

WiNG 5.9.1.0-29R Release Notes

Overview	1
1. Platforms Supported	1
2. New Features in WiNG 5.9.1	3
3. General Information for Firmware Upgrade / Downgrade	5
3.1 Device Upgrade/Downgrade matrix.....	5
3.2 Device Upgrade/Downgrade Procedure	7
3.3 AutoInstall	7
4. Firmware Upgrade / Downgrade – Controllers	10
4.1 Platform Important notes	10
4.2 Device Upgrade Options.....	11
4.3 Auto Upgrade.....	11
5. Firmware Upgrade/Downgrade – Independent APs	12
5.1 Platform Important Notes on Upgrade / Downgrade	12
6. Upgrade / Downgrade - NSight, ExtremeGuest and Captive Portal	13
6.1 Important Notes on Upgrade – ExtremeGuest	13
6.2 Important Notes on Upgrade – NSight and Integrated WiNG Captive Portal.....	13
6.3 Important Notes on Downgrade – NSight and Integrated WiNG Captive Portal.....	15
7. Important Notes	15
8. DFS Tables, Sensor and Radio Share	33
9. Vulnerability updates	35
10. Issues Fixed	37
11. Known Issues	39

Overview

WiNG 5.9.1 is a minor release that continues to build on the innovative WiNG 5 architecture across 802.11n and 802.11ac Enterprise WLAN portfolio. WiNG 5.9.1 introduces support for new AP platforms – AP 7632, AP 7662, and AP 7612. The release also merges the AP 7622 and AP 7602 support into the WiNG 5.9.1 baseline.

In addition, WiNG 5.9.1 release includes several new feature enhancements and critical customer fixes.

1. Platforms Supported

Dependent AP platforms – AP 621, 622, 650 are EOL and engineering support has ended. No new images will be released or supported for those platforms.

AP 6511, AP 6511E, AP 7131, AP 7181, AP 8222, ES 6510 are EOL and engineering support has ended. No new images will be released or supported for those platforms.

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

WiNG 5.9.1 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.

AP 7161 image is now called AP7161-<version>.img and not AP71XX-<version>.img as in previous releases.

AP 8232 image is now called AP8232-<version>.img and not AP82XX-<version>.img as in previous releases.

Note:

APXXXX-LEAN-5.9.1.0-29R.img - built **without GUI component**. AP lean images are also bundled within controller full image.

NXXXXX-LEAN-5.9.1.0-29R.img – built **without AP images**.

WiNG 5.9.1 supports the following platforms with the corresponding firmware images:

Controller Platform	Firmware Image
RFS 4010	RFS4000-5.9.1.0-29R.img, RFS4000-LEAN-5.9.1.0-29R.img
RFS 6000	RFS6000-5.9.1.0-29R.img, RFS6000-LEAN-5.9.1.0-29R.img
NX 9500/ NX 9510	NX9500-5.9.1.0-29R.img, NX9500-LEAN-5.9.1.0-29R.img
NX 9600 / NX 9610	NX9600-5.9.1.0-29R.img, NX9600-LEAN-5.9.1.0-29R.img
NX 75XX	NX7500-5.9.1.0-29R.img, NX7500-LEAN-5.9.1.0-29R.img
NX 5500	NX5500-5.9.1.0-29R.img, NX5500-LEAN-5.9.1.0-29R.img

Virtual Platform	Firmware Image
VX 9000 ¹ —production iso/img image	VX9000-INSTALL-5.9.1.0-29R.iso, VX9000-5.9.1.0-29R.img, VX9000-LEAN-5.9.1.0-29R.img
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-5.9.1.0-29R.iso ²

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

²The 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.

WiNG Express Manager	Firmware Image
NX 5500E	NX5500E-5.9.1.0-29R.img
NX 7510E	NX7500E-5.9.1.0-29R.img
VX 9000E	VX9000E-INSTALL-5.9.1.0-029R.iso

AP Platforms	Firmware Image
AP 6521 / AP 6521E	AP6521-5.9.1.0-29R.img AP6521-LEAN-5.9.1.0-29R.img (included in all Controller images)
AP 6522 / AP 6522E	AP6522-5.9.1.0-29R.img AP6522-LEAN-5.9.1.0-29R.img (included in all Controller images)
AP 6532	AP6532-5.9.1.0-29R.img AP6532-LEAN-5.9.1.0-29R.img ³ (included in all Controller images)
AP 6562 / AP 6562E	AP6562-5.9.1.0-29R.img AP6562-LEAN-5.9.1.0-29R.img (included in all Controller images)
AP7161	AP7161-5.9.1.0-29R.img AP7161-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7532	AP7532-5.9.1.0-29R.img

	AP7532-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7522	AP7522-5.9.1.0-29R.img AP7522-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7522E	AP7522E-5.9.1.0-29R.img (included in the express controller images)
AP 7562	AP7562-5.9.1.0-29R.img AP7562-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7502 / AP 7502E	AP7502-5.9.1.0-29R.img AP7502-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 8132 / AP 8122 / AP 8163	AP81XX-5.9.1.0-29R.img AP81XX-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 8232	AP8232-5.9.1.0-29R.img AP8232-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 8533	AP8533-5.9.1.0-29R.img AP8533-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 8432	AP8432-5.9.1.0-29R.img AP8432-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7602	AP7602-5.9.1.0-29R.img AP7602-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7622	AP7622-5.9.1.0-29R.img AP7622-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7612	AP7612-5.9.1.0-29R.img AP7612-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7632	AP7632-5.9.1.0-29R.img AP7632-LEAN-5.9.1.0-29R.img (included in all NX controller images)
AP 7662	Image will be released post WiNG 5.9.1 release

2. New Features in WiNG 5.9.1

New AP platforms:

AP 7632

The AP 7632 external and internal antenna Access Points are mid-tier products for dependable and efficient network performance. The AP 7632 is a dual radio Wave 2 802.11ac Access with a built-in IoT radio that supports Bluetooth® Low Energy (BLE) v4.2 radio technology, and is IEEE 802.15.4 compliant. Available in two form factors to meet high aesthetics use case and flexible high temperature use cases. The AP 7632i (internal antenna) features a durable low profile polycarbonate enclosure and four distinct mounting options. The AP 7632e (external antenna) features an all metal enclosure and internal circuitry to extend the operating temperature from -20°C to 60°C; ideal for maximum range and performance in demanding industrial applications.

AP 7662

The AP 7662 is designed for installation in harsh environments; from hurricane force winds to sub-zero temperature. The AP 7662 Wave 2 802.11ac IP67 outdoor rated access point extends the ExtremeWireless WiNG enterprise grade wireless coverage outdoors in a sleek form factor that is easy to install against an exterior wall, or mount on a pole. AP 7662 is a dual radio 802.11a/b/g/n/ac, fully compatible with every wireless device from legacy 802.11abgn devices up to the newest 802.11ac MU-MIMO smartphones. Available in two form factors to meet different deployment use cases. The AP 7662i (internal antenna) features an IP67 outdoor rated enclosure with three distinct mounting options for easy installation. The AP 7662e (external antenna) features an outdoor rated IP67 enclosure and internal circuitry to extend the operating temperature from -40C to 70C; ideal for maximum range and performance in demanding industrial applications.

AP 7612

The AP 7612 is Wave 2 802.11ac, enterprise-grade wall plate designed for hospitality market with one enterprise-grade access point per guest room. The AP 7612 is a dual radio Wave 2 802.11ac Access with a built-in radio that supports Bluetooth® Low Energy (BLE) v4.2. This surprisingly small AP is rich in functionality that can differentiate your business. The AP 7612 is so ingeniously designed that it can be installed in minutes.

AP 7622

The 7622 is a small form factor ceiling mount 802.11AC access point with internal omni-directional antennas. The 7622 includes an integrated BT2.0 and BLE radio, along with a multi-mode 802.11 radio. The 7622 supports dual band 1x1:1 or single band 2x2:2 MIMO.

AP 7602

The 7602 is a wedge shaped Wallplate 802.11AC access point. The internal antennas provide horizontal gain in the front of the AP. The 7602 includes an integrated BT2.0 and BLE radio, along with a multi-mode 802.11 radio. The 7602 supports dual band 1x1:1 or single band 2x2:2 MIMO.

ExtremeGuest

WiNG 5.9.1 adds:

- Built-in, default Splash templates for various onboarding workflows supporting instantaneous solution roll-out.
- Ability to view all blocked users count and list from Monitor->users section.
- Option to unblock a blocked user; unblock operation can be performed from the Active user's grid.
- Preserves user grid view preferences across the login session.
- Report Enhancements –
 - a. User's report is enhanced to provide the user walk-in trend chart.
 - b. Visit history report includes user's gender, source, email.

NSight

Added new widget to show "Downlink/Uplink Throughput" statistics for APs and clients.

Virtual Controller (VC) Enhancements

Heterogeneous AP management

Adds support on the Virtual Controller (VC) AP to manage heterogeneous AP models for the 802.11ac AP platforms.

The following AP models can be deployed in a heterogenous AP VC scenario:

AP 8533

AP 8432

AP 7632/AP 7662/AP 7612

AP 7622/AP7602

AP 7532/AP 7522/AP 7562

Following are the supported adoption hierarchy:

- AP 7662/7632 can adopt AP 7662/7632/7612
- AP 8533/8432 can adopt AP 8533/8432/7562/7532/7522/7662/7632/7622/7612/7602
- AP7532/AP7522/AP7562 can be managed by AP8533/AP8432 but not by AP7632/AP7662

Note:

- Image upload capability will only be enabled on the AP that is elected as VC
- VC can manage up to 64 APs

AVC DPI Engine Upgrade

Application Visibility DPI engine on the supported APs upgraded to a newer version 17.03.17.

Additional Enhancements

Dynamic Mesh: Adds dynamic mesh selection (root/non-root) capability to AP 7562 (available in legacy AP 7161 and AP 8163) to support changing configuration environments.

Client Bridge Scalability: Client Bridge scalability on AP 7532/7522/7562/7602/7622 has been extended to support up to 64 clients (older releases supported 14 clients).

RFDM Scalability: RF-Domain Manager scalability on AP 8533/8432/7632, selected as RFDM manager, has been extended to support up to 256 devices, 4096 clients.

Aeroscout (RTLS) tag support: Adds Aeroscout (RTLS) Tag support on AP 7532/7522/7562/7622/8533/8432

Bonjour Enhancement: Adds option to Bonjour advertisement (discovery policy) to include instance name along with the service.

Fast-Termination: Adds support for fast-termination on AP 7532 and AP 8432, to work in conjunction with ADSP Sensor functionality. Please refer to ADSP release notes for compatibility.

Elastic Storage support for NSight, ExtremeGuest: Ability to dynamically allocate storage after the initial configuration of VX (NSight, ExtremeGuest) without having to repartition the disk.

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 6521	v5.2 onwards	v5.2 onwards	AP 6521 image is contained within the controller image
AP 6522	v5.4 onwards	v5.4 onwards	AP 6522 image is contained within the controller image
AP 6562	v5.4.4 onwards	v5.4.4 onwards	AP 6562 image is contained within the controller image

Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
AP 6532	v5.1 onwards	v5.1 onwards	AP 6532 image is contained within the controller image
AP 7161	v5.1.1, v5.1.4, v5.2 onwards	v5.1.1, v5.1.4, v5.2 onwards	
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
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 8122	v5.5.2 onwards	v5.5.2 onwards	AP 8122 image is not within the RFS controller image but is contained within NX controller image
AP 8132	v5.2.6, 5.4.2 onwards	v5.2.6, 5.4.2 onwards	AP 8132 image is not within the RFS controller image but is contained within NX controller image
AP 8163	v5.6 onwards	v5.6 onwards	AP 8163 images are not within the controller image
AP 8232	v5.5.3 onwards	v5.5.3 onwards	AP 8232 image is not within the RFS controller image but is contained within NX 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	
RFS 6000	v5.0 onwards	v5.0 onwards	
NX 5500	v5.8 onwards	v5.8 onwards	NX 5500 is supported starting with v5.8

Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
NX 75XX	v5.5.2 onwards	v5.5.2 onwards	Note: WiNG 5.6 doesn't support NX 7500.
NX 7510E/VX 9000E/NX 5500E / AP 6521E / AP 6522E / AP 6562E / AP 7502E / AP 7522E	v5.5.3 onwards	-	NX 7510E and VX 9000E are supported starting with v5.7 NX 5500E is supported starting with v5.8
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 your 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.
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
- WingRFS.RFS6000
- WingNX.NX7500
- WingNX.NX9000
- WingNX.VX

AP:

- WingAP.AP6521
- WingAP.AP6522
- WingAP.AP6562
- WingAP.AP6532
- WingAP.AP7161
- WingAP.AP7502
- WingAP.AP7522
- WingAP.AP7532
- WingAP.AP7562
- WingAP.AP7602
- WingAP.AP7612
- WingAP.AP7622
- WingAP.AP7632
- WingAP.AP7662
- WingAP.AP8132
- WingAP.AP8122
- WingAP.AP8232
- WingAP.AP8163
- WingAP.AP8533
- WingAP.AP8432

3.3 General Important Notes on Upgrade / Downgrade

1. Recommend using Controller LEAN images for HM deployments and only upload AP/controller images needed for the deployment.
2. WiNG 5.9.0 release extends the number of DNS ACL rules support from 10 to 64. When downgrading the AP from v5.9.0 to a prior release, all DNS ACL rules are forcefully removed to maintain backward compatibility. User needs to re-configure the DNS ACL rules after the downgrade.
3. WiNG 5.9.0 enables support to configure EU country codes on WR SKU.
- 3 Application Visibility / DPI Engine – Downgrading to an older version from WiNG 5.9.0 will lead to loss of configuration that contains new application and protocol names introduced with the new DPI engine in WiNG 5.9.0. Configuration containing application and/or protocol names that are available in both WiNG 5.9.0 and prior versions will be preserved upon downgrade.
- 4 WiNG 5.8.4 introduced NTP Server string alias configuration. When downgrading from 5.8.4 or above to an earlier WiNG release and NTP server string alias is configured, for example:

```
alias string $NTP-HOST <string>  
ntp server NTP-HOST
```

the string alias configuration needs to be removed before going through the downgrade operation:

```
no ntp server $NTP-HOST  
no alias string $NTP-HOST <string>  
commit write
```


- 5 With WiNG 5.8.4, the length of logout FQDN and localization FQDN configuration in captive portal has changed from 256 to 128 characters. When upgrading to WiNG 5.8.4 or above from previous releases, if the logout and/or localization FQDN is longer than 128, then a reconfiguration with lower character length is required.
- 6 WiNG 5.8.4 introduced 'vlan' keyword to the DNS critical resource-monitoring configuration. When upgrading to 5.8.4 or above from an earlier WiNG release and DNS critical resource-monitoring is configured, for example:
critical-resource dn monitor-using-flows any dns A.B.C.D/M
the DNS critical resource-monitoring configuration needs to be removed before going through the upgrade and reconfigured with the 'vlan' option after the upgrade:
critical-resource dn monitor-using-flows any dns vlan <1-4094> | A.B.C.D/M
- 7 DHCP Vendor Class changes:
DHCP Vendor Class Identifier has been changed in WiNG 5.7.1 and later to use "Wing", e.g. WingAP.AP7532, WingAP8132, WingRFS.RFS4000 and etc.
Note: DHCP vendor class should be modified on DHCP servers prior to upgrading APs.
- 8 When downgrading from WiNG 5.7.2 (or newer) to WiNG 5.7.1 (or older), the SNMP trap host configuration will need to be re-applied due to the newly introduced encrypted community string option.
v5.7.2 (or newer):
*(config-management-policy-default)#snmp-server host 1.1.1.1 v2c community ?
0 Enter a clear text trap community name
1 Enter an encrypted trap community name
WORD Enter Trap Community Name*
v5.7.1 (or older):
*(config-management-policy-default)#snmp-server host 1.1.1.1 v2c community ?
WORD Enter Trap Community Name*
- 9 Prior to upgrading to WiNG 5.7.1 or above if you have Onboard-Radius Server with LDAP Authentication configured, please note the following:
"(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" – is not supported.
"(sAMAccountName=%{Stripped-User-Name})" – is supported.
Configurations using "(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" need to be updated to "(sAMAccountName=%{Stripped-User-Name})" prior to performing the upgrade process.
- 10 When downgrading from WiNG 5.8.x to a version prior to WING 5.4.x through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
device-upgrade rf-domain <RF domain name> all no-reboot ... this downgrades all APs (including the RF domain manager) without rebooting them
reload on <RF domain name> ... this reboots the entire RF domain.
Staggered reboot option is not supported in this downgrade scenario.
- 11 Customers upgrading from an earlier WiNG 5 release not requiring ONEVIEW, the procedure is the same as before.
Customers using ONEVIEW in WiNG 5.5, please see the WiNG 5.5 training for details of upgrade/downgrade. **Note the use of the "Lean Controller image" which does not include AP images** – since the controller image size is now significantly larger than WiNG 5.4.x release.

- 12 In Virtual Controller deployments, APs running version 5.4.x will not adopt to a virtual controller running WiNG v5.8. First upgrade APs to WiNG v5.8 (manually) and then upgrade the Virtual Controller. New APs need to be upgraded to 5.5.x manually before connecting to a WiNG 5.8 Virtual Controller network.
- 13 Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

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 processAfter 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.

4.2 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. When downgrading AP 8132 from v5.8.4 or above to an earlier release, the Bluetooth settings in "interface bluetooth 1" are not translated into a value for the deprecated setting "bluetooth-detection". Instead, the downgraded config just uses the default, which is "no bluetooth-detection".
 - b. 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.
 - c. 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 6532:
 - a. WiNG 5.8.2 and above - Upgrading AP 6532
 - WiNG 5.8.2 and above mitigates AP 6532 image size issue by introducing 2 different images:
 - *AP6532-LEAN-5.9.1.0-29R.img*: built without the GUI component and is included in the controller images
 - *AP6532-5.9.1.0-29R.img*: standard image, however without the GUI help files, for independent APs that require GUI support.
 - Standalone/Independent AP deployment:
 - AP can be upgraded using *AP6532-5.9.1.0-29R.img* image. However, AP must be upgraded to a version WiNG 5.5.4 or above prior to upgrading to WiNG 5.8.2
 - Once upgraded, if the non-active (Secondary) flash partition has image version prior to WiNG 5.7.2, load *AP6532-5.9.1.0-29R.img* image to the partition

- b. Upgrade for AP 6532 from a release prior to v5.2.13 directly to v5.4.x or later is NOT seamless and requires additional steps. AP should first be updated to WiNG 5.2.13 image.
- 5. 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 these support the new NAND, but previous versions do not.

6. Upgrade / Downgrade - NSight, ExtremeGuest and Captive Portal

6.1 Important Notes on Upgrade – ExtremeGuest

- 1. Upgrade of integrated WiNG Captive Portal solution to ExtremeGuest solution is not supported.
- 2. Upgrading from WiNG 5.9.0 and upwards - ExtremeGuest
 - a. Upgrade all ExtremeGuest devices to new firmware using the upgrade command. DO NOT reboot the devices.
 - b. Reboot the Arbiter and wait for the device to come up and join the replica-set.
 - c. Disable ExtremeGuest server on primary replica-set member:

```
Primary #self
Enter configuration commands, one per line. End with CNTL/Z.
Primary (config-device-00-0C-29-35-AE-F6)#no eguest-server
Primary (config-device-00-0C-29-35-AE-F6)#comm wr
Primary (config-device-00-0C-29-35-AE-F6)#end
```

- d. Reboot the primary replica-set member and wait for the device to come up and join the replica-set. Make sure that the replica-set is up. Use the below-mentioned command to verify:

```
Primary#sh database status
-----
MEMBER          STATE          ONLINE TIME
-----
192.168.210.200* PRIMARY        0 hours 2 min 17 sec
192.168.210.201 SECONDARY      15 hours 15 min 53 sec
192.168.210.203 ARBITER        15 hours 47 min 16 sec
-----
```

[*] indicates this device.

- e. Enable ExtremeGuest Server on primary replica-set member:

```
Primary #self
Enter configuration commands, one per line. End with CNTL/Z.
Primary (config-device-00-0C-29-35-AE-F6)#eguest-server
Primary (config-device-00-0C-29-35-AE-F6)#comm wr
Primary (config-device-00-0C-29-35-AE-F6)#end
```
- f. Repeat steps (c) to (e) for Secondary member of replica-set.

6.2 Important Notes on Upgrade – NSight and Integrated WiNG Captive Portal

- 1. Upgrading from WiNG 5.8.2 and upwards - NSight

- a. Upgrade all devices to new firmware using the upgrade command. DO NOT reboot the devices.
- b. Reboot the Arbiter and wait for the device to come up and join the replica-set.
- c. Disable NSight-server on primary replica-set member:

```
Primary #self
Enter configuration commands, one per line. End with CNTL/Z.
Primary (config-device-00-0C-29-35-AE-F6)#no use nsight-policy
Primary (config-device-00-0C-29-35-AE-F6)#comm wr
Primary (config-device-00-0C-29-35-AE-F6)#end
```

- d. Reboot the primary replica-set member and wait for the device to come up and join the replica-set. Make sure that the replica-set is up. Use the below-mentioned command to verify:

```
Primary#sh database status
-----
MEMBER          STATE          ONLINE TIME
-----
192.168.210.200* PRIMARY        0 hours 2 min 17 sec
192.168.210.201 SECONDARY      15 hours 15 min 53 sec
192.168.210.203 ARBITER        15 hours 47 min 16 sec
-----
```

[*] indicates this device.

- e. Enable NSight-server on primary replica-set member:

```
Primary #self
Enter configuration commands, one per line. End with CNTL/Z.
Primary (config-device-00-0C-29-35-AE-F6)#use nsight-policy <nsight-policy>
Primary (config-device-00-0C-29-35-AE-F6)#comm wr
Primary (config-device-00-0C-29-35-AE-F6)#end
```
- f. Repeat steps (c) to (e) for Secondary member of replica-set.

2. Upgrading from 5.8.0/5.8.1 to WiNG 5.8.2 or later

The database file definitions for NSight and Captive Portal in WiNG 5.8.2 have been changed:

- There is no portability of NSight data from the earlier versions (WiNG 5.8.0 and WiNG 5.8.1). In the case of needing to downgrade to WiNG 5.8.0 or WiNG 5.8.1, the user must do a database backup before upgrading to WiNG 5.8.2 or later.
- For Captive Portal data, the user must do a database backup (export using JSON format) from the earlier versions (WiNG 5.8.0 and WiNG 5.8.1) before upgrading to WiNG 5.8.2, and can be imported after the upgrade.

The following are upgrade steps for NX 7500, NX 9500 and NX 9600 (please refer WiNG 5.8.1 notes and ensure NX 9600 is configured for RAID10):

- o Load WiNG 5.8.2 or later image on to the device using upgrade and reload commands:

```
Upgrade tftp://<server-ip-address>/NX9XXX-5.8.2.0-030R.img
```
- o After the device reloaded and prompt appears, execute the following commands. The device will reload after the last command:

```
service database server stop
service database remove-all-files
All database files will be removed, do you want to continue? (y/n): y
```

VX 9000 requires re-install using the VX9000-INSTALL-5.9.1.0-29R.ISO image due to 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 configuration from backup

6.3 Important Notes on Downgrade – NSight and Integrated WiNG Captive Portal

1. When downgrading from WiNG 5.8.4 to earlier versions of WiNG and a database replica-set is configured, the replica-set configuration must be removed before downgrading on all members of the replica-set.
 - On each member of the replica-set, remove the database-policy

```
self
no use database-policy
commit write
```
 - Commit the changes. Once 'show database status' on all the devices show database is not enabled, reload each device into the new downgraded version.
 - After the devices reload, reapply the database-policy with the replica-set configuration to bring up the replica-set

```
self
use database-policy <replicat-set>
commit write
```
2. When downgrading from WiNG 5.8.2 to prior versions, following are the downgrade steps needed for NX 7500 (for Captive Portal), NX 9500, NX 9600 and VX 9000, if NSight or Captive portal are enabled
 - Backup the database for any future use
 - Load the required image version on to the device using upgrade and additional commands listed below:

```
upgrade tftp://<server-ip-address>/<filename>
no use nsight-policy (Needed only if NSight was enabled)
commit write
service database server stop
service database remove-all-files
All database files will be removed; do you want to continue? (y/n): y
```
 - After the device reloads, restore the captive portal database, and the device is ready for deployment.

7. Important Notes

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 includes 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:
 - o Chrome – ver 56.0.2924.87 (64-bit) or later.
 - o 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 'impact-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 YearNSight 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 I2 tunnel broadcast optimization.
I2-tunnel-forward-additional-packet-types ?
wnmp Forward WNMP packets across I2 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 it 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.
14. If using SNMP alias password in WiNG 5.8.6 and need to downgrade to prior versions, first remove new SNMP configuration.
15. NSight UI: Rogue AP changes:
 - a. Friendly Rouge AP column was removed
 - b. Renamed the column "Interfering Rogue AP" to "Inactive Rogue AP".
 - c. Scroll bar was added to show all reporting APs.
16. AP 7502 MCX support for 2.4 radio
AP 7502 MCX support for 2.4 radio only was implemented in WiNG 5.8.4 as Beta feature. WiNG 5.8.6 has finished validating the solution

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. NX9500 image change – instead of previously used NX9000-<version>.img – image was renamed to NX9500-<version>.img.
3. 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.
4. 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).
5. 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.
6. 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'
7. 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.
8. To prevent gateways being marked as clients - mac-address-table detect-gateways default changed to enabled.
9. "show cluster history" command was added in this release.

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 also 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. WiNG NSight – please refer to “NSight Deployment guide” posted on Support site under product manuals.
2. 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.
3. VX 9000 - Not supported on Amazon instance type C4 due to kernel limitation.
4. 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
5. SWIFT UI: Adoption mode under basic settings will take effect with pressing commit button twice.
6. Import running configuration function is supported only through the CLI.

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. WiNG 5.8.1 adds GUI support for PSK key overrides per rf-domain.
5. 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.
6. If the CLI command - "upgrade <URL> on <device-name>" is being used, then please note it has been changed to "upgrade <URL> <device-name ...>".
7. 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. Centralized EX-3500 switch management
 - User must add VLAN to the VLAN database before assigning VLAN to a port
 - While configuring processor/memory threshold commands from a centralized NX/VX controller, the falling threshold must be set prior to rising the threshold.
 - Switch port VLAN configurations may not get configured properly after the controller reload operation
- 10. The commit warning pop-up message will appear when VPN step-by-step wizard is selected to ensure the previous config changes are saved.
- 11. WiNG Express
 - Express Manager, NX 5500E, comes preloaded (default) with 128 Express AP adoption licenses.
 - The preloaded adoption licenses on the existing Express Manager platforms, VX 9000E and NX 7510E, has been changed from 64 to 128 starting with WiNG 5.8.
- 12. To operate Cisco phones with AP 7532, the interface radio settings should include dynamic-chain-selection strict
- 13. Captive Portal: OAUTH may not work properly with Lumina phone running older Windows version (< 8.1). Please upgrade Lumina phones to latest OS.
- 14. 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 v5.7.2

1. WiNG 5.7.2 includes performance improvements for AP 7532/7522 when connected to 3af power source.
2. Added support for host alias for critical-resource ip-address that user can define on AP device or Profile context.
3. WiNG 5.7.2 adds NAND fixes and new bit error correction algorithm for AP 650/6532 to reduce potential flash corruption issues.
4. WiNG 5.7.2 validated VMM support on AP 7562.

New in v5.7.1

1. AP 622, 6522, 6562 - Default value for radio lna control on 2.4GHz has been changed to improve receive sensitivity and range in low/medium AP density environments.
2. DHCP Vendor Class Identifier has been changed use "Wing", e.g. WingAP.AP7532, WingAP8132, WingRFS.RFS4000 etc.
3. Captive Portal internal web-page templates are enhanced for mobile-friendly rendering. Existing WiNG5.x deployments using internally hosted web-pages for captive portal will

automatically get this functionality on upgrading to WiNG5.7.1. Please note that there will be slight changes to pages – page style, background color, font color etc.

4. AP 7562 sensor functionality will be supported in later ADSP release.

New in v5.7.0

1. FIPS: Encrypted parts of the configuration are lost when downgrading from WiNG 5.7.
Workaround:
 - disable password encryption before the downgrade `#no password-encryption secret 2 <password>`
 - perform the downgrade
 - enable password encryption `#password-encryption secret 2 <password>`
2. '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.
3. The AP 6521 will include support for configuration and management of the on-board AAA server in the HTTP User Interface. This UI is found on the standard WiNG OS for the AP 6521, and the AP 6521 Express. Please note that the Virtual Controller function will be disabled when the on-board AAA server is enabled on a standalone AP 6521. To use the Virtual Controller function, you must disable the on-board AAA server.
4. Web Filtering:
 - URLs in custom category will get priority over standard/predefined category irrespective of precedence configured
 - Web Filtering is not supported on the NX65xx/NX45xx platforms
5. Wired captive portal – to support clients with MAC authentication, 802.1x configuration is also required for the controller
6. 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"
7. WiNG Express Manager
 - a. Express Manager (NX 7510E) can be accessed using default IP 192.168.0.1 and 'admin' is the supported user role.
 - b. Smart-RF is enabled by default with channel override capabilities on individual APs. Any Smart-RF channel list change will take effect after the device reboot.
 - c. RADIUS services will not be supported on AP 6511 and AP 6521.
 - d. DHCP service should be started at the site-level and APs have to adopted to the Express Manager before starting the DHCP service.
 - e. VLAN 1 and 2200 are reserved VLANs – they are not available for user configuration
 - f. GUI will be supported on the following browsers/version
 - i. IE10 and above
 - ii. Chrome
 - iii. Firefox
 - g. The country code should be configured at the site-level for the AP radios to function.

- h. The auto-provisioning policy must be created before adopting APs to a site. Express Manager needs to be reloaded for any changes to the auto-provisioning policy to take effect.
 - i. Event history page may experience slow to refresh when the event table size is large
 - j. Default profile configuration (inherited from the system) can be modified at the site-level, however, needs manual reconfiguration to revert to defaults
 - k. Disable DFS checkbox under Advanced Smart-RF tab removes DFS channels from the available channel list
 - l. Floor maps should be loaded independently on the standby in a cluster scenario
 - m. Firmware upgrade for the Express Manager should be administered through the System basic configuration screen. Upgrading through the devices screen is not supported.
 - n. Access to the NX 7510E USB port is not available from the Express Manager UI
 - o. There is no periodic auto-refresh for the UI charts, tables, and map. Needs manual page refresh using refresh button.
 - p. Site icon can be removed from the Dashboard map only after the corresponding site profile has been deleted from the system.
 - q. AP upgrade status is shown on the Active Express Manager while the upgrade is initiated from the Standby in a cluster setup
 - r. Site connectivity to the Express Manager needs to be active for the mac-registration feature to function.
 - s. For infinite lease option on the DHCP pool configuration, the user needs to set "0" for the day, hours and minutes.
8. 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
9. 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 |
10. AP 6522/6532/6562/7161 - VRRP and OSPF feature support have been removed

New in v5.6.x

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.

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. Dataplane support does not work correctly with Microsoft HyperV. It works fine with other supported hypervisors.

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).

eBGP Scaling by platform is as follows:

- RFS 4000/RFS 6000 – 6000 routes
- NX 9510 – 9000 routes
- NX 4500/NX 6500 – 12 routes

T5 adoption – https must be enabled on the WiNG controller for T5 adoption to work

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.

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 v5.5.6

1. Currently, for all events, forward-to-switch is on by default. Due to this setting, a controller adopting many APs gets too many events sometimes. So for certain events, the forward-to-switch

setting will be off by default. This will apply whether event-system-policy is used or not. The events being changed are:

"dot11 client-associated", "dot11 client-disassociated", and "dot11 client-info".

2. Flow control on AP 6511 has been disabled to prevent transmission and receive of pause packets.
3. AP discovery tool will work on windows 7 laptop only with static IP.

New in v5.5.5

1. When upgrading to WiNG 5.5.5 – AP statistics will not be available on the controller until APs have also been upgraded to WiNG 5.5.5.
2. CPLD images on AP 7131/7161/7181 have been updated. AP 7131N CPLD image is without change.
3. “No service” page for captive portal enhancements:
WiNG 5.5 has introduced support for “no service” page support. However - the failure page was ONLY displayed if the Access Point (or Wireless Client) can reach a DNS server. WiNG 5.5.5 addresses the issue with DNS reachability and provides option to configure "service monitor dns crm <crm-name> vlan <failover-vlan>". This service command will monitor DNS server reachability. When DNS server is not reachable, the clients are moved to failover-vlan. In the failover-vlan every time DNS request comes from captive portal clients, they are redirected to No-service page since DNS server is not reachable.
In the case of extended VLAN, CRM for service monitor should be configured on the controller with sync-adoptees option. Any CRM state changes would be forwarded to the adopted devices which would redirect the wireless clients on the WLAN to the no-service page in case the monitored CRM is down.
4. AP 622/6522/6562 enhancement for radio 1.
New configuration option added to improve Rx sensitivity of Radio 1 (2.4GHz) on AP622/AP6522/AP6562 platform. Useful for deployments with low AP density, high ceilings (warehouses), VOIP services etc.
Under radio configuration (profile/device → interface radio 1): “*service radio-lna ms*”
Default is “*service radio-lna ang*”.
5. MCD devices with Jedi radios can have connectivity issues when 5.5 and 11 mbps 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.

New in v5.5.4

1. A new event was added to track down IP address of associated client. All events are enabled by default in the system.
Rfs4000(config-event-policy)#event dot11 client-info
2. One can now configure SNMP community strings for SNMP traps. Previously it was using default community string – public.
Rfs4000(config-management-policy-default)#snmp-server host <ip> <ver> <port>
changed to
Rfs4000(config-management-policy-default)##snmp-server host <ip> <ver> <port>

community ?

WORD Enter Trap Community Name

Host and Version are mandatory parameters while port (default 162) and community (default public) is optional parameters. Default community string is public.

New in v5.5.3

1. The command - "*device-upgrade load-image <image-type> URL*" changed to "*device-upgrade load-image <image-type> <URL> <on device or domain name>*". When on device or domain name is given then the image will be loaded on a remote device or RF domain manager respectively. If URL is missing, then the location of the image will be images loaded on the self device.
2. The command - "*show device-upgrade versions on rf-domain-manager*" changed to "*show device-upgrade versions on <device or domain name>*".
3. New web UI:
When using new web UI to configure Express SKU Aps – use of CLI at the same time is not recommended as it can lead to configuration corruption.
New web UI configuration can't be done though Nexus 7 chrome browser as all the fields are misplaced in UI.
4. Currently, device upgrade on multiple rf-domains does not work from NOC controller when the RFDs are all controller managed. Each domain needs to be upgraded separately.
5. Smart-rf calibration has been removed in this release.
6. NX 9xxx controller will not reboot correctly if USB flash drive is mounted. Please remove the USB when rebooting the controller.
7. 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.
8. WiNG 5.5.x release introduced an enhancement to learn the APs wired side connected port through CDP or LLDP packet processing, so the CDP packet flooding needs to be avoided to eliminate the excessive packet flooding from the APS to the controller.
9. WiNG 5.5.4 does NOT include support for ADSP unified mode for NX 7500 series.

New in v5.5.2

1. Change in behavior for "*show wireless xxxxx*" CLI commands and techsupport for centralized controller deployments:

For centralized controller deployments (multiple RF-Domains across distributed locations), all "*show wireless xxxxx*" commands will resolve only to the local rf-domain. This will prevent a "*show wireless xxxxx*" CLI command without any rf-domain specified or a techsupport dump operation initiated on the centralized controller from collecting statistics information from all the distributed locations (rf-domains). New mechanisms have been added to collect rf-domain specific statistics individually or globally.

2. New Display Mode in the CLI to view RF-Domain specific or global (across all rf-domains) wireless statistics:

From the CLI (in EXEC mode/privileged EXEC mode):

"*on rf-domain <rf-domain_name>*" sets the display mode for wireless statistics to show commands to resolve to a particular rf-domain, all "*show wireless xxxxx*" commands executed in this mode will automatically return the output corresponding to that rf-domain without the user specifying the "*on <rf-domain_name>*" extension to every command.

"*on rf-domain all*" sets the display mode for wireless statistics to show commands to run in global mode – i.e. for each "*show wireless xxxxx*" command that you run, the controller will display statistics across all rf-domains.

3. Ability to generate wireless stats summary report on a per rf-domain basis or globally (across all rf-domains):

From the CLI (in privileged EXEC mode) –

```
"service copy stats-report rf-domain <rf-domain-name> <URL>"
```

```
"service copy stats-report global <URL>"
```

Note: The above option could be utilized for generating inventory/reporting at a system level.

4. **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 is capable of supporting only TKIP encryption, they are required 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; wlangs 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 wlangs 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.
5. Change in terminology for adoption/upgrade related action commands/events/traps:
With WiNG 5.5 One View deployment scenarios supporting controllers to be adopted and managed by a centralized controller cluster, existing "ap-xxxx" action commands have been replaced with "device-xxxx" action commands. For example: ap-upgrade xxxx will now be referred to as device-upgrade xxxx.
All adoption related events and traps are modified to reflect the "device" terminology instead of "ap".
 6. 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.
 7. 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.

New in v5.5.1

1. NIST SP 800-131A regulation made 1028 bit certificates obsolete as of January 1, 2014. All self-signed on-board certificates which are 1028 bits will be regenerated upon upgrade. Customers need to upgrade all third party certificates to be compliant with new regulations.
2. "show global domain managers" will show incorrect values for the number of APs if the domain has APs on the version below WiNG 5.5.

New in v5.5.x

1. 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.
2. 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.
3. WiNG 5.5 extended L2tpv3 support for AP 6521, AP 621 and AP 6511. In addition, on configuring l2tpv3 settings on those APs – following is required to be set in AP profile for l2tpv3 to work – “service l2tpv3 enable”.
4. 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
5. 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.
6. **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 strings.
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.

New in v5.4.x

1. 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”.
2. ADSP SA cannot be run through a mesh with AP7131N tri-radio; non-root AP has 3rd radio as sensor
3. 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.
4. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.
5. MCX max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where the range is 24km.
6. It's recommended disabling IP DoS attacks in firewall policy when configuring IGMP snooping.

7. 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.
8. There is a single profile for AP71XX. However, for AP 7161 placement is set to "outdoor" at the device level. So even though the profile in the controller doesn't have the "outdoor" setting, when the configuration is pushed to the AP, the outdoor placement is automatically enforced.
9. On low memory APs, when adopted by a controller, the GUI is disabled, to make the memory available for other core functions such as additional mint routes. It is assumed that when an AP is adopted to a controller the controllers' GUI will be used for its configuration. To re-enable the GUI on these APs - use the "memory profile" parameter.

If APs are already separated from the controller:

- Connect to AP CLI.
- Set memory profile to 'standalone' under device override or profile context.

If APs are adopted to controller then memory profile configuration change can be applied from controller CLI:

- Connect to Controller CLI.
- Set memory profile to 'standalone' under AP profile context.

Changing the memory profile reboots the AP which then comes up with GUI.

e.g. CONTROLLER(config-profile-default-ap6511)#memory-profile (adopted | standalone).

From previous releases (prior to 5.4.0.0):

When using Juniper ex2200-24p-4g or related models when connecting WiNG Access Points – either disable IGMP snooping on the Juniper switches to ensure AP adoption or configure firewall policy filter that will allow the flow of traffic to specified destination-mac-address – 01:A0:F8:00:00/48.

If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gig E wired switch, please set link speed to 100 full, or user a GigE Power Injector.

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.

If using TFTP to upgrade an AP 6521 on the TFTP server please configure the following settings: Per packet timeout – 15 seconds and Maximum retries – 20.

When using iPods as clients, you may see WPA2 group key rotation handshake failures while MUs are idle (2.4GHz band). Change the handshake timeout to 2 sec to correct this problem. From the wlan config, the CLI command is: wpa-wpa2 handshake timeout X (where X is the timeout in ms, within a range of 10-5000)

Auto assign sensor is not available for AP 6521 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.

To safeguard against unknown attacks, it is recommended that management access is restricted to authorized hosts/subnets. This can be done using the restrict-mgmt-access host/subnet CLI command under management-policy.

When AP adopts to the Controller, the clock is not getting sync with controller clock immediately. It happens over a period of time depending on time delta.

8. DFS Tables, Sensor and Radio Share

1. Following is the DFS support in WiNG 5.9.1 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 6532	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 6521	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled
AP 6522 AP 6562	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled
AP 8132	Disabled	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled
AP 8122	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled	Disabled
AP 8163	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled	Enabled	Disabled
MOD-8132-6001S-WW	NA	NA	NA	NA	Enabled	Enabled	Enabled	Enabled
AP 8232	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	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	Disabled	Enabled	Enabled	Enabled	Disabled
AP 8432	Enabled	Enabled	Enabled	Disabled	Enabled	Enabled	Enabled	Disabled
AP 7602	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
AP 7622	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled	Enabled
AP 7612	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Enabled	Disabled
AP 7632	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Enabled	Disabled
AP 7662	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Enabled	Disabled

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:

Network Assurance Toolset when Radio is dedicated as a sensor	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Testing	Connectivity Testing
AP 6521 ¹	No	Yes	Yes	Yes	Yes	Yes
AP 6532	Yes	No	Yes	Yes	Yes	Yes
AP 6522/6562	No	Yes	Yes	Yes	Yes	Yes
AP 7161	Yes	No	Yes	Yes	Yes	Yes
AP 7532/7522/7562	No	Yes	Yes	Yes	Yes	Yes
AP 8132/8122	No	Yes	Yes	Yes	Yes	Yes
AP 8232	No	No	No	No	No	No
AP 7502	No	No	No	No	No	No
AP 8533 ²	No	Yes	No	Yes	Yes	Yes
AP 8432 ²	No	Yes	Yes	Yes	Yes	Yes
AP 7602	No	No	No	No	No	No
AP 7622	No	No	No	No	No	No
AP 7612	No	No	No	No	No	No
AP 7632	No	No	No	No	No	No
AP 7662	No	No	No	No	No	No

Notes:

¹GUI is disabled and the number of SSH sessions is limited to 1

²Support 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:

Network Assurance Toolset with Radio Share	Spectrum Analysis ²	Advanced Spectrum Analysis ³	Live RF	Live View	AP Testing	Connectivity Testing
AP 6521 ¹	No	Yes	Yes	Yes	Yes	Yes
AP 6532	No	No	Yes	Yes	Yes	Yes
AP 6522/6562	No	Yes	Yes	Yes	Yes	Yes
AP 7161	No	No	Yes	Yes	Yes	Yes
AP 7532/7522/7562	No	No	Yes	Yes	Yes	Yes
AP 8132/8122/8163	No	Yes	Yes	Yes	Yes	Yes
AP 8232	No	No	No	No	No	No
AP 7502	No	No	No	No	No	No
AP 8533	No	No	No	No	No	No
AP 8432	No	No	No	No	No	No
AP 7602	No	No	No	No	No	No
AP 7622	No	No	No	Yes	No	No
AP 7612	No	No	No	No	No	No
AP 7632	No	No	No	No	No	No

Network Assurance Toolset with Radio Share	Spectrum Analysis ²	Advanced Spectrum Analysis ³	Live RF	Live View	AP Testing	Connectivity Testing
AP 7662	No	No	No	No	No	No

Notes:

¹GUI is disabled when Radio Share is enabled.

²Spectrum Analysis is not supported with Radio share enabled.

³Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.

9. 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 5.9.1

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

10. Issues Fixed

Following issues have been fixed in WiNG 5.9.1 release:

SPR/CR	Description
SPR-3284	Multiple corruption panics on AP 7562 when configured for MCX and MCX-ACS feature
SPR-3294	AP 7161 fails to upgrade properly due to DDR timing issue
SPR-3315	AP 8533/7532 crash is seen when configured for sniffer redirect mode
SPR-3329	AP 7161: Antenna mode 1xALL causes rx.chainmask error message
SPR-3333	AP 8533 sensor device table full [fixed]; rogue client alarm goes from active to inactive
SPR-3334	DPI and application policy configuration missing after cfgd process restart on VX 9000
SPR-3337	Adoption gets into 'unknown' state when the site auto-provisioning rule has leading characters before rfd alias
SPR-3338	CLI guide has wrong statement in regards to AP7562 support of rate selections for opportunistic
SPR-3339	AP 7532/7522 Sensor panic at ECM_ThreadFunc while terminating clients
SPR-3341	Cannot upgrade VX9000E controllers to 5.9.0.x or later builds
SPR-3343	AP-7532-67030-IA SKUs have duplicate SNMP Engine ID – new CLI command added to reset SNMP engine ID.
SPR-3344	Descriptions for client bridge events not available on CLI guide
SPR-3345	Guest Registration DB is not updating with new clients
SPR-3347	Unable to modify default IP SNMP ACL
SPR-3348	NX 7500: unable to execute "service trace cfgd"
SPR-3350	AP 7502: MAC authentication not working on FE ports.
SPR-3352	Malformed MDNS response packet causes stack overflow and dpd2 crash in AP
SPR-3353	HSD core on captive-portal client session timeout
SPR-3354	AP 7522 configured as client bridge forwards masqueraded mac to wired client

SPR/CR	Description
SPR-3356	NSight: APs marked incorrectly as offline
SPR-3357	Secondary cluster member generates device offline event notifications
SPR-3358	On upgrading devices from v5.4.4 to v5.8.4 and above, the default trustpoint uses default key with invalid length - 1024
SPR-3359	Cannot set radio data rates to MCS3-Stream or MCS4-Stream for ANYAP profile
SPR-3360	AP 8432 cfgd core when "no led" command is executed
SPR-3361	AP stopped sending RSSI data to RTL Server after a period.
SPR-3362	GUI: Event history not ordering domains alphabetically and thus difficult to search
SPR-3363	SSM Core, Panic and low memory tech dump seen on AP 7532 when DPI metadata is enabled
SPR-3364	SSM process doesn't restart properly sometimes
SPR-3365	NSight GUI becomes unavailable due to a cursor leak in MongoDB
SPR-3368	wingStatsRfdWlWlanTable SNMP OID times out in large scale deployments – SNMP performance improvements implemented to streamline several SNMP tables.
SPR-3369	On AP 6562 probe table is getting full with MU expiration time showing wrong values and RIM CPU utilization is high
SPR-3371	Captive Portal: Password in CP voucher displayed as wing_supressed when password encryption enabled
WING-34349	GUI: Usability problem with app groups drop down for DPI – better search is needed to effectively find apps.
WING-34562	EGuest: Database Export send same routes multiple times
WING-34587	NSight: AP Test - AP Test should use a non-sensor AP only when any of the sensor APs is not the smart rf radio neighbor
WING-34739	Access point guide: Virtual controller adoption limit mentioned is incorrect
WING-34891	EUCLID: Wipisd cores seen on AP 6522/AP 7522 when the RSSI feeds for Euclid server is enabled
WING-34999	For HM deployment device-upgrade, when site controllers are not using auto-upgrade, device-upgrade for APs is not done if they are not adopted at time of upgrade trigger
WING-35014	EGuest: The active user page doesn't show the loyalty field to identify the loyalty app user
WING-35137	NSight: APTTest/ASA failure in Virtual Controller setup
WING-35192	Streamline RFD, NOC and device statistics to allow faster response for ADSP queries
WING-35193	NSight: App group widget does not display correct Tx/Rx or Count
WING-35196	EGuest: The device type widget not showing some device on y axis
WING-35197	Need to increase op log size and optimize the time taken to build the indexes
WING-35203	NSight: Client distribution by WLAN widget does not display Guest clients
WING-35219	EGuest: The "male" and "Male" are also treated different gender group in the user report

SPR/CR	Description
WING-35221	NSight: Dashboard widget - Client count filter with WLAN Query times out
WING-35229	EGuest: Database export fails if username contains @
WING-35269	NSight: UI is crashing with latest chrome version (59.0.3071.86)
WING-35297	EGuest: Cfgd key_list error seen in controller after initiating splash template notification
WING-35298	EGuest: splash template notification does not identify multiple controllers split in same location
WING-35299	External mac_registration registration process / process does not receive registration request from Controller
WING-35303	EGuest: Database import fails when attempted multiple times
WING-35420	Captive Portal: when mac auth is enforced, the role assignment is failing when the server is sending a new role through CoA
WING-35424	EGuest: Block user from pushing splash templates to locations which are not allowed - through allowed-locations settings
WING-35474	NSight: AP names are not properly displayed on the MapView
WING-35475	NSight: Mapview - 2.4 GHz channel is displayed for a turned off radio
WING-35542	critical-resource and l2tpv3 specific show command must be allowed for helpdesk user
WING-35543	During upgrade of a Site cluster from NOC, standby gets upgraded multiple times when the APs are adopting to the active
WING-35569	EGuest: Splash template push fails with error - Cannot read property 'length' of undefined
WING-35582	NSight: SSM uses TLSv1.0 for HTTPS connection which causes failure in connectivity
WING-35589	AP fails to connect with Extreme Location server when there is a CA certificate deployed on the server
WING-35628	Default 802.1x re-authentication period of 60 seconds is too short, should be 3600 seconds
WING-35658	Captive Portal Voucher is not legible when printing on a Zebra ZQ520 portable printer
WING-35675	NSight: Channel to be displayed only if Radio is ON
WING-35806	EGuest: Social Facebook Check in redirect url needs fix across default templates
WING-35924	Do not fragment bit is set in all packets sent from user space

11. Known Issues

Following issues are known issue in WiNG 5.9.x:

CQ/ SPR	Headline	Comments
WING-23199	Even after disabling routing "show ip route" has all static route entry and traffic between two networks is not dropped	

CQ/ SPR	Headline	Comments
WING-26986	AP 8132 sends Aggregated FT response with both category code 126 and 6 in a certain configuration condition	
WING-27180	EAP termination functionality may not work with certain versions of Cisco-ISE	
WING-29260	AP 8533 - Port is down permanently when changing from auto duplex to Half duplex/Full duplex (Speed 100Mbps)	Avoid setting Half duplex on AP 8533; use another interface to correct setting
WING-30078	SWIFT UI: User can't add both WLAN and MCX on the same radio	In wing-express Meshpoint and WLAN can't be mapped to the same radio .
WING-30726	Captive portal: MAC registration fallback with WeChat social authentication is not supported	
WING-31987	Error message while configuring Subnet/exclude-IP under Profiles-Network-Bridge VLAN in GUI	Workaround is to use CLI
WING-32272	On board Radius server authentication is failing with ttls mschapv2	This is due to incompatibility of new openssl version and older Radius version.
WING-33284	NSight - In the Rf-Matrix, the legend masked on donut is not getting updated when you change between different parameters	
WING-34210	NSight: Devices get marked as offline randomly when the stats update interval is set to 5 minutes	Workaround - set update interval for Aps to no more than 2 min. For larger setup - only MU stats set to 5.
WING-34795	iPhone device gives error "disallowed user-agent" for google authentication	Enable "bypass captive-portal-detection" and use regular browser for google authentication.
WING-34972	NSight Dashboard: Themes and Widgets not visible during start up when Mongo DB is not fully loaded	Wait few minutes to open NSight UI after appliance start.
WING-34981	Dynamic VC: UI: newly elected VC is not marked as VC.	
WING-35482	AP 7612 OCS scans all channels every 30 seconds regardless of configuration and OCS channel list. (This is due to QCA limitation)	
WING-35568	AP 7612: Cisco phone connection is not stable	
WING-35560	AP 7612: Failed to login via Console when cable is plugged after AP bootup	Plug the serial cable prior to boot up.
WING-35869	Controller UI doesn't allow to configure more than 14 clients for CB AP.	Issue is only on the controller UI. AP UI shows correct limit. Workaround: use cli to configure the limit.