

**PASSPORT TECHNOLOGIES INC.
SICM INSTALLATION
MANUAL ADDENDUM
USER INTERFACE GUIDE**

JANUARY – 2018

WWW.PASSPORTTECHNOLOGIES.COM

**Copyright © 2016 PASSPORT TECHNOLOGIES INC.
All rights reserved**

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights reserved, in particular in the event of a patent being granted or the registration of a utility model or design.

Disclaimer of Liability

We have checked the contents of this manual for compliance with the hardware and software described. Nevertheless, discrepancies may exist. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions. Suggestions for improvement are welcomed.

Table of Contents

1. Landing Page	4
2. System Status	4
3. Checkins (Optional).....	5
4. General: Users and Date Time.....	5
5. Settings.....	5
6. Provider Source	6
7. Schedule (Optional)	6
8. Member Restrictions (Optional)	6
9. Manual Enrollment (Optional, Biometric systems only)	7
10. Universal Code Access (Passkeys).....	7
11. Tailgate (Optional)	8
12. Tailgate Notifications (Optional).....	8
13. Tailgate Configuration (Optional).....	9
14. Reports (Optional)	9
15. Diagnostics (Standard) and Synchronize (Optional).....	10
16. Network Availability	10

SICM User Interface Guide

Thank you for purchasing a Passport Technologies Inc. Software Interface and Control Module (SICM). This section applies to systems with Options that require access to the SICM User Interface typically found at <http://sicism>. We recommend that you bookmark or favorite the url or IP address of your SICM for easy access as required.

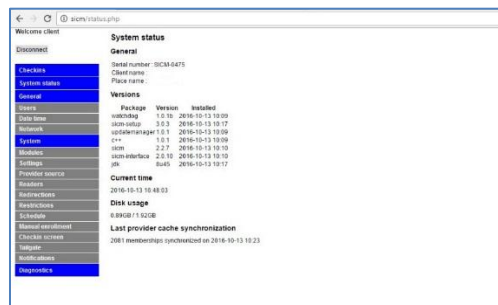
1. Landing Page

You can find the SICM Interface on any web browser on the same network as the access system using its IP address or at <http://sicism>. The landing page looks like the following and if you click on the Configuration Icon on top and towards the right (indicated by the black arrow), it will bring you to the Connection page where you will be required to enter a Username and Password. For the initial session, use the word “client” (lowercase, no quotation marks) as both the Username and the Password. You can change the Password under the Users tab if so desired.



2. System Status

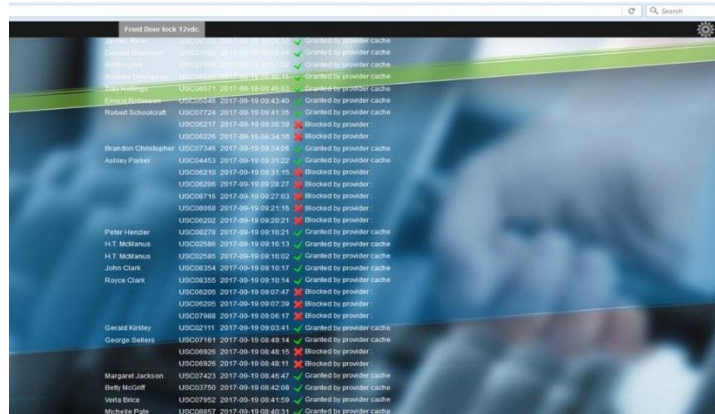
Once you've entered your Username and Password and clicked the Connect button, the System Status page will appear.



As you can see from the menu to the left, there are several sections of the SICM Interface available. Keep in mind that your device may have more or fewer sections and that not all sections will be enabled depending on the Options installed at the time of order. The System Status page provides an overview of system configuration as well as information on the latest Database Synchronization (or Local Database download), if applicable.

3. Checkins (Optional)

If the Passport Checkin Screen Option is enabled, the Checkins page provides a scrolling list of member access attempts along with an indication of whether access was granted or denied and why, along with their membership photo if available. The Checkin screen also includes a virtual door unlock button that allows staff to unlock the access door from the screen. The Unlock button may be activated remotely through third party remote control applications such as: TeamViewer, LogMeIn, AeroAdmin, RemotePC, etc. If it is not enabled, the link will simply bring you back to the Landing page. Please contact the Passport Technologies Technical Support team (support@passporttechnologies.com) for further details or to order the option.

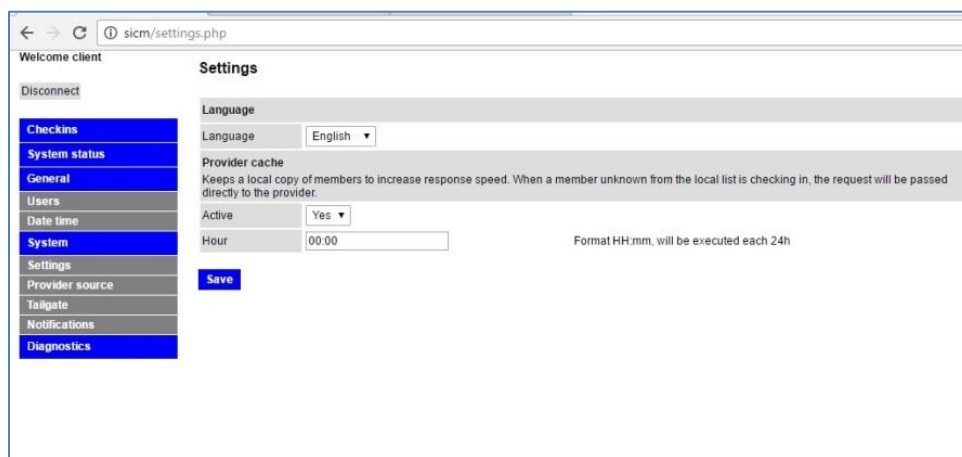


4. General: Users and Date Time

The General tab includes the Users section as well as the Date and Time section. Click on the Users tab if you would like to change the Password required for accessing the Interface. Store the Password safely as you won't be able to access the Interface if you forget it. Click on the Date Time tab if you would like to change the date and/or time on your device.

5. Settings

You will find the Settings tab under System. This is where you can enable or disable the Local Database Option (or Membership Synchronization Option) as well as change the time at which the download/synchronization occurs. Be careful to select a time that is not generally busy at the facility nor on the internet/network as the process can consume significant bandwidth.

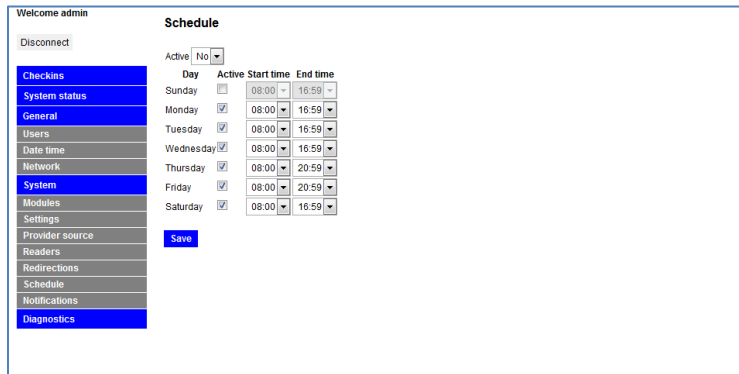


6. Provider Source

This section is for information purposes **ONLY. DO NOT**, under any circumstances, change any information on the Provider Source section as this will disable the integration with your software provider and re-integration charges may apply.

7. Schedule (Optional)

The Schedule section is used to configure the active weekly schedule for your Passport Technologies access management system (if the Option is enabled). If the Active checkbox is selected next to the day of the week, the scheduling option is enabled for that day and the access system will be operational between the start and end times indicated. If the Active checkbox next to the day of the week is not selected, the scheduling option is disabled and the access system will be disabled for the entire day. **NOTE:** Outside the Active schedule, members will **NOT** be able to access facilities using their ID device, even if their memberships are valid.



The screenshot shows the 'Schedule' configuration page. On the left is a navigation menu with 'Schedule' highlighted. The main content area has a 'Disconnect' button and an 'Active' dropdown set to 'No'. Below is a table for configuring the weekly schedule:

Day	Active	Start time	End time
Sunday	<input type="checkbox"/>	08:00	16:59
Monday	<input checked="" type="checkbox"/>	08:00	16:59
Tuesday	<input checked="" type="checkbox"/>	08:00	16:59
Wednesday	<input checked="" type="checkbox"/>	08:00	16:59
Thursday	<input checked="" type="checkbox"/>	08:00	20:59
Friday	<input checked="" type="checkbox"/>	08:00	20:59
Saturday	<input checked="" type="checkbox"/>	08:00	16:59

A 'Save' button is located below the table.

8. Member Restrictions (Optional)

The Member Restrictions section is used to configure the active schedule for different membership types (if the Option is enabled and your software platform supports the feature). If the Active checkbox is selected next to the day of the week, the Restrictions option is enabled for that day and the access system will be operational between the start and end times indicated. If the Active checkbox next to the day of the week is not selected, the scheduling option is disabled and the access system will be disabled for the entire day. The list of available Member Restriction groups may be selected from the "Service Category" only. **NOTE:** Outside the Active schedule, members will **NOT** be able to access facilities using their ID device, even if their memberships are valid. Please contact Passport Technologies support for more information.



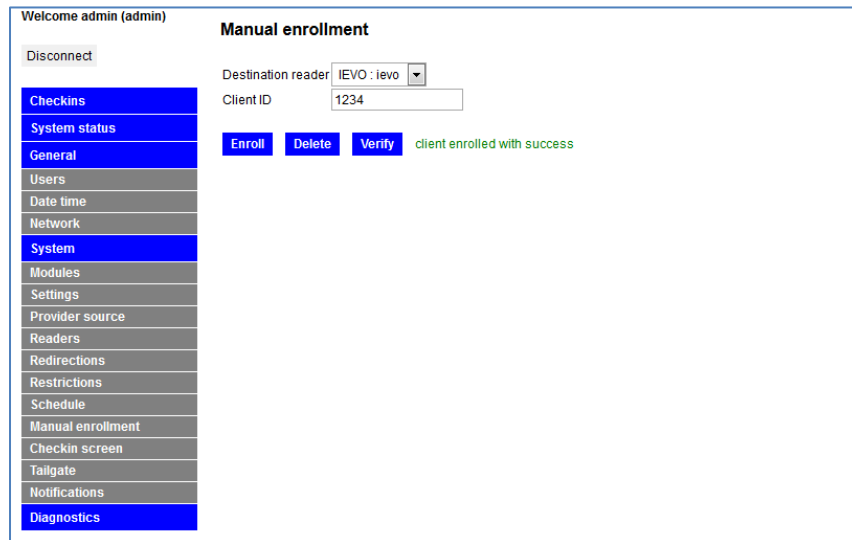
The screenshot shows the 'Restrictions' configuration page. On the left is a navigation menu with 'Restrictions' highlighted. The main content area has a 'Disconnect' button and a table for configuring member restrictions:

Name	Outputs	Programs	Day	Active	Start time	End time
Week-end swimming	Sélection : 1	Sélection : 1	Sunday	<input type="checkbox"/>	00:00	23:59
			Monday	<input type="checkbox"/>	00:00	23:59
			Tuesday	<input type="checkbox"/>	00:00	23:59
			Wednesday	<input type="checkbox"/>	00:00	23:59
			Thursday	<input type="checkbox"/>	00:00	23:59
			Friday	<input checked="" type="checkbox"/>	08:00	19:59
			Saturday	<input checked="" type="checkbox"/>	08:00	19:59
Restriction 1	Sélection : 0	Sélection : 0	Sunday	<input checked="" type="checkbox"/>	00:00	23:59
			Monday	<input checked="" type="checkbox"/>	00:00	23:59
			Tuesday	<input checked="" type="checkbox"/>	00:00	23:59
			Wednesday	<input checked="" type="checkbox"/>	00:00	23:59
			Thursday	<input checked="" type="checkbox"/>	00:00	23:59
			Friday	<input checked="" type="checkbox"/>	00:00	23:59
			Saturday	<input checked="" type="checkbox"/>	00:00	23:59

A 'Save' button is located below the table.

9. Manual Enrollment (Optional, Biometric systems only)

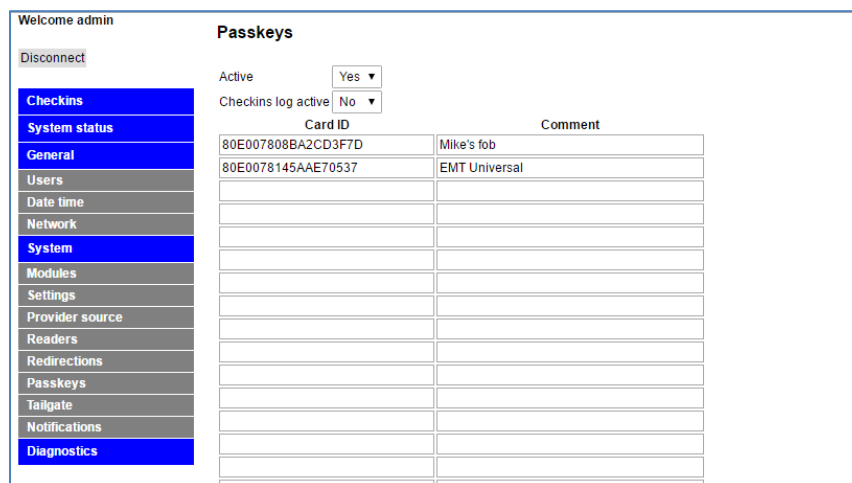
If your system includes a Fingerprint scanner, the Manual Enrollment Section is used to upload and convert biometric data used to identify members on your membership management platform. Select the desired biometric reader from the drop down list; enter the Client ID number (8 numeric digits max); have the member present their fingerprint (index finger recommended); click Enroll and wait for the response message. To test, have the member present the same fingerprint and click verify. The biometric data is now converted into numeric data for your software platform. Don't forget to save the Client ID number in the appropriate field in your Membership Management platform!



The screenshot shows the 'Manual enrollment' section of the admin interface. On the left is a navigation menu with 'Manual enrollment' selected. The main area contains a 'Destination reader' dropdown menu set to 'IEVO : ievo' and a 'Client ID' text input field containing '1234'. Below these are three buttons: 'Enroll', 'Delete', and 'Verify'. A green message 'client enrolled with success' is displayed to the right of the buttons. A 'Disconnect' button is located at the top left of the main content area.

10. Universal Code Access (Passkeys)

This Option allows you to configure up to 10 separate member IDs for Universal Access. Allowing the ID holder to access the facilities under any condition, unless power is out. The Universal Passkeys are typically assigned to facilities owners and managers as well as local authorities as required. The only way to deny access for the ID holder is to remove the ID number from the Passkeys list.

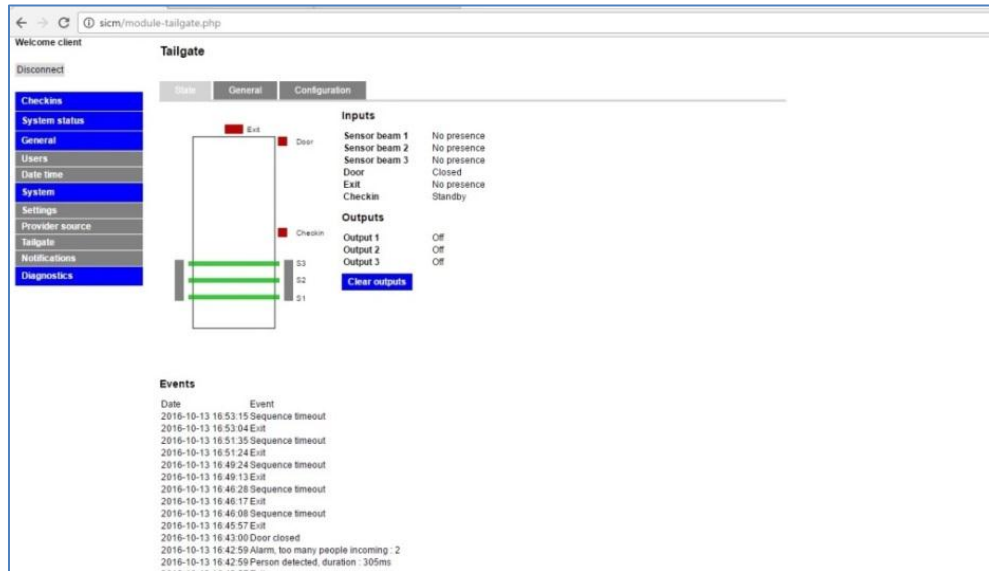


The screenshot shows the 'Passkeys' configuration section. It includes an 'Active' dropdown menu set to 'Yes' and a 'Checksins log active' dropdown menu set to 'No'. Below these is a table with columns for 'Card ID' and 'Comment'. The table contains two entries: one with Card ID '80E007808BA2CD3F7D' and Comment 'Mike's fob', and another with Card ID '80E0078145AAE70537' and Comment 'EMT Universal'. There are several empty rows below the existing entries.

Card ID	Comment
80E007808BA2CD3F7D	Mike's fob
80E0078145AAE70537	EMT Universal

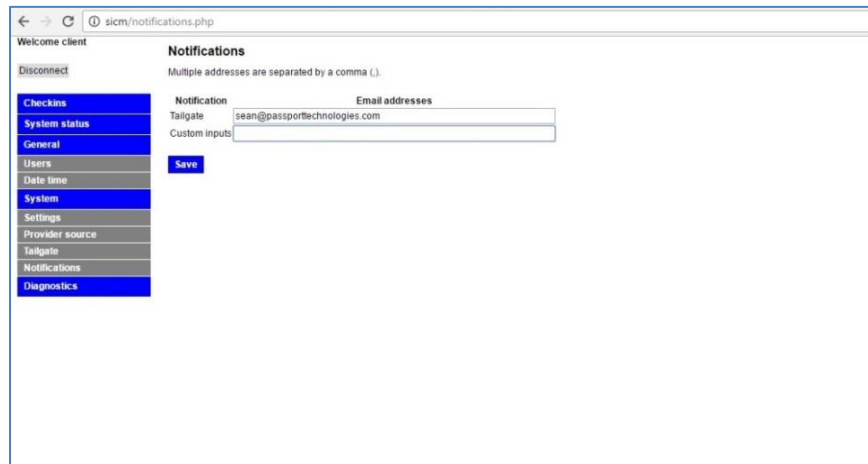
11. Tailgate (Optional)

The Tailgate section is used to provide status for your tailgate system (if the Option is enabled and the system is installed) as well as to allow certain configuration changes. **WARNING:** changes to your Tailgate configuration may disrupt system functionality. Please contact the Passport Technologies Technical Support team for further details or troubleshooting support as required.



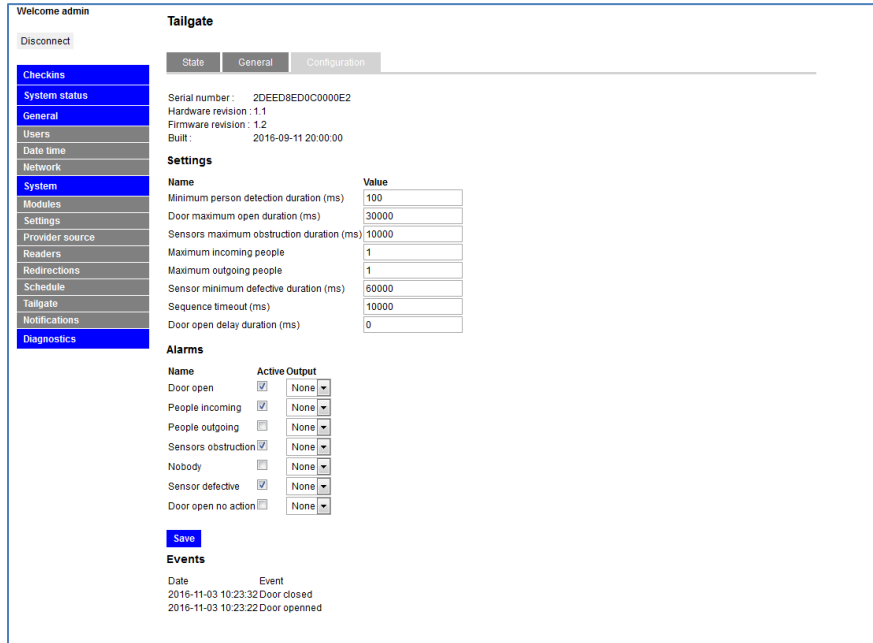
12. Tailgate Notifications (Optional)

The Notifications section only appears if the Tailgate Option was installed. It is used strictly to change the email addresses for tailgate notifications. Use a comma to separate multiple email addresses.



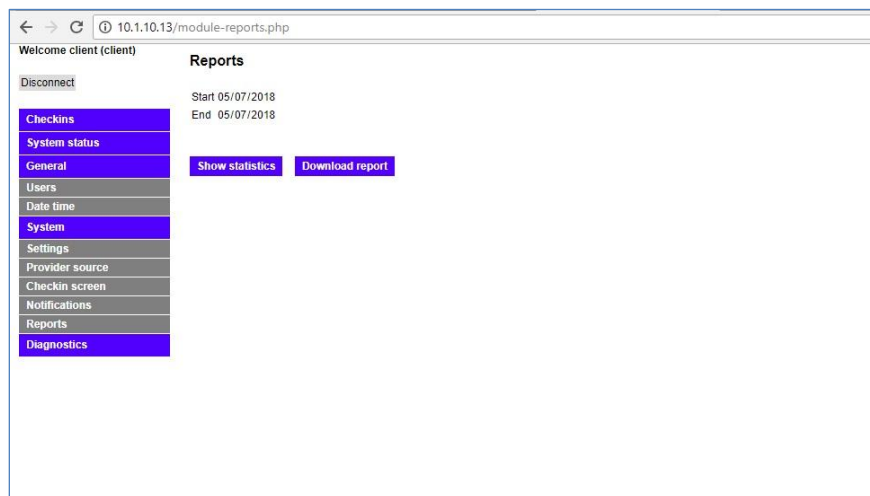
13. Tailgate Configuration (Optional)

The Configuration tab under the Tailgate section only appears if the Tailgate Option was installed. It is used to enable and disable Tailgate output features as well as to adjust feature settings. **Note:** The settings are configured to Factory standards and should only be adjusted under specific circumstances as improper configuration may result in a malfunction of the Tailgate system. Please contact Passport Technologies Support for more information.



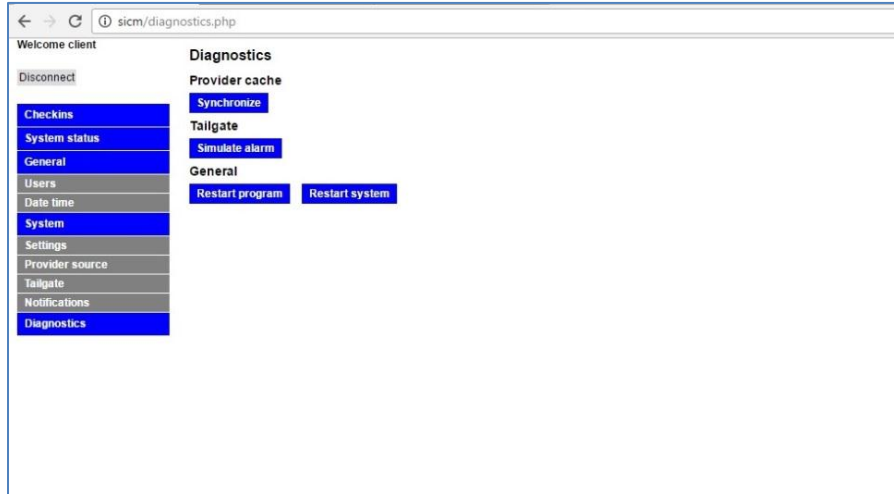
14. Reports (Optional)

The Reports page allows you to view and download the checkin attempts based on a selectable date range. This feature can be useful for customer service to follow up on failed checkin attempts as well as for reporting on all access point activities for various purposes.



15. Diagnostics (Standard) and Synchronize (Optional)

The Diagnostics page varies in appearance based on the Options installed on the SICM. If installed, the Provider Cache Synchronize button allows you to immediately download your entire active membership database from your software platform so that all current members will be able to access the facility in the event of internet disruptions. This process consumes significant bandwidth and should not be initiated more than twice per day. The Tailgate Alarm button only appears if the Tailgate Option was installed and is used to simulate an alarm (buzzer or light) if applicable and if installed.



16. Network Availability

The SICM is a network/internet based device and as such must be connected to the network via router only, and not a modem. To view the SICM Interface, its IP address is required. There are several tools available to ensure that the SICM is properly connected to the network and to find the SICM IP Address as required. Here are a few suggestions that may or may not apply to your specific computer depending on the configuration of your network:

Windows PCs offer several tools to find the SICM IP address on your network:

From the Start Up menu, open Search and type cmd in the search field. Open the Command Prompt and type in the following command: “ping sicm” and press Enter on your keyboard. If the SICM is found on your network, the IP address will appear in the ping response message.

MAC computers and the App Store offer tools to access your network information:

Open Terminal from within the Applications/Utilities folder, or just type Terminal into Spotlight (CMD + SPACEBAR) and click on the icon when it’s found. Once Terminal is open, type “ping sicm.local” and hit Enter. If the SICM is found on your network, the IP address will appear in the ping response message. Fing is a network discovery application that is available through the App Store.



In order to reconnect with the network. Under certain conditions, the SICM may lose connectivity with the local network. To reconnect, simply unplug the 5VDC power supply to the SICM from the 120VAC power outlet and make sure the bottom RED light on the front of the SICM goes out for at least 5 seconds. Reapply power to the unit and wait 5 minutes for the SICM to reboot and obtain its network connection and IP Address. Please refer to Question 5 to verify that the SICM is now connected to the network. If this fails to resolve the issue, please contact Passport Technologies support.

Passport Technologies Inc. warrants its products to be free from defect and workmanship for a period of one year from date of delivery. Phone and internet support is included within the warranty period - for Passport Technologies Inc. products only. Support for external devices such as computers or network connections is available at a reasonable hourly rate if required. Software support is provided by your software provider and is typically included in their monthly fees.

Passport Technologies Inc.
320 College Street North
Richmond, QC J0B 2H0
Canada

<http://www.passporttechnologies.com/support-and-tools.html>

Toll Free: 1.855.727.7832 Ext. 2
Email: support@passporttechnologies.com