Extreme™
Customer-Driven Networking

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

WiNG 7.1.0.0-138R Release Notes

CONTENTS

OVERVIEW

WiNG 7.1 brings unique software platform to the market combining the scale, features and functions of ExtremeWireless and ExtremeWireless WiNG, offering flexible deployment option covering both campus mode and distributed mode. WING 7.1 introduces support for new 11ax AP portfolio for ExtremeWireless OmniEdge product line.

1. PLATFORMS SUPPORTED

Note:
APXXXX-LEAN-7.1.0.0-138R.img - built **without GUI component**. AP lean images are also bundled within controller full image.
NXXXXX-LEAN-7.1.0.0-138R.img – built **without AP images.**

WiNG 7.1 supports the following platforms with the corresponding firmware images:

Controller Platform	Firmware Image
NX 9500/ NX 9510	NX9500-7.1.0.0-138R.img, NX9500-LEAN-7.1.0.0-138R.img
NX 9600 / NX 9610	NX9600-7.1.0.0-138R.img, NX9600-LEAN-7.1.0.0-138R.img
NX 75XX	NX7500-7.1.0.0-138R.img, NX7500-LEAN-7.1.0.0-138R.img
NX 5500	NX5500-7.1.0.0-138R.img, NX5500-LEAN-7.1.0.0-138R.img

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

Virtual Platform	Firmware Image
VX 9000[1]–production iso/img image	VX9000-INSTALL-7.1.0.0-138R.iso, VX9000-7.1.0.0-138R.img, VX9000-LEAN-7.1.0.0-138R.img
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-7.1.0.0-138R.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
AP505/510	AP5xx-7.1.0.0-138R.img AP5xx-LEAN-7.1.0.0-138R.img (included in all Controller images)

2. NEW FEATURES IN WING 7.1

AP 505/510 support

Extreme Networks is adding a new family of turbo charged Access Points to Extreme's Smart OmniEdge portfolio with 802.11ax (Wi-Fi 6) technology that enables enterprises to support more users and IoT devices with greater performance and efficiency; enhancing the user experience. The ExtremeMobility AP 505i, AP 510i and AP 510e access points represent the latest in Wi-Fi technology, incorporating software programmable dual radio, 4x4 802.11ax which is the 6th generation of 802.11 technology, dual GbE or Multi-Rate Gig ports, integrated Bluetooth radio for guest engagement and analytics or supporting IoT connectivity with Thread™.

Rather than focusing on top speed, 802.11ax technology increases the efficient use of available spectrum, supporting more devices simultaneously and ensuring each device achieves greater performance. It is projected that 802.11ax will deliver up to 182% improvement over 802.11ac. These new access points adapt seamlessly to the diverse needs of wireless users and IoT devices. While prior generations addressed greater performance, 802.11ax uniquely addresses greater capacity, supporting more devices simultaneously and making better use of available spectrum with increased efficiencies. 802.11ax dynamically adjust bandwidth for different devices / applications as required.

- Flexible Deployment Modes

  ExtremeMobilty AP 505i, AP 510i and AP 510e are part of the Smart OmniEdge portfolio. As such, these access points will be available to operate running WiNG 7 OS with different operational modes: Campus or Distributed.
- Please review section 6 – Important notes for features not supported in this release.

3. GENERAL INFORMATION FOR FIRMWARE UPGRADE / DOWNGRADE

3.1 Device Upgrade/Downgrade matrix

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

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

Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
AP 505/510	V7.1 onwards	V7.1	AP 5xx 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 General Important Notes on Upgrade / Downgrade

IMPORTANT:

- **AP505i/510 that have rev AA on the label – need to be upgraded to release firmware prior to operation. Please refer to instructions posted on** https://extr.co/2Tyivv3.

- WiNG controller must be running a WiNG 7 controller code to be able to recognize, adopt and upgrade 11ax APs.
- Extreme Cloud Appliance must be running version 4.36.01 or later to be able to adopt and upgrade AP 505/510.
- Always create config back-up before the upgrade.
- Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. Where APs are powered through PoE connections to WLAN controllers, the controller needs to stay up during the upgrade process.
- Both the WiNG controller and WiNG 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.

3.3 Device Upgrade/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.

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

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

3.4 AutoInstall

AutoInstall in WiNG 5 works via the DHCP server. This requires the definition of Vendor Class and three sub-options that can be either sent separately or under option 43:
Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to enter as a string: —ftp://admin:admin123@192.168.1.10‖)
Option 187 - defines the firmware path and file name
Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the VLAN interface which is being used to perform the above autoinstall.
DHCP vendor class for platforms is noted below:
Appliances:

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

AP:

- WingAP.AP505
- WingAP.AP510

4. FIRMWARE UPGRADE / DOWNGRADE – CONTROLLERS

4.1 Platform Important notes

1. VX 9000:
   a. Secondary storage: VX 9000 has disk size limitation on the default disk of 2TB. However, when a secondary virtual disk is used, VX 9000 can support disks size larger than 2TB
      - Enabling secondary storage does not copy data files to the new location
      - It is recommended immediately after provisioning the guest instance, before enabling NSight or Captive-Portal
      - If the secondary storage needs to be enabled after NSight/Captive-portal, it is recommended to back up the database, and restore the database after secondary storage is enabled.
      - If the VX 9000 instance is not a primary (replica-set member), the database server will perform full data sync after it is restarted with the new secondary storage disk.
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 the upgrade of all the corresponding devices.
Available firmware on the controller can be checked using the below command:
nx9600#show device-upgrade versions

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

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

- **Manual Upgrade**

Firmware upgrade can be initiated on a single or a list of Aps using the below command.
nx9600#device-upgrade 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**

Firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. Firmware upgrade on the Aps follows the configured upgrade time.
nx9600# device-upgrade all ?
no-reboot No reboot (manually reboot after the upgrade)
reboot-time Schedule a reboot time
staggered-reboot Reboot one at a time without network being hit
upgrade-time Schedule an upgrade time

- **Upgrade through RF Domain manager**

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

4.3 Auto Upgrade

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

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

5. FIRMWARE UPGRADE/DOWNGRADE – INDEPENDENT APS

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

5.1 Standalone AP Upgrade / 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. From CLI the command is —reload.

5.2 Virtual Controller upgrade

1. If there are no adopters/controllers in the network and several APs are required to be upgraded, use WiNG Virtual Controller (VC) mode to perform bulk AP upgrades.
2. Use WiNG configuration wizard to configure Virtual Controller (VC) on the AP.
3. When done with the WiNG configuration wizard, upgrade the VC to the latest image by using following command:
   ap510-1349AC#upgrade tftp://<hostname|IP>path/file
4. After 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 Virtual Controller (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 ExtremeCloud Appliance

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 ExtremeCloud Appliance, upon adoption ExtremeCloud Appliance will automatically upgrade the AP image.
3. If the AP is adopted by a WiNG 7 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 v7.1

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

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

- 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

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 – please 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 – please use default rates.

Deriving secondary IP

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

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.

8. DFS TABLES, SENSOR AND RADIO SHARE

1. Following is the DFS support in WiNG 7.1 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 505	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled
AP 510	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled

2. Air Defense sensor capabilities are NOT supported on the 802.11ax APs in this release.

As a dedicated sensor	WIPS & Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Test	Connection Troubleshooting	WVA
AP 505/510	No	No	No	No	No	No	No	No

3. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is NOT available on the 802.11ax APs in this release:

In Radio Share mode	WIPS & Advanced Forensics	Spectrum Analysis[2]	Advanced Spectrum Analysis[3]	Live RF	Live View	AP Test[5]	Connection Troubleshooting	WVA
AP 505/510	No	No	No	No	No	No	No	No

9. VULNERABILITY UPDATES

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

WiNG 7.1

No updates in this release

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

10. KNOWN ISSUES

Following issues are known issues in WiNG 7.1:

CQ/ SPR	Headline	Comments
WING-37960	Setting custom rates is not supported until WiNG 7.2 release.	Please use default rates until support is provided.
WING-38275	Multigig support shows low throughput with ExosX620	
WING-38282	Loyalty App detection with AVC cannot be used in ExtremeGuest.	Loyalty app with localization FQDN works
WING-38293	AP 5xx has intermittent issues with forwarding IPv6 traffic	
WING-38304	Repeated radar detection when smart-rf channel list only includes DFS channels – can put AP in the state where it's not able to serve clients	
WING-38337	AP 510i is not operating in 40Mhz channel consistently	
WING-38381	LED is Keep on Blinking after AP 5xx adopted Extreme Cloud Appliance	Functionality is not impacted.
WING-38393	AMSDU receive aggregation is not working properly and might impact AMSDU capable clients (for example iOS devices)	
WING-38401	Admission Control doesn't function properly in Centralized mode	
WING-38415	In Fabric Attach setup using tagged Management VLAN, automatic discovery of operation mode is not working correctly.	
WING-34838	If channel-list id defined under smart-rf policy, when using dual 5Ghz mode – AP will not be able to switch channels when radar is detected	Remove smart-rf channel list as is not supported for dual 5Ghz mode.

GLOBAL SUPPORT:

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

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

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

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

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