



# ThingSpace Manage

## User Guide v2.0

As of 01/18/2024

### **Important — Please Read**

Verizon Confidential & Proprietary.

© 2024 Verizon. All rights reserved.

Restricted and Controlled Distribution. Not to be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Verizon.

All information herein is subject to change without notice. The information provided was considered accurate at the time the document(s) were developed, and Verizon disclaims and makes no guarantee or warranty, express or implied, as to the accuracy or completeness of any information contained or referenced herein.

VERIZON DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

Verizon does not guarantee or warrant the availability of the network nor the compatibility of a network with any device, service or product. Verizon disclaims liability for any damages or losses of any nature whatsoever whether direct, indirect, special or consequential resulting from the use of or reliance on any information contained or referenced herein.

Technical data contained in this document may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

Verizon and Verizon logos are trademarks of Verizon. Other product and brand names may be trademarks or registered trademarks of their respective owners.

Contents

What’s New with ThingSpace Manage 2.0 ..... 7

    Feature Summary ..... 7

    ThingSpace Services ..... 7

    ThingSpace APIs ..... 8

Accessing ThingSpace Manage ..... 9

    Site Stucture ..... 10

Header ..... 11

Left Navigation ..... 12

Content Area ..... 13

    Default Home Page ..... 13

    Favorites ..... 13

Support Options ..... 14

    Providing Feedback ..... 15

Verizon Applications ..... 16

    Profile Options ..... 16

    Sign out of the portal. .... 16

    Settings ..... 17

    Preferences ..... 17

    Application Settings ..... 18

Anomaly Detection ..... 19

Custom Fields ..... 20

    ID Formats ..... 21

    Service Plans ..... 21

Devices ..... 22

Searching for Devices ..... 24

    Performing a Bulk Search ..... 25

    Applying Filters ..... 26

    Sorting Data ..... 26

    Taking Actions ..... 27

    Provisioning Actions ..... 27

    Activating Devices in Bulk ..... 28

Quick Activations ..... 31

    Resubmit Orders ..... 32

Assigning Attributes and Saving Address locations ..... 33

Bulk Service Plan Changes ..... 34

Quick Service Plan Changes ..... 37

## ThingSpace Manage v2.0 – User Guide

---

Bulk Wireless Number Changes.....	39
Quick Wireless Number Changes .....	41
Suspending Devices in Bulk .....	42
Quick Suspending Devices .....	44
Resuming Devices in Bulk.....	45
Quick Resuming Devices.....	47
Swapping Devices in Bulk.....	48
Quick Swapping of Devices .....	50
Deactivating Devices in Bulk .....	51
Quick Deactivating Devices .....	54
Deleting Devices.....	56
Changing Cost Center Codes in Bulk .....	57
Quick Cost Center Code Changes .....	59
Changing Custom Fields in Bulk .....	60
Quick Custom Field Changes .....	62
Changing Device Groups in Bulk .....	64
Quick Device Group Changes .....	66
Sending an SMS.....	68
Reporting Actions.....	69
Location Actions.....	70
Creating a Geofence .....	71
View Location Console .....	74
View Location Report .....	75
SIM Secure Actions .....	76
Schedule Action.....	77
Create a campaign .....	78
Exporting Device Lists.....	79
Customizing Your View.....	80
Custom Views .....	81
Device Details.....	82
Device identity .....	83
Network.....	83
Provisioning.....	84
Service plan and billing .....	85
Attributes .....	86
Subscriptions .....	87
Location.....	88

Advanced diagnostics.....	89
Device Groups.....	90
Software Management .....	91
Searching for Software.....	93
Taking Actions .....	94
Create a campaign .....	94
Show legacy view .....	94
Software Details .....	95
Software Details .....	96
Eligible Devices.....	96
Subscriptions .....	97
User Management.....	98
Alerts.....	99
Searching Alerts .....	100
Applying Filters .....	100
Acknowledging Alerts.....	101
Campaigns.....	102
Search for Campaigns.....	103
Taking Actions.....	103
Deleting a Campaign.....	103
Campaign Details .....	104
Legacy View .....	105
Dashboards.....	106
Device Status Filters.....	107
Device Status Pod .....	108
Recent Alerts Pod .....	108
Recent Transactions Pod .....	109
Average Provisioning Time Pod.....	109
Analytics Dashboards.....	110
Filtering .....	110
To build a custom filter .....	110
Search .....	111
Export Data.....	111
Analytics Dashboard Views.....	111
Wireless Network Performance .....	116
Downloads.....	117
Logs.....	118
Searching Logs.....	119
Applying Filters .....	120



Taking Actions.....	121
Provisioning Actions .....	121
View Application Log .....	121
Download the Transaction Log .....	122
Log Details .....	122
Application Log.....	124
Reports.....	125
Running Select Reports.....	126
Running Advanced Reports .....	127
Aggregated Usage Report .....	128
Daily Usage Report.....	128
Connection History Report.....	129
Session History Report .....	130
Rated Unbilled Usage Report .....	131
Usage Anomaly Report .....	131
Usage Trending Chart.....	132
Cloud Connectors.....	133
Create a Stream .....	134
Using REST URL.....	135
Using Amazon Web Services .....	136
Using Microsoft Azure .....	138
Configure Devices .....	141
Additional Device Information .....	143
Device information.....	144
Configuration history .....	145
Device history .....	146
Geofences .....	147
Search for Geofences .....	148
Taking Actions.....	148
Edit a Geofence.....	149
Deleting a Geofence .....	150
Rules.....	151
Searching Rules .....	153
Applying Filters .....	153
Enable/Disable a Rule.....	154
Edit the Default Usage Alert Rule.....	154
Edit a Rule .....	155
Create a Rule.....	157
Rule Engine 2.0 for Real-Time Reporting (RTR).....	158
Usage Rule Example .....	161

---

User Quick Start Guide.....	166
For Network: .....	166
For Usage: .....	167
For Transactions:.....	171
Scheduled Reports.....	172
Run a Report.....	173
Edit a Scheduled Report.....	174
Delete a Scheduled Report.....	175
Frequently Asked Questions .....	176
Glossary .....	177
Appendix.....	179
Field Definitions.....	179
General .....	182
Location.....	186
Software.....	186

## What's New with ThingSpace Manage 2.0

We have rebuilt ThingSpace Manage from the ground up with a stylish user experience. ThingSpace Manage 2.0 offers enhancements to the capabilities you've grown accustomed to, and introduces many new features developed in response to your feedback. Go to the ThingSpace website [What's New](#) page for a complete list of these new features, and to stay informed of the latest ThingSpace Manage developments.

### Overview

ThingSpace Manage is Verizon's portal for managing Internet of Things (IoT) device connectivity on the Verizon Wireless network. IoT-specific connectivity management functions include viewing and monitoring connectivity status, data usage, dashboards, device lists, reports, and alerts. You can also use near real-time usage data to choose service plans, suspend devices, troubleshoot connectivity, and more.

This user guide provides a basic introduction to the ThingSpace Manage web portal and describes the types of features that are available to manage your IoT devices.

## Feature Summary

You can provision, monitor, and control service, connectivity, and device usage with ThingSpace. These capabilities include the following features:

- 24/7 access to activate, suspend, restore, or deactivate service, and adjust your IoT service plans.
- Real-time monitoring of connectivity, activity, and status from the system level down to the individual device. Real-time monitoring and control of devices, data usage, and costs.
- Device naming, grouping, and tracking by custom properties.
- Configurable notifications for provisioning events, maximum and minimum threshold violations, abnormal disconnects, unauthorized equipment relocations, and more.
- On-demand reports.
- The ability to detect an overly chatty device, and either suspend it or change its service plan. The ability to detect devices that fail to deliver data.
- Bulk and SKU-based operations.

## ThingSpace Services

ThingSpace Services is a suite of value-added utilities built on top of Verizon IoT Connectivity to build and manage IoT solutions easier. Verizon IoT Connectivity reduces the complexity of attaching an IoT device to a wireless network. ThingSpace Services build upon connectivity by offering additional services that can be applied to many devices (e.g., software updates, device diagnostics and device location). For more information about these subscription-based offerings, please visit the ThingSpace website [ThingSpace Services](#) page.

### ThingSpace APIs

The ThingSpace platform has rich features that can easily be integrated with enterprise applications using RESTful APIs. With this capability you can improve operational efficiencies by automating high-volume service provisioning, as well as monitoring and controlling wireless IoT devices.

Using the ThingSpace APIs, you can perform most of the same self-service tasks you take through the ThingSpace Manage portal. The Connectivity Management APIs allow you to integrate IoT connectivity management with your enterprise software systems, such as enterprise resource planning (ERP), supply chain, and customer service management. In this way, you can add, activate, monitor, and analyze your devices, as well as perform many other connectivity management tasks. For additional information about the APIs, please refer to the [ThingSpace API Documentation](#).

## Accessing ThingSpace Manage

You can log directly into ThingSpace Manage (<https://m2mdeveloper.verizon.com/>), or log in through My Business (<https://sso.verizonenterprise.com/amserver/sso/login.go>).

To access ThingSpace Manage, you need a My Business Account that is set up for M2M connectivity. The *Machine to Machine / ThingSpace Manage* checkbox must be checked in your My Business profile. Your account representative can set this up, or you can complete our [contact form](#).

### To access ThingSpace Manage from My Business


1. On the navigation menu, click **Manage Account**.
2. Select the **ThingSpace Manage** tab next to **Wireless & Mobility**.
3. Click the desired page to start in.

The ThingSpace Manage screen that appears after you log in depends on the [Default Landing Page](#) setting of your User Profile. Initially, the default landing page is *Dashboard*.



**Access rights** ⓘ

Select the entities to which you want to provide access for this user

Search 

---

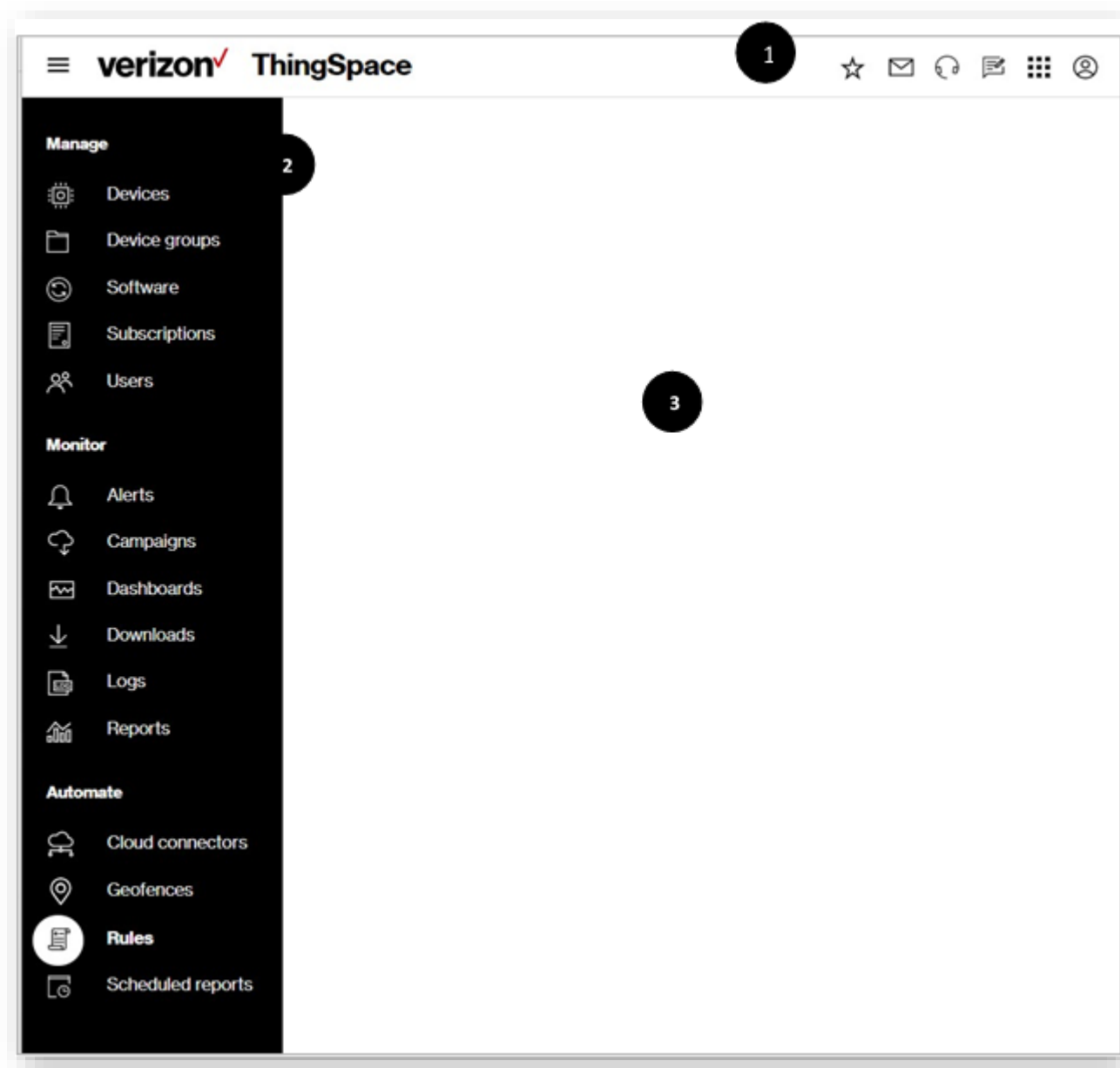
☐ Access rights ↓

---

☒ Machine to Machine / ThingSpace Manage

## Site Structure








The site structure consists of a [header](#) (1), [left navigation](#) (2), and a [content area](#) (3).



# Header

The header appears at the top of every page and contains the following elements.

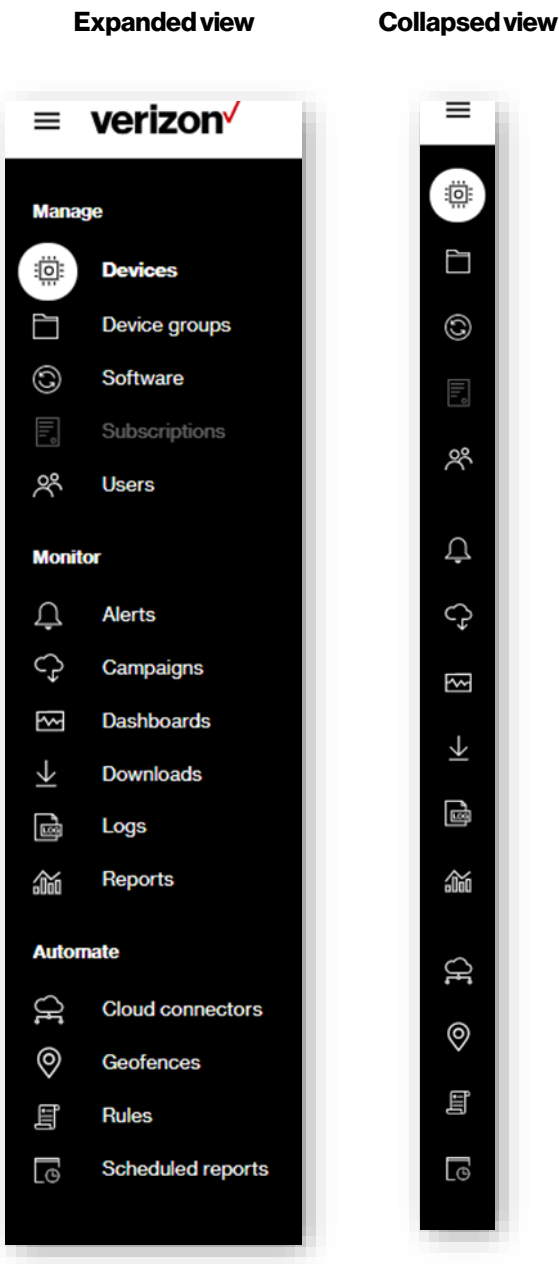


Elements on the header		
1		<a href="#">Left Navigation</a> – Expand or collapse the left pane with links to various application pages.
2		<a href="#">ThingSpace</a> – Open the default home page.
3		<a href="#">Favorites</a> – Open the Favorite links menu.
4		Envelope – Open a coming soon tooltip for an upcoming Message center.
5		<a href="#">Support</a> – Open the Support menu.
6		<a href="#">Feedback</a> – Open the Feedback form where you can tell us about your experience.
7		<a href="#">Verizon Apps</a> – Open a list of Verizon applications to open.
8		<a href="#">Profile</a> – Open the Profile menu.

# Left Navigation

The left navigation is used to move around the website. From here, click any link to access the corresponding page within the portal.

Your user role determines what displays on the left navigation and may differ between users with alternative roles. You can see your role in the profile menu.





## Content Area

The content area contains the primary web page. The side navigation links take you to different pages that render in the content area. The content area for every page is different, but follows certain guidelines.

The content area contains the following common features:

**Breadcrumb** – This is a secondary navigation that reveals the website location hierarchy. The breadcrumb is located at the top-left of every page and provides links to preceding levels of the hierarchy.

**Page title** – This is the page name you are on and is found just beneath the Breadcrumb links.

**Action icons** – These are interactive graphics that provide various page functions. Each page has a unique set of actions for completing specific tasks on the page. Hover over each icon to view a tooltip description. Click an icon to initiate the action.




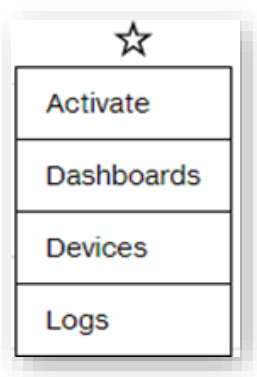
## Default Home Page

Click the **ThingSpace** icon open the default landing page (or home page). The home page defaults to the Dashboards page unless it is changed in [Settings](#).

**COMING SOON:** The ability to set your own default home page.

## Favorites

The favorites icon  displays a menu containing links to your most used functions. Set your favorite links in [Settings](#). Currently, these links are preset, but will be customizable in an upcoming release.

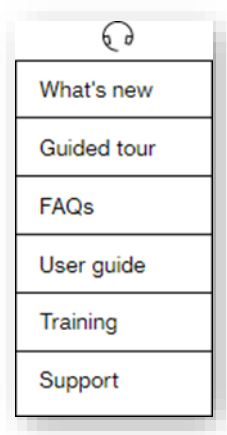


**COMING SOON:** The ability to set your favorite links.


## Support Options

The support icon  displays a menu containing links to:

- Learn what is new or changed in ThingSpace Manage.
- Take a guided video tour of the new 2.0 experience.
- Review [Frequently Asked Questions](#).
- View or download this user guide.
- Check the training schedule and register for a class.
- View how to get support.



## Providing Feedback

Click the feedback icon  at the top of any page to tell us about your experience. Select an overall rating with the level of satisfaction you experienced with the website. Fill out any of the other questions available and click **Submit**. We review all feedback and contact any users requesting a follow-up.

verizon

ThingSpace

Overall, how satisfied are you with the website?

Dissatisfied

Satisfied

What was the main purpose for your visit today?


Please Select Option

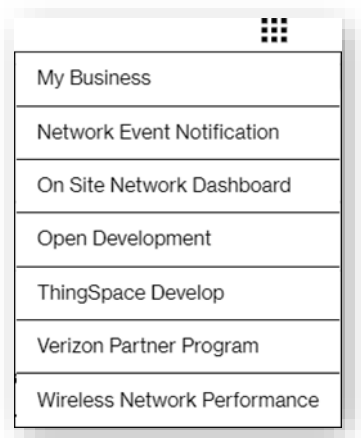
Close

Submit


Powered by Medallia

## Verizon Applications

Click the Verizon apps icon  to open other Verizon applications. A selected application opens in a new tab.

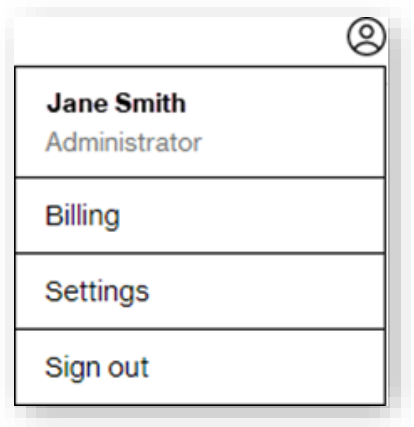


## Profile Options

The user profile icon  displays a menu of links that you can use to: View the name and role of the user that is currently logged in.

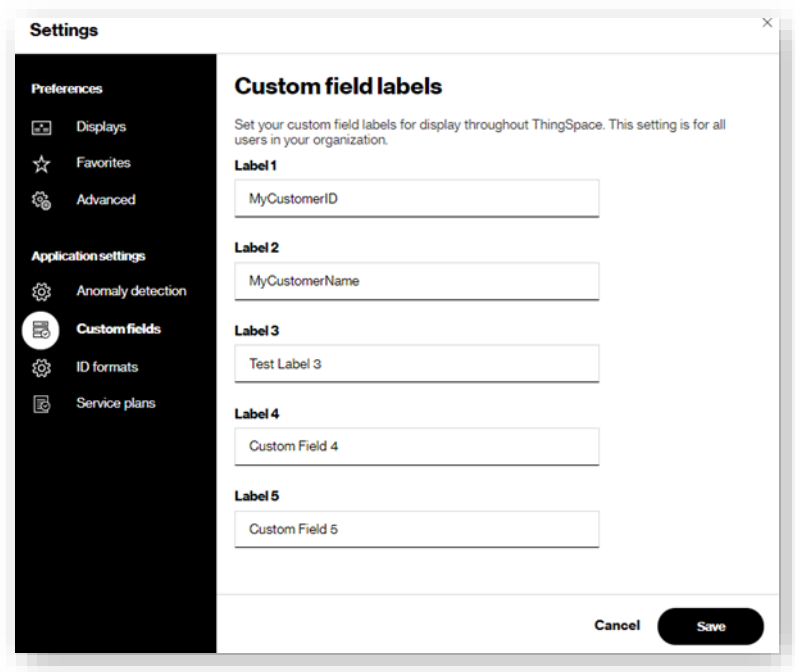
Go to My Business to view your bill. View user and application settings

## Sign out of the portal.



## Settings

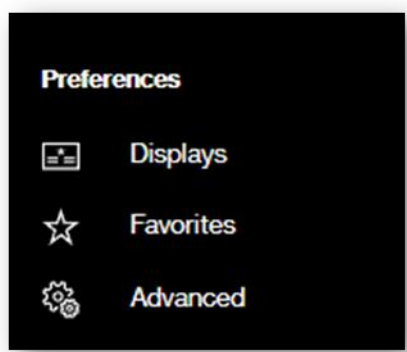
Manage user preferences and application settings here. Click the side navigation to access each section.



**NOTE:** Only users with an Administrator role can revise application settings.

## Preferences

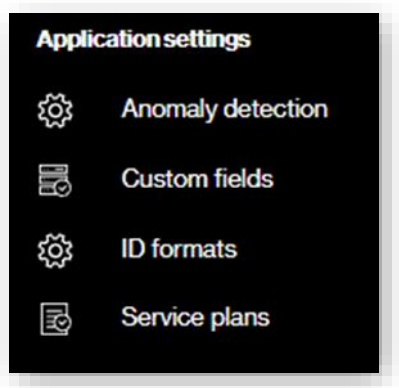
Preferences are *user-specific* settings that allow you to customize the portal to your unique choices. Currently, the **Displays** page supports the setting of a light or dark display mode



**COMING SOON:** The ability add preferred links to your [Favorites](#) menu and set advanced customizations.

## Application Settings

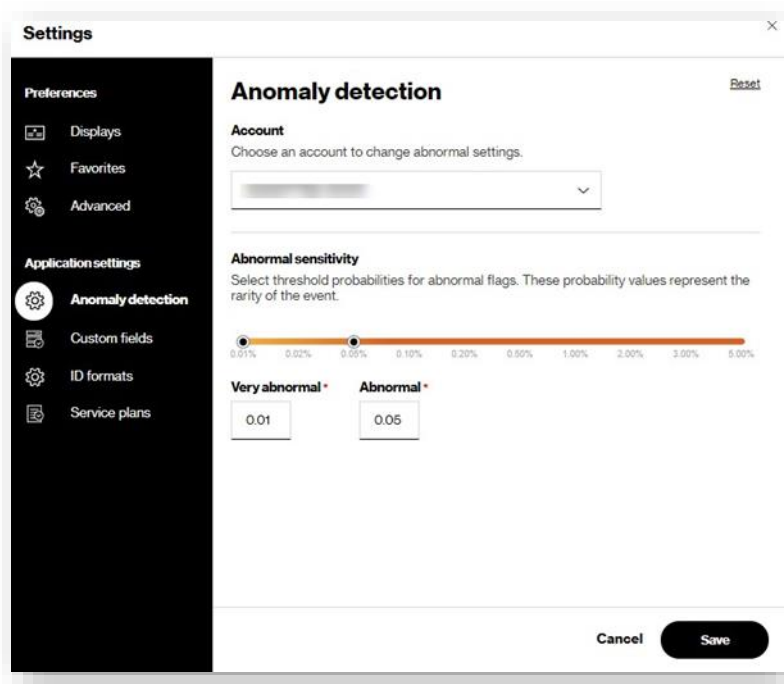
Application settings allow Administrators to set certain attributes that apply across the portal. Changes to application settings impact all users.



## Anomaly Detection

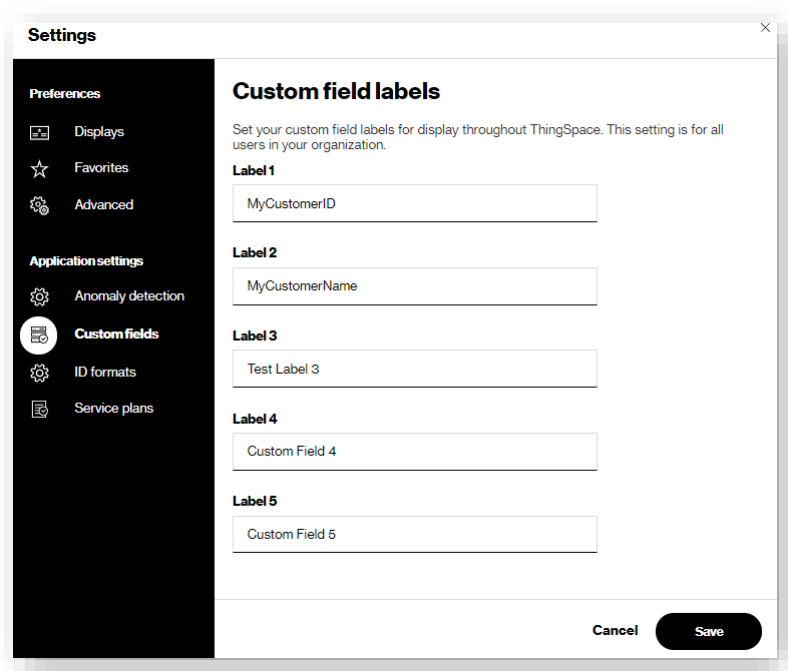
For users subscribed to the ThingSpace premium Intelligence bundle, use the *Anomaly detection* settings to set sensitivity thresholds. Anomaly detection uses machine learning to classify and cluster different devices on your account and alert you for unusual behavior in the device data usage patterns. The unusual alert or event is based on the sensitivity to which you would classify this as anomalous or not. You can set anomaly detection thresholds at the account level.

Each anomaly alert has a rarity score. The rarity score setting allows you to define what is considered “abnormal” and what is “very abnormal” in the context of the billing account. These definitions are used in the analytics dashboard, reports and rules.



# Custom Fields

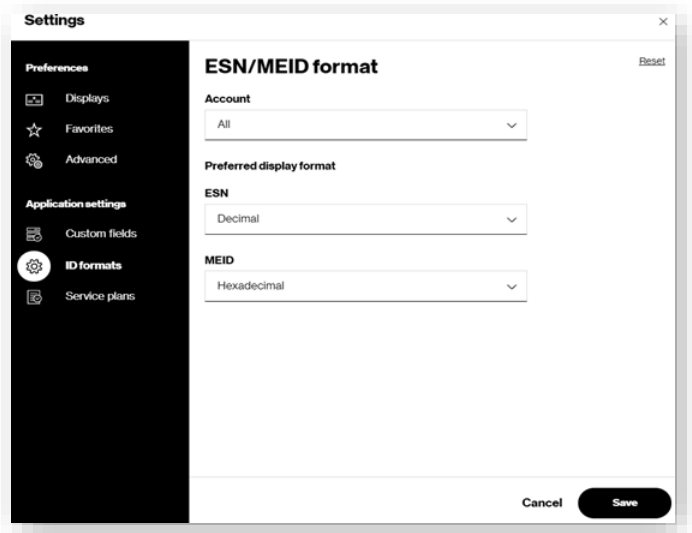
Use the *Custom fields* settings to name the fields you add, which display throughout your application. These custom fields are available for you to use to set values for your devices and use in any way you like. You can set the value of the custom fields at any time or set them when activating your devices. These labels are also available as columns in the devices list so that you can add them to any of your custom table views.





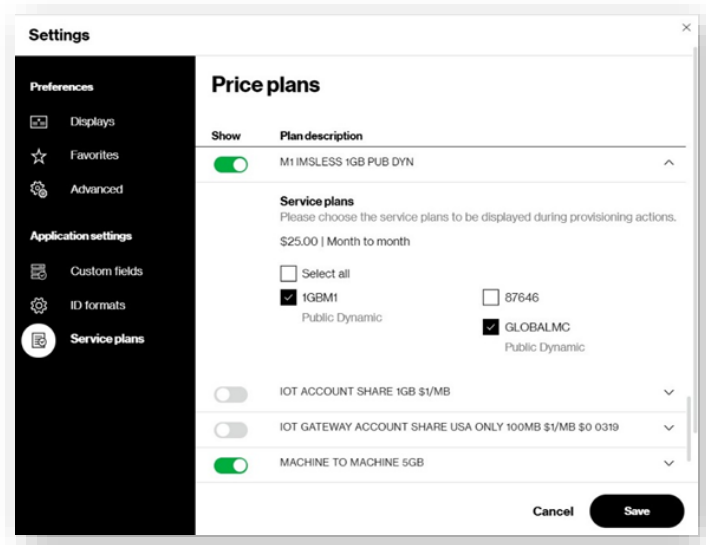
## ID Formats

Use *ID Formats* to choose how you want your device ESN/MEIDs to be displayed in the portal and reports. The available formats are *Decimal* and *Hexadecimal*. You can mix formats across accounts, or keep them the same for all. Once saved, these formats are used throughout the portal and reports that contain those fields.



## Service Plans

Use *Service Plans* to view the service plans for each price plan and to show/hide them in the list while taking provisioning actions.



To hide a price plan completely, toggle *Show* to off so that it appears gray. To show the price plan, toggle *Show* to on so that it appears green. To hide a service plan, open the price plan panel by clicking the down arrow. This shows all the service plans that belong to the price plan. Then, check on those to be display. Only those that are checked are displayed during provisioning actions.

# Devices

The *Devices* page is the primary place for managing your devices. It displays a list of the devices you have access to view. You can perform searches and filter your device list. From this page, you can also run reports and take a variety of actions on your devices.

On the side navigation, click **Devices** to open the page. The [action icons](#) apply to all devices, or only to selected devices.

Manage

Devices

Device groups

Software

Subscriptions

Users

Monitor

Alerts

Campaigns

Dashboards

Downloads

Logs

Reports

Automate

Cloud connectors

Geofences

Rules

Scheduled reports

Manage > Devices

Devices

1

3-10

2

11

12

Search by IMEI, ICCID, MDN, or IP Address

Bulk search

62,421 Results












Filter

AccountView

	Device identifier	Account	MDN/MSISDN	IP address	Device status	Connection
<input type="checkbox"/>					Active	Connected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Suspend	Disconnected
<input type="checkbox"/>				0.0.0.0	Suspend	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Suspend	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected
<input type="checkbox"/>				0.0.0.0	Suspend	Disconnected
<input type="checkbox"/>				0.0.0.0	Active	Disconnected

Show 100 per page

1 2 624 625

Elements on the Devices page					
1		<a href="#">Search</a> – Locate a specific device.	2.		<a href="#">Bulk search</a> – Locate up to 500 devices at once.
3		<a href="#">Actions</a> – Open a menu of options.	4		<a href="#">Reports</a> – Manage device reports.
5		<a href="#">Location</a> – Subscribers can take location actions, such as enable or disable location updates.	6		<a href="#">Security</a> – Subscribers can manage SIM Secure Services
7		<a href="#">Schedule</a> – Automate a report.	8		<a href="#">Campaign</a> – Create a strategy for updating device firmware or software.
9		<a href="#">Download</a> – Export listed device information.	10		Reload – Refresh the page with new data.
11		<a href="#">Filter</a> – Limit the list to devices with specific attributes.	12		<a href="#">Table view</a> – Customize your view.

## Searching for Devices

The *Devices* page contains a *Search* field to locate device data by IMEI, ICCID, MDN, or IP address (up to 500 devices). Wildcard (%) search is supported for all Device IDs.



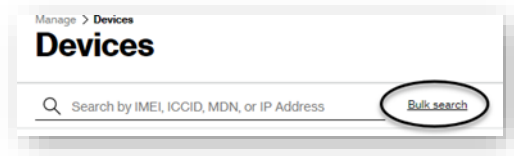
**NOTE:** Search does not support wildcards for IP address. You must search for the exact IP address.

## Performing a Bulk Search

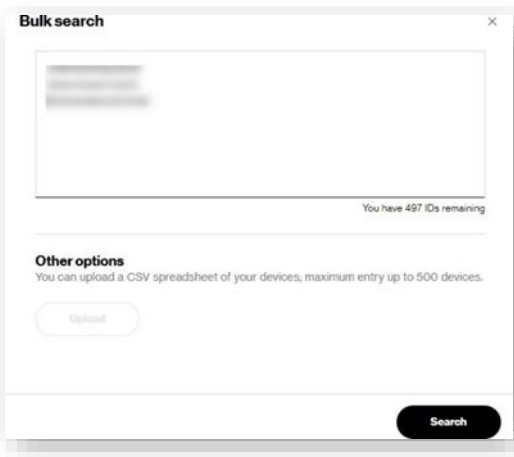
You can search for up to 500 devices at a time using the Bulk search link.

To bulk search

On the left navigation, click **Devices**. The *Devices* page opens.



1. Click **Bulk search**: The Bulk search dialog opens.



2. In the *Bulk search* field, type up to 500 MDNs, IMEIs, ICCIDs, or IP addresses separated by commas, or list one per line. Alternatively, click Upload under Other options to import a Comma Separated Values (CSV) file containing up to 500 device IDs.
3. In the dialog that appears, navigate to the CSV file.
4. Select the file and click **Open**.
5. Click **Search** to invoke the search function.



**COMING SOON:** The ability to search for even more devices at one time! This feature will submit the search in the background while you continue working. When the search is complete, your search results will be available in the [Downloads](#) center.

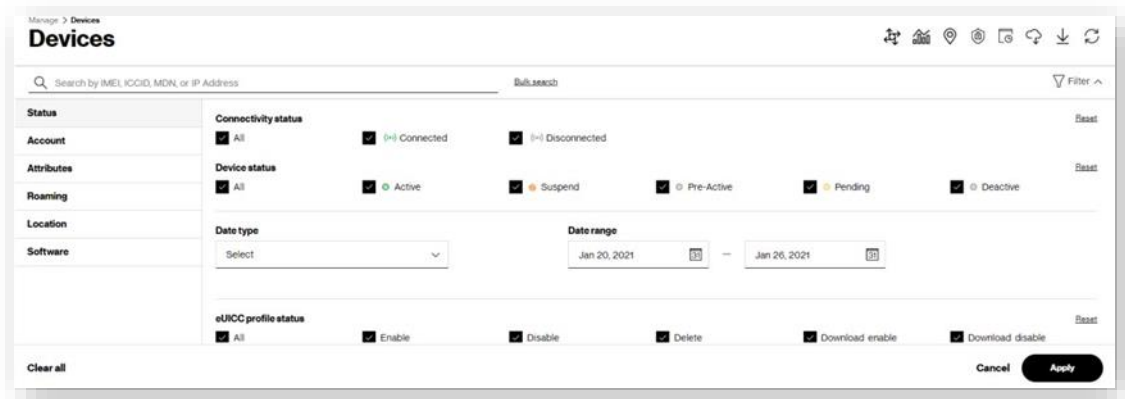
## Applying Filters

Use filters to view a limited set of devices by specific attributes such as: **Connectivity status**, **Device status**, **Date type**, **Date range**, and others. Select from the following filter categories on the left:

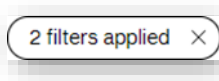
Status Account Attributes Roaming Location Software.

### How to apply filters

1. On the left navigation, click **Devices**. The *Devices* page opens.
2. Click the filter icon  **Filter** . The following filters screen appears.





3. Click each tab or scroll through the list to view all available filters. Select the desired filters to apply and click **Apply**.
4. The **Reset** link of each filter category allows you to select all filters in the category with one click.
5. To apply the selected filters, click **Apply**. A filters applied count appears next to the drop-down menu.



**NOTE:** For a device to appear on the *Devices* page, it must match **all** of the selected filter criteria. This means that you can apply additional filters to shorten the filter results.

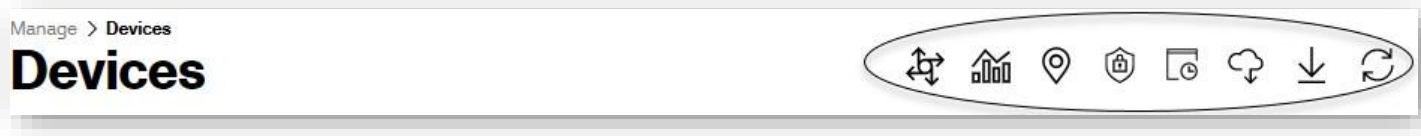
**COMING SOON:** The ability to save filters!

## Sorting Data


You can sort data by clicking the sort icon next to the column name. If sort is enabled for a column, click on the sort icons to sort in ascending  or descending  order.

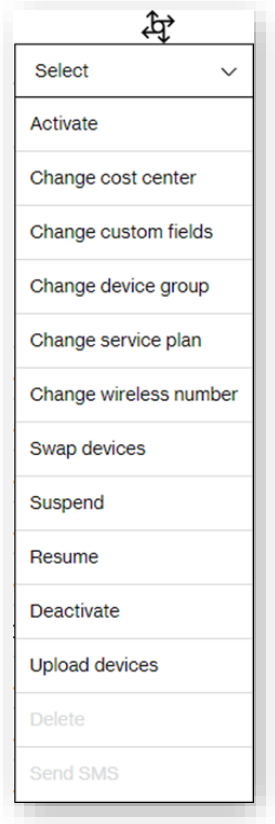
## Taking Actions

The *Devices* page offers a set of icons to apply various actions to your devices. Not all of the icons appear for all customers. Some icons appear only if you subscribe to value added ThingSpace Services, such as Location Services, SIM Secure, or Software Management.



## Provisioning Actions

The actions icon  displays a drop-down menu with a list of actions. The majority of these are provisioning actions, such as activate, change service plan, change wireless number, suspend, resume, swap, deactivate, and delete devices. The other actions allow you to make changes to cost center codes, custom field values, and device groups, as well as send an SMS messages to your devices.




There are two types of actions that you can take:

- **Bulk actions** – Take actions on a list of devices that you enter manually or upload from a file.
- **Quick actions** – Take actions on devices selected from the devices list.

# Activating Devices in Bulk

## How to activate devices in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

- 1. With no devices selected, click the actions icon  and select **Activate**. The *Activate* page opens.

Manage > Devices > Activate

Cancel

Activate

Let's activate your devices.

Select activation type

Please select an activation type and options. This helps determine what parameters you'll need to enter below.

☒ Device and SIM

☐ Device only (embedded SIM)

☐ SKU and SIM

Select additional options

Please enter any required fields. Select available options if you would like to add them to your activation.

☐ IP Address

☐ Upload to Verizon

Enter devices

You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.


For the manual option, enter up to 10,000 device IDs for activation, one device per line. For 4G activations, enter IMEI (device ID) and ICCID (SIM ID), separated with a comma.

Example format:  
IMEI, ICCID  
IMEI, ICCID

You have 10,000 remaining.

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 10,000 lines per spreadsheet order. You can include many activation parameters directly in your file upload. Explore the options when you [create and download](#) a template data entry file.

Upload

 activation\_template.xlsx ×

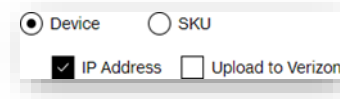
Next

28



2. Select the type of activation (Device or SKU).

For *Device activations*, type a list of IMEI and/or ICCIDs separated by commas. If you choose the IP Address checkbox, include the IP Address for each device. If you choose the checkbox to **Upload to Verizon**, you must provide the Verizon SKU and email address that's associated with the user's Open Development account.



A screenshot of a form with two radio buttons: 'Device' (selected) and 'SKU'. Below them are two checkboxes: 'IP Address' (checked) and 'Upload to Verizon' (unchecked).

For *SKU*, type the Verizon SKU ID and then enter the list of ICCIDs.

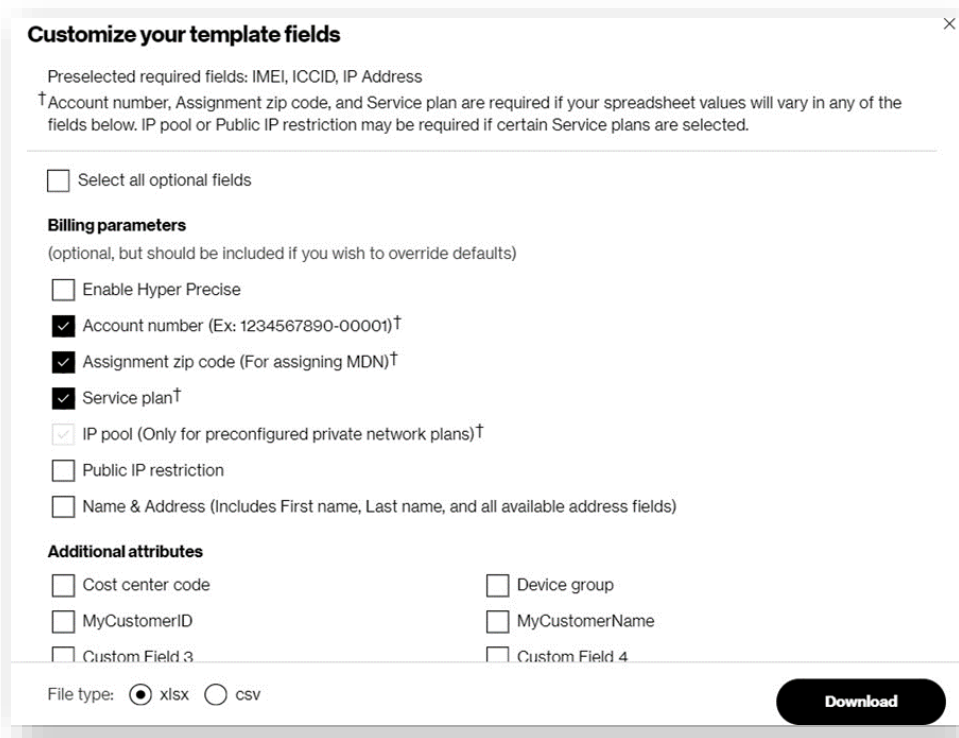


A screenshot of a form with two radio buttons: 'Device' (unchecked) and 'SKU' (selected). To the right of the 'SKU' button is a text input field containing 'SKU for all devices'.

Type the device identifiers manually or upload a file of up to 10,000 devices.

To upload a file, click create and download to select the parameters to use in creating a dynamic template for entering your data. You can select any or all of the available fields on the screen below.

*Account*, *Service plan*, and *Assignment zip code (mdnZipCode)* are all required fields when entering different device attributes to the template.

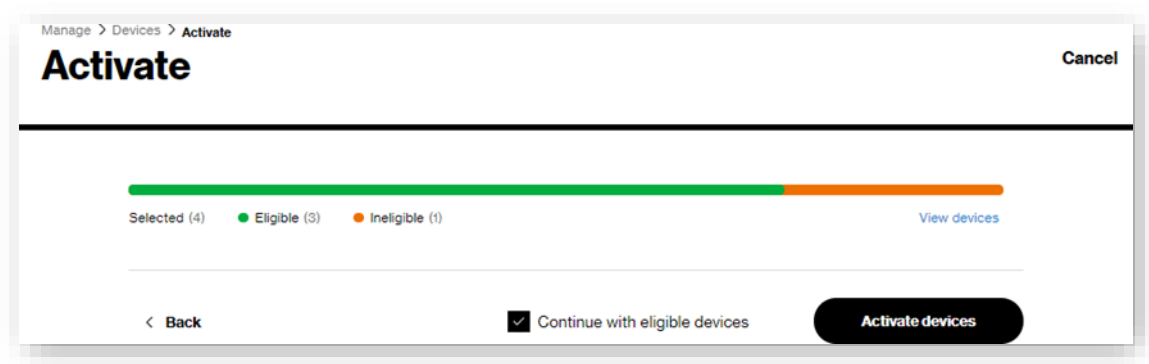


A screenshot of a dialog box titled 'Customize your template fields'. It contains the following sections:

- Preselected required fields:** IMEI, ICCID, IP Address
- † Account number, Assignment zip code, and Service plan are required if your spreadsheet values will vary in any of the fields below. IP pool or Public IP restriction may be required if certain Service plans are selected.**
- Select all optional fields:** (checkbox)
- Billing parameters** (optional, but should be included if you wish to override defaults):
  - Enable Hyper Precise (checkbox)
  - Account number (Ex: 1234567890-00001)† (checkbox, checked)
  - Assignment zip code (For assigning MDN)† (checkbox, checked)
  - Service plan† (checkbox, checked)
  - IP pool (Only for preconfigured private network plans)† (checkbox, checked)
  - Public IP restriction (checkbox)
  - Name & Address (Includes First name, Last name, and all available address fields) (checkbox)
- Additional attributes:**
  - Cost center code (checkbox)
  - MyCustomerID (checkbox)
  - Custom Field 3 (checkbox)
  - Device group (checkbox)
  - MyCustomerName (checkbox)
  - Custom Field 4 (checkbox)
- File type:** ☒ xlsx ☐ csv
- Download** button

- a. Click **Download** to download the customized template.
- b. Add your data to the template file and save. You can have different values for each column in the template.
- c. Click **Upload** to complete the upload process.

- 3. On the Activate page, click **Next**. The second *Activate* page opens.



Review device eligibility. To view the list of the devices and any associated error messages, click **View devices**. The *Eligibility details* dialog opens.

The screenshot shows the 'Eligibility details' dialog box, which displays 4 results in a table. The table has the following columns: IMEI, ICCID, Eligibility, and Message. The data rows are as follows:

IMEI	ICCID	Eligibility	Message
[Redacted]	[Redacted]	Eligible	
[Redacted]	[Redacted]	Eligible	
[Redacted]	[Redacted]	Eligible	
[Redacted]	[Redacted]	Ineligible	Device/SIM not found in DMD.


- 4. Review **Continue with eligible devices** for ineligible devices to proceed.
- 5. Click **Activate devices** to submit the activation order.

## Quick Activations

Activate multiple devices using default values in just one click.

How to activate devices quickly

On the left navigation, click **Devices**. The *Devices* page opens.

- 1. Select devices using the *Device identifier* checkbox.
- 2. Click the actions icon  and select **Activate**. A review page opens.

Please review and you are all set to activate devices!

Selected (3)

Eligible (2)

Ineligible (1)

View devices

Billing account \*

Select the account number you wish to be billed.

Add more information

Assignment zip code \*

Type the MDN zip code.

07920

Service plan

All

Private dynamic

Private static

Public dynamic

Public static

Setup5GB

Machine to machine 5GB

Month to month

Private Static

See plan details

Setup10GB

Machine to machine 10GB

Month to month

Private Static

See plan details

85695

Machine to machine 10GB

24 months

Private Static

See plan details

86562

Mobile broadband M2M

24 months

Private Static

See plan details

☒ Continue with eligible devices

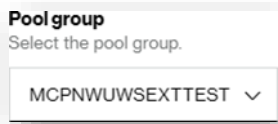
Submit

- 3. Review eligible and ineligible device counts.
- 4. Review the **Billing account** and **assignment zip code**, revising them if necessary. The zip code determines the MDN assigned to your devices when activated.

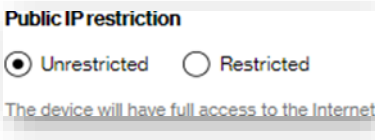
31

- 5. Assign a **Service plan** to the devices. You can filter the service plans by clicking on **Private dynamic**, **Private static**, **Public dynamic**, and **Public static**.

For private network plans, if the selected service plan has associated IP pools, the Pool group section displays to select the IP Pool group. The devices are assigned IP addresses from within the selected IP pool group.




For public static plans, you can choose the type of restriction to apply. Unrestricted IPs provide full access to the Internet. Restricted IPs have limited access to content provided by Verizon Wireless and are restricted from accessing the Internet.



- 6. Click **Add more information** to set additional details, such as *Device Groups*, *Custom Fields*, or *Cost Center*.

Resubmit Orders

If an activation order fails, users have the option of clicking the actions icon  and selecting “Resubmit activation”:

verizon ThingSpace

Company : MCPPNWUWSEXTTEST

Dashboards

Manage

Monitor

Monitor > Logs > ef8dc64d-5d73-4c39-a328-5a77db595191

Log details

Failure Activation

Resubmit activation

Service plan

Unknown

Submitted by

Public Network

Submitted date

08/22/2023 01:34:01 PM

Request ID

ef8dc64d-5d73-4c39-a328-5a77db595191

Submitted

1

Success

0

Pending

0

Failed

1

Search by Device ID or MDN

1 Results

Device identifier

ICCIDIMEIMDN/MSISDNIP addressStatusDescription

ef8dc64d-5d73-4c39-a328-5a77db595191

ef8dc64d-5d73-4c39-a328-5a77db595191ef8dc64d-5d73-4c39-a328-5a77db595191ef8dc64d-5d73-4c39-a328-5a77db595191ef8dc64d-5d73-4c39-a328-5a77db595191FailureYour request failed due to an internal system e...

## Assigning Attributes and Saving Address locations

To assign attributes and save address locations

On the left navigation, click **Devices**. The *Devices* page opens.

1. Click **Add more information** to open an additional section where you can enter other details, such as First name, Last name, Address, Device group, Cost center code, and Custom Fields. You can also select from a list of **Saved locations**, or click **Add** to save the entered location. The *Add* function becomes available after you provide a name for the **Saved location name**.



2. Check **Continue with eligible devices** if necessary to proceed.

**Please review and you are all set to activate devices!**

**Saved location**

Select

**First name \***

Jane

**Address 1 \***

1 Verizon Way

**City \***

Basking Ridge

**Last name \***

Doe

**Address 2**

**State \***

New Jersey

**Zip code \***

07920

**Saved location name**

Work

Add

3. Click **Submit** to complete the device activation.

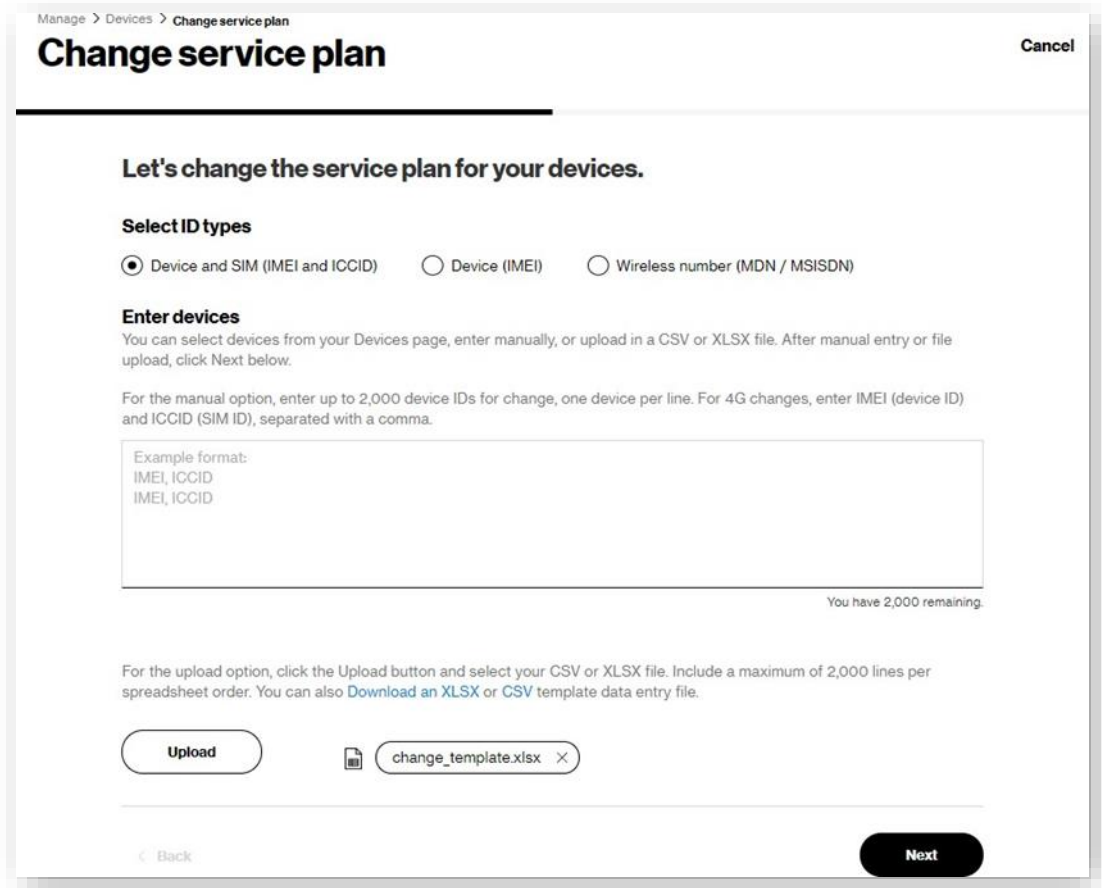
33

## Bulk Service Plan Changes

### How to change service plans in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon , and select **Change service plan**. The *Change Service Plan* page opens.



Manage > Devices > Change service plan

### Change service plan

Cancel

**Let's change the service plan for your devices.**

**Select ID types**

☒ Device and SIM (IMEI and ICCID) ☐ Device (IMEI) ☐ Wireless number (MDN / MSISDN)

**Enter devices**



You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.

For the manual option, enter up to 2,000 device IDs for change, one device per line. For 4G changes, enter IMEI (device ID) and ICCID (SIM ID), separated with a comma.

Example format:  
IMEI, ICCID  
IMEI, ICCID

You have 2,000 remaining.

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

**Upload**  change\_template.xlsx 

[Back](#) **Next**

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data to the template file and save.
  - c. Click **Upload** to complete the upload process.

4. On the *Change service plan* page, click **Next**. The second *Change service plan* page opens.

Manage > Devices > Change service plan

## Change service plan

Cancel

Please review and you are all set to change your service plan!

Selected (3) Eligible (1) Ineligible (2) [View devices](#)

Effective date

☒ Today ☐ Backdate

Service plan

All Private dynamic Private static Public dynamic **Public static**

**Setup5GBPubStat**

Machine to machine 5GB

Month to month  
Public Static

[See plan details](#)

Public IP restriction

☒ Unrestricted ☐ Restricted

The device will have full access to the Internet.

☒ Continue with eligible devices

**Submit**

[< Back](#)

5. Review eligible or ineligible device counts. To view the list of the devices and any associated error messages, click **View devices**. The Eligibility details dialog opens.

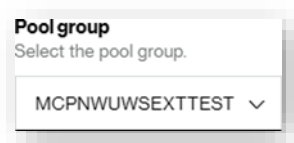
IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is not active.
[REDACTED]	[REDACTED]	Ineligible	Identifiers do not match records.

6. Select the **Effective date**. You can select today's date, or backdate it so that the plan change takes effect at the beginning of the billing cycle.
7. Assign a **Service plan** to the devices. You can filter the service plans by clicking **Private dynamic**, **Private static**, **Public dynamic**, and **Public static**.

## ThingSpace Manage v2.0 – User Guide

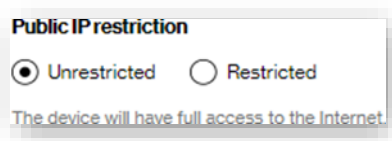
---

For private network plans, if the selected service plan has associated IP pools, the Pool group section displays to select the IP Pool group for the devices. The devices are assigned IP addresses from within the selected IP pool group.



A screenshot of a web form element titled "Pool group" with the instruction "Select the pool group." Below the text is a dropdown menu showing the selected value "MCPNWUWSEXTTEST" followed by a downward arrow.

For public static plans, you can choose the type of Public IP restriction to apply. Unrestricted IPs provide full access to the Internet. Restricted IPs only have access to content provided by Verizon Wireless and are restricted from accessing the Internet.



A screenshot of a web form element titled "Public IP restriction". It contains two radio button options: "Unrestricted" (which is selected) and "Restricted". Below the radio buttons, there is a line of text: "The device will have full access to the Internet."

8. Check **Continue with eligible devices** if necessary to proceed.
9. Click **Submit** to complete the process.



## Quick Service Plan Changes

### How to make quick plan changes on selected devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select devices using the *Device identifier* checkbox.

**NOTE:** All selected devices must be from the same billing account.

2. Click the actions icon , and then select **Change service plan**. A review page opens.

Please review and you are all set to change your service plan! ×

Selected (3)

Eligible (2)

Ineligible (1)

[View devices](#)

Effective date

☒ Today

☐ Backdate

Service plan

All

Private dynamic

Private static

Public dynamic

**Public static**

5GBPubStatic

Machine to machine 5GB

Month to month

Public Static

[See plan details](#)

Public IP restriction

☒ Unrestricted

☐ Restricted

The device will have full access to the Internet.

☒ Continue with eligible devices

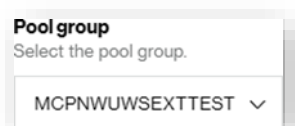
**Submit**

3. Review eligible and ineligible device counts.
4. Select the **Effective date**. You can select today's date, or backdate it so that the plan change takes effect at the beginning of the bill cycle.
5. Assign a **Service plan** for the devices. You can filter the service plans by clicking **Private dynamic**, **Private static**, **Public dynamic**, and **Public static**.

## ThingSpace Manage v2.0 – User Guide

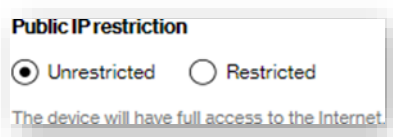
---

For private network plans, if the selected service plan has associated IP pools, the Pool group section displays to select the IP Pool group. The devices are assigned IP addresses from within the selected IP pool group.



A screenshot of a web form element titled "Pool group" with the instruction "Select the pool group." Below the text is a dropdown menu showing the selected option "MCPNWUWSEXTTEST" followed by a downward arrow.

For public static plans, you can choose the type of Public IP restriction to apply. Unrestricted IPs provide full access to the Internet. Restricted IPs only have access to content provided by Verizon Wireless and are restricted from accessing the Internet.




A screenshot of a web form element titled "Public IP restriction". It contains two radio button options: "Unrestricted" (which is selected) and "Restricted". Below the radio buttons, there is a line of text: "The device will have full access to the Internet."

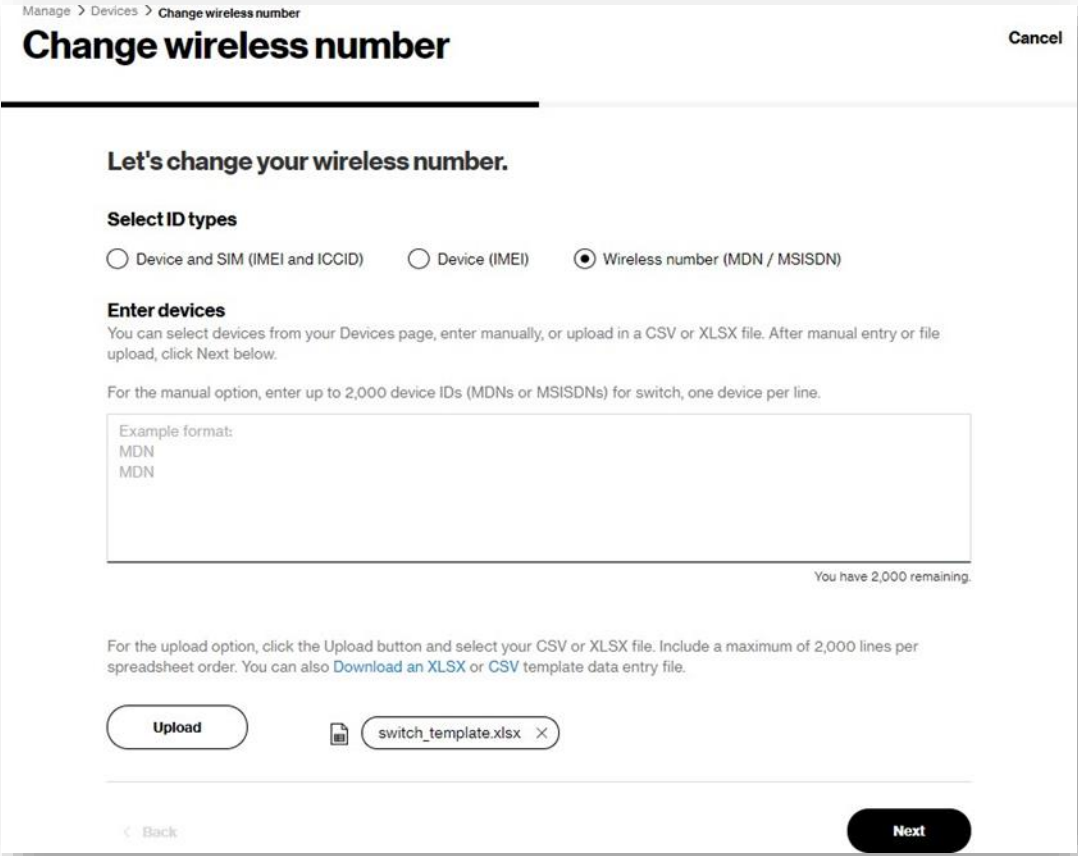
6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

## Bulk Wireless Number Changes

### How to change wireless numbers in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon , and then select **Change wireless number**. The *Change wireless number* page appears:



Manage > Devices > Change wireless number

**Change wireless number** Cancel

**Let's change your wireless number.**

**Select ID types**

☐ Device and SIM (IMEI and ICCID) ☐ Device (IMEI) ☒ Wireless number (MDN / MSISDN)

**Enter devices**

You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.


For the manual option, enter up to 2,000 device IDs (MDNs or MSISDNs) for switch, one device per line.

Example format:

MDN  
MDN

You have 2,000 remaining.

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

 switch\_template.xlsx

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** link to download the template.
  - b. Add your data to the template file and save.
  - c. Click **Upload** to complete the upload process.

4. Click **Next**. The Change wireless number page opens.

Manage > Devices > Change wireless number

## Change wireless number

Cancel

Please review and you are all set to change your wireless number!

Selected (3) ● Eligible (1) ● Ineligible (2) [View devices](#)

**Assignment zip code**

07920

The assignment zip code will be used to derive a new wireless number for each eligible device.

☒ Continue with eligible devices **Submit**

[< Back](#)

5. Review eligible and ineligible device counts. To view the list of devices, click **View devices**. A popup appears with the Eligibility details.

Eligibility details

3 Results

IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is not active.
[REDACTED]	[REDACTED]	Ineligible	Identifiers do not match records.

6. Select the **Assignment zip code**. The assignment zip code determines the wireless number for each eligible device.
7. Check **Continue with eligible devices** if necessary to proceed.
8. Click **Submit** to complete the bulk change number process.

## Quick Wireless Number Changes


### How to make quick MDN changes on selected devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select devices using the *Device identifier* checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon  , and then select **Change wireless number**. A review page opens.



**Please review and you are all set to change your wireless number!** ×

Selected (3) ● Eligible (2) ● Ineligible (1) [View devices](#)

**Assignment zip code**

07920

The assignment zip code will be used to derive a new wireless number for each eligible device.


☒ Continue with eligible devices **Submit**

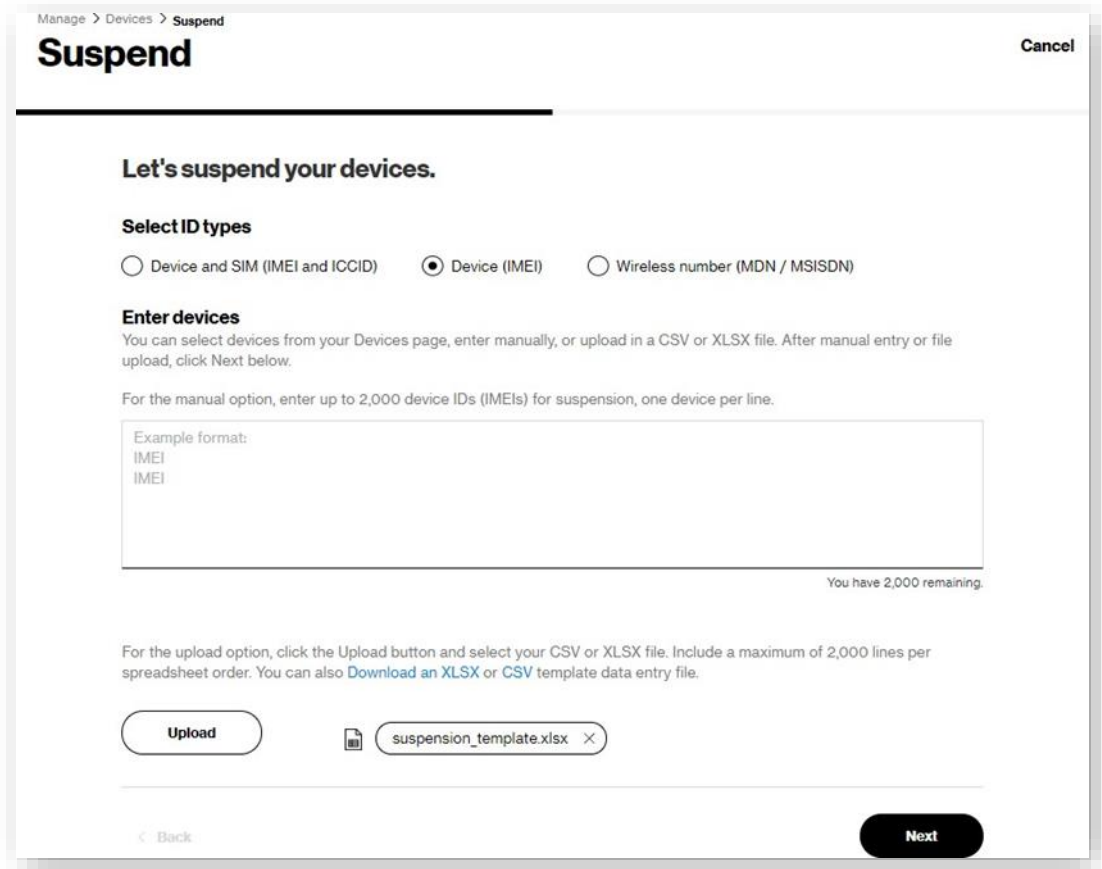
3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Enter the **Assignment zip code**. The assignment zip code determines the wireless number for each eligible device.
5. Check **Continue with eligible devices** if necessary to proceed.
6. Click **Submit** to complete the process.

## Suspending Devices in Bulk

### How to suspend devices in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon , and then select **Suspend**. The *Suspend* page opens.



Manage > Devices > Suspend

### Suspend

Cancel

**Let's suspend your devices.**

**Select ID types**

☐ Device and SIM (IMEI and ICCID) ☒ Device (IMEI) ☐ Wireless number (MDN / MSISDN)

**Enter devices**

You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.

For the manual option, enter up to 2,000 device IDs (IMEIs) for suspension, one device per line.

Example format:

IMEI  
IMEI

You have 2,000 remaining.

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

Upload

suspension\_template.xlsx

Back Next

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click the **Download an XLSX or CSV** link to download the template.
  - b. Add your data to the template file and save.
  - c. Click **Upload** to complete the upload process.

4. Click **Next**. The *Suspend* page opens.

Manage > Devices > Suspend

**Suspend** Cancel

Please review and you are all set to suspend devices!

Selected (3) Eligible (2) Ineligible (1) [View device](#)

**Reason for suspension\***

Seasonal / Vacation (SV) ☐ Suspend with billing

**NOTE:** Your order will be submitted as a suspend without billing unless you select the Suspend with billing option.

☒ Continue with eligible devices Submit

[< Back](#)

5. Review the eligible or ineligible devices. To view the list of devices, click **View devices**. The *Eligibility details* dialog opens.

**Eligibility details** ×

2 Results

IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is not active.

6. Select a **Reason for suspension**. Available reason codes are:
- Lost / Stolen (21)
  - Seasonal / Vacation (SV)
7. Check **Suspend with billing**. If not checked, the devices are suspended without billing.
8. Check **Continue with eligible devices** if necessary to proceed.
9. Click **Submit** to complete the process.


## Quick Suspending Devices

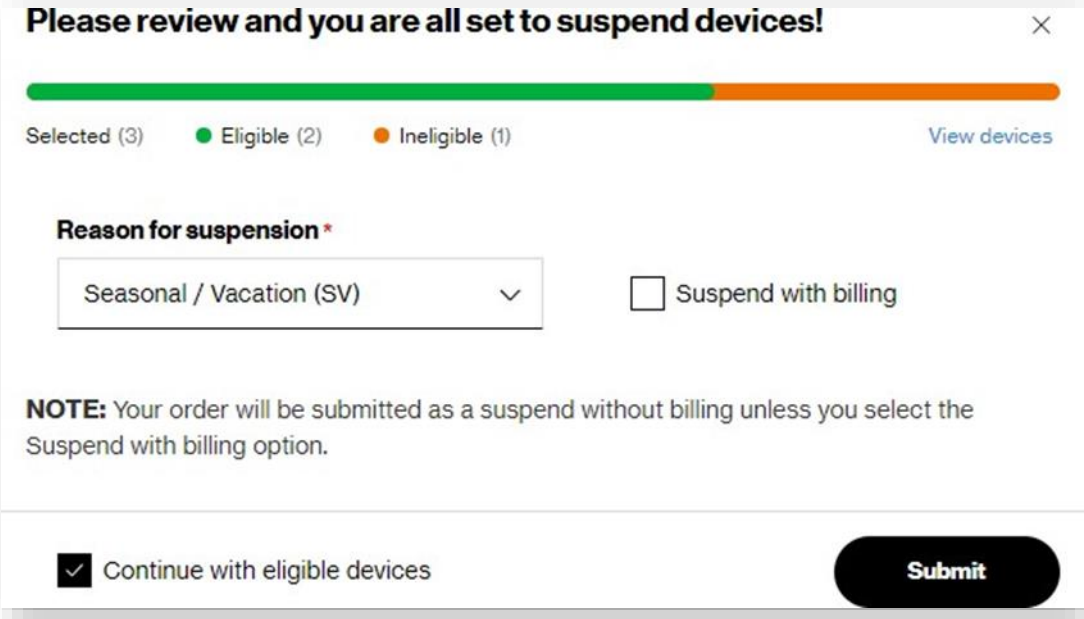
### How to suspend devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select devices using the *Device identifier* checkbox.

**NOTE:** You must only select devices from the same billing account.

2. Click the actions icon , and then select **Suspend**. A review page opens.



**Please review and you are all set to suspend devices!** ×

Selected (3) ● Eligible (2) ● Ineligible (1) [View devices](#)

**Reason for suspension \***

Seasonal / Vacation (SV) ▼ ☐ Suspend with billing

**NOTE:** Your order will be submitted as a suspend without billing unless you select the Suspend with billing option.

☒ Continue with eligible devices Submit


3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Select a **Reason for suspension**. Available reason codes are:
  - Lost / Stolen (21)
  - Seasonal / Vacation (SV)
5. Check **Suspend with billing**. If not checked, the devices are suspended without billing.
6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

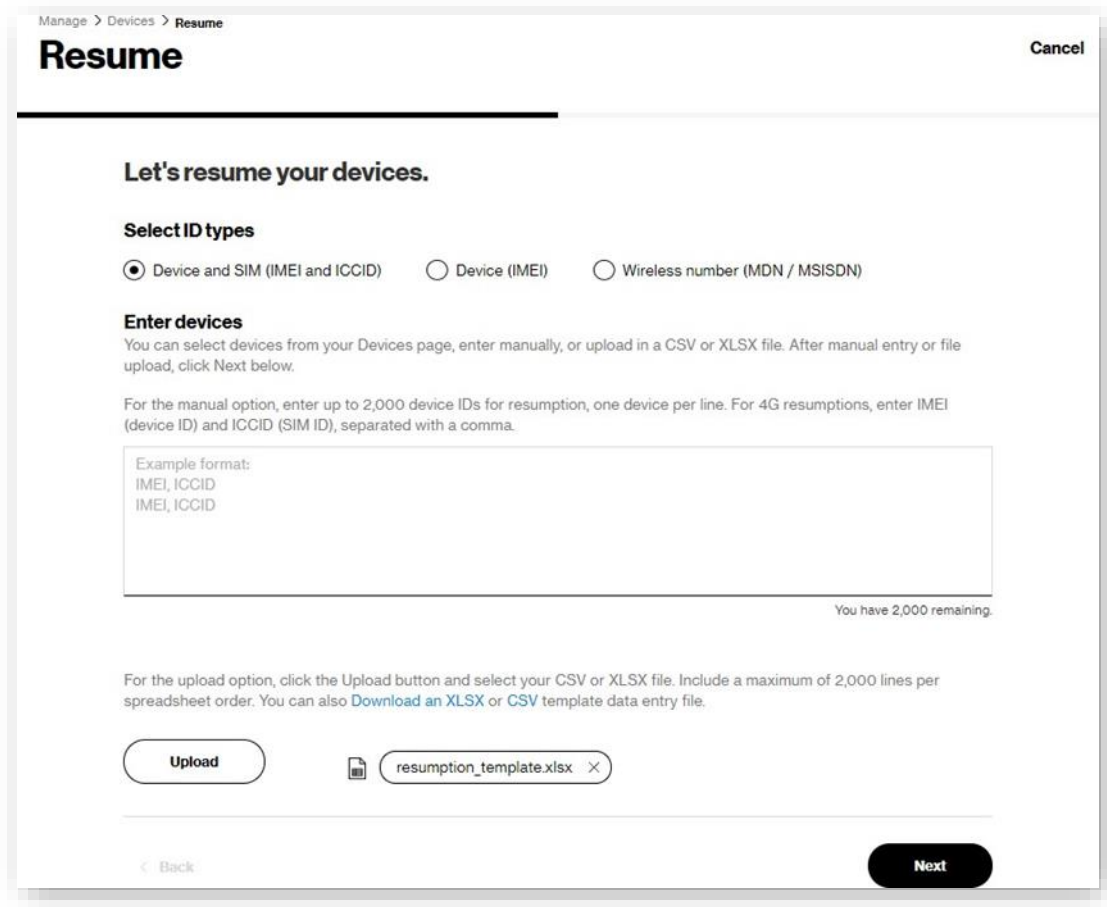


## Resuming Devices in Bulk

### How to resume devices in bulk

On the left navigation, click Devices. The Devices page opens.

1. With no devices selected, click the actions icon  then select **Resume**. The Resume page opens.



Manage > Devices > Resume

## Resume

Cancel

**Let's resume your devices.**

**Select ID types**

☒ Device and SIM (IMEI and ICCID) ☐ Device (IMEI) ☐ Wireless number (MDN / MSISDN)

**Enter devices**


You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.

For the manual option, enter up to 2,000 device IDs for resumption, one device per line. For 4G resumptions, enter IMEI (device ID) and ICCID (SIM ID), separated with a comma.

Example format:  
IMEI, ICCID  
IMEI, ICCID

You have 2,000 remaining.

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

**Upload**  resumption\_template.xlsx ×

Back Next

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data to the template file and save.
  - c. Click **Upload**.

- 4. Click **Next**. The *Resume* page opens.



- 5. Review eligible and ineligible device counts. To view the list of devices, click **View devices**. The Eligibility details dialog opens.

Eligibility details

3 Results

IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Ineligible	Device is not suspended.
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is not suspended.

- 6. Check **Continue with eligible devices** if necessary to proceed.
- 7. Click **Submit** to complete the process.


## Quick Resuming Devices

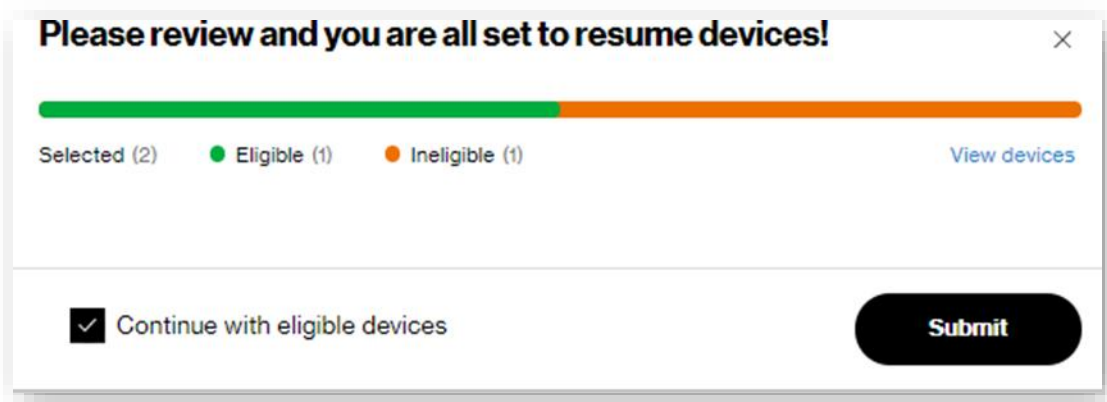
### How to resume devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select devices using the *Device identifier* checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon  then select **Resume**. A review page opens.



A modal window titled "Please review and you are all set to resume devices!" with a close button (X) in the top right corner. Below the title is a progress bar: a green segment followed by an orange segment. Under the green segment, it says "Selected (2)". Under the orange segment, it says "Eligible (1)" with a green dot and "Ineligible (1)" with an orange dot. To the right of the progress bar is a link "View devices". At the bottom left, there is a checked checkbox followed by the text "Continue with eligible devices". At the bottom right is a black button labeled "Submit".

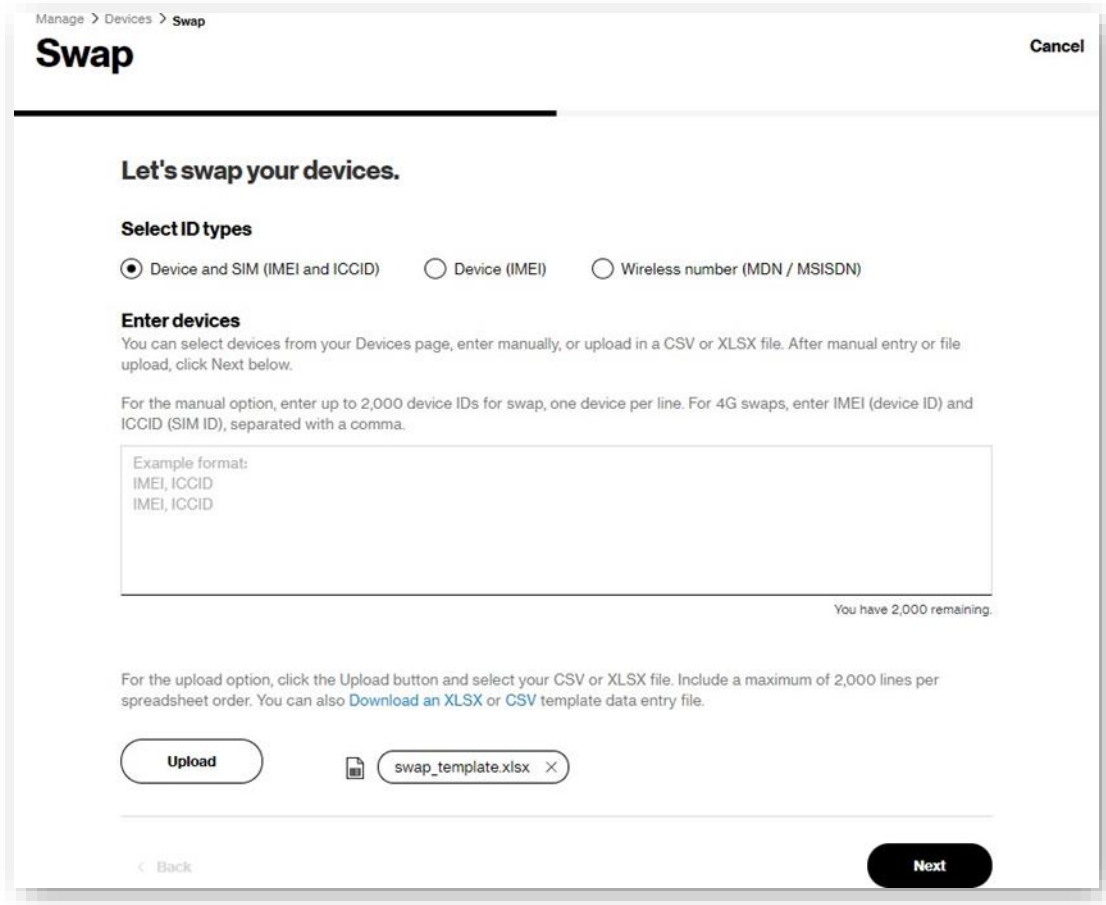
3. Review eligible and ineligible devices counts. To view the list of selected devices, click **View devices**.
4. Check **Continue with eligible devices** if necessary to proceed.
5. Click **Submit** to complete the process.

## Swapping Devices in Bulk

### How to swap devices in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon  then select **Swap devices**. The *Swap* page appears.



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data and save.
  - c. Click **Upload** to complete the upload process.

4. Click **Next**. The Swap page opens.

Manage > Devices > Swap

# Swap

Cancel

Please review and you are all set to swap devices!

Selected (3) ● Eligible (2) ● Ineligible (1) [View devices](#)

Current IMEI	Current ICCID	New IMEI	New ICCID
● [blurred]	[blurred]	Enter field	Enter field
● [blurred]	[blurred]	Enter field	Enter field
● [blurred]	[blurred]	Enter field	Enter field

☒ Continue with eligible devices Submit

[< Back](#)

5. Review eligible and ineligible device counts. To view the list of devices, click **View devices**. The Eligibility details dialog opens.

### Eligibility details

3 Results

IMEI	ICCID	Eligibility	Message
[blurred]	[blurred]	● Eligible	
[blurred]	[blurred]	● Eligible	
[blurred]	[blurred]	● Ineligible	Identifiers do not match records.

6. Enter a new **IMEI or ICCID** for each device you want to swap.
7. Check **Continue with eligible devices** if necessary to proceed.
8. Click **Submit** to complete the process.


## Quick Swapping of Devices

### How to swap devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select devices using the *Device identifier* checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon  , and then select **Swap**. A review page opens.

Please review and you are all set to swap devices!

Selected (2)

Eligible (2)

Ineligible (0)

[View devices](#)

Current IMEI	Current ICCID	New IMEI	New ICCID
<div></div>	<div></div>	Enter field	Enter field
<div></div>	<div></div>	Enter field	Enter field

Submit

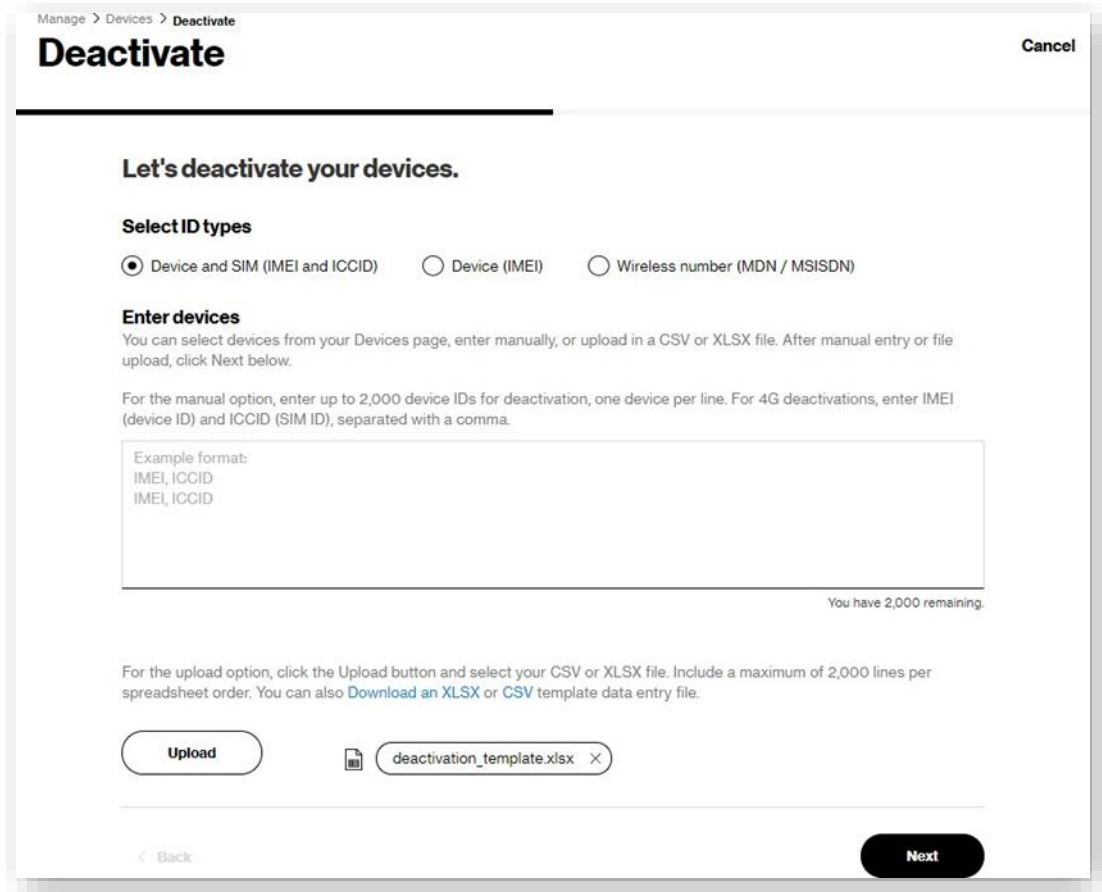
3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Enter a new **IMEI or ICCID** for each device.
5. Check **Continue with eligible devices** if necessary to proceed.
6. Click **Submit** to complete the process.

## Deactivating Devices in Bulk

### How to deactivate devices in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon  then select **Deactivate**. The *Deactivate* page opens.



Manage > Devices > Deactivate

## Deactivate

Cancel

**Let's deactivate your devices.**

**Select ID types**

☒ Device and SIM (IMEI and ICCID) ☐ Device (IMEI) ☐ Wireless number (MDN / MSISDN)

**Enter devices**



You can select devices from your Devices page, enter manually, or upload in a CSV or XLSX file. After manual entry or file upload, click Next below.

For the manual option, enter up to 2,000 device IDs for deactivation, one device per line. For 4G deactivations, enter IMEI (device ID) and ICCID (SIM ID), separated with a comma.

Example format:  
IMEI, ICCID  
IMEI, ICCID

You have 2,000 remaining.

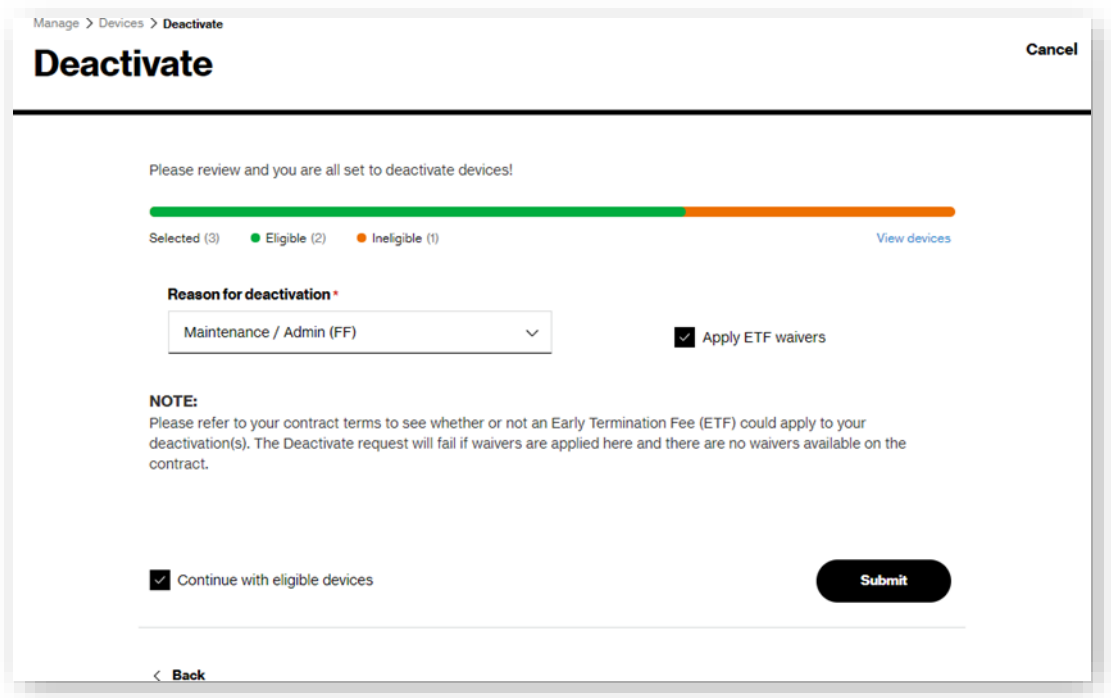
For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

**Upload**  deactivation\_template.xlsx 

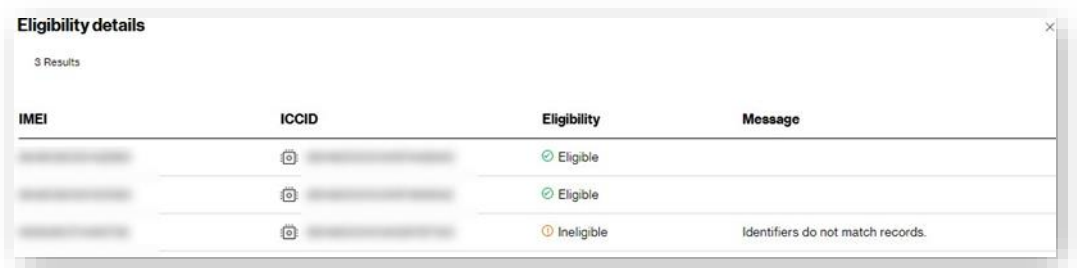
[< Back](#) [Next](#)

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data and save.
  - c. Click **Upload**.

4. Click **Next**. The *Deactivate* page opens.



5. Review eligible and ineligible device counts. To view the list of devices, click **View devices**. The Eligibility details dialog opens.



6. Select a **Reason for deactivation**. Available reason codes are:

- No Signal / Coverage Issue (A4)
- Competitor Promotion (BC)
- Employer Change (F2)
- Maintenance / Admin (FF)
- Financial Hardship (JJ)
- Customer Guarantee (PP)

7. Check **Apply ETF waivers** if applicable.

**NOTE:** Please refer to your contract terms to verify if an Early Termination Fee (ETF) applies to your deactivation(s). If you apply waivers here and there are no waivers available on the contract, the Deactivate request fails.



8. Check **Continue with eligible devices** if necessary to proceed.
9. Click **Submit** to complete the process.


## Quick Deactivating Devices

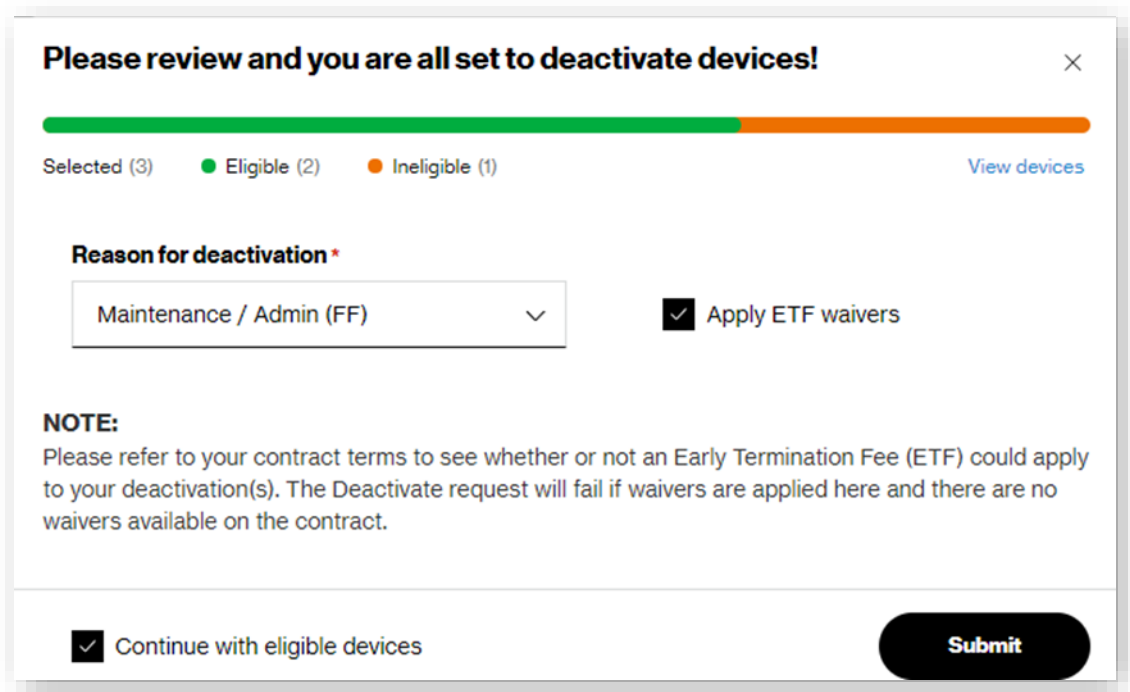
### How to deactivate devices

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the *Device identifier* checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon , and then select **Deactivate**. A review page opens.



**Please review and you are all set to deactivate devices!**

Selected (3)   ● Eligible (2)   ● Ineligible (1)   [View devices](#)

**Reason for deactivation \***

Maintenance / Admin (FF)   ☒ Apply ETF waivers

**NOTE:**  
Please refer to your contract terms to see whether or not an Early Termination Fee (ETF) could apply to your deactivation(s). The Deactivate request will fail if waivers are applied here and there are no waivers available on the contract.

☒ Continue with eligible devices   **Submit**

3. Review eligible and ineligible device counts. To view the list of selected devices, click the **View devices** link.
4. Select a **Reason for deactivation**. Available reason codes are:
  - No Signal / Coverage Issue (A4)
  - Competitor Promotion (BC)
  - Employer Change (F2)
  - Maintenance / Admin (FF)
  - Financial Hardship (JJ)
  - Customer Guarantee (PP)
5. Check **Apply ETF waivers** if applicable.

**NOTE:** Please refer to your contract terms to verify if an Early Termination Fee (ETF) applies to your deactivation(s). If you apply waivers here and there are no waivers available on the contract, the Deactivate request fails.

6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

## Deleting Devices

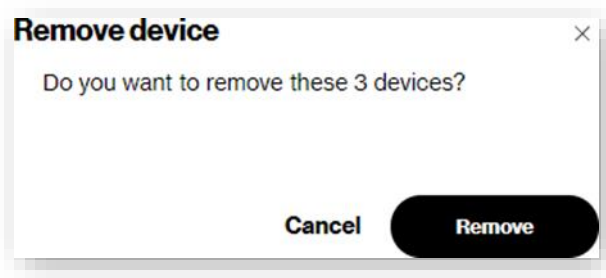
### How to remove devices from your plan

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the *Device identifier* checkbox.

**NOTE:** You must select devices in a **Pre-active** or **Deactive** state.

2. Click the actions icon , and then select **Delete**. The *Remove device* dialog opens.



3. Click **Remove**.

**NOTE:** When you remove a device from your plan, you are *permanently* deleting all device data from the system.


**COMING SOON:** The ability to remove devices from your plan in bulk.

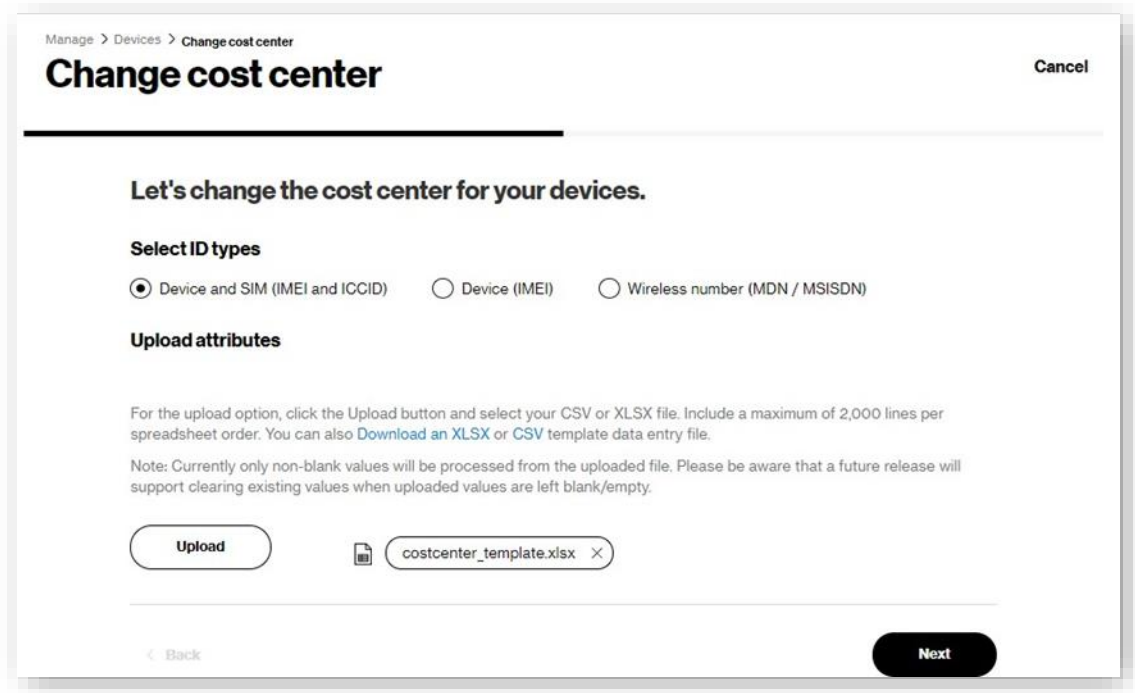
## Changing Cost Center Codes in Bulk

*Cost center code* is a user-defined string used by companies to assign to a device. Customers use cost centers in different ways, but typically for billing purposes. Valid Cost Center Codes consist of no more than 36 alphanumeric characters, and may include space, dash (-), exclamation point (!), and pound sign (#) characters.

### How to change cost center codes in bulk

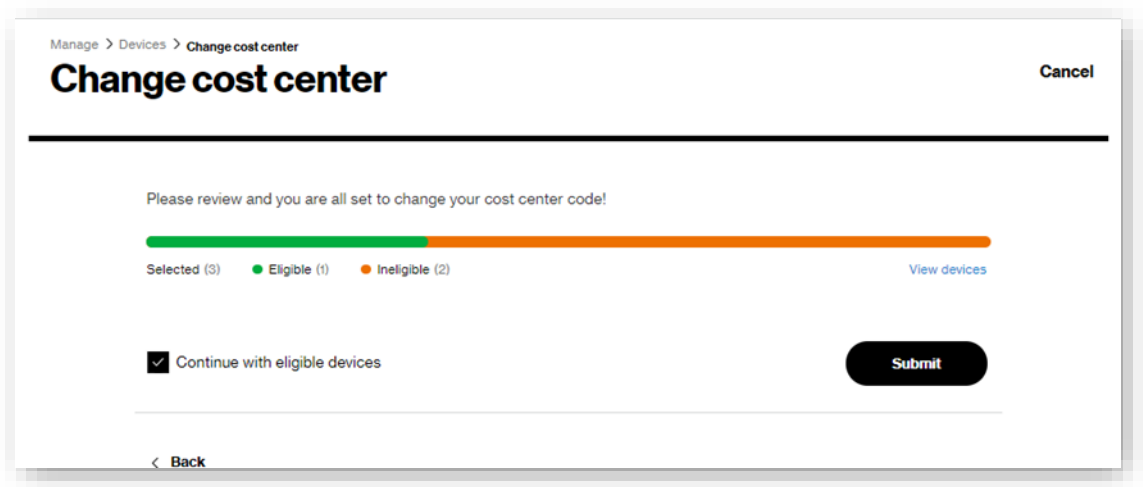
On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon , and then select **Change cost center**. The *Change cost center* page appears.



2. Select the **ID types** to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data and save.
  - c. Click **Upload**.

- 4. Click **Next**. The second *Change cost center* page opens.



- 5. Review eligible or ineligible device counts. To view the list of devices, click **View devices**. The Eligibility details dialog opens.

Eligibility details

3 Results

IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is not active.
[REDACTED]	[REDACTED]	Ineligible	Identifiers do not match records.

- 6. Check **Continue with eligible devices** if necessary to proceed.
- 7. Click **Submit** to complete the process.

## Quick Cost Center Code Changes

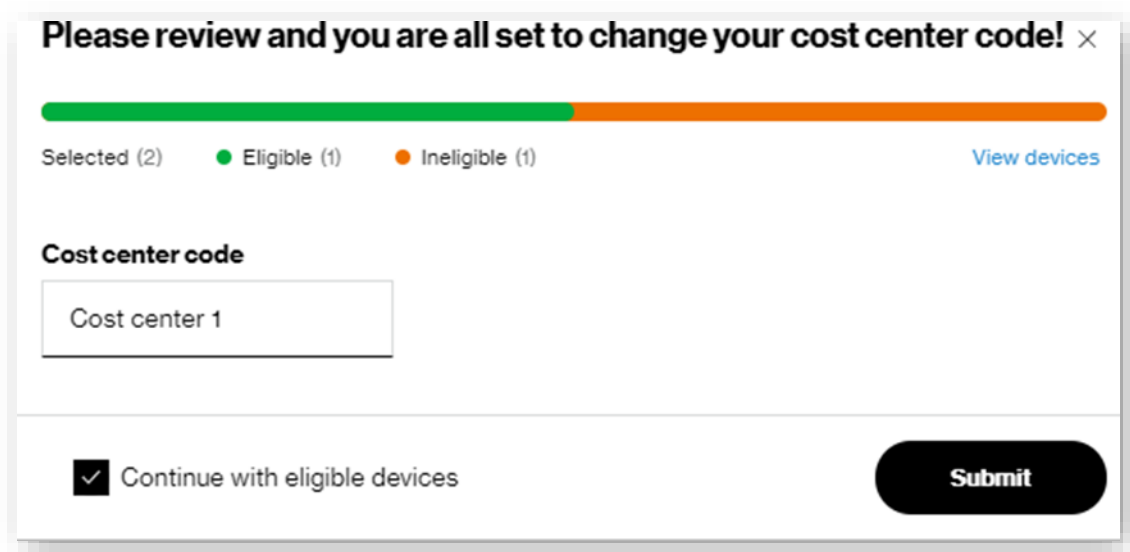
### How to change cost center codes

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the Device identifier checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon , and then select **Change cost center**. A review page opens.



Please review and you are all set to change your cost center code! ×

Selected (2) ● Eligible (1) ● Ineligible (1) [View devices](#)

**Cost center code**

Cost center 1

☒ Continue with eligible devices **Submit**


3. Review eligible and ineligible device counts. To view the list of selected devices, click the **View devices** link.
4. Type the **Cost center code** to assign. Limit 36 characters.
5. Check **Continue with eligible devices** if necessary to proceed.
6. Click **Submit** to complete the process.

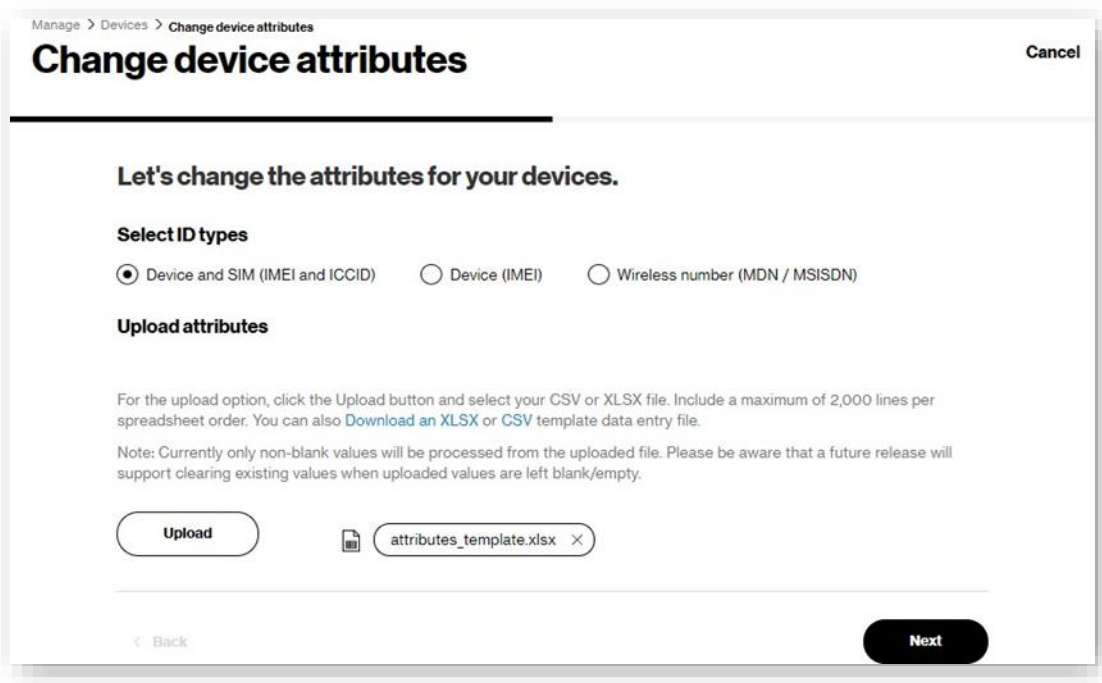
## Changing Custom Fields in Bulk

Customers use custom fields to assign their own values to devices and typically contain device type, region, business unit, or some information that further characterizes the device. These fields display alternative label text when custom labels have been assigned. See [Custom Field Labels](#) for additional information.

### How to change custom fields in bulk

On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon , and then select **Change custom fields**. The *Change device attributes* page appears.



Manage > Devices > Change device attributes

### Change device attributes

Cancel

**Let's change the attributes for your devices.**


**Select ID types**

☒ Device and SIM (IMEI and ICCID) ☐ Device (IMEI) ☐ Wireless number (MDN / MSISDN)

**Upload attributes**

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also [Download an XLSX](#) or [CSV](#) template data entry file.

Note: Currently only non-blank values will be processed from the uploaded file. Please be aware that a future release will support clearing existing values when uploaded values are left blank/empty.

 attributes\_template.xlsx

2. Select the **ID types** to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data and save.
  - c. Click **Upload**.



- 4. Click **Next**. The second *Change device attributes* page opens.



- 5. Review eligible or ineligible device counts. To view the list of devices, click **View devices**. The Eligibility details dialog opens.

Eligibility details

4 Results

IMEI	ICCID	Eligibility	Message
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Eligible	
[REDACTED]	[REDACTED]	Ineligible	Device is in pending status.

- 6. Check **Continue with eligible devices** if necessary to proceed.
- 7. Click **Submit** to complete the process.

## Quick Custom Field Changes

### How to change custom fields

On the left navigation, click Devices. The Devices page opens.

1. Select the Device identifier checkbox.

**NOTE:** You must select devices from the same billing account.

2. Click the actions icon  and then select **Change custom fields**. The *Assign custom fields* page opens.

Assign custom fields

×

Select the field(s) you would like to update and enter new text values. Selecting a field and leaving the text blank will clear existing values.

MyCustom Field 1

☒ Primary value

MyCustom Field 2

☒ Secondary value

MyCustom Field 3

☐

MyCustom Field 4

☐

MyCustom Field 5

☐

Devices may already have values assigned to these fields. Clicking Save overwrites any existing custom field values for the 2 selected devices.

Cancel

Save

3. Select a custom field label.
4. Type the **Value**.
5. Click **Save** to complete the process.


**NOTE:** The following special characters are allowed in custom field values.

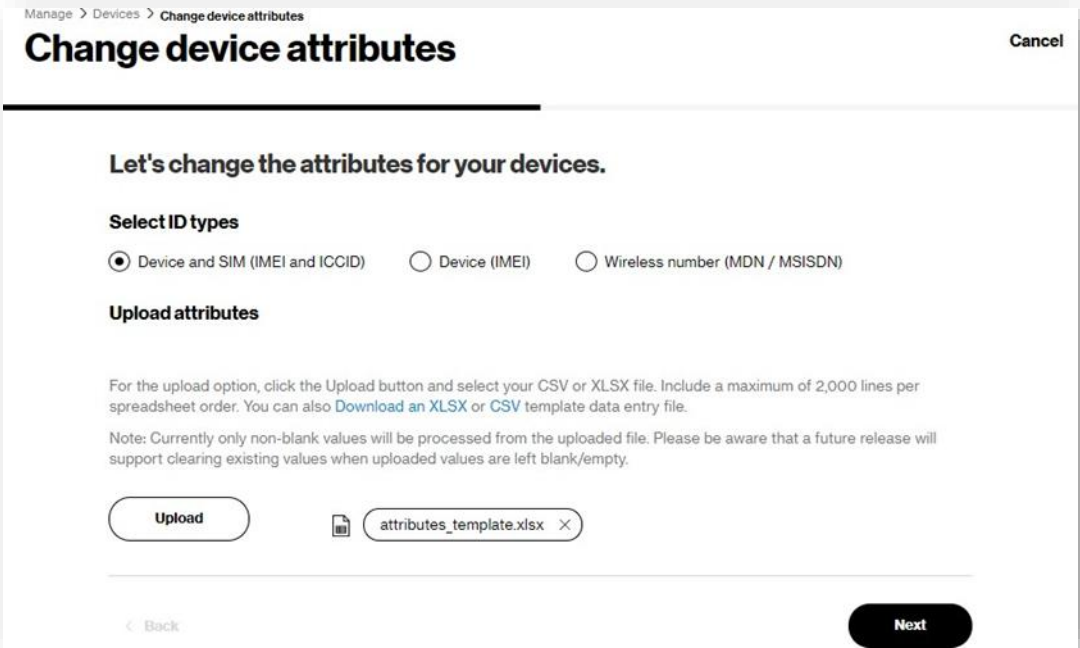
- Alphanumeric characters
- / (forward slash)
- SPACE
- @ (at sign)
- . (period)
- , (comma)
- : (colon)
- - (hyphen)
- \_ (underscore)
- ( (open parenthesis)
- ) (close parenthesis)
- [ (open bracket)
- ] (close bracket)
- # (number sign or hash tag)

## Changing Device Groups in Bulk

### How to device groups in bulk

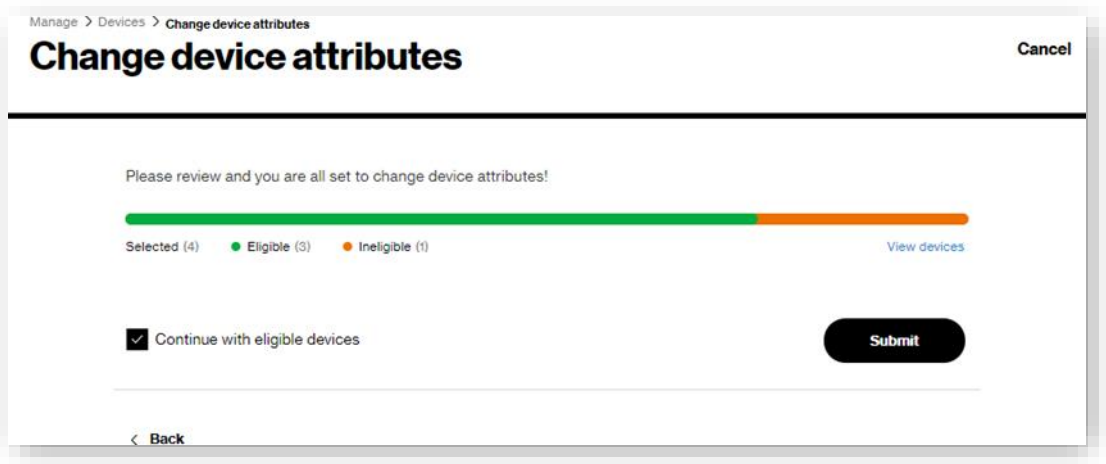
On the left navigation, click **Devices**. The *Devices* page opens.

1. With no devices selected, click the actions icon  and then select **Change device groups**. The *Change device attributes* page opens.



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
  - a. To upload a file, click **Download an XLSX or CSV** to download the template.
  - b. Add your data and save.
  - c. Click **Upload** to complete the upload process.

4. Click **Next**. The *Change device attributes* page opens.



5. Review eligible or ineligible device counts. To view the list of devices, click **View devices**. The *Eligibility details* dialog opens.

The screenshot shows the 'Eligibility details' dialog with a close button (X) in the top right. It indicates '4 Results'. The table below has the following data:

IMEI	ICCID	Eligibility	Message
[blurred]	[blurred]	Eligible	
[blurred]	[blurred]	Eligible	
[blurred]	[blurred]	Eligible	
[blurred]	[blurred]	Ineligible	Device is in pending status.

6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

## Quick Device Group Changes

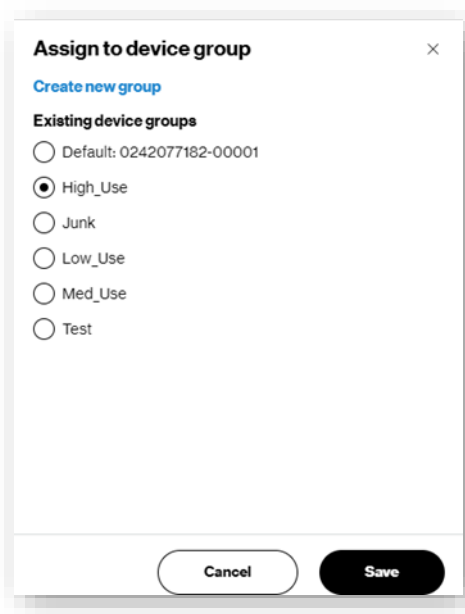
### How to change the device groups

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the *Device identifier* checkbox.

**NOTE:** A device is currently only allowed to be in one group at a time.

2. Click the actions icon  and then select **Change device group**. The *Assign to device group* page opens.



The image shows a modal dialog box titled "Assign to device group" with a close button (X) in the top right corner. Inside the dialog, there is a link "Create new group" in blue. Below it, the section "Existing device groups" contains a list of radio button options: "Default: 0242077182-00001", "High\_Use" (which is selected), "Junk", "Low\_Use", "Med\_Use", and "Test". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

3. You have two options for assigning a device to a group:
  - Select an existing device group.
  - Click **Create new group**. The *Assign to device group* dialog refreshes with a new group form.



The image shows a dialog box titled "Assign to device group" with a close button (X) in the top right corner. Inside the dialog, there is a link "Add to existing group" in blue. Below this, there is a section for "New group name" with a text input field containing the placeholder text "New group". Underneath that is a section for "Description" with a text input field containing the placeholder text "This is my new group". At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

- a. For **New group name**, type a descriptive label.
  - b. Type an optional **Description** of the new group name.
  - c. Click **Save**. The *Assign to device group* dialog closes.
4. On the *Assign to device group* page, click **Save** to complete the process.

## Sending an SMS

### How to send an SMS to a device

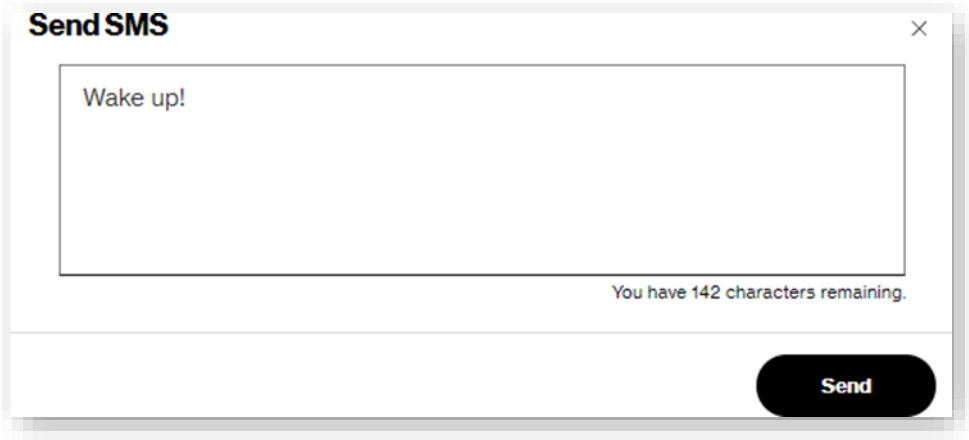
On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the **Device identifier** checkbox.

You can only send an SMS to one device at a time.

**COMING SOON:** The ability to send SMS messages to multiple devices.

2. Click the actions icon  and then click **Send SMS**. The *Send SMS* dialog opens.




The image shows a 'Send SMS' dialog box. It has a title bar with 'Send SMS' and a close button (X). Inside, there is a large text input area containing the text 'Wake up!'. Below the input area, on the right, it says 'You have 142 characters remaining.' At the bottom right of the dialog is a black button with the word 'Send' in white.

3. Type the SMS message up to a maximum of 150 characters.
4. Click **Send** to complete the process.




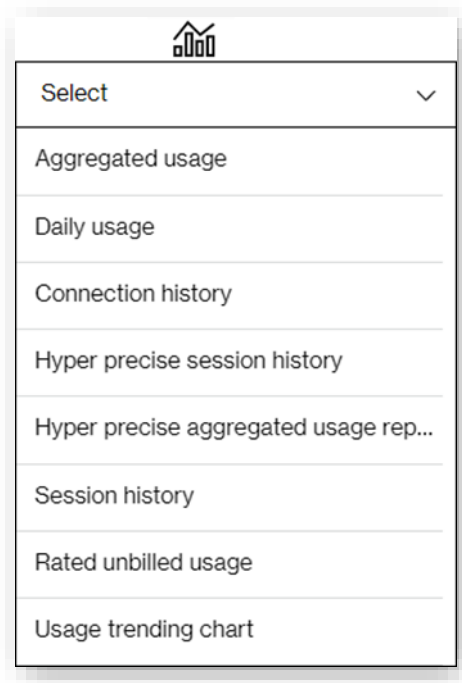
## Reporting Actions

Use the reports icon  to run standard reports on up to 10 devices at a time. To run reports on more than 10 devices, go directly to the [Reports](#) page and create an advanced report.

### How to run reports

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the *Device identifier* checkbox.
2. Click the reports icon  and select a report from the menu. The following reports are available. Refer to the Reports section of this user guide for details on each report.



- [Aggregated usage](#) – Track overall usage for all devices on your plan.
- [Daily usage](#) – Identify “normal” usage patterns.
- [Connection history](#) – Research or troubleshoot connectivity issues by examining the Start and Stop events associated with a device’s connections.
- Hyper precise session history – Monitor a device’s hyper precise session history (requires subscription).
- Hyper precise aggregated usage – Track overall usage a device’s hyper precise location (requires subscription).
- [Session history](#) – Monitor a device’s connectivity patterns by examining details of its connected sessions.
- [Rated unbilled usage](#) – View rated usage per device for the current billing cycle (to appear on the next bill).
- [Usage trending chart](#) – View the total usage by day for a device in a graph.

When you select a report, the [Reports](#) page opens to enter further selection criteria.

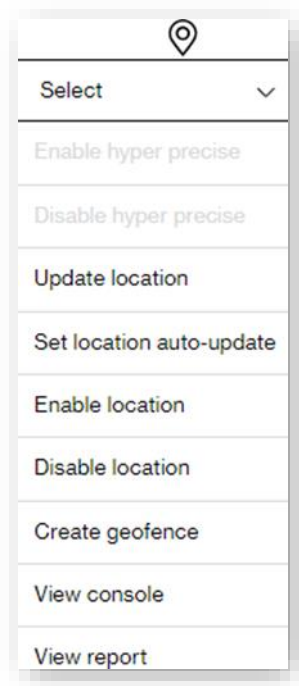
## Location Actions

For customers subscribed to *Location* or *Hyper Precise Location Services*, you can take location actions on selected devices.

### To take Location actions

On the left navigation, click **Devices**. The *Devices* page opens.

1. Select the ID checkbox.
2. Click the locations icon  and then select an action from the menu. The following menu items are available:




- **Enable hyper precise** – Enables Hyper Precise Location.
- **Disable hyper precise** – Disables Hyper Precise Location.
- **Update location** – Sends a request to update the location of selected devices.
- **Set location auto-update** – Enables location updates based on a scheduled interval.
- **Enable location** – Enables location updates.
- **Disable location** – Disables location updates.
- **Create geofence** – See the section on [creating a geofence](#) for more details.
- **View console** – Open the location console where you locate devices anywhere on our network, view location history, receive alerts when they move outside of their expected location, and more.
- **View report** – Runs the location report.

## Creating a Geofence

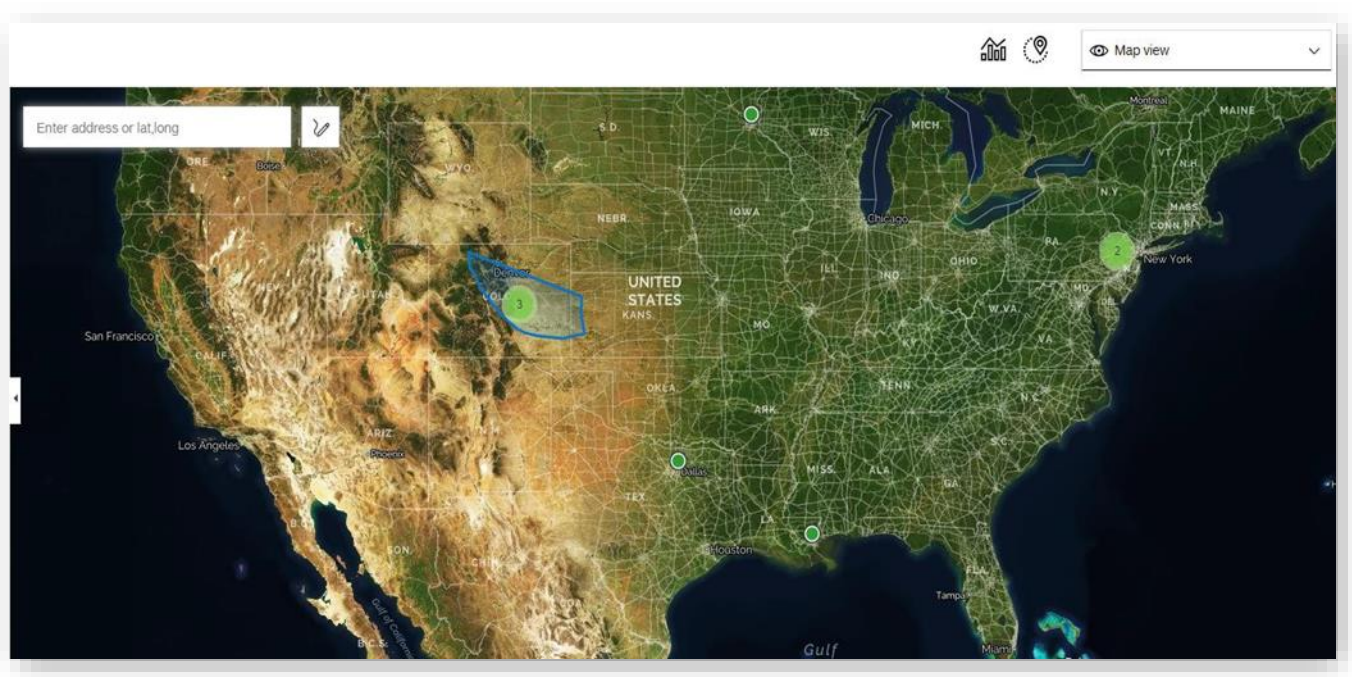
Create a geofence to view real-world geographic areas around your devices. Alarms can be set to notify you when your device moves outside of the set geofence boundaries.


### To create a geofence

On the left navigation, click **Devices**. The *Devices* page opens.

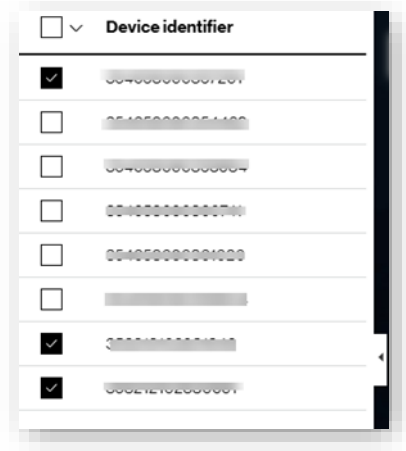
1. Select **Map view**.
2. Click the drawing tool .
3. Click and drag on the map to form the geofence shape. This automatically selects any devices within the on the map.

**NOTE:** You must select devices from the same billing account to create a geofence rule.

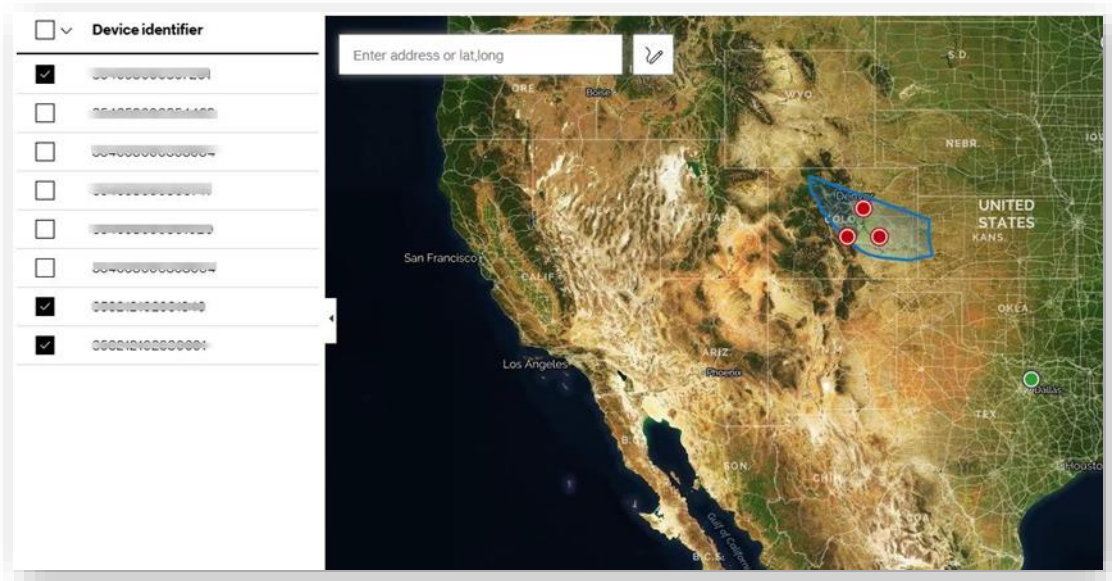


4. Click devices on the map, or open the list  to select / unselect.

5. Verify all devices to include for the alert are selected, and then choose Create geofence from the Location actions menu.



6. Use the drawn shape for all selected devices, or you can specify a radius to create an individual geofence circle around each selected device. The *Create geofence* page opens.



**NOTE:** The system evaluates the geofence rule each time the platform receives a location update for the device. Make sure to set the auto location update rate on all devices.

8. For **Geofence name**, type a descriptive label.
7. Choose how to create the geofence.
  - **Drawn geofence** – draw the geofence in a map.
  - **Device geofence** – specify the geofence for each device based on distance.

9. Select notification trigger.

- **Geofence exit** – sends a notification when the device exits the geofence.
- **Geofence entry** – sends a notification when the device enters the geofence.
- **Dwell time within geofence** – sends a notification when the device stays within the geofence for a set period of time.

The image displays two side-by-side screenshots of the 'Create geofence' dialog box, showing different sections of the configuration process.

**Left Screenshot: 'Create geofence' dialog box**

- Geofence name \***: Specify a name for your geofence. (Empty text box)
- Geofence type**:
  - ☒ **Drawn geofence**: Use the shape you've drawn as the geofence.
  - ☐ **Device geofence**: Specify the geofence for each device. (Includes a numeric input '1' and a unit dropdown 'Meter(s)')
- Notify**: Specify notification.
  - ☒ Geofence exit
  - ☒ Geofence entry
  - ☒ Dwell time within geofence (Includes a numeric input '1' and a unit dropdown 'Hour(s)')
- Buttons**: Cancel, Next

**Right Screenshot: 'Create geofence' dialog box**

- Setup reminder \***: Includes a numeric input '1' and a dropdown menu 'Hourly'.
- Severity \***: please select severity. (Dropdown menu showing 'Major')
- Email notification \***: Send email notifications to specific people. (Text area containing 'test@email.com')
- Buttons**: Cancel, Back, Save

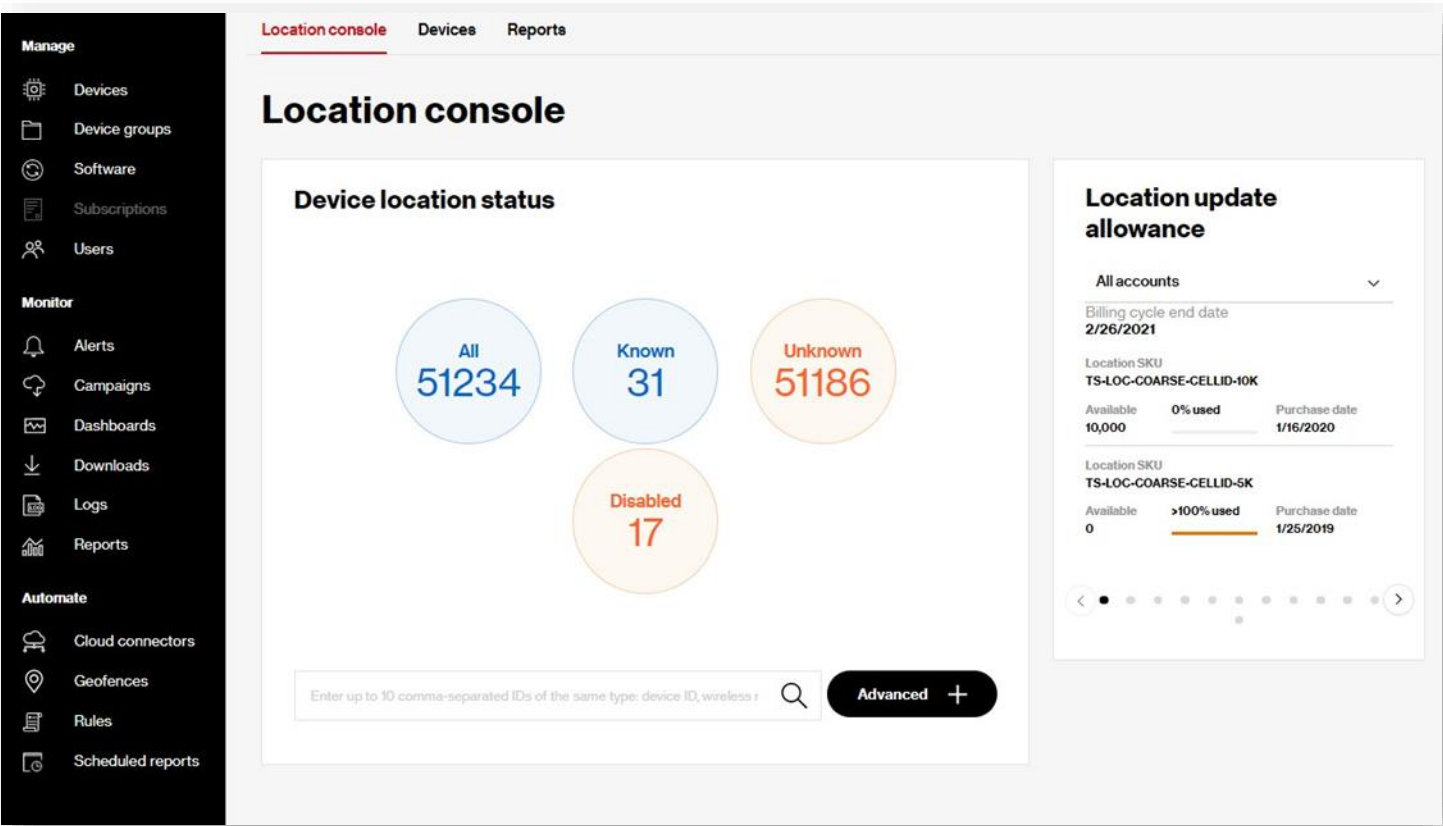
10. Click **Next**.

- **Setup reminder** – sends a reminder depending on how you set this option up.
- **Severity** – Select the severity of this geofence. The severity is included in the notification email.
- **Email notification** – Type the notification recipient's email addresses.

11. Click **Save** to complete.

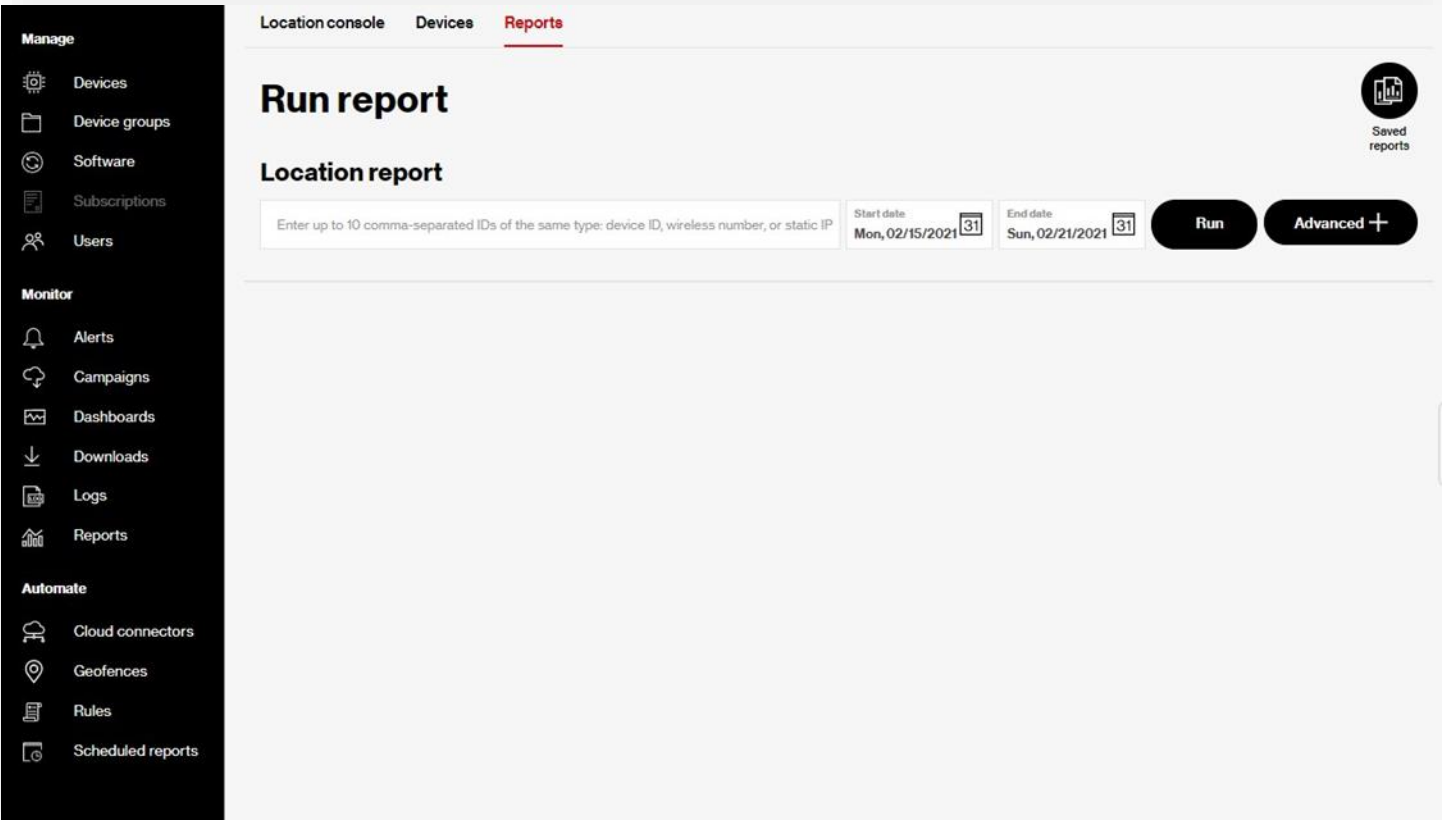
# View Location Console

Use the *Location Console* page to view *Location Services* enabled devices




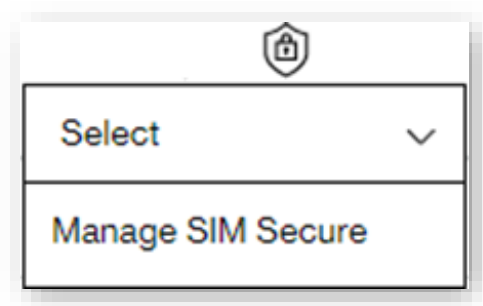
# View Location Report

Use the *Location Report* page to run the Location Report.



## SIM Secure Actions

For customers that are subscribed to SIM Secure Services, you can manage services by clicking the security icon  and selecting **Manage SIM Secure**. The legacy *SIM Secure* page opens.



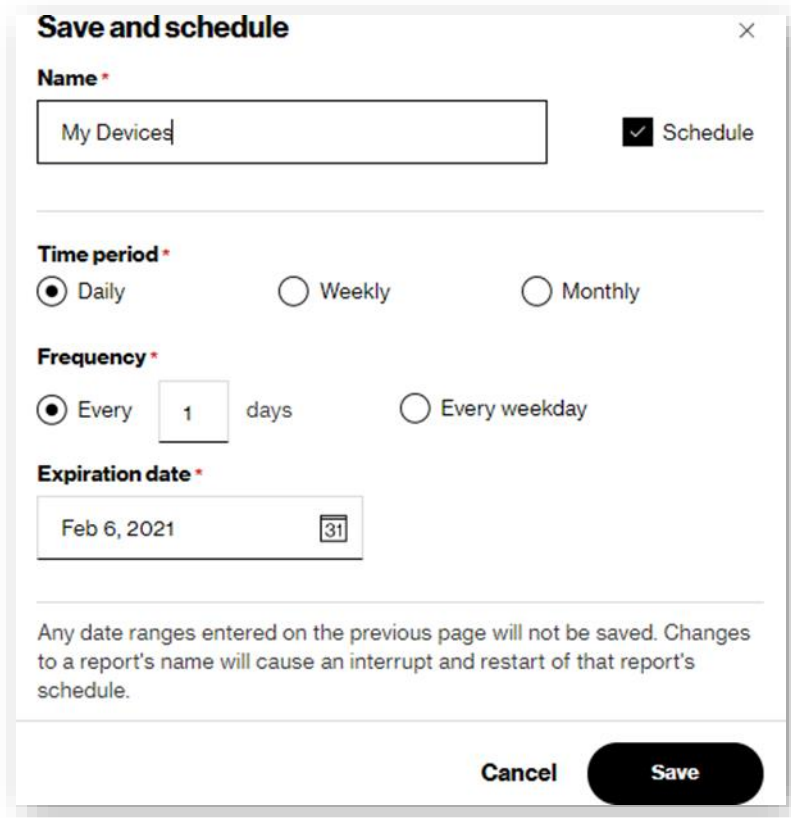
**COMING SOON:** The ability to assign SIM Secure licenses directly from the [Devices](#) page.



## Schedule Action

How to save and/or schedule your devices list as a report

Click the schedule icon . The *Save and schedule* page opens.



**Save and schedule** ×

**Name \***

My Devices ☒ Schedule

---

**Time period \***

☒ Daily ☐ Weekly ☐ Monthly

**Frequency \***

☒ Every  days ☐ Every weekday

**Expiration date \***

Feb 6, 2021

Any date ranges entered on the previous page will not be saved. Changes to a report's name will cause an interrupt and restart of that report's schedule.

Cancel **Save**

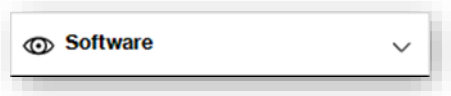
1. For **Name**, type a descriptive label for the devices report.
2. Check **Schedule** to run this report at a predetermined date and time.
  - a. Select the **Time period** for your scheduled report.
  - b. Set the **Frequency** for the report to run.
  - c. Select an *Expiration date* for the report to end the schedule.
3. Click **Save** to complete the process.



## Create a campaign

For customers subscribed to *Software Management Services*, you can create a campaign to update devices with the most recent software release.


### How to create a campaign

- 1. Click on the View drop-down menu, and then select Software.



- 2. Click the filter icon  Filter .
- 3. On the left navigation, click **Software**.

A screenshot of a software filter configuration dialog. On the left is a vertical navigation menu with items: Status, Account, Attributes, Roaming, Location, and Software. The 'Software' item is selected and has a checkmark. The main area of the dialog is titled 'FOTA make and model' and contains a description: 'The FOTA (Firmware-over-the-air) make and model represent the make and model reported by the device eligible for software upgrades. In some cases, this is equivalent to the device make and model; in other cases it represents the modem make and model of the device.' Below this description are two dropdown menus: the first is labeled 'NOKIA' and the second is labeled '822'. Below these is another section titled 'Software name' with a description: 'These are software upgrades available for your devices.' Below this is a single dropdown menu showing 'HOSTEDTOSS\_NOKIA\_822\_1572421732449'. At the bottom of the dialog are three buttons: 'Clear all', 'Cancel', and 'Apply'.

- 4. Select the **FOTA make and model** and **Software name** from the menus.
- 5. Click **Apply**. This filters the devices list to devices that are eligible to receive a software download.
- 6. Select the IDs checkbox of the devices to include in the campaign.
- 6. Click the campaign icon , and then select **Create campaign**.

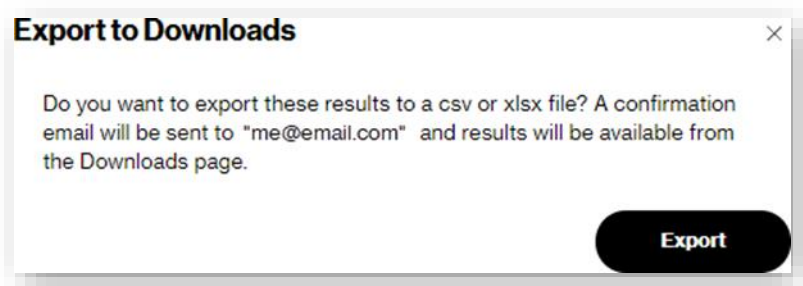
**NOTE:** The Create campaign option is disabled when the selected devices are not eligible for a software update.

- 7. Follow the [Create a campaign](#) wizard to complete the creation of your campaign.

## Exporting Device Lists

### How to export your devices list


1. Click the download icon . The *Export to Downloads* dialog opens



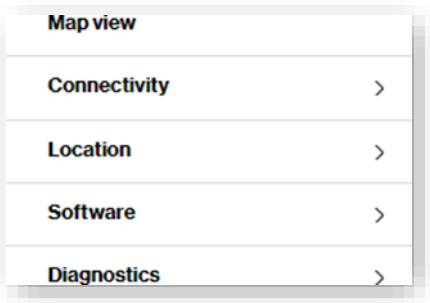
2. Click **Export**.

**NOTE:** The *Downloads* center accepts all the devices on the list to download them when the report is available. You receive an email notification when the download is ready. You can view the download in the [Downloads](#) page.

## Customizing Your View

Customize your devices list display by creating custom table views. Table views are found on a menu with the view icon . Select a view to refresh the devices list with fields in that view.

**Predefined Views** are table views containing groups of related fields based on your interest. Predefined views display in bold font to distinguish from custom views. You cannot edit predefined views. Only views that you create, which are custom views, can you edit.




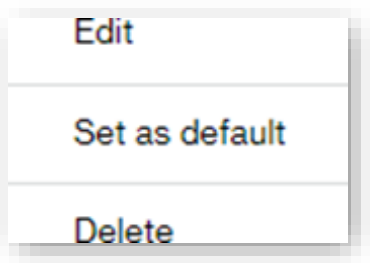
Available predefined views are:

- **Map View** – Open a list of devices on a map, like in the image below. From this view, Location Services subscribers can also create a geofence.

**NOTE:** In order to view your devices on the map, you must be subscribed to Location Services and your devices must be enabled for location updates

- **Connectivity View** – Open fields related to device connectivity.
- **Location View** – Open fields related to device location.
- **Software View** – Open fields related to software management.
- **Diagnostics View** – Open fields related to device diagnostics and are useful for troubleshooting issues.

Click on the expand icon  to view the available options.

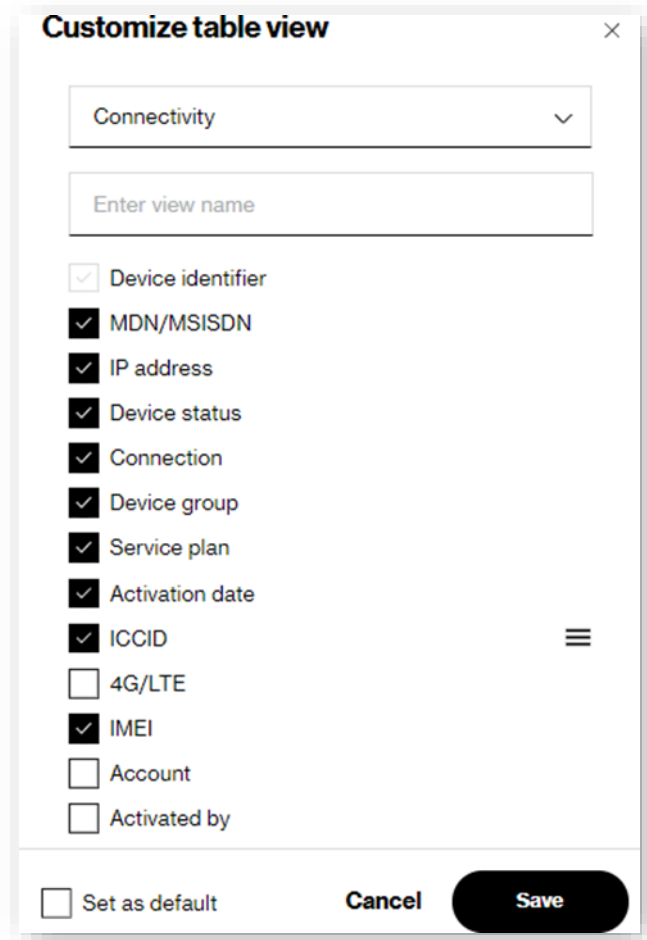


## Custom Views

Custom views are table views you develop from predefined views.

### To create a Custom View

1. Click the view icon  and select Create View. The Customize table view dialog opens.



**Customize table view** [X]

Connectivity [v]

Enter view name

- ☐ Device identifier
- ☒ MDN/MSISDN
- ☒ IP address
- ☒ Device status
- ☒ Connection
- ☒ Device group
- ☒ Service plan
- ☒ Activation date
- ☒ ICCID [≡]
- ☐ 4G/LTE
- ☒ IMEI
- ☐ Account
- ☐ Activated by

☐ Set as default    **Cancel**    **Save**

2. Select a predefined view from the menu.
3. For **Enter the view name**, type a descriptive label that identifies the view. Character limit is 32 alphanumeric characters including spaces and underscores.
  - a. Select the fields to include.
  - b. Reorder the fields as desired.
  - c. Hover the cursor over the right side of the field name until the move icon appears. [≡]
  - d. Drag and drop the field to the desired position on the list.
  - e. Check the **Set as default** checkbox to make this your default view.
4. Click **Save** to complete the process.

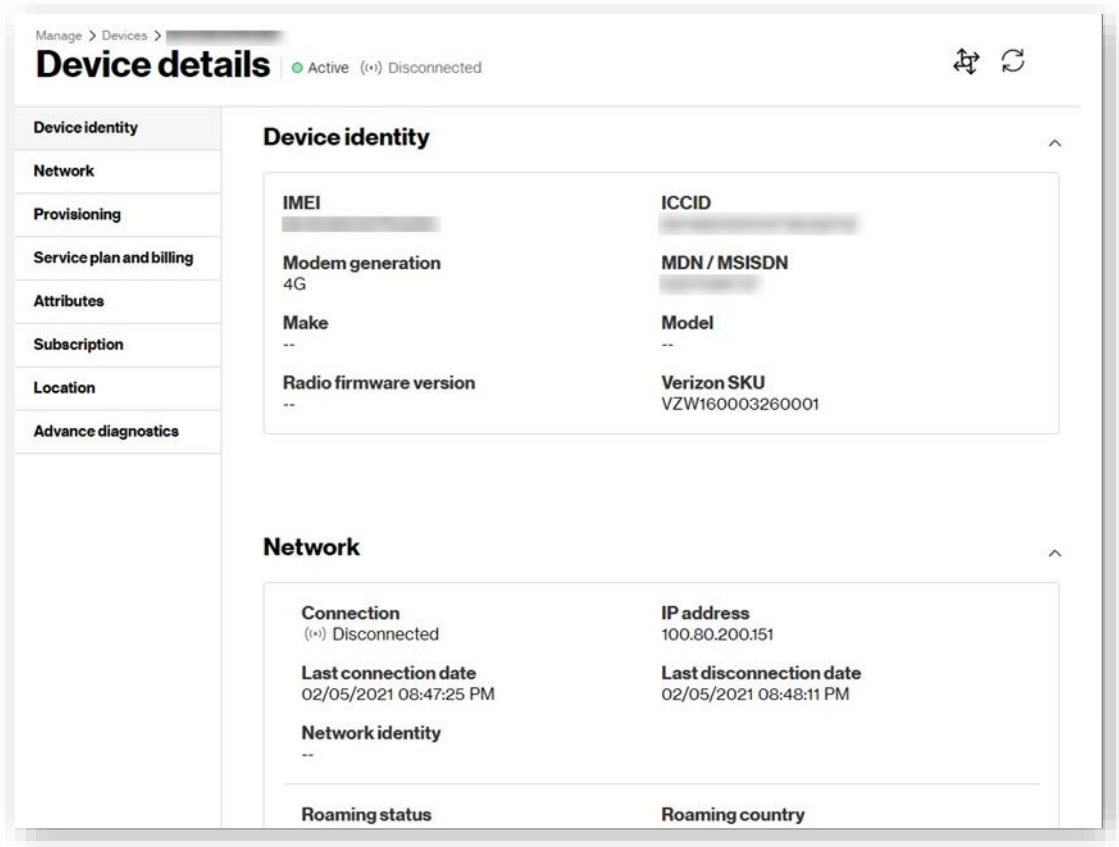
## Device Details

You can drill down into device details from the *Devices* page by clicking a **Device ID**. This opens device attributes, behavior, usage, and other associated information.

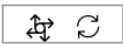
To view device details

On the left navigation, click **Devices**. The *Devices* page opens.

1. Click the **Device identifier**. A *Device details* page opens with details about the selected device.



2. Use the left navigation to open the relevant section.
3. Take actions on the device by clicking on one of the icons on the top right side of the page.
4. Use the actions icon to send an SMS to the device and reload the page.
5. The following information is available in the *Device details* page.



## Device identity

The *Device identity* section provides the following details:

Device identity	
<b>IMEI</b> [REDACTED]	<b>ICCID</b> [REDACTED]
<b>Modem generation</b> 4G	<b>MDN / MSISDN</b> [REDACTED]
<b>Make</b> --	<b>Model</b> --
<b>Radio firmware version</b> --	<b>Verizon SKU</b> VZW160003260001

## Network

The *Network* section provides the following details:

Network	
<b>Connection</b> (●●) Connected	<b>IP address</b> 100.76.36.136
<b>Last connection date</b> 01/30/2021 05:31:09 PM	<b>Last disconnection date</b> 01/30/2021 05:18:36 PM
<b>Network identity</b> --	
<b>Roaming status</b> Not roaming	<b>Roaming country</b> Not applicable
<b>MNC</b> 270	<b>MCC</b> 311

## Provisioning

The *Provisioning* section provides the following details:

Provisioning

Device status

Active

Activation date

04/23/2021 11:43:39 AM

Suspended date

--

SIM OTA timestamp

04/23/2021 11:46:38 AM

Deactivation date

--

Expected resume date

--

Last order status

SUCCESS

Last order ID

909993637

Request ID

f094ae1c-486b-4256-9146-56ab582de430

View order

Transaction history

Order	Status	Date	Submitted by
Activation	<div>Success</div>	04/23/2021 11:43:39 AM	Mark Nicholson



## Service plan and billing

The *Service plan and billing* section provides the following details:

Service plan and billing

Account

Billing cycle

23 days left

Cycle starts

January 29, 2021

Cycle ends

February 28, 2021

Rated usage

--

SMS

--

Last updated date

--

Raw usage

3.09MB

Last updated date

02/05/2021

Service plan description

IOT ACCOUNT SHARE 1GB \$1/MB

Service plan code

CCMPub

Service plan type

Public Dynamic

Feature codes(SFO)

84840, 84206, 83905, 84777, 75802, 75706, 47309, 48526

Network public feature codes

84777

# Attributes

The *Attributes* section provides the following details:

Attributes

Cost center

--

Device group

Default:

MyCustom Field 1

--

MyCustom Field 2

--

MyCustom Field 3

--

MyCustom Field 4

--

MyCustom Field 5

--

Name

Address

--

## Subscriptions

The *Subscription* section provides the following details:

Subscription

Location services SKU

TS-BUNDLE-KTO-LOC-COARSE-MRC

FOTA SKU

TS-BUNDLE-KTO-SWMT-MRC

Bundle SKU

TS-BUNDLE-KTO-MRC

Diagnostics SKU

TS-BUNDLE-KTO-DIAG-LWM2M-MRC

The *Location* section provides the following details:

## Advanced diagnostics

The *Advanced* diagnostics section is available by subscription and is used to provide details that help in troubleshooting device issues. You can also reboot devices on this page. See [Appendix](#) for field descriptions.

Advance diagnostics

Modem

--

APN1

--

APN2

--

Battery level

0%

Battery status

--

Power sources

--

Last streamed value

Cell ID

--

Network bearer

--

RF signal strength

0

RF link quality

0

Streaming statuses

Live stream

Cell ID

--

Network bearer

--

RF signal strength

--

RF link quality

--

Streaming statuses

Live stream

Cell ID

--

Network bearer

--

RF signal strength

--

RF link quality

--

Timers

PSM timer

--

Active timer

--

eDRX timer

--

Paging time window

--

# Device Groups

Use the *Device Groups* page to assign devices to individual groups. A device can only be assigned to one group at a time. Use the left navigation to open the *Device Groups* page.

Manage

Devices

**Device groups**

Software

Subscriptions

Users

Monitor

Alerts

Campaigns

Dashboards

Downloads

Logs

Reports

Automate

Cloud connectors

Geofences

Rules

Scheduled reports

Manage device groups

Devices

Add devices or attributes

113 Device groups

Search

+

Group name	Description	Account	Devices	Actions
ArulTest_Group	ArulTest_Group	0844021539-00001	0	<div>View</div> <div>Edit</div>
ATestingGroup123		0844021539-00001	188	<div>View</div> <div>Edit</div>
awesome group		0552018439-00001	0	<div>View</div> <div>Edit</div>
CCU	CCU	0844021539-00001	4	<div>View</div> <div>Edit</div>
CCU	CCU	0844021539-00001	0	<div>View</div> <div>Edit</div>
csvgroup_imeiniccid		0844021539-00001	31	<div>View</div> <div>Edit</div>
DanielLiangDeviceGrp1		0844021539-00001	17	<div>View</div> <div>Edit</div>
DanielLiangT1		0107787298-00001	855	<div>View</div> <div>Edit</div>
Default: 0107787298-00001	Default: 0107787298-00001	0107787298-00001	10938	<div>View</div> <div>Edit</div>

# Software Management

Use the *Software* page to keep your IoT device software current with the latest firmware using our firmware-over-the-air (FOTA) services. Here you can manage firmware or software that is available to download to devices.

For new update packages to appear in the ThingSpace portal, the following prerequisites must be in place:

- **Account eligibility** – You must have an existing ThingSpace account with an Enterprise ID and Unified Web Service credentials. You can get these from your Verizon account representative.
- **License availability** – You must have ThingSpace software management licenses (bundled or a la carte) available on your account. You can get these from your Verizon account representative. This is included for IoT marketplace users.
- **Device eligibility** – You must have certified devices on your account that have qualified FROM firmware version loaded.
- **Certified package** – Verizon must have certified a qualified FROM version — TO version upgrade path package and published it for use.
- **Ready for campaign** – You see that FOTA campaign is available for eligible firmware on eligible devices.

**NOTE:** A subscription to ThingSpace Software Management Services is required for Manage Software access.

Manage

Devices

Device groups

**Software**

Subscriptions

Users

Monitor

Alerts

Campaigns

Dashboards

Downloads

Logs

Reports

Automate

Cloud connectors

Geofences

Rules

Scheduled reports

Manage > Software

Software

2

1

Search by Software name

982 Results

Software name	Pilot verified	Protocol	FOTA make
<input type="radio"/> FW-7889-5787-1		OMADM	Qualcomm
<input type="radio"/> Test App 100	Not Verified	HTTP	VERIZON
<input type="radio"/> Test App 100	Not Verified	HTTP	VERIZON
<input type="radio"/> Test App 78		MODEL-A	Qualcomm
<input type="radio"/> Test App 0		HTTP	Verizon
<input type="radio"/> Sierra_Wireless_MC7354_1103925_9902266_MC7354_05_0		OMADM	Sierra Wireless
<input type="radio"/> Sierra_Wireless_MC7354_1103925_9902266_MC7354_05_0		OMADM	Sierra Wireless
<input type="radio"/> Test_Wireless_MC7354_11039277		OMADM	TEST Wireless
<input type="radio"/> Sierra_Wireless_MC7354_1103925_9902266_MC7354_05_0			Sierra Wireless
<input type="radio"/> FOTA_Verizon_Model-A_01To02_HF			Verizon
<input type="radio"/> FW-7889-5787-1			Qualcomm
<input type="radio"/> FW-7889-5787-1			Qualcomm
<input type="radio"/> FOTA_Verizon_Model-A_54To55_HF_LW_MOTIVE		LWM2M	Verizon
<input type="radio"/> FOTA_Verizon_Model-A_62To63_HF_LW_MOTIVE		LWM2M	Verizon

Show

100

per page



<

1

2

>

## Elements on the Software page

1		<a href="#">Search</a> – Locate a specific software by name.
2		<a href="#">Campaign</a> – Create a strategy to update software.



## Searching for Software

Type a software name in the **Search** field at the top-left of the *Software* page to locate the software.

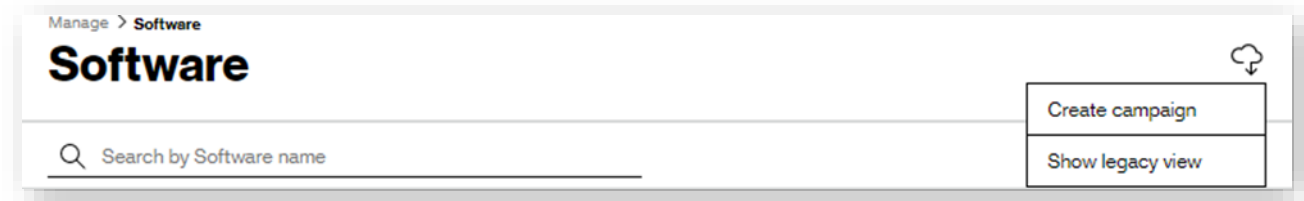
**NOTE:** Search does not support wildcard characters at this time.



**NOTE:** Searches are not case sensitive.

## Taking Actions


A menu of action items is available at the top-right of the *Software* page.



### Create a campaign

#### How to create a campaign

On the left navigation, click **Software**. The *Software* page opens.

1. Select a software name from the list of available software. You can only select one software option at a time.
2. Click the campaign icon  and select **Create campaign**. The *Create campaign* page opens when one or more device is eligible for the new software.
3. Follow the Create a campaign wizard to complete the creation of your campaign.

### Show legacy view

#### How to view the legacy Software Management page

On the left navigation, click **Software**. The *Software* page opens.

Click the campaign icon , and select **Show legacy view**. The legacy *Software* page opens.

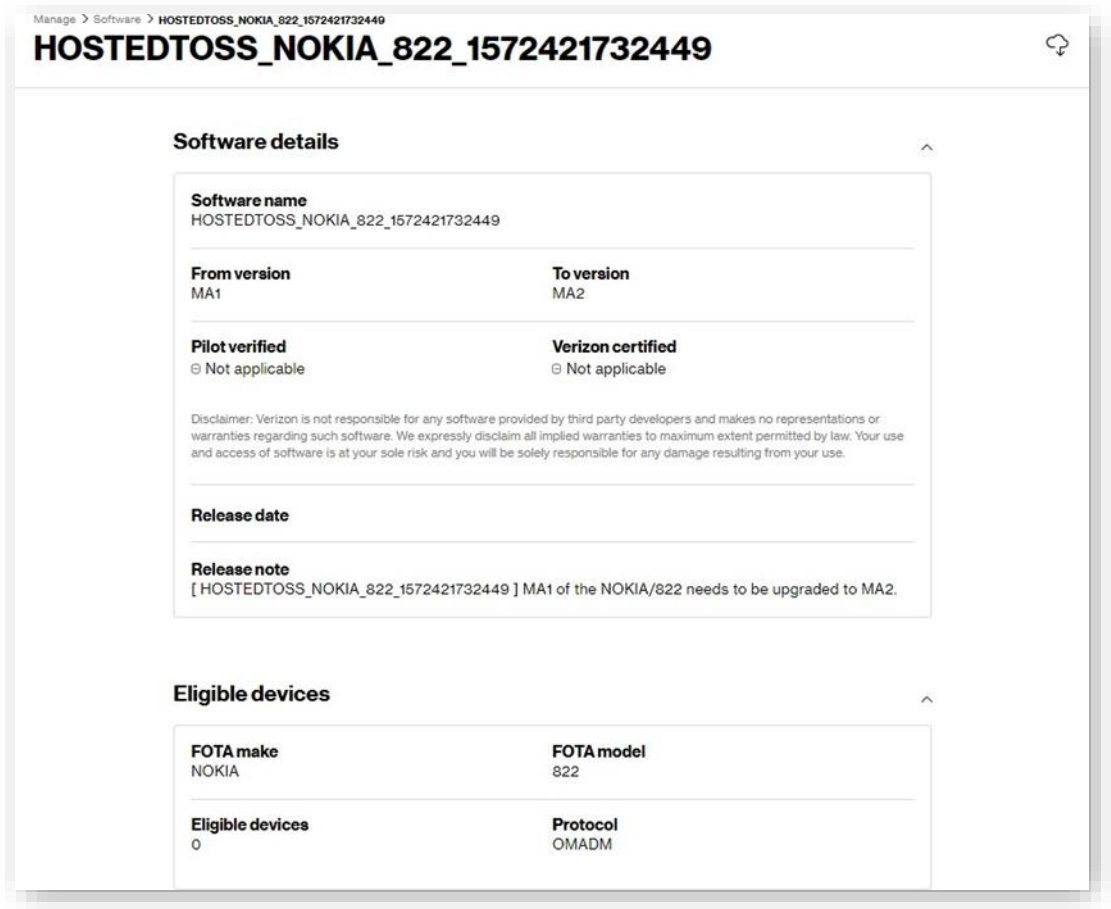
## Software Details


The *Software details* page provides metadata about the software itself. You can view the prerequisites required: make, model and from version as well as the anticipated target (to) version. Other details include the protocol that is being used, the level of testing (whether it is Verizon certified or pilot verified) that has been done. You can also create a campaign based on the eligible devices that meet the criteria.

How to view software details

On the left navigation, click **Software**. The *Software* page opens.

1. Click the **Software name** to view. The *Software Details* page opens with details about the selected software.



2. Click the campaign icon  to create a campaign, or go to the legacy view.

The following information is available in the *Software Details* page.

## Software Details

The *Software details* section provides the following information:

Software details

Software name

HOSTEDTOSS\_NOKIA\_822\_1572421732449

From version

MA1

To version

MA2

Pilot verified

☐ Not applicable

Verizon certified

☐ Not applicable

Disclaimer: Verizon is not responsible for any software provided by third party developers and makes no representations or warranties regarding such software. We expressly disclaim all implied warranties to maximum extent permitted by law. Your use and access of software is at your sole risk and you will be solely responsible for any damage resulting from your use.

Release date

Release note

[ HOSTEDTOSS\_NOKIA\_822\_1572421732449 ] MA1 of the NOKIA/822 needs to be upgraded to MA2.

## Eligible Devices

The *Eligible devices* section provides the following details:

Eligible devices

FOTA make

NOKIA

FOTA model

822

Eligible devices

0

Protocol

OMADM

# Subscriptions

Use the *Subscriptions* page to view all of the available ThingSpace Services, which are subscription based services that may be added to your account. The *Subscribed* section contains a list of all your subscribed services. Any services you are not subscribed to are listed in the **Available** section. You can click on **learn more** to access additional information for each service.

Manage > Subscriptions

## Subscriptions

---

### Subscribed

**SIM-Secure**

SIM-Secure binds a SIM to your device, preventing a malicious actor from moving the SIM to an unauthorized device. If your SIM is removed from the authorized device, SIM-Secure prevents it from successfully authenticating to the Verizon network.

[View devices](#)

---

**Software management**

Software Management reports the running software on your IoT devices and allows you to update them. It gives you access to deliver your over-the-air updates either through ThingSpace Manage or via representational state transfer (REST) APIs. Once a new update is available, you can schedule your remote update campaigns at a time that best suits your needs. This puts you in control, so you don't have to be dependent on an OEM/module maker to push the updates your way.

[View campaigns](#)

---

**Advanced diagnostics**

Diagnose your device and network connection health using ThingSpace Diagnostics Services. Decrease troubleshooting steps and learn how the Verizon Network sees your devices. For select devices this service also enables monitoring device connectivity performance in near real time or historically.

[View devices](#)

---

**Intelligence**

ThingSpace Intelligence is a set of value-added cloud platform services that make network and device management easier and smarter for IoT customers. ThingSpace Intelligence offers a suite of integrated services to manage IoT deployments and lifecycle, specifically for troubleshooting, billing, and security use cases.

ThingSpace Analytics is a new capability within the ThingSpace Intelligence suite of services. Analytics is a new way to understand your connectivity data through interactive visualization dashboards.

[View dashboards](#)

---

**Location**

Verizon's ThingSpace platform enables location-based services to easily track device location and enable geolocation services for your applications. Generate location reports, manage consent and privacy, view location history and even receive alerts when your assets move outside of their expected location.

[View location console](#)

---

**Hyper precise location**

Hyper Precise Location solution provides centimeter-level location accuracy. Verizon has built and deployed Real Time Kinematics (RTK) reference stations nationwide to provide pinpoint level accuracy to RTK compatible IoT devices. IoT devices currently using RTK can be accessed and managed through Verizon's ThingSpace platform portal and APIs.

[View devices](#)

---

# User Management

Use the *Users* page to view the list of users that have access to your organization's accounts. On the left navigation, click **Users** to open the page.

Manage

Devices

Device groups

Software

Subscriptions

**Users**

Monitor

Alerts

Campaigns

Dashboards

Downloads

Logs

Reports

Automate

Cloud connectors

Geofences

Rules

Scheduled reports

Manage users

User groups

Preferences

App log

343 Users - VZW M2M TEST ORG

Actions + 🔍 +

<input type="checkbox"/>	Name	Email	Accounts	Role	Active
<input type="checkbox"/>	*****	*****@verizon.com	00001, -00001...	Administrator	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com	00001, -00001...	Alerts Only User	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>Off</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>On</div>
<input type="checkbox"/>	1, Test	Test1@gmail.com		Alerts Only User	<div>On</div>
<input type="checkbox"/>	a, reddy	joshitha@verzionrfgdfgdfg1532416...	-00001, -00001...	Unified Web Services	<div>On</div>
<input type="checkbox"/>	A, Taf	*****@verizon.com	-00001, -00001...	Administrator	<div>Off</div>

**NOTE:** You are only able to create Alerts Only and Unified Web Services (UWS) users. Use MyBiz Profile Administration to add regular portal users.

**COMING SOON:** The ability to manage all users.

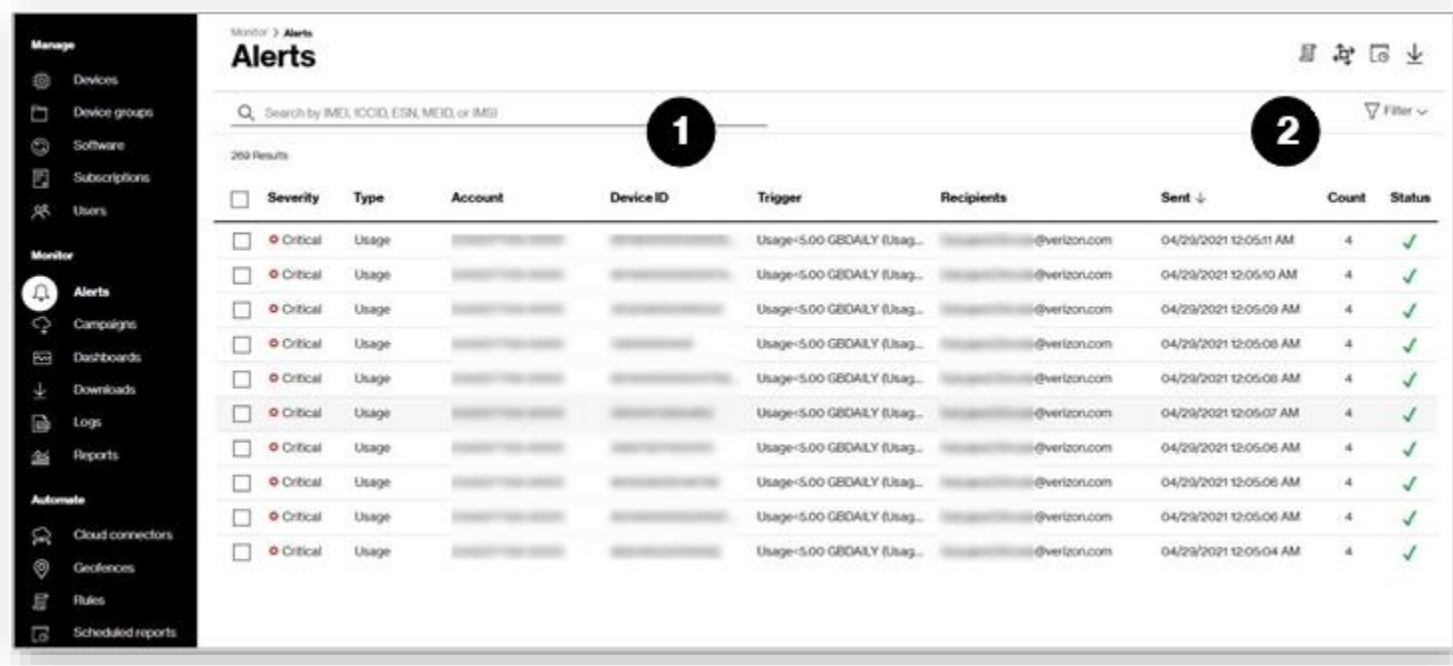
# Alerts

ThingSpace includes a notification feature that alerts groups of users when a value or status associated with a device changes, specific device events occur, or when certain data thresholds are breached. For example, you can establish a rule that notifies a field service technician when a remote device is consuming too much data or too little data, indicating a malfunction. When the conditions of a notification rule are met, the system sends out a message using the media (email or SMS) specified for each recipient. Use the *Alerts* page to view these notifications.

When an initial notification is sent and, if it is not acknowledged by one of the users in the notification group, up to three subsequent messages are sent at an hourly interval (maximum = 4). The system resends a notification message only when a notification has not been acknowledged.

Any user defined in the notification’s target group can acknowledge a notification. Notifications are acknowledged from the Notification Log screen only.

**NOTE:** The content of a notification message is preformatted and you cannot change it.



Elements on the Alerts page		
1		<a href="#">Search</a> – Locate an alert by device identifier.
2		<a href="#">Filter</a> – Limit the list to only alerts having specific attributes.

## Searching Alerts



Use the **Search** field to search for devices by IMEI, ICCID, ESN, MEID, or IMSI. Wildcard (%) search is supported for Device IDs.

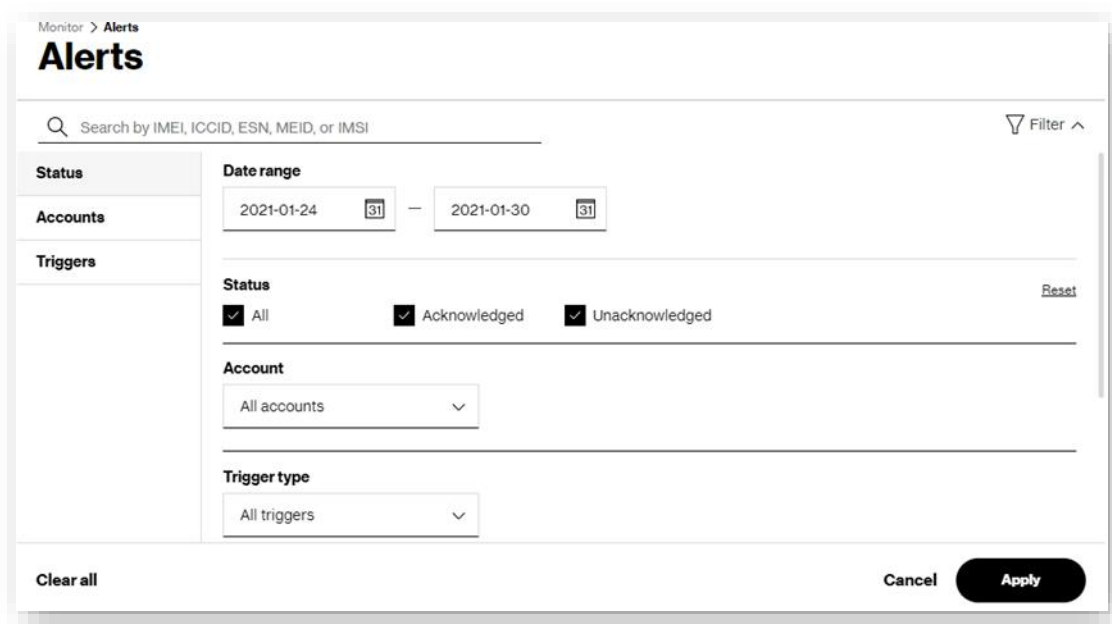


## Applying Filters

### How to apply filters

On the left navigation, click **Alerts**. The *Alerts* page opens.

Click the filter icon  **Filter** . The *Filters* page opens.



1. Click on each left navigation page, or scroll through the list to view all available filters.
2. Select the desired filters.
3. Click **Reset** in a filter category to select all filters in that category. To apply a date ranger filter, enter a date range of no more than 31 days.
4. Click **Apply**. The count of filters applied displays.



## Acknowledging Alerts

Alerts that are not acknowledged are set to send scheduled reminders. To stop receiving reminders, you must acknowledge the alert. To acknowledge an alert, click the check mark in the Actions column for the appropriate alert. When the alert is acknowledged, the checkmark changes from gray to green.



You can also perform bulk acknowledgements.

### How to acknowledge alerts in bulk

1. Select each alert checkbox.
2. Click the actions icon  and then select **Acknowledge** to complete the process.

# Campaigns

Use the *Campaigns* page to manage software upgrade campaigns.

To open the *Campaigns* page

On the left navigation, go to **Campaigns**. The *Campaigns* page opens.

The screenshot displays the 'Campaigns' page in the ThingSpace Manage v2.0 interface. The left sidebar is divided into three sections: 'Manage' (Devices, Device groups, Software, Subscriptions, Users), 'Monitor' (Alerts, Campaigns, Dashboards, Downloads, Logs, Reports), and 'Automate' (Cloud connectors, Geofences, Rules, Scheduled reports). The 'Campaigns' page is active, showing a list of 637 results. The table columns are: Campaign name, Campaign status, Start date, Software version (to), Included devices, FOTA make, and Actions. The table lists various campaigns with their respective statuses (Completed, Cancelled, Request Failed, Request Pending) and start dates. The bottom right corner shows pagination controls with 'Show 100 per page' and a page number '1'.

## Elements on the Campaigns page

1		<a href="#">Search</a> – Locate a campaign by name.
2		<a href="#">Campaign</a> – Open the Campaign menu.
3		<a href="#">Delete</a> – Permanently remove a campaign.

## Search for Campaigns

Use the **Search** field to locate campaigns by name.

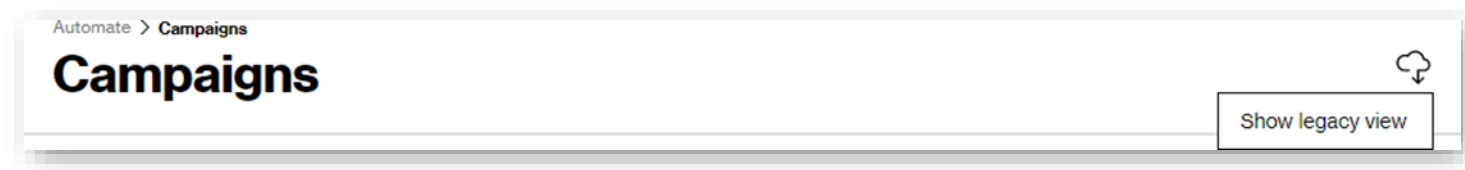
**NOTE:** Search does not support wildcards for campaign name.



**NOTE:** Searches are not case sensitive.

## Taking Actions

The *Campaigns* page action menu contains the *Show legacy view* action.



## Deleting a Campaign

**NOTE:** Only campaigns that have not been started are able to be deleted.

### How to delete a campaign

On the left navigation, click **Campaigns**. The *Campaigns* page opens.

Click on the Campaign's delete icon . The Campaign is removed from the list.

## Campaign Details

Use the *Campaign details* page to view upgrade status. View details of your campaign, including reports on the devices that were included in the campaign, state of the campaign metadata, start dates, the software included, specific device information, such as what devices are included in the campaign, and the status of the upgrades.

To view campaign details

On the left navigation, click **Campaigns**. The *Campaigns* page opens.

Click the **Campaign name**. A *Campaign details* page opens with details about the selected campaign.

Automate > Campaigns > 27c9a8ab-7d66-46c7-825d-1dac017b5c07

27c9a8ab-7d66-46c7-825d-1dac017b5c07

Completed

Download

Software name

Campaign ID

27c9a8ab-7d66-46c7-825d-1dac017b5c07

FOTA make

FOTA model

From version

1102788\_9902266\_SWI9X15C\_05.05.58.99\_0\_0\_VZW\_005.032\_099

To version

1102788\_9902266\_SWI9X15C\_05.05.58.05\_0\_0\_VZW\_005.032\_000

Start date

Jan 22, 2019

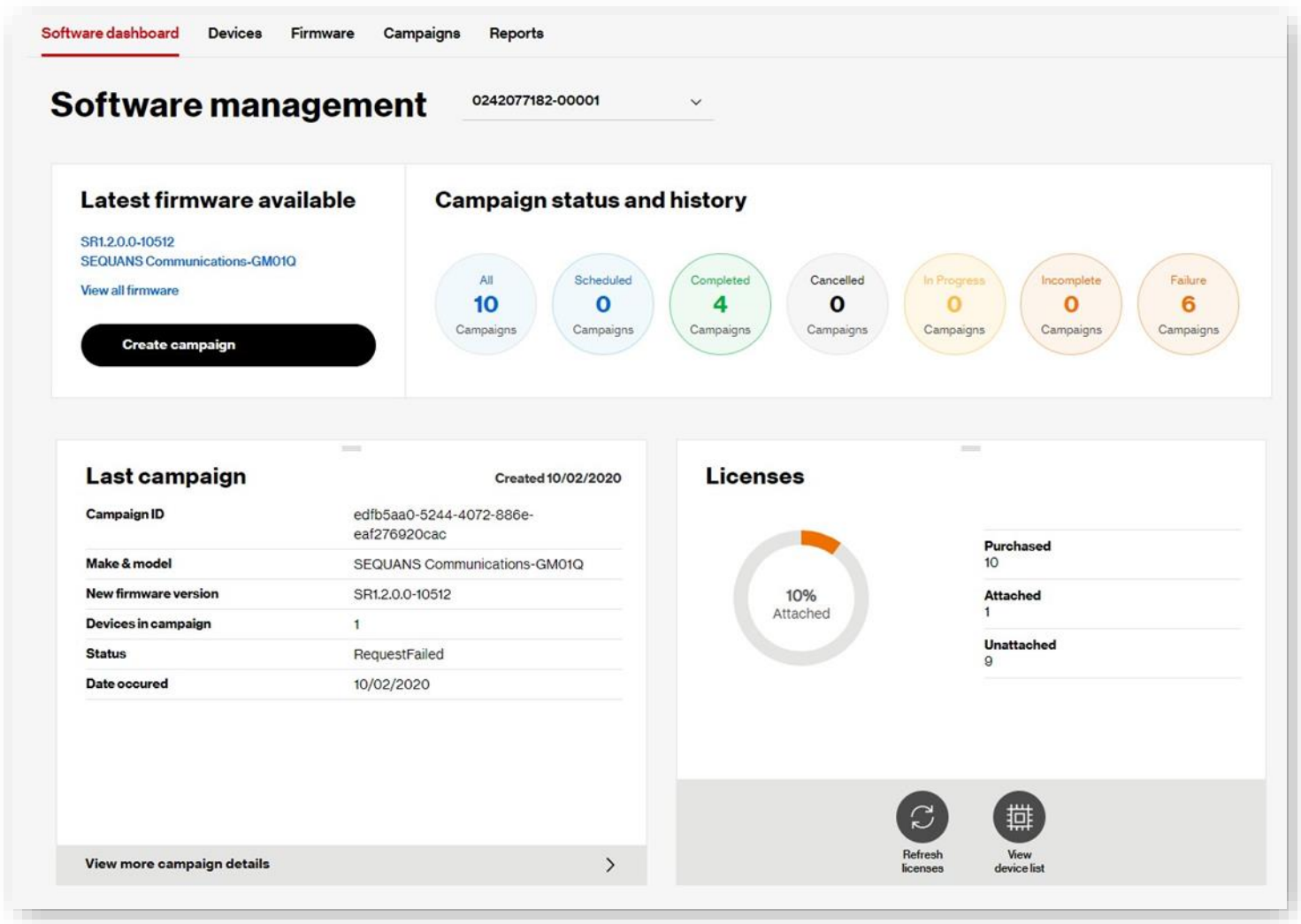
End date

0 Results

Device identifier	Status	Details
359225055602569	UpgradeFailed	Firmware update to device failed

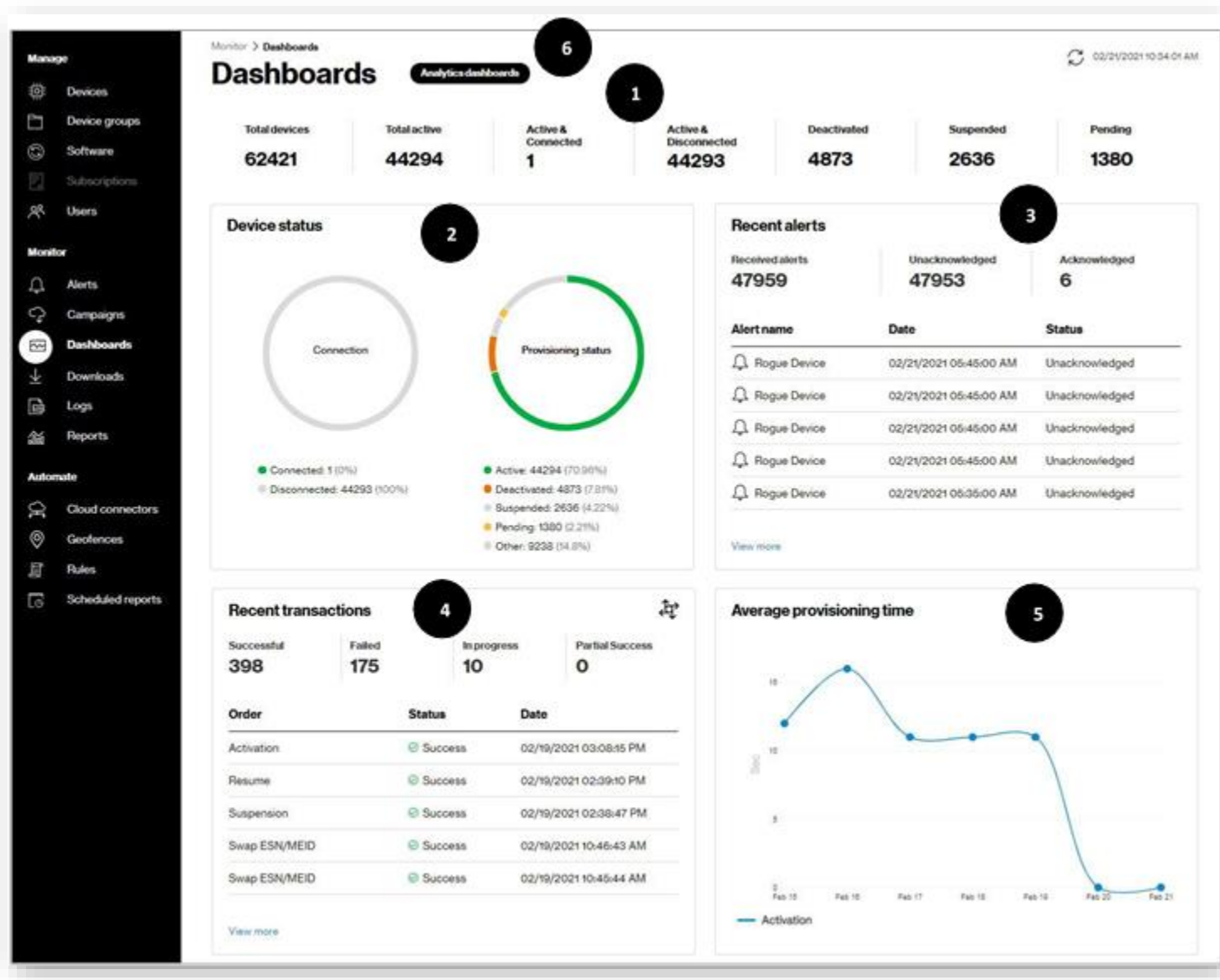
# Legacy View

The legacy *Software management* page is shown below.



## Dashboards

The *Dashboards* page provides a system overview, quick searches, filters, and useful navigation links. Use this page to get a snapshot of your account, total number of devices, and all connected, suspended, or deactivated devices. The *Dashboards* page is available from the left navigation and is set as the default home page for first-time users. You can change your default home page in [Settings](#).



**COMING SOON:** The ability to customizable your dashboard and arrange pods to your business needs.

Elements on the Dashboard	
1	Device Status filters
2	<a href="#">Device Status pod</a>
3	<a href="#">Recent Alerts pod</a>
4	<a href="#">Recent Transactions pod</a>
5	<a href="#">Average Provisioning Time pod</a>
6	<a href="#">Analytics Dashboards</a>

Device Status Filters

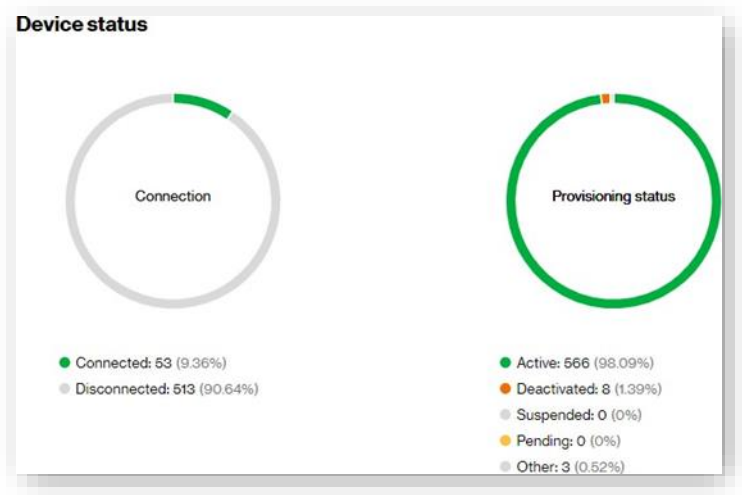
The device status filter results display along the top of the page. These filters show the device counts on a company’s account, along with the total active, active-connected, active-disconnected, deactivated, suspended, and pending. Click a filter name to open the [Devices](#) page with devices that correspond to the selected filter. For example, click **Total Devices** to open the *Devices* page with a list of the total number of devices.

Total devices	Total active	Active & Connected	Active & Disconnected	Deactivated	Suspended	Pending
577	566	53	513	8	0	0

**COMING SOON:** See how many devices are in Pre-active status.

## Device Status Pod

The *Device status* pod uses color-coded pie charts to show the connectivity and provisioning status for devices. Clicking in the **Connection** or **Provisioning** circle opens the *Devices* page listing devices with their connection and provisioning status. Clicking on the links the pie chart has the same result.



## Recent Alerts Pod


The *Recent alerts* pod contains filters and a recent alerts list.

Three filters at the top of the pod show the total number of received, unacknowledged, and acknowledged alerts. The table below the filters lists the five most recent alerts, the date and time when they occurred, and their status.

Recent alerts		
Received alerts 149	Unacknowledged 147	Acknowledged 2
Alert name	Date	Status
Deactivation Request	08/27/2020 12:05:32 PM	Unacknowledged
Deactivation Request	08/27/2020 12:05:30 PM	Unacknowledged
Deactivation Request	08/27/2020 12:05:28 PM	Unacknowledged
Activation Request	08/27/2020 12:04:14 PM	Unacknowledged
Activation Request	08/27/2020 12:04:11 PM	Unacknowledged
<a href="#">View more</a>		



## Recent Transactions Pod

The *Recent transactions* pod contains filters along the top of the pod showing the total number of recent transactions that were performed successfully, are in progress, or have failed. The table that follows these filters lists the five most recent provisioning orders, their status, and the date and time when they occurred. Clicking on an order takes you to the *Log Details* for the order. The actions icon  allows you to quickly run bulk transactions with a single click.

Recent transactions

Successful  
366

Failed  
55

In progress  
3

Order	Status	Date
Deactivation	Failure	01/26/2021 08:00:55 AM
Change Service Plan	Failure	01/26/2021 08:00:36 AM
Resume	Failure	01/26/2021 08:00:07 AM
Suspension	Failure	01/26/2021 07:59:17 AM
Activation	Success	01/26/2021 07:55:53 AM

[View more](#)

Select

Activate

Change cost center

Change custom fields

Change device group

Change service plan

Change wireless number

Swap devices

Suspend

Resume

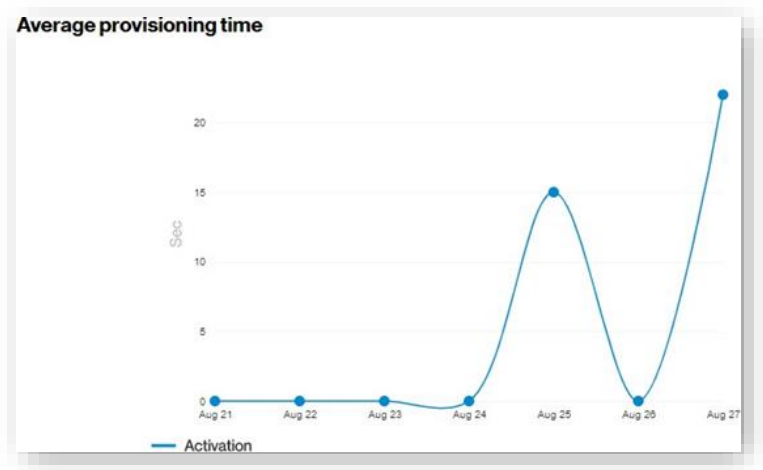
Deactivate

Upload devices

## Average Provisioning Time Pod

The *Average Provisioning Time* pod shows a graph with an average of device activation time, by day, over the last seven days (from the time the activation order was submitted until the order completes).

**NOTE:** Additional transaction support is planned for a future release.

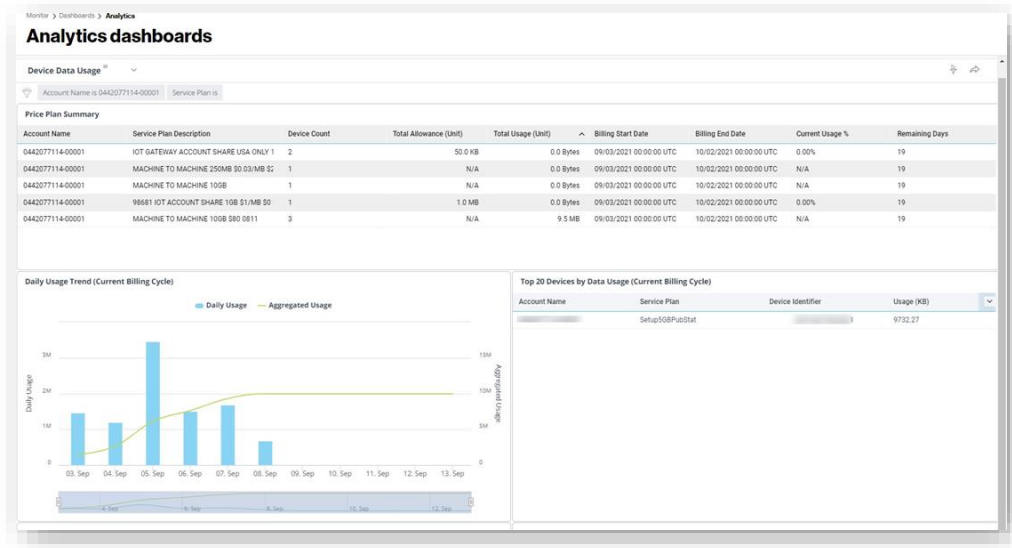


## Analytics Dashboards

*ThingSpace Analytics* is a new capability within the ThingSpace Intelligence suite of services. ThingSpace Intelligence subscribers can use the Analytics dashboards to understand connectivity data through interactive visualization dashboards. Also included in ThingSpace Intelligence service is access to the [Wireless Network Performance](#) tool, which offers deeper insights into the Verizon network.

Contact your Verizon representative for additional information, and to subscribe to this feature.


On the left navigation, go to **Dashboard > Analytics dashboards** to open the page.



## Filtering

Apply quick filters and custom filters across all dashboard elements (all charts).

### To apply filters to all charts

1. Click the filter icon  below the view title in the upper-left of the page. The *Filters* dialog opens.
2. Select existing filters or build a custom filter. To apply existing filters, click one or more toggle(s).

## To build a custom filter

Click **Add**. The *Edit filter* dialog opens.

1. Select the Field to filter.
2. Select the Condition type.
3. Select the *Value* to filter on.
4. Click **Save**.

You can also click a chart filter icon  to apply separate filtering for just that chart.

### Search

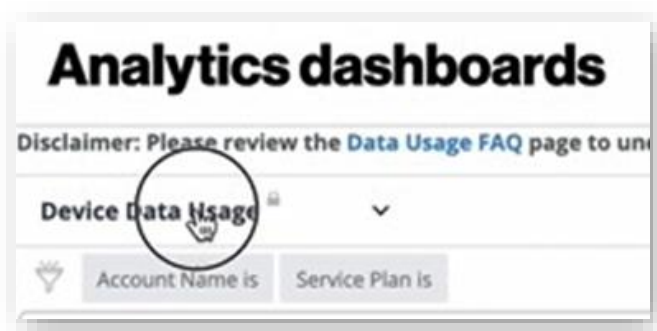
Click the search icon  to type a keyword, or click the Natural Language Processor icon  to type a question.

### Export Data

You can export individual charts into multiple formats. Visualizations may export to images, tabular data may export to CSV or XLS files. You can also download filtered data to a PDF file. Click the pen in the *Share and Email Options* dialog and click **Export as PDF**.

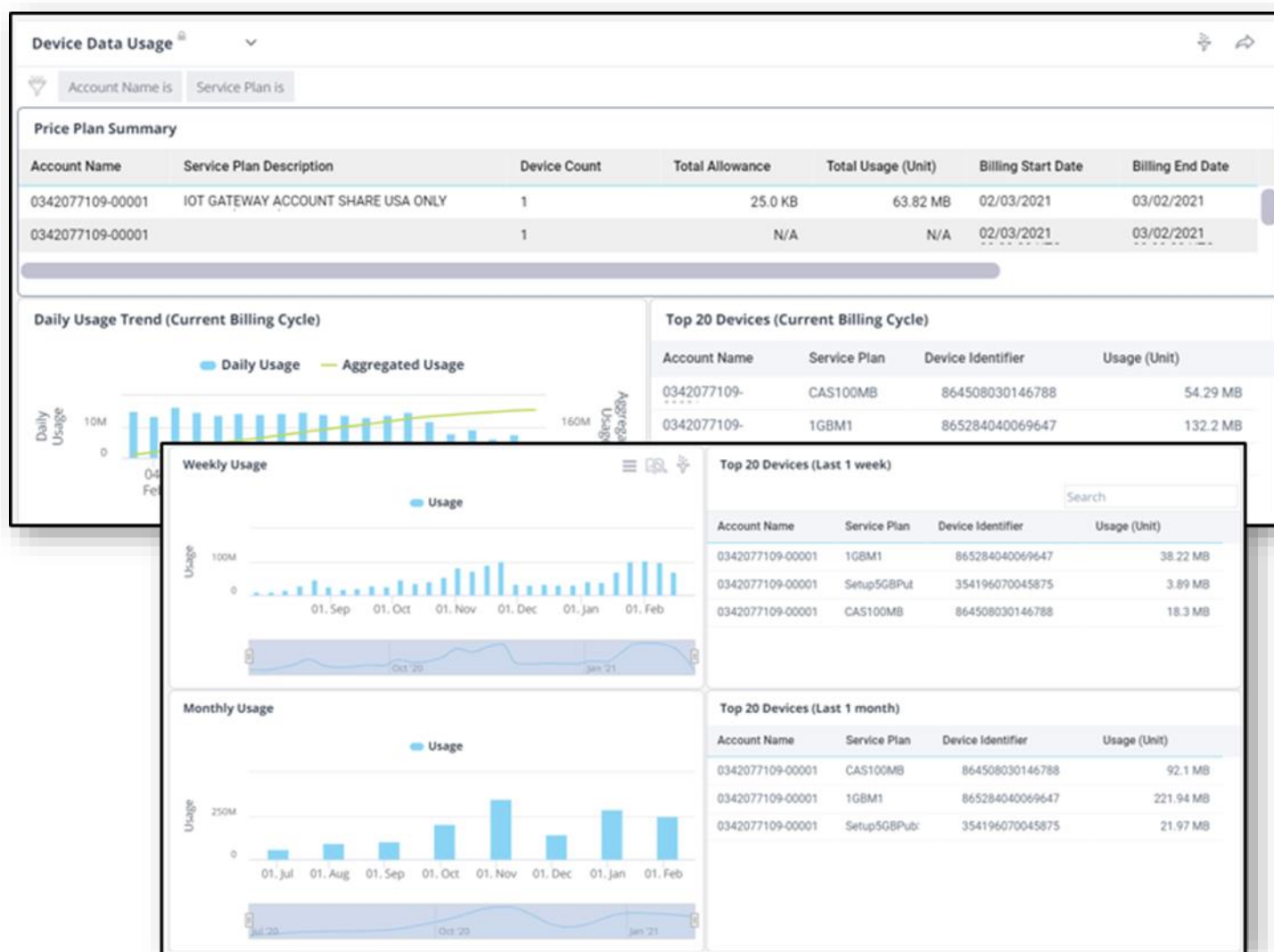
### Analytics Dashboard Views

Click the view menu to select one of the following views.

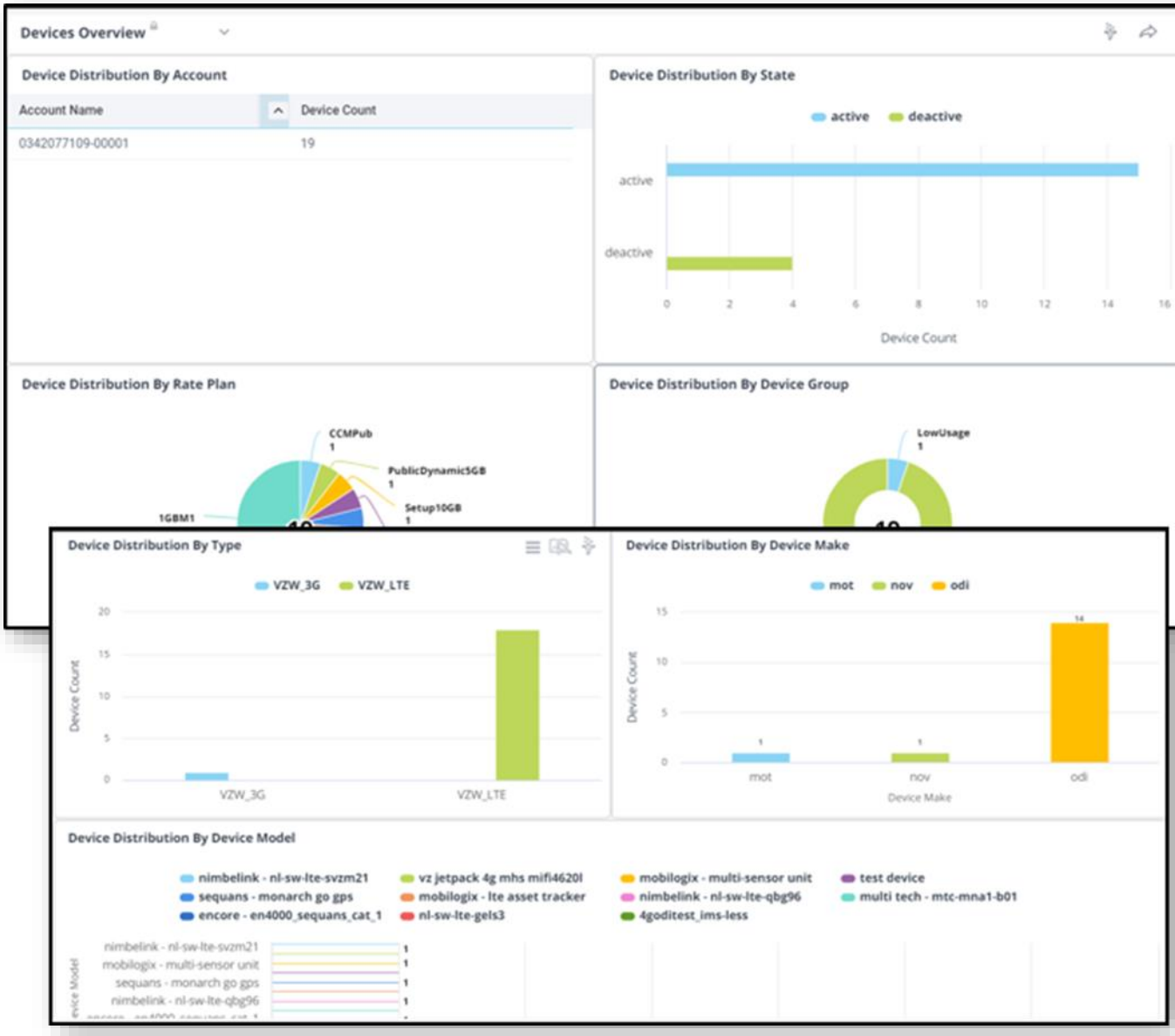


## ThingSpace Manage v2.0 – User Guide

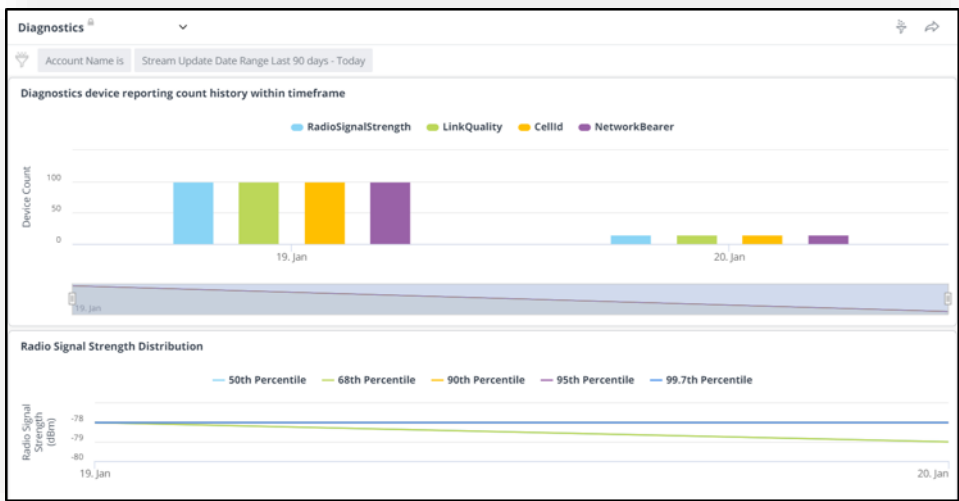
*Device Plan Data Usage* dashboard provides insights into aggregate usage trends on a daily and cumulative basis. You can also see devices with top data usage within the billing cycle, the last seven days, and the last 30 days.



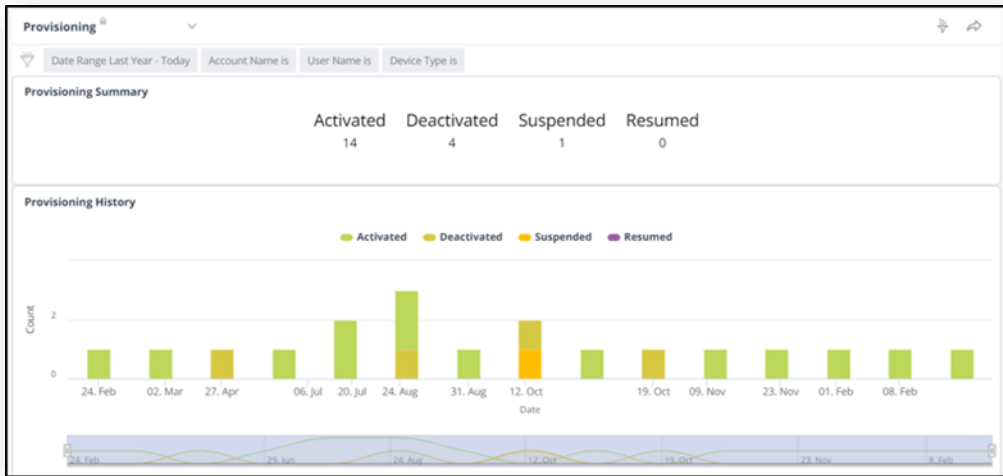
Devices Overview dashboard provides insights into device attributes and distributes, such as states, rate plans, groups, make and model, etc.



Diagnostics analytics dashboard provides insights into LWM2M diagnostic streaming events if compatible LWM2M devices are streaming.

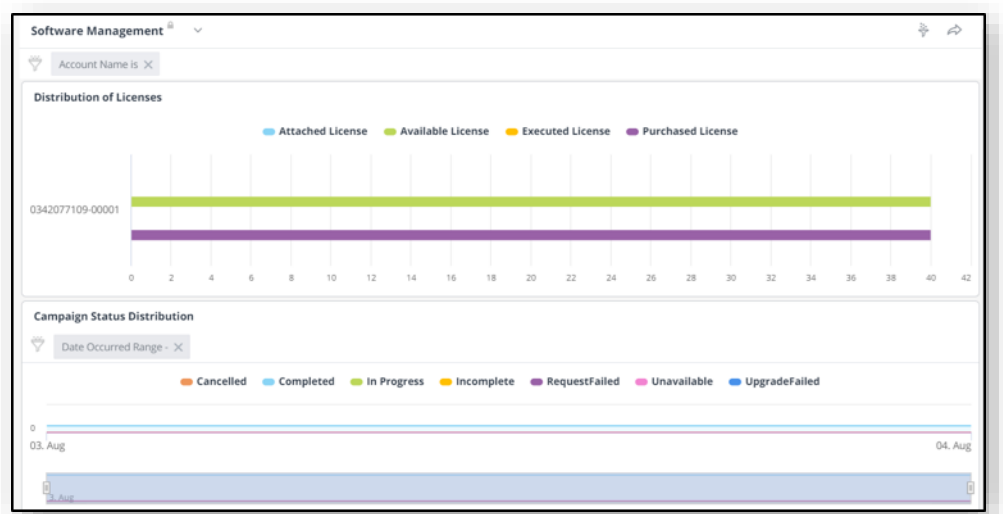


Provisioning analytics dashboard provides insights into provisioning history.

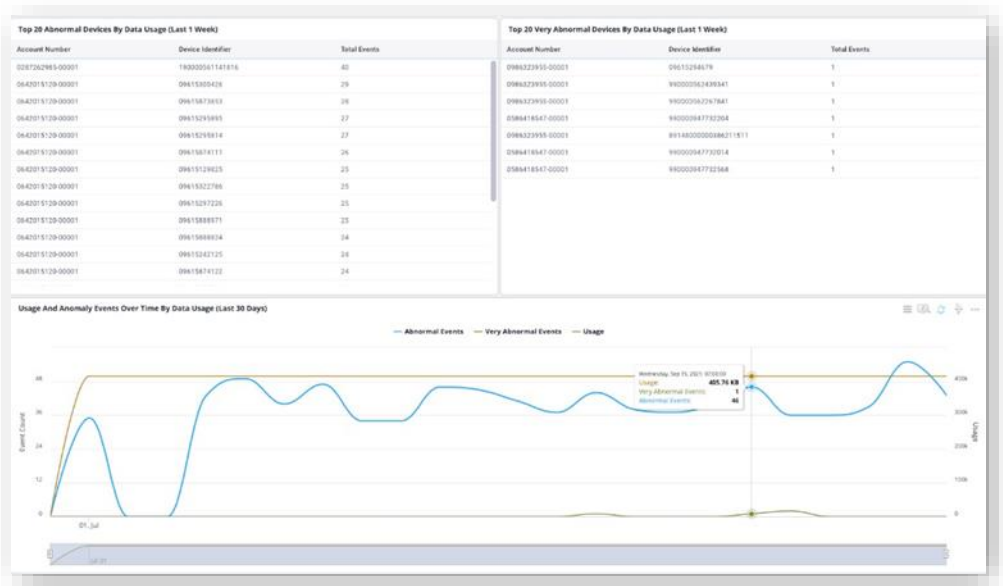


ThingSpace Manage v2.0 – User Guide

Software Management and SIM-Secure analytics dashboards provide insights into license utilization and campaign history (if available).



For users subscribed to the ThingSpace Intelligence premium bundle, an **Anomaly detection** dashboard view is also available.



The anomaly charts display the top 20 anomalous devices by data usage. Those devices can be run in the reports page to retrieve any anomalous event. These charts can be useful to gauge the # of anomaly events at a macro level. For example, if many devices suddenly spiked in usage this chart would highlight the trend and spikes.

## Wireless Network Performance

Wireless Network Performance (WNP) is a My Business analytics tool that offers deeper insights into your Verizon network device data. WNP is available in Basic and Premium tier. ThingSpace Intelligence subscribers can use WNP, which is available in Basic and Premium tier. The Intelligence bundle includes WNP when ordered in basic (licensed) or tiered plans.

Open WNP from the [Verizon Apps](#) menu .



The screenshot displays the Verizon Wireless Network Performance (WNP) dashboard. At the top, the Verizon logo is on the left, and the user's name 'Hi, Khamsi' is on the right. The 'WNP' header is prominently displayed. Below the header, there is a navigation bar containing a date selector set to '09/08/2021', a dropdown menu for '-- Select Or Type Company Name--', another dropdown for '-- Select By --', and buttons for 'Go' and 'Report Filters'. The central part of the dashboard is a map of the United States, showing major cities and state boundaries. On the right side of the map, there is a sidebar with a list of service status options: 'Service Status', 'Check My Saved Locations', 'Check My Service', 'Device Locations', 'Near Real-Time LTE Coverage Map', 'Site Proximity', and 'VZ Coverage Map'. At the bottom of the map, there is a disclaimer: 'Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement. Leaflet | Powered by Esri'.



# Downloads

The *Downloads* page lists all the files that are available for downloading.

On the left navigation, click **Downloads** to open the page.

**Downloads**

File type: ☒ XLSX ☐ CSV


Report name	Report type	Date/time created	File size	File status
Download icon	Connected Session Hist...	02/20/2021 12:00:30 AM	0.19 KB	Delivered
Download icon	Daily Usage Report	02/20/2021 12:00:22 AM	0.11 KB	Delivered
Download icon	Devices	02/19/2021 04:39:00 AM	8966.9 KB	Complete
Download icon	Aggregated Device Usage...	02/19/2021 04:28:14 AM	0.49 KB	Complete
Download icon	Connected Session Hist...	02/19/2021 04:01:16 AM	0.68 KB	Downloaded
Download icon	Connected Session Hist...	02/19/2021 04:01:09 AM	0.68 KB	Downloaded
Download icon	Connected Session Hist...	02/19/2021 03:59:41 AM	0.68 KB	Downloaded
Download icon	Connected Session Hist...	02/19/2021 01:19:09 AM	2.52 KB	Delivered
Download icon	Connection History Rep...	02/19/2021 01:17:06 AM	1.07 KB	Downloaded
Download icon	Aggregated Device Usage...	02/19/2021 12:17:01 AM	0.31 KB	Delivered
Download icon	Connection History Rep...	02/19/2021 12:00:23 AM	0.21 KB	Downloaded
Download icon	Service State Transition ..	02/19/2021 12:00:14 AM	0.12 KB	Delivered
Download icon	Connected Session Hist...	02/19/2021 12:00:05 AM	0.19 KB	Delivered
Download icon	Daily Usage Report	02/19/2021 12:00:05 AM	0.18 KB	Delivered
Download icon	Connected Session Hist...	02/18/2021 09:39:41 AM	15.61 KB	Complete
Download icon	Connection History Rep...	02/18/2021 09:41:05 AM	0.21 KB	Complete

Show 100 per page

## Elements on the Downloads page

1		<b>File Type options</b> – Select the file format to download.
2	↓	<b>Download</b> – Export the file.

### How to download a report

- At the top-right of the *Downloads* page, click the **File type** of your choice (XLSX or CSV).
- Click the *Report name* download icon . The file exports to your device

# Logs

The *Logs* page is a list of submitted provisioning transactions.

On the left navigation, click **Logs** to open the page.

**NOTE:** This is the equivalent of the *Transactions* page in legacy ThingSpace Manage.

Manage

Devices

Device groups

Software

Subscriptions

Users

Monitor

Alerts

Campaigns

Dashboards

Downloads

Logs

Reports

Automate

Cloud connectors

Geofences

Rules

Scheduled reports

Monitor > Logs

Logs

2-4

1

5

Search by Request ID, Device ID or MDN

Filter






553 Results

Request ID	Date	Order type	Status	Devices	Submitted by	Account
3fd385ea-a6eb-4899-9f08-ebbfeb19d672	02/19/2021 03:08:15 PM	Activation	Success	6	CHINTAN SHETH	1539-00001
7d990bc1-be6e-4974-89a6-7a5de4db0ff6	02/19/2021 02:39:10 PM	Resume	Success	2	CHINTAN SHETH	1439-00001
7aabdc33-da7e-47ab-bc88-932ef6067592	02/19/2021 02:38:47 PM	Suspension	Success	2	CHINTAN SHETH	1439-00001
52e3497a-bf57-4ef6-b4bd-16b9f9ac7013	02/19/2021 10:46:43 AM	Swap ESN/MEID	Success	1	Jie Liang	1539-00001
08ecd7db-eeec-480d-adad-5aa845433f22	02/19/2021 10:45:44 AM	Swap ESN/MEID	Success	1	Jie Liang	1539-00001
4c2ebd5e-9a97-4368-a412-799dbbfff7443	02/19/2021 10:45:44 AM	Swap ESN/MEID	Success	1	Jie Liang	1539-00001
5ae2256c-44c1-4f96-b0e4-7a1fe7261bf2	02/19/2021 10:45:34 AM	Swap ESN/MEID	Failure	1	Jie Liang	1539-00001
c6a53817-dc47-451d-bbd0-b2cabec08473	02/19/2021 10:41:11 AM	Swap IMEI ICCID	Success	1	Jie Liang	1439-00001
356272c2-94b3-420b-bb57-159a01fc8b29	02/19/2021 10:41:10 AM	Swap IMEI	Success	1	Jie Liang	1539-00001
d37d4014-5635-4a05-6716-c3211c337c55	02/19/2021 10:41:08 AM	Swap ICCID	Success	1	Jie Liang	1539-00001
df83e603-5ff9-4262-b5ae-a1753b007412	02/19/2021 10:35:32 AM	Change MDN	Success	1	Jie Liang	1539-00001
aa53945e-ce53-456b-a315-2118a5d2db90	02/19/2021 10:35:32 AM	Change MDN	Success	1	Jie Liang	1539-00001
ba553d5d-9ceb-4a99-8b5e-6930c288c3...	02/19/2021 10:35:32 AM	Change MDN	Success	1	Jie Liang	0844021539-00001
932b758d-bfac-4d2e-9233-6f4f2fa88e98	02/19/2021 10:35:32 AM	Change MDN	Success	1	Jie Liang	0844021539-00001

Show 100 per page

1 2 5 6 >

## Elements on the Logs page

1		<a href="#">Search</a> – Locate a specific log by request or device identifiers.
2		<a href="#">Actions</a> – Open the Logs action menu.
3		<a href="#">Show application log</a> – View and download the <i>Applications log</i> .
4		<a href="#">Download</a> – Export the list.
5		<a href="#">Filter</a> – Limit the list to logs with specific attributes.

## Searching Logs



Use search to view the log records that match the entered criteria. You can enter a Request ID or a Device ID to narrow your search results. Wildcard (%) search is supported for Device ID and MDN search only.

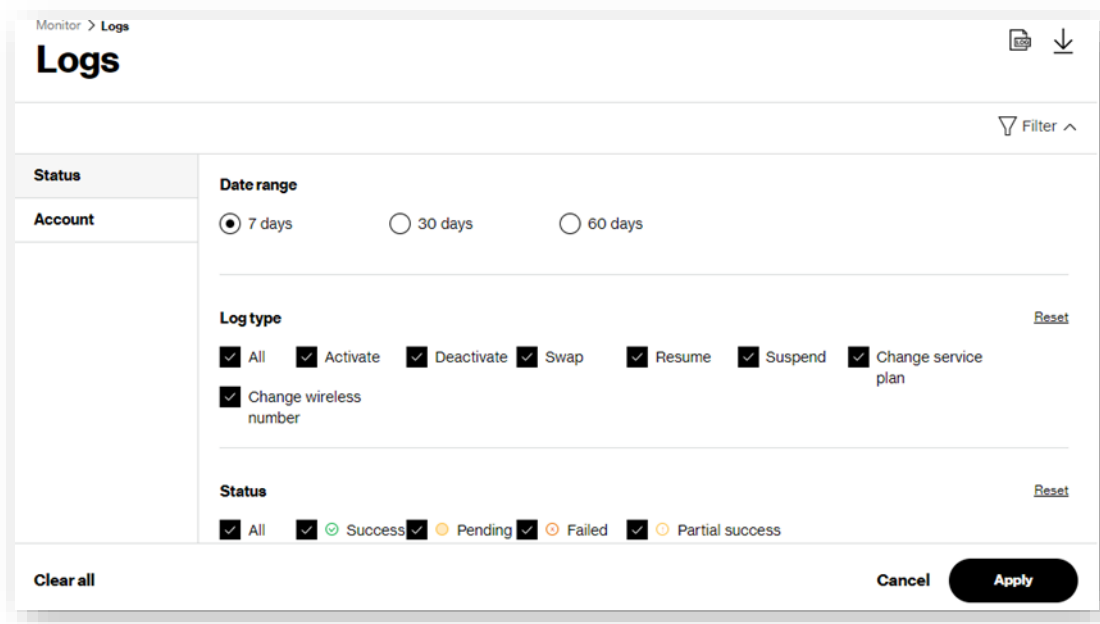


**NOTE:** Searches are not case sensitive.

## Applying Filters



### How to apply filters

Click  Filter . The *Filter* page opens.



Monitor > Logs

### Logs

 Filter 

**Status**

**Account**

**Date range**





☒ 7 days ☐ 30 days ☐ 60 days

**Log type** [Reset](#)

☒ All ☒ Activate ☒ Deactivate ☒ Swap ☒ Resume ☒ Suspend ☒ Change service plan

☒ Change wireless number


**Status** [Reset](#)

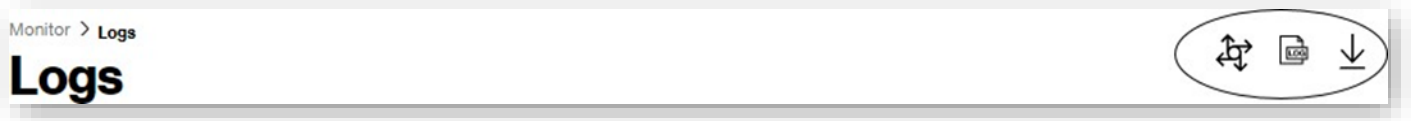
☒ All ☒  Success ☒  Pending ☒  Failed ☒  Partial success

[Clear all](#) [Cancel](#) [Apply](#)

1. Use the left navigation to view all available filters. Click **Reset** to select all filters in the category.
2. Click **Apply**. A count of filters applied appears with the filtered results.

## Taking Actions

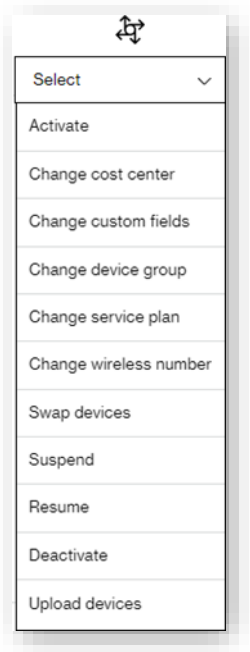
Use the actions icon  to display a menu of actions.



## Provisioning Actions

The majority of Logs page actions are provisioning actions, such as activate, change service plan, change wireless number, swap, suspend, resume, and deactivate. Other actions include revising cost center codes, custom field values, and device groups.

Administrators can also upload devices identifiers from this menu.




## View Application Log

### How to access the application log

Click the application logs icon . The legacy Application Log page opens.

## Download the Transaction Log

### How to download the transaction log


Click the download icon  to download the transaction log.

## Log Details

Click a Request ID to drill down into log details.

### To view log details

On the left navigation, click **Logs**. The *Logs* page opens.

1. Click a **Request ID**. The *Logs Details* page opens with details about the provisioning transaction.
2. Click the download icon  to download the details of the transaction. The following information is available in the Log details page.

Monitor > Logs > dddde539-9988-4f96-b8f6-2ebc254027a4

### Log details

Success
Activation

Service plan

IOT GATEWAY 100MB \$1/MB

Submitted by

jing luo

Submitted date

04/22/2021 07:09:27 PM

Request ID

dddde539-9988-4f96-b8f6-2ebc254027a4

Submitted

1

Success

1

Pending

0

Failed

0

Q

Search by Device ID or MDN

1 Results

Device Identifier	ICCID	IMEI	MDN/MSISDN	IP address	Status	Description
					Success	Device was moved from a different account

ThingSpace Manage v2.0 – User Guide

For Activation orders that have completed in the past seven days, you can click the status value (e.g. Success, Failed) to view the order status.

This is a **successful** activation order example.

Latest activation order

Updated: 2/5/21 9:17 PM

100 % Success

Account & Credit Verification

Device Validation

Number & IP Allocation

Provisioning Configuration

Network Registration

Order Completion

Device identifier:

Service plan: CCMPub

Billing account:

Progress	Status	Time	Message
Account & Credit Verification	Success	02/04/2021 05:20:21 PM	
Device Validation	Success	02/04/2021 05:20:21 PM	
Number & IP Allocation	Success	02/04/2021 05:20:22 PM	
Provisioning Configuration	Success	02/04/2021 05:20:26 PM	
Network Registration	Success	02/04/2021 05:20:28 PM	
Order Completion	Success	02/04/2021 05:20:35 PM	

The following is a **failed** activation order example. You can identify where in the provisioning process the transaction failed. In this example, the failure occurred in the Provisioning Configuration step because the device was already active on another line.

Latest activation order

Updated: 2/5/21 9:19 PM

16 % Failed

Account & Credit Verification

Device Validation

Number & IP Allocation

Provisioning Configuration

Network Registration

Order Completion

Device identifier:

Service plan:

Billing account:

Progress	Status	Time	Message
Account & Credit Verification	Success	02/04/2021 11:47:17 AM	
Device Validation	Error	02/04/2021 11:47:18 AM	
Number & IP Allocation	N/A		
Provisioning Configuration	Error		Device ID or ICCID not found in DMD
Network Registration	N/A		
Order Completion	N/A	02/04/2021 11:47:18 AM	Client callback sent.

# Application Log

The *Application log* page lists application actions users have made while in ThingSpace Manage.

On the left navigation, click **Logs** to open the legacy page.

Application log

Users

User groups

Preferences

224 logs

🔍

⬇

🔄

Date	Account	Device	User	Interface	Event type	Description
02/05/2021 09:37:24 PM				Application Log	AccessApplicatio...	Access to Application Log successful.
02/05/2021 09:37:16 PM				Application Log	AccessApplicatio...	Access to Application Log successful.
02/05/2021 09:37:08 PM				Manage Users	GetUsersList	Get users search successful.
02/05/2021 09:37:01 PM				Manage Users	GetUsersList	Get users search successful.
02/05/2021 09:36:53 PM				Manage Users	AccessManageUser...	Access to Manage users successful.
02/05/2021 09:34:34 PM				DeviceGroup	GetDeviceGroupsL...	Get device groups list successful.
02/05/2021 09:34:33 PM				DeviceGroup	GetDeviceGroupsL...	Get device groups list successful.
02/05/2021 09:34:32 PM				DeviceGroup	AccessManageDevi...	Access to Manage Device Groups successful.
02/05/2021 09:05:15 PM				Manage Users	GetUsersList	Get users search successful.
02/05/2021 09:05:07 PM				Manage Users	GetUsersList	Get users search successful.

Show per page

10

1

2

...

23

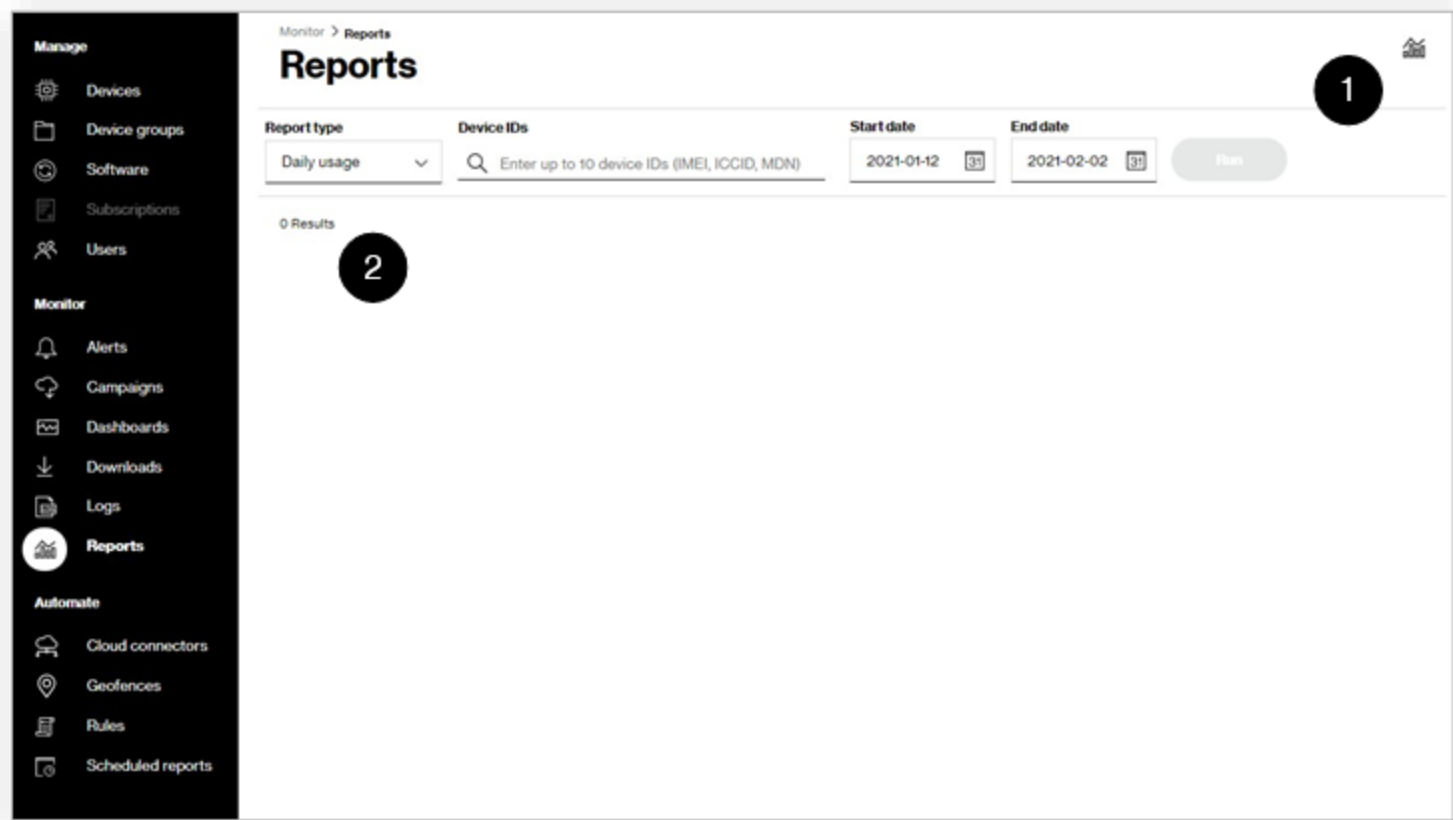
Next >



# Reports

Use the Reports page to run reports from a selected list over a period of time.

On the left navigation, click **Reports** to open the page.



## Elements on the Reports page

1		<b>Reports</b> – Create an advanced report
2		<b>Report type</b> – Open a menu to select a report category.


## Running Select Reports

### How run reports

On the left navigation, click **Reports**. The *Reports* page opens.

Select report criteria:

1. Select the **Report type**. The available report types are listed below with details in their own section. You can run these reports and get the results delivered quickly (online report), or submit them using the advanced reporting option and get the results when they complete (offline report). The maximum date range is 45 days for online reports.
  - Aggregated usage Daily usage Connection history
  - Hyper precise session history – Hyper Precise Location Services subscription required. Hyper precise aggregated usage – Hyper Precise Location Services subscription required. Location – for customers that subscribe to Location Services
  - Session history Rated unbilled usage
  - Usage anomaly – ThingSpace premium Intelligence bundle subscription required. Usage trending chart
2. Type up to 10 **Device IDs**
3. Select a Start date Select an **End date**
4. Click **Run**.

Alternatively, you can open the *Reports* page from the [Devices](#) page by selecting one or more devices and clicking the reports icon  and then choosing the report to run.

## Running Advanced Reports

Use the reports  icon to create, save, and/or schedule advanced reports. These reports usually take longer and are submitted in the backend for processing. Finished reports are available on the [Downloads](#) page.

Create and schedule a report

Select report type. Filter and schedule selections are optional.

Report type

Daily usage

IDs and dates

Accounts

Attributes

View

Schedule

Device IDs

Enter up to 10 device IDs (IMEI, ICCID, MDN Or IP Address)

Start date

2021-01-24

End date

2021-01-30

Run

## Aggregated Usage Report

Use the *Aggregated Usage Report* to track overall usage for all devices on your plan. This report includes sums for data and/or SMS usage within a specified date range. Usage for the current date is the accumulation from 12:00 AM to within approximately 15 minutes of the end of the latest data session, and to within approximately six hours for 4G devices that stay connected for extended periods.

**NOTE:** The offline reporting maximum date range is 12 months.

Monitor > Reports

### Reports

Report type: Aggregated usage (dropdown)

Device IDs: [Search bar]

Start date: 2021-01-24 (calendar icon)

End date: 2021-01-30 (calendar icon)

[Run button]

1 Result

Device identifier	MDN	Account	ESN	MEID	IMEI	ICCID	IP address
							100.71

## Daily Usage Report

Use the *Daily Usage Report* to establish normal usage patterns by examining daily usage. This report provides a breakdown, by day, of the amount of data transported to and from a device, or a list of devices within a specified date range. The daily usage period is from 12:00 AM to 11:59 PM, Pacific Daylight Time (UTC-7). Usage for the current date is the accumulation from 12:00 AM to within approximately 15 minutes of the end of the latest data session, and to within approximately six hours for 4G devices that stay connected for extended periods.

**NOTE:** The offline reporting maximum date range is 12 months.

Monitor > Reports

### Reports

Report type: Daily usage (dropdown)

Device IDs: [Search bar]

Start date: 2021-01-24 (calendar icon)

End date: 2021-01-30 (calendar icon)

[Run button]

3 Results

Device identifier	MDN	Account	ESN	MEID	IMEI	ICCID	IP address
							100.8
							100.8
							100.8

## Connection History Report

The *Connection History Report* shows each connection event for a specified device(s) over a particular date range, and provides the start and stop events associated with a device’s connections. This report also shows data usage during each connection.

**NOTE:** The online reporting date range limit is seven days, and for offline reporting, the maximum is three months.

Monitor > Reports

Reports

Report type

Device IDs

Start date

End date

Run

1,840 Results

Device identifier	MDN	ESN	MEID	IMEI	ICCID	IP address	Event
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21
							1/30/21

## Session History Report

The *Session History Report* provides information about one or more device connected sessions within a specified time period. This includes both data usage consumed and duration of each session. A connection session is delineated by Start and Stop records. For offline reporting, the maximum date range is three months. This report only contains information about data sessions that have ended. The report does not contain information about current, ongoing data sessions, including those of 4G devices connected for an extended period.

Monitor > Reports

Reports

Report type

Session history

Device IDs

Start date

2021-01-24

End date

2021-01-30

Run

919 Results

Device identifier	MDN	ESN	MEID	IMEI	ICCID	IP address	Start
							01/30
							01/30
							01/30
							01/30
							01/30
							01/30
							01/30
							01/30
							01/30
							01/30

## Rated Unbilled Usage Report

The *Rated Unbilled Usage Report* provides unbilled data and SMS usage for one or more devices from the billing cycle start to the latest date usage data is available. This report contains rated, unbilled data for the selected device's current bill cycle only. Historical data is not relevant. Usage data in this report is typically two days in arrears for non-roaming data. Therefore, to obtain a report that contains usage data for the first half of a bill cycle, wait until about Day 17 to generate a report. Roaming data may be updated less frequently. Rated usage data is not available to display in this report until about six days after the selected device's bill cycle start.

When you attempt to generate a report before data for the current bill cycle is available, this report displays data and SMS usage from the most recent bill cycle. Consult the column labeled “Start Date – End Date” to determine the billing period of the usage data included in the report.

Device identifier	ICCID	IP address	Cost code center	Wireless#	Used ↓	Allowance used(%)	SMS usage
		0.0.0.0			87 MB	870	0
		0.0.0.0			84 MB	840	0
		0.0.0.0			61 MB	610	0
		0.0.0.0			35 MB	350	0
		0.0.0.0			34 MB	340	0
		0.0.0.0			25 MB	250	0
		0.0.0.0			21 MB	210	0
		0.0.0.0			12 MB	120	0
		0.0.0.0			10 MB	100	0
		0.0.0.0			5 MB	50	0
		0.0.0.0			0 MB	0	0
		0.0.0.0			0 MB	0	0

## Usage Anomaly Report

For users subscribed to the ThingSpace premium Intelligence bundle, a **Usage anomaly** report type is available.

The *Usage anomaly* report shows anomaly events for a specified device(s) over a particular date range. Each event includes:

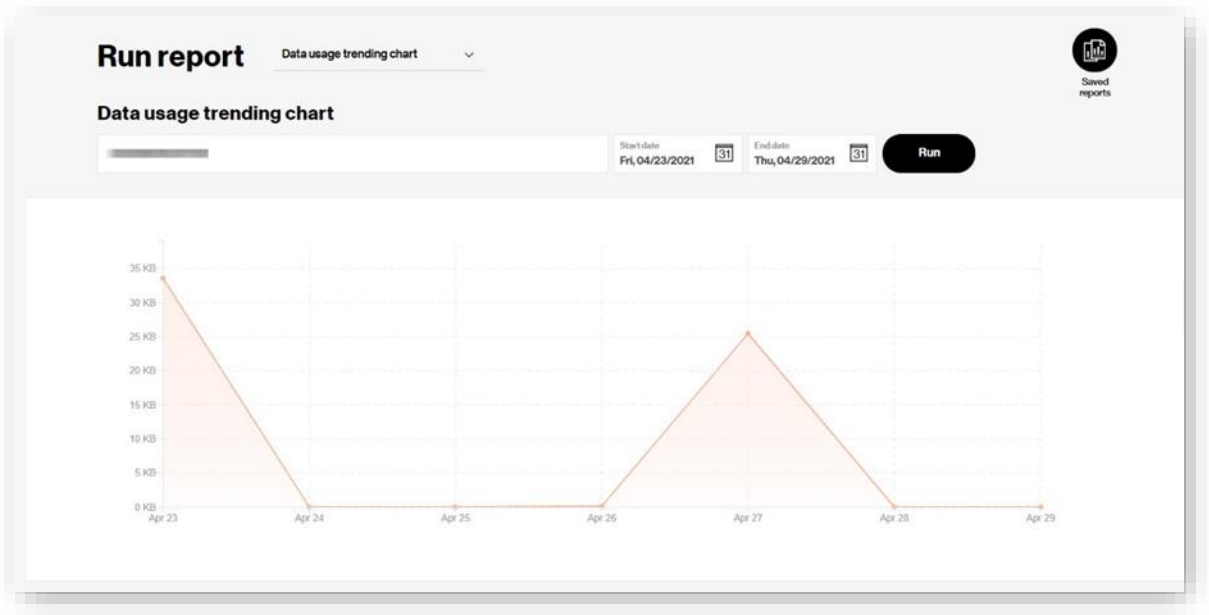
- **ICCID:** The SIM card number associated with the device
- **Event date:** The timestamp (within the hour) from which this anomalous event occurred
- **Usage (KB/h):** The reported data usage from the hour within the event
- **Anomaly rarity:** The probability value that represents the rarity of the event
- **Anomaly flag:** The type of anomaly (Abnormal or Very Abnormal) as defined in Anomaly Settings
- **Anomaly reason:** The options only over and under expected usage?

Users can request to be alerted about these events by configuring a Usage anomaly rule in the Rules page.

**NOTE:** The machine learning algorithm requires a minimum of 2 weeks to become trained for a particular device. Expect a high number of false positives early in the device lifecycle with this service.

## Usage Trending Chart

This report provides a chart that shows data usage patterns over a specified time period.

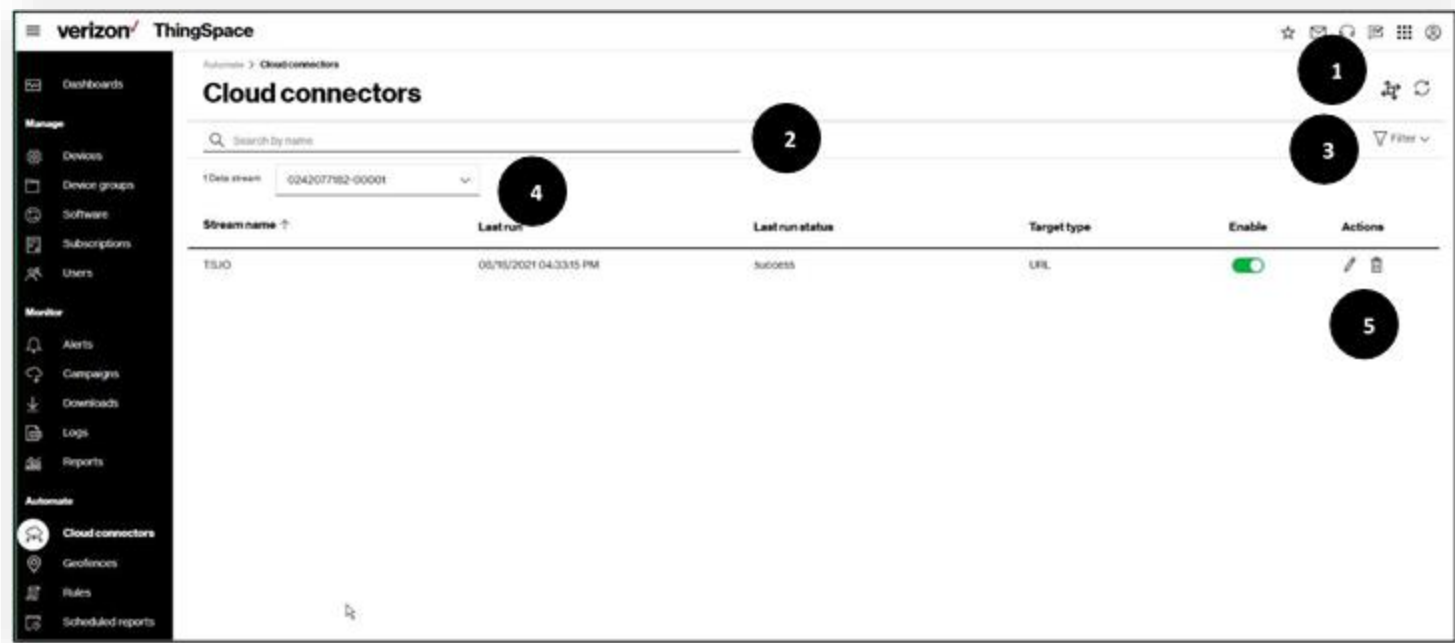




## Cloud Connectors

Use the *Cloud Connectors* page to configure Critical Asset Sensor (CAS) devices and stream the data to a set endpoint.

On the left navigation, click **Cloud connectors** to open the page.



### Elements on the Cloud connectors page

1		<b>Actions</b> – Open a menu to configure devices or create a stream.
		<b>Refresh</b> – Reload the page with up-to-date data.
2		<b>Search</b> – Type a stream name to locate a specific connection.
3		<b>Filter</b> – Open the Filters page to limit the connections on the page to those with specific attributes.
4		<b>Data streams</b> – A menu of connections.
5		<b>Edit</b> – Open the <i>Stream setup</i> page and revise stream attributes.
		<b>Delete</b> – Permanently remove the record from the system. This action cannot be undone.

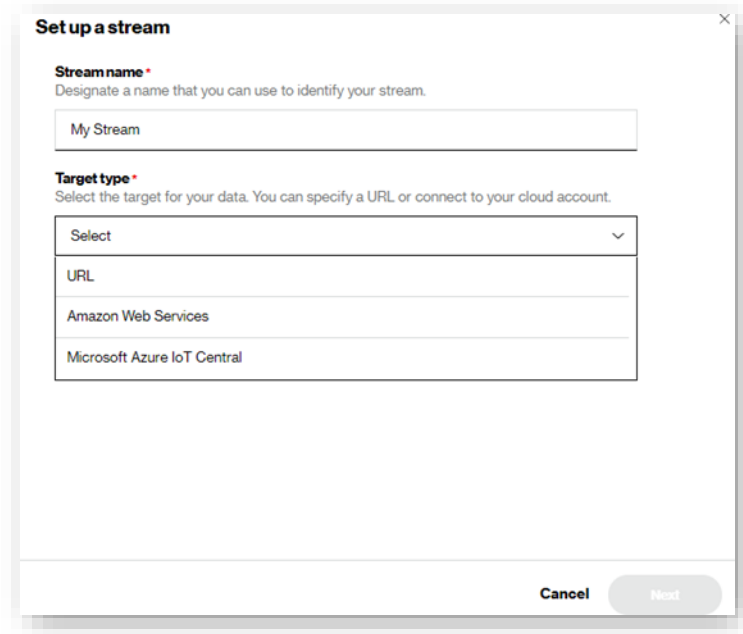
## Create a Stream

Streaming requires a target resource to define the endpoint, and a subscription resource to define what is streamed to the target.

### How to create a stream

On the left navigation, click **Cloud connectors**. The *Cloud connectors* page opens.

1. Click the actions icon , and select **Create stream**. The *Setup a stream* dialog opens.



**Setup a stream**

**Stream name \***  
Designate a name that you can use to identify your stream.

My Stream

**Target type \***  
Select the target for your data. You can specify a URL or connect to your cloud account.

Select

URL

Amazon Web Services

Microsoft Azure IoT Central

Cancel Next

2. For **Stream name**, type a descriptive label to easily identify the stream.
3. For **Target type**, select the type of streaming you are defining (URL streaming, streaming to Amazon Web Services, or streaming to Microsoft Azure IoT Central).
4. Click **Next**. The *Authentication type* menu opens. See [Using REST URL](#), [Using Amazon Web Services](#), or [Using Microsoft Azure IoT Central](#) to continue the Add Stream process.

## Using REST URL

### How to configure a stream to your cloud account

When a URL is selected, the Authentication type menu opens. The selections are:

The screenshot shows a dialog box titled "Set up a stream". Inside, there's a section for "Authentication type" with a subtext "Select the URL authentication options for streaming APIs." Below this is a dropdown menu currently showing "Select" with a downward arrow. The dropdown is open, revealing three options: "None", "Basic", and "OAuth 2.0". At the bottom of the dialog, there are three buttons: "Cancel", "Back", and "Next".

**None** – The Target location field opens to type the URL address.

**Basic** – In addition to specifying the Target location, you must also include a User ID and Password. Also, you must add the following field to the body of the request `"httpheaders": {"Authorization": "Basic <<>>"}`

**OAuth 2.0** - In addition to specifying the Target location field, you must also include an Access token. Optional fields are offered with this selection, and you must add the following fields to the body of the request:

`"key1": "Bearer <<>>"`

`"oauth": {"body": {"grant_type": "refresh_token", "refresh_token": "<<>>", "scope": "<<>>"}}`

`"headers": {"Authorization": "Basic <<>>", "Content-Type": "application/x-www-form-urlencoded"}`

`"host": {"hostandpath": "<<>>"}`}. To obtain the `BASE64_CLIENTID:CLIENTSECRET`

Do the following:

1. Concatenate the `CLIENTID` and the `CLIENTSECRET`, with a colon between them into a continuous string, like this: `CLIENTID:CLIENTSECRET`.
2. Encode the entire string in Base64 format. (To learn more about encoding in Base64 format, visit <https://www.base64encode.org/>).
3. Use the Base64 encoded value of `CLIENTID:CLIENTSECRET` in the API.

**NOTE:** *Target location* is the address, or URL, for the endpoint receiving data streams. The format depends on the selected address scheme but is often a host:port value. The endpoint must support a secure HTTP (HTTPS) connection and the endpoint server Transport Layer Security (TLS) certificate must be issued by a trusted certificate authority. This standard across all authorization types.

Click **Next**. The *Subscription* dialog opens.

## Using Amazon Web Services

ThingSpace uses an external identifier for increased security when streaming to Amazon Web Services (AWS). You generate the identifier in ThingSpace, then use it when configuring an AWS account and a ThingSpace target resource.

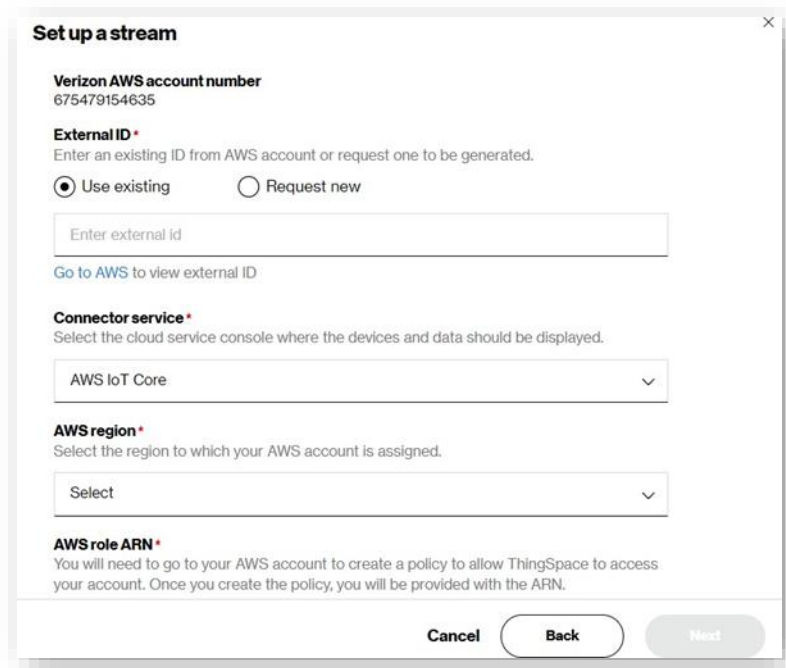
### How to configure an AWS account

1. Sign in to AWS.
2. Browse to IAM (Identity and Access Management).
3. From the *IAM Dashboard*, click **Roles**.
4. Click **Create role**.
5. For the type of trusted identity, select *AWS account*.
6. Type the *Verizon Account ID*, which is 675479154635.
7. Check **Require external ID**.
8. Select **Existing** or **Request new**.
9. Use the **Go to AWS** link to view the external ID and paste in the ID
10. Click **Next**.
11. Select these permissions:
  - AWSIoTDataAccess
  - w AWSIoTFullAccess
  - w AWSIoTThingsRegistration.
12. Click **Next**. Tags - No AWS tags are required.
13. Click **Next** Enter a name for the role (for example, *ThingSpace*).
14. Click **Create Role** to complete the process.

### How to configure a stream to your AWS account

Create a target for AWS streaming. A target resource defines an endpoint that can be used for streaming. After creating a target, use the target ID from the response when you create a subscription to set up a data stream. Note the requirements for these values to stream to AWS: address scheme must be *streamawsiot*. The address is the ARN provided by AWS for the role created above. Region is the AWS region where your application connects to AWS IoT services. See AWS Regions and Endpoints for a table of regions for the AWS IoT Core service. Note that Things and data from one region are not visible in another region. Name (and description) are not required but resource names can be used to query for resources later.

With all required *Stream setup* fields complete, click **Next**. The *Subscription* dialog opens.



The screenshot shows a dialog box titled "Set up a stream" with a close button (X) in the top right corner. The dialog contains the following fields and options:


- Verizon AWS account number**: 675479154635
- External ID \***: Enter an existing ID from AWS account or request one to be generated.
  - ☒ Use existing
  - ☐ Request new
  - Text input field: Enter external id
  - [Go to AWS to view external ID](#)
- Connector service \***: Select the cloud service console where the devices and data should be displayed.
  - Dropdown menu: AWS IoT Core
- AWS region \***: Select the region to which your AWS account is assigned.
  - Dropdown menu: Select
- AWS role ARN \***: You will need to go to your AWS account to create a policy to allow ThingSpace to access your account. Once you create the policy, you will be provided with the ARN.

At the bottom of the dialog, there are three buttons: "Cancel", "Back", and "Next". The "Next" button is highlighted in grey.

## Using Microsoft Azure

You can create a livestream from ThingSpace into Microsoft Azure IoT Central.

### How to configure an Azure connection

1. Sign into your Azure IoT Central account.
2. Click **Build a solution**.
3. On the left navigator, click the Build icon . The *Build your IoT application* page opens.
4. On the desired application tile, click **Create app**. The *New application* page opens.
5. For **Application name**, type an identifiable label, such as *TS Connector*. **Take note of the URL as this string is required later in this process.**
6. Select a **Price plan**.
7. Click **Create**. An IoT application is created that allows you to stream ThingSpace IoT data to.

With the Azure IoT application in place, you must now create two Cloud Connector APIs; a target that defines an endpoint for streaming to Azure, and a subscription that defines a data streaming channel that sends data from devices in the account to the endpoint defined in the target.

**NOTE:** Only one target/subscription pair for a ThingSpace account. Any existing target/subscription pair for the account must be removed before enabling this service.

### How to configure a stream to your Azure account

The screenshot shows a dialog box titled "Setup a stream" with a close button (X) in the top right corner. It contains two main sections:

- Azure IoT Central application \***  
HTTPS URL of the central application streaming endpoint.  
A text input field contains the placeholder text: `https://yourendpoint.azureiotcentral.com`.  
Below the field is a link: [Show instructions and where to get it](#).
- Shared access signature IoT of the central application \***  
Every Azure IoT central application has a shared access signature. Navigate to administration > API tokens > Generate token > Select admin role > Generate. Or do it programmatically [Api Tokens - Create\(Azure IoT central\) | Microsoft Docs](#).  
A text input field is labeled "Enter shared access signature".

At the bottom of the dialog are three buttons: "Cancel", "Back", and "Next". The "Next" button is disabled.

For **Azure IoT central application**, type the Azure IoT Central Application Endpoint URL from the [Using Microsoft Azure](#) procedure.

For **Shared access signature IoT of the central application**, obtain the Shared Access Signature Token from Azure Central IoT:

1. On the Azure IoT Central dashboard left navigation, go to **My apps** > (your new application) > **Administration** > **API tokens**. The *API tokens* page opens.
2. Click **Generate token**. The *Generate token* dialog opens.
3. Type a descriptive **Token name**, select the appropriate **Role**, and click **Generate**. The *Token successfully generated* dialog opens with the Shared Access Signature token.
4. Copy the token and paste into Shared access signature IoT of the central application in ThingSpace.
5. Click **Next**. The wizard advances.

The screenshot shows a dialog box titled "Set up a stream" with a close button (X) in the top right corner. It contains two main sections:

- Account**  
0242077182-00001
- Event types**  
Specify the types of data that will be displayed.  
Two radio buttons are present:   
- ☒ **Sensor data** (with a small gear icon)  
- ☐ **Diagnostics**

At the bottom of the dialog are three buttons: "Cancel", "Back", and "Save". The "Save" button is highlighted in black.

6. For **Event types**, select **Sensor data**.
7. Click **Save** to close the wizard and complete the process. The new connection is listed on the *Cloud connections* page.

You can now view your CAS device data in Azure IoT Central and on the ThingSpace Devices page.



## Configure Devices

You can change the status reporting frequency of each device, and whether or not location information via GPS is running.

**NOTE:** The more often a device reports back, or if GPS is turned on, the more energy is consumed by the battery.

### How to configure devices

On the left navigation, click **Cloud connectors**. The *Cloud connectors* page opens.

1. Click the action icon, and select **Configure devices**. The legacy *Configure devices* page opens.

**Configure devices** 0642233522-00001

Cloud connectors

All devices 5 Frequency

Ultra low 0 Frequency

Low 0 Frequency

Medium 2 Frequency


High 1 Frequency

Enter up to 10 comma-separated IDs of the same type: device ID or IMEI. Advanced +

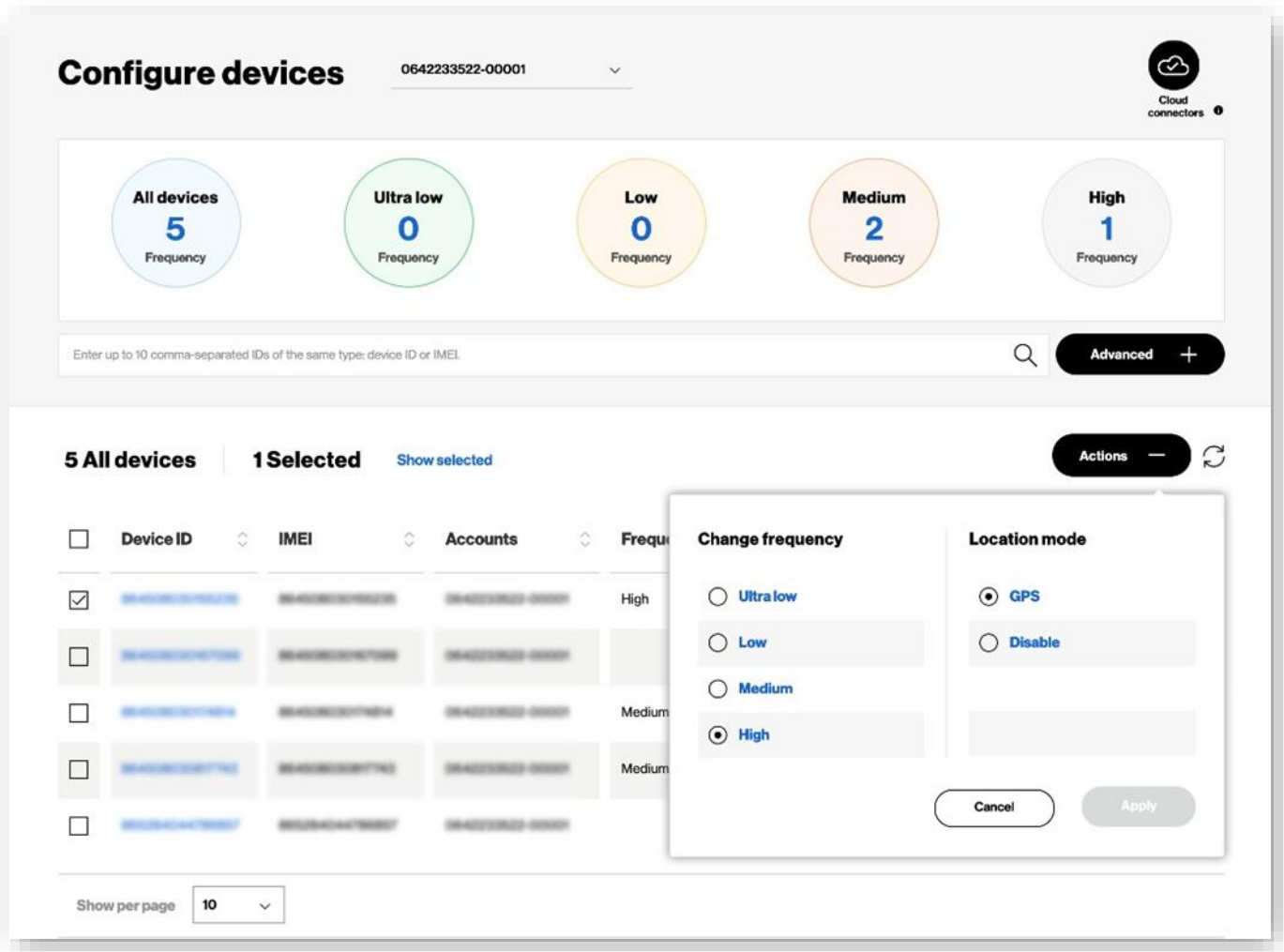
5 All devices 0 Selected Show selected Actions + ↺

<input type="checkbox"/>	Device ID	IMEI	Accounts	Frequency ⓘ	Configuration status ⓘ	Last updated	Location mode
<input type="checkbox"/>	0642233522-00001	0642233522-00001	0642233522-00001	High	update	07/18/2020 07:10:00 AM	gps
<input type="checkbox"/>	0642233522-00002	0642233522-00002	0642233522-00002		pending	03/16/2021 02:45:08 PM	
<input type="checkbox"/>	0642233522-00003	0642233522-00003	0642233522-00003	Medium	update	07/18/2020 07:16:01 AM	gps
<input type="checkbox"/>	0642233522-00004	0642233522-00004	0642233522-00004	Medium		06/30/2021 02:46:00 PM	gps
<input type="checkbox"/>	0642233522-00005	0642233522-00005	0642233522-00005		error	06/02/2021 03:26:00 PM	

Show per page 10

2. Click the Cloud connectors icon  to return to the *Cloud connectors* page. Type a Device ID in *Search* to locate a specific Device. Click **Advanced** for additional search options. See [Additional Device Information](#).
3. Select one or more *Device ID* check boxes. *Actions* is enabled.

4. Click **Actions**. A dialog opens where you can change *Frequency* and *Location mode* settings.



5. Select the **Change frequency** and **Location mode** option.
6. Click **Apply** to complete the process.

## Additional Device Information

Click a **Device ID** on the [Configure devices](#) page to open the *Device property* page.

Device property

Device ID:

Device property

Device information

Configuration history

Device history

Device property	Value
acceleration	{ "x": 0.9147, "y": 0.0090, "z": -0.2438 }
battery	1
deviceAlarm	{ "battery": { "Threshold": 15, "ThresholdRange": 80, "al...
deviceConfig	{ "device": { "checkFota": 1 } }
deviceDiagnostic	{ "firmwareVersion": 2.3.7, "radioFirmwareVersion": ...
humidity	16
light	0
location	{ "altitude": 0, "latitude": 41.886124, "longitude": -87.631...
orientation	{ "motionInX": 1.0, "motionInY": 255.0, "motionInZ": 0.0...
pressure	1011
signalStrength	-106
temperature	20.8


Close


Click the icons to open the following dialogs:


Device information


### Device information

Device ID:

  
Device property

  
Device information

  
Configuration history

  
Device history

<b>Device ID</b> <span></span>	<b>IMEI</b> <span></span>	<b>IMSI</b> -	<b>ICCID</b> <span></span>
<b>Accounts</b> <span></span>	<b>Frequency</b> High	<b>Last updated</b> 07/18/2020 07:10:00 AM	<b>Location mode</b> gps
<b>Configuration status</b> update	<b>Error description</b> -		

Close

Configuration history

Monitor > Reports

Reports

Report type

Connection history

Device IDs

Start date

2021-01-24

End date

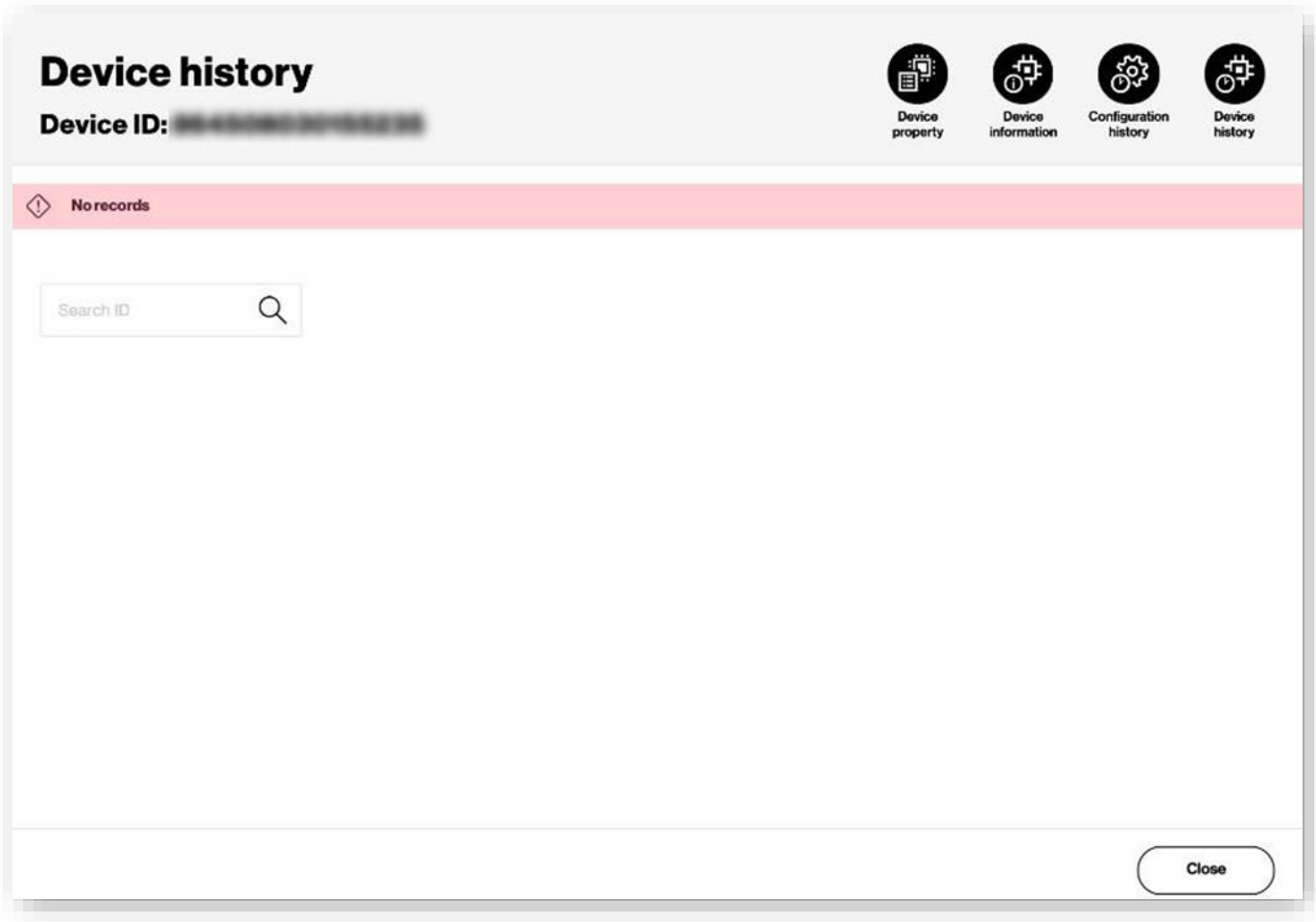
2021-01-30

Run

1,840 Results

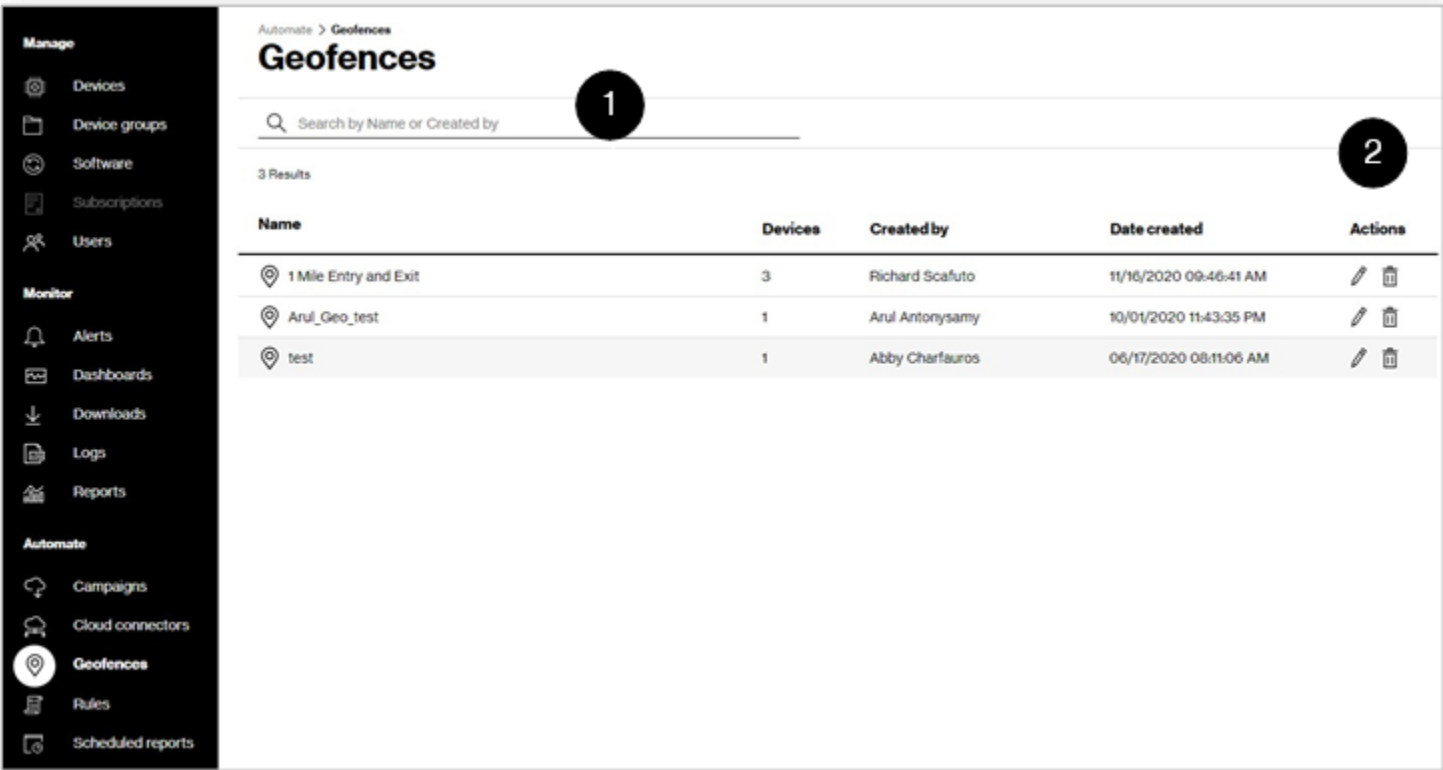
Device identifier	MDN	ESN	MEID	IMEI	ICCID	IP address	Event
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/
							1/30/

Device history



# Geofences

In the *Automate* section of the left navigation, click **Geofences** to open a list of geographical areas.



## Elements on the Geofences page

1		<a href="#">Search</a> – Type a geofence name to locate a specific geofence.
2	 	<a href="#">Edit</a> - Open the <i>Edit geofence</i> dialog to make revisions. <a href="#">Delete</a> - Permanently remove the record from the system. This action cannot be undone.

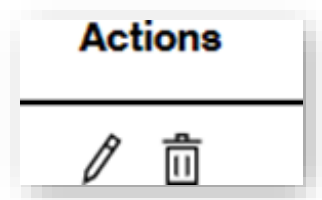
## Search for Geofences

Use **Search** for locating geofences by name or by the user name who created the geofence.



## Taking Actions

Action icons are available on each row of the *Geofences* list. To create a geofence, refer to the [Creating a geofence](#) in the *Devices* section.



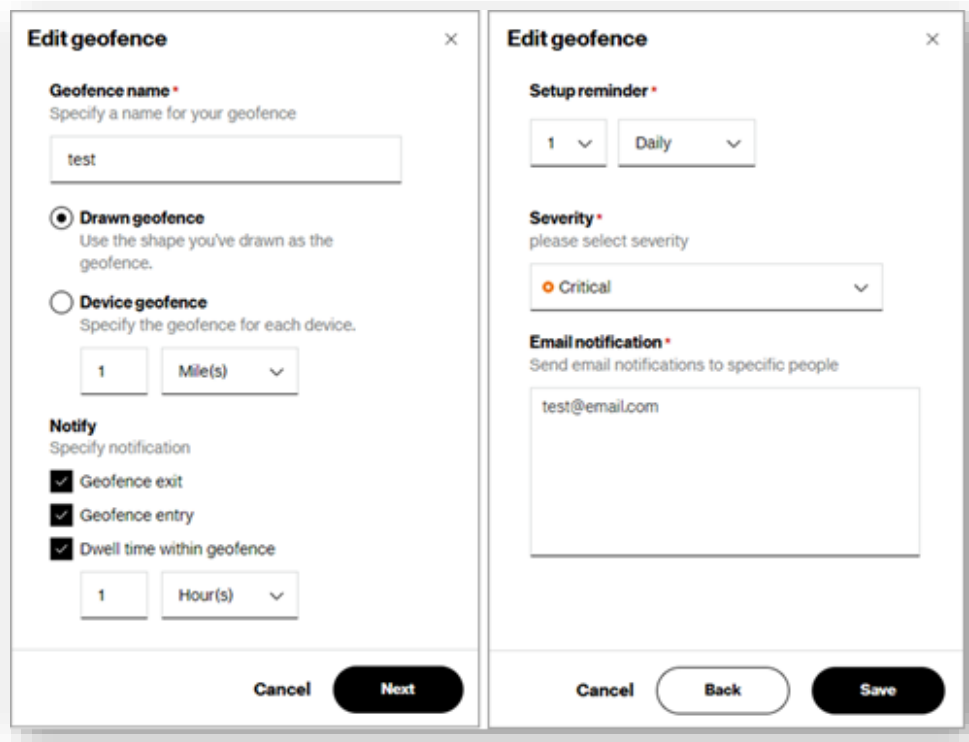


## Edit a Geofence

### How to edit a geofence

On the left navigation, click Geofences. The Geofences page opens.

1. Click the edit icon  of the geofence. The *Edit geofence* page opens




The image displays two panels of the 'Edit geofence' form. The left panel contains the 'Geofence name' field (value: test), radio buttons for 'Drawn geofence' (selected) and 'Device geofence', and a 'Notify' section with checkboxes for 'Geofence exit', 'Geofence entry', and 'Dwell time within geofence'. The right panel contains the 'Setup reminder' section (value: 1, Daily), a 'Severity' dropdown (value: Critical), and an 'Email notification' text area (value: test@email.com). Both panels have 'Cancel' and 'Next'/'Back'/'Save' buttons at the bottom.

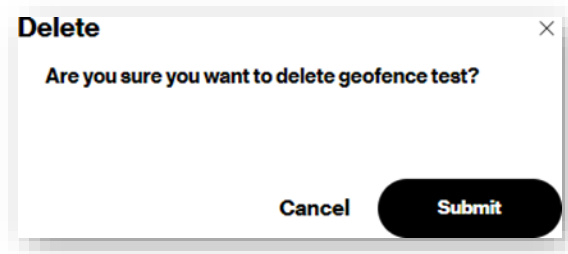
2. For **Geofence name** – a descriptive label to easily identify the geofence. For type of geofence:
  - **Drawn geofence** – A geofence that is drawn in a map.
  - **Device geofence** – A geofence that is defined for each device based on distance.
3. For **Notify**:
  - **Geofence exit** – A notification is sent when the device exits the geofence.
  - **Geofence entry** – A notification is sent when the device enters the geofence.
  - **Dwell time within geofence** – A notification is sent when the device stays within the geofence for a set period of time.
4. Click **Next**. A second page of settings opens.
  - **Setup reminder** – Send a reminder.
  - **Severity** – Select the severity of this geofence. The severity is included in the notification email.
  - **Email notification** – Enter the email addresses of those that are to receive the notification email.
5. Click **Save** to complete the process.

## Deleting a Geofence

### How to delete a geofence

On the left navigation, click **Geofences**. The *Geofences* page opens.

1. Click the delete icon  of the geofence. A confirmation dialog opens.
2. Click **Submit** to complete the process.



# Rules

Use the *Rules* page to set and view alert rules. Rules can be established for the following types of conditions:

**Data usage threshold** - This type of threshold applies when M2M data passing over a network surpasses a quantity specified in kilobytes (KB) within a particular time period (daily, weekly or monthly). Accumulated usage data is an estimate, and is current to within approximately 15 minutes of the latest data session ending, and to within approximately six hours for 4G devices that stay connected for extended periods.

**Provisioning activity threshold** - This type of threshold is reached either when a specific provisioning event occurs or a specific number of device provisioning events occur within a certain time period (daily, weekly or monthly).

**Value/state change** - This type of alert is generated at the point when a value associated with a device or the state of a device changes.






There are default usage alerts that, when enabled for your account, are automatically available for use. The Default usage alerts always appear as the first row of the table and cannot be deleted.

On the left navigation, click **Rules** to open the page.

The screenshot displays the 'Rules' page in the ThingSpace Manage v2.0 interface. The left sidebar contains navigation links for 'Manage' (Devices, Device groups, Software, Subscriptions, Users) and 'Monitor' (Alerts, Campaigns, Dashboards, Downloads, Logs, Reports). The 'Automate' section includes 'Cloud connectors', 'Geofences', 'Rules' (highlighted), and 'Scheduled reports'. The main content area is titled 'Rules' and features a search bar (labeled 1) and a filter dropdown (labeled 2). Below the search bar, it indicates '207 Results'. The table below lists rules with columns: Type, Name, Trigger, Account, Device group, User group, Enable (labeled 4), and Actions (labeled 5). The table includes a 'Default usage alert' and several 'Geofence' rules. The 'Enable' column uses toggle switches, and the 'Actions' column provides edit and delete icons for each rule. At the bottom, there is a 'Show 20 per page' option and a pagination control showing '1 2 ... 14 15 >'.

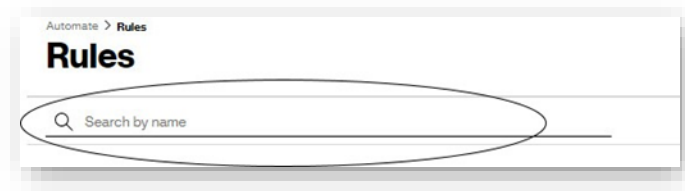
Type	Name	Trigger	Account	Device group	User group	Enable	Actions
Default usage ale...	Data usage	100%	All accounts	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	fasdf	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	fasdfasdf	Geofence rule	39-00001	All Devices	Individual recipients	<input type="checkbox"/>	/
Network	1ChangeBSID_020121_ED...	Excessive Connecti...	38-00001	All Devices	newUserGroup_0177	<input checked="" type="checkbox"/>	/
Network	22222	BSID Change	38-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	308123075810599_test_2	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	4593616975_Geofence_A...	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	5 Devices	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	5+ devices	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	82378037	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	82378037a	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	82378037b	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	Abdullah_device_geofence	Geofence rule	39-00001	All Devices	Individual recipients	<input checked="" type="checkbox"/>	/
Geofence	Abdullah_NPDIOTP-66688	Geofence rule	39-00001	All Devices	Individual recipients	<input type="checkbox"/>	/

## Elements on the Rules page

1		<a href="#">Search</a> - Locate a rule by name. Wildcard (%) search is supported.
2		<a href="#">Filter</a> - Reduce the list to rules with specific attributes.
3		<a href="#">Rule</a> - Open the <i>Rules Actions</i> menu to create, enable or disable a rule.
4		<a href="#">Enable/Disable</a> - Toggle to turn a rule on or off.
5	 	<a href="#">Edit</a> - Open the <i>Edit a rule</i> page to make revisions. Delete – Permanently remove a rule from the application.

## Searching Rules



Use **Search** to locate a rule by name. Wildcard (%) search is supported.

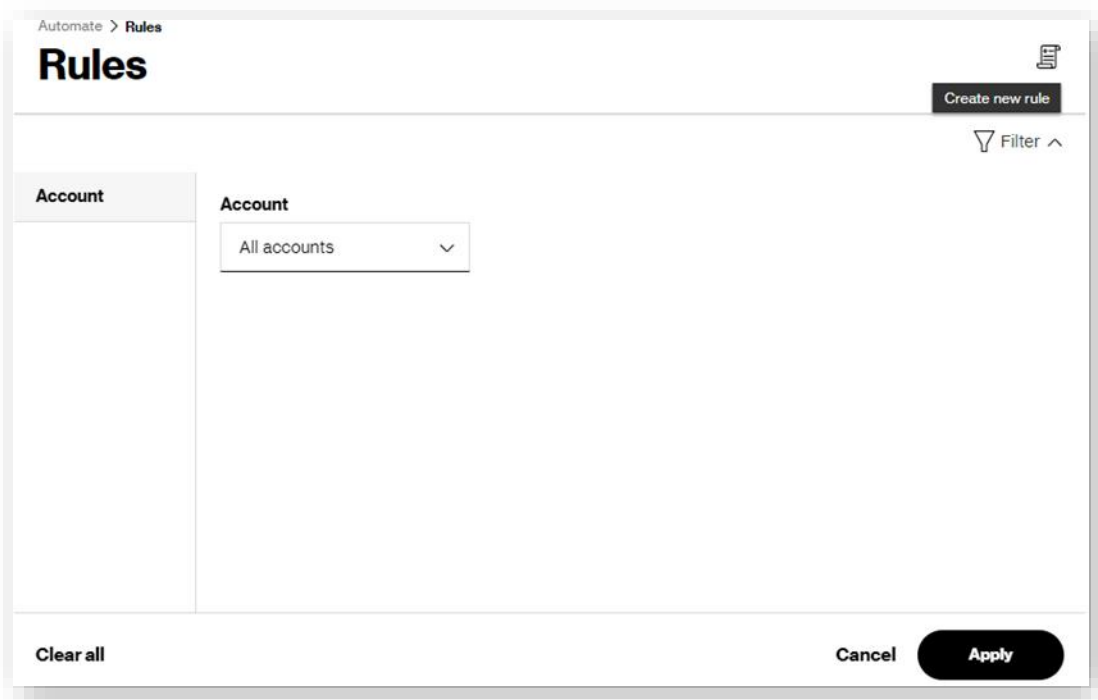


**NOTE:** Searches are not case sensitive.

## Applying Filters

How to apply filters

Click  Filter . The filters page opens.

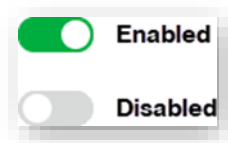


1. Select a filter from the *Account* menu.
2. Click **Apply**. A filters applied count appears.

## Enable/Disable a Rule

### How to enable or disable an automation rule

Toggle the switch  to turn the rule on (green), or off (gray).

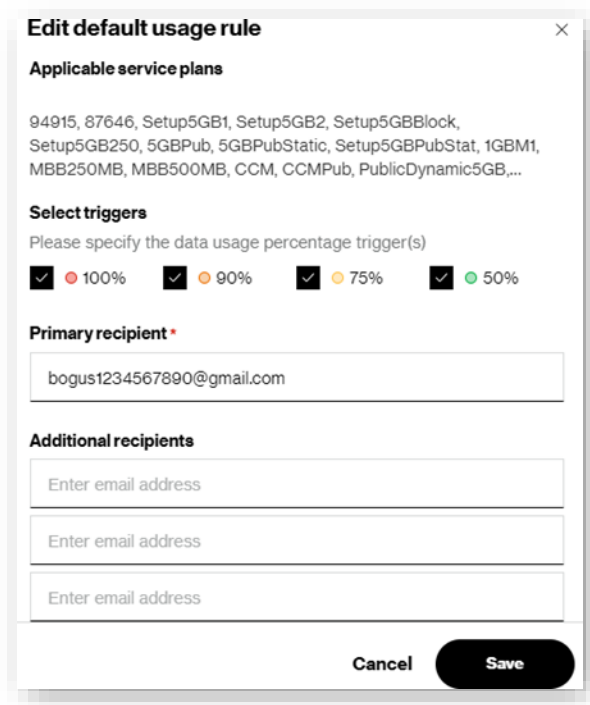


## Edit the Default Usage Alert Rule

If your account is enabled for Default alerts, the rule is the first entry on the Rules page. Use the Default usage alert rule to trigger an alert when an account uses 50%, 75%, 90%, and/or 100% of its data allocation.

### How to edit the default usage automation rule

On the Rules page, click the **Default usage alerts** rule Edit icon . The Edit default usage rule page opens.

A modal dialog box titled 'Edit default usage rule' with a close button (X) in the top right corner. The dialog contains several sections: 'Applicable service plans' with a list of plan IDs; 'Select triggers' with a prompt and four radio button options for 100%, 90%, 75%, and 50% usage; 'Primary recipient' with a text input field containing 'bogus1234567890@gmail.com'; and 'Additional recipients' with three empty text input fields. At the bottom are 'Cancel' and 'Save' buttons.

**Edit default usage rule** ×

**Applicable service plans**

94915, 87646, Setup5GB1, Setup5GB2, Setup5GBBlock, Setup5GB250, 5GBPub, 5GBPubStatic, Setup5GBPubStat, 1GBM1, MBB250MB, MBB500MB, CCM, CCMPub, PublicDynamic5GB,...

**Select triggers**

Please specify the data usage percentage trigger(s)

☒ 100% ☒ 90% ☒ 75% ☒ 50%

**Primary recipient\***

bogus1234567890@gmail.com

**Additional recipients**

Enter email address

Enter email address

Enter email address

Cancel Save

- For **Select the trigger(s)**, specify to receive an alert email when your usage reaches 50%, 75%, 90% and 100%.
- For **Primary recipient**, type the email address to send the alert.
- For **Additional recipients**, type the auxiliary email addresses to send the alert.

Click **Save** to complete the process.

## Edit a Rule

### How to edit a rule

On the *Rules* page, click on the rule edit icon . The *Edit a rule* page opens.

Automate > Rules > Edit a rule

Exit

### Edit a rule

Let's edit a rule

Enable ☒

Rule type \*

Select the type of rule

Network

Select account & devices \*

Please choose the account

00001

☒ All devices ☐ Device group

Define trigger \*

☐ Base Station ID Change

☐ Abnormal Disconnect

☒ Excessive Connections

4 or more per hour

Select severity \*

Please choose severity

Major

Setup reminders \*

Frequency: Hourly

Max number: 1

Select recipients \*

[Go manage user groups](#)

newUserGroup\_0177

And/Or enter up to 4 emails \*

Enter email address

Enter email address

Enter email address

Enter email address

Optional actions

☐ Suspend device

Rule name \*

Designate a name

1ChangeBSID\_020121\_EDIT

Save


1. Choose the **Rule type**.
2. Select an account & devices.
3. Define a trigger.
4. Select a severity.
5. Setup Reminders.
6. Select Recipients.
7. Enter other recipients.
8. Select optional actions.
9. Provide a rule name.
10. Click **Save**.

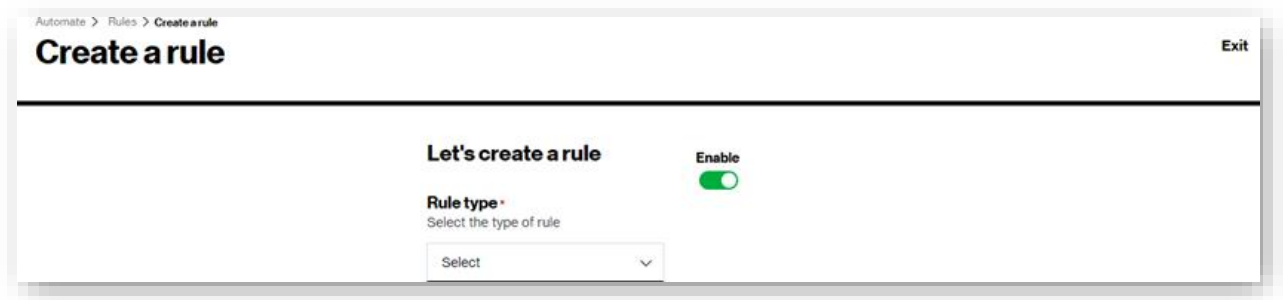


## Create a Rule

### How to create an automation rule

On the left navigation, click **Rules**. The *Rules* page opens.

1. Click the rule icon . The *Create a rule* page opens.



2. Choose the **Rule type**. Depending on the type of rule you are creating, different options display.
  - **Daily** - The system determines the initial criteria level (i.e., the data usage or number of device provisioning activity occurrences) daily at 12:00 am UTC, and resets the timer. The system evaluates the criteria when various events occur throughout the day to check for threshold breaches, and generates notifications when you meet or exceed a threshold value.
  - **Weekly** - For all weekly notification types, the system determines the weekly criteria level (i.e., the data usage or number of service provisioning activity occurrences) at 12:00 am UTC on Monday of each week, and resets the timer. The system also generates notifications at this time for any weekly threshold breaches not related to usage. The system evaluates accumulated usage data throughout the week for any weekly usage threshold breaches. The system generates notifications when you meet or exceed a usage threshold value.
  - **Monthly** - The system determines the initial criteria level (i.e., the data usage or number of device provisioning activities occurrences) at 12:00 am UTC on the billing cycle first day each month, and resets the counter. The system evaluates the criteria when various events occur throughout the month for any threshold breaches. The system generates notifications when you meet or exceed a threshold value.

**NOTE:** You cannot change the timing of the daily, weekly, and monthly checks.

# Rule Engine 2.0 for Real-Time Reporting (RTR)

Rule Engine 2.0 allows a user to set rules for devices across their account or rules for individual devices based on data usage, network connection or transactions. These rules can suspend a device, for all devices in the account or just send an alert. When a condition is met, the account can also change price plans. Customer must be enabled for RTR.

**Note:** When a rule is enabled, it will be in effect every month and continue to run every month unless the rule is disabled. Use the edit to modify the rule or disable the rule.

Click the rule icon . The *Create a rule* page opens. Use the drop down to select if the rule being created will be Network, Usage or Transaction:

## ThingSpace Manage v2.0 – User Guide

1. For the rule type selected, choose the condition being monitored:

**Create a rule**

**Category**

**Rule type**  
Select the type of rule  
Network

**Select account & devices**  
Please choose the account  
0442389666-00001  
☒ All devices ☐ Device group

**Trigger**  
Choose the condition  
Base station ID change

**Condition**  
Choose the condition  
Base station ID change  
Abnormal disconnect  
Excessive connections  
SMS count  
Session duration  
IMEI change detection

**Severity**  
Select your severity tag for this trigger  
Critical

**Action**  
Choose a suspend duration  
30 days

**Note**  
You can suspend a line of service for a maximum of 90 consecutive days. If you restore to the device service to the device and then suspend it again, the 90-day counter is reset. You can suspend a line of service for a maximum of 365 days out of the last 365 days. That is, it is rolling 365-day window looking back 365 days from the current day, the service can't have been suspended more than 180 of those days.

**Notification**

**Select recipients**  
Go manage user groups  
Select a user group and/or add individual emails

**Notification method**  
Select how you want to receive notifications

2. Scroll down and select the duration of the change made when the condition is met:

**Automate**

**Suspend duration**  
Choose a suspend duration  
30 days  
Until next billing cycle  
60 days  
90 days

**Notification**

**Select recipients**  
Go manage user groups  
Select a user group and/or add individual emails  
Select user group  
Enter email address  
Enter email address  
Enter email address  
Enter email address

**Notification method**  
Select how you want to receive notifications  
☒ Email ☒ SMS ☒ Callback

**SMS notification**  
Send additional SMS notifications to up to 5 numbers  
Add SMS number

**Setup reminders**  
Frequency Max  
Daily 1

**Name**

**Rule name**  
Designate a name  
Enter Alert Name

**Enable**  
☒

Save

- Before the rule is saved, the user can select how the rule sends a notification and who the notification is sent to:

The screenshot shows the 'Create a rule' form in the ThingSpace Manage v2.0 interface. The form is divided into several sections for configuring a rule:

- Category:** A dropdown menu with 'Usage' selected.
- Rule type:** A dropdown menu with 'Usage' selected.
- Criteria:** A dropdown menu with 'Accounts' selected. Below it, under 'Accounts', there is a list of accounts with checkboxes: 'Select all' (checked), '0442366666-00001' (checked), and '0642078568-00001' (checked).
- Trigger:** A section with a 'Condition' dropdown set to 'Individual device usage'. Below it are three dropdowns: 'More than' (set to '1'), 'MB' (set to '1'), and 'Monthly' (set to 'Monthly'). A note below these says: '\*Day = 12am UTC Week = Sunday - Saturday Month = Billing cycle month'.
- Severity:** A dropdown menu with 'Critical' selected.
- Action:** A section with an 'Action' dropdown set to 'Notification only'.
- Notification:** A section with a 'Notification type' dropdown set to 'Per event'.
- Notification method:** A section with three checkboxes: 'Email' (checked), 'SMS' (checked), and 'Callback' (checked).

The form is titled 'Create a rule' and has a 'Cancel' button in the top right corner. The left sidebar contains navigation links for 'Manage' (Dashboards, Devices, Devices groups, Software, Subscriptions, Users, User groups) and 'Monitor' (Alerts, Campaigns, Downloads, Logs, Reports). The bottom of the sidebar has 'Automate' links (Cloud connectors, Geofences, Rules, Scheduled reports).

### Usage Rule Example

In the *Create a rule* page, by selecting rule type usage the next step is to select the criteria:

The screenshot shows the 'Create a rule' interface in Verizon ThingSpace. The left sidebar contains navigation links for Dashboards, Manage (Devices, Devices groups, Software, Subscriptions, Users, User groups), Monitor (Alerts, Campaigns, Downloads, Logs, Reports), and Automate (Cloud connectors, Geofences, Rules, Scheduled reports). The main content area is titled 'Create a rule' and includes a 'Cancel' button. The form is divided into several sections: 'Category' (Rule type: Usage), 'Trigger' (Condition: Individual device usage, More than, MB, Monthly), 'Action' (Action: Notification only), and 'Notification' (Notification type: Per event). The 'Criteria' dropdown menu is open, showing options: Select, Accounts, Device groups, and Price plans. Below the 'Notification' section, there are links for 'Select recipients' and 'SMS notification'.

In selection of accounts, the selection of “select all” means all the accounts under the given profile the profile has access to:

The screenshot shows the 'Create a rule' interface with the 'Criteria' dropdown menu set to 'Accounts'. The 'Accounts' section displays a list of accounts with checkboxes: 'Select all' (checked), '0442386666-00001', and '0642078588-00001'. The 'Severity' dropdown menu is also open, showing 'Critical' selected. The 'Rule type' remains 'Usage', the 'Condition' is 'Individual device usage', and the 'Notification type' is 'Per event'.

## ThingSpace Manage v2.0 – User Guide

Select the trigger condition:

**Create a rule**

**Category**

**Rule type**  
Select the type of rule  
Usage

**Criteria**  
Select the criteria for this rule  
Accounts

**Accounts**  
Select one or more accounts  
☒ Select all  
☒ 0442386666-00001  
☒ 0642078588-00001

**Trigger**

**Condition**  
Choose the condition  
Individual device usage  
Individual device usage  
Combined device usage  
Day = Sunday - Saturday Week = Sunday - Saturday Month = Billing cycle month

**Severity**  
Select your severity tag for this trigger  
Critical

**Action**

**Action**  
Specify the action when alert is triggered  
Notification only

**Notification**

**Notification type**  
Choose notification type  
Per event

**Notification method**  
Select how you want to receive notifications  
☒ Email ☒ SMS ☒ Callback

Provide the size of the trigger according to available values:

**Create a rule**

**Category**

**Rule type**  
Select the type of rule  
Usage

**Criteria**  
Select the criteria for this rule  
Accounts

**Accounts**  
Select one or more accounts  
☒ Select all  
☒ 0442386666-00001  
☒ 0642078588-00001

**Trigger**

**Condition**  
Choose the condition  
Individual device usage

**Severity**  
Select your severity tag for this trigger  
Critical

**Action**

**Action**  
Specify the action when alert is triggered  
Notification only

**Notification**

**Notification type**  
Choose notification type  
Per event

**Notification method**  
Select how you want to receive notifications  
☒ Email ☒ SMS ☒ Callback

## ThingSpace Manage v2.0 – User Guide

**Create a rule**

**Category**

**Rule type**  
Select the type of rule  
Usage

**Criteria**  
Select the criteria for this rule  
Accounts

**Accounts**  
Select one or more accounts  
☒ Select all  
☒ 0442386666-00001  
☒ 0642078588-00001

**Trigger**

**Condition**  
Choose the condition  
Individual device usage

**Severity**  
Select your severity tag for this trigger  
Critical

**Action**

**Action**  
Specify the action when alert is triggered  
Notification only

**Notification**

**Notification type**  
Choose notification type  
Per event

**Notification method**  
Select how you want to receive notifications  
☒ Email ☒ SMS ☒ Callback

**Create a rule**

**Category**

**Rule type**  
Select the type of rule  
Usage

**Criteria**  
Select the criteria for this rule  
Accounts

**Accounts**  
Select one or more accounts  
☒ Select all  
☒ 0442386666-00001  
☒ 0642078588-00001

**Trigger**

**Condition**  
Choose the condition  
Individual device usage

**Severity**  
Select your severity tag for this trigger  
Critical

**Action**

**Action**  
Specify the action when alert is triggered  
Notification only

**Notification**

**Notification type**  
Choose notification type  
Per event

**Notification method**  
Select how you want to receive notifications  
☒ Email ☒ SMS ☒ Callback

## ThingSpace Manage v2.0 – User Guide

Select the action to take:

Usage

Accounts

Accounts

Select one or more accounts

☒ Select all

☒ 0442386666-00001

☒ 0642078588-00001

**Trigger**

**Condition**

Choose the condition

Individual device usage

More than  MB Monthly

\*Day = 12am UTC Week = Sunday - Saturday Month = Billing cycle month

**Action**

**Action**

Specify the action when alert is triggered

Notification only

**Notification**

Suspend device(s)

Choose notification type

Per event

**Notification method**

Select how you want to receive notifications

☒ Email ☒ SMS ☒ Callback

**Select recipients**

Go manage user groups

Select a user group and/or add individual emails

Select

**SMS notification**

Send additional SMS notifications to up to 5 numbers

Add SMS number

Please add at least one SMS number

And select the notification type and frequency:

Individual device usage

Critical

Less than  MB Monthly

\*Day = 12am UTC Week = Sunday - Saturday Month = Billing cycle month

**Action**

**Action**

Specify the action when alert is triggered

Notification only

**Notification**

**Notification type**

Choose notification type

Daily summary

Daily summary

Weekly summary

Select

**Notification method**

Select how you want to receive notifications

☒ Email ☒ SMS ☒ Callback

**SMS notification**

Send additional SMS notifications to up to 5 numbers

Add SMS number

Please add at least one SMS number

**Setup reminders**

Frequency Max

Hourly 1

**Name**

**Rule name**

Designate a name

Enable

**Note:** If the user chooses to use a callback notification, then they need to subscribe to the callback prior to using the rule.



## ThingSpace Manage v2.0 – User Guide

Note that a severity level can also be set for the trigger:

The screenshot shows the 'Create rule' form in the ThingSpace Manage v2.0 interface. The form is divided into several sections:

- Category:** A dropdown menu with 'Usage' selected.
- Rule type:** A dropdown menu with 'Usage' selected.
- Criteria:** A dropdown menu with 'Device groups' selected. Below it are radio buttons for 'Existing' (selected) and 'Create new'.
- Device group:** A dropdown menu with 'DC3\_Migration' selected.
- Trigger:** A dropdown menu with 'Individual device usage' selected.
- Condition:** A dropdown menu with 'Less than' selected, followed by a text input '22', a dropdown menu 'MB', and a dropdown menu 'Month'.
- Severity:** A dropdown menu is open, showing options: Critical, Critical, Major, Minor, Notice, and None.
- Action:** A dropdown menu with 'Notification only' selected.
- Notification type:** A dropdown menu with 'Weekly summary' selected.
- Notification method:** Checkboxes for 'Email', 'SMS', and 'Callback' (selected).
- Select recipients:** A link 'Go manage user groups' and a text input 'Select a user group and/or add individual emails'.
- SMS notification:** A link 'Send additional SMS notifications to up to 5 numbers'.

If “Price Plan” is selected from the drop-down menu, the user will see options for price plans to use (based on the price plans available to the account):

The screenshot shows the 'Create rule' form in the ThingSpace Manage v2.0 interface. The form is divided into several sections:

- Category:** A dropdown menu with 'Usage' selected.
- Rule type:** A dropdown menu with 'Usage' selected.
- Criteria:** A dropdown menu with 'Price plans' selected.
- Price plan:** A list of radio buttons with the following options: 'MACHINE TO MACHINE 1024KB OP', 'MACHINE TO MACHINE 1MB ACCT SHARE \$0...', 'RatePlanGroup:3626491\_73', '4G MACHINE TO MACHINE PAYGO \$0.0097656...', 'MACHINE TO MACHINE 1MB NATL SHARE \$0...', and 'DB3 Private Static'.
- Plan type:** A dropdown menu with the following options: 'AccountShare', 'AccountShare', 'AccountShareGroup', 'PayAsYouGo', 'ProfileShare', and 'StandAlone Pool'.
- Trigger:** A dropdown menu with 'Individual' selected.
- Usage condition:** A dropdown menu with 'Individual' selected.
- Severity:** A dropdown menu with 'Critical' selected.
- Accounts:** A section with the text 'Select one or more accounts' and checkboxes for 'Select all', '0442386666-00001', '0642078588-00001', and '0642078588-00002'.

## User Quick Start Guide

Rules Engine 2.0 has 3 categories to set alerts in:

- Network (How the device connects and is identified)
- Usage (How the device is consuming data)
- Transactions (How the device is set up or updated)

**Note:** Users can build multiple rules in the same category but each rule can only perform one action.

### For Network:

1. Select if the rule will apply to the entire account, all devices or a specific device group
2. Choose the trigger for the rule:
  - a. Base station ID change
  - b. Abnormal disconnect
  - c. Excessive connections
  - d. SMS count
  - e. 4 Session duration
  - f. IMEI change detection
3. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice
4. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
5. Name the rule
6. Click the Enable button

## For Usage:

Usage has 3 sub-categories:

- ♦ Accounts
- ♦ Device groups
- ♦ Price plans

## For Usage – Accounts:

1. Select all accounts or individual accounts
2. Choose the trigger condition:
  - a. Individual device usage
  - b. Combined device usage
3. Choose the trigger measurement:
  - a. More or less than a value
  - b. Units of the value (MB/KB/GB)
  - c. Measured period (Daily/Weekly/Monthly)
4. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice
5. Choose the action to perform when condition is triggered:
  - a. Notify
  - b. Suspend (with or without billing)

**Note:** Suspend can be set to auto-resume at the next bill cycle or in 30, 60 or 90 days. The action selected also has a severity value associated.
6. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
7. Name the rule
8. Click the Enable button

## For Usage – Device Groups:

1. Select an existing device group or:
  - a. Create a new device group with an individual account
  - b. Create a new group with multiple accounts
2. Choose the trigger condition:
  - a. Individual device usage
  - b. Combined device usage
3. Choose the trigger measurement:
  - a. More or less than a value
  - b. Units of the value (MB/KB/GB)
  - c. Measured period (Daily/Weekly/Monthly)
4. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice
5. Choose the action to perform when condition is triggered:
  - a. Notify
  - b. Suspend (with or without billing)

**Note:** Suspend can be set to auto-resume at the next bill cycle or in 30, 60 or 90 days. The action selected also has a severity value associated.
6. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
7. Name the rule
8. Click the Enable button

### For Usage – Price Plans:

1. Select a price plan from the list:
  - a. Stand alone
  - b. Account group share
2. Choose the trigger condition:
  - a. Individual device usage
  - b. Combined device usage

**Note:** Individual device usage rule will be in effect during the bill cycle. Price plan changes will be backdated or current dated. Rules will only work if lines were active from the beginning of the bill cycle and from low to high price plan within a group.

### For Individual Device Usage – Account Group Share:

3. Select the action:
  - a. Notify
  - b. Change from a price plan to another price plan
  - c. Suspend (with or without billing)
  - d. If suspended, auto resume (Yes or No) and if resumed at the next bill cycle or in 30, 60 or 90 days.

### For Shared Pool Usage – Account Group Share:

3. Select the action:
  - a. Notify
  - b. Price plan change – Verizon automation
  - c. Price plan change – Custom automation (Based on usage less than or more than 100%)

**Note:** The share pool usage rule will be in effect on the last day of the billing cycle. Share pool usage will allow the setup of price plan changes. Share pool usage will allow VZW Automation or Customized selection to calculate account share pool monthly total. Share pool will move from low to high to avoid the overage and from high to low if the pool is under performing.

**Note:** Suspend is not supported for share pool usage

4. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice

5. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
6. Name the rule
7. Click the Enable button

### **For Stand Alone Price Plans:**

1. Select all accounts or one or more specific accounts.
2. Choose a trigger condition:
  - a. Usage allowance – account level
  - b. Usage allowance – individual
  - c. Aging (Price plan changes to lines which were active on a selected price plan for a number of bill cycles)
3. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice
4. Choose the action to perform when condition is triggered:
  - a. Notify
  - b. Price plan change (from price plan to price plan)
  - c. Suspend (with or without billing)

**Note:** Suspend can be set to auto-resume at the next bill cycle or in 30, 60 or 90 days. The action selected also has a severity value associated.

5. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
6. Name the rule
7. Click the Enable button

## **For Transactions:**

1. Select all accounts, one or more specific accounts or a device group.
2. Choose the trigger condition:
  - a. Provisioning failure
  - b. Provisioning success
  - c. A provisioning request
  - d. A specified number of provisioning requests
  - e. Auto resume
3. Choose the severity of the notification:
  - a. Critical
  - b. Major
  - c. Minor
  - d. Notice
4. Select the recipients of the notification (user group or individual) and the method:
  - a. Email
  - b. SMS (text message)
  - c. Callback
5. Name the rule
6. Click the Enable button

## Scheduled Reports

Use the *Scheduled reports* page to view saved and/or scheduled reports. On the left navigator, click **Scheduled reports** to open the page.

Automate > Scheduled reports

### Scheduled reports

4 Results

Name	Type	Date created ↑	Schedule	Actions
daily test	Aggregated device usage report	5/14/2020 5:21:05 PM		<a href="#">Run</a> <a href="#">Edit</a> <a href="#">Delete</a>
test	Aggregated device usage report	5/14/2020 5:20:44 PM		<a href="#">Run</a> <a href="#">Edit</a> <a href="#">Delete</a>
Test Save and Schedule for FOTA	FotaDevices	2/6/2020 9:41:33 AM	Expired	<a href="#">Run</a> <a href="#">Edit</a> <a href="#">Delete</a>
Test Search	Devices	1/22/2020 1:18:19 PM		<a href="#">Run</a> <a href="#">Edit</a> <a href="#">Delete</a>

1-3

### Elements on the Rules page

1	<a href="#">Run</a>	<a href="#">Run</a> - Initiate the report manually.
2	<a href="#">Edit</a>	<a href="#">Edit</a> - Open the <i>Edit a Scheduled Report</i> page to revise the schedule.
3	<a href="#">Delete</a>	<a href="#">Delete</a> - Permanently remove a scheduled report.

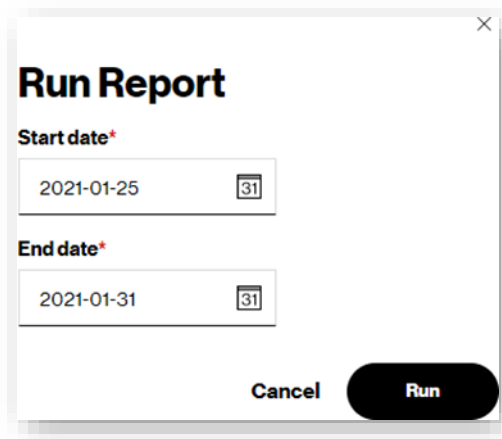


## Run a Report

### How to run a report

On the left navigation, click **Scheduled reports**. The *Scheduled reports* page opens.

1. Click the report's run icon . The *Run Report* dialog opens to enter a date range.



The **Run Report** dialog box is shown. It has a title bar with a close button (X). The main content area contains two date input fields. The first field is labeled **Start date\*** and contains the text '2021-01-25' with a calendar icon to its right. The second field is labeled **End date\*** and contains the text '2021-01-31' with a calendar icon to its right. At the bottom right of the dialog, there are two buttons: a 'Cancel' button and a 'Run' button.

2. Enter a *Start date* and an *End date*.
3. Click **Run**.

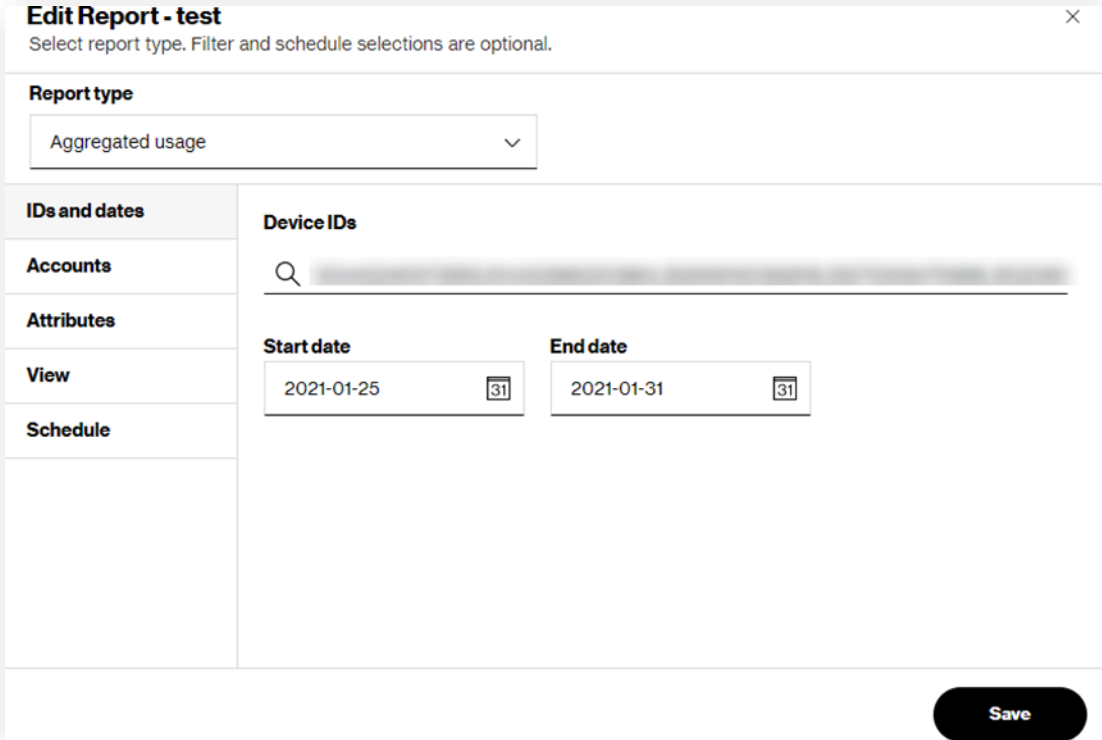
Your report is sent for processing and available on the [Downloads](#) page when processing is complete and the system sends you an email notification when the report is available.

## Edit a Scheduled Report

### How to edit a scheduled report

On the left navigation, click **Scheduled reports**. The *Scheduled reports* page opens.

1. Click the report's edit icon . The Edit Report page opens.



**Edit Report - test** ×

Select report type. Filter and schedule selections are optional.

**Report type**

Aggregated usage ▼

**IDs and dates**

**Accounts**

**Attributes**

**View**

**Schedule**

**Device IDs**

🔍

**Start date** 2021-01-25 📅 **End date** 2021-01-31 📅

**Save**

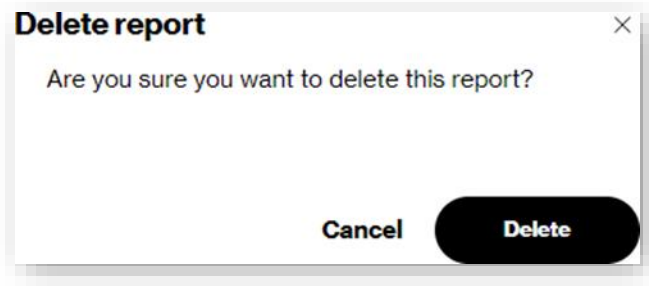
2. Choose the **Report type**.
3. Click on any of the tabs on the left side of the page to scroll to the relevant section. Update any of the selection criteria.
  - Update your table **View**.
  - Update the **Schedule**.
4. If the report is not scheduled to run at a later time, Click **Save**.
5. If the report is scheduled to run at a later time, Click **Schedule**.

## Delete a Scheduled Report

### How to delete a scheduled report

On the left navigation, go to Scheduled reports. The Scheduled reports page opens.

1. Click the report's Delete icon . A conformation dialog opens.



2. Click Delete to complete the process.

## Frequently Asked Questions

*What is the difference between an online report and an offline report?*

Online reports run instantly with results provided on the screen. Offline reports are submitted for processing in the backend and are available on the Downloads page when processing is completed.

*Where are my transactions?*

The legacy Transactions page was renamed to Logs. Provisioning transactions are now located there. For additional information, please visit our [FAQs page](#) on the ThingSpace website.

## Glossary

Glossary of Terms	
Account	A list of billing account(s) to which you have access.
API	An application programming interface (API) you can use to manage your information through an external application rather than through the web portal.
Device	IoT devices that you can activate, and are associated with your account.
ESN	The manufacturer assigned unique Electronic Serial Number of a CDMA device.
ICCID	The Integrated Circuit Card Identifier is the unique serial number assigned to and imprinted on a SIM card by the manufacturer.
IP Address	The Internet Protocol Address that gets assigned to a device during activation. A device's IP address is always shown when you have static IP addresses for devices. When you have dynamic IP addresses, a device's IP address is only shown when the device is connected. When the device is not connected, the IP address is zero-filled (0.0.0.0) because no IP address is assigned to the device.
IMEI	The International Mobile Equipment Identity is a unique identifier of a 4G device.
IMSI	<p>The International Mobile Subscriber Identifier is stored on a SIM card. This identifies and authenticates the user on the network, which Verizon also calls the subscriber. The IMSI is only revealed to, and known by, the carrier. The IMSI comprises the following codes:</p> <p><b>MCC</b> – Mobile Country Code (311)</p> <p><b>MNC</b> – Mobile Network Code (480)</p> <p><b>MSIN</b> – Mobile Subscription Identification Number, a unique number for the subscriber on the Verizon network.</p>
MDN	The unique 10-digit Mobile Directory Number Verizon assigned to a device at activation. MDNs comprise the area code (three digits), exchange (three digits), and number (four digits).
MEID	The unique Mobile Equipment Identifier of a 3G device.

MIN	The unique Mobile Identification Number that Verizon uses internally to track and route traffic to and from a device.
MSISDN	The Mobile Station International Subscriber Directory Number is a unique 11-digit phone number associated with a 4G device at activation. It is functionally equivalent to a 3G device's MDN.
Organization	An organization with M2M accounts on the ThingSpace platform.
pre-IMEI	The IMEI value of the device from before the most recent over-the-air provisioning event completed.
pre-SKU	The SKU value of the device from before the most recent over-the-air provisioning event completed.
PPU	The Primary Place of Use is the address where the wireless number of a device is derived.
Rate Plan	A contracted plan between an organization and an account, defining how each Device is charged for both subscription fees and usage of the network.
Role	Each user has an associated Role that defines the privileges the user has for seeing and working with data and functionality in the portal.
SKU	The Stock Keeping Unit assigned to a device.
SIM	The Subscriber Identity Module is a unique identifier, which can be embedded or on a physical card that is inserted in a 4G device to establish cellular connectivity.
Session	A single data context established between a device and the ThingSpace platform.
User	A unique sequence of characters used to identify a user and allow access.
Wildcard	Using a wildcard character allows you to use the percent sign (%) at the end of the string and search for everything that starts with that string.

## Appendix

### Field Definitions

This section contains field/column definitions found on pages throughout the portal.

Column Name	Definition
Active timer	Active timer = T3324 as defined in [3GPP-TS_24.008].  The time the UE has to remain reachable after transitioning to idle state in case there is pending data from the NW to send out. At the end of T3324 UE can go into a deep sleep mode while keeping the PDN connection(s) active.
Battery level	Contains the current battery level as a percentage (with a range from 0 to 100). This value is only valid when the value of Available Power Sources Resource is 1.
Battery status	Only valid when the value of Available Power Sources Resource is 1.  Values can be of 0-6 and this value represents current status of the battery listed as below: <b>0:</b> Normal <b>1:</b> Charging <b>2:</b> Charge Complete <b>3:</b> Damaged <b>4:</b> Low Battery <b>5:</b> Battery is not installed. <b>6:</b> Unknown.
Cell ID	(0-65535) Cell ID / eNB ID

Column Name	Definition
Cell ID stream status	Status of streamed information if a live stream is running
Cell ID updated date	Last date update occurred of Cell ID
EDRX timer	Extended Discontinuous Reception ( <b>eDRX</b> ) allows IoT devices to not listen to the network for extended periods. Downlink Paging opportunities occur every 1.28 seconds. This is the minimum time a UE using eDRX can decide to stay in idle mode, up to a maximum of 43.69 minutes.
Link quality	Contains received link quality, or the signal-to-noise ratio in integer value.
Link quality stream status	Status of streamed information when a live stream is running.
Link quality updated date	Last date a Link quality update occurred.
LWM2M streaming eligible	The device has Lwm2M registered to Verizon.
Modem	Modem information, if available.
Network bearer	<p>The network bearer used for the current LWM2M communication session from the following network bearer list:</p> <p><b>0~20</b> are Cellular Bearers</p> <p><b>0:</b> GSM cellular network</p> <p><b>1:</b> TD-SCDMA cellular network</p> <p><b>2:</b> WCDMA cellular network</p> <p><b>3:</b> CDMA2000 cellular network</p> <p><b>4:</b> WiMAX cellular network</p> <p><b>5:</b> LTE-TDD cellular network</p> <p><b>6:</b> LTE-FDD cellular network</p> <p><b>7~20:</b> Reserved for other type cellular network.</p> <p><b>21~40</b> are Wireless Bearers.</p> <p><b>21:</b> WLAN network</p> <p><b>22:</b> Bluetooth network</p> <p><b>23:</b> IEEE 802.15.4 network</p> <p><b>24~40:</b> Reserved for other type local wireless network.</p> <p><b>41~50</b> are Wireline Bearers.</p>



Column Name	Definition
Network bearer (continued)	<p><b>41:</b> Ethernet</p> <p><b>42:</b> DSL</p> <p><b>43:</b> PLC</p> <p><b>44~50:</b> reserved for others type wireline networks.</p>
Network bearer stream status	Status of streamed information if a live stream is running.
Network bearer update date	Last date the Network bearer update occurred.
Paging timer window	Extended DRX parameters (Paging Time Window and eDRX value) for which the UE can request from the network. This resource is encoded as octet 3 in [3GPP- TS_24.008, clause 10.5.5.32]. See also <a href="#">eDRX</a> and <a href="#">PSM</a> .
Power sources	<p><b>1:</b> DC power</p> <p><b>2:</b> Internal Battery</p> <p><b>3:</b> External Battery</p> <p><b>4:</b> Power over Ethernet</p> <p><b>5:</b> USB</p> <p><b>6:</b> AC (Mains) power</p> <p><b>7:</b> Solar</p> <p>The same Resource Instance ID MUST be used to associate a given Power Source (Resource ID 6) with its Present Voltage (Resource ID=7) and its Present Current (Resource ID=8).</p>
PSM timer	<p>This is the only time period in a PSM cycle when UE responds to Verizon LTE network's downlink paging.</p> <p>Power save mode (PSM) timer as defined in [3GPP-TS_23.682].</p> <p>PSM Timer = Extended T3412. Max interval between periodic TAU if there is no other transmission from the device. During a deep sleep mode, the device is unreachable but keeps the PDN connection(s) active. Implementation of Power Saving Mode in an application requires a careful choice of UE Sleep Time and Awake Time. UE Sleep time is captured by timer Extended T3412 and UE awake Time is captured by timer T3324. Verizon network accepts all 3GPP defined values for T3324 and enforces a minimum of 186 minutes for Extended T3412. 3GPP defined values for Extended 3412 and T3324 are available in 3GPP TS24.008.</p>

Column Name	Definition
Radio signal strength	<p>Represents the entire received power including noise.</p> <p>This resource contains the average value of the received signal strength indication used in the current network bearer. In case Network Bearer Resource indicates a Cellular Network (RXLEV range 0&amp;64) 0 is &lt; 110dBm, 64 is &gt; -48 dBm).</p> <p>Excellent=-65 Good=-65 to -75</p> <p>Fair=-75 to -85</p> <p>Poor=-85</p>
Radio signal strength stream status	Status of streamed information when a live stream is running.
Radio signal strength updated date	Last Radio signal strength update.
APN1	Access Point Name
APN2	Access Point Name

## General

These fields may be found in multiple pages throughout the portal and are consolidated here.

Term Used	Definition
Device identifier	IMEI or ICCID. If the line is activated as SIM only or SIM/SKU, the ICCID is the Device Identifier, as the system does not yet know the IMEI. Once the device boots and the OTA occurs, the Device Identifier updates with the IMEI.
MDN/MSISDN/Pseudo	Mobile Device Number. The phone number assigned the line.
IP address	The device IP address. This may be 0.0.0.0 if the device is not connected / in an active data session for a dynamic IP addressed device (default).
Device status	Active, Deactive, Suspended. <i>Active</i> implies billing, <i>Deactive</i> implies not billing, and <i>Suspended</i> is usually suspended (up to 90 days) without billing.

Term Used	Definition
Connection	Connected or Not Connected. <i>Connected</i> indicates an Active Data Session over the wireless network; <i>Not Connected</i> implies that data is not present (devices could be powered off).
Device group	Group assigned. All lines automatically get added to the default group, which is named the account number.
Service plan	Service plan assigned. The Service Plan is a bundle of the rate plan plus feature codes (SFOs), such as SMS, VMail, International, etc.
Activation date	The device on-boarded to ThingSpace date. If Support re-synced the device to ThingSpace by toggling the TS SFO, this date reflects when the device was re-synced to ThingSpace (not the original activation date).
ICCID	SIM hardware identifier
IMEI	Device hardware identifier
4G/LTE	3G or 4G
Account	The account number and sub account number. Always starts with a zero for ThingSpace.
Activated by	The person who activated the line.
Billing cycle end date	The billing cycle end date.
Cost code center	Your alphanumeric data. Available in MyBusiness and ThingSpace.
Deactivated by	The name of the person that deactivated the device.
Deactivation date	The date the line was last deactivated.
EID	Electronic Identifier. A unique number to identify wireless equipment.
ESN	Electronic serial numbers were created by the U.S. Federal Communications Commission to uniquely identify mobile devices.

<b>Term Used</b>	<b>Definition</b>
eUICC profile status	
First name	Your alphanumeric data. Available in MyBusiness and ThingSpace.
Last connection date	The last active PPP data session seen on the network.
Last name	Your alphanumeric data. Available in MyBusiness and ThingSpace.
Last roaming status update	The last roaming status update.
Make and model	The make and model as stored in the device management database (DMD).
MDN	The 10-digit telephone number assigned to a CDMA line.
MEID	Mobile Equipment Identifier - A globally unique number identifying a physical piece of CDMA equipment.
Middle name	Your alphanumeric data. Available only in ThingSpace.
MIN	Mobile Identification Number – A unique 10-digit number that a wireless carrier uses to identify a mobile phone.
Modem category	Category of device modem, if known.
MSISDN	A number uniquely identifying a subscription in a Global System for Mobile (GSM) communications.
MyCustomField1	Your alphanumeric data. Available only in ThingSpace.
MyCustomField2	Your alphanumeric data. Available only in ThingSpace.
MyCustomField3	Your alphanumeric data. Available only in ThingSpace.
MyCustomField4	Your alphanumeric data. Available only in ThingSpace.
MyCustomField5	Your alphanumeric data. Available only in ThingSpace.

Term Used	Definition
Pending action	Line is pending between states or database updates. Used during pending provisioning states or database updates, such as Cost Center.
pre-IMEI	IMEI assigned during activation.
pre-SKU	SKU assigned during activation.
Roaming country	The country the device is roaming in.
Roaming status	Device current roaming status. Can be <i>null</i> , <i>roaming</i> , or <i>not roaming</i> .
Scheduled resume date	90 days from suspend date.
Sim OTA timestamp	When the current MDN/MSISDN first attached to Verizon.
SKU	The Open Development Stock Keeping Unit number.
DACC	Seems to be editable in ODI portal at time of device upload.
SACC	SIM Attribute Composite Code. Mdnless only,

## Location

Term Used	Definition
Hyper Precise capable	Whether or not the device is Hyper Precise capable
Hyper Precise status	
Last location attempt	Last attempted coarse location request.
Last location update	Last successful coarse location request.
Last location update status	Last coarse location update status. <i>Can be null, failed, or successful.</i>
Location update frequency	If set to auto update coarse location, this is the setting in seconds.
Location update note	<i>Can be null, Device is Unreachable, or Specified device category is not IoT.</i>

## Software

Term Used	Definition
Current software	Current version of software running on the device. This could be baseband firmware, application firmware, or a configuration file. This is the last known reported. A device may have zero, one, or many of these at any time.
Firmware campaign status	Device-level status based on last firmware campaign. The status codes are documented under "Campaign Lifecycle Flow" <a href="https://thingspace.verizon.com/documentation/apis/software-management/getting-started.html">https://thingspace.verizon.com/documentation/apis/software-management/getting-started.html</a> .
FOTA campaign ID	Unique ID of a particular FOTA upgrade campaign. Campaign ID links to campaign details (what software, when, which devices, device status). For a particular device, this is the last campaign that device was included in.

Term Used	Definition
FOTA eligibility	Whether or not the device has registered to our FOTA server(s). Incompatible devices cannot bootstrap or register to Verizon's FOTA servers. If compatible devices have not registered, the firmware on the device cannot be determined.
FOTA license status	Indicates an attached MRC (unlimited FOTA) license. Event licenses can still be used, but still show as "unattached" since they are per use.
FOTA license type	If MRC is attached, it's a Subscription. Options are <i>Subscription</i> or blank.
FOTA make	The make of the device, as reported by FOTA server. Options are <i>Subscription</i> or blank. FOTA make and model may not match the device make and model.
FOTA model	The model of the device, as reported by FOTA server.
FOTA protocol	The FOTA protocol the device is using to communicate with ThingSpace. LWM2M and OMA-DM are used for baseband. HTTP can be used for baseband, application, and configuration files.
FOTA security compliance	<i>Not compliant</i> indicates new software is available. <i>Compliant</i> indicates up to date. Retired in ThingSpace 2.0. Implicit based on whether or not <i>New software</i> field is populated.
Last firmware update	Last firmware campaign on the device.
New software	New software available to upgrade for that device. If that particular software (see <a href="#">Current Software</a> ) has an eligible upgrade path, this is where it shows.
Software name	Software name associated with current->new upgrade epath. As certified by Verizon Open Development. For LWM2M and OMADM, this is a make_model_from_to concatenation. For HTTP, this is typically make_model.