ThingSpace Manage

User Guide

v2.0

As of 12/24/2024

Verizon Customer Support 1-800-922-0204, option 5

Important—Please Read

Verizon Confidential & Proprietary.

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 warrantee 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.

Contents

Welcome to ThingSpace

ThingSpace Manage is Verizon's portal for managing Internet of Things (IoT) and Fixed Wireless Access (FWA) 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 the complete lifecycle of 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 Connectivity to build and manage solutions easier. Verizon Connectivity reduces the complexity of attaching an IoT or Fixed Wireless Access (FWA) 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.

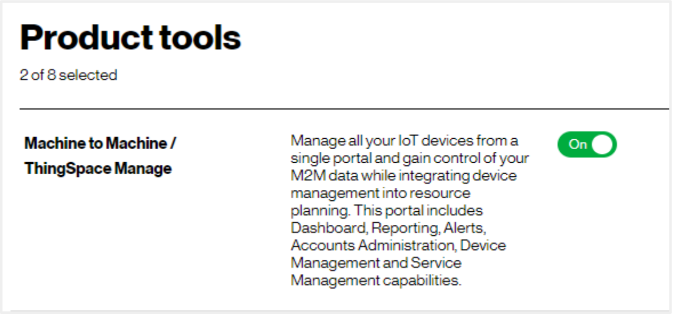
ThingSpace APIs

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 or log in through My Business. To access ThingSpace Manage, you need a My Business Account that is set up for M2M connectivity. The Machine to Machine / ThingSpace Manage option button must be "On" in your My Business profile (see below). Your account representative can set this up.



Product tools

2 of 8 selected

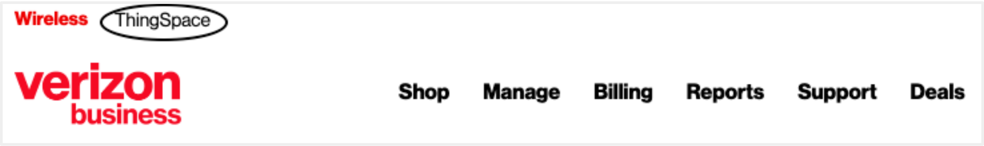
Machine to Machine / ThingSpace Manage — Manage all your IoT devices from a single portal and gain control of your M2M data while integrating device management into resource planning. This portal includes Dashboard, Reporting, Alerts, Accounts Administration, Device Management and Service Management capabilities. — On

To access ThingSpace Manage directly

1. In your browser, type in the following URL http://thingspace.verizonwireless.com/Portal/manage/.

To access ThingSpace Manage from My Business

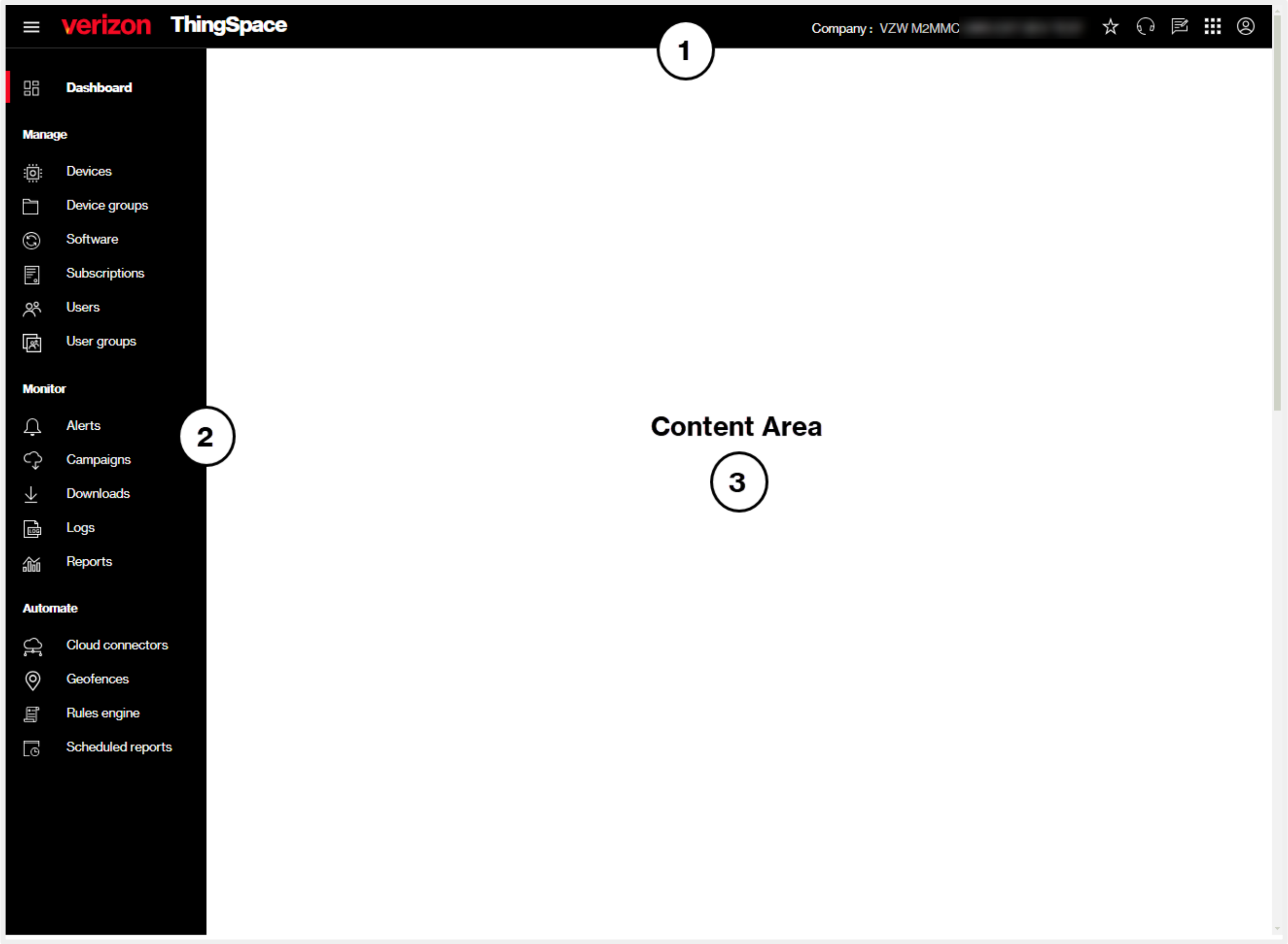
1. On the header, above the Verizon logo, there should be two links, one for **Wireless** and the other for **ThingSpace**. If you don't see the ThingSpace link, it's most likely due to your account not being setup for ThingSpace.
2. Click on the **ThingSpace** link.



3. 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 the *Dashboards* page.

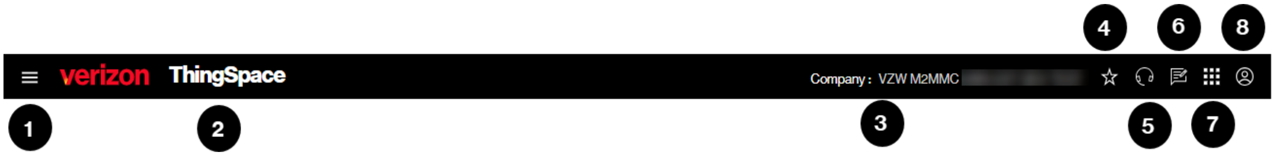
Site structure

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



Header

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



Elements on the header		
1	≡	Left Navigation – Expand or collapse the left pane with links to various application pages.
2		**ThingSpace** – Click to open the default home page.
3		**Company** – Identifies the company name of the user that is logged in.
4	☆	Favorites – Open the Favorite links menu.
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 in a new window.
8	👤	Profile – Open the Profile menu.

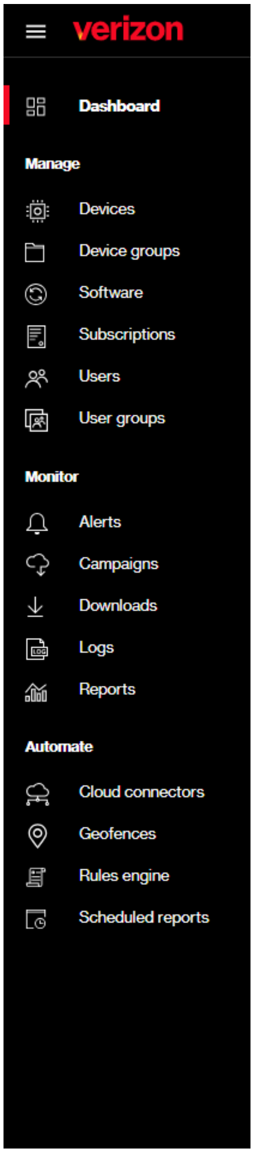
Default home page

Click the ThingSpace link in the header to open the default landing page (or home page). The default home page is the Dashboards page. The ability to set your own default home page such as the Devices page is an enhancement that is planned in the future.

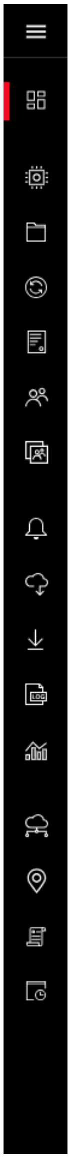
Left navigation

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

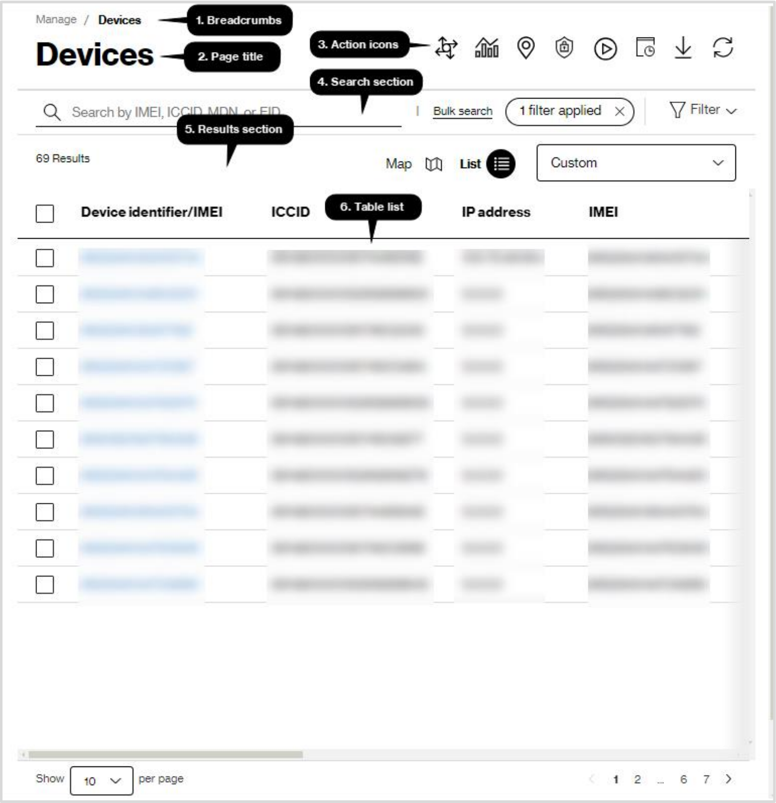


Collapsed view



Content area

The content area is the main area for the content served to the web page. Each page is different, but follows certain guidelines. Most pages' content area contains the following common features:



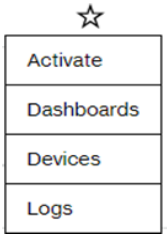
Elements on the content area	
1	**Breadcrumbs** – This is a secondary navigation that reveals the website location hierarchy. Breadcrumbs are located at the top-left of every page and provides links to preceding levels of the hierarchy.
2	**Page title** – This is the name of the page you are on and is found just beneath the Breadcrumbs links.
3	Action icons – These are icons that provide various actions that are available for each page. Action icons are located to the far right of the page title.
4	Search section – This section contains a search bar, filter icon, and may contain other links. This section is just below the page title.
5	Results section – This section contains the results of any searches or filters applied to the table list that is below it.
6	Table list – This table lists information pertinent to the page. The list can be filtered and sorted to find what you are looking for.

Action icons

Action icons are displayed on the top right side of the header and are available for all pages. 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.

Favorites

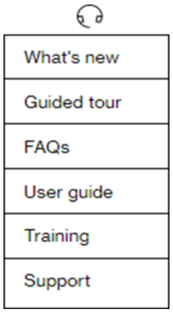
The favorites icon ☆ displays a menu containing links to your most used functions. Set your favorite links in Settings. Currently, these links are preset, but will be customizable in the future.



Support options

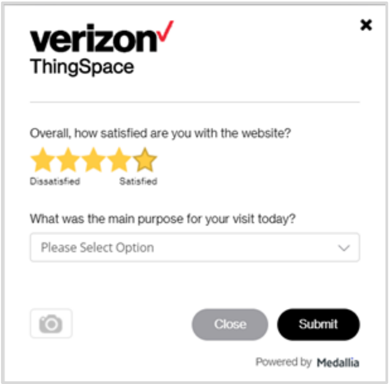
The support icon 🎧 displays a menu containing links to:

- Learn what is new or changed in ThingSpace Manage.
- Take a guided video tour of the ThingSpace experience.
- Review Frequently Asked Questions.
- View or download this user guide.
- Access the training materials such as video tutorials.
- View how to get support.



Providing feedback

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



verizon✓
ThingSpace

Overall, how satisfied are you with the website?

★★★★★

Dissatisfied Satisfied

What was the main purpose for your visit today?

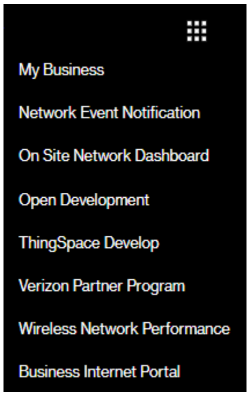
Please Select Option

Close Submit

Powered by Medallia

Verizon applications

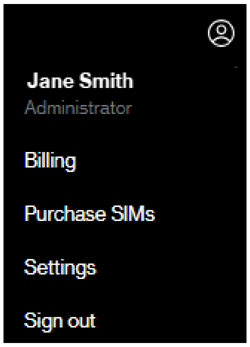
Click the Verizon apps icon ⠿ to open other Verizon applications on a separate tab. Depending on your level of access, not all applications will be displayed.



- My Business
- Network Event Notification
- On Site Network Dashboard
- Open Development
- ThingSpace Develop
- Verizon Partner Program
- Wireless Network Performance
- Business Internet Portal

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, purchase SIMs in bulk, view user and application settings, and sign out of the portal.



Jane Smith
Administrator

- Billing
- Purchase SIMs
- Settings
- Sign out

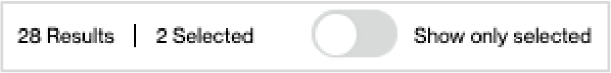
Performing searches

Pages that contain a search bar usually states the type of information that can be searched for. For example, the Devices page's search bar is used to locate device data by IMEI, ICCID, MDN, or IP address (up to 500 devices). The Users page's search bar is used to located a user by last name.

NOTE: A wildcard % can be used at the end of a search term.

Results

When a search is made or filters are applied to the information on the page, the results section displays the total number of rows returned. If any rows of the table are checked, this section also displays the total number of rows selected. Click **Show only selected** to view ONLY the selected rows and exclude the rest.



28 Results | 2 Selected Show only selected

Table list

A table lists columns of information pertinent to the page. Checkboxes on each row are to select that row so you can take an action on it. You can select one or more rows or select ALL rows on the page.

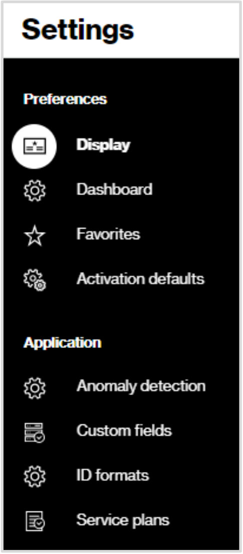
NOTE: The ability to make selections across pages is not supported.

Sorting data

You can sort data on any table/list by clicking the sort icon next to the column name. If you hover over the column name, a sort icon may appear. If one does appear, that means sort is enabled for that column. Click on the sort icons to sort in ascending ↑ or descending ↓ order.

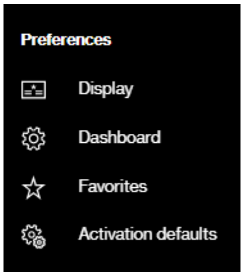
Settings

In the **User profile** menu select **Settings**. Manage user preferences and application settings here. Click the side navigation on the Settings display to access each section.



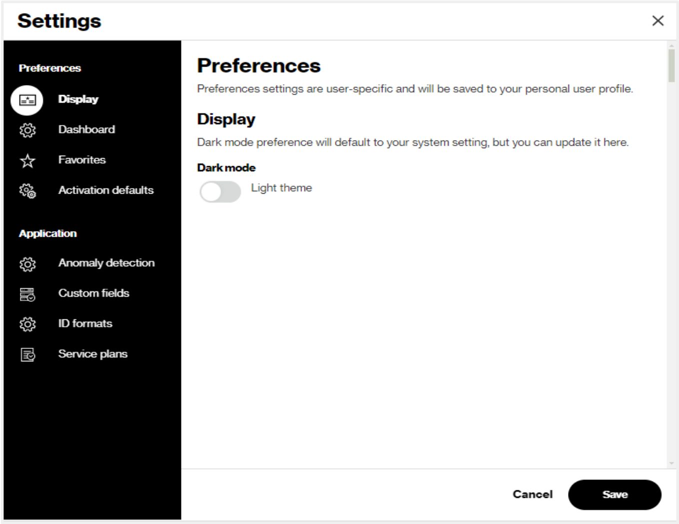
User preferences

Preferences are user-specific settings that allow you to customize the portal to your unique choices.



Display setting

The **Display** setting supports the setting of a light or dark display mode. Click on the Dark mode toggle button on for Dark mode or off for the Light theme.



Preferences

Preferences settings are user-specific and will be saved to your personal user profile.

Display

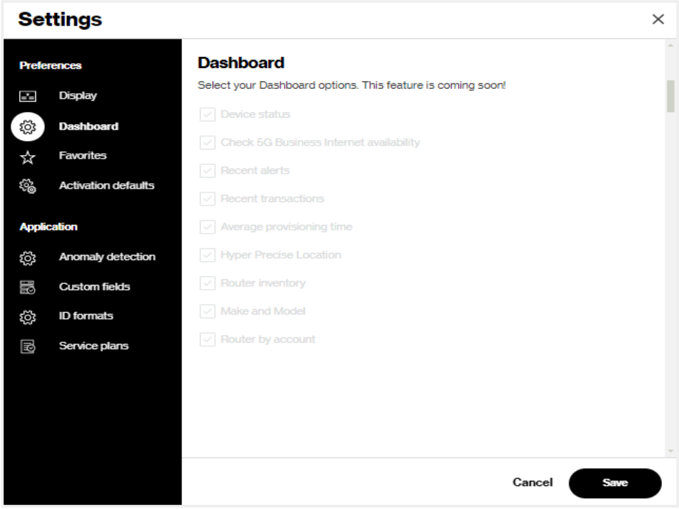
Dark mode preference will default to your system setting, but you can update it here.

Dark mode

Light theme

Dashboard settings

The **Dashboard** setting is a planned feature that will allow you to select the pods/widgets that will appear on the Dashboard.



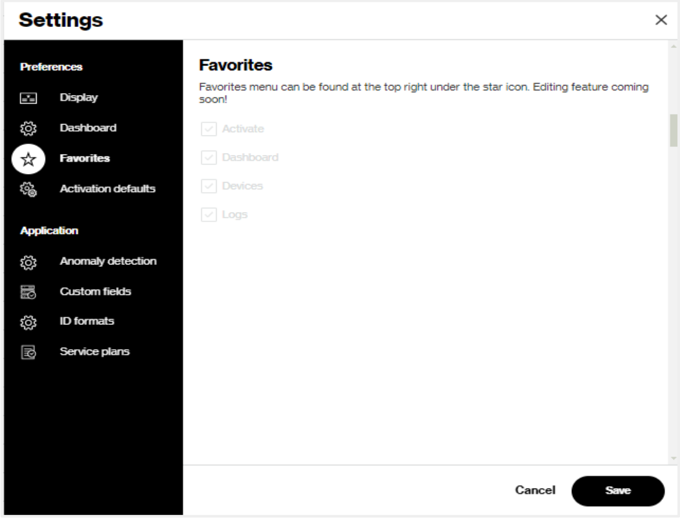
Dashboard

Select your Dashboard options. This feature is coming soon!

- ☑ Device status
- ☑ Check 5G Business Internet availability
- ☑ Recent alerts
- ☑ Recent transactions
- ☑ Average provisioning time
- ☑ Hyper Precise Location
- ☑ Router inventory
- ☑ Make and Model
- ☑ Router by account

Favorites settings

The **Favorites** setting is a planned feature that will allow you to select the menu options that appear in the Favorites menu.



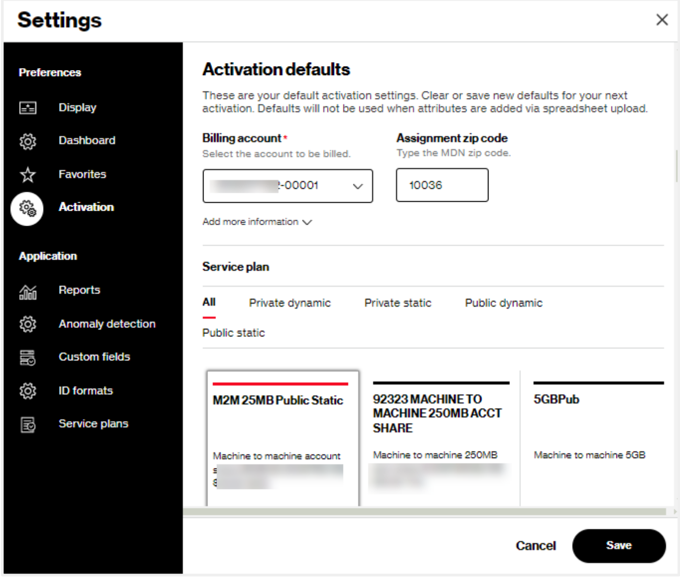
Favorites

Favorites menu can be found at the top right under the star icon. Editing feature coming soon!

- ☑ Activate
- ☑ Dashboard
- ☑ Devices
- ☑ Logs

Activation defaults settings

The **Activation defaults** setting allows you to set the default values for your device activations. You can set the default billing account, assignment zip code, and service plan. You can also set name, address, cost center, device groups, and custom fields in the **Add more information** section. You can always change the values prior to submitting the activation request.



Activation defaults

These are your default activation settings. Clear or save new defaults for your next activation. Defaults will not be used when attributes are added via spreadsheet upload.

Billing account *
Select the account to be billed.
[redacted]-00001

Assignment zip code
Type the MDN zip code.
10036

Service plan

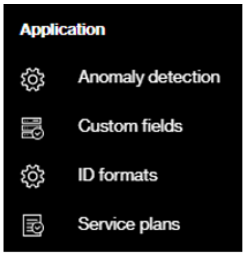
M2M 25MB Public Static
Machine to machine account [redacted]

92323 MACHINE TO MACHINE 250MB ACCT SHARE
Machine to machine 250MB [redacted]

5GBPub
Machine to machine 5GB

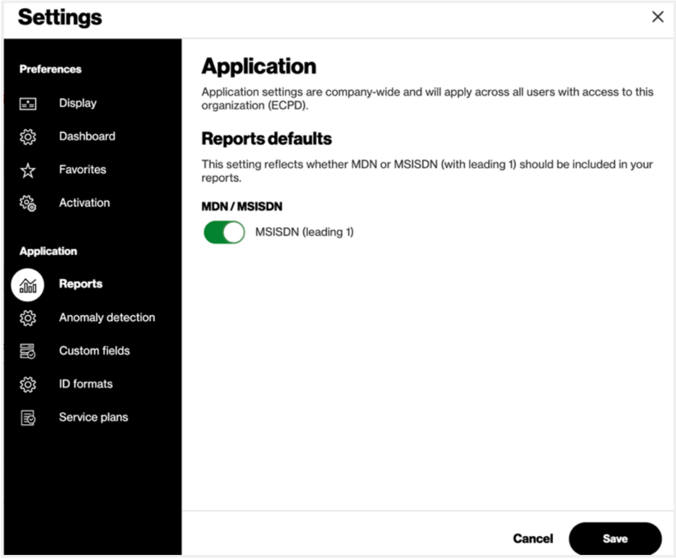
Application settings

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



Reports settings

This setting reflects whether MDN or MSISDN (with leading 1) should be included in your reports.



Application

Application settings are company-wide and will apply across all users with access to this organization (ECPD).

Reports defaults

This setting reflects whether MDN or MSISDN (with leading 1) should be included in your reports.

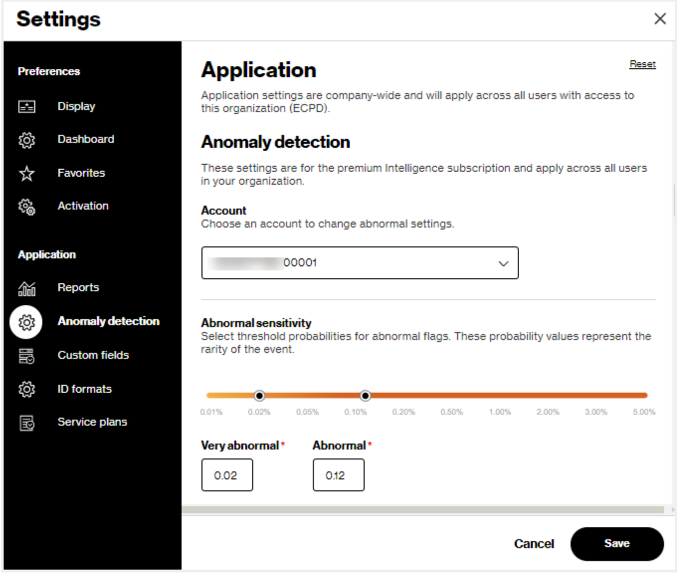
MDN / MSISDN

● MSISDN (leading 1)

Anomaly detection settings

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.



Application

Application settings are company-wide and will apply across all users with access to this organization (ECPD).

Anomaly detection

These settings are for the premium Intelligence subscription and apply across all users in your organization.

Account
Choose an account to change abnormal settings.

[redacted]00001

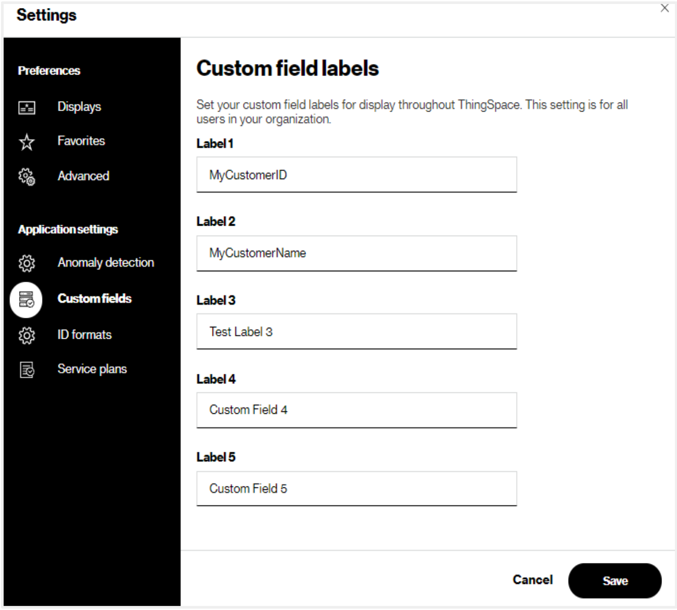
Abnormal sensitivity
Select threshold probabilities for abnormal flags. These probability values represent the rarity of the event.

Very abnormal*: 0.02

Abnormal*: 0.12

Custom fields settings

Use the Custom fields settings option 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.



Custom field labels

Set your custom field labels for display throughout ThingSpace. This setting is for all users in your organization.

Label 1: MyCustomerID

Label 2: MyCustomerName

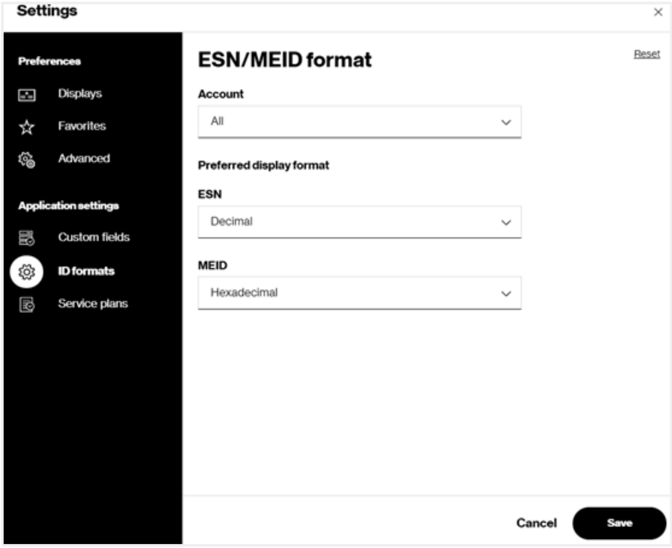
Label 3: Test Label 3

Label 4: Custom Field 4

Label 5: Custom Field 5

ID formats settings

Use the ID Formats settings 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.



ESN/MEID format

Account: All

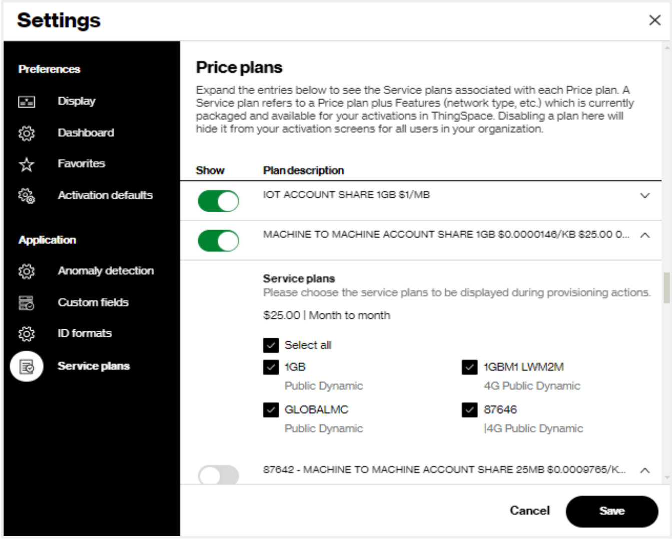
Preferred display format

ESN: Decimal

MEID: Hexadecimal

Service plans settings

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



Price plans

Expand the entries below to see the Service plans associated with each Price plan. A Service plan refers to a Price plan plus Features (network type, etc.) which is currently packaged and available for your activations in ThingSpace. Disabling a plan here will hide it from your activation screens for all users in your organization.

Show	Plan description
●	IOT ACCOUNT SHARE 1GB $1/MB
●	MACHINE TO MACHINE ACCOUNT SHARE 1GB $0.0000146/KB $25.00 0...
○	87642 - MACHINE TO MACHINE ACCOUNT SHARE 25MB $0.0009765/K...

Service plans

Please choose the service plans to be displayed during provisioning actions.

$25.00 | Month to month

☑ Select all

☑ 1GB
Public Dynamic

☑ 1GBM1 LWM2M
4G Public Dynamic

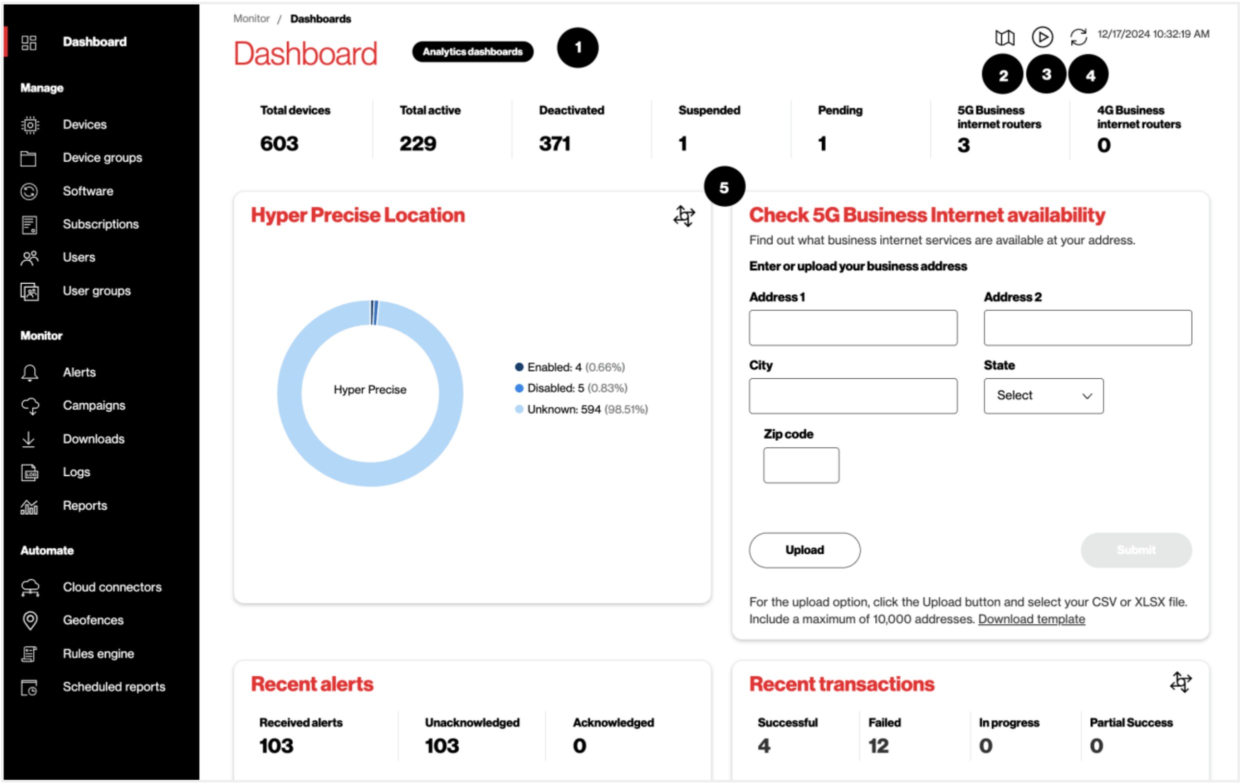
☑ GLOBALMC
Public Dynamic

☑ 87646
|4G Public Dynamic

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.

Dashboards

The Dashboards page is available from the left navigation and is set as the default home page for first-time users. The page provides a system overview, quick searches, filters, and useful navigation links. Use this page to get a snapshot of your account. There are several **pods** or **widgets** containing different types of information. Depending on your user role and level of access, you may not have visibility into all of them. Each pod will be explained in more detail.



Total devices	Total active	Deactivated	Suspended	Pending	5G Business internet routers	4G Business internet routers
603	229	371	1	1	3	0

- Enabled: 4 (0.66%)
- Disabled: 5 (0.83%)
- Unknown: 594 (98.51%)

Find out what business internet services are available at your address.

Enter or upload your business address

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 10,000 addresses. Download template

Received alerts	Unacknowledged	Acknowledged
103	103	0

Successful	Failed	In progress	Partial Success
4	12	0	0

Elements on the Dashboard page		
1		Analytics dashboards – Access the Analytics dashboards.
2	🗺	Map – View devices on a map.
3	▷	Tutorial videos – View available video tutorials.
4	↻	Refresh – Refresh the page.
5	□	Pods – Various pods/widgets based on user's role and authorization.

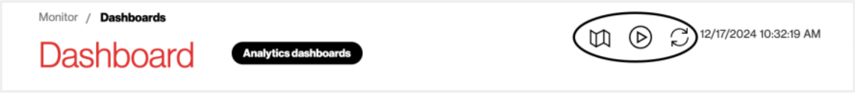
Analytics dashboards

For accounts subscribed to ThingSpace Intelligence, you will also notice an option for **Analytics dashboards** on the Dashboard page. This feature set is explained in more detail later in this user guide.

Analytics dashboards

Dashboard actions

The Dashboard features actions on the top right of the page.


Monitor / **Dashboards**

Dashboard

Analytics dashboards

12/17/2024 10:32:19 AM

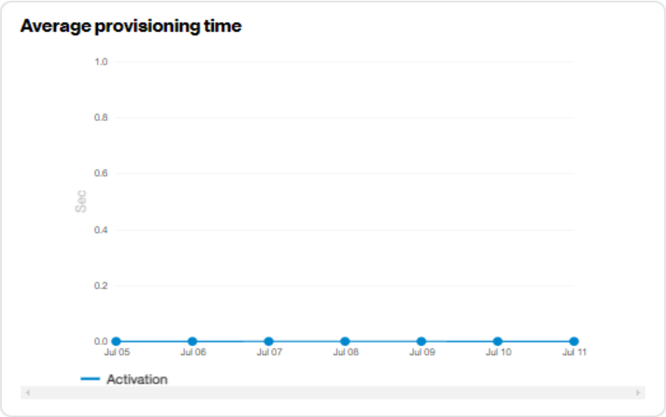
Use the map icon 🗺 if you use addresses during activation, plan changes, or set them explicitly for your devices. ThingSpace will save the address, independent of the actual location.

Use the Tutorial icon ▷ to view training videos available throughout the ThingSpace Manage portal. These videos are contextual to the page so the available videos will vary based on the context.

Click the reload icon ⟳ to refresh the page. The information in all of the pods/widgets will reload with updated content.

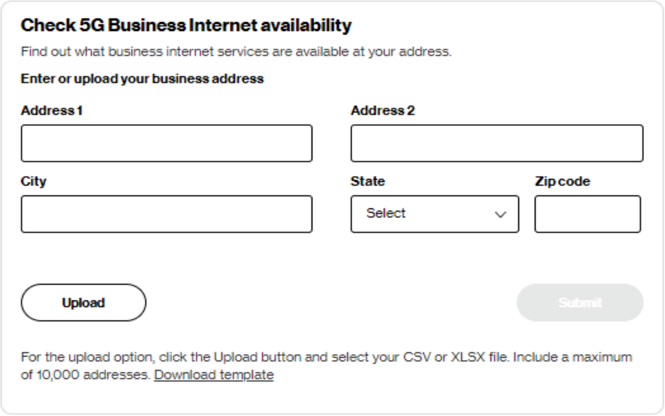
Average provisioning time pod

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). Additional transaction support is planned for a future release.



Check 5G Business Internet availability pod

For profiles with 5G Business internet plans onboarded to ThingSpace, they will notice a 5G Business Internet address qualification pod on the Dashboard. The Check 5G Business Internet availability pod allows you to enter an address and check to see if it 5G Business Internet is available in the area.



Check 5G Business Internet availability

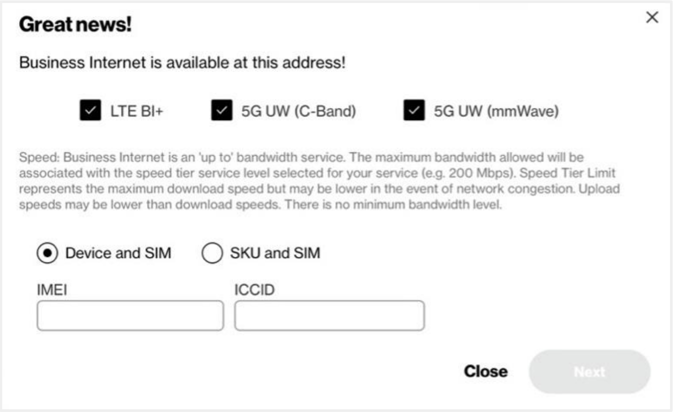
Find out what business internet services are available at your address.

Enter or upload your business address

For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 10,000 addresses. Download template

By entering a single address and selecting Submit, ThingSpace will perform a real-time address qualification to support FWA Unlimited Plans for LTE BI+, 5G UW (C-Band) and 5G UW (mmWave).

Regardless of the qualification, this pod offers you the ability to activate any plan at this address by entering IMEI+ICCID or SKU+ICCID followed by the available plans. Note that if your plan requires 5G BI, the address qualification will be done again as part of the activation process.



Great news!

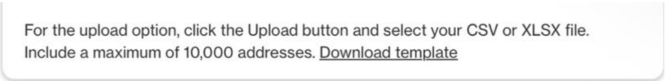
Business Internet is available at this address!

☑ LTE BI+ ☑ 5G UW (C-Band) ☑ 5G UW (mmWave)

Speed: Business Internet is an 'up to' bandwidth service. The maximum bandwidth allowed will be associated with the speed tier service level selected for your service (e.g. 200 Mbps). Speed Tier Limit represents the maximum download speed but may be lower in the event of network congestion. Upload speeds may be lower than download speeds. There is no minimum bandwidth level.

● Device and SIM ○ SKU and SIM

This address qualification screen also allows you to qualify in bulk for 5G UW (C-Band) only. Download the template, enter your addresses and select Upload. The report will be made available on the downloads page.

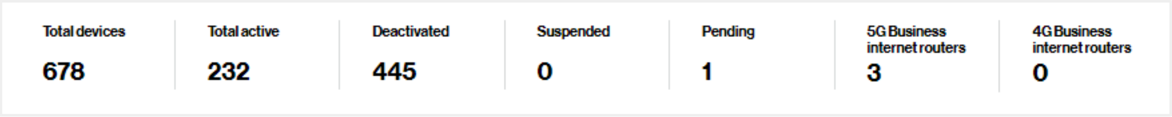


For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 10,000 addresses. Download template

Device counts pod

The Device counts pod show the total devices on a company's account along with the total active, deactive, suspended, and pending. It also shows the number of 5G and4G Business Internet routers on the account.

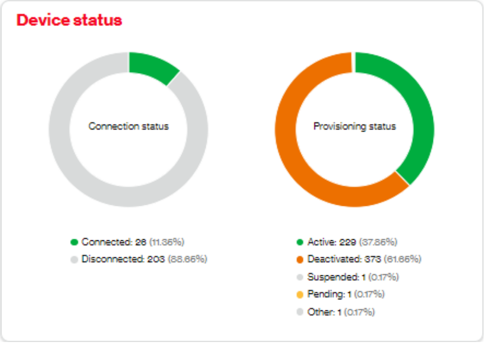
Each number is a filter. Click one of the numbers to open the Devices page with devices corresponding to the selected filter. For example, click **Total active** to open the *Devices* page filtered by all devices with an active status.



Total devices	Total active	Deactivated	Suspended	Pending	5G Business internet routers	4G Business internet routers
678	232	445	0	1	3	0

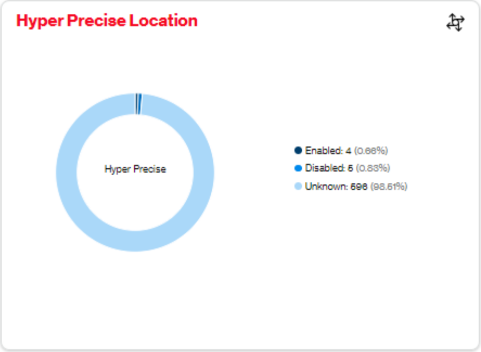
Device status pod

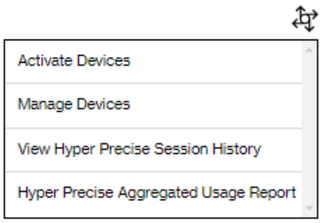
The Device status pod uses color-coded donut charts to show the connectivity and provisioning status for devices. Clicking in the **Connection** or **Provisioning** circle opens the *Devices* page listing devices with their connection and provisioning status. Clicking on the links the chart has the same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



Hyper precise location pod

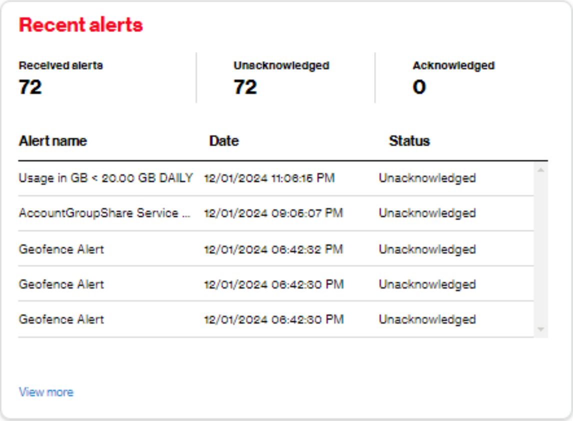
The Hyper precise location pod displays the number of devices enabled for the Hyper Precise Location service.




Activate Devices
Manage Devices
View Hyper Precise Session History
Hyper Precise Aggregated Usage Report

Recent alerts pod

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



Recent alerts

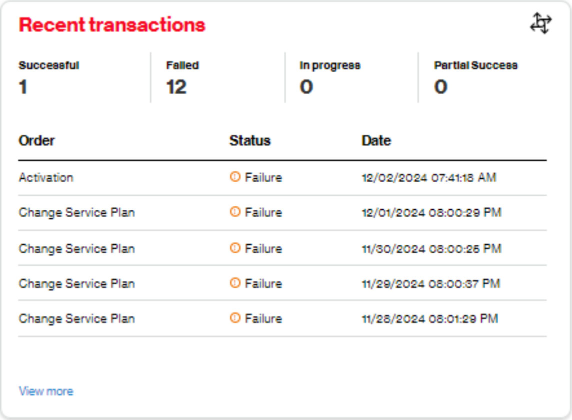
Received alerts	Unacknowledged	Acknowledged
72	72	0

Alert name	Date	Status
Usage in GB < 20.00 GB DAILY	12/01/2024 11:08:16 PM	Unacknowledged
AccountGroupShare Service ...	12/01/2024 09:06:07 PM	Unacknowledged
Geofence Alert	12/01/2024 06:42:32 PM	Unacknowledged
Geofence Alert	12/01/2024 06:42:30 PM	Unacknowledged
Geofence Alert	12/01/2024 06:42:30 PM	Unacknowledged

View more

Recent transactions

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

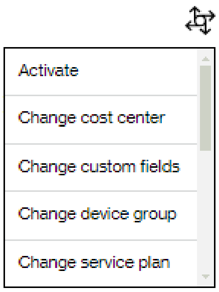


Recent transactions

Successful	Failed	In progress	Partial Success
1	12	0	0

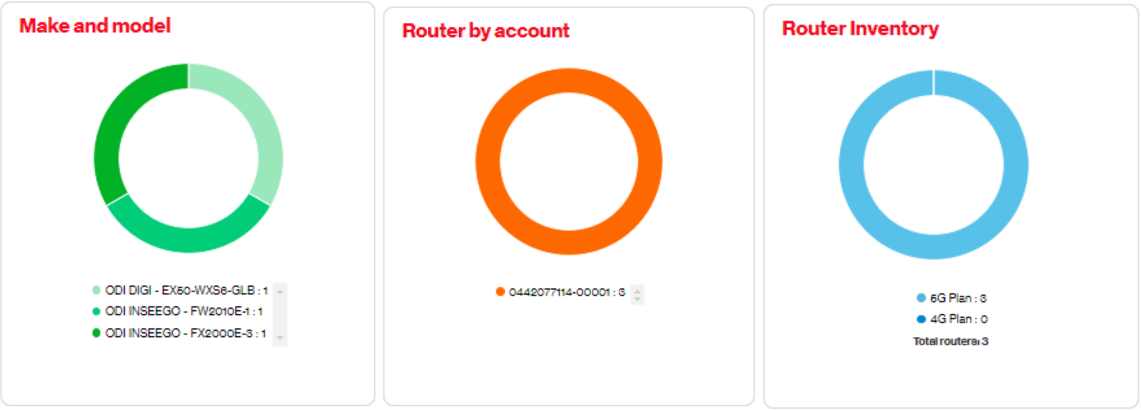
Order	Status	Date
Activation	Failure	12/02/2024 07:41:18 AM
Change Service Plan	Failure	12/01/2024 08:00:29 PM
Change Service Plan	Failure	11/30/2024 08:00:26 PM
Change Service Plan	Failure	11/29/2024 08:00:37 PM
Change Service Plan	Failure	11/28/2024 08:01:29 PM

View more



Verizon Business Internet router pods

If you have Verizon Business Internet (BI) plans, you will see additional pods related to routers.



Make and model pod

The Make and model pod displays the number of FWA devices by make and model.

Router by account pod

The Router by account pod displays the number of FWA devices by account.

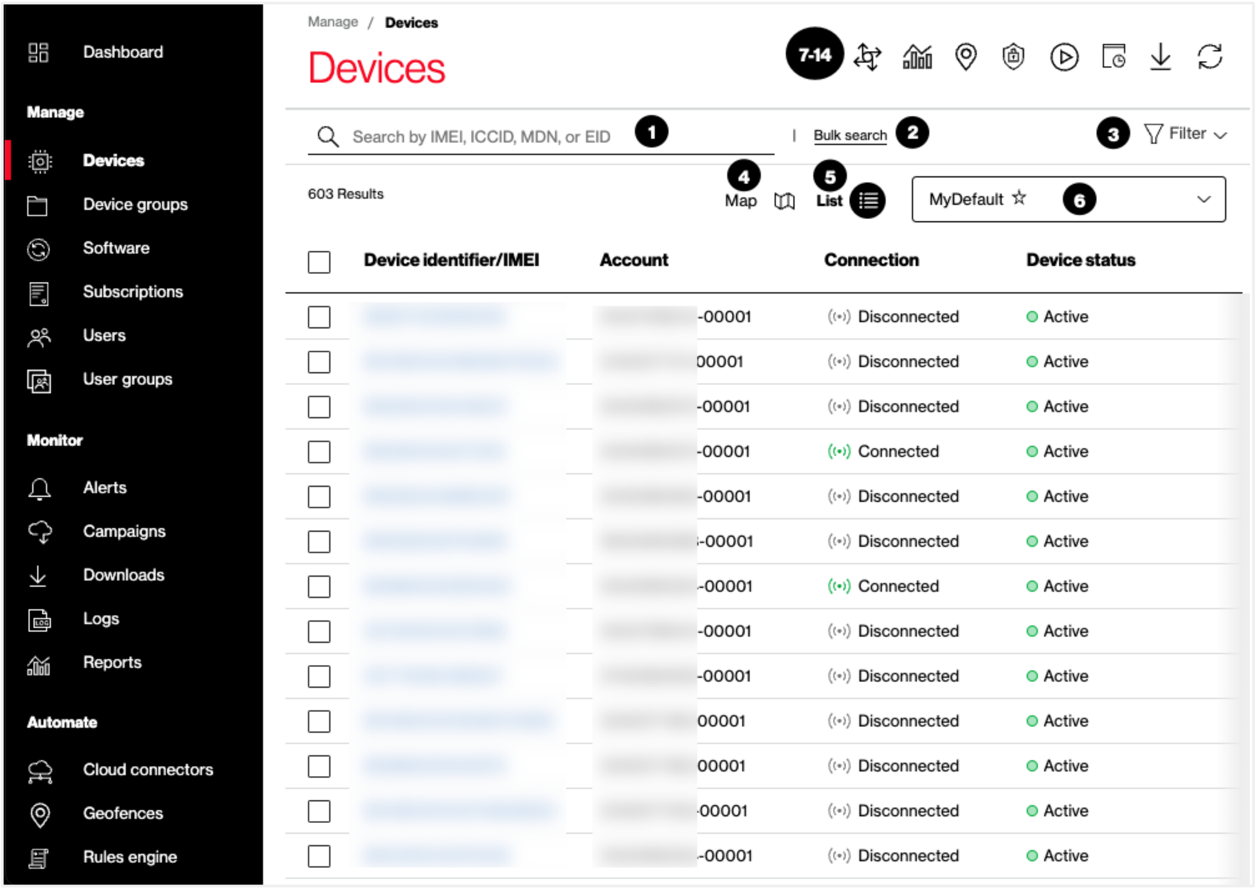
Router inventory pod

The Router inventory pod displays the number of FWA devices by plan.

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 on the top right of the page apply to devices in bulk or only to selected devices.

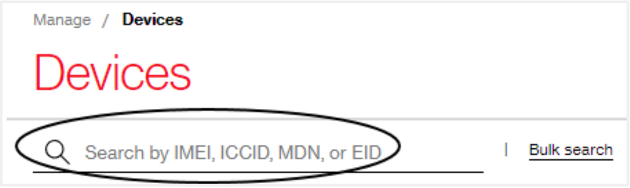


□	Device identifier/IMEI	Account	Connection	Device status
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Connected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Connected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active
□	[redacted]	[redacted]00001	Disconnected	● Active
□	[redacted]	[redacted]00001	Disconnected	● Active
□	[redacted]	[redacted]00001	Disconnected	● Active
□	[redacted]	[redacted]-00001	Disconnected	● Active

Elements on the Devices page					
1	🔍	Search – Locate a specific device.	2	Bulk search	Bulk search – Locate up to 500 devices at once.
3	▽	Filter – Limit the list to devices with specific attributes.	4	Map 🗺	Map view – View devices on a map.
5	List ☰	List view – View devices in a table list.	6	Connectivity ⌄	Table view – Customize your view.
7	✥	Actions – Open a menu of actions.	8	📊	Reports – Run device reports.
9	📍	Location – Subscribers can take location actions, such as enable or disable location updates.	10	🛡	Security – Subscribers can manage SIM Secure Services.
11	▷	Video – View short training videos relevant to this page.	12	📅	Schedule – Automate and schedule a report.
13	↓	Download – Export listed device information.	14	⟳	Reload – Refresh the page with new data

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.



Manage / Devices

Devices

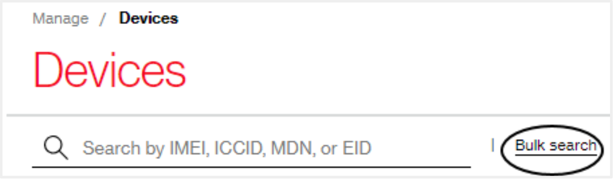
NOTE: Search does not support wildcards for IP address. You must search for the exact IP address.

Performing a bulk search

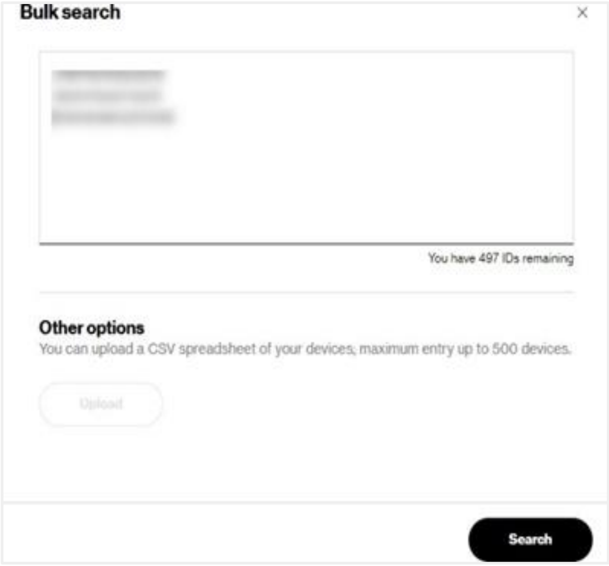
You can search for up to 500 devices at a time using the Bulk search link.

To perform a bulk search

1. Click the **Bulk search** link: 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.



[redacted]

You have 497 IDs remaining

Other options

You can upload a CSV spreadsheet of your devices, maximum entry up to 500 devices.

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.

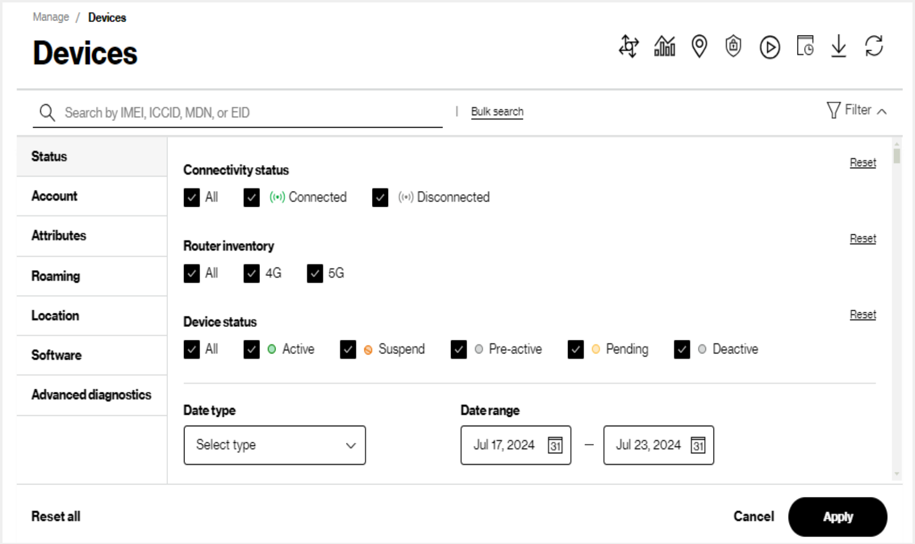
Applying device filters

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 device filters

1. Click the filter icon ▽ Filter ⌄. The following filters screen appears.



Connectivity status
☑ All ☑ Connected ☑ Disconnected

Router inventory
☑ All ☑ 4G ☑ 5G

Device status
☑ All ☑ Active ☑ Suspend ☑ Pre-active ☑ Pending ☑ Deactive

Date type: Select type

Date range: Jul 17, 2024 – Jul 23, 2024

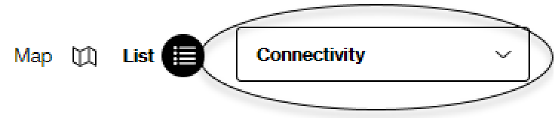
2. Click each tab or scroll through the list to view all available filters. Select the desired filters to apply and click **Apply**.
3. The **Reset** link of each filter category allows you to select all filters in the category with one click.
4. The **Reset all** link resets all filters.
5. To apply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

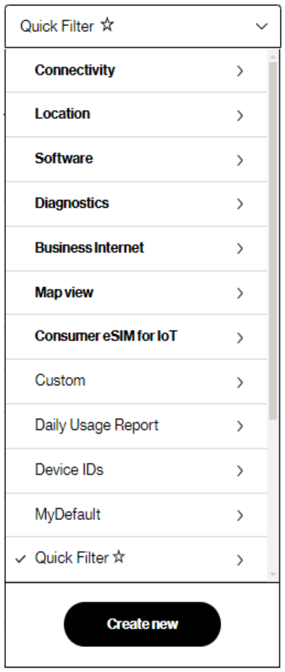
   2 filters applied ×

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.

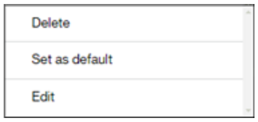
Table views

Table views change the columns displayed on the devices list. Table views are found on the View dropdown located on the results section. Select a view to refresh the devices list with fields in that view.

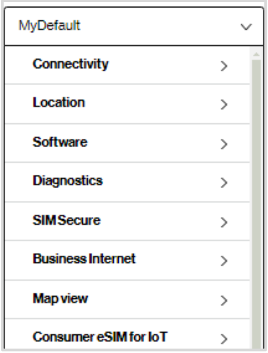




Click on the expand icon > to view the available options. Options include editing and deleting a custom view and setting a view as the default view.



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, which are views you create. You cannot edit predefined views only custom views.



Available predefined views are:

- **Connectivity View** – View columns of information related to device connectivity.
- **Location View** – View columns of information related to device location.
- **Software View** – View columns of information related to software management.
- **Diagnostics View** – View columns of information related to device diagnostics, useful for troubleshooting issues.
- **SIM Secure** – View columns of information related to device with SIM secure.
- **Business Internet** – View columns of information related to Business Internet.
- **Map View** – View a list of devices on a map.
- **Consumer eSIM for IoT** – View columns of information related to consumer eSIM for IoT.

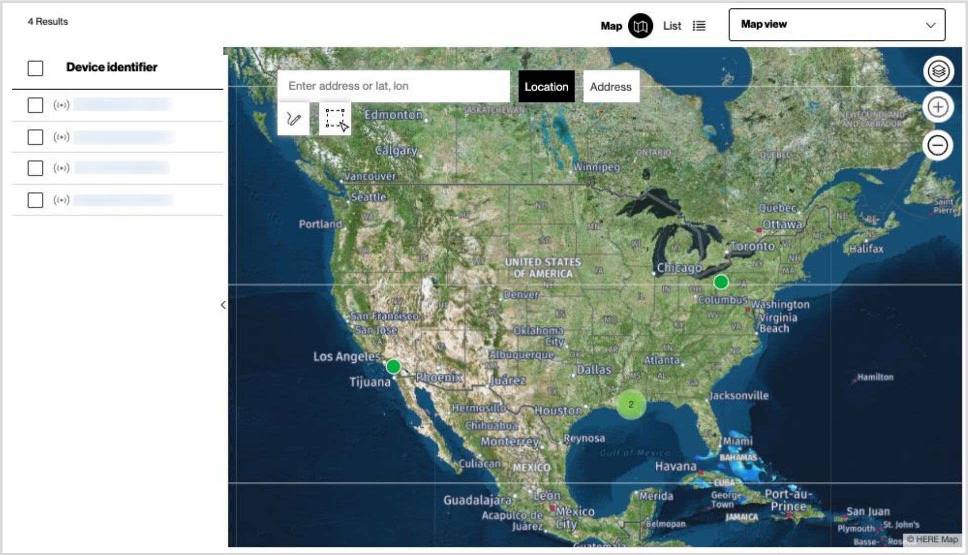
Custom views are table views you develop from predefined views. See Create a custom view.

Map view

The map view allows you to see the location or the address of your devices plotted. The location is plotted provided you updated the location through a Location action. The address is plotted provided it was set during the activation, change service plan or set explicitily by using the "change services address" action.

To view devices on a map, select the **Map view** from the dropdown or click on the Map icon Map. The table will change to a view of the map and will have circles representing devices and their locations or addresses, based on the toggle at the top of the map. When you select a device on the map, it will provide additional information about its location or address.

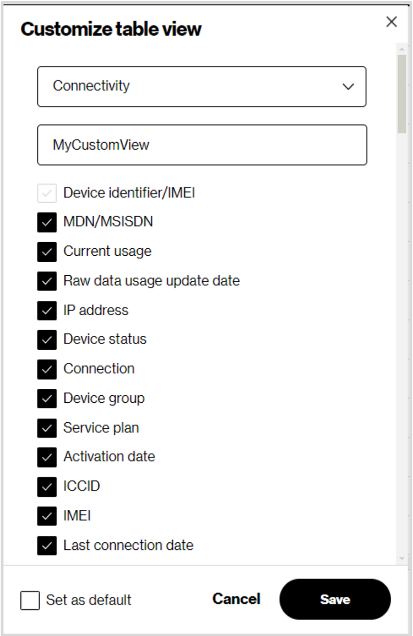
The device identifiers are listed to the left of the map. You can perform actions including change service plan or change service address from the actions option. To switch back to the devices list, click the List icon List.



Create a custom view

How to create a custom view

1. Click the view dropdown and select **Create new**. The *Customize table view* dialog opens.



Customize table view

Connectivity

MyCustomView

- ☑ Device identifier/IMEI
- ☑ MDN/MSISDN
- ☑ Current usage
- ☑ Raw data usage update date
- ☑ IP address
- ☑ Device status
- ☑ Connection
- ☑ Device group
- ☑ Service plan
- ☑ Activation date
- ☑ ICCID
- ☑ IMEI
- ☑ Last connection date

□ Set as default

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 by hovering the cursor over the right side of the field name until the move icon appears. ≡

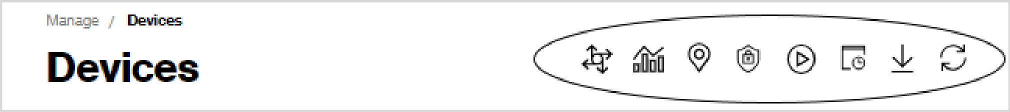
   c. Drag and drop the field to the desired position on the list.

   d. Check the **Set as default checkbox** to make this your default view.

4. Click **Save** to complete the process.

Taking actions on devices

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



Manage / **Devices**

Devices

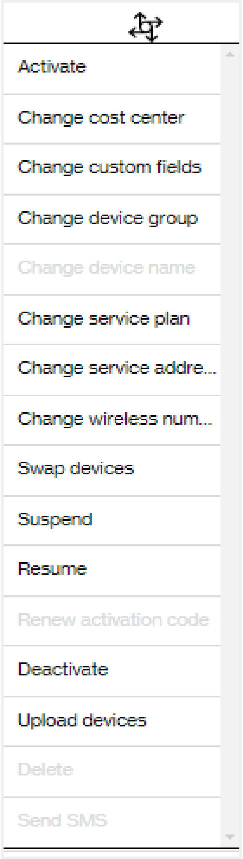
There are two types of actions that you can take:

Bulk actions – Take actions on a list of devices that you enter manually or upload from a file.

Quick actions – Take quick actions on devices selected from the devices list.

Provisioning actions

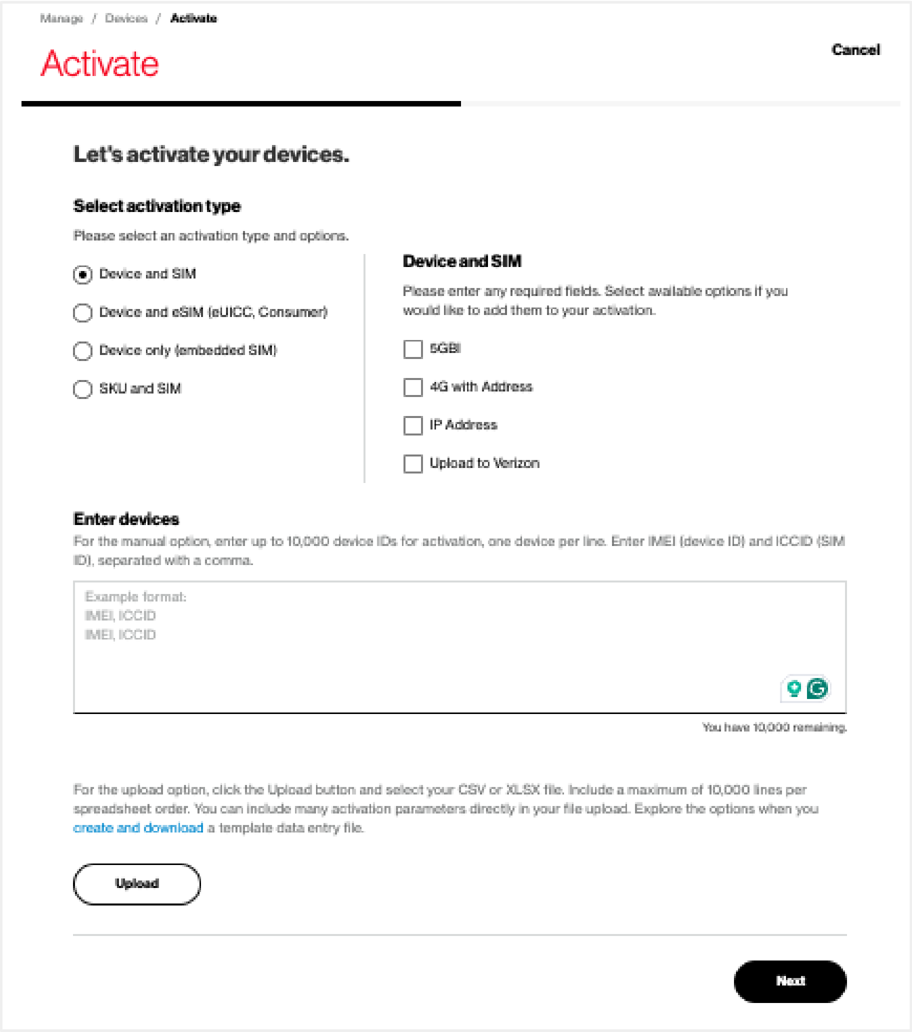
The actions icon ✥ displays a drop-down menu with a list of actions. The majority of these are provisioning actions, such as activate, change service plan, change wireless number, suspend, resume, swap, and deactivate devices. The other actions allow you to make changes to cost center codes, custom field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


Activate
Change cost center
Change custom fields
Change device group
Change device name
Change service plan
Change service addre...
Change wireless num...
Swap devices
Suspend
Resume
Renew activation code
Deactivate
Upload devices
Delete
Send SMS

Activate devices

How to activate devices in bulk

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



Activate

Let's activate your devices.

Select activation type

Please select an activation type and options.

● Device and SIM

○ Device and eSIM (eUICC, Consumer)

○ Device only (embedded SIM)

○ SKU and SIM

Device and SIM

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

□ 5GBI

□ 4G with Address

□ IP Address

□ Upload to Verizon

Enter devices

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

Example format:
IMEI, ICCID
IMEI, ICCID

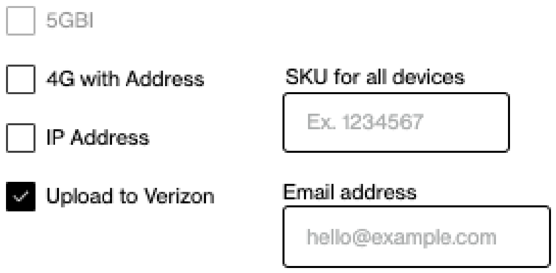
You have 10,000 remaining.

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

2. Select the type of activation. Depending on the type of activation, other options will be displayed to the right. When you choose one of the other options, the example format in the **Enter devices** section will provide an example of how the data is to be entered. You can also upload a list from your computer. See uploading a device list.

3. Enter the device identifiers manually or upload a file of up to 10,000 devices in the **Enter devices** section.

    a. For **Device and SIM** activations, enter a list of IMEI and ICCIDs. If you choose the checkbox to **Upload to Verizon**, you must provide the Verizon SKU and email address that is associated with the user's Open Development account. Selecting this option will first upload the devices to Verizon's DMD prior to the activation.



□ 5GBI

□ 4G with Address

□ IP Address

☑ Upload to Verizon

SKU for all devices

Ex. 1234567

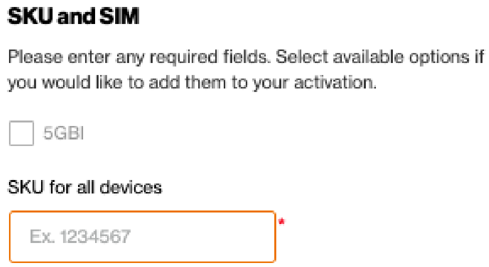
Email address

hello@example.com

b. For **Device and eSIM (eUICC, Consumer)** activations, enter a list of EIDs and IMEIs.

c. For **Device only (embedded SIM)** activations, enter a list of IMEIs.

d. For **SKU and SIM** activations, enter a list of ICCIDs. The Verizon SKU ID and the email address used to login to the Open Development portal is required.



SKU and SIM

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

□ 5GBI

SKU for all devices

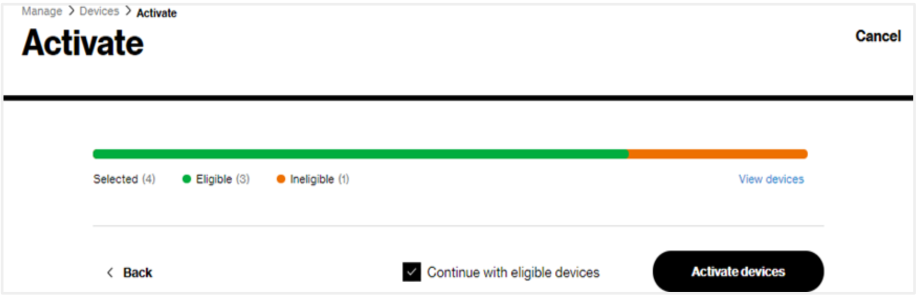
Ex. 1234567 *

e. If the "IP address" option is selected: For customers with IP pools, they can specify the desired IP address in the activation alongside the device identifier(s).

f. If the "5G BI" option is selected: This is required if the line is a 5G Business Internet Fixed Wireless Access Line. You must specify the address that should qualify for that plan alongside the device identifier(s).

g. If the "4G with Address" option is selected: This is optional for non 5G BI plans (both IoT & FWA) where the address will be stored in ThingSpace for plan changes and mapping. It is recommended if you want to move to a 5G Business Internet plan eventually. Provide the address alongside the device identifier(s).

4. Click **Next**. The second Activate page opens.



Manage > Devices > Activate

Activate

Cancel

Selected (4) ● Eligible (3) ● Ineligible (1)

View devices

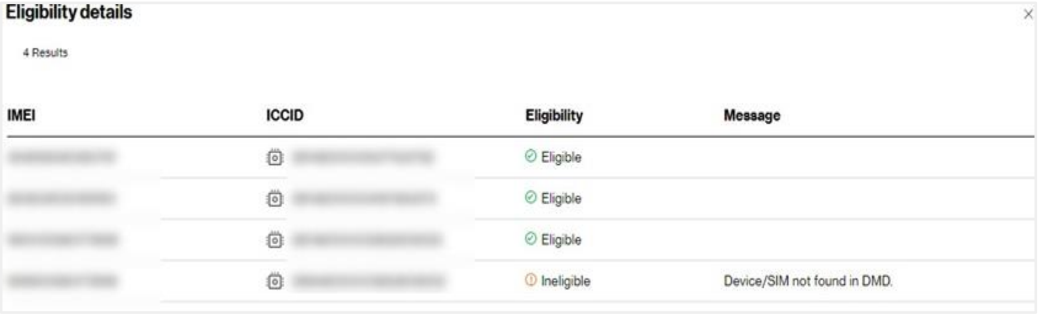
< Back

☑ Continue with eligible devices

Activate devices

5. Review device eligibility. To view the list of the devices and any associated error messages, click the **View devices** link. The *Eligibility details* dialog opens. If there are devices that are ineligible for activation, you can

continue with only the eligible devices. Check **Continue with eligible** devices to proceed.



Eligibility details

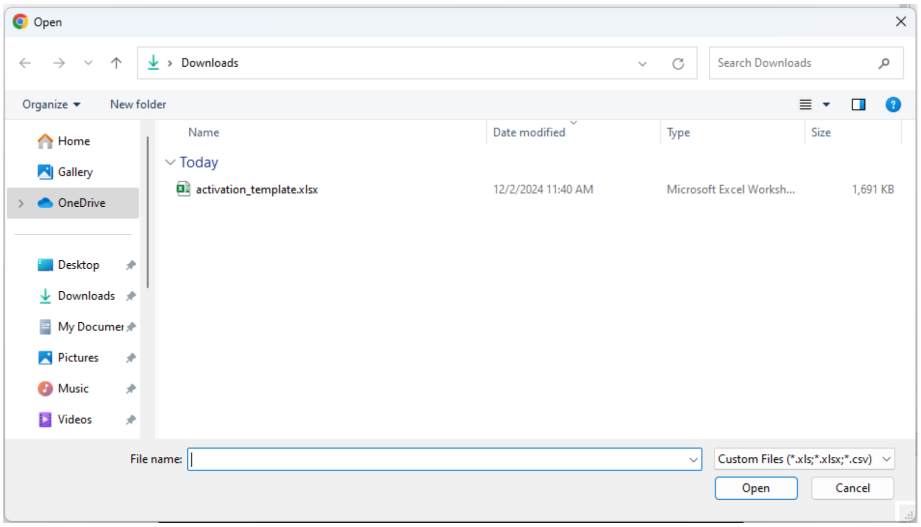
4 Results

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

6. Click **Activate devices** to submit the activation order.

Uploading a device list

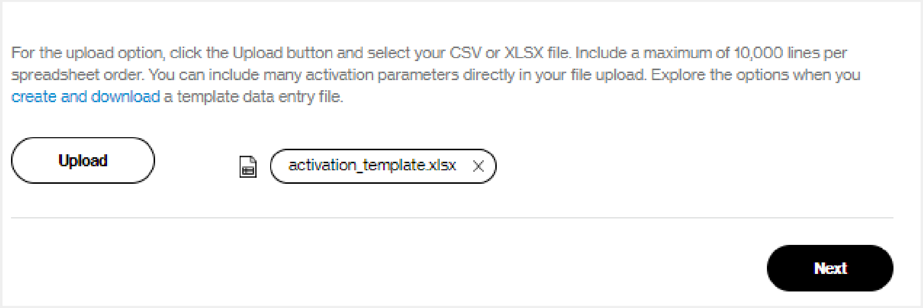
1. To upload a file, click **Upload** to be prompted to select a file from your hard drive.
2. Click the file to upload from the Open dialog box.



Name	Date modified	Type	Size
Today			
activation_template.xlsx	12/2/2024 11:40 AM	Microsoft Excel Worksh...	1,691 KB

File name:

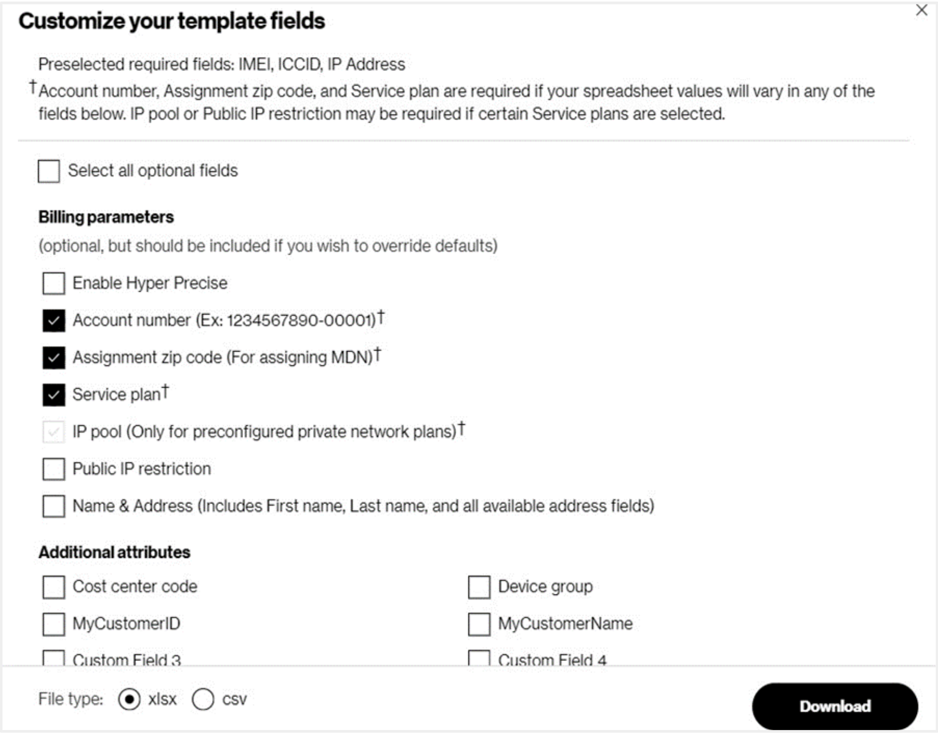
3. Click **Open** to return to the prior screen. You will see the name of the file you selected next to the Upload button.



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

Customizing dynamic templates

1. To create a customized template 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.
2. Account, Service plan, and Assignment zip code (mdnZipCode) are all required fields when entering different device attributes to the template.



Customize your template fields

Preselected required fields: IMEI, ICCID, IP Address

†Account number, Assignment zip code, and Service plan are required if your spreadsheet values will vary in any of the fields below. IP pool or Public IP restriction may be required if certain Service plans are selected.

□ Select all optional fields

Billing parameters

(optional, but should be included if you wish to override defaults)

□ Enable Hyper Precise

☑ Account number (Ex: 1234567890-00001)†

☑ Assignment zip code (For assigning MDN)†

☑ Service plan†

☑ IP pool (Only for preconfigured private network plans)†

□ Public IP restriction

□ Name & Address (Includes First name, Last name, and all available address fields)

Additional attributes

□ Cost center code

□ MyCustomerID

□ Custom Field 3

□ Device group

□ MyCustomerName

□ Custom Field 4

File type: ● xlsx ○ csv

3. Click **Download** to download the customized template.
4. Add your data to the template file and save. You can have different values for each column in the template.
5. Click **Next** continue with the activation.

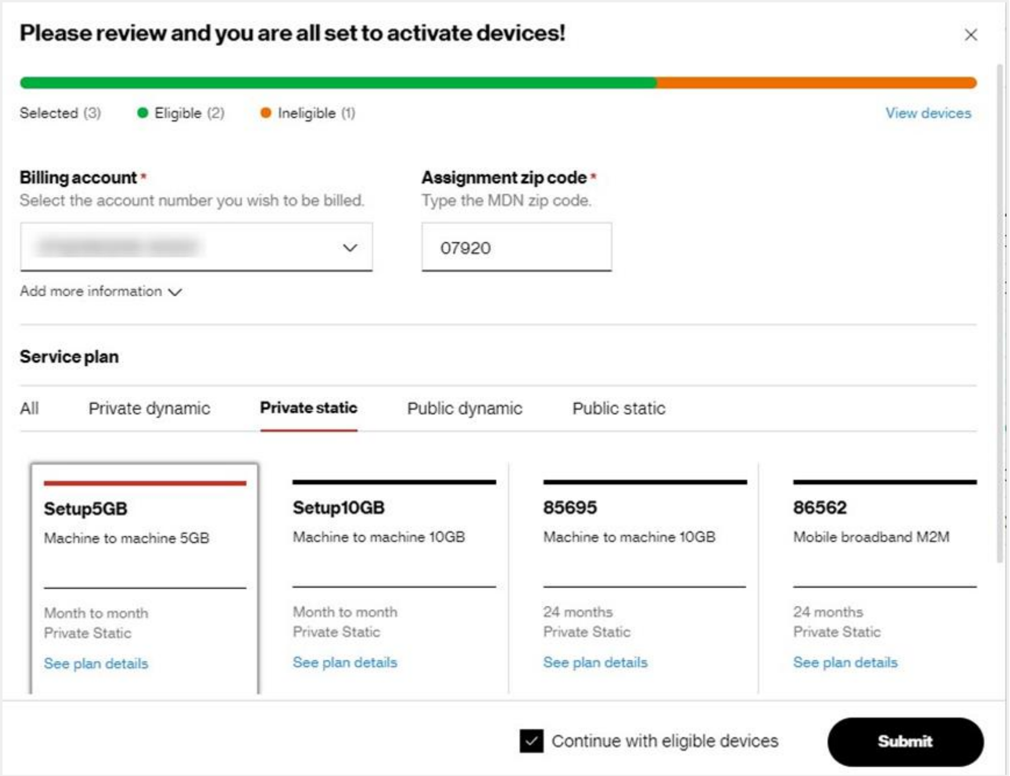
Quick activations

Activate multiple devices using default values in just one click.

How to quickly activate devices

1. Select devices in the devices list using the Device identifier checkbox.

2. Click the actions icon and select **Activate**. A review dialog opens next.



Please review and you are all set to activate devices!

Selected (3) ● Eligible (2) ● Ineligible (1)

Billing account *
Select the account number you wish to be billed.
[redacted]

Assignment zip code *
Type the MDN zip code.
07920

Service plan

Setup5GB	Setup10GB	85695	86562
Machine to machine 5GB	Machine to machine 10GB	Machine to machine 10GB	Mobile broadband M2M
Month to month Private Static	Month to month Private Static	24 months Private Static	24 months Private Static
See plan details	See plan details	See plan details	See plan details

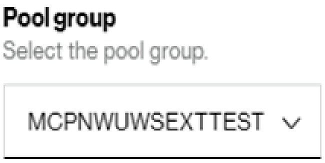
☑ Continue with eligible devices

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. Check whether to enable **Hyper precise location** for the selected device(s).

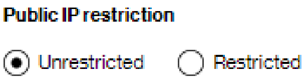
5. Assign a **Service plan** to the devices. You can filter the service plans by clicking on **Private dynamic, Private static, Public dynamic**, or **Public static**.

   a. 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.



Pool group
Select the pool group.
MCPNWUWSEXTTEST

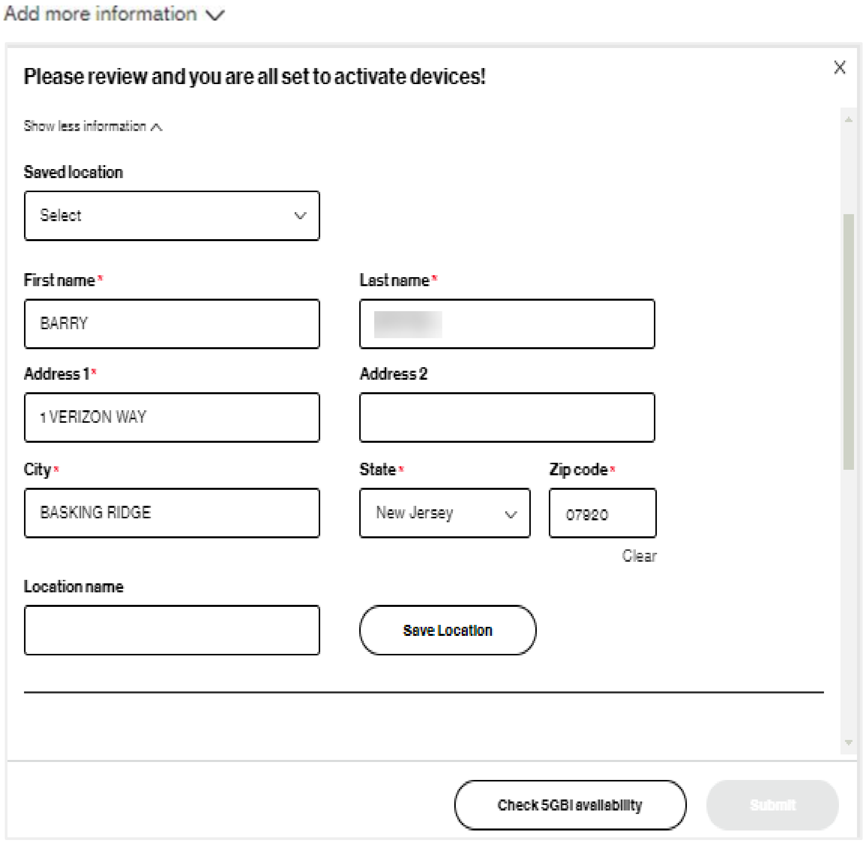
   b. For public static plans, you can choose the type of restriction to apply. Unrestricted IPs provide full access to the Internet. Restricted IPs have limited access to content provided by Verizon Wireless and are restricted from accessing the Internet.



Public IP restriction

● Unrestricted ○ Restricted

6. Click **Add more information** to set additional details, such as *Name, Address, Device groups*, *Custom fields*, *Cost Center*. A new section will be displayed. In this section you can also check whether 5GBI plans are available in a particular location.



Add more information ∨

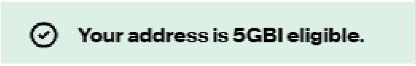
Please review and you are all set to activate devices!

Show less information ∧

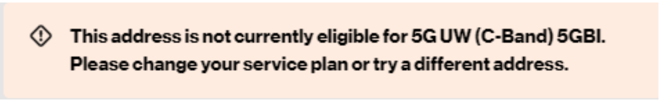
Saved location: Select		
First name*: BARRY	Last name*: [redacted]	
Address 1*: 1 VERIZON WAY	Address 2:	
City*: BASKING RIDGE	State*: New Jersey	Zip code*: 07920
Location name:		

a. You can select a **Saved location** or enter a new address to save and click **Save location**. The *Save location* function becomes available after you provide a name for the location.

b. If you enter an address or select a saved location and you have 5G Business Internet price plans on your account, the **Check 5G BI availability** button will be enabled so that you can check whether 5G BI plans are available at that location. Click on it to check availability. If the location is 5G BI eligible, you will see a banner on the top of the page that says the address is 5G BI eligible. Otherwise, a banner will be displayed saying the address is not eligible.



✓ Your address is 5GBI eligible.



This address is not currently eligible for 5G UW (C-Band) 5GBI. Please change your service plan or try a different address.

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

8. Check **Save these selections as my favorites** if you want to save the information for future use.

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

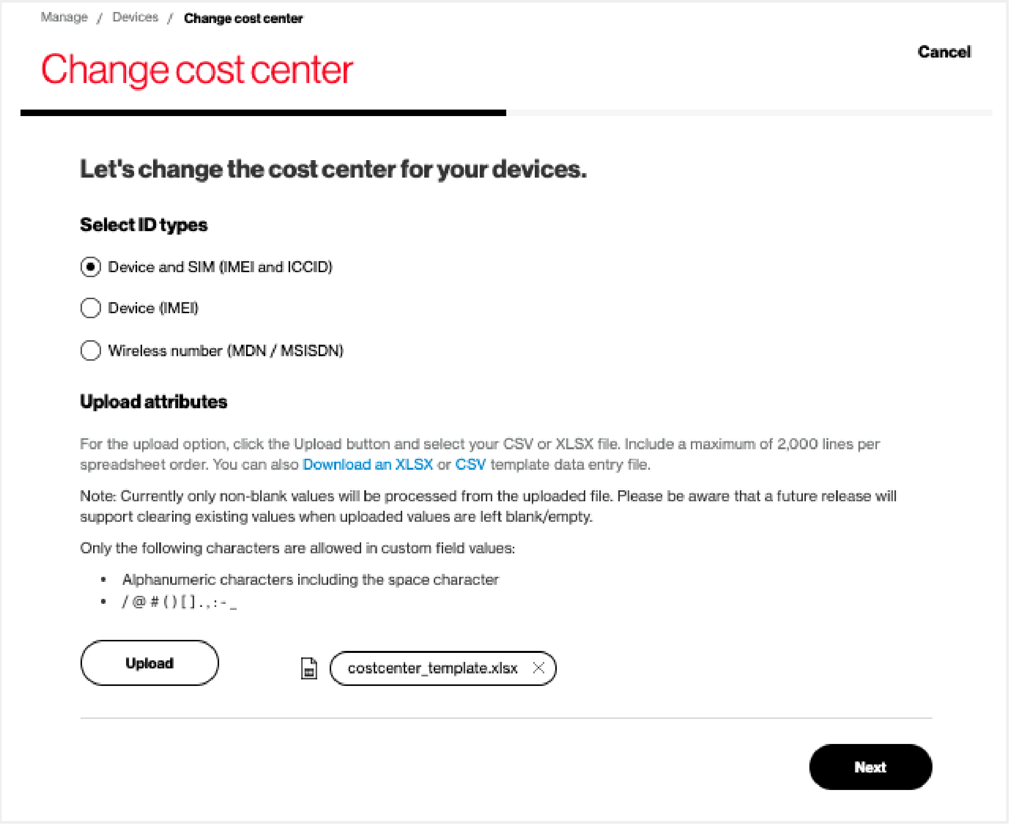
10. Check the status of the transaction(s) in the **Logs.**

Change cost center codes

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

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



Manage / Devices / **Change cost center**

Change cost center

Cancel

Let's change the cost center for your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Upload attributes

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

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

Only the following characters are allowed in custom field values:

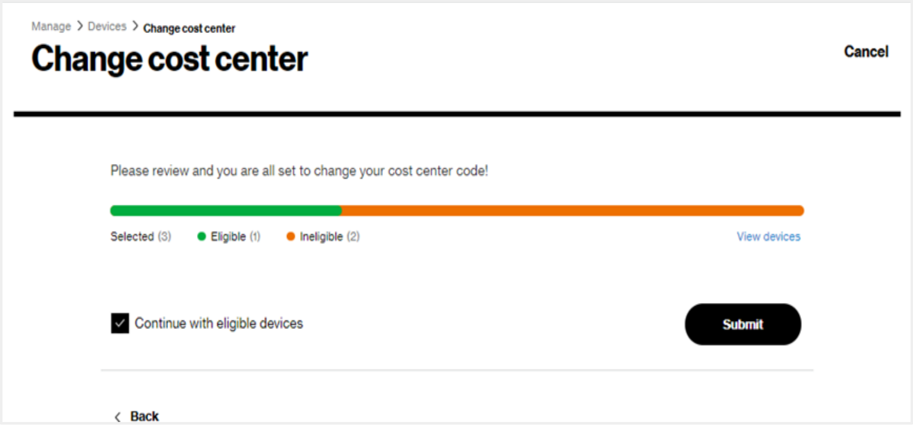
- Alphanumeric characters including the space character
- / @ # ( ) [ ] . , : - _

Upload

costcenter_template.xlsx ✕

Next

2. Select the **ID types** to use (Device and SIM, Device only, or Wireless number).
3. Upload an existing file with the information or click **Download an XLSX or CSV** to download the template if needed.
4. Click **Next**. A review dialog opens next.



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

Selected (3) ● Eligible (1) ● Ineligible (2)

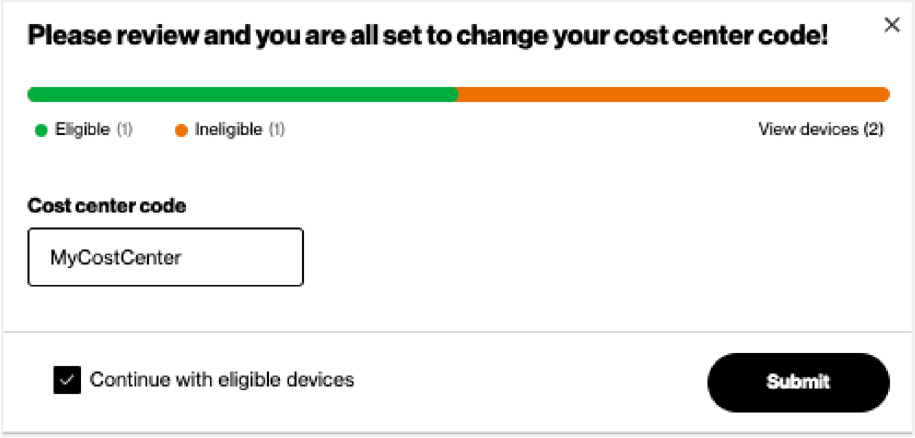
☑ Continue with eligible devices

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

Quick cost center code changes

How to quickly change cost center codes

1. Select the Device identifier checkbox. Devices must be from the same billing account.
2. Click the actions icon and then select **Change cost center**. A review page opens.



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

● Eligible (1) ● Ineligible (1)

Cost center code: MyCostCenter

☑ Continue with eligible devices

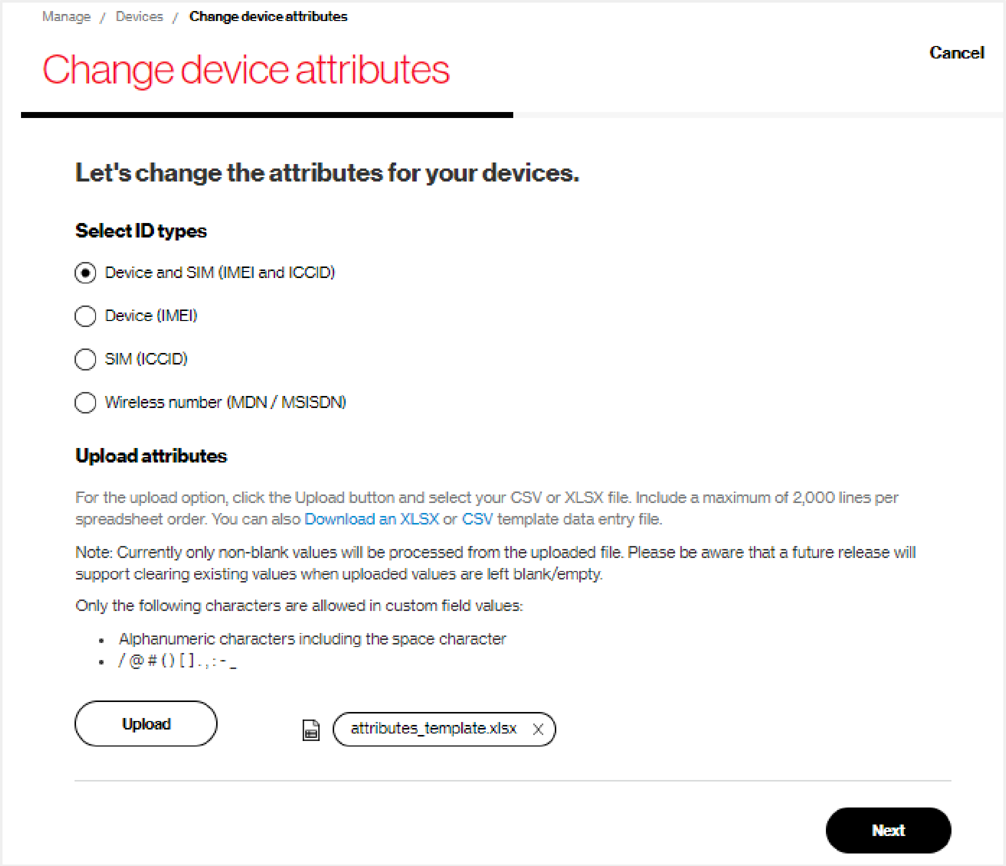
3. Review eligible and ineligible device counts. To view the list of selected devices, click the **View devices** link.
4. Type the **Cost center code** to assign. Limit 36 characters.
5. Check Continue with eligible devices if necessary to proceed.
6. Click **Submit** to complete the process.

Change custom fields

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 fields setting for additional information.

How to change custom fields in bulk

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



Change device attributes

Let's change the attributes for your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ SIM (ICCID)

○ Wireless number (MDN / MSISDN)

Upload attributes

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

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

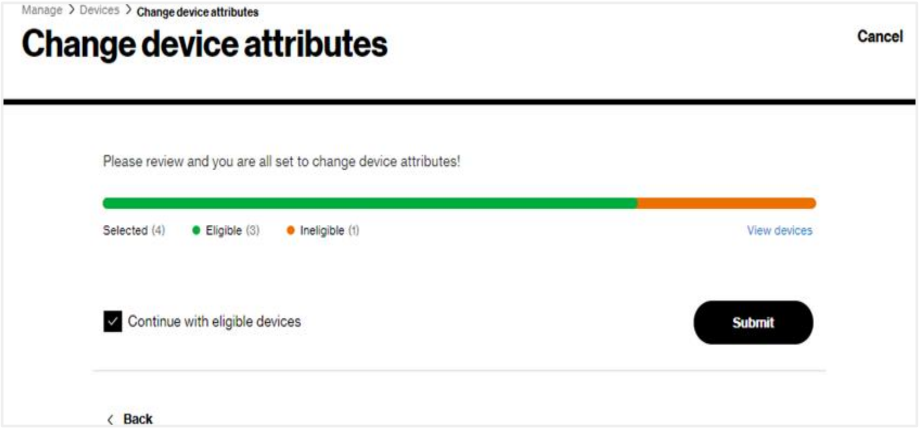
Only the following characters are allowed in custom field values:

- Alphanumeric characters including the space character
- / @ # ( ) [ ] . , ; : - _

2. Select the **ID types** to use (Device and SIM, Device only, or Wireless number).

3. **Upload** an existing file with the information or click **Download an XLSX or CSV** to download the template if needed.

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



Manage > Devices > Change device attributes

Change device attributes

Cancel

Please review and you are all set to change device attributes!

Selected (4) ● Eligible (3) ● Ineligible (1) View devices

☑ Continue with eligible devices

Submit

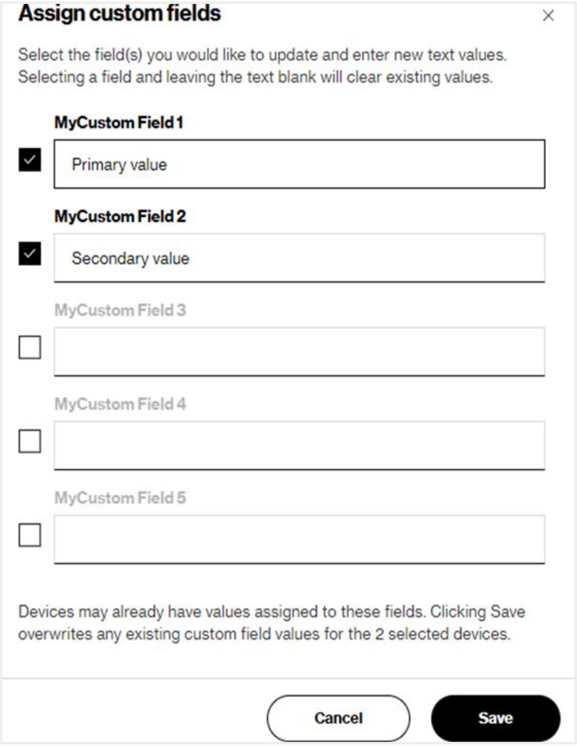
‹ Back

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

Quick custom field changes

How to quickly change custom fields

1. Select the Device identifier checkbox. Devices must be from the same billing account.
2. Click the actions icon and then select **Change custom fields**. The *Assign custom fields* dialog opens.



Assign custom fields ×

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

MyCustom Field 1

☑ Primary value

MyCustom Field 2

☑ Secondary value

MyCustom Field 3

☐

MyCustom Field 4

☐

MyCustom Field 5

☐

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

Cancel Save

3. Select a custom field label to update by checking the checkbox next to it.
4. Type the **Value**.
5. Click **Save** to complete the process.

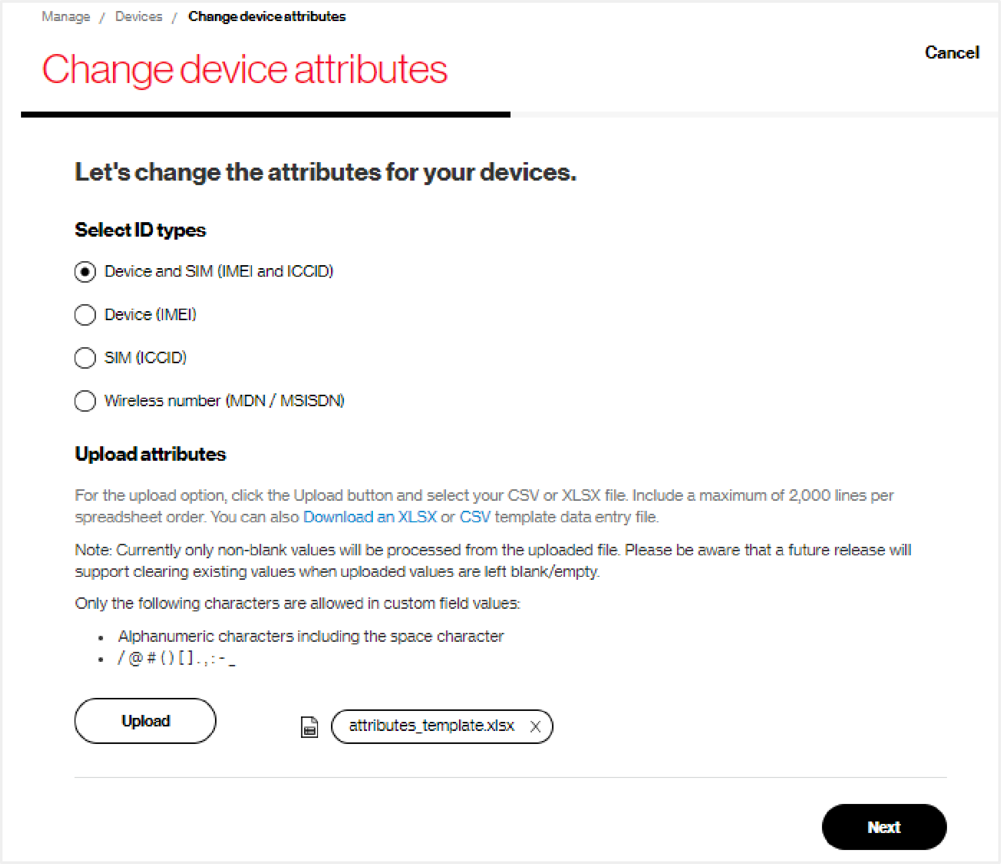
The following **special characters** (alphanumeric) are allowed in custom field values.

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

Change device groups

How to change device groups in bulk

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



Change device attributes

Let's change the attributes for your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ SIM (ICCID)

○ Wireless number (MDN / MSISDN)

Upload attributes

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

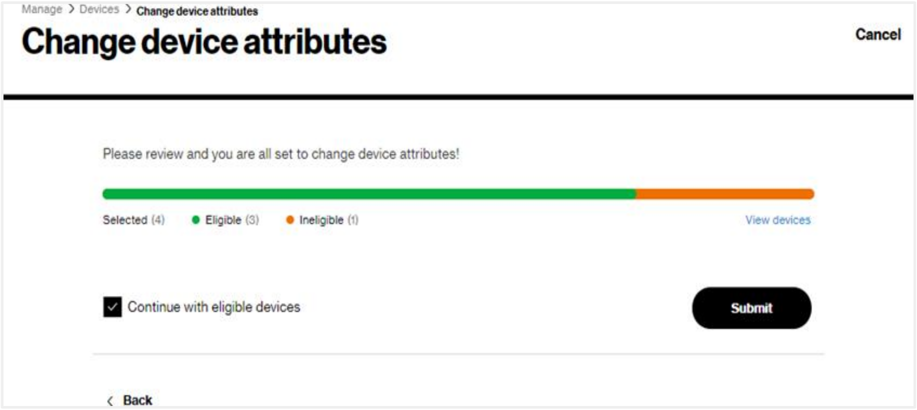
Note: Currently only non-blank values will be processed from the uploaded file. Please be aware that a future release will support clearing existing values when uploaded values are left blank/empty.

Only the following characters are allowed in custom field values:

- Alphanumeric characters including the space character
- / @ # ( ) [ ] . , : - _

attributes_template.xlsx X

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. **Upload** an existing file with the information or click **Download an XLSX or CSV** to download the template if needed.
4. Click **Next**. A review dialog opens next.



Manage > Devices > Change device attributes

Change device attributes

Cancel

Please review and you are all set to change device attributes!

Selected (4) ● Eligible (3) ● Ineligible (1) View devices

☑ Continue with eligible devices

Submit

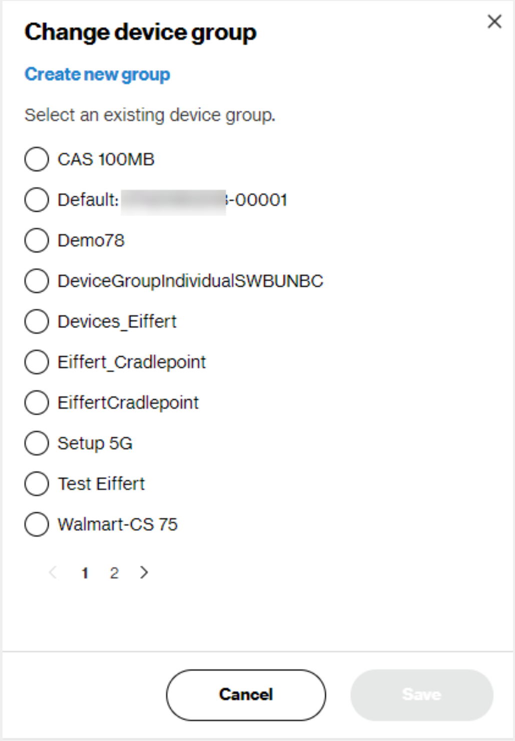
‹ Back

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

Quick device group changes

How to quickly change the device groups

1. Select devices using the *Device identifier* checkboxes. Note that 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 *Change device group* dialog opens.



Change device group ×

Create new group

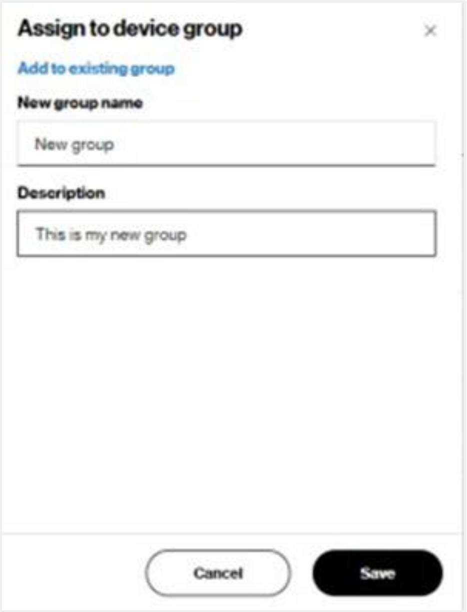
Select an existing device group.

○ CAS 100MB
○ Default: [redacted]-00001
○ Demo78
○ DeviceGroupIndividualSWBUNBC
○ Devices_Eiffert
○ Eiffert_Cradlepoint
○ EiffertCradlepoint
○ Setup 5G
○ Test Eiffert
○ Walmart-CS 75

‹ 1 2 ›

Cancel Save

3. You have two options for assigning a device to a group:
   a. Select an existing device group from the options presented
   b. Click **Create new group**. When clicked, the Assign to device group dialog refreshes with a new group form.



Assign to device group

Add to existing group

New group name

New group

Description

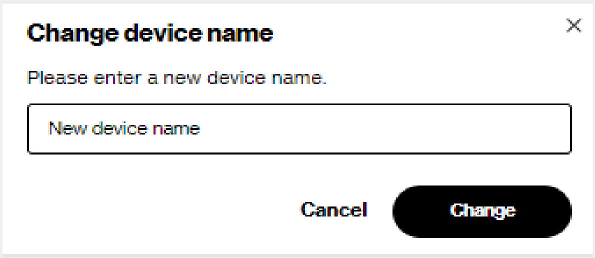
This is my new group

4. For **New group name**, type a descriptive label.
5. Type an optional **Description** for the new group name.
6. Click **Save**. The Assign to device group dialog closes.
7. On the Assign to device group page, click **Save** to complete the process.

Change device name

How to quickly change device names

1. Select the Device identifier checkbox of the devices you want to select.
2. Click the actions icon ✥ and select **Change device name**. The *Change device name* dialog is displayed.



Change device name

Please enter a new device name.

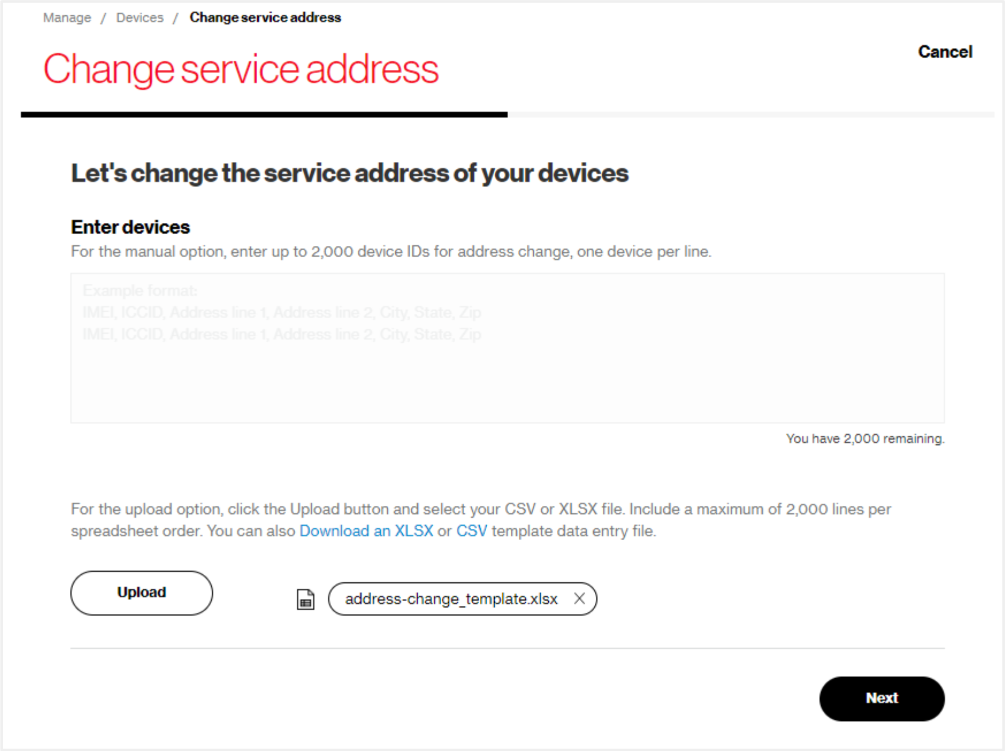
New device name

3. Click **Change** to proceed.

Change service address

How to change service addresses in bulk

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



Manage / Devices / Change service address

Change service address

Cancel

Let's change the service address of your devices

Enter devices

For the manual option, enter up to 2,000 device IDs for address change, one device per line.

Example format:
IMEI, ICCID, Address line 1, Address line 2, City, State, Zip
IMEI, ICCID, Address line 1, Address line 2, City, State, Zip

You have 2,000 remaining.

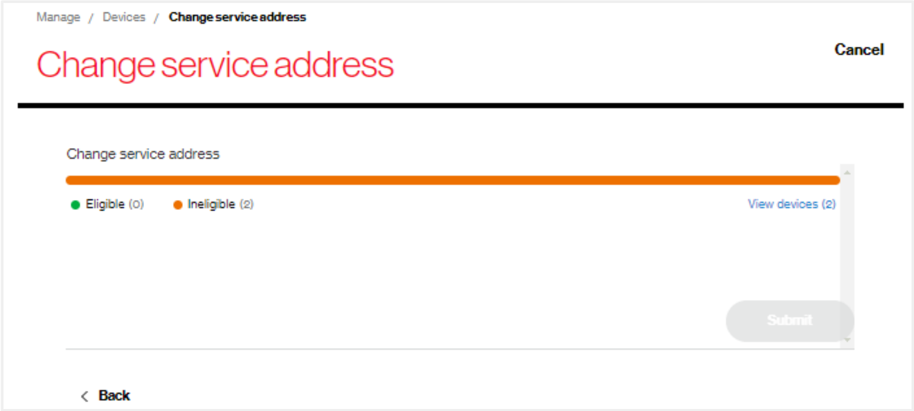
For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also Download an XLSX or CSV template data entry file.

Upload

address-change_template.xlsx ✕

Next

2. Enter the device identifiers manually or upload a file of up to 2,000 devices in the **Enter devices** section.
3. Click **Next** to proceed. A review dialog opens.



Manage / Devices / Change service address

Change service address

Cancel

Change service address

● Eligible (0) ● Ineligible (2) View devices (2)

Submit

< Back

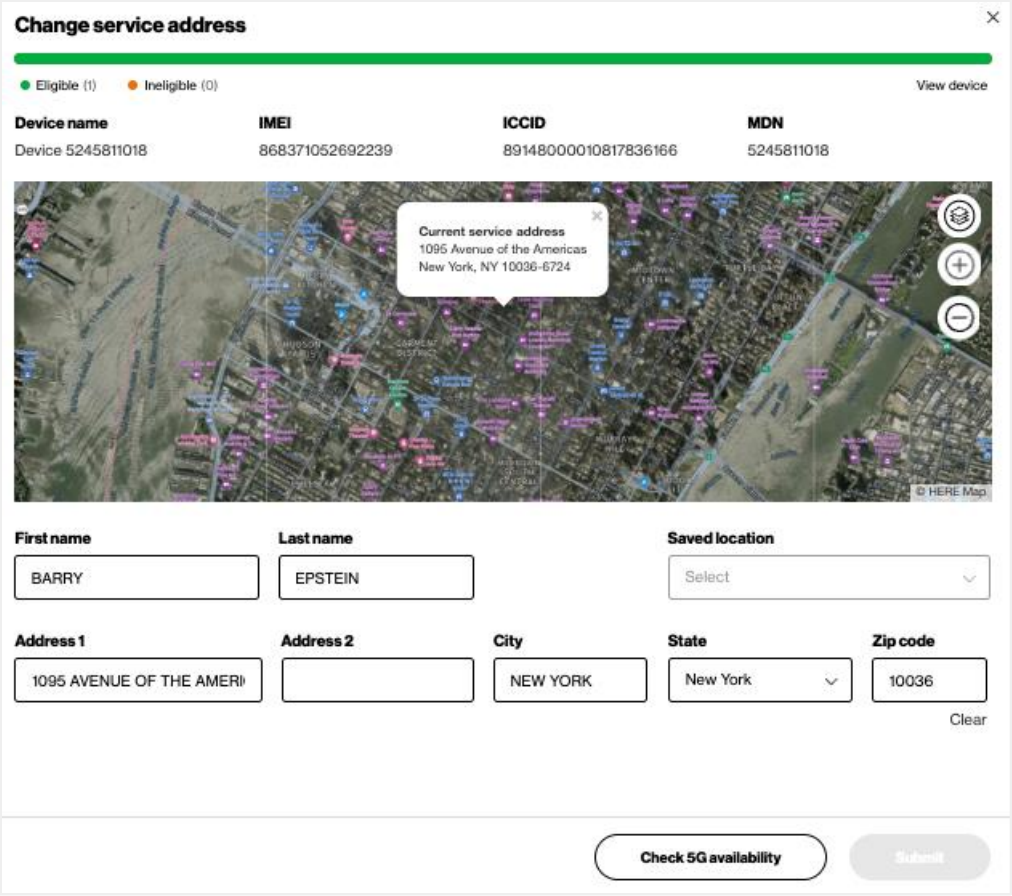
4. Review eligible or ineligible devices.
5. Click **Submit** to complete the process.

6. Note: For 5G Business Internet lines, the addresses will only change if the new address qualifies for 5G Business Internet.
7. Check the status of the transaction(s) in the **Logs.**

Quick service address changes

How to quickly change the service address of devices

1. Select the Device identifier checkbox of the devices you want to select.
2. Click the actions icon and then click **Change service address**. The *Change service address* dialog opens.



Change service address ×

● Eligible (1) ● Ineligible (0) View device

Device name	IMEI	ICCID	MDN
Device 5245811018	868371052692239	89148000010817836166	5245811018

Current service address
1095 Avenue of the Americas
New York, NY 10036-6724

© HERE Map

First name	Last name		Saved location	
BARRY	EPSTEIN		Select	
Address 1	**Address 2**	**City**	**State**	**Zip code**
1095 AVENUE OF THE AMERI		NEW YORK	New York	10036

Clear

If the device is on the Verizon Network, this dialog will attempt to plot the location. If it is not online and the line has a last known coarse location, it will plot that instead. Otherwise, it will not plot the last known location.

This dialog will plot the current service address, if there is one set.

3. Click **Submit** to complete the process.

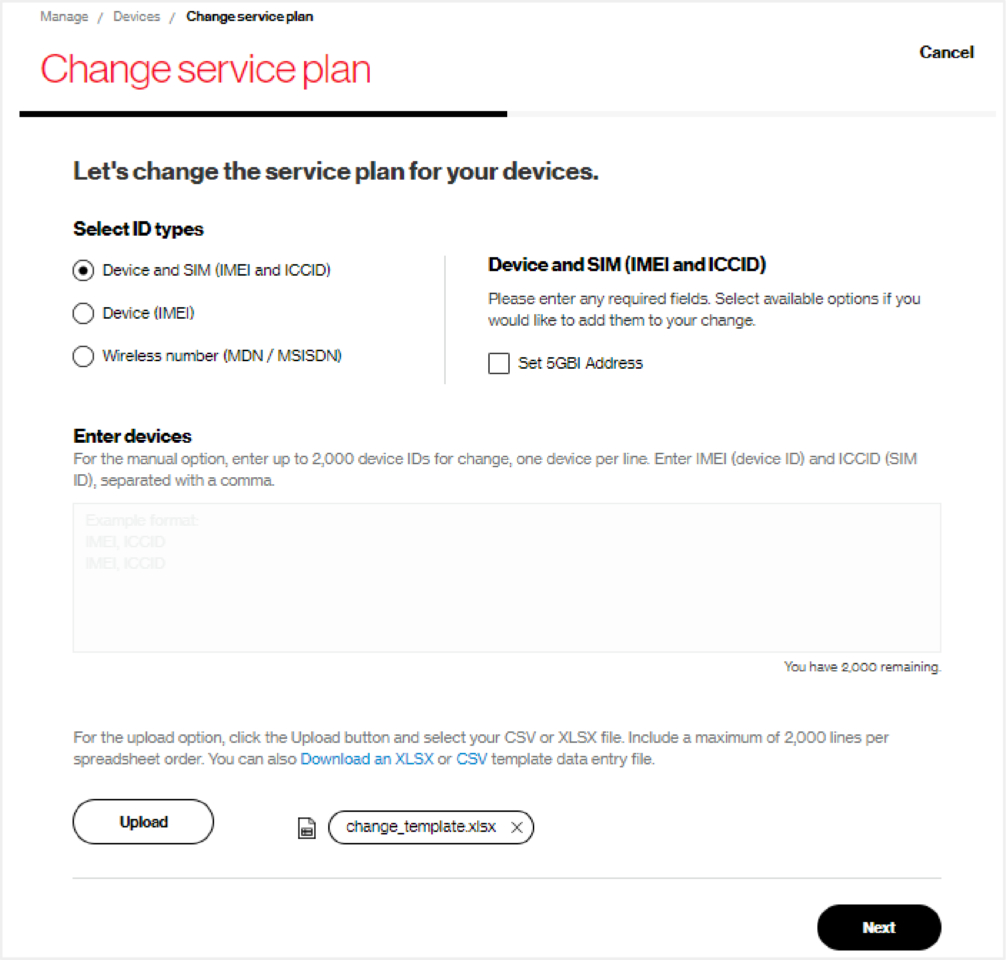
NOTE: Note: If this line is a 5G Business Internet line there will be a "Check 5G availability" option which must confirm the new address qualified for 5G Business Internet. If the new address doesn't qualify, you need to change the price plan and you can change/set the address at that time.

4. Check the status of the transaction(s) in the **Logs.**

Change service plan

How to change service plans in bulk

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



Manage / Devices / **Change service plan**

Change service plan

Cancel

Let's change the service plan for your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Device and SIM (IMEI and ICCID)

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

□ Set 5GBI Address

Enter devices

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

Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

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

Upload

change_template.xlsx ×

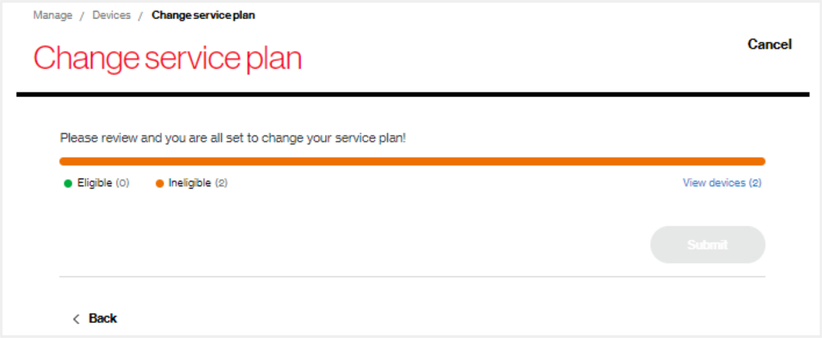
Next

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).

NOTE: Note: If you are changing to a 5G Business Internet plan, you have the option to change the service address.

3. Type the IDs or upload a file of up to 2,000 devices.

4. Click **Next**. A review dialog opens.



Change service plan

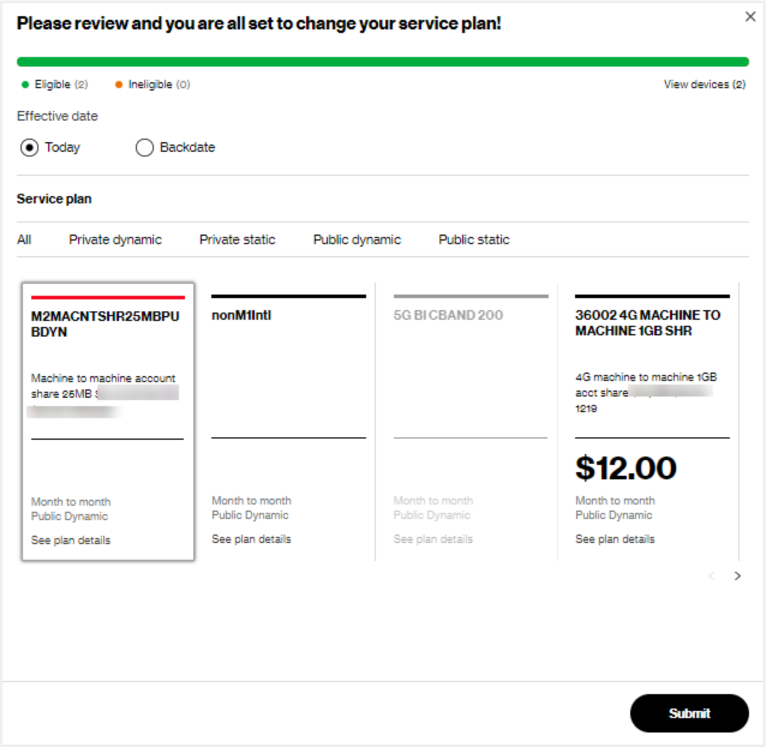
Please review and you are all set to change your service plan!

5. Review eligible or ineligible devices.
6. Click **Submit** to complete the process.
7. Check the status of the transaction(s) in the **Logs.**

Quick service plan changes

How to make quick plan changes on selected devices

1. Select devices using the *Device identifier* checkboxes. All selected devices must be from the same billing account.
2. Click the actions icon and then select **Change service plan**. A review page opens.



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

Effective date

◉ Today ○ Backdate

Service plan

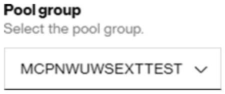
M2MACNTSHR25MBPU BDYN — Machine to machine account share 26MB [redacted] — Month to month, Public Dynamic — See plan details

nonM1Intl — Month to month, Public Dynamic — See plan details

5G BI CBAND 200 — Month to month, Public Dynamic — See plan details

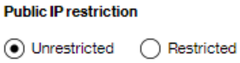
36002 4G MACHINE TO MACHINE 1GB SHR — 4G machine to machine 1GB acct share [redacted] 1219 — $12.00 — Month to month, Public Dynamic — See plan details

3. Review eligible and ineligible device counts.
4. Note: If you choose a 5G Business Internet plan which requires address qualification, you must enter an address for those plans. ThingSpace will perform an address qualification during the plan change.
5. 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.
6. Assign a Service plan for the devices. You can filter the service plans by clicking **Private dynamic, Private static, Public dynamic**, or **Public static**.
    a. 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.



Pool group
Select the pool group.
MCPNWUWSEXTTEST

    b. 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.



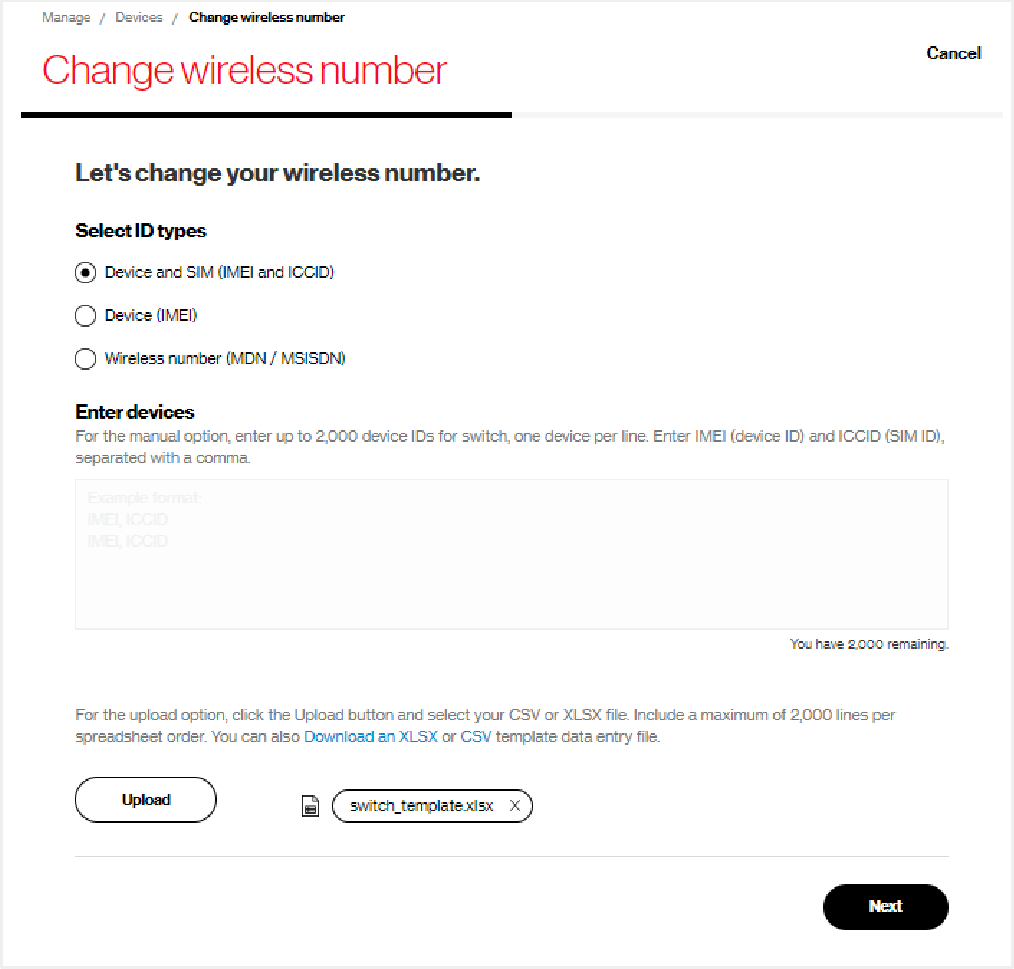
Public IP restriction
● Unrestricted ○ Restricted

7. Check **Continue** with eligible devices if necessary to proceed.
8. Click **Submit** to complete the process.
9. Check the status of the transaction(s) in the **Logs.**

Change wireless number

How to change wireless numbers in bulk

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



Manage / Devices / **Change wireless number**

Change wireless number

Cancel

Let's change your wireless number.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Enter devices

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

Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

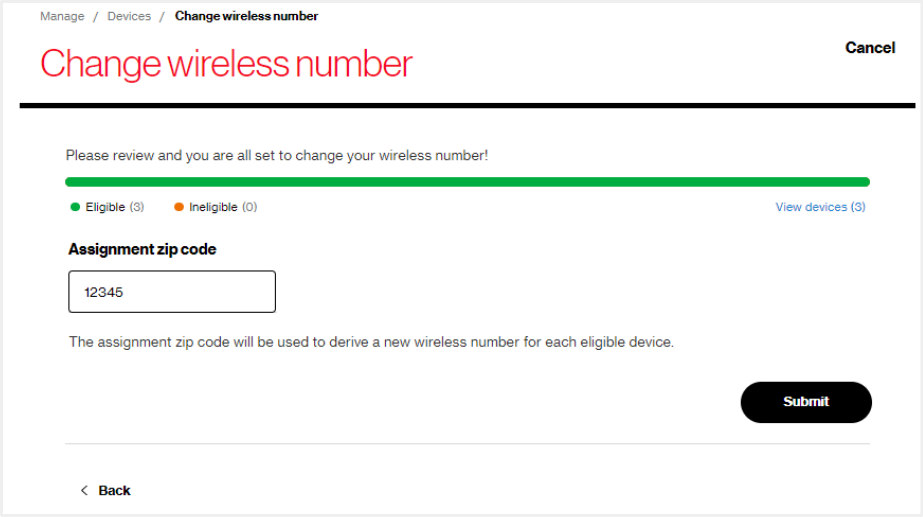
For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also Download an XLSX or CSV template data entry file.

Upload

switch_template.xlsx X

Next

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
4. Click **Next**. A review dialog opens next.



Change wireless number

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

● Eligible (3) ● Ineligible (0)

Assignment zip code: 12345

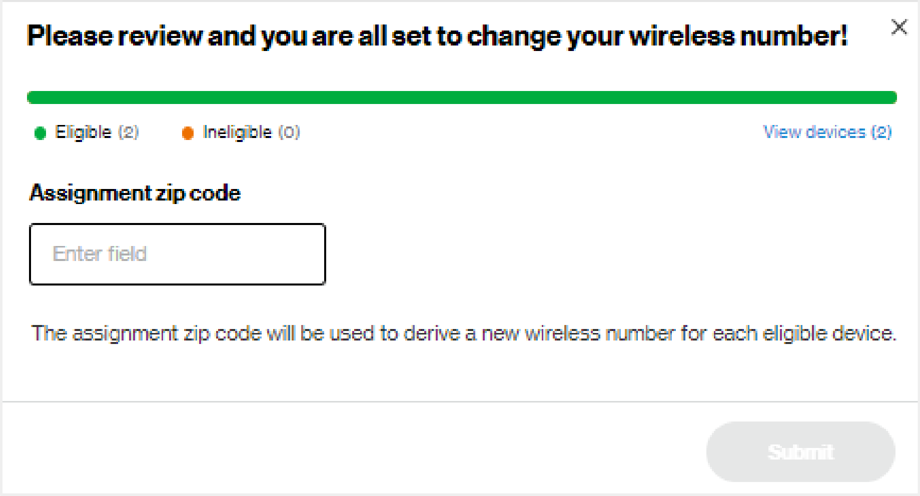
The assignment zip code will be used to derive a new wireless number for each eligible device.

5. Review eligible and ineligible devices.
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

1. Select devices using the *Device identifier* checkboxes. All selected devices must be from the same billing account.
2. Click the actions icon and then select **Change wireless number**. A review page opens.



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

● Eligible (2) ● Ineligible (0)

Assignment zip code: Enter field

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

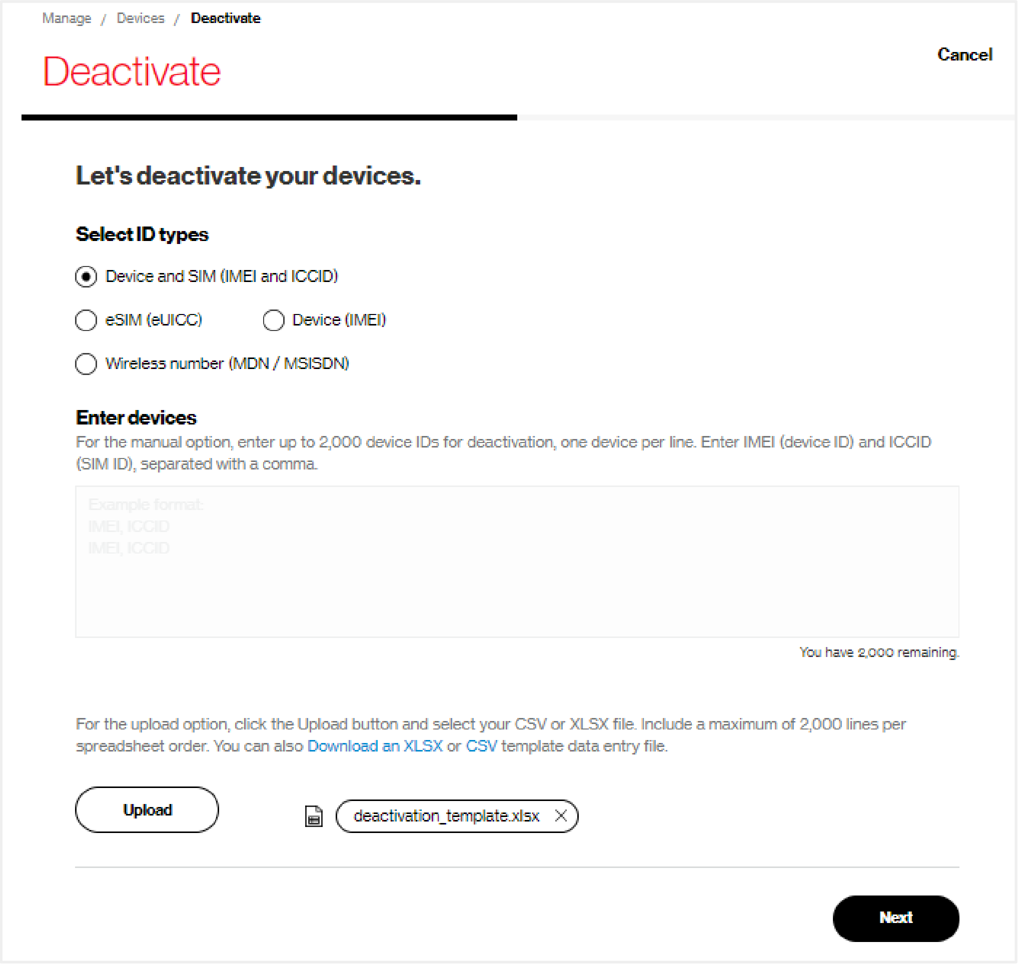
3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.

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.

Deactivate devices

How to deactivate devices in bulk

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



Manage / Devices / **Deactivate**

Deactivate

Cancel

Let's deactivate your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ eSIM (eUICC) ○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Enter devices

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

Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

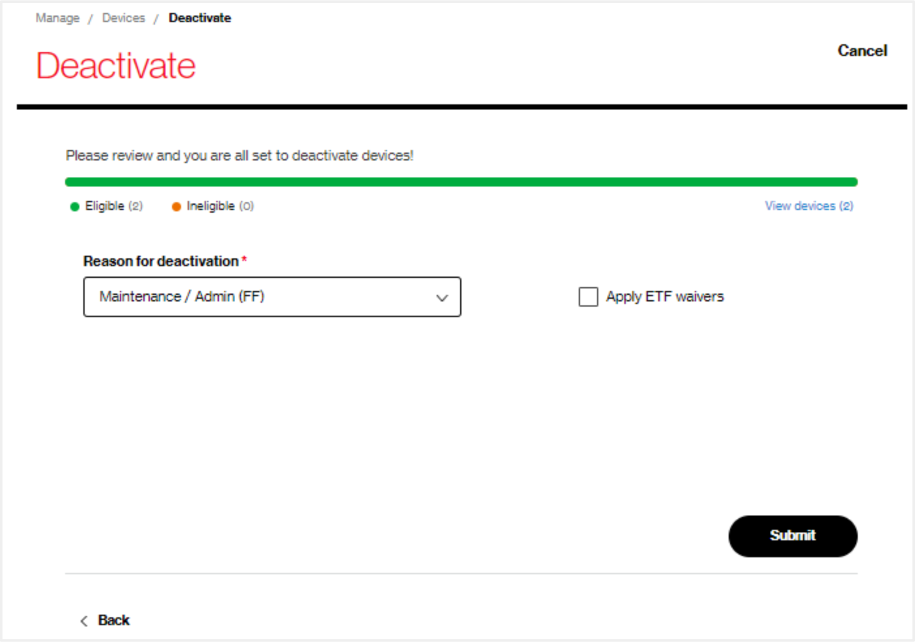
For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also Download an XLSX or CSV template data entry file.

Upload

deactivation_template.xlsx ✕

Next

2. Select the ID types to use (Device and SIM, eSIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
4. Click **Next**. A review dialog opens.



Please review and you are all set to deactivate devices!

● Eligible (2) ● Ineligible (0)

Reason for deactivation *: Maintenance / Admin (FF)

□ Apply ETF waivers

5. Review eligible and ineligible devices.
6. Select a **Reason for deactivation**. Available reason codes are:
    a. No Signal / Coverage Issue (A4)
    b. Competitor Promotion (BC)
    c. Employer Change (F2)
    d. Maintenance / Admin (FF)
    e. Financial Hardship (JJ)
    f. 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.

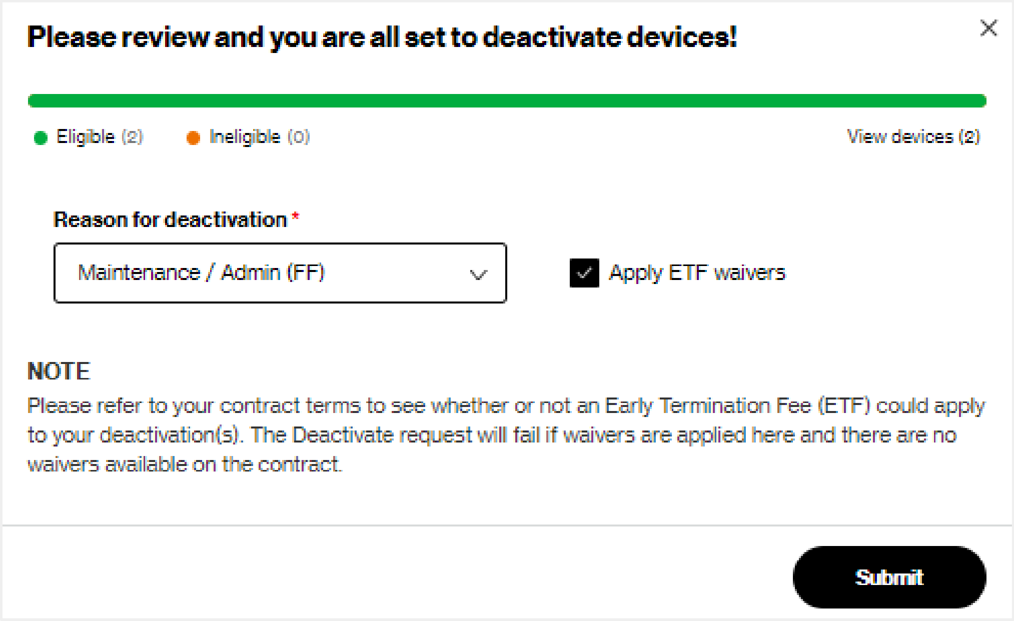
8. Check **Continue with eligible** devices if necessary to proceed.
9. Click **Submit** to complete the process.

Quick deactivating devices

How to quickly deactivate devices

1. Select devices using the *Device identifier* checkboxes. You must select devices from the same billing account.

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



Please review and you are all set to deactivate devices!

● Eligible (2) ● Ineligible (0) View devices (2)

Reason for deactivation *

Maintenance / Admin (FF)

☑ Apply ETF waivers

NOTE

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

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:
   a. No Signal / Coverage Issue (A4)
   b. Competitor Promotion (BC)
   c. Employer Change (F2)
   d. Maintenance / Admin (FF)
   e. Financial Hardship (JJ)
   f. Customer Guarantee (PP)
5. Check **Apply ETF waivers** if applicable.

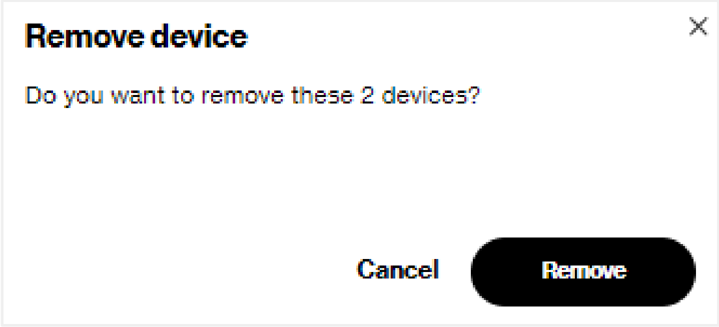
   NOTE: Please refer to your contract terms to verify if an Early Termination Fee (ETF) applies to your deactivation(s). If you apply waivers here and there are no waivers available on the contract, the Deactivate request fails.

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

Delete/Remove devices

How to quickly remove devices from your plan

1. Select the *Device identifier* checkbox of the devices to remove. You must select devices in a **Pre-active** or **Deactive** state.
2. Click the actions icon ⤧ and then select **Delete**. You will be prompted to confirm removal.



Remove device

Do you want to remove these 2 devices?

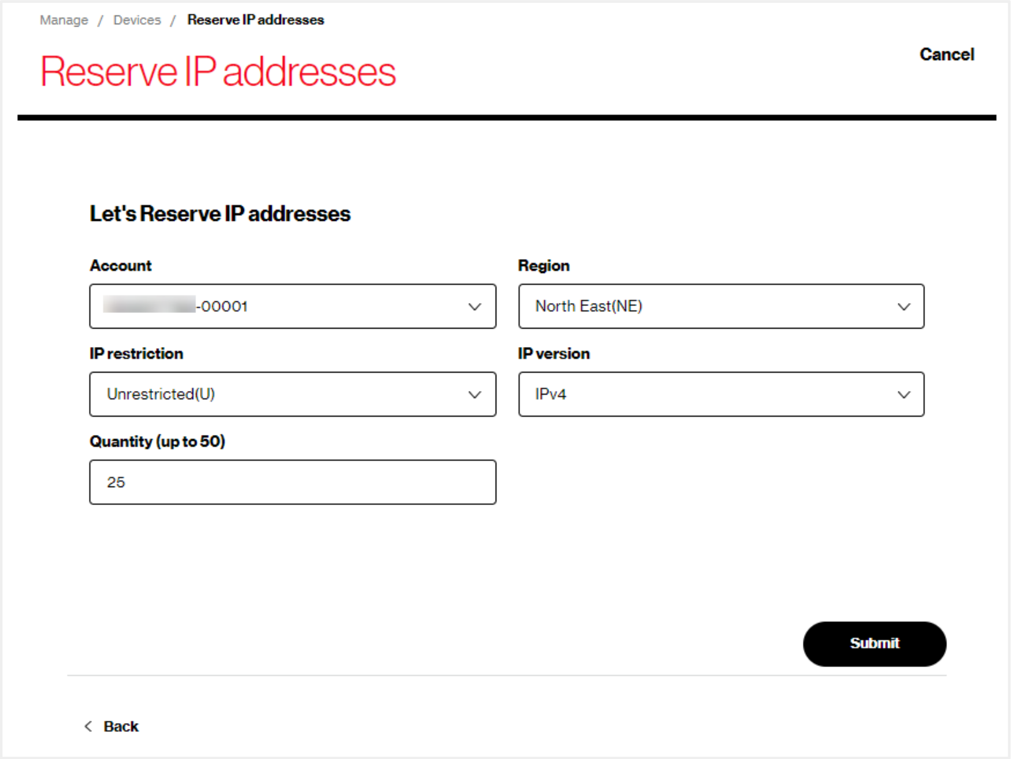
3. Click **Remove**.

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

Reserve IP addresses

How to quickly reserve IP Addresses

1. With no devices selected, click the actions icon ✥ then select **Reserve IP addresses**. The *Reserve IP addresses* page opens.



Reserve IP addresses

Let's Reserve IP addresses

Account: [redacted]-00001

Region: North East(NE)

IP restriction: Unrestricted(U)

IP version: IPv4

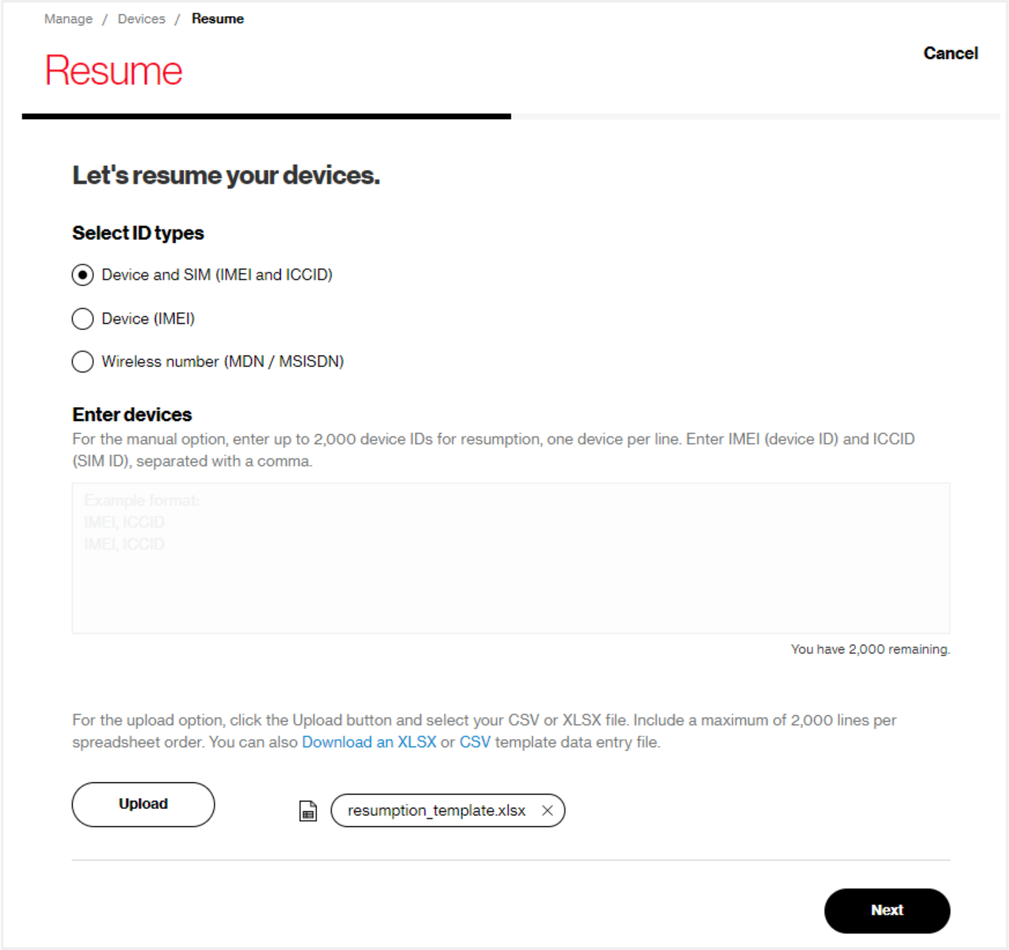
Quantity (up to 50): 25

2. Select an Account number.
3. Select a Region. Available Regions are:
    a. Headquarters (HQ)
    b. Mid West (MW)
    c. North East (NE)
    d. South (SO)
    e. West (WE)
4. Select an IP restriction: Restricted IPs, Unrestricted IPs.
5. Select an IP version: IPv4, IPv6
6. Click **Submit** to complete the process.

Resume devices

How to resume devices in bulk

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



Manage / Devices / **Resume**

Resume

Cancel

Let's resume your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Enter devices

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

Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

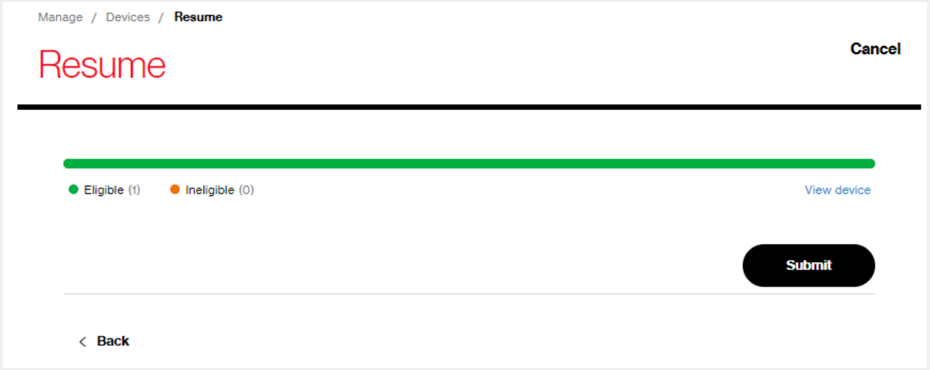
For the upload option, click the Upload button and select your CSV or XLSX file. Include a maximum of 2,000 lines per spreadsheet order. You can also Download an XLSX or CSV template data entry file.

Upload

resumption_template.xlsx ×

Next

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs or upload a file of up to 2,000 devices.
4. Click **Next**. A review dialog opens next.

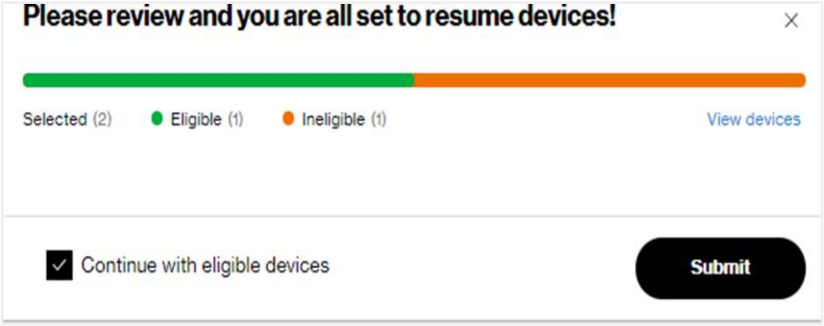


5. Review eligible and ineligible devices.
6. Check **Continue with eligible devices** if necessary to proceed.
7. Click **Submit** to complete the process.

Quick resuming devices

How to quickly resume devices

1. Select devices using the *Device identifier* checkboxes. All selected devices must be from the same billing account.
2. Click the actions icon ✥ then select **Resume**. A review page opens.


Please review and you are all set to resume devices!
×
Selected (2)
● Eligible (1)
● Ineligible (1)
View devices
☑ Continue with eligible devices
Submit

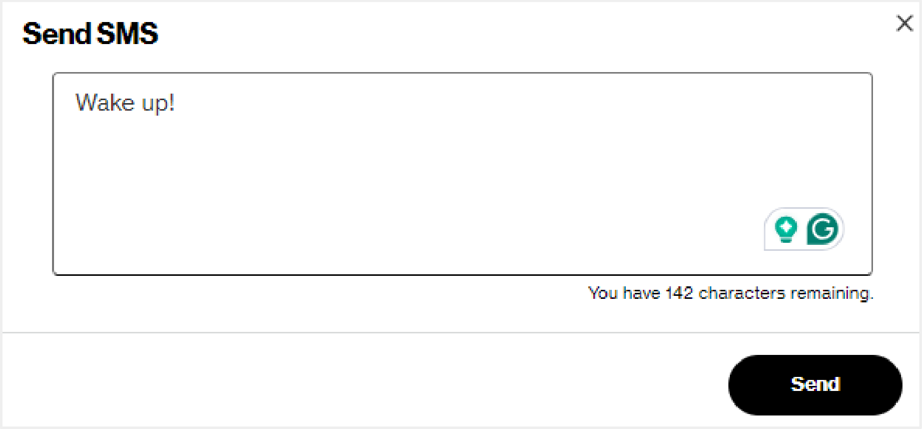
3. Review eligible and ineligible devices counts. To view the list of selected devices, click `View devices`.
4. Check **Continue with eligible devices** if necessary to proceed.
5. Click **Submit** to complete the process.

Send an SMS

How to quickly send an SMS to a device

1. Select devices using the *Device identifier* checkboxes. Note that you can only send an SMS to one device at a time.

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



Send SMS

Wake up!

You have 142 characters remaining.

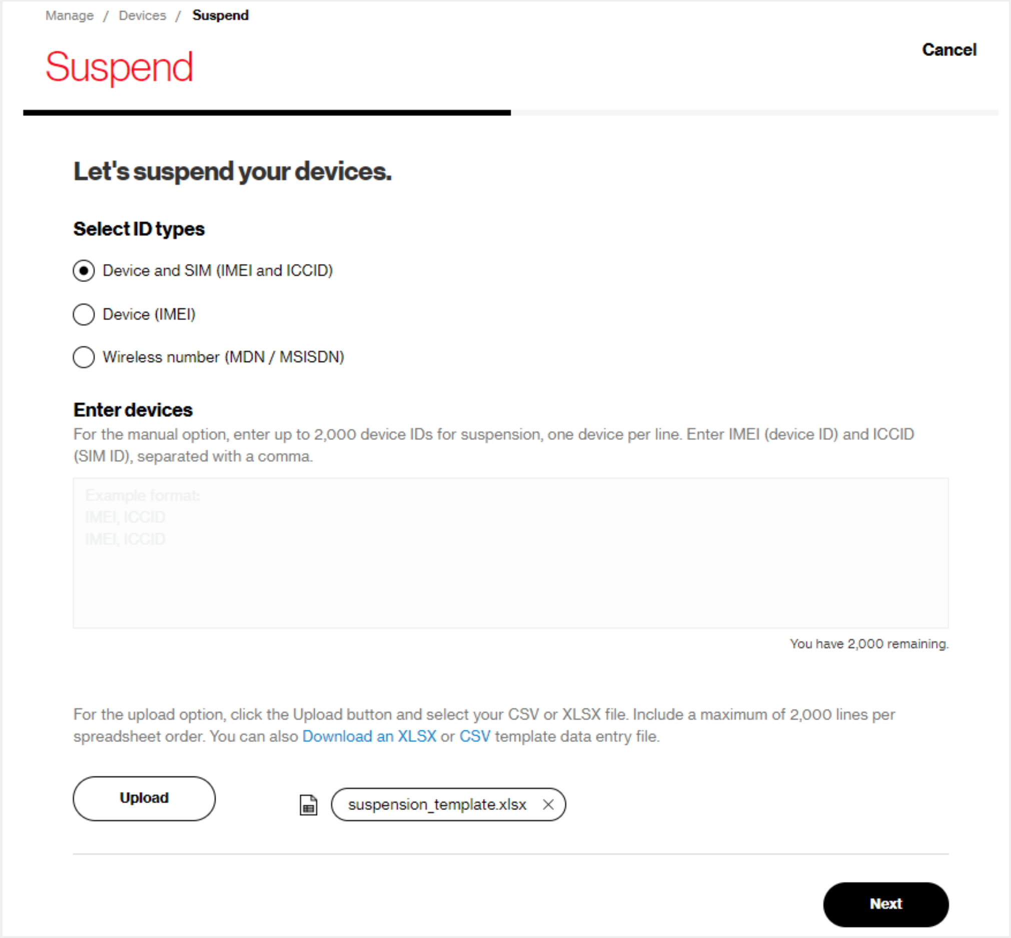
3. Type the message up to a maximum of 150 characters.

4. Click **Send** to complete the process.

Suspend devices

How to suspend devices in bulk

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



Manage / Devices / Suspend

Suspend

Let's suspend your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Enter devices

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

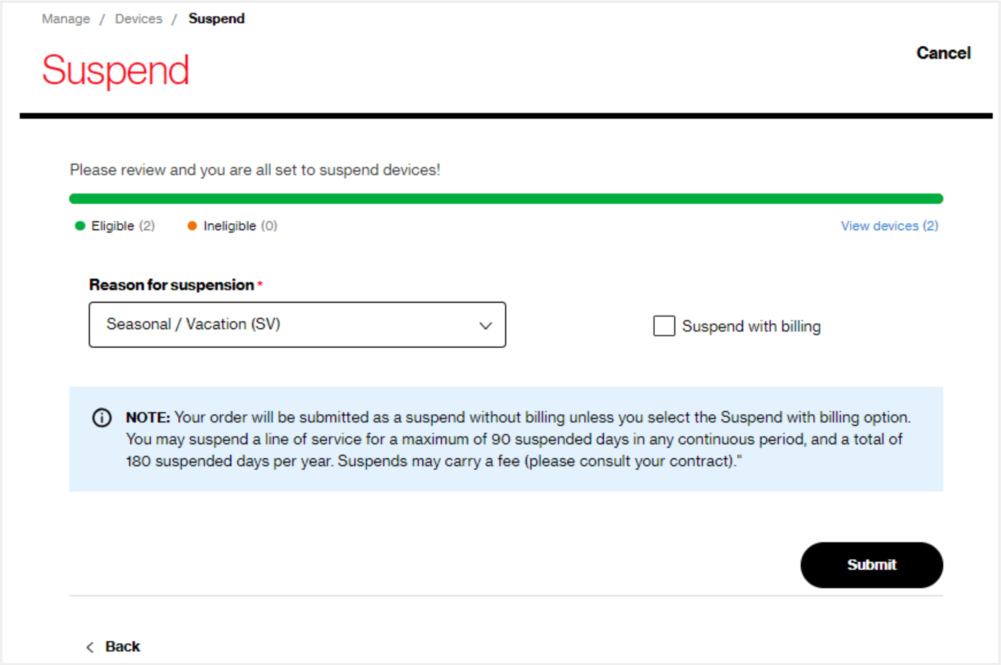
Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

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

suspension_template.xlsx

2. Select the ID types to use (Device and SIM, Device only, or Wireless number).
3. Type the IDs, or upload a file of up to 2,000 devices.
4. Click **Next**. A review page opens next.



Suspend

Please review and you are all set to suspend devices!

● Eligible (2) ● Ineligible (0) View devices (2)

Reason for suspension *

Seasonal / Vacation (SV)

□ Suspend with billing

ⓘ **NOTE:** Your order will be submitted as a suspend without billing unless you select the Suspend with billing option. You may suspend a line of service for a maximum of 90 suspended days in any continuous period, and a total of 180 suspended days per year. Suspends may carry a fee (please consult your contract)."

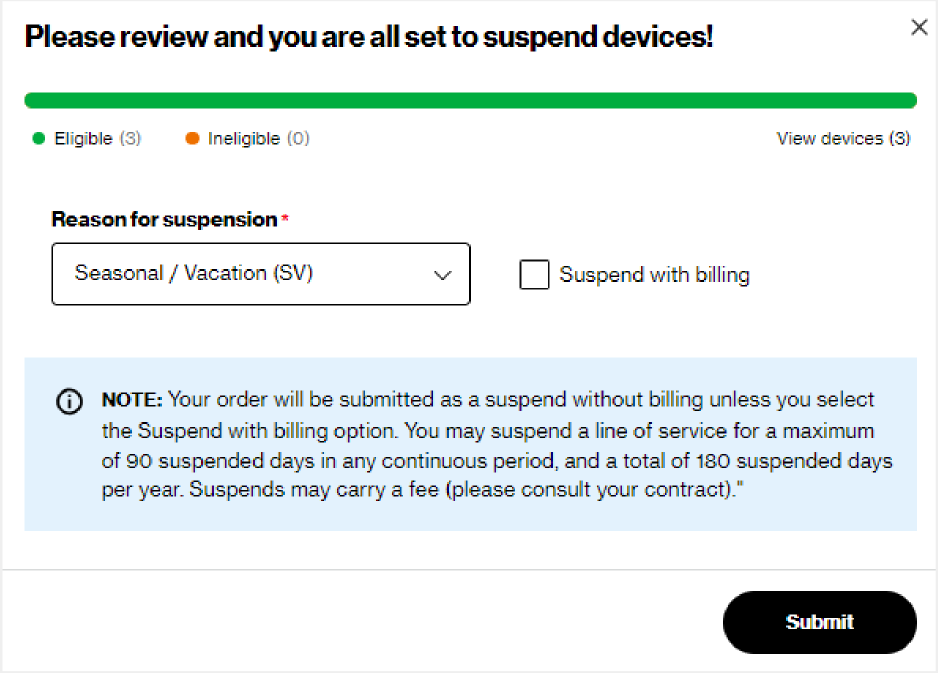
5. Review the eligible or ineligible devices.
6. Select a **Reason for suspension**. Available reason codes are:
   a. Lost / Stolen (21)
   b. Seasonal / Vacation (SV)
7. Check **Suspend with billing**. If not checked, the devices are suspended without billing.
8. Check **Continue with eligible devices**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

Quick suspending devices

How to quickly suspend devices

1. Select devices using the *Device identifier* checkboxes. All selected devices must be from the same billing account.

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



Please review and you are all set to suspend devices!

● Eligible (3) ● Ineligible (0) View devices (3)

Reason for suspension *

Seasonal / Vacation (SV)

□ Suspend with billing

NOTE: Your order will be submitted as a suspend without billing unless you select the Suspend with billing option. You may suspend a line of service for a maximum of 90 suspended days in any continuous period, and a total of 180 suspended days per year. Suspends may carry a fee (please consult your contract)."

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:

   a. Lost / Stolen (21)

   b. Seasonal / Vacation (SV)

5. Check **Suspend with billing**. If not checked, the devices are suspended without billing.

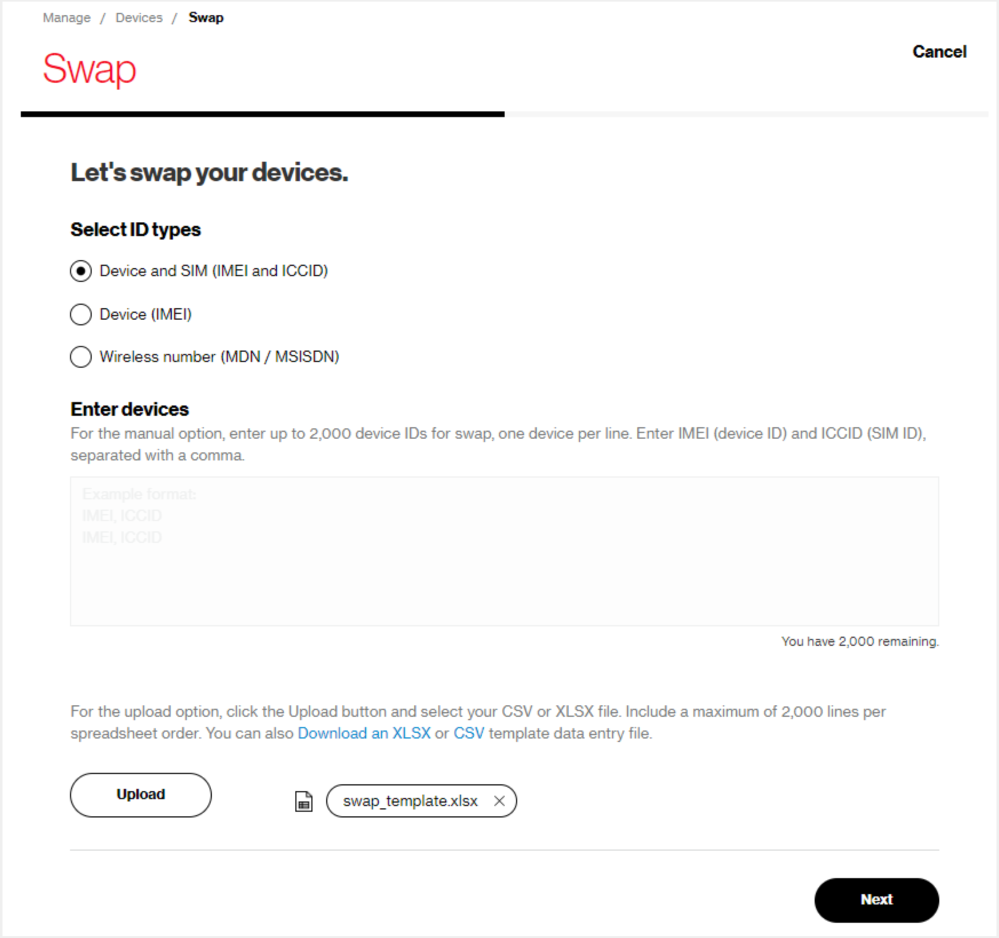
6. Check **Continue with eligible devices** if necessary to proceed.

7. Click **Submit** to complete the process.

Swap devices

How to swap devices in bulk

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



Manage / Devices / **Swap**

Swap

Cancel

Let's swap your devices.

Select ID types

● Device and SIM (IMEI and ICCID)

○ Device (IMEI)

○ Wireless number (MDN / MSISDN)

Enter devices

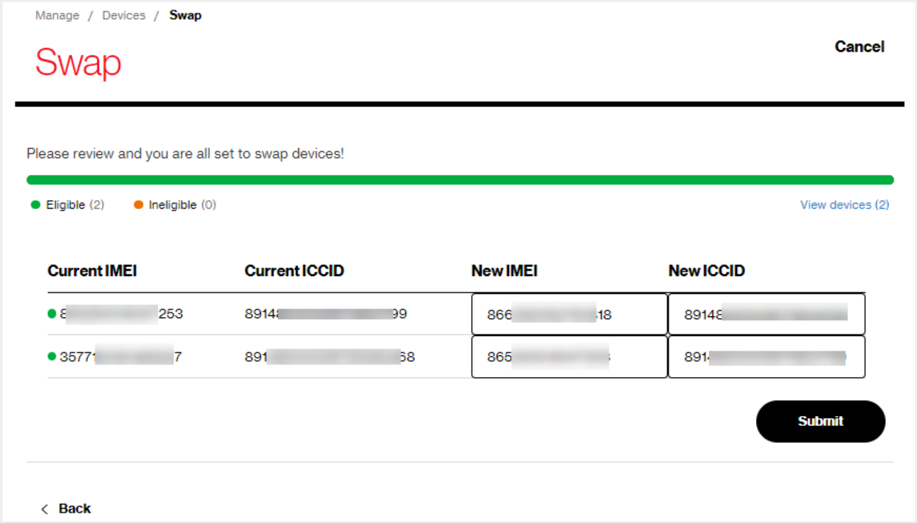
For the manual option, enter up to 2,000 device IDs for swap, one device per line. Enter IMEI (device ID) and ICCID (SIM ID), separated with a comma.

Example format:
IMEI, ICCID
IMEI, ICCID

You have 2,000 remaining.

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

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.
4. Click **Next** to continue. A review dialog opens next.



Swap

Please review and you are all set to swap devices!

● Eligible (2) ● Ineligible (0) View devices (2)

Current IMEI	Current ICCID	New IMEI	New ICCID
● [redacted]	[redacted]	[redacted]	[redacted]
● [redacted]	[redacted]	[redacted]	[redacted]

5. Review eligible and ineligible devices.

6. Enter a new **IMEI** or **ICCID** for each device you want to swap.

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

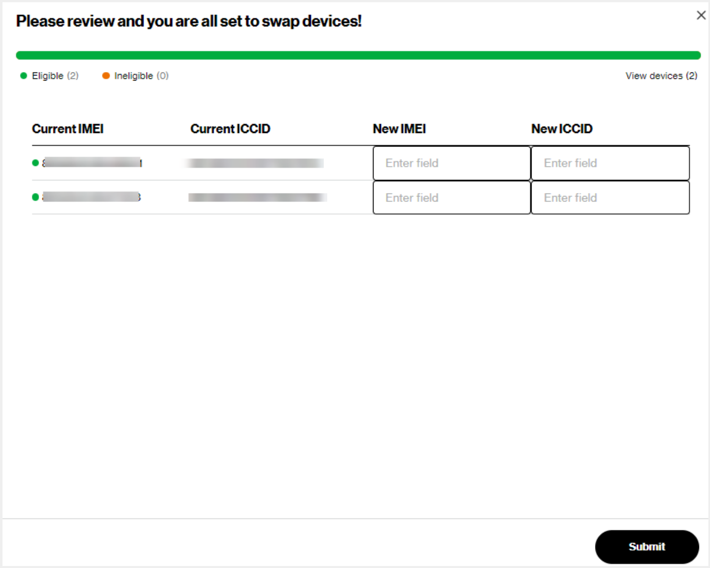
8. Click **Submit** to complete the process.

Quick swapping of devices

How to quickly swap devices

1. Select devices using the *Device identifier* checkboxes. All selected devices must be from the same billing account.

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



Please review and you are all set to swap devices!

● Eligible (2) ● Ineligible (0) View devices (2)

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

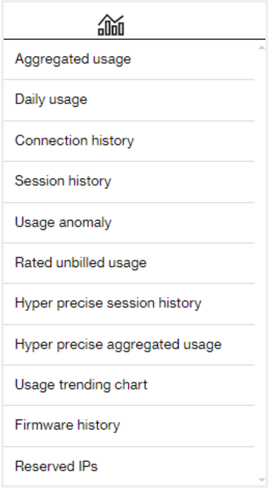
3. Review eligible and ineligible device counts. To view the list of selected devices, click **View devices**.
4. Enter a new IMEI or ICCID for each device you want to swap.
5. Check **Continue with eligible devices** if necessary to proceed.
6. Click **Submit** to complete the process.

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

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

Firmware history – Report to firmware changes as a result of firmware over the air (FOTA) campaigns in ThingSpace for a device.

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).

Rated unbilled usage – View rated usage per device for the current billing cycle (to appear on the next bill).

Reserved IPs –View a list of reserved IP addresses.

Session history – Monitor a device's session history.

Usage anomaly – Monitor usage anomalies.

Usage trending chart – View the total usage by day for a device in a graph.

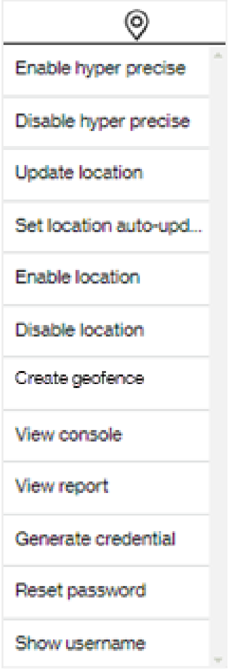
When you select a report, the Reports page opens to present further selection criteria.

Location actions

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

How to take Location actions

1. Select devices using the *Device identifier* checkboxes.
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 on the selected devices.

Disable hyper precise – Disables Hyper Precise Location on the selected devices.

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 on the selected devices.

Disable location – Disables location updates on the selected devices.

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.

Generate credential – Generates credentials.

Reset password – Resets the password.

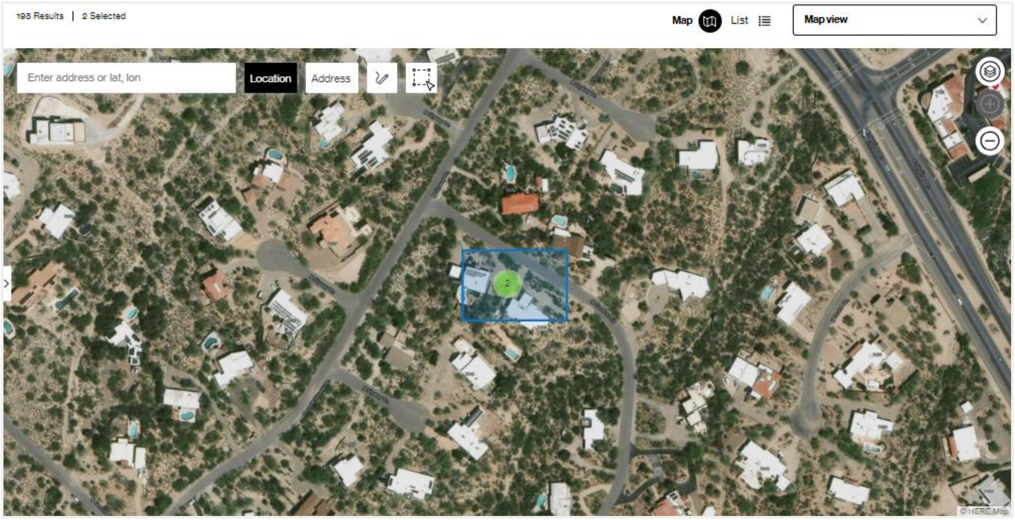
Show username – Shows the username.

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.

How to create a geofence

1. Select **Map view** from the dropdown or click on the Map icon Map 🕮. The devices that are enabled for location will be shown on the map.
2. Select the devices to create a geofence around.
   a. Click one of the drawing tools ✎ ⬚
   b. Click and drag on the map to form the geofence. This automatically selects any devices within the geofence. Use the drawn shape for all selected devices, or you can specify a radius to create an individual geofence circle around each selected device.

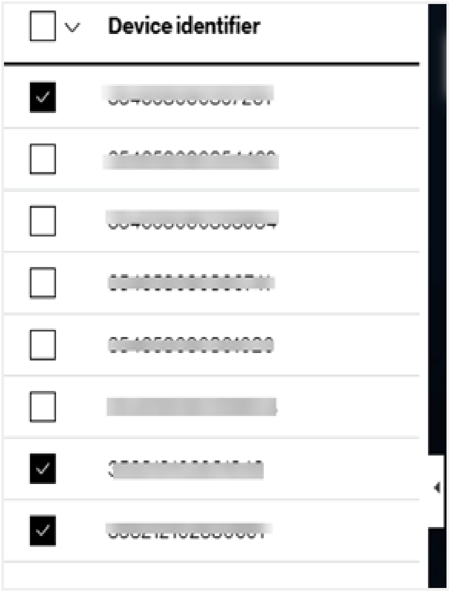


198 Results | 2 Selected

Map view

NOTE: Devices must be from the same billing account.

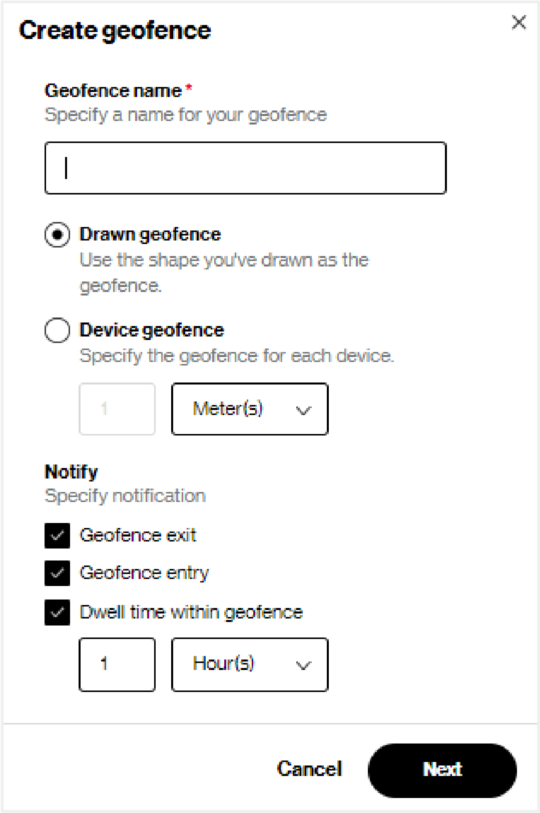
   c. Click devices on the map, or open the list with the icon › to select / unselect the device identifiers.



□	Device identifier
☑	[redacted]
□	[redacted]
□	[redacted]
□	[redacted]
□	[redacted]
□	[redacted]
☑	[redacted]
☑	[redacted]

d. Verify all devices to include for the alert are selected.

3. Choose **Create geofence** from the Location actions menu. The *Create geofence* dialog opens.



Create geofence

Geofence name *
Specify a name for your geofence

● **Drawn geofence**
Use the shape you've drawn as the geofence.

○ **Device geofence**
Specify the geofence for each device.
1 Meter(s)

Notify
Specify notification

☑ Geofence exit

☑ Geofence entry

☑ Dwell time within geofence
1 Hour(s)

c. For **Geofence name**, type a descriptive label.

d. Choose how to create the geofence.

i. Drawn geofence – draw the geofence in a map.

   ii. Device geofence – specify the geofence for each device based on distance.

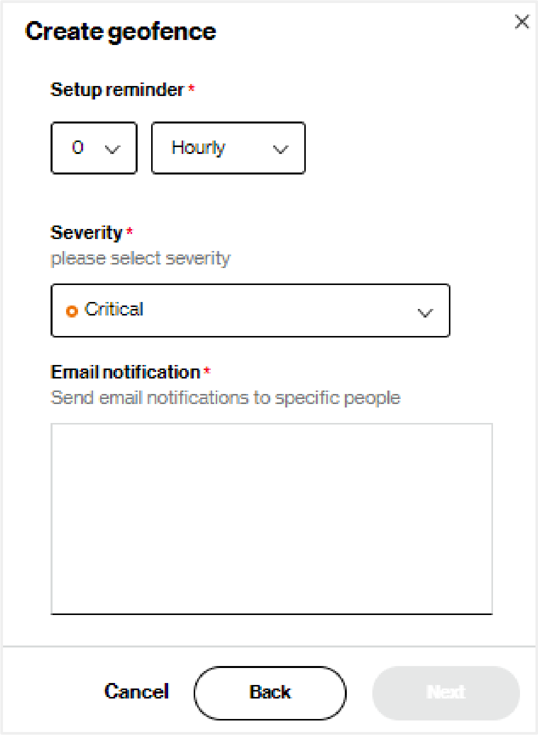
e. Select notification trigger.

   i. **Geofence exit** – sends a notification when the device exits the geofence.

   ii. **Geofence entry** – sends a notification when the device enters the geofence.

   iii. **Dwell time within geofence** – sends a notification when the device stays within the geofence for a set period of time.

f. Click **Next**. Another dialog opens.



Create geofence

Setup reminder *

0 Hourly

Severity *

please select severity

Critical

Email notification *

Send email notifications to specific people

g. Setup reminder – sends a reminder depending on how you set this option up.

h. Severity – Select the severity of this geofence. The severity is included in the notification email.

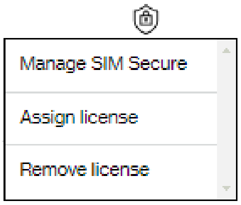
i. Email notification – Type the notification recipient's email addresses.

4. Click **Next** to continue back to the map.

5. Click **Save** to save the geofence.

SIM Secure actions

For customers that are subscribed to SIM Secure Services, you can easily assign SIM Secure licenses to up to 500 devices at a time. The following menu items are available:



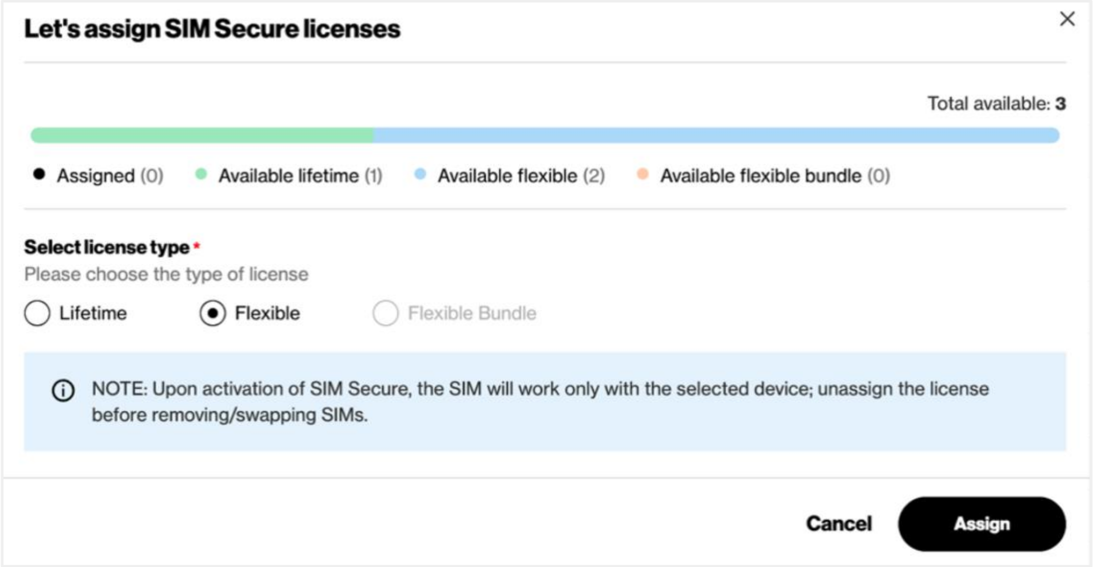
Manage SIM Secure

Selecting the Manage SIM Secure option will display the Legacy Manage SIM Secure page.

Assigning and removing licenses

How to assign a license

1. Select devices using the *Device identifier* checkboxes.
2. Click the security icon 🔒.
3. Select **Assign license**. This assigns a SIM Secure license to the selected devices (assuming there are any to assign).
4. A dialog box appears showing the available license types



Let's assign SIM Secure licenses

Total available: **3**

● Assigned (0) ● Available lifetime (1) ● Available flexible (2) ● Available flexible bundle (0)

Select license type *

Please choose the type of license

○ Lifetime ● Flexible ○ Flexible Bundle

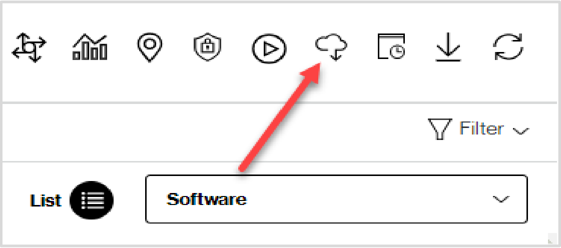
NOTE: Upon activation of SIM Secure, the SIM will work only with the selected device; unassign the license before removing/swapping SIMs.

How to remove a license

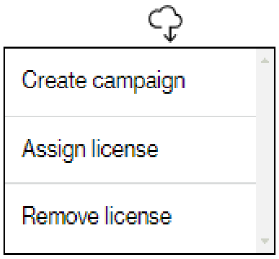
1. Select devices using the *Device identifier* checkboxes.
2. Click the security icon .
3. Select **Remove license**. This removes the SIM Secure licenses from the selected devices.

Software actions

When the table view selected is the Software view, subscribers of Software Management will see the Software icon as part of the action icons.



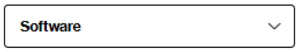
The following menu items are available:



Creating a campaign

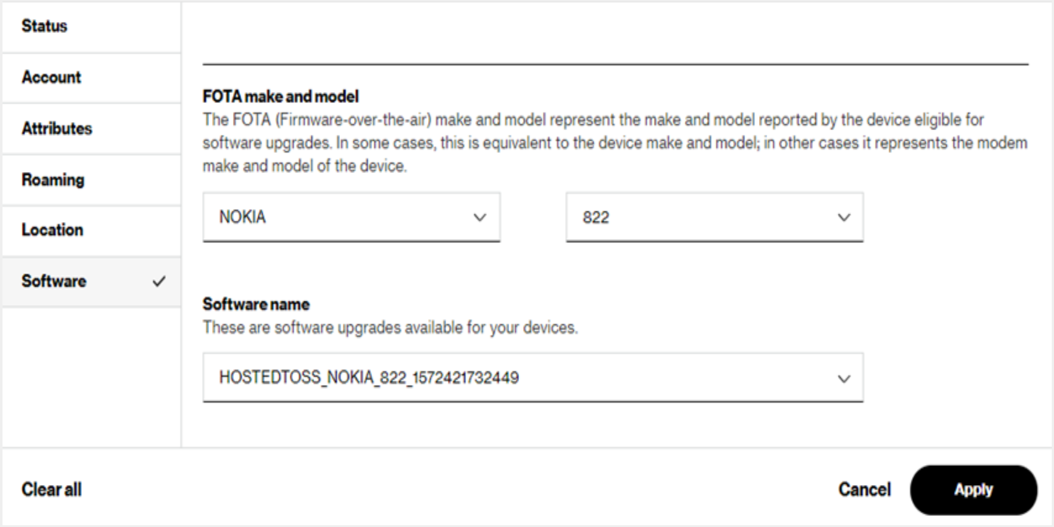
How to create a campaign

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



2. Click the filter icon Filter ⌄.

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



FOTA make and model
The FOTA (Firmware-over-the-air) make and model represent the make and model reported by the device eligible for software upgrades. In some cases, this is equivalent to the device make and model; in other cases it represents the modem make and model of the device.

NOKIA | 822

Software name
These are software upgrades available for your devices.

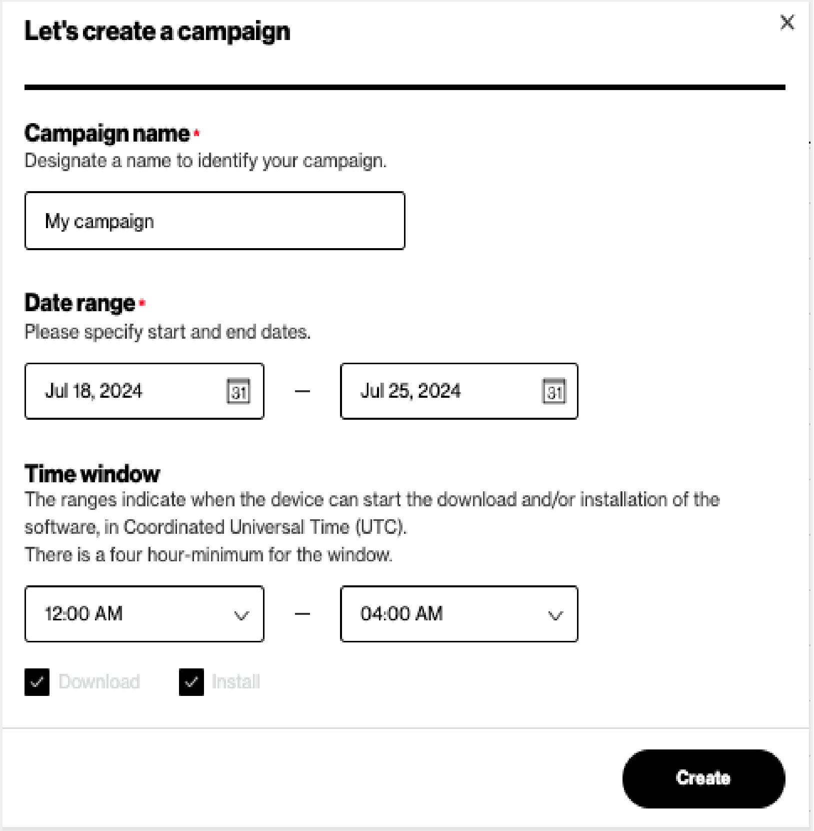
HOSTEDTOSS_NOKIA_822_1572421732449

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. In the devices list, select the IDs checkbox of the devices to include in the campaign.

7. Click the campaign icon and then select **Create campaign**. The *Let's create a campaign* dialog is displayed.


Let's create a campaign

Campaign name *
Designate a name to identify your campaign.

My campaign

Date range *
Please specify start and end dates.

Jul 18, 2024 – Jul 25, 2024

Time window
The ranges indicate when the device can start the download and/or installation of the software, in Coordinated Universal Time (UTC).
There is a four hour-minimum for the window.

12:00 AM – 04:00 AM

☑ Download ☑ Install

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

a. For **Campaign name**, type a name to identify your campaign.

b. Select the **Date range** for your campaign.

c. Optionally enter the time interval that indicates when the download and/or installation of the software can should occur.

d. Check **Download** to have the software downloaded to the device.

e. Check **Install** to have the software installed on the device.

f. To add additional time windows click **Add time window**.

8. Click **Create** to create the campaign.

Assigning and removing licenses

How to assign and remove licenses

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

Software

2. Click the campaign icon ☁ .

3. Select **Assign license**. This assigns a Software Management license to the devices selected (assuming there are any to assign).

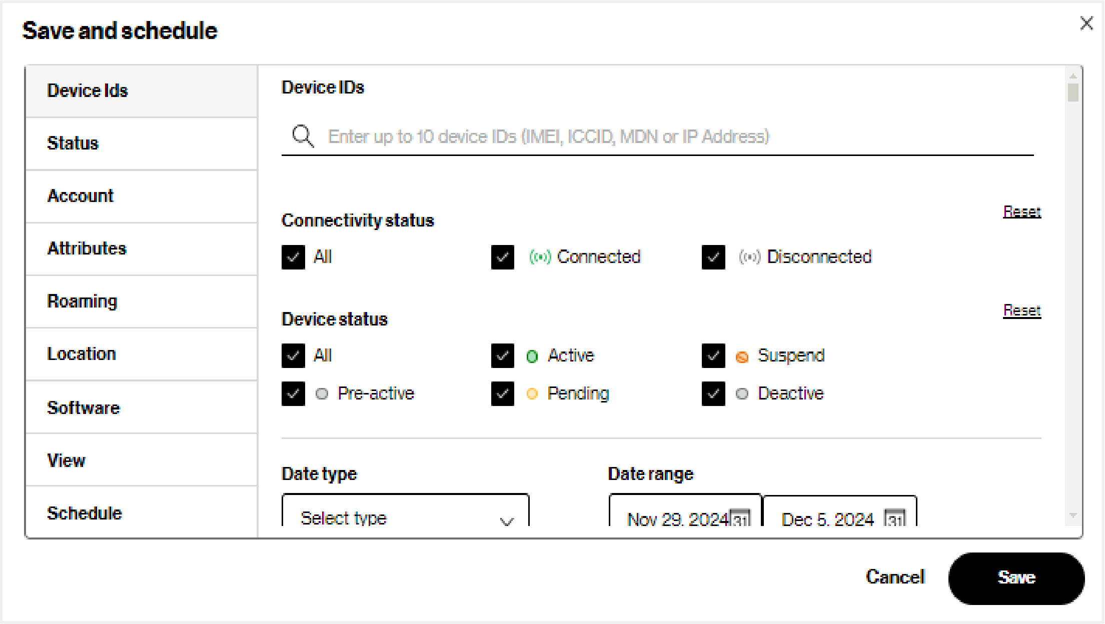
4. Select **Remove license**. This removes the Software Management license from the selected devices.

Schedule action

You can schedule to have your devices list available as a report that can be downloaded. You can also limit the report output by choosing from multiple options.

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

1. Click the schedule icon . The *Save and schedule* dialog opens.



Save and schedule

- Device Ids
- Status
- Account
- Attributes
- Roaming
- Location
- Software
- View
- Schedule

Device IDs

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

Connectivity status Reset

☑ All ☑ Connected ☑ Disconnected

Device status Reset

☑ All ☑ Active ☑ Suspend

☑ Pre-active ☑ Pending ☑ Deactive

Date type: Select type

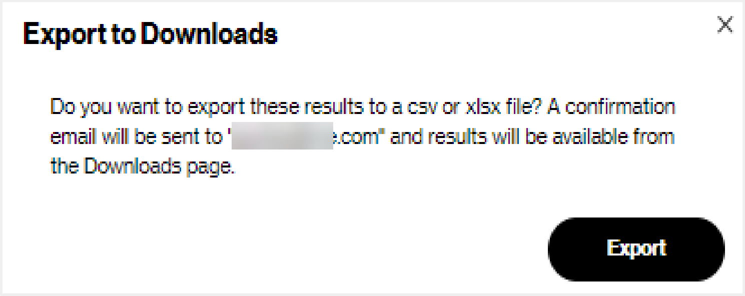
Date range: Nov 29, 2024 – Dec 5, 2024

2. Select from all of the available options to limit the report output.
   a. For **Name**, type a descriptive label for the devices report.
   b. Check **Schedule** to run this report at a predetermined date and time.
      (1) Select the Time period for your scheduled report.
      (2) Set the Frequency for the report to run.
      (3) Select an Expiration date for the report to end the schedule.
3. Click **Save** to complete the process.

Download action

How to export your devices list

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



Export to Downloads

Do you want to export these results to a csv or xlsx file? A confirmation email will be sent to '[redacted].com" and results will be available from the Downloads page.

2. Click **Export** to run the report. 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.

Reload page action

Click the reload icon ↻ to refresh the page.

Tutorial video actions

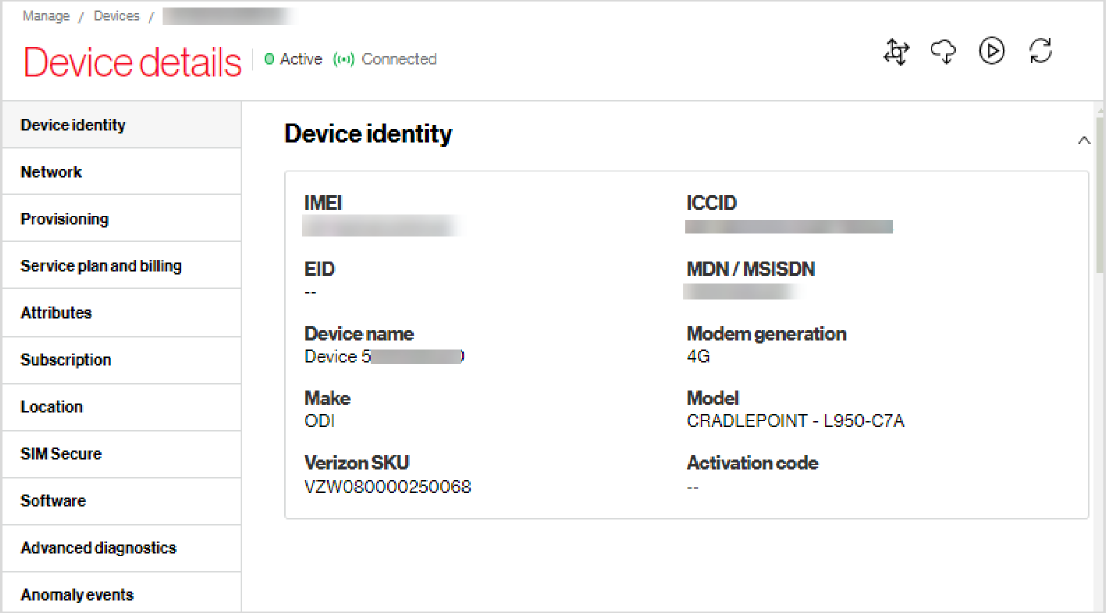
Click on the Tutorial videos icon ▷ and select from any of the available videos on the list.

Device details

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

To view device details

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



Device identity

IMEI
[redacted]

ICCID
[redacted]

EID
--

MDN / MSISDN
[redacted]

Device name
Device 5[redacted])

Modem generation
4G

Make
ODI

Model
CRADLEPOINT - L950-C7A

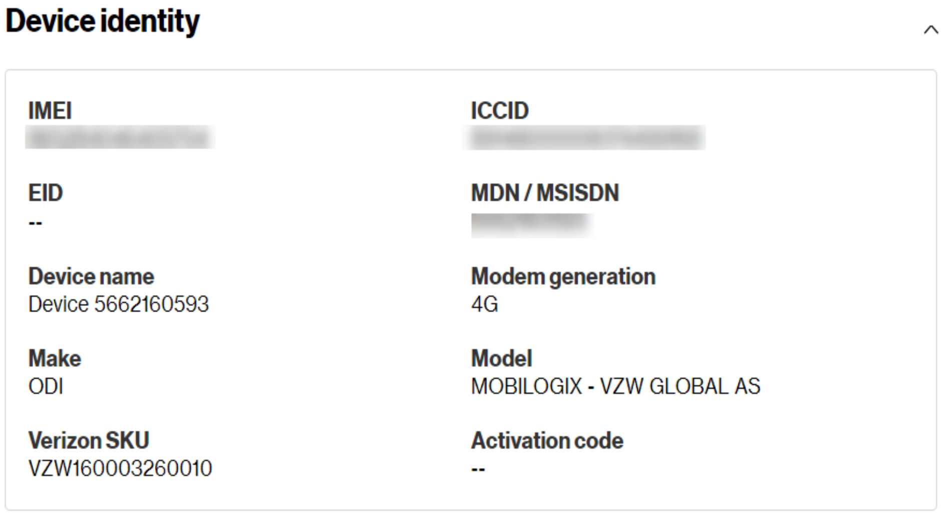
Verizon SKU
VZW080000250068

Activation code
--

2. Use the tabs on the left 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. The following information is available in the Device details page.

Device identity section

The *Device identity* section provides the following details:



Device identity

IMEI
[redacted]

ICCID
[redacted]

EID
--

MDN / MSISDN
[redacted]

Device name
Device 5662160593

Modem generation
4G

Make
ODI

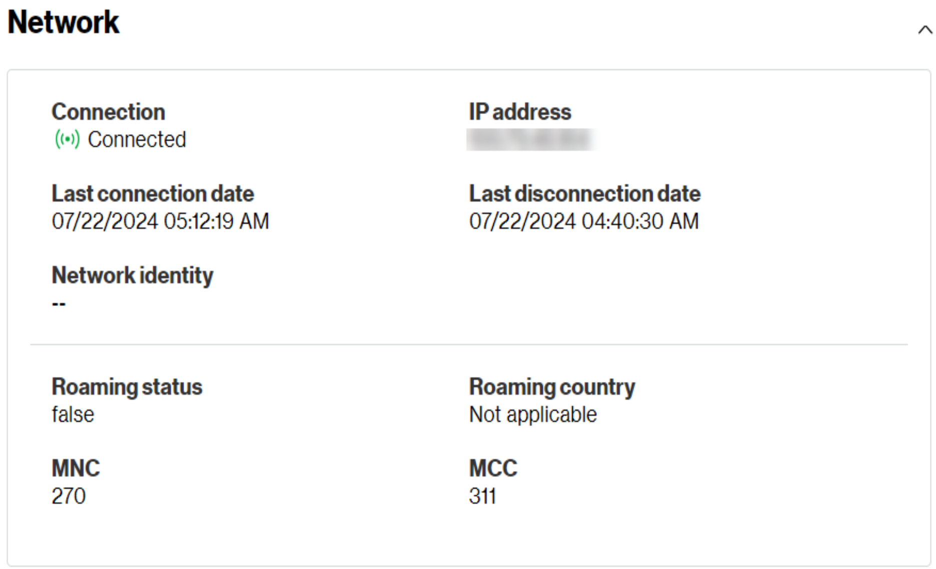
Model
MOBILOGIX - VZW GLOBAL AS

Verizon SKU
VZW160003260010

Activation code
--

Network section

The *Network* section provides the following details:



Network

Connection
((•)) Connected

IP address
[redacted]

Last connection date
07/22/2024 05:12:19 AM

Last disconnection date
07/22/2024 04:40:30 AM

Network identity
--

Roaming status
false

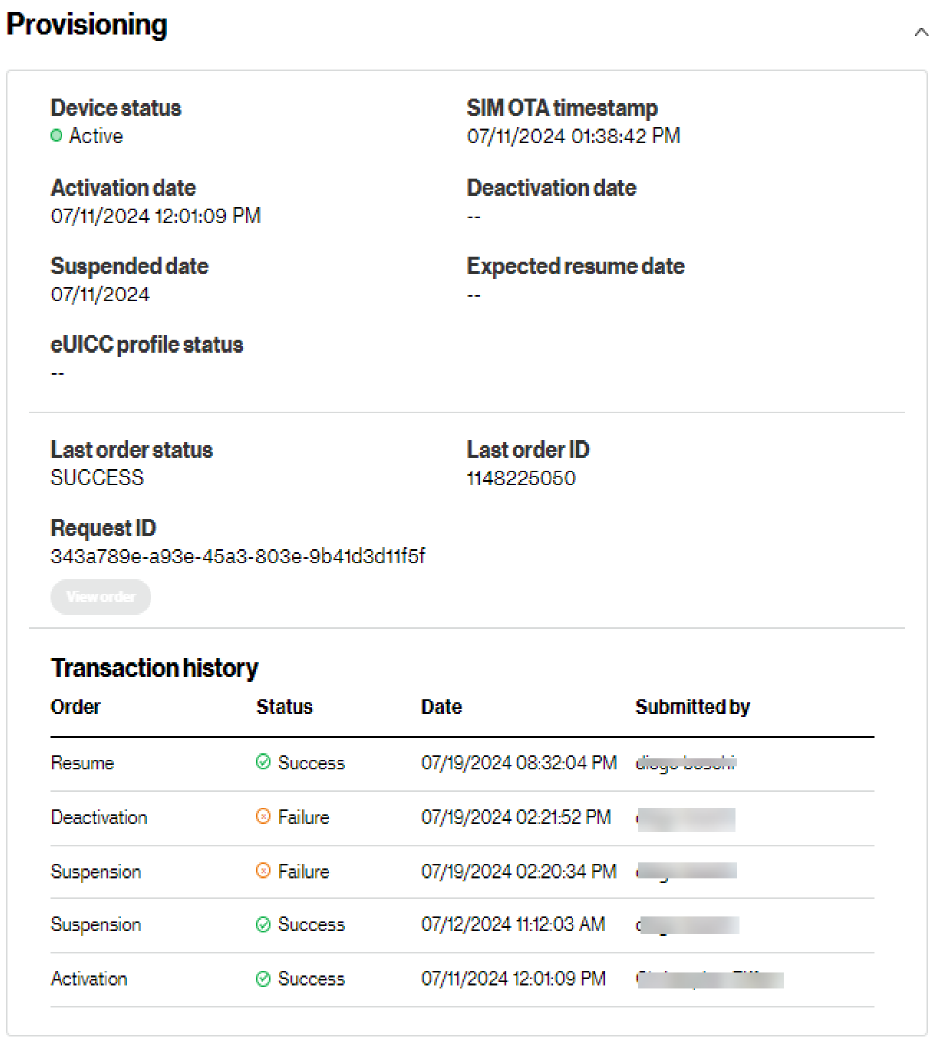
Roaming country
Not applicable

MNC
270

MCC
311

Provisioning section

The *Provisioning* section provides the following details:



Provisioning

Device status
● Active

SIM OTA timestamp
07/11/2024 01:38:42 PM

Activation date
07/11/2024 12:01:09 PM

Deactivation date
--

Suspended date
07/11/2024

Expected resume date
--

eUICC profile status
--

Last order status
SUCCESS

Last order ID
1148225050

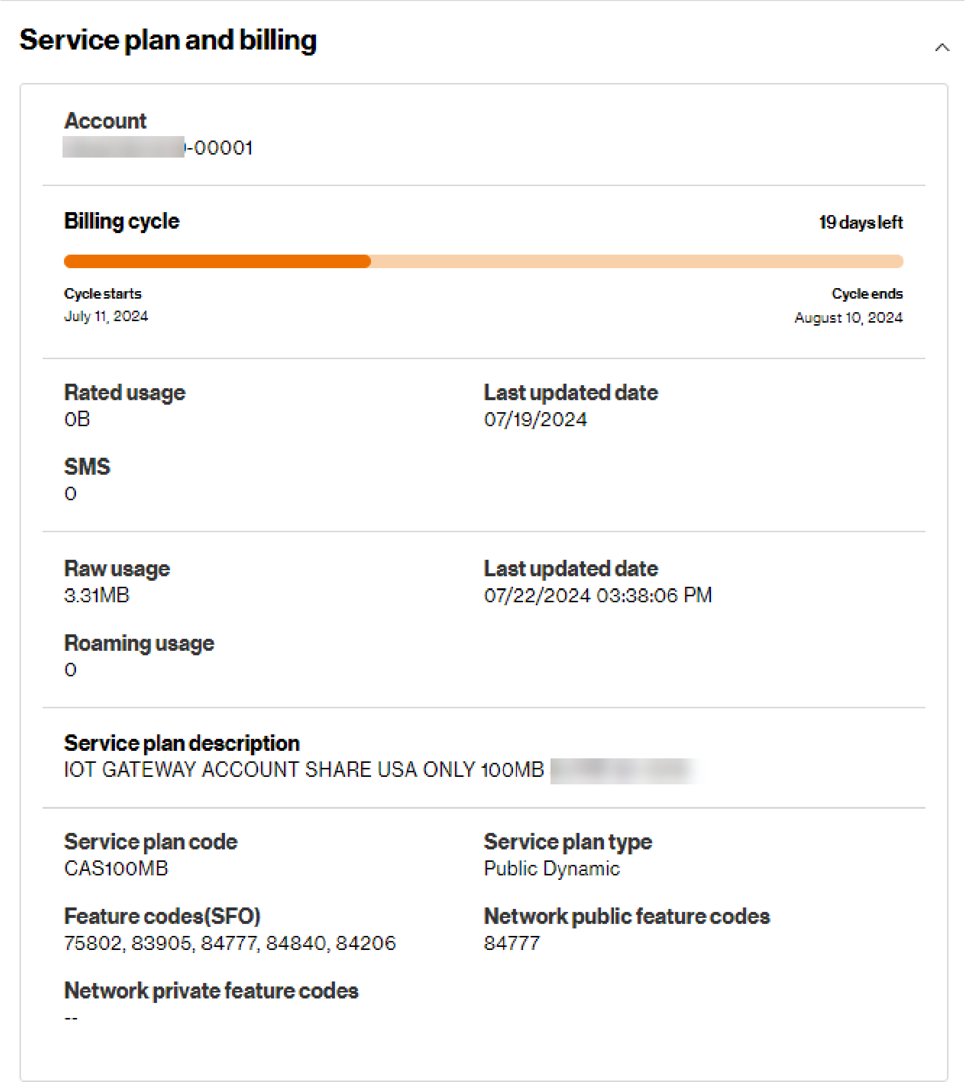
Request ID
343a789e-a93e-45a3-803e-9b41d3d11f5f

Transaction history

Order	Status	Date	Submitted by
Resume	✓ Success	07/19/2024 08:32:04 PM	[redacted]
Deactivation	⊗ Failure	07/19/2024 02:21:52 PM	[redacted]
Suspension	⊗ Failure	07/19/2024 02:20:34 PM	[redacted]
Suspension	✓ Success	07/12/2024 11:12:03 AM	[redacted]
Activation	✓ Success	07/11/2024 12:01:09 PM	[redacted]

Service plan and billing section

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



Service plan and billing

Account
[redacted]-00001

Billing cycle — **19 days left**

Cycle starts
July 11, 2024

Cycle ends
August 10, 2024

Rated usage
0B

Last updated date
07/19/2024

SMS
0

Raw usage
3.31MB

Last updated date
07/22/2024 03:38:06 PM

Roaming usage
0

Service plan description
IOT GATEWAY ACCOUNT SHARE USA ONLY 100MB [redacted]

Service plan code
CAS100MB

Service plan type
Public Dynamic

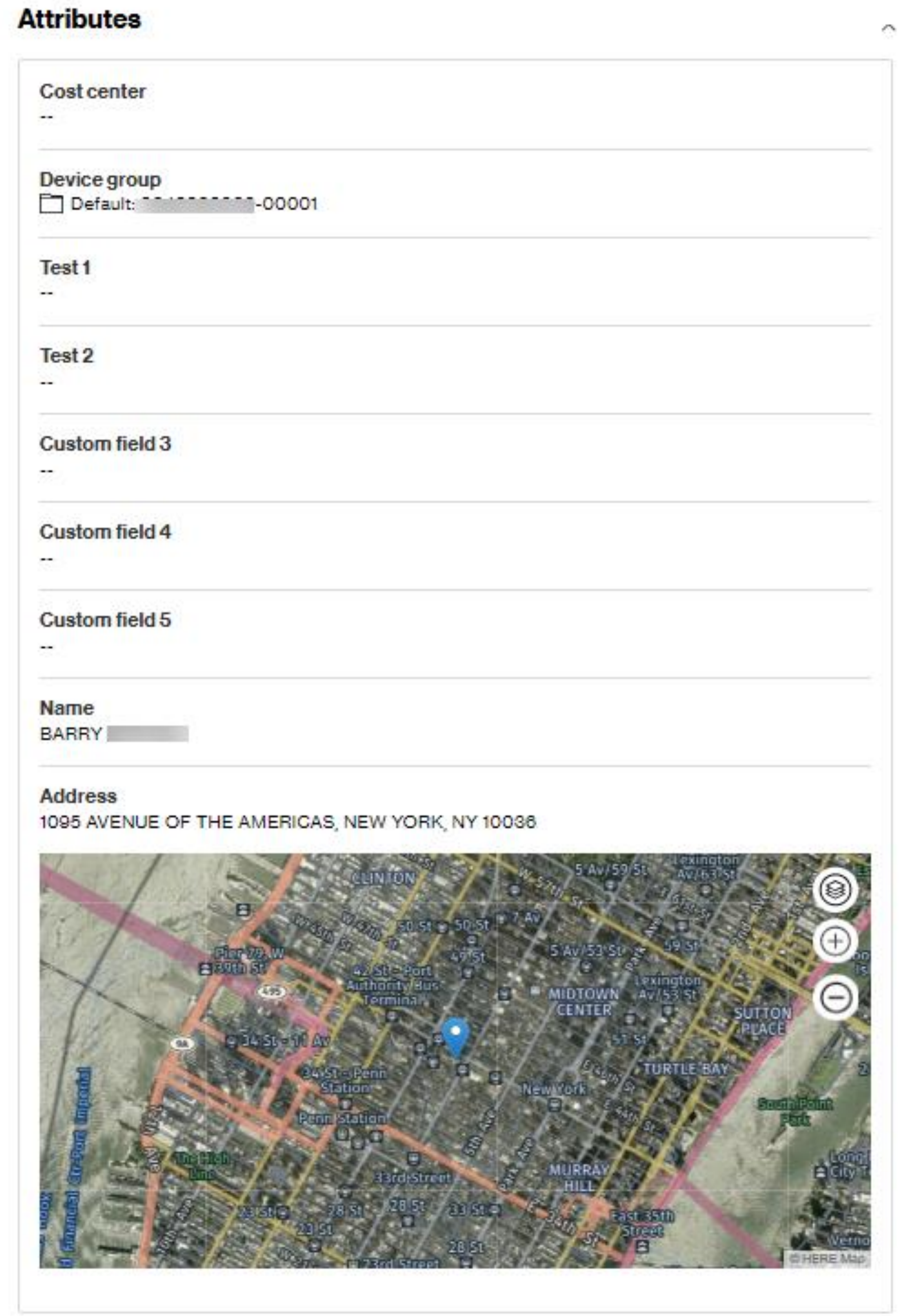
Feature codes(SFO)
75802, 83905, 84777, 84840, 84206

Network public feature codes
84777

Network private feature codes
--

Attributes section

The *Attributes* section provides the following details which are all set the the user. This address does not necessarily represent the location of the device, but rather it is the address entered by the user during an activation, service plan change or set explicitly.



Attributes

Cost center
--

Device group
Default: [redacted]-00001

Test 1
--

Test 2
--

Custom field 3
--

Custom field 4
--

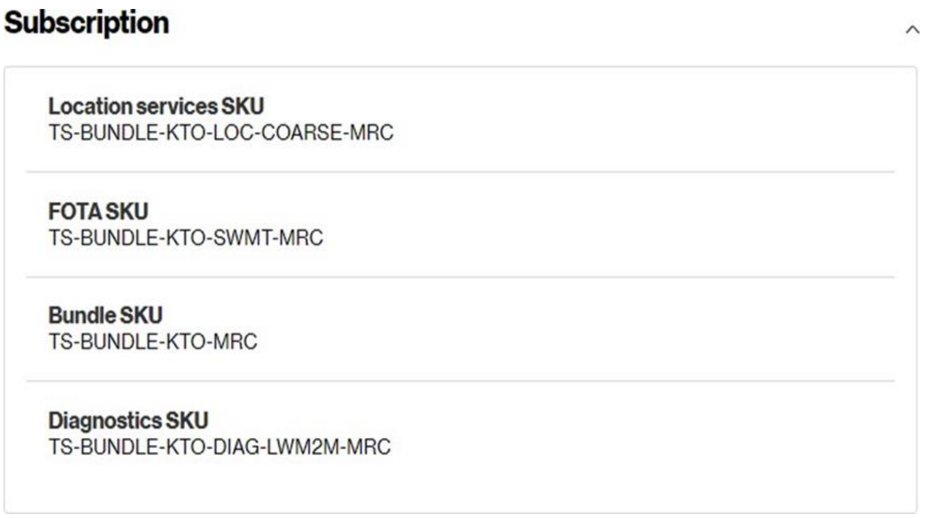
Custom field 5
--

Name
BARRY [redacted]

Address
1095 AVENUE OF THE AMERICAS, NEW YORK, NY 10036

Subscriptions section

The *Subscription* section provides the following details:



Subscription

Location services SKU
TS-BUNDLE-KTO-LOC-COARSE-MRC

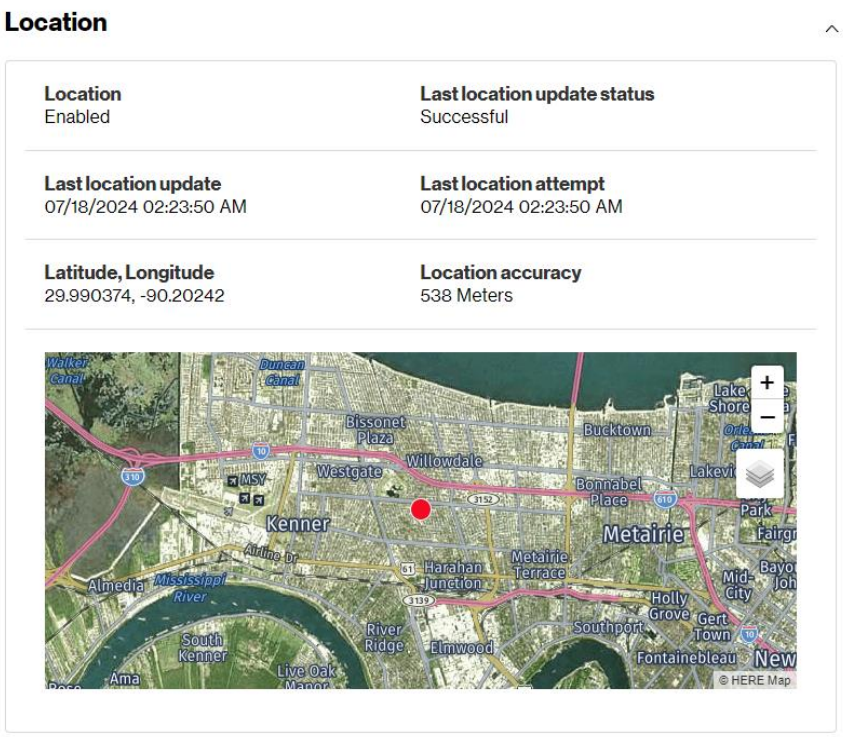
FOTA SKU
TS-BUNDLE-KTO-SWMT-MRC

Bundle SKU
TS-BUNDLE-KTO-MRC

Diagnostics SKU
TS-BUNDLE-KTO-DIAG-LWM2M-MRC

Location section

The *Location* section provides the following details:

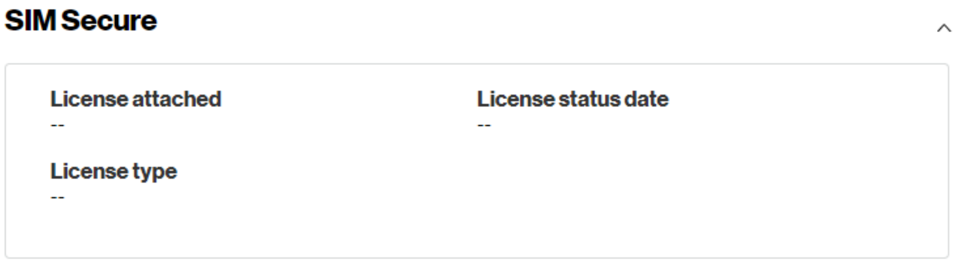


Location

Location Enabled	**Last location update status** Successful
Last location update 07/18/2024 02:23:50 AM	**Last location attempt** 07/18/2024 02:23:50 AM
Latitude, Longitude 29.990374, -90.20242	**Location accuracy** 538 Meters

SIM Secure section

The *SIM Secure* section provides the following details:



SIM Secure

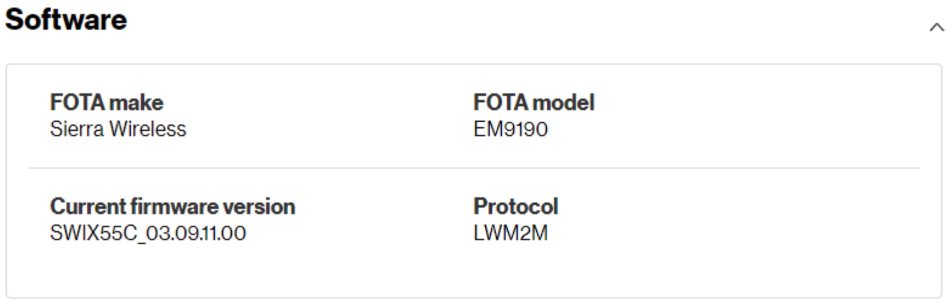
License attached
--

License status date
--

License type
--

Software section

The *Software* section provides the following details:



Software

FOTA make
Sierra Wireless

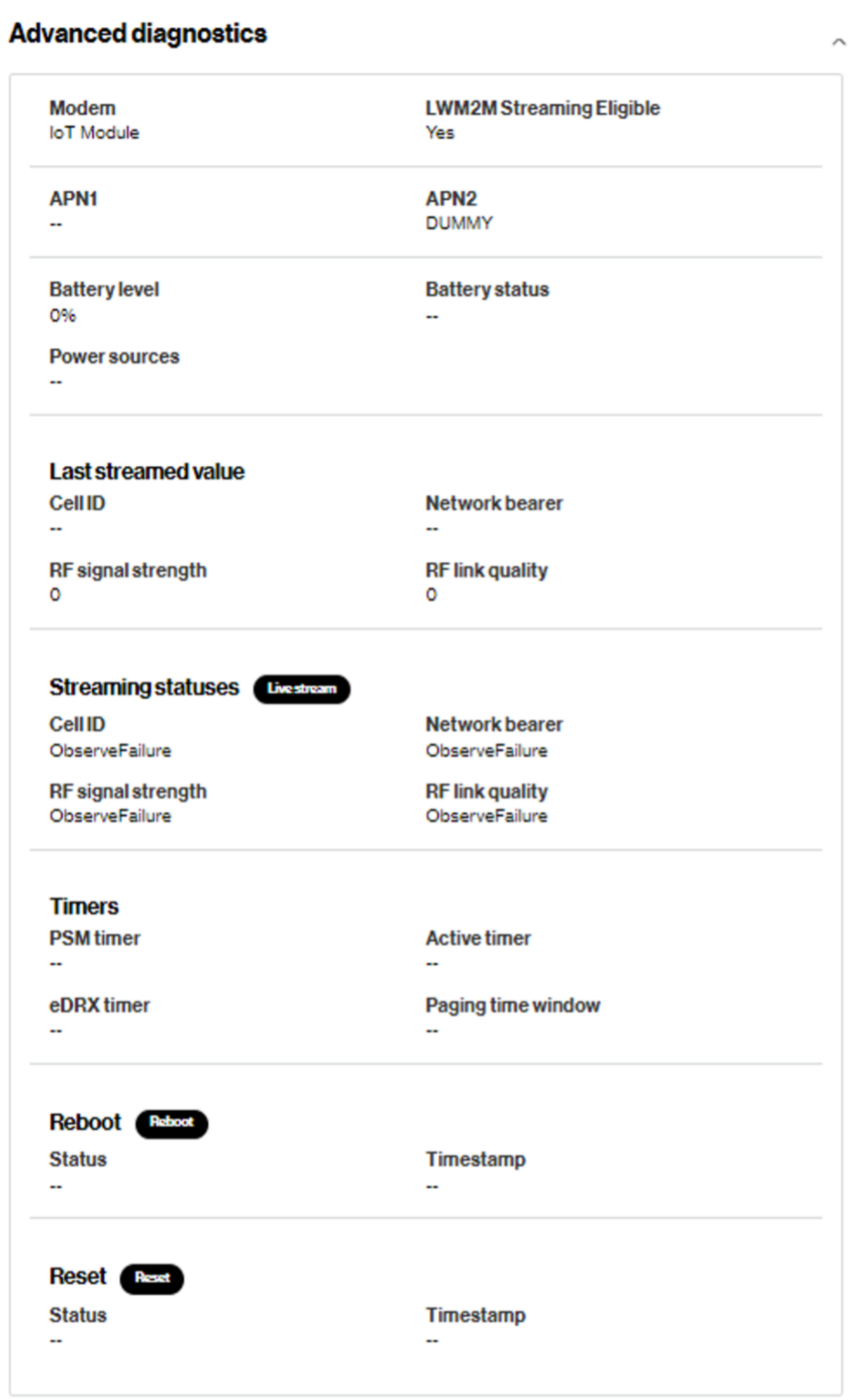
FOTA model
EM9190

Current firmware version
SWIX55C_03.09.11.00

Protocol
LWM2M

Advanced diagnostics section

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 the Appendix for field descriptions.



Advanced diagnostics

Modem IoT Module	**LWM2M Streaming Eligible** Yes
APN1 --	**APN2** DUMMY
Battery level 0%	**Battery status** --
Power sources --	

Last streamed value

Cell ID --	**Network bearer** --
RF signal strength 0	**RF link quality** 0

Streaming statuses

Cell ID ObserveFailure	**Network bearer** ObserveFailure
RF signal strength ObserveFailure	**RF link quality** ObserveFailure

Timers

PSM timer --	**Active timer** --
eDRX timer --	**Paging time window** --

Reboot

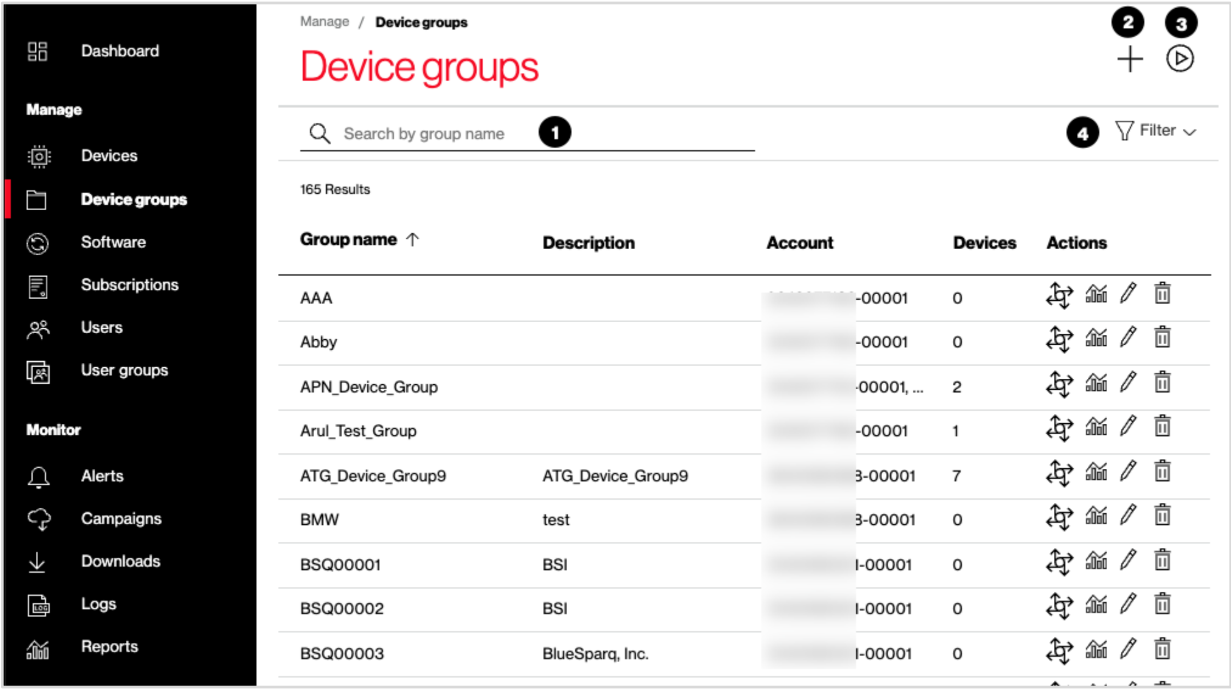
Status --	**Timestamp** --

Reset

Status --	**Timestamp** --

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.



Device groups

Search by group name

165 Results

Group name ↑	Description	Account	Devices	Actions
AAA		[redacted]-00001	0	
Abby		[redacted]-00001	0	
APN_Device_Group		[redacted]-00001, ...	2	
Arul_Test_Group		[redacted]-00001	1	
ATG_Device_Group9	ATG_Device_Group9	[redacted]3-00001	7	
BMW	test	[redacted]3-00001	0	
BSQ00001	BSI	[redacted]1-00001	0	
BSQ00002	BSI	[redacted]1-00001	0	
BSQ00003	BlueSparq, Inc.	[redacted]1-00001	0	

Elements on the Device groups page		
1	🔍	Search – Locate a specific software by name.
2	+	Add – Add a device group.
3	▷	Tutorial videos – View available video tutorials.
4	▽	Filters – Apply filters to minimize the results on the page.

Searching for device groups

Type a group name or part of one in the **Search** field at the top-left of the page to locate the device group.

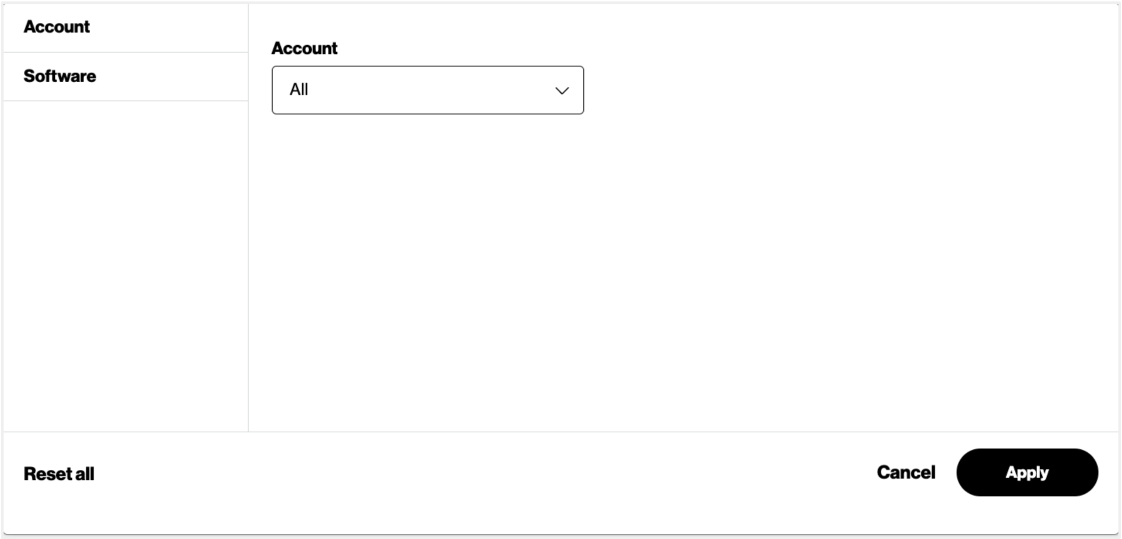
Search by group name

Applying device group filters

Use filters to view a limited set of device groups by: **Accounts** and **Attributes**. Select from the filter categories on the left.

How to apply device filters

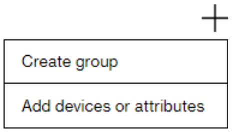
1. Click the filter icon ▽ Filter ∨. The following filters screen appears.



2. Click each tab or scroll through the list to view all available filters.
3. The **Reset all** link resets all filters.
4. Click **Apply**.

Device groups actions

The *Device groups* page offers a set of icons to apply various actions to your devices. + ⊳



Watching tutorial videos

Click on the Tutorial videos icon ⊳ and select from any of the available videos on the list.

Software management

For customers subscribed to *Software Management Services*, you 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.

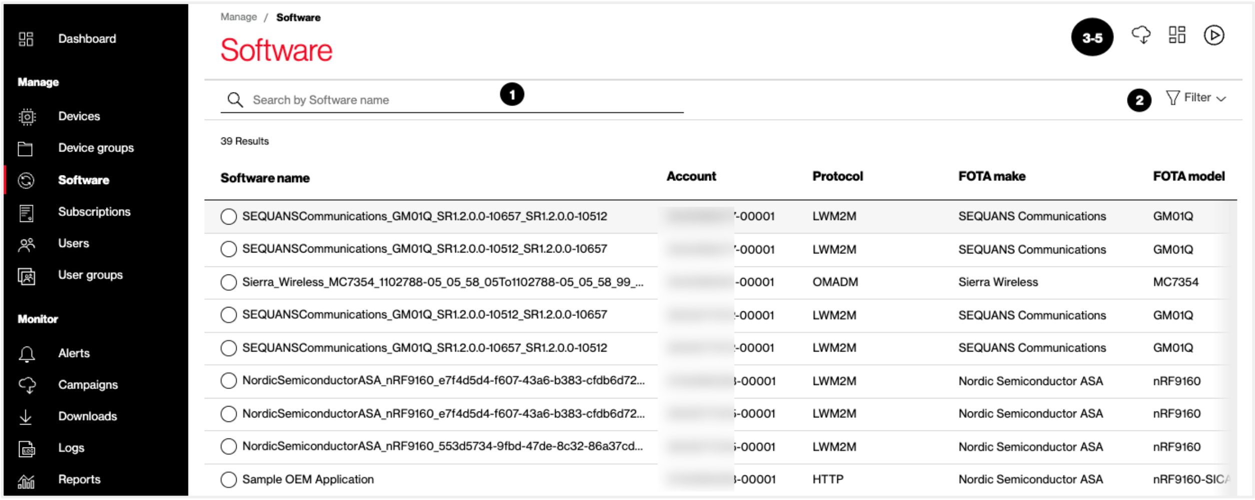
Device eligibility – You must have certified devices on your account that have qualified FROM firmware version loaded.

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.

A subscription to ThingSpace Software Management Services is required for manage firmware updates.

Use the left navigation to open the *Software* page.



Software

Search by Software name

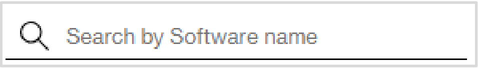
39 Results

Software name	Account	Protocol	FOTA make	FOTA model
○ SEQUANSCommunications_GM01Q_SR1.2.0.0-10657_SR1.2.0.0-10512	[redacted]-00001	LWM2M	SEQUANS Communications	GM01Q
○ SEQUANSCommunications_GM01Q_SR1.2.0.0-10512_SR1.2.0.0-10657	[redacted]-00001	LWM2M	SEQUANS Communications	GM01Q
○ Sierra_Wireless_MC7354_1102788-05_05_58_05To1102788-05_05_58_99_...	[redacted]-00001	OMADM	Sierra Wireless	MC7354
○ SEQUANSCommunications_GM01Q_SR1.2.0.0-10512_SR1.2.0.0-10657	[redacted]-00001	LWM2M	SEQUANS Communications	GM01Q
○ SEQUANSCommunications_GM01Q_SR1.2.0.0-10657_SR1.2.0.0-10512	[redacted]-00001	LWM2M	SEQUANS Communications	GM01Q
○ NordicSemiconductorASA_nRF9160_e7f4d5d4-f607-43a6-b383-cfdb6d72...	[redacted]-00001	LWM2M	Nordic Semiconductor ASA	nRF9160
○ NordicSemiconductorASA_nRF9160_e7f4d5d4-f607-43a6-b383-cfdb6d72...	[redacted]-00001	LWM2M	Nordic Semiconductor ASA	nRF9160
○ NordicSemiconductorASA_nRF9160_553d5734-9fbd-47de-8c32-86a37cd...	[redacted]-00001	LWM2M	Nordic Semiconductor ASA	nRF9160
○ Sample OEM Application	[redacted]-00001	HTTP	Nordic Semiconductor ASA	nRF9160-SIC

Elements on the Software page		
1	🔍	Search – Locate a specific software by name.
2	▽	Filter – Apply filters to minimize the results on the page.
3	☁	Campaign – Create a strategy to update software.
4	▦	Show legacy view – Shows the legacy Software management page.
5	▶	Tutorial videos – View available video tutorials.

Searching for software

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



Search by Software name

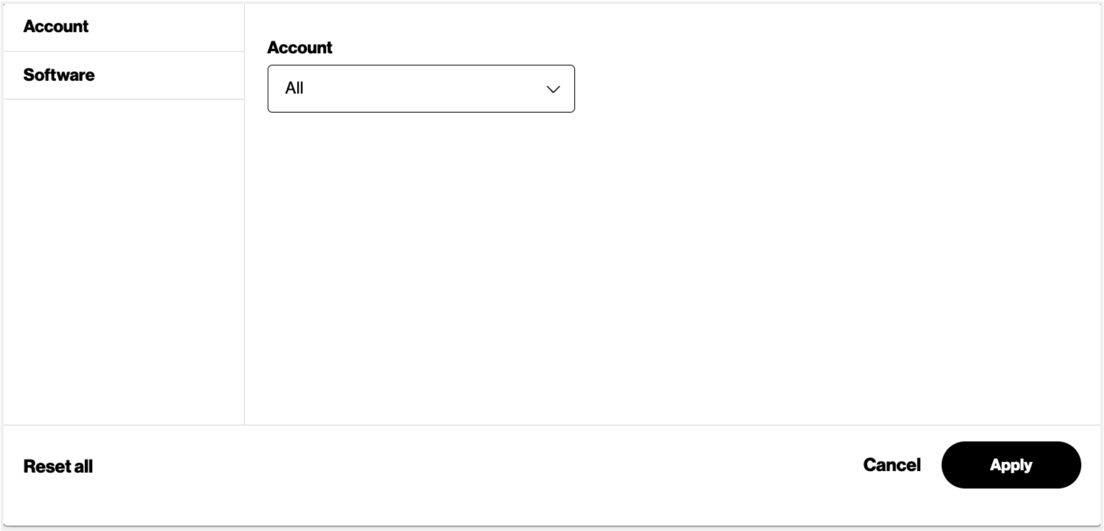
NOTE: Search does not support wildcard characters at this time. Searches are not case sensitive.

Applying software filters

Use filters to view a limited set of software by: **Accounts** and **Attributes**. Select from the filter tabs on the left.

How to apply device filters

1. Click the filter icon ▽ Filter ⌄. The following filters screen appears.



Account
Software

Account: All

2. Click each tab or scroll through the list to view all available filters.

3. The **Reset all** link resets all filters.
4. Click **Apply**.

Creating a campaign

See the Devices section on how to create a campaign.

Watching tutorial videos

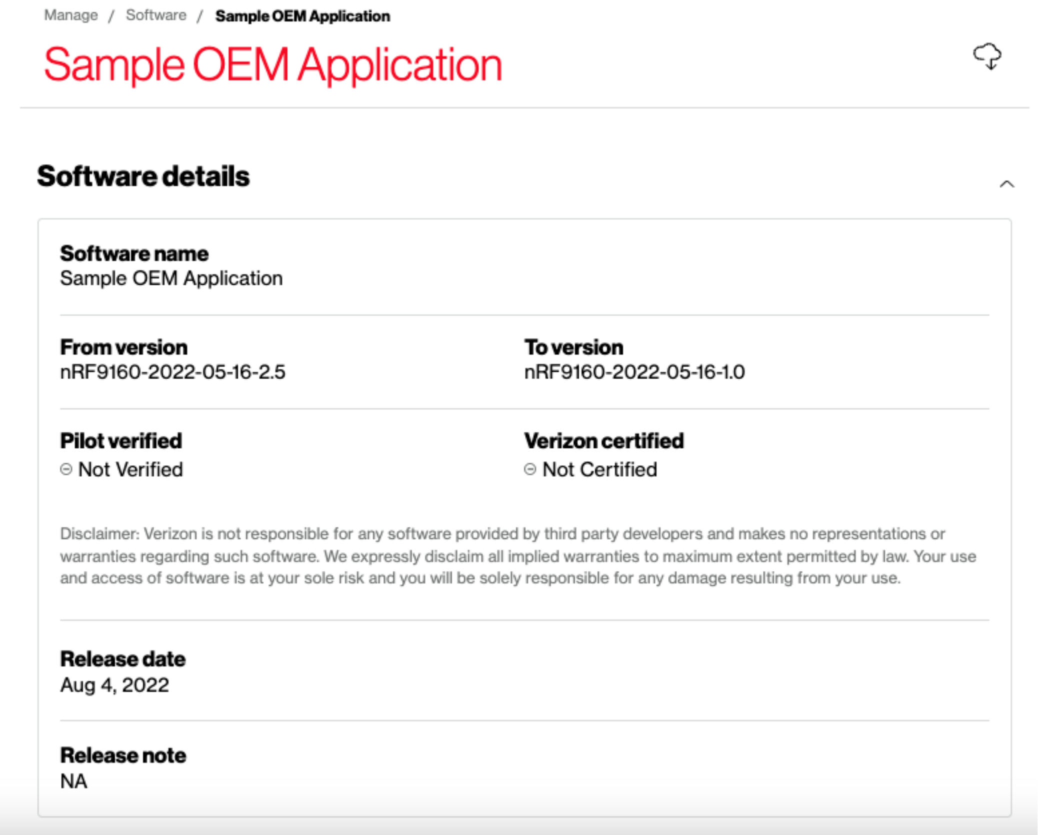
Click on the Tutorial videos icon ▷ and select from any of the available videos on the list.

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

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



Manage / Software / **Sample OEM Application**

Sample OEM Application

Software details

Software name
Sample OEM Application

From version
nRF9160-2022-05-16-2.5

To version
nRF9160-2022-05-16-1.0

Pilot verified
⊝ Not Verified

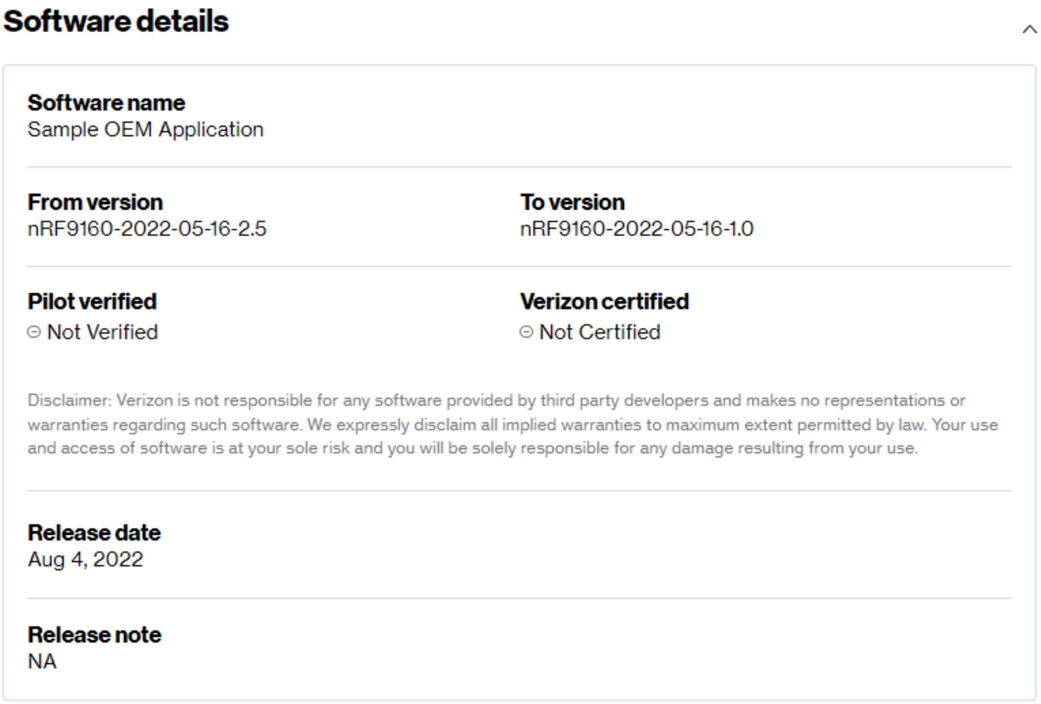
Verizon certified
⊝ Not Certified

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

Release date
Aug 4, 2022

Release note
NA

2. Click the campaign icon ☁ to create a campaign. See the Devices section to learn how to create a campaign.



Software details

Software name
Sample OEM Application

From version nRF9160-2022-05-16-2.5	**To version** nRF9160-2022-05-16-1.0
Pilot verified ⊝ Not Verified	**Verizon certified** ⊝ Not Certified

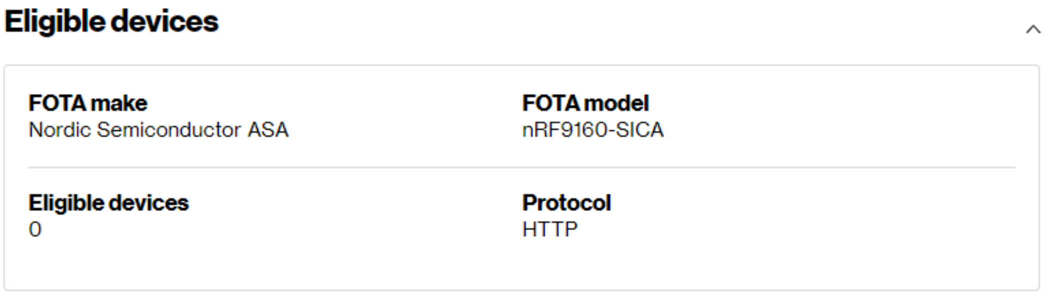
Disclaimer: Verizon is not responsible for any software provided by third party developers and makes no representations or warranties regarding such software. We expressly disclaim all implied warranties to maximum extent permitted by law. Your use and access of software is at your sole risk and you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

Release date
Aug 4, 2022

Release note
NA

Eligible devices section

The *Eligible devices* section provides the following details:

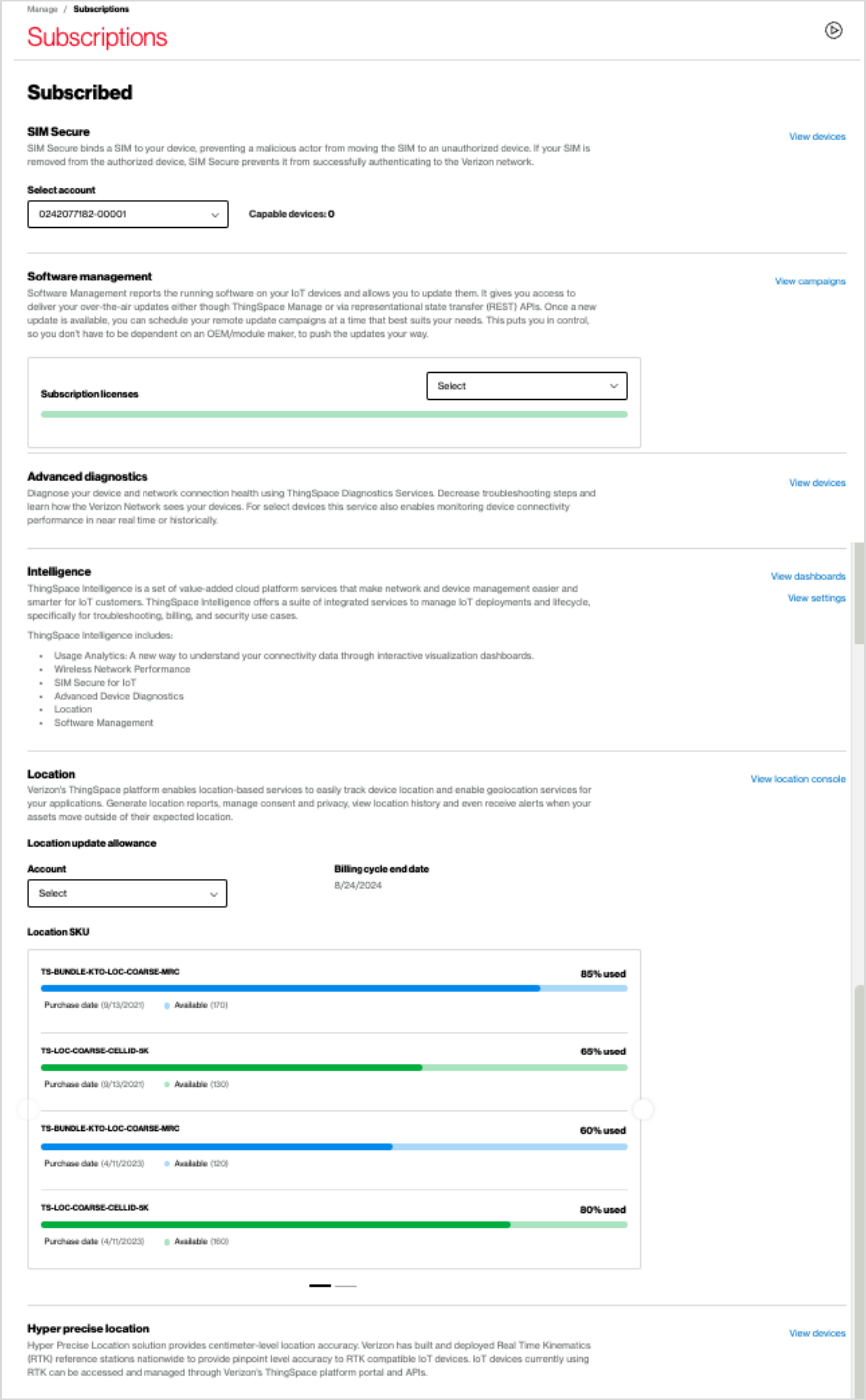


Eligible devices

FOTA make Nordic Semiconductor ASA	**FOTA model** nRF9160-SICA
Eligible devices 0	**Protocol** HTTP

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. From there you can purchase or try out the service.



Subscriptions

Subscribed

SIM Secure

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

Select account 0242077182-00001

Capable devices: 0

Software management

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

Subscription licenses Select

Advanced diagnostics

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

Intelligence

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

ThingSpace Intelligence includes:

- Usage Analytics: A new way to understand your connectivity data through interactive visualization dashboards.
- Wireless Network Performance
- SIM Secure for IoT
- Advanced Device Diagnostics
- Location
- Software Management

Location

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

Location update allowance

Account Select

Billing cycle end date 8/24/2024

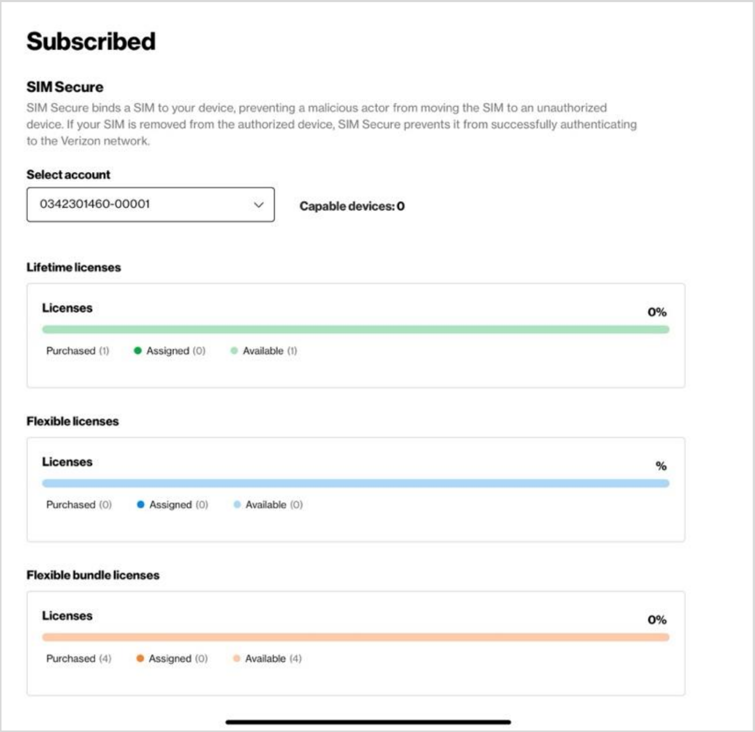
Location SKU

SKU	Used	Purchase date	Available
TS-BUNDLE-KTO-LOC-COARSE-MRC	85% used	(9/13/2021)	(170)
TS-LOC-COARSE-CELLID-5K	65% used	(9/13/2021)	(130)
TS-BUNDLE-KTO-LOC-COARSE-MRC	60% used	(4/11/2023)	(120)
TS-LOC-COARSE-CELLID-5K	80% used	(4/11/2023)	(160)

Hyper precise location

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

Once you are subscribed, the individual sections offer details on your subscription utilization including Location, SIM Secure and Software Management. For example, this is what to expect if you are subscribed to SIM Secure or Location services. You can monitor the license utilization.



Subscribed

SIM Secure

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

Select account

0342301460-00001

Capable devices: 0

Lifetime licenses

Licenses 0%

Purchased (1) ● Assigned (0) ● Available (1)

Flexible licenses

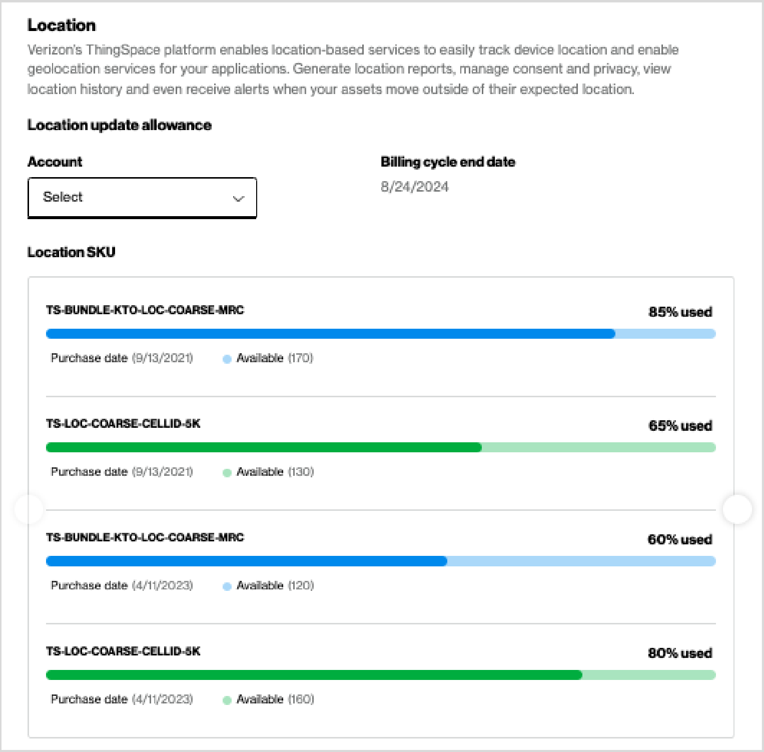
Licenses %

Purchased (0) ● Assigned (0) ● Available (0)

Flexible bundle licenses

Licenses 0%

Purchased (4) ● Assigned (0) ● Available (4)



Location

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

Location update allowance

Account

Select

Billing cycle end date

8/24/2024

Location SKU

TS-BUNDLE-KTO-LOC-COARSE-MRC 85% used

Purchase date (9/13/2021) ● Available (170)

TS-LOC-COARSE-CELLID-5K 65% used

Purchase date (9/13/2021) ● Available (130)

TS-BUNDLE-KTO-LOC-COARSE-MRC 60% used

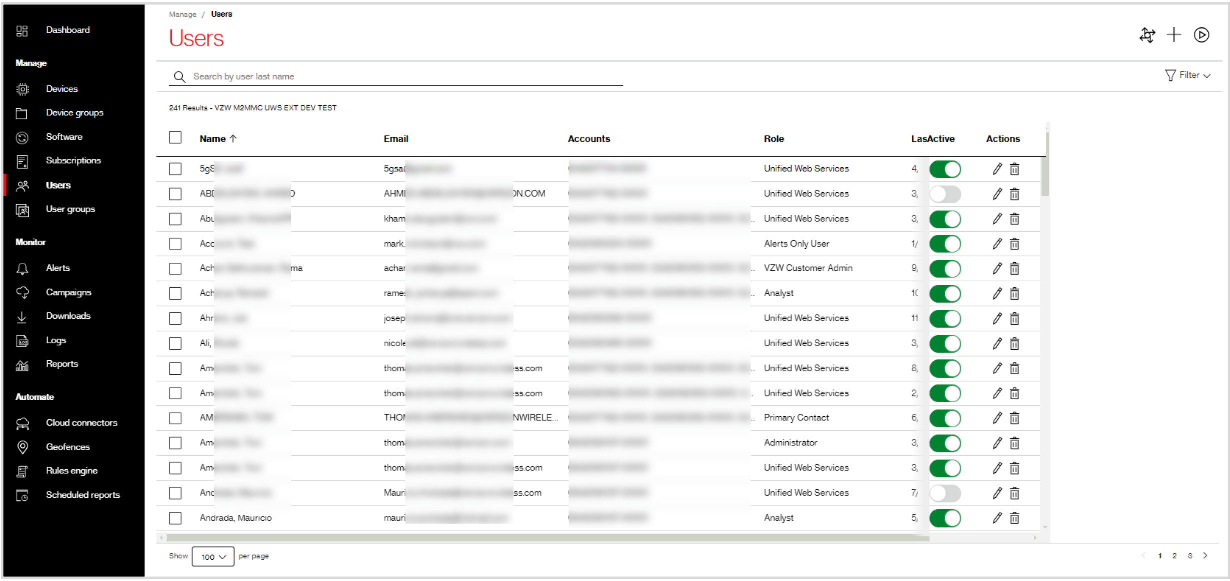
Purchase date (4/11/2023) ● Available (120)

TS-LOC-COARSE-CELLID-5K 80% used

Purchase date (4/11/2023) ● Available (160)

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.



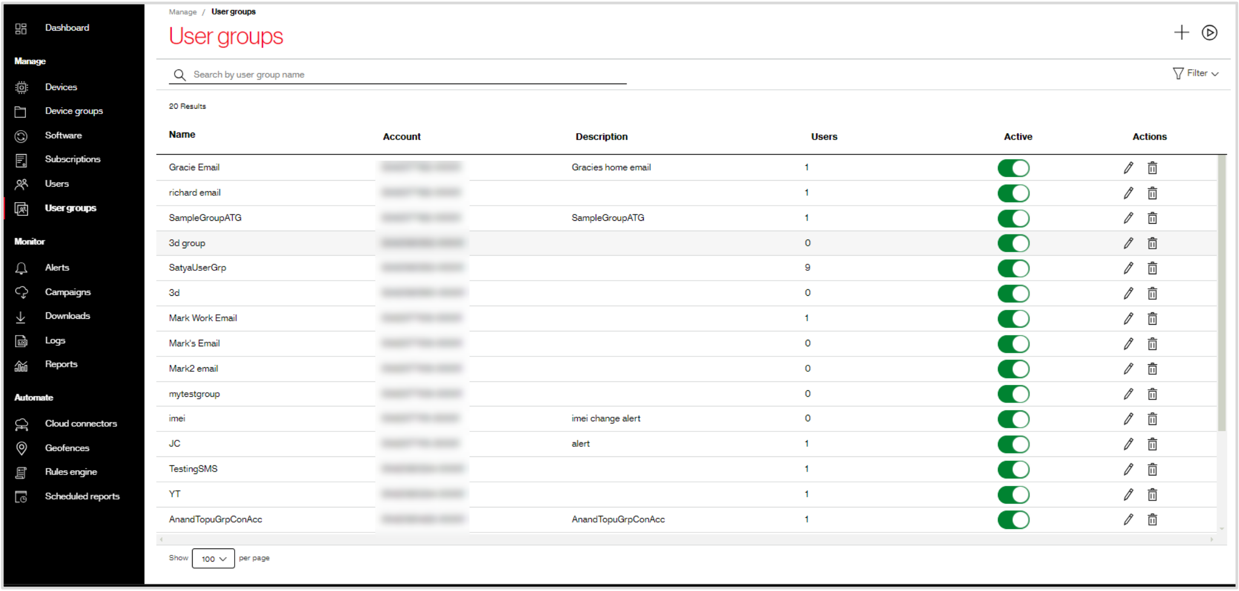
241 Results - VZW M2MMC UWS EXT DEV TEST

□	Name ↑	Email	Accounts	Role	LasActive		Actions
□	5gS[redacted]	5gsa[redacted]	[redacted]	Unified Web Services	4,	●	✎ 🗑
□	ABI[redacted]D	AHMI[redacted]N.COM	[redacted]	Unified Web Services	3,	○	✎ 🗑
□	Abu[redacted]	kham[redacted]	[redacted]	Unified Web Services	3,	●	✎ 🗑
□	Acc[redacted]	mark.[redacted]	[redacted]	Alerts Only User	1/	●	✎ 🗑
□	Ach[redacted]ma	achar[redacted]	[redacted]	VZW Customer Admin	9,	●	✎ 🗑
□	Ach[redacted]	rames[redacted]	[redacted]	Analyst	1(	●	✎ 🗑
□	Ahr[redacted]	josep[redacted]	[redacted]	Unified Web Services	11	●	✎ 🗑
□	Ali, [redacted]	nicole[redacted]	[redacted]	Unified Web Services	3,	●	✎ 🗑
□	Am[redacted]	thom[redacted]ss.com	[redacted]	Unified Web Services	8,	●	✎ 🗑
□	Am[redacted]	thom[redacted]ss.com	[redacted]	Unified Web Services	2,	●	✎ 🗑
□	AM[redacted]	THO[redacted]NWIRELE...	[redacted]	Primary Contact	6,	●	✎ 🗑
□	Am[redacted]	thom[redacted]	[redacted]	Administrator	3,	●	✎ 🗑
□	Am[redacted]	thom[redacted]ss.com	[redacted]	Unified Web Services	3,	●	✎ 🗑
□	And[redacted]	Mauri[redacted]ss.com	[redacted]	Unified Web Services	7/	○	✎ 🗑
□	Andrada, Mauricio	mauri[redacted]	[redacted]	Analyst	5,	●	✎ 🗑

NOTE: You are only able to create **Alerts Only** and **Unified Web Services** (UWS) users. Use MyBiz Profile Administration to add regular portal users. Check out the tutorial videos on the top right of this page for a walk through on how to create regular portal users.

User groups

Use the *User Groups* page to assign users to individual groups. Use the left navigation to open the *User Groups* page.



20 Results

Name	Account	Description	Users	Active	Actions
Gracie Email	[redacted]	Gracies home email	1	●	✎ 🗑
richard email	[redacted]		1	●	✎ 🗑
SampleGroupATG	[redacted]	SampleGroupATG	1	●	✎ 🗑
3d group	[redacted]		0	●	✎ 🗑
SatyaUserGrp	[redacted]		9	●	✎ 🗑
3d	[redacted]		0	●	✎ 🗑
Mark Work Email	[redacted]		1	●	✎ 🗑
Mark's Email	[redacted]		0	●	✎ 🗑
Mark2 email	[redacted]		0	●	✎ 🗑
mytestgroup	[redacted]		0	●	✎ 🗑
imei	[redacted]	imei change alert	0	●	✎ 🗑
JC	[redacted]	alert	1	●	✎ 🗑
TestingSMS	[redacted]		1	●	✎ 🗑
YT	[redacted]		1	●	✎ 🗑
AnandTopuGrpConAcc	[redacted]	AnandTopuGrpConAcc	1	●	✎ 🗑

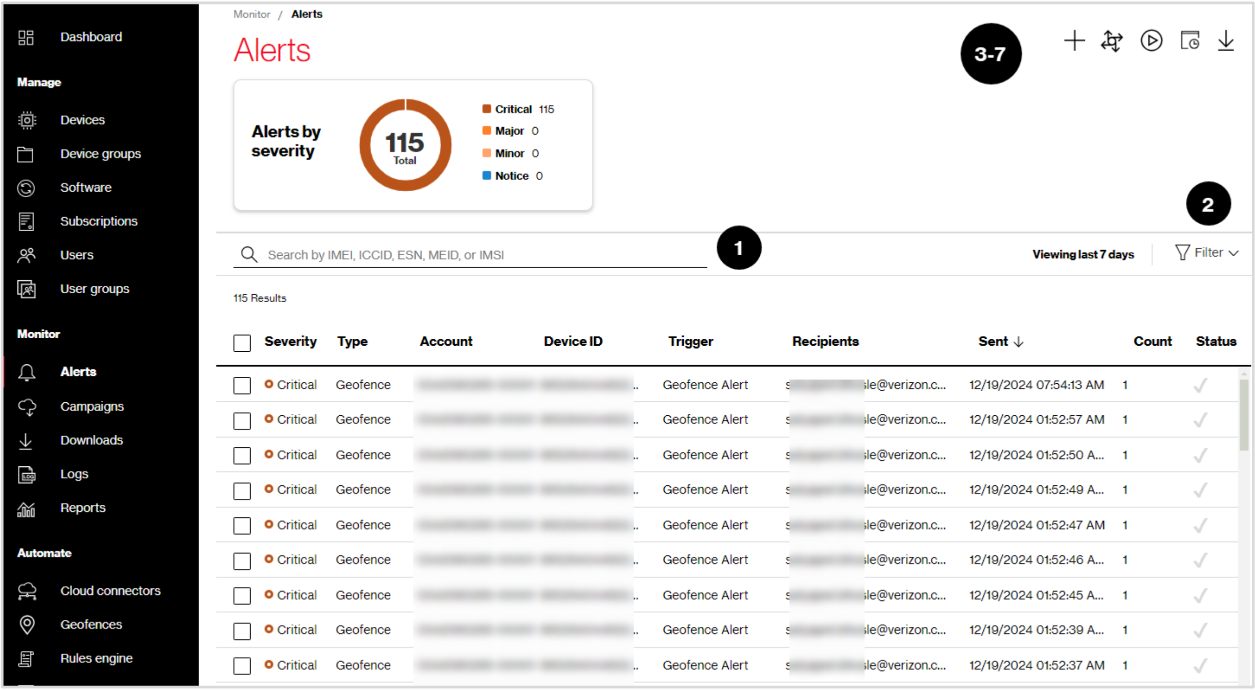
Alerts

ThingSpace includes a notification feature that alerts 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 triggered, the system sends out an alert using the method specified (email, SMS, or API callback) for each recipient. Use the *Alerts* page to view these alerts.

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 included in the notification's target group can acknowledge a notification. Notifications are acknowledged from the Alerts page only.

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



115 Results

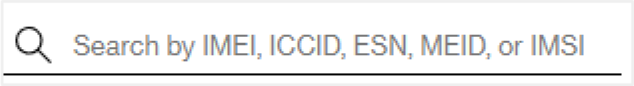
□	Severity	Type	Account	Device ID	Trigger	Recipients	Sent ↓	Count	Status
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 07:54:13 AM	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:57 AM	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:50 A...	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:49 A...	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:47 AM	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:46 A...	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:45 A...	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:39 A...	1	✓
□	○ Critical	Geofence	[redacted]	[redacted]..	Geofence Alert	s[redacted]le@verizon.c...	12/19/2024 01:52:37 AM	1	✓

Elements on the Alerts page		
1	🔍	Search – Locate an alert by device identifier.
2	▽	Filter – Limit the list to only alerts having specific attributes.
3	+	Create new rule – Takes you to the Create a rule page

4	✥	Actions – Open a menu of actions.
5	▷	Video – View short training videos relevant to this page.
6	🗓	Schedule – Automate and schedule a report of the alerts log.
7	↓	Download – Export the alerts log.

Searching alerts

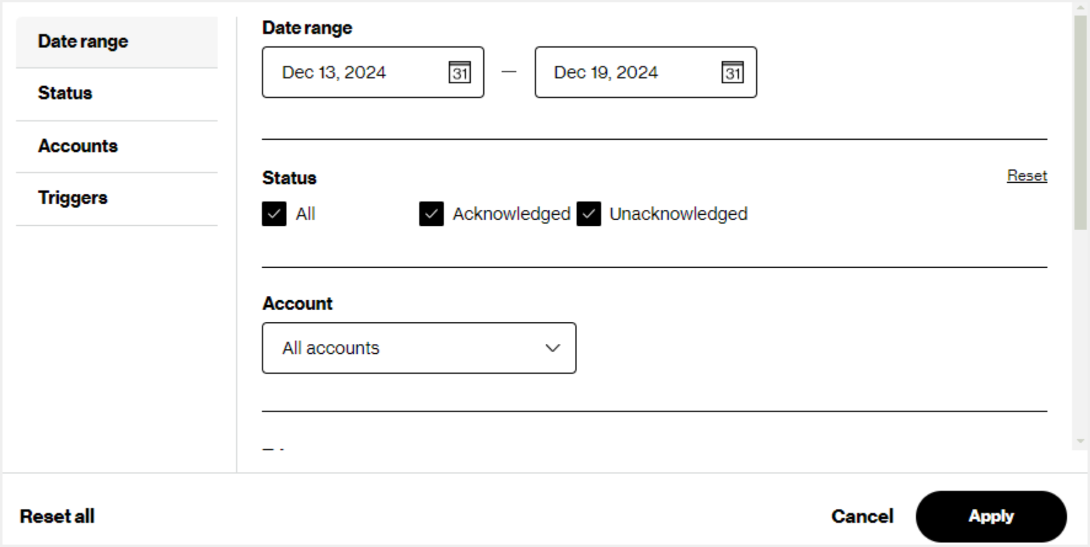
Use the **Search** field to search for devices by IMEI, ICCID, ESN, MEID, or IMSI. Wildcard (%) search is supported for Device IDs.



Applying alert filters

How to apply filters

1. On the left navigation, click **Alerts**. The *Alerts* page opens.
2. Click the filter icon ∇ Filter ⌄. The *Filters* page opens.



Date range: Dec 13, 2024 – Dec 19, 2024

Status: ☑ All ☑ Acknowledged ☑ Unacknowledged

Account: All accounts

3. Click on each tab on the left, or scroll through the list to view all available filters.
4. Select the desired filters.

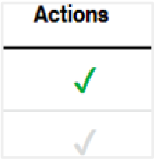
5. Click **Reset** in a filter category to select all filters in that category. To apply a date ranger filter, enter a date range of no more than 31 days.

6. 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 a single 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

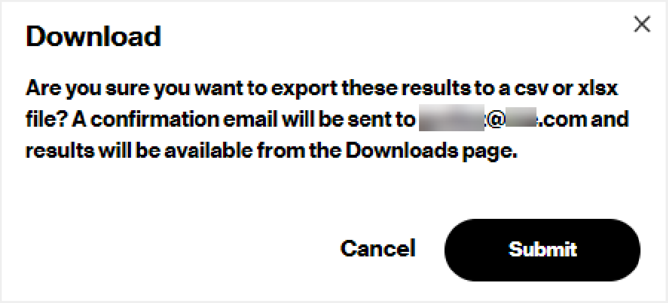
1. Select each alert checkbox.

2. Click the actions icon and then select **Acknowledge** to complete the process.

Downloading the alerts log

How to export your alerts log

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



Download

Are you sure you want to export these results to a csv or xlsx file? A confirmation email will be sent to [redacted]@[redacted].com and results will be available from the Downloads page.

2. Click **Submit** to download the file.

You will receive an email notification when the download is ready. You can view the download in the Downloads page.

Watching tutorial videos

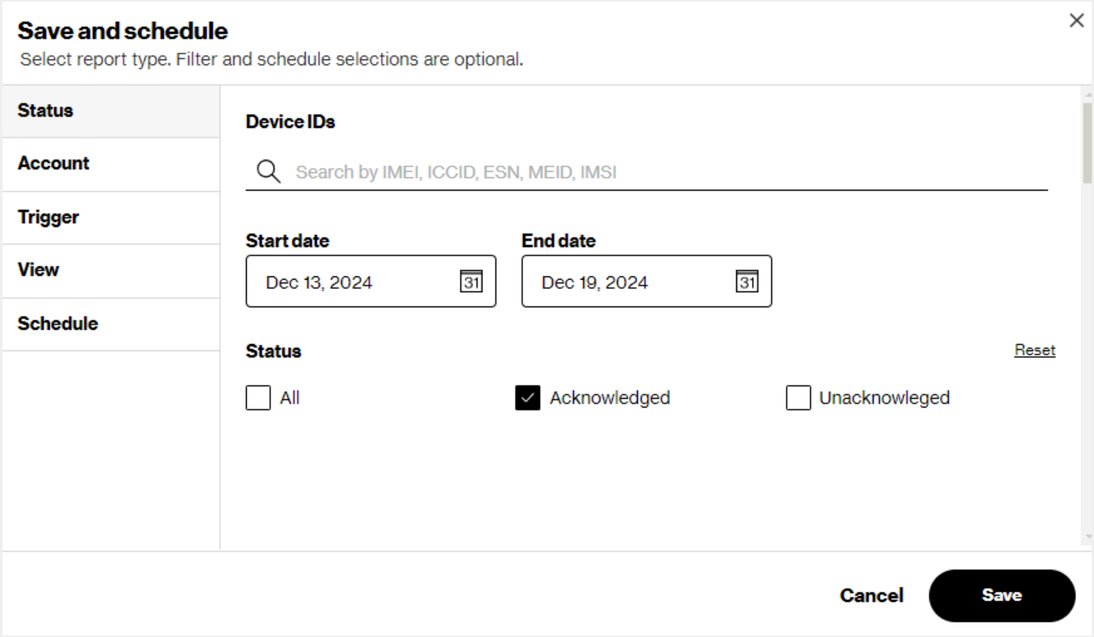
Click on the Tutorial videos icon ▷ and select from any of the available videos on the list.

Scheduling an alerts report

You can schedule to have your alerts log available as a report that can be downloaded. You can also limit the report output by choosing from multiple options.

How to save and/or schedule your alerts log as a report

1. Click the schedule icon 🕒. The *Save and schedule* dialog opens.



Save and schedule

Select report type. Filter and schedule selections are optional.

Start date: Dec 13, 2024

End date: Dec 19, 2024

Status

□ All ☑ Acknowledged □ Unacknowleged

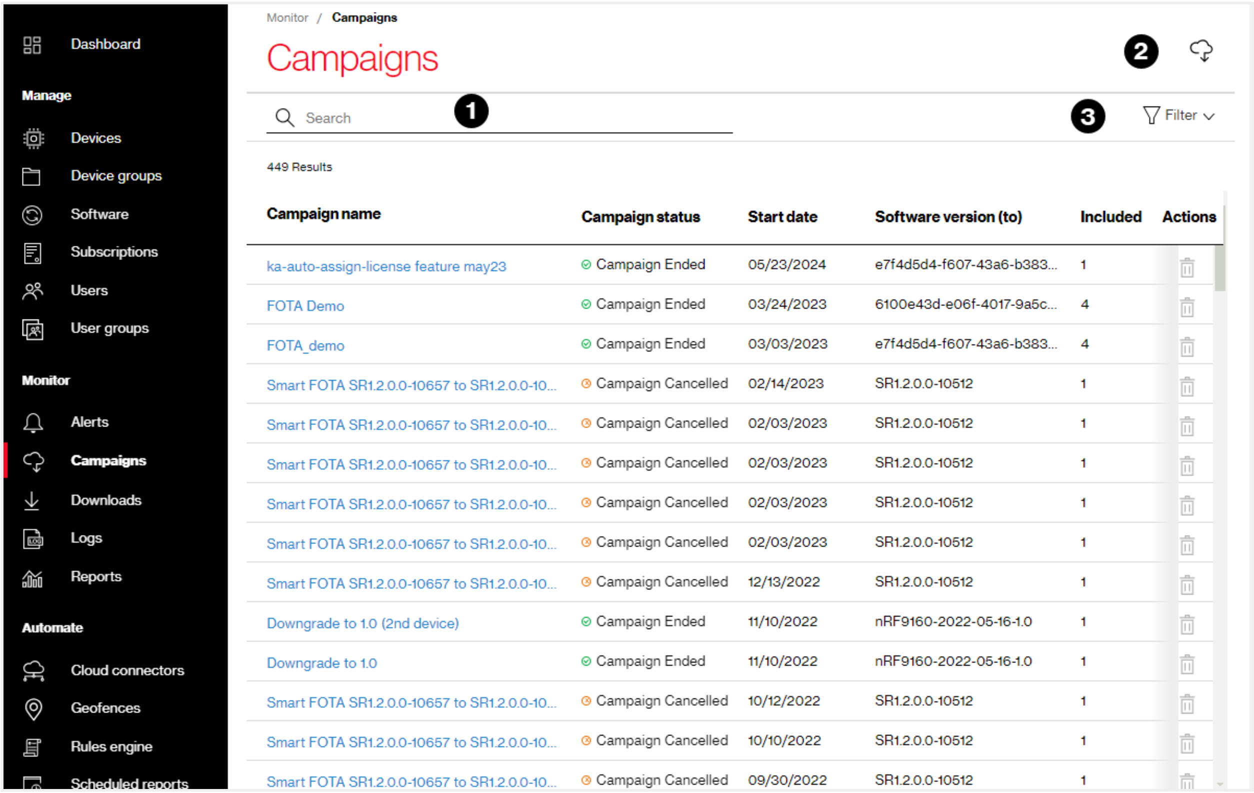
2. Select from all of the available options to limit the report output.
   a. For **Name**, type a descriptive label for the devices report.
   b. Check **Schedule** to run this report at a predetermined date and time.
      (4) Select the Time period for your scheduled report.
      (5) Set the Frequency for the report to run.
      (6) Select an Expiration date for the report to end the schedule.
3. Click **Save** to complete the process.

Campaigns

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

To open the Campaigns page

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



449 Results

Campaign name	Campaign status	Start date	Software version (to)	Included	Actions
ka-auto-assign-license feature may23	Campaign Ended	05/23/2024	e7f4d5d4-f607-43a6-b383...	1	
FOTA Demo	Campaign Ended	03/24/2023	6100e43d-e06f-4017-9a5c...	4	
FOTA_demo	Campaign Ended	03/03/2023	e7f4d5d4-f607-43a6-b383...	4	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	02/14/2023	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	02/03/2023	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	02/03/2023	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	02/03/2023	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	02/03/2023	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	12/13/2022	SR1.2.0.0-10512	1	
Downgrade to 1.0 (2nd device)	Campaign Ended	11/10/2022	nRF9160-2022-05-16-1.0	1	
Downgrade to 1.0	Campaign Ended	11/10/2022	nRF9160-2022-05-16-1.0	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	10/12/2022	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	10/10/2022	SR1.2.0.0-10512	1	
Smart FOTA SR1.2.0.0-10657 to SR1.2.0.0-10...	Campaign Cancelled	09/30/2022	SR1.2.0.0-10512	1	

Elements on the Campaigns page		
1	🔍	Search – Locate a campaign by name.
2	☁	Campaign – Open the Campaign menu.
3	▽	Filter – Limit the list to campaigns with specific attributes.
4	🗑	Delete – Permanently remove a campaign.

Search for campaigns

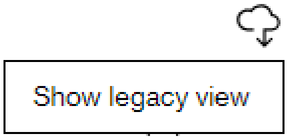
Use the **Search** field to locate campaigns by name.

NOTE: Search does not support wildcards for campaign name.

NOTE: Searches are not case sensitive.

Taking campaign actions

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



Deleting a campaign

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

How to delete a campaign

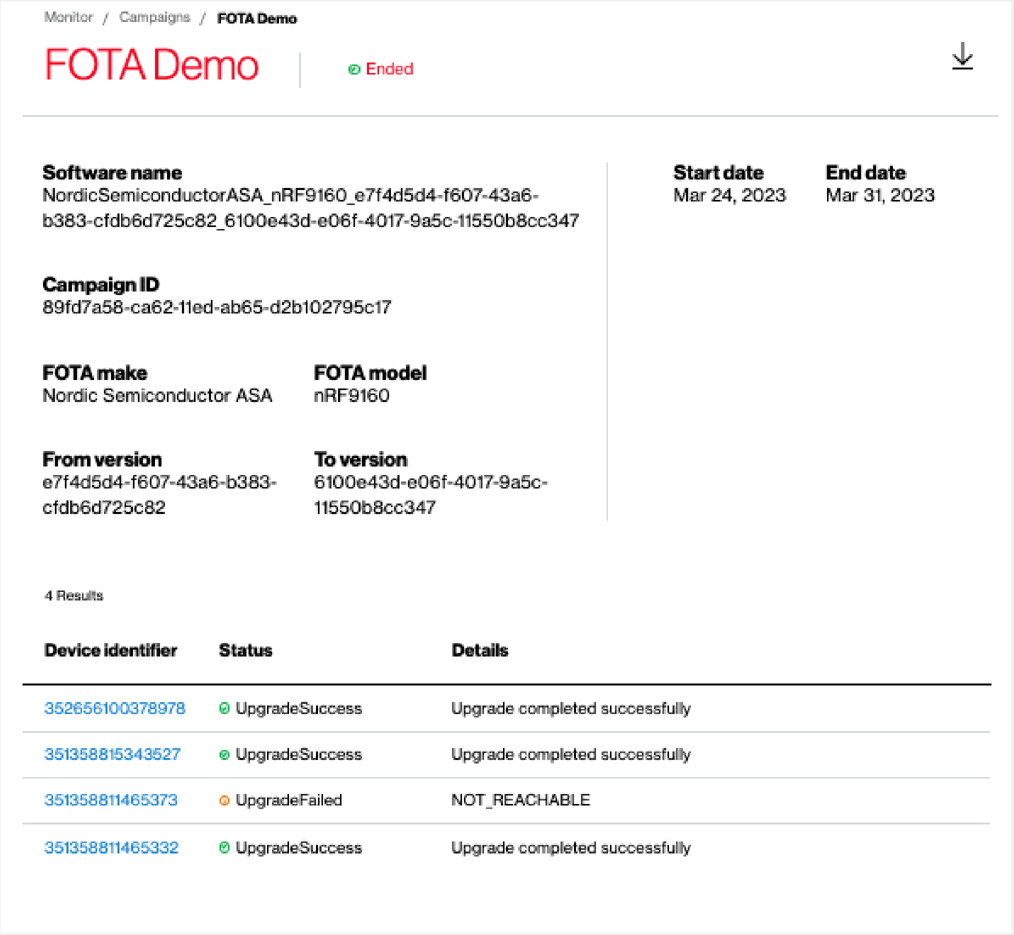
1. On the left navigation, click **Campaigns**. The *Campaigns* page opens.
2. Click on the Campaign's delete icon 🗑. The Campaign is removed from the list.

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

1. On the left navigation, click **Campaigns**. The *Campaigns* page opens.
2. Click the **Campaign name**. A *Campaign details* page opens with details about the selected campaign.



Monitor / Campaigns / FOTA Demo

FOTA Demo | Ended

Software name
NordicSemiconductorASA_nRF9160_e7f4d5d4-f607-43a6-b383-cfdb6d725c82_6100e43d-e06f-4017-9a5c-11550b8cc347

Campaign ID
89fd7a58-ca62-11ed-ab65-d2b102795c17

FOTA make
Nordic Semiconductor ASA

FOTA model
nRF9160

From version
e7f4d5d4-f607-43a6-b383-cfdb6d725c82

To version
6100e43d-e06f-4017-9a5c-11550b8cc347

Start date
Mar 24, 2023

End date
Mar 31, 2023

4 Results

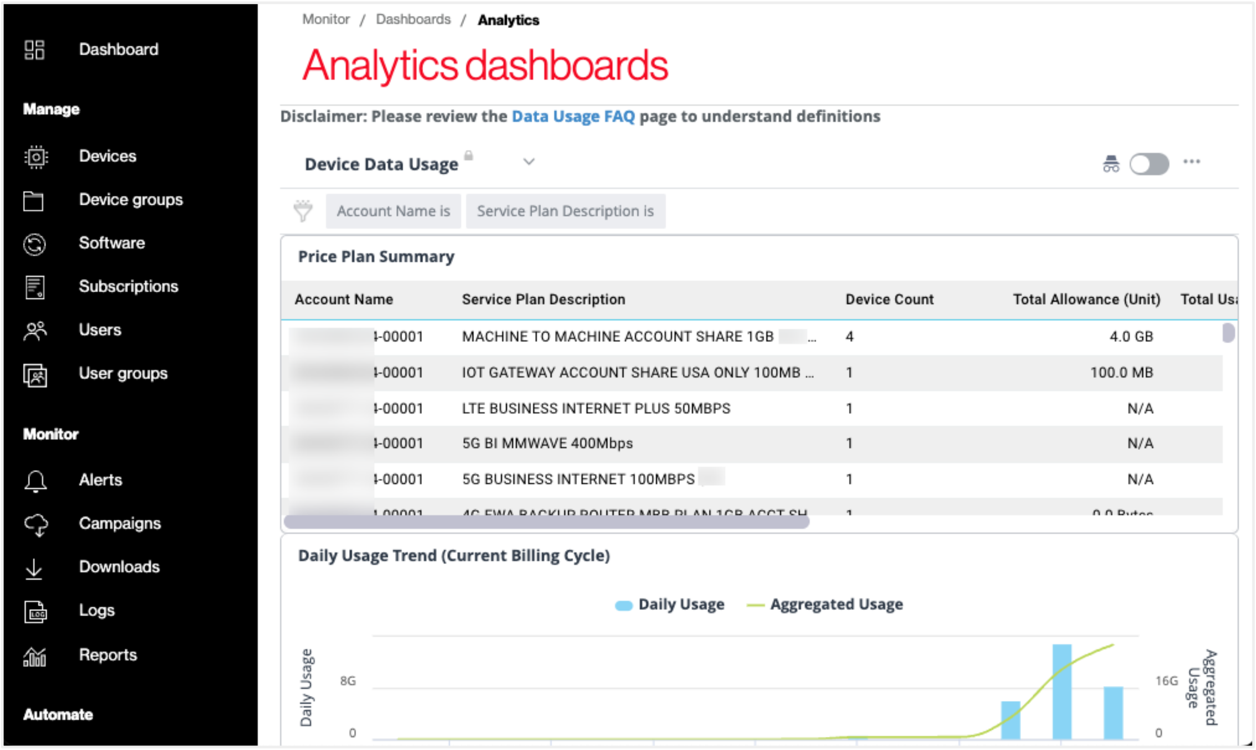
Device identifier	Status	Details
352656100378978	UpgradeSuccess	Upgrade completed successfully
351358815343527	UpgradeSuccess	Upgrade completed successfully
351358811465373	UpgradeFailed	NOT_REACHABLE
351358811465332	UpgradeSuccess	Upgrade completed successfully

Analytics dashboards

ThingSpace Analytics is a 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.



Disclaimer: Please review the Data Usage FAQ page to understand definitions

Price Plan Summary

Account Name	Service Plan Description	Device Count	Total Allowance (Unit)	Total Us
[redacted]-00001	MACHINE TO MACHINE ACCOUNT SHARE 1GB ...	4	4.0 GB	
[redacted]-00001	IOT GATEWAY ACCOUNT SHARE USA ONLY 100MB ...	1	100.0 MB	
[redacted]-00001	LTE BUSINESS INTERNET PLUS 50MBPS	1	N/A	
[redacted]-00001	5G BI MMWAVE 400Mbps	1	N/A	
[redacted]-00001	5G BUSINESS INTERNET 100MBPS	1	N/A	
[redacted]-00001	4G FWA BACKUP ROUTER MBR PLAN 1GB ACCT SH	1	0.0 Bytes	

Daily Usage Trend (Current Billing Cycle)

Filtering a dashboard

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).

Build a custom filter

1. Click **Add**. The *Edit filter* dialog opens.
   a. Select the Field to filter.
   b. Select the Condition type.
   c. Select the *Value* to filter on.
   d. Click **Save**.

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

Search

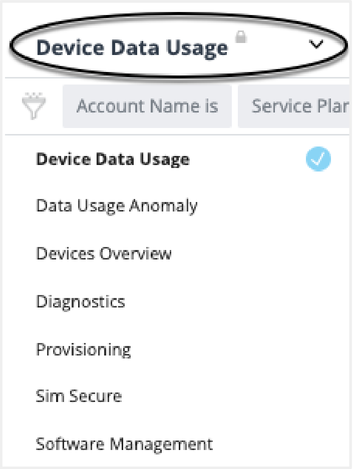
Click the search icon 🔍 to type a keyword, or click the Natural Language Processor icon to type a question.

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

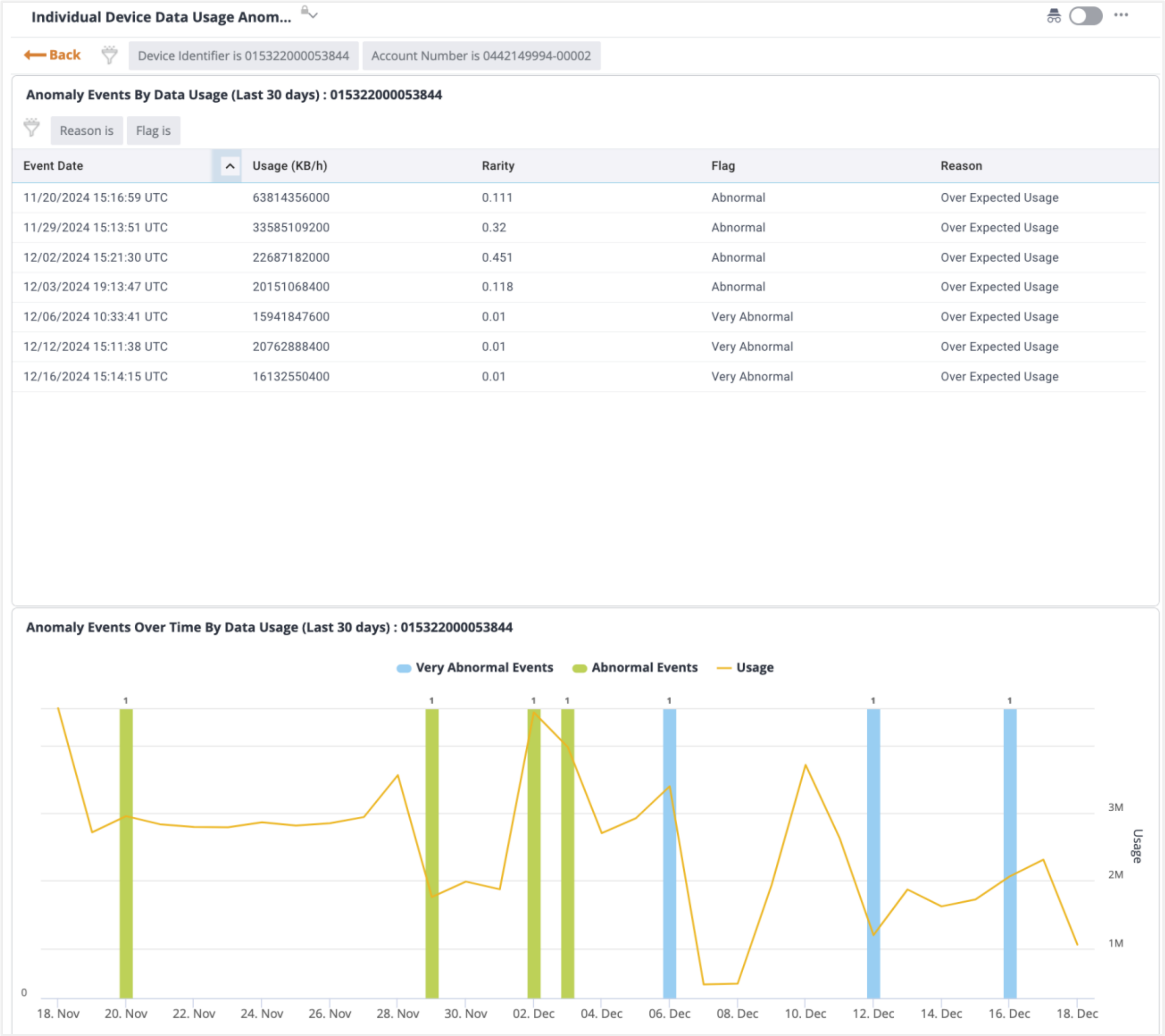
Click the view dropdown to select one of the following dashboard views.



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

Data Usage Anomaly

Data Usage Anomaly dashboard provides insights data usage anomalies. 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.



Individual Device Data Usage Anom...

Device Identifier is 015322000053844 | Account Number is 0442149994-00002

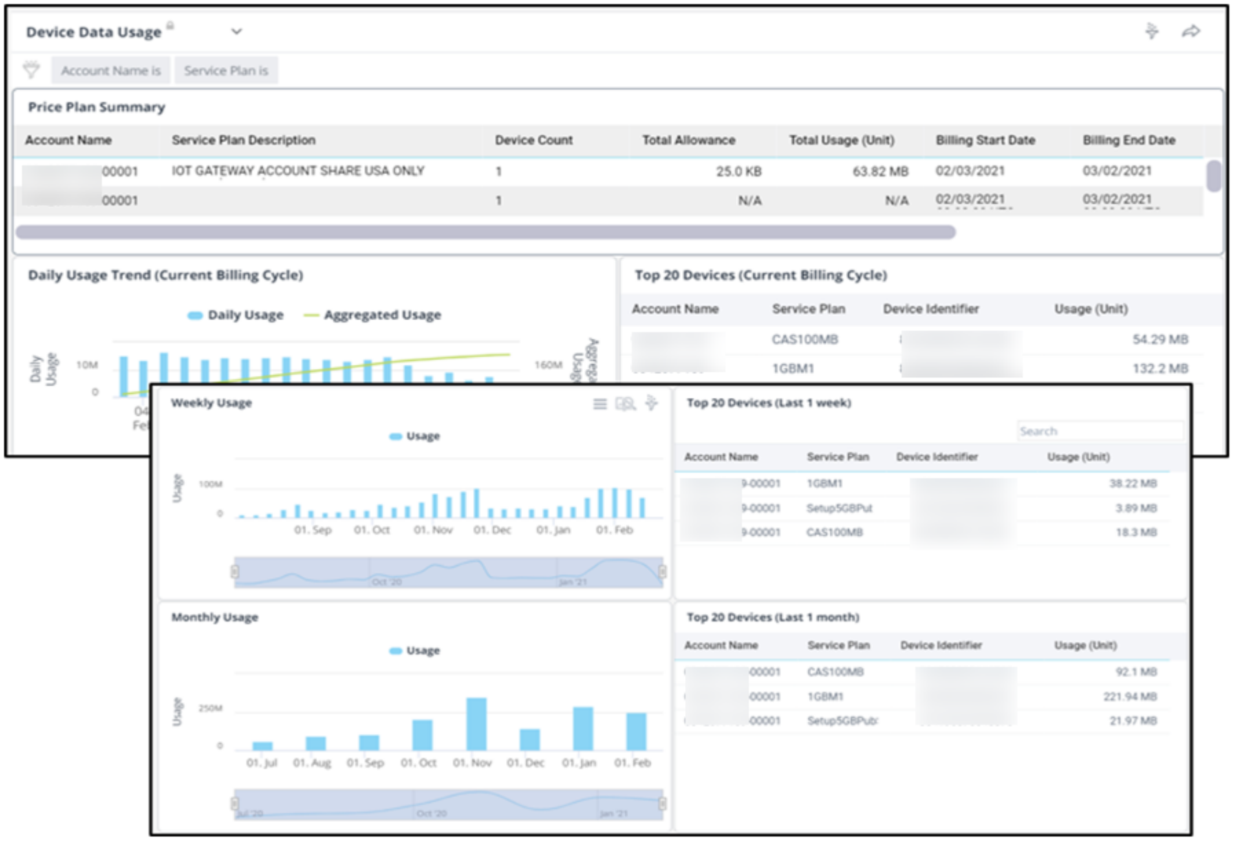
Anomaly Events By Data Usage (Last 30 days) : 015322000053844

Event Date	Usage (KB/h)	Rarity	Flag	Reason
11/20/2024 15:16:59 UTC	63814356000	0.111	Abnormal	Over Expected Usage
11/29/2024 15:13:51 UTC	33585109200	0.32	Abnormal	Over Expected Usage
12/02/2024 15:21:30 UTC	22687182000	0.451	Abnormal	Over Expected Usage
12/03/2024 19:13:47 UTC	20151068400	0.118	Abnormal	Over Expected Usage
12/06/2024 10:33:41 UTC	15941847600	0.01	Very Abnormal	Over Expected Usage
12/12/2024 15:11:38 UTC	20762888400	0.01	Very Abnormal	Over Expected Usage
12/16/2024 15:14:15 UTC	16132550400	0.01	Very Abnormal	Over Expected Usage

Anomaly Events Over Time By Data Usage (Last 30 days) : 015322000053844

Device Data Usage

Device 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.



Price Plan Summary

Account Name	Service Plan Description	Device Count	Total Allowance	Total Usage (Unit)	Billing Start Date	Billing End Date
[redacted]00001	IOT GATEWAY ACCOUNT SHARE USA ONLY	1	25.0 KB	63.82 MB	02/03/2021	03/02/2021
[redacted]00001		1	N/A	N/A	02/03/2021	03/02/2021

Top 20 Devices (Current Billing Cycle)

Account Name	Service Plan	Device Identifier	Usage (Unit)
[redacted]	CAS100MB	[redacted]	54.29 MB
[redacted]	1GBM1	[redacted]	132.2 MB

Top 20 Devices (Last 1 week)

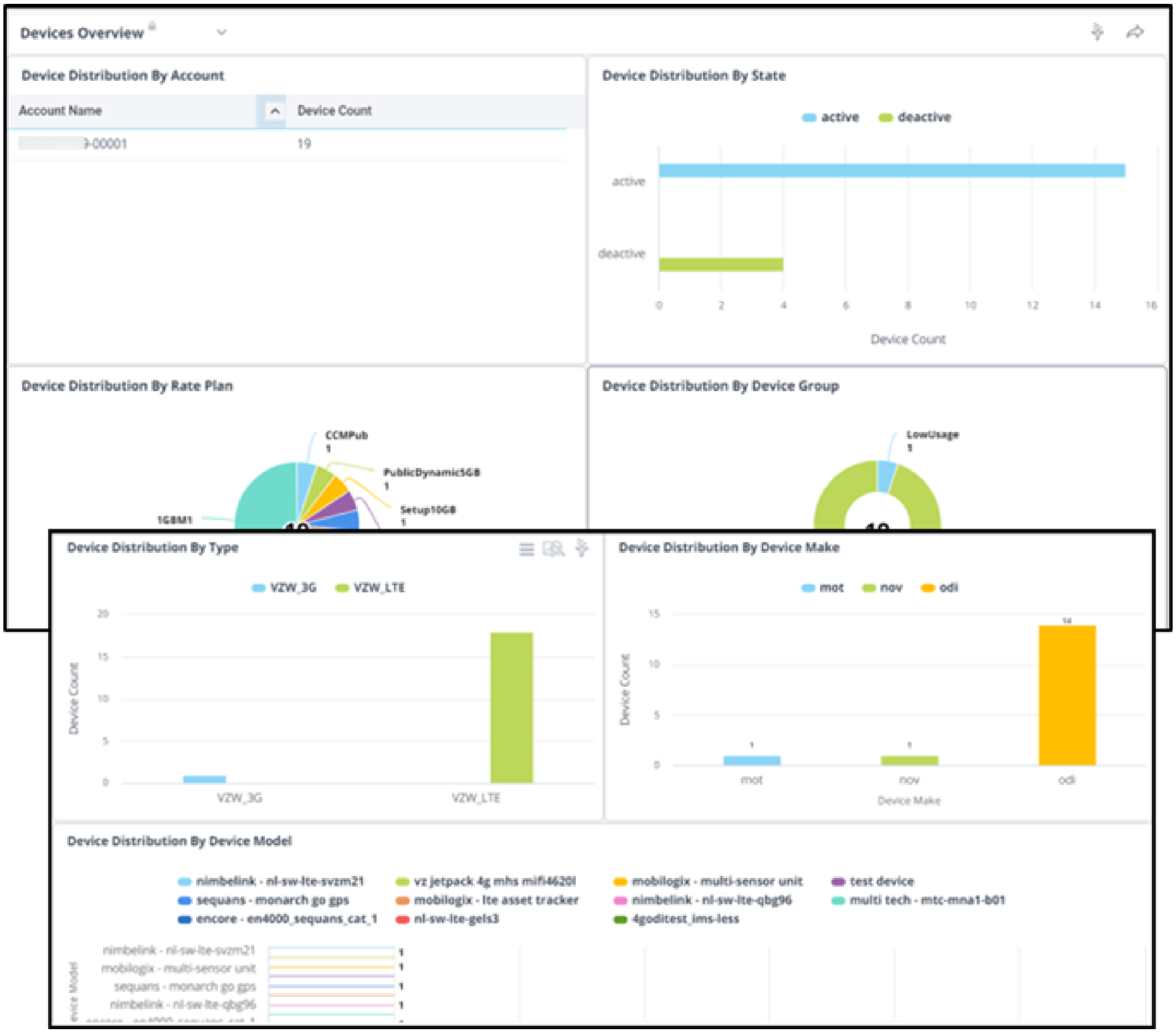
Account Name	Service Plan	Device Identifier	Usage (Unit)
[redacted]9-00001	1GBM1	[redacted]	38.22 MB
[redacted]9-00001	Setup5GBPut	[redacted]	3.89 MB
[redacted]9-00001	CAS100MB	[redacted]	18.3 MB

Top 20 Devices (Last 1 month)

Account Name	Service Plan	Device Identifier	Usage (Unit)
[redacted]00001	CAS100MB	[redacted]	92.1 MB
[redacted]00001	1GBM1	[redacted]	221.94 MB
[redacted]00001	Setup5GBPub	[redacted]	21.97 MB

Devices Overview

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



Devices Overview

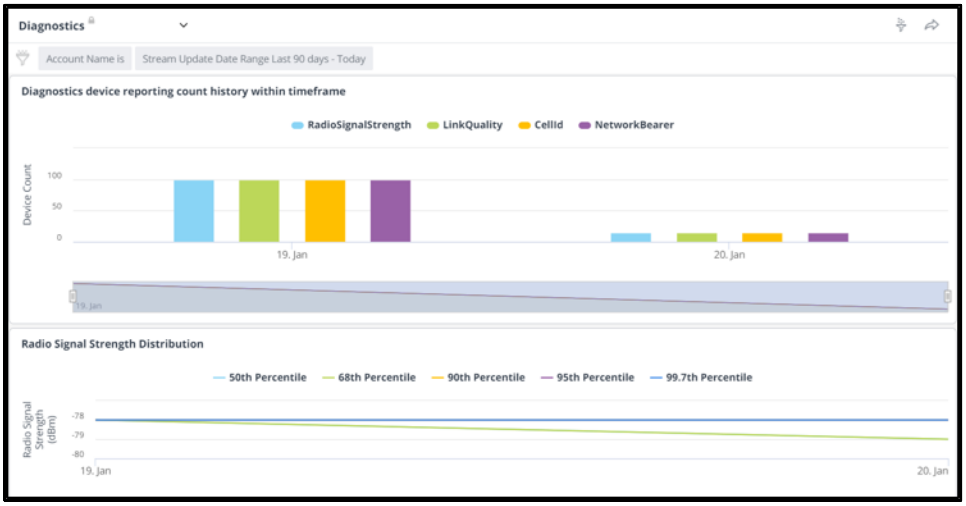
Device Distribution By Account

Account Name	Device Count
[redacted]-00001	19

Device Distribution By State
active
deactive
active
deactive
0
2
4
6
8
10
12
14
16
Device Count
Device Distribution By Rate Plan
CCMPub
1
PublicDynamic5GB
1
Setup10GB
1
1GBM1
Device Distribution By Device Group
LowUsage
1
Device Distribution By Type
VZW_3G
VZW_LTE
20
15
10
5
0
Device Count
VZW_3G
VZW_LTE
Device Distribution By Device Make
mot
nov
odi
15
10
5
0
Device Count
1
1
14
mot
nov
odi
Device Make
Device Distribution By Device Model
nimbelink - nl-sw-lte-svzm21
vz jetpack 4g mhs mifi4620l
mobilogix - multi-sensor unit
test device
sequans - monarch go gps
mobilogix - lte asset tracker
nimbelink - nl-sw-lte-qbg96
multi tech - mtc-mna1-b01
encore - en4000_sequans_cat_1
nl-sw-lte-gels3
4goditest_ims-less
nimbelink - nl-sw-lte-svzm21
mobilogix - multi-sensor unit
sequans - monarch go gps
nimbelink - nl-sw-lte-qbg96
1
1
1
1
evice Model

Diagnostics

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

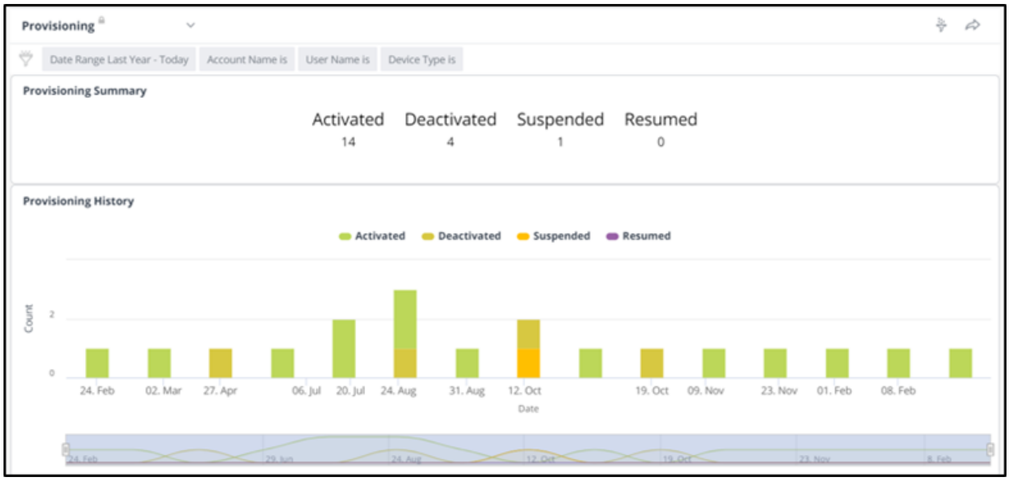


Diagnostics

Account Name is | Stream Update Date Range Last 90 days - Today

Provisioning

Provisioning analytics dashboard provides insights into provisioning history.



Provisioning

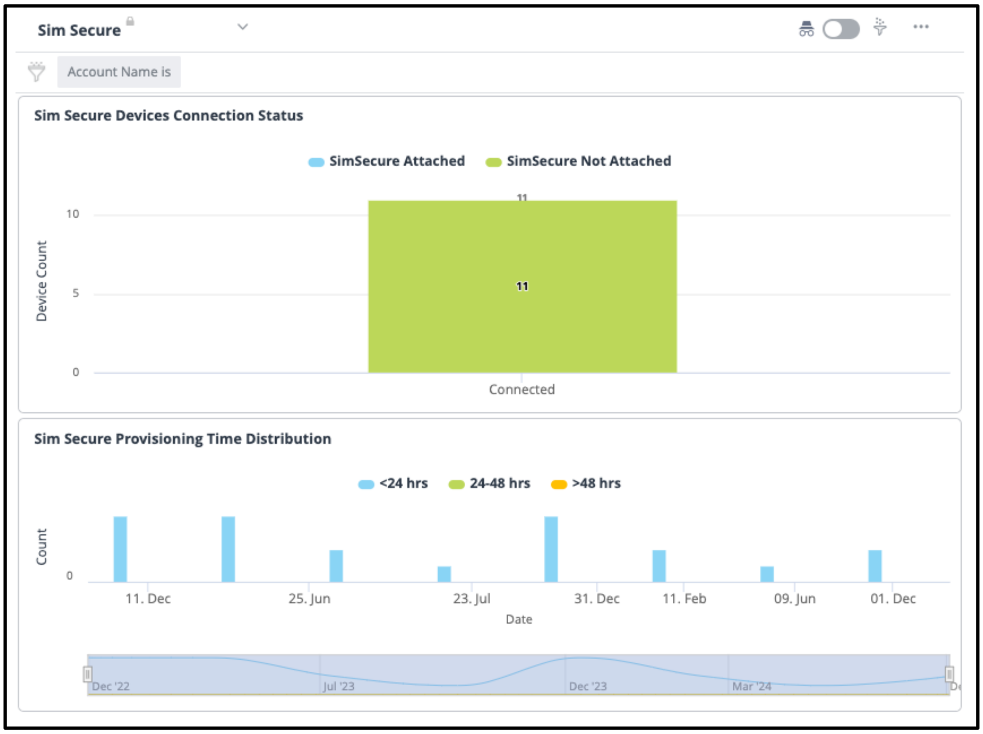
Date Range Last Year - Today | Account Name is | User Name is | Device Type is

Provisioning Summary

Activated	Deactivated	Suspended	Resumed
14	4	1	0

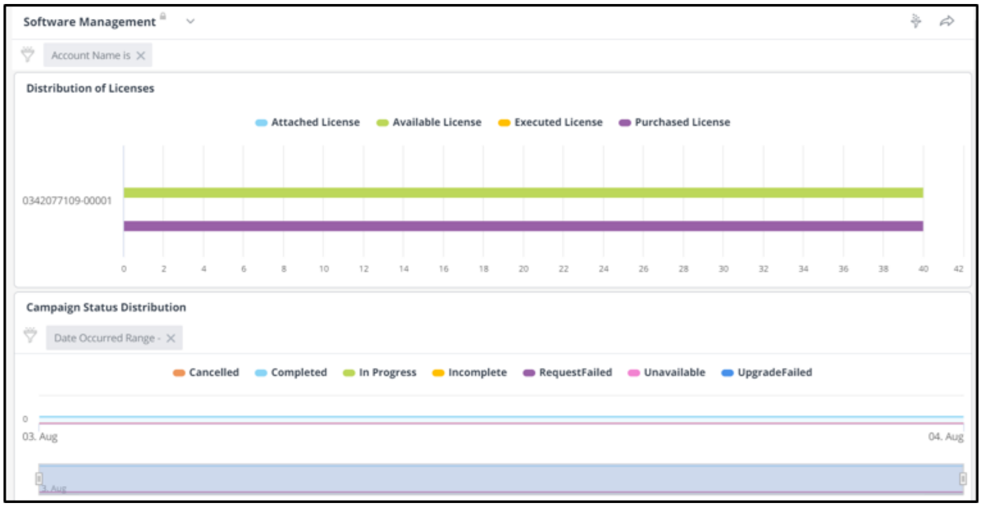
SIM Secure

SIM-Secure analytics dashboards provide insights into license utilization and provisioning time (if available).

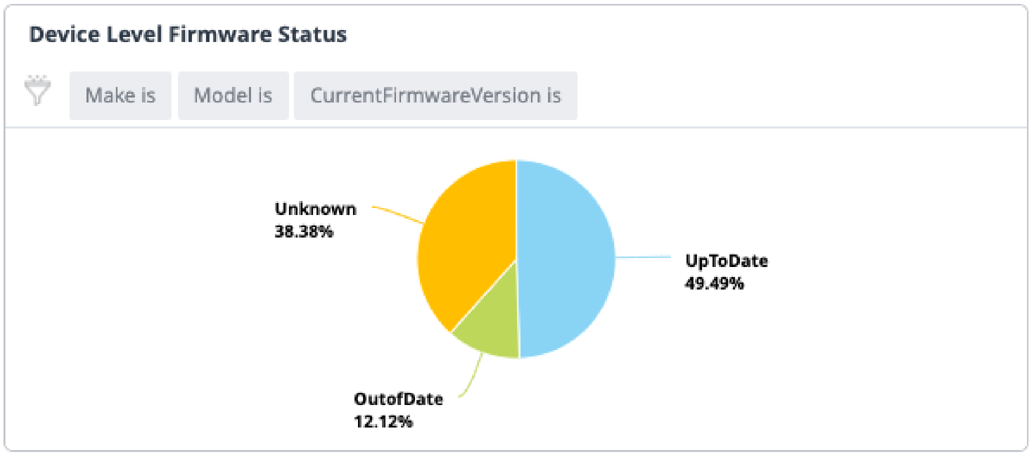


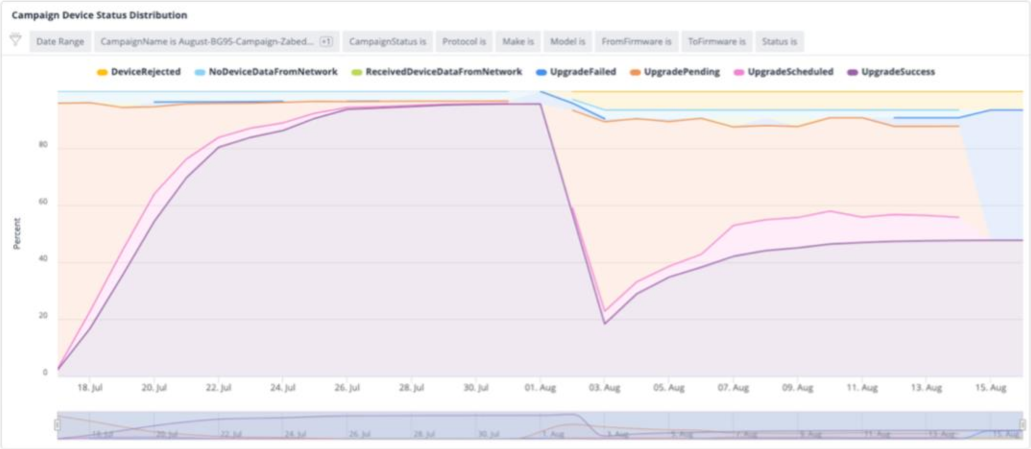
Software Management

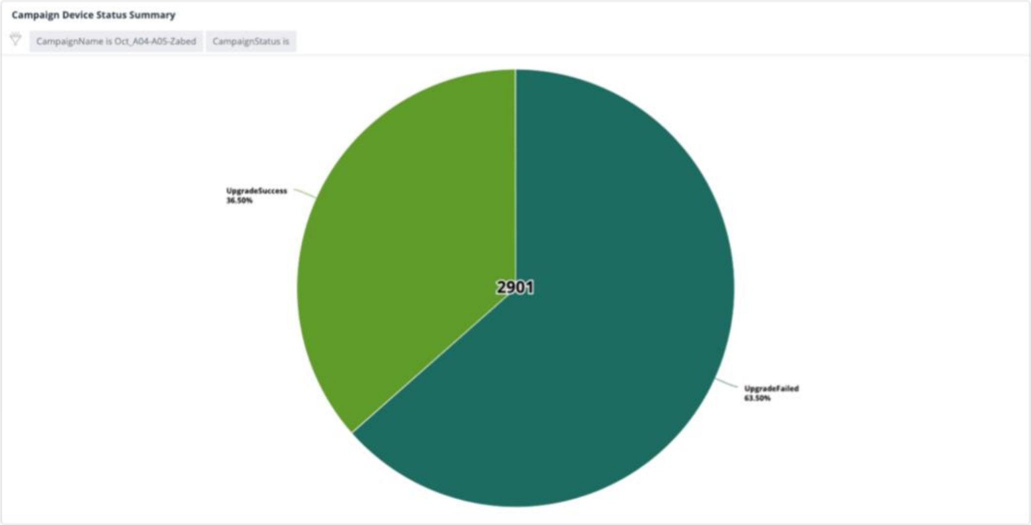
Software Management analytics dashboard provides a quick view of how many devices are up-to-date on their firmware and which require new firmware. You can provide a make, model or current firmware (from and to).



The second and third charts provide campaign-level analytics. For example, the second chart provides time series view of the campaign status. The third chart provides the status as of the previous evening. Search by providing campaign name(s) of interest.

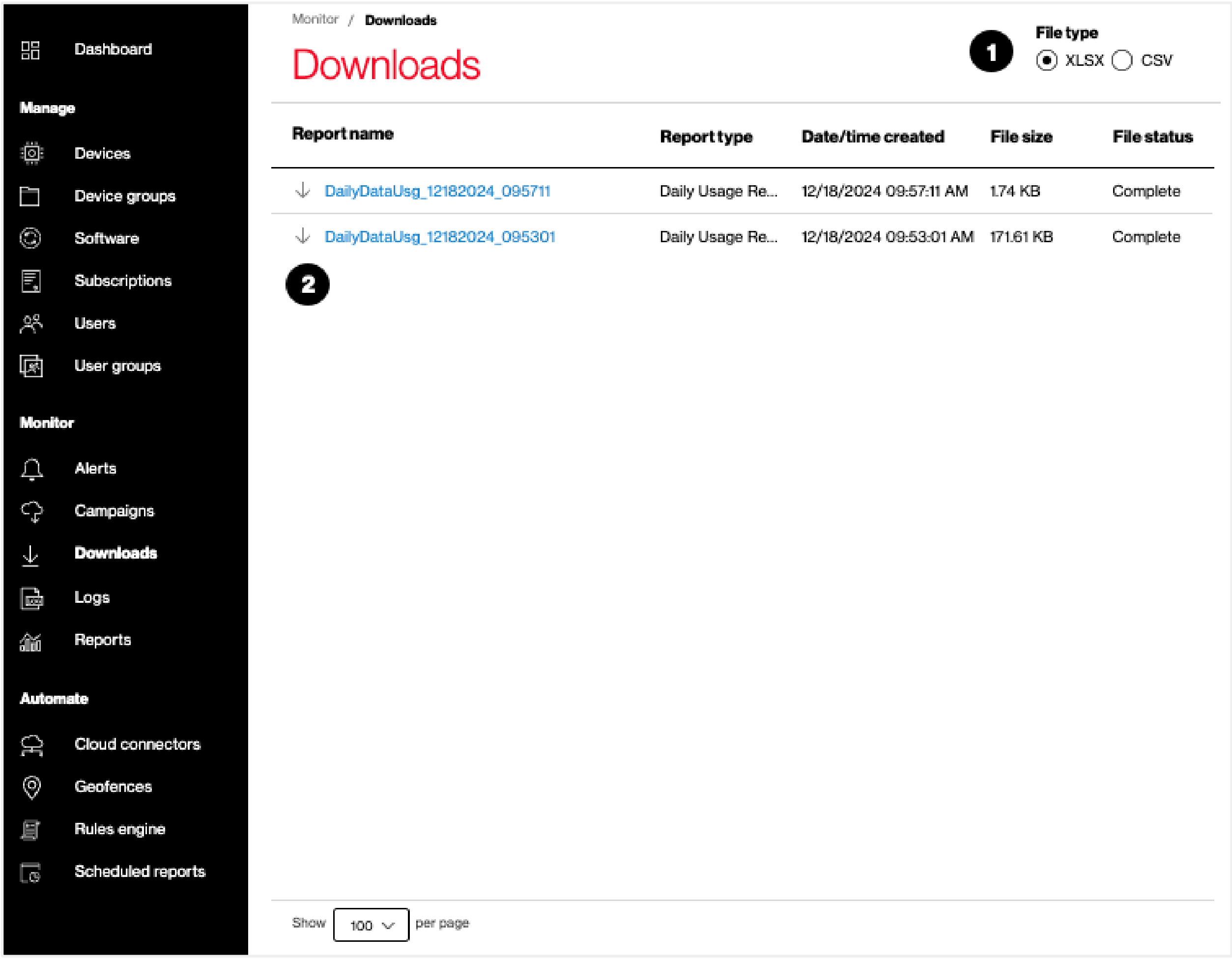






Downloads

The *Downloads* page lists all the files that are available for downloading. On the left navigation, click **Downloads** to open the page.



File type ● XLSX ○ CSV

Report name	Report type	Date/time created	File size	File status
DailyDataUsg_12182024_095711	Daily Usage Re...	12/18/2024 09:57:11 AM	1.74 KB	Complete
DailyDataUsg_12182024_095301	Daily Usage Re...	12/18/2024 09:53:01 AM	171.61 KB	Complete

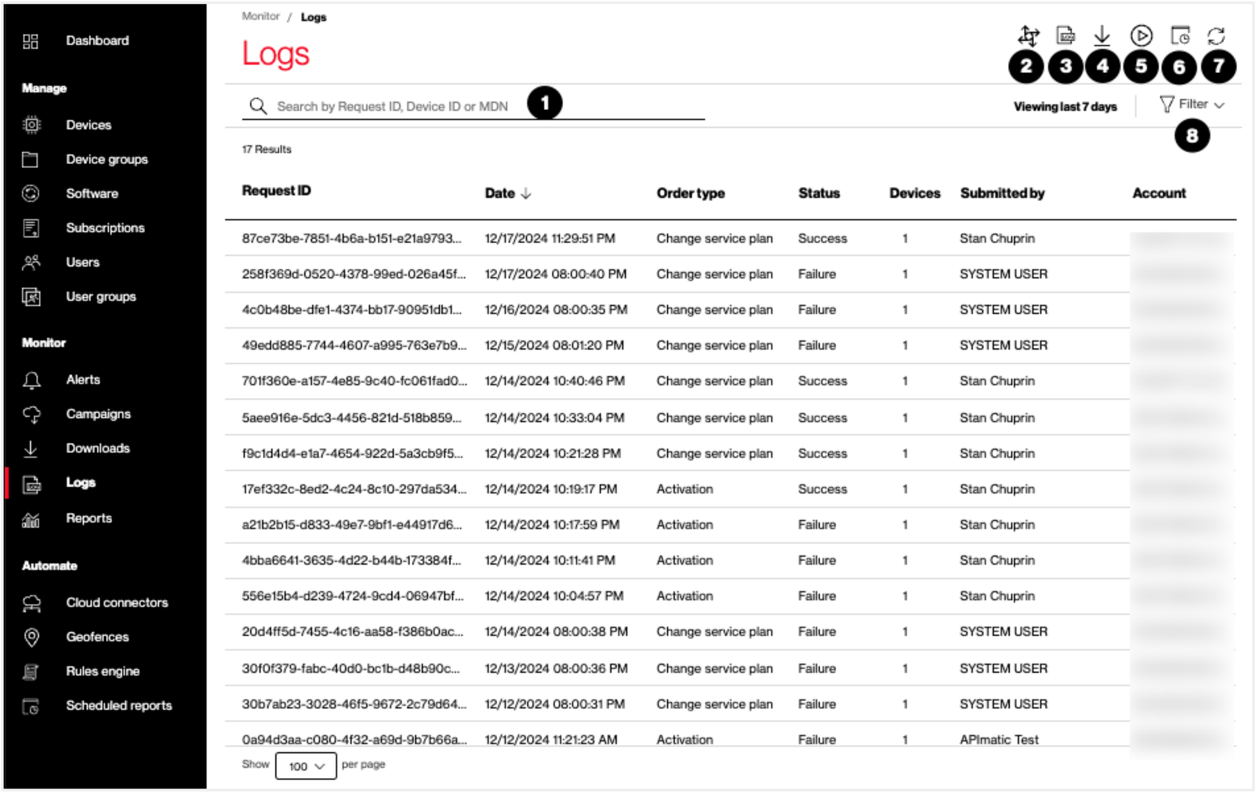
Elements on the Downloads page		
1		**File Type options** – Select the file format to download.
2	↓	**Download** – Export the file.

How to download a report

2. At the top-right of the *Downloads* page, click the **File type** of your choice (XLSX or CSV).
3. 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.



Search by Request ID, Device ID or MDN

17 Results

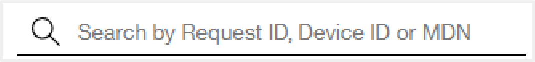
Request ID	Date ↓	Order type	Status	Devices	Submitted by	Account
87ce73be-7851-4b6a-b151-e21a9793...	12/17/2024 11:29:51 PM	Change service plan	Success	1	Stan Chuprin	[redacted]
258f369d-0520-4378-99ed-026a45f...	12/17/2024 08:00:40 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
4c0b48be-dfe1-4374-bb17-90951db1...	12/16/2024 08:00:35 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
49edd885-7744-4607-a995-763e7b9...	12/15/2024 08:01:20 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
701f360e-a157-4e85-9c40-fc061fad0...	12/14/2024 10:40:46 PM	Change service plan	Success	1	Stan Chuprin	[redacted]
5aee916e-5dc3-4456-821d-518b859...	12/14/2024 10:33:04 PM	Change service plan	Success	1	Stan Chuprin	[redacted]
f9c1d4d4-e1a7-4654-922d-5a3cb9f5...	12/14/2024 10:21:28 PM	Change service plan	Success	1	Stan Chuprin	[redacted]
17ef332c-8ed2-4c24-8c10-297da534...	12/14/2024 10:19:17 PM	Activation	Success	1	Stan Chuprin	[redacted]
a21b2b15-d833-49e7-9bf1-e44917d6...	12/14/2024 10:17:59 PM	Activation	Failure	1	Stan Chuprin	[redacted]
4bba6641-3635-4d22-b44b-173384f...	12/14/2024 10:11:41 PM	Activation	Failure	1	Stan Chuprin	[redacted]
556e15b4-d239-4724-9cd4-06947bf...	12/14/2024 10:04:57 PM	Activation	Failure	1	Stan Chuprin	[redacted]
20d4ff5d-7455-4c16-aa58-f386b0ac...	12/14/2024 08:00:38 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
30f0f379-fabc-40d0-bc1b-d48b90c...	12/13/2024 08:00:36 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
30b7ab23-3028-46f5-9672-2c79d64...	12/12/2024 08:00:31 PM	Change service plan	Failure	1	SYSTEM USER	[redacted]
0a94d3aa-c080-4f32-a69d-9b7b66a...	12/12/2024 11:21:23 AM	Activation	Failure	1	APImatic Test	[redacted]

Show 100 per page

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	▷	Tutorial videos – View available video tutorials.
6	🗓	Schedule – Automate and schedule a report.
7	↻	Refresh – Refresh the page.
8	▽	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.



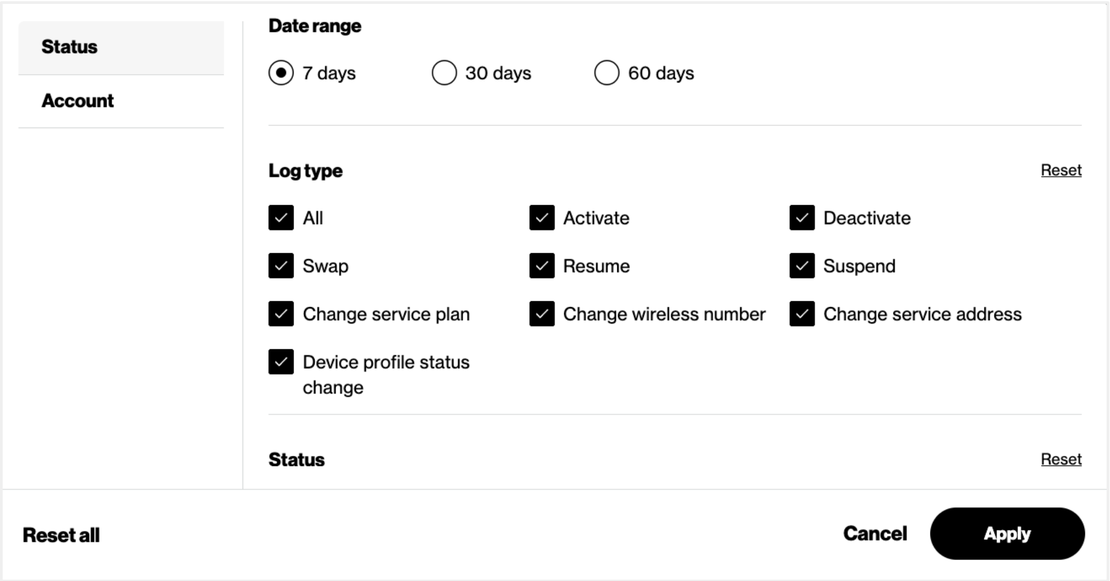
Search by Request ID, Device ID or MDN

NOTE: Searches are not case sensitive.

Applying logs filters

How to apply filters

1. Click Filter ⌄. The *Filter* page opens.



Status

Account

Date range

● 7 days ○ 30 days ○ 60 days

Log type Reset

☑ All ☑ Activate ☑ Deactivate

☑ Swap ☑ Resume ☑ Suspend

☑ Change service plan ☑ Change wireless number ☑ Change service address

☑ Device profile status change

Status Reset

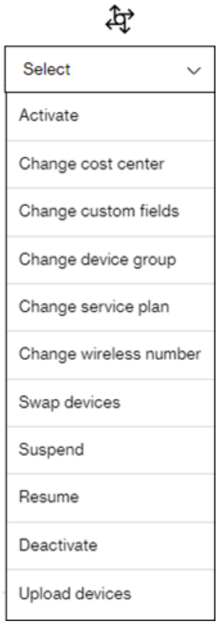
Reset all **Cancel** **Apply**

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

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.



NOTE: See Provisioning actions in the Devices section for more information.

View application log

Click the application logs icon. The legacy Application Log page opens. See the section on the Applications Log for more details.

Download the transaction log

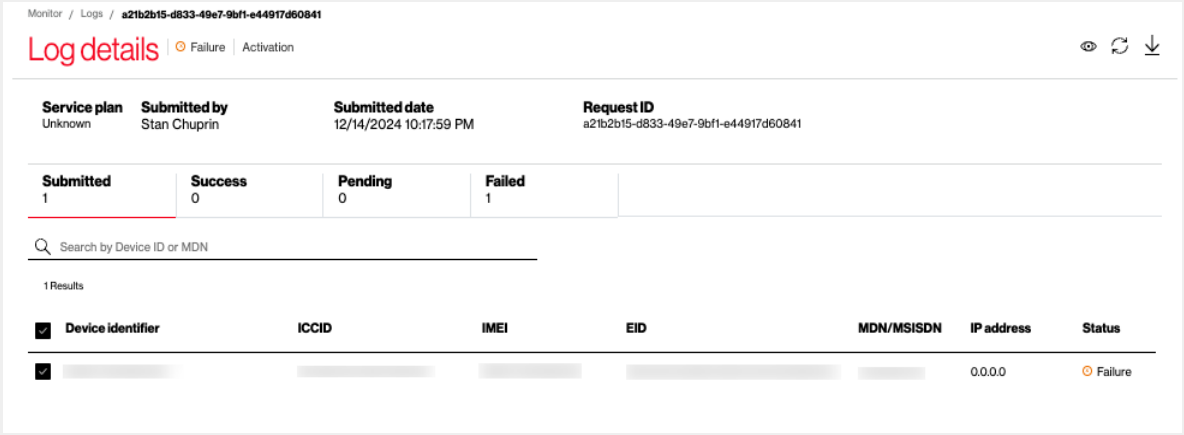
Click the download icon to download the application log.

Log details

The *Log details* page shows additional details for a transaction.

To view log details

1. On the left navigation, click **Logs**. The *Logs* page opens.
2. Click a **Request ID**. The *Logs Details* page opens with details about the provisioning transaction.



Monitor / Logs / a21b2b15-d833-49e7-9bf1-e44917d60841

Log details | Failure | Activation

Service plan	Submitted by	Submitted date	Request ID
Unknown	Stan Chuprin	12/14/2024 10:17:59 PM	a21b2b15-d833-49e7-9bf1-e44917d60841

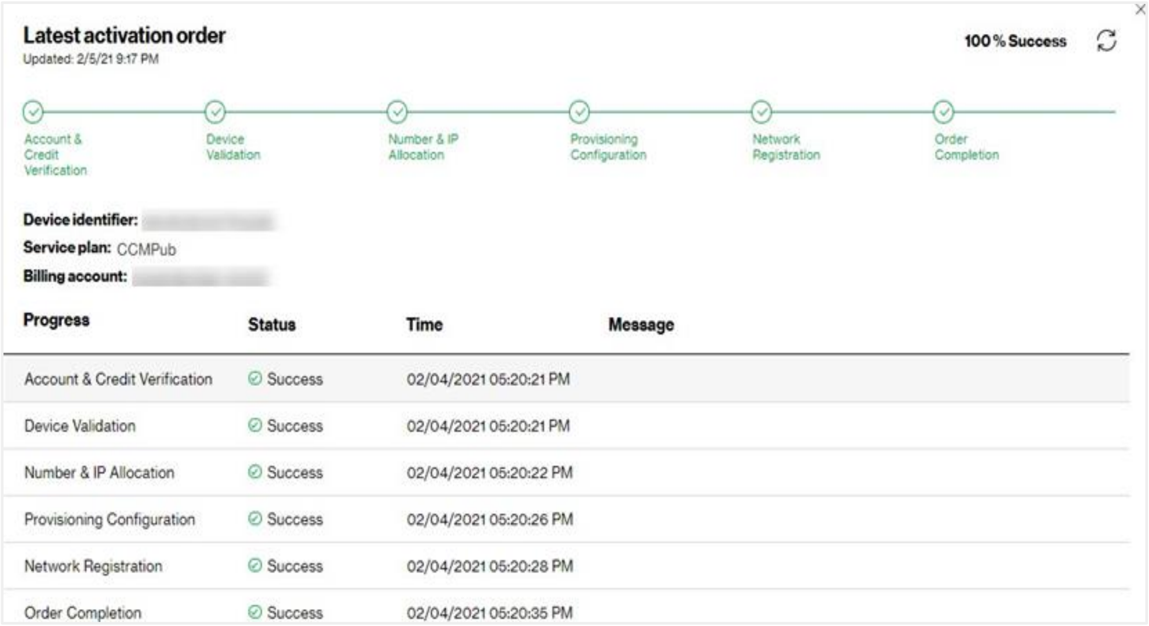
Submitted	Success	Pending	Failed
1	0	0	1

Search by Device ID or MDN

1 Results

☑	Device identifier	ICCID	IMEI	EID	MDN/MSISDN	IP address	Status
☑						0.0.0.0	Failure

For Activation orders that have completed in the past seven days, you can click the status value (e.g. Success, Failure) to view the order status. The following is an example of a **successful** activation order.



Latest activation order

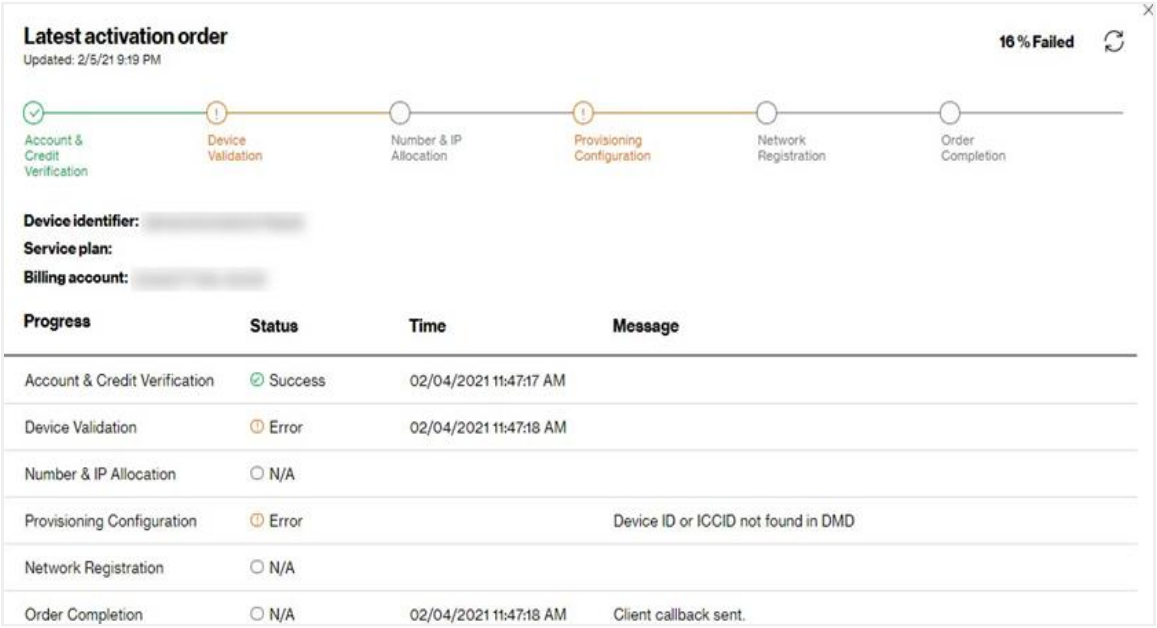
Updated: 2/5/21 9:17 PM

100 % Success

Device identifier:
Service plan: CCMPub
Billing account:

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

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



Latest activation order
Updated: 2/5/21 9:19 PM

16 % Failed

Device identifier: [redacted]
Service plan:
Billing account: [redacted]

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

Resubmit an order

If an activation order fails, users have the option of resubmitting the activation order. Click the eye icon 👁 and select **Resubmit activation**.

Refresh page action

Click the refresh icon ↻ to refresh the page.

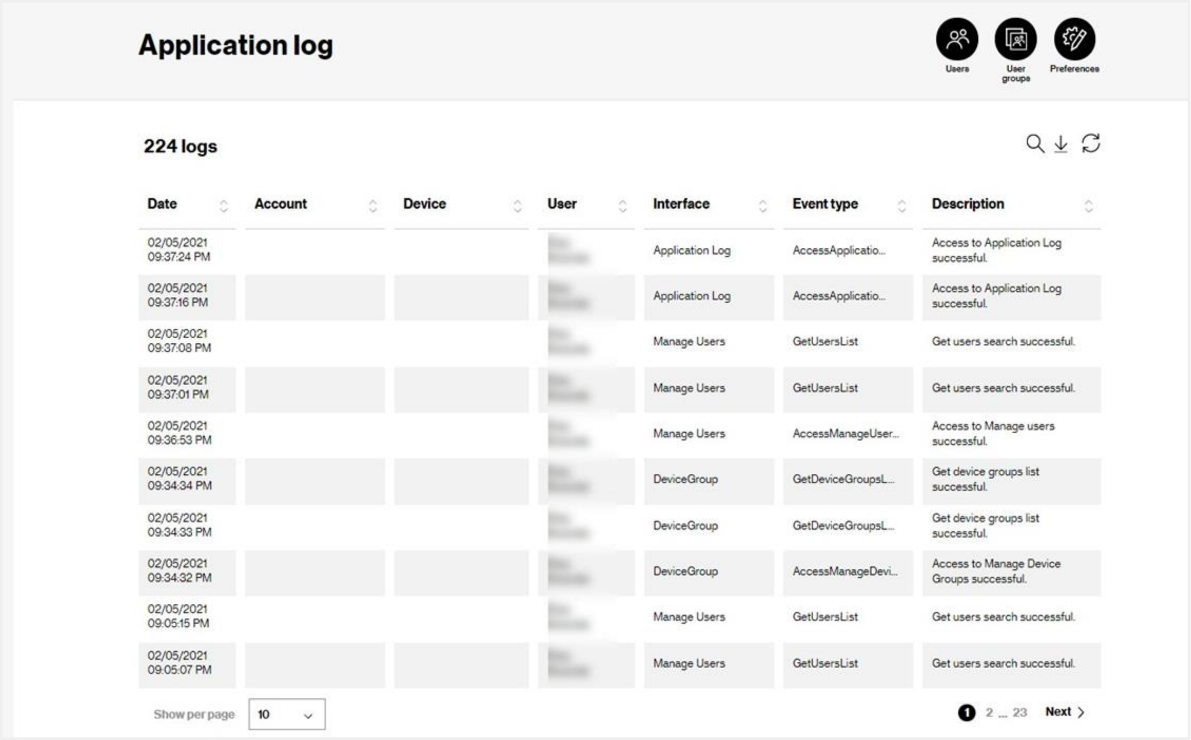
Download a report

Click the download icon ⤓ to download the report that is on the results page.

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.

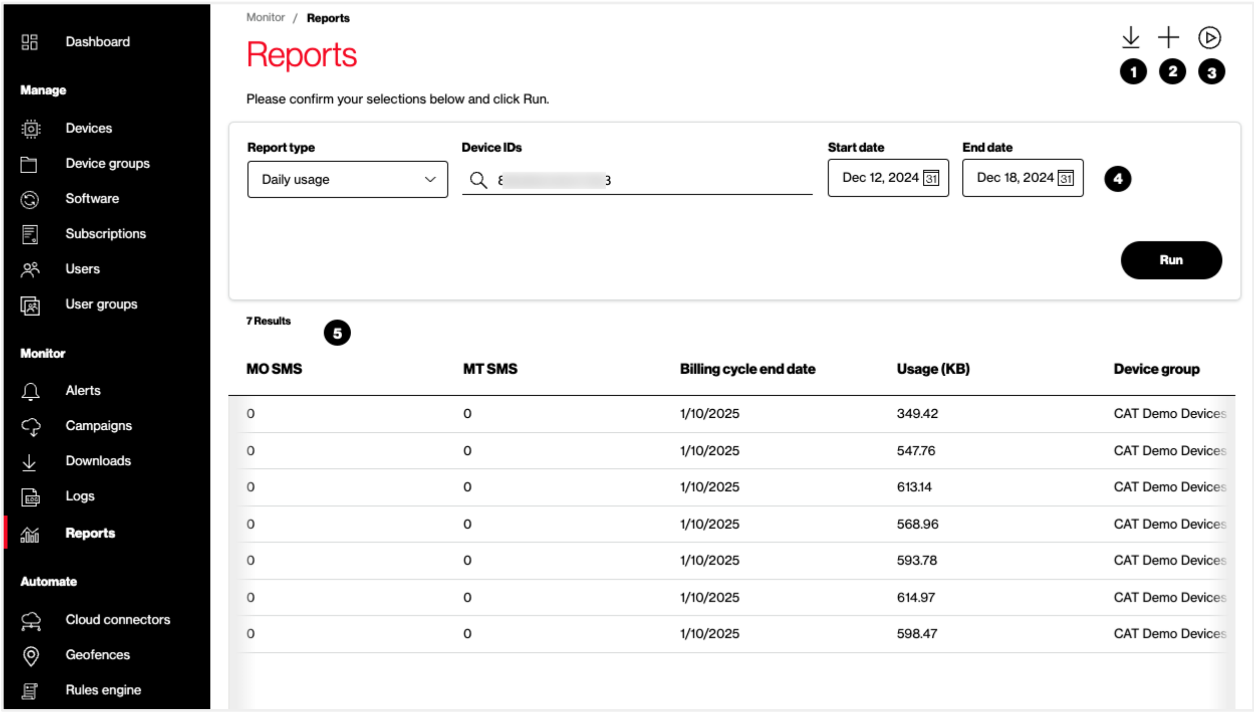


224 logs

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

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.



Reports

Please confirm your selections below and click Run.

Report type: Daily usage

Device IDs: [redacted]

Start date: Dec 12, 2024

End date: Dec 18, 2024

7 Results

MO SMS	MT SMS	Billing cycle end date	Usage (KB)	Device group
0	0	1/10/2025	349.42	CAT Demo Devices
0	0	1/10/2025	547.76	CAT Demo Devices
0	0	1/10/2025	613.14	CAT Demo Devices
0	0	1/10/2025	568.96	CAT Demo Devices
0	0	1/10/2025	593.78	CAT Demo Devices
0	0	1/10/2025	614.97	CAT Demo Devices
0	0	1/10/2025	598.47	CAT Demo Devices

Elements on the Reports page		
1	↓	**Download** – Download the report.
2	+	**Create and schedule** – Create a new report and schedule it to run at predetermined dates/times.
3	▷	Tutorial videos – View available video tutorials.
4		**Report criteria** – Enter the selection criteria for the report.
5		**Results page** – The area where online reports are displayed.

There are two types of reports that you can take:

Online reports – Run reports immediately. Results will display in the results pane.

Offline reports – These reports are run in the background and will be sent to the Downloads center when complete. Scheduled reports are usually offline reports.

Download a report

How to download an online report

4. Click the download icon ⤓ to download the report that is on the results page.

Running online reports

How to run online reports

1. On the left navigation, click **Reports**. The *Reports* page opens.
2. Enter the report criteria:
    a. 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.

    b. Type up to 10 **Device IDs**

    c. Select a **Start date**

    d. Select an **End date**

    e. Click **Run**.

The report will display in the results pane.

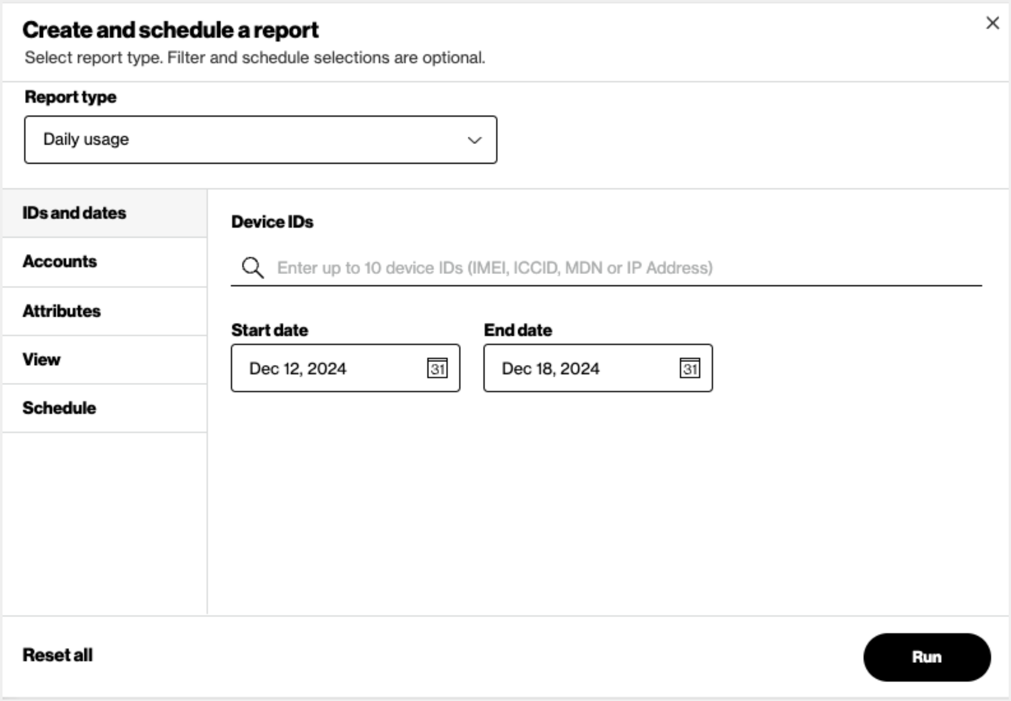
NOTE: Alternatively, you can open the *Reports* page from the Devices page by selecting one or more devices and clicking the reports icon 📊 and then choosing the report to run.

Running advanced reports

Use the *Create and schedle advanced reports* + icon to create, save, and/or schedule advanced reports. These reports usually take longer and are submitted in the background for processing. When reports complete, they are made available on the Downloads page.

How to create and schedule an offline report

1. On the left navigation, click **Reports**. The *Reports* page opens.
2. Click the plus icon + . The *Create and schedule a report* screen appears.



Create and schedule a report

Select report type. Filter and schedule selections are optional.

Report type

Daily usage

Device IDs

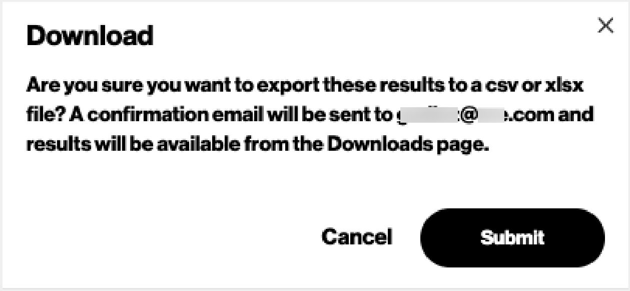
Enter up to 10 device IDs (IMEI, ICCID, MDN or IP Address)

Start date Dec 12, 2024

End date Dec 18, 2024

3. Select the **Report type**.
4. Enter select **Device IDs**. If you want the report to apply to all devices enter the “%” wildcard character.
5. Enter the **Start date** and **End date**.
6. Select an **Account** or choose “All” for all accounts.
7. Select any **Service plans** or choose “All” for all service plans.
8. Select **Attributes** such as device groups or special fields.
9. Select a **Table view** to use the predefined view. The view has a list of columns that come standard with the view. You can also create a new view by clicking **Create new**. See the section on *Creating a report view*.
10. Select the **Schedule type**.
    a. Run as soon as possible – This will run the report immediately as an online report.
    b. Schedule for later – This will schedule the report to run in the background as an offline report.

11. Give the report a **Name**. This field is required when scheduling a report.
12. Click **Run**. A confirmation popup will ask you to confirm whether to submit the report request.

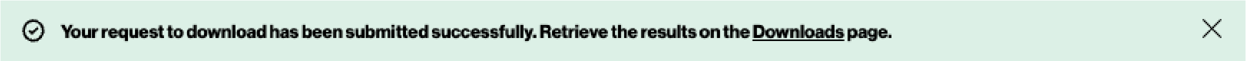


Download

Are you sure you want to export these results to a csv or xlsx file? A confirmation email will be sent to [redacted]@[redacted].com and results will be available from the Downloads page.

13. Click **Submit**.

You will see a message at the top of the page indicating that the report has been submitted and to retrieve it in the Downloads page. You will get an email once the report has completed.

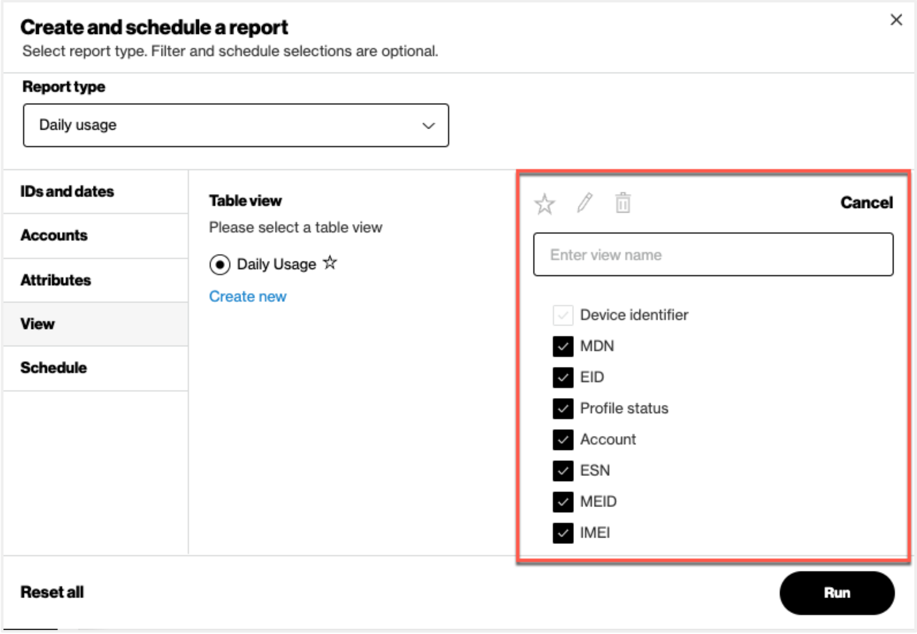


Your request to download has been submitted successfully. Retrieve the results on the Downloads page.

Report views

How to create and new report view

1. From the *Create and schedule a report* screen, click the **View** tab.
2. Select the **Create new**. The righthand side of the screen is enabled.



Create and schedule a report

Select report type. Filter and schedule selections are optional.

Report type: Daily usage

Table view

Please select a table view

● Daily Usage ☆

Create new

Enter view name

☑ Device identifier
☑ MDN
☑ EID
☑ Profile status
☑ Account
☑ ESN
☑ MEID
☑ IMEI

3. Give the view a **name**.
4. Scroll through the list of available fields and check the **fields** you want to appear on the report.

5. At the bottom of the list, click **Save**. Yor new view will appear on the list of available table views.

How to edit a report view

1. From the *Create and schedule a report* screen, click the **View** tab.
2. Select a **Table view**.

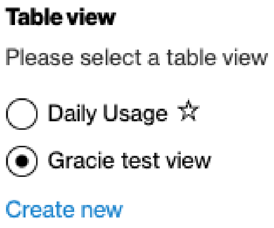


Table view

Please select a table view

○ Daily Usage ☆

● Gracie test view

Create new

The icons on the right side of the screen are enabled.

☆ ✎ 🗑

3. Click the edit icon ✎ . The righthand side of the screen is enabled.
4. Make your changes.
5. Click **Save**.

How to delete a report view

1. From the *Create and schedule a report* screen, click the **View** tab.

   Select a **Table view**. The icons on the right side of the screen are enabled.

   ☆ ✎ 🗑

2. Click the delete icon 🗑 . You will be prompted to confirm deletion.
3. Click **Submit**.

How to make a report view the default layout

1. From the *Create and schedule a report* screen, click the **View** tab.

   Select a **Table view**. The icons on the right side of the screen are enabled.

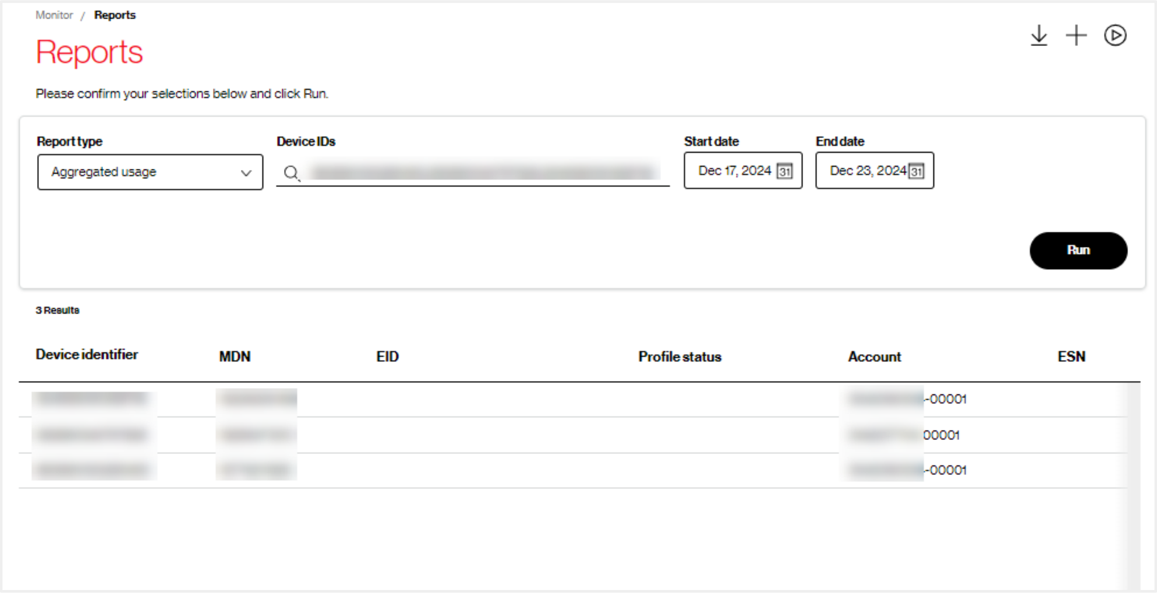
   ☆ ✎ 🗑

2. Click the star icon ☆ . You will be prompted to confirm setting the view as the default layout.
3. Click **Submit**.

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.

The offline reporting maximum date range is 12 months.



Reports

Please confirm your selections below and click Run.

Report type: Aggregated usage

Device IDs: [redacted]

Start date: Dec 17, 2024

End date: Dec 23, 2024

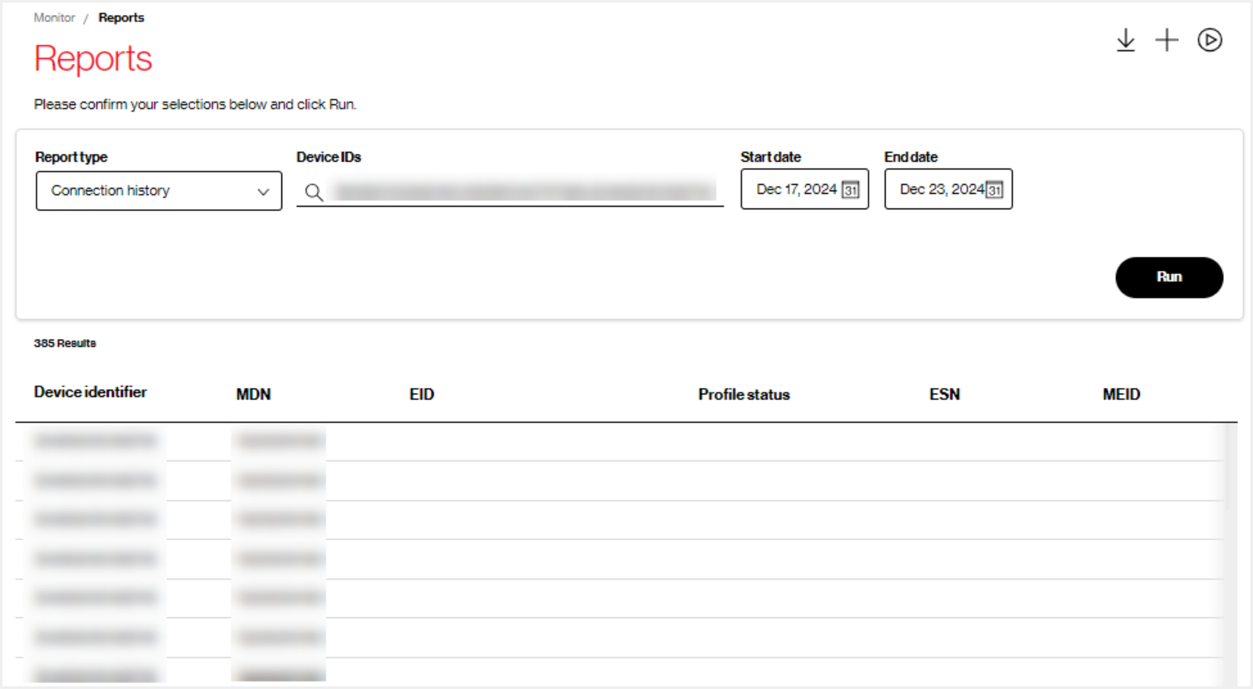
3 Results

Device identifier	MDN	EID	Profile status	Account	ESN
[redacted]	[redacted]			[redacted]-00001	
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]-00001	

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.

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



Reports

Please confirm your selections below and click Run.

Report type: Connection history

Device IDs: [redacted]

Start date: Dec 17, 2024

End date: Dec 23, 2024

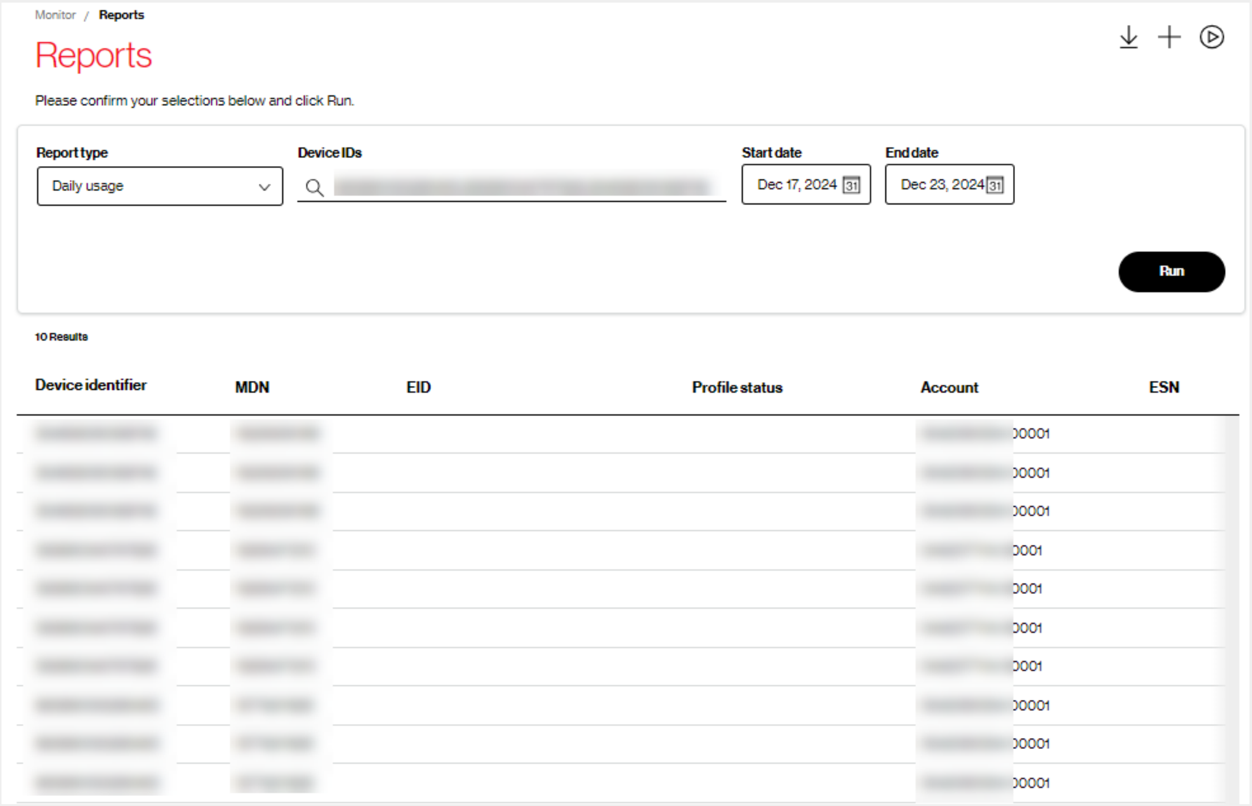
385 Results

Device identifier	MDN	EID	Profile status	ESN	MEID
[redacted]	[redacted]				
[redacted]	[redacted]				
[redacted]	[redacted]				
[redacted]	[redacted]				
[redacted]	[redacted]				
[redacted]	[redacted]				
[redacted]	[redacted]				

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.

The offline reporting maximum date range is 12 months.



Monitor / Reports

Reports

Please confirm your selections below and click Run.

Report type: Daily usage

Device IDs: [redacted]

Start date: Dec 17, 2024

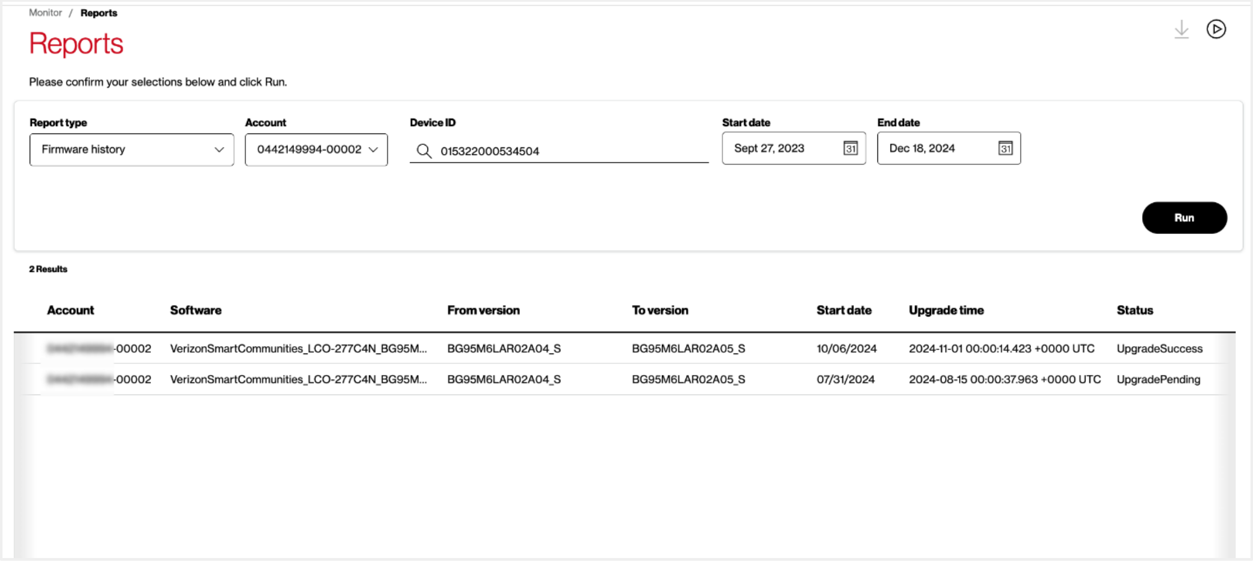
End date: Dec 23, 2024

10 Results

Device identifier	MDN	EID	Profile status	Account	ESN
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]0001	
[redacted]	[redacted]			[redacted]0001	
[redacted]	[redacted]			[redacted]0001	
[redacted]	[redacted]			[redacted]0001	
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]00001	
[redacted]	[redacted]			[redacted]00001	

Firmware history report

Use the *Firmware history* report to firmware changes as a result of firmware over the air (FOTA) campaigns in ThingSpace for a device.



Reports

Please confirm your selections below and click Run.

Report type	Firmware history
Account	0442149994-00002
Device ID	015322000534504
Start date	Sept 27, 2023
End date	Dec 18, 2024

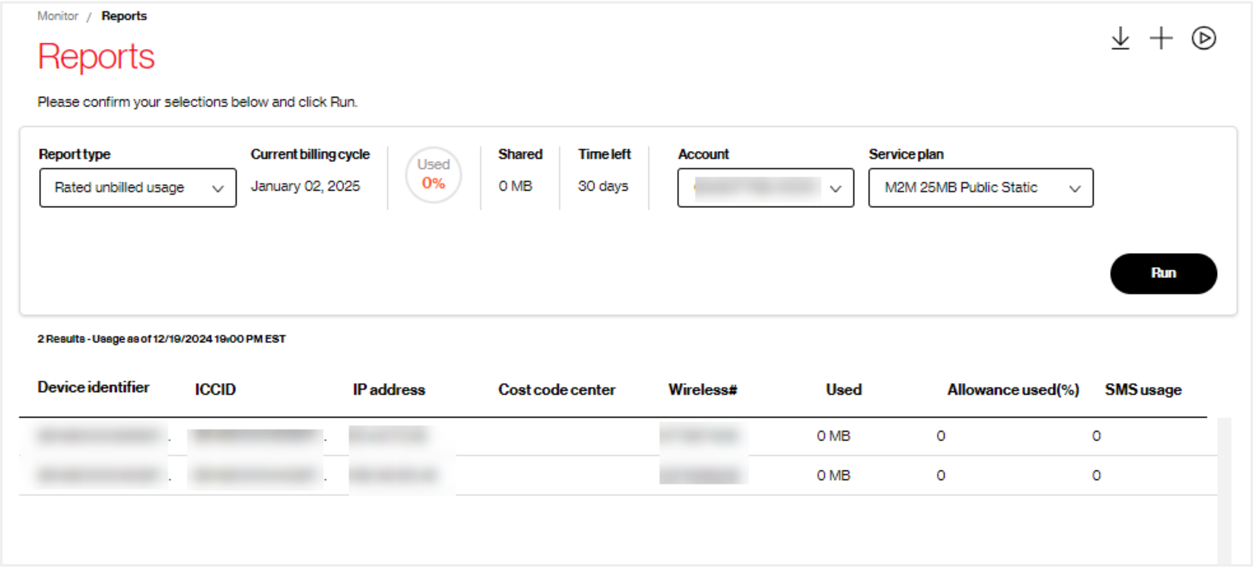
2 Results

Account	Software	From version	To version	Start date	Upgrade time	Status
[redacted]-00002	VerizonSmartCommunities_LCO-277C4N_BG95M...	BG95M6LAR02A04_S	BG95M6LAR02A05_S	10/06/2024	2024-11-01 00:00:14.423 +0000 UTC	UpgradeSuccess
[redacted]-00002	VerizonSmartCommunities_LCO-277C4N_BG95M...	BG95M6LAR02A04_S	BG95M6LAR02A05_S	07/31/2024	2024-08-15 00:00:37.963 +0000 UTC	UpgradePending

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.



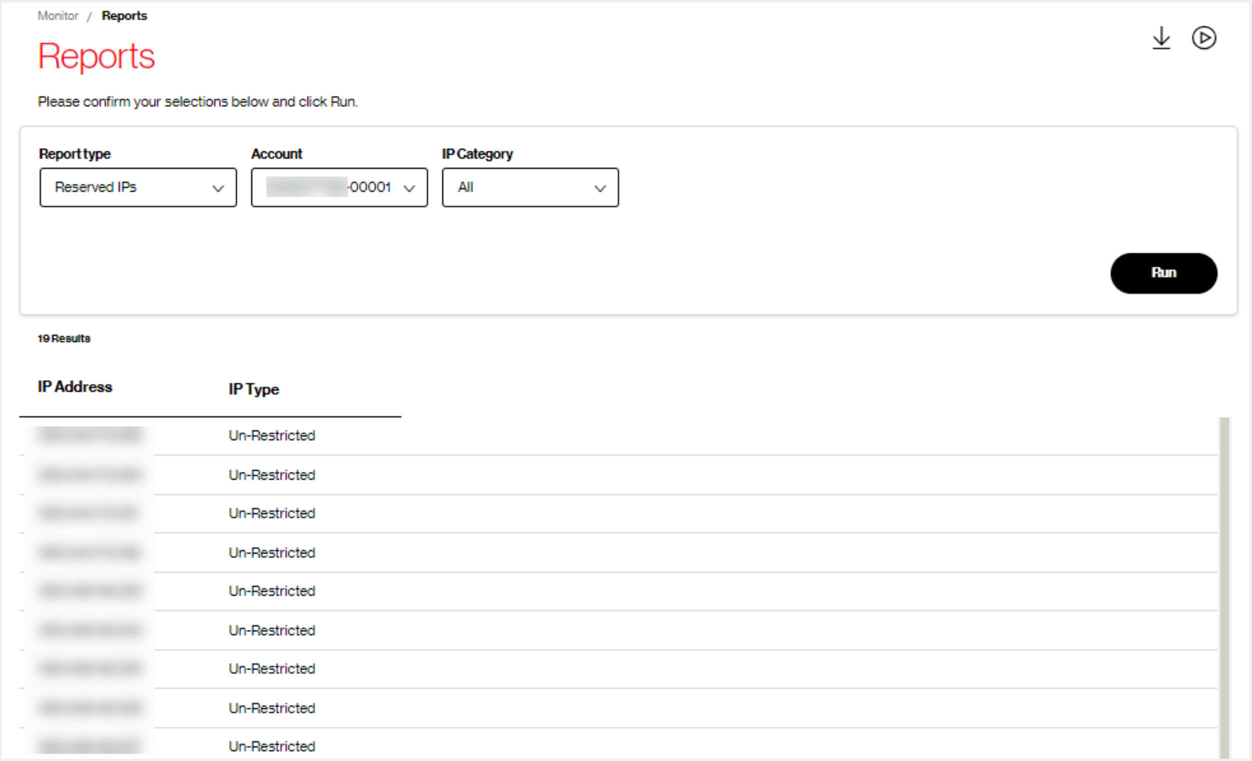
Please confirm your selections below and click Run.

Report type	Current billing cycle	Used	Shared	Time left	Account	Service plan
Rated unbilled usage	January 02, 2025	0%	0 MB	30 days	[redacted]	M2M 25MB Public Static

2 Results - Usage as of 12/19/2024 19:00 PM EST

Device identifier	ICCID	IP address	Cost code center	Wireless#	Used	Allowance used(%)	SMS usage
[redacted]	[redacted]	[redacted]		[redacted]	0 MB	0	0
[redacted]	[redacted]	[redacted]		[redacted]	0 MB	0	0

Reserved IPs



Monitor / **Reports**

Reports

Please confirm your selections below and click Run.

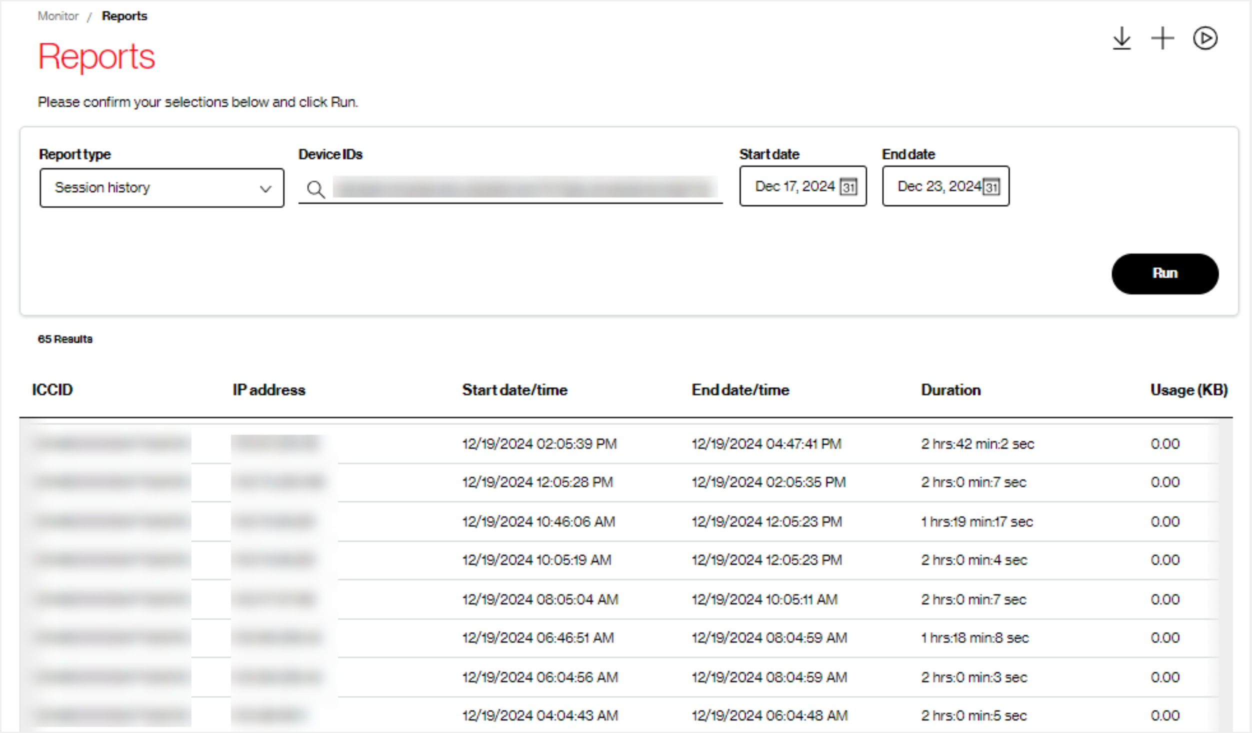
Report type	Account	IP Category
Reserved IPs	[redacted]-00001	All

19 Results

IP Address	IP Type
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted
[redacted]	Un-Restricted

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.



Reports

Please confirm your selections below and click Run.

Report type: Session history

Device IDs: [redacted]

Start date: Dec 17, 2024

End date: Dec 23, 2024

65 Results

ICCID	IP address	Start date/time	End date/time	Duration	Usage (KB)
[redacted]	[redacted]	12/19/2024 02:05:39 PM	12/19/2024 04:47:41 PM	2 hrs:42 min:2 sec	0.00
[redacted]	[redacted]	12/19/2024 12:05:28 PM	12/19/2024 02:05:35 PM	2 hrs:0 min:7 sec	0.00
[redacted]	[redacted]	12/19/2024 10:46:06 AM	12/19/2024 12:05:23 PM	1 hrs:19 min:17 sec	0.00
[redacted]	[redacted]	12/19/2024 10:05:19 AM	12/19/2024 12:05:23 PM	2 hrs:0 min:4 sec	0.00
[redacted]	[redacted]	12/19/2024 08:05:04 AM	12/19/2024 10:05:11 AM	2 hrs:0 min:7 sec	0.00
[redacted]	[redacted]	12/19/2024 06:46:51 AM	12/19/2024 08:04:59 AM	1 hrs:18 min:8 sec	0.00
[redacted]	[redacted]	12/19/2024 06:04:56 AM	12/19/2024 08:04:59 AM	2 hrs:0 min:3 sec	0.00
[redacted]	[redacted]	12/19/2024 04:04:43 AM	12/19/2024 06:04:48 AM	2 hrs:0 min:5 sec	0.00

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

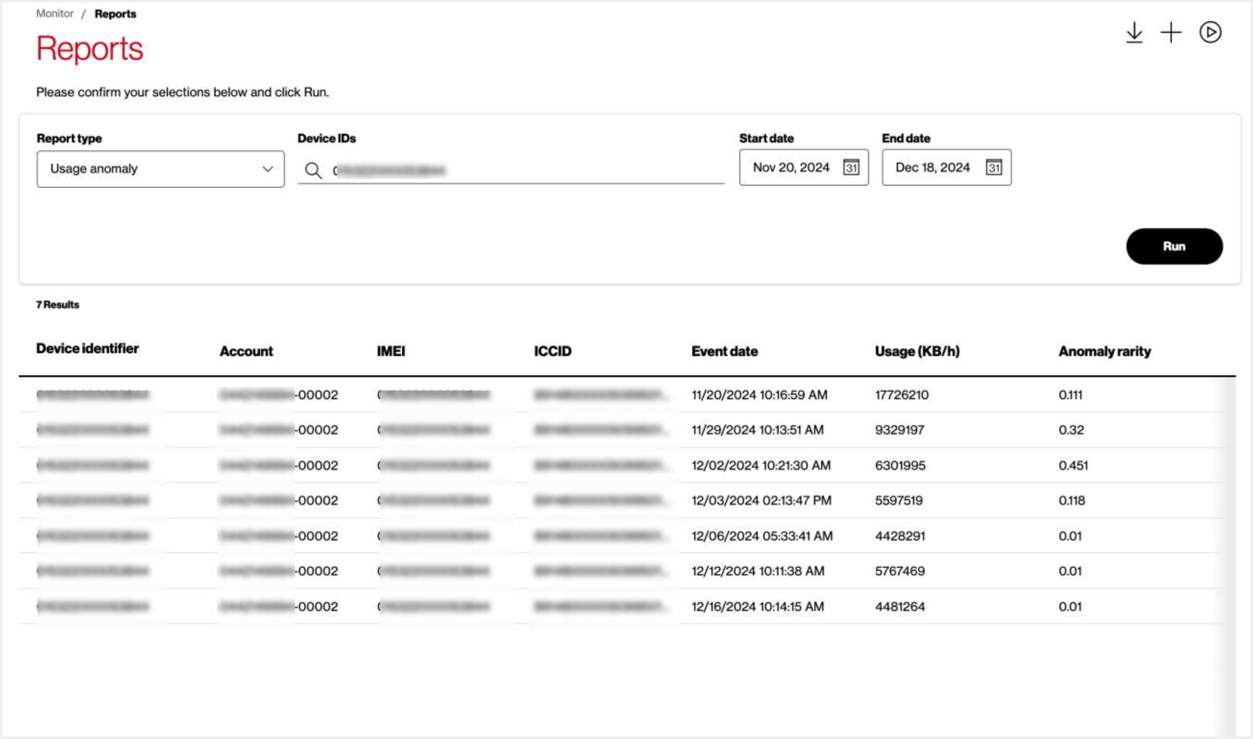
Anomaly rarity: The probability value that represents the rarity of the event

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.

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.



Please confirm your selections below and click Run.

Report type: Usage anomaly

Device IDs: [redacted]

Start date: Nov 20, 2024

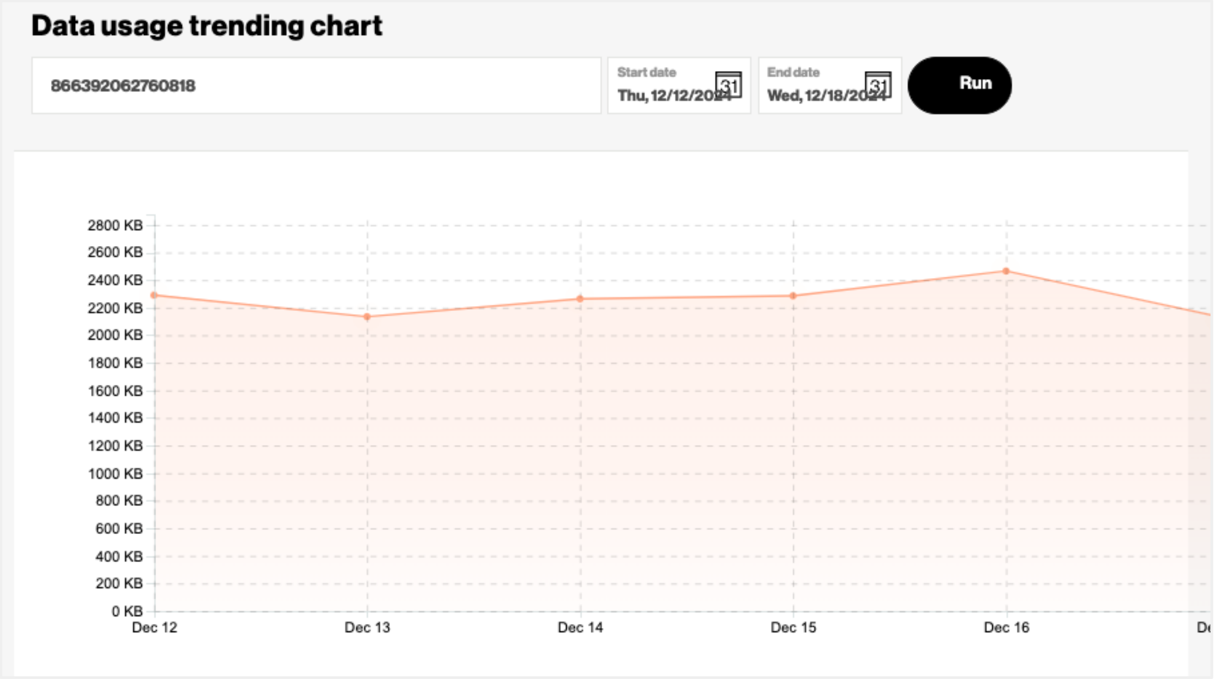
End date: Dec 18, 2024

7 Results

Device identifier	Account	IMEI	ICCID	Event date	Usage (KB/h)	Anomaly rarity
[redacted]	[redacted]-00002	[redacted]	[redacted]	11/20/2024 10:16:59 AM	17726210	0.111
[redacted]	[redacted]-00002	[redacted]	[redacted]	11/29/2024 10:13:51 AM	9329197	0.32
[redacted]	[redacted]-00002	[redacted]	[redacted]	12/02/2024 10:21:30 AM	6301995	0.451
[redacted]	[redacted]-00002	[redacted]	[redacted]	12/03/2024 02:13:47 PM	5597519	0.118
[redacted]	[redacted]-00002	[redacted]	[redacted]	12/06/2024 05:33:41 AM	4428291	0.01
[redacted]	[redacted]-00002	[redacted]	[redacted]	12/12/2024 10:11:38 AM	5767469	0.01
[redacted]	[redacted]-00002	[redacted]	[redacted]	12/16/2024 10:14:15 AM	4481264	0.01

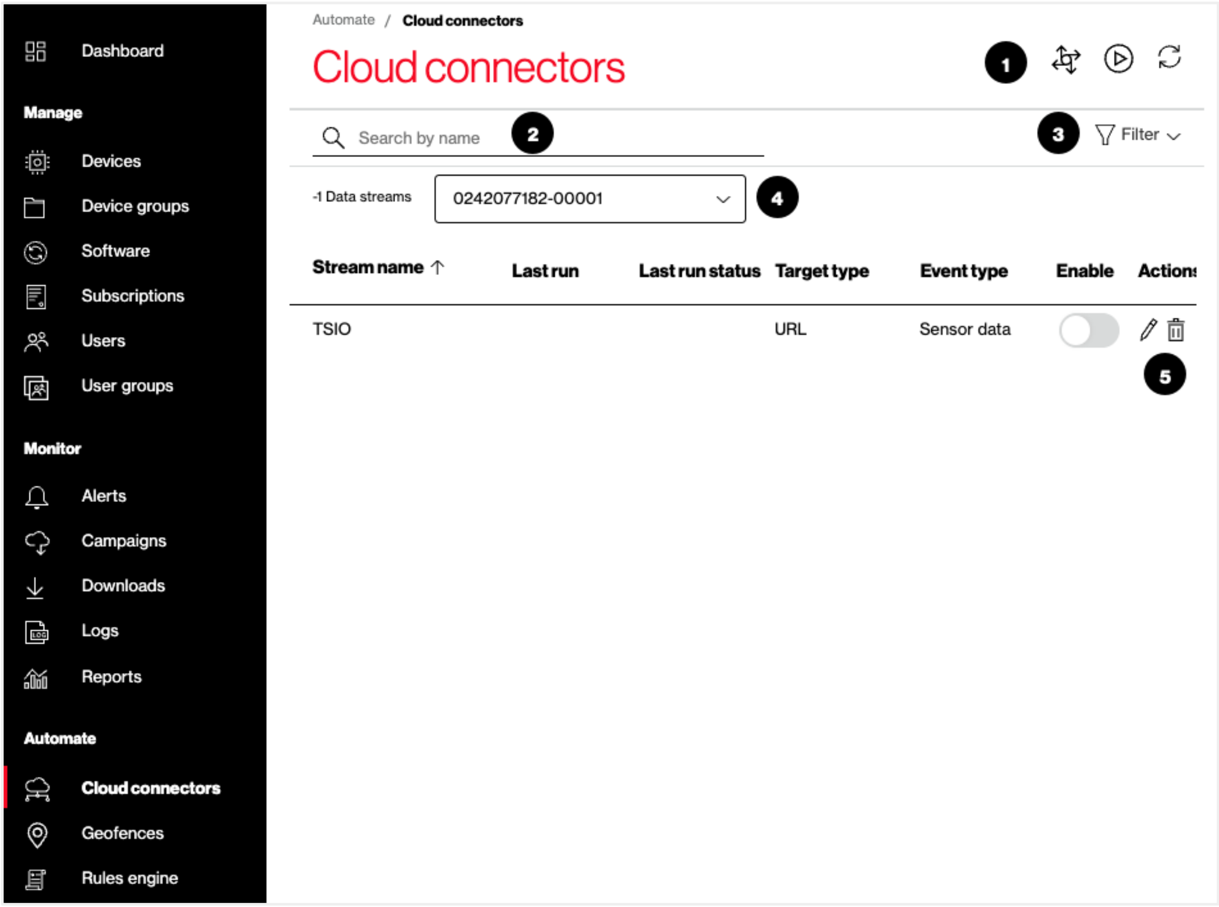
Usage trending chart

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.



1 Data streams: 0242077182-00001

Stream name ↑	Last run	Last run status	Target type	Event type	Enable	Actions
TSIO			URL	Sensor data	○	✎ 🗑

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 cloud 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.

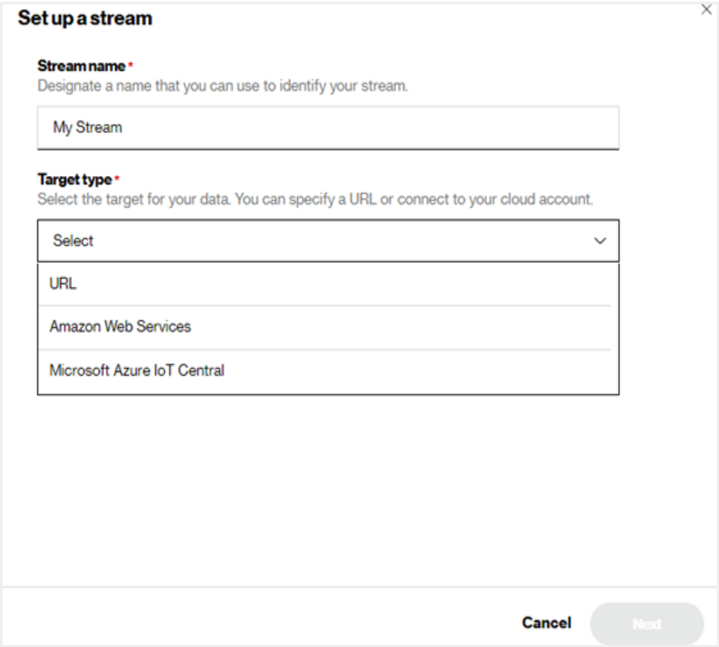
Create a stream

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

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

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



Set up a stream

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

My Stream

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

Select

   a. For **Stream name**, type a descriptive label to easily identify the stream.

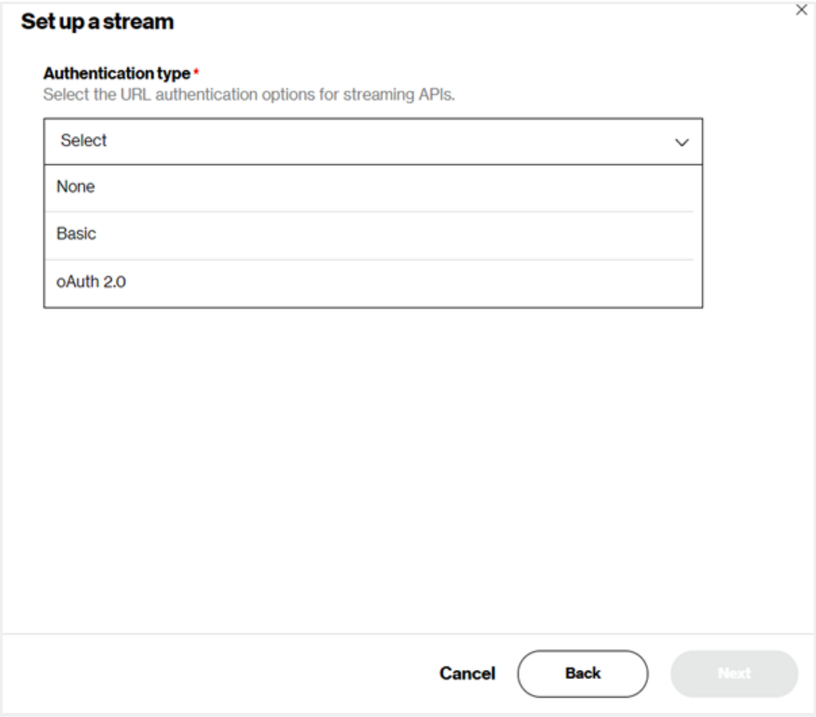
   b. For **Target type**, select the type of streaming you are defining (URL streaming, streaming to Amazon Web Services, or streaming to Microsoft Azure IoT Central.

   c. 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

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



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

b. **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 <<>>" }

c. **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
```

d. Do the following:

   (1) Concatenate the CLIENTID and the CLIENTSECRET, with a colon between them into a continuous string, like this: CLIENTID:CLIENTSECRET.

   (2) Encode the entire string in Base64 format. (To learn more about encoding in Base64 format, visit https://www.base64encode.org/).

(3) Use the Base64 encoded value of CLIENTID:CLIENTSECRET in the API.

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

3. 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.

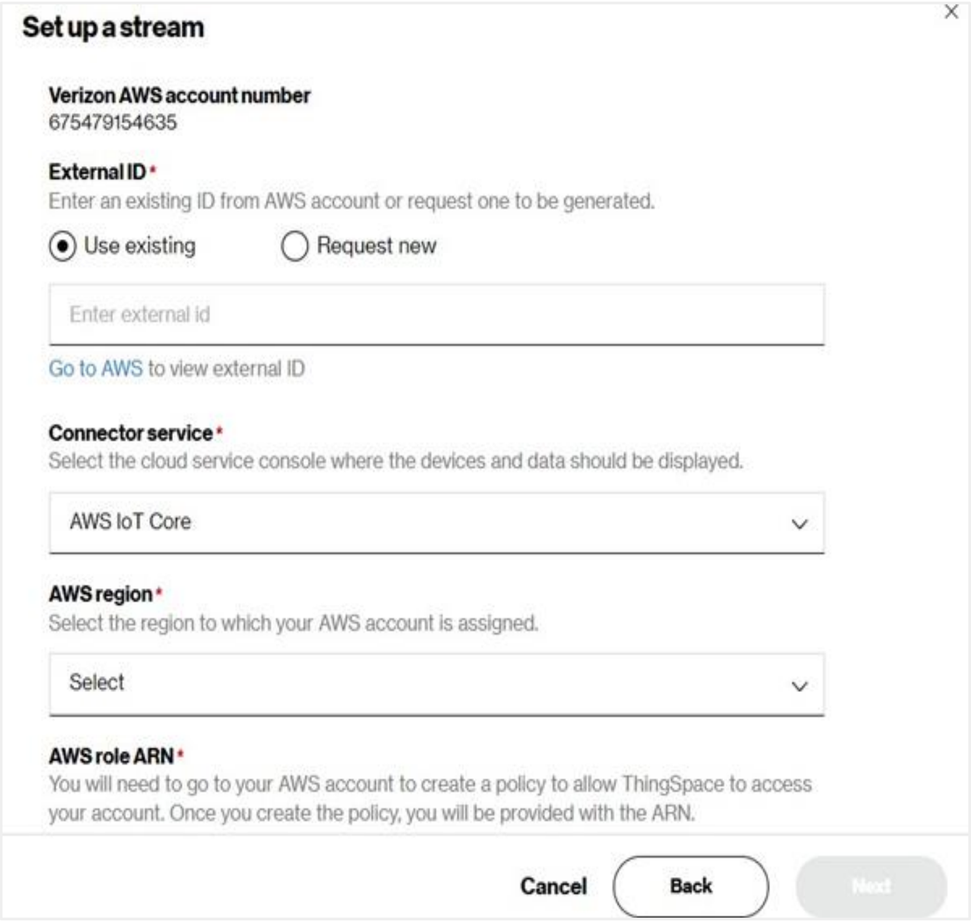
How to configure an AWS account

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:
    a. AWSIotDataAccess
    b. w AWSIoTFullAccess
    c. 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.



Set up a stream

Verizon AWS account number
675479154635

External ID *
Enter an existing ID from AWS account or request one to be generated.

● Use existing ○ Request new

Enter external id

Go to AWS to view external ID

Connector service *
Select the cloud service console where the devices and data should be displayed.

AWS IoT Core

AWS region *
Select the region to which your AWS account is assigned.

Select

AWS role ARN *
You will need to go to your AWS account to create a policy to allow ThingSpace to access your account. Once you create the policy, you will be provided with the ARN.

Using Microsoft Azure

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

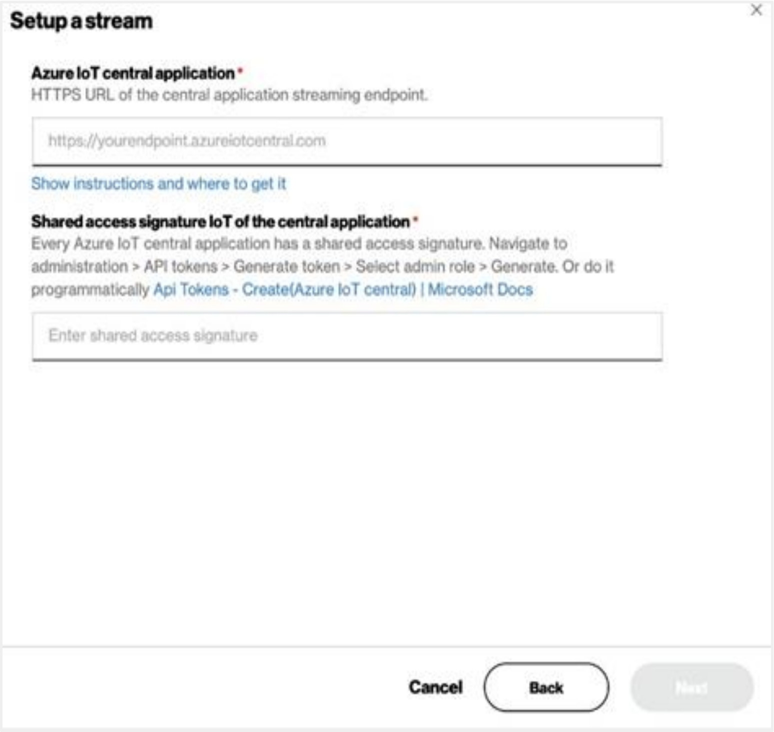
How to configure an Azure connection

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



Setup a stream

Azure IoT central application *

HTTPS URL of the central application streaming endpoint.

https://yourendpoint.azureiotcentral.com

Show instructions and where to get it

Shared access signature IoT of the central application *

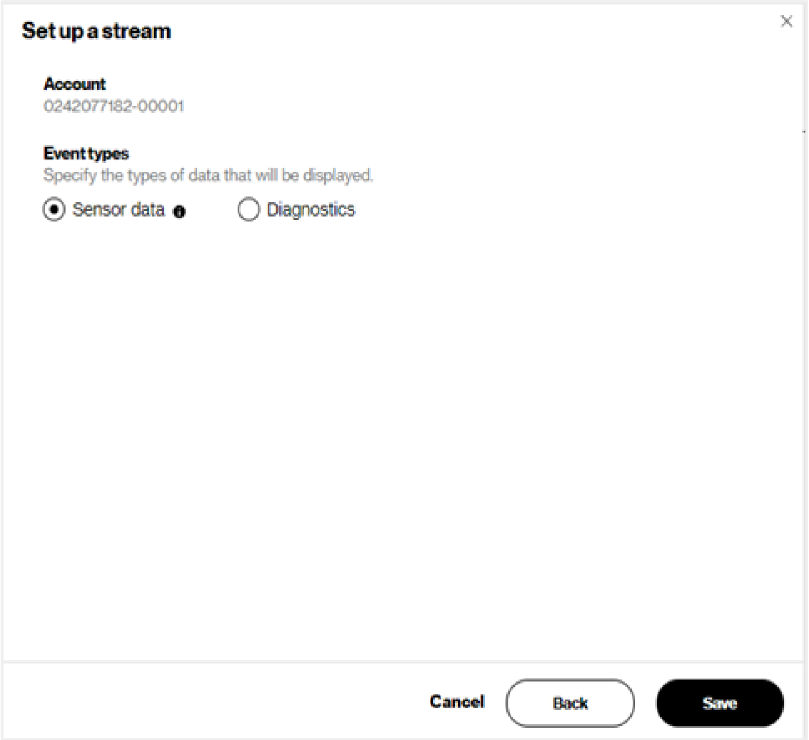
Every Azure IoT central application has a shared access signature. Navigate to administration > API tokens > Generate token > Select admin role > Generate. Or do it programmatically Api Tokens - Create(Azure IoT central) | Microsoft Docs

Enter shared access signature

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.



Set up a stream

Account
0242077182-00001

Event types
Specify the types of data that will be displayed.

● Sensor data ○ Diagnostics

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.

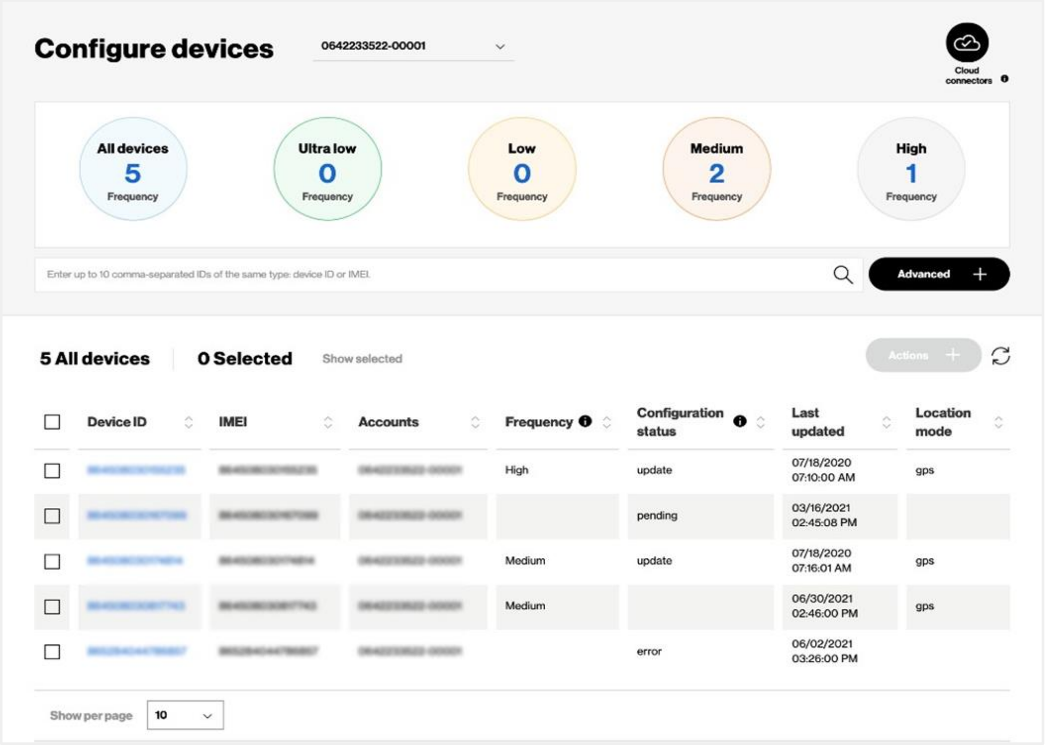
Configure devices

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

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

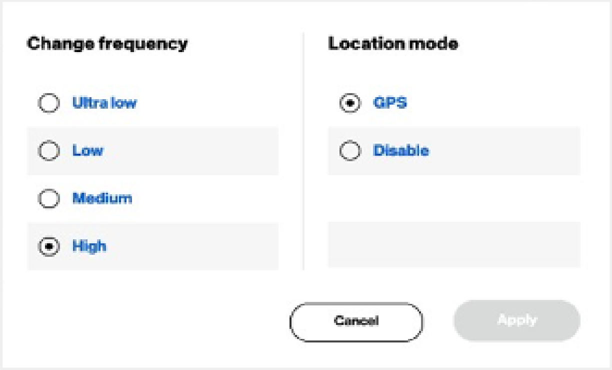
1. One the left navigation, click **Cloud connectors**. The *Cloud connectors* page opens.
2. Click the action icon, and select **Configure devices**. The legacy *Configure devices* page opens.



□	Device ID	IMEI	Accounts	Frequency	Configuration status	Last updated	Location mode
□	[redacted]	[redacted]	[redacted]	High	update	07/18/2020 07:10:00 AM	gps
□	[redacted]	[redacted]	[redacted]		pending	03/16/2021 02:45:08 PM	
□	[redacted]	[redacted]	[redacted]	Medium	update	07/18/2020 07:16:01 AM	gps
□	[redacted]	[redacted]	[redacted]	Medium		06/30/2021 02:46:00 PM	gps
□	[redacted]	[redacted]	[redacted]		error	06/02/2021 03:26:00 PM	

3. 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.]()
4. Select one or more *Device ID* check boxes. *Actions* is enabled.

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



Change frequency

○ Ultra low
○ Low
○ Medium
● High

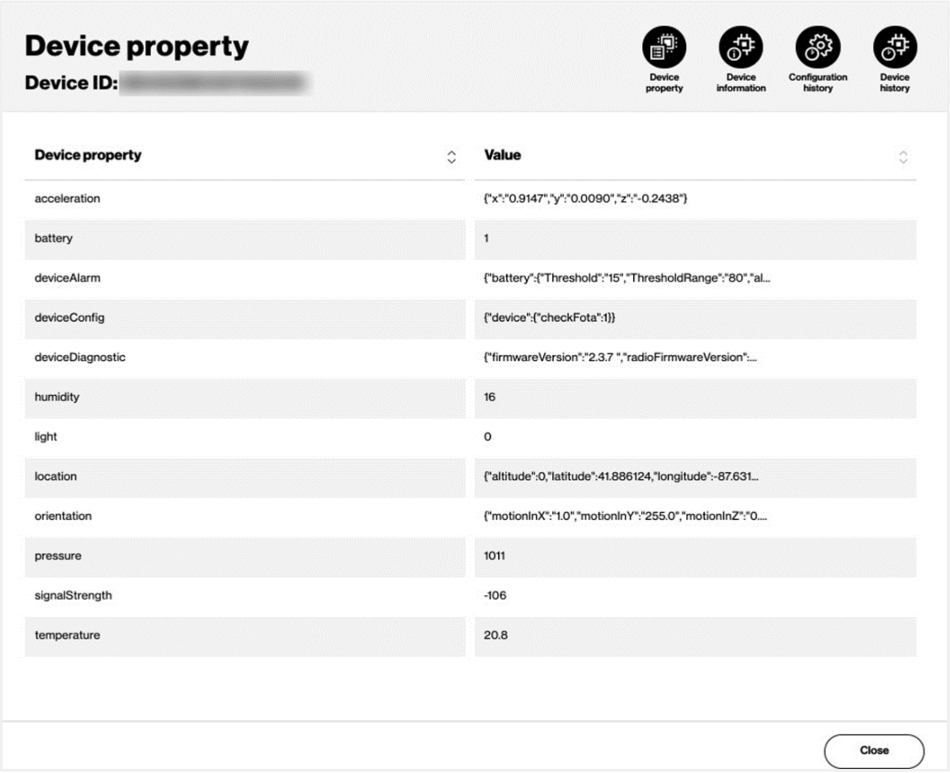
Location mode

● GPS
○ Disable

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

Additional device information

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



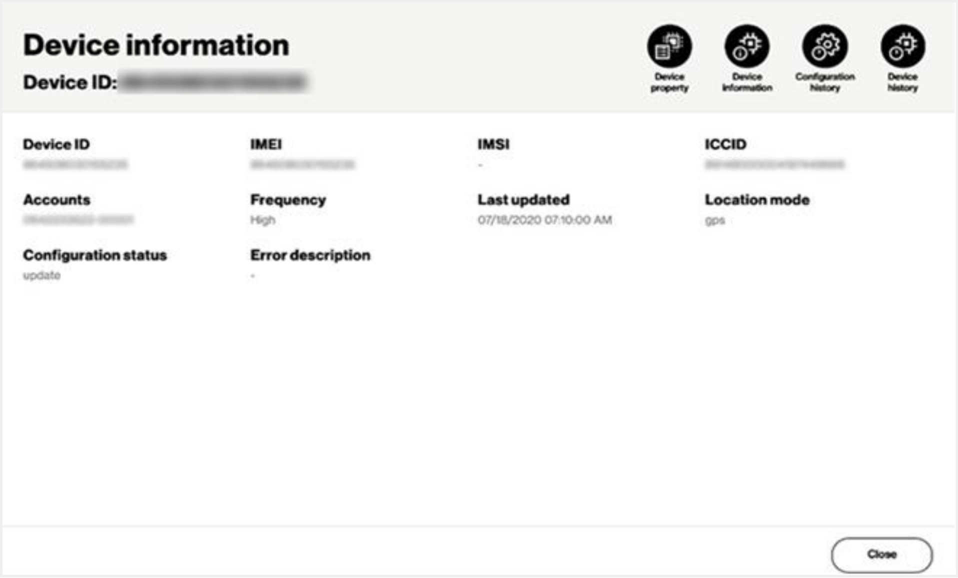
Device property

Device ID: [redacted]

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

Click the icons to open the following dialogs:

Device information



Device information

Device ID: [redacted]

Device ID
[redacted]

IMEI
[redacted]

IMSI
-

ICCID
[redacted]

Accounts
[redacted]

Frequency
High

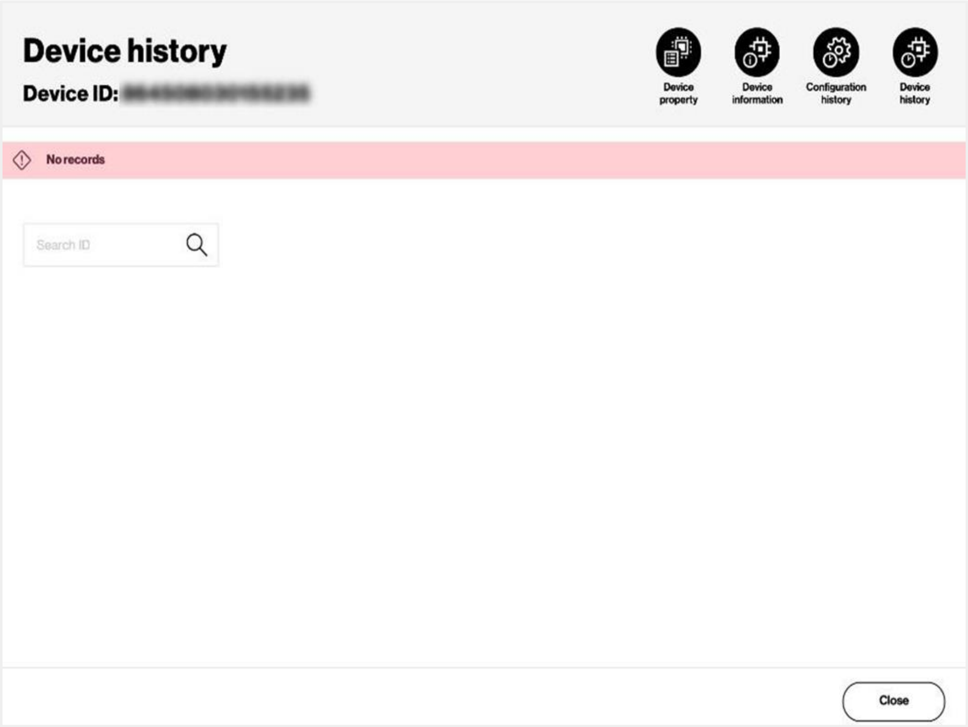
Last updated
07/18/2020 07:10:00 AM

Location mode
gps

Configuration status
update

Error description
-

Device history



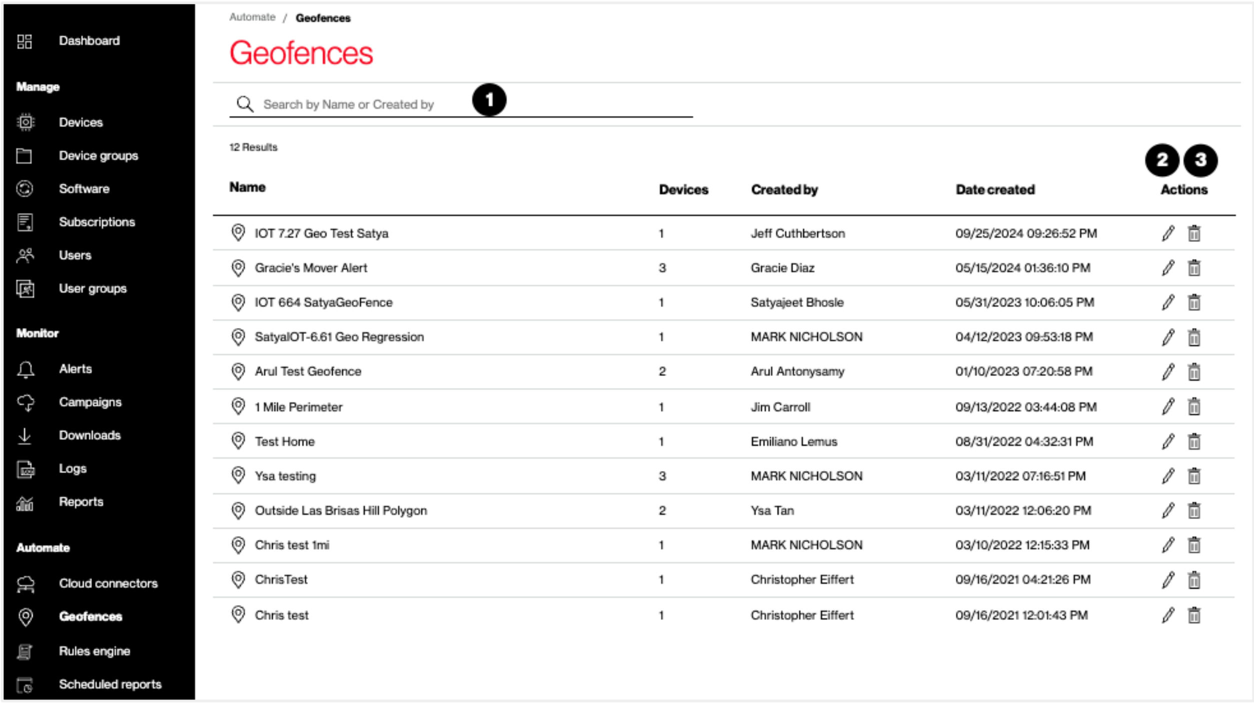
Device history

Device ID: [redacted]

No records

Geofences

On the left navigation, click **Geofences** to open a list of geographical areas.



Geofences

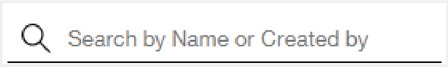
12 Results

Name	Devices	Created by	Date created	Actions
IOT 7.27 Geo Test Satya	1	Jeff Cuthbertson	09/25/2024 09:26:52 PM	✎ 🗑
Gracie's Mover Alert	3	Gracie Diaz	05/15/2024 01:36:10 PM	✎ 🗑
IOT 664 SatyaGeoFence	1	Satyajeet Bhosle	05/31/2023 10:06:05 PM	✎ 🗑
SatyaIOT-6.61 Geo Regression	1	MARK NICHOLSON	04/12/2023 09:53:18 PM	✎ 🗑
Arul Test Geofence	2	Arul Antonysamy	01/10/2023 07:20:58 PM	✎ 🗑
1 Mile Perimeter	1	Jim Carroll	09/13/2022 03:44:08 PM	✎ 🗑
Test Home	1	Emiliano Lemus	08/31/2022 04:32:31 PM	✎ 🗑
Ysa testing	3	MARK NICHOLSON	03/11/2022 07:16:51 PM	✎ 🗑
Outside Las Brisas Hill Polygon	2	Ysa Tan	03/11/2022 12:06:20 PM	✎ 🗑
Chris test 1mi	1	MARK NICHOLSON	03/10/2022 12:15:33 PM	✎ 🗑
ChrisTest	1	Christopher Eiffert	09/16/2021 04:21:26 PM	✎ 🗑
Chris test	1	Christopher Eiffert	09/16/2021 12:01:43 PM	✎ 🗑

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.
3	🗑	Delete – Permanently remove the record from the system. This action cannot be undone.

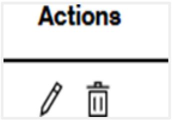
Search for geofences

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



Taking geofence 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.

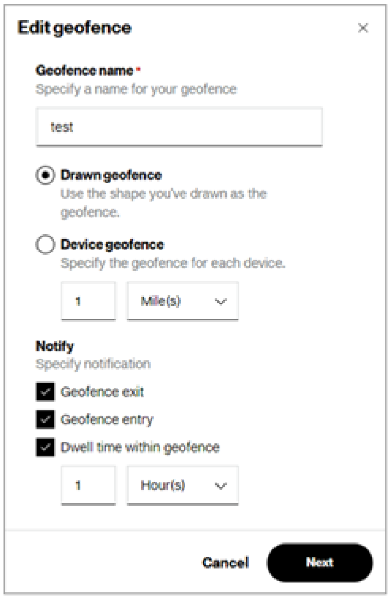


Edit a geofence

How to edit a geofence

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

2. Click the edit icon ✎ . The *Edit geofence* page opens



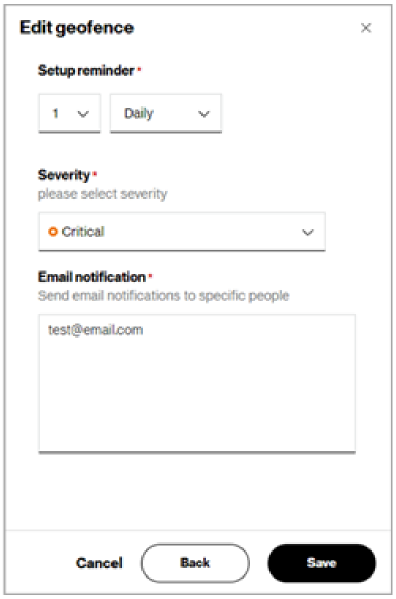
Edit geofence ×

Geofence name *
Specify a name for your geofence
test

● Drawn geofence
Use the shape you've drawn as the geofence.

○ Device geofence
Specify the geofence for each device.
1 Mile(s)

Notify
Specify notification
☑ Geofence exit
☑ Geofence entry
☑ Dwell time within geofence
1 Hour(s)



Edit geofence ×

Setup reminder *
1 Daily

Severity *
please select severity
Critical

Email notification *
Send email notifications to specific people
test@email.com

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

4. For **Notify**:
   a. **Geofence exit** – A notification is sent when the device exits the geofence.
   b. **Geofence entry** – A notification is sent when the device enters the geofence.
   c. **Dwell time within geofence** – A notification is sent when the device stays within the geofence for a set period of time.

5. Click **Next**. A second page of settings opens.

   a. **Setup reminder** – Send a reminder.

   b. **Severity** – Select the severity of this geofence. The severity is included in the notification email.

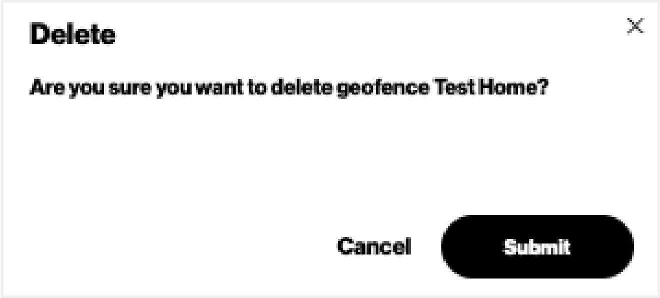
   c. **Email notification** – Enter the email addresses of those that are to receive the notification email.

6. Click **Save** to complete the process.

Deleting a geofence

How to delete a geofence

1. On the left navigation, click **Geofences**. The *Geofences* page opens.
2. Click the delete icon 🗑 of the geofence. A dialog opens to confirm deletion.



Delete

Are you sure you want to delete geofence Test Home?

3. Click **Submit** to complete the delete request.

Rules

Use the *Rules* page to define custom logic and actions based on data received from IoT devices. The rules engine enables automation of tasks, alerts, and data management processes within the platform. It monitors your devices and if specific triggers occur, automatically takes appropriate actions such as suspend devices or change price plans. Rules can apply to devices across their accounts or for individual devices based on certain conditions. 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.

Network activity threshold - This type of threshold is reached when a specific network event occurs such as abnormal disconnects, excessive connections, IMEI changes, and others.

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.

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

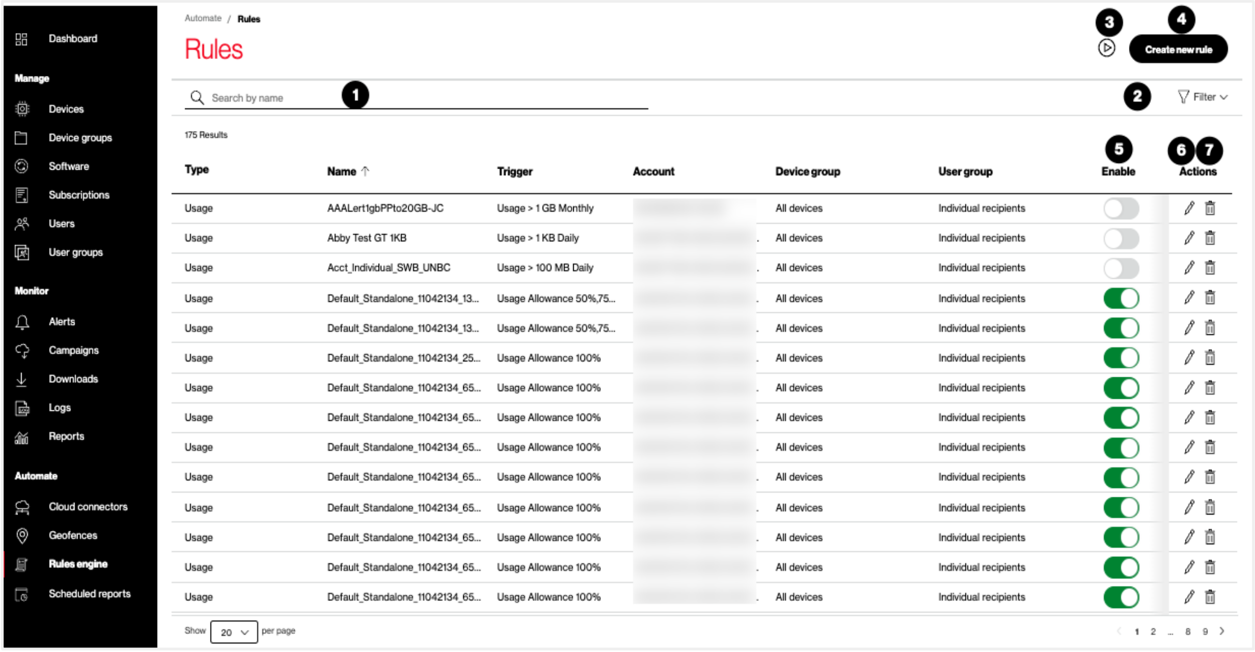
Rules Engine 2.0

ThingSpace has a new Rules Engine 2.0 for Real-Time Reporting (RTR) that, in addition to the basic capabilities stated above, provide additional features such as price plan optimization:

- Leveraging pooling and plan type changes to minimize costs
- End of cycle price plan optimizations
- “On the fly” price plan creation
- Cost/Pricing abstracted from their customers
- Alerts across all accounts
- Auto resume suspended devices at bill cycle start of after a certain number of days

NOTE: In order to use the Rules Engine 2.0 for RTR, your company profile must be enabled for RTR. See your account representative and ask them to enable your organization for the Rules Engine 2.0.

To access the Rules page, click **Rules** on the left navigation to open the page. If you are enabled for the Rules Engine 2.0 you will see **Rules engine** on the left navigation.



Rules

175 Results

Type	Name ↑	Trigger	Account	Device group	User group	Enable	Actions
Usage	AAALert1gbPPto20GB-JC	Usage > 1 GB Monthly	[redacted]	All devices	Individual recipients	○	✎ 🗑
Usage	Abby Test GT 1KB	Usage > 1 KB Daily	[redacted]	All devices	Individual recipients	○	✎ 🗑
Usage	Acct_Individual_SWB_UNBC	Usage > 100 MB Daily	[redacted]	All devices	Individual recipients	○	✎ 🗑
Usage	Default_Standalone_11042134_13...	Usage Allowance 50%,75...	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_13...	Usage Allowance 50%,75...	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_25...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑
Usage	Default_Standalone_11042134_65...	Usage Allowance 100%	[redacted]	All devices	Individual recipients	●	✎ 🗑

Show 20 per page

‹ 1 2 ... 8 9 ›

Elements on the Rules page		
1	🔍	Search – Locate a rule by name.
2	▽	Filter – Reduce the list to rules with specific attributes.
3	▷	Tutorial videos – View available video tutorials.
4		Create new rule – Open the *Create a rule* page to create a new rule.
5	●	Enable – Toggle the option to enable or disable a rule.
6	✎	Edit – Open the *Edit a rule* page to make revisions to a rule.
7	🗑	**Delete** – Permanently remove a rule from the application.

Searching rules

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

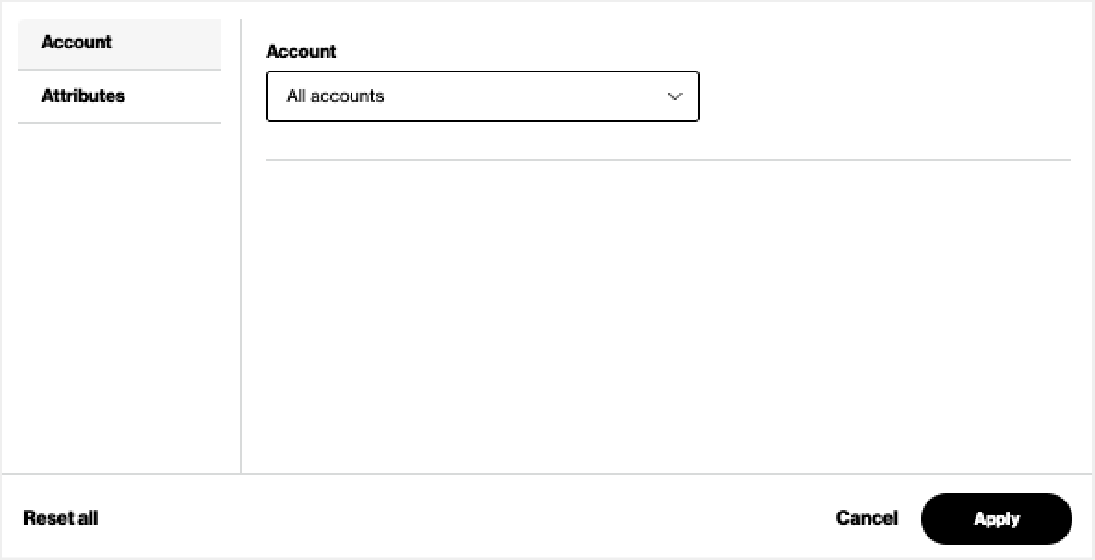
Search by name

NOTE: Searches are not case sensitive.

Applying rule filters

How to apply filters

1. Click ▽ Filter ⌄. The filters page opens.



2. Click each tab or scroll through the list to view all available filters.
3. Select the desired filters.
4. The **Reset all** link resets all filters.
5. Click **Apply**.

Watching tutorial videos

Click on the Tutorial videos icon ▷ and select from any of the available videos on the list.

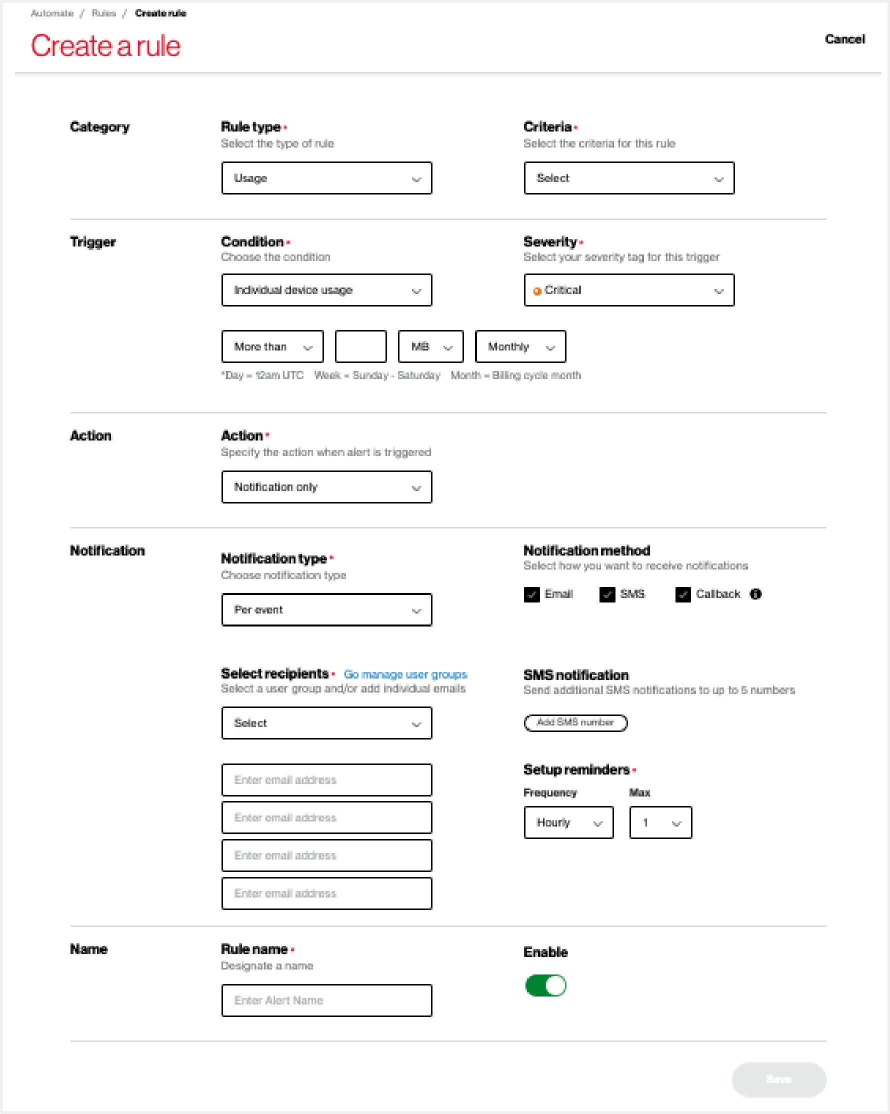
Rules engine quick start guide

The following is a quick guide on how to create a rule and edit a rule. Additional details will follow based on the rule caategory selected.

Create a rule

How to create an alert rule

1. On the left navigation, click **Rules**. The *Rules* page opens.
2. Click **Create new rule**. The *Create a rule* page opens.



Automate / Rules / **Create rule**

Create a rule

Cancel

Category

Rule type *
Select the type of rule
Usage

Criteria *
Select the criteria for this rule
Select

Trigger

Condition *
Choose the condition
Individual device usage

Severity *
Select your severity tag for this trigger
● Critical

More than | | MB | Monthly

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

Action

Action *
Specify the action when alert is triggered
Notification only

Notification

Notification type *
Choose notification type
Per event

Notification method
Select how you want to receive notifications
☑ Email ☑ SMS ☑ Callback ⓘ

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

Enter email address
Enter email address
Enter email address
Enter email address

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

Setup reminders *
Frequency Hourly
Max 1

Name

Rule name *
Designate a name
Enter Alert Name

Enable

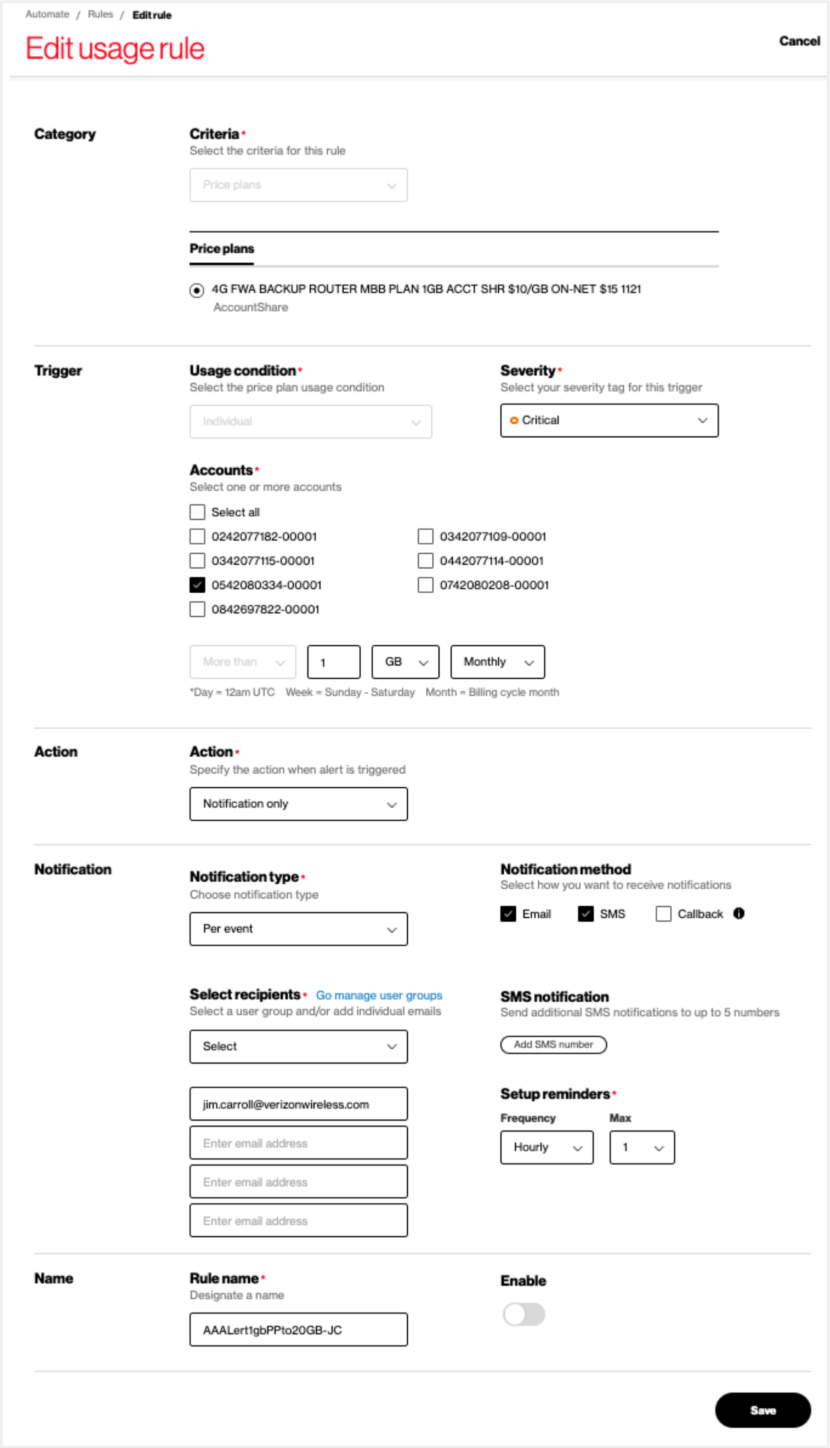
Save

3. Choose a **Category**.
4. Select a **Condition** that **Triggers** an action and designate a **Severity**.
5. Choose the **Action** to take.
6. Select **Notification** options.
7. Give the rule a **Name**.
8. Toggle the **Enable** option to enable the rule. If not enabled, the rule will be created, but will not run.
9. Click **Save**.

Edit a rule

How to edit a rule

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



Edit usage rule

Category

Criteria* Select the criteria for this rule

Price plans

Price plans

● 4G FWA BACKUP ROUTER MBB PLAN 1GB ACCT SHR $10/GB ON-NET $15 1121
AccountShare

Trigger

Usage condition* Select the price plan usage condition

Individual

Severity* Select your severity tag for this trigger

Critical

Accounts* Select one or more accounts

☐ Select all
☐ 0242077182-00001
☐ 0342077115-00001
☑ 0542080334-00001
☐ 0842697822-00001
☐ 0342077109-00001
☐ 0442077114-00001
☐ 0742080208-00001

More than | 1 | GB | Monthly

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

Action

Action* Specify the action when alert is triggered

Notification only

Notification

Notification type* Choose notification type

Per event

Notification method Select how you want to receive notifications

☑ Email ☑ SMS ☐ Callback

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

Select

jim.carroll@verizonwireless.com
Enter email address
Enter email address
Enter email address

SMS notification Send additional SMS notifications to up to 5 numbers

Setup reminders*

Frequency: Hourly
Max: 1

Name

Rule name* Designate a name

AAALert1gbPPto20GB-JC

Enable

2. Update the **Category**.

3. Update the **Condition,** and **Trigger** and **Severity**.
4. Update the **Action**.
5. Update **Notification** options.
6. Update the **Name**.
7. Choose to enable or disable the rule
8. Click **Save**.

Rule categories

The Rules Engine has four rule categories or types to set alerts on. Users can build multiple rules in the same category but each rule can only perform one action.

- Network - How the device connects and is identified
- Transactions - How the device is set up or updated
- Usage - How the device is consuming data
- Usage Anomaly - How the device is consuming data that is not normal

Network rules

1. Select whether the rule will apply to the entire account, all devices or a specific device group
2. Choose the **condition** that will the **trigger** the alert
   a. Base station ID change
   b. Abnormal disconnect
   c. Excessive connections (select the threshold for the total excessive connections in a day)
   d. SMS count (choose the threshold values, unit of measure, and measured period)
   e. Session duration (select the threshold in seconds for the duration period)
   f. IMEI change detection
3. Assign a **severity** (Critical, Major, Minor, Notice)
4. Sect the **recipients** who will receive the alert notification (user group or individuals)
5. Select the **notification method** (Email, SMS (text message), Callback)
6. Give the rule a **name**
7. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

Transaction rules

1. Select whether the rule will apply to all accounts, one or more specific accounts or a device group.
2. Choose the **condition** that will the **trigger** the alert

  a. Provisioning types (Failures, Successes, On request, On a number of requests) and Transaction types (Activate, Deactivate, Suspend, Resume, Change service plan)
  b. Auto resume (the alert will be sent 7 days before the device is scheduled to auto-resume)

3. Assign a **severity** (Critical, Major, Minor, Notice)
4. Sect the **notificaton type** (Per event, Daily summary, Weekly summary)
5. Select the **notification method** (Email, SMS text message, Callback)
6. Sect the **recipients** who will receive the alert notification (user group or individuals)
7. Give the rule a **name**
8. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

Usage rules

Select whether the rule will apply to the one or more accounts, device groups, or price plans

Account usage

8. Select all **accounts** or individual accounts
9. Choose the **condition** that will the **trigger** the alert
   - Individual device usage
   - Combined device usage (Account level) – Choose combined or Separate accounts
   a. Select the threshold values, unit of measure, and measurement period
10. Assign a **severity** (Critical, Major, Minor, Notice)
11. Choose the **action** to perform when the condition is triggered
    a. Notify only
    b. Suspend device(s) with or without billing (provide the suspend threshold, suspend duration, and the accounts to suspended devices from)
12. Select the **notification type** (Per event)
13. Select the **notificaton method** (Email, SMS, Callback)
14. Sect the **recipients** who will receive the alert notification (user group or individuals)
15. Optionally send an additional **SMS notification** to up to 5 people
16. Give the rule a **name**
17. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

Device groups usage

1. Select an existing **device group** or create a new one
2. Choose the **condition** that will the **trigger** the alert
   a. Individual device usage
   b. Combined device usage

   c. Select the threshold values, unit of measure, and measurement period

3. Assign a **severity** (Critical, Major, Minor, Notice)
4. Choose the **action** to perform when the condition is triggered
   a. Notify only
   b. Suspend device(s) with or without billing (provide the suspend threshold and suspend duration)
5. Select the **notification type** (Per event)
6. Select the **notificaton method** (Email, SMS, Callback)
7. Select the **recipients** who will receive the alert notification (user group or individuals)
8. Optionally send an additional **SMS notification** to up to 5 people
9. Give the rule a **name**
10. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

Price Plan Usage

1. Select a **price plan** or a price **plan group** - select standalone price plans or account plan groups (group share) from the list
2. Choose the **conditions** that will the **trigger** the alert
   a. Account level
   b. Aging (price plan changes to lines which were active on a selected price plan for a number of bill cycles)
   c. Individual lines
   d. Share pool usage (100%, 90%, 75%, 50%)
   e. Usage allowance (100%, 90%, 75%, 50%)
3. Choose the **action** to perform when the conditions are triggered
   a. Notify only
   b. Suspend device(s) with or without billing
      i. Provide the suspend usage threshold, suspend duration, and/or the accounts to suspended devices from
   c. Change price plans (current date or backdated)
      i. Select the price plan to change from and the price plan to change to
      ii. Agree to the terms and conditions

For Aging triggers, select an **aging value** (bill cycles)

For Individual device triggers you can assign usage percentages to individual price plans or apply the same usage percentages to all plans.

i. Select the **usage percentage** (100%, 90%, 75%, and 50%)
ii. Select the **alert type** (All, Individual price plans).

2. Select the **notification type** (Per event, Daily Summary)
3. Select the **notificaton method** (Email, SMS, Callback)
4. Select the **recipients** who will receive the alert notification (user group or individuals)
5. Optionally send an additional **SMS notification** to up to 5 people
6. Give the rule a **name**
7. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

NOTE: An 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.

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.

NOTE: Suspend is not supported for share pool usage

NOTE: The share pool usage rule will be in effect on the last day of the billing cycle. Share pool usage will allow the setup of price plan changes. Share pool usage will allow VZW Automation or a 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.

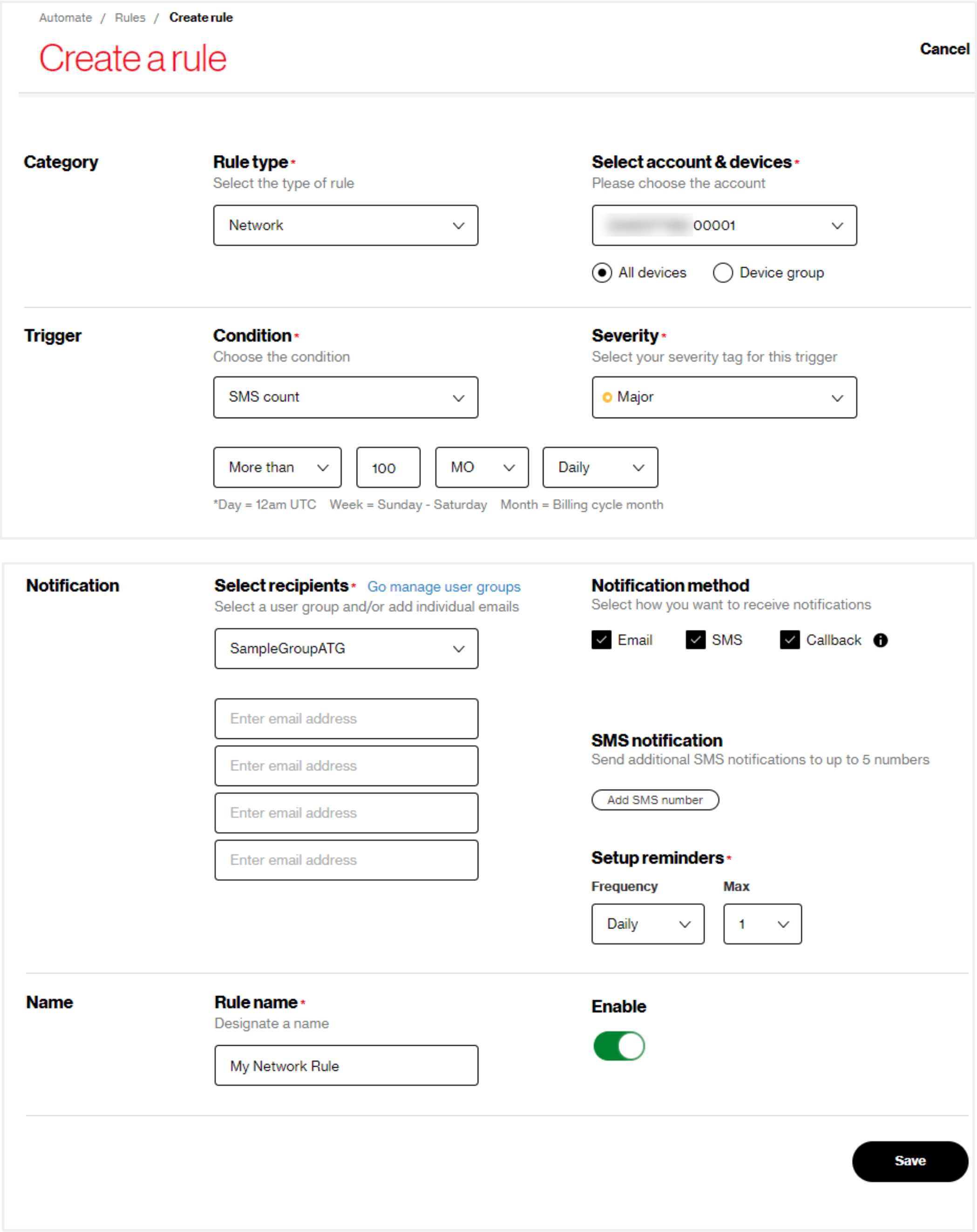
Usage Anomaly rules

1. Choose the **condition** that will the **trigger** the alert
   a. Choose the anomaly flag(s) (Abnormal, Very Abnormal)
   b. Choose the anomaly reason (Over expected usage, Under expected usage)
2. Assign a **severity** (Critical, Major, Minor, Notice)
3. Select the **notification type** (Daily Summary, Weekly Summary)
4. Sect the **recipients** who will receive the alert notification (user group or individuals) and the **notification method** (Email, SMS (text message), Callback)
5. Optionally send an additional **SMS notification** to up to 5 people
6. Give the rule a **name**
7. Click the **Enable** button to enable the rule. If not enabled, the rule will be created, but will not run

Example rules

Network – SMS count exceeded

This network rule monitors the IoT devices on one account triggers a Major alert and notifies a group of individuals via Email, SMS, and via Callback when the SMS count on the account exceeds more than 100 mobile originated (MO) in a day.



Automate / Rules / **Create rule**

Create a rule

Cancel

Category

Rule type *
Select the type of rule
Network

Select account & devices *
Please choose the account
[redacted]00001
● All devices ○ Device group

Trigger

Condition *
Choose the condition
SMS count

Severity *
Select your severity tag for this trigger
Major

More than | 100 | MO | Daily

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

Notification

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

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

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

Setup reminders *
Frequency: Daily
Max: 1

Name

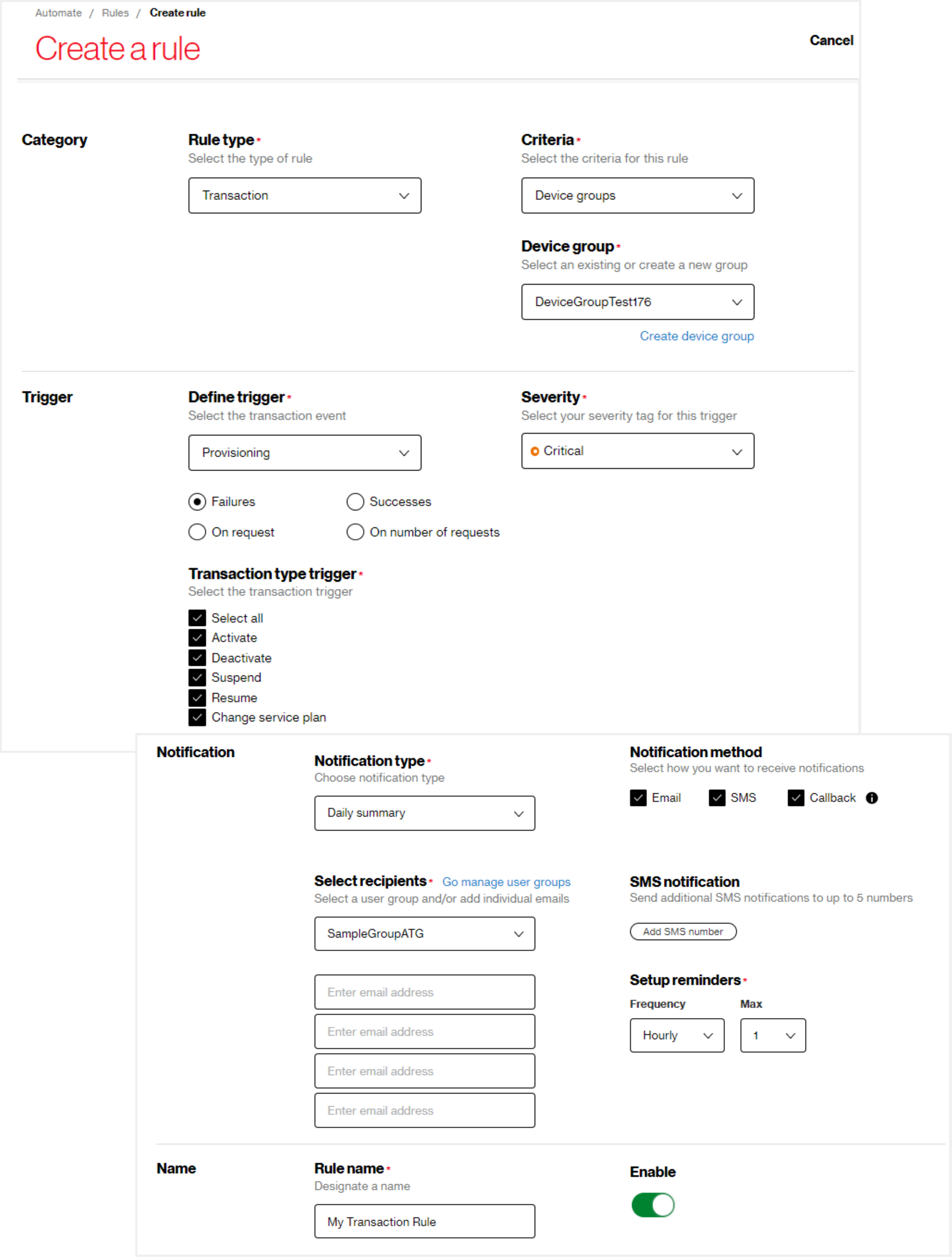
Rule name *
Designate a name
My Network Rule

Enable

Save

Transaction rule – provisioning failures

This transaction rule monitors the IoT devices of a specific device group triggers a Critical alert and notifies a group of individuals with a Daily summary via Email, SMS, and via Callback when any of the selected provisioning transactions (Activate, Deactivate, Suspend, Resume, Change service plan) fail.



Automate / Rules / Create rule

Create a rule

Cancel

Category

Rule type *
Select the type of rule
Transaction

Criteria *
Select the criteria for this rule
Device groups

Device group *
Select an existing or create a new group
DeviceGroupTest176
Create device group

Trigger

Define trigger *
Select the transaction event
Provisioning

● Failures ○ Successes
○ On request ○ On number of requests

Severity *
Select your severity tag for this trigger
Critical

Transaction type trigger *
Select the transaction trigger
☑ Select all
☑ Activate
☑ Deactivate
☑ Suspend
☑ Resume
☑ Change service plan

Notification

Notification type *
Choose notification type
Daily summary

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

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

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

Setup reminders *
Frequency: Hourly
Max: 1

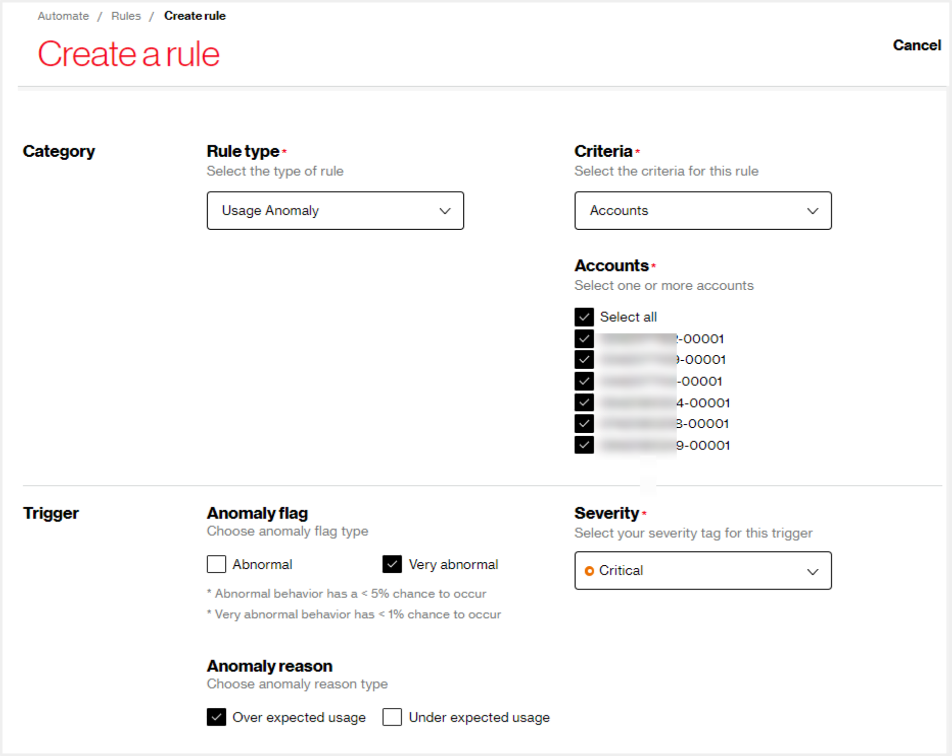
Name

Rule name *
Designate a name
My Transaction Rule

Enable

Usage anomaly – very abnormal usage

This usage anomaly rule monitors the IoT devices on multiple accounts triggers a Critical alert and and notifies a group of individuals via Email, SMS, and via Callback when there has been a very abnormal data usage over what was expected.



Automate / Rules / Create rule

Create a rule

Cancel

Category

Rule type*
Select the type of rule
Usage Anomaly

Criteria*
Select the criteria for this rule
Accounts

Accounts*
Select one or more accounts

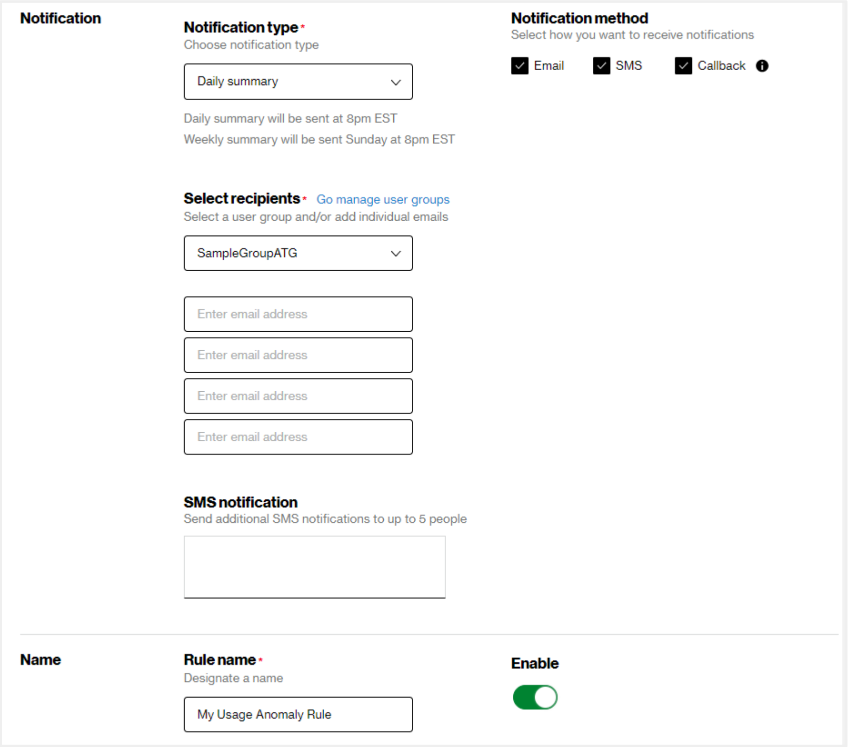
☑ Select all
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]4-00001
☑ [redacted]3-00001
☑ [redacted]9-00001

Trigger

Anomaly flag
Choose anomaly flag type
□ Abnormal ☑ Very abnormal
* Abnormal behavior has a < 5% chance to occur
* Very abnormal behavior has < 1% chance to occur

Severity*
Select your severity tag for this trigger
Critical

Anomaly reason
Choose anomaly reason type
☑ Over expected usage □ Under expected usage



Notification

Notification type*
Choose notification type
Daily summary
Daily summary will be sent at 8pm EST
Weekly summary will be sent Sunday at 8pm EST

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

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

SMS notification
Send additional SMS notifications to up to 5 people

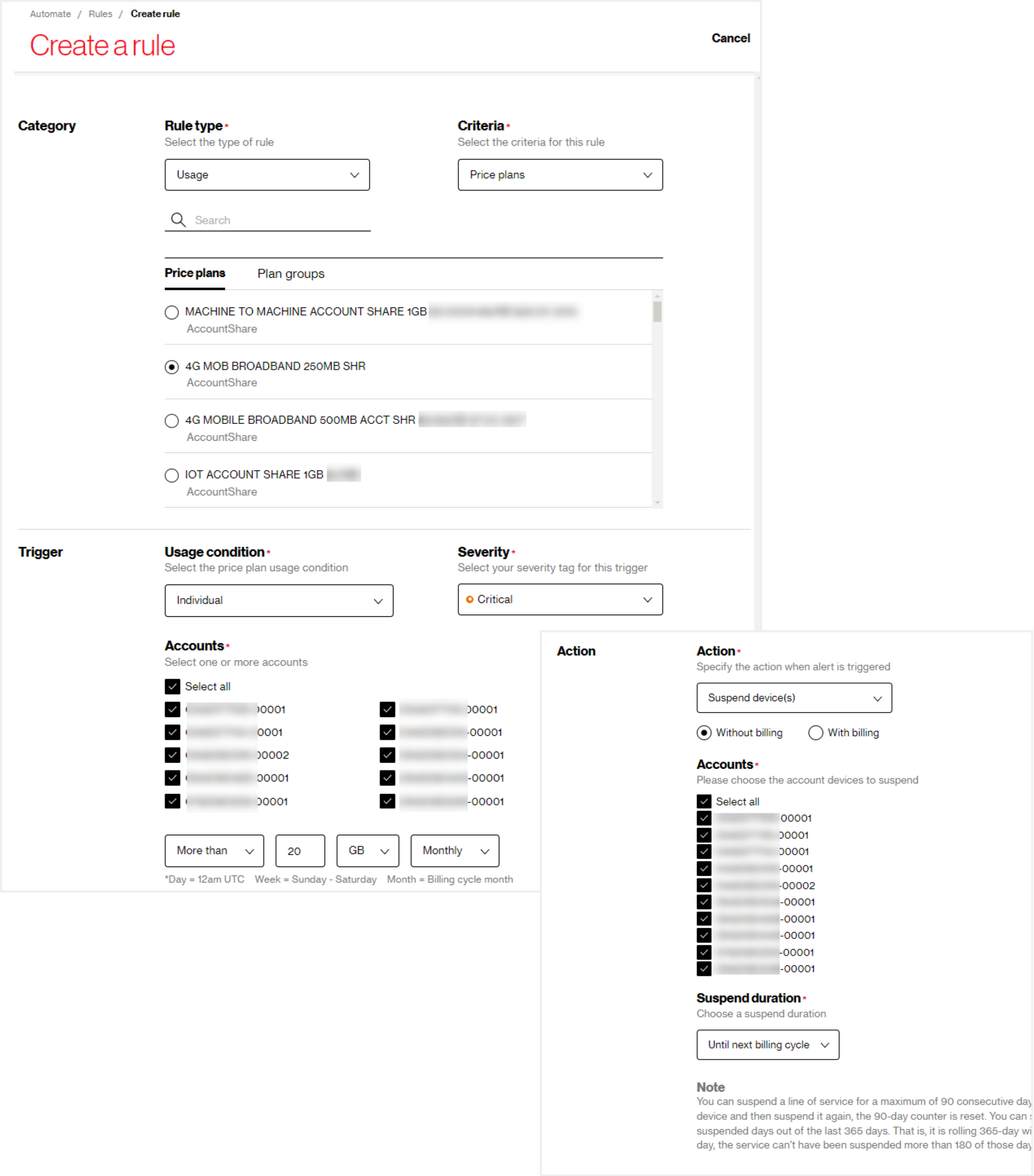
Name

Rule name*
Designate a name
My Usage Anomaly Rule

Enable

Usage rule – suspend when device usage exceeded

This usage rule monitors the IoT devices on multiple accounts with a particular price plan and suspends devices without billing when individual device usage exceed 20 GB in a month until the next billing cycle.



Create a rule

Category

Rule type *
Select the type of rule
Usage

Criteria *
Select the criteria for this rule
Price plans

○ MACHINE TO MACHINE ACCOUNT SHARE 1GB [redacted]
AccountShare

● 4G MOB BROADBAND 250MB SHR
AccountShare

○ 4G MOBILE BROADBAND 500MB ACCT SHR [redacted]
AccountShare

○ IOT ACCOUNT SHARE 1GB [redacted]
AccountShare

Trigger

Usage condition *
Select the price plan usage condition
Individual

Severity *
Select your severity tag for this trigger
Critical

Accounts *
Select one or more accounts

☑ Select all

☑ [redacted]00001
☑ [redacted]0001
☑ [redacted]00002
☑ [redacted]00001
☑ [redacted]00001

☑ [redacted]00001
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001

More than | 20 | GB | Monthly

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

Action

Action *
Specify the action when alert is triggered
Suspend device(s)

● Without billing ○ With billing

Accounts *
Please choose the account devices to suspend

☑ Select all
☑ [redacted]00001
☑ [redacted]00001
☑ [redacted]00001
☑ [redacted]-00001
☑ [redacted]-00002
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001
☑ [redacted]-00001

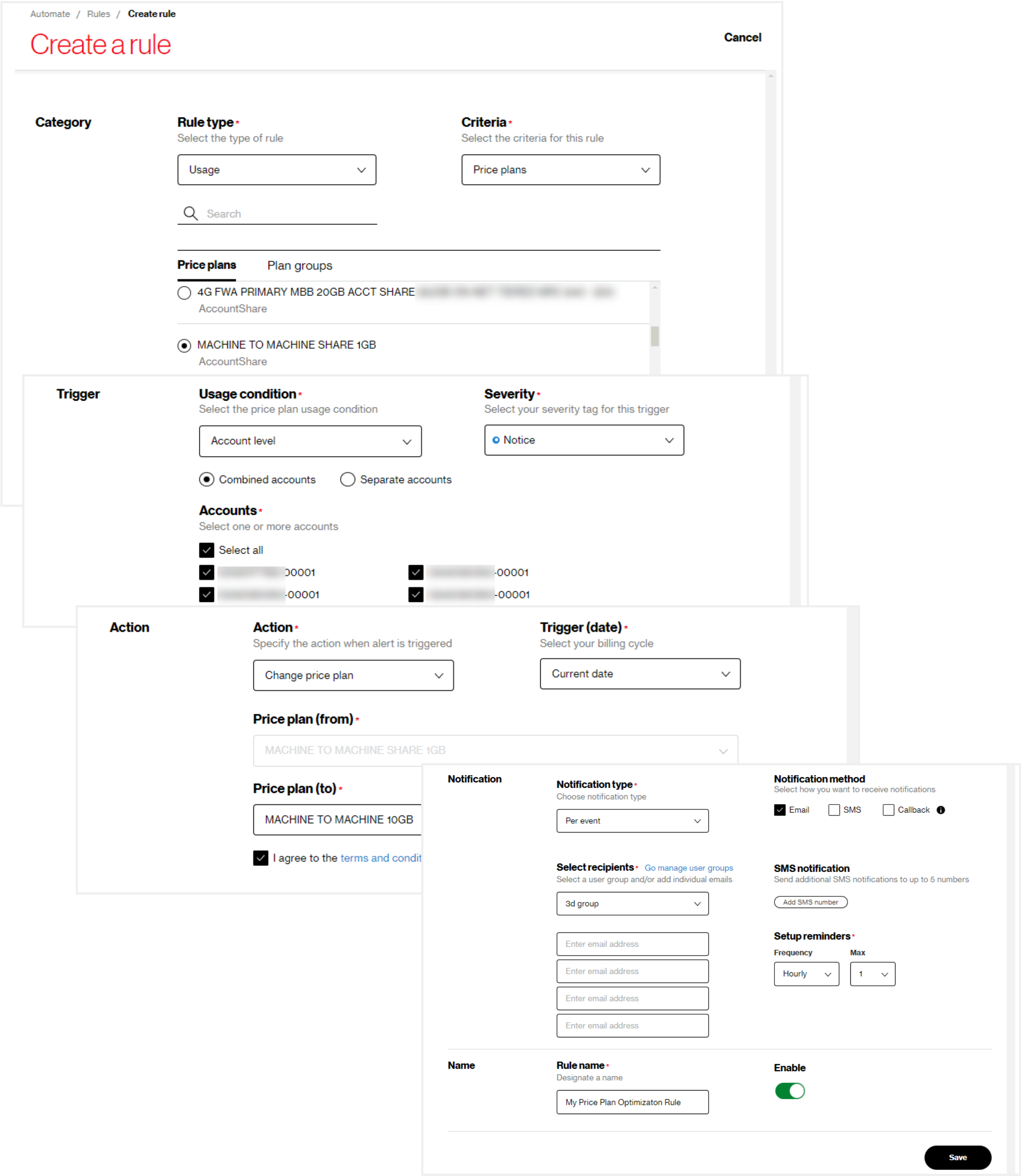
Suspend duration *
Choose a suspend duration
Until next billing cycle

Note
You can suspend a line of service for a maximum of 90 consecutive day device and then suspend it again, the 90-day counter is reset. You can suspended days out of the last 365 days. That is, it is rolling 365-day wi day, the service can't have been suspended more than 180 of those day

Usage rule – price plan optimization

This usage rule monitors the IoT devices on multiple accounts with and triggers a Notice alert

suspends devices without billing when individual device usage exceed 20 GB in a month until the next billing cycle.



Automate / Rules / Create rule

Create a rule

Cancel

Category

Rule type *
Select the type of rule
Usage

Criteria *
Select the criteria for this rule
Price plans

Search

Price plans | Plan groups

○ 4G FWA PRIMARY MBB 20GB ACCT SHARE [redacted]
AccountShare

● MACHINE TO MACHINE SHARE 1GB
AccountShare

Trigger

Usage condition *
Select the price plan usage condition
Account level

● Combined accounts ○ Separate accounts

Severity *
Select your severity tag for this trigger
Notice

Accounts *
Select one or more accounts

☑ Select all
☑ [redacted]00001 ☑ [redacted]-00001
☑ [redacted]-00001 ☑ [redacted]-00001

Action

Action *
Specify the action when alert is triggered
Change price plan

Trigger (date) *
Select your billing cycle
Current date

Price plan (from) *
MACHINE TO MACHINE SHARE 1GB

Price plan (to) *
MACHINE TO MACHINE 10GB

☑ I agree to the terms and condit

Notification

Notification type *
Choose notification type
Per event

Notification method
Select how you want to receive notifications
☑ Email ☐ SMS ☐ Callback

Select recipients * Go manage user groups
Select a user group and/or add individual emails
3d group
Enter email address
Enter email address
Enter email address
Enter email address

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

Setup reminders *
Frequency: Hourly
Max: 1

Name

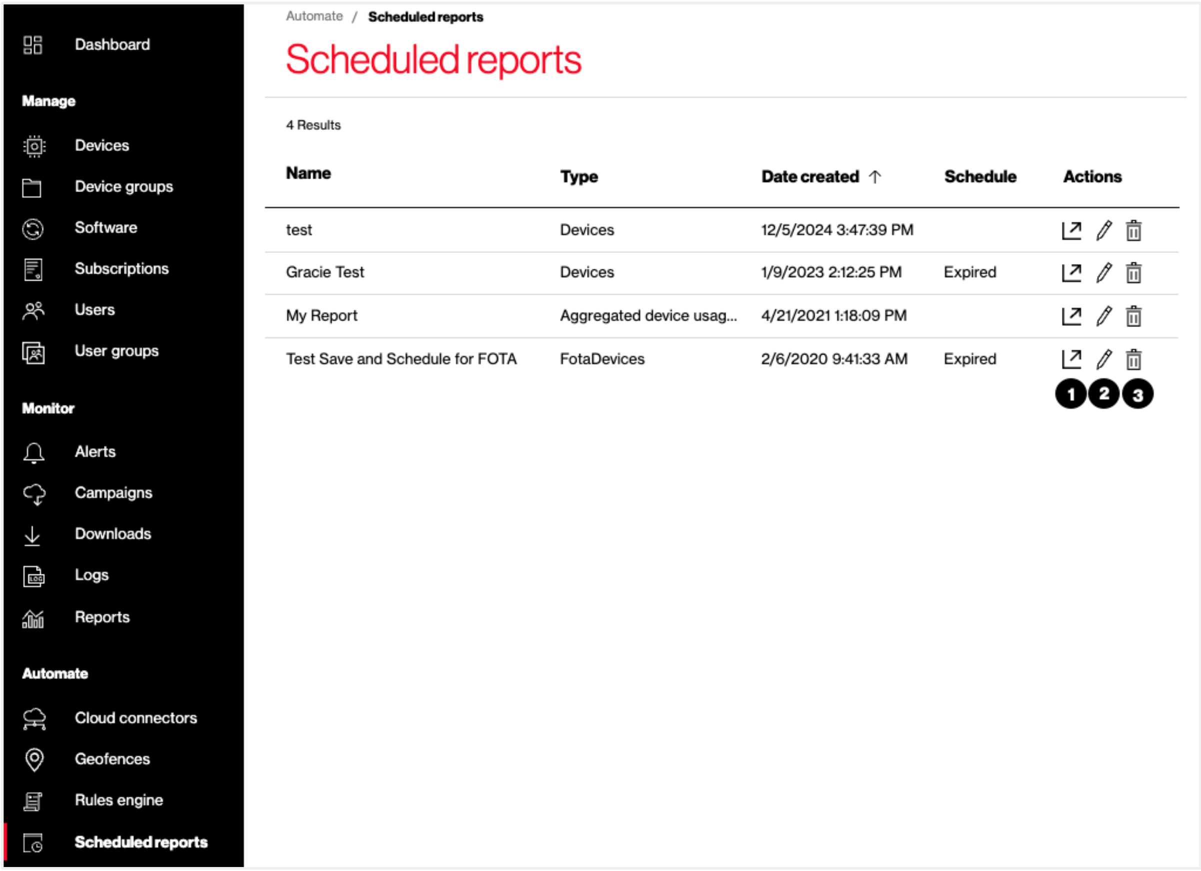
Rule name *
Designate a name
My Price Plan Optimizaton Rule

Enable

Save

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.



Scheduled reports

4 Results

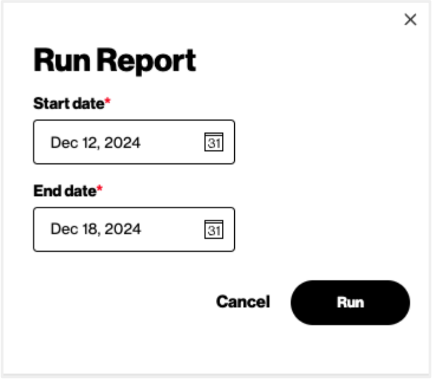
Name	Type	Date created ↑	Schedule	Actions
test	Devices	12/5/2024 3:47:39 PM		↗ ✎ 🗑
Gracie Test	Devices	1/9/2023 2:12:25 PM	Expired	↗ ✎ 🗑
My Report	Aggregated device usag...	4/21/2021 1:18:09 PM		↗ ✎ 🗑
Test Save and Schedule for FOTA	FotaDevices	2/6/2020 9:41:33 AM	Expired	↗ ✎ 🗑

Elements on the Scheduled reports 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 ↗

1. On the left navigation, click **Scheduled reports**. The *Scheduled reports* page opens.
2. Click the report's run icon ↗. The *Run Report* dialog opens to enter a date range.



Run Report

Start date*

Dec 12, 2024

End date*

Dec 18, 2024

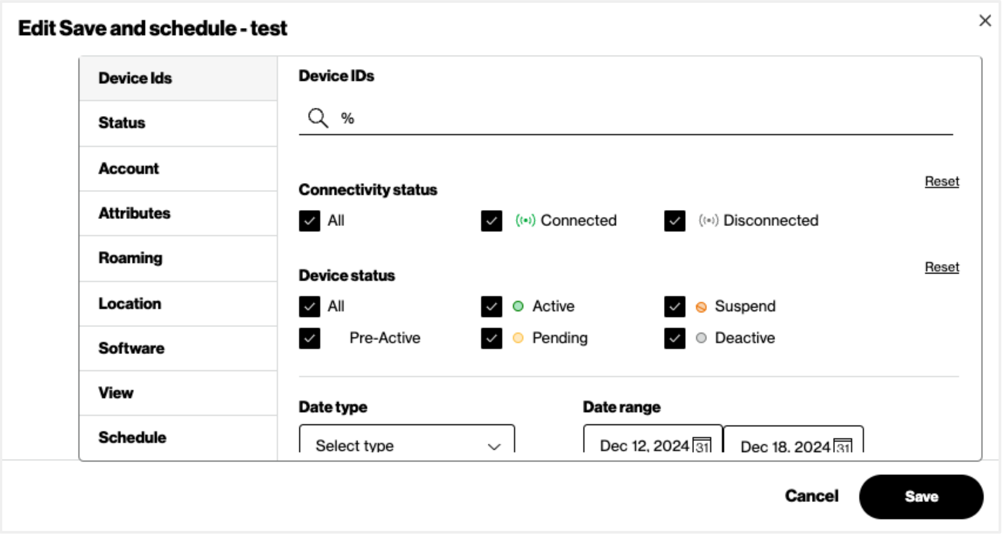
3. Enter a **Start date** and an **End date**.
4. Click **Run**.

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

1. On the left navigation, click **Scheduled reports**. The *Scheduled reports* page opens.
2. Click the report's edit icon ✎. The Edit Report page opens.



Edit Save and schedule - test

Device IDs

%

Connectivity status

☑ All ☑ Connected ☑ Disconnected

Device status

☑ All ☑ Active ☑ Suspend

☑ Pre-Active ☑ Pending ☑ Deactive

Date type

Select type

Date range

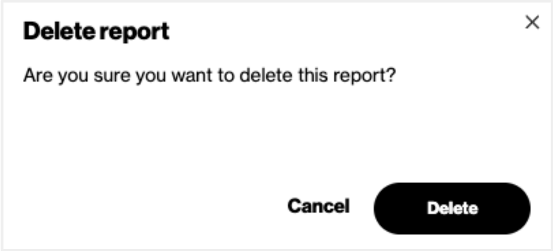
Dec 12, 2024 Dec 18, 2024

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.
4. Update the **View**.
5. Update the **Schedule**.
6. If the report is scheduled to run at a later time, check the **Schedule** option.
7. Click **Save**.

Delete a scheduled report

How to delete a scheduled report

1. Click the report's Delete icon🗑. You will be prompted to confirm deletion.



Delete report

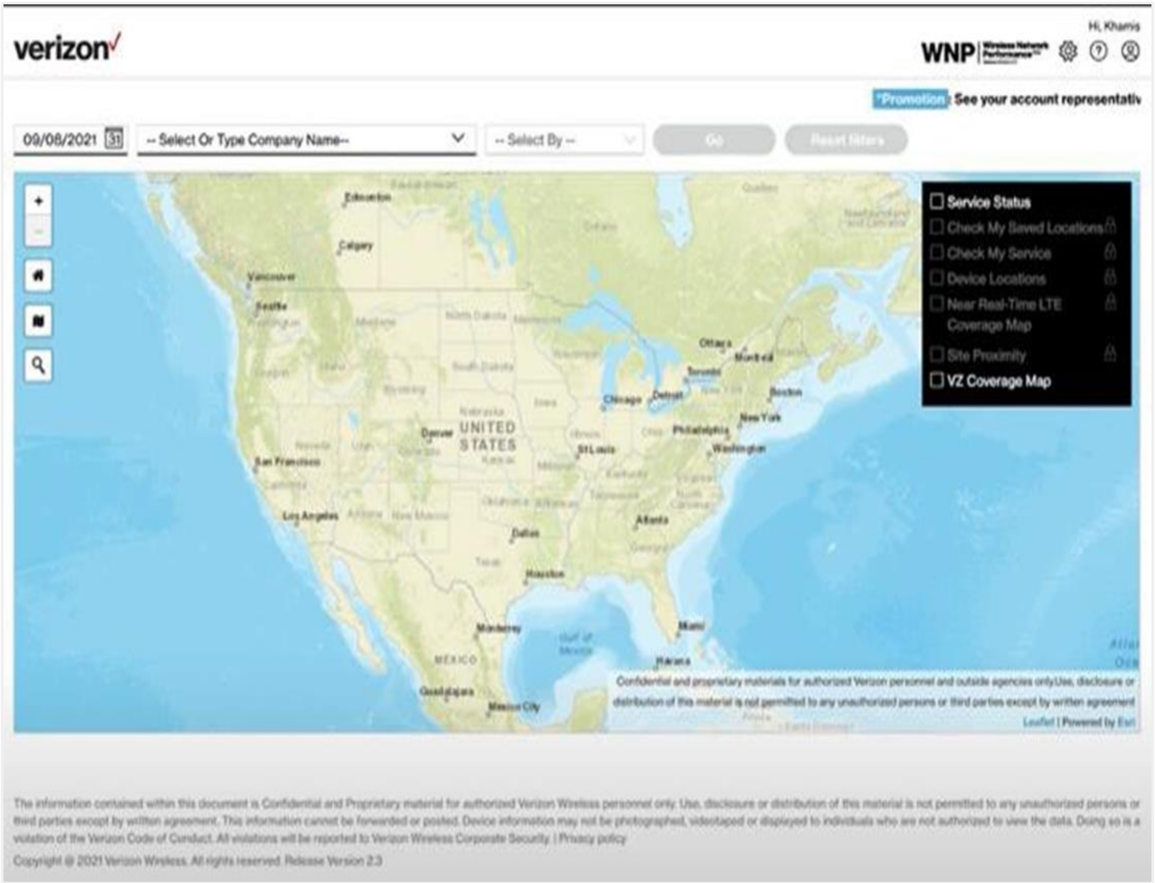
Are you sure you want to delete this report?

2. Click **Delete** to complete the process.

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 ⠿.



*Promotion: See your account representativ

Date: 09/08/2021

Confidential and proprietary materials for authorized Verizon personnel and outside agencies onlyUse, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement

The information contained within this document is Confidential and Proprietary material for authorized Verizon Wireless personnel only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement. This information cannot be forwarded or posted. Device information may not be photographed, videotaped or displayed to individuals who are not authorized to view the data. Doing so is a violation of the Verizon Code of Conduct. All violations will be reported to Verizon Wireless Corporate Security. | Privacy policy

Copyright @ 2021 Verizon Wireless. All rights reserved. Release Version 2.3

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: **MCC** – Mobile Country Code (311) **MNC** – Mobile Network Code (480) **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.
Address or PPU	The Primary Place of Use is the address where the wireless number of a device is derived. This is present if you use addresses during activation, plan changes or setting them explicitly for your devices. This is not necessarily the Location of the device.
Rate Plan	A contracted plan between an organization and an account, defining how each Device is charged for both subscription fees and usage of the network.
Role	Each user has an associated Role that defines the privileges the user has for seeing and working with data and functionality in the portal.
SKU	The Stock Keeping Unit assigned to a device.
SIM	The Subscriber Identity Module is a unique identifier, which can be embedded or on a physical card that is inserted in a 4G device to establish cellular connectivity.
Session	A single data context established between a device and the ThingSpace platform.
User	A unique sequence of characters used to identify a user and allow access.
Wildcard	Using a wildcard character allows you to use the percent sign (%) at the end of the string and search for everything that starts with that string.

Appendix

Field definitions

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

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

Column name	Definition
LWM2M streaming eligible	The device has LwM2M registered to Verizon.
Modem	Modem information, if available.

Radio signal strength	Represents the entire received power including noise.
	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).
	Excellent=-65 Good=-65 to -75
	Fair=-75 to -85
	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.
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.

Term used	Definition
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.
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 terms

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 management terms

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.
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.

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.