Software House

C•CURE 9000 v3.10 Go Reader User Guide

www.swhouse.com

A1638371LU A

August 2025

Contents

Overview

C•CURE Go Reader is a mobile security solution that validates personnel credentials and performs roll calls during an emergency. The C•CURE Go Reader Android app is available on an all-in-one Android device with an embedded read head, such as the Coppernic Access-ER or Coppernic C-One². It also can be installed on an Android mobile device and paired with a Serialio idChamp card reader with BLE or SPP mode support, an rfIDEAS WaveID® Nano USB-C reader, or a MagTek iDynamo 6 USB-C reader.

You can use the Go Reader to:

- Control check points.
- Manage swipe access.
- Collect card swipe GIS geographical location for display on a C•CURE 9000 workstation map.

Figure 1 shows the components of the C•CURE Go Reader mobile security solution for Android devices.

Figure 2 shows the components of the C•CURE Go Reader mobile security solution for Access ER and C-One² devices.

See C•CURE Go Reader tested on Android devices for information on the Go Reader 3.00 components.

Figure 1: C•CURE Go Reader components for Android devices

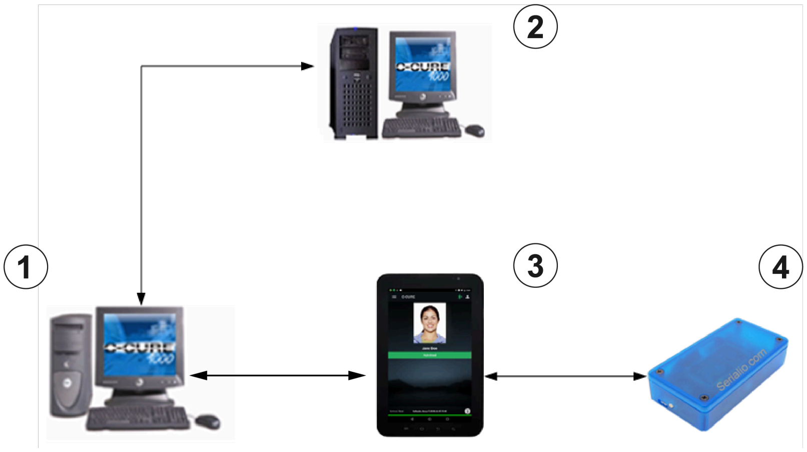


Table 1: C•CURE Go Reader components for Android devices

Callout	Component
1	C•CURE 9000 Application Server running Internet Information Services (IIS) and victor Web Services
2	C•CURE 9000 Database Server
3	Android device running C•CURE GoReader app
4	Serialio idChamp HS3 card reader, rf IDEAS WaveID® Nano USB-C reader, or MagTek iDynamo 6 USB-C reader.

Figure 2: C•CURE Go Reader components for C-One² devices

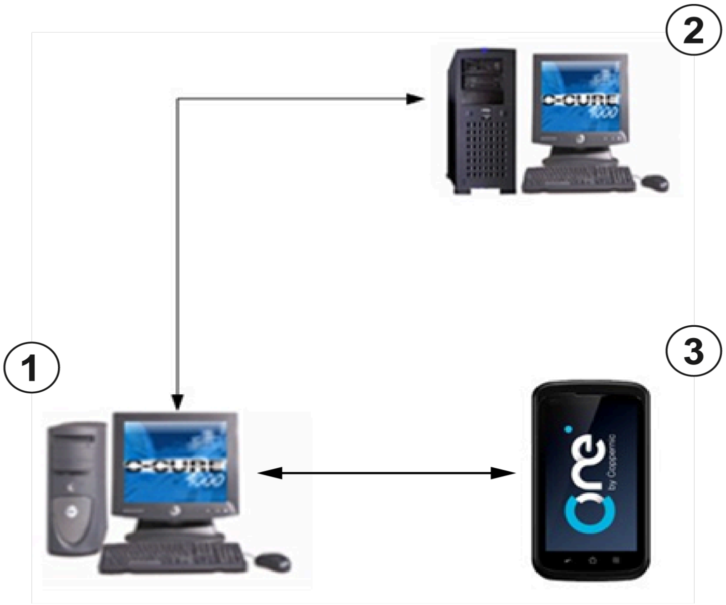


Table 2: C•CURE Go Reader components for Access-ER and C-One² devices

Callout	Component
1	C•CURE 9000 Application Server running Internet Information Services (IIS) and victor Web Services
2	C•CURE 9000 Database Server
3	Access-ER or C-One² device

Use C•CURE Go Reader for the following:

- **Configuring and managing C•CURE Go Reader doors:**
  - Configuring a Serialio idChamp RS3 reader, see Serialio idChamp RS3 configuration sequence.
  - Configuring an rfIDEAS WaveID Nano USB-C reader, see Configuring Wave ID Nano USB-C reader.
  - Configuring a MagTek iDynamo 6 USB-C reader, see Configuring MagTek card formats on the Go Reader editor.
  - Configuring card formats for Serialio idChamp RS3 reader, see Configure card formats in the Serialio idChamp RS3 reader.
  - Enabling or disabling reader modes and options, see Go Reader editor tasks.
  - View the status of devices that you are using with the Go Reader app, see C•CURE Go device editor.
- **Validating personnel credentials:**
  - Downloading and installing the C•CURE Go Reader app on Android devices, see Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices.
  - View card access status on Android devices when a card is swiped, see C•CURE Go Reader screen.
- Activating facility code validation, see Activating facility code validation.
- Enabling and viewing GIS location in card swipe journal messages, see View GIS location in card swipe journal message.
- **Determining the number of missing personnel in an area:**
  - Viewing roll call, see Roll call.
  - Viewing a list of roll call areas that have missing personnel, see Area information screen.
  - Viewing a list of missing personnel in each roll call area, see Viewing personnel in a missing area.

  - Setting the maximum personnel for roll call display, see Setting the maximum personnel for roll call display.
- **Monitoring and managing check-in and check-out of personnel at doors with check point:**
  - Activating check point, see Activating check point.
  - Creating a check point, see Creating a check point.
  - Activating check-in and check-out modes, see Activating check in mode.
  - Activating validation mode, see Activating validation mode.
  - Removing personnel when validation mode is activated, see Removing personnel when validation mode is activated.
  - Checking in personnel when validation mode is activated, see Checking in personnel when validation mode is activated.
  - Viewing personnel in filter mode, see View personnel in filter mode.
  - Downloading and saving check point personnel lists into a PDF file, see Downloading personnel lists for check point.
- Randomly screening personnel at doors, see Go Reader editor.
- Selecting custom fields for roll call and swipe and show, see Adding a custom data field for swipe and roll call.
- **Impersonating doors:**
  - Activate door impersonation mode and select a door to impersonate, see Impersonating a door.
  - Viewing card swiping with door impersonation enabled, see Impersonate a door using the Go Reader app.
- **Enforcing timed anti-passback:**
  - Activating timed anti-passback, see Activating timed anti-passback.
  - Swiping cards with timed anti-passback on the GoReader app, see Card swiping with timed anti-passback on the Go Reader app.
- **Manually mustering personnel:**
  - Activate the manual mustering feature, see Activating manual mustering.
  - Muster a person who does not have access to their card, see Manual mustering with roll call.
  - Activate the offline mustering feature, see Activating offline mustering.
- Re-synchronizing data from the C•CURE 9000 system to the C•CURE Go Reader device manually, see Synchronizing the C•CURE Go Reader from the C•CURE Go Reader device.
- Configuring C•CURE event triggers based on reader activation state and synchronization status, see Configuring triggers and events.

Considerations for Access-ER and C-One² devices

Coppernic designs, produces, and deploys professional mobile devices of control and global mobility technologic solutions combining hardware, software, and analysis and data management. Where necessary, this user guide describes additional concepts and procedures that are required to use the C•CURE Go Reader app on Coppernic Access-ER and C-One² Android hand-held devices.

You can use the C•CURE Go Reader app with the following models of the Access-ER and C-One² Android handheld units.

- Access-ER with HID-CK OMNIKEY 5127 read head with HF and LF cards, including iCLASS and Seos.
- C-One² with the ASK read head. HF cards are used for special circumstances.
- C-One² with the HID SE3200 MK2 read head with HF and LF cards, including iCLASS and Seos. This is the standard model for most applications. The part number is COP-C2-1710082.

For more information about the components of the C•CURE Go Reader mobile security solution for Access-ER and C-One² devices, see C•CURE Go Reader tested on Access-ER and C-One² devices.

Compatibility and connectivity

The C•CURE Go Reader app connects to a C•CURE 9000 system. The C•CURE 9000 Enterprise architecture is supported, however, the Go Reader server integration is not directly installed on the Master Application Server (MAS). See Use Go Reader in an enterprise environment for more details.

You might need to install a third-party application to your Android device to establish a VPN connection to your server. You can also use a separate mobile device as a portable Wi-Fi hotspot to create a connection between your C•CURE Go Reader device and the server. If you are connecting through a Wi-Fi connection, you must be on the same network as your C•CURE 9000 Server.

ⓘ **Note:** The C•CURE Go Reader app is supported on Android 8.0 and later. It is not supported on Apple iOS, Windows Phone and the Windows desktop operating systems.

ⓘ **Note:** Wi-Fi Protected Access (WPA) is a security certification that secures wireless computer networks on Android devices. WPA2-Enterprise and WPA3-Enterprise offer a high level of security control as they both use an 802.1X server for authentication. WPA2-Enterprise certification is used on older devices and WPA3-Enterprise certification on newer devices. This does not impact use of the Go Reader application or Go Reader Driver Services application.

ⓘ **Note:** If the IP address of the C•CURE 9000 system changes, a full synchronization of the unit is required.

For more information about creating VPN and Wi-Fi connections, see Creating connections.

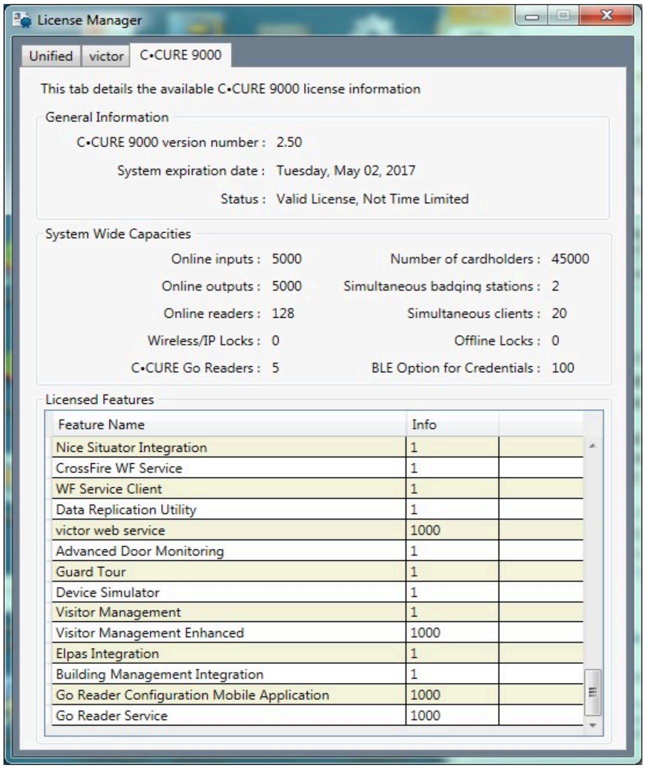
Licensing

The number of Android C•CURE Go Reader devices that you can simultaneously connect to your C•CURE 9000 server is determined by your C•CURE 9000 license. Two items are required:

- C•CURE Go Reader count.
- victor Web Service counts each connection between the Android C•CURE Go Reader device and the C•CURE 9000 server.

Figure 3 shows a license with a maximum of 5 C•CURE Go Reader devices that can be connected.

Figure 3: License with 5 C•CURE Go Reader devices



This tab details the available C•CURE 9000 license information

General Information

C•CURE 9000 version number : 2.50

System expiration date : Tuesday, May 02, 2017

Status : Valid License, Not Time Limited

System Wide Capacities

Online inputs :	5000	Number of cardholders :	45000
Online outputs :	5000	Simultaneous badging stations :	2
Online readers :	128	Simultaneous clients :	20
Wireless/IP Locks :	0	Offline Locks :	0
C•CURE Go Readers :	5	BLE Option for Credentials :	100

Licensed Features

Feature Name	Info	
Nice Situator Integration	1	
CrossFire WF Service	1	
WF Service Client	1	
Data Replication Utility	1	
victor web service	1000	
Advanced Door Monitoring	1	
Guard Tour	1	
Device Simulator	1	
Visitor Management	1	
Visitor Management Enhanced	1000	
Elpas Integration	1	
Building Management Integration	1	
Go Reader Configuration Mobile Application	1000	
Go Reader Service	1000	

C•CURE Go Reader device hardware requirements

The following hardware is required for C•CURE Go Reader:

- An Android mobile device with:
  - Android operating system 8.1 (Oreo) with API 25 or later.
  - Minimum storage of 8GB or 16 GB depending on your system size.
  - Minimum RAM of 2GB.
- A Serialio RS3 BLE reader with BLE and SPP support, rf IDEAS WaveID USB-C Nano reader, or MagTek iDynamo 6 USB-C reader if using an Android device.

Note: Software House is not responsible for any instability of the Go Reader connection due to customer’s unstable wireless network or of the Android tablet devices. Consult with your network administrator or the Android tablet provider in this type of connection issue.

MagTek iDynamo 6 card reader

The C•CURE Go Reader app uses a iDynamo 6 USB-C card reader to read magnetic stripe cards and to determine the number of absent personnel in an area during an emergency.

Wave ID Nano USB-C card reader

The C•CURE Go Reader app uses a Wave ID Nano USB-C card reader to read card swipes and to determine the number of absent personnel in an area during an emergency.

Serialio idChamp RS3 card reader

The C•CURE Go Reader app uses a Serialio RS3 BLE card reader with bluetooth connectivity to read card swipes and to determine the number of absent personnel in an area during an emergency.

C•CURE Go Reader tested on Android devices

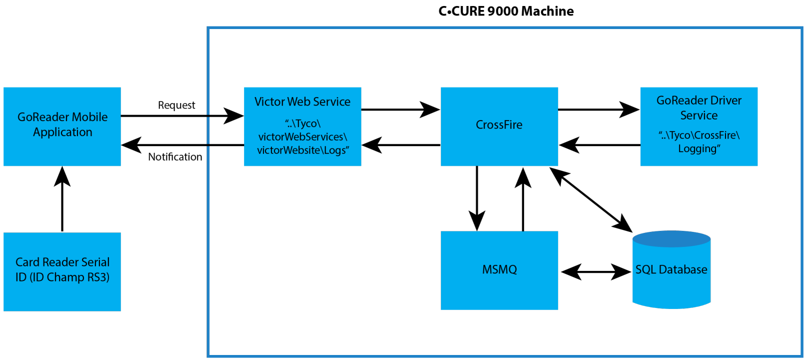
C•CURE Go Reader has been tested on the following mobile phones with Android v8.0, v10, v12, v13, v14, and v15:

- Google Pixel 6
- Google Pixel 7
- Google Pixel 7 Pro
- Samsung Galaxy S21
- Google Pixel 9
- Google Pixel 9 Pro

For more information on testing C•CURE Go Reader on Access-ER and C-One² devices, see C•CURE Go Reader tested on Access-ER and C-One² devices.

ⓘ **Note:** The C•CURE Go Reader application does not support landscape orientation mode.

Figure 4: Go Reader components for Android


C•CURE 9000 Machine
GoReader Mobile Application
Request
Notification
Victor Web Service
“..\Tyco\ victorWebServices\ victorWebsite\Logs”
CrossFire
GoReader Driver Service
“..\Tyco\CrossFire\ Logging”
Card Reader Serial ID (ID Champ RS3)
MSMQ
SQL Database

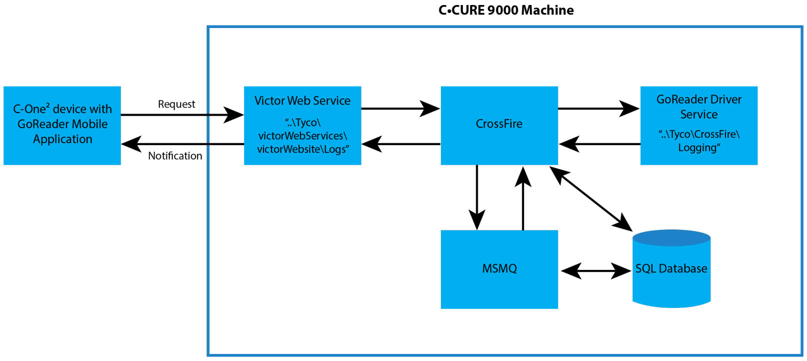
C•CURE Go Reader tested on Access-ER and C-One² devices

C•CURE Go Reader has been tested on the following with Android v8.0, v8.1, and v10.0:

- Access-ER device with HID read head.
- C-One² device with HID read head and ASK read head.

ⓘ **Note:** The C•CURE Go Reader application does not support landscape orientation mode.

Figure 5: Go Reader components for Access-ER and C-One²


C•CURE 9000 Machine
C-One² device with GoReader Mobile Application
Request
Notification
Victor Web Service
“..\Tyco\ victorWebServices\ victorWebsite\Logs”
CrossFire
GoReader Driver Service
“..\Tyco\CrossFire\ Logging”
MSMQ
SQL Database

Installation

This chapter contains instructions for installing C•CURE Go Reader driver, downloading and installing the C•CURE Go Reader app to your Android device, and connecting your device to the C•CURE 9000 server.

C•CURE Go Reader setup checklist

To install the Go Reader driver and application, you must complete the following procedures.

Setting up the Go Reader app and reader

If you are using the Access-ER device, complete the following:

- Connect CopperApps to the Johnson Controls repository. See Setting up CopperApps on Access-ER.
- Ensure the Barcode Manager and Core Services are installed and running the most recent version. See Installing and updating barcode manager on Access-ER and Installing and updating Core Services on Access-ER.
- Download and configure the Go Reader app. See Downloading the Go Reader app on Access-ER devices and Configuring the Go Reader app on Access-ER devices for more information.

If you are using the C-ONE² device, complete the following:

- Download and install the C•CURE Go Reader app from the Google Play Store. See Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices for more information.

  ⓘ **Note:** Check the compatibility matrix in the Go Reader release notes to ensure you are downloading the correct version of Go Reader before proceeding with installation.

- In the Go Reader app, tap **Settings** > **Advanced** > **ENABLE** to activate diagnostic information. Logs are saved in mobile device storage, `GoReader-Logs/Date.log`.

If you are using an Android device with a Serialio reader, complete the following:

- Download and install the C•CURE Go Reader app from the Google Play Store. See Downloading the C•CURE Go Reader .apk file from Google Play Store for more information.
- Configure Serialio device so it can communicate with the C•CURE Go Reader. See Serialio idChamp RS3 configuration sequence.

If you are using an Android device with a rfIdeas reader, complete the following:

- Download and install the C•CURE Go Reader app from the Google Play Store. See Downloading the C•CURE Go Reader .apk file from Google Play Store for more information.
- Configure rfIdeas device so it can communicate with the C•CURE Go Reader. See WAVE ID Nano configuration sequence.

If you are using an Android device with a MagTek reader, complete the following:

- Download and install the C•CURE Go Reader app from the Google Play Store. See Downloading the C•CURE Go Reader .apk file from Google Play Store for more information.
- Configure the C•CURE Go Reader app on the MagTek device. See MagTek iDynamo 6 configuration sequence for more information.

Setting up the C•CURE 9000 target system

- Ensure that the .NET Framework 3.5 is installed on C•CURE server.
- Ensure victor Web Service is installed on the C•CURE 9000 target system. See Pre-requisites for installing the C•CURE Go Reader driver and Troubleshooting.
- Log on with the C•CURE Go Reader app. See Launching the C•CURE Go Reader app.

- Type the IP address of the system where victor Web Service is hosted. Ensure that the operator is shown in the **Currently Active Connections** list. If the operator is not shown, check the victor Web Service log file `..\Tyco\victorWebServices\victorWebSite\Logs`.
- Activate MSMQ features:
  a. Navigate to **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off**.
  b. Select the **Microsoft Message Queue (MSMQ) Server** check box.
  c. Click **OK**.
- Ensure that Go Reader Driver service is listed in the Server Configuration Application. See Troubleshooting for more information.
- In SQL Server Management Studio, navigate to the **Tables** folder in the **ACVSCore** database. Ensure that the following Go Reader specific database tables are listed:
  - dbo.BarcodeDataFields
  - dbo.GoDevice
  - dbo.GoReader
  - dbo.GoReaderAreaLink
  - dbo.GoReaderCardFormatLink
  - dbo.GoReaderCheckPoint
  - dbo.GoReaderDesfireSettings
  - dbo.GoReaderDoorAssociation
  - dbo.GoReaderFacilityCodeLink
  - dbo.GoReaderMagTekSettings
  - dbo.GoReaderMiFareSettings
  - dbo.GoReaderReaderObject
  - dbo.NotificationMessages
  - ⓘ **Note:** victor Web Service and GoReader driver service interact through the Go Reader Crossfire component (TSP.GoReader.ServiceRequest.dll).
- Activate Go Reader diagnostic switch as shown in Activating Go Reader diagnostic switch. The log file can be found in `...Tyco\CrossFire\Logging`.
- Ensure that a valid license is applied to Crossfire Services.
- Ensure that the user has permission to connect to the database.

Activating Go Reader diagnostic switch

Activate the Go Reader diagnostic switch to capture Go Reader logs. Ensure you complete these steps under the supervision of technical support.

1. In the Server Configuration application, click the **Diagnostics** tab.

   ⓘ **Note:** If there is no **Diagnostics** tab, click the top right corner of the Server Configuration Application five times. The **Diagnostics** tab appears.

2. Click **Connect**.
3. In the **Switches Filter** field, type `GoReader Driver`.
4. Click the **GoReader Driver** switch four times, until it becomes green in color. You can now see logs.
5. When you have completed troubleshooting, click the **GoReader Driver** switch two times, until it becomes red in color again.
6. Click **Disconnect**.

C•CURE Go Reader integration installation checklist

ⓘ **Note:** Before you complete these steps, you must install the Go Reader driver on the C•CURE 9000 server and C•CURE client machines. For more information, see Installing the C•CURE Go Reader driver.

Before you install or upgrade the Go Reader driver, complete these steps:

1. Ensure the user has Administrator rights on the C•CURE 9000 target system.
2. When User Account Control appears, click **Yes** for the Go Reader driver installation to make changes to the C•CURE 9000 target system.

Reporting installation failure

You can view installation logs to share when reporting installation failure. Complete these steps to prepare for reporting installation failure:

ⓘ **Note:** For Android devices, complete the following procedure. For C-One² devices, complete the procedure in Reporting installation failure for C-One² devices.

1. Install the Go Reader Integration driver.
2. Click on the **View** tab of the File Explorer of the C: drive.
3. Select the **Hidden item** check box. The Program Data folder is partially visible.
4. Double-click the **Program Data** folder.
5. Navigate to `C:\ProgramData\Tyco\InstallerTemp`.
6. Locate the `C-CURE GO_Reader_YYYYMMDDTimeStamp` compressed zipped folder.
7. Capture a screenshot of the error message that displays on the Go Reader Installation wizard, if any.
8. From the Start menu, search for the **Event Viewer** program. Open **Event Viewer**.
9. Navigate to `Event Viewer(Local)/Windows Logs/Application`. Any errors from the installation process appear in the **Application** list.

Reporting installation failure for C-One² devices

You can view installation logs to share when reporting installation failure. Complete these steps to prepare for reporting installation failure:

1. From the **Start** menu, search for the **Run** program. Click **Run**.
2. In the **Open** field, type `%temp%` . Click **OK**.

   The installation logs are located in the zip file named `C-CURE GoReader_YYYYMMDD`, where `YYYYMMDD` is the date and time the log is created.
3. Capture a screenshot of the error message that displays on the Go Reader Installation wizard, if any.
4. From the **Start** menu, search for the **Event Viewer** program. Open **Event Viewer**.
5. Navigate to `Event Viewer(Local)/Windows Logs/Application`. Any errors from the installation process appear in the **Application** list.

C•CURE Go Reader installation and configuration sequence

Table 3 explains the installation and configuration sequence for the C•CURE Go Reader.

Table 3: C•CURE GoReader installation and configuration sequence

Step	Task	See
1.	Install the C•CURE 9000 driver on your C•CURE 9000 target system.	Installing the C•CURE Go Reader driver
2.	Download and install the C•CURE GoReader app to your Android device.	Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices
3.	**Optional:** Configure the Serialio idChamp RS3 card reader to process card swipes and to communicate with the Android device. Follow the instructions in the Serialio idChamp RS3 configuration sequence.	Serialio idChamp RS3 configuration sequence
4.	**Optional:** Configure the Wave ID Nano USB-C card reader to process card swipes and to communicate with the Android device. Follow the instructions in the Wave ID Nano USB-C configuration sequence.	WAVE ID Nano configuration sequence
5.	**Optional:** Configure the MagTek iDynamo 6 USB-C card reader to process card swipes and to communicate with the Android device. Follow the instructions in the MagTek iDynamo 6 USB-C configuration sequence.	MagTek iDynamo 6 configuration sequence
6.	Connect your Android device to the C•CURE 9000 server.	Creating connections
7.	Launch the C•CURE Go Reader app on the Android device.	Launching the C•CURE Go Reader app
8.	Activate the C•CURE Go Reader on the C•CURE 9000 Administration Station.	Activating the Go Reader
9.	Use the Go Device editor in the C•CURE 9000 Administration Station to: • Name and describe the Android device the C•CURE Go Reader app is installed on. • View general and status information about the device.	C•CURE Go device editor
10.	Use the Go Reader editor in the C•CURE 9000 Administration Station to configure C•CURE Go Reader settings and modes.	Go Reader editor tasks

Installing the C•CURE Go Reader driver

This section provides pre-requisites and instructions to install the C•CURE Go Reader Driver on the C•CURE 9000.

Pre-requisites for installing the C•CURE Go Reader driver

Ensure the following pre-requisites before installing the C•CURE Go Reader driver:

- C•CURE 9000 v2.90 or higher is installed on a 64-bit operating system.
- victor Web Service is installed and licensed on the target system. Use the C•CURE 9000 Unified Installer Dashboard to install victor Web Service. For more information, refer to the *C•CURE 9000 Installation and Upgrade Guide*.
- victor Web Service version is the same as the Crossfire version.
- Ports 443 or 80 must be open and available. Port 443 is used for secure log on and port 80 is used for non-secure log on.

ⓘ **Note:** To activate Windows Firewall and add ports for Windows 8.1, Windows 2008 R2, or Windows Server 2012 R2 operating systems, refer to the Microsoft Help and Support Webpages. You must be logged on as an administrator to perform the necessary procedures.

ⓘ **Note:** Go Reader activities do not display on a remote client Monitoring Station if the Go Reader driver is not installed on a remote client. Install the Go Reader driver on the remote client system to show all Go Reader activities on a remote client.

Downloading the C•CURE Go Reader driver

You can download the C•CURE Go Reader driver from the Software House website, http://www.swhouse.com/. You must logon to the Software House website to download the C•CURE Go Reader driver. If you do not have an account, you must create one.

1. Navigate to http://www.swhouse.com/.
2. Select **Software Downloads**, then select **Connected Partner Program**.
3. From the list, select **C•CURE GoReader**.
4. Select the C•CURE Go Reader driver version from the right side of the page.
5. Unzip the files to a folder on your local machine, or on a shared network drive.

Installing the C•CURE Go Reader driver on a remote client

Complete the following steps to install the C•CURE Go Reader driver on a remote client.

1. Open the Go Reader Integration installer.
2. On the **Welcome to C-CURE 9000 GoReader Setup Wizard**, click **Next**.
3. Select **I accept the terms in the License Agreement** in the EULA, then click **Install**.
4. Click **Finish**.

   ⓘ **Note:** By default, the option **Open Log file after pressing Finish** is not selected in the Go Reader Setup screen. Click to open the log file after clicking **Finish**.

   ⓘ **Note:** There is no **Start Crossfire Service after pressing Finish** if you install Go Reader on a remote client.

Installing the C•CURE Go Reader driver on a C•CURE server configured with local victor Web Service

If your target system is configured with local victor Web Service (vWS), complete the following steps to install the C•CURE Go Reader driver on a server.

1. Open the Go Reader Integration installer.
2. On the **Welcome to C-CURE 9000 GoReader Setup Wizard**, click **Next**
3. Select **I accept the terms in the License Agreement** in the EULA, then click **Next**.

   ⓘ **Note:** If the CrossFire Framework Service is not running, the installation aborts with this message `Installation aborted: To restart the installation run the CrossFire Service`. Click **Finish** and start the CrossFire services.

4. On the **Victor Web Service Details** screen, select **Yes**. See Figure 7.
5. Click **Next**. The message `CrossFire services will be stopped` appears. Click **OK**.
6. Click **Install** to confirm the **C•CURE GoReader Setup Summary**. After the installation process finishes, the message Product Installation completed successfully displays.

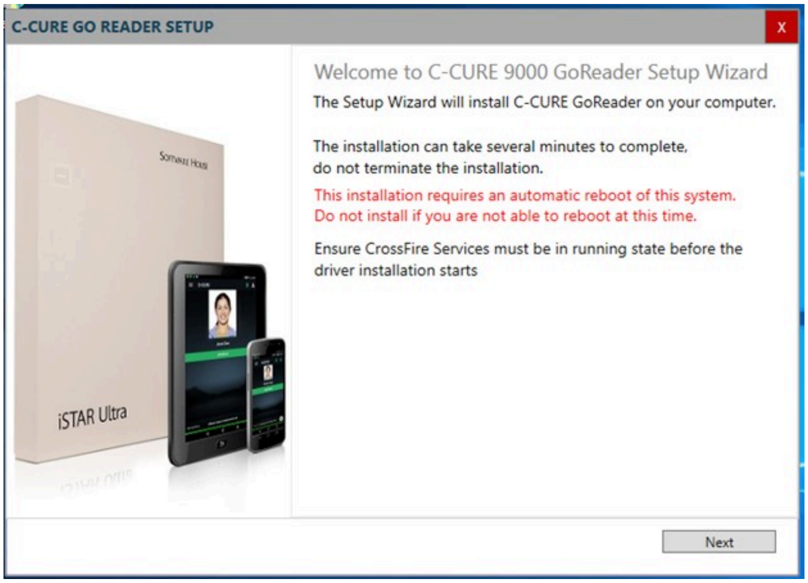
   ⓘ **Note:** If the **Microsoft Message Queue MSMQ Server** option is not enabled in **Windows Features**, the message `GoReader setup will continue after an automatic reboot` displays. Click **OK** to restart the system. The installation process resumes automatically after the system restart.

7. Click **Finish**.

   ⓘ **Note:** By default, the option **Start Crossfire Service after pressing Finish** is selected and the option**Open Log file after pressing Finish** is not selected in the Go Reader Setup screen.

   ⓘ **Note:** The **Microsoft Message Queue (MSMQ) Server** option is enabled in **Windows Features** after installing the Go Reader driver .

Figure 6: Go Reader installation wizard



C-CURE GO READER SETUP

Welcome to C-CURE 9000 GoReader Setup Wizard

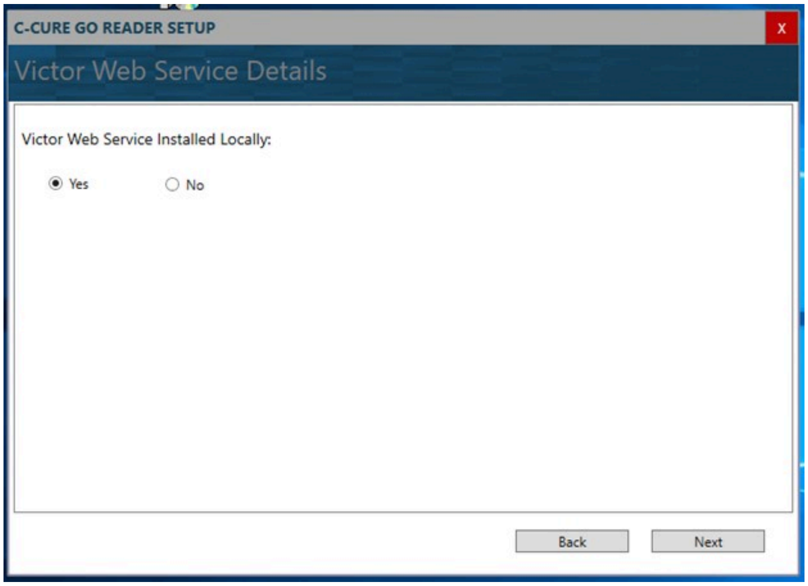
The Setup Wizard will install C-CURE GoReader on your computer.

The installation can take several minutes to complete, do not terminate the installation.

This installation requires an automatic reboot of this system. Do not install if you are not able to reboot at this time.

Ensure CrossFire Services must be in running state before the driver installation starts

Figure 7: Victor Web Service details



C-CURE GO READER SETUP

Victor Web Service Details

Victor Web Service Installed Locally:

● Yes ○ No

Installing the C•CURE Go Reader driver on a C•CURE server with remote victor Web Service

If your target system is configured with remote victor Web Service (vWS), complete the following steps to install the C•CURE Go Reader driver on a server.

1. Complete steps 1-2 of Installing the C•CURE Go Reader driver on a remote client.
2. Select **I accept the terms in the License Agreement** in the EULA, then click **Next**.

3. On the **Victor Web Service Details** screen, select **No**.
4. In the **Enter Server Details** field, enter the IP address and name of the machine with victor Web Service. See Figure 8. Click **Validate**.

   Note:
   - If the CrossFire Framework Service is not running, the installation aborts with this message `Installation aborted: To restart the installation run the CrossFire Service`. Click **Finish** and start the CrossFire services.
   - If you enter an incorrect IP address and click **Validate**, the message `Instance of victor web service is not found` displays.
   - The Go Reader installer waits for 100 seconds to get the validation of vWS response back from the vWS system.

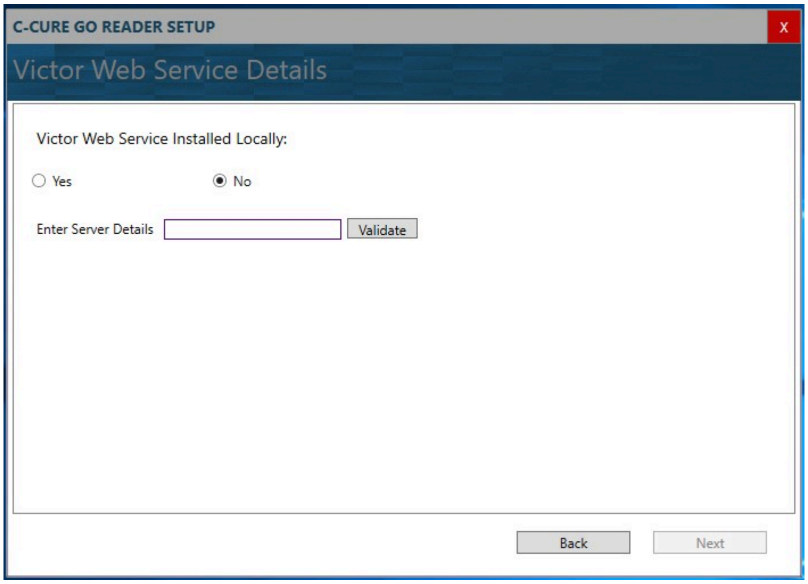
5. The message `Victor Web Service instance validated successfully, click Next to continue` displays. Click **Next** to resume installation.
6. The message `CrossFire Services will be stopped` appears. Click **OK**.
7. Click **Install** to confirm the **C•CURE GoReader Setup Summary**. After the installation process finishes, the message `Product Installation completed successfully` displays.

   Note: If the **Microsoft Message Queue MSMQ Server** option is not enabled in **Windows Features**, the message `Go Reader setup continues after an automatic reboot` displays. Click **OK** to restart the system. The installation process resumes automatically after the system restarts.

8. Click **Finish**.

   Note:
   - By default, the option **Start Crossfire Service after pressing Finish** is selected and the option **Open Log file after pressing Finish** is not selected in the Go Reader Setup screen.
   - The **Microsoft Message Queue (MSMQ) Server** option is activated in **Windows Features** after installing the Go Reader driver .

Figure 8: Victor Web Service details with server



C-CURE GO READER SETUP

Victor Web Service Details

Victor Web Service Installed Locally:

○ Yes ● No

Enter Server Details

After installing the C•CURE Go Reader Driver Service, you must activate it in the **Server Configuration application**.

Upgrading the C•CURE Go Reader driver

1. Open the Go Reader Integration installer.
2. On the **Welcome to CCURE 9000 Go Reader Setup Wizard**, click **Next**.
3. Click **Upgrade** to confirm the **C•CURE Go Reader Setup Summary**.
4. After the upgrade completes, click **Finish**.

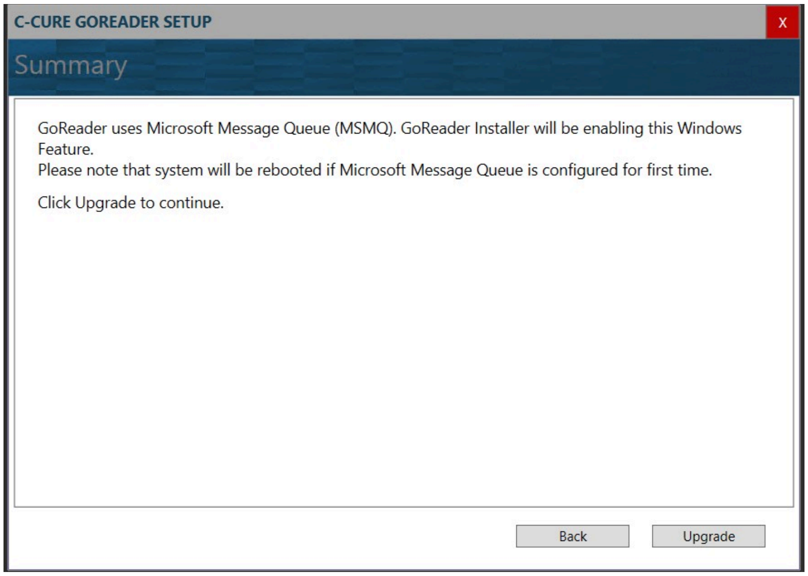
Note:

Before upgrading the Go Reader driver from any C•CURE 2.90-compatible version to C•CURE 3.10, it is strongly recommended to first uninstall the existing driver. Follow these steps to complete the process:

a. Uninstall the existing Go Reader driver without dropping the database to preserve existing data.
b. Upgrade C•CURE to version 3.10.
c. Install the new Go Reader driver that is compatible with C•CURE 3.10.

Following this sequence ensures compatibility and helps prevent service initialization issues, including those related to the CrossFire framework service.

Figure 9: Upgrade screen



GoReader uses Microsoft Message Queue (MSMQ). GoReader Installer will be enabling this Windows Feature.
Please note that system will be rebooted if Microsoft Message Queue is configured for first time.

Click Upgrade to continue.

Repairing the C•CURE Go Reader driver

To repair the C•CURE Go Reader driver, complete the following steps:

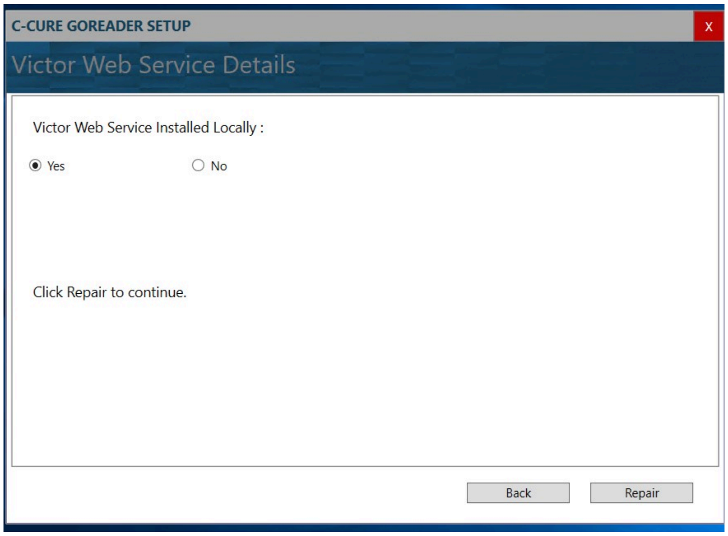
1. From the Windows Start menu, select **Control Panel** > **Programs** > **Programs and Features**.
2. From the list of programs, right-click on **C•CURE Go Reader** .
3. From the list of available actions, select **Change**.
4. In the **Welcome to C•CURE 9000 Reader Setup Wizard** screen, click **Next**.
5. Choose the most appropriate next step:
   - If your target system has locally installed vWS, on the **Victor Web Service Details** screen, select **Yes**, and then click **Repair**. See Figure 10.
   - If your target system does not have vWS installed locally, on the **Victor Web Service Details** screen, select **No**. In the **Enter Server Details field**, enter the IP address and name of the machine with victor Web Service. Click **Validate**. See Figure 11.

ⓘ **Note:**

- If you enter an incorrect IP address and click **Validate**, the message `Instance of victor web service is not found` displays.
- The GoReader installer waits for 100 seconds to get the validation of vWS response back from the vWS system.

6. Click **Repair** to confirm the **C•CURE Go Reader Setup Summary**. After the update finishes, the message `Product Installation completed successfully` displays.
7. Click **Restart** to restart your computer to complete the update.

Figure 10: victor Web Service details for update

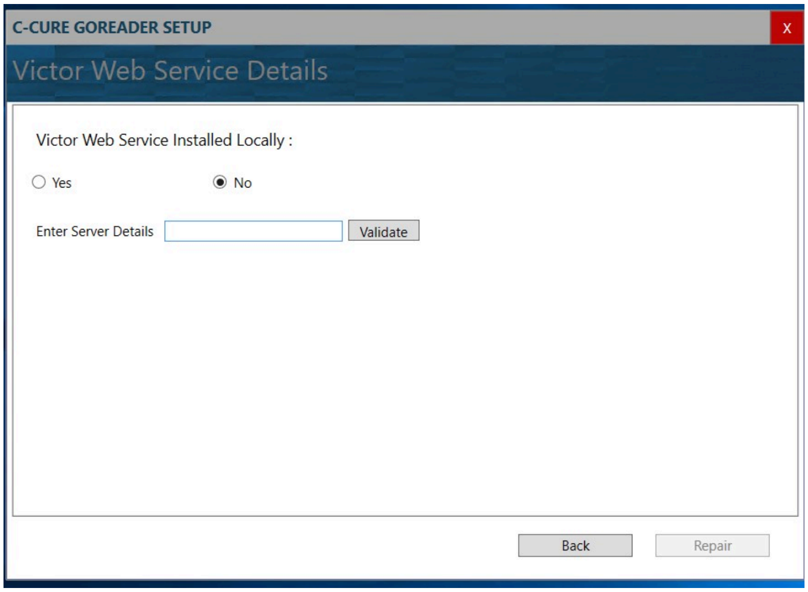


Victor Web Service Installed Locally :

● Yes ○ No

Click Repair to continue.

Figure 11: victor Web Service details for update with server



Victor Web Service Installed Locally :

○ Yes ● No

Enter Server Details

Uninstalling the C•CURE Go Reader driver

You can uninstall the C•CURE Go Reader from the **Programs and Features** module in Windows. This opens the C•CURE 9000 C•CURE Go Reader Setup Wizard.

1. From the Windows Start menu, select **Control Panel** > **Programs and Features**.
2. From the list of programs, right-click on **C•CURE Go Reader**.
3. From the list of available actions, select **Uninstall**.
4. In the **Welcome to C•CURE 9000 Reader Setup Wizard** screen, click **Next**.
5. **Optional:** Select **Drop records from DB Server** if you want to delete database entries for C•CURE Go Reader, then click **Uninstall**. The message `CrossFire services will be stopped` appears. Click **OK**.
6. After the uninstalling completes, the message `Product Removal Completed successfully` displays. Click **Finish**.

   Note: By default, the option **Start Crossfire Service after pressing Finish** is selected and the option **Open Log file after pressing Finish** is not selected in the Go Reader Setup screen.

Uninstalling the Service Bus

Go Reader uses Microsoft Message Queuing instead of the Service Bus. To uninstall the Service Bus, complete the following steps.

1. In **All Programs**, search for **Service Bus Configuration**. Open **Service Bus Configuration**.
2. In the **Service Bus Configuration** wizard, click **Leave Farm**.
3. Click the tick to proceed with the Service Bus removal. The configuration progress barshows the progress of the Service Bus removal.
4. When the Service Bus removal is complete, the message `Remove current computer from Service Bus farm` displays with a green tick. Click the tick to exit the Service Bus Configuration Wizard.
5. In **All Programs**, search for **Services**. Open **Services**.

   Ensure that these four services are no longer on the list of services:

   - Service Bus Gateway
   - Service Bus Message Broker
   - Service Bus Resource Provider
   - Service Bus VSS
6. In **All Programs**, search for **SQL Server Management Studio**. Open **SQL Server Management Studio** and and click **Connect** to connect to the SQL database.

   In the **Object Explorer** pane, delete these three databases:

   - SbGatewayDatabase01
   - SBManagementDB01
   - SBMessageContainer01

   To delete the databases, right-click on the database name and click **Delete**. Select the **Close existing connections** check box and click **OK**. Repeat for each database.

C•CURE Go Reader driver configuration files

Use the C•CURE Go Reader driver configuration files to view C•CURE Go Reader driver system settings, and to make changes to default values that apply to the C•CURE Go Reader driver.

The following table lists the configuration files and their locations.

Table 4: C•CURE Go Reader driver configuration files

Configuration File	File Location
GoReaderServiceRequest.xml	`..\Tyco\CrossFire`
GoReaderConfiguration.xml	`..\Tyco\CrossFire\ServerComponents`

C•CURE Go Reader service request settings

The following table describes the configuration settings for **GoReaderServiceRequest.xml**.

Table 5: C•CURE Go Reader service request settings

Configuration Settings	Description	Value	Default
GoReaderDatabaseLocation	Specifies the location of personnel, images and configuration databases created for downloading to device. ⓘ **Note:** If you edit the Go Reader Database Location you must update the Database Folder setting in the **GoReaderConfiguration.xml** file. The database path must be located on the local system drive.	String	`C:\GoReaderDatabase\`
DiscoveryProxyService	Specifies the URL for accessing the C•CURE Go Reader discovery service.	String	`net.tcp://localhost:9012/DiscoveryProxyService`

C•CURE Go Reader configuration settings

The following table describes the configuration settings for **GoReaderConfiguration.xml.**

Table 6: C•CURE Go Reader configuration settings

Configuration Setting	Description	Value	Default
DataBaseFolder	Specifies the location of personnel, images and configuration databases created for downloading to device. ⓘ **Note:** If you edit the Database Folder setting, you must update the GoReaderDatabaseLocation setting in the **GoReaderServiceRequest.xml** file. The database path must be located on the local system drive.	String	`C:\GoReaderDatabase\`
PersonnelDBMax	Specifies the number of personnel stored in database files created for personnel records in the C•CURE 9000 system.	Numeric	2000
ImageDBMax	Specifies the number of images stored in database files created for images records in the C•CURE 9000 system.	Numeric	1000

Table 6: C•CURE Go Reader configuration settings

Configuration Setting	Description	Value	Default
ConfigurationDBMax	Specifies the number of C•CURE 9000 configurations for schedules, holidays and holiday groups stored in each database file synchronized with the C•CURE Go Reader device.	Numeric	2000
DeletedRecordsDBMax	Specifies the number of deleted personnel stored in each database file synchronized with the C•CURE Go Reader device.	Numeric	5000

Use Go Reader in an enterprise environment

You can use Go Reader in an Enterprise environment.

- In an Enterprise environment, Go Reader objects are located on the Satellite Application Server (SAS) and cannot be correctly attached to a Master Application Server (MAS).
- Install the Go Reader drive client components on a remote MAS client pointing to a MAS server system, or a remote SAS client pointing to a SAS server system.
- In an Enterprise environment, you can facilitate global or personnel with Go Reader.
- The Enterprise environment supports all clearances, global and local, except for All Doors global clearance.

Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices

You can download the C•CURE Go Reader driver from the Software House website and the `.apk` files from the Google Play Store app. This is applicable to C-ONE² and Android devices.

Downloading the C•CURE Go Reader .apk file from Google Play Store

This is required for C-ONE² and Android devices. To download the C•CURE Go Reader app on an Access-ER device, see Configuring the Go Reader app on Access-ER devices.

ⓘ **Note:** The C•CURE Go Reader app supports Android devices running Android v8.1 and later.

1. Set up an account on Google to access Google apps.
2. From your Android device, open the Google Play Store.
3. Search for `Tyco` to find the Tyco specific apps that are available.
4. Tap **C•CURE Go Reader**, then tap **Install**.

The app downloads and installs to your device.

Downloading and installing the Go Reader integration driver from the Software House website

To download the C•CURE Go Reader app driver from the Software House website you must have:

- Log on credentials for the Software House website.
- A USB cable.
- A file manager application on your C-One² device. If you do not have this application on your device, you can download a third party application to access your file manager.

1. Navigate to http://www.swhouse.com.

2. Click **Products**.
3. Click **Software Downloads** > **Connected Partner Program** > **C•CURE Go Reader**.
4. Download the C•CURE Go Reader driver to your local drive.
5. Connect your Android device to your PC using a USB cable.
6. Copy the C•CURE Go Reader driver to a folder in the device.
7. Open the file manager application on your device.
8. Find the location of the C•CURE Go Reader app driver.
9. Tap the C•CURE Go Reader driver and select **Install**. The device installs the C•CURE Go Reader app.

Upgrading the Go Reader application

To upgrade the Go Reader application complete the following steps:

1. From your Android device, open Google Play Store.
2. Search for `Tyco` to find the Tyco specific apps that are available.
3. Tap **C•CURE Go Reader**.
4. Tap **Update**.

The latest version of the app downloads and installs to your device.

Configuring the Go Reader application after upgrade without using secure connection

This version of the Go Reader application does not support self-signed certificates for secure connection. If you upgrade from an older version of Go Reader, you need to complete one of these procedures.

If you previously connected the Go Reader application to the C•CURE server without using **Secure Connection**, complete the following steps:

1. On the **Home** screen, tap **Settings**.
2. On the **General** tab, tap **SELECT READER**.
3. Tap the name of a reader to associate with the Go Reader application.

Configuring the Go Reader application after upgrade with secure connection

If you previously connected the Go Reader application to the C•CURE server using **Secure Connection**, complete these steps:

1. Tap **LOGIN** and enter your credentials.
2. Restart the Go Reader application on your device.
3. On the **Home** screen, tap **Settings**.
4. On the **General** tab, tap **SELECT READER**.
5. Tap the name of a reader to associate with the Go Reader application.

   ⓘ **Note:** The previously associated reader is deactivated automatically from the server, but the object is still visible in C•CURE. Manually delete the previous reader and activate the new reader so that a complete synchronization can be performed.

Downloading and installing the Go Reader driver services app on C-ONE^2 device

In order to use barcode scanning with **Barcode scan or Low or High Frequency HID Card** on a C-ONE^2 device, you also need to install the Go Reader driver services app.

1. In the Google Play Store, download the Go Reader C-ONE^2 Driver Services app.
2. Open the Go Reader C-ONE^2 Driver Services app.
3. To accept the app permissions, read the permissions and tap **ALLOW**.
4. To access media and files on your device, tap **ALLOW**.

5. To connect to barcode reader peripherals, tap **ALLOW**.
6. When a confirmation message appears, tap **OK**.
7. To start the Go Reader C-ONE^2 driver service, navigate to the **HOME** tab.

When the service completes, on the **HOME** tab, in **Driver Health Information**, the following information appears:

- **Go Reader App Version**
- **Go Reader C-ONE^2 Driver Version**
- **CPC Core Service**
- **Barcode Manager Service**

Barcode feature testing prerequisites for C-One^2 devices

In order to be able to perform barcode scanning, the user needs to remap the `BARCODE_SCAN` key. For more information, see Remapping the BARCODE_SCAN key for C-One^2 devices.

Remapping the BARCODE_SCAN key for C-One^2 devices

To remap the `BARCODE_SCAN` key to perform barcode scans, complete the following procedure:

1. On your C-One^2 device, navigate to **Settings**.
2. Tap **Remap Key and Shortcut**.
3. Tap **P1-Unspecified**.
4. On the pop-up window, select the **Remap key** radio button.
5. Navigate to the key selection screen, and select **BARCODE_SCAN** key.

Install and configure apps on Access-ER device

You can download, update, and uninstall apps from the CopperApp store on the Access-ER device. You must install and configure Barcode Manager and Core Services before configuring the Go Reader app.

Setting up CopperApps on Access-ER

Access-ER is an Android Open-Source Project (AOSP) device and you use the CopperApps application to install, uninstall, and update applications on your device. CopperApps is pre-installed on your Access-ER device. You must connect your Access-ER device to the Johnson Controls app repository in the CopperApps application before attempting to download apps.

Figure 12: CopperApps icon

1. On the home screen, tap the **CopperApps** icon.
2. In the CopperApps application, tap **Settings**.
3. In the **Settings** menu, tap **Repositories** > **Add**.
4. In the **Repositories address** field, type `http://fdroid.coppernic.fr/customers/tyco/2ba8adc/fdroid/repo/`.
5. Tap **Add**.

The Coppernic repository for Johnson Controls, titled **Coppernic repo for JCI**, has been added to CopperApps on your Access-ER device.

The C•CURE Go Reader and C•CURE Go Reader Driver Services apps are available for download from CopperApps. For more information, see Downloading the Go Reader app on Access-ER devices and Downloading the C•CURE Go Reader Driver Service app on Access-ER devices.

Downloading the C•CURE Go Reader Driver Service app on Access-ER devices

You must connect CopperApps to the Johnson Controls app repository before downloading apps. See Setting up CopperApps on Access-ER.

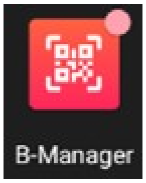
1. On the home screen, tap the **CopperApps** icon.
2. In the search bar, type `GoReader`.
3. From the search results, tap **Go Reader Coppernic Driver Service App** .
4. Tap **Install**.

The C•CURE Go Reader Driver Service app is installed on your Access-ER device. For more information, see Setting up Go Reader Driver Service App for Access-ER devices.

Installing and updating barcode manager on Access-ER

1. On the home screen, tap **CopperApps**.
2. Tap on the search bar and type `Barcode Manager`.
3. Choose the most appropriate next step:
   - If Barcode Manager is not installed, tap **Install**.
   - If Barcode Manager is running an old version, tap **Update**.
4. When Barcode Manager has been installed or updated, return to the home screen.
5. Navigate to the **B-Manager app** icon and tap to open the application. See Figure 13.

Figure 13: Barcode manager icon



6. Choose between:
   - If the barcode service is active, return to the **HOME** screen.
   - If the barcode service is not active, tap **START BARCODE SERVICE**.

Installing and updating Core Services on Access-ER

Core Services handle power management and key remapping. You must ensure that the most recent version of Core Services is installed on your device.

To install or update Core Services:

1. On the home screen, tap **CopperApps**.
2. Tap on the search bar and type `Core Services`.
3. Choose the most appropriate next step:
   - If Core Services are not installed, tap **Install**.
   - If Core Services is running an old version, tap **Update**.
   - If Core Services is running the current version, return to the main menu.

Downloading the Go Reader app on Access-ER devices

You must connect CopperApps to the Johnson Controls app repository before downloading apps. See Setting up CopperApps on Access-ER.

1. On the home screen, tap **CopperApps**.
2. Tap the search bar and type `Go Reader`.
3. Tap the **Go Reader** icon and then tap **Install**.

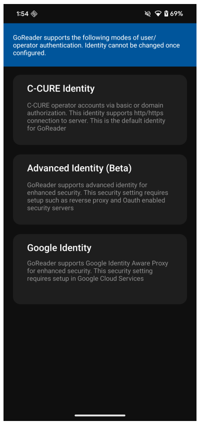
To configure the Go Reader app on your Access-ER device, see Configuring the Go Reader app on Access-ER devices.

Configuring the Go Reader app on Access-ER devices

1. On the home screen, tap on the **Go Reader app** icon.
2. Tap **YES** to activate Go Reader app notifications.
3. On the welcome screen, tap **PROCEED**.
4. Read the Privacy Notice, then tap **ACCEPT**.
5. On the Go Reader identity screen, choose **C-CURE Identity**.

   For more information on the **Advanced Identity (Beta)** option, see Go Reader Identity: Advanced identity (beta) mode.

Figure 14: Go Reader Identity screen



GoReader supports the following modes of user/operator authentication. Identity cannot be changed once configured.

C-CURE Identity

C-CURE operator accounts via basic or domain authorization. This identity supports http/https connection to server. This is the default identity for GoReader

Advanced Identity (Beta)

GoReader supports advanced identity for enhanced security. This security setting requires setup such as reverse proxy and Oauth enabled security servers

Google Identity

GoReader supports Google Identity Aware Proxy for enhanced security. This security setting requires setup in Google Cloud Services

6. In the **Operator Name** field, enter your operator name.
7. In the **Operator Password** field, enter your password.
8. In the **Server Address** field, enter the IP server address.
9. **Optional:** If you logon to the app across an unsecured network, select the **Use Secure Connection** check box. Otherwise, ensure that the check box is cleared.
10. Tap **LOGIN**.
11. On the **Associate Card Reader** screen, select **Access ER** and then tap **YES**.
12. You must activate the reader in the C•CURE 9000 Administration Workstation, see Activating the Go Reader.
13. On the Go Reader app home screen, click on the **USER** icon.
14. Type your **C-CURE Identity** to log on to the Settings menu.

The C•CURE Go Reader app is now configured on your Access-ER device.

Activating hardware feedback on Access-ER

You can activate and disable the hardware feedback option from the settings menu of the Access-ER device. If you activate hardware feedback, data related to hardware performance is collected and processed by Qualcomm Technologies.

1. On the home screen, click **Settings**.
2. In the **Settings** menu, scroll to **Hardware Feedback**.
3. Choose between:
   - Select the check box to activate hardware feedback.
   - Clear the check box to disable hardware feedback.

Setting Access-ER devices to sync with the Network Time Protocol (NTP) server

Access-ER devices do not automatically sync with the Network Time Protocol (NTP) server. You must set your Access-ER device to manually sync with the Network Time Protocol (NTP) server.

ⓘ **Note:** If your Access-ER device is offline and the battery discharges fully, the device reverts to the default time zone. You must run the custom Network Time Protocol (NTP) command again.

1. Activate **Developer Options** mode on your Access-ER device.
   a. On the home screen, tap to open the **Settings** application.
   b. Navigate to **About phone** > **Build number**.
   c. Tap the **Build number** field 7 times.
2. You must activate USB debugging mode on your Access-ER device.
   a. In the **Settings** application, navigate to **System**.
   b. Tap **Advanced** > **Developer Options**.
   c. Turn on the **USB debugging** toggle switch.
3. Download and install Android SDK Platform Tools from Android Studio on a computer.
4. Use a USB-C cable to connect your Access-ER device to the computer that you installed Android SDK Platform Tools on.
5. In the **Windows Search** box, type `cmd`, right-click **Command Prompt** and from the context menu, select **Run as administrator**.
6. In the **Command Prompt** window, run the following prompts:
   a. To view a list of the devices, type `adb devices`.
   b. To set the custom Network Time Protocol (NTP) command, type `adb shell settings put global ntp_server <<NTP Server IP/NAME>>`.
   c. To restart your Access-ER device, type `abd reboot`.
   d. When the device restarts, to confirm that the device is using the custom Network Time Protocol (NTP) command, type `adb shell settings get global ntp_server`.
7. **Optional:** If the `adb devices` command does not display a list of devices or returns the message `adb is not recognized as an internal or external`, complete the following steps:
   a. Copy the `platform-tools` folder that you download in Step 3.
   b. Paste the `platform-tools` folder to the following folder: `C:\Users\<user name>\AppData\Local\Android\Sdk\`
   c. In **File Explorer**, navigate to **This PC**.
   d. Right-click **This PC**, and from the context menu, select **Properties**.
   e. In the **Settings** windows, in the **Related settings** list, click **Advanced system settings**.
   f. In the **System Properties** window, on the **Advanced** tab, click **Environment Variables...**.
   g. In the **Environment Variables** window, in the **System variables** pane, from the list, select **Path**, then click **Edit**.

   h. In the **Edit environment variable** window, click **New**.
   i. In the open field, enter `C:\Users\<user name>\AppData\Local\Android\Sdk\platform-tools`.
   j. Click **OK**.
   k. In the **Environment Variables** window, click**OK**.
8. **Optional**: Repeat steps 1 -5 on your other Access-ER devices.

Creating connections

You must create a connection from the Android device to the C•CURE 9000 server to access the C•CURE Go Reader app. The connection can be made through VPN or Wi-Fi. To access the server through a public Internet connection, install a third party application to establish a VPN connection to your server.

Requirements for creating a VPN connection

Ensure that you have completed the following pre-requisites:

- Internet Information Services (IIS) is installed on the C•CURE 9000 target system.
- victor Web Service is installed on the C•CURE 9000 target system.
- A third-party application installed on your Android device that can establish a VPN connection with your server.

Creating a VPN connection

1. Download and install a third-party application that accesses the VPN.
2. Verify that the third-party application has installed correctly and you have established access to the VPN.
3. Log on to the C•CURE Go Reader app with your operator credentials. For more information about how to log on, see Launching the C•CURE Go Reader app.

   ⓘ **Note:** The operator must have System All Privilege.

Creating a VPN connection with a portable Wi-Fi hotspot

You can use a separate mobile device as a portable Wi-Fi hotspot to create a VPN connection.

1. Activate the portable Wi-Fi hotspot feature on the separate mobile device.
2. Connect the Android device with the C•CURE Go Reader app to the Wi-Fi hotspot.
3. Use the third-party application installed on the device with the C•CURE Go Reader app to connect to the VPN.
4. Logon to the C•CURE Go Reader app with your operator credentials. For more information about how to logon, see Launching the C•CURE Go Reader app.

   ⓘ **Note:** The operator must have System All Privilege.

Using cellular network on Access-ER

If you want to use your Access-ER device outside of a Wi-Fi network, you can connect to the Internet using a cellular network.

1. Insert a SIM card into the SIM card slot of your Access-ER device.
2. Navigate to **Settings** > **Network & internet** > **Mobile Network** > **Advanced** .
3. Use the toggle switch to activate **Automatically Select Network**.
4. Tap **Preferred Network Type** and choose between:
   - 4G/3G/2G
   - 3G/2G
5. Use the toggle switch to activate **Mobile Data**.

Creating a Wi-Fi connection

You must create a Wi-Fi connection to the same Wi-Fi network as the C•CURE 9000 target system.

1. Tap **Settings** on your Android device's home page.
2. Select the Wi-Fi network you want to connect to.
3. Connect to the Wi-Fi network.
4. Log on to the C•CURE Go Reader app.

Configuration

This chapter provides instructions for configuring the the WAVE ID Nano card reader, Serialio idChamp RS3 card reader, C•CURE Go Reader editor and Go Device editor, configuring Operator privileges for using the C•CURE Go Reader, configuring C•CURE Go Reader clearances, manual actions, server-based check points, roll-call with previous doors, expiring clearance, iSTAR online reader mode enhancements, Go Reader online status notifications, and FASC-N support.

WAVE ID Nano configuration sequence

The WAVE ID Nano USB-C reader is a compact USB-C form reader that is inserted into the USB-C port on a mobile phone or tablet. You must configure the Wave ID Nano USB-C reader for it to communicate with the Android device. The Wave ID Nano USB-C reader can be configured using the rf IDEAS Configuration Utility tool.

Table 7: WAVE ID Nano models

Model series	Firmware	Android version
Proximity (RDR-6xUxAKU (125 kHz)	10.0.3	Android 10 and later
iClass (RDR-7xUxAKU (13.56 MHz)	16.2.3	Android 10 and later

Ensure that the following pre-requisites have been completed:

- The C•CURE Go Reader Driver has been installed. For more information, see Installing the C•CURE Go Reader driver.
- The C•CURE Go Reader app has been installed on your Android device. For more information see Downloading the C•CURE Go Reader .apk file from Google Play Store.

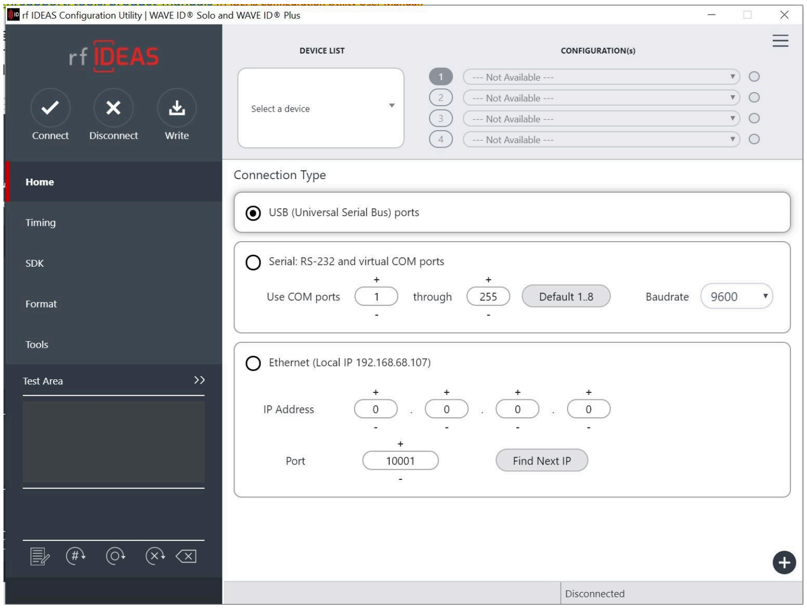
Configuring Wave ID Nano USB-C reader

You configure the Wave ID Nano USB-C Reader using the rf IDEAS Configuration Utility tool. You must configure the Nano USB-C reader before using the reader with a mobile device or tablet. You download the Configuration Utility tool from the rf IDEAS website.

For more information about Wave ID Nano USB-C reader configurations, see the Support Pages on the rf IDEAS website.

1. Download rf IDEAS Configuration Utility for Win 10/11 64 Bit.
2. Follow the instructions in the rf IDEAS Configuration Utility User Manual to install the Configuration Utility tool.
3. After installing the Configuration Utility tool, connect the Nano USB-C reader to your computer or laptop .
4. Open the Configuration Utility tool and click **CONNECT**.

Figure 15: rf IDEAS configuration utility tool user interface



rf IDEAS Configuration Utility | WAVE ID® Solo and WAVE ID® Plus

DEVICE LIST: Select a device

CONFIGURATION(s):
1 --- Not Available ---
2 --- Not Available ---
3 --- Not Available ---
4 --- Not Available ---

Connection Type

● USB (Universal Serial Bus) ports

○ Serial: RS-232 and virtual COM ports
Use COM ports 1 through 255 Default 1..8 Baudrate 9600

○ Ethernet (Local IP 192.168.68.107)
IP Address 0 . 0 . 0 . 0
Port 10001 Find Next IP

Disconnected

5. From the **DEVICE LIST**, select the device you want to connect.
6. From the menu list, click on **Timing**.
7. Set **card data hold time**, click the plus icon to increase the value or click the minus icon to decrease the value.
8. Set **lock-out time for repetitive reads**, click the plus icon to increase the value or click the minus icon to decrease the value.

   ⓘ **Note:** Set card data hold time to 100ms and lock-out time for repetitive reads to 2000ms. Card read timing affects the number of times a card is read by a reader. When the values are not set correctly, this can lead to errors.

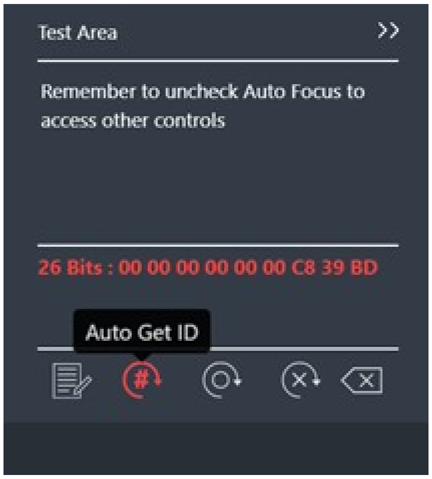
9. From the menu list, click **FORMAT** and then click on the **DATA FORMAT** tab.
10. Turn on the **Send ID** toggle switch.
11. Select the **Invert Wiegand bits** check box.

    ⓘ **Note:** Do not add Parity bits during configuration, this is handled by the GoReader app.

12. Click on the **Delimiters** tab.
13. In the **FAC/ID delimiter** field, enter **:** as the value.
14. From the **Menu** list, select **Write**. This writes all the required data to the connected WAVE ID Nano USB-C Reader.
15. From the **Menu** list, click **Test Area**.
16. Select **Auto Get ID**, then swipe a test card to the reader.

    The bits and Hex value of the card displays. This data is used for conversion and verification purpose. For example, you can convert the output HEX value into Binary and Decimal that matches the card value. See Figure 16.

Figure 16: Test Area bits and Hex value



Test Area

Remember to uncheck Auto Focus to access other controls

26 Bits : 00 00 00 00 00 00 C8 39 BD

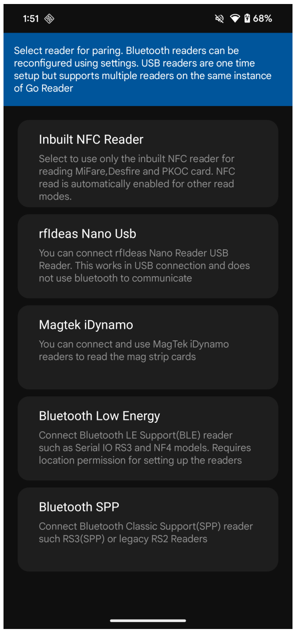
17. From the **Menu** list, click **Disconnect**.

Setting up Go Reader app for Wave ID Nano USB-C reader

Complete the following steps to set up the Go Reader app to use with Wave ID Nano USB-C reader:

1. Download and install the latest version of rf IDEAS Configuration Utility tool. See Configuring Wave ID Nano USB-C reader.
2. Insert the Wave ID Nano USB-C reader into the USB-C port of your mobile phone or tablet.
3. From the device home screen, tap on the **Go Reader app**.
4. Tap **YES** to `Allow GoReader to send you notifications?`.
5. On the **Reader Head Modes** screen, choose **rfIdeas Nano (USB Mode)** and then tap **PROCEED**.

Figure 17: Reader head modes



Select reader for paring. Bluetooth readers can be reconfigured using settings. USB readers are one time setup but supports multiple readers on the same instance of Go Reader

Inbuilt NFC Reader

Select to use only the inbuilt NFC reader for reading MiFare,Desfire and PKOC card. NFC read is automatically enabled for other read modes.

rfIdeas Nano Usb

You can connect rfIdeas Nano Reader USB Reader. This works in USB connection and does not use bluetooth to communicate

Magtek iDynamo

You can connect and use MagTek iDynamo readers to read the mag strip cards

Bluetooth Low Energy

Connect Bluetooth LE Support(BLE) reader such as Serial IO RS3 and NF4 models. Requires location permission for setting up the readers

Bluetooth SPP

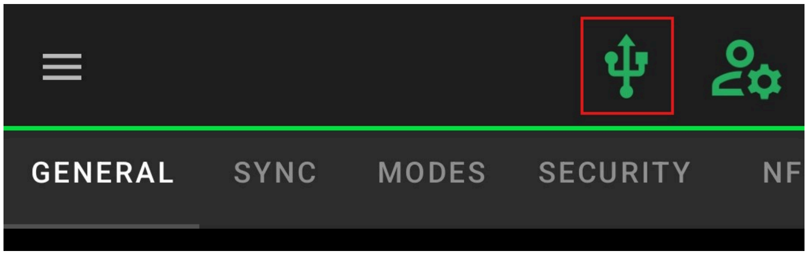
Connect Bluetooth Classic Support(SPP) reader such RS3(SPP) or legacy RS2 Readers

6. On the **Permissions** screen, tap **ACCEPT** to accept all permissions for the Go Reader app.
7. On the **Go Reader Permission Denied** box, tap **ANDROID APP SETTINGS**.
8. On Go Reader Android app permissions screen, tap each permission and select **ALLOW**.

9. Read the Privacy Notice, then tap **ACCEPT**.
10. On the **GoReader Identity** screen, select **C-CURE Identity**.

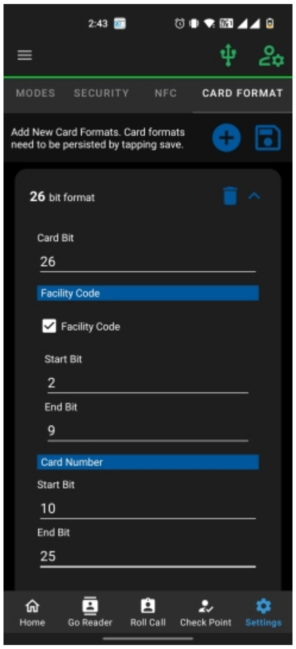
    For more information on the **Advanced Identity (Beta)** option, Go Reader Identity: Advanced identity (beta) mode.
11. In the **Operator Name** field, enter your operator name.
12. In the **Operator Password** field, enter your password.
13. In the **Server Address** field, enter the server address.
14. **Optional:** If you logon to the app across an unsecured network, tap **Use Secure Connection** to select the check box. Otherwise, ensure that the check box is cleared.
15. Tap **LOGIN**.
16. Select the **rf Ideas USB Reader** check box and then tap **YES** to register the device.
17. You must activate the reader in the C•CURE 9000 Administration Workstation, see Activating the Go Reader.
18. Open the Go Reader app on your Android device and tap the **USB Connection** icon.

Figure 18: USB connection icon - Go Reader app



19. Tap **OK** to access the USB Keyboard. The USB Connection icon changes from red to green when the Nano USB-C reader is connected.
20. On the home screen of the Go Reader app, tap the **USER** icon.
21. Type your **C-CURE Identity** user name and password. You must be logged on to use the Settings menu.
22. Tap the **HOME** icon, then tap **Settings**.
23. In the **Settings** menu, tap the **CARD FORMAT** tab.
24. In the **CARD FORMAT** tab, you configure the bit lengths the Nano USB-C reader can read. See the following figures for examples of three card formats you can configure.

Figure 19: Nano USB-C reader - 26 bit configuration



Add New Card Formats. Card formats need to be persisted by tapping save.

26 bit format

Card Bit: 26

Facility Code

☑ Facility Code

Start Bit: 2

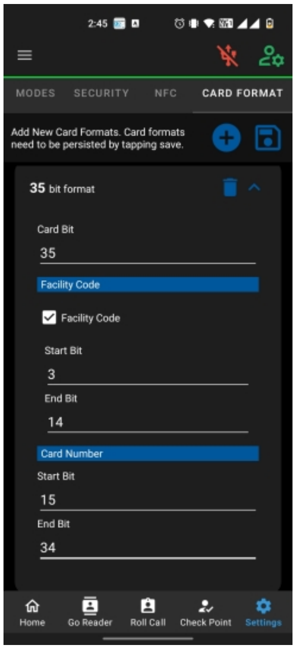
End Bit: 9

Card Number

Start Bit: 10

End Bit: 25

Figure 20: Nano USB-C reader - 35 bit configuration



Add New Card Formats. Card formats need to be persisted by tapping save.

35 bit format

Card Bit: 35

Facility Code

☑ Facility Code

Start Bit: 3

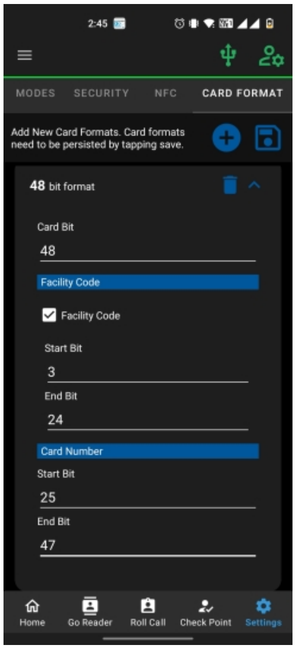
End Bit: 14

Card Number

Start Bit: 15

End Bit: 34

Figure 21: Nano USB-C reader - 48 bit configuration



Add New Card Formats. Card formats need to be persisted by tapping save.

48 bit format

Card Bit: 48

Facility Code

☑ Facility Code

Start Bit: 3

End Bit: 24

Card Number

Start Bit: 25

End Bit: 47

Card format configuration on Nano USB-C reader

This section describes how to test card format configurations with the Wave ID Nano USB-C reader and the C•CURE Go Reader app.

Ensure the following pre-requisites have been completed before testing:

- Installation of the C•CURE Go Reader driver. See Installing the C•CURE Go Reader driver.
- Installation of the C•CURE Go Reader app. See Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices.
- Enable the reader mode in the Go Reader editor. See Go Reader Configuration tab.
- If testing for FAC, activate Facility Card validation in the Go Reader editor. See Activating facility code validation.

Testing card format configurations

1. You must configure the Wave ID Nano USB-C reader using the rf IDEAS Configuration Utility tool. For more information, see Configuring Wave ID Nano USB-C reader.
2. You must set up the Go Reader app on your Android device.
3. On your Android device, tap the **Go Reader** icon to open the app.
4. On the C•CURE Go Reader app homepage, tap **Go Reader**.
5. Swipe a card on the Nano USB-C reader.

The personnel credentials for the card displays. If the card swipe is from an unregistered card, the card number displays.

MagTek iDynamo 6 configuration sequence

The MagTek iDynamo 6 USB-C reader is a compact USB-C form reader that is inserted into the USB-C port on a mobile phone or tablet. iDynamo 6 readers are used to scan magnetic stripe cards.

Ensure that you complete the following pre-requisites:

- The C•CURE Go Reader Driver has been installed. For more information, see Installing the C•CURE Go Reader driver.

- The C•CURE Go Reader app has been installed on your Android device. For more information see Downloading the C•CURE Go Reader .apk file from Google Play Store.

Setting up the iDynamo 6 USB-C reader in the Go Reader application

1. Insert the MagTek iDynamo 6 USB-C reader into the USB-C port on your mobile device.
2. On the home screen of your mobile device, open the **Go Reader application**.
3. On the `Allow Go Reader to send you notifications?` screen, tap **YES**.
4. On the **Reader Mode** screen, select **Magtek iDynamo**, then tap **YES** to confirm your choice.
5. On the **Permissions** screen, tap **ACCEPT** to accept all permissions for the Go Reader application.

   ⓘ **Note:** In the Settings application of your Android device, you can edit permissions for the Go Reader application. Navigate to **Settings** > **Apps** > **Permissions**.

6. On the **Go Reader Identity** screen, select **C-CURE Identity**.
7. On the **Associate Card Reader** screen, select **Magtek iDynamo**, then tap **YES** to register the device.

   The Go Device and Go Reader objects are created and activated in the C•CURE 9000 Administration Workstation.

8. On the Go Reader application **Home** screen, tap the **USB Connection** icon.
9. Tap **OK** to allow Go Reader access the iDynamo 6 reader.

   The USB Connection icon changes from red to green when the MagTek USB-C reader is connected.

10. On the home screen of the Go Reader app, tap the **USER** icon.
11. Type your **C-CURE Identity** user name and password. You must be logged onto use the Settings menu.
12. Tap **HOME** > **SETTINGS** and select the **MAGTEK** tab.
13. In the **MAGTEK** tab, configure the **Track** and **Card Bit** fields.
14. Tap **SAVE** to confirm the changes.

Inbuilt NFC reader configuration sequence

You can use the inbuilt NFC reader on your Android smartphone to scan cards with the Go Reader application. For a list of tested devices, see C•CURE Go Reader tested on Android devices.

Ensure that the following pre-requisites have been completed:

- The C•CURE Go Reader Driver has been installed. For more information, see Installing the C•CURE Go Reader driver.
- The C•CURE Go Reader app has been installed on your Android device. For more information see Downloading the C•CURE Go Reader .apk file from Google Play Store.

Setting up the Inbuilt NFC reader in the GoReader application

1. On the home screen of your mobile device, open the **Go Reader application**.
2. On the `Allow Go Reader to send you notifications?` screen, tap **YES**.
3. On the **Reader Mode** screen, select **Inbuilt NFC**, then tap **YES** to confirm your choice.
4. On the **Permissions** screen, tap **ACCEPT** to accept all permissions for the Go Reader application.

   ⓘ **Note:** In the Settings application of your Android device, you can edit permissions for the Go Reader application. Navigate to **Settings** > **Apps** > **Permissions**.

5. On the **Go Reader Identity** screen, select **C-CURE Identity**.
6. On the **Associate Card Reader** screen, select **Inbuilt NFC**, then tap **YES** to register the device.

   The Go Device and Go Reader objects are created and activated in the C•CURE 9000 Administration Workstation.

7. You must configure custom card formats to use the Inbuilt NFC reader. For more information, see Configuring custom MIFARE cards for Inbuilt Android NFC reader and Configuring custom DESFire cards for Inbuilt Android NFC reader.

Adding custom card formats for Inbuilt NFC readers

To add custom MIFARE and DESFire format cards on Android devices using an Inbuilt NFC reader, complete the following steps:

1. Open the Go Reader app, and tap the **CARD FORMAT** tab.
2. In the **CARD FORMAT** tab, tap the **Add** icon.
3. In the **Facility Code** section, select the **Set Facility Code** check box.
4. In the **Card Bit** field, enter the bit value of the custom card.
5. To configure the Facility Code start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in the **Facility Code** section, enter the **Start bit** number you want.
   b. To configure the end bit number, in the **Facility Code** section, enter the **End bit** number you want.

   ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.
6. To configure the **Card Number** start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in the **Card Number** section, enter the **Start bit** number you want.
   b. To configure the end bit number, in the **Card Number** section, enter the **End bit** number you want.

   ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.
7. Tap the **Save** icon.

The message `Card Format successfully saved to device` displays.

Configuring custom MIFARE cards for Inbuilt Android NFC reader

Before you begin:
You must complete the steps in Setting up the Inbuilt NFC reader in the GoReader application before configuring custom MIFARE cards.

1. On the home screen of your mobile device, tap to open the Go Reader application.
2. Tap **HOME** > **SETTINGS** and select the **CARD FORMAT** tab.
3. Tap the **Add** icon to configure a new card format.
4. In the **Facility Code** section, select the **Set Facility Code** check box.
5. In the **Start bit** and **End bit** fields, enter the values that match the MIFARE cards.
6. Tap the **SAVE** icon.

   If the changes are saved successfully, the message `Card Format successfully saved to device` displays.
7. Tap the **NFC** tab.
8. Expand the **MiFare Settings** section.
9. **Optional**: To read the serial number of MIFARE cards, select the **Read UID** check box.
10. **Optional**: To use factory default authentication keys, select the **Use factory default authentication key** check box.
11. In the **Sector and Block** section, use the **Sector** and **Block** lists to select the values.
12. Tap **SAVE**.

To check the card type swiped on the Inbuilt NFC reader, in the **NFC** tab, expand the **Card Information** section, and then swipe a card. The binary and bit size details of the card display.

Configuring custom DESFire cards for Inbuilt Android NFC reader

Before you begin:

You must check the **Application Id** of DESFIRE cards before configuring this card format. The Application Id of DESFire cards can be inverted from their originally programmed values by some programming applications. For example, if you use the Application Id `ABCDEF` to program a card, then the Application Id read by the application is `EFCDAB`.

To confirm the **Application Id** of DESFire cards, see Reading the Application Id of DESFire cards.

1. On the home screen of your mobile device, tap to open the Go Reader application.
2. Tap **HOME** > **SETTINGS** and select the **CARD FORMAT** tab.
3. Tap the **Add** icon to configure a new card format.
4. In the **Facility Code** section, select the **Set Facility Code** check box.
5. In the **Start bit** and **End bit** fields, enter the values that match the DESFire cards.
6. Tap the **SAVE** icon.

   If the changes are saved successfully, the message `Card Format successfully saved to device` displays.
7. Tap the **NFC** tab.
8. Expand the **Desfire Settings** section.
9. **Optional**: To read the serial number of DESFire cards, select the **Read UID** check box.
10. **Optional**: To use factory default authentication keys, select the **Use factory default authentication key** check box.
11. In the **Key**, **Application Id**, and **File Id** fields, enter the data values used to program DESFire cards.
12. In the **Encryption Type** section, choose between:
    - AES (Advanced Encryption Standard)
    - DES (Data Encryption Standard)
    - 3K3DES (Triple Data Encryption Standard)
13. Tap **SAVE**.

Serialio idChamp RS3 configuration sequence

If you are using an Android device, configure the Serialio reader with BLE or SPP mode enabled to communicate with the Android device. The Serialio idChamp RS3 reader can be configured using the pcProx Configuration Utility, for up to two card formats, called Configurations.

The Serialio idChamp RS3 card reader configuration sequence is described in Table 8. For more information about Serialio configurations, see the Support Pages on the Serialio website.

Ensure you complete the the following pre-requisites:

- You have installed the C•CURE Go Reader Driver. For more information see Installing the C•CURE Go Reader driver.
- You have installed the C•CURE Go Reader app on your Android device. For more information see Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices.

Table 8: Serialio idChamp RS3 Configuration Sequence

Step	Task	See
1	Configure the DIP switches in the Serialio idChamp RS3 reader board to connect the reader to your computer.	Serialio Support Pages: How to configure the idChamp RS3 for BLE mode.
2	Use the pcProx Configuration Utility to connect your Serialio idChamp RS3 reader to your computer.	Serialio Support Pages: Setup idChamp RS3 LE Bluetooth Low Energy 4.0 (BLE) RFID Reader for Windows.
3	Use the pcProx Configuration Utility to configure the card format for validating card swipes. You can configure the Serialio idChamp Reader to process the card number and facility code, and also set the delimeter value.	Configure card formats in the Serialio idChamp RS3 reader
4	Launch the C•CURE Go Reader app.	Launching the C•CURE Go Reader app

Configure card formats in the Serialio idChamp RS3 reader

Use the pcProx Configuration Utility to configure card formats in the Serialio idChamp RS3 reader.

The latest version of pcProx Configuration Utility can be downloaded from the RFIDeas website.

The Serialio idChamp RS3 reader supports prox, iCLASS and MIFARE cards, depending on the model. The basic configurations for 26-bit Wiegand cards in the pcProx Configuration Utility are:

- Strip the leading parity bits
- Strip the trailing parity bits
- Set the ID field bit count to 16

The C•CURE Go Reader app supports card number and Facility Code (FAC) output. The following section provides instructions for configuring these card formats in the pcProx Configuration Utility.

Ensure you have completed the following pre-requisites before configuring the Serialio idChamp RS3 reader:

- Download the latest version of pcProx Configuration Utility.
- Connect the Serialio idChamp RS3 reader to your computer using the pcProx Configuration Utility. For more information, see Setup idChamp RS3 LE Bluetooth Low Energy 4.0 (BLE) RFID Reader for Windows on the Serialio idChamp RS3 Support Pages.

Configuring the Serialio idChamp RS3 reader card formats for 26-bit Wiegand

1. Open the pcProx Configuration Utility.
2. Click the **Data format** tab.
3. In the **Strip leading bit count** field, set the value to `1`.
4. In the **Strip trailing bit count** field, set the value to `1`.
5. To configure card format processing modes:
   - Select the **Send ID** check box to process the Card Number(ID).
   - Select the **Send FAC** check box to process the Facility Code (FAC).
6. Set the value of the **ID field bit count** to `16`.
7. Select the **Invert Wiegand bits** check box.
8. If you need to process the Facility Code (FAC):
   a. Click the **Delimeters** tab.
   b. Click **FAC/ID delimeter** keyboard icon.

c. In the virtual keyboard, click the colon key **:**.

d. Click **Insert**.

9. Click **Device** and select **Write Settings**.

   Example: 26 bit card data

   26-bit card data example displays the settings for a 26 bit Wiegand card.

   Card format:

   - Start Position: 10
   - Length: 16

26-bit card data example

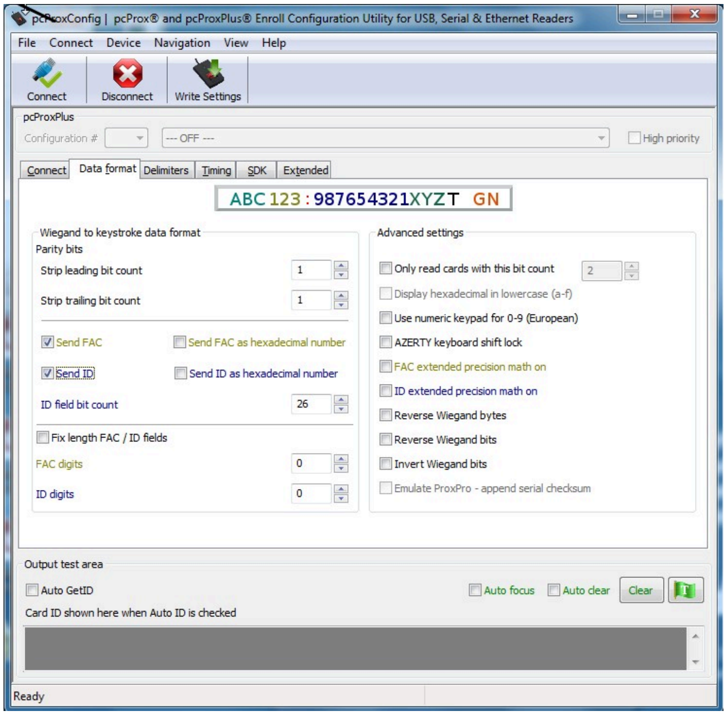
Figure 22 displays the settings for a 26 bit Wiegand card.

Card format:

- Start Position: 10
- Length: 16

ⓘ **Note:** Other card formats may require different settings. For more information, refer to the Serialio Support Pages.

Figure 22: pcProxConfiguration Utility Data format tab



Configuration # --- OFF --- □ High priority

ABC 123 : 987654321XYZT GN

Wiegand to keystroke data format

Parity bits

Strip leading bit count: 1

Strip trailing bit count: 1

☑ Send FAC □ Send FAC as hexadecimal number

☑ Send ID □ Send ID as hexadecimal number

ID field bit count: 26

□ Fix length FAC / ID fields

FAC digits: 0

ID digits: 0

Advanced settings

□ Only read cards with this bit count: 2

□ Display hexadecimal in lowercase (a-f)

□ Use numeric keypad for 0-9 (European)

□ AZERTY keyboard shift lock

□ FAC extended precision math on

□ ID extended precision math on

□ Reverse Wiegand bytes

□ Reverse Wiegand bits

□ Invert Wiegand bits

□ Emulate ProxPro - append serial checksum

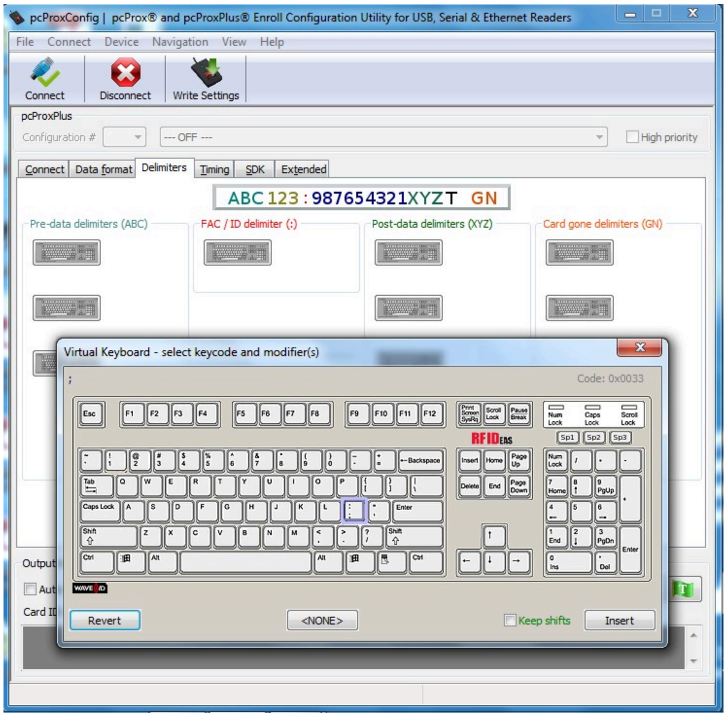
Output test area

□ Auto GetID □ Auto focus □ Auto clear

Card ID shown here when Auto ID is checked

Ready

Figure 23: pcProxConfiguration Utility Delimiters tabs


pcProxConfig | pcProx® and pcProxPlus® Enroll Configuration Utility for USB, Serial & Ethernet Readers
File Connect Device Navigation View Help
Connect
Disconnect
Write Settings
pcProxPlus
Configuration #
--- OFF ---
High priority
Connect
Data format
Delimiters
Timing
SDK
Extended
ABC 123 : 987654321XYZT GN
Pre-data delimiters (ABC)
FAC / ID delimiter (:)
Post-data delimiters (XYZ)
Card gone delimiters (GN)
Virtual Keyboard - select keycode and modifier(s)
;
Code: 0x0033
RFIDeas
Output
Card ID
Revert
<NONE>
Keep shifts
Insert

Card format configuration testing on Serialio idChamp RS3 reader

This section describes how to test card format configurations with the Serialio idChamp RS3 reader and the C•CURE Go Reader app.

Ensure the following pre-requisites have been completed before testing:

- Installation of the C•CURE Go Reader driver. See Installing the C•CURE Go Reader driver.
- Installation of the C•CURE Go Reader app. See Downloading and installing the C•CURE Go Reader app on C-ONE² and Android devices.
- Activate reader mode in the Go Reader editor. See Go Reader Configuration tab.
- If testing for FAC, activate facility card validation in the Go Reader editor. See Activating facility code validation.

Testing card format configurations

1. Set the DIP switches in the Serialio idChamp RS3 card reader to Bluetooth. For more information, see the Serialio Support pages.
2. Log on to the C•CURE Go Reader app using your log on credentials. For more information see Launching the C•CURE Go Reader app.
3. On the C•CURE Go Reader Home page, tap **Go Reader** .
4. Swipe a card on the Serialio idChamp RS3 card reader.

The personnel credentials for that card displays.

If the card swipe is from an unregistered card, the card number displays.

Go Reader Driver Service App for Access-ER and C-One² devices

To process card swipes and scan barcodes using the Go Reader app on Access-ER and C-One² devices, you must use the Go Reader driver service app.

You can use the Go Reader driver service app with the following models:

- Access-ER with HID read head

- C-One 2 with the ASK read head
- C-One 2 with the HID SE3200BS0 read head

For a C-ONE² device with ASK read heads, the user can select either SAM or without SAM options for processing of card swipes.

Setting up Go Reader Driver Service App for Access-ER devices

To process card swipes and scan barcodes using the Go Reader app on Access-ER devices, you must ensure the Go Reader driver service is active.

1. From the home screen, open the **GoReader Driver Service app**.
2. Tap on the **HID** tab.
3. Under **General Information**, ensure that **HID OMNIKEY 5127 CK 0** reader name is displayed.
4. **Optional:** If the information displayed in General Information is incorrect, return to the **HOME** tab and check **Driver Health Information**. This is required for the Go Reader application to function correctly.

Standard and custom modes in Access-ER and C-One² units with a HID head head

For Access-ER and C-One² HID read heads, the default configuration is standard. If standard is selected, you cannot configure the start bits and end bits of the card number or the facility code. Instead, the default number formats read.

In the following examples, **Standard** is selected in **Coppernic-HID (For HID Readhead)**, on the **GoReader Driver Service Screen**.

In the following table, the cardholder swipes a 35-bit HID Corp 1000 card on an Access-ER or C-One² HID unit. The card number reads correctly but the facility code reads incorrectly.

Table 9: Facility code reading error in standard mode with 35-bit card and Access-ER or C-One² HID unit

Card type	**Expected Card Number and Facility Code**		**Standard**	
			Actual Card Number and Facility Code	
	Card Number	Facility Code	Card Number	Facility Code
HID SeosIP (HID Corporate 1000- 35-bit)	1037816	4095	1037816	-1

To correct the facility code reading for a 35-bit HID Corp 1000 card, complete the procedure in Correcting the card number and facility code for a 35-bit HID Corp 1000 card. After you complete this procedure, the correct card number and facility code display. For more information, see the following table:

Table 10: Fixed facility code reading in standard mode with 35-bit card and HID Seos IP

Card type	**Expected Card Number and Facility Code**		**Custom**					
			Facility Code		**Card Number**		**Actual Card Number and Facility Code**	
	Card Number	Facility Code	Start Bit	End Bit	Start Bit	End Bit	Card Number	Facility Code
HID SeosIP (HID Corporate 1000-35bit)	1037816	4095	8	19	20	39	1037816	-1

In the following example, the cardholder swipes a 37-bit HID Seos IP H10304 card. The card number and the facility code read incorrectly.

Table 11: Fixed facility code reading in standard mode with 35-bit card and HID Seos IP

Card type	Expected Card Number and Facility Code		Standard	
			Actual Card Number and Facility Code	
	Card Number	Facility Code	Card Number	Facility Code
HID SeosIP (H10304) - 37bit	3	3746	1963982851	-1

To correct the card number and facility code reading for a 35-bit HID Corp 1000 card, complete the steps in Correcting the card number and facility code for a HID Seos IP (H10304 Format) 37-bit card on page 100. After you complete this procedure, the correct card number and facility code display.

Table 12: Fixed facility code reading in standard mode with 35-bit card and HID Seos IP

Card type	Expected Card Number and Facility Code		Custom					
			Facility Code		Card Number		Actual Card Number and Facility Code	
	Card Number	Facility Code	Start Bit	End Bit	Start Bit	End Bit	Card Number	Facility Code
HID SeosIP (H10304) - 37bit	3	3746	9	20	21	39	3	3746

Read head default configurations

Depending on the read head you use, different configuration options are enabled by default for the user. For more information, see the following examples:

- HID SE3200BS0 read head: In **Coppernic-HID (For HID Readhead)**, you select **Standard** or **Custom**. The default configuration is **Standard**.
- ASK read head: In **Coppernic-ASK (For ASK Readhead)**, you select **SAM** or **Without SAM**. The default configuration is **SAM**.

Correcting the card number and facility code for a 35-bit HID Corp 1000 card

1. On the **GoReader Driver Service Screen**, in **Coppernic-HID (For HID Readhead)**, tap **Custom**.
2. In **Facility Code**, select **Set Facility Code**.
3. In **Facility Code**, move **Start bit** to a value of `8`.
4. In **Facility Code**, move **End bit** to a value of `19`.
5. In **Card Number**, move **Start bit** to a value of `20`.
6. In **Card Number**, move **End bit** to a value of `39`.
7. **Optional**: To reverse the PACS bits data when the card is read, activate **Reverse PACS Data**.
8. **Optional**: To read the CSN instead of the card number and the facility code when a cardholder swipes a card, activate **Process CSN Instead of Card Number**.

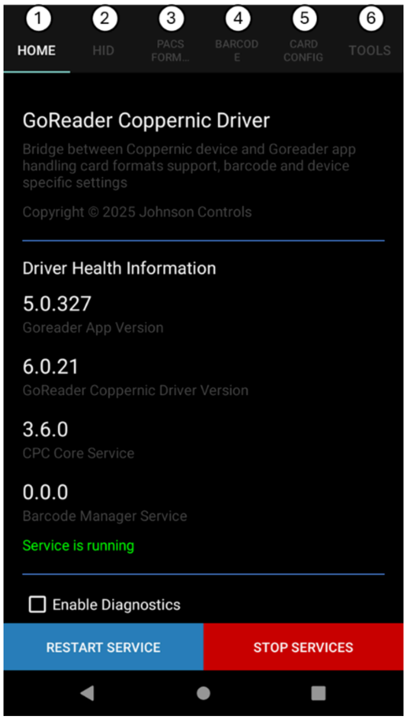
Correcting the card number and facility code for a HID Seos IP (H10304 Format) 37-bit card

1. On the **GoReader Driver Service Screen**, in **Coppernic-HID (For HID Readhead)**, tap **Custom**.
2. In **Facility Code**, select **Set Facility Code**.
3. In **Facility Code**, move **Start bit** to a value of `9`.
4. In **Facility Code**, move **End bit** to a value of `20`.
5. In **Card Number**, move **Start bit** to a value of `21`.
6. In **Card Number**, move **End bit** to a value of `39`.
7. **Optional**: To reverse the PACS bits data when the card is read, activate **Reverse PACS Data**.

8. **Optional**: To read the CSN instead of the card number and the facility code when a cardholder swipes a card, activate **Process CSN Instead of Card Number**.

Navigate the driver services app on Access-ER

Figure 24: Navigating the Driver Services app on Access-ER



GoReader Coppernic Driver

Bridge between Coppernic device and Goreader app handling card formats support, barcode and device specific settings

Copyright © 2025 Johnson Controls

Driver Health Information

5.0.327
Goreader App Version

6.0.21
GoReader Coppernic Driver Version

3.6.0
CPC Core Service

0.0.0
Barcode Manager Service

Service is running

□ Enable Diagnostics

Table 13: Navigating the Driver Services app on Access-ER

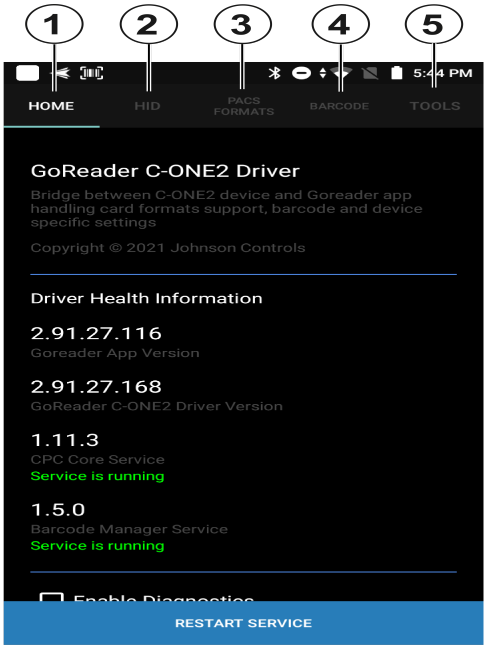
Callout	Option	Description
1	**HOME** tab	On the **HOME** tab, you can view the following driver health information: • Go Reader app version • Go Reader driver version • CPC core service • Barcode manager service On the **HOME** tab, you can complete the following actions: • Restart a service • Stop services • Enable diagnostics
2	**HID** tab	On the **HID** tab, you can view the HID interactor version, select the card read mode, activate the PACS data, and process the CSN.
3	**PACS FORMATS** tab	On the **PACS FORMATS** tab, you can perform the following actions: • Edit PACS formats for different card types • Add up to five PACS formats • Delete a PACS format • Import or export a PACS format
4	**BARCODE** tab	On the **Barcode** tab, you can read the barcode directly using default mode or read the Barcode by setting start and end bit index for payload processing with custom processing.

Table 13: Navigating the Driver Services app on Access-ER

Callout	Option	Description
5	**CARD CONFIG** tab	On the **Card Config** tab, you can customize how AccessER reads various card types, including MiFare Classic 1K/4K, MiFare DesFire, PKOC, and PIV cards.
6	**TOOLS** tab	On the **TOOLS** tab, you can view card swipe data. To enable the TOOLS tab, see Activating the TOOLS tab for Access-ER devices.

Navigate the driver services app on HID Read head C-ONE^2 devices

Figure 25: Navigating the Driver Services app on HID read head C-ONE^2 devices



GoReader C-ONE2 Driver

Bridge between C-ONE2 device and Goreader app handling card formats support, barcode and device specific settings

Copyright © 2021 Johnson Controls

Driver Health Information

2.91.27.116
Goreader App Version

2.91.27.168
GoReader C-ONE2 Driver Version

1.11.3
CPC Core Service
Service is running

1.5.0
Barcode Manager Service
Service is running

Table 14: Navigating the Driver Services app on HID readhead C-ONE^2 devices

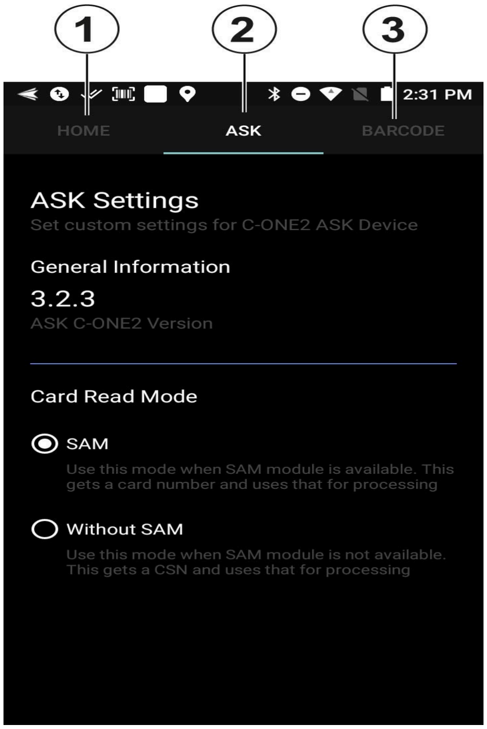
Callout	Option	Description
1	**HOME** tab	On the **HOME** tab, you can view the following driver health information: • Go Reader app version • Go Reader driver version • CPC core service • Barcode manager service On the **HOME** tab, you can complete the following actions: • Restart a service • Enable diagnostics
2	**HID** tab	On the **HID** tab, you can view the HID interactor version, select the card read mode, activate the PACS data, and process the CSN.
3	**PACS FORMATS** tab	On the **PACS FORMATS** tab you can to do the following actions: • Edit PACS formats for different card types • Add up to five PACS formats • Delete a PACS format • Import or export a PACS format

Table 14: Navigating the Driver Services app on HID readhead C-ONE² devices

Callout	Option	Description
4	**BARCODE** tab	On the **Barcode** tab, you can read the barcode directly using default mode or read the Barcode by setting start and end bit index for payload processing with custom processing.
5	**TOOLS** tab	On the **TOOLS** tab, you can view card swipe data. To enable the **TOOLS** tab, see Activating the TOOLS tab for HID read head C-ONE² devices and Activating the TOOLS tab for Access-ER devices.

Navigate the driver services app on ASK read head devices

Figure 26: Navigating the Driver Services app on ASK read head C-ONE² devices



ASK Settings

Set custom settings for C-ONE2 ASK Device

General Information

3.2.3

ASK C-ONE2 Version

Card Read Mode

● SAM

Use this mode when SAM module is available. This gets a card number and uses that for processing

○ Without SAM

Use this mode when SAM module is not available. This gets a CSN and uses that for processing

Table 15: Navigating the Driver Services app on ASK readhead C-ONE² devices

Callout	Option	Description
1	**HOME** tab	On the **HOME** tab, you can view the following driver health information: • Go Reader app version • Go Reader C-ONE² driver version • CPC core service • Barcode manager service On the **HOME** tab, you can complete the following actions: • Restart a service • Enable diagnostics
2	**ASK** tab	On the **ASK** tab, you can view general information and select the card read mode.
3	**BARCODE** tab	On the **Barcode** tab, you can read the barcode directly using default mode or read the Barcode by setting start and end bit index for payload processing with custom processing.

HOME tab

On the **HOME** tab, you can start a service, activate the diagnostics, and view the following driver health information:

- **GoReader App Version**
- **GoReader Driver Version**
- **CPC Core Service**
- **Barcode Manager Service**

HID tab

On the **HID** tab, in **Settings**, you can do the following:

- View the **HID Interactor Version**
- Select the **Card Read Mode**:
  - **Standard Format:** Select **Standard Format** to use the default card processing logic. **Standard Format** is the default format.
  - **Custom Format:** Select **Custom Format** to use the bit format configuration you define in **PACS Formats** on the **PACS FORMATS** tab.

On the **HID** tab, in **Advanced Settings**, you can do the following:

ⓘ **Note:** The advanced settings options are disabled by default. To activate the settings, in **Card Read Mode**, select **Custom Format**.

- Activate **Reverse PACS Data** to reverse the PACS Data. For example, you can processes LSB data as MSB data or process MSB data as LSB data.
- Activate **Process CSN**.

PACS formats tab

Use the PACS FORMATS tab to do the following actions:

- Edit PACS formats for different card types
- Add up to five PACS formats
- Delete a PACS format
- Import or export a PACS format

By default, you cannot use the **PACS FORMATS** tab. To use the **PACS FORMATS** tab, on the **HID** tab, in **Card Read Mode**, select **Custom Format**.

Card swipes register if you configure the required PACS format data of the card on the **PACS FORMATS** tab.

Adding a PACS format on the PACS FORMAT tab

You can add a maximum of five PACS formats. To add a PACS format, complete the following steps:

1. On the **PACS FORMATS** tab, in **Add new format**, enter the number of bits you want to configure.
2. To add the new PACS format, tap the **Add** icon.
3. In **Facility Code**, select the **Set Facility Code**.
4. To configure the Facility Code start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in **Facility Code**, move **Start bit** to the number you want.
   b. To configure the end bit number, in **Facility Code**, move **End bit** to the number you want.

   ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.
5. To configure the **Card Number** start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in **Card Number**, move **Start bit** to the number you want.

b. To configure the end bit number, in **Card Number**, move **End bit** to the number you want.

ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.

Exporting PACS formats on the PACS FORMAT tab

To export created PACS formats, complete the following steps:

1. On the **PACS FORMATS** tab, in **PACS Formats**, tap **Import/Export**.
2. In **Export**, tap **SHARE**.
3. In **Facility Code**, select **Set Facility Code**.
4. To share the format, select one of the sharing options.

   The shared PACS formats are in an encrypted JSON format.

Importing PACS formats on the PACS FORMAT tab

ⓘ **Note:** You can export a PACS format JSON file from an Access-ER or C-One² device that you previously configured and import the file to another Access-ER or C-ONE² device.

To import a PACS format JSON file, complete the following steps:

1. On the **PACS FORMATS** tab, in **PACS Formats**, tap **Import/Export**.
2. In **Import**, tap **Select File**.
3. Navigate to the file manager on your mobile device. Find and select the PACS format JSON file you want.
4. To import the PACS formats JSON file, tap **IMPORT**.
5. **Optional:** If you already imported a JSON file that contains the same PACS format start and end bit data, you must complete one of the following options:
   - To overwrite the old PACS format with the new configuration, in the dialog box, tap **YES**.
   - To keep the existing PACS format and reject the new configuration, in the dialog box, tap **NO**.

Deleting PACS formats on the PACS FORMAT tab

1. On the **PACS FORMATS** tab, in **PACS Formats**, expand the PACS format you want to delete.
2. Tap the x button.
3. To permanently delete the PACS format, in the dialog box, tap **OK**.

TOOLS tab

Use the **TOOLS** tab to view the following information when a cardholder swipes a card:

- Card Number
- Card PACS Bit length
- Card PACS Bit Stream
- Frame Bit Length
- Frame Bit Stream
- PACS Bytes
- Frame Bytes
- PACS Hexadecimal
- Frame Hexadecimal

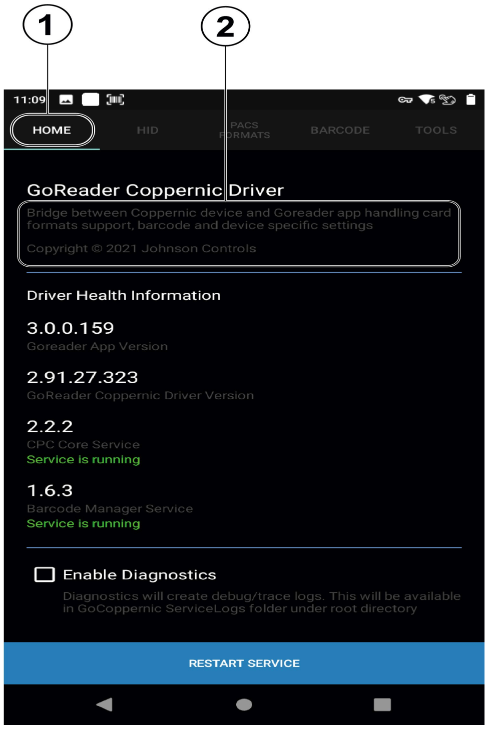
You can edit the facility code and card number PACS format data of the card.

ⓘ **Note:** You use the **TOOLS** tab on HID read head C-ONE devices . When you open the Go Reader Driver Services app, the **TOOLS** tab is always disabled. To activate the **TOOLS** tab, see Activating the TOOLS tab for HID read head C-ONE² devices.

Activating the TOOLS tab for Access-ER devices

1. Go to the **HOME** tab.
2. To activate the **TOOLS** tab, in **GoReader Coppernic Driver**, tap the description 7 times. For more information, see the following figure.

Figure 27: Tapping the GoReader Access ER Driver description to activate the TOOLS tab



GoReader Coppernic Driver

Bridge between Coppernic device and Goreader app handling card formats support, barcode and device specific settings

Copyright © 2021 Johnson Controls

Driver Health Information

3.0.0.159
Goreader App Version

2.91.27.323
GoReader Coppernic Driver Version

2.2.2
CPC Core Service
Service is running

1.6.3
Barcode Manager Service
Service is running

□ Enable Diagnostics

Diagnostics will create debug/trace logs. This will be available in GoCoppernic ServiceLogs folder under root directory

Callout	Option
1	**HOME** tab
2	Area to tap

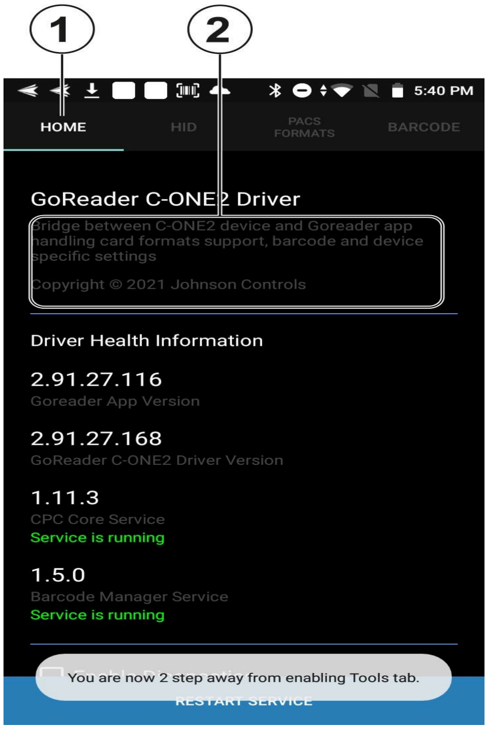
The **TOOLS** tab is now available.

Activating the TOOLS tab for HID read head C-ONE² devices

ⓘ **Note:** You can activate the **TOOLS** tab on HID read head C-ONE² devices.

1. Go to the **HOME** tab.
2. To activate the **TOOLS** tab, in **GoReader C-ONE2 Driver**, tap the description 5 times. For more information, see the following figure.

Figure 28: Tapping the GoReader C-ONE² Driver description to activate the TOOLS tab



GoReader C-ONE2 Driver

Bridge between C-ONE2 device and Goreader app handling card formats support, barcode and device specific settings

Copyright © 2021 Johnson Controls

Driver Health Information

2.91.27.116
Goreader App Version

2.91.27.168
GoReader C-ONE2 Driver Version

1.11.3
CPC Core Service
Service is running

1.5.0
Barcode Manager Service
Service is running

You are now 2 step away from enabling Tools tab.

Callout	Option
1	**HOME** tab
2	Area to tap

The **TOOLS** tab is now available.

BARCODE tab

Use the **BARCODE** tab to complete the following actions:

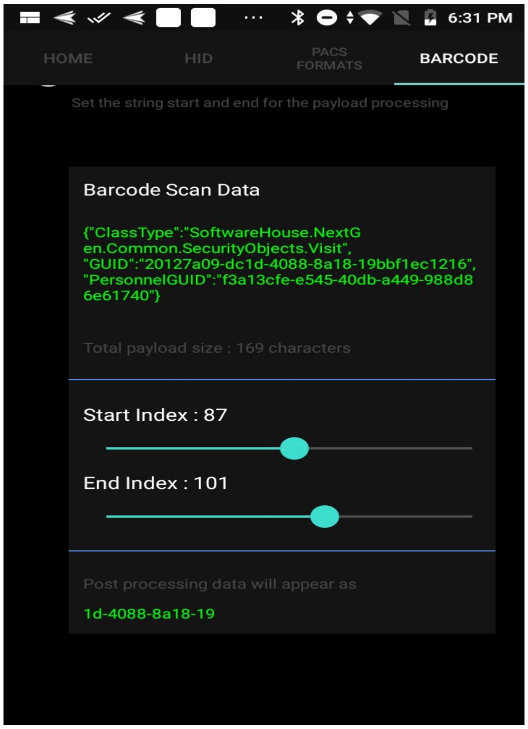
- Set **Barcode Read Mode** to the following options:
  - **Default**: Read the barcode directly without processing the barcode payload.
  - **Custom Processing**: Set the barcode string start and end bit index for payload processing.

Adding a new custom process

1. To view **Barcode Scan Data**, on the **BARCODE** tab, in **Barcode Read Mode**, select **Custom Processing**.
2. Scan the barcode that you want to filter. When the barcode scans successfully, in **Barcode Scan Data**, the data displays.
3. To configure the start index, in **Barcode Scan Data**, move **Start Index** to the index you want.
4. To configure the end index, in **Barcode Scan Data**, move **End Index** to the index you want.

   ⓘ **Note:** To keep the configuration, do not disable **Custom Processing**.

Figure 29: Barcode scan data



Set the string start and end for the payload processing

Barcode Scan Data

```
{"ClassType":"SoftwareHouse.NextG
en.Common.SecurityObjects.Visit",
"GUID":"20127a09-dc1d-4088-8a18-19bbf1ec1216",
"PersonnelGUID":"f3a13cfe-e545-40db-a449-988d8
6e61740"}
```

Total payload size : 169 characters

Start Index : 87

End Index : 101

Post processing data will appear as

1d-4088-8a18-19

Adding custom format cards on Access-ER

To add custom format cards on Access-ER devices, complete the following steps:

1. Open the GoReader Driver Services App, tap the **PACS FORMAT** tab, then tap the **HID** tab.
2. On the **HID Settings** screen, in the **Card Read Mode** section, select the **Custom Format** option.
3. On the **PACS Format** tab, tap the **Add** icon.
4. In the **Card Bit** field, enter the bit value of the custom card.
5. In the **Facility Code** section, select the **Set Facility Code** check box.
6. To configure the Facility Code start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in the **Facility Code** section, enter the **Start bit** number you want.
   b. To configure the end bit number, in the **Facility Code** section, enter the **End bit** number you want.

   ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.
7. To configure the **Card Number** start and end bit numbers, complete the following steps:
   a. To configure the start bit number, in the **Card Number** section, enter the **Start bit** number you want.
   b. To configure the end bit number, in the **Card Number** section, enter the **End bit** number you want.

   ⓘ **Note:** You can configure a minimum of 8 bits and maximum 128 bits.
8. Use the **TOOLS** tab to read the card number and facility code values of the MIFARE or DESFire card. For more information, see TOOLS tab.

You can configure MIFARE and DESFire cards on the GoReader Driver Service App. For more information, see Configuring MIFARE cards on Access-ER and Configuring DESFire cards on Access-ER.

Configuring MIFARE cards on Access-ER

Before you begin:

Before configuring MIFARE cards on an Access-ER device, you must add custom 128-bit format cards that define the start bits and ends bits of the Facility Code and Card Number. These bit definitions must match the values programmed on the MIFARE cards. For more information, see Adding custom format cards on Access-ER.

ⓘ **Note:** You must download and install Go Reader Driver App v.6.0.17 or later from the CopperApp Store to configure MIFARE cards.

1. On your Access-ER device, on the **Home** screen, tap to open the **Go Reader Driver App**.
2. On the Go Reader Driver App, tap the **MIFARE** tab.
3. On the **MIFARE Settings** screen, expand the **MIFARE Classic 1K/4K** section.
4. To read the serial number of MIFARE cards, select the **Read UID** check box.
5. To read sector and block data from MIFARE cards, select the **Sector and Block** check box.
6. In the **Reader key number**, **Sector**, **Block**, and **MIFARE Key A/B** fields, enter the data values used to program MIFARE cards.

   ⓘ **Note:** In the **Reader key number** field, use the default value of 1.
7. Tap **Save**.

Configuring DESFire cards on Access-ER

Before you begin:

Before configuring DESFire cards, you must add custom 128-bit format cards that define the start bits and ends bits of the Facility Code and Card Number. These bit definitions must match the values programmed on the DESFire cards. For more information, see Adding custom format cards on Access-ER.

You must check the **Application Id** of DESFire cards before completing the following procedure. For more information, see Reading the Application Id of DESFire cards.

ⓘ **Note:** You must download and install Go Reader Driver Services App v.6.0.17 or above to configure DESFire cards.

1. On your Access-ER device, on the **Home** screen, tap to open the Go Reader Driver Services App.
2. On the Go Reader Driver Services App, tap the **MIFARE** tab.
3. On the **MIFARE Settings** screen, expand the **MIFARE DESFire** section.
4. **Optional**: To read the serial number of DESFire cards, select the **Read UID** check box.
5. **Optional**: To read **Application Id** and **File** data from DESFire cards, select the **App Id and File** check box.
6. In the **Key**, **Application Id**, and **File Id** fields, enter the data values used to program DESFire cards.

   ⓘ **Note:** The default value for the **Reader Key Slot Id** is 240 and the default value for **Card Key Number** is 1. It is best practice to use the default values.
7. In the **Encryption Type** section, choose between:
   - AES (Advanced Encryption Standard)
   - DES (Data Encryption Standard)
   - 3K3DES (Triple Data Encryption Standard)
8. Tap **Save**.

Reading the Application Id of DESFire cards

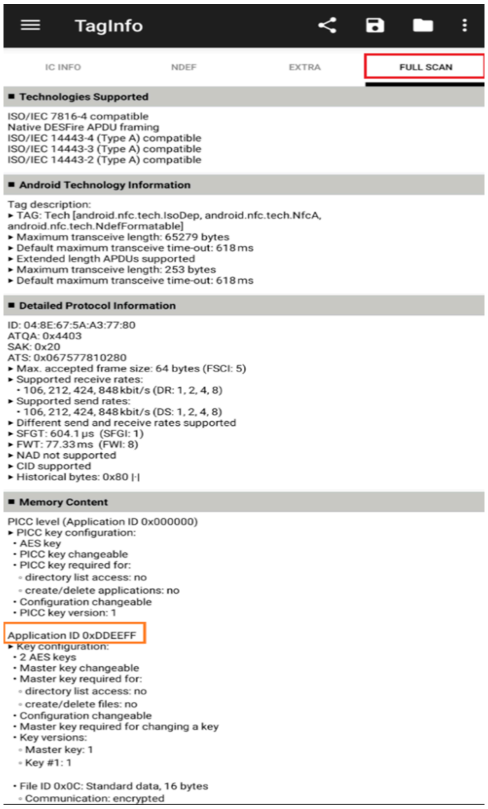
The **Application Id** of DESFire cards can be inverted from their originally programmed values by some programming applications. For example, if you use the Application Id `ABCDEF` to program a card, then the Application Id read by the application is `EFCDAB`.

You must download and install the **NFC TagInfo by NXP** application on an NFC enabled Android smartphone to ensure you enter the correct Application Id.

Note: You cannot install the NFC TagInfo by NXP app on Access-ER devices.

1. On your Android smartphone, open the **Google Play Store**.
2. In the search bar, type `NFC TagInfo by NXP`.
3. Tap **Install**.
4. When the download is complete, open the **NFC TagInfo by NXP** app.
5. Present a DESFire card to the back of your smartphone.
6. Tap on the **FULL SCAN** tab, and take note of the **Application Id**.

Figure 30: TagInfo - Application Id



```
■ Technologies Supported
ISO/IEC 7816-4 compatible
Native DESFire APDU framing
ISO/IEC 14443-4 (Type A) compatible
ISO/IEC 14443-3 (Type A) compatible
ISO/IEC 14443-2 (Type A) compatible

■ Android Technology Information
Tag description:
▸ TAG: Tech [android.nfc.tech.IsoDep, android.nfc.tech.NfcA,
android.nfc.tech.NdefFormatable]
▸ Maximum transceive length: 65279 bytes
▸ Default maximum transceive time-out: 618 ms
▸ Extended length APDUs supported
▸ Maximum transceive length: 253 bytes
▸ Default maximum transceive time-out: 618 ms

■ Detailed Protocol Information
ID: 04:8E:67:5A:A3:77:80
ATQA: 0x4403
SAK: 0x20
ATS: 0x067577810280
▸ Max. accepted frame size: 64 bytes (FSCI: 5)
▸ Supported receive rates:
  • 106, 212, 424, 848 kbit/s (DR: 1, 2, 4, 8)
▸ Supported send rates:
  • 106, 212, 424, 848 kbit/s (DS: 1, 2, 4, 8)
▸ Different send and receive rates supported
▸ SFGT: 604.1 µs  (SFGI: 1)
▸ FWT: 77.33 ms  (FWI: 8)
▸ NAD not supported
▸ CID supported
▸ Historical bytes: 0x80 |·|

■ Memory Content
PICC level (Application ID 0x000000)
▸ PICC key configuration:
 • AES key
 • PICC key changeable
 • PICC key required for:
  ◦ directory list access: no
  ◦ create/delete applications: no
 • Configuration changeable
 • PICC key version: 1

Application ID 0xDDEEFF
▸ Key configuration:
 • 2 AES keys
 • Master key changeable
 • Master key required for:
  ◦ directory list access: no
  ◦ create/delete files: no
 • Configuration changeable
 • Master key required for changing a key
 • Key versions:
  ◦ Master key: 1
  ◦ Key #1: 1

 • File ID 0x0C: Standard data, 16 bytes
  ◦ Communication: encrypted
```

C•CURE Go Reader objects

For each C•CURE Go Reader, two objects are created in the C•CURE 9000 hardware tree. A C•CURE **Go Reader Device**, that represents the specific Android device you are using, and a C•CURE **Go Reader**, located in the doors folder in the hardware tree. The **Go Reader** is a door object that you use in the clearances tab of the personnel editor to define the personnel profiles that are validated on the device. You can also use the **Go Reader** door object to configure specific Roll Call parameters.

Unlike other C•CURE 9000 hardware objects such as iSTAR controllers, you cannot create a C•CURE Go Device or C•CURE Go Reader in the hardware tree. The two objects are automatically created in the hardware tree after the first time that the app is authorized and activated from C•CURE 9000. Activation is complete when an operator edits the new **Go Reader** and activates it.

Use the Go Device editor to:

- Name and provide a description for the Go Device.
- View general system information about the Android device connected to C•CURE 9000.

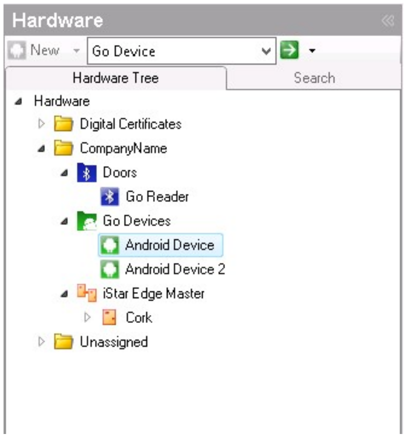
For more information, see C•CURE Go device editor.

Use the GoReader editor to:

- Activaate the C•CURE Go Reader app.
- Activate and disable roll call, reader, image download and message suppression modes.
- Activate facility code validation in the Go Reader.
- Assign roll call areas and missing areas to the C•CURE Go Reader app.
- View the status and state information of the C•CURE Go Reader.
- Assign events and triggers to the C•CURE Go Reader app.

For more information, see Go Reader editor.

Figure 31: C•CURE Go Reader objects



C•CURE Go device editor

The **Go Device** object is located in the hardware tree and represents the specific Android device that you are using with the C•CURE Go Reader app.

The Go Device object is automatically created in the hardware tree after the first time the app is authorized from C•CURE 9000. Activation of the C•CURE Go Reader is completed by enabling the C•CURE Go Reader app with the Go Reader editor. For more information, see Activating the Go Reader.

Use the Go Device editor to:

- Name and provide a description for the Go Device.
- View general system information about the Android device connected to C•CURE 9000.

C•CURE Go Device Tabs:

- Go Device general tab
- Go Device status tab

Accessing the Go Device Editor

Access the Go Device editor from the hardware tree in the C•CURE Administration Station.

1. In Administration Workstation, in the **Navigation** pane, select **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand the **Go Devices** folder.
4. Choose from the following options:
   - Right-click the **Go Device** you want to access and select **Edit**.
   - Double-click the **Go Device** you want to access.

Go Device general tab

Use the **General Tab** to edit the name and description of the C•CURE Go Reader device and view general information about the device.

Table 16: GoDevice fields and descriptions

Field	Description
Serial Number	(Read Only) Unique identity of the device hardware.
Operating System Version	(Read Only) Operating system version of the device.
Operating System Type	(Read Only) Operating system type of the device.

Go Device status tab

Use the **Status Tab** to view the communication status of Go Device. The **Last Communicated Time** field is a read-only field that shows the most recent time that the C•CURE 9000 server communicated with the device.

Go Reader editor

The **Go Reader** editor is located in the doors folder in the hardware tree. The **Go Reader** is a door object that you use in clearances to define the personnel profiles that are validated on the device.

You cannot create the Go Reader object in the hardware tree. The Go Reader object is automatically created the first time that the app is authorized and activated from C•CURE 9000. Activation is complete when the operator enables the Go Reader app with the Go Reader editor. For more information, see Activating the Go Reader.

Use the Go Reader editor to:

- Activate the C•CURE Go Reader app.
- View and edit configuration information.
- Activate and disable roll call, reader, image download and message suppression modes.
- Activate facility code validation in the Go Reader.
- Assign roll call areas and missing areas to the C•CURE Go Reader app.
- View the status and state information of the C•CURE Go Reader.
- Assign events and triggers to the C•CURE Go Reader app.

C•CURE Go Reader editor tabs:

- Go Reader Configuration tab
- Go Reader Reader tab
- Go Reader Roll Call tab
- Go Reader Check Point tab
- Go Reader Card Formats tab
- Go Reader Barcode tab
- Go Reader MiFare Settings tab
- Go Reader DesFire Settings tab
- Go Reader Secure Cards tab
- Go Reader System Information tab
- Go Reader Triggers tab
- Go Reader Status tab

- Go Reader State Images tab

C•CURE Go Reader editor tasks:

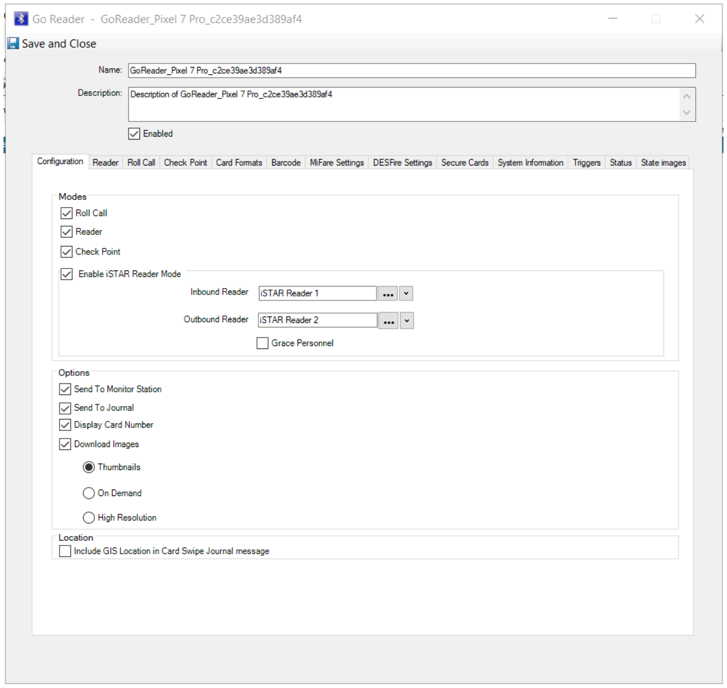
- Accessing the Go Reader editor
- Activating the Go Reader
- Disabling the Go Reader
- Assigning a roll call area
- Assigning a missing area
- Activating facility code validation
- Configuring triggers and events
- Removing triggers and events

Go Reader Configuration tab

Use the Configuration tab to name and provide a description of the Go Reader and to activate the following modes and options on the Go Reader device:

- Roll Call
- Reader
- Check Point
- Enable iSTAR Reader Mode
- Send to Monitoring Station
- Send to journal
- Display card number
- Download images
- Include GIS location in Card Swipe Journal message

Figure 32: Go Reader Configuration tab



Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

Modes

☑ Roll Call

☑ Reader

☑ Check Point

☑ Enable iSTAR Reader Mode

Inbound Reader: iSTAR Reader 1

Outbound Reader: iSTAR Reader 2

☐ Grace Personnel

Options

☑ Send To Monitor Station

☑ Send To Journal

☑ Display Card Number

☑ Download Images

● Thumbnails

○ On Demand

○ High Resolution

Location

☐ Include GIS Location in Card Swipe Journal message

Table 17: Configuration tab fields and descriptions

Option	Description
Modes	
Roll Call	Select to activate or disable Roll Call in the C•CURE Go Reader. After disabling: • The Roll Call function is not available in the C•CURE Go Reader. • The Roll Call tab options in the GoReader editor are read only. If you activate or disable this mode and click **Save and Close**, a notification displays in the Go Reader app.
Reader	Select to activate or disable Reader mode in the C•CURE Go Reader. After disabling: • The Reader function is not available in the C•CURE Go Reader • The Reader tab options in the Go Reader editor are read only. If you activate or disable this mode and click **Save and Close**, a notification displays in the Go Reader app.
Check Point	Select to activate or disable Check Point mode in the C•CURE Go Reader. After disabling: • The Check Point function is not available in the C•CURE Go Reader. • The Check Point tab options in the Go Reader editor are read only. If you activate or disable this mode and click **Save and Close**, a notification displays in the Go Reader app.
Enable iSTAR Reader Mode	Select to activate or disable iSTAR Reader Mode in the C•CURE Go Reader. After enabling: • The user must choose either **Inbound Reader**, **Outbound Reader**, or both. If both are selected, the readers must be connected to the same controller. • Optionally, the user can enable or disable the **Grace Personnel** feature. If you activate or disable this mode and click **Save and Close**, a notification displays in the Go Reader app.
Options	
Send to Monitor Station	Select to log journal messages to the Monitoring Station.
Display Card Number	Select to display the card number of valid users that swipe at the reader. The card number displays in the Go Reader, Roll Call, and Check Point modules. The **Display Card Number** option is enabled by default. If you activate or disable this mode and click **Save and Close**, a notification displays in the Go Reader app.
Send to Journal	Select to log journal messages to the Journal Database.
Download Images	Select to download images to C•CURE Go Reader device. **Thumbnails**, **On Demand**, and **High Resolution** images are available. **High Resolution** is enabled by default. If you activate or disable this mode and click **Save and Close**, a messages displays `This will initiate synchronization! Are you sure you want to continue?`. Click **Yes** to synchronize with the Go Reader app. A notification displays in the Go Reader app. ⓘ **Note:** If you select the **On Demand** option and click **Save and Close**, the `This will initiate synchronization! Are you sure you want to continue?` message does not display.

Table 17: Configuration tab fields and descriptions

Option	Description
Location	
Include GIS Location in Card Swipe Journal message	Select to include the geographic information system (GIS) location in the journal message is enabled by default. See View GIS location in card swipe journal message for more information.

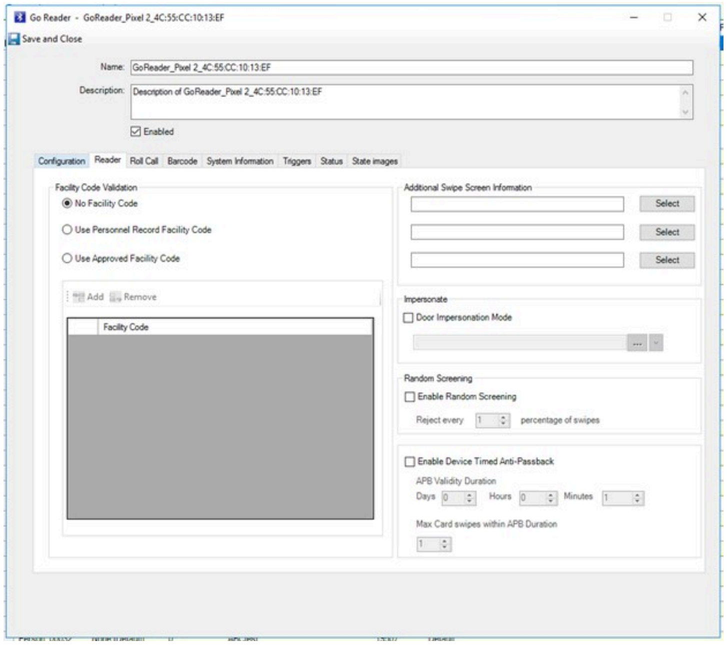
ⓘ **Note:** If the Go Reader device is not connected to the server when you activate or disable any mode or option, the changes are sent when the device comes online, connects to server, and synchronization is initiated.

Go Reader Reader tab

Use the Reader tab to activate the following functions:

- Facility Code validation
- Additional swipe screen information
- Door Impersonation Mode
- Random screening
- Timed anti-passback

Figure 33: Go Reader Reader tab



Go Reader - GoReader_Pixel 2_4C:55:CC:10:13:EF

Save and Close

Name: GoReader_Pixel 2_4C:55:CC:10:13:EF

Description: Description of GoReader_Pixel 2_4C:55:CC:10:13:EF

☑ Enabled

Facility Code Validation

● No Facility Code

○ Use Personnel Record Facility Code

○ Use Approved Facility Code

Additional Swipe Screen Information

Impersonate

□ Door Impersonation Mode

Random Screening

□ Enable Random Screening

Reject every 1 percentage of swipes

□ Enable Device Timed Anti-Passback

APB Validity Duration

Days 0 Hours 0 Minutes 1

Max Card swipes within APB Duration 1

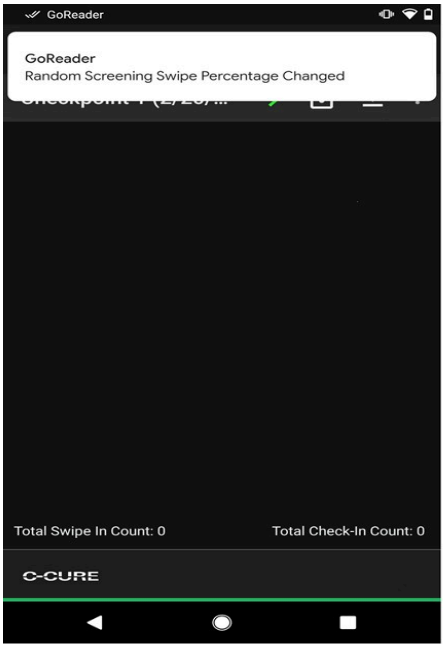
Table 18: Reader tab fields and descriptions

Field	Description
Facility Code Validation	
No Facility Code	Select this option to disable facility code validation so that the Go Reader validates a card swipe based on the card number (ID).

Table 18: Reader tab fields and descriptions

Field	Description
Use Personnel Record Facility Code	Select this option to activate facility code validation so that the Go Reader validates a card swipe when the facility code encoded in the card matches the facility code in the personnel record's credentials. For information about configuring facility codes in personnel records, refer to the *C•CURE 9000 Personnel Configuration Guide.*
Use Approved Facility Code	Select this option to activate facility code validation so that the Go Reader validates a card swipe if it has a facility code from the list of approved facility codes.
Add	Click to add a row to the list of approved facility codes. There is no limitation on the amount of approved facility codes you can add to the list. This option is available if you activate **Use Approved Facility Code**.
Remove	Click to remove a row from the list of approved facility codes. This option is available if you activate **Use Approved Facility Code**.
Additional Swipe Screen Information	
Select	Click to access the **Personnel Field Picker**. Select a personnel field and click **OK** to add the field to the additional swipe screen information. This information is included during card swipe and roll call. See Use custom data fields for swipe and roll call for more information.
Impersonate	
Door Impersonation Mode	Select to activate **Door Impersonation Mode** to impersonate a particular door. Use when there are issues with a physical door. Click ... to select a door to impersonate. See Impersonating a door for more information.
Random Screening	
Enable Random Screening	Select to activate the **Random Screening** feature that rejects a selected percentage of card swipes. Figure 34 shows the notification that random screening is enabled on the GoReader application for Android devices.
Reject every # percentage of swipes	To configure the percent field, increase or decrease the percentage of card swipes randomly screened.
Anti-Passback	
Enable Device Timed Anti-Passback	Select to activate timed anti-passback. Anti-passback prevents personnel from "passing back" a card for another person to swipe. Timed anti-passback is device specific. See Activating timed anti-passback for more information.
APB Validity Duration	Set the anti-passback expiry time to a duration of between 1 minutes and 7 days.
Max card swipe within APB Duration	Identifies the maximum number of card swipes during the anti-passback duration. Type in a number to change the maximum number of card swipes. The maximum number of card swipes in APB duration is 10.

Figure 34: Go Reader Random Screening notification



GoReader

GoReader
Random Screening Swipe Percentage Changed

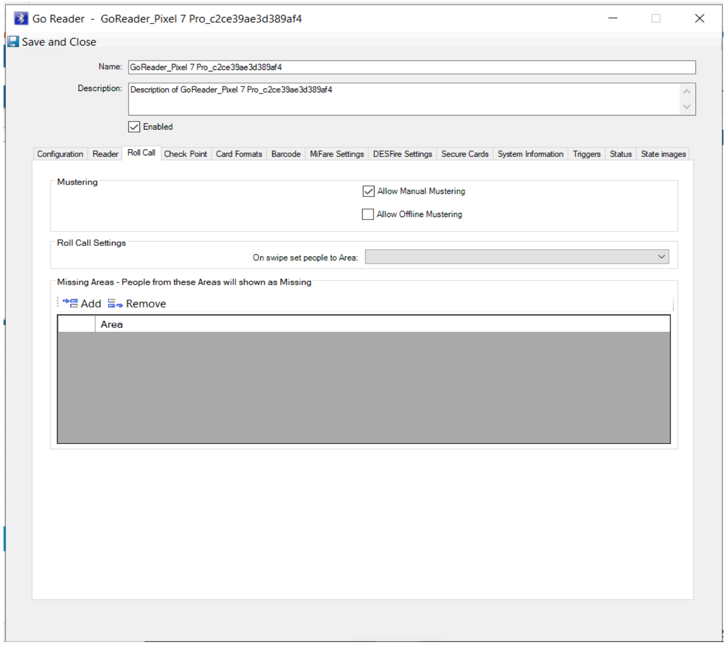
Total Swipe In Count: 0

Total Check-In Count: 0

Go Reader Roll Call tab

Use the Roll Call tab to assign a Roll Call area and add Missing areas to the Go Reader. Table 19 describes the settings in the Roll Call tab.

Figure 35: Roll Call tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

Mustering

☑ Allow Manual Mustering

☐ Allow Offline Mustering

Roll Call Settings

On swipe set people to Area:

Missing Areas - People from these Areas will shown as Missing

Table 19: Roll Call tab

Field/Button	Description
Allow Manual Mustering	Select to activate manual mustering.
Allow Offline Mustering	Select to activate offline mustering.

Table 19: Roll Call tab

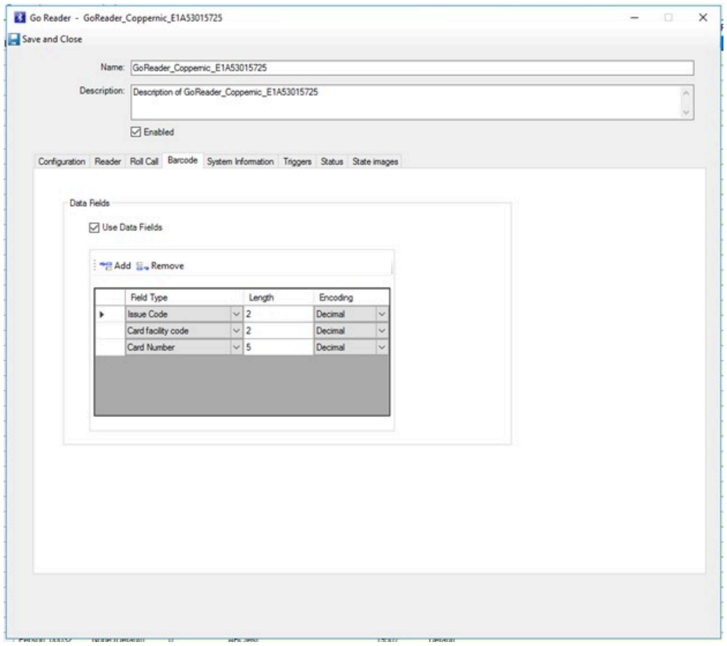
Field/Button	Description
Roll Call Settings	Select an area to assign to roll call settings. This is the area where, when a card is swiped, the card holder is registered in that selected area.
Missing Areas	Select an area to assign to missing areas. Personnel from these areas are registered as missing from the roll call area.

Go Reader Barcode tab

Use the Barcode tab to assign a field type, length, and encodings to the Go Reader device. You can include the following field types: issue code, card facility code, and card number. Table 20 describes the settings in the Barcode tab. The functions in the Barcode tab are available for C-One², Access-ER, and Android devices.

Note: You can add a maximum of 3 field types.

Figure 36: Barcode tab



Name: GoReader_Coppernic_E1A53015725

Description: Description of GoReader_Coppernic_E1A53015725

☑ Enabled

☑ Use Data Fields

Field Type	Length	Encoding
Issue Code	2	Decimal
Card facility code	2	Decimal
Card Number	5	Decimal

Table 20: Barcode tab

Field/Button	Description
Use Data Fields	Select to activate the data fields. You can then change the field type, length, and encoding type, as shown in Figure 36. The following field types are available: • Issue Code • Card Facility Code • Card Number The following encoding types are available: • Decimal • HEX • ASCII

Barcode use cases

The following are example use cases for barcode with Go Reader.

To create a badge layout to use the barcode, see Barcode use cases with default processing.

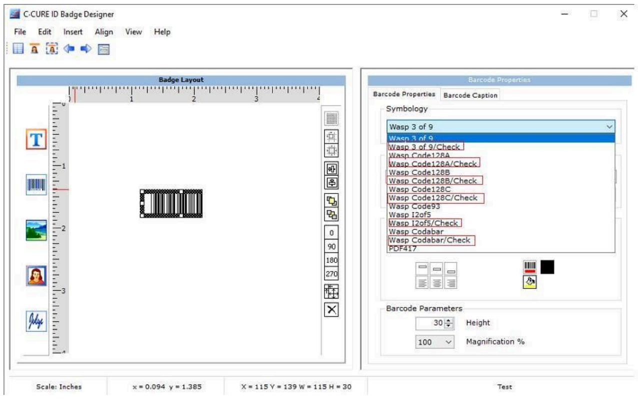
The following symbology is supported:

- Wasp 3 of 9
- Wasp Code128A
- Wasp Code128B
- Wasp Code128C
- Wasp I2of5
- Wasp Codabar
- PDF417
- QR Code
- GS1 DataMatrix

The following symbology is not supported, as shown in Figure 37:

- Wasp 3 of 9/Check
- Wasp Code128A/Check
- Wasp Code128B/Check
- Wasp Code 128C/Check
- Wasp I2of5/Check
- Wasp Codabar/Check

Figure 37: C•CURE ID Badge Designer



Symbology

Wasp 3 of 9

Wasp 3 of 9
Wasp 3 of 9/Check
Wasp Code128A
Wasp Code128A/Check
Wasp Code128B
Wasp Code128B/Check
Wasp Code128C
Wasp Code128C/Check
Wasp Code93
Wasp I2of5
Wasp I2of5/Check
Wasp Codabar
Wasp Codabar/Check
PDF417

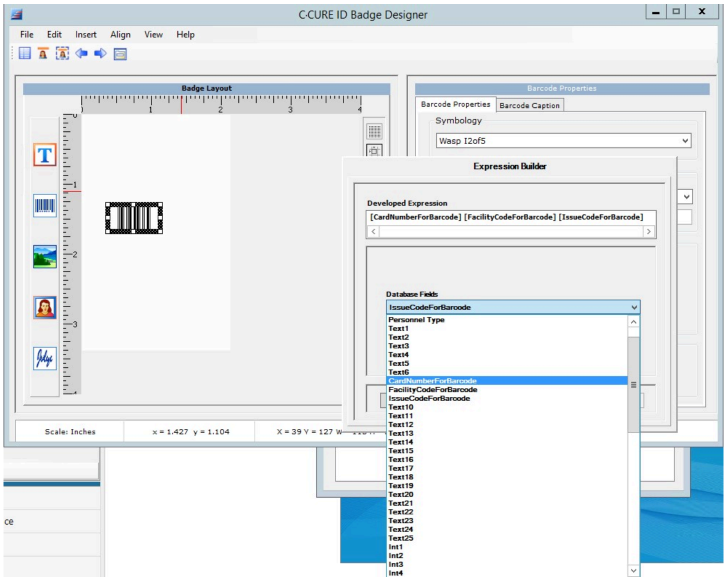
Barcode Parameters

30 Height

100 Magnification %

Scale: Inches | x = 0.094 y = 1.385 | X = 115 Y = 139 W = 115 H = 30 | Test

Figure 38: Expression builder



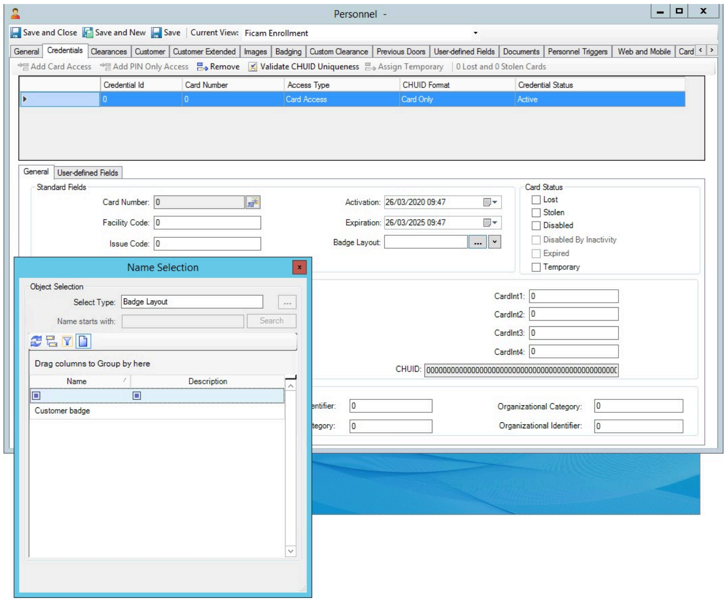
Symbology: Wasp I2of5

Developed Expression: [CardNumberForBarcode] [FacilityCodeForBarcode] [IssueCodeForBarcode]

Database Fields: IssueCodeForBarcode

Personnel Type
Text1
Text2
Text3
Text4
Text5
Text6
CardNumberForBarcode
FacilityCodeForBarcode
IssueCodeForBarcode
Text10
Text11
Text12
Text13
Text14
Text15
Text16
Text17
Text18
Text19
Text20
Text21
Text22
Text23
Text24
Text25
Int1
Int2
Int3
Int4

Figure 39: Credentials tab



Current View: Ficam Enrollment

☑ Validate CHUID Uniqueness

0 Lost and 0 Stolen Cards

Credential Id	Card Number	Access Type	CHUID Format	Credential Status
0	0	Card Access	Card Only	Active

Card Number: 0

Facility Code: 0

Issue Code: 0

Activation: 26/03/2020 09:47

Expiration: 26/03/2025 09:47

Badge Layout:

□ Lost
□ Stolen
□ Disabled
□ Disabled By Inactivity
□ Expired
□ Temporary

CardInt1: 0

CardInt2: 0

CardInt3: 0

CardInt4: 0

CHUID: 000000000000000000000000000000000000000000000000

entifier: 0

tegory: 0

Organizational Category: 0

Organizational Identifier: 0

Select Type: Badge Layout

Name starts with:

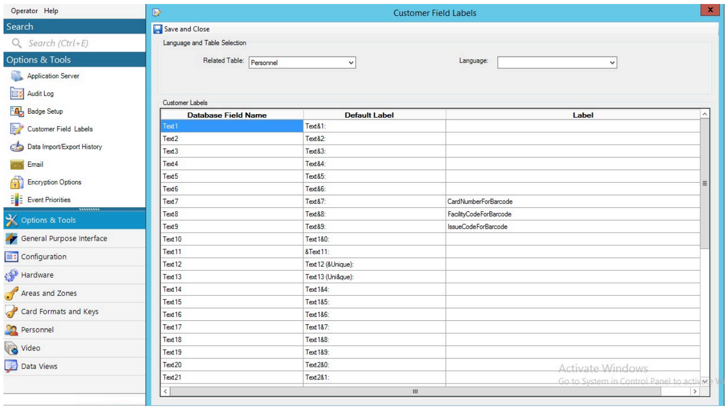
Name	Description
Customer badge	

Renaming custom fields

You need to rename custom fields for identification for mapping, so that you can use the custom field to map the badge layout expression for the barcode. Complete the following steps before completing any of the use cases.

1. In the Administration Workstation, in the **Navigation** pane, click **Options & Tools**.
2. Click **Customer Field Labels**.
3. The following steps are an example of how you can rename the custom fields foridentification. Rename the fields in the best way that works foryou.
   - In the **Label** column, enter `CardNumberForBarcode` beside **Text&7:** to rename **TEXT7**.
   - In the **Label** column, enter `FacilityCodeForBarcode` beside **Text&8:**to rename **TEXT8**.
   - In the **Label** column, enter `IssueCodeForBarcode` beside **Text&9:** to rename **TEXT9**.
4. Click **Save and Close**.

Figure 40: Customer Field Labels



Language and Table Selection

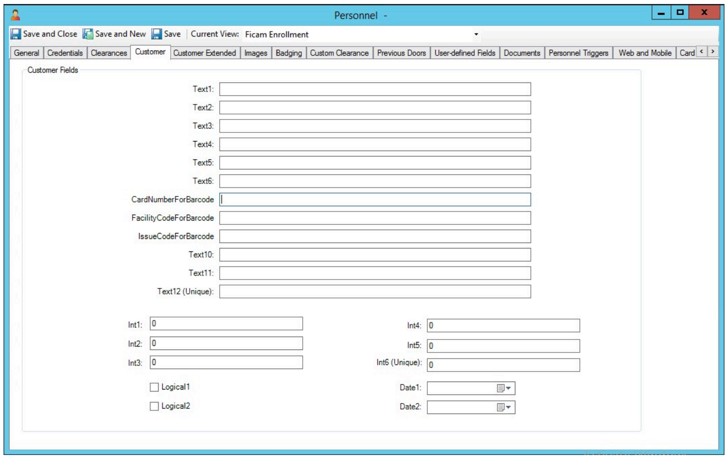
Related Table: Personnel

Language:

Customer Labels

Database Field Name	Default Label	Label
Text1	Text&1:	
Text2	Text&2:	
Text3	Text&3:	
Text4	Text&4:	
Text5	Text&5:	
Text6	Text&6:	
Text7	Text&7:	CardNumberForBarcode
Text8	Text&8:	FacilityCodeForBarcode
Text9	Text&9:	IssueCodeForBarcode
Text10	Text1&0:	
Text11	&Text11:	
Text12	Text12 (&Unique):	
Text13	Text13 (Uni&que):	
Text14	Text1&4:	
Text15	Text1&5:	
Text16	Text1&6:	
Text17	Text1&7:	
Text18	Text1&8:	
Text19	Text1&9:	
Text20	Text2&0:	
Text21	Text2&1:	

Figure 41: Personnel Customer tab



Current View: Ficam Enrollment

Customer Fields

Text1:

Text2:

Text3:

Text4:

Text5:

Text6:

CardNumberForBarcode

FacilityCodeForBarcode

IssueCodeForBarcode

Text10:

Text11:

Text12 (Unique):

Int1:	0	Int4:	0
Int2:	0	Int5:	0
Int3:	0	Int6 (Unique):	0
☐ Logical1		Date1:	
☐ Logical2		Date2:	

Barcode use cases with default processing

Add card number, issue code, and facility code data types with decimal, HEX, or ASCCI encoding with default processing.

For decimal encoding, see Adding card number, issue code, and facility code data types with decimal encoding.

For HEX encoding, see Adding card number, issue code, and facility code data types with HEX encoding.

For ASCCI encoding, see Adding card number, issue code, and facility code data types with ASCII encoding.

Adding card number, issue code, and facility code data types with decimal encoding

1. Right-click the Go Reader object and select **Edit**.
2. Click the **Reader** tab, then select **Use Personnel Record Facility Code**.
3. Click the **Barcode** tab, then select the **Use Data Fields** check box.
4. Click **Add**. Select **Issue Code** for the field type and select **Decimel** for the encoding type. Enter a length issue code, for example, `2`.
5. Click **Add**. Select **Card facility code** for the field type and select **Decimel** for the encoding type. Enter a length for the card facility code, for example, `2`.
6. Click **Add**. Select **Card Number** for the field type and select **Decimel** for the encoding type. Enter a length for the card number, for example, `5`.
7. Click **Save and Close**. The changes synchronize to the Go Reader device.

Adding card number, issue code, and facility code data types with HEX encoding

1. Right-click the Go Reader object and select **Edit**.
2. Click the **Reader** tab, then select **Use Personnel Record Facility Code**.
3. Click the **Barcode** tab, then select the **Use Data Fields** check box.
4. Click **Add**. Select **Issue Code** for the field type and select **HEX** for the encoding type. Enter a length issue code, for example, `1`.
5. Click **Add**. Select **Card facility code** for the field type and select **HEX** for the encoding type. Enter a length for the card facility code, for example, `2`.
6. Click **Add**. Select **Card Number** for the field type and select **HEX** for the encoding type. Enter a length for the card number, for example, `4`.
7. Click **Save and Close**. The changes synchronize to the Go Reader device.

Adding card number, issue code, and facility code data types with ASCII encoding

1. Right-click the Go Reader object and select **Edit**.
2. Click the **Reader** tab, then select **Use Personnel Record Facility Code**.
3. Click the **Barcode** tab, then select the **Use Data Fields** check box.
4. Click **Add**. Select **Issue Code** for the field type and select **ASCII** for the encoding type. Enter a length issue code for example, `2`.
5. Click **Add**. Select **Card facility code** for the field type and select **ASCII** for the encoding type. Enter a length for the card facility code for example, `2`.
6. Click **Add**. Select **Card Number** for the field type and select **ASCII** for the encoding type. Enter a length for the card number.
7. Click **Save and Close**. The changes synchronize to the Go Reader device.

Creating a badge layout for a barcode

1. In the **Navigation** pane, click **Personnel**.
2. From the **Personnel** pane list, select **Badge Layout** and then click **New**.
3. In the **Name** field, enter a name.
4. Click **Launch C•CURE ID Badge Designer**.
5. Click and drag the barcode icon onto the badge layout.
6. To open **Expression Builder**, from **Barcode Properties**, click **Expr**.
7. From the **Database Fields** list, select the custom field to be the placeholder for the card number you create in Renaming custom fields, for example: `CardNumberForBarcode`. Click **Add**.
8. Select the custom field that is the placeholder for the facility code that you create in Renaming custom fields, for example: `FacilityCodeForBarcode`. Click **Add**.
9. Select the custom field that is the placeholder for the issue code that you create in Renaming custom fields, for example: `IssueCodeForBarcode`. Click **Add**.
10. Click **OK**.
11. Exit the **C•CURE ID Badge Designer**, then click **Save and Close** to save the badge layout.

Creating a personnel record for a barcode

1. In the **Navigation** pane, click **Personnel**.
2. From the list, select **Personnel** and then click **New**.
3. On the **Credentials** tab, add credentials in the **Card Number**, **Issue Code** and **Facility Code** fields. For example: **Card Number**: `10434`, **Facility Code**: `10`, **Issue Code**: `2`.
4. Click the ellipsis beside **Badge Layout**. Select the badge layout for this personnel record.

5. Navigate to **Customer** tab and enter values in decimal in the Card Number, Issue code and Facility code fields.
6. On the **Clearances** tab, add a clearance to the personnel record, then click **Save and Close**. The changes synchronize to the Go Reader device.
7. Open the Go Reader Driver application and then the Go Reader application on your device.
8. Click **Swipe and Show**.
9. On the **Badging** tab of the Personnel editor in the C•CURE Administration Station, click **Preview Badge**.
10. Scan the barcode from the device by using the **Swipe and Show** screen of the Go Reader application. The card admit message displays on the Go Reader device and on the C•CURE Monitoring Station.

Barcode use cases with custom processing

Add card number, issue code, and facility code data types with a combination of decimal, HEX, or ASCCI encoding with custom processing. You can then create a badge layout for a barcode and create a personnel record.

For more information on configuring the card number, facility code, or issue code from extracted data, see Configuring the card number, facility code, and issue code from extracted data.

For more information on creating a personnel record with custom processing, see Creating a personnel record with custom processing.

Configuring the card number, facility code, and issue code from extracted data

Before you begin:
You must add custom processing. For more information, see Adding a new custom process.

You can configure all or any combination of the following data fields from extracted barcode data:

- Card number
- Facility code
- Issue code

ⓘ **Note:** This procedure uses the following extracted processing data as an example: `1d-4088-8a18-19`.

1. In the **Navigation** pane, from **Options & Tools**, select **Personnel**.
2. Right-click the Go Reader object and select **Edit**.
3. On the **Reader** tab, select **Use Personnel Record Facility Code**.
4. On the **Barcode** tab, in **Data Fields**, select the **Use Data Fields** check box.
5. **Optional:** To add an issue code, in **Data Fields**, complete the following steps:
   a. Click **Add**, and from the **Field Type** list, select **Issue Code**.
   b. In **Issue Code**, enter `1d`. This value refers to the extracted processing data example.
   c. In **Length**, enter `2`.
   d. From the **Encoding Type** list, select **HEX**.
6. **Optional:** To add a facility code, in **Data Fields**, complete the following steps:
   a. Click **Add** and from the **Field Type** list, select **Facility Code**.
   b. In **Facility Code**, enter `4088`. This value refers to the extracted processing data example.
   c. In **Length**, enter `4`.
   d. From the **Encoding Type** list, select **Decimal**.
7. **Optional:** To add a card number, in **Data Fields**, complete the following steps:
   a. Click **Add** and from the **Field Type** list, select **Card Number**.
   b. In **Facility Code**, enter `88a1819`. This value refers to the extracted processing data example.
   c. In **Length**, enter `7`.
   d. From the **Encoding Type** list, select **Hex**.
8. Click **Save and Close**. The changes synchronize to the Go Reader device.

Creating a personnel record with custom processing

ⓘ **Note:** This procedure uses the following extracted processing data as an example: `1d-4088-8a18-19`.

1. In the **Navigation** pane, click **Personnel**.
2. Select **Personnel** and then click **New**.
3. Go to the **Credentials** tab.
4. On the **General** tab, in **Standard Fields**, add credentials in the following fields, depending on the data fields you add in Configuring the card number, facility code, and issue code from extracted data. For example, you can add all or any combination of the following:
    - **Optional:** In **Card Number**, enter `143267865` in decimal.
    - **Optional:** In **Facility Code**, enter `408`.
    - **Optional:** In **Issue Code**, enter `29` in decimal.
5. On the **Customer** tab, use the **Custom Label Field editor** to label the custom fields as Card Number, Facility Code, and Issue Code, depending on the data fields you add in Configuring the card number, facility code, and issue code from extracted data.
6. In the new custom fields, enter the card number, facility code, and issue code values from the extracted data, depending on the data fields you add in Configuring the card number, facility code, and issue code from extracted data. For example, you can add all orany combination of the following:
    - **Optional:** In **Card Number**, enter `88a1819` in HEX
    - **Optional:** In **FacilityCode**, enter `4088`.
    - **Optional:** In **Issue Code**, enter `1d`.
7. On the **Clearances** tab, add a clearance to the personnel record, then click **Save and Close**. The changes synchronize to the Go Reader device.
8. Open the Go Reader Driver application and then open the Go Reader application on your device.
9. Click **Swipe and Show**.
10. In the C•CURE Administration Workstation, in the **Personnel** editor, on the **Badging** tab, click **Preview Badge**.
11. In the Go Reader application, go to the **Swipe and Show** tab and then scan the barcode with the device.

The card admit message displays on the Go Reader device and on the C•CURE Monitoring Station.

Go Reader Check Point tab

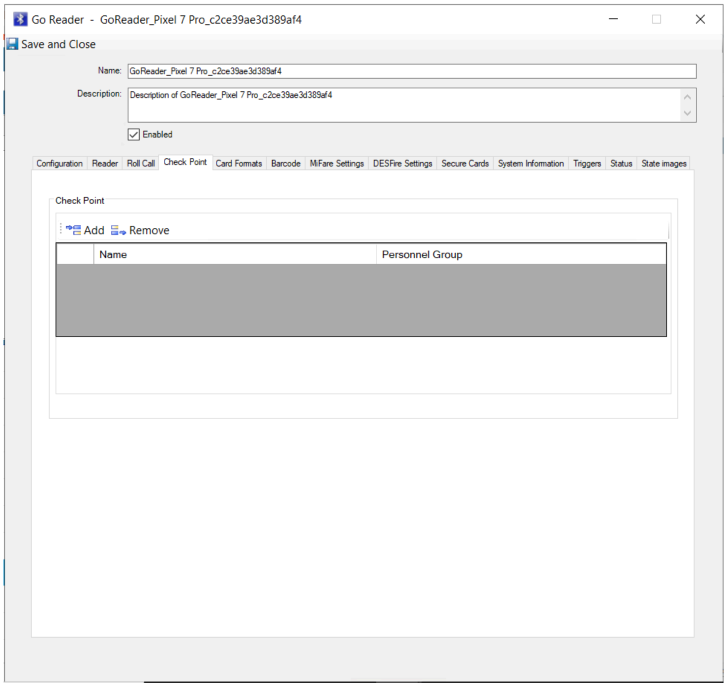
Use the Check Point tab to add or remove check points and assign them to personnel groups for the Go Reader.

Table 21 describes the settings in the Check Point tab.

Table 21: Check Point tab

Field/Button	Description
Check Point	Add or remove checkpoints and assign them to personnel groups. These checkpoints appears on the Go Reader device along with those created directly from the Go Reader app.

Figure 42: Check Point tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

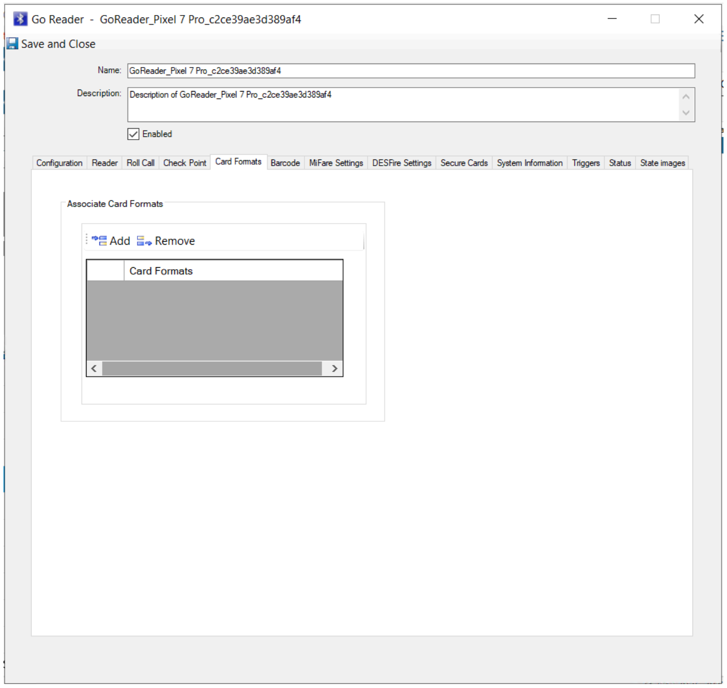
Go Reader Card Formats tab

Use the Card Formats tab to add or remove card formats to the Go Reader.Table 22 describes the settings in the Card Formats tab.

Table 22: Card Formats tab

Field/Button	Description
Associate Card Formats	Add or remove card formats to associate with the Go Reader device.

Figure 43: Card Formats tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

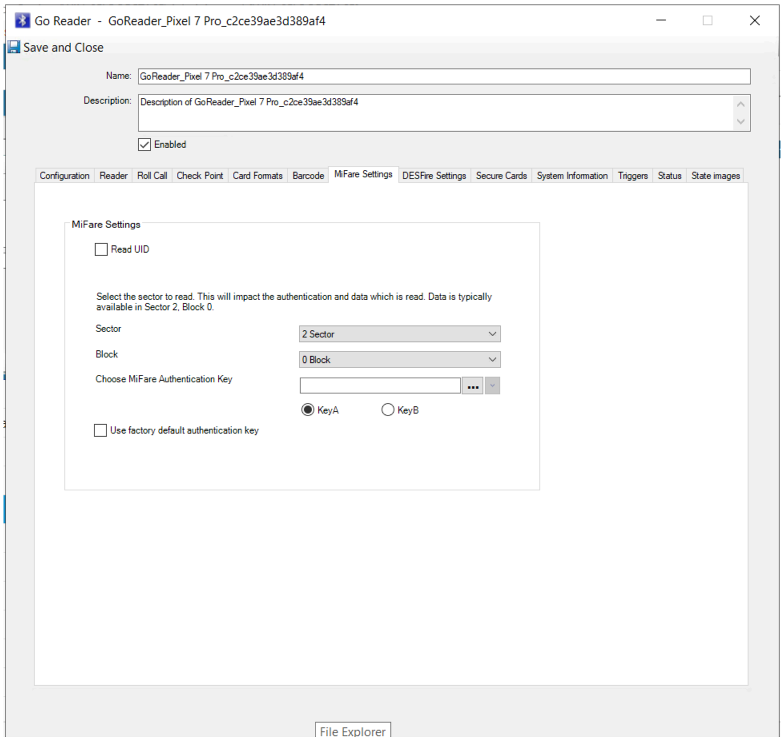
Go Reader MiFare Settings tab

Use the MiFare Settings tab to configure the Go Reader to read MiFare cards. The device can read a MiFare card either by retrieving its UID or by accessing data stored in a specific sector. Table 23 provides details of the settings available in the MiFare Settings tab.

Table 23: MiFare Settings tab

Field/Button	Description
Read UID	Enables the Go Reader to read the UID (Unique Identifier) of the MiFare card. Activating this option disables all other settings in this tab.
Sector	Select the sector of the MiFare card from which the data will be read.
Block	Select the block of the MiFare card sector from which the data will be read.
Choose MiFare Authentication Key	Select the authentication key used to verify access to the card's sector, ensuring the reader has the correct credentials.
KeyA/KeyB	Select the type of authentication key to be used—either Key A or Key B.
Use factory default authentication key	Select this option to use the factory default authentication key.

Figure 44: MiFare Settings tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

MiFare Settings

☐ Read UID

Select the sector to read. This will impact the authentication and data which is read. Data is typically available in Sector 2, Block 0.

Sector: 2 Sector

Block: 0 Block

Choose MiFare Authentication Key: ● KeyA ○ KeyB

☐ Use factory default authentication key

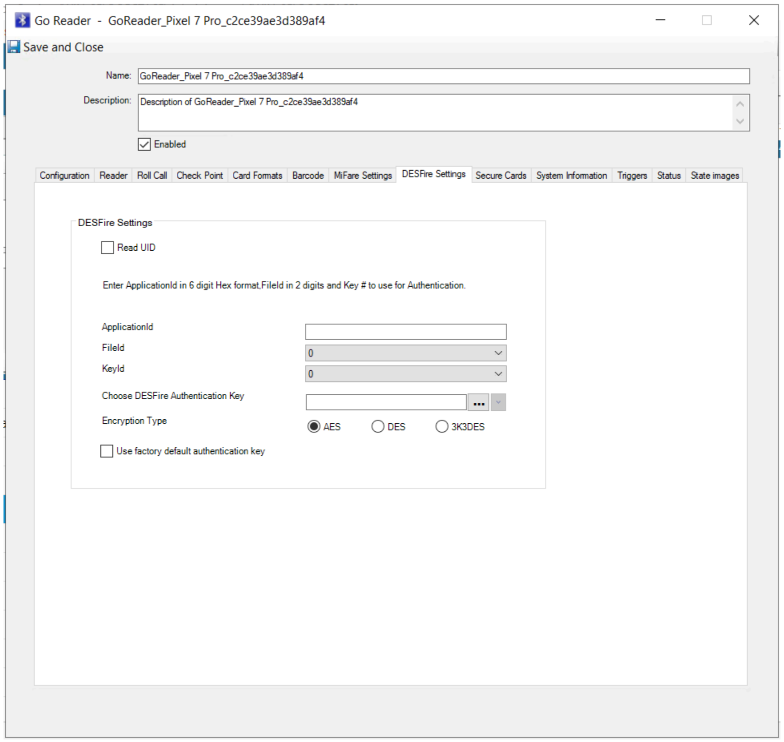
Go Reader DesFire Settings tab

Use the DesFire Settings tab to configure the Go Reader to read DesFire cards. The DesFire card can be read either by retrieving its UID or by accessing data stored in a specific application. Table 24 describes the settings in the DesFire Settings tab.

Table 24: DesFire Settings tab

Field/Button	Description
Read UID	Enables the Go Reader to read the UID (Unique Identifier) of the DesFire card. Activating this option disables all other settings in this tab.
Application ID	Select the application ID from which the data will be read on the DesFire card.
Field ID	Specifies the field ID within the selected application from which the data will be read.
Key ID	Select the key ID used for authentication with the DesFire card.
Choose DesFire Authentication Key	Select the authentication key used to verify access to a specific application on the card.
Encryption Type	Specifies the type of encryption key to be used—AES, DES, or 3K3DES.
Use factory default authentication key	Enables the use of the factory default authentication key for accessing the DesFire card.

Figure 45: DesFire Settings tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

DESFire Settings

□ Read UID

Enter ApplicationId in 6 digit Hex format,FileId in 2 digits and Key # to use for Authentication.

ApplicationId

FileId 0

KeyId 0

Choose DESFire Authentication Key

Encryption Type ● AES ○ DES ○ 3K3DES

□ Use factory default authentication key

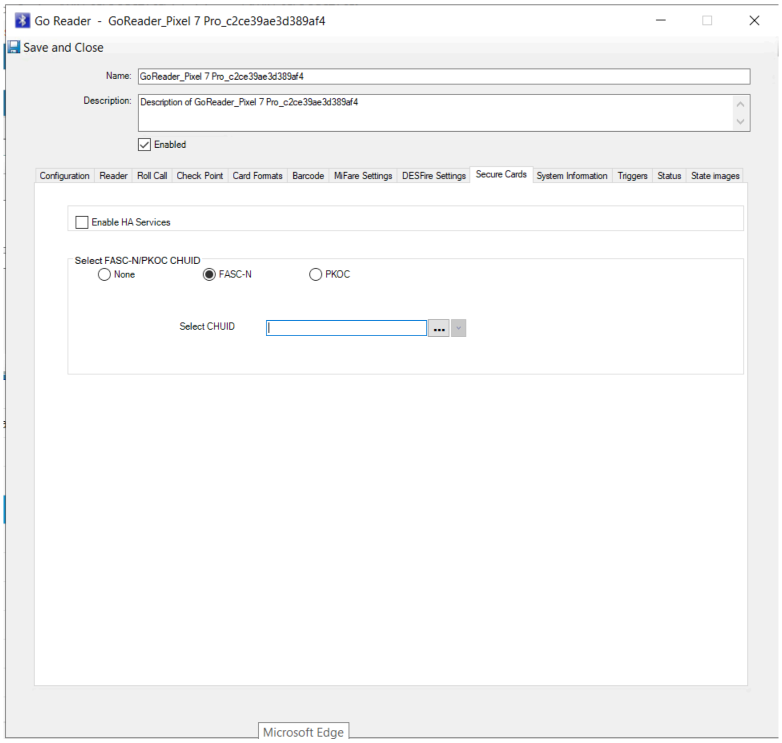
Go Reader Secure Cards tab

Use the Secure Cards tab to configure the Go Reader to read FASC-N/PKOC cards. Any modifications made in this tab will trigger a synchronization once the user clicks the **Save and Close** button. Table 25 describes the settings in the Secure Cards tab.

Table 25: DesFire Settings tab

Field/Button	Description
None	This is the default selection. Use this option when neither FASC-N nor PKOC cards are being used.
FASC-N	Select this option to configure the Go Reader to read FASC-N cards.
PKOC	Select this option to configure the Go Reader to read PKOC cards.
Select CHUID	Select the CHUID (Credential Holder Unique Identifier) associated with either FASC-N or PKOC. Personnel with matching credentials will be synced to the reader.

Figure 46: Secure Cards tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

□ Enable HA Services

Select FASC-N/PKOC CHUID

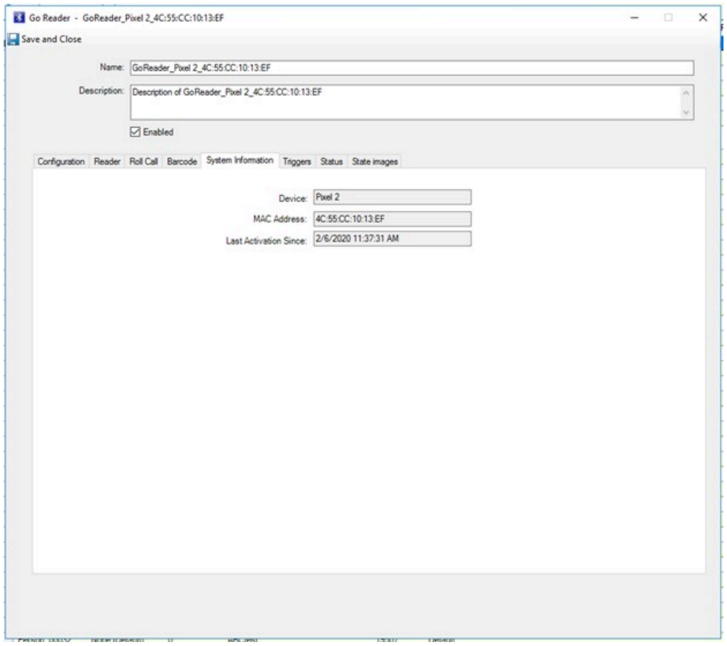
○ None ● FASC-N ○ PKOC

Select CHUID

Go Reader System Information tab

Use the **System Information** tab to view information about the Go Reader device. The fields in the **Configuration** tab are read-only. Table 26 describes the fields in the System Information tab.

Figure 47: Go Reader System Information tab



Go Reader - GoReader_Pixel 2_4C:55:CC:10:13:EF

Name: GoReader_Pixel 2_4C:55:CC:10:13:EF

Description: Description of GoReader_Pixel 2_4C:55:CC:10:13:EF

☑ Enabled

Device: Pixel 2

MAC Address: 4C:55:CC:10:13:EF

Last Activation Since: 2/6/2020 11:37:31 AM

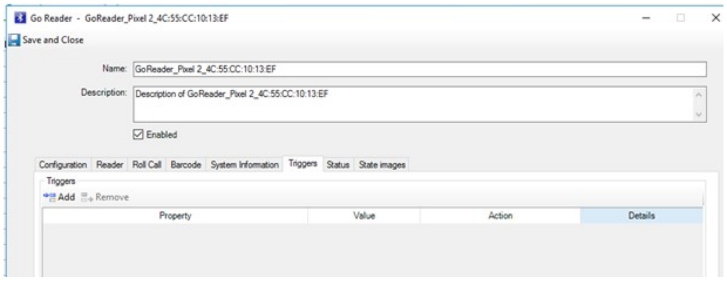
Table 26: System Information tab

Field	Description
Device	The name of the associated device.
MAC Address	Unique identifier of Go Reader hardware.
Last Activation Since	Last activation time of the reader from C•CURE 9000. For more information, see Activating the Go Reader.

Go Reader Triggers tab

Use the Go Reader Triggers tab to configure triggers and events related to the C•CURE Go Reader device. The Go Reader Triggers tab uses events to trigger actions from the C•CURE Go Reader. Table 27 describes the fields in the Triggers tab.

Figure 48: Go Reader Triggers tab



Go Reader - GoReader_Pixel 2_4C:55:CC:10:13:EF

Save and Close

Name: GoReader_Pixel 2_4C:55:CC:10:13:EF

Description: Description of GoReader_Pixel 2_4C:55:CC:10:13:EF

☑ Enabled

Property	Value	Action	Details

Table 27: Go Reader Triggers tab fields and descriptions

Field	Options	Description
Property	Reader Activation State	Sets Activation State of the Go Reader as the trigger property.
	Synchronization Status	Sets Synchronization Status of the Go Reader as the trigger property.
	Admit Status	Sets Admit Status of the Go Reader as the trigger property.
	Online Status	Sets Online Status of the Go Reader as the trigger property.

Table 27: Go Reader Triggers tab fields and descriptions

Field	Options	Description
Value	Activated	Sets trigger value to Activated.
	Not Activated	Sets trigger value to Not Activated.
	Synchronization Initiated	Sets trigger value to Synchronization Initiated.
	Synchronizing	Sets trigger value to Synchronizing.
	Finished Synchronization	Sets trigger value to Finished Synchronization.
	Synchronization Pending	Sets trigger value to Synchronization Pending.
	Synchronization Canceled	Sets trigger value to Synchronization Cancelled.
	Admit	Sets trigger value to Admit.
	Reject	Sets trigger value to Reject.
	Noticed Admit	Sets trigger value to Noticed Admit when the Noticed check box is selected in the Personnel editor. For more information on the Noticed checkbox, refer to the *Personnel General Tab* chapter in the *C•CURE Personnel Configuration Guide.*
	Noticed Reject	Sets trigger value to Noticed Reject when the Noticed check box is selected in the Personnel editor.
Action	Activate Event	Selects Activate Event as the action.
Event	Select an event that is activated. Table 28 describes the available C•CURE 9000 Events.	

Table 28: C•CURE Events and descriptions

Event	Description
Assistance Request Journal Trigger Event	When an operator clicks the Assist button this trigger activates the Assistance Request Journal Trigger Event. For more information on the Assist button, refer to the *Personnel* chapter in the *C•CURE 9000 Personnel Guide*.
Audit Log Backup Event	When an Audit Log Backup Message is logged, this trigger activates the Audit Log Backup Event.
Battery Low Journal Trigger Event	When a Battery Low Journal Message is logged, this trigger activates the System Error Journal Event.
Device Error Journal Trigger Event	When a Device Error Journal Message is logged, this trigger activates the Device Error Journal Event.
Intrusion Zone Error Journal Trigger Event	When an Intrusion Zone Error Journal Message is logged, this trigger activates the System Error Journal Event.
Journal Log Backup Event	When a Journal Log Backup is logged, this triggeractivates the Journal Log Backup event.
Remove Report Results	Selects Report Result object in the database and deletes these report results permanently. Conditions include both setting the **Delete automatically** flag to true. The date value in **Delete after** is in the past.
System Error Journal Triggers Event	When a System Error Journal Message is logged, this trigger activates the System Error Journal Event.

Table 28: C•CURE Events and descriptions

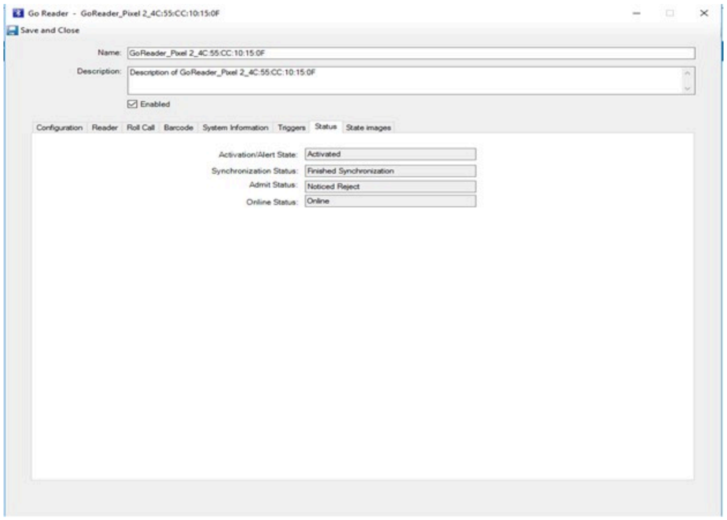
Event	Description
Watchlist Assistance Request Trigger Event	When an operator clicks the Assist button while working with a person who is on the watchlist, this trigger activates the Watchlist Assistance Request Trigger Event. For more information on the Assist button, refer to the *Personnel* chapter in the *C•CURE 9000 Personnel Guide*.
Watchlist Check-in Journal Trigger Event	When a visitor from the watchlist has been checked in for a visitor, this trigger activates the watchlist Check-in Journal Trigger Event. For more information on the watchlist, refer to the *Personnel* chapter in the *C•CURE 9000 Personnel Guide*.
Watchlist Visitor Scheduled Trigger Event	When a visitor from the watchlist is appended to a visit registered in the system, the Watchlist Visitor Schedule Audit Trigger activates the Watchlist Visitor Scheduled Trigger Event. For more information on the watchlist, refer to the *Personnel* chapter in the *C•CURE 9000 Personnel Guide*.

To assign triggers and events to the C•CURE Go Reader device, see Configuring triggers and events.

Go Reader Status tab

Use the Go Reader Status tab to view the Go Reader's activation state, synchronization status, card admit status, and online status in the C•CURE 9000 system.

Figure 49: Go Reader Status tab



Name: GoReader_Pixel 2_4C:55:CC:10:15:0F

Description: Description of GoReader_Pixel 2_4C:55:CC:10:15:0F

☑ Enabled

Activation/Alert State: Activated

Synchronization Status: Finished Synchronization

Admit Status: Noticed Reject

Online Status: Online

Table 29: Go Reader Status tab field and status properties

Field	Property	Description
Activation State	Unknown	The Go Reader is not recognized in C•CURE 9000.
	Activate	The Go Reader is activated in C•CURE 9000.
	Not Activated	The Go Reader has been de-activated in C•CURE 9000.

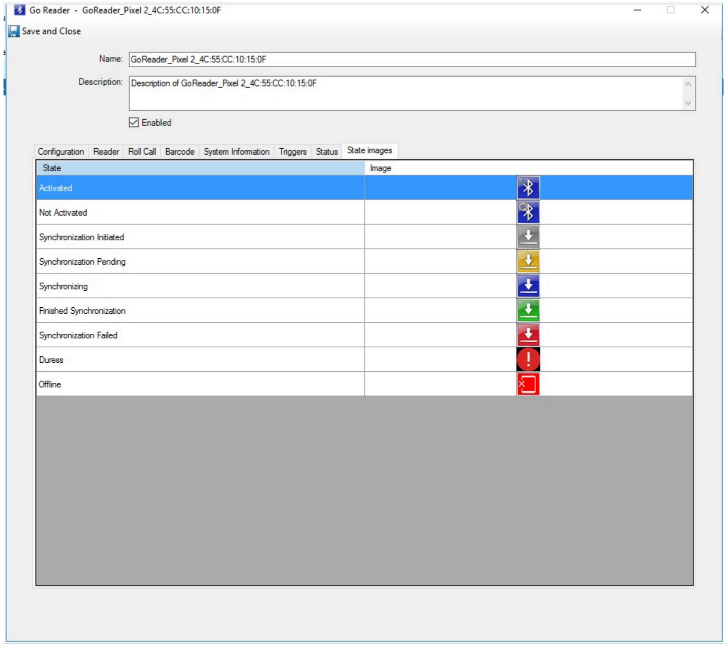
Table 29: Go Reader Status tab field and status properties

Field	Property	Description
Synchronization Status	Unknown	Go Reader Synchronization is not yet initiated.
	Synchronization Initiated	Go Reader Synchronization is initiated from C•CURE 9000.
	Synchronizing	The Go Reader app is synchronizing with data from C•CURE 9000 database.
	Finished Synchronization	The Go Reader app has finished synchronization.
	Synchronization Failed	The Go Reader app synchronization has failed.
	Synchronization Pending	The C•CURE 9000 database is waiting for the Go Reader app to initiate download.
Admit Status	Admit	When a card is swiped, the Admit event is triggered in the Go Reader app.
	Reject	When a card is swiped, the Reject event is triggered in the Go Reader app.
	Noticed Admit	When a card is swiped, the Noticed Admit event is triggered in the Go Reader app.
	Noticed Reject	When a card is swiped, the Noticed Reject event is triggered in the Go Reader app.
Online Status	Offline	The Go Reader device is offline.
	Online	The Go Reader device is online.

Go Reader State Images tab

The Go Reader State Images tab lists icons displayed in the Monitoring Station. A full description of the Go Reader state images and corresponding states is listed in Table 30.

Figure 50: Go Reader State images tab



Name: GoReader_Pixel 2_4C:55:CC:10:15:0F

Description: Description of GoReader_Pixel 2_4C:55:CC:10:15:0F

☑ Enabled

State	Image
Activated	ᛒ
Not Activated	ᛒ
Synchronization Initiated	⬇
Synchronization Pending	⬇
Synchronizing	⬇
Finished Synchronization	⬇
Synchronization Failed	⬇
Duress	!
Offline	×

Table 30: State Images

State Image	Name	Description
ᛒ	Activated	C•CURE 9000 has activated the Go Reader app.
ᛒ	Not activated	C•CURE 9000 has not activated the Go Reader app.
⬇	Synchronization initiated	Synchronization is initiated between C•CURE 9000 and the Go Reader app.
⬇	Synchronization pending	The C•CURE 9000 database is waiting for the Go Reader app to initiate download.
⬇	Synchronizing	The Go Reader app is synchronizing data from C•CURE 9000 database.
⬇	Finished synchronization	The Go Reader app has completed synchronizing data from the C•CURE 9000 database.
⬇	Synchronizing failed	Synchronization has failed.
!	Duress	A duress event is active.
×	Offline	The Go Reader device is offline.

Configuring card formats using the Go Reader editor

You can configure, manage, and assign card formats for rfIdeas Nano USB readers and Inbuilt NFC readers from the Administration Station. This is useful if you have one or more Go Reader devices as you can assign the card formats to all your Go Reader devices. You must create card formats in the Administration Station before assigning them to a Go Reader device. For more information on card formats, refer to the *C•CURE Card Formats and Smart Card Keys Guide*.

ⓘ **Note:** For Access-ER devices, card formats must be created on the device. For more information, see Adding custom format cards on Access-ER.

1. In the Go Reader editor, click on the **Card Formats** tab.
2. In the **Associate Card Formats** section, choose between the following options:
   - Click **Add** to assign a card format to the Go Reader device.
   - Click **Remove** to remove a card format from the Go Reader device.
3. **Optional**: Click the **Menu** icon next to a card format to edit the parameters of the card format.
4. Click **Save and Close** to confirm the changes.

   A notification stating `Card format updates received appears` on the Go Reader device.

Configuring MIFARE card formats using the Go Reader editor

You can create, manage, and assign MIFARE card formats for rfIdeas Nano USB readers and Inbuilt NFC readers from the Administration Station. You must create card formats in the Administration Station before assigning them to a Go Reader device. For more information on card formats, refer to the *C•CURE Card Formats and Smart Card Keys Guide*.

ⓘ **Note:** For Access-ER devices, card formats must be created on the device. For more information, see Adding custom format cards on Access-ER.

1. In the Go Reader editor, click on the **MiFare Settings** tab.
2. **Optional:** To read the serial number of MIFARE cards, select the **Read UID** check box.
3. Use the **Sector** list to choose the sector details.
4. Use the **Block** list to choose the block details.
5. In the **Choose MiFare Authentication Key** field, use the **Menu** icon to choose the authentication key.

   ⓘ **Note:** You must configure smart card keys before assigning them to a Go Reader device. For more information, refer to the *C•CURE Card Formats and Smart Card Keys Guide*.
6. **Optional**: If you are using the default factory authentication key, select the **Use factory default authentication key** check box.
7. Click **Save and Close** to confirm the changes.

A notification stating `MiFare server updates received` displays on the Go Reader device.

To check the MIFARE settings on the Go Reader app, on your Go Reader device, navigate to **Settings** > **NFC**, then expand **MiFare Settings**.

Configuring DESFire card formats using the Go Reader editor

Before you begin:
You must verify the Application Id before completing the following steps. For more information, see Reading the Application Id of DESFire cards.

You can create, manage, and assign DESFire card formats for rfIdeas Nano USB readers and Inbuilt NFC readers from the Administration Station.

You must create card formats in the Administration Station before assigning them to a Go Reader device. For more information on card formats, refer to the *C•CURE Card Formats and Smart Card Keys Guide*.

ⓘ **Note:** For Access-ER devices, card formats must be created on the device. For more information, see Adding custom format cards on Access-ER.

1. In the Go Reader editor, click the **DESFire Settings** tab.
2. **Optional**: To read the serial number of DESFire cards, select the **Read UID** check box.
3. In the **Application Id**, **File Id**, and **Key Id** fields, enter the data values used to program DESFire cards.

   ⓘ **Note:** The default value for the **Reader Key Slot Id** is 240 and the default value for **Card Key Number** is 1. It is best practice to use the default values.

4. In the **Choose MiFare Authentication Key** field, use the **Menu** icon to choose the authentication key.
5. In the **Encryption Type** section, choose between:
   - AES (Advanced Encryption Standard)
   - DES (Data Encryption Standard)
   - 3K3DES (Triple Data Encryption Standard)
6. **Optional**: If you are using the default factory authentication key, select the **Use factory default authentication key** check box.
7. Click **Save and Close** to confirm the changes.

A notification stating `DESFire server updates received` displays on the Go Reader device.

To check the DESFire settings on the Go Reader app, on your Go Reader device, navigate to **Settings** > **NFC**, and expand **Desfire Settings**.

Configuring MagTek card formats on the Go Reader editor

Before you begin:
You can create, manage, and assign MagTek card formats for MagTek iDynamo USB-C readers from the Administration Station. You must create card formats in the Administration Station before assigning them to a Go Reader device. For more information on card formats, refer to the *C•CURE Card Formats and Smart Card Keys Guide*.

1. In the Go Reader editor, click on the **MagTek Settings** tab.
2. **Optional**: To read the serial number of MagTek cards, select the **Read UID** check box.
3. To read custom magnetic stripe cards, from the **Set the track for the reader to read the card information** list, select the track number.
4. In the **Associate Card Formats** section, choose from the following options:
   - Click **Add** to assign a card format to the Go Reader device.
   - Click **Remove** to remove a card format from the Go Reader device.
5. Click **Save and Close** to confirm the changes.

A notification stating `MagTek server updates received` displays on the Go Reader device.

To check the MagTek card format settings on the Go Reader app, navigate to **Settings** > **MagTek**.

Go Reader editor tasks

Use the Go Reader editor to complete the following tasks:

- Accessing the Go Reader editor
- Activating the Go Reader
- Disabling the Go Reader
- View GIS location in card swipe journal message
- Activating facility code validation

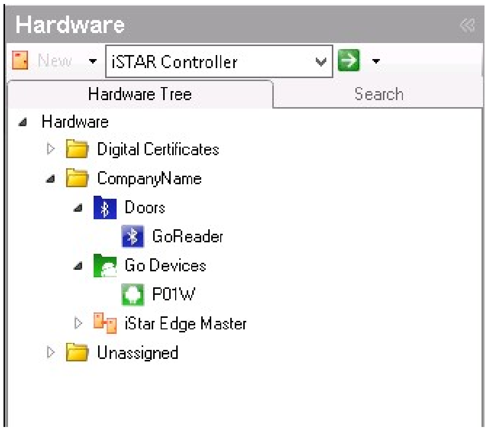
- Use custom data fields for swipe and roll call
- Impersonating a door
- Using manual mustering with the roll call screen
- Activating timed anti-passback
- Assigning a missing area
- Configuring triggers and events
- Removing triggers and events

Accessing the Go Reader editor

Access the Go Reader editor from the **Hardware Tree** in the C•CURE Administration Station.

1. In the **Navigation** pane, click **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand **Doors**.
4. Choose between the following options:
   - Right-click the **GoReader** and select **Edit**.
   - Double-click the **GoReader**.

Figure 51: Accessing the Go Reader editor



Activating the Go Reader

To activate the Go Reader, you must first add it in C•CURE 9000.

1. In the **Navigation** pane, click **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand the **Doors** folder.
4. Choose between the following options:
   - Right-click the **GoReader** and select **Edit**.
   - Double-click the **GoReader**.
5. Select the **Enabled** check box.
6. Click **Save and Close**.

Disabling the Go Reader

Use the Go Reader editor to disable the Go Reader from C•CURE 9000.

1. In the **Navigation** pane, select **Hardware**.
2. Expand the **CompanyName** folder.

3. Expand the **Doors** folder.
4. Choose from the following options:
   - Right-click the **GoReader** and select **Edit** from the context menu.
   - Double-click the **GoReader**.
5. Clear the **Enabled** check box.
6. Click **Save and Close**.

Activating check point

Activate check point using the Go Reader editor to create check points and manage a list of swiped in personnel.

1. On the **Configuration** tab of the Go Reader editor, select the **Check Point** check box to activate or disable check point mode.
2. Click **Save and Close**. A notification is sent to the Go Reader device.

View GIS location in card swipe journal message

Use the Configuration tab in the Go Reader editor to activate capturing location details with all swipe activities. You can include the GIS location in the card swipe journal message and view the swipe location in the journal.

Activating GIS location

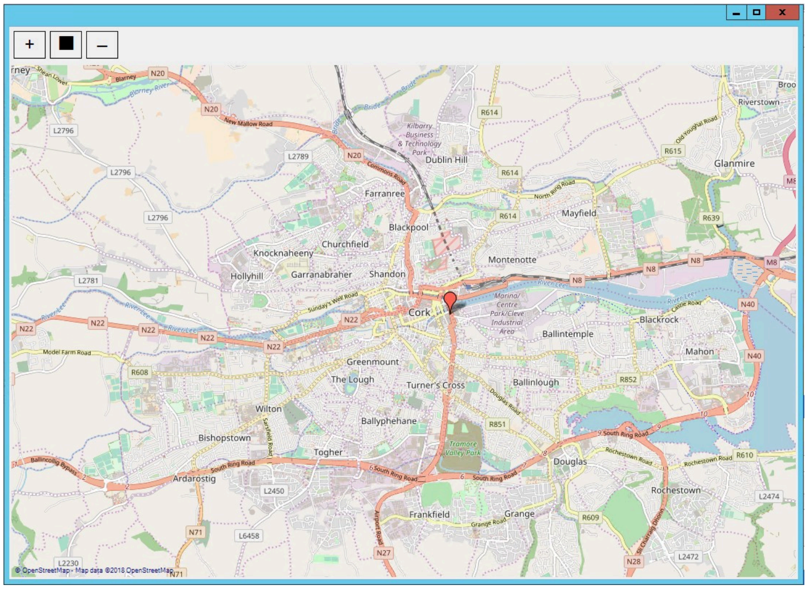
1. In the **Navigation** pane, click **Hardware**.
2. Expand the **CompanyName** folder.
3. Right-click the Go Reader that you want to configure and click **Edit**.
4. Click the **Configuration** tab.
5. In the **Location** section, select the **Include GIS location in Card Swipe Journal message** check box to include the GIS location in the journal message for all swipes.
6. Click **Save and Close**.

Viewing GIS location

You can view the GIS location from personnel card swipes using a journal query.

1. In the Monitoring Station, right-click on the Card Admitted journal message for a person and select **Find in Journal** from the context menu.
2. Edit the filter type and value for the query and click **Run**.
3. In the Journal dynamic view, right-click on a column heading to display a context menu. Click **More columns**.
4. From the list of Journal columns, select **Location** and click **OK**. A **Location** column displays in the dynamic view that shows coordinate details for card swipes.
5. Right-click on journal message and select **Show Location On Map**. A map displays showing the location of the card swipe, as shown in Figure 52.

Figure 52: Swipe location map



Activating facility code validation

Use the Reader tab in the Go Reader editor to activate and disable facility code validation in the Go Reader. After activating Facility Code validation, the Go Reader uses the Facility Code as part of the card format when validating a card swipe. For more information about the facility code validation settings, see Go Reader Reader tab.

Before activating facility code validation, ensure that you have configured the Serialio idChamp RS3 reader to process the Facility Code when a card is swiped. For more information see Configure card formats in the Serialio idChamp RS3 reader.

1. Navigate to the Go Reader that you want to activate facility code validation for.
2. Select the required facility code validation check box:
   - **Use Personnel Record Facility Code**
   - **Use Approved Facility Code.**
3. Click **Save and Close**.

Disabling facility code validation

- To disable Facility Code validation, select the **No Facility Code** check box in the Go Reader editor Reader tab.

Use custom data fields for swipe and roll call

Use the **Additional Swipe Screen Information** fields to add extra details during card swipe and roll call. You can use a maximum of three fields from the following three:

- Custom fields
- Personnel types and options
- Credential activation and deactivation

Adding a custom data field for swipe and roll call

Use the **Additional Swipe Screen Information** fields to add extra details during card swipe and roll call. You can use a maximum of three fields from the following three:

- Custom fields
- Personnel types and options

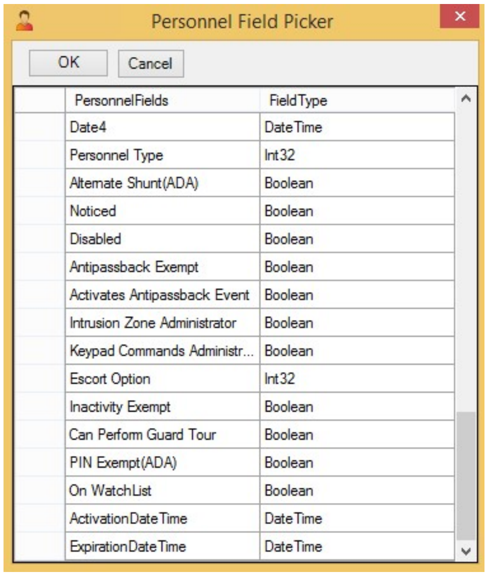
- Credential activation and deactivation

1. Navigate to the Go Reader that you want to add custom fields to. Click the **Reader** tab.
2. In the **Additional Swipe Screen Information** fields, click **Select**. The **Personnel Field Picker** displays, as shown in Figure 41.
3. Click a field from the **Personnel Field Picker** and then click **OK**. The chosen field displays under**Additional Swipe Screen Information**.
4. Click **Save and Close**. A notification is sent to the Go Reader device and synchronization is initiated and completed with the changes.

   When the changes are synchronized to the Go Reader device, the chosen custom data fields display in the Go Reader app for each person when they swipe their card.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you make the changes for **Additional Swipe Screen Information**, the changes are sent when the device comes online, connects to the server, and synchronization is initiated.

Figure 53: Personnel Field Picker



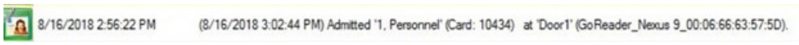
PersonnelFields	FieldType
Date4	DateTime
Personnel Type	Int32
Alternate Shunt(ADA)	Boolean
Noticed	Boolean
Disabled	Boolean
Antipassback Exempt	Boolean
Activates Antipassback Event	Boolean
Intrusion Zone Administrator	Boolean
Keypad Commands Administr...	Boolean
Escort Option	Int32
Inactivity Exempt	Boolean
Can Perform Guard Tour	Boolean
PIN Exempt(ADA)	Boolean
On WatchList	Boolean
ActivationDateTime	DateTime
ExpirationDateTime	DateTime

Impersonating a door

Use the Reader tab in the Go Reader editor to activate **Door Impersonation Mode** to impersonate a particular door if there are issues with that door. It can also be used to access different clearance sets. When you choose a door, all the existing clearances assigned to the Go Reader door are nullified and the clearance and schedule of the impersonated door are downloaded. **When Door Impersonation Mode** is removed, a full download of the Go Reader door is initiated.

1. Select the **Door Impersonation Mode** check box to activate **Door Impersonation Mode**.
2. Click ... and select a door to impersonate.
3. Click **Save and Close**.

   A notification displays on the Go Reader app and the reader name changes to the name of the impersonated door. When a person swipes a card and is admitted or rejected, a journal message with the name of the impersonated door and the name of the GoReader device is displayed on the Monitoring station instead of the Go Reader door name.



8/16/2018 2:56:22 PM (8/16/2018 3:02:44 PM) Admitted '1, Personnel' (Card: 10434) at 'Door1' (GoReader_Nexus 9_00:06:66:63:57:5D).

ⓘ **Note:**

- The **Door Impersonation Mode** check box is disabled by default.
- You cannot assign the same door for multiple Go Reader door objects.
- If the Go Reader device is not connected to the server when you activate or disable **Door Impersonation Mode**, the changes are sent when the device comes online, connects to the server, and synchronization is initiated.

There are three advanced access rules limitations (not supported):

- APB
- Area
- Hardware IO

Activating timed anti-passback

Use the Reader tab in the Go Reader editor to activate timed anti-passback. Timed anti-passback has a basic time and card swipe count schedule.

1. Select the **Enable Device Timed Anti-Passback** check box.
2. Under **APB Validity Duration**, set the anti-passback expiry time to a duration of between 1 minutes and 7 days.
3. Under **Max Card swipes within APB Duration**, set the maximum amount of card swipes during the anti-passback duration.
4. Click **Save and Close**.

   A notification displays on the Go Reader app. If a person swipes the reader when the maximum card swipe value is reached in the defined anti-passback validity duration their card is rejected with the message: `Rejected (Device Timed Anti Passback)`. See Card swiping with timed anti-passback on the Go Reader app for more information. If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station with this information.

ⓘ **Note:**

- The maximum card swipes during the anti-passback duration is 10.
- The default value for **Minutes** is 1.
- The default value for **Max Card Swipes within APB Duration** is 1.
- If the Go Reader device is not connected to the server when you activate or disable anti-passback, the changes are sent when the device comes online and connects to the server.

Using manual mustering with the roll call screen

You can manually muster a person by searching for the personnel name from the **Roll Call** screen. Use for scenarios where a person does not have access to their card. Enable manual mustering using the **Roll Call** tab in the Go Reader editor. See Manual mustering with roll call for information on using manual mustering with the Go Reader app.

Activating manual mustering

You can manually muster a person by searching for the personnel name from the **Roll Call** screen. Use for scenarios where a person does not have access to their card. Activate manual mustering using the **Roll Call** tab in the Go Reader editor. See Manual mustering with roll call for information on using manual mustering with the Go Reader app.

1. On the Go Reader editor **Roll Call** tab, select the **Allow Manual Mustering** check box.
2. Click **Save and Close**. A notification is sent to the Go Reader device.

ⓘ **Note: Allow Manual Mustering** is activated by default.

Offline mustering with the roll call screen

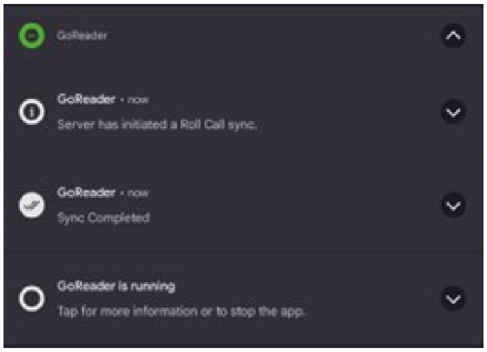
ⓘ **Note:** You must be using C•CURE 9000 v3.00.1 Critical Update 01 and Go Reader Integration Driver v6.0.82.82 or above to activate offline mustering.

Offline mustering is a function where users present a card to a Go Reader device and the operator views a running total of personnel when in offline mode with no access to Wi-Fi or cellular service. The feature is supported on all Go Reader devices. You must activate offline mustering when the Go Reader is online so the device has an up to date iSTAR Area personnel count.

All mustered credentials are synchronized with C•CURE when the Go Reader device is back online. You can check the number of personnel that were mustered offline using the C•CURE 9000 Administration Workstation and the Go Reader app. If you use multiple Go Reader devices, you must dock all the GoReader devices before viewing the missing personnel. If you have assigned multiple Go Reader devices to a server, you cannot activate offline mustering on all the devices.

Offline mustering synchronization is initiated when you activate offline mustering on the roll call tab. You must make sure offline mustering synchronization has completed to ensure that all personnel records in the missing area are up to date and can be used for mustering in offline mode. You must not activate online mustering until personnel and image synchronization has finished.

Figure 54: Offline mustering synchronization



GoReader

GoReader • now
Server has initiated a Roll Call sync.

GoReader • now
Sync Completed

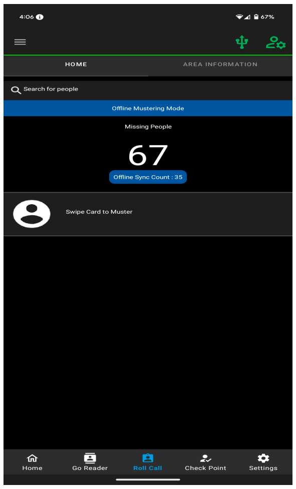
GoReader is running
Tap for more information or to stop the app.

Offline mustering synchronization is triggered automatically when there is a change to the iSTAR area that has been assigned as a missing area for the Go Reader device. If personnel enter a missing area, offline mustering synchronization is triggered automatically.

Activating offline mustering

1. In the **Navigation** pane, click **Hardware**.
2. In the **Hardware** tree, expand the **Company Name** folder.
3. Right-click the Go Reader device you want to configure and select **Edit**.
4. Select the **Roll Call** tab.
5. On the Go Reader editor **Roll Call** tab, select the **Allow Offline Mustering** check box.
6. Click **Save and Close**. A notification is sent to the Go Reader device.

Figure 55: Offline mustering mode enabled



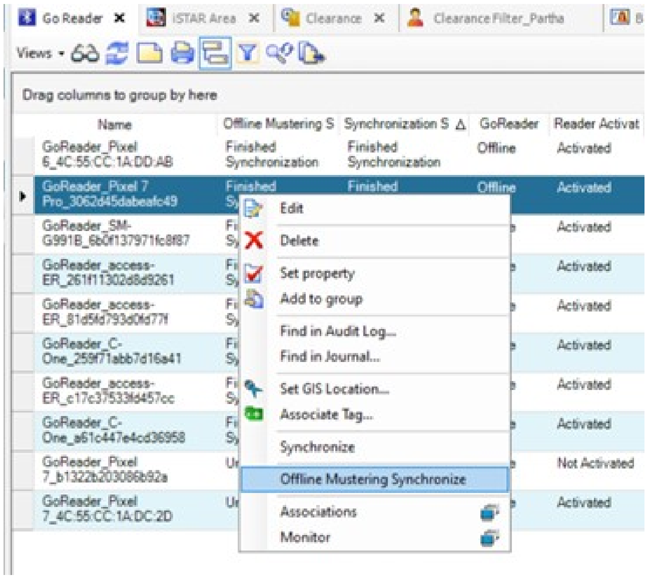
Manually initiating offline mustering synchronization

If you encounter a network or synchronization issue while synchronizing personnel for offline mustering, you can manually initiate offline mustering synchronization in C•CURE 9000. Also, if you notice a count discrepancy between the number of missing people and the Offline Sync Count, you can manually initiate offline synchronization to resolve this issue.

Note: You cannot initiate manual offline mustering synchronization if previous synchronization attempts have not been completed.

1. In the **Navigation** pane, click **Hardware**.
2. In the **Hardware** tree, expand the **Company Name** folder.
3. Right-click the Go Reader device you want to synchronize and select **Offline Mustering Synchronize**.

Figure 56: Offline mustering synchronize



Name	Offline Mustering S	Synchronization S	GoReader	Reader Activat
GoReader_Pixel 6_4C:55:CC:1A:DD:AB	Finished Synchronization	Finished Synchronization	Offline	Activated
GoReader_Pixel 7 Pro_3062d45dabeafc49	Finished Sy	Finished	Offline	Activated
GoReader_SM-G991B_6b0f137971fc8f87	Fi Sy		e	Activated
GoReader_access-ER_261f11302d8d9261	Fi Sy		e	Activated
GoReader_access-ER_81d5fd793d0fd77f	Fi Sy		e	Activated
GoReader_C-One_259f71abb7d16a41	Fi Sy		e	Activated
GoReader_access-ER_c17c37533fd457cc	Fi Sy		e	Activated
GoReader_C-One_a61c447e4cd36958	Fi Sy		e	Activated
GoReader_Pixel 7_b1322b203086b92a	Ur		e	Not Activated
GoReader_Pixel 7_4C:55:CC:1A:DC:2D	Ur		e	Activated

Using manual mustering in offline mode

You can manually muster personnel that do not have access to their card when you are mustering personnel offline. You must activate Offline Mustering on the Roll Call tab to use this function.

1. On the C•CURE Go Reader home screen, tap **Roll Call**.
2. Tap **Search for people** and type the name of the person you want to manually muster.
3. From the list of personnel, tap to select the person you want to manually muster.
4. Choose between:
   - Tap **YES** to muster the person to the roll call area.
   - Tap **NO** to return to the personnel list without making any changes.

Assigning a roll call area

A roll call area is a designated area where personnel gatherduring an emergency. The C•CURE Go Reader app uses the roll call module to determine the number of personnel missing from the roll call area.

ⓘ **Note:** If an area is configured as a muster area, it cannot be selected as a missing area. For more information about configuring mustering areas, refer to the *C•CURE 9000 Areas and Zones User Guide*.

1. In the **Navigation** pane , click **Hardware**.
2. In the **Hardware** tree, expand the **CompanyName** folder.
3. Right-click the Go Reader that you want to configure and select **Edit**.
4. Click the **Roll Call** tab.
5. In the **Roll Call Settings** section, select an area from the list.
6. Click **Save and Close**.

Assigning a missing area

The **Roll Call** module in the Go Reader app counts how many people are in a missing area to determine how many personnel are outside a roll call area. Use the **Roll Call** tab to configure an area as a missing area. There is no restriction on the amount of areas that you can configure as missing areas.

ⓘ **Note:** If mustering status is activated for an area, it cannot be selected as a missing area. For more information about enabling and disabling a mustering status, see the *C•CURE 9000 Areas and Zones User Guide*.

1. In the **Navigation** pane, click **Hardware**.
2. Expand the **CompanyName** folder.
3. Right-click the Go Reader that you want to configure and select **Edit**.
4. Click the **Roll Call** tab.
5. In the **Missing Areas** section, click **Add**.
6. Select the area that you want to assign.
7. Click **Save and Close**.

Configuring triggers and events

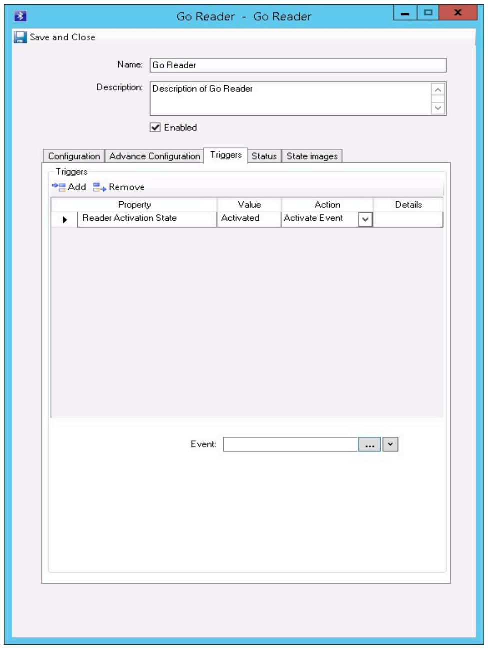
Use the Go Reader **Triggers** tab to configure triggers and events related to the Go Reader. The Go Reader **Triggers** tab uses pre-defined journal events to trigger actions from the C•CURE Go Reader app. However, you can create custom events to assign to the Go Reader app.

For more information about creating Events and Triggers, refer to the *C•CURE 9000 Software Configuration Guide*.

1. In the Go Reader editor, click the **Triggers** tab.
2. Click **Add**.
3. Click **Property** and click the ellipses.

4. Click the trigger that you want to configure.
5. From the **Value** list, select a value.
6. From the **Action** list, select an action.
7. Choose between:
   - In the **Event** field, click ellipses.
   - Click the arrow to create a new event.
8. Click **Save and Close**.

Figure 57: Assigning triggers and events



Name: Go Reader

Description: Description of Go Reader

☑ Enabled

	Property	Value	Action	Details
▶	Reader Activation State	Activated	Activate Event	

Event:

Configuring a card admit trigger using a host-based event

Use the Triggers tab in the Go Reader editor to configure events to trigger in the C•CURE 9000 Monitoring Station when a card is admitted or rejected in the Go Reader application. Events are triggered for the following admit status values:

- Admit
- Reject
- Noticed Admit
- Noticed Reject

1. On the **Triggers** tab, click **Add**.
2. From the **Property** list, select **Admit Status**.
3. From the **Value** list, select an admit status value.

   ⓘ **Note:** When a card is admitted in the Roll Call tab in the Go Reader application, the admit status event is not triggered, and the admit status does not change in the Status tab in the Go Reader editor.

   If the first card swipe event is active, subsequent card swipes do not trigger an event. For example, if Person A swipes a card and is admitted, the Admit event becomes active. If Person B swipes a card at the same time as Person A, the Admit event is not triggered for Person B.

Configuring an online status event

Use the Triggers tab in the Go Reader editor to configure events to trigger in the C•CURE 9000 Monitoring Station based on the online status of the Go Reader device.

View changes to the online status in the Status tab of the Go Reader editor. The status of the Go Reader device changes from offline to online after certain actions, such as card swipes, searches for users, check point creation, roll call mustering, and database synchronization. For the online status to change, you must perform the actions in the Go Reader application, and the Go Reader device must be connected to a C•CURE 9000 system.

ⓘ **Note:** When a Go Reader device is synchronizing, the online status does not change.

1. On the **Triggers** tab, click **Add**.
2. From the **Property** list, select **Online Status**.
3. From the **Value** list, select **Online** or **Offline**.
4. From the **Action** list, select **Activate Event**.

Changing the time period for the offline trigger

By default, the offline status is re-triggered five minutes after the action that changed the status to online is complete. You can adjust the time period in the server's configuration file to anywhere in the range of 1 to 30 minutes.

1. On your PC, navigate to the filepath `Tyco\CrossFire\ServerComponents`.
2. Open the `GoReader Driver Service .exe.config` file in a text editor.
3. Change the value of the key `<add key="GoReaderOfflineTimeout" value="300000" />`. The value of the key is listed in milliseconds. For example, the value for one minute is 60000, the value for five minutes is 300000, and the value for 30 minutes is 1800000.
4. Save the configuration file.

Removing triggers and events

Use the Triggers tab in the Go Reader editor to remove triggers and events.

1. In the Go Reader editor, select the **Triggers** tab.
2. Select the trigger row that you want to remove.
3. Click **Remove**.
4. Click **Save and Close**.

C•CURE Go Reader privileges

A privilege is a collection of rights you configure to operators so they can access security objects. To access the C•CURE Go Reader, an operator must be assigned with C•CURE Go Reader privileges. Use the Privilege Editor to configure C•CURE Go Reader privileges. Use the Operator Editor to assign the C•CURE Go Reader Privileges to an operator.

You must have Administrator rights in C•CURE 9000 to configure and assign privileges.

This section provides instructions for configuring C•CURE Go Reader privileges. For more detailed information about privileges and permission classes, refer to the *C•CURE 9000 Software Configuration Guide.*

Configuring C•CURE Go Reader privileges

Use the **Privileges Editor** to configure C•CURE Go Reader privileges.

1. In the **Navigation** pane, select **Configuration**.
2. From the **Configuration** list, select **Privilege**.
3. Click the **Go Search** icon to open a dynamic view with all privileges.

4. Choose between:
   - Double-click the privilege you want to assign the C•CURE Go Reader permissions to.
   - Right-click a privilege and select **Edit**.
5. In the **Classes** menu, in the **Defaults** tab, expand **Other**.
6. Click **Go Device** and assign the required permissions.
7. Click **C•CURE GoReader** and assign the required permissions.
8. Click **Save and Close**.

   ⓘ **Note:**
   - The Monitoring Station displays `Operator Logged In` or `Operator Logged Out` message when the C•CURE Go Reader is not in use. This is a connection validation logged by the victor Web Service.
   - You cannot edit the **SYSTEM ALL**, **Access to common Objects** privilege or any **Full Privilege for Partition** privilege.
   - To save changes to a predefined privilege, click **Create Copy**, give it a new name, and click **Save and Close** after you have made your changes.

Assigning C•CURE Go Reader privileges

Use the Operator editor to assign C•CURE Go Reader privileges to an operator profile.

1. In the **Navigation** pane, click **Configuration**.
2. From the **Configuration** pane list, select **Operator**.
3. Click the drop down arrow to view a list of operators.
4. Choose between:
   - Double-click an operator you want to assign the C•CURE Go Reader privilege to.
   - Right-click an operator and select **Edit**.
5. In the **General** tab, under **Privileges and Schedules**, click **Add**.
6. Select a privilege configured with C•CURE Go Reader permissions.
7. Click the ellipses to assign a **Schedule**.
8. Click **Save and Close**.

Manual actions

Use the C•CURE 9000 Administration Station for the following manual actions:

- Synchronizing the C•CURE Go Reader
- Resetting the Go Device
- Deleting the C•CURE Go Reader
- Deleting the Go Device

Synchronizing the C•CURE Go Reader

Before you begin:
Ensure the following prerequisites have been met before synchronizing the C•CURE Go Reader device:

- The C•CURE Go Reader device is activated in C•CURE 9000.
- The C•CURE Go Reader status is **Connected to Server** in the C•CURE Go Reader app.
- Synchronization is not already in progress.

ⓘ **Note:** If synchronization is in progress, the **Synchronize** option is not displayed.

After the first time that the app has been authorized and activated from C•CURE 9000, the C•CURE Go Reader app automatically performs a full synchronization of configuration data and personnel data with C•CURE 9000. Any updates made to C•CURE 9000 configurations after the app has been activated results in a differential download to the C•CURE Go Reader app. You can manually synchronize the C•CURE Go Reader app in the Administration Station to a perform a full synchronization with C•CURE 9000 and to remove all previous configurations.

When you synchronize the C•CURE Go Reader, the following statuses are displayed in the Monitoring Station:

- Synchronization Initiated
- Synchronization Pending
- Synchronization Failed
- Synchronizing
- Finished Synchronization

This section provides information about using a manual action to synchronize the C•CURE Go Reader. See Synchronizing the C•CURE Go Reader from the C•CURE Go Reader device for instructions on how to synchronize the C•CURE Go Reader from your device.

1. In the **Navigation** pane, select **Hardware**.
2. In the **Hardware** tree, expand the **CompanyName** folder.
3. Expand **Doors**.
4. Right-click the C•CURE Go Reader you want to synchronize.
5. In the context menu, click **Synchronize**.

Resetting the Go Device

In the C•CURE 9000 Administration Station, use manual actions to reset the Go Device. Resetting the Go Device performs a factory reset of C•CURE Go Reader that deletes all personnel information and card swipe history.

This section describes how to use a manual action in C•CURE to reset the device. See Resetting the C•CURE Go Reader from the C•CURE Go Reader app for instructions on how to reset the Go Device from your Android device.

1. In the **Navigation** pane, select **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand **Doors**.
4. Right-click the Go Device you want to reset.
5. Choose between:
   - Click **OK** to continue with reset.
   - Click **Cancel** to cancel.

Deleting the C•CURE Go Reader

Before you delete the C•CURE Go Reader, disable it in the C•CURE Go Reader editor, otherwise an error message is displayed. For information on how to disable the C•CURE Go Reader, see Disabling the Go Reader.

1. In the **Navigation** pane, select **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand **Doors**.
4. Right-click the C•CURE Go Reader that you want to delete.
5. In the context menu, click **Delete**.
6. Choose between:
   - Click **Yes** to confirm deletion.
   - Click **No** to cancel.

After deleting the Go Device, the C•CURE GoReader is removed from the **Hardware Tree** and the C•CURE Go Reader app returns to the log on screen.

Deleting the Go Device

You must delete the C•CURE Go Reader before deleting the Go Device from C•CURE 9000, otherwise an error message is displayed. For information about deleting the C•CURE Go Reader, see Deleting the C•CURE Go Reader.

1. In the **Navigation** pane, select **Hardware**.
2. Expand the **CompanyName** folder.
3. Expand **Go Devices**.
4. Right-click the Go Device you want to delete.
5. Choose between:
   - Click **Yes** to confirm.
   - Click **No** to cancel.

C•CURE Go Reader clearances

A clearance specifies the doors or door groups that a person can access, and when that access can occur. You can configure a specific C•CURE Go Reader clearance and assign that clearance to a personnel profile, or you can add a C•CURE Go Reader door to an existing clearance that may also contain C•CURE 9000 doors or door groups.

This section provides instructions for configuring a C•CURE Go Reader clearance. For more information about clearances, refer to the *C•CURE 9000 Software Configuration Guide*.

Configuring a C•CURE Go Reader clearance

Use the Clearance editor to configure a C•CURE Go Reader clearance.

1. In the **Navigation** pane, click **Personnel**.
2. From the **Personnel** pane list, select **Clearance**.
3. Click **New**.
4. In the **Name** field, type a name for the clearance.
5. In the **Description** field, type a description for the clearance.
6. On the **General** tab, choose activation and expiration settings for the clearance.
7. Click the **Doors** tab.
8. Click **Add**.
9. From the list, select a C•CURE Go Reader door. You can add more than one C•CURE Go Reader to the clearance.
10. Click **OK**.
11. Select a schedule.
12. Click **Save and Close**.

> ⓘ **Note:** Editing an existing clearance results in an automatic synchronization across all devices, changes are made to the C•CURE Go Reader device associated with the edited clearance.

Adding a Go Reader clearance to personnel

Use the **Clearances** tab in the Personnel editor to assign a C•CURE Go Reader clearance to a personnel profile. You can assign multiple C•CURE Go Reader clearances to individual personnel.

1. In the **Navigation** pane, select **Personnel**.
2. From the **Personnel** pane list, select **Personnel**.
3. Open the dynamic view for personnel.
4. Select a personnel profile that you want to assign the clearance.
5. In the **Personnel** editor, click the **Clearances** tab .

6. Select a C•CURE Go Reader configured clearance.

   For more information about configuring C•CURE Go Reader clearances, see Configuring a C•CURE Go Reader clearance.

Expiring clearance

Go Reader's expiring clearance feature is part of C•CURE Clearance.

- You do not have to follow other user-defined C•CURE schedules.
- There is no need to set Always schedule.
- You can assign Go Reader devices to operate within specific time intervals.

For more info about expiring clearance, refer *C•CURE 9000 Personnel Configuration Guide*.

Go Reader online status notifications

Go Reader supports three distinct notification statuses to keep users informed:

- **Online:** This status indicates that the app and server are online and connected.
- **Offline:** This status indicates that the app and server are offline and not connected.
- **Idle:** This status indicates that the Go Reader device is inactive.

ⓘ **Note:** You can configure the time intervals for each status in Go Reader’s driver configuration files.

FASC-N support

FASC-N is a data structure that is used to store the Federal Agency Smart Credential Number which is a 32-digit identifier on a Personal Identity Verification (PIV) card. It is required for physical access control as per the Federal Information Processing Standards (FIPS).

To use FASC-N card format in Go Reader, import or create a new CHUID format in C•CURE 9000. No configuration changes are required in the app.

Configuring CHUID format for FASC-N in C•CURE

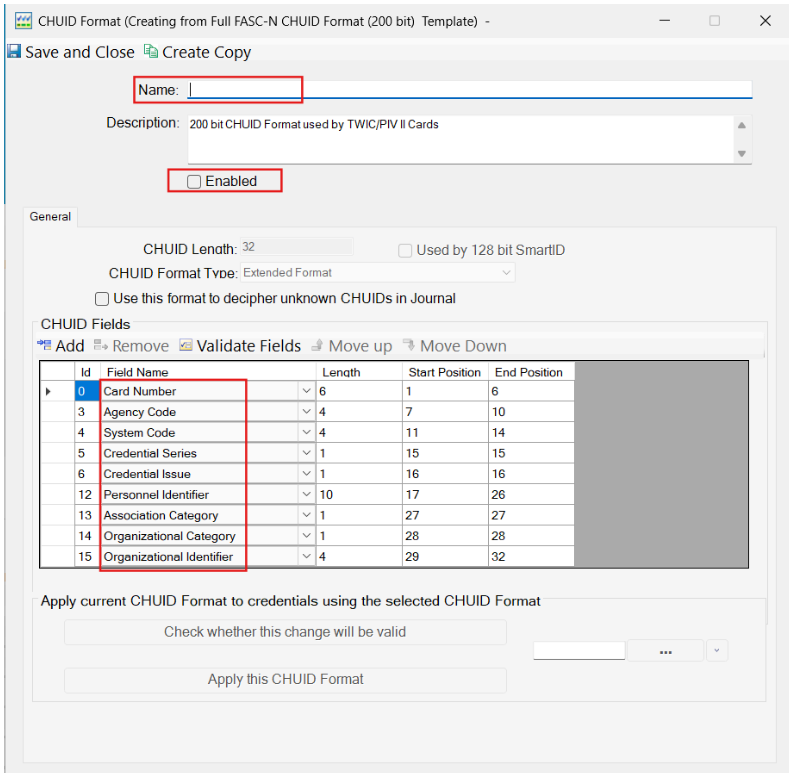
You can configure CHUID format for FASC-N cards in C•CURE as it has an inbuilt CHUID format template.

1. In the Navigation Pane of the Administration Workstation, click **Personnel**.
2. In the **Personnel** pane, select **CHUID Format** from the dropdown list.
3. Click the arrow on the **New** button and then click **Full FASC-N CHUID Format (200 bit) Template**.

   The CHUID Format editor opens.
4. Enter the name and description, then select **Enabled** check box.
5. Check the value in the following fields:
   - Card Number
   - Agency Code
   - System Code
   - Credential Series
   - Credential Issue
   - Person Identifier
   - Association Category
   - Organizational Category
   - Organizational Identifier
6. Click **Save and Close** button.

CHUID format template is configured for FASC-N cards.

Figure 58: CHUID format



CHUID Format (Creating from Full FASC-N CHUID Format (200 bit) Template) -

Save and Close   Create Copy

Name:

Description: 200 bit CHUID Format used by TWIC/PIV II Cards

☐ Enabled

General

CHUID Length: 32   ☐ Used by 128 bit SmartID

CHUID Format Type: Extended Format

☐ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

Add   Remove   Validate Fields   Move up   Move Down

Id	Field Name	Length	Start Position	End Position
0	Card Number	6	1	6
3	Agency Code	4	7	10
4	System Code	4	11	14
5	Credential Series	1	15	15
6	Credential Issue	1	16	16
12	Personnel Identifier	10	17	26
13	Association Category	1	27	27
14	Organizational Category	1	28	28
15	Organizational Identifier	4	29	32

Apply current CHUID Format to credentials using the selected CHUID Format

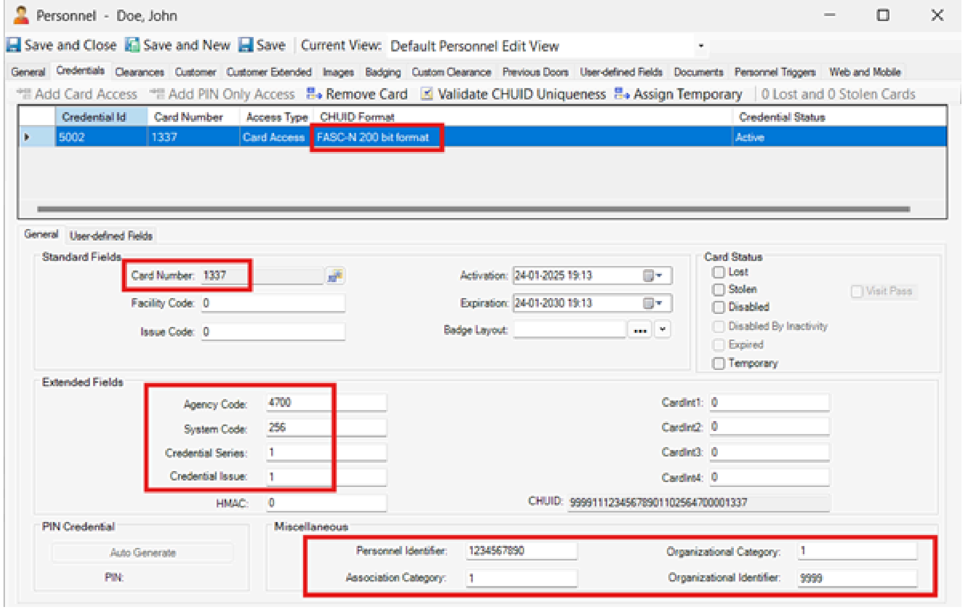
Check whether this change will be valid

Apply this CHUID Format

Creating personnel with FASC-N CHUID format

1. When creating personnel with FASC-N credentials, choose the newly created FASC-N CHUID format.
2. In the **Credentials** tab, enter the credential values into **Standard Fields**, **Extended Fields** and, **Miscellaneous**.

Figure 59: Personnel Edit View



Personnel - Doe, John

Save and Close   Save and New   Save   Current View: Default Personnel Edit View

General | Credentials | Clearances | Customer | Customer Extended | Images | Badging | Custom Clearance | Previous Doors | User-defined Fields | Documents | Personnel Triggers | Web and Mobile

Add Card Access   Add PIN Only Access   Remove Card   Validate CHUID Uniqueness   Assign Temporary   0 Lost and 0 Stolen Cards

Credential Id	Card Number	Access Type	CHUID Format	Credential Status
5002	1337	Card Access	FASC-N 200 bit format	Active

General | User-defined Fields

Standard Fields

Card Number: 1337

Facility Code: 0

Issue Code: 0

Activation: 24-01-2025 19:13

Expiration: 24-01-2030 19:13

Badge Layout:

Card Status

☐ Lost

☐ Stolen

☐ Disabled

☐ Disabled By Inactivity

☐ Expired

☐ Temporary

☐ Visit Pass

Extended Fields

Agency Code: 4700

System Code: 256

Credential Series: 1

Credential Issue: 1

HMAC: 0

CardInt1: 0

CardInt2: 0

CardInt3: 0

CardInt4: 0

CHUID: 99991112345678901102564700001337

PIN Credential

Auto Generate

PIN:

Miscellaneous

Personnel Identifier: 1234567890

Association Category: 1

Organizational Category: 1

Organizational Identifier: 9999

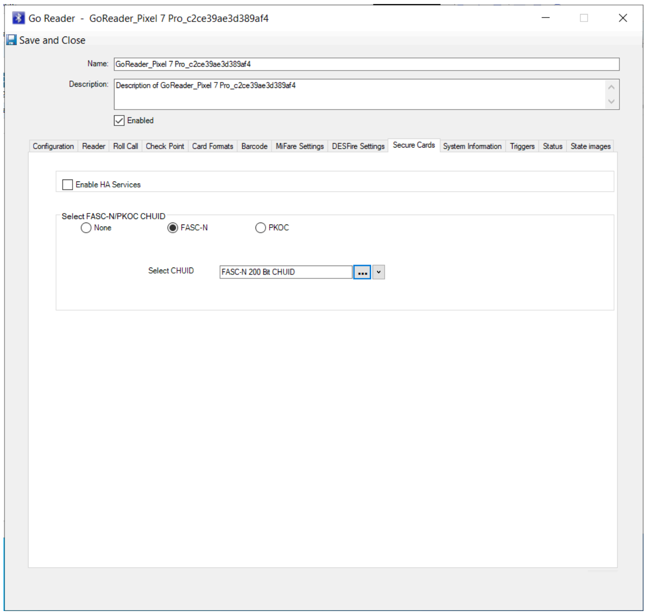
Configuring Go Reader to read FASC-N credentials

Before you begin:

Ensure the Go Reader device is activated and the FASC-N CHUID is created in the C•CURE 9000 system.

1. Open the **Go Reader Editor**.
2. Click the **Secure Cards** tab.
3. Select the **FASC-N** radio button.
4. In the **Select CHUID** field, choose the created FASC-N CHUID.
5. Click the **Save and Close** button.
6. When prompted, click **Yes** on the pop-up message to proceed with synchronization.

Figure 60: FASC-N CHUID selection in Secure Card tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Save and Close

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

Configuration | Reader | Roll Call | Check Point | Card Formats | Barcode | MiFare Settings | DESFire Settings | Secure Cards | System Information | Triggers | Status | State images

□ Enable HA Services

Select FASC-N/PKOC CHUID

○ None ● FASC-N ○ PKOC

Select CHUID: FASC-N 200 Bit CHUID

Using FASC-N Cards with Go Reader

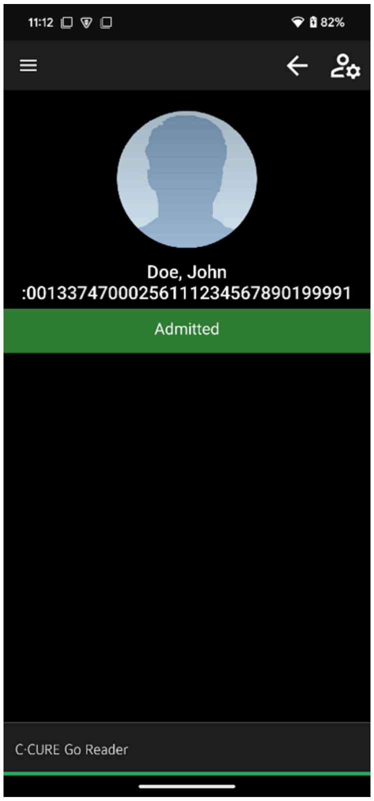
Before you begin:

Ensure that you have created personnel with FASC-N CHUID format in C•CURE 9000, and these personnels are sychronized to the C•CURE Go Reader.

1. On the C•CURE Go Reader Home screen, tap **Go Reader**.
2. Swipe a person's card.

   The C•CURE Go Reader screen displays the card status.
3. If CHUID format is imported or created successfully in the C•CURE Go Reader app then the card status displays as **Admitted**.

Figure 61: Admitted Personnel



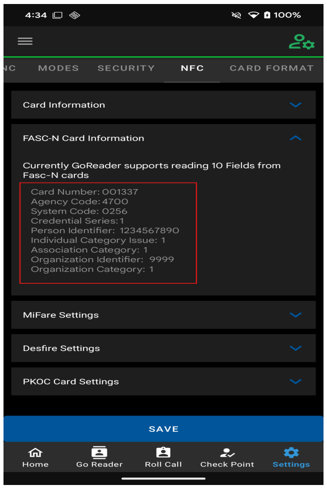
ⓘ **Note:** iSTAR Online Reader mode and does not support FASC-N.

Viewing FASC-N Card on BYO devices

1. In the Go Reader app, tap **Settings** > **NFC** tab.
2. Expand the **FASC-N Card Information** section.
3. To check the FASC-N Card information, swipe a person's card.

FASC-N card information appears on the screen.

Figure 62: FASC-N card information



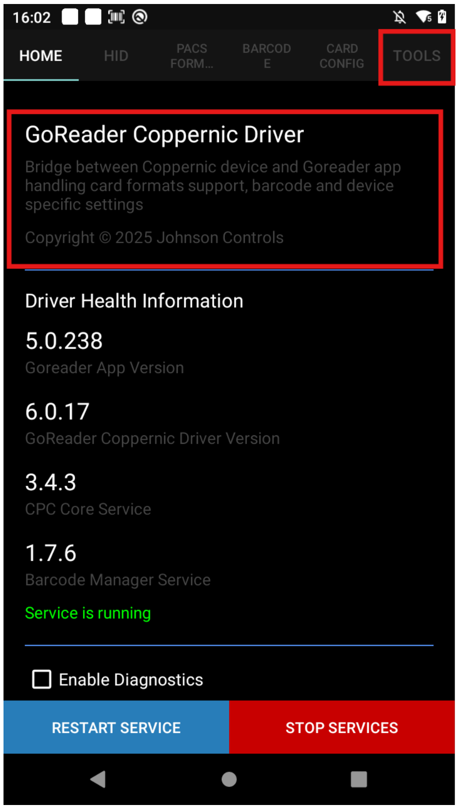
Currently GoReader supports reading 10 Fields from Fasc-N cards

Card Number: 001337
Agency Code: 4700
System Code: 0256
Credential Series: 1
Person Identifier: 1234567890
Individual Category Issue: 1
Association Category: 1
Organization Identifier: 9999
Organization Category: 1

Viewing FASC-N Card on Coppernic Access ER

1. Open the Go Reader Coppernic Driver Service app.
2. To enable the **Tools** tab, tap the title **Go Reader Coppernic Driver** multiple times.

Figure 63: FASC-N card diagnostics



GoReader Coppernic Driver

Bridge between Coppernic device and Goreader app handling card formats support, barcode and device specific settings

Copyright © 2025 Johnson Controls

Driver Health Information

5.0.238
Goreader App Version

6.0.17
GoReader Coppernic Driver Version

3.4.3
CPC Core Service

1.7.6
Barcode Manager Service

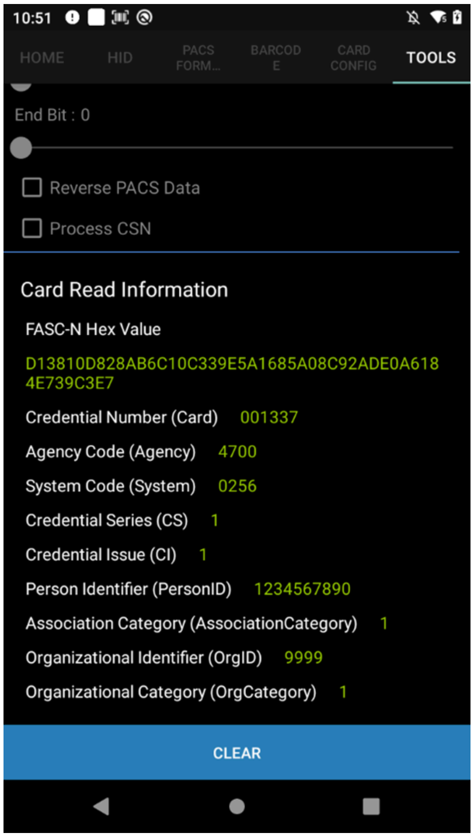
Service is running

□ Enable Diagnostics

3. On the **Tools** tab, scroll down to the bottom of the page and display any person’s card.

FASC-N card information appears on the screen.

Figure 64: Card read information



End Bit : 0

□ Reverse PACS Data

□ Process CSN

Card Read Information

FASC-N Hex Value

D13810D828AB6C10C339E5A1685A08C92ADE0A618
4E739C3E7

Credential Number (Card)	001337
Agency Code (Agency)	4700
System Code (System)	0256
Credential Series (CS)	1
Credential Issue (CI)	1
Person Identifier (PersonID)	1234567890
Association Category (AssociationCategory)	1
Organizational Identifier (OrgID)	9999
Organizational Category (OrgCategory)	1

PKOC support

Public Key Open Credential (PKOC) cards can be configured to operate in one of three bit lengths:

- 64 Bit
- 128 Bit
- 256 Bit

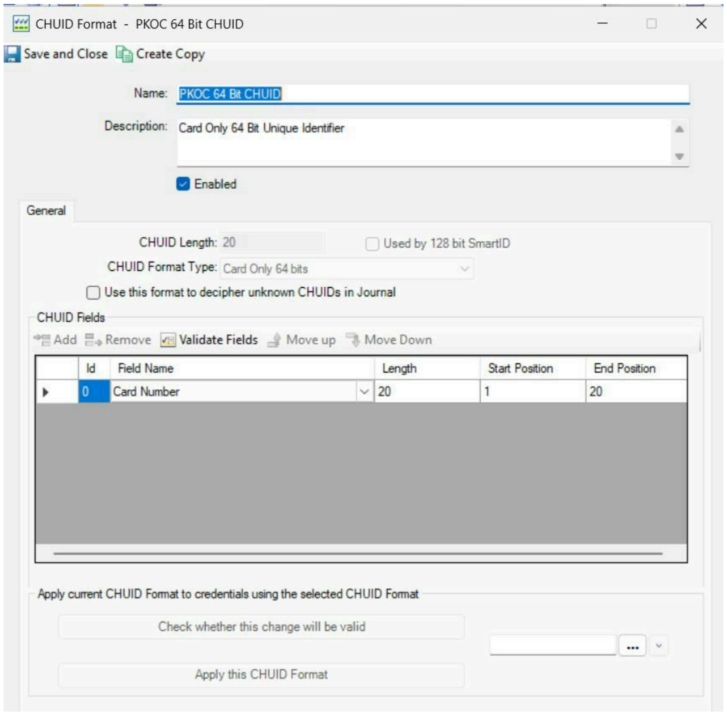
All three configurations are valid. However, it is essential to select one bit length and ensure that both the C•CURE 9000 system and the Go Reader device are configured accordingly. This alignment is necessary for the PKOC card to function properly.

Creating 64 Bit PKOC CHUID format

To configure a 64-bit PKOC CHUID format in the CCure Admin Workstation, follow these steps:

1. In the **CCure Admin Workstation**, navigate to the **CHUID Format** section in the left pane and click **New**.
2. **(Optional)**: From the **CHUID Templates** drop-down, select **Card Only 64 Template**.
3. Add the following field with the specified parameters:
   - **Field Name:** Card Number
   - **Length:** 20
   - **Start Position:** 1
   - **End Position:** 20
4. Enter a **Name** for the format, check the **Enabled** box, then click **Save and Close**.

Figure 65: Adding card number field in 64-Bit PKOC CHUID format



Name: PKOC 64 Bit CHUID

Description: Card Only 64 Bit Unique Identifier

☑ Enabled

CHUID Length: 20

□ Used by 128 bit SmartID

CHUID Format Type: Card Only 64 bits

□ Use this format to decipher unknown CHUIDs in Journal

Id	Field Name	Length	Start Position	End Position
0	Card Number	20	1	20

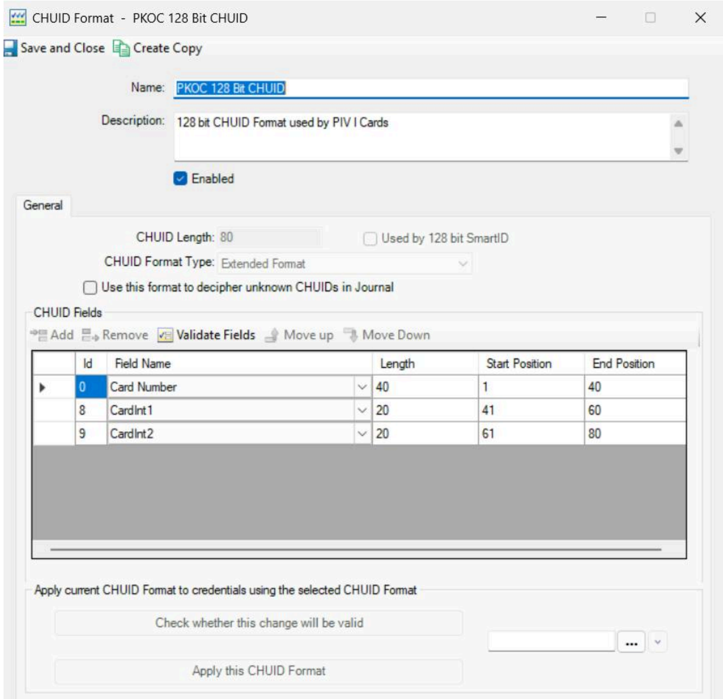
Apply current CHUID Format to credentials using the selected CHUID Format

Creating 128 Bit PKOC CHUID format

To create a 128-bit PIV I CHUID format in CCure Admin Workstation:

1. In the left pane of the CCure Admin Workstation, navigate to the **CHUID Format** section.
2. Click **New** to create a new CHUID format.
3. (Optional) From the list of CHUID templates, select **PIV I CHUID Format (128-bit) Template**.
4. Add the following fields with the specified lengths and positions:
   - **Card Number**: Length = 40, Start Position = 1, End Position = 40
   - **Card Int 1**: Length = 20, Start Position = 41, End Position = 60
   - **Card Int 2**: Length = 20, Start Position = 61, End Position = 80
5. Enter a descriptive **Name** for the format.
6. Check the **Enabled** checkbox to activate the format.
7. Click **Save and Close** to complete the configuration.

Figure 66: Configuring a 128-Bit PIV I CHUID Format in CCure Admin Workstation



CHUID Format - PKOC 128 Bit CHUID

Name: PKOC 128 Bit CHUID

Description: 128 bit CHUID Format used by PIV I Cards

☑ Enabled

CHUID Length: 80

□ Used by 128 bit SmartID

CHUID Format Type: Extended Format

□ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

Id	Field Name	Length	Start Position	End Position
0	Card Number	40	1	40
8	CardInt1	20	41	60
9	CardInt2	20	61	80

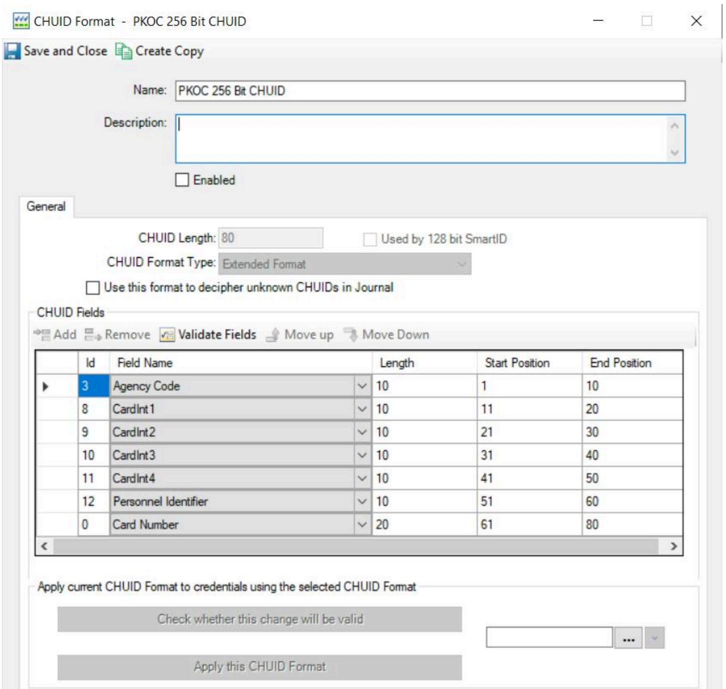
Apply current CHUID Format to credentials using the selected CHUID Format

Creating 256 Bit PKOC CHUID format

To create a custom CHUID format in CCure Admin Workstation:

1. In the left pane of the CCure Admin Workstation, navigate to the **CHUID Format** section.
2. Click **New** to create a new CHUID format.
3. Add the following fields with the specified lengths and positions:
   - **Agency Code**: Length = 10, Start Position = 1, End Position = 10
   - **Card Int 1**: Length = 10, Start Position = 11, End Position = 20
   - **Card Int 2**: Length = 10, Start Position = 21, End Position = 30
   - **Card Int 3**: Length = 10, Start Position = 31, End Position = 40
   - **Card Int 4**: Length = 10, Start Position = 41, End Position = 50
   - **Personnel Identifier**: Length = 10, Start Position = 51, End Position = 60
   - **Card Number**: Length = 20, Start Position = 61, End Position = 80
4. Enter a descriptive **Name** for the format.
5. Check the **Enabled** check box to activate the format.
6. Click **Save and Close** to complete the configuration.

Figure 67: Field Configuration for Custom CHUID Format in CCure Admin Workstation



CHUID Format - PKOC 256 Bit CHUID

Save and Close | Create Copy

Name: PKOC 256 Bit CHUID

Description:

☐ Enabled

General

CHUID Length: 80 ☐ Used by 128 bit SmartID

CHUID Format Type: Extended Format

☐ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

Add | Remove | Validate Fields | Move up | Move Down

Id	Field Name	Length	Start Position	End Position
3	Agency Code	10	1	10
8	CardInt1	10	11	20
9	CardInt2	10	21	30
10	CardInt3	10	31	40
11	CardInt4	10	41	50
12	Personnel Identifier	10	51	60
0	Card Number	20	61	80

Apply current CHUID Format to credentials using the selected CHUID Format

Check whether this change will be valid

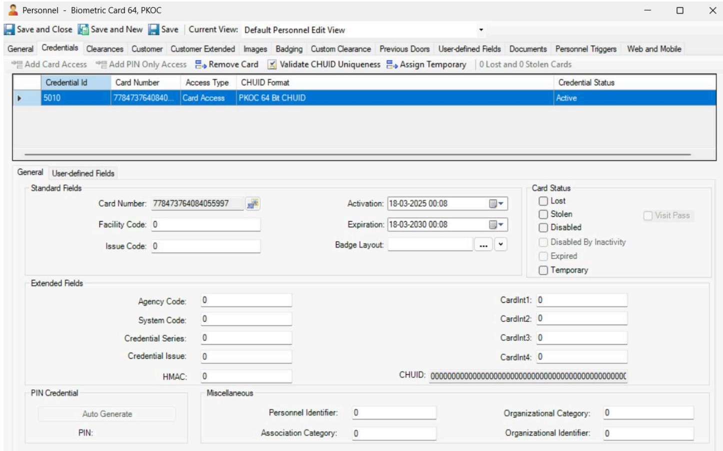
Apply this CHUID Format

Creating personnel with 64 Bit PKOC CHUID format

To create personnel with the 64-bit PKOC CHUID format in CCure Admin Workstation:

1. Navigate to the **Personnel** section and begin adding or editing a personnel record.
2. In the **Credential** tab, add a new PKOC credential.
3. From the **CHUID Format** drop down, select **PKOC 64 Bit CHUID**.
4. Enter values into the respective fields as defined by the selected CHUID format.
5. Complete the remaining personnel details as required and save the record.

Figure 68: Assigning a PKOC Credential Using the 64-Bit CHUID Format



Personnel - Biometric Card 64, PKOC

Save and Close | Save and New | Save | Current View: Default Personnel Edit View

General | Credentials | Clearances | Customer | Customer Extended | Images | Badging | Custom Clearance | Previous Doors | User-defined Fields | Documents | Personnel Triggers | Web and Mobile

Add Card Access | Add PIN Only Access | Remove Card | Validate CHUID Uniqueness | Assign Temporary | 0 Lost and 0 Stolen Cards

Credential Id	Card Number	Access Type	CHUID Format	Credential Status
5010	7784737640840...	Card Access	PKOC 64 Bit CHUID	Active

General | User-defined Fields

Standard Fields

Card Number: 778473764084055997

Facility Code: 0

Issue Code: 0

Activation: 18-03-2025 00:08

Expiration: 18-03-2030 00:08

Badge Layout:

Card Status

☐ Lost

☐ Stolen

☐ Disabled

☐ Disabled By Inactivity

☐ Expired

☐ Temporary

☐ Visit Pass

Extended Fields

Agency Code: 0

System Code: 0

Credential Series: 0

Credential Issue: 0

HMAC: 0

CardInt1: 0

CardInt2: 0

CardInt3: 0

CardInt4: 0

CHUID: 000000000000000000000000000000000000000000000

PIN Credential

Auto Generate

PIN:

Miscellaneous

Personnel Identifier: 0

Association Category: 0

Organizational Category: 0

Organizational Identifier: 0

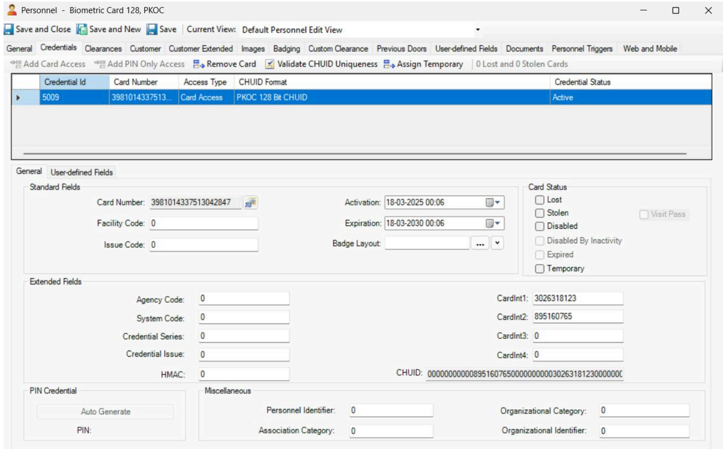
Creating personnel with 128 Bit PKOC CHUID format

To create personnel with the 128-bit PKOC CHUID format:

1. Navigate to the **Personnel** section in the CCure Admin Workstation.
2. Add a new personnel record or open an existing one for editing.

3. Go to the **Credential** tab.
4. Click **Add** to create a new PKOC credential.
5. From the **CHUID Format** dropdown, select **PKOC 128 Bit CHUID**.
6. Enter the required values into each field as defined by the selected CHUID format.
7. Complete any remaining personnel details as needed.
8. Click **Save**.

Figure 69: Assigning a PKOC Credential Using the 128-Bit CHUID Format



Credential Id	Card Number	Access Type	CHUID Format	Credential Status
5009	3981014337513...	Card Access	PKOC 128 Bit CHUID	Active

Standard Fields

Card Number: 3981014337513042847

Facility Code: 0

Issue Code: 0

Activation: 18-03-2025 00:06

Expiration: 18-03-2030 00:06

Badge Layout:

Card Status

□ Lost

□ Stolen

□ Disabled

□ Disabled By Inactivity

□ Expired

□ Temporary

□ Visit Pass

Extended Fields

Agency Code: 0

System Code: 0

Credential Series: 0

Credential Issue: 0

HMAC: 0

CardInt1: 3026318123

CardInt2: 895160765

CardInt3: 0

CardInt4: 0

CHUID: 000000000008951607650000000000030263181230000000

PIN Credential

PIN:

Miscellaneous

Personnel Identifier: 0

Association Category: 0

Organizational Category: 0

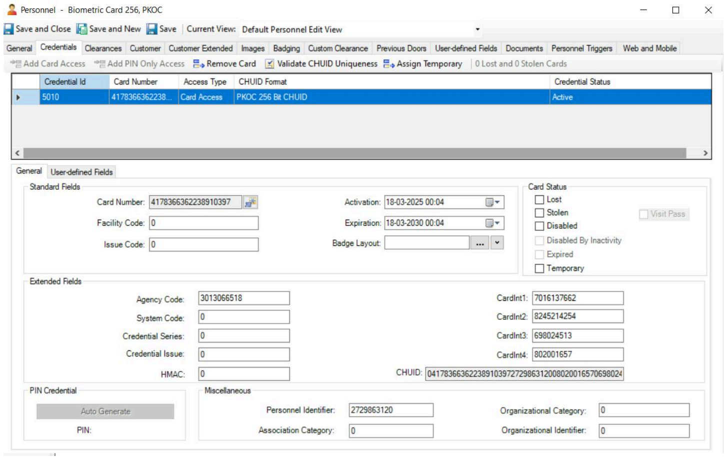
Organizational Identifier: 0

Creating personnel with 256 Bit PKOC CHUID format

To create personnel with the 256-bit PKOC CHUID format:

1. Navigate to the **Personnel** section in the CCure Admin Workstation.
2. Add a new personnel record or open an existing one for editing.
3. Go to the **Credential** tab.
4. Click **Add** to create a new PKOC credential.
5. From the **CHUID Format** dropdown, select **PKOC 256 Bit CHUID**.
6. Enter the required values into each field as defined by the selected CHUID format.
7. Complete any remaining personnel details as needed.
8. Click **Save**.

Figure 70: Assigning a PKOC Credential Using the 256-Bit CHUID Format



Credential Id	Card Number	Access Type	CHUID Format	Credential Status
5010	4178366362238...	Card Access	PKOC 256 Bit CHUID	Active

Standard Fields

Card Number: 4178366362238910397

Facility Code: 0

Issue Code: 0

Activation: 18-03-2025 00:04

Expiration: 18-03-2030 00:04

Badge Layout:

Card Status

□ Lost

□ Stolen

□ Disabled

□ Disabled By Inactivity

□ Expired

□ Temporary

□ Visit Pass

Extended Fields

Agency Code: 3013066518

System Code: 0

Credential Series: 0

Credential Issue: 0

HMAC: 0

CardInt1: 7016137662

CardInt2: 8245214254

CardInt3: 698024513

CardInt4: 802001657

CHUID: 04178366362238910397272986312008020016570698024

PIN Credential

PIN:

Miscellaneous

Personnel Identifier: 2729863120

Association Category: 0

Organizational Category: 0

Organizational Identifier: 0

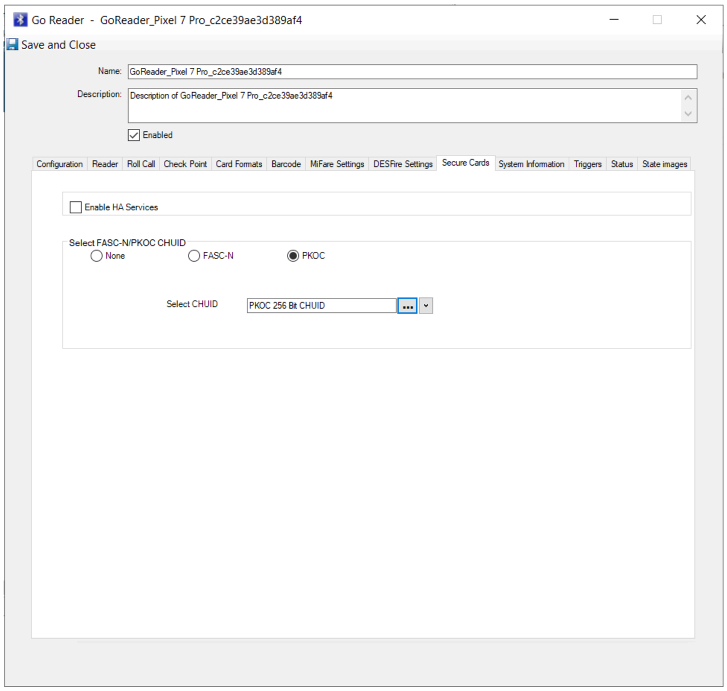
Configuring Go Reader driver to read PKOC Credentials

Before you begin:

Ensure that the **Go Reader device is activated** and the required **PKOC CHUID format** (64-bit, 128-bit, or 256-bit) has been created in the **C•CURE 9000 system**.

1. Open the **Go Reader Editor**.
2. Click the **Secure Cards** tab.
3. Select the **PKOC** radio button.
4. In the **Select CHUID** field, choose the previously created PKOC CHUID format. You may select any format with a length of **64-bit**, **128-bit**, or **256-bit**, depending on your configuration requirements.
5. Click **Save and Close**.
6. When prompted, click **Yes** on the pop-up message to proceed with synchronization.

Figure 71: PKOC CHUID selection in Secure Card tab



Go Reader - GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Name: GoReader_Pixel 7 Pro_c2ce39ae3d389af4

Description: Description of GoReader_Pixel 7 Pro_c2ce39ae3d389af4

☑ Enabled

☐ Enable HA Services

Select FASC-N/PKOC CHUID: ○ None ○ FASC-N ● PKOC

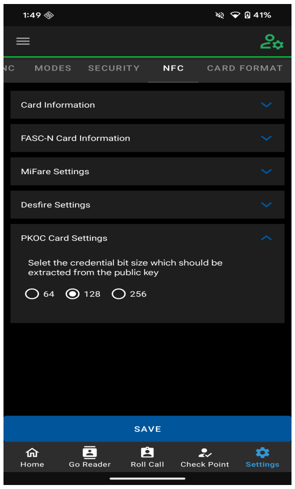
Select CHUID: PKOC 256 Bit CHUID

Configuring BYO device to read PKOC credentials

To configure PKOC bit length in the GoReader Main App:

1. Open the **GoReader Main App** and navigate to the **Settings** section.
2. In the **NFC** tab, expand the **PKOC** section.
3. Select the **bit length** (64-bit, 128-bit, or 256-bit) based on your configuration.
4. Ensure that the selected bit length matches the **PKOC CHUID format** previously configured on the Go Reader device via the Admin Workstation.
5. Tap the **Save** button to apply the changes.

Figure 72: Selecting PKOC Bit length in Go Reader main app



Selet the credential bit size which should be extracted from the public key

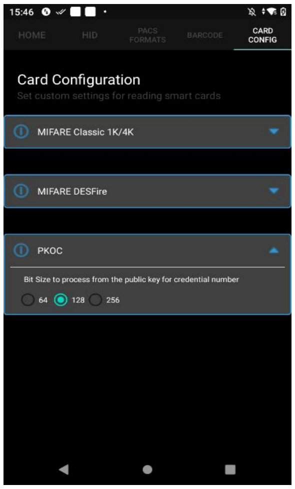
○ 64 ● 128 ○ 256

Configuring Access-ER to read PKOC credentials

To configure Access-ER to read PKOC credentials:

1. Open the **Go Reader Driver Service App** and navigate to the **Card Config** tab.
2. Expand the **PKOC** section.
3. Select the appropriate **bit length** (64-bit, 128-bit, or 256-bit) based on your credential configuration.
4. Ensure that the selected bit length matches the **PKOC CHUID format** previously configured on the Go Reader device via the Admin Workstation.
5. Tap the **Save** button to apply the changes.

Figure 73: Configuring PKOC Bit Length in Go Reader Driver Service App



Card Configuration

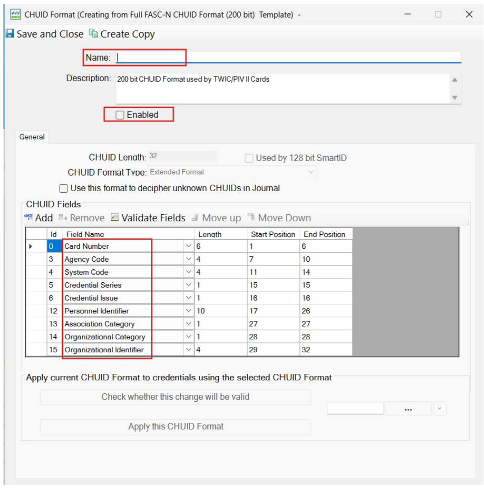
Set custom settings for reading smart cards

Bit Size to process from the public key for credential number

○ 64 ● 128 ○ 256

The CHUID format template is configured to support **FASC-N cards**, ensuring compatibility with Federal Agency Smart Credential Number standards. This configuration allows for secure identification and credentialing in accordance with PKOC specifications.

Figure 74: CHUID format



CHUID Format (Creating from Full FASC-N CHUID Format (200 bit) Template) -
Save and Close
Create Copy
General
CHUID Fields
Add
Remove
Validate Fields
Move up
Move Down
Check whether this change will be valid
Apply this CHUID Format
...

Name:

Description: 200 bit CHUID Format used by TWIC/PIV II Cards

□ Enabled

CHUID Length: 32

□ Used by 128 bit SmartID

CHUID Format Type: Extended Format

□ Use this format to decipher unknown CHUIDs in Journal

Id	Field Name	Length	Start Position	End Position
0	Card Number	6	1	6
3	Agency Code	4	7	10
4	System Code	4	11	14
5	Credential Series	1	15	15
6	Credential Issue	1	16	16
12	Personnel Identifier	10	17	26
13	Association Category	1	27	27
14	Organizational Category	1	28	28
15	Organizational Identifier	4	29	32

Apply current CHUID Format to credentials using the selected CHUID Format

Using the C•CURE Go Reader app

This chapter provides instructions for logging into the C•CURE Go Reader app, accessing and using the C•CURE Go Reader modules for roll call, card reading and settings for C•CURE Go Reader.

Log on screen

The Log On screen is the first screen in the application. It is where you enter the credentials associated with your C•CURE 9000 operator account.

Launching the C•CURE Go Reader app

Ensure the following prerequisites have been met:

- Your Android device is connected to the C•CURE 9000 server. For more information, see Creating connections.
- You have a C•CURE 9000 operator user name and password.
- You have the server IP address for the C•CURE 9000 server you want to logon to.

ⓘ **Note:** You must have C•CURE Go Reader Privilege rights enabled on your C•CURE 9000 operator profile to log on to the C•CURE Go Reader app. For information about enabling C•CURE Go Reader Privileges, see Activating the Go Reader, or contact your C•CURE 9000 Administrator to confirm your operator privileges.

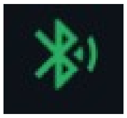
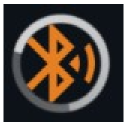
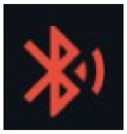
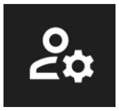
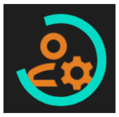
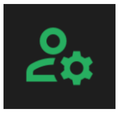
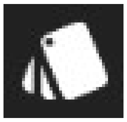
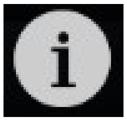
C•CURE Go Reader icons

The following icons are displayed in the C•CURE Go Reader app:

Table 31: C•CURE Go Reader icons

Icon	Description	Action
☰	Menu icon.	Tap to open the menu.
🏠	Home screen icon.	Tap to return to the home screen after navigating to other screens.

Table 31: C•CURE Go Reader icons

Icon	Description	Action
	C•CURE Go Reader has successfully connected to the Serialio idChamp RS3 card reader.	Tap to disconnect Serialio idChamp RS3 card reader.
	C•CURE Go Reader is attempting to connect to the Bluetooth enabled Serialio idChamp RS3 card reader.	Tap to establish connection with Bluetooth enabled Serialio idChamp RS3 card reader.
	C•CURE Go Reader unable to connect to Bluetooth enabled Serialio idChamp RS3 card reader.	Tap to establish connection with Bluetooth enabled Serialio idChamp RS3 card reader.
	Operator has logged on.	Tap to log off. ⓘ **Note:** After you log off, all modules except settings are available. Log on to access settings.
	Operator log on is in process.	Tap to change log on credentials for operator.
	Operator is logged off.	Tap to log on using your operator log on details or to change operator.
	Device registered in C•CURE 9000.	Read only.
	C•CURE Go Reader version information.	Tap to display C•CURE Go Reader app version details.

Starting the Go Reader application

Before you begin:

Ensure the following prerequisites have been met:

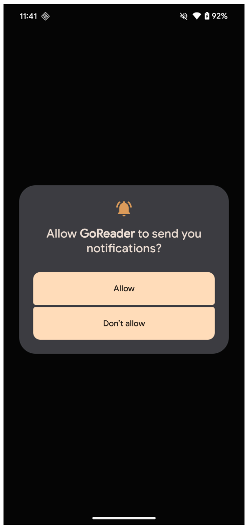
- Verify that your Android device can connect to the C•CURE 9000 server. For more information, see Creating connections.
- Go Reader Driver service must be running in the C•CURE 9000 server.
- You have a C•CURE 9000 operator user name and password.
- You have the server IP address for the C•CURE 9000 server you want to log on to.

ⓘ **Note:** You must have C•CURE Go Reader privilege rights enabled in your C•CURE 9000 operator profile to log on to the C•CURE Go Reader app. For information about enabling C•CURE Go Reader privileges, see Activating the Go Reader, or contact your C•CURE 9000 administrator to confirm your operator privileges.

1. From the device Home screen or from the device app menu, tap the **C•CURE Go Reader** icon.

2. When the notification permission popup appears, select **Allow** to enable GoReader notifications. See Figure 75.

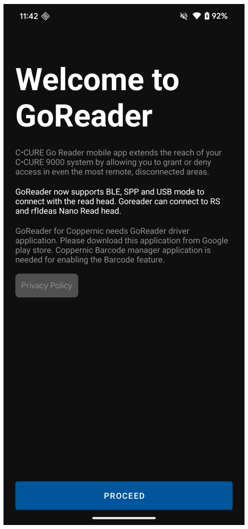
Figure 75: Notification access request



Allow **GoReader** to send you notifications?

3. Tap **Proceed** on the welcome screen. To view the privacy policy before continuing, tap the **Privacy Policy** button. See Figure 76.

Figure 76: Welcome screen



Welcome to GoReader

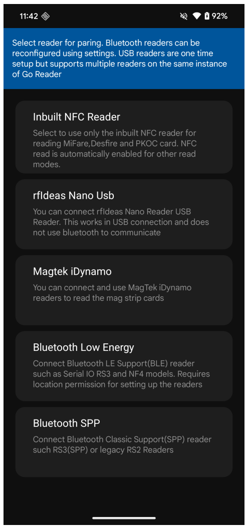
C•CURE Go Reader mobile app extends the reach of your C•CURE 9000 system by allowing you to grant or deny access in even the most remote, disconnected areas.

GoReader now supports BLE, SPP and USB mode to connect with the read head. Goreader can connect to RS and rfIdeas Nano Read head.

GoReader for Coppernic needs GoReader driver application. Please download this application from Google play store. Coppernic Barcode manager application is needed for enabling the Barcode feature.

4. Select the appropriate reader mode as shown in Figure 77. Tap **YES** to confirm and accept the reader mode message.

Figure 77: Reader modes



Select reader for paring. Bluetooth readers can be reconfigured using settings. USB readers are one time setup but supports multiple readers on the same instance of Go Reader

Inbuilt NFC Reader

Select to use only the inbuilt NFC reader for reading MiFare,Desfire and PKOC card. NFC read is automatically enabled for other read modes.

rfIdeas Nano Usb

You can connect rfIdeas Nano Reader USB Reader. This works in USB connection and does not use bluetooth to communicate

Magtek iDynamo

You can connect and use MagTek iDynamo readers to read the mag strip cards

Bluetooth Low Energy

Connect Bluetooth LE Support(BLE) reader such as Serial IO RS3 and NF4 models. Requires location permission for setting up the readers

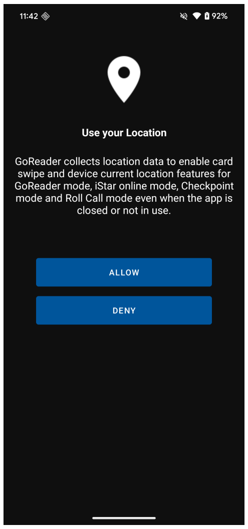
Bluetooth SPP

Connect Bluetooth Classic Support(SPP) reader such RS3(SPP) or legacy RS2 Readers

5. On the permissions screen, tap **ACCEPT** to accept all permissions for the Go Reader app.
   a. The following permissions display:
      i. Tap **ALLOW** to access the devices location.
      ii. Tap **ALLOW** to access photos, media, and files on your Go Reader device.
      iii. Tap **ALLOW** to make and manage phone calls.

   See an example in Figure 78. Tap **OK** to proceed. The Go Reader Identity screen displays.

Figure 78: Permissions screen

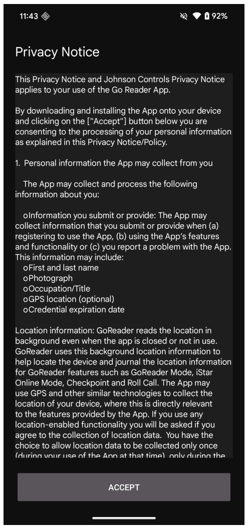


Use your Location

GoReader collects location data to enable card swipe and device current location features for GoReader mode, iStar online mode, Checkpoint mode and Roll Call mode even when the app is closed or not in use.

6. Select **Accept** on the Privacy Notice screen to proceed. See Figure 79.

Figure 79: Privacy notice screen



Privacy Notice

This Privacy Notice and Johnson Controls Privacy Notice applies to your use of the Go Reader App.

By downloading and installing the App onto your device and clicking on the ["Accept"] button below you are consenting to the processing of your personal information as explained in this Privacy Notice/Policy.

1. Personal information the App may collect from you

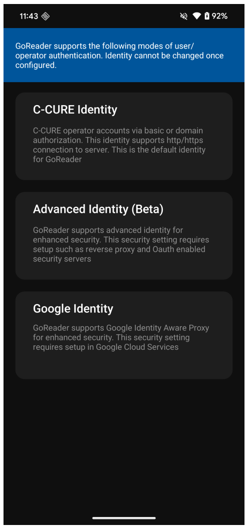
The App may collect and process the following information about you:

oInformation you submit or provide: The App may collect information that you submit or provide when (a) registering to use the App, (b) using the App’s features and functionality or (c) you report a problem with the App. This information may include:
oFirst and last name
oPhotograph
oOccupation/Title
oGPS location (optional)
oCredential expiration date

Location information: GoReader reads the location in background even when the app is closed or not in use. GoReader uses this background location information to help locate the device and journal the location information for GoReader features such as GoReader Mode, iStar Online Mode, Checkpoint and Roll Call. The App may use GPS and other similar technologies to collect the location of your device, where this is directly relevant to the features provided by the App. If you use any location-enabled functionality you will be asked if you agree to the collection of location data. You have the choice to allow location data to be collected only once (during your use of the App at that time), only during the

7. Tap **C•CURE Identity** to proceed. For more information on the **Advanced Identity (Beta)** option, see Go Reader Identity: Advanced identity (beta) mode. See Figure 80.

Figure 80: Identity mode options screen



GoReader supports the following modes of user/operator authentication. Identity cannot be changed once configured.

C-CURE Identity

C-CURE operator accounts via basic or domain authorization. This identity supports http/https connection to server. This is the default identity for GoReader

Advanced Identity (Beta)

GoReader supports advanced identity for enhanced security. This security setting requires setup such as reverse proxy and Oauth enabled security servers

Google Identity

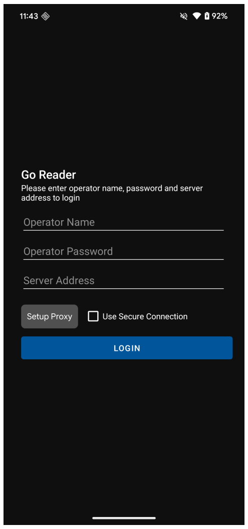
GoReader supports Google Identity Aware Proxy for enhanced security. This security setting requires setup in Google Cloud Services

8. Enter your username, password, and server IP on the screen, then tap **Login** to proceed. See Figure 81.
   a. In the **Operator Name** field, type your operator name. If you are a member of a domain, the format is `<domain name>` or `<username>`.
   b. In the **Operator Password** field, type your password.
   c. Choose between the following options:
      - If vWS is installed locally on the C•CURE server, in the **Server Address** field, enter the C•CURE server IP address.
      - If vWS is installed remotely, in the **Server Address** field, enter the vWS system IP address.
   d. **Optional**: If you log on to the app across an unsecured network, tap **Use Secure Connection** to clear the check box. Otherwise, ensure that the check box is selected.
   e. **Optional**: If you need a certificate, tap **Certificate**.

f. **Note:**

- victor Web Service must be associated with a verifiable and trusted server certificate that is signed by a globally trusted certification authority.
- Devices that run the Go Reader application must have a trusted root certificate installed. This enables the client device to establish a secure connection and complete the transport layer security (TLS) handshake.

Figure 81: Trusted root certificate installation



11:43 92%

Go Reader

Please enter operator name, password and server address to login

Operator Name

Operator Password

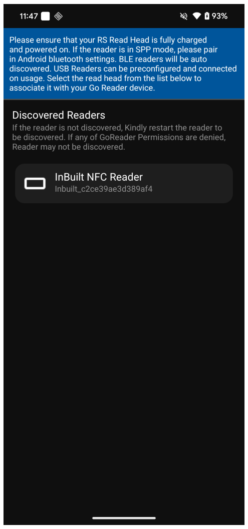
Server Address

Setup Proxy ☐ Use Secure Connection

LOGIN

9. If the log on credentials are verified, the **Discovered Readers** screen is displayed with a list of readers, as shown in Figure 82. Select any reader from the list and tap **Yes** to confirm registration.

Figure 82: List of available readers



11:47 93%

Please ensure that your RS Read Head is fully charged and powered on. If the reader is in SPP mode, please pair in Android bluetooth settings. BLE readers will be auto discovered. USB Readers can be preconfigured and connected on usage. Select the read head from the list below to associate it with your Go Reader device.

Discovered Readers

If the reader is not discovered, Kindly restart the reader to be discovered. If any of GoReader Permissions are denied, Reader may not be discovered.

InBuilt NFC Reader
Inbuilt_c2ce39ae3d389af4

10. The Go Device object is created in the C•CURE 9000 Administration Station. See C•CURE Go device editor. For information about enabling the C•CURE Go Reader, see Activating the Go Reader.
11. If activation is successful, the C•CURE Go Reader home screen displays.
12. **Optional:** Tap the **Menu** icon at the top left of the screen, then tap **About** to view the Go Reader version, host name operator name, and current identity.

13. **Optional:** Tap the **Menu** icon at the top left of the screen, then tap **Help** to access the Go Reader page on the Software House portal.

    Note:

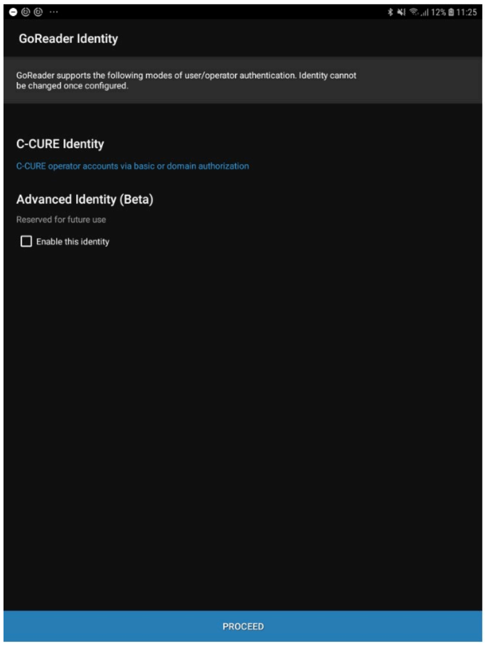
    - After the C•CURE Go Reader connects to the C•CURE 9000 server, all C•CURE 9000 data for personnel,credentials, clearance, holidays and schedules are downloaded to the C•CURE Go Reader. See C•CURE Go Reader clearances.
    - If you have not paired your device with a Bluetooth reader, the app directs you to the Bluetooth settings module of your Android device. Select the Bluetooth reader that you want to pair with your device.

Go Reader Identity: Advanced identity (beta) mode

To use the **Advanced Identity (Beta)** mode, complete the following steps:

1. Complete steps 1 to 3 of Launching the C•CURE Go Reader app.
2. Tap **Advanced Identity (Beta)**, then tap **Enable this identity**. See Figure 83.
3. Tap **OK** to confirm. See Figure 84.
4. Tap **Proceed**, then tap **SIGN IN** and enter the credentials provided by the operator.
5. Tap **Certificate** to get the certificate and tap **Login** to access the device.

Figure 83: Go Reader Identity screen



GoReader Identity

GoReader supports the following modes of user/operator authentication. Identity cannot be changed once configured.

C-CURE Identity

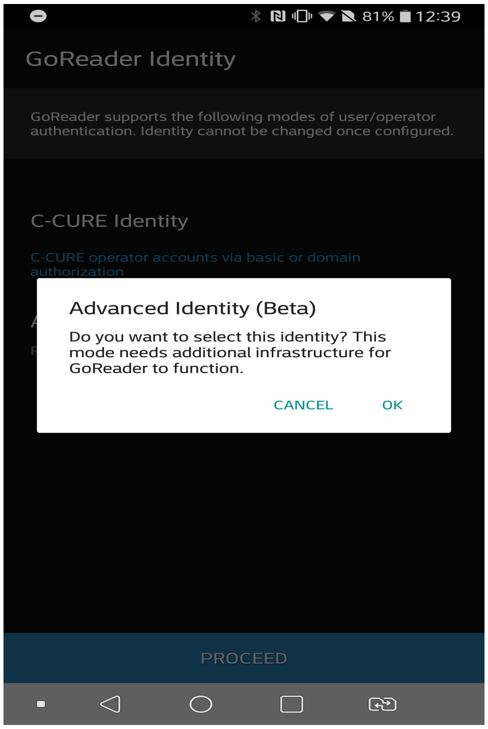
C-CURE operator accounts via basic or domain authorization

Advanced Identity (Beta)

Reserved for future use

□ Enable this identity

Figure 84: Advanced Identity option



GoReader Identity

GoReader supports the following modes of user/operator authentication. Identity cannot be changed once configured.

C-CURE Identity

C-CURE operator accounts via basic or domain authorization

Advanced Identity (Beta)

Do you want to select this identity? This mode needs additional infrastructure for GoReader to function.

C•CURE Go Reader notifications

The C•CURE Go Reader app sends notifications to your Android device to indicate connectivity to the C•CURE 9000 server. The following table lists the C•CURE Go Reader app notifications.

Table 32: C•CURE Go Reader notifications

Notification Icon	Description
🟢	Connected to server.
🟡	Log on failed.
🔴	• Disconnected from server. • Device disabled from C•CURE.

C•CURE Go Reader driver status and notifications

The following C•CURE Go Reader driver notifications are sent to the C•CURE Go Reader app.

Table 33: C•CURE GoReader driver status and notifications

Status and Notification	Description
Connection to victor Web Service.	C•CURE Go Reader app has established a connection with victor Web Service.
Disconnected from victorWeb Service.	C•CURE Go Reader app cannot establish a connection with victor Web Service.
C•CURE GoReader Extension Service is stopped. All the Extension Service dependent operations are queued and triggered when the C•CURE Go Reader Extension Service is running.	C•CURE Go Reader driver service is stopped.
Unable to reach victor Web Service. Check if victor Web Service is online or data connection is activated in device.	C•CURE Go Reader app cannot connect to the victor Web Service.

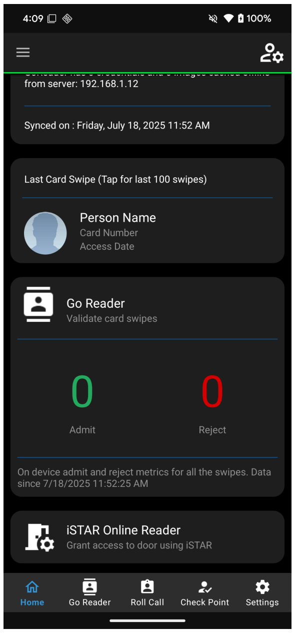
Home screen

The home screen is displayed after successful log on and activation of the C•CURE Go Reader device. It contains a list of C•CURE Go Reader app modules. Tap the different links to access them.

Information about the reader connected to the device, including the number of credentials and images synchronized displays at the top of the home screen. After synchronization completes, the last sync time displays. See Figure 85.

You can access options from the home screen or the side menu. See Table 34 for information on the options. To access options from the side menu, tap the menu icon. See Figure 86.

Figure 85: C•CURE Go Reader app home screen - Android



4:09 100%

from server: 192.168.1.12

Synced on : Friday, July 18, 2025 11:52 AM

Last Card Swipe (Tap for last 100 swipes)

Person Name
Card Number
Access Date

Go Reader
Validate card swipes

0
Admit

0
Reject

On device admit and reject metrics for all the swipes. Data since 7/18/2025 11:52:25 AM

iSTAR Online Reader
Grant access to door using iSTAR

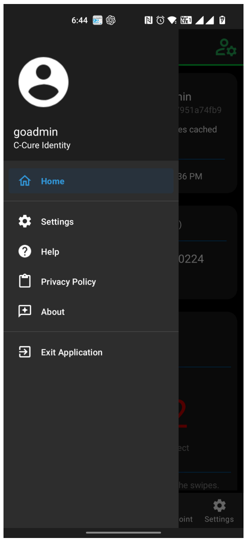
Table 34: Home screen and menu options

Option	Description
Home screen options	
Last Card Swipe	Displays the last swiped card details. Tap this button to display the history of swipe activity on the Go Reader device.

Table 34: Home screen and menu options

Option	Description
Go Reader	Displays the total count of admitted and rejected credentials on the device. Tap this button to launch the C•CURE Go Reader module or swipe and show screen. Select to view card information after a card swipe.
iStar Online Reader	Tap this button to navigate to the iStar Online Reader mode. See iSTAR online reader screen for more information.
Bottom Navigation Bar	
Home	Tap this button to navigate back to the Home screen.
Go Reader	Tap this button to launch the C•CURE Go Reader module or swipe and show screen. Select to view card information after a card swipe.
Roll Call	Tap this button to navigate to the Roll Call screen, to view missing persons and area information for missing persons.
Check Point	Tap this button to navigate to the Check Point screen, to create check points and manage list of swiped in personnel.
Settings	Tap this button to navigate to the Settings screen, to view and configure General, Database and Advanced settings options.
Side Menu	
Home	Tap this button to navigate back to the Home screen.
Settings	Tap this button to navigate to the Settings screen, to view and configure General, Database and Advanced settings options.
Help	Tap this button to view to the Go Reader product page on the Software House Portal.
Privacy Policy	Tap this button to view to the Go Reader privacy policy.
About	Tap this button to view the About screen and view the Go Reader version, host name, operator name, and current identity.
Exit	Tap this button to close the application.

Figure 86: C•CURE Go Reader app side menu

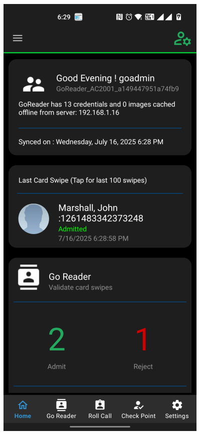


Using the access metrics widget on the Go Reader app

You can view card swipe information on the access metrics widget on the Go Reader app Home screen. The access metrics widget displays the number of admitted and rejected card swipes.

- On the **Home** screen, tap **Go Reader**.

Figure 87: C•CURE Go Reader app - Access metrics widget



Good Evening ! goadmin
GoReader_AC2001_a149447951a74fb9

GoReader has 13 credentials and 0 images cached offline from server: 192.168.1.16

Synced on : Wednesday, July 16, 2025 6:28 PM

Last Card Swipe (Tap for last 100 swipes)

Marshall, John
:1261483342373248
Admitted
7/16/2025 6:28:58 PM

Go Reader
Validate card swipes

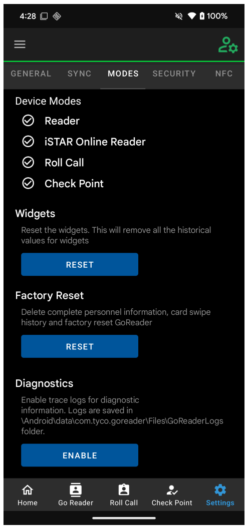
2 Admit
1 Reject

Resetting access metrics widget data

To reset metrics data on the access metrics widget, complete the following steps:

1. In the Go Reader app, on the **Home** screen, tap **Settings**.
2. In **Settings**, on the **Modes** tab, in the **Widgets** pane, tap **RESET**.

Figure 88: C•CURE Go Reader app - Widget reset



Device Modes
- ✓ Reader
- ✓ iSTAR Online Reader
- ✓ Roll Call
- ✓ Check Point

Widgets
Reset the widgets. This will remove all the historical values for widgets

Factory Reset
Delete complete personnel information, card swipe history and factory reset GoReader

Diagnostics
Enable trace logs for diagnostic information. Logs are saved in \Android\data\com.tyco.goreader\Files\GoReaderLogs folder.

The previous data is removed and the metrics data is reset.

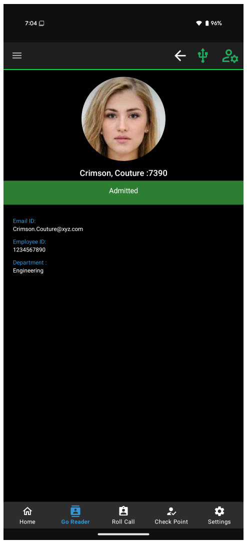
C•CURE Go Reader screen

The C•CURE Go Reader screen displays the card status when a card is swiped on the Bluetooth enabled Serialio idChamp RS3 card reader. The C•CURE Go Reader module has a read-only function and is accessed from the C•CURE Go Reader Home screen.

After swiping a card, the following outcomes appear on the screen:

- If the person has access to the clearance configured to the C•CURE Go Reader app, the card status is displayed as **Admitted**, as shown in Figure 89.
- If the person does not have access to the clearance configured in the C•CURE Go Reader app, the card status is displayed as **Rejected**.
- If the card is not registered in the C•CURE 9000 system, the card number displays on the screen.
- If you configured additional swipe screen information to add extra details, these display on the screen. See Use custom data fields for swipe and roll call for information on adding additional swipe screen information.
- If you enabled facility code validation and there is a facility code mismatch, the card status is displayed as **Rejected (Facility Code Mismatch)**.

Figure 89: C•CURE Go Reader screen on Android device



Crimson, Couture :7390

Admitted

Email ID:
Crimson.Couture@xyz.com

Employee ID:
1234567890

Department :
Engineering

iSTAR online reader screen

On the iSTAR Online Reader screen you can grace personnel, view reader statuses, cardholder information, admit or reject statuses, cardholder swipe history, and passback alerts. To access the iSTAR Online Reader screen, from the home screen, tap **iSTAR Online Reader**.

iSTAR Online Reader mode enables the Go Reader device to assume the identity of an actual iSTAR reader, from an online iSTAR controller, such as iSTAR Pro, iSTAR eX, iSTAR Edge, or iSTAR Ultra/Ultra SE with the required firmware revision update. You can use the Go Reader device to enforce anti-passback control, using the areas that have been configured on the iSTAR.

For more information on navigating the iSTAR Online Reader screen in the Go Reader app, see Navigate the iSTAR Online Reader screen on the Go Reader app.

To update the Go Reader driver service config file, see Updating the Go Reader driver service config file.

For more information on the antipassback feature in the iSTAR Online Reader screen, see Anti-passback feature in the iSTAR online reader screen.

Navigate the iSTAR Online Reader screen on the Go Reader app

You can view the following information on the iSTAR online reader screen in the Go Reader app:

- Reader statuses
- Cardholder information

- Admit or reject statuses
- Cardholder swipe history
- Passback alerts

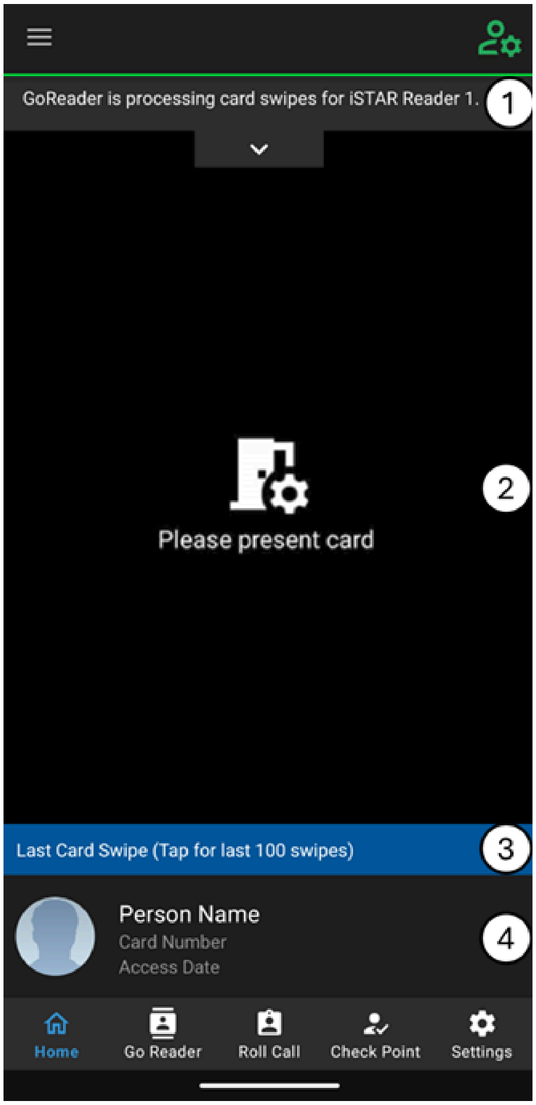
For more information, see Table 35.

Note:

- If your device is not connected to the server, you cannot access the iSTAR Online Reader screen.
- If your device is connected to the server but the iSTAR driver is offline or is not running, the following message displays on the iSTAR Online Reader: `iSTAR offline: GoReader cannot process card swipes`

  To troubleshoot the iSTAR driver, refer to the documentation of your C•CURE 9000 iSTAR driver.

Figure 90: iSTAR Online Reader screen user interface



GoReader is processing card swipes for iSTAR Reader 1.

Please present card

Last Card Swipe (Tap for last 100 swipes)

Person Name
Card Number
Access Date

Table 35: iSTAR Online Reader screen interface elements

Callout	Name	Description
1	Reader selector	Displays status information about an inbound or outbound reader.
		Expand the menu to select a different reader type. By default, the inbound reader displays.
2	Card swipe information	Displays the following card swipe details: • Admit or reject status • Passback alert or clearance
3	Swipe history	Tap to view the last 100 card swipes in the Swipe History screen. You can download the swipe history in PDF format.
4	User data	Displays the user name, card number, last card swipe, and the admit or reject date.

Updating the Go Reader driver service config file

The default poll interval for the iSTAR Online Reader driver is 30 seconds. To update the Go Reader driver service config file, complete the following steps:

1. Open the Go Reader Driver Service Config file at the following path: `...\CrossFire\ServerComponents \GoReader Driver Service.exe.config`
2. Append the following key to the config file: `add key="iStarProbePollInterval" value="30000" /`

   ⓘ **Note:** The time you enter for value is in milliseconds. In the example above, as the default poll interval for the iSTAR Online Reader driver is 30 seconds, enter 30000 milliseconds.

3. Save the config file.

Anti-passback feature in the iSTAR online reader screen

Anti-passback prevents personnel from passing back a card for another person to swipe. You can use the anti-passback feature on Android and C-One² devices.

For more information on anti-passback pre-requisites, see Anti-passback prerequisites.

For more information on anti-passback configuration for a Go Reader door object in the server, see Anti-passback configuration for a Go Reader door object in the server.

To authorize users and devices and grace personnel in the server, see Authorizing users and devices and gracing personnel in the server.

For more information on swiping with timed anti-passback, see Card swiping with timed anti-passback on the Go Reader app.

For more information on anti-passback use cases, see Anti-passback use cases.

Anti-passback prerequisites

To support anti-passback, the Go Reader integration uses the 2FA API to receive information from an iStar controller. An example of this information is the reject or admit information of a cardholder. The type of 2FA depends on the firmware version of your iSTAR devices. For more information on iSTAR devices and the firmware versions that support 2FA, see Table 36:

Table 36: iSTAR devices and the firmware versions that support 2FA

Device	Firmware version
iSTAR Ultra	v6.5.2 or later
iSTAR Ultra SE	v6.5.2 or later

Table 36: iSTAR devices and the firmware versions that support 2FA

Device	Firmware version
iSTAR Ultra LT	v6.5.2 or later
iSTAR Edge/Ex	v6.2.6 or later
iSTAR Pro	v5.2.D or later

Anti-passback configuration for a Go Reader door object in the server

You can configure the following anti-passback options for a door object:

- **Inbound Reader:** This option is mandatory. For more information on readers, refer to *C•CURE Hardware Configuration Guide*.
- **Outbound Reader:** This option is not mandatory. For more information on readers, refer to *C•CURE Hardware Configuration Guide*.
- **Grace Personnel:** This option is not mandatory. For more information on gracing personnel, see Gracing personnel use case or refer to Antipassback Grace in *C•CURE Areas and Zones Guide*.

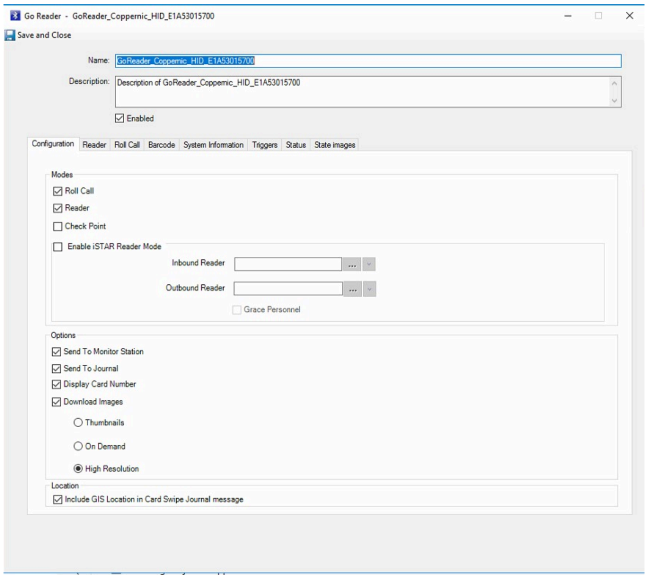
To select one or more of these options, see Configuring a door object for anti-passback.

Configuring a door object for anti-passback

1. On the **Configuration tab** of the Go Reader editor, in the **Modes** area, select **Enable iSTAR Reader Mode**.
2. In the **Inbound Reader** field, type the name of the inbound reader or click the browse button to browse to the inbound reader you want to configure.
3. In the **Outbound Reader** field, type the name of the outbound reader or click the browse button to browse to the outbound reader you want to configure.
4. **Optional**: To activate the personnel gracing, select the **Grace Personnel** check box.

   If a card is rejected due to anti-passback, you can accept the card manually on the Go Reader app.

Figure 91: Configuring a door object for anti-passback in the editor



Go Reader - GoReader_Coppernic_HID_E1A53015700

Name: GoReader_Coppernic_HID_E1A53015700

Description: Description of GoReader_Coppernic_HID_E1A53015700

☑ Enabled

Modes

☑ Roll Call

☑ Reader

□ Check Point

□ Enable iSTAR Reader Mode

Inbound Reader

Outbound Reader

□ Grace Personnel

Options

☑ Send To Monitor Station

☑ Send To Journal

☑ Display Card Number

☑ Download Images

○ Thumbnails

○ On Demand

● High Resolution

Location

☑ Include GIS Location in Card Swipe Journal message

Authorizing users and devices and gracing personnel in the server

The iSTAR Online Reader appears in the Go Reader app Home screen. To authorize iSTAR Online Reader cardholder access, complete the following steps in the Go Reader editor:

1. On the **Configuration** tab of the Go Reader editor, in the **Modes** area, select **Enable iSTAR Reader Mode**.

2. In the **Inbound Reader** field, type the name of the inbound reader or click the browse button to browse to the inbound reader you want to configure.
3. In the **Outbound Reader** field, type the name of the outbound reader or click the browse button to browse to the outbound reader you want to configure.
4. **Optional:** To enable the personnel gracing, select **Grace Personnel**. For more information on gracing personnel, refer to anti-passback grace in *C•CURE Areas and Zones Guide*.
5. Click **Save and Close**.

   Go Reader Message dialog box appears with the following message: `Make sure iSTAR driver is running and controller is online to use this feature.`
6. Click **OK**.

The user can now access the iSTAR Online Reader from the Go Reader app Home screen.

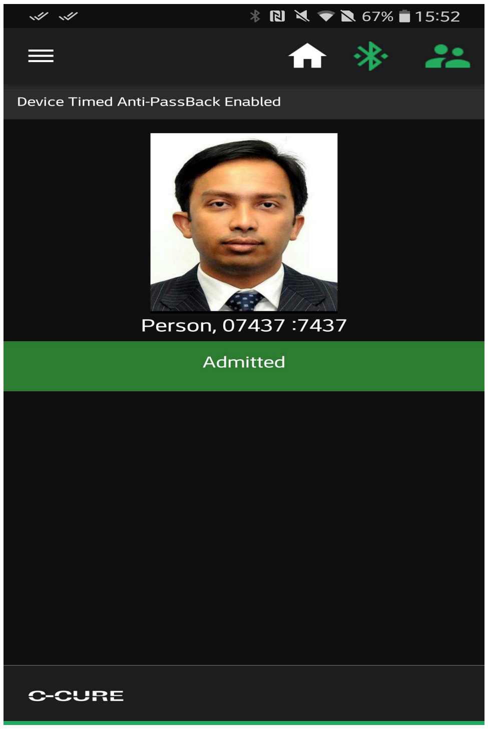
Card swiping with timed anti-passback on the Go Reader app

If you activate timed anti-passback in the Go Reader editor, you can use the Go Reader app to reject card swipes in your chosen time frame. See Activating timed anti-passback for more information on configuring timed anti-passback.

1. On the C•CURE Go Reader Home screen, tap **GoReader**.

   The Go Reader module opens on the **Home** screen. If you have enabled timed anti-passback, **Device Timed AntiPassback Enabled** displays in a banner on the screen.
2. Swipe a person's card to admit them to the clearance. The card status displays as **Admitted**, as shown in Figure 92.

Figure 92: Admitted with timed anti-passback



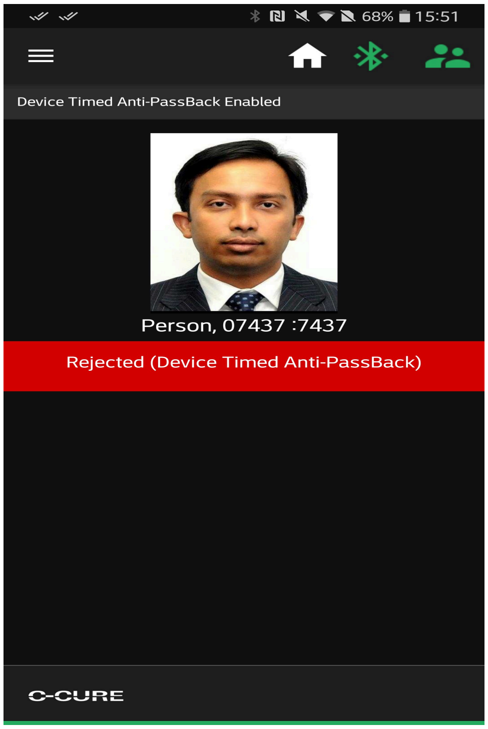
Device Timed Anti-PassBack Enabled

Person, 07437 :7437

Admitted

3. Swipe the same person's card during the anti-passback duration. The card displays as **Rejected**, as shown in Figure 93.

Figure 93: Rejected with timed anti-passback



Device Timed Anti-PassBack Enabled

Person, 07437 :7437

Rejected (Device Timed Anti-PassBack)

Anti-passback use cases

The following use cases apply to the anti-passback feature in the Go Reader app:

- Normal anti-passback enforcement for both iSTAR areas. For more information, see Normal anti-passback enforcement for both areas use case.
- Timed anti-passback enforcement for both iSTAR areas . For more information, see Timed anti-passback enforcement for both areas use case.
- Carpool. For more information, see Setting up carpool anti-passback.
- Gracing personnel. For more information, see Gracing personnel use case.
- Downloading swipe history information. For more information, see Normal anti-passback enforcement for both areas use case.

Normal anti-passback enforcement for both areas use case

In the following use case scenario, the anti-passback enforcement type is normal for both areas.

1. The users elects the inbound reader and swipes the card.
2. In the Monitoring Station, two journal messages log.
3. If the same card reads a second time on the same inbound reader, an anti-passback alert triggers and the card is rejected. The following alert appears in the iSTAR Online Reader and two passback alerts log on the journal: `Rejected (Passback)`
4. To admit the card, on the iSTAR Online Reader screen, swipe down to open the reader selector menu and select the outbound reader.
5. The cardholder swipes the card.

The cardholder is removed from the area.

Timed anti-passback enforcement for both areas use case

In the following use case scenario, the anti-passback enforcement type for both areas is timed.

1. Set **Trigger violation on re-entry within** to the re-entry violation time you want. For more information, see Activating timed anti-passback.
2. From the **Home** screen, tap **iSTAR Online Reader**.
3. Swipe down to open the reader selector menu and select the inbound reader.
4. The cardholder swipes the card.
5. If the cardholder swipes the card in the **Trigger violation on re-entry within** value, the card is rejected. The following alert appears in the iSTAR Online Reader and two passback alerts log on the journal: `Rejected (Passback)`

Setting up carpool anti-passback

1. Create a carpool group. For more information on carpool anti-passback, refer to carpool anti-passback in *C•CURE Areas and Zones Guide*.
2. Add personnel to the carpool group.
3. In **Anti-passback Enforcement** type, activate **Antipassback**.
4. Select the carpool area and then select **Allow any personnel in carpool group to exit in area option**.

   ⓘ **Note:** You cannot use any anti-passback features on an area that is not a carpool area, even if it is adjacent to a carpool area.

5. A cardholder in the carpool group swipes the card.
6. If the same card swipes again on same inbound reader, the card is rejected. The following alert appears in the iSTAR Online Reader and two passback alerts log on the journal: `Rejected (Passback)`

Gracing personnel use case

To activate Grace Personnel, complete Step 4 in Authorizing users and devices and gracing personnel in the server.

For more information on gracing personnel, refer to Anti-passback Grace in *C•CURE Areas and Zones Guide*.

1. From the GoReader Home screen, tap **iSTAR Online Reader**.
2. To access the **Swipe History** screen, tap **Last Card Swipe (Tap for last 100 swipes)**.
3. Tap the check mark icon beside the rejected personnel record.
4. To grace the personnel, tap **OK**.

A success notification appears on the iSTAR Online Reader screen and two passback alerts log on the journal.

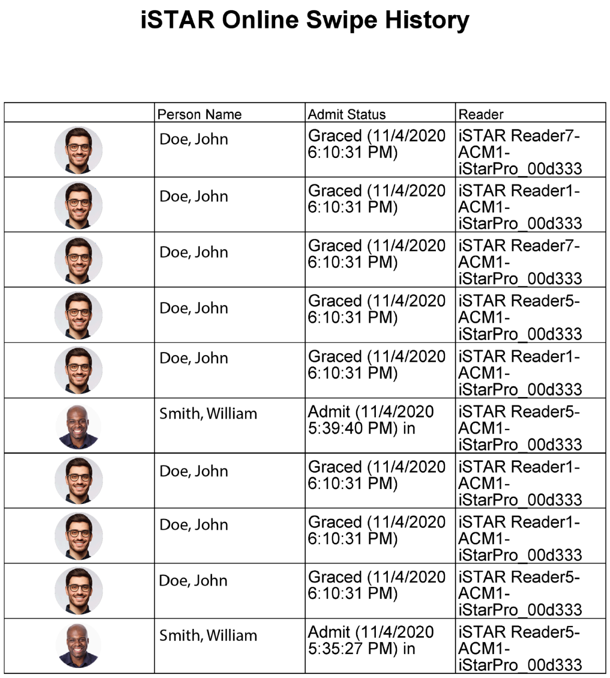
Downloading swipe history information use case

1. From the Go Reader **Home** Screen, tap **iSTAR Online Reader**.
2. To access the **Swipe History** screen, tap **Last Card Swipe (Tap for last 100 swipes)**.
3. Tap the **Download** icon.

The card swipe history downloads in PDF format. The file contains the following information:

- Primary image of personnel
- Personnel name
- Admit and reject status
- Reader information

Figure 94: iStar online swipe history



iSTAR Online Swipe History

	Person Name	Admit Status	Reader
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader7-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader1-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader7-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader5-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader1-ACM1-iStarPro_00d333
	Smith, William	Admit (11/4/2020 5:39:40 PM) in	iSTAR Reader5-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader1-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader1-ACM1-iStarPro_00d333
	Doe, John	Graced (11/4/2020 6:10:31 PM)	iSTAR Reader5-ACM1-iStarPro_00d333
	Smith, William	Admit (11/4/2020 5:35:27 PM) in	iSTAR Reader5-ACM1-iStarPro_00d333

Back to work features

This document describes the new features of the C•CURE Go Reader application that improve usability and activate Go Reader to be more effective in back-to-work scenarios. The features is supported on either the following Go Reader hardware platforms:

- Access-ER
- C-ONE²
- RS3

Temporary clearance filter

The Temporary Clearance Filter function was introduced in 2.70 SP7, 2.80 SP5 and 2.90 SP2. To support this function, use Online iSTAR Reader Mode and configure the necessary custom events.

ⓘ **Note:** Name the iSTAR door with an appropriate name that indicates that the Temporary Clearance Filter is in use.

Online validation mode

Online validation mode displays the most recent updated personnel data when a card is swiped at a Go Reader unit and efficiently validates all credentials in a C•CURE database.

In online validation mode, you can validate personnel records and credentials without checking clearances. This enables quick use of Go Reader on any C•CURE system without needing to assign clearances to the personnel.

When a cardholder swipes a card, the complete personnel record is fetched without downloading or synching. On a system with 250,000 personnel using a Wi-Fi connection, Go Reader processes the card swipe, retrieves the host data, and displays it on the screen in 2 to 3 seconds.

Online validation mode ignores clearances and instead validates the following values:

- Credential card number

- Credential facility code
- Credential activation
- Credential expiration dates
- Lost flags
- Disabled flags
- Stolen flags

ⓘ **Note:** You can use online validation mode if the Go Reader unit and the Go Reader app are both online.

Journal history in Go Reader mode

In the Go Reader journal history, you can view the last 100 transactions with Go Reader mode. The Go Reader journal history is similar to the journal history available in the current Online Reader mode.

Beeper settings

You can configure different beeper sound and number of beeps for admits and rejects in the Go Reader app settings. The following table displays the beep number and duration configuration options:

Table 37: Beep number and duration configuration options

Description	Admit	Reject
Number of beeps you can configure	1-3	1-3
Default number of beeps	One 5/10s beep	One 1s beep
Minimum beep duration	2/10s	2/10s
Maximum beep duration	3s	3s
Default beep duration	5/10s	1s

Duress button

Tap the duress button to signal a duress or assistance event to C•CURE. The duress icon is located on each screen and is similar to the Alert feature in C•CURE.

You can activate the duress button in the Go Reader app settings.

To send a duress signal with the duress button, see Sending a duress signal with the duress button.

If the Go Reader is offline, the icon is grayed out.

An event can be triggered, as a minimum through journal triggers.

Sending a duress signal with the duress button

1. Tap the duress button.
2. Type a comment in the dialog box.
3. Tap **SEND**.

The duress signal is sent and the comment is included in the journal. The Go Reader app delivers the activity message with the GIS location of the Go Reader to C•CURE.

Track Go Reader unit with GIS coordinates

You can track a Go Reader unit with GIS coordinates. Configure the beacon settings to send the GIS location to the C•CURE server at a predefined rate.

To map the Go Reader unit with OpenStreets maps, right-click on the Go Reader unit.

iSTAR online reader mode enhancements

You can use iSTAR Online Reader Mode functionality to assign different readers from different doors as Inbound or Outbound reader combinations. You can choose to assign only an Inbound reader or only an Outbound reader to a GoReader device, leaving the other reader slot empty.

Impersonate a door using the Go Reader app

Configure **Door Impersonation Mode** in the Go Reader editor to impersonate a particular door if there are issues with that door. It can also be used to access different clearance sets. See Impersonating a door for more information on configuration.

Card swiping with door impersonation

1. On the C•CURE Go Reader Home screen, tap **GoReader**.

   If you have enabled **Door Impersonation Mode**, **Impersonate Door Enabled** displays in a banner on the screen and the name of the impersonated door displays instead of a Go Reader door.
2. Swipe a person's card to admit them at the impersonated door. The card status displays as **Admitted** or **Rejected**.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you activate or disable **Door Impersonation Mode**, the changes are sent when the device comes online, connects to the server, and synchronization is initiated.

Roll call

Use the roll call feature to view and manage personnel during an emergency. The roll call feature uses up-to-date information on personnel and their iSTAR area status to identify personnel that are not accounted for.

You can use the roll call feature when the GoReader app is connected to the C•CURE server.

Access the **Roll Call** module from the **Home Screen** of the C•CURE Go Reader app. It consists of two modules:

- **Home** - Displays the number of missing personnel and last card swipe information.
- **Area Information** - Displays the amount of card users located outside of the roll call area. Tap an area link to view personnel information in that area.

Roll call home screen

Use the **Roll Call Home Screen** to view the number of personnel missing from the roll call area. When a card is swiped on the Bluetooth enabled Serialio idChamp RS3 card reader, the number of missing people is reduced. When the count reads `0`, it is inferred that there are no more missing personnel.

If you configured additional swipe screen information to add extra details, these display on the screen. See Use custom data fields for swipe and roll call for information on adding additional swipe screen information.

Area information screen

Use the **Area Information Screen** to view details of cardholders located outside the roll call area.

Tap an **Area** to view information about personnel located in that area. When an area is tapped, a list of personnel inside that area is displayed. You can download orsend an email of the details of all missing personnel.

The following icons are displayed in an area:

Table 38: Area information screen

Icon	Description	Action
⬇	Download	Tap to download a PDF file containing the details and portraits of missing personnel.
✉	Send email	Tap to send details of the missing personnel in an email.

Viewing personnel in a missing area

Use the **Area Information** module in **Roll Call** to view credential details about personnel in a missing area.

1. On the C•CURE Go Reader **Home** screen, tap **Roll Call**.
   The Roll Call module opens on the **Home** screen.
2. Choose between:
   - Tap **Area Information**.
   - On the Roll Call **Home** screen, swipe from right to left .
3. Tap the **Area** that you want to view.

A list of personnel in the missing area displays.

Setting the maximum personnel for roll call display

Use the **General Settings** tab to configure the number of personnel displayed in an area when it is selected from the **Area Information** screen.

1. On the C•CURE Go Reader **Home** screen, tap **Settings**.
   The **Settings** module opens on the **General** screen.
2. Tap the drop down list under **Max Personnel for Roll Call Area Display**.
3. Select one of the following values:
   - 100
   - 1000
   - 10000

The value selected sets the personnel count displayed in an area when it is selected from the **Area Information** screen.

Manual mustering with roll call

Use the **Roll Call** module to manually muster a person if they do not have access to their card. Ensure that **Allow Manual Mustering** is enabled on the Go Reader editor. See Using manual mustering with the roll call screen for more information.

1. On the C•CURE Go Reader **Home** screen, tap **Roll Call**.
2. Tap **Search for people**.
3. Type the name of the person you want to manually muster. A list of matching people displays.
4. Tap the name of the person you want to manually muster. A message displays that says `Muster <Person Name>?`.
5. Choose between:
   - Tap **YES**. This musters the person to the roll call area.
   - Tap **NO**. This does not muster the person to the roll call area.

Roll-Call with previous doors

Use this feature to view details about personnel who accessed the Missing Area along with the last swiped access door. This feature aims to improve security and tracking of personnel movements.

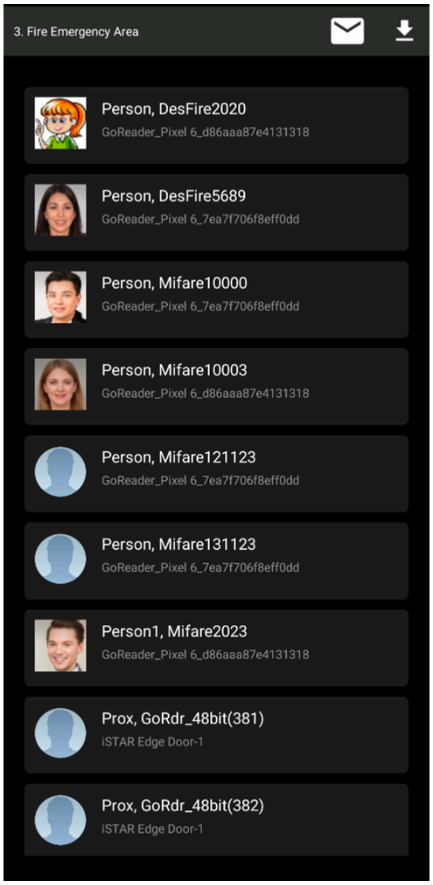
1. On the C•CURE Go Reader Home screen, tap **Roll Call**.

   The Roll Call module opens on the Home screen.
2. Tap **Area Information** and tap the **Area** that you want to view.

   A list of missing area displays.
3. Tap any one of the listed **Missing Area**.

- The personnel details display along with Go Reader name and the last swiped access door name.
- The name of that iSTAR Door displays in the Area Information field when personnel swipe card on any iSTAR Door.

Figure 95: Missing area information



3. Fire Emergency Area

Person, DesFire2020
GoReader_Pixel 6_d86aaa87e4131318

Person, DesFire5689
GoReader_Pixel 6_7ea7f706f8eff0dd

Person, Mifare10000
GoReader_Pixel 6_7ea7f706f8eff0dd

Person, Mifare10003
GoReader_Pixel 6_d86aaa87e4131318

Person, Mifare121123
GoReader_Pixel 6_7ea7f706f8eff0dd

Person, Mifare131123
GoReader_Pixel 6_7ea7f706f8eff0dd

Person1, Mifare2023
GoReader_Pixel 6_d86aaa87e4131318

Prox, GoRdr_48bit(381)
iSTAR Edge Door-1

Prox, GoRdr_48bit(382)
iSTAR Edge Door-1

Check point

Use **check point** mode to create check points and manage a list of swiped in personnel. Check point mode is also referred to as field trip mode, or bus mode. Use check point mode to manage personnel as they enter and exit a check point. Use check in mode to keep track of personnel who swipe on to a bus and use check out mode to keep track of personnel who swipes off of the bus. You can then identify if any personnel is missing from the original check in group.

Access **check point** mode from the **home screen** of the C•CURE Go Reader app.

The following icons are displayed in the **check point** module:

Table 39: Check point module

Icon	Description	Action
⊕	Create a check point icon	Tap to create a check point.
←	Check out mode	Displays that the check point has check out mode enabled. Tap to activate check in mode.
→	Check in mode	Displays that the check point has check in mode enabled. Tap to activate check out mode.
🔒	Validation mode	Displays that the check point is in validation mode. Tap to disable validation mode.
🔓	Validation mode disabled	Displays that the check point is not in validation mode. Tap to activate validation mode.
⋮	Filter mode	Tap to display **View All**, **View Unchecked**, and **View Checked** options.
⤓	Download	Tap to download a PDF file of the personnel list for the check point.
🗑	Delete	Tap to delete the selected check point.

ⓘ **Note:** You cannot navigate to the **Check Point** module if it is disabled in C•CURE 9000. If you tap Check Point on the Go Reader app when it is disabled this message displays: `Check Point option is not authorized for this device.`

Ensuring check point is activated

Navigate to the settings screen to see if the check point module is activated.

1. In the Go Reader app, on the **Home** screen, tap **Settings**.
2. Tap **Advanced**. The device modes that are activated and disabled are displayed.

Creating a check point

Use the **check point** module to create a check point.

ⓘ **Note:**

- If you download and install Go Reader application v5.0.238 and above, you can create up to ten check points.
- If the Go Reader device is not connected to the server when you create a checkpoint, the journal message displays when the device comes online and connects to the server.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.
2. Tap the **Create a Check Point** icon.
3. In the **Enter a Check Point name** field, type a name for the check point.
4. Tap **OK** to save your changes.

The check point displays in the check point module with a record of the creation date. If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

Removing a check point

Use the **check point** module to remove a check point.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.
2. Tap the **Delete** icon next to the check point that you want to remove.
3. To remove the selected check point, tap **OK**.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you remove a check point, the journal message displays when the device comes online and connected to the server.

Activating check in mode

Use the active **check point** screen to activate check in mode.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.
2. Tap the name of the check point to open the active **Check Point** screen.
3. Tap the **Check Out mode** icon to activate Check In mode. The message `Check-In mode enabled for '<Name of Check Point>'` displays on the app.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you activate check in mode, the journal message displays when the device comes online and connects to the server.

Activating check out mode

Use the active **check point** screen to activate check out mode.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.

   The check point module opens on the **Home** screen.
2. Tap the name of the check point to open the active **Check Point** screen.
3. Tap the **Check In mode** icon to activate check out mode.

   The message `Check-Out mode enabled for '<Name of Check Point>'` displays on the app.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you activate check out mode, the journal message displays when the device comes online and connected to the server.

Activating validation mode

Use the **Check Point** screen to activate validation mode. When validation mode is activated, users can manually remove and check in personnel in check point.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.
2. Tap the name of the check point to open the active **Check Point** screen.
3. Tap the **Validation mode** icon to activate validation mode.

   The message `Validation mode enabled for '<Name of Check Point>'` displays on the app.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

   ⓘ **Note:** Validation mode is disabled by default.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

ⓘ **Note:** If the Go Reader device is not connected to the server when you activate check out mode, the journal message displays when the device comes online and connects to the server.

Disabling validation mode

Use the active **check point** screen to disable validation mode.

1. On the C•CURE Go Reader **Home** screen, tap **Check Point**.
2. Tap the name of the check point to open the active **Check Point** screen.
3. Tap the **Validation mode disabled** icon to disable validation mode.

   The message `Validation mode disabled for '<Name of Check Point>'` displays on the app.

   If the Go Reader device is connected to the server, a journal message displays in the Monitoring Station.

   ⓘ **Note:** If the Go Reader device is not connected to the server when you activate check out mode, the journal message displays when the device comes online and connects to the server.

Checking in personnel when validation mode is activated

1. Tap the **Validation mode** icon to activate validation mode.
2. Tap the name of the person you want to check in and swipe left. A message displays that says `Click to check-in`.
3. Tap **Click to check-in** to check the person in to the check point.

A journal message with this information is sent to the Monitoring Station.

Removing personnel when validation mode is activated

1. Tap the **Validation mode** icon to activate validation mode.
2. Tap the name of the person you want to remove and swipe right. A pop-up message displays that says `Remove <Person Name> from <Check Point Name>?`.
3. Choose between:
   - Tap **YES**. This removes the person from the check point list.
   - Tap **NO**. This does not remove the person from the check point list.

A journal message with this information is sent to the Monitoring Station.

View personnel in filter mode

Tap the Filter mode icon to display **View All**, **View Unchecked**, and **View Checked** options.

- Select **View All** to view all personnel information in the check point.
- Select **View Unchecked** to view unchecked personnel information in the check point.
- Select **View Checked** to view checked in personnel information in the check point.

Downloading personnel lists for check point

- On the check point screen, tap the **Download** icon to download a PDF file of the list of personnel for the check point.

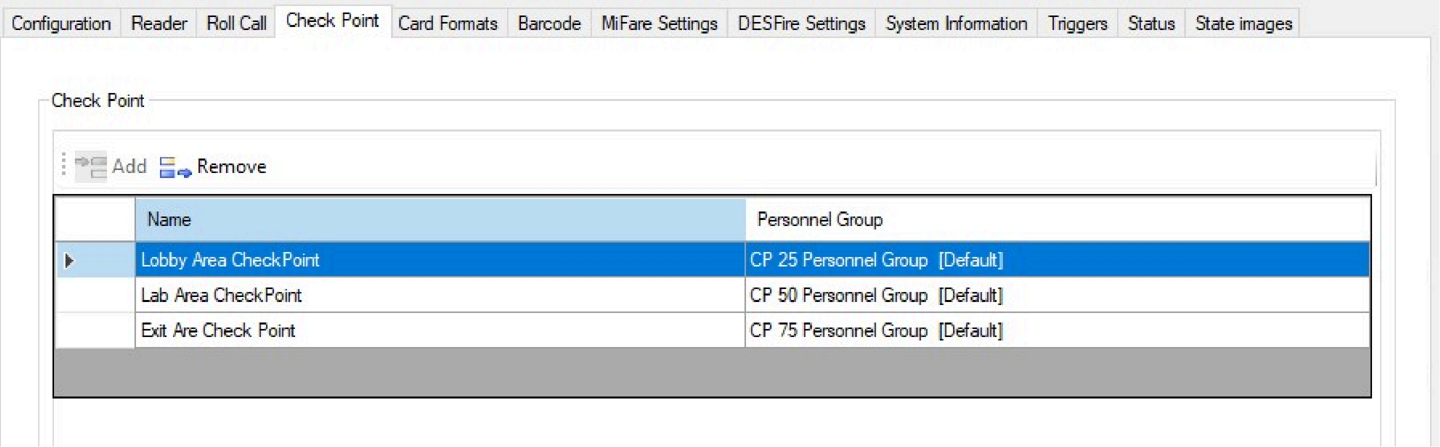
  The PDF file is created and saved under Go Reader Log folders on the Go Reader device.

Server based check points

Server based check points feature is also known as reverse occupancy.

The Go Reader driver sends check points from the server to mobile devices. The server can create up to three check points and send to each mobile device. These check points can accommodate up to 100 personnel, that is used to count reverse occupancy of a particular area or zone. These 100 personnel for each check point are assigned by **Personnel Group** from the server.

Figure 96: Check point assignment

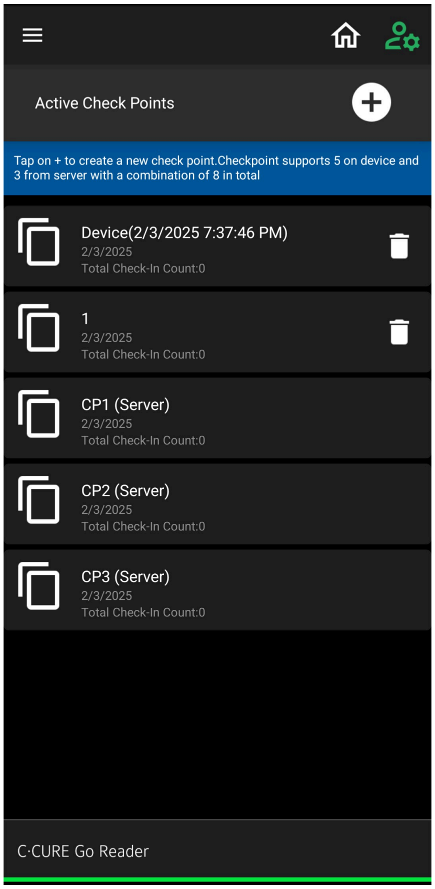


	Name	Personnel Group
▶	Lobby Area CheckPoint	CP 25 Personnel Group [Default]
	Lab Area CheckPoint	CP 50 Personnel Group [Default]
	Exit Are Check Point	CP 75 Personnel Group [Default]

- Go Reader now supports a maximum of eight checkpoints in total. Out of these, three can be created and sent from the server to mobile devices, and five can be created manually on each Go Reader device.
- When a new check point is sent to the mobile devices, the users are notified about the received check point updates in the device notification area.
- When check points are sent from the server, they are displayed with the Server subtitle as shown in the Figure 97. This indicates that these check points are created and sent from the central server.

  When check points are created manually from the device, they are listed with names that can be typed manually by the user. The default name of the check point is Device (Date & Time) as shown in the Figure 97.
- If check points are created manually from device then you can delete them using **Bin** icon available next to the check point name. If checkpoints are sent from the server then you cannot delete them from the device but they can be removed from the server.

Figure 97: Active check points



Active Check Points

Tap on + to create a new check point.Checkpoint supports 5 on device and 3 from server with a combination of 8 in total

Device(2/3/2025 7:37:46 PM)
2/3/2025
Total Check-In Count:0

1
2/3/2025
Total Check-In Count:0

CP1 (Server)
2/3/2025
Total Check-In Count:0

CP2 (Server)
2/3/2025
Total Check-In Count:0

CP3 (Server)
2/3/2025
Total Check-In Count:0

C·CURE Go Reader

Online validation mode

When you swipe a card at a Go Reader unit, the online validation mode displays the most recent updated personnel data and validates all credentials in a C•CURE database. While synchronization is in process, the app validates personnel records and credentials. This mode is available when Go Reader is connected to C•CURE server and in the online state.

Activating online validation mode

Online validation mode works when valid Go Reader clearances are assigned to the Go Reader device. The credentials that are validated are the card number, facility code, activation and expiration dates, and the lost, disabled, and stolen flags. This means that you can use GoR eader on any C•CURE system without needing to assign clearances to personnel.

1. Navigate to the C•CURE Go Reader app main screen.
2. Tap **GoReader Card Swipe**.
3. Select the **Process card swipe in server** check box.
4. Swipe a card at a Go Reader unit.

When you swipe your card, the server validates your credentials and the app displays an admit or reject message. The message is also journaled in Monitoring Station.

Manually configuring card formats on the Go Reader device

You can manually configure, manage, and assign card formats in the Go Reader app.

1. On your Go Reader device, open the **Go Reader app**.
2. Tap on **Home** > **Settings**, and select the **CARD FORMAT** tab.
3. Tap the **Add** icon to create a new card format.
4. In the **Facility Code** field, enter the bit value.
5. In the **Card Number** field, enter the bit value.
6. Tap **SAVE**.

A notification stating `Card Format successfully saved to device` appears on the Go Reader device.

Settings

Tap the **Settings** link on the Home screen to access the **Settings** module.

Use the **Settings** module to:

- Access the general, database and advanced setting screens.
- Set your preferences for offline card transaction buffer size, roll call polling intervals, and the maximum personnel for roll call area display.
- Re-synchronizing and re-setting the device.

ⓘ **Note:**

- To access the settings screen you must have full access to permissions in your assigned C•CURE Go Reader privileges. Contact your C•CURE 9000 Administrator to confirm your C•CURE Go Reader privileges.
- When you tap the**Settings** module, you are prompted to log on with your operator credentials. If you want to change the operator credentials, tap **Change Operator**.

General settings

Use the General tab to configure:

- Offline card transaction buffer size.
- Roll call polling interval.
- The maximum number of personnel that appear in the roll call area list.
- The maximum amount of time that a card number displays on the reader screen for.
- To assign a C•CURE Go Reader.

Table 40: General settings options and actions

Option	Description	Action
Offline Card Transaction Buffer Size	Set the amount of swipes that must be saved during offline mode and sent to the monitoring station when the C•CURE Go Reader is back online. **Example:** If you select 100 card swipes, the most recent 100 card swipes are sent to the Monitoring Station when the C•CURE Go Reader is back online. The rest of the card swipes are deleted. ⓘ **Note:** If the device has a lower storage capacity, set a lower Offline Card Transaction to improve functionality of the C•CURE Go Reader app.	Tap the list to select a card transaction buffer size less than 100, 1000 or 10 000 swipes.
Roll Call Polling Interval	Sets the interval time (in seconds) between roll call polling.	Tap the list to select a roll call polling time.
Max Personnel for Roll Call Area Display	Sets the maximum number of personnel that display on the Roll Call Area Information screen at one time. **Example:** If you select 100 people and there are 200 people in the missing area, the Area Information screen displays a maximum of 100 personnel.	Tap the list to select the numberof personnel to show on the Roll Call Area Information screen. Select from 100, 1000 or 10 000 personnel.
Display Swipe Details for	Sets the maximum amount of time in seconds that card information displays on the reader screen for. If you select **Never**, the card number displays on the reader screen until the next card is swiped.	Tap the list to selet the amount of time in seconds that the card information displays on the Readerscreen for.
Assign C•CURE Go Reader to this Device	Selects a Serialio idchamp reader to assign to the device.	Tap **ASSIGN GOREADER** to assign a reader to the device.
Beep on Reject	Plays a beep sound when Go Reader rejects a card. This is active by default.	Select **Beep on Reject** to play a beep sound when GoReader rejects a card. Clear **Beep on Reject** to not play a sound.

Database tab

Use the Database tab to re-synchronize the device and to view the amount of credentials and images synchronized from the C•CURE 9000 server.

For more information, see Synchronizing the C•CURE Go Reader from the C•CURE Go Reader device.

Synchronizing the C•CURE Go Reader from the C•CURE Go Reader device

Use the **Re-Sync** option in **Database Settings** to re-synchronize personnel, credential and card format data from the C•CURE 9000 system to the C•CURE Go Reader. Synchronizing the C•CURE Go Reader app from the device initiates a differential download from the C•CURE 9000 server. You can manually synchronize the C•CURE Go Reader app from the Administration Station to initiate a full synchonization and remove all previous configurations. For more information, see Synchronizing the C•CURE Go Reader.

When you synchronize the C•CURE Go Reader, the following notifications are displayed on the Android device:

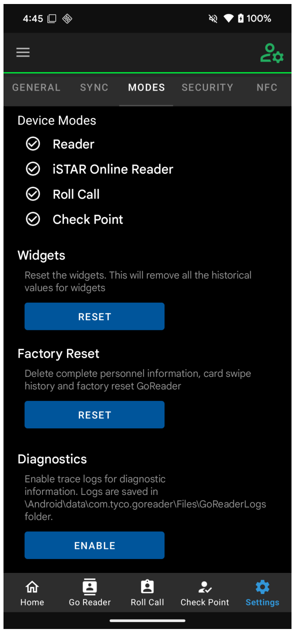
- Synchronization Started
- Synchronization Completed

1. On the **Home** screen, tap **Settings**.
2. Navigate to **Sync** tab.
3. Tap **Sync**.
4. Choose between:
   - Tap **Yes** to resynchronize.
   - Tap **No** to cancel.

Modes settings

Use the **Modes Settings** screen to reset the C•CURE Go Reader device.

Figure 98: Modes settings screen



Device Modes

- Reader
- iSTAR Online Reader
- Roll Call
- Check Point

Widgets

Reset the widgets. This will remove all the historical values for widgets

Factory Reset

Delete complete personnel information, card swipe history and factory reset GoReader

Diagnostics

Enable trace logs for diagnostic information. Logs are saved in \Android\data\com.tyco.goreader\Files\GoReaderLogs folder.

For more information on resetting the C•CURE Go Reader from the C•CURE Go Reader app, see Resetting the C•CURE Go Reader from the C•CURE Go Reader app.

For more information on configuring card format for RS3 reader, see Configure card formats in the Serialio idChamp RS3 reader.

For more information on enabling tracing in the C•CURE Go Reader app, see Activating tracing in the C•CURE Go Reader app.

For more information on security settings, see Security settings.

Resetting the C•CURE Go Reader from the C•CURE Go Reader app

Reset the device to delete personnel information, card swipe history, and to perform a factory reset of the C•CURE Go Reader app. A factory reset of the C•CURE Go Reader app resets the C•CURE Go Reader app and its associated data, it does not reset the Android device.

ⓘ **Note:** When you reset from the C•CURE Go Reader app, the current session expires in victor Web Service. victor Web Service logs the following message in **dbo.DeviceTable**: `External System ('C•CURE GoReader') was created by <OperatorName> in Audit log.`

For information on how to reset the C•CURE Go Reader device from C•CURE, see Resetting the Go Device.

1. On the **Home** screen, tap **Settings**.
2. Tap **Modes**.
3. Tap **RESET**.
4. Choose between:
   - Tap **Yes** to reset.
   - Tap **No** to cancel.

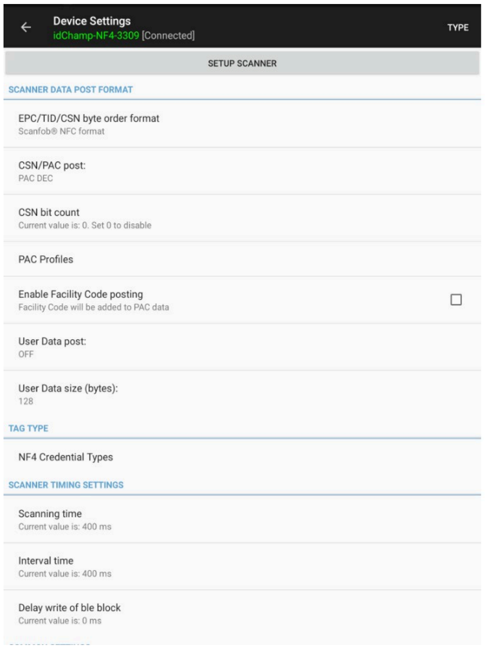
The C•CURE Go Reader device resets and the user is directed to the C•CURE Go Reader log on screen.

Configuring card format and facility code for an NF4 reader

You can configure the card format and facility code for an NF4 reader by using the PACS Settings in Go Reader.

1. On the **Home** screen, tap **Settings**.
2. Tap **Advanced**.
3. Under **PACS Settings**, tap **SETTINGS**.

Figure 99: SETUP SCANNER screen



idChamp-NF4-3309 [Connected]

SCANNER DATA POST FORMAT

EPC/TID/CSN byte order format
Scanfob® NFC format

CSN/PAC post:
PAC DEC

CSN bit count
Current value is: 0. Set 0 to disable

PAC Profiles

Enable Facility Code posting ☐
Facility Code will be added to PAC data

User Data post:
OFF

User Data size (bytes):
128

TAG TYPE

NF4 Credential Types

SCANNER TIMING SETTINGS

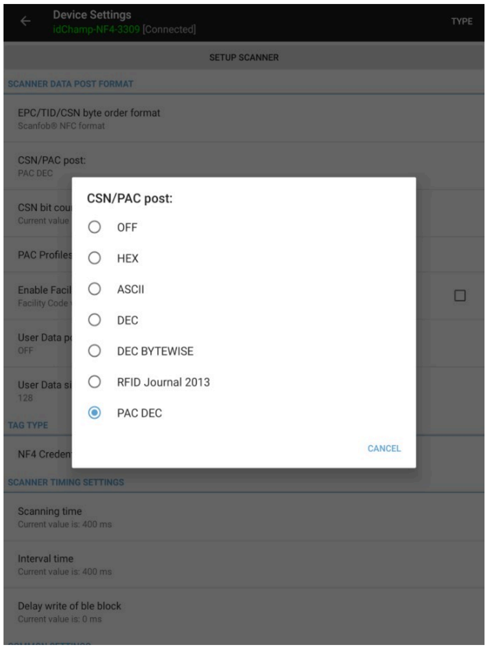
Scanning time
Current value is: 400 ms

Interval time
Current value is: 400 ms

Delay write of ble block
Current value is: 0 ms

4. Tap **CSN/PAC post** and then select **PAC DEC**. For more information, see Figure 100.

Figure 100: CSN/PAC post screen



Device Settings
idChamp-NF4-3309 [Connected]

SETUP SCANNER

SCANNER DATA POST FORMAT

EPC/TID/CSN byte order format
Scanfob® NFC format

CSN/PAC post:
PAC DEC

CSN/PAC post:

○ OFF
○ HEX
○ ASCII
○ DEC
○ DEC BYTEWISE
○ RFID Journal 2013
● PAC DEC

SCANNER TIMING SETTINGS

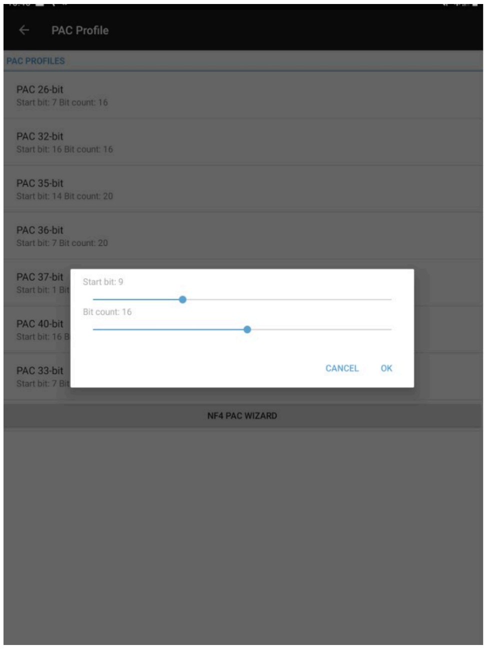
Scanning time
Current value is: 400 ms

Interval time
Current value is: 400 ms

Delay write of ble block
Current value is: 0 ms

5. On the **SETUP SCANNER** screen, tap **PACS Profile**.
6. Select the format and set the **Start Bit** and **Bit Count** values. See Figure 101.

Figure 101: Card format example



PAC Profile

PAC PROFILES

PAC 26-bit
Start bit: 7 Bit count: 16

PAC 32-bit
Start bit: 16 Bit count: 16

PAC 35-bit
Start bit: 14 Bit count: 20

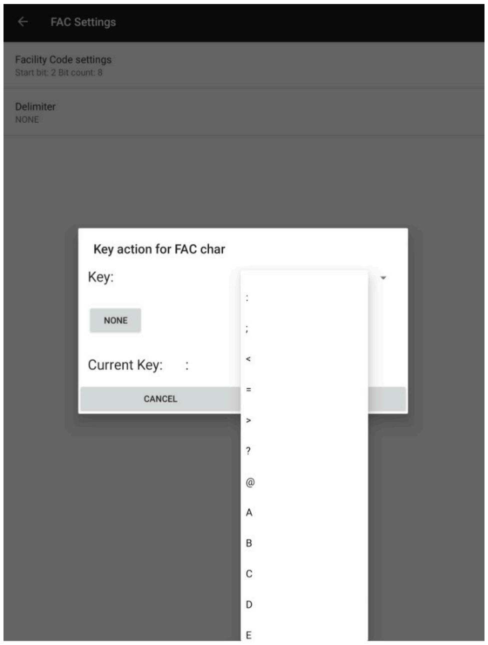
PAC 36-bit
Start bit: 7 Bit count: 20

Start bit: 9

Bit count: 16

7. On the **SETUP SCANNER** screen, tap **Enable Facility Code posting**.
8. Go to the **FAC Settings** screen.
9. Tap **Delimiter** and from the **Key** list, select **:**. For more information, see Figure 102.

Figure 102: Delimiter key for FAC settings



FAC Settings

Facility Code settings
Start bit: 2 Bit count: 8

Delimiter
NONE

Key action for FAC char

Key:

Current Key: :

10. On the **FAC Settings** screen, tap **Facility Code settings**.
11. In the **Facility Code settings** dialog box, set the **Start Bit** and **Bit Count** values you want.

Note:

- This works for BLE readers, not SPP readers.
- Users can configure card number start bit and bit count, not the card number configuration.

Activating tracing in the C•CURE Go Reader app

Activate tracing to capture Go Reader integration trace logs and view errors if you require Go Reader specific logs during troubleshooting. Use the Advanced Settings tab to activate and disable tracing.

1. On the **Home** screen, tap **Settings** .
2. Tap **Advanced**.
3. In the **Diagnostics** option, tap the **Enable** button.

Security settings

Use the **Security Settings** screen to change the operator or activate log on behavior.

Activating log on behavior

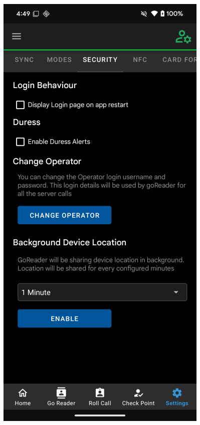
- If **Display Login page on app restart** check box is selected, the user needs to log on whenever they restart the Go Reader application.
- If **Display Login page on app restart** check box is cleared, the log on page does not appear, even when a user closes and reopens or restarts the Go Reader application.

Changing operator log on

To change the operator on the Go Reader app, complete the following steps:

1. Tap **CHANGE OPERATOR** to change the operator log on. The app redirects to the log on screen.
2. Log on with new operator credentials.

Figure 103: Security screen



4:49 100%

SYNC MODES SECURITY NFC CARD FOR

Login Behaviour

□ Display Login page on app restart

Duress

□ Enable Duress Alerts

Change Operator

You can change the Operator login username and password. This login details will be used by goReader for all the server calls

CHANGE OPERATOR

Background Device Location

GoReader will be sharing device location in background. Location will be shared for every configured minutes

1 Minute

ENABLE

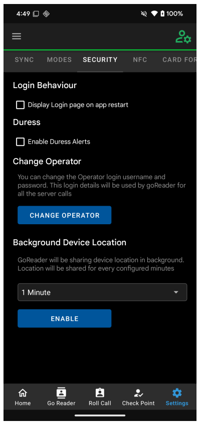
Home Go Reader Roll Call Check Point Settings

Activating background device location

Use background device location to track a Go Reader device through geographic information system (GIS) co-ordinates.

1. Open the Go Reader app and navigate to the **Settings** screen.
2. Tap the **SECURITY** tab.
3. Navigate to the **Background Device Location** section.
4. Select the **Enable** check box.
5. **Optional:** From the menu, configure how often the GIS location is sent to the C•CURE server. By default, the app shares the device location every minute. You can adjust this to any time in the range of 1 to 20 minutes.

Figure 104: Activating background device location



4:49 100%

SYNC MODES SECURITY NFC CARD FOR

Login Behaviour

□ Display Login page on app restart

Duress

□ Enable Duress Alerts

Change Operator

You can change the Operator login username and password. This login details will be used by goReader for all the server calls

CHANGE OPERATOR

Background Device Location

GoReader will be sharing device location in background. Location will be shared for every configured minutes

1 Minute

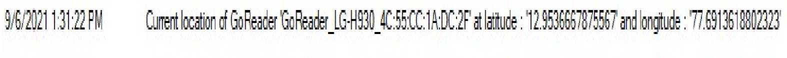
ENABLE

Home Go Reader Roll Call Check Point Settings

View GIS location in Monitoring Station

When you activate background device location, the device current latitude and longitude details are journaled in Monitoring Station.

Figure 105: Device latitude and longitude



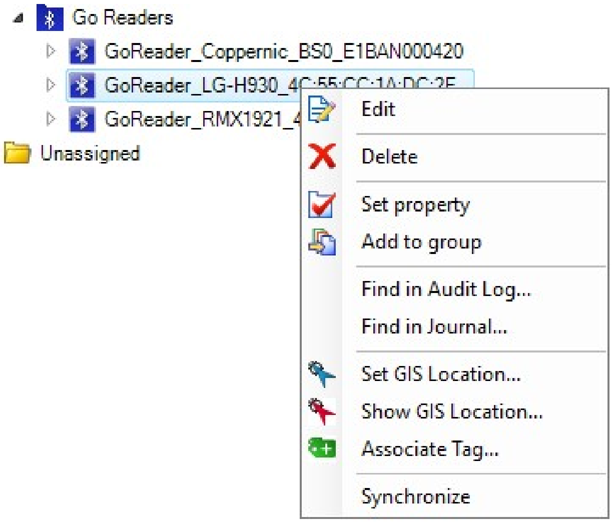
```
9/6/2021 1:31:22 PM        Current location of GoReader 'GoReader_LG-H930_4C:55:CC:1A:DC:2F' at latitude : '12.9536667875567' and longitude : '77.6913618802323'
```

Viewing GIS location in Administration Station

You can view the location of the device on a GIS map in Administration Station.

1. In Administration Station, from **Hardware Tree**, right-click the reader device.
2. Click **Show GIS Location...** to view the location of the device on a GIS map.

Figure 106: Show GIS location



ⓘ **Note:**

- In the GoReader app v5.0.238 and above, location permission is not set to Always On. When the device sends the GIS location to the C•CURE server, if the device is locked then an `Incorrect location details` message displays in the diagnostics logs until the device is unlocked.
- If you do not activate background device location in the app, then the **Show GIS Location...** option is not available in Administration Station.
- The device sends the GIS location when connected to the C•CURE server.

Scanning barcodes and QR codes on an Android device

You must install the Go Reader application v5.0.238 and above to use the barcode and QR code scanning feature.

1. In the **Navigation** pane of the Administration Station, click **Hardware**.
2. In the **Hardware** tree, expand the **Company Name** folder, then select **Go Reader**.
3. On the **Barcode** tab of the Go Reader editor, in the **Data Fields** section, select the **Use Data Fields** check box.
4. Configure the **Card facility code** and **Card Number** fields.
5. Click **Save and Close** to confirm the changes.
6. On your Android device, open the **Go Reader** application.
7. Tap **HOME**, then tap **Go Reader**, and select **SCAN BARCODE**.
8. Use the camera to scan the barcode or QR code.

C•CURE Go Reader driver and service logging

C•CURE Go Reader service logging records the events, errors and exceptions that occur in the C•CURE Go Reader app. For more information, see C•CURE Go Reader service logging.

For more information on C•CURE Go Reader driver logging features, see C•CURE Go Reader Driver Logging.

C•CURE Go Reader service logging

C•CURE Go Reader service logging records the events, errors and exceptions that occur in the C•CURE Go Reader app.

The logs consist of:

- Logging in C•CURE Go Reader
- Live debug traces

Log files on C•CURE Go Reader

Any exceptions in the C•CURE Go Reader app are logged in the log file. Logs are saved to the Android device memory in the `root/GoReaderLogs` folder. The log file is available as a single zip file in the temp folder of your computer.

The log file naming convention is **YYYYMMDD-00001.log**. Each file is limited to 10MB. When the log file reaches 10MB, another log file is created as **YYYYMMDD-00002.log**. Every day a new log file is generated.

When the total size of all log files reach 1GB the C•CURE Go Reader Service logging overwrites the oldest log file.

The format of the log message is displayed as:

```
[Yyyy-MM-dd HH:mm:ss] [Log Level] [Log Message]
```

Example:

```
2017-03-16 11:00:10 [Error] C•CURE GoReader: Log Message
```

ⓘ **Note:** C•CURE Go Reader service logging only supports error level logging.

C•CURE Go Reader Driver Logging

To view tracing in C•CURE 9000, turn on the **C•CURE Go Reader Driver** switch in the C•CURE 9000 **Diagnostics Window**.

The following tracing is supported in the C•CURE Go Reader driver:

- Function calls
- Building database for differential download
- Application level exceptions
- Function level exceptions

Validating C•CURE Go Reader driver functionality

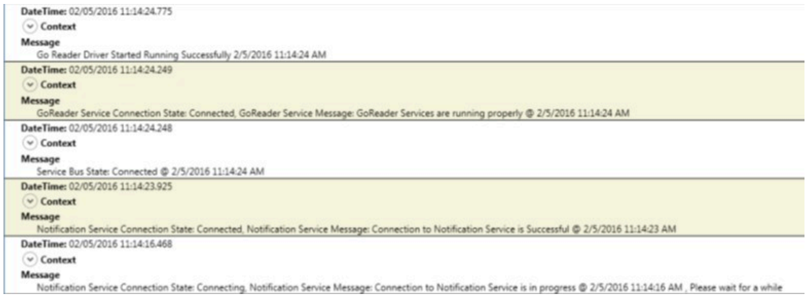
1. Ensure that the C•CURE 9000 target system meets all installation pre-requisites described in Installing the C•CURE Go Reader driver.
2. Verify that victor Web Service is installed and functioning on the C•CURE 9000 target system:
   a. Open the Windows Internet Information Services (IIS) Manager.
   b. Expand **Sites**.
   c. Expand **Default Web Site**.
   d. Right-click **victorwebservice** and select **Manage Application**.
   e. Click **Browse**.

      If victor Web Service is functioning, the web browser displays a page with the message, `Welcome to the victor Web Service homepage`.
3. Verify the reader count registered by the C•CURE Go Reader license:
   a. Open the C•CURE 9000 License Manager.
   b. Open the **License** tab.
   c. In the **System Wide Capacities** table, verify that the C•CURE Go Reader value reflects the amount of registered C•CURE Go Reader devices. The number of Go Reader devices that you can connect to with

your server is determined by your licensing agreement when you purchase the software.

4. Verify that the C•CURE Go Reader Driver Service is functioning:
   a. Open the **Server Configuration** application.
   b. In the **C•CURE Go Reader driver service field**, click **Stop**.
   c. Click the **Diagnostics** tab.
   d. Click **Connect**.
   e. Start the **C•CURE Go Reader Driver Service**. If the C•CURE Go Reader driver is functioning, the messages in Figure 107 display.

Figure 107: C•CURE Go Reader Driver Messages



```
DateTime: 02/05/2016 11:14:24.775
Context
Message
  Go Reader Driver Started Running Successfully 2/5/2016 11:14:24 AM
DateTime: 02/05/2016 11:14:24.249
Context
Message
  GoReader Service Connection State: Connected, GoReader Service Message: GoReader Services are running properly @ 2/5/2016 11:14:24 AM
DateTime: 02/05/2016 11:14:24.248
Context
Message
  Service Bus State: Connected @ 2/5/2016 11:14:24 AM
DateTime: 02/05/2016 11:14:23.925
Context
Message
  Notification Service Connection State: Connected, Notification Service Message: Connection to Notification Service is Successful @ 2/5/2016 11:14:23 AM
DateTime: 02/05/2016 11:14:16.468
Context
Message
  Notification Service Connection State: Connecting, Notification Service Message: Connection to Notification Service is in progress @ 2/5/2016 11:14:16 AM , Please wait for a while
```

Troubleshooting

This section provides troubleshooting instructions for issues that can occur while using the C•CURE Go Reader app.

MIFARE/DESFire card scan or save error

An error message displays when you scan a MIFARE or DESFire card or when you save a MIFARE or DESFire card configuration.

Solution

Table 41: MIFARE and DESFire card error messages and solutions

Error message	Solution
`Smart card authentication failed` displays when you scan a MIFARE or DESFire card.	The authentication key configured for the MIFARE or DESFire card is incorrect. For more information, refer to the *OMNIKEY 5x27CK Keyboard Wedge Configuration User Guide*.
`Could not load key into reader` displays when you attempt to save a MIFARE or DESFire card configuration.	There is an error in the **Reader Key Slot Id** or **Card Key Number** configured. The default value for the Reader Key Slot Id is 240 and the default value for Card Key Number is 1. It is best practice to use the default values. For more information, refer to the *OMNIKEY 5x27CK Keyboard Wedge Configuration User Guide*.
`Smart card authentication failed` displays when you scan a MIFARE or DESFire card.	The authentication key configured for the MIFARE or DESFire card is incorrect. For more information, refer to the *OMNIKEY 5x27CK Keyboard Wedge Configuration User Guide*.
`Failed to read MIFARE sector` displays when you scan a MIFARE card.	There is an issue in the **Sector** and **Block** values for the authentication key. For more information, refer to the *OMNIKEY 5x27CK Keyboard Wedge Configuration User Guide*.

Table 41: MIFARE and DESFire card error messages and solutions

Error message	Solution
`Problem Failed to select DESFire application` displays when you scan a DESFire card.	There is an error loading the **Application Id** from the DESFire card. To resolve the issue, you must verify the Application Id on the Go Reader application. For more information, see Reading the Application Id of DESFire cards.
`Failed to read DESFire file` displays when you scan a DESFire card.	There is an error loading the **Application Id** from the DESFire card. To resolve the issue, you must verify the Application Id using the Go Reader application. For more information, see Reading the Application Id of DESFire cards.

Barcode scan unavailable offline (Android)

Unable to use the barcode scanning feature on an Android device in offline mode.

Solution

When using the barcode scanning feature on an Android device, the device must be online and connected to the Administration Station. You cannot use the barcode scanning feature in offline mode as barcode length configuration data is not stored on Android devices.

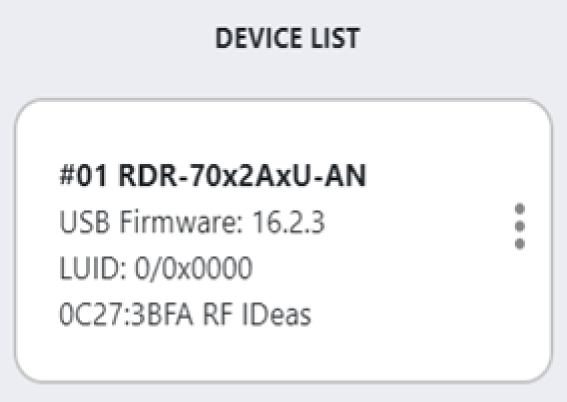
Firmware upgrade fails on Wave ID Nano USB-C reader

You cannot upgrade the firmware on your Wave ID Nano USB-C reader.

Solution

There are two types of Wave ID Nano USB-C readers, Proximity and iClass. You must ensure you download the correct firmware version for the reader type. See Figure 108 and Figure 109 to check which device list to download the firmware from.

Figure 108: iClass reader - WAVE ID Nano



DEVICE LIST

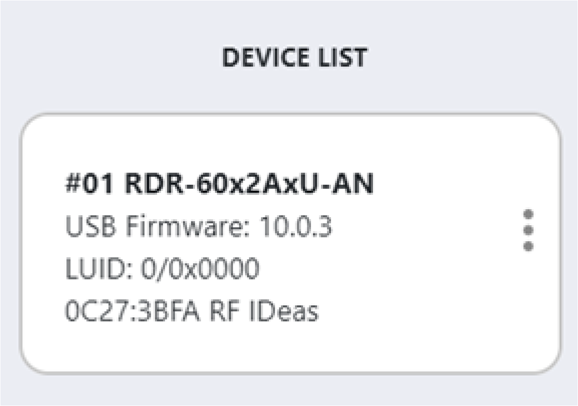
#01 RDR-70x2AxU-AN

USB Firmware: 16.2.3

LUID: 0/0x0000

0C27:3BFA RF IDeas

Figure 109: Proximity reader - WAVE ID Nano



DEVICE LIST

#01 RDR-60x2AxU-AN
USB Firmware: 10.0.3
LUID: 0/0x0000
0C27:3BFA RF IDeas

If there is a error in the reader name and you have issues upgrading the firmware, contact Software House Technical Support.

Go Reader apps missing in CopperApps store

The CopperApps store does not load all the apps that are hosted in the Go Reader repository.

Solution

If the CopperApps store does not load all the apps, it is likely that the Coppernic IT team are updating the app repository. You must wait for the update to complete, then return to the CopperApps store and download the required apps.

Login fails with 'unable to connect to service' error

- The C•CURE Go Reader app displays the message: `Service Down`
- After entering correct user name, password and Server IP, the C•CURE Go Reader app displays the message: `Unable to connect to service`.

Solution

Verify that victor Web Service is installed and functioning on the C•CURE 9000 target system:

1. Open the Windows Internet Information Services (IIS) Manager.
2. Expand **Sites**.
   a. Expand **Default Web Site**.
   b. Right-click **victor web service** and select **Manage Application**.
   c. Click **Browse**.

If victor Web Service is functioning, the message: `Welcome to the victor Web Service homepage` displays.

OR

Type the following URL in a browser on the Android device to verify the victor Web Service connectivity: `http://IP address/victorwebservice` where **IP address** is the IP Address of the C•CURE 9000 target system.

Example:

```
http://10.47.84.50/victorwebservice
```

If victor Web Service is functioning, the message `Welcome to the victor Web Service homepage` is displayed. If this message does not display, then the C•CURE Go Reader app is unable to connect with victor Web Service, and any activity performed in the C•CURE Go Reader app is not logged.

Login fails after C•CURE Server IP change

Unable to log on to the C•CURE Go Reader app after changing the IP address of the C•CURE 9000 server.

Solution

- If the C•CURE 9000 server is in a Dynamic Host Configuration Protocol (DHCP) domain environment, use the system name of the C•CURE 9000 server in the **Server Address** field on the C•CURE Go Reader log on page.

  ⓘ **Note:** If the IP address of the C•CURE 9000 server changes after you have logged on to the C•CURE Go Reader app with the IP address instead of the system name, you must reset the C•CURE Go Reader device. Resetting the device automatically logs you out of the C•CURE Go Reader app. Use the system name to log on.

- If the C•CURE 9000 server is in a workgroup environment, do not change the IP address of the C•CURE 9000 server. If you change the IP address, you must reset the C•CURE Go Reader device log on with the new IP address.

Sync fails when victor Web Service is off

If victor Web Service is off, C•CURE Go Reader app does not synchronize after you update Personnel and Credential objects in C•CURE 9000.

Solution

1. Restart the victor Web Service. For more information, refer to the *victor Web Service User Guide*.
2. Restart the C•CURE Go Reader driver.
   a. Launch the **Server Configuration** application.
   b. On the **Software House CrossFire C•CURE Go Reader Driver Service**, click **Stop**
   c. When the **Software House CrossFire C•CURE Go Reader Driver Service** status is **Stopped**, click **Start**.

Go Reader does not return to log on screen after driver stops

If the C•CURE Go Reader driver status is **Stopped**, the C•CURE Go Reader app does not return to the log on screen after you delete a Go Reader or Go Device.

Solution

Use **RESET** in the **Advanced Settings** tab in the C•CURE Go Reader app to reset the C•CURE Go Reader. See Resetting the C•CURE Go Reader from the C•CURE Go Reader app.

Disabling roll call fails if Personnel screen is open

When you disable roll call in the C•CURE Go Reader editor, the C•CURE Go Reader does not disable if the Personnel screen is open in the C•CURE Go Reader app.

Solution

Tap the Home screen icon to return to the **Home Screen**. The Roll Call option is disabled.

Go Reader loop when assigned reader is deleted

When you assign another reader from the C•CURE Go Reader app Settings module, and then delete that reader instead of activating it in C•CURE 9000, the C•CURE Go Reader app goes into a loop.

Solution

Close and re-open the C•CURE Go Reader app.

Log on fails if details change during sync

Changing operator or credential details after starting synchronization causes the status to remain as **Synchronization Pending** if you try to log on from the **Login Failed** notification.

Solution

Reset the C•CURE Go Reader app in the C•CURE 9000 Administration Station. See Resetting the C•CURE Go Reader from the C•CURE Go Reader app.

Go Reader fails to detect idChamp RS3 reader

The Serialio idChamp RS3 card reader does not communicate with the C•CURE Go Reader.

Solution

Verify that the following settings have been completed:

1. The DIP switches on the Serialio idChamp RS3 card reader are configured for BLE communications. The DIP switches might still be in the PC Communications mode. See Serialio idChamp RS3 configuration sequence.
2. The Bluetooth service is enabled in your Android device.
3. The Serialio idChamp RS3 card reader is paired with your Android device.
4. In the C•CURE Go Reader app, tap the bluetooth icon to restart Bluetooth pairing between the Android device and the Serialio idChamp RS3 card reader.

Known card marked as unknown or rejected

A registered swipe card shows as Unknown (Card Not Found) in the Go Reader app, however, in the activity comes in as a known card but as a Reject (Clearance).

Solution

This is due to a mismatch in the C•CURE Go Reader's database, in some cases after an upgrade of the app. To fix the problem, perform a manual synchronization of the C•CURE Go Reader Ddvice from the Administration Station. See Synchronizing the C•CURE Go Reader from the C•CURE Go Reader device.

Go Reader fails after password change

Go Reader driver fails to operate after Windows password changes.

Solution

If your Windows password changes, you must update the Go Reader installation with the new password.

To add the new password to the Go Reader installation, complete these steps:

1. From the **Start** menu, search for Programs and Features. Open Programs and Features.
2. Click **C•CURE Go Reader** and then click **Change**. The Go Reader Setup wizard displays. Click **Next**.
3. In the **Password** field, type the new Windows password . Click **Next**.
4. Click **Repair** to confirm the **C•CURE Go Reader Setup Summary** and apply the new password to the Go Reader installation.

Inaccurate offline mustering count

Offline mustering personnel count is not accurate.

Solution

1. Restart the Go Reader integration driver.
2. Disable and re-enable the Go Reader from the Administration Workstation.

3. Reset Go Reader from the settings menu on your Android device.
4. Upgrade the Go Reader app on your device.
5. Manually synchronize the offline mustering personnel count. See Manually initiating offline mustering synchronization.

CrossFire does not start after Go Reader upgrade

After upgrading C•CURE to version 3.10 and subsequently updating the Go Reader driver from version 2.9 to 3.10, the CrossFire framework service may fail to start.

Solution:

1. Open **Control Panel** and navigate to **Programs > Programs and Features**.
2. Locate **Victor Application Server** in the list.
3. Right-click and select **Change** from the context menu or installer options.
4. Proceed with the **Repair** process for the Victor Application Server.
5. Once the repair is complete, **restart the system** to ensure all services and dependencies are properly reloaded.

© 2025 Johnson Controls. All rights reserved. JOHNSON CONTROLS and Software House are trademarks of Johnson Controls.