Innometriks

Innometriks Rhino Reader User Guide

8200-1521-02

REVISION B

MAY 2024

6 Technology Park Drive
Westford, MA 01886
http://www.innometriksinc.com
Phone: 760-542-0200

Johnson Controls

Canadian Radio Emissions Requirements

The digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

FCC Digital Device Limitations

Radio and Television Interference

This equipment has been tested and found to comply with the limits for a digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and television reception.

> Caution: Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

Table of Contents

Preface

The Rhino Reader is for new and experienced security system users who want to learn to use this product for their Security Management System.

In this chapter:

How to Use this Manual

This manual contains chapters that provide the following information about the Innometriks Rhino Reader system.

Chapter 1: Overview on Page 8

- Provides basic information about Rhino Reader

Chapter 2: Network Connectivity on Page 14

- Provides instructions for connecting the reader to a network

Chapter 3: Reader Administration on Page 17

- Describes the reader's administration menus and options

Chapter 4: Reader Diagnostic Menus on Page 24

- Provides instructions for accessing and using diagnostic information

Chapter 5: Biometric Authentication on Page 30

- Provides examples of using the fingerprint module

Chapter 6: Browser Based Administration on Page 39

- Provides instructions for administering the reader through the web

Appendix A: Screen Differences between WebGui and Reader Local on Page 1

- Describes differences between WebGUI displays and displays at the reader

Appendix 7: Supported Card Types and Smart Card Formats on Page 1

- Lists supported card types and supported smart card formats

Conventions

This guide uses the following text formats and symbols.

Convention	Meaning
Bold	Bold text describes one of the following items: • A command or character to type • A button or option on the screen to press • A key on your keyboard to press • A screen element or name
<text>	Indicates a variable.

The following items are used to indicate important information.

NOTE Indicates a note. Notes call attention to any item of information that may be of special importance.

TIP Indicates an alternate method of performing a task.

Indicates a caution. A caution contains information essential to avoid damage to the system. A caution can pertain to hardware or software.

Indicates a warning. A warning contains information that advises users that failure to avoid a specific action could result in physical harm to the user or to the hardware.

Indicates a danger. A danger contains information that users must know to avoid death or serious injury.

Overview

This document is a guide for the administration and use of the Innometriks Rhino Reader as viewed from both the WebGUI web interface and the onboard (local) screens at the physical reader. Where the same functionality exists on both WebGUI and onboard screens, the WebGUI screens are described in detail since reader administration is more commonly done remotely.

For installation instructions, refer to the Rhino Reader Quick Start Guide.

In this chapter:

Reader Functionality

The Rhino Reader is a networked smart card reader that supports **TCP/IP**[1] communication between the reader and the PACS host system, and Wiegand communication between the reader and the PACS interface panel.

It is designed to be easy to deploy, flexible and secure, providing a strong authentication solution for physical access.

[1]TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Wiegand Input and Output

Standard ***Wiegand***[1] input and output means that the Rhino Reader will integrate with any Wiegand based physical access control system on the market.

Smart Card Authentication

Smart Card Authentication Services

Innometriks smart card authentication solution provides:

- Smart card registration services
- Smart card certificate trust path validation
- Revocation verification
- **FASC-N**[2] harvesting
- TWIC Privacy Key (TPK) distribution
- Reader based card certificate authentication
- Reader based **biometric**[3] card holder authentication
- **Wiegand**[4] communication with PACS reader interface panels

Smart Card Authentication Process

A user's smart card, such as a TWIC card, is registered into the PACS host system using a contact reader. The user's Federal Agency Smart Card Number (FASC-N) and TWIC Privacy Key are stored as part of the user's record in the PACS database.

To authenticate a smart card holder, the following steps occur:

1. The user presents a smart card to a Rhino Reader.

---

[1]The Wiegand interface is a de facto wiring standard which arose from the popularity of Wiegand effect card readers in the 1980s. It is commonly used to connect a card swipe mechanism to the rest of an electronic entry system.
[2]Federal agency smart card number
[3]Biometrics refers to metrics related to human characteristics. Biometrics authentication, or realistic authentication, is used by access control systems as a form of identification and access control.
[4]The Wiegand interface is a de facto wiring standard which arose from the popularity of Wiegand effect card readers in the 1980s. It is commonly used to connect a card swipe mechanism to the rest of an electronic entry system.

2. The reader reads the unique FASC-N ID from the smart card and uses the number to retrieve the user's TWIC Privacy Key stored in the PACS during card registration.
3. The reader executes an active card authentication consisting of:
   a. Certificate validation
   b. Card Authentication Key (CAK) asymmetric challenge/response
4. The reader retrieves the user's biometric template from the interface on the card and deciphers the template using the TWIC Privacy Key.
5. The reader performs a Biometric User Authentication of the smart card holder by prompting the holder for a fingerprint and comparing it to the biometric template retrieved from the card.
6. The reader communicates the users FASC-N and authentication status to the PACS reader interface using OSDP or Wiegand protocol.
7. The PACS panel decides if the user has access rights to the portal and, depending on those rights, either door strikes are released or access is denied.

NOTE See Appendix B for *Supported Card Types* and for *Smart Card Formats*.

Advanced Biometric Authentication

The Rhino Reader **biometric**[1] search configuration provides true **one-to-many**[2] *authentication*. *Enrollments* are captured and stored in a central database. The template images are synced to appropriate readers for instant access. Advanced biometric authentication features include:

- One-to-Many fingerprint
- **One-to-One**[3] PIN + fingerprint
- Ultra-fast search algorithm
- 10,000+ template capacity

---

[1]Biometrics refers to metrics related to human characteristics. Biometrics authentication, or realistic authentication, is used by access control systems as a form of identification and access control.
[2]A type of comparison where one example is compared to many others - for instance when comparing a person's fingerprint to a set of fingerprints stored in a database.
[3]A comparison where one example is compared to a known sample as verification - for example when a PIN entered is compared to the stored PIN associated with an identity.

Intelligent Reader Management

Network-based services allows enterprise-wide implementations to be managed from a central location.

- Secure browser-based management
- Network-based and OSDP based firmware upgrades
- Configuration file cloning

Multiple Communication Interfaces

Supports multiple communication protocols to bridge the gap between dated **physical access control system**[1] technology, and new IP based technology.

- Wiegand In and Wiegand Out
- Ethernet and RS-485
- Relay NO/NC
- TTL In and TTL Out

Proven in Tough Environments

Ruggedized to operate in both indoor and outdoor environments. Optional outdoor and extreme kits allow the unit to withstand harsh direct weather conditions.

- Vandal resistant aluminum housing
- Optional Extreme Seal Kit
- MTBF 60,000 hours
- No Maintenance

Operational Boundaries

- Power: 12VDC, 1 amp
- Ambient temperature rating is 20°F (-6°C) tom 120°F (48.9°C) at 12v 1 amp.
- Humidity: 0-95% RH non-condensing

---

[1] A PACS is a particular type of physical access control system used as an electronic security countermeasure.

- Weatherproof: Build to **IP65**[1] standards

Reader Models

Figure 1: Rhino Reader

[1]IP rating is also known as Ingress Protection or International Protection ratings. These standards are used to define the levels of sealing effectiveness of electrical enclosures against intrusion from foreign bodies such as dirt and water.

Ordering Codes

Table 1 on Page 13 lists the product codes for ordering specific models of the Rhino Reader family.

Table 1: Reader Product Codes

Product Codes	Description
INN-RHNO-XS	Innometriks Rhino biometric reader, with keypad and LCD, contactless, indoor, with Lumidigm sensor
INN-RHNO-XS-OD	Innometriks Rhino biometric reader, with keypad and LCD, contactless, outdoor, with Lumidigm sensor

Network Connectivity

This chapter describes Rhino Reader configuration for network connectivity.

In this chapter:

Network Enabled Readers

Innometriks readers utilize network connectivity to provide advanced ***authentication***[1] modes that require distributed services, centralized data repositories and external *certificate authority* access. All Innometriks and most third party applications communicate with readers using Ethernet. C•CURE utilizes RS485 or Wiegand interfaces. You must check application requirements.

In addition, networked readers can be upgraded remotely, greatly simplifying administrative overhead. In certain authentication modes, the readers can be configured to run independent of any network infrastructure.

---

[1]Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or on an authentication server. If the credentials match, the process is completed and the user is granted authorization for access.

Network Planning

Most of the reader Operational Modes do not require the reader to be connected to network, and the reader NIC must be disconnected from the network.

Network based reader configuration, firmware upgrades, and server communication require each reader to be correctly configured to match the environment that they are deployed in. Each reader must have core network settings defined by an administrator or integrator. These settings allow the reader to “see and be seen” on the location's network infrastructure, when required using special operational modes.

Prior to reader implementation it is important to consult with a network administrator responsible for the Ethernet infrastructure at the facility. Readers' settings must match the existing network environment.

Things to Consider

- What Netmask is used?
- Does the existing network use **DHCP**[1] or do devices use static IP addresses?
- Are there routers and/or switches in place?
- Are **TCP/IP**[2] ports blocked at any point between workstations, servers, or readers?
- Is a ***gateway***[3] in place, and if so what is the IP address?
- Do reader ***MAC addresses***[4] need to be submitted to network administration?

At a minimum, the following information must be defined for each reader:

- Is DHCP enabled?
- If DHCP is disabled, the following must be defined:
  - Static IP address

---

[1]The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters, such as IP addresses, for interfaces and services.

[2]TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

[3]A network gateway is an interconnecting system capable of joining together two networks that use different base protocols.

[4]A media access control address (MAC address) of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi.

- Netmask
- Gateway address if needed
- Domain Name Server (DNS)

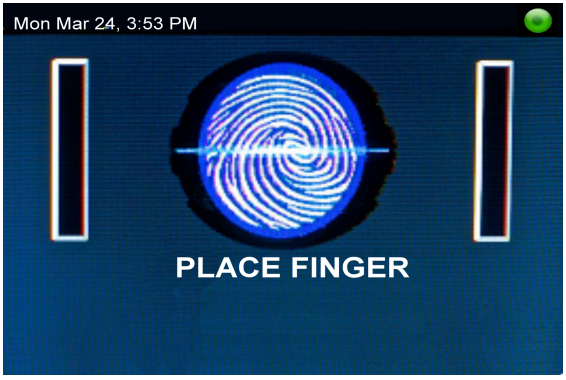
Actions Prior to Setting New Ethernet Parameters

For each new reader, Ethernet parameters must be set before using browser-based administration to complete the configuration across a TCP/IP network connection.

To prepare for configuring Ethernet settings at the reader:

1. DHCP enabled - Have the correct network settings at hand.
2. Make sure the reader is properly wired for 12 VDC power or PoE (Power over Ethernet) and is connected to the network.
3. Apply power to the reader. A fully booted reader should display a user interface specific to your application (touch sensor, present card, etc). See Figure 2 on Page 16.

Figure 2: Display Example



NOTE In Figure 2 on Page 16, and in similar figures in this guide, the image shows a symbol for a fingerprint instead of an actual fingerprint. The symbol is a substitute used when the *Show Finger Image* option in the General tab has been disabled. That option may be enabled or disabled by the administrator.

Reader Administration

This chapter explains the Rhino Reader administration menus and relevant options.

In this chapter:

Reader Administration Parameters

Each reader provides an administrative menu structure which allows parameters to be set at the reader.

All readers are shipped with access to the reader keypad Administration Mode disabled. Configuration of the reader should be performed using the readers web interface. Configuration through the readers front keypad option can also be enabled from the web interface, but is not recommended for security reasons.

To enable the reader keypad Administration Mode for the first time, the user must set a PIN code.

- The default reader Front Panel keypad 'Front Panel Access' type is set to 'Disabled'. To change this to 'PIN', you must set a PIN.
- The reader Front Panel keypad ‘Reader Configuration’ login PIN code must meet security requirements, before the first reader Front Panel ‘Reader Configuration Login’ attempt.

NOTE The following PIN codes are not allowed: 123456 and 654321. You must set a PIN code that has 6, 7, or 8 digits.

- The default reader Front Panel keypad ‘Reader Configuration Login’ type of ‘NONE’ option has been removed. The user must now select a reader Front Panel keypad ‘Reader Configuration Login’ type: PIN, Finger, or PIN + Finger.
- If you want to configure the reader to authenticate fingerprints, you must configure the scanner and enroll additional PINs and fingerprints using front panel reader configuration.

Each reader runs an embedded HTTPS service to provide administrative access across the network from any workstation with a web browser. No administration application is required to manage and upgrade readers.

Secure administrator access to all parameters is provided at the reader and through the network.

Integrators and PACS administrators to fine tune several aspects of the reader using definable parameters, including:

- Mode of operation
- Elevation of Security State
- Transaction logging options
- Wiegand communication options
- Centralized server settings
- Failover server settings

Reader Menus and Options

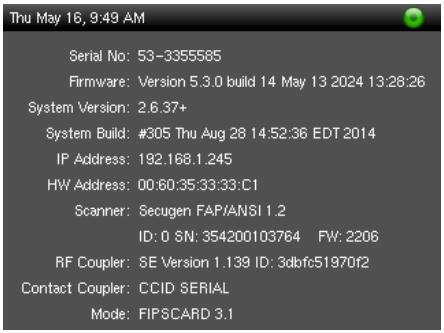
Function	Keys
Enter Main Menu	**Press and hold** * and 1 at the same time.
Move through Main Menu	(Down and Up Arrow Keys)
Enter Submenu	(Right Arrow Key)
Exit Admin Mode or submenu	(Exit Key)
Move between Submenu Tabs	(Plus and Minus Keys)
Move between Submenu Fields	(Right Arrow and Left Arrow Keys)
Toggle Checkbox	
Move through List Box	
Enter Numeric Values	1 (Numeric Keys)
Exit Submenu or Admin Mode	# (Pound Key)
Save or Reject Changes	(Check and X Keys)

Reader Configuration Summary

Press and hold * and then press F1 soft function key to display detailed reader configuration information.

You must have this information available when you contact Innometriks Support.

Figure 3: Configuration Summary Screen

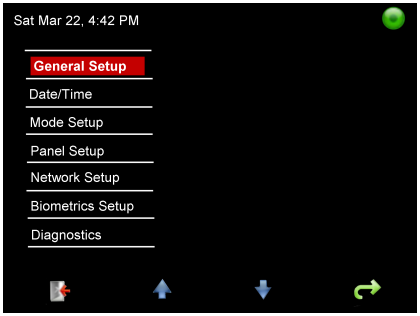


Reader Administrative Functions

All readers are shipped with Front Panel Access type set to disabled. The reader Front Panel keypad 'Reader Configuration' login 'PIN' code must be changed to six digits, on the first reader Front Panel 'Reader Configuration Login' attempt.

To enter Administration Mode, press * and the 1 keys at the same time. On the PIN entry screen, you must enter your PIN and if prompted, present your fingerprint to the scanner. If authentication succeeds, the following screen appears on your Rhino Reader:

Figure 4: Main Menu



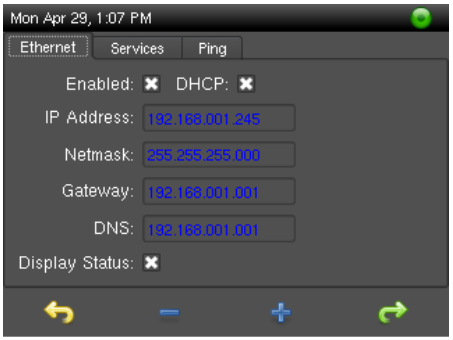
Before placing the readers into general use, one or more administrators should be added to each reader. Authentication can be set to PIN, Finger, or PIN + Finger. This is done using the Admin tab in the General Setup.

NOTE You use the Front Panel 'Admin' submenu to enroll administrators. The WebGUI's Administration submenu shows a list of enrolled administrator PINs.

Setting Ethernet Parameters from Main Menu

1. To set new reader Ethernet parameters from the main menu, **press** the four times to highlight the Network Setup menu item. **Press**. You should see the following screen:

Figure 5: Network Setup Screen



2. **Press** once to move to the Enabled field and **press** to activate the network functions on the reader.

3. **Press** once to move to the DHCP field. **Press** to enable DHCP, and press to disable DHCP. If DHCP is enabled, the remaining fields are not accessible.

4. **Press** to activate static IP address configuration.

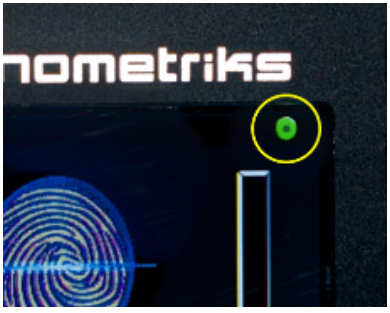
5. If you want to use a static IP, do not enable DHCP. Use to advance to the IP Address field, and use the numeric keypad to enter an IP address. Repeat this process to set the Netmask, Gateway and DNS IP addresses.

NOTE You must enter a leading **0** for any values under 100. You can use the **Plus** and **Minus** keys to move the cursor left or right in the address.

6. To move to the **Display Status** field, **press** . Then **press** to display the Network Connection icon in the upper right corner of the screen. Press to hide the icon.
7. When the settings are correct, **press** the # key to exit this menu. The reader prompts you to save changes. **Press** the key to save, or the key to cancel.
8. At the main menu, **press** to exit Admin mode.

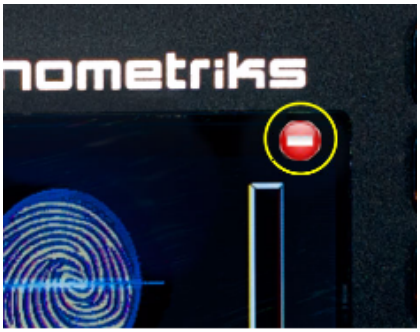
A network enabled reader that has a network connection displays in the upper right corner of the screen:

Figure 6: Screen Showing Network Connected



A network enabled reader that does not have a network connection displays in the upper right corner of the screen:

Figure 7: Screen Showing Network Disconnected



Reader Diagnostic Menus

This chapter describes the Rhino Reader Diagnostics.

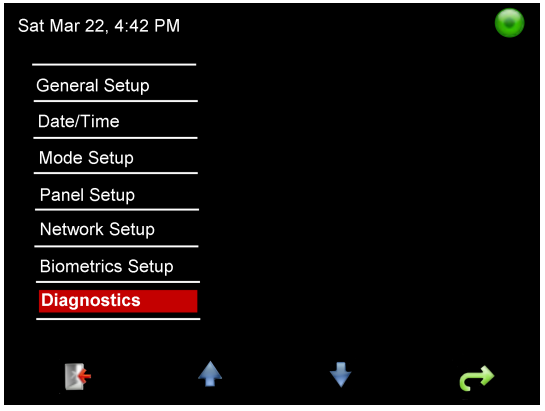
In this chapter:

Diagnostics Menu Access

From the reader administration main menu, **Enter** the Diagnostics submenu.

NOTE The Diagnostics submenu is not available in the WebGUI interface.

Figure 8: Selecting Diagnostics from the Main Menu



The initial Diagnostics screen displays the list of submenus .

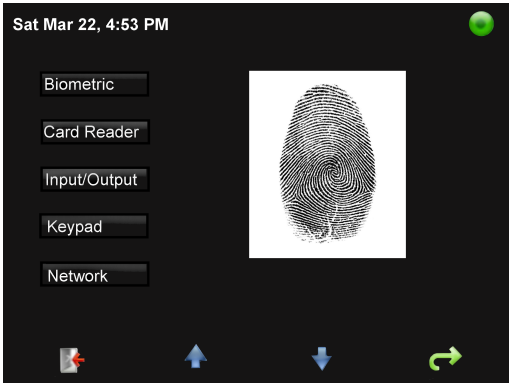
Figure 9: Diagnostics Submenu

Biometric

This test verifies that the fingerprint module is operational.

Responding to the **Place Finger** prompt, a person places their finger into the fingerprint module of the reader. After the finger is scanned, the person's fingerprint is displayed:

Figure 10: Biometric Test Screen

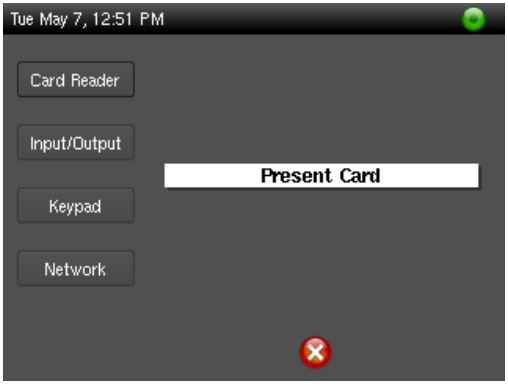


Improper placement of the finger into the fingerprint module can result in a "scanner timeout" error.

Card Reader

This test prompts the administrator to present an identification card to the Rhino Reader:

Figure 11: Card Read: Present Card



After the card is presented to the Rhino Reader, the **Present Card** display is replaced with the ID read from the card:

Figure 12: Card Read: Display ID

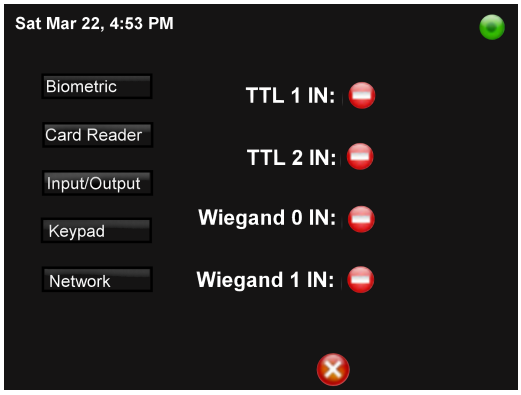
The screen above shows the ID data read from the card, such as card serial number, as appropriate.

NOTE The unsecured card serial number can be used to access secure content stored on the card. You must not use the card serial number as an access code. Many cards return content that can be used to retreive secure information from the card, such as a card ID.

Input/Output

This test detects input on TTL and Wiegand input channels. Green indicates live input, red indicates no input detected. In addition, the test toggles the TTL output, Wiegand output and Relay outputs:

Figure 13: Input/Output Test



Keypad

This test is used to determine if a keypad is failing. It displays value of any key pressed, including function keys.

To begin the Keypad test:

1. From the Diagnostics menu, click on the **Keypad** selection.
2. Next click on the right arrow key to display the blank small window, labeled *** + 0 to exit**.
3. Then click on any key and the screen shows the key that was pressed.
4. Press and hold the **Star** key, then press the **0** key to exit.

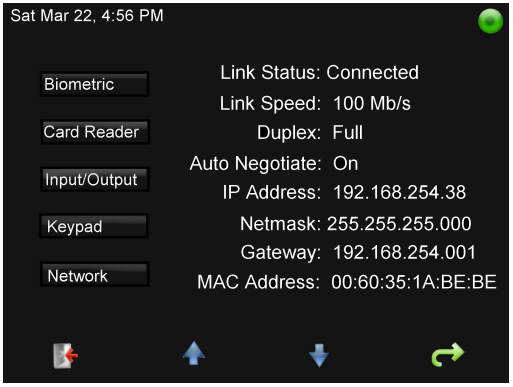
Figure 14: Keypad Test Screen

Network

To display network status and current settings:

1. From the **Diagnostics** menu, use the **Up** and **Down** arrows to select the **Network** submenu.
2. Press the right arrow icon to show the current network settings. The network status is shown in the icon at the top right of the screen, green for connected, red for disconnected.

Figure 15: Network Test Screen



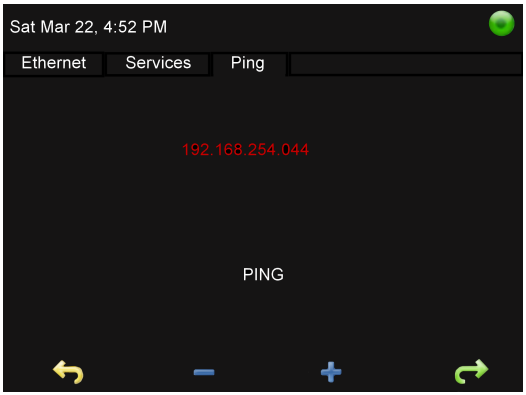
Ping

This test is accessed in the Network Setup menu on the third tab, as shown in Figure 16 on Page 29.

To begin the Ping test:

1. Use the plus key to move to the Ping tab, and the right arrow key to access the IP address field.
2. Enter the IP address to ping using the number keys. Then use the right arrow key to move down to the PING button.
3. Use the plus key to trigger the ping.
4. The reader pings the IP address entered and displays it in green if successful and red if unsuccessful.

Figure 16: Ping Test Screen



Biometric Authentication

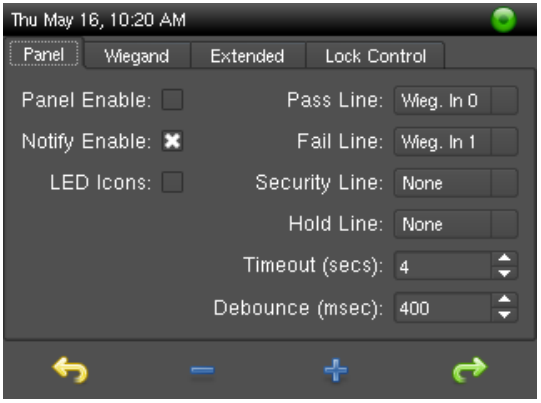
This chapter explains the Rhino Reader administration menus for authentication utilizing the fingerprint module.

In this chapter:

LED Icons

The **LED**[1] icon feature provides feedback on access granted and access denied in an easy to understand colored bar format. LED icons are enabled on the panel settings menu through the reader admin interface. Select the **LED Icons** check box to enable this feature.

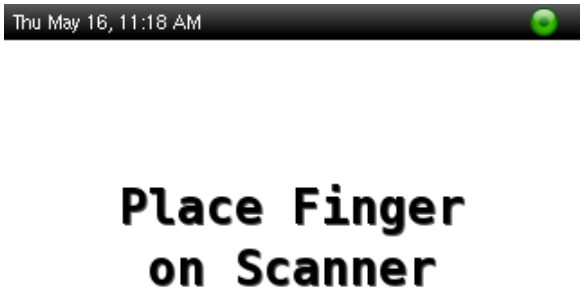
Figure 17: LED Icon Screen



[1]A light-emitting diode (LED) is a two-lead semiconductor light source. In this case, the LED is graphically emulated rather than actual.

Prompt for Identification

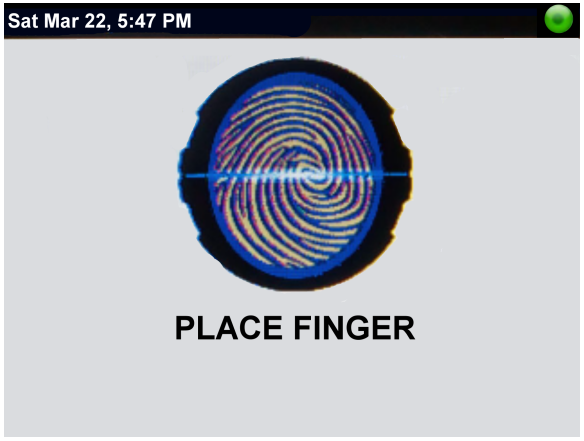
Figure 18: Prompt for User to Place Fingertip



High Contrast Interface

Outdoor installation with direct sun exposure may benefit from the high contrast screen background setting. Settings for contrast level can be made in the General option from the main screen.

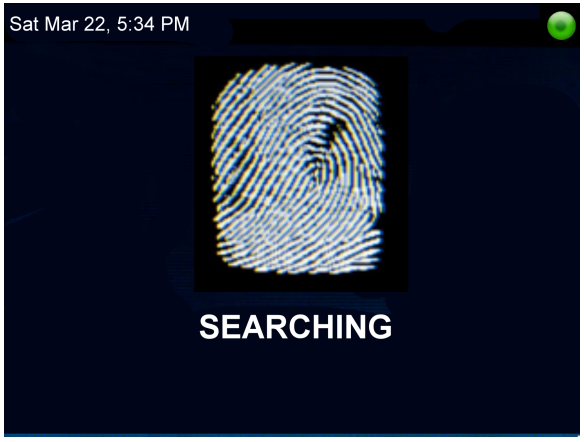
Figure 19: High Contrast Prompt



For information on the fingerprint symbol used in Figure 19 on Page 32 and some screens below, see the note at the end of Chapter 2: Network Connectivity

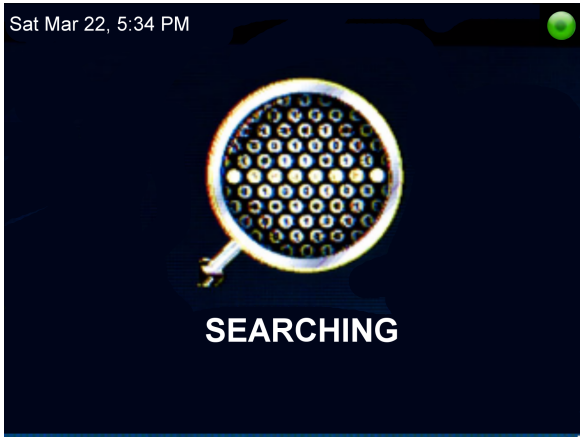
Searching for Match with Show Fingerprint Image Enabled

Figure 20: Show Fingerprint Enabled



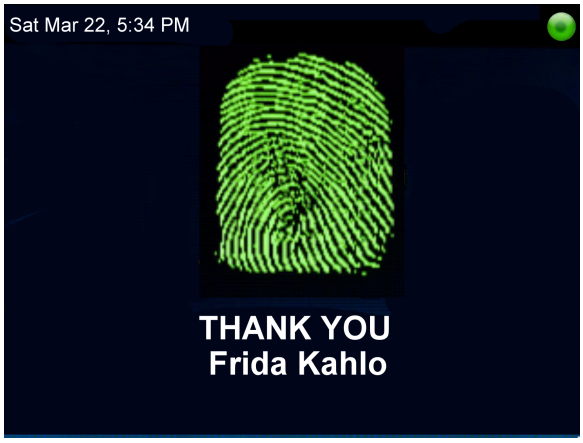
Searching for Match with Show Fingerprint Image Disabled

Figure 21: Show Fingerprint Disabled



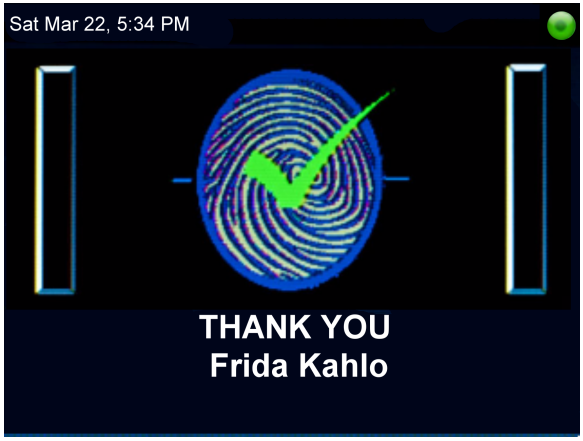
User Identified with Show Fingerprint Image Enabled

Figure 22: ID With Show Fingerprint Enabled



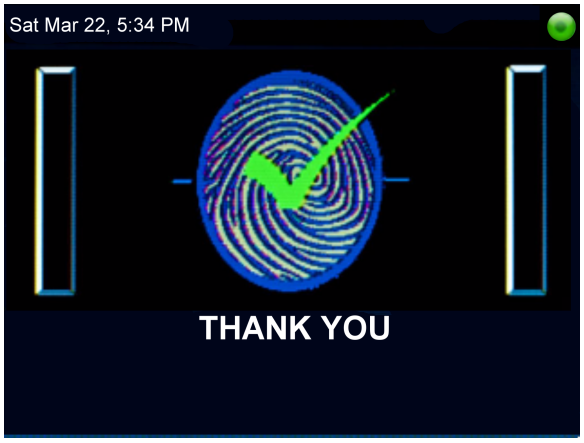
User Identified with Show Fingerprint Image disabled

Figure 23: ID With Show Fingerprint Disabled



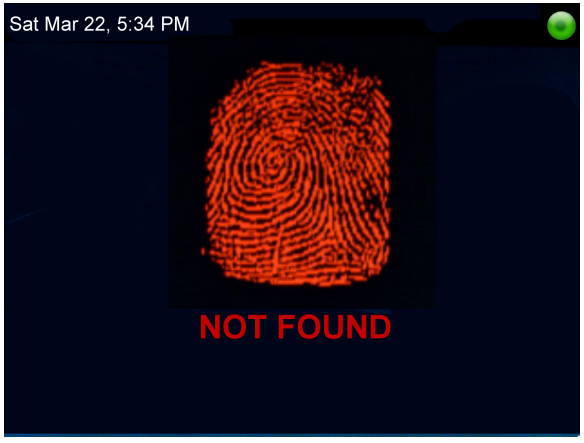
User Identified with Show Name and Fingerprint Image Disabled

Figure 24: ID With Show Fingerprint Enabled and Show Name Disabled



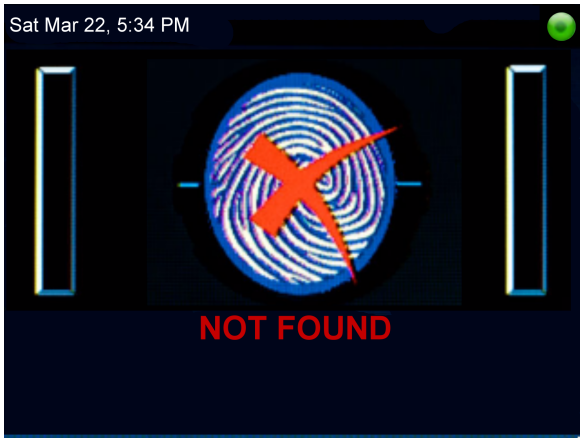
User Not Identified with Show Fingerprint Image Enabled

Figure 25: No Identification with Show Fingerprint Enabled and Show Name Disabled



User Not Identified with Show Fingerprint Image Disabled

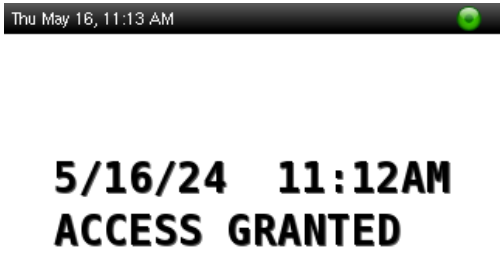
Figure 26: No Identification with Show Fingerprint and Show Name Disabled



Access Granted with LED Icons Enabled

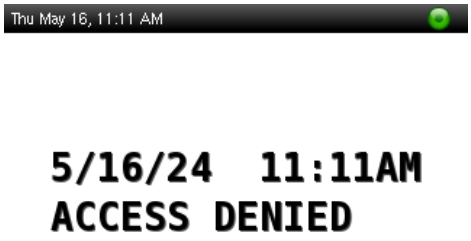
In the next two screens, the green vertical bars (signifying access granted) and the red vertical bars (signifying access denied) **are displayed** if the setting **LED Icons** is **enabled** in the reader's Panel Setup screen accessed from the main menu. See Enter Reader Admin Mode on Page 1

Figure 27: Access Granted with LED Icons Enabled



Access Denied with LED Icons Enabled

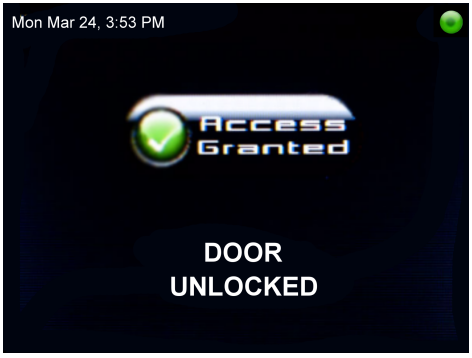
Figure 28: Access Denied with LED Icons Enabled



Access Granted with LED Icons Disabled

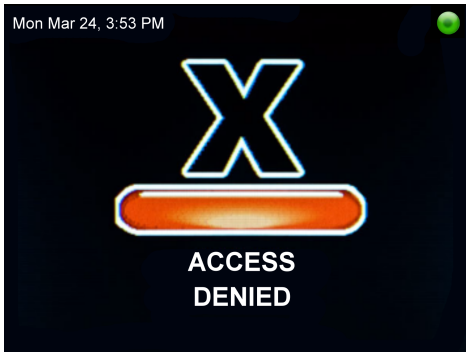
In the next two screens, green vertical bars (signifying access granted) and red vertical bars (signifying access denied) are **not displayed** when the setting **LED Icons** is **disabled** in the reader's Panel Setup screen.

Figure 29: Access Granted with LED Icons Disabled



Access Denied with LED Icons Disabled

Figure 30: Access Denied with LED Icons Disabled



Browser Based Administration

This chapter describes the administration of the Rhino Reader over the web.

In this chapter:

Managing Readers using the reader Web interface

To access a reader's WebGUI Home screen, launch a browser on a workstation that has network access to the readers and enter the reader's IP address as the URL using HTTPS.

Figure 31: The WebGUI Admin Login

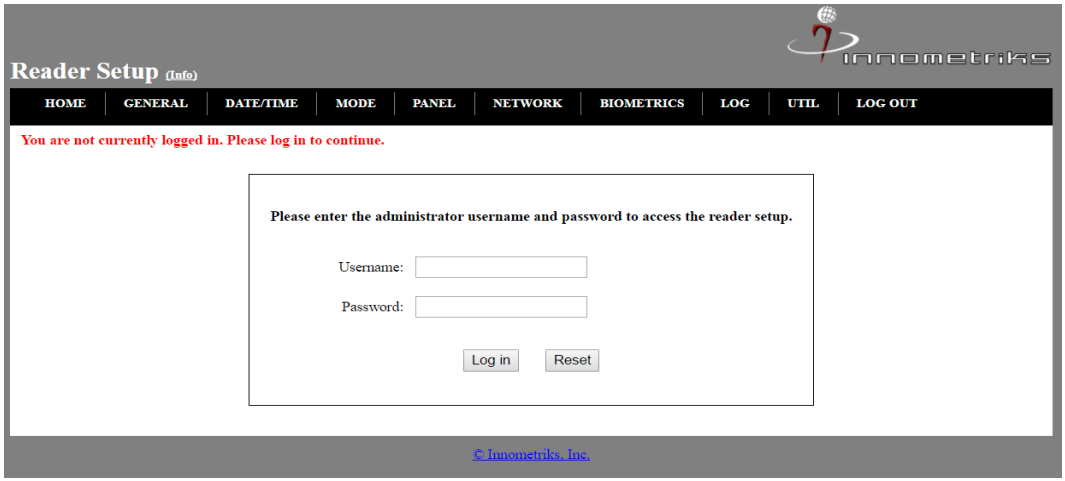
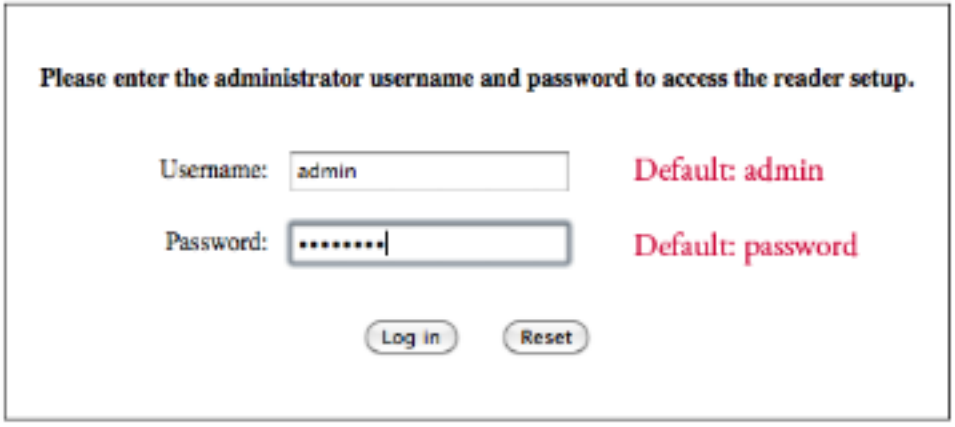


Figure 32: The Default WebGUI Admin User Name and Password



Each reader is shipped with the same default WebGUI login credentials. For security purposes, you must change the password before proceeding. See Appendix B for differences between the WebGUI interface and the reader's onboard screens.

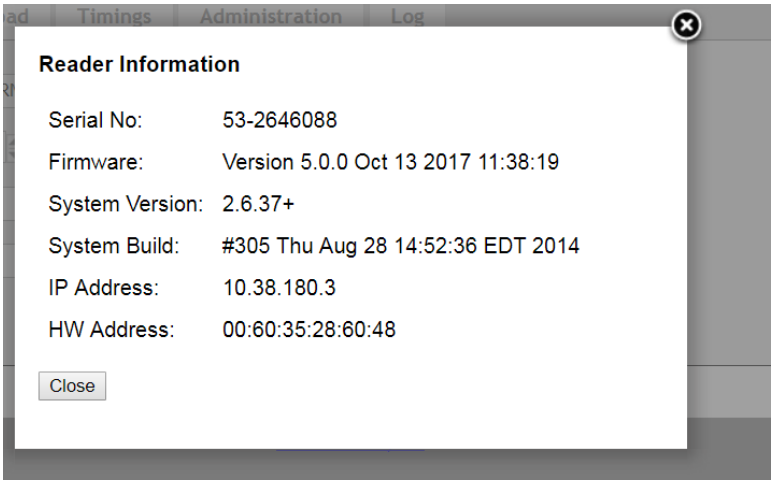
NOTE

When changing settings using the WebGUI, press Enter or click on the ***Update Settings*** button in the lower right hand corner to commit the changes to the reader. The reader configuration does not reflect any updates until you commit the changes. If you navigate to the home screen, the changes are not saved.

Reader Information

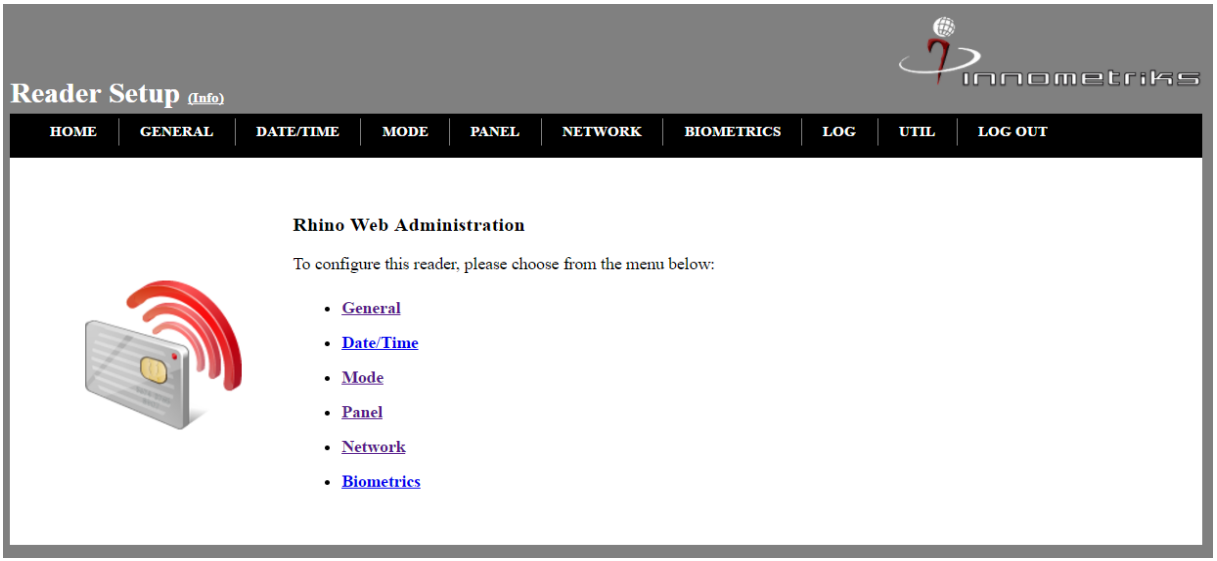
Detailed system level information about the reader can be viewed by **selecting** the text **(info)** next to the **Reader Setup** header at the top of the WebGUI Admin login screen above. This information is useful during a reader upgrade cycle. It provides instant access to the reader IP address and hardware (MAC) address. Please have this information available if calling Innometriks Tech Support.

Figure 33: Reader Information



Home Screen

Figure 34: WebGUI Home Screen



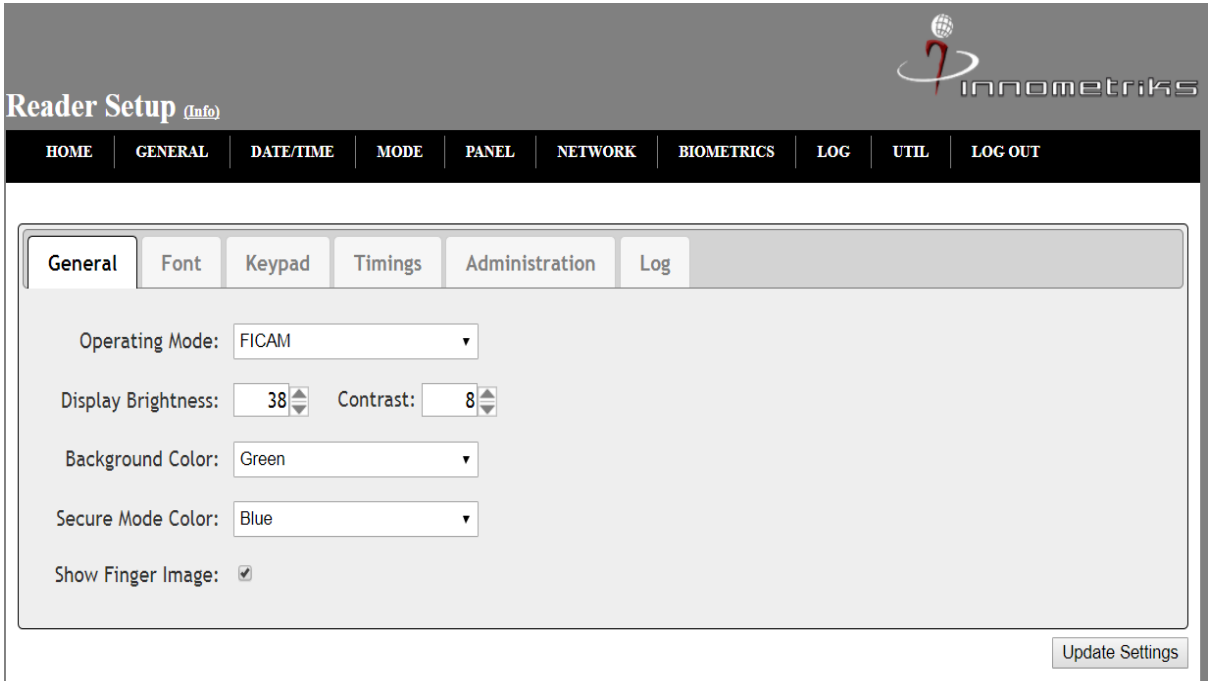
NOTE

"Screen" refers to the major headings along the top of the WebGUI Home Screen, e.g. General, Date/Time, ...Logout. "Tab" refers to the tabs displayed in those screens. So, in Figure 34 on Page 42, Operating Mode is located at General Screen/General tab. If you switch to another screen, the changes are not saved. However, if you switch to another tab, the changes are saved. Press **Update Settings** from any tab to save the changes from all the tabs.

General Screen

General Tab

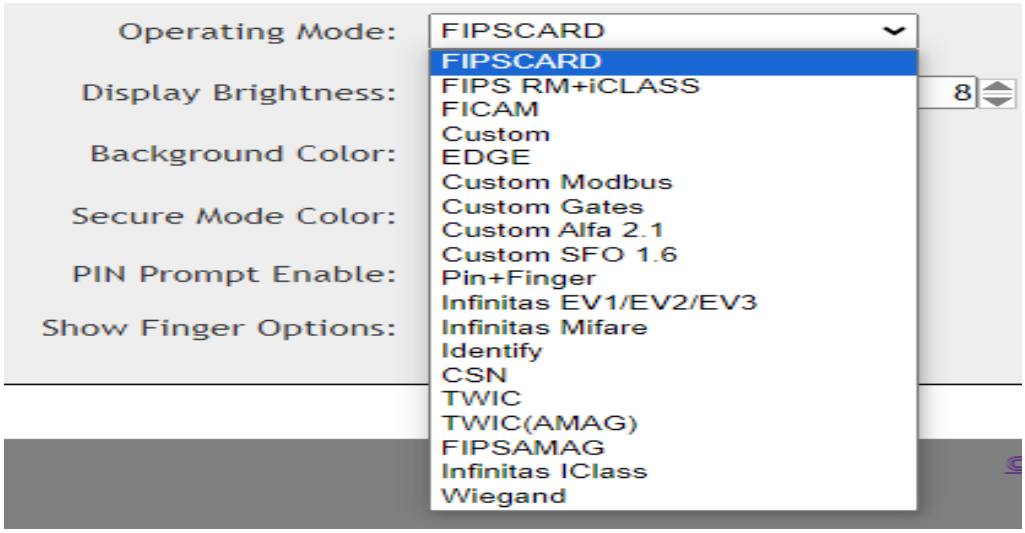
Figure 35: General Screen - General Tab



Operating Mode defines the authentication mode of the reader. Innometriks offers a variety of authentication modes, which are bundled together by implementation environment and the authentication goal.

The next screen shows the Operating Mode dropdown menu from the General tab:

Figure 36: General Screen - General Tab - Operating Mode



Changing the operating mode:

- Using the WebGUI to administer the reader
  - The operating mode can be changed using the General Screen/General tab. This change does not take effect until you press **Enter** on the keyboard or click **Update Settings** in the WebGUI.
- At the reader
  - When the operating mode is changed at the reader using the General menu option, the change takes effect when you either exit Admin mode or cycle power on the reader. In the General menu, press **#** on to exit and then click **SAVE CHANGES**.

Operating mode options

The operating mode options available on a given reader are determined by firmware version. Included in the current list shown Figure 36 on Page 44 are:

- **Identify**
  - **Identify**, i.e. **one-to-many comparison**, refers to the type of authentication where the person's fingerprint read by the reader is compared to the set of fingerprints in the entire system database.
- **PIN + Finger**

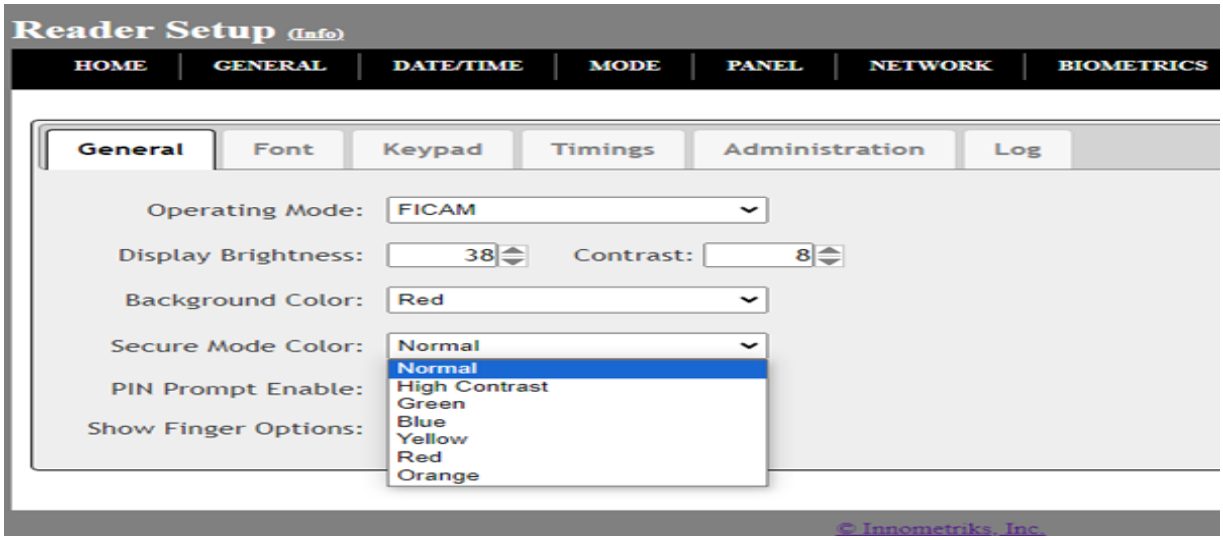
- **PIN + Finger** mode enables PIN plus biometric authentication at the reader. The user must enter a PIN number then a biometric authentication. This mode is considered a one-to-one comparison, as opposed to the one-to-many comparison used in Identify mode.

NOTE

For systems that do not have a failover server or network access to a server, when you change the reader Operating Mode to “EDGE”, “OUT OF SERVICE” displays on the reader. When using the WebGUI, this display occurs immediately after performing “Update Settings”. When changing the mode at the reader, this display occurs after you exit Admin mode.

Innometriks readers can respond to a change in security threat levels by elevating required authentication factors, and by presenting a different screen color to notify users.

Figure 37: General Screen - General Tab - Secure Mode Color



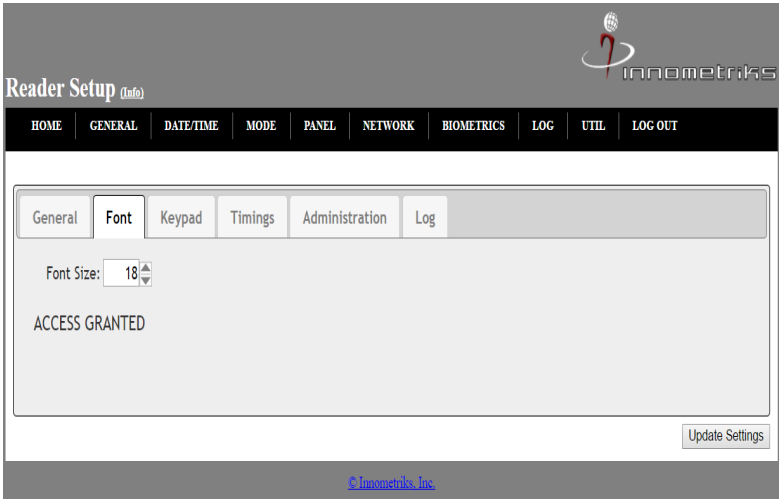
Display Brightness, **Contrast**, and **Background Color** allow the display to be adjusted to its environment. Bright sun demands one setting; a darkened interior setting requires another.

NOTE

In FICAM and OSDP operating mode, you cannot change the background color for Secure Mode. The color remains the same as the color set in Normal Mode.

Font Tab

Figure 38: General Screen - General Tab - Font

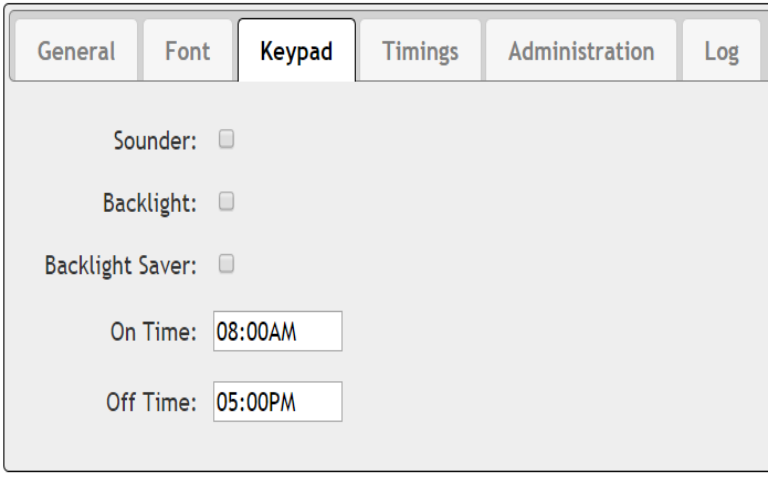


The Font Tab screen shows the font size selected along with an example of text at that font setting.

Keypad Tab

Keypad settings allow the reader keypad to be adjusted to its environment. When Sounder is enabled, the keypad emits a “beep” if any key is pressed.

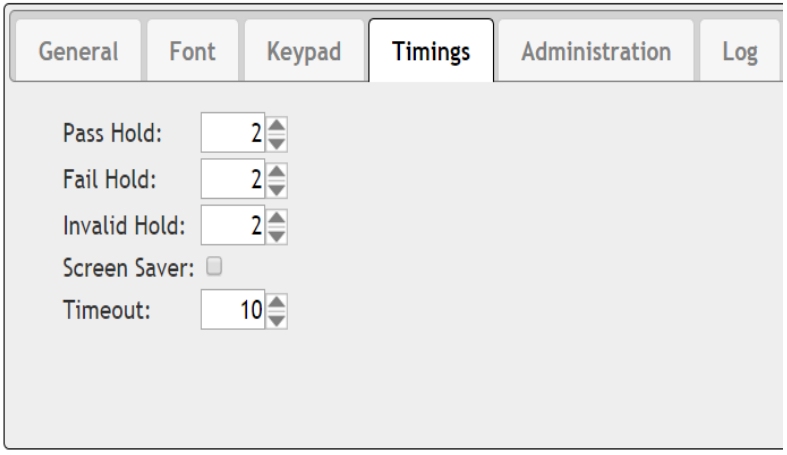
Figure 39: General Screen - General Tab - Keypad



Timings Tab

In the following screen, timing units are in seconds.

Figure 40: General Screen - General Tab - Timings in Seconds



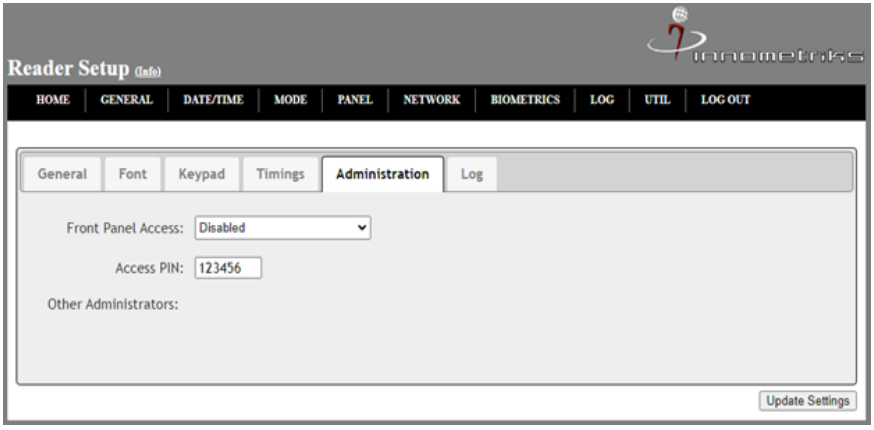
Timings control the duration of display events.

When a successful authentication occurs and the individual has been granted access, the reader displays “Access Granted”. The duration of the display is set using **Pass Hold**. The “Access Denied” display duration is set using **Fail Hold** and the “Invalid User” display duration is set using **Invalid Hold**.

The screen saver becomes active if no reader activity occurs in the **Timeout** interval. A unique screen saver graphic can be created by an administrator and imported from the WebGUI UTIL menu.

Administration Tab

Figure 41: General Screen - General Tab - Administration

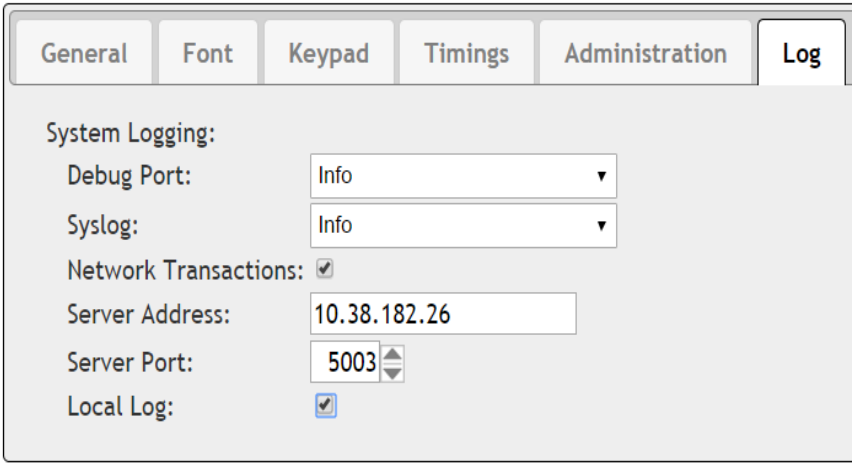


All readers are shipped with front panel access disabled. Before using the reader, you can add one or more administrators to each reader. Authentication can be set to Disabled, PIN, PIN + Finger, or Finger. You can configure front panel access using the WebGUI or the front panel Admin tab. You use the WebGUI to set the web front panel PIN. You use the Admin tab to enroll and delete administrators.

Administrators must be enrolled at the reader using reader based admin mode. The Admin Security level can be defined using WebGUI.

Log Tab

Figure 42: General Screen - General Tab - Log



Transaction Logging[1] keeps a history of authentication outcomes and communication errors. Logging provides administrators with a detailed history of what has occurred at a reader.

For most of the operating modes, enabling Local Log allows all transactions to be stored and viewed on the reader using the front panel. You can view, search, download, and clear tranactions using the Log tab in the WebGUI. The Rhino Reader can store the last 50k transactions before overwriting the first transaction logged. Some operating modes, such as FICAM, do not support the storing of logs in the reader. In those cases, the logs can be viewed by the Innometriks Panel Logger if it is installed in the system.

With Network Transactions enabled, all transactions are posted to a network based logging service running at the defined server IP address and listening to the defined Port ID. The logging services are a component of the Innometriks suite of applications.

In a reader development lab environment, a workstation with a terminal emulator can be attached to the RS232 Debug Port on the back of the unit. All transactions that match the Debug Port criteria are posted to the terminal emulator.

---

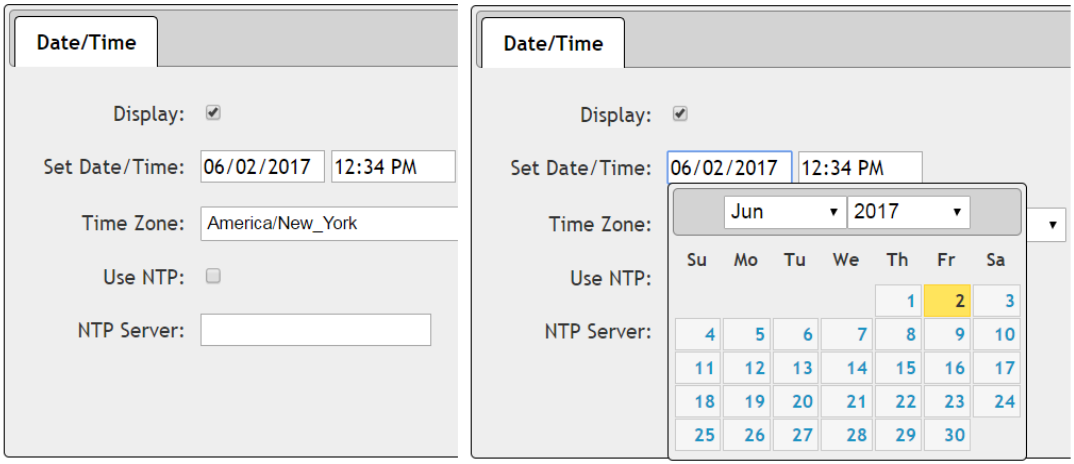
[1] A transaction log is a file, an integral part of every SQL Server database. It contains log records produced during the logging process in a SQL Server database.

Syslog[1] is a network-based development logging service that captures detailed reader information defined in Syslog criteria. To use, network service settings must be defined on the Services tab of the Network submenu.

Date/Time Screen

Date/Time Tab

Figure 43: Date/Time Screen



The date and time are typically set one of two ways:

- The time and date can be manually set using WebGUI interface or the reader Admin mode. The local time zone can also be set. If Display is enabled, the time and date is visible in the upper left hand corner of the reader display.
- Enable **NTP**[2] and define the IP address of the server providing network time protocol services.

---

[1]Syslog is a logging mechanism for network devices to send event messages to a logging server, usually known as a Syslog server. The Syslog protocol is supported by a wide range of devices and can be used to log different types of events.

[2]Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

NOTE Setting the date and time using the reader's Date/Time tab may conflict with the date and time displayed on the reader that is sent from the PACS or from a time server. If this is the case, you can clear the Display box in the reader's "Date/ Time" tab.

Mode Screen

The Mode screen display is dependent on the Operating Mode set in the General Screen / General tab. Not every operating mode has a mode setup screen. For those operating modes that do not have a Mode Setup, selecting the Mode tab from the main WebGui screen results in the message “The current mode does not have a mode setup page”.

In the current firmware version, the mode setup screens for their related operating modes are displayed as follows:

Mode Setup for Operating Mode: FIPSCARD

Figure 44: *FIPSCARD* Mode Setup GENERAL Tab

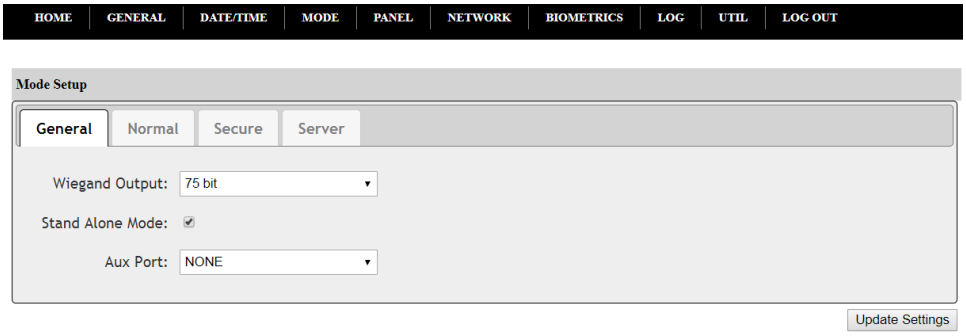


Figure 45: *FIPSCARD* Mode Setup NORMAL Tab

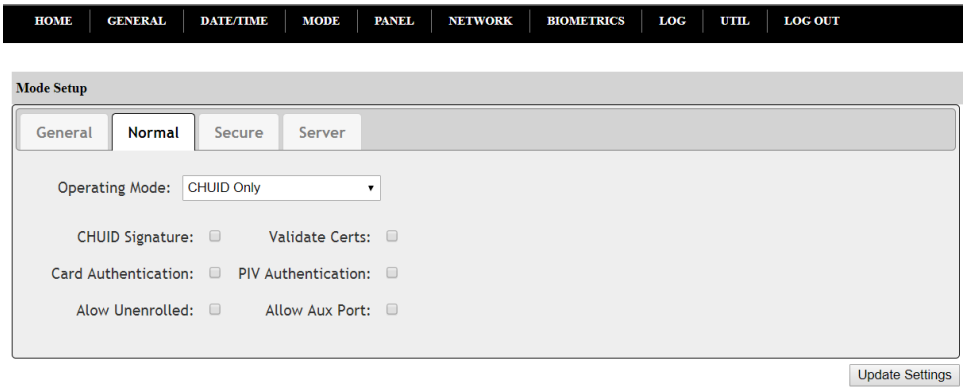


Figure 46: *FIPSCARD* Mode Setup SECURE Tab

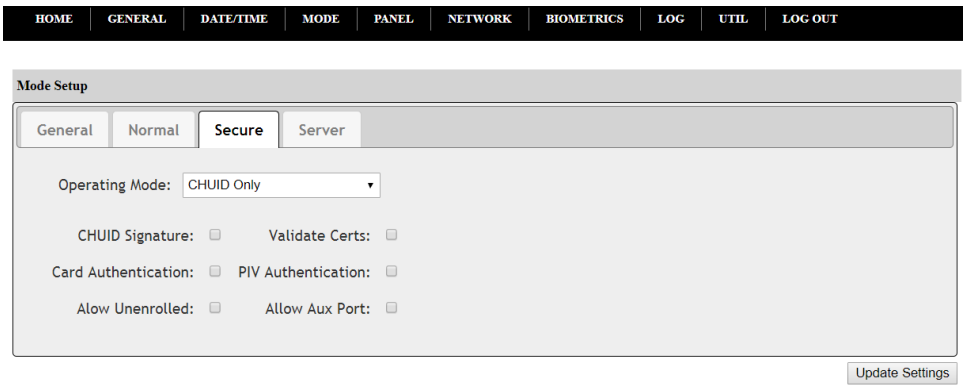
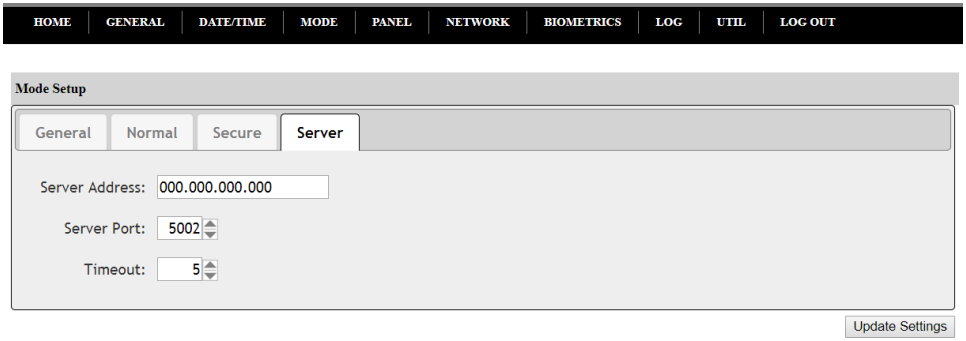
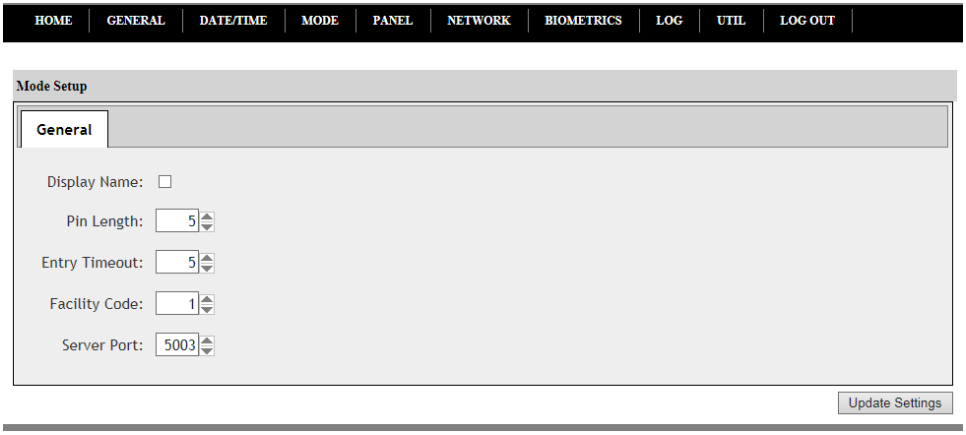


Figure 47: *FIPSCARD* Mode Setup SERVER Tab



Mode Setup for Operating Mode: Pin + Finger

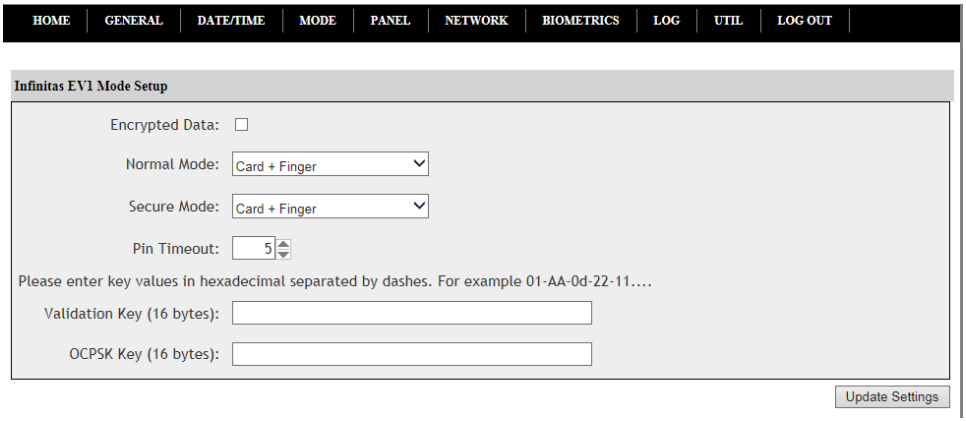
Figure 48: *Pin + Finger* Mode Setup GENERAL Tab



When "Display Name" is enabled, the reader displays the name associated with the fingerprint match. When not enabled, the reader simply displays a green checkmark to indicate a successful authentication.

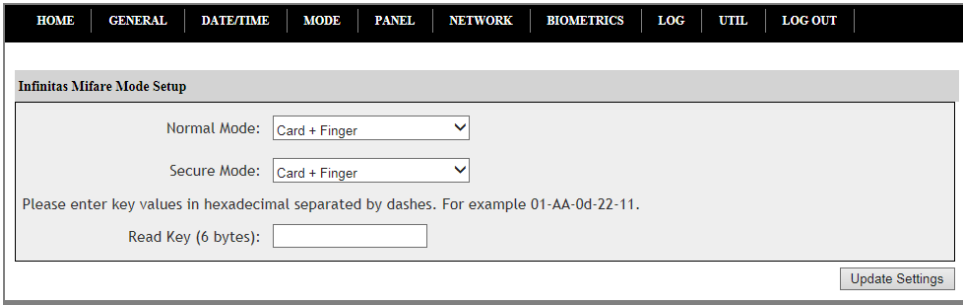
Mode Setup for Operating Mode: Infinitas EV1

Figure 49: *Infinitas EV1* Mode Setup Tab



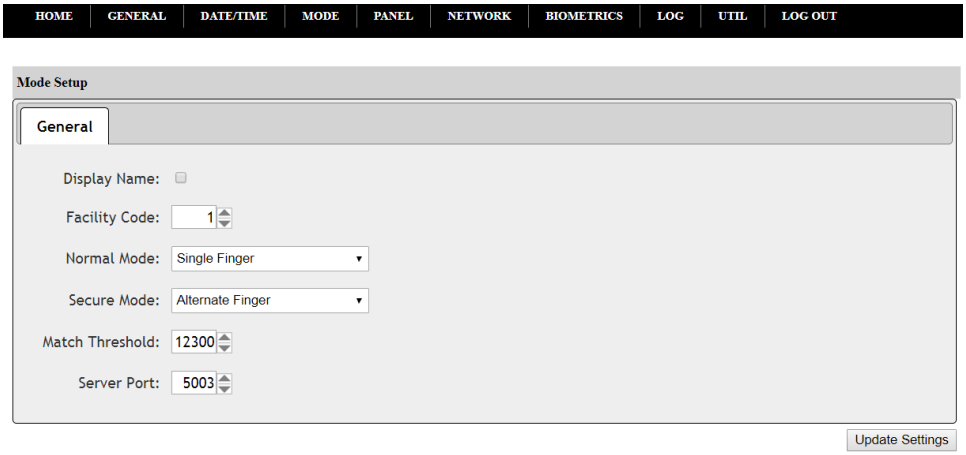
Mode Setup for Operating Mode: Infinitas Mifare

Figure 50: *Infinitas Mifare* Mode Setup Tab



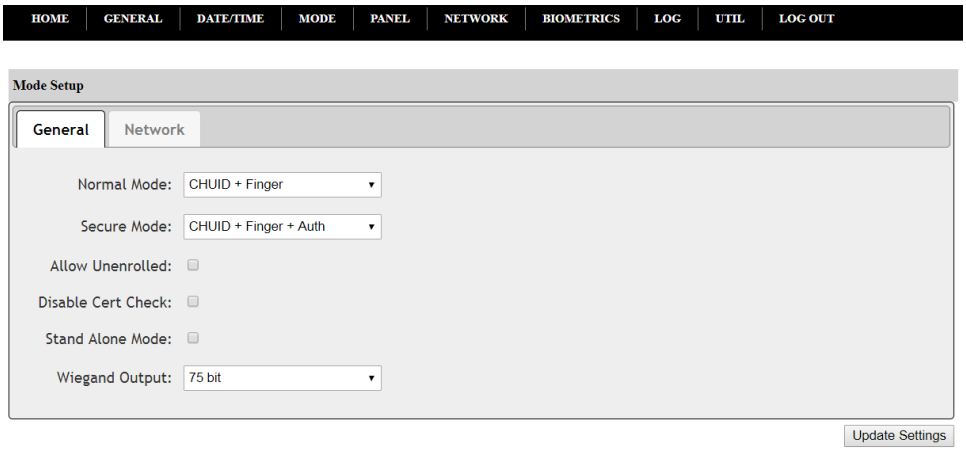
Mode Setup for Operating Mode: Identify

Figure 51: *Identify* Mode Setup GENERAL Tab



Mode Setup for Operating Mode: TWIC

Figure 52: *TWIC and TWIC(AMAG)* Mode Setup GENERAL Tab



Mode Setup for Operating Mode: FIPSAMAG

Figure 53: *FIPSAMAG* Mode Setup GENERAL Tab

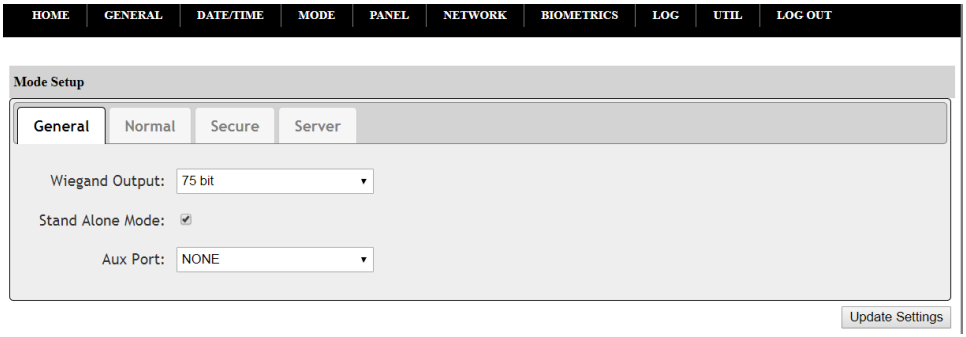


Figure 54: *FIPSAMAG* Mode Setup NORMAL Tab

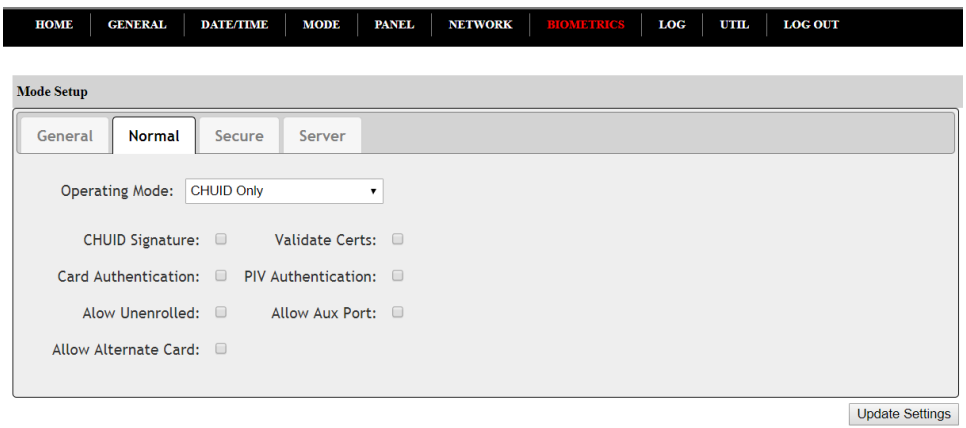


Figure 55: *FIPSAMAG* Mode Setup SECURE Tab

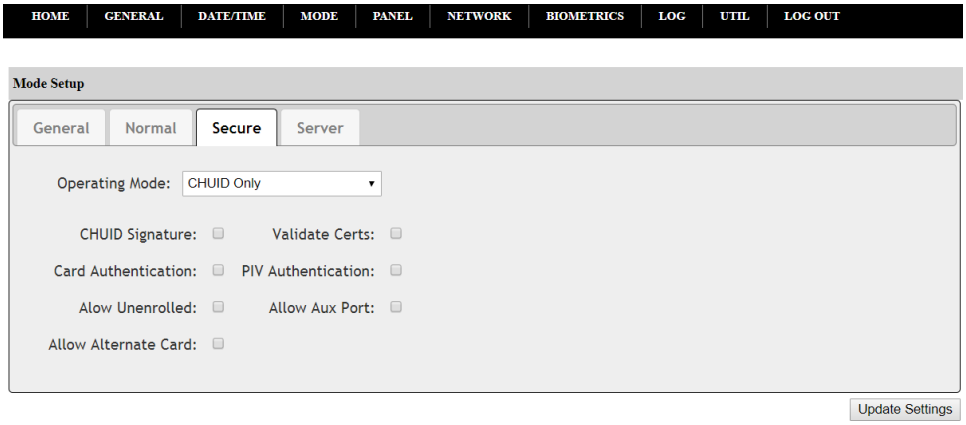
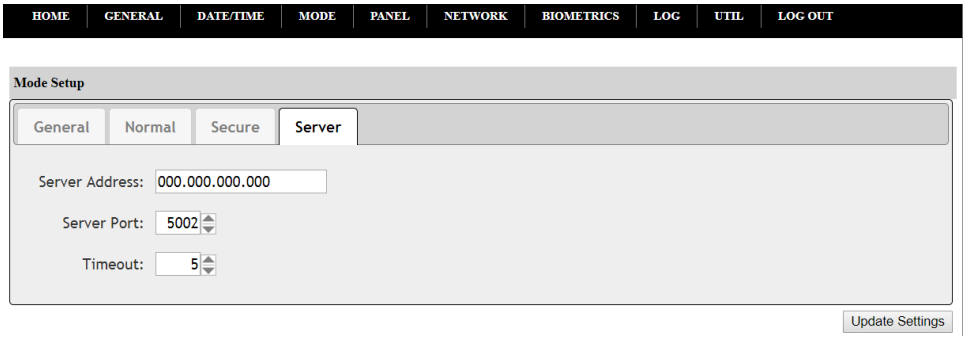
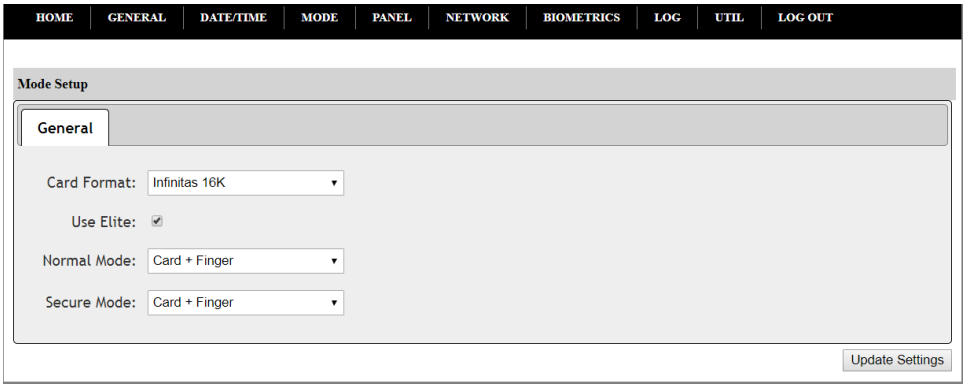


Figure 56: *FIPSAMAG* Mode Setup SERVER Tab



Mode Setup for Operating Mode: Infinitas iCLASS

Figure 57: *Infinitas iCLASS* Mode Setup GENERAL Tab



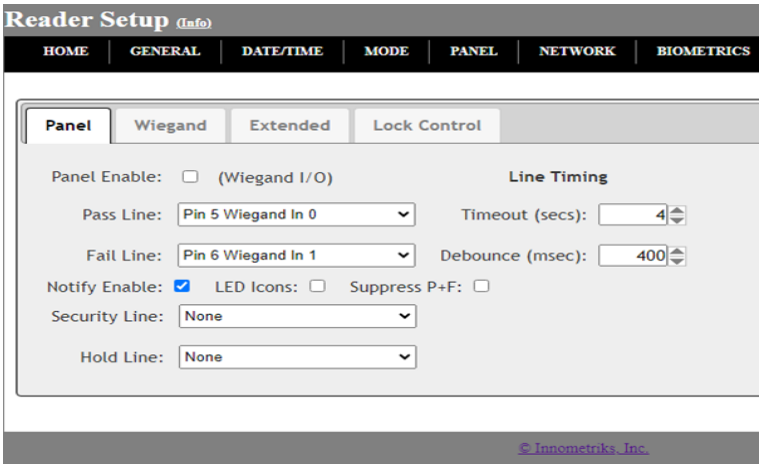
In the display above:

- Card Format can be set to either *Infinitas 16k* or *QS 32k*.
- Normal Mode and Secure Mode can be set to either *Card Only* or *Card + Finger*.

Panel Screen

Panel Tab

Figure 58: The Panel Setup

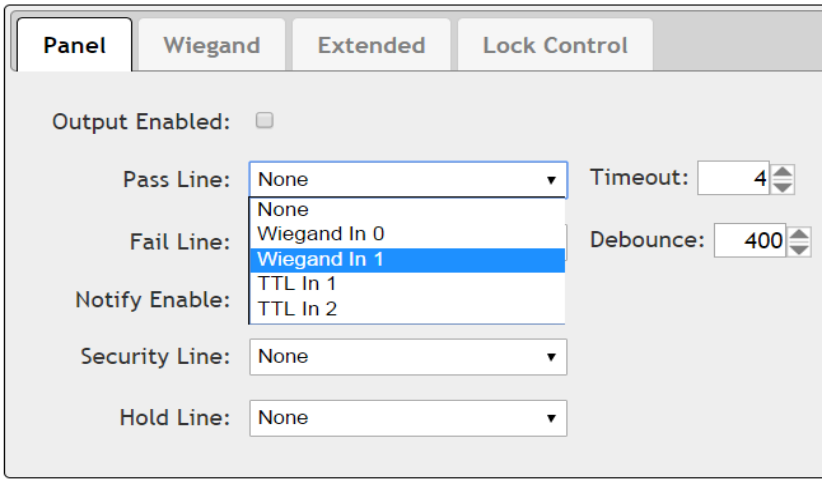


Bi-directional communication between a reader and the physical access control system occurs through the panel interface. These settings configure the reader to match the communication expectations of the PACS panel and PACS host application. The reader is also configured to properly handle the return communication from the PACS.

Panel **Output Enabled** must be set if reader to PACS panel communication is required.

Pass Line and **Fail Line** allow the reader to provide feedback to the user requesting access. The user may authenticate successfully at the reader but not have PACS rights to enter the protected portal.

Figure 59: Pass/Fail Wiring Connections



Pass Line defines which reader input is wired to the PACS panel “pass” or “green” TTL output. Typically this is set to Wiegand In 0 or 1. TTL In 1 or 2 may also be used.

Fail Line defines which reader input is wired to the PACS panel “fail” or “red” TTL output. Typically this is set to Wiegand In 0 or 1. TTL In 1 or 2 may also be used.

Timeout defines how long (sec) the reader waits for a return pass/fail signal from the panel.

Debounce determines how long the reader waits for a stable signal from the panel.

With **Notify Enable** set, the reader forwards keypad entry to the PACS allowing PIN entry to be passed from the reader to the PACS panel. Use requires PACS support of this feature.

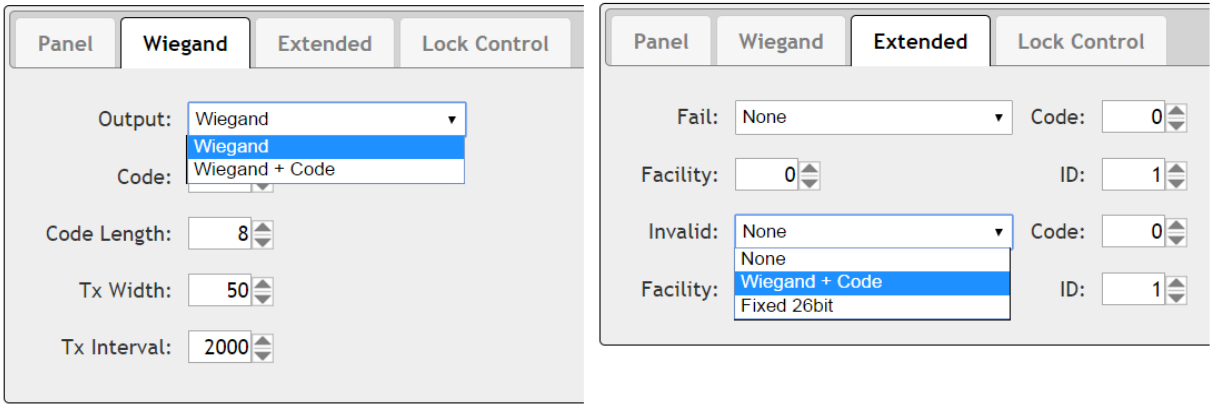
Security Line triggers a change in the reader’s security mode to elevate the reader from Normal Mode to Secure Mode. If this setting is enabled, the reader also changes the display color to alert users in most modes (see note following on Page 39).

Hold Line disables the reader user interface, effectively blocking new authentication events. When combined with lock control, this feature may be used to facilitate “man-trap” and “lock down” functionality.

Wiegand Tab

Wiegand Output

Figure 60: Wiegand and Extended Tabs



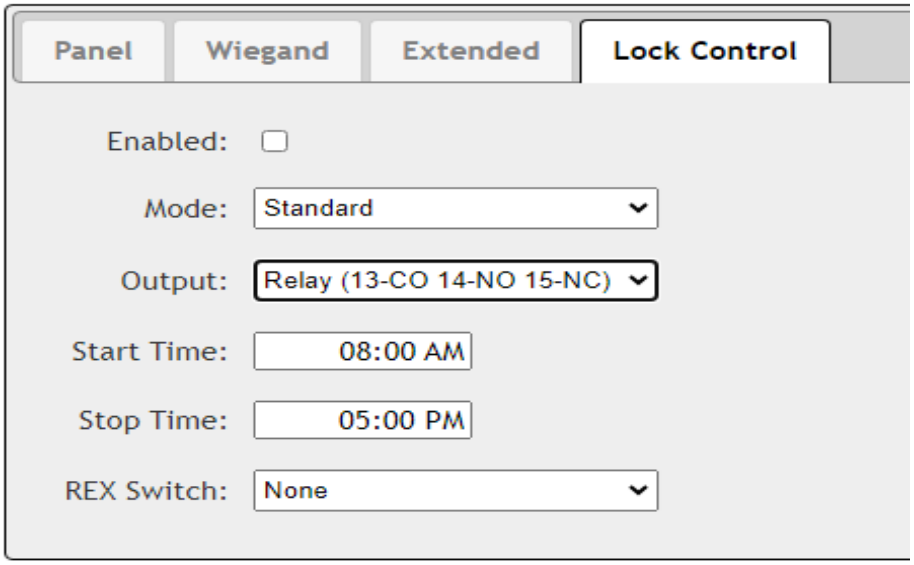
Wiegand Output is set to match the format and content that the PACS panel expects. The formats are authentication mechanism specific (PIV card) and PACS panel specific (200 bit CHUID vs. 75 bit FASCN).

In addition, site and facility codes may be embedded in the Wiegand stream. The content of the embedded code is usually specific to the environment. The Wiegand output from the reader must provide what the PACS panel expects.

The settings on the Wiegand and Extended tabs enable integrators and PACS specialists to match the Wiegand output from a pass, fail and invalid authentication event from the reader with the PACS requirements.

Lock Control Tab

Figure 61: The Lock Control Tab



With Lock Control enabled, the reader can trigger external relays. This feature is very useful for securing remote gates and in environments without a PACS. Door relays can be opened and closed based on the outcome of authentication event. You can use the Lock Control feature in Wiegand modes only.

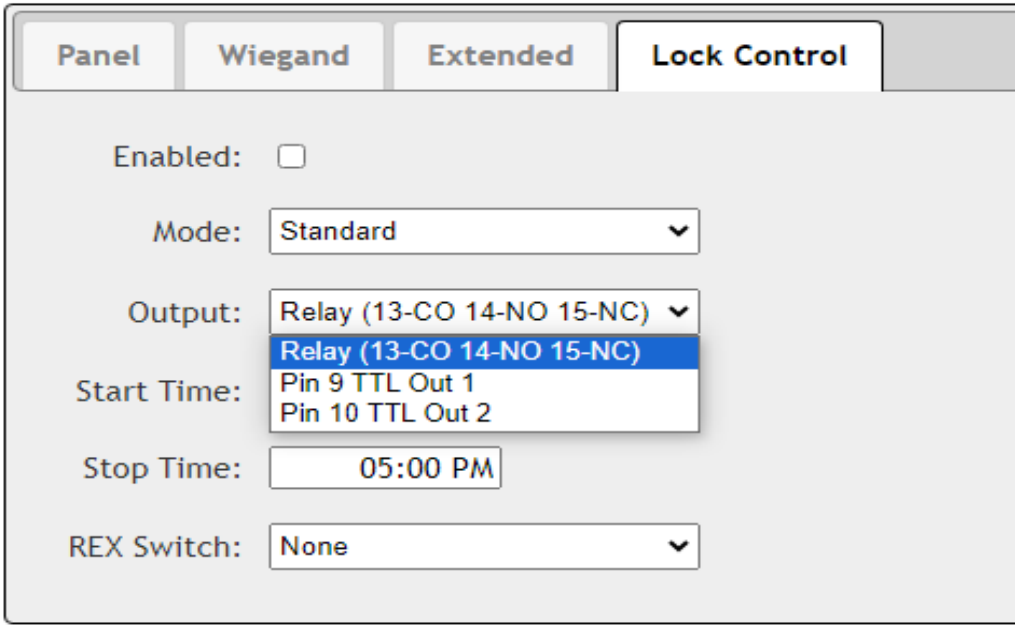
In environments where the reader is tied to a PACS, the reader typically passes a user's ID along with the authentication pass/fail outcome. The PACS then determines if the user has permission to enter the protected portal. If the reader is in control of the door lock device instead of the PACS panel, input from the PACS panel can set to trigger the “open” or “close” event.

Output defines the reader output channel that triggers an external device when a successful authentication occurs.

The REX Switch setting is a request-to-exit used to fire the onboard relay in Wiegand based configurations. It is not used in FICAM configurations.

NOTE The Lock Control feature can be used in Wiegand modes only. When you use a Wiegand mode, the outputs **Wiegand out d0** and **Wiegand out d1** are not in the Outputs list.

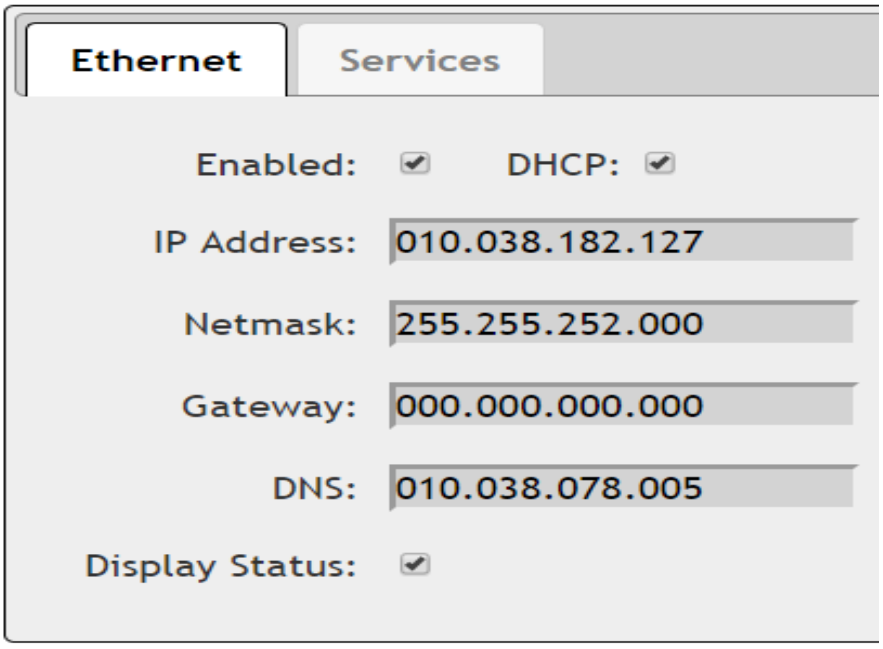
Figure 62: Defining Lock Control Output



Network Screen

Ethernet Tab

Figure 63: The Ethernet Tab



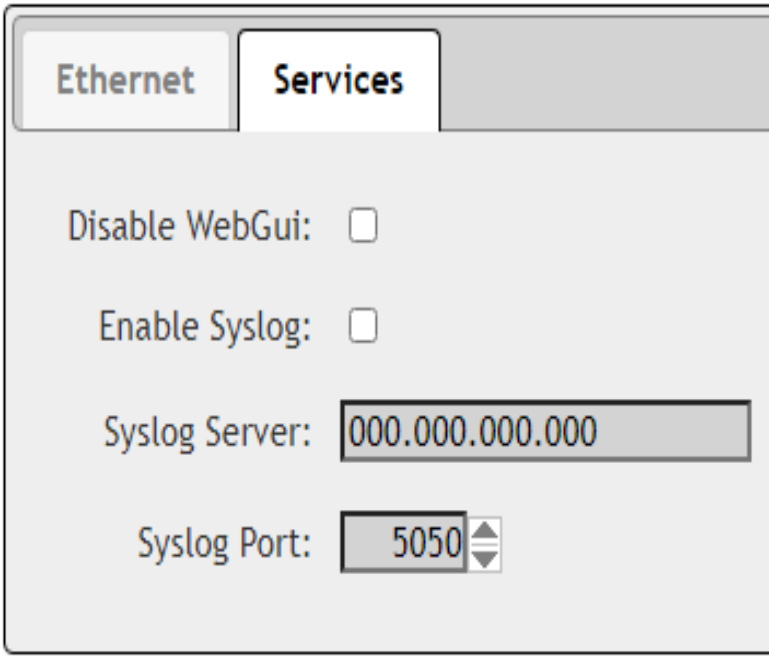
For each new reader, Ethernet parameters must be set using the reader-based admin mode. Once network connectivity is established, the browser-based WebGUI can be used to configure the reader.

Determine if existing network devices utilize DHCP. If so, enable **DHCP**.

If DHCP is not used, define a static IP address and the environment's Netmask. If required, add a gateway IP address.

Services Tab

Figure 64: The Services Tab



The WebGUI is enabled by default but can be disabled. When it is disabled over the web, it can only be enabled at the reader. If you select the **Disable WebGUI** checkbox, the web interface is disabled.

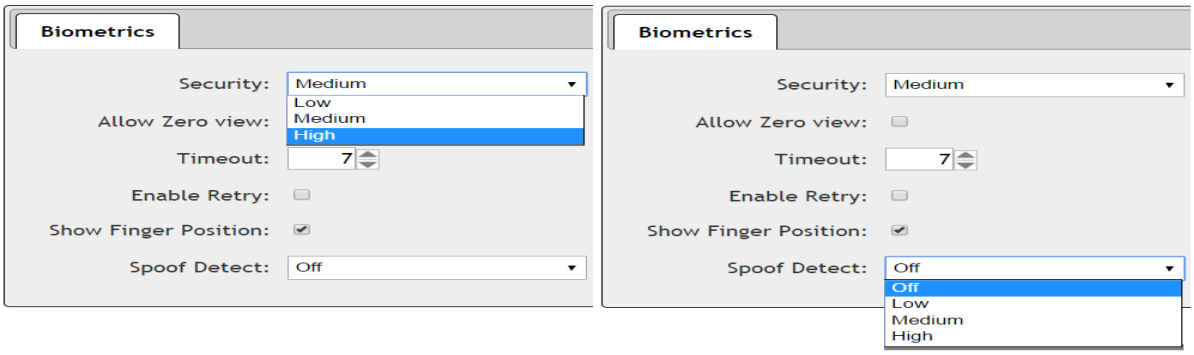
Syslog is a network-based event logging service that captures the detailed reader information defined by the Syslog criteria on the Log tab of the General submenu. To use, enable Syslog and define the IP address where a Syslog service is running.

NOTE **Syslog** is disabled by default. Do not activate **Syslog** unless you are instructed to by an Innometriks technician.

Biometrics Screen

Biometrics Tab

Figure 65: The Biometrics Tab



Security is tied to the match score generated when a fingerprint is compared to a template. The higher the security level, the higher the threshold is for a “pass” authentication.

This setting is usually set to **Medium**, but can be lowered to accommodate a large enrollment population with widespread template quality issues. It can also be set to **High** for a small population of individuals accessing a high security area.

Timeout is the length of time in seconds that a sensor attempts to capture a fingerprint.

Enable Retry determines if a user is given a second chance to authenticate.

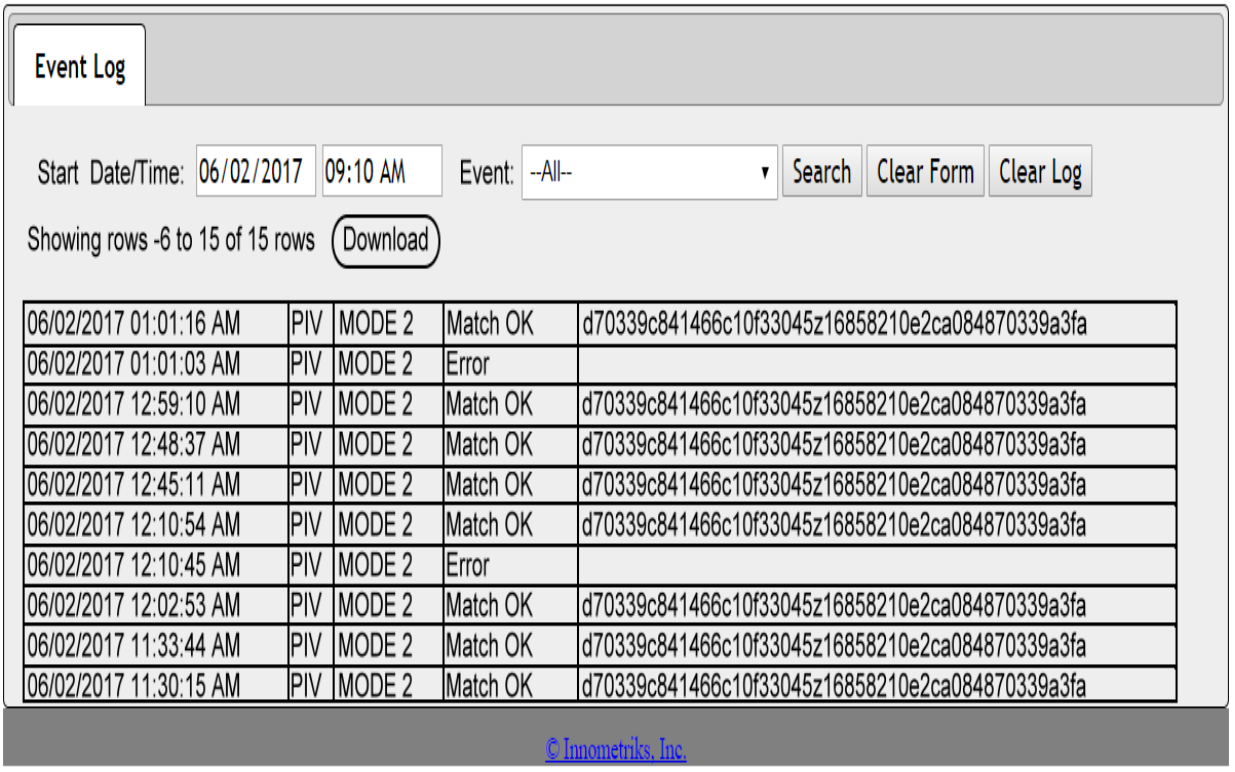
Spoof Detect utilizes an advanced “liveness test” feature available on the Lumidigm scanner.

NOTE The General screen menu on the web interface does not show the Biometric tab until the Lumidign fingerprint scanner has been configured. Unless there is a special use case, select the **Lumidigm Extract** option.

Log Screen

Event Log Tab

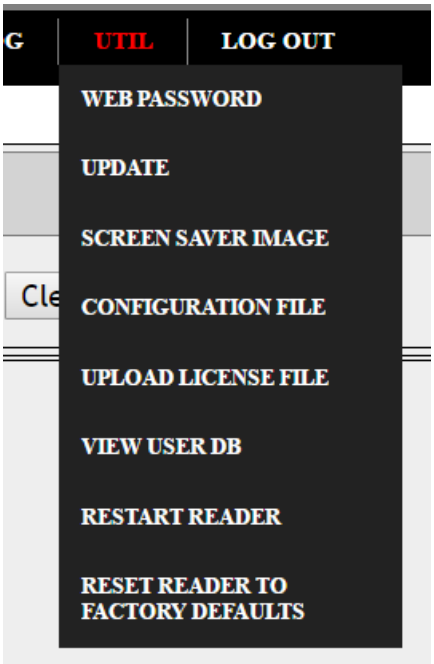
Figure 66: the Event Log



The reader event log provides administrators with a detailed history of events that have occurred at a reader. WebGUI allows an administrator to pull, view and purge logs from a specific reader. This feature is useful when investigating a pattern of failed authentication events. The logs are useful when troubleshooting a reader that is not performing as expected.

Util Screen

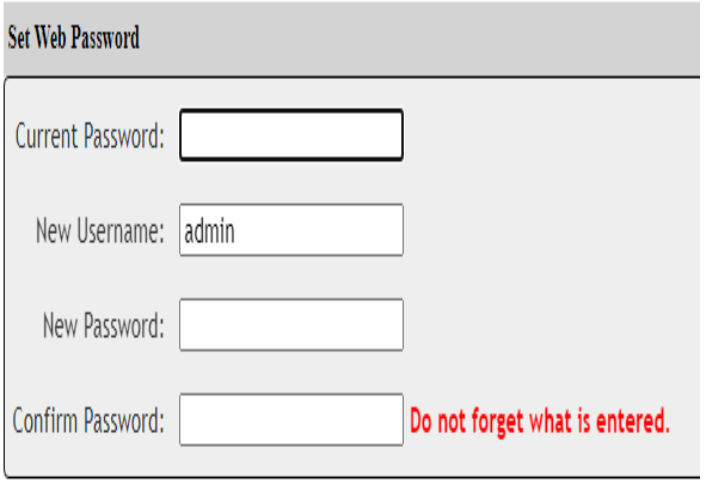
Figure 67: The UTIL tab



The UTIL tab displays various utility functions that are available to the administrator.

Web Password Tab

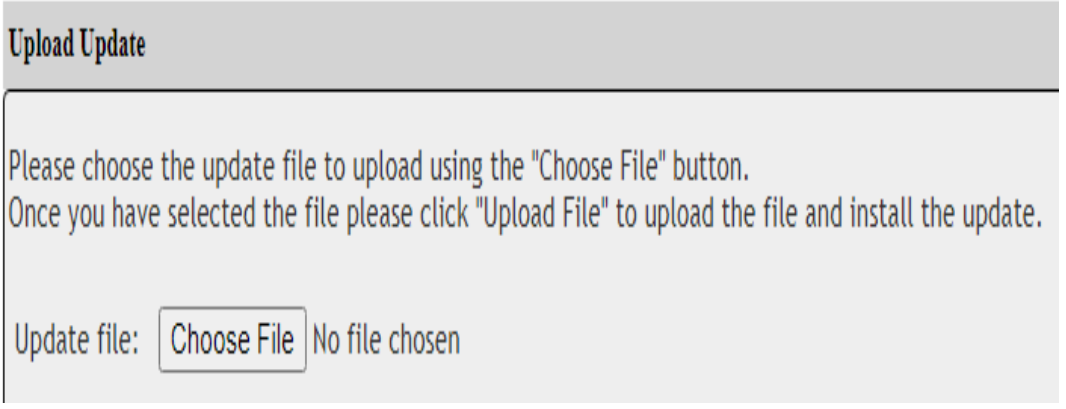
Figure 68: Set Web Password



The Set Password function is used to set the username and password required to access the connected reader's WebGUI interface.

Update Tab

Figure 69: Upload Update



The Upload Update function on the Update tab is used to remotely update readers. Boot loader, Kernel and firmware packages are supplied by Innometriks, and can be loaded independently of each other and in any order. It is common for the Boot loader and Kernel to remain untouched throughout several firmware upgrade cycles.

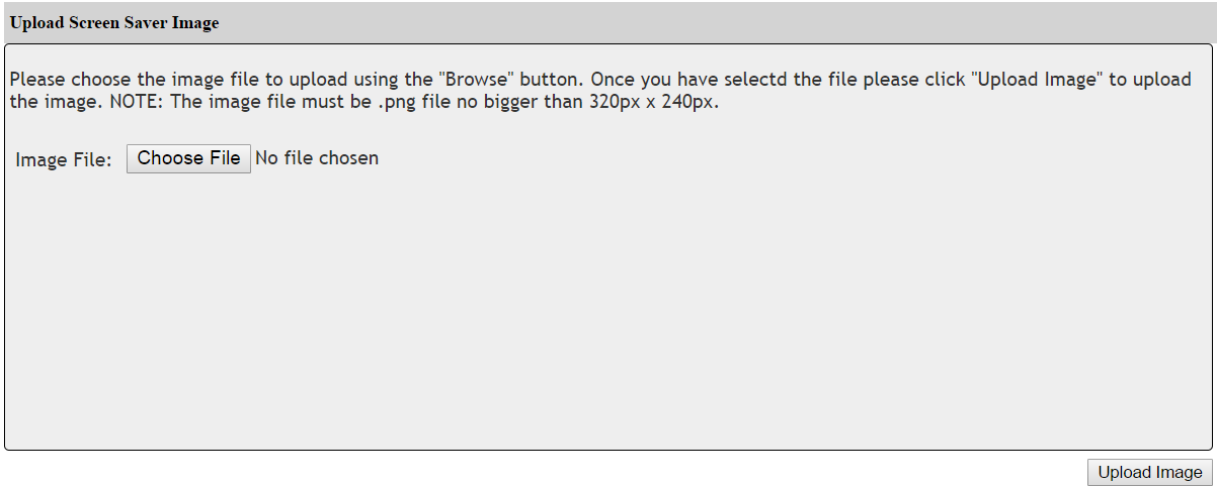
The images are packaged as .update files. The reader automatically determines the package type, extracts the image, and performs the installation.

Reader Update Steps:

- **Obtain** the update package(s) from Innometriks, typically available on the Innometriks FTP site.
- **Choose** the update you intend to upload.
- **Select** Upload File to transfer the package to the reader and **initiate** the update.

Screen Saver Image Tab

Figure 70: Upload Screen Saver Image



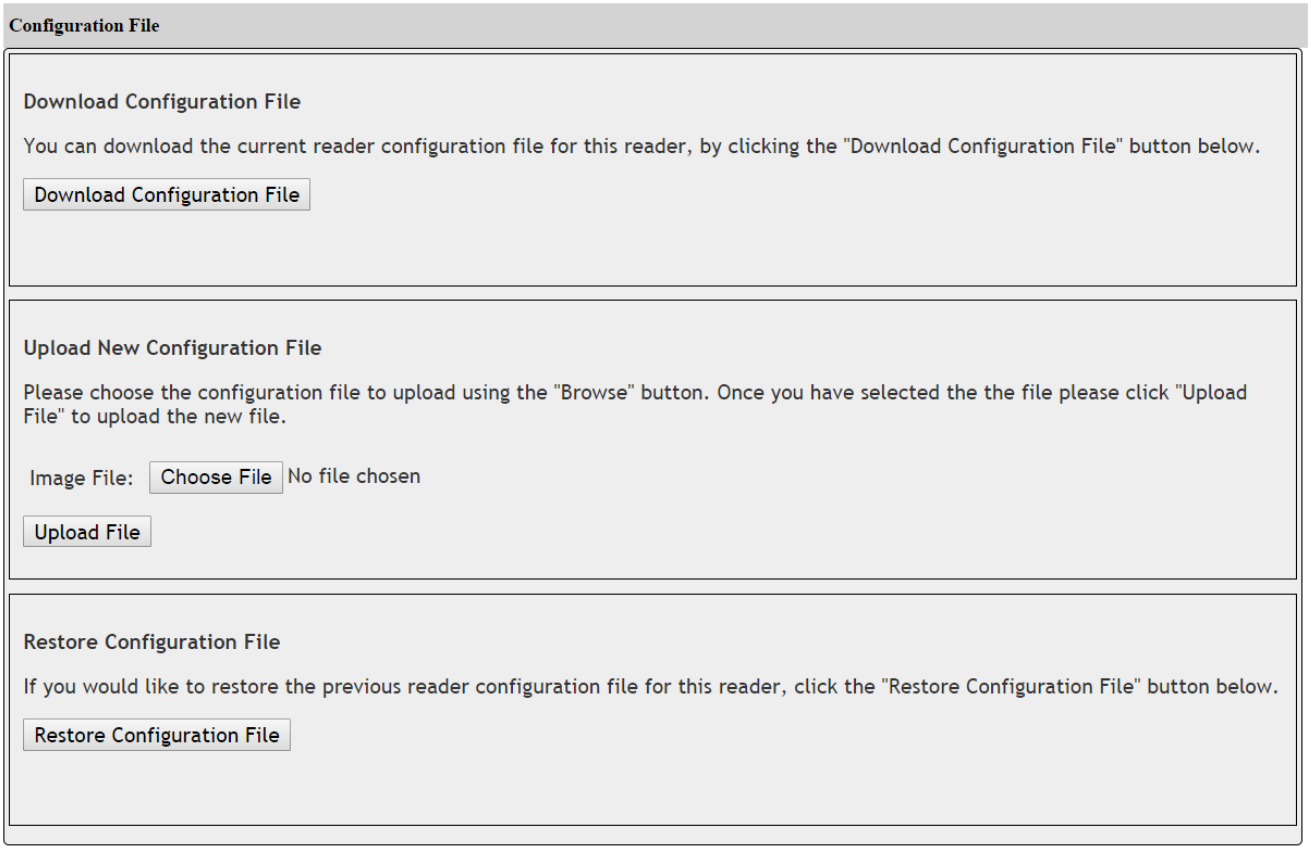
The Rhino Reader offers a screen saver feature to reduce display burn. The screen saver becomes active if no reader activity occurs within the timeout interval, which is defined on the Timings tab of the General submenu. A unique screen saver graphic can be created by an administrator and uploaded to the reader. The graphic must be in a .png format (24 bit is acceptable), and must be no bigger than 320px by 240px. DPI setting impacts the size of the graphic displayed. 72dpi is recommended.

The Upload Screen Saver Image function on the Screen Saver Image tab uploads the screen saver file of your choice.

NOTE You cannot set a screen saver if you are using FICAM (OSDP) mode or RM mode.

Configuration File Tab

Figure 71: Configuration File

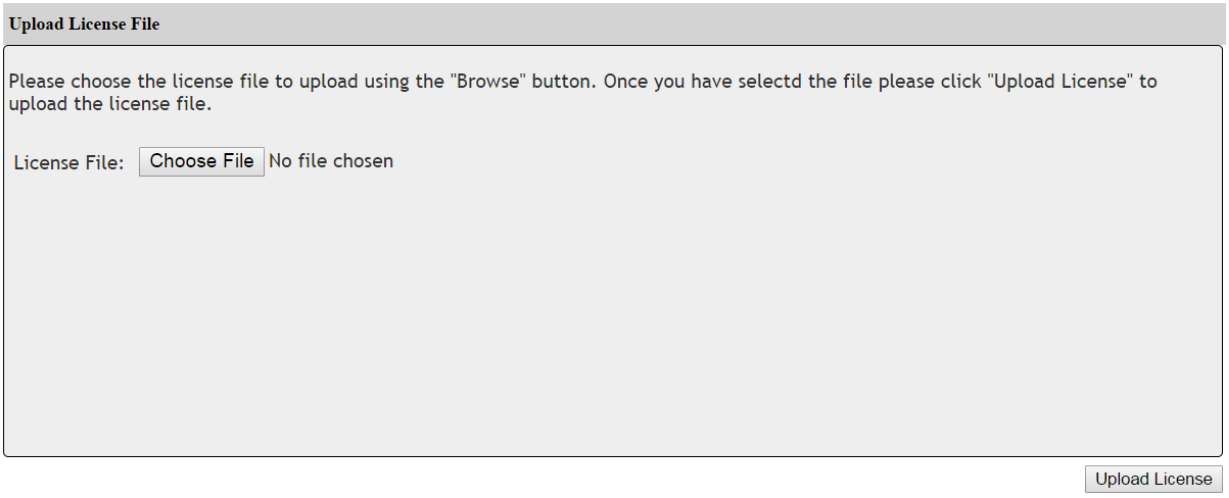


The Configuration File function provides administrators with a reader backup and recovery mechanism. Backup readers pressed into service can be configured to the settings of the reader being replaced.

Another use would be to transfer all settings from a reference reader to a group of new readers. Only individual network settings would need to be changed.

Upload License File Tab

Figure 72: Upload License File



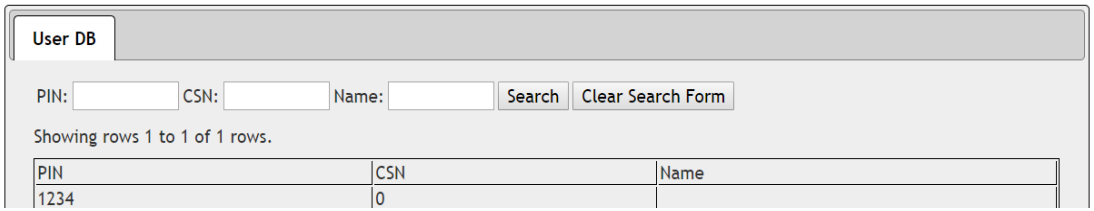
Innometriks utilizes a biometric processing algorithm that requires a license specific to the reader's MAC address. All new readers are shipped with the license in place; however a complete re-image of a reader may require the installation of a new license file.

Innometriks generates the license files and forwards them to the administrator for installation. Please have the reader's MAC address available when you contact Innometriks support.

The Upload License File function is used to send the license file to the reader which then performs the license installation.

View User DB Tab

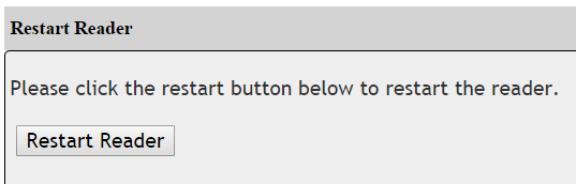
Figure 73: View User Database



The User DB function on the View User DB tab allows an administrator to view all the enrollments currently stored in the readers' user database. It is useful when validating that the central enrollment database was successfully synced out to all readers. It is also used to verify that an individual's enrollment templates are stored at the reader, which assists efforts to identify the individual causing repeated failed authentication attempts.

Restart Reader Tab

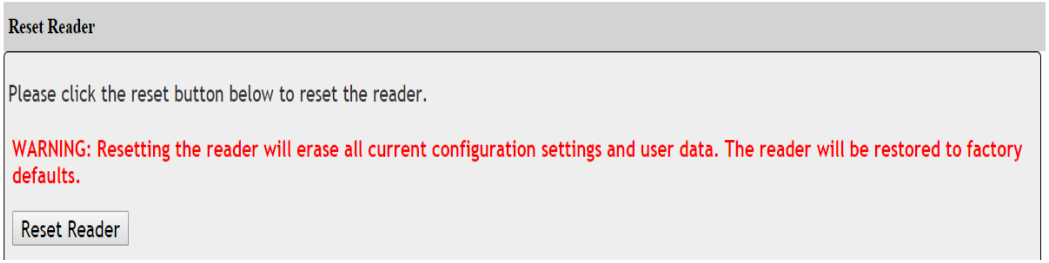
Figure 74: Restart Reader



The Restart Reader function allows an administrator to remotely reboot a reader.

Reset Reader to Factory Defaults Tab

Figure 75: Reset Reader To Factory Defaults



The Reset Reader to Factory Defaults utility erases all current settings and enrollment data. Use this utility with caution.

Logout

Clicking on the Logout tab of the WebGUI home screen immediately logs you out of the WebGUI interface.

7

Supported Card Types and Smart Card Formats

This appendix lists the supported card types and smart card formats.

Supported Card Types

The Rhino Reader offers enhanced security through encryption and is compatible with major card formats, including:

- The contactless reader contains a HID contactless smart reader module.
  - The HID SE module functions as the Cheetah SE's contactless smart card reader.
  - The carrier frequency of the RF interface is 13.56 MHz.
  - Supports the following card formats: CAC, DESFire + Infinitas EV1/EV2/EV3, HID Elite Media Keys, iCLASS, MIFARE, PIV, PIV-I, TWIC, smart card CSN, HID SEOS.

Reading a card using the contactless method

At the Present Card prompt display on the reader, place a card close to the reader and centered on the antennae markings.

Index

O

P

R

S

T

U

V

W

Glossary

A

authentication

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or on an authentication server. If the credentials match, the process is completed and the user is granted authorization for access.

B

biometric

Biometrics refers to metrics related to human characteristics. Biometrics authentication, or realistic authentication, is used by access control systems as a form of identification and access control.

C

CHUID

Card Holder Unique Identifier.

D

DESFIRE Card

MIFARE DESFire is the NXP Semiconductors-owned trademark of a series of chips widely used in contactless smart cards and proximity cards.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks. The DHCP is controlled by a DHCP server that dynamically distributes network configuration parameters, such as IP addresses, for interfaces and services.

F

FASC-N

Federal agency smart card number

G

gateway

A network gateway is an interconnecting system capable of joining together two networks that use different base protocols.

I

ICLASS Card

iCLASS smart cards from HID Global are 13.56 MHz read/write credentials for secure access control.

IP65

IP rating is also known as Ingress Protection or International Protection ratings. These standards are used to define the levels of sealing effectiveness of electrical enclosures against intrusion from foreign bodies such as dirt and water.

L

LED

A light-emitting diode (LED) is a two-lead semiconductor light source. In this case, the LED is graphically emulated rather than actual.

liveness test

A test performed to test if the biometric traits are from a living person rather than an artificial or lifeless person.

M

MAC address

A media access control address (MAC address) of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi.

Molex

Molex connector is the vernacular term for a two-piece pin and socket interconnection.

N

NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

O

OCSP

The Online Certificate Status Protocol (OCSP) is an internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track.

one-to-many

A type of comparison where one example is compared to many others - for instance when comparing a person's fingerprint to a set of fingerprints stored in a database.

One-to-One

A comparison where one example is compared to a known sample as verification - for example when a PIN entered is compared to the stored PIN associated with an identity.

P

physical access control system

A PACS is a particular type of physical access control system used as an electronic security countermeasure.

Ping

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

PIV Card

A personal identity verification (PIV) card is a United States Federal smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and to assure appropriate levels of security for all applicable Federal applications.

R

RS232

In telecommunications, RS-232 is a standard for serial communication transmission of data.

RS485

RS-485, also known as TIA-485(-A), EIA-485, is a standard defining the electrical characteristics of drivers and receivers for use in serial communications systems. Electrical signaling is balanced and multipoint systems are supported.

S

Syslog

Syslog is a logging mechanism for network devices to send event messages to a logging server, usually known as a Syslog server. The Syslog protocol is supported by a wide range of devices and can be used to log different types of events.

T

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the internet. It can also be used as a

communications protocol in a private network (either an intranet or an extranet).

Transaction Logging

A transaction log is a file, an integral part of every SQL Server database. It contains log records produced during the logging process in a SQL Server database.

TWIC Card

The Transportation Worker Identification Credential, also known as a TWIC® card, is required by the Maritime Transportation Security Act for workers who need access to secure areas of the nation's maritime facilities/vessels and other secure facilities.

W

WebGUI

WebGUI is an open source content management system released under the GNU General Public License.

Wiegand

The Wiegand interface is a de facto wiring standard which arose from the popularity of Wiegand effect card readers in the 1980s. It is commonly used to connect a card swipe mechanism to the rest of an electronic entry system.