CV-350 (Ver 5.0.4)
2 Door Access Control Unit

Intallation Instructions
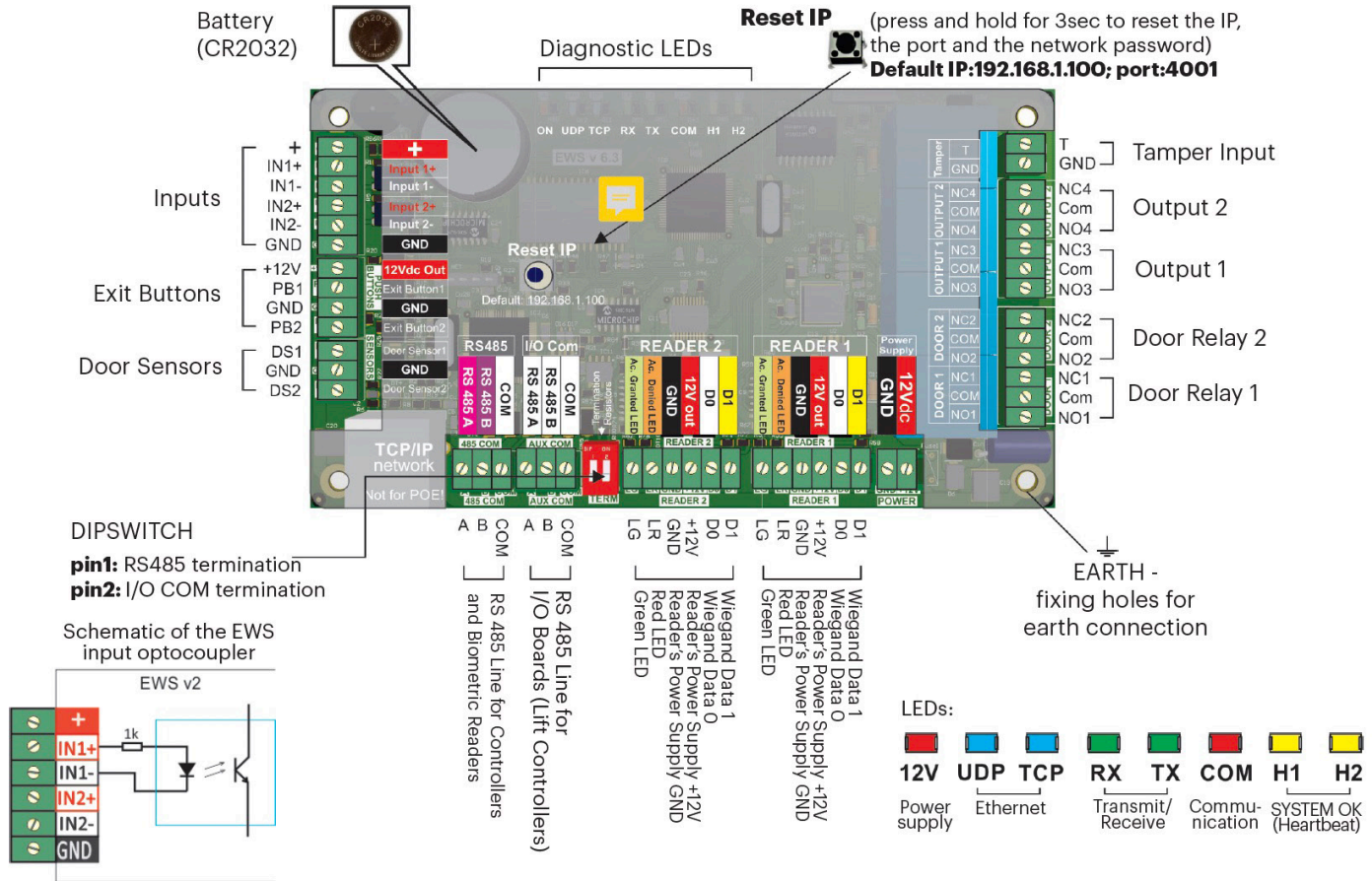
Contents

1. CV-350 - 2 Door Access Controller
Camden Access Manager Software (CAMS)

1.1 Specifications

- Power Supply: 11-15VDC
- User Capacity: max. 15000
- Event Capacity: max. 30000
- Communication: TCP/IP or RS485
- Controllers per System: unlimited
- Door Relays: 2 (250 VAC, 10A)
- Programmable Outputs: 2 (250 VAC, 10A)
- Readers: 2
- Programmable Inputs: 2 (5-30VDC, 3-28mA)
- Door Sensors: 2

- Exit Button Inputs: 2
- Wiegand interface: 26 bit, 34 bit or customizable (8 to 128 bit)
- Entry Mode: Card, PIN, Finger, Card or/and PIN, Card or/and Finger, PIN or/and Finger, Finger on Card
- Environment Temperature: 32°F - 113°F (0°C - 45°C)
- Humidity: 0-80 %, non condensing
- Tamper: Yes
- Consumption: 300 mA (without readers)

1.2 Installations

1.2.1 CV-352 Metal Enclosure with Power Supply

- The unit may only be installed by suitably trained personnel.

- Avoid any liquids or metallic items entering the unit. Use sealed type lead-acid battery 12VDC/7,2Ah.

- Do not fix this device in a place subject to direct sunlight, high temperatures, high humidity.

- The unit must be earthed.

Mounting

12"
[305mm]

12 3/4"
[324mm]

10 1/16"
[265mm]

13 3/4"
[350mm]

3 1/16"
[78mm]
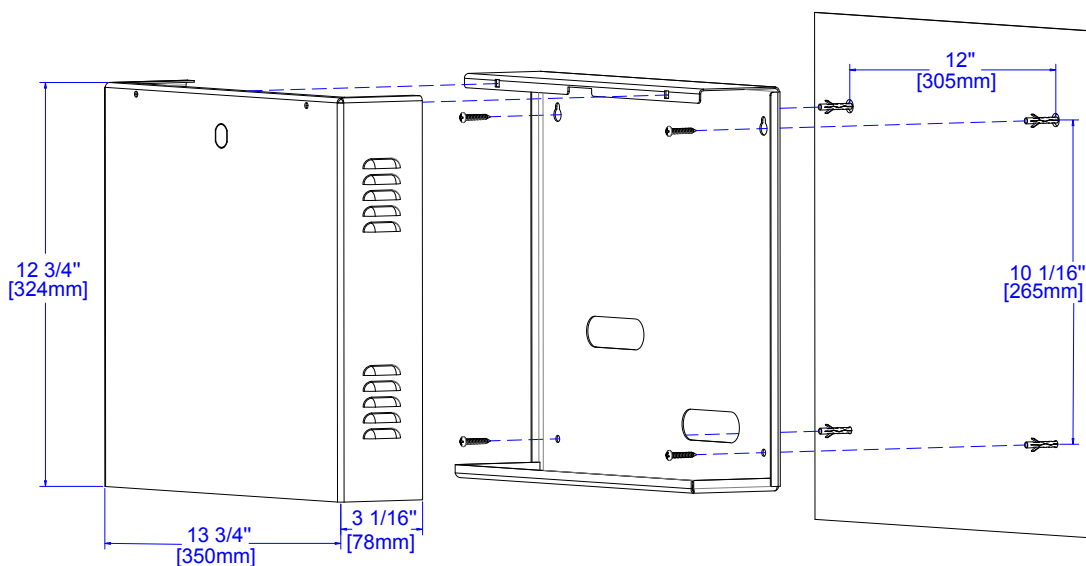
Earthing

Caution: Connect the front metal cover with the wire provided.

Wiring

Caution: Before doing any kind of wiring, disconnect the unit by extracting the mains terminal fuse.

Do not short the output terminals or output lead wires, otherwise fire or damage will result.

Note: To wire the controller, please refer to the controller's manual.

Specifications

- Input Voltage: 110-220 VAC 40 VA, 60 Hz.
- Output Voltage: 12.8 V to 13.8VDC, Nominal 13.5 VDC
- Output Current: Average 1.5 A, Maximum 2A
- Monitoring: Green LED indicates output

- Battery Specification: 12V, 7.2 Ah sealed lead acid type battery
- IP Factor: IP30

Installations

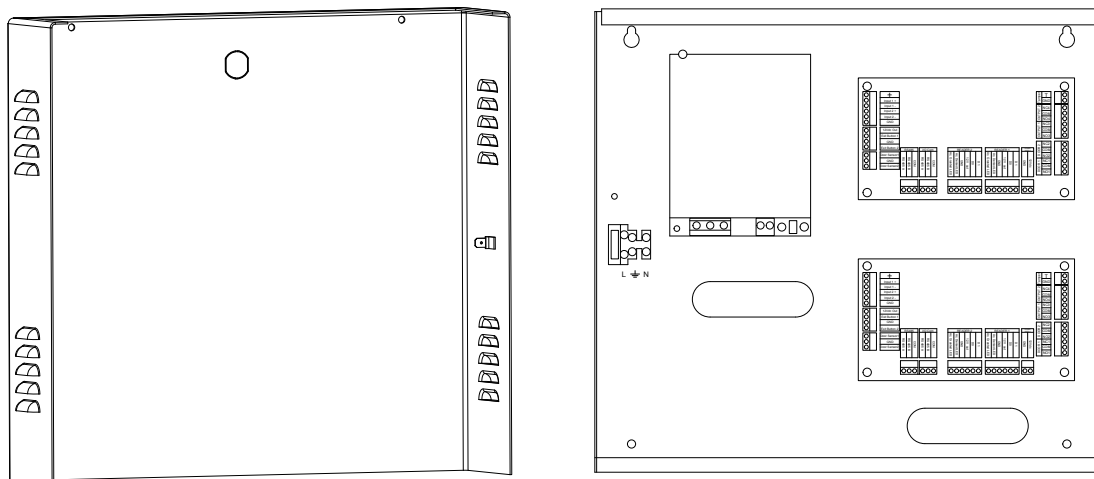### 1.2.2 CV-354 Metal Enclosure with Power Supply

- The unit may only be installed by suitably trained personnel.
- Avoid any liquids or metallic items entering the unit. Use sealed type lead-acid battery 12VDC/7,2Ah.
- Do not fix this device in a place subject to direct sunlight, high temperatures, high humidity.
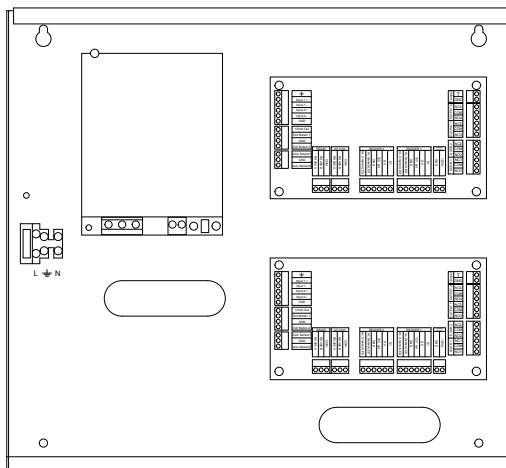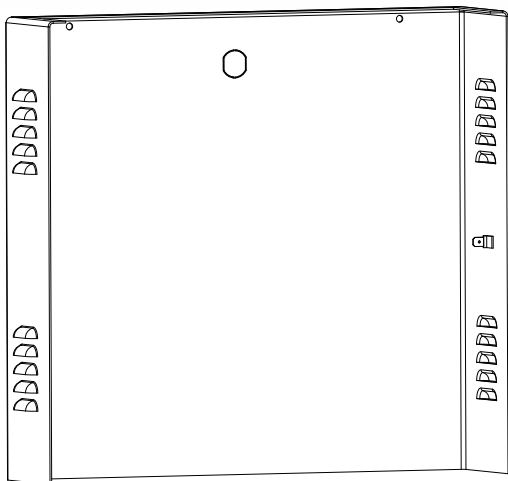- The unit must be earthed.

Mounting
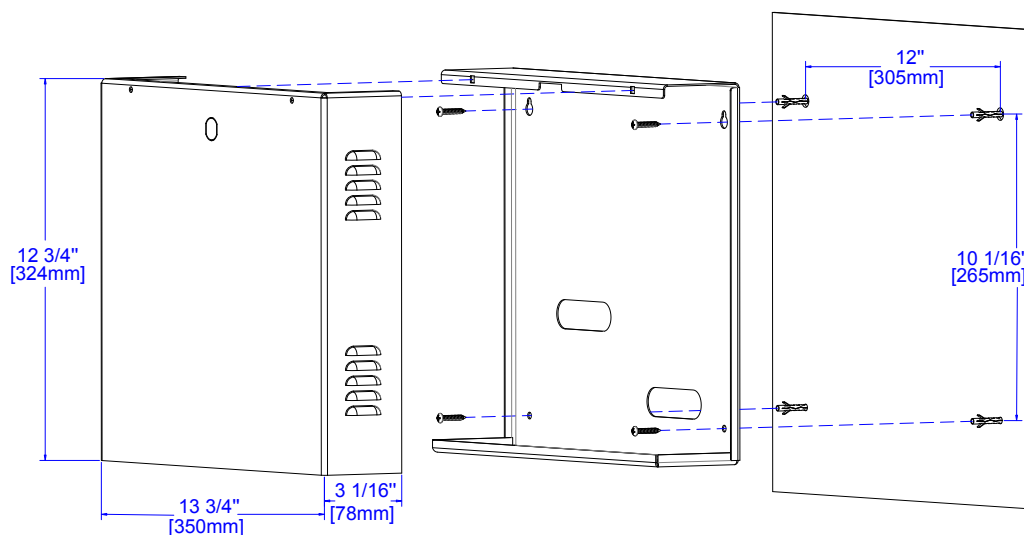
Earthing
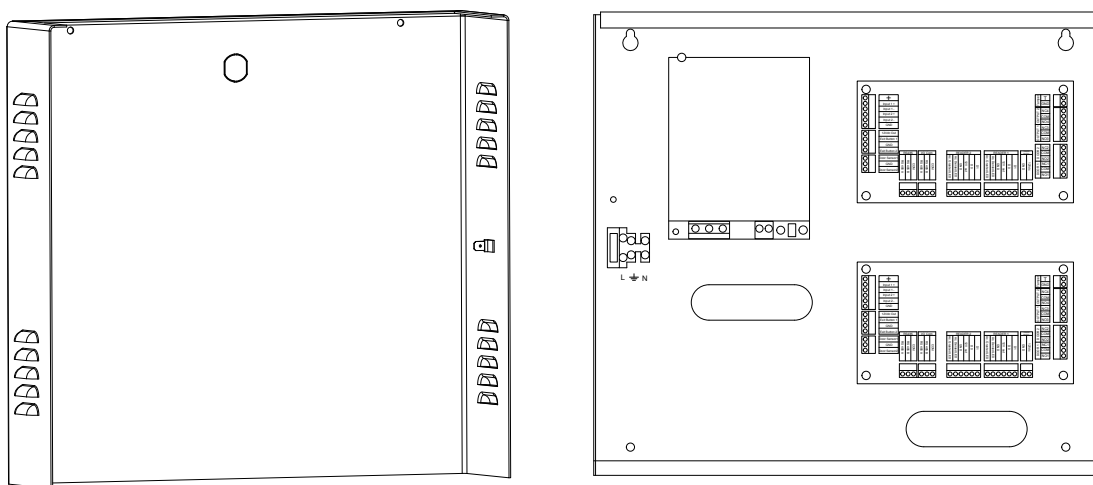
Caution: Connect the front metal cover with the wire provided. Bring the earth wire on the mains input terminal.

Wiring
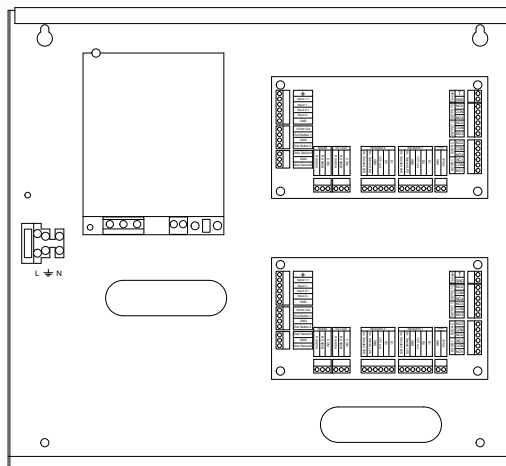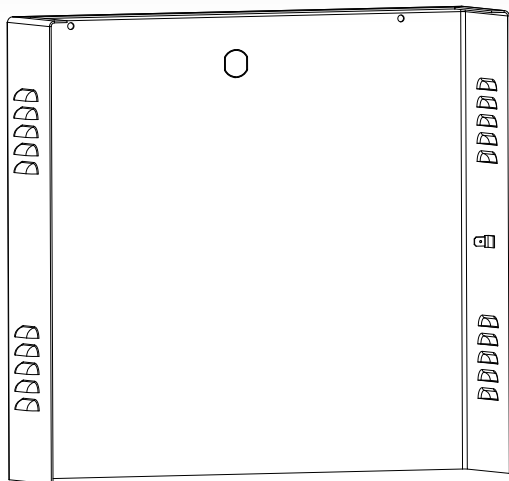
Caution: Before doing any kind of wiring, disconnect the unit by extracting the mains terminal fuse.

Do not short the output terminals or output lead wires, otherwise fire or damage will result.

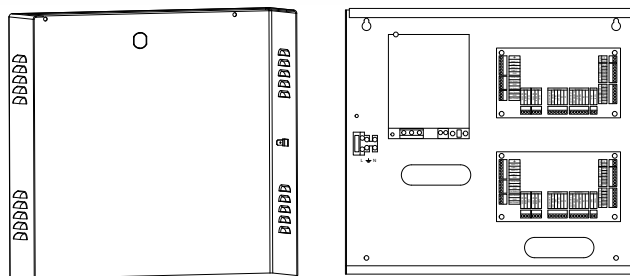Note: To wire the controller, please refer to the controller's manual.

Specifications

- Input Voltage: 110 - 220 VAC 40 VA, 60 Hz.
- Output Voltage: 12.8 V to 13.8VDC, Nominal 13.5 VDC
- Output Current: Average 1.5 A, Maximum 2A
- Monitoring: Green LED indicates output

- Battery Specification: 12V, 7.2 Ah sealed lead acid type battery
- IP Factor: IP30

Installations

1.2.3 CV-350 Installation

1. Insert the battery provided with the hardware kit.

2. Connect the devices according to the connection diagram above.

3. Use the diodes provided when the door lock is DC powered or the capacitor+10K resistor when the lock is AC powered.

4. Use the provided resistors for RS485 tuning.

1.3 Instructions

1. Keep the distance reader to controller less than 164 ft. (50 meters.)

2. Always use twisted pair cables when wiring a RS485 network (biometric readers or CV-350 controllers).

3. Do not use twisted pair cables for the Wiegand wires (D0 and D1).

4. Always keep the RS485 line in daisy chain.

5. Make sure that the terminal block is correctly Inserted, make sure that is not shifted left/right by one position and see if the wires are not put in reverse order.

6. Do not swap the RS485 terminal with the power supply terminal.

7. All the controllers that are communicating via TCP/IP must have different IP address.

1.4 Communication
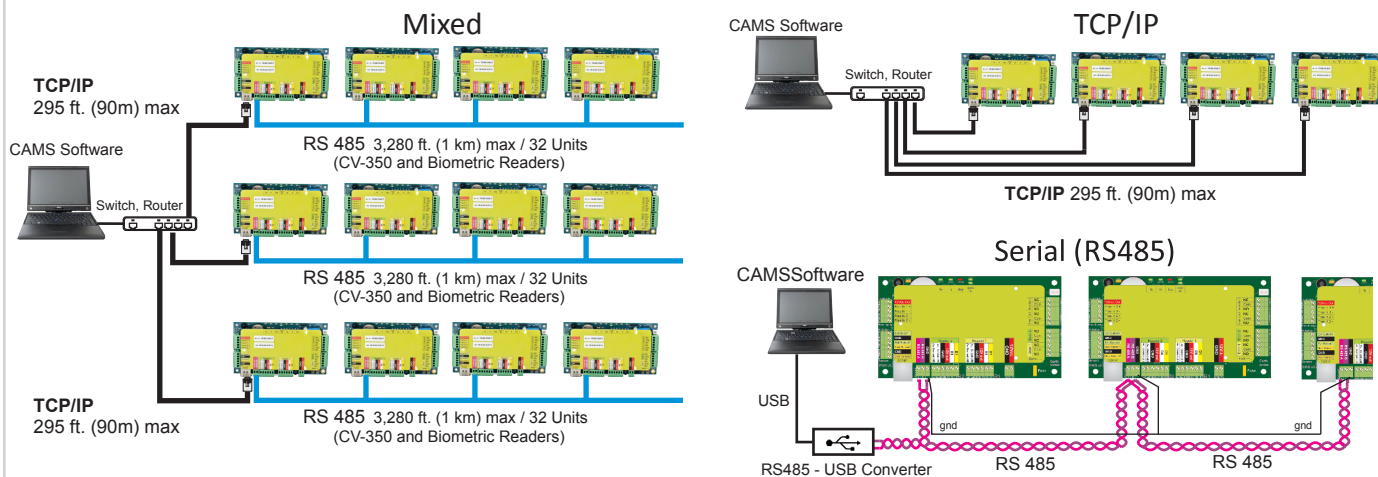
RS485 Tuning
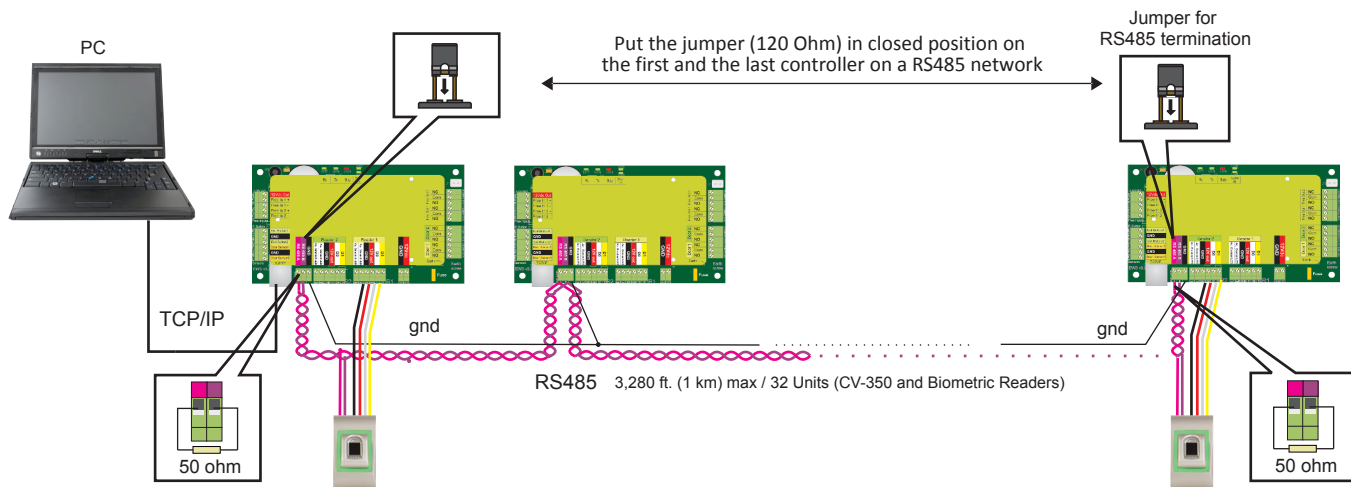
Important Note

- The RS485 Communication Line must be made in daisy chain, NOT in a star type configuration.

- The cable must be twisted and shielded. If the shield is used, connect the EARTH at ONE side of the RS485 Line to the shield cable.

- Connect the ground of each unit in the RS485 Line using a third wire in the same cable.

RS485 Termination Resistors

- Terminate both ends of the line with 120 Ohm resistor. If the end of the line is the CV-350, use the built in resistor (120 Ohm) by closing the jumper.

- If the communication is not established and stable, use the external resistors provided in the hardware kit.

When using CAT 5 compatible cable, in most of the cases, termination made with 50 Ohm external resistor or a combination of 50 Ohm external and termination resistor from the CV-350 (120 Ohm) should be the solution.

2. Installing Camden Access Manager Software (CAMS)

1. You can install the following products with the CAMS setup:

- Client only
- Client + Server
- Client + Server + Web Server (for generating reports only)

CAMS Installation Steps

Installation requirements

CAMS requires additional components to be installed in order to work properly. If some of the components are already installed, they will not be shown in this list (see picture below).
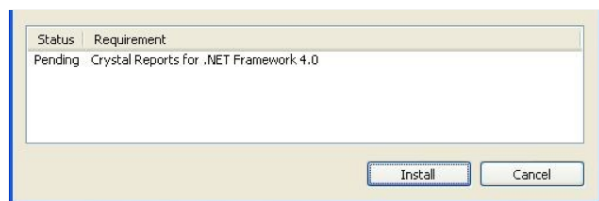
Installation folder

The CAMS installation folder can be changed during installation.

CAMS Products

There are three products included in the CAMS setup: Client, Server and Web Server.

- Client is the software that connects to the Server and it is used for configuring and maintaining hardware, users and other configurations.

- Server is the software that communicates with the hardware and the clients (Client software) and reads/ writes data into the database.

- Web Server is the software used for generating reports from an internet browser (Internet Explorer, Google Chrome, Mozilla Firefox...)

The installation of the Server and Web Server is optional and if it is not required you can choose "This feature will not be available" from the setup window.
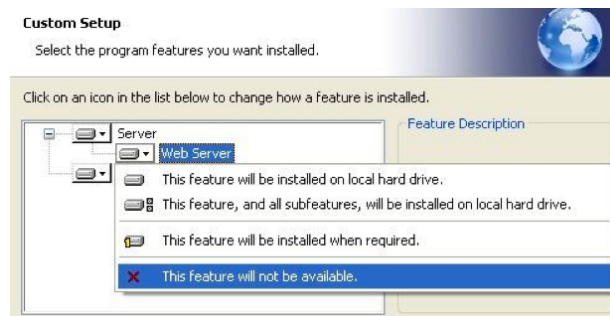
Database Eequirements

CAMS can run either with Access 2007 database or with SQL database.

If it runs with Access database NO extra configuration or installation is needed.

If it runs with SQL database and the database will be placed on the same PC as the Server, then installation of SQL Server Express is required.

Minimum SQL requirements are SQL Server 2008 R2 or SQL Express 2008 R2.

SQL Express 2008 R2 can be downloaded from

http://www.microsoft.com/en-us/download/details. aspx?id=30438

 (Download the file - SQLEXPRWT_x86_ENU.exe).

Once downloaded run the SQLEXPRWT_x86_ENU.exe file. The setting shown on the picture bellow MUST be set when installing SQL Server. The password entered in the field is required (record the password and keep in a safe place for future use of SQL Server). All other settings should be left as their default values.
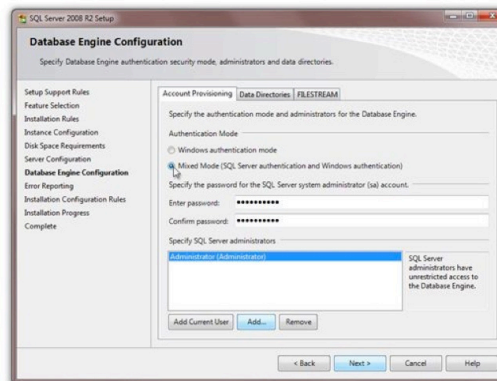
2.1 Server Setup

Making changes to Server configuration and changing the Database type (SQL or Access) is done with CAMS Server Setup.

(Start->All Programs->CAMDEN->CAMS->CAMS Server Setup)

Default values for login are:

- Operator name: Admin
- Password: admin

and can be changed later in the Client.

Server Configuration

In the Server Setup window you can see the Server status in the top of the window, the ports used for communication between the C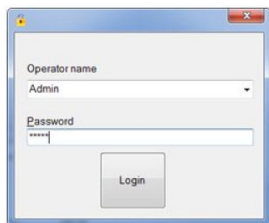lient and the Server, and the buttons for starting, stopping and removing the Server service (The Server is running as a windows service, not as a standard windows application).

After installing the Server, the service is started automatically. There are no additional setup required. If a connection to the server cannot be established, please check that the server service is running. The STATUS of the server is shown at the top of the Server Setup screen.
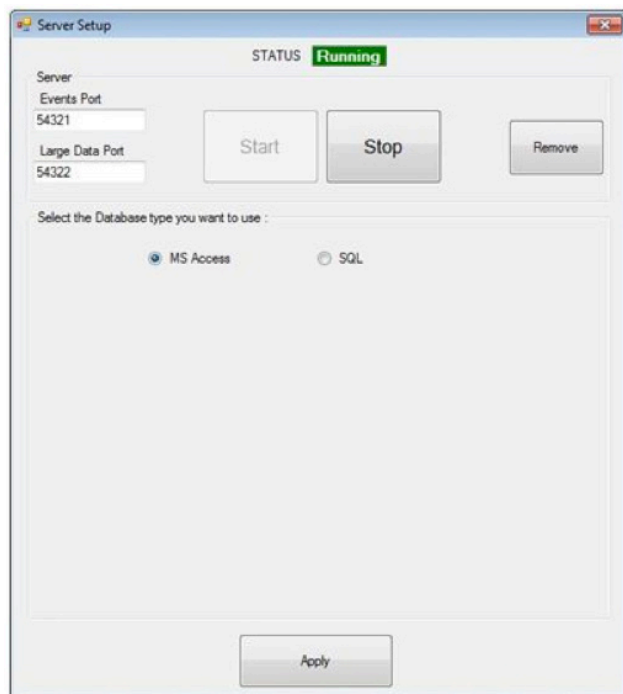
- START button – registers the Server as a windows service and starts it immediately

- STOP button – stops the Server

- REMOVE button – stops the Server and removes it from windows services

Note: You do not need to press the APPLY button after pressing the START, STOP or REMOVE button.

Database Configuration

If you want to change the Database type used for storing data in the software you can choose from the options either MS Access or SQL.

WARNING: When switching from Access to SQL or from SQL to Access – data is not transferred. You will have to enter all hardware and user configuration manually.

If SQL is chosen the following screen appear
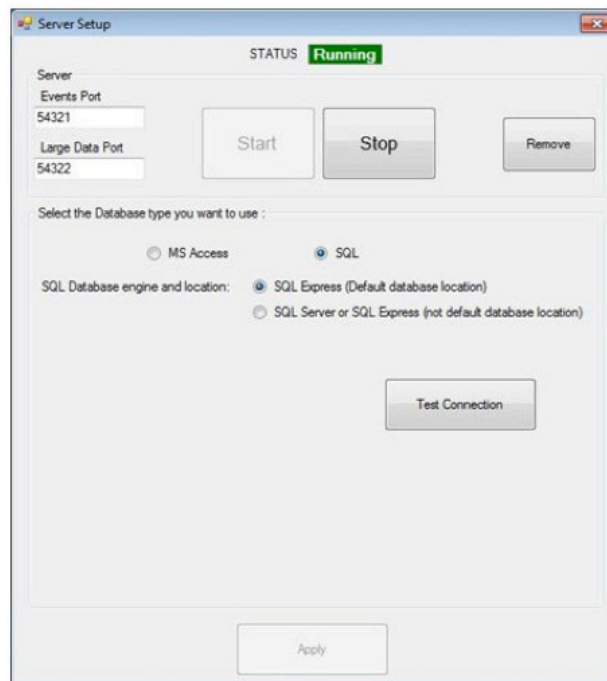
SQL database can be at its default location (in CAMS installation folder) and attached to local SQL Server Express or it can be on a remote SQL Server and attached to it (the location of the database that needs to be attached on the remote SQL Server is: "CAMDEN\CAMS\ Blank Database"). If the second option is chosen the following screen appears
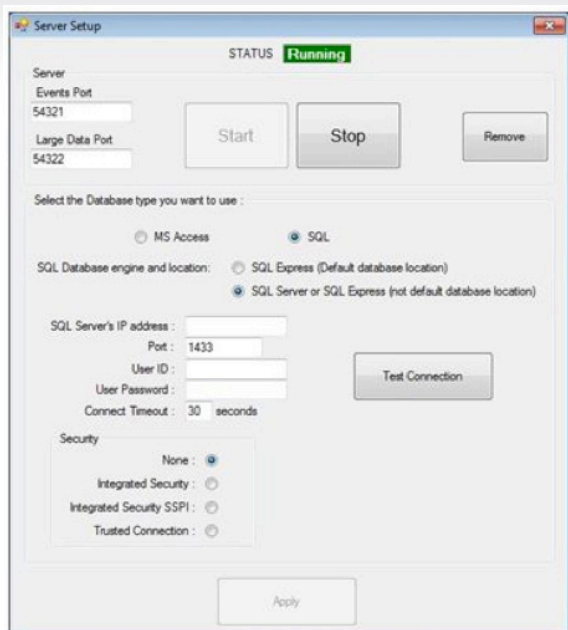
Here, the SQL Server address and login credentials are entered (these settings are provided by the SQL Server administrator).

After choosing the SQL database location, connection with the server must be tested (Test Connection button) so that the settings can be applied.

After this dialog appears, the Apply button is enabled and database setup is finished. If some error dialog box appears instead of the one in the picture, something is not set correctly.

The most common issues are:

- SQL Server is not installed on the local PC (if Default database location chosen)

- SQL Server is installed but authentication mode is Windows authentication mode– not Mixed mode

- Problem with the local network/internet connection (if Not default database location chosen).

- Not all parameters are correct – IP Address, Port, User, Password, Security... (if Not default database location chosen).

2.2 Client Setup

Client setup is made through the menu Settings->Servers. Here you can change or add new Servers. The default server is Local (Local = the Client is on the same PC as the Server). If your Server is on a remote PC (not the same PC as the Client) then you will need to add new Server with the IP address of the remote PC and the port (Events port) configured in the Server Setup (default is 54321).
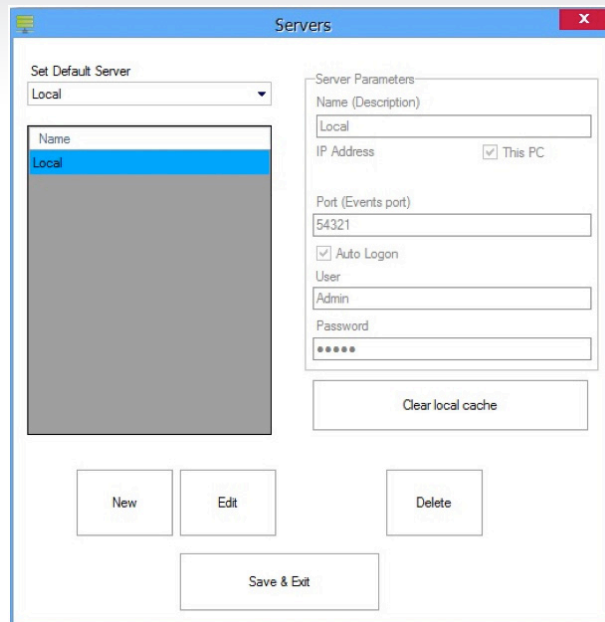
Client keeps local cache for each Server in order to speed up the connecting procedure with the server (the necessary data for a client to run is taken from the Server only once. Each subsequent connection only loads new changes made.)

After configuring the Servers, you can choose a Server from the "Connect To" menu in the top-right corner of the Client. You can connect to other Servers without closing the Client by clicking the Disconnect button and then choose a server in the dropdown list. If you want to see info about the current server, just click on the icon next to the "Connect To" menu and an info window will be displayed onscreen.
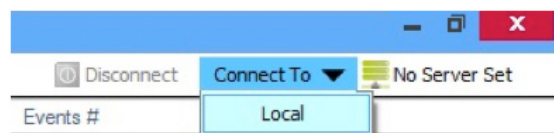
If "Auto Logon" is not checked for the current server, when connecting a login window appears onscreen asking for credentials. (The default setting is Operator name = "Admin" and Password = "admin")
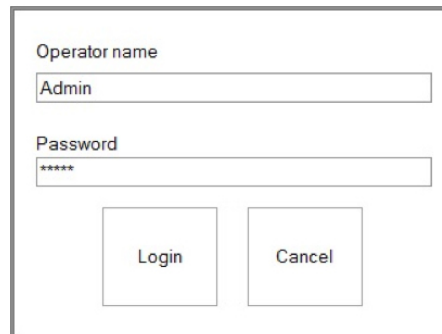
3. Creating Portals

3.1 What is a portal?

A Portal is a communication link between the Server and the devices in the system. A Portal has two parts - logical, recognizable by the software, and physically – an electronic device connected to a computer and other devices in the system known as converters.

The Logical part can be:

1. Serial port (COM)
2. Network port

The Physical part can be:

1. TCP/IP port on a CV-350 controller
2. RS232 to RS485 converter, connected to a logical Serial port
3. USB to RS485 converter, connected to a logical Serial port
4. TCP/IP to RS485 converter, connected to a logical Network port

The Server can use more than one portal to connect to devices in the system. Devices in the system can be connected to the Server, with one portal only. Only one Serial portal can be used in the Server.
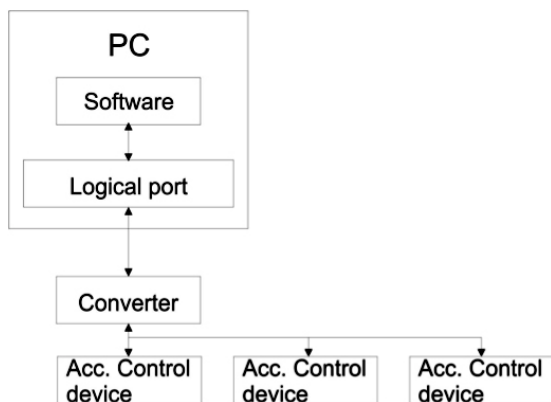
3.2 Add a Network Portal

- Right-click on the Portals item and select "Add portal"
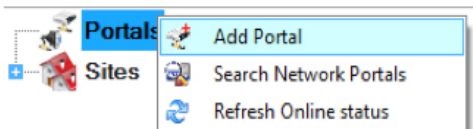
- Check the Network communication option
- Consult your installer for the portal's IP address and Port, and fill in the Portal properties window with the data.
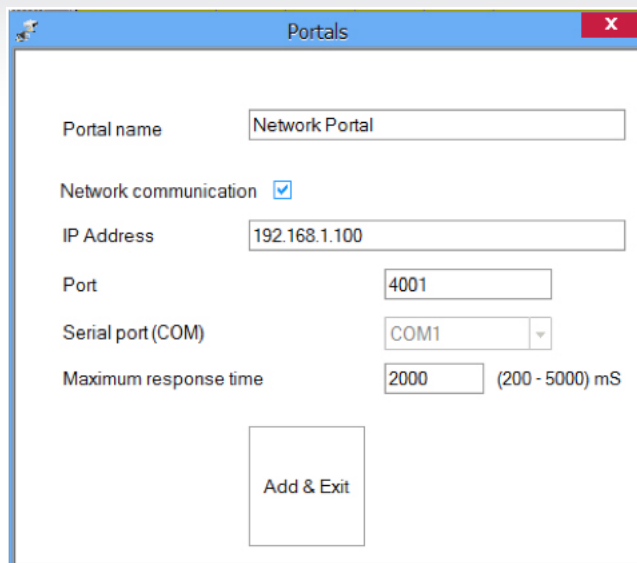
- Click on Add & Exit
- The new portal is shown below the Portals item with a given name and a picture of the network portal

3.3 Search Network Portals

This procedure is valid only if you have CV-350 controllers connected to the network

- Right-click on the Portals icon and select the Search network portals
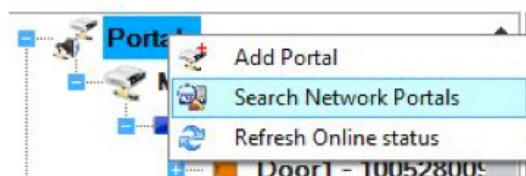
- On the Search portal window select the port to search (default is 8000)
- Click on the Search button and wait

- If any portal is found, it will be displayed in the table

- If the Portal does not exist in the Server click on the Add column button in the portal row.

- The Portal will be added to your collection of Portals and will use the IP address as its name.

3.4 Configure the Portal

- Right-click on the Portals icon and select the Search network portals

- On the Search portal window select the port to search (the default is 8000)

- Click on the Search button and wait
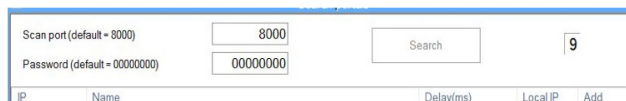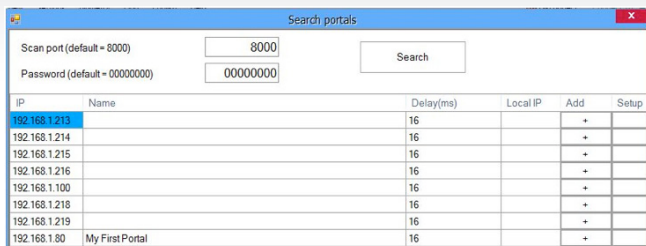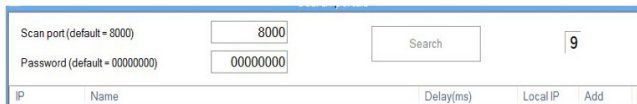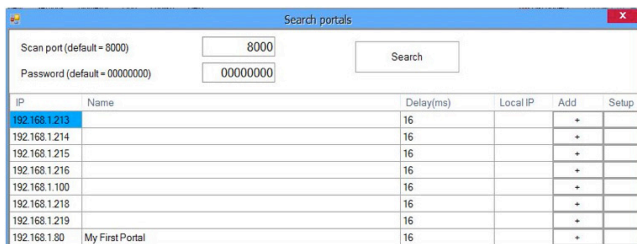

- If any portal is found, it will be displayed in the table

- Enter an 8 digit device password (factory default is 00000000)

- Find a row with a portal to configure and click on the appropriate Setup button. The following window will be shown

- After the server executes the request, the setup portal window will be shown with the portal settings. If the values are empty, settings from the CV-350 cannot be read.
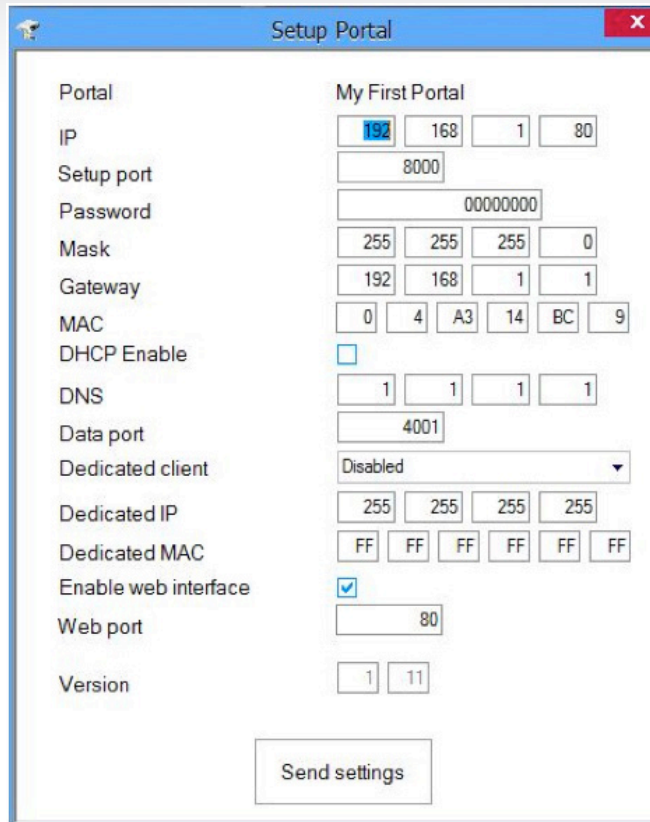
- Enter new settings:

- IP: IP address of device

- Setup Port: Network port for search and setup. Changing is not recommended

- Password: Password for access to read and change the settings of the CV-350. It is recommended to change the default password and use it for all converters in the system.

- Mask: Enter the device subnet mask

- Gateway: Default gateway

- MAC: Physical address of the device. Changing is not recommended

- DHCP Enable: Enable the DHCP client

- DNS: Address of the DNS server

- Data Port: Port used for communication between the Server and devices behind the converter

- Dedicated Client: To forbid unauthorized access to devices connected to the portal from another system, select one of the following options

  a) Disabled - no source security checking

  b) MAC only- the source MAC address must be equal to the Dedicated MAC value

 c) IP only– the source IP address must be equal to the Dedicated IP value

d) IP or MAC - at least one of the conditions from point b and c must be true

e) IP & MAC - both b and c conditions must be true

- Enable Web Interface: enable or disable the CV-350 web interface for configuration

- Web Port: Web interface port

- Version: Read-only field displaying the firmware version of the converter

- Click on Send settings to configure the device. After the server sends the settings the following will be shown in the event window.

Time	Portal	Controller	Reader	Door	Event
29-Jan-14 3:56:53 PM					Setup Portal : Service setup done.

3.5 Add a Serial Portal

- Right-click on the Portals item and select "Add Portal"


-
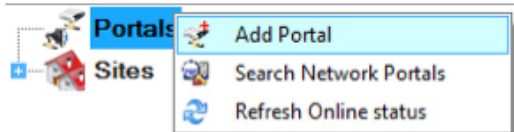
Enter the portal name

- Make sure that the Network communication option is not checked

- Select the COM port from the Serial port drop-down list (COM ports on the Server PC)

- Click on Add & Exit
- The New portal is shown below the Portals item with a given name and a picture of the serial portal

4. Add a Controller

- Right-click on a portal connected to the controller and select Add controller>EWS
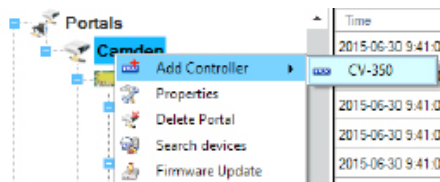
- Enter Name and Serial number of the controller. The Serial number is provided on the controller's board.

- Click on the Save and Exit button

- The New controller and the controller peripherals are shown under the portal item
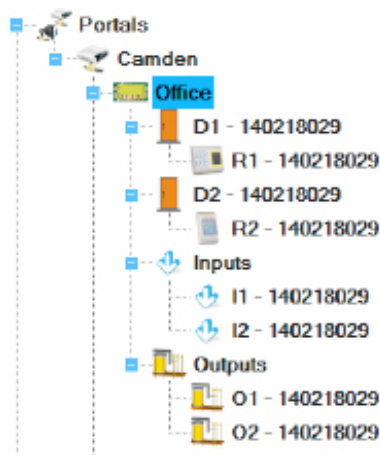
- In order to see if the CV-350 is online and communicating with the PC, right click on the Controller and select "Check Version" from the controller drop-down menu. In the event panel it will be indicated if the controller is on line or not. If the Serial Number does not match, the controller will not go on line. If there is no communication, the controller name will have a red background color in the tree view.

5. Readers

- Expand the Door item to view the readers
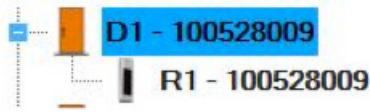
- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu

- Set the values in the Basic tab
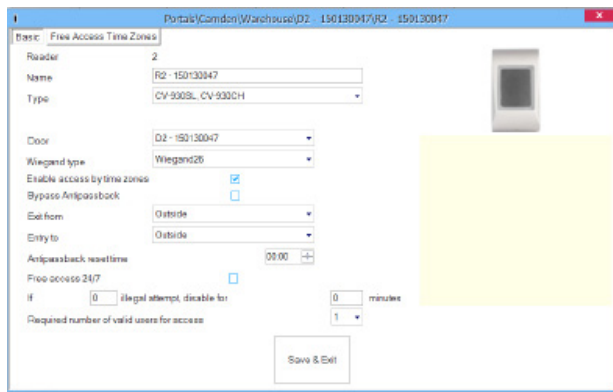
- Name: Enter the Reader's Name

- Type: Select the Reader's Type

- Entry mode: This selection is optional and is visible if reader supports different modes of entry. E.g. if using a CV-930-20 Card/Keypad Code reader then four modes of entry are available.
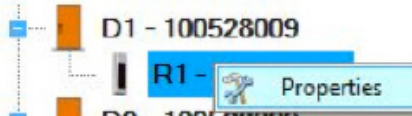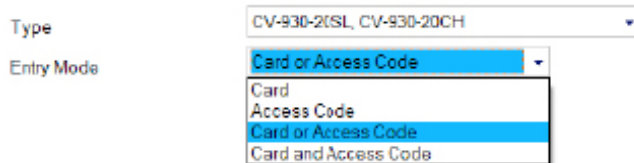

- Door: Select which controller door the reader is attached to.

- Wiegand Type: Select the Wiegand type of the Reader

- Enable access by time zones: enables the settings in the Free Access Time Zones tab.

- Bypass Antipassback: if this is checked antipassback will not be valid for this reader.

- Exit from: set the area which is exited.

- Entry to: set the area which is entered.

- Antipassback reset time: set the duration time of antipassback.

- Free access 24/7: grant all users 24/7 utilisation.

- In the event of (number) illegal attempts disable for (number) minutes: set the number of illegal attempts and the time of disabling the reader.

- Required number of valid users for access: Number of different users that must be registered at the reader to grant access.

- Select the Free Access Time Zones.

- Apply the time zones for the reader.

- Click on the Save & Exit button

- Repeat the reader configuration procedure on the other readers driven by the same controller

5.1 Fingerprint Readers

If fingerprint readers are used, additional reader menu items are available
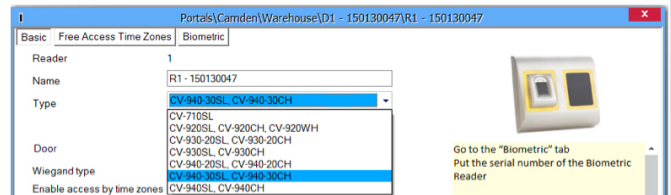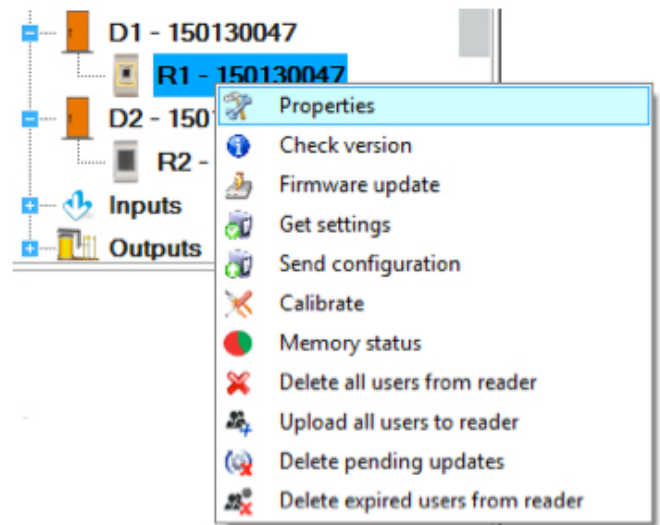

5.2 Add or Modify a Reader

- Expand the Door item to view the readers

- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu

- Set the reader type to one of the fingerprint models in the Basic tab

- Select the Biometric tab and set the values

- Serial: Fingerprint Reader Serial Number

  - Buzzer: Select if the reader will provide audible annunciation when a finger is presented.

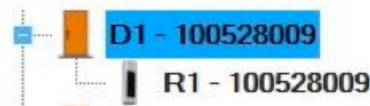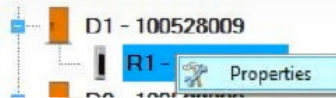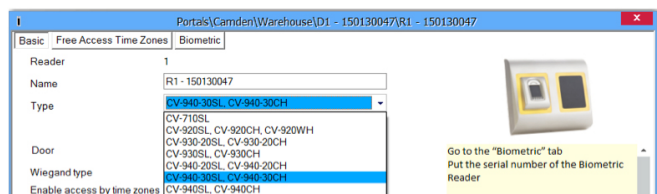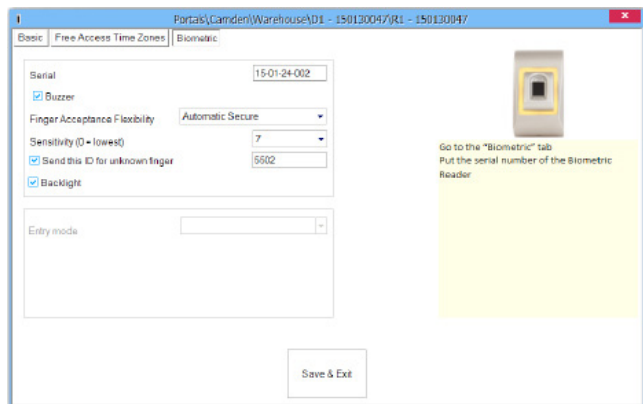 - Finger Acceptance Flexibility: Accepted tolerance. The recommended value is "Automatic Secure".

  - Sensitivity: Bio-sensor sensitivity, the recommended value is 7, most sensitive.

- If devices have a keypad (CV-940-20, CV-940-30), further settings will be available:

  - Entry Mode:

    "Finger" (the keypad is inactive)

    "Access Code or Finger" (The Fingerprint Reader will be configured to accept either Access Codes or fingers)

    "Access Code and Finger" (The Fingerprint Reader will be configured for double security, requiring a Access Code and a corresponding finger. Only the right combination will send the user Wiegand to the CV-350)

- Send this ID for unknown finger:

    Sends the desired Wiegand when an unknown finger is applied.

- Click on the Save & Exit button

6. Users

Double-click on the Users item in the Users Panel to open the Users window

6.1 Add a user

- Click on the New User button

- Enter the Name of the User
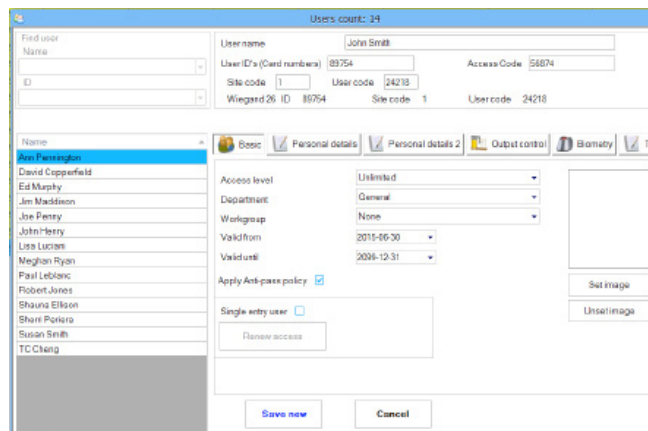
- Enter theUser ID (card number). If there are two numbers on the card with values less than 65536 then use the Site code and the User code box.

  - Enter Access Code if in the system will be used devices with keypads

  - Select the Access level from the Access level drop-down list box

  - Select the Department from the drop-down list box

  - Select Workgroup

  - Select the from-until validity period

  - Click on the Set image button and then browse for the User's image

- If Apply Anti-pass policy option is checked, user must behave by APB settings of the readers, otherwise user will have no APB restriction.   - Single entry user: A User will have one-time entry an all readers defined by user access level. If the user has used his/her one-time entry, on the next upload of the user in the CV-350 controller, one-time entry will be renewed.

- Fill Personal details of the user if required in the Personal details tabs.

- If the User should activate some outputs (not door relays), click on the Output control tab to select outputs

- Click on Save

- The entered User is added to the user table on the left side

6.2 Edit a User

- Select the User to be modified in the users table on the left side of the Users window

- Click on the Edit button

- Modify the user data (including the name if required)

- Click on the Save button

6.3 Delete a User

WARNING!

Deleting a user erases the user from database. If you need to keep an activity record of the user, you can change the access level to "No access" instead of deleting the user, or generate the necessary reports and save them to a file (PDF is recommended), before deleting the user.

- Select the user to be deleted in the users table on the left side of the Users window

- Click on the Delete button

7. Troubleshooting

- CV-350 portal is not found in "Search network portals"

  1. Check if the CV-350 is powered

  2. Check if the CV-350 and the PC are connected to the network

  3. Disable the network firewall

  4. Check the port value in the search window

- CV-350 portal is found, but cannot be configured

  1. Check if the password in the search window matches the CV-350 password. If you forget the password, use the reset button in the CV-350 to reset it to its default values.

  2. Check the port value in the search window

  3. If the PC IP address has a different IP network, set it to the same network, configure the router and restore the PC settings to the previous value.

     • Example:

       - If the PC IP address is 10.10.10.5 and the CV-350 IP address is 192.168.1.100, set the PC IP to value 192.168.1.X where X is between 1 and 254, taking care not to set the same address as the CV-350 or another existing IP address in the network

       - Configure CV-350

       - Set the PC IP address back to 10.10.10.5

- CV-350 does not react on the reader reading (Reader's LED stays inactive)

  1. CV-350 Wiegand is not set to match the reader

  2. Check the reader power supply

  3. Replace the reader

- Devices connected to the USB to RS485 converter are offline

  1. The USB converter is represented as a COM Port on the PC side. If the converter is plugged into another USB port, the COM port number will have changed. The solution is to plug the converter into the initial USB port or to change the COM port value in the Portal properties.

  2. Check the converter connections

- Controllers change connection state (controller icon changes background color to red)

  1. If the controller is using an RS485 connection, check for cable damage, termination load (120 Ohm) and quality of cables

  2. More than 31 controllers and/or readers are connected to the same RS485 bus

- Cannot get the events report for a User

1. The user was deleted and entered again with the same name. Once the user is deleted, all events for the user are deleted. Entering a new user with same name will not retrieve the events. The solution is not to delete the user (you can change the access level to "No Access" instead) or generate reports for the user and export them to a PDF, Excel or Text file for keeping.

7.1 Biometry

- Reader reading performance is decreased

1. Check if the fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use a soft and dry cloth only.

2. The reading area is damaged. If the damage is minor, try to calibrate the sensor

- Fingerprint is not recognized normally

1. If your finger is wet, retry after drying it.

2. When your finger is too dry, retry after blowing on your fingertip.

3. If you have a cut on your registered finger, register another fingerprint.

- Fingerprint is recognized, but CV-350 reports another ID number

1. If the user is not deleted from the reader and the user is enrolled again with a new ID, the reader will recognize the finger with the first ID. To resolve this, delete all users from the reader and re-upload all users to the reader.

Appendix A

Using CV-7400 Reader with the CV-350 Series Access Control System

When using Camden CV-7400 dual format readers are easily interfaced with Camden CV-350 Series access control systems. Some consideration must be given to the wiring and software setup to ensure a quick and easy installation.
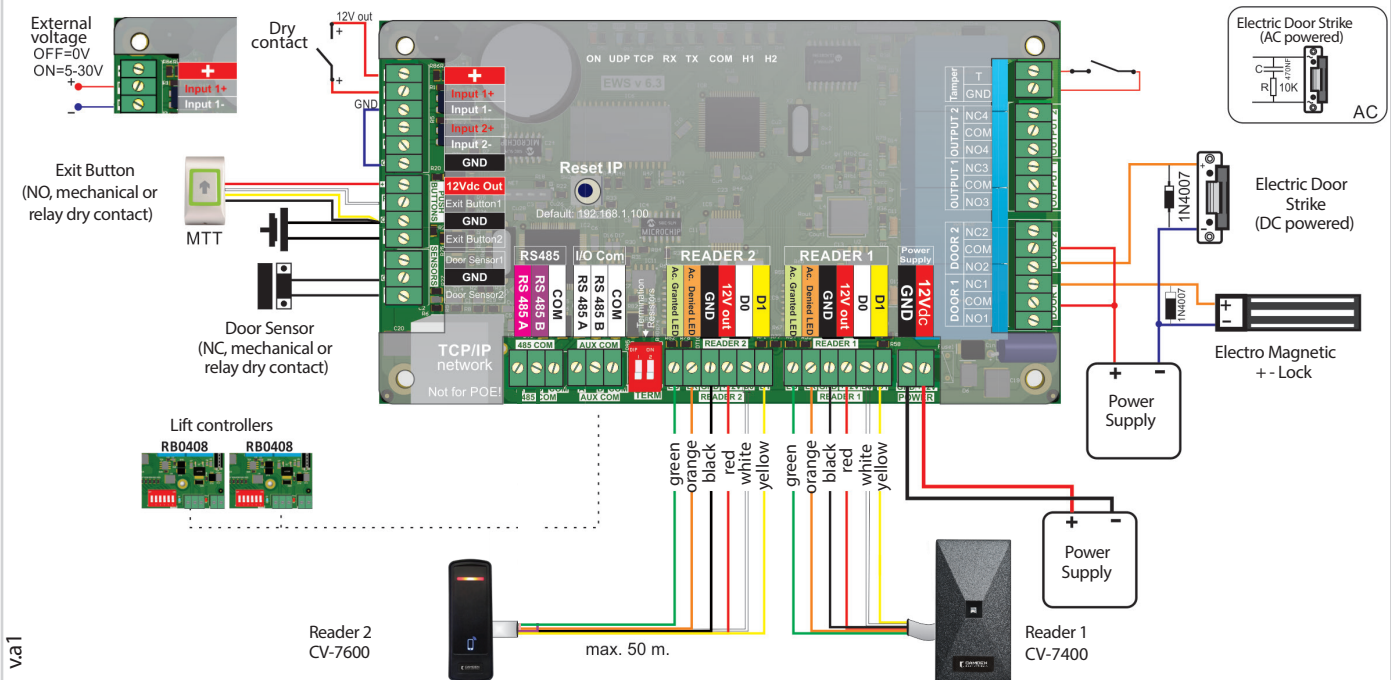

Software

Camden HID 37 bit formatted cards require additional configuration in the CAMS (Camden Access Manager Software) in order to be read and displayed properly.

Create a Custom HID format

From within CAMS access the Settings Menu. Select Wiegand. The Wiegand screen will appear. On this screen you can setup customized wiegand formats. To setup Camden HID 37 bit format cards, use the following settings:
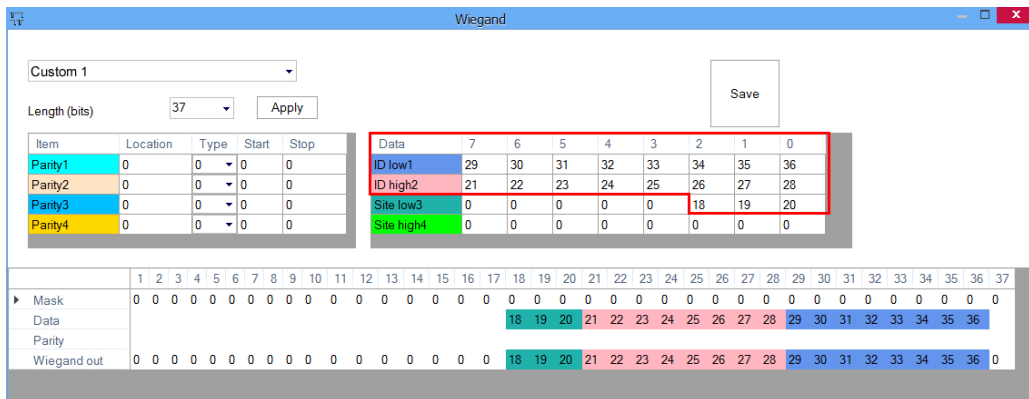
- Select Custom 1 from the pull down menu.
- Set the Length (bits) to 37 and select APPLY.
- Set the DATA as shown in the outlined box above.
- Select SAVE.

Add a CV-7400 to CAMS

When a controller is added to a portal within CAMS, default readers are selected. Open the Properties dialog for the reader you wish to setup.
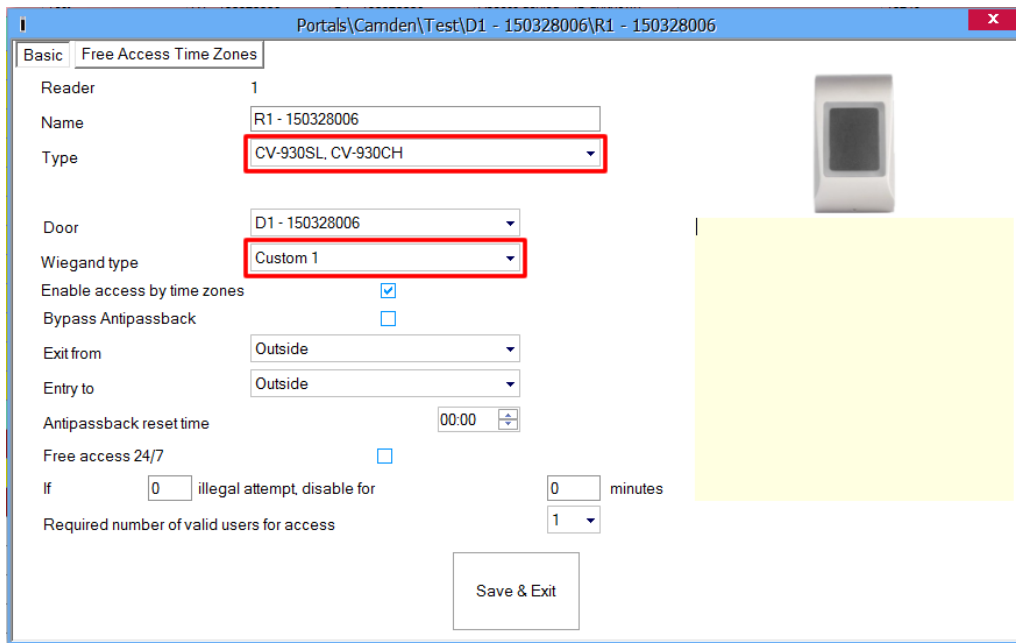
- Select the Reader Type as CV-930SL, CV-930CH.
- Select the Wiegand type as Custom 1

| Push Buttons | Keypads | Strikes | Magnetic Locks | Key Switches | Relays & Timers | Access Control |