



EGUANA



Evolve ESST™ / Evolve 0513U

Fleet Installer Web Application

Account and Device Administration Guide

IMPORTANT INSTRUCTIONS

This manual contains important product information for your Evolve home energy storage system. This document is accurate at the time of publishing. Eguana reserves the right to make updates to the product without notice. For the latest Evolve documents, please visit our website at www.eguanatech.com

WARNING! Read this document in its entirety before using this product. Failure to follow instructions or warnings can result in electrical shock, serious injury, or death. Operating the product in a way that it was not intended can also result in permanent damage to the product.

This manual applies to the following products:

- Evolve 0513 ESS & Evolve Hub EMS-A
- Evolve 0513U & E-Gear ATS/EMC Panel

Table of Contents

1 INTRODUCTION - FLEET INSTALLER WEB APPLICATION SOFTWARE	1
1.1 DASHBOARD REVIEW	1
2 ACCOUNT ADMINISTRATION	2
2.1 : THE ON-BOARDING PROCESS: REGISTERING YOUR COMPANY AS AN AUTHORIZED INSTALLER.....	2
2.2 ADMINISTRATOR TASKS	2
2.2.1 Add employee.....	2
2.2.2 Create signing key.....	3
2.2.3 Issue certificate.....	3
2.2.4 Add organization information.....	3
2.3 EMPLOYEE TASKS – SYSTEM INSTALLERS ONLY	4
2.3.1 Request certificate	4
2.3.2 Download certificate	4
2.3.3 Install certificate - Google Chrome	5
3 DEVICE MANAGEMENT	6
3.1 ADD NEW DEVICE.....	6
3.2 DEVICE INFORMATION.....	7
3.2.1 Transferring system ownership	7
3.3 DEVICE CONFIGURATION – MANAGE CONSUMER FEATURES.....	8
3.3.1 Granting sytem owner control permissions: power reserve & emergency power reserve.....	8
3.4 DEVICE STATUS – PERFORMANCE DATA	9
3.4.1 Downloading device data	9
4 CUSTOMER ADMINISTRATION	10
4.1 SEND WELCOME EMAIL TO THE CUSTOMER	10

Glossary

EMC	Energy Management Controller
PKI	Public Key Infrastructure
UID	Unique Identifier Device
Device	Energy Storage System

1 Introduction - Fleet Installer Web Application Software

This document is intended for authorized installation companies of Eguana Evolve home energy storage systems. The guide covers user account and device administration of an installation company's fleet of energy storage systems.

Note: The Fleet Installer application also permits remote commissioning and diagnostics. These topics are covered in a separate guide, see - *Fleet Installer Web Application: Remote Commissioning and Diagnostics*.

The Fleet Installer application runs on a web browser platform. Google Chrome, Firefox and Safari are supported. Microsoft IE and Edge are not supported. Login at:

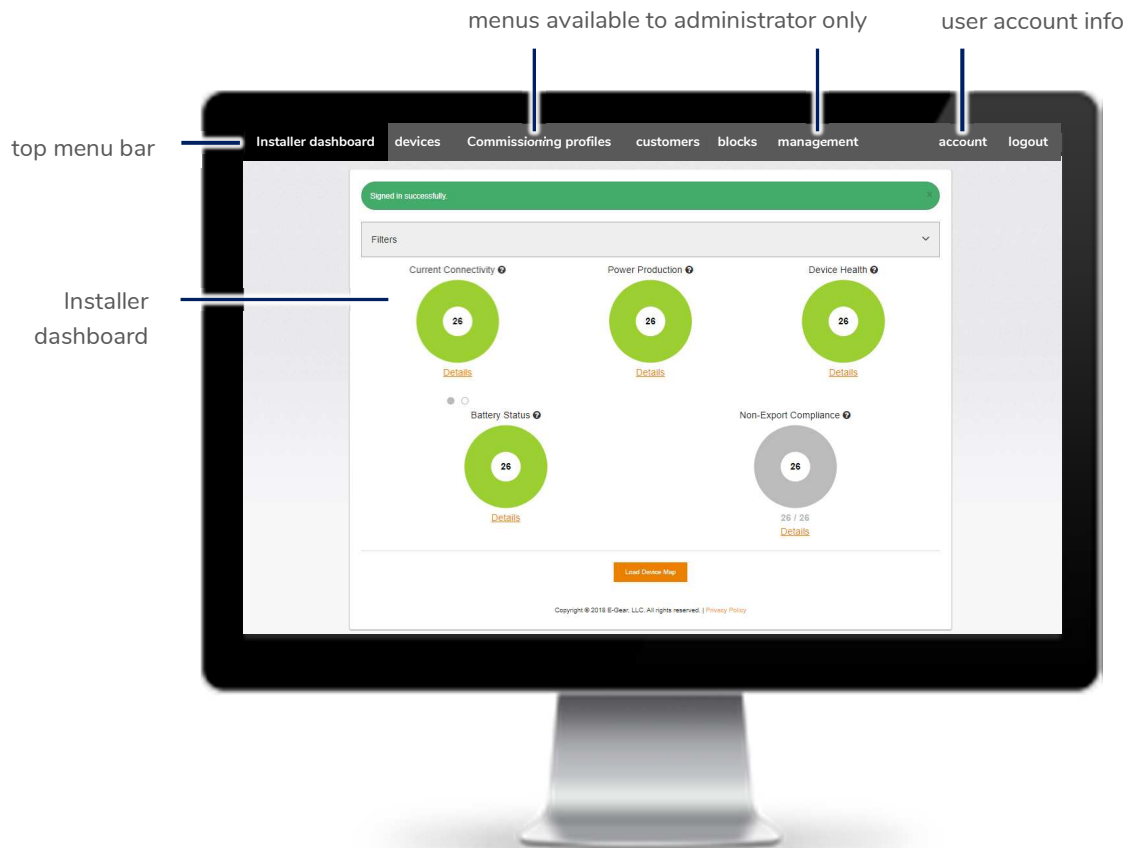
https://www.mypowermyway.com/fleet_installer

Enter your login credentials as assigned in your invitation email. A password change is recommended after the first login.

1.1 Dashboard review

Each category in the dashboard provides a high level view of the health of all systems monitored under the company account. Systems that are flagged in any category can be reviewed by selecting [\[Details\]](#).

Note: Data is polled from the systems in approximately 5 minute intervals.



2 Account Administration

Commissioning the Evolve energy storage system is achieved via a USB connection from a laptop to the energy management controller (EMC) within the Evolve Hub. The EMC incorporates public key infrastructure (PKI) as a security measure to prevent unauthorized access to the system configuration settings. To manage the security of the company's fleet of installed systems, the Fleet Installer administrator can:

- Add / delete employees with access to the fleet installer dashboard.
- Issue / revoke certificates to employees that are deployed to commission systems.

2.1 : The on-boarding process: registering your company as an authorized installer

IMPORTANT! The company must be registered with Eguana to be assigned an authorized installer account with the Fleet Installer web application. Contact a regional office nearest you at www.eguanatech.com to request an administrator account. Once approved, you will be assigned an account with an invitation email from "My Power. My Way."

Note: An Eguana service tech will initially have administrative access to a new company account. This provision is in place to provide remote support during the training phase. This can be disabled by the company administrator at any time.

2.2 Administrator permissions and tasks

IMPORTANT! Ensure all permission levels are checked before completing admin tasks within this section.

Installer dashboard devices Commissioning profiles customers blocks management **account** logout

Permissions

- User can add and edit customers and devices
- Can send welcome email to customers
- User can edit other users from this organization

Save

2.2.1 Add employee

Installer dashboard devices Commissioning profiles customers blocks **management** account logout

1. From the top menu bar, select: **management > employees**
2. Click [\[Add new employee\]](#)
3. Enter personal (company) contact details, including: email address, phone number, and first/last name
4. Scroll down to **Permissions**, and assign the relevant permissions
The installers should have permission to the following:
 - User can add and edit customer devices.
 - Can send welcome email to customers.Note: Editing other users should be restricted to the administrator only.
5. Press [\[Create\]](#) to complete. This will trigger an automatic email invitation from My Power. My Way.

2.2.2 Create signing key

The signing key provides the administrator with the authority to issue certificates to employees that will commission systems.



1. From the top menu bar (right), select your **user account**
2. Scroll down to **Signing Keys**, and click on **[Create Signing Key]**
3. Complete the password fields in the pop-up menu. The employee login password is your login password. The signing key password is created here. You can use the same password as the employee login password.
4. Press **[Save]** to complete.

A white pop-up window titled 'New signing key' with a close button (X) in the top right corner. It contains three text input fields: 'Employee Login Password', 'Signing Key Password', and 'Signing Key Password Confirmation'. Below the fields is an orange 'Save' button.

2.2.3 Issue certificate

Note: The prerequisite for this task is based on a certificate request from the employee(s) that will commission systems - see section 4 - Employee tasks.



1. From the top menu bar, select: **management > certificates**
2. Scroll down to the employee in the employee list that has requested a certificate, and select **[Issue]** or **[Reject]** in the right-most column.
3. If issued, enter the signing key password that was created in section 3.2 to issue the certificate, and select **[Issue]**

A white pop-up window titled 'Issue user certificate' with a close button (X) in the top right corner. It contains a dropdown menu for 'Issuing Certificate Authority' with 'Eguana Technologies' selected. Below it is a text input field for 'Signing Key Password'. At the bottom is an orange 'Issue' button.

2.2.4 Add organization information

This section is used to establish email issued service alarms from the company's fleet of systems.

1. From the top menu bar, select: **management > organization**
2. Enter the company web address and main service contact info.
3. Assign employees that will receive system service alarms by email.
4. Upload a company logo. This logo will appear in the system owner's dashboard support widget.

2.3 Employee tasks – system installers only

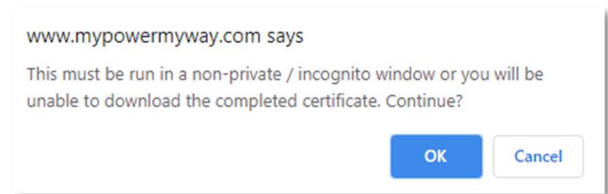
In order to connect to an EMC, a valid certificate must be installed on the employee's laptop. The following instructions only apply to employees responsible for on site system commissioning.

IMPORTANT! The certificate is web browser specific. Use the same web browser for the certificate request /download /install, and connections to the EMC. Google Chrome is the preferred browser for all computer operating systems; including Windows, MAC, and Linux.



2.3.1 Request certificate

1. From the top menu bar, select your **user account**
2. Scroll down to **Certificates**, and click on [\[Request a Certificate\]](#)
3. A pop-up window warns the user to ensure that a public browser window is open for the certificate request. Press [OK].
4. Notify your administrator that the certificate has been requested.



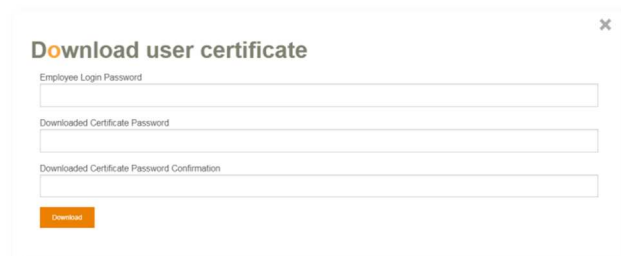
2.3.2 Download certificate

Your administrator will notify you that the certificate has been approved.

1. From the top menu bar, select your **user account**
2. Scroll down to **Certificates**, and click on [\[Download\]](#)

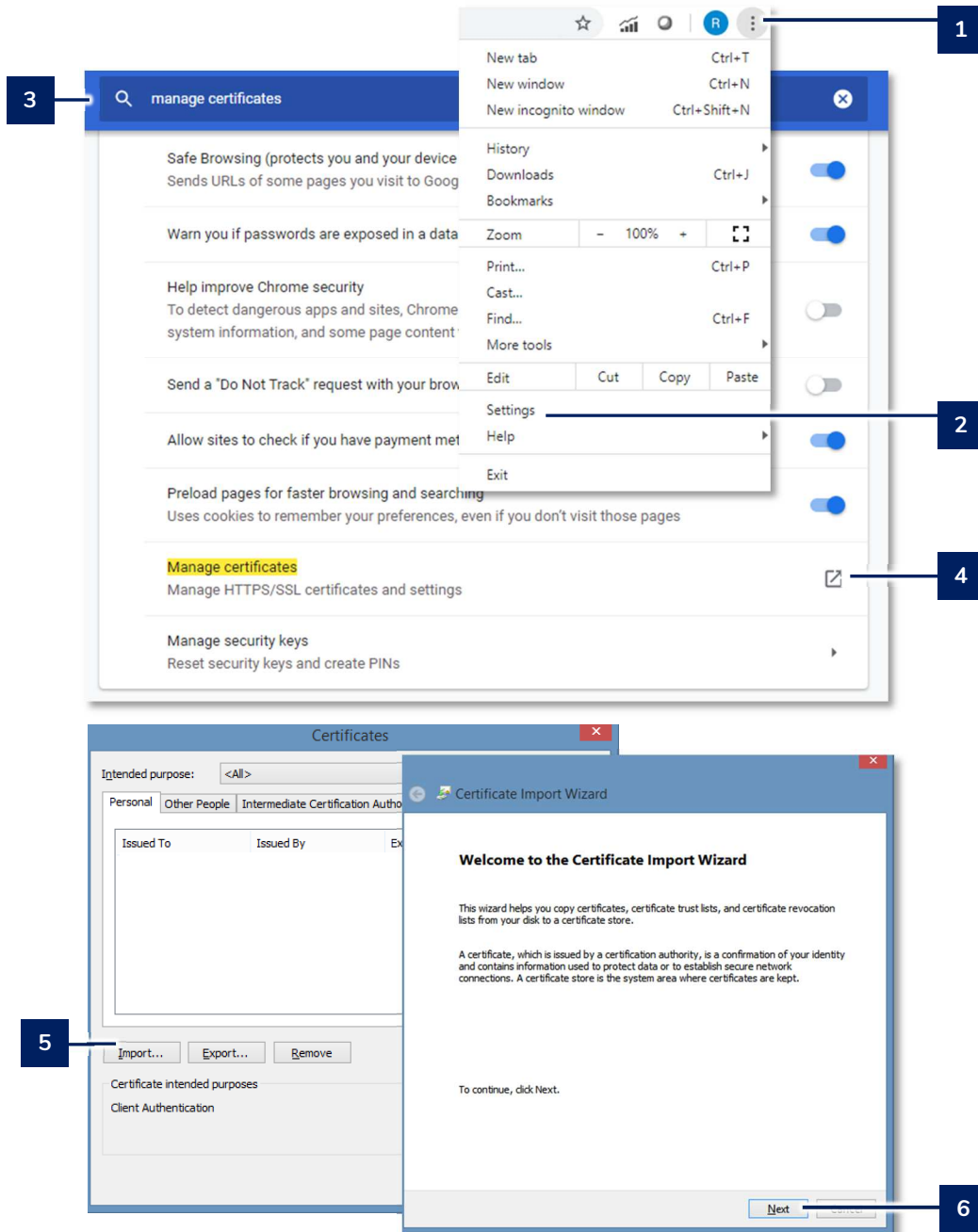
A pop-up menu appears:

3. Enter the employee login password. This is the password used to log in to your account.
4. Create a "downloaded certificate password". You can use the same password as the employee login password.
5. Select [\[Download\]](#)
6. Save the certificate to your desktop, or retrieve from your downloads folder. The certificate is a personal type (*.P12).



2.3.3 Install certificate - Google Chrome

1. Select the customize chrome button at top-right of the window.
2. Click **settings**.
3. In the search bar, type “**manage certificates**”
4. Click [more] at the bottom of the search list (if applicable), and scroll down to select **manage certificates**
5. Select [Import]
6. The Certificate Import Wizard pop-up menu appears. Select [Next] and follow the instructions in the Wizard to complete the certificate installation.



3 Device Management

3.1 Add new device

1

Devices

Add New Device **2**

Filters

UID ▲	Ownership start date	Current Firmware Version	Current Owner	Address	On-Site Service Requested	Connection	Last Known Status	Cell Status	Current Connection Status	Last Reported At
00080003-00000000-0300044F-#####	2020-05-13	1.0.0	John Doe	123 Main Street, New York, NY 10001		WiFi	Green	Red	Green	May 13, 2020 10:18am EDT
00080003-00000000-0300044F-#####	2020-05-13	1.0.0	John Doe	123 Main Street, New York, NY 10001		WiFi	Green	Red	Green	May 13, 2020 10:18am EDT

New device **3** Complete form.

Customer Information

System owner's email used to trigger invitation to their monitoring system.

Email **?** First name Last name

Address line 1

Device Information

Enter info from the label attached to the EMC card.

UID **?** Serial number **?**

Estimated Generation (kWh/yr) **?** Total Inverter AC Capacity (kW) **?** Solar inverter parameters.

PV Inverter Manufacturer Battery Inverter Type Number of Battery Modules **?** Total number of battery modules in the battery cabinets.

Cell Is Primary Connection

Device Management

Customer Ownership Start Date

Monitored

Applicable to states with special utility interactive requirements.

Device Location

Country State

Geographic Region Utility PV system Interconnected to

Utility Grid Compliance Profile **?** Utility Tariff **?** TOU Tariff **?** Utility specific data base where TOU rates apply.

Address Line 1

4

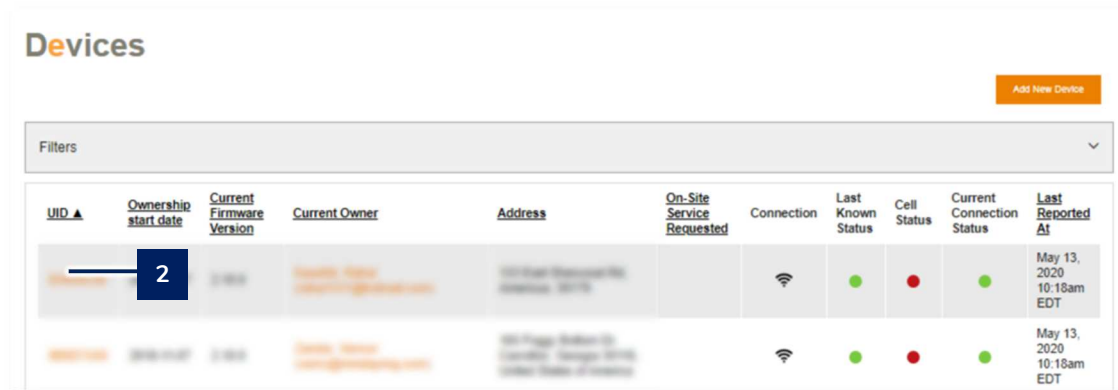
3.2 Device information

This menu is a summary of the information entered in section 3.1.

3.2.1 Transferring system ownership

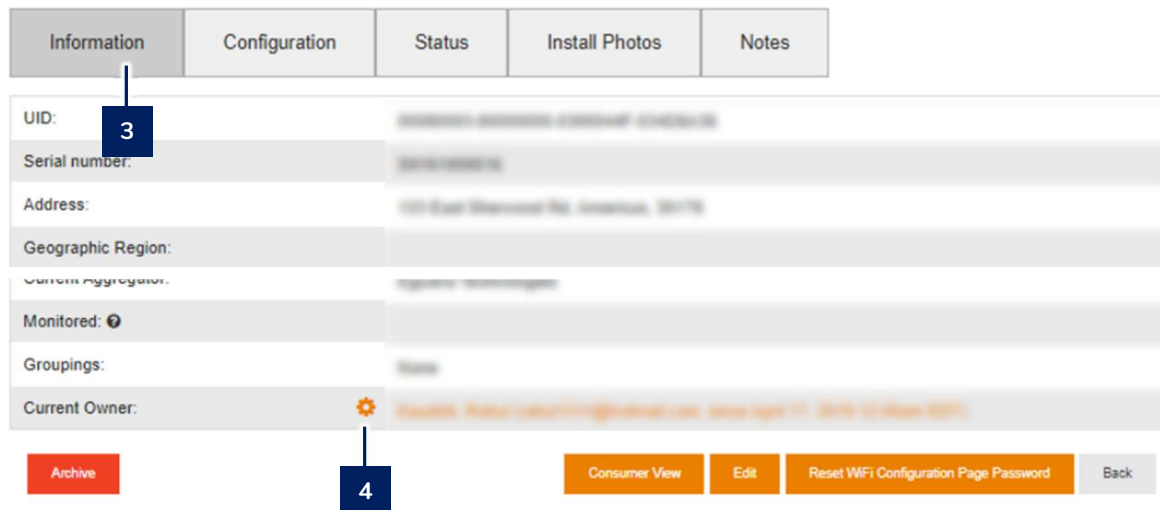
The **Current Owner** field contains the information that assigns a consumer monitoring interface to the system owner. When the system is transferred to a new owner, the **Current Owner** field must be updated.

1. From the top menu bar, select: **devices**
2. In the **UID** column, click on the **UID number** of the device for which the ownership will be transferred.
3. Select the **Information** sub-menu.
4. Click the gear icon and enter the new owner's email and contact information in the pop-up window, to secure the transfer.




UID ▲	Ownership start date	Current Firmware Version	Current Owner	Address	On-Site Service Requested	Connection	Last Known Status	Cell Status	Current Connection Status	Last Reported At
00000000000000000000000000000000	2020-05-13	1.0.0	John Doe (john.doe@example.com)	101 East Broadway St, Newark, NJ 07102		Wi-Fi	●	●	●	May 13, 2020 10:18am EDT
00000000000000000000000000000000	2020-05-13	1.0.0	John Doe (john.doe@example.com)	101 East Broadway St, Newark, NJ 07102		Wi-Fi	●	●	●	May 13, 2020 10:18am EDT

Device



Information	Configuration	Status	Install Photos	Notes
UID:	00000000000000000000000000000000			
Serial number:	0000000000			
Address:	101 East Broadway St, Newark, NJ 07102			
Geographic Region:				
Current Aggregator:	T-Mobile			
Monitored:	●			
Groupings:	None			
Current Owner:	John Doe (john.doe@example.com) since April 11, 2020 10:18am EDT			

Archive  Consumer View Edit Reset WiFi Configuration Page Password Back

3.3 Device configuration – manage consumer features

IMPORTANT! This menu provides access to features which can remotely alter the configuration settings of the energy management controller. Only the features relevant to administrators are covered in this section. Proceed with care.

3.3.1 Granting system owner control permissions: power reserve & emergency power reserve

While the energy storage system is entirely automated, the system can be provisioned to allow manual adjustment of the battery reserve capacity by the system owner. This permission is administered by a fleet installer account holder. There are two levels of permissions:

- Power reserve:

By default, the battery is maximized for daily use as part of an energy savings algorithm; either solar self consumption or time of use plans, where applicable. Approximately 25% is reserved for battery backup. This appears as a slider in the battery widget in the consumer interface, which can be adjusted to increase or decrease backup reserve capacity. This feature requires a manual adjustment for each time a change is required.

- Emergency power reserve:

This feature allows the system owner to maintain a full battery for a defined period, in anticipation of a probable grid outage. This could be driven by an extreme weather event, for example. The duration of this mode is selectable by the owner.

1. From the top menu bar, select: **devices**
2. Select the **Configuration > Configurations** sub-menus.
3. Select **[Manage Consumer Features]**
4. Check the reserve features for which permission will be granted.
5. Click **[Save]**

Enabled consumer features ✕

Battery Block

- Power Reserve
- Emergency Power Reserve

Save

Last updated at July 11, 2019 9:31am MDT by McNemie, Randy. [more...](#)

3.4 Device status – Performance Data

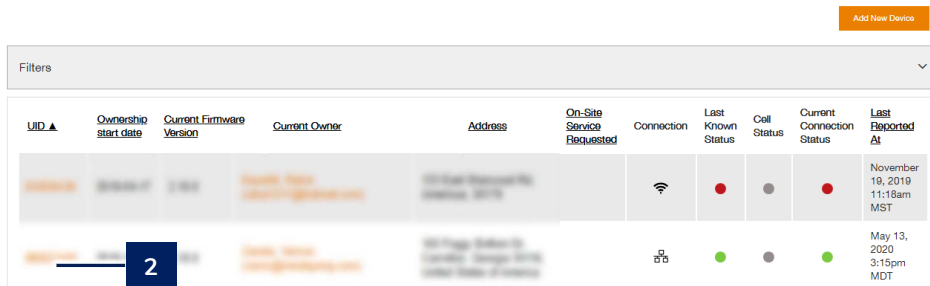
Each energy storage system collects system data in 15 second intervals. This data includes unique identifier information, energy production from the battery / solar / grid sources, and performance and fault data from the battery modules and the PCS. This data may be requested for the following uses:

- Battery module warranty claims
- Incentive programs that require proof of performance – ie) SGIP applications

3.4.1 Downloading device data

1. From the top menu bar, select: **devices**
2. In the **UID** column, click on the **UID number** of the device for which the data will be downloaded.
3. Select the **Status > Production > Downloads** sub-menus.
4. Open the **New Download** sub-menu.
5. Select **Raw EMC data** from the **report type** drop-down list.
6. Enter a file name and select the start time and stop time from the lookup calendar that follows.
7. Click **[Create]** to begin download. Depending on the file size, the download may take up to 30 minutes to complete. It will be saved in .CSV format which can be opened in any spreadsheet application.

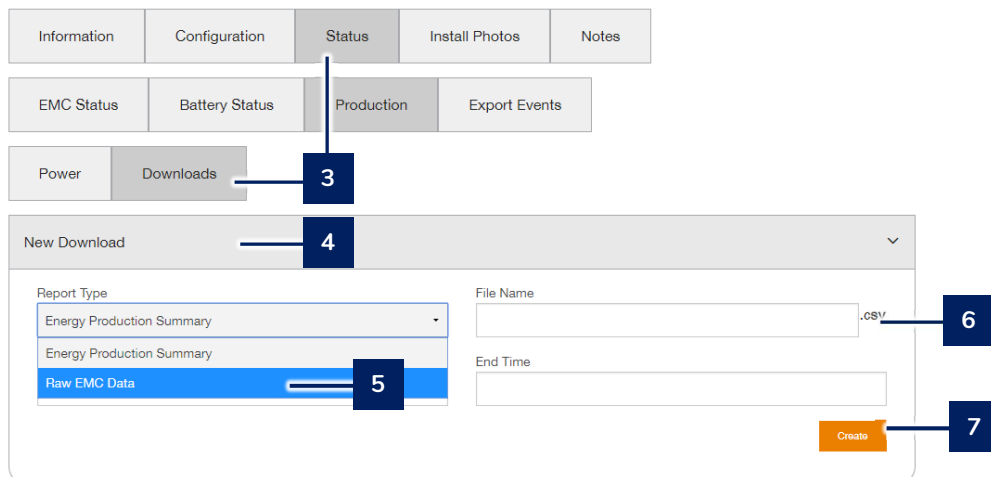
Devices



Filters ▼ Add New Device

UID ▲	Ownership start date	Current Firmware Version	Current Owner	Address	On-Site Service Requested	Connection	Last Known Status	Cell Status	Current Connection Status	Last Reported At
123456789	2019-01-01	1.0.0	ABC Energy Solutions	1234 Main St, Anytown, NY 12345		📶	●	●	●	November 19, 2019 11:18am MST
987654321	2020-05-13	1.0.0	ABC Energy Solutions	1234 Main St, Anytown, NY 12345		📶	●	●	●	May 13, 2020 3:15pm MDT

Device



Information | Configuration | **Status** | Install Photos | Notes

EMC Status | Battery Status | **Production** | Export Events

Power | Downloads **3**

New Download **4**

Report Type: Energy Production Summary | Energy Production Summary | **Raw EMC Data** **5**

File Name: .CSV **6**

End Time:

Create **7**

4 Customer Administration

A customer is defined as the system owner, or person which will receive access to the monitoring system at the consumer level only. This is defined as the *Consumer Interface*, which is entirely separate from the Fleet Installer application. As per section 3.1, the customer's contact information is recorded as part of adding a new device to the fleet installer. Once completed, the customer's info is recorded under the customers tab in the top menu bar.

4.1 Send welcome email to the customer

1. From the top menu bar, select: **customers**
2. In the customer column, click on the **customer name**.
3. Scroll down to the **Welcome email last sent at** field and click on the email icon in the adjacent column.
4. Click **[Send]** in the pop up menu that follows.

The customer will receive an automated email with an account login from My Power. My Way.