User guide

Verizon Mobile Device Management Portal

Top 7 unified endpoint management (UEM) admin activities to manage company assets

verizon

Contents

Thank you for purchasing Business Mobile Secure. Business Mobile Secure is a powerful combination of Lookout®—to help protect your mobile devices against phishing and app-, network- and device-based threats—and unified endpoint management (UEM), a feature of Verizon Mobile Device Management (MDM) that allows you to easily streamline device and app deployments, set controls and maintain security. This multilayer security approach includes access to tech experts who can help with onboarding, setup and end-user support.

It's time to set up your Verizon MDM portal. You can do this by logging into Verizon My Business (MyBiz) and clicking the **Verizon MDM** link to gain access to your customer portal. The Verizon MDM guide will provide instructions on how to effectively manage device permissions and control your mobile devices.

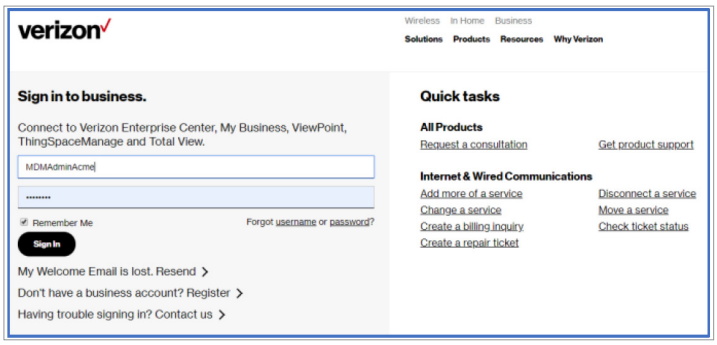
Reminder: You also need to activate your Lookout for Small Business license using the Lookout portal. The Lookout for Small Business guide will provide instructions on how to enroll your mobile devices, helping to protect them against the latest security threats.

Introduction

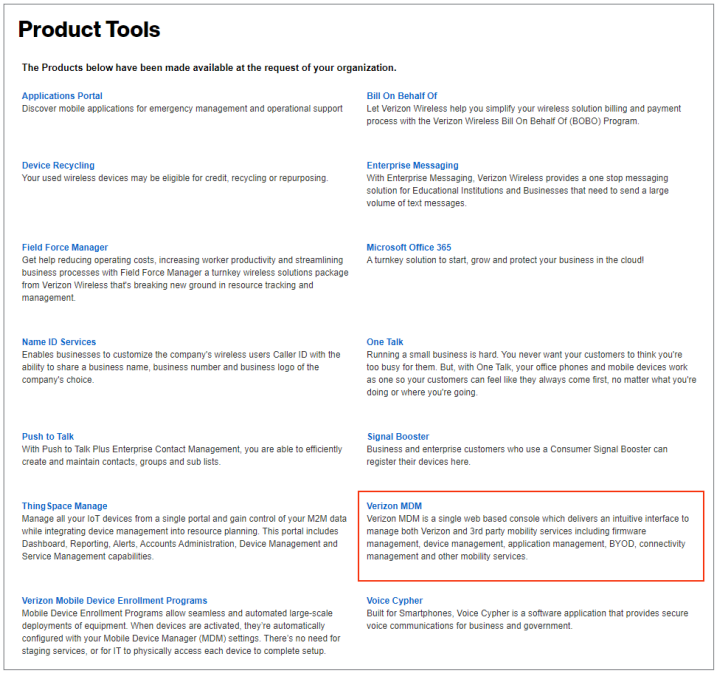
This guide describes how to use the top seven administrative controls over the most important features of the Verizon MDM portal and is intended for admins as a quick-start guide for managing your remote company assets. This introduction covers commonly used features that include password policy, device restrictions, installing apps, passcode resets, wiping remote devices, and events and actions.

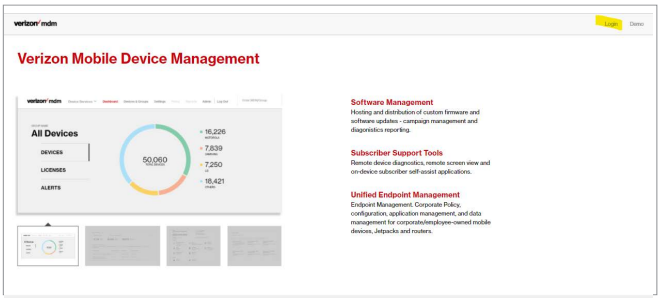
1. Login

Log in to Verizon's My Business (MyBiz) site, then follow the path below:



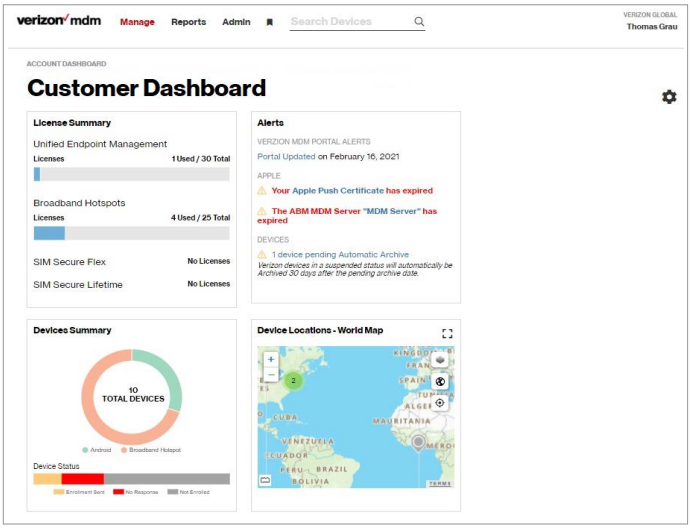
MyBiz Login > Manage Account > Product Tools > View All > click the Verizon MDM link





You will be presented with the Dashboard display of your company's instance.

The License Summary displays the number of licenses consumed from the total.



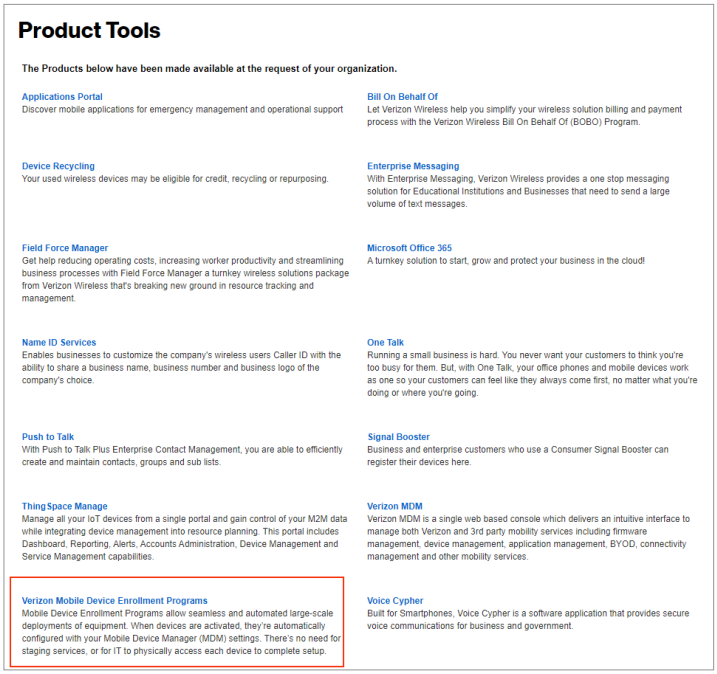
The Verizon MDM portal has a wide range of controls for admins to deploy, and group orientation is a persistent theme in controlling remote assets. Some groups, like warehouse staff, for example, have access to specific applications for their work roles (e.g., a QR code reader) and need policies crafted for those roles (e.g., "Restrict Apple Pay® setup"). Others, such as management staff, will have access to applications specific to their roles (e.g., QuickBooks®) and policies crafted for their respective roles (e.g., "Enable watch migration in Apple® iOS").

Some policies apply to all user roles and are configured from the admin portal in advance of the device being activated and enrolled in your group policies.

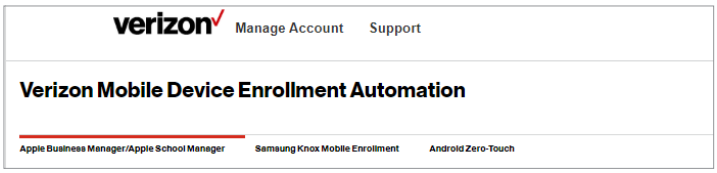
2. Verizon Mobile Device Enrollment

As a prerequisite to managing your smart devices via your Verizon MDM portal, your device IDs must be enrolled in their respective original equipment manufacturer (OEM) enrollment programs. The Verizon Mobile Device Enrollment program can be accessed in your My Business account under Product Tools.

MyBiz login > Manage Account > Product Tools > View All > click the **Verizon Mobile Device Enrollment Programs** link



You will be presented with the following landing page to select the appropriate OEM enrollment program:



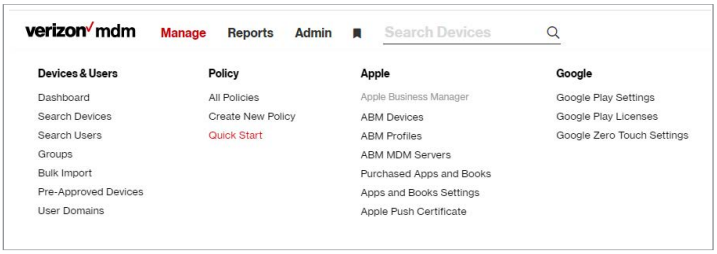
After enrolling your devices, they must be synced from the Apple Business Manager/Apple School Manager to your Verizon MDM portal instance. In your Samsung Knox® Mobile Enrollment (KME) portal, device IDs will get pushed to your Verizon MDM portal instance using the Android Package (APK) URL you entered. In Zero Touch, a coded message is pasted into your Zero Touch portal that points back to your MDM portal. In both KME and Zero Touch, either device records must be in the portal or the device International Mobile Equipment Identities (IMEIs) must be in the preapproved devices list.

3. Policies

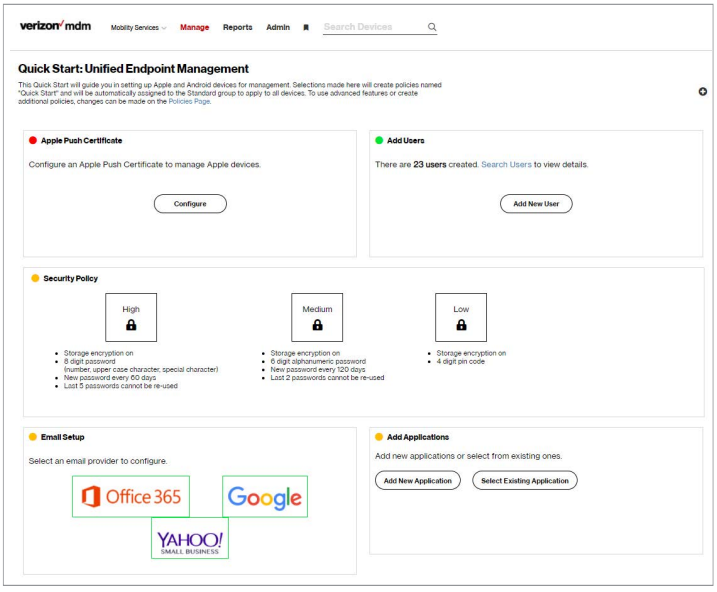
3.1. Passwords

Passwords are set by assigning the passcode policy to a group whose membership contains devices where the passcode requirements will be applied. When those devices enroll and check in, the policy will be pushed and installed, and users will need to change or improve their device passwords to match the policy requirements.

The easiest way to set a password policy is via the Quick Start menus on the portal dashboard. Select **Dashboard** in the menu, then **Unified Endpoint Management** under Quick Start Menu:



Select **Security Policy** and choose **High**, **Medium** or **Low**. Descriptions are below. These policies are automatically assigned to the Standard group. The Standard group contains all new users and devices by default:



Password requirements can be configured via Policy > Add a Policy > Passcode Policies.

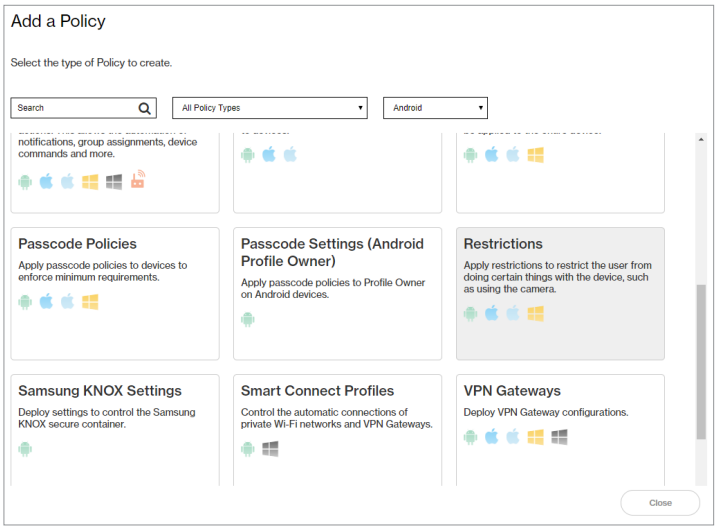
After creating a new password policy, you will be asked to assign it to a group. You can also edit policies created via the Quick Start method above.

3.2. Restrictions

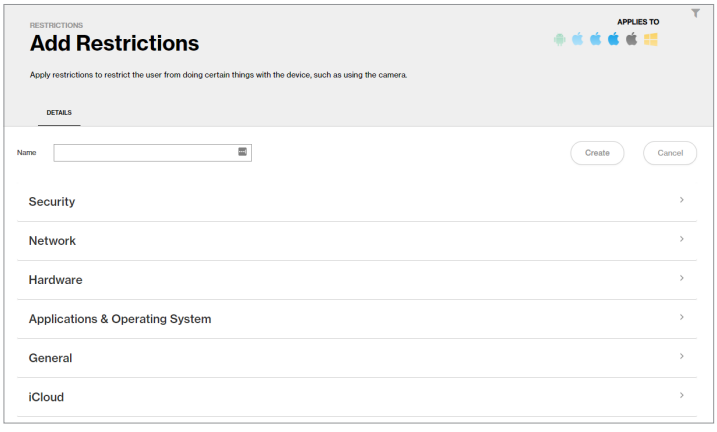
Many restrictions can be applied to devices under management, from blocking the camera to allowing calls from certain numbers.

All the restrictions are defined in one policy, but within that policy, different platforms (like Apple or Android) can have different settings.

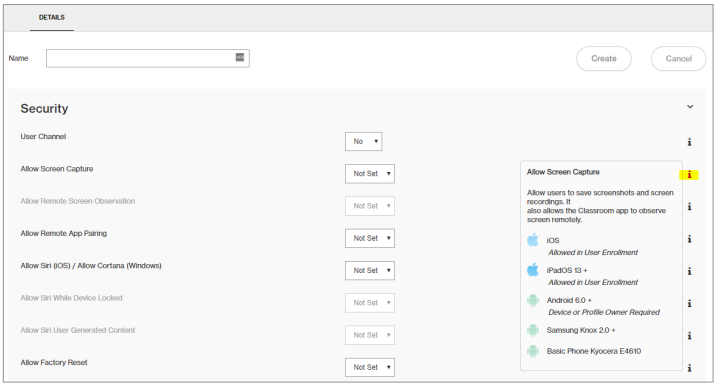
Create a restrictions policy via Policy > Add a Policy > Restrictions:



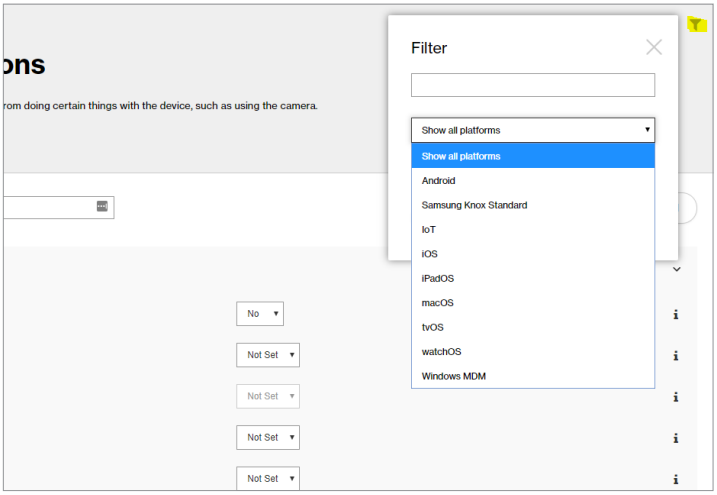
The restrictions policy provides an extensive range in managing groups of devices, and contains five major sections: Security, Network, Hardware, Applications and Operating Systems:



Within each section and for each setting, hovering over the “i” (for “information”) will show which devices will be affected by that setting:



You can also use the Filter button in the upper right to limit the features based on operating system:



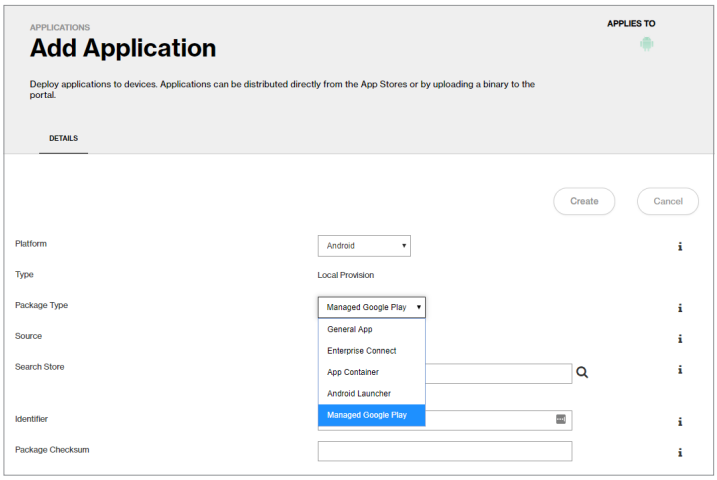
4. Installing apps

Apps can be automatically installed on devices when they check in to the portal. Apps can be downloaded from online stores (Apple or Google) or uploaded directly to the portal.

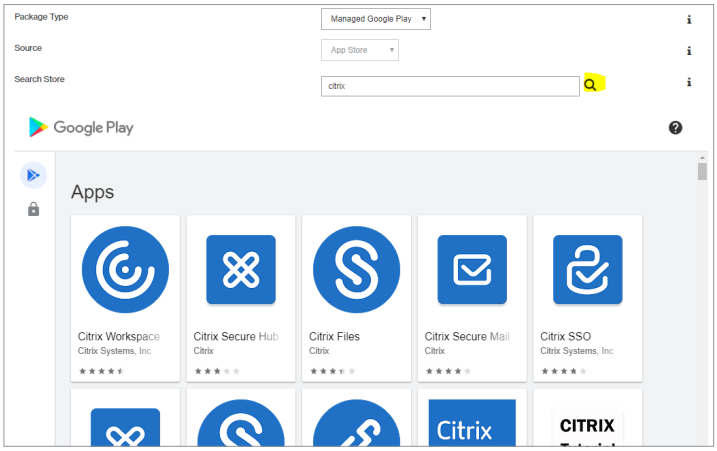
Apple App Store® and Google Play® store apps are best installed with Apple Business Manager or Managed Google Play and must be set up before applications are created. Apple apps are configured inside the Apple Business Manager portal, not Verizon MDM. Using those services are described in separate documents.

Here's the process: Create the app definition and assign it to a group. As a device in that group checks in, the app will be retrieved and installed on the device.

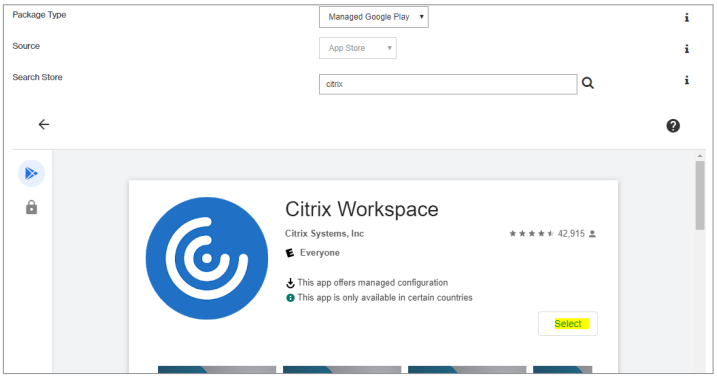
Browse to Policy > Add a Policy > Add Application:



Search for an app:



Choose your app and click **Select**, then **Create** and **Assign to a group**:



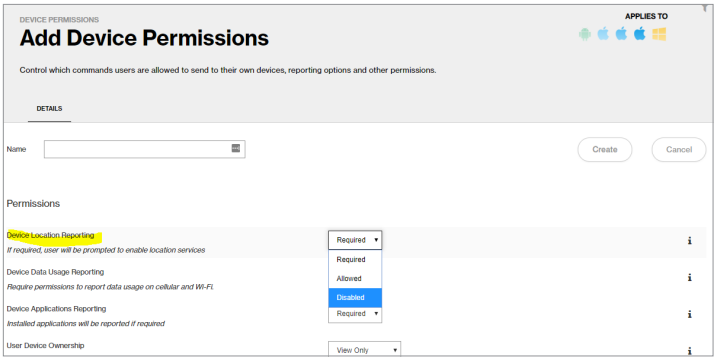
(Apple App Store apps are synced to Verizon MDM from Apple Business Manager and only group assignment is done in Verizon MDM.)

5. Device and portal location settings

Location must be enabled on devices and can be checked using the Settings control.

In the portal, from the Devices page in the Location tab, there will be a map with the location of your managed device as reported on its last check-in.

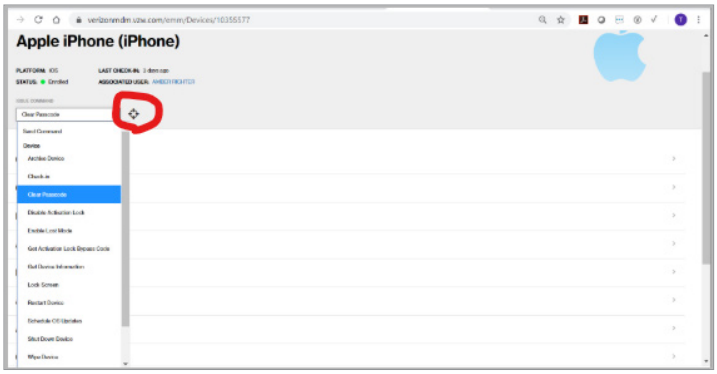
If device location reporting is not desired for a group, just assign a device permissions policy with Device Location Reporting set to Disabled:



6. Reset passcode

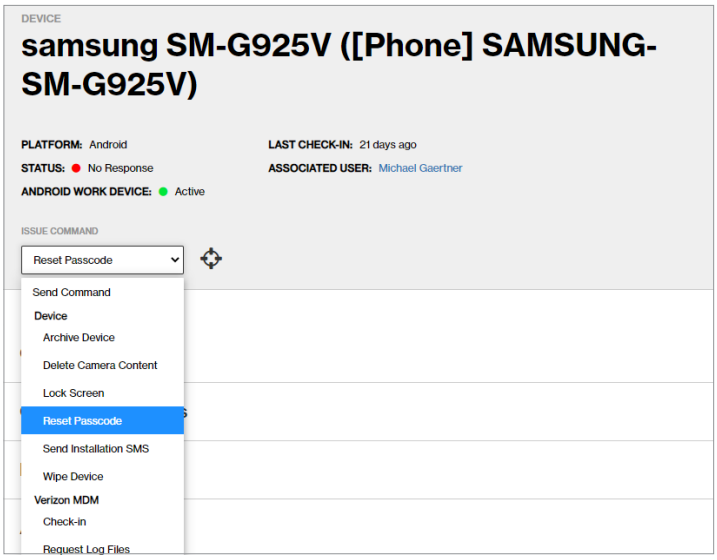
6.1. Apple

The Verizon MDM portal includes a Clear Passcode command for Apple iPhone® and iPad® devices, which you can use by selecting it from preset commands and clicking the **Send Command** button (circled in red):

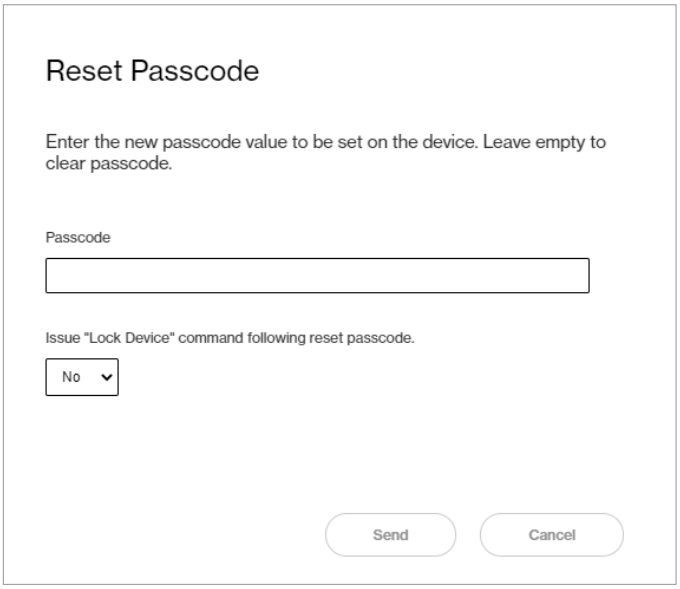


6.2. Google Android

On the device page, choose **Reset Passcode** and click the **Send Command** button:

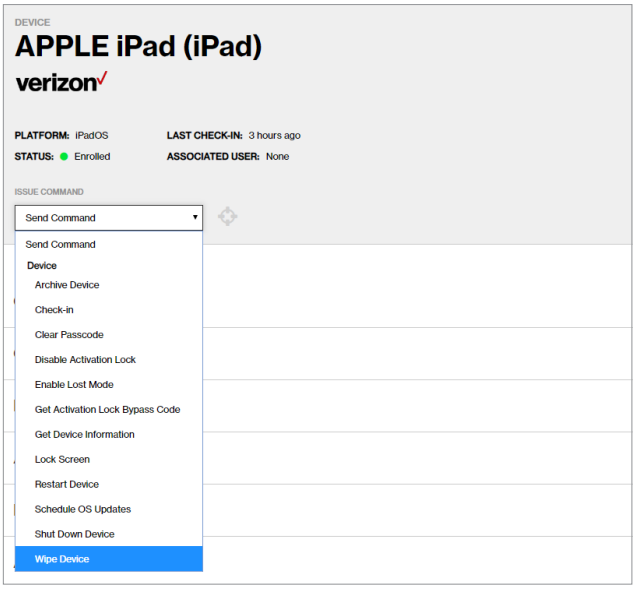


You can either reset the password or clear it and allow the user to reset it:



7. Wipe

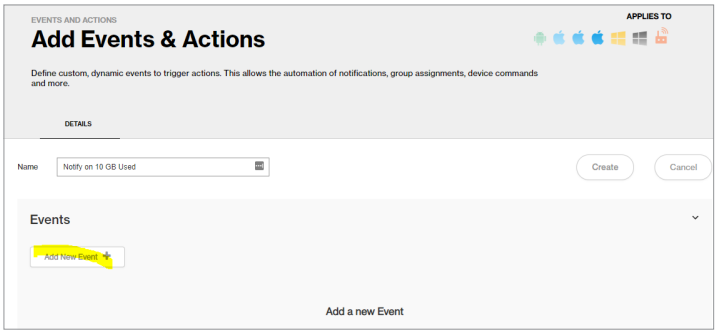
A factory reset “wipe” can be issued to any enrolled device from the device page. It immediately delivers a factory reset command over the air to the device and commands the device when received.

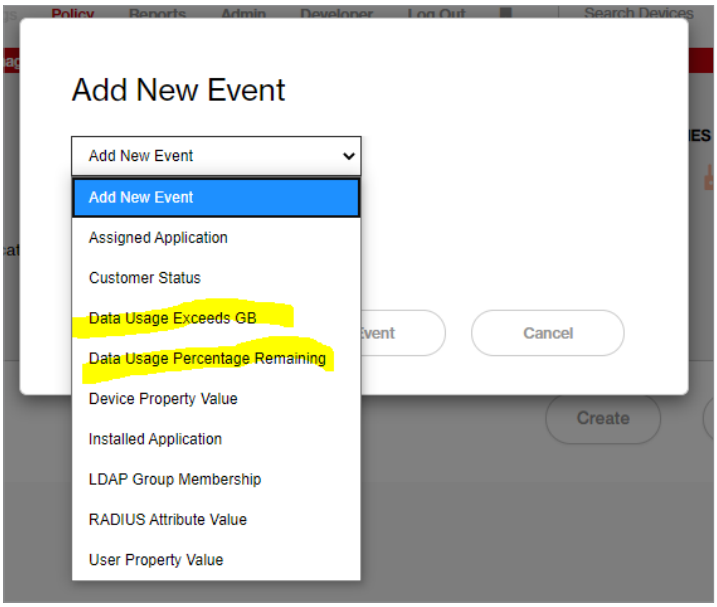


8. Events and actions

As a new policy to be added, select **Add Events & Actions** for certain events, such as the new data usage events “Data Usage Exceeds GB” and “Data Usage Percentage Remaining.”

Add a new event and choose **Data Usage Exceeds GB**, for example.

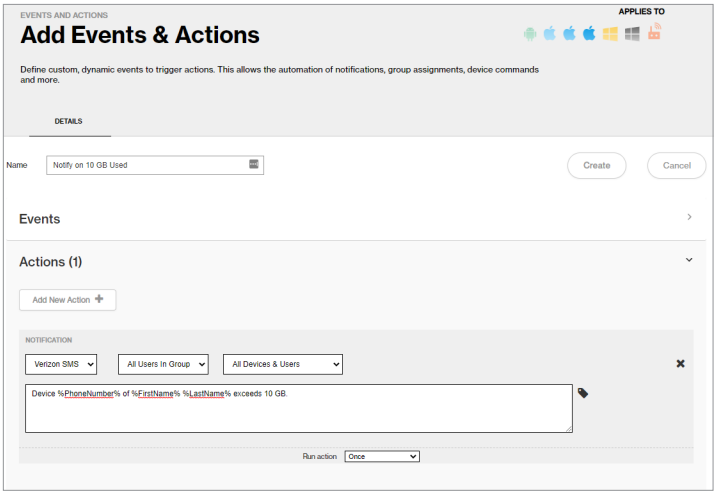




Then set an action (notification) that will be triggered by the device exceeding the data usage event. Select **Notification** from the pull-down menu.

Indicate the notification method from the preset choices (Verizon SMS), any group assignment for the notification and the payload of the notification message.

Message input can be text and replacement tokens like phone number, first name and last name if the device is associated with a user in the portal:



The Label button to the right of the message box can be used to see all the available replacement tokens: