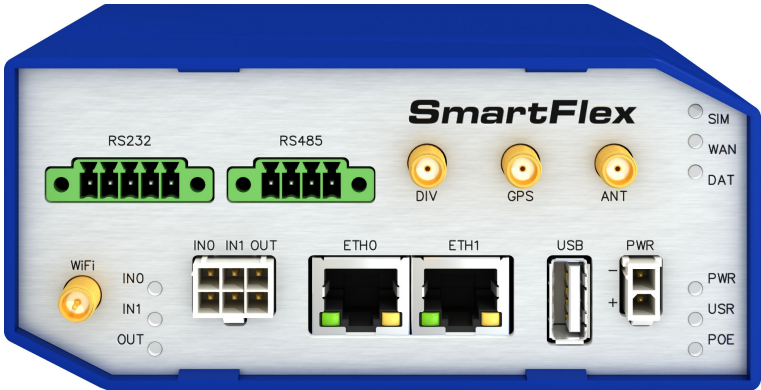
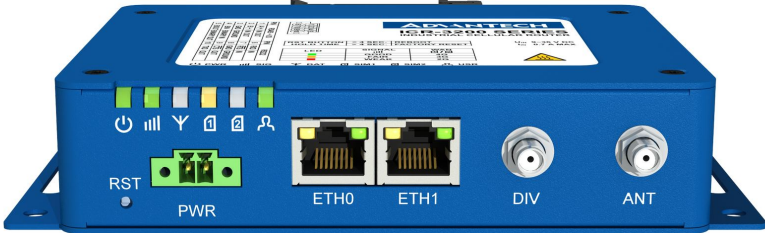




Firmware 6.2.5

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:** 6.2.5
- **Release date:** June 13, 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

Mobile WAN Status Page Enhancement

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 SL306
 SmartMotion ST352 SmartMotion ST355 ICR-320x ICR-321x ICR-323x ICR-324x ICR-383x

Mobile WAN status page now lists information of *PN offset* read out from the CDMA module. Each CDMA base-station sector is assigned an identifier called a *PN offset*, which is a timing offset based on the GPS even-second clock. Since each base station assigned to a particular frequency carrier operates at the same center frequency, the PN offset is used to distinguish base stations from one another.

Support for 802.1X Authenticator

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 SL306
 SmartMotion ST352 SmartMotion ST355 ICR-320x ICR-321x ICR-323x ICR-324x ICR-383x

Enabled wired driver in hostapd to enable an user module to implement 802.1X authenticator (server-side).

Changed Password Encryption

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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have changed the password encryption method from MD5 to a more secure SHA256 method. Please note that an existing password is stored with original encryption until it is updated.

Configuration File Parameters

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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

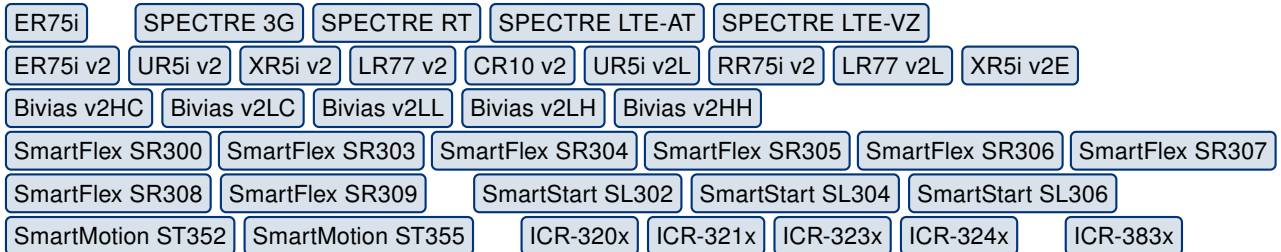
The maximum number of parameters in a configuration file was increased from 200 to 1000. This allows a user module to store even more parameters to the configuration file.

Firmware Update Improvement

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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

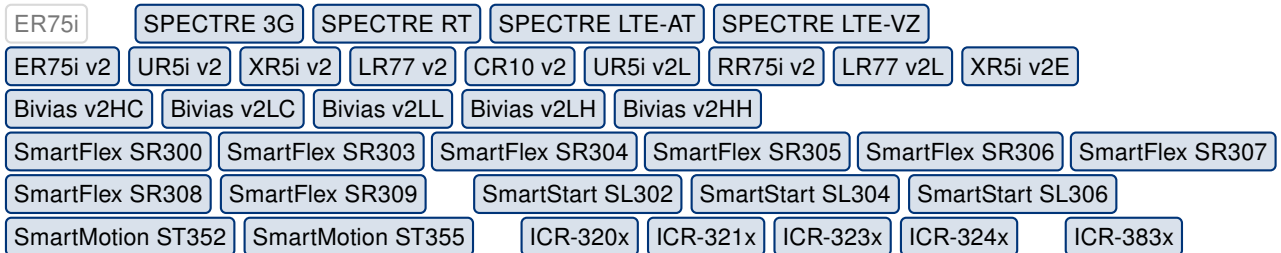
The process of firmware update was improved for devices with eMMC memory. One of the benefits is that the firmware update time was reduced significantly.

Disabled Password Auto-completion



We have disabled auto-completion of the password in a browser when adding or changing the user's password. In this case, the user can see all the previously used passwords in cleartext. This violates the password masking and could leak the password. This is considered a security issue e.g. by Nessus (<https://www.tenable.com/plugins/was/98081>), but also others like OWASP. The login-page is OK as the dedicated password-completion implemented in browsers does not display cleartext passwords. The problem is that this secure password auto-completion is not used for the add/change dialogs and cleartext is shown.

Hidden Sensitive Information



Some sensitive information were hidden the web interface. Below is the list of affected fields:

- WiFi -> Access Point -> RADIUS Auth Password,
- WiFi -> Access Point -> RADIUS Acct Password,
- WiFi -> Station -> RADIUS Password.

Fixed Kernel Crash

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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have fixed a Linux kernel crash triggered by unaligned memory access.

Fixed Linux Kernel Vulnerability

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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

This update has fixed [CVE-2019-19447](#) (medium) in the Linux kernel.

Updated StrongSwan 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 SL306				
SmartMotion ST352	SmartMotion ST355	ICR-320x	ICR-321x	ICR-323x	ICR-324x	ICR-383x		

We have updated the StrongSwan software to version 5.8.4.

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.