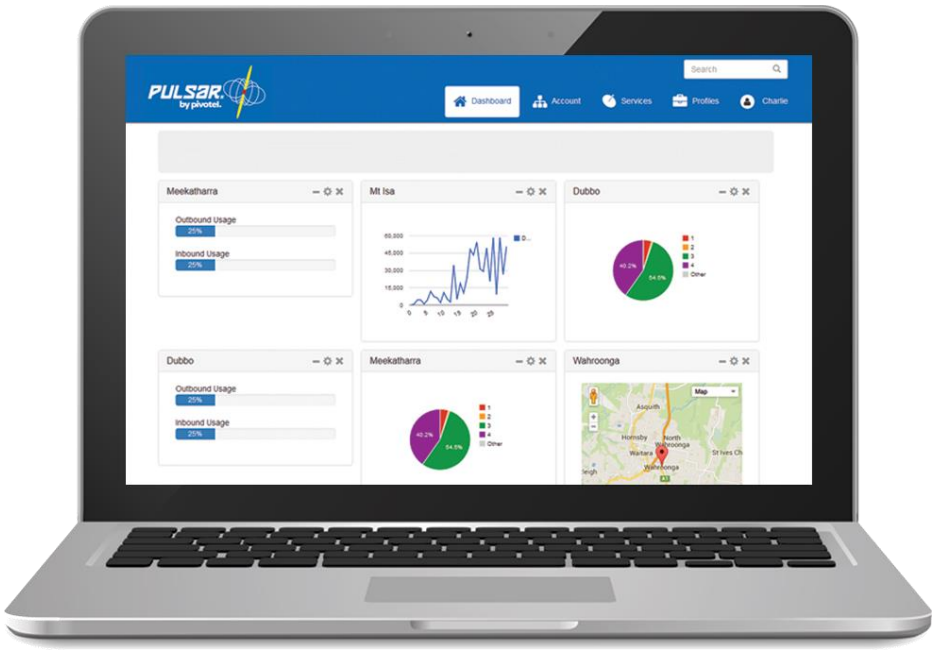
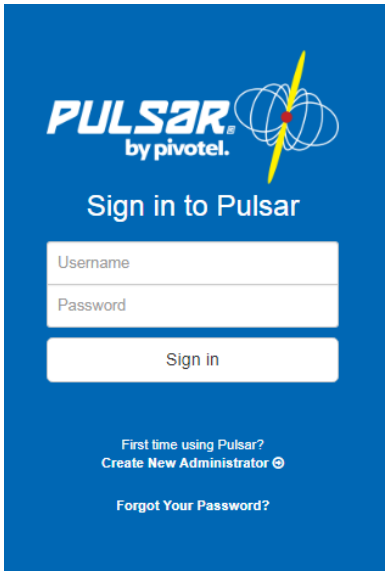
Pulsar User Guide



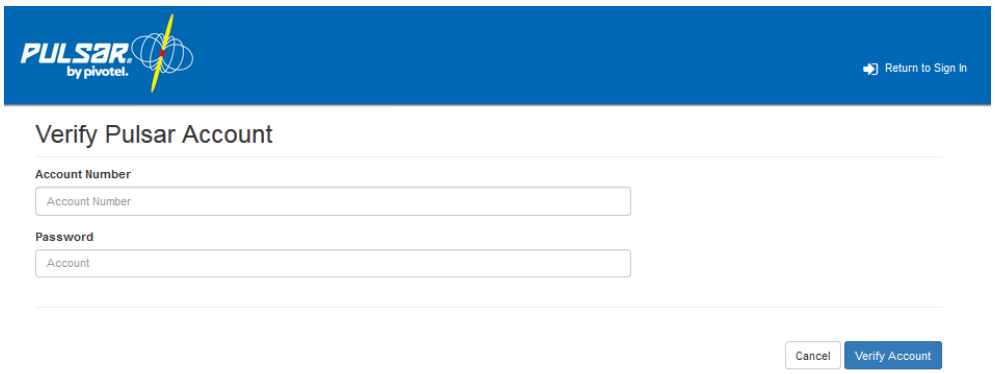
Step 1: Create Your Administrator Login

1.1 Open your browser and navigate to **https://www.pulsarportal.com**

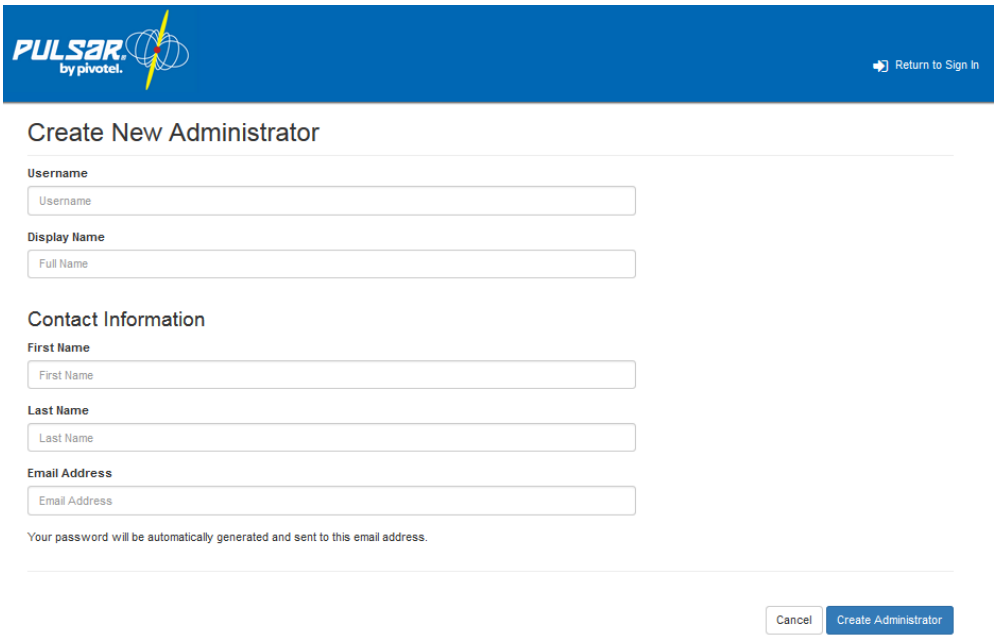


1.2 Under 'First time using Pulsar?' click '**Create New Administrator**'.

1.3 Enter your Pivotel Account Number and Password and click 'Verify Account'. If you do not know your Pivotel Account Number and Password, please contact Pivotel Customer Care.

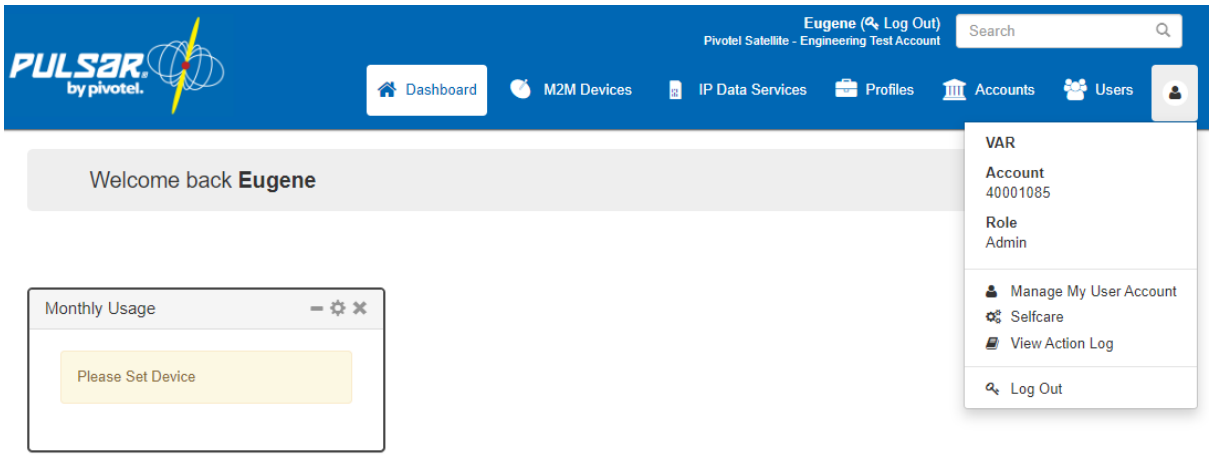


1.4 Choose and enter a Username, Display Name and your Contact Information in the fields provided. Your Username is used to login to PULSAR, and your Display Name will be displayed in the PULSAR PORTAL. Click '**Create Administrator**' and a password will be emailed to your Contact Email Address.

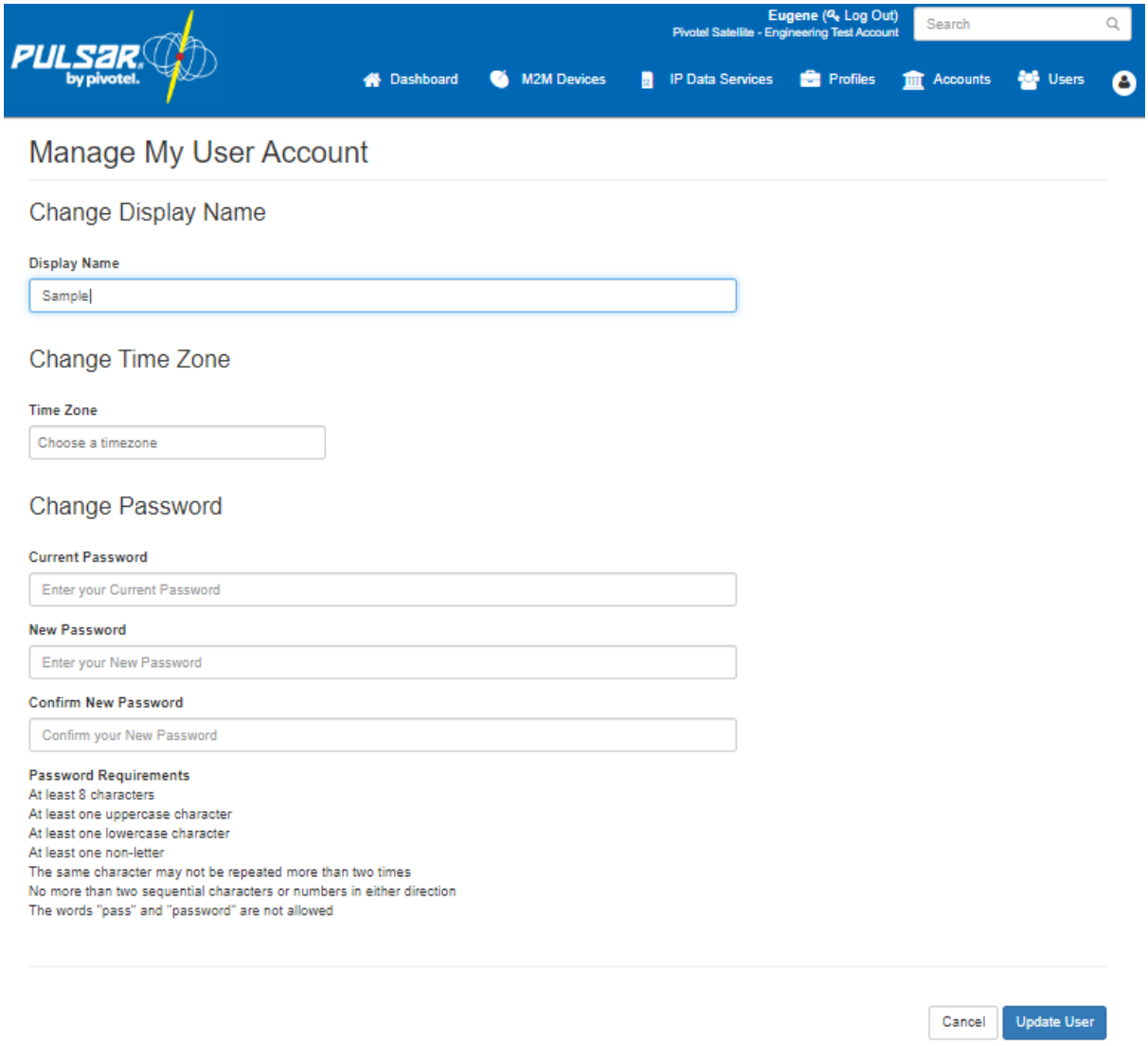


1.5 Click 'Return to Sign In' at the top right of your screen and enter the Username and Password sent to your Contact Email Address.

1.6 After login, you can change this password by clicking  and then selecting '**Manage My User Account**'.



1.7 Under '**Change Password**', enter the Password sent to your Contact Email Address in the 'Current Password', enter your new Password in 'New Password' and repeat your new Password in 'Confirm New Password'. Click '**Update User**' to save the changes.



1.8 Once the new Password is saved, you will return to the login page to login using the Username and new Password.

Step 2: Create Your Profile

Every PULSAR data service is automatically assigned to the PULSAR default profile when activated. Pulsar sends alert emails to the Email Address registered on your Pivotel account when your data usage for each individual or shared plan reaches 50%, 85%, 100% of a pre-set data alert limit and automatically bars data usage when it reaches a pre-set data bar limit. The PULSAR default profile cannot be edited or deleted.

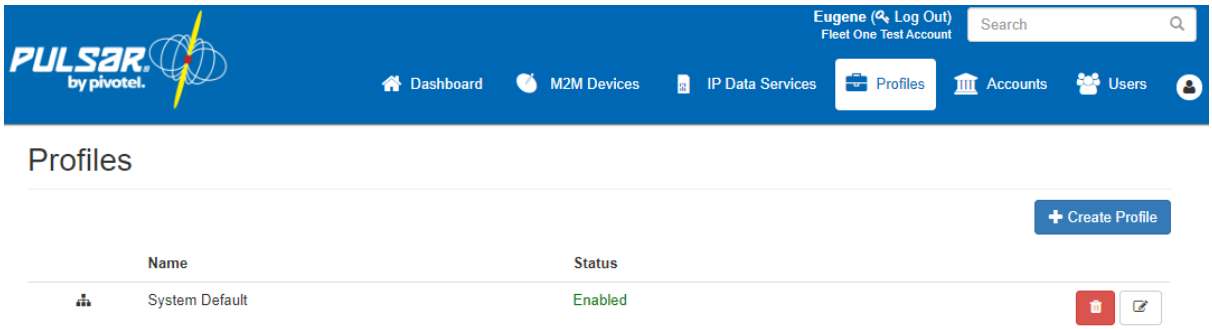
For plans with a data inclusion, for example Inmarsat BGAN M2M 10MB, the PULSAR default profile will send email notifications at 50% (5MB), 85% (8.5MB), 100% (10MB) of the data inclusion and bar usage at 150% of the data inclusion (15MB).

For plans with no data inclusion, for example IsatHub Casual plan, the PULSAR default profile will send email notifications at 50%, 85%, 100% of a set limit (50MB) and bar usage at a set limit (50MB).

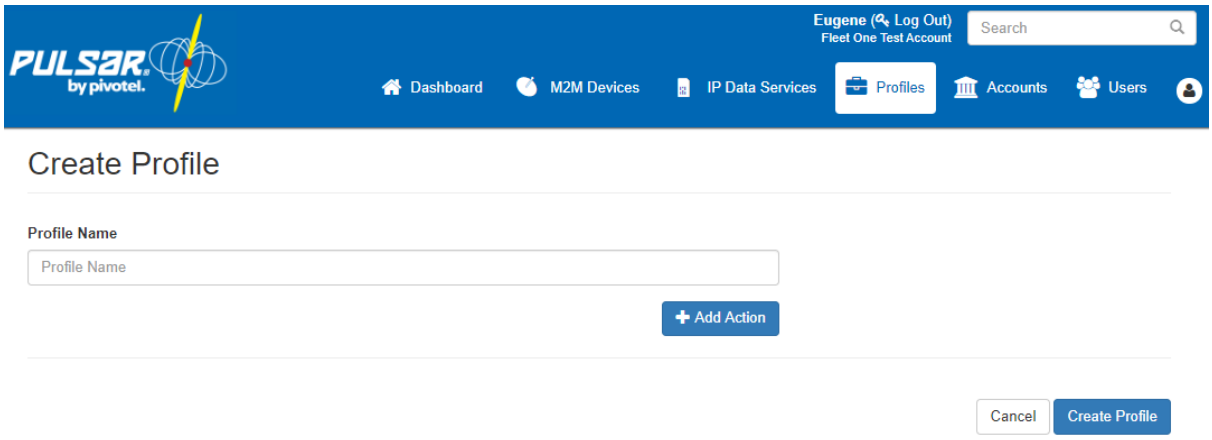
You can set different data alerts and bar limits, remove a data bar and/or change the email addresses to receive PULSAR notifications. **First you need to create a new PULSAR profile (Step 2) and assign devices to your profile (Step 3) for the profile to take effect. Each service can only be assigned to one profile.**

Every time you update a profile, the profile actions will refresh and impact every device associated with that profile. The actual data usage of the service will not reset with a new updated profile. If you need to update an alert or bar the service at a certain MB used, you need to update the profile level to be the current usage plus the new MB data usage for the alert or bar. For example, if your current data usage for your service is 80MB and you would like to get an alert at the next 50MB used, you need to update the profile to alert you at 130MB.

2.1 Once logged in, select 'Profiles'. Click '**+ Create Profile**'.



2.2 Enter a Profile Name. Click '**+ Add Action**'.

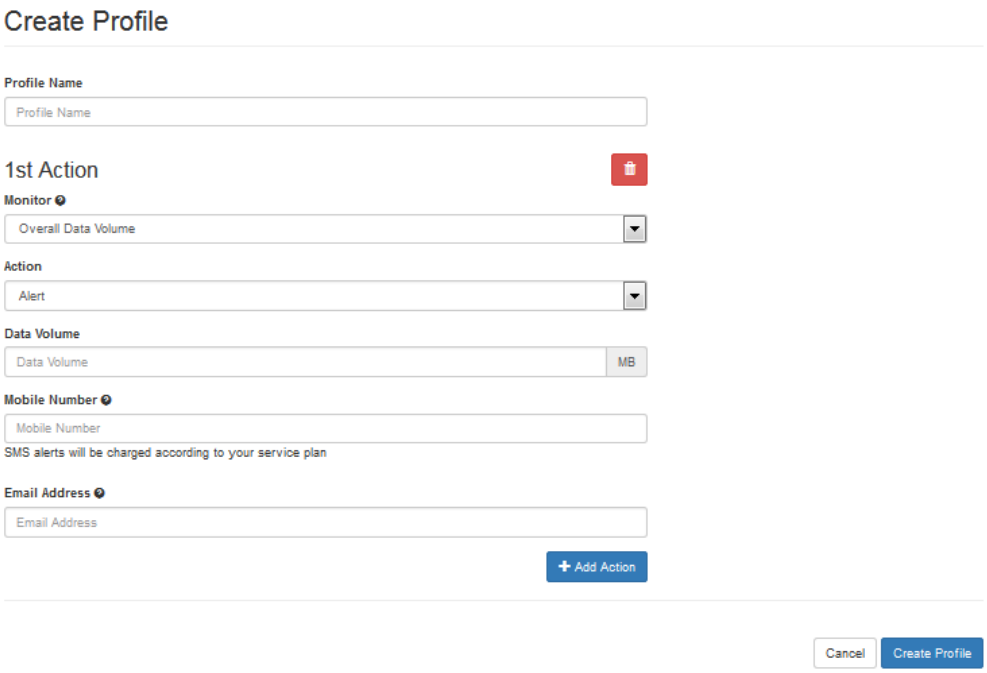


2.3 Under 'Monitor', select and enter a value for one of the options below (excluding 'c'):

a. Overall Data Volume (MB)

b. Percentage of Data Allowance (Refers to % of data inclusion if the plan has a data inclusion limit or % of data limit for a casual plan with no data inclusion. Max limit is 300%)

c. Portal User Action (Monitor changes made by Users)



2.4 Under 'Action', select one of the options below:

a. Alert

b. Individual Service – Bar Data

c. Individual Service – Unbar Data

d. Group - Bar Data

e. Group - Unbar Data

Alert refers to sending email and/or SMS alerts to the configured recipients in step 2.5. when the data usage reaches the configured data limit in step 2.3.

Bar/Unbar refers to barring/unbarring the service and sending email and/or SMS alerts to the configured recipients in step 2.5. when the data usage reaches the configured data limit in step 2.3.

Group service refers to Shared Corporate Allowance Plans (SCAP), e.g. Inmarsat BGAN M2M SCAP 50MB.

2.5 You can choose one of the following for each Action. This is useful when you want to send alert notifications to your team members who are not registered with a Pivotel account.

a. Email alert only

b. SMS alert to mobile only

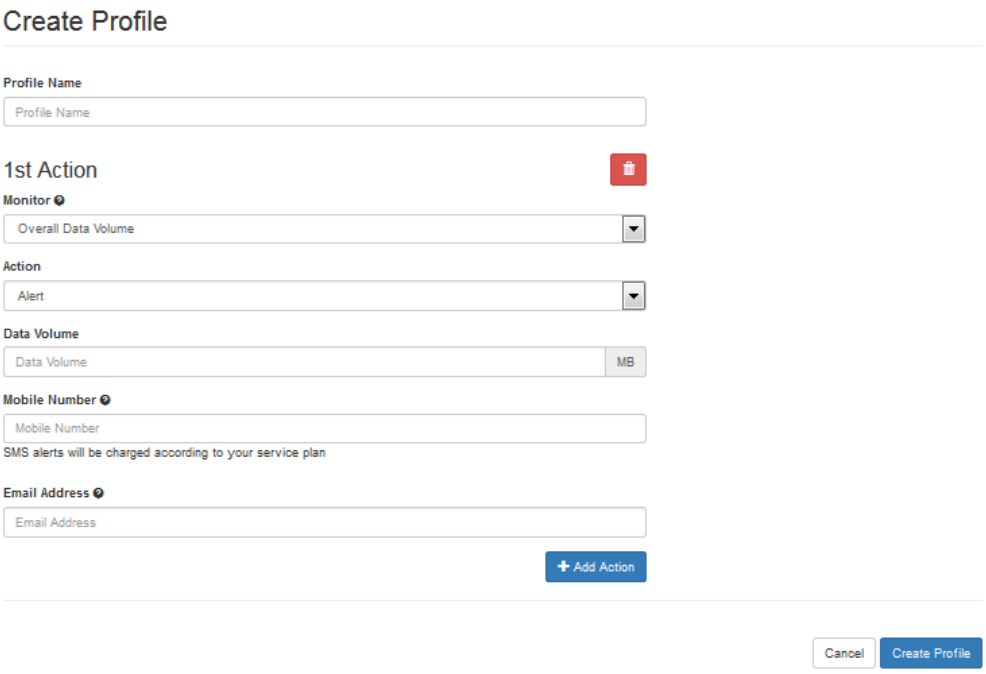
c. Email and SMS alerts

Email alerts are free. You can enter as many Email Addresses as required. Remember to separate multiple Email Addresses with a comma and ensure there is no space in between.

Each SMS alert is charged as a satellite SMS. You can enter as many mobile numbers as required. Mobile numbers must be entered in international format. Remember to separate multiple mobile numbers with a comma and ensure there is no space in between.

Email and SMS alerts are recommended for each Data Bar action to ensure you and your team members receive these critical notifications. When the service is data barred, you can log into PULSAR to unbar the service in real time. See Step 4.1.

2.6 You can have multiple actions under one profile. Click ‘Create Profile' to save.



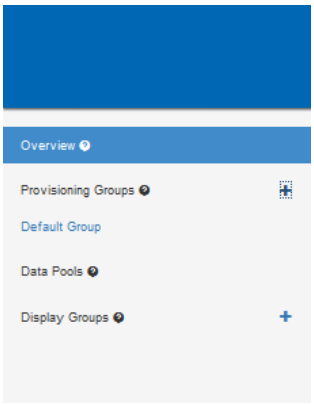
Step 3: Allocate Services To Your Profile

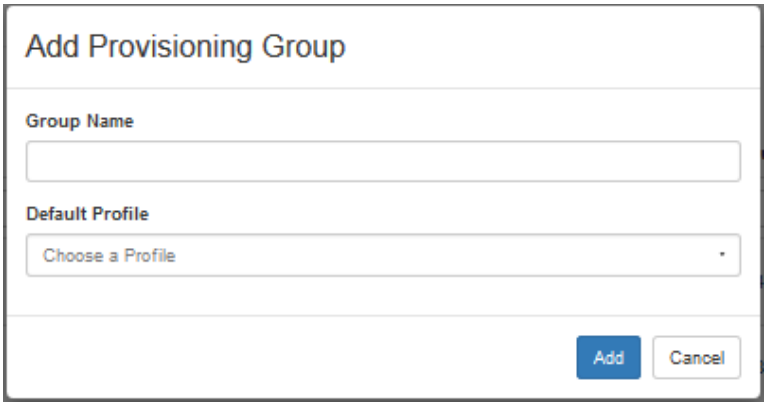
Once a new PULSAR profile is created as above, you need to create a new Provisioning Group with your new Profile and assign services to the new Provisioning Group for the profile to take effect. A service is assigned to a PULSAR default profile unless you re-assigned it to your new profile.

3.1 For IP based services such as Iridium Certus, Inmarsat Fleet One, Inmarsat BGAN M2M, Inmarsat IsatHub and Thuraya IP, select 'IP Data Services'. For store-and-forward services such as Iridium SBD and Globalstar Simplex (SPOT Trace, SPOT 3), select 'M2M Services'.

M2M services is currently under development and only offers limited information.

3.2 Under 'Provisioning Groups', click '**+ Add Provisioning Group**'. Enter your Group Name and select your Profile. Click '**Add**' to save.

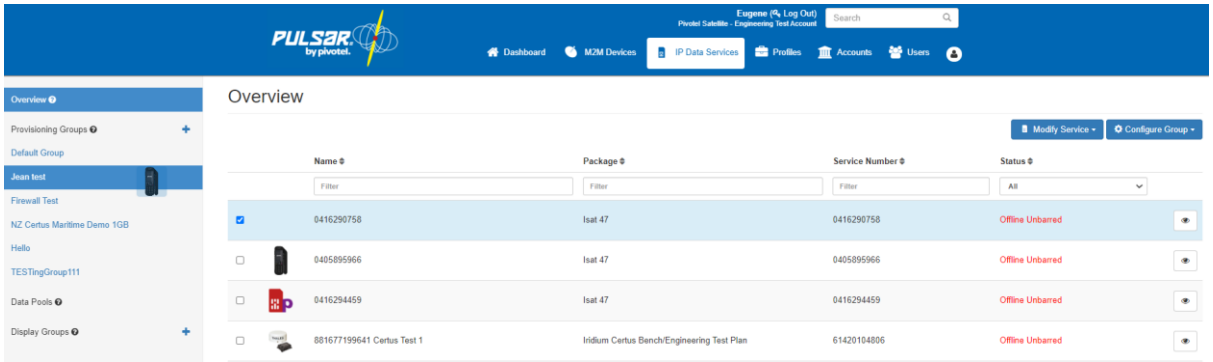


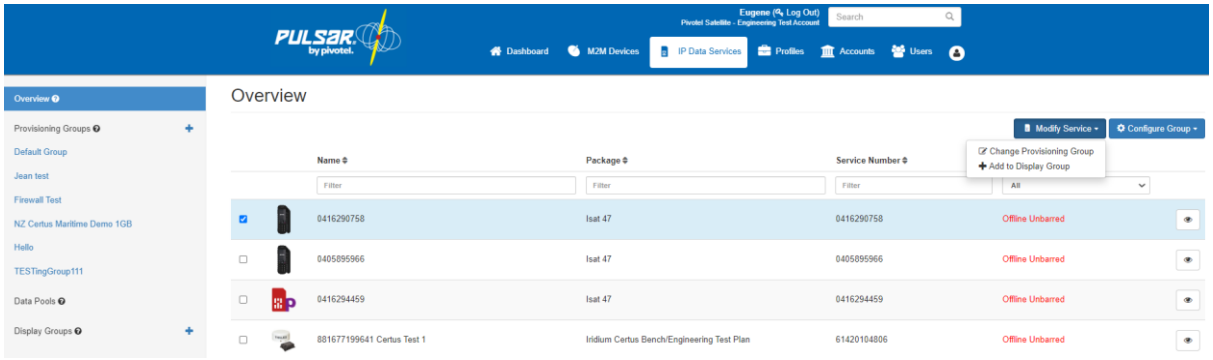


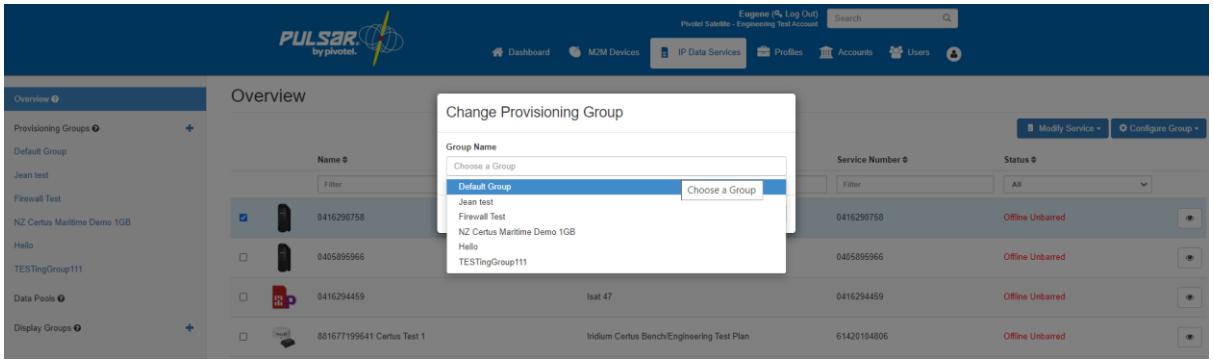
3.3 To move a service to a new Provisioning Group, you can

a. Click on the terminal image or SIM image and drag the services from the Default Group to your new Provisioning Group, or

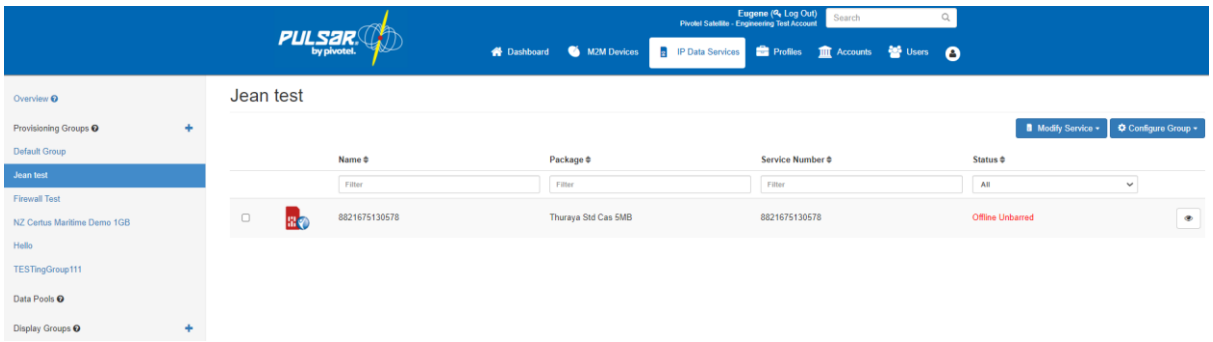
b. select the service, then click '**Modify Service**', select 'Change Provisioning Group', select the group you wish to move the service to and click '**Add**' to save.



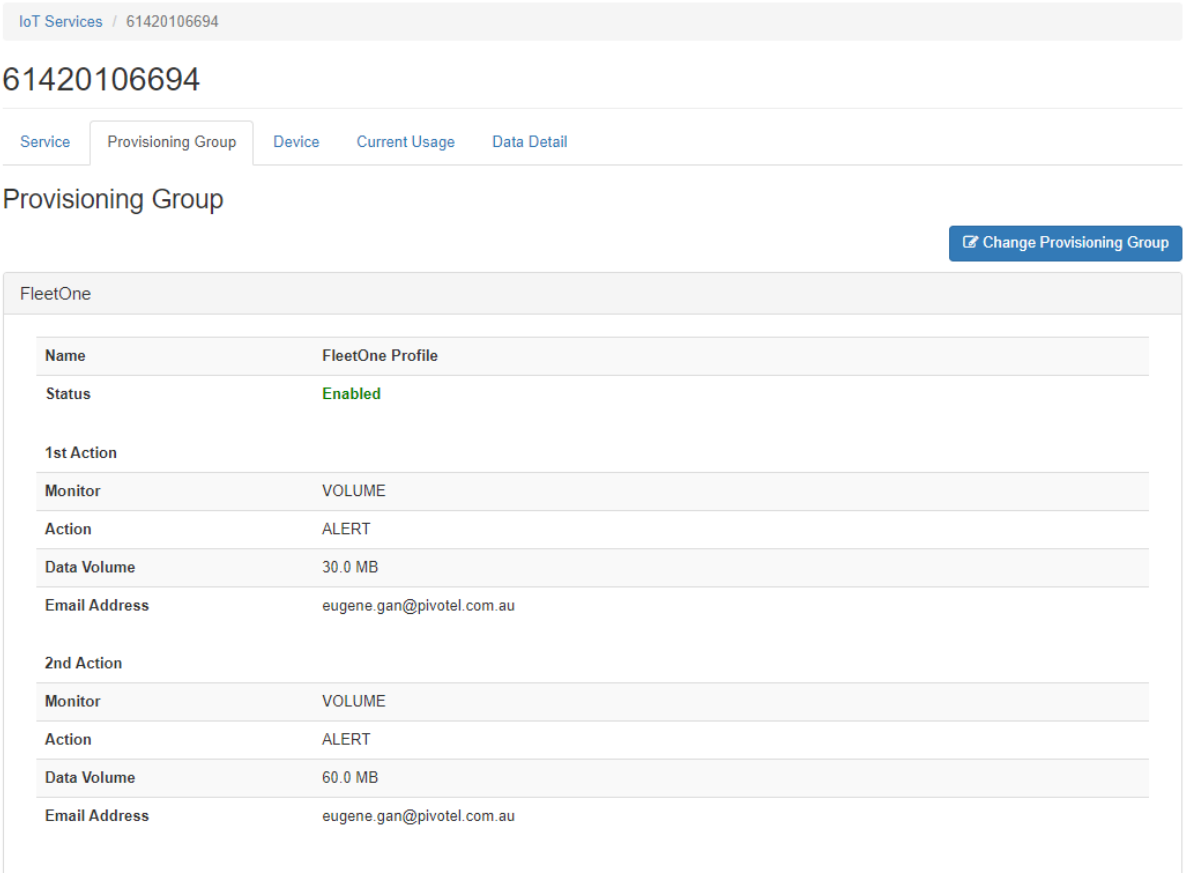




3.4 You can now click on your new Provisioning Group to view the services assigned to the Group.



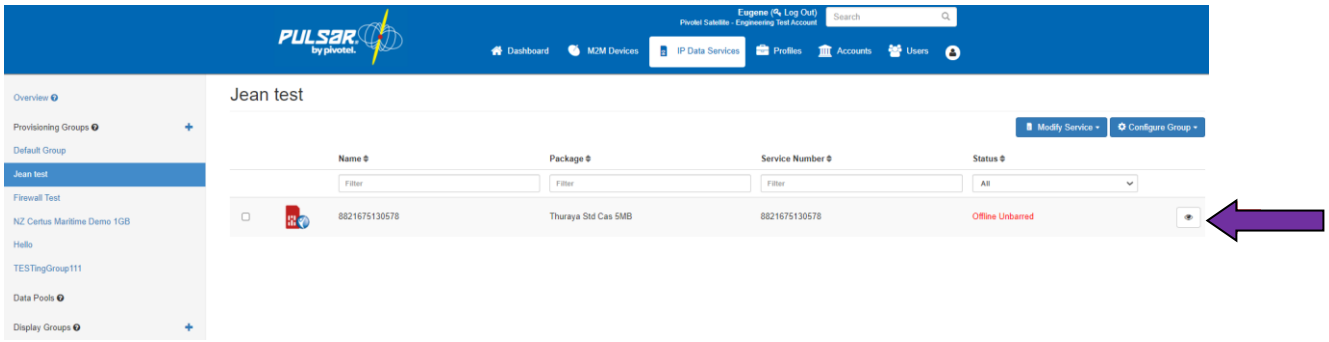
3.5 You can click into service detail and select Provisioning Group to view the Profile set for the service.



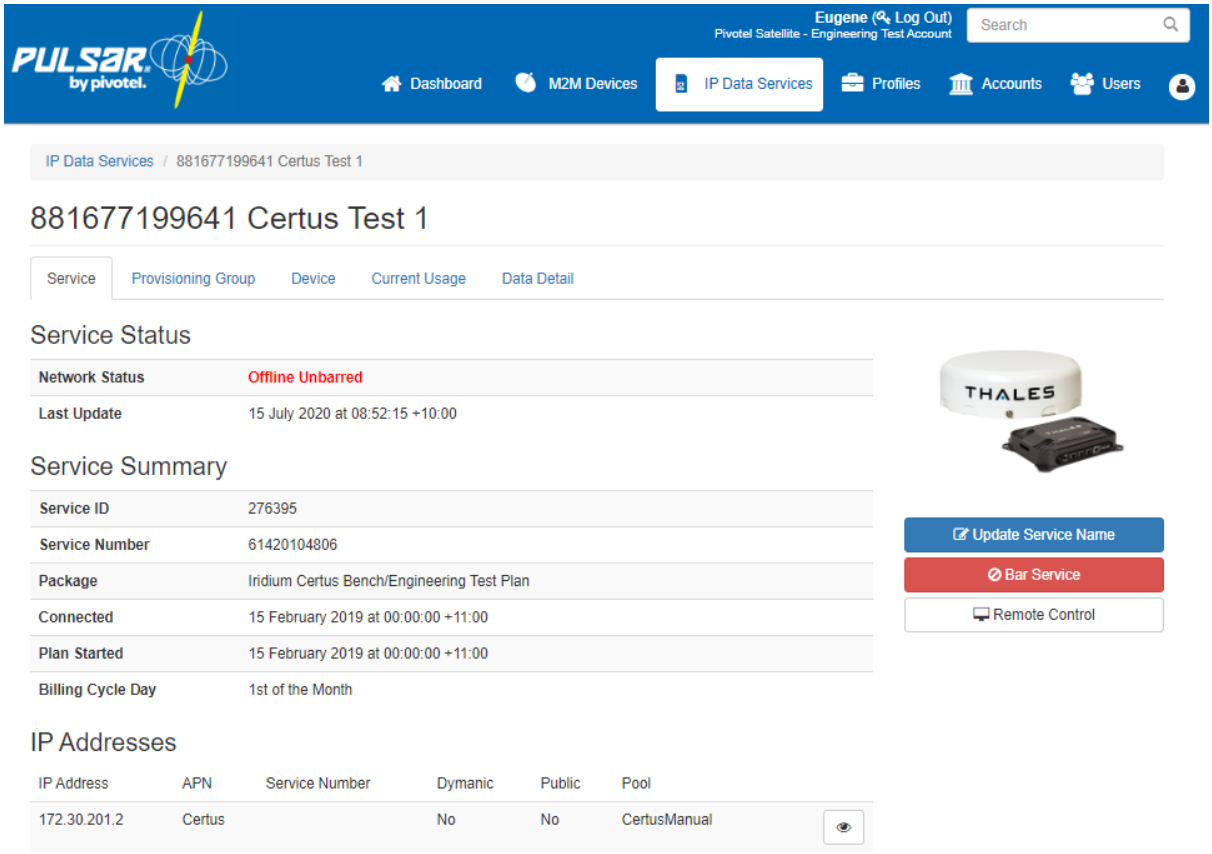
Step 4: Monitor Your Data Usage

To view your current month's data usage (usage since last bill)

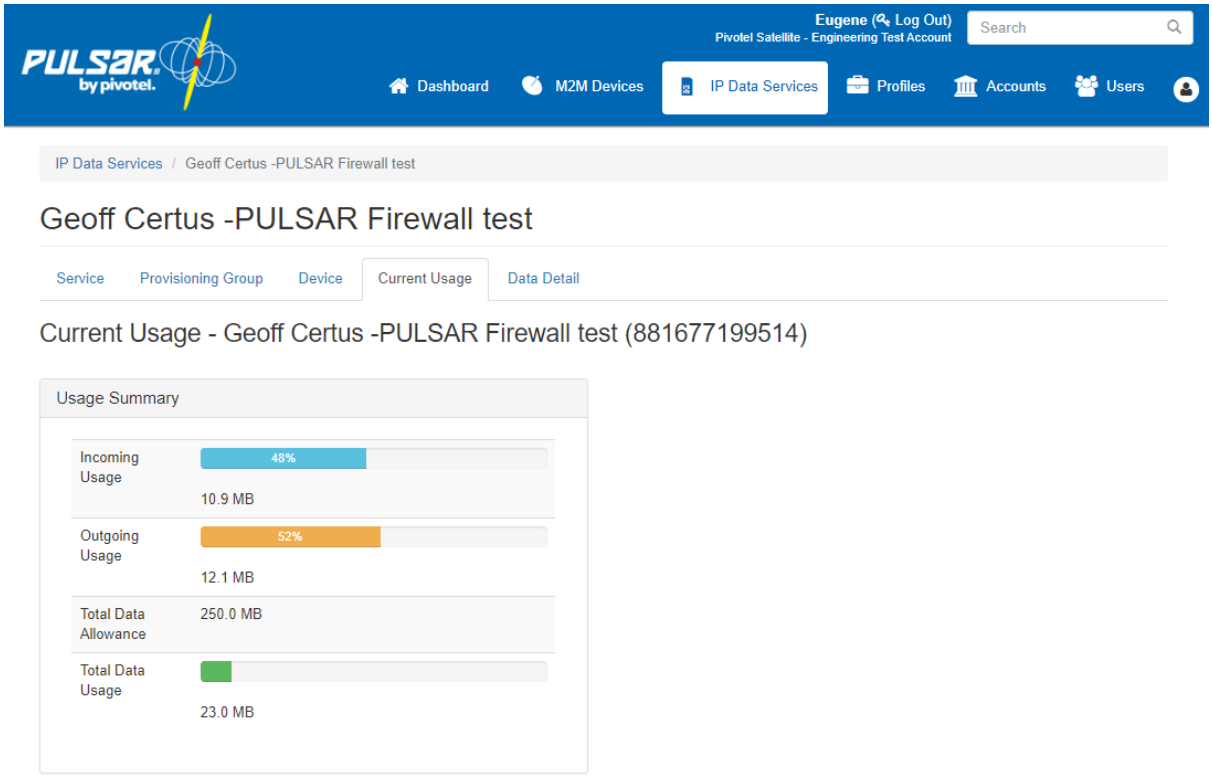
4.1 Click on for the service you wish to check.



Under Service, you can choose to Update Service Name, or Bar/ Unbar service in real time.



4.2 Select the 'Current Usage' tab and view the 'Total Data Usage' under 'Usage Summary'.



Usage Summary in Current Usage:

- Incoming Usage, Outgoing Usage and Total Data Usage are for analytical purposes only.

Step 5: Manage Firewall Rules Of Your Service

The Pulsar Firewall Management capabilities allow you to manage your own firewall rules for your service for outbound or inbound data traffic.

Outbound

- To allow all traffic except the configured rules
  OR;
- To deny all traffic except the configured rules

Inbound (Only for service with Public IP address)

- To deny all traffic except the configured rules

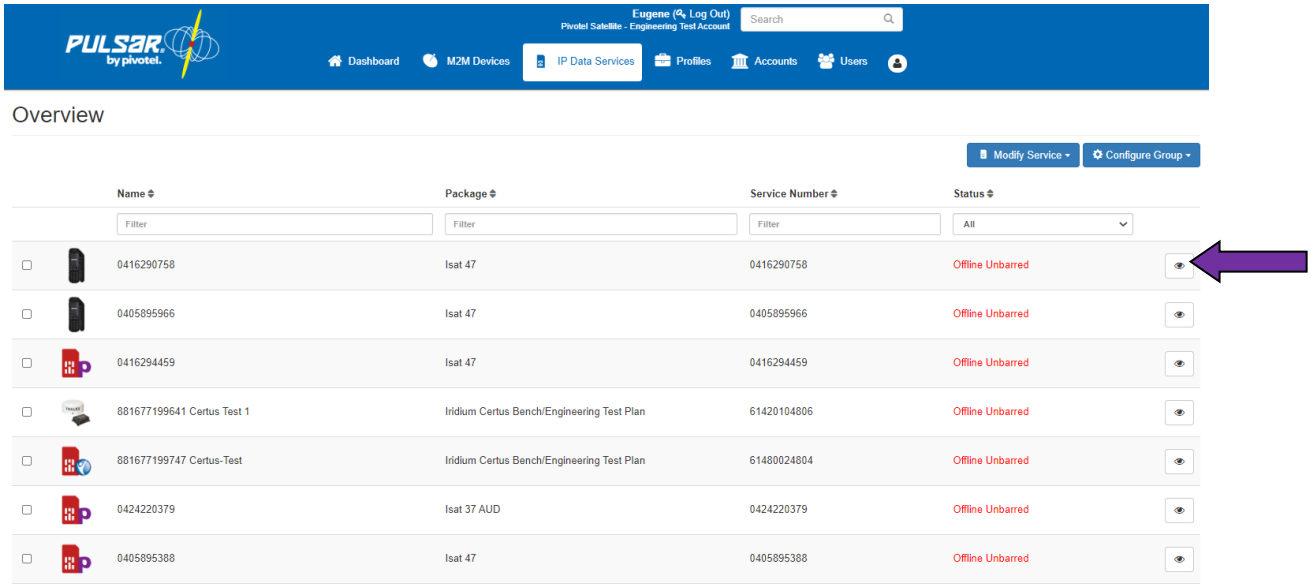
Note:

1. *The firewall operation configured with Pulsar occurs within the ground core network. This means that any denial of IP traffic outbound from the satellite terminal will only occur once the initial requests have traversed the satellite network, resulting in some data usage, which may be chargeable. To avoid this data usage, firewall protection can be set at the satellite terminal (if the terminal supports firewall configuration) or through the use of a suitable external firewall router such as the RedPort Optimizer. Configured correctly this will deny IP data traffic before it can be transmitted over the satellite network.*
2. *Pulsar Firewall Management does not support category filtering (e.g OS update category, gaming category, illegal drug category and etc.) It is the responsibility of the service user to configure the correct IP addresses, fully qualified domain names and necessary protocols and ports to ensure the firewall operates for the users intended purpose.*

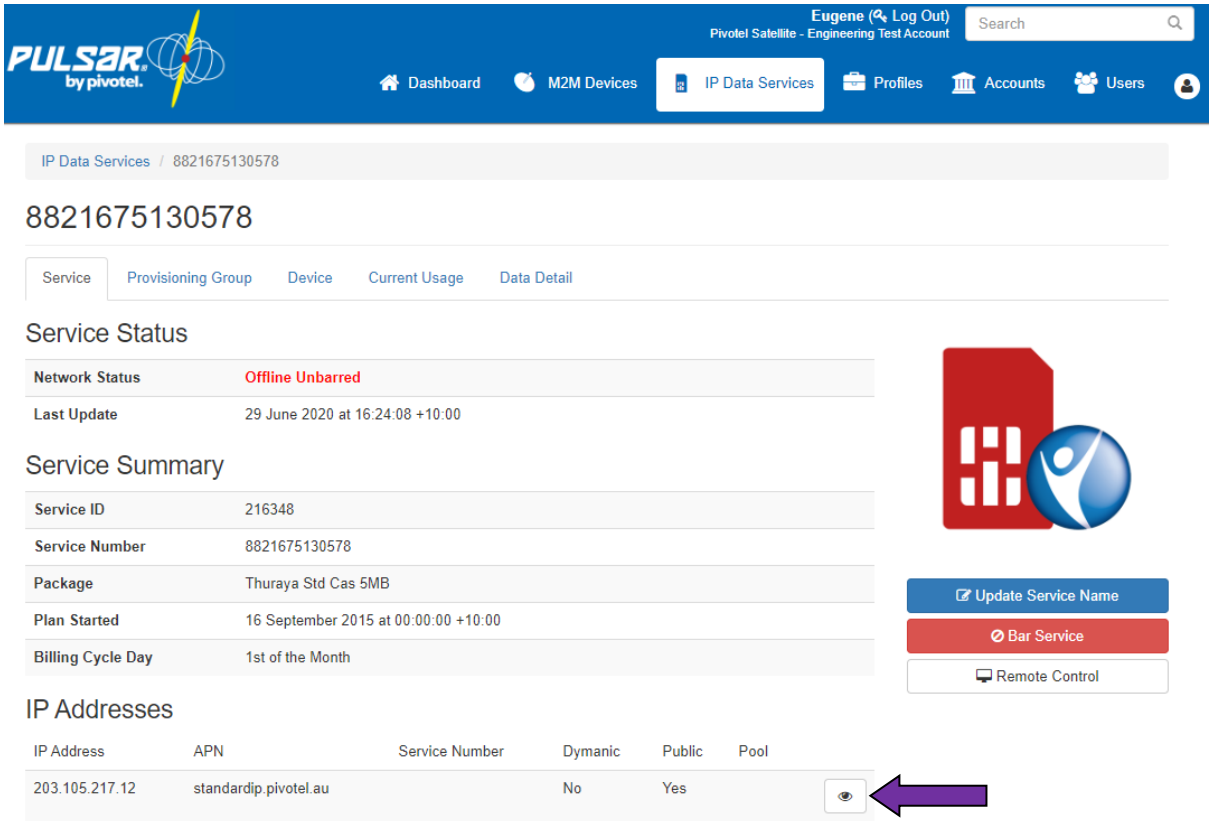
By default, your service will allow all outbound data traffic and deny all incoming data traffic. If you subscribe a Public IP address for the service, you can also manage the whitelist IP addresses to allow incoming data traffic.

To manage the firewall rules for your service,

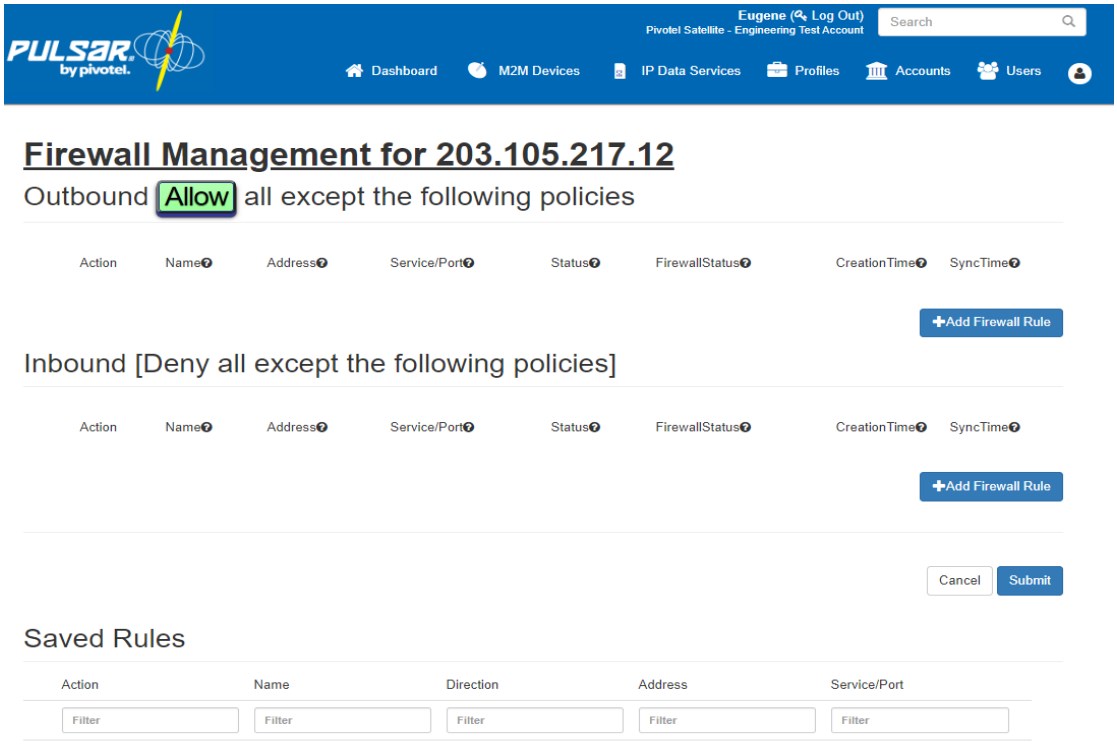
1. Click on icon of the service to manage the firewall rules.



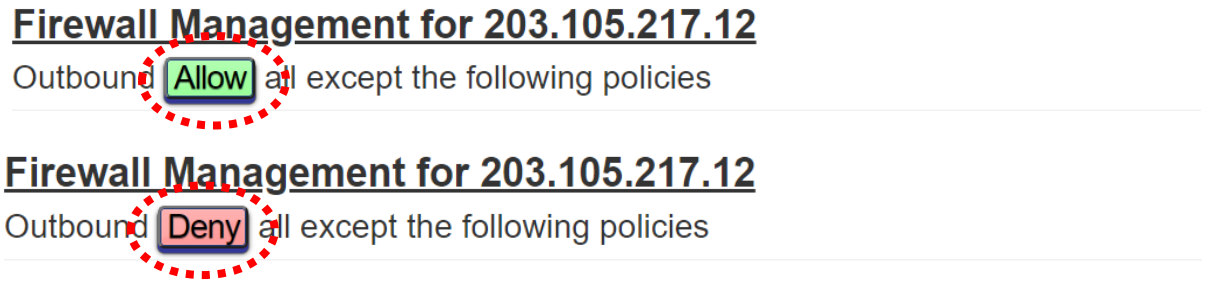
2. Click on the icon in IP Addresses section



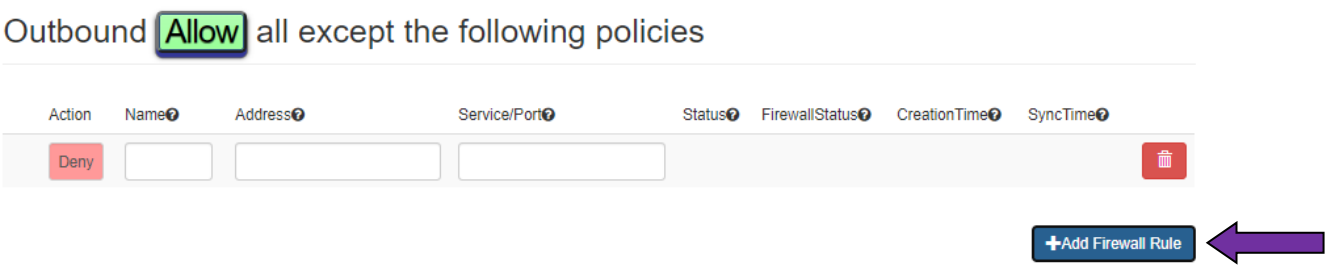
3. This will open the firewall management page for the IP address you wish to configure



4. To configure the outbound traffic, you need to decide if the outbound rule will be to allow all traffic except the configured rules or deny all traffic except the configured rules by toggling the "**Allow**" or "**Deny**" button.

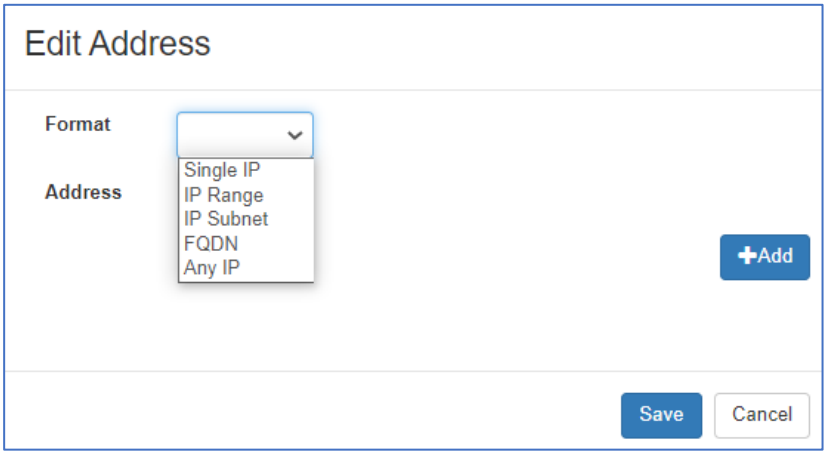


a. To add a new firewall rule, click the **+Add Firewall Rule** button and start to configure the rule. To remove a configured rule before it has been submitted click the icon.

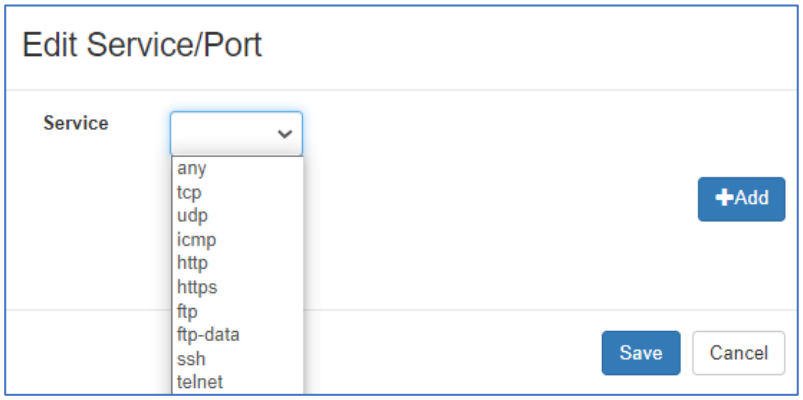


Note that the Action on the rule will say 'Deny' if you have chosen to 'Allow all except' or it will say 'Allow' if you have chosen to 'Deny all except'. To configure the rule take the following steps:

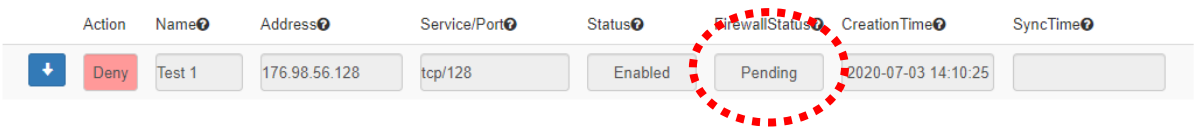
i. Enter a Name for the outbound rule.
ii. Click on the Address box to configure the IP address.
    a. A selection of formats can be configured. After configuring the IP address for the rule, click **+Add** to add to the list. You can continue to add other formats of IP address. Please note that the service type will be defined in the next configuration parameter so it is recommended to only group addresses together that will utilise the same Service type, eg FTP, HTTP etc. Click **Save** when done.
    b. Options for Format include
        - Single IP – used to apply the rule to a single IP Address
        - IP Range – used to apply the rule to an IP Address Range
        - IP Subnet – used when applying the rule to an entire subnet
        - FQDN – used to apply the rule to a Fully Qualified Domain Name. eg www.google.com
        - Any IP - used when applying the rule to all IP addresses to a particular service type. Service type is addressed in the next configuration parameter.



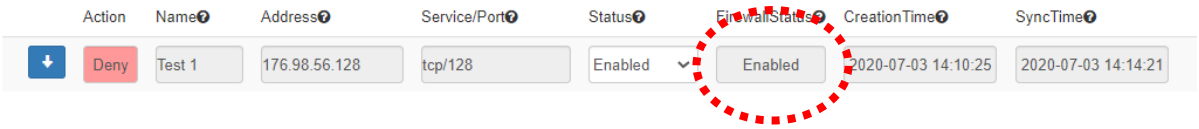
iii. Click on the Service/Port to configure the firewall rule service. A selection of services can be configured based on the drop-down menu. After selection of the service, click **+Add** to add it to the list. You can continue to add other services as they apply to the IP Addresses that have already been added in the previous step. Note if you don't want each of the services to apply to all of the IP Addresses identified it is better to separate them out into separate rules. Click **Save** when done.



b. Repeat step a, if you wish to configure additional rules, else click **Submit**.
Please note the FirewallStatus of the newly added rule will display as "Pending" followed by "InProgress" while waiting to synchronize with the firewall.

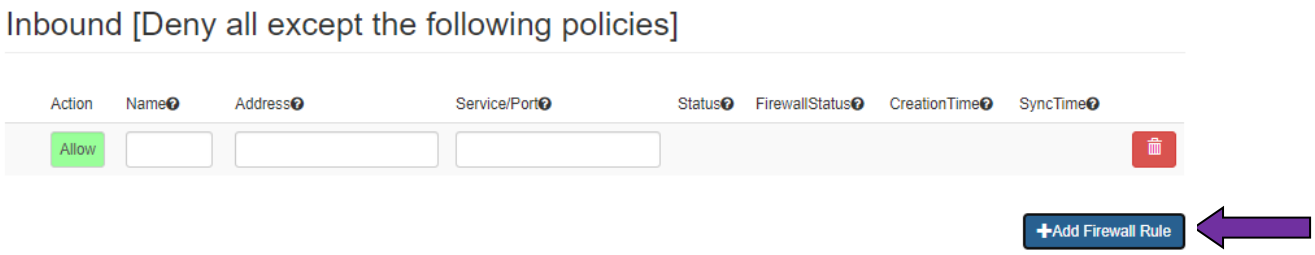


The FirewallStatus will change to “Enabled” once synchronization has been completed. During the “Pending” or “InProgress” status, you will not be allowed to add, delete, or save any further rules. Once the rule is successfully synchronized to the firewall, the FirewallStatus will be changed to Enabled.
*Note: The synchronization process can take up to 5 minutes to complete. The ‘**Refresh**’ button can be used to refresh the web page to provide an update of the FirewallStatus.*

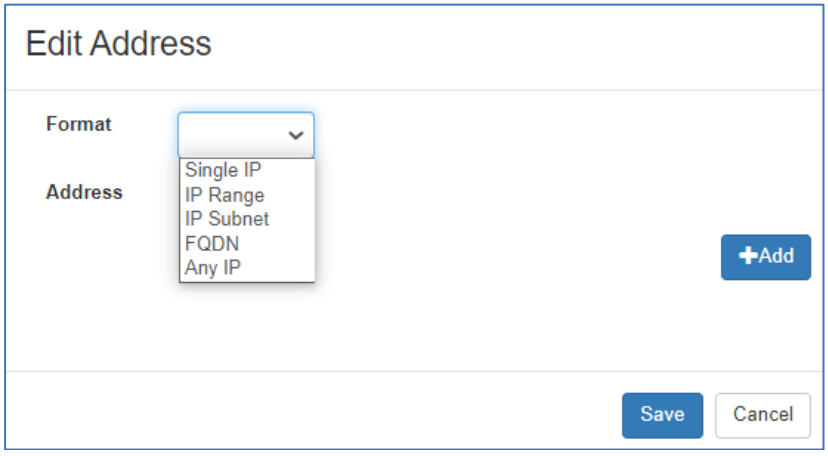


c. If the rules fail to be enabled in the firewall, an alert window will be displayed and the FirewallStatus will update to Failed. Please contact Pivotel Technical Support at TechSupport@pivotel.com.au to resolve the issue.

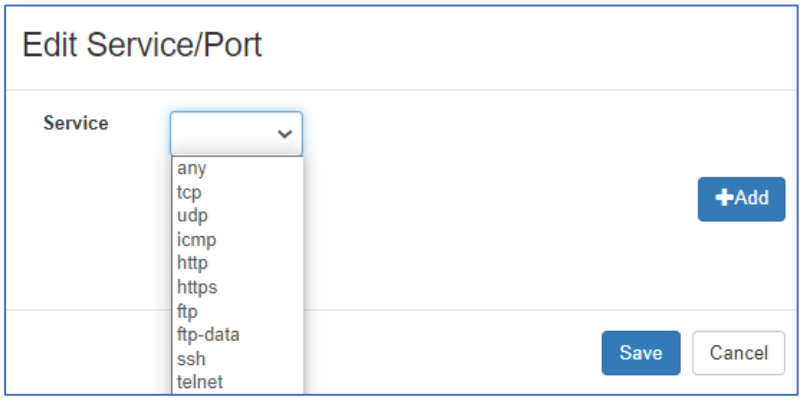
5. To configure the inbound traffic rules of your service,
   a. Click the **+Add Firewall Rule** button and start to configure the rule. To remove a configured rule before it has been submitted click the icon.



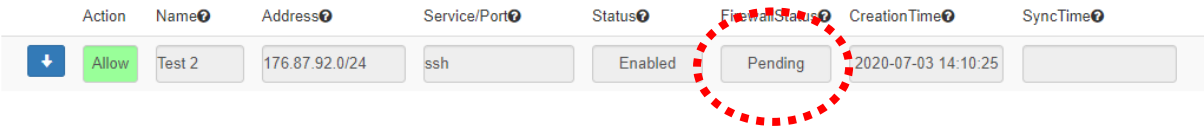
To configure the rule take the following steps:
i. Enter a Name for the inbound rule.
ii. Click on the Address box to configure the IP address.
   a. A selection of format can be configured. After configuring the IP address for the rule, click the **+Add** to add to the list. You can continue to add other formats of IP addresses. Click **Save** when done. See 4 above for an explanation of the formats provided.



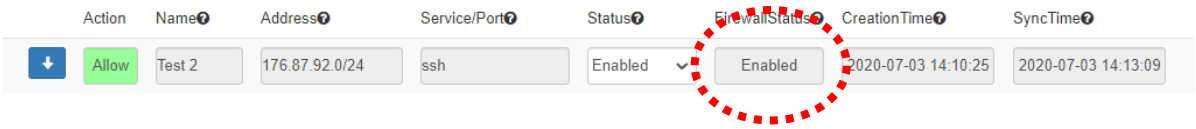
iii. Click on the Service/Port to configure the firewall rule service. A selection of services can be configured based on the drop-down menu. After selection of the service, click **+Add** to add it to the list. You can continue to add other services as they apply to the IP Addresses that have already been added in the previous step. Note if you don’t want each of the services to apply to all of the IP Addresses identified it is better to separate them out into separate rules.. Click **Save** when done.



b. Repeat step a, if you wish to configure additional rules, else click **Submit**.
Please note the FirewallStatus of the newly added rule will display as "Pending" followed by "InProgress" while waiting to synchronize with the firewall.



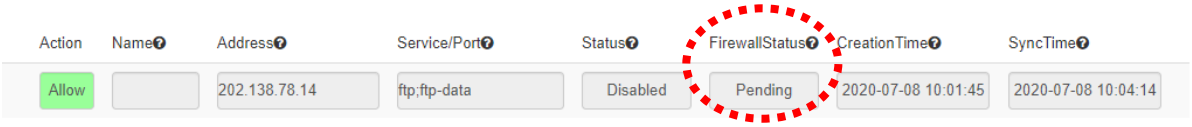
The FirewallStatus will change to "Enabled" once synchronization has been completed. During the "Pending" or "InProgress" status, you will not be allowed to add, delete, or save any further rules. Once the rule is successfully synchronized to the firewall, the FirewallStatus will be changed to Enabled.
Note: The synchronization process can take up to 5 minutes to complete.
*The '**Refresh**' button can be used to refresh the web page to provide an update of the FirewallStatus.*



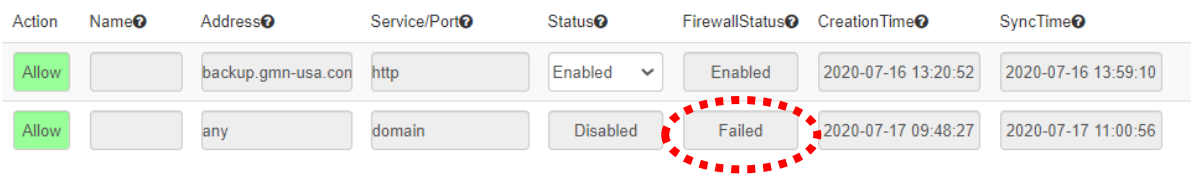
c. If the rules fail to be enabled in the firewall, an alert window will be displayed and the FirewallStatus will update to Failed. Please contact Pivotel Technical Support at TechSupport@pivotel.com.au to resolve the issue.

6. To disable the inbound or outbound rules, click on the Status drop down menu of the rules and select **Disabled** then click **Submit.**

Please note the FirewallStatus of the disabled rules will display as "Pending" or "InProgress" while waiting to synchronize with the firewall.



a. If the rules are successfully disabled in the firewall, the rules will be removed from the firewall management UI.
b. If the rules fail to disable in the firewall, an alert window will be displayed and the FirewallStatus will update to Failed. Please contact Pivotel Technical Support at TechSupport@pivotel.com.au to resolve the issue.



7. You can save a configured inbound and outbound rule to the Saved Rules section which allows you to apply the same rule on other services within the same account.

   To save a rule, click the icon adjacent to the rule that you wish to save. The rule will now appear in the Saved Rules section at the bottom of the page. Prior to submitting the saved rules list, you can remove a rule that has been selected to be saved by clicking the icon beside the rule in the Saved Rules section. Click **Submit** to save the selected rules to the Saved Rules section.

   Note: If a rule does not display the icon, it means the rule has already been saved to the Saved Rules section.

   You can assign a saved rule to the Inbound or Outbound firewall rules configuration if that rule is currently not configured for the service. The Direction column identifies whether a rule is for inbound or outbound use.

   Click the icon of the rule that you wish to apply to the service.

   To view services that currently using the rule, click on the icon.

   To delete the rule from the Saved Rules, click on the icon.