Technical Support

For technical support, please contact your Cleaver-Brooks authorized service representative. C-B representative contact information is available at www.cleaverbrooks.com/Find-a-Rep/Index.aspx

Sierra Monitor Corporation does not provide direct support. Should circumstances require, Cleaver-Brooks will contact Sierra Monitor Corporation on your behalf.

Support Contact Information:

Cleaver-Brooks
221 Law Street
Thomasville, GA 31792

Customer Service:
(229) 227-2614
(800) 250-5883 / (229) 226-3024

Website: www.CleaverBrooks.com
Before registering:
The following items should be complete before moving forward with SMC Cloud registration.

- FieldServer products intended for SMC Cloud registration must already be installed and running.
- FieldServer Gateway(s) and/or Router(s) are connected to the internet.
- The manufacturer's SMC Cloud Administrator has already set up an SMC Cloud account.
- The field installer has received SMC Cloud login information from the SMC Cloud Administrator.

A Quick Start Guide for Field Installation

- Type the FieldServer IP Address into a web browser.
- Once connected, the FS-GUI or customer applications will be displayed.

- Obtain login details from support.
- Go to the SMC Cloud registration page and fill in ALL relevant information.
  - For FS-GUI, click the "SMC Cloud™" button on the top right corner of the page.
  - For customer application features, click the "SMC Cloud™" tab on the left side of the page.
  - For the BACnet Router, EZ Gateway Modbus to BACnet and EZ Gateway KNX to BACnet, click the "SMC Cloud™" tab along the top of the page.

- Go to www.SMCCloud.io and type in the appropriate login information as per registration login.
- Confirm the registered FieldServer is viewable from the Device Management tab.

- Device Management
- User Management (Admin only)
- Notifications

- Reports
- Audit Logging
- Data Logging (Admin only)
CONTENTS

CONNECTING TO FIELDSERVER (FOR FIELD INSTALLERS) ................................. 7
   Discover the IP Address of the FieldServer ........................................... 7
   Change Network Settings for the FieldServer ......................................... 7

LOGGING IN (FOR FIELD INSTALLERS) .......................................................... 9
   New User Setup ......................................................................................... 9
   Registration Process ................................................................................. 10

CUSTOMER APPLICATION FEATURES ......................................................... 12
   Using System View to Generate Data Logging ......................................... 12
   Using Historian to View Data Logging Information .................................. 14
   Using Device View to Send a Snapshot of the Device Data ....................... 16

LOGGING INTO AND USING THE SMC CLOUD (FOR SUPPORT) ............... 17
   Account Management .............................................................................. 17
      Editing the Profile .................................................................................. 18
      Changing the Password ......................................................................... 18
      Enabling/Disabling Notification Audio Alerts ......................................... 18
   Device Management ................................................................................ 19
      Map Elements ....................................................................................... 19
      Connecting to a Device ......................................................................... 20
   Notifications ............................................................................................ 21
      Configure a Notification Delivery ......................................................... 21
      Using System View Events to Generate Notifications ........................... 22
   Dashboards .............................................................................................. 24
      Rename a Dashboard ............................................................................ 24
      Set Up Dashboard .................................................................................. 24
      Change the Dashboard Time Range ...................................................... 25
      Delete a Dashboard ............................................................................... 27
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FieldServer Toolbox</td>
<td>7</td>
</tr>
<tr>
<td>Configure Device Window</td>
<td>8</td>
</tr>
<tr>
<td>Device Network Settings Window</td>
<td>8</td>
</tr>
<tr>
<td>Welcome to SMC Cloud</td>
<td>9</td>
</tr>
<tr>
<td>Setting User Details</td>
<td>10</td>
</tr>
<tr>
<td>FS-GUI Screen</td>
<td>10</td>
</tr>
<tr>
<td>Customer Application Landing Screen</td>
<td>11</td>
</tr>
<tr>
<td>Registration Information Page</td>
<td>11</td>
</tr>
<tr>
<td>System View Listing Device</td>
<td>12</td>
</tr>
<tr>
<td>System View Showing Online and Offline Devices</td>
<td>12</td>
</tr>
<tr>
<td>Device View Page</td>
<td>13</td>
</tr>
<tr>
<td>Data Logging Window</td>
<td>13</td>
</tr>
<tr>
<td>Periodic Log Type</td>
<td>13</td>
</tr>
<tr>
<td>Change of Value Log Type</td>
<td>13</td>
</tr>
<tr>
<td>Historian Page</td>
<td>14</td>
</tr>
<tr>
<td>Historian Settings Window</td>
<td>14</td>
</tr>
<tr>
<td>Historian Graph</td>
<td>14</td>
</tr>
<tr>
<td>Selected Portion of Historian Graph</td>
<td>15</td>
</tr>
<tr>
<td>Confirmation Window</td>
<td>15</td>
</tr>
<tr>
<td>Device View Screen Showing Send Snapshot Field</td>
<td>16</td>
</tr>
<tr>
<td>Email with Snapshot Attachment</td>
<td>16</td>
</tr>
<tr>
<td>SMC Cloud Login Screen</td>
<td>17</td>
</tr>
<tr>
<td>User Account Dropdown Menu</td>
<td>17</td>
</tr>
<tr>
<td>Edit Profile Menu</td>
<td>18</td>
</tr>
<tr>
<td>Change Password Menu</td>
<td>18</td>
</tr>
<tr>
<td>SMC Cloud Device Management Page</td>
<td>19</td>
</tr>
<tr>
<td>Connecting Remotely to a Device</td>
<td>20</td>
</tr>
<tr>
<td>Device FS-GUI (left) or Customer Application (right)</td>
<td>20</td>
</tr>
<tr>
<td>Notifications Page</td>
<td>21</td>
</tr>
<tr>
<td>Notifications Configuration Menu</td>
<td>21</td>
</tr>
<tr>
<td>System View Listing Device</td>
<td>22</td>
</tr>
<tr>
<td>System View Showing Online and Offline Devices</td>
<td>22</td>
</tr>
<tr>
<td>Device View Screen</td>
<td>23</td>
</tr>
<tr>
<td>Event Settings Window</td>
<td>23</td>
</tr>
<tr>
<td>Event Logger Page</td>
<td>23</td>
</tr>
<tr>
<td>Dashboard Creation Window</td>
<td>24</td>
</tr>
<tr>
<td>Dashboard</td>
<td>25</td>
</tr>
<tr>
<td>Data Source Configuration Window</td>
<td>25</td>
</tr>
<tr>
<td>Time Range Field</td>
<td>26</td>
</tr>
<tr>
<td>Delete Dashboard</td>
<td>27</td>
</tr>
<tr>
<td>Forgot Password Window</td>
<td>28</td>
</tr>
<tr>
<td>Password Reset</td>
<td>28</td>
</tr>
<tr>
<td>DNS Address Not Found</td>
<td>29</td>
</tr>
<tr>
<td>Registration Warning Message</td>
<td>29</td>
</tr>
<tr>
<td>View Site Information</td>
<td>30</td>
</tr>
<tr>
<td>View Details</td>
<td>31</td>
</tr>
<tr>
<td>View Certificate</td>
<td>31</td>
</tr>
<tr>
<td>Certificate</td>
<td>31</td>
</tr>
<tr>
<td>Filter Using Field Search</td>
<td>32</td>
</tr>
<tr>
<td>Filter Using Column Dropdown Menu</td>
<td>32</td>
</tr>
<tr>
<td>Filtering Using User Type Checkbox</td>
<td>32</td>
</tr>
<tr>
<td>Clearing Filters</td>
<td>32</td>
</tr>
<tr>
<td>User Management Page - Export Options</td>
<td>33</td>
</tr>
</tbody>
</table>
1. CONNECTING TO FIELDSERVER (FOR FIELD INSTALLERS)

Find the supplied IP Address for the FieldServer and type the IP Address into the local PC’s browser address bar to move onto registering the FieldServer. (Section PART 2)

**NOTE:** The default IP Address for a ProtoAir or ProtoNode is 192.168.1.24 with a Subnet Mask of 255.255.255.0. If the PC and FieldServer have different Subnets, assign a static IP Address to the PC on the 192.168.1.xxx network.

If the FieldServer IP Address is unknown, follow the directions to discover an existing IP Address in the next section (Section 1.1).

To view or change the FieldServer network settings, follow directions in Section 1.2.

**NOTE:** The SMC Cloud uses TCP ports 80 and 443 by default.

1.1 Discover the IP Address of the FieldServer

- Check that a CAT5 Ethernet cable (straight through or cross-over) is connected between the local PC and FieldServer or the local PC is connected to the same Ethernet Network as the FieldServer.
- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer Toolbox.zip via the Sierra Monitor Resource Center Software Downloads.
- Extract the executable file and complete the installation.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check the FieldServer IP Addresses from the device listings.

![FIGURE 1 - FieldServer Toolbox](image)

- Type the appropriate IP Address into the browser address bar or click the Connect button to move onto registering the FieldServer (Section PART 2).

1.2 Change Network Settings for the FieldServer

- Follow the FieldServer Toolbox setup instructions in Section 1.1 if needed.
- Once the FieldServer Toolbox is open, find the FieldServer that requires network setting review or changes.
- From the Toolbox main page, click on the configure icon .
- Select <Network Settings>.
• Review or modify the necessary network fields.

**NOTE:** If the FieldServer is connected to a router, the IP Gateway of the FieldServer should be set to the IP Address of that router.

The following fields may be review or changed as needed:

- IP Address (N1 IP Address field)
- Netmask (N1 Netmask field)
- DHCP Client State (N1 DHCP Client State field)
- IP Gateway (Default Gateway field)
- DNS 1 & 2 (Domain Name Server fields) - Ensure DNS1 is 8.8.8.8 and DNS2 is 8.8.4.4

**NOTE:** Do not change the DHCP Server State (N1 DHCP Server State field).

• Click “Update IP Settings”, then click on “Change and Restart” to restart the FieldServer and activate the new network settings. Note that if the FieldServer was open in a browser, the browser will need to be pointed to the new IP Address to access the FieldServer.

• Power cycle the FieldServer.

• Record the IP Address assigned to the ProtoNode for future reference.
2. LOGGING IN (FOR FIELD INSTALLERS)

If existing login details were received from the manufacturer's support team, record the information and move on to Section 2.2. Otherwise continue to new user setup.

2.1 New User Setup

When a new user is generated, a “Welcome to SMC Cloud” email will be automatically sent out to set up a login.

Follow the instructions below to set up login details:

• Find the “Welcome to SMC Cloud” email.

![Welcome to SMC Cloud email](image)

**FIGURE 4 - Welcome to SMC Cloud**

**NOTE:** If no SMC Cloud email was received, check the spam/junk folder. Contact the manufacturer's support team if the email cannot be found.

• Click the `<Complete Registration>` button to go to the SMC Cloud webpage and set up user details.
Fill in the name, phone number and password fields.
Click <Save> to save the user details.
Record the email account and password for future use.

2.2 Registration Process
Find the “FieldPoP” icon using one of the cases described below:
- On the FS-GUI screen, click the “FieldPoP” icon on the top right corner of the page.

NOTE: If the gateway opens on the Web Configurator page, the “Diagnostics and Debugging” button in the bottom right corner of the page must be clicked to access FS-GUI.

- For FieldServers with customer application features, BACnet Explorer and the EZ Gateway M Bus to Modbus & BACnet, click the “FieldPoP” tab on the left side of the page
The following informational splash page may appear, click <Close> to move on to register the device.

NOTE: If a warning message appears instead of the splash page, see Appendix A.5.
3. CUSTOMER APPLICATION FEATURES

System View, Historian and Event Logger are part of the optional Application Engine platform, which allows local applications to easily browse and manage FieldServer information or settings. These applications also have the option to supply FieldServer data to the SMC Cloud.

If the customer's FieldServer uses these local applications, login to the FieldServer by entering the IP Address into a browser on the local PC to see the pages described below.

3.1 Using System View to Generate Data Logging

Once the device has appeared on the system view page, click on the device.

**NOTE:** A device will not appear on the system view on first login. The gateway must be configured before devices can be seen in system view. Follow the gateway configuration instructions found in the corresponding gateway start-up guide. If the start-up guide is not on hand, look up the guide online via the Sierra Monitor Resource Center.

![System View Listing Device](image1.png)

**FIGURE 9 - System View Listing Device**

**NOTE:** The System View shows if a device is online or offline by highlighting the device green if online and showing no highlight if offline. See example below.

![System View Showing Online and Offline Devices](image2.png)

**FIGURE 10 - System View Showing Online and Offline Devices**

Clicking on the device will open the device view page, which shows all the data elements that can be gathered from the device, location and status.
Click on the graph icon to the left of the listed data elements to open the Data Logging window.

Select the type of logging for the data point and set the logging interval, COV threshold value or COV max scan time as they apply.

Click <Save> to set the data logging settings and move on to Section 3.2.

**NOTE:** Data is recorded for up to 30 days.
3.2 Using Historian to View Data Logging Information

**NOTE:** The Historian can log up to 8,000 values per data point.
- Click the Historian tab on the left side of the page.
- Click on the Settings button to set up data to graph.
- Click the checkbox next to the data element to graph. Any combination of elements can be selected.

**NOTE:** A data element is only visible when it is set for data logging as shown in Section 3.1.
- Click <Submit> to generate a graph for each element selected.

After a few seconds, the graph should appear.
To view individual values of data, scroll across the graph to show a text box that states each exact point and the location of that point on the graph via a blue dot.

To view a graph of only select dates/time frames, move the cursor towards the miniature version of the graph that is shown just below the full size graph. Hover the cursor over the miniature graph so that the cursor becomes a crosshair (+).

Click and hold near the beginning or ending time frame desired, then drag the crosshair towards the ending or beginning time frame; all within the confines of the miniature graph.

The full size version of the graph will populate accordingly.

Any additional edits to the time frame can be adjusted by clicking and dragging the wedge markers on either side of the highlighted portion of the miniature graph.

To delete a log and its resulting graph, go to Settings and check the boxes next to the properties to remove. Click the delete button; once the confirmation window appears, click <Yes> to confirm.
3.3 Using Device View to Send a Snapshot of the Device Data

To get a snapshot of the summarized device data, follow the instructions below.

- Ensure that the FieldServer is registered to the SMC Cloud (Section 2.2)
- Connect to the FieldServer via browser.
- Enter the Device View page via System View.
- Scroll to the bottom of the page to find the “Send Snapshot” field; enter an email address and click <Send> to receive the data summary from the device.

An email with the snapshot as an attached .txt file will appear in the previously referenced inbox.
4. LOGGING INTO AND USING THE SMC CLOUD (FOR SUPPORT)

After the FieldServer is registered, go to www.SMCCloud.io and type in the appropriate login information as per registration credentials.

For new users, the instructions for login and password setup are shown in Section 2.1. If the login password is lost, see Appendix A.2 for recovery instructions.

**NOTE:** Sections 4.2 - 4.4 represent each of the tabs that appear at the top of the page once logged into SMC Cloud and describe their functions.

4.1 Account Management

Account management can be done on any screen by simply clicking on the user icon in the top right corner of the page.
Once the icon has been clicked, the dropdown menu with options to Edit Profile, Change Password, Notifications and Logout will appear.

See the subsections that follow for Account Management features and instructions.

4.1.1 Editing the Profile

- Click <Edit Profile> in the dropdown menu.
- Enter or alter the profile details as needed.

4.1.2 Changing the Password

To change the password, fill in the password information as needed.

**NOTE:** Hover over the password strength to see comments related to the entered password.

4.1.3 Enabling/Disabling Notification Audio Alerts

Notification audio alerts can be turned on or off by clicking “Notifications” in the dropdown menu. When audio alerts are enabled, the local computer will make a 'ping' sound. This is the sound that will occur when any notification type takes place in real-time.

The status of notification audio alerts can be viewed in the dropdown menu by looking at the speaker icon to the right of the “Notifications” text.

Audio alerts Enabled: 🔊 Audio alerts Disabled: 🔊
4.2 Device Management

Gives an overview of devices registered to SMC Cloud. This page includes the following features:

4.2.1 Map Elements

The map shows the location of all the devices registered on SMC Cloud using Google Maps pins.

![SMC Cloud Device Management Page](image)

Each pin is color-coded to show the device status:

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grey</td>
<td>Offline</td>
</tr>
<tr>
<td>Green</td>
<td>Normal</td>
</tr>
<tr>
<td>Yellow</td>
<td>Warning</td>
</tr>
<tr>
<td>Red</td>
<td>Alarm</td>
</tr>
<tr>
<td>Blue</td>
<td>Trouble</td>
</tr>
</tbody>
</table>

**NOTE:** See Appendix B.3 for details on map navigation.
4.2.2 Connecting to a Device

- Click on a pin on the map to bring up registered device details. This shows pertinent device information.

- Click on “Connect” to remotely access a device via HTTPS.

FIGURE 27 - Connecting Remotely to a Device

FIGURE 28 - Device FS-GUI (left) or Customer Application (right)
4.3 Notifications
This page shows the notifications for all devices.

The following fields are displayed and can be used as filters to find a specific notification:

- Notification Type
- Notification Message
- Device Name
- MAC Address
- Company
- Date

**NOTE:** If certain fields are not present, they may be hidden. To make them viewable follow the Data Table Dropdown Menu instructions in Appendix B.2.

### 4.3.1 Configure a Notification Delivery

Notifications can be configured to be sent via email and/or SMS.

Click the Configuration icon on the bottom right side of the page.

Click the corresponding checkbox to have notifications sent as email or SMS.

Browse and select the device(s) for notification.

Click «Configure» to save settings.
4.3.2 Using System View Events to Generate Notifications

System View and Event Logger are part of the optional Application Engine platform, which allows local applications to easily browse and manage FieldServer information or settings. In the near future, these applications will also have the option to supply FieldServer data to SMC Cloud.

If the customer's FieldServer uses these local applications, login to the FieldServer by entering the IP Address into a browser on the local PC to see the pages described below.

- Once the device has appeared on the system view page, click on the device.

![FIGURE 31 - System View Listing Device](image1)

NOTE: The System View shows whether a device is online or offline by highlighting the device a color based on its status if online and showing no highlight if offline. See example below.

![FIGURE 32 - System View Showing Online and Offline Devices](image2)

Clicking on the device will open the device view page, which shows all the data elements that can be gathered from the device, location and status.
Click on the bell icon ( ) next to an element to attach an event and open the Event Settings window.

**NOTE:** Event Settings allow the FieldServer to go into Trouble, Warning or Alarm status based on the settings entered. These events appear on the FieldServer Event Logger page and populate onto the SMC Cloud Notifications page if the FieldServer is registered.

- Select the desired event type to open up additional parameters to customize when events occur.

The following parameters are available for configuration:

- **Set Point** - point at which an event will trigger
- **Falling Value** - click the checkbox if the event should trigger if values fall below the set point; leave unchecked if event should trigger above the set point
- **Deadband** - the difference above or below the set point before the event is cleared.

Click Save to set the Event Settings.

Events can be viewed on the device by clicking on the Event Logger tab to open the Event Logger Page.

In SMC Cloud, this information can be viewed on the Notifications Page if the device is registered. Additionally, device status information will populate on the Device Management page via color coded icons (Section 4.2.1).
4.4 Dashboards

Data visualization by means of graphs and gauges is available in a variety of predefined dashboard templates. To create a dashboard:

- Click the **New Dashboard** button on the bottom right corner of the screen.
- Add a Dashboard Name and choose the Dashboard Type from the template options shown.

![Add Dashboard Template](image)

**FIGURE 36 - Dashboard Creation Window**

- Click Create and a message will appear declaring that the new Dashboard was successfully created.
- Click the OK button.

**4.4.1 Rename a Dashboard**

Click the edit icon on the right side of the desired dashboard entry to rename.

The Dashboard name is now editable; rename and click **Save**.
4.4.2 Set Up Dashboard

Click **View dashboard** on the desired dashboard entry to open the dashboard proper.

Click on the wrench icon next to either gauges or graphs for data configuration.

Select the data for visualization via gauge or graph by clicking the gray checkbox to the left of the desired value.

Gateway Names, Device or Value can be filtered by entering desired search information in the search box above the listed data sources

For gauges, only one data source can be selected

For graphs, multiple data sources can be selected

Once selected data points appear at the bottom of the Data source configuration window, modify the Title (name of gauge or graph), Label (name for the specific data point) or Max Range (gauge only) as desired.
Click <Change> once configuration is complete to generate the gauge or graph.

**NOTE:** For gauges, to change what color a range of values represents, click the left pointing arrow icon to the right of the gauge. Click the range to modify and then choose the new color.

**NOTE:** For graphs, values can be hidden by click the data point item where the label is written out next to a square of its representative color.

**4.4.3 Change the Dashboard Time Range**

To change the time range of the presented data (x-axis for graphs and average calculation for gauges), select from the four representation types under the time_select parameter near the top of the page.

Select a type of time range representation by clicking any of the four circles under the dropdown menu or clicking on the white arrows pointing left or right on the left and right edges of the screen.

There are four ways to visualize the selected data in terms of time range. These include:

- **Quick** - Offers straightforward time selections such as 'this week', 'previous month', 'last 12 hours', etc.
- **Relative** - Allows representation of data from the current time to a chosen number of minutes, weeks, months, etc. in the past. Click the Go button to update graphs and gauges.
Absolute - An explicit range of year, month, day, hour, minute, second, and fraction of a second is selectable (YYYY-MM-DD HH:mm:ss:SSS). Click the Go button to update graphs and gauges.

Time Animation - This selection allows viewing of graphical data as it occurred in consecutive aggregates of minute, hour, day, month, etc. Select the total time frame using one of the previously described representation methods and change the 'round to the nearest' dropdown menu for the desired time frame jumps. Use the transport buttons - ▶ play, ▪ pause, and ▾ ◀ skip forward/backward - to move the time frame manually.

4.4.4 Delete a Dashboard

Click the trash icon -trash on the right side of the desired dashboard entry to delete.

A message will appear to confirm; click <Delete Dashboard>.

Another message will appear stating that the dashboard was deleted successfully; click the OK button.
APPENDIX A - Troubleshooting

A.1 Device Management Map

A.1.1 Device Pin Turns Gray Unexpectedly
If a device pin turns gray on the Device Management Page:
• Check FieldServer is connected to the internet.
• Ensure power LED is lit on the FieldServer.

A.1.2 Scroll Wheel Doesn't Change Map Magnification
If the mouse scroll wheel is used and the Device Management Map shows the message “Use ctrl + scroll to zoom the map”, hold down the Ctrl key while using the wheel to zoom in or out of the map.

A.2 Lost SMC Cloud Login Password
If the password is lost, follow the below instructions:
• Click “Forgot Password” on the SMC Cloud Login Screen.
  
  ![Forgot Password Window](FIGURE 41 - Forgot Password Window)
  
  • Once the Password Reset Window appears, enter the email address of the SMC Cloud account and click Submit.
  • Click on the “Reset Your Password” button in the email sent from notification@SMCCloud.io to reset the SMC Cloud password.

  ![Password Reset](FIGURE 42 - Password Reset)
  
  • Enter and confirm the new password then click Save.
A.3 SMC Cloud Cannot Remotely Connect to a Device

Check if the screen below appears when trying to remotely connect to a device. If so, try clearing the DNS cache (in the cmd window type “ipconfig /flushdns”) or validate the local computer's DNS against the network DNS settings. Contact technical support if the problem persists.

A.4 General Connection Notes

It is important to check that the FieldServer's network settings are set up with the following Domain Name Server (DNS) settings for proper communication:

- DNS1 = 8.8.8.8
- DNS2 = 8.8.4.4

Any time changes to the network settings are done, remember to click "Update IP Settings" and then power cycle or soft reboot the FieldServer to save the new settings.

The SMC Cloud uses TCP ports 80 and 443 by default.

A.5 SMC Cloud Connection Problems

If there is a problem with connecting to the SMC Cloud a warning will appear.

Follow the directions presented in the warning message and check that the DNS settings meet the requirements mentioned in Appendix A.4.
APPENDIX B - Useful Features

B.1 Security

SMC Cloud to FieldServer and FieldServer to browser connections are secured with HTTPS, which uses TLS/SSL (Transport Layer Security/Secure Sockets Layer). The HTTPS certificate is issued by SSL.com. Details are viewable via any local PC browser by following the instructions found in Appendix B.1.3.

NOTE: SMC Cloud keeps information private between individual OEMs and individual enterprise users. There is no bleed between different OEMs and different enterprise users.

B.1.1 PC to SMC Cloud

To browse SMC Cloud via PC, type the following domain into the PC's internet browser: www.SMC-Cloud.io (port 80 and 443).

B.1.2 FieldServer to SMC Cloud

To allow the FieldServer to connect to SMC Cloud, use the following domain: www.SMCCloud.io (port 80 and 443).

To connect to a ProtoNode via SMC Cloud, a device tunnel is created that has a unique subdomain in the URL. The best way to configure a firewall rule with this in mind is to use a wildcard domain: *.tunnel.SMCCloud.io (port 443).

Additional security can be added by allowing the FieldServer to exclusively access the *.SMC-Cloud.io. This provision can be set up in the customer's firewall.

B.1.3 Viewing the Certificate

Open a web browser on the local PC and go to https://www.SMCCloud.io.

Move the cursor to the padlock icon next to the website address.

Right-click the padlock icon to open a dropdown menu for website information and browser settings. Click the Details link to open the security overview information panel.
Review the information and click the <View certificate> button.

Examine the certificate as needed.

To download the certificate, click the Details tab and click the 'Copy to File' button.
B.2 Data Table Features

The following features are available on any Data Table Page.

B.2.1 Additional Filter Options

Column Field Search - Specific details can be typed into the text box at the top of each column to locate users.

![Figure 49 - Filter Using Field Search]

Column Dropdown Menu - The downward pointing arrow to the right of each field name can be selected to sort in ascending, descending or hide the selected column. To bring a hidden column back into the table, use the Data Table Dropdown Menu.

![Figure 50 - Filter Using Column Dropdown Menu]

User Type Checkbox - Additionally, the Registered Users listing and Audit Logs listing can be filtered using the user type checkboxes across the top of the page by unchecking to exclude the user types in question and checking to include those same users.

![Figure 51 - Filtering Using User Type Checkbox]

Data Table Dropdown Menu - Click on the gray menu icon on the top right corner of the desired data table. This will open a dropdown list that includes the option to clear all filters and lists the columns available for this specific data set. Columns clicked will be hidden or added to the table depending on whether they are present in the table or not.

![Figure 52 - Clearing Filters]
B.2.2 Exporting Data

Click on the blue <Export Options> button on the bottom right corner of the Data Table.

Choose one of the export file options below:

- Export all data as CSV
- Export visible data as CSV
- Export all data as PDF
- Export visible data as PDF

**NOTE:** If any columns have been made invisible via the additional filter options shown in Appendix B.2.1 then the export options that reference “visible data” will not include those columns.

The data file will automatically download to the local computer's default “Downloads" folder.

B.3 Device Management Map Controls

B.3.1 Mouse

For the mouse control descriptions below, “left” and “right” refer to the left and right mouse buttons.

- Left click and hold - This allows dragging to orient the map as desired.
- Double left click - Zoom in one interval.
- Double right click - Zoom out one interval.
- Scroll wheel - Roll forward to zoom in and roll back to zoom out.

**NOTE:** If the scroll wheel stops changing the map magnification, see Appendix A.1.2.
B.3.2 Additional Controls

The following icons are located in the bottom right corner of the Device Management Map:

- Google Street View - Enable street level navigation from Google Maps
- Zoom In - Based on current center of screen
- Zoom Out - Based on current center of screen
- Full Screen - Open map in full screen view
- Exit Full Screen - Exit the map full screen view

B.4 Session Time Out

If SMC Cloud is left open without any input a pop up a reminder will occur 10 min after last input and state that log out will occur in 5 minutes.

SMC Cloud will automatically show the following window if no input is received after 15 minutes:

To log back on, click OK to be sent back to the SMC Cloud Login screen and log in as normal.
B.5 User Roles - Type and Hierarchy

The SMC Cloud user hierarchy consists of OEM and Enterprise Customer accounts, with OEM accounts hierarchically above Enterprise Customer accounts. Each account type is further subdivided into Admin, Manager (OEM accounts only) and User categories.

**Admin** can:
- Register or deregister devices
- Create Admin or User accounts on the same or lower level of hierarchy
- Change the role of existing users between Admin and User
- View all devices accessible to the Admin's organization
- Assign a device to a User on the same level of hierarchy, granting access to view the device

**User** can:
- Register devices
- View and edit device(s) that are assigned to the User's account by an Admin of the same company

**Enterprise Customer Admin** can:
- Update the firmware of a device via SMC Cloud
- View and edit device(s) that are registered to the Enterprise Customer Admin's organization
- Not view, create or modify OEM Users

**OEM Manager** can:
- Create Enterprise Customer Admin or OEM User accounts
- Modify Enterprise Customer Admin or OEM User accounts within an organization that has been previously assigned to the OEM Manager
- Add a new company to the SMC Cloud system by creating a new Enterprise Customer Admin
- Assign a device to an Enterprise Customer Admin (in an organization assigned to or created by the OEM Manager), making the device visible to that company's Enterprise Customer Admins
- Assign a device to a OEM User, granting the user access to view the device
- View and edit device(s) that are registered to the organizations assigned to the OEM Manager, or devices created by or assigned to the OEM Manager
- Not view or modify users, devices or organizations that aren't part of the organizations assigned to the OEM Manager, or devices created by or assigned to the OEM Manager

On the SMC Cloud website, devices are associated with the company and hierarchy level of the account that registered it. This includes which roles will be able to view the device.

- If an OEM User registers a device, the device is also immediately assigned to that user.
- If an Enterprise Customer User registers a device, that user will automatically be assigned that device. The registering Enterprise Customer User and all Enterprise Customer Admins within the same organization will be able to view the device.
APPENDIX C - WARRANTY

Cleaver-Brooks warrants this product to be free from defects in workmanship or material under normal use and service for two years after date of shipment. C-B will repair or replace any equipment found to be defective during the warranty period. Final determination of the nature and responsibility for defective or damaged equipment will be made by C-B personnel.

All warranties hereunder are contingent upon proper use in the application for which the product was intended and do not cover products which have been modified or repaired without C-B approval or which have been subjected to accident, improper maintenance, installation or application, or on which original identification marks have been removed or altered. This Limited Warranty also will not apply to interconnecting cables or wires, consumables or to any damage resulting from battery leakage.

In all cases C-B's responsibility and liability under this warranty shall be limited to the cost of the equipment. The purchaser must obtain shipping instructions for the prepaid return of any item under this warranty provision and compliance with such instruction shall be a condition of this warranty.

Except for the express warranty stated above, C-B disclaims all warranties with regard to the products sold hereunder including all implied warranties of merchantability and fitness and the express warranties stated herein are in lieu of all obligations or liabilities on the part of C-B for damages including, but not limited to, consequential damages arising out of/or in connection with the use or performance of the product.