Service Release Notes for WiNG 5.9.2.4-004R

Please Note: *Service releases are made available to fix specific customer reported issues in a timely manner. Service releases are not as extensively tested as main releases (such as 5.9.2.0-032R). The next maintenance or manufacturing release will incorporate all qualifying and preceding service releases.*

This document is an addendum to the release notes for the main release 5.9.2.0-032R.

Contents

.....1
1. Resolved Issues 1
2. Important Notes 2
3. Platforms Supported 3
4. Firmware Upgrade/Downgrade Procedure 3

1. Resolved Issues

This release provides SMART-RF backwards compatibility between WiNG 5.9.2 and earlier versions.
The scenarios that are supported are the following:

- RF Domain manager running WiNG 5.9.2.4 or above with mix of 5.9.2.4 and 5.9.1.x APs with the Select Shutdown feature enabled
  - Expected behavior:
    - WiNG 5.9.2.4 APs will operate with select-shutdown feature enabled
    - WiNG 5.9.1.x APs will operate normal to WiNG 5.9.1 with no select-shutdown feature.

- RF Domain manager running WiNG 5.9.2.4 or above with mix of 5.9.2.4 and 5.9.1.x APs with the Select Shutdown feature disabled
  - Expected behavior:
    - All APs will operate normal to WiNG 5.9.1 with no select-shutdown feature.

Having device running WiNG 5.9.1 as an RF Domain manager with other Aps running WiNG 5.9.2.4 is not supported and the behavior is not defined.

Controller-managed rf-domains:
- all domains need to have smart-rf policy mapped if select-shutdown needs to be enabled/disabled properly.
- Select-shutdown feature needs to have the same value (either enable or disable) for all smart-rf policies used by the controller.

This service release 5.9.2.4-004R contains important fixes for reported issues.

Following is a list of SPRs/CRs fixed in this release:

SPR/CQ	Description
SPR-3478	AP 7632 performance issues with MC18 when client sends invalid HT element.
SPR-3482	AP 7532/AP 7522: CB is not sending VHT IE in the Association request
SPR-3496	AP 7632 loosing ge1 config on reboot in mixed version operation
SRP-3500	AP 7612 CB 4-way handshake timeout
SPR-3501	GUI doesn't have client bridge configuration for AP 7632/7662
SPR-3503	Nsightd error alive_dev.py:153:run : Exception (<class 'pymongo.errors.DocumentTooLarge'>, DocumentTooLarge('BSON document too large
SPR-3507	APs unadopts when IPSec tunnel renegotiates keys. Added new CLI option (ikev2 peer reauth) under "crypto remote-vpn-client" to control the reauthentication behavior upon IKE rekey. If 'ikev2 peer reauthentication is disabled, then IPSec SA's will not be re-created upon IKE rekey.
SPR-3508	AP 7632/7662 – only allow boot prompt access when Esc is pressed
SPR-3511	APs not synchronizing time with mapped NTP server on controller
SPR-3517	AP 7632 panic on MCX deployment connecting to AP 8432
SPR-3522	NX7500 frequent SSM crashes seen controller managed RFDM AP count is more than 1024
WING-37291	Indonesia regulatory updates – conducted operating power reduced to 100 mW indoor
WING-37330	Client Bridge: When client bride has Trust point with only CA certificate, PEAP authentication is allowed without server validation
WING-37334	Smart RF: radio turn off after adding/removing WLAN on a hidden radio
WING-37338	Smart RF: modifying sensitivity profile cause select-shutdown to disable the radio
WING-37387	AP 7662 VMM mesh disconnects after idling for a while
WING-37410	Some Aeroscout functionality (i.e temperature reading) not working on AP 75xx series of Aps.
WING-37427	AP 7xxx sends wrong WMM element in the association request causing DHCP failures with some 3rd party Aps.

2. Important Notes

- Mixed version deployment:
  - When NX controllers has firmware version 5.9.1.x version, configuration push to AP running WiNG 5.9.2.x might throw the following/similar error message.

    *USER-3-ERR: main.pyo: Feb 23 18:50:57 2018: %USER-3-ERR: main.pyo: * * ERROR: 4 - commit unknown exception - object of type 'Lacp_Cfg' has no len() Feb 23 18:50:57 2018: %USER-3-ERR: main.pyo: * * ERROR: update own config failed*

    To address this issue – CfgdLacpUpdate.patch needs to be installed on controllers running WING 5.9.1.x versions. Patch can be obtained thru Extreme Support.

  - Roaming – credential cache update message is not compatible between WiNG 5.9.2 and earlier versions. To mitigate that – new command is added at rf-domain level, which is disabled by default.

When enabled it will only send the old cred cache message to the neighbor devices. New command can only be configured if controller running WiNG 5.9.2.4 version or above.

ap7532-1A1B18(config-rf-domain-default)#service cred-cache ?
legacy-compatible Force use legacy credential cache format when mixed versions are deployed

- AP 7632 BLE: The current default power is set such that user can detect BLE beacons at distance up to 30'. The user may have to reduce the TX power for their use-case, e.g. micro-locationing. Note that the TX power setting is not the power in dBm, but only an index that follows a logarithmic relation to the output power in dBm.

- Due to upgrade of radius module in WiNG 5.9.2 – if you have Onboard-Radius Server with LDAP Authentication, please note the following:
  Configurations using "(sAMAccountName=%{Stripped-User-Name})" need to be updated to "(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" prior to performing the upgrade process.

  For WiNG 5.7.1 till WiNG 5.9.1 when running Onboard-Radius Server with LDAP Authentication configured, following was required:
  Configurations using "(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" need to be updated to "(sAMAccountName=%{Stripped-User-Name})" prior to performing the upgrade process.

- Chrome v67 and above, automatically redirects traffic sent to 1.1.1.1 to Cloudflare, which is a new service offering DNS over HTTPS.

  Many captive portal vendors, including WiNG, use 1.1.1.1 as an internal redirection IP/hostname for guest network splash pages. It's best practices to update Captive Portal Server hostname to make sure that process is working correctly.

3. Platforms Supported

This release applies to all platforms released with WiNG 5.9.2.0-032R.

Reminder:
Dependent AP platforms: AP 621, 622, 650 are EOL and engineering support has ended.

Independent AP platforms: AP 6511, AP 6511E, AP 6521, AP 6532, AP 7131, AP 7181, AP 8122, AP 8132, AP 8222, AP 8232, ES 6510 are EOL and engineering support has ended.
Controller platforms: RFS 4011, RFS 6000, RFS 7000, NX 9000, NX 45XX and NX 65XX platforms are EOL and engineering has ended.

4. Firmware Upgrade/Downgrade Procedure

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

For detailed upgrade procedure – please refer to WiNG 5.9.2 release notes.

Upgrade from WiNG v5.x.x.x to WiNG v5.9.2.x

1. Copy the controller image to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**‖, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the controller. From CLI the command is —reload.