tyco | Innometriks

Innometriks Cheetah SE Reader

User Guide

May 2023 8200-1558-02

G

www.swhouse.com

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.

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

Cheetah SE Reader™ is a trademark of Johnson Controls.

Products offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your regional sales representative.

Table of Contents

Preface 1

Conventions 2

Chapter 1 - Overview 3

Chapter 2 - Features 4

Reader models 5

Ordering codes 5

Reader components 6

Reader communications 7

Firmware updates 7

Configuration file operations 7

Standards 9

Open standards compliance 9

UL 294 rated features 9

Reading smart cards 10

Reader hardware modules 10

Chapter 3 - Installation 11

Pre-installation checks 12

Equipment 12

Site 12

Tools 12

Reader dimensions 13

Mounting Plate 13

Installation Instructions 13

Reader wiring 16

Molex 6-pin connector properties 17

Molex 9-Pin connector properties 17

End of Line Termination 18

Enabling EOL termination 18

Circuit properties 18

Wiring diagrams 20

Wiring for FICAM/OSDP mode or Hybrid OSDP mode connectivity 20

Wiring for RM connectivity 21

Wiring supervised inputs 22

Chapter 4 - Configuration 23
C•CURE 24
Keypad operation 25
Default factory settings 26
Chapter 5 - Network connectivity 27
RS485 reader communications 28
PACS / Reader formations 28
Offline network configuration setup for reader firmware update 29
Network information to note 29
Chapter 6 - Reader administration 30
Preparation for browser based administration 31
Browser-based administration 32
Configuring additional profile parameters 33
Chapter 7 - Profile Details 35
Profile FICAM 36
Profile Hybrid 37
Profile FIPS RM + iCLASS 38
Profile RM + CSN 39
Profile RM + SeOS 39
Profile RM + DESFire - Infinitas 40
Profile RM + DESFire - LEAF 41
Profile RM + Mifare 42
Profile RM + iCLASS 43
Profile OSDP + CSN 44
Profile OSDP + SeOS 44
Profile OSDP + DESFire - Infinitas 45
Profile OSDP + Mifare 46
Profile RM + DESFire - LEAF 46
Profile OSDP + iCLASS 48
Chapter 8 - HID Elite Key Installation 49
Introduction to iCLASS Elite and SE Elite programs 50
Provisioning iCLASS SE Reader Module with Elite Media keys 51
Loading Elite Media Keys to Cheetah SE Reader 51
Verifying Cheetah SE reader HID module firmware 51
Load the Elite Media Keys to the Cheetah SE Reader 52
Verifying successful loading of Elite Key Configuration cards 52
Appendix A - Usage of virtual output 53
Normal and Secure modes 54

Preface

The Cheetah SE 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:

Conventions 2

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 pertains 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

The Cheetah SE Reader is a networked smart card reader supporting OSDP and RM communication between the reader and the PACS interface panel.

You can use reader web services to manage the reader from an offline computer.

- Secure browser-based management
- Web-based firmware upgrades
- OSDP-based firmware upgrades
- Reader configuration file cloning

View default or modified settings at the reader using the reader keypad and LCD display. See Keypad operation on Page 25. The only configuration performed at the reader is modifying the LCD display brightness. Configure the other reader parameters in a web browser.

Features

This chapter describes Cheetah SE Reader features.

In this chapter:

Reader models 5
Reader components 6
Reader communications 7
Configuration file operations 7
Standards 9
Reading smart cards 10

Reader models

There are two indoor models of the Cheetah SE Reader:

- contact
- contactless and contact.

Additional gaskets protect the corresponding outdoor models against weather.

Ordering codes

Table 1: Cheetah SE Reader Product codes

Product codes	Description
INN-SECHTA-RF	Indoor: RF Only (Contactless)
INN-SECHTA-CT	Indoor: RF and Contact
INN-SECHTA-RFO	Outdoor: RF Only (Contactless)
INN-SECHTA-CTO	Outdoor: RF and Contact

Reader components

- LCD display - 2 x 16 characters for displaying reader parameters. You can adjust the contrast using the Set Contrast function on the keypad.
- Keypad - 3 x 4 touchpad contains numerals 0 to 9 and four unmarked function keys F1 to F4.
- Buzzer - Buzzer operation is controlled by the host.
- LED light bars
  - Two LED light bars at the left and right sides of the reader indicate status:
    - Green: **Access Granted**
    - Red: **Access Denied**, or **Reader Not Ready**
  - On units with a bottom contact reader, the LED light bar blinks amber to indicate that the reader is ready for the user to insert a contact card.
- Tamper support - enabled in PACS software
- Inputs and outputs
  - Two supervised inputs
  - Two physical outputs
    - One dry contact relay
    - One optically isolated TTL output
- One virtual output
  - The virtual input controls secure and normal mode.
  - It is controlled by the state of physical output.
  - See Appendix A - Usage of Virtual Output for more information.
- Power: 12 VDC, 1 A
- Temperature: 31° F (-35° C) to 150.8° F (66° C)
- Operational limits for LCD: -4° F (-20° C) to 150.8° F (66° C)
- Humidity: 0 to 95% RH non-condensing

Reader communications

- Multiple Communication Interfaces
  - Ethernet and RS-485
  - Relay Normally Open (NO) and Normally Closed (NC)
  - Supervised inputs
- Support for both RM and OSDP protocols
  - RM communication to iSTAR physical access control system
  - The reader supports FICAM and OSDP communication through an RS-485 port to the panel in an iSTAR Ultra or iSTAR Ultra SE.
  - OSDP profiles, including FICAM and HYBRID profiles, communicate through an RS-485 port to compatible panels such as the iSTAR Ultra and iSTAR Ultra SE.
- Controller communications
  - Gigabit Ethernet communication to host network. Use for configuration and troubleshooting.

NOTE

- Innometriks services communicate with readers web configuration interface.
- Only connect the Cheetah SE reader Ethernet network port when the reader operational configuration is set up on the web configuration interface. The Cheetah SE reader does not requite an Ethernet network to perform access control functions.
- Operation with an Ethernet cable is not UL tested. OSDP operation is not UL tested.

Firmware updates

- Perform updates by uploading firmware files through a web browser or through OSDP file transfer.

Configuration file operations

- Web User Interface
  - Save configurations to a file.
  - Restore configurations to this Cheetah SE reader, or any other configured Cheetah SE reader, from any saved configuration file.
  - Restore previous configuration.

NOTE The configuration file contains all independent reader settings such as card support configuration, LCD contrast setting, and reader communication options, such as RM or OSDP.

- OSDP File Transfer
  - Upload configurations to reader from the C•CURE host using OSDP file transfer.
  - Support for OSDP file transfers was added to Cheetah SE in firmware version 2.3.4. All firmware versions released after version 2.3.4 can be updated using OSDP download for systems with C•CURE 2.90 SP5 or later, and iSTAR Ultra FW 6.9.0 or later.
  - Updating readers using OSDP file transfer takes up to an hour to complete per reader. However, users can track the progress. Real time operations are not affected during the download process.
  - When the file transfer has been completed, the reader will reboot. The standard reboot takes 15 to 30 seconds and real time operations are impacted during this time. After the reboot, the reader runs the updated firmware version.

- Users can update multiple Cheetah SE readers per iSTAR simultaneously. Users can also update readers across multiple iSTAR controllers simultaneously. Each reader is updated using the process described above.

Refer to the *C•CURE 9000 Hardware Configuration Guide* for more information on performing the Cheetah SE update using OSDP File Transfer.

Standards

The Cheetah SE Reader complies with the following standards:

Open standards compliance

- ANSI 378
- FIPS 201
- FICAM
- ISO 14443
- ISO 15693

UL 294 rated features

- Destructive Attack: Level I
- Endurance: Level IV
- Line Security: Level I
- Power Standby: Level I

NOTE

- Cheetah SE readers are tested to UL 294 (Access Control Systems) standard.
- UL has not evaluated operations using an Ethernet cable, FICAM, Hybrid, or OSDP.

Reading smart cards

The Cheetah SE grants access to users through different smart card reading methods.

Reader hardware modules

There are two types of Cheetah SE Readers, contactless and contactless with contact.

- 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, Type B, DESFire + Infinitas, DESFire + LEAF, HID Elite Media Keys, EV1, EV2, iCLASS, MIFARE, PIV, PIV-I, TWIC, smart card CSN, HID SEOS.
- The contactless with contact reader contains the HID SE module for contactless card reading and the Microchip SEC1210 smart card reader module for contact card reading.
  - The HID module supports all features shown above.
  - The reader supports CAC, PIV, PIV-I and TWIC smart cards. A slot at the bottom of the reader accepts insertion of these chip cards.

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.

Reading a card using the contact method

At the **Present Card** prompt display on the reader, insert a card into the bottom of the reader with the card chip facing forward. Inserting the card incorrectly results in a card read error.

Installation

This chapter describes Cheetah SE Reader installation process.

In this chapter:

Pre-installation checks 12
Reader dimensions 13
Mounting Plate 13
Reader wiring 16
End of Line Termination 18
Wiring diagrams 20

Pre-installation checks

Before installing the reader, ensure you complete the following:

Equipment

- Verify that the contents of the shipped boxes match the packaging lists. See Table 2 for a detailed list of contents.

Table 2: Cheetah SE Reader box contents

Reader environment	Contents
Indoor	• Cheetah SE Reader • Quick start guide
Outdoor	• Cheetah SE Reader • Quick start guide • Outdoor install kit

- Use anchoring systems capable of sustaining at least 25 lb when installing the reader.

Site

- Check power, wiring, equipment clearances, and code compliance at the site.
- Ensure that the mounting site is ready by verifying that:
  - the site is approved and all wiring complies with UL requirements and other codes, as appropriate.
  - all preliminary site work is complete.
  - an appropriate power supply is accessible.
  - the site is clean and free of dust or other contaminants.
- Reader operating temperature is -31° F (-35° C) to 150.8° F (66° C).
- Operational limits of LCD: -4° F (-20° C) to 150.8° F (66° C)

Tools

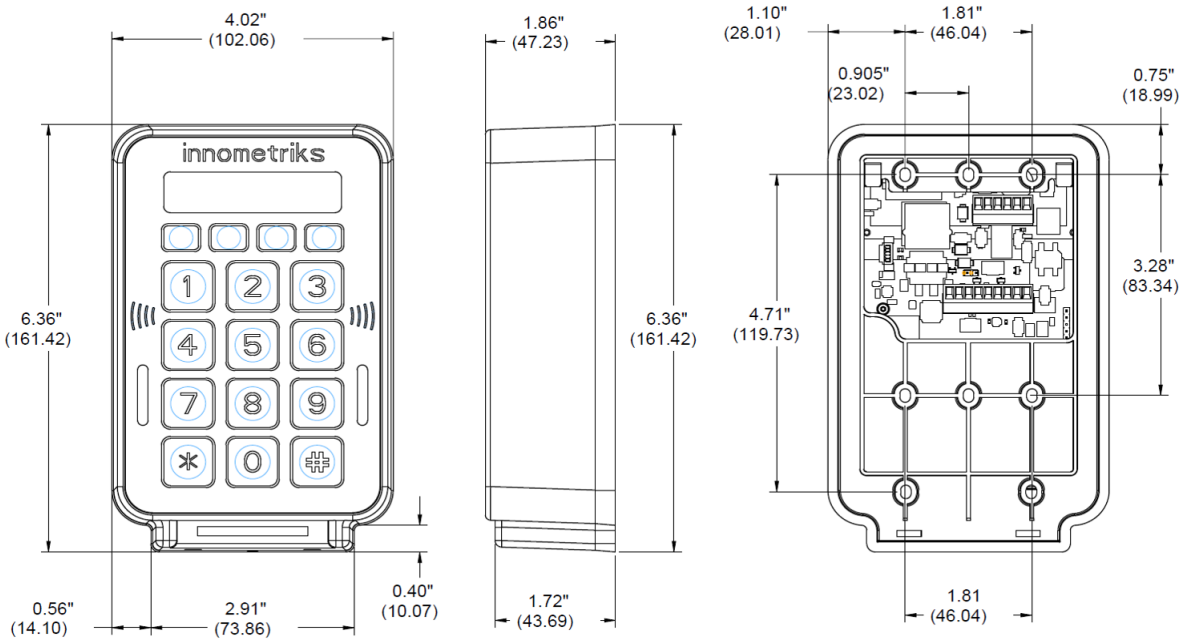
Ensure the proper tools, not supplied, are available:

- Small needle nose pliers
- Small Phillips screwdriver
- Small Torx screwdriver
- Wire strippers

Reader dimensions

Figure 1 shows the physical dimensions of the Cheetah SE readers. The dimensions of the contactless reader are the same as the contact models, except that the contact models have a card insertion slot at the bottom and the contactless models do not.

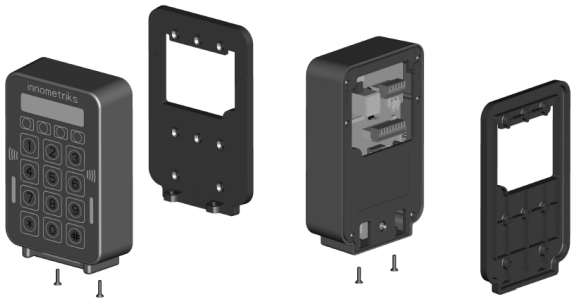
Figure 1: Reader dimensions



Mounting Plate

Figure 2 shows front and back views of the mounting plate for the Cheetah SE readers.

Figure 2: Mounting plate front and back views



Installation Instructions

You must complete a number of procedures to install the reader.

Removing the mounting plate from the reader housing:

1. Remove the two Torx screws located at the bottom of the reader housing using a Torx screwdriver - not supplied.
2. Separate the mounting plate from the reader housing.
3. Remove the 6-pin and 9-pin Molex connectors from the reader housing if already connected.

Wiring the connectors:

Disconnect all power sources before modifying the wiring.

1. Use proper ElectroStatic Discharge (ESD) procedures and follow instructions shown in Reader wiring on Page 16.
2. Reconnect the Molex connectors to the reader housing.

Attaching gaskets to mounting plate for outdoor installations:

- Insert the perimeter gasket to the front of the mounting plate and attach the wall gasket to the rear of the mounting plate. The Outdoor Install Kit includes both gaskets. See Figure 3 for an illustration of the outdoor gaskets using Table 3 as a legend.

Figure 3: Mounting plate with outdoor gaskets

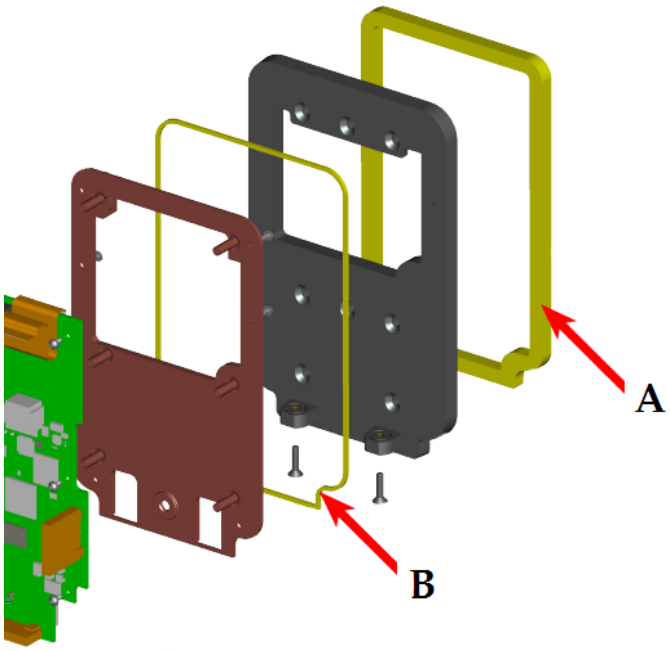


Table 3: Mounting plate gasket legend

Key	Description
A	Wall gasket
B	Perimeter gasket

Securing the mounting plate to a support:

Figure 2 on Page 13 shows the dimensions of the mounting plate for the Cheetah SE Reader.

With the mounting plate facing forward, attach the mounting plate to a wall or other support by inserting two or four screws into the mounting plate holes. See Figure 4 for an illustration of the mounting plate holes using Table 4 as a legend. The type of screws depends on the type of support used. See Table 5 on Page 15.

Figure 4: Mounting reader to a support

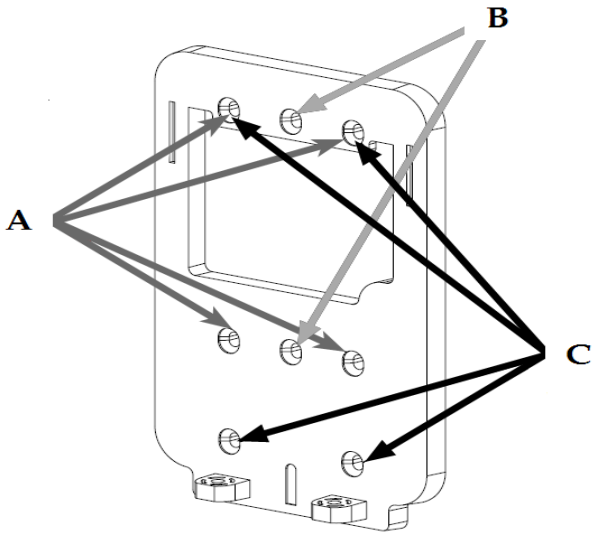


Table 4: Mounting reader to a support legend

Key	Description
A	Use the four outer holes for mounting to a double gang US wall box
B	Use the two middle holes for mounting to a single gang US wall box
C	Use these four holes for mounting to an exterior wall without a wall box

Figure 5: Screws for attaching reader to brick wall

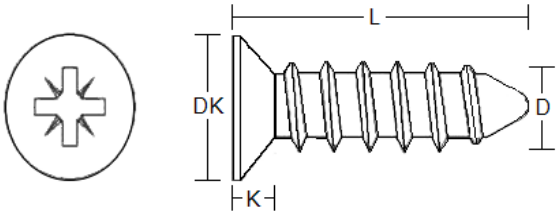


Table 5: Mounting reader to a support legend

Location	Anchor (not supplied)
Outdoor	No. 6 (3.5mm) x 1 in.(25.4 mm) long minimum PHIL CSK Tapping Screw A2 Stainless Steel: Gauge/Metric: #6 (3.5 mm) dk: 6.44 mm to 6.80 mm; k (max): 2.10 mm; d (drive): #2
Indoor	• ANCH PL W/O SCR 7/8L #6 #8 #10 • Butterfly Wall Plug for #6 Screw (for hollow or dry wall)

Attaching the reader housing to the mounting plate:

1. Affix the reader housing to the secured mounting plate.
2. Secure the reader housing to the mounting plate using proper ESD procedures by inserting the supplied screws into the two seats at the bottom of the reader. The type of screws are 4-40 UNC x 0.5 in. (12.7 mm) CSK Socket.
3. Apply power to the reader.

Reader wiring

Figure 6 shows the connector ports at the rear of the Cheetah SE Reader. Table 6 describes the function of each of these ports.

Figure 6: Cheetah SE Reader connectors

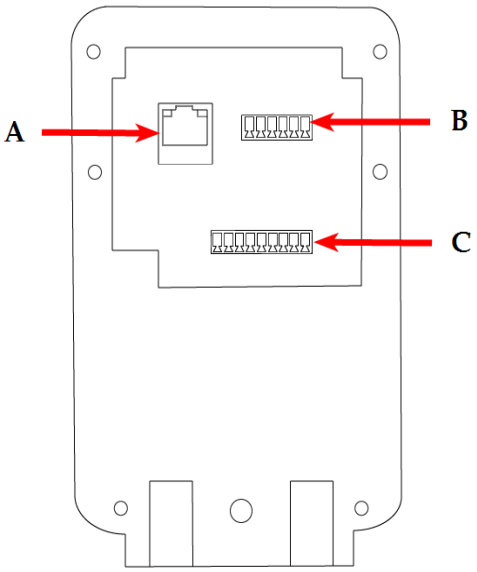


Table 6: Connector descriptions

Key	Connector	Description
A	Ethernet	RJ45 connector. Provides network connectivity for applications and browser based reader configuration
B	6-pin Molex	Bus, Relays, Output, Digital and Common Ground. See Table 7 on Page 17 for more information
C	9-pin Molex	Ground, Power, Bus, RS-485, and Supervised Inputs. See Table 8 on Page 17 for more information

Molex 6-pin connector properties

Table 7 describes the 6-pin Molex keyed connector. The connector is keyed, with pin 6 on the left and with pin 1 on the right as you face the rear of the reader.

Table 7: 6-Pin Molex connector properties

Pin #	Pin Name	Properties	Wiring
1	5 VDC	5 VDC outputs at 0.5 A	Optional 5 VDC supplied to external connector
2	RELAY1_ COM	Relay CO (Common)	Relay can be used to control magnetic and electric strikes.
3	RELAY_ NC	Relay NC	Relay can be used to control magnetic and electric strikes.
4	RELAY_ NO	Relay NO	Relay can be used to control magnetic and electric strikes.
5	CONN_WOUT0	Output 0	For RM or OSDP to PACS or device.
6	GND	Signal Ground	Reference.

Molex 9-Pin connector properties

Table 8 describes the 9-pin Molex keyed connector. The connector is keyed, with pin 9 on the left and with pin 1 on the right as you face the rear of the reader.

Table 8: 9-Pin Molex connector properties

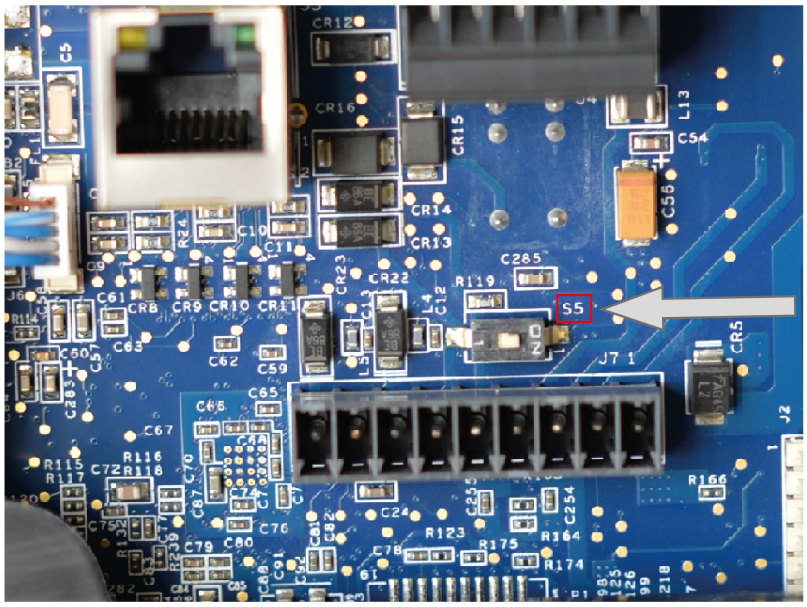
Pin #	Pin Name	Properties	Wiring
1	GND	Chassis Ground	Connect to Earth Ground by a low impedance path
2	PowerIN_N	Power Negative line	From negative terminal of power source
3	PowerIN_P	Power Positive line	From positive terminal of power source
4	5 VDC	5 VDC outputs at 0.5 A	Optional 5 VDC to external connector
5	RS-485-A	EIA-485 differential line 1: '+', TxD-/RxD-, or inverting pin	To PACS Panel RS-485 4-pin reader connector
6	RS-485-B	EIA-485 differential line 2:'−', TxD+/RxD+, or non-inverting pin	To PACS Panel RS-485 4-pin reader connector
7	GND	Signal Ground	Reference
8	SUPRV_ INPUT1	Supervised Input 1. Maximum length of 2000 ft (610 m)	From PACS Panel
9	SUPRV_ INPUT2	Supervised Input 2. Maximum length of 2000 ft (610 m)	From PACS Panel

End of Line Termination

End- of-Line (EOL) termination on both ends of the RS-485 lines is required for both OSDP or RM mode.

The EOL Termination slide switch (S5) is located just above the 9-pin (J7) connector as shown below. This switch is enabled by default.

Figure 7: S5 location on PC board



Enabling EOL termination

Slide the EOL Termination slide switch (S5) to the ON position to enable EOL termination.

When EOL Termination switch is enabled a 121.4Ω resistance is placed across the two RS-485 communication lines.

NOTE A standard 120Ω resistor can be used instead of the 121.4Ω resistor, wired across the RS-485 lines. The End-of-Line Termination slide switch (S5) must be disabled by sliding switch to the "1" position. This is to prevent a double termination condition when adding an external resistor.

Circuit properties

Table 9 shows additional information regarding circuits.

Table 9: Circuits power properties

Circuit	Voltage	Current
Power input	12 V	0.6 A
Power input	24 V	0.3 A
Relay Output (dry)	30 VDC	1 A

Table 9: Circuits power properties (continued)

Circuit	Voltage	Current
5 V Output (two connections provided)	5 V	0.5 A (combined maximum)
Optical Relay (wet)	5 V	0.05 A

Wiring diagrams

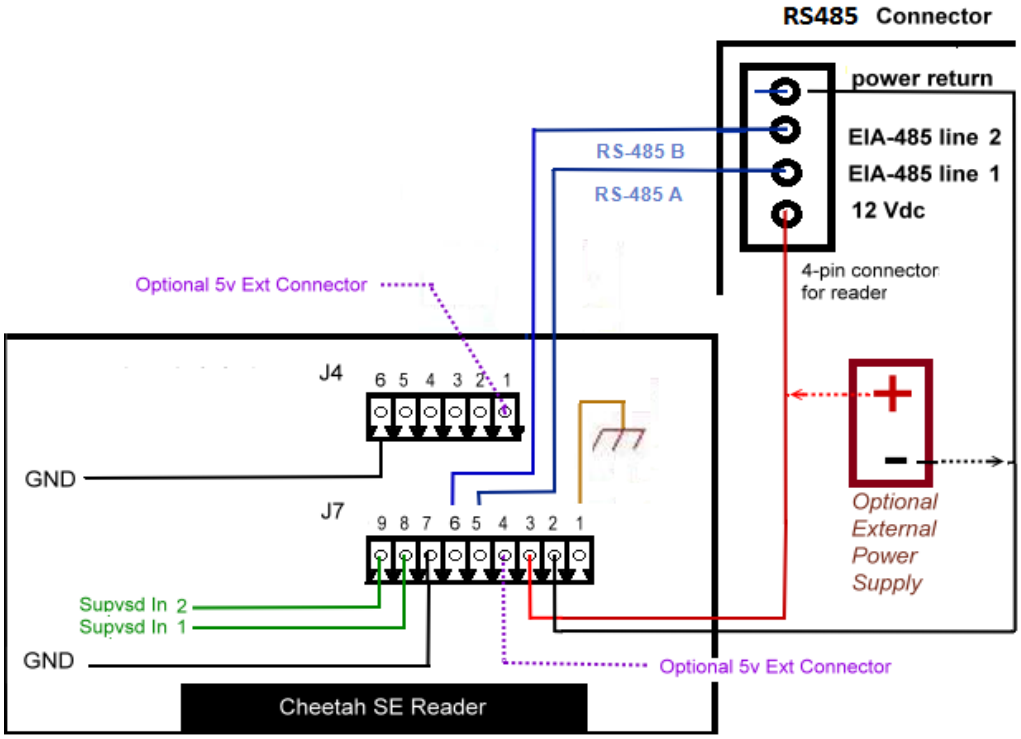
These diagrams provide an illustration of the correct wiring of the reader.

Wiring for FICAM/OSDP mode or Hybrid OSDP mode connectivity

Figure 8 shows an example of FICAM/OSDP mode or Hybrid OSDP mode wiring. Figure 10 on Page 22 shows wiring for supervised inputs.

NOTE If using C•CURE 2.70 SP2 or higher and iSTAR firmware v6.6.5 or higher, do not use an RS-485 board. Wire readers directly to the ACM board. See Figure 9 on Page 21.

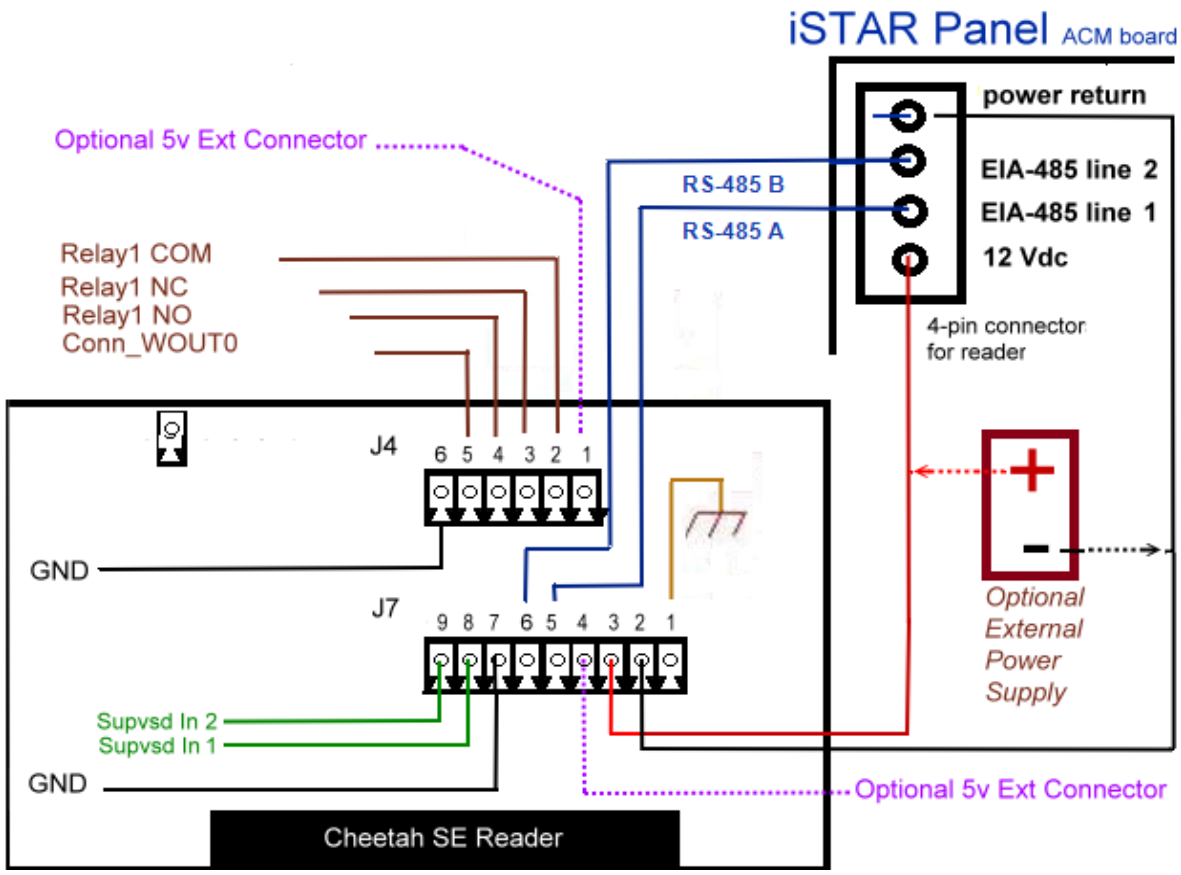
Figure 8: FICAM/OSDP or Hybrid OSDP mode wiring



Wiring for RM connectivity

Figure 9 shows an example of RM wiring. Figure 10 on Page 22 shows wiring for supervised inputs.

Figure 9: RM wiring



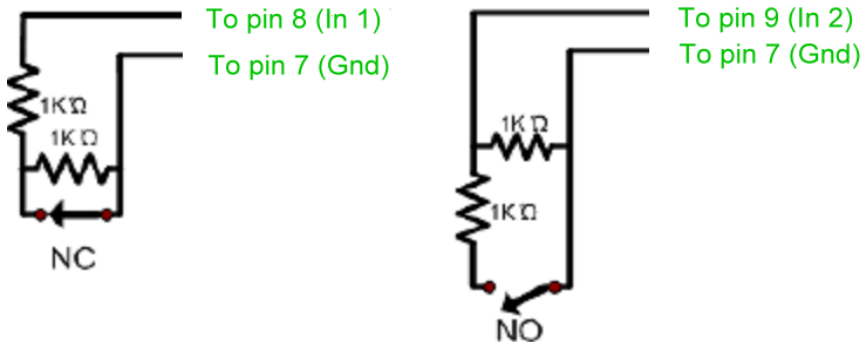
NOTE RM wiring connects directly to the ACM board

Wiring supervised inputs

Figure 10 shows examples of wiring normally closed (NC) and normally open (NO) supervised inputs.

The pin numbers refer to the 9-pin Molex connectors (J7) shown in Figure 8 on Page 20 and Figure 9 on Page 21.

Figure 10: Examples of supervised inputs



Configuration

This chapter describes Cheetah SE Reader configuration.

In this chapter:

C•CURE 24
Keypad operation 25

C•CURE

For LAN configurations, configure information for member controllers in the C•CURE Administration application. The C•CURE Administration Station downloads member configuration information to the master at start-up, and the master uses the information to configure the member controllers.

Refer to the *C•CURE 9000 Hardware Configuration Guide* and the C•CURE 9000 help documentation for configuration information.

Configuring over LAN

Requirements for LAN configurations vary from site to site. The following procedure describes most configurations:

1. Connect and power all iSTAR controllers.
2. Use the **ICU** to configure the following elements:
   - Define the master.
   - Specify the IP address of the master.
   - Obtain the Domain Name Server addresses automatically.
   - Define the host IP address or Fully Qualified Domain Name (FQDN) that the master communicates with.
3. Use the C•CURE Administration application to configure the following criteria:
   - Master and member names.
   - Master and member IP and MAC addresses.
4. Use the C•CURE Administration application to configure the cluster and download cluster information.

Keypad operation

Configuration of settings is not available at the reader. You must change these settings in the browser based administration. See Browser-based administration on Page 32 for more information on configuring the reader from a browser.

Displaying configured settings:

View configured settings at the reader.

- Press function keys **F1** and **F4** at the same time to display the Status Screen.
- Press a key, **1** to **9**, to display a setting.

Table 10 lists all available keypad operations in the Status Screen.

Table 10: Keypad operation on Cheetah SE Reader

Key	Status Screen Display
1	Current firmware version
2	Reader IP address
3	Ethernet Status: Connected or Not Connected
4	Reader Address
5	Reader Baud Rate
6	Unused
7	Tamper Status: Alarm or Secure
8	Supervised Inputs
9	Unused
0	Unused
#	Exit the status menu

Configuring reader brightness

Adjust reader brightness at the reader.

1. Pressing reader keys **F2** and **F4** simultaneously displays the screen contrast setting.

NOTE Sample text displays on line one; control keys display on line two.

2. Use the **F2** to increase or **F3** to decrease the display contrast.

Default factory settings

The Cheetah SE Reader has a number of default settings:

- The reader starts initially showing the default **RM + CSN** profile.
- Web user name set to **admin** and password set to **password**.

NOTE

For Administration Mode, you must set a new password after you first log on to the Cheetah SE Web Server.

Your password must contain at least 8 characters and 3 of the following 4 following requirements:

- 1 upper case letter
- 1 lower case letter
- 1 number
- 1 special character

You cannot recover a forgotten password. Return the reader to Innometriks for a reader firmware reinstallation by following the RMA returns process if the reader password is forgotten.

- IP set to **Static**.
- IP address set to **192.168.0.100**.
- RM address set to **1**.
- RM baud rate set to **9600**.
- Screen brightness and contrast set to the normal setting.

Network connectivity

This chapter describes Cheetah SE Reader configuration for Ethernet-based reader firmware update connectivity and RS485 or RS232 connectivity.

In this chapter:

RS485 reader communications 28
Offline network configuration setup for reader firmware update 29

RS485 reader communications

Innometriks readers communicate with the iSTAR Ultra family of controllers using the RS485 connections.

PACS / Reader formations

Install readers in one of the following formations:

- Single reader
- Daisy chain

Connecting two readers in a daisy chain formation

1. Connect the two data wires between pins 5 and 6 of both reader's 9-pin Molex connector.
2. Connect the two power wires between pins 2 and 3 of both reader's 9-pin Molex connector. Alternatively, the power source can be from an external power supply.
3. For FICAM mode or Hybrid mode, connect the first reader to one of the panel's RS-485 ports.
4. Ensure the last reader on the RS-485 communication lines have End of Line Termination enabled (slide S5 switch to ON). The other reader on the RS-485 communication lines must have the End of Line Termination disabled (slide S5 switch to "1").

NOTE Daisy chaining more than two Cheetah SE readers on one RS-485 bus, in either FICAM/OSDP or RM mode, is not recommended. Innometriks recommends one Cheetah SE reader per RS485 bus.

Offline network configuration setup for reader firmware update

Configure each reader to match the offline network environment before performing reader firmware updates via the Ethernet interface.

Network information to note

Before configuring the network settings, check the following:

- The Netmask you are using.
- If the network uses DHCP or Static IP addresses.
- If there are routers or switches in place.
- If TCP/IP ports are blocked between workstations, servers, or readers.
- The IP address of a gateway, if one is in place.
- If reader MAC addresses need to be submitted to network administration.

Ensure you define the following information for each reader:

- Enable or disable DHCP.
- If DHCP is disabled, the following must be defined:
  - Static IP address
  - Netmask
  - Gateway address if needed
  - Domain Name Server (DNS)

Reader administration

This chapter explains the Cheetah SE Reader administration menus and relevant options.

View the default or configured settings for the reader in the reader LCD display. Use browser-based administration to change all settings in the reader. You can only configure the LCD brightness at the reader. See Keypad operation on Page 25 for information on changing LCD brightness.

In this chapter:

Preparation for browser based administration 31
Browser-based administration 32

Preparation for browser based administration

Provide the administrator with the IP address of each reader before performing browser-based administration across a TCP/IP network connection.

Preparing for browser-based administration

1. Verify that the reader is properly wired for 12 VDC power.
2. Verify that the reader is connected to the network.
3. Apply power to the reader.
4. Obtain the reader IP address using the SE reader keypad and LCD display by pressing function keys **F1** and **F4** simultaneously, then pressing the **2** key.

Browser-based administration

Configure the reader settings using a web browser. You must configure the reader in C•CURE to enable browser based administration. Refer to **Chapter 12: Configuring Readers** in the *C•CURE 9000 Hardware Configuration Guide* for information on configuring a reader.

Powering On the reader

After configuring and applying power, a fully initialized reader, with default settings, displays **PRESENT CARD**. See Figure 11 for an illustration of this display.

Figure 11: Example of Reader Main Screen

To begin browser-based administration, you must get the reader IP address from the reader LCD display. See Preparation for browser based administration on Page 31 for instructions on viewing a reader IP address.

Browsers supported

Browser based administration is available through the latest stable version of the following browsers:

- Microsoft Edge
- Mozilla Firefox
- Apple Safari
- Google Chrome

Connecting to the reader from a networked host

1. From a web browser, connect to the reader using the reader's IP address. The login screen displays.

NOTE When connecting to the reader IP address, ensure you preface it with **https://** for a secure connection. For example, **https://10.10.101.10**.

2. On the login screen, enter the default web interface account name in the account name field.
   - The default account name is `admin`.
3. Enter the default password in the password field.
   - The default password is `password`.
4. You must change the default password, and, optionally, the account name before continuing to log into the web interface for the first time.
   a. (Optional) In the account name field, enter your new account name and submit it.
   b. In the password field, enter your new password then enter your password again to confirm it. Click submit. Your password must contain at least 8 characters and contain 3 of the following 4 items:
   - 1 upper case letter
   - 1 lower case letter
   - 1 number
   - 1 special character

NOTE
- You cannot recover a forgotten password or a forgotten account name. If you forget the password, return the reader to Innometriks for a reader firmware reinstallation by following the RMA returns process.
- Ensure that you enter your account name correctly if changing it in the web interface. An incorrect account name will cause future login attempts to fail.

Choosing a Profile

1. Select **Set Profile** to display the **Choose Profile** screen.
2. Choose a profile from the drop-down menu. The available profile selections are listed in Profile Details on Page 35.
3. Click on **Save Profile** to restart the reader with the changed profile parameters. Upon the reader restarting, log back in as administrator.

Configuring additional profile parameters

Configure additional parameters in the submenu of each profile. See Profile Details on Page 35 for details on these additional parameters.

Configuring network for Static or DHCP

1. Select **Network** from the main screen **Network** tab or from the main screen bulleted option **Network**.
2. Enable a static or DHCP network:
   - Static: Enter the IP Address, Netmask, Gateway and DNS in the appropriate fields.
   - DHCP: Select the checkbox to enable DHCP.

3. Select **Update Settings**. The reader restarts with the updated settings.

Selecting Utility Options

Selecting the **UTILITY** tab from the main screen displays the utility options:

- **WEB PASSWORD**
  - To change the browser-based administration password, select **WEB PASSWORD**.
- **UPDATE**
  - To update reader firmware, select **UPDATE** and supply the location of a new firmware file. Click the **Upload File** button to upload the file to the reader and update the firmware. The reader then restarts, if required.
- **CONFIGURATION FILE**
  - To display options to download, upload, or restore a configuration file, select **CONFIGURATION FILE**.
- **RESET FACTORY SETTING**
  - To reset the reader to factory defaults, select **RESET FACTORY SETTING**.
- **GET READER SE3200 MODULE FIRMWARE VERSION**
  - To retrieve the Cheetah SE Reader HID SE3200 Module firmware version, select **GET READER SE3200 MODULE VERSION**. You can view the Reader HID SE3200 Module firmware version number, on the SysInfo web page.
- **LOAD JCOP CARD ELITE KEYS**
  - To provision a Cheetah SE Reader HID SE3200 Mark 2 Module with Elite Media keys, select **LOAD JCOP CARD ELITE KEYS**.
- **RESTART**
  - To restart the reader, select **RESTART**.

Profile Details

This chapter explains the Cheetah SE Reader submenus of the **Profile** settings.

In this chapter:

Profile FICAM 36
Profile Hybrid 37
Profile FIPS RM + iCLASS 38
Profile RM + CSN 39
Profile RM + SeOS 39
Profile RM + DESFire - Infinitas 40
Profile RM + DESFire - LEAF 41
Profile RM + Mifare 42
Profile RM + iCLASS 43
Profile OSDP + CSN 44
Profile OSDP + SeOS 44
Profile OSDP + DESFire - Infinitas 45
Profile OSDP + Mifare 46
Profile RM + DESFire - LEAF 46
Profile OSDP + iCLASS 48

Select **Set Profile** from the main screen and choose a profile to view its settings.

Profile FICAM

Change settings of the profile by editing the fields outlined in the table.

Table 11: FICAM fields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	This can be set or cleared through the reader web interface. Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR controller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Enable Card PIN Prompt Beep	This can be set or cleared through the reader web interface. When set, the reader produces a beep sound that prompts for PIN entry.
Require Card PIN in Normal Mode (not to be set if using 'High Assurance')	Select this check box if you require a smart-card PIN for access in Normal Mode. Normal Mode is the default when output 2 is inactive.
Require Card PIN in Secure Mode (not to be set if using 'High Assurance')	Select this check box if you require a smart-card PIN for access in Secure Mode. Secure Mode is the default when output 2 is active.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile Hybrid

Change settings of the profile by editing the fields outlined in the table.

Table 12: Hybrid fields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	This can be set or cleared through the reader web interface. Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR controller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Enable Card PIN Prompt Beep	When enabled, the reader generates a beep sound to prompt for PIN entry.
Require Card PIN in Normal Mode (not to be set if using 'High Assurance')	Select check box if users require a PIN for access in this mode.
Require Card PIN in Secure Mode (not to be set if using 'High Assurance')	Select check box if users require a PIN for access in this mode.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile FIPS RM + iCLASS

Change settings of the profile by editing the fields outlined in the table.

Table 13: FIPS RM+ iCLASS fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Enable Card PIN Prompt Beep	When set, the reader produces a beep sound to prompt for PIN entry.
Require Card PIN in Normal Mode	Select this check box if you require a smart-card PIN for access in Normal Mode. Normal Mode is the default when output 2 is inactive.
Require Card PIN in Secure Mode	Select this check box if you require a smart-card PIN for access in Secure Mode. Secure Mode is the default when output 2 is active.
Allow Alt Card in Normal Mode	Allow FIPS card types and alternative card types in this mode.
Allow Alt Card in Secure Mode	Allow FIPS card types and alternative card types in this mode.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

NOTE

- In this reader version, the **Alt Card** (alternative card type) currently supports **iCLASS**.
- There is no PIN requirement for iCLASS cards when Allow Alt Card and Require Card PIN are both selected.

Profile RM + CSN

Change settings of the profile by editing the fields outlined in the table.

Table 14: RM + CSN fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + SeOS

Change settings of the profile by editing the fields outlined in the table.

Table 15: RM + SeOS fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + DESFire - Infinitas

Change settings of the profile by editing the fields outlined in the table.

Table 16: RM + DESFire - Infinitas fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
App Read Key	UID (Unique IDentifier) based diversified key stored on the card.
Finger App Key (OCPSK)	UID based diversified key that calculates the digital signature in each data object.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + DESFire - LEAF

Change settings of the profile by editing the fields outlined in the table.

Table 17: RM + DESFire - LEAFfields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	This can be set or cleared through the reader web interface. Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR contoller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Application Read Only Key	UID (Unique IDentifier) based diversified key stored on the card.
Key Number	Read Access Rights via 8 keys.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + Mifare

Change settings of the profile by editing the fields outlined in the table.

Table 18: RM + Mifare fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Mifare Key	UID (Unique IDentifier) based diversified key stored on the card.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + iCLASS

Change settings of the profile by editing the fields outlined in the table.

Table 19: RM + iCLASS fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile OSDP + CSN

Change settings of the profile by editing the fields outlined in the table.

Table 20: OSDP + CSN fields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR contoller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile OSDP + SeOS

Change settings of the profile by editing the fields outlined in the table.

Table 21: OSDP + SeOS fields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	This can be set or cleared through the reader web interface. Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR contoller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile OSDP + DESFire - Infinitas

Change settings of the profile by editing the fields outlined in the table.

Table 22: OSDP + DESFire - Infinitas fields and descriptions

Field	Description
Reader Address	Set to values 1 through 8.
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR contoller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Application Read Only Key	UID based diversified key that is stored on the card.
OCPSK Key	UID based diversified key that calculates the digital signature in each data object.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

NOTE The user inputs the **Validation Key** and OCPSK Key provided by the panel software.

Profile OSDP + Mifare

Change settings of the profile by editing the fields outlined in the table.

Table 23: FIPS OSDP + Mifare fields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR controller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
Mifare Key	UID (Unique IDentifier) based diversified key stored on the card.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile RM + DESFire - LEAF

Change settings of the profile by editing the fields outlined in the table.

Table 24: RM + DESFire - LEAFfields and descriptions

Field	Description
Enable Keypad Beeper	Select check box if you require a beep for each key press.
Enable Key Installation	This can be set or cleared through the reader web interface. Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Require Secure Channel	This can be set or cleared through the reader web interface. When set, the iSTAR contoller and the Cheetah SE reader must use "OSDP-SC, full security" mode for communications. The reader will communicate outside of this mode to enter secure channel but it will not allow control or provide sensitive status. Software House recommends setting the "Require Secure Channel" flag.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Application Read Only Key	UID (Unique IDentifier) based diversified key stored on the card.
Key Number	Read Access Rights via 8 keys.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

Profile OSDP + iCLASS

Change settings of the profile by editing the fields outlined in the table.

Table 25: OSDP + iCLASS fields and descriptions

Field	Description
Enable Key Installation	Replaces a default well-known key with a secure key known only to the panel. This creates a secure connection to the reader. The panel clears the check box and only accepts the use of the secure key for further connections to the reader. Select the check box again if you move the reader to a different panel. NOTE: Enable Key Installation is off by default.
Enable Keypad Beeper	Select check box if you require a beep for each key press.
OSDP Address	Set to values 0 through 7.
Baud Rate	Set to 9600, 19200, 38400, 57600, or 115200 baud.
Enable Biometrics in Normal Mode	Select this check box if you require fingerprint biometric for access in Normal Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometrics in Secure Mode	Select this check box if you require fingerprint biometric for access in Secure Mode. This is only applicable for Cheetah SE Bio models.
Enable Biometric Retry on Fail	Select this check box if you want users to retry for access using biometrics after a failed attempt. This is only applicable for Cheetah SE Bio models.
Biometric Timeout	Choose a value in seconds after which users can reattempt entry. This is only applicable for Cheetah SE Bio models.
Biometric Matching Threshold	From the menu, choose a value. There are 3 value options, Low, Medium, and High. This is only applicable for Cheetah SE Bio models.
Submit	Reboot the reader with the new profile settings in effect.
Cancel	Clear any changes and return to the main screen.

HID Elite Key Installation

This chapter explains HID Elite Key installation.

In this chapter:

Introduction to iCLASS Elite and SE Elite programs 50
Provisioning iCLASS SE Reader Module with Elite Media keys 51
Loading Elite Media Keys to Cheetah SE Reader 51
Verifying Cheetah SE reader HID module firmware 51
Load the Elite Media Keys to the Cheetah SE Reader 52
Verifying successful loading of Elite Key Configuration cards 52

Introduction to iCLASS Elite and SE Elite programs

The iCLASS Elite and SE Elite programs include a credential format and custom authentication key, specifically assigned to each customer, with end users receiving their own proprietary key to increase security. This key protects the card number within the access control application of the card. iCLASS Elite and SE Elite are available for qualified end-users via formal enrollment and acceptance by HID Global.

HID assigns the key to guarantee uniqueness, and programs the site-specific readers and credentials. This private key is shared between the iCLASS or SE credential and the Elite enabled physical access reader. The reader will only be able to authenticate credentials that are loaded with the same private key following mutual authentication. Only matching cards and readers will work together, prohibiting cards and readers from foreign populations to enter and function within the company's Elite secured population. The Elite Program can use any format, including the HID Corporate 1000 format.

Provisioning iCLASS SE Reader Module with Elite Media keys

To provision an iCLASS SE Reader Module with Elite Media keys, you must obtain a pair of JCOP cards from HID.

There are two JCOP cards supplied by HID:

■ Elite Preparation card - this replaces the HID Admin SNMP keys contained in the iCLASS SE Reader Module with the Elite version, in preparation for loading the Elite Media keys.

■ Elite Keyset Configuration card containing SNMP messages to load the Elite Media keys. These messages are encrypted using the Elite HID Admin SNMP keys previously loaded into the iCLASS SE Reader Module.

NOTE

- Once a configuration card has been applied to an iCLASS SE Reader Module, the same card cannot be applied again until a different configuration card has been applied.
- If the application of a configuration card is interrupted, represent the same configuration card to finish the application process.

Loading Elite Media Keys to Cheetah SE Reader

This section describes how to verify if a Cheetah SE reader has the correct HID module firmware and how to load HID Elite Media Keys to a Cheetah SE reader.

NOTE

Cheetah SE readers produced prior to Jan 2022 have the 'HID SE3200 Mark 1' module installed and will not correctly process the Elite Media Key Configuration cards.

Verifying Cheetah SE reader HID module firmware

Follow the steps below to verify the Cheetah SE reader HID module firmware:

1. Login to Reader Web interface.
2. Select and invoke the **Util – Get SE3200 Module Firmware Version** option. The reader reboots.
3. Login to the Reader Web Interface.
4. Select **Info** or **System Information**.
5. Go to Web Interface Info summary web page to view the **SE3200ModuleVersion** entry.
    a. If the HID SE3200 Mark 2 module is installed, the **SE3200ModuleVersion** value is equal to 1.139. The reader supports HID Elite Media Key installation cards.
    b. If the HID SE3200 Mark 1 module is installed, the **SE3200ModuleVersion** value is equal to 1.25. The reader does not support HID Elite Media Key installation cards.

NOTE

Do not apply HID Elite Media Keys installation cards to a HID SE3200 Mark 1 module. This corrupts the HID Standard Media Keys values, disables the Cheetah SE reader card read functionality, and permanently damages the reader.

Load the Elite Media Keys to the Cheetah SE Reader

To load the Elite Media Keys to the Cheetah SE Reader, you must ensure you have the required pair of Site JCOP Configuration cards:

- Elite Admin Keys Configuration card
- Elite Media Keys Configuration card

NOTE Each of the steps must be performed for each of the Elite Keys Configuration cards.

Follow the steps below to load the Elite Media Keys to a Cheetah SE reader:

1. Login to the Cheetah SE Web interface, navigate to the Utilitytab and select Load JCOP Card Elite Keys. The Cheetah SE reader displays the following text:

   ```
   ELITE KEY MODE

   CYCLE RDR POWER
   ```

2. Disconnect and reconnect power to the reader.
3. Within 2 seconds of powering the reader, present the Elite Admin keys configuration card. Place the card against the front of the reader body just below the 4 function keys. Hold the card in this position for 34 seconds. The reader will reboot within
4. Repeat steps 1 - 3 to install the Elite Media Keys configuration card.

Verifying successful loading of Elite Key Configuration cards

Follow these steps to verify that both Elite Key Configuration cards were applied successfully:

1. Present the Site Elite Access card to the Cheetah SE reader.
2. If `Read Error` is displayed on the reader, the site Elite Key installation has failed. Repeat the installation procedure, starting with the Elite Admin Keys Configuration card.

A

Usage of virtual output

Normal and Secure modes

Virtual Outputs have two modes, Normal and Secure. In Normal access conditions, the reader is set to Normal mode. In states of heightened security, the reader will switch to Secure mode.

A virtual switch controls the 'local' security state. The local ‘Secure’ state is activated using a virtual switch connected to the second output. The second output is controlled by PACS.

High Assurance uses full PKI authentication when in Normal and Secure states. Security options and security mode is controlled by PACS. PACS determine if a CARD PIN or fingerprint is required, and when iClass cards are permitted. 'Local' options are turned off when using High Assurance.

During High Assurance enrollment, there is an option to share or withhold the CARD PIN. High Assurance requires 'local' PINs to be stored as a Secure PIN Entry (SPE). PACS control the second output when SPE is used. If you require a 'local' PIN and a High Assurance PIN, the reader will ask for two PIN entries or two fingerprint checks.

NOTE

- The second output works in one direction. You cannot force the output high or low, this will not change the ‘local’ security condition.
- High Assurance is a licensed feature. FICAM and HYBRID are the only profiles that work with ‘High Assurance’.
- In Secure PIN Entry (SPE), the CARD PIN is stored in the reader. If a local biometric option is used, SPE is selected automatically. The reader requires SPE to read fingerprint templates from the card.