Tutorial 4:
Using eGuard Manager

Article ESA-1004T
February 25, 2014

Contents

4.1 eGuard Manager .......................................................... 2
4.1.1 What is eGuard Manager? ........................................... 2
4.1.2 Who is eGuard for? ................................................... 5
4.1.3 Access-rights Management within eGuard ....................... 5
4.2 Creating an eGauge.net account and requesting access .......... 8
4.3 eGuard Device View ...................................................... 9
4.4 eGuard Device Alerts .................................................... 12
4.5 Administrating eGuard Access ........................................ 14
4.1 eGuard Manager

4.1.1 What is eGuard Manager?

eGuard is an administrative management system for eGauge devices that allows an individual to monitor and manage multiple eGauge systems from a single web interface.

The eGuard interface allows you to see the current status and statistics for all devices you have rights to. With proper authorization, you can also use eGuard to enable remote administration and create device notes for future reference.

Alerts may be sent to the user in situations such as device connectivity loss, low production, high usage, and incorrect time setting.

Groups can be divided into subgroups, creating a hierarchical access-rights system in which a company or group may divide device responsibilities in a practical manner.

Figure 4.1: A collection of managed devices within eGuard
Device Table Menu

→ **Display Group** (If applicable) - Change eGuard device group displayed in the table.

→ **View Map** - Display a map of all devices in the displayed group. The eGauge map will only display devices that have a valid Latitude and Longitude set in Settings → General Settings on the eGauge, and will ask to zoom to your current location. The eGauge map features are described in the following section.

→ **Max rows to display** - Determines the maximum number of devices that display in the table. This value defaults to 50 if there are greater than 50 devices in the selected group. If there are less than 50 devices, the only option is *All*.

→ **Search** - An instantaneous search that filters devices based on the string entered. Searching is case insensitive, and will search Job/Site, Rev, Name and device label (the original device name which is printed on the eGauge unit – visible by hovering over Name, if applicable) for an exact match.

→ The **Device info** and **Power stats** check boxes allow you to show or hide specified columns.
Cross and eGauge Map

If an eGauge has a valid location value set in Settings → General Settings, a cross icon will appear next to the device notes icon. Clicking this cross will open the eGauge map for this group, zoomed to the chosen device. Note that this option may not update for up to an hour when changed on a device.

Clicking the eGauge icon will display device details. Listed here are the device name and status (represented by a green or red circle), device Label, Group, Job, and any Installer Notes that have been saved for the device.

An image of the location, if available, will appear to the right of this information. Clicking on this picture will bring you to the Street View for this location, if available, otherwise, you will be zoomed in as far as possible.

Figure 4.4: Device on map, showing details.
4.1.2 Who is eGuard for?

eGuard is a complimentary tool for those who need to manage multiple (5 or more) devices and require quick and direct access to current status and information. eGauge highly recommends that any new organization ordering multiple eGauges contact support@egauge.net to set-up an eGuard account before shipping time.

Use eGuard to identify problems early and as a customer relationship management (CRM) tool or in conjunction with other CRM software. *eGuard is intended as a tool for installers and device administrators and will not be used by an end-user that may have only one to a few devices installed at a single location.*

4.1.3 Access-rights Management within eGuard

The access-rights system within eGuard is designed to enable delegation both within a single company and across companies. Within a single company, there may be multiple administrators with equal rights. eGuard reflects this as administrators managing the same group. If a company has subsidiaries or franchisees, it may be desirable to delegate administration of certain devices to particular subsidiaries/franchisees. eGuard reflects this by assigning the device to a subgroup of the main group and then have the subsidiaries be administrators of those subgroups. In this fashion, subsidiaries have full control over their own devices, while still giving full rights to the administrators of the parent company.

Another type of delegation occurs when an entity owns a set of devices but wants to grant another entity the right to manage all or some of the devices. In eGuard, this can be accomplished by assigning the devices to a subgroup and then granting the second entity to right to manage that group. The manager will be able to manage the devices within the subgroup he or she manages (e.g., turn on/off remote administration) but will not be authorized to affect the rights of the first entity (administrators).

**Groups**

eGuard manages access-rights based primarily on the group that a device belongs to. Group-names are hierarchical and consist of a sequence of group-name-components which are separated by colons (:). Components may consist of any characters other than colons (:) or commas (,). The left-most component is the top-level component, right-most the bottom component. For example, given group name fruit:apple:fuji, fruit would be the parent of apple, and apple would be the parent of fuji. If a user had certain rights for group fruit those rights automatically apply to all subgroups as well. However, if another user had rights only to group fruit:pear, then those rights would not apply to fruit:apple or any of its subgroups.

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>Access to</th>
</tr>
</thead>
<tbody>
<tr>
<td>sunville</td>
<td>John Hoover</td>
<td>ACE:sunville</td>
</tr>
<tr>
<td>svilleCO</td>
<td></td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td>starpower</td>
<td>Scott Rapport</td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>jstan</td>
<td>Jacob S</td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>earthflow</td>
<td></td>
<td>ACE:earthflow</td>
</tr>
<tr>
<td>mark2253</td>
<td>Mark</td>
<td>ACE:acme_solar</td>
</tr>
</tbody>
</table>

Figure 4.5: User sunville is an administrator of group sunville, a subgroup of ACE. svilleCO is a manager of sv_colorado, a subgroup of sunville which is a subgroup of ACE.
Administrators

Administrators are users who have special rights in administrating the devices belonging to a particular company. A user can be the administrator of at most one group and its subgroups (in addition to being a manager of other groups). In addition to the manager rights listed below, administrators have the following additional rights:

- Upon request, may grant other users the right to manage or administer their group or a subgroup thereof.
- May revoke the right of other users to manage or administer a (sub-)group. All administrators for a given group are treated equally, so administrator A may revoke the right from administrator B of the same group and vice versa. However, an administrator of a subgroup cannot affect the rights of an administrator managing a super-group of that subgroup.
- May view/edit the installation notes associated with a device (if any).
- May edit the site/job-name associated with a device (if any).
- May view the contact information for the user that registered as the owner of the device (if any).

Managers

Managers have access to all the devices in the group(s) that they manage. They have the right to perform the following operations:

- View the device data collected by eGuard including average power produced/consumed, firmware version, network speed, internal device temperature and availability status of the device.
- Enable/disable remote administration on a device.
- Reassign a device to another group, provided the device stays within a parent-group which the manager is managing. For example, a manager of fruit:apple could move a device to group fruit:apple:fuji (because fruit:apple is a shared parent), but not to fruit:pear (because even though fruit is a common parent, the manager doesn’t have access to that parent).
- Create a subgroup for any of the managed groups.
- Delete a subgroup, provided no devices are assigned to that subgroup.
- May view the site/job-name associated with a device (if any).
Administrator vs. Manager – how to choose?

As a rule-of-thumb, if you’re a reseller that retains control of your eGauge devices, and you have a customer that buys more than one or two devices from you, you’ll probably want to create a new sub-group for that customer. Make that customer the administrator of that sub-group. When you sell a device to that customer, use eGuard to assign the devices just sold to the customer’s sub-group so the customer will have full control over his/her devices. You will still have access to the device, but should of course respect the customer’s ownership in agreement with your sales contract. Note that the customer can then create his or her own subgroups and sub-divide administration of the devices even further.

If a customer buys a device through some channel and then hires a third party to install the device, it is often useful to allow the installer to manage the device(s) that were installed for the customer. This way, the installer has an easy way to track the health of the device(s) that s/he installed and it also allows the installer to make adjustments to device’s settings if needed. This can be accomplished in eGuard as follows: the customer creates a subgroup for the installer and then allows the installer to manage that subgroup (without marking the installer as an administrator).

---

**Table:**

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>Access to</th>
</tr>
</thead>
<tbody>
<tr>
<td>sunville</td>
<td>John Hoover</td>
<td>ACE:sunville</td>
</tr>
<tr>
<td>svilleCO</td>
<td></td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td>starpower</td>
<td>Scott Rapport</td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>jstan</td>
<td>Jacob S</td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>earthflow</td>
<td></td>
<td>ACE:earthflow</td>
</tr>
<tr>
<td>mark2253</td>
<td>Mark</td>
<td>ACE:acme_solar</td>
</tr>
</tbody>
</table>

**Figure 4.6:** User sunville is an administrator of ACE:sunville and can change everything related to ACE:sunville, including access rights for this group. User svilleCO is a manager of ACE:sunville:sv_colorado and has more limited privileges within ACE:sunville:sv_colorado
4.2 Creating an eGauge.net account and requesting access

1. Visit http://www.egauge.net and click Log In at the top of the page.

2. Click Register here and enter appropriate information and submit your information. Be sure to check your email and click the verification link to activate your account.

3. Click on the user dropdown menu, choose Account Settings. Click Update contact information and enter relevant information. Next, open the Manage Access page from under the eGuard manager.
4. Under **Request Access to Other User’s Devices**, enter the user name of the owner of the devices you wish to have access to, informing them you have requested access on eGuard.

The request will be seen by the owner of the devices when they enter the Manage Access screen on their account, described further in section **4.5, Administering eGuard Access**.

If no administrator exists for the devices and you would like to create an account, send an email to support@egauge.net with the request, along with proof-of-ownership or verifiable permission from the devices’ owner.

### 4.3 eGuard Device View

Choosing **View Devices** from your eGuard Manager will bring up a table of all devices you have access-rights to. In the image below identify (left to right) the notepad icon, cross icon, Group, Job/Site, Name, S (status), Avail (availability; uptime), Tmp (temperature), TX (transmission rate), Rev (firmware revision), Sum (include in summation option), and statistics for the device. This information is updated once every hour.

![Device management page](image-url)

**Figure 4.7: Device management page**

**Device Notes**

![Device notes button](image-url)

**Figure 4.8: Device notes button**
The notepad icon in the left-most column will allow you to access the specified device page. The device page contains the following information:

- Registration info (Administrators only, if the device was registered).
- Enable or disable remote administration (Administrators and Managers).
- Copy the configuration from a device to this device (Administrators only).
- Download most recent firmware for EG30xx offline firmware updates (Administrators only).
- Privileged info, such as MAC address and Device-ID (Administrators only).
- Job/Site name (Administrators can modify and Managers can view).
- Installer Notes (Administrators only).

**Figure 4.9:** Example device page. Notice how the installer notes have relevant information about the particular eGauge system installation.
The *Group* column lists what group the device is currently assigned to.  

*Job/Site* will display the job name that is set from the device’s page via the yellow notepad icon.  

The *S* column contains either a red or green circle, denoting whether the device is currently communicating with the eGauge.net proxy server.  

*Avail* lists the percentage of time the device has been up over the past week. Hover your mouse over the percentage for an up vector as well as the date and time the device was last seen by the proxy server.

![Figure 4.10: Upvector- offline for 5 hours](image)

The up vector is read from left to right. 1 represents that the device was on line, communicating to the proxy server during the last hourly check. 0 represents that the device was not communicating with the proxy server during the last check.  

Note in the image, the device appeared to not have communicated with the proxy server for 5 hours. This does NOT indicate any data loss: the eGauge will continue to monitor and record even when it does not have Internet connectivity as long as the unit is receiving power.

![Figure 4.11: Upvector- unstable connection](image)

In the event the up vector is erratic, such as in the image above, the connectivity of the system should be verified: Internet connectivity, home plug signal (Refer to the Status page for current HomePlug speed), and other networking concerns such as older hardware and multiple HomePlug adapters. If the device is always accessible via LAN access, and has a bad uptime record from the proxy, the issue is likely caused by a router or network control device. For more information, view the FAQ entries from the eGauge.net support page.

*Tmp* is the internal temperature of the eGauge.  

*TX* is the transmission rate between the eGauge and home plug adapter in Mbps (Megabits/sec). 10+ Mbps is desirable, and below 2 Mbps can be an indication of communication problems between the eGauge and HomePlug adapter. In this case, the HomePlug adapter should be relocated closer to the eGauge, and steps taken to minimize signal loss between the two devices.  

*Rev* is the firmware revision the device is using. Note that if this value is red you should contact support@egauge.net regarding whether this particular revision has an issue that should be remedied by upgrading the firmware.  

*Sum* adds the device to the Cumulative Average Power calculation at the bottom of the devices table.  

The right half of the row describes the average usage and generation over several time intervals.
Summation

The Sum column checkbox can be marked for any device you wish to summate in the bottom row, labeled Cumulative Average Power. The checkbox in the cumulative row can be checked to select between all or none of the devices listed. Summation will only work for devices currently seen in the list.

![Table of Cumulative Average Power](image)

**Figure 4.12:** The Cumulative Average Power row adds statistics from any row that has the Sum column checked

### 4.4 eGuard Device Alerts

The eGuard Alerts Manager page lets you pick what type of alerts you are signed up for. You can select different alert conditions for different groups of devices, or have all of your managed devices treated in the same way. eGuard updates its data once an hour and checks alerts once a day (around midnight). Normally, you'll receive at most one mail a day and once reported, the same alert will not be reported again until the alert-condition has been resolved. At the bottom of this page, you can also view a list of currently pending alerts.

**Alert Rules**

<table>
<thead>
<tr>
<th>For:</th>
<th>Raise Alert When:</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Cross] My_Device_Group1</td>
<td>Energy used in last 24 hours is more than 1000 kWh.</td>
</tr>
<tr>
<td>![Cross] My_Device_Group1</td>
<td>Energy generated in last 24 hours is less than 3 kWh.</td>
</tr>
<tr>
<td>![Cross] All of my devices.</td>
<td>Unable to contact device for over 24 hours.</td>
</tr>
</tbody>
</table>

**Figure 4.13:** Alert Rules will show you the current active rules for the chosen groups you have access to.
Figure 4.14: Add/Update rule will allow you to select a type of alert-condition and for which devices it should be set for. See the eGuard Alerts Manager page to see the available rules.

Figure 4.15: Pending Alerts let you see any device alerts that have not been resolved.
4.5 Administrating eGuard Access

**Summary of Your Access-rights**

- You are logged in as Ace-Monitoring.
- You are an administrator for ACE.
- You are a manager of many groups.

![Figure 4.16: Summary of your current credentials](image)

**Group Management**

- Create new group: [Input field] as a subgroup of [Dropdown: earthflow] [Create]
- Delete group: [Dropdown: acme_solar, earthflow, starpowersolar, sunville, sunville_sv_colorado] [Delete]

![Figure 4.17: Group Management allows you to create or delete subgroups.](image)

Access-rights management allows you to view and manage who has access to your devices. Administrative access will show as red, and manager access will show as green.

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>Access to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>sunville</td>
<td>John Hoover</td>
<td>ACE:sunville</td>
</tr>
<tr>
<td>svilleCO</td>
<td>Scott Rapport</td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td>starpower</td>
<td>Scott Rapport</td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>jstan</td>
<td>Jacob S</td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td>earthflow</td>
<td>Mark</td>
<td>ACE:earthflow</td>
</tr>
<tr>
<td>mark2253</td>
<td>Mark</td>
<td>ACE:acme_solar</td>
</tr>
</tbody>
</table>

![Figure 4.18: Example of authorized users](image)

For this example, the user that is logged in is Ace-Monitoring and is the administrator for the group ACE. As such, the accounts sunville, svilleCO, starpower, jstan, earthflow, and mark2253 were all created and requested access to ACE devices, as shown in 4.2, and approved and assigned to the appropriate group by Ace-Monitoring.

sunville is a subgroup of ACE, which has a login of its own. There is a subgroup of sunville called sv_colorado, which the users svilleCO and jstan manage. Ace-Monitoring is the only account that has administrative access to acme_solar and starpowersolar.
Clicking the login name will give a link to the user’s email address, and clicking the group after the login name will give a pop up box allowing you to choose what groups that user has access to.

For example, if you were to click on ACE:acme_solar to the right of mark2253, you would see a pop up box like below:

![Example of user-group management](image1)

**Figure 4.19:** Example of user-group management

If you were to give Mark administrative access to ACE:acme_solar, and provide him with manager access to ACE:earthflow, you would check off the Admin checkbox, and choose ACE:earthflow from the drop down menu, as shown in the images below:

![Example: Clicking the drop-down menu will give you a list of groups you have permission to assign others to.](image2)

**Figure 4.20:** Example: Clicking the drop-down menu will give you a list of groups you have permission to assign others to.

![The populated group list shows current permissions and access-rights. You may erase entries by clicking the to the left of the group name.](image3)

**Figure 4.21:** The populated group list shows current permissions and access-rights. You may erase entries by clicking the to the left of the group name.

<table>
<thead>
<tr>
<th>Login</th>
<th>Name</th>
<th>Access to</th>
</tr>
</thead>
<tbody>
<tr>
<td>sunville</td>
<td>John Hoover</td>
<td>ACE:sunville</td>
</tr>
<tr>
<td>svilleCO</td>
<td></td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td>starpower</td>
<td>Scott Rapport</td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>jstan</td>
<td>Jacob S</td>
<td>ACE:sunville:sv_colorado</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE:starpowersolar</td>
</tr>
<tr>
<td>earthflow</td>
<td></td>
<td>ACE:earthflow</td>
</tr>
<tr>
<td>mark2253</td>
<td>Mark</td>
<td>ACE:acme_solar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE:earthflow</td>
</tr>
</tbody>
</table>

**Figure 4.22:** The new permissions in the updated table.
To assign or change a device to a specific group, click on the group name or empty cell and choose the appropriate group from the drop-down menu. To remove a device from a group, choose the empty blank value.

![Selecting the blank spot will remove the device from the group](image)

**Figure 4.23:** Selecting the blank spot will remove the device from the group