WiNG 5.8.5.0-016R Release Notes

Overview

WiNG 5.8.5 is a maintenance release that continues to build on the innovative WiNG 5 architecture across 802.11n and 802.11ac Enterprise WLAN portfolio. WiNG 5.8.5 introduces several feature enhancements and provides critical customer fixes.

1. Platforms Supported

RFS 4011, NX 9000, NX45XX and NX65XX platforms are EOL and support has ended. No new images will be released or supported for those platforms.

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

AP 7181 is EOL and support has ended. No new images will be released or supported for this platform.

Important: Image name change: NX9500 image is now called NX9500-<version>.img and not NX9000-<version>.img as in previous releases.

WiNG 5.8.5 supports the following platforms with the corresponding firmware images:

Controller Platform	Firmware Image
RFS 4000	RFS4000-5.8.5.0-016R.img, RFS4000-LEAN-5.8.5.0-016R.img
RFS 6000	RFS6000-5.8.5.0-016R.img, RFS6000-LEAN-5.8.5.0-016R.img

Controller Platform	Firmware Image
RFS 7000	RFS7000-5.8.5.0-016R.img, RFS7000-LEAN-5.8.5.0-016R.img
NX 9500/ NX 9510	NX9500-5.8.5.0-016R.img
NX 9600 / NX 9610	NX9600-5.8.5.0-016R.img, NX9600-LEAN-5.8.5.0-016R.img
NX 75XX	NX7500-5.8.5.0-016R.img, NX75XX-LEAN-5.8.5.0-016R.img
NX 5500	NX5500-5.8.5.0-016R.img, NX5500-LEAN-5.8.5.0-016R.img

Virtual Platform	Firmware Image
VX 9000[1]–production iso/img image	VX9000-INSTALL-5.8.5.0-016R.iso, VX9000--5.8.5.0-016R.img, VX9000-LEAN-5.8.5.0-016R
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-5.8.5.0-016R.iso[2]

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

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

WiNG Express Manager	Firmware Image
NX 5500E	NX5500E-5.8.5.0-016R.img
NX 7510E	NX7500E-5.8.5.0-016R.img
VX 9000E	VX9000E-INSTALL-5.8.5.0-016R.iso

AP Platforms	Firmware Image
Dependent APs	
AP 650	AP650-5.8.5.0-016R.img AP650-LEAN-5.8.5.0-016R.img[3] (included in all Controller images)
Independent /Adaptive APs	
AP 6511 / AP 6511E	AP6511-5.8.5.0-016R.img (included in NX controller images)
AP 6521 / AP 6521E	AP6521-5.8.5.0-016R.img (included in all Controller images)
AP 6522 / AP 6522E	AP6522-5.8.5.0-016R.img (included in all Controller images)
AP 6532	AP6532-5.8.5.0-016R.img AP6532-LEAN-5.8.5.0-016R.img[3] (included in all Controller images)
AP 6562 / AP 6562E	AP6562-5.8.5.0-016R.img (included in all Controller images)
AP 7131 / AP7161	AP71XX-5.8.5.0-016R.img (included in NX controller images)
AP 7532	AP7532-5.8.5.0-016R.img (included in the NX controller images)
AP 7522	AP7522-5.8.5.0-016R.img (included in the NX controller images)
AP 7522E	AP7522E-5.8.5.0-016R.img (included in the express controller images)
AP 7562	AP7562-5.8.5.0-016R.img (included in the NX controller images)
AP 7502 / AP 7502E	AP7502-5.8.5.0-016R.img (included in the NX controller images)
AP 8132 / AP 8122 / AP 8163	AP81XX-5.8.5.0-016R.img (included in NX controller images)
AP 8222 / AP 8232	AP82XX-5.8.5.0-016R.img (included in NX controller images)
AP 8533	AP8533-5.8.5.0-016R.img (included in NX controller images)
AP 8432	AP8432-5.8.5.0-016R.img (included in NX controller images)
Independent /Adaptive Wall Switch	
ES 6510	AP6511-5.8.5.0-016R.img (ES 6510 uses AP 6511 image)

*[3]AP6532-LEAN-5.8.5.0-016R.img / AP650-LEAN-5.8.5.0-016R.img built **without** **GUI component**.*

2. New Features in WiNG 5.8.5

WiNG 5.8.5 introduces support for following new features/enhancements:

Client Bridge support for AP 7532, AP 7522 and AP 7562 product family
WiNG 5.8.5 extended client bridge functionality to 11ac portfolio by adding support on AP 7532/7522/7562 product family. Client bridges provide simple, cost-effective Wireless LAN connectivity for wired-only devices (printers, point-of-sale, etc).

802.1X support extended to all 11ac AP product family
WiNG 5.8.5 extended 802.1X support for AP 7562, AP 8533 and AP 8432.

500 wireless client support:
WiNG 5.8.5 adds support for up to 500 associated client devices per access point and up to 16 BSSIDs per radio for AP 8533 and AP 8432. Up to 256 clients will be supported per radio.

200 wireless client support:
WiNG 5.8.5 adds support for up to 200 associated client devices per radio and up to 16 BSSIDs per radio for AP 7532, AP 7522, and AP 7562. Up to 256 clients is supported per AP.

Captive Portal Enhancement: Database export functionality
WiNG 5.8.5 adds ability to schedule Captive Portal database export at a set frequency (CLI parameter) to periodically export the records (in CSV format).
Database export functionality will provide simple way of tracking user visit frequency.

SNMP enhancements:
WiNG 5.8.5 adds following new OIDs:

- Number of clients - successful captive portal Authentication (RF-domain and radio-level)
- Number of clients - failed captive portal authentication (RF-domain and radio-level)
- Number of adopted APs (NOC and device level)

Troubleshooting enhancements:

- **Loop detection enhancement -** provides more visibility into loop detection by adding information for the customer in following areas: interface/VLAN where the loop is detected and last seen event.
- **ACL check enhancement –** provides a simple one view to show ACLs status applied on the device. ACLs carry critical firewall rules to allow/disallow traffic to the network. As such it’s critical to know if all rules have been properly applied at device level

Device deployment enhancement:
AP replace option – new "replace" option automates AP replacement process by combining the "clone" and "no apxxxx <mac-address>" into a single operation. New “replace” command is accessible by "device-provisioning-admin".

NSight enhancements:
NSight Guest client count - adds Guest Client count as an "icon" in the Monitor key metrics stripe to display the total number of guest clients at all levels in the tree (RFD, System etc).

3. Firmware Upgrade / Downgrade – Controllers and Dependent APs

3.1 Important Notes on Upgrade / Downgrade

1. 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

2. When downgrading AP 8132 from 5.8.4 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".

3. 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.

4. 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*

5. WiNG 5.8.2 and above - Upgrading AP 6532 / AP 650
   - WiNG 5.8.2 and above mitigates AP 6532 image size issue by introducing 2 different images:
     - *AP6532-LEAN-5.8.5.0-016R.img:* built without the GUI component and is included in the controller images
     - *AP6532-5.8.5.0-016R.img:* standard image, however without the GUI help files, for independent APs that require GUI support.
   - Controller based deployment:
     - Upgrade the AP with AP6532-LEAN-5.8.5.0-016R.img image (included in the controller images).
     - Once upgraded, if the non-active (Secondary) flash partition has image version prior to WiNG 5.7.2, load AP6532-LEAN-5.8.5.0-016R.img image to the partition.

6. 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.

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
    2    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. 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.
10. 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.
11. 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 patch **AP75XX-CPU-Bringup-1.0.patch**.
    AP 7532/7522 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:
    - Load the kernel patch for AP 7532/7522 device models on controller using device-upgrade load-image option:
      - “device-upgrade load-image ap7522 tftp://<server ip address >/AP75XX-CPU-Bringup-1.0.patch”
    - Execute “device-upgrade all force no-reboot” from the controller to upgrade the APs with the patch.
    - Use “boot system primary” or “boot system secondary" based on the WiNG 5.5.5/5.5.4 image location on the APs and reload the APs from the controller.

12. 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.

13. 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.
14. 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.

15. 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.
16. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

3.2 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.

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS + AP 650	v4.3.x onwards on the controller	v4.3.x onwards on the controller	AP 650 image is contained within the controller image
RFS + AP 7131/AP 7131N	v4.1.1 onwards on the AP v4.3.x onwards on the controller	v4.1.1 onwards on the AP v4.3.x onwards on the controller	AP 7131/AP 7131N v5.x image is not within the controller image
RFS + AP 6532	v5.1 onwards	v5.1 onwards	AP 6532 image is contained within the controller image
RFS + AP 6511	v5.1 onwards	v5.1 onwards	AP 6511 image is not contained within the controller image
RFS + ES 6510	v5.4 and higher	v5.4 and higher	ES 6510 uses the same image file as the AP 6511. The image is not contained within the controller image
RFS 4011 with AP 650	v5.1 onwards	v5.1 onwards	
RFS/NX 9XXX + AP 7161	v5.1.1, v5.1.4, v5.2 onwards	v5.1.1, v5.1.4, v5.2 onwards	
RFS/NX 9XXX + AP 6521	v5.2 onwards	v5.2 onwards	AP 6521 image is contained within the controller image
RFS/NX 9XXX + AP 6522	v5.4 onwards	v5.4 onwards	AP 6522 image is contained within the controller image
RFS/NX 9XXX + AP 6562	v5.4.4 onwards	v5.4.4 onwards	AP 6562 image is contained within the controller image
RFS/ NX + AP 8132	v5.2.6, 5.4.2 and higher	v5.2.6, 5.4.2 and higher	AP 8132 image is not within the RFS controller image but is contained within NX controller image

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS/ NX + AP 82XX	v5.5.3 and higher	v5.5.3 and higher	AP 82XX image is not within the RFS controller image but is contained within NX controller image
RFS/ NX + AP 8122	v5.5.2 and higher	v5.5.2 and higher	AP 8122 image is not within the RFS controller image but is contained within NX controller image
NX 7500	v5.5.2 and higher	v5.5.2 and higher	Note: WiNG 5.6 doesn’t support NX 7500.
RFS/NX + AP 7532/AP 7522	v5.5.3.1 and higher, excluding v5.6.x	v5.5.3.1 and higher, excluding v5.6.x	AP image is contained within the NX controller image in v5.5.4
RFS/NX + AP 7562	v5.7.1 and higher	v5.7.1 and higher	AP image is contained within the NX controller image in v5.7.1
RFS/NX + AP 7502	v5.5.4.1 and higher, excluding v5.6.x	v5.5.4.1 and higher, excluding v5.6.x	AP image is contained within the NX controller image in v5.5.5
RFS/ NX + AP 8163	v5.6 and higher	v5.6 and higher	AP 8163 images are not within the controller image
VX + all supported APs	v5.6 and higher	v5.6 and higher	
NX 7510E/VX 9000E/NX 5500E + AP 6511E / AP 6521E / AP 6522E / AP 6562E / AP 7502E / AP 7522E	v5.5.3 and higher	-	NX 7510E and VX 9000E are supported starting with v5.7 NX 5500E is supported starting with v5.8
NX 96XX	v5.5.6 and higher	v5.5.6	NX 96XX is not supported with v5.6.x and v5.7.x
NX 5500	v5.8	v5.8	NX 5500 is supported starting with v5.8
RFS/NX + AP 8533	v5.8.3 and higher	v5.8.3 and higher	AP image is contained within the NX controller image in v5.8.3
RFS/NX + AP 8432	v5.8.3 and higher	v5.8.3 and higher	AP image is contained within the NX controller image in v5.8.3

3.3 Upgrade / Downgrade Procedure for WLAN Controllers

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 in particular the use of the "Lean Controller image" which does not include AP image***s – since the controller image size is now significantly larger than WiNG 5.4.x release.
The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

IMPORTANT: Always create config back-up before the upgrade.

1. Copy the RFSX000-5.8.X.X-0XXR.img or NXXX00-5.8.X.X-0XXR.img to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the controller. From CLI the command is —reload.

3.4 Upgrade / Downgrade Procedure for dependent APs connected to RFS controllers – AP 650

Note: If upgrading from any of the following releases 4.x, 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.8.
A WiNG 5.x controller can upgrade an AP 650 running 4.x code to 5.x using the WISPe upgrade. This capability is enabled using "legacy-auto-update" command for the controller, either under the device or profile. The controller will first adopt the access point using the standard WISPE protocol messages (just as a 4.x controller would adopt it) and then download the new image to it, which would convert the AP to WiNG 5.x version of the code.
Legacy-auto-update is enabled by default. If legacy-auto-update is disabled, use the following CLI instructions to enable the Legacy-auto-update feature:

```
rfs4000-22A136#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs4000-22A136(config)#profile rfs4000 default-rfs4000
rfs4000-22A136(config-profile-default-rfs4000)#legacy-auto-update
rfs4000-22A136(config-profile-default-rfs4000)#commit
rfs4000-22A136(config-profile-default-rfs4000)#
```

3.5 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:

```
nx9500-6C8647#show device-upgrade versions
```

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

```
nx9500-6C8647# 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.

```
nx9500-6C8647# device-upgrade ap71xx-16C7B4 ?
  no-reboot       No reboot (manually reboot after the upgrade)
  reboot-time     Schedule a reboot time
  upgrade-time  Schedule an upgrade time

nx9500-6C8647# device-upgrade ap71xx 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.

```
nx9500-6C8647# 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

```
nx9500-6C8647# #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
```

3.6 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.

```
rfs4000-22A1B8(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.

```
rfs4000-22A1B8(config-device-XXX)# device-upgrade count ?
  <1-20>  Number of concurrent AP upgrades
```

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

3.7 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:

- WingRFS.RFS4000
- WingRFS.RFS6000
- WingRFS.RFS7000
- WingNX.NX7500
- WingNX.NX9000
- WingNX.VX
- WingNX.NX5500

4. Firmware Upgrade/Downgrade – Independent APs

4.1 Important Notes on Upgrade / Downgrade

1. 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

2. When downgrading AP 8132 from 5.8.4 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".

3. 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.

4. 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*

5. 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-5.8.5.0-016R.img:* built without the GUI component and is included in the controller images
     - *AP6532-5.8.5.0-016R.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 AP6532-5.8.5.0-016R.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 AP6532-5.8.5.0-016R.img image to the partition

6. 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.

7. 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
    2    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
   ```

8. 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.

9. When downgrading from WiNG 5.5.x to a lower WiNG 5.x version 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.

10. Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP. Please allow time for devices to complete the upgrade.

11. 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.

12. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

4.2 Upgrade / Downgrade Matrix

Independent/Adaptive Access Point	Upgrade from	Downgrade to	Notes
AP 6511	v5.1 onwards	v5.1 onwards	
ES 6510	v5.4 onwards	v5.4 onwards	
AP 6521	v5.2.x onwards	v5.2.x onwards	
AP 6522	v5.4 onwards	v5.4 onwards	
AP 6532	v5.1 onwards	v5.1 onwards	See Note 2
AP 6562	v5.4.4 onwards	v5.4.4 onwards	
AP 7131	v4.1.1 onwards	v4.1.1 onwards	
AP 7161	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	
AP 7502	v5.5.5 onwards	v5.5.5 onwards	No support in v5.6.x
AP 7532/ AP 7522	v5.5.3.1 onwards	v5.5.3.1 onwards	No support in v5.6.x
AP 7562	v5.7.1 onwards	v5.7.1 onwards	
AP 8132	v5.2.6, 5.4.2 onwards	v5.2.6	
AP 8122	v5.5.2 onwards	v5.5.2 onwards	
AP 8222/AP 8232	v5.5.3 onwards	v5.5.3 onwards	
AP 8163	v5.6 onwards	v5.6 onwards	
AP 6511E / AP 6521E / AP 6522E / AP 6562E / AP 7502E / AP 7522E	v5.5.3 onwards	v5.5.3 onwards	
AP 8533	v5.8.3 onwards	v5.8.3 onwards	
AP 8432	v5.8.3 onwards	v5.8.3 onwards	

Notes:

1. If upgrading from any of the following releases 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.5.x.

4.3 AP Upgrade / Downgrade Procedure

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.
1. Copy the APXXXX-5.8.X.X-0XXR.img to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **AccessPoint->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the Access Point. From CLI the command is —reload.

Note: WiNG 5.1.3 added support for the new NAND for AP 7131N. 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.

Note: 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.

4.4 AutoInstall

AutoInstall in WiNG 5 works via DHCP. 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 be entered 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:

- WingAP.AP6511
- WingAP.AP6521
- WingAP.AP6522
- WingAP.AP6562
- WingAP.AP6532
- WingAP.AP7131
- WingAP.AP7161
- WingAP.AP7502
- WingAP.AP7522
- WingAP.AP7532
- WingAP.AP7562
- WingAP.AP8122
- WingAP.AP8132
- WingAP.AP8222
- WingAP.AP8232
- WingAP.AP8163
- WingAP.AP8533
- WingAP.AP8432

5. Upgrade / Downgrade - NSight and Captive-Portal

5.1 Important Notes on Upgrade – NSight and Captive Portal

1. Upgrading from WiNG 5.8.2 to WiNG 5.8.3 - NSight
   - Upgrade all devices to new firmware using the upgrade command. DO NOT reboot the devices.
   - Disable NSight-server on both primary and secondary replica-set members:

```
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

Secondary #self
Enter configuration commands, one per line.  End with CNTL/Z.
Secondary (config-device-00-0C-29-35-AE-F7)#no use nsight-policy
Secondary (config-device-00-0C-29-35-AE-F7)#comm wr
Secondary (config-device-00-0C-29-35-AE-F7)#end
```

   - 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 before rebooting the secondary replica-set member. 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.

Secondary#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.
```

- Reboot the secondary and wait for the device to come up and join the replica-set. As mentioned in in the previous step, verify that the replica-set is up using '*sh database status*' command.
- Reboot the Arbiter and wait for the device to come up and join the replica-set.
- Enable nsight-server on both primary and secondary:

```
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

Secondary #self
Enter configuration commands, one per line.  End with CNTL/Z.
Secondary (config-device-00-0C-29-35-AE-F7)#use nsight-policy <nsight-policy>
Secondary (config-device-00-0C-29-35-AE-F7)#comm wr
Secondary (config-device-00-0C-29-35-AE-F7)#end
```

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):

- 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
```

- 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-5.8.5.0-016R.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

5.2 Important Notes on Downgrade – NSight and 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 lower versions of WiNG, 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.

6. Important Notes

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.

<u>New in v5.8.4</u>

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 8533 and AP 8432 do not support multiple SSIDs per BSSID due to restrictions enforced by the chipset/driver.
10. AP 8533 and AP 8432 require a WLAN is always mapped (no shutdown) to BSS1.
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
   - A 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

- 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 backup 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
- VX 9000 requires re-install using the VX9000-INSTALL-5.8.5.0-016R.ISO image if the user intends to configure NSight / Captive portal functionality. This is due to the changes to the flash partition (25% of the allocated disk size – 4GBMin, 128GB Max) to take effect:
  - Export configuration before reinstalling the VX.
  - To preserve the same MAC address (and therefore the serial number for licensing)
    - Delete current hard disk from the VM
    - Add new virtual hard disk
    - Connect ISO file as virtual CD
    - Boot into CD to start installation process

    After installation is complete, restore the configuration.

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 timezone

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.

<u>New in v5.7.2</u>

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.

<u>New in v5.7.1</u>

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 and 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

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 6522/6532/6562/71xx - VRRP and OSPF feature support have been removed

<u>New in v5.6.x</u>

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 particular 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.

<u>New in v5.5.6</u>

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 on 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.

<u>New in v5.5.5</u>

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 mpbs rates configured on infrastructure. Impacted devices are: MC1790, MC5590, MC7590, MC7594, MC9590, MC9596, MC3190, MC75, MC9190, MC55, VC6090, VC6096, MT2090, MK3900, MK4900, MK590.
   If SSID/band is used exclusively for 802.11g or 802.11gn devices (i.e. no 802.11b devices), configure the data-rates on the SSID/radio to be “g-only” or “gn” or custom with 5.5 and 11 Mbps excluded from the basic rate set.
   If SSID/band is used by 802.11b-only devices as well, configure the data-rates on the SSID/radio to be custom with 1 Mbps and/or 2 Mbps as basic and exclude 5.5 Mbps and 11 Mbps from the supported rates.

<u>New in v5.5.4</u>

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.

<u>New in v5.5.3</u>

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; wlans requiring to support TKIP clients should use tkip-ccmp as the encryption type.

- Upgrading from a prior WiNG 5.x to release to WiNG 5.5.3 will automatically modify the configurations for wlans using 'tkip' as encryption type to 'tkip-ccmp' and will add "service wpa-wpa2 exclude-ccmp" command to avoid any post upgrade incompatibility issues.
- For new configurations, to handle certain legacy/non-Wi-Fi compliant client situations where the client driver is incompatible or does not operate properly in a mixed mode TKIP-CCMP configuration, add the following command "service wpa-wpa2 exclude-ccmp" to the wlan configuration. This configuration allows the wlan to operate in TKIP only modes until the non-compliant wireless clients are phased out of the network.

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-xxxxx" action commands have been replaced with "device-xxxxx" action commands. For example: ap-upgrade xxxx will now be referred to as device-upgrade xxxxx.
   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.

<u>New in v5.5.1</u>

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.

<u>New in v5.5</u>

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 stings.
   Following line needs to be modified under function **getQueryVariable(variable),**
   var vars = query.split("?"); === change it to ==□ var vars = query.split(/[?&]/);
   Please ensure that this function gets updated in all the captive portal pages that uses it.

<u>New in version 5.4.x</u>

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 and AP 7181 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 AP 6511, AP 6521, ES 6510, 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. Note that when an adopted AP (6521, 6511) or ES 6510 is separated from a controller to operate in standalone mode, the GUI will remain disabled due to this feature, unless the above command is used.
   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:F8:00:00:00/48.

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 (& ES) 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, AP 6511, ES 6510 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 6511, AP 6521, ES 6510– 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.

7. DFS Tables, Sensor and Radio Share

1. Following is the DFS support in WiNG 5.8.5 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 650 AP 6532	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7131	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

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 6511	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 8222/8232	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

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 6511/6521[1]	No	Yes	Yes	Yes	Yes	Yes
AP 650/6532	Yes	No	Yes	Yes	Yes	Yes
AP 6522/6562	No	Yes	Yes	Yes	Yes	Yes
AP 7131/7161	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/ 8222	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

Notes:

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

[2] Support is limited to the dedicated sensor (Radio 3) for AP 8533. Support is limited to the dedicated sensor (Radio 1) for AP 8432.

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

Network Assurance Toolset with Radio Share	Spectrum Analysis[2]	Advanced Spectrum Analysis[3]	Live RF	Live View	AP Testing	Connectivity Testing
AP 6511/ 6521[1]	No	Yes	Yes	Yes	Yes	Yes
AP 650/6532	No	No	Yes	Yes	Yes	Yes
AP 6522/6562	No	Yes	Yes	Yes	Yes	Yes
AP 7131/7161	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 8232/8222	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

Notes:
[1] GUI is disabled when Radio Share is enabled.
[2] Spectrum Analysis is not supported with Radio share enabled.
[3] Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.

8. Vulnerability updates

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

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

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

WiNG 5.8.3
OpenSSL package has been updated to 1.0.1p to incorporate latest security vulnerability fixes.
CVE-2015-7547: Glibc getaddrinfo stack-based buffer overflow
TLS/SSL Server Support for DES and IDEA Cipher Suites (ssl-des-ciphers) was removed
TLS 1.0 and TLS 1.1 disabled by default.
The SSH server support for the diffie-hellman-group1-sha1 key exchange algorithm, which is known to have a potential security weakness has been removed.

WiNG 5.8.2
Linux kernel patched to address security vulnerability CVE-2015-5707
WiNG 5.8.1
OpenSSL package has been updated to 0.9.8zg to incorporate latest security vulnerabilities fixes.

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

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

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

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

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

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

WiNG 5.5.1
Cross-Site Request Forgery (CSRF) based on CWE-352 family vulnerability
SecScan Qualys: Deprecated Public Key Length (QualysVersion Scanner 7.3.31-1, Vulnerability Signatures 2.2.580-2)
OpenSSH vulnerabilities - SSH Insecure HMAC algorithms enabled and SSH RC4 Cipher enabled

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

9. Issues Fixed

Following issues have been fixed in WiNG 5.8.5 release:

SPR#	Description
SPR 29359	Security: MongoDB Service Without Authentication Detection
SPR 29820	Poor video performance across mesh when using birch
SPR 30060	Event-history page unable to display large amounts of event history records.
SPR 30124	Device incorrectly classified as Rouge SSID AP
SPR 30154	SWiFT UI: Unable to map Meshpoint to the radio of Anyap AP profile via GUI on VX
SPR 30162	Bulk user feature fails on NX5500 to generate users on GUI.
SPR 30181	MCX: Root AP Broadcast Issue
SPR 30210	DNS snoop table is not updated with all the IP addresses received in DNS response
SPR 30224	SNMP walk times out and takes longer on few OIDs
SPR 30265	Bonjour Gateway fails when policy name exceeds 16 characters.
SPR 30281	Legacy Non 802.11r client cannot associate to WLAN which has 802.11r enabled
SPR 30293	Beacon missing WME IE when setting custom rates on meshpoint
SPR 30297	DPD2 crash while processing bonjour query response
SPR 30308	AP 7161 is not able to negotiate power properly of Avaya PoE switch when LLDP is enabled
SPR 30324	Configuration modified under “meshpoint …” context is not being sent in outside-in fashion
SPR 30350	Captive-portal guest registration request gets dropped in rfs6000 site-controller
SPR 30351	NSight reports: unable to generate client inventory report in CSV format Under Tree Node.
SPR 30352	Radius fallback should fallback to local only if the radius is unreachable.
SPR 30363	Configuring / in the name of the tree-node configuration should be disallowed
SPR 30394	5GHz WLAN mapping on AP6521E not being sent by Express Manager
SPR 30396	Captive portal pages uploaded via GUI causes the file to be created with surrounding quotes.
SPR 30407	APs can’t connect to NSight server when DNS server is not reachable on boot up.
SPR 30408	Configuring “use enterprise-ui” for an AP on controller results in controller rebooting a second time after it boots up due to initiated reload
SPR 30422	Captive-portal database fails to start in Wing Express controller VX9000 running 5.8.4.0. “Show guest-registration client mac <MU-mac-address>” returns error: “Unable to connect to the database” message.
SPR 30423	Captive-portal Social authentication: Facebook/Google app requires query string to have field names explicitly mentioned in it so that Facebook/Google response will have the values of fields requested pertaining to the Facebook/Google user
SPR 30440	DPI Metadata kernel panic observed in university due to enabling DPI metadata on NX 9XXX platforms
SPR 30447	LBS: Wireless clients not seen on the floor plan for AP 6532, AP 6522 with 5.8.4.
SPR 30470	Captive-portal-page-upload load-file” command does not support “#” in SFTP password field

SPR#	Description
SPR 30521	After Failover of active and standby in cluster, both controllers are showing as ACTIVE
SPR 30527	Single radio mu are being reported as a dual channel capable for band steering in mixed AP environment.
SPR 30630	AP7532 radio2 resets when high bandwidth wireless traffic is received with radio configured for DFS channel
SPR 30705	Last email status always reported as successful in guest registration even if it's not
SPR 30706	Registration email structure is corrupt when edited via GUI
SPR 30782	Service show command-history displays passwords in clear text with password-encryption secret 2 enabled
SPR 30792	dpd2 memory usage spikes while processing bonjour packets with malformed TLVs
SPR 30800	"service radius test" and "authentication server" show up as clear text in command history
SPR 30814	SSM memory leak seen on site controllers that don't support DPI while feature is enabled for APs that do support it
SPR 30887	dpd2 crashes while calculating extended VLAN broadcast routing table due to corruption in extended VLAN bitmap
SPR 30899	Full list of printers is not populating in the AP cache for Bonjour services
SPR 31024	SMS configuration username field does not allow "." character and API-ID field does not allow "==" character.
WING-30242	The same WLAN mapped to the 2 radios of the same AP, 1 radio's state shows up as Rogue SSID and the other as unsanctioned ap.
WING-30905	Band steering: probe entries age-out is not being displayed correctly at times in the proc table
WING-31640	AP 8533 with 3af and radios operating in 2X4, in pcap only 2Tx and 2 Rx fields set.
WING-31714	Nearby Analytics - Data send is not happening after anald process restarted
WING-31716	Nearby Analytics - Remove the "http-analyze controller" as it's obsolete
WING-31758	AP 7562 multiple panics when using MCX and inline sensor.
WING-31765	APs unadopt and never readopts while maintaining a MiNT link
WING-31793	NX 9600 fails to write panic file sometimes
WING-31794	Need to add cluster history command
WING-31795	Cluster Hello packet is getting looped when cluster is created using cluster join command
WING-31878	cfgd crash when the session is closed abruptly during "service delete-offline-aps all"
WING-31910	Captive Portal: smart registration feature is not enabled in NX 96XX platform
WING-31991	Hostname width customization does not work properly for CLI command - show wireless radio
WING-32003	AP 8533 dynamic-chain-selection with 3af power is not functioning.
WING-32178	If the authentication is rejected from RADIUS/TACACS, local authentication should not happen even if fallback is configured
WING-32221	11a clients get disconnected and don't roam in mixed mode (11n +11a clients) in stress roaming test.
WING-32259	LLDP negotiation with Cisco switch fails when Cisco tags LLDP packet with VLAN 1 which is not part of the trunked port config.

SPR#	Description
WING-32305	NX 5500 panic does not leave panic dump file
WING-32360	Wrong RSSI values for AP 81XX reporting to Euclid in the range of -10K to -21K
WING-32382	Wired Captive Portal: Add the wired captive portal support in case of extended VLAN
WING-32409	Count of clients with successful hotspot authentication is greater than the number of clients
WING-32425	AP 7562 panic when using MCX - PC is at wlc_nar_free
WING-32700	MCX-ACS shows the wrong reason for turning off the radio when invalid channels have been configured.
WING-32773	AP 8533 client connectivity issues when the 3rd radio is in sensor background scan.
WING-32774	AP 7532 panic - PC is at wrap_802_3_in_mint
WING-32777	Incorrect LLDP power negotiation with certain Cisco switches on boot up. 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.
WING-32812	AP 7532 panic – PC is at dp_pkt_pull
WING-32813	BLE feature is not functioning properly on Wave-2 AP 8533
WING-32868	AP 8533 is reading 3at power-injector as 3af
WING-32905	Multiple Clock update events published by NTPD in quick succession causing potential memory leak
WING-33108	wireddot1x is not working on AP 7532, AP 7522, AP 8432, AP 8533
WING-33233	AP 7532 and AP 7562 power tables are incorrect in WiNG 5.8.4.
WING-33330	Database drop <database-name> returns an error, stating NSight must be stopped when it’s not running.
WING-33345	LLC packets from POS controllers are being dropped by AP 7532.

10. Known Issues

Following issues are known issue in WiNG 5.8.x:

CQ/ SPR	Headline	Comments
WING-24110	CP Bandwidth voucher: User is not getting configured data limit for bandwidth based voucher	
WING-23199	Even after disabling routing "show ip route" has all static route entry and traffic between two networks is not dropped	
WING-27376	EX 3500 Management: Configuring class-map and policy-map description do not allow special characters	
WING-27180	EAP termination functionality may not work with certain versions of Cisco-ISE	
WING-26986	AP 8132 sends Aggregated FT response with both category code 126 and 6 in a certain configuration condition	

CQ/ SPR	Headline	Comments
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: User can't add both WLAN and MCX on the same radio	
WING-29042	AP Test: AP Test on ap6511 radioshare mode fails with the message "BSS is on channel on which sensor not allowed to transmit"	Only seen when used changes radio band. Workaround: reboot AP after band change and before running the test.
WING-30726	Captive portal: MAC registration fallback with WeChat social authentication is not supported	
WING-31747	AP 8533 / AP 8432: On radar detection, the radio will always switch to 20 MHz channel	
WING-30714	Remote VPN clients not able to get DNS/WINS Server IPs from the NX 7500 VPN Gateway	
WING-30478	Captive portal: With caching enabled, Chrome browser displays 'disconnected' while using internal welcome page	
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.

© Extreme Networks. 2016. All rights reserved.