6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

WiNG 5.9.7.0-011R Release Notes

CONTENTS

OVERVIEW

WiNG 5.9.7 is a maintenance release that continues to build on the innovative WiNG 5 architecture across 802.11n and 802.11ac Enterprise WLAN portfolio.

In addition, WiNG 5.9.7 release includes several new feature enhancements and critical customer fixes.

1. PLATFORMS SUPPORTED

The following AP hardware platforms – AP 621, AP 622, AP 650, AP 6511, AP 6511E, AP 6521, AP 6532, AP 6522, AP 6562, AP 7131, AP 7161, AP 7181, AP 8122, AP 8132, AP 8222, AP 8232, ES 6510 are EOL and engineering software support has ended. No new images will be released or supported for those platforms.

The following Controller hardware platforms - RFS 4011, RFS 6000, RFS 7000, NX 9000, NX 45XX and NX 65XX platforms are EOL and engineering software support has ended. No new images will be released or supported for those platforms.

WiNG 5.9.7 release firmware keeps the CLI references for these EOL platforms to support backward compatibility on downgrade of the network to prior WiNG releases.
Important: Image name change:
NX 9500 image is now called NX9500-<version>.img and not NX9000-<version>.img as in previous releases.
Note:

APXXXX-LEAN-5.9.7.0-011R.img - built **without GUI component**. AP lean images are also bundled within controller full image.
NXXXXX-LEAN-5.9.7.0-011R.img – built **without AP images.**

WiNG 5.9.7 supports the following platforms with the corresponding firmware images:

Controller Platform	Firmware Image
RFS 4010	RFS4000-5.9.7.0-011R.img, RFS4000-LEAN-5.9.7.0-011R.img
NX 9500/ NX 9510	NX9500-5.9.7.0-011R.img, NX9500-LEAN-5.9.7.0-011R.img
NX 9600 / NX 9610	NX9600-5.9.7.0-011R.img, NX9600-LEAN-5.9.7.0-011R.img
NX 75XX	NX7500-5.9.7.0-011R.img, NX7500-LEAN-5.9.7.0-011R.img
NX 5500	NX5500-5.9.7.0-011R.img, NX5500-LEAN-5.9.7.0-011R.img

Virtual Platform	Firmware Image
VX 9000[1]–production iso/img image	VX9000-INSTALL-5.9.7.0-011R.iso, VX9000-5.9.7.0-011R.img, VX9000-LEAN-5.9.7.0-011R.img
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-5.9.7.0-011R.iso[2]

[1]*VX 9000 image has default 64 AP license starting WiNG 5.8.3.*

[2]*The VX demo image is a 60-day trial image of the VX 9000 software VM that can be used for demos and in the lab environments. This image does not need any additional licenses; it comes with 16 AAP licenses built-in. There is no migration from the demo image to the production image.*

AP Platforms	Firmware Image
AP 7532	AP7532-5.9.7.0-011R.img AP7532-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7522/AP 7522E	AP7522-5.9.7.0-011R.img AP7522-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7562	AP7562-5.9.7.0-011R.img AP7562-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7502 / AP 7502E	AP7502-5.9.7.0-011R.img AP7502-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 8163	AP8163-5.9.7.0-011R.img AP8163-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 8533	AP8533-5.9.7.0-011R.img AP8533-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 8432	AP8432-5.9.7.0-011R.img AP8432-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7602	AP7602-5.9.7.0-011R.img AP7602-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7622	AP7622-5.9.7.0-011R.img AP7622-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7612	AP7612-5.9.7.0-011R.img AP7612-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7632	AP7632-5.9.7.0-011R.img AP7632-LEAN-5.9.7.0-011R.img (included in all NX controller images)
AP 7662	AP7662-5.9.7.0-011R.img AP7662-LEAN-5.9.7.0-011R.img (included in all NX controller images)

2. NEW FEATURES IN WING 5.9.7

Additional Enhancements

- **AP lookup through NSight API** – This enhancement adds backend support for AP lookup via AP name/IP/MAC/BT-BLE MAC. API is available in NSight release 5.9.3.1.

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

- **Smart-RF enhancement to blacklist channel on an AP** – Adds capability to block/blacklist certain channels from getting included in smart-rf analysis for various reasons, e.g. continuous beacon stuck etc.
- **Smart-RF enhancement to configure power per area –** Implements capability to provide output power range for a configured area.

```
smart-rf-policy test
      group-by area
      sensitivity custom
      assignable-power 5GHz max 2
      assignable-power 5GHz min 1
      assignable-power 2.4GHz max 2
      assignable-power 2.4GHz min 1
      channel-width 5GHz 80MHz
      area 1 assignable-power 5GHz min 3
      area 1 assignable-power 5GHz max 4
      area 1 assignable-power 2.4GHz min 3
      area 1 assignable-power 2.4GHz max 4
```

- **Read only user role for WING API access –** Adds a new read-only user for accessing WING APIs.
- **Device discovery through WNMP –** Adds support for discovery and reset of mis-configured APs via WNMP. AP MAC address and serial number is required in host tool to use this feature for security reasons.
- **Macau power tables --** Macau power tables are added for AP7522/7532/7562/7612/7632/7662/8432/8533

3. GENERAL INFORMATION FOR FIRMWARE UPGRADE / DOWNGRADE

3.1 Device Upgrade/Downgrade matrix

This section documents allowed upgrade/ downgrade combinations. Please ensure that the controller and AP are on the same WiNG version after the upgrade is complete in the controller deployment.

Note: All Motorola branded software (below v5.7.0.0 with exception of v5.5.6.0) is not available for download through Support Portal at this point.

Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
AP 7502	v5.5.4.1 onwards, excluding v5.6.x	v5.5.4.1 onwards, excluding v5.6.x	AP image is contained within the NX controller image
AP 7532/AP 7522	v5.5.3.1 onwards, excluding v5.6.x	v5.5.3.1 onwards, excluding v5.6.x	AP image is contained within the NX controller image
AP 7562	v5.7.1 onwards	v5.7.1 onwards	AP image is contained within the NX controller image

Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
AP 7602/7622	v5.8.4.20, v5.8.4.21, 5.9.1	v5.8.4.20/5.8.4.21	v5.8.4.20/5.8.4.21 was limited release. AP image is contained within the NX controller image
AP 7612/7632/7662	v5.9.1	v5.9.1	AP image is contained within the NX controller image.
AP 8163	v5.6 onwards	v5.6 onwards	AP 8163 images are not within the controller image
AP 8533/ AP 8432	v5.8.4 onwards	v5.8.4 onwards	AP image is contained within the NX controller image.
RFS 4000	v5.0 onwards	V5.0 onwards	
NX 5500	v5.8 onwards	v5.8 onwards	NX 5500 is supported starting with v5.8
NX 75XX	v5.5.2 onwards	v5.5.2 onwards	Note: WiNG 5.6 doesn't support NX 7500.
NX 9500	v5.2.1 onwards	v5.2.1 onwards	
NX 9510	v5.4.1 onwards	v5.4.1 onwards	
NX 96XX	v5.5.6 onwards	v5.5.6 onwards	NX 96XX is not supported with v5.6.x and v5.7.x
VX + all supported APs	v5.6 onwards	v5.6 onwards	

3.2 Device Upgrade/Downgrade Procedure

IMPORTANT:

- Always create config back-up before the upgrade.
- Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. Where APs are powered through PoE connections to WLAN controllers, the controller needs to stay up during the upgrade process.
- Both the controller and the AP should be upgraded to the same versions – a firmware mismatch can cause network disruptions and should be avoided. When upgrading, the controllers should be upgraded first and then the APs. When downgrading, the APs should be downgraded first, and then the controller.

1. Copy firmware image for device that needs to be upgraded to you ftp/tftp server. Refer to section 2 for correct firmware image for your device.

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.

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

3. Restart the device. From CLI the command is —reload.

3.3 AutoInstall

AutoInstall in WiNG 5 works via the DHCP server. This requires the definition of Vendor Class and three sub-options that can be either sent separately or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to enter as a string: —ftp://admin:admin123@192.168.1.10‖)

Option 187 - defines the firmware path and file name

Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable “ip dhcp client request options all” on the VLAN interface which is being used to perform the above autoinstall.

DHCP vendor class for platforms is noted below:

Appliances:

- WingRFS.RFS4010
- WingNX.NX5500
- WingNX.NX7500
- WingNX.NX9500
- WingNX.NX9600
- WingVX.VX9000

AP:

- WingAP.AP8163
- WingAP.AP7502
- WingAP.AP7602
- WingAP.AP7522
- WingAP.AP7532
- WingAP.AP7562
- WingAP.AP7612
- WingAP.AP7632
- WingAP.AP7662
- WngAP.AP7622
- WingAP.AP8533
- WingAP.AP8432

4. FIRMWARE UPGRADE / DOWNGRADE – CONTROLLERS

4.1 Platform Important notes

1. VX 9000:
   a. Secondary storage: VX 9000 has disk size limitation on the default disk of 2TB. However, when a secondary virtual disk is used, VX 9000 can support disks size larger than 2TB
      - Enabling secondary storage does not copy data files to the new location
      - It is recommended immediately after provisioning the guest instance, before enabling NSight or Captive-Portal
      - If the secondary storage needs to be enabled after NSight/Captive-portal, it is recommended to back up the database, and restore the database after secondary storage is enabled.
      - If the VX 9000 instance is not a primary (replica-set member), the database server will perform full data sync after it is restarted with the new secondary storage disk.
   b. VX 9000 requires re-install using the VX9000-INSTALL-5.8.2.0-030R.ISO image if the user intends to configure NSight / Captive portal functionality. This is due to the changes to the flash partition (25% of the allocated disk size – 4GBMin, 128GB Max) to take effect:
      - Export configuration before reinstalling the VX.
      - To preserve the same MAC address (and therefore the serial number for licensing)
        - Delete current hard disk from the VM

- Add new virtual hard disk
- Connect ISO file as virtual CD
- Boot into CD to start installation process

After installation is complete, restore the configuration.

2. NX 9600:
   a. WiNG 5.8.6 introduced support for new RAID controller for NX 9600 platform. For platforms shipping with new RAID – downgrade below v5.8.6 will be disallowed.
   b. WiNG 5.8.1 changed default RAID configuration for NX 9600 from RAID 5 to RAID 10 to improve performance. Note: RAID configuration cannot be changed upon upgrade or downgrade.
      NX 9600 controllers manufactured with v5.8.1 or above will have RAID 10 configured. NX 9600 controllers manufactured with v5.5.6 will have RAID 5 configured. RAID configuration can only be changed by authorized personnel.
3. RFS 4000:
   a. When downgrading an RFS 4000 from WiNG 5.8 to WiNG 5.7, the user first needs to downgrade the RFS 4000 to WiNG 5.7.2 before moving to WiNG 5.7.
4. When upgrading from prior versions – new profiles for newly supported platforms will not be present in the startup-config. The user can either create a default profile or do “erase startup-config”.

4.2 Device Upgrade Options

WiNG 5.x supports device firmware upgrade from the controller. For firmware upgrade through the controller, firmware image needs to be loaded onto a controller and the same can be used for the upgrade of all the corresponding devices.
Available firmware on the controller can be checked using the below command:
nx9600#show device-upgrade versions

If device firmware is not part of controller image, a new image can be uploaded using the following command:
nx9600#device-upgrade load-image

Once device firmware is loaded on the controller, below are the different options that are available for device firmware upgrade:

- **Manual Upgrade**

Firmware upgrade can be initiated on a single or a list of Aps using the below command.

```
nx9600#device-upgrade ap7532 ?
  no-reboot      No reboot (manually reboot after the upgrade)
  reboot-time    Schedule a reboot time
  upgrade-time   Schedule an upgrade time

nx9600#device-upgrade ap7532 all ?
  force              Force upgrade on all devices
  no-reboot          No reboot (manually reboot after the upgrade)
  reboot-time        Schedule a reboot time
  staggered-reboot   Reboot one at a time without network being hit
  upgrade-time       Schedule an upgrade time
```

- **Scheduling Firmware upgrade**

Firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. Firmware upgrade on the Aps follows the configured upgrade time.

nx9600# device-upgrade all ?
no-reboot No reboot (manually reboot after the upgrade)
reboot-time Schedule a reboot time
staggered-reboot Reboot one at a time without network being hit
upgrade-time Schedule an upgrade time

- **Upgrade through RF Domain manager**

Manual Firmware upgrade can be initiated through a domain manager
nx9600#device-upgrade rf-domain ?
DOMAIN-NAME RF-Domain name
all Upgrade all RF Domains
containing Specify domains that contain a sub-string in the domain name
filter Specify additional selection filter

4.3 Auto Upgrade

Auto firmware upgrade can be enabled on the controller using the below command. When enabled, any AP with a firmware version different than the controller will be upgraded to the controller's version on adoption.
nx9600 (config-device-XXX)# device-upgrade auto
The number of concurrent firmware upgrades can be configured using the below command based on the bandwidth available between the controller and the Aps.
nx9600(config-device-XXX)# device-upgrade count ?
<1-20> Number of concurrent AP upgrades

Note: Auto upgrade on the APs always happens through the controller.

5. FIRMWARE UPGRADE/DOWNGRADE – INDEPENDENT APS

5.1 Platform Important Notes on Upgrade / Downgrade

1. AP 8533/AP 8432:
    a. AP 8533/8432 manufactured with v5.8.4 or above cannot be downgraded to v5.8.3.
    b. When upgrading AP 8533 running v5.8.3.x to v5.8.6, please upgrade to v5.8.4 first and then to v5.8.6.
2. AP 7532/AP 7522/AP 7562:
    a. AP 7522, AP 7532, and AP 7562 manufactured after July 2017 use new NAND chipset. Downgrading to a release prior to WiNG 5.8.0 will render these units irrecoverable. Please refer field flash “FN-417 – AP 7522, AP 7532, AP 7562 Component Change” for the affected hardware revision and software downgrade version restrictions.
    b. When downgrading from WiNG 5.8 to WiNG 5.5.5 or WiNG 5.5.4 on AP 7532/7522, the user needs to apply kernel patch **AP75XX-CPU-Bringup-1.0.patch**.
    AP7532/AP7522 running WiNG 5.5.6/5.7.x has an updated kernel version and the patch is required when the AP downgrades to a firmware with a prior kernel version.
    Steps to apply the patch:
        - Copy AP75XX-CPU-Bringup-1.0.patch to your tftp server.
        - Apply the patch using upgrade command:
            - “upgrade tftp://<server ip address >/AP75XX-CPU-Bringup-1.0.patch”
        - Use “boot system primary” or “boot system secondary" based on the WiNG 5.5.5/5.5.4 image location on the AP and reload.
3. AP 8XXX:

a. WiNG 5.8.1 added support for new NAND chipset for AP 8122, AP 8132, AP 8163, AP 8222 and AP 8232. APs manufactured with new NAND cannot be downgraded to the prior version.
b. WiNG 5.5.2 added support for new NAND for AP 8XXX platforms. Downgrade to prior releases on hardware with new NAND will be prevented.

4. AP 7161:
   a. WiNG 5.1.4 added support for the new NAND for AP 7161. Hardware revs with the new NAND will be unable to downgrade below these versions or version 4.1.5 – as this supports the new NAND, but previous versions do not.
   b.

6. IMPORTANT NOTES

New in v5.9.7

1. Discovery and configuration reset via WNMP for recently online and discovered APs.
2. Blacklisting of channels for smart-rf blocked due to various conditions.
3. Captive portal now includes message for blocking user access.
4. Smart-rf per area output power range for included channels can be set.
5. Read-only user for WING APIs.

New in v5.9.6

1. Aeroscout locationing is fully supported on AP 8163.
2. IP TTL for DHCP and DHCP relay was updated to 64.
3. New cli command for MCX configuration to allow rescan to happen at a specific time:
   acs rescan-time:
   rfs4000-22A1B8(config-profile-Root-meshpoint-MCX)#acs rescan-time
   2.4GHz 5GHz
   rfs4000-22A1B8(config-profile-Root-meshpoint-MCX)#acs rescan-time 5GHz ?
   HH:MM:SS Time of day in HH:MM:SS

New in v5.9.5

1. For credential cache update to work in mixed environment, "service cred-cache legacy-compatible" command is required under rf-domain to work with pre-5.9.5 releases. WiNG 5.9.2.x releases will not work with WiNG 5.9.5 in the mixed environment.

New in v5.9.4

1. **NSight has been disabled on WiNG controllers in this release.**
2. WiNG 5.9.5 includes the fixes from WiNG 5.9.3.1 and WiNG 5.9.3.2 releases.
3. BLE feed to 3rd party server and ExremeLocation simultaneously is not supported – applicable to all releases that support both features.
4. A CLI command was added under “Radio Mode”
   #beacon meshpoint-threshold <-128 - -40>

   Default value is -128 dBm. The mesh will ignore the incoming beacons whose RSSIs are below the value defined by this command
5. The description of 'beacon txpower' for bluetooth interface is as mentioned below:
   <-15-31> BLE beacon transmit power index
   <-15 to 6> for AP7612, AP7622, AP7602, AP8432, AP8533,
   <1 to 31> for AP7632, AP7662

If any device is configured through 'anyap' profile, and if the
beacon txpower for the bluetooth interface is out of it's valid range, the default value is set during commit. So please make sure to set correct value for txpower, including multiple anyap profiles if needed.
AP7632/AP7662 has default txpower value of 10
And others have a default txpower value of 0.

New in v5.9.3

1. Application Visibility DPI engine on the supported APs upgraded to a newer version 18.07.06. As a result – some application names have been deprecated and new application signatures were added.
2. 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. 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.
4. AP 7632 BLE radio doesn't support "mode bt-sensor" – mode needs to be changed to "mode le-beacon".
5. 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
6. 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.

7. smart-rf coverage-hole-recovery and rx-sensitivity-threshold cannot enable at the same time, otherwise coverage-hole-recovery will not work correctly.

8. **Remote-debug using sftp mode:**
    - The remote-debug copy-techsupport will not be able to run on "self" host. If the "self" device is included in the rf-domain when running reug copy-techsupport, then self-host will be excluded if sftp is used to copy.
    - When capturing large data with remote-debug in sftp mode, the device may run out of space and will not be able to copy all the data. If this is noticed, please use area, floor, count filters to minimize the number of devices and the size

9. **Fabric Attach**
   When FA is used in Untagged Management mode, User must configure TRUNK port and configure VLAN 1 as the NATIVE VLAN.
   Edge switch port might belong to VLAN-X, and while configuring FA mapping User should configure like below, "Y" is the WLAN vlan and "Z" is the corresponding ISID

```
interface ge1
switchport mode trunk
switchport trunk allowed vlan 1, Y
switchport trunk native vlan 1
swithcport trunk fabric-attach vlan Y isid Z
```

10. **New CLI commands added:**
    - Location server status
      show wireless location-server ?
      on On AP/Controller
      | Output modifiers
      > Output redirection
      >> Output redirection appending
      <cr>

    - Trustpoint point CB changes:
      Changed the CLI 'show wireless bridge certificate status' to 'show wireless bridge client-certificate status'
      Added New CLI 'show wireless bridge ca-certificate status' to check the ca trustpoint status.

- BSSID added to "show wireless radio detail"

- New CLI option under “crypto remote-vpn-client” to control the reauthentication behavior upon IKE rekey.
  crypto remote-vpn-client
  [no] ikev2 peer reauth
  If 'ikev2 peer reauth' is disabled, then IPSec SA's will not be re-created upon IKE rekey.

- New CLI for server configuration in imagotag policy
  (config-iot-device-type-imagotag-policy-test)#server ?
  hostname Server hostname. It can be FQDN, partial DN or any.
  ip-address Server IP address

- New AP 8432 CLI configuration option to control the USB port power state. The new option ‘usb-enable’ is available under the ‘power-config’ command. The default value is “enable”.
  (config-device-12-34-56-12-34-56)#power-config usb-enable
  (config-device-12-34-56-12-34-56)#no power-config usb-enable

New in v5.9.2

1. **New CLI Commands added**
   - New command: “**show snmpv3 engineID**” to allow reading snmp engineID of the device.
   - In reload command added option “all” to reload devices in all rf-domains:
     Reload [|staggered] on <rf-domain-name|**all**> [|containing <substring> |filter <device-type> | exclude-controllers| exclude-rf-domain-manager]
   - Added new functionality to switch boot partition on devices from controller. It is available over rf-domain.
     boot system (active | inactive) [on (device <mac|hostname> | rf-domain <name>)]
     The option active will check if the current boot is primary or secondary and will change next boot to the current boot. Inactive will do the exact opposite.
   - Add CLI command and update device config schema to configure the hello-interval and adjacency-hold-time of cluster MiNT links:
     cluster hello-interval <1-120> adjacency-hold-time <2-600>
   - Command “**802.11v bss-transition**” under WLAN context is not hidden anymore.
   - CLI command to force preemption of L2TPV2 tunnel back to primary:
     “<no> preempt (|delay <60-600>)”

2. **ExtremeGuest:**
   - VX9000 based ExtremeGuest application is not supported with WiNG 5.9.2.
   - Use UpgradeVX9000ToEGuest.patch to migrate the VX9000 based ExtremeGuest application to ExtremeGuest 5.9.2 release.
   - License Management for ExtremeGuest is only available at User Interface, CLI based license management is not supported.
   - ExtremeGuest user interface is accessible through http(s)://hostname.domainname.com/
   - Set WLAN registration type as “user” when setting up onboarding policy for the network to deliver One-Time-Passcode/Passcode on sponsor approval.
   - Enable Message Parts at Clickatell SMS integration when customized SMS text message exceeds 160 characters length.
   - Device fingerprinting report may not provide accurate Device, Browser and OS types when using Frictionless Onboarding for a network.

- Following ExtremeGuest functionalities are not supported for Captive-Portal Gateway Deployment
  - Frictionless Onboarding
  - Loyalty Application detection
  - Disconnect from network
  - Welcome Back Message

3. **ADSP incompatibility:**

   Due to 3rd party module upgrade in WiNG 5.9.2 (openSSL, openSSH and others) – there is incompatibility between WING 5.9.2 and ADSP 9.5. Following ADSP features are impacted:
   - Manual Data poll. Auto data poll/collection also fails, but ADSP gets required data for sanctioning BSS and clients by then.
   - Readiness Test
   - Command run and log
   - Firmware upgrade downgrade from ADSP for AP and sensor.
   - Configuration Compliance check(Audit) and enable auto-correction
   - Configuration push

   ADSP 10.0 release should address this incompatibility.

4. **Fabric Attach**

   When the WiNG devices connected to an FA enabled edge switch, the device would auto-learn interface configuration from the edge switch. That means, the WiNG device would auto-configure the VLAN on that interface supplied from the edge switch. The edge switch may mark/unmark the VLAN for tagging and this would reflect in the interface configuration of the WiNG device.

   The auto-configure would be local to the AP/Controller and would not be supposed to persist the reboot. It is recommended to have “no auto-learn staging-config” configured on adoption controller. Controller should have the AP’s interface configuration pre-configure at Profile level; otherwise controller would override the AP’s configuration and AP may lost connectivity to controller.

   Default LLDP TX timer is 60 seconds. i.e LLDP sends out packet on every 60 seconds and this applies to FA messages as well. Whereas VSP/ERS switches’ default Element TLV timeout is 40 seconds. So, this might cause the FA switch to complain about Element TLV timeout. One may configure AP/Controller’s LLDP timer less than 40s to overcome this issue – under profile/device “lldp timer <5-900>”.

5. **Imagotag support**
   - AP’s IP address and AP-ID needs to be configured in ESL server for communication between ESL communicator (USB dongle) and ESL server.
   - AP-ID can be determined by “show iot-device-type-imagotag status” command.
   - If after configuration of AP’s IP and AP-ID in ESL server, AP’s IP is changed (statically or via DHCP), the AP needs to be reconfigured again as per #1.
   - AP-ID is saved in a file on AP after imago policy configuration so that same AP-ID is used by after reboots, however if a DD install is done on AP, this file will be erased and AP needs to be configured again with new AP-ID as per #1.
   - USB dongle has a color led which has following connotations –
     a. Red – no userspace process (thinAP2) is controlling dongle; probable causes may be,
        i. No policy configured
        ii. IP address and/or AP-ID of AP is changed
     b. Ember – communication between ESL server and userspace process (thinAP2) is getting established.

c. Blue – communication between ESL server and userspace process (thinAP2) is established.

6. Following features are now supported on AP 7612/7632/7662 in this release:
   a. RSSI locationing
   b. L3 Mobility
   c. PPOE, VRRP, OSPF, MSTP
   d. 802.1x authentication on ge port

7. Following features are now supported on AP 76027622 in this release:
   a. RSSI locationing
   b. 802.1x authentication on ge port.
   c. Radius VSA
   d. Role based firewall.

New in v5.9.1

1. Heterogenous AP:
   a) When using Heterogenous AP management 'anyap' profiles must be used to configure Access Points which are not the same model as the Virtual Controller. These profiles must exist on the Virtual Controller prior to the Virtual Controller adopting and managing other Access Point models. Adoption and management of other Access Point models will succeed without any defined auto provisioning rules if the 'anyap' profiles are named "default-<AP_MODEL>". For example, an AP 8533 Virtual Controller will successfully adopt and manage an AP 7602 Access Point without an AP 7602 auto provisioning rule if the AP 8533 has an 'anyap' profile named "default-ap7602". Otherwise you will need to create suitable auto provisioning rules for the other Access Point models if you choose to use a different naming convention for your 'anyap' profiles.
   b) When using Heterogenous AP management be aware that APs operating as Virtual Controllers have much less persistent storage than actual WiNG controllers. Because of this it may not be possible for you to update all APs simultaneously when using multiple AP models. The Virtual Controller may not have enough free persistent storage to hold the firmware update images for multiple AP models. The amount of free persistent storage is unique to every Virtual Controller installation. If your Virtual Controller does not have enough free storage for multiple firmware update files you will need to download a single appropriate firmware update file to the Virtual Controller, update the AP models that correspond to that firmware update file, delete that firmware update file from the Virtual Controller, then repeat the download/update/delete process for the next AP model.
   c) Only VC AP will have image upload capabilities for upgrade in this release.
2. Added "show adoption status all" command to display adoption on all connected sites.
3. Added the service command "service snmpv3 reset engineID" which will generate the new engineID and reboot the device.
4. WiNG 5.9.1 incudes DPI performance improvements.
5. NSight/ExtremeGuest: Added "service show database collections statistics" – to show size of the collection, number of documents.
6. ExtremeGuest: Added "service eguest remove-data deleted-devices|offline-for" to delete the devices reported at ExtremeGuest that are offline/removed from the network.
7. Database Replica Sets - Be aware when using FQDN hostnames for the members of the replica-sets, if a replica set member goes down, DNS queries from the remaining replica set

members and database clients can be high for a short period as it tries to resolve (and contact) the missing replica-set member.

8. Configuration command under interface context - "dot1x_auth_max_reauth_req <1-10>" is changed to "dot1x authenticator max-reauth-count <1-10>".
9. TCP_RTT metadata collection and reporting is not accurate if enabled.
10. AP 7612/7632/7662 – off channel scans runs only every 30 seconds.
11. NSight: Recurrence reports are not generated as per the schedule once Daylight Savings Time kicks in.
12. Following features are not supported for AP 7612/7632/7662 in this release:
    a. BLE on AP 7632
    b. Cisco phones
    c. Sensor functionality
    d. MCX and mesh related features
    e. Client bridge
    f. MU-MIMO, Transmit beamforming
    g. L3 mobility
    h. 3rd party locationing
    i. PPOE
    j. Keyguard
    k. GRE, VRRP, OSPF
    l. WeChat
    m. NSight – sensor functionality
13. Following features are not supported for AP 7602/7622
    a. MCX beyond 1 hop mesh
    b. WIPS functionality beyond what's supported in WiNG 5.8.4.20/5.8.4.21

New in v5.9.0

1. ExtremeGuest: -
    a. ExtremeGuest Deployment– please refer to "ExtremeGuest Deployment guide" posted on Support site under product manuals.
    b. ExtremeGuest is supported on VX 9000 instance.
    Note: NX 9600 platform can be used as ExtremeGuest for demo only (non-production).
    c. Preloaded for 100 client devices/60days without licensing
    d. Recommended browser when using ExtremeGuest in v5.9.0 are:
        - Chrome – ver 56.0.2924.87 (64-bit) or later.
        - Firefox 53.0.3
    e. Refer to ExtremeGuest datasheet for the VX resource requirements to deploy ExtremeGuest solution at various scale.
    f. ExtremeGuest and NSight services are not supported on the same VX instance.
    g. Splash Template Management – Make sure to add the below command to controller's/VC's before attempting to push the advanced templates from ExtremeGuest to WiNG Controller/Virtual Controller.

    (config)#rf-domain

    (config-rf-domain-{ALL})#override-wlan <WLAN-NAME> template test

    **test – template name has no significance, just a dummy template name.*
    h. When configuring a database-policy replica-set using FQDN, enable ip dns-server-forwarding on all ExtremeGuest devices participating in the replica set.
    i. Configure 'geo-coordinates <latitude> <longitude>' in RF domain context to specify site locations for ExtremeGuest Google map view

   j. Configure 'location' in RF domain context to specify Facebook site-id used during Facebook Check-in.
   k. When enabling wired captive portal based registration with ExtremeGuest, create a dummy wlan '$location-vlan-VLAN-ID' on the wired device where captive portal is enforced. $location – value of rf-domain location string.
2. Content Caching: No longer support Smart cache feature configurations.
3. AP 8432 – DFS channels for Korea country code are enabled.
4. WiNG 5.9.0 enables support to send RSSI data feed to ExtremeLocation service. Simultaneous RSSI feed to ADSP and ExtremeLocation services are not supported.
5. NSight AVC: –
   a. NSight widgets may show applications and protocols from previous release in case there is no matching application with new DPI engine.
   b. New client per app widget – new widget allows user to see the new dashboard which shows app name, number of clients using the app, and throughput usage.
6. NSight new alarm - Low or Zero Clients Alarms on Radio. NSight alarm management will raise alarms for a given AP radio when there are no clients associated for 7 days or more.
7. NSight client list report includes more details (SNR, RSSI, RX/TX traffic, session-length) in the CSV report.
8. WiNG Wired Captive Portal based self-registration and onboarding is supported with ExtremeGuest in external mode (i.e. splash template should be hosted on ExtremeGuest and Captive Portal should be configured with External URLs)
9. RF Domain location service commands are now called as 'location-server' instead of 'mpact-server'.
10. Adoption – "adoption-mode controller|cloud" configuration option is moved to profile and device-override mode, from rf-domain mode. Upgrade to WiNG 5.9.0 firmware will automatically migrate the configuration to device-override mode.
11. Enhanced "show wireless radio statistics rf" command to show channel utilization details.
12. WiNG 5.9.0 adds 'ignore-failure' option to device-upgrade staggered command – this option will continue to reboot next set of APs even if one or more APs fail to come back after reboot.
13. RTLS: -
   a. Added support to configure rtl-server-policy parameters from RFS 6000 controller.
   b. Increased RSSI feed URL length from 64 to 256 characters.
14. Enhanced "CLI: "show adoption pending" to show cdp/lldp information of an AP.

New in v5.8.6

1. Recommended browser when using NSight in v5.8.6 are:
   -Chrome – ver 56.0.2924.87 (64-bit) till ver 58.0.3029.110 and from ver 59.0.3071.109 and up.
2. In Split VX environment, if the NSight server is rebooted without disabling nsight-policy, it will not be able to establish connection to Mongo and following error is seen:
   MongoError: Topology is broken.
   To fix this user needs to disable and then re-enable NSight.
3. Default update/data aggregation intervals for NSight has been modified to the following:
   1 Minute - 8 Hours
   10 Minutes - 1 Month
   1 Hour - 6 Months
   1 Day - 1 Year
   NSight database summary duration 8 720 4320 8760
   wireless client stats update interval to 60 seconds.

Recommended statistics update interval for Aps is no more than 2 minutes. For large deployments – recommended statistics update interval for clients is 5 minutes.

4. When configuring DPI – use DPI capable device as RFDM manager. It's not recommended to use non-DPI capable devices when using this feature.
5. NSight ASA: UI slowness while running ASA and browsing old ASA results
   The slowness of UI is caused due to a large number data points that has to be plotted on the UI in Spectrum Analysis for Spectrogram and Spectral Density charts. Expect approximately 1-minute delay before the plotting begins on the ASA window.
   This limitation, however, is not applicable to Duty Cycle, FFT or Interference charts.
6. When configuring a database-policy replica-set using FQDN, enable ip dns-server-forwarding on all WiNG devices participating in the replica set and the NSight/Guest-Manager application servers.
7. New CLI command for WiNG 5.8.6 to support forwarding of packet types that are not normally forwarded by l2 tunnel broadcast optimization.
   l2-tunnel-forward-additional-packet-types ?
   wnmp Forward WNMP packets across l2 tunnels
8. To form a mesh redundant link - STP packets coming from a mesh port need to be forwarded to wired ports. Prior to WiNG 5.8.6 is was not allowed and blocked by STP. By default, the STP packets destined to bridge group mac address coming from a mesh port was not allowed to cross the bridge. This behavior is changed.
9. AP 8163 – DFS channels for Korea country code are disabled.
10. WiNG 5.8.6 adds ability to use "service reset interface ge", "clear counters interface all", and "clear counters all" on rf-domain level.
    clear counters all on ?
    DEVICE-OR-DOMAIN-NAME AP/Controller/RF-Domain name
    clear counters interface all on ?
    DEVICE-OR-DOMAIN-NAME AP/Controller/RF-Domain name
    service reset interface ge 1 on ?
    DEVICE-OR-DOMAIN-NAME AP/Controller/RF-Domain name
11. WiNG provides new CLI to configure NAS-IP-ADDRESS. User now has control on which IP to set as the NAS-IP-ADDRESS.
    Following command is now part of AAA policy:
    attribute nas-ip-address <IP address>
12. WiNG 5.8.6 adds enhancement to replace device feature added in WiNG 5.8.5 for replacement of old existing device with newly added devices by allowing to add the replacement device first to the configuration.
13. To help user to copy startup configuration from one AP to another WiNG 5.8.6 replaces <device-type self-mac> with "self" in startup-config.

New in v5.8.5

1. WiNG 5.8.5 resolves radio power output issue for AP 7532, 7562 as well as power issue when using 3af power source for AP 8533 and AP 8432.
2. Disallowed configuration of character '/' in the names of tree-nodes for an RF-Domain (i.e. country/region/city/campus names) If one has already configured '/' in the names of tree-nodes for an RF-Domain (i.e. country/region/city/campus names), then after upgrading the '/' characters in the names of tree-nodes will be replaced by '-' character. The e.g. name "West/Coastal" and "West/Plateau" will be replaced by "West-Coastal" and "West-Plateau". The downgrade will not restore the character '/' back in the names if they were changed during the upgrade. If the customer had enabled NSight while character '/' was present in

any of the tree-node name configuration, the customer should
drop the database before upgrading to the release containing this change.

3. Adding a new CLI under firewall policy to log all ICMP packets allowed by our firewall.
   firewall-policy fw-default
   logging icmp-all
   default is false (no logging).
4. WiNG 5.8.5 adds ability to configure Mongo DB security. Mongo authentication is controlled by a configurable parameter in the database-policy, with the default case being disabled.
5. Corrected the behavior of radius.
   Fallback is only used when the external LDAP server fails. And not on auth REJECT.
   'authentication data-source ldap fallback'
6. Incorrect LLDP power negotiation with certain Cisco switches on boot up is seen. New CLI configuration “service LLDP tx-init-count” cli added with default count of 3 packets. This will allow sending multiple LLDP packets to allow for correct power negotiation with certain Cisco switches.
7. To prevent gateways being marked as clients - mac-address-table detect-gateways default changed to enabled.

New in v5.8.4

1. WiNG NSight
    a. The VX-Split Mongo deployment scale and resource requirements:
        i. Scales up to 100,000 APs, 1 Million clients, and 2000 RF-domains without AVC metadata (2 minutes’ update interval)
            1. NSight-Server (UI): 12 GB RAM, 16 Core, 200GB
            2. NSight-Mongo Server: 384 GB RAM, 24 Core CPU, 4 TB (8000 sustained writes)
        ii. Scales up to 50,000 APs, 500K Clients and 1000 RF-domains with AVC metadata (1-minute update interval)
            1. NSight-Server (UI): 12 GB RAM, 16 Core, 200GB
            2. NSight-Mongo Server: 256 GB RAM, 24 Core CPU, 4 TB (8000 sustained writes)
    b. Added configuration ‘geo-coordinates <latitude> <longitude>’ in RF domain context to specify site locations for NSight Google map view.
    c. Site wide statistics, for example, Worst sites by RFQI, my present misleading values when of the radios on all APs in the site is disabled.
    d. Scheduled reports may need to be reconfigured to adjust to the Daylight Savings time switch.
    e. AVC application statistics collection might miss the last update before roam for a roaming client
2. Captive Portal: WeChat social authentication is supported only in distributed mode. No support for centralized captive portal deployment model.
3. Port description TLV has been added in LLDP packet parsing for ‘show lldp’ command outputs and can be used in auto-provisioning policy for LLDP-match.
4. Added ‘vlan’ keyword to the DNS critical resource-monitoring configuration to support dynamically assigned IP addresses.
5. Added an optional ‘hide-encrypted-values’ parameter to the ‘show running-configuration’ to display consistent (standard) characters for encrypted strings in the configuration. This facilitates periodic check for changes in configuration by customer monitoring systems.
6. The length of logout FQDN and localization FQDN configuration in captive portal has changed from 256 to 128 characters.

7. AP 8533 and AP 8432 with a manufacturing date before June 28, 2016, does not support MU-MIMO with WiNG 5.8.4 firmware hardware driver.
8. The Bluetooth configuration in AP 81XX profile settings only applies to AP 8132 and not for AP 8122 and AP 8163.
9. AP 7532, AP 7522, AP 7562, AP 8533 and AP 8432 do not support multiple SSIDs per BSSID due to restrictions enforced by the chipset/driver.
10. AP 7532, AP 7522, AP 7562, AP 8533 and AP 8432 require a WLAN is always mapped (no shutdown) to BSS1 for any radio functionality to work properly.
11. Web/Content Filtering is not supported with Tunnel mode configuration.

New in v5.8.3

1. HTTPS connections will use TLS 1.2 ciphers by default. To allow backward compatibility for non TLS 1.2 capable devices to connect– configure in management policy, “no https use-secure-ciphers-only".
2. Added an event log message to report an error condition when an ACL using alias (network, network-group etc) definitions results in expanding to more than 500 rules per ACL. The ACL will not get applied and the following log message is generated (event history/syslog) – “ACL rules exceeded the maximum limit; reduce the rules for ACL to get installed”.
3. EX 3500 and T5 adoption running non TLS1.2 compatible versions will need to have “no https use-secure-ciphers-only” configured to get adopted.
4. NSight: In addition to being able to search for a mac-address in the global search box using 11-22-33-44-55-66/11:22:33:44:55:66/112233445566 formats, now a user can search using the Cisco MAC Address format 1122.3344.5566 as well.
5. Added a CLI command in mint global policy to enable/disable the checksum validation for certain mint control packets such as LSP.
   To ensure the integrity of the LSP packets received checksum is added as an optional field.
   [no] lsp checksum
6. The ftp server throttles simultaneous connection from same host to a limit and it is implementation specific. The new CLI can be used to configure the simultaneous connection to a FTP server.
   remote-debug max-ftp-sessions <1-400>
   [no] remote-debug max-ftp-sessions
   device-override remote-debug max-ftp-sessions
7. SSH diffie-hellman-group1-sha1 key exchange algorithm was removed due to this older SSH applications might not work with WiNG 5.8.3 and customer will need to update to use newer more secure versions of SSH clients.

New in v5.8.2

1. Application Visibility
   - In bridge-mode tunnel setup where Application Visibility is enabled on the controller, APs will also have to be enabled for application visibility (DPI engine support on the platform is required) for Wireless Client statistics
   - Number of clients and top client information may be missing from certain entries on all application list. This may happen when the application is detected on the wired side or in the case where the usage for this application is very minimal.
2. VX 9000 - Not supported on Amazon instance type C4 due to kernel limitation.
3. Multi-byte (Chinese Character) SSID
   - Max limit of 64-character length for multi-byte SSID
   - Known limitation with Windows 7 Clients: Available Networks UI display unexpected characters for multi-byte SSID

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

New in v5.8.1

1. Some mobile devices (Apple) that use LDAP EAP-TLS as primary means of authentication can fail authenticating to WiNG controller. Work-around would be configuring authentication type as PEAP-MSCHAPv2 on the controller when using LDAP.
2. AP7522, AP7532, AP7562, AP8232, AP 8222 and AP7502 do not support multiple SSIDs per BSSID due to restrictions enforced by the chipset/driver.
   WiNG 5.8.1 adds commit time validation for multiple SSIDs per BSS for AP 7522, AP 7532, AP 7562, AP 82xx and AP 7502 and will throw an error if misconfiguration is detected.
3. Adaptivity recovery on/off command gives the user ability to configure adaptivity recovery. When adaptivity recovery is turned off, if radio enters adaptivity mode then it will not switch channels. By default – this feature is enabled.
4. LDAP chase referral has been disabled by default in all platforms to address memory and authentication related issues. It can be enabled if necessary under radius server policy.
5. If the CLI command - "upgrade <URL> on <device-name>" is being used, then please note it has been changed to "upgrade <URL> <device-name ...>".
6. Added additional filters to be used on rf-domain when remote-debug is done on rf-domain. Additional filters include area, floor, and containing a field which takes a substring of hostname and selects devices matching that hostname string to run remote-debug.

New in v5.8

1. WiNG NSight
   - WiNG NSight is supported on the NX 9500, NX 9600 and VX 9000 platforms with the following scale limits:
     - VX 9000: Supports up to 10,000 APs (@ 500 RF domains) / 5,000 (@ 1000 RF domains)
     - NX 9500: Supports up to 6,000 APs (@ 200 RF domains)
     - NX 9600: Supports up to 3,000 APs (@ 200 RF domains)
       [Note: NSight scale numbers are relatively lower in NX 9600 than NX 9500 due to IOPS limits in RAID5 disk configuration. Future WiNG releases will change RAID configuration in NX 9600 to RAID1+0 for improved IOPS]

   - WiNG NSight license is preloaded in WiNG 5.8 (platforms: NX 9500, NX 9600, VX 9000) for immediate use, limited to 120 days from the date of install. The user is expected to purchase and install required number of WiNG NSight subscription license for continued operation.
   - New dashboard created via one browser session will not be visible/available on a different, already open session. It will be available for any new session logins.
   - The filters, for instance – selecting a specific WLAN, on the Dashboard widgets will apply even when the user moves across sites/levels on the left-side navigation tree.
   - *Top/bottom 10 grid tables in the summary page (and in the widgets) will not show any data if the table entries values are zero.*
   - For WiNG NSight system running for a limited amount of time (few hours), 'Top App by usage' may not show details for larger aggregate statistic duration (1 month, 3 months).
   - 'location' command in the rf-domain configuration will be used to store geo-coordinates of the site-location for MAPVIEW functionality.
   - *While using 'Heatmap' on the MapView/Floormap, user must select one channel at a time for correct heatmap view*
   - *In Hierarchical Mode, an offline AP may show up as online status under local controller details. The correct AP status is shown on the Key Metric Strip or the device list/details.*
   - *In MapView/Floormap the user defined custom columns in show table option may not be retained after page refresh.*

- *The top X charts in the summary page may show incorrect client count when the clients are roaming*

2. Captive-Portal
   - Captive portal user database storage is supported on the NX 95XX/ NX 96XX/ VX 9000 and NX 75XX platforms with the following scale limits:
     - NX 95XX/ NX 96XX / VX 9000 - 2 Million user identities
     - NX 75XX - 1 Million user identities
   - If client device roams (to a nearby AP) between the initial connection redirect and the registration action, the registration may not work and user needs to close/open the browser to connect/register to the captive portal.
   - Upgrade to 5.8 (from 5.5.x and above) will do a one-time import on the existing (SQlite) user database into the newer MongoDB database.
   - Configure “bypass captive-portal-detection” in the captive-portal-policy to ensure the OAUTH functionality works properly on the iPhones and Windows mobile phones.
   - While uploading logo/images for captive portal using sftp in CLI, the user will not be prompted for a password and is expected to supply along with the username in the command line.
   - With over 1.5 million user entries in the Captive-Portal database, the controller may respond with a delay for the CLI command “show guest-registration user trends time all” when issued after restart/reboot.
   - User trend data graphs and charts are shown in UTC time zone.
3. Application Visibility & Control
   - The Blackberry/email, Blackberry/encrypted and Blackberry/messenger will be categorized under the application ‘Blackberry’
   - *Clearing application stats resets the tx and rx counts to zero and does not affect the currently active flows.*
4. Client-Bridge
   - Packet capture on the infra-AP with traffic using CCMP are unencrypted packets due to hardware based CCMP encrypt/decrypt operation.
   - The INF WLAN VLAN must match the VLAN used in the Client Bridge GE1, WLAN, and SVI.
5. Wired 802.1x with Mac-Authentication enabled: Microsoft Windows clients must have "Fallback to unauthorized network access" enabled for mac-authentication to occur in the event of an 802.1x failure
6. EAP Termination
   - MS-CHAPv2 is mandatory for EAP termination functionality
7. VX 9000
   - Flash partition has been increased to 1Gb with the .iso install. Simple .img upgrade will continue to work with the old 64MB flash partition.
   - The user may observe “Low memory on the running VM” message when installing VX for the first time with large disk size allocations (1TB or more).
8. AP 7502
   - AP 7502 does not support WEP-128 and Keyguard on the 5GHz radio
9. To operate Cisco phones with AP 7532, the interface radio settings should include dynamic-chain-selection strict
10. Captive Portal: OAUTH may not work properly with Lumina phone running older Windows version (< 8.1). Please upgrade Lumina phones to latest OS.
11. The WiNG GUI may become unresponsive in Firefox browser when 10,000+ adopted APs are displayed on the navigation tree. This is due to Shockwave plugin.

New in v5.7.0

1. 'no ip dhcp trust' functionality does not work on the AP 7502 FE ports.
   FE port on AP 7502 will not drop the packet because switch on AP 7502 is not configured to drop. FE port will pass discover packets from dhcp server irrespective of "no ip dhcp trust" to ge1. User can configure GE1 to drop.
2. Wired captive portal – to support clients with MAC authentication, 802.1x configuration is also required for the controller
3. OpenDNS:
   - The dhcp server/pool policy configuration is required to include the OpenDNS IP (*208.67.220.220, 208.67.222.222***)** as the dns-server
   - The ip access-list is required to include the following firewall rules to prevent clients from using any unauthorized DNS server
     permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description "allow dns queries only to OpenDNS"
     deny udp any any eq dns rule-precedence 10 rule-description "block all other dns queries"
4. ETSI 1.7.1 Adaptivity Limitation on AP 622, AP 6522, AP 6562
   This note applies to the following APs that end with "-EU". These APs are sold to countries that comply with the EU directives - AP 622, AP 6522, and AP 6562. This does not apply to APs that end in "-US" or "-WR"
   - Radio 1 will support operation as a 2.4Ghz data radio compliant with ETSI 1.7.1 adaptivity directive
   - Radio 2 cannot be enabled for operation as a 2.4Ghz data radio. Radio 2 will support operation as a 5Ghz data radio only
   - If using Radio 2 in 2.4Ghz, please enable Radio 1 for data access in 2.4Ghz
   - When Radio 2 is configured as a dual-band security sensor with an ADSP appliance;
   - Radio 2 will not support Air Termination, AP Test, and Network Assurance at 2.4Ghz band
   - Radio 2 will support receive packet and forensic security analysis at 2.4Ghz band
   - Radio 2 will support Air Termination, AP Test, Network Assurance and all packet receive functions on the 5Ghz band
5. The following defaults and CLI commands / help-strings have been changed as part of the de-branding:

	WiNG 5.7.x	**Older versions**
Default username / password	admin / admin123	admin / motorola
Default DNS name	"WiNG-wlc"	"Motorola-wlc"
Default WLAN name	"WLAN-1"	"Motorola"
CLI command	"wing-extensions"	"motorola-extensions"
	"wing-ie"	"symbol-ie"
CLI help string	WiNG	Motorola or Symbol
802.1x default username / password	admin / admin123	admin / motorola

6. AP 6522/6532/6562/7161 - VRRP and OSPF feature support have been removed

New in v5.6.x

1. IPV6:

   - IPv6 ACLs do not support the object-oriented firewall feature in this release.
   - The IPv6 implementation does not support IPsec VPNs in this release.
   - IPv6 – MLD snooping is not supported on the ethernet switch ports on the NX 4524 and NX 6524 platforms. It is supported only on UP1, UP2 ports.
   - IPv6 – When there are multiple DHCP servers (one for IPv4 and another for IPv6) that respond to option 191, ensure that both provide valid IP addresses/ hostnames. Otherwise, with both servers responding the later response will override the previous response. If the

later response does not contain valid information, AP will not be able to adopt to the controller.

2. VX 9000:
   - MAC address of the device should not be changed once installed/configured.
   - Only 1 GE1 interface is supported on the VX platform.
   - VX 9000 instances running in Amazon EC2 must use "Elastic IP" to retain the public IP when the instance is stopped and restarted.
   - VX 9000 - VMWare and other hypervisors need to be configured in promiscuous mode for features like VRRP to work correctly.
   - When creating a cluster between multiple VX 9000's, all instances should use identical resources (e.g. replication from one instance with higher memory to a smaller one can lead the smaller instance to run out of memory).
   - VX 9000 – Ipv6 is not supported when using Microsoft HyperV as the virtualization platform.
3. Captive Portal Time Based Voucher is only supported with Active: Standby configurations. Active: Active based clusters are not supported. The database gets replicated from the Active Controller to the Standby Controller periodically (default is 5 min).
4. Wired Captive Portal
   - If wired captive portal is being used along with wireless captive portal on the same controller, then same captive portal policy needs to be used for both wired and wireless captive portal enforcement.
   - If Wired captive portal is being implemented for a bridged VLAN on the controller's physical interface that receives APs traffic, then applying wireless captive portal for the same bridge vlan is not valid, since the wireless client will then be subjected to captive portal enforcement twice.
5. The following default values have been changed/ corrected:
   - *route-limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 1| route -limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 3:* reset time was changed from 1 to 3.
   - vrrp-state-check command previously present in "router ospf" context, has been moved to device/profile context
   - min-misconfiguration-recovery-time 120: increased from 60 to 120.

New in v5.5.x

1. Deprecating the usage of TKIP Encryption:

From January 1st , 2014, the WPA-TKIP is no longer allowed for Wi-Fi Alliance product certification. For AP/STA products wishing to support a legacy device that can support only TKIP encryption, customer needs to implement mixed mode with WPA/WPA2.

Following changes are enforced from WiNG 5.5.3 release onwards to comply with the above Wi-Fi Alliance requirement:

- Configuring encryption type as TKIP for a wlan will no longer be supported; wlans requiring to support TKIP clients should use tkip-ccmp as the encryption type.
- Upgrading from a prior WiNG 5.x to release to WiNG 5.5.3 will automatically modify the configurations for wlans using 'tkip' as encryption type to 'tkip-ccmp' and will add "service wpa-wpa2 exclude-ccmp" command to avoid any post upgrade incompatibility issues.
- For new configurations, to handle certain legacy/non-Wi-Fi compliant client situations where the client driver is incompatible or does not operate properly in a mixed mode TKIP-CCMP configuration, add the following command "service wpa-wpa2 exclude-ccmp" to the wlan configuration. This configuration allows the wlan to operate in TKIP only modes until the non-compliant wireless clients are phased out of the network.

2. Ability to optionally include 'DHCP client-identifier' as part of DHCP Discover/Request packets:
   If your DHCP server uses DHCP client identifier for static bindings (DHCP lease reservations) and responds only to DHCP Discover/Requests with DHCP client identifier present, then the client identifier can be included by configuring the following command "DHCP client include client-identifier" under the SVI (interface VLAN X) which is configured as DHCP client.
3. Auto-provisioning policy: 'reevaluate-everytime' command is modified to 'evaluate-always' and moved to 'auto-provisioning-policy' from device/profile context. Upgrade from 5.5.1 to 5.5.3 or later versions should work in accordance with location and syntax changes. However, a downgrade from 5.5.3 to former versions would cause the command to disappear from all contexts.
4. Zebra devices with Jedi radios can have connectivity issues when 5.5 and 11 mpbs rates configured on infrastructure. Impacted devices are: MC1790, MC5590, MC7590, MC7594, MC9590, MC9596, MC3190, MC75, MC9190, MC55, VC6090, VC6096, MT2090, MK3900, MK4900, MK590.
   If SSID/band is used exclusively for 802.11g or 802.11gn devices (i.e. no 802.11b devices), configure the data-rates on the SSID/radio to be "g-only" or "gn" or custom with 5.5 and 11 Mbps excluded from the basic rate set.
   If SSID/band is used by 802.11b-only devices as well, configure the data-rates on the SSID/radio to be custom with 1 Mbps and/or 2 Mbps as basic and exclude 5.5 Mbps and 11 Mbps from the supported rates.
5. CDP and LLDP protocols are enabled by default on WiNG devices. If the wired infrastructure has a combination of managed and unmanaged switches and some are not CDP protocol aware, then CDP protocol needs to be disabled on AP profiles to avoid the L2 switch flooding the packets to all ports.
6. WLAN controller does not retain saved auto upgrade configuration when downgrading from 5.5 to pre-5.5 release. This is because "ap-upgrade" commands were renamed to "device-upgrade" in 5.5. When upgrading to 5.5, the conversion happens automatically, however, when downgrading from 5.5 the previous firmware release does not understand "device-upgrade". The workaround is to manually fix the configuration.
7. Mesh Connex Migration – With the introduction of Auto Channel Select, Mesh Connex Configuration will be migrated when the WLAN controller reboots. The following parameters get migrated:
   - Channel list from smart-rf is copied on to the rf-domain.
   - Priority meshpoint name and root recovery parameters are copied to the meshpoint-device configuration under device context or profile of the APs.
8. WiNG 5.5 introduced the addition of precedence to ip nat rules.
   ip nat inside source list mylist ?
   precedence Set precedence of access list
   For example ip nat inside source list mylist precedence 1 interface vlan2 overload
9. In WiNG 5.5 legacy mesh related show commands have been replaced with 'mint' to remove confusion with meshpoint functionality. Use "show wireless mint links" to see the legacy mesh links.
10. **Captive Portal Deployments using External (or) Advanced pages:**
    Captive portal query string delimiter has been changed to '&' instead of '?' from WiNG 5.5 onwards. When upgrading to a 5.5.x based firmware, the JavaScript embedded in the external or advanced webpage(s) needs to be updated to parse the new style of query stings.
    Following line needs to be modified under function **getQueryVariable(variable),**
    var vars = query.split("?"); === change it to ==▯ var vars = query.split(/[?&]/);
    Please ensure that this function gets updated in all the captive portal pages that uses it.

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

New in v5.4.x

1. Interoperability with Samsung S2 devices:
   A Samsung Galaxy S2 device sometimes fails to connect using EAP-MAC authentication and WEP64 encryption. It's recommended to reduce the number of attempts (authentication eap wireless-client attempts) from default 3 to 2.
2. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.
3. MCX max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where the range is 24km.
4. It's recommended disabling IP DoS attacks in firewall policy when configuring IGMP snooping.
5. 10 GbE support on the NX 9510 is limited to SFP+ SR interfaces that are included in the controller. LR or XR SFP+ are not supported.

Deriving secondary IP

APs have a shadow or secondary IP for gaining access to the AP if the IP address of the AP is not known but the MAC address is known. To derive the shadow IP address of an AP, use the last two hex bytes of the AP's MAC address to determine the last two octets of the IP address.

- AP MAC address - 00:C0:23:00:F0:0A
- AP IP address equivalent – 169.254.240.10

To derive the AP's IP address using its factory assigned MAC address

- Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.
- With the Calculator displayed, select View>Scientific. Select the Hex radio button.
- Enter a hex byte of the AP's MAC address. For example, F0.
- Select the Dec radio button. The calculator converts the F0 to 240. Repeat this process for the last AP MAC address octet.

7. DFS TABLES, SENSOR AND RADIO SHARE

1. Following is the DFS support in WiNG 5.9.7 for the supported radio platforms:

Product	Master DFS FCC	Master DFS IC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS IC	Client DFS ETSI	Client DFS Japan
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 6522 AP 6562	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled
AP 8163	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled	Enabled	Disabled
AP 7502	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 7532 AP 7522	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7562	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8533	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8432	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled	Disabled
AP 7602	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Disabled	Disabled

Product	Master DFS FCC	Master DFS IC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS IC	Client DFS ETSI	Client DFS Japan
AP 7622	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7612	Enabled	Enabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled
AP 7632	Enabled	Enabled	Enabled	Disabled	Enabled	Disabled	Enabled	Disabled
AP 7662	Enabled	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled

2. Air Defense sensor capabilities are supported on the 802.11n/802.11ac APs in this release and are available for enabling the WIPS functionality as well as the Network Assurance Capabilities. There are some caveats on managing the AP directly via ADSP, for certain AP platforms:

As a dedicated sensor	WIPS & Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Test	Connection Troubleshooting	WVA
AP 6522/6562	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7161	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
AP 7532/7522/7562[1]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8163	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7502	No	No	No	No	No	No	No	No
AP 8533[2]	Yes	No	Yes	No	Yes	Yes	Yes	Yes
AP 8432[2]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7602/7622	Yes	No	No	No	Yes	No	No	No
AP 7632/ 7662/ 7612[1]	Yes	No	Yes	No	Yes	No	No	No

Notes:
[1]AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 7612 radios are band-locked, entire AP needs to be dedicated as sensor
[1]Support is limited to the dedicated sensor (Radio 3) for AP 8533. Support is limited to the dedicated sensor (Radio 1) for AP 8432.

3. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is available on the 802.11n/802.11ac APs with some caveats – please see details below:

In Radio Share mode	WIPS & Advanced Forensics	Spectrum Analysis[2]	Advanced Spectrum Analysis[3]	Live RF	Live View	AP Test[5]	Connection Troubleshooting	WVA
AP 6522/6562[1]	No	No	Yes	Yes	Yes	Yes	Yes	No
AP 7161	No	No	No	Yes	Yes	Yes	Yes	No
AP 7532/7522/7562[4]	Yes	No	No	Yes	Yes	No	Yes	No
AP 8163	No	No	Yes	Yes	Yes	Yes	Yes	No

In Radio Share mode	WIPS & Advanced Forensics	Spectrum Analysis[2]	Advanced Spectrum Analysis[3]	Live RF	Live View	AP Test[5]	Connection Troubleshooting	WVA
AP 7502	No	No	No	No	No	No	No	No
AP 8533	No	No	No	No	No	No	No	No
AP 8432	Yes	No	No	No	Yes	No	Yes	No
AP 7602/7622	No	No	No	No	No	No	No	No
AP 7632/ 7662/ 7612[4]	Yes	No	No	No	Yes	No	No	No

Notes:

[1]AP 6522, 6562 – The first radio is band-locked to 2.4Ghz. The second radio is capable of ABGN sensor operation.

- In Radio 1 = Sensor, Radio 2 = Wlan configuration, the sensor will only scan 2.4Ghz channels on Radio 1.
- In Radio 1 = Wan, Radio 2 = Sensor configuration, the sensor will scan both bands on Radio 2
- In Radio 1 = Sensor, Radio 2 = Sensor configuration, the sensor will scan 2.4GHz on Radio 1 and 5GHz on Radio 2

[2]Spectrum Analysis is not supported with Radio share enabled.
[3]Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.
[4]AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 7612 radios are band-locked, both radios are required for sensing
[5]AP Testing in radio share mode - only single-cell/internal BSS AP testing is supported. AP Testing on remote BSS is not supported.

8. VULNERABILITY UPDATES

In case a patch has been applied to address vulnerability even though vulnerability was addressed – some security scans only check the version number of the component as opposed to testing the actual vulnerability – and therefore might still report issue being present.

WiNG 5.9.7

CVE-2019-13012: The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.60.0 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used.

WiNG 5.9.6

CVE-2018-2048: Wget updated to v1.20.1.
CVE-2019-11477: TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs).

WiNG 5.9.5

CVE-2019-11234 and CVE-2019-11235: radius vulnerabilities have been patched.
CVE-2017-18258: allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file – has been patched.
CVE-2019-3822, CVE-2019-3833: libcurl: stack-based buffer overflow vulnerability. Libcurl was updated to v7.57.0.
CVE-2015-9261: huft_build in archival/libarchive/decompress_gunzip.c in BusyBox before 1.27.2 misuses a pointer, causing segfaults and an application crash during an unzip operation on a specially crafted ZIP file – has been patched.
CVE-2018-10883: A local user can cause an out-of-bounds write in jbd2_journal_dirty_metadata(), a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.

CVE-2009-5155: parse_reg_exp in posix/regcomp.c misparses alternatives,
which allows attackers to cause a denial of service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.
CVE-2009-3002: The Linux kernel before 2.6.31-rc7 does not initialize certain data structures within getname functions, which allows local users to read the contents of some kernel memory locations by calling getsockname.
CVE-2017-18221: The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service
CVE-2009-3001: The llc_ui_getname function in net/llc/af_llc.c in the Linux kernel 2.6.31-rc7 and earlier does not initialize a certain data structure.

WiNG 5.9.4
OpenSSL upgraded to 1.0.2q
CVE-2017-18344: The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function.
CVE-2018-15473: OpenSSH through 7.7 is prone to a user enumeration vulnerability (Qualys Scans) – patch applied to openSSH 7.6 version to address this vulnerability.

WiNG 5.9.3
OpenSSL upgraded to 1.0.2o.
CVE-2018-5390 [VU#962459] [FICORA #1052508] Vulnerability Notification
CVE-2018-10124 Allows DoS attack by local users, via INT_MIN argument
CVE-2018-10087 denial of service by triggering an attempted use of the -INT_MIN value
CVE-2018-8897 The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions, may result in unexpected behavior
CVE-2018-0739 Constructed ASN.1 types with a recursive definition could result in a DoS attack.
CVE-2017-18255 Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow)

WiNG 5.9.2
Following modules were upgraded in WiNG 5.9.2 to pick up latest vulnerability fixes:
Radiusd upgraded to v3.0.11.
OpenSSH updated to v7.6.
Lighttpd upgraded to v1.4.48.
openSSL upgraded to 1.0.2m.
libCurl upgraded to 7.57.0
NTP upgraded to 4.2.8p11.

CVE-2017-18208 Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop). CVE-2018-10940 CVE-2017-1000251 against linux 2.6.32.24 and 2.6.35.9 (cpe:/o:linux:linux_kernel:2.6.32.24 and 2.6.35.9)
Multiple CVE's against openssl: 1.0.2h and 1.0.2j: CVE-2017-3737 and CVE-2017-3738
Multiple CVE's against Linux kernel 2.6.28.9, 2.6.32.24, 2.6.35.9 (CVE-2017-17052, CVE-2017-15116, CVE-2017-17807).
CVE-2017-15102, CVE-2017-15115, CVE-2017-16994, CVE-2017-16939, CVE-2017-12193 and CVE-2017-15868 against Linux kernel 2.6.28.9, 2.6.32.24 and 2.6.35.9
CVE-2017-1000257: An IMAP FETCH response line indicates the size of the returned data, in number of bytes.

CVE-2017-15906: The process_open function in sftp-server.c in OpenSSH
before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
libcurl 7.52.1 (cpe:/a:haxx:libcurl:7.52.1): CVE-2017-1000254, CVE-2017-1000100, CVE-2017-8816 and CVE-2017-8817
Multiple vulnerabilities against cpe:/a:gnu:glibc (CVE-2013-4237, CVE-2014-0475 , CVE-2013-4458, CVE-2014-6040, CVE-2013-4332, CVE-2013-7423, CVE-2013-7423, CVE-2014-8121, CVE-2014-7817, CVE-2017-16997)

WiNG 5.9.1
CVE-2017-10983,CVE-2017-10982,CVE-2017-10981,CVE-2017-10980,CVE-2017-10979,
CVE-2017-10978 – FreeRadius 2.2.3 was patched to address those vulnerabilities
CVE-2016-9806 - Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service.
CVE-2017-7494 – Samba package was patched to address remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

WiNG 5.9.0
CVE-2015-4680: FreeRADIUS 2.2.x before 2.2.8 and 3.0.x before 3.0.9 does not properly check revocation of intermediate CA certificates.
NTPD package has been upgraded to ntp-4.2.8p10 to incorporate latest security vulnerability: CVE-2017-6464, CVE-2017-6462, CVE-2017-6463, NTP-01-011 NTP, NTP-01-010 NTP.
CVE-2015-8983: Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU can allow for DoS
CVE-2015-8984: The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service
CVE-2015-2877: Kernel Samepage Merging (KSM) in the Linux kernel 2.6.32 through 4.x does not prevent use of a write-timing side channel
CVE-2017-6074: DCCP double-free vulnerability which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call, has been fixed
CVE-2016-3076: Heap-based buffer overflow in the j2k_encode_entry function in Pillow 2.5.0 through 3.1.1 allows remote attackers to cause a denial of service (memory corruption) via a crafted Jpeg2000 file is fixed by Updated pillow to 3.2.0 version.
Libcurl package updated to 7.52.1 to address multiple vulnerabilities: CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625.

WiNG 5.8.5
OpenSSL package has been upgraded to 1.0.2j to incorporate latest security vulnerability fixes.

WiNG 5.8.4
CVE-2015-7560: Samba (smbd) package patched to address remote authenticated user access to arbitrary ACLs.
libxml2 package has been upgraded to v2.9.2 and addresses CVE-2013-0339 and CVE-2014-3660 security vulnerabilities.
CVE-2015-8552: Xen PCI driver patch fixes the denial of service vulnerability.

WiNG 5.8.3
OpenSSL package has been updated to 1.0.1p to incorporate latest security vulnerability fixes.

CVE-2015-7547: Glibc getaddrinfo stack-based buffer overflow
TLS/SSL Server Support for DES and IDEA Cipher Suites (ssl-des-ciphers) was removed
TLS 1.0 and TLS 1.1 disabled by default.
The SSH server support for the diffie-hellman-group1-sha1 key exchange algorithm, which is known to have a potential security weakness has been removed.

WiNG 5.8.2
Linux kernel patched to address security vulnerability CVE-2015-5707

WiNG 5.8.1
OpenSSL package has been updated to 0.9.8zg to incorporate latest security vulnerabilities fixes.
CVE-2015-5600 – OpenSSH package has been patched to address this vulnerability.
OpenLDAP package has been updated to incorporate latest security vulnerabilities fixes.

WiNG 5.8
cURL and libcurl packages have been patched to address security vulnerability CVE-2015-3143, CVE-2015-3145, and CVE-2015-3148.
RC4 algorithm has been disabled in SSL/TLS package used to address security vulnerability CVE-2015-2808.
NTP package has been upgraded to version 4.2.8p2 to address security vulnerabilities CVE-2015-1798 and CVE-2015-1799
Linux kernel patched to address security vulnerability CVE-2014-8160.
Xen package has been patched to address security vulnerabilities CVE-2014-8866, CVE-2015-2044, CVE-2015-2150, and CVE-2015-2151.
OpenSSL package has been upgraded to version 0.9.8zf to address security vulnerabilities CVE-2015-0289 and CVE-2015-0293.

WiNG 5.7
OpenSSL package has been upgraded from version 0.9.8za to 0.9.8zc to address Purecloud security scan vulnerabilities.
OpenSSH package has been ungraded to 6.6p1 and addresses security vulnerability CVE-2014-2532.

WiNG 5.5.6:
NTP v4.2.8p1 that addresses the following security vulnerabilities outlined in CVE-2014-9297, CVE-2014-9298, CVE-2014-9295, CVE-2014-9295, CVE-2014-9295, CVE-2014-9296 .
CVE-2015-0235 - GHOST Linux Vulnerability.
CVE-2014-4877 - wget updated to v1.16.

WiNG 5.5.5
Updated GNU bash program for NX series of controllers that fixes the Shellshock family of security vulnerabilities outlined in CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, and CVE-2014-6278.
Includes ability to disable/enable sslv3 for https module under management policy context. This is to address CVE-2014-3566 aka Poodle attack. The new command is “https sslv3”. The default setting is “no https sslv3”.

WiNG 5.5.2
Security Scan reports NTP "monlist" Feature Denial of Service Vulnerability "Serious; see EUI"

WiNG 5.5.1
Cross-Site Request Forgery (CSRF) based on CWE-352 family vulnerability

SecScan Qualys: Deprecated Public Key Length (QualysVersion Scanner 7.3.31-1, Vulnerability Signatures 2.2.580-2)
OpenSSH vulnerabilities - SSH Insecure HMAC algorithms enabled and SSH RC4 Cipher enabled

WiNG 5.4.x
CVE-2010-4478 - OpenSSH J-PAKE Session Key Retrieval Vulnerability
CVE-2012-0814 - OpenSSH Commands Information Disclosure Vulnerability
CVE-2012-3547 - Radius Security Vulnerability: freeradius and EAP-TLS length checks buggy
CVE-2013-4559 - lighttpd: setuid/setgid/setgroups return values not checked
CVE-2011-4362 - lighttpd: out-of-bounds read due to signedness error

9. ISSUES FIXED

Following issues have been fixed in WiNG 5.9.7 release:

CR/ESR	Description
WING-39661	SPR-3690 AP7662 running v5.9.6 rim crash is seen
WING-39551	SOMWSW-217 Add device discovery using WNMP
WING-39653	Session created in controller for NSight tools are not getting deleted
WING-39599	"service show discovered-devices reset-log" shows the "unknown state"
WING-39595	keyword "TRON" is missing under license Feature name
WING-39561	"service show discovered-devices" shows the IP addresses in Little Endian format.
WING-39557	SPR-3680 Kernel panic due to mesh and tx deadlocks on multiple CPUs
WING-39548	AP stops transmitting and receiving in the presence of motion-sensor
WING-42209	Radius Group/Schedule/Access By Timer required
WING-42199	NX using device containing cli command not taking on all adopted access points
WING-42015	SPR-3688 Crash PC is at 0x0N LR is at process_tx_info+0x158/0x9c0 [qca_ol]
WING-42002	Some CLI commands don't show interface ge 2 in help or command completion even though the hardware supports ge2
WING-41994	5.9.7.0:Rest-api-user-roles:rest-api-user only rest user can access readonly permision, ssh telnet console should not be allowed to login
WING-39186	CVE-2019-13012
WING-39194	CLONE - Live view is not showing control frames for AP7632.
WING-39223	AP should not allow client internet access when client registers with one wlan and then associates to another
WING-39222	Include Reason for blocking the user in message . Presently user is shown "Internet access is blocked"
WING-39671	AP75xx: there is no smart-rf debug log (4D)
WING-39623	SPR-3685 RIM crash due to negative wlan index
WING-39607	[Regulatory:] "show wireless regulatory ..." command shows invalid power for country-code "Macau" (CFT version 5.1)
WING-39604	Add an option to specify MAC address in "service send discovery" command
WING-39602	Add an option to specify outgoing interface (g1/xge1 etc) while sending WiNG device discovery and reset request

CR/ESR	Description
WING-39605	Add number of discovered-devices to output of "service show discovered-devices"
WING-39673	AP75xx: rim core every 30 minutes with no clients (4D)
WING-39672	AP75xx: smart-rf didn't coverge, channel stay 1/36 (4D)
WING-39529	SPR-3679 AP8432 generates thinap2 core when debug is enabled
WING-42215	Smart-rf: Radio 2 doesn't discern neighbors and its operates max power
WING-42210	alphanet: ssm core after upgrade from 5.9.7.0-8D to 9D.
WING-42030	[Regulatory:] AP7612/32/62 Radio jumps to a different channel when channels 149-165 is configured for country-code 'mo'
WING-42017	Using AP Discovery Tool, One can factory Default a Controller with adopted APs.
WING-37589	Nsight:APT not working with poplar/willow as sensor-ap, throws test aborted at wips,birch cypress work fine
WING-37637	CLONE - ccmp aptest is fail with 7632 dedicated sensor
WING-38456	Remove Nsight directory from WiNG repo
WING-38523	SPR-3621: Panic file “PC is at hs_tx_dns_rsp” seen on AP when processing DNS response
WING-39053	Mapsim: Make mapsim independent of build machine architecture
WING-39042	SPR-3648: HSD process core seen when sending DNS response to CP client
WING-39262	SOMWSW-190 SMART-RF enhancement: ability to configure power per area
WING-39263	SOMWSW-178 User role with Read-only access for API
WING-39265	SPR-3663: Access point generated duplicate SNMPv3 EngineID
WING-39264	SOMWSW-188 Add Macau Regulatory Power Tables
WING-39279	Flex UI build fails intermittently
WING-39283	SPR-3664: Client-detail event needs to be turned off/disabled by default for WiNG deployments
WING-39287	SOMWSW-218 API to fetch/publish AP information
WING-39253	SPR-3662: Onboard WIPS Rogue/Unsanctioned Events UI displays SSID, Syslog does not display SSID
WING-39336	SPR-3667: WiNG device improperly routes UDP packet with source port 54345 across subnets
WING-39337	SPR-3666: BSSID missing from 'show wireless radio detail' output
WING-39373	SPR-3671: Cfgd crashes with overflowError when corrupt packet received from APs during adoption.
WING-39374	SPR-3672: Cfgd crashes with KeyError when corrupt packet is received from AP during adoption.
WING-39391	AP 7632 incorrectly updates basic rate when all 11b and ofdm rates are configured
WING-39466	SPR-3676: MCX: "show wireless meshpoint on rf-domain" shows root host name <unknown>
WING-39414	Panic file name shows date of the upgrade sometimes instead of date of the panic
WING-39341	UPS : l2tp tunnel of rf-domain manager stuck in standby state, although self is the rfdm.

CR/ESR	Description
WING-39370	SPR-3668: Softlockup happened when the CPU was otherwise idle
WING-39384	Reload on platform type doesn't work correctly for APs in the same family
WING-39413	Enable TRON config on NX5500 and NX 7500 controller as well as licensing
WING-39431	SPR-3673: HSD core crashes on APs with high quantity of clients connected
WING-39481	SPR-3677 Panic due to interim account timeout has become zero and MU roaming happened at same time
WING-39494	SPR-3675 WLAN data-rate override for 2.4GHz is throwing error on 5GHz radio
WING-39495	Latest event-history is not getting collected in techdump
WING-39518	cfgd error with OverflowError: signed integer is greater than maximum

10. KNOWN ISSUES

Following are known issues in WiNG 5.9.7:

CR/ESR	Headline	Comment(s)
WING-37808	CLONE - Sensor is able to terminate both Wireless client(intel) and BSS(Extreme AP) by sending unprotected De-Auth even though PMF enabled.	Requires BRCM SDK upgrade scheduled in WING 7.4.0.0.
WING-39182	Unable to handle kernel NULL pointer dereference at virtual address 00000004 PC is at skb_recycler_alloc+0xec/0x280 LR is at __netdev_alloc_skb+0x14/0x64	
WING-42183	Remote capture - WiNG AP - Protocol filters not working when both IP and MAC filters are used	Retest is suggested with modified filters.
WING-39659	WLAN shutdown when critical resource is down	
WING-42232	AP7632 broadcasts ssid when radio is in radar scan	Potential fix is suggested.
WING-39674	[SPR-3691]Fabric Attach with WiNG APs flushes out interface configuration when controller not present and connected to FA untagged mgmt VLAN	
WING-38618	AP76XX: Packet Capture Issues	
WING-39530	SPR-3681 Virtual controller deployment MU arp drop	
WING-38471	UI support for Wired side Dot1x supplicant with EAP-TLS support	
WING-39497	not able to upgrade RFD manager ap7502 from 5.9.2.5-001R to any higher version like 5.9.6.0-007R, flash space issue	AP7502 flash is small compared to growing size of WING upgrade images.

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

CR/ESR	Headline	Comment(s)
WING-39185	CVE-2019-13272 - In linux kernel - allows local users to obtain root access by leveraging certain scenarios	For legacy AP platforms, there is no plan to upgrade kernel version.
WING-42216	Smart-rf : Radio-1 operates lower than min power configured in smart-rf profile	
WING-39372	SPR-3670: Cfgd Stats pull for arp, mac-address, ntp, and dhcp-vendor option from NSM not working	Unable to reproduce in-house.
WING-38907	SPR-3633: AP7602 interface ge2 auto negotiation failed with same platform	
WING-38586	AP7632: high CPU usage on wipsd process when sensor is on	
WING-39440	SPR-3674 AP7662 panics in MCX deployment	
WING-42039	AP75xx: 'service pktcap on interface radio 1/2' display wrong channel info	
WING-39040	SPR-3646: Framed-MTU size is not honored when proxying through controller	
WING-39196	show firewall neighbors snoop-table does not give any output for ipv6 on AP8533VC . Works fine on NX9600	
WING-42041	5.9.7.0:rest-api-user roles:Post rest api request should not have access for rest-api-user	

6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

GLOBAL SUPPORT:

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.