

Service Release Notes for WiNG 5.9.2.5-001R

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 1

3. Platforms Supported 2

4. Firmware Upgrade/Downgrade Procedure 2

1. Resolved Issues

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

| SPR/CQ | Description |
|------------|--|
| WING-37572 | WiNG APs show high CPU usage by cfgd when connected to Extreme Cloud appliance |

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**.

© Extreme Networks. 2018. All rights reserved.