# 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

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 accustom 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

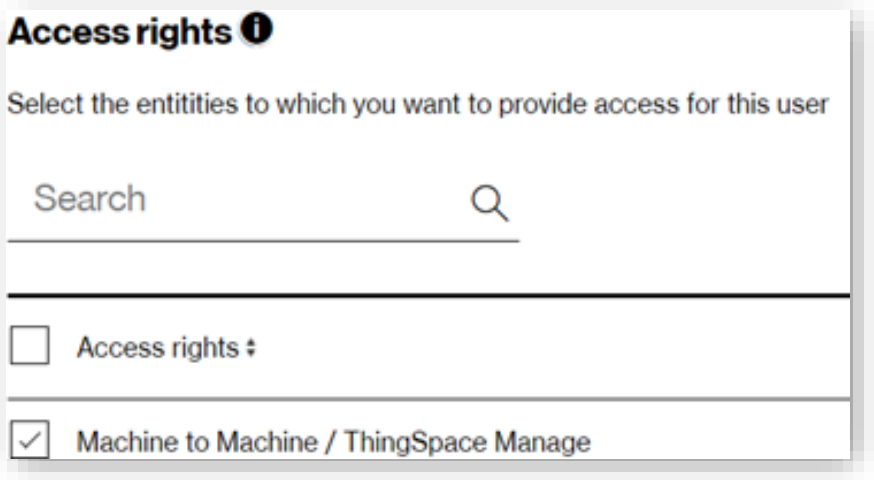
You can log directly into ThingSpace Manage (https://m2mdeveloper.verizon.com/), or log in through My Business (https://sso.verizonenterprise.com/amserver/sso/login.go).

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

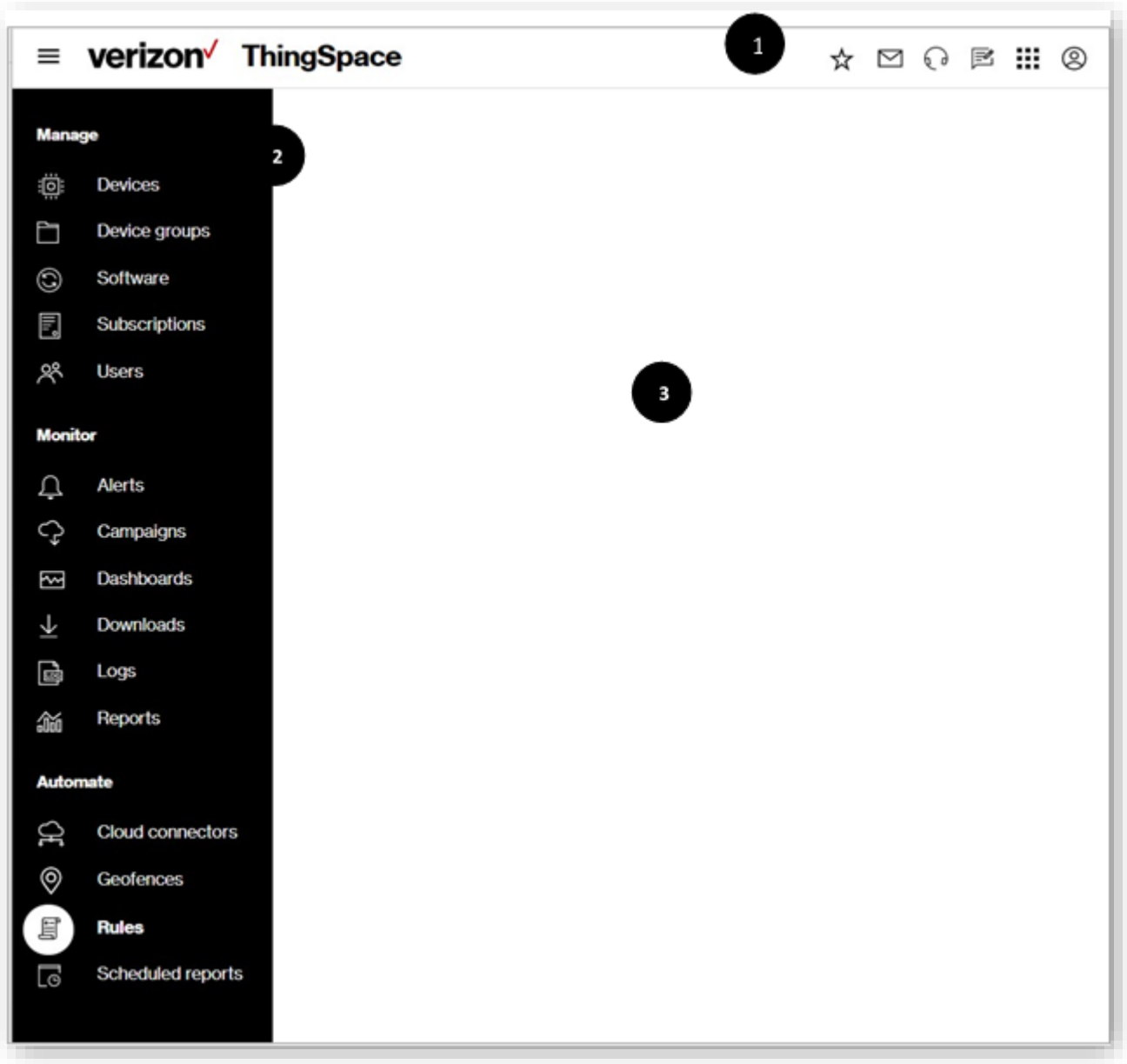
1. On the navigation menu, click **Manage Account**.
2. Select the **ThingSpace Manage** tab next to **Wireless & Mobility.**
3. Click the desired page to start in.

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*.



## Site Stucture

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.

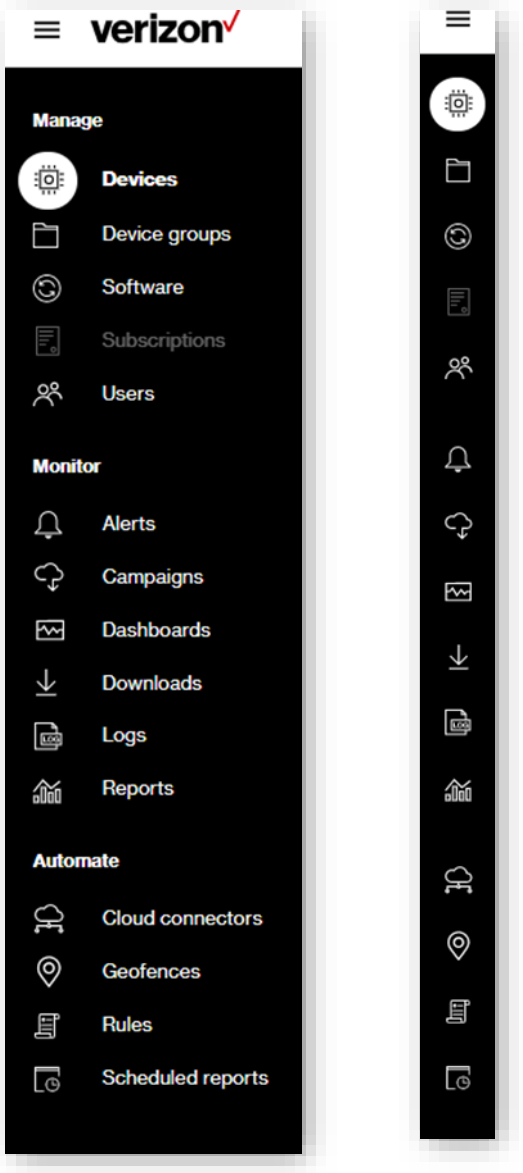
| Elements on the header | | |
|---|---|---|
| 1 | ≡ | Left Navigation – Expand or collapse the left pane with links to various application pages. |
| 2 | | ThingSpace – Open the default home page. |
| 3 | ☆ | Favorites - Open the Favorite links menu. |
| 4 | ✉ | Envelope – Open a coming soon tooltip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

**Expanded view** **Collapsed view**



# 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.

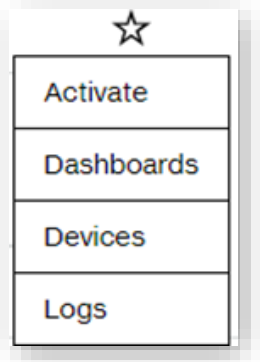
## Default Home Page

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.

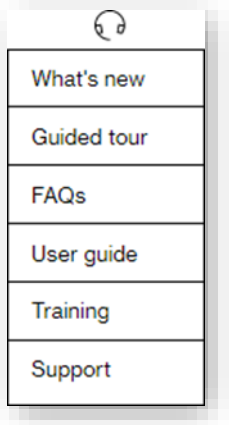



**COMING SOON:** The ability to set your favorite links.

# Support Options

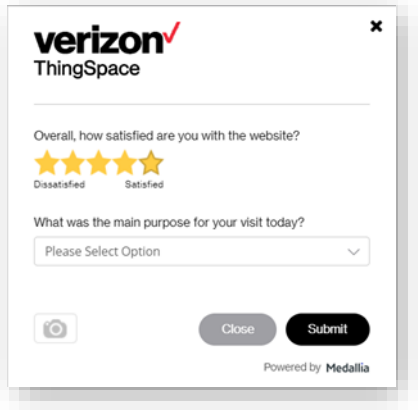
The support icon displays a menu containing links to:

- 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.



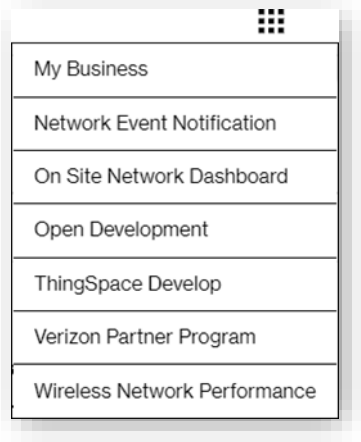
# Providing Feedback

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 Applications

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

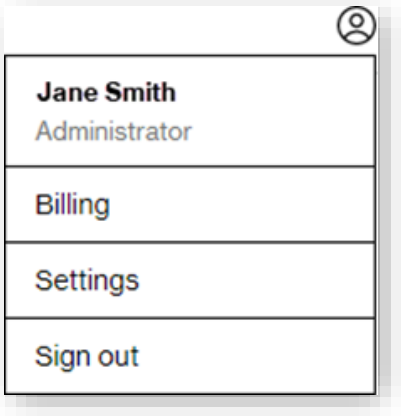



## Profile Options

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.

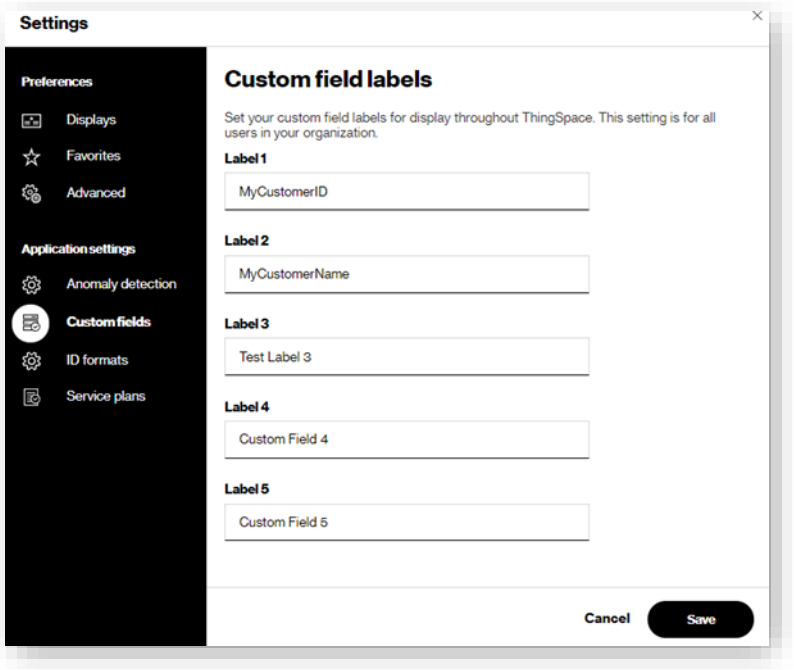
Go to My Business to view your bill. View user and application settings

## Sign out of the portal.



# Settings

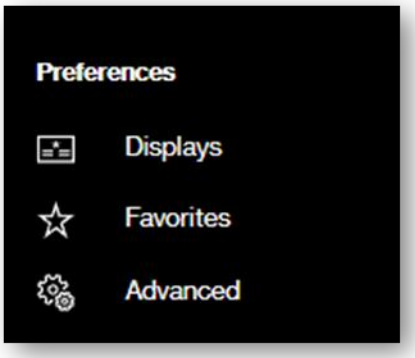
Manage user preferences and application settings here. Click the side navigation to access each section.




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

# Preferences

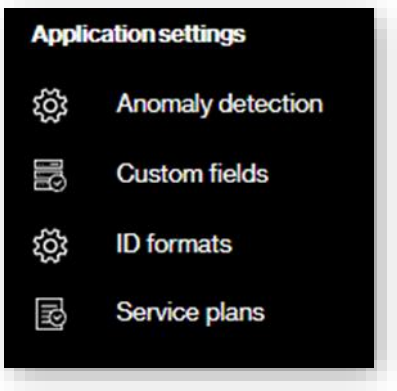
Preferences are *user-specific* settings that allow you to customize the portal to your unique choices. Currently, the **Displays** page supports the setting of a light or dark display mode




**COMING SOON:** The ability add preferred links to your Favorites menu and set advanced customizations.

# Application Settings

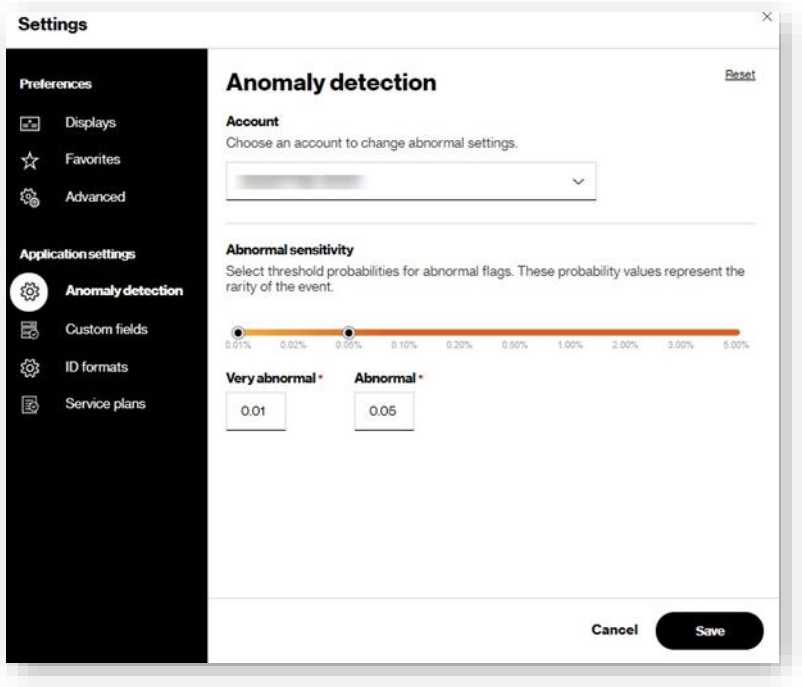
Application settings allow Administrators to set certain attributes that apply across the portal. Changes to application settings impact all users.



# Anomaly Detection

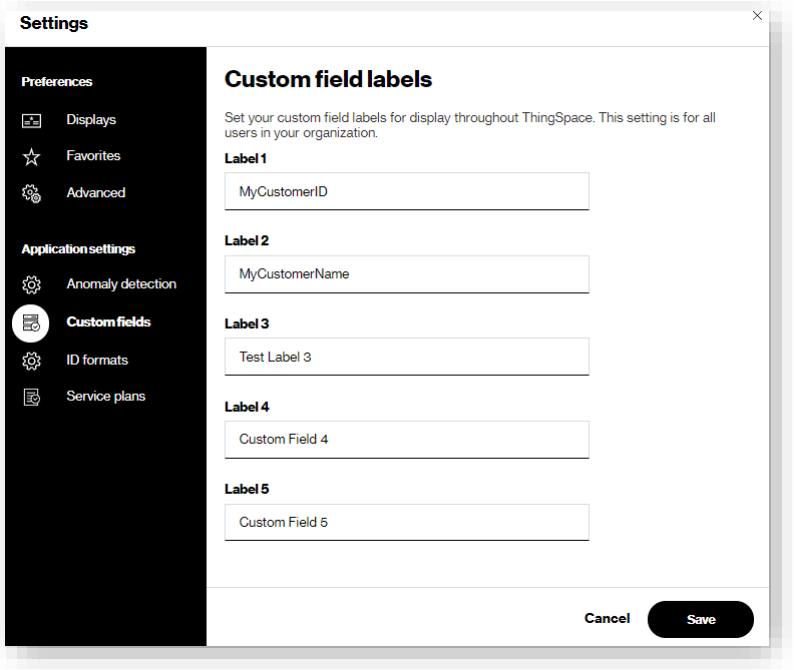
For users subscribed to the ThingSpace premium Intelligence bundle, use the *Anomaly detection* settings to set sensitivity thresholds. Anomaly detection uses machine learning to classify and cluster different devices on your account and alert you for unusual behavior in the device data usage patterns. 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.



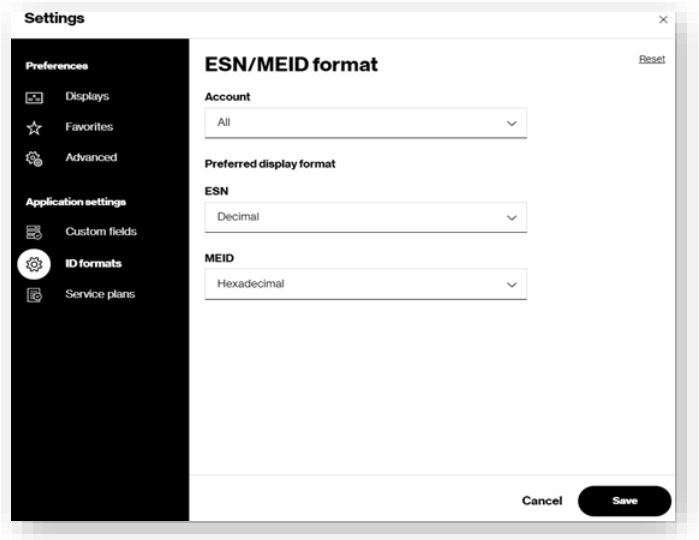
# Custom Fields

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.



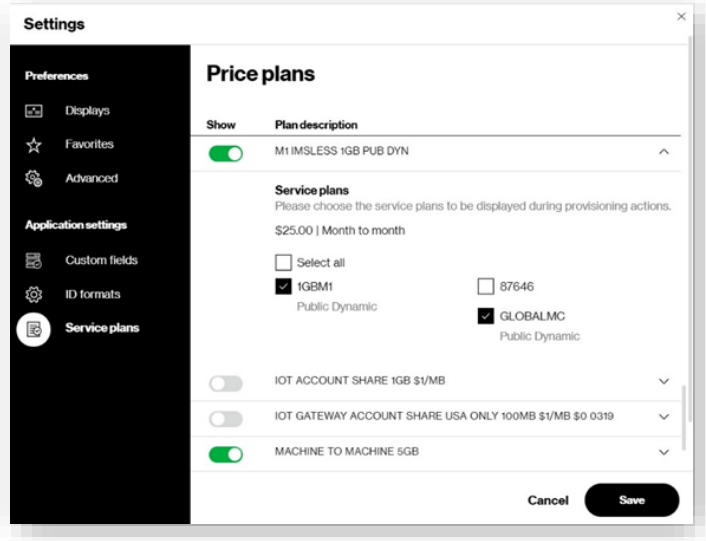
## ID Formats

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.

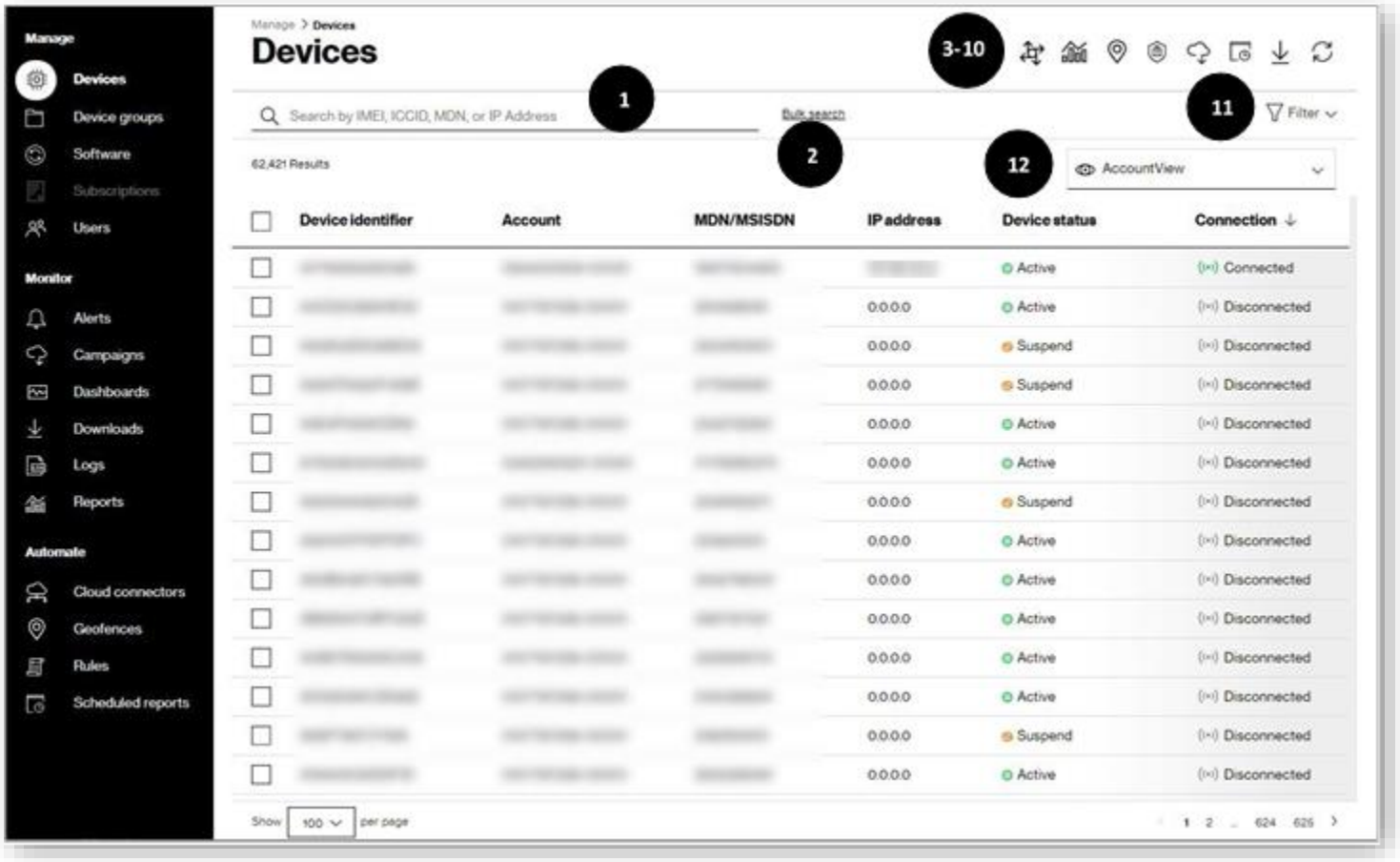



To hide a price plan completely, toggle *Show* to off so that it appears gray. To show the price plan, toggle *Show* to on so that it appears green. To hide a service plan, open the price plan panel by clicking the down arrow. This shows all the service plans that belong to the price plan. Then, check 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.



## Elements on the Devices page

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

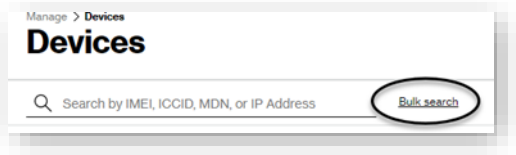
**NOTE:** Search does not support wildcards for IP address. You must search for the exact IP address.

# Performing a Bulk Search

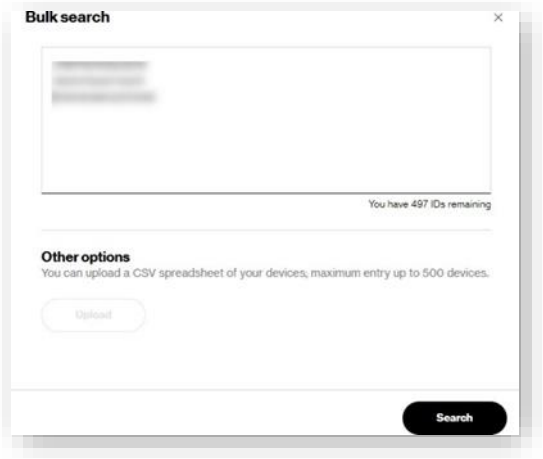
You can search for up to 500 devices at a time using the Bulk search link.

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.

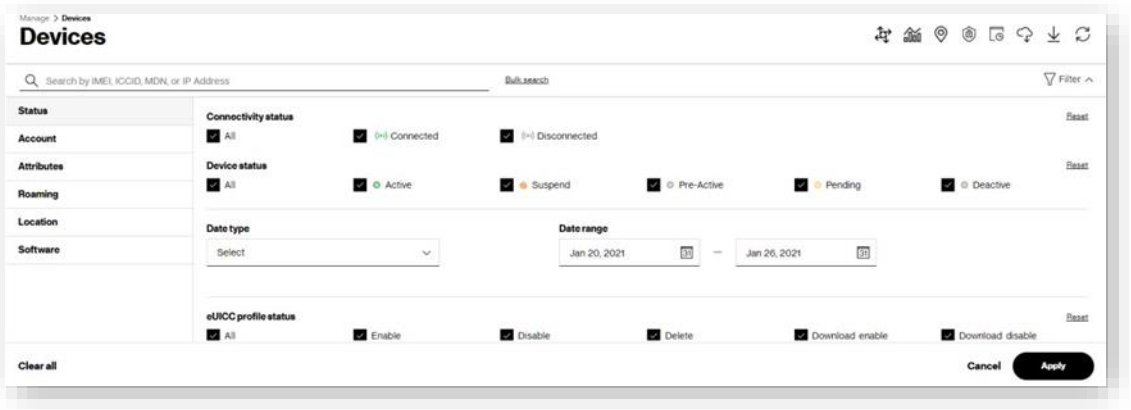
## Applying Filters

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:

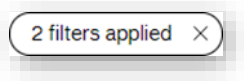
Status Account Attributes Roaming Location Software.

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.

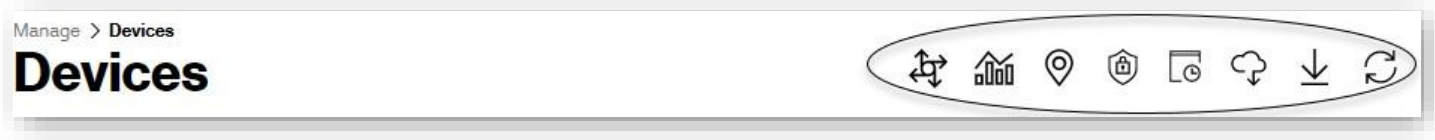
**COMING SOON:** The ability to save filters!

## 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.

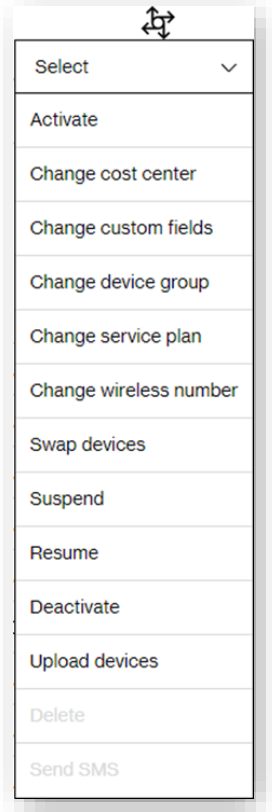
## Taking Actions

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:

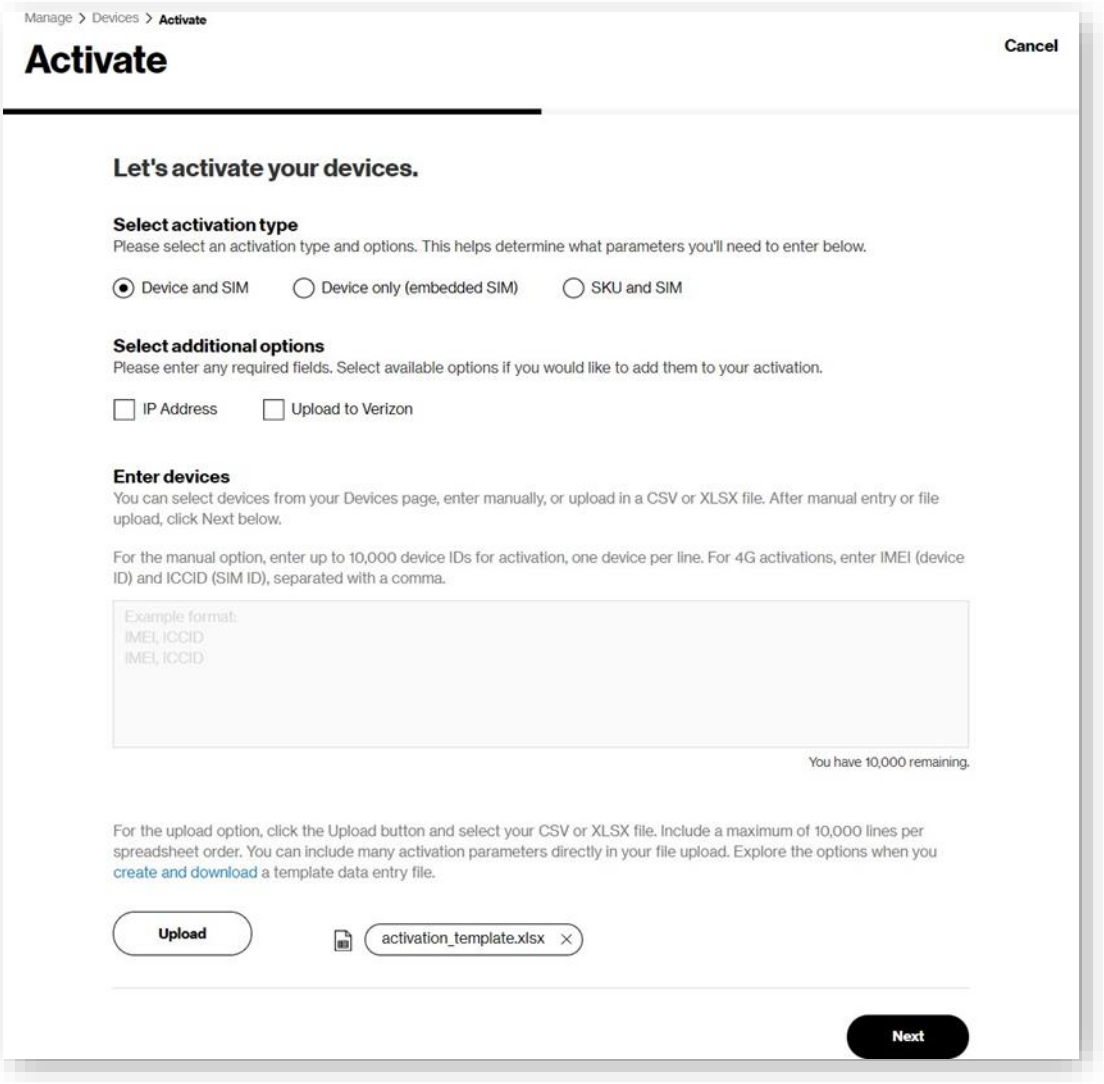
- **Bulk actions** – Take actions on a list of devices that you enter manually or upload from a file.
- **Quick actions** – Take actions on devices selected from the devices list.

# Activating Devices in Bulk

## How to activate devices in bulk

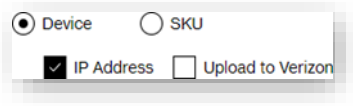
On the left navigation, click **Devices**. The *Devices* page opens.

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

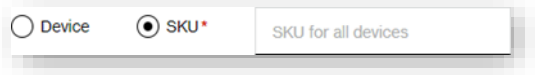


2. Select the type of activation (Device or SKU).

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.



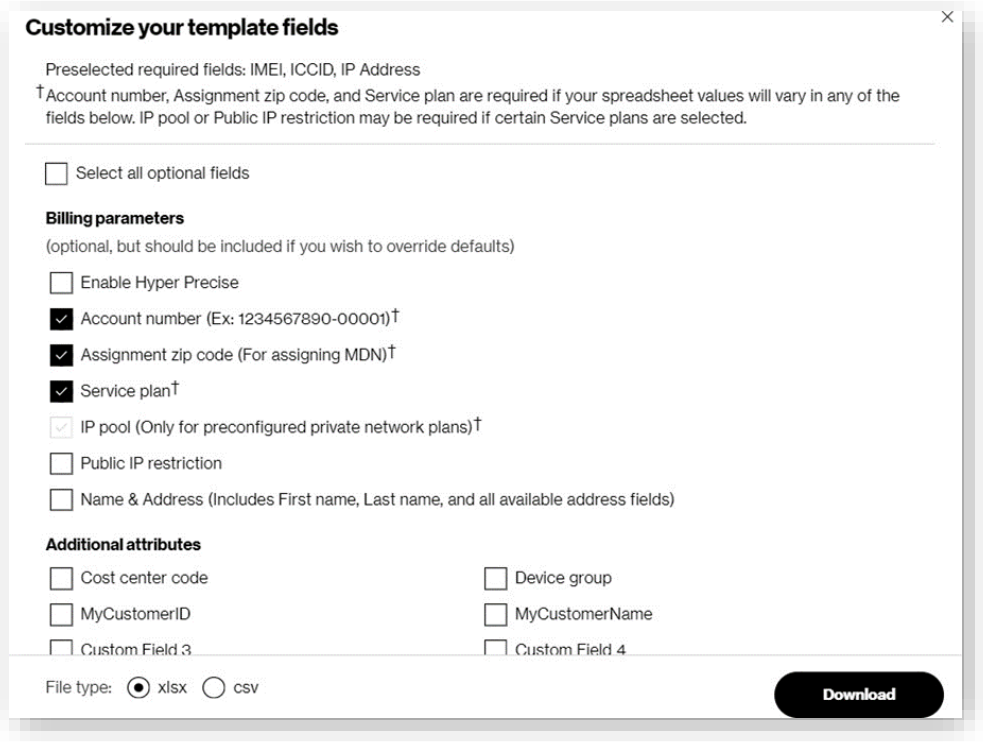

For *SKU*, type the Verizon SKU ID and then enter the list of ICCIDs.




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.

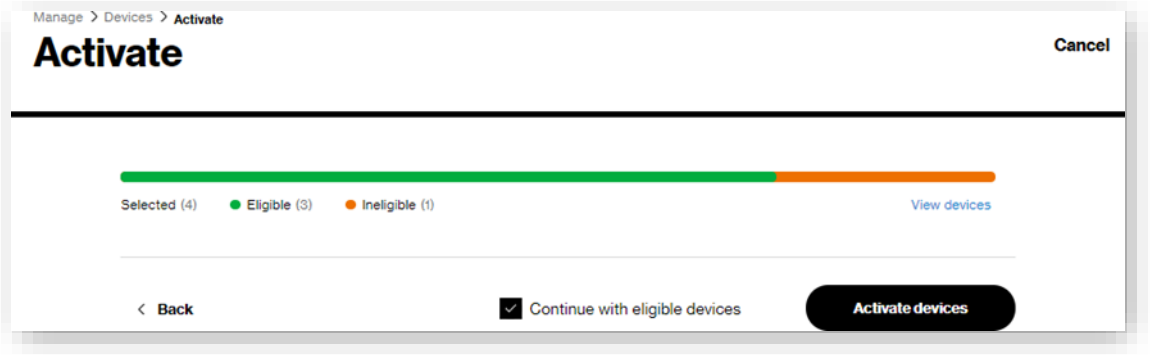



a. Click **Download** to download the customized template.

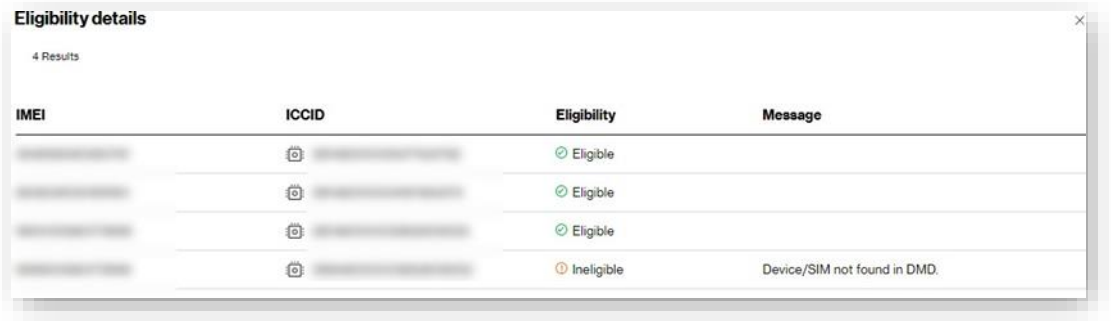
b. Add your data to the template file and save. You can have different values for each column in the template.

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.




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

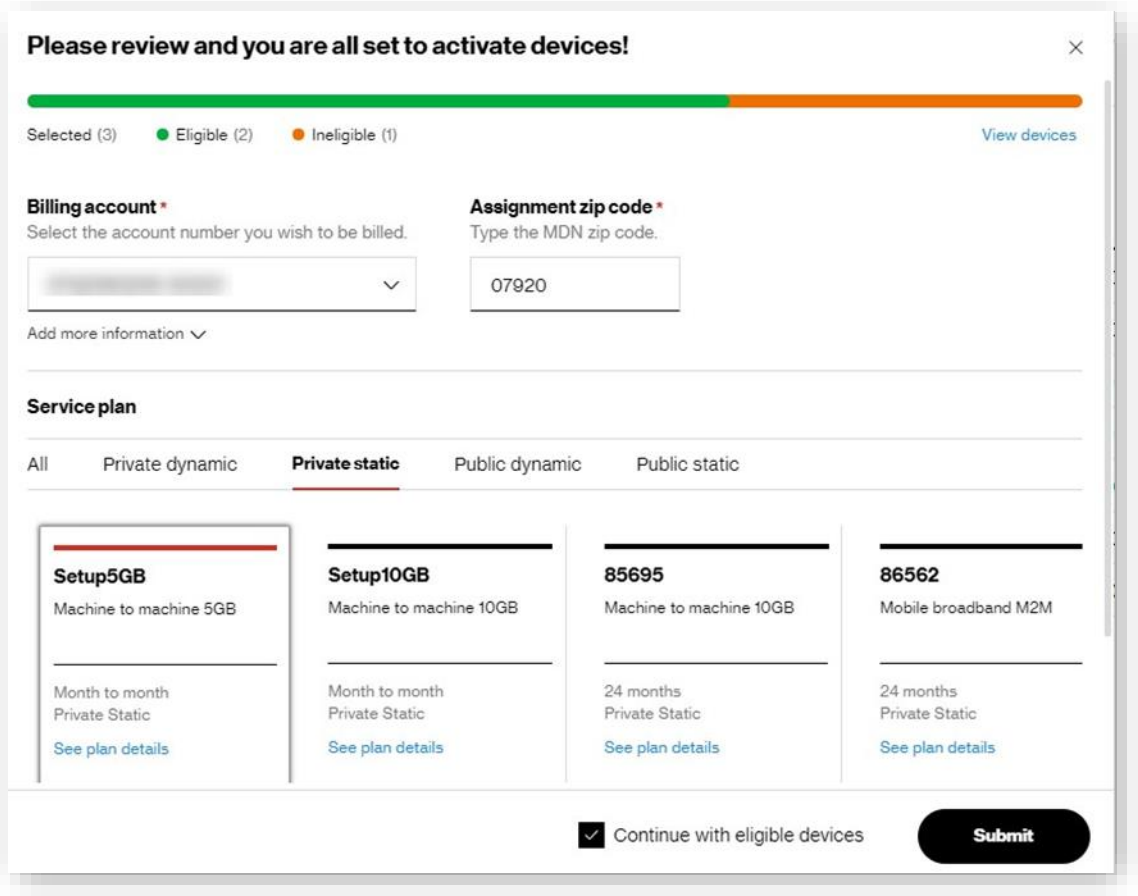
# Quick Activations

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.

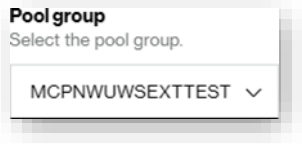
1. Select devices using the *Device identifier* checkbox.
2. Click the actions icon and select **Activate**. A review page opens.



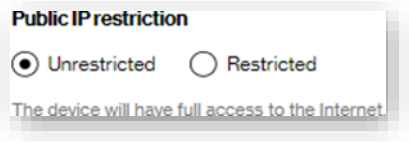

3. Review eligible and ineligible device counts.
4. Review the **Billing account** and **assignment zip code**, revising them if necessary. The zip code determines the MDN assigned to your devices when activated.

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.



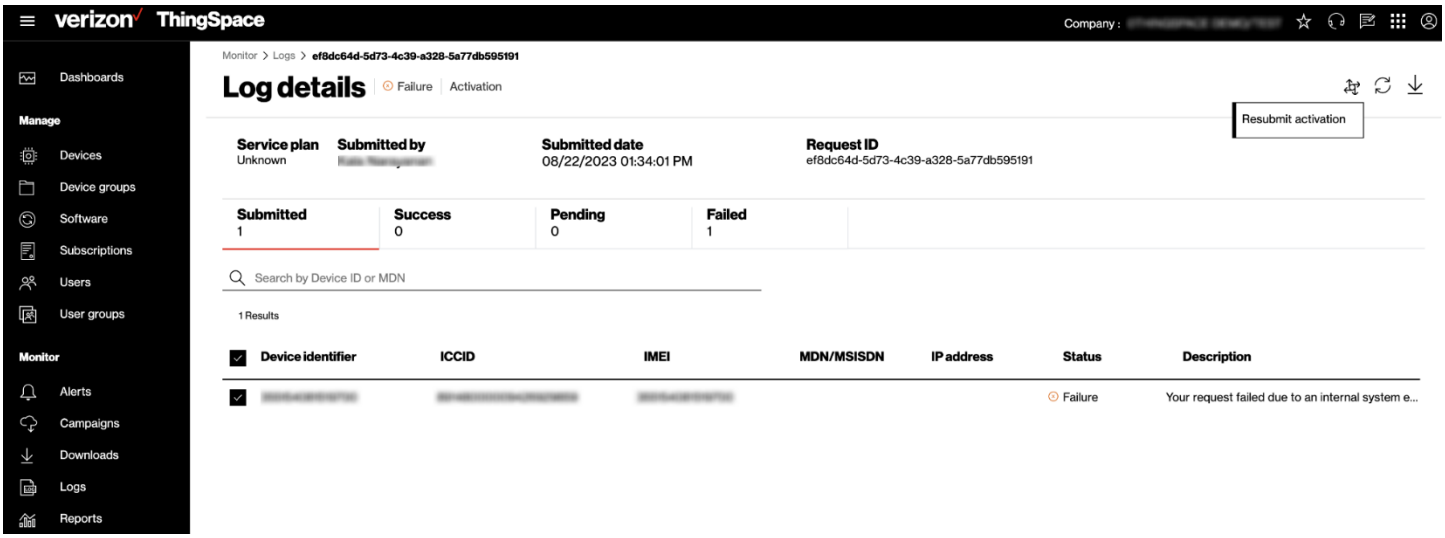

For public static plans, you can choose the type of restriction to apply. Unrestricted IPs provide full access to the Internet. Restricted IPs have limited access to content provided by Verizon Wireless and are restricted from accessing the Internet.




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":

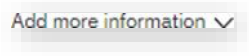


# Assigning Attributes and Saving Address locations

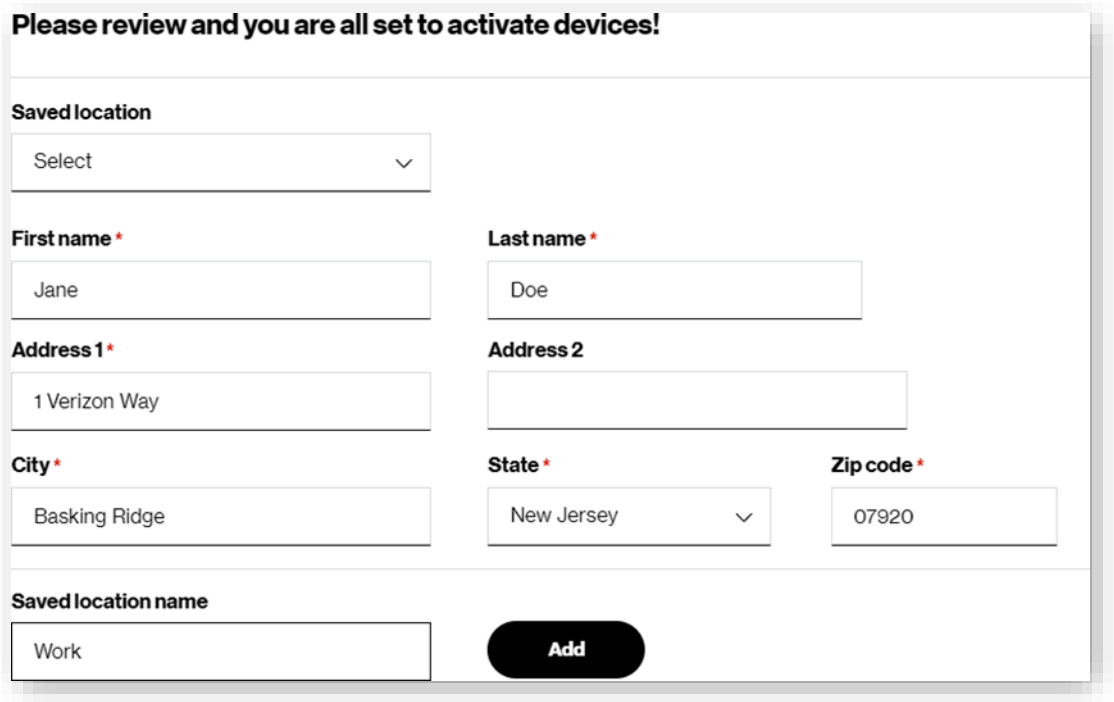
To assign attributes and save address locations

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.



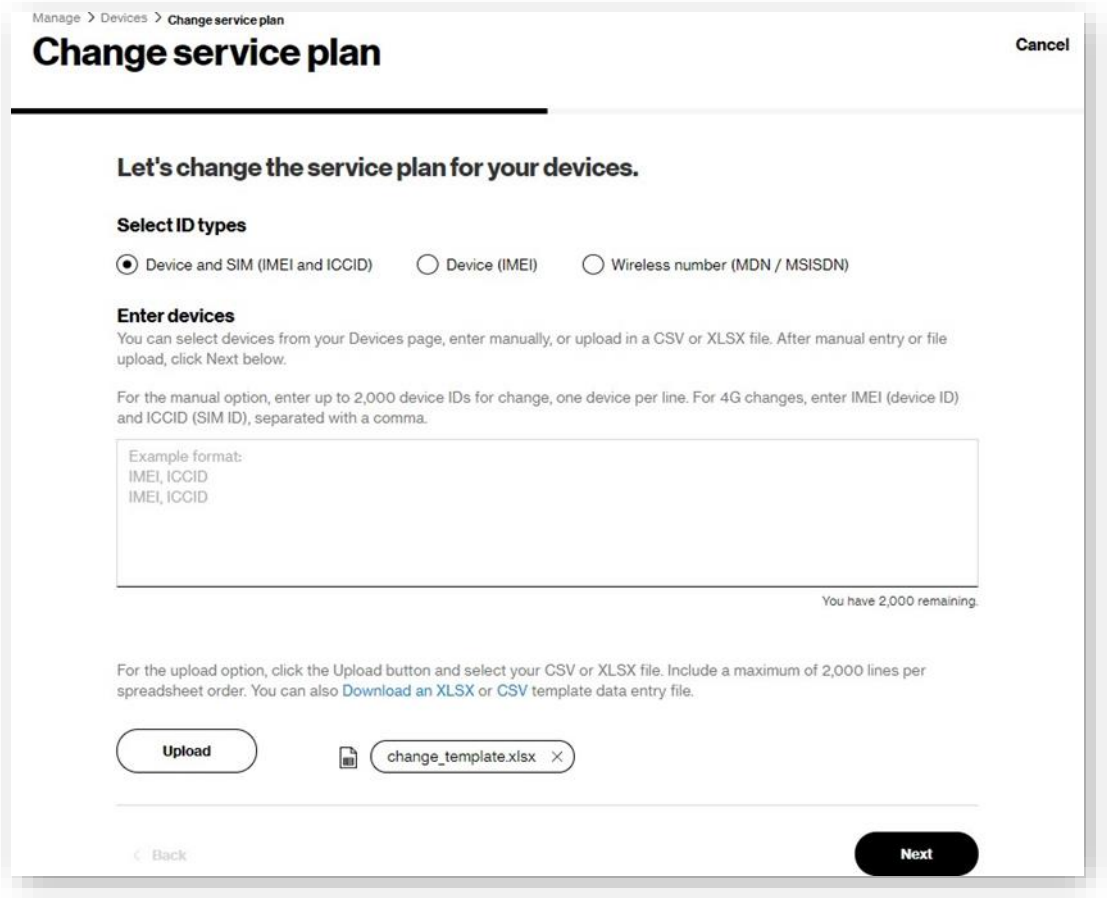

3. Click **Submit** to complete the device activation.

# Bulk Service Plan Changes

## How to change service plans in bulk

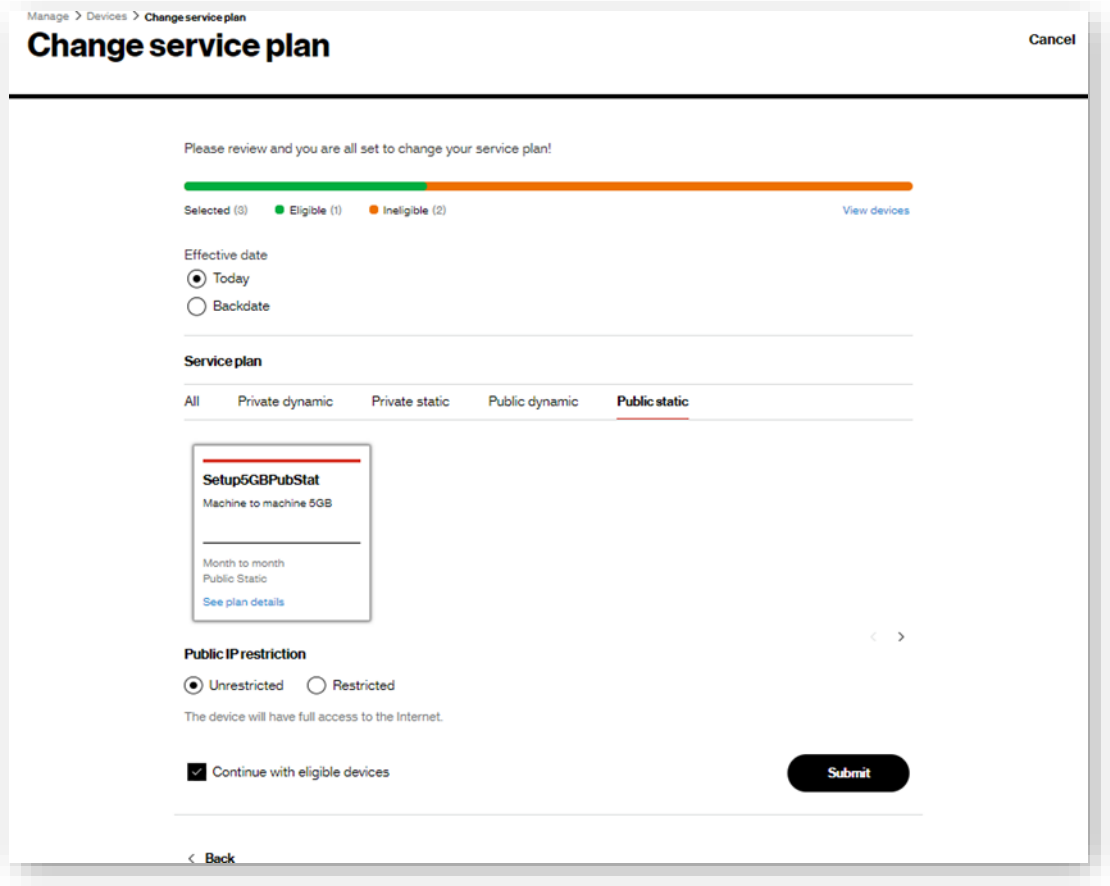
On the left navigation, click **Devices**. The *Devices* page opens.

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

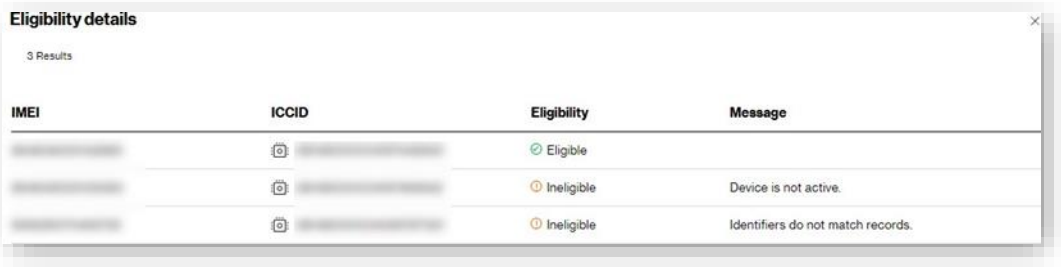



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data to the template file and save.
    c. Click **Upload** to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

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

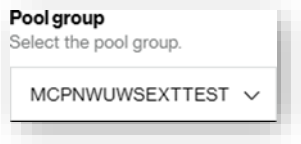



5. Review eligible or ineligible device counts. To view the list of the devices and any associated error messages, click **View devices**. The Eligibility details dialog opens.

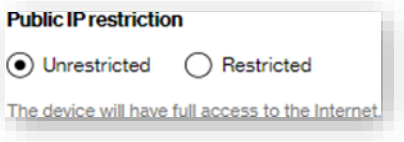



6. Select the **Effective date**. You can select today's date, or backdate it so that the plan change takes effect at the beginning of the billing cycle.
7. Assign a **Service plan** to the devices. You can filter the service plans by clicking **Private dynamic**, **Private static**, **Public dynamic**,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

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.




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.




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

# Quick Service Plan Changes

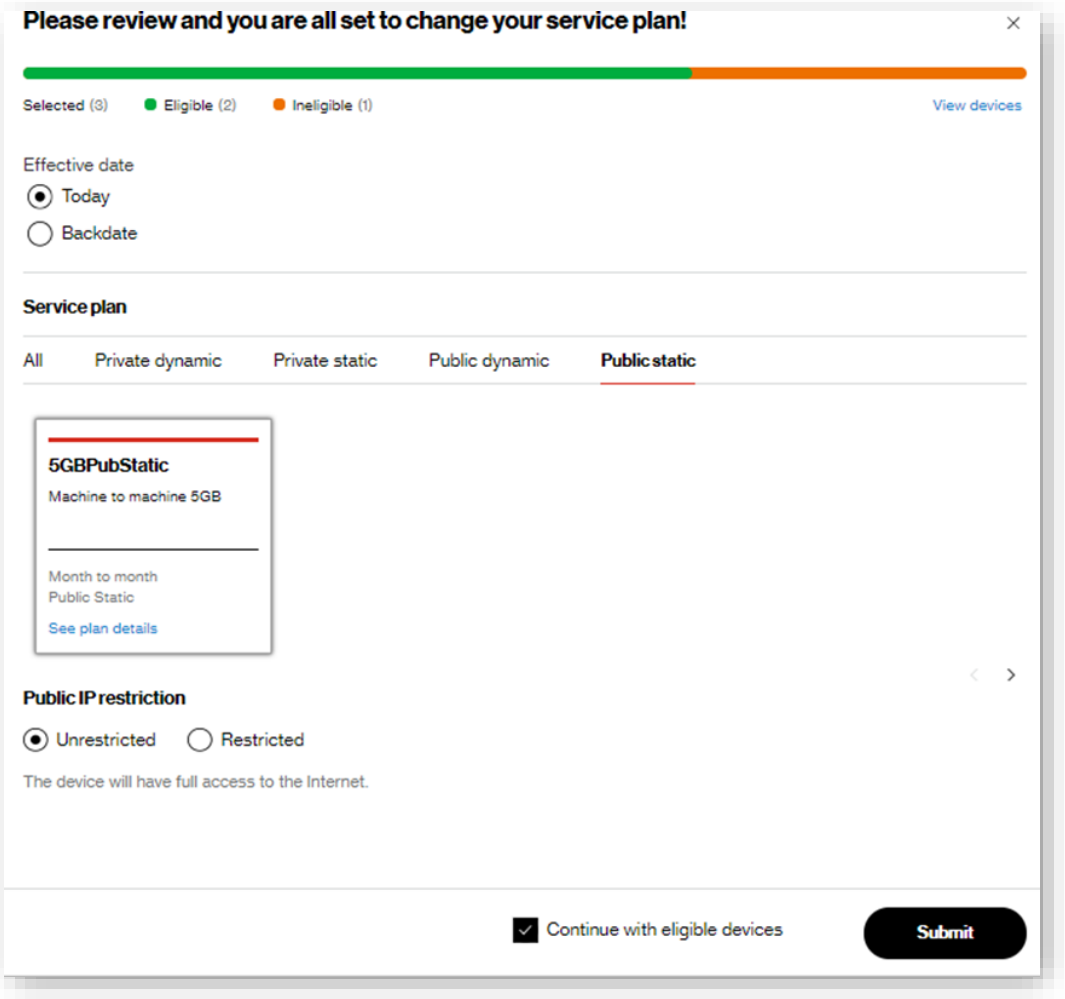
How to make quick plan changes on selected devices

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

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

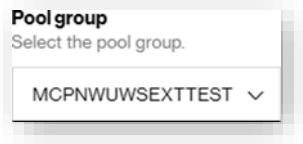
**NOTE:** All selected devices must be from the same billing account.

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

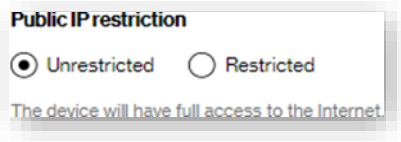



3. Review eligible and ineligible device counts.
4. Select the **Effective date**. You can select today's date, or backdate it so that the plan change takes effect at the beginning of the bill cycle.
5. Assign a **Service plan** for the devices. You can filter the service plans by clicking **Private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

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 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.



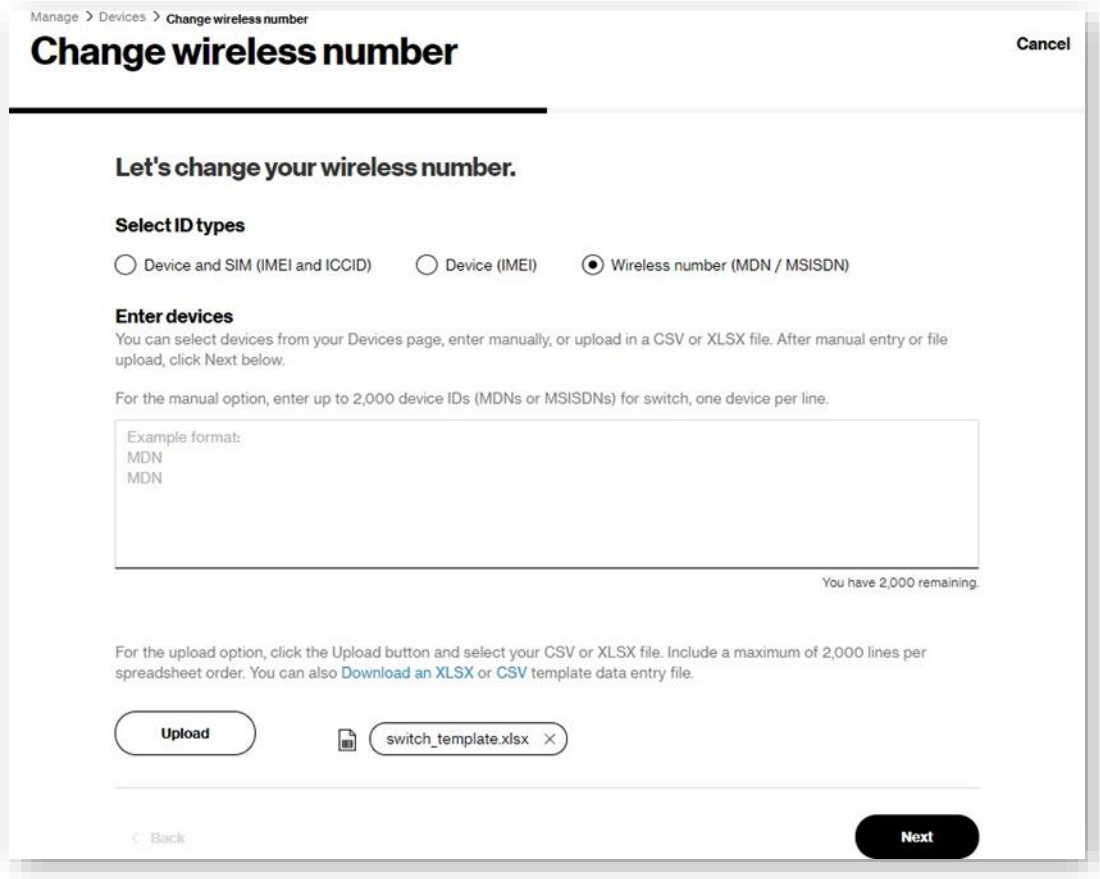

6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

# Bulk Wireless Number Changes

## How to change wireless numbers in bulk

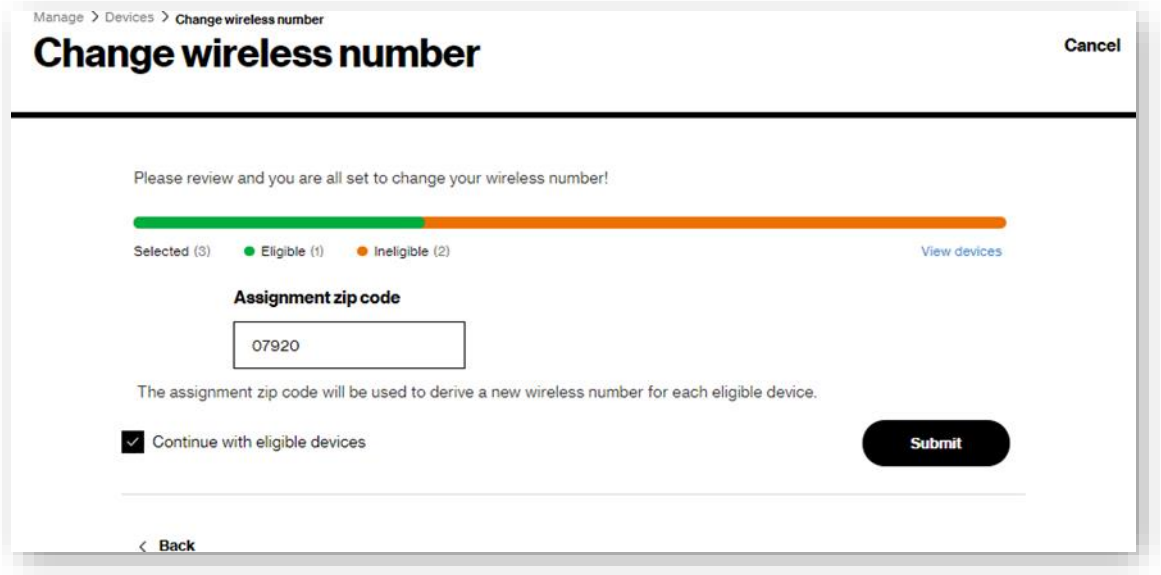
On the left navigation, click **Devices**. The *Devices* page opens.

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

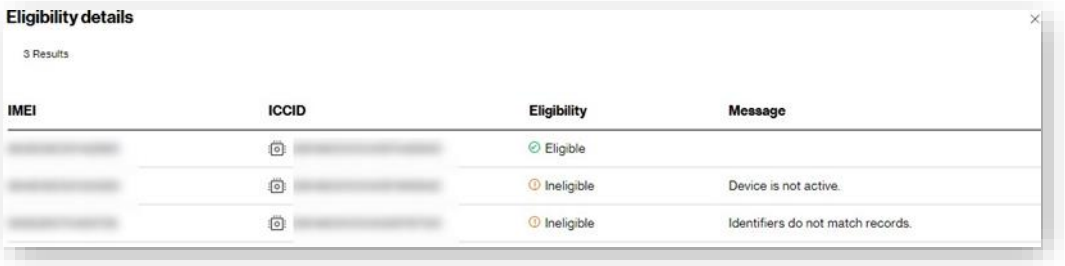



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** link to download the template.
    b. Add your data to the template file and save.
    c. Click **Upload**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

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




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




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

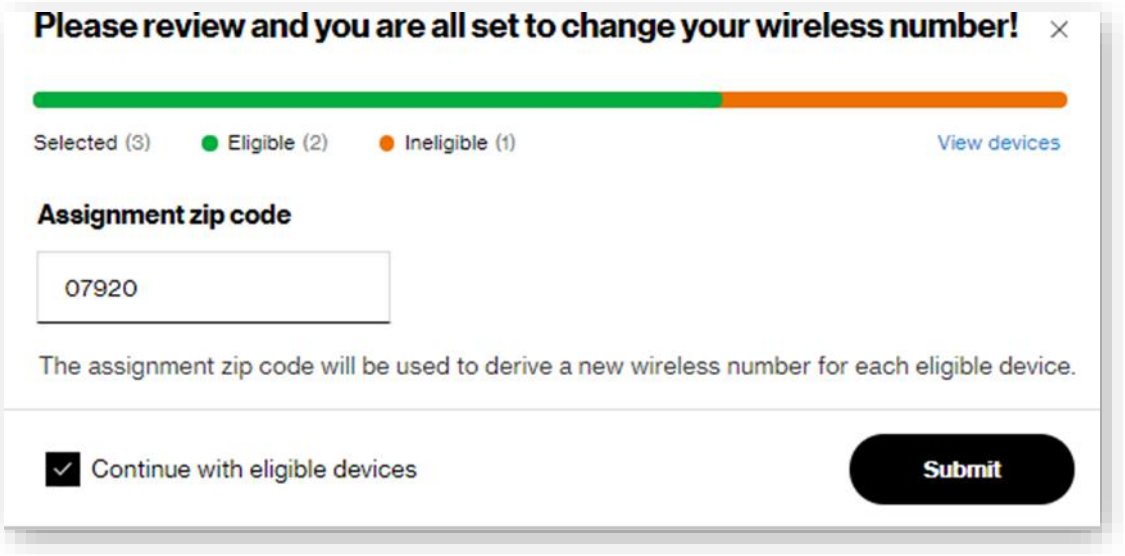
How to make quick MDN changes on selected devices

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.



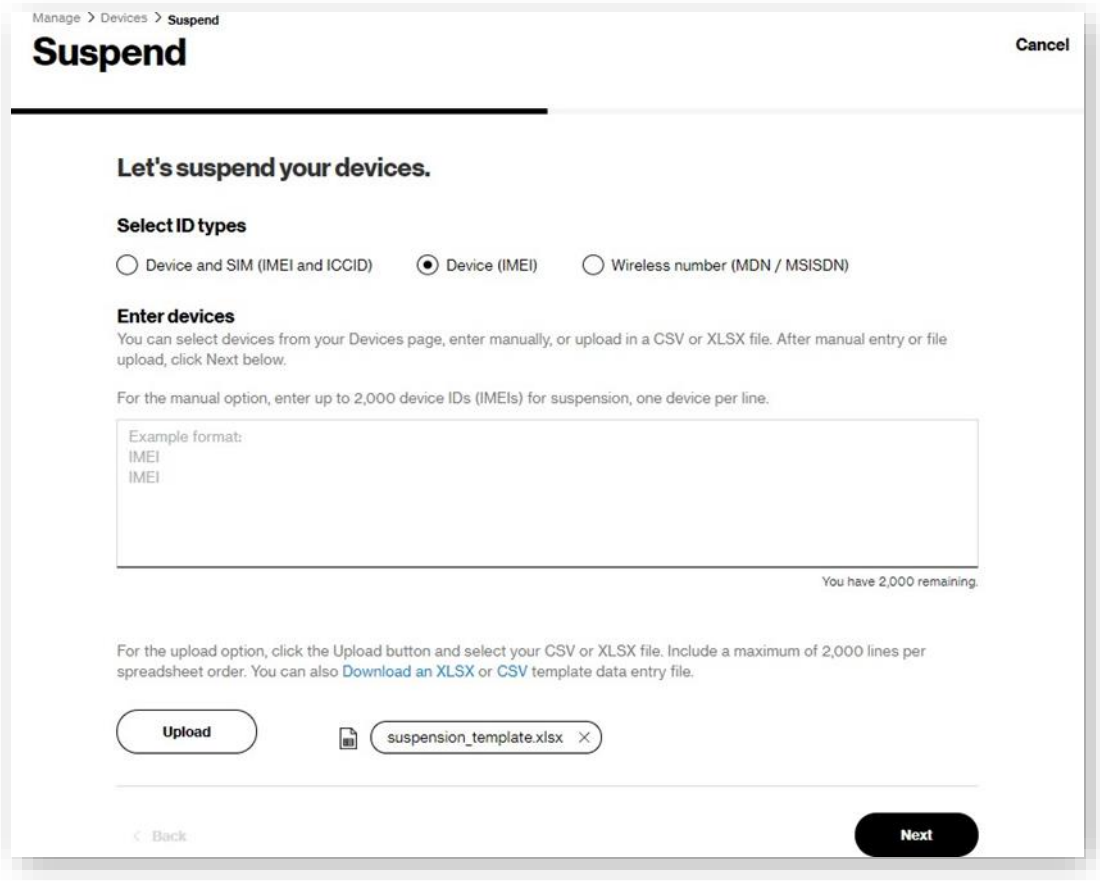

3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Enter the **Assignment zip code**. The assignment zip code determines the wireless number for each eligible device.
5. Check **Continue with eligible devices** if necessary to proceed.
6.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

# Suspending Devices in Bulk

## How to suspend devices in bulk

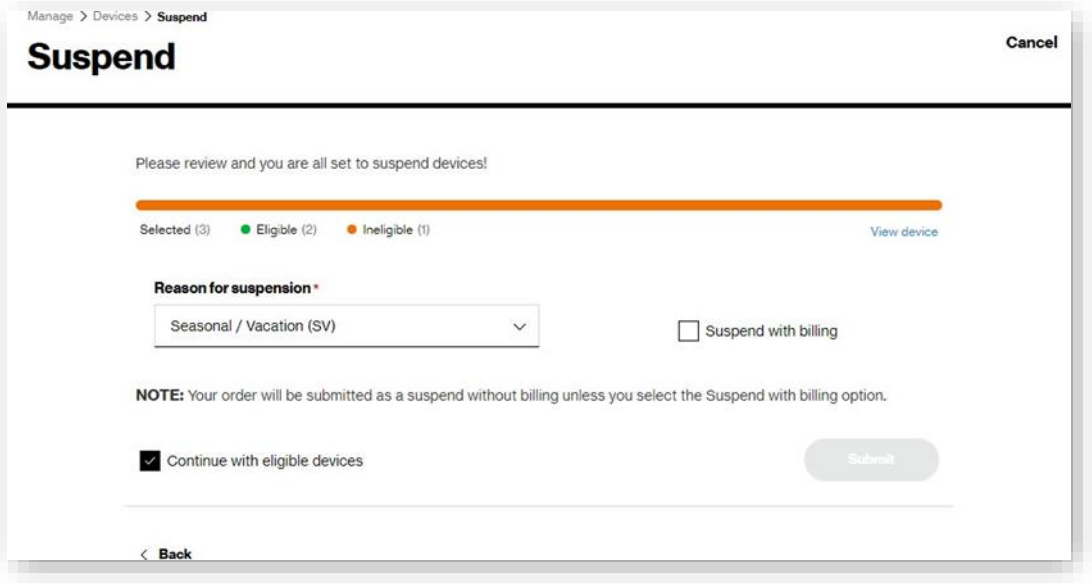
On the left navigation, click **Devices**. The *Devices* page opens.

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

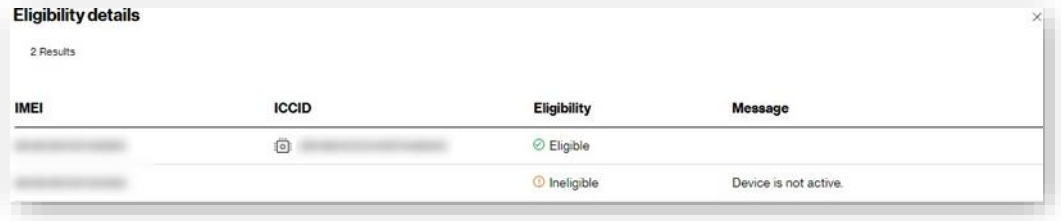



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click the **Download an XLSX or CSV** link to download the template.
    b. Add your data to the template file and save.
    c. Click **Upload**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

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




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




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

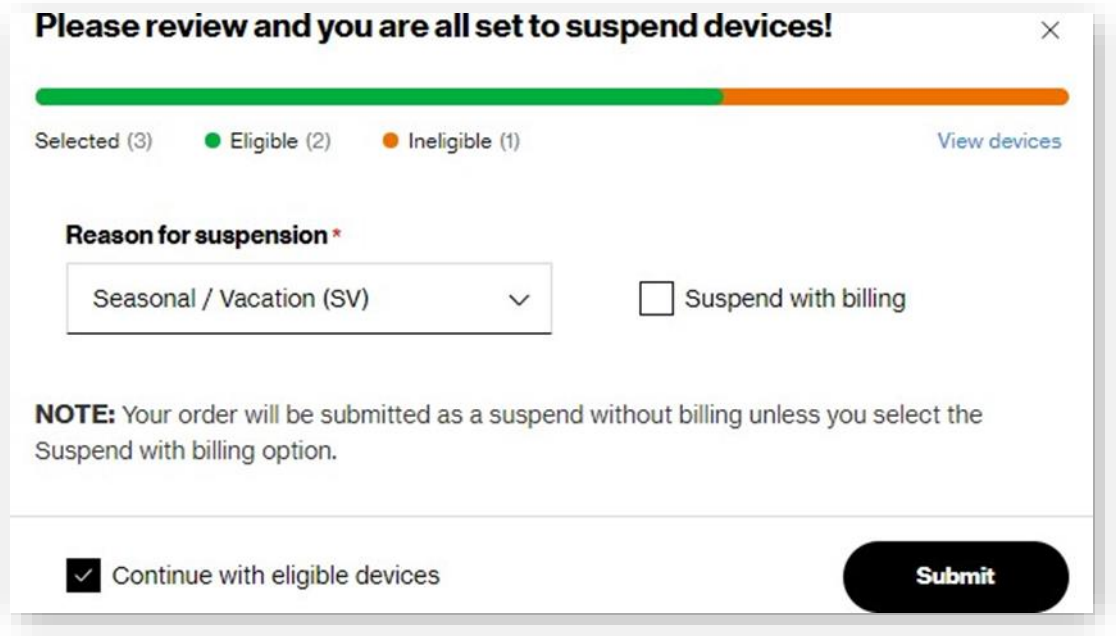
## How to suspend devices

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.



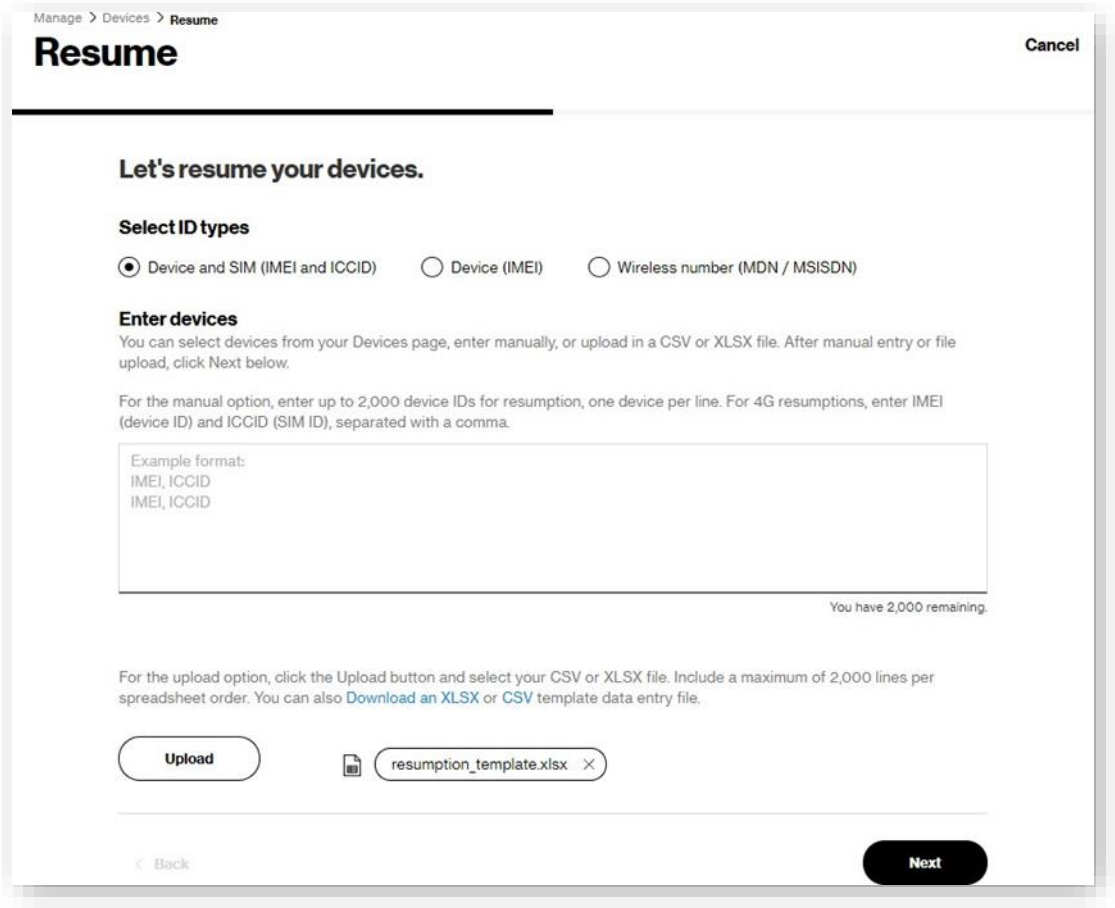

3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Select a **Reason for suspension**. Available reason codes are:
   - Lost / Stolen (21)
   - Seasonal / Vacation (SV)
5. Check **Suspend with billing**. If not checked, the devices are suspended 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

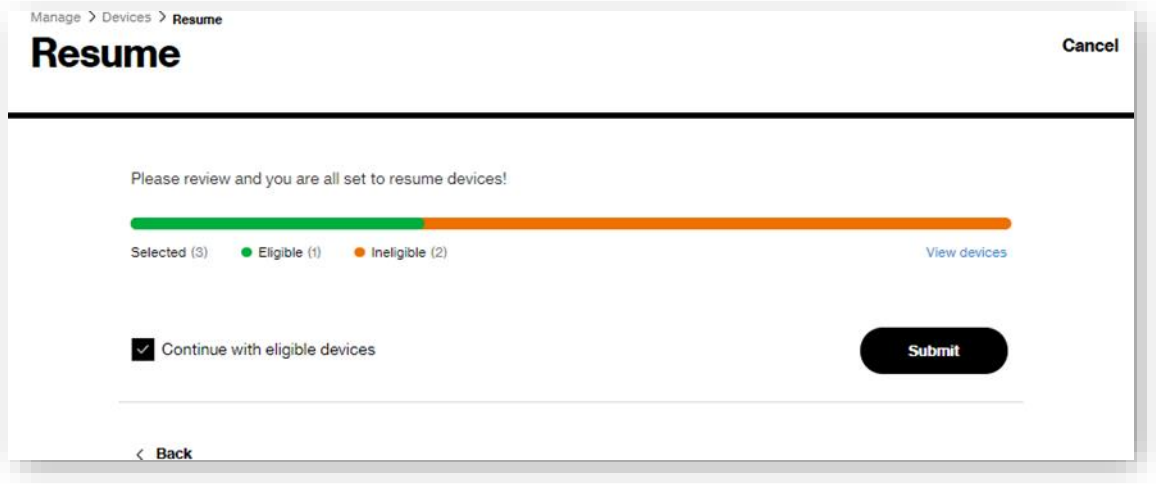
On the left navigation, click Devices. The Devices page opens.

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

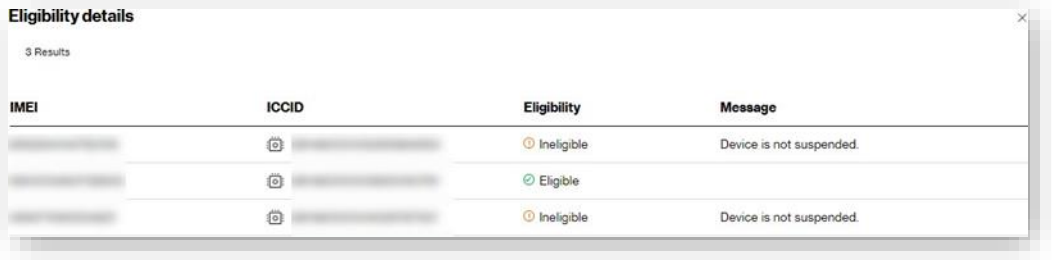



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data to the template file and save.
    c. Click **Upload**.

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.




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

# Quick Resuming Devices

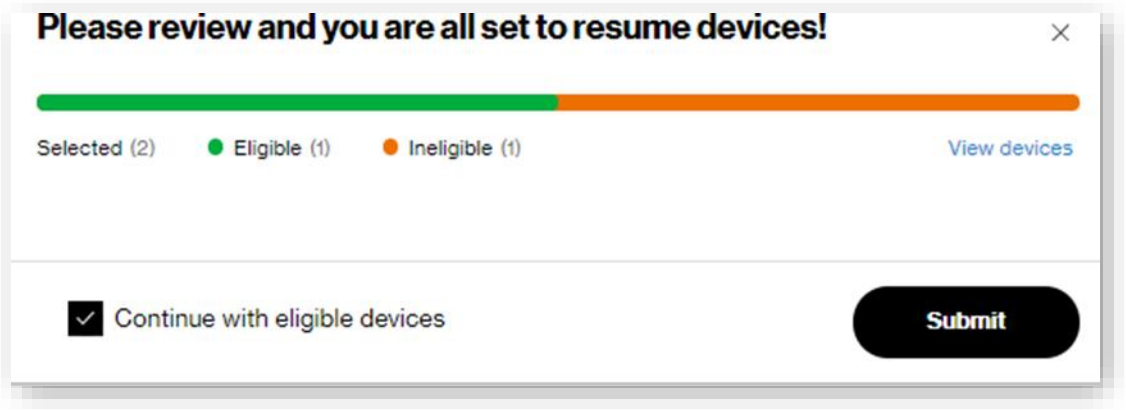
How to resume devices

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.



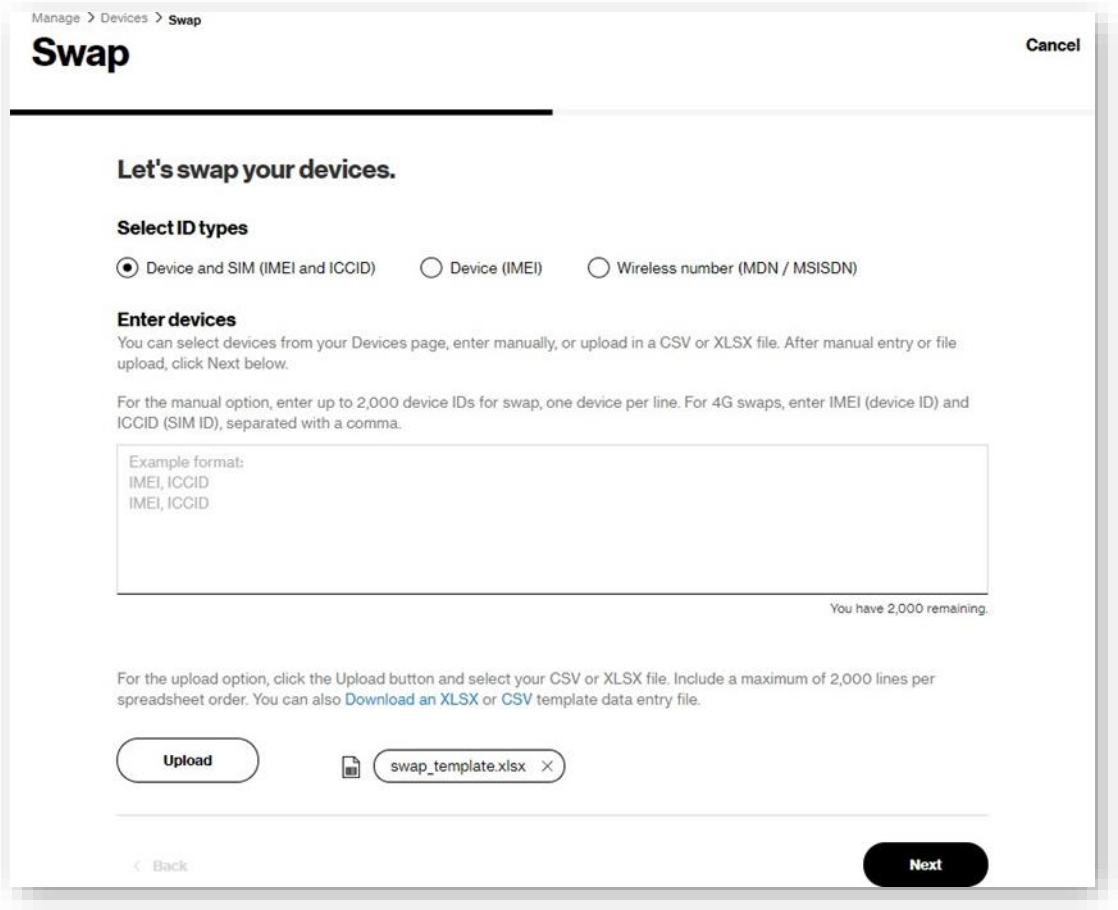

3. Review eligible and ineligible devices counts. To view the list of selected devices, click **View devices**.
4. Check **Continue with eligible devices** if necessary to proceed.
5. Click **Submit** to complete the process.

# Swapping Devices in Bulk

How to swap devices in bulk

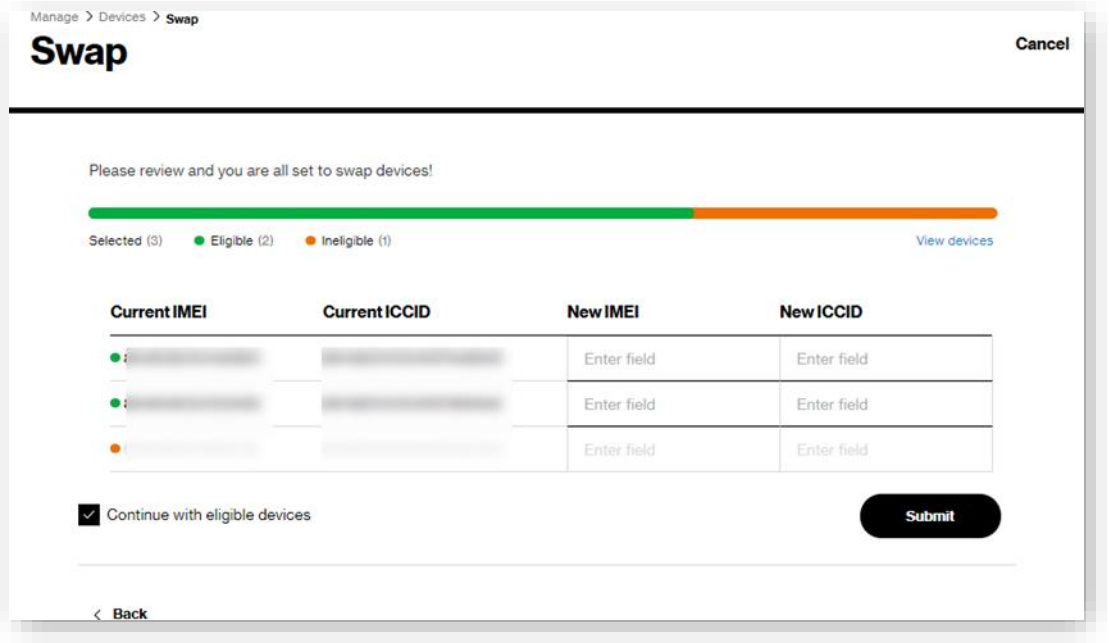
On the left navigation, click **Devices**. The *Devices* page opens.

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

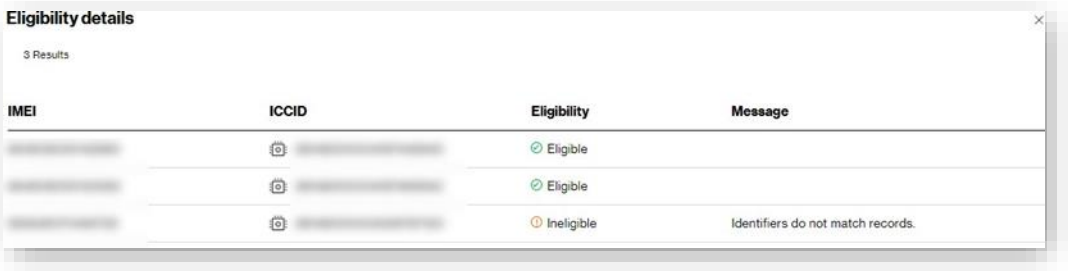



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data and save.
    c. Click **Upload** to complete the upload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

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




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




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

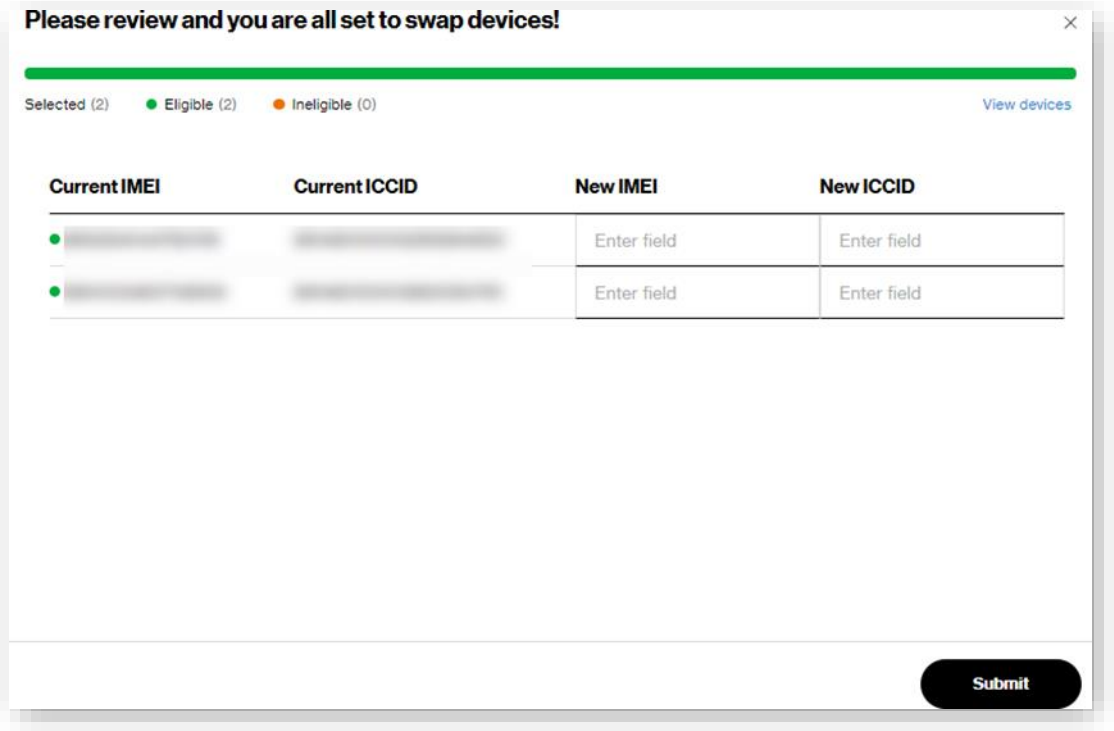
## How to swap devices

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.



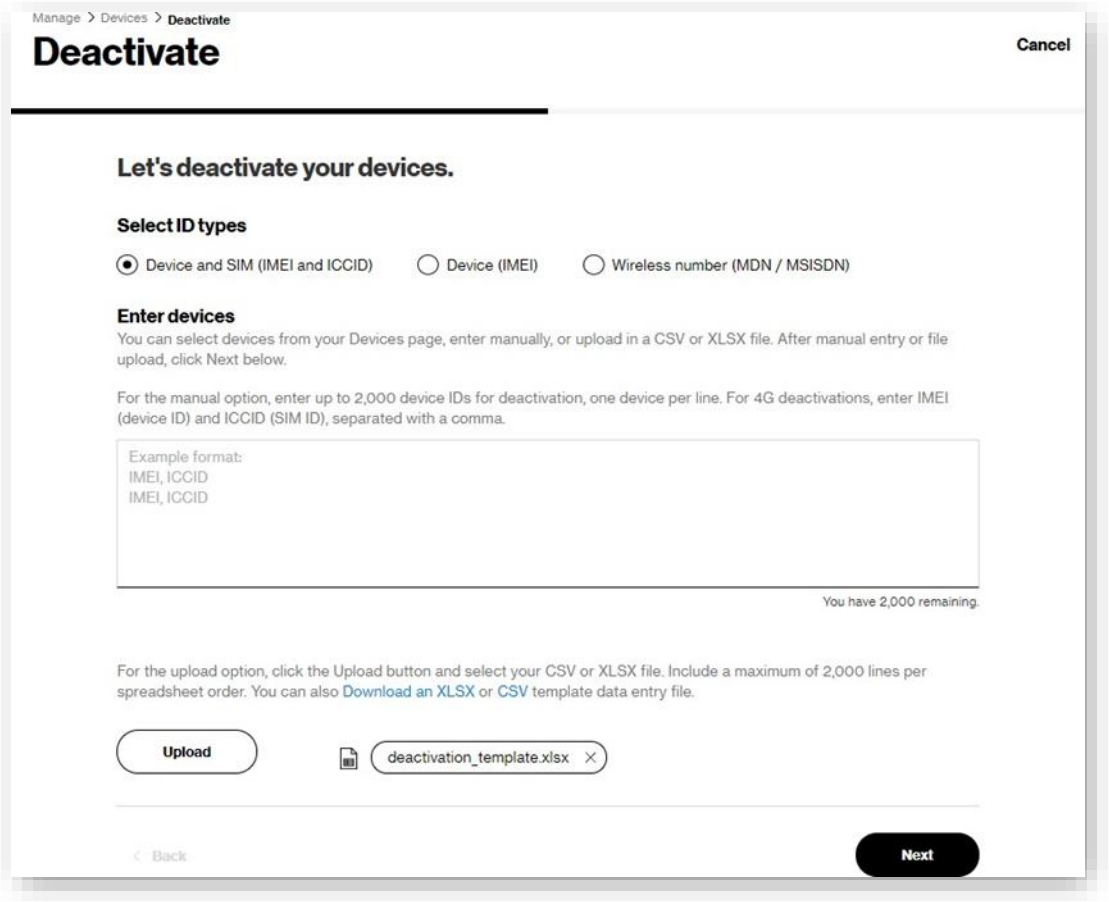

3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Enter a new **IMEI or ICCID** for each device.
5. Check **Continue with eligible devices** if necessary to proceed.
6. Click **Submit** to complete the process.

# Deactivating Devices in Bulk

## How to deactivate devices in bulk

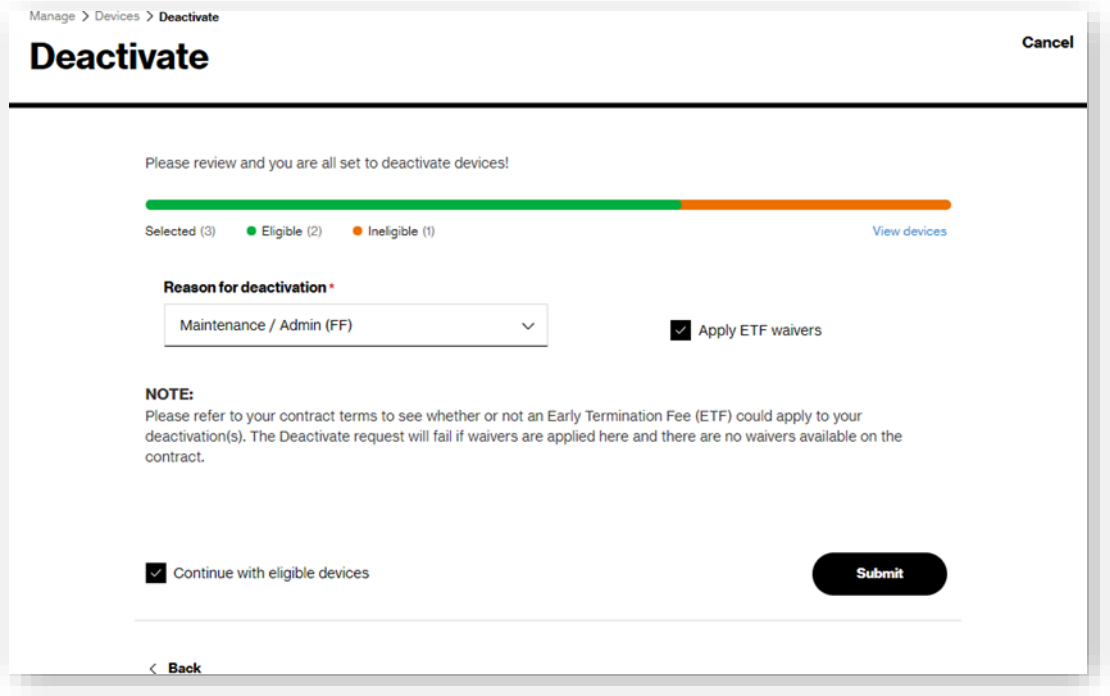
On the left navigation, click **Devices**. The *Devices* page opens.

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

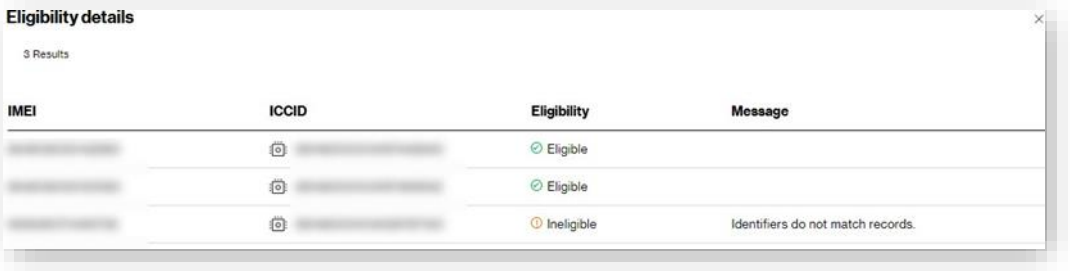



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data and save.
    c. Click **Upload**.

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

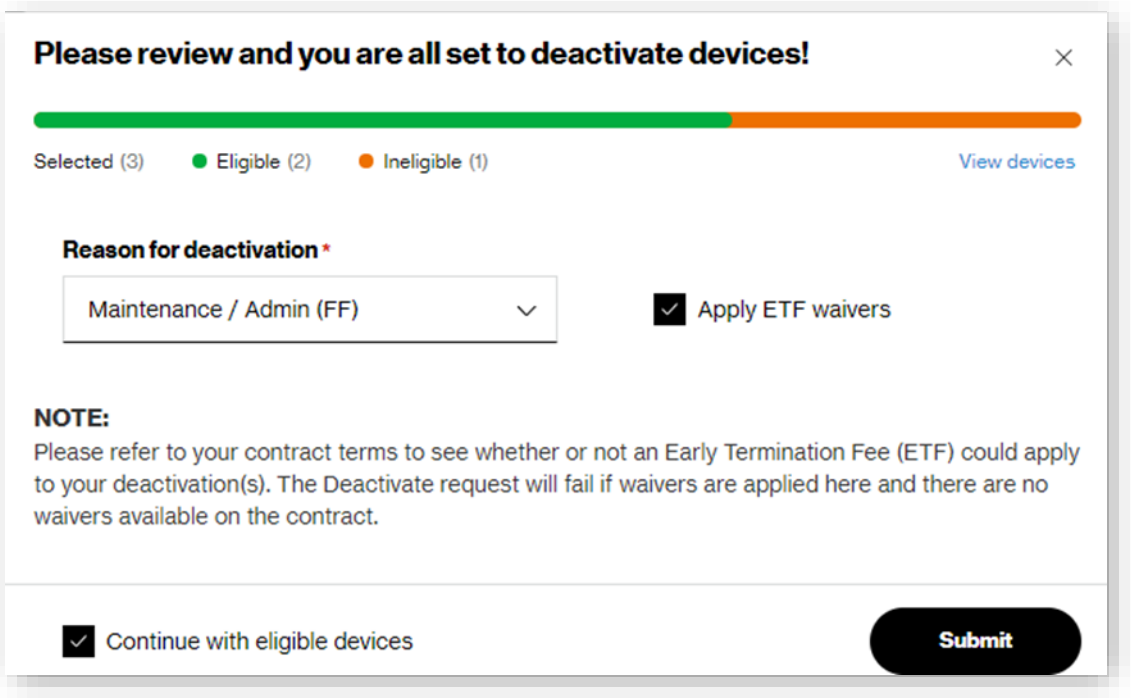
## How to deactivate devices

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.




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

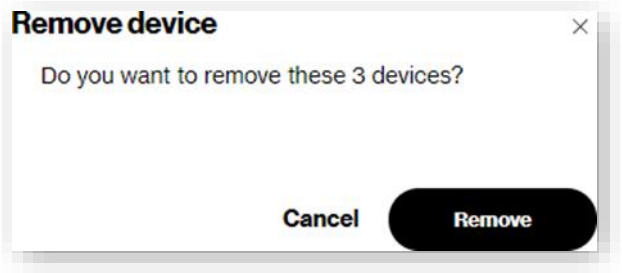
How to remove devices from your plan

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.

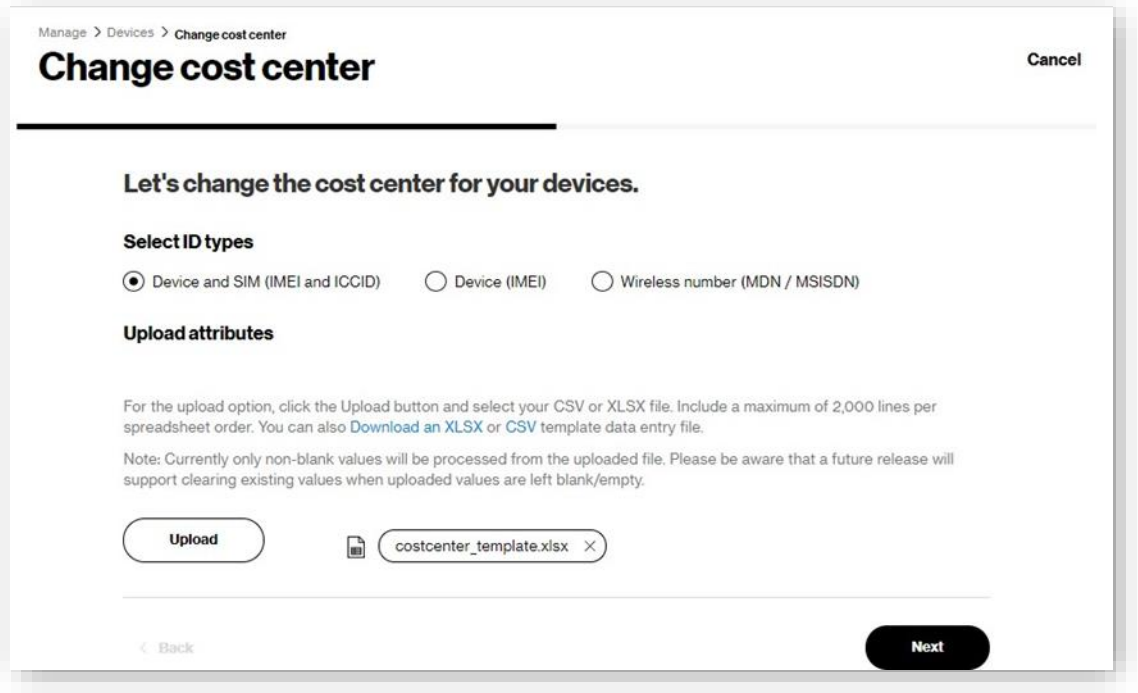
# Changing Cost Center Codes in Bulk

*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

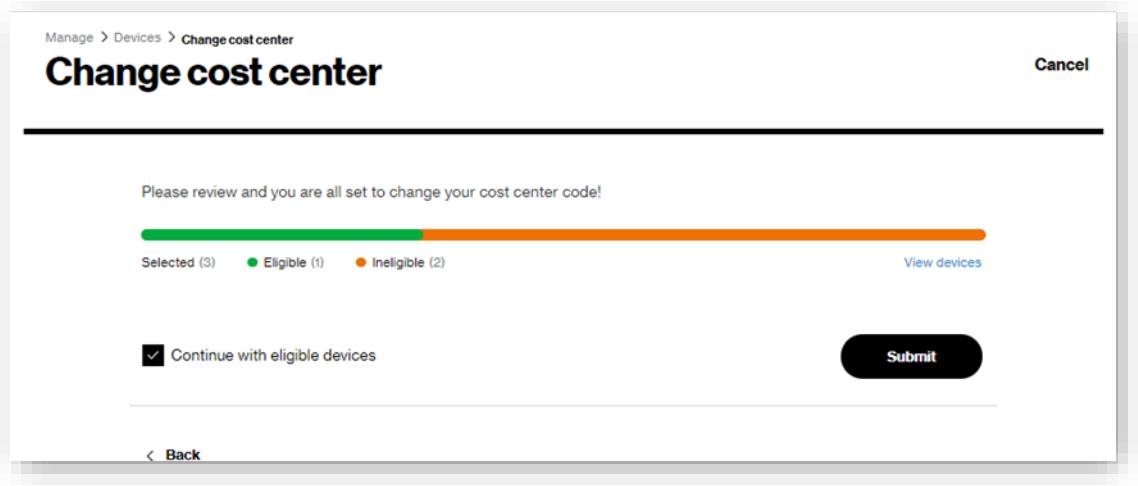
On the left navigation, click **Devices**. The *Devices* page opens.

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

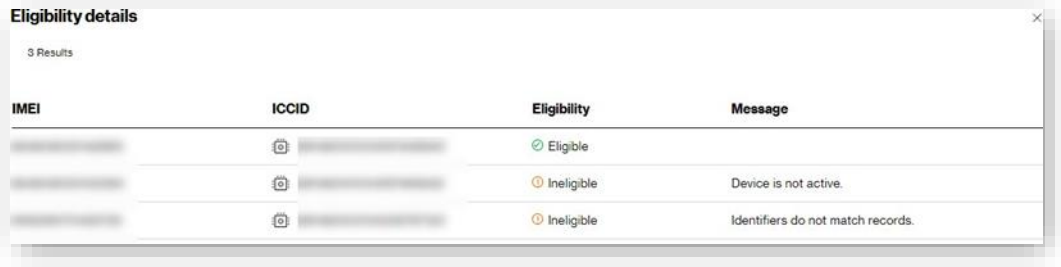



2. Select the **ID types** to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data and save.
    c. Click **Upload**.

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.




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

# Quick Cost Center Code Changes

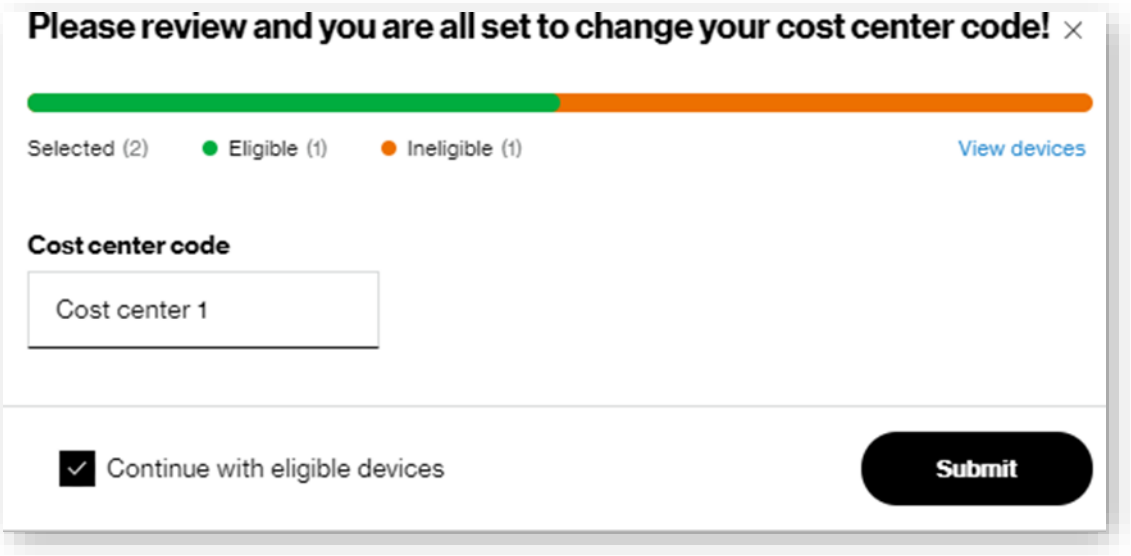
How to change cost center codes

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.




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.

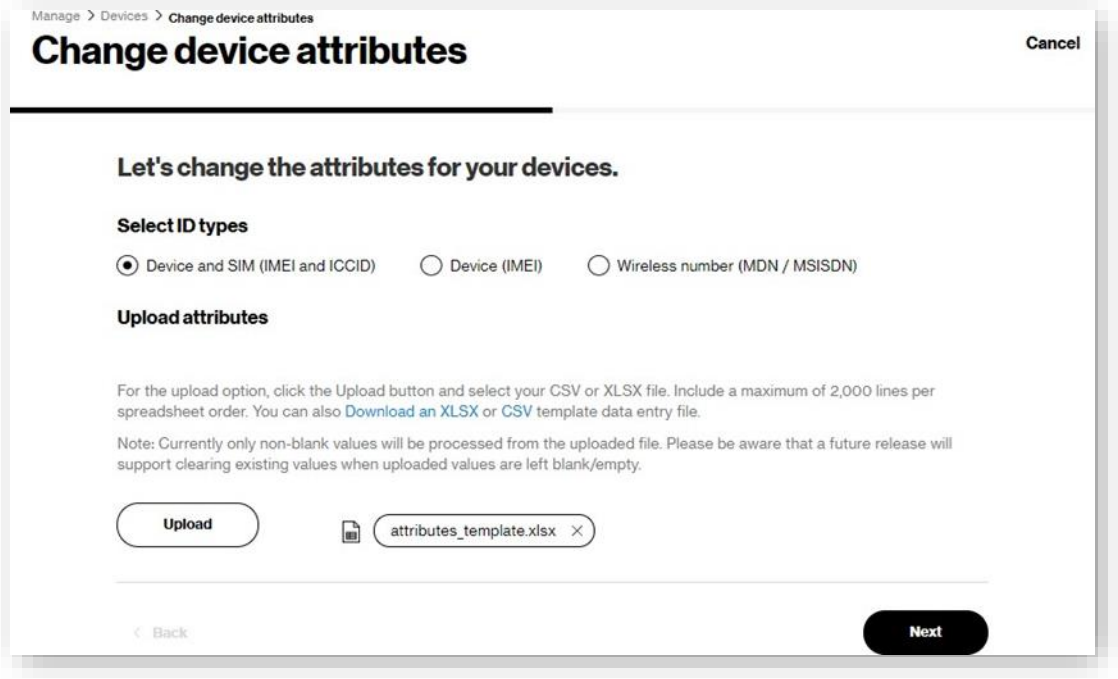
# Changing Custom Fields in Bulk

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.

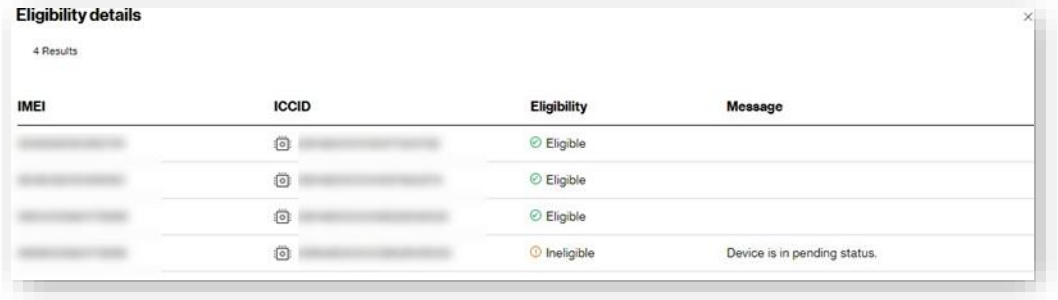
1. With no devices selected, click the actions icon , and then select **Change custom fields**. The *Change device attributes* page appears.




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.




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

# Quick Custom Field Changes

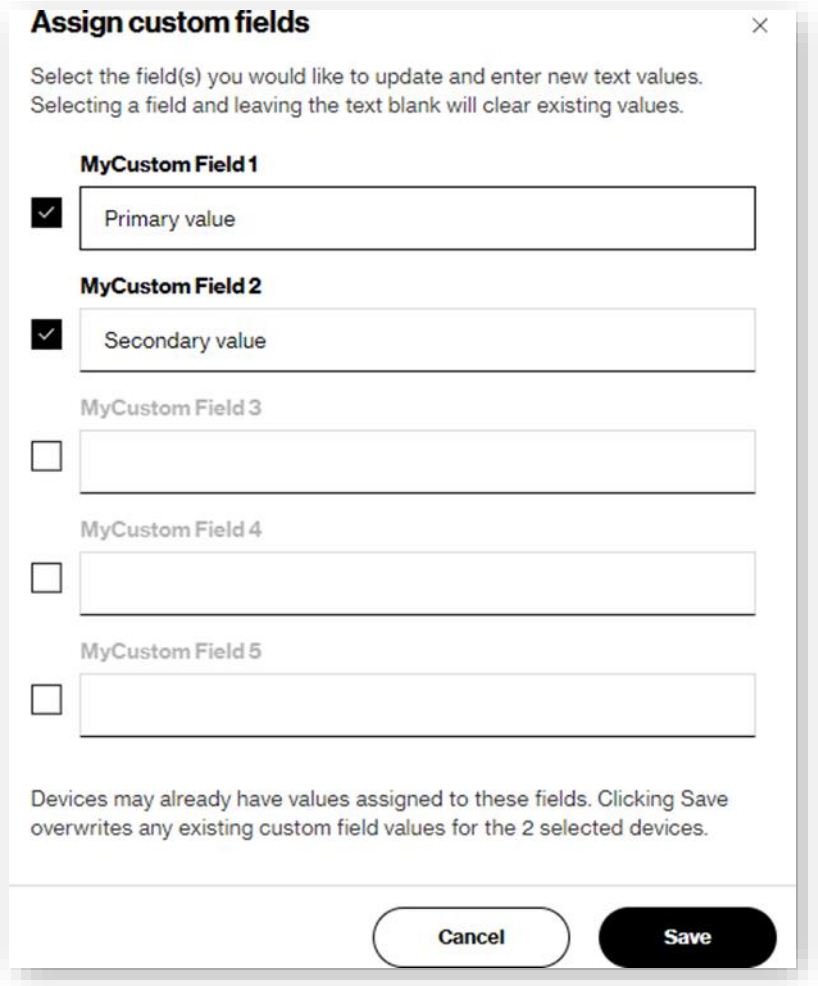
How to change custom fields

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.




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.

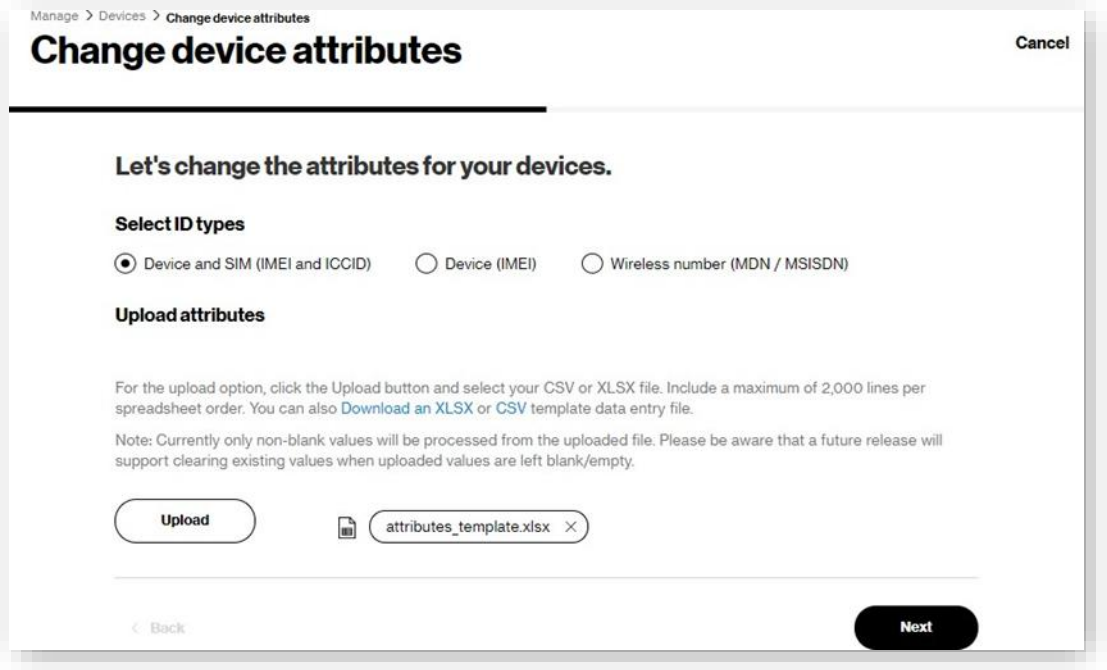
- Alphanumeric characters
- / (forward slash)
- SPACE
- @ (at sign)
- . (period)
- , (comma)
- : (colon)
- - (hyphen)
- _ (underscore)
- ( (open parenthesis)
- ) (close parenthesis)
- [ (open bracket)
- ] (close bracket)
- # (number sign or hash tag)

# Changing Device Groups in Bulk

How to device groups in bulk

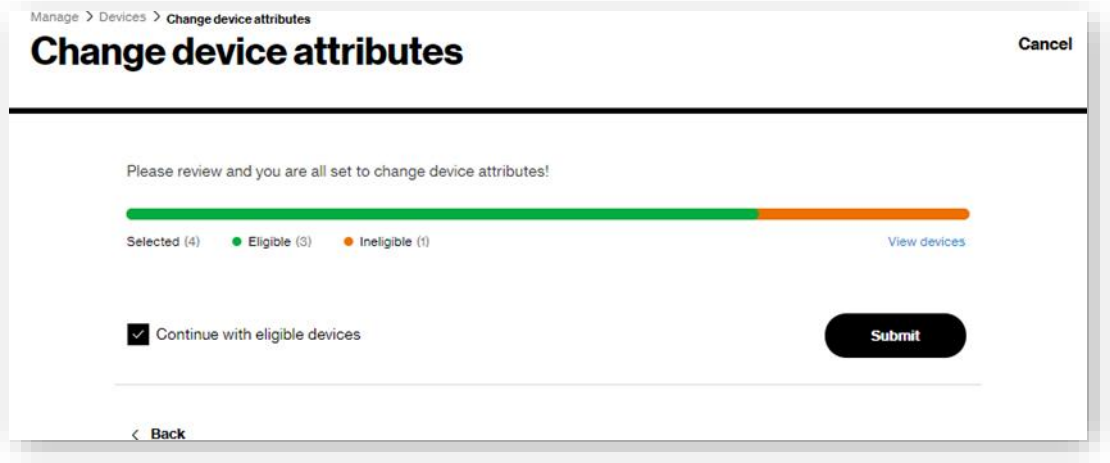
On the left navigation, click **Devices**. The *Devices* page opens.

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

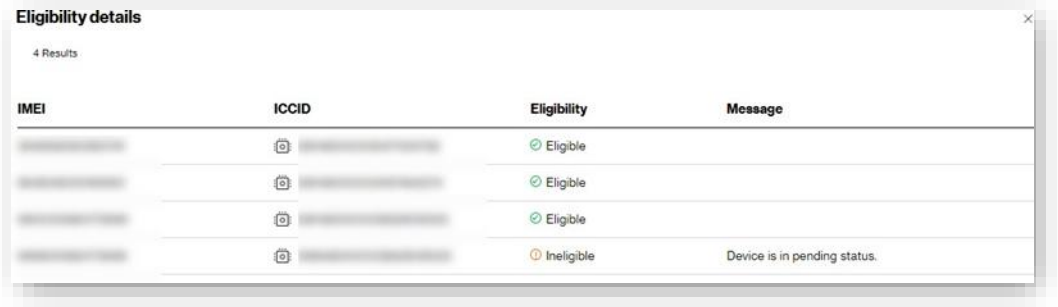



2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
    a. To upload a file, click **Download an XLSX or CSV** to download the template.
    b. Add your data and save.
    c. Click **Upload** to complete the upload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




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

# Quick Device Group Changes

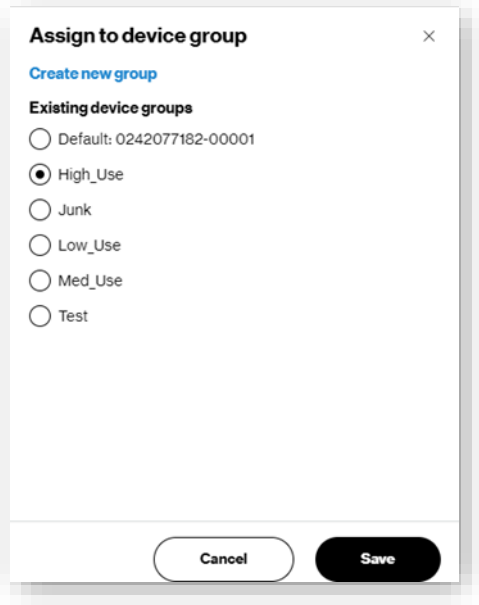
## How to change the device groups

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.



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.

   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

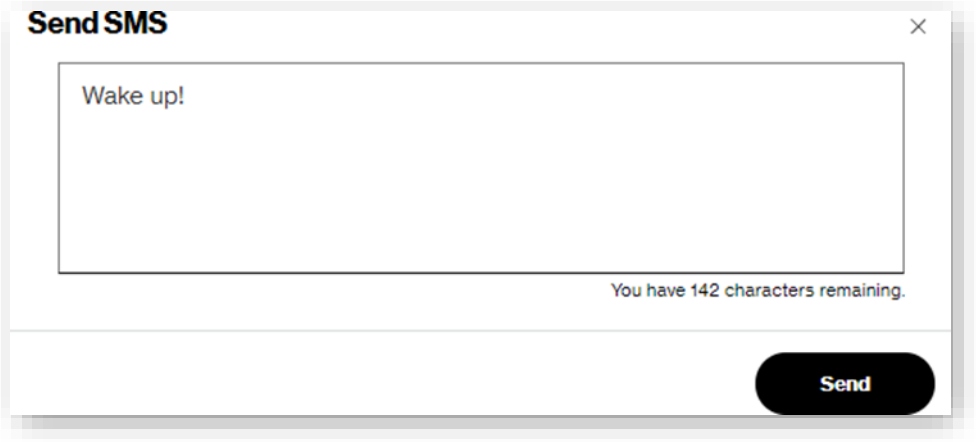
On the left navigation, click **Devices**. The *Devices* page opens.

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.




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

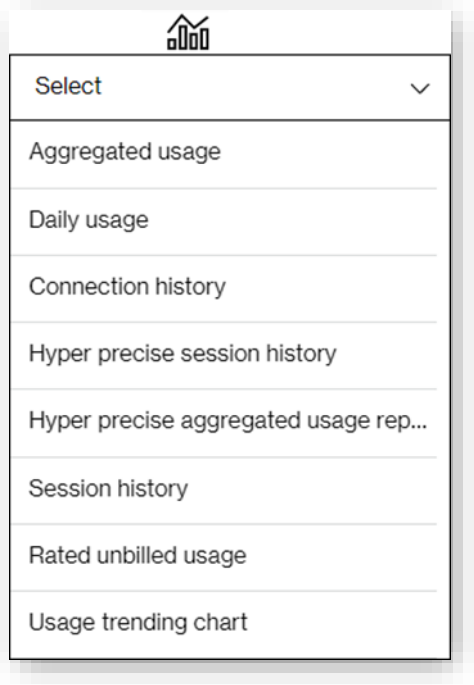
# Reporting Actions

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.

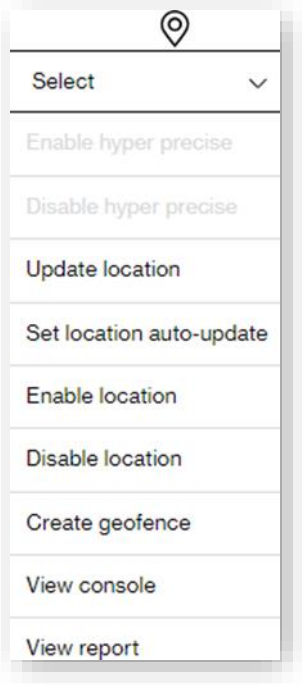
# Location Actions

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

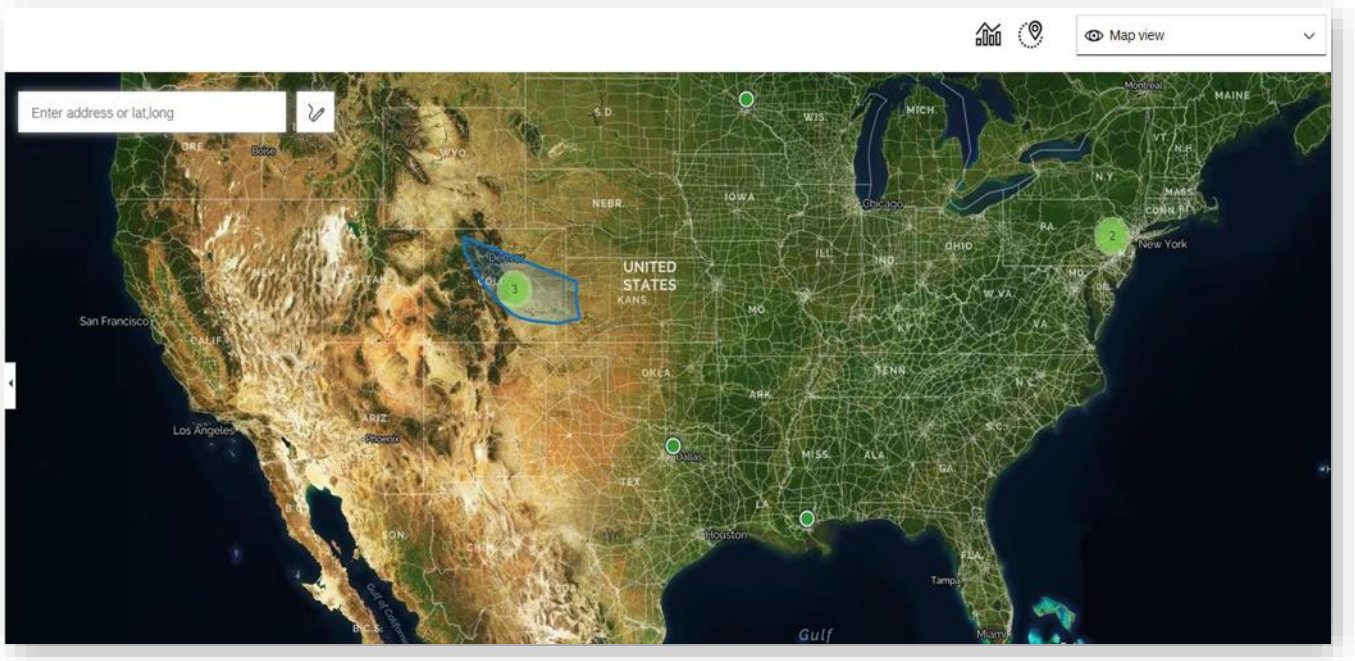
Create a geofence to view real-world geographic areas around your devices. Alarms can be set to notify you when your device moves outside of the set geofence boundaries.

To create a geofence

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

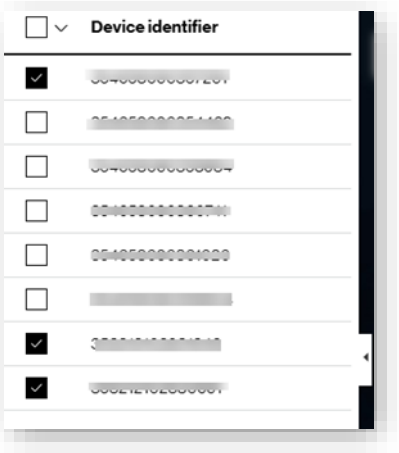
1. Select **Map view**.
2. Click the drawing tool .
3. Click and drag on the map to form the geofence shape. This automatically selects any devices within the on the map.

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

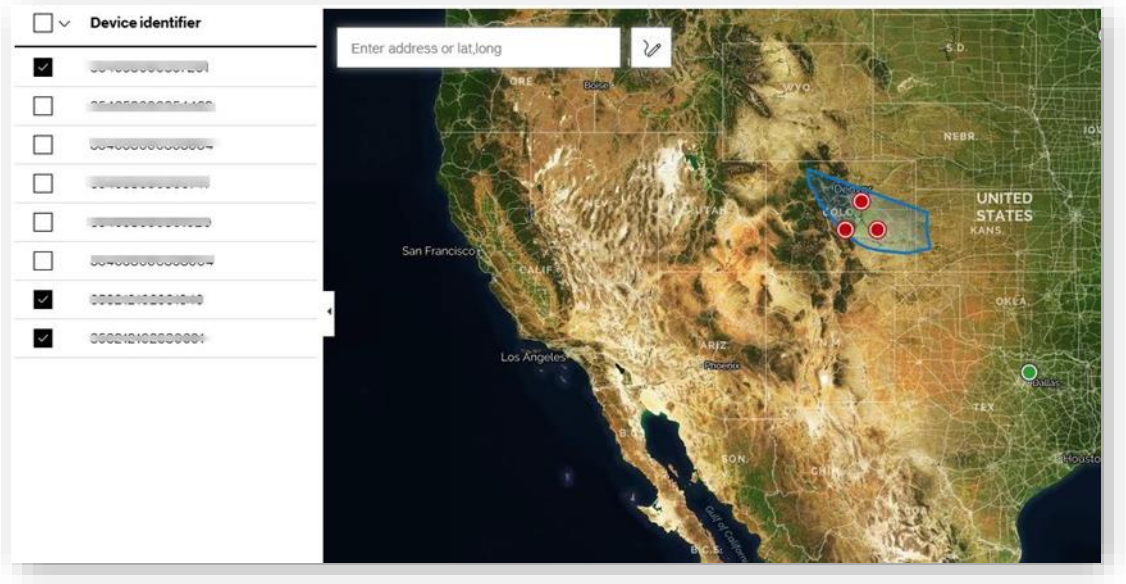



4. Click devices on the map, or open the list to select / unselect.

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.



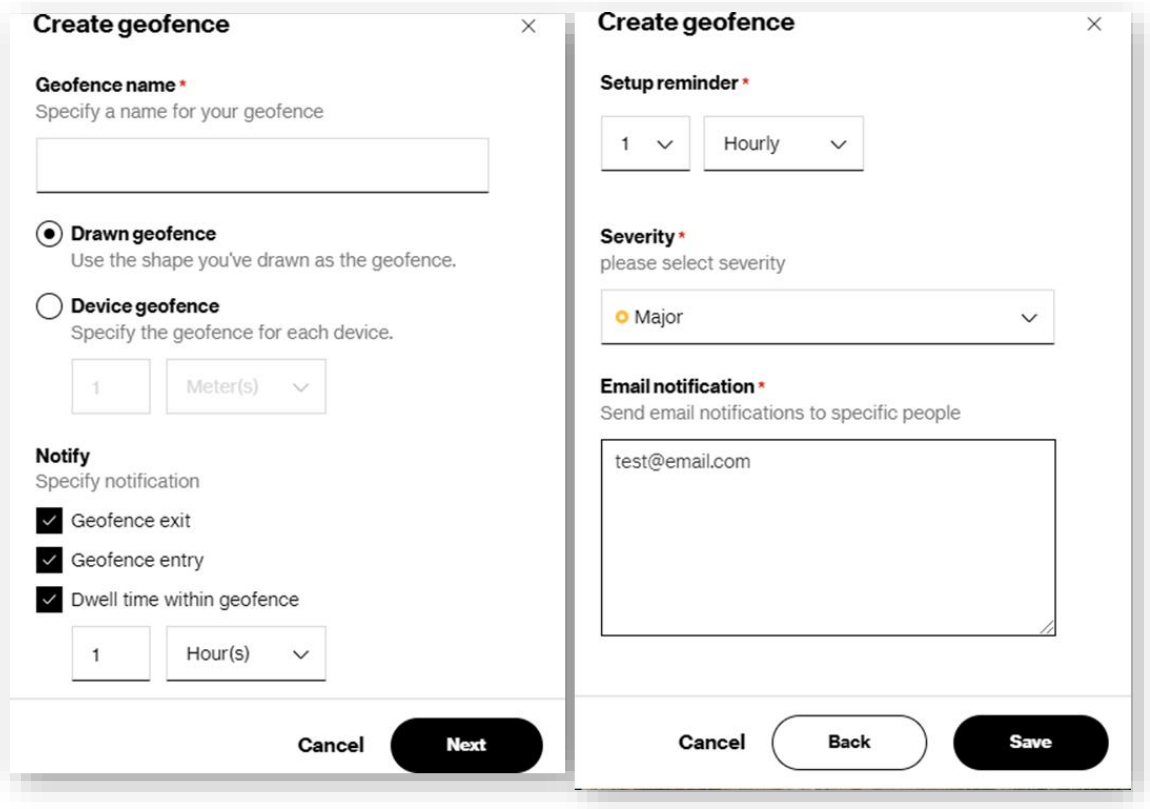

**NOTE:** The system evaluates the geofence rule each time the platform receives a location update for the device. Make sure to set the auto location update rate on all devices.

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.

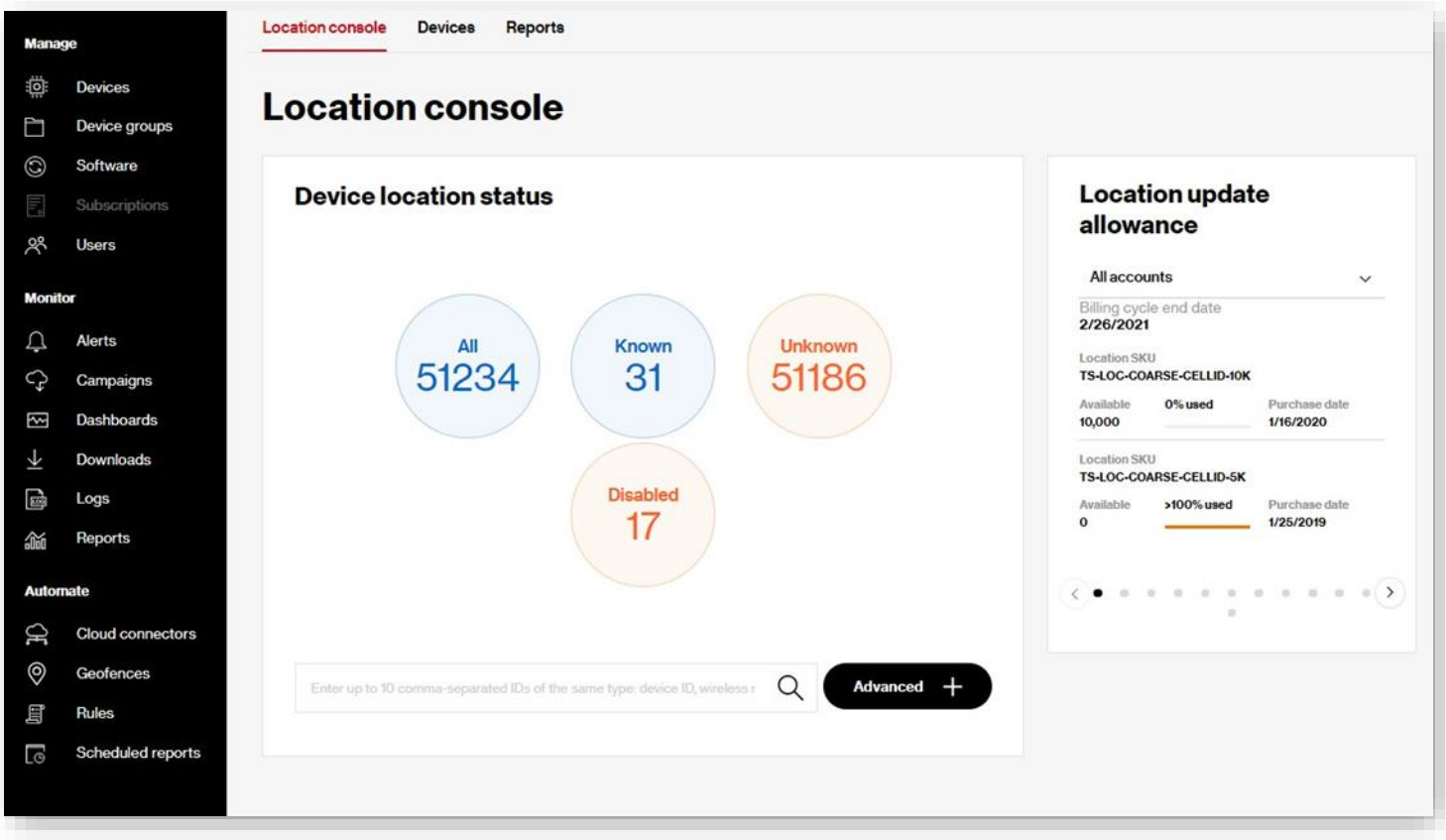
9. Select notification trigger.
    - **Geofence exit** – sends a notification when the device exits the geofence.
    - **Geofence entry** – sends a notification when the device enters the geofence.
    - **Dwell time within geofence** – sends a notification when the device stays within the geofence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




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.

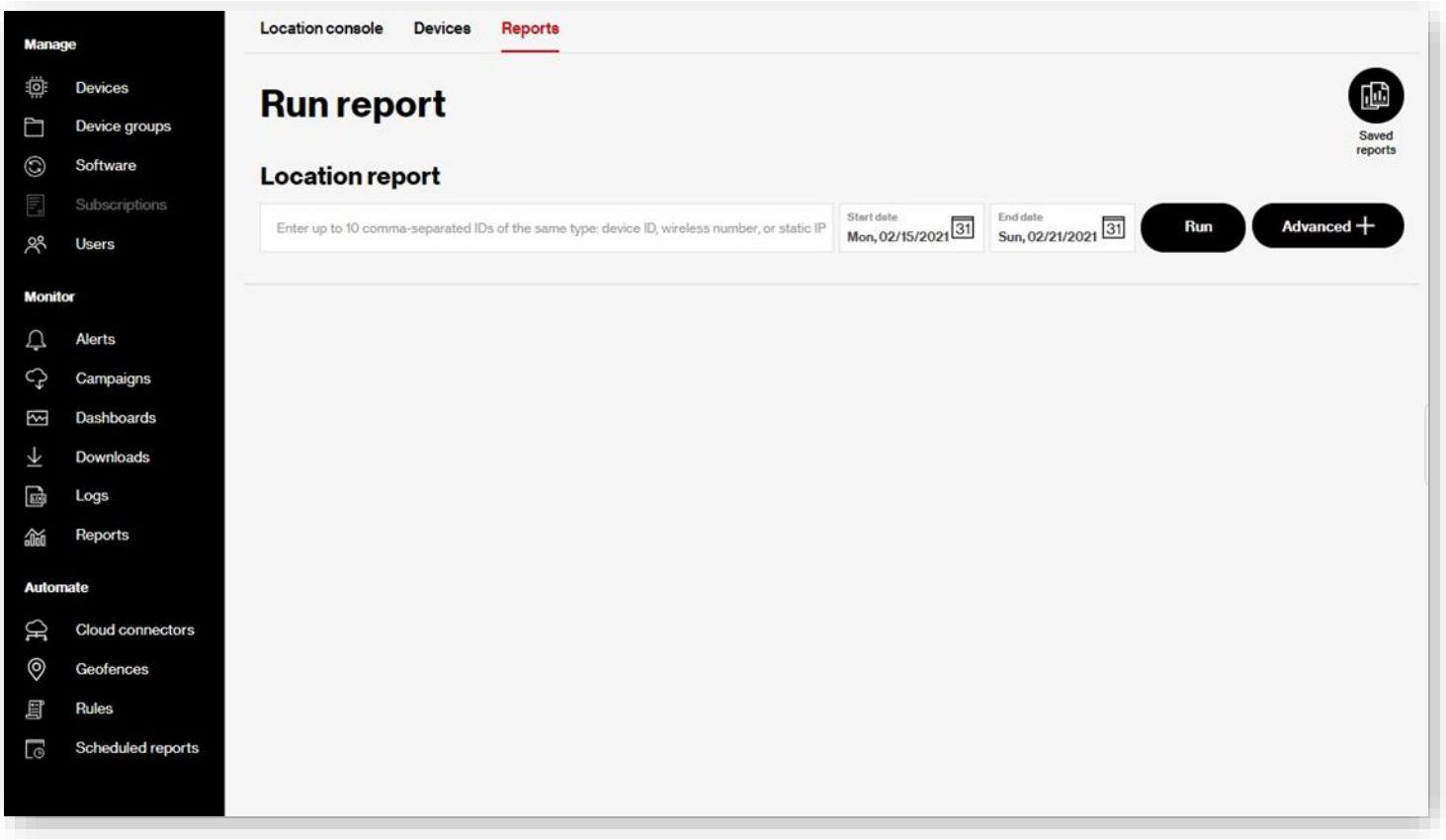
# View Location Console

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



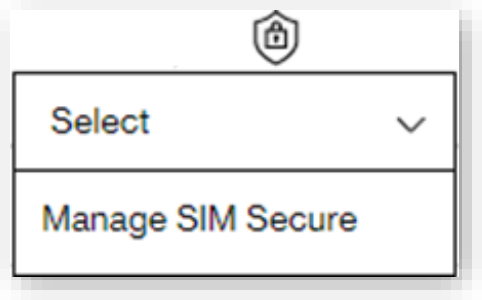
# View Location Report

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.

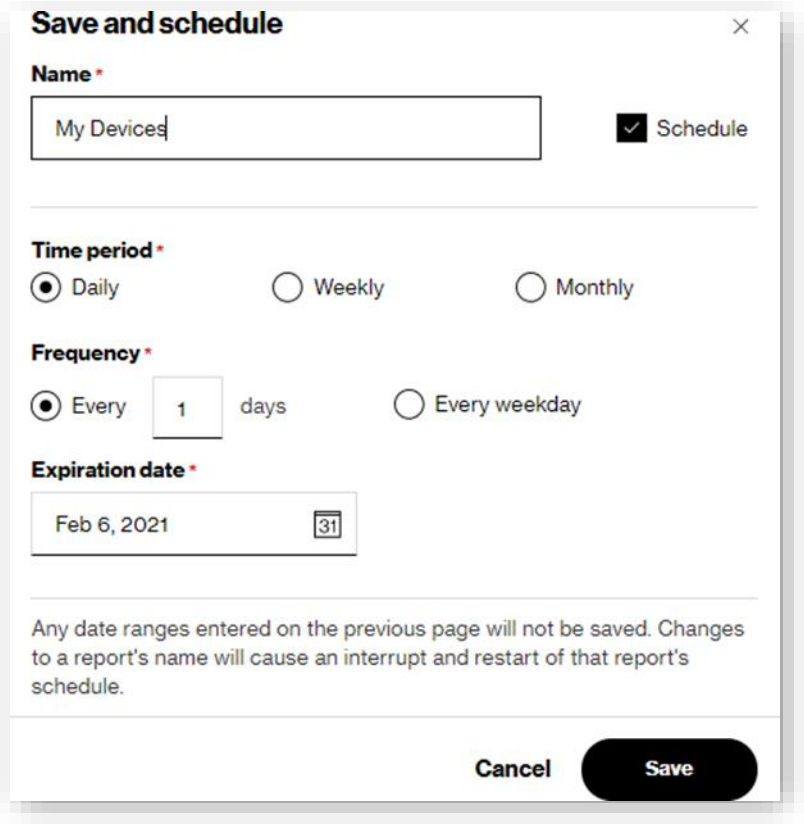



**COMING SOON:** The ability to assign SIM Secure licenses directly from the Devices page.

# Schedule Action

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

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



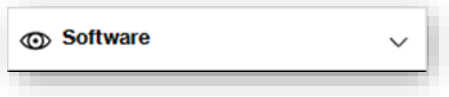

1. For **Name**, type a descriptive label for the devices report.
2. Check **Schedule** to run this report at a predetermined date and time.
   a. Select the **Time period** for your scheduled report.
   b. Set the **Frequency** for the report to run.
   c. Select an *Expiration date* for the report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

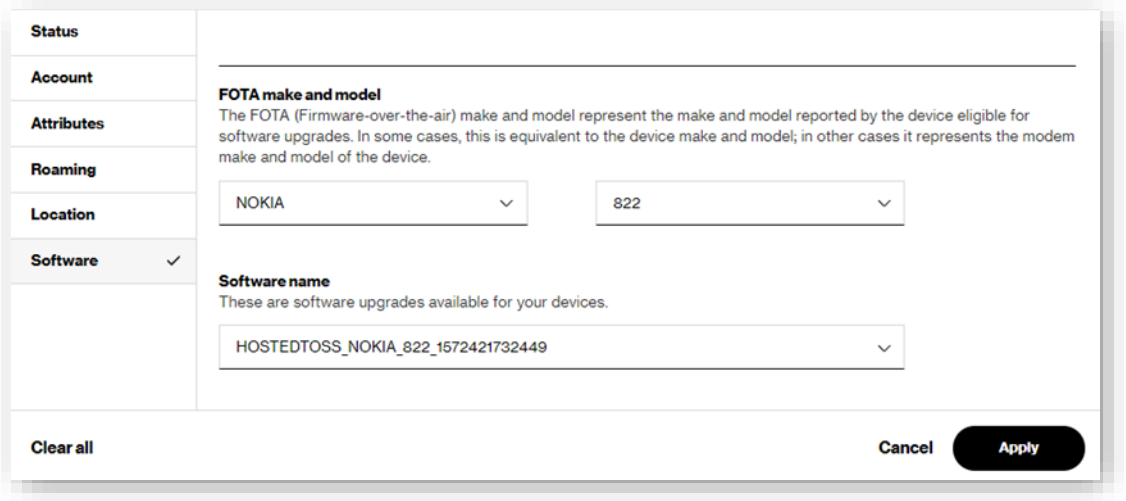
How to create a campaign

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




2. Click the filter icon .

3. On the left navigation, click **Software**.




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**.

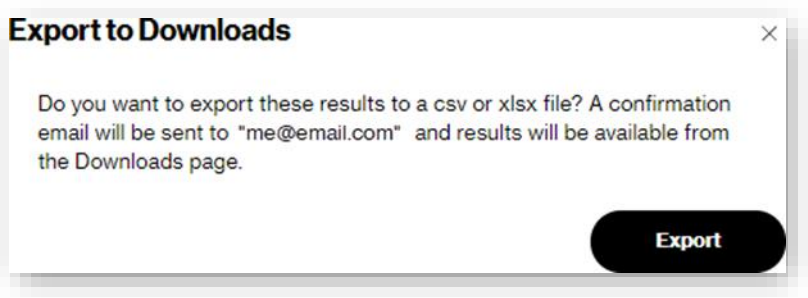
**NOTE:** The Create campaign option is disabled when the selected devices are not eligible for a software update.

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



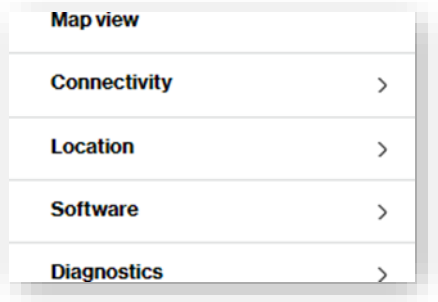

2. Click **Export**.

**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.



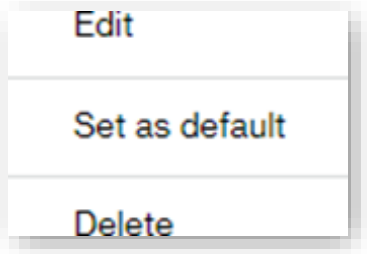

Available predefined views are:

- **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.

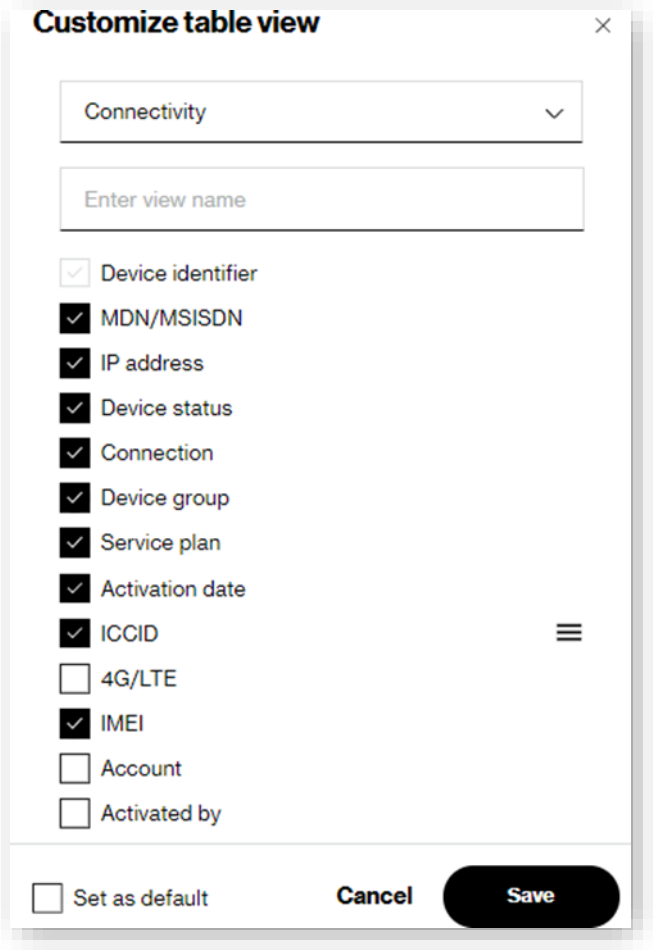


# Custom Views

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.




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.

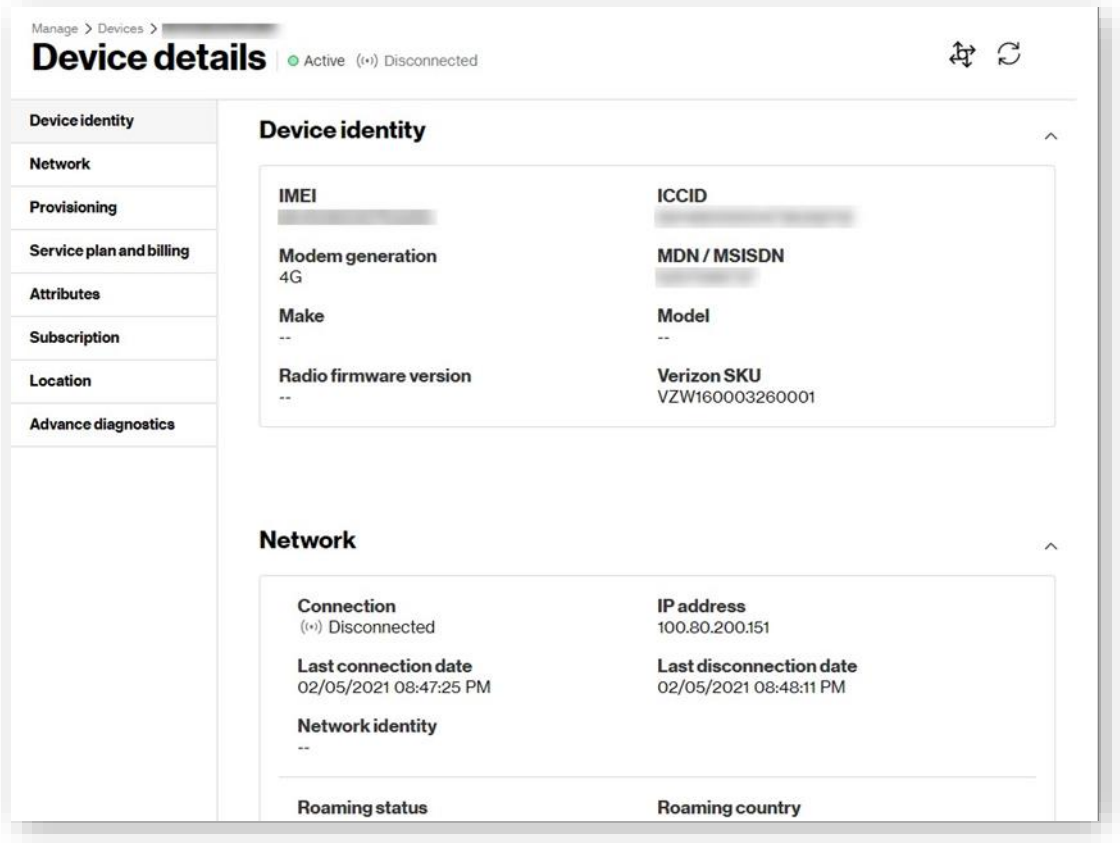
# Device Details

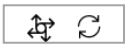
You can drill down into device details from the *Devices* page by clicking a **Device ID**. This opens device attributes, behavior, usage, and other associated information.

To view device details

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

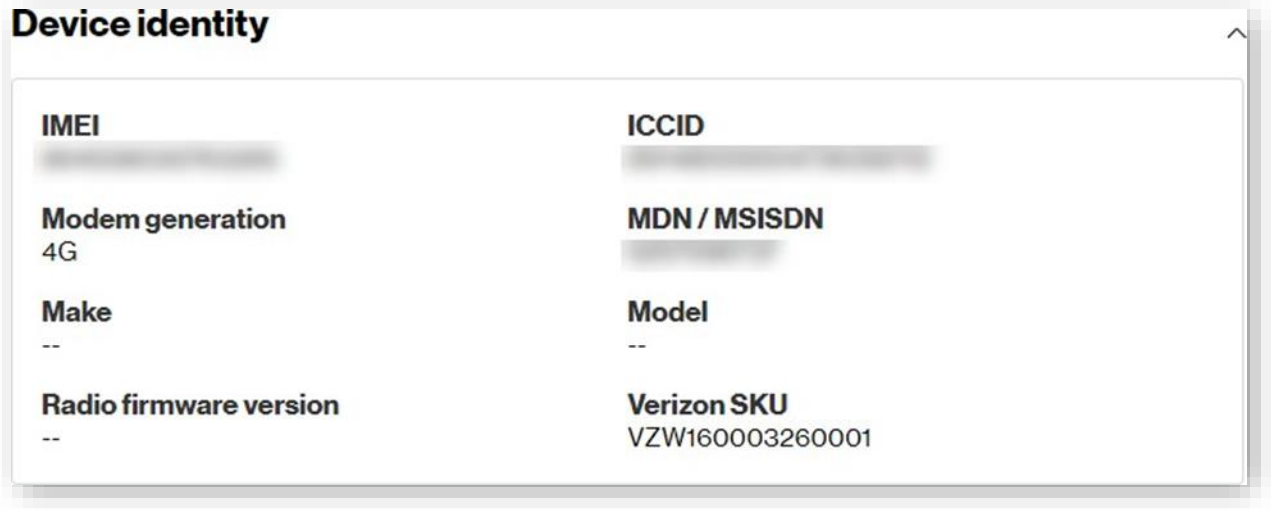
1. Click the **Device identifier**. A *Device details* page opens with details about the selected device.




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.

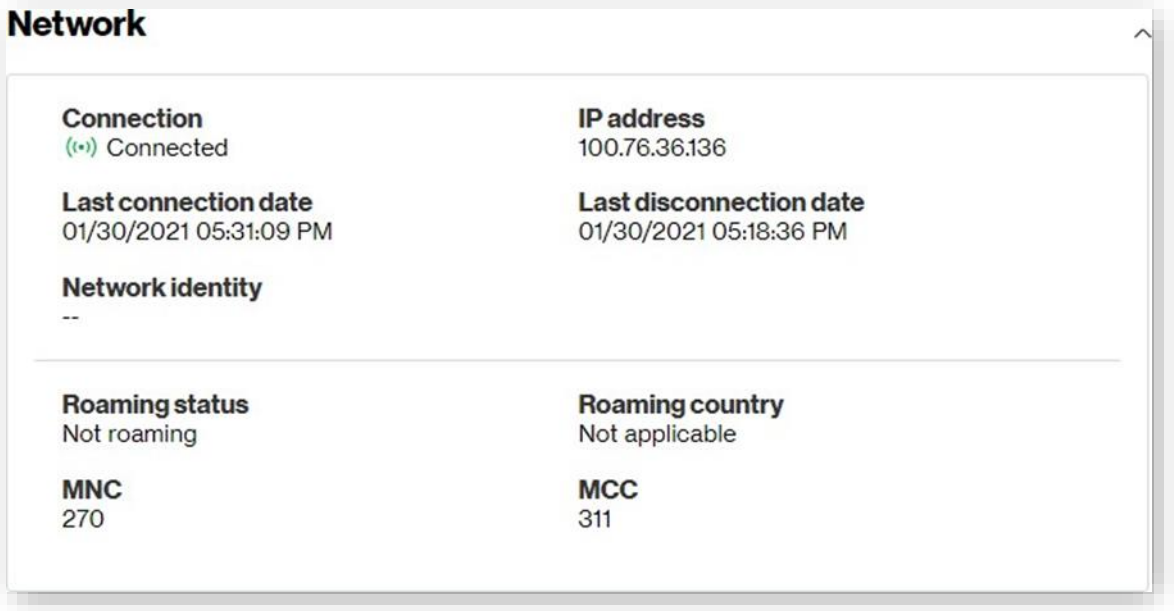
# Device identity

The *Device identity* section provides the following details:



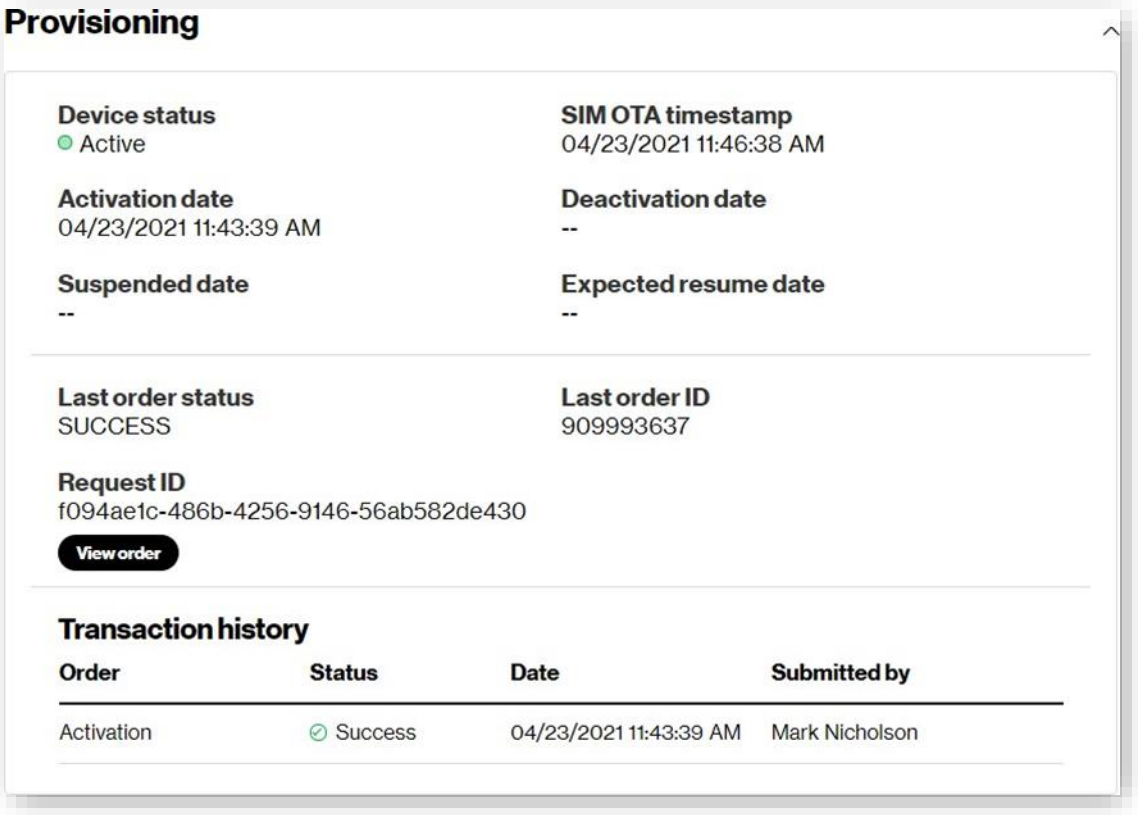

## Network

The *Network* section provides the following details:



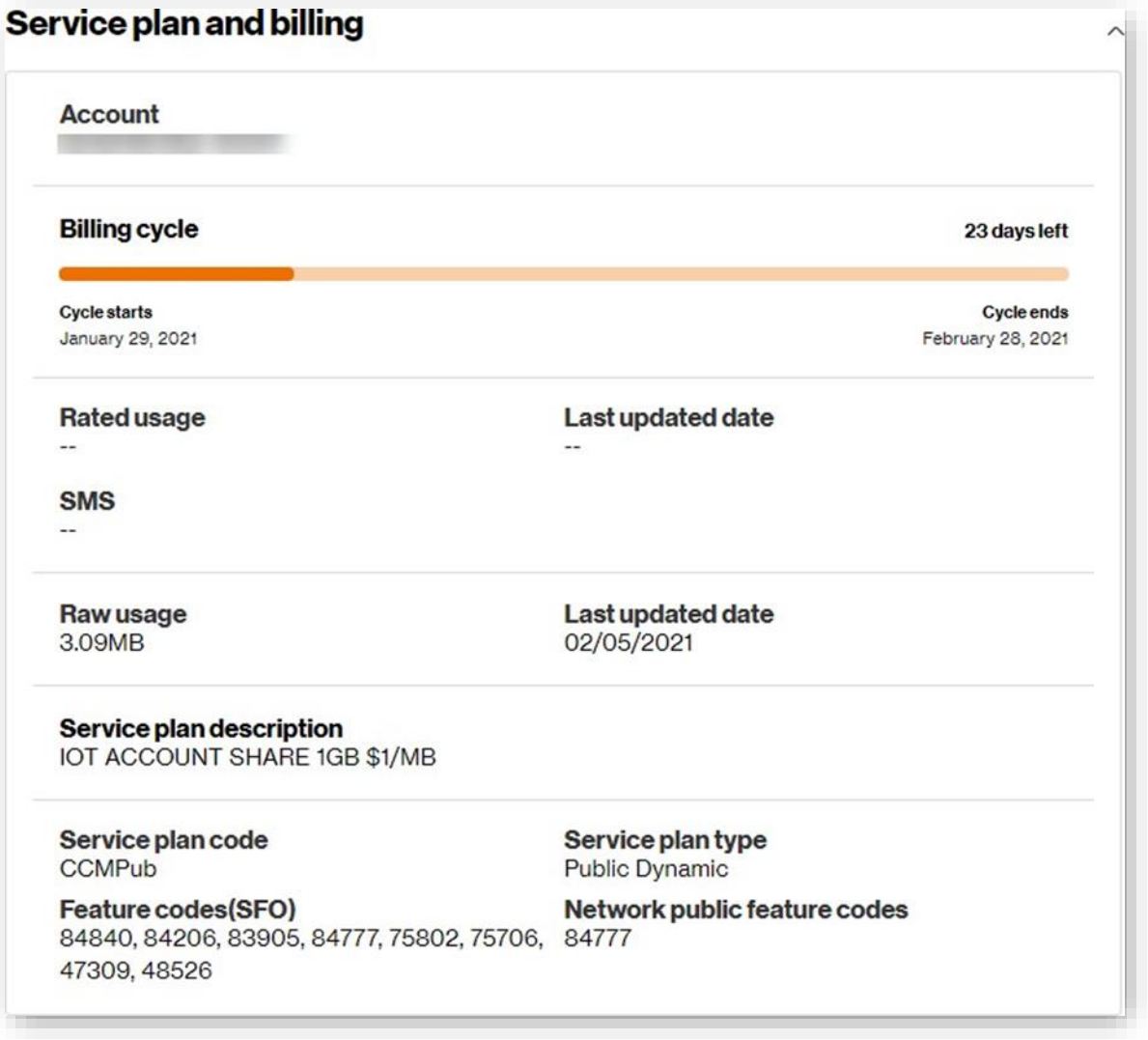
# Provisioning

The *Provisioning* section provides the following details:



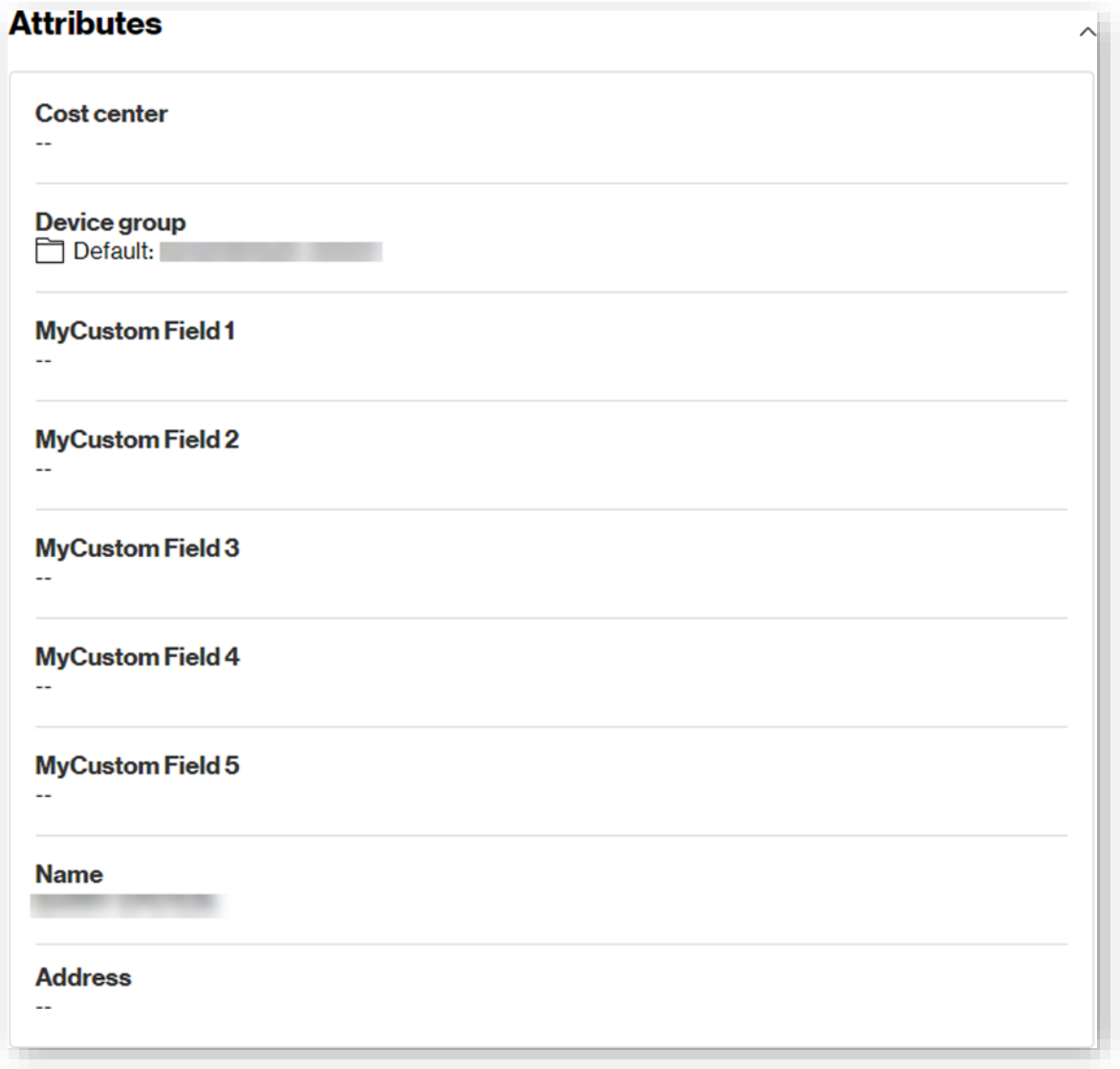
## Service plan and billing

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



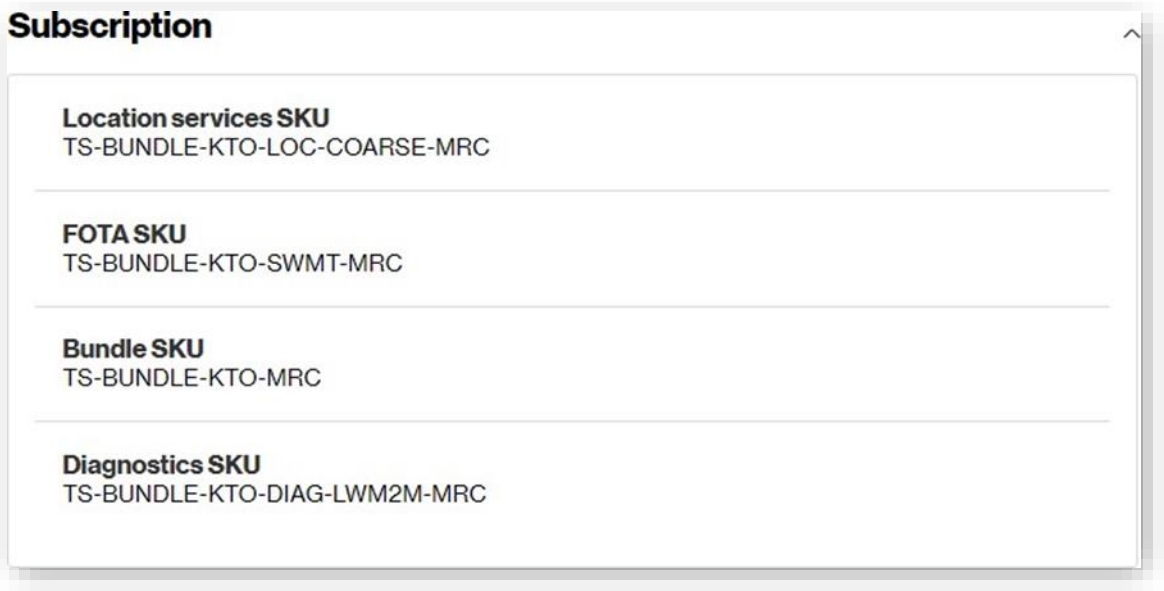
## Attributes

The *Attributes* section provides the following details:



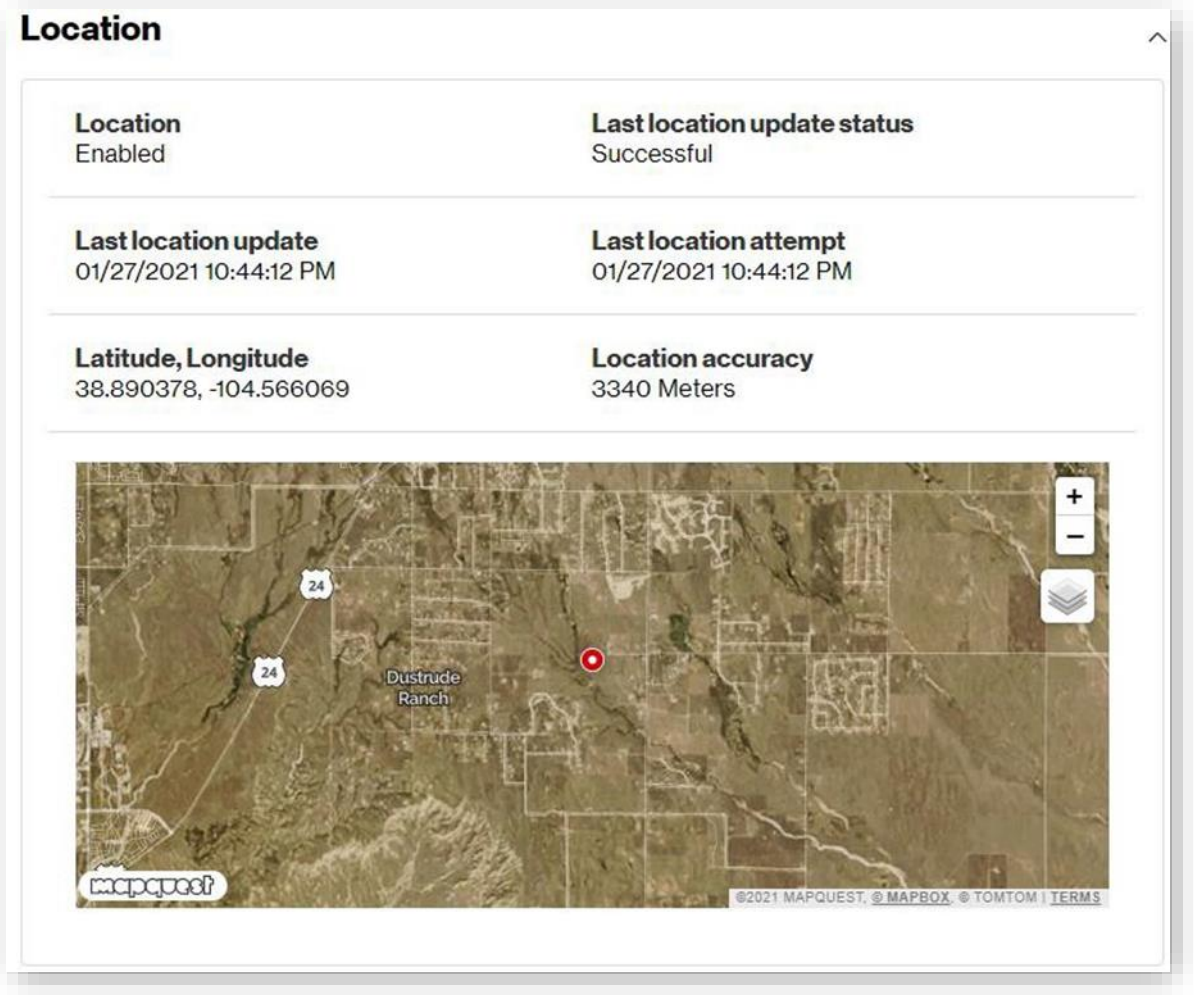
## Subscriptions

The *Subscription* section provides the following details:



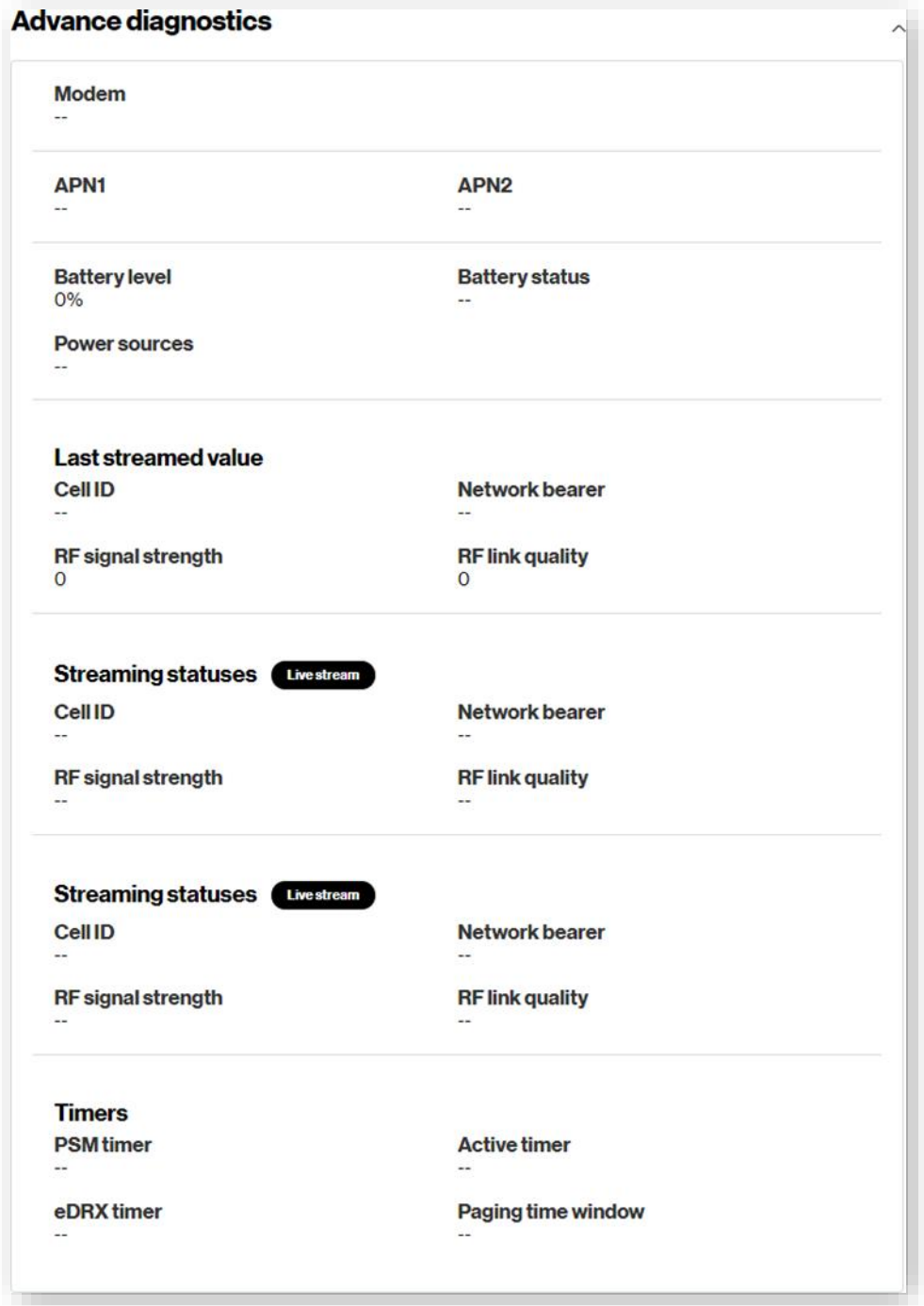
# Location

The *Location* section provides the following details:



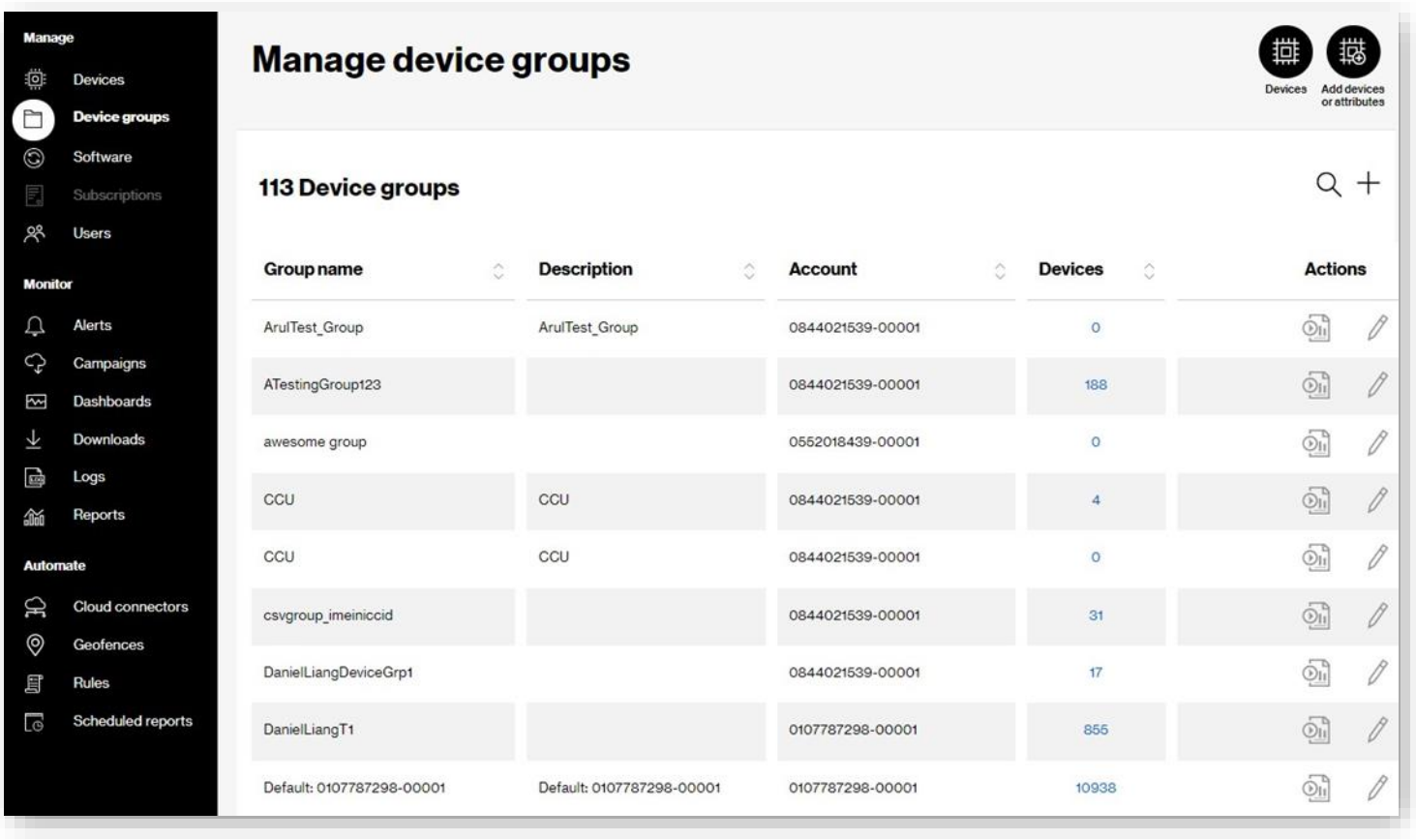
# Advanced diagnostics

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.



# 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.



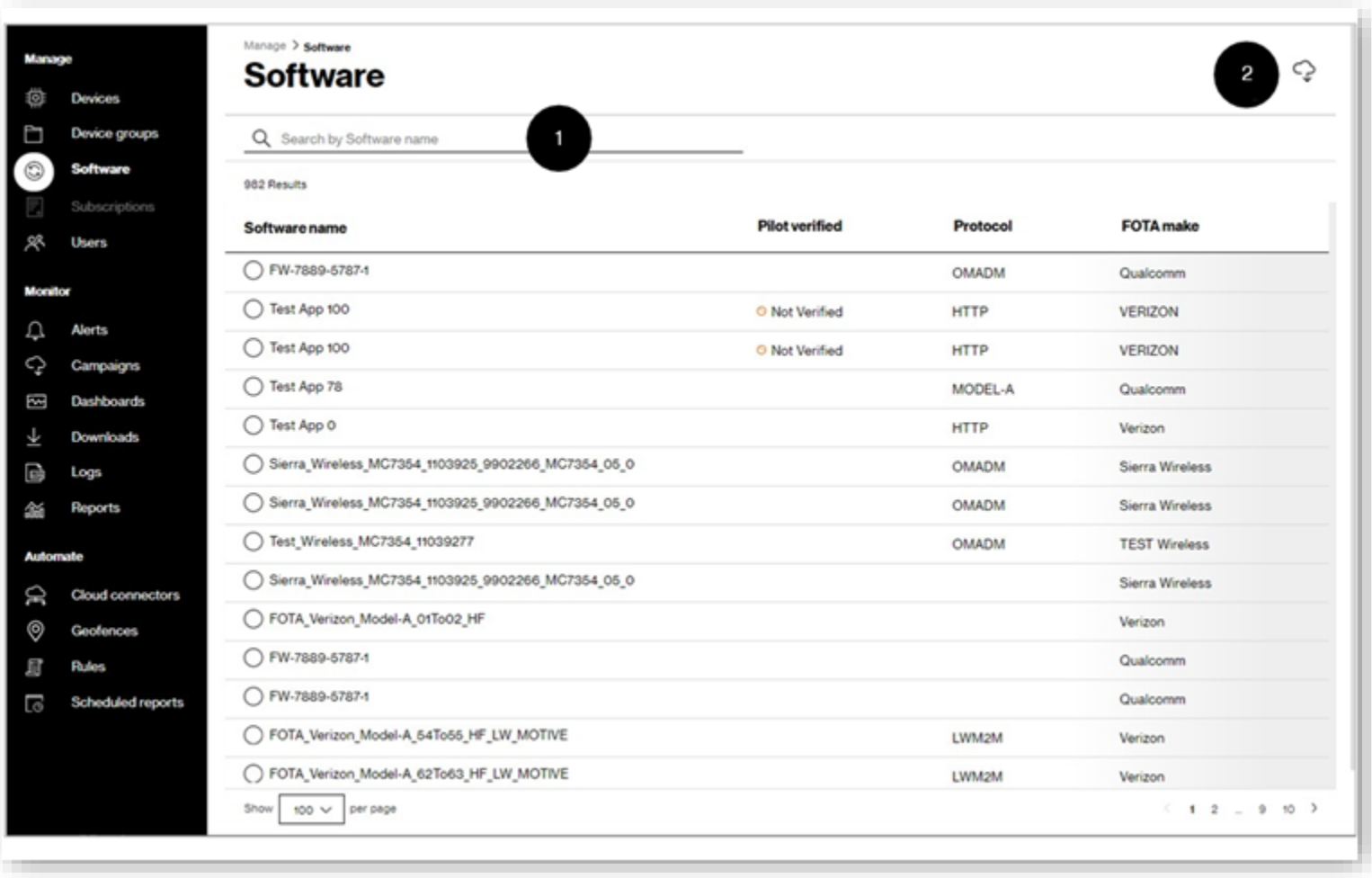
# Software Management

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.

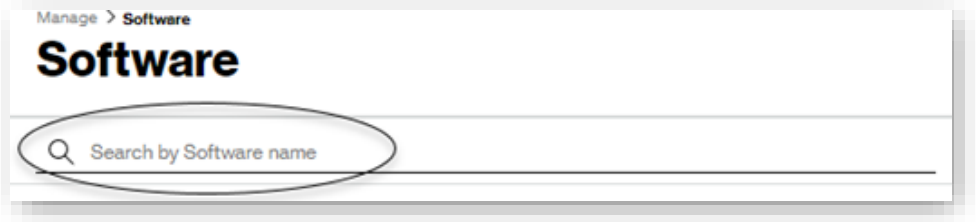


| Elements on the Software page | | |
|---|---|---|
| 1 | | Search – Locate a specific software by name. |
| 2 | | Campaign – Create a strategy to update software. |

# 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.

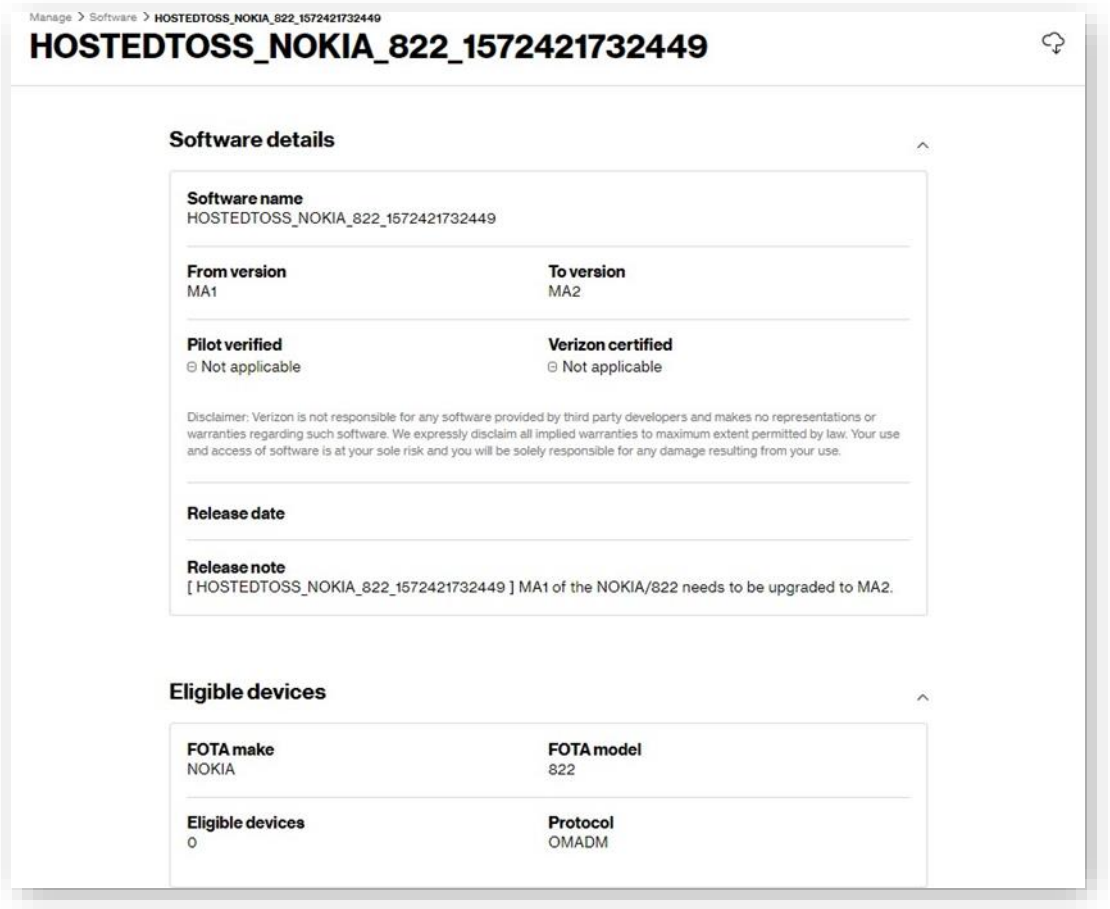
# Software Details

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.

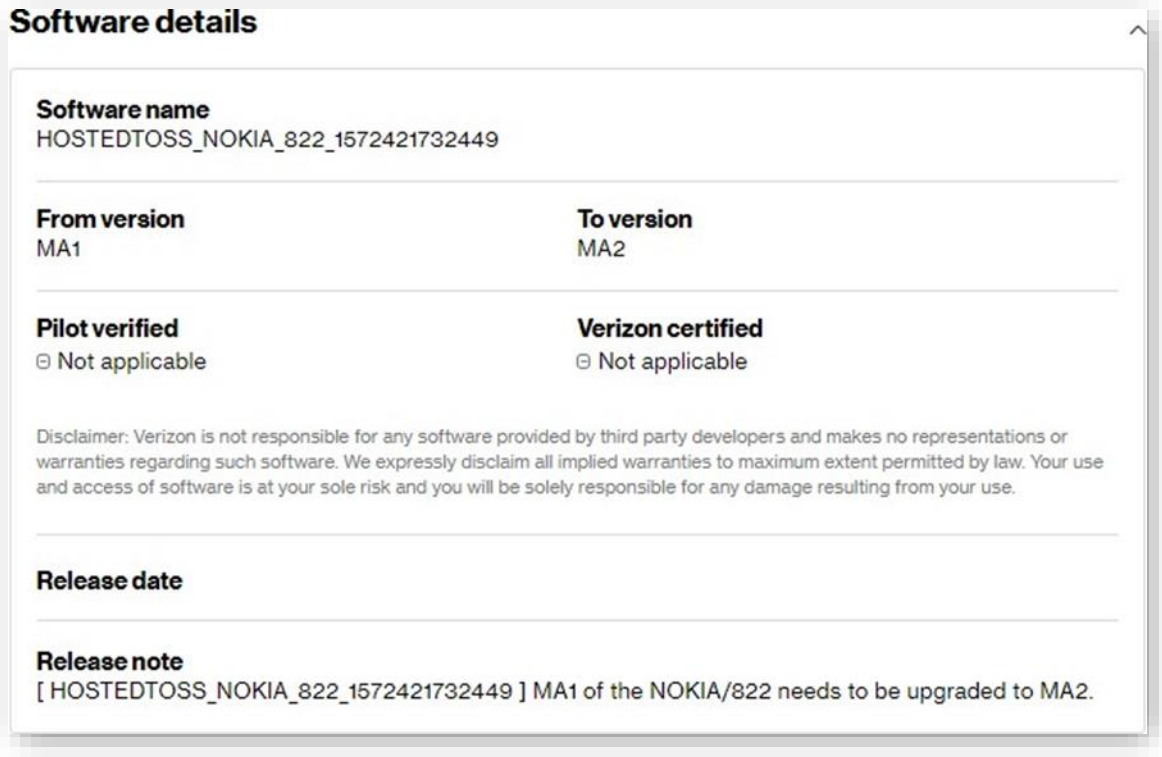



2. Click the campaign icon to create a campaign, or go to the legacy view.

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

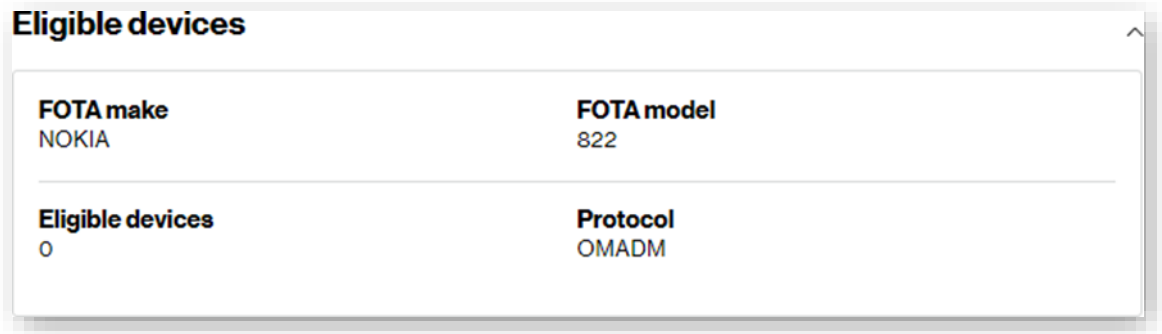
# Software Details

The *Software details* section provides the following information:



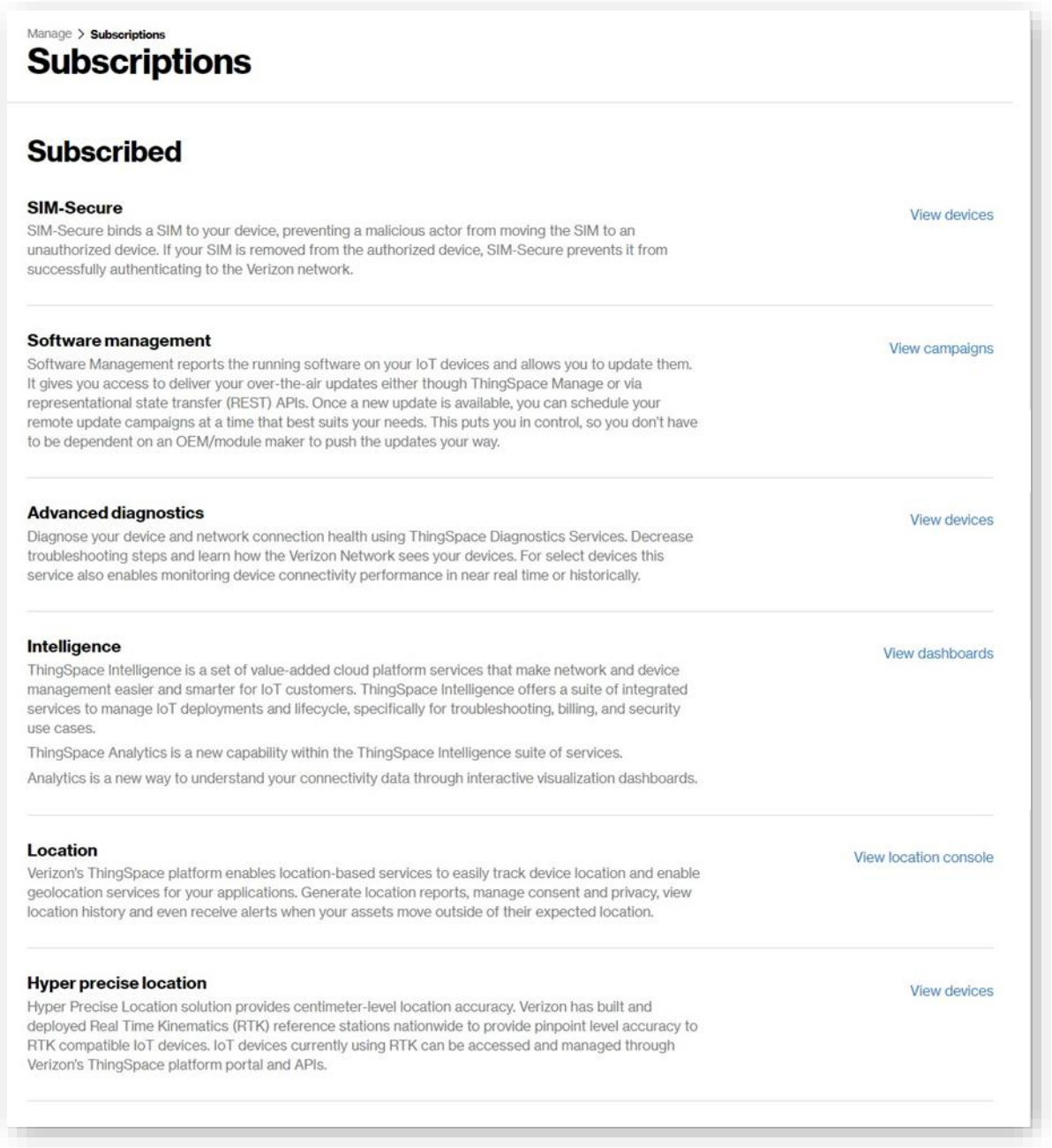

## Eligible Devices

The *Eligible devices* section provides the following details:



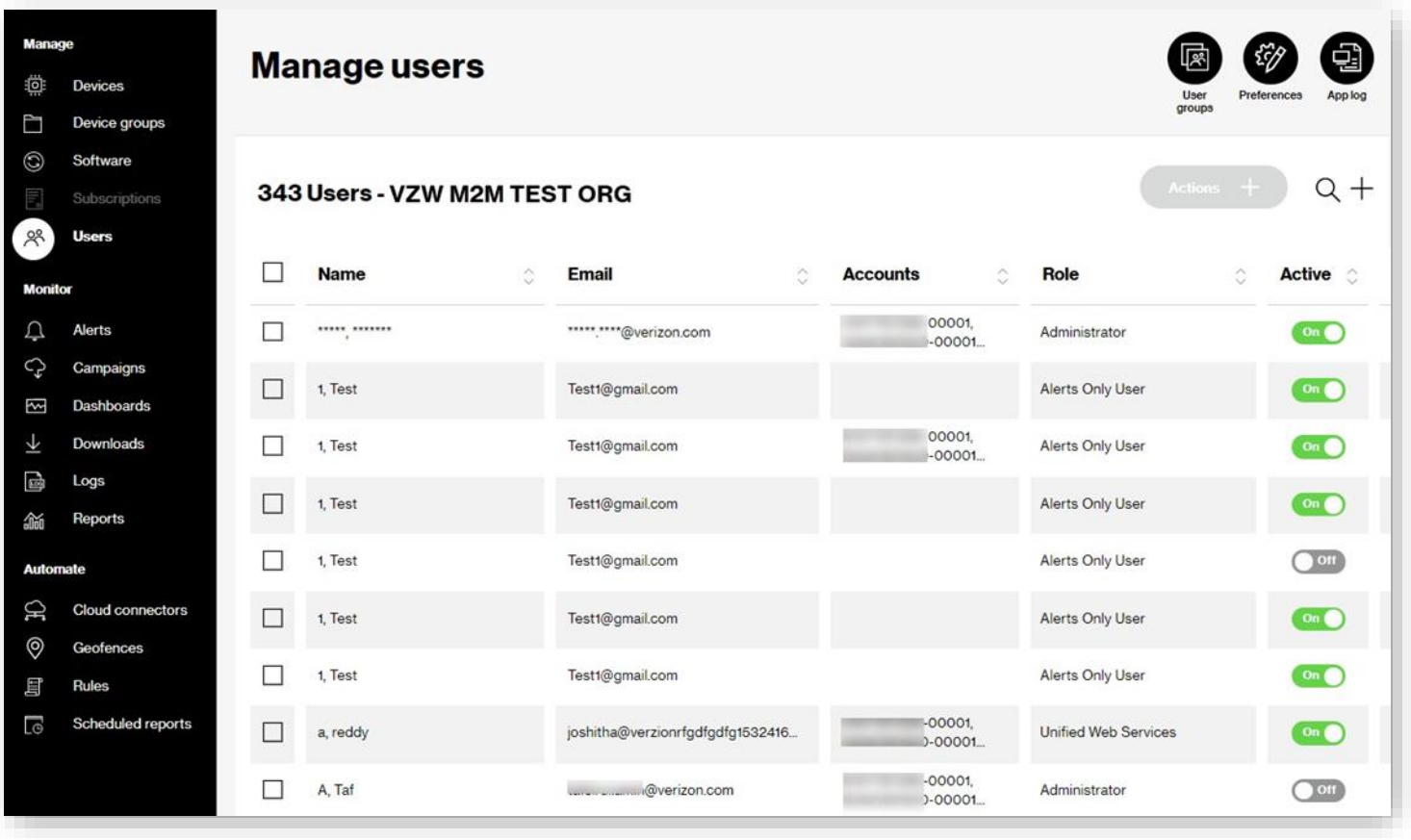
# Subscriptions

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.



# 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.




**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.

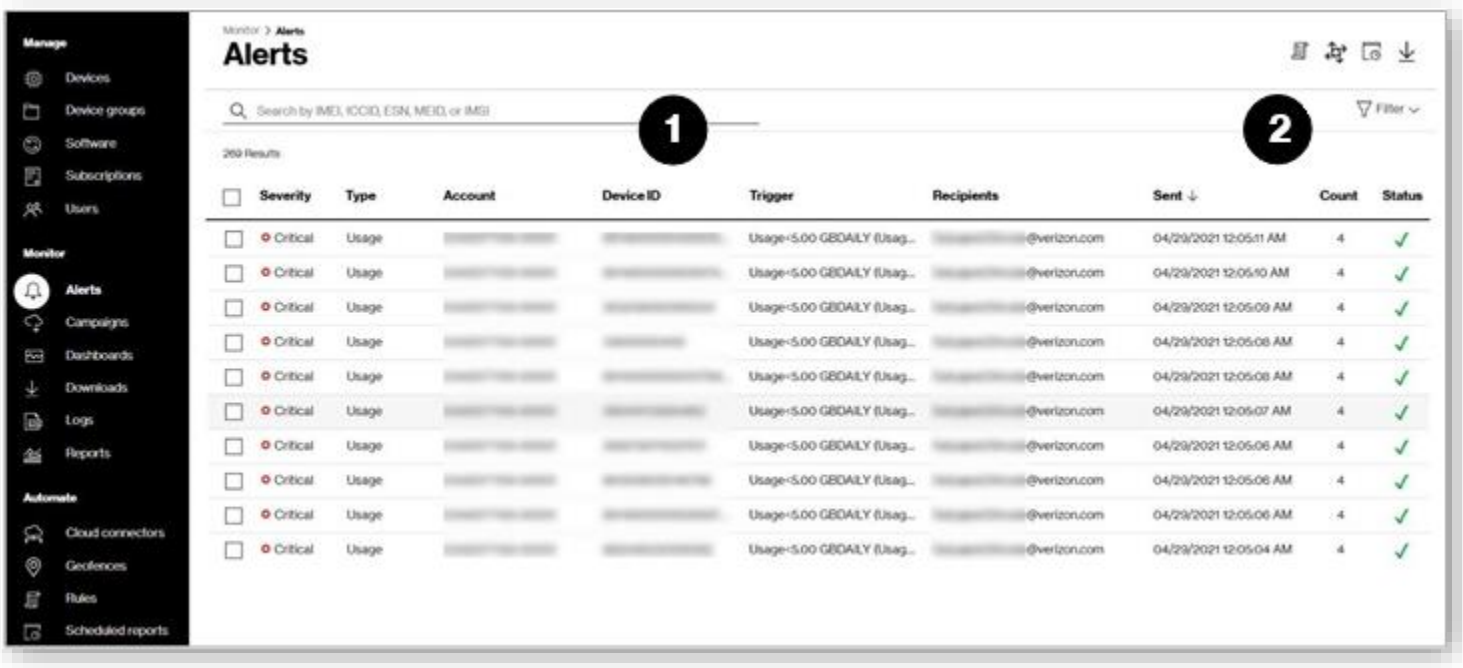
# Alerts

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 | 🔍 | Search – Locate an alert by device identifier. |
| 2 | ▽ | Filter – Limit the list to only alerts having specific attributes. |

# Searching Alerts

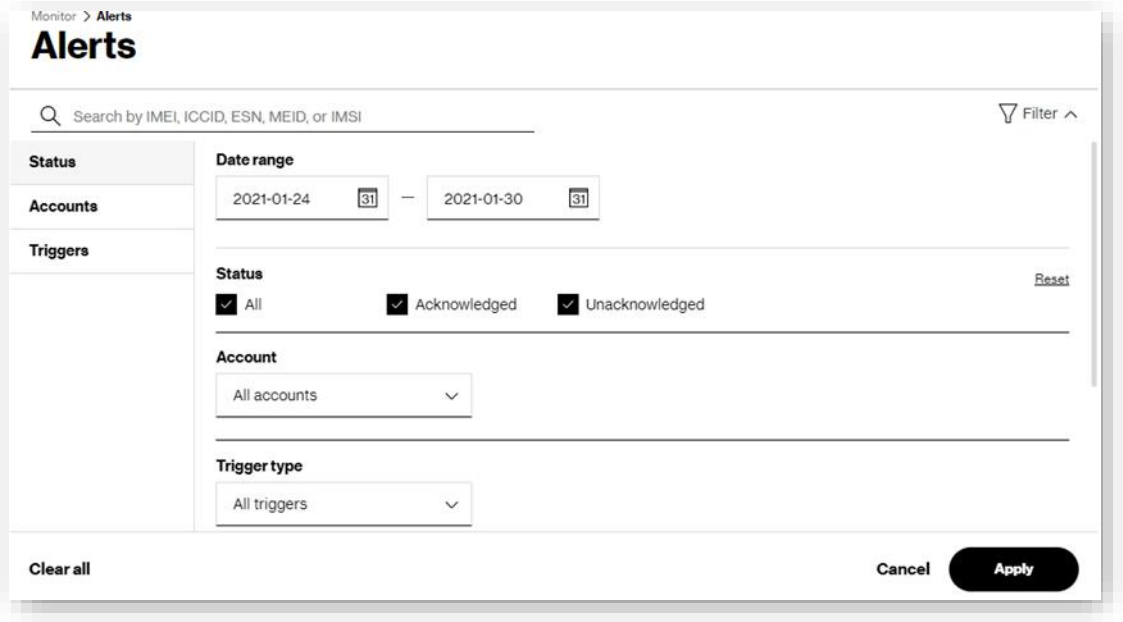
Use the **Search** field to search for devices by IMEI, ICCID, ESN, MEID, or IMSI. Wildcard (%) search is supported for Device IDs.

## 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

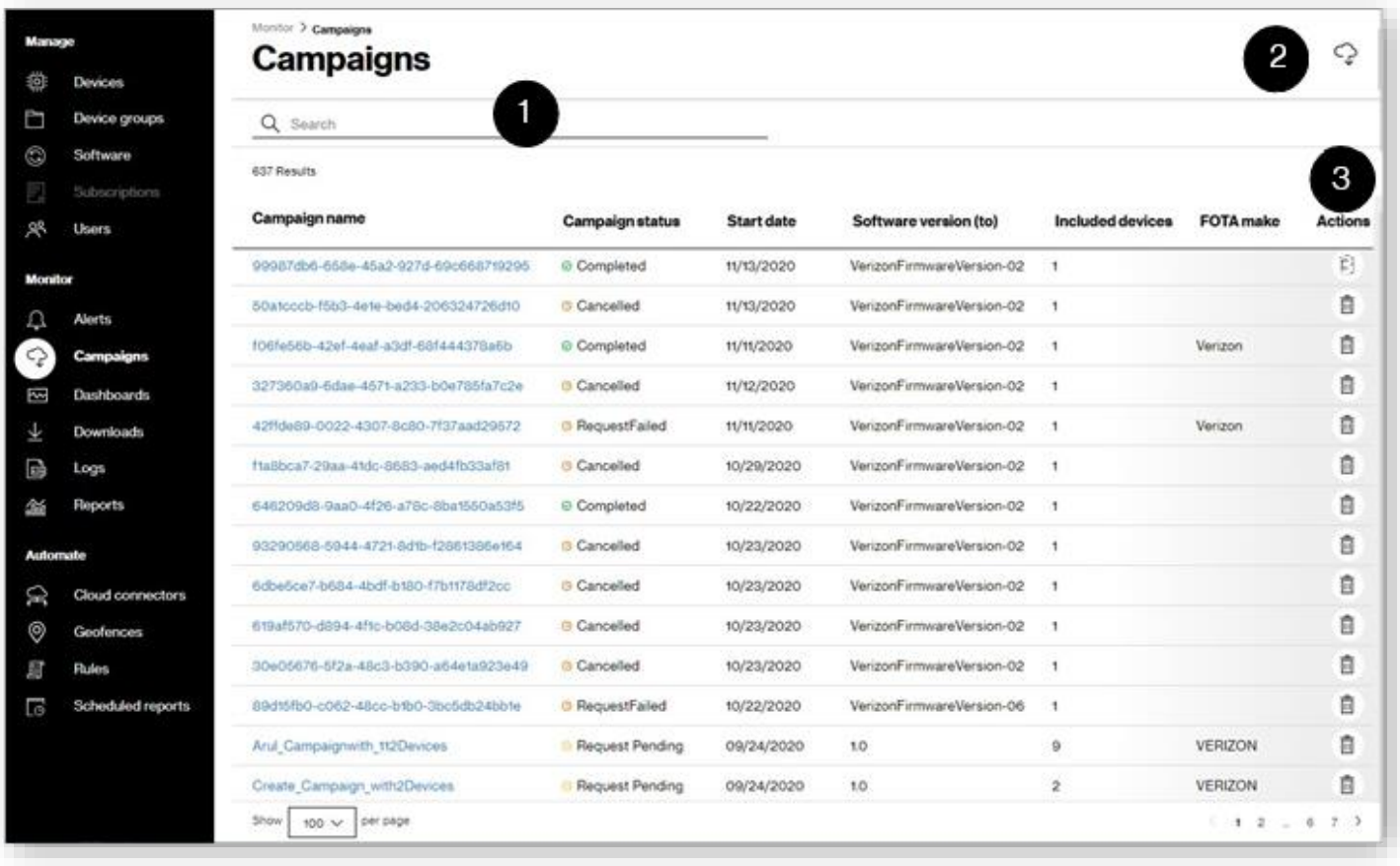
1. Select each alert checkbox.
2. Click the actions icon and then select **Acknowledge** to complete the process.

# 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.




| Elements on the Campaigns page | | |
|---|---|---|
| 1 | 🔍 | Search – Locate a campaign by name. |
| 2 | ☁ | Campaign – Open the Campaign menu. |
| 3 | 🗑 | Delete – Permanently remove a campaign. |

# Search for Campaigns

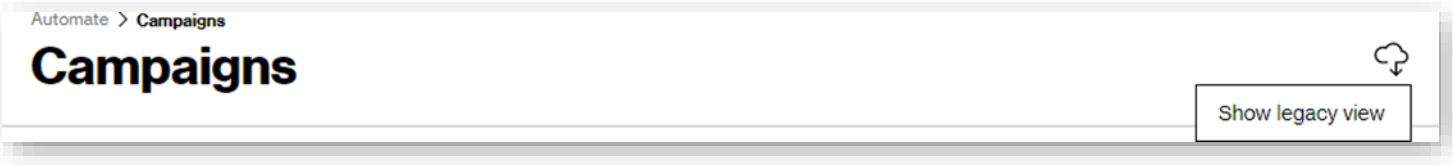
Use the **Search** field to locate campaigns by name.

**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.

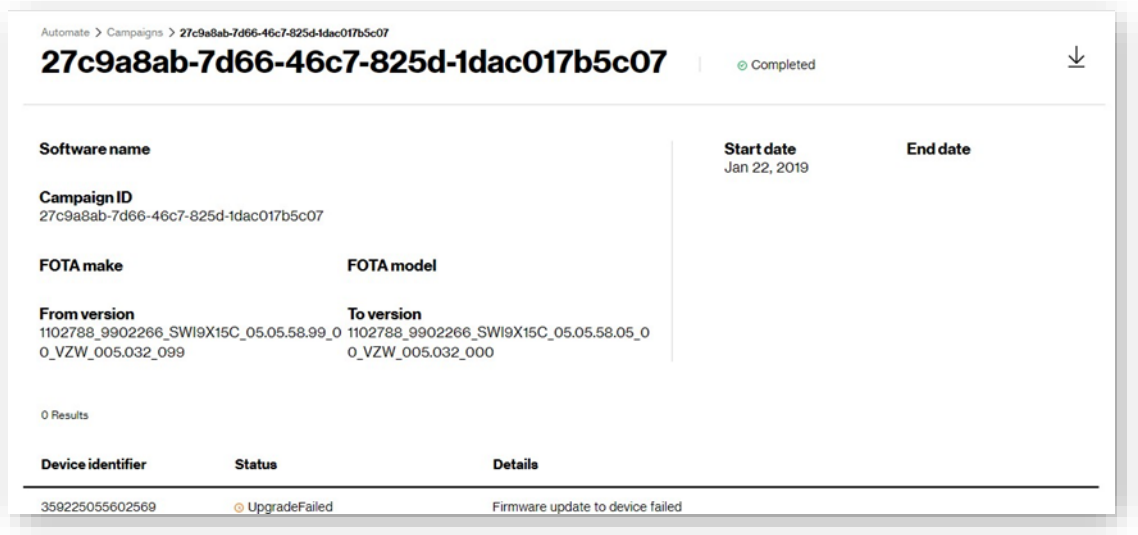
# Campaign Details

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

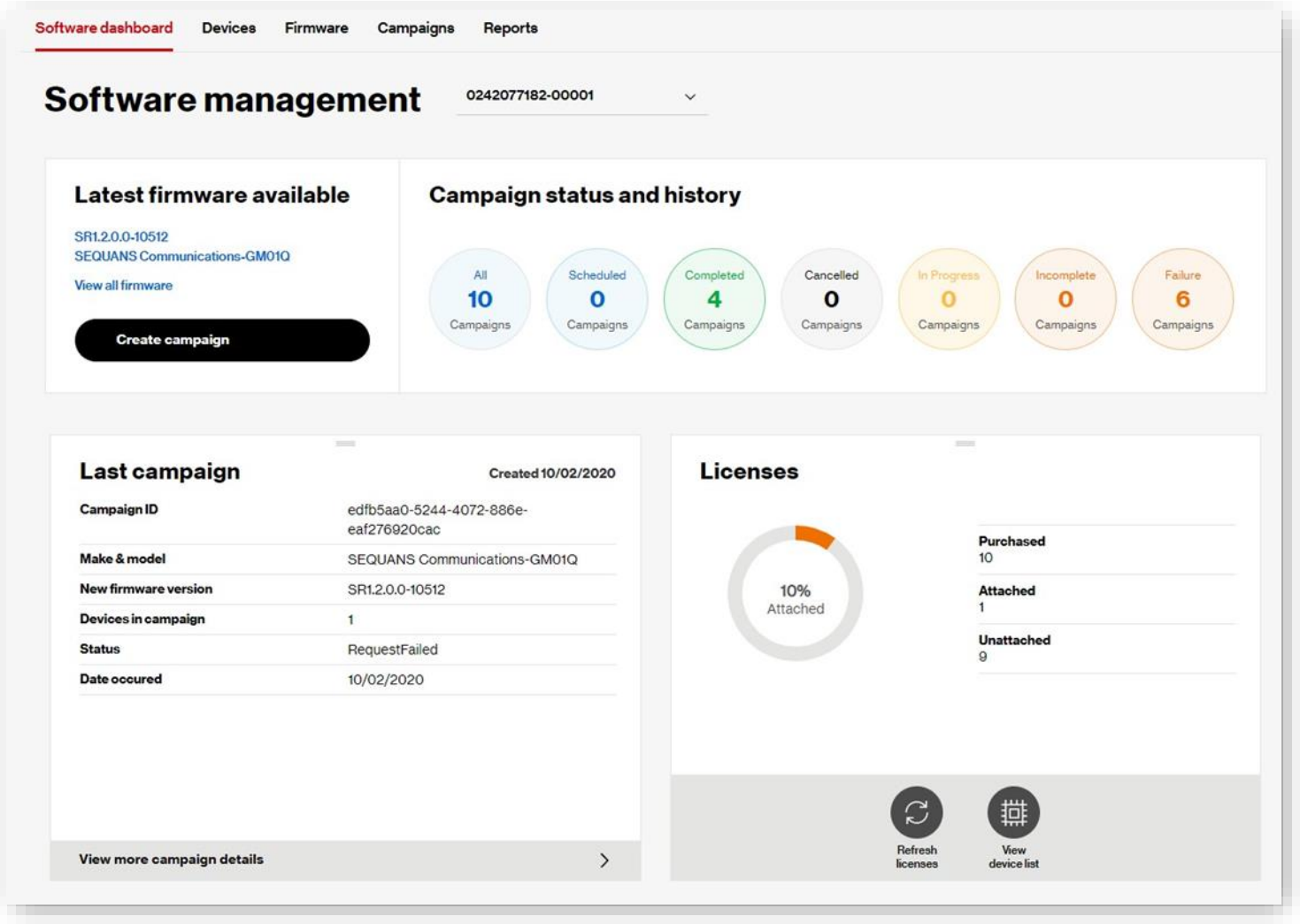
On the left navigation, click **Campaigns**. The *Campaigns* page opens.

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



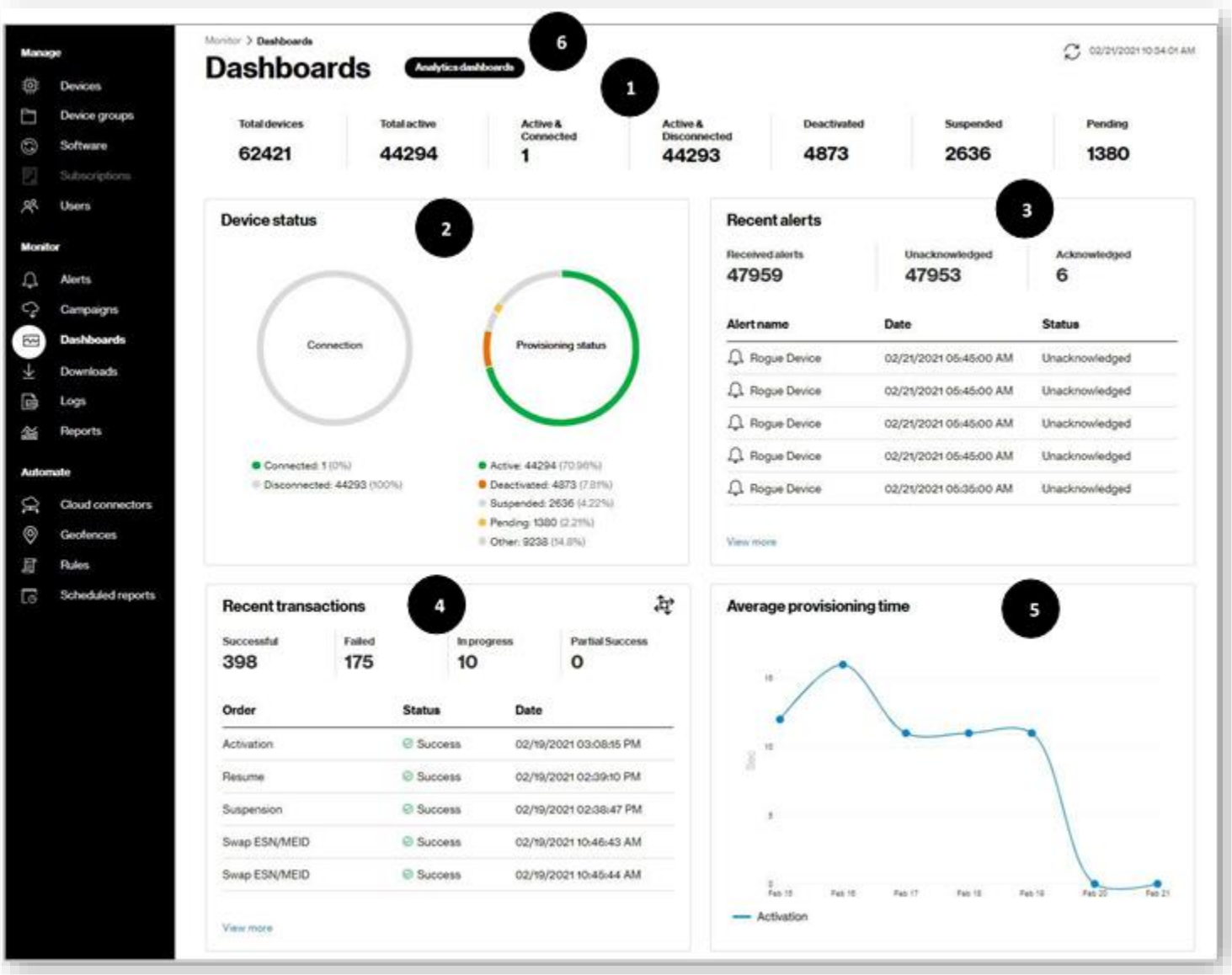
# Legacy View

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 | Device Status pod |
| 3 | Recent Alerts pod |
| 4 | Recent Transactions pod |
| 5 | Average Provisioning Time pod |
| 6 | Analytics Dashboards |

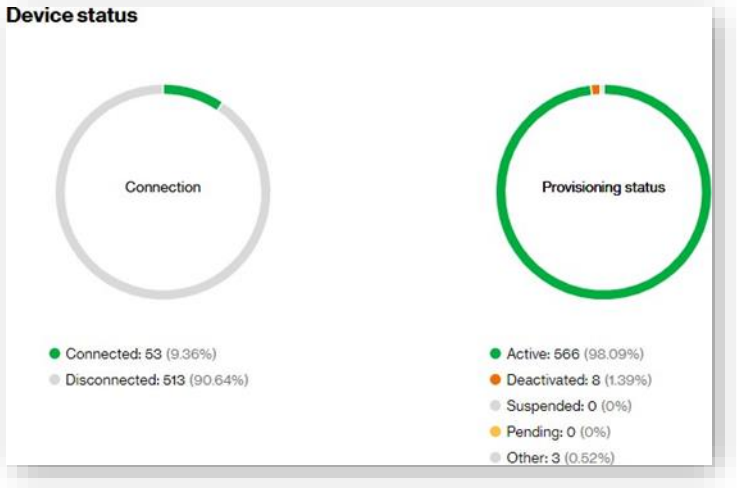
## Device Status Filters

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.

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

## Device Status Pod

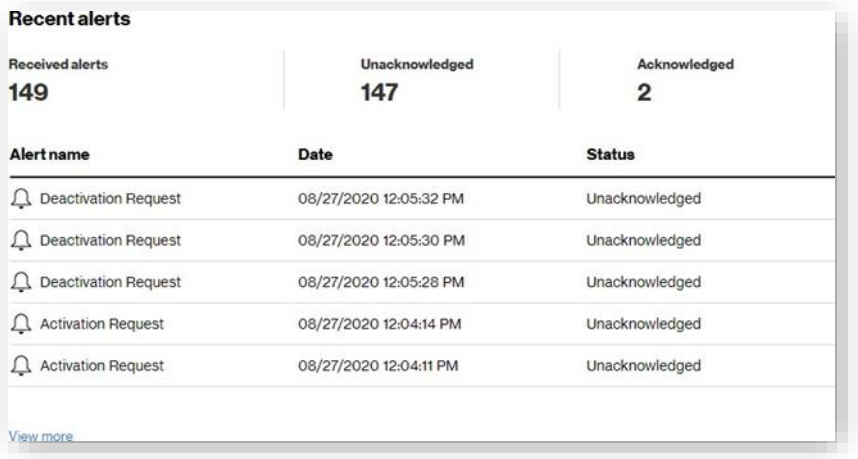
The *Device status* pod uses color-coded pie charts to show the connectivity and provisioning status for devices. Clicking in the **Connection** or **Provisioning** circle opens the *Devices* page listing devices with their connection and provisioning status. Clicking on the links the pie chart has the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




## Recent Alerts Pod

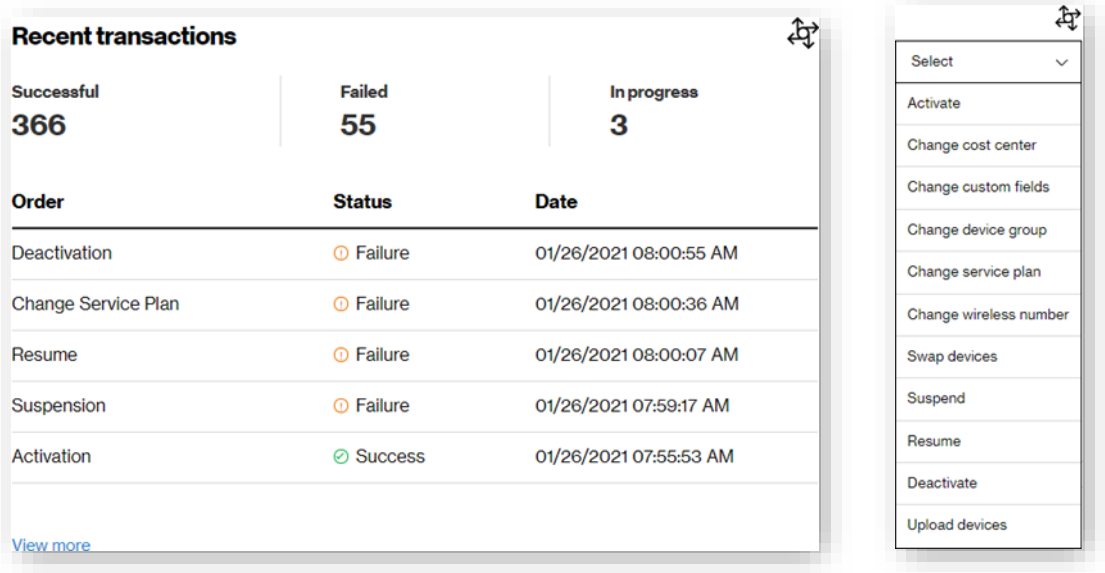
The *Recent alerts* pod contains filters and a recent alerts list.

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 Transactions Pod

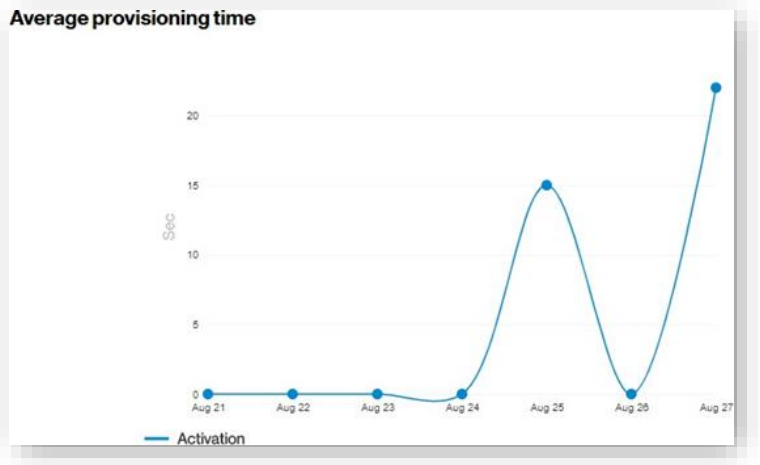
The *Recent transactions* pod contains filters along the top of the pod showing the total number of recent transactions that were performed successfully, are in progress, or have failed. The table that follows these filters lists the five most recent provisioning orders, their status, and the date and 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.




## 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.

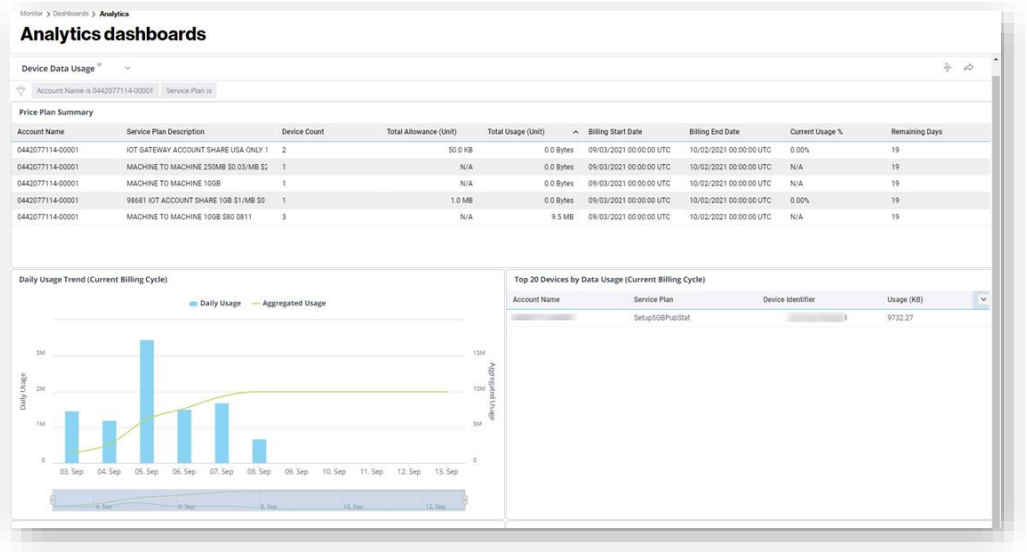


# Analytics Dashboards

*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

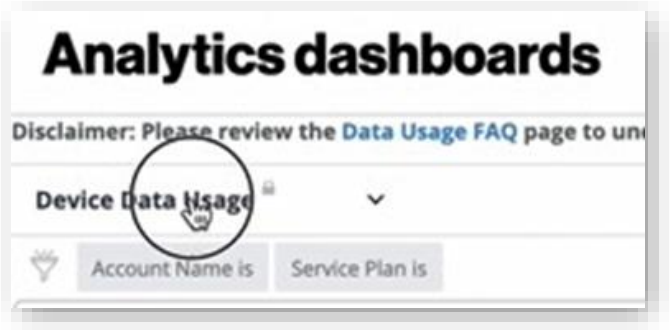
Click the search icon to type a keyword, or click the Natural Language Processor icon to type a question.

## Export Data

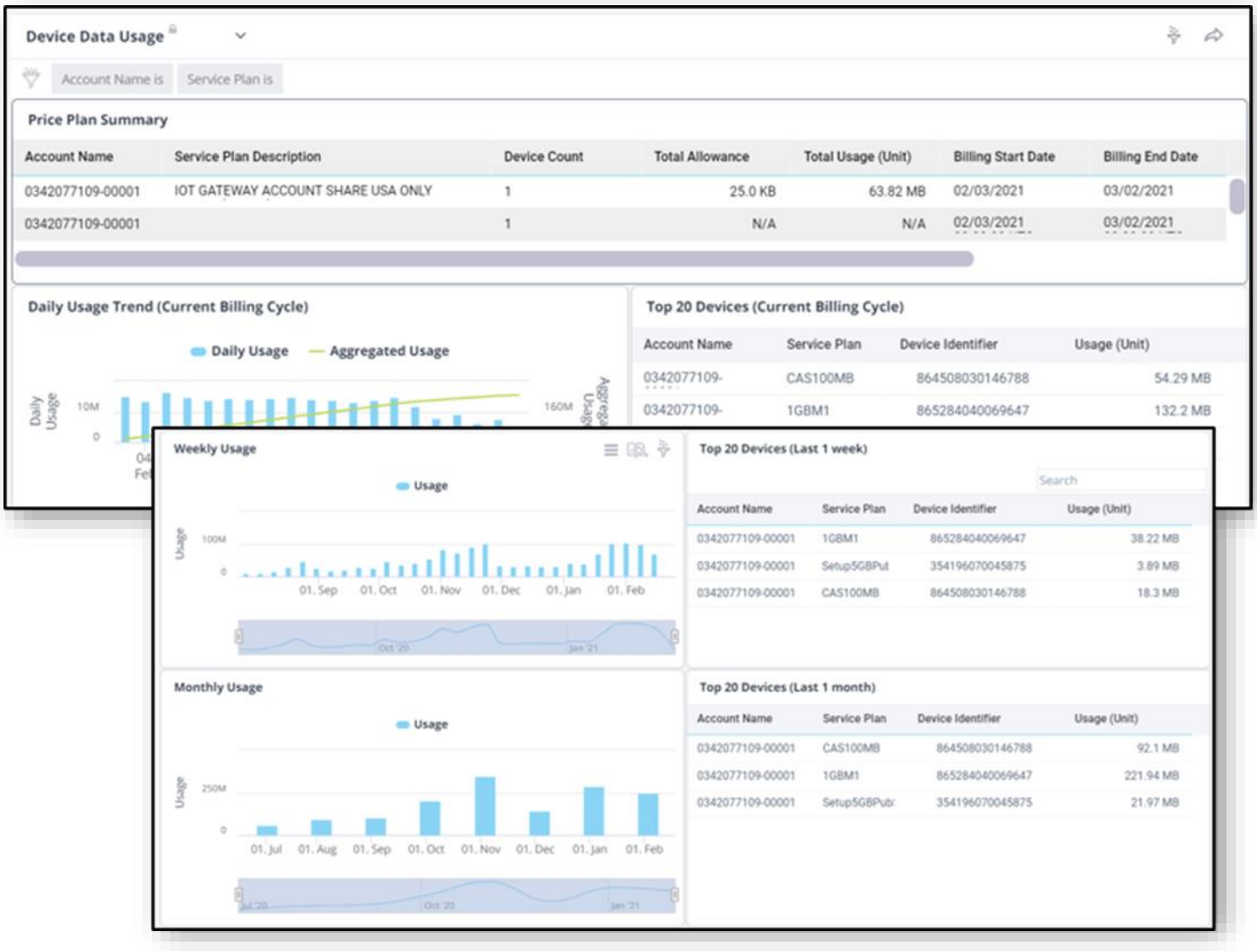
You can export individual charts into multiple formats. Visualizations may export to images, tabular data may export to CSV or XLS files. You can also download filtered data to a PDF file. Click the pen the *Share and Email Options* dialog and click **Export as PDF**.

## Analytics Dashboard Views

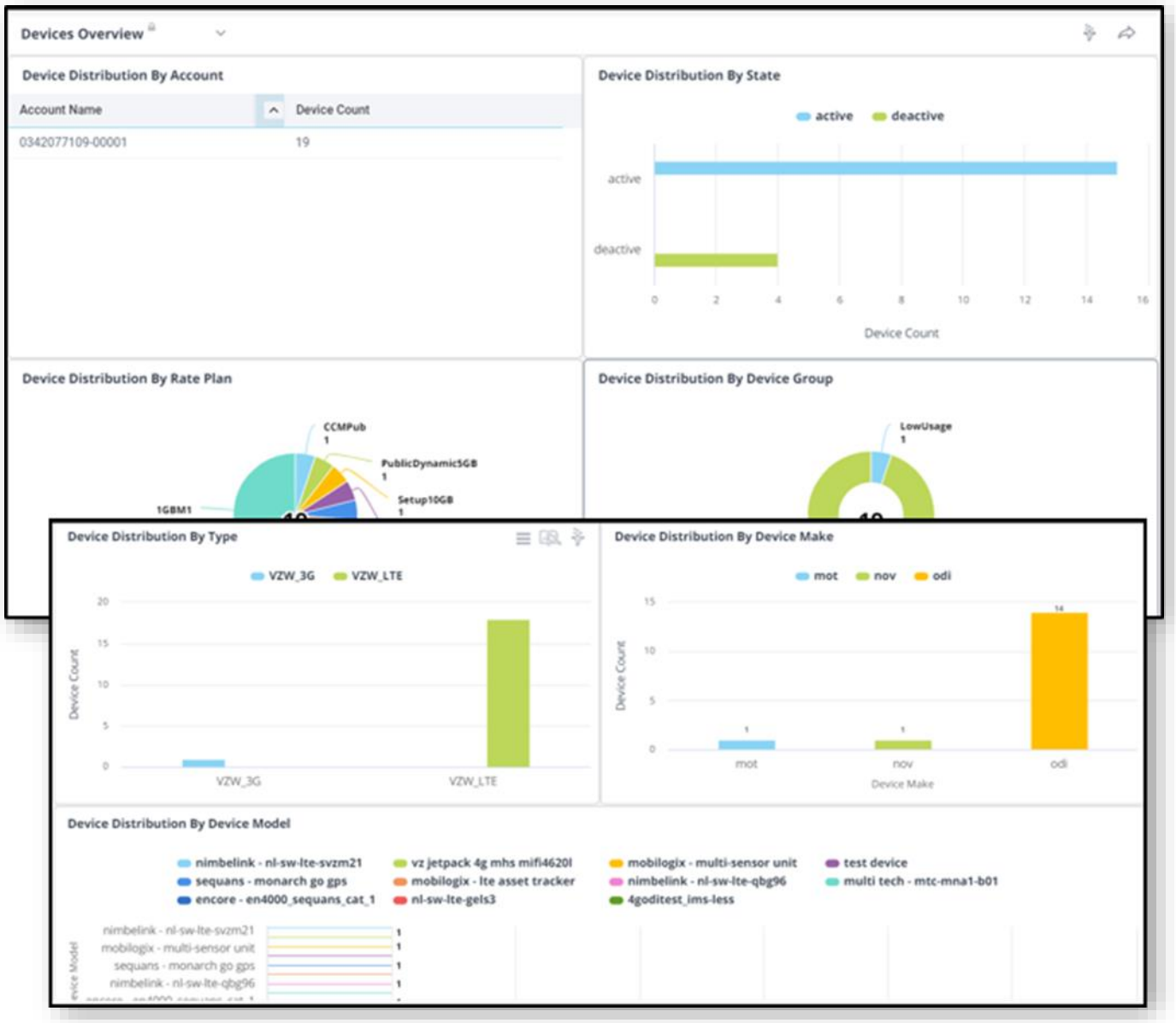
Click the view menu to select one of the following views.



*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.

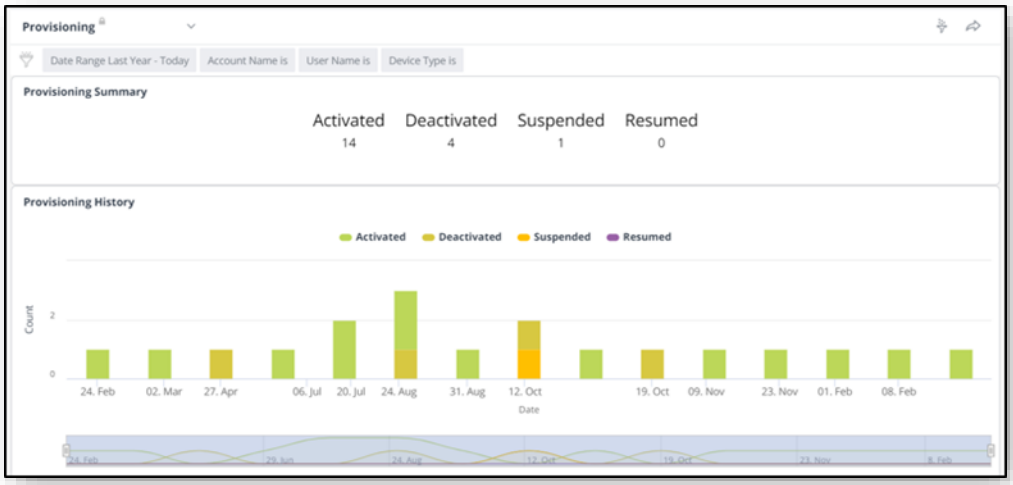


*Devices Overview* dashboard provides insights into device attributes and distributes, such as states, rate plans, groups, make and model, etc.



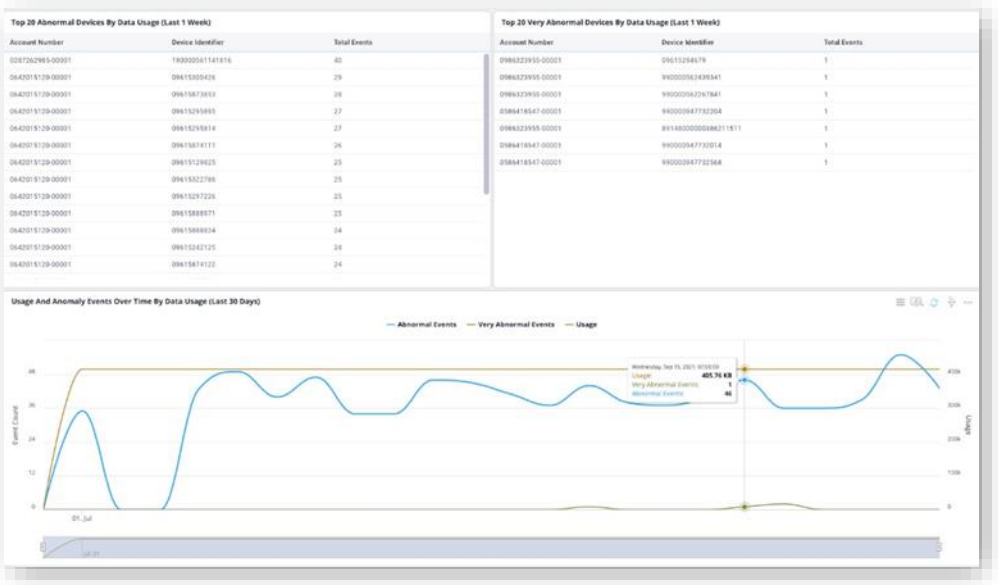
*Diagnostics* analytics dashboard provides insights into LWM2M diagnostic streaming events if compatible LWM2M devices are streaming.

*Provisioning* analytics dashboard provides insights into provisioning history.



*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

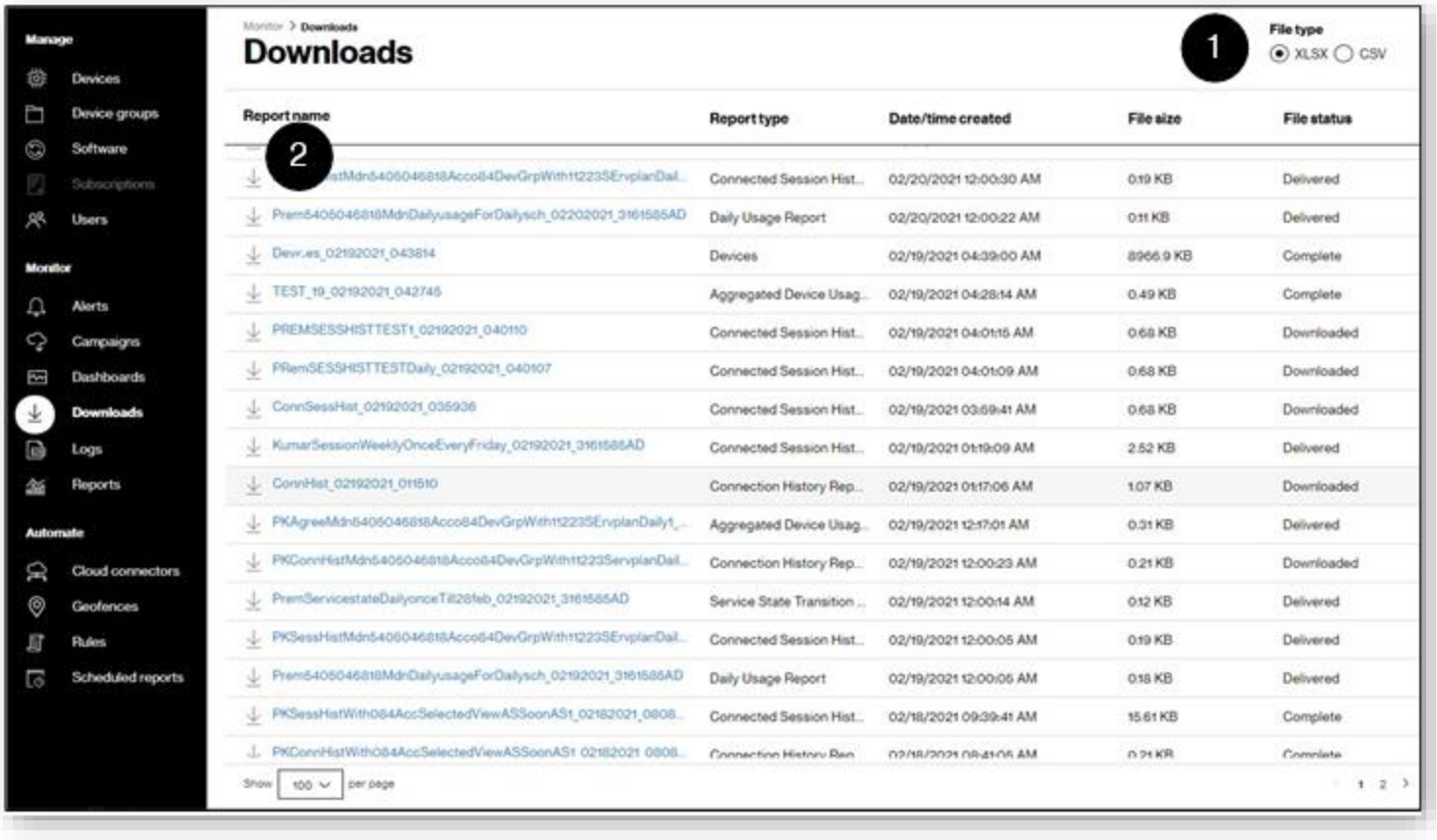
Wireless Network Performance (WNP) is a My Business analytics tool that offers deeper insights into your Verizon network device data. WNP is available in Basic and Premium tier. ThingSpace Intelligence subscribers can use WNP, which is available in Basic and Premium tier. The Intelligence bundle includes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

Open WNP from the Verizon Apps menu .

# Downloads

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

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




| Elements on the Downloads page | | |
|---|---|---|
| 1 | | **File Type options** – Select the file format to download. |
| 2 | ↓ | **Download** – Export the file. |

How to download a report

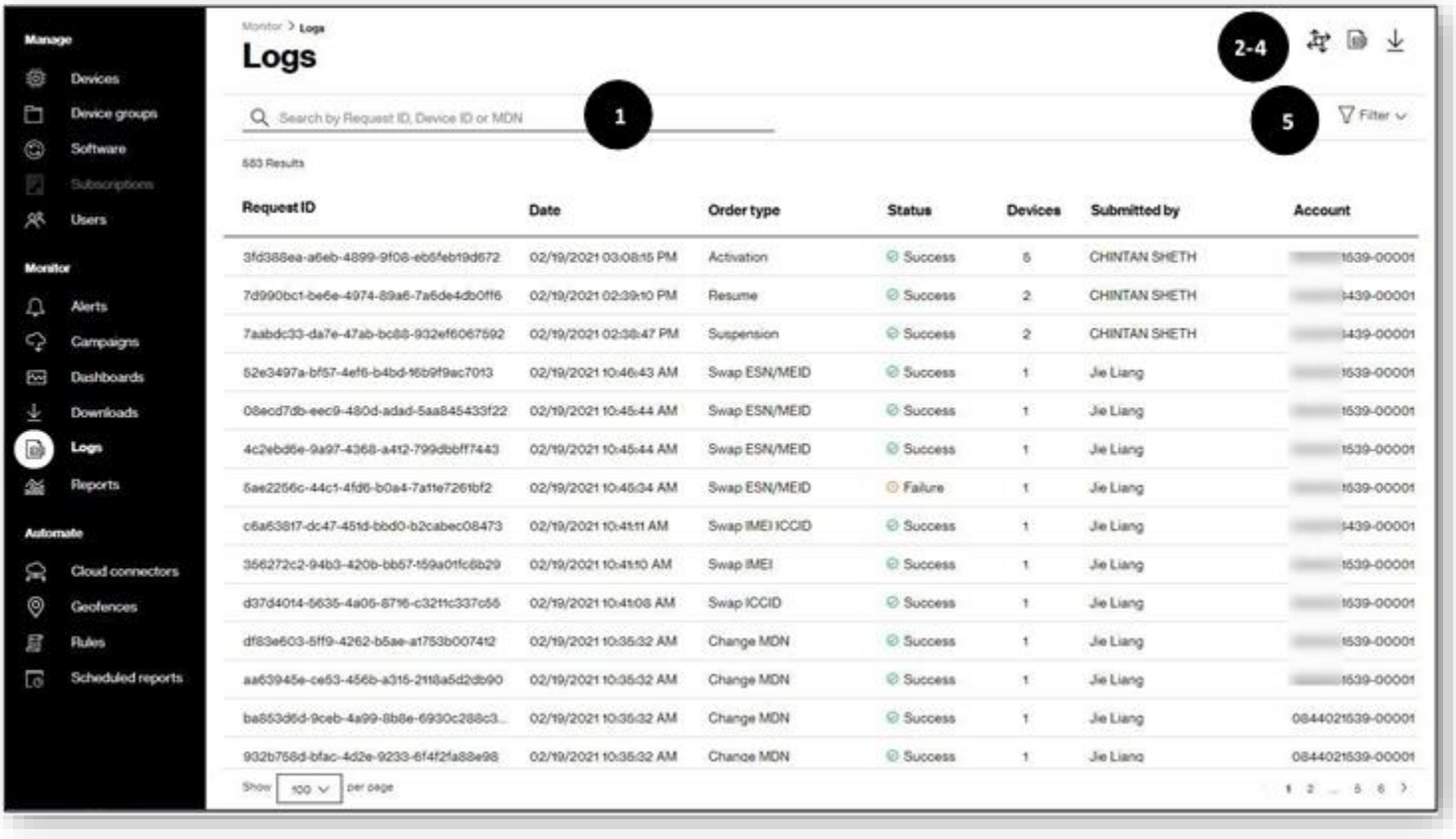
1. At the top-right of the *Downloads* page, click the **File type** of your choice (XLSX or CSV).
2. Click the *Report name* download icon ↓ . The file exports to your device

# 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.



| Elements on the Logs page | | |
|---|---|---|
| 1 | | Search – Locate a specific log by request or device identifiers. |
| 2 | | Actions – Open the Logs action menu. |
| 3 | | Show application log – View and download the *Applications log*. |
| 4 | | Download – Export the list. |
| 5 | | Filter – Limit the list to logs with specific attributes. |

## Searching Logs

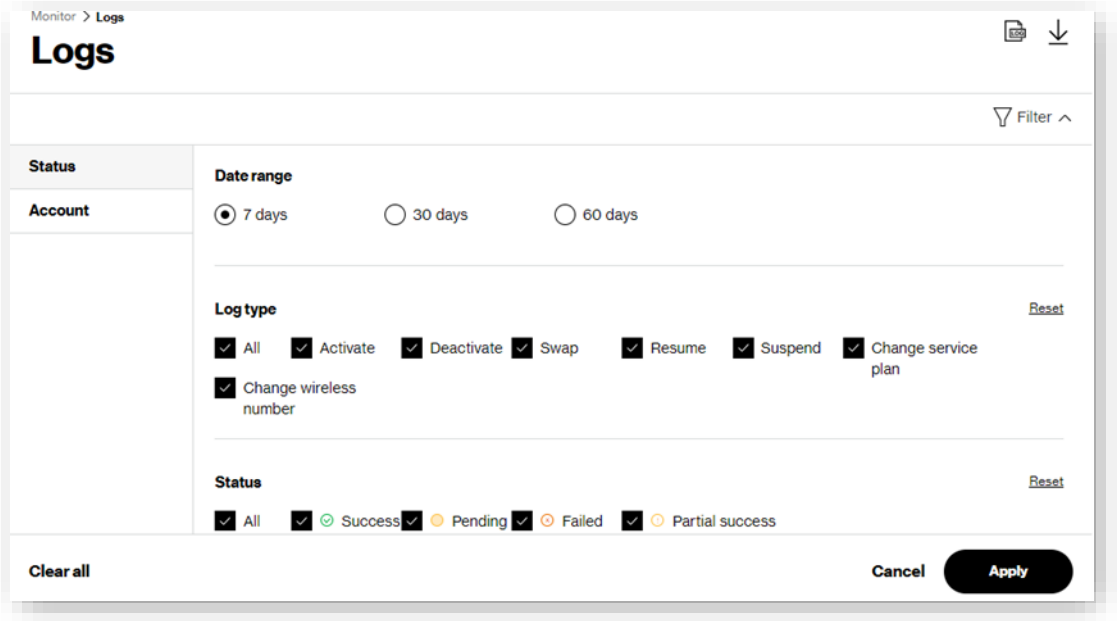
Use search to view the log records that match the entered criteria. You can enter a Request ID or a Device ID to narrow your search results. Wildcard (%) search is supported for Device ID and MDN search only.

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

# Applying Filters

How to apply filters

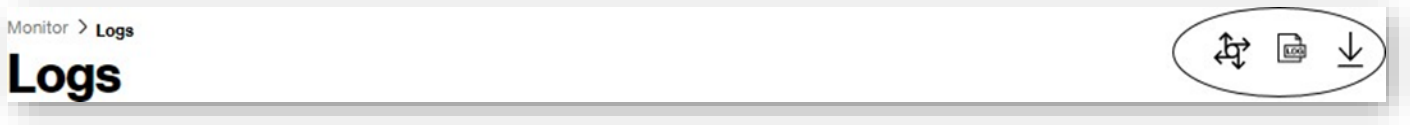
Click Filter . The *Filter* page opens.




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

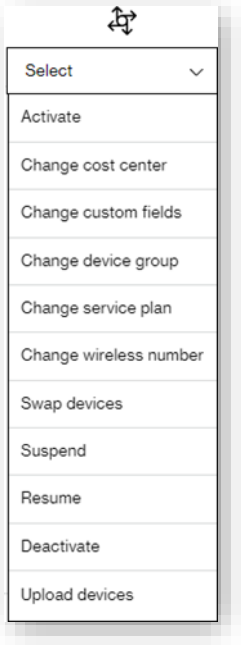
Use the actions icon to display a menu of actions.




## 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.

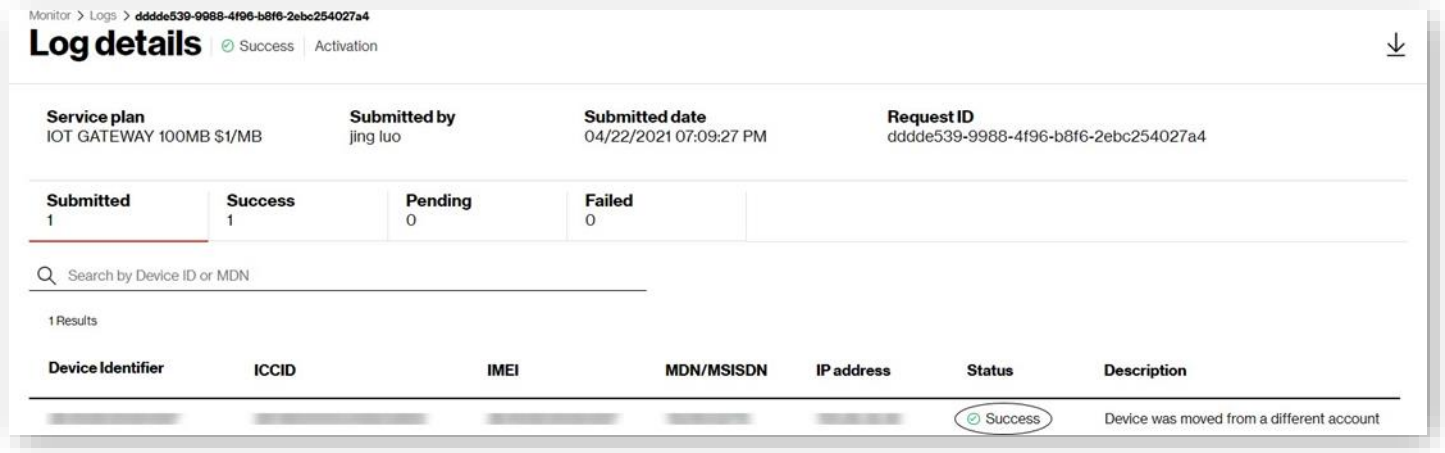
# Log Details

Click a Request ID to drill down into log details.

To view log details

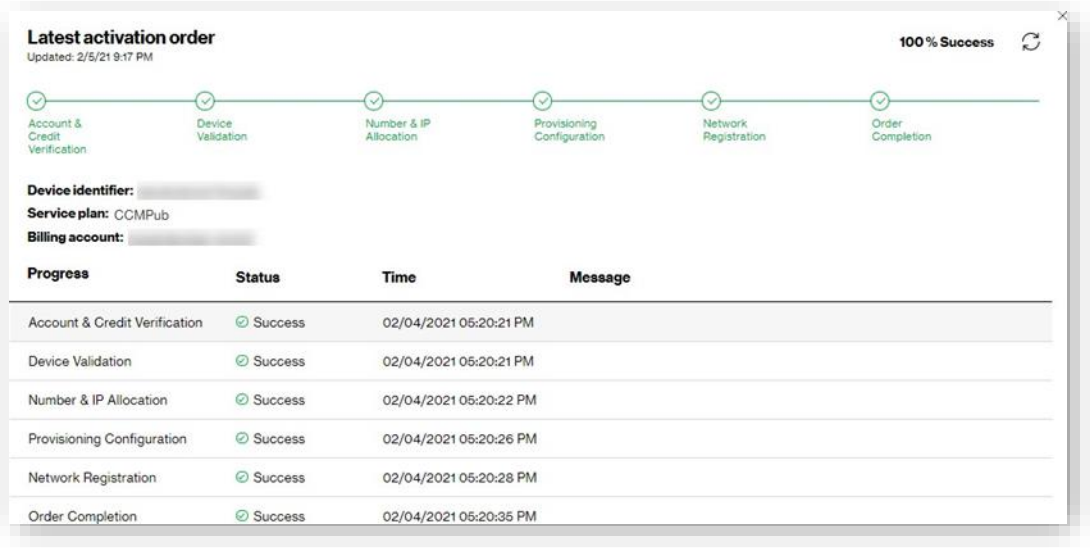
On the left navigation, click **Logs**. The *Logs* page opens.

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.

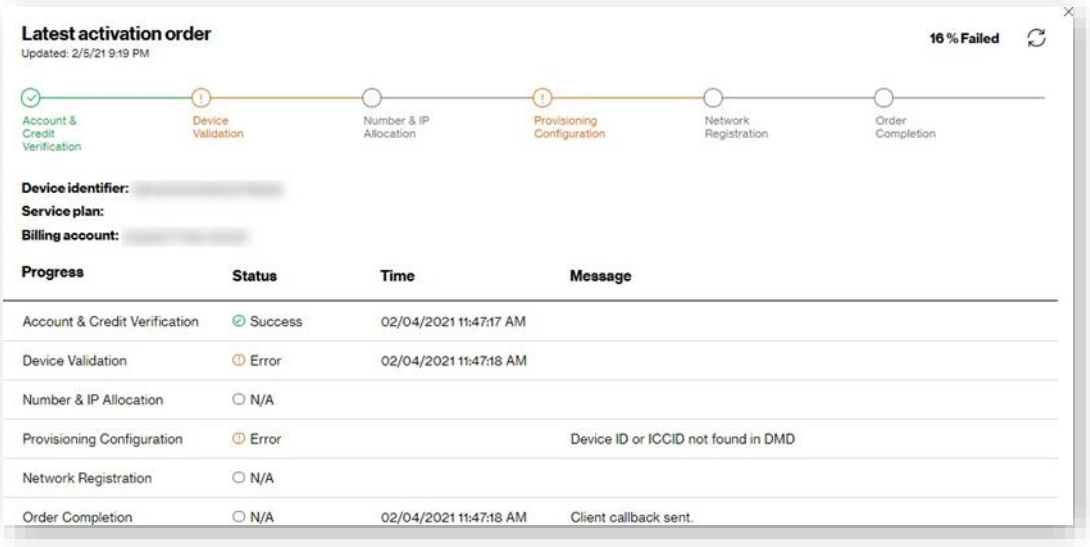


For Activation orders that have completed in the past seven days, you can click the status value (e.g. Success, Failed) to view the order status.

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



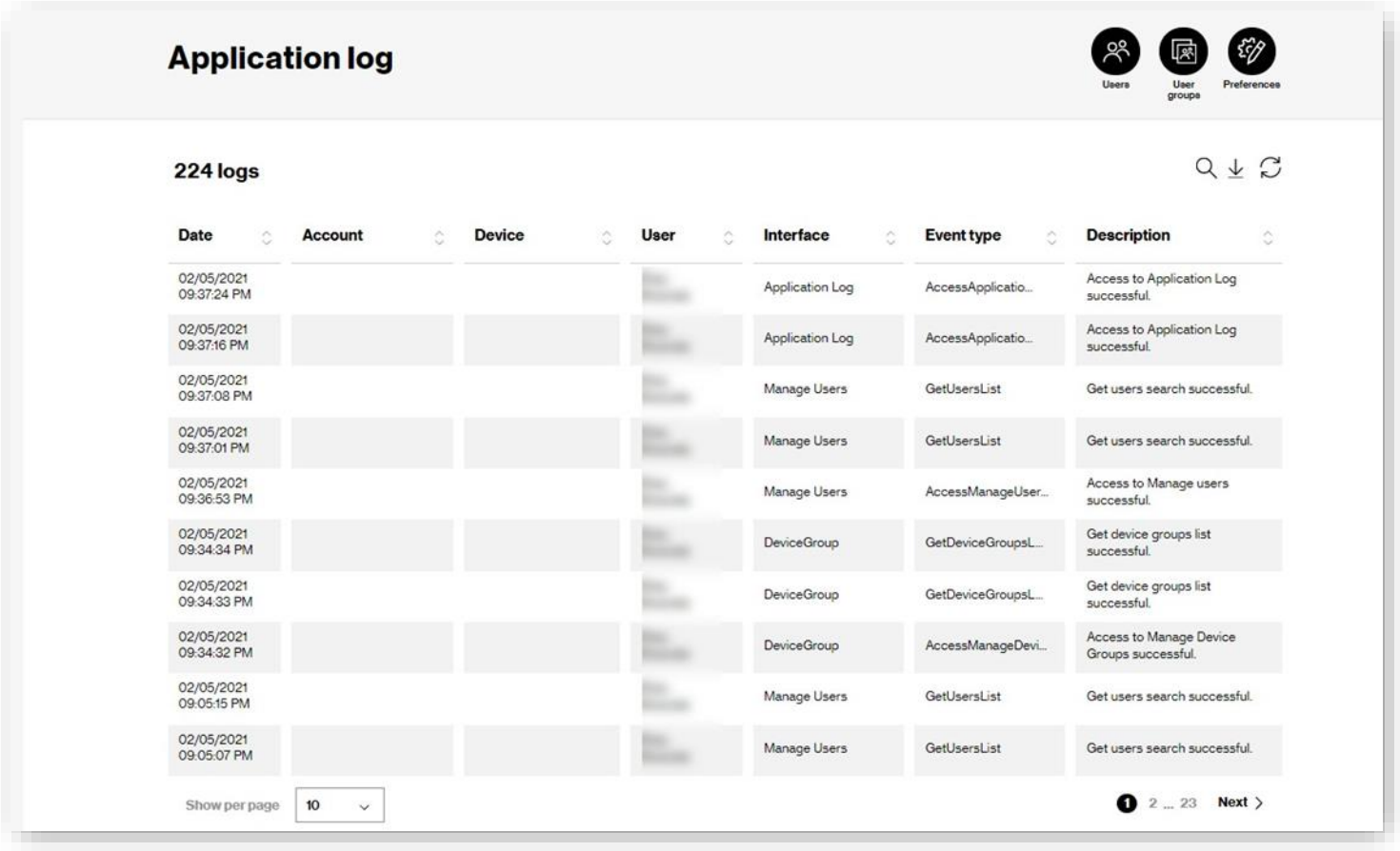

The following is a **failed** activation order example. You can identify where in the provisioning process the transaction failed. In this example, the failure occurred in the Provisioning Configuration step because the device was already active on another line.



# Application Log

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

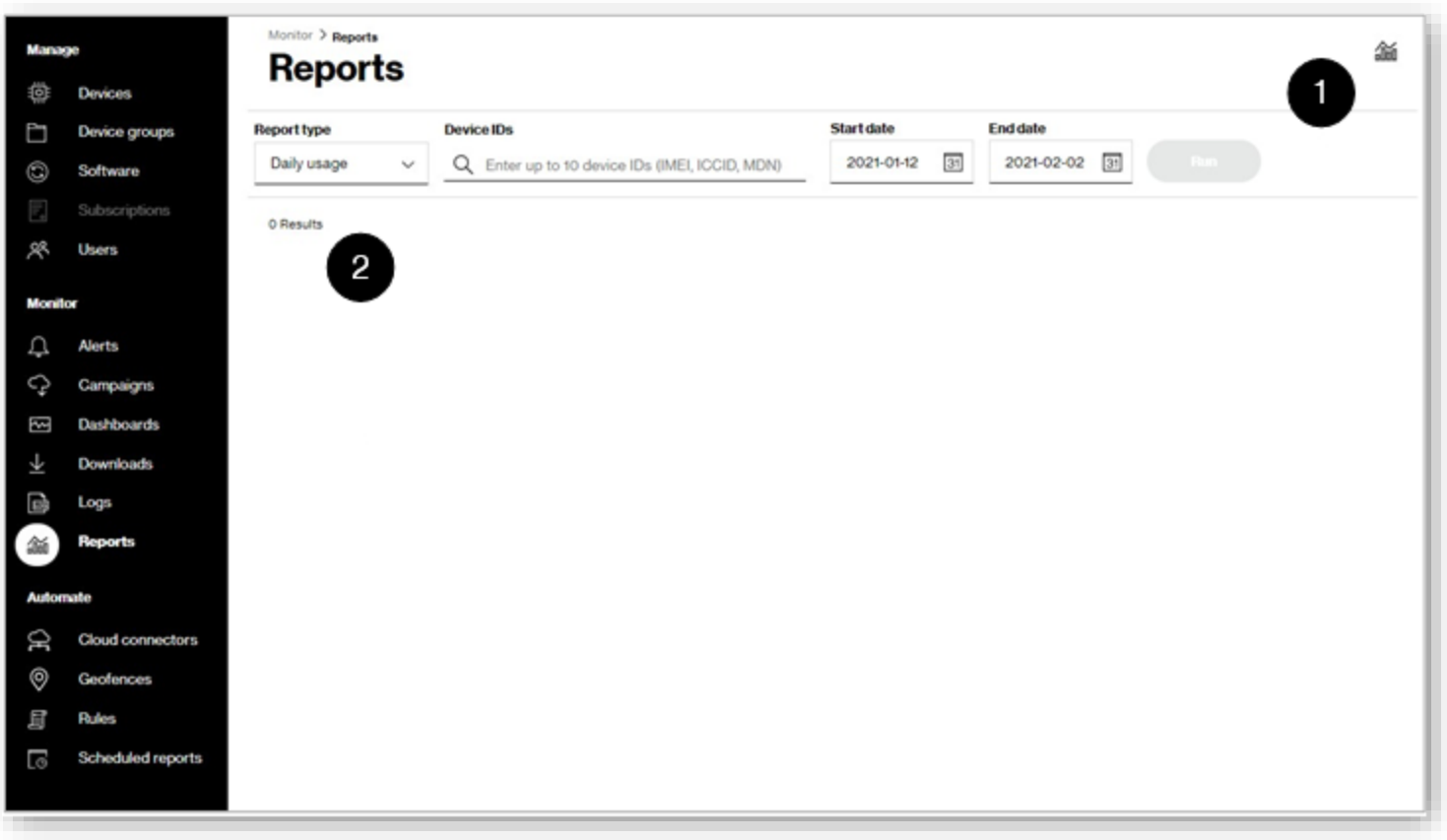
On the left navigation, click **Logs** to open the legacy page.



# 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 | | **Reports** – Create an advanced report |
| 2 | | . **Report type** – Open a menu to select a report category. |

# Running Select Reports

How run reports

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

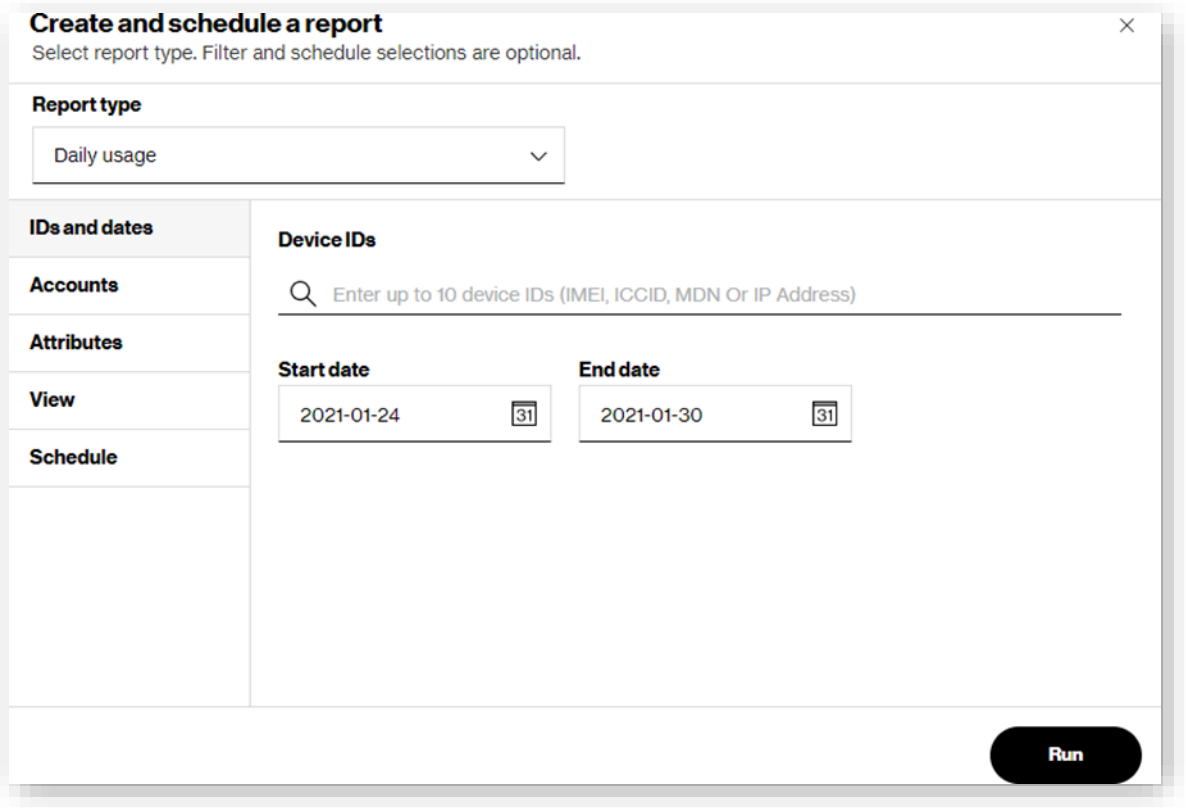
Select report criteria:

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

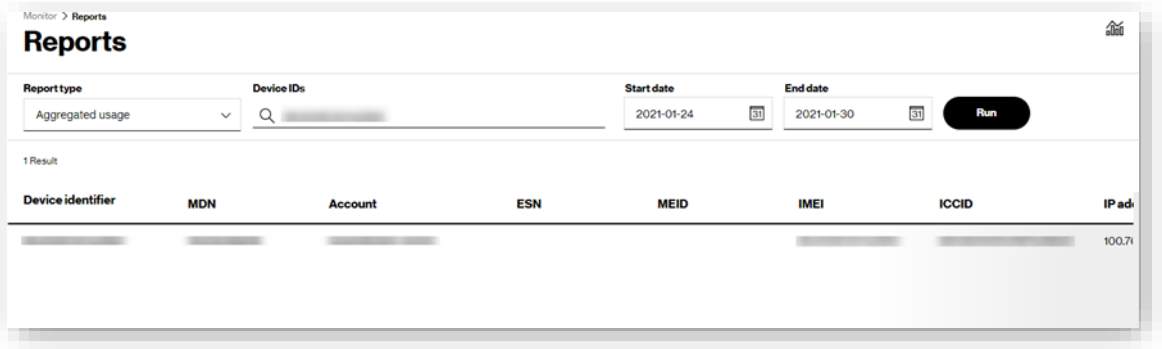
Use the reports icon to create, save, and/or schedule advanced reports. These reports usually take longer and are submitted in the backend for processing. Finished reports are available on the Downloads page.



## 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.

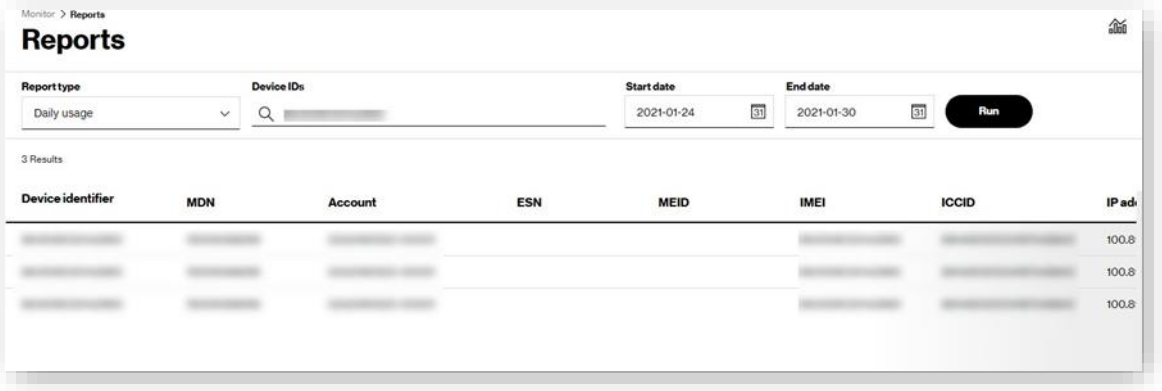
**NOTE:** The offline reporting maximum date range is 12 months.




## 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.

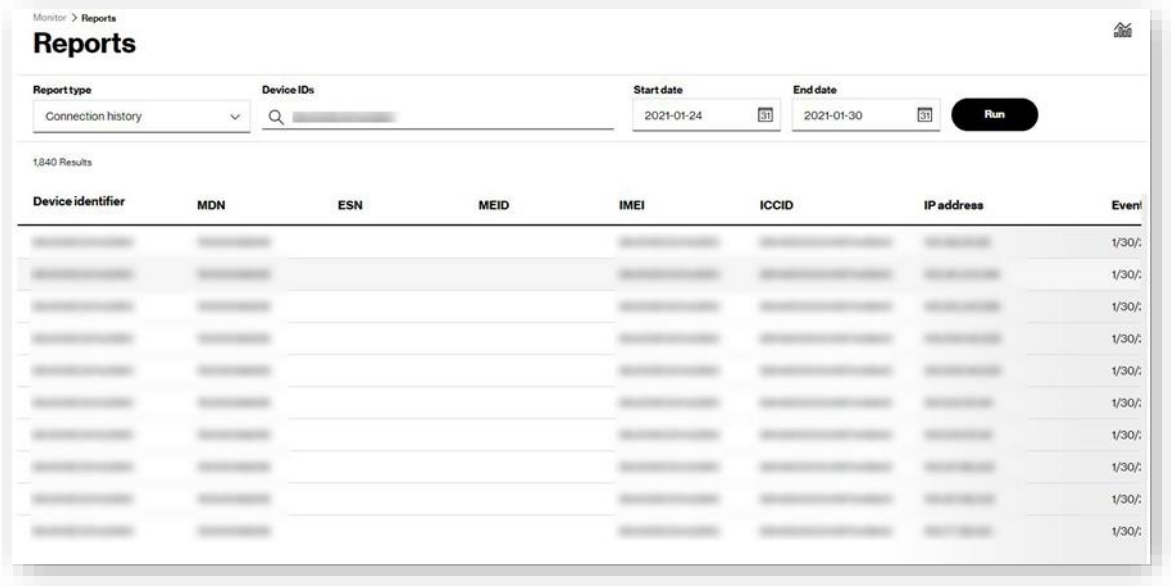
**NOTE:** The offline reporting maximum date range is 12 months.



# Connection History Report

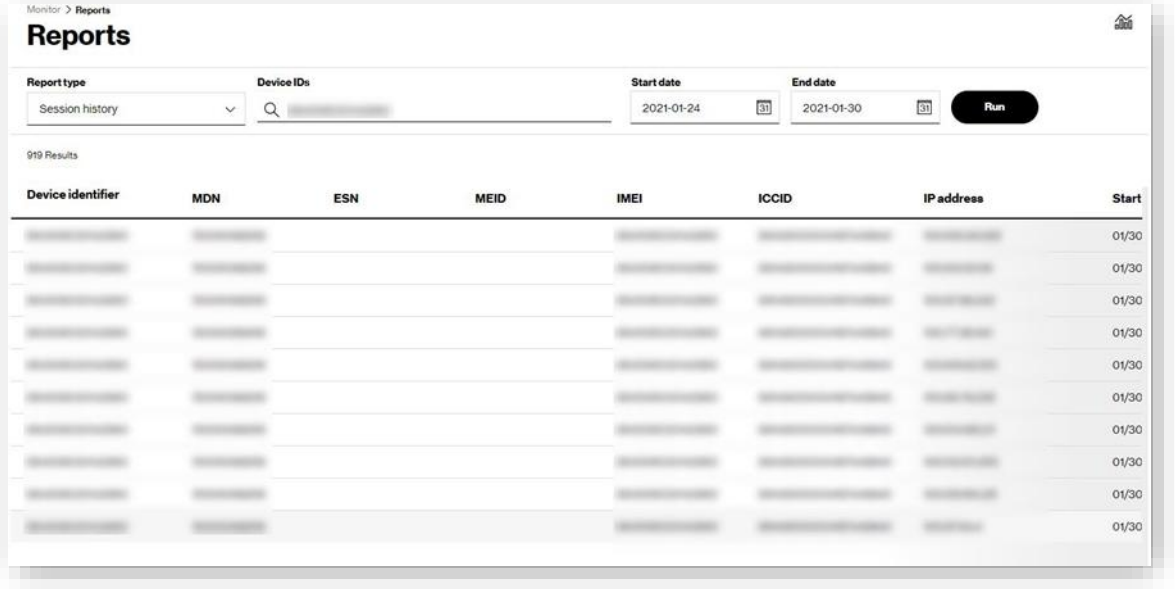
The *Connection History Report* shows each connection event for a specified device(s) over a particular date range, and provides the start and stop events associated with a device's connections. This report also shows data usage during each connection.

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



# Session History Report

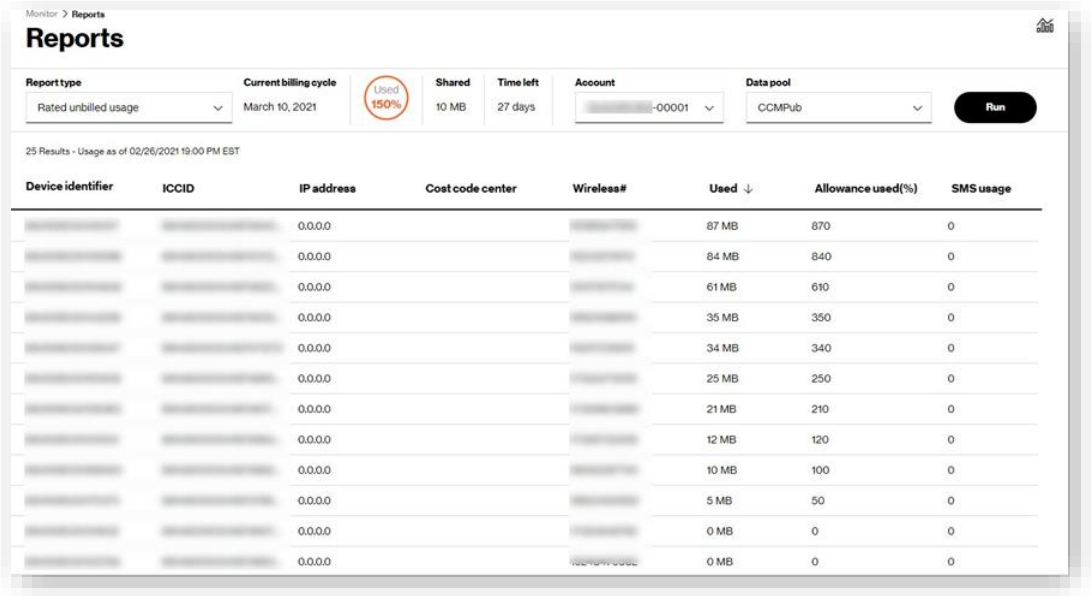
The *Session History Report* provides information about one or more device connected sessions within a specified time period. This includes both data usage consumed and duration of each session. A connection session is delineated by Start and Stop records. For offline reporting, the maximum date range 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.



## 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.




## 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:

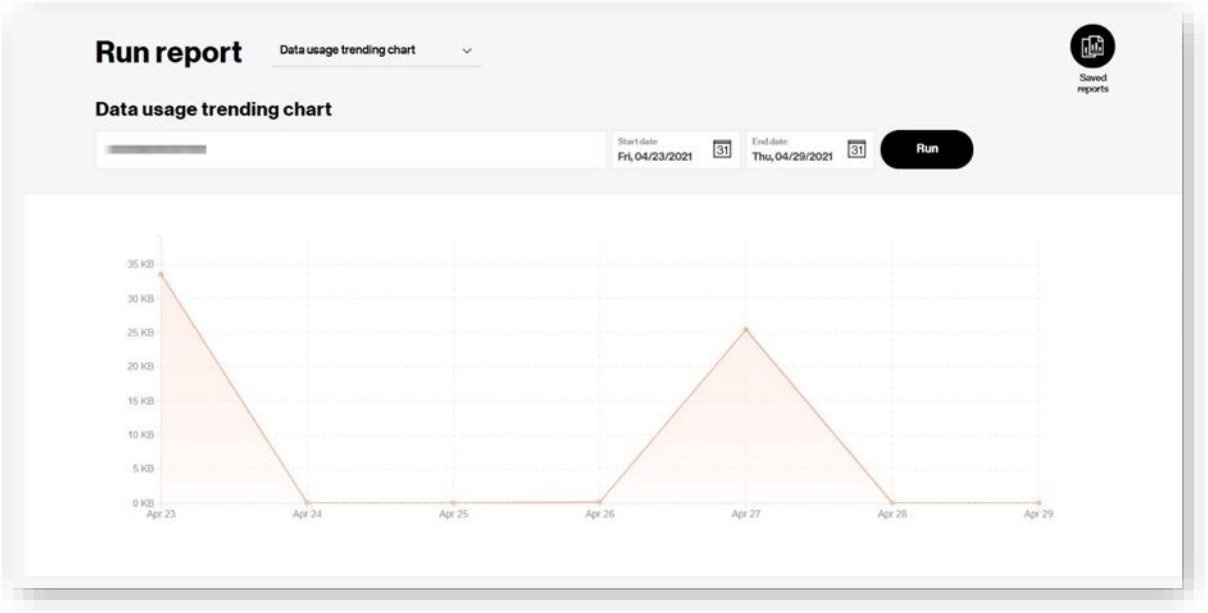
- **ICCID**: The SIM card number associated with the device
- **Event date**: The timestamp (within the hour) from which this anomalous event occurred
- **Usage (KB/h)**: The reported data usage from the hour within the event
- **Anomaly rarity**: The probability value that represents the rarity of the 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

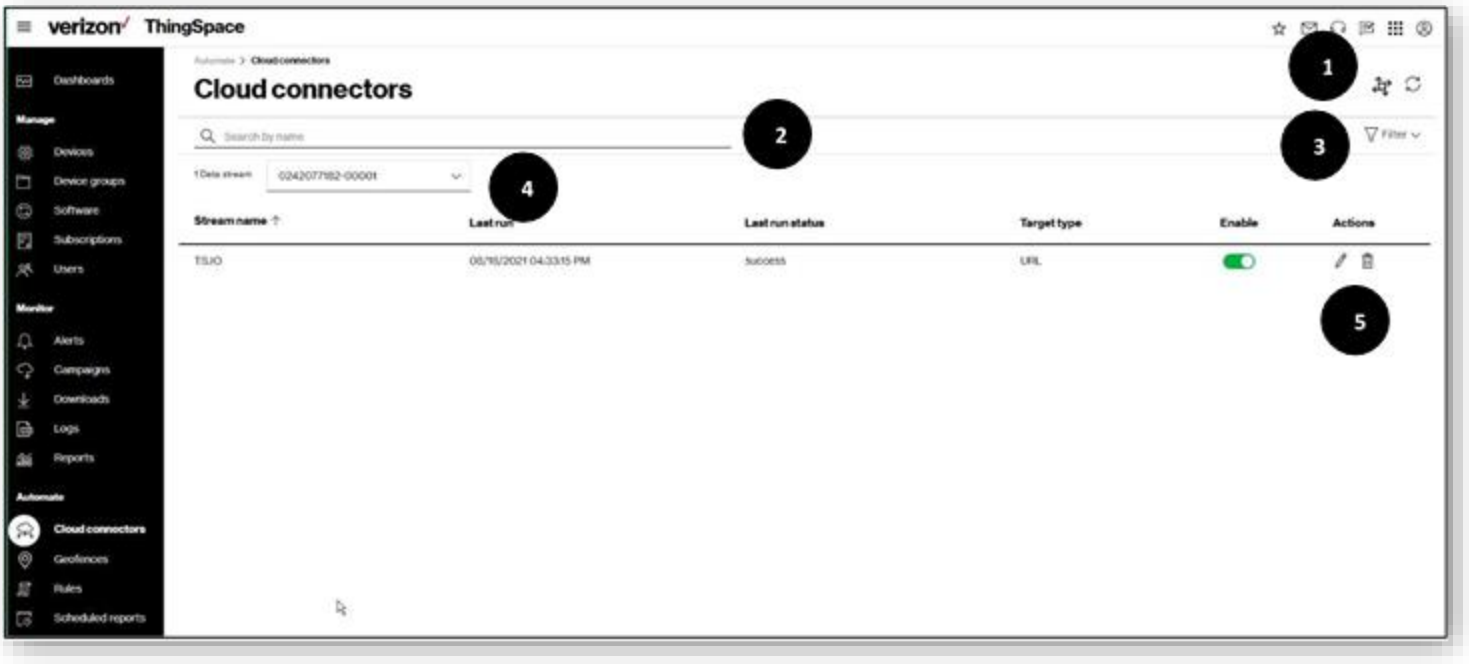
This report provides a chart that shows data usage patterns over a specified time period.



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

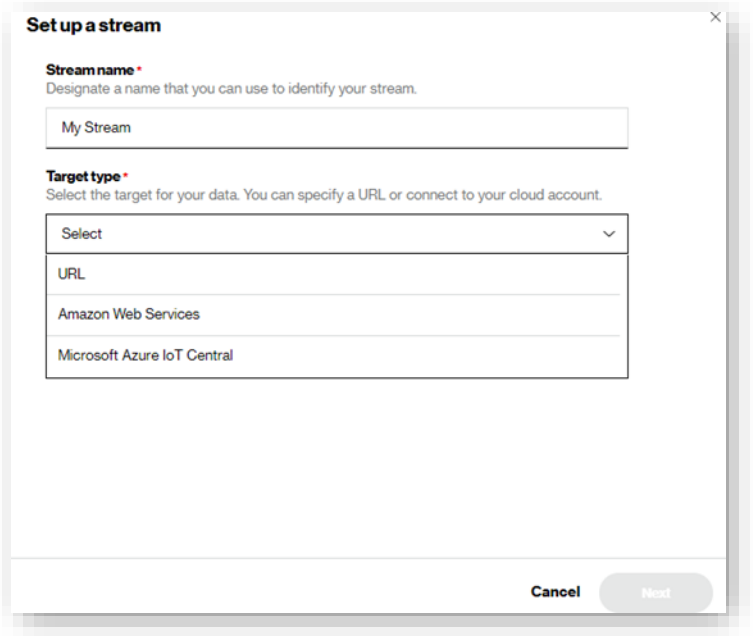
# Create a Stream

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.

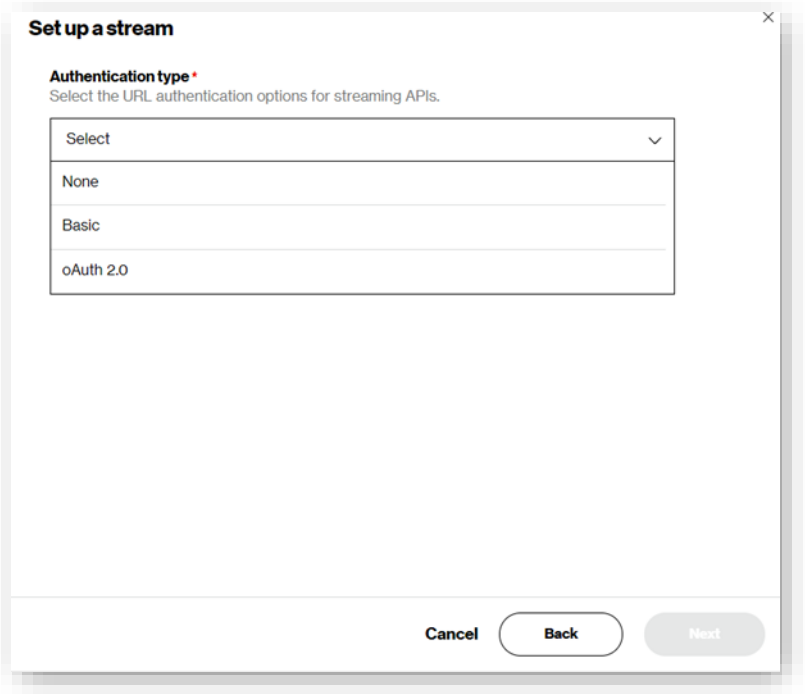



2. For **Stream name**, type a descriptive label to easily identify the stream.
3. For **Target type**, select the type of streaming you are defining (URL streaming, streaming to Amazon Web Services, or streaming to Microsoft Azure IoT Central.
4. Click **Next**. The *Authentication type* menu opens. 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:




**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 CLIENTIDand 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:CLIENTSECRETin 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.

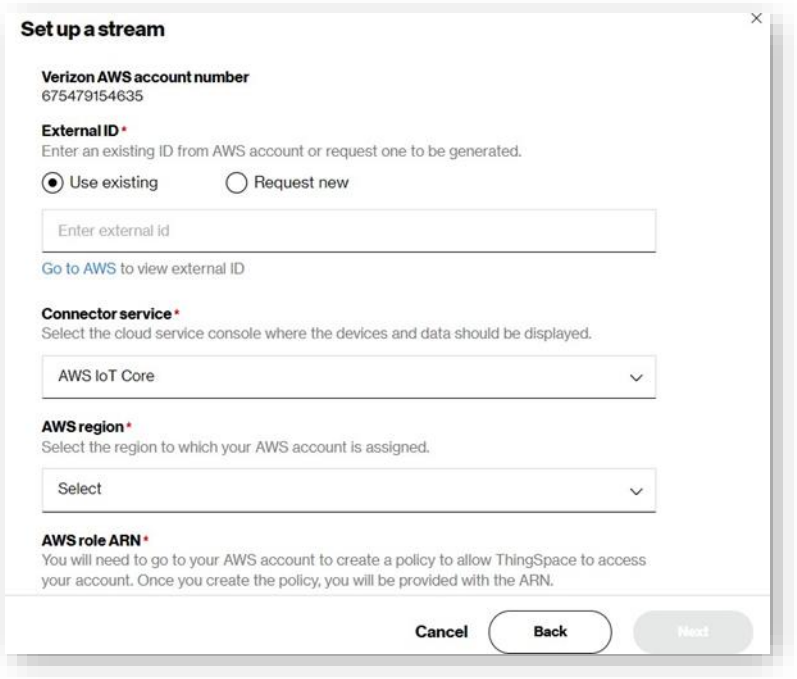
How to configure an AWS account

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 late.

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



# Using Microsoft Azure

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

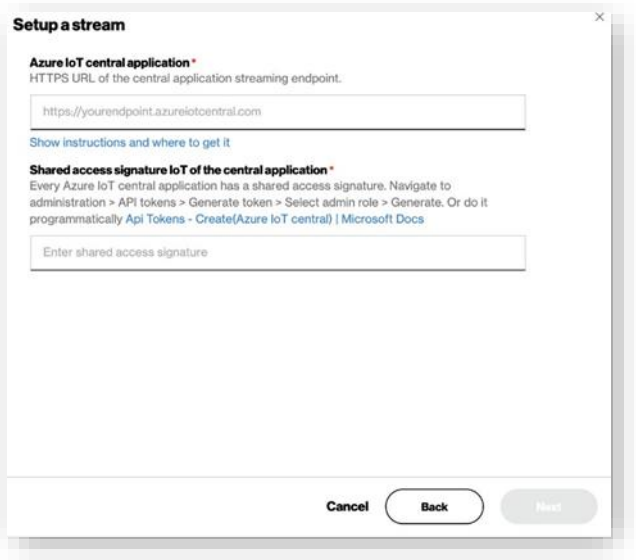
How to configure an Azure connection

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.

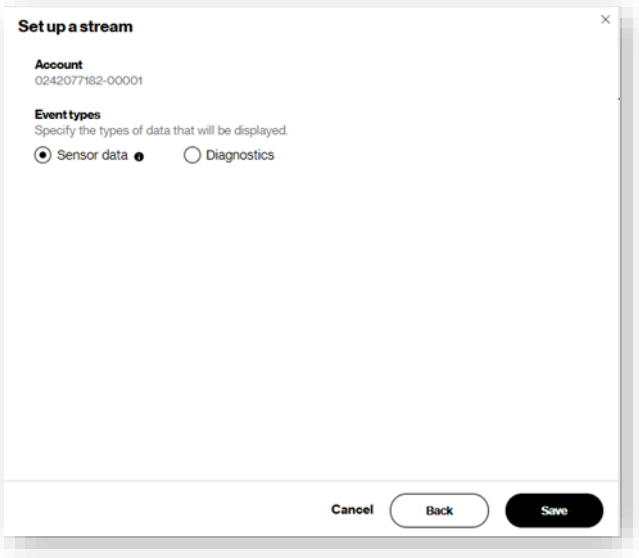
How to configure a stream to your Azure account




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.



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

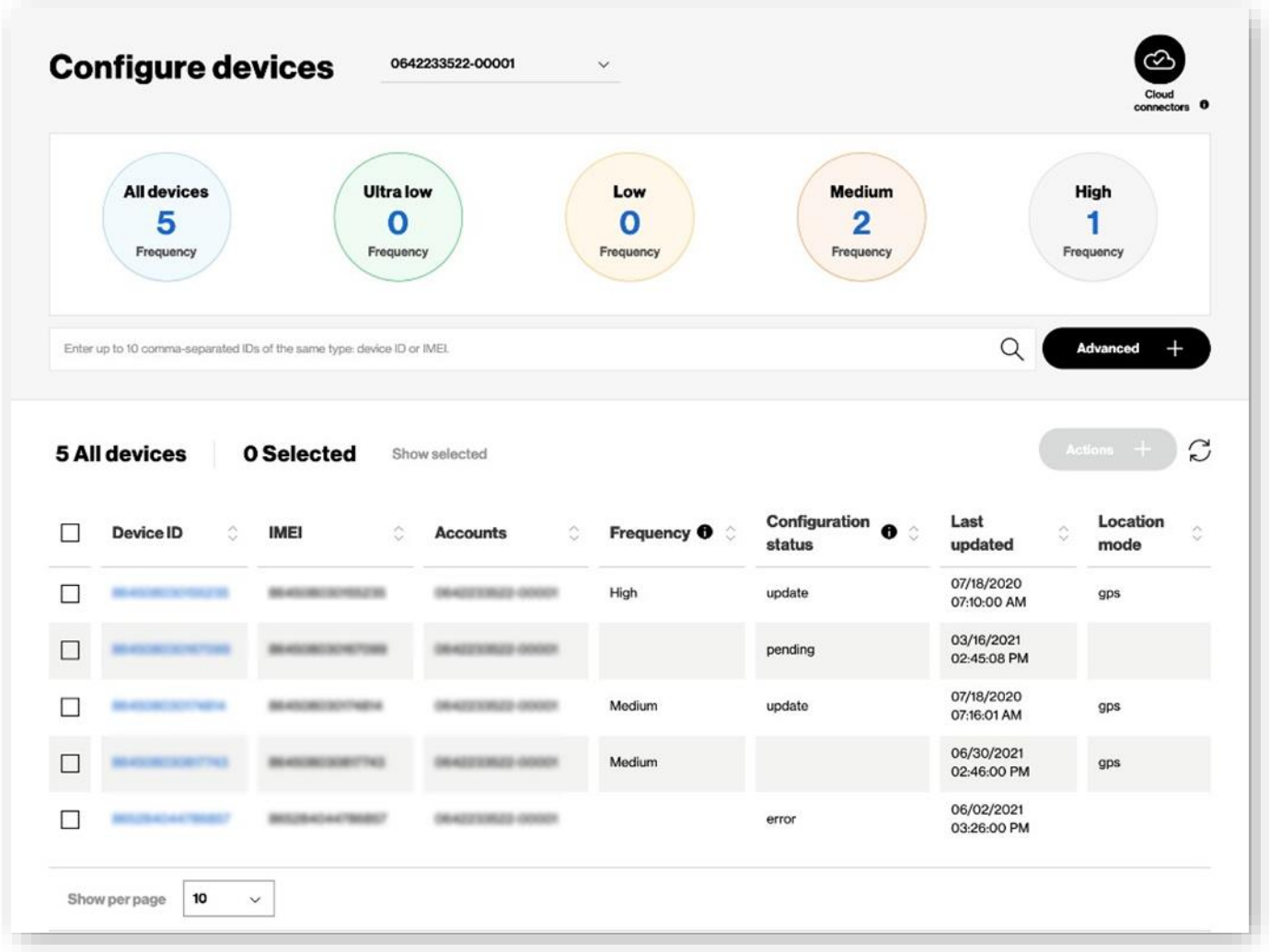
You can change the status reporting frequency of each device, and whether or not location information via GPS is running.

**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

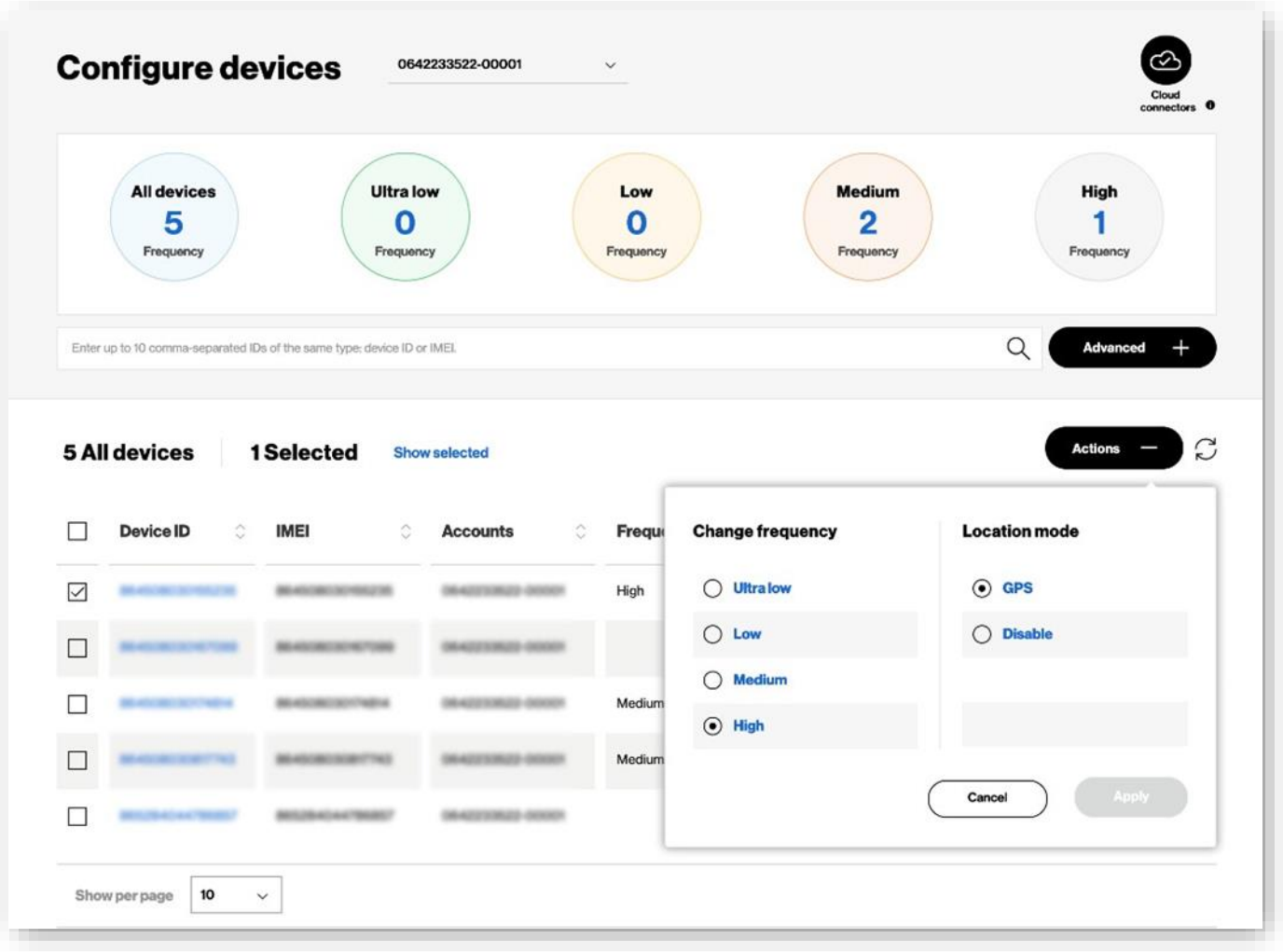
One the left navigation, click **Cloud connectors**. The *Cloud connectors* page opens.

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




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.

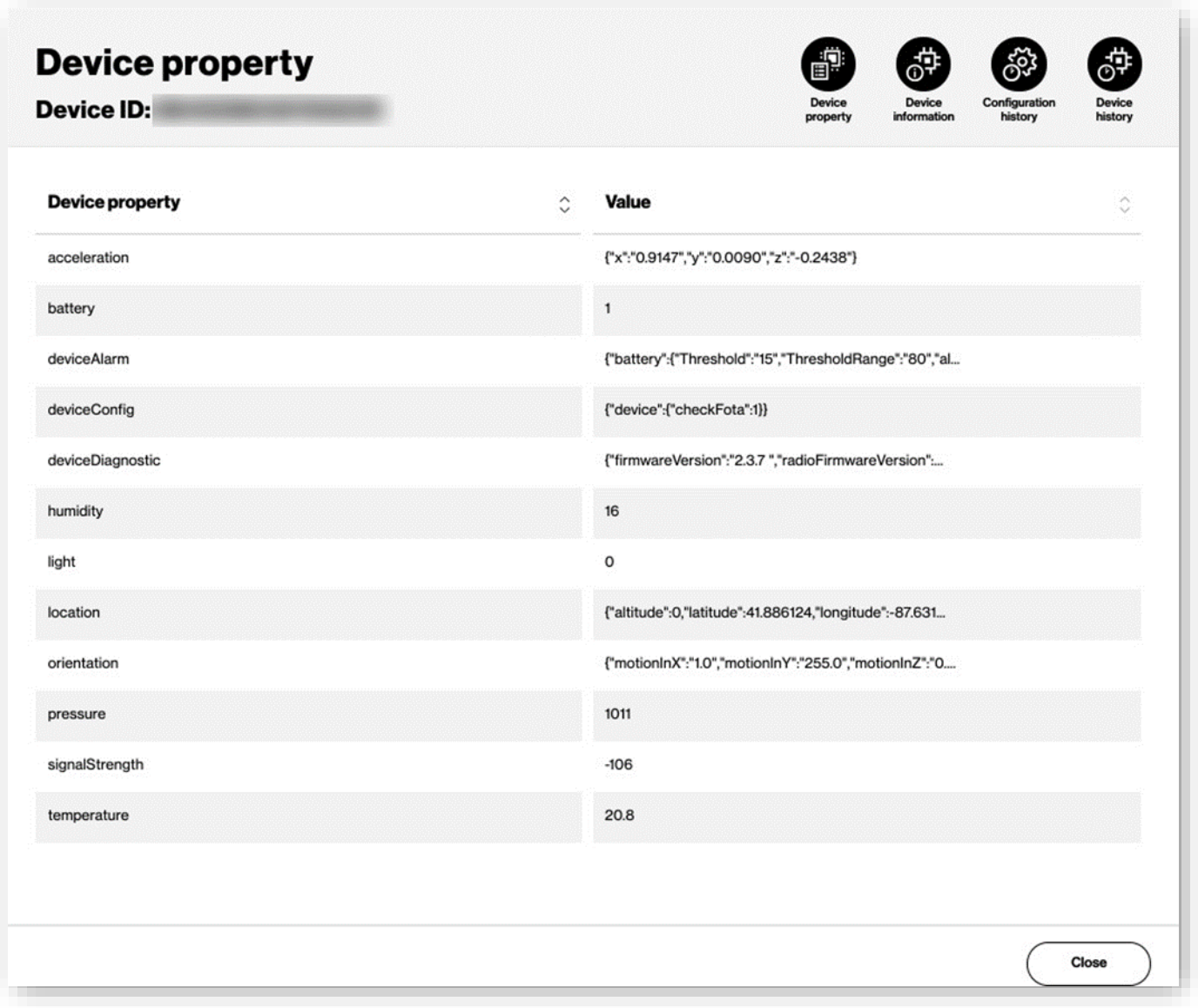
4. Click **Actions**. A dialog opens where you can change *Frequency* and *Location mode* settings.




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

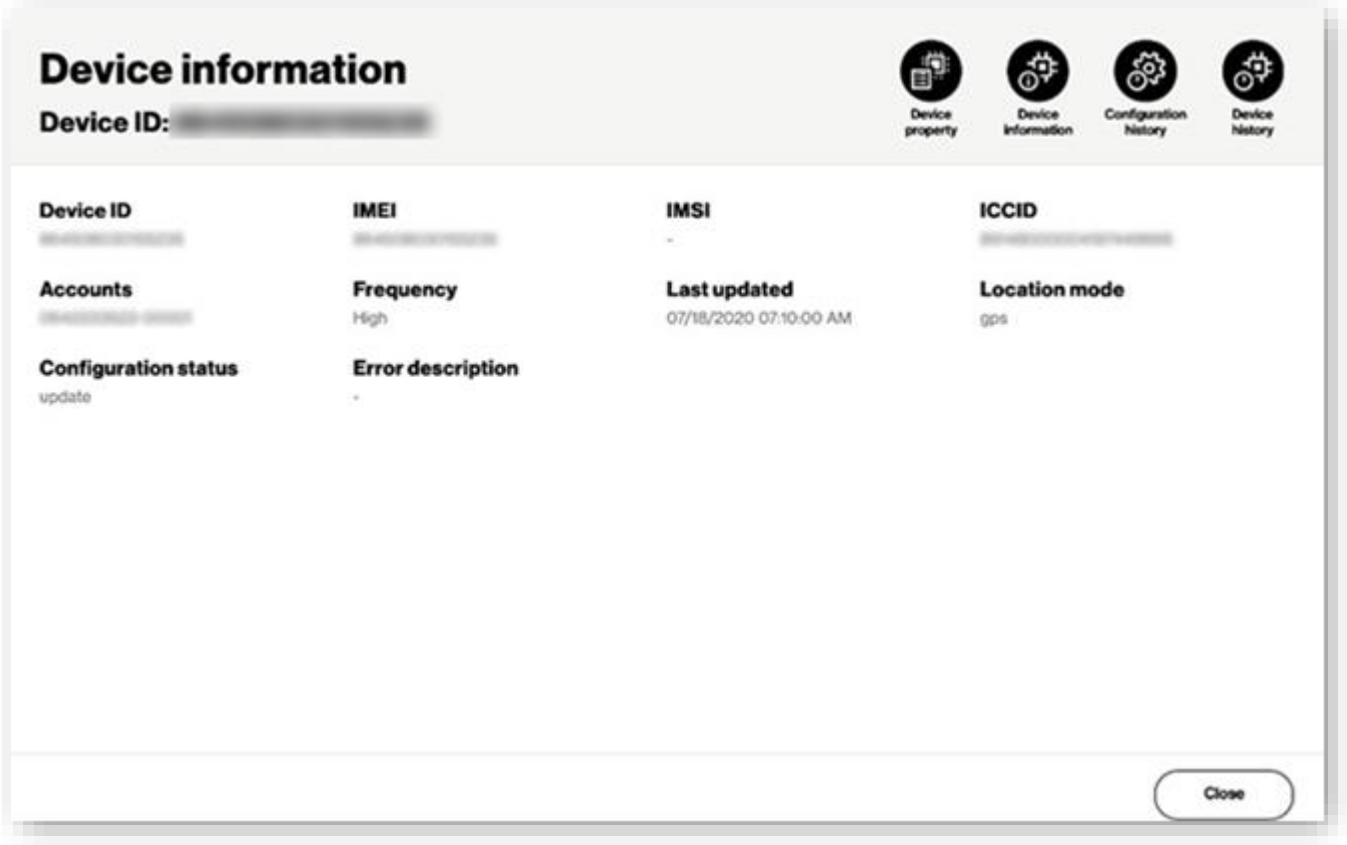
# Additional Device Information

Click a **Device ID** on the Configure devices page to open the *Device property* page.

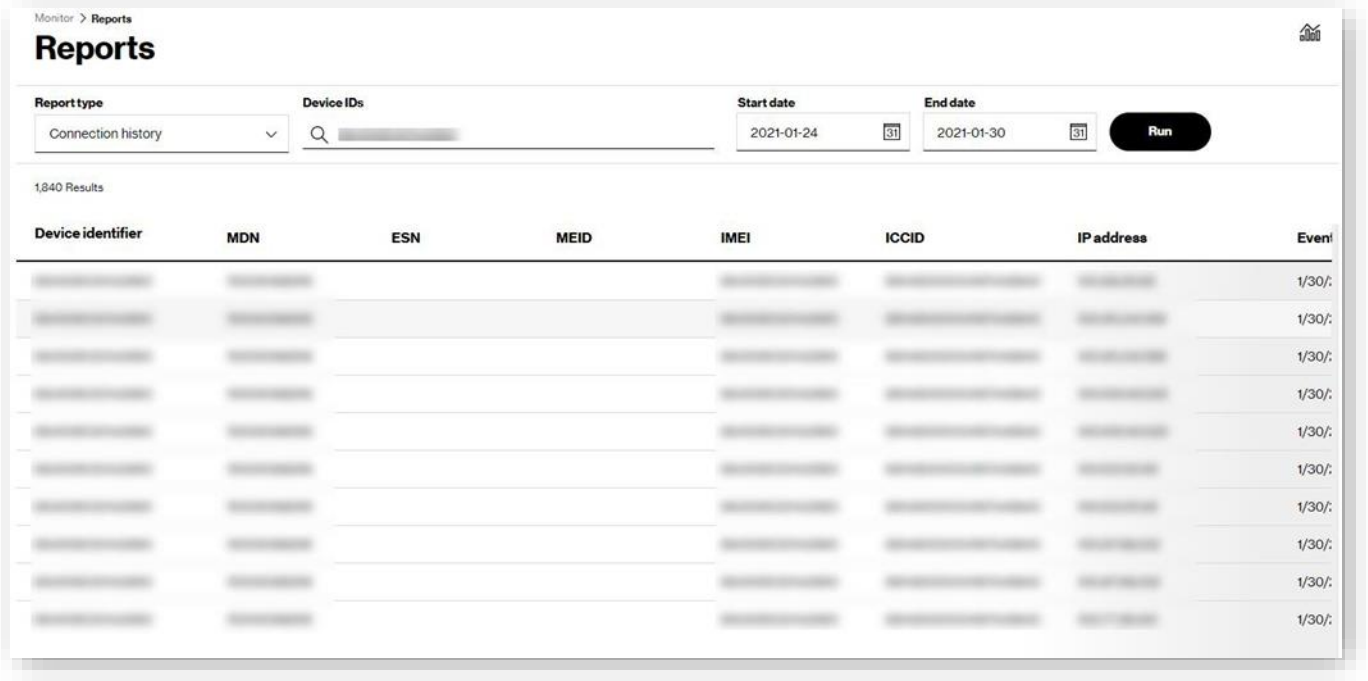



Click the icons to open the following dialogs:

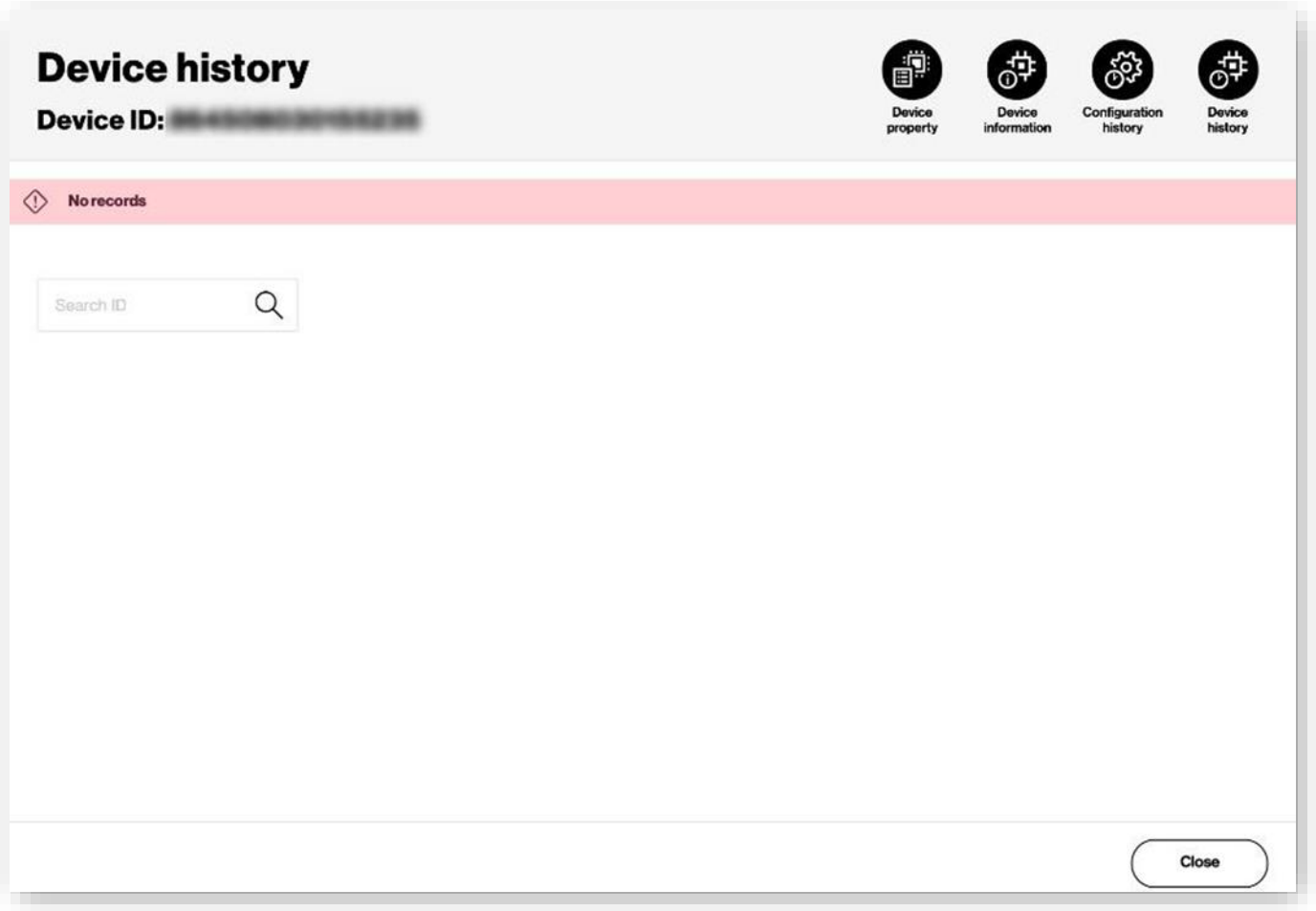
# Device information



# Configuration history

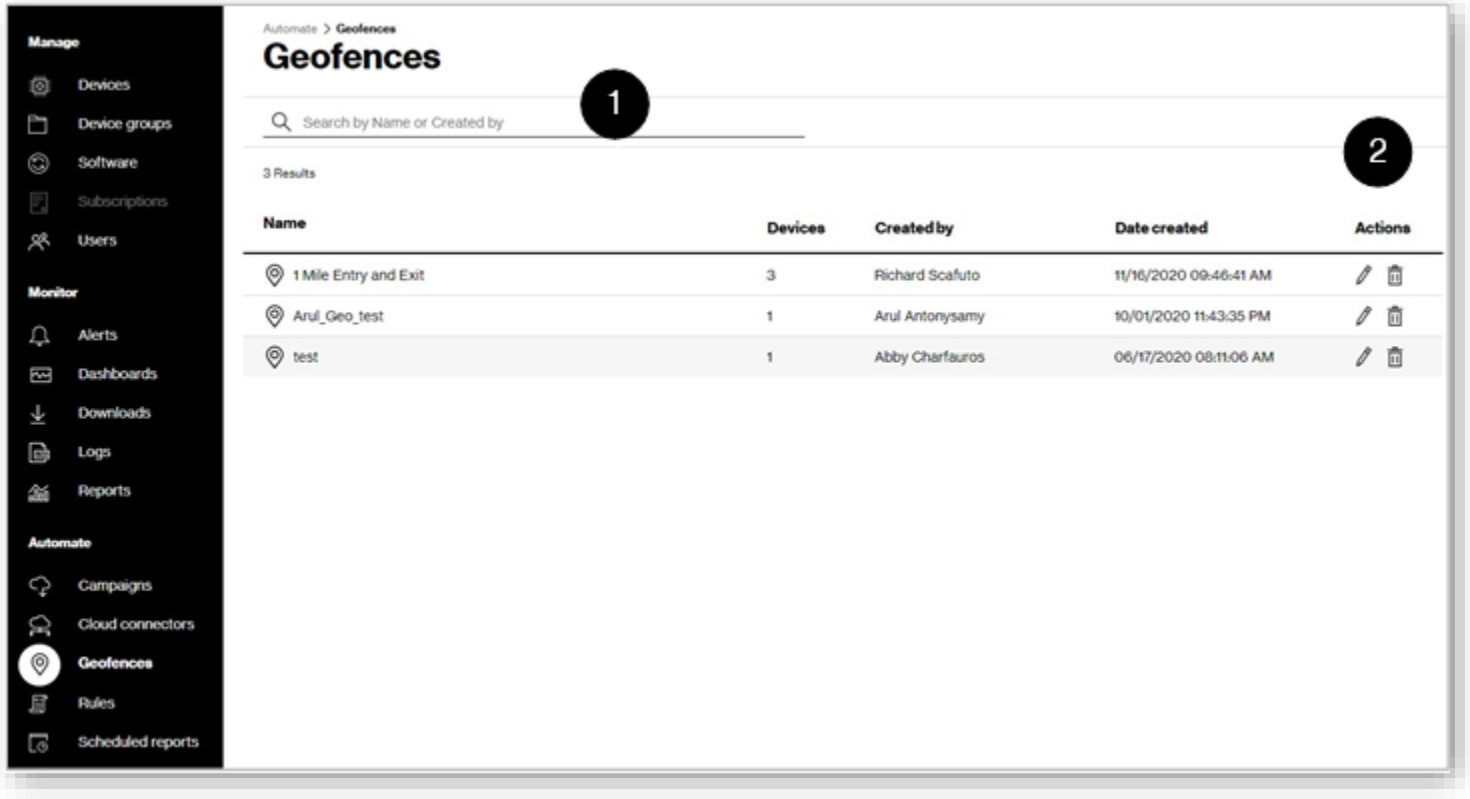


# Device history



# Geofences

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




| Elements on the Geofences page | | |
|---|---|---|
| 1 | | Search – Type a geofence name to locate a specific geofence. |
| 2 | | Edit - Open the *Edit geofence* dialog to make revisions.<br>Delete - 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

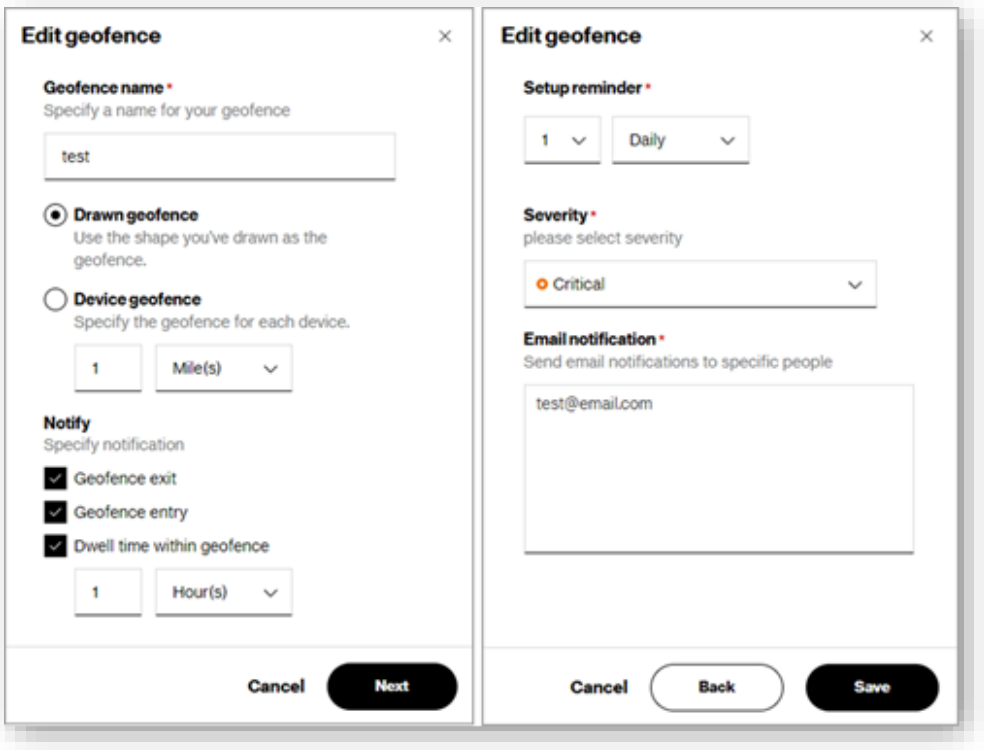
Action icons are available on each row of the *Geofences* list. To create a geofence, refer to the Creating a geofence in the *Devices* section.

# 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



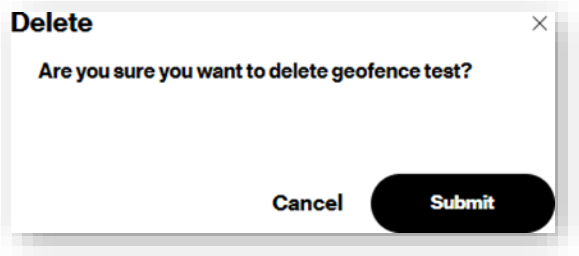

2. For **Geofence name** – a descriptive label to easily identify the geofence. For type of geofence:
   - **Drawn geofence** – A geofence that is drawn in a map.
   - **Device geofence** – A geofence that is defined for each device based on distance.
3. For **Notify**:
   - **Geofence exit** – A notification 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:

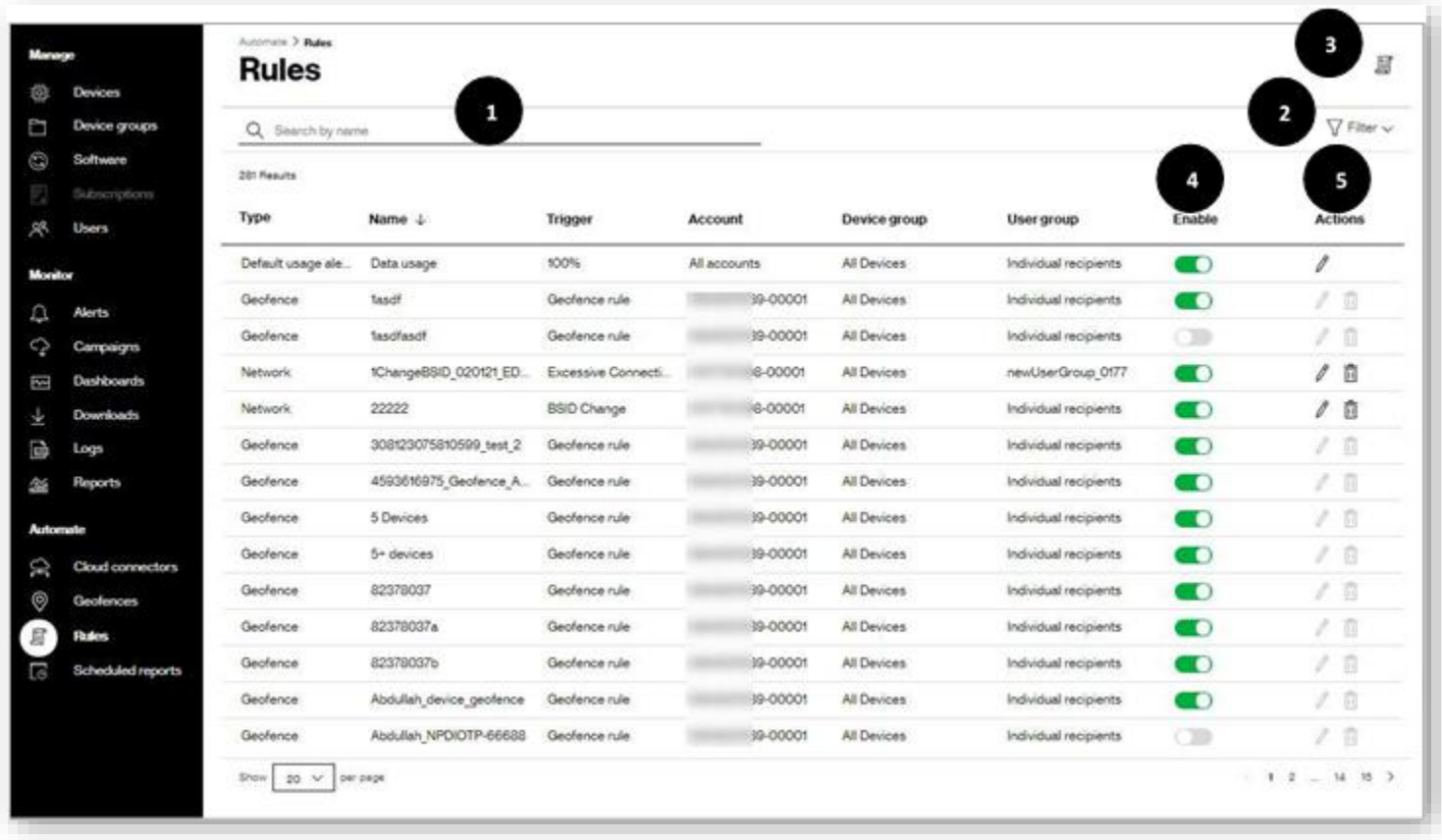
**Data usage threshold** - This type of threshold applies when M2M data passing over a network surpasses a quantity specified in kilobytes (KB) within a particular time period (daily, weekly or monthly). Accumulated usage data is an estimate, and is current to within approximately 15 minutes of the latest 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.

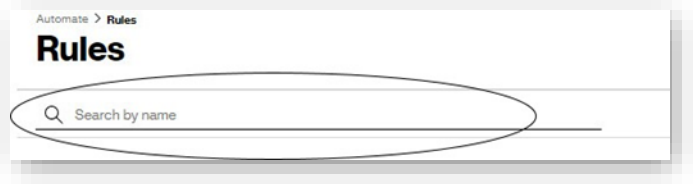
On the left navigation, click **Rules** to open the page.



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

## Searching Rules

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

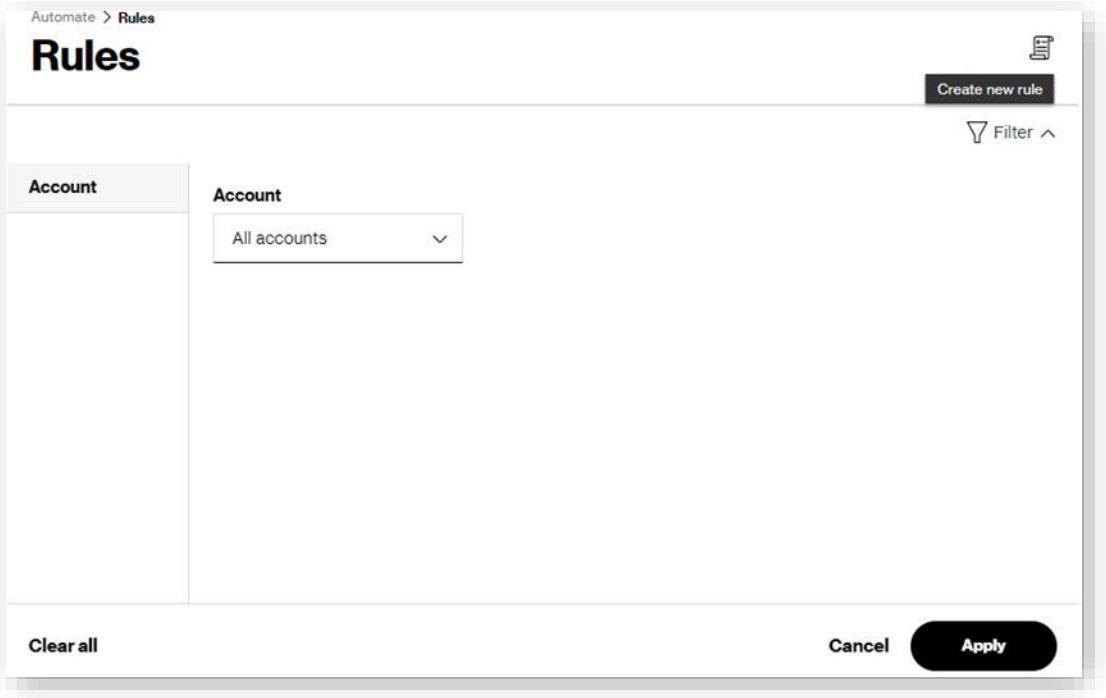



**NOTE:** Searches are not case sensitive.

## Applying Filters

How to apply filters

Click Filter . The filters page opens.

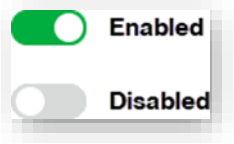



1. Select a filter from the *Account* menu.
2. Click **Apply**. A filters applied count appears.

## Enable/Disable a Rule

How to enable or disable an automation rule

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

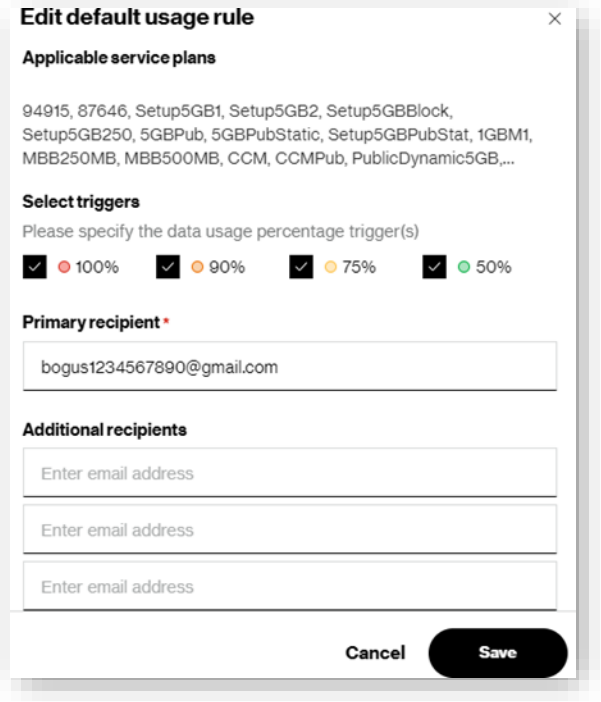



## Edit the Default Usage Alert Rule

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.



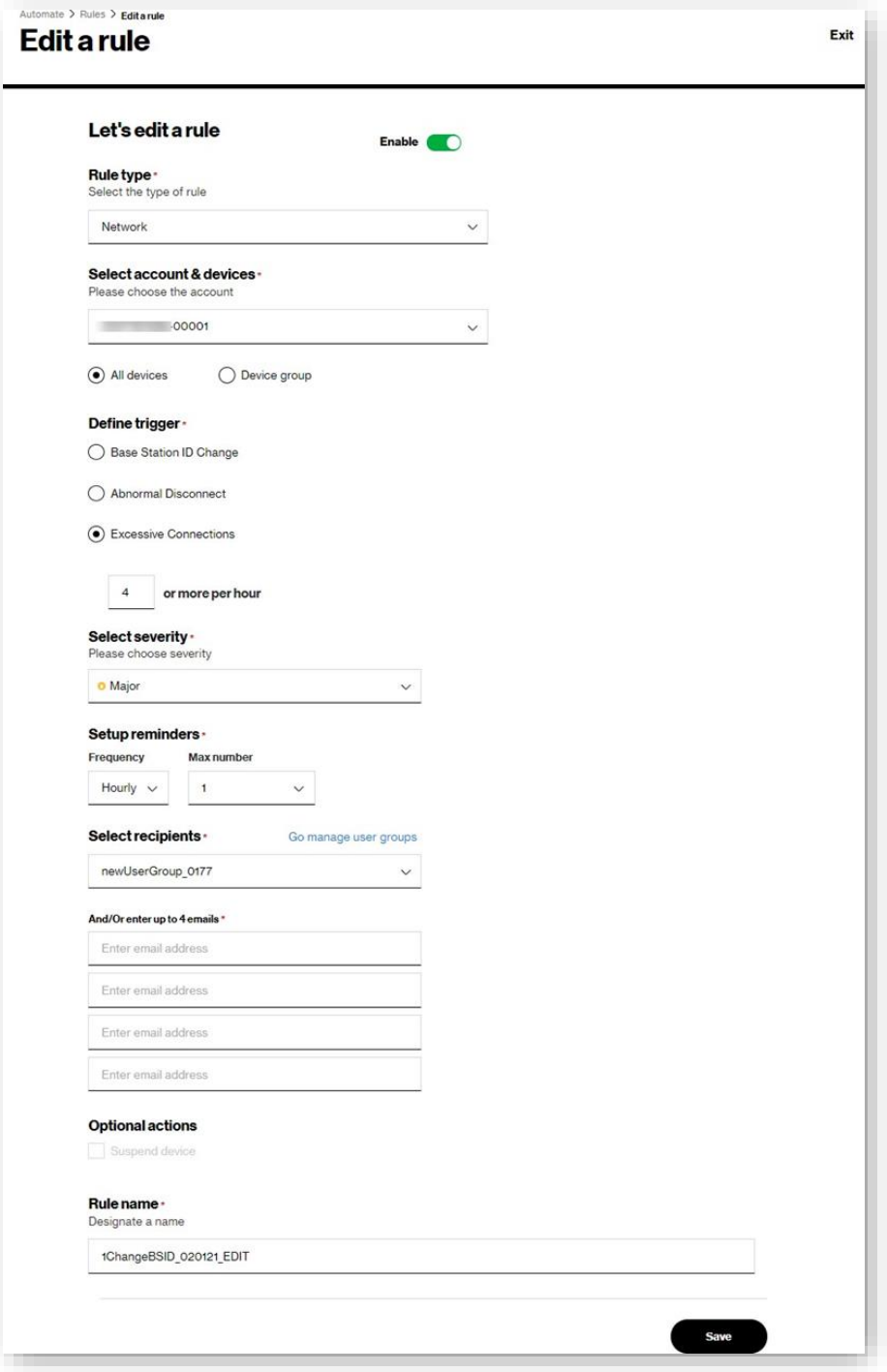

- For **Select the trigger**(s), specify to receive an alert email when your usage reaches 50%, 75%, 90% and 100%.
- For **Primary recipient**, type the email address to send the alert.
- For **Additional recipients**, type the auxiliary email addresses to send the alert.

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.



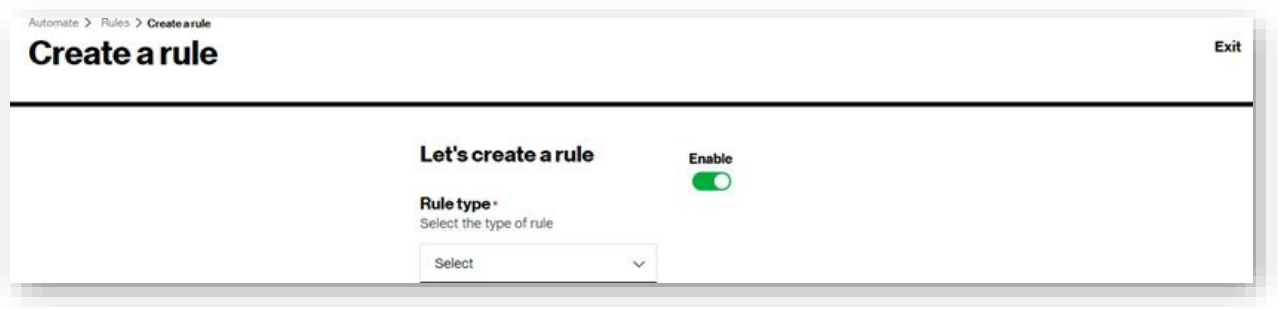
1. Choose the **Rule type**.
2. Select an account & devices.
3. Define a trigger.
4. Select a severity.
5. Setup Reminders.
6. Select Recipients.
7. Enter other recipients.
8. Select optional actions.
9. Provide a rule name.
10. Click **Save**.

# 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.

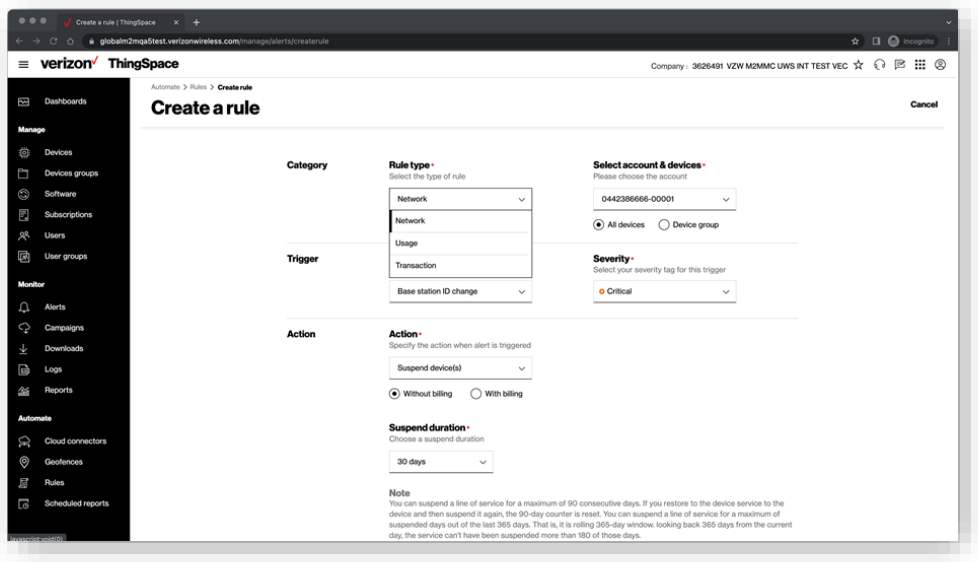
**NOTE:** You cannot change the timing of the daily, weekly, and monthly checks.

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

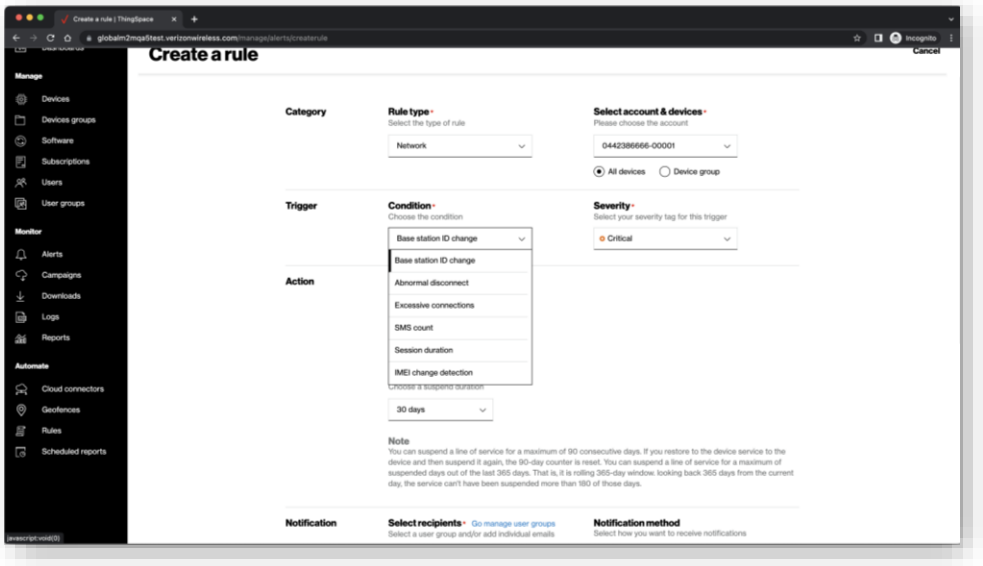
Rule Engine 2.0 allows a user to set rules for devices across their account or rules for individual devices based on data usage, network connection or transactions. These rules can suspend a device, for all devices in the account or just send an alert. When a condition is met, the account can also change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

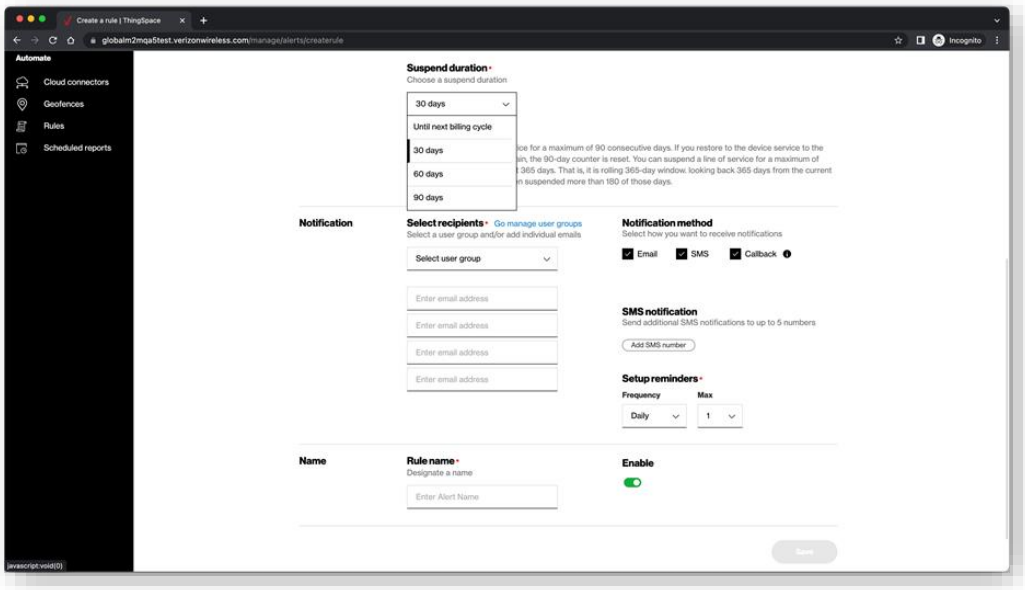
Click the rule icon . The *Create a rule* page opens. Use the drop down to select if the rule being created will be Network, Usage or Transaction:



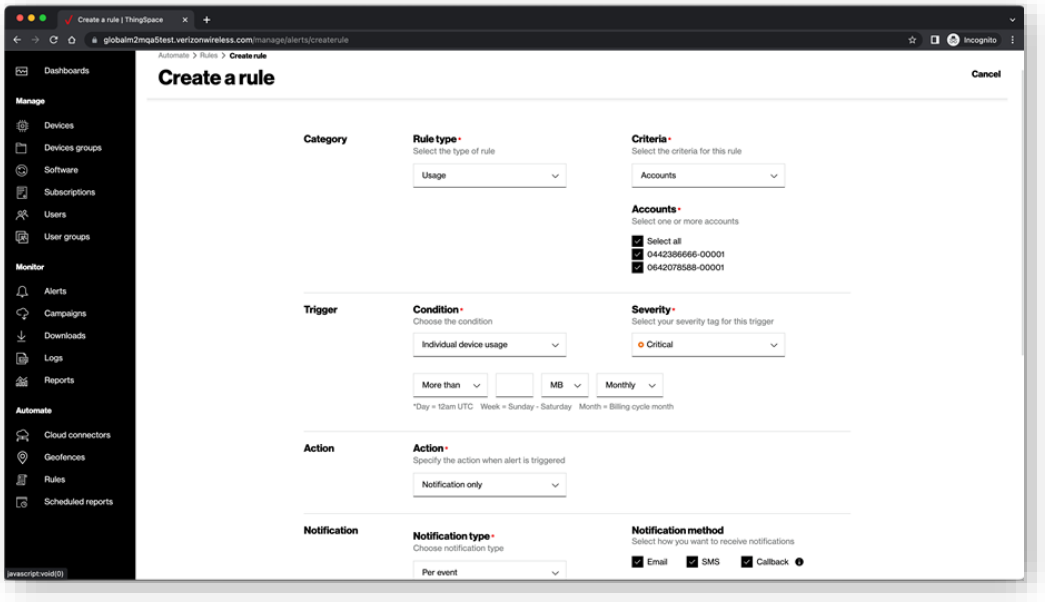
1. For the rule type selected, choose the condition being monitored:




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

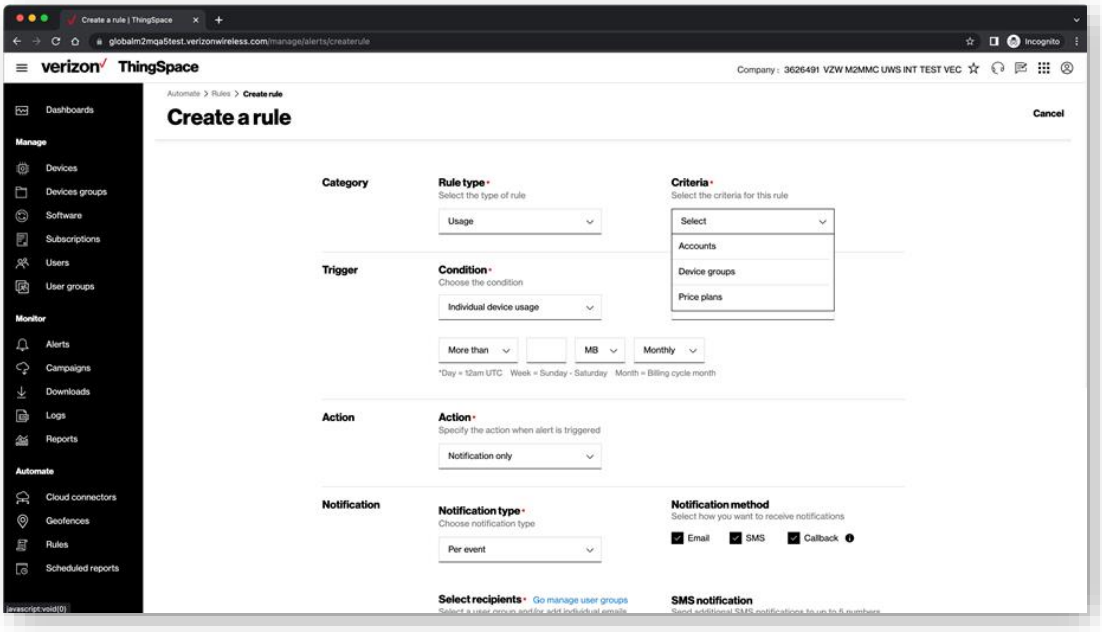


3. Before the rule is saved, the user can select how the rule sends a notification and who the notification is sent to:

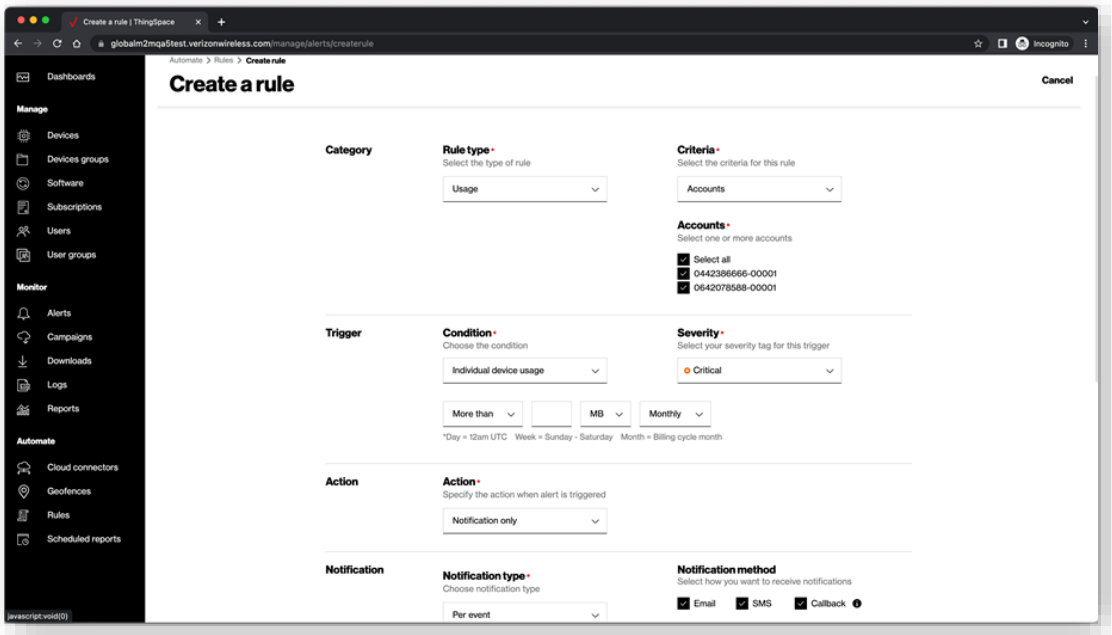


# Usage Rule Example

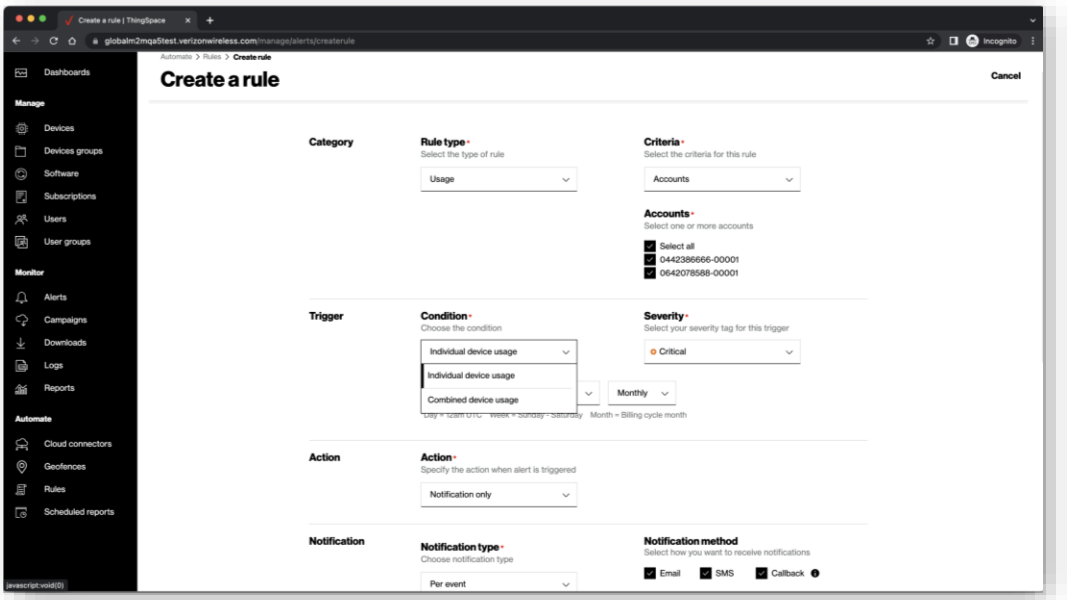
In the *Create a rule* page, by selecting rule type usage the next step is to select the criteria:



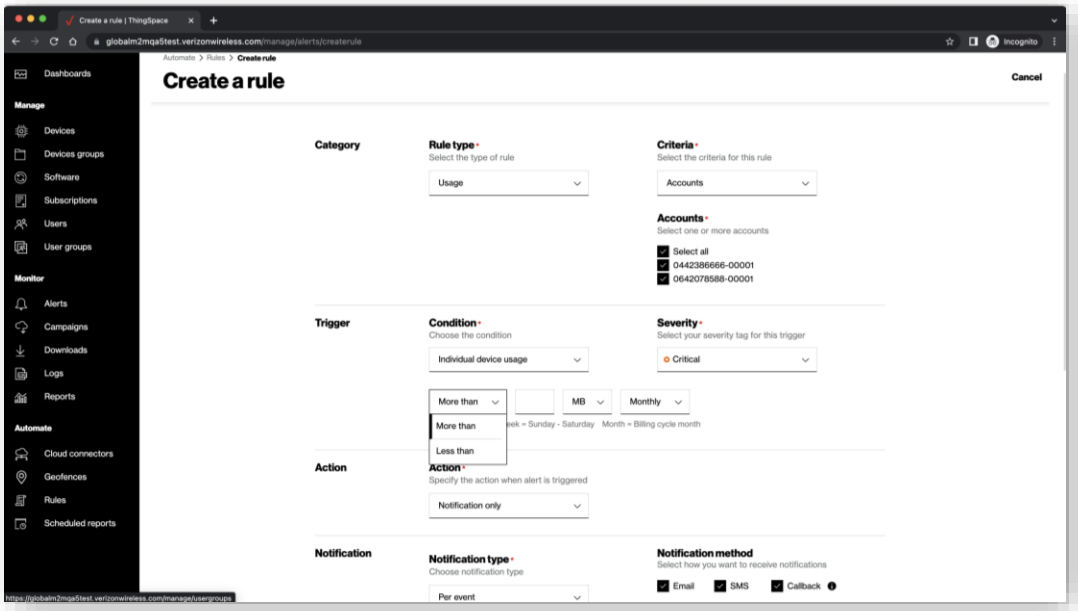

In selection of accounts, the selection of “select all” means all the accounts under the given profile the profile has access to:

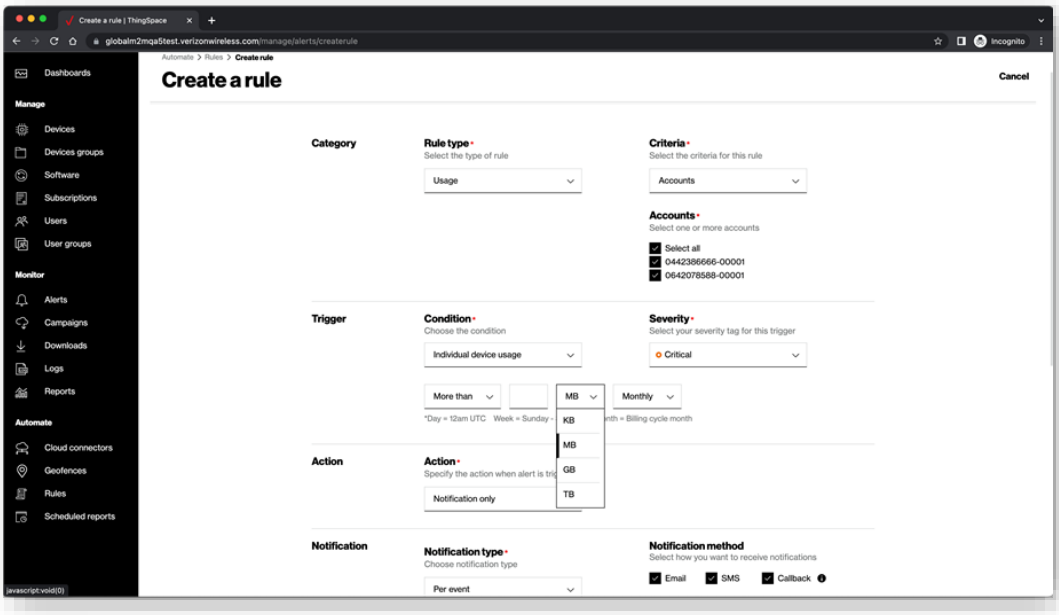


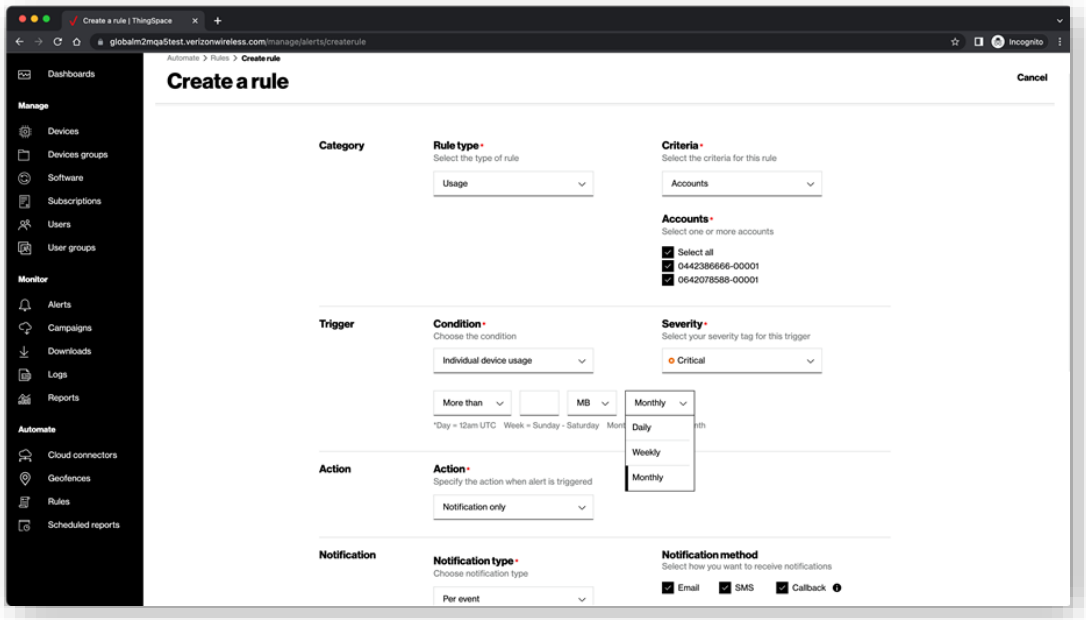
Select the trigger condition:



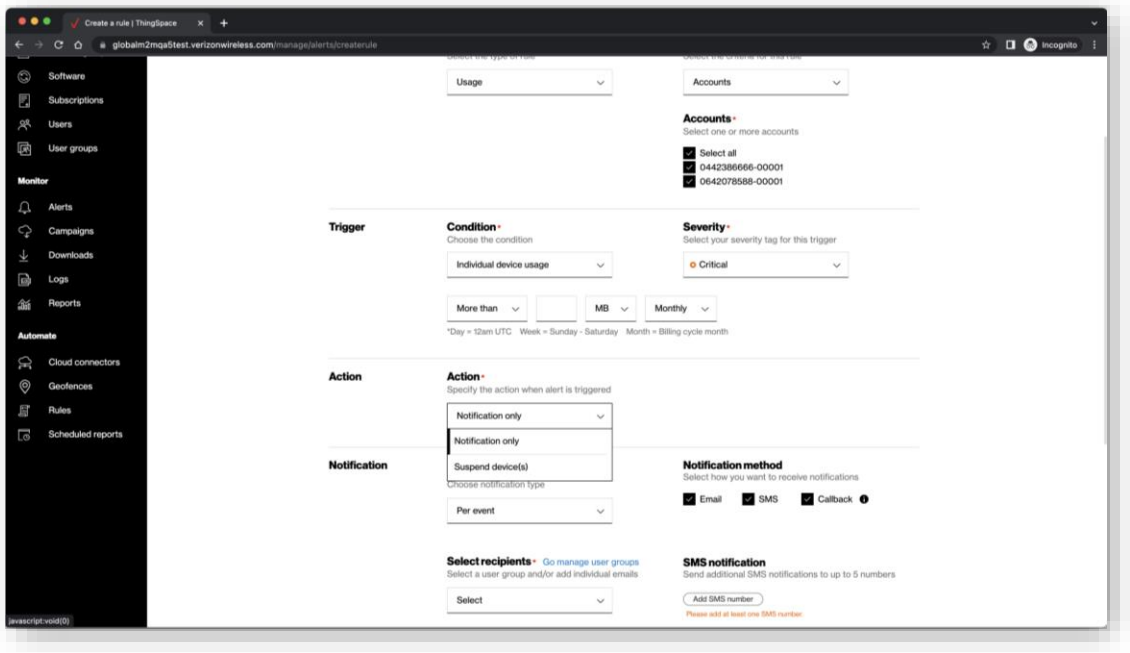

Provide the size of the trigger according to available values:



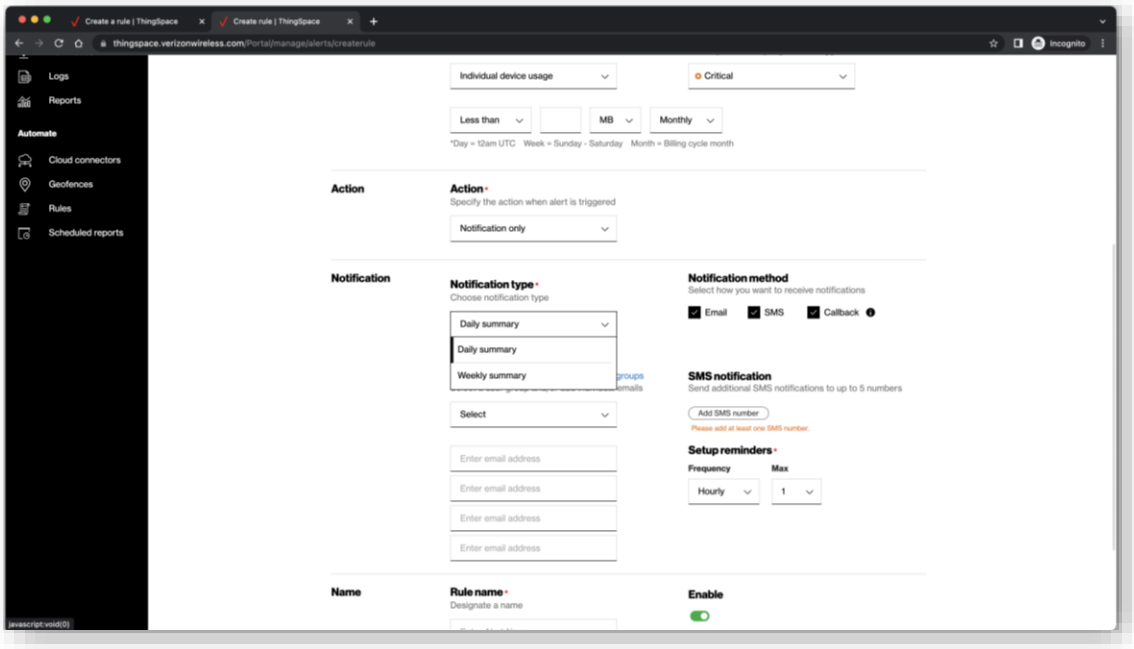

Create a rule | ThingSpace
globalm2mqa5test.verizonwireless.com/manage/alerts/createrule
Incognito
Automate > Rules > Create rule
Create a rule
Cancel
Dashboards
Manage
Devices
Devices groups
Software
Subscriptions
Users
User groups
Monitor
Alerts
Campaigns
Downloads
Logs
Reports
Automate
Cloud connectors
Geofences
Rules
Scheduled reports
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
More than
MB
Monthly
KB
MB
GB
TB
Action
Action*
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 | ThingSpace
globalm2mqa5test.verizonwireless.com/manage/alerts/createrule
Incognito
Automate > Rules > Create rule
Create a rule
Cancel
Dashboards
Manage
Devices
Devices groups
Software
Subscriptions
Users
User groups
Monitor
Alerts
Campaigns
Downloads
Logs
Reports
Automate
Cloud connectors
Geofences
Rules
Scheduled reports
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
More than
MB
Monthly
Daily
Weekly
Monthly
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

Select the action to take:

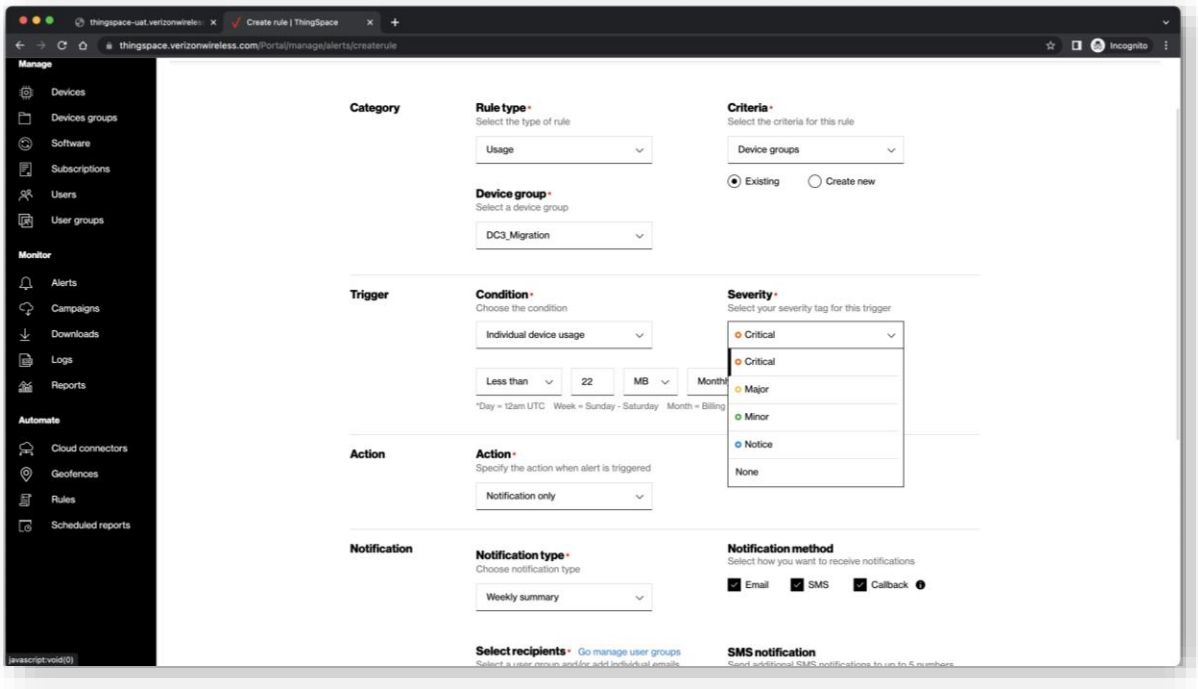



And select the notification type and frequency:

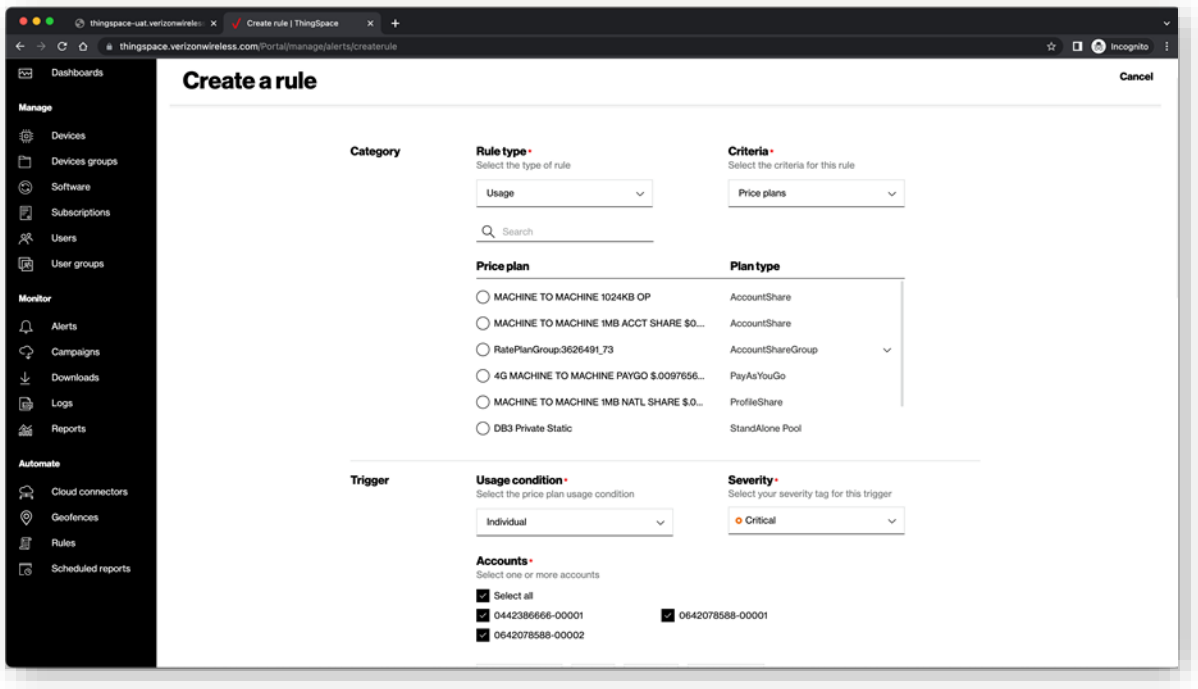



**Note:** If the user chooses to use a callback notification, then they need to subscribe to the callback prior to using the rule.

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




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):



# 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 poll 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)

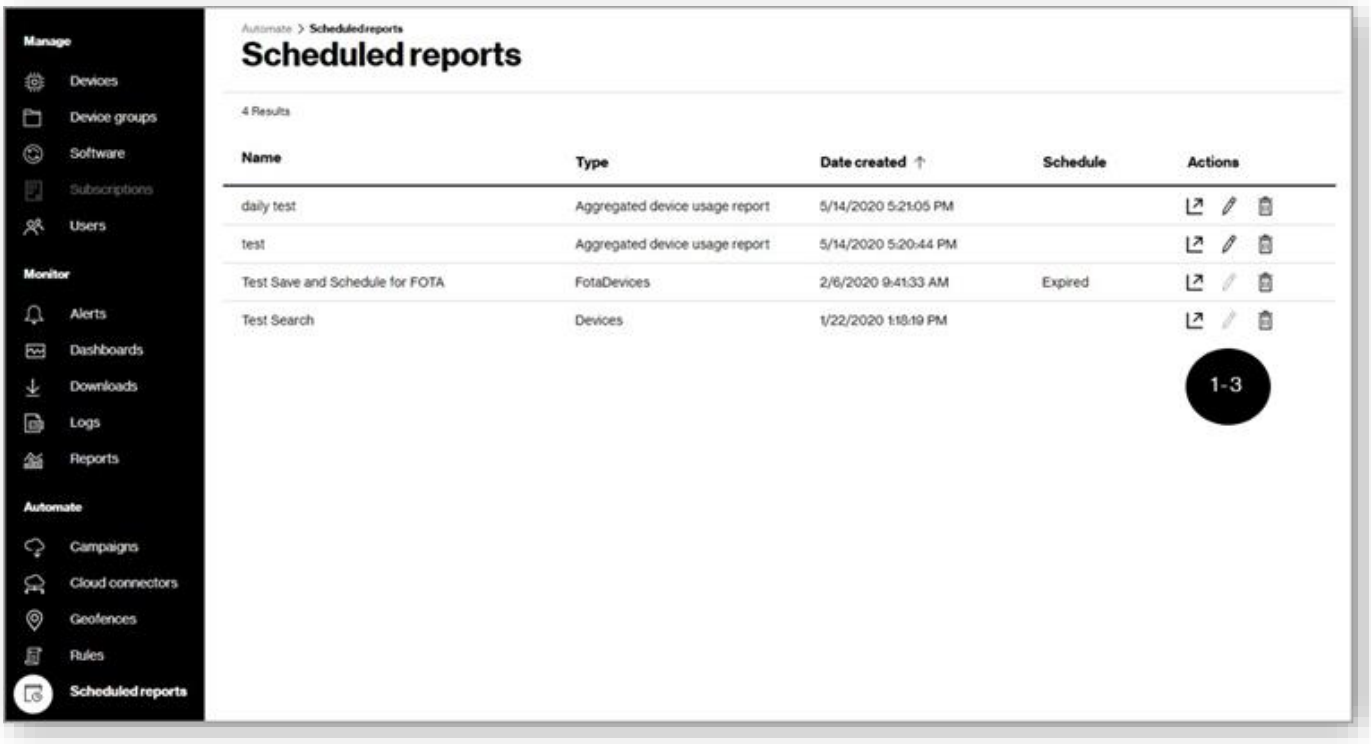
        **Note:** Suspend can be set to auto-resume at the next bill cycle or in 30, 60 or 90 days. The action selected also has a severity value associated.
5. Select the recipients of the notification (user group or individual) and the method:
    a. Email
    b. SMS (text message)
    c. Callback
6. Name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



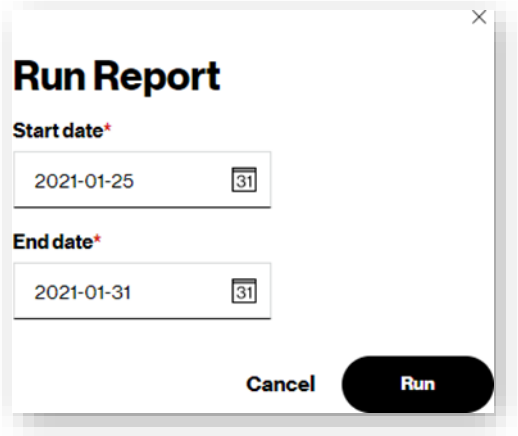

| Elements on the Rules page | | |
|---|---|---|
| 1 | | Run - Initiate the report manually. |
| 2 | | Edit - Open the *Edit a Scheduled Report* page to revise the schedule. |
| 3 | | Delete – Permanently remove a scheduled report. |

# 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.




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

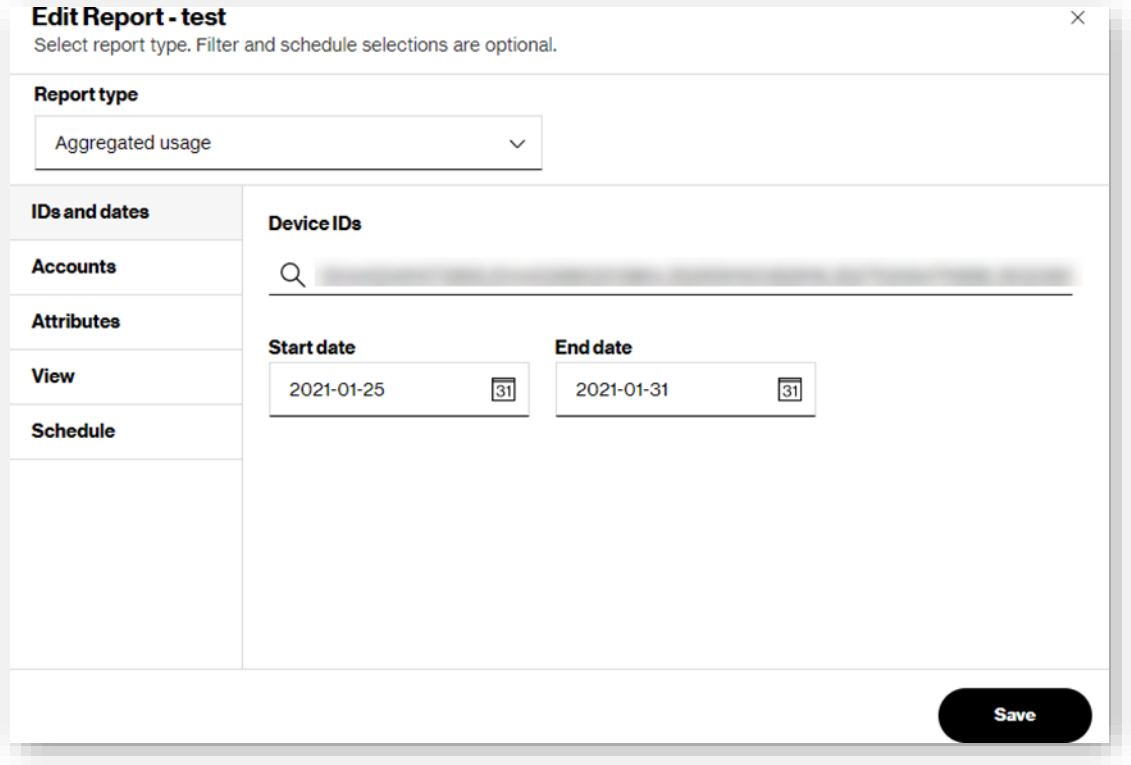
Your report is sent for processing and available on the Downloads page when processing is complete and the system sends you an email notification when the report is available.

# 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.



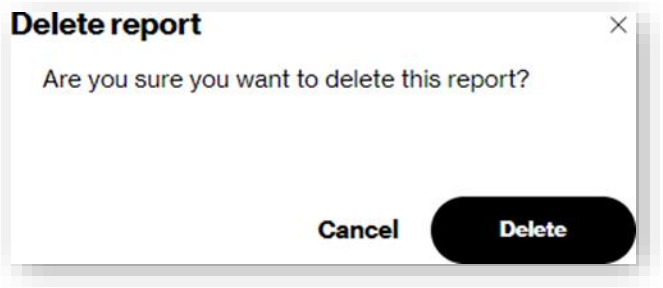

2. Choose the **Report type**.
3. Click on any of the tabs on the left side of the page to scroll to the relevant section. Update any of the selection criteria.
   - Update your table **View**.
   - Update the **Schedule**.
4. If the report is not scheduled to run at a later time, Click **Save**.
5. 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 | 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:<br>**MCC** – Mobile Country Code (311)<br>**MNC** – Mobile Network Code (480)<br>**MSIN** – Mobile Subscription Identification Number, a unique number for the subscriber on the Verizon network. |
| 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].<br>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.<br>Values can be of 0-6 and this value represents current status of the battery listed as below:<br>**0**: Normal<br>**1**: Charging<br>**2**: Charge Complete<br>**3**: Damaged<br>**4**: Low Battery<br>**5**: Battery is not installed.<br>**6**: 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 (**eDRX**) 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 | The network bearer used for the current LWM2M communication session from the following network bearer list:<br>**0~20** are Cellular Bearers<br>**0**: GSM cellular network<br>**1**: TD-SCDMA cellular network<br>**2**: WCDMA cellular network<br>**3**: CDMA2000 cellular network<br>**4**: WiMAX cellular network<br>**5**: LTE-TDD cellular network<br>**6**: LTE-FDD cellular network<br>**7~20**: Reserved for other type cellular network.<br>**21~40** are Wireless Bearers.<br>**21**: WLAN network<br>**22**: Bluetooth network<br>**23**: IEEE 802.15.4 network<br>**24~40**: Reserved for other type local wireless network.<br>**41~50** are Wireline Bearers. |

| Column Name | Definition |
|---|---|
| Network bearer (continued) | **41**: Ethernet<br>**42**: DSL<br>**43**: PLC<br>**44~50**: reserved for others type wireline networks. |
| 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 eDRX and PSM. |
| Power sources | **1**: DC power<br>**2**: Internal Battery<br>**3**: External Battery<br>**4**: Power over Ethernet<br>**5**: USB<br>**6**: AC (Mains) power<br>**7**: Solar<br>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). |
| PSM timer | This is the only time period in a PSM cycle when UE responds to Verizon LTE network's downlink paging.<br>Power save mode (PSM) timer as defined in [3GPP-TS_23.682].<br>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. |

| Column Name | Definition |
|---|---|
| Radio signal strength | Represents the entire received power including noise.<br>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&64) 0 is < 110dBm, 64 is >-48 dBm).<br>Excellent=-65 Good=-65 to -75<br>Fair=-75 to -85<br>Poor=<-85 |
| 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. *Active* implies billing, *Deactive* implies not billing, and *Suspended* is usually suspended (up to 90 days) without billing. |

| Term Used | Definition |
|---|---|
| Connection | Connected or Not Connected. *Connected* indicates an Active Data Session over the wireless network; *Not Connected* 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. |

| Term Used | Definition |
|---|---|
| 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. |
| MyCustom Field 1 | Your alphanumeric data. Available only in ThingSpace. |
| MyCustom Field 2 | Your alphanumeric data. Available only in ThingSpace. |
| MyCustom Field 3 | Your alphanumeric data. Available only in ThingSpace. |
| MyCustom Field 4 | Your alphanumeric data. Available only in ThingSpace. |
| MyCustom Field 5 | 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 *null*, *roaming*, or *not roaming*. |
| 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 course location request. |
| Last location update | Last successful course location request. |
| Last location update status | Last course location update status. Can be *null*, *failed*, or *successful*. |
| Location update frequency | If set to auto update coarse location, this is the setting in seconds. |
| Location update note | Can be *null*, *Device is Unreachable*, or *Specified device category is not IoT*. |

## 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" https://thingspace.verizon.com/documentation/apis/software-management/getting-started.html. |
| 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 *Subscription* or blank. |
| FOTA make | The make of the device, as reported by FOTA server. Options are *Subscription* 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 | *Not compliant* indicates new software is available. *Compliant* indicates up to date. Retired in ThingSpace 2.0. Implicit based on whether or not *New software* 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 Current Software) 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. |