USER GUIDE

Verizon
M2M Management Center

VERIZON BUSINESS ONLINE SOLUTIONS

Verizon Wireless My Business Account and Verizon Enterprise Center

August 2014

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 guaranty or warranty, express or implied, as to the accuracy or completeness of any information contained or referenced herein.

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

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

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

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

Submit technical questions to
Customer Support at 800.525.0481.

Contents

1 Introduction

1.1 Welcome to the M2M Management Center

The Verizon M2M Management Center is an environment where you can manage the connectivity of your machine-to-machine (M2M) devices. You can use the M2M Management Center to monitor device performance, usage and connection status; generate and export current and historical reports on device usage and provisioning; and set up notifications to be triggered when a specific event occurs or when a predefined threshold is exceeded.

1.2 About this User Guide

This User Guide is organized as follows to assist you in completing tasks in the M2M Management Center quickly and efficiently:

Chapter 1 Introduction describes the features and user interface elements of the M2M Management Center.

Chapter 2 M2M Management Center Tasks presents step-by-step instructions for all tasks you can perform in the application. Gaining access to the M2M Management Center is explained first, followed by tasks that help you customize the interface. Then, more frequently performed tasks are presented before those performed infrequently.

Chapter 3 Screen Property Details defines all elements on the screens that comprise the M2M Management Center.

Chapter 4 About the M2M Management Center includes in-depth topics and technical details that apply to overall use of the M2M Management Center for device connectivity management and how system interactions affect data shown in the M2M Management Center.

1.3 New in This Release

The August 2014 release of the M2M Management Center includes the new Download Center repository, which holds report files you have exported for up to seven days.

1.4 M2M Management Center Features

The M2M Management Center offers the following features for managing the connectivity of machine-to-machine devices:

+ Direct access to the Verizon Wireless My Business Account and Verizon Enterprise Center Web online business portals to perform device management and provisioning
+ Ability to select the first screen to display upon entering the M2M Management Center from either a Verizon Wireless My Business Account or Verizon Enterprise Center Web portal
+ Support for multiple billing accounts, allowing you to switch between individual billing accounts to view and manage devices or to display data/devices for all billing accounts to which you have access
+ Data usage primarily calculated from near-real-time records written to an M2M Management Center database
+ An interactive Dashboard you can design and filter to ascertain system, device and device group status at a glance, plus drill-down capability to obtain device and system details when needed
+ Comprehensive Device List, from which you can view the state of your devices in several ways
+ Ability to search and sort devices by group, customer-defined properties such as name or location, activation date, service plan, connection status, and more
+ Up to five custom fields to use per device for internal names and/or attributes for identifying, sorting, tracking and filtering
+ Reports that show connection status, connected session history, transaction status and device usage by day and over a date range

- Inclusion of selected AAA Attribute Value Pairs (AVPs) in Connection History Report views for individual devices, providing more insight into device connectivity for troubleshooting
- Controls to create and edit customized views of the Device List and all reports, plus the ability for any user to designate any view as his/her default for the Device List or any report
- A Data Usage Trending histogram to graphically analyze data usage patterns over a specific period of time
- Optional notification feature to generate alerts for M2M Management Center users and non-users when a value or status changes, device provisioning actions are triggered and/or action-related or usage thresholds are exceeded
- Device grouping capability to perform select actions on and/or generate alarms for multiple devices at once
- Ability for users with Customer Admin privileges to specify device attributes in bulk for up to 1000 devices by file or 10 devices by screen entry
- Complete historical logs of system events such as device provisioning transactions and alerts, as well as user actions in the M2M Management Center
- Ability to issue remote Preferred Roaming List (PRL) updates for one or multiple devices specifically configured with a software client capable of performing the update[1]

1.5 About the M2M Management Center Interface

The user interface of the M2M Management Center employs the following common elements throughout:

- Navigation Menu
- Common Button Controls
- Required Fields
- Default and Advanced Search Criteria
- Date Pop-Up
- Page Navigation Controls
- Page Manipulation Controls
- List Manipulation
- Wildcard Character
- Help Icon

1.5.1 Navigation Menu

The M2M Management Center Navigation menu includes the following tabs:

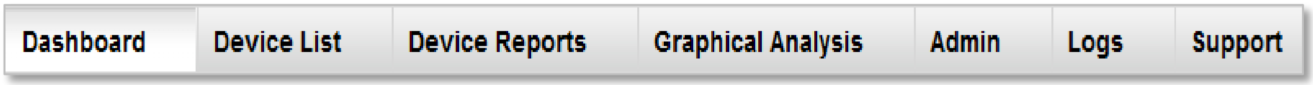


Figure 1-1 Navigation menu

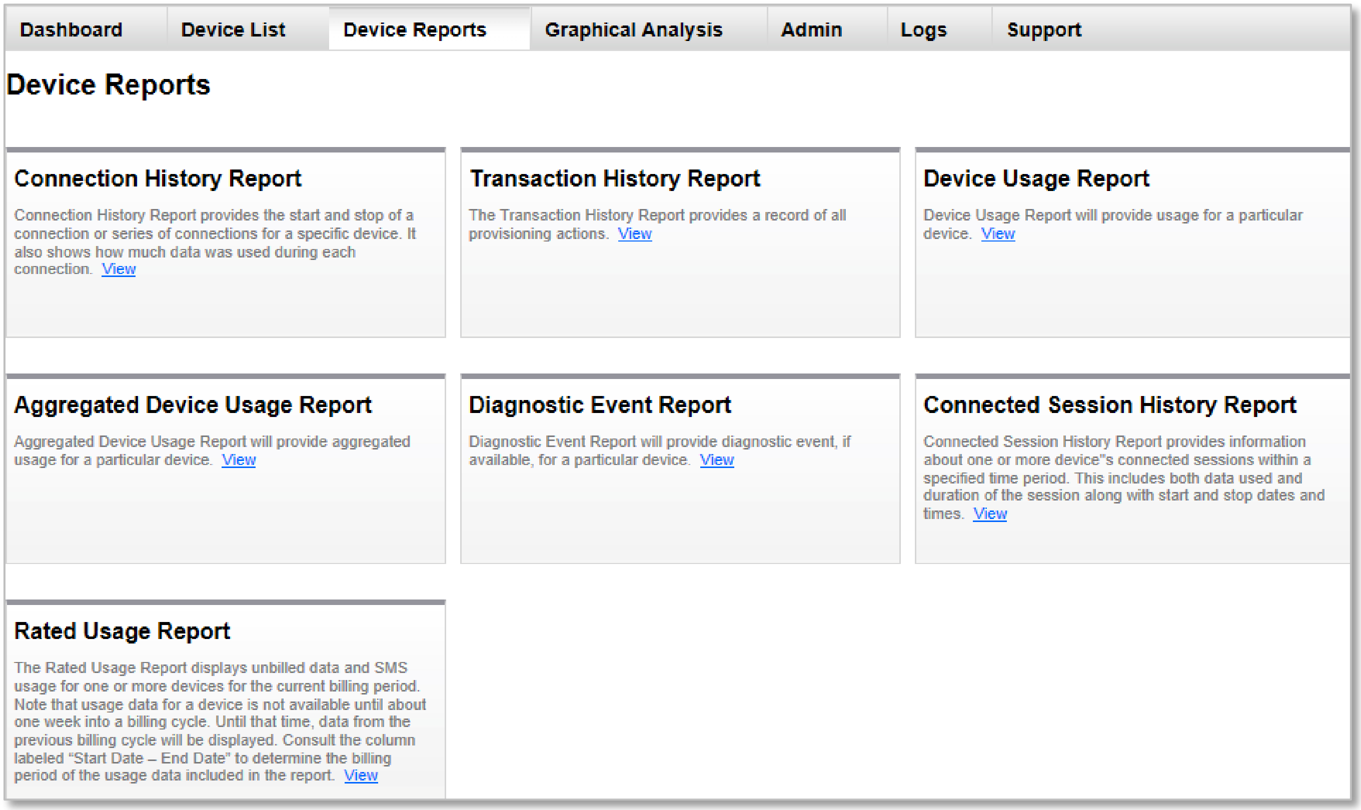
Functional areas represented on the Navigation menu include:

- Dashboard—Provides both quick, at-a-glance graphical status monitoring (via real-time charts and tables) of key device-related data and drill-down capability to access detail when needed.

[1] Devices must be specifically configured with a software client capable of performing the update.

- Device List—Displays information about individual devices. Offers device-related actions such as creating or changing custom information about devices, grouping devices, and waking up one or more devices.
- Device Reports— Includes links to the following historical and current reports as well as the Download Center:
    - Connection History Report
    - Transaction History Report
    - Connected Session History Report
    - Device Usage Report
    - Aggregated Device Usage Report
    - Diagnostic Events Report (optional report displayed only for customers with Device Diagnostics feature)
    - Rated Usage Report

  When you click directly on the Device Reports tab without selecting a sub-menu item, the Device Reports landing screen appears:



Device Reports

Connection History Report

Connection History Report provides the start and stop of a connection or series of connections for a specific device. It also shows how much data was used during each connection. View

Transaction History Report

The Transaction History Report provides a record of all provisioning actions. View

Device Usage Report

Device Usage Report will provide usage for a particular device. View

Aggregated Device Usage Report

Aggregated Device Usage Report will provide aggregated usage for a particular device. View

Diagnostic Event Report

Diagnostic Event Report will provide diagnostic event, if available, for a particular device. View

Connected Session History Report

Connected Session History Report provides information about one or more device"s connected sessions within a specified time period. This includes both data used and duration of the session along with start and stop dates and times. View

Rated Usage Report

The Rated Usage Report displays unbilled data and SMS usage for one or more devices for the current billing period. Note that usage data for a device is not available until about one week into a billing cycle. Until that time, data from the previous billing cycle will be displayed. Consult the column labeled "Start Date – End Date" to determine the billing period of the usage data included in the report. View

Figure 1-2 Device Reports landing screen

- Graphical Analysis—Generate a trending histogram by selecting the Data Usage Trending Chart command.
- Admin—Provides access to a sub-menu of the following administrative functions:
    - Contact Setup- Edit settings for M2M Management Center users and create records for non-system users who receive notifications.
    - Notification Setup- Set up rules that the system uses to generate alerts.
    - Notification Group Setup- Group M2M Management Center users and non-users who receive notifications.
    - Dashboard Config – Customize the Dashboard to show information important to you.

    - Device Group– Form meaningful groups of devices.
    - Custom Field Labels– Assign labels to custom fields to standardize their use.
    - Upload Devices– Apply device group and custom field settings to multiple devices using screen or file input.
    - Account Preferences– Set the display format for Electronic Serial Number (ESN) and Mobile Equipment Identifier (MEID) device identifiers.
- Logs—Leads to a sub-menu of the following choices:
    - Master Log– View a record of all M2M Management Center actions.
    - Notification Log– View a record of notifications generated.
- Support—Supplies links to customer support, documentation and other helpful information.

1.5.2 Common Button Controls

Use the following buttons as described anywhere they appear in the M2M Management Center:

Button Label	Function
Add New	Display the fields and controls that allow you to create a new record.
Cancel	Close the current window without performing any action.
Close	Dismiss the current display-only window.
Export	Generate a comma-separated value (CSV) file of selected data offline. Retrieve the exported file from the M2M Management Center Download Center when you receive an email stating it is ready. **NOTE:** + **The source for data in exported lists and reports is a reporting database, which differs from the primary database used for displaying data in the M2M Management Center user interface. Thus, exported data may be a few hours older than what you see in the M2M Management Center.** + **You can export up to ten (10) reports per day.**
Generate Report	Display a report using the criteria specified. Subsequent clicks resubmit the report query and refresh the data in a displayed report. **NOTE:** + **When the system determines that a report is too lengthy to generate on-screen, you will be offered the option of generating it offline, in which case it becomes available in the M2M Management Center Download Center, similar to exporting a report (see previous row).** + **To print any report, you must either execute a Print Screen from the keyboard when the report is displayed or export the report to the Download Center, import it into another application such as a text editor or spreadsheet, and print it.**
Reset	Clear all search criteria fields.
Save	Save the information entered to the database.
Search	Find all records that match the criteria entered.
Submit	Initiate the action on the selected device(s).

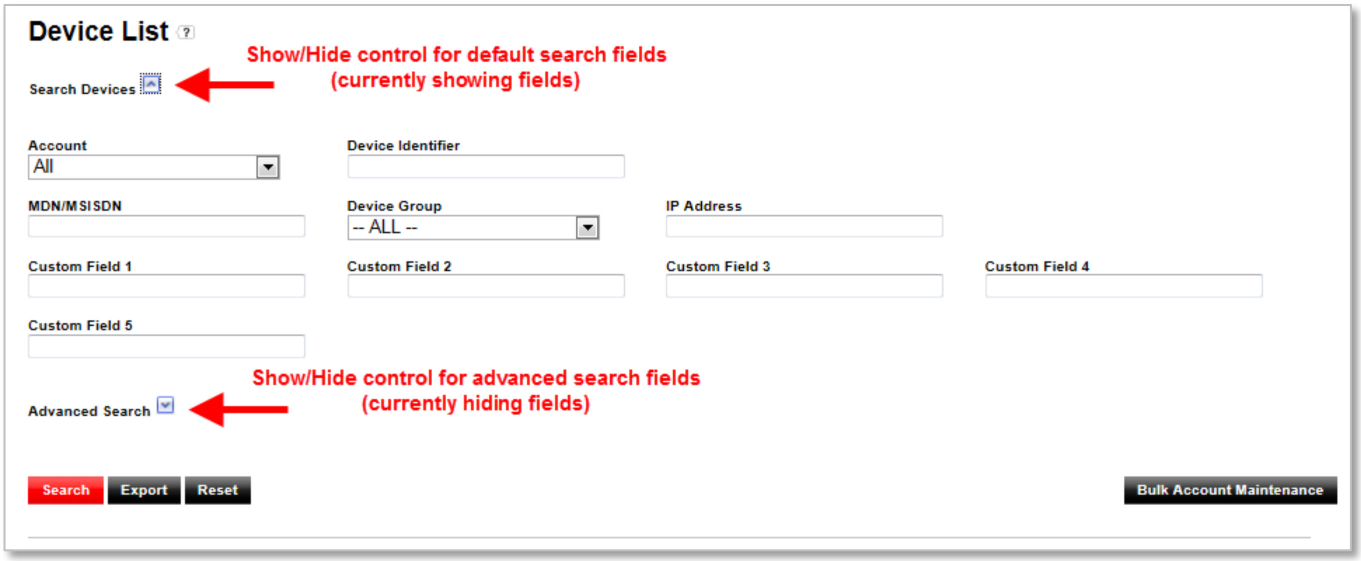
1.5.3 Required Fields

Any field requiring input is denoted with a red asterisk (*).

1.5.4 Default and Advanced Search Criteria

Many screens, including the Device List and screens for all reports, accept criteria to help you target your results to display only relevant data. Search criteria are divided into default and advanced categories, where default criteria are displayed at the top of the page and represent the most commonly used search fields.

When you need to target your data results more than what the default search criteria offer, click the expand control to show the Advanced Search fields. Likewise, when the default search criteria are hidden, use the expand control located near the screen heading to show the default search fields.



Device List

Show/Hide control for default search fields (currently showing fields)

Search Devices

Account: All

Device Identifier

MDN/MSISDN

Device Group: -- ALL --

IP Address

Custom Field 1

Custom Field 2

Custom Field 3

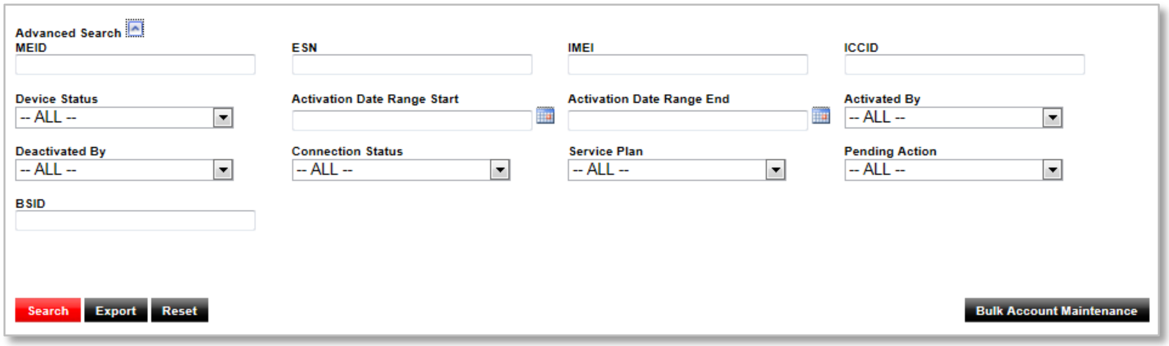
Custom Field 4

Custom Field 5

Show/Hide control for advanced search fields (currently hiding fields)

Advanced Search

Figure 1-3 Device List default search fields and search criteria controls



Advanced Search

MEID

ESN

IMEI

ICCID

Device Status: -- ALL --

Activation Date Range Start

Activation Date Range End

Activated By: -- ALL --

Deactivated By: -- ALL --

Connection Status: -- ALL --

Service Plan: -- ALL --

Pending Action: -- ALL --

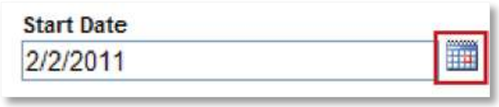
BSID

Figure 1-4 Advanced Search fields

When you populate search criteria in the Device List or a report and then navigate to another screen with the same search fields, your entries are retained. Use the Reset button to clear all search field entries and start a new search.

1.5.5 Date Pop-Up

In addition to entering a date directly, you can employ the Date pop-up to enter a date. To display the Date pop-up, first click the Date icon:

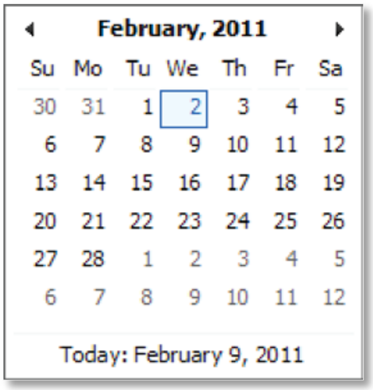


Start Date

2/2/2011

Figure 1-5 Date icon

The Date pop-up appears:



February, 2011

Su	Mo	Tu	We	Th	Fr	Sa
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

Today: February 9, 2011

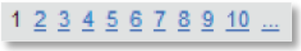
Figure 1-6 Date pop-up

Use the left and right arrow controls that frame the month name and year to display the previous and next month, respectively.

Select a date by clicking it in the calendar represented in the Date pop-up.

1.5.6 Page Navigation Controls

Some reports that you generate display over multiple pages. Use the paging controls at the bottom of each report page to click the number of the page you want to view:

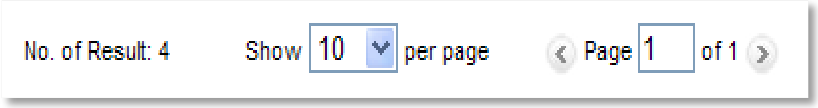


1 2 3 4 5 6 7 8 9 10 ...

Figure 1-7 Page navigation controls

1.5.7 Page Manipulation Controls

The controls below, which are found at the bottom left of a list or report results page, when applicable, allow you to manipulate the length of the displayed output. Use them as follows:



No. of Result: 4 Show 10 per page Page 1 of 1

o

Figure 1-8 Page manipulation controls

- No. of Result—Displays the total number of rows in the report.
- Show X per Page—Specify the number of rows to display per page by entering the number or selecting from the drop-down. This setting is saved when you exit the report screen.
- Page X of Y—Specify the page to display (X) out of all possible pages (Y) by entering the number of the selected page. Use the left and right arrow controls to display the previous and next pages of the current report, respectively.

1.5.8 List Manipulation

Sort listed data displayed in the M2M Management Center by clicking any underlined column heading. This sorts the list or report by the data in the column you click. Subsequent clicking on the column heading switches between ascending and descending order.

1.5.9 Wildcard Character

The wildcard character employed by the M2M Management Center is the percent sign (%). You must use this character when you are unsure of the exact data to enter in a required search field (marked with a red asterisk). For example, to search for all items regardless of value, enter "%"; to search for all items starting with the letter S, enter "S%"; to search for all items ending with the letter S, enter "%S"; or, to search for all items containing the letter S, enter "%S%". In search fields that are not required (no asterisk), the wildcard character is optional. When you leave a field that is not required blank, all values are returned in a search.

1.5.10 Help Icon

Click this icon to display a help topic corresponding to the current screen or control, plus gain access to the entire online help system.

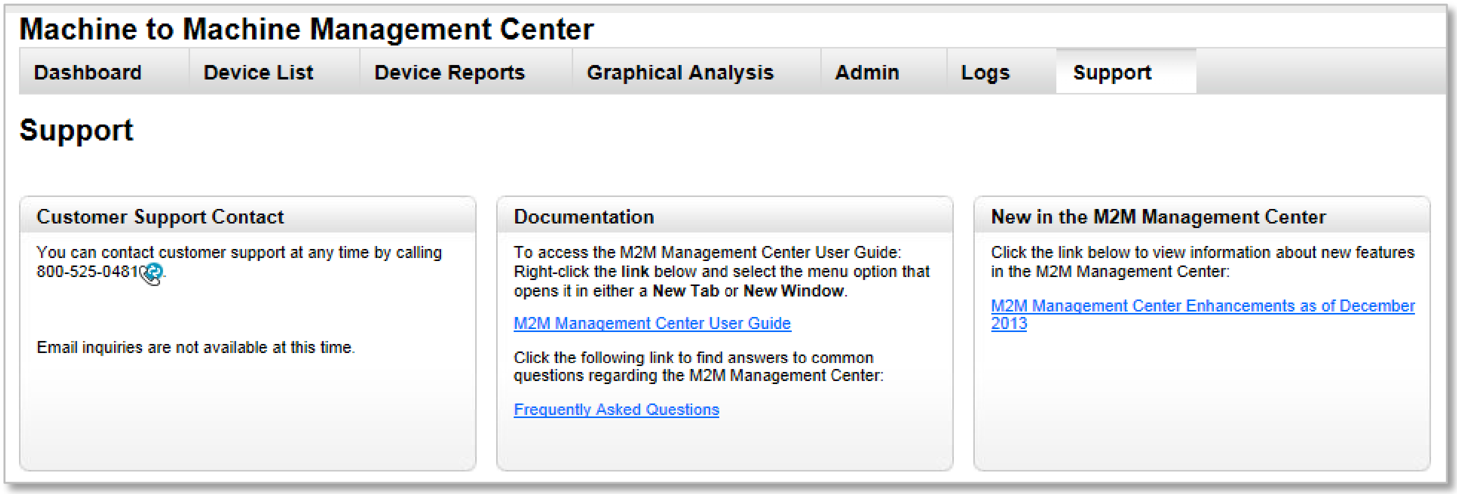
Figure 1-9 Help icon

When a help window is displayed, click a hyperlink in the Table of Contents at the left to display the corresponding topic at the right.

NOTE: The online help system contains topics that do not apply to the M2M Management Center within the Verizon Wireless My Business Account or Verizon Enterprise Center.

1.6 Support Screen

The Support screen provides technical support contact information as well as links for a downloadable User Guide, information about enhancements made for the latest version of the M2M Management Center and answers to Frequently Asked Questions (FAQs).



Support

Customer Support Contact

You can contact customer support at any time by calling 800-525-0481.

Email inquiries are not available at this time.

Documentation

To access the M2M Management Center User Guide: Right-click the **link** below and select the menu option that opens it in either a **New Tab** or **New Window**.

M2M Management Center User Guide

Click the following link to find answers to common questions regarding the M2M Management Center:

Frequently Asked Questions

New in the M2M Management Center

Click the link below to view information about new features in the M2M Management Center:

M2M Management Center Enhancements as of December 2013

Figure 1-10 Support screen

2 M2M Management Center Tasks

This chapter is a “how-to” guide for completing tasks in the M2M Management Center. Some tasks are accompanied by links to screen property details in Chapter 3 Screen Property Details or to background information in Chapter 4 About the M2M Management Center.

2.1 Access the M2M Management Center

The following Web browsers support the M2M Management Center:

- Microsoft Internet Explorer® versions IE9 and IE10
- Mozilla® Firefox® versions 20+

Other Web browsers are not officially supported and may not provide an optimal user experience.

NOTE: For Microsoft Internet Explorer users only: To ensure that you always see your latest M2M Management Center portal settings whenever a screen refresh occurs, make the following browser setting:

1. Under the Tools menu, select Internet Options.

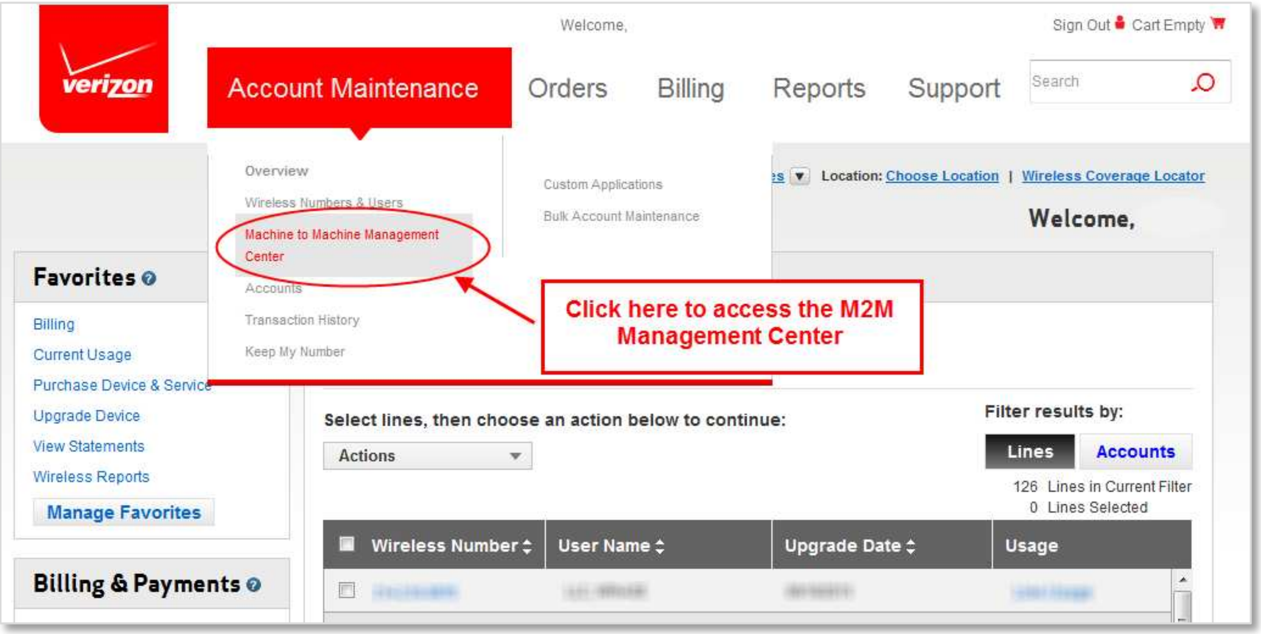
2. On the General tab, under Browsing History, click the Settings button.

3. Select the “Every time I visit the webpage” option. Ensure that “Automatically” is checked.

4. Restart Microsoft Internet Explorer.

Open the M2M Management Center

Log into either the Verizon Wireless My Business Account or Verizon Enterprise Center Web portal to reach the M2M Management Center from multiple locations. An example is shown below.

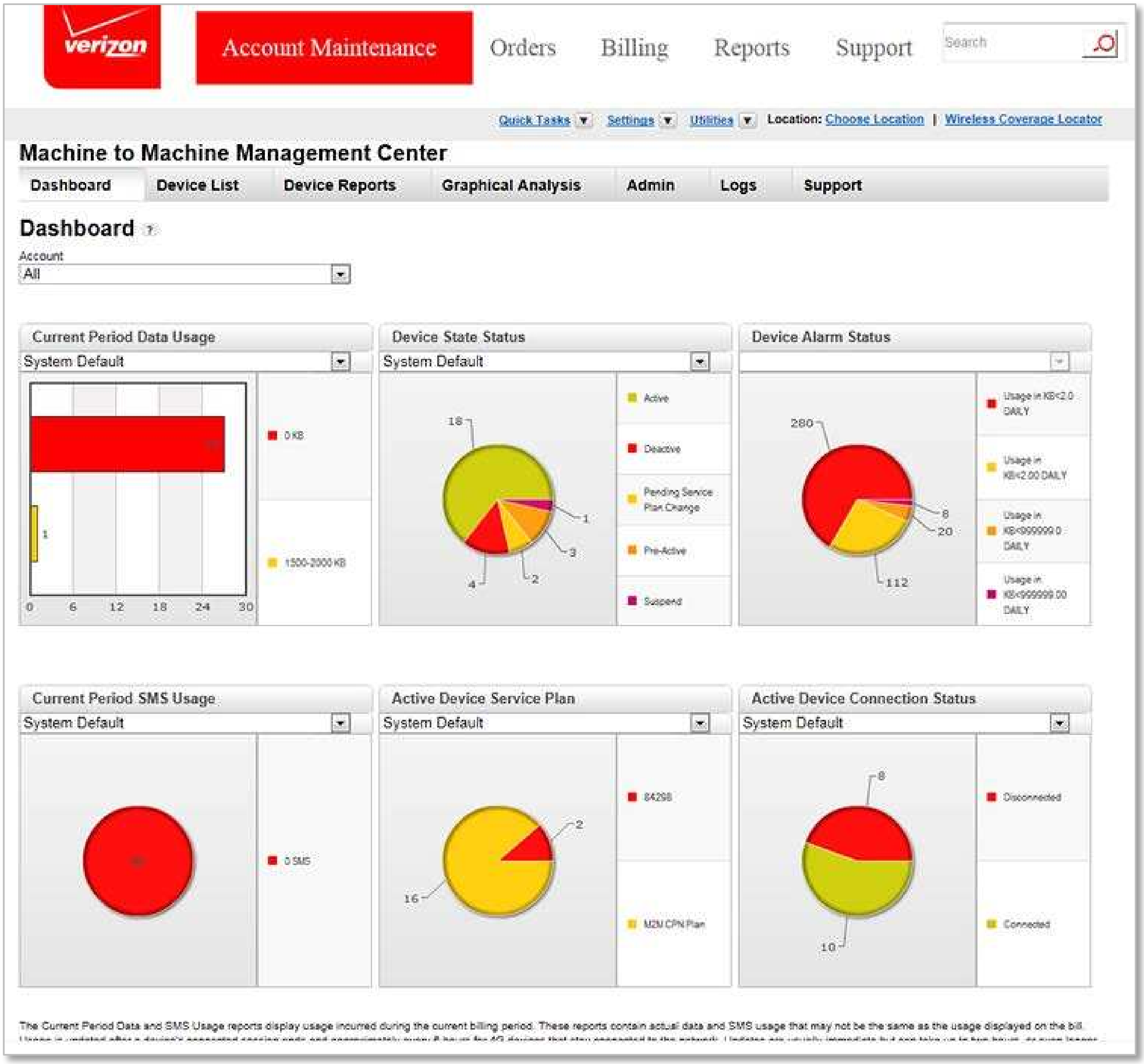


Click here to access the M2M Management Center

Figure 2-1 Accessing the M2M Management Center

Another control you can use to open the M2M Management Center is the Access Machine to Machine button in the Custom Applications area.

The M2M Management Center screen that appears depends on the Portal Landing Page setting in your contact (system user) record. The default setting is the Dashboard.



The Current Period Data and SMS Usage reports display usage incurred during the current billing period. These reports contain actual data and SMS usage that may not be the same as the usage displayed on the bill.

Figure 2-2 M2M Management Center—Dashboard

Initially, the Account selection for the Dashboard is All, meaning that the charts displayed reflect data for all billing accounts to which you have access. If you have access to more than one account and want to change the display, drop down the Account list and select a different billing account to view. Your choice will follow you as you navigate through the M2M Management Center until you make another account selection.

2.2 Suggested Setup Tasks by User Role

Related Information

User Role Access Permissions

This section includes lists of recommended tasks to be executed by each type of system user to prepare the M2M Management Center for daily use. These tasks are optional and some may not apply depending on the way you plan to conduct your machine-to-machine business. Step-by-step instructions for these tasks are found in this chapter.

2.2.1 Customer Admin Tasks

To set up the M2M Management Center for use, perform the following tasks listed below in order:

NOTE: To perform the first step, users (otherwise known as contacts) must access the M2M Management Center from the Verizon My Business or Verizon Enterprise Center portal at least once to establish contact records (Accessing the M2M Management Center).

1. Access the contact record of each user and enter his/her Time Zone and optionally change the Portal Landing Page, which is the first screen that appears every time the user enters the M2M Management Center (Edit a Contact Record).

2. Assign custom field labels for device properties you want to track for your organization (Assign Labels to Custom Fields).

3. Specify the preferred way to display Verizon 2G/3G device identifiers throughout the M2M Management Center (Choose Device Identifier Display Preferences).

4. If you are using notifications, perform the following sub-steps:

    a. To aggregate data or actions for multiple devices, create device groups either via the Device List or using Admin > Device Groups (Create a Device Group from the Device List; Create a Device Group from the Admin Tab).

    b. Organize system users into notification groups (Create a Notification Group). Note that users must first access the M2M Management Center, at which point their contact records are established. Optionally add Alerts Only contact records for non-users to which you want to send notifications (Add an Alerts Only Contact).

    c. Define notification rules (Create a Notification Rule).

5. Change the system default views of the Device List and reports, plus the Dashboard filter system defaults, if necessary (Edit or Delete a View; Manage Filters).

2.2.2 Cust Operator Tasks

To set up the M2M Management Center for use, perform the following tasks listed below in order:

1. Create customized Dashboard(s) for your All accounts view and for each account to which you have access (Configure Dashboards).

2. Create custom filters to apply to most Dashboard charts (Manage Filters).

3. Define custom views for the Device List and device reports (Create a View); designate default views if you do not want the system defaults.

2.3 Customize Your M2M Management Center

Any user can set up custom views for the Dashboard, Device List and any report in the M2M Management Center.

If you are an administrative-level user, you can define labels for up to five custom fields that can be used to describe devices. The labels you define will be visible to all users in your organization and seen throughout the application. They will serve to remind users where to enter certain information about devices.

This section includes instructions for the following customization tasks:

- Configure Dashboards
- Customize the Device List, Reports and Data Usage Trending Chart Screens
- Assign Custom Field Labels

2.3.1 Configure Dashboards

Dashboards contain key device-related charts in various graphical formats and are fully configurable. You can configure the following characteristics of a Dashboard:

- Content and layout, including the charts included in a Dashboard and the format for each chart
- Additional settings, including the value ranges known as usage buckets, reflected on certain Dashboard charts
- Filters to apply to most charts included in a Dashboard
- Display features, such as legends and callouts

Define a Dashboard Layout

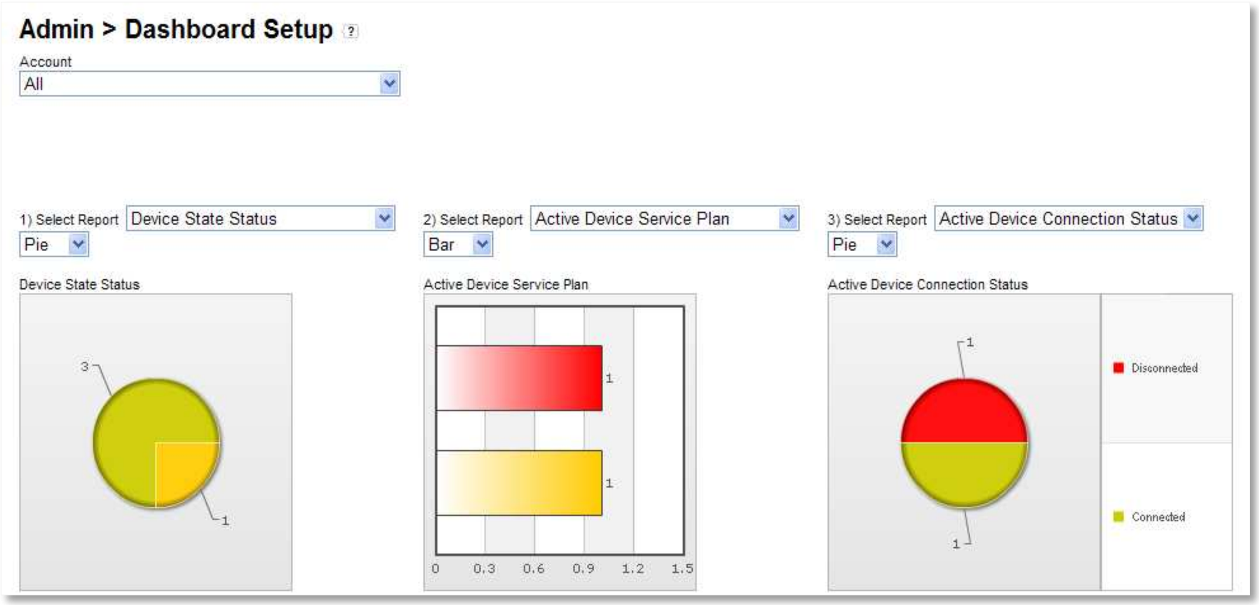
Related Information

Dashboard Properties

Use the Dashboard Setup screen to configure the appearance and content of a Dashboard. Dashboard layouts are defined by account; therefore, you can have several layouts when you have access to multiple billing accounts. Design each Dashboard to show the relevant charts for each account to which you have access. You can select up to six charts to include on a Dashboard.

To configure the layout of a Dashboard:

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears, showing the current Dashboard configuration of the selected account:



Admin > Dashboard Setup

Account: All

1) Select Report: Device State Status — Pie

2) Select Report: Active Device Service Plan — Bar

3) Select Report: Active Device Connection Status — Pie

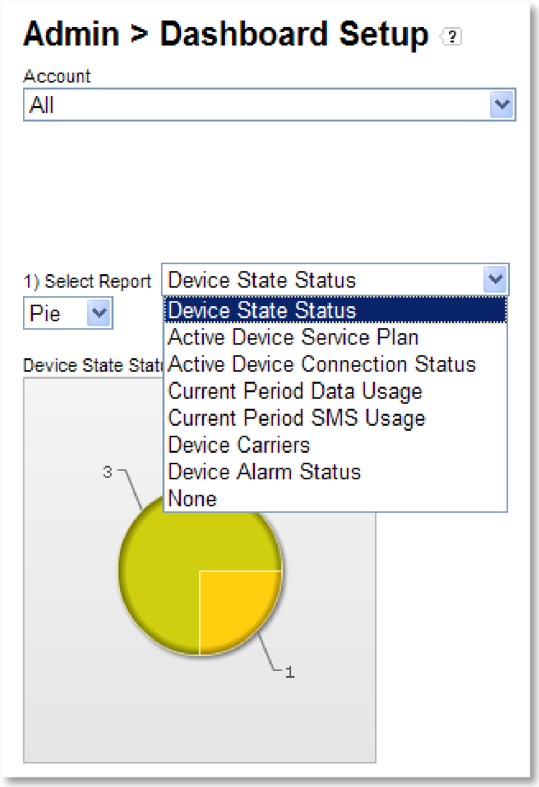
Figure 2-3 Dashboard Setup screen

NOTE:

- **Up to six positions (numbered 1 to 6), organized in two rows of three, are reserved for charts on a Dashboard. Each chart position has corresponding drop-downs where you can select a chart type and format. Select None from the Select Report list to leave a position empty.**
- **You can define a custom Dashboard layout for each billing account to which you have access, as well as the All billing accounts view.**

2. Drop down the Account list and choose the billing account for which you want to design or edit a Dashboard; select All to design or edit the Dashboard that includes data and devices for all billing accounts to which you have access.

3. To modify the chart shown in a position on the Dashboard, drop down the corresponding Select Report list and choose the chart to display in the position.



Admin > Dashboard Setup

Account: All

1) Select Report: Device State Status

Pie

Figure 2-4 Select Report drop-down

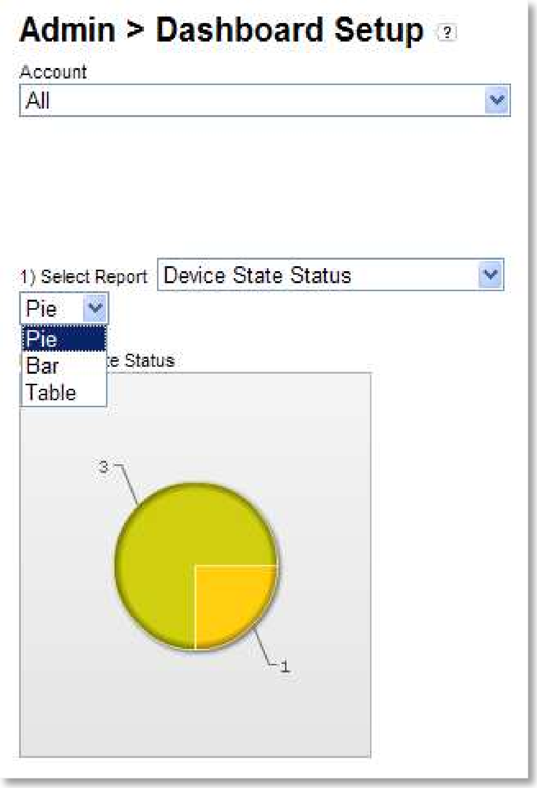
NOTE:

- **When displayed in either Pie or Bar format, the charts on the Dashboard screen include “hot spots”, which allow you to drill down and view the in-depth screens and reports shown in the table below, depending on the location where you click.**
- **This feature does not apply to charts with the Table format.**

Dashboard Chart	Drills Down to	Display Details
Active Device Service Plan	Device List	Active devices with the corresponding service plan.
Active Device Connection Status	Device List	Active devices in the corresponding connection state.
Current Period Data Usage	Aggregated Device Usage Report	Devices in the corresponding data usage bucket, further sorted by device with most usage to least in the current billing period.
Current Period SMS Usage	Aggregated Device Usage Report	Devices in the corresponding SMS usage bucket, further sorted by device with most SMS usage to least in the current billing period.
Device Alarm Status	Notification Log	Acknowledged and unacknowledged notifications for each device’s current bill cycle sent to the logged-in user’s notification group(s) for each alarm type configured for the group(s).
Device Carriers	Device List	Active devices with the carrier Verizon Wireless. **NOTE: This feature has limited value as this chart contains**

Dashboard Chart	Drills Down to	Display Details
		only one carrier, Verizon Wireless.
Device State Status	Device List	Devices in the corresponding device state.

4. To change the format of a chart to Pie, Bar or Table (examples below), select the format from the drop-down list located below the corresponding Select Report field:



Admin > Dashboard Setup

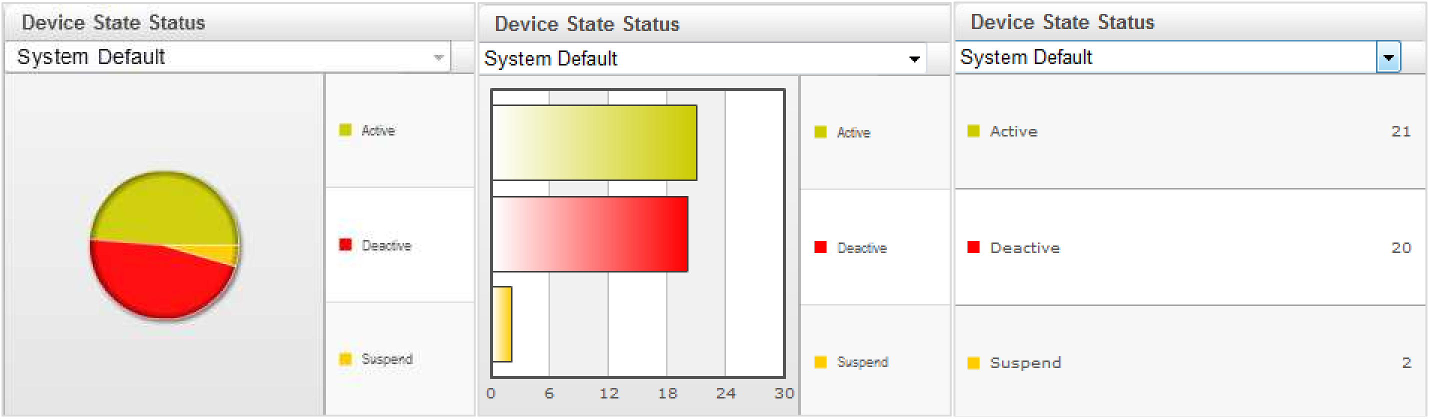
Account: All

1) Select Report: Device State Status

Pie

Figure 2-5 Report format drop-down

You can display a chart in Pie, Bar or Table format:

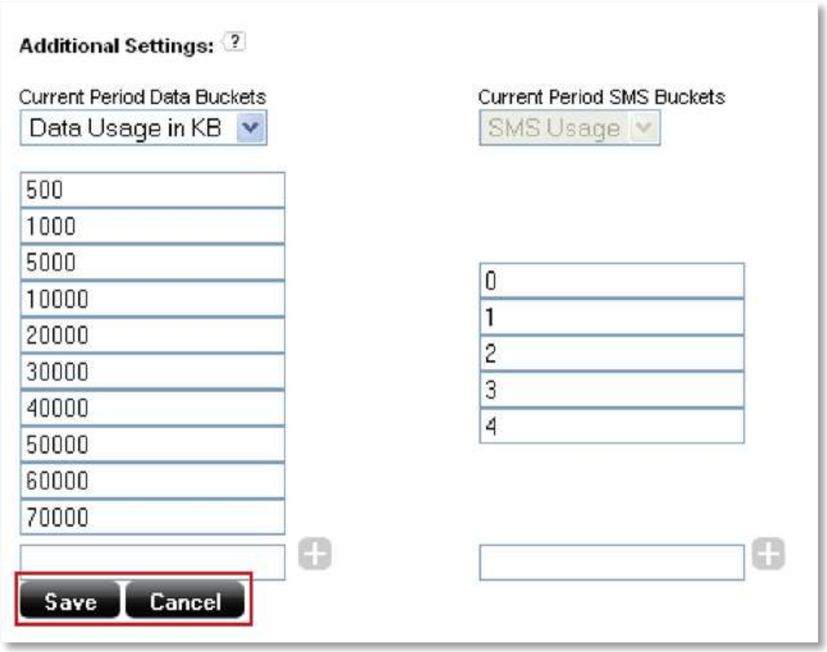


Device State Status — System Default

🟨 Active	21
🟥 Deactive	20
🟨 Suspend	2

Figure 2-6 Pie, Bar and Table format variations for Device State Status chart

5. When your Dashboard content is configured, either click Save to save your modifications or click Cancel to discard your changes. These button controls are found at the bottom left of the Dashboard Setup screen, below the Additional Settings:



Additional Settings: ?

Current Period Data Buckets: Data Usage in KB

500
1000
5000
10000
20000
30000
40000
50000
60000
70000

Current Period SMS Buckets: SMS Usage

0
1
2
3
4

Figure 2-7 Save and Cancel buttons

Modify Usage Buckets

Related Information

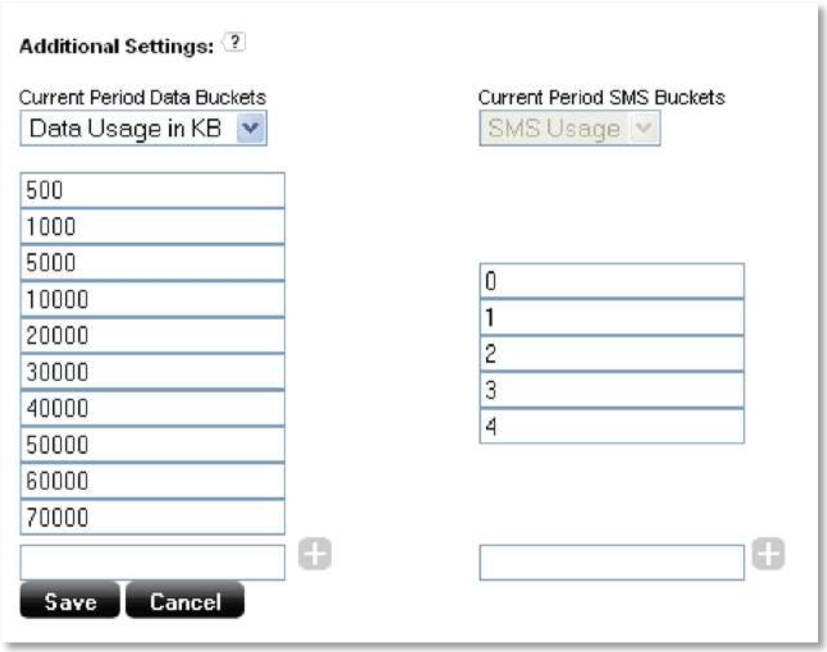
About Current Period and Bill Cycle

Accumulated Data Usage Calculations

Data Usage Bucket Defaults

SMS Usage Bucket Defaults

Use the Additional Settings area to modify usage buckets for charts shown in a Dashboard. Two types of buckets are available: Current Period Data Buckets and Current Period SMS Buckets.



Additional Settings: ?

Current Period Data Buckets: Data Usage in KB

500
1000
5000
10000
20000
30000
40000
50000
60000
70000

Current Period SMS Buckets: SMS Usage

0
1
2
3
4

Figure 2-8 Additional Settings configuration

Modify Current Period Data Buckets

To modify data usage buckets shown in the Additional Settings area:

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears.

2. Drop down the Account list and select the billing account of the Dashboard you want to modify.

3. At the top left of the Additional Settings area, at the bottom left of the Dashboard Setup screen, drop down the Current Period Data Buckets list and select Data Usage in MB or Data Usage in KB.

4. In the unlabeled fields below the drop-down, enter sequential values (top to bottom) corresponding to the upper limit of the data usage range you want to define. To delete a value, clear the field and enter nothing or zero (0).For example, for the values shown in Figure 2-6, the corresponding buckets would be: 0 to 500, 501 to 1000, 1001 to 2000, etc.

5. Click the + button to add each new value. This action also opens another usage bucket field for definition, if needed.

6. When you have defined all usage buckets, either click Save to write them to the database and use them in subsequent displays or click Cancel to discard your changes.

Modify Current Period SMS Buckets

To modify SMS buckets shown in the Additional Settings area:

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears.

2. Drop down the Account list and select the billing account of the Dashboard you want to modify.

3. In the unlabeled fields at the right of the Additional Settings area, which is located at the bottom left of the Dashboard Setup screen, enter sequential values (top to bottom) corresponding to the upper limit of the SMS range you want to define. To delete a value, clear the field and enter nothing or zero (0). For example, for the values shown in Figure 2-6, the corresponding buckets would be: 0, 1, 2, etc.

4. Click the + button to add each new value. This action also opens another SMS bucket field for definition, if needed.

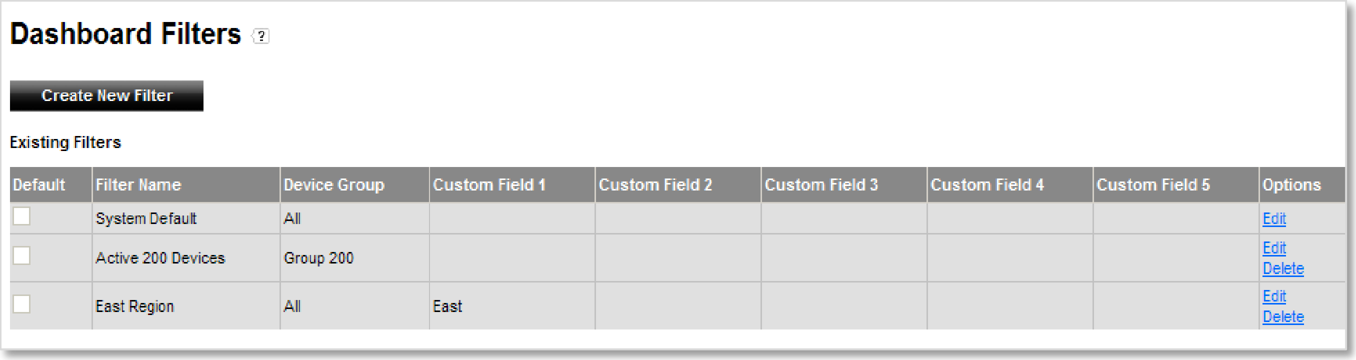
5. When you have defined all SMS buckets, either click Save to use them in subsequent displays, or click Cancel to discard your changes.

Manage Filters

Dashboard filters are applied to charts in the Dashboard to display data that is pertinent to you. The Dashboard Filters area of the Dashboard Setup screen allows you to create, edit and delete filters.

NOTE:

- **Filters can be applied to all Dashboard charts except Device Alarm Status.**
- **Dashboard filters are created at the contact (system user) level; therefore, the filters you create will be listed on the Dashboards of all accounts to which you have access. To apply filters correctly, be sure your Account selection is compatible with the device group selected in a selected filter.**



Dashboard Filters

Existing Filters

Default	Filter Name	Device Group	Custom Field 1	Custom Field 2	Custom Field 3	Custom Field 4	Custom Field 5	Options
□	System Default	All						Edit
□	Active 200 Devices	Group 200						Edit Delete
□	East Region	All	East					Edit Delete

Figure 2-9 Dashboard Filters area of Dashboard Setup screen

Create a Filter

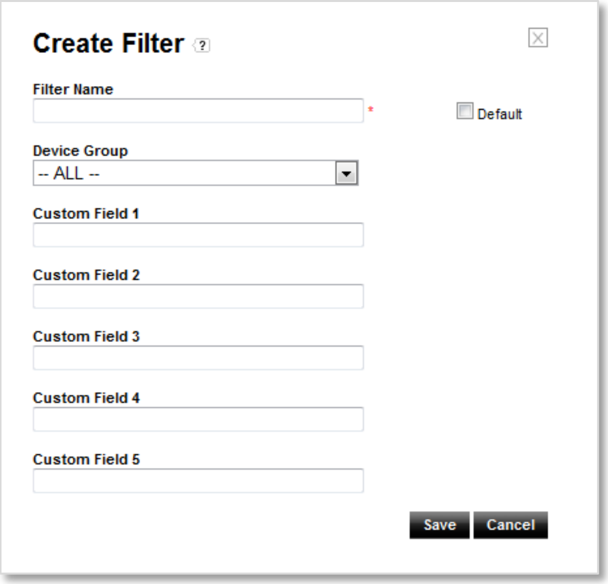
NOTE: Your pop-up may look different from the example below if your Customer Administrator assigned labels to one or more custom fields (see Assign Custom Field Labels).

To create a filter:

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears.

2. Drop down the Account list and select the billing account of the Dashboard for which you want to create a new filter.

3. In the Dashboard Filters area at the bottom of the screen, click Create New Filter. The Create Filter pop-up appears.



Create Filter

Filter Name *

□ Default

Device Group: -- ALL --

Figure 2-10 Create Filter

4. Give your new filter a name.

5. To designate the new view as your default, check the Default box; otherwise, leave the checkbox blank.

6. Use the Device List drop-down and custom fields to configure the filter to show the data you want to see in one or more Dashboard charts.

NOTE: Populated fields in the Create Filter screen are combined using "and" logic. For example, when you choose a Device Group and provide one or more custom field values, the Dashboard chart to which the filter is applied includes devices that are part of the specified group and match the custom field value(s) provided.

7. Click Save to add the filter to the list; click Cancel to close the Create Filter pop-up without performing any action.

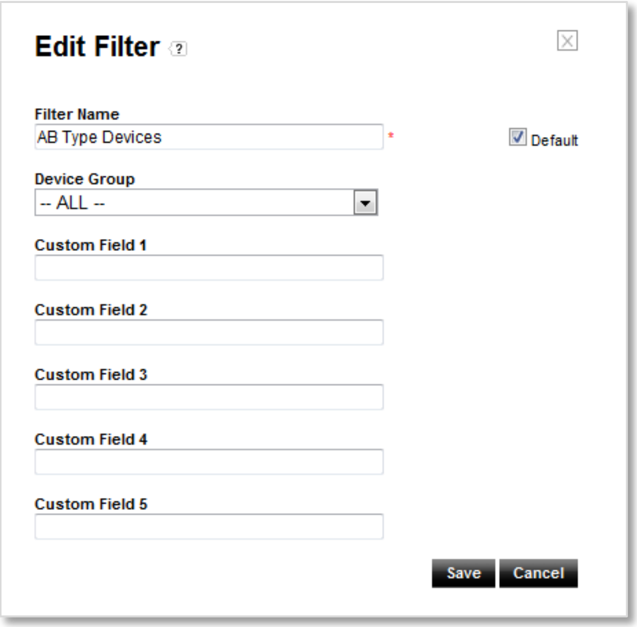
Edit a Filter

NOTE: Your pop-up may look different from the example below if your Customer Administrator assigned labels to one or more custom fields (see Assign Custom Field Labels**).**

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears.

2. Drop down the Account list and select the billing account of the Dashboard for which you want to modify a filter.

3. In the Dashboard Filters area at the bottom of the screen, locate the filter you want to modify and click the Edit link in its row, in the Options column. The Edit Filter pop-up appears.



Edit Filter

Filter Name

AB Type Devices *

☑ Default

Device Group

-- ALL --

Custom Field 1

Custom Field 2

Custom Field 3

Custom Field 4

Custom Field 5

Figure 2-11 Create Filter

4. Modify the filter using the controls and fields on the pop-up.

5. Click Save to save your changes; click Cancel to dismiss the pop-up without changing the filter.

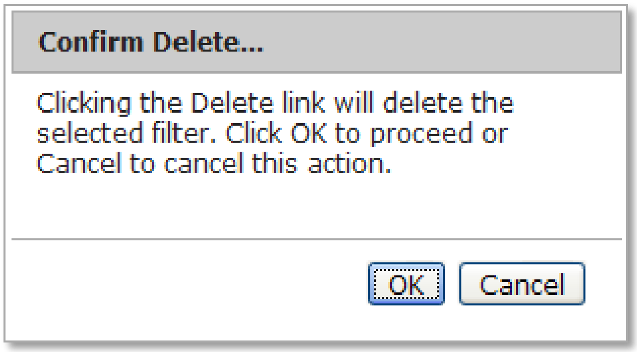
Delete a Filter

NOTE: Your pop-up may look different from the example below if your Customer Administrator assigned labels to one or more custom fields (see Assign Custom Field Labels).

1. Click the Admin tab and select the Dashboard Config sub-menu command. The Dashboard Setup screen appears.

2. Drop down the Account list and select the billing account of the Dashboard for which you want to modify a filter.

3. In the Dashboard Filters area at the bottom of the screen, locate the filter you want to remove and click the Delete link in its row, in the Options column. A confirmation dialog appears.



Confirm Delete...

Clicking the Delete link will delete the selected filter. Click OK to proceed or Cancel to cancel this action.

Figure 2-12 Confirm Delete confirmation for filter

4. Click OK to delete the filter from all lists; click Cancel to dismiss the dialog and retain the filter.

Apply a Filter

When you have established filters for the Dashboard using the Dashboard Setup screen, you can apply them to one or more charts displayed in the Dashboard. Applying a filter to a Dashboard chart allows you to target a specific device group, see only devices that share certain custom attributes, or combine these fields to display only data that makes sense for performing your job or monitoring your M2M business.

NOTE:

- **Filters can be applied to all Dashboard charts except Device Alarm Status.**
- **Dashboard filters are created at the contact (system user) level; therefore, the filters you create will be listed on the Dashboards of all accounts to which you have access. To apply filters correctly, be sure your Account selection is compatible with the device group selected in a selected filter.**
- **When you choose a filter that specifies a device group, be sure to choose the group's corresponding Account (or All accounts) in the Dashboard to properly populate the chart(s) to which the filter is applied with device data.**
- **You can designate one of your filters to be the default for charts on the Dashboard. A system default, called "System Default", is provided initially for Dashboard charts. Only the user with Customer Admin privileges is permitted to edit the system default filter; however, its name cannot be modified.**
- **The filter designated as the default is always selected the first time you access the Dashboard during an M2M Management Center session until you change it. When you change the selected filter for any chart, your selection remains until you change it again, even when you navigate away from the Dashboard and return to it later.**

To apply a filter to a Dashboard chart, drop down the Filter list control above the report and make a selection. The Dashboard chart changes automatically.

Add/Remove Display Features

Legends and callouts help to describe information included in a Dashboard. Both features apply to all charts shown in a Dashboard. Use the instructions below to add or remove these display features to a Dashboard; the figures below show how these features affect a Dashboard display.

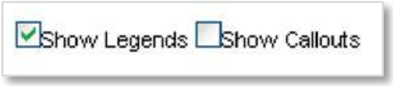
Add/Remove Legends

Legends are on-screen guides to the color-coded information shown in Dashboard charts. They provide definitions for each color used in Dashboard charts.

To add or remove legends:

1. Click the Dashboard tab. The Dashboard of the currently selected account appears. Change to another account's Dashboard by dropping down the Account list and making another selection.

2. At the bottom of the screen, check Show Legends to turn legends on; uncheck it to turn legends off:



☑Show Legends □Show Callouts

Figure 2-13 Show Legends option (with Legends turned on)

The following examples show the effects of the Show Legends feature:

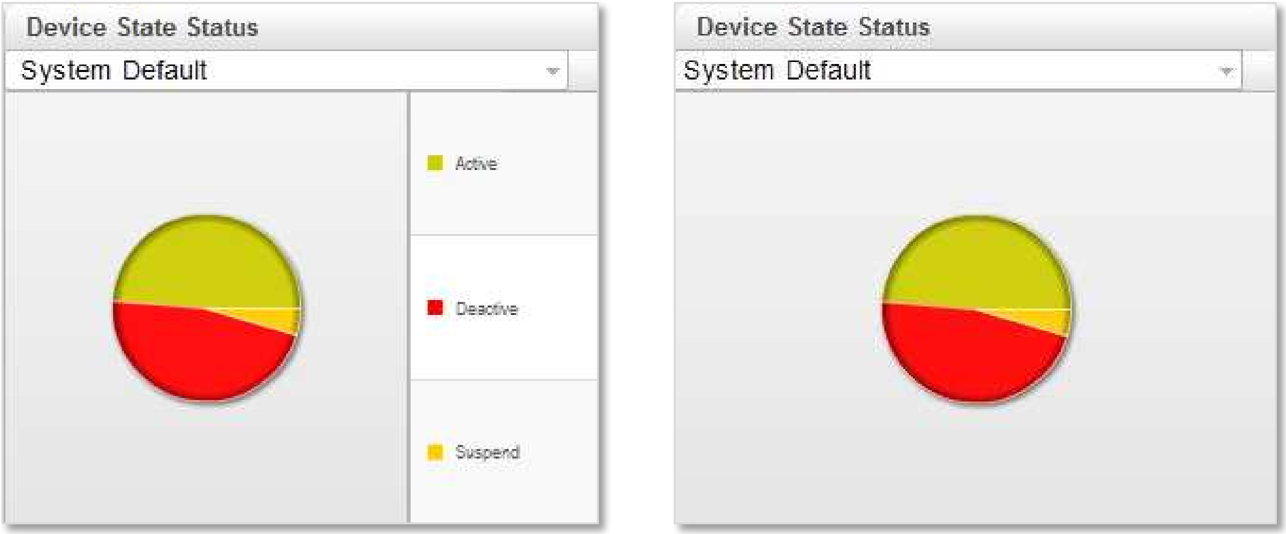


Figure 2-14 Pie chart with legends (left) and without legends (right)

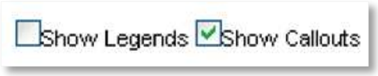
Add/Remove Callouts

Callouts are text-based descriptions for information shown in Dashboard charts.

To add or remove callouts:

1. Click the Dashboard tab. The Dashboard of the currently selected account appears. Change to another account's Dashboard by dropping down the Account list and making another selection.

2. Check Show Callouts to turn callouts on; uncheck it to turn callouts off:



□ Show Legends ☑ Show Callouts

Figure 2-15 Show Callouts option (with Callouts turned on)

The following examples show the effects of the Show Callouts feature:

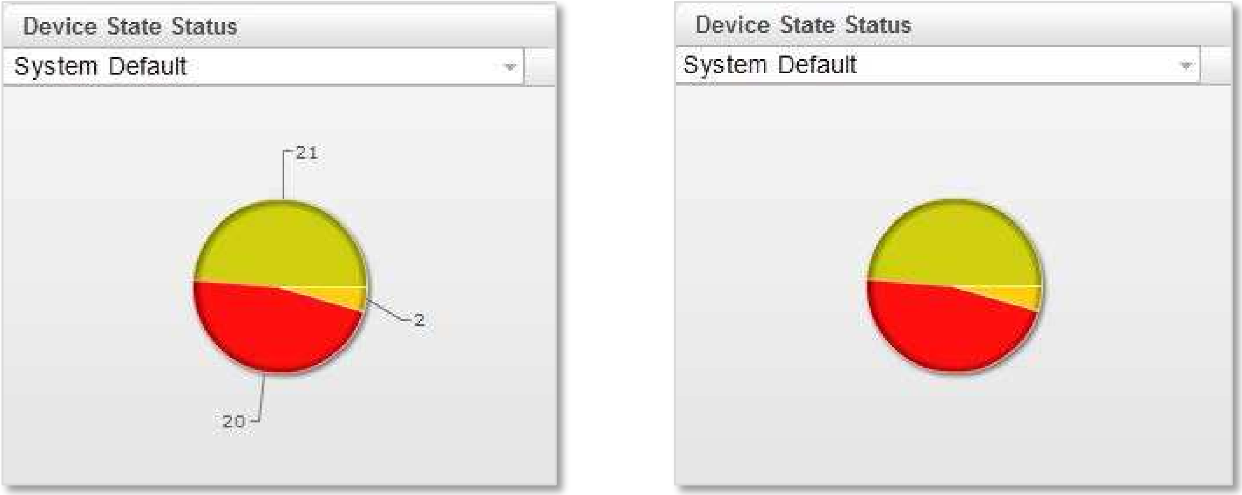


Figure 2-16 Pie chart with callouts (left) and without callouts (right)

2.3.2 Customize the Device List, Reports and Data Usage Trending Chart Screens

The Device List, reports and Data Usage Trending Chart screens include controls to change the displayed view, edit an existing view and create a new view. You can create as many personalized views as you need. In addition, you can designate one of your views to be the default for a screen. A view called "System Default" is provided initially for the Device List, all device reports and Data Usage Trending Chart screens. Only the user with the Customer Admin role is permitted to edit the System Default view; however, its name cannot be modified.

The view designated as the default is always selected the first time you access the Device List, a device report or the Data Usage Trending Chart screen during an M2M Management Center session until you change it. When you change the selected view in any screen, your selection remains until you change it again, even when you navigate away from the screen and return to it later.

Change the View on a Screen

NOTE:

- **Every view drop-down list includes a Default View section, which lists the view designated as the default. The view that is designated as the default is initially selected the first time you navigate to the Device List, a report or the Data Usage Trending Chart screen. It remains selected until you change to another view.**
- **Every screen of the M2M Management Center includes a view named "System Default". System Default is the designated default view until you select another view as your default. The name "System Default" cannot be changed; however, a user with Customer Admin privileges can edit the content and column order of the System Default view.**

The Device List, device reports and Data Usage Trending Chart screens include a drop-down list of available views. To change the view of a screen, drop down the list of views and select one. The displayed view automatically changes upon your selection.

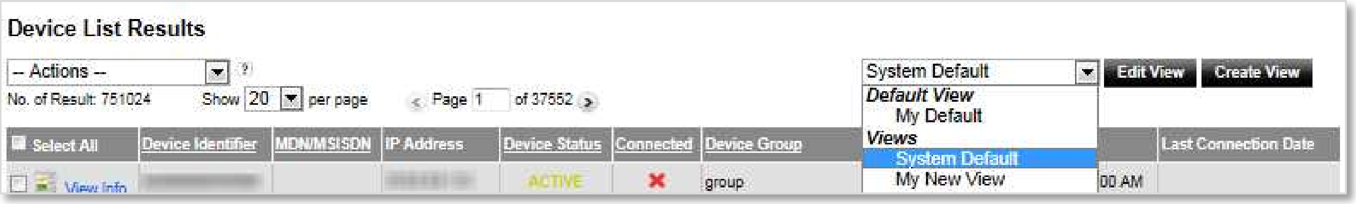


Figure 2-17 View drop-down on Device List

Edit or Delete a View

Editing includes changing and deleting a view. Both of these actions can be done from the same pop-up.

NOTE:

- **Only users with the Customer Admin role can select the system view named "System Default" for editing.**
- **The system view named "System Default" cannot be deleted.**
- **The Edit/Delete View pop-up corresponding to the Data Usage Trending Chart has different controls and fields than the pop-ups for the Device List and reports. An example is shown below and step-by-step instructions are included in the following process.**

Related Information

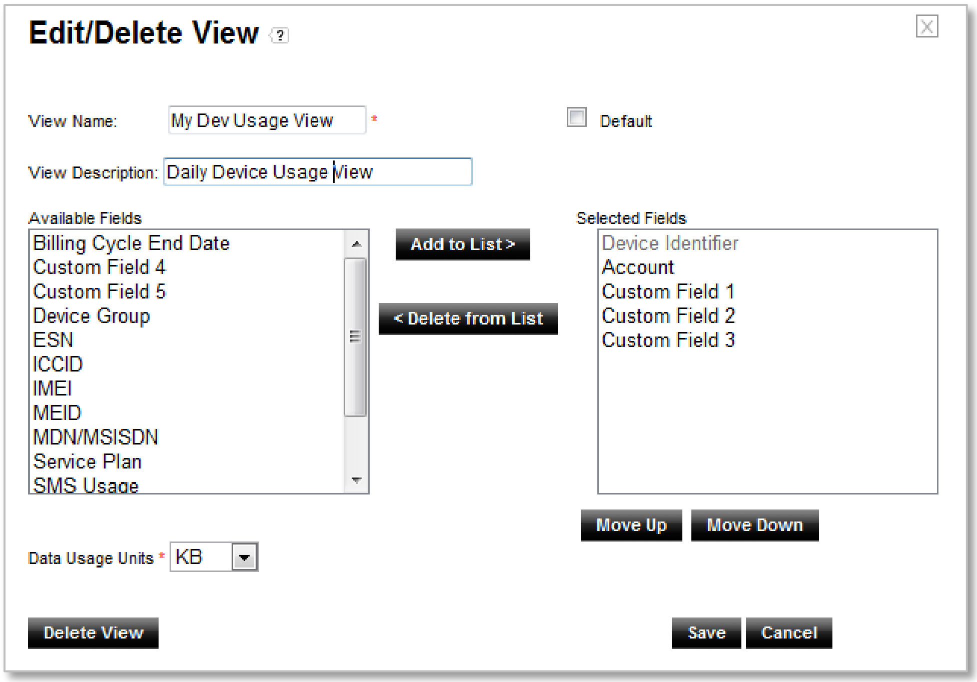
[View Properties]

To edit or delete a view:

1. Display the Device List by clicking its tab on the Navigation menu; display a device report screen by clicking the Device Reports tab and selecting a report from the sub-menu or landing page; display the Data Usage Trending Chart screen by clicking the Graphical Analysis tab and selecting Data Usage Trending Chart from the sub-menu.

2. Drop down the list of views on the screen and select the view you want to edit or delete.

3. Click the Edit View button, which appears next to the view drop-down control. The Edit/Delete View pop-up appears. To edit the view, proceed to the next step; to delete the view, go to Step 8.


Edit/Delete View

View Name: My Dev Usage View *

□ Default

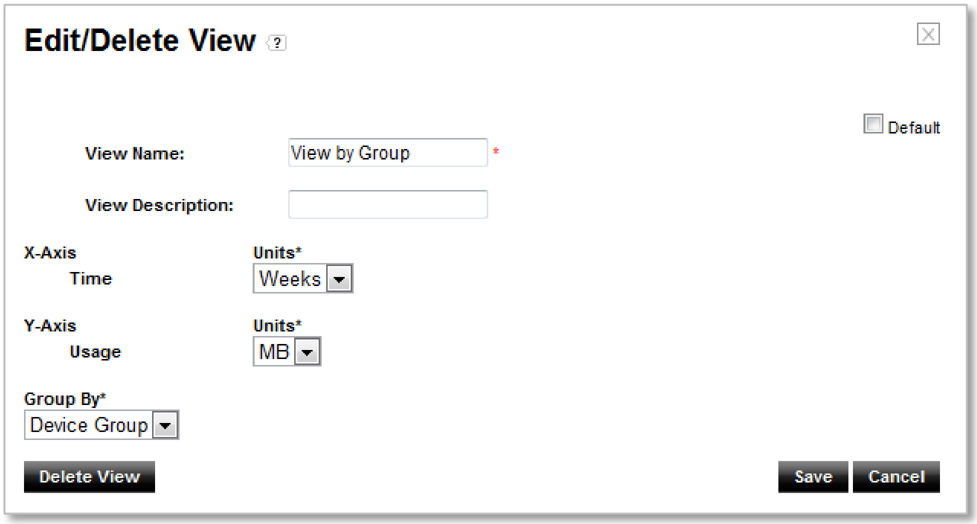
View Description: Daily Device Usage View

Available Fields:
Billing Cycle End Date
Custom Field 4
Custom Field 5
Device Group
ESN
ICCID
IMEI
MEID
MDN/MSISDN
Service Plan
SMS Usage

Selected Fields:
Device Identifier
Account
Custom Field 1
Custom Field 2
Custom Field 3

Data Usage Units * KB

Figure 2-18 Edit/Delete View pop-up for Device List and reports (example is for Device Usage Report; note that the Data Usage Units control is shown on certain Edit/Delete View screens only)


Edit/Delete View

□ Default

View Name: View by Group *

View Description:

X-Axis Time — Units* Weeks

Y-Axis Usage — Units* MB

Group By* Device Group

Figure 2-19 Edit/Delete View pop-up for Data Usage Trending Chart

4. Rename the view, if needed; describe the view; or designate it as your default. For views of the Device List or a device report, go to Step 5; for views of the Data Usage Trending Chart, go to Step 6.

5. Manipulate the data in the view using the list box controls to add/delete columns from the view's list. Reorder the columns by moving them up or down, or change the Usage Units, when applicable. Go to Step 7.

6. Specify new Units for the X-Axis and Y-Axis, when necessary, or drop down the Group By list and select a new grouping strategy for the view.

7. Click Save to modify the view with your changes or click Cancel to close the pop-up without changing the view. Your edits are complete.

8. Click the Delete View button. A confirmation message reading "Clicking the Delete button will delete this existing view. Click OK to proceed or Cancel to cancel this action" appears.

9. Click OK to remove the view from the view drop-down list; click Cancel to close the message and Edit/Delete View pop-ups without performing any action.

Create a View

Related Information

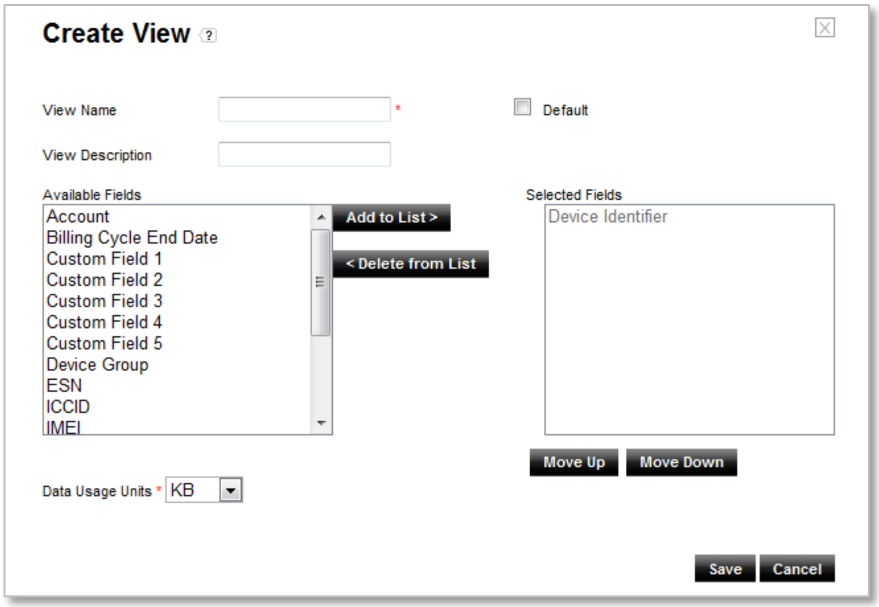
View Properties

NOTE: The Create View pop-up corresponding to the Data Usage Trending Chart has different controls and fields than the pop-ups for the Device List and reports. An example is shown below and step-by-step instructions are included in the following process.

To create a new view for the Device List, a device report or the Data Usage Trending Chart:

1. Display the Device List by clicking its tab on the Navigation menu; display a device report screen by clicking the Device Reports tab and selecting a report from the sub-menu or landing page; display the Data Usage Trending Chart screen by clicking the Graphical Analysis tab and selecting Data Usage Trending Chart from the sub-menu.

2. Click the Create View button. The Create View pop-up appears.



Create View

View Name *

□ Default

View Description

Available Fields

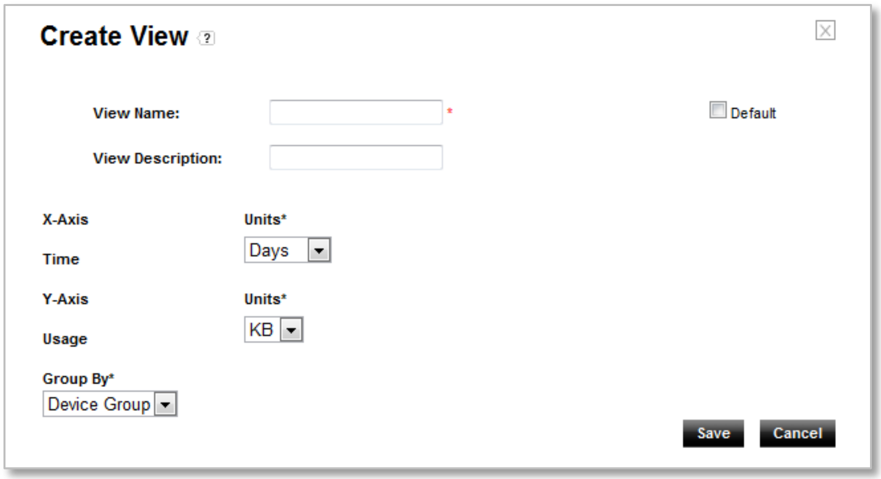
Account
Billing Cycle End Date
Custom Field 1
Custom Field 2
Custom Field 3
Custom Field 4
Custom Field 5
Device Group
ESN
ICCID
IMEI

Selected Fields

Device Identifier

Data Usage Units * KB

Figure 2-20 Create View pop-up for Device List and reports (example is for Device Usage Report; note that Data Usage Units control shown on select Create View screens only)



Create View

View Name: *

View Description:

□ Default

X-Axis Time — Units*: Days

Y-Axis Usage — Units*: KB

Group By*: Device Group

Figure 2-21 Create View pop-up for Data Usage Trending Chart

3. Give your new view a name and an optional description.

4. To designate the new view as your default, check the Default box; otherwise, leave the checkbox blank.

5. To create a view for the Device List or a device report, continue to Step 6. To create a view for the Data Usage Trending Chart, go to Step 8.

6. Use the list boxes and Add to List/Delete from List buttons to add and remove columns from your view; use the Move Up/Move Down buttons to set the order of the columns in your display. For a view of the Device List or a report that does not show usage, continue to Step 9; for a usage-driven report view, go to the next step.

7. Change the Usage Units for the report view, if necessary. Go to Step 9.

8. Use the drop-down controls to select Units for both the X-Axis and Y-Axis. Drop down the Group By list and choose to display data by Device Group or to aggregate usage data for All devices associated with the selected billing account.

9. Click Save to add the view to the drop-down list of views for the screen; click Cancel to close the Create View pop-up without performing any action.

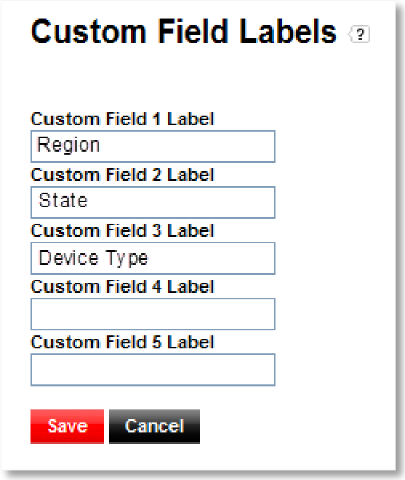
2.3.3 Assign Custom Field Labels

NOTE: This function is available only to users with the Customer Admin role.

Use this feature to guide the users in your organization to employ custom fields in a standard manner. When you assign labels to custom fields, your users will know where to supply information your organization wants to track for a device. For example, when you change the label of Custom Field 1 to “Location”, a user knows to enter a device’s location in that field.

Assign Labels to Custom Fields

1. Go to the Admin tab and select Custom Field Labels from the sub-menu. The Custom Field Labels screen appears.



Custom Field Labels

Custom Field 1 Label: Region

Custom Field 2 Label: State

Custom Field 3 Label: Device Type

Custom Field 4 Label:

Custom Field 5 Label:

Figure 2-22 Custom Field Labels screen

2. Enter labels for as many custom fields as you want to define. Remember that the labels will appear throughout the M2M Management Center for all users in the selected organization.

3. Click Save to assign the label(s) to the custom field(s); click Cancel to close the Custom Field Labels screen without making any changes.

2.3.4 Set Device Identifier Display Preferences

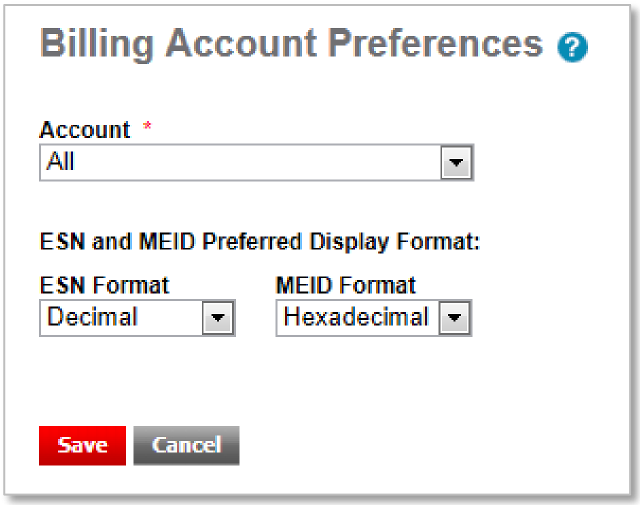
NOTE:

- **This function is available only to users with the Customer Admin role.**
- **Display preferences apply to types ESN and MEID only, which are primarily used to identify Verizon 2G/3G devices. 4G devices may also be identified by MEID.**
- **ESN/MEID identifier preferences apply to displayed format only. Device identifier entry fields in the M2M Management Center (including Device Identifier, ESN, and MEID fields) are not affected by these settings.**

Set Device Identifier Display Format

To set the preferred display format for 2G and 3G device identifiers:

1. Navigate to Admin > Account Preferences. The Billing Account Preferences screen appears:



Billing Account Preferences

Account *

All

ESN and MEID Preferred Display Format:

ESN Format: Decimal

MEID Format: Hexadecimal

Figure 2-23 Billing Account Preferences screen

2. Either accept All to set preferences for all billing accounts that comprise your organization or drop down the Account list and select the specific billing account for which you want to set preferences. Your settings will affect all users of the selected billing account.
3. Set the preferred display format for either or both ESN and MEID identifiers. The M2M Management Center will display these identifiers in the preferred format wherever they appear.

2.4 Manage Devices

Device management tasks include:

- Find Devices by Filtering
- Select from Device List
- Display Device Details
- Print the Device List
- Export Device Data
- Group Devices
- Upload Attributes for Devices by File
- Upload Attributes for Devices by Screen Entry

Other related device tasks include changing the state of a device. These tasks are found in Perform Device-related Actions.

Find Devices by Filtering

Related Information

Device List Properties

NOTE:

Improvements have been made to display Device Lists in the M2M Management Center. As a result, when you first enter the Device List screen, it displays all devices in the selected account as an unsorted list.

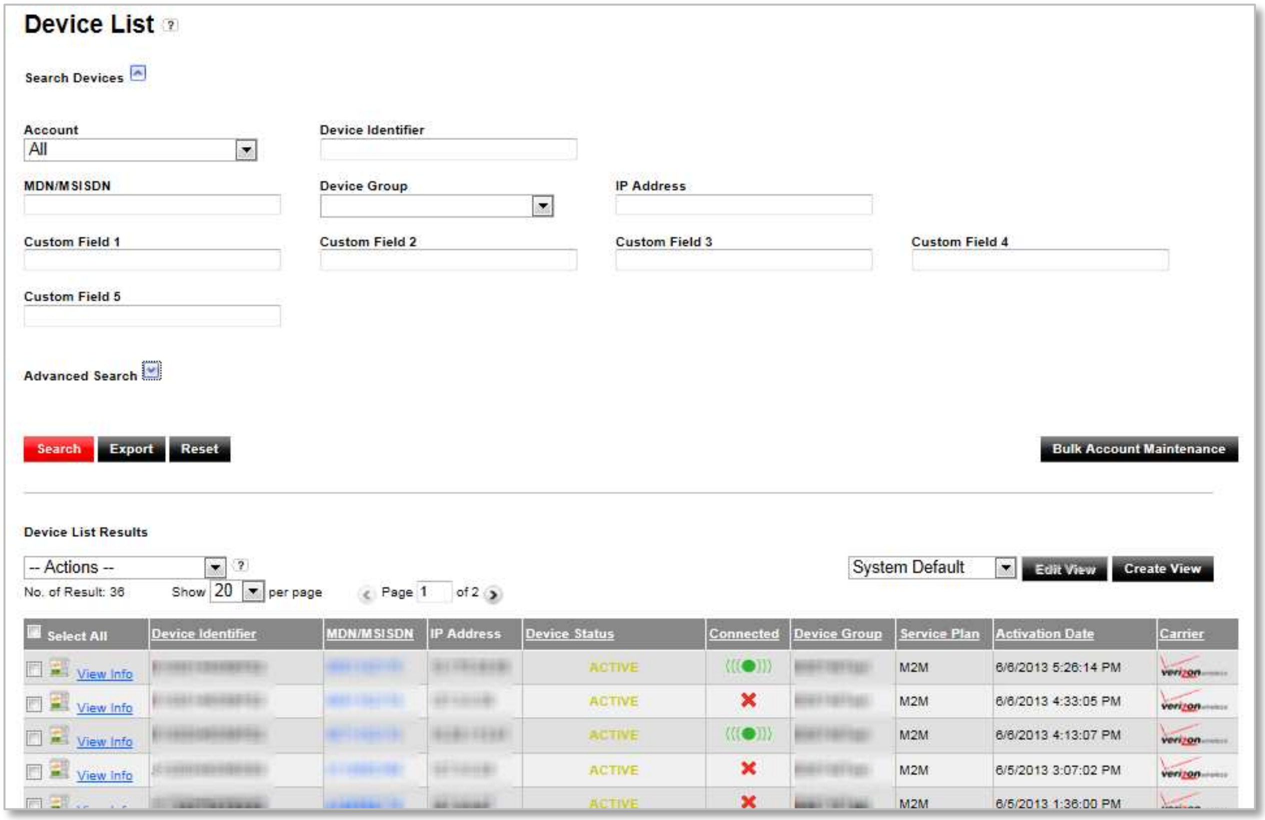
In addition, we suggest using the following tips when working with lengthy Device Lists:

- **Limit sorting and/or filtering to the following columns:**

- **Account**
- **Device Identifier**
- **MDN/MSISDN**
- **Custom Fields**
- **MEID, ESN, IMEI, or ICCID**
- **Device Status**
- **Activation Date (filter using a range composed of Start and End Dates)**
- **Activated By**
- **Connection Status**

To use the search function to find specific devices:

1. From the Navigation menu, click Device List. The Device List screen appears, populated with all devices:



Device List ?

Search Devices

Account: All

Device Identifier:

MDN/MSISDN:

Device Group:

IP Address:

Custom Field 1:

Custom Field 2:

Custom Field 3:

Custom Field 4:

Custom Field 5:

Advanced Search

Device List Results

-- Actions -- ?

System Default

No. of Result: 36 Show 20 per page Page 1 of 2

☐ Select All	Device Identifier	MDN/MSISDN	IP Address	Device Status	Connected	Device Group	Service Plan	Activation Date	Carrier
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	((●))	[redacted]	M2M	6/6/2013 5:26:14 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/6/2013 4:33:05 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	((●))	[redacted]	M2M	6/6/2013 4:13:07 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/5/2013 3:07:02 PM	verizon
☐	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/5/2013 1:36:00 PM	

Figure 2-24 Device List

2. Enter values into one or more of the device search fields found at the top of the Device List screen. If you need additional criteria, expand the search area to show Advanced Search fields. The more fields you populate, the more targeted your search.

3. Click Search. The Device List is filtered to show only devices that match your search criteria.

Select from Device List

The checkbox that appears at the left of every device row and the Select All checkbox in the Device List are used to select one or more devices from the list on which to perform various actions.

Clicking the Select All checkbox selects all rows in the current page of the Device List. Alternatively, you can select individual rows by clicking in the checkbox that appears at the left of every row in the Device List.

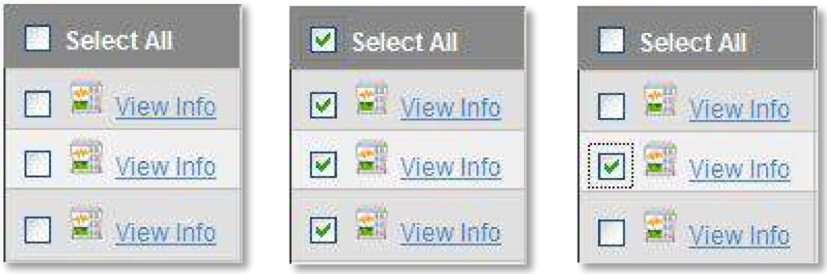


Figure 2-25 Selecting devices in the Device List with the Select All checkbox and individual checkboxes

Display Device Details

Related Information

Device List Properties

Device Information Pop-Up Properties

NOTE: The M2M Management Center displays one of the following views of the Device Information pop-up depending on certain characteristics of the device:

- **Basic view – Device has no active promotions and is not part of a partner program. Only pertinent, basic information about the device appears.**
- **Promotions view – Device has one or more active promotions applied to it. You will see the Basic view, plus promotion information.**
- **Partner view – Device was activated under an organization that is designated as a Verizon Partner. You will see the Basic view plus partner fields.**

To see detailed information for a device:

1. From the Navigation menu, click Device List. The Device List screen appears.

2. In the Device List screen, specify criteria for the device you want to view.

3. Click Search. The Device List appears, filtered to include only devices that match your criteria.

4. From the list, locate the row of the device for which you want to display more information and click the View Info link for the device, as shown below:

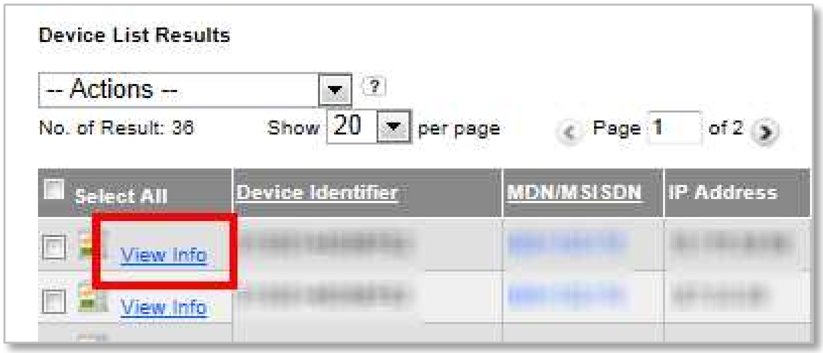
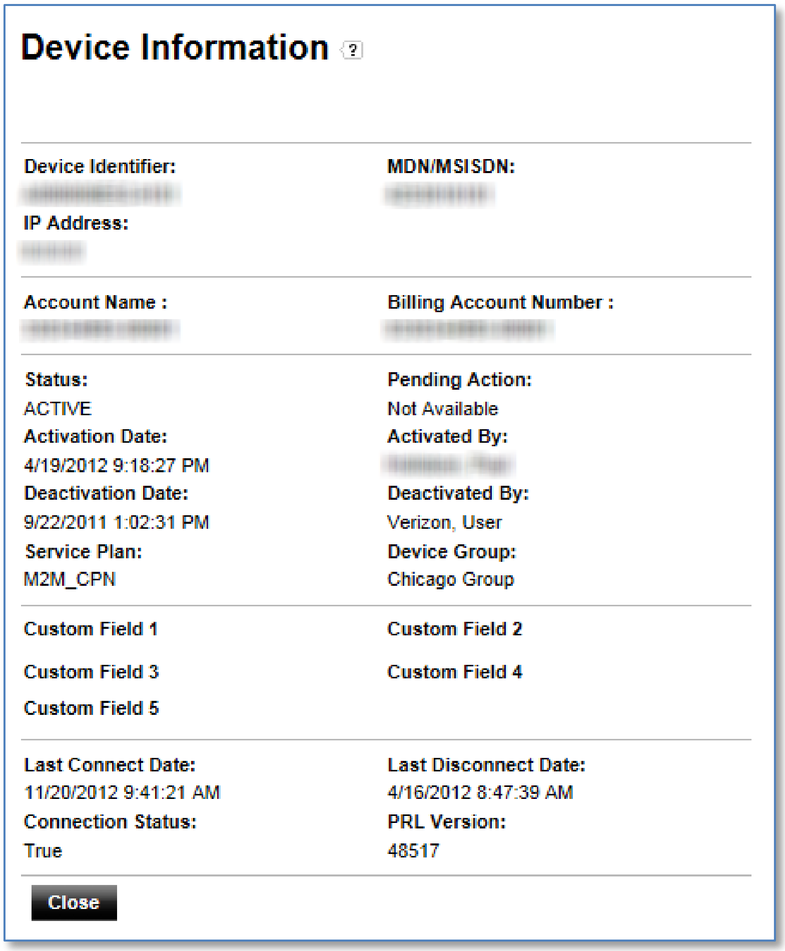


Figure 2-26 View Info link in Device List

One of the pop-up windows described above appears. The basic view is shown below:



Device Information

Device Identifier: [redacted]	**MDN/MSISDN:** [redacted]
IP Address: [redacted]	
Account Name : [redacted]	**Billing Account Number :** [redacted]
Status: ACTIVE	**Pending Action:** Not Available
Activation Date: 4/19/2012 9:18:27 PM	**Activated By:** [redacted]
Deactivation Date: 9/22/2011 1:02:31 PM	**Deactivated By:** Verizon, User
Service Plan: M2M_CPN	**Device Group:** Chicago Group
Custom Field 1	**Custom Field 2**
Custom Field 3	**Custom Field 4**
Custom Field 5	
Last Connect Date: 11/20/2012 9:41:21 AM	**Last Disconnect Date:** 4/16/2012 8:47:39 AM
Connection Status: True	**PRL Version:** 48517

Figure 2-27 Basic Device Information pop-up view

5. Click Close to dismiss the Device Information pop-up.

Display Diagnostic Information for a Device

NOTE:

- **This function applies only to customers with the Device Diagnostics feature.**
- **Devices display different diagnostic data depending on their capabilities (for more information, go to M2MDeveloper.Verizon.com). Minimally, this screen will show data regarding the selected device's current session and last completed session (applies to Not Enabled devices); for Enabled Advanced M2M devices, this screen will show the connected session information plus a more extensive set of diagnostic attributes.**

Related Information

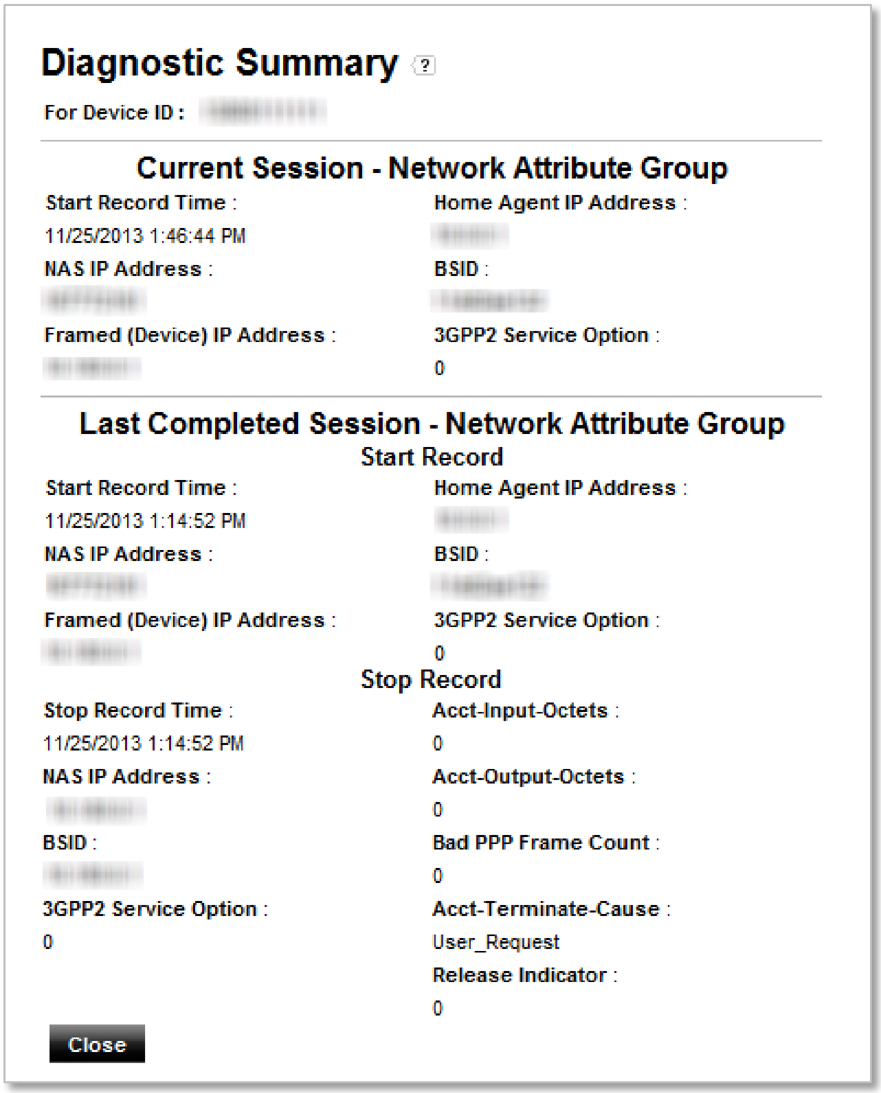
Diagnostic Summary Data

To see diagnostic data for a device:

1. From the Navigation menu, click Device List. The Device List screen appears.
2. In the Device List screen, specify criteria for the device you want to view.

3. Click Search. The Device List appears, filtered to include only devices that match your criteria.

4. From the list, select the device for which you want to display diagnostic information, drop down the Actions menu and choose Diagnostic Summary. A screen similar to the following appears:



Diagnostic Summary

For Device ID : [redacted]

Current Session - Network Attribute Group

Start Record Time : 11/25/2013 1:46:44 PM

Home Agent IP Address : [redacted]

NAS IP Address : [redacted]

BSID : [redacted]

Framed (Device) IP Address : [redacted]

3GPP2 Service Option : 0

Last Completed Session - Network Attribute Group

Start Record

Start Record Time : 11/25/2013 1:14:52 PM

Home Agent IP Address : [redacted]

NAS IP Address : [redacted]

BSID : [redacted]

Framed (Device) IP Address : [redacted]

3GPP2 Service Option : 0

Stop Record

Stop Record Time : 11/25/2013 1:14:52 PM

Acct-Input-Octets : 0

NAS IP Address : [redacted]

Acct-Output-Octets : 0

BSID : [redacted]

Bad PPP Frame Count : 0

3GPP2 Service Option : 0

Acct-Terminate-Cause : User_Request

Release Indicator : 0

Figure 2-28 Diagnostic Summary pop-up

Export Device Data

Related Information

Device List Properties

Retrieving Files from the Download Center

You can export a Device List and retrieve it from the Download Center when you receive an email indicating the report is ready. The M2M Platform generates export files in comma-separated value (CSV) format, which you can open in many types of applications such as spreadsheets, or use for other application-specific purposes. An exported Device List includes the data as you see it displayed in the M2M Management Center.

NOTE:

- **The source for data in exported lists and reports is a reporting database, which differs from the primary database used for displaying data in the M2M Management Center user interface. Thus, exported data may be a few hours older than what you see in the M2M Management Center.**
- **You can export up to ten (10) reports per day.**

1. From the Navigation menu, click Device List. The Device List screen appears.
2. To export data for the devices included in the Device List as it appears when you first display it, go to Step 5. To export specific devices, go to Step 3.
3. Use the criteria fields at the top of the Device List screen to perform a device search.
4. Click Search. A filtered version of the Device List appears at the bottom of the screen.
5. Click Export, as shown below:

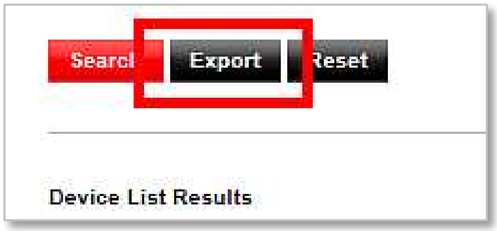
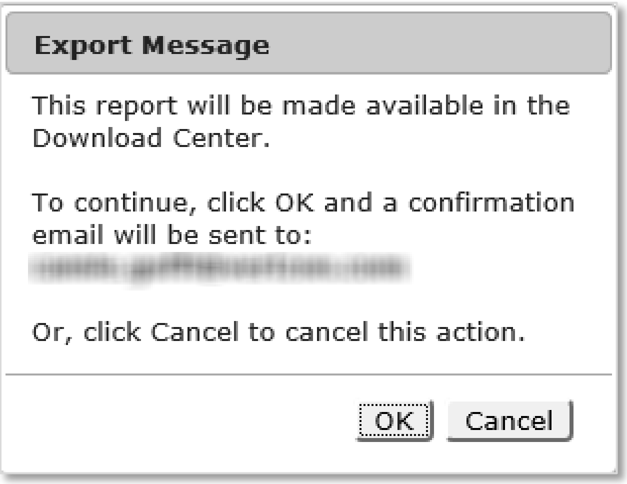


Figure 2-29 Export Device List

6. The following dialog appears for you to confirm or dismiss the export action:



Export Message

This report will be made available in the Download Center.

To continue, click OK and a confirmation email will be sent to: [redacted]

Or, click Cancel to cancel this action.

Figure 2-30 Confirm export

7. Click OK to generate the file, or click Cancel to dismiss the confirmation dialog and return to the Device List. When you generate an export file, the system sends you two emails: one to confirm your request and a second to inform you of the outcome.

2.4.1 Group Devices

You group devices for two purposes:

- To perform actions on all devices in the group
- To aggregate data for the group on which to trigger alarm notifications

You can group devices from either the Device List or by using the Device Group command on the Admin sub-menu. This section describes both methods of forming a device group.

In addition to creating device groups, you can also edit and delete them. These functions are only available from the Device Group command on the Admin sub-menu.

NOTE:

- **The M2M Management Center allows you to perform tasks for multiple devices in the Device List. When you regularly perform tasks for the same devices, consider grouping these devices.**
- **Device groups can contain an unlimited number of devices.**
- **All devices you are grouping must be associated with the same Billing Account.**
- **Devices can belong to only one group at a time. The Default group is automatically created when your system is initialized; originally, it contains all devices.**
- **You can group 2G, 3G, and 4G devices together; however, certain actions such as wakeup and PRL update are not allowed for 4G devices. Because of this restriction, you may want to consider grouping devices by connection type.**

Create a Device Group from the Device List

1. From the Navigation menu, click Device List. The Device List screen appears.
2. Use the criteria fields at the top of the Device List screen to specify the devices you want to group. If you need additional criteria, expand the search area to show Advanced Search fields.
3. Click Search. The Device List appears, filtered to show the devices that match your criteria.
4. Locate the rows of the devices that you want to group and check each device's checkbox in the left-most column.
5. Drop down the Actions menu found at the top left of the Device List and select Assign to Device Group:

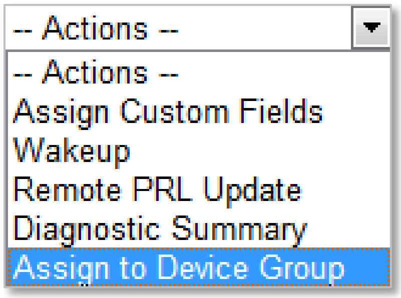
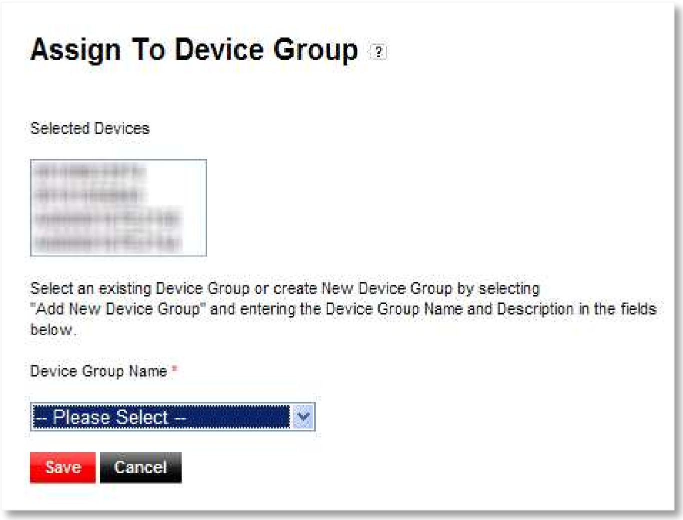


Figure 2-31 Assign to Device Group on Actions menu

The Assign To Device Group pop-up appears, listing your selected devices.



Assign To Device Group

Selected Devices

[redacted]

Select an existing Device Group or create New Device Group by selecting "Add New Device Group" and entering the Device Group Name and Description in the fields below.

Device Group Name *

Figure 2-32 Assign To Device Group pop-up

6. Drop down the Device Group Name list and either select the existing group to which you want to add the selected devices or choose Add New Device Group to create a new group containing the selected devices. If you are assigning devices to an existing group, go to Step 8; if you are creating a new group, proceed to the next step.

7. Supply a Device Group Name and an optional Device Group Description for the new group.

8. Click Save to save your changes; click Cancel to dismiss the Assign To Device Group pop-up without making changes. A message appears to warn you that some devices may be removed from their present device group to become part of this new device group.

9. Click OK to make the proposed device group changes or click Cancel to dismiss the message window and return to the Device List.

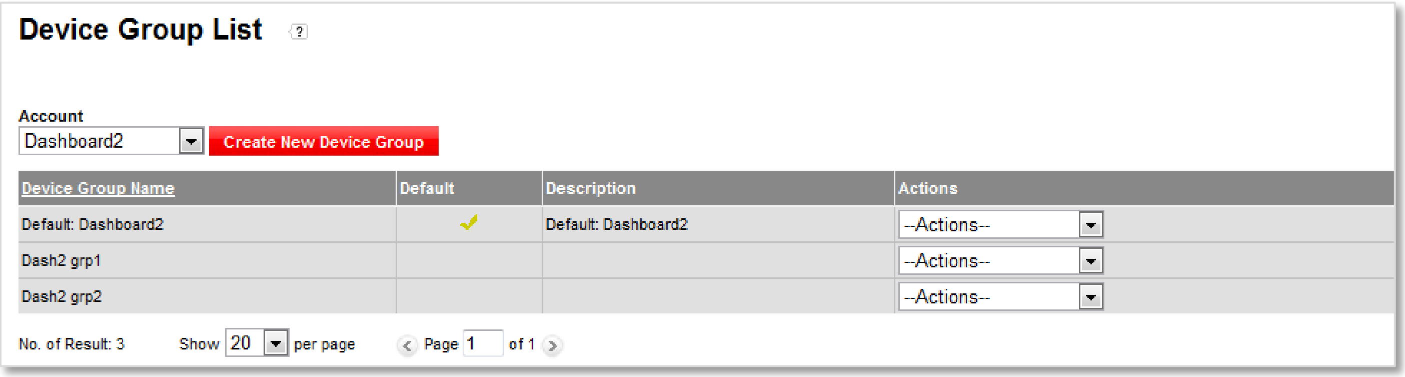
Create a Device Group from the Admin Tab

Related Information

Device Group Properties

To create a device group:

1. From the Navigation menu, click Admin and choose the Device Group sub-menu. The Device Group List screen appears:



Device Group List

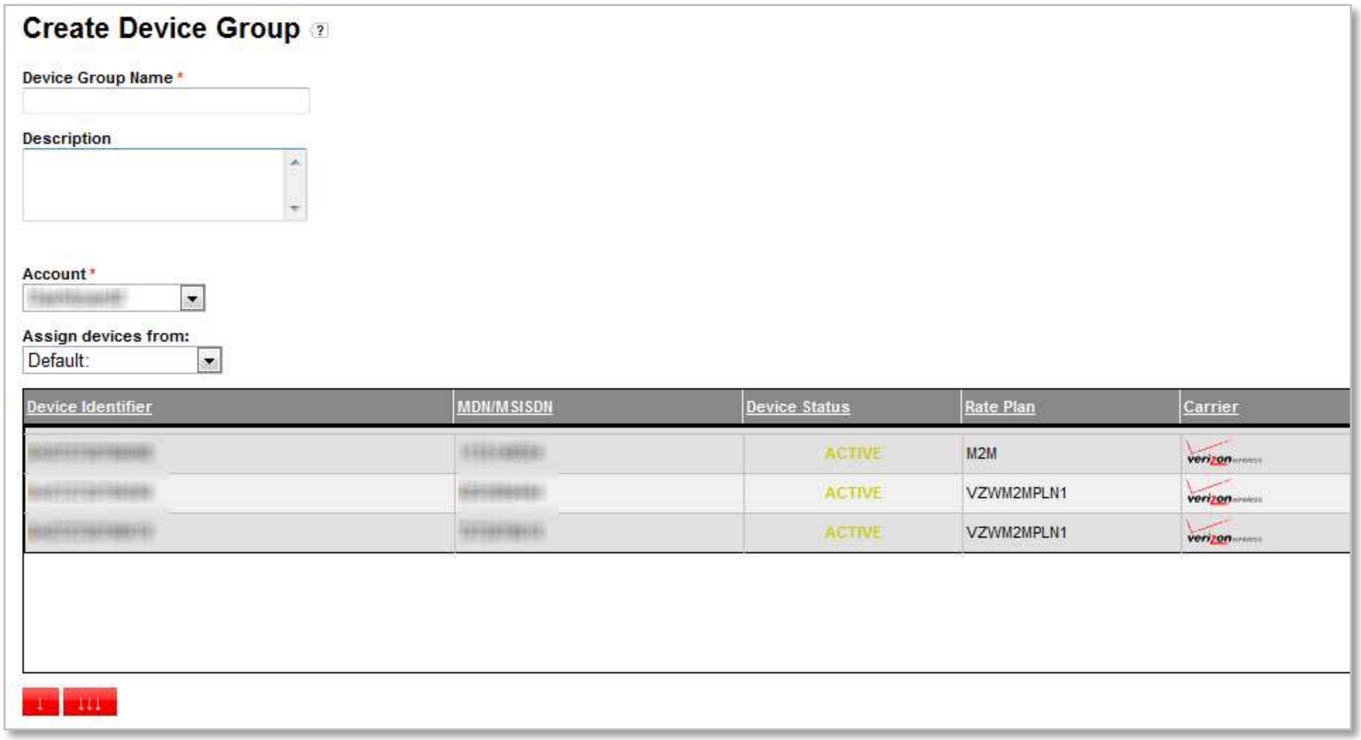
Account: Dashboard2

Device Group Name	Default	Description	Actions
Default: Dashboard2	✓	Default: Dashboard2	--Actions--
Dash2 grp1			--Actions--
Dash2 grp2			--Actions--

No. of Result: 3 Show 20 per page Page 1 of 1

Figure 2-33 Device Group List

2. Click Create New Device Group. The Create Device Group screen appears:



Create Device Group ?

Device Group Name *

Description

Account * [redacted]

Assign devices from: Default:

Device Identifier	MDN/MSISDN	Device Status	Rate Plan	Carrier
[redacted]	[redacted]	ACTIVE	M2M	verizon wireless
[redacted]	[redacted]	ACTIVE	VZWM2MPLN1	verizon wireless
[redacted]	[redacted]	ACTIVE	VZWM2MPLN1	verizon wireless

Figure 2-34 Create Device Group screen

3. Enter the general properties of the device group.

4. Drop down the Account list and choose the billing account of the devices you want to group.

5. Drop down the Assign devices from list and select a group from which to choose devices for the group in the bottom portion of the screen. Devices can only belong to one group at a time. The Default group is automatically created when you initialize your system; originally, it contains all devices.

6. To add all devices in the selected group to the group in the bottom portion of the screen, go directly to Step 7. To choose specific devices for the group represented in the bottom portion of the screen, select the devices from the top list using standard selection techniques (Ctrl+Click to select discretely; Shift+Click to select contiguously).

7. Use one of the following software controls to move devices between the group you have selected in the top table and the group in the Assigned Devices list at the bottom:

Software Control	Click to...
↓ (Down Arrow)	Add selected devices to the Assigned Devices list in the bottom portion of the screen. This action removes the devices from the group displayed in the top list.
↓↓↓ (3 Down Arrows)	Add all devices to the Assigned Devices list in the bottom portion of the screen. This action removes the devices from the group displayed in the top list.
Undo	Remove the device from the device group in the bottom portion of the screen and return it to the group in the top portion of the screen. This link is only visible when newly assigned devices have not yet been saved.

8. Click the Create/Save Device Group button to save the device group changes you have made; click Cancel to dismiss your changes and close the Create Device Group screen.

Edit a Device Group from the Admin Tab

Related Information

Device Group Properties

NOTE: The M2M Management Center has one default device group that initially contains all devices. You cannot change the default designation; however, you can change the name of the default device group and its contents change as you move devices in and out of the default group.

To edit a device group's properties or contents:

1. From the Navigation menu, click Admin and choose the Device Group sub-menu. The Device Group List screen appears, with a list of all device groups at the top.

2. Locate the row of the device group you want to modify, drop down the Actions menu and select Edit:

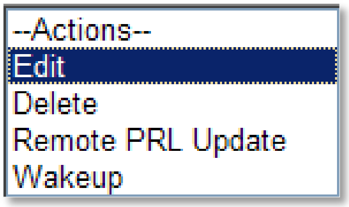


Figure 2-35 Actions menu

The Create Device Group screen appears.

3. Refer to Steps 3-7 of the task Create a Device Group from the Device List for instructions on how to modify the information and devices that compose a device group.

Delete a Device Group from the Admin Tab

NOTE: The M2M Management Center has one default device group that initially contains all devices. You cannot delete the default device group.

To remove a device group from the system:

1. From the Navigation menu, click Admin and choose the Device Group sub-menu. The Device Group List screen appears, with a list of all device groups at the top.

2. Locate the row of the device group you want to delete, drop down the Actions menu and select Delete.

3. A browser-dependent confirmation window appears. Respond appropriately to complete this procedure. All devices in the deleted group will return to the default device group.

Upload Attributes for Devices by File

Related Information

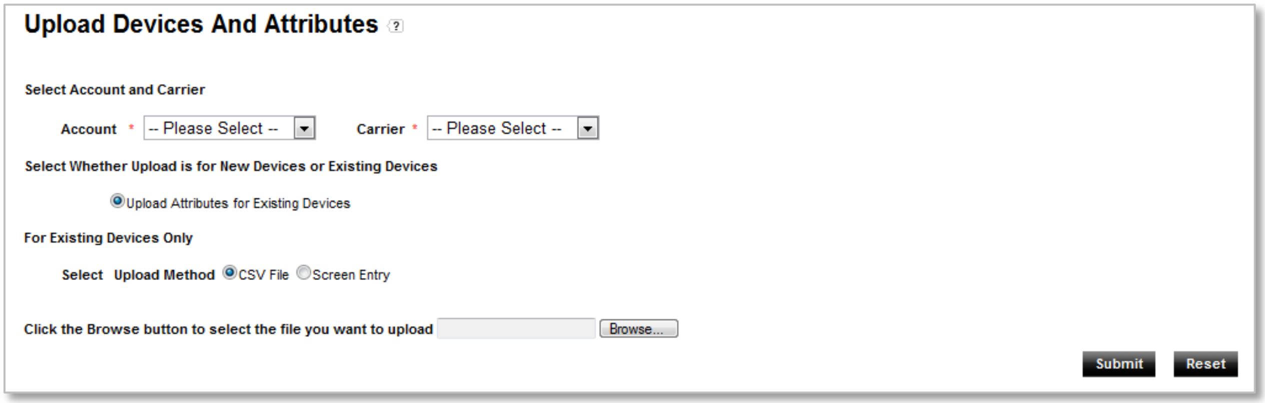
Device Upload File Format

NOTE:

- **This function is reserved for users with the Customer Admin role.**
- **To prepare an upload file, first refer to** [Device Upload File Format]**, which documents the file format requirements and includes recommendations for creating and using upload files.**
- **For file uploads, when you leave the Device Group or any Custom Field blank for a device, the device's current Device Group assignment or Custom Field value will be deleted. To retain a device's current information, be sure to include it in the upload file. Using the recommended best practice in** [Device Upload File Format] **will help you avoid this situation.**

To upload a file with data for up to 1000 existing devices:

1. Go to the Admin tab and select Upload Devices from the sub-menu.



Upload Devices And Attributes

Select Account and Carrier

Account * -- Please Select -- Carrier * -- Please Select --

Select Whether Upload is for New Devices or Existing Devices

● Upload Attributes for Existing Devices

For Existing Devices Only

Select Upload Method ● CSV File ○ Screen Entry

Click the Browse button to select the file you want to upload

Figure 2-36 Upload Devices and Attributes screen— File Upload

2. Use the drop-down controls at the top of the screen to select the Account and Carrier associated with the devices you are updating.

3. Specify that you are updating devices by CSV File.

4. Click Browse, navigate to the file you have prepared with device data, select the file and click Open.

5. Click Submit to begin the upload process. The following warning message appears to inform you about blank values overwriting a device's current information:

   Any existing device group and custom field values will be over-written with a blank value if the field value you are uploading here is blank. To maintain existing values, please ensure that they are included in this upload file/screen grid.

6. Click OK to continue, or click Cancel to dismiss the warning window without updating any devices.

Upload Attributes for Devices by Screen Entry

Related Information

[Fields for Device Screen Entry]

NOTE:

- **This function is reserved for users with the Customer Admin role.**

- **When manually uploading device data, when you when you leave the Device Group or any Custom Field blank for a device, the device's current Device Group assignment or Custom Field value will be deleted. To retain a device's current information, be sure to include it in the screen entry grid.**

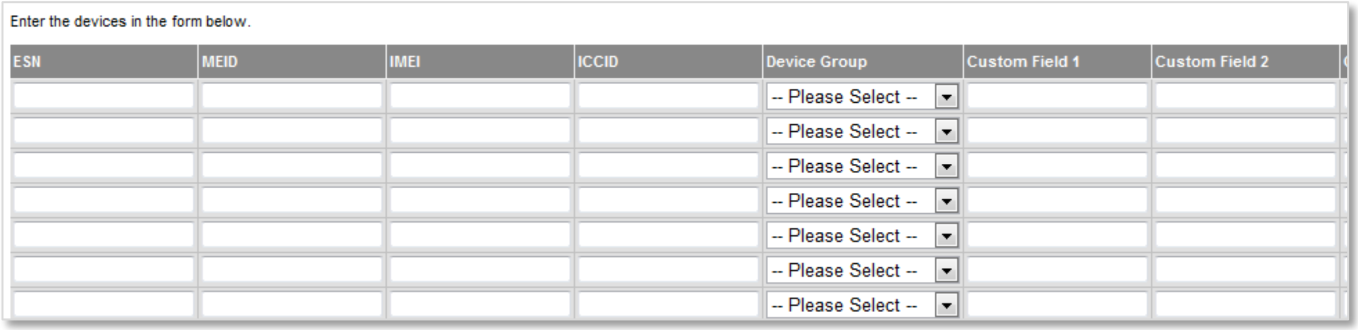
To manually enter information for up to 10 devices:

1. Go to the Admin tab and select Upload Devices from the sub-menu,

2. Use the drop-down controls at the top of the screen to select the Account and Carrier associated with the devices you are updating.

3. Specify that you are updating devices by Screen Entry.

4. Specify the devices you want to update by identifier and enter attributes for the devices in the grid at the bottom of the screen. Remember, to retain a device's current information that you do not want to update, you must include it in the grid or it will be erased when you upload new information.



Enter the devices in the form below.

ESN	MEID	IMEI	ICCID	Device Group	Custom Field 1	Custom Field 2
				-- Please Select --		
				-- Please Select --		
				-- Please Select --		
				-- Please Select --		
				-- Please Select --		
				-- Please Select --		
				-- Please Select --		

Figure 2-37 Upload Devices and Attributes entry grid

5. Click Submit to begin the upload process. The following warning message appears to inform you about blank values overwriting a device's current information:

   Any existing device group and custom field values will be over-written with a blank value if the field value you are uploading here is blank. To maintain existing values, please ensure that they are included in this upload file/screen grid.

6. Click OK to continue, or click Cancel to dismiss the warning window without updating any devices.

2.5 Perform Device-related Actions

Service provisioning actions for devices, such as activate, change service plan, suspend and resume, are performed in the Wireless Number Center. The Device List screen contains links for performing provisioning actions in the Wireless Number Center, as described in the sub-sections below.

From the Device List of the M2M Management Center, you can group devices (explained in Create a Device Group from the Device List), modify custom information about devices, remotely update the Preferred Roaming List (PRL) of one or more devices and wake up one or more devices.

Related Information

About Device-State Changes

Navigate to Provisioning Actions for a Single Device

Related Information

Device List Properties

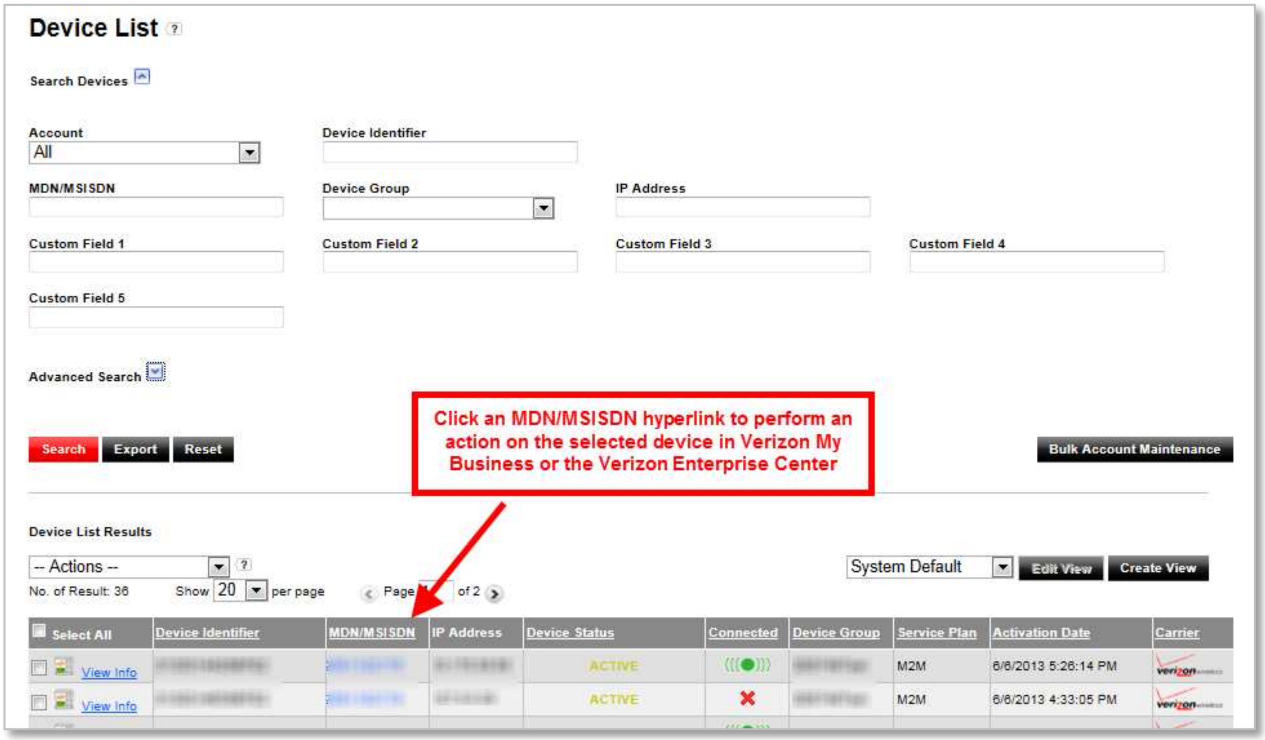
To select a device and perform device-provisioning actions, use the following procedure:

1. From the Navigation menu, click Device List. The Device List screen appears.

2. Use the criteria fields at the top of the Device List screen to find the device you want to provision. If you need additional criteria, expand the search area to show Advanced Search fields.

3. Click Search.

4. Locate the row of the device you want to provision and click its MDN/MSISDN hyperlink. An example is illustrated below (note that you might need to choose a view that includes the MDN/MSISDN of a device if it is not displayed):



Device List ?

Search Devices

Account: All

Device Identifier

MDN/MSISDN

Device Group

IP Address

Custom Field 1

Custom Field 2

Custom Field 3

Custom Field 4

Custom Field 5

Advanced Search

Click an MDN/MSISDN hyperlink to perform an action on the selected device in Verizon My Business or the Verizon Enterprise Center

Device List Results

-- Actions -- ?

No. of Result: 36   Show 20 per page   Page 1 of 2

System Default

□ Select All	Device Identifier	MDN/MSISDN	IP Address	Device Status	Connected	Device Group	Service Plan	Activation Date	Carrier
□ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	●	[redacted]	M2M	6/6/2013 5:26:14 PM	verizon
□ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/6/2013 4:33:05 PM	verizon

Figure 2-38 MDN hyperlink to provision a single device

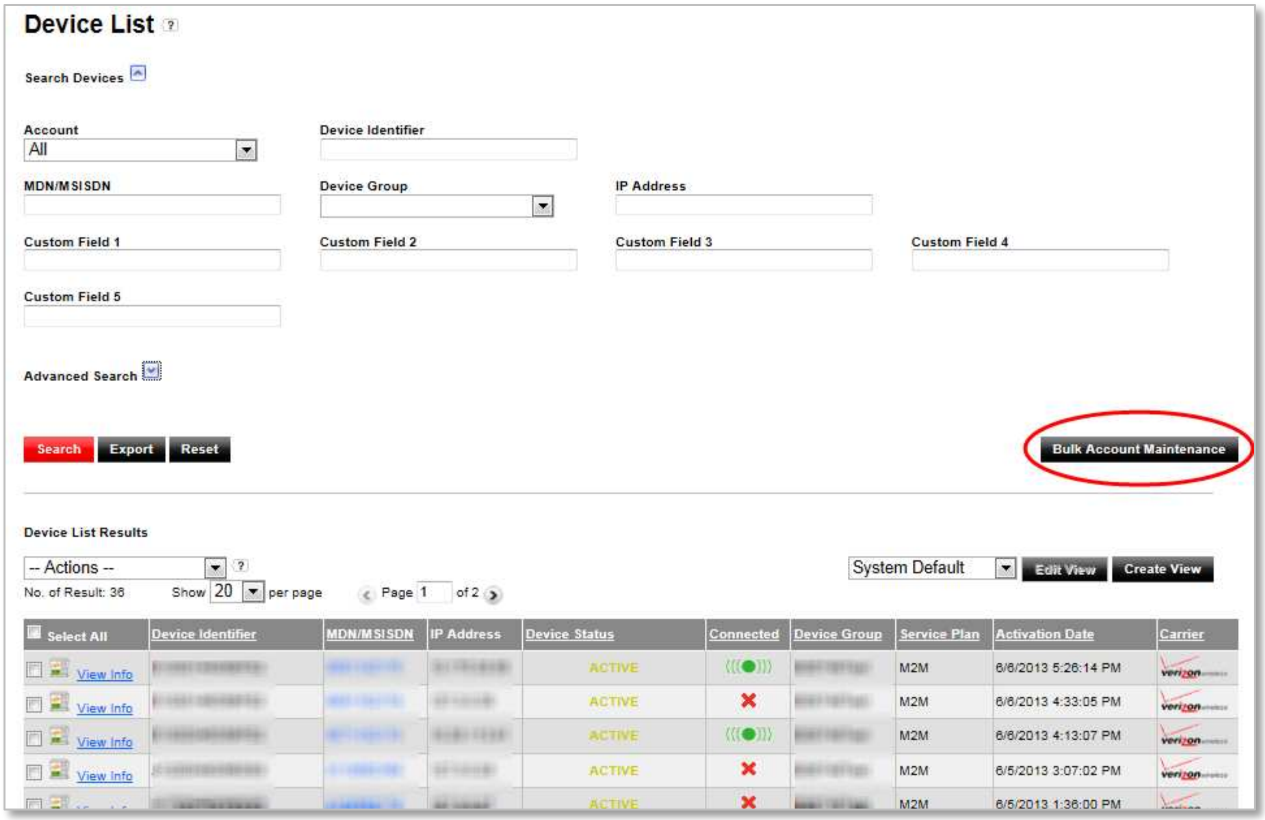
The Verizon Wireless Number Center within Account Maintenance appears. This screen offers device-state change actions for the device and also includes a link to return to the M2M Management Center.

Navigate to Provisioning Actions for Multiple Devices

To perform service provisioning actions (including the changes listed above) for multiple devices, use the procedure in this sub-section. No devices will be selected for provisioning. In the Verizon Wireless Bulk Account Maintenance area, enter the IDs of the devices you want to provision, or import device IDs. Use the link provided to return to the M2M Management Center.

1. From the Navigation menu, click Device List. The Device List screen appears.

2. Click the Bulk Account Maintenance button:



☐ Select All	Device Identifier	MDN/MSISDN	IP Address	Device Status	Connected	Device Group	Service Plan	Activation Date	Carrier
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	●	[redacted]	M2M	6/6/2013 5:26:14 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/6/2013 4:33:05 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	●	[redacted]	M2M	6/6/2013 4:13:07 PM	verizon
☐ View Info	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/5/2013 3:07:02 PM	verizon
☐	[redacted]	[redacted]	[redacted]	ACTIVE	✗	[redacted]	M2M	6/5/2013 1:36:00 PM	

Figure 2-39 Bulk Account Maintenance button to provision multiple devices

The Account Maintenance area of the Wireless Number Center interface appears. This screen offers device-state change actions for multiple devices and also includes a link to return to the M2M Management Center.

Assign Custom Fields to Devices

Related Information

Device List Properties

Related Task

Assign Custom Field Labels

Custom fields for devices are optional. They are usually used to categorize, identify and track devices. You can modify up to five custom fields for each device. These searchable fields can represent regions, business units, device types and models or any other information that is helpful in categorizing, identifying, sorting and monitoring devices.

To modify custom fields for one or more devices:

1. From the Navigation menu, click Device List. The Device List screen appears.

2. Use the criteria fields at the top of the Device List screen to specify the devices to view. If you need additional criteria, expand the search area to show Advanced Search fields.

3. Click Search. The Device List appears, filtered to show the devices that match your criteria.

4. Locate the rows of the devices for which you want to change custom fields and check each device's checkbox in the left-most column.

5. Drop down the Actions menu found at the top left of the Device List and select Assign Custom Fields:

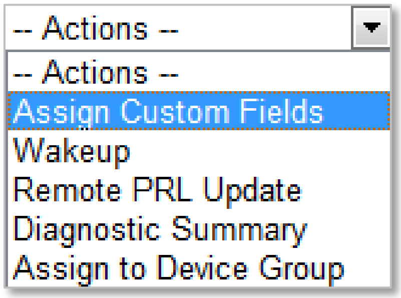
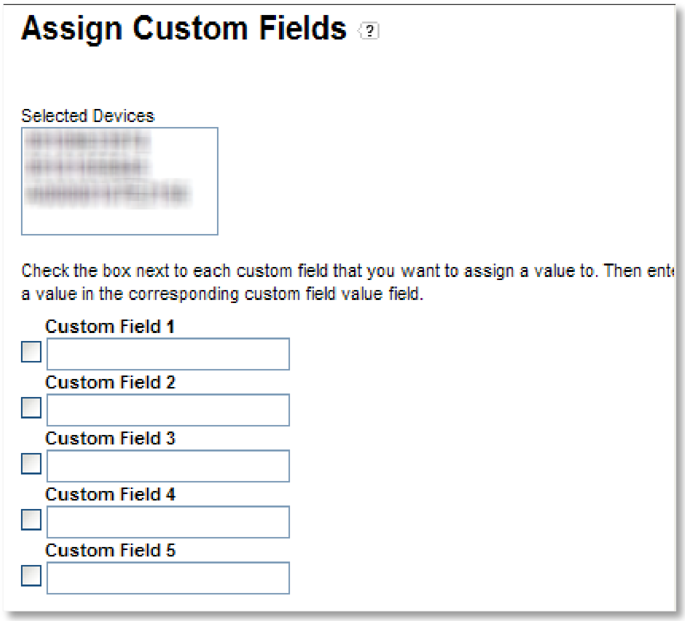


Figure 2-40 Actions menu

The Assign Custom Fields pop-up appears, showing your selected device(s).

NOTE:

- **When one device is selected for assignment, the Assign Custom Fields pop-up will display data in any custom field that was previously populated. When more than one device is selected for assignment, all custom fields in the pop-up will be blank, even if they were previously populated for any selected device. Newly assigned values in custom fields will overwrite previously entered data in this case.**
- **Your pop-up may look different from the example below if your Customer Administrator assigned labels (see Assign Custom Field Labels).**
- **In addition to all alphanumeric characters and SPACE, the following special characters are allowed in custom fields:**
  - , (comma)
  - . (period)
  - : (colon)
  - - (hyphen)
  - _ (underscore)
  - / (forward slash or virgule)
  - @ (at sign)
  - ((open parenthesis)
  -) (close parenthesis)
  - [(open bracket)
  -] (close bracket)
  - # (number sign or hash)



Assign Custom Fields

Selected Devices

[redacted]

Check the box next to each custom field that you want to assign a value to. Then ent
a value in the corresponding custom field value field.

Custom Field 1

□

Custom Field 2

□

Custom Field 3

□

Custom Field 4

□

Custom Field 5

□

Figure 2-41 Assign Custom Fields pop-up

6. Click the checkbox at the left of a custom field to enable it to accept a value, and enter the value. Up to five custom values of up to 50 characters can be entered for the selected device(s). When you check a field and enter nothing, the existing custom values for all selected devices will be erased.

7. Click Submit to save your changes; click Cancel to dismiss the Assign Custom Fields pop-up without making changes. A message appears to indicate whether or not the operation was successful.

8. Click Close to dismiss the message window.

Update the PRL of One or More Non-Grouped Devices Remotely

Related Information

Device List Properties

Periodically updating a device's Preferred Roaming List (PRL) is recommended, particularly for devices that are deployed remotely and roam on a regular basis. This update allows a device to optimize its selection of a roaming carrier or partner when needed.

To perform a remote PRL update for one device or multiple *non-grouped* devices, use the instructions in this task. To perform a remote PRL update for a device group, go to the task Update the PRL for All Devices in a Device Group Remotely.

NOTES:

- **Only devices with a Verizon Advanced M2M Client accept PRL update commands.**
- **All devices selected for remote PRL update must have an Active status.**
- **The success of a PRL update is device-dependent (the device must support the PRL update client and the client must be installed on the device). Furthermore, the device must be registered on the Verizon Enterprise Network and within network coverage.**
- **For best performance, update the PRL of each device once and only once every 90 days.**
- **When you choose devices in the same base-station sector, some requests may be queued by the throttling mechanism. The system generates a message in the Master Log to inform you of this situation. Any requests that are throttled will be released automatically in a first-in-first-out manner as previous requests complete.**

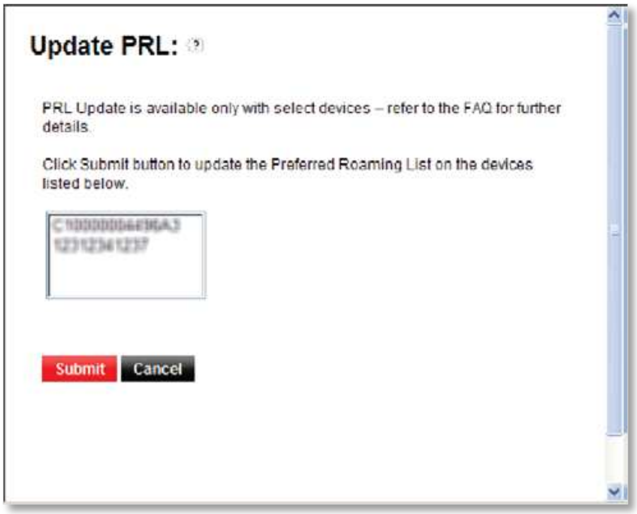
1. From the Navigation menu, click Device List. The Device List screen appears.

2. Use the criteria fields at the top of the Device List screen to specify the devices to view. If you need additional criteria, expand the search area to show Advanced Search fields.

3. Click Search. The Device List appears, filtered to show the devices that match your criteria.

4. Locate and select the active device(s) for which you want to perform a remote PRL update.

5. Drop down the Actions menu and select Remote PRL Update. The Update PRL pop-up appears, showing your selected device(s):



Update PRL:

PRL Update is available only with select devices – refer to the FAQ for further details.

Click Submit button to update the Preferred Roaming List on the devices listed below.

[redacted]

Figure 2-42 Update PRL pop-up

6. Click Submit to perform the update; click Cancel to dismiss the Update PRL pop-up without updating the selected device(s). A message appears to indicate whether or not the operation was successful. Check the Transaction History Report for the outcome of the transaction.

7. Click Close to dismiss the message window.

Update the PRL for All Devices in a Device Group Remotely

Regularly updating a device's Preferred Roaming List (PRL) is recommended, particularly for devices that are deployed remotely and roam on a regular basis. This update allows a device to optimize its selection of a roaming carrier or partner when needed.

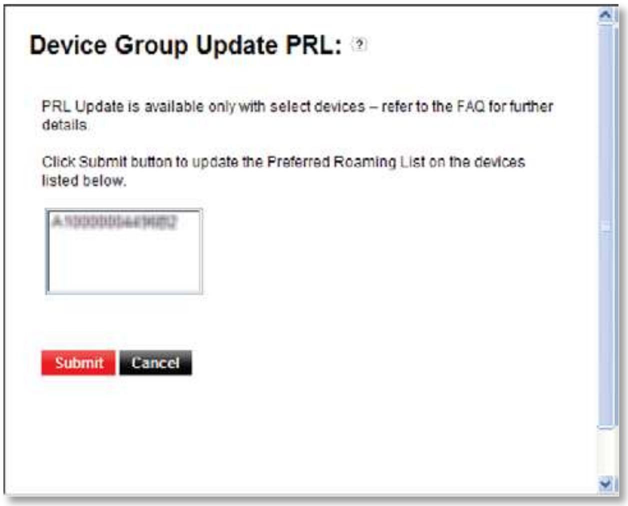
NOTES:

- **Only devices with a Verizon Advanced M2M Client accept PRL update commands.**
- **All devices selected for remote PRL update must have an Active status.**
- **For best performance, update the PRL of each device once and only once every 90 days.**
- **The success of a PRL update is device-dependent (the device must support the PRL update client and the client must be installed on the device). Furthermore, the device must be registered on the Verizon Enterprise Network and within network coverage.**
- **When you choose devices in the same base station sector, some requests may be queued by the throttling mechanism. The system generates a message in the Master Log to inform you of this situation. Any requests that are throttled will be released automatically in a first-in-first-out manner as previous requests complete.**

1. From the Navigation menu, click Admin and choose the Device Group sub-menu. The Device Group List screen appears.

2. Go to the Actions menu in the row of the device group you want to update and choose Remote PRL Update.

3. The Device Group Update PRL screen appears, showing a list of the devices in the group that will be updated:



Device Group Update PRL:

PRL Update is available only with select devices – refer to the FAQ for further details.

Click Submit button to update the Preferred Roaming List on the devices listed below.

[redacted]

Figure 2-43 Device Group Update PRL pop-up

4. Click Submit to perform the update; click Cancel to dismiss the Device Group Update PRL pop-up without updating the selected devices. A message appears to indicate whether or not the operation was successful. Check the Transaction History Report for the outcome of the transaction.

5. Click Close to dismiss the message window.

Wake Up One or More Non-Grouped Devices

Related Information

Device List Properties

At times, a device enters an idle state to conserve energy when it is not needed. The device is still active, but before you perform further action on it, you must send a wakeup call to be sure it is receptive and ready. A device that continually times out when you attempt to send it instructions via IP usually requires a wakeup.

To wake up one device or multiple *non-grouped* devices, use the instructions in this task. To issue a wakeup to all the devices in a device group, go to the task Wake Up All Devices in a Device Group.

NOTES:

- **Only devices with a Verizon Advanced M2M Client accept and execute Wakeup commands.**
- **All devices selected for wakeup must have an Active status.**
- **Wakeup messages will generate some wireless data or Short Message Service (SMS) usage and will be charged according to your service plan.**

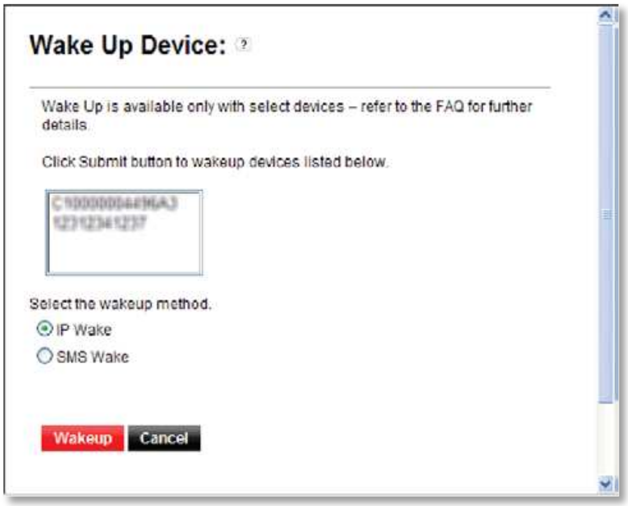
1. From the Navigation menu, click Device List. The Device List screen appears.

2. Use the criteria fields at the top of the Device List screen to specify the devices to find for wakeup. If you need additional criteria, expand the search area to show Advanced Search fields.

3. Click Search. The Device List appears, filtered to show the devices that match your criteria.

4. Locate and select the device(s) that you want to wake.

5. Drop down the Actions menu and select Wakeup. A Wake Up Device pop-up appears, showing your selected device(s):



Wake Up Device:

Wake Up is available only with select devices – refer to the FAQ for further details.

Click Submit button to wakeup devices listed below.

[illegible]
[illegible]

Select the wakeup method.

● IP Wake
○ SMS Wake

Figure 2-44 Wake Up Device pop-up

6. Specify a method to use for wakeup. Your choices include:

+ IP Wake, which looks up the current IP address of a device from the M2M Management Center eAAA server and issues an IP wakeup call to the device. (This option is available on select devices only.)

+ SMS Wake, which issues an SMS message to the device. (This is the only functional option for devices on a Customer Private Network account.)

7. Click Wakeup to send a wakeup to the selected device(s); click Cancel to dismiss the Wake Up Device pop-up without waking up any device. A message appears to indicate whether or not the operation was successful. Check the Transaction History Report for the outcome of the transaction.

8. Click Close to dismiss the message window.

Wake Up All Devices in a Device Group

NOTES:

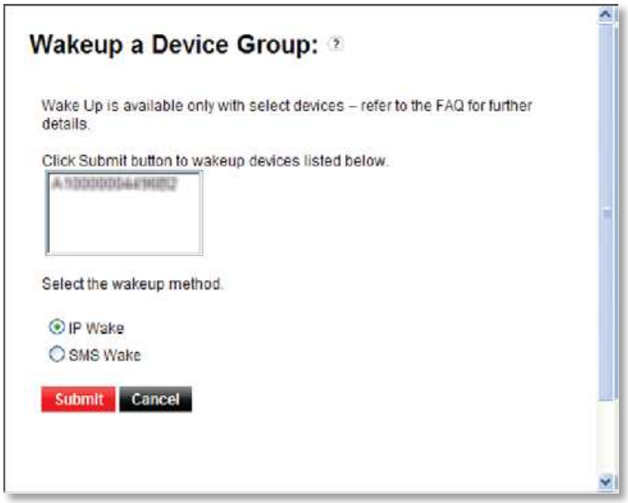
+ Only devices with a Verizon Advanced M2M Client accept and execute Wakeup commands.

+ All devices selected for wakeup must have an Active status.

+ Wakeup messages will generate some wireless data or SMS usage and will be charged according to your service plan.

1. From the Navigation menu, click Admin and choose the Device Group sub-menu. The Device Group List screen appears.

2. Go to the Actions menu in the row of the device group you want to wake up. The Wakeup a Device Group screen appears, showing a list of the devices in the group that will be woken:



Wakeup a Device Group:

Wake Up is available only with select devices – refer to the FAQ for further details.

Click Submit button to wakeup devices listed below.

[redacted]

Select the wakeup method.

● IP Wake
○ SMS Wake

Figure 2-45 Wakeup a Device Group pop-up

3. Specify a method to use for wakeup. Your choices include:

- IP Wake, which looks up the current IP address of all devices in the group from the M2M Management Center eAAA server and issues an IP wakeup call to each device. (This option is available on select devices only.)
- SMS Wake, which issues an SMS message to all devices in the group. (This is the only functional option for devices on a Customer Private Network account.)

4. Click Submit to wake up the devices; click Cancel to dismiss the Wakeup a Device Group pop-up without waking the devices in the selected group. A message appears to indicate whether or not the operation was successful. Check the Transaction History Report for the outcome of the transaction.

5. Click Close to dismiss the message window.

2.6 Set Up and Use Notifications

2.6.1 Task Order for Notifications

The M2M Management Center includes an optional notification feature that can be set to alert contacts (i.e., system users) when certain conditions you define are met or breached. Use the following steps when setting up notifications:

1. Maintain a list of system contacts. Optionally add records for Alerts Only contacts to which you want to send notifications. Alerts Only contacts do not have access to Verizon My Business or the Verizon Enterprise Center; therefore, they do not have access to the M2M Management Center.

2. Organize contacts into notification groups.

3. Optionally group devices (see Create a Device Group from the Device List or Create a Device Group from the Admin Tab)

4. Establish notification rules.

5. View notification alerts and optionally acknowledge them.

NOTE: Alerts Only contacts cannot view or acknowledge notifications because they do not have access to the M2M Management Center.

Related Information

About Notifications

Alerts Only Contacts

2.6.2 Maintain System Contacts

Contact maintenance is reserved for Customer Admin users only. It involves:

- Searching for a contact
- Adding an Alerts Only contact
- Editing a contact's record
- Deleting an Alerts Only contact

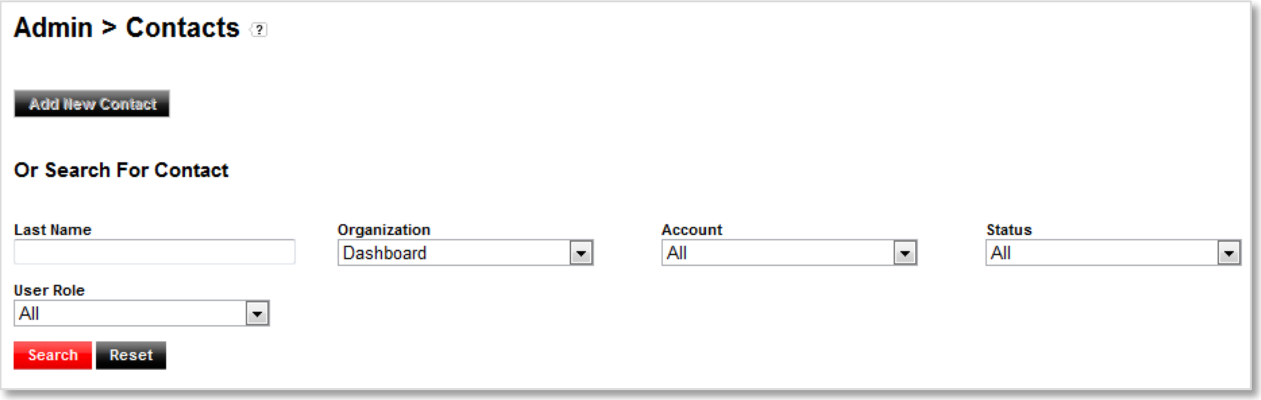
Search for a Contact

NOTE: This action applies only if you are a user with the Customer Admin role.

Related Information

Contact Properties

1. Click the Admin tab and select the Contact Setup sub-menu command. The Contacts screen appears:



Last Name	
Organization	Dashboard
Account	All
Status	All
User Role	All

Figure 2-46 Contacts screen

2. Use the search criteria fields to specify contact information for the user you want to find.

3. Click Search. The search results are displayed in a grid in the bottom portion of the screen.

Add an Alerts Only Contact

Related Information

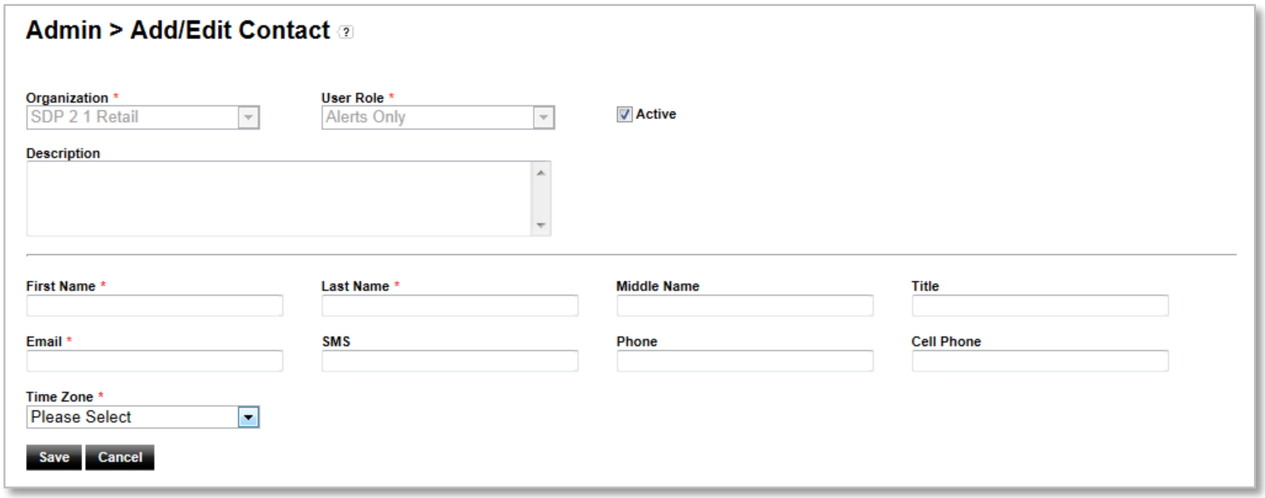
Contact Properties

Alerts Only Contacts

To add a contact record for a person or group to which you want to send notifications only:

1. Click the Admin tab and select the Contact Setup sub-menu command. The Contacts screen appears.

2. Click Add New Contact. The Add/Edit Contact screen appears:



Admin > Add/Edit Contact

Organization * SDP 2 1 Retail

User Role * Alerts Only

☑ Active

Description

First Name *

Last Name *

Middle Name

Title

Email *

SMS

Phone

Cell Phone

Time Zone * Please Select

Figure 2-47 Add/Edit Contact screen

3. Provide required and optional information for the contact.

4. Click Save to save the Alerts Only contact information to the database, or click Cancel to dismiss your changes without saving.

Edit a Contact Record

Related Information

Contact Properties

About System Users

About Time Zone

NOTE: The following rules apply to this task:

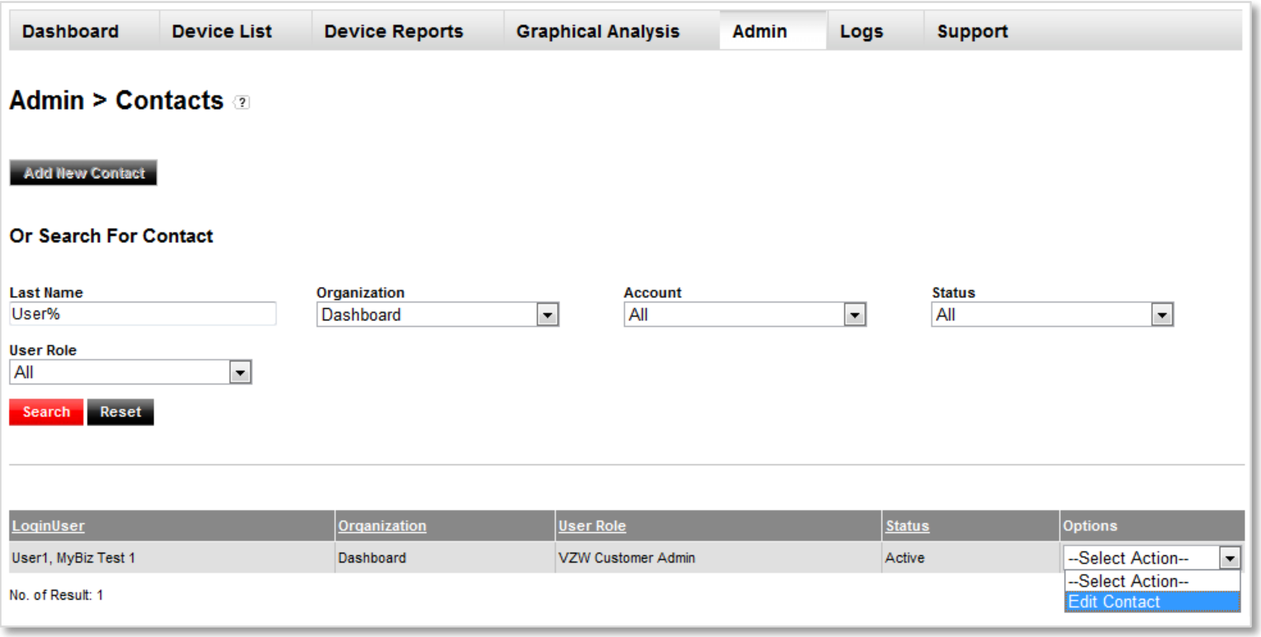
- **Contact records for M2M Management Center users are created automatically the first time a user accesses the M2M Management Center. Therefore, a user must gain access to the M2M Management Center from either the My Business Account or Verizon Enterprise Center portal to have a contact record.**
- **You can specify and modify the phone numbers, Time Zone, and Portal Landing Page fields only in a system user's record. These fields remain populated and do not get overwritten by data from the Verizon Wireless My Business Account or Verizon Enterprise Center. All fields can be edited for Alerts Only contacts.**
- **The Add/Edit Contact screen for an Alerts Only contact includes a Delete Contact button control. You can click it to delete the contact's record. You must confirm the deletion by clicking OK on the dialog that appears to complete the action.**

To edit contact information:

1. Click the Admin tab and select the Contact Setup sub-menu command. Use the search criteria to find the contact you need to modify.

2. Click Search. The search results are displayed in the bottom portion of the Contacts screen.

3. Locate the row of the contact record you need to edit, drop down the Options menu and choose Edit Contact:



Admin > Contacts

Or Search For Contact

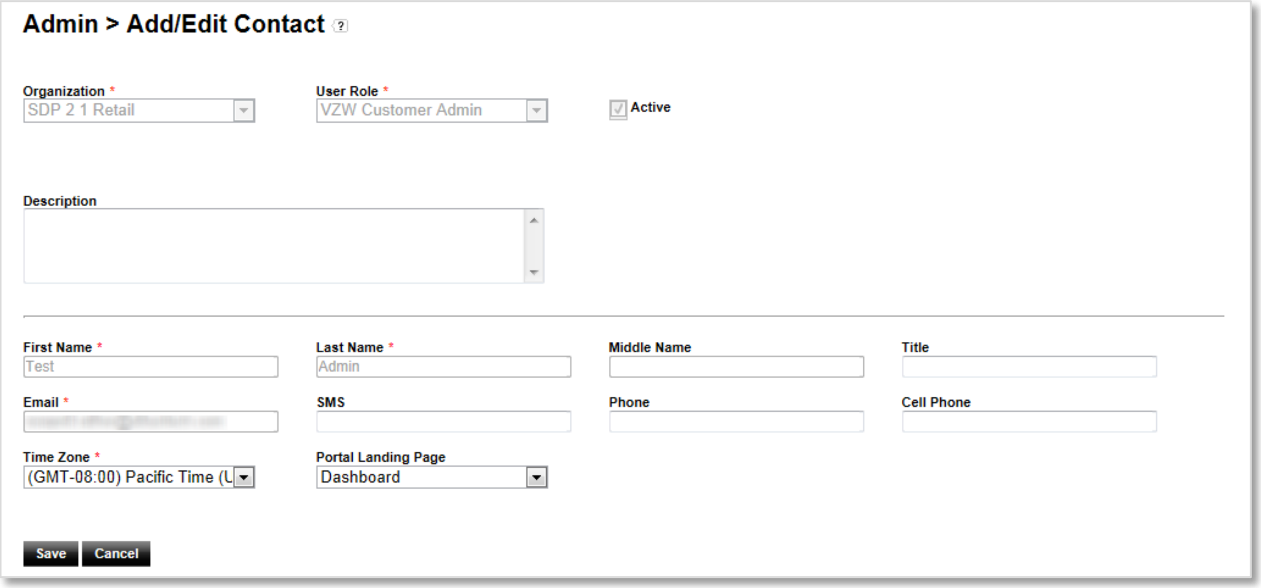
Last Name: User%	Organization: Dashboard	Account: All	Status: All
User Role: All			

LoginUser	Organization	User Role	Status	Options
User1, MyBiz Test 1	Dashboard	VZW Customer Admin	Active	--Select Action-- --Select Action-- Edit Contact

No. of Result: 1

Figure 2-48 Edit Contact option

The Add/Edit Contact screen appears:



Admin > Add/Edit Contact

Organization *: SDP 2 1 Retail	User Role *: VZW Customer Admin	☑ Active	
Description:			
First Name *: Test	Last Name *: Admin	Middle Name:	Title:
Email *: [redacted]	SMS:	Phone:	Cell Phone:
Time Zone *: (GMT-08:00) Pacific Time (U	Portal Landing Page: Dashboard		

Figure 2-49 Add/Edit Contact screen

4. Edit the contact's information as needed.

5. Click Update to save the contact information to the database, or click Cancel to dismiss your changes without saving.

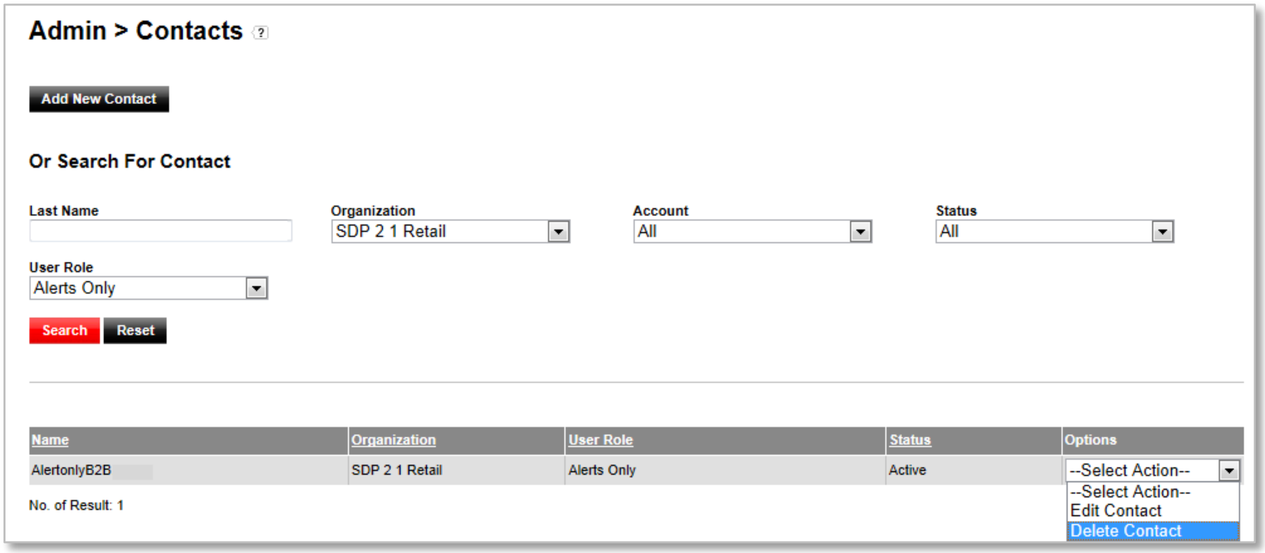
Delete an Alerts Only Contact

Related Information

Alerts Only Contacts

To delete an Alerts Only contact record:

1. Click the Admin tab and select the Contact Setup sub-menu command.
2. Use the search criteria to find the contact you want to delete.
3. Click Search. The search results are displayed in the bottom portion of the Contacts screen.
4. Locate the row of the Alerts Only contact record you need to delete, drop down the Options menu and choose Delete Contact



Last Name:

Organization: SDP 2 1 Retail

Account: All

Status: All

User Role: Alerts Only

Name	Organization	User Role	Status	Options
AlertonlyB2B	SDP 2 1 Retail	Alerts Only	Active	--Select Action--

No. of Result: 1

Figure 2-50 Add/Edit Contact screen

5. Confirm that you want to delete the contact by clicking OK. The contact will be removed from the table. To dismiss the confirmation dialog and retain the Alerts Only contact record, click Cancel.

2.6.3 Organize Contacts into Notification Groups

A notification group is a set of contacts that is alerted when the conditions attached to a notification rule are met or exceeded and generate a notification as a result. Notification rule setup is described in the task Create a Notification Rule. There is no limit to the number of contacts in a notification group. You can also create a notification group containing one contact.

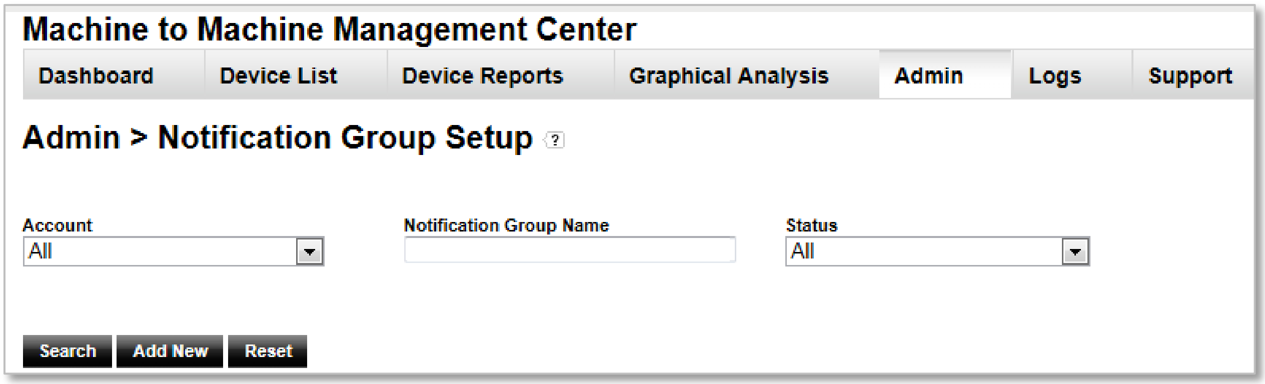
Create a Notification Group

Related Information

Notification Group Properties

To create a new notification group:

1. Click the Admin tab and select the Notification Group Setup sub-menu command. The Notification Group Setup screen appears:



Machine to Machine Management Center

Admin > Notification Group Setup ?

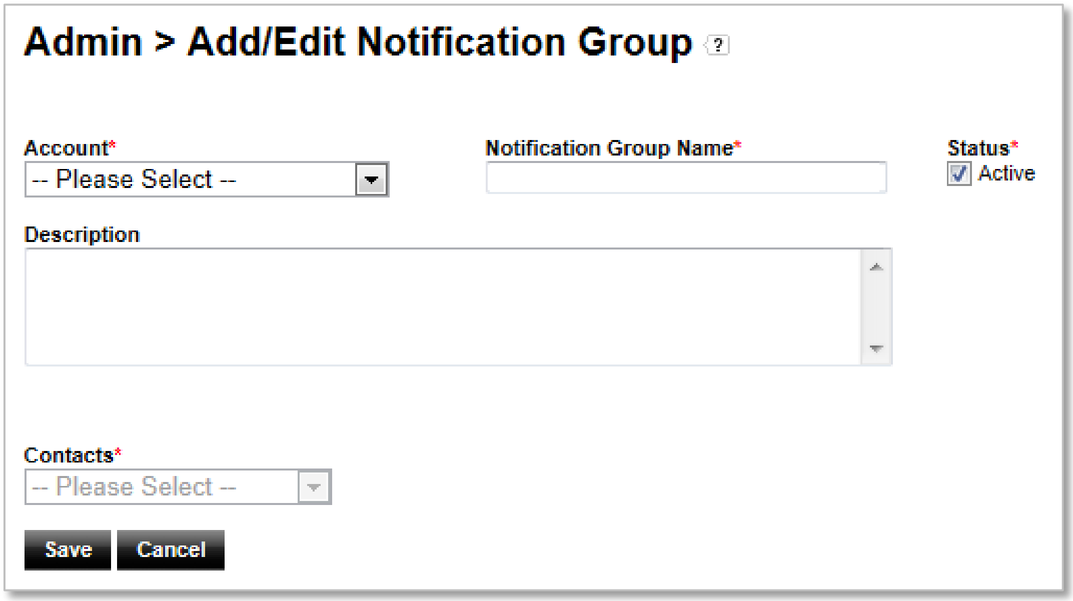
Account: All

Notification Group Name:

Status: All

Figure 2-51 Notification Group Setup screen

2. Click Add New. Fields for the new notification group appear on the Notification Group Setup screen:



Admin > Add/Edit Notification Group ?

Account*: -- Please Select --

Notification Group Name*:

Status*: ☑ Active

Description:

Contacts*: -- Please Select --

Figure 2-52 Notification Group Setup screen

3. Supply the properties for the new notification group.

4. Build the notification group by selecting from the Contacts drop-down. A contact can belong to multiple notification groups. A notification group can also have only one contact.

NOTE:

- **If the Contact list does not contain a system user you want to add to a notification group, the user may not have a contact record yet. Ensure that the user has accessed the M2M Management Center at least once to establish a contact record in the application.**
- **To add an Alerts Only contact on-the-fly, choose Add New Contact in the Contact drop-down. The Add/Edit Contact screen appears (see Add an Alerts Only Contact).**

5. When you select a contact from the drop-down or return from adding an Alerts Only contact, the Notification Method field appears. Select a Notification Method for the current Contact.

6. Click the Add button, which appears next to the Notification Method drop-down, to add the contact to the current notification group.

7. To add more contacts to the notification group, return to Step 4. When the notification contact list is complete, continue to the last step.

8. Click Save to save the notification group to the database; click Cancel to dismiss the information entered for the group.

Edit a Notification Group

Related Information

Notification Group Properties

You can edit the general properties of a notification group, the contacts in a group, or both.

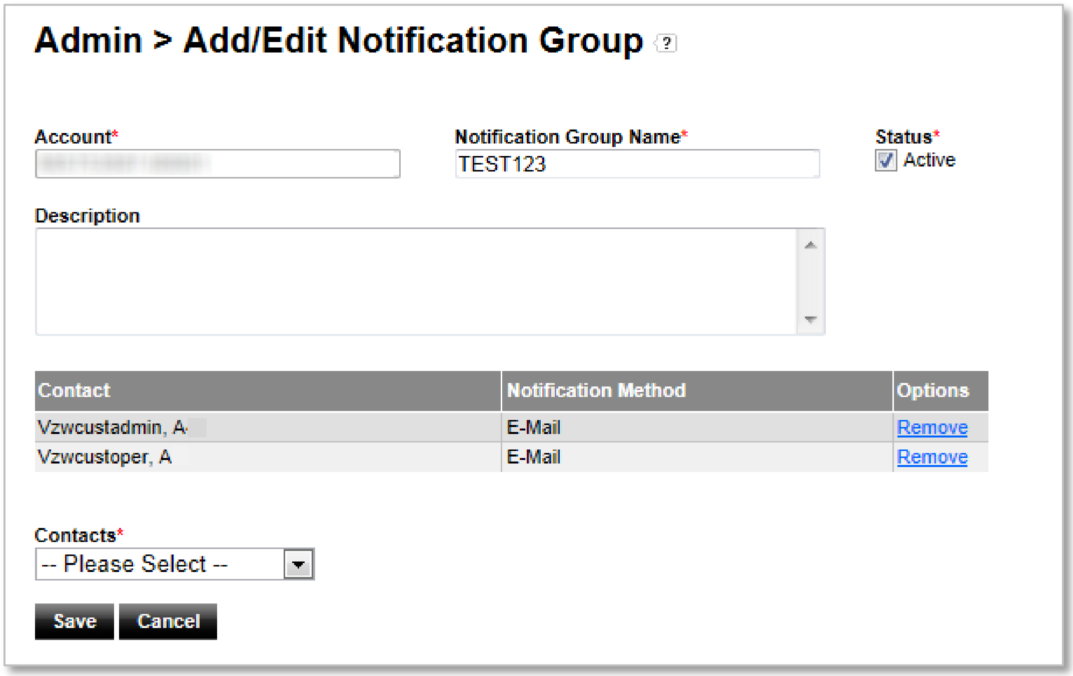
To view an existing notification group and make changes to it:

1. Click the Admin tab and select the Notification Group Setup sub-menu command.

2. When the Notification Group Setup screen appears, use the criteria fields to specify the groups you want to find. The more information you provide, the more targeted your search.

3. Click Search. The groups matching your criteria appear in a table at the bottom of the screen.

4. Find the row of the group you want to modify and click the Edit link in the Options column. The Add/Edit Notification Group screen appears, showing the Description and list of contacts that comprise the group:



Admin > Add/Edit Notification Group

Account*: [redacted]

Notification Group Name*: TEST123

Status*: ☑ Active

Description:

Contact	Notification Method	Options
Vzwcustadmin, A	E-Mail	Remove
Vzwcustoper, A	E-Mail	Remove

Contacts*: -- Please Select --

Figure 2-53 Edit a notification group

5. Modify the properties of the notification group, if necessary. When you are finished, go to Step 10. To edit the contact list of the group, go to Step 6.

6. Each contact currently associated with the group is listed in a row, with a checkbox that indicates whether the contact is currently active (and can therefore receive notifications). To delete a contact, go to Step 7. To start or stop notification alerts for a contact, go to Step 8. To add a new contact to the group, go to Step 9.

7. To delete a contact, click the corresponding Remove link. Go to Step 10 to continue.

8. The checkbox in each contact's row denotes whether or not the contact is active and eligible to receive notifications. To make a contact eligible to receive notifications, click the checkbox to mark it; likewise, to stop notifications for a contact, uncheck the checkbox by clicking it. Go to Step 10 to continue.

9. To add a new contact to the group, select a new name from the Contact drop-down list, specify a Notification Method and click Add. When you are finished adding contacts to the group, go to Step 10 to continue.

10. Click Save to accept your changes; click Cancel to discard them.

Delete a Notification Group

Related Information

Notification Group Properties

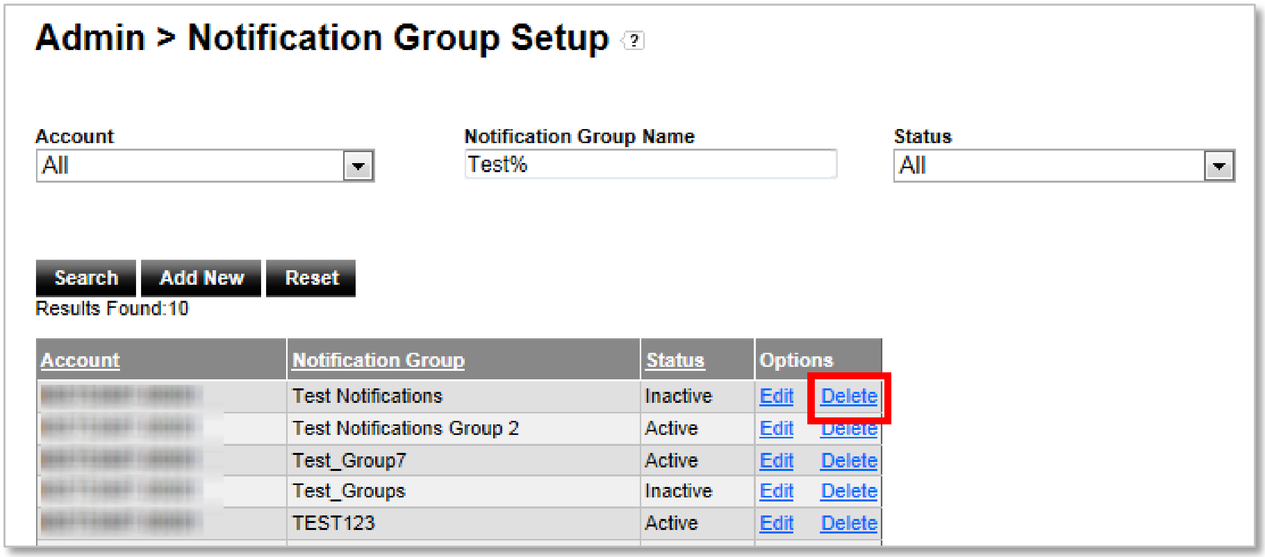
To delete a notification group:

1. Click the Admin tab and select the Notification Group Setup sub-menu command.

2. When the Notification Group Setup screen appears, use the criteria fields to find the group you want to delete. The more information you provide, the more targeted your search.

3. Click Search. The groups matching your criteria appear at the bottom of the screen.

4. Locate the row of the group you want to delete and click the Delete link in the Options column:



Admin > Notification Group Setup

Account: All

Notification Group Name: Test%

Status: All

Results Found:10

Account	Notification Group	Status	Options	
[redacted]	Test Notifications	Inactive	Edit	Delete
[redacted]	Test Notifications Group 2	Active	Edit	Delete
[redacted]	Test_Group7	Active	Edit	Delete
[redacted]	Test_Groups	Inactive	Edit	Delete
[redacted]	TEST123	Active	Edit	Delete

Figure 2-54 Delete a notification group

5. A browser-specific confirmation message appears, asking if you are sure about deleting this notification group. You can choose to proceed or cancel the deletion.

2.6.4 Establish Notification Rules

Create a Notification Rule

Related Information

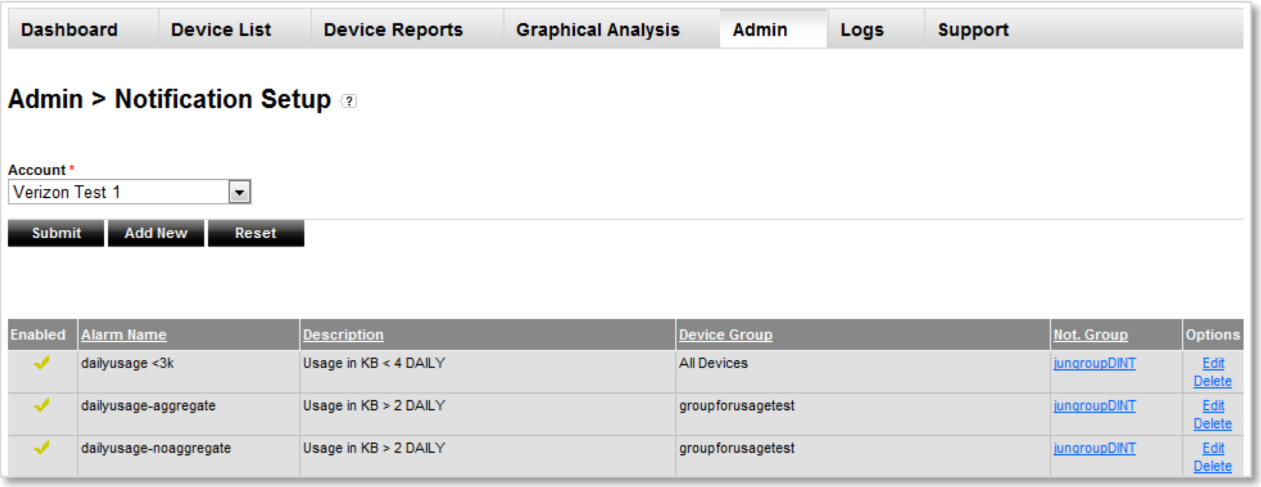
Notification Properties

A notification rule defines the conditions under which a notification alarm will be generated.

To create a new notification rule:

1. Click the Admin tab and select the Notification Setup sub-menu command. The Notification Setup screen appears.

2. Select your account and click Submit. A list of existing notification rules appears (this list will be empty when no rules have been defined):

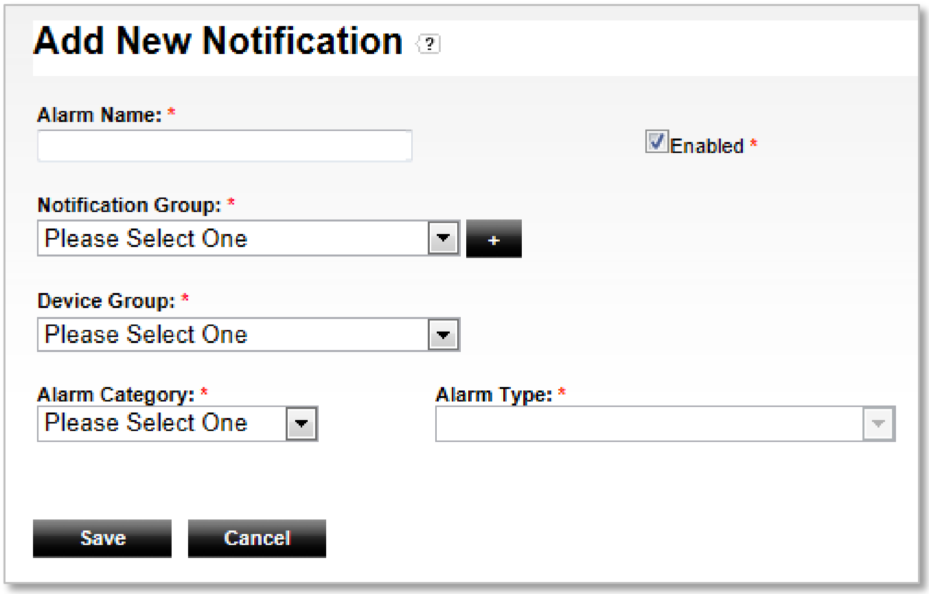


Account *
Verizon Test 1

Enabled	Alarm Name	Description	Device Group	Not. Group	Options
✓	dailyusage <3k	Usage in KB < 4 DAILY	All Devices	jungroupDINT	Edit Delete
✓	dailyusage-aggregate	Usage in KB > 2 DAILY	groupforusagetest	jungroupDINT	Edit Delete
✓	dailyusage-noaggregate	Usage in KB > 2 DAILY	groupforusagetest	jungroupDINT	Edit Delete

Figure 2-55 Notification Setup screen

3. Click Add New. The Add New Notification screen appears:


Add New Notification

Alarm Name: *

☑ Enabled *

Notification Group: * Please Select One

Device Group: * Please Select One

Alarm Category: * Please Select One

Alarm Type: *

Figure 2-56 Add New Notification screen

4. Complete the fields required to create a new notification rule.

5. Click Save to create and store the new notification rule in the system, or click Cancel to dismiss the Add New Notification screen without making any changes.

Edit a Notification Rule

Related Information

Notification Properties

Notification Group Properties

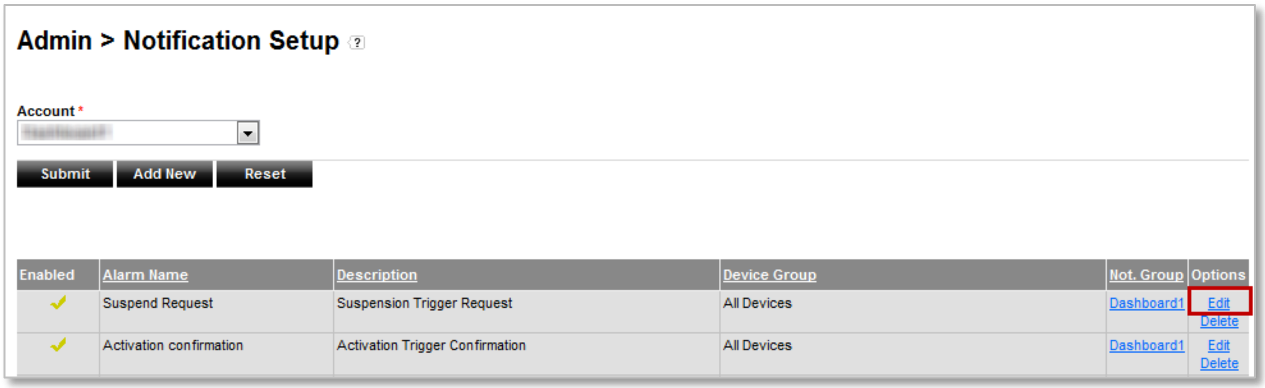
To modify an existing notification rule and/or the notification group associated with a notification rule:

1. Click the Admin tab and select the Notification Setup sub-menu command.

2. When the Notification Setup screen appears, drop down the Account list and choose the account with the notification you want to change.

3. Click Submit. A list of the rules defined for the selected Account appears.

4. To edit a notification rule, find its row, click the Edit link in the Options column, and go to Step 5. To edit the notification group associated with a rule, find the rule's row, click the link in the Notification Group column, and go to Step 6.

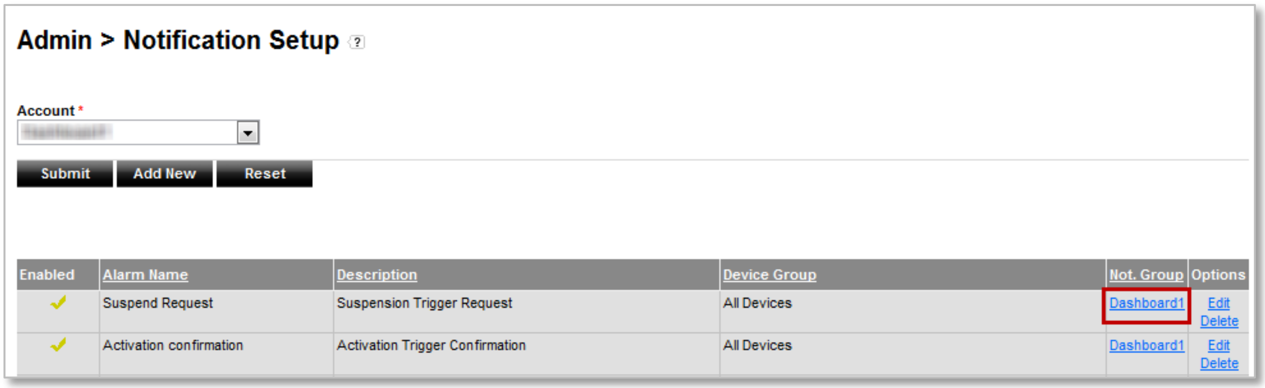


Admin > Notification Setup

Account *

Enabled	Alarm Name	Description	Device Group	Not. Group	Options
✓	Suspend Request	Suspension Trigger Request	All Devices	Dashboard1	Edit Delete
✓	Activation confirmation	Activation Trigger Confirmation	All Devices	Dashboard1	Edit Delete

Figure 2-57 Edit notification rule link



Admin > Notification Setup

Account *

Enabled	Alarm Name	Description	Device Group	Not. Group	Options
✓	Suspend Request	Suspension Trigger Request	All Devices	Dashboard1	Edit Delete
✓	Activation confirmation	Activation Trigger Confirmation	All Devices	Dashboard1	Edit Delete

Figure 2-58 Edit notification group link

5. Adjust the properties of the notification rule, if necessary. When you are finished, go to Step 7.

6. Modify the members and/or method of notification for members in the notification group and go to the next step.

7. Click Save to save your changes, or click Cancel to dismiss the editing screen without saving.

Delete a Notification Rule

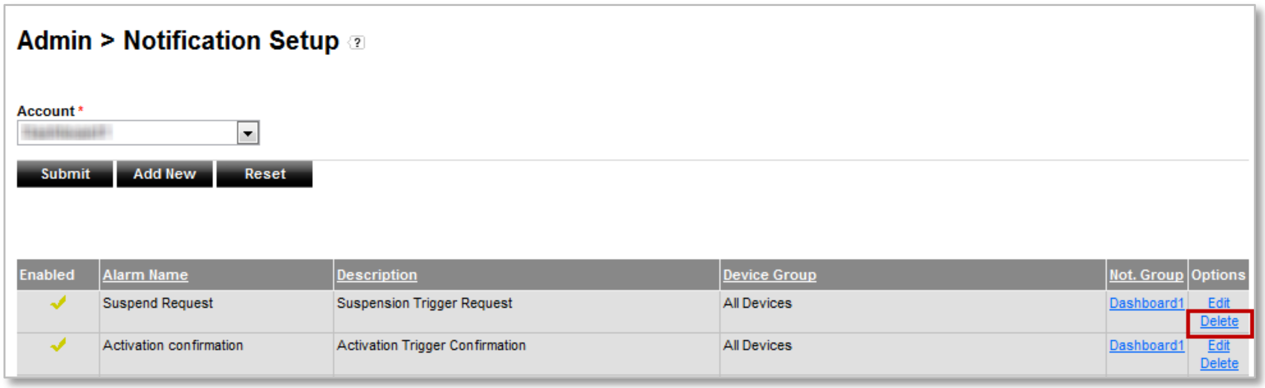
To remove a notification rule from the system:

1. Click the Admin tab and select the Notification Setup sub-menu command.

2. When the Notification Setup screen appears, drop down the Account list and choose the account with the notification you want to delete.

3. Click Submit. A list of the rules defined for the selected Account appears.

4. Locate the row of the alarm you want to delete and click the Delete link in the Options column:



Admin > Notification Setup ?

Account *: [redacted]

Enabled	Alarm Name	Description	Device Group	Not. Group	Options
✓	Suspend Request	Suspension Trigger Request	All Devices	Dashboard1	Edit Delete
✓	Activation confirmation	Activation Trigger Confirmation	All Devices	Dashboard1	Edit Delete

Figure 2-59 Delete notification link

5. A browser-specific confirmation message appears, asking if you are sure about deleting the notification. You can choose to proceed or cancel the deletion.

2.6.5 Acknowledge Notifications

View and Acknowledge Notifications

Related Information

Notification Log

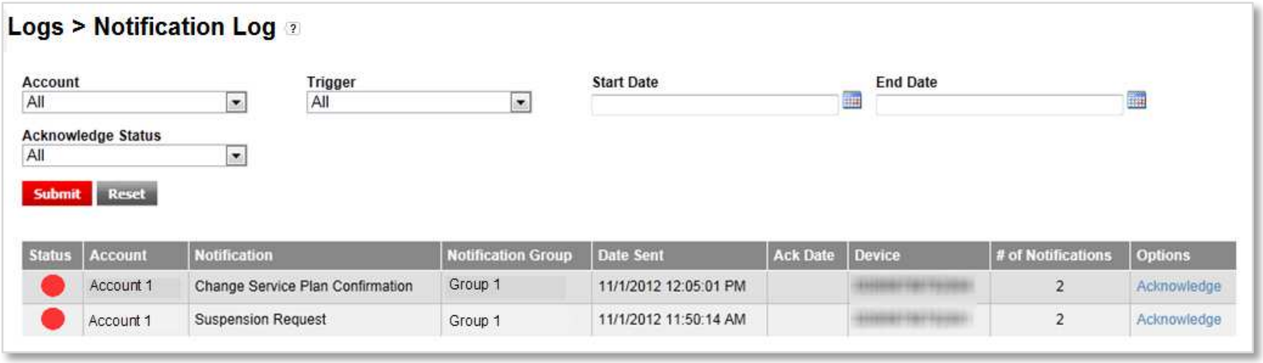
Notifications are accumulated by the M2M Management Center and appear in the Notification Log, where you can view them and optionally acknowledge them if acknowledgement is part of your standard operating procedure.

NOTE:

- **When you have a user role other than Customer Admin, the Notification Log displays only the alerts generated for the notification groups in which you are included.**
- **The Notification Log shows all notifications generated by the system when you have the Customer Admin role.**

To view your list of notifications that the system has generated as a result of the notification rules:

1. Click the Logs tab and select the Notification Log sub-menu command. A default list appears, showing your notifications:



Logs > Notification Log ?

Account: All

Trigger: All

Start Date:

End Date:

Acknowledge Status: All

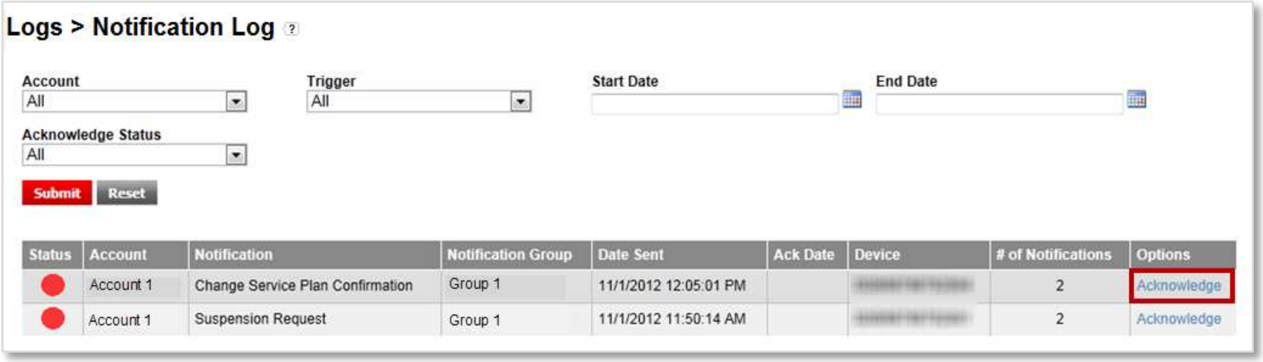
Status	Account	Notification	Notification Group	Date Sent	Ack Date	Device	# of Notifications	Options
●	Account 1	Change Service Plan Confirmation	Group 1	11/1/2012 12:05:01 PM		[redacted]	2	Acknowledge
●	Account 1	Suspension Request	Group 1	11/1/2012 11:50:14 AM		[redacted]	2	Acknowledge

Figure 2-60 Notification Log

2. Use the fields at the top of the screen to specify criteria by which to filter the list.

3. Click Submit. A filtered Notification Log is displayed using the selected criteria.

4. Locate the row of the notification that you want to acknowledge and click the Acknowledge link in the Options column:



Logs > Notification Log

Account: All

Trigger: All

Start Date:

End Date:

Acknowledge Status: All

Status	Account	Notification	Notification Group	Date Sent	Ack Date	Device	# of Notifications	Options
●	Account 1	Change Service Plan Confirmation	Group 1	11/1/2012 12:05:01 PM		[redacted]	2	Acknowledge
●	Account 1	Suspension Request	Group 1	11/1/2012 11:50:14 AM		[redacted]	2	Acknowledge

Figure 2-61 Acknowledging a notification

After you acknowledge a notification, the Status indicator changes to yellow.

2.7 Generate Reports and the Data Usage Trending Chart

NOTE: To print any report, you must either execute a Print Screen from the keyboard when the report is displayed or export the report to the Download Center, import it into another application such as a text editor or spreadsheet, and print it.

Related Information

Report and Chart Properties

The M2M Management Center provides the following reports that can contain data for one or more devices:

+ Connection History Report

  NOTE: The date range limit for the Connection History Report is seven (7) days.

+ Transaction History Report

  NOTE: The date range limit for the Transaction History Report is 30 days.

+ Device Usage Report
+ Aggregated Device Usage Report
+ Diagnostic Events Report
+ Connected Session History Report
+ Rated Usage Report

In addition, the M2M Management Center offers a Data Usage Trending Chart for graphical analysis.

Examples of the reports and Data Usage Trending Chart are found in About Device Reports and Graphical Analysis Charts.

Generate a Report for One or More Devices

NOTE: To print any report, you must either execute a Print Screen from the keyboard when the report is displayed or export the report to the Download Center, import it into another application such as a text editor or spreadsheet, and print it.

Related Information

[Reports and Charts Input Criteria]

[About Device Reports and Graphical Analysis Charts]

[Retrieve Files from the Download Center]

To generate a report containing data for one or more devices:

1. On the Navigation menu, move the cursor to the Device Reports tab to see the Reports sub-menu. Or, click the tab to display the Device Reports landing screen appears. Both are shown below:

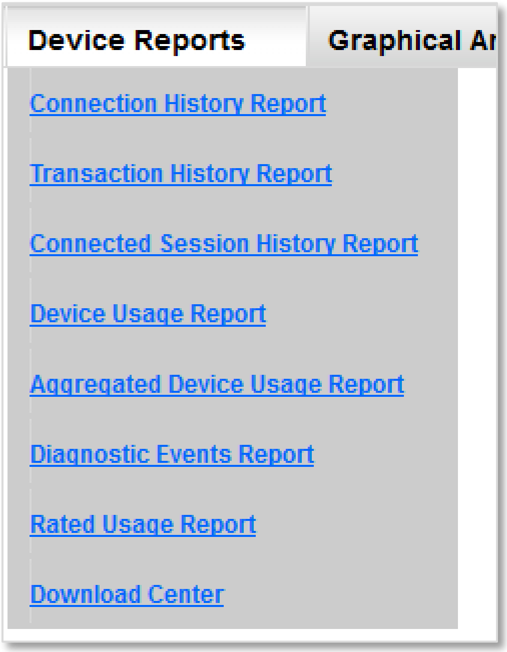
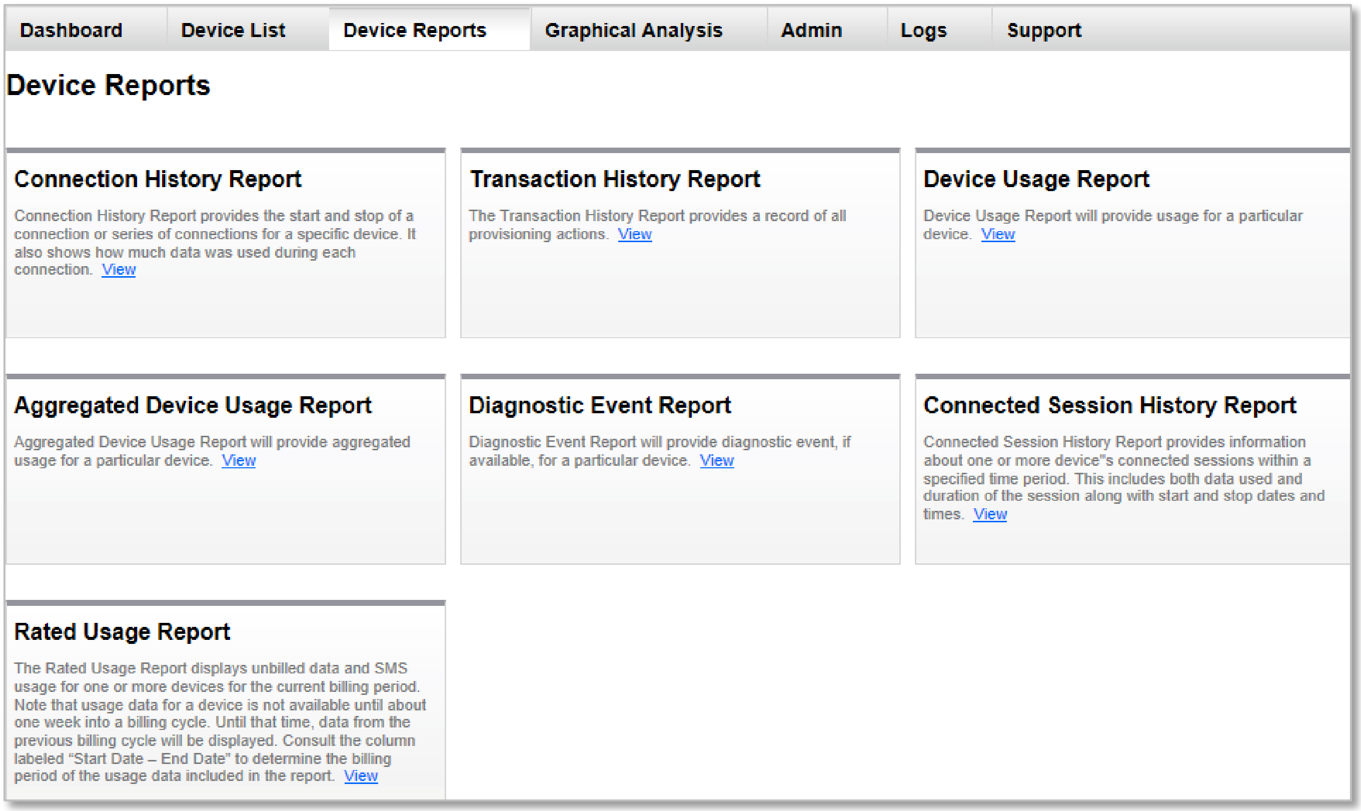

Device Reports
Graphical Ar
Connection History Report
Transaction History Report
Connected Session History Report
Device Usage Report
Aggregated Device Usage Report
Diagnostic Events Report
Rated Usage Report
Download Center

Figure 2-62 Device Reports sub-menu



Device Reports

Connection History Report

Connection History Report provides the start and stop of a connection or series of connections for a specific device. It also shows how much data was used during each connection. View

Transaction History Report

The Transaction History Report provides a record of all provisioning actions. View

Device Usage Report

Device Usage Report will provide usage for a particular device. View

Aggregated Device Usage Report

Aggregated Device Usage Report will provide aggregated usage for a particular device. View

Diagnostic Event Report

Diagnostic Event Report will provide diagnostic event, if available, for a particular device. View

Connected Session History Report

Connected Session History Report provides information about one or more device"s connected sessions within a specified time period. This includes both data used and duration of the session along with start and stop dates and times. View

Rated Usage Report

The Rated Usage Report displays unbilled data and SMS usage for one or more devices for the current billing period. Note that usage data for a device is not available until about one week into a billing cycle. Until that time, data from the previous billing cycle will be displayed. Consult the column labeled “Start Date – End Date” to determine the billing period of the usage data included in the report. View

Figure 2-63 Device Reports landing screen

2. Select the sub-menu command of the report you want to generate or click the View link on the landing screen of the report you want to generate.

3. Specify report criteria. Both default and advanced search fields are available for most reports.

4. Click Generate Report. The selected report appears if it can be generated on-screen. To export the report results, go to the next step.

   If the report cannot be generated because the result set is too large, you will be given the option to send the report to the Download Center. Click OK to produce a comma-separated values (CSV) file to be generated and sent to the Download Center.

5. Click Export to produce a CSV file to be generated and sent to the Download Center. Exported reports include data as it is displayed in your report.

   You will receive emails regarding the export’s progress. When the file is ready in the Download Center, you can download it into another application, such as a text editor or spreadsheet.

Generate a Single-Device Report from the Device List Screen

NOTE: To print any report, you must either execute a Print Screen from the keyboard when the report is displayed or export the report to the Download Center, import it into another application such as a text editor or spreadsheet, and print it.

Related Information

[Reports and Charts Input Criteria]()

[About Device Reports and Graphical Analysis Charts]()

[Retrieve Files from the Download Center]()

To generate a report for a device selected from the Device List:

1. From the Navigation menu, select Device List. The Device List screen appears.
2. Use the fields at the top of the Device List screen to specify criteria for the device you want to include in the Device List.
3. Click Search. A filtered Device List appears.
4. Locate the row of the device for which you want to generate a report and click the Report icon:

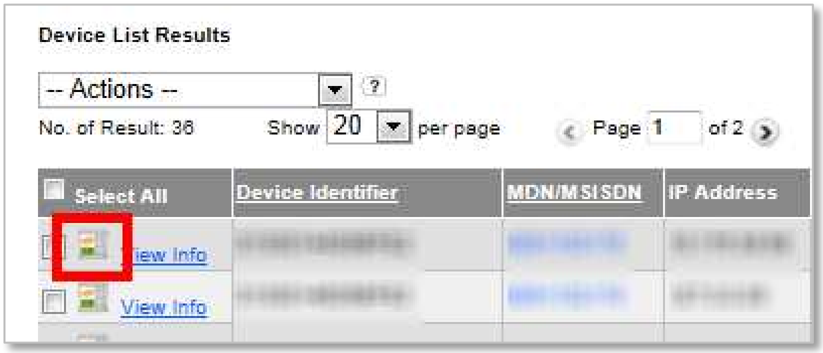


Figure 2-64 Report icon

The Report generation for device pop-up appears:

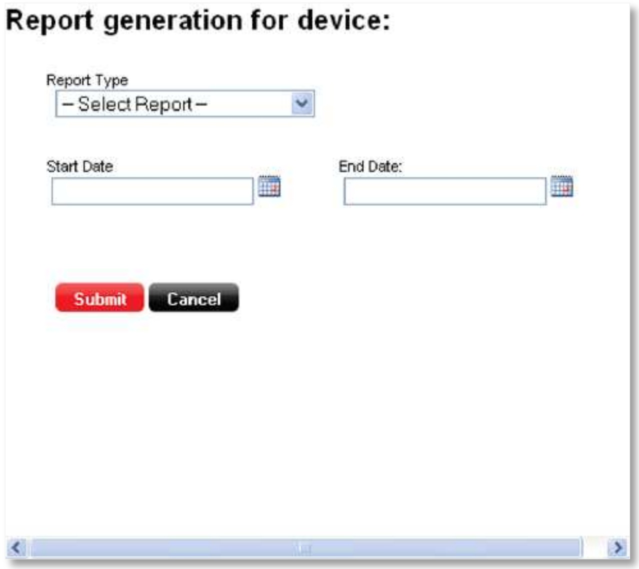


Figure 2-65 Report generation for device pop-up

6. Drop down the Report Type list and choose the report you want to generate.

7. Specify a date range by entering a Start Date and End Date. Note that the Rated Usage Report populates these fields automatically with dates for the selected device's current or most recent bill cycle; consequently, they are hidden.

8. Click Submit to generate the selected report and proceed to the next step; click Cancel to dismiss the pop-up.

9. The selected report screen with your results appears in place of the Report generation for device pop-up. To export the report results, continue to the last step.

   If the report cannot be generated because the result set is too large, you will be given the option to send the report to the Download Center. Click OK to produce a comma-separated values (CSV) file to be generated and sent to the Download Center.

10. Click Export to produce a CSV file and send it to the Download Center. Exported reports include data as it is displayed in your report.

    You will receive emails regarding the export's progress. When the file is ready in the Download Center, you can download it into another application, such as a text editor or spreadsheet.

Generate a Data Usage Trending Chart

Related Information

Reports and Charts Input Criteria

About Device Reports and Graphical Analysis Charts

To generate a Data Usage Trending Chart:

1. On the Navigation menu, move the cursor to the Graphical Analysis tab and select Data Usage Trending Chart from the sub-menu.
2. Specify report criteria. When basic criteria are not sufficient, expand and use the advanced search fields.

NOTE: The Data Usage Trending Chart has the following display parameters:

- **Maximum bars in the histogram: 50**
- **Maximum weeks: 12**
- **Maximum days: 50**
- **Maximum device groups: 7**

3. Click Generate Report. The Data Usage Trending histogram appears at the bottom of the screen.

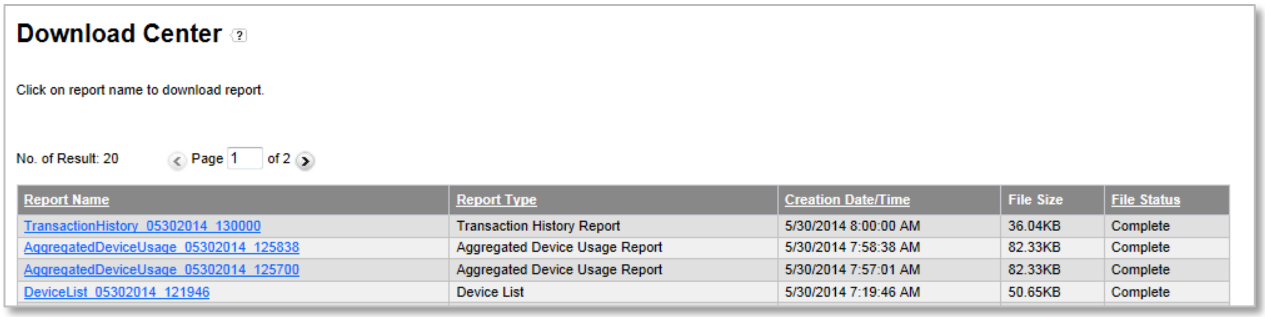
2.8 Retrieve Files from the Download Center

The Download Center stores the lists and reports you export within the M2M Management Center for up to seven (7) days. Some reports that are too lengthy to display on-screen may also be generated as files and made available in the Download Center.

All files in the Download Center are in comma-separated value (CSV) format, which you can open in many types of applications such as text editors and spreadsheets, or use for other application-specific purposes.

To retrieve a file from the Download Center:

1. Navigate to Device Reports > Download Center. The Download Center screen appears; the most recent file is listed at the top:



Download Center

Click on report name to download report.

No. of Result: 20 Page 1 of 2

Report Name	Report Type	Creation Date/Time	File Size	File Status
TransactionHistory_05302014_130000	Transaction History Report	5/30/2014 8:00:00 AM	36.04KB	Complete
AggregatedDeviceUsage_05302014_125838	Aggregated Device Usage Report	5/30/2014 7:58:38 AM	82.33KB	Complete
AggregatedDeviceUsage_05302014_125700	Aggregated Device Usage Report	5/30/2014 7:57:01 AM	82.33KB	Complete
DeviceList_05302014_121946	Device List	5/30/2014 7:19:46 AM	50.65KB	Complete

Figure 2-66 Download Center

2. Find the file you want to download by its report name, which was included in the email you received, and click its link. A browser-dependent Open File dialog appears.

3. Save the file to your computer.

Open a Downloaded File in Microsoft® Excel®

NOTE: Microsoft Excel 2010 was used for this procedure, which may vary when using other versions of the application.

To open a file you downloaded from the M2M Management Center in Microsoft Excel, use the following instructions to ensure it displays correctly:

1. Open Excel, go to the Data tab, and select the From Text option.
2. When the Import Text File window appears, navigate to the downloaded file you saved to your computer and click Import. The Text Import Wizard appears.
3. For Step 1 of the wizard, choose the following options:
   - Delimited
   - Start import at row 1
   - File origin = Windows (ANSI)
4. Click Next to proceed to Step 2 of the wizard.
5. Set the Delimiter to Comma (you may need to unselect Tab) and click Next to go to Step 3 of the wizard.
6. Click anywhere in the following device identifier columns, when applicable, and set them to Text format:
   - Device Identifier
   - MDN/MSISDN
   - ESN
   - MEID
   - IMEI
   - ICCID
7. Click Finish. When the Import Data dialog appears, click the Properties… button.
8. Choose the following properties for the file:
   - Save query definition

- Prompt for file name on refresh
- Adjust column width
- Preserve cell formatting
- Insert entire rows for new data, clear unused cells

9. Click OK on the Properties dialog, then click OK again on the Import Data dialog. The file will open in Excel with identifiers that match the values you see in the M2M Management Center.

2.9 Monitor System Activity in the Master Log

The Master Log displays events that have been logged by the M2M Management Center in addition to the outcome of certain actions. For example, you can check the Master Log for the results of device provisioning, PRL updates and device wakeups.

Populate the Master Log

Related Information

Master Log Search Criteria

Master Log Columns

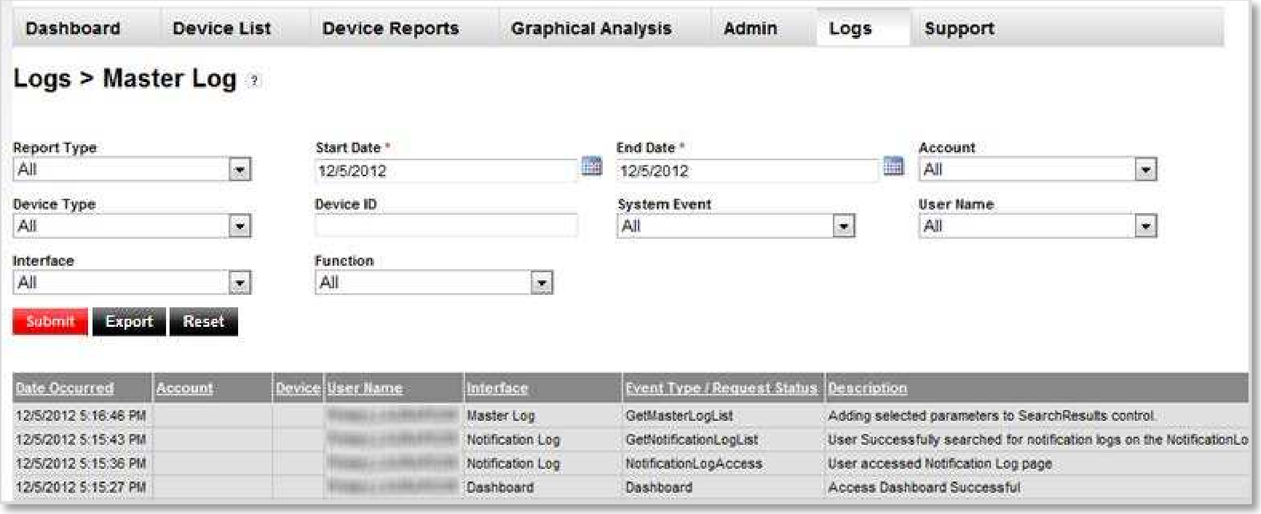
By default, the Master Log displays a list of all user and system events, in the order in which they occurred. To search for specific users and/or events to populate the Master Log:

1. Click the Logs tab and select the Master Log sub-menu command.

NOTE: Search fields on this screen are related to the type of log you want to view. For best results, choose a Report Type, either System Events or User Events. Not specifying a Report Type (accepting the default, "All") may produce unexpected results.

2. Enter values into the search fields, found at the top of the Master Log screen. The more fields you populate, the more targeted your search.

3. Click Submit. The Master Log is generated.



Logs > Master Log

Report Type: All
Start Date *: 12/5/2012
End Date *: 12/5/2012
Account: All
Device Type: All
Device ID:
System Event: All
User Name: All
Interface: All
Function: All

Date Occurred	Account	Device	User Name	Interface	Event Type / Request Status	Description
12/5/2012 5:16:46 PM			[redacted]	Master Log	GetMasterLogList	Adding selected parameters to SearchResults control.
12/5/2012 5:15:43 PM			[redacted]	Notification Log	GetNotificationLogList	User Successfully searched for notification logs on the NotificationLo
12/5/2012 5:15:36 PM			[redacted]	Notification Log	NotificationLogAccess	User accessed Notification Log page
12/5/2012 5:15:27 PM			[redacted]	Dashboard	Dashboard	Access Dashboard Successful

Figure 2-67 Master Log

Export the Master Log

NOTE: To print a Master Log, you must either execute a Print Screen from the keyboard when the report is displayed or export the report to the Download Center, import it into another application such as a text editor or spreadsheet, and print it.

Related Information

Master Log Search Criteria

Master Log Columns

Retrieving Files from the Download Center

To export a Master Log to a CSV file:

1. Click Logs and select the Master Log sub-menu command.
2. To export the entire Master Log as it appears when you first display it, go to Step 5. To export specific events or user actions, continue to the next step.
3. Use the criteria fields at the top of the Master Log screen to filter the log.
4. Click Submit. A filtered version of the Master Log appears at the bottom of the screen.
5. Click Export to generate a CSV file of the log, which will be generated and sent to the Download Center. You will receive emails regarding the file's status.

3 Screen Property Details

The sections that comprise this chapter contain definitions for the fields, controls and list column headings that appear on the screens of the M2M Management Center. When applicable, the Type of the field will be included in a table, to further define the way you interact with a field or control.

Each section provides links to related tasks that make use of the properties. Where applicable, sections also provide links to additional related information.

3.1 Dashboard Properties

Related Tasks

Define a Dashboard Layout

Modify Usage Buckets

3.1.1 Dashboard Select Report Options

Related Information

Wireless Network Services APIs

Accumulated Data Usage Calculation

Current Period

NOTE: Each chart on the Dashboard screen includes one or more "hot spots", which allow you to drill down and view detailed screens and reports depending on the location where you click (see Define a Dashboard Layout **for more information on this feature).**

Dashboard Chart	Description
Device State Status	Reflects the provisioning status distribution among devices.
Active Device Service Plan	Shows the service plan distribution of selected active devices by service plan name. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in this chart.
Active Device Connection Status	Presents the current connection status of selected active devices.
Current Period Data Usage	Reports the number of devices whose accumulated usage falls into each data bucket. Accumulated usage for each device is measured from the last bill cycle date. You can define data buckets, which are data ranges measured and expressed in either MB or KB.
Current Period SMS Usage	Reports the number of devices with accumulated SMS messages that fall into each message bucket. Accumulated SMS messages for each device are measured from the last bill cycle date. You can define SMS message buckets.
Device Carriers	Shows active device breakdown by carrier. Carrier is always Verizon Wireless. NOTE: This feature has limited value as this chart contains only one carrier, Verizon Wireless.
Device Alarm Status	Reports the number of acknowledged and unacknowledged notifications sent to the logged-in user's notification group(s) for each alarm type during the current bill cycle of each device.

Dashboard Chart	Description
None	Do not display a report in the selected position.

3.1.2 Data Usage Bucket Defaults

The M2M Management Center has five pre-defined data usage buckets:

- 0 KB (Empty usage)
- 1 KB to 500 KB
- 501 KB to 1,000 KB
- 1001 KB to 1,500 KB
- 1,501 KB to 2,000 KB
- 2,000+ KB (Implied)

3.1.3 SMS Usage Bucket Defaults

The M2M Management Center has four pre-defined SMS buckets:

- 0 SMS (Empty usage)
- 1 to 5 SMS
- 6 to 15 SMS
- 16 to 25 SMS
- 25+ SMS (Implied)

3.1.4 Dashboard Filters Properties

The Dashboard Filters list is found at the bottom of the Dashboard Setup screen.

Column	Description
Default	Checkmark shown for default filter, which is always selected for all charts the first time you view the Dashboard during an M2M Management Center session. A system default filter named "System Default" is supplied and used until you change it. Only a user with the Customer Admin role is permitted to edit the System Default filter. The name cannot be changed.
Filter Name	Name of Dashboard chart filter.
Device Group	Group of devices on which data is filtered in a corresponding Dashboard chart. NOTE: A device group corresponds to a billing account; therefore, when you filter on device group, you must select the applicable Account on the Dashboard (or All accounts) to populate Dashboard charts with data.
Custom Field 1-5	Value on which data is filtered in a corresponding Dashboard chart. Custom fields are typically used for device identity, type, region, business unit or some other data that further characterizes a device. NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).
Options	Hyperlinks to actions you can perform on filters, including Edit and Delete. Delete is not an option for the System Default filter.

3.1.5 Create Filter and Edit Filter Properties

Label	Type	Description
Filter Name	Entry field	Name assigned to Dashboard chart filter. Up to 32 alphanumeric characters are allowed and the name must begin with an alphabetic character. "System Default" is a reserved name and cannot be used.
Default	Checkbox	Check to designate the filter as the default, which is selected for all Dashboard charts when you view the Dashboard for the first time during a session until you change the filter for a report. Uncheck this control if you do not want the filter to be the default. Only one default filter is permitted. The system default filter (named "System Default") is used until you designate a new default. Only a user with the Customer Admin role can edit the System Default filter; the System Default filter cannot be deleted.
Device Group	Drop-down	Select the group of devices on which to filter data for one or more Dashboard chart(s). NOTE: A device group corresponds to a billing account; therefore, when you filter on device group, you must select the applicable Account (or All accounts) on the Dashboard to populate Dashboard charts with data.
Custom Field 1-5	Entry field	Enter the value on which to filter data for one or more Dashboard chart(s). Custom field values can be up to 50 characters in length; some special characters are accepted (see the list of acceptable characters in Assign Custom Fields to Devices). NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).
Save	Button	Click to write the filter information to the database. A saved filter will appear in the Filter List on the Dashboard Setup screen and it will be listed in all filter selection controls on the Dashboard.
Cancel	Button	Click to dismiss the pop-up and return to the Dashboard Setup screen without adding a new filter or modifying an existing filter.

3.2 View Properties

Related Tasks

Edit or Delete a View

Create a View

Label	Type	Description
All View Screens		
View Name	Entry field	Name assigned to custom view of Device List or report. Up to 32 alphanumeric characters are allowed and the name must begin with an alphabetic character.
View Description	Entry field	Description of custom view for Device List or report. Up to 256 characters are allowed.
Default	Checkbox	Check to select the view as the default, which displays when you access the screen for the first time during a session until you change the view. Uncheck this control if you do not want the view to be the default. Only one default per screen is allowed. A system default named "System Default" is used until you select a new default. Only a user with the Customer Admin role can edit the System Default view; the name cannot be changed.

Label	Type	Description
Delete View	Button	Click to remove the selected view from the drop-down list on the Device List or report screen.
Device List and Reports View Screens		
Available Fields	List box	List of fields eligible for the view you are designing. You can use standard selection techniques to choose multiple fields in this list box.
Add to List	Button	Select one or more “Available Fields” and click to move your selection(s) to the “Selected Fields” list box, thus making the column(s) visible in the view.
Delete from List	Button	Select one or more “Selected Fields” and click to move your selection(s) to the “Available Fields” box, thus removing the column(s) from your view.
Selected Fields	List box	Fields chosen to be part of the view. You can use standard selection techniques to choose multiple fields in this list box. NOTE: The Device Identifier field must be part of every view and cannot be deleted from this list box.
Move Up	Button	Select one or more “Selected Fields” and click to move them up one position in the order, which causes the column(s) to appear further to the left in the grid when it is displayed.
Move Down	Button	Select one or more “Selected Fields” and click to move them down one position in the order, which causes the column(s) to appear further to the right in the grid when it is displayed.
Usage Units	Drop-down	Select the units in which to display usage on the report. NOTE: Appears only on the Create View and Edit/Delete View windows for reports that include usage.
Data Usage Trending Chart View Screens		
X-Axis Units	Drop-down	Select the Time unit for the chart view. The chart can display up to 50 days or 12 weeks of data.
Y-Axis Units	Drop-down	Select the Usage unit for the chart view.
Group By	Drop-down	Select the grouping method for the chart view: All aggregates usage for all devices and displays one bar per time unit; Device Groups displays a separate bar per time unit for each group in the selected account. The chart can display up to seven (7) device groups per time unit. When you have more than seven device groups in an account, select All for this option or an error message will be displayed instead of the chart.

3.3 Device Properties

Related Task

Upload Attributes for Devices by Screen Entry

3.3.1 Fields for Device Screen Entry

Label	Type	Description
ESN	Entry field	Electronic Serial Number of 2G/3G device to update. NOTE: + Only one type of device identifier is accepted. + Use either Decimal or Hexadecimal format for your entry.
MEID	Entry field	Mobile Equipment Identifier of 2G/3G device to update. NOTE: + Only one type of device identifier is accepted. + Use either Decimal or Hexadecimal format for your entry.
IMEI	Entry field	International Mobile Equipment Identifier of 4G device.
ICCID	Entry field	Integrated Circuit Card Identifier of 4G device.
Device Group	Drop-down	Optionally select the device group to associate with the device.
Custom Field 1-5	Entry field	Optionally enter up to five custom attributes to associate with the device. Custom field values can be up to 50 characters in length; some special characters are accepted (see the list of acceptable characters in Assign Custom Fields to Devices). NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).

3.4 Device List Properties

NOTE:

Improvements have been made to display Device Lists in the M2M Management Center. As a result, when you first enter the Device List screen, it displays all devices in the selected account as an unsorted list.

In addition, we suggest using the following tips when working with lengthy Device Lists:

- **Limit sorting and/or filtering to the following columns:**
  - **Account**
  - **Device Identifier**
  - **MDN/MSISDN**
  - **Custom Fields**
  - **MEID, ESN, IMEI, or ICCID**
  - **Device Status**
  - **Activation Date (filter using a range composed of Start and End Dates)**

- **Activated By**
- **Connection Status**

Related Tasks

Find Devices by Filtering

Display Device Details

Export Device Data

Create a Device Group from the Device List

Navigate to Provisioning Actions for a Single Device

Navigate to Provisioning Actions for Multiple Devices

Assign Custom Fields to Device

Assign Custom Field Labels

Update the PRL of One or More Non-Grouped Devices Remotely

Wake Up One or More Non-Grouped Devices

Generate a Single-Device Report from the Device List Screen

Related Information

Wireless Network Services APIs

3.4.1 Device List Search Fields

Search Criterion	Type	Description
Default Search Fields		
Account	Drop-down	List of billing accounts to which you have access; All encompasses data and devices for all accessible billing accounts.
Device Identifier	Entry field	MEID, ESN, IMEI or ICCID of device. MEID stands for Mobile Equipment Identifier, a globally unique number used to identify a physical piece of mobile station equipment. ESN stands for Electronic Serial Number, and is another method of uniquely identifying a mobile device. IMEI stands for International Mobile Equipment Identity and is used to uniquely identify a 4G device. ICCID stands for Integrated Circuit Card Identifier, which is imprinted on the SIM (Subscriber Identity Module) card in a 4G device. NOTE: As of the December 2013 release, you can enter ESN and MEID identifiers in either Decimal or Hexadecimal format.
MDN/MSISDN	Entry field	Ten-digit phone number of 2G/3G device. MDN stands for Mobile Directory Number. Fifteen-digit number assigned to 4G device. MSISDN stands for Mobile Station International Subscriber Directory Number.
Device Group	Drop-down	Group with which device is associated.
IP Address	Entry field	Internet Protocol address assigned to device.

Search Criterion	Type	Description
Custom Fields 1 - 5	Entry field	Data used to filter devices. Custom fields are typically used for device identity, type, region, business unit or some other data that further characterizes a device. NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels). They are always found just above the Advanced Search control (four fields on top deck; one field on bottom deck).
Advanced Search Fields		
MEID	Entry field	MEID of device. NOTE: You can use either Decimal or Hexadecimal format for your entry.
ESN	Entry field	ESN of device. NOTE: You can use either Decimal or Hexadecimal format for your entry.
IMEI	Entry field	IMEI of 4G device. This field accepts up to 16 alphanumeric characters.
ICCID	Entry field	Integrated Circuit Card Identifier associated with 4G device's SIM (Subscriber Identity Module) card. This field accepts up to 20 alphanumeric characters.
Device Status	Drop-down	+ ALL—Show all devices, regardless of status. + ACTIVE—Show only active devices. Active devices are enabled to use the wireless network. + DEACTIVE—Show only deactivated devices. Deactivated devices are no longer provisioned for M2M Management Center services, although they can be enabled for another purpose on the Verizon Enterprise Network. + SUSPEND—Show only suspended devices. Suspended devices are not currently enabled to use the wireless network.
Activation Date Range	Entry field/Date pop-up	A starting date in the field at the left and an ending date in the field at the right specify a date range during which a device was activated.
Activated By	Drop-down	Name of user who activated device.
Deactivated By	Drop-down	Name of user who deactivated device.
Carrier	Drop-down	Wireless network carrier; list contains ALL and Verizon Wireless; however, both options return the same results as Verizon Wireless is the only carrier.
Connection Status	Drop-down	+ ALL—Include all devices regardless of connection status. + Connected—Show only devices that have a current radio or data session on the wireless network. + Disconnected—Show only devices that do not have a radio or data session on the wireless network.
Service Plan	Drop-down	Name of service plan assigned to the selected device.
Pending Action	Drop-down	Device provisioning action that was requested by a custom application using a Wireless Network Services API, but the request has not yet been processed. Includes the following: + ALL + Pending Activation + Pending Deactivation + Pending ESN/MEID Change

Search Criterion	Type	Description
		+ Pending MDN Change + Pending Resume + Pending Service Plan Change + Pending Suspend
BSID	Entry field	Base Station Identifier, which is the servicing point of attachment for the device. NOTE: The BSID is a concatenation of SID (2 octets) + NID (2 octets) + Cell Identifier Type 2 (2 octets). In the Cell Identifier Type 2, the 12 upper bits are Cell ID and the 4 lower bits are Sector. Each item is encoded u sing hexadecimal uppercase ASCII characters. For example, the BSID 005F00BD1803 denotes: SID: 005F (95) NID: 00BD (189) Cell Identifier Type 2: 1803 (6147) Cell ID: 180 (384) Sector: 3 (3)
Diagnostics-Enabled	Drop-down	NOTE: This command is only available when your organization has the Device Diagnostics feature. + ALL—Include all devices regardless of diagnostics capability. + Enabled—Show only Verizon Advanced M2M devices with diagnostics capability. + Not Enabled—Show only devices that do not have diagnostics capability; this list may include Verizon Advanced M2M devices.

3.4.2 Device List Results

The Device List shows all devices that meet your criteria. For many tasks, you can choose multiple devices. When you regularly perform tasks for the same devices, consider creating a device group (see one of the following tasks: Create a Device Group from the Device List or Create a Device Group from the Admin Tab).

NOTES:

- **The results displayed and the order in which they appear are dependent on the view selected. The table below lists all possible fields that can be displayed in a Device List. Fields are listed in alphabetic order following the descriptions of the controls that are part of the list. Columns that are part of the System Default view are in bold text.**
- **Custom fields will display alternative labels when custom labels have been assigned (see Assign Custom Field Labels).**

Column Heading/ Control	Description
□ Select All	Check this box to mark all checkboxes in the left-most column and select all devices on the current Device List page; uncheck this box to empty all checkboxes in the left-most column and deselect all devices on the current Device List page.
📊	Click the Report icon to view report options and generate reports for a single device.
View Info	Click this link to display the Device Information pop-up.
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.

Column Heading/ Control	Description
Account	Billing account with which device is associated.
Activation Date	Most recent activation date and time of M2M Management Center services (expressed in the time zone selected for the current contact), when applicable.
Billing Cycle End Date	Last day of device's current bill cycle.
BSID	Base Station Identifier, which is the servicing point of attachment and used to approximately locate a device. NOTE: The BSID is a concatenation of SID (2 octets) + NID (2 octets) + Cell Identifier Type 2 (2 octets). In the Cell Identifier Type 2, the 12 upper bits are Cell ID and the 4 lower bits are Sector. Each item is encoded using hexadecimal uppercase ASCII characters. For example, the BSID 005F00BD1803 denotes: SID: 005F (95) NID: 00BD (189) Cell Identifier Type 2: 1803 (6147) Cell ID: 180 (384) Sector: 3 (3)
Carrier	Wireless network carrier; list contains only Verizon Wireless.
Connected	One of two graphical indicators of a device's connection state: ● Connected—Device has a current radio or data session on the wireless network. ✗ Disconnected—Device does not have a radio or data session on the wireless network.
Custom Fields 1 to 5	Data that is used to filter devices. Custom fields typically contain data like device type, region, business unit or some other information that further characterizes a device. NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).
Device Group	Name of group with which device is associated.
Device Identifier (ID)	MEID or ESN of 2G/3G device; IMEI or ICCID of 4G device.
Device Status	+ ACTIVE—Devices are enabled to use the wireless network. + DEACTIVE—Devices are no longer provisioned for M2M Management Center services, although they can be enabled for another purpose on the Verizon Enterprise Network. The date the device was deactivated is also displayed. + SUSPEND—Devices are not currently enabled to use the wireless network.
Diagnostics	NOTE: This column is only displayed when your organization has the Device Diagnostics feature. One of two graphical indicators showing whether or not a Verizon Advanced M2M device has a resident client with diagnostics capability: ✓ Advanced M2M device has a resident client with diagnostics capability. ✗ Device does not have a resident client with diagnostics capability.

Column Heading/ Control	Description
ICCID	ICCID of 4G device's SIM.
IMEI	IMEI of 4G device.
IP Address	Internet Protocol (IP) address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number of 2G or 3G device/15-digit number assigned to 4G device.
Pending Action	Indicates that a device provisioning action has been requested by a custom application using a Wireless Network Services Application Programming Interface (WNS API), but the request has not yet been processed. For example, a device Suspend request has been submitted, but the actual suspension of the device is still pending. This column shows "Not Available" for changes requested by a Verizon Wireless My Business Account or Verizon Enterprise Center user.
Scheduled Resume Date	Date when service is scheduled to automatically resume for a device in the Suspend state. The Verizon Enterprise Network passes this date to the M2M Management Center for devices suspended using one of the following methods: + System automatically suspends rogue device + Customer employs a Wireless Network Services API to suspend device When the network does not provide this date, this column displays "Not Available" for the suspended device. For devices in other states, this column is empty.
Service Plan	Service plan of the selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in the Device List.

3.4.3 Device Information Pop-Up Properties

Related Tasks

Display Device Details

Label	Description
Device Identifier	MEID or ESN of 2G/3G device; IMEI or ICCID of 4G device.
MDN/MSISDN	Ten-digit phone number of 2G or 3G device/15-digit number of 4G device.
IP Address	Internet Protocol (IP) address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
Account Name	Number assigned to identify billing account.

Label	Description
Billing Account Number	Number assigned to identify billing account (same as previous field).
Status	Active, Deactive or Suspend. When Deactive, a Deactivation Date is also given.
Pending Action	Populated with "Not Available" when device-state change action initiated from Verizon Wireless My Business Account or Verizon Enterprise Center; for actions initiated with Wireless Network Services (WNS), populated with "Pending <State>." <State> reflects the action requested.
Activation Date	Most recent activation date and time for M2M Management Center services (expressed in the time zone selected for the current contact), when applicable.
Activated By	Always displays "Verizon User."
Deactivation Date	Most recent deactivation date and time for M2M Management Center services (expressed in the time zone selected for the current contact), when applicable.
Deactivated By	Always displays "Verizon User."
PRL Version	Applies to 2G/3G devices only: Displays "Retrieving" when you first display the pop-up until the PRL version is obtained from the Verizon Enterprise Network, at which time the device's current PRL version appears. When the PRL version is unavailable for a device, this field displays the message "Not available – please try again later".
Service Plan	Service plan for the selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in this pop-up.
Device Group	Name of group with which device is associated.
Promotion Start Date*	Date on which current promotional package applied to the device took effect.
Promotion Scheduled End Date*	Date on which the current promotional package is scheduled to end.
Data Promotion*	The current data usage promotion applied to the selected device.
SMS Promotion*	The current SMS usage promotion applied to the selected device.
Voice Promotion*	The current voice promotion applied to the selected device.
Custom Fields	Up to five optional custom fields used to describe a device. Up to 50 alphanumeric and/or special characters can represent device identity, region, business unit, device type, etc. NOTE: These fields will display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).
Last Connect Date	Last date and time the device started a radio/data session with the wireless network. Time is displayed in the time zone selected for the current contact.
Last Disconnect Date	Last date and time the device was disconnected from the wireless network. Time is displayed in the time zone selected for the current contact.
Connection Status	Indicates the device's state on the wireless network: + Connected—Device has a current radio or data session on the wireless network. + Disconnected—Device does not have a radio or data session on the wireless network.
Customer Name†	Name of customer who owns the device.

Label	Description
Customer Address†	Street address of customer who owns the device.
Customer City†	City of customer who owns the device.
Customer State†	State of customer who owns the device.
Customer Zip Code†	Zip Code of customer address.
Service Zip Code†	Zip Code supplied when device was activated, which usually denotes the device's location.
Lead Identification Number†	Identification of lead salesperson associated with the customer.

* NOTE:

+ All promotion-related fields are shown only when a device has at least one current promotion applied to it. A device may have one to three promotions (data, SMS, and voice) applied at any time.
+ Because the data in this field is updated once per day, promotional details may appear up to 24 hours after a promotion has started.

† NOTE: These fields appear only for certain customers in Verizon partner programs. They are synchronized with the Verizon Partner Relationship Management (PRM) application.

3.4.4 Diagnostic Summary Data

Related Task

Display Diagnostic Information for a Device

The Diagnostic Summary will display the following data for any selected device:

Label	Description
Current Session-Network Attribute Group	
Start Record Time	Time when current connected session started.
NAS IP Address	IP address of Network Access Server employed during current session.
Framed (Device) IP Address	IP address used by device during current session.
Home Agent IP Address	IP address of home agent used during current session.
BSID	Identifier of base station being used by the current session.
3GPP2 Service Option	Standard 3GPP2 service option employed by the current session, when applicable.
Last Completed Session-Network Attribute Group – Start Record	
Start Record Time	Time when last complete connected session started.
NAS IP Address	IP address of Network Access Server employed during last complete connected session.
Framed (Device) IP Address	IP address used by device during last complete connected session.
Home Agent IP Address	IP address of home agent used during last complete connected session.
BSID	Identifier of base station being used at the start of the last complete connected session.
3GPP2 Service Option	Standard 3GPP2 service option employed at the start of the last complete connected

Label	Description
	session, when applicable.
Last Completed Session-Network Attribute Group – Stop Record	
Stop Record Time	Time when last complete connected session ended.
NAS IP Address	IP address of Network Access Server employed during last complete connected session.
BSID	Identifier of base station being used at the end of the last complete connected session.
3GPP2 Service Option	Standard 3GPP2 service option employed at the end of the last complete connected session, when applicable.
Acct-Input-Octets	Number of octets received during last complete connected session.
Acct-Output-Octets	Number of octets sent during last complete connected session.
Bad PPP Frame Count	Number of bad frames sent using Point-to-Point Protocol during last complete connected session.
Acct-Terminate-Cause	Indicates how the last complete session ended.
Release Indicator	Reason for sending the stop record of the last complete connected session.

The Diagnostic Summary will include the following data for Advanced M2M devices with Device Diagnostics capabilities. Only the attribute groups with data to display will be included in the summary.

Label	Description
Device Attribute Group	
Device Description	Textual description of device.
Serial Number	Device identifier.
HW Version	Hardware version associated with device.
SW Version	Version of software installed on device.
Modem Attribute Group	
Modem Description	Textual description of modem.
Serial Number	Modem identifier (ESN, MEID, IMEI, etc.).
HW Version	Hardware version associated with modem.
SW Version	Version of software installed in modem.
RF Attribute Group	
RF Technology	Radio access technology (CDMA, EVDO, GSM, EDGE, UMTS, LTE).
Signal Strength (dBm)	Strength of signal, expressed in dBm.
Signal Quality (dB)	Quality of signal, expressed in dB.
RF Operator	Network operator identifier (SID-NID, MCC-MNC).
Roaming Ind	Roaming indicator.
Disconnect Reason	Reason for disconnect.

Label	Description
Memory Attribute Group	
KB RAM Remaining	Number of KB of memory left.
MB Internal Remaining	Number of MB remaining on internal storage media.
MB External Remaining	Number of MB remaining on external storage media.
Watchdog Attribute Group	
Watchdog Type	Watchdog that expired (0=DCF).
Block Attribute Group	
Application Block Reason	Application blocking reason: + 0=no service + 1=roaming + 2=RF
Data Connection Attribute Group	
Failure Code	Code of data connection authentication failure.

3.5 Device Group Properties

Related Tasks

Create a Device Group from the Device List

Create a Device Group from the Admin Tab

Edit a Device Group

Delete a Device Group

Update the PRL for All Devices in a Device Group Remotely

Wake Up All Devices in a Device Group

3.5.1 Device Group List

Column Heading	Description
Account	Billing account with which device groups in the list are associated.
Device Group Name	Descriptive name for device group.
Default	Checkmark in this column denotes the default device group. The default device group is automatically created at account setup and initially, it contains all devices. Whenever you delete a device group, all devices return to the default group.
Description	Additional description to define the content or characteristics of a device group.
Actions	Drop-down list of actions that can be performed for the device group, including: + Edit + Delete (appears for all except the Default device group)

Column Heading	Description
	+ Remote PRL Update + Wakeup

3.5.2 Create/Edit Device Group from the Admin Tab

Label	Type	Description
Account	Drop-down	Billing account with which devices you want to assign to a group are associated.
Device Group Name	Entry field	Descriptive name for device group; field accepts up to 100 alphanumeric characters.
Description	Entry field	Additional description to define the content or characteristics of a device group; field accepts up to 255 alphanumeric characters.
Assign devices from	Drop-down	List of device groups from which to choose devices for a new group, or group from which devices were last selected for an existing group.
Device Properties		
Device Identifier		MEID or ESN of 2G/3G device; IMEI or ICCID of 4G device.
MDN/MSISDN		Ten-digit phone number of 2G or 3G device/15-digit number assigned to 4G device.
Device Status		ACTIVE, DEACTIVE or SUSPEND, displayed in the colors green, red and yellow, respectively.
Service Plan		Service plan of the device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of “M2M” or “M2M_CPN” (when you have the Customer Private Network option) will continue to appear for devices.
Carrier		Carrier is always Verizon Wireless.

3.6 Contact Properties

Related Tasks

Search for a Contact

Add an Alerts Only Contact

Edit a Contact Record

Delete an Alerts Only Contact

Related Information

System Users

User Role Access Permissions

3.6.1 Contact Search Criteria

Search Criterion	Type	Description
Last Name	Entry field	Last name associated with a contact's login name. Leave blank to find all contacts (no wildcard is needed in this field). Enter a full last name or partial name to find matching contacts. For example, you can enter "Smith" to find contacts with a last name of "Smith" or starting with the letters "Smith", or you can enter "S" to find contacts with last names starting with the letter "S."
Organization	Drop-down	Select the company with which the contact is associated.
Account	Drop-down	Select an available billing account. Accounts are used to organize data and devices.
Status	Drop-down	+ All—Finds both Active and Inactive contacts. + Active—Display only Active contacts, who can receive notifications. + Inactive—Display only inactive contacts, who cannot receive notifications until re-activated.
User Role	Drop-down	Constrains a search to find only those users who are assigned to a particular security role, such as an Admin role, Operator role, or Alerts Only role.

3.6.2 Contact List

Column Heading	Description
Name	Last name, first name of contact.
Organization	Company with which contact is associated.
User Role	Role assigned to contact.
Status	Contact's status, either Active or Inactive.
Options	Links to actions in this column depend on the user's role. The column can contain the following links: + Edit Contact + Delete Contact

3.6.3 Add/Edit Contact

NOTES:

The following rules apply to the fields on the Add/Edit Contact screen:

- **You can specify and modify the phone-related fields (including SMS), plus the Time Zone and Portal Landing Page fields only for M2M Management Center users. These fields remain populated and do not get overwritten by data from Verizon Wireless My Business Account or Verizon Enterprise Center.**
- **More contact fields are displayed on the Add/Edit Contact screen; however, they cannot be edited for M2M Management Center users. Any modifications you make to other fields on the Contacts screen (e.g., name fields, Email, etc.) will be overwritten with information from the Verizon Wireless My Business Account or Verizon Enterprise Center the next time that contact accesses the M2M Management Center.**
- **All fields displayed for Alerts Only contacts can be edited and will not be overwritten.**

Related Information

System Users

User Role Access Permissions

Label	Type	Description
Organization	Display only	The company with which the contact is associated, carried over from the Notification Group Setup screen.
User Role	Display only	The contact's role as assigned by Verizon My Business or Verizon Enterprise Center, or Alerts Only. NOTE: Contacts with the Alerts Only user role do not have access to the M2M Management Center; they only receive notifications.
Active	Checkbox	Indicates whether the contact is active and able to receive notifications. This box is checked by default. Uncheck the box to make the contact inactive for the notification feature. Inactivating a contact is useful when you want to revoke a user's privilege to receive notifications in the M2M Management Center without deleting the user's record.
Description	Entry field	Free form text describing the contact.
First Name/Last Name	Entry fields	Contact's name; The Last Name and First Name fields are required; however, a space is considered a valid entry in both fields. The entries in these fields display as the Contact at the upper right corner of every M2M Management Center screen when the contact is a system user.
Middle Name	Entry field	Contact's middle name; this field is optional.
Title	Entry field	Optional job title of contact.
Email	Entry field	Required email address of contact, which may be used for notification alerts when the notification feature is active.
SMS	Entry field	Contact's Short Message Service (SMS) email address, which is one way to receive notifications. For this field, enter a US phone number in the identifier field and a US carrier text messaging domain in the domain field, such as 8585550000@vtext.com.
Phone/Cell Phone	Entry fields	Optional 10-digit phone numbers (US format) associated with contact.
Time Zone	Drop-down	Required time zone selection that corresponds to the contact's location. This time zone value is used to convert timestamps registered and displayed by the M2M Management Center to the contact's local time.
Portal Landing Page	Drop-down	M2M Management Center screen to display when you click a "Machine to Machine" link in a Verizon Wireless My Business Account or Verizon Enterprise Center Web portal (refer to Accessing the M2M Management Center). Your choices are: + Dashboard (default) + Device List + Device Usage Report + Aggregated Device Usage Report + Connected Session History Report + Connection History Report + Notification Log

3.7 Notification Group Properties

Related Tasks

Create a Notification Group

Edit a Notification Group

Delete a Notification Group

3.7.1 Notification Group Search Criteria

Search Criterion	Type	Description
Account	Drop-down	Select an available billing account. Accounts are used to organize data and devices.
Group Name	Entry field	Name of the notification group.
Status	Drop-down	+ All—Show both Active and Inactive notification groups. + Active—Show only Active notification groups, which are eligible to receive notification alerts. + Inactive—Show only Inactive notification groups, which are set to not receive notification alerts.

3.7.2 Notification Group List

Column Heading	Description
Account	Account associated with notification group.
Notification Group	Name of notification group.
Active	+ Active—Group is eligible to receive notification alerts. + Inactive—Group is not eligible to receive notification alerts.
Options	Links to actions in this column depend on your user role and can include: + Edit—You are authorized to edit the notification group. + Delete—You are authorized to remove the group from the database.

3.7.3 Add New/Edit Notification Group

Label	Type	Description
Account	Drop-down	Select an available billing account. Accounts are used to organize data and devices.
Notification Group Name	Entry field	Name of the notification group; up to 40 characters are allowed.
Active	Checkbox	Check the Active checkbox to make the group eligible to receive notifications. Uncheck the Active checkbox to remove the notification group from eligibility to receive alerts. Inactivating a notification group is useful when you want to stop sending alerts to a particular group without deleting the group entirely.
Description	Entry field	Description of the notification group; up to 100 characters are allowed.

Label	Type	Description
Contact	Drop-down	Select a contact to add to the group, or select Add New Contact to go to the Add/Edit Contact screen and create an Alerts Only contact. When you select a contact from the list or return from adding an Alerts Only contact, the Notification Method field appears.
Notification Method	Drop-down	How to send alerts to the contact displayed at the left. Choices include Email and SMS.

3.8 Notification Properties

Related Tasks

Create a Notification Rule

Edit a Notification Rule

Delete a Notification Rule

Related Information

Wireless Network Services APIs

3.8.1 Notification Properties

Column Heading	Description
Enabled	Graphical indicator of the status of a notification: ✓ The notification rule is enabled. ✗ The notification is not enabled.
Alarm Name	Name of the notification rule.
Description	Free-form description of the notification rule.
Notification Group	Hyperlink to Notification Group Setup screen, which displays the details of the group set to receive this notification alert when it is sent.
Options	Links to actions in this column depend on your user role and can include: + Edit—You are authorized to edit the notification. + Delete—You are authorized to remove the notification from the database.

3.8.2 Add New/Edit Notification

Label	Type	Description
Alarm Name	Entry field	Name of the notification rule. Up to 50 characters are permitted in this field.
Enabled	Checkbox	Check to activate the notification rule. Uncheck to disable the notification rule. Disabling a notification is useful when you want to stop sending an alert when the rule's condition is met without deleting the notification rule altogether.

Label	Type	Description
Notification Group	Drop-down	Select the group of users to receive this notification alert when it is sent. NOTE: To set up a notification group on-the-fly, click the plus sign (+) button and refer to the task Create a Notification Group.
Device Group	Drop-down	Optionally choose the group of devices that affect the triggering of this notification alert. NOTE: The “Aggregate of Alarms” alarm category requires you to choose a device group.
Alarm Category	Drop-down	Choose one of the following categories to filter the available Alarm Types (Alarm Types are listed under each category below): + Account Maintenance ▪ Activate ▪ Deactivate ▪ Service Plan Change ▪ Suspend ▪ Resume ▪ Auto Resume ▪ IMEI Change + Usage ▪ Usage ▪ Rogue Device + Network ▪ BSID Change ▪ Abnormal Disconnect + Aggregate of Devices ▪ Usage in KB ▪ No. Resume Requests ▪ No. Activate Requests ▪ No. Deactivate Requests ▪ No. Change Service Plan Change Requests ▪ No. Suspend Requests

Label	Type	Description
Alarm Type	Drop-down	Account Maintenance Alarms + Activate†∞—Generate a notification whenever service for a device is activated. + Deactivate †∞—Generate a notification whenever service for a device is deactivated. + Change Service Plan†∞—Generate a notification whenever a service plan for a device is changed. + Suspend †∞—Generate a notification whenever service for a device is suspended. + Resume †∞—Generate a notification whenever service to a device is resumed. + Auto Resume—Generate a notification seven (7) days before service to a suspended device is set to be automatically restored according to network rules. + IMEI Change†– Generate an email notification whenever the system detects a change to the IMEI of a 4G device, including when the IMEI value changes to null. Usage Alarms + Usage†—Generate a notification based on a data usage threshold. + Rogue Device*†—Automatically suspend a device that accumulates data usage greater than a specified number of KB per monthly bill cycle. Network Alarms + BSID Change†—Generate a notification or generate a notification and suspend the corresponding device whenever the BSID of a 3G device changes. + Abnormal Disconnect — Generate a notification whenever a device loses its connection unexpectedly. Aggregate of Devices Alarms + Usage in KB*—Generate a notification based on a data usage threshold. + No. of Resume Requests*—Generate a notification based on a number of resume service requests made over a specific period. + No. of Activate Requests*—Generate a notification based on a number of activation requests made over a specific period. + No. of Deactivate Requests*—Generate a notification based on a number of deactivation requests made over a specific period. + No. of Service Plan Change Requests*—Generate a notification based on a number of service plan change requests made over a specific period. + No. of Suspend Requests*—Generate a notification based on a number of suspend service requests made over a specific period. NOTES: + Alarm types marked with an asterisk (*) are threshold-triggered alarms for which you specify Alarm Criteria (see next row). + Alarm types marked with a cross (†) apply to single-device actions + Alarm types marked with the infinity symbol (∞) can be configured to generate notifications at different times in the device state change cycle. See the “Notify on” options below. + To receive alerts when service to a device is resumed by a Verizon Enterprise Network system either manually or automatically, you must choose the “Notify on Confirmation” option (explained below).

Label	Type	Description
		+ Auto Resume only: This notification is generated only when devices are suspended using the following methods: User selects Suspend command from Device List or Device Group List System automatically suspends rogue device Customer employs a Wireless Network Services API to suspend device
Alarm Criteria (three unlabeled fields)	Drop-down Entry field Drop-down	For threshold-triggered alarm types, you must specify the following: + Comparison operator—Choices include Greater than (>) or Less than (<). Less than (<) applies only to non-aggregated thresholds. + Comparison value—Number of KB that, when exceeded or not reached, will trigger the notification to be sent or action to be taken. + Time period—DAILY, WEEKLY or MONTHLY.
Action	Drop-down	Accompanies the BSID Change trigger: Select whether you want to Email only or Email and Suspend a device when it experiences a change to this identifier.
"Notify On" Options	Radio button	Select the time in the device-state change cycle at which you want to generate a notification: + Notify on Request—Trigger notification when the M2M Management Center receives a state change request. + Notify on Confirmation—Trigger notification when system retrieves a successful reply, after the device-state change has been fully processed by both the M2M Management Center and the Verizon Enterprise Network. This is the default selection. + Notify on Failure—Trigger notification when system retrieves a failure status from the database, after the device state change has been fully processed by both the M2M Management Center and the Verizon Enterprise Network.

3.9 Notification Log Properties

Related Task

View and Acknowledge Notifications

3.9.1 Notification Log Search Fields

Search Criterion	Type	Description
Account	Drop-down	Select an available billing account. Accounts are used to organize data and devices.

Search Criterion	Type	Description
Trigger	Drop-down	Service Provisioning Action Triggers + Activate –Sent any time a device is activated. + Deactivate – Sent any time a device is deactivated. + Service Plan Change– Sent any time the service plan for a device is changed. + Suspend – Sent any time service for a device is suspended. + Resume – Sent any time service for a device is resumed. + No. of Activate Requests – Sent when a certain number of activation requests are made within a specific timeframe. + No. of Deactivate Requests – Sent when a certain number of deactivation requests are made within a specific timeframe. + No. of Service Plan Change Requests - Sent when a certain number of service plan change requests are made within a specific timeframe. + No. of Suspend Requests – Sent when a certain number of suspend service requests are made within a specific timeframe. + No. of Resume Requests – Sent when a certain number of resume service requests are made within a specific timeframe. Network-related Trigger + Abnormal Disconnect – Sent when a device's connection is severed unexpectedly. Usage Triggers + Usage in KB – Sent when a data usage threshold is breached by grouped devices (see About Notifications). + Usage – Sent when a data usage threshold is breached by a single device (see About Notifications). + Rogue Device Value Change Triggers + BSID Change – Sent when a device's Base Sector Identifier changes, which indicates that the device's location has changed. + IMEI Change – Sent when a 4G device's IMEI value is changed.
Start Date	Entry field/Date pop-up	This field and the next, End Date, define a date range for notifications to include in the log.
End Date	Entry field/Date pop-up	This field and the Start Date field define a date range for notifications to include in the log.
Acknowledge Status	Drop-down	+ All + Acked (Acknowledged) + UnAcked (Unacknowledged)

3.9.2 Notification Log Results

Related Information

Acknowledgement and Resend Logic

Column Heading	Description
Status	One of the following symbols, which indicate whether a notification has been acknowledged or not: 🟡 Notification was acknowledged. 🔴 Notification was not acknowledged.
Account	Billing account associated with the alarm type.
Notification	Type of event that triggered the alert.
Notification Group	Group of users to which the notification was sent. When you are not a Customer Admin user, this column displays only groups to which you belong. Customer Admin users see all notification groups.
Date Sent	Date and time (expressed in the time zone selected for the current contact) at which the notification was sent.
Ack Date	Date on which the notification was acknowledged.
Device	Identifier of the device (MEID, ESN, IMSI, or ICCID) that triggered the notification.
# of Notifications	Number of notifications sent (max = 4). When a notification is not acknowledged, the system will generate and resend the notification every hour, up to four total (or three additional) times.
Options	Click the Acknowledge link to change the notification's state from UnAcked to Acked. The symbol in the Status column changes from red to yellow.

3.10 Report and Chart Properties

Related Tasks

Generate a Report for One or More Devices

Generate a Single-Device Report from the Device List Screen

Generate a Data Usage Trending Chart

Retrieve Files from the Download Center

Related Information

Device Reports and Graphical Analysis Charts

3.10.1 Reports and Charts Input Criteria

The default criteria in the table below apply to all reports in the M2M Management Center, including the Connection History Report, Transaction History Report, Connected Session History Report, Device Usage Report, Aggregated Device Usage Report and Data Usage Trending Chart. Report criteria you supply for one report populates the same fields when you navigate to the next report in the M2M Management Center during the same session.

Advanced criteria for each report are defined by individual report in the table as well.

Report Criterion	Type	Description
Default Criteria for All Reports (except Diagnostic Events Report, which is listed in the next sub-section of this table)		
Account	Drop-down	Billing accounts to which you have access; All considers all billing accounts to which you have access.
Device Identifier	Entry field	Device's ESN, MEID or IMEI to include in the selected report. To include multiple devices, enter each device's identifier, separated by a comma. Use %, the wildcard character when you are uncertain about a device's identifier. NOTE: As a shortcut, you can copy and paste device identifiers from the Device List into this field.
Start Date	Entry field/Date pop-up	Date on which to start including data in the report. NOTE: + The date range limit for the Connection History Report is seven (7) days. + The date range limit for the Transaction History Report is 30 days. + This field does not appear for the Rated Usage Report. It is automatically populated with the first day of the selected device's current or most recent bill cycle.
End Date	Entry field/ Date pop-up	Date on which to stop including data in the report. NOTE: + The date range limit for the Connection History Report is seven (7) days. + The date range limit for the Transaction History Report is 30 days. + This field does not appear for the Rated Usage Report. It is automatically populated with the last date on which rated usage data was received.
MDN/MSISDN	Entry field	Ten-digit phone number of 2G or 3G device/15-digit number of 4G device.
Device Group	Drop-down	Default selection is ALL. Or, select the group that includes the devices you'd like to see in the report.
IP Address	Entry field	Static Internet Protocol address assigned to device.
Custom Fields 1-5	Entry fields	Data used to filter devices. Custom fields are typically used for device type, region, business unit or some other data that further characterizes a device. NOTE: These fields display alternative label text when custom labels have been assigned (see Assign Custom Field Labels).
Default Criteria for Diagnostic Events Report		
Device Identifier	Entry field	ESN, MEID or IMEI of device to include in the selected report.
Last Number of Records	Radio button Drop-down	Select this option to enable this control, which displays the most current *N* records collected by the device. Drop-down list has values starting at 10 to a maximum of 50 at an interval of 10. When you select this option, you disable the date fields.
Date Range	Radio button Entry fields/Date pop-ups	Select this option to enable the date controls, which allow you to display all records collected by a device over a date range to a maximum of one week. Specify both Start Date and End Date using the controls. When you select this option, you disable the "Last Number of Records" option.
Account	Drop-down	Billing accounts to which you have access; All considers all billing accounts to which you

Report Criterion	Type	Description
		have access.
Advanced Criteria for Connection History Report		
MEID	Entry field	MEID of device in either Decimal or Hexadecimal format.
ESN	Entry field	ESN of device in either Decimal or Hexadecimal format.
IMEI	Entry field	IMEI of 4G device.
ICCID	Entry field	ICCID of 4G device's SIM card.
Event Type	Drop-down	Type of event, including: + All + Start + Stop + Accounting – Off
BSID	Entry field	Base Station Identifier, or servicing point of attachment for the device. NOTE: The BSID is a concatenation of SID (2 octets) + NID (2 octets) + Cell Identifier Type 2 (2 octets). In the Cell Identifier Type 2, the 12 upper bits are Cell ID and the 4 lower bits are Sector. Each item is encoded using hexadecimal uppercase ASCII characters. For example, the BSID 005F00BD1803 denotes: SID: 005F (95) NID: 00BD (189) Cell Identifier Type 2: 1803 (6147) Cell ID: 180 (384) Sector: 3 (3)
Advanced Criteria for Transaction History Report		
MEID	Entry field	MEID of device in either Decimal or Hexadecimal format.
ESN	Entry field	ESN of device in either Decimal or Hexadecimal format.
IMEI	Entry field	IMEI of 4G device.
ICCID	Entry field	ICCID of 4G device's SIM card.
Service Plan	Drop-down	Service plan assigned to the device.
Event Type/Request Status	Drop-down	Type of event and status of request: + All + Account Update Confirmed/Pending + Activation Confirmed/Pending + Change MDN Confirmed/Pending + Change Service Plan Confirmed/Pending + Deactivation Confirmed/Pending + Mobile Originated/Terminated SMS Message + Pending Preactivation/Preactivation Confirmed

Report Criterion	Type	Description
		+ PRL Update Request/Pending + Promo Added/Dropped + Reconnect MDN Confirmed/Pending + Resume Confirmed/Pending + Status Update Confirmed/Pending + Suspend Period Depletion Switch + Suspension Confirmed/Pending + Update ESN/MEID Confirmed/Pending
Event Status	Drop-down	Outcome of event: + All + Success + Fail
Event By	Entry field	Name of user who initiated event.
Advanced Criteria for Device Usage and Aggregated Device Usage Reports		
MEID	Entry field	MEID of device in either Decimal or Hexadecimal format.
ESN	Entry field	ESN of device in either Decimal or Hexadecimal format.
IMEI	Entry field	IMEI of 4G device.
ICCID	Entry field	ICCID of 4G device's SIM card.
Service Plan	Drop-down	Service plan assigned to the device.
Advanced Criteria for Rated Usage Report		
MEID	Entry field	MEID of device in either Decimal or Hexadecimal format.
ESN	Entry field	ESN of device in either Decimal or Hexadecimal format.
IMEI	Entry field	IMEI of 4G device.
ICCID	Entry field	ICCID of 4G device's SIM card.
Advanced Criteria for Data Usage Trending Chart		
MEID	Entry field	MEID of device in either Decimal or Hexadecimal format.
ESN	Entry field	ESN of device in either Decimal or Hexadecimal format.
IMEI	Entry field	IMEI of 4G device.
ICCID	Entry field	ICCID of 4G device's SIM card.
Service Plan	Drop-down	Service plan assigned to the device.

3.10.2 Connection History Report Results

Related Information

Connection History Report

The following columns are available for the Connection History Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.
BSID	Base Station Identifier, which is the servicing point of attachment and helps determine an approximate location for a device. NOTE: The BSID is a concatenation of SID (2 octets) + NID (2 octets) + Cell Identifier Type 2 (2 octets). In the Cell Identifier Type 2, the 12 upper bits are Cell ID and the 4 lower bits are Sector. Each item is encoded using hexadecimal uppercase ASCII characters. For example, the BSID 005F00BD1803 denotes: SID: 005F (95) NID: 00BD (189) Cell Identifier Type 2: 1803 (6147) Cell ID: 180 (384) Sector: 3 (3)
Custom Fields 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Device Connection Group	Refer to AAA Attributes in the Connection History Report, which includes information on how to use each of the following Attribute-Value Pairs (AVPs) in the Device Connection Group for troubleshooting: + 3GPP2-Release-Indicator + 3GPP2-Correlation-Id + 3GPP2-Inbound-Mobile-IP-Sig-Octets + 3GPP2-Outbound-Mobile-IP-Sig-Octets + 3GPP2-Session-Continue + 3GPP2-Active-Time + 3GPP2-Last-User-Activity-Time + 3GPP2-Begin-Session + Acct-Status-Type + Acct-Session-Id + Acct-Session-Time + Acct-Input-Packets + Acct-Output-Packets + Acct-Terminate-Cause + Event-Timestamp
Device Group	Group with which device is associated.

Report Column	Description
Device Identifier	Identifier (ESN/MEID/IMEI) associated with device. This field must appear on all Connection History Reports; it cannot be hidden from view.
Device Identity Group	Refer to AAA Attributes in the Connection History Report, which includes information on how to use each of the following AVPs in the Device Identity Group for troubleshooting: + User-Name + Framed-IP-Address + Calling-Station-Id
Device Traffic Group	Refer to AAA Attributes in the Connection History Report, which includes information on how to use each of the following AVPs in the Device Traffic Group for troubleshooting: + 3GPP2-Terminating-SDB-Octet-Count + 3GPP2-Originating-SDB-Octet-Count + 3GPP2-Terminating-Number-SDBs + 3GPP2-Originating-Number-SDBs
ESN	Electronic Serial Number of device.
Event	+ Start—Occurs when a device connects to the network (data session starts). + Stop—Occurs when a device disconnects from the network or terminates a data session.
Event Date	Date and time of connection event. Times are expressed in the time zone selected for the current contact.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
In Bound Bytes Used	Amount of raw data received by the device during session.
IP Address	Internet Protocol address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number associated with 4G device.
MEID	Mobile Equipment Identifier of device.
Network Information Group	Refer to AAA Attributes in the Connection History Report, which includes information on how to use each of the following AVPs in the Network Information Group for troubleshooting: + NAS-IP-Address + NAS-PORT + 3GPP2-Home-Agent-IP-Address + 3GPP2-PCF-IP-Address + 3GPP2-BSID + 3GPP2-Compulsory-Tunnel-Indicator + NAS-Identifier
Out Bound Bytes Used	Amount of raw data emitted by the device during session.

Report Column	Description
RF Info Group	Lists the following AVPs for the device: + 3GPP2-Forward-FCH-Mux-Option + 3GPP2-Reverse-FCH-Mux-Option + 3GPP2-Service-Option + 3GPP2-Forward-Traffic-Type + 3GPP2-Reverse-Traffic-Type + 3GPP2-FCH-Frame-Size + 3GPP2-Forward-FCH-RC + 3GPP2-Reverse-FCH-RC + 3GPP2-IP-Technology + 3GPP2-Bad-PPP-Frame-Count
RF Technology	Indicates whether a connection was made using the 2G (1xRTT), 3G (EV-DO), or 4G (LTE) network.
Total Bytes Used	Total amount of raw data usage during the specified time period, before rounding and other rules are applied. Reflects estimated usage per session and includes both inbound and outbound data.

3.10.2.1 AAA Attributes in the Connection History Report

NOTE:

- **Abbreviations/acronyms that apply only to information in the table below include the following:**
  - **AAA—Authentication, Authorization and Accounting**
  - **ANI—Automatic Number Identification**
  - **FA—Foreign Agent**
  - **FCH—Fundamental Channel**
  - **MS—Mobile Station or Mobile Subscriber**
  - **NAI—Network Address Identifier**
  - **NAS—Network Access Server**
  - **PCF—Packet Control Function**
  - **PDSN—Packet Data Serving Node**
  - **PPP—Point-to-Point Protocol**
  - **RADIUS—Remote Authentication Dial-In User Service**
  - **RAN—Remote Access Network**
  - **RF—Radio Frequency**
  - **SDB—Short Data Burst**
- **"Values not present for attributes in this legend" is displayed when the carrier sends no value for an attribute.**
- **Attributes appended with an asterisk (*) are returned for 2G/3G devices only. Unmarked attributes are returned for all devices.**

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
Device Connection Group			
3GPP2-Release-Indicator*	Reason for sending stop record.		Stop
3GPP2-Correlation-Id	Unique accounting ID, in ASCII format, created by serving PDSN for each packet data session.	Correlate multiple accounting records for each associated R-P or P-P connection.	Start and Stop
3GPP2-Inbound-Mobile-IP-Sig-Octets*	Total number of octets in registration requests and solicitations sent by MS.		Start and Stop
3GPP2-Outbound-Mobile-IP-Sig-Octets*	Total number of octets in registration replies and agent advertisements sent to MS prior to any compression and/or fragmentation.		Start and Stop
3GPP2-Session-Continue*	Integer value: 0=False; 1=True. "True" means it is not the end of a session and an Accounting Stop is immediately followed by an Accounting Start record. "False" means end of session.		Stop
3GPP2-Active-Time*	Active time reported by RAN in Active Stop record.		Stop
3GPP2-Last-User-Activity-Time*	Timestamp (in number of seconds from Jan 1 1970 UTC) of last known user activity.	Verify when last data packet was sent or received from device. May be used to determine if session remained active too long after device went idle. Also may help troubleshoot session drop problems, e.g., if device made too many back-to-back session requests or if last sent/rcvd packet time had the same time as previous session end time, These conditions mean that device had more data to exchange but session was dropped for some reason.	Stop
3GPP2-Begin-Session	Integer value: 0=False; 1=True. "True" means new packet data session is established; "False" means continuation of previous packet data session.		Stop
Acct-Status-Type	Indicates whether Accounting-Request marks beginning of user service (Start) or end (Stop). Value field is four octets: + 1= Start + 2= Stop + 3= Interim-Update + 7= Accounting-On + 8=Accounting-Off	Identify session Starts and Stops, which could be used as a trigger by a machine-to-machine application, for example.	Start and Stop

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
	+ 9 to 14=Reserved for Tunnel Accounting + 15=Reserved for Failure		
Acct-Session-Id	Unique Accounting ID. Start and Stop records for given session MUST have same Acct-Session-Id. Accounting-Request packet MUST have Acct-Session-Id. Access-Request packet MAY have Acct-Session-Id; if it does, NAS MUST use same Acct-Session-Id in Accounting-Request packets for the session.	Correlate Start and Stop records for diagnostics and debugging.	Start and Stop
Acct-Session-Time	Number of seconds during which user received service. Can only be present in Accounting-Request records where Acct-Status-Type is set to Stop.		Stop
Acct-Input-Packets	Number of packets received from port over course of service being provided to framed user. Can only be present in Accounting-Request records where Acct-Status-Type is set to Stop.	Debug issues related to packet overhead. If, for example, there are too many packets for too few octets, there is too much header overhead since IP packets are small. In this case, the customer needs to optimize packet size to minimize amount of header overhead and stay within limits of service plan budget.	Stop
Acct-Output-Packets	Number of packets sent to port while delivering service to framed user, Is only present in Accounting-Request records where Acct-Status-Type is set to Stop.	Debug issues related to packet overhead. If, for example, there are too many packets for too few octets, there is too much header overhead since IP packets are small. In this case, the customer needs to optimize packet size to minimize the amount of header overhead and stay within limits of service plan budget.	Stop
Acct-Terminate-Cause	Indicator of how session was terminated. Can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. NOTE: When the system receives a value that does not match a code in the database for this attribute, this field displays “Unrecognized Code.” Possible causes include: + Admin-Reset—Port was reset by Administrator. + Host-Request—Session was terminated by Login-IP-Host. Can indicate normal termination or that remote host crashed	Diagnose reason for data session termination.	Stop

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
	or became unreachable. + Idle-Timeout—Idle time expired for user or port. + Lost-Carrier—Modem disconnected because user or modem hung up on other end (no problem), line was dropped, line took noise hit too extreme for modem recovery, etc. + Port-Error—PortMaster had to reset port. Most commonly done when device attached to port causes too many interrupts. + Session-Timeout—Session time expired for user. + User-Error—PortMaster ended session because it received PPP Configuration Request or ACK during established session. Caused by PPP implementation error in dial-in client. + User-Request—Dial-in PPP client requested session termination as expected.		
Event-Timestamp	Time reference as seconds since Jan 1, 1970 00:00 UTC.	Decide when to connect to device next, when to change a sensor configuration on device, etc.	Start and Stop
Device Identity Group			
User-Name	Name of device to be authenticated by RADIUS server. Sent either in Access-Request or Access-Accept packet. Field often used to populate Network Address Identifier. When used as NAI, uses the form user@domain to identify user and home network of device.	Verify the mobile IP NAI of a device. NAI must map to same ESN/MDN pair. May indicate fraudulent use when mapping cannot be verified.	Start and Stop
Framed-IP-Address	Mobile IP address assigned to device. Can be static private or dynamic private address.	Verify that IP address belongs to customer's pool range, particularly for Private Network customers.	Start and Stop
Calling-Station-Id (MIN)	Phone number of device that initiated data session. Sent by NAS in Access-Request packet. Uses ANI or similar technology.	Correlate a data session to a device's MDN, which is unique, to ensure that device is using its own line subscription and not another device's.	Start and Stop
Device Traffic Group			
3GPP2-Terminating-SDB- Octet-Count*	Total number of octets sent to MS via SDBs. Direct proxy for volume of SMS data sent to device.	Track SMS usage information.	Start and Stop

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
3GPP2-Originating-SDB-Octet-Count*	Total number of octets sent by MS via SDBs. Direct proxy for volume of SMS data sent from device.	Track SMS usage information.	Start and Stop
3GPPP2-Terminating-Number-SDBs*	Total number of SDB transactions with MS. Direct proxy for number of SMS messages sent to mobile.	Troubleshoot device wakeups, PRL updates and general SMS messaging to device.	Start and Stop
3GPP2-Originating-Number-SDBs*	Total number of SDB transactions with MS. Direct proxy for number of SMS messages sent to mobile.	Diagnose general SMS messaging from device.	Start and Stop
Network Information Group			
NAS-IP-Address	Equivalent to IP address of PDSN/FA in Verizon Enterprise Network that is requesting authentication for the device requesting a data session. Address should be unique within scope of RADIUS server.	Ascertain that device was in an area of network coverage served by specific PDSN/FA. Device may experience sub-optimal data session performance when it is on a boundary between two PDSNs. When too many mobile IP re-registration requests are made because the point of attachment is not well-defined, thrashing may occur.	Start and Stop
NAS-PORT	Physical port type of AAA server in Verizon Enterprise Network that authenticated device requesting data session. May be any of the following: + Async + Sync + ISDN + ISDN-V120 + ISDN-V110	Ensure that correct AAA port type was used to authenticate device.	Start and Stop
3GPP2-Home-Agent-IP-Address	IPv4 address of Home Agent.	Identify issues with mobile IP authentication and authorization by establishing the chain of network servers involved in the process of setting up the requested data session.	Start and Stop
3GPP2-PCF-IP-Address*	IPv4 address of serving PCF in serving RAN.	Identify issues with mobile IP authentication and authorization by establishing the chain of network servers involved in the process of setting up the requested data session.	Start and Stop
3GPP2-BSID*	Base Station Identifier servicing point of attachment for device. Format is: Concatenation of SID (4 octets) + NID (4 octets) + Cell Identifier Type 2 (4 octets). In the Cell Identifier, 12 upper bits are Cell ID; 4 lower bits are Sector. Each item is	Locate a device down to its cell/sector, which is useful for: + Diagnosing problems by location, e.g., when RF signal is not good due to fade. + Integrating or overlaying	Start and Stop

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
	encoded using hexadecimal uppercase ASCII characters.	geographic information into machine-to-machine application. + Forming device groups for monitoring, diagnostics (DPS) and/or provisioning.	
3GPP2-Compulsory-Tunnel-Indicator*	Compulsory tunnel that was established on behalf of device for providing Private Network and/or ISP access during a single packet data connection.	Ensure that reverse tunneling is enforced (i.e., there is no triangular routing for mobile IP). Normally, triangular routing is used for routing to public addresses from a device.	Start and Stop
NAS-Identifier*	Identifier of PDSN/FA in Verizon Enterprise Network requesting authentication of device requesting data session. Either NAS-IP-Address or NAS-Identifier MUST be present in Access-Request packet.	Verify connection to correct NAS.	Start and Stop
RF Info Group			
3GPP2-Forward-FCH-Mux-Option*	Forward FCH Multiplex option.		Start and Stop
3GPP2-Reverse-FCH-Mux-Option*	Reverse FCH Multiplex option.		Start and Stop
3GPP2-Service-Option	Service option received from RAN that indicates type of service granted, voice, packet data, etc.	Determine if EV-DO–capable device is falling back to 1xRTT data speeds, which causes slow data rates from device or intermittent connectivity issues). Also may indicate problem with device radio modem hardware, software or device needing PRL update.	Start and Stop
3GPP2-Forward-Traffic-Type*	Forward direction traffic type; either Primary or Secondary. Usually Primary.		Start and Stop
3GPP2-Reverse-Traffic-Type*	Reverse direction traffic type; either Primary or Secondary. Usually Primary.		Start and Stop
3GPP2-FCH-Frame-Size*	Quality of RF conditions experienced by device.	Evaluate quality of RF conditions.	Start and Stop
3GPP2-Forward-FCH-RC*	Format and structure of radio channel in Forward Fundamental Channel. Set of forward transmission formats that are characterized by data rates, modulation characteristics and spreading rates.	Troubleshoot throughput problems.	Start and Stop
3GPP2-Reverse-FCH-RC*	Format and structure of radio channel in Reverse Fundamental Channel. Set of reverse transmission formats that	Troubleshoot throughput problems.	Start and Stop

Attribute	Definition	Use this Attribute to:	Included in Start, Stop, or Both Start and Stop Message(s)
	are characterized by data rates, modulation characteristics and spreading rates.		
3GPP2-IP-Technology*	IP technology to use for call: Simple IP or Mobile IP. On some roaming partner networks, only Simple IP may be available.	Diagnose connectivity issues.	Start and Stop
3GPP2-Bad-PPP-Frame-Count*	Number of bad PPP frames.	Evaluate connectivity or throughput problems with Mobile IP by checking whether PPP frames are being sent or received correctly (e.g., bad CRC).	Stop

3.10.3 Transaction History Report Results

Related Information

Transaction History Report

Wireless Network Services APIs

The following columns are available for the Transaction History Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.
Custom Fields 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Description	Provides details of provisioning events and can be used to troubleshoot events with the status of Failure.
Device Group	Group to which device belongs.
Device Identifier	Identifier associated with device (ESN, MEID or IMEI). This field must appear on all Transaction History Reports; it cannot be hidden from view.
ESN	Electronic Serial Number of device.
Event By	Displays "Verizon Wireless" when event was initiated by a customer using a self-serve portal, a Verizon Customer Service representative, or a Verizon Account Team member. Displays the name of a custom application's Unified Web Services login account when event was initiated by a custom application using Wireless Network Services APIs.
Event Date	Date and time event occurred.
Event Status	Indicates whether the event resulted in Success or Failure.

Report Column	Description
Event Type / Request Status	Requested service provisioning action and corresponding state: + Activation Pending/Confirmed—Device enabled to use the Verizon Enterprise Network. + Change Service Plan Pending/Confirmed*—New service plan requested for device. + Deactivation Pending/Confirmed—Device no longer provisioned for M2M Management Center services, although it can be enabled for another purpose on the network. + Suspension Pending/Confirmed—Device not enabled to use the Verizon Enterprise Network. + Promo Added/Promo Dropped—Promotional pricing applied or removed. *NOTE: This event type only applies to service plan changes initiated by customer applications that make use of Wireless Network Service APIs. Service plan changes initiated in either the Verizon Wireless My Business Account or Verizon Enterprise Center Web portal or by a Verizon Customer Service representative or a Verizon Account Team member are not included in this report.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
IP Address	Internet Protocol address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number associated with 4G device).
MEID	Mobile Equipment Identifier of device.
Service Plan	Service plan for the selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in this report.

3.10.4 Connected Session History Report Results

Related Information

Connected Session History Report

NOTE; 4G devices often connect for long periods of time and do not generate Stop records until these long connections end. This report will not include data for ongoing sessions that have not yet ended.

The following columns are available for the Connected Session History Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.

Report Column	Description
BSID	Base Station Identifier, which is the servicing point of attachment and helps determine an approximate location for a device. NOTE: The BSID is a concatenation of SID (2 octets) + NID (2 octets) + Cell Identifier Type 2 (2 octets). In the Cell Identifier Type 2, the 12 upper bits are Cell ID and the 4 lower bits are Sector. Each item is encoded using hexadecimal uppercase ASCII characters. For example, the BSID 005F00BD1803 denotes: SID: 005F (95) NID: 00BD (189) Cell Identifier Type 2: 1803 (6147) Cell ID: 180 (384) Sector: 3 (3)
Custom Field 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Data Usage	Amount of data used, expressed in KB.
Device Group	Group to which device belongs.
Device Identifier	Identifier of device (ESN, MEID or IMEI). This field must appear on all Connected Session History Reports; it cannot be hidden from view.
Duration	Length of connection session, calculated by subtracting Start Date/Time from End Date/Time.
End Date/Time	The time at which a connection session was terminated.
ESN	Electronic Serial Number of device.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
IP Address	Internet Protocol (IP) address of device during connection session. Devices with static IP addresses should display the same address for all sessions.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number associated with 4G device.
MEID	Mobile Equipment Identifier of device.
Start Date/Time	The time at which a connection session began.
Usage(KB)	Amount of data used during a connection session, expressed in kilobytes.

3.10.5 Device Usage Report Results

Related Information

Device Usage Report

Wireless Network Services APIs

Usage Data Calculations

The following columns are available for the Device Usage Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.
Custom Fields 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Device Group	Group to which device belongs.
Device Identifier	Identifier of device (ESN, MEID or IMEI). This field must appear on all Device Usage Reports; it cannot be hidden from view.
ESN	Electronic Serial Number of device.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
IP Address	Internet Protocol address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number assigned to 4G device.
MEID	Mobile Equipment Identifier of device.
Service Plan	Service plan for selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in this report.
SMS Usage	Number of SMS messages sent and received.
Usage(KB)	Amount of data used, expressed in KB.
Usage Date	The date on which the usage occurred.

3.10.6 Aggregated Device Usage Report Results

Related Information

Aggregated Device Usage Report

Usage Data Calculations

The following columns are available for the Device Usage Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.
Custom Fields 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Device Group	Group to which device belongs.
Device Identifier	Identifier of device (ESN, MEID or IMEI). This field must appear on all Aggregated Device Usage Reports; it cannot be hidden from view.
ESN	Electronic Serial Number of device.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
IP Address	Internet Protocol address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number assigned to 4G device.
MEID	Mobile Equipment Identifier of device.
Service Plan	Service plan for selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will continue to appear in this report.
SMS Usage	Sum of all SMS usage over the date range.
Usage(KB)	Sum of all data usage over the date range, expressed in kilobytes.
Usage Date	Date range selected for report.

3.10.7 Rated Usage Report Results

Related Information

Rated Usage Report

NOTE:

- **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 behind the date on which you generate the report. Therefore, to obtain a report that contains usage data for the first half of a bill cycle, wait until about Day 17 in the cycle to generate a report.**
- **Rated usage data is not available to display in this report until about six days after the start of the selected device's bill cycle. 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.**

The following columns are available for the Rated Usage Report (columns are listed alphabetically because of the custom view feature, which allows you to define the layout of this report); columns that are part of the System Default view are in **bold text**:

Report Column	Description
4G/LTE	Logo denotes 4G/LTE devices; cell is empty for 2G/3G devices.
Account	Billing account with which device is associated.
Billing Cycle End Date	Last day of device's current bill cycle.
Custom Fields 1-5	Generally contain information to help sort or categorize devices, such as business unit, device type, location, etc. NOTE: These fields may display alternative label text when custom field labels have been assigned by your administrator (see Assign Custom Field Labels).
Data Usage(KB)	Sum of all data usage for the current bill cycle to the current date, expressed in kilobytes.
Device Group	Group to which device belongs.
Device Identifier	Identifier of device (ESN, MEID or IMEI). This field must appear on all Aggregated Device Usage Reports; it cannot be hidden from view.
ESN	Electronic Serial Number of device.
ICCID	ICCID assigned to SIM card installed in 4G device.
IMEI	Unique identifier associated with 4G device.
IP Address	Internet Protocol address assigned to device. 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 field is zero-filled (0.0.0.0) because no address is assigned to the device.
MDN/MSISDN	Ten-digit phone number associated with 2G or 3G device/15-digit number assigned to 4G device.
MEID	Mobile Equipment Identifier of device.
Service Plan	Service plan for selected device. NOTE: For some established customer accounts that have not been updated with service plan names, the service plan name values of "M2M" or "M2M_CPN" (when you have the Customer Private Network option) will appear in this report.
SMS Usage	Sum of all SMS usage for the current bill cycle to the current date.
Start Date – End Date	Date range of report; start date is the first day of the device's bill cycle for which rated data is available; end date is the latest date for which usage was available (usually two days prior to current date or last day of most recent bill cycle).

3.10.8 Diagnostic Events Report

Related Information

Diagnostic Events Report

This report shows only events that apply to the selected device. The following events may appear depending on the events recorded over the selected data or record range. Each event is defined by its ID, a short and long description, a link to the relevant attributes of the session during which it occurred, and the timestamp of its occurrence.

Event ID	Event Description (short)
1900	Application Blocking
2000	Diagnostics Report
10000	Device Restarted
10100	Modem Restarted
10200	Watchdog Expired
10300	Application Processor Memory Low
10310	Application Processor Internal Storage Low
10320	Application Processor External Storage Low
10400	Data Connection Started
10401	Data Connection Ended wo/Error
10402	Data Connection Ended w/Error
10403	Data Connection Start Attempt w/Error
10500	Cell Signal Low
10501	Cell Signal Normal

Information for the records of the last completed session appears when you click the Attributes link associated with an event:

Report Column	Description
Last Completed Session-Network Attribute Group – Start Record	
Start Record Time	Time when last complete connected session started.
NAS IP Address	IP address of Network Access Server employed during last complete connected session.
Framed (Device) IP Address	IP address used by device during last complete connected session.
Home Agent IP Address	IP address of home agent used during last complete connected session.
BSID	Identifier of base station being used at the start of the last complete connected session.
3GPP2 Service Option	Standard 3GPP2 service option employed at the start of the last complete connected session, when applicable.

Last Completed Session-Network Attribute Group – Stop Record	
Stop Record Time	Time when last complete connected session ended.
NAS IP Address	IP address of Network Access Server employed during last complete connected session.
BSID	Identifier of base station being used at the end of the last complete connected session.
3GPP2 Service Option	Standard 3GPP2 service option employed at the end of the last complete connected session, when applicable.
Acct-Input-Octets	Number of octets received during last complete connected session.
Acct-Output-Octets	Number of octets sent during last complete connected session.
Bad PPP Frame Count	Number of bad frames sent using Point-to-Point Protocol during last complete connected session.
Acct-Terminate-Cause	Indicates how the last complete session ended.
Release Indicator	Reason for sending the stop record of the last complete connected session.

In addition, the following data will appear as attributes for Advanced M2M devices with Device Diagnostics capabilities. Only the attribute groups with data to display will be displayed.

Label	Description
	Device Attribute Group
Device Description	Textual description of device.
Serial Number	Device identifier.
HW Version	Hardware version associated with device.
SW Version	Version of software installed on device.
	Modem Attribute Group
Modem Description	Textual description of modem.
Serial Number	Modem identifier (ESN, MEID, IMEI, etc.).
HW Version	Hardware version associated with modem.
SW Version	Version of software installed in modem.
	RF Attribute Group
RF Technology	Radio access technology (CDMA, EVDO, GSM, EDGE, UMTS, LTE).
Signal Strength (dBm)	Strength of signal, expressed in dBm.
Signal Quality (dB)	Quality of signal, expressed in dB.
RF Operator	Network operator identifier (SID-NID, MCC-MNC).
Roaming Ind	Roaming indicator.
Disconnect Reason	Reason for disconnect.
	Memory Attribute Group

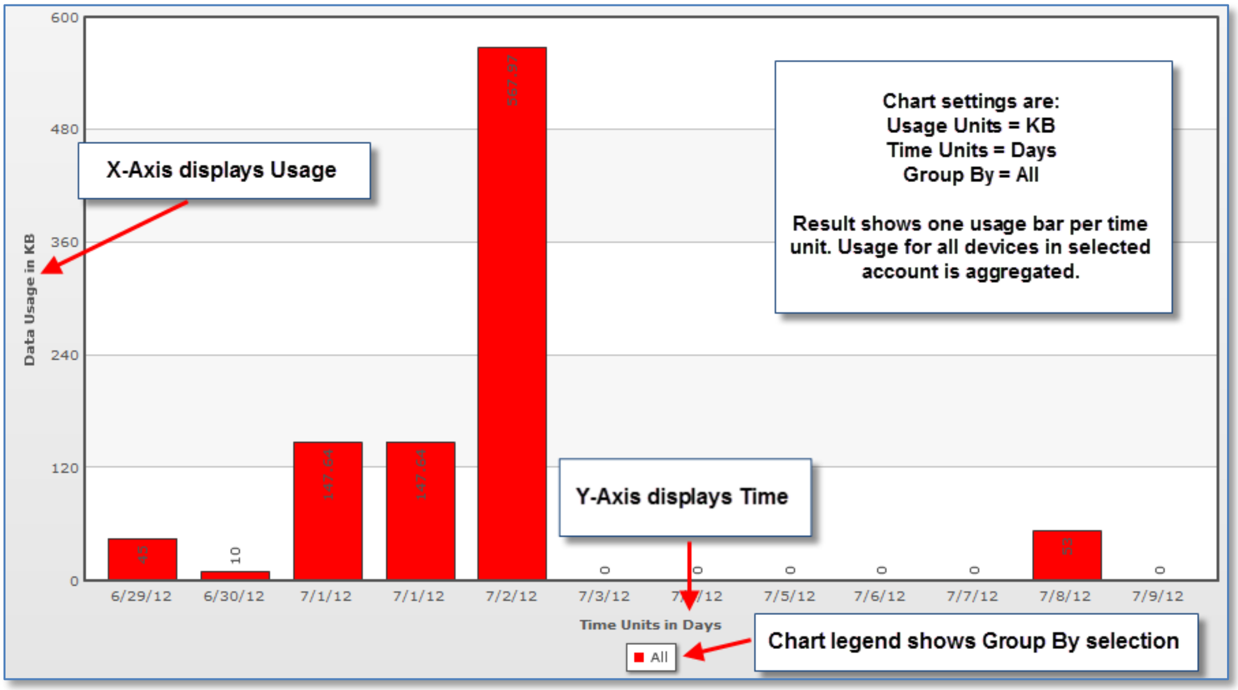
Label	Description
KB RAM Remaining	Number of KB of memory left.
MB Internal Remaining	Number of MB remaining on internal storage media.
MB External Remaining	Number of MB remaining on external storage media.
Watchdog Attribute Group	
Watchdog Type	Watchdog that expired (0=DCF).
Block Attribute Group	
Application Block Reason	Application blocking reason: + 0=no service + 1=roaming + 2=RF
Data Connection Attribute Group	
Failure Code	Code of data connection authentication failure.

3.10.9 Data Usage Trending Chart Results

Related Information

Data Usage Trending Chart

Refer to the diagram below, which calls out the data points that comprise the histogram for the Data Usage Trending Chart:



X-Axis displays Usage

Chart settings are:
Usage Units = KB
Time Units = Days
Group By = All

Result shows one usage bar per time unit. Usage for all devices in selected account is aggregated.

Y-Axis displays Time

Chart legend shows Group By selection

Figure 3-1 Data Usage Trending Chart properties

NOTE: Usage values in this chart are rounded to two decimal places. Be sure to set the usage units for the X-axis appropriately to ensure that the chart includes usage as you want to view it.

3.11 Master Log Properties

Related Tasks

Populate the Master Log

Export the Master Log

Related Information

About Unified Web Services and Wireless Network Services APIs

3.11.1 Master Log Search Criteria

Search Criterion	Type	Description
Report Type	Drop-down	+ All—Results show all events, regardless of type. + System Events—Results show only system events. + User Events—Results show only user events. The remaining criteria at the top of the screen change to show only fields applicable to the selected report type.
Start Date	Entry field/Date pop-up	Date on which to start reporting events.
End Date	Entry field/Date pop-up	Date on which to stop reporting events.
Account	Drop-down	Select an available billing account. Accounts are used to organize data and devices.
Device Type	Drop-down	All is the only selection in this drop-down list.
Device ID	Entry field	ESN MEID or IMEI of device; enter multiple device identifiers separated by commas to include more than one device in the Master Log.
System Event	Drop-down	System event to include in a System Events or All Master Log: + All + Update PRL NOTE: Both choices in this drop-down produce the same results; only PRL update transactions are listed.
User Name	Drop-down	One or more users to include in a User Events or All Master Log.
Interface	Drop-down	One or more screens from the M2M Management Center interface to include in a User Events or All Master Log. Note that not all listed interface selections apply to the M2M Management Center. The Master Log will report on the screens selected from this list and visited by the logged-in user. + All + AggregatedDeviceUsageReport

Search Criterion	Type	Description
		+ ConnectedSessionHistoryReport + ConnectionHistoryReport + ContactSetup + Create/Edit DashboardFilter + CreateView + CustomFieldLabels + Dashboard + DashboardConfig + DeviceGroup + DeviceGroupPRLUpdate + DeviceInfo + DeviceList + DeviceUsageReport + DiagnosticEventsReport + Edit/Delete View + Integrated Portal Handler + Login + MasterLog + NotificationGroupSetup + NotificationLog + NotificationSetup + PRLUpdateReportModal + RatedUsageReport + PRLUpdate + RatedUsageReport + ReportModal + Retrieve diagnostic data + Support + SwitchOrganization + TransactionHistoryReport + UploadDevices + UsageTrendingReport + Wakeup + WakeupDeviceGroup
Function	Drop-down	One or more functional actions to include in a User Events or All Master Log. Each function has an explanation of the user action that is logged by the application for display in the Master Log. + All + Access Page—Display a new screen in the M2M Management Center. + Acknowledge—Click the Acknowledge link in the Notification Log. + Add New—Click any Add New button.

Search Criterion	Type	Description
		+ Change Password—Not applicable to M2M Management Center. + Control—This function is not currently available. Modifications will be made in a future software release. + Delete—Click any Delete link. + Edit—Click any Edit link. + Export—Click any Export button. + Export/View User Events—Access and/or export a Master Log containing user events. + Login—Not applicable to M2M Management Center. + Notification Triggers—This function is not currently available. Modifications will be made in a future software release. + Print Page—Click any Print button. + Reset Alarm—This function is not currently available. Modifications will be made in a future software release. + Save/Commit—Click any Save button to commit changes to the database. + Search/Refresh—Click any Search button to refresh the interface. + Security—Not applicable to M2M Management Center. + Update—Click any Submit button to update a record.

3.11.2 Master Log Columns

Column Heading	Description
Date Occurred	Date and time (expressed in the time zone selected for the current contact) at which the event was logged.
Account	Account against which event was logged.
Device	Device associated with event; for user events, this column is blank.
User Name	User name of person who was logged in when event occurred; for any action initiated by a custom application, column contains user name of Unified Web Services login when event occurred. Displays as blank when no user was associated with the event displayed.
Interface	For system events, this column is blank; for user events, this column displays the screen on which the event occurred.
Event Type/Request Status	For all events, this column displays the system or user event that occurred or was initiated.
Description	Event description.

4 About the M2M Management Center

4.1 Wireless Network Services APIs

Application developers can use the Verizon M2M Platform's Wireless Network Services APIs to integrate service provisioning and management functions for M2M devices with enterprise-level back-end applications. Wireless Network Services APIs are standards-compliant Web services that provide a single, simplified and portable interface to the Verizon Enterprise Network.

When you have custom applications that perform device-provisioning actions with Wireless Network Services APIs, the device-state changes are reflected in the screens and reports of the M2M Management Center, as noted throughout this document.

4.2 Usage Data Calculations

Three types of usage data are calculated and displayed by the M2M Management Center: data usage, SMS usage and rated usage. These usage data types originate from the following sources:

- The M2M Platform updates data usage estimates in near real time, to within 15 minutes of the end of a device's last data session. For 4G devices that stay connected for extended periods, the Verizon M2M Platform updates usage estimates approximately every 6 hours until the device disconnects.
- The Verizon Enterprise Network updates SMS usage data every 24 hours, with SMS usage accumulated as of 48 hours in the past, for a total maximum delay of three days.
- A Verizon Data Warehouse feed updates rated data and SMS usage daily, with unbilled, non-roaming usage data that is usually two days in arrears. Roaming data may be updated less frequently.

4.2.1 Accumulated Data Usage Calculations

Calculations of accumulated data usage within a specified time period are used in the following places within the M2M Management Center:

- Current Period Data Usage Report in the Dashboard
- Device Usage and Aggregated Device Usage Reports
- Notifications based on usage

Accumulated data usage is an estimate of usage since the start of the current bill cycle.

4.3 Current Period and Bill Cycle

Certain Dashboard charts, the Rated Usage Report and some notifications are based on the current period. Current period corresponds to a device's current Verizon Wireless bill cycle, which is passed to the M2M Management Center with the daily usage feed. At the beginning of each device's bill cycle, the software clears the amount of data accumulated for the device and returns it to the bucket with the lowest value range, thus resetting its accumulated usage.

When a time period in the M2M Management Center is based on the Verizon Wireless bill cycle, as it is for the Dashboard Current Usage and Rated Usage reports and for monthly threshold notification rules, the M2M Management Center uses the bill cycle date that it receives in each Verizon Wireless Data Warehouse feed. For example, when the bill cycle of a device starts on the 15th of the month, monthly usage calculations will accumulate usage starting on the 15th at 12:00 AM PST (UTC-8).

When changes to the bill cycle are communicated, the M2M Management Center automatically adjusts its usage calculations. However, it does not prorate or perform other adjustments due to changed bill cycle date.

Bill cycles tracked in the M2M Management Center and those used to calculate Verizon invoices are off by approximately six hours. Thus, usage accumulated during the final six hours of the M2M Management Center bill cycle may appear on the subsequent Verizon invoice.

4.4 Device Reports and Graphical Analysis Charts

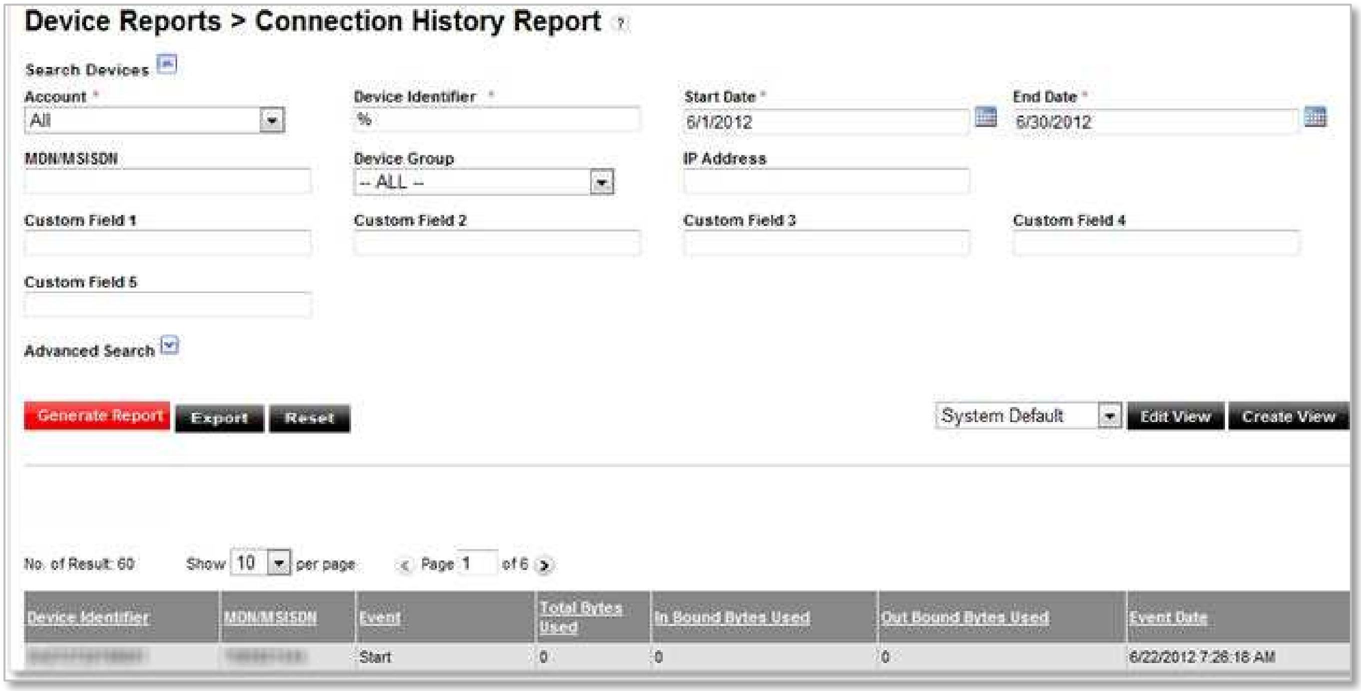
This section contains high-level descriptions and samples of the following reports:

- Connection History Report
- Transaction History Report
- Connected Session History Report
- Device Usage Report
- Aggregated Device Usage Report
- Rated Usage Report
- Diagnostic Events Report
- Data Usage Trending Chart

4.4.1 Connection History Report

The Connection History Report shows each connection event for a specified device(s) over a particular date range.

NOTE: The date range limit for the Connection History Report is seven (7) days.



Device Reports > Connection History Report

Search Devices

Account *	Device Identifier *	Start Date *	End Date *
All	%	6/1/2012	6/30/2012
MDN/MSISDN	Device Group	IP Address	
	-- ALL --		
Custom Field 1	Custom Field 2	Custom Field 3	Custom Field 4
Custom Field 5			

Advanced Search

No. of Result: 60 Show 10 per page Page 1 of 6

Device Identifier	MDN/MSISDN	Event	Total Bytes Used	In Bound Bytes Used	Out Bound Bytes Used	Event Date
[redacted]	[redacted]	Start	0	0	0	6/22/2012 7:26:18 AM

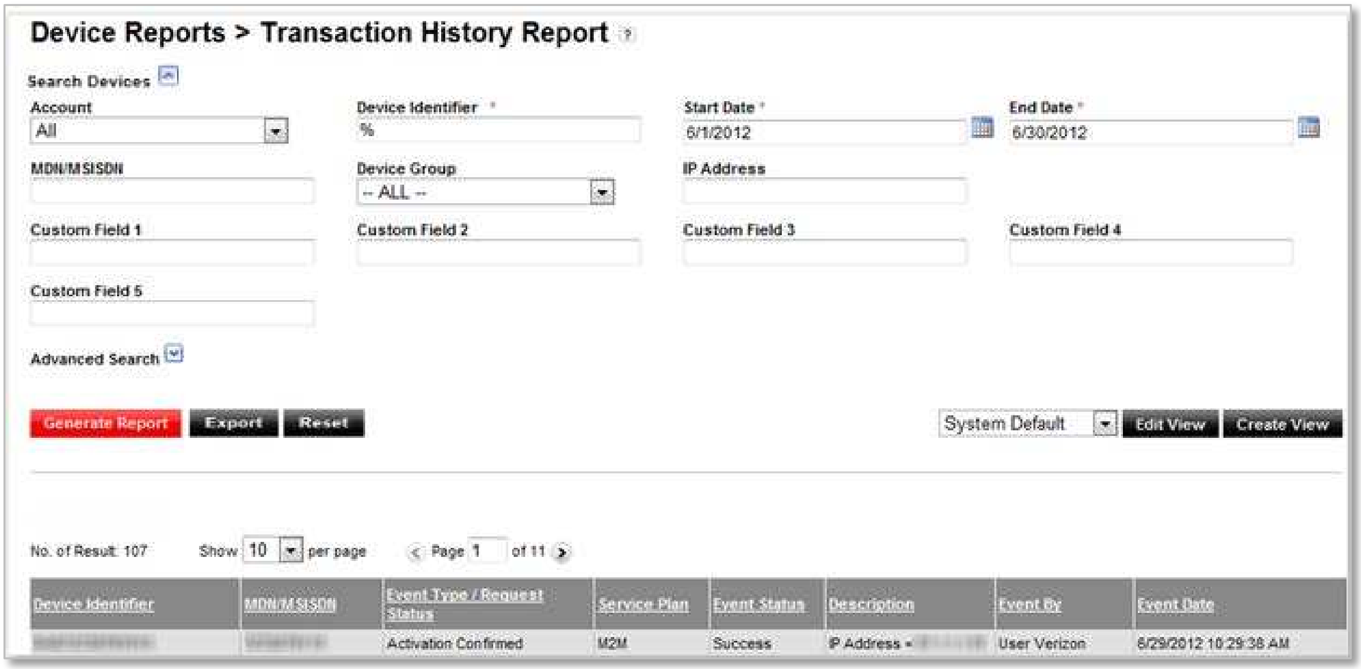
Figure 4-1 Connection History Report example

4.4.2 Transaction History Report

The Transaction History Report lists the provisioning actions applied to a selected device(s) within a specified date range. The provisioning actions available for the report encompass all transactions, including those initiated by the following:

- Custom applications using Wireless Network Services APIs
- Customers using a Verizon self-service portal
- Customer Service representatives
- Account Team members

NOTE: The date range limit for the Transaction History Report is 30 days.



Device Reports > Transaction History Report

Search Devices

Account: All	Device Identifier *: %	Start Date *: 6/1/2012	End Date *: 6/30/2012
MDN/MSISDN:	Device Group: -- ALL --	IP Address:	
Custom Field 1:	Custom Field 2:	Custom Field 3:	Custom Field 4:
Custom Field 5:			

Advanced Search

No. of Result: 107 Show 10 per page Page 1 of 11

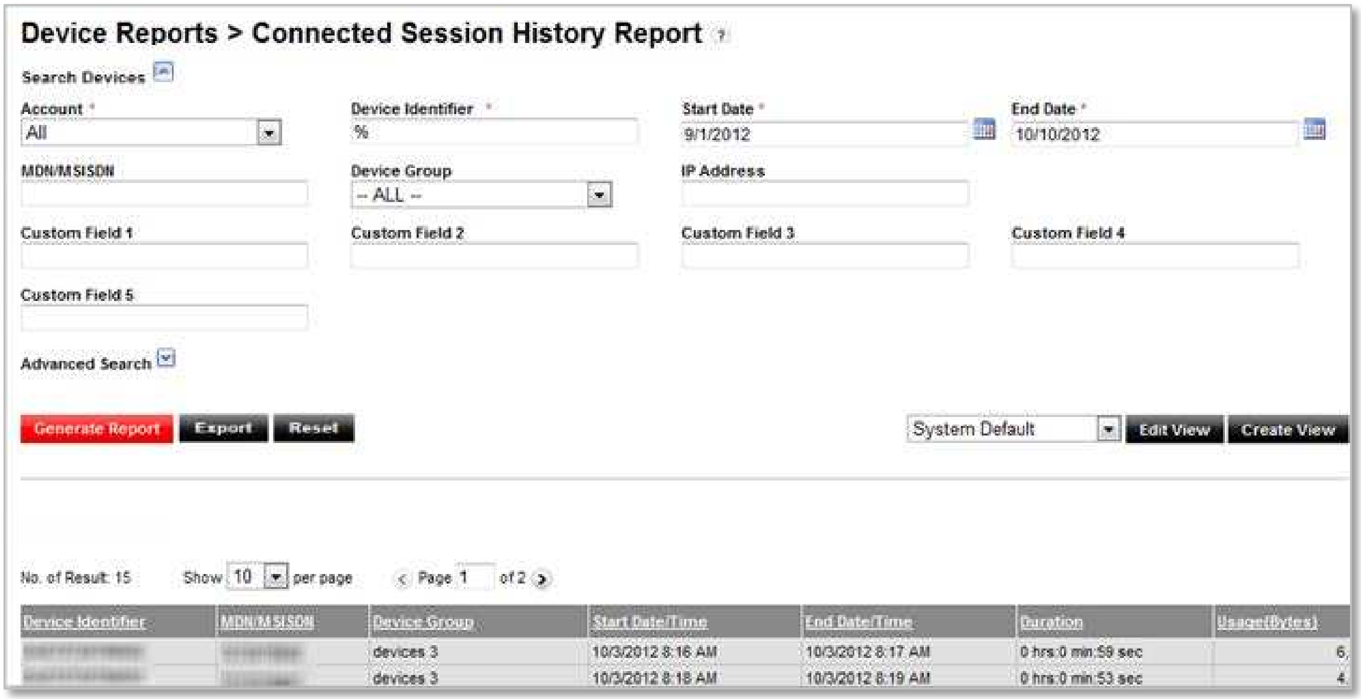
Device Identifier	MDN/MSISDN	Event Type / Request Status	Service Plan	Event Status	Description	Event By	Event Date
[redacted]	[redacted]	Activation Confirmed	M2M	Success	IP Address - [redacted]	User Verizon	6/29/2012 10:29:38 AM

Figure 4-2 Transaction History Report example

4.4.3 Connected Session History Report

The Connected Session History Report can show all connection sessions for one or more devices, plus the usage consumed and duration of each session, over a specific date range. A connection session is delineated by Start and Stop records.

NOTE; The Connected Session History 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 that have been connected for an extended period.



Device Reports > Connected Session History Report

Search Devices

Account * All	Device Identifier * %	Start Date * 9/1/2012	End Date * 10/10/2012
MDN/MSISDN	Device Group -- ALL --	IP Address	
Custom Field 1	Custom Field 2	Custom Field 3	Custom Field 4
Custom Field 5			

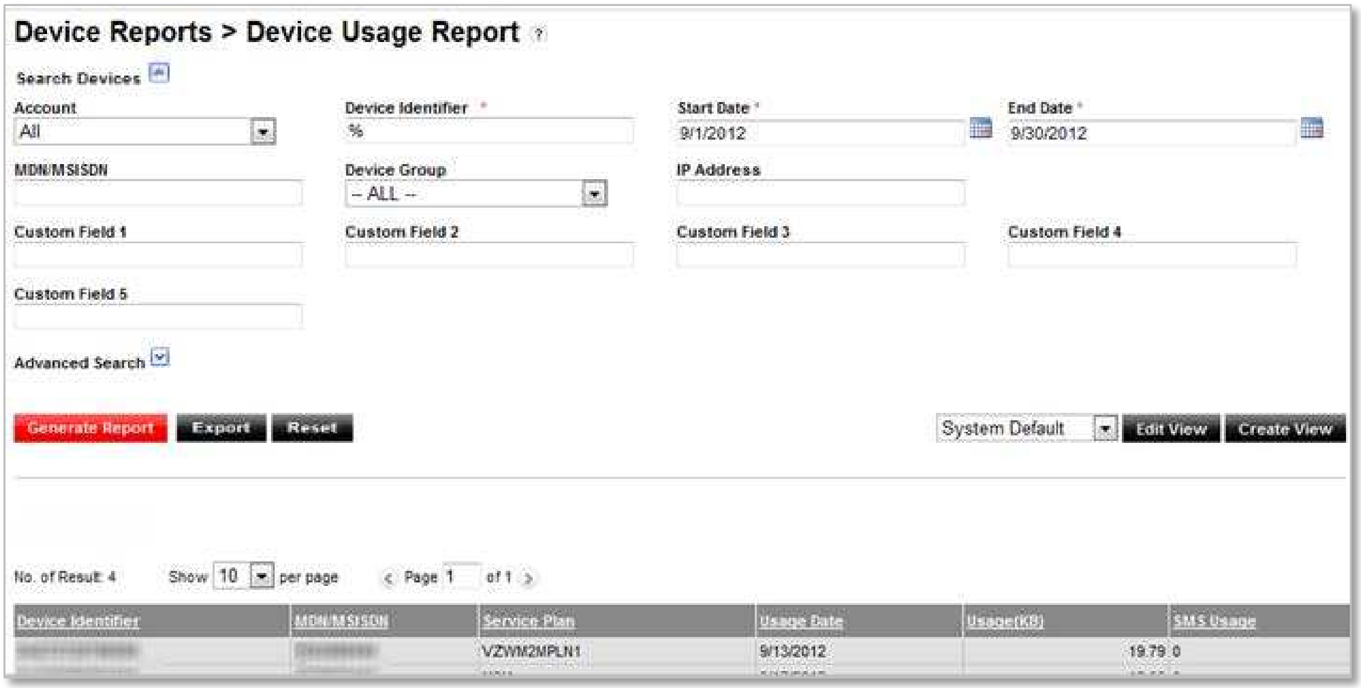
No. of Result: 15 Show 10 per page Page 1 of 2

Device Identifier	MDN/MSISDN	Device Group	Start Date/Time	End Date/Time	Duration	Usage(Bytes)
[redacted]	[redacted]	devices 3	10/3/2012 8:16 AM	10/3/2012 8:17 AM	0 hrs:0 min:59 sec	6,
[redacted]	[redacted]	devices 3	10/3/2012 8:18 AM	10/3/2012 8:19 AM	0 hrs:0 min:53 sec	4,

Figure 4-3 Connected Session History Report example

4.4.4 Device Usage Report

The Device Usage Report can give 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 6 hours for 4G devices that stay connected for extended periods.



Device Reports > Device Usage Report

Search Devices

Account: All

Device Identifier *: %

Start Date *: 9/1/2012

End Date *: 9/30/2012

MDN/MSISDN

Device Group: -- ALL --

IP Address

Custom Field 1

Custom Field 2

Custom Field 3

Custom Field 4

Custom Field 5

Advanced Search

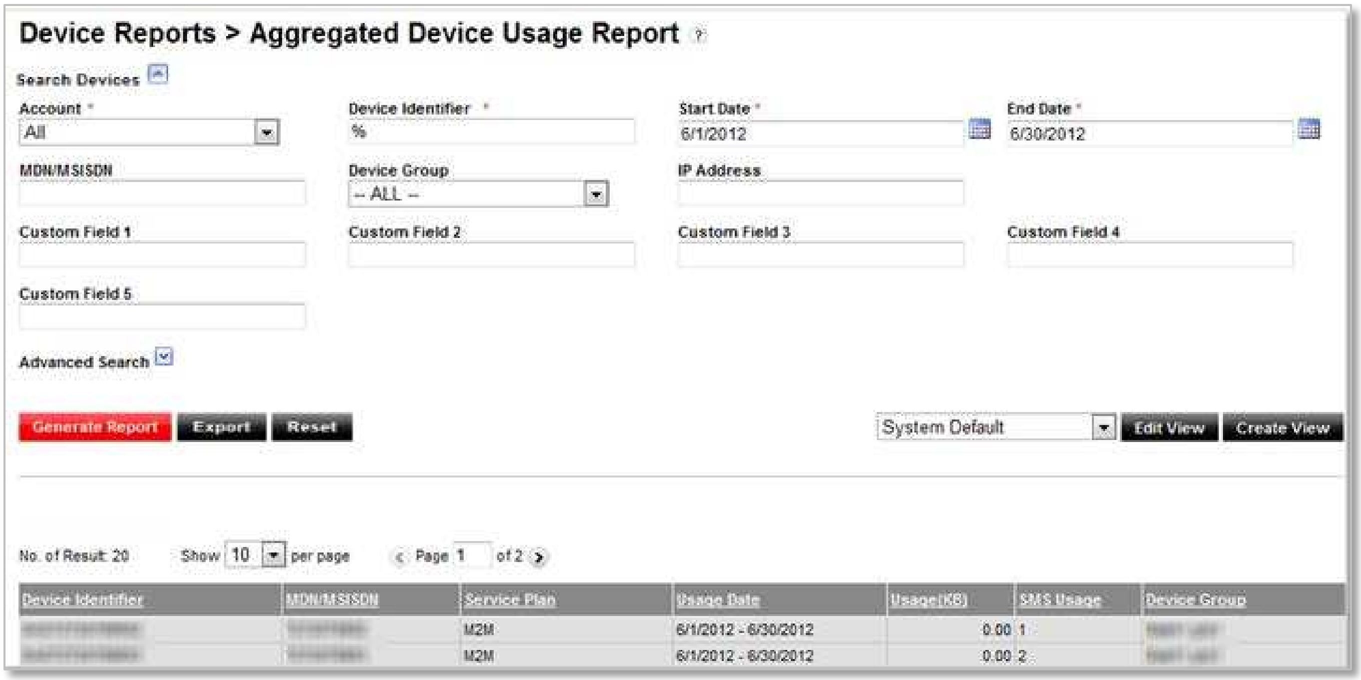
No. of Result: 4 Show 10 per page Page 1 of 1

Device Identifier	MDN/MSISDN	Service Plan	Usage Date	Usage(KB)	SMS Usage
[redacted]	[redacted]	VZWM2MPLN1	9/13/2012	19.79	0

Figure 4-4 Device Usage Report example

4.4.5 Aggregated Device Usage Report

The Aggregated Device Usage Report can include sums for data and/or SMS usage within a specified date range for devices included in the report. 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 6 hours for 4G devices that stay connected for extended periods.



Device Reports > Aggregated Device Usage Report

Search Devices

Account *: All

Device Identifier *: %

Start Date *: 6/1/2012

End Date *: 6/30/2012

MDN/MSISDN

Device Group: -- ALL --

IP Address

Custom Field 1

Custom Field 2

Custom Field 3

Custom Field 4

Custom Field 5

Advanced Search

No. of Result: 20 Show 10 per page Page 1 of 2

Device Identifier	MDN/MSISDN	Service Plan	Usage Date	Usage(KB)	SMS Usage	Device Group
[redacted]	[redacted]	M2M	6/1/2012 - 6/30/2012	0.00	1	[redacted]
[redacted]	[redacted]	M2M	6/1/2012 - 6/30/2012	0.00	2	[redacted]

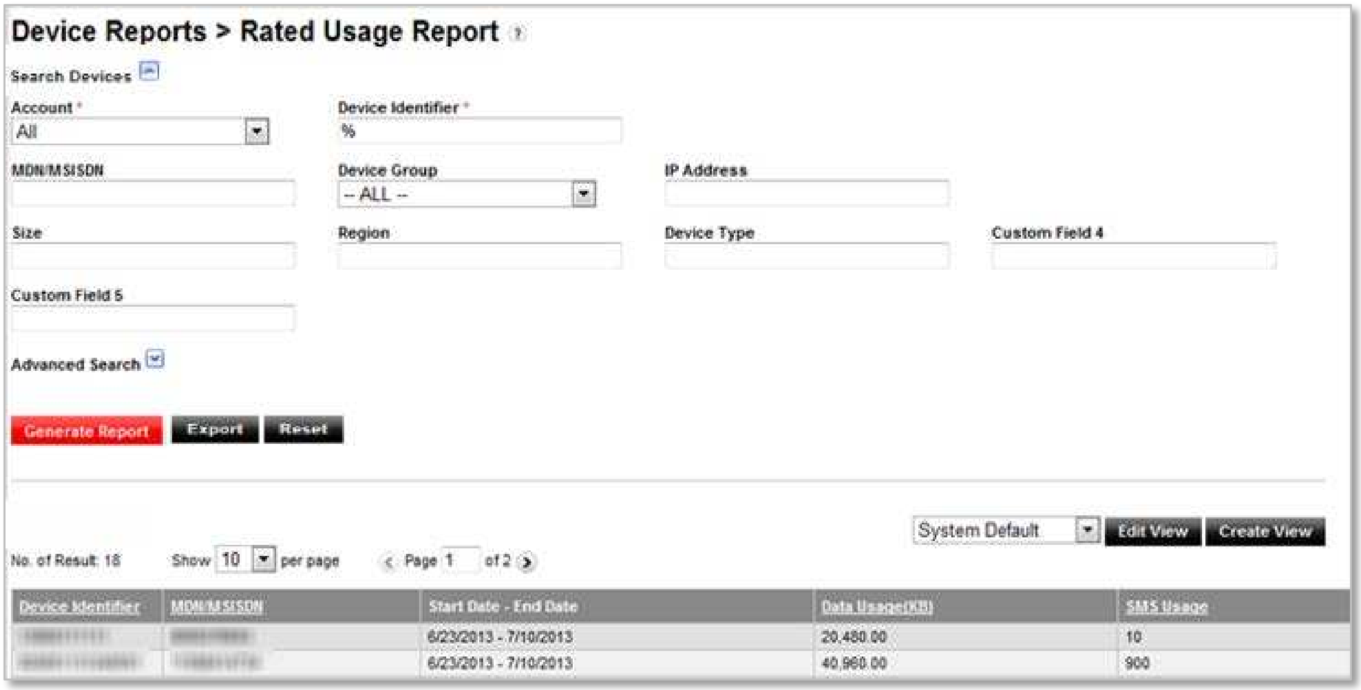
Figure 4-5 Aggregated Device Usage Report example

4.4.6 Rated Usage Report

The Rated Usage Report includes sums of unbilled data and SMS usage from the start of the selected device's current bill cycle to the latest date for which usage data is available.

NOTE:

- **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 start of the selected device's bill cycle. When you attempt to generate a report before data for the current bill cycle is available, this report displays data and SMS usage from the most recent bill cycle. Consult the column labeled "Start Date – End Date" to determine the billing period of the usage data included in the report.**



Device Reports > Rated Usage Report

Search Devices

Account *: All

Device Identifier *: %

MDN/MSISDN:

Device Group: -- ALL --

IP Address:

Size:

Region:

Device Type:

Custom Field 4:

Custom Field 5:

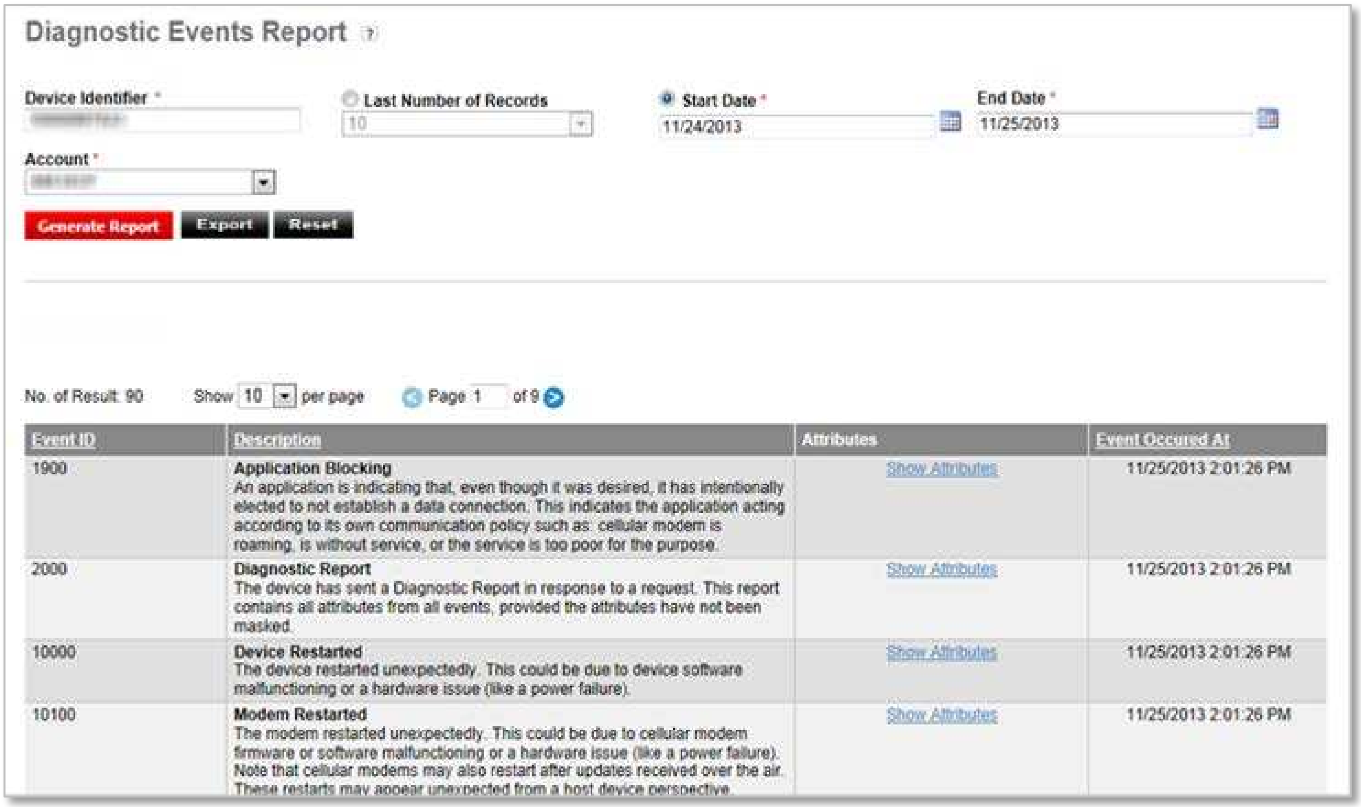
Advanced Search

No. of Result: 18   Show 10 per page   Page 1 of 2

Device Identifier	MDN/MSISDN	Start Date - End Date	Data Usage(KB)	SMS Usage
[redacted]	[redacted]	6/23/2013 - 7/10/2013	20,480.00	10
[redacted]	[redacted]	6/23/2013 - 7/10/2013	40,960.00	900

Figure 4-6 Rated Usage Report example

4.4.7 Diagnostic Events Report



Diagnostic Events Report

Device Identifier *: [redacted]

○ Last Number of Records: 10

● Start Date *: 11/24/2013

End Date *: 11/25/2013

Account *: [redacted]

No. of Result: 90 Show 10 per page Page 1 of 9

Event ID	Description	Attributes	Event Occured At
1900	**Application Blocking** An application is indicating that, even though it was desired, it has intentionally elected to not establish a data connection. This indicates the application acting according to its own communication policy such as: cellular modem is roaming, is without service, or the service is too poor for the purpose.	Show Attributes	11/25/2013 2:01:26 PM
2000	**Diagnostic Report** The device has sent a Diagnostic Report in response to a request. This report contains all attributes from all events, provided the attributes have not been masked.	Show Attributes	11/25/2013 2:01:26 PM
10000	**Device Restarted** The device restarted unexpectedly. This could be due to device software malfunctioning or a hardware issue (like a power failure).	Show Attributes	11/25/2013 2:01:26 PM
10100	**Modem Restarted** The modem restarted unexpectedly. This could be due to cellular modem firmware or software malfunctioning or a hardware issue (like a power failure). Note that cellular modems may also restart after updates received over the air. These restarts may appear unexpected from a host device perspective.	Show Attributes	11/25/2013 2:01:26 PM

Figure 4-7 Diagnostic Events Report example

4.4.8 Data Usage Trending Chart

This histogram shows data usage patterns of selected devices over a specified time period.

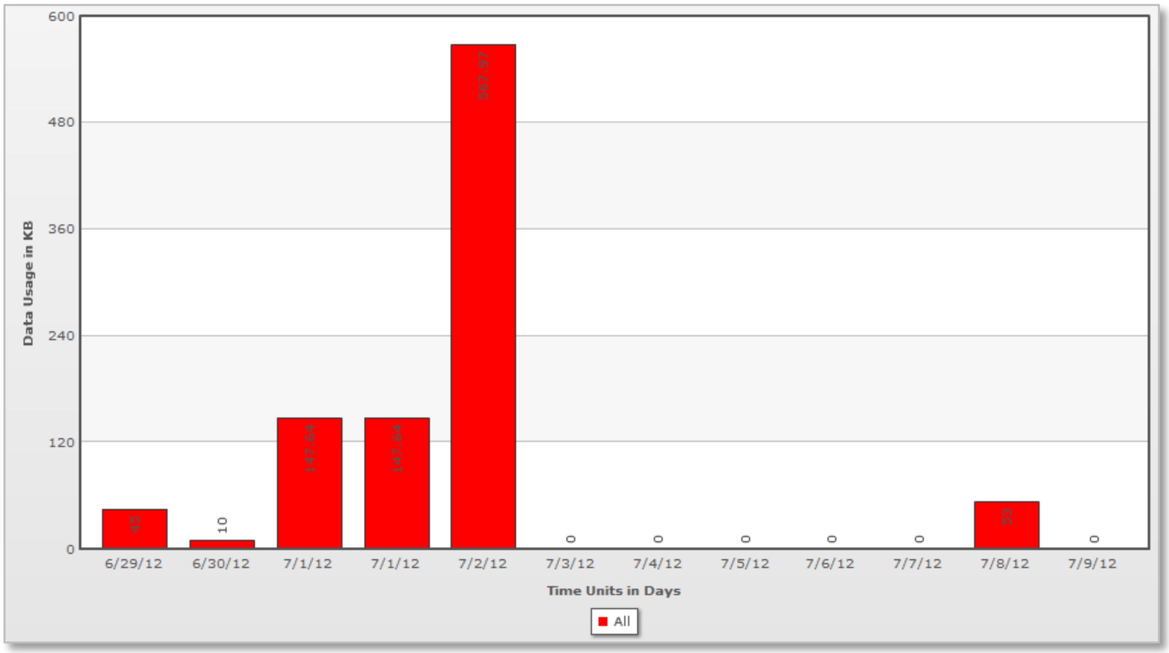


Figure 4-8 Data Usage Trending Chart example

4.5 Notifications

The M2M Management Center includes a notification feature that alerts groups of users when a value or status associated with a device changes, specific device events occur, or when certain data thresholds are breached. For example, you can establish a rule that notifies a field service technician when a remote device is consuming too much data or too little data, indicating a malfunction.

When the conditions of a notification rule are met, the system sends out a message using the media (email or SMS) specified for each recipient.

4.5.1 Notification Rules

Notification rules can be established for the following types of conditions:

+ **Data usage threshold**—This type of threshold applies when M2M data that passes 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 end of the latest data session and to within approximately 6 hours for 4G devices that stay connected for extended periods.
+ **Provisioning activity threshold**—This type of threshold is reached either when a specific provisioning event occurs or a specific number of device provisioning events occur within a certain time period (daily, weekly or monthly).
+ **Value/state change**—This type of alert is generated at the point when a value associated with a device or the state of a device changes.

Data usage and provisioning activity threshold notification rules are based on the following time periods:

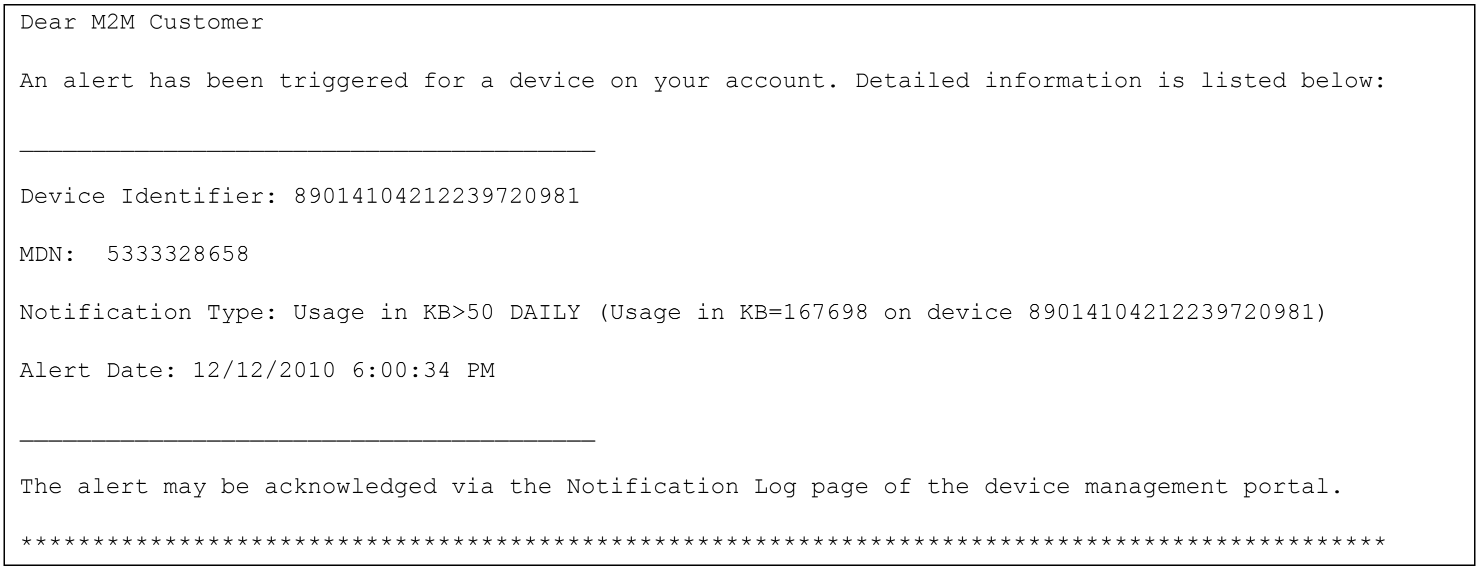
Notification Period	Description
Daily	The system determines the initial criteria level—i.e., the data usage or number of device provisioning activities that have occurred—daily at 12:00 am UTC, at which time the counter is reset. The system evaluates the criteria when various events occur throughout the day to determine if any threshold has been breached and generates notifications when a threshold value has been met or exceeded.
Weekly	For all weekly notification types, the system determines the weekly criteria level—i.e., the data usage or number of service provisioning activities that have occurred—at 12:00 am UTC on Monday of each week, at which time the counter is reset. The system also generates notifications at this time when any weekly threshold not related to usage has been breached. The system evaluates accumulated usage data throughout the week to determine if any weekly usage threshold has been breached. The system generates notifications when it determines that a usage threshold value has been met or exceeded.
Monthly	The system determines the initial criteria level—i.e., the data usage or number of device provisioning activities that have occurred—at 12:00 am UTC on the first day of the bill cycle each month, at which time the counter is reset. The system evaluates the criteria when various events occur throughout the month to determine if any threshold has been breached. Notifications are generated when the system determines that a threshold value has been met or exceeded.

You cannot change the timing of the daily, weekly and monthly checks described in the table above.

4.5.2 Notification Alerts

Notification alerts are either encapsulated in email messages or SMS messages that are sent to one or more recipients. The content of a notification message is preformatted and cannot be changed.

Below are two examples of notification alerts in both formats:



```
Dear M2M Customer

An alert has been triggered for a device on your account. Detailed information is listed below:

________________________________________

Device Identifier: 89014104212239720981

MDN:  5333328658

Notification Type: Usage in KB>50 DAILY (Usage in KB=167698 on device 89014104212239720981)

Alert Date: 12/12/2010 6:00:34 PM

________________________________________

The alert may be acknowledged via the Notification Log page of the device management portal.

***********************************************************************************************
```

Figure 4-9 Sample notification email

```
(M2M Portal Notification for <account>) <account> Alarm Notification
Device: <device MDN>. MDN/MSISDN: <device MDN/MSISDN>. Desc: Usage=
104KB >100.0KB DAILY,5/26/2010 2:03:00 PM
```

Figure 4-10 Sample notification SMS message

4.5.3 Acknowledgement and Resend Logic

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

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

4.6 System Users

NOTE: This section applies to Administrative-level users.

The M2M Management Center maintains contact information for notification purposes. When any user first enters the M2M Management Center within the Verizon Wireless My Business Account or the Verizon Enterprise Center, he/she is set up automatically as a contact.

As an administrator, you can specify and modify the Time Zone and SMS phone number fields for contacts in the M2M Management Center. Modifications to all other fields, such as name, phone number, etc., will be overwritten with information from the Verizon Wireless My Business Account or Verizon Enterprise Center the next time the user logs in. The Email field is an exception to this rule. When it is passed in from a user's record in the Verizon Wireless My Business Account or Verizon Enterprise Center, it populates the Email field in the M2M Management Center and is overwritten every time the user logs in. When it is not passed in and an administrative user displays a contact record, the Email field must be populated before exiting the screen. In this case, the Email address is saved with the contact's record.

When you update the Time Zone field to correlate with a contact's own time zone (default is Eastern Standard Time), time-related information in the M2M Management Center is changed to reflect the contact's time zone. When you use the notification feature and send SMS alerts, be sure to keep the SMS numbers of all contacts up to date so that notification alerts sent via SMS reach their recipients.

4.6.1 Alerts Only Contacts

Alerts Only contacts do not have access to My Business Account or the Verizon Enterprise Center; therefore, they are not users of the M2M Management Center. Alerts Only contacts only receive notifications; they do not have privileges to perform any other M2M device-related actions. You can also use the Alerts Only contact mechanism to set up an alias for a group to which you want to send notifications. Determine how you want to set the group up using the required fields listed below. Note that the First Name and Last Name fields accept space as a character.

+ First Name
+ Last Name
+ Email Address

4.7 System Security

NOTE: This section applies to Administrative-level users.

The M2M Management Center has two methods for securing an account and its underlying data: data security and role security. Data security is used to define a user's ability to view data related to specific devices or groups of devices. Role security is used to define a user's ability to access specific GUI functions.

Security Type	Description
Data	The system allows a user to access only devices and data that belong to the user's account (identified by Verizon Wireless company ID). A user assigned to an account will see all devices belonging to his/her account and only the devices belonging to his/her account. Note that users belonging to Verizon Wireless Internal Administrator groups have access to all Verizon Wireless customer accounts/devices.
Role	Role security defines the user interface functions that are accessible to users. Functions performed from within the M2M Management Center are assigned to roles, and roles are assigned to users. Different users have different access rights in the system. The M2M Management Center implements role security as follows: + When a user doesn't have access to a screen, the screen will not be an option in the menu. + When a user doesn't have access to a function, it is not visible and the user is not allowed to perform that function.

4.7.1 User Role Access Permissions

The following table shows the access permissions that apply to the two user roles recognized by the M2M Management Center:

User Action	My Business Account/Verizon Enterprise Center Customer Admin Role Access	My Business Account/Verizon Enterprise Center Cust Operator Role Access
Dashboard	✓	✓
Select Filter	✓	✓
Get Device List	✓	✓
Export Device List	✓	✓
View Device Info	✓	✓
Select View	✓	✓
Create View	✓	✓
Edit View	✓	✓
Delete View	✓	✓
Edit Default View	✓	
Assign Custom Fields	✓	✓
Wake Up Device	✓	✓
Remote PRL Update Device	✓	
Diagnostic Summary Device	✓	✓
Assign Device Group	✓	
Generate Connection History Report	✓	✓
Generate Transaction History Report	✓	✓
Generate Device Usage Report	✓	✓
Generate Diagnostic Events Report	✓	✓
Generate Aggregated Device Usage Report	✓	✓
Generate Connected Session History Report	✓	✓
Generate Rated Usage Report	✓	✓
Export Connection History Report	✓	✓
Export Transaction History Report	✓	✓

User Action	My Business Account/Verizon Enterprise Center Customer Admin Role Access	My Business Account/Verizon Enterprise Center Cust Operator Role Access
Export Device Usage Report	✓	✓
Export Diagnostic Events Report	✓	✓
Export Aggregated Device Usage Report	✓	✓
Export Connected Session History Report	✓	✓
Export Rated Usage Report	✓	✓
Download Report	✓	✓
Generate Data Usage Trending Chart	✓	✓
Get Contacts List	✓	
Add Contact (User Role = Alerts Only)	✓	
Edit Contact	✓	✓ (limited editing capabilities)
Delete Contact	✓	
Print Contacts	✓	
Get Notification Group List	✓	
Notification Group Setup	✓	
Notification Group Edit	✓	
Notification Group Delete	✓	
Get Notification List	✓	
Notification Setup	✓	
Notification Edit	✓	
Notification Delete	✓	
Dashboard Setup	✓	✓
Create Filter	✓	✓
Edit Filter	✓	✓
Delete Filter	✓	✓
Edit Default Filter	✓	
Get Device Group List	✓	✓
Create Device Group	✓	
Device Group Edit	✓	
Device Group Delete	✓	
Wake Up Device Group	✓	✓
Remote PRL Update Device Group	✓	
Set Custom Field Labels	✓	
Upload Attributes for Devices	✓	
Billing Account Preferences	✓	
Get Master Log	✓	
Print Master Log	✓	
Get Notification Log	✓	✓

User Action	My Business Account/Verizon Enterprise Center Customer Admin Role Access	My Business Account/Verizon Enterprise Center Cust Operator Role Access
Notification Log Acknowledge	✓	✓
Support tab	✓	✓

4.8 Time Zone

The M2M Management Center tracks all time-stamped data internally according to Coordinated Universal Time (UTC). However, your administrator can edit the Time Zone setting in your contact record to translate all time-related transactions that appear in the M2M Management Center to display in your local time. The default for the Time Zone setting is Eastern Standard Time (EST). Your local time zone can be set using the Add/Edit Contact screen (see the task Edit a Contact). Contact Setup is an administrative task.

4.9 Device-State Changes

Device-state changes include the following:

- Activate
- Deactivate
- Change ESN/MEID
- Change Service Plan
- Suspend
- Resume

Information that is passed from My Business Account or the Verizon Enterprise Center regarding these device-state changes drives certain features in the M2M Management Center such as the Master Log and Notification Engine.

The Master Log shows all activities that involve the M2M Management Center as well as system events reported as part of the Mobile Telephone Activation System (MTAS) feed to the M2M Management Center, including device-state changes.

The Notification Engine has the ability to send email and SMS notifications regarding device-state changes. It too is updated by the MTAS feed to the M2M Management Center.

4.10 Device Wakeup

The following rules apply to device wakeup:

- For any wakeup command to succeed, the device must have the Verizon Advanced M2M Client software.
- For an IP or SMS wakeup to be successful, the device must be powered on and registered on the Verizon Wireless or a roaming partner network.
- When a device is powered on but in an idle state, only an SMS wakeup will be successful.
- For accounts with the Customer Private Network feature, only SMS wakeup applies.

4.11 Device Upload File Format

The files you prepare to update devices must adhere to the following rules:

- File format must be comma-separated value (CSV) with column headers removed.
- Each line in the file corresponds to a single device record.

- A Verizon 2G/3G device record must identify a device by either its ESN or MEID. Including both identifiers is not acceptable; for instance, when both the ESN and MEID are provided for a 2G/3G device, only the ESN is stored.
- A Verizon 4G device record must identify a device by both its IMEI and ICCID. When both identifiers are not supplied, the update record is rejected.

File Format for Uploading Device Attributes

The format for uploading data for up to 1000 devices is:

```
ESN,MEID,IMEI,ICCID,Device Group Name,Custom Field 1,Custom Field 2,Custom Field 3,Custom Field
4,Custom Field 5
```

The following is an example file containing three device records:

```
09613615956,,,,ROUTERS,WEST,RTR-1AW,,,
09613615459,,,,ROUTERS,SOUTH,RTR-1BS,,,
,A1000009D61A21,,,ROUTERS,WEST,RTR-1BW,,,
```

Recommended Best Practices for Creating and Uploading a File

Use the following procedure to create a template for an upload file:

1. Go to the Device List and click Create View.
2. Give your view a name that denotes its purpose; for example, “Upload File Template”.
3. Include the following fields in this order in your new view.
   - Device Identifier
   - ESN
   - MEID
   - IMEI
   - ICCID
   - Device Group
   - Custom Fields 1-5, in order
4. Save your view.

The following procedure explains how to use your template to create an upload file:

1. Select your template view for the Device List and set the length of the Device List to show the maximum of 500 records.
2. Use the criteria to find the devices you want to update and click Search. (When your search returns more than 500 records, you must create multiple export files and combine the results in your spreadsheet application).
3. Click Export to create a CSV file containing the devices you want to update. The list will be exported as it appears and sent to the Download Center. You will receive an email when it is ready.
4. When your exported file is ready, go to the Download Center select the file you created from your template, and open it in a spreadsheet application. If you created multiple files because you have more than 500 devices (but not more than 1000) to upload, combine the files' results in the spreadsheet application.

   NOTE: If you are using Excel and your device identifier columns are not importing as plain text, use the procedure below titled Opening a File with the Excel Text Import Wizard.
5. In each device row, populate the Device Group and Custom Fields with the information you want to upload. When you leave a field blank for a device, its current value will be erased.
6. When all updates are complete, remove the first column of the file containing the Device Identifier.

7. Save the file in a CSV format and close your spreadsheet application.
8. Open the file in Notepad, remove the first row containing the column headers, and use File > Save As to save the file with a CSV format. The file is now ready to use as your upload file.

Opening a File with the Microsoft Excel Text Import Wizard

NOTE: Microsoft Excel 2010 was used for this procedure, which may vary when using other versions of the application.

The following procedure ensures that your device identifiers are not truncated. They will appear and be saved with the same format as identifiers you see in the M2M Management Center.

1. Open Excel, go to the Data tab, and select the From Text option.
2. When the Import File window appears, navigate to the file you exported from the M2M Management Center and click Open. The Text Import Wizard appears.
3. For Step 1 of the wizard, choose the following options:
   - Delimited
   - Start import at row 1
   - File origin = Windows (ANSI)
4. Click Next to proceed to Step 2 of the wizard.
5. Set the Delimiter to Comma (you may need to unselect Tab) and click Next to go to Step 3 of the wizard.
6. Click anywhere in the following columns and set them to Text format:
   - Device Identifier
   - ESN
   - MEID
   - IMEI
   - ICCID
7. Click Finish. When the Import Data dialog appears, click the Properties… button.
8. Choose the following properties for the file:
   - Save query definition
   - Prompt for file name on refresh
   - Adjust column width
   - Preserve cell formatting
   - Insert entire rows for new data, clear unused cells
9. Click OK on the Properties dialog, then click OK again on the Import Data dialog. The file will open in Excel with identifiers that match the values you see in the M2M Management Center.

4.12 Error Messages

The following error messages apply to the M2M Management Center. Each message contains instructions on how to proceed. Error messages are listed in alphabetical order.

Error Message	Occurs When:	Resolution
A Custom Field label must start with a letter or number.	You entered an invalid custom field label.	Supply a new custom field label that starts with an alphanumeric character.

Error Message	Occurs When:	Resolution
A group name may only contain letters, numbers, and a colon.	You did not supply a valid Device Group Name.	Enter a Device Group Name using only accepted alphanumeric characters and the colon.
Alarm criteria requires a date range selection.	You did not specify a period of daily, weekly or monthly.	Select the period at which to evaluate the alarm criteria from the drop-down list.
Alarm criteria requires a numeric value.	You did not enter a value in the KB/MB field.	Enter a numeric value in the KB/MB field.
Alarm criteria value is missing.	You did not specify KB or MB.	Drop down the Value list and select KB or MB.
Alarm name already exists.	You entered a name for the alarm that already exists.	Enter a unique Alarm Name value.
Alarm Type is not selected.	You did not select an alarm type for the notification.	Drop down the Alarm Type list and select a type.
An error has occurred while processing the current request. Please contact Customer Support. Click here for support information.	An error has occurred that prevents the system from completing your request.	Click the link provided to contact Customer Support.
An invalid character is included in the filter name. Filter names may only consist of alphanumeric characters and spaces.	You entered an invalid filter name.	Rename your filter, starting with an alphabetic character and using only alphanumeric characters and spaces.
An invalid character is in the name, names may only consist of letters, numbers, and spaces.	You entered an invalid view name.	Rename your view, starting with an alphabetic character and using only alphanumeric characters and spaces.
At least one account has to be selected from Available Accounts.	You did not select an account for the contact.	Select at least one account to associate with the contact.
At least one Contact and Notification Method has to be added.	You did not select at least one contact/notification method combination for your new notification group.	Drop down the Contact list and select a contact; then, choose a Notification Method for the contact and click the Add button.
At least one Role has to be selected from the Available User Roles.	You did not select any user roles for the new contact.	Select at least one user role to associate with the contact.
Available field selections for your view have been updated. Please re-create your view with the new selections.	You selected a custom view for the Connection History Report that includes a AAA group. AAA attributes must be selected individually for custom views of this report.	Edit the view to include one or more attributes in a AAA group, or all attributes in the group as preferred.
Because of the density of possible result data, the difference between the start date and the end date cannot be more than six months.	This report returns a large volume of data that has the potential to affect system performance.	Re-enter a date range that spans six months or less.
Connection history can be requested for a maximum date range of 7 days. Please adjust the date range and try again.	You specified a date range greater than seven days.	Adjust the date range to be seven days or less.

Error Message	Occurs When:	Resolution
Custom Field labels may only consist of letters, numbers, and spaces.	You supplied an invalid custom field label.	Enter a new custom field label using only alphanumeric characters and spaces.
Database error, please contact the Web administrator.	A data retrieval or commit operation could not be completed.	Contact your database administrator.
Data bucket values cannot be negative.	You entered a negative value in a data usage bucket field.	Enter a positive value in the data usage bucket.
Device Group is not selected.	You did not choose a device group for which to aggregate notifications.	Drop down the Device Group list and select a group.
Device Identifier is required field.	You failed to provide a Device Identifier on which to report.	Enter a Device Identifier or use the wildcard character.
Device Identifier can only contain alphanumeric characters.	You entered an invalid Device Identifier.	Re-enter the Device Identifier using only alphanumeric characters.
Devices from different billing accounts may not be added to the same group.	You tried to create a mixed-account device group.	Close the Assign To Device Group pop-up and select only devices with the same Account value for grouping.
Duplicate alarm name, name has been used.	You entered an alarm name that was used for another notification.	Re-enter a unique Alarm Name.
Duplicate group name.	You entered a device group name that was used for another device group.	Re-enter a unique Device Group Name.
Either the End date format is not correct or the start date is later than the end date.	You entered an invalid date in the End Date field.	Enter the End Date using MM/DD/YYYY format or select an End Date from the Date pop-up that is later than the Start Date specified.
Email address is missing.	No value provided in the Email field of the Add/Edit Contact screen.	Populate the Email field for the contact with a valid address.
emailId field is blank/empty.	The emailId field is blank/empty.	Populate the Email field for the contact with a valid address.
End Date must be greater than or equal to the Start Date.	You entered a date range in reverse order.	Re-enter the End Date, ensuring it is later than the Start Date, or enter a new, correct date range.
Enter a custom field value that contains alphanumeric and valid special characters only. Refer to the User Guide or online help documentation for the list of special characters that can be used for custom fields.	You entered at least one invalid character in a custom field.	Check the list of accepted characters (see Assign Custom Fields to Devices) and re-enter the custom field value.
Error while creating device group.	You entered a duplicate Device Group Name.	Enter a new, unique Device Group Name.
[Field] is too long.	Your entry has exceeded the restrictions of the named field.	Re-enter information in the field, adhering to the data length rules.
Invalid character in custom field.	You entered a non-alphanumeric character in a Custom Field.	Correct the invalid Custom Field value using up to 50 alphanumeric characters.

Error Message	Occurs When:	Resolution
Invalid group name.	You entered invalid characters in the Device Group Name field.	Re-enter a valid Device Group Name. Device Group Name should begin with an alphabetic character, followed by alphanumeric characters, up to a maximum of 100 characters. Acceptable special characters include SPACE and colon (:).
Invalid group name (too short or too long).	You entered no characters or more than 100 characters in the Device Group Name field.	Re-enter a valid Device Group Name.
Invalid new group name.	You entered no characters or invalid characters in the Device Group Name field.	Re-enter a valid Device Group Name. Device Group Name should begin with an alphabetic character, followed by alphanumeric characters, up to a maximum of 100 characters. Acceptable special characters include SPACE and colon (:).
Maximum PRL update requests over last 'X' days exceeded. ('X' is configured at on-boarding.).	You attempted to perform one or more PRL updates and exceeded the maximum number of updates allowed during the configured period.	You must wait until the current period ends and the new period begins before attempting to perform any PRL updates.
Notification Group is not selected.	You did not select a notification group to receive alerts.	Drop down the Notification Group list and select a group.
Notification Group name already exists.	You entered a duplicate notification group name.	Enter a unique Notification Group Name.
Notification Group name cannot be left blank.	You did not supply a name for the new notification group.	Enter a unique Notification Group Name.
No wildcards are allowed for the device identifier.	You entered the wildcard character (%) in the Device Identifier field.	Wildcard searches are not allowed in report criteria fields; enter a complete Device Identifier, or copy and paste an identifier from the Device List screen.
Only one device can be selected for the Report.	You supplied more than one device identifier for the report.	Enter only one device identifier on which to report.
Phone: Please use the format 8001112222 for the phone number.	You entered an invalid phone number.	Enter the phone number in the proper format.
Please enter an Alarm Name.	You did not enter an alarm name for a notification rule.	Enter a unique Alarm Name.
Please enter an email with valid format (yourname@yourdomain.com).	You did not enter a valid email address.	Enter the email address in the proper format.
Please enter a valid integer for the Alarm Compare Value.	You entered a non-numeric or invalid value for the alarm type to compare.	Enter a valid value to compare in the alarm criteria.
Please enter a valid integer for the Rogue Device Compare Value.	You entered non-numeric data in the number of KB field.	Enter the number of KB for the compare value.
Please provide values for all required fields	You did not populate at least one required field on the Add/Edit Contact screen.	Provide all required information for the contact.

Error Message	Occurs When:	Resolution
Please select an alarm compare operator.	You neglected to choose < or > for an alarm that requires criteria definition.	Drop down the Comparison Operator list and choose one.
Please select a device for the report.	You chose to generate a report, but did not specify any devices to include.	Supply at least one device identifier on which to report.
Please select a Device Group.	You checked the Aggregate checkbox, but did not select a Device Group for the notification.	Drop down the Device Group list and choose a group for the notification rule.
Please select an account.	You did not select a billing account when you entered the M2M Management Center.	Drop down the Billing Account Selection list, choose the nine-digit billing account that includes the devices you want to manage and click Apply.
Please select an alarm check interval.	You neglected to choose the period at which to evaluate the notification condition.	Drop down the list and select DAILY, WEEKLY or MONTHLY.
Please select an alarm type.	You did not choose an Alarm Type for the notification.	Drop down the Alarm Type list and choose one for your notification.
Please select a Notification Group.	You neglected to select a Notification Group to which to send alerts.	Drop down the Notification Group list and choose a list of contacts to receive the notification.
Please select a time zone.	The contact record does not have a Time Zone associated with it.	Drop down the Time Zone list and choose one for the contact.
Please select a valid action for the Rogue Device.	You did not choose the Suspend action for the Rogue Device rule.	Drop down the Action menu and choose the only selection: Suspend.
Please select only one device for this function.	Either you chose more than one device for the Diagnostic Summary command or multiple devices match the search criteria you provided for the Diagnostic Events Report.	Select only one device before trying to view the summary or generate the report.
Please select the device(s) from the list.	You selected an action from the Device List Actions menu, but did not select a device.	Return to the Device list and select one or more devices, depending on the action you want to perform.
REQUEST_FAILED. Device is already active	The Verizon Enterprise Network system rejected your request because you tried to activate a device that is already Active.	Select another device to activate.
REQUEST_FAILED. Device is not valid	The Verizon Enterprise Network system rejected a device ESN because it was not determined to be E911-compliant.	Select an E911-compliant device for the action.
REQUEST_FAILED. Maximum daily Suspend/Reconnect limit reached for MDN.	The Verizon Enterprise Network system rejected your request because it exceeded the daily limit allowed for the transaction type.	Wait and try the transaction again another day.
PRL Update Request Not Admitted. Please check device.	The Base Station Identifier (BSID) is not available.	Re-try the PRL update request.

Error Message	Occurs When:	Resolution
[Required field] is missing.	You did not supply any information in the named required field.	Enter required information.
Rogue device criteria require an action selection.	You did not specify the Suspend action for the Rogue Device Alarm Type.	Drop down the Action menu and select the only option: Suspend.
Rogue device criteria require a numeric value.	You entered non-numeric data in the KB field.	Enter numeric data into the KB field.
Since the magnitude of the result is huge, the query is timing out at the database, please decrease the time interval between Start Date and End Date by at least half and try again.	The date range you entered returns a large volume of data that has affected system performance.	Re-enter a new date range of one month or less.
SMS bucket values cannot be negative.	You entered a negative value in an SMS bucket field.	Enter only positive numeric values in the SMS bucket fields.
SMS: Please use the format 6195551234@domain for a phone number or the format name@site.com for an email address.	You used an invalid format for an SMS value.	Enter SMS values using the proper format for phone number or email address.
Some of the data buckets are not in numeric format.	You entered non-numeric data in a data usage field.	Enter only numeric values in the data usage bucket fields.
Some of the data bucket values are too large.	You exceeded the value restrictions on at least one data usage bucket.	Enter data usage bucket values, keeping within the acceptable range allowed for the field, which is 1 to 1,999,999,999.
Some of the sms buckets are not in numeric format.	You entered non-numeric data in an SMS bucket field.	Enter only positive numeric values in SMS bucket fields.
Some of the sms bucket values are too large.	You exceeded the value restrictions in at least one SMS bucket field.	Enter SMS bucket values, keeping within the acceptable range allowed for the field, which is 1 to 1,999,999,999.
Specified device does not support PRL update.	You selected to update the PRL of a device that does not support the feature.	Ensure that all devices chosen for PRL update have a Verizon Advanced M2M client.
Specified device was not found in system.	You selected a device for PRL update that cannot be located in the database.	Re-enter a valid device ID.
The Contact already belongs to this Application.	You selected a duplicate account for the contact.	Inspect the list of accounts associated with the contact and delete any duplicates.
The Contact and Notification Method combination already exists.	You entered a duplicate contact/notification method combination for a notification group.	Either select another contact for the method selected or choose another notification method for the contact.
The description contains an illegal character, only alphanumerics and spaces are allowed.	You entered an invalid view description.	Enter a new description for the view, using only alphanumeric characters and spaces.
The device identifier doesn't belong to your account or the device identifier is not correct.	You entered an invalid Device Identifier.	Enter the identifiers to include in the report. You may cut and paste identifiers from the Device List screen.

Error Message	Occurs When:	Resolution
The name of a filter must begin with a letter.	You entered an invalid filter name.	Provide a filter name that starts with an alphabetic character.
The name of a view must begin with a letter.	You entered an invalid view name.	Enter a view name that starts with an alphabetic character.
The selected devices already belong to a Device Group. Clicking OK will move these items from their current Device Group to the new Device Group.	This message is not an error; it is meant to inform you that devices will be removed from their current group because they can only belong to one group at a time.	Either accept (click OK) or reject (click Cancel) the proposed device moves.
The start date cannot be later than the end date.	You entered a date range in reverse order.	Enter the Start and End Dates again, ensuring that the Start Date is earlier that the End Date.
The start date cannot be more than six months in the past. Please select a more current date.	You entered a date more than six months prior to the current date. Data is only retained for six months.	Enter a Start Date that is less than six months prior to the current date.
The start date format is not correct.	You entered an invalid date in the Start Date field.	Enter the Start Date, using MM/DD/YYYY format, or select a date from the Date pop-up.
There are no notification methods available for this contact.	The contact you selected does not have any entries in the Email or SMS fields.	Select another contact to notify, or add an email address or SMS information to the contact record.
There are some errors on loading the page, please contact Customer Support for further assistance.	The system has encountered problems and cannot display the M2M Management Center screen you requested.	Go to the Support page, which includes contact information for the Customer Support organization.
This Chart filter name is already being used.	You entered a duplicate filter name.	Enter a new, unique filter name.
This Notification Group is currently being used by a Notification, please reassign the Notification Group before deactivating it.	You chose to deactivate a notification group that is currently selected to receive alerts.	Drop down the list and choose another notification group, or remove the notification group from all notifications before deactivating it.
This page cannot be viewed in another window. Please close this window and return to the previous browser session.	Occurs when you break out of an iFrame by right-clicking and opening a link in a new tab. The M2M Management Center detects this by noticing that it is no longer part of a frameset.	Close the current window and return to your previous browser session, or start a new browser session when needed.
This report cannot be generated on the screen. Instead, it will be sent to the Download Center. To continue, click OK. A confirmation email will be sent to: [logged-in user's email address from contact record] Or, click Cancel to cancel this action.	The data set is too large to render the report on-screen.	Click OK to generate a report file offline and make it available in the Download Center, or click Cancel to dismiss the message.

Error Message	Occurs When:	Resolution
This view cannot be applied to the selected data set because it exceeds the number of allowable data points to be displayed. Please refer to the User's Guide or Online Help for information on chart data limitations and then select another view.	You chose a view that results in a data set that exceeds the number of individual bars that can be rendered legibly in the chart. The maximum number of bars the chart displays is 50. Other limits of this report include: + Maximum days: 50 + Maximum weeks: 12 + Maximum device groups: 7	Adjust the criteria for the report to reduce the number of device groups or days selected for display, or select another view with less data points to display. When you have more than seven (7) device groups in an account, you should set the Group By option for your views to All to populate this chart with data.
Transaction history can be requested for a maximum date range of 30 days. Please adjust the date range and try again.	You specified a date range greater than 30 days.	Adjust your date range to be 30 days or less.
UpdatePRL action is valid only for 'ACTIVE' devices. Please select a device group with only active devices to perform this action.	You chose the Remote PRL Update action for a device group that has one or more devices with a status of Deactive or Suspend.	Choose a device group with all devices in an Active state and then select the Remote PRL Update action.
UpdatePRL action is valid for 'ACTIVE' devices. Please select only active devices to perform this action.	You chose the Remote PRL Update action for one or more devices with a status of Deactive or Suspend.	Choose only devices with an Active status and then select Remote PRL Update action.
Username already exists for another user, please select another username for this contact.	You entered a duplicate Username value for a contact.	Enter a unique Username value for the contact.
Username is missing.	You did not supply a Username value for a contact.	Enter a unique Username value for the contact.
Wakeup action is valid only for 'ACTIVE' devices. Please select a device group with only active devices to perform this action.	You chose the Wakeup action for a device group that has one or more devices with a status of Deactive or Suspend.	Choose a device group with all devices in an Active state and then select the Wakeup action.
Wakeup action is valid for 'ACTIVE' devices. Please select only active devices to perform this action.	You chose the Wakeup action for one or more devices with a status of Deactive or Suspend.	Choose only devices with an Active status and then select the Wakeup action.
Warning: You are nearing the maximum number of PRL Update requests allowed in this 'x'-day period.	You have submitted a PRL Update request that is near Y% of the limit, where Y is a configurable value that is usually set to 80%.	No action is necessary. This message is a warning.
We are currently experiencing issues, please select another option from the main menu and try again.	Appears when you try to connect to the M2M Management Center from a Verizon Wireless My Business Account entry point and the connection cannot be established. This may happen when: + The connection is lost. + An error occurs when validating the security token.	Return to the Verizon Wireless My Business Account or Enterprise Center and re-access the M2M Management Center using one of the links available.
You are allowed 10 report requests per day. Please try this request again tomorrow.	You attempted to export more than ten reports/lists in a single day.	Wait until tomorrow to export a report or list.

Error Message	Occurs When:	Resolution
You do not have privileges to access this page.	You attempted to navigate to a screen for which you do not have the proper role for access.	Choose another screen in the M2M Management Center that is compatible with your user role.
You may only modify one device at a time.	You selected multiple devices for an action that can be performed on one device only.	Select only one device and then choose your selection again from the Actions menu.
Your XXX request was unsuccessful. Please review your request with your Company Administrator to see whether it can be administered via Verizon Enterprise Center or My Business. NOTE: This error message applies to all transactions.	You tried to change the state/service plan of a device that was already in the requested state/had the requested service plan. NOTE: For Change Price Plan, this error can arise due to the potential for inconsistency in device service plan information between Verizon Enterprise Network and the M2M Management Center.	No action is necessary. You may check the Transaction History Report to determine when the device state/service plan change was made.