000 feet (Data Only -- see Recommended Wire Chart).

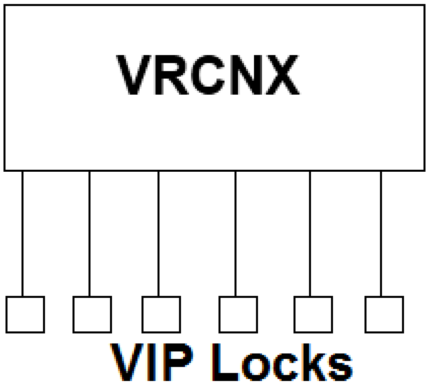
Daisy chain configuration

In a daisy chain configuration, the Schlage VIP Locks are connected to one another in series. Up to 16 devices can be connected to the VRCNX-R/M/A controller. This configuration is not the preferred method. If the chain/wire is broken in the loop, the last devices will not communicate with the VRCNX-R/M/A.



Multiplex configuration

In a multiplex configuration the Schlage VIP Locks are connected to the communication channels J4 to J11 on the main VRCNX-R/M/A board in parallel. A maximum of 16 VIP Locks can be connected in this manner.



Note: Only identical devices can be on the same channel.

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. Use the VIP Address Chart below to address the VIP Lock.

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

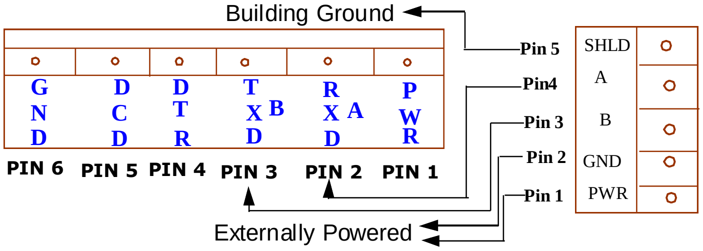
Note: Only the first 4 switches are used for addressing.

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

Wiring Diagram for VRCNX-R/M/A to VIP lock

Choose one of the connectors between J4 and J11 on VRCNX-R/M/A board.



VRCNX-R/M/A - VIP Lock

VRCNX-R/M/A J4-J11	VIP Lock J3 on Inside Board
Pin 2 (A)	Pin 4 (A)
Pin 3 (B)	Pin 3(B)

Data received by the VRCNX-R/M/A

Five contact inputs status are sent back from lock with each poll. However only four (4) are reported to the VRCNX-R/M/A board (1-2-3-4).

- Contact 1: REX -- Request to Exit from the lock, normally closed.
- Contact 2: DOD -- Door open detect, normally closed.
- Contact 3: LBM -- Latch Bolt Monitor, normally closed.
- Contact 4: KEY -- Key position turned from the lock, normally closed
- Contact 5: Spare -- not used

Note: All five (5) contact points are non-supervised.

Programming information

- Keypad mode and degraded mode are not available for VIP locks.
- To use a Schlage VIP Lock in the system, you need to select Schlage VIP as the reader model.

CHAPTER 25

Assa Abloy Aperio Series Wireless Locks

Aperio Wireless Locks

Overview

Assa Abloy Aperio wireless locks can be seamlessly integrated with the SMS system. The Aperio AH30 hub communicates directly to the VRCNX-R/M/A via RS-485 protocol and can support up to 8 Aperio Series locks (A100, K100, IN100 or PR100 only). Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Note: For the Aperio AH30 hub to communicate with the VRCNX-R, the VRCNX-R must have firmware v6.40 or higher installed. Full compliance with Assa Abloy Aperio certification requires firmware v6.41 or higher installed.

SMS Programming Notes:

It is recommended the following documents be available to the installer/programmer for proper configuration of the Aperio hardware with the Vanderbilt SMS system. The Aperio hardware settings which are mandatory for their use with the SMS software are specified in this document. See the following documents for additional information.

- Aperio Online Configuration Guide
- Aperio Online Technology Reference Manual
- Aperio Online Mechanical Installation Guide
- TriBee USB Bootloader and Drivers Instruction Manual

The following items must be taken into consideration when programming the Aperio locks in SMS.

- SMS supports the AH30 Hub with either v2 or v3 firmware. Aperio v3 Hub firmware required for full v3 lock functionality.
- SMS supports the Aperio PR100, IN100, A100 and K100 v2 locks and the IN100 v3 lock.
- SMS does not support any MRO (Manual Reader Override) commands to the Aperio v2 locks.
- SMS supports MROs to the Aperio IN100 v3 lock with AH30 Gen 4 hub or newer with Aperio v3 firmware.
- Aperio locks are only supported for use on the VRCNX-R/M/A Hardware Controllers.
- The Aperio HUB (AH30) must be connected to a dedicated channel on the VRCNX-R/M/A controller separate from other Vanderbilt or Schlage Lock hardware.
- SMS supports only the following ARO (Automatic Reader Override) commands to the Aperio v2 Locks.
- SMS additionally supports door lock/unlock AROs to the Aperio IN100 v3 lock ***only when using the AH30 v3 Gen 5 hub***.

Aperio IN100 v2:

- Door Strike Relay Reporting Disabled: Default Setting is “ALWAYS”
- Exit Request Reporting Disabled: Default Setting is “ALWAYS”
- Activate Keypad Reader: Default Setting is “NEVER”

Aperio K100 v2 (Cabinet Lock):

- Door Strike Relay Reporting Disabled: Default Setting is “NEVER”

NOTE: Activating this Automatic Override will disable the “Lock Jammed” transaction. It is recommended that this remain programmed at “NEVER”

- Exit Request Reporting Disabled: Default Setting is “ALWAYS”
- Activate Keypad Reader: Default Setting is “NEVER”

Aperio PR100 v2:

- Door Strike Relay Reporting Disabled: Default Setting is “ALWAYS”
- Exit Request Reporting Disabled: Default Setting is “ALWAYS”
- Activate Keypad Reader: Default Setting is “NEVER”

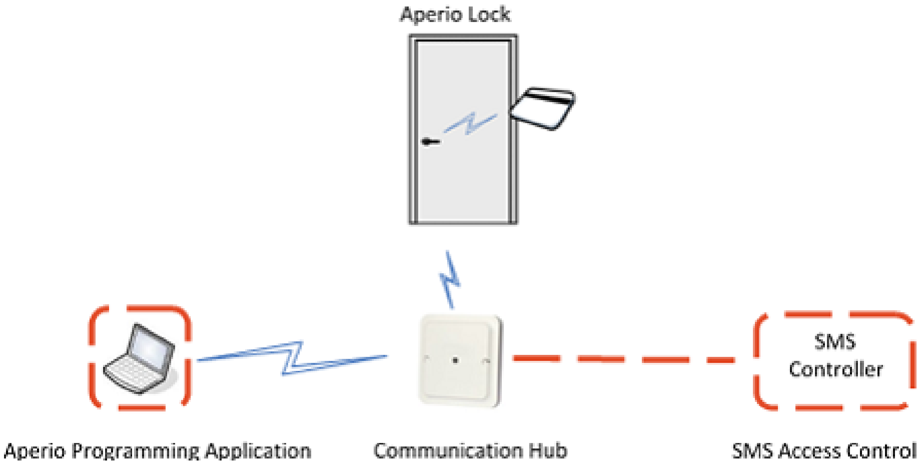
Aperio A100 v2:

- Door Strike Relay Reporting Disabled: Default Setting is “ALWAYS”
- Exit Request Reporting Disabled: Default Setting is “ALWAYS”
- Activate Keypad Reader: Default Setting is “NEVER”

Aperio Components

The Aperio Series wireless system contains two different types of modules:

- Wireless HUB (AH30)
- Wireless Lock



The Aperio HUB (AH30) is hard wired to the reader controller (VRCNX-R/M/A) communication channels via RS-485 protocol. The HUB (AH30) installation location is determined by the location of the Aperio lock with which it will communicate. The Aperio HUB (AH30) communicates with the supported Aperio locks using a wireless IEEE 802.15.4 (2.4GHz) radio frequency. The maximum distance of the HUB from the lock is subject to the Aperio stipulations for maintaining a reliable RF signal but is typically 50 - 80 feet.

The Aperio lock is installed at the access point where access will be controlled and monitored.

Aperio Wireless Components

The two components of the Aperio system, the Aperio HUB (AH30) and the Aperio Locks, are detailed in the following sections.

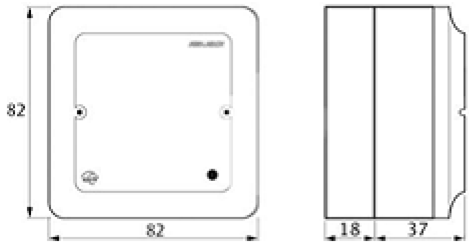
AH30 Hub

The AH30 Communication HUB is the link between Aperio locks and the Vanderbilt SMS access control system. Up to 8 locks can be paired to one HUB (AH30). Each lock connects to the SMS VRCNX-R/M/A controller through a standard RS-485 connection. It communicates directly with Aperio enabled locks via an encrypted IEEE 802.15.4 (2.4GHz) wireless link and is designed to be positioned above the door within the supported distance of the lock. The maximum distance of the HUB from the lock is subject to the Aperio stipulations for maintaining a reliable RF signal but is typically 50 - 80 feet.

- Connect up to 8 Aperio devices on a single hub
- RS485 interface
- Encrypted radio communication
- Integrated antenna
- LED status for visual indication

Specifications

- **Power:** 8-24vdc
- **Power consumption:** 250 mA Minimum 80mA at 12vdc
- **Radio standard:** IEEE 802.15.4 (2.4 GHz) - 16 channels (11-26)
- **Encryption:** AES 128 Bit
- **Status:** LED (Red/Green/Orange)
- **Range between locks and Hubs:** 50 - 80 feet depending on building environments.
- **Operating temperature:** 5°C to 35°C
- **Humidity:** < 95% non-condensation
- **IP-degree:** IP 20
- **Dimensions:** 82 x 82 x 55 mm
- **Dimensions (Inches):** 3.22 x 3.22 x 2.17 in (Approx. H x W x D)



- **Approvals:** CE, ETL, FCC, IC, C-Tick
- **Safety and Emissions:**

FCC 47CFR Part 15 subpart

B and subpart C; IC RSS-210

EN ETSI 301 489-17 v2.1.1

EN ETSI 300 328 v1.7.1

EN 60950-1 ed.2 2007

UL 294-2010; C22.2

Card Formats

- Supports HID® 125 kHz proximity or 13.56 MHz CLASS® (full authentication, all formats) credentials

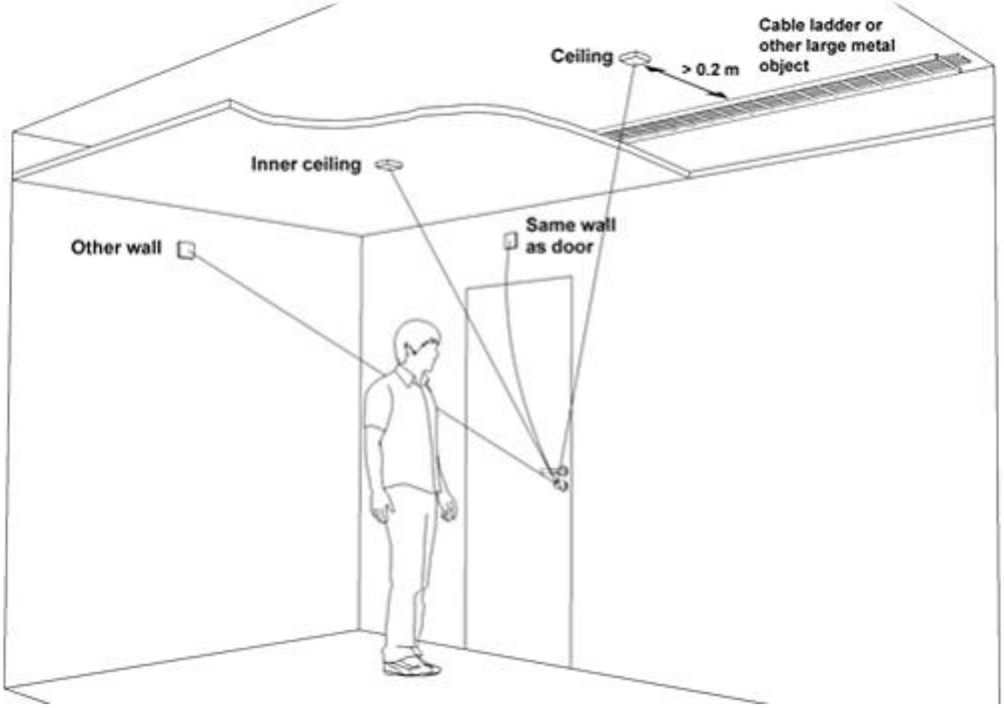
Specifications for the HUB (AH30) with SMS

- RS-485 Communication to VRCNX-R/M/A reader controller
- VRCNX-R/M/A can support multiple Aperio HUB (AH30) devices
- Up to 16 total Lock devices on the VRCNX-R/M/A. 8 Aperio Locks per HUB (AH30). The SMS Access Control System (v6.0 and above) does not count the HUB (AH30) as a device.

Placement options for the HUB (AH30)

The HUB (AH30) is designed so that it can establish a reliable radio link regardless of the mounting position of the communication hub and the type of lock being used. Please review individual lockset installation manuals for more information regarding distance limitations.

The AH30 communication hub can be mounted according to the following figure.



Avoid installing the communication hub in a low position, where radio waves can be blocked by objects or passing by people during operation.

With internal antenna, the radio coverage backwards is very limited. It also depends on type of wall it is installed into. Maximum 3 meters.

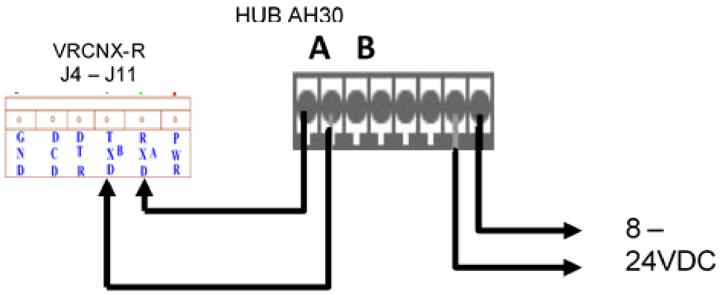
With external antenna, the radio coverage will increase as well as providing additional installation angles. The lock and the communication hub should be placed on the same side of the door. Shorter distance and "light" materials in the walls also permits placement on opposite sides.

Be aware of that nearby metallic sheet or mesh will attenuate the radio signal. Inner ceiling, for example, is sometimes covered with foil or metallic mesh.

Mirrors, heat insulating windows and larger metallic objects (like cable ladders) have a significant effect on radio signals and should not be closer than 8 inches from lock or communication hub.

In difficult environments (for example when heavy radio interference is expected), or when the requirements on the radio link quality are very high, it is recommended to keep the distance between the lock and the Communication hub well below the maximum distance. There is no minimum distance.

Connecting to the VRCNX-R/M/A



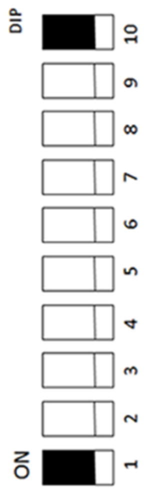
* Depending on the power that is connected to J1 on the VRCNX-R/M/A backplane, the GND & PWR from the connector J4 - J11 can provide up to 24 Volts DC to the AH30 HUB.

Configuration of the AH30 communication hub

This chapter describes how to configure the RS-485 AH30 Aperio hub for use with the SMS access control system. For additional information please refer to the Aperio Online Technology Reference Manual.

Configuration of the communication hub to the EAC includes setting the DIP switches and if not done earlier, connecting it to the RS-485 bus and connecting it to power supply, according to applicable section below.

Setting the DIP switches for SMS – Legacy Hub

	DIP 10	ON	Internal / external antenna
	DIP 9	OFF	Not used
	DIP 8	OFF	Activates termination of EAC bus
	DIP 7	OFF	Activation of pull up resistor
	DIP 6	OFF	Activation of pull down resistor
	DIP 5	OFF	Manual EAC Address (only possible with one lock paired)
	DIP 4	OFF	Manual EAC Address
	DIP 3	OFF	Manual EAC Address
	DIP 2	OFF	Manual EAC Address
	DIP 1	ON	Manual EAC Address / Automatic pairing

See below for an explanation on how to set the DIP Switches for use with the SMS access control system. For more information on DIP switch settings please refer to the Aperio Programming manual.

DIP SWITCH 1

DIP switch 1 is used to set the mode that will be used for pairing the HUB with the Aperio locks. When used with the SMS access control system DIP switch 1 must be set to **ON** for automatic pairing. Manual EAC addressing is not used with SMS on the HUB AH30.

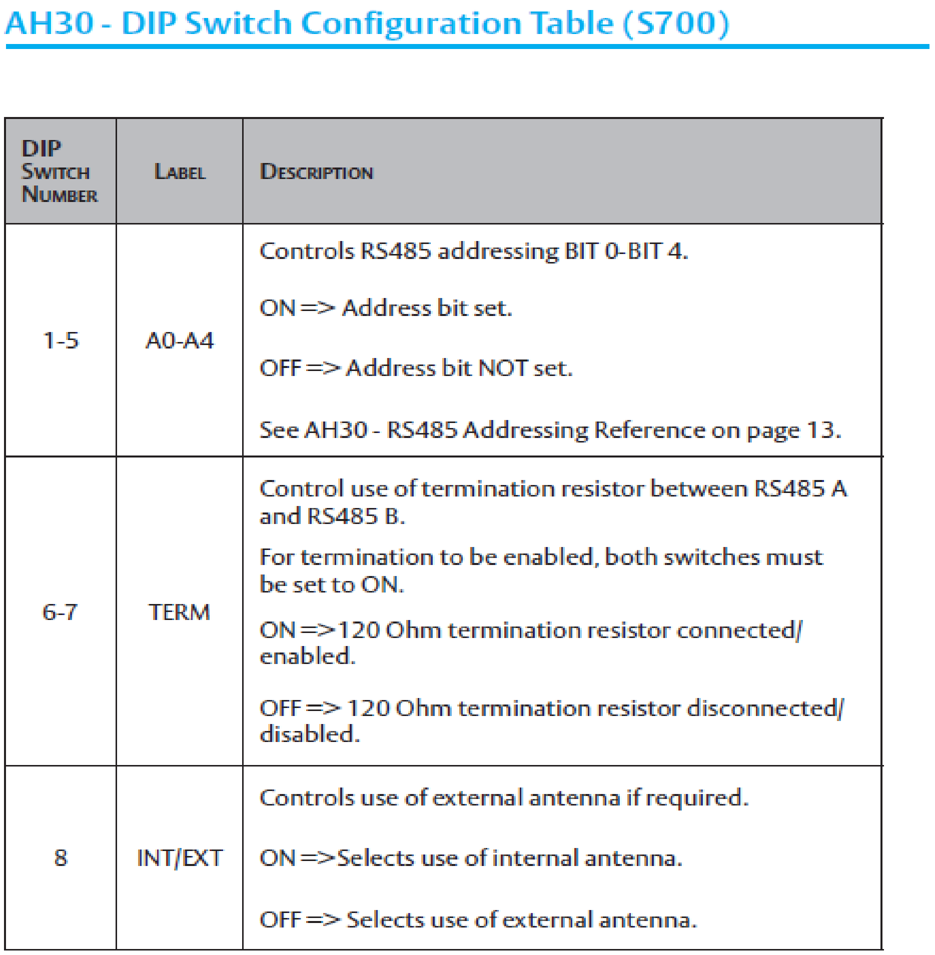
DIP SWITCH 2 - 9

DIP switches 2 - 9 must remain **OFF** for proper functionality with the SMS access control system.

DIP SWITCH 10

Normally the communication hub's internal antenna is sufficient. In a difficult installation environment or if the radio signal needs to be amplified for extended range, an external antenna can be used. Set the DIP 10 to **ON** to use the hubs internal antenna.

Setting the DIP switches for SMS – Gen 5 Hub

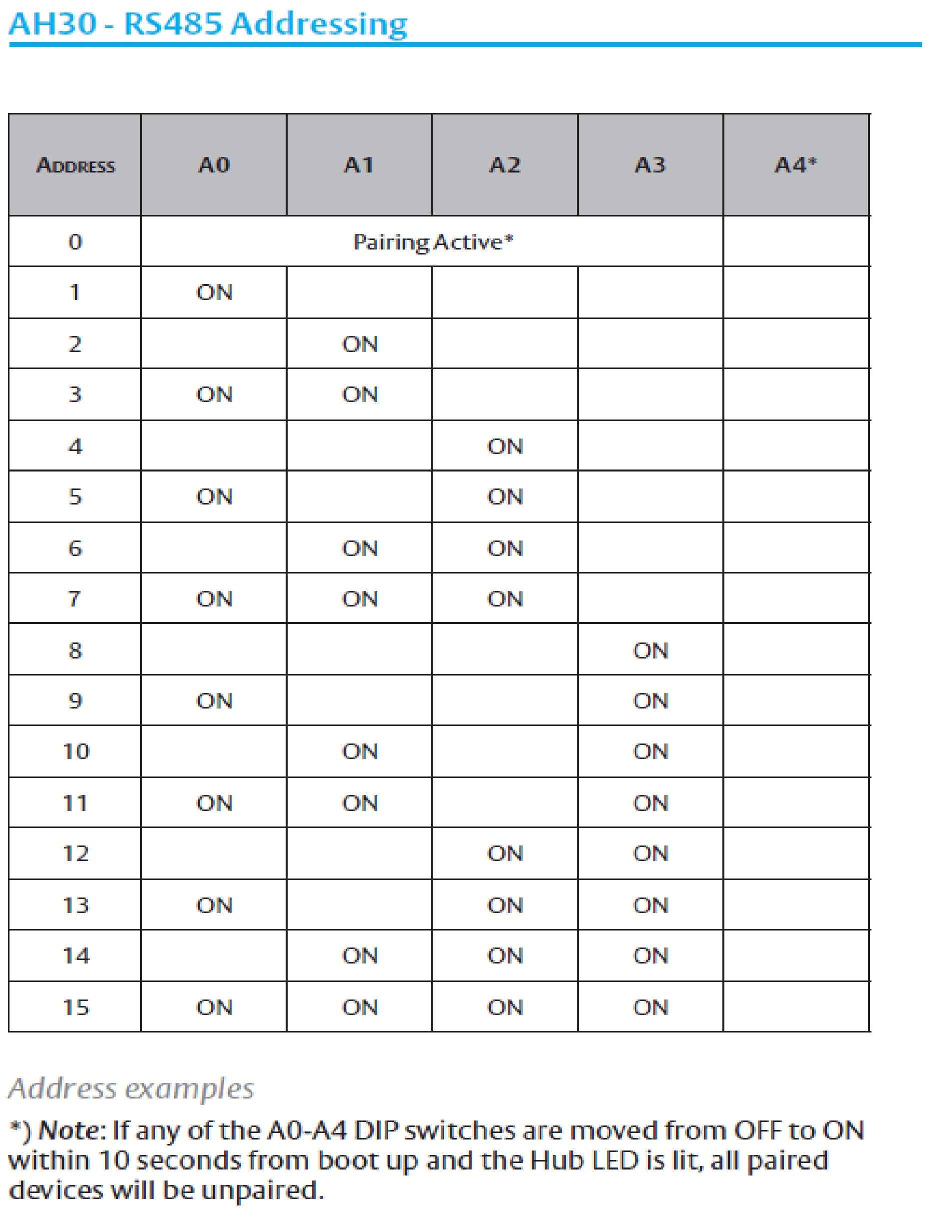


AH30 - DIP Switch Configuration Table (S700)

DIP Switch Number	Label	Description

1-5	A0-A4	Controls RS485 addressing BIT 0-BIT 4.
		ON => Address bit set.
		OFF => Address bit NOT set.
		See AH30 - RS485 Addressing Reference on page 13.

6-7	TERM	Control use of termination resistor between RS485 A and RS485 B. For termination to be enabled, both switches must be set to ON. ON =>120 Ohm termination resistor connected/ enabled. OFF => 120 Ohm termination resistor disconnected/ disabled.
8	INT/EXT	Controls use of external antenna if required. ON =>Selects use of internal antenna. OFF => Selects use of external antenna.



AH30 - RS485 Addressing

Address	A0	A1	A2	A3	A4*
0	Pairing Active*				
1	ON				
2		ON			
3	ON	ON			
4			ON		
5	ON		ON		
6		ON	ON		
7	ON	ON	ON		
8				ON	
9	ON			ON	
10		ON		ON	
11	ON	ON		ON	
12			ON	ON	
13	ON		ON	ON	
14		ON	ON	ON	
15	ON	ON	ON	ON	

Address examples

*) ***Note***: If any of the A0-A4 DIP switches are moved from OFF to ON within 10 seconds from boot up and the Hub LED is lit, all paired devices will be unpaired.

SMS Currently Supports 8 Paired Aperio Locks / Hub

HUB Configuration

The Aperio Programming Application is used to configure the Aperio HUB (AH30) and the Aperio locks. A USB Radio dongle is used to communicate to the wireless HUB for configuration and pairing of the Aperio wireless locks.

Initial setup of the wireless locks requires:

- Installation of the Aperio Programming Application (refer to the Aperio Online Technology Reference Manual)
- Configuration of the Aperio HUB
- Pairing and configuration of the Aperio Locks

Aperio Programming Application

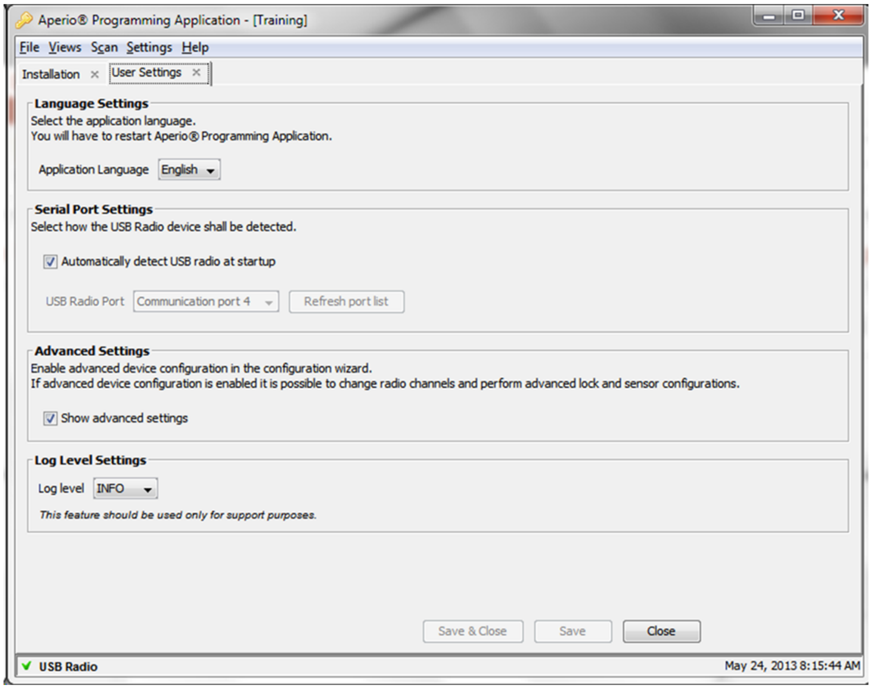
This section defines applicable settings for the Aperio HUB and locks when they are being used with the SMS Access Control System. For more information regarding these features please refer to your Aperio Programming manual.

1 Apply power to the Aperio Hub and start the Aperio Programming Application.

2 Create a new installation or open an existing predefined installation file

3 Choose Settings - Then USER SETTINGS

4 The **Show Advanced Settings** option must be enabled.



Language Settings
Select the application language.
You will have to restart Aperio® Programming Application.

Application Language: English

Serial Port Settings
Select how the USB Radio device shall be detected.

☑ Automatically detect USB radio at startup

USB Radio Port: Communication port 4 | Refresh port list

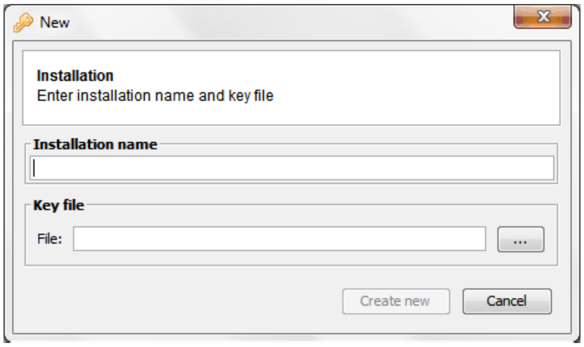
Advanced Settings
Enable advanced device configuration in the configuration wizard.
If advanced device configuration is enabled it is possible to change radio channels and perform advanced lock and sensor configurations.

☑ Show advanced settings

Log Level Settings
Log level: INFO

This feature should be used only for support purposes.

5 Create a new Programming File to store the hub and lock settings by selecting **File** - > **New**



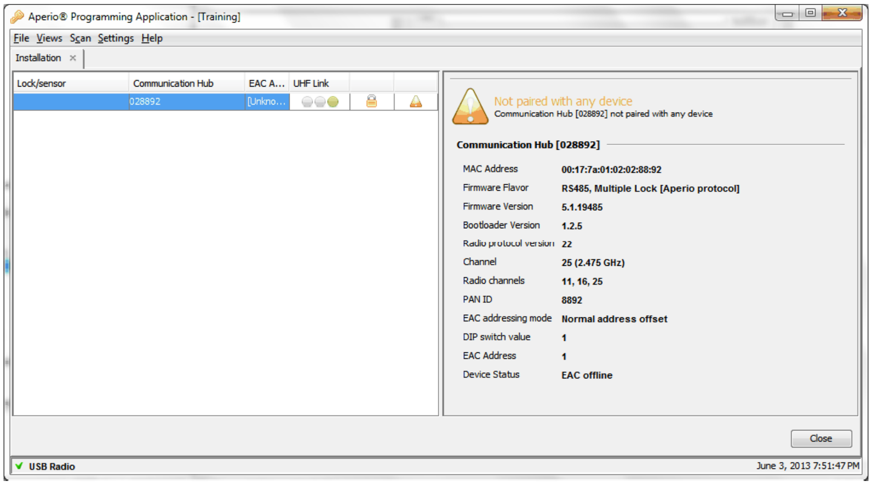
Installation
Enter installation name and key file

Installation name

Key file
File:

6 Name the installation and navigate to the **Key File** provided to you by Assa Abloy.

7 Select the HUB from the window and select Show Details


Aperio® Programming Application - [Training]
File Views Scan Settings Help
Installation ×
Close
USB Radio
June 3, 2013 7:51:47 PM

Lock/sensor	Communication Hub	EAC A...	UHF Link
	028892	[Unkno...	

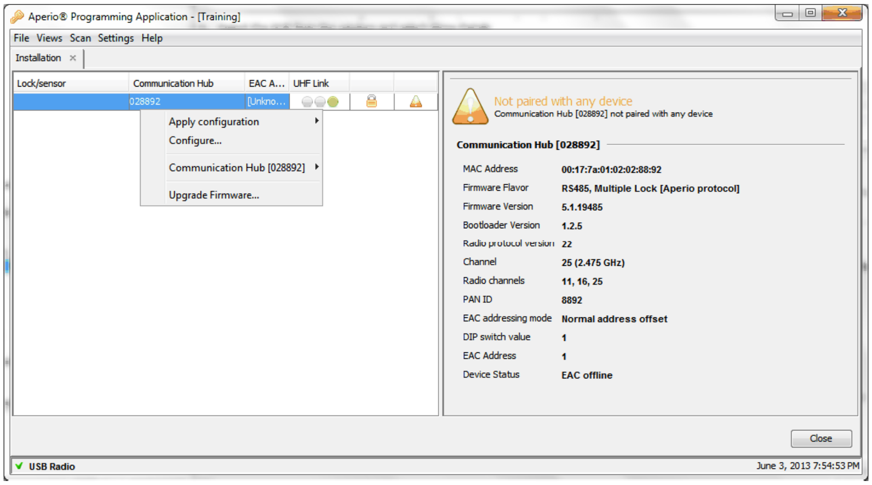
Not paired with any device

Communication Hub [028892] not paired with any device

Communication Hub [028892]

MAC Address	00:17:7a:01:02:02:88:92
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	5.1.19485
Bootloader Version	1.2.5
Radio protocol version	22
Channel	25 (2.475 GHz)
Radio channels	11, 16, 25
PAN ID	8892
EAC addressing mode	Normal address offset
DIP switch value	1
EAC Address	1
Device Status	EAC offline

8 Right-Click on the HUB and choose the CONFIGURE option.



Lock/sensor	Communication Hub	EAC A...	UHF Link
	028892	[Unkno...	

Not paired with any device

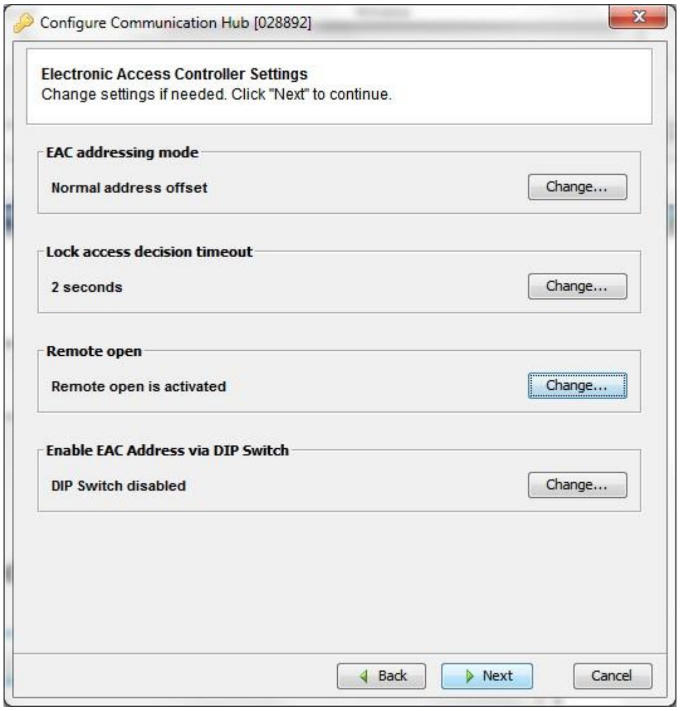
Communication Hub [028892] not paired with any device

Communication Hub [028892]

MAC Address	00:17:7a:01:02:02:88:92
Firmware Flavor	RS485, Multiple Lock [Aperio protocol]
Firmware Version	5.1.19485
Bootloader Version	1.2.5
Radio protocol version	22
Channel	25 (2.475 GHz)
Radio channels	11, 16, 25
PAN ID	8892
EAC addressing mode	Normal address offset
DIP switch value	1
EAC Address	1
Device Status	EAC offline

Adjust the applicable settings below for use with the Vanderbilt SMS access control system. Although only the settings mandatory for use with SMS are noted here. The not applicable settings may be important for Aperio lock functionality. For more information regarding "Not Required" settings please refer to your Aperio Programming Manual."

9 Adjust the **Electronic Access Controller Settings for proper functionality with the SMS Access Control System**



Configure Communication Hub [028892]

Electronic Access Controller Settings
Change settings if needed. Click "Next" to continue.

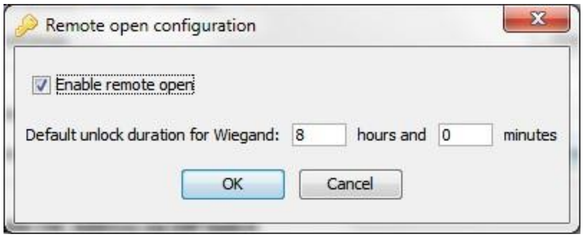
EAC addressing mode
Normal address offset

Lock access decision timeout
2 seconds

Remote open
Remote open is activated

Enable EAC Address via DIP Switch
DIP Switch disabled

- EAC addressing mode - Normal address offset
- Lock access decision timeout - 2 Seconds
- Remote Open - Enabled



Remote open configuration

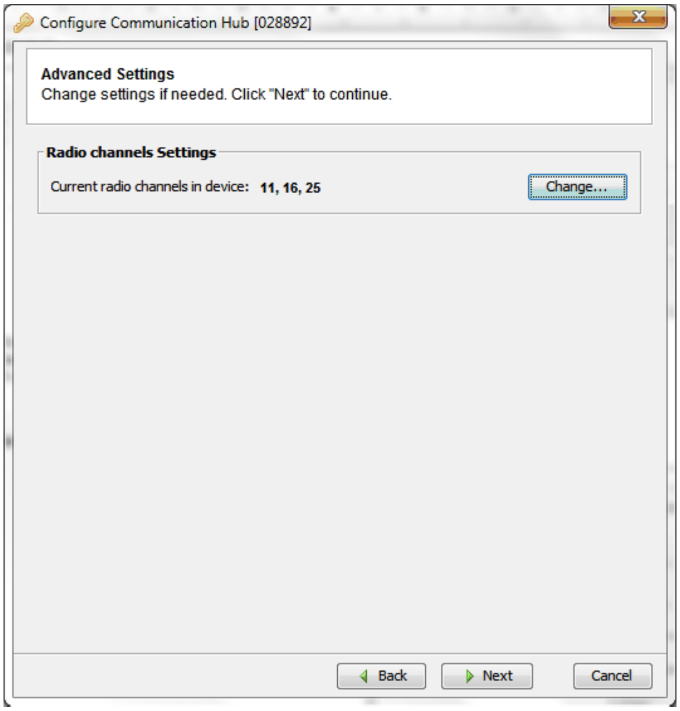
☑ Enable remote open

Default unlock duration for Wiegand: 8 hours and 0 minutes

10 Enable EAC Address via DIP Switch - Disabled

11 Select **Next** to continue

12 If necessary, adjust the **radio channel settings**


Configure Communication Hub [028892]

Advanced Settings
Change settings if needed. Click "Next" to continue.

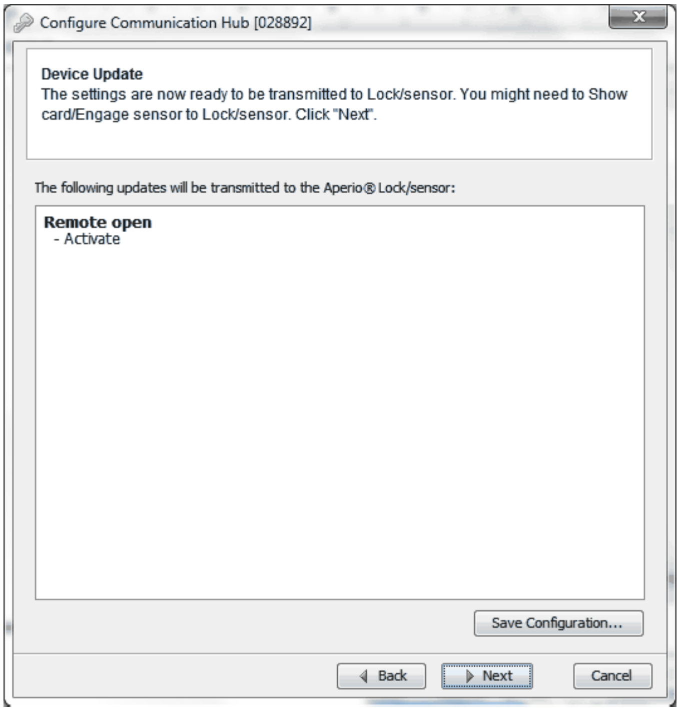
Radio channels Settings

Current radio channels in device: **11, 16, 25**

13 Select **Next** to continue

14 Review the device updates and select **Next** to send the changes to the HUB

NOTE - The configuration settings can be saved and applied to future HUB installations by selecting Save Configuration.

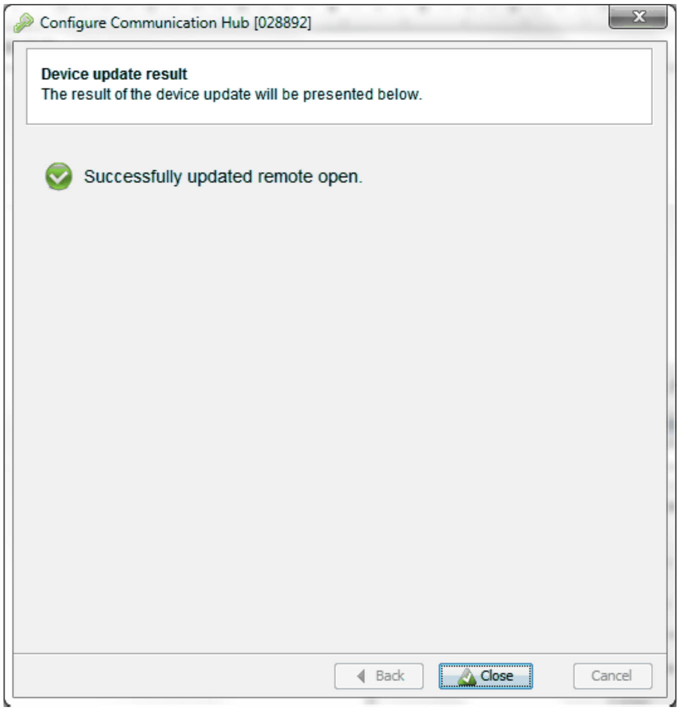

Configure Communication Hub [028892]

Device Update
The settings are now ready to be transmitted to Lock/sensor. You might need to Show card/Engage sensor to Lock/sensor. Click "Next".

The following updates will be transmitted to the Aperio® Lock/sensor:

Remote open
- Activate

15 Verify the successful update of the HUB



Device update result

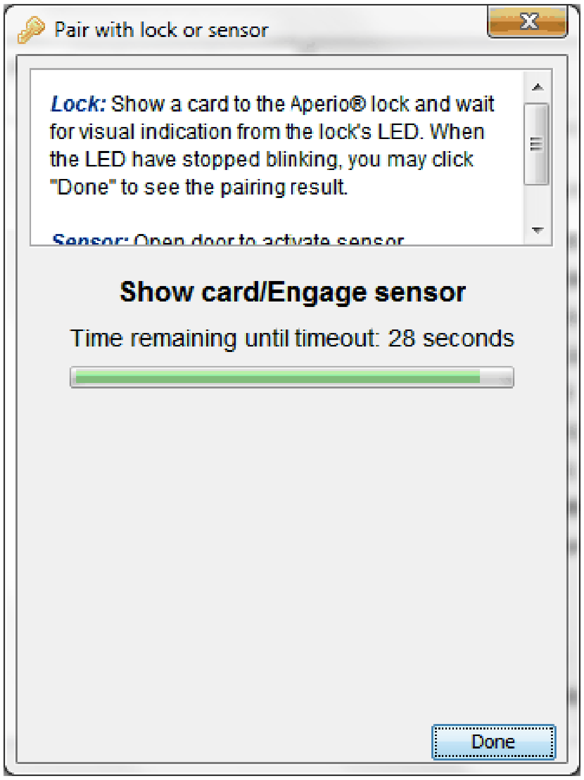
The result of the device update will be presented below.

✓ Successfully updated remote open.

Pair the Aperio Lock to the HUB

The next step will be to Pair the Aperio HUB with the lock.

1. Right click on the HUB -> Select Communication Hub -> Pair with Lock or sensor
2. Follow the onscreen instructions to Pair the lock to the HUB



Pair with lock or sensor

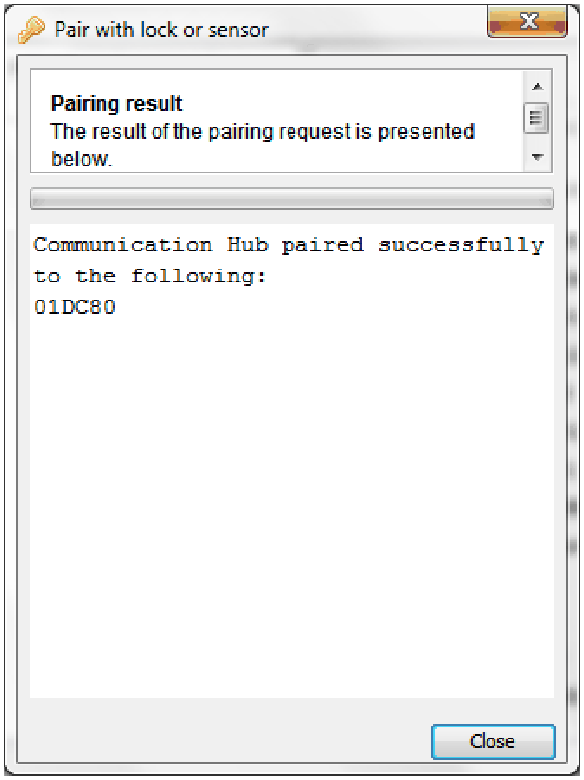
Lock: Show a card to the Aperio® lock and wait for visual indication from the lock's LED. When the LED have stopped blinking, you may click "Done" to see the pairing result.

Sensor: Open door to activate sensor

Show card/Engage sensor

Time remaining until timeout: 28 seconds

3 Verify successful pairing of the lock

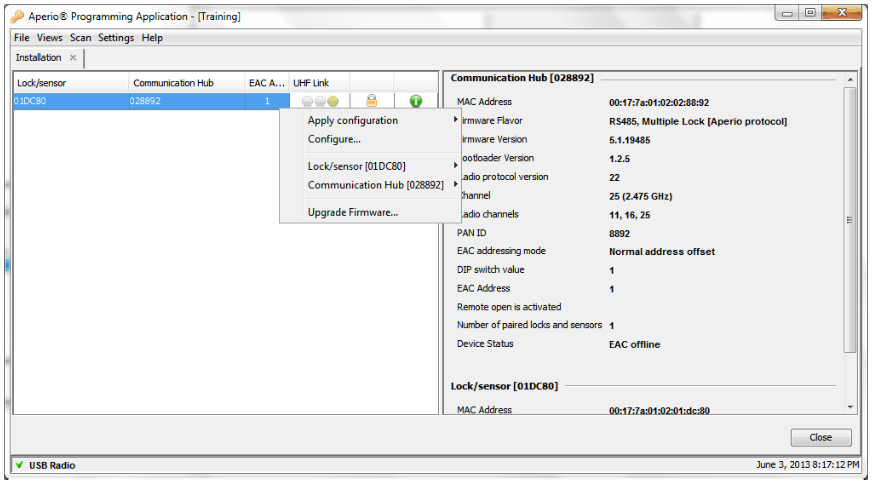


Pair with lock or sensor

Pairing result
The result of the pairing request is presented below.

```
Communication Hub paired successfully
to the following:
01DC80
```

4 Right-click on the Aperio HUB/Lock to configure the Paired lock with the HUB


Aperio® Programming Application - [Training]
File Views Scan Settings Help
Installation ×
Apply configuration
Configure...
Lock/sensor [01DC80]
Communication Hub [028892]
Upgrade Firmware...
Close
USB Radio

Lock/sensor	Communication Hub	EAC A...	UHF Link
01DC80	028892	1	

Communication Hub [028892]

MAC Address	00:17:7a:01:02:02:88:92
irmware Flavor	RS485, Multiple Lock [Aperio protocol]
irmware Version	5.1.19485
ootloader Version	1.2.5
adio protocol version	22
hannel	25 (2.475 GHz)
adio channels	11, 16, 25
PAN ID	8892
EAC addressing mode	Normal address offset
DIP switch value	1
EAC Address	1
Remote open is activated	
Number of paired locks and sensors	1
Device Status	EAC offline

Lock/sensor [01DC80]

MAC Address	00:17:7a:01:02:01:dc:80

June 3, 2013 8:17:12 PM

Adjust the applicable settings below for use with the Vanderbilt SMS access control system. Although only the settings mandatory for use with SMS are noted here. The not applicable settings may be important for Aperio lock functionality. For more information regarding "Not Required" settings please refer to your Aperio Programming Manual."

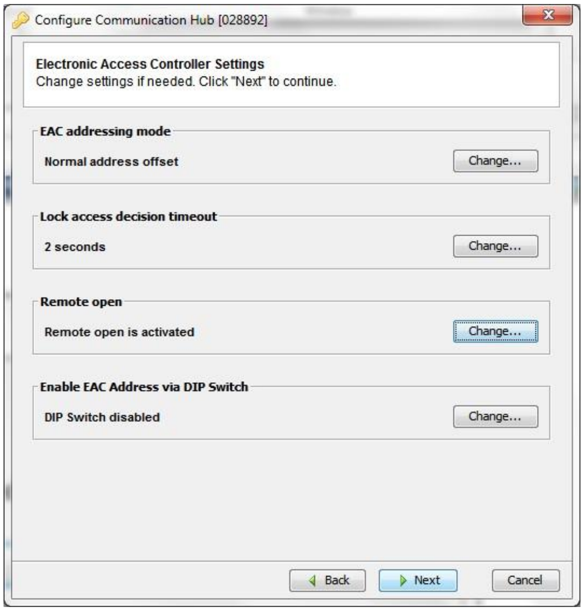
1 RFID Configuration - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

2 Keypad configuration - Not required to be configured on the HUB AH30 for SMS installation

3 Override Credential - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

4 Security Mode - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

5 Electronic Access Controller Settings



Electronic Access Controller Settings
Change settings if needed. Click "Next" to continue.

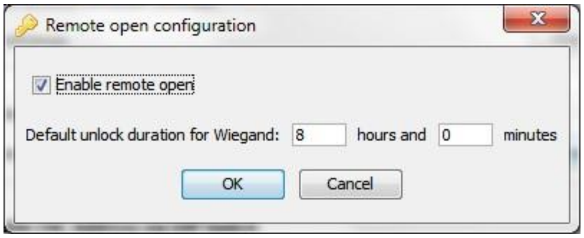
EAC addressing mode
Normal address offset

Lock access decision timeout
2 seconds

Remote open
Remote open is activated

Enable EAC Address via DIP Switch
DIP Switch disabled

- EAC addressing mode - Normal address offset
- Lock access decision timeout - 2 Seconds
- Remote Open - Enabled



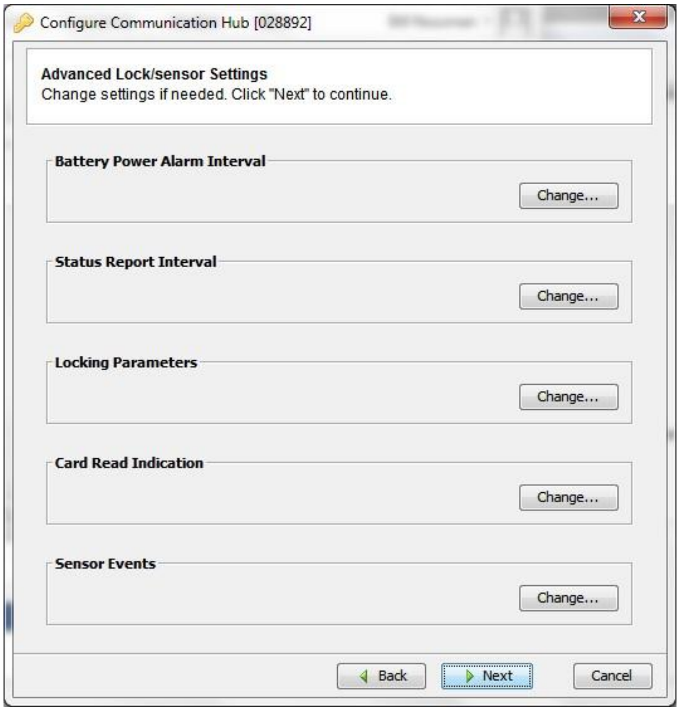
Remote open configuration

☑ Enable remote open

Default unlock duration for Wiegand: 8 hours and 0 minutes

- Enable EAC Address via DIP Switch - Disabled

6 **Advanced Settings** - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.



Configure Communication Hub [028892]

Advanced Lock/sensor Settings

Change settings if needed. Click "Next" to continue.

Battery Power Alarm Interval

Status Report Interval

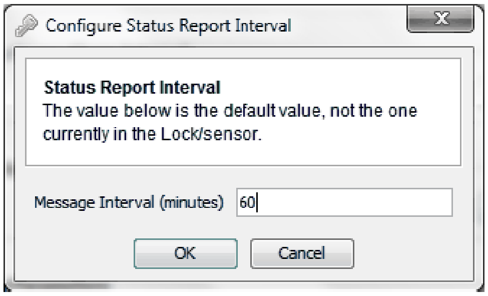
Locking Parameters

Card Read Indication

Sensor Events

7 **Advanced Lock/Sensor Settings**

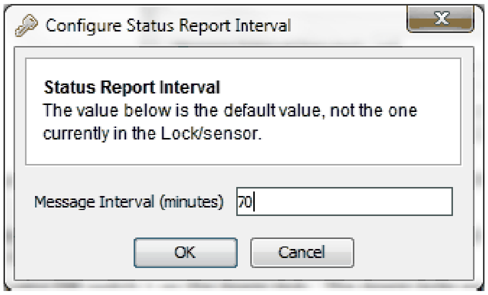
- Battery Power Alarm Interval - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.
- Status Report Interval -When one Aperio Lock is being paired with one Aperio Hub the default setting of 60 Minutes can be used..


Configure Status Report Interval

Status Report Interval
The value below is the default value, not the one currently in the Lock/sensor.

Message Interval (minutes) 60

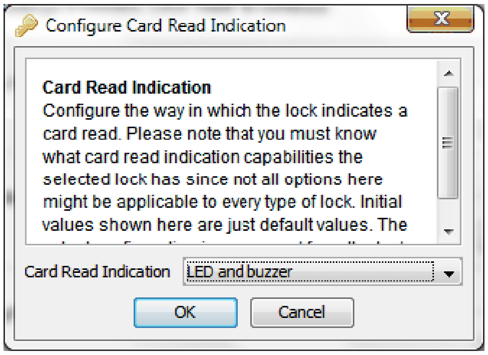
- When configuring the Status Report Interval with multiple Aperio Locks the Message Interval should be set higher for the HUB. Recommended setting is 70


Configure Status Report Interval

Status Report Interval
The value below is the default value, not the one currently in the Lock/sensor.

Message Interval (minutes) 70

- Locking Parameters - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.
- Card Read Indication - Recommended setting is LED and buzzer. See the Aperio Programming Manual for more information regarding the use of this feature.


Configure Card Read Indication

Card Read Indication
Configure the way in which the lock indicates a card read. Please note that you must know what card read indication capabilities the selected lock has since not all options here might be applicable to every type of lock. Initial values shown here are just default values. The

Card Read Indication LED and buzzer

- Sensor Events - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

8 Device Update - **Save the Configuration**

Pair Additional Locks to the HUB

This section defines applicable settings for the Aperio HUB and locks when they are being used with the SMS Access Control System. Please refer to your Aperio Programming manual for more information regarding these features.

Automatic pairing must be enabled using DIP switch 1 on the Aperio Hub. The Aperio locks are addressed automatically by the programming application.

A maximum of 8 Aperio wireless locks may be paired to a single AH30 Hub.
A maximum of 8 locks may be installed on a single VRCNX-R/M/A controller channel.

The addresses of the Aperio locks relate to the programming within the SMS software as noted below:

First / Single AH30 Hub EAC Address = 1		
Paired Aperio Lock	**Aperio Programming Application Address**	**SMS Address**
1	1	1
2	17	2
3	33	3
4	49	4
5	65	5
6	81	6
7	97	7
8	113	8

Add Additional HUBs to the VRCNX-R/M/A Controller

This section defines applicable settings for the 2nd and subsequent Aperio Hubs and locks when they are being used with the SMS Access Control System. This specific example assumes a single lock on the first AH30 Hub on the channel and 7 locks on a 2nd AH30 Hub on the same channel. However, locks may be divided as desired across up to 8 AH30 Hubs per channel following the addressing guidance below.

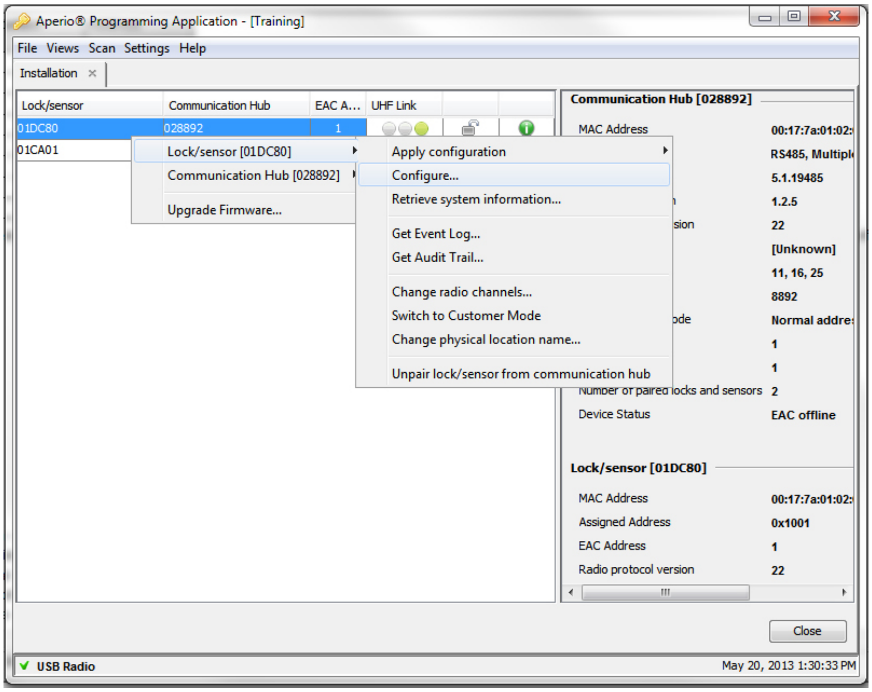
Automatic pairing must be enabled using DIP switch 1 on the Aperio Hub. The Aperio locks are addressed automatically by the programming application.

The addresses of the Aperio locks relate to the programming within the SMS software as noted below:

2nd AH30 Hub Same Channel; EAC Address = 2		
Paired Aperio Lock	**Aperio Programming Application Address**	**SMS Address**
1	EAC Address	1
2	Paired Lock 1 + 16	2
3	Paired Lock 2 + 16	3
4	Paired Lock 3 + 16	4
5	Paired Lock 4 + 16	5
6	Paired Lock 5 + 16	6
7	Paired Lock 6 + 16	7

> The sequence above must be followed for each additional AH30 Hub added to the VRCNX-R/M/A.

To configure the Aperio Locks chose the lock from the installation window of the programming application. Right click on the lock, choose lock/sensor then select configure to begin.



Lock/sensor	Communication Hub	EAC A...	UHF Link
01DC80	028892	1	
01CA01			

Communication Hub [028892]

MAC Address 00:17:7a:01:02:

RS485, Multipl

5.1.19485

1.2.5

sion 22

[Unknown]

11, 16, 25

8892

ode Normal addre

1

1

Number of paired locks and sensors 2

Device Status EAC offline

Lock/sensor [01DC80]

MAC Address 00:17:7a:01:02:

Assigned Address 0x1001

EAC Address 1

Radio protocol version 22

May 20, 2013 1:30:33 PM

1 RFID Configuration -Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

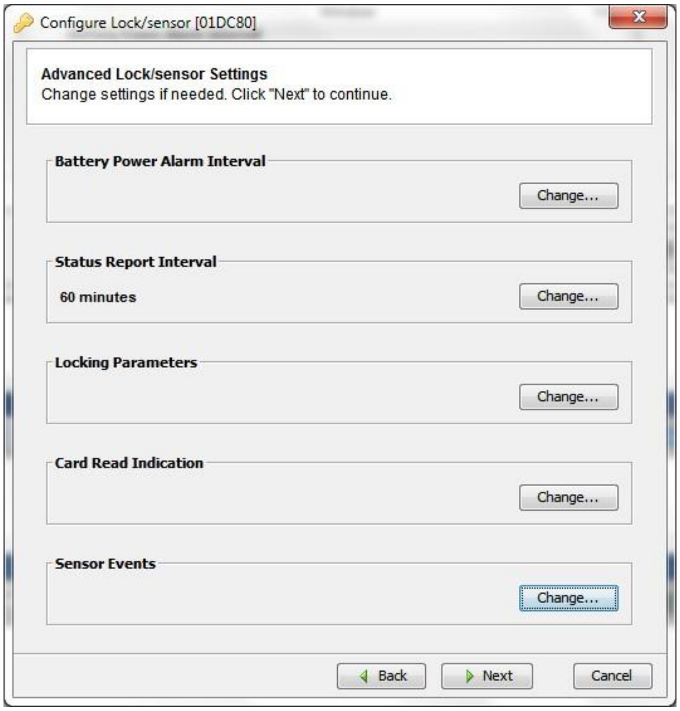
2 Keypad configuration - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

- Default Settings: User enters the PIN followed by the ***** on the keypad. User can use the # on the keypad to clear and start again.

3 Override Credential - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

4 Security Mode - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

5 Advanced Settings - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.



Configure Lock/sensor [01DC80]

Advanced Lock/sensor Settings
Change settings if needed. Click "Next" to continue.

Battery Power Alarm Interval

Status Report Interval
60 minutes

Locking Parameters

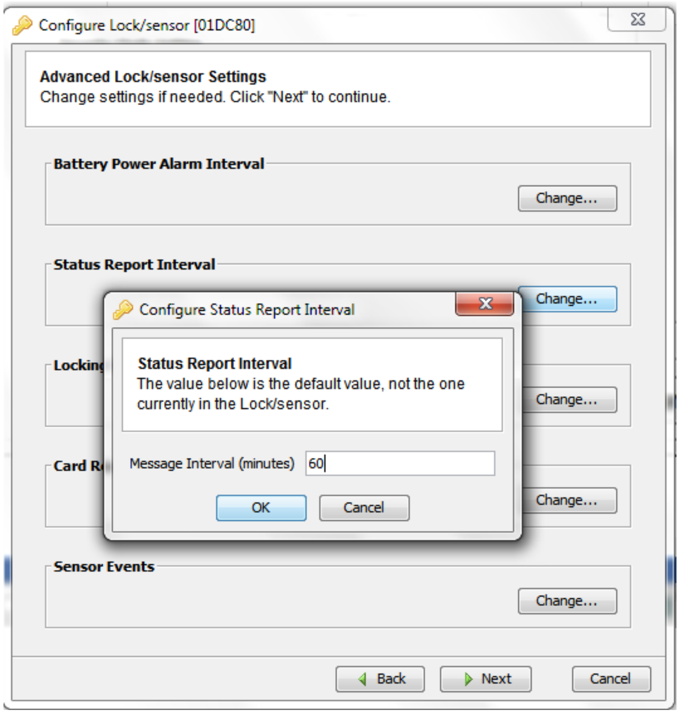
Card Read Indication

Sensor Events

Advanced Lock/Sensor Settings

1 Battery Power Alarm Interval - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

- Status Report Interval - Should be set lower than the Status report interval of the HUB. If the HUB has been set to 70 minutes this recommended settings is 60 minutes.



Configure Lock/sensor [01DC80]

Advanced Lock/sensor Settings
Change settings if needed. Click "Next" to continue.

Battery Power Alarm Interval

Status Report Interval

Lockin

Card R

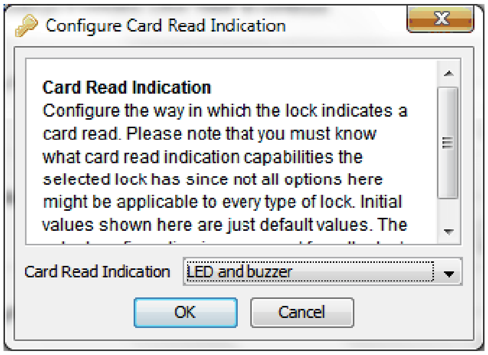
Sensor Events

Configure Status Report Interval

Status Report Interval
The value below is the default value, not the one currently in the Lock/sensor.

Message Interval (minutes) 60

- Locking Parameters - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.
- Card Read Indication - Recommended setting is LED and buzzer. See the Aperio Programming Manual for more information regarding the use of this feature.



Configure Card Read Indication

Card Read Indication
Configure the way in which the lock indicates a card read. Please note that you must know what card read indication capabilities the selected lock has since not all options here might be applicable to every type of lock. Initial values shown here are just default values. The

Card Read Indication LED and buzzer

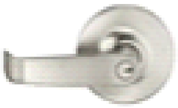
- Sensor Events - Not required for SMS installation. See the Aperio Programming Manual for more information regarding the use of this feature.

2 Device Update - Save the Configuration file. This file can be applied to future locks. The saved configuration settings would then be applied to the new lock.

3 Confirm the settings - follow the onscreen instructions to complete the pairing presenting a card to the device.

Aperio Locks

IN100 v2 / v3 Mortise Locks



The IN100 utilizes HID® iCLASS® 13.56 MHz smart card technology and is available in mortise lock and cylindrical lock configurations.

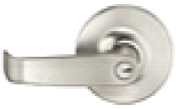
Mechanical Features

- Certified ANSI/BHMA A156.2 Series 4000 - Grade 1
- UL/ULC Listed for fire doors*
- Windstorm & Florida Building Code information is listed on page 11
- Motor driven Cylindrical Lock
- Latch Stainless Steel, 1/2" (13mm) throw
- 2-3/4" (70mm) backset standard
- For 1-3/4" (44mm) thick door standard. Consult factory for other thicknesses
- Handing easily field reversible without disassembling lockbody
- Heavy duty lever spring return
- Steel mounting studs
- Not available with 10-UL-, 82-, 83-, 84- options

Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 - 80 feet depending on building environments.
- EAC Communication: RS-485 or Wiegand
- Power: 6 AA batteries
- Security: AES 128 encryption
- Compatible with desktop, laptop or netbook with Windows XP or Windows 7, Java 6.2 or greater, and USB 2.0 port.

IN100 v2 / v3 Cylindrical Locks



The IN100 utilizes HID® iCLASS® 13.56 MHz smart card technology and is available in mortise lock and cylindrical lock configurations.

Mechanical Features

- Certified ANSI/BHMA A156.2 Series 4000 - Grade 1
- UL/ULC Listed for fire doors*
- Windstorm & Florida Building Code information is listed on page 11
- Motor driven Cylindrical Lock
- Latch Stainless Steel, 1/2" (13mm) throw
- 2-3/4" (70mm) backset standard
- For 1-3/4" (44mm) thick door standard. Consult factory for other thicknesses
- Handing easily field reversible without disassembling the lock body
- Heavy duty lever spring return
- Steel mounting studs
- Not available with 10-UL-, 82-, 83-, 84- options

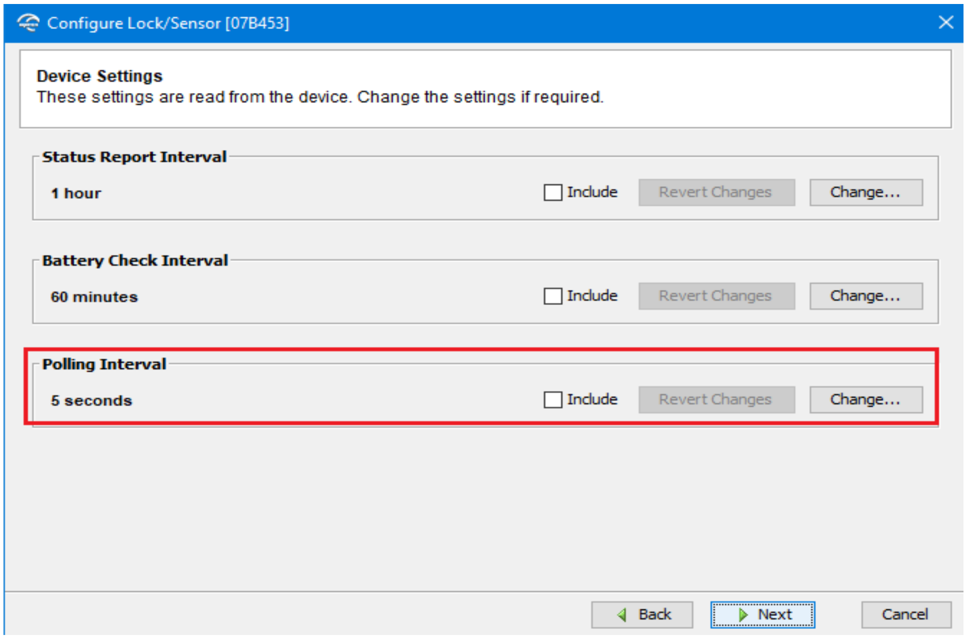
Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 - 80 feet depending on building environments.
- EAC Communication: RS-485 or Wiegand
- Power: 6 AA batteries
- Security: AES 128 encryption
- Compatible with desktop, laptop or netbook with Windows XP or Windows 7, Java 6.2 or greater, and USB 2.0 port.

IN100 v3 – Gen 5 Hub Only Features

Certain new features are available for IN100 v3 locks when using the Gen 5 Hub:

Fast Polling – improved performance for MROs and AROs:



Configure Lock/Sensor [07B453]

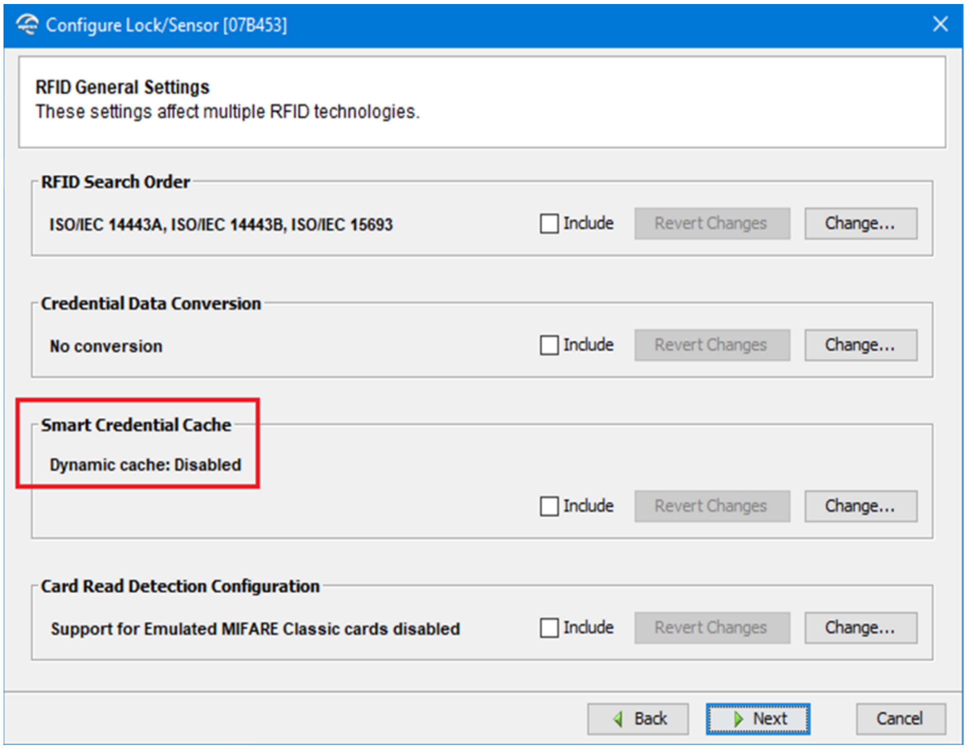
Device Settings
These settings are read from the device. Change the settings if required.

Status Report Interval
1 hour — □ Include — Revert Changes — Change...

Battery Check Interval
60 minutes — □ Include — Revert Changes — Change...

Polling Interval
5 seconds — □ Include — Revert Changes — Change...

Cache Mode – Configurable Credential Cache if Hub communications is lost:



Configure Lock/Sensor [07B453]

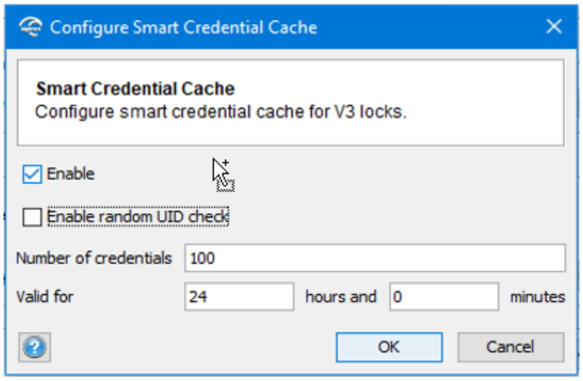
RFID General Settings
These settings affect multiple RFID technologies.

RFID Search Order
ISO/IEC 14443A, ISO/IEC 14443B, ISO/IEC 15693 — □ Include — Revert Changes — Change...

Credential Data Conversion
No conversion — □ Include — Revert Changes — Change...

Smart Credential Cache
Dynamic cache: Disabled — □ Include — Revert Changes — Change...

Card Read Detection Configuration
Support for Emulated MIFARE Classic cards disabled — □ Include — Revert Changes — Change...



Smart Credential Cache
Configure smart credential cache for V3 locks.

☑ Enable

□ Enable random UID check

Number of credentials 100

Valid for 24 hours and 0 minutes

- Number of credentials to cache – default is 100.

- Total amount of most recent valid credentials the IN100 V3 Lock will hold in Cache Memory while communicating to the AH30 Hub Gen 5.

- Cached credentials will still gain access to the lock when communications to the AH30 HUB is lost.

- Valid for Hours and minutes – defaults are 24 hours & 0 minutes. Credentials will no longer gain access after this time has expired.

PR100 v2 Mortise Locks

The PR100 utilizes HID® 125 kHz proximity or 13.56 MHz iCLASS® technology and is available in mortise lock, cylindrical lock or exit device configurations with reader only or reader/keypad.

Mechanical Features

- Certified ANSI/BHMA A156.2 Series 4000 - Grade 1 UL/ULC Listed for fire doors*
- Windstorm & Florida Building Code information is listed on page 16
- Motor driven Cylindrical Lock
- Latch Stainless Steel, 1/2" (13mm) throw
- 2-3/4" (70mm) backset standard
- For 1-3/4" (44mm) thick door standard. Consult factory for other thicknesses
- Non-Handed lock body, levers may be handed (Specify RH, RHR, LH or LHR)
- Heavy duty lever spring return
- Steel mounting studs
- Not available with 10-UL-, 82-, 83-, 84- options

Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 - 80 feet depending on building environments.
- EAC Communication: RS-485 or Wiegand
- Power: 6 AA batteries
- Security: AES 128 encryption
- Compatible with desktop, laptop or netbook with Windows XP or Windows 7, Java 6.2 or greater, and USB 2.0 port.

PR100 v2 Cylindrical Locks

The PR100 utilizes HID® 125 kHz proximity or 13.56 MHz iCLASS® technology and is available in mortise lock, cylindrical lock or exit device configurations with reader only or reader/keypad.

Mechanical Features

- Certified ANSI/BHMA A156.2 Series 4000 - Grade 1 UL/ULC Listed for fire doors*
- Windstorm & Florida Building Code information is listed on page 16
- Motor driven Cylindrical Lock
- Latch Stainless Steel, 1/2" (13mm) throw
- 2-3/4" (70mm) backset standard
- For 1-3/4" (44mm) thick door standard. Consult factory for other thicknesses
- Non-Handed lock body, levers may be handed (Specify RH, RHR, LH or LHR)
- Heavy duty lever spring return
- Steel mounting studs
- Not available with 10-UL-, 82-, 83-, 84- options

Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 to 80 feet depending on building environment
- EAC Communication: RS-485 or Wiegand
- Power: 6 AA batteries
- Security: AES 128 encryption
- Compatible with desktop, laptop or netbook with Windows XP or Windows 7, Java 6.2 or greater, and USB 2.0 port.

K100 v2 Cabinet Locks

The Aperio K100 wireless cabinet lock makes it easy and cost effective to bring real-time access control to cabinets and drawers where audit trail and monitoring are becoming increasingly critical. The K100 cabinet lock uses local wireless communication between the lock and an Aperio hub to connect to the SMS access control system eliminating the cost and difficulty of bringing integrated access control to the cabinet.

Benefits

- Integrated reader, monitoring and short-range wireless radio simplifies installation and reduces material cost.
- Real-time cabinet door and latch locked status monitoring with integrated door position, latch locked, tamper and low battery signals. Know and respond immediately to situations at opening.
- 90,000 cycles of operation with a single CR123A battery, providing an extremely long life with minimal impact to the environment
- Two forms of battery fail over-ride, including a mechanical key override feature and a battery jump port to provide complete assurance against battery failure.
- Supports HID 13.56 MHz iClass contactless credentials (full authentication, all formats). Integrates easily with existing smart card credential systems.

Aperio Technology

- Minimal field configuration for quick, easy wireless deployments that eliminate the cost and inconvenience of complex wireless site surveys.
- Fully-encrypted AES 128 wireless communication between the 620 cabinet lock and the hub. High security standardized communications ensures data security.
- Global Aperio technology is ideal for companies who wish to deploy a standard infrastructure across multi-national locations.
- Available across a range of locking hardware from ASSA ABLOY Group brands, Aperio provides the flexibility to address a variety of applications through your facility

Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 to 80 feet depending on building environment
- EAC Communication: RS-485 or Wiegand
- Power: 1 standard CR123A
- Security: AES 128 encryption
- Provides alarms for Tamper, Low Battery and Lock Jamb
- Auto Re-Lock.

A100 v2

The A100 utilizes HID® 125 kHz proximity or 13.56 MHz iCLASS® technology and is available in reader only or reader/keypad configurations.

Mechanical Features

- ANSI/BHMA Grade 1 Hardware
- Field selectable handing
- Vandal resistant lever with break-away (resettable) clutch
- Mortise cylinder override
- Efficient power usage; 4 AA alkaline batteries - 60,000 activations

Access Control Features

- Wireless Communication: IEEE 802.15.4 (2.4 GHz)
- Wireless Range: 50 - 80 feet depending on building environments.
- EAC Communication: RS-485 or Wiegand
- Power: 6 AA batteries
- Security: AES 128 encryption
- Compatible with desktop, laptop or netbook with Windows XP or Windows 7, Java 6.2 or greater, and USB 2.0 port.

NOTE: Keypad Clear and Re-enter via "*" as well as Send via "#" are reversed from all other supported Aperio Locks

CHAPTER 26

Assa Abloy IP-Enabled Locks

Overview

ASSA ABLOY IP-Enabled locks tap into a building's existing data network to provide the ultimate in security and ease of installation. PoE and WiFi IP-Enabled locks can be seamlessly integrated with the SMS system. The local decision (offline) IP-Enabled locks communicate directly to the Assa Abloy Door Service Router (DSR) web service via TCP/IP. The SMS - DSR bridge service communicates to the SMS SQL database and System Processor (SP) and to the DSR to program the locks and return lock activity to SMS. Once configured the locks can be fully managed from within SMS. Specifications and guidelines for configuring the IP-Enabled devices in SMS are in the pages that follow.

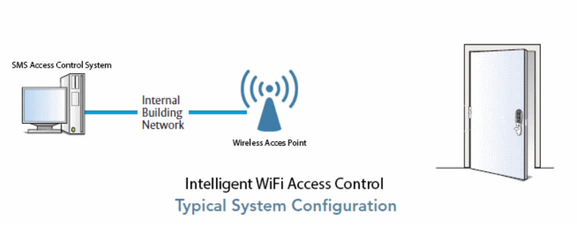
Wireless

ASSA ABLOY's WiFi-enabled locksets utilize standard nonproprietary wireless access points to connect to a facility's network. The locks work with any open architecture access control system, providing centrally managed control without many of the costs, labor and infrastructure upgrades associated with traditional hardware. Wireless locks communicate to the SMS Access Control System via the DSR at preset times (up to 4 times per day) and during programmed alarm events.

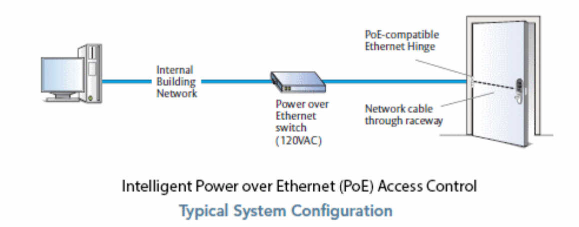
Power Over Ethernet (PoE)

With this edge-of-network access control solution from ASSA ABLOY, all data and power are sent to the lock through standard CAT-5 wiring. Once connected, the lock instantly integrates with the building's security control platform, providing real-time monitoring capabilities and centralized control over all openings. PoE locks communicate in near real-time with the SMS Access Control System via the DSR.

Typical Configurations



Intelligent WiFi Access Control
Typical System Configuration


Internal Building Network
Power over Ethernet switch (120VAC)
PoE-compatible Ethernet Hinge
Network cable through raceway

Intelligent Power over Ethernet (PoE) Access Control
Typical System Configuration

SMS Programming Notes:

An Assa Abloy certified installer must perform the initial installation and configuration of Assa Abloy DSR and IP-Enabled locks before they can be configured for use within SMS.

SMS only supports the specific Assa Abloy IP-Enabled locks identified later in this section. The results of using untested IP-Enabled lock models is unpredictable and unsupported.

SMS supports the following automated features for use with Assa Abloy IP-Enabled Locks:

- Unlock Command with User Defined Timezones (with multiple intervals per Timezone)
- Holiday Exception Definitions
- Scheduled Unlocks (Automatic Overrides) with User Defined Timezones (single interval per Timezone)
- Credential Enabled Scheduled Unlock (ARO Initiated by First Person In)

Note: The following restrictions must be kept in mind when programming the WiFi IP-Enabled Locks

Access, Timezones, Holidays, AROs or First Person In Additions or Modifictions Will NOT Be Downloaded to the Locks Except As Defined By The Wireless Connection Schedule Unless the WiFi locks are Manually Woken Up for Communication to the DSR.

SMS DSR Configuration Notes:

SMS requires that the DSR is configured to filter the transactions listed below.

- USERADDED
- USERDELETED
- DATETIMESET
- LOGCLEARED
- DBRESET
- COMMSTARTED
- COMMENDED
- NVRAMPBCLEAR
- NVRAMLAYOUTCHANGE
- NVRAMOK
- USERREPLACED
- USERUPDATED
- PASSAGEACTIVE
- BATTERYCHECKHELDOFF
- CHECKSUMCONFIG
- CHECSUMTZ
- RADIOTIMEOUT

Before You Begin

Each lock ships from the factory with three preprinted labels specifying each lock's unique serial number and MAC address.

The smaller label can be found affixed just below the battery holder on the lock controller while the two larger labels (Figure 1) can be found both in the box and affixed to the outside of the box (for easy identification).

The blank fields should be filled in and it is recommended that a label (and/or its information) be placed in an easily accessible and visible location such as a blank page on a clipboard or notebook for later reference.

The following items (in a kit ordered separately) are needed for initial configuration of the locks:

- Installation CD: Includes both Network and Lock Configuration Tool applications.

IMPORTANT: There are three different cable types that can be used to connect the laptop to the lock:

- A standard DB9 (female) serial-to-RJ11 cable
- An eight-pin Molex (female) to DB9 (female) serial port

Both cables require a DB9 serial port connection on the laptop.
If there is no such connection, an RS232-to-USB Adapter, which provides the needed DB9 (male) RS232 serial port may be required.

- A USB Mini cable

PoE Controller LED's

When power is applied to the controller, three lights indicate status:

- Red LED (bottom of unit): Power ON
- Red LED (middle): Controller is enabled and measures 9V to Auxiliary Power
- Green flashing LED (Upper): Indicates network connectivity

Overview

The Network and Lock Configuration Tools are Windows-based applications that create secure configuration files containing the network communication parameters required to allow a lock controller to communicate with the Assa Abloy DSR. SMS communicates with the DSR via a bridge service. Since this configuration information is site-specific and highly confidential, the configuration process should be conducted onsite using customer- supplied data.

Prerequisites

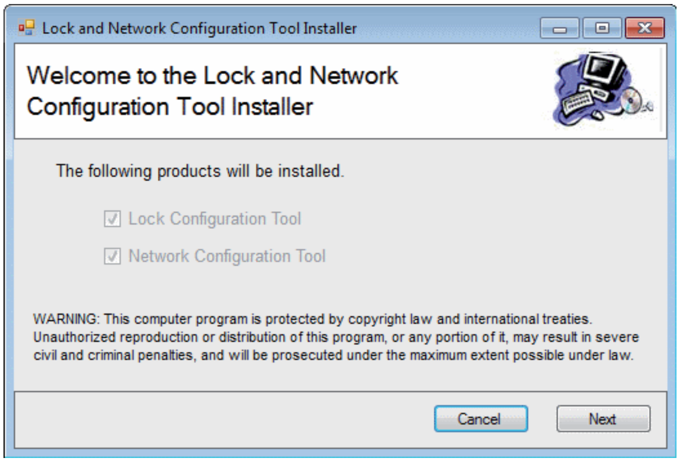
The following items are required for this combined installation of the configuration tools:

- A Windows PC laptop running the Microsoft Windows 2000, XP Professional, Vista, Windows 7 or Windows 8 operating system
- Installation CD with the Network and Lock Configuration Tool installation files
- Information regarding the local network environment (site-specific)
- Firmware file (on installation CD and also available at io.com)

Installation

Place the installation CD (provided with the lock shipment) in the PC's drive. On most computers, an autorun program launches automatically. Upon activation of the application the "User Account Control" Windows dialog appears to alert the user that this program must be run in "Administrator Mode".

Press **Yes** to accept and continue.



Lock and Network Configuration Tool Installer

Welcome to the Lock and Network Configuration Tool Installer

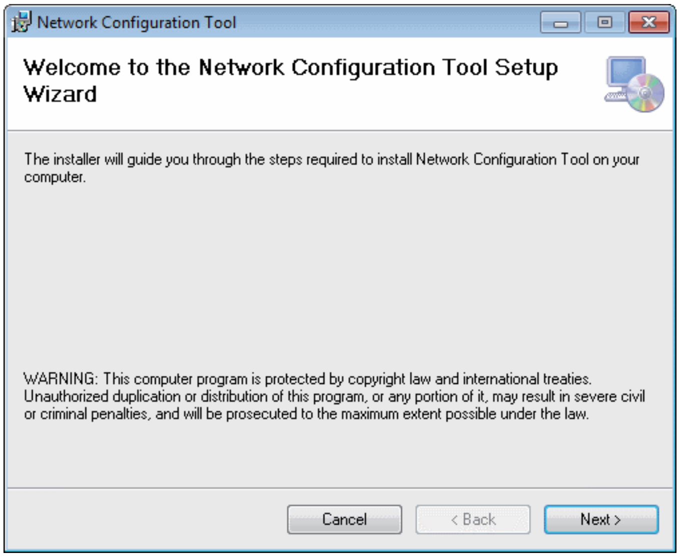
The following products will be installed.

☑ Lock Configuration Tool

☑ Network Configuration Tool

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted under the maximum extent possible under law.

Select **Next** in the “Lock and Network Configuration Tool Installer” window to install both the Lock Configuration Tool and Network Configuration Tool applications.



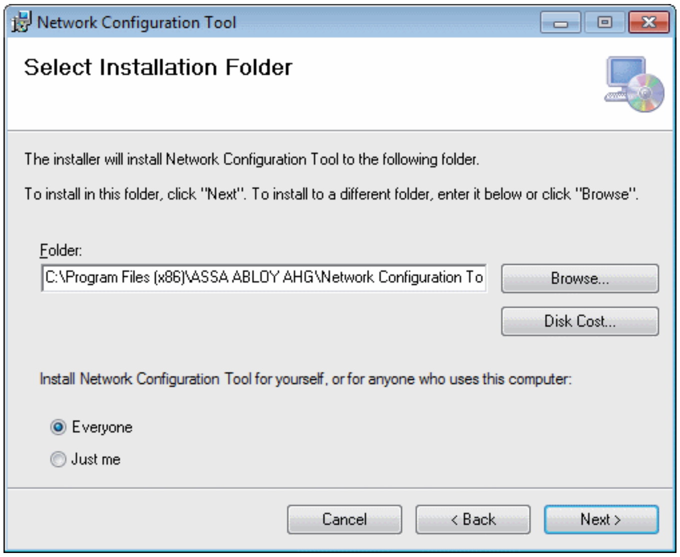
Network Configuration Tool

Welcome to the Network Configuration Tool Setup Wizard

The installer will guide you through the steps required to install Network Configuration Tool on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Select **Next** in the NCT "Welcome" screen to continue installation.



Network Configuration Tool

Select Installation Folder

The installer will install Network Configuration Tool to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

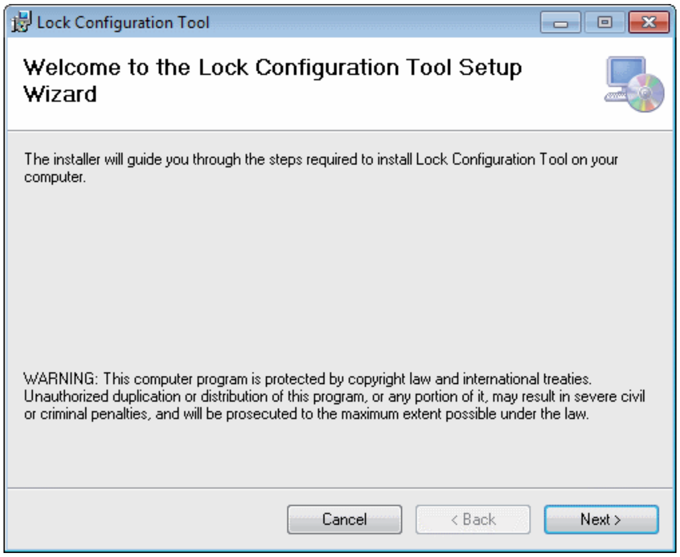
Folder:
C:\Program Files (x86)\ASSA ABLOY AHG\Network Configuration To

Install Network Configuration Tool for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Vanderbilt recommends selecting the **Disk Cost** button once the "Select Installation Folder" dialog is displayed to review available drives, space available and space required for installation.

Select **Next** to continue and Network Configuration Tool installation will begin. The Lock Configuration Tool Setup Wizard will initiate once installation has completed.



Lock Configuration Tool

Welcome to the Lock Configuration Tool Setup Wizard

The installer will guide you through the steps required to install Lock Configuration Tool on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Click **Next** and follow the on-screen prompts to complete the installation.

Network Configuration Tool

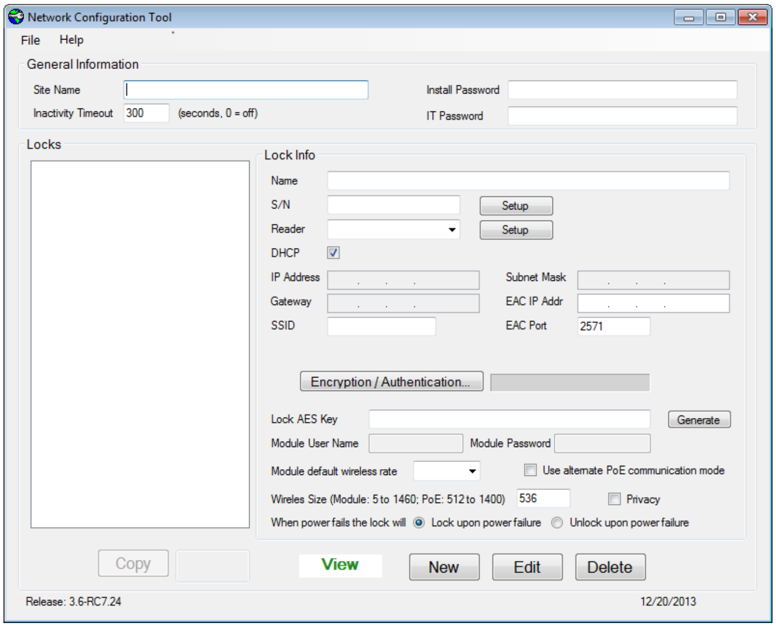
The Network Configuration Tool application creates secure configuration files that contain the network communication parameters required to allow a lock controller to communicate with SMS.

This configuration information is site specific and highly confidential, the configuration process should be done onsite using customer-supplied data.

Creating a Configuration File

Open the NCT application by either double-clicking the "Network Configuration Tool" icon placed on the desktop or navigating to Start --> All Programs --> Network Configuration Tool --> Network Configuration Tool(.exe).

The main window is divided into two sections:



Inactivity Timeout 300 (seconds, 0 = off)

DHCP ☑

EAC Port 2571

☐ Use alternate PoE communication mode

Wireles Size (Module: 5 to 1460; PoE: 512 to 1400) 536

☐ Privacy

When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

Release: 3.6-RC7.24

12/20/2013

General Information:

- Site Name - identifies the set of locks and is typically represented by the company name, company and division, etc.
- Installer Password - allows the installer to use the data but not view the network communication parameters
- IT Password - allows the installer to view and edit all network communication parameters
- Inactivity Timeout - determines how long the Lock Configuration Tool will wait for user input before automatically terminating
  A security measure for protecting against unauthorized access. Disable by setting to 0. Default = 300 seconds.

Locks:

- Name - Used to identify the lock (*"West Stairwell Door" or "Rear Exterior Door", etc.*)
- S/N - the 16-character lock serial number from the label on the lock controller (*refer to "Before You Begin"*)
- Reader - drop-down list for selecting the type of card you are using (*configure as required by Assa Abloy*)

- DHCP - Checked to enable Dynamic Host Configuration Protocol for lock IP addressing (*enabled by default*)
- IP Address - Use to assign lock static IP address (*if DHCP is not enabled*)
- Subnet Mask - Use to assign lock static Subnet Mack (*if DHCP is not enabled*)
- Gateway - Use to assign lock static default Gateway (*if DHCP is not enabled*)

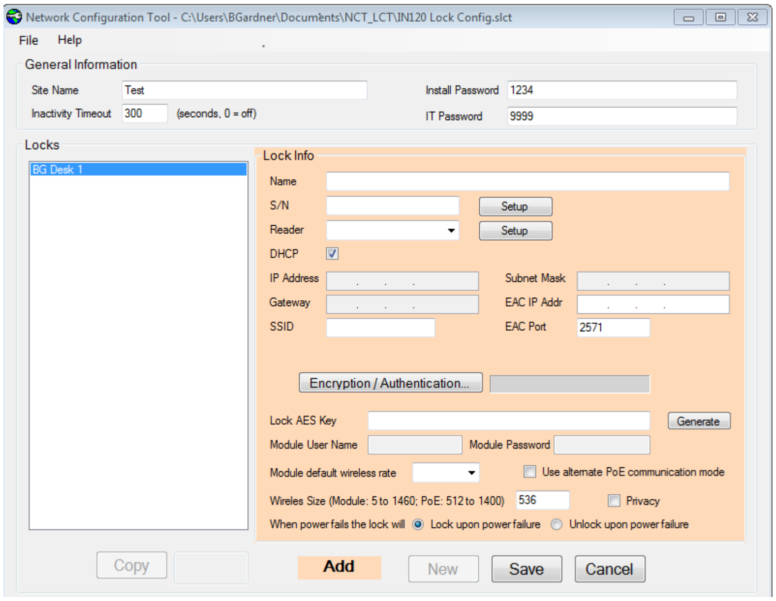
IP Address, Subnet Mask and Gateway must be supplied if DHCP is not enabled

- EAC IP Address - IP of Door Service Router (DSR)
- SSID - Used to specify Service Set Identifier for wireless networks only (*case-sensitive*)
- EAC Port - 2571 by default (see NOTE).
- Encryption/ Authentication - Select to choose method of Security Encryption (*lock AES Key*)
- Generate - Select to generate key (*if AES used*)
- Module User Name - *reserved for future use*
- Module Password - *reserved for future use*
- Module default wireless rate - N/A
- Use alternate PoE communication mode - *not used*
- Wireless Size - The size, in bytes, of the largest protocol data unit that can pass
- Privacy -
- When Power Fails - Used to specify the desired lock mode on loss of power

Creating a New Lock Entry

The "Locks" section is in "View Mode" by default.

Once the "General Information" section has been completed, click **New** to enable the "Locks" section for data entry.



Network Configuration Tool - C:\Users\BGardner\Documents\NCT_LCT\IN120 Lock Config.slct

General Information

Site Name: Test

Inactivity Timeout: 300 (seconds, 0 = off)

Install Password: 1234

IT Password: 9999

Locks

BG Desk 1

Lock Info

DHCP ☑

EAC Port: 2571

Module default wireless rate

☐ Use alternate PoE communication mode

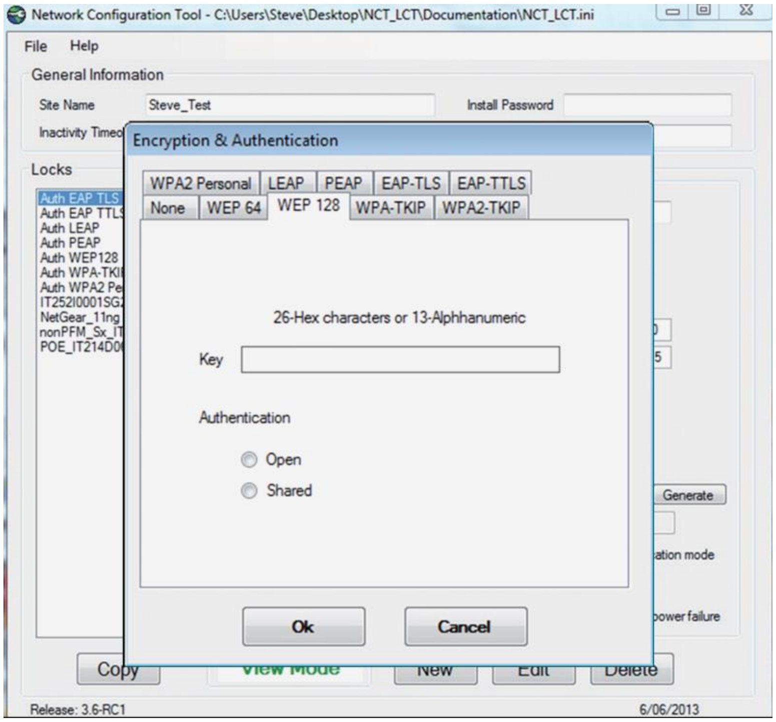
Wireles Size (Module: 5 to 1460; PoE: 512 to 1400): 536

☐ Privacy

When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

Cancel can be selected at any time to abort the New Lock operation after confirmation.

Click **Encryption/Authentication** to bring up the "Encryption & Authentication" dialog



Site Name Steve_Test

Select the appropriate tab to select and configure the desired encryption and authentication.

- None: no encryption
- WEP-64: enter an encryption key for 64-bit WEP authentication
- WEP-128: enter an encryption key for 128-bit WEP authentication
- WPA-TKIP: enter an encryption key for WPA-TKIP authentication
- WPA2-TKIP: enter an encryption key for WPA2-TKIP authentication

Use WPA2-Personal mode on networks supporting WPA2-AES only.

Do NOT Use WPA2-Personal on networks supporting both WPA2 and WPA. Networks supporting both WPA2 and WPA are in "migration mode". Assa Abloy IP Enabled locks must use WPA2-TKIP or WPA-TKIP to connect to networks in Migration Mode.

- WPA2-Personal: enter an encryption key for WPA2-Personal authentication
- LEAP: enter the username and password for LEAP authentication
- PEAP: click the file browser icon to locate and bind to the CA Certificate File. Enter the identification name and password for EAP authentication
- EAP-TLS: enter the CA Certificate filename, the Client Certificate filename, Private-KeyCertificate, Private-Key password, and the identification name and password for EAP authentication. Select Free-Radius to default to these values.

Saving Lock Info

Click **Save** to validate and save the lock configuration once all information has been entered.

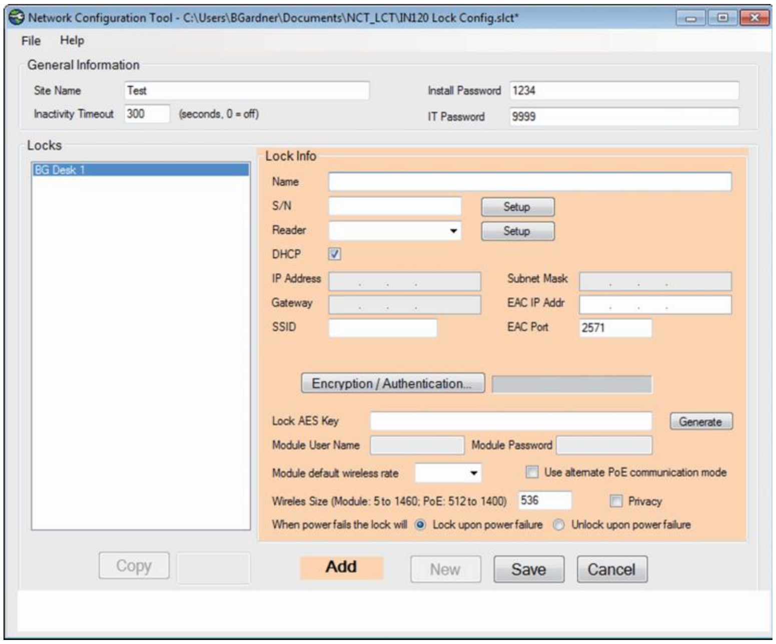
The new lock will appear listed in alphabetically order in the lock list and the tool will revert to "View Mode".

Copying a Lock

Use the Copy function to create a new lock with configuration settings similar to an existing lock.

Select the source lock in the list and click **Copy** below the list.

The configuration tool will copy all data from the source lock to a new lock entry and the tool will enter "Add Mode".


Network Configuration Tool - C:\Users\BGardner\Documents\NCT_LCT\IN120 Lock Config.slct*

General Information

Site Name: Test

Inactivity Timeout: 300 (seconds, 0 = off)

Install Password: 1234

IT Password: 9999

Locks

BG Desk 1

Lock Info

Name:

S/N:

Reader:

DHCP: ☑

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

EAC IP Addr: . . .

SSID:

EAC Port: 2571

Lock AES Key:

Module User Name:

Module Password:

Module default wireless rate:

□ Use alternate PoE communication mode

Wireles Size (Module: 5 to 1460; PoE: 512 to 1400): 536

□ Privacy

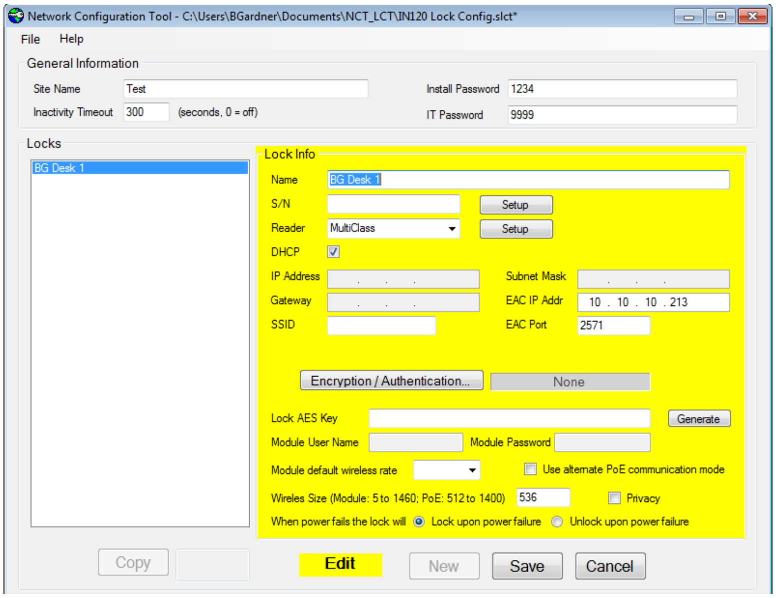
When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

Notice that the "Edit" button change to "Save" and the "Delete" button changes to "Cancel.

All configuration data from the source lock can now be edited and saved to the new lock.

Editing an Existing Lock

Select an existing lock from the list and click **Edit** to modify the configuration for an existing lock.



Network Configuration Tool - C:\Users\BGardner\Documents\NCT_LCT\IN120 Lock Config.slct*

General Information

Site Name: Test

Inactivity Timeout: 300 (seconds, 0 = off)

Install Password: 1234

IT Password: 9999

Locks: BG Desk 1

Lock Info

Name: BG Desk 1

S/N:

Reader: MultiClass

DHCP: ☑

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

EAC IP Addr: 10 . 10 . 10 . 213

SSID:

EAC Port: 2571

Encryption / Authentication... None

Lock AES Key:

Module User Name:

Module Password:

Module default wireless rate:

□ Use alternate PoE communication mode

Wireles Size (Module: 5 to 1460; PoE: 512 to 1400) 536

□ Privacy

When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

Notice that the "Edit" button change to "Save" and the "Delete" button changes to "Cancel.

All configuration data from the selected lock can now be edited and saved.

Deleting A Lock

Select an existing lock from the list and click **Delete**.

Selecting **Yes** to confirm the deletion will remove the lock configuration from the tool.

Saving a Configuration File

Select **Save** or **Save As...** from the **File** menu to save a configuration file. Save will behave like Save As... for new files.

Provide a file name when prompted. Use ".slct" for the file extension.

Click on the **File name** drop-down menu to select existing "Secure LCT Configuration Files (*.slct)".

Closing a Configuration File

Select **Close** from the **File** menu to close the currently open configuration file.

You will be prompted to save or discard any changes made to the current configuration.

Select **Yes** to retain current modifications or **No** to discard. Click **Cancel** to abort.

Opening an Existing Configuration File

Select **Open...** from the **File** menu to open an existing configuration file.

Once a specific configuration file has been selected, a prompt for the IT Password will be displayed.

Enter the IT Password to load the configuration file for editing.

Terminating the Application

Select **Exit** from the **File** menu or click the **Close** box in the upper right corner of the main window to close and terminate the application.

You will be prompted to save or discard any changes made to the current configuration.

Select **Yes** to retain current modifications or **No** to discard. Click **Cancel** to abort.

Lock Configuration Tool

Overview

The Lock Configuration Tool (LCT) is a Windows application used to minimally configure the lock controllers. Minimal information must be configured to allow a lock controller to communicate with the Door Service Router (DSR) and thereby with SMS. Once connection to the DSR and SMS is established successfully, all lock users and schedules are downloaded, and lock configuration is complete.

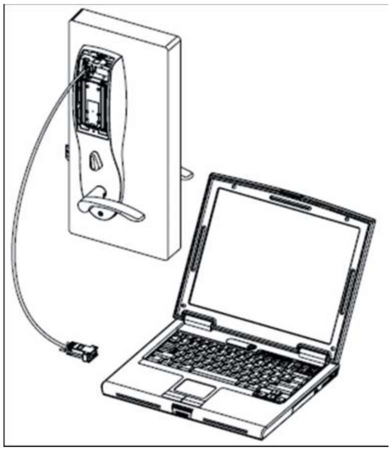
Setup files for installing the LCT are found on the NCT/LCT Installation CD provided with the locks should have been installed as part of the combined installation on install of the Network Configuration Tool.

Requirements

The following items are required to perform basic lock configuration at the time of lock installation.

- Windows laptop running either the Microsoft Windows 2000, Windows XP Professional, Windows Vista, Windows 7 or Window 8 operating system.
- Lock Configuration Tool application (from installation CD)
- Firmware file (from installation CD or **io.com**)
- Credential for testing installed locks
- Security tool to open lock battery cover
- Local Configuration File with associated Installer Password; and optionally IT Password (*created with NCT*)

- Standard DB9 (female) serial to RJ11 cable; or 8-pin Molex (female) to DB9 (female) serial port; or mini-USB cable



Each lock must be supplied with the appropriate communications parameters before it can communicate properly to the DSR and SMS.

Configuration information is typically supplied by the customer via a Configuration File created using the Network Configuration Tool. The Configuration File contains an entry for each lock controller to be configured. A name/description, encryption key, network communication parameters and the lock serial number is provided for each lock.

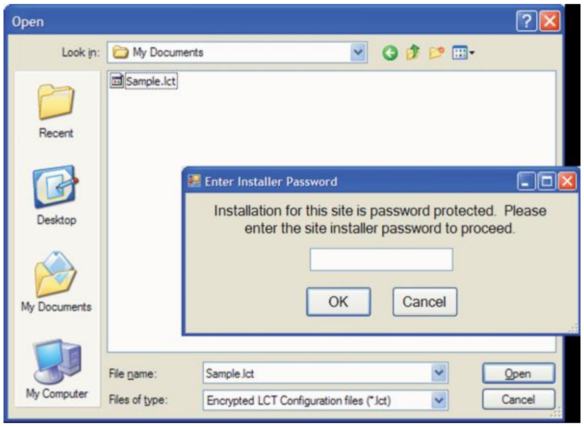
Programming a Lock

Customer should provide the installer with the Configuration File and the Installer Password.

Open Config File

Launch the Lock Configuration Tool and select **Open** from the **File** menu.

Choose the desired configuration file.



Look in: My Documents

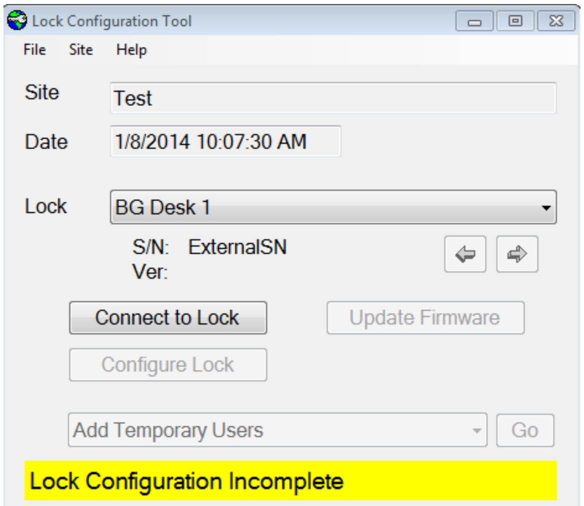
Installation for this site is password protected. Please enter the site installer password to proceed.

File name: Sample.lct

Files of type: Encrypted LCT Configuration files (*.lct)

The Installer Password will appear immediately if one was assigned.

The basic site information, the date and time that the configuration file was generated, the list of defined locks and the current lock status are displayed once the Installer Password is correctly entered. The arrow buttons can be used to step through the set of defined locks or a particular lock can be selected directly using the drop-down.



Site: Test

Date: 1/8/2014 10:07:30 AM

Lock: BG Desk 1

S/N: ExternalSN

Ver:

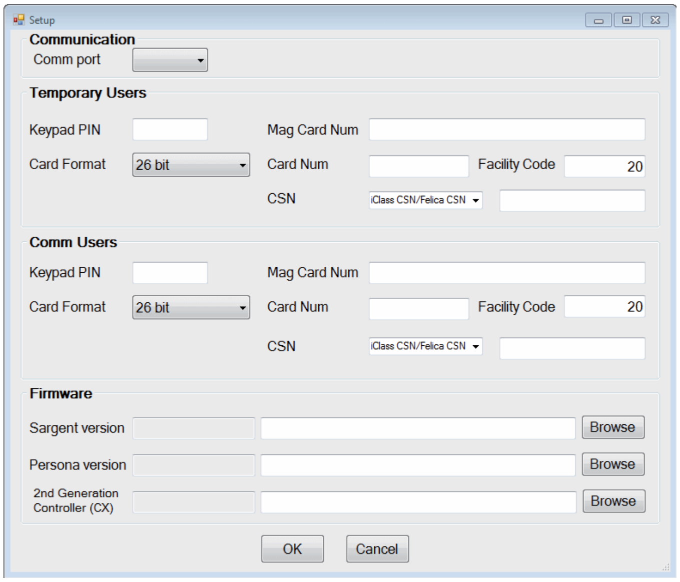
Lock Configuration Incomplete

Lock status is maintained until a configuration file with a different site name is loaded, even if the application is stopped and restarted or the same configuration file is reloaded.

Setup

Select **File** --> **Setup** --> **Setup Dialog** to configure a lock.

The Setup dialog contains four sections:



Communication

Comm port

Temporary Users

Keypad PIN

Mag Card Num

Card Format: 26 bit

Card Num

Facility Code: 20

CSN: iClass CSN/Felica CSN

Comm Users

Keypad PIN

Mag Card Num

Card Format: 26 bit

Card Num

Facility Code: 20

CSN: iClass CSN/Felica CSN

Firmware

Sargent version

Persona version

2nd Generation Controller (CX)

- Communication - Use to specify the laptop COM port for communications to the lock controller
- Temporary Users - Use to configure temporary users

- Comm Users - Use to configure Communications Users
- Firmware - Use to define the latest firmware which will be used to update the lock controllers

Temporary Users

Temporary Users can be used for testing lock configuration and until the lock is successfully connected to SMS. The information is sent to the lock controller using the "Add Temporary Users" command. If any field is left blank, the user will not be loaded into the lock. Credential info must exactly match the physical cards used for testing or temporary access.

Communications Users

Communications Users can be used to "wake up" a WiFi lock so that it will accept programming and transmit stored events. The information is sent to the lock controller using the "Add Comm Users" command. If any field is left blank, the user will not be loaded into the lock. Credential info must exactly match the physical cards used for waking the lock. Note: CSN is only required for locks that are set for CSN.

Firmware

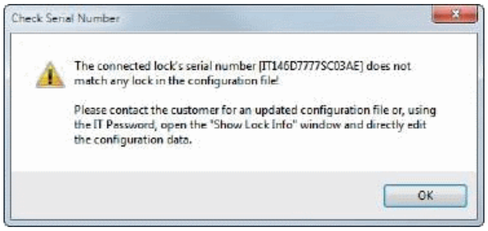
It is recommended that firmware is copied from the installation CD (or **io.com**) and copied to a local folder on the installation/configuration laptop. Once the full path to a valid firmware file is entered, or one is located using the **Browse** option, the file is scanned to extract the version number and the path is stored internally. The original file must remain in this location.

Configuring the Lock

Connect to the Lock

Selecting **Connect to Lock,** after connecting the laptop to the lock controller, establishes the initial communication session with the lock controller and verified its identity vis the serial number.

If the lock serial number does not match any of the locks defined in the Lock Configuration File, the following message will be displayed.

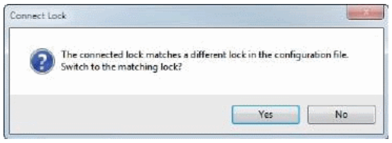


Check Serial Number

The connected lock's serial number [IT146D7777SC03AE] does not match any lock in the configuration file!

Please contact the customer for an updated configuration file or, using the IT Password, open the "Show Lock Info" window and directly edit the configuration data.

If the lock serial number does not match the currently displayed lock controller but does match another lock defined in the configuration file, the following message is displayed.

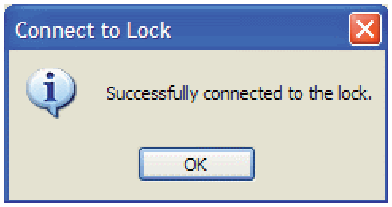


Connect Lock

The connected lock matches a different lock in the configuration file. Switch to the matching lock?

Select **Yes** to switch to the lock controller information matching the connected lock.

Once the connected lock correctly matches the serial number of the displayed lock, the following message is displayed, and lock configuration can proceed.

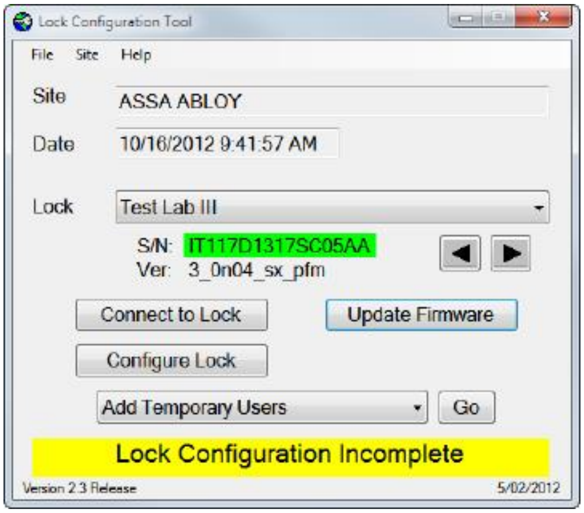


Successfully connected to the lock.

The controller must be connected to a reader to properly configure a lock. If a battery powered controller must be disconnected from its reader for any reason, at least one battery should be removed to prevent battery drain while disconnected from the reader.

Update Firmware

Select **Update Firmware** from the LCT main screen if a firmware update is required.



Site ASSA ABLOY

Date 10/16/2012 9:41:57 AM

Lock Test Lab III

S/N: IT117D1317SC05AA

Ver: 3_0n04_sx_pfm

Lock Configuration Incomplete

Version 2.3 Release 5/02/2012

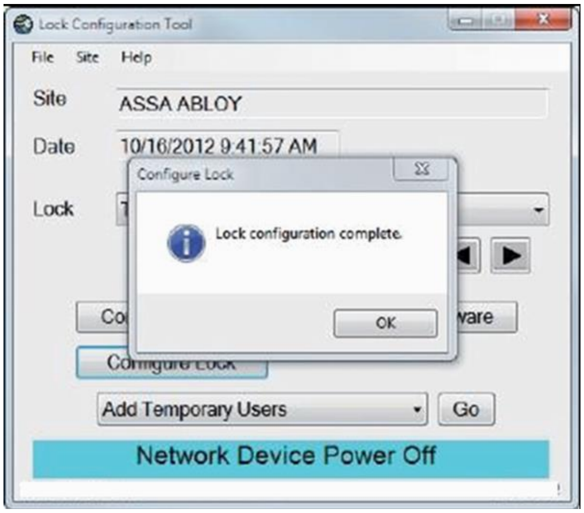
Configure Lock

The lock is ready to receive the network communication parameters once the latest firmware has been loaded.

An active network connection can be used for lock configuration if one is available to the lock controller either via WiFi or direct connection. Enable the "Verify DHCP" checkbox; if a network connection is active, it can be used.

Select **Configure Lock**.

The following confirmation will be displayed once lock configuration is successfully completed.



ASSA ABLOY

10/16/2012 9:41:57 AM

Lock configuration complete.

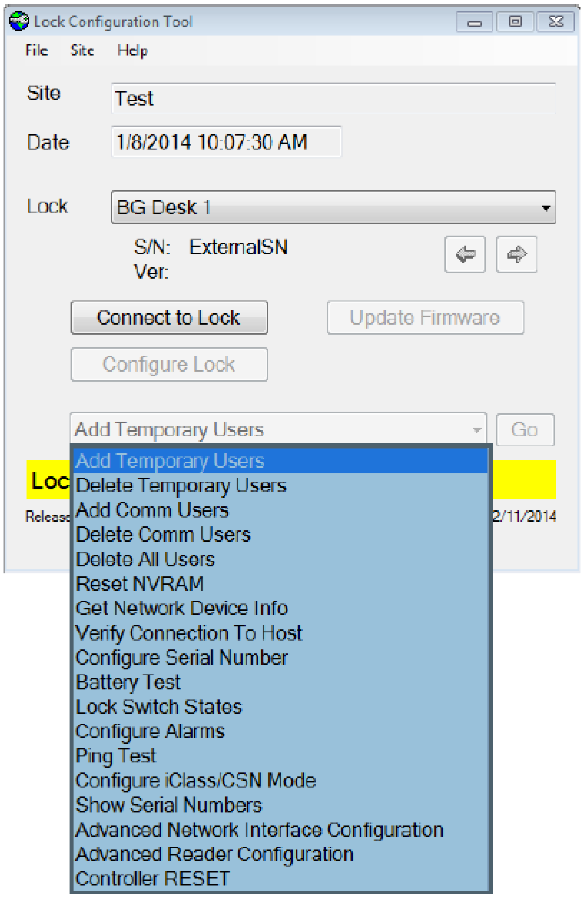
Network Device Power Off

Additional Commands for WiFi Locks

Immediately above the status message is a drop-down menu of additional commands that can be used to further configure the lock controller for testing.

These commands can be issued one-at-a-time by selecting the command from the menu and clicking **Go**.

A full list of command which may be available (*depending on the specific lock)* is shown below.



Site: Test

Date: 1/8/2014 10:07:30 AM

Lock: BG Desk 1

S/N: ExternalSN

Ver:

Add Temporary Users

Downloads any configured Temporary Users to the lock controller. SMS will overwrite these users on successful connection.

Delete Temporary Users

Deletes the set of Temporary Users downloaded to the lock using the "Add Temporary Users" command.

Add Comm Users

Downloads any configured Communication Users to the lock controller. SMS will overwrite these users on successful connection.

Delete Comm Users

Deletes the set of Communication Users downloaded to the lock using the "Add Comm Users" command.

Delete All Users

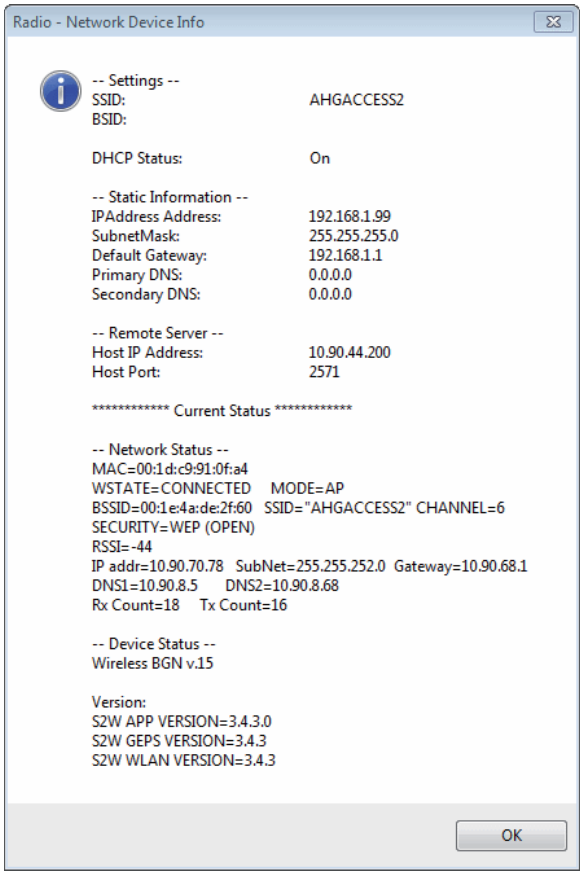
Deletes all users currently configured in the lock controller. Particularly useful if the lock had previously been configured and must be wiped for reconfiguration.

Reset NVRAM

Removes / cleans ALL types of configuration data. Useful to setting the lock back to the factory default configuration state.

Get Network Device Info for WiFi Locks

Collects and displays useful diagnostic communications information directly from the 802.11 compliant network device configured within the lock.

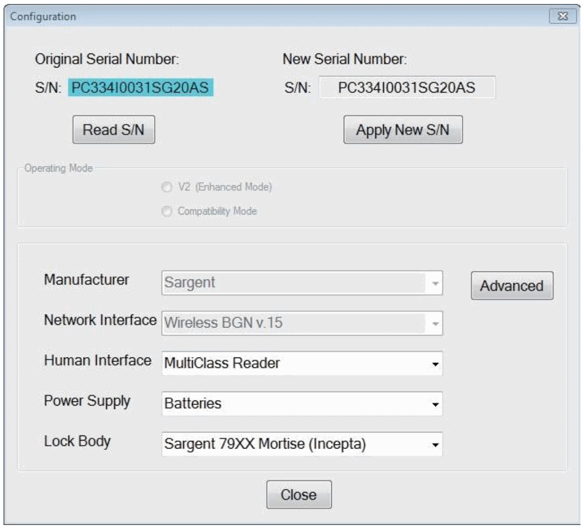


Radio - Network Device Info

```
-- Settings --
SSID:                        AHGACCESS2
BSID:

DHCP Status:                 On

-- Static Information --
IPAddress Address:           192.168.1.99
SubnetMask:                  255.255.255.0
Default Gateway:             192.168.1.1
Primary DNS:                 0.0.0.0
Secondary DNS:               0.0.0.0

-- Remote Server --
Host IP Address:             10.90.44.200
Host Port:                   2571

************ Current Status ************

-- Network Status --
MAC=00:1d:c9:91:0f:a4
WSTATE=CONNECTED    MODE=AP
BSSID=00:1e:4a:de:2f:60   SSID="AHGACCESS2" CHANNEL=6
SECURITY=WEP (OPEN)
RSSI=-44
IP addr=10.90.70.78   SubNet=255.255.252.0   Gateway=10.90.68.1
DNS1=10.90.8.5      DNS2=10.90.8.68
Rx Count=18     Tx Count=16

-- Device Status --
Wireless BGN v.15

Version:
S2W APP VERSION=3.4.3.0
S2W GEPS VERSION=3.4.3
S2W WLAN VERSION=3.4.3
```

Configure Serial Number

Allows custom specification of the last six characters of a lock's serial number. This capability offers greater flexibility (*in refining controller type*) in the field.



Configuration

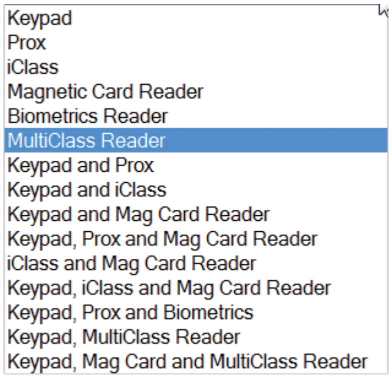
Original Serial Number:
S/N: PC334I0031SG20AS

New Serial Number:
S/N: PC334I0031SG20AS

Manufacturer: Sargent
Network Interface: Wireless BGN v.15
Human Interface: MultiClass Reader
Power Supply: Batteries
Lock Body: Sargent 79XX Mortise (Incepta)

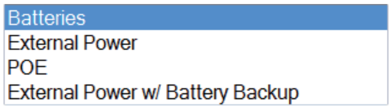
Human Interface

Use to select the reader / credential input options for the lock.


Keypad
Prox
iClass
Magnetic Card Reader
Biometrics Reader
MultiClass Reader
Keypad and Prox
Keypad and iClass
Keypad and Mag Card Reader
Keypad, Prox and Mag Card Reader
iClass and Mag Card Reader
Keypad, iClass and Mag Card Reader
Keypad, Prox and Biometrics
Keypad, MultiClass Reader
Keypad, Mag Card and MultiClass Reader

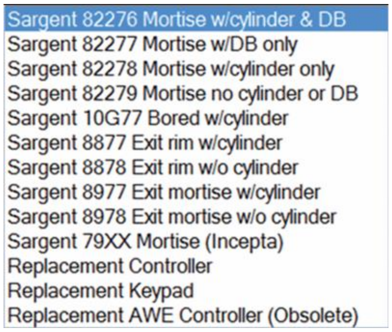
Power Supply

Use to specify the lock power source (with or without backup). Used to indicate when a WiFi lock is powered externally.

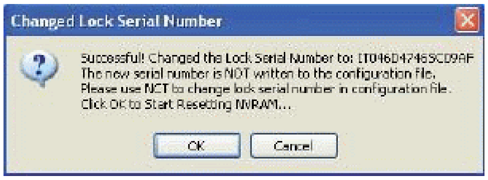


Lock Body

Use to specify the locking device including lock specific options.


Sargent 82276 Mortise w/cylinder & DB
Sargent 82277 Mortise w/DB only
Sargent 82278 Mortise w/cylinder only
Sargent 82279 Mortise no cylinder or DB
Sargent 10G77 Bored w/cylinder
Sargent 8877 Exit rim w/cylinder
Sargent 8878 Exit rim w/o cylinder
Sargent 8977 Exit mortise w/cylinder
Sargent 8978 Exit mortise w/o cylinder
Sargent 79XX Mortise (Incepta)
Replacement Controller
Replacement Keypad
Replacement AWE Controller (Obsolete)

Applying a new Lock Body may change the lock serial number in the LCT (not in the configuration file).



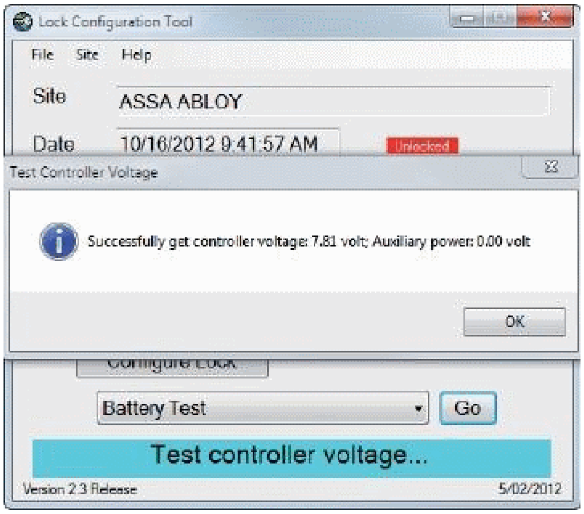
Successful! Changed the Lock Serial Number to: IT046D47465CD9AF
The new serial number is NOT written to the configuration file.
Please use NCT to change lock serial number in configuration file.
Click OK to Start Resetting NVRAM...

Battery Test

Use to retrieve lock's real-time battery voltage as well as auxiliary (hard-powered) voltage.

Issuing this command for PoE locks will report the auxiliary voltage as the controller's on-board voltage, not the 48V network voltage.

- WiFi with batteries and hard powered, measures and reports AUX voltage = 9 volts
- PoE with no batteries, measures and reports AUX voltage = 9 volts



Site ASSA ABLOY

Date 10/16/2012 9:41:57 AM

Successfully get controller voltage: 7.81 volt; Auxiliary power: 0.00 volt

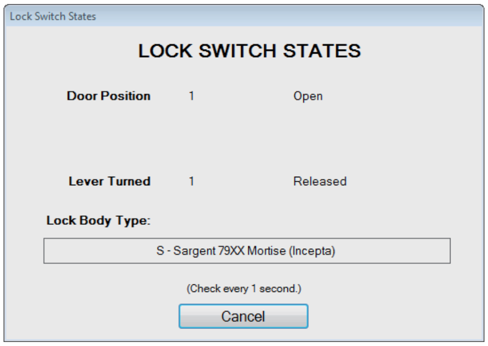
Battery Test

Test controller voltage...

Lock Switch States

Use to display the various switch states to allow confirmation that the lock switch monitoring is functioning properly.

- All switches should report a value of 1 when door is closed.
- The LCT display may take up to 2 seconds to update if a switch is held.



LOCK SWITCH STATES

Door Position	1	Open
Lever Turned	1	Released

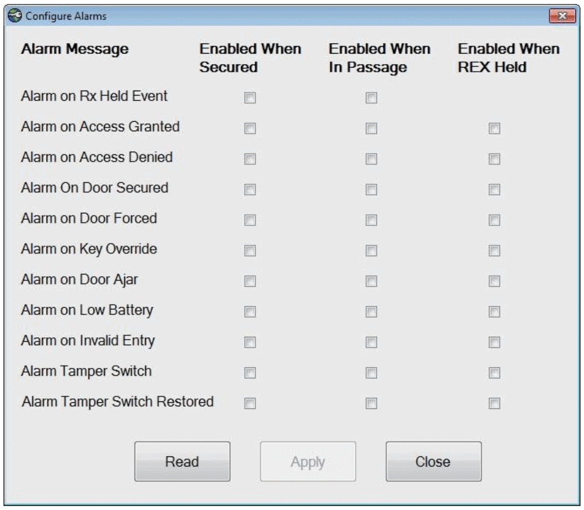
Lock Body Type:

S - Sargent 79XX Mortise (Incepta)

(Check every 1 second.)

Configure Alarms

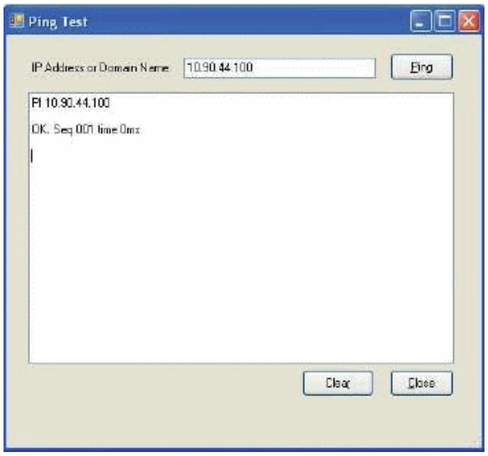
Use to select / deselect alarms. **Note:** Selecting "Configure Lock" sets all alarms to "off"



Alarm Message	Enabled When Secured	Enabled When In Passage	Enabled When REX Held
Alarm on Rx Held Event	□	□	
Alarm on Access Granted	□	□	□
Alarm on Access Denied	□	□	□
Alarm On Door Secured	□	□	□
Alarm on Door Forced	□	□	□
Alarm on Key Override	□	□	□
Alarm on Door Ajar	□	□	□
Alarm on Low Battery	□	□	□
Alarm on Invalid Entry	□	□	□
Alarm Tamper Switch	□	□	□
Alarm Tamper Switch Restored	□	□	□

Ping Test

Use to confirm communications between the lock controller IP address and the host computer IP address (*PoE locks only*).



IP Address or Domain Name: 10.90.44.100

```
PI 10.90.44.100
OK, Seq 001 time 0ms
```

Configure iClass / CSN Mode

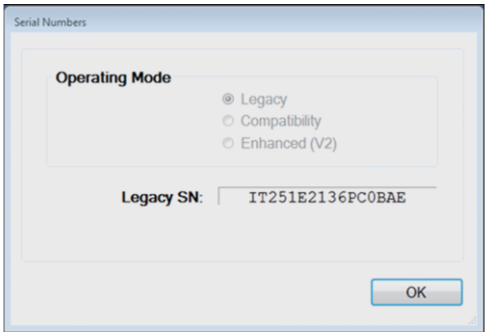
Use to configure one of the following Smart Card Reader Mode settings:

- iClass Application Data
- iClass CSN / Felica CSN
- Mifare CSN
- DesfFire CSN

iClass Only. Does NOT apply to multiCLASS locks

Show Serial Numbers

Use to display the lock reported Serial Number



Serial Numbers

Operating Mode

● Legacy
○ Compatibility
○ Enhanced (V2)

Legacy SN: IT251E2136PC0BAE

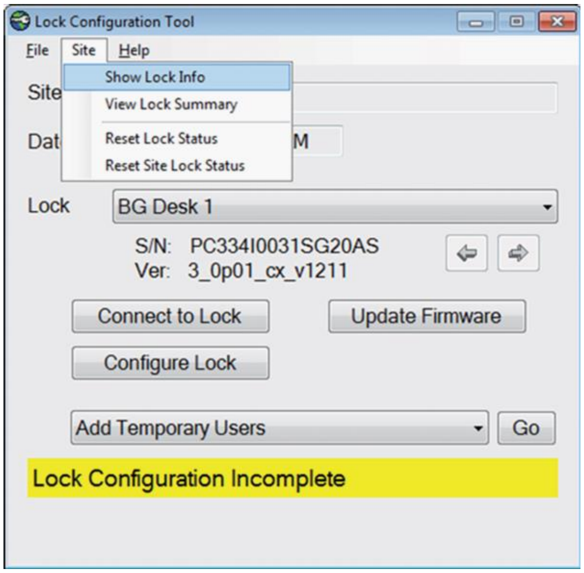
Operating Mode

Use to configure at least one of the three displayed modes:

- Legacy: non-multiCLASS controllers; controllers without privacy or tamper
- Compatibility: Serial Number used to preserve backwards compatibility with OEM systems of multiCLASS lockset
- *Internal: controller's Serial Number on multiCLASS devices. Serial Number configured here or the Compatibility Serial Number may be used by OEMs to identify the controller / lockset.

Show Lock Info

Use to view or edit the lock controller parameters if required during configuration. Select **Site** --> **Show Lock Info**.

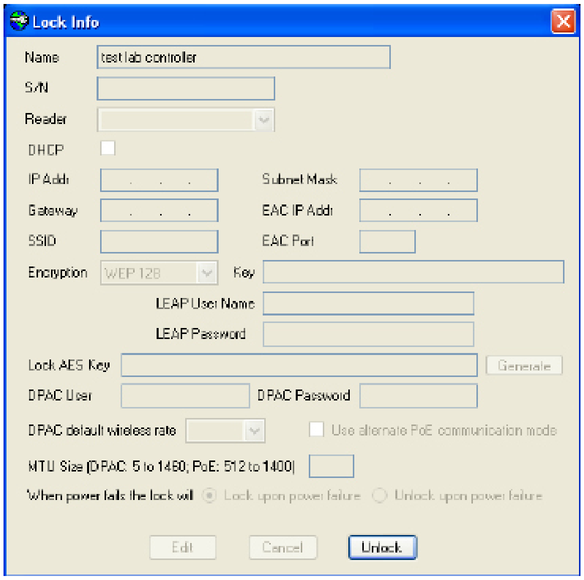


Lock: BG Desk 1

S/N: PC334I0031SG20AS
Ver: 3_0p01_cx_v1211

Add Temporary Users

Lock Configuration Incomplete



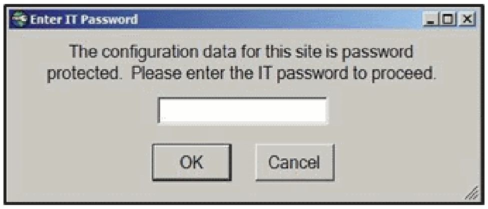
Name: test lab controller

Encryption: WEP 128

When power fails the lock will ● Lock upon power failure

The Name field is the only field editable without unlocking the application with the IT password.

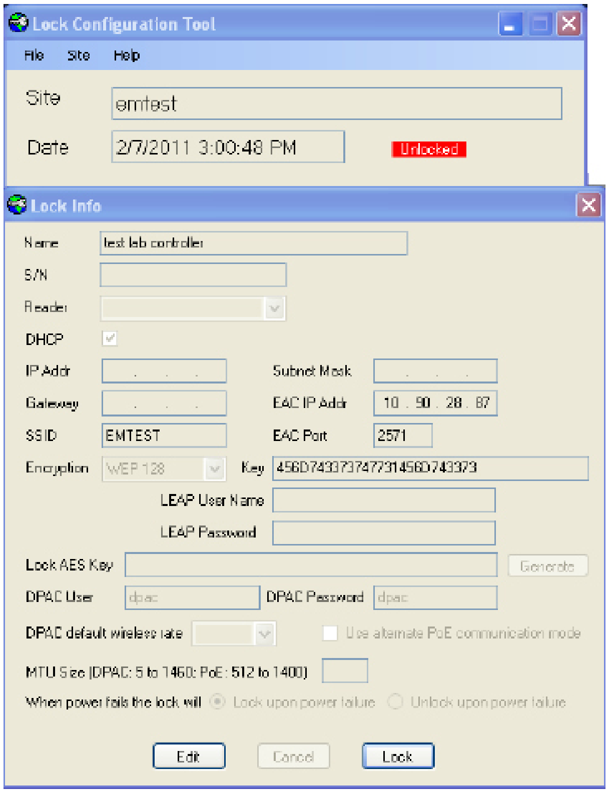
Click **Unlock** to enter the IT password.



The configuration data for this site is password protected. Please enter the IT password to proceed.

The LCT will display "Unlocked" in red once the IT password has been entered. Lock parameters may now be modified.

Selecting the **Lock** button will return the LCT to the secured state, requiring re-entry of the IT password for further editing.

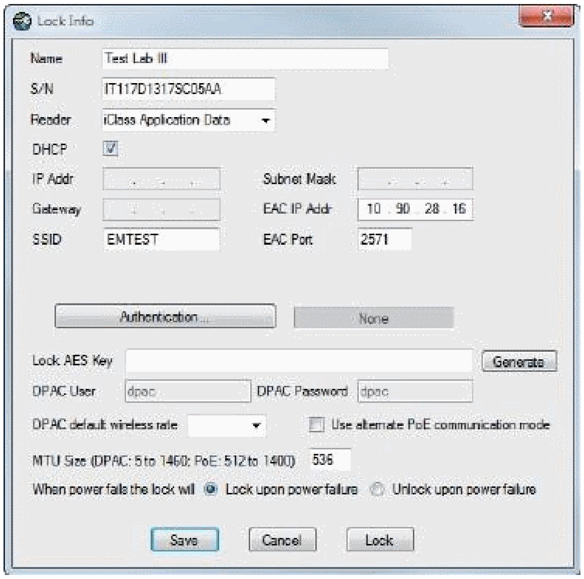


Site: emtest
Date: 2/7/2011 3:00:48 PM
Unlocked

Name: test lab controller
S/N:
Reader:
DHCP: ☑
IP Addr: . . .
Subnet Mask: . . .
Gateway: . . .
EAC IP Addr: 10 . 90 . 28 . 87
SSID: EMTEST
EAC Port: 2571
Encryption: WEP 128
Key: 456D74337374773145 6D743373
LEAP User Name:
LEAP Password:
Lock AES Key:
DPAC User: dpac
DPAC Password: dpac
DPAC default wireless rate:
□ Use alternate PoE communication mode
MTU Size (DPAC: 5 to 1460: PoE: 512 to 1400):
When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

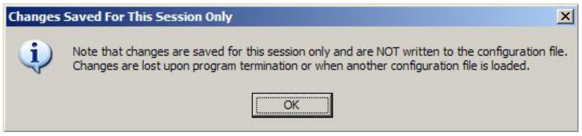
Click the **Edit** button to enable editing of all fields. **Edit** will change to **Save**.

Modifications are only stored during the current configuration session.



Name: Test Lab III
S/N: IT117D1317SC05AA
Reader: iClass Application Data
DHCP: ☑
IP Addr: . . .
Subnet Mask: . . .
Gateway: . . .
EAC IP Addr: 10 . 90 . 28 . 16
SSID: EMTEST
EAC Port: 2571
Lock AES Key:
DPAC User: dpac
DPAC Password: dpac
DPAC default wireless rate:
□ Use alternate PoE communication mode
MTU Size (DPAC: 5 to 1460: PoE: 512 to 1400): 536
When power fails the lock will ● Lock upon power failure ○ Unlock upon power failure

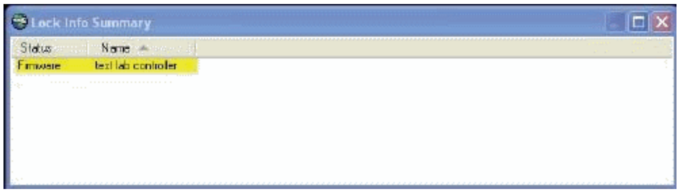
Click **Save** to commit the changes for the current session. A dialog confirming that the changes are temporary will be displayed.



Note that changes are saved for this session only and are NOT written to the configuration file. Changes are lost upon program termination or when another configuration file is loaded.

View Lock Summary

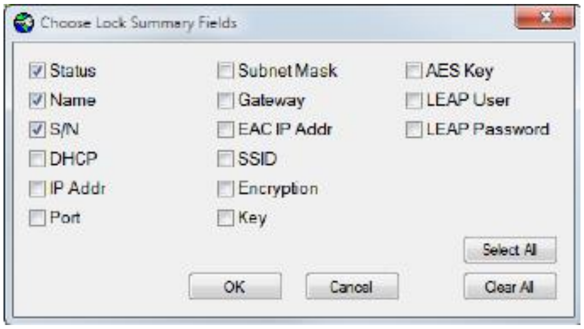
Displays the Lock Info Summary windows which provides a quick means to review the configuration status of all locks defined in the configuration file.



Status	Name
Firmware	test lab controller

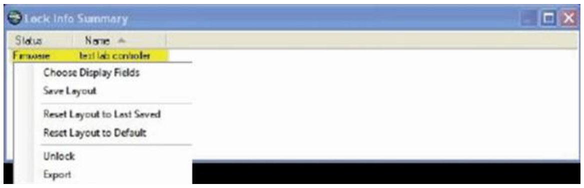
The Lock Info Summary window supports a context menu (right-click anywhere in the window) with the following options.

- **Choose Display Fields** - select columns to display in the Lock Info Summary screen

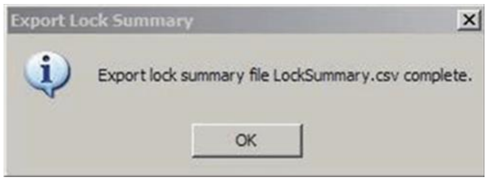


☑ Status
☑ Name
☑ S/N
□ DHCP
□ IP Addr
□ Port
□ Subnet Mask
□ Gateway
□ EAC IP Addr
□ SSID
□ Encryption
□ Key
□ AES Key
□ LEAP User
□ LEAP Password

- **Save Layout** - saves the current View Lock Summary window configuration (columns, column width, window size)
- **Reset Layout to Last Saved** - restores the last saved View Lock Summary window configuration
- **Reset Layout to Default** - restores the default View Lock Summary window configuration
- **Unlock** - displays all lock information (*those configured under Choose Display Fields*) after the IT Password is provided



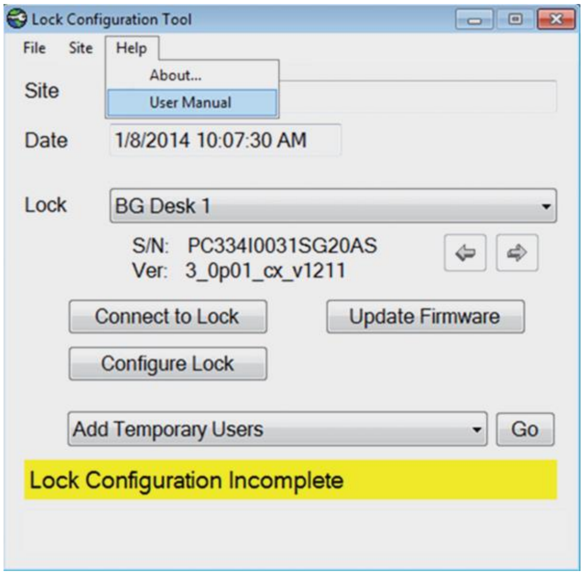
- **Export** - creates "c:\Program Files\Assa Abloy\AHG\Lock Configuration Tool\LockSummary.csv" which can be viewed/editing using Excel.



Export lock summary file LockSummary.csv complete.

Help

Opens the "Network & Lock Configuration Tool User Manual". Select **Help** --> **User Manual**.



Site

Date 1/8/2014 10:07:30 AM

Lock BG Desk 1

S/N: PC334I0031SG20AS
Ver: 3_0p01_cx_v1211

Add Temporary Users

Lock Configuration Incomplete

IP-Enabled Lock Components

IP-Enabled Locks

IN120 (WiFi)

The IN120 WiFi (CX based) local decision (offline) lock offers the ease and flexibility of WiFi in a streamlined design. The IN120 leverages the existing IT network infrastructure to reduce cost and complexity.

Features

- Utilizes IEEE 802.11b/g/n WiFi infrastructure
- HID® multiCLASS SE™ Technology
- Intelligence built into lock for local decision making
- Privacy button
- Field selectable communication frequency

- Integrated ANSI/BHMA Grade 1 hardware available in cylindrical and mortise lock configurations
- Available with a wide range of finishes and decorative levers

Benefits

- Ideal for hard-to-wire locations
- Significantly reduces installation costs
- Supports Multiple credential types
- Lock operates regardless of network status
- Supports up to 2,400 users per lock
- Local lockdown capabilities
- Intelligence built into lock for local decision making
- High quality hardware from Corbin Russwin and Sargent

Sargent Passport 1000 P1 (PoE) / Corbin Russwin Access 700 PIP1 (PoE)

An online ANSI/BHMA Grade 1 lock utilizing Power over Ethernet (PoE) technology, these PX based local decision (offline) locks provide a cost-effective, future-proof solution for campuses. Featuring HID® multiCLASS SE™ technology, they provide simultaneous support for multiple credentials and offers an easy migration path to higher security credentials. Recognized for its contribution to sustainable buildings, the P1 re-uses existing IEEE 802.3af PoE infrastructure, streamlines the installation process, reduces costs and components, and minimizes power consumption. The Access 700 PIP1 also integrates all standard access control components into one device - ANSI /BHMA Grade 1 quality lock or exit device, card reader, door position switch and Request-to-Exit sensor - and is available in mortise lock, cylindrical lock and exit device configurations.

Features

- Utilizes IEEE 802.3af PoE enabled network infrastructure for power and data
- HID® multiCLASS SE™ Technology with magnetic stripe reader
- Intelligence built into lock for local decision making
- Privacy button
- Field selectable communication frequency
- Keypad options available
- Integrated ANSI/BHMA Grade 1 hardware available in cylindrical, mortise lock and exit device configurations
- Available with a wide range of finishes and decorative levers

Benefits

- Ideal for hard-to-wire locations
- Significantly reduces installation costs
- Supports Multiple credential types
- Lock operates regardless of network status
- Two-facto authentication offers enhanced security
- Supports up to 2,400 users per lock
- Local lockdown capabilities
- Intelligence built into lock for local decision making
- High quality hardware from Corbin Russwin and Sargent

Sargent Profile Series v.S1 (PoE) / Corbin Russwin Access 800 IP1 (PoE)

The SX based Profile Series v.S1/Corbin Russwin Access 800 IP1 locks bring the power of your network to your door hardware. ANSI/BHMA Grade 1 locks utilizing Power over Ethernet (PoE) technology, these locks connect to the building's Ethernet network, and make decisions locally (offline). Non-proprietary cable, PoE switches and midspans allow easy and cost-effective installations. Supporting real-time door status monitoring and alarm notification, these locks are available in exit device, mortise and cylindrical lock configurations.

Features

- Utilizes IEEE 802.3af PoE enabled network infrastructure for both power and data (class 2 device)
- Supports HID® 125 kHz prox or 13.56 MHz iCLASS® credentials (26 - 39 bit); supports CSN reads for other common 13.56 MHz cards, including MiFare.
- Intelligence built into lock for local decision making
- Privacy button
- Field selectable communication frequency
- Keypad options available
- Integrated ANSI/BHMA Grade 1 hardware available in cylindrical and mortise lock configurations
- Available with a wide range of finishes and decorative levers

Benefits

- Ideal for hard-to-wire locations, Significantly reduces installation costs
- Supports Multiple credential types
- Lock operates regardless of network status
- Two-factor authentication offers enhanced security
- Supports up to 2,400 users per lock
- Local lockdown capabilities
- Intelligence built into lock for local decision making
- High quality hardware from Corbin Russwin and Sargent

Sargent Passport P1000 P2 (WiFi) / Corbin Russwin Access 700 PWI1 & 800 WI1 (WiFi)

ANSI/BHMA Grade 1 local decision (offline) locks using WiFi technology, these locks provide a cost effective, future-proof solution for campuses. Featuring HID® multiCLASS SE® technology, they provide simultaneous support for multiple credentials and offer an easy migration path to higher security credentials. Installation is fast, easy and affordable with no wiring required.

Features

- Utilizes IEEE 802.11 WiFi infrastructure
- HID multiclass SE® Technology with magnetic stripe reader (keypad options available)
- Intelligence built into lock for local decision making
- Field-upgradeable 802.11b/g/n radio
- Privacy button
- Integrated ANSI/BHMA Grade 1 hardware available in cylindrical, mortise and exit device configurations
- Available with a wide range of finishes and decorative levers

Benefits

- Ideal for hard-to-wire locations, significantly reduces installation costs
- Supports Multiple credential types (available two-factor authentication offers enhanced security)

- Lock operates regardless of network status
- Supports up to 2,400 users per lock/10,000 event transaction history
- Local lockdown capabilities
- Intelligence built into lock for local decision making
- High quality hardware from Corbin Russwin and Sargent

CHAPTER 27

Schlage Adaptable AD-400 Series Wireless Locks

Schlage Adaptable AD-400 Series Lock

Overview

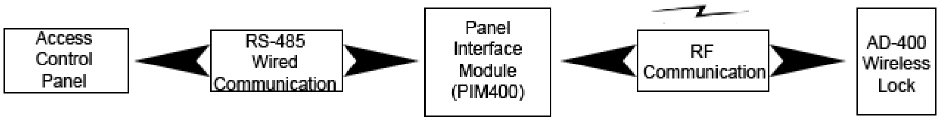
Schlage wireless devices can be seamlessly integrated with the SMS system. The PIM400-485-SMS communicates directly to the VRCNX-R/M/A, VSRC-400 or VMRC-1/2 via RS-485 protocol and can support up to 16 Schlage AD-400 Series locks. Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Note: For the PIM400 to communicate with the VRCNX-R, the VCRNX-R must have firmware v5.92 or higher installed.

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-SMS) is hard wired to the reader controller (VRCNX-R/M/A or VSRC-400) 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-SMS)

The PIM400-485-SMS works in conjunction with the AD-400 Locks. The PIM400-485-SMS module is hard wired directly to the VRCNX-R/M/A or VSRC-400 reader controller communication channels and communicates via RS-485 protocol. The PIM400-485-SMS can support up to 16 AD-400 locks.

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-SMS 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 Must use external power supply
  (*cannot be powered from VRCNX-R/M/A*)

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

Specifications for the PIM400-485-SMS

- RS-485 Communication to VRCNX-R/M/A or VSRC-400 reader controller
- Supports 16 Wireless Devices
- VRCNX-R can support multiple PIM400-485-SMS

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 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 the reader controller (VRCNX-R/M/A, VSRC-400, VMRC-1/2 or SRCNX-Legacy).

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 Lock-out 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. These locksets are controlled by the Vanderbilt Security Management System (SMS).

Internal Push Button (IPB) - If the AD-400 lock is defined in SMS as having an IPB function (either LockDown or Toggle) this button activates that option (see the SMS Software Manual for details).

Toggle LED - When the IPB is used as a Toggle switch the LED will flash depending on the state of the lock. (Only if running firmware V2.1.7 or higher. Lower firmware versions will have full IPB functionality, but the LED will not respond.)

- In Toggle - 4 green flashes
- Out of Toggle - 1 red flash

LockDown LED - When the IPB is used as a LockDown switch the LED will flash depending on the state of the lock. (Only if running firmware V2.1.7 or higher. Lower firmware versions will have full IPB functionality, but the LED will not respond.)

- In Lockdown - 4 red flashes
- Out of Lockdown - 1 red flash

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 4.3 volts before we get Low Battery.

  - At 4.1 volts we get battery critical at which point the lock 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): 4VDC to 26 VDC
- Current Requirements: Standby: 55 micro Amps typical (Proximity version)
- Maximum: 250ma peak (transmitting)
- 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 via RF with the VRCNX-R/M/A, VMRC-1/2, VSRC-400, or SRCNX (Legacy) reader controller, through a mating Panel Interface Module (PIM400-485-SMS). 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 10 seconds for ARO and MRO 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

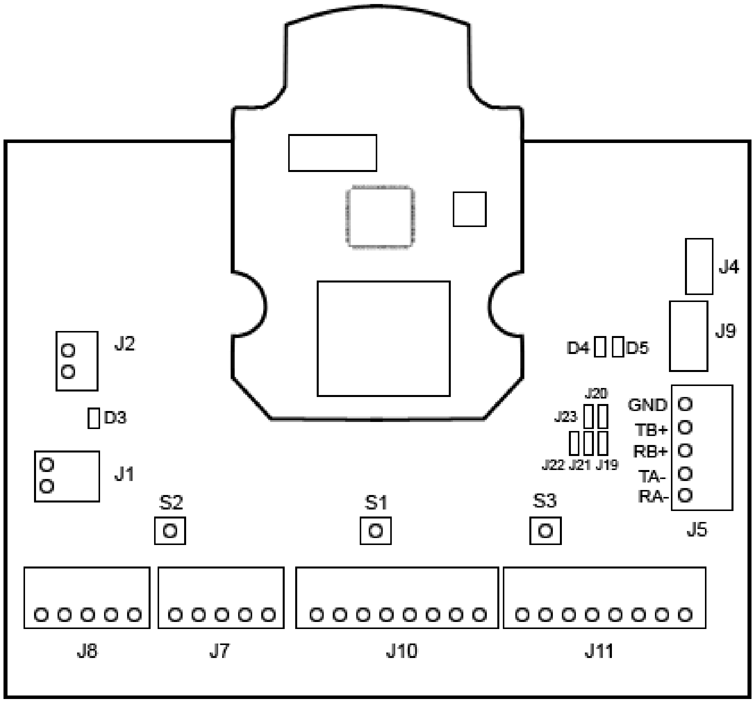
Power source

- 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 and the expansion modules (PIM EXP) are capable of accommodating Remote Antenna Modules.

Wiring Instructions



All Schlage wireless devices should be powered separately with a 12VDC power supply. They cannot be powered from the VRCNX-R/M/A, VSRC-400 or VMRC-1/2. Communication between the VRCNX-R/M/A, VSRC-400 or VMRC-1/2 reader controller and the PIM400-485-SMS is via RS-485 protocol.

Wiring between Controller and PIM400

VRCNX-R/M/A to PIM400-485-SMS

VRCNX-R/M/A J4 – J11	PIM400-485-SMS J5
RXD (A)	RA-
TXD (B)	RB+

Note: A jumper is required at J19 and J20 of the PIM400.

VSRC-400 to PIM400-485-SMS

VSRC-400 P2	PIM400-485-SMS J5
Pin 1 (CLK) = Data B	RB+
Pin2 (DAT) = Data A	RA-

Note: A jumper is required at J19 and J20 of the PIM400.

VMRC-1/2 to PIM400-485-SMS

VMRC-1 / 1L	VMRC-2 / 2L	PIM400-485-SMS J5
TB2-4 (TR+)	TB3-3 (TR+)	RB+
TB2-5 (TR-)	TB3-2 (TR-)	RA-

Note: A jumper is required at J19 and J20 of the PIM400.

PIM400 Configuration

The Schlage Utility Software (SUS) located on the included HHD (Hand Held Device) must be used to configure each PIM400-485-SMS. 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.

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 HHD. Follow the steps below to log in:

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

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

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 HHD

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

1 Log in to SUS (see steps above).

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

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

4 Put the PIM400 into **Pairing Mode** (this is necessary for the HHD 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 HHD 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 HHD once. After pairing the PIM400 and HHD will communicate whenever connected.

Set PIM400 Address

The SUS is used to set the address of the PIM. 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. SMS uses 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 in SMS. Also, 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 SMS, the PIM400 will be addressed as 1 (0+1=1) and the AD-400 locks will be addressed as 1 through 8.

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 have 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 SMS, this PIM400 will be addressed at 9 and the AD-400 locks communicating with it will be addressed from 9 through 14.

SMS Address	SUS Address
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

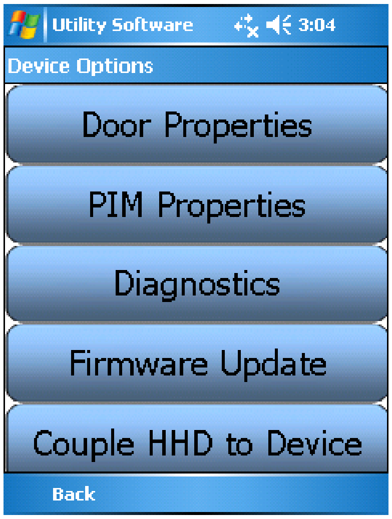
SMS Address	SUS Address
9	8
10	9
11	10
12	11
13	12
14	13
15	14
16	15

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).

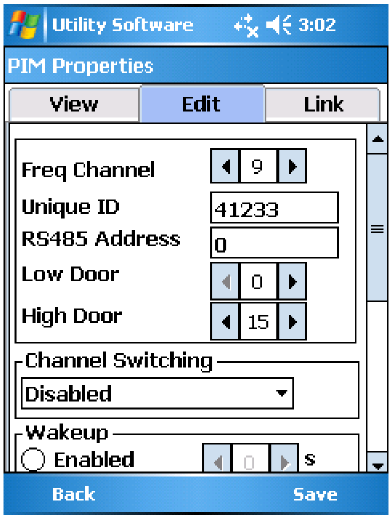
2 Connect the HHD to the PIM400 using the supplied USB cable.

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



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

5 Click the **Edit** tab.



Freq Channel 9

Unique ID 41233

RS485 Address 0

Low Door 0

High Door 15

Channel Switching: Disabled

Wakeup: ○ Enabled 0 s

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 HHD 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 HHD. A Menu will open with a list of programs.

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

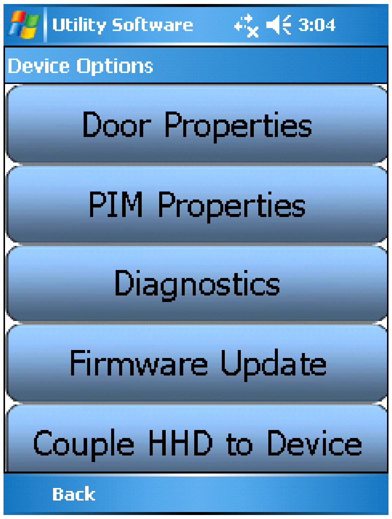
3 Select **Manager** from the **Log on as** drop-down menu.

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.**

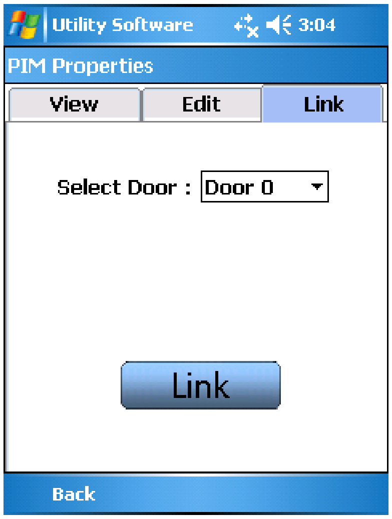
6 Connect the HHD to the PIM400 using the supplied USB cable.

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



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

9 Go to the **Link** tab.



Select Door : Door 0

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 Click **Stop** on the SUS. The AD-400 is now linked to this PIM400 with the specified address.

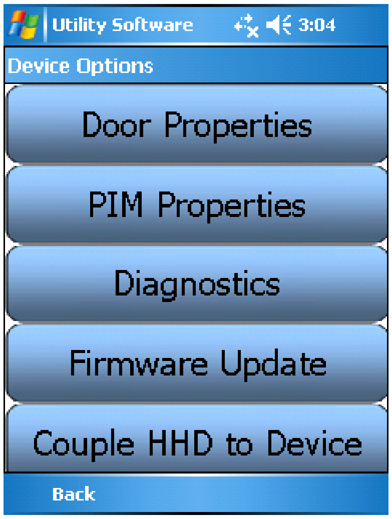
Diagnostics

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

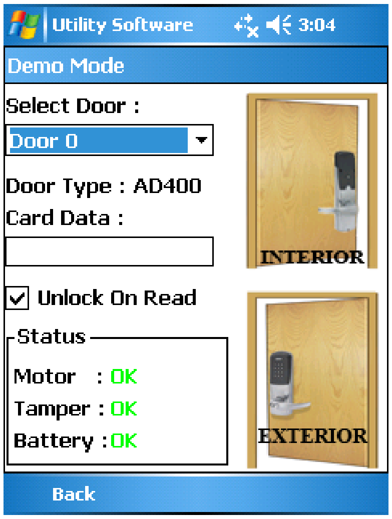
1 Log in to SUS (see steps above).

2 Connect the HHD 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.



Select Door : Door 0

Door Type : AD400

Card Data :

☑ Unlock On Read

Status

Motor : OK

Tamper : OK

Battery : OK

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

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

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 it 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.

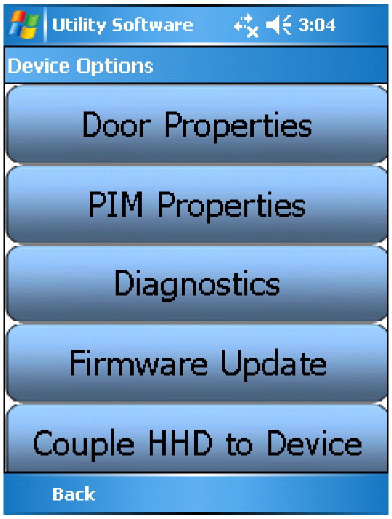
Coupling with the HHD

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. **SUS** will open.
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.

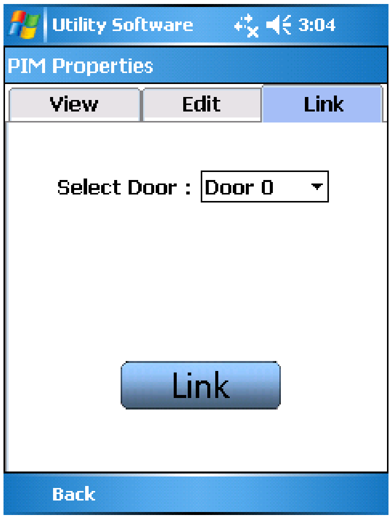


Utility Software 3:04

Device Options

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

9 Go to the **Link** tab.



Utility Software 3:04

PIM Properties

Select Door : Door 0

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). After a moment, **WRI400** will be displayed at the bottom of the screen.

4 You are now ready to configure the WRI400.

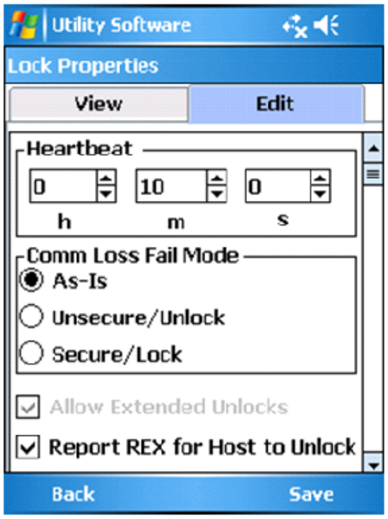
Configure Heartbeat

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

2 Click on **Lock Properties**.

3 Click on the **Edit tab**.

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



Heartbeat
0 h 10 m 0 s

Comm Loss Fail Mode
● As-Is
○ Unsecure/Unlock
○ Secure/Lock

☑ Allow Extended Unlocks

☑ Report REX for Host to Unlock

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

6 Click **Save**.

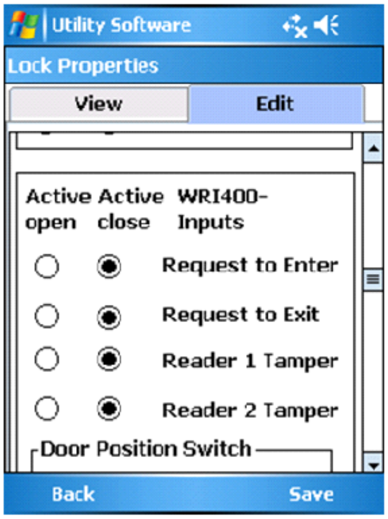
Configure Request to Exit

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

2 Click on **Lock Properties**.

3 Click on the **Edit tab**.

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



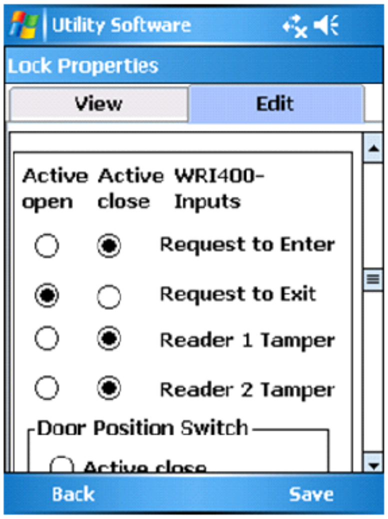
Lock Properties

Active open	Active close	WRI400-Inputs
○	●	Request to Enter
○	●	Request to Exit
○	●	Reader 1 Tamper
○	●	Reader 2 Tamper

Door Position Switch

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:



Lock Properties

Active open	Active close	WRI400-Inputs
○	●	Request to Enter
●	○	Request to Exit
○	●	Reader 1 Tamper
○	●	Reader 2 Tamper

Door Position Switch

○ Active close

Correct Configuration

6 Click **Save**.

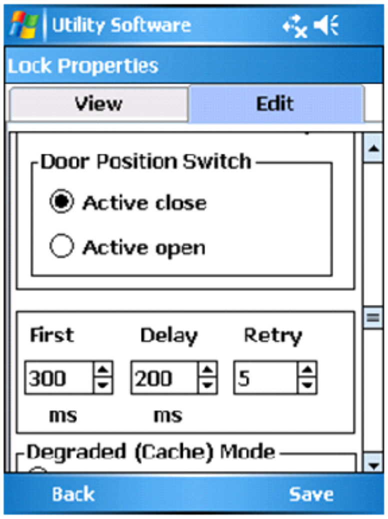
Configure Door Position Switch

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

2 Click on **Lock Properties**.

3 Click on the **Edit tab**.

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



Door Position Switch
● Active close
○ Active open

First 300 ms
Delay 200 ms
Retry 5

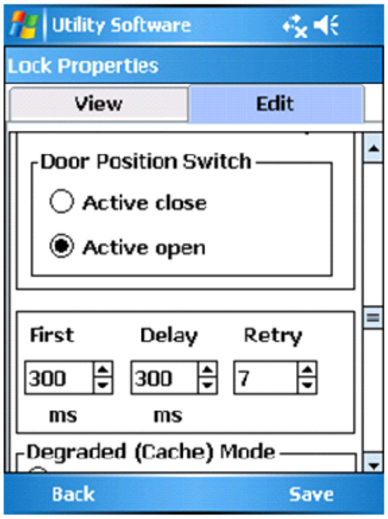
Degraded (Cache) Mode

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:



Door Position Switch
○ Active close
● Active open

First 300 ms
Delay 300 ms
Retry 7

Degraded (Cache) Mode

Correct Configuration

8 Click **Save**.

CHAPTER 28

Schlage NDE Series Wireless Locks with ENGAGE

Schlage NDE Series Wireless Lock with ENGAGE Technology

Overview

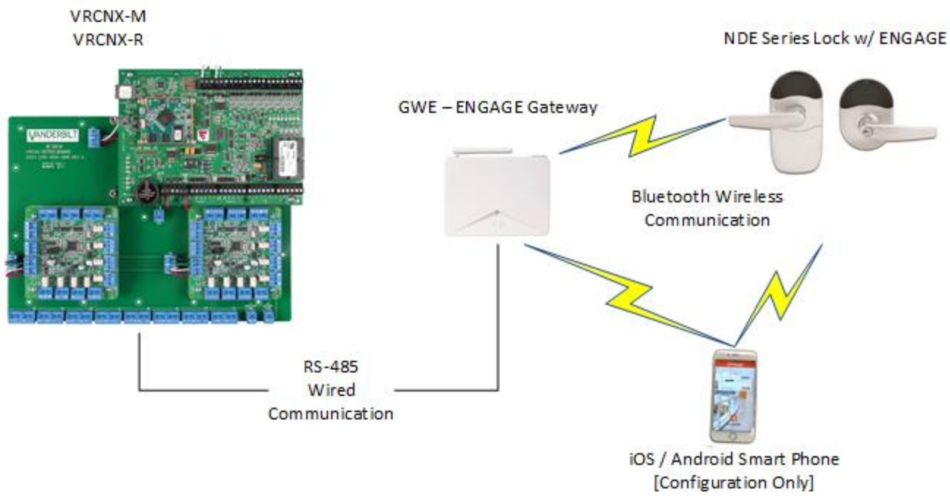
Schlage NDE Series wireless devices can be seamlessly integrated with the SMS system. The GWE – ENGAGE Gateway communicates directly to the VRCNX-R/M/A or VMRC-1/2 over RS-485 via RSI protocol and can support up to 10 Schlage NDE Series wireless locks with ENGAGE technology. Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Note: For the GWE – ENGAGE Gateway to communicate with the VRCNX-R/M, the VCRNX-R/M must have firmware v6.60V / v6.70M or higher installed.

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


VRCNX-M
VRCNX-R
NDE Series Lock w/ ENGAGE
GWE – ENGAGE Gateway
Bluetooth Wireless Communication
RS-485 Wired Communication
iOS / Android Smart Phone [Configuration Only]

The GWE – ENGAGE Gateway is hard wired to the reader controller (VRCNX-R/M/A or VMRC-1/2) 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 30 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 VRCNX-R/M/A reader 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/A*)

Specifications for the GWE – ENGAGE Gateway

- 2.4 GHz Bluetooth v4.0
- Spread spectrum
- Dynamic channel switching (40 channels)
- Range: Up to 30' line of site to door
- Gateway to Lock Encryption: AES 256-bit
- Certifications: UL294, FCC Part 15, Industry Canada (IC), RoHS
- RS-485 Communication to VRCNX-R/M/A
- 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 reader controller (VRCNX-R/M/A or VMRC-1/2) 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 30 feet line of site to door

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 Battery 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 Vanderbilt Security Management System (SMS).

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

- VRCNX-M/R/A powered 12 – 24 VDC
- GWE – ENGAGE Gateway powered by external 24 VDC power supply

VRCNX-M/R/A to GWE – ENGAGE Gateway

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

VRCNX-R/M/A J4 – J11	GWE – ENGAGE Gateway
RXD (A)	TX–
TXD (B)	TX+

VMRC-1/2 to GWE – ENGAGE Gateway

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

VMRC-1 / 1L	VMRC-2 / 2L	GWE – ENGAGE Gateway
TB2-4 (TR+)	TB3-3 (TR+)	TX+
TB2-5 (TR-)	TB3-2 (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. The address defined in the Gateway for the NDE locks ranges from 0 to 9. SMS uses an address of 1 through 10.

SMS Addresses Will Always Be 1 Value Higher than the Gateway and NDE Lock Address set via the ENGAGE iOS or Android app. An address of 0 for the Gateway and NDE lock translates to an address of 1 in SMS. Also, the 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). SMS configuration will require the Gateway address to be specified as 1 (0 in ENGAGE app + 1) and the NDE locks will be addressed in SMS as 1 through 5.

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 5 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 9.

Configure SMS to communicate with the 2nd Gateway at address 6 and the NDE locks communicating with it will be addressed from 6 through 10.

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.

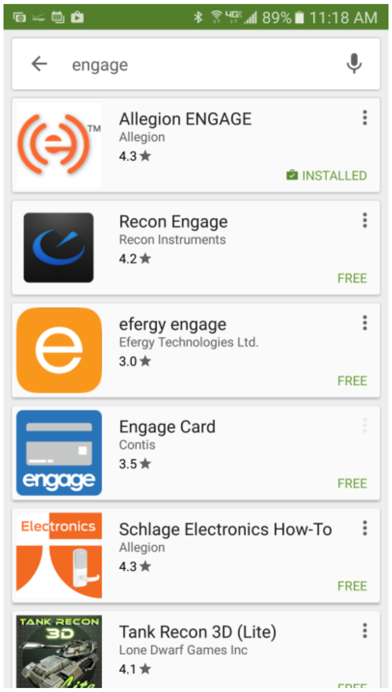
Vanderbilt will create an ENGAGE Site and forward an Invite via email which must be accepted prior to lock commissioning and configuration. Use the Vanderbilt provided ENGAGE account username (email address) and password in the ENGAGE Android or iOS mobile app as indicated below.

Download ENAGE app

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

Allegion provides frequent updates to the ENGAGE iOS and Android apps to improve usability and functionality. The screen images provided herein are for reference only and the functionality specified may appear differently on screen or under different pages than displayed below. If there is any difficulty locating the specified parameters which must be configured for SMS please contact Allegion Support at 888-671-7011.

Android



89% 11:18 AM

engage

Allegion ENGAGE
Allegion
4.3 ★
INSTALLED

Recon Engage
Recon Instruments
4.2 ★
FREE

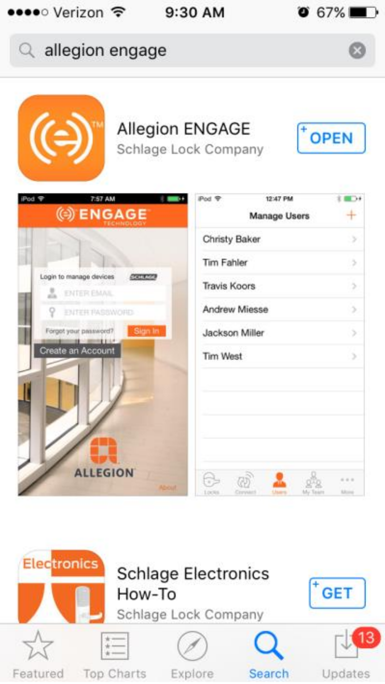
efergy engage
Efergy Technologies Ltd.
3.0 ★
FREE

Engage Card
Contis
3.5 ★
FREE

Schlage Electronics How-To
Allegion
4.3 ★
FREE

Tank Recon 3D (Lite)
Lone Dwarf Games Inc
4.1 ★

iOS



●●●●○ Verizon 9:30 AM 67%

allegion engage

Allegion ENGAGE
Schlage Lock Company
OPEN

ENGAGE
Login to manage devices
ENTER EMAIL
ENTER PASSWORD
Forgot your password? Sign In
Create an Account
ALLEGION

Manage Users
Christy Baker
Tim Fahler
Travis Koors
Andrew Miesse
Jackson Miller
Tim West

Schlage Electronics How-To
Schlage Lock Company
GET

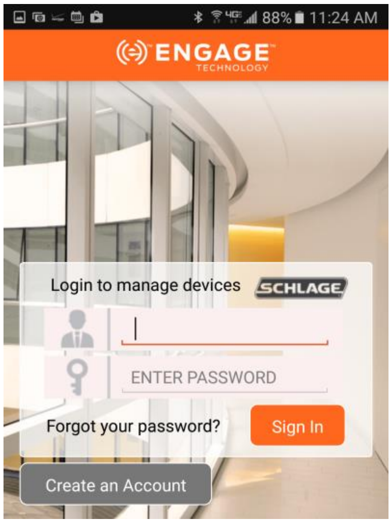
Featured Top Charts Explore Search Updates 13

- Click on the Allegion ENGAGE application
- Click Install

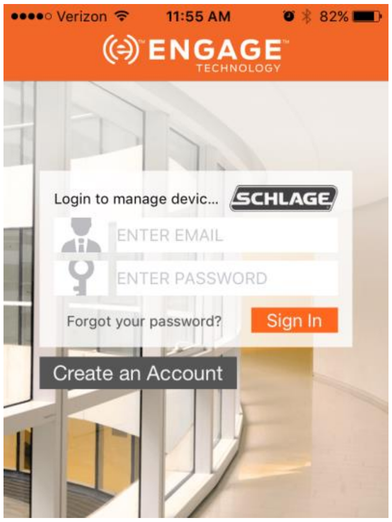
Commission / Configure GWE – ENGAGE Gateway

- Open the ENGAGE app on the mobile device

Android

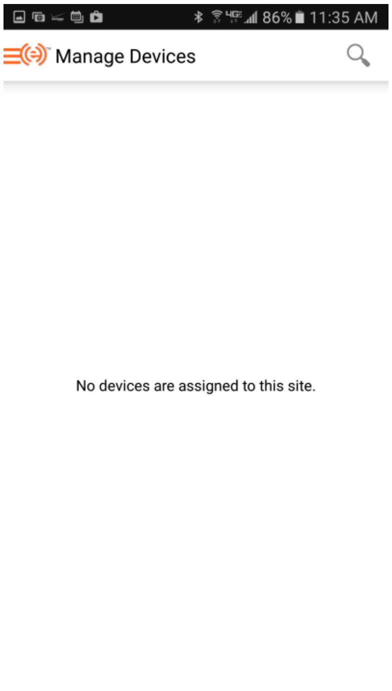


iOS



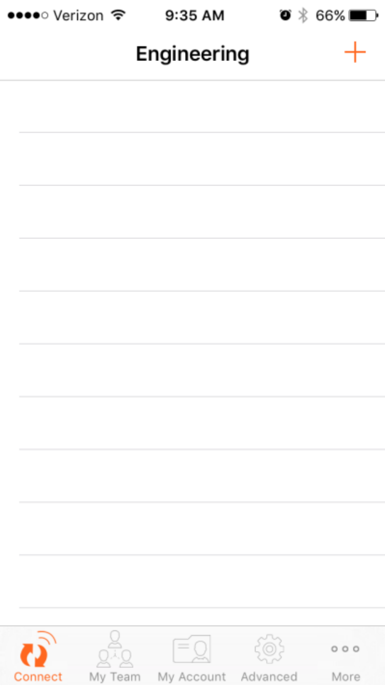
- Login to the unique site using the credentials provided by Vanderbilt
- The initial “Manage Devices” screen will be empty until the first lock or gateway is added to the site

Android



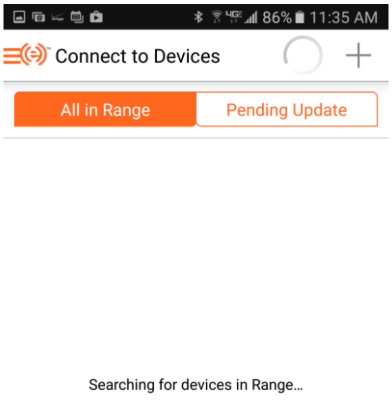
No devices are assigned to this site.

iOS



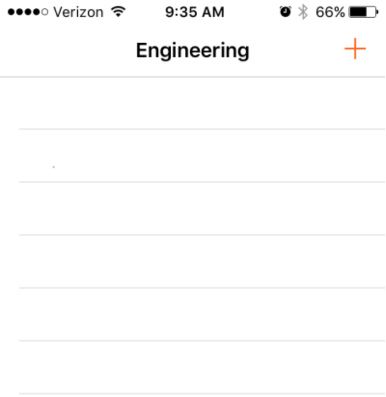
- Select Connect to devices / Add Device

Android



Searching for devices in Range…

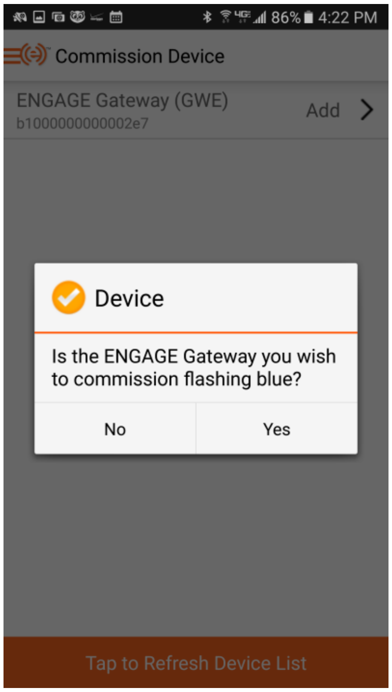
iOS



Site Name Listed At Top

- 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.

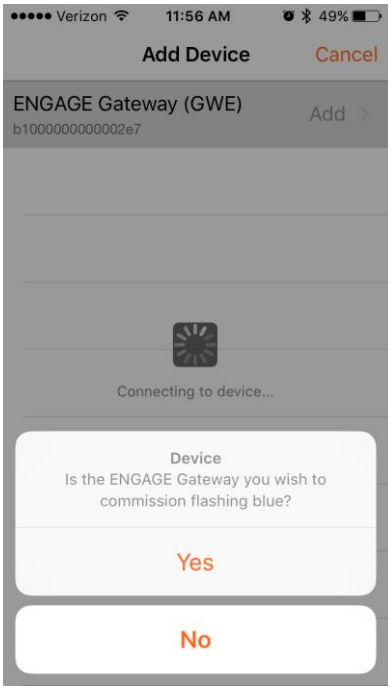
Android



Device

Is the ENGAGE Gateway you wish to commission flashing blue?

iOS



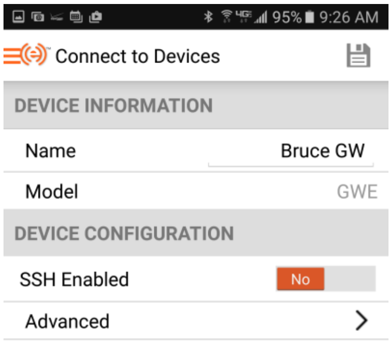
Connecting to device...

Device

Is the ENGAGE Gateway you wish to commission flashing blue?

- Click “Yes”.
- Configure Device will open
- Name the Gateway and click Save / Next

Android



95% 9:26 AM

Connect to Devices

DEVICE INFORMATION

Name Bruce GW

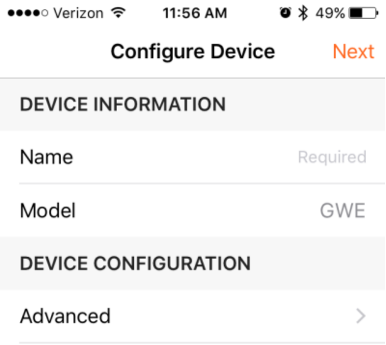
Model GWE

DEVICE CONFIGURATION

SSH Enabled No

Advanced >

iOS



●●●●○ Verizon 11:56 AM 49%

Configure Device Next

DEVICE INFORMATION

Name Required

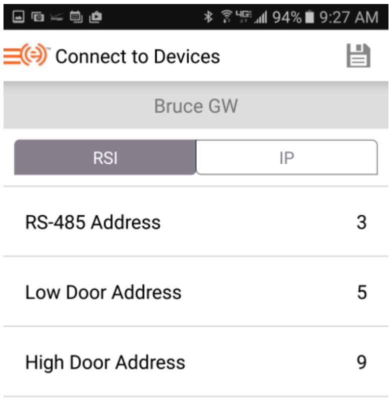
Model GWE

DEVICE CONFIGURATION

Advanced >

- 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).

Android



94% 9:27 AM

Connect to Devices

Bruce GW

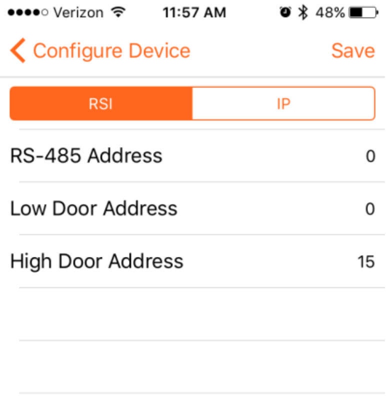
RSI | IP

RS-485 Address 3

Low Door Address 5

High Door Address 9

iOS



●●●●○ Verizon 11:57 AM 48%

< Configure Device Save

RSI | IP

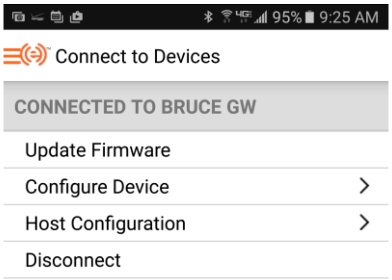
RS-485 Address 0

Low Door Address 0

High Door Address 15

- Set the Gateway, Low Door and High Door Addresses
- Click “Save” – Commissioning is completed

Android



95% 9:25 AM

Connect to Devices

CONNECTED TO BRUCE GW

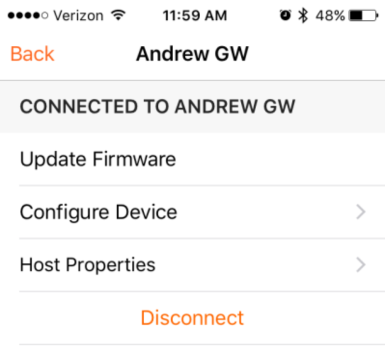
Update Firmware

Configure Device >

Host Configuration >

Disconnect

iOS



●●●●○ Verizon 11:59 AM 48%

Back Andrew GW

CONNECTED TO ANDREW GW

Update Firmware

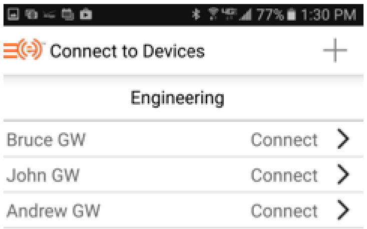
Configure Device >

Host Properties >

Disconnect

- Click “Disconnect”
- The Gateway will now be displayed in the Connect to Device / Site screen

Android



77% 1:30 PM

Connect to Devices +

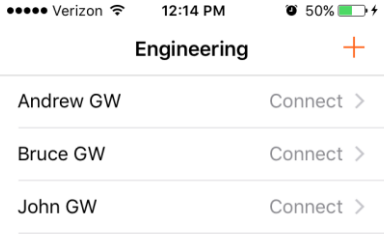
Engineering

Bruce GW Connect >

John GW Connect >

Andrew GW Connect >

iOS



●●●●● Verizon 12:14 PM 50%

Engineering +

Andrew GW Connect >

Bruce GW Connect >

John GW Connect >

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

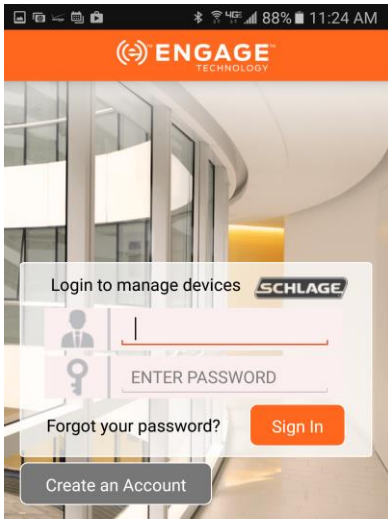
Schlage NDE Locks must be fully assembled, batteries installed with the battery cover in place and a Factory Default Reset (FDR) performed prior to commissioning.

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

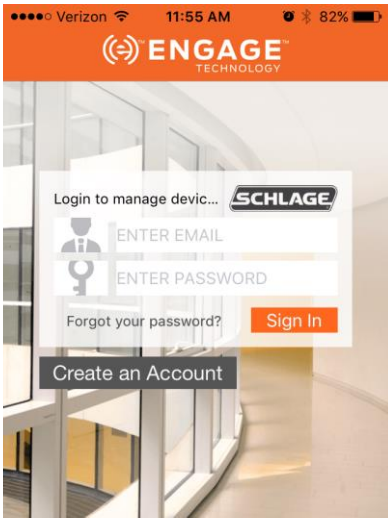
Do Not Modify Settings Other Than Those Specified Below During the Commissioning Process

- Open the ENGAGE app on the mobile device

Android



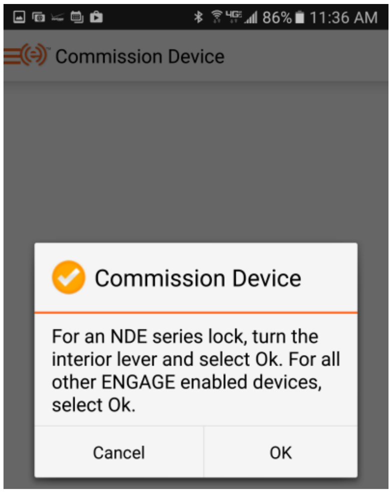
iOS



- 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

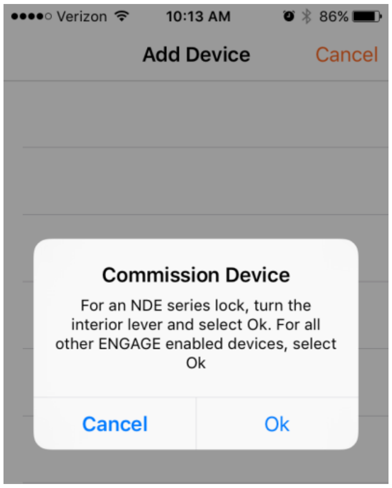
Android



Commission Device

For an NDE series lock, turn the interior lever and select Ok. For all other ENGAGE enabled devices, select Ok.

iOS

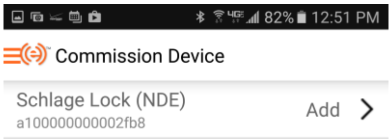


Commission Device

For an NDE series lock, turn the interior lever and select Ok. For all other ENGAGE enabled devices, select Ok

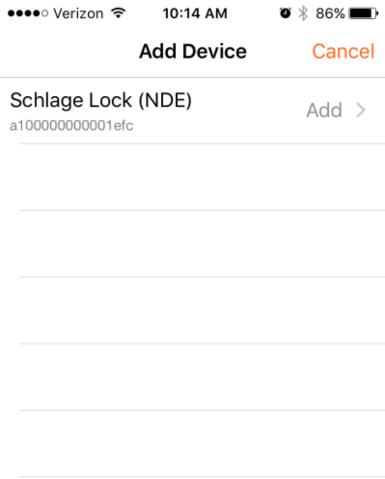
- Turn and release the NDE lock inside lever as indicated
- Click "OK"
- The NDE lock should now display in the ENGAGE app

Android



Schlage Lock (NDE)
a100000000002fb8

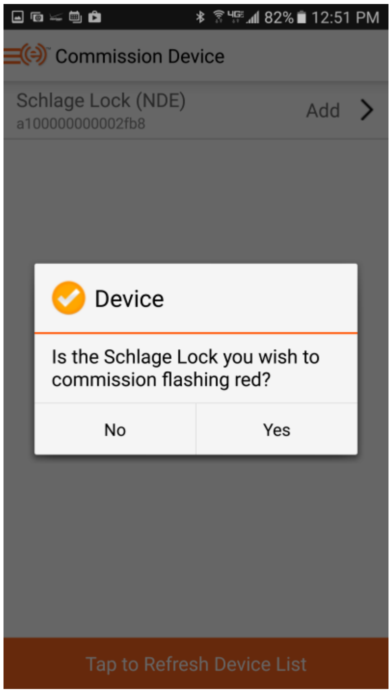
iOS



Schlage Lock (NDE)
a100000000001efc

- Select "Add"
- The NDE lock should start flashing red

Android



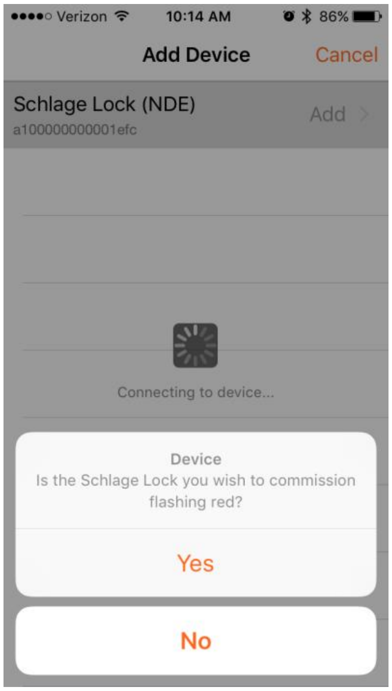
Schlage Lock (NDE)
a100000000002fb8

Device

Is the Schlage Lock you wish to commission flashing red?

No | Yes

iOS



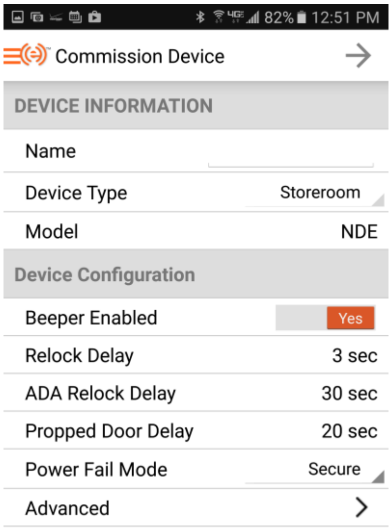
Schlage Lock (NDE)
a100000000001efc

Connecting to device...

Device
Is the Schlage Lock you wish to commission flashing red?

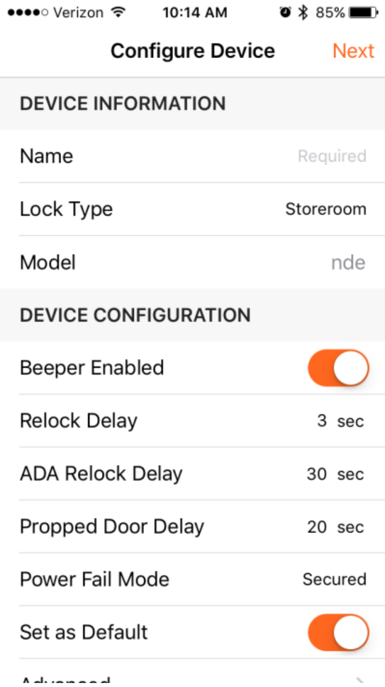
- Select "Yes"

Android



DEVICE INFORMATION	
Name	
Device Type	Storeroom
Model	NDE
Device Configuration	
Beeper Enabled	Yes
Relock Delay	3 sec
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secure

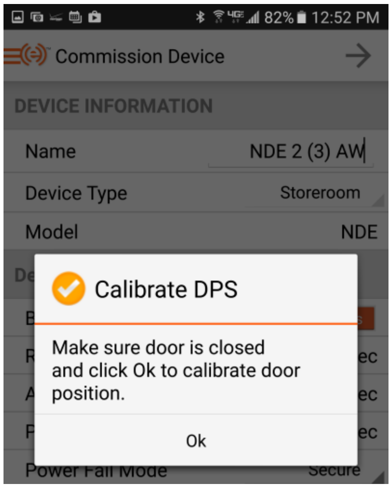
iOS



DEVICE INFORMATION	
Name	Required
Lock Type	Storeroom
Model	nde
DEVICE CONFIGURATION	
Beeper Enabled	●
Relock Delay	3 sec
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secured
Set as Default	●

- Enter a Name for the NDE lock and click "→" / "Next"
- The ENGAGE app will prompt for magnetic Door Position Switch (DPS) calibration

Android



82% 12:52 PM

Commission Device

DEVICE INFORMATION

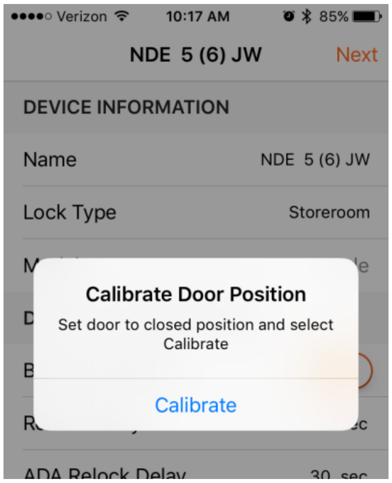
Name	NDE 2 (3) AW
Device Type	Storeroom
Model	NDE
Power Fail Mode	Secure

Calibrate DPS

Make sure door is closed and click Ok to calibrate door position.

Ok

iOS



Verizon 10:17 AM 85%

NDE 5 (6) JW Next

DEVICE INFORMATION

Name	NDE 5 (6) JW
Lock Type	Storeroom
ADA Relock Delay	30 sec

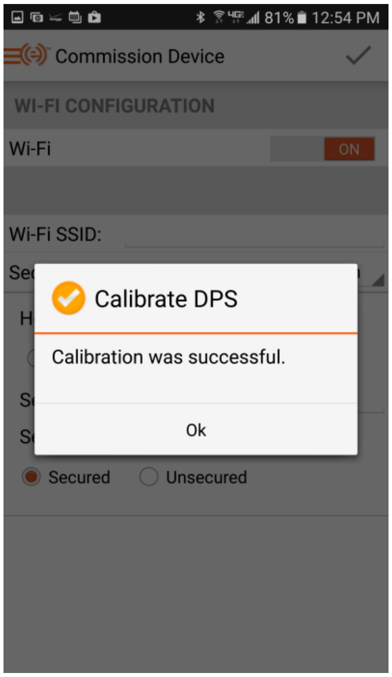
Calibrate Door Position

Set door to closed position and select Calibrate

Calibrate

- Close the door
- Click “OK” / “Calibrate” to initiate DPS calibration

Android



81% 12:54 PM

Commission Device

WI-FI CONFIGURATION

Wi-Fi ON

Wi-Fi SSID:

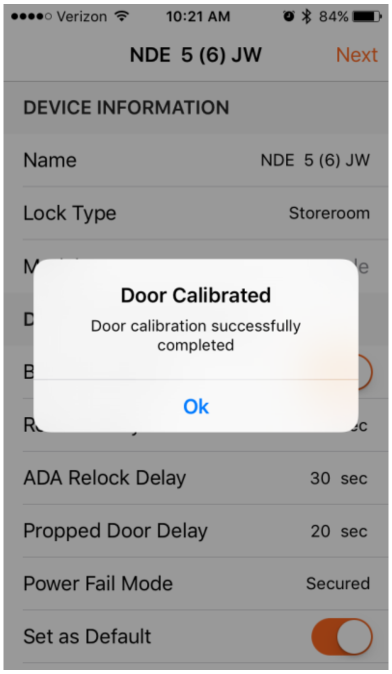
Calibrate DPS

Calibration was successful.

Ok

● Secured ○ Unsecured

iOS



Verizon 10:21 AM 84%

NDE 5 (6) JW Next

DEVICE INFORMATION

Name	NDE 5 (6) JW
Lock Type	Storeroom
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secured
Set as Default	ON

Door Calibrated

Door calibration successfully completed

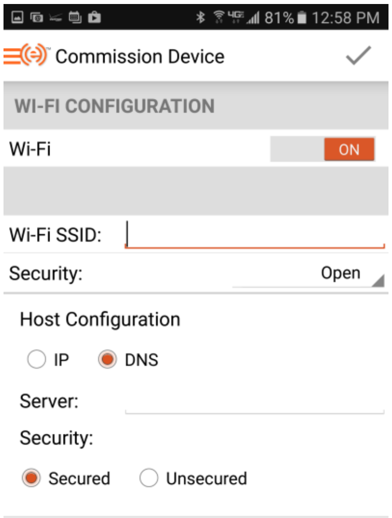
Ok

- 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

Android



Commission Device ✓

WI-FI CONFIGURATION

Wi-Fi ON

Wi-Fi SSID:

Security: Open

Host Configuration

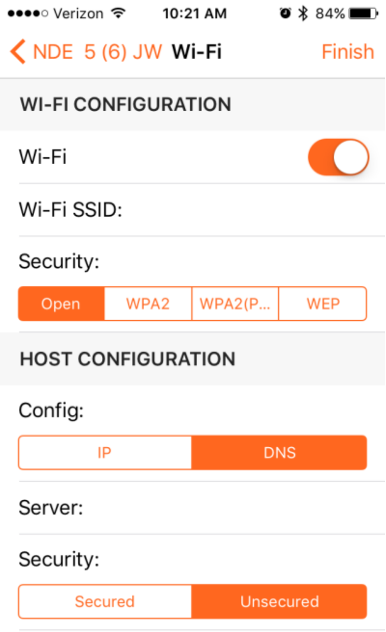
○ IP ● DNS

Server:

Security:

● Secured ○ Unsecured

iOS



< NDE 5 (6) JW **Wi-Fi** Finish

WI-FI CONFIGURATION

Wi-Fi ●

Wi-Fi SSID:

Security:

[✓ Open] WPA2 WPA2(P... WEP

HOST CONFIGURATION

Config:

IP [✓ DNS]

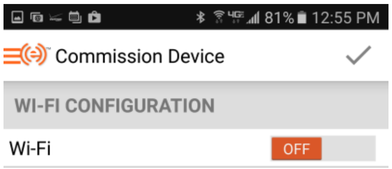
Server:

Security:

Secured [✓ Unsecured]

- Turn Wi-Fi OFF

Android

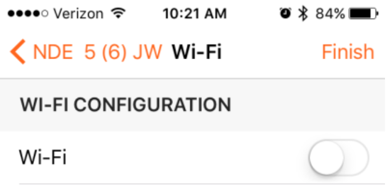


Commission Device ✓

WI-FI CONFIGURATION

Wi-Fi OFF

iOS



< NDE 5 (6) JW **Wi-Fi** Finish

WI-FI CONFIGURATION

Wi-Fi ○

- Click "✓" / "Finish" to complete commissioning

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

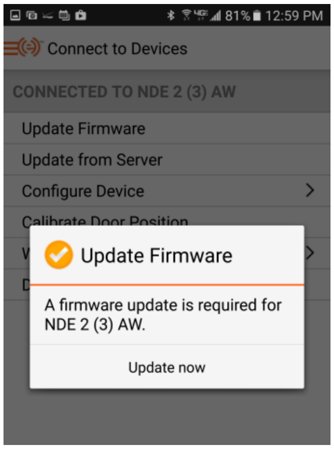
- Follow the ENGAGE app prompts to update the firmware if required

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

- Android


81% 12:59 PM

Connect to Devices

CONNECTED TO NDE 2 (3) AW

Update Firmware

Update from Server

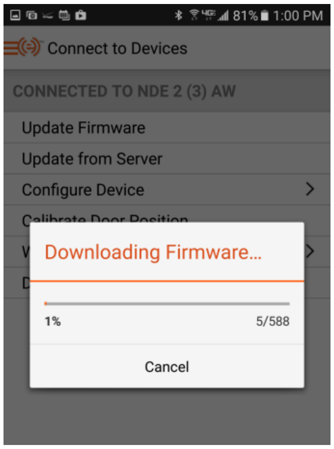
Configure Device

Calibrate Door Position

Update Firmware

A firmware update is required for NDE 2 (3) AW.

Update now


81% 1:00 PM

Connect to Devices

CONNECTED TO NDE 2 (3) AW

Update Firmware

Update from Server

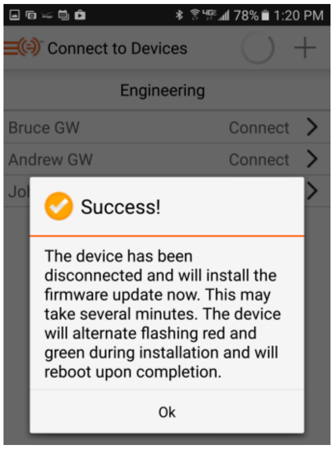
Configure Device

Calibrate Door Position

Downloading Firmware...

1% 5/588

Cancel


78% 1:20 PM

Connect to Devices

Engineering

Bruce GW Connect

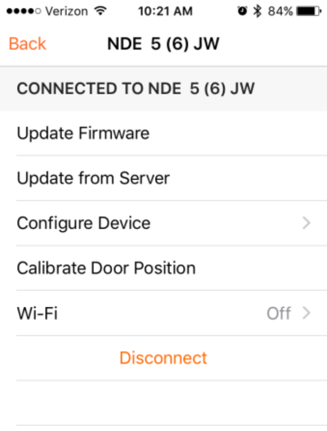
Andrew GW Connect

Success!

The device has been disconnected and will install the firmware update now. This may take several minutes. The device will alternate flashing red and green during installation and will reboot upon completion.

Ok

- iOS


Verizon 10:21 AM 84%

Back NDE 5 (6) JW

CONNECTED TO NDE 5 (6) JW

Update Firmware

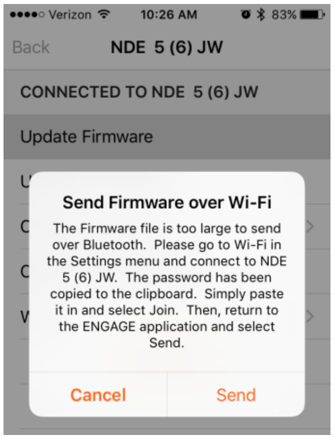
Update from Server

Configure Device

Calibrate Door Position

Wi-Fi Off

Disconnect


Verizon 10:26 AM 83%

Back NDE 5 (6) JW

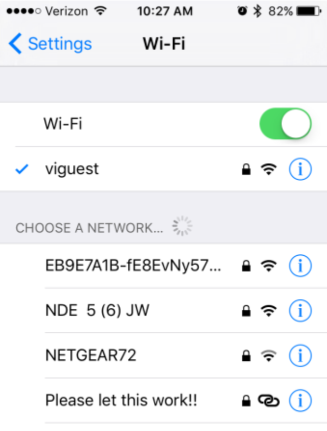
CONNECTED TO NDE 5 (6) JW

Update Firmware

Send Firmware over Wi-Fi

The Firmware file is too large to send over Bluetooth. Please go to Wi-Fi in the Settings menu and connect to NDE 5 (6) JW. The password has been copied to the clipboard. Simply paste it in and select Join. Then, return to the ENGAGE application and select Send.

Cancel Send


Verizon 10:27 AM 82%

Settings Wi-Fi

Wi-Fi

✓ viguest

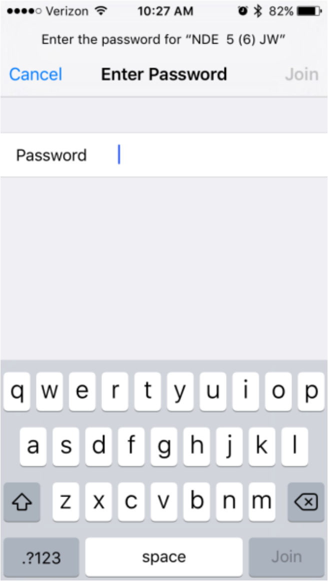
CHOOSE A NETWORK...

EB9E7A1B-fE8EvNy57...

NDE 5 (6) JW

NETGEAR72

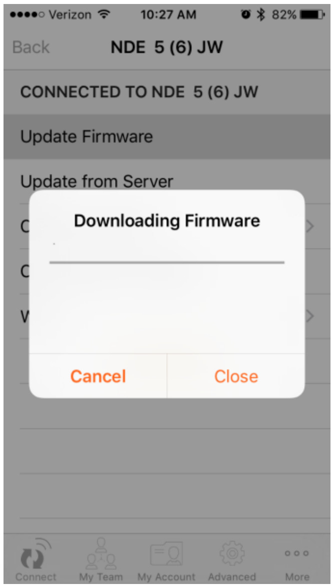
Please let this work!!


Verizon 10:27 AM 82%

Enter the password for "NDE 5 (6) JW"

Cancel **Enter Password** Join

Password


Verizon 10:27 AM 82%

Back NDE 5 (6) JW

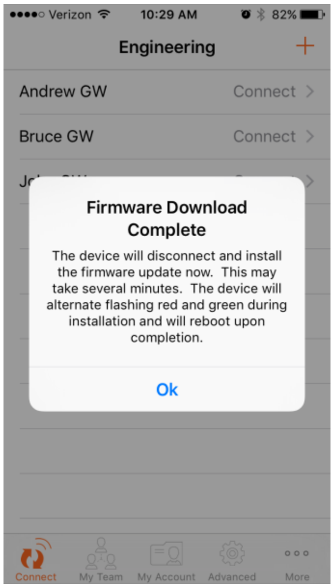
CONNECTED TO NDE 5 (6) JW

Update Firmware

Update from Server

Downloading Firmware

Cancel Close


Verizon 10:29 AM 82%

Engineering

Andrew GW Connect

Bruce GW Connect

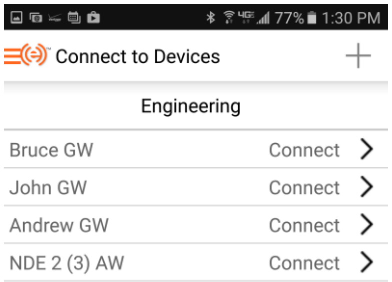
Firmware Download Complete

The device will disconnect and install the firmware update now. This may take several minutes. The device will alternate flashing red and green during installation and will reboot upon completion.

Ok

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

Android



77% 1:30 PM

Connect to Devices +

Engineering

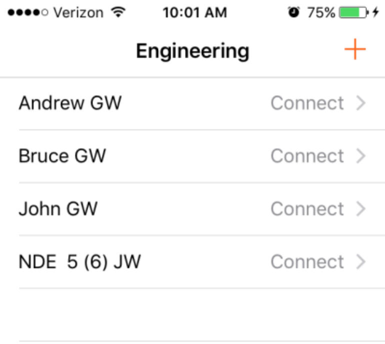
Bruce GW Connect >

John GW Connect >

Andrew GW Connect >

NDE 2 (3) AW Connect >

iOS



●●●●○ Verizon 10:01 AM 75%

Engineering +

Andrew GW Connect >

Bruce GW Connect >

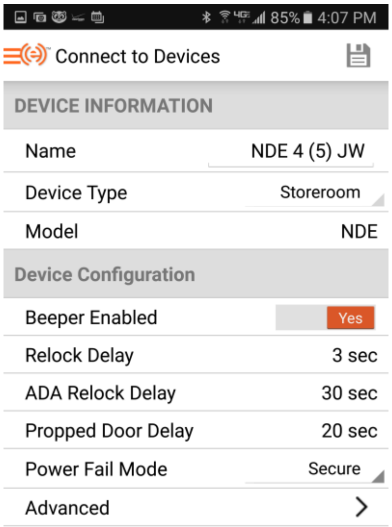
John GW Connect >

NDE 5 (6) JW Connect >

Configure Communications Delay and Retry Timing

- Select “Connect” and “Configure Device”
- Select “Advanced”

Android

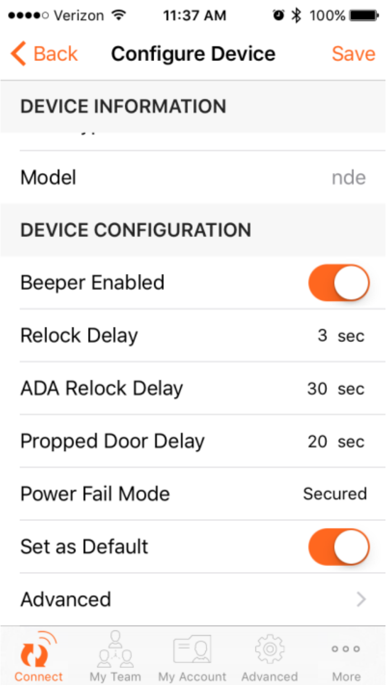


85% 4:07 PM

Connect to Devices

DEVICE INFORMATION	
Name	NDE 4 (5) JW
Device Type	Storeroom
Model	NDE
Device Configuration	
Beeper Enabled	Yes
Relock Delay	3 sec
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secure
Advanced	>

iOS



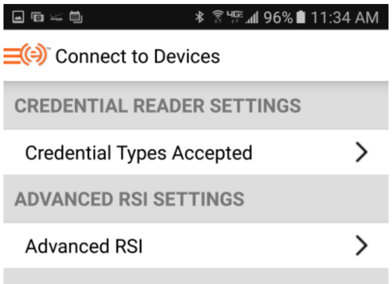
●●●●○ Verizon 11:37 AM 100%

< Back Configure Device Save

DEVICE INFORMATION	
Model	nde
DEVICE CONFIGURATION	
Beeper Enabled	●
Relock Delay	3 sec
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secured
Set as Default	●
Advanced	>

- Select “Advanced RSI”

Android



96% 11:34 AM

Connect to Devices

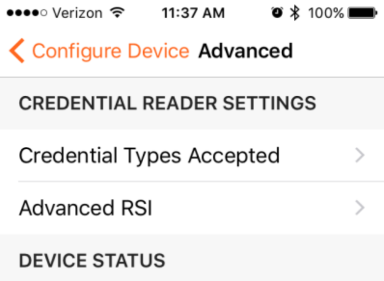
CREDENTIAL READER SETTINGS

Credential Types Accepted

ADVANCED RSI SETTINGS

Advanced RSI

iOS



Verizon 11:37 AM 100%

Configure Device Advanced

CREDENTIAL READER SETTINGS

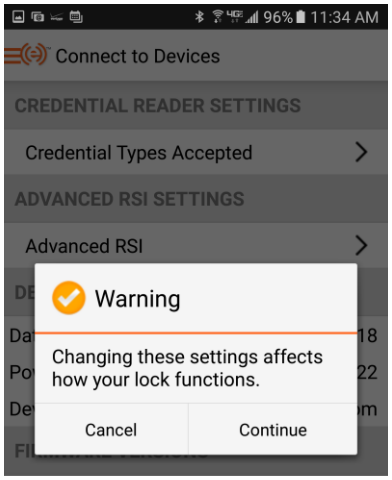
Credential Types Accepted

Advanced RSI

DEVICE STATUS

- Acknowledge the Warning by Clicking “Continue”

Android



96% 11:34 AM

Connect to Devices

CREDENTIAL READER SETTINGS

Credential Types Accepted

ADVANCED RSI SETTINGS

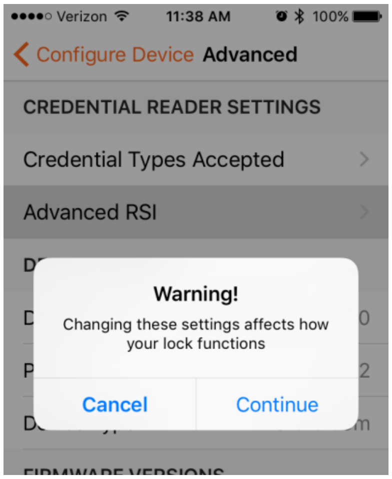
Advanced RSI

Warning

Changing these settings affects how your lock functions.

Cancel Continue

iOS



Verizon 11:38 AM 100%

Configure Device Advanced

CREDENTIAL READER SETTINGS

Credential Types Accepted

Advanced RSI

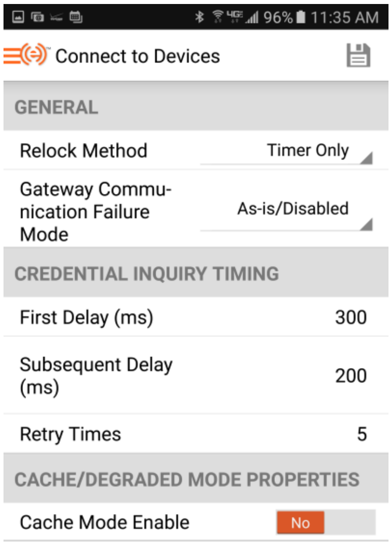
Warning!

Changing these settings affects how your lock functions

Cancel Continue

- Acknowledge the Warning by Clicking “Continue”

Android



96% 11:35 AM

Connect to Devices

GENERAL

Relock Method: Timer Only

Gateway Communication Failure Mode: As-is/Disabled

CREDENTIAL INQUIRY TIMING

First Delay (ms): 300

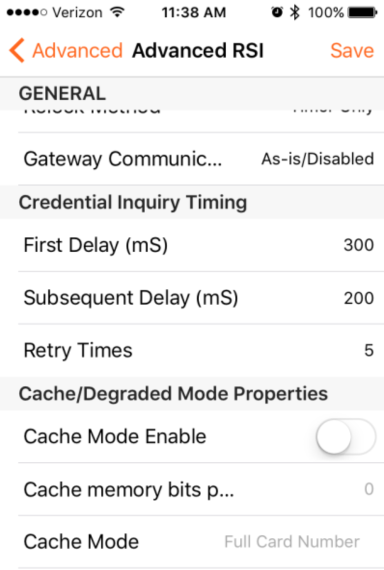
Subsequent Delay (ms): 200

Retry Times: 5

CACHE/DEGRADED MODE PROPERTIES

Cache Mode Enable: No

iOS



Verizon 11:38 AM 100%

Advanced Advanced RSI Save

GENERAL

Gateway Communic...: As-is/Disabled

Credential Inquiry Timing

First Delay (mS): 300

Subsequent Delay (mS): 200

Retry Times: 5

Cache/Degraded Mode Properties

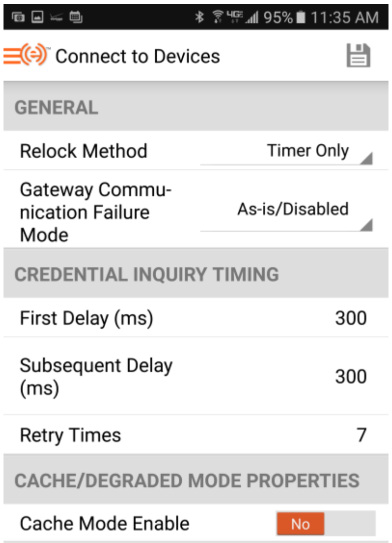
Cache Mode Enable

Cache memory bits p...: 0

Cache Mode: Full Card Number

- Set the following Credential Inquiry Timing parameters:
  - Set First Delay (ms) = 300
  - Set Subsequent Delay (ms) = 300
- Set Retry Times = 7

Android



Connect to Devices

GENERAL

Relock Method: Timer Only

Gateway Communication Failure Mode: As-is/Disabled

CREDENTIAL INQUIRY TIMING

First Delay (ms): 300

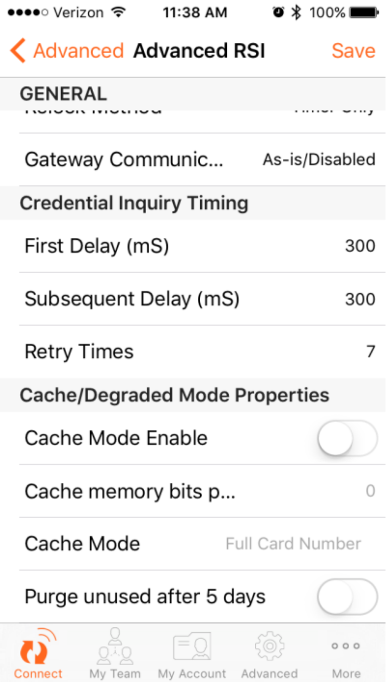
Subsequent Delay (ms): 300

Retry Times: 7

CACHE/DEGRADED MODE PROPERTIES

Cache Mode Enable: No

iOS



< Advanced **Advanced RSI** Save

GENERAL

Gateway Communic... As-is/Disabled

Credential Inquiry Timing

First Delay (mS): 300

Subsequent Delay (mS): 300

Retry Times: 7

Cache/Degraded Mode Properties

Cache Mode Enable

Cache memory bits p...: 0

Cache Mode: Full Card Number

Purge unused after 5 days

- Select Save
- Repeat the above process for each Schlage NDE lock to be utilized with SMS
- 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.

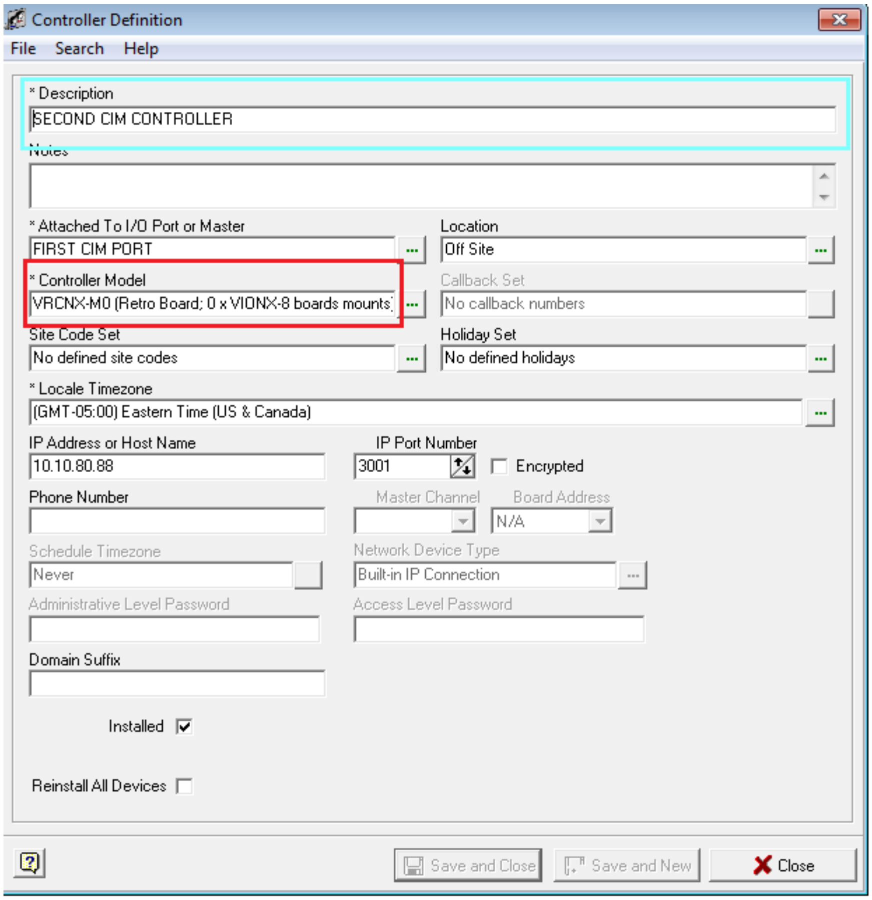
Define ENGAGE Devices in SMS

A valid, operational VRCNX-R/M/A controller must be defined prior to defining ENGAGE devices in SMS.

- Launch SMS and login with an Operator with administrative privileges
- Open the System Manager application
- Select the Hardware Map

Define Gateway

- Select Edit Controller and Navigate to the desired controller and open the Edit Controller dialog



* Description: SECOND CIM CONTROLLER

Notes:

* Attached To I/O Port or Master: FIRST CIM PORT

Location: Off Site

* Controller Model: VRCNX-M0 (Retro Board; 0 x VIONX-8 boards mounts)

Callback Set: No callback numbers

Site Code Set: No defined site codes

Holiday Set: No defined holidays

* Locale Timezone: (GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name: 10.10.80.88

IP Port Number: 3001

□ Encrypted

Phone Number:

Master Channel:

Board Address: N/A

Schedule Timezone: Never

Network Device Type: Built-in IP Connection

Administrative Level Password:

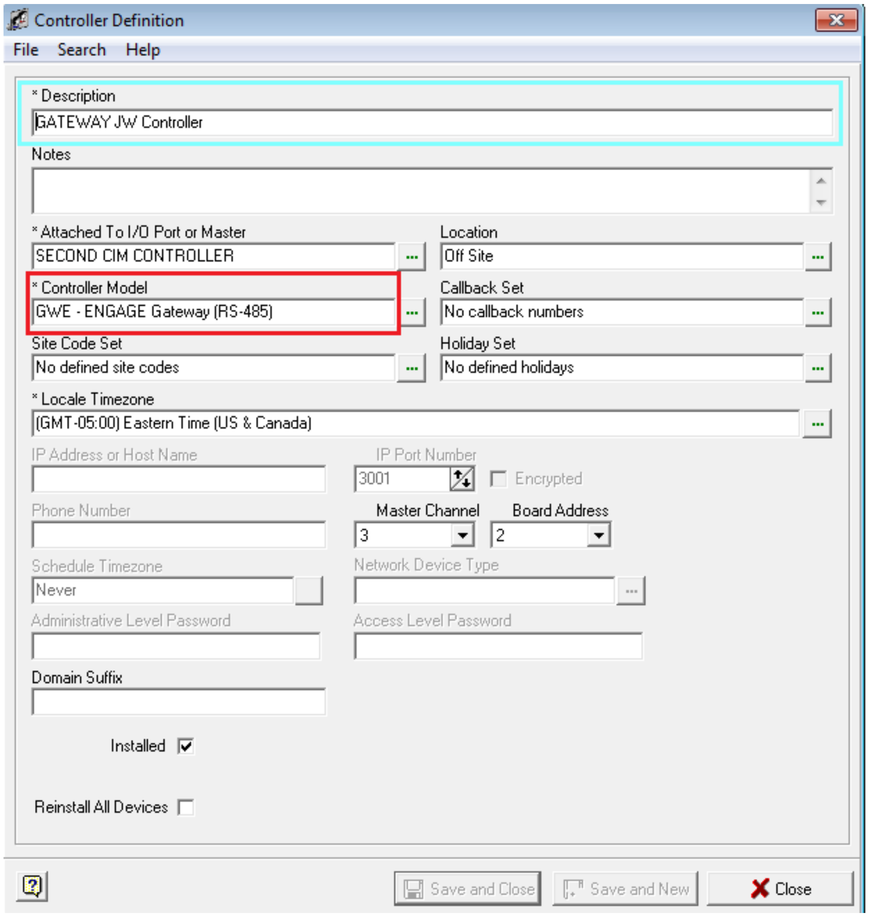
Access Level Password:

Domain Suffix:

Installed ☑

Reinstall All Devices □

- Click the “+” symbol in the lower grid menu bar to add a new Controller
- Select “GWE – ENGAGE Gateway (RS – 485)” as the Controller model



* Description: GATEWAY JW Controller

Notes:

* Attached To I/O Port or Master: SECOND CIM CONTROLLER

Location: Off Site

* Controller Model: GWE - ENGAGE Gateway (RS-485)

Callback Set: No callback numbers

Site Code Set: No defined site codes

Holiday Set: No defined holidays

* Locale Timezone: (GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name:

IP Port Number: 3001

□ Encrypted

Phone Number:

Master Channel: 3

Board Address: 2

Schedule Timezone: Never

Network Device Type:

Administrative Level Password:

Access Level Password:

Domain Suffix:

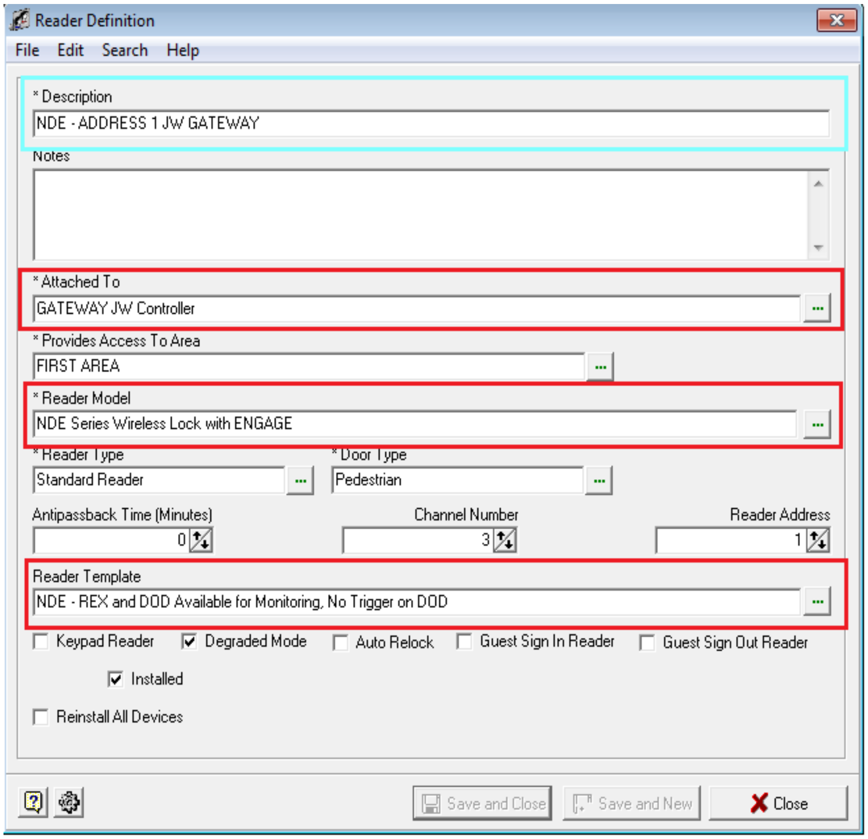
Installed ☑

Reinstall All Devices □

- Select the appropriate RS-485 Channel and Address
- Click “Save and Close” or “Save and New” as required to define additional Gateways

Define NDE Lock

- Highlight a defined GWE – ENGAGE Gateway
- Click “Edit Readers”
- Click the “+” symbol in the lower grid menu bar to add a new Reader
- Select “NDE Series Wireless Lock with ENGAGE” as the Reader model
- Select “NDE – REX and DOD Available for Monitoring No Trigger on DOD” as the Reader template



* Description: NDE - ADDRESS 1 JW GATEWAY

Notes:

* Attached To: GATEWAY JW Controller

* Provides Access To Area: FIRST AREA

* Reader Model: NDE Series Wireless Lock with ENGAGE

* Reader Type: Standard Reader

* Door Type: Pedestrian

Antipassback Time (Minutes): 0

Channel Number: 3

Reader Address: 1

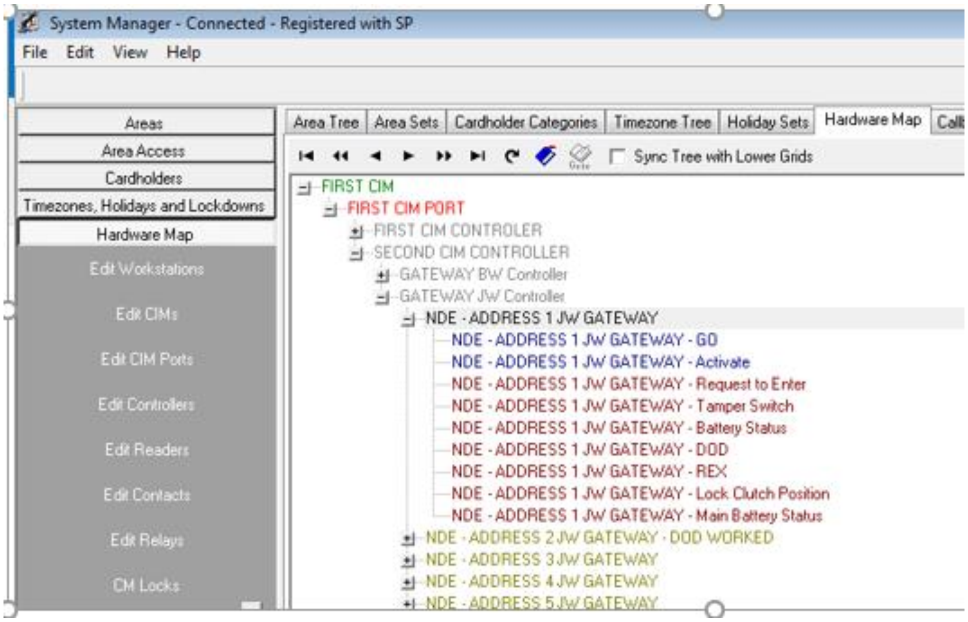
Reader Template: NDE - REX and DOD Available for Monitoring, No Trigger on DOD

☐ Keypad Reader ☑ Degraded Mode ☐ Auto Relock ☐ Guest Sign In Reader ☐ Guest Sign Out Reader

☑ Installed

☐ Reinstall All Devices

- Set the appropriate Reader Address
- Click “Save and Close” or “Save and New” as required to define additional Locks for the Gateway
- The Gateway and NDE Locks will be visible in the Hardware Map



```
FIRST CIM
  FIRST CIM PORT
    FIRST CIM CONTROLER
    SECOND CIM CONTROLLER
      GATEWAY BW Controller
      GATEWAY JW Controller
        NDE - ADDRESS 1 JW GATEWAY
          NDE - ADDRESS 1 JW GATEWAY - GO
          NDE - ADDRESS 1 JW GATEWAY - Activate
          NDE - ADDRESS 1 JW GATEWAY - Request to Enter
          NDE - ADDRESS 1 JW GATEWAY - Tamper Switch
          NDE - ADDRESS 1 JW GATEWAY - Battery Status
          NDE - ADDRESS 1 JW GATEWAY - DOD
          NDE - ADDRESS 1 JW GATEWAY - REX
          NDE - ADDRESS 1 JW GATEWAY - Lock Clutch Position
          NDE - ADDRESS 1 JW GATEWAY - Main Battery Status
        NDE - ADDRESS 2 JW GATEWAY - DOD WORKED
        NDE - ADDRESS 3 JW GATEWAY
        NDE - ADDRESS 4 JW GATEWAY
        NDE - ADDRESS 5 JW GATEWAY
```

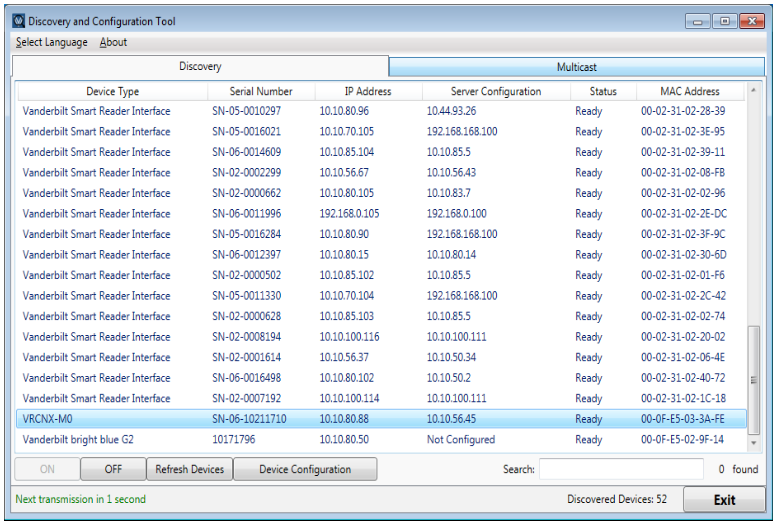
Link NDE Locks to GWE – ENGAGE Gateway

Linking the GWE – ENGAGE Gateway and NDE Wireless Locks with ENGAGE Technology is accomplished using the Vanderbilt Discovery Tool provided with SMS.

Discovery Tool v1.4.7 or newer is required.

VRCNX-M Controllers firmware v6.70 or newer and VRCNX-R Controllers firmware v6.60 or newer is required.

- Launch the Discovery Tool and click “ON” to enable auto-discovery



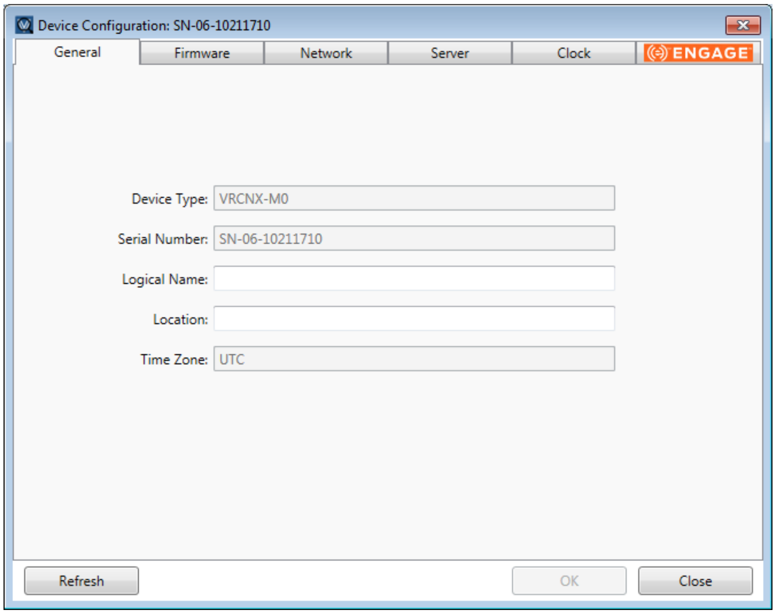
Device Type	Serial Number	IP Address	Server Configuration	Status	MAC Address
Vanderbilt Smart Reader Interface	SN-05-0010297	10.10.80.96	10.44.93.26	Ready	00-02-31-02-28-39
Vanderbilt Smart Reader Interface	SN-05-0016021	10.10.70.105	192.168.168.100	Ready	00-02-31-02-3E-95
Vanderbilt Smart Reader Interface	SN-06-0014609	10.10.85.104	10.10.85.5	Ready	00-02-31-02-39-11
Vanderbilt Smart Reader Interface	SN-02-0002299	10.10.56.67	10.10.56.43	Ready	00-02-31-02-08-FB
Vanderbilt Smart Reader Interface	SN-02-0000662	10.10.80.105	10.10.83.7	Ready	00-02-31-02-02-96
Vanderbilt Smart Reader Interface	SN-06-0011996	192.168.0.105	192.168.0.100	Ready	00-02-31-02-2E-DC
Vanderbilt Smart Reader Interface	SN-05-0016284	10.10.80.90	192.168.168.100	Ready	00-02-31-02-3F-9C
Vanderbilt Smart Reader Interface	SN-06-0012397	10.10.80.15	10.10.80.14	Ready	00-02-31-02-30-6D
Vanderbilt Smart Reader Interface	SN-02-0000502	10.10.85.102	10.10.85.5	Ready	00-02-31-02-01-F6
Vanderbilt Smart Reader Interface	SN-05-0011330	10.10.70.104	192.168.168.100	Ready	00-02-31-02-2C-42
Vanderbilt Smart Reader Interface	SN-02-0000628	10.10.85.103	10.10.85.5	Ready	00-02-31-02-02-74
Vanderbilt Smart Reader Interface	SN-02-0008194	10.10.100.116	10.10.100.111	Ready	00-02-31-02-20-02
Vanderbilt Smart Reader Interface	SN-02-0001614	10.10.56.37	10.10.50.34	Ready	00-02-31-02-06-4E
Vanderbilt Smart Reader Interface	SN-06-0016498	10.10.80.102	10.10.50.2	Ready	00-02-31-02-40-72
Vanderbilt Smart Reader Interface	SN-02-0007192	10.10.100.114	10.10.100.111	Ready	00-02-31-02-1C-18
VRCNX-M0	SN-06-10211710	10.10.80.88	10.10.56.45	Ready	00-0F-E5-03-3A-FE
Vanderbilt bright blue G2	10171796	10.10.80.50	Not Configured	Ready	00-0F-E5-02-9F-14

Search: 0 found

Next transmission in 1 second

Discovered Devices: 52

- Locate the VRCNX-M/R Controller to which the GWE – ENGAGE Gateway is wired and double-click to open the Device Configuration dialog.



Device Type: VRCNX-M0

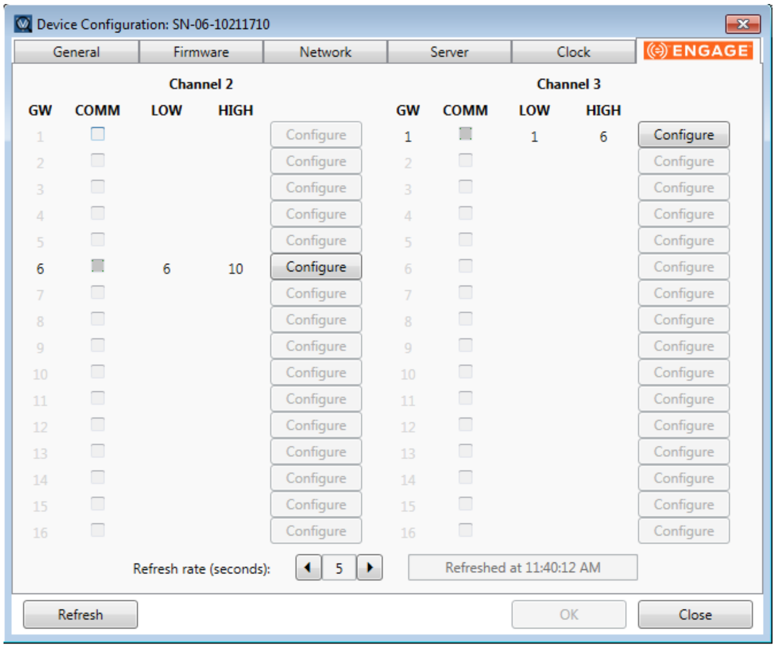
Serial Number: SN-06-10211710

Logical Name:

Location:

Time Zone: UTC

- Select the “ENGAGE” tab once displayed



Device Configuration: SN-06-10211710

Channel 2					Channel 3				
GW	COMM	LOW	HIGH		GW	COMM	LOW	HIGH	
1	☐			Configure	1	☒	1	6	Configure
2	☐			Configure	2	☐			Configure
3	☐			Configure	3	☐			Configure
4	☐			Configure	4	☐			Configure
5	☐			Configure	5	☐			Configure
6	☒	6	10	Configure	6	☐			Configure
7	☐			Configure	7	☐			Configure
8	☐			Configure	8	☐			Configure
9	☐			Configure	9	☐			Configure
10	☐			Configure	10	☐			Configure
11	☐			Configure	11	☐			Configure
12	☐			Configure	12	☐			Configure
13	☐			Configure	13	☐			Configure
14	☐			Configure	14	☐			Configure
15	☐			Configure	15	☐			Configure
16	☐			Configure	16	☐			Configure

Refresh rate (seconds): 5

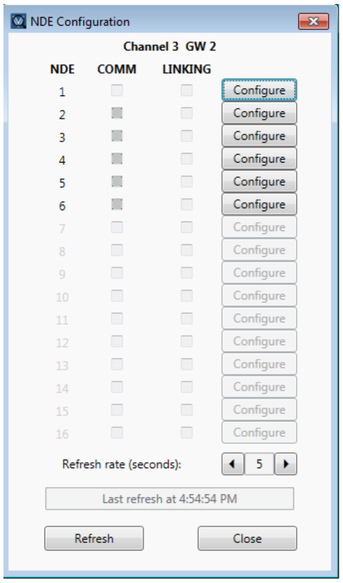
Refreshed at 11:40:12 AM

- 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 SMS. ENGAGE Device Addressing is 0-based while SMS Addressing is 1-based. See *GWE – ENGAGE Gateway, NDE Lock and SMS 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.



NDE Configuration

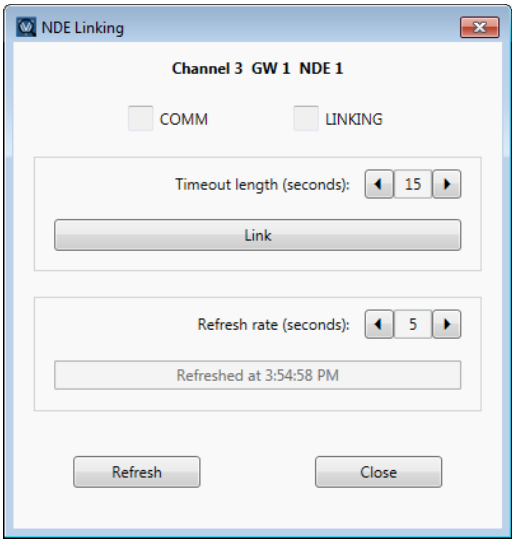
Channel 3 GW 2

NDE	COMM	LINKING	
1	☐	☐	Configure
2	☒	☐	Configure
3	☒	☐	Configure
4	☒	☐	Configure
5	☒	☐	Configure
6	☒	☐	Configure
7	☐	☐	Configure
8	☐	☐	Configure
9	☐	☐	Configure
10	☐	☐	Configure
11	☐	☐	Configure
12	☐	☐	Configure
13	☐	☐	Configure
14	☐	☐	Configure
15	☐	☐	Configure
16	☐	☐	Configure

Refresh rate (seconds): 5

Last refresh at 4:54:54 PM

- Click “Configure” on the NDE Lock to Link



Channel 3 GW 1 NDE 1

Timeout length (seconds): 15

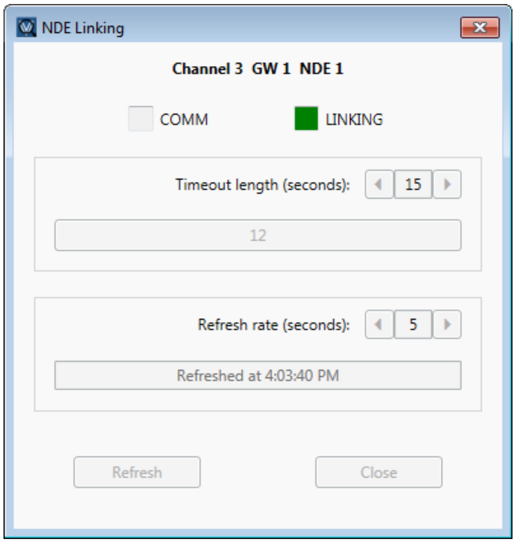
Refresh rate (seconds): 5

Refreshed at 3:54:58 PM

- 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

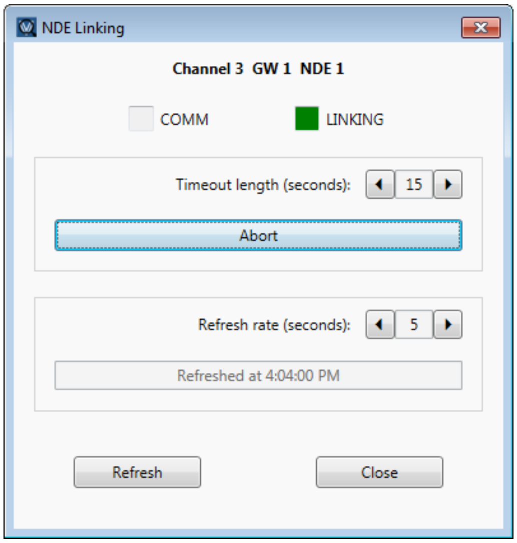


Channel 3 GW 1 NDE 1

Timeout length (seconds): 15

Refresh rate (seconds): 5

Refreshed at 4:03:40 PM



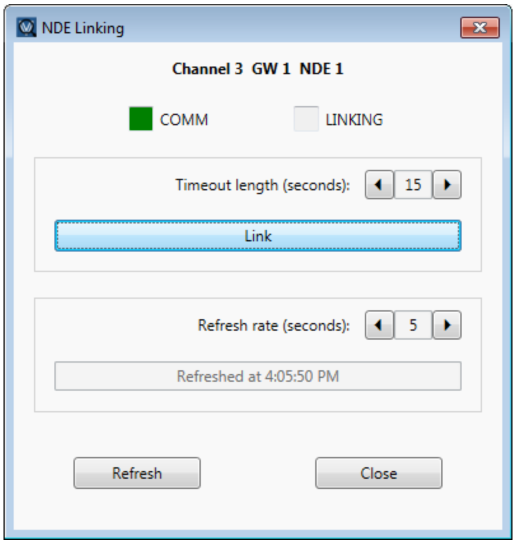
Channel 3 GW 1 NDE 1

Timeout length (seconds): 15

Refresh rate (seconds): 5

Refreshed at 4:04:00 PM

- 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)



NDE Linking

Channel 3 GW 1 NDE 1

🟩 COMM □ LINKING

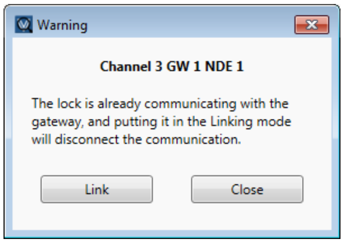
Timeout length (seconds): 15

Refresh rate (seconds): 5

Refreshed at 4:05:50 PM

- 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.

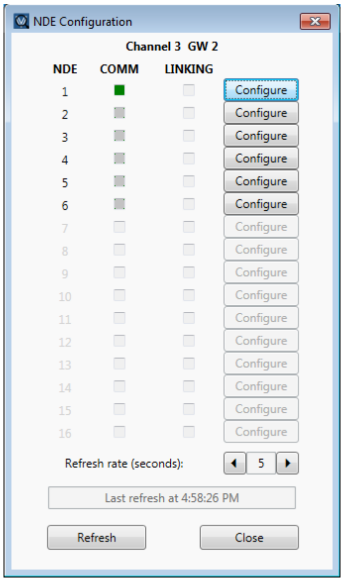


Warning

Channel 3 GW 1 NDE 1

The lock is already communicating with the gateway, and putting it in the Linking mode will disconnect the communication.

- The Lock will display communicating in the Available Locks dialog.



NDE Configuration

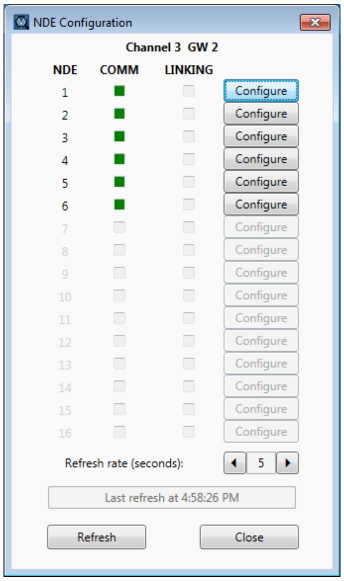
Channel 3 GW 2

NDE	COMM	LINKING	
1	🟩	□	Configure
2	▨	□	Configure
3	▨	□	Configure
4	▨	□	Configure
5	▨	□	Configure
6	▨	□	Configure
7	□	□	Configure
8	□	□	Configure
9	□	□	Configure
10	□	□	Configure
11	□	□	Configure
12	□	□	Configure
13	□	□	Configure
14	□	□	Configure
15	□	□	Configure
16	□	□	Configure

Refresh rate (seconds): 5

Last refresh at 4:58:26 PM

- Repeat the above process to link additional NDE Locks to the selected Gateway



NDE Configuration

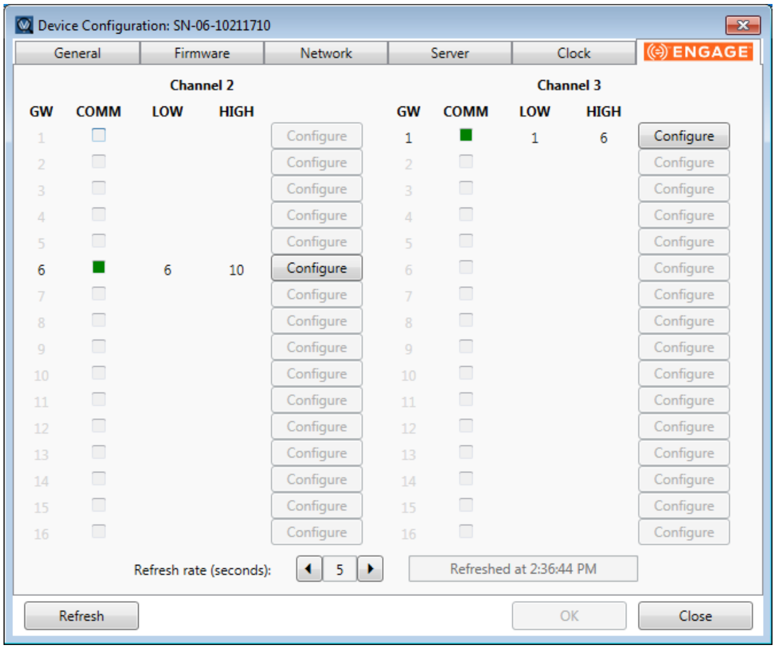
Channel 3 GW 2

NDE	COMM	LINKING	
1	🟩	□	Configure
2	🟩	□	Configure
3	🟩	□	Configure
4	🟩	□	Configure
5	🟩	□	Configure
6	🟩	□	Configure
7	□	□	Configure
8	□	□	Configure
9	□	□	Configure
10	□	□	Configure
11	□	□	Configure
12	□	□	Configure
13	□	□	Configure
14	□	□	Configure
15	□	□	Configure
16	□	□	Configure

Refresh rate (seconds): 5

Last refresh at 4:58:26 PM

- Close the dialog once all desired NDE Locks are linked to the Gateway



Device Configuration: SN-06-10211710

Channel 2					Channel 3				
GW	COMM	LOW	HIGH		GW	COMM	LOW	HIGH	
1	□			Configure	1	🟩	1	6	Configure
2	□			Configure	2	□			Configure
3	□			Configure	3	□			Configure
4	□			Configure	4	□			Configure
5	□			Configure	5	□			Configure
6	🟩	6	10	Configure	6	□			Configure
7	□			Configure	7	□			Configure
8	□			Configure	8	□			Configure
9	□			Configure	9	□			Configure
10	□			Configure	10	□			Configure
11	□			Configure	11	□			Configure
12	□			Configure	12	□			Configure
13	□			Configure	13	□			Configure
14	□			Configure	14	□			Configure
15	□			Configure	15	□			Configure
16	□			Configure	16	□			Configure

Refresh rate (seconds): 5

Refreshed at 2:36:44 PM

- Repeat for additional GWE – ENGAGE Gateways and NDE Wireless Locks as required.

- Close the Device Configuration dialog when complete

- Exit the Discovery Tool

CHAPTER 29

Von Duprin ENGAGE RM / RU Exit Devices

ENGAGE RM / RU Exit Device Option

Overview

Von Duprin created the Remote Undogging (RU) and Remote Monitoring (RM) options to address the need for remote monitoring and control of secondary doors which are frequently left unlocked or propped open. The Von Duprin® RU option is a battery powered wireless solution that enables remote undogging and door status monitoring. It enhances perimeter security by providing electronic override of mechanical dogging for emergency facility lockdown. The RM option is a sensor only configuration for exit only or fire rate doors that require monitoring. It provides visibility to request to exit (RX), latchbolt monitor (LX) and door position switch (DPS). Both are modular kits that can be added to any existing Von Duprin 98/99 or 33A/35A Series device. They connect to SMS via connection to the ENGAGE™ GWE RS-485 gateway similarly to NDE Series locks. ENGAGE RM/RU modules can be mixed with NDE Series locks on the same GWE Gateway.

The ENGAGE RM/RU devices can also be installed into a double-door configuration with no mullion. This represents a special “paired” configuration since some door status events require status of the paired door which must be identified in the SMS configuration.

Note: ENGAGE RM/RU support requires VRCNX-R/M/A firmware v6.65V / v6.87M / v7.16A or higher installed.

ENGAGE RM/RU Components

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

- One or more GWE – ENGAGE Gateways
- One or more ENGAGE RM/RU Series wireless modules (maximum 10 per gateway)
- Android or iOS Smartphone with ENGAGE app for configuration

The GWE – ENGAGE Gateway is hard wired to the reader controller (VRCNX-R/M/A or VMRC-1/2) communication channels via RS-485 protocol. The Gateway installation location is determined by the location of the RM/RU series modules (maximum distance between Gateway and ENGAGE modules is 30 feet) with which it will communicate wirelessly via Bluetooth.

Gateway (GWE - ENGAGE)

The GWE – ENGAGE works in conjunction with the RM/RU modules. The GWE – ENGAGE Gateway is hard wired directly to the VRCNX-R/M/A reader controller communication channels and communicates via RS-485 protocol. The GWE – ENGAGE can support up to 10 RM/RU modules or 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 – *not applicable for RM/RU*
- 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-R/M/A*)

Specifications for the GWE – ENGAGE Gateway

- 2.4 GHz Bluetooth v4.0
- Spread spectrum
- Dynamic channel switching (40 channels)
- Range: Up to 30’ line of site to door
- Gateway to Lock Encryption: AES 256-bit
- Certifications: UL294, FCC Part 15, Industry Canada (IC), RoHS
- RS-485 Communication to VRCNX-R/M/A
- Supports 10 RM/RU or NDE Wireless Devices
- VRCNX-R/M/A can support multiple GWE - ENGAGE

ENAGE RM/RU Wireless Modules

Von Duprin ENGAGE RM/RU modules contain all of the elements needed to electronically control and monitor access through an exit door wirelessly. It is a modular battery powered kit that can be added on to existing 98/99 and 33A/35A series devices. The RM option is a sensor only configuration for exit only or fire rate doors that require monitoring. It provides visibility to request to exit (RX), latchbolt monitor (LX) and door position switch (DPS). The modules include an RF transceiver for communicating with a GWE – ENGAGE Gateway or smart phone (for configuration only). The GWE – ENGAGE Gateway interfaces to the reader controller (VRCNX-R/M/A or VMRC-1/2) via wired RS-485.

Performance

- Wake Up on Radio - Allows the GWE - ENGAGE to alert the RM/RU modules in case of a Lock-out event. Responds to command from SMS within 5 seconds when linked to GWE – ENGAGE Gateway.
- Addressing
- Bluetooth Low Energy v4.2 when used with GWE – ENGAGE Gateway
- Range: up to 30 feet line of site to door

Electronics Certifications

- UL 294 Indoor
- FCC Part 15 – Commercial

Exit Devices Will Retain the Following Mechanical Specifications

- BHMA A156.3 (Grade 1)
- UL305, Windstorm WX98/9927
- Tornado FEMA 361 ANSI/ICC500
- ADA ANSI A117.1
- UL 10C 3 hour
- ANSI / BHMA 156.18-2012 QUV
- Power: 4 AA alkaline batteries
- Battery Life: up to 2 years

Operating voltage

- The 4 AA batteries will supply 6.0 volts.
    - The locks will continue to operate down to <5.0 volts when Low Battery will be reported.
    - The locks will report Critical Battery at <4.8 volts and into a fail-safe, fail secure or fail as-is mode depending on lock configuration via ENGAGE mobile app.

Operational environment

- Temperature: - 4° to 140° F (-20° to 60°C)
- Humidity: 0% to 100% non-condensing

Available Sensors

- Request-to-Exit
- Door Position
- Interior Cover Tamper
- Magnetic Tamper
- Battery Status
- Communications Status
- Dog/Undog Status

GWE – ENGAGE Gateway Wiring Instructions

Power

- VRCNX-M/R/A powered 12 – 24 VDC
- GWE – ENGAGE Gateway powered by external 24 VDC power supply

VRCNX-M/R/A to GWE – ENGAGE Gateway

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

VRCNX-R/M/A J4 – J11	GWE – ENGAGE Gateway
RXD (A)	TX–
TXD (B)	TX+

VMRC-1/2 to GWE – ENGAGE Gateway

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

VMRC-1 / 1L	VMRC-2 / 2L	GWE – ENGAGE Gateway
TB2-4 (TR+)	TB3-3 (TR+)	TX+
TB2-5 (TR-)	TB3-2 (TR-)	TX-

GWE – ENGAGE Gateway, RM/RU 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) RM/RU or NDE Series devices can communicate with a Gateway on the same channel. The address defined in the Gateway for the RM/RU or NDE devices ranges from 0 to 9. SMS uses an address of 1 through 10.

SMS Addresses Will Always Be 1 Value Higher than the Gateway and RM/RU or NDE Address set via the ENGAGE iOS or Android app. An address of 0 for the Gateway and RM/RU or NDE translates to an address of 1 in SMS. The Gateway will have the same address as the RM/RU or NDE device with the lowest address.

Setting the address of the Gateway requires designation of the range of addresses being used by the RM/RU device that will communicate with the Gateway: designate both a Low and a High address for the RM/RU devices to allow the Gateway to maintain the correct open addresses for the RM/RU devices.

> **Example**: A Gateway is defined which will be supporting 5 devices. 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 devices will be addressed from 0 to 4). SMS configuration will require the Gateway address to be specified as 1 (0 in ENGAGE app + 1) and the devices will be addressed in SMS as 1 through 5.
>
> Additional Gateways on the same controller channel, should be addressed with the next available address and its Low / High range for the devices 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 RM/RU or NDE devices communicating with the 2nd Gateway. Addresses of the 1st Gateway and devices have already been set (see above example). These addresses must be considered when addressing the 2nd Gateway and additional devices. 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 SMS to communicate with the 2nd Gateway at address 6 and the devices communicating with it will be addressed from 6 through 10.

Configuring GWE – ENGAGE Gateway and RM/RU Modules

See documentation provided with the ENGAGE RM/RU option modules for device specific commissioning and linking instructions.

See the Schlage NDE Series Wireless Locks with ENGAGE chapter for detailed instructions for configuring the GWE Gateway and NDE Locks. The process is similar for the ENGAGE RM/RU option modules with any exceptions noted below.

Allegion ENGAGE Account

Process identical to NDE Series devices.

Download ENAGE app

Process identical to NDE Series devices.

Commission / Configure GWE – ENGAGE Gateway

Process identical to NDE Series devices.

Commission ENGAGE RM/RU Modules

> ENGAGE RM/RU Modules 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.

Process identical to NDE Series devices.

Configure Communications Delay and Retry Timing

Process identical to NDE Series devices except as noted below:

- Select “Connect” and “Configure Device”
- Credential Reader Settings are not applicable

> If the Von Duprin ENGAGE RM/RU Modules are not successfully commissioned and configured via the Android or iOS mobile device, the lock(s) will have to be reverted to the Factory Default settings prior to a 2nd attempt to commission. See the ENGAGE RM/RU Installation Instruction Guide for Factory Default Reset instructions.

Define ENGAGE Devices in SMS

A valid, operational VRCNX-R/M/A controller must be defined prior to defining ENGAGE devices in SMS.

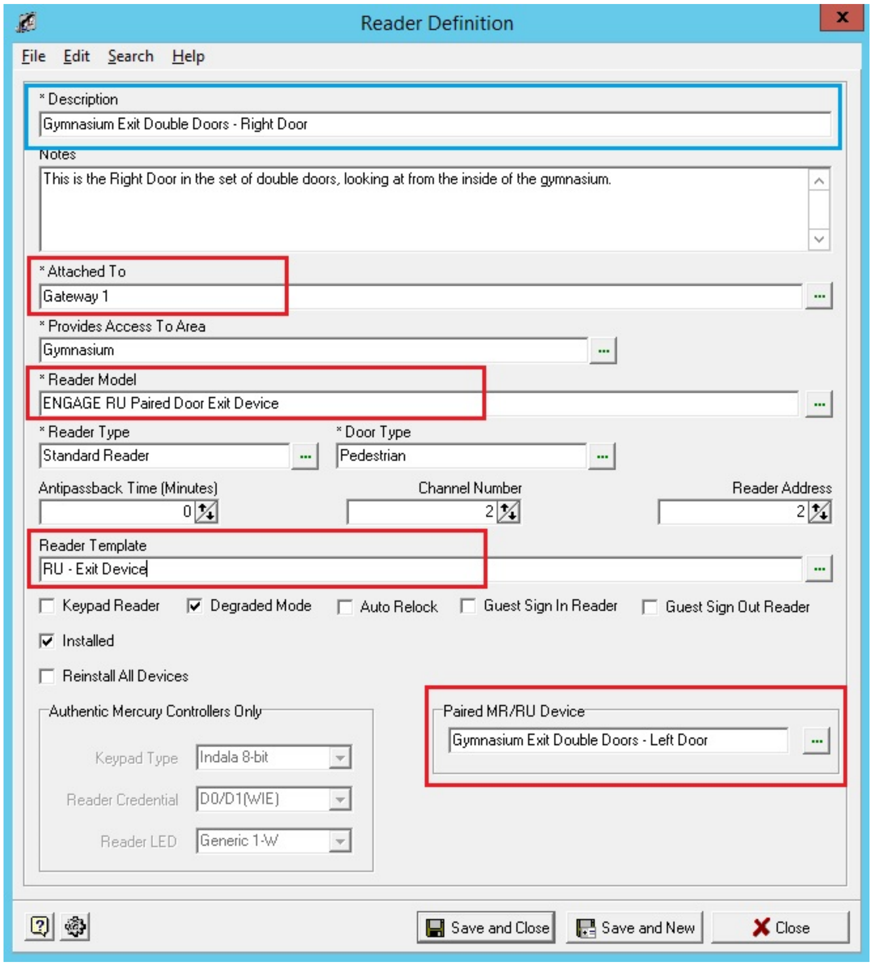
Process identical to NDE Series devices.

Define Gateway

Process identical to NDE Series devices.

Define ENGAGE RM/RU Module

- Highlight a defined GWE – ENGAGE Gateway.
- Click “Edit Readers”.
- Click the “+” symbol in the lower grid menu bar to add a new Reader.
- Select either “ENGAGE RU Exit Device”, “ENGAGE RM Exit Device”, ENGAGE RU Paired Door Exit Device or “ENGAGE RM Paired Exit Device” for the Reader model as appropriate.
- Select appropriate ENGAGE RM or RU Reader template.
- If an ENGAGE RM or RU “Paired Door” device is selected, a new selection will be exposed at the bottom right of the Reader Definition dialog.
    - Select the Paired RM/RU Device installed physically adjacent to the current ENGAGE RM or RU Paired Door device.
    - That there will be no devices available for pairing until at least 2 ENGAGE RU or RM Paired Door Exit Devices are defined **on the same controller** (doors can be paired across different ENGAGE GWE gateways as long as both gateways are attached to the same controller).
    - System Manager will automatically make the matching partner device selection in the partner device Paired RM/RU Device setting so that the paired doors are pointing to each other.
    - Changes to the Paired RM/RU Device setting for either paired device will automatically affect the partner device.
- Set the appropriate Reader Address
- Click “Save and Close” or “Save and New” as required to define additional devices for the Gateway



* Description: Gymnasium Exit Double Doors - Right Door

Notes: This is the Right Door in the set of double doors, looking at from the inside of the gymnasium.

* Attached To: Gateway 1

* Provides Access To Area: Gymnasium

* Reader Model: ENGAGE RU Paired Door Exit Device

* Reader Type: Standard Reader

* Door Type: Pedestrian

Antipassback Time (Minutes): 0

Channel Number: 2

Reader Address: 2

Reader Template: RU - Exit Device

□ Keypad Reader ☑ Degraded Mode □ Auto Relock □ Guest Sign In Reader □ Guest Sign Out Reader

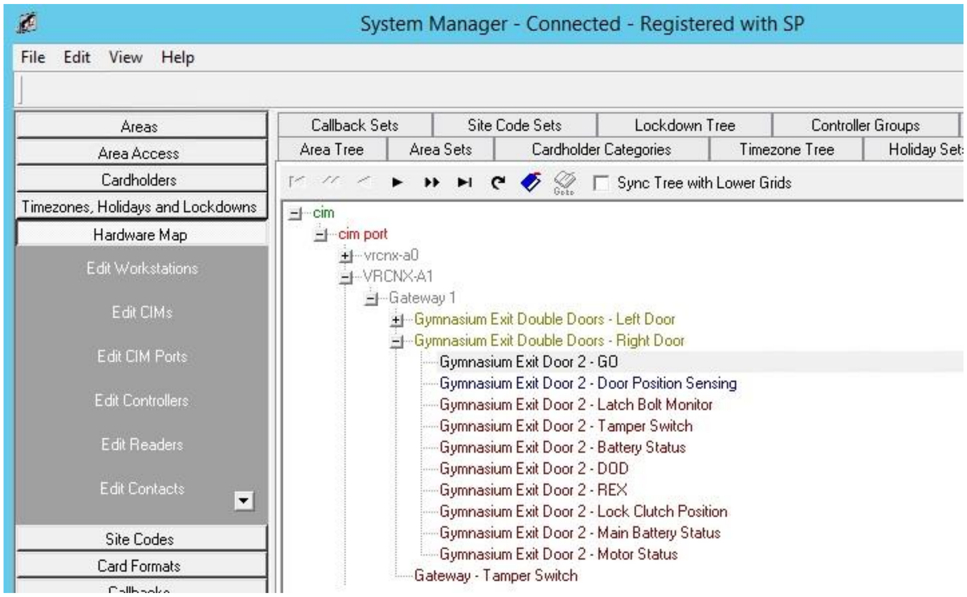
☑ Installed

□ Reinstall All Devices

Authentic Mercury Controllers Only
Keypad Type: Indala 8-bit
Reader Credential: D0/D1(WIE)
Reader LED: Generic 1-W

Paired MR/RU Device: Gymnasium Exit Double Doors - Left Door

- The Gateway and RM/RU devices will be visible in the Hardware Map



```
cim
  cim port
    vrcnx-a0
    VRCNX-A1
      Gateway 1
        Gymnasium Exit Double Doors - Left Door
        Gymnasium Exit Double Doors - Right Door
          Gymnasium Exit Door 2 - GO
          Gymnasium Exit Door 2 - Door Position Sensing
          Gymnasium Exit Door 2 - Latch Bolt Monitor
          Gymnasium Exit Door 2 - Tamper Switch
          Gymnasium Exit Door 2 - Battery Status
          Gymnasium Exit Door 2 - DOD
          Gymnasium Exit Door 2 - REX
          Gymnasium Exit Door 2 - Lock Clutch Position
          Gymnasium Exit Door 2 - Main Battery Status
          Gymnasium Exit Door 2 - Motor Status
        Gateway - Tamper Switch
```

Link ENGAGE RM/RU Modules to GWE – ENGAGE Gateway

Linking the GWE – ENGAGE Gateway and ENGAGE RM/RU devices is accomplished using the Vanderbilt Discovery Tool provided with SMS or the ENGAGE app (see Allegion documentation for this method).

Discovery Tool v1.4.7 or newer is required.

VRCNX-R/M/A Controller firmware v6.65V / v6.87M / v7.16A or newer is required.

Process identical to NDE Series devices.

Schlage LE Series
Wireless Locks with ENGAGE

CHAPTER 30

Schlage LE Series Wireless Lock with ENGAGE Technology

Overview

The LE design packages the mortise lock, credential reader, and access control sensors together in to a small footprint that is both elegant and affordable. They feature two sleek trim options with broad range of decorative lever choices. The LE mortise chassis can be ordered with an interior push button or deadbolt for specific applications. Capability includes the use of both proximity (125 kHz) and/or Smart (13.56 MHz) credentials which feature a much higher level of security and versatility. They connect to SMS via connection to the ENGAGE™ GWE RS-485 gateway similarly to NDE Series locks. LE Series locks can be mixed with ENGAGE RM/RU devices and NDE Series locks on the same GWE Gateway. A maximum of 10 NDE, LE or RM/RU devices can be linked to a single GWE gateway.

Note: Schlage LE Series support requires VRCNX-R/M/A firmware v6.65V / v6.87M / v7.16A or higher installed.

LE Series Components

The Schlage LE Series wireless lock system with ENGAGE technology 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 reader controller (VRCNX-R/M/A or VMRC-1/2) 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 LE Series locks is 30 feet) with which it will communicate wirelessly via Bluetooth.

Gateway (GWE - ENGAGE)

The GWE – ENGAGE works in conjunction with the LE Series locks. The GWE – ENGAGE Gateway is hard wired directly to the VRCNX-R/M/A or VMRC-1/2 reader controller communication channels and communicates via RS-485 protocol. The GWE – ENGAGE can support up to 10 LE Series locks, RM/RU modules or 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-R/M/A*)

Specifications for the GWE – ENGAGE Gateway

- 2.4 GHz Bluetooth v4.0
- Spread spectrum
- Dynamic channel switching (40 channels)
- Range: Up to 30’ line of site to door
- Gateway to Lock Encryption: AES 256-bit
- Certifications: UL294, FCC Part 15, Industry Canada (IC), RoHS
- RS-485 Communication to VRCNX-R/M/A
- Supports 10 RM/RU or NDE Wireless Devices
- VRCNX-R/M/A can support multiple GWE - ENGAGE

Schlage LE Series Wireless Locks

Schlage LE Series wireless locks simplify installation by combining the lock, credential reader, door position sensor and request-to-exit switch all in one unit. LE wireless locks require only minor modifications to existing mechanical mortise prep with no wires to run to the lock or additional hardware necessary. LE is ideal for office and suite entries, conference rooms, common area doors, resident units, and sensitive storage areas with a mortise door prep. Built-in Bluetooth® enables LE wireless locks to connect directly to smart phones and tablets; no need for a proprietary handheld device for set-up and configuration. The GWE – ENGAGE Gateway interfaces to the reader controller (VRCNX-R/M/A or VMRC-1/2) via wired RS-485.

Performance

- Wake Up on Radio - Allows the GWE - ENGAGE to alert the LE Series locks in case of a Lock-out event. Responds to command from SMS within 5 seconds when linked to GWE – ENGAGE Gateway.
- Addressing

- Bluetooth Low Energy v4.2 when used with GWE – ENGAGE Gateway
- Range: up to 30 feet line of site to door

Certifications

- ANSI/BHMA A156.25-2013 (Indoor/Outdoor)
- ANSI/BHMA A156.13-2012, Series 1000, Grade 1
- UL 294
- ULC S319
- UL10C (3-hour fire rated)
- FCC Part 15
- IC RSS-210
- ADA
- RoHS
- ICC ANSI A117.1
- FL3905
- FL12400
- FL14482

Operating voltage

- Power: 4 AA alkaline batteries
- Battery Life: up to 2 years
- The 4 AA batteries will supply 6.0 volts.
    - The locks will continue to operate down to <5.0 volts when Low Battery will be reported.
    - The locks will report Critical Battery at <4.8 volts and into a fail-safe, fail secure or fail as-is mode depending on lock configuration via ENGAGE mobile app.

Operational environment

- Temperature: - 4° to 140° F (-20° to 60°C)
- Humidity: 0% to 100% non-condensing

Available Sensors

- Request-to-Exit
- Door Position
- Interior Cover Tamper
- Battery Status
- Lock/Unlock Status
- Communications Status
- Deadbolt Position Status (MD only)
- Interior Pushbutton Status (MB only)

GWE – ENGAGE Gateway Wiring Instructions

Power

- VRCNX-M/R/A powered 12 – 24 VDC

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

VRCNX-M/R/A to GWE – ENGAGE Gateway

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

VRCNX-R/M/A J4 – J11	GWE – ENGAGE Gateway
RXD (A)	TX–
TXD (B)	TX+

VMRC-1/2 to GWE – ENGAGE Gateway

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

VMRC-1 / 1L	VMRC-2 / 2L	GWE – ENGAGE Gateway
TB2-4 (TR+)	TB3-3 (TR+)	TX+
TB2-5 (TR-)	TB3-2 (TR-)	TX-

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 Series, RM/RU or NDE Series devices can communicate with a Gateway on the same channel. The address defined in the Gateway for the LE, RM/RU or NDE devices ranges from 0 to 9. SMS uses an address of 1 through 10.

SMS Addresses Will Always Be 1 Value Higher than the Gateway and LE, RM/RU or NDE Address set via the ENGAGE iOS or Android app. An address of 0 for the Gateway and LE, RM/RU or NDE translates to an address of 1 in SMS. The Gateway will have the same address as the LE, RM/RU or NDE device with the lowest address.

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

Example: A Gateway is defined which will be supporting 5 devices. 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 devices will be addressed from 0 to 4). SMS configuration will require the Gateway address to be specified as 1 (0 in ENGAGE app + 1) and the devices will be addressed in SMS as 1 through 5.

Additional Gateways on the same controller channel, should be addressed with the next available address and its Low / High range for the devices 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, RM/RU or NDE devices communicating with the 2nd Gateway. Addresses of the 1st Gateway and devices have already been set (see above example). These addresses must be considered when addressing the 2nd Gateway and additional devices. 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 SMS to communicate with the 2nd Gateway at address 6 and the devices communicating with it will be addressed from 6 through 10.

Configuring GWE – ENGAGE Gateway and LE Series Locks

See documentation provided with the LE Series wireless locks for device specific commissioning and linking instructions.

See the Schlage NDE Series Wireless Locks with ENGAGE chapter for detailed instructions for configuring the GWE Gateway and NDE Locks. The process is similar for the LE Series wireless locks with any exceptions noted below.

Allegion ENGAGE Account

Process identical to NDE Series devices.

Download ENAGE app

Process identical to NDE Series devices.

Commission / Configure GWE – ENGAGE Gateway

Process identical to NDE Series devices.

Commission LE Series Locks

LE Series wireless 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.

Process identical to NDE Series devices.

Configure Communications Delay and Retry Timing

Process identical to NDE Series devices.

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

Define ENGAGE Devices in SMS

A valid, operational VRCNX-R/M/A controller must be defined prior to defining ENGAGE devices in SMS.

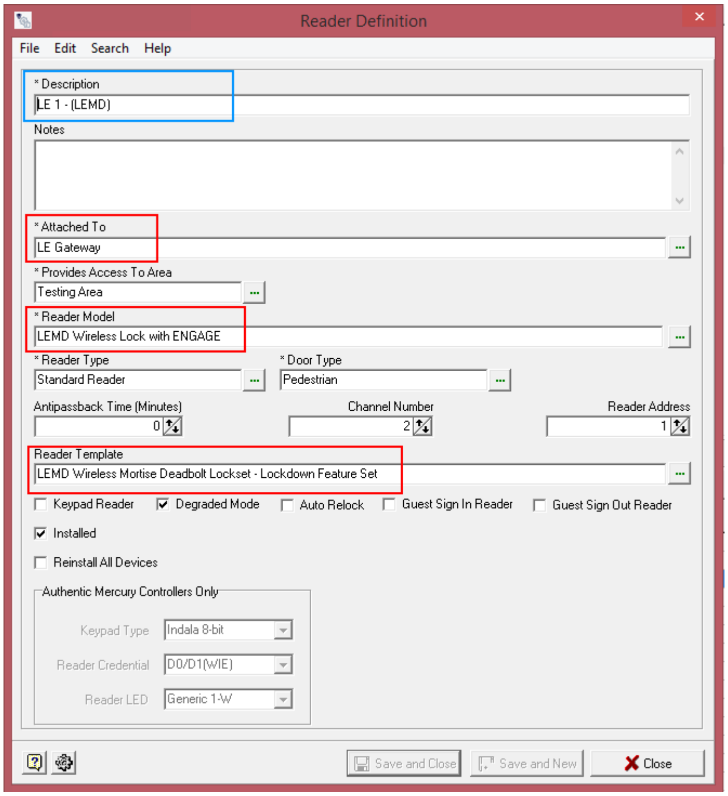
Process identical to NDE Series devices.

Define Gateway

Process identical to NDE Series devices.

Define LE Series Wireless Lock

- Highlight a defined GWE – ENGAGE Gateway.
- Click “Edit Readers”.
- Click the “+” symbol in the lower grid menu bar to add a new Reader.
- Select either the appropriate LE Series wireless lock.
- Select the appropriate Le Series Reader Template.
- Set the appropriate Reader Address
- Click “Save and Close” or “Save and New” as required to define additional devices for the Gateway



* Description: LE 1 - (LEMD)

Notes:

* Attached To: LE Gateway

* Provides Access To Area: Testing Area

* Reader Model: LEMD Wireless Lock with ENGAGE

* Reader Type: Standard Reader

* Door Type: Pedestrian

Antipassback Time (Minutes): 0

Channel Number: 2

Reader Address: 1

Reader Template: LEMD Wireless Mortise Deadbolt Lockset - Lockdown Feature Set

□ Keypad Reader ☑ Degraded Mode □ Auto Relock □ Guest Sign In Reader □ Guest Sign Out Reader

☑ Installed

□ Reinstall All Devices

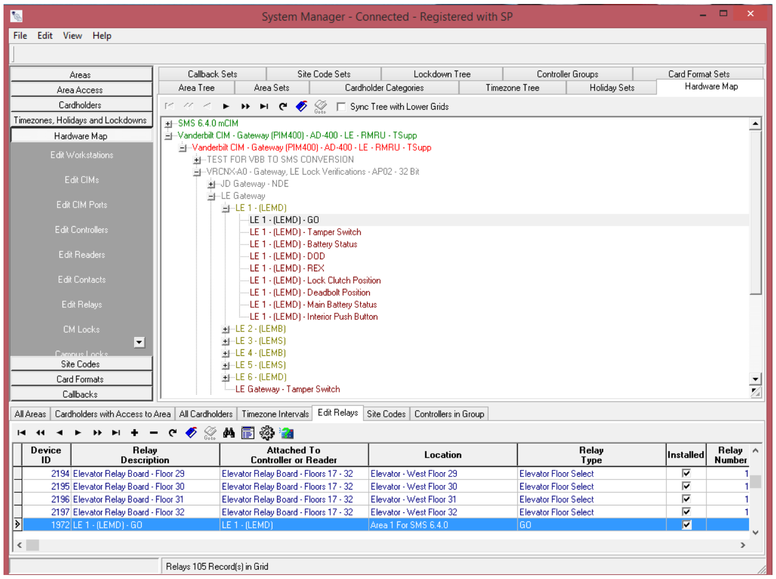
Authentic Mercury Controllers Only

Keypad Type: Indala 8-bit

Reader Credential: D0/D1(WIE)

Reader LED: Generic 1-W

- The Gateway and LE Series wireless locks will be visible in the Hardware Map



```
SMS 6.4.0 mCIM
Vanderbilt CIM - Gateway (PIM400) - AD-400 - LE - RMRU - TSupp
  Vanderbilt CIM - Gateway (PIM400) - AD-400 - LE - RMRU - TSupp
    TEST FOR VBB TO SMS CONVERSION
    VRCNX-A0 - Gateway, LE Lock Verifications - AP02 - 32 Bit
      JD Gateway - NDE
      LE Gateway
        LE 1 - (LEMD)
          LE 1 - (LEMD) - GO
          LE 1 - (LEMD) - Tamper Switch
          LE 1 - (LEMD) - Battery Status
          LE 1 - (LEMD) - DOD
          LE 1 - (LEMD) - REX
          LE 1 - (LEMD) - Lock Clutch Position
          LE 1 - (LEMD) - Deadbolt Position
          LE 1 - (LEMD) - Main Battery Status
          LE 1 - (LEMD) - Interior Push Button
        LE 2 - (LEMB)
        LE 3 - (LEMS)
        LE 4 - (LEMB)
        LE 5 - (LEMS)
        LE 6 - (LEMD)
        LE Gateway - Tamper Switch
```

Device ID	Relay Description	Attached To Controller or Reader	Location	Relay Type	Installed	Relay Number
2194	Elevator Relay Board - Floor 29	Elevator Relay Board - Floors 17 - 32	Elevator - West Floor 29	Elevator Floor Select	☑	1
2195	Elevator Relay Board - Floor 30	Elevator Relay Board - Floors 17 - 32	Elevator - West Floor 30	Elevator Floor Select	☑	1
2196	Elevator Relay Board - Floor 31	Elevator Relay Board - Floors 17 - 32	Elevator - West Floor 31	Elevator Floor Select	☑	1
2197	Elevator Relay Board - Floor 32	Elevator Relay Board - Floors 17 - 32	Elevator - West Floor 32	Elevator Floor Select	☑	1
1972	LE 1 - (LEMD) - GO	LE 1 - (LEMD)	Area 1 For SMS 6.4.0	GO	☑	

Relays 105 Record(s) in Grid

Link LE Series Wireless Locks to GWE – ENGAGE Gateway

Linking the GWE – ENGAGE Gateway and LE Series wireless locks is accomplished using the Vanderbilt Discovery Tool provided with SMS or the ENGAGE app (see Allegion documentation for this method).

Discovery Tool v1.4.7 or newer is required.

VRCNX-R/M/A Controller firmware v6.65V / v6.87M / v7.16A or newer is required.

Process identical to NDE Series devices.

CHAPTER 31

Schlage Wireless Readers

Wireless reader

Overview

Schlage wireless devices can be seamlessly integrated to your SMS system. The PIM-485-OTD communicates directly to the VRCNX-R/M/A or SRCNX (Legacy) via RS-485 protocol and can support up to 15 Schlage wireless devices. Specifications and guidelines for configuring the wireless devices are in the pages that follow.

Abbreviations

Terms and description

Term	Description
PIM	Panel Interface Module
WAPM	Wireless Access Point Module
MIRL	Modular Integrated Reader Lock
WRI	Wireless Reader Interface
WPR	Wireless Portable Reader
WSM	Wireless Status Monitor
WTK	Wireless Test Kit

The Schlage Wireless Access product line contains several expressions of the same module.

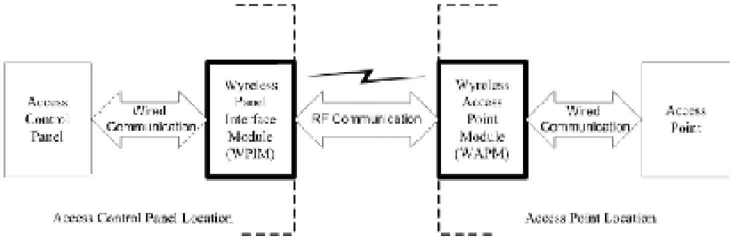
Wireless Access Modules

Name	Acronym	Type
Panel Interface Module	PIM	WPIM
Modular Integrated Reader Lock	MIRL	WAPM
Out/In Wireless Reader Interface	WRI-Out/In-12	WAPM
Wireless Portable Reader Version 2	WPR 2	WAPM
Wireless Status Monitor	WSM	

Schlage wireless system components

There are various wireless devices that are used to integrate with the Vanderbilt Security Management System. The Schlage wireless system contains two different types of modules:

- One wireless panel interface module (WPIM or PIM)
- One wireless access point module (WAPM)



Wireless system block diagram

The WPIM (PIM-485-OTD) is hard wired to the reader controller communication channels via RS-485 protocol. The WPIM (TD-2/TD-4) are hard wired to the reader interfaces (VRINX) reader port via RS-485 protocol to the reader controller. The WPIM 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 and WPIM are used, the communication link is always RF.

Schlage wireless modules

There are several types of Wireless Access Point Modules (WAPM) and Panel Interface Modules (PIM) provided by Schlage: the MIRL, WPR, WRI, and WSM along with the PIM-485-OTD and PIMTD2/TD4. The following sections detail each one of these modules.

Wireless Panel Interface Modules TD2 and TD4

The PIM-TD2/TD4 works in conjunction with several types of wireless peripherals devices. The TD-2 and the TD-4 modules hard wire to the reader interfaces (VRINX). The reader interface then communicates to the VRCNX-R/M/A or SRCNX (Legacy) reader controller via RS-485 protocol.

The PIM is capable of configuring the following items:

- Heartbeat interval (The resolution and maximum time of the heartbeat interval are WAPM dependent, refer to each WAPM for details)
- 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-TD2/TD4 shall accept card formats up to 255 bits via the VRINX.

Operational environment

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

Power Source

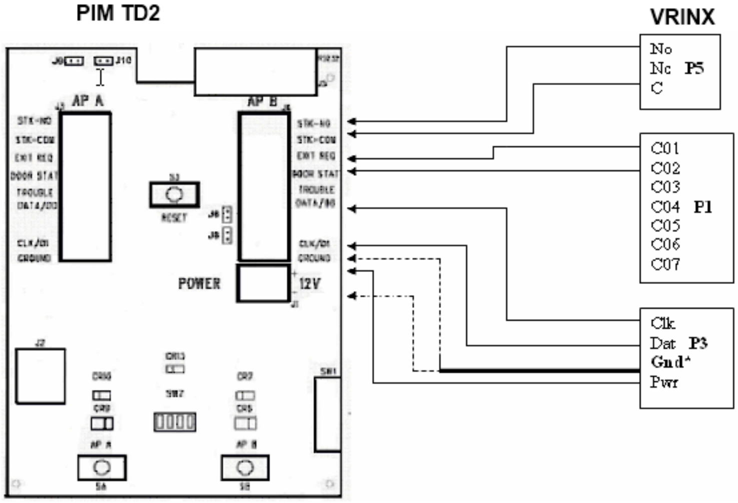
- Power Requirements -12VDC power supply (cannot be powered from the VRCNX-R/M/A)
- Operating Voltage - 7.5 to 14.0 VDC

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 TD2 and the expansion module (PIM EXP) are capable of accommodating Remote Antenna Modules.

Specifications for the PIM TD2

- PIM TD2/TD4 distance from VRINX is 500 feet. (refer to the Recommended Wire Chart)
- VRINX is supported by the VRCNX-R/M/A series reader controllers
- Wiegand Output to VRINX
- Supports 2 Wireless Devices
- PIM distance from Wireless Readers - 200 feet. Radius or 1000 to 4000 feet. line of sight with optional Long-Range Antenna



Gnd* - Two connections must be made from P3 on VRINX to PIM TD2 (ground & *-12VDC*

Wireless Panel Interface Module (WPIM PIM-485-OTD)

The PIM-485-OTD works in conjunction with several types of wireless peripherals devices. The PIM-485-OTD module is hard wired directly to the VRCNX-R/M/A or SRCNX (Legacy) reader controller communication channels via RS-485 protocol. The PIM-485-OTD can support up to 15 wireless devices.

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-485-OTD 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 Must use external power supply.
  (Cannot be powered from the VRCNX-R/M/A)

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 PIM485-OTD and the expansion module (PIM EXP) are capable of accommodating Remote Antenna Modules.

Specifications for the PIM-485-OTD

- RS-485 Communication to VRCNX-R reader controller
- Supports 15 Wireless Devices
- VRCNX-R can support multiple PIM-485-OTD
- Up to 16 devices total on the VRCNX-R/M/A including PIM-485-OTD

Wireless Access Point Module (WAPM)

There are several types of WAPM modules provided by **Schlage** such as the MIRL, WPR, WRI, and WSM. The following sections detail each one of these modules.

Modular Integrated Reader Lock (MIRL)

The Modular Integrated Reader Lock (MIRL) is a product in the Schlage Wireless Access Point Module (WAPM) category. Schlage Wireless Modular Locksets 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 to VRCNX-R/M/A or SRCNX (Legacy).

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, iCLASS & Indala 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 Schlage wireless modular lockset 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 Wireless Modular Locksets provide a way to lock or unlock a door and monitor access from a remote location. Schlage Wireless locks are fail-safe from the protected side of the door. These locksets are controlled by the Vanderbilt Security Management System.

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 an 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 Wireless Modular Lockset 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 Schlage Wireless Modular Lockset 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 TD2 and the expansion module (PIM EXP) are capable of accommodating Remote Antenna Modules.

Range - The Schlage Wireless Modular Lockset can have a range up to 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
- Wiegand technology to external reader

Wireless Portable Reader (WPR2)

The WPR2 contains all of the elements needed to read an access control card, transmit the card data to a PIM via an RF link and indicate if the card is valid, determined by VRCNX-R/M/A. The WPR2 includes a power supply (battery pack), a card reader, visual/audible indicators and an RF transceiver for communicating with another RF transceiver in a Panel Interface Module (PIM) which interfaces to VRCNX-R/M/A or SRCNX (Legacy).

Performance

- Verification Time - Less than 0.10 second (not including panel delays)
- Communications (Heartbeat) Interval - Configurable in 15 second increments from 15 seconds to 273 hours
- Addressing - Automatic during Linking
- Battery operated
- Red and Green Led operation
- Used for Extending Perimeter, Mustering and Bus Operations

Card formats

- The WPR2 can read all card formats up to 255 bits.

Operational environment

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

Power source

- The WPR2 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 polarized connectors.
- Operating Voltage - 5.5 to 13.2 VDC
- Battery Life - The WPR2 battery pack is capable of providing power for two and one-half years with 40,000 card swipes/presentations per year with a ten-minute heartbeat period. It provides power for three and one-half 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 modules and the expansion modules (PIM EXP) are capable of accommodating Remote Antenna Modules.

Wireless Reader Interface (WRI - Indoor or Outdoor)

The WRI-IN/OUT-12VDC acts as a remote card reading device that communicates via RF with the VRCNX-R/M/A or SRCNX (Legacy) reader controller, 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.
- Elevator Control – WRI/OTD with Optional Long-Range Antenna
- 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
- 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 and the expansion modules (PIM EXP) are capable of accommodating Remote Antenna Modules.

Wireless Status Monitor (WSM)

The WSM contains all of the elements needed to electronically monitor a dry contact via an RF link to a PIM. The WSM includes a power supply (battery pack), terminals for monitoring a dry contact switch/sensor, and an RF transceiver for communicating with another RF transceiver in a Panel Interface Module (PIM) which interfaces to the VRCNX-R/M/A or SRCNX (Legacy) reader controller.

Performance

- Reporting Time - Less than 0.1 second not including access panel delays
- Communications (Heartbeat) Interval - Configurable in 15 second increments from 15 seconds to 273 hours
- Addressing - Automatic during Linking

Operational environment

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

Power source

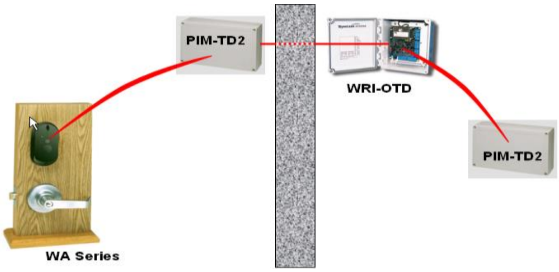
- The Schlage Wireless WSM uses 8 no-button AA alkaline cells welded together into a battery pack insulated with a shrink-wrap wrapper. It has two wire leads and a polarized connector compatible with connectors.
- Operating Voltage - 5.5 to 13.2 VDC
- Current Requirements - Standby - 55 micro Amps typical (Proximity version), Maximum - 400mA peak (transmitting)
- Battery Life - Battery life is up to five (5) years.

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 TD2 and the expansion module (PIM EXP) are capable of accommodating Remote Antenna Modules.

Repeaters

Repeaters are used for outdoor applications where moving objects such as trees may interfere with line of sight installations.



Device capacities

PIM-485-TD2 modules

- Contact 1 - PIM module Tamper state – NC

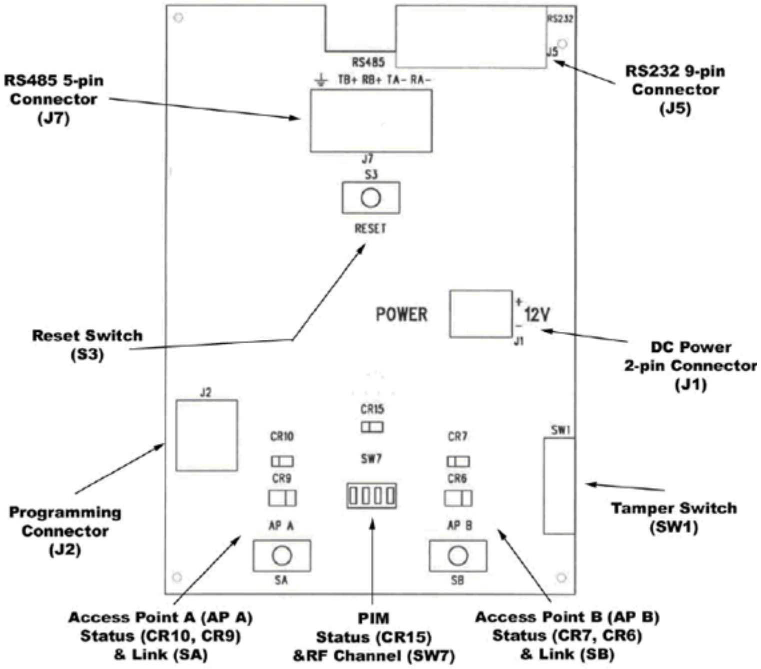
WAPM modules

- Relay 1 for the lock
- Relay 1 state will be reported back to VRCNX-R/M/A reader controller
- Relay 2 for Aux Relay - WRI only
- Relay 2 state will not be reported to the VRCNX-R/M/A reader controller
- Contact 1 for REX – Normally Open, Non-supervised
- Contact 2 for DOD – Normally Closed, 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

WSM modules

- Rex
- DOD
- Tamper
- Request to enter

Wiring instructions


RS232
J5
RS485
TB+ RB+ TA- RA-
J7
S3
RESET
POWER
+
12V
-
J1
J2
CR15
CR10
CR7
SW7
SW1
CR9
CR6
AP A
AP B
SA
SB
RS485 5-pin Connector (J7)
RS232 9-pin Connector (J5)
Reset Switch (S3)
DC Power 2-pin Connector (J1)
Programming Connector (J2)
Tamper Switch (SW1)
Access Point A (AP A) Status (CR10, CR9) & Link (SA)
PIM Status (CR15) &RF Channel (SW7)
Access Point B (AP B) Status (CR7, CR6) & Link (SB)

All Schlage wireless devices should be powered separately with a 12VDC power supply. They cannot be powered from the VRCNX-R/M/A or SRCNX (Legacy). The communication between VRCNX-R/M/A or SRCNX (Legacy) reader controller and the PIM-485-TD2 is via RS-485 protocol.

Wiring between Reader Controller and PIM Module

VRCNX-R/M/A or SRCNX (Legacy) - PIM

Reader Controller J4 – J11	PIM-485-TD2 J7
RXD (A)	TA- RA-
TXD (B)	TB+ RB+

Jumper between (TA-RA-) and (TB+RB+)

Wireless reader modules configuration

The Schlage Utility Software (SUS) located on the HHD (Hand Held Device) must be used to configure and set the address of each PIM-485-OTD. All PIM module must be address sixteen (16) in the Vanderbilt Security Management System.

A maximum of fifteen (15) wireless readers can communicate with a PIM module on the same channel, with all reader types. Address can be 1 through 15 which is set as 0 to 14 by the SUS.

Example - if a WAPM is configured as address 5 in the SUS then its corresponding address in SMS software reader definition is 6.

Linking and addressing locks to the WPIM

Requirements - A RS232 to USB adapter is required to connect the HHD to the WPIM.

Configuring WPIM

1. The WPIM must be paired to the HHD.
2. Log in to the SUS software. (Refer to the SUS User Guide for log-in procedure.)
3. Connect the HHD to the PIM using the RS232 adapter cable.
4. Click on the **Options** button at the bottom of the HHD screen. A list of options will open.
5. After this connection is made, hold down one of the PIM link switches (SA – SB). Continue to hold the link switch and press the reset button (S3). You must hold down the link switch until the firmware version is displayed and the communication is restored. The LED's (CR6 – 10) on the PIM starts flashing telling you the firmware version of the PIM. When completed, (CR7 and 10) will continue to flash RED and CR15 will continue to blink GREEN. The PIM is now in Pairing Mode.
6. On the HHD click the **Pair PDA to Device** option. A pop-up will display when the pairing process is complete.
7. The PIM-485-TD2 will be defaulted to address sixteen (16) in the Vanderbilt SMS Software.

Configuring the WRI

Configuration of the WRI is accomplished by the SUS while the HHD is connected to the PIM. After the PIM has been configured you can Link WRI modules to it and address them.

Follow these steps to place the WRI into the Link Mode in order to setup proper address in the SUS. There are two WRI models; WRI -OTD and WRI - IN.

1. Go to the Link tab in SUS.
2. Using the **Select Door** drop down to set the address of the WRI.

   Note: Wireless Address selections start at address 0. Security Management System software addresses start at address 1.

3. Click the **Link** button.
4. Place the WRI-OTD into the link mode by pressing reset switch.
5. Place the WRI-IN into the link mode by recycling power.
6. Click **Stop** on the SUS. The WRI is now linked to this PIM with the specified address.
7. Go to **Device Options>Lock Properties**.

8 Click on the **Edit** tab. This tab is where the Heartbeat / First / Delay / Retry / FC Mode or Card Number Mode are set.

Note: The Heartbeat default will be set to 10 minutes, but you will need to change the First & Delay settings to 300 and the Retry to 7. This configuration needs to be set to run properly using the SMS software.

- The Heart Beat is used for communication from the WRI back to the PIM.
- The First / Delay and Retry settings should be set to our recommended defaults.
- FC or Card Number Mode / Auto Purge can be set for Degraded Mode

9 When settings are complete, you must click on the Save button at the bottom of the SUS. You may need to produce a transaction in order for these settings to be sent to the WRI.

10 At this point you have completed the configuration of your WRI, if you are going to set up another WRI you will need to select the next panel address available and follow the previous procedures.

Disconnecting WRI from the link mode

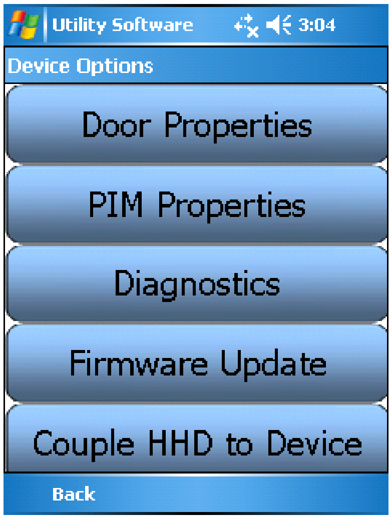
1 To disconnect WRI from the link mode, close the SUS application.

Configuring MIRL

Follow these steps to place the MIRL into the Link Mode in order to setup the address

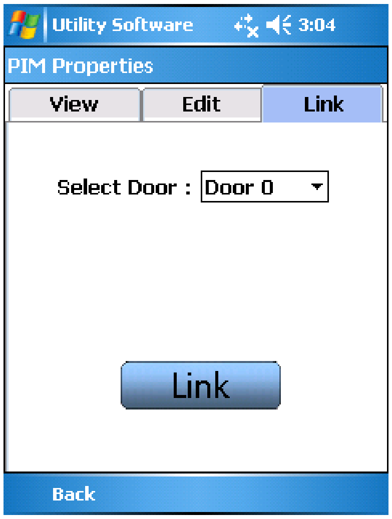
1 Once the PIM has been Paired with the HHD, connect the HHD to the PIM using the RS232 adapter cable.

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



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

4 Go to the **Link** tab.



5 Using the Select Door drop down, set the address of the MIRL.

Note: Wireless address selections start at address zero (0) and the Security Management System software addresses start at address one (1).

6 When the address has been specified, click the **Link** button.

7 Put the MIRL in linking mode:

a) On the MIRL, activate the Exit Request handle and hold down while presenting a card reader to the reader.

b) Continue holding down the Exit Request for approximately 15 seconds. You will then see the LED on the MIRL blinking Green very rapidly.

c) You may now release the Exit Request Handle. 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.

8 Go to **Device Options>Lock Properties** and click on the **Edit** tab to set the Heartbeat / First / Delay / Retry / FC Mode.

Note: The Heartbeat default will be set to 10 minutes, but you will need to change the First & Delay settings to 300 and the Retry to 7. This configuration needs to be set to run properly using the Access control system software.

- The Heart Beat is used for communication from the MIRL back to the PIM.
- The First / Delay and Retry settings should be set to our recommended defaults.
- FC mode can be set for Degraded Mode.

9 When settings are complete, you must click on the **Save** button at the bottom. You may need to produce a transaction in order for these settings to be sent to the MIRL.

Disconnecting MIRL from the link mode

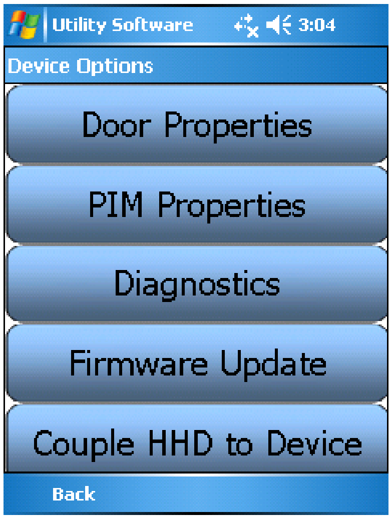
1 To disconnect MIRL from the link mode, close the SUS application.

Configuring WPR2

Follow these steps to place the WPR2 in to Link Mode in order to setup the address.

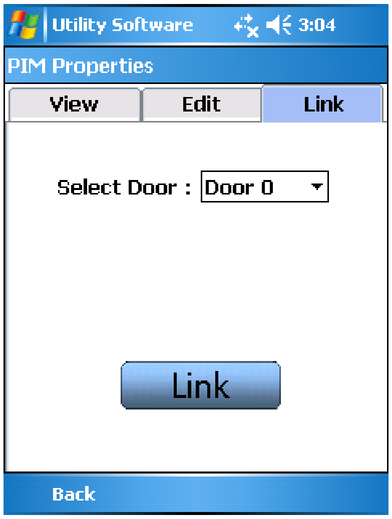
1 Once the PIM has been Paired with the HHD, connect the HHD to the PIM using the RS232 adapter cable.

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



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

4 Go to the **Link** tab.



Select Door : Door 0

5 Using the Select Door drop down, set the address of the WPR2.

Note: Wireless address selections start at address zero (0) and the **Vanderbilt SMS** software addresses start at address one (1).

6 When the address has been selected, click the **Link** button.

7 Put the WPR2 in linking mode:

a) On the WPR2, activate the Reset Switch. You will then see the LED on the WPR2 blinking Green very rapidly. 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.

8 Go to **Device Options>Lock Properties** and click on the **Edit** tab to set the Heartbeat / First / Delay / Retry / FC Mode.

Note: The Heartbeat default will be set to 10 minutes, but you will need to change the First & Delay settings to 300 and the Retry to 7. This configuration needs to be set to run properly using the Vanderbilt Security Management System software.

- The Heart Beat is used for communication from the WPR2 back to the WPIM.
- The First / Delay and Retry settings should be set to our recommended defaults.
- FC mode can be set for Degraded Mode

9 When settings are complete, you must click on the **Save** button at the bottom. You may need to produce a transaction in order for these settings to be sent to the WPR2.

Disconnecting WPR2 from the link mode

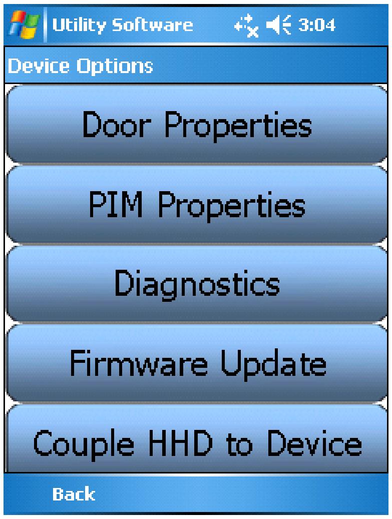
1 To disconnect WPR2 from the link mode, close the SUS application.

Configuring WSM

Follow these steps to place the WSM in to Link Mode in order to setup the address.

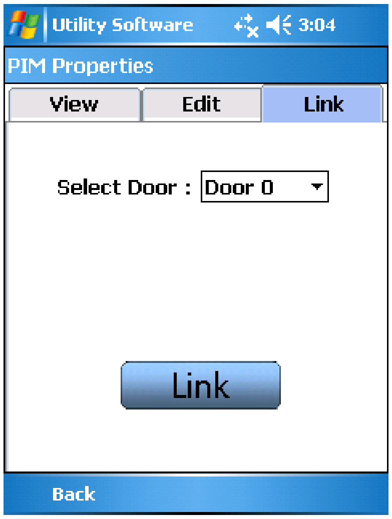
1 Once the PIM has been Paired with the HHD, connect the HHD to the PIM using the RS232 adapter cable.

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



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

4 Go to the **Link** tab.



Select Door : Door 0

Link

5 Using the Select Door drop down, set the address of the WSM.

Note: Wireless address selections start at address zero (0) and the **Vanderbilt SMS** software addresses start at address one (1).

6 When the address has been specified, click the **Link** button.

7 Put the WSM in linking mode:

a) On the WPR2, activate the Reset Switch. You will then see the LED on the WSM blinking Green very rapidly. 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.

8 Go to **Device Options>Lock Properties** and click on the **Edit** tab to set the Heartbeat / First / Delay / Retry / FC Mode.

Note: The Heartbeat default will be set to 10 minutes, but you will need to change the First & Delay settings to 300 and the Retry to 7. This configuration needs to be set to run properly using the Vanderbilt Security Management System software.

- The Heart Beat is used for communication from the WSM back to the WPIM.
- The First / Delay and Retry settings should be set to our recommended defaults.
- FC mode can be set for Degraded Mode

9 When settings are complete, you must click on the **Save** button at the bottom. You may need to produce a transaction in order for these settings to be sent to the WSM.

Disconnecting WSM from the link mode

1 To disconnect WSM from the link mode, close the SUS application.

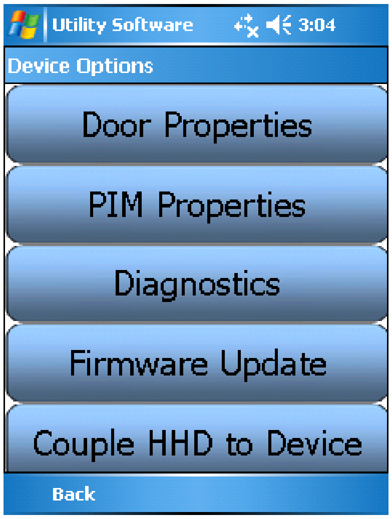
Linking Diagnostics

Follow the steps below to determine if you have correctly linked your wireless module to your PIM:

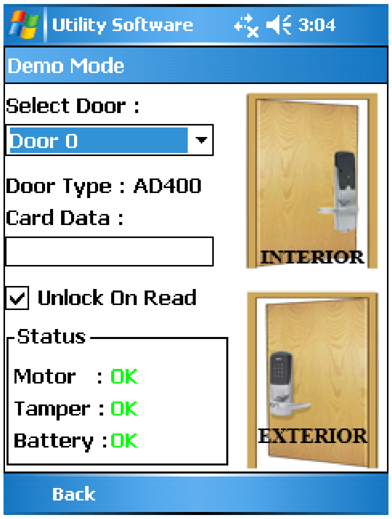
1 Log in to SUS (see steps above).

2 Connect the HHD to the PIM using the RS232 adapter.

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



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



Select Door :
Door 0

Door Type : AD400
Card Data :

☑ Unlock On Read

Status
Motor : OK
Tamper : OK
Battery : OK

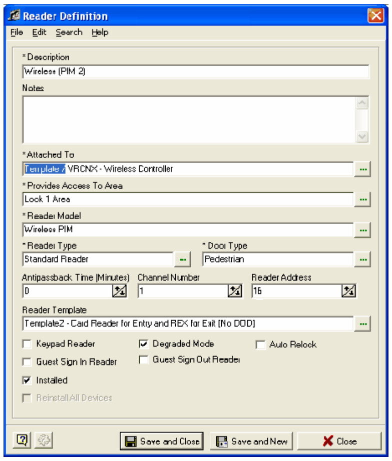
5 Using the **Select Door** drop down, select the address of the module you wish to test.

6 If the **Status** section shows **OK**, then you have successfully linked the wireless module.

Software configuration

The **Vanderbilt SMS** software has to be set up accordingly to integrate the wireless readers. The wireless readers can be defined using the System Manager module.

Wireless PIM (Panel interface module) reader definition



*Description: Wireless (PIM 2)

Notes:

*Attached To: Template / VRCNX - Wireless Controller

*Provides Access To Area: Lock 1 Area

*Reader Model: Wireless PIM

*Reader Type: Standard Reader

*Door Type: Pedestrian

Antipassback Time (Minutes): 0

Channel Number: 1

Reader Address: 16

Reader Template: Template2 - Card Reader for Entry and REX for Exit (No DOD)

□ Keypad Reader ☑ Degraded Mode □ Auto Relock

□ Guest Sign In Reader □ Guest Sign Out Reader

☑ Installed

□ Reinstall All Devices

1 **Description** - Enter the description of the PIM reader.

2 **Attached to** - Select the controller that the PIM is attached to.

3 **Provides Access to the Area** - Set as Offsite or an area that the reader is providing access.

4 **Reader Model**- Select wireless PIM as the reader model.

5 **Reader Type** - Select Standard Reader as the reader type.

6 **Door Type** - This selection depends on the type of door that you are securing.

7 **Antipassback Time** - N/A

8 **Channel Number** - Select the channel number that you are using to connect the PIM.

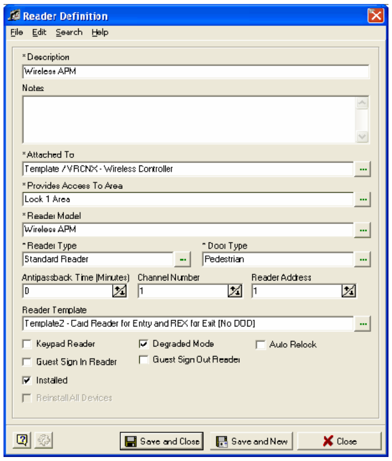
9 **Reader Address** - The reader address must be set to 16.

10 **Reader Template** - No template

11 **Installed** - Select the check box to install the reader.

12 **Click Save and Close** to save the definition. Click **Save and New** to save the definition and create a new one. Click **Close** to close the window without saving your changes.

Wireless APM reader definition (WAPM)



*Description: Wireless APM

Notes:

*Attached To: Template / VRCNX - Wireless Controller

*Provides Access To Area: Lock 1 Area

*Reader Model: Wireless APM

*Reader Type: Standard Reader

*Door Type: Pedestrian

Antipassback Time (Minutes): 0

Channel Number: 1

Reader Address: 1

Reader Template: Template2 - Card Reader for Entry and REX for Exit (No DOD)

□ Keypad Reader ☑ Degraded Mode □ Auto Relock

□ Guest Sign In Reader □ Guest Sign Out Reader

☑ Installed

□ Reinstall All Devices

1. **Description** - Enter the description of the WAPM reader.
2. **Attached to** - Select the controller that the WAPM is attached to.
3. **Provides Access to the Area** - Set as Offsite or specify an area that the reader provides access.
4. **Reader Model**- Select Wireless APM as the reader model.
5. **Reader Type** - Select Standard Reader as the reader type.
6. **Door Type** - This selection depends on the type of door that you are securing.
7. **Antipassback Time** - Please refer to Vanderbilt Security Management System software user manual>System Manager>Reader Definition chapter for further information.
8. **Channel Number** - You need to connect the WAPM to the same channel that you used for PIM. E.G If you have connected the PIM to channel 1 the WAPM must be connected to channel 1.
9. **Reader Address** - Set the reader address using the up and down arrows. It can be any number between 1 to 15.
10. **Reader Template** - No template
11. **Installed** - Select the check box to install the reader.
12. **Degrades Mode-** A Wireless Access Point Module (WAPM) can be configured and used in Degraded Mode when the WAPM can only communicate with its host system due to some type of system failure. WAPMs uses a Cache Memory (CM) concept to implement local access control decisions within the WAPM when the WAPM is in degraded mode.

Enabling Degraded Mode

1. The degraded mode is enabled using the SUS. By setting the Data Bits field in the **Edit Tab** to a non-zero value. The value entered in the field determines which cards will be checked for CM entry/validation. For a Wiegand type card, the value entered is the number of bits of the card. For a magstripe type card, the value entered is the number of total encoded digits times 4 (4 bits per digit, not including starting and ending sentinel characters).
2. **Two CM Options** - When enabled, the CM operations in one of two modes - Facility Code or Card Number.
3. **Facility Code Mode** - In its degraded mode, a WAPM will momentarily unlock the door whenever a card is presented whose facility code matches a facility code stored in the WAPM’s CM. A facility code is stored when a card with the facility code is granted during normal system operation. Currently there are three Proximity card formats that can be used in Facility Code Mode - 26-bit, 34-bit and 37-bit cards.
   - For 26-bit cards, 8 bits (bit 2 to bit 9) are extracted as card facility code
   - For 34-bit and 37-bit cards, 16 bits (bit 2 to bit 17) are extracted as card facility code
   - Any other proximity cards are not supported in Facility Code Mode
   - Each WAPM can store multiple facility codes and the exact number can be stored depending on the number of bits in a facility code.
   - For 26-bit cards, maximum 56 facility codes can be stored in CM
   - For 34-bit or 37-bit cards, maximum 44 facility codes can be stored in CM
4. **Card Number Mode** - In its degraded mode, a WAPM will momentarily unlock the door whenever a card is presented whose bit pattern matches a pattern that is stored in the WAPM’s CM. A card pattern is stored when a card is granted during normal system operation. Each WAPM can store multiple card number and the exact number can be stored depending on the number of bits on each card.
   - For 26-bit cards, maximum 32 card patterns can be stored in CM
   - For 34-bit cards, maximum 28 card patterns can be stored in CM
   - For 35-bit cards, maximum 28 card patterns can be stored in CM
   - For 37-bit cards, maximum 28 card patterns can be stored in CM

- If the WAPM's CM is full and a new card is access granted, the oldest facility code (or card number) in the CM is removed and the new one is stored
- If the FC Mode is unchecked then that WAPM'S CM will operate in the card number mode

5 Click **Save and Close** to save the definition. Click **Save and New** to save the definition and create a new one. Click **Close** to close the window without saving your changes

Programming Conventions

1 When programming the Activation time for the go relay on the WAPM, regardless of what time has been entered into the Trigger definitions, the Relay released time will be displayed 3 to 4 seconds after the Relay Energized transaction had been received. The physical hardware activation and release of the go relay will follow the programmed times

2 When programming the Activation time for the go relay on the APM, you must not set any of the triggers with duration set to zero. It won't activate the relay.

3 ARO / MRO feature with Wireless Readers that are running using Battery or AC power.

4 Readers models WRI – IN / OTD can be set to use ARO / MRO since they are running using 12VDC power supply, so the heartbeat can be set to 10 seconds for constant communication between the WPIM and WRI – OTD reader. By setting the heartbeat to 10 seconds you will be able to perform a manual override (MRO) or automatic override (ARO) with a max latency of only 10 seconds for each send command.

5 Reader models that are running with battery, the default heart beat is set to 10 minutes. For battery life expectancy the wireless reader will communicate back to the PIM every 10 minutes to pull information, so it does not waste the battery. Using the Manual Override (MRO) with readers using batteries it could take up to 10 minutes for the override to execute. It is recommended to use the APM –Mortise or Cylindrical models with monitor transmission presence, (Request to enter option) so the RF communication enables the PIM to download instructions to the APM every time you press the button on the reader.

Note: Automatic Override (ARO) can take up to 10 minutes after the override is set to execute since the heartbeat of the reader is set to 10 minutes. However, if you use APM - Mortise or Cylindrical models with monitor transmission presence, (request to Enter option) so the RF communication enables the PIM to download instructions to the APM every time you press the button on the reader it will wake up the reader so there is no need to wait for 10 minutes.

CHAPTER 32

Contact Supervision

Overview

The purpose of supervising contact inputs is to detect any tampering with the equipment, including breaks and/or shorts in the wire between the reader controller and the supervised input point. End-of-line resistors are installed at the contact point end of the wire to detect trouble in the circuit. These resistors allow the SRCNX (Legacy) reader controller to distinguish between a contact point normal opening/closing from the circuit opening/shorting. The controller supports three methods of supervision.

Method 1: Both series and parallel resistors at the end-of-line (contact input)

Method 2: A single series resistor at the end-of-line (contact input)

Method 3: A single parallel resistor at the end-of-line (contact input)

When planning for contact point supervision using either the single series resistor or single parallel resistor, it’s important to keep in mind the basic function of supervision: to create an alarm when trouble on the circuit is detected. When using Method 1 or Method 2 supervision, care must be taken to insure the desired result is accomplished.

Types of alarms generated by SRCNX (Legacy)

- Door Held Open (DHO) or Door Forced Open (DFO)
- Contact Secured
- Trouble Open (break in the circuit)
- Trouble Short (a short in the circuit)

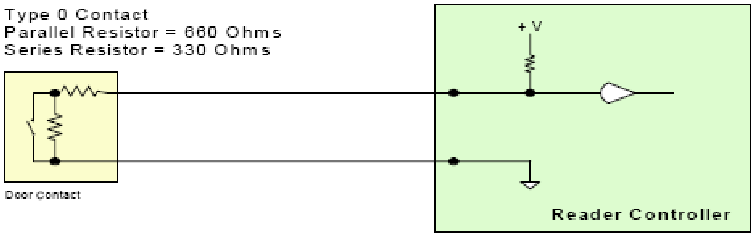
Method 1 Supervision

Series and parallel resistors

Method 1 configuration: the SRCNX (Legacy) reader controller will detect approximately 990 ohms of impedance when the contact is open and 330 ohms of impedance when the contact is closed.

If a break in the circuit occurs, the voltage measured at the controller will be near +V, causing the controller to issue a trouble open alarm.

If a short appear in the circuit, the voltage measured at the controller will be near ground, causing, the controller to report a trouble short alarm.



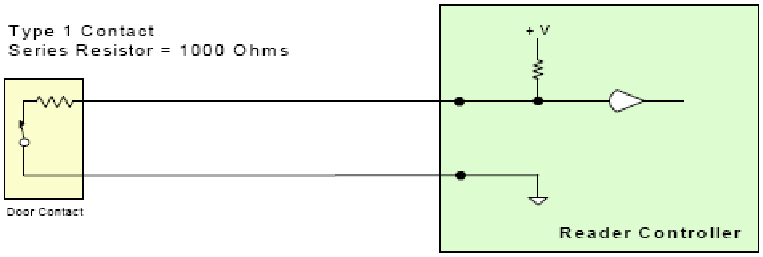
Both Parallel and Series Resistors at the Contact

Method 2 Supervision

Single Resistor in Series

A single resistor in series with the contact input should be used when the contact is normally closed. The SRCNX (Legacy) reader controller will detect a voltage drop in the circuit when the contact point is closed. When the contact opens, or when the circuit is broken, the voltage measured at the reader controller will be close to +V, causing the controller to issue a contact active alarm. If the circuit is shorted, the controller will detect a voltage of near ground and issue a trouble short alarm.

A single resistor in series does not work well with a normally open contact. When used with a normally open contact, it is impossible to distinguish between the normal open state of the contact and a break in the line. Cutting the wire between the point and the controller would appear to the controller as the normal condition and the controller would not issue an alarm.



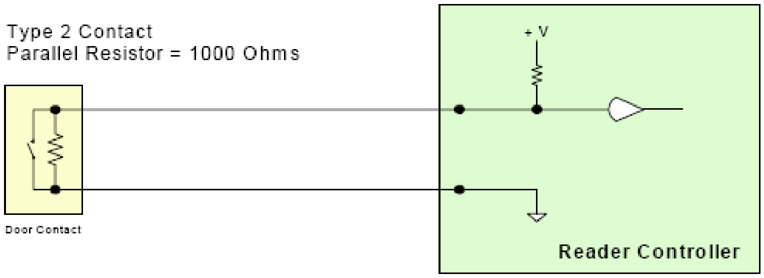
Single Resistor in Series with the Contact

Method 3 Supervision

Single Resistor in Parallel

Method 3 Configuration: A single resistor in parallel with the contact input should be used when the contact is normally open. The SRCNX (Legacy) reader controller will detect a voltage drop in the circuit when the contact point is open. When the contact closes, or the circuit is shorted, the controller will detect a voltage ground and issue a contact active alarm. If the circuit is broken, the voltage measured at the controller will be near +V, causing the controller to issue a trouble open alarm.

A single resistor in parallel with the contact does not work well with a normally closed contact. When used with a normally closed contact, it is impossible to distinguish between normal, contact secure state and a short in the circuit. Shorting the wires between the reader controller and the contact would appear to the reader controller as the normal condition and the controller would not issue an alarm.



Single Resistor in Parallel with the Contact

Index

VANDERBILT

vanderbiltindustries.com

Vanderbilt Industries
2 Cranberry Road
Parsippany, NJ 07054

☎ 973 316 3900

@VanderbiltInd

Vanderbilt Industries

an ACRE company

06021-1219