Extreme networks
ADVANCE WITH US

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

WiNG 7.6.3.1-001R Release Notes

CONTENTS

OVERVIEW

WiNG 7.6.3.1 release continues to improve unique WiNG7 software architecture that combines the scale, features, and functions of ExtremeWireless^{TM} and ExtremeWirelessWiNG^{TM}, offering flexible deployment option covering both campus and distributed modes. WING 7.6.3.1 is a minor release that extends feature support for new 11ax AP portfolio (including universal HW APs) for ExtremeWireless OmniEdge product line as well as provides stability fixes.

1. PLATFORMS SUPPORTED

Note:

APXXXX-LEAN-7.6.3.1-001R.img - built **without GUI component**. AP lean images are also bundled within controller full image.

NXXXXX-LEAN-7.6.3.1-001R.img – built **without AP images.**

WiNG 7.6.3.1 supports the following platforms with the corresponding firmware images:

Controller Platform	Firmware Image
NX 9500/ NX 9510	NX9500-7.6.3.1-001R.img, NX9500-LEAN-7.6.3.1-001R.img
NX 9600 / NX 9610	NX9600-7.6.3.1-001R.img, NX9600-LEAN-7.6.3.1-001R.img

Controller Platform	Firmware Image
NX 75XX	NX7500-7.6.3.1-001R.img, NX7500-LEAN-7.6.3.1-001R.img
NX 5500	NX5500-7.6.3.1-001R.img, NX5500-LEAN-7.6.3.1-001R.img

Virtual Platform	Firmware Image
VX 9000[1]–production iso/img image	VX9000-INSTALL-7.6.3.1-001R.iso, VX9000-7.6.3.1-001R.img, VX9000-LEAN-7.6.3.1-001R.img
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-7.6.3.1-001R.iso[2]

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

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

AP Platforms	Firmware Image
AP302W	AP302W-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP305C/AP305CX	AP3xxC-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP410C/AP460C AP460S6C/AP460S12C	AP4xxC-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP310/360	AP3xx-7.6.3.1-001R.img AP3xx-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP410/460	AP4xx-7.6.3.1-001R.img AP4xx-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP505/510/560	AP5xx-7.6.3.1-001R.img AP5xx-LEAN-7.6.3.1-001R.img (included in all Controller images)
AP 7522	AP7522-7.6.3.1-001R.img AP7522-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 7532	AP7532-7.6.3.1-001R.img AP7532-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 7562	AP7562-7.6.3.1-001R.img AP7562-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 8533	AP8533-7.6.3.1-001R.img AP8533-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 8432	AP8432-7.6.3.1-001R.img AP8432-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 7612	AP7612-7.6.3.1-001R.img AP7612-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 7632	AP7632-7.6.3.1-001R.img AP7632-LEAN-7.6.3.1-001R.img (included in all NX controller images)
AP 7662	AP7662-7.6.3.1-001R.img AP7662-LEAN-7.6.3.1-001R.img (included in all NX controller images)

2. NEW FEATURES IN WING 7.6.3.1

New features

No new features are introduced in this service release.

3. GENERAL INFORMATION FOR FIRMWARE UPGRADE / DOWNGRADE

3.1 Device Upgrade or Downgrade matrix

This following table provides the allowed upgrade or downgrade combinations. Ensure that the WiNG controller and AP are on the same WiNG version after the upgrade is complete in the controller deployment.

AP	Upgrade from	Downgrade to	Notes
AP7532/AP7522	v5.5.3.1 onwards, excluding v5.6.x	v5.5.3.1 onwards, excluding v5.6.x	AP image is contained within the controller image
AP7612/AP7632/AP7662	v5.9.1	v5.9.1	AP image is contained within the controller image
AP8533/AP8432	v5.8.4 onwards	v5.8.4 onwards	AP image is contained within the controller image
AP505/AP510i	v7.1 onwards	v7.1	AP 5xx image is contained within the controller image
AP510e	v7.1.1 onwards	V7.1.1	AP 5xx image is contained within the controller image
AP560i-FCC	v7.1.1 onwards	v7.1.1	AP 5xx image is contained within the controller image
AP560h-FCC	v7.1.2 onwards	V7.1.2	AP 5xx image is contained within the controller image
AP410/AP460i	v7.3.0.0 onwards	v7.3.0.0	AP 4xx image is contained within the controller image
AP410/AP460e	v7.3.0.0 onwards	v7.3.0.0	AP 4xx image is contained within the controller image
AP310i/e	v7.3.1.0 onwards	v7.3.1.0	AP 3xx image is contained within the controller image
AP360i/e	v7.5.1.1 onwards	v7.5.1.1	AP 3xx image is contained within the controller image
AP305C/AP305CX	v7.5.2.0 onwards	v7.5.2.0	AP 3xxC image is contained within the controller image
AP302W	v7.6.0.0 onwards	v7.6.0.0	AP 302W image is contained within the controller image
AP410C/AP460C/ AP460S12C/AP460S6C	v7.6.2.0 onwards	v7.6.2.0	AP 4xxC image is contained within the controller image
NX 5500	v5.8 onwards	v5.8 onwards	NX 5500 is supported starting with v5.8
NX 75XX	v5.5.2 onwards	v5.5.2 onwards	Note: WiNG 5.6 doesn't support NX 7500
NX 9500	v5.2.1 onwards	v5.2.1 onwards	
NX 9510	v5.4.1 onwards	v5.4.1 onwards	
NX 96XX	v5.5.6 onwards	v5.5.6 onwards	NX 96XX is not supported with v5.6.x and v5.7.x
VX 9000	v5.6 onwards	v5.6 onwards	

3.2 Software compatibility matrix with Extreme Products

WiNG	XCC	ADSP	ExtremeGuest	ExtremeNSight	ExtremeLocation

WiNG 7.1	4.36.01	n/a	5.9.3.1	n/a	n/a
WiNG 7.1.1	4.36.02	10.1.0-13a	5.9.3.1	n/a	n/a
WiNG 7.1.2	4.36.03	10.1.0-13a	5.9.3.1	n/a	2.1
WiNG 7.2.0	4.56.01	10.2.x	5.9.3.1	n/a	2.1
WiNG 7.2.1	4.56.02	10.2.x	5.9.3.1/6.0	n/a	3.1
WiNG 7.3.0	4.76.01	10.3	n/a	n/a	n/a
WiNG 7.3.1	4.76.03	10.4	n/a	n/a	n/a
WiNG 7.4.0	5.06.01	10.4.0-20a7	n/a	n/a	n/a
WiNG 7.4.1	5.16.02	10.4.1	n/a	n/a	n/a
WiNG 7.5.1	5.16.01	10.4.1	n/a	n/a	n/a
WiNG 7.5.2	5.26.01	10.4.1	n/a	n/a	n/a
WiNG 7.6.0	5.26.02	10.4.1	n/a	n/a	n/a
WiNG 7.6.1	5.26.03	10.5	n/a	n/a	n/a
WiNG 7.6.2	5.36.01	10.5	n/a	n/a	n/a
WiNG 7.6.3	5.36.02	10.5	n/a	n/a	n/a

3.3 General Important Notes on Upgrade or Downgrade

IMPORTANT:

- WiNG controller must be running a WiNG7 controller code to be able to recognize, adopt and upgrade 11ax APs.
- Always create config back-up before the upgrade.
- Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Allow time for devices to complete the upgrade. Where APs are powered through PoE connections to WLAN controllers, the controller needs to stay up during the upgrade process.
- Both the WiNG controller and WiNG AP must be upgraded to the same firmware versions – a firmware mismatch can cause network disruptions. When upgrading, the controller should be upgraded first and then the AP. When downgrading, the AP should be downgraded first, and then the controller.

3.4 Device Upgrade or Downgrade Procedure

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

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

3. Restart the device. Type the CLI command —reload.

3.5 AutoInstall

AutoInstall in WiNG5 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 mentioned autoinstall.
DHCP vendor class for platforms is noted below:

Appliances:

- WingNX.NX5500
- WingNX.NX9000
- WingNX.NX7500
- WingNX.VX

AP:

- WingAP.AP302
- WingAP.AP305
- WingAP.AP410
- WingAP.AP505
- WingAP.AP7522
- WingAP.AP7612
- WingAP.AP8432
- WingAP.AP8533
- WingAP.AP310
- WingAP.AP460
- WingAP.AP510
- WingAP.AP7532
- WingAP.AP7632
- WingAP.AP360
- WingAP.AP560
- WingAP.AP7562
- WingAP.AP7662

4. FIRMWARE UPGRADE OR DOWNGRADE – CONTROLLERS

4.1 Platform Important Notes

1. VX 9000:
   a. Secondary storage: VX 9000 has disk size limitation on the default disk of 2TB. However, when a secondary virtual disk is used, VX 9000 can support disks size larger than 2TB
      - Enabling secondary storage does not copy data files to the new location
      - Enable secondary storage immediately after provisioning the guest instance, before enabling NSight or Captive-Portal
      - If the secondary storage needs to be enabled after NSight/Captive-portal, the best practice is to back up the database and restore the database after secondary storage is enabled

  - If the VX 9000 instance is not a primary (replica-set member), the database server will perform full data sync after it is restarted with the new secondary storage disk

2. When upgrading from prior versions – new profiles for newly supported platforms will not be present in the startup-config. The user can either create a default profile or do “erase startup-config”.

4.2 Device Upgrade Options

WiNG 7.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 upgrading all corresponding devices.

To check available firmware on the controller, use the following command:

```
nx9600#show device-upgrade versions
```

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

```
nx9600#device-upgrade load-image
```

Once device firmware is loaded on the controller, the following options are available for device firmware upgrade:

- **Manual Upgrade**

Firmware upgrade can be initiated on a single AP or a list of APs using the following command:

```
nx9600#device-upgrade ap505 ?
  no-reboot      No reboot (manually reboot after the upgrade)
  reboot-time    Schedule a reboot time
  upgrade-time   Schedule an upgrade time

nx9600#device-upgrade ap510 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**

You can schedule and configure the upgrade time and reboot time on a controller. Firmware upgrade on the APs follows the configured upgrade time.

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

- **Upgrade through RF Domain Manager**

Manual firmware upgrade can be initiated through a domain manager

```
nx9600#device-upgrade rf-domain ?
  DOMAIN-NAME  RF-Domain name
  all          Upgrade all RF Domains
  containing   Specify domains that contain a sub-string in the domain name
```

filter *Specify additional selection filter*

4.3 Auto Upgrade

Auto firmware upgrade can be enabled on the controller using the following command. When enabled, any AP with a firmware version different than the controller will be upgraded to the controller's version on adoption.

```
nx9600 (config-device-XXX)# device-upgrade auto
```

The number of concurrent firmware upgrades can be configured using the following command based on the bandwidth available between the controller and the Aps.

```
nx9600(config-device-XXX)# device-upgrade count ?
  <1-20> Number of concurrent AP upgrades
```

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

5. FIRMWARE UPGRADE OR DOWNGRADE – INDEPENDENT APS

5.1 Standalone AP Upgrade or Downgrade

1. Copy firmware image for device that needs to be upgraded to you ftp/tftp server. Refer to section 2 for correct firmware image for your device.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the device. Type the CLI command —reload.

5.2 Virtual Controller upgrade

* Note that the Virtual Controller is not supported on UAPs.

1. If there are no adopters or controllers in the network and several APs require an upgrade, use WiNG Virtual Controller (VC) mode to perform bulk AP upgrades.
2. Use WiNG configuration wizard to configure VC on the AP.
3. When done with the WiNG configuration wizard, upgrade the VC to the latest image by using the following command:
   ap510-1349AC#upgrade tftp://<hostname|IP>path/file
4. After the upgrade is done, reboot the AP to load the latest code.
   ap510-1349AC#reload
5. Load the AP image file on to the VC by using following command:
   ap510-1349AC#device-upgrade load-image ap510 tftp://<hostname|IP>/path/file
6. Add rest of the APs to the network, the VC will listen to the MLCP request from new APs, adopt and upgrade all the APs automatically.

5.3 Upgrading APs through WiNG controller or Extreme Cloud Controller (XCC)

1. APs with default unknown operation mode will find appropriate controllers based on the network provided discovery mechanism i.e. DHCP or DNS.
   - Standard DHCP option 191
   - Standard DHCP option 192

- Vendor Class Identifier DHCP option 191
- DNS response for 'wing-wlc*'

2. If the AP is being adopted by the XCC, upon adoption XCC will automatically upgrade the AP image.
3. If the AP is adopted by a WiNG7 controller, the controller will perform an upgrade based on how it's configured for upgrades i.e. auto upgrade upon adoption or on demand upgrade – refer to section 4.2 in this document.

6. IMPORTANT NOTES

New in v7.6.3

- WiNG distributed HTML5 management UI – Nova
- AP transmit power adjustment for cable attenuation.
- Regulatory updates
- Following campus features are also introduced in this release. Refer to XCC 5.36.02 User Guide for more information.
  - Hotspot 2.0 Enhancements: Increase number of roaming Consortiums

New in v7.6.2

- Following campus features are introduced in this release. Refer to XCC 5.36.01 User Guide for more information.
  - LLDP Neighbor Discovery reporting.
  - MCX/CB adjustment to support Single Interface Universal APs: Wired port can be configured as client port when either CB or MP (non-root MCX) is configured.
  - MCX backhaul link detection and recovery: If MPR (root) AP looses wired connectivity, AP automatically switches to MP (non-root) to attempt to rebuild mesh path via another root.
  - MCX support on AP302W in campus mode.

New in v7.6.1

- BLE/IOT functions for 302W

New in v7.6.0

- Following campus features are also introduced in this release. Refer to XCC 5.26.02 User Guide for more information.
  - Mesh and Client Bridge support on AP302W
  - Adjust Locate LED logic to support explicit ON-OFF state through configuration

New in v7.5.2

- Following campus features are also introduced in this release. Refer to XCC 5.26.01 User Guide for more information.
  - AP health connectivity
  - Mesh and Client Bridge support on UAPs
  - Client port capacity increase: 128 clients per port

  To switch UAPs from on-prem mode to cloud mode:

WiNG distributed mode:
CLI: "ap305c-AE1880#operational-mode xiq-cloud"
WiNG campus mode:
XCC: Configure/Access Points/Action/Release to Cloud
AP CLI: "AP305c-100072# cset operational-mode xiq-cloud"

New in v7.5.1.1

- Following campus features are introduced in this release. Refer to XCC 5.16.02 user guide for more information.
  - Beta mesh support on Wi-Fi6 APs
  - Certificate based IPSec secure tunnel between AP and XCC
  - Expanding Fabric Attach Support w/Authentication-Key
  - Wi-Fi Alliance Enhanced Open, OWE support

New in v7.5.1.0

- Following campus features are introduced in this release. Refer to XCC 5.16.01 User Guide for more information.
  - Enhanced client bridge functionality
    - Per initial client bridge functionality, the radio that is selected for Client-Bridge "back-haul" does not support service. In this release CB supports wireless services on same radio where CB "back-haul" is configured.
    - This release further improves protection for getting client bridge APs stranded.
  - Wi-Fi6 AP network authentication
    - Any installation which follow strict security practices can take advantage of this feature to enable AP authentication to network using PEAR and/or certificates. Devices needs to be pre-provisioned with correct credentials in order to be authorized to connect to the network.

New in v7.4.1

- Following features are introduced in WiNG 7.4.1:

  Campus mode:
  - Power configuration
    - This feature provides option to configure and represent power for wifi6 APs based on per chain or total AP power.
  - Client Bridge enhancement
    - This feature provides support for FA topology on CB APs.
  - Cell size control improvement.
    - This feature provides the following configuration knobs to control RF cell size.
      1) Guard Interval
      2) Low RSS probe suppression
      3) Probe Responses Retry Limit
      4) RX Sensitivity Reduction (DB)
      5) Airtime Fairness
      6) Maximum Distance
  - URL-Redirect (Cisco-AVP) and URL-Redirect ACL support enhancement.

- This feature implements dual factor authentication by chaining 802.1x and Central Web Authentication (CWA) with external Extreme Control.

<u>New in v7.4.0</u>

- Following features are now supported in WiNG 7.4.0:

  <u>Distributed mode:</u>

  - Secure ImagoTag connectivity for all 11ax APs and AP8432.
    - **IMPORTANT** 7.4.0.0 doesn’t support unencrypted mode of connectivity with ESL server. Also, with any existing ImagoTag policy in AP, AP will not be able to connect to ESL server on-prem or on-cloud supporting encrypted communication. On-prem ESL server should be upgraded and appropriate configuration changes to ImagoTag policy made for a successful communication.
    - **CONFIGURATION**

      ```
      iot-device-type-imagotag-policy VCLOUD
        enable
        output-power Level-A
        window-size 14
        payload-size 32
        ssl
        no ssl-cn-verify
        no ssl-strict-verify
        no fcc-mode
        trustpoint <trustpoint-name>
        channel managed
        server hostname <server> port 7354
      ```

      - **ssl** Mandatory for encrypted communication
      - **ssl-cn-verify** Enable to validate the Common Name in server certificate with configured server IP or hostname.
      - **ssl-strict-verify** Enable strict validation of server certificates.
      - **trustpoint** Trustpoint pointing to CA certificate (Global or local).
      - **port** Default port is 7353 which is for cleartext communication. For secure communication port is 7354 which needs to be specified.
  - MCX support on AP4xx

  <u>Campus mode:</u>

  - Enhanced Client Bridge support on all 11ax APs
  - XCC redirection
  - Configurable Redirect Port for HTTP-Proxy Environments
  - URL-Redirect (Cisco-AVP) and URL-Redirect ACL support
  - Policy rules are extended from 64 to 256 for each MU
  - VxLAN support
  - Telemetry support to report AP’s CPU, memory and disk usage
  - Multiple new MU capabilities reporting

<u>New in v7.3.1</u>

- Following features are now supported in WiNG 7.3.1:
  Distributed mode:
  - Virtual controller support on wifi6 APs. Refer to WiNG 7.3.1.1 release note for details.
  - Imagotag ESL support on AP4xx and AP3xx.

New in v7.3.0

- Following features are now supported in WiNG 7.3.0:
  Distributed and Campus mode:
  - ADSP support:
    - Spectrum Analysis.
    - AP Test
  - SU/MU-11ac Beamforming is supported on AP505/510/560/410/460
  - STBC/SU MU_MIMO is supported in HE field on AP505/510/560/410/460
  - OFDMA needs to be disabled for AP500 and AP400.
  - Solid LED enable/disable command
    CLI command will look as below.
    [no] led change-blinking-to-solid-on
    Default value: "Disabled"

New in v7.2.1

- Following features are now supported in WiNG 7.2.1:
  - Imagotag support for AP5xx.
  - Euclid, 3rd party RTLS support.
- Apple client support:
  - Apple client will not stay associated to WLAN with Fast BSS and FT-over DS reason code:17. Disable PMF and Multiband operation to work around this issue.
  - Any Apple mobile client with iOS Version less than 12.1.1, won't connect to a WPA2/WPA3 transition mode WLAN.
    Official support for WPA3 is set for iOS version 13.
- Agile Multiband Operation
  - PMF-optional, 802.11v, 802.11u, 802.11k turned on by default now.
  - Default Value: "Enabled"
- Smart Sensor important notes:
  - BLE sensor and smart-sensor feature currently can't be enabled simultaneously
  - 3rd radio on AP 8533 must be disabled in the config.
  - When smart-sensor feature is enabled in the config – trigger command needs to be issued on the domain to start sensor assignment.
  - When using smart-sensor feature – use AP 8533 profile – not anyap profile.
  - BLE sensor and smart-sensor currently can't be enabled together.
  - Smart-sensor feature currently can't be triggered in controller-managed rf-domains.
- New 11ax config:
  - OFDMA enable/disable command:
    CLI Command will look as below under Radio context:
    [no] 11axOFDMA(dl | ul | both)

Default value: “Disabled”

- BSS Coloring:
  [no] 11axBSS-color (1-63)
  Default Value: “Disabled”
  Note: This functionality is currently not fully supported.
- TWT enable/disable command:
  [no] 11axTWT
  Default value: “Disabled”
  Note: This functionality is currently not fully supported.
- Guard Interval:
  We already have a CLI command to set GI on legacy AP with options GI-Any or GI-Long
  3 new options added in WING-7.2.0 release as “base | double | quadruple”

- 11ax added functionality:
  - Custom rates are now supported.
  - 160Mhz channels are now supported on 5Ghz.
  - Existing ldpc has been turned on by default now.
  - Sniffer re-direct support for 11ax
    - OFDMA, MU-MIMO not supported yet.

<u>New in v7.2.0</u>

- Following features are now supported in WiNG 7.2.0:

  <u>Distributed and Campus mode:</u>
  - ExtremeLocation support:
    - Following features are supported:
      - Zone tracking (requires 6 sec feed interval)
      - Position tracking (requires 1 sec feed interval)
  - ADSP support on AP 5xx:
    - 802.11ax LiveView.
    - Radio share support
  - AP 5xx: SmartRF Support for Dual 5GHz split radio mode.

  <u>Distributed mode</u>:
  - AeroScout RTLS is now supported on AP 5xx.
  - ExtremeAnalytics (Purview):
    - Support for TCP RTT.
    - Support for custom applications rules.
  - WPA3 support:
    - When the WPA3 is configured, no inferior encryption shall exist on the same AP as WPA3. This is enforced by WiFi Alliance as the mandatory requirement for WPA3.
    - New CLI command to configure WPA3 authentication type:

```
ap505-1344D4(config-wlan-temp)#authentication-type ?
  sae       WPAv3-Personal (SAE Authentication)
  sae-psk   WPAv3-Compatibility (SAE or WPAv2 PSK authentication)
```

  - AP 5xx Sniffer-redirect is now (Note: 802.11ax protocol support will be added in later release).

  Campus mode:

  a. RTLS – AiristaFlow (EKAHAU), AeroScout, Centrak, Euclid.
  b. OCS support when SMART-RF is not enabled for ADSP sensor and ExremeLocation sensor support.
  c. DFS Fallback Channels on 5Ghz Radio in Campus mode - Adding the Client Load Balance on AP505/AP510/AP560. This feature allows the APs in the same load balance group to communicate with each other to balance the number of clients associated with each APs inside the same group. Requires XCA 4.56.01 release.
  d. Client Load Balance on AP505/510 In Campus mode - Adding the support of a predefined channel on the 5GHz band on AP505/AP510/AP560 which allows the AP to switch to this predefined channel in case there is a Rader signal detected by DFS algorithm on the operational channel. Note: feature already exists in Distributed mode. Requires XCA 4.56.01 release.
  e. AP “Name” in the Beacon in Campus mode – Ability to add AP hostname to the beacon. Requires XCA 4.56.01 release.

- WiNG 7.2 added ability to enable/disable 11ax functionality on the AP 5505/AP510/AP560:

  ```
  ap510-137D1E(config-device-94-9B-2C-13-7D-1E-if-radio2)#?
  Radio Mode commands:
    11axSupport Configure support for 802.11ax mode

  ap510-137D1E(config-device-94-9B-2C-13-7D-1E-if-radio2)#no 11axSupport
  ap510-137D1E(config-device-94-9B-2C-13-7D-1E-if-radio2)#11axSupport
  ```

  The default value is “11axSupport” which enables the 11ax mode on the radio.

- AP 5xx 11ax radio functionality limitations:
  - 11ax enabled WLAN must be on the 1st BSS
  - 40Mhz channels are not supported on 2.4 Ghz radio.
  - Customer rates are not supported – use default rates only.
  - Channel width of 160Mhz is not supported.

- AP 5xx now supports 512 clients per radio.

- When adopting any AP running firmware prior to WING 7.2, wireless clients fail to associate to APs running prior version with reason code “max-clients on wlan associated”. WLANs mapped to those APs will need to use the workaround of setting “wireless-client count-per-radio 256”.

- There is a configuration error issue when adopting APs that don't support RRM-TPC report with firmware prior to 7.2.0.0 and 5.9.6. Workaround: Disable RRM-TPC in WLAN when it is adopting AP5xx with firmware prior to 7.2.0.0 or other APs running 5.9.5 or earlier that don't support RRM-TPC.

<u>New in v7.1.2</u>

1. Following features are now supported in WiNG 7.1.2:

   <u>Distributed and Campus mode:</u>

   - ExtremeLocation support (limited):
     - Following features are supported:
       - Presence
     - Following is not yet fully supported in this release:
       - Zone tracking (requires 6 sec feed interval)
       - Position tracking (requires 1 sec feed interval)
   - IoT support:
     - iBeacon
     - Eddystone
     - iBeacon Scan
     - Eddystone-url Scan

   <u>Distributed mode</u>:

   a. LACP support for AP 5xx.
   b. USP port support on AP 5xx.
   c. Strict 11ac association for AP5xx.

   <u>Campus mode</u>:

   d. Smart-RF (requires ExtremeCloudAppliance 4.36.03 release). Note: select-shutdown feature is not supported in this release.

2. AP560h antenna options – there are two options for AP560h internal antenna:
   ap560(config-device)#antenna-id internal ?
   internal-560h-30 *Internal 560h eight feed 30 degree sector antenna* (Default option)
   internal-560h-70 *Internal 560h eight feed 70 degree sector antenna*

3. ExtremeAnalytics (Purview) important notes:

   a. Application policy for ExtremeAnalytics DPI engine can be configured from WING controllers for ExtremeAnalytics DPI engine supporting APs. WING controllers however don't support ExtremeAnalytics DPI engine in current release. Support for same will be enabled on WING controllers in a future release.
   b. Application and application category names are different in legacy application policy and Purview application policy rules.
   c. RTP and TCP-RTT metadata configuration and extraction is not supported in current release for Purview DPI engine supporting APs.
   d. Application groups for ExtremeAnalytics DPI engine applications will not work with NSight release 5.9.3.
   e. Custom application configuration no longer supports multiple url-lists for hostnames, common names and server names and port-proto rules. If custom application configuration exists with multiple such rules, make sure to split it up

into multiple custom application configuration each containing only one rule for url-list, common name, server name and port-proto rule as applicable.

f. WiNG 7.1.2 doesn't have UI support for configuring Purview (ExtremeAnalytics) policy – configuration only available in CLI.

New in v7.1.1

1. WiNG 7.1 controllers can adopt WiNG 5.9.4 and WiNG 5.9.4.1 APs in this release. WiNG 5.9.4 APs should be in separate rf-domain from WiNG 7.1 APs.
2. Following features are now supported in WiNG 7.1.1:

   Distributed mode:

   a. REST API
   b. ADSP sensor – dedicated mode only (refer to matrix below for features supported).
   c. Smart-rf Select-shutdown
   d. Dynamic VC (note: heterogenous AP deployment is not supported yet).
   e. IPsec and L2TPv3 tunneling
   f. Layer 3 assisted mobility
   g. NAT
   h. Bonjour support
   i. WiNG extensions (including scan assist)
   j. USB port

   Campus mode:

   a. ADSP sensor
   b. Energy Efficient ethernet

3. AP 510e - configuring "antenna-id" command in device/profile of the AP is needed to radio to operate.
   "antenna-id group-1 antenna_name"– use for 2.4/5GHz dual band antenna types.
   "antenna-id group-2 antenna_name" - use for 5GHz single band antenna types.
4. For AP 510e when using high gain directional antennas in 4x4 mode – lower channels are not supported, and radio will not be enabled. Reference antenna guide for correct channel, power and antenna settings.

New in v7.1

1. WiNG 7.1 will only support AP 505/510 in this release. 11AC ExtremeWireless WiNG APs will be added in later release.
2. Following features are not supported on AP505/510 in this release:
   Distributed mode:
   - NSight
   - ADSP sensor
   - Location sensor (all modes)
   - MCX and MCX related features
   - REST API
   - Layer 3 assisted mobility
   - Smart-RF:

  - Select-shutdown
  - Dual 5Ghz radio support
- Client Bridge
- IoT/BLE
- AVC and Application Policy
- Dynamic VC and Heterogenous AP deployment has not been tested
- NAT
- Bonjour support
- WiNG extensions (including scan assist)
- IPsec and L2TPv3 tunneling
- LACP
- Receive Sensitivity
- PPPoE
- 802.11k
- RTLS (Aeroscout, Centrak, and Ekahau)
- USB port is not supported yet
- Sniffer redirect

Campus mode:

- 802.11r (Fast Transition)
- Smart-RF
- Client Load Balance/Band Steering
- Airtime Fairness
- Admission Control
- IoT/BLE/Thread
- ADSP sensor
- ExtremeLocation sensor
- Positioning
- RTLS (Aeroscout, Centrak, and Ekahau
- Probe Suppression on Low RSS
- USB port not supported

3. Smart-rf for dual 5Ghz radio on AP510 is not supported currently – assign channel and power statically.
4. WiNG 7.1 controllers can adopt WiNG 5.9.3 APs only in this release. WiNG 5.9.3 APs should be in separate rf-domain from WiNG 7.1 APs.
5. Default BLE beacon tx power must be changed to value permitted for 7632/62 platform to permit adoption – i.e. beacon tx power 10.
6. AP 505/510 - default password in all modes is admin123 for all operational modes.
7. Setting of custom rates is not supported in this release – use default rates.

Deriving secondary IP

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

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

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

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

7. DFS TABLES, SENSOR AND RADIO SHARE

1. Following is the DFS support in WiNG 7.6.3.1 for the supported radio platforms:

Product	Master DFS FCC	Master DFS IC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS IC	Client DFS ETSI	Client DFS Japan
AP 302W	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 305C	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 305CX	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 410C	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 460C	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 460S6C	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 460S12C	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 310i	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 310e	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 360i	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
AP 360e	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
AP 410i	Enabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled
AP 410e	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
AP 460i	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 460e	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 505i	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 505e	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 510i	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 510e	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a
AP 560i	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a

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 560e	Enabled	Enabled	Enabled	Enabled	Disabled	n/a	n/a	n/a

2. Air Defense sensor capabilities interop matrix supported on the 802.11ax APs
   Refer to ADSP 10.5 release notes.

3. Radio Share functionality
   Refer to ADSP 10.5 release notes.

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 7.6.3.1
(AP7632/AP7662/AP7612)
CVE-2020-24586 – Not clearing fragments from memory when (re)connecting to a network
CVE-2020-24587 – Reassembling fragments encrypted under different keys
CVE-2020-24588 – Accepting non-SPP A-MSDU frames

WiNG 7.6.3
CVE-2020-24586 – Not clearing fragments from memory when (re)connecting to a network
CVE-2020-24587 – Reassembling fragments encrypted under different keys
CVE-2020-24588 – Accepting non-SPP A-MSDU frames

WiNG 7.6.2
CVE-2020-24586 – Not clearing fragments from memory when (re)connecting to a network
CVE-2020-24587 – Reassembling fragments encrypted under different keys
CVE-2020-24588 – Accepting non-SPP A-MSDU frames

WiNG 7.6.1
CVE-2020-1968 – Racoon attack

WiNG 7.6.0
PSIRT-43: RCE vulnerability in hotspot interface - thanks to reactivity@wearehackerone.com for discovering and reporting this vulnerability to Extreme Networks, Inc.

WiNG 7.5.2
No updates in this release

WiNG 7.5.1
No updates in this release

WiNG 7.4.1
No updates in this release

WiNG 7.4.0
No updates in this release

WiNG 7.3.1
No updates in this release

WiNG 7.3.0
CVE-2019-16275: hostapd before 2.10 Allow an incorrect indication of disconnection in certain situations because source address validation is mishandled.
CVE-2019-13012: GNOME GLib (aka glib2.0).

WiNG 7.2.1
CVE-2018-2048: Wget vulnerability in version 1.16
CVE-2019-13377: Timing-based side-channel attack against WPA3's Dragonfly handshake when using Brainpool curves

WiNG 7.2.0
Linux Kernel 4.1.51 Patch Update for Vulnerability: TCP SACK panic, CVE-2019-11477.
WPA supplicant updated to v2.8 to mitigate following WPA3 vulnerabilities: CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499.

WiNG 7.1.2
Both Campus and Distributed mode are using same openSSL version 1.0.2q

WiNG 7.1/7.1.1
No updates in this release

9. ISSUES FIXED

Following issues have been fixed in WiNG 7.6.3.1 release:

CR/ESR	Description
CFD-6540	When ssh to VX getting error: Unable to load host key
CFD-6373	AP302w 7.6.0.1 back to default after reload
WOS-2474	QCA patches for CVE-2020-24586, CVE-2020-24587, CVE-2020-24588

10. KNOWN ISSUES

CR/SPR	Headline	Comments
WOS-1230	AP460: there is no output from "show bluetooth radio"	

CR/SPR	Headline	Comments
WOS-1655	AP302W: wireless client not able to connect to 16th BSS on 5ghz	
WOS-1774	Radio1 sensor on AP302W (mode 2) supports full 2.4 GHz only	
WOS-1991	7.6.1.0:07R Hanshow: Esl Usb Dongle: On Ap305cx Kernel panic	
WOS-2000	FT authentication not supported on AP410C client bridge	
WOS-2073	Client Bridge: Vendor name shows Aerohive instead of Extreme	
WOS-2219	ESL USB interface: packet capture on the USB interface captures only incoming packet	
WOS-2222	ESL USB Dongle: ping with source as USB interface fails with ping: unknown iface USB error	
WOS-2293	QoS doesn’t work for client on AP302W client bridge	
CFD-6527	VX9000 7.6.1.0 Does not send LDAP request	
CFD-6540	When ssh to VX getting error: Unable to load host key	
CFD-6587	VX9000 crash after upgrade 7.6.2.0-018R	

11. KNOWN NOVA GUI ISSUES

WOS-2429	NOVA_NX75xx: Radio ID (R1 , R2 and R3) notification not present in smart-rf neighbor report	
WOS-2371	NOVA: Statistics --> Devices --> Default does not display the IP address for the controller. Works fine for the AP's adopted	
WOS-2414	NOVA: policies>radius user pool, error message when 'apply' after switch from 'limited' to 'unlimited'	
WOS-2432	NOVA UI_NX75xx : Single VLAN change to VLAN pool and max client set to 0, when change the VLAN 1 to any other VLAN	
WOS-2438	NOVA_NX75xx: WIPS signature enable option, doing reverse behavior	
WOS-2445	NOVA_NX75xx: QOS-Map enable Option not available in GUI	
WOS-2446	NOVA_NX75xx: Port channel "enabled" but status shows disabled	
WOS-2454	NOVA_NX75xx: 5Ghz ac/ax data rates not available in profile	

12. GLOBAL SUPPORT

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)
For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com
By Web: www.extremenetworks.com/support/

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

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