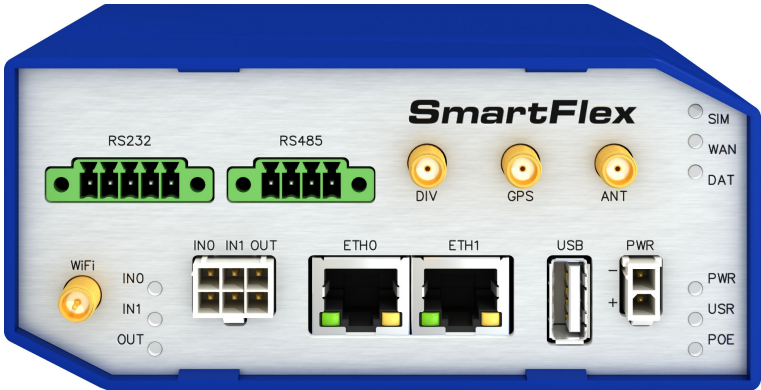
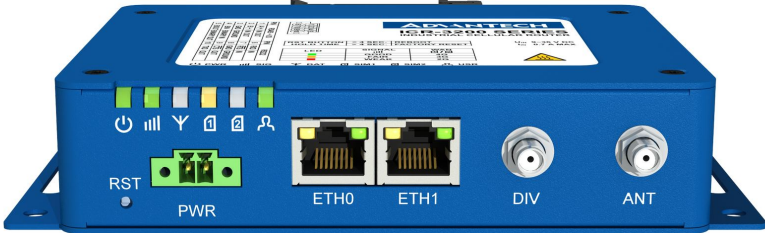




Firmware 6.2.7

RELEASE NOTES



Abstract

This document describes:

- Firmware update instructions.
- Description of all new features, fixes and other changes implemented in the firmware.
- Known issues related to a firmware version.

Firmware Details

- **Firmware version:** 6.2.7
- **Release date:** December 17, 2020
- **Hardware compatibility:** applicable to the Advantech routers

Please note that not all new Advantech routers are produced and shipped with the latest release of the firmware. The reason for this is usually an existing certification valid for a specific carrier or a region. For more information about the latest version of the firmware for your router, see the *Firmware Distribution Overview* document.



For current and detailed information about the router configuration see the latest version of the *Configuration Manual* for your router.

Product related documents and applications including the firmware can be obtained on *Engineering Portal* at <https://ep.advantech-bb.cz/> address.

Part I

Firmware Update Instructions

General Update Instructions and Notices

HTTPS certificates: The HTTPS certificate format in the router was updated in FW 5.3.5 to improve the security. Existing HTTPS certificates on previously manufactured routers will not automatically be updated with the firmware update! It is possible to update the HTTPS certificates by deleting the files within `/etc/certs/https*` in the router (e.g. via SSH). The certificates will be re-created automatically during the router's next start.

Specific Update Instructions

New filename: If the filename of firmware for your router was changed, you will meet with an issue during manual firmware updating or with automatic firmware update feature. This warning message will appear during the firmware updating process: *"You are trying to upload file "xx.bin" but "yy.bin" is expected. Are you sure to continue?"*

To proceed with the firmware updating please follow these steps: Check the table below for details about recent firmware filename changes and make sure you have the correct firmware file for your router. Go ahead with manual firmware updating and confirm the displayed warning message.

To proceed with automatic firmware updating, rename new firmware files (*.bin and *.ver) to filenames valid before the filename change. This should allow the router to pass through the process of automatic firmware updating. Next time, the automatic firmware update feature will work as expected with no need to rename the file.

Router model	FW ver.	New filename	Original filename
SmartMotion ST352 SmartMotion ST355	6.0.2	SPECTRE-v3T-LTE.bin	BIVIAS-v3LL.bin
SmartStart SL302	6.0.3	SPECTRE-v3L-LTE-US.bin	SPECTRE-v3L-LTE-AT.bin

Table 1: Recent Firmware Filename Changes

Updating Firmware of Version Less than 5.3.0



It is necessary to follow specific update instructions below only if you are updating from firmware older than 5.3.0.

Due to a bug in the firewall (now fixed) when a WAN device is part of a bridged interface, caution should be taken when updating in following case:

Condition: When a WAN device is part of a bridged interface, access to that WAN device (HTTPS, SSH) is always granted regardless of configuration.

Problem: If this is your configuration, it is highly likely that you are not aware of this, so the undesired effect of the bridge firewall fix may render the router inaccessible.

Recommended Action: Enable access to both the web and ssh services before updating if you want to retain the current behavior (access to the WAN interface). This can be done on the *NAT* page in the *Configuration* section of the router's Web interface.

Change the root's password:

It is necessary to change the password for the *root* user when updating to the firmware version 5.3.0 or newer. The reason for this is an update of the authentication system (encryption algorithm *crypt* was changed to *MD5*; passwords are now stored in the */etc/shadow* file instead of */etc/passwd*). The change of the password is required before setting up the remote access on the *NAT Configuration* page.

Please note that when downgrading from 5.3.0+ to previous firmware versions, the password for the *root* user is reset to the default one, which is *root*.

Part II
Changelog



Legend: Affected products are marked as shown below for every changelog item:

Affected product Not affected product

WiFi Short GI Configuration

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ					
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E	
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH					
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307				
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x			

We have added support of short guard interval (GI) configuration to the WiFi AP configuration GUI. The guard interval is the space between symbols (characters) being transmitted. The guard interval is there to eliminate inter-symbol interference, which is referred to as ISI.

In normal 802.11 operation, the guard interval is 800 ns. With 802.11n, shorter guard intervals are possible. The short guard interval time is 400 ns, or half of what it used to be. Using Short Guard Interval can increase the data rate by roughly 10%, depending on the operating environment.

WiFi AP Bandwidth Configuration

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ					
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E	
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH					
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307				
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x			

Configuration of the 80 MHz bandwidth is supported from now in the WiFi AP GUI. The current *BW 40 MHz* configuration option was replaced with the *Bandwidth* option, where the 20 MHz, 40 MHz or 80 MHz bandwidth can be chosen. Please note that the 80 MHz bandwidth is supported for the 802.11ac mode and ICR-3200 products only.

Support for Hardware UUID

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

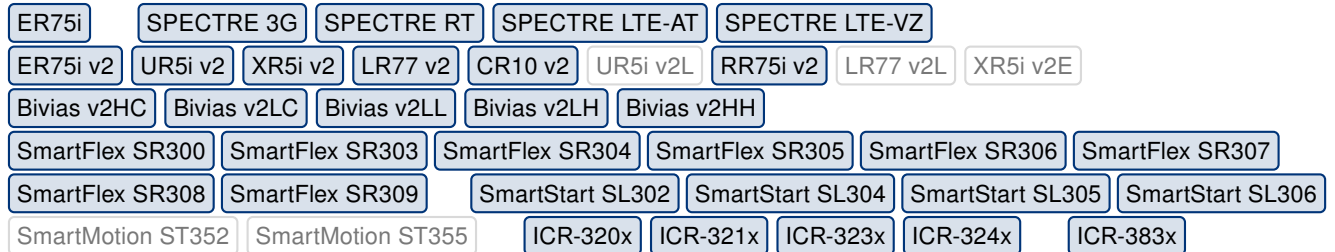
We have implemented the router UUID, a unique identification string, which is stored in the U-Boot environment. This feature is reserved for future usage.

Radio Technology Status

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

The LTE-M and NB-IoT radio access technologies are now supported by the *Technology* item on the *Mobile WAN* status page. By now, both of these technologies were indicated by LTE string.

Expansion Ports Commands



We have added two new commands to the CLI to control the expansion ports. These programs are *port1* and *port2*, the *port1* command controls the first expansion port, the *port2* command controls the second expansion port. Syntax for both commands is described below.

Synopsis:

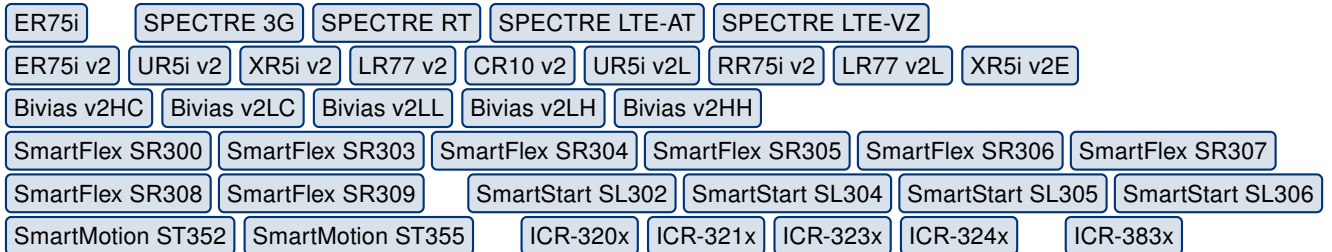
```
port1 [on|off|auto|rs232|rs485]
port2 [on|off|auto|rs232|rs485]
```

Options:

Option	Description
on	Turn on the expansion port.
off	Turn off the expansion port.
auto	Turn on the expansion port and set the flow control (CTS signal) to RS232 or RS485 mode depending on the type of the expansion board.
rs232	Turn on the expansion port and set the flow control (CTS signal) to RS232 mode.
rs485	Turn on the expansion port and set the flow control (CTS signal) to RS485 mode.

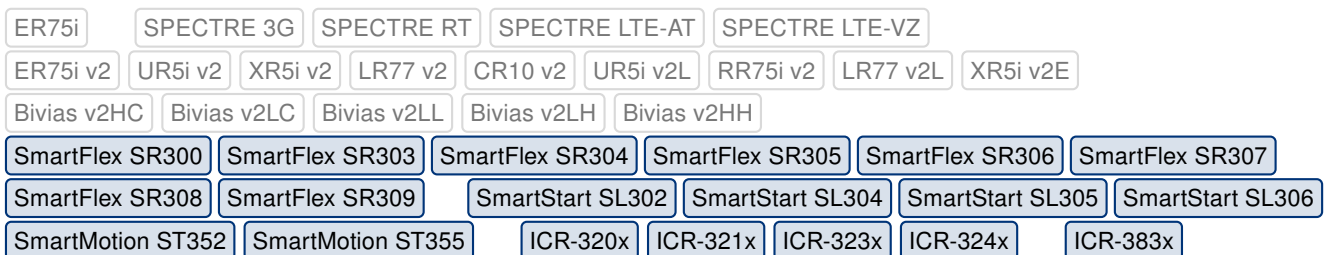
Table 2: port1 and port2 options

User Authentication Logging



We have added logging of unsuccessful web login event into the syslog, due to the security and monitoring reasons.

Product ID Usage



We have implemented a feature for reading out the *ProdID* from the U-Boot environment. The *ProdID* is string representing product name of the router and is written in the U-Boot environment for all newly manufactured products. The product name is now part of the product title used in the administration GUI of the router. The table below lists the title formats for various product lines:

Old Product Title	New Product Title
SmartFlex LAN Router	SmartFlex <ProdID> LAN Router
SmartFlex LTE Router	SmartFlex <ProdID> LTE Router
SmartStart LAN Router	SmartStart <ProdID> LAN Router
SmartStart LTE Router	SmartStart <ProdID> LTE Router
SmartMotion LTE/LTE Router	SmartMotion <ProdID> LTE/LTE Router
ICR-xxxx Industrial Communication Router	<ProdID> LAN Router
ICR-xxxx Industrial Cellular Router	<ProdID> LTE Router

Table 3: Product Title Overview

Commands Permission Check

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

A strict permission check is now performed when running a command requiring the administration (root) permission. This type of command is not executed any more, instead the *Permission denied* error message is returned. This fix will eliminate a confusion with incorrect command output, for a command requiring the administration permission, such as `status`, `report`, `gsmat`, `io`, etc., if executed without the administration permission.

POSIX Message Queues Support

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have enabled the POSIX message queues in Linux kernel, so it can be used by a user module. POSIX message queues allow processes to exchange data in the form of messages. For more information see [mq_overview manual page](#).

Fixed Key File Importing

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have fixed an issue with importing of an encrypted private key file when the file content was not processed correctly.

Fixed Linux Kernel Vulnerabilities

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

This update has fixed [CVE-2020-10135](#) (medium), [CVE-2020-12351](#) (high), [CVE-2020-12352](#) (medium), [CVE-2020-24490](#) (high) and [CVE-2020-25705](#) (high) in the Linux kernel.

Updates for WiFi Module

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

The firmware of the *Laird SU60* WiFi module updated to fix the throughput issue. Moreover, the module driver was updated to the latest version of number 8.2.0.17.

Updated TACACS+ Module

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have updated the *TACACS+* authentication PAM module to version 1.6.1. This update has fixed [CVE-2020-27743](#) (critical) and [CVE-2020-13881](#) (high).

Updated OpenSSL Library

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have updated the *OpenSSL* library to version 1.1.1i. This update has fixed [CVE-2020-1968](#) (low) and [CVE-2020-1971](#) (high).

Updated OpenVPN Software

ER75i	SPECTRE 3G	SPECTRE RT	SPECTRE LTE-AT	SPECTRE LTE-VZ				
ER75i v2	UR5i v2	XR5i v2	LR77 v2	CR10 v2	UR5i v2L	RR75i v2	LR77 v2L	XR5i v2E
Bivias v2HC	Bivias v2LC	Bivias v2LL	Bivias v2LH	Bivias v2HH				
SmartFlex SR300	SmartFlex SR303	SmartFlex SR304	SmartFlex SR305	SmartFlex SR306	SmartFlex SR307			
SmartFlex SR308	SmartFlex SR309	SmartStart SL302	SmartStart SL304	SmartStart SL305	SmartStart SL306			
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have updated the *OpenVPN* software to version 2.4.10. For more details about this release, see the webpage at <https://openvpn.net/community-downloads/>.

Part III

Known Issues

Firmware Update – Unexpected Filename

If the filename of firmware for your router was changed, you could have an issue during manual firmware updating or with Automatic Update feature. This warning message will appear: *"You are trying to upload file "xx.bin" but "yy.bin" is expected. Are you sure to continue?"* To fix this issue follow instructions in Part I - [Firmware Update Instructions](#).

Automatic Update – Update to Version 6.1.10

The feature of automatic firmware update will not recognize the firmware version 6.1.10 as a new version in case the installed version of firmware is from 6.1.0 to 6.1.8. To fix this issue, either update the firmware by the automatic update to version 6.1.9 first or update it manually directly to the version 6.1.10.

WiFi Configuration – Lost After Firmware Downgrade

If the firmware is downgraded to the version less than 6.2.0, the WiFi configuration will be lost completely.

ICR-3200 – Country Code for WiFi

The first version of the firmware for the WiFi module does not support the settings of the country code. Due to this issue, the settings of the country code made on the configuration page has no effect at all. The country code is set up during the manufacturing process according to the product destination region.

SmartStart – Cellular Network Registration

It is necessary to use router's firmware version 6.1.5 or higher if the *Telit* cellular module installed in your SmartStart router has following version of the firmware:

- *Telit LE910-EU V2* cellular module with firmware version 20.00.403 or newer,
- *Telit LE910-NA1* cellular module with firmware version 20.00.014 or newer.

Note: The model name and firmware version of the cellular module can be found on router's web GUI at *Mobile WAN Status* page in *Mobile Network Information* section.

SmartStart SL302 – Cellular Network Authentication

It is not possible to use username and password when connecting to Mobile WAN network (on *Mobile WAN Configuration* page) if your SmartStart SL302 router has the 20.00.522 firmware version inside the Telit LE910-NA1 cellular module. The version of cellular module firmware can be found at *Mobile WAN Status* page in *Mobile Network Information* section.

SmartStart SL302 – SMS in Verizon Network

SmartStart SL302 router (equipped with the *Telit* modules *LE910-SV1* or *LE910-NA1*) supports sending and receiving of SMS in *Verizon* cellular network since the firmware version 6.1.4. Please note that to support SMS receiving, cellular module with Verizon firmware version higher than 20.00.012 is required.