Preventing Unauthorized Device Data Usage

Link: https://help.wextelematics.com/deep-dive/preventing-unauthorized-device-data-usage/ Last Updated: June 25th, 2021

Some GPS devices are capable of providing internet access and/or custom cellular connectivity. This article discusses the impact of if/when the use of these devices leads to unintended/unexpected data usage because of internet or cellular activity.

What is Unauthorized Data Usage?

In general, unauthorized data usage is any instance where a device's internet or cellular connection is used to access data that is outside the authorized use of your service provider and/or your organization. Examples include using a device's hosted wifi to access social media sites or tapping into a device's cellular connection to SMS (text) or make calls.

How is this Type of Activity Monitored?

Device data usage is monitored daily with alert systems created to notify our Support team when a device reports exceptionally high, or otherwise odd, data usage. When the alert system is triggered our team reviews the activity of the device, including researching the time frame for the data usage increase and, if necessary, the IP addresses of sites the device was using.

What to Expect if Unauthorized Data Usage is Detected

If our team has identified a device experiencing unauthorized data usage, the device's service is suspended and an email notification is sent to your organization's lead contact(s). This email notification requests the contact, or designated personnel at your organization, work directly with our team so that we may detail the type of usage detected, define how the device and usage will be handled moving forward, and ultimately determine how and when to reactivate the device for service.