SMART/RG®
forward thinking

/SOFTWARE RELEASE NOTES

Release 2.5.0.9

Relevant Models:
SR350N
SR350NE
SR360n
SR500N
SR500NE
SR505n
SR510n
SR550n
SR552n

Release 2.5.0.9
October 1, 2015

SMART/RG®
forward thinking

TABLE OF CONTENTS

DOCUMENT HISTORY

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	12/30/14	Adam Fox	Document Creation
1.1	10/05/15	David La Cagnina	Updated Formatting

Notice of Document Integrity

The contents of this document are current as of the date of publication. SmartRG Inc. reserves the right to change the contents without prior notice. In no event will SmartRG be liable for any damages or for commercial losses resulting from information contained in this document.

SW REVISION SUMMARY

SW REVISION	DSP PHY/XDSL LINE DRIVER	CFE BOOTLOADER	WIRELESS DRIVER VERSION	DATE
2.5.0.9	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	10/1/15
2.5.0.8	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	6/26/15
2.5.0.7	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	5/19/15
2.5.0.6	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	12/30/14
2.5.0.5	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	10/10/14
2.5.0.4	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N) A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n/SR552n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	7/7/14
2.5.0.3	A2pG038i.d25d (SR360n) A2pD038f.d25d (SR350N) A2pv6C039b.d25d (SR500N)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	6/6/14

	A2pv6F039j.d25d (SR505n/SR510n) A2pvbF039j.d25d (SR550n)			
2.5.0.2	A2pG038i.d25 (SR360n) A2pD038f.d25 (SR350N) A2pv6C039b.d25 (SR500N) A2pv6F039b.d25 (SR505n/SR510n) A2pvbF038n.d25 (SR550n)	1.0.38-114.185	6.30.163.23.cpe4.12L08.1	4/18/14
2.5.0.1	A2pD038f.d24m (SR350N) A2pG038i.d24m (SR360n) A2pv6C039b.d24m (SR500N) A2pv6F039b.d24m (SR505n/SR510n) A2pvbF038n.d24m (SR550n)	1.0.38-114.70	6.30.102.7.cpe4.12L08.0	12/19/13
2.4.4.6	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N) A2pv6F037a.d24a (SR505n)	1.0.38-112.70	5.100.138.2001.cpe4.12L04.3	8/26/2013
2.4.4.5	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N) A2pv6F037a.d24a (SR505n)	1.0.38-112.70	5.100.138.2001.cpe4.12L04.3	6/5/2013
2.4.4.4	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	11/12/2012
2.4.4.3	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	10/11/2012
2.4.4.2	A2pD035j.d24a (SR350N) A2pv6C035j.d24a (SR500N)	1.0.37-106.24	5.100.138.2001.cpe4.12L04.3	7/30/2012
2.4.3.7	A2pD030n.d23c (SR350N) A2pv6C032a.d23c (SR500N)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	5/31/2012
2.4.3.6	A2pD030n.d23c (SR350N) A2pv6C032a.d23c (SR500N)	1.0.37-106.24	5.60.120.11.cpe4.06L.03.8	4/26/2012

CHANGES AND FIXES

REFERENCE NUMBER	DESCRIPTION
RB-1035	Addressed anomaly which allowed user to configure the loopback or multicast address on the secondary LAN interface.
RB-1069	Addressed anomaly that allowed entry of the local broadcast and network IP to be configured as the STUN server IP.
RB-1139	Addressed anomaly on the 360n where the Fault Management tab was not appearing.
RB-1330	Addressed anomaly which allowed for the duplicate entry of port forwards.
RB-1442	Addressed GUI stability anomaly when maximum number of Wireless clients are associated.
RV-1474	Addressed anomaly of a white line appearing on the left side of the GUI using certain browsers.
RB-1516	Addressed anomaly with the policy routing page crashing due to adding a route without input of a valid interface.
RB-1563	Addressed anomaly where the ACL would stop allowing the CPE's WAN IP to be entered.
RB-1571	Addressed anomaly where the Clear Statistics on the IPoE WAN interface was not functioning.
RB-1714	Addressed anomaly which allowed local access for certain protocols via the Guest SSID.
RB-1820	Addressed anomaly with DHCP option 18 causing spurious characters to be appended within file path.
RB-1822	Addressed anomaly where static routes entered via the CLI were being flushed after a reboot.
RB-1841	Addressed anomaly which URL filters erroneously accepted space character and prevented their removal.
RB-1842	Updated French language support for GUI.
RB-1856	Addressed anomaly were the wireless channel was not being pushed from the ACS properly.
RB-1866	Addressed inability to set MTU size >1500 bytes on the SR510n via CLI.
RB-1878	Addressed anomaly when DNS proxy is disabled and NAT disabled, LAN-side DHCP clients obtained DNS server info of CPE IP address instead of parameters obtained from the WAN side.
RB-1879	Addressed an anomaly when using base MAC address as WPA passphrase which caused the passphrase to be configured with all capital letters. Passphrase will display in lowercase as per previous software releases.
RB-1885	Addressed anomaly with 4G LTE WAN service.
RB-1886	Addressed anomaly with using multiple NTP servers.
RB-1892	Addressed GUI anomaly with the network status page displaying no Internet connection after receiving WAN IP.
RB-1897	Addressed an anomaly with the TFTP download feature where configuration files were erroneously stored in the running configuration location.
RB-1902	Addressed GUI stability anomaly when creating a 4in6 tunnel with name longer than 32 character limit.

RB-1904	Addressed anomaly where the CPE would not respond to group specific multicast queries from the WAN.
RB-1905	Updated the default configuration for G.inp as Enabled for all SmartRG gateways.
RB-1906	Addressed issue where under certain scenarios, such as power outage or DSL outage, the PPPoE session was not always in sync with the last known session ID.
RB-1924	Addressed some minor anomalies with user access control defaults and actions.

NEW FEATURES

REFERENCE NUMBER	DESCRIPTION
RB-1651	Changed default DSL latency to Path 0 and 1 being enabled by default.

IMPROVEMENTS

REFERENCE NUMBER	DESCRIPTION
RB-1254	Updated dropbear SSH to apply all latest security updates.
RB-1740	Changed default ACS URL to acs.smartrg.com.
RB-1863	Updated the interaction of how PPP sessions are handled when making changes from the ACS. Device no longer requires a full reset be performed. Requires update to ACS.
RB-1877	Addressed the operation of adding and deleting virtual servers and how they are returned to default based on configuration.
RB-1894	Addressed anomaly with supporting a virtual server using port 80, removing the requirement for reboot.

COMPATIBILITY/SYSTEM NOTES

The introduction of the Custom Default Settings feature requires the CFE to be upgraded when moving from any firmware version 2.4.4.2 or before. Firmware upgrades from any version below 2.4.4.3 to 2.4.4.3 or newer require the CFE to be upgraded by use of the firmware that includes a new CFE. Firmware files containing a CFE contain the string "cfe" in the filename. For example, the file, CA_PBCA_2.4.4.3_24742_SR350NN_cfe_fs_kernel, would be used to upgrade the firmware on a SR350NN gateway.

Failure to upgrade the CFE when moving from a firmware version before version 2.4.4.3 will result in unpredictable operation of the gateway and unknown factory default settings.

Downgrading from 2.4.4.3 and newer versions to pre 2.4.4.3 versions is not advised. If a downgrade must be accomplished, a factory default of the device via the reset button must be performed. The downgrade must be accomplished using the CFE image of the target firmware release. Factory default the device after the firmware has been downgraded by holding the reset button for at least 10 seconds after applying power to the device. Power must be off before pressing the reset button.

Downgrading from 2.5.0.7 and newer releases is not advised due to the increased configuration size. If a downgrade must be accomplished, a factory default of the device via the reset button must be performed. See the above paragraph for more information.

SR552n devices: In order to support expanded configuration files, it is recommended that the SR552n be upgraded to 2.5.0.5 or later. The cfe_fs_kernel image is required for the upgrade. Note that this will result in a factory reset only during the initial upgrade. All subsequent upgrades will retain the configuration.

IGMP Snooping Definitions:

Standard Mode - in standard mode, if multicast traffic is present on a LAN port but no membership report (join) was received, the traffic will flood to all ports. If a membership report was received, multicast traffic will be forwarded only to the LAN ports on which the IGMP membership reports arrived.

Blocking Mode - in blocking mode, multicast traffic will be blocked from all ports until such time as a report is received.

If IGMP snooping is disabled the CPE floods multicast packets to all its ports. IGMP Snooping is disabled by default.

This software supports Physical Layer Retransmission (PhyR) which operates at layer 1 and uses a mechanism similar to TCP where retransmits occur if errors are detected. This results in high effective INP with minimal interleave delay. Sync rate increases from 2 to 4Mbps have been reported in addition to the line being more robust and resistant to noise/interference generated from treadmills, ceiling fans, etc. PhyR is disabled by default but can be enabled in the DSL menu.

Wireless is enabled by default with SSID = SmartRGxxxx (x = last four characters of base MAC). Wireless security is Mixed WPA2/WPA-PSK, passphrase = OneCpeToRuleThemAll, Rekey interval = 0 and encryption = TKIP+AES.

Included PBCA Features:

- Control Panel
- Content Filtering
- Time Blocking
- Captive Portal
- Connect and Surf
- STUN and UDP Connection Request

- Advanced Connected Device Monitor
- Bandwidth Monitor
- WiFi Performance Monitor
- Dynamic Content Filtering

Prior FW Releases

Contact SmartRG support for the release notes for prior firmware releases.

FW UPGRADE PROCEDURE

Upgrade Firmware

1. Open a web browser, connect to 192.168.1.1/admin, and login with username **admin** and password **admin** (or customer specific IP address and login info)
2. Click Management →Update Software and click the Browse button.
3. Locate and select the appropriate firmware image.
4. Click the Update Software Button. The image will be uploaded to the device and the device will automatically reboot upon completion.

Verify

1. Press the F5 Key to refresh your browser and reconnect to 192.168.1.1/admin to log back into the device.
2. Click on Device Info.
3. Verify the version information in the *Software Version* field.

Restore Defaults

1. Click on the Management Link
2. Click on settings.
3. Click on Restore Default.

CUSTOM DEFAULTS

The Custom Defaults feature allows the importation of a set of defaults to the gateway that will be restored when the Restore Default Settings is activated. This set of defaults can be defined and updated via the GUI, CLI or CWMP support of the gateway.

To create a set of Custom Default settings, configure the gateway as required. Use the Backup Running Configuration button on the Backup Settings to upload a configuration file from the gateway. After the file is uploaded, choose the file and click the Update Working Settings button on the Update Settings window to download the file to the gateway. The gateway will use the downloaded settings as the custom default whenever the Restore Default operation is invoked.

TECH SUPPORT

CPE Issues

Submit a ticket using our Customer Portal at https://smartrg.atlassian.net.

RMAs

Open a Customer Portal ticket with Type "RMA" and attach a spreadsheet which includes Model, MAC address, Issue, and Firmware version.

Firmware

Login to the Customer Portal to download firmware.

Additional Contact Info

Phone: +1 360 859 1780, Option 4 Hours: 5am –5pm PST (UTC-0800) Email: support@smartrg.com