

## WiNG 7.9.1.0-022R Release Notes

### CONTENTS

|   |           |
|---|-----------|
| <b>Overview .....</b>   | <b>2</b>  |
| <b>1. Platforms Supported .....</b>                                 | <b>2</b>  |
| <b>2. New Features in WiNG 7.9.1.0.....</b>                         | <b>3</b>  |
| 2.1 New features .....  | 3         |
| <b>3. General Information for Firmware Upgrade / Downgrade.....</b> | <b>4</b>  |
| 3.1 Device Upgrade or Downgrade matrix .....                        | 4         |
| 3.2 Software Compatibility Matrix with Extreme Products.....        | 6         |
| 3.3 Important Notes on Upgrade or Downgrade.....                    | 7         |
| 3.4 Device Upgrade or Downgrade Procedure .....                     | 7         |
| 3.5 AutoInstall.....  | 8         |
| <b>4. Firmware Upgrade or Downgrade – Controllers .....</b>         | <b>9</b>  |
| 4.1 Platform Important Notes .....                                  | 9         |
| 4.2 Device Upgrade Options .....                                    | 10        |
| 4.3 Auto Upgrade.....   | 11        |
| <b>5. Firmware Upgrade or Downgrade – Independent APs .....</b>     | <b>11</b> |
| 5.1 Standalone AP Upgrade or Downgrade .....                        | 11        |
| 5.2 Virtual Controller upgrade.....                                 | 11        |
| 5.3 Upgrading APs through WiNG controller.....                      | 12        |
| <b>6. Important Notes.....</b>                                      | <b>12</b> |
| <b>7. DFS Tables, Sensor and Radio Share.....</b>                   | <b>23</b> |
| <b>8. Vulnerability updates .....</b>                               | <b>24</b> |
| <b>9. Issues Fixed .....</b>  | <b>27</b> |
| <b>10. Known Issues .....</b>                                       | <b>27</b> |
| <b>11. Global Support .....</b>                                     | <b>28</b> |

## OVERVIEW

WiNG 7.9.1.0 release continues to improve unique WiNG7 software architecture that combines the scale, features, and functions of ExtremeWireless WiNG™, offering flexible deployment options. WiNG 7.9.1.0 is a minor release that extends feature support for new 6E Universal AP portfolio for ExtremeWireless WiNG™ product line and provides stability fixes.

## 1. PLATFORMS SUPPORTED

### Note:

APXXXX-LEAN-7.9.1.0-022R.img - built **without GUI component**. AP lean images are also bundled within controller full image.

NXXXXX-LEAN-7.9.1.0-022R.img – built **without AP images**.

WiNG 7.9.1.0 supports the following platforms with the corresponding firmware images:

| Controller Platform | Firmware Image  |
|---------------------|---|
| NX9600 / NX9610     | NX9600-7.9.1.0-022R.img, NX9600-LEAN-7.9.1.0-022R.img |
| NX75XX              | NX7500-7.9.1.0-022R.img, NX7500-LEAN-7.9.1.0-022R.img |
| NX5500              | NX5500-7.9.1.0-022R.img, NX5500-LEAN-7.9.1.0-022R.img |

| Virtual Platform                              | Firmware Image   |
|---|--|
| VX9000 <sup>1</sup> –production iso/img image | VX9000-INSTALL-7.9.1.0-022R.iso, VX9000-7.9.1.0-022R.img, VX9000-LEAN-7.9.1.0-022R.img |
| VX9000 – demo iso image                       | VX9000-DEMO-INSTALL-7.9.1.0-022R.iso <sup>2</sup>                                      |

<sup>1</sup>VX9000 image has default 64 AP license.

<sup>2</sup>The VX demo image is a 60-day trial image of the VX9000 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   |
|---|--|
| AP5010  | AP5xxx-LEAN-7.9.1.0-022R.img (included in all Controller images) |
| AP302W  | AP302W-LEAN-7.9.1.0-022R.img (included in all Controller images) |
| AP305C/AP305CX<br>AP305C-1                      | AP3xxC-LEAN-7.9.1.0-022R.img (included in all Controller images) |
| AP410C/AP460C<br>AP460S6C/AP460S12C<br>AP410C-1 | AP4xxC-LEAN-7.9.1.0-022R.img (included in all Controller images) |

| AP Platforms                      | Firmware Image   |
|-----------------------------------|--|
| AP310/360<br>AP310i-1<br>AP310e-1 | AP3xx-7.9.1.0-022R.img<br>AP3xx-LEAN-7.9.1.0-022R.img (included in all Controller images)      |
| AP410/460<br>AP410i-1             | AP4xx-7.9.1.0-022R.img<br>AP4xx-LEAN-7.9.1.0-022R.img (included in all Controller images)      |
| AP505/510/560<br>AP510i-1         | AP5xx-7.9.1.0-022R.img<br>AP5xx-LEAN-7.9.1.0-022R.img (included in all Controller images)      |
| AP7522                            | AP7522-7.7.1.7-005R.img<br>AP7522-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP7532                            | AP7532-7.7.1.7-005R.img<br>AP7532-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP7562                            | AP7562-7.7.1.7-005R.img<br>AP7562-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP8533                            | AP8533-7.7.1.7-005R.img<br>AP8533-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP8432                            | AP8432-7.7.1.7-005R.img<br>AP8432-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP7612                            | AP7612-7.7.1.7-005R.img<br>AP7612-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP7632                            | AP7632-7.7.1.7-005R.img<br>AP7632-LEAN-7.7.1.7-005R.img (included in all NX controller images) |
| AP7662                            | AP7662-7.7.1.7-005R.img<br>AP7662-LEAN-7.7.1.7-005R.img (included in all NX controller images) |

## 2. NEW FEATURES IN WING 7.9.1.0

### 2.1 New features

SES-Imagotag ESL Support (except AP5010 – future release)

AP5010 Client Bridge Support

AP5010 MCX Mesh Support

Increased number of Supported GRE Tunnels for IQ Engine AP Termination

- NX5500 - Up to 512 GRE Tunnels
- NX75XX – Up to 1000 GRE Tunnels
- NX9610 – Up to 1024 GRE Tunnels

Added “IL” support for Israel on AP5010

XIQ Integration Improvements

NOVA UI Enhancements

- Option to configure Default Gateway
- Support to disconnect wireless clients
- Advanced tab for radio interface
- 6 GHz channel and power configuration for smart rf policy
- 6 GHz Meshpoint data rates
- Meshpoint configuration support for AP410C-1
- Configure EAP types in WLAN config page
- Added Stop-only in AAA radius server accounting settings
- Guest-Management policy support
- Captive portal policy is now available in Policies section
- Support to configure UMUSCHEDBRCMONLY parameter
- Configure SAE Authentication under Bridge Tab
- Option to edit static routes in ROUTING tab
- Health- [RF Domain Specific] > Radios

This release does not support the following:

- ADSP on 6 GHz Radio
- VMM
- PPPoE

To be supported in future software release:

| CR       | Headline                       |
|----------|--------------------------------|
| WOS-1804 | ADSP on 6 GHz Radio for AP5010 |
| WOS-4784 | Imagotag Validation for AP5010 |

### 3. GENERAL INFORMATION FOR FIRMWARE UPGRADE / DOWNGRADE

#### 3.1 Device Upgrade or Downgrade matrix

The 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.

| Adaptive with the controller         | Upgrade from                      | Downgrade to                      | Notes   |
|--------------------------------------|-----------------------------------|-----------------------------------|---|
| AP7532/AP7522                        | v5.5.3.1 onward, excluding v5.6.x | v5.5.3.1 onward, excluding v5.6.x | AP image is contained within the NX controller image  |
| AP7612/AP7632/AP7662                 | v5.9.1                            | v5.9.1                            | AP image is contained within the NX controller image  |
| AP8533/AP8432                        | v5.8.4 onward                     | v5.8.4 onward                     | AP image is contained within the NX controller image  |
| AP5010                               | v7.9 onward                       | v7.9                              | AP5xxx image is contained within the controller image |
| AP505/AP510i                         | v7.1 onward                       | v7.1                              | AP5xx image is contained within the controller image  |
| AP510i -1                            | v7.7.1 onward                     | v7.7.1                            | AP5xx image is contained within the controller image  |
| AP510e                               | v7.1.1 onward                     | v7.1.1                            | AP5xx image is contained within the controller image  |
| AP560i-FCC                           | v7.1.1 onward                     | v7.1.1                            | AP5xx image is contained within the controller image  |
| AP560h-FCC                           | v7.1.2 onward                     | V7.1.2                            | AP5xx image is contained within the controller image  |
| AP410/AP460i                         | v7.3.0.0 onward                   | v7.3.0.0                          | AP4xx image is contained within the controller image  |
| AP410i-1                             | v7.7.1 onward                     | v7.7.1                            | AP4xx image is contained within the controller image  |
| AP410/AP460e                         | v7.3.0.0 onward                   | v7.3.0.0                          | AP4xx image is contained within the controller image  |
| AP310i/e                             | v7.3.1.0 onward                   | v7.3.1.0                          | AP3xx image is contained within the controller image  |
| AP310i-1<br>AP310e-1                 | v7.7.1 onward                     | v7.7.1                            | AP3xx image is contained within the controller image  |
| AP360i/e                             | v7.5.1.1 onward                   | v7.5.1.1                          | AP3xx image is contained within the controller image  |
| AP305C/AP305CX                       | v7.5.2.0 onward                   | v7.5.2.0                          | AP3xxC image is contained within the controller image |
| AP305C-1                             | v7.7.1.3 onward                   | v7.7.1.3                          | AP3xxC image is contained within the controller image |
| AP302W                               | v7.6.0.0 onward                   | v7.6.0.0                          | AP302W image is contained within the controller image |
| AP410C/AP460C/<br>AP460S12C/AP460S6C | v7.6.2.0 onward                   | v7.6.2.0                          | AP4xxC image is contained within the controller image |

| Adaptive with the controller | Upgrade from    | Downgrade to  | Notes   |
|------------------------------|-----------------|---------------|---|
| AP410C-1                     | v7.7.1.3 onward | v7.7.1.3      | AP4xxC image is contained within the controller image |
| NX5500                       | v5.8 onward     | v5.8 onward   | NX5500 is supported starting with v5.8                |
| NX75XX                       | v5.5.2 onward   | v5.5.2 onward | <i>Note:</i> WiNG 5.6 does not support NX7500         |
| NX96XX                       | v5.5.6 onward   | v5.5.6 onward | NX96XX is not supported with v5.6.x and v5.7.x        |
| VX9000                       | v5.6 onward     | v5.6 onward   |   |

### 3.2 Software Compatibility Matrix with Extreme Products

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

| WiNG       | XCC     | ADSP        | ExtremeGuest         | ExtremeLocation |
|------------|---------|-------------|----------------------|-----------------|
| WiNG 7.6.4 | 5.36.03 | 10.5        | n/a                  | n/a             |
| WiNG 7.7.0 | 5.46.01 | 10.5        | ExtremeGuest 6.0.2.0 | n/a             |
| WiNG 7.7.1 | n/a     | 10.5.0-05a6 | n/a                  | n/a             |
| WiNG 7.9.0 | n/a     | 10.5.0-5B3  | n/a                  | n/a             |
| WiNG 7.9.1 | n/a     | 10.6.0-04   | n/a                  | n/a             |

### 3.3 Important Notes on Upgrade or Downgrade

- WiNG controller must be running a WiNG7 controller code to be able to recognize, adopt and upgrade 6E and 11ax APs.
- Always create configuration backup 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.
- For 6E and 11ax APs, both the WiNG controller and WiNG AP must be upgraded to the same firmware versions – a firmware mismatch can cause network disruptions. When upgrading, upgrade the controller first, then upgrade the APs. When downgrading, downgrade the APs first, then downgrade the controller.

### 3.4 Device Upgrade or Downgrade Procedure

1. Copy the firmware image for the device that needs to be upgraded (ftp/tftp server). Refer to section 1. *Platforms Supported*, for the correct firmware image to use 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 sent either 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 filename
- Option 188 - defines the config path and filename

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

The DHCP vendor class for the platform types and models is as described below.

| Controller Platform | DHCP Option Vendor Class |
|---------------------|--------------------------|
| NX5500              | WingNX.NX5500            |
| NX7500              | WingNX.NX7500            |
| NX9600/NX9610       | WingNX.NX9000            |

| AP Platform | DHCP Option Vendor Class |
|-------------|--------------------------|
| AP5010      | WingAP.AP5010            |
| AP302W      | WingAP.AP302W            |
| AP305C      | WingAP.AP305C            |
| AP305CX     | WingAP.AP305CX           |
| AP305C-1    | WingAP.AP305C-1          |
| AP410C      | WingAP.AP410C            |
| AP460C      | WingAP.AP460CC           |
| AP460S6C    | WingAP.AP460CC           |
| AP460S12C   | WingAP.AP460S12CC        |
| AP410C-1    | WingAP.AP410C-1C         |
| AP310       | WingAP.AP310             |
| AP360       | WingAP.AP360             |



| AP Platform       | DHCP Option Vendor Class |
|-------------------|--------------------------|
| AP310i-1          | WingAP.AP310-1           |
| AP310e-1          | WingAP.AP310-1           |
| AP410             | WingAP.AP410             |
| AP460             | WingAP.AP460             |
| AP505/AP510/AP560 | WingAP.AP510             |
| AP510i-1          | WingAP.AP510-1           |
| AP7522            | WingAP.AP7522            |
| AP7532            | WingAP.AP7532            |
| AP7562            | WingAP.AP7562            |
| AP7612            | WingAP.AP7612            |
| AP7632            | WingAP.AP7632            |
| AP7662            | WingAP.AP7662            |
| AP8432            | WingAP.AP8432            |
| AP8533            | WingAP.AP8533            |

## 4. FIRMWARE UPGRADE OR DOWNGRADE – CONTROLLERS

### 4.1 Platform Important Notes

- VX9000:

Secondary storage: VX9000 has disk size limitation on the default disk of 2TB. However, when a secondary virtual disk is used, VX9000 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 VX9000 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.
- 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 an “erase startup-config”.

## 4.2 Device Upgrade Options

WiNG 7.x supports device firmware upgrade from the controller. For firmware upgrade through the controller, upload the firmware image to a controller and use it to upgrade 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, upload a new image using the following command:

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

After uploading device firmware to the controller, the following options are available for device firmware upgrade:

- **Manual Upgrade**

A 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 happens through the controller.

## 5. FIRMWARE UPGRADE OR DOWNGRADE – INDEPENDENT APs

### 5.1 Standalone AP Upgrade or Downgrade

1. Copy the firmware image for the device that requires an upgrade to your ftp/tftp server. Refer to 1. Platforms Supported for the 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:** The Virtual Controller is not supported on Universal APs.

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

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\*'

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 v7.9.1

- SES-Imagotag ESL Support (except AP5010)
- AP5010 Client Bridge Support
- AP5010 MCX Mesh Support
- Increased number of Supported GRE Tunnels for IQ Engine AP Termination
- Added “IL” support for Israel on AP5010
- XIQ Integration Improvements
- NOVA UI Enhancements

### New in v7.9.0

- AP5010 6E Support
- For new and existing/upgrade installations
  - NOVA UI is **Enabled** by default
  - Flash UI is **Disabled** by default (can be manually enabled via CLI)
- AP/Controller Version Support
  - WiNG 7.7.x.x – 11ac Wave 1 and Wave 2 APs
  - WiNG 7.9.x.x – 11ax/6E APs and Controllers
- 11ac Wave1/Wave2 Default AP Profile
  - In order to remain at WiNG 7.7.x.x, Wave 1 and Wave 2 AP Profiles will default to: *'enforce version adoption none'*
- Universal 6E and 11ax APs
  - Reminder: **No** Virtual Controller Support

**New in v7.7.1**

Power mode CLI is updated to include AT power configuration.

# power-config mode ?

3af Force AP comes up at 3af power mode

3at Force AP comes up at 3at power mode

auto Power detection auto mode

**New in v7.6.4**

- Following campus features are introduced in this release. Refer to XCC 5.36.03 User Guide for more information.
  - Band steering per SSID (WLAN service) for Wi-Fi6 APs

**New in v7.6.3**

- 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 loses 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 follows 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.

### New in v7.4.0

- Following features are now supported in WiNG 7.4.0:

#### Distributed mode:

- Secure ImagoTag connectivity for all 11ax APs and AP8432.
  - **IMPORTANT** 7.4.0.0 does not 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 V CLOUD
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.
- o MCX support on AP4xx

#### Campus mode:

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

#### New in v7.3.1

- Following features are now supported in WiNG 7.3.1:

##### Distributed mode:

- o Virtual controller support on wifi6 APs. Refer to WiNG 7.3.1.1 release note for details.
- o Imagetag 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:

- o ADSP support:
  - Spectrum Analysis.
  - AP Test
- o SU/MU-11ac Beamforming is supported on AP505/510/560/410/460
- o STBC/SU MU\_MIMO is supported in HE field on AP505/510/560/410/460
- o OFDMA needs to be disabled for AP500 and AP400.
- o 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, 3<sup>rd</sup> 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, will not 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 cannot 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 AP8533 profile – not ANYAP profile.
  - BLE sensor and smart-sensor currently cannot be enabled together.
  - Smart-sensor feature currently cannot 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.
  - 160 MHz channels are now supported on 5 GHz.
  - Existing ldpc has been turned on by default now.
  - Sniffer re-direct support for 11ax
    - OFDMA, MU-MIMO not supported yet.

## New in v7.2.0

- Following features are now supported in WiNG 7.2.0:

### Distributed and Campus mode:

- 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 5 GHz split radio mode.

### Distributed mode:

- AeroScout RTLS is now supported on AP5xx.
- 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:

- RTLS – AiristaFlow (EKAHAU), AeroScout, Centrak, Euclid.
- OCS support when SMART-RF is not enabled for ADSP sensor and ExtremeLocation sensor support.
- DFS Fallback Channels on 5 GHz 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.
- Client Load Balance on AP505/510 In Campus mode - Adding the support of a predefined channel on the 5 GHz 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.

- 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.
- AP5xx 11ax radio functionality limitations:
  - 11ax enabled WLAN must be on the 1<sup>st</sup> BSS
  - 40 MHz channels are not supported on 2.4 GHz radio.
  - Customer rates are not supported – use default rates only.
  - Channel width of 160 MHz is not supported.
- AP5xx 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.

### **New in v7.1.2**

1. Following features are now supported in WiNG 7.1.2:

#### Distributed and Campus mode:

- 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

Distributed mode:

- LACP support for AP 5xx.
- USP port support on AP 5xx.
- Strict 11ac association for AP5xx.

Campus mode:

- 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:
  - 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.
  - Application and application category names are different in legacy application policy and Purview application policy rules.
  - RTP and TCP-RTT metadata configuration and extraction is not supported in current release for Purview DPI engine supporting APs.
  - Application groups for ExtremeAnalytics DPI engine applications will not work with NSight release 5.9.3.
  - 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.
  - WiNG 7.1.2 does not 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:

  - REST API
  - ADSP sensor – dedicated mode only (refer to matrix below for features supported).
  - Smart-rf Select-shutdown

- Dynamic VC (note: heterogenous AP deployment is not supported yet).
- IPsec and L2TPv3 tunneling
- Layer 3 assisted mobility
- NAT
- Bonjour support
- WiNG extensions (including scan assist)
- USB port

Campus mode:

- ADSP sensor
- Energy Efficient ethernet

3. AP510e - configuring “antenna-id” command in device/profile of the AP is needed to radio to operate.  
“antenna-id group-1 antenna\_name” – use for 2.4/5 GHz dual band antenna types.  
“antenna-id group-2 antenna\_name” - use for 5 GHz single band antenna types.
4. For AP510e 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**

- WiNG 7.1 will only support AP505/510 in this release. 11AC ExtremeWireless WiNG APs will be added in later release.
- 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
- Smart-rf for dual 5 GHz radio on AP510 is not supported currently – assign channel and power statically.
  - 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.

- Default BLE beacon tx power must be changed to value permitted for 7632/62 platform to permit adoption – i.e. beacon tx power 10.
- AP505/510 - default password in all modes is admin123 for all operational modes.
- 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

Following is the DFS support in WiNG 7.9.1.0 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 |
|-----------|----------------|---------------|-----------------|------------------|----------------|---------------|-----------------|------------------|
| AP5010    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP302W    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP305C    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP305CX   | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP410C    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP460C    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP460S6C  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP460S12C | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP310i    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP310e    | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP360i    | Enabled        | Enabled       | Enabled         | Disabled         | Disabled       | Disabled      | Disabled        | Disabled         |

| Product | Master DFS FCC | Master DFS IC | Master DFS ETSI | Master DFS Japan | Client DFS FCC | Client DFS IC | Client DFS ETSI | Client DFS Japan |
|---------|----------------|---------------|-----------------|------------------|----------------|---------------|-----------------|------------------|
| AP360e  | Enabled        | Enabled       | Enabled         | Disabled         | Disabled       | Disabled      | Disabled        | Disabled         |
| AP410i  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | Disabled      | Disabled        | Disabled         |
| AP410e  | Enabled        | Enabled       | Enabled         | Disabled         | Disabled       | Disabled      | Disabled        | Disabled         |
| AP460i  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP460e  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP505i  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP505e  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP510i  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP510e  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP560i  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |
| AP560e  | Enabled        | Enabled       | Enabled         | Enabled          | Disabled       | n/a           | n/a             | n/a              |

- Air Defense sensor capabilities interop matrix supported on the 802.11ax APs

Refer to ADSP 10.5.0-05a5 release notes.

- Radio Share functionality

Refer to ADSP 10.5.0-05a5 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 7.9.1

No updates in this release

### WiNG 7.9.0

No updates in this release

### WiNG 7.7.1

No updates in this release



**WiNG 7.7.0**

No updates in this release

**WiNG 7.6.4**

Following vulnerabilities are fixed for 11ac APs in this release. 11ax APs are already patched in previous releases.

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**

No updates in this release

**WiNG 7.6.2**

Following vulnerabilities are fixed for 11ax APs.

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 – Raccoon 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 7.9.1.0 release:

| CR/ESR                        | Description   |
|-------------------------------|---|
| CFD-8106, CFD-8885, CFD-8619, | AP310's TIM announces buffered data until client disconnects  |
| CFD-8802                      | -1 APs (Distributed) fails to report online in XIQ  |
| CFD-8916                      | WiNG 7.7.1.5 - AP460i/e allows user to incorrectly configure radio1 to 4x4 mode   |
| CFD-8996                      | WiNG v7.9.0.1 Release Notes Missing Vendor Class Identifier for New AP Models   |
| CFD-9014                      | Distributed: [xiq] VX9000, NX controllers and WiNG APs running 7.9.1.0 goes offline from XIQ frequently, controller reboot is required to bring back online |
| CFD-9140                      | Smart-rf: APs selecting channel 36 in-spice of not being configured in smart-rf channel-list after interference recovery.                                   |
| CFD-9201                      | VX9000 7.5.1.6 Crash Files Found Frequently   |
|                               |   |

## 10. KNOWN ISSUES

| CR/SPR   | Description   |
|----------|---|
| WOS-3846 | -1 APs: auto install firmware and autoinstall configuration missing in default profile of -1 APs, when compared with other platform APs |
| WOS-4824 | NOVA cannot show clients sometime due to client system char encoding is not UTF8  |
| WOS-5031 | Windows 10 clients not able to connect to WPA3-Enterprise EAP-TLS network   |
| WOS-5117 | 802.11r Fast-Roaming with EAP-PEAP authentication fails in iphone with iOS version 15.6, works on 16.0 version                          |
| WOS-5134 | AP5010 : Client Bridge establishing in 20 MHz channel width in spite of configuring in 40 MHz on radio 3.                               |
| WOS-5163 | AP5010: Mesh link is not establishing most of the times with channel configured as 'smart', works rarely                                |
| WOS-5191 | Default RTS threshold is wrong  |
| WOS-5112 | NX controllers (NX9600, NX9500 and NX5500) fails to report online in XIQ  |

## 11. 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/](http://www.extremenetworks.com/support/)

By Email: [support@extremenetworks.com](mailto:support@extremenetworks.com)

By Web: [www.extremenetworks.com/support/](http://www.extremenetworks.com/support/)

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

---

©Extreme Networks. 2023. All rights reserved.