



Pivotel Pulsar User Guide

Contents

1.0 Overview of Pulsar	2
2.0 Create your Pulsar login.....	2
3.0 Pulsar Details.....	4
3.1 Dashboard.....	4
3.2 Services & Devices.....	5
3.2.1 Overview of services	5
3.2.2 Summary of a Service	6
3.2.3 Details of a Service	7
3.3 Profiles	8
3.3.1 To create a new Alert Profile	8
3.3.2 To create a new Barring Profile	10
3.3.3 To create a new Firewall Profile	10
3.3.4 Assign Profile to a Service	12
3.4 Account Management - Users	12

1.0 Overview of Pivotel Pulsar

Pivotel provides the Pulsar web-based portal that allows users to view, control and manage their data services and costs. Pivotel Pulsar provides real time service status, data usage information and the ability to configure and control network barring and firewall rules. Every Pivotel data service is automatically assigned to the Pulsar default profile when activated. Pulsar sends alert emails to the email address registered on the Pivotel account when the data usage for each individual or shared plan reaches 50%, 85%, 100% of a pre-set data alert limit and automatically bars the data usage when it reaches 150% of the data inclusion or a pre-set data bar limit. To meet the business requirements, users can create customised data Alerting and Barring Profiles with different thresholds and change the email addresses to receive Pulsar notifications.

2.0 Create your Pulsar login

1. Open your browser and navigate to <https://new.pulsarportal.com/>
2. Under First time using Pulsar?, click Create New Account.



3. Enter your Pivotel Account Number and Billing Password, then click Verify Account. If you do not know your Pivotel Account Number and Billing Password, please contact Pivotel Support. You can find Pivotel contact detail at <https://www.pivotel.com/contact-us>



Verify Billing Account

Account Number

Billing Password

[Verify Account](#)

4. Enter a Username, Display Name and your Contact Information in the fields provided. Your Username will be the User ID for your Pulsar login. Your Display Name will be displayed on the top of the Pulsar portal after you login, typically it is your Pivotel account name or organisation name. Click Create Administrator to create a Pulsar login account.



Create New Administrator

Username

Display Name

Contact Information

First Name

Last Name

Email Address

Your password will be automatically generated and sent to this email address.

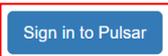
[Create Administrator](#)

5. When your account is created successfully, Pulsar will send a Password to your Contact Email Address.
6. Click 'Sign in to Pulsar' then enter the Username and Password sent to your Contact Email Address.



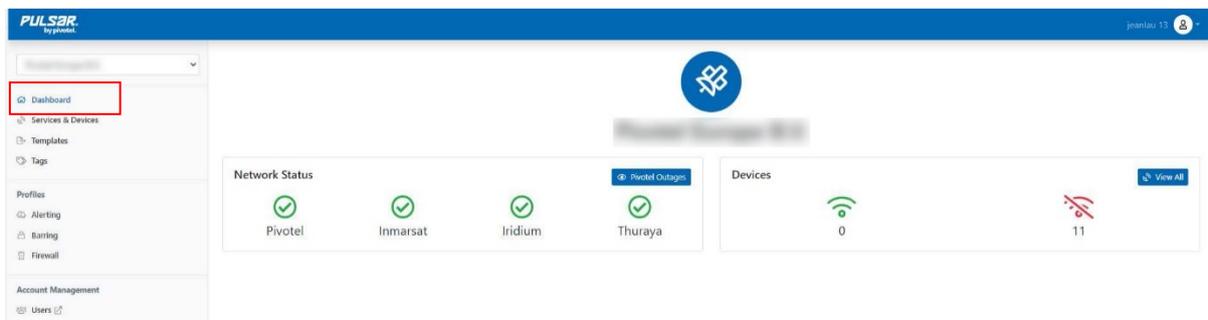
Administrator Created

You can now sign into Pulsar using your new credentials. Please check the email address provided for your automatically generated password.



3.0 Pulsar Details

3.1 Dashboard



When you login, the Dashboard will show an overview of

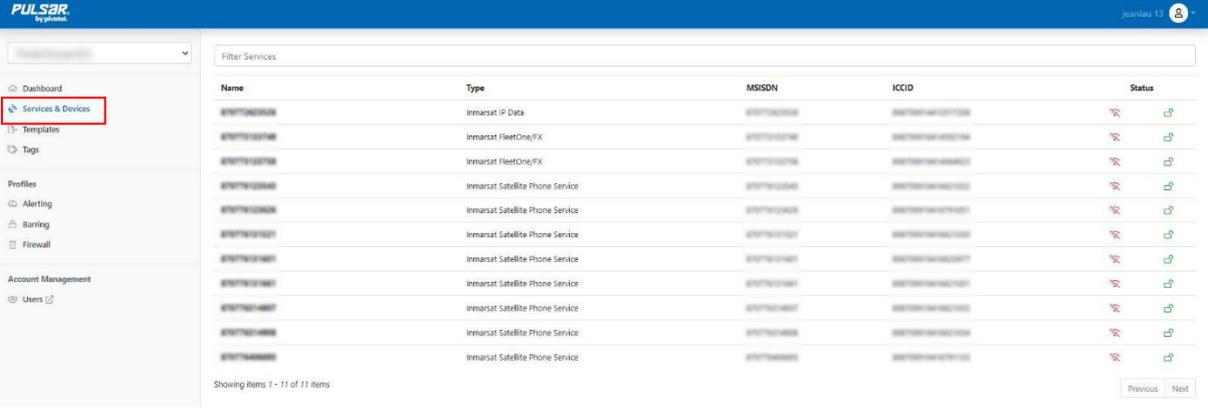
- The network Status of Pivotel, Inmarsat, Iridium and Thuraya.
- The number of Devices in your account that are currently Online or Offline .

You can click on Pivotel Outages under Network Status to view the details of any current outages.

You can click on View All under Devices or select the Services & Devices tab on the left panel to view all of your services.

3.2 Services & Devices

3.2.1 Overview of services



Name	Type	MSISDN	ICCID	Status
01777020200	Inmarsat IP Data	01777020200	00000000000000000000	 
01777020200	Inmarsat FleetOne/FX	01777020200	00000000000000000000	 
01777020200	Inmarsat FleetOne/FX	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 
01777020200	Inmarsat Satellite Phone Service	01777020200	00000000000000000000	 

When you click on Services & Devices, all of your services will be listed with the information below.

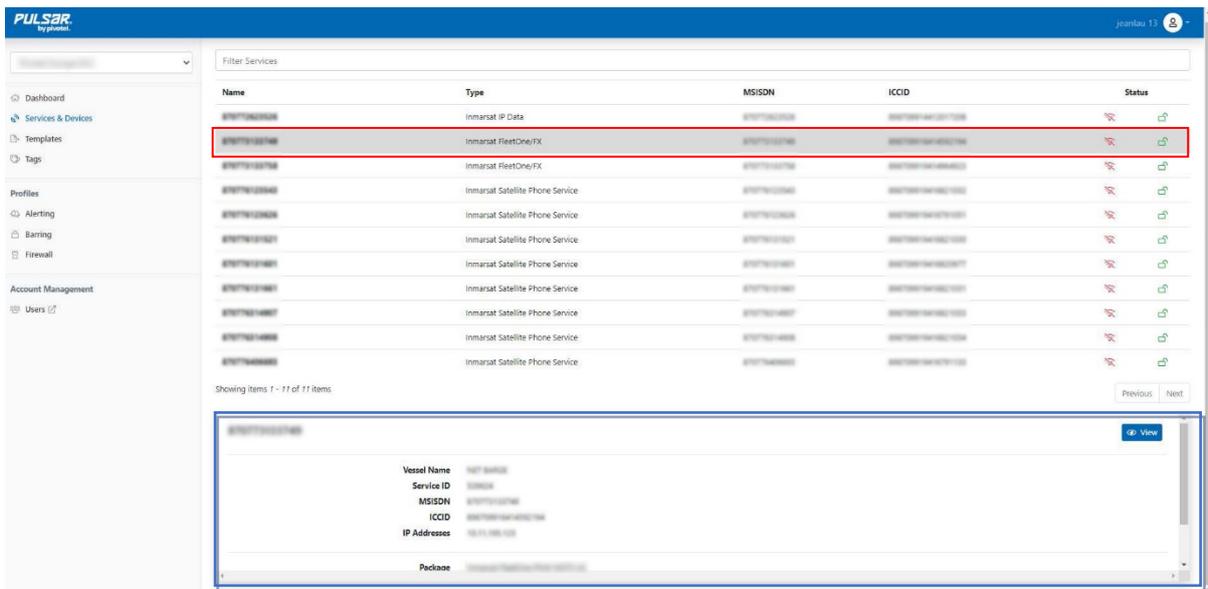
- Name –By default, it shows the service number. You can edit the service name in the service detail page.
- Type – displays the network and service type information. The network types are Iridium, Inmarsat, Thuraya and Pivotel. The service types are Voice – Data, IP Data, Certus, etc.
- MSISDN - Mobile Station International Subscriber Directory Number (MSISDN) is your service number.
- ICCID - Integrated Circuit Card Identifier (ICCID) is your SIM card number.
- Status – displays the online  or offline  status and data unbarred  or barred  status of your service

If you have more than 20 services, please scroll to the bottom and click Next to view additional services.

3.2.2 Summary of a Service

To view a summary of a service, click on the service. Some of the useful information on the summary page are as below:

- the IP addresses of your service
- the plan that your service is connected to
- the billing cycle of your service.

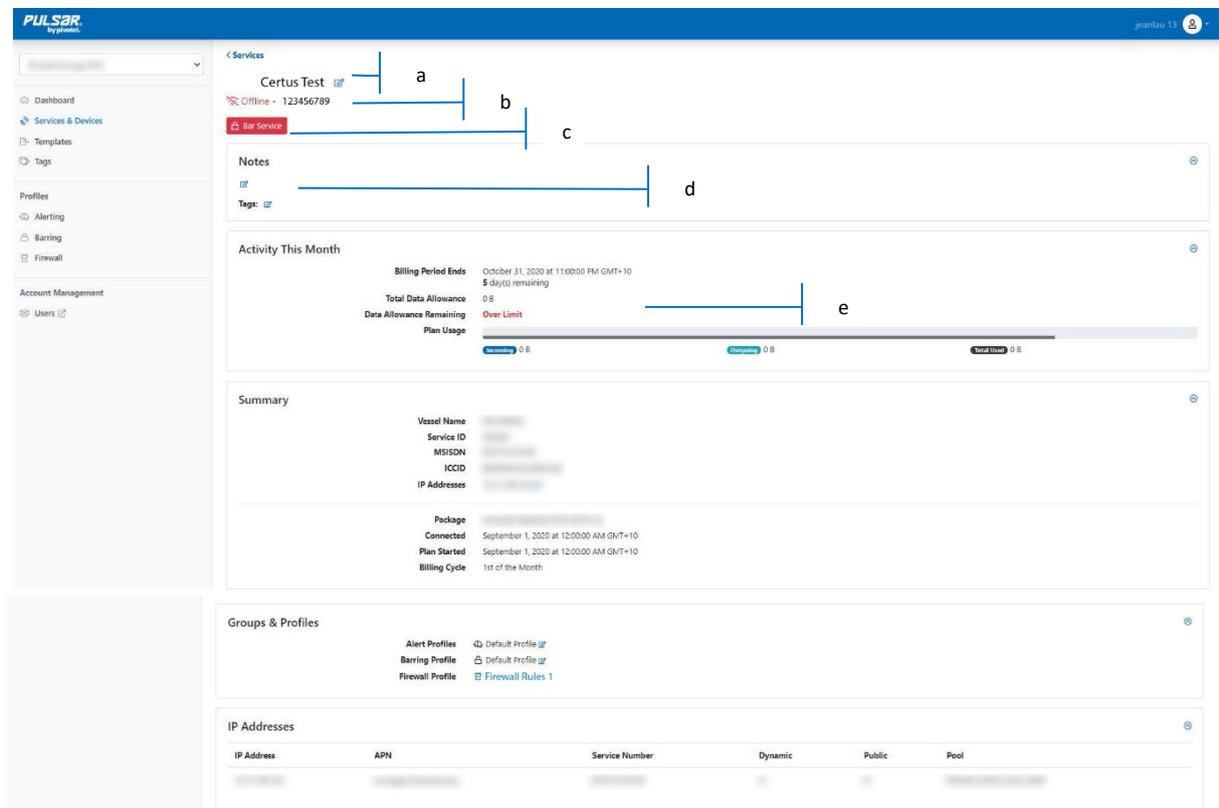


3.2.3 Details of a Service

To view the service details, click View  . The details are shown below.

On the service detail page, you can do the following

- a. Edit the service name
- b. View the status of the service and the service number
- c. Bar and unbar the service in real time
- d. Add Note and Tags to the service. Tags allow you to tag or categorize your service with keyword phrase to help you to search your service(s) easily.
- e. View your data usage in the current billing cycle. The usage will be reset at the start of each billing cycle.



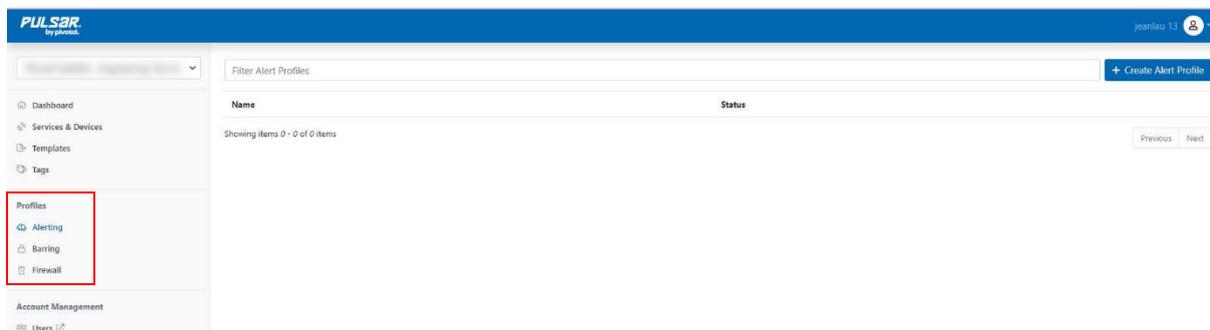
The screenshot shows the 'Certus Test' service details page in the PULSAR interface. The page includes a navigation sidebar on the left with options like Dashboard, Services & Devices, Templates, Tags, Profiles, Alerting, Barring, Firewall, and Account Management. The main content area is divided into several sections:

- Service Header:** Shows 'Certus Test' with an edit icon (a), 'Offline - 123456789' with a status icon (b), and a 'Bar Service' button (c).
- Notes and Tags:** A section for adding notes and tags (d).
- Activity This Month:** A section showing billing information: 'Billing Period Ends October 31, 2020 at 11:00:00 PM GMT+10 (5 days) remaining', 'Total Data Allowance 0 B', and 'Data Allowance Remaining Over Limit' with a progress bar (e).
- Summary:** A section listing key details: Vessel Name, Service ID, MSISDN, ICCID, IP Addresses, Package, Connected (September 1, 2020 at 12:00:00 AM GMT+10), Plan Started (September 1, 2020 at 12:00:00 AM GMT+10), and Billing Cycle (1st of the Month).
- Groups & Profiles:** A section listing profiles: Alert Profiles (Default Profile), Barring Profile (Default Profile), and Firewall Profile (Firewall Rules 1).
- IP Addresses:** A table with columns for IP Address, APN, Service Number, Dynamic, Public, and Pool.

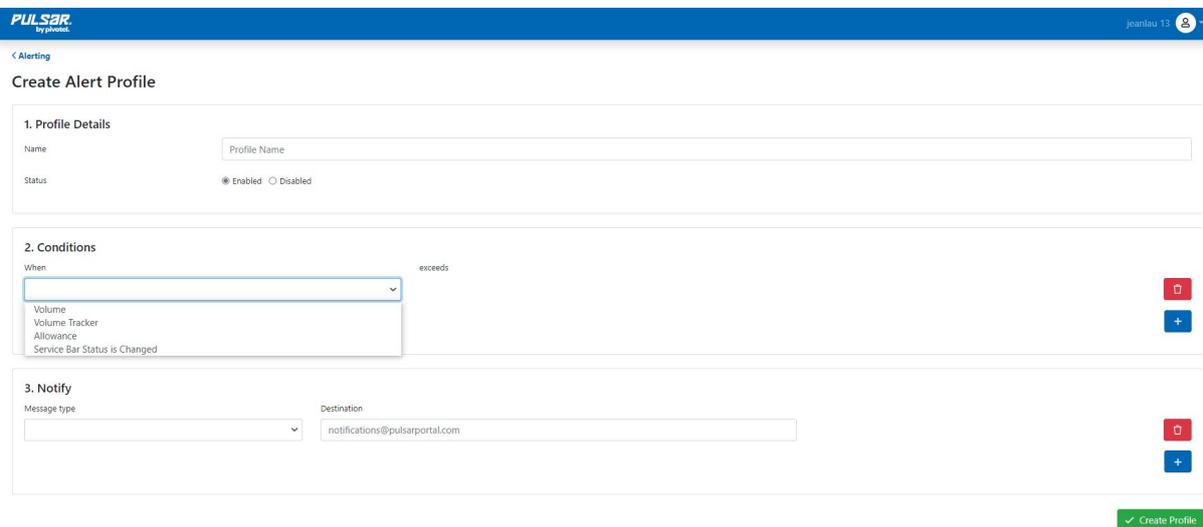
3.3 Profiles

You can create, view and edit your own data Alert, Barring and/or Firewall profiles under Profiles. A profile must be assigned to a service or services for the profile to take effect.

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.



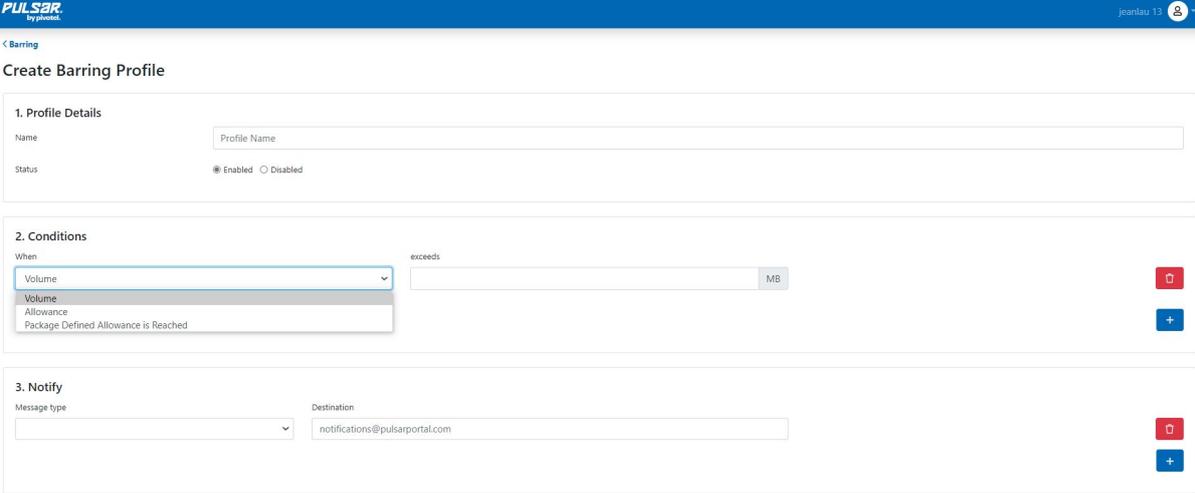
3.3.1 To create a new Alert Profile



- Click Create Alert Profile
- Under the Profile Details
 - Enter a Profile Name
 - Ensure the Status is Enabled. You can disable a profile if you do not want to use it.

- Under Conditions, you can select one or a combination of the following conditions to send the Pulsar alerts. Click + to add the next condition.
 - Volume - when the data usage exceeds a configured volume of MB. For example, send an alert when the data usage exceeds 100MB.
 - Volume Tracker - when the data usage exceeds a configured volume of MB and then every incremental configured volume of MB. For example, send an alert when the data usage exceeds 100MB, and then send alerts every 10MB after that, eg at 110MB, 120MB, 130MB etc. There is no limit to the number of alerts, Pulsar will continue to send alerts until the data usage is reset in the next billing cycle.
 - Allowance – when the data usage exceeds a configured % of the data plan inclusion. For example, send an alert when the data usage exceeds 200% of the data plan inclusion. If your plan includes 30MB, Pulsar will send an alert when the data usage exceeds 60MB, ie 200% of the data inclusion of 30MB.
 - Service Bar Status is Changed – When the service status is changed from barred to unbarred.
- Under Notify, you can choose to send the alert via email and/or SMS. This is useful when you want to send alert notifications to your team members who are not registered with a Pivotel account.
 - Email alerts are free. You can enter as many Email Addresses as required. Please add one email address per line and click + to add the next recipient.
 - 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. Please add one mobile number per line and click + to add the next recipients.
 - 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. Please be aware that any excess data usage above the data allowance will be charged the applicable data usage rate. If data usage above the data allowance is not controlled, this could result in high billing charges.
- Click Create Profile to save.

3.3.2 To create a new Barring Profile



- Click Create Barring Profile [+ Create Barring Profile](#)
- Profile Details and Notify configurations are the same as 3.3.1.
- Under Conditions, you can select one or a combination of the following conditions to bar your data service. Pulsar will bar the data service and send a notification when the service is data barred under the condition configured below. Click + to add the next condition.
 - Volume - when the data usage exceeds a configured volume of MB. For example, bar and send a notification when the data usage exceeds 100MB.
 - Allowance – when the data usage exceeds a configured % of the data plan inclusion. For example, bar and send a notification when the data usage exceeds 200% of the data plan inclusion. If your plan includes 30MB, Pulsar will bar and send a notification when the data usage exceeds 60MB, i.e. 200% of the data inclusion of 30MB.
 - Package Defined Allowance is Reached – when the data usage exceeds 100% of the data inclusion. For example, if your plan includes 30MB, Pulsar will bar and send a notification when the data usage exceeds 30MB, i.e. 100% of the data inclusion of 30MB.

3.3.3 To create a new Firewall Profile

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

By default, your IP data service is assigned a private IP address. It allows all outbound data traffic and denies all incoming data traffic. Firewall rules are only applicable to outbound data traffic.

If you subscribe a Public IP address for the service, you can apply firewall rules to both outbound and inbound traffic.

With outbound traffic, you can set the firewall rules:

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

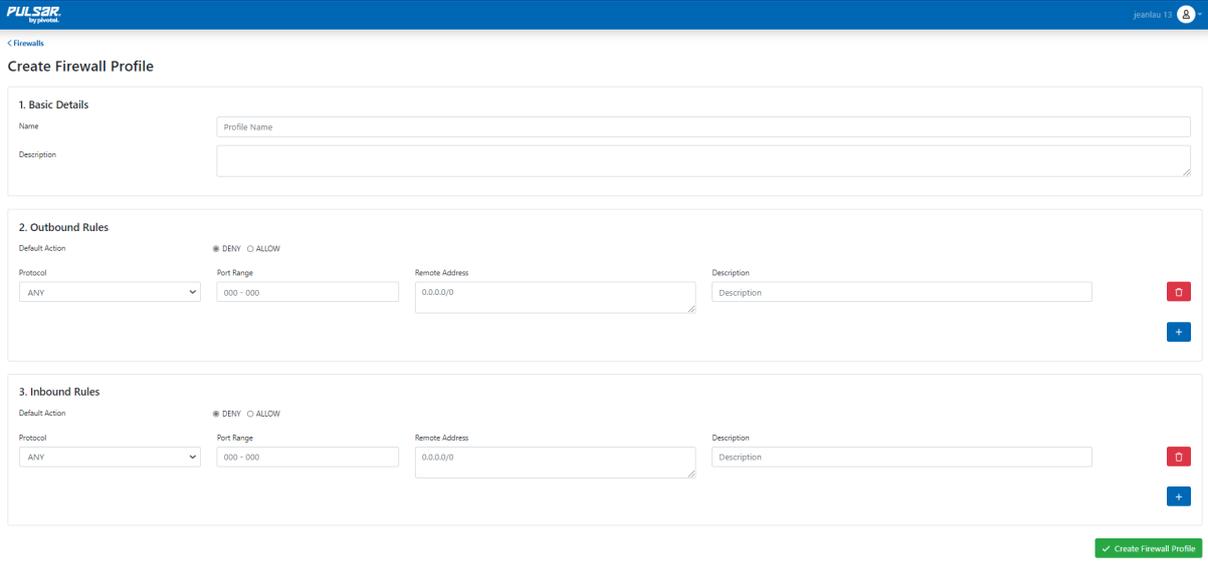
With inbound traffic (only for service with Public IP address), you can set the firewall rules:

- to deny all traffic except the configured rules

Note:

1. The firewall operation configured using 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 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.



The screenshot shows the 'PULSAR by pivotel' interface for creating a firewall profile. The form is titled 'Create Firewall Profile' and is divided into three sections:

- 1. Basic Details:** Contains two text input fields for 'Name' (with a placeholder 'Profile Name') and 'Description'.
- 2. Outbound Rules:** Features a 'Default Action' section with radio buttons for 'DENY' (selected) and 'ALLOW'. Below this are four input fields: 'Protocol' (a dropdown menu set to 'ANY'), 'Port Range' (a text box with '000 - 000'), 'Remote Address' (a text box with '0.0.0.0/0'), and 'Description' (a text box with 'Description'). A red 'X' icon and a blue '+' icon are visible on the right side of this section.
- 3. Inbound Rules:** Mirrors the structure of the Outbound Rules section, with 'DENY' selected as the default action and the same input fields for Protocol, Port Range, Remote Address, and Description.

A green button labeled '+ Create Firewall Profile' is located at the bottom right of the form.

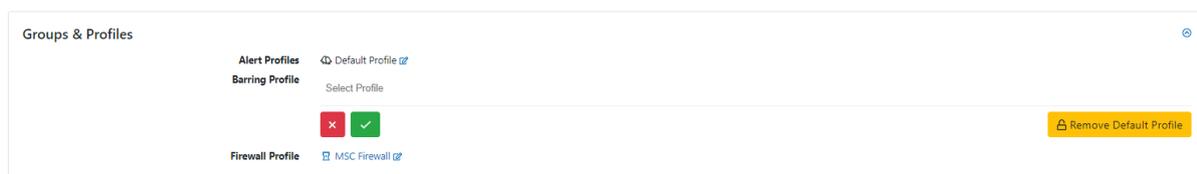
To create the firewall rules for your service,

- Click Create Firewall Profile 
- Under Basic Details, enter the Name and Description.

- Under Outbound Rules, Select the default Action to Deny (blacklist) or Allow (whitelist). Enter the Protocol, Port Range, Remote Address (destination IP address) and description. If you are not sure of the Protocol, select ANY. If you are not sure of the Port Range, select 000-000.
- Under Inbound Rules, only configure if your service has a Public IP address. Select the default action to Deny (blacklist) or Allow (whitelist). Enter the Protocol, Port Range, Remote Address (destination IP address) and description. If you are not sure of the Protocol, select ANY. If you are not sure of the Port Range, leave it blank.
- Click Create Firewall Profile to save.

3.3.4 Assign Profile to a Service

After a Profile is created, it must be assigned to the service for the profile to take effect.



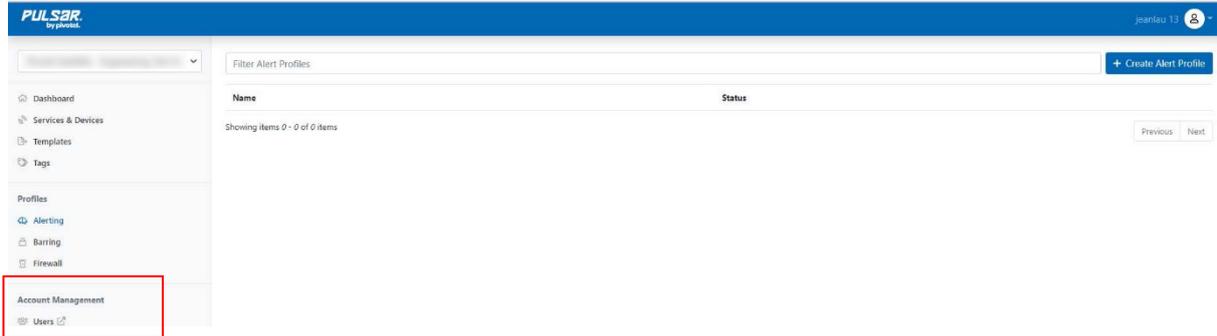
Under Groups & Profiles, Alert and Barring Profiles are automatically assigned with Pivotel default Profiles, under which Pulsar sends alert emails to the email address registered on the Pivotel account when the data usage for each individual or shared plan reaches 50%, 85%, and 100% of the plan data inclusion or a pre-set data alert limit and automatically bars the data usage when it reaches 150% of the plan data inclusion or a pre-set data bar limit.

You can remove the Default Profile for barring and leave it blank if you do not want automatic data barring on the service.

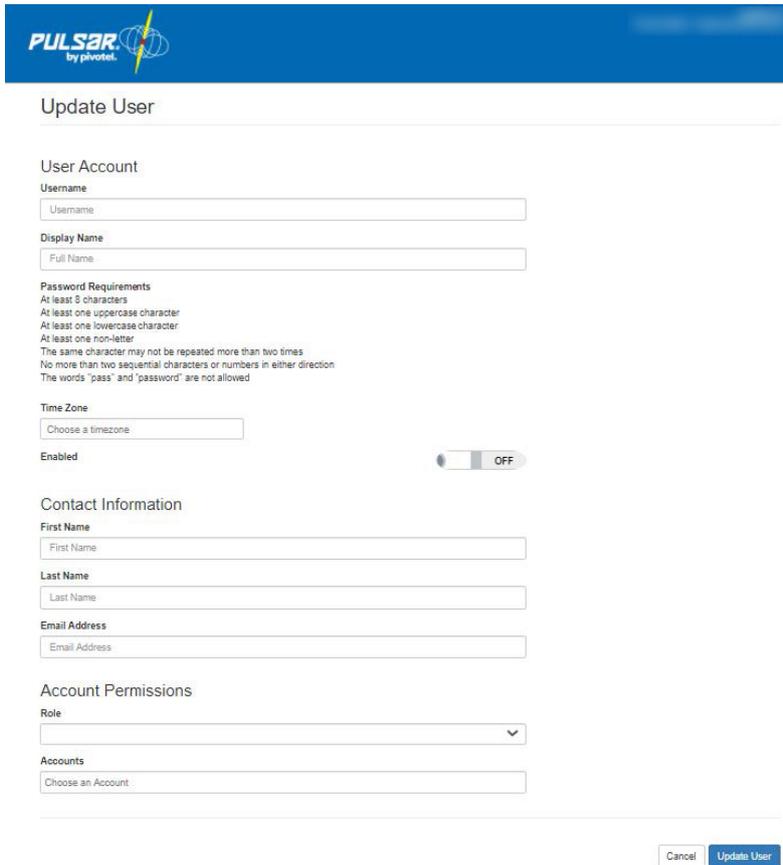
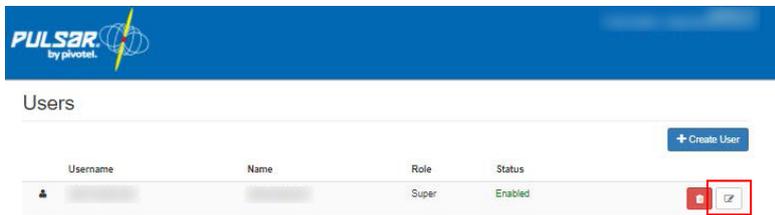
You can also allocate a data alert, barring and/or firewall profiles that you have created under profiles to the service. To change the profile, click edit next to the profile, enter the name of the profile and select yes to save.

3.4 Account Management - Users

Under account management, you can edit the Username, Display Name, Time Zone and add other users.



When you click on Users, a new window as below appears. Click edit to edit the Username, Display Name, Time Zone and add other users. Click Update User to save.



We strongly recommend that you logout when you are finished.

The screenshot shows the PULSAR by pivotel dashboard. The top navigation bar is blue with the PULSAR logo on the left and a user profile dropdown on the right containing the name 'james11' and a 'Logout' button. A left-hand sidebar contains navigation links for Dashboard, Services & Devices, Templates, Tags, Profiles, Alerting, Billing, Firewall, and Account Management (Users). The main content area features a central header with a blue icon and the text 'PULSAR by pivotel. Empowering the Network'. Below this are two main sections: 'Network Status' and 'Devices'. The 'Network Status' section displays four service providers: Pivotel, Inmarsat, Iridium, and Thuraya, each with a green checkmark icon. A blue button labeled 'Pivotel Outages' is positioned above the Thuraya status. The 'Devices' section shows a green Wi-Fi icon with the number '1' and a red Wi-Fi icon with a slash and the number '30'. A blue 'View All' button is located to the right of the 'Devices' section.