FORTINET
High Performance Network Security

FortiWLC

Release 8.5.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Contents

About FortiWLC 8.5.1

FortiWLC release 8.5.1 introduces 802.11ax standards based Universal Access Points (FAP-Us), FAP-U431F/FAP-U433F. To view details on what is delivered in this release; see sections, What's New and Enhancements.

What's New

This section describes the new features introduced in this release of FortiWLC. For other product improvements, see section Enhancements.

FortiAP-U431F and FortiAP-U433F

This release introduces Fortinet 11ax Universal Access Points (FAP-Us) providing greater bandwidths in high density networks and enhancing user experience in data, voice, and video applications in enterprise class deployments.

The FortiAP-U431F and FortiAP-U433F indoor access points are 802.11ax, 4x4 MIMO, tri-radio, dual band (2.4GHz/5GHz) access points and are compliant with the IEEE 802.3at PoE specifications.

Note: FAP-U43xF access points are **NOT** compliant with IEEE 802.3af PoE specifications.

FAP-U431F

FAP-U433F

These access points are delivered with dual redundant PoE Gigabit Ethernet ports (LAN1 2.5G & LAN2 1G RJ-45) and ten internal (FAP-U431F) and external (FAP-U433F) antennas. For hardware description, deployment, and instruction on setting up these access points, see the *FAP-U43xF Quick Start Guide* and *FAP-U43xF Deployment Guide*.

For more information on the supported features, see *FortiWLC 8.5.1 Support Matrix*.

Notes:

- Vcell is not supported on FAP-U43xF.
- Packet capture configured on FAP-U43xF does not work if the AP channel changes. Reboot the AP to use packet capture.

The following features are not supported on FAP-U43xF in the current release. Support for these **will be** provided in the **upcoming releases**:

- AP survivability
- Hotspot 2.0
- Roaming Across Controllers (RAC)
- IPv6 support
- Multiple PSK in Bridge mode
- Remote RADIUS
- Mesh
- QoS Bridge mode
- VLAN Mesh
- Wired clients on uplink with Mesh
- Service Assurance Manager (SAM)
- IPSec
- AirIQ (Spectrum)
- Spectralink
- Non-CE DFS
- Voice and data on the same radio

The following are some supported **maximum counts** for FAP-U43xF access points:

- Maximum ESS profiles supported – 8/radio
- (ARRP enabled) Maximum number of clients supported – 512 clients

Upgrading for FAP-43xF Support

You are required to download the FAP-U43xF image file as it is NOT bundled in the controller image. Follow this procedure to download and install the FAP-U43xF image.

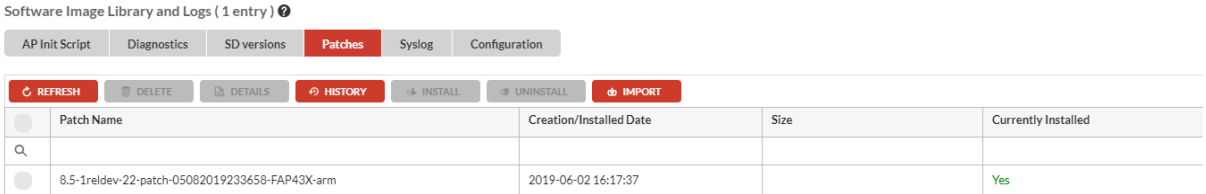
Note: Direct upgrade to 8.5.1 can be done from releases 8.4.0 and above.

1. Download the FAP-U43xF image file from the remote server to the controller.
   For example,
   [FortiWLC controllers]
   *copy scp://download:download@<remote_server_IP>/<image_file_location>/**forti**-8.5-1build-16-patch-24102019120556-FAP43X-arm-generic-rpm.tar.fwlc*
   [MC controllers]
   *copy scp://download:download@<remote_server_IP>/<image_file_location>/**meru**-8.5-1build-16-patch-24102019120556-FAP43X-arm-generic-rpm.tar.fwlc*
2. Run the **sh patch** command to verify that the image file is copied successfully to the controller.
3. Run the **patch install <image filename>** command to install the image file on the controller.

   OR

1. Download the image file from the remote server and navigate to *Maintenance > File Management > Patches > Import* in the controller GUI.

2. Select the imported image file and click **Install**. This step is required only if the auto-upgrade is disabled.



After the FAP-U43xF image file is installed in the controller, run the **upgrade ap same all** command to upgrade the APs.

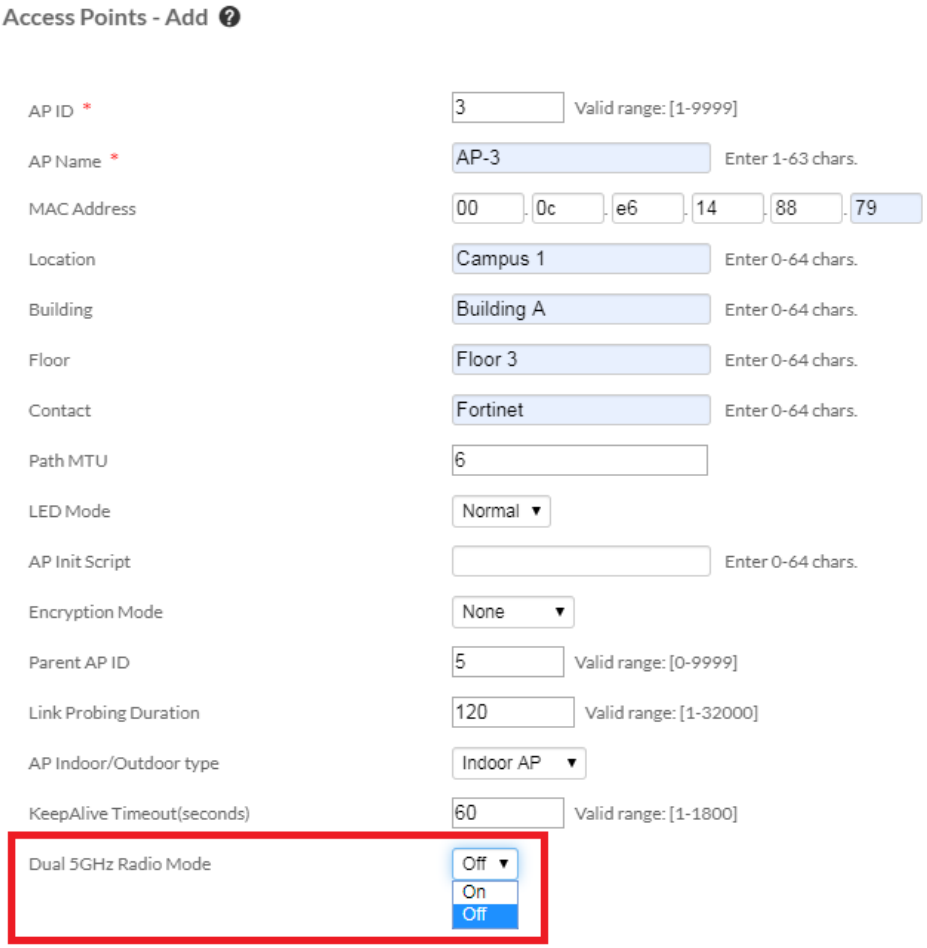
Dual 5 GHz Radio Configuration

FortiAP-U43xF supports configuring two radio interfaces in the 5GHz band. This option is supported for FAP-U43xF ONLY and is disabled by default; when enabled/disabled, the radios operate with the default configurations described in this table.

Dual 5GHz Radio Mode	Interface 1	Interface 2	Interface 3
Disabled (default)	[Service Mode] • 2.4 GHz • 4x4 MIMO • 802.11ax_2g RF band	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band	[Scan Spectrum Mode] • 2.4/5GHz • 2x2 MIMO • 802.11ac RF band • BLE scanning
Enabled	• [Service Mode] 2.4 GHz 2x2 MIMO • 802.11bgn RF band • [Scan Spectrum Mode] 2.4/5GHz • 2x2 MIMO • 802.11bgn RF band • BLE scanning	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band • Low band operating in channels 36 – 64.	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band • High band operating in channels 100 – 165

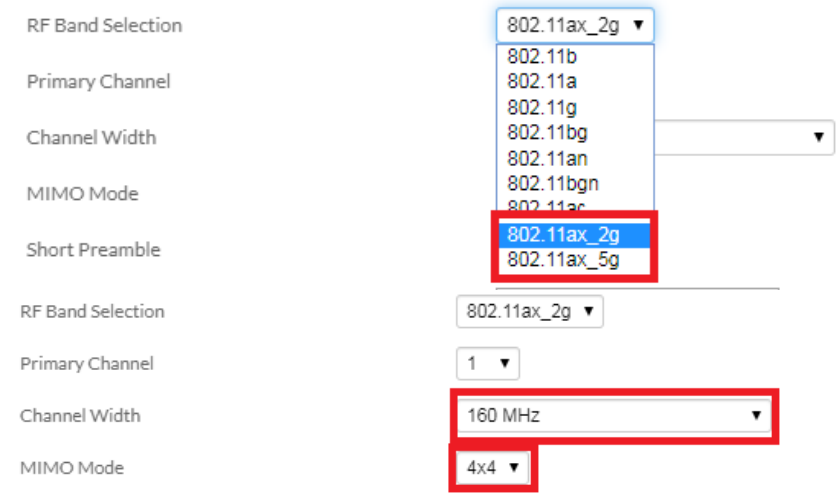
To enable **Dual 5GHz Radio Mode**; navigate to *Configuration > Devices > APs*.

Note:
The AP reboots whenever the **Dual 5GHz Radio Mode** is changed - enabled/disabled**.**



You can modify these default configurations as per your requirement; navigate to *Configuration > Devices > Wireless > Radio.* Note that the following configuration options are added for FAP-U43xF:

- RF band Selection: **802.11ax_2g** and **802.11ax_5g**
- Channel Width: **160 MHz**



Deployment Guidelines

Apply this upgrade procedure to laptops (with Intel Wi-Fi drivers installed) for connectivity to FAP-U43xF access points, where, the ESSID is not displayed in the Wi-Fi list; the ESSIDs are not detected by default on laptops with Intel Wi-Fi drivers installed.

Follow these steps to upgrade Intel client drivers.

1. Browse to https://downloadcenter.intel.com/ and select **Wireless Networking**.
2. Click on **View by product** and select **Intel Wireless Products**; the browser page reloads.
3. Click on **View by product** again and select the applicable **Intel Wireless Series.** (For example, Intel Wireless 9000/8000/7200 Series); the browser page reloads.
   Note: The number your chipset starts with is your wireless series, for example, chipset starting with 8260 indicates Intel Wireless 8100 Series.
4. Select your chipset version.
5. Select the drivers based on the installed OS and download them.
6. Install the downloaded drivers; on the prompt, select **Upgrade**.
7. Restart the laptop after the drivers are successfully installed.

You are now able to see the ESSID.

Note: It is recommended to use tunnel mode of deployment.

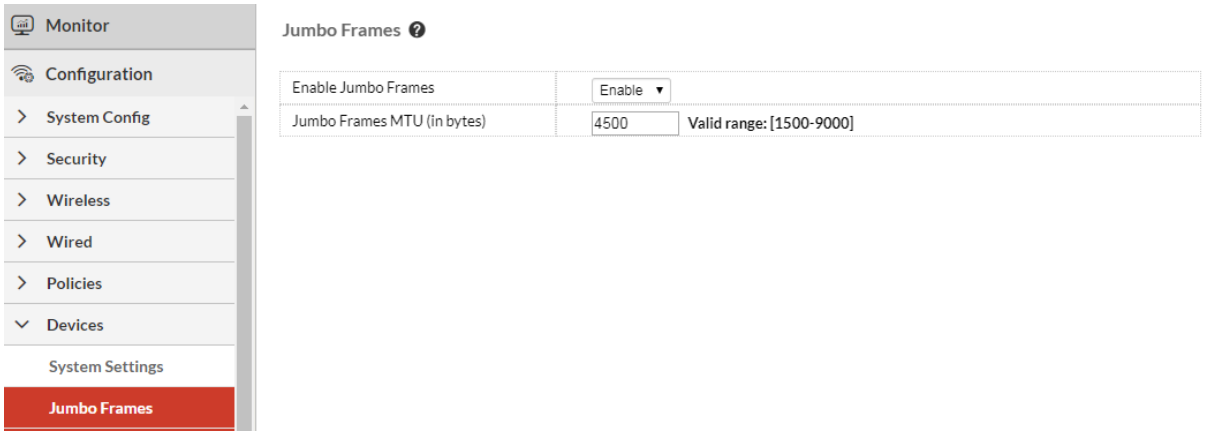
For more information on deploying FAP-U43xF, see the *FAP-U43xF Deployment Guide*.

Jumbo Frames

An Ethernet frame is classified as Jumbo when its size exceeds the standard Maximum Transmission Unit (MTU) of 1500 bytes.

For wireless clients, Jumbo frames are NOT supported; aggregation is supported in the tunnel mode only. Wireless payload is aggregated into jumbo frames to improve the system throughput.

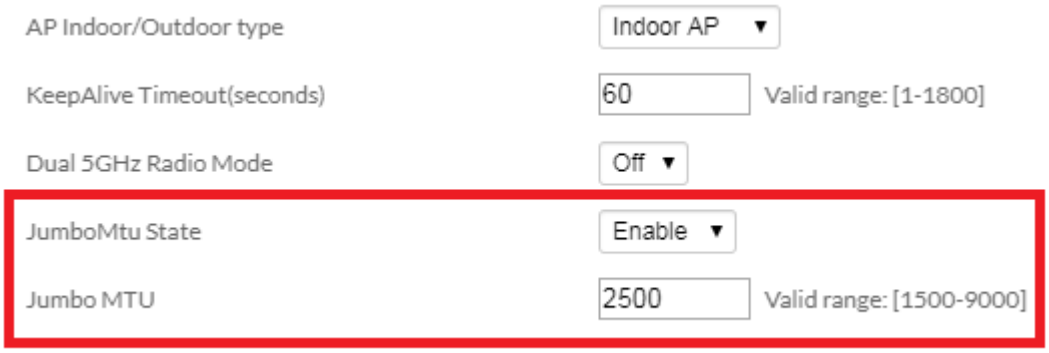
Navigate to *Configuration* > *Devices* > *Jumbo Frames* to configure the MTU for controllers.



The valid range is 1500 - 9000 bytes; default is 4500 bytes for controllers.

Note:
Ping from wireless clients for packet sizes more than 1500 bytes does not work when the configured MTU is more than 1500 bytes.

Navigate to *Configuration* > *Devices* > *APs* to configure the MTU for APs. Jumbo MTU is supported only on 11ac APs.



- [All 11ac APs (*except* AP832)] The valid MTU range is **1500 - 2500** bytes and the default is 2500 bytes.
- [AP832] The valid MTU range is **1500 - 9000** bytes and the default is 2500 bytes.

Notes:

- [AP832] Configuring the MTU size to 9000 bytes (with a large number of clients) may lead to low memory.
- [AP832] Using application visibility (DPI) along with jumbo frames may lead to low memory.
- Jumbo MTU is not supported for port profiles configured on AP122.
- Jumbo MTU is not supported on *Open VPN* APs.
- [AP822 and AP122] Upstream TCP throughput degradation of ~ 30% observed with Jumbo Frames enabled.

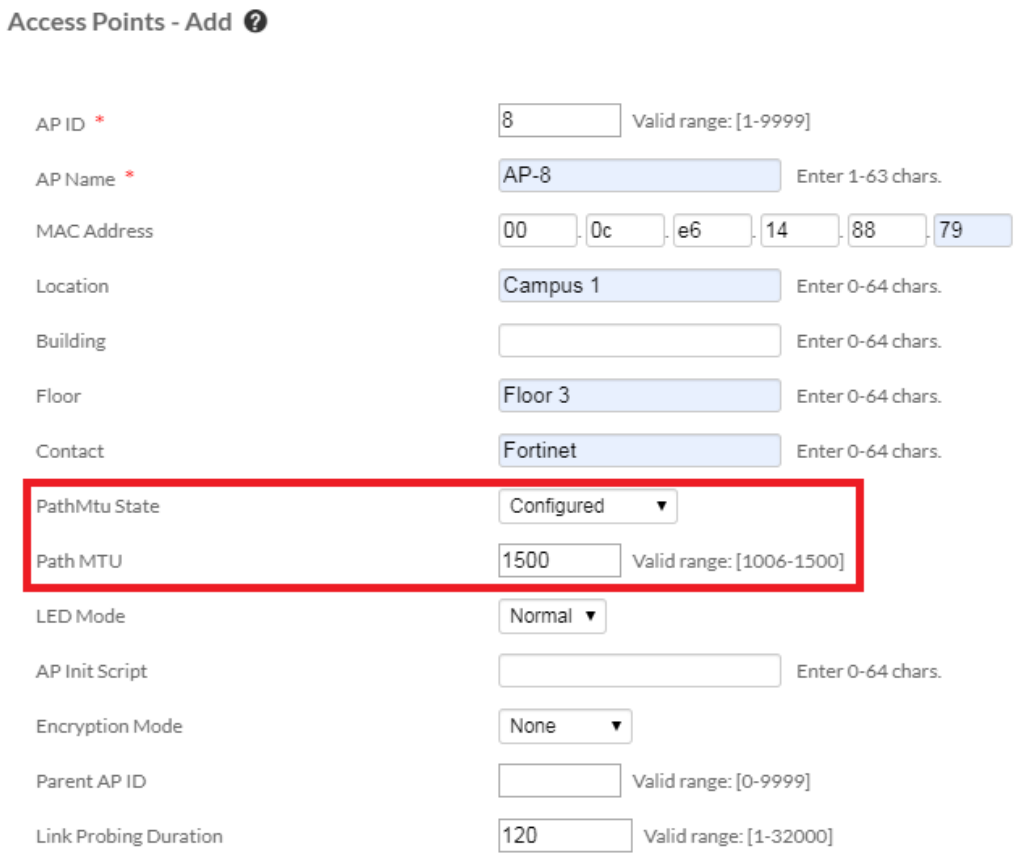
This feature is supported on AP122, AP822, AP832, OAP832, FAP-U42xEV, FAP-U422EV (outdoor), FAP-U32xEV, FAP-U22xEV, and FAP-U24JEV.

Path MTU

The Path MTU discovery enables FortiWLC to determine the maximum transmission unit size on the network path between AP and controller; the packets sent conform to the MTU along the path, avoiding fragmentation and improving the network performance.

The path MTU is discovered dynamically only when the AP is discovered/re-discovered. For example, if IPSec tunnel is configured between the controller and AP, Path MTU of 1438 bytes is set.
Any update in the path MTU due to network changes (modification of MTU settings in L3 switch or router between AP and controller) does not take effect periodically; the AP must be rebooted.

Due to specific network requirements or the path MTU discovered by FortiWLC not being optimum, you can configure a value for path MTU. Select **Configured**, the **Path MTU** option is enabled. The valid range is 1006 to 1500 bytes; the default is 1500 bytes. You are required to reboot the AP for the configured Path MTU to take effect. Navigate to *Configuration > Devices > AP*.



This feature is supported on AP122, AP822, AP832, OAP832, FAP-U42xEV, FAP-U422EV (outdoor), FAP-U32xEV, FAP-U22xEV, and FAP-U24JEV.

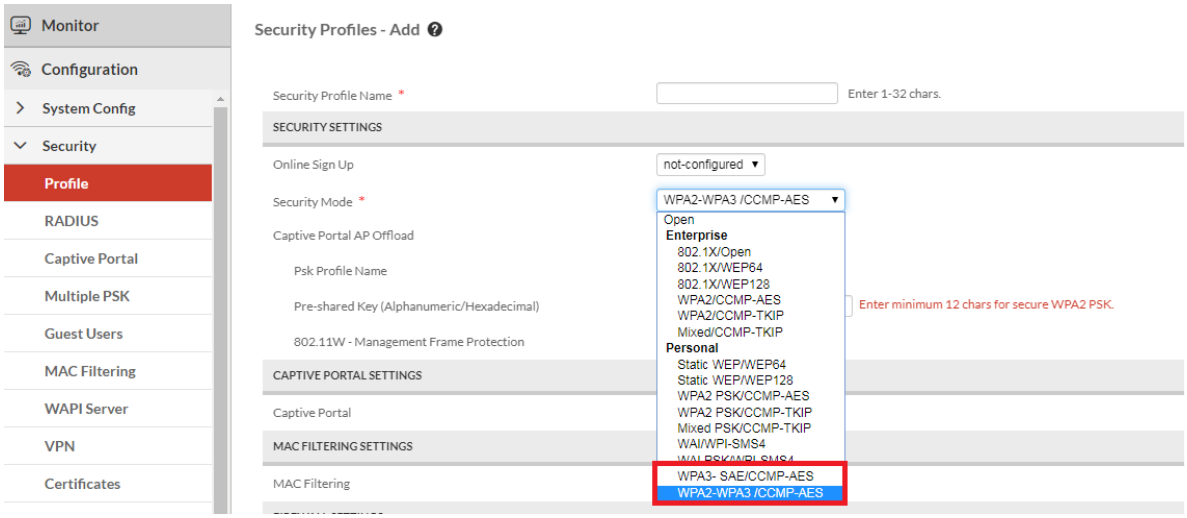
WPA3 Support

The WPA3 security mode is now supported. You can add these while configuring the security profile.

WPA3-SAE/CCMP-AES: Uses the Simultaneous Authentication of Equals (SAE) encryption method and requires a pre-shared key.

WPA2-WPA3/CCMP-AES: Uses the CCMP-AES and SAE encryption methods and requires a pre-shared key.

Navigate to *Configuration > Security > Profile*.



This feature is supported on AP122, AP822, AP832, OAP832, FAP-U42xEV, FAP-U422EV (outdoor), FAP-U32xEV, FAP-U22xEV, FAP-U24JEV, and FAP-U43xF.

Others

- VLAN support is available for Multiple PSK in both bridge and tunnel mode (except FAP-U43xF).
- While configuring ARRP, you can set the **Neighbour RSSI Threshold**. The minimum RSSI value for the neighbouring APs. The default is -85dbm and the valid range is -95dbm to -30dbm. Navigate to *Configuration > Wireless > ARRP*.
- The station log events generated by FortiWLC now include the AP ID and the BSSID.
- This release resolves the issue of RADIUS requests sent with the same port number for different IDs.
- syslog for *station-log* is disabled by default in 8.5.1.

Enhancements

The following enhancements are delivered in this release.

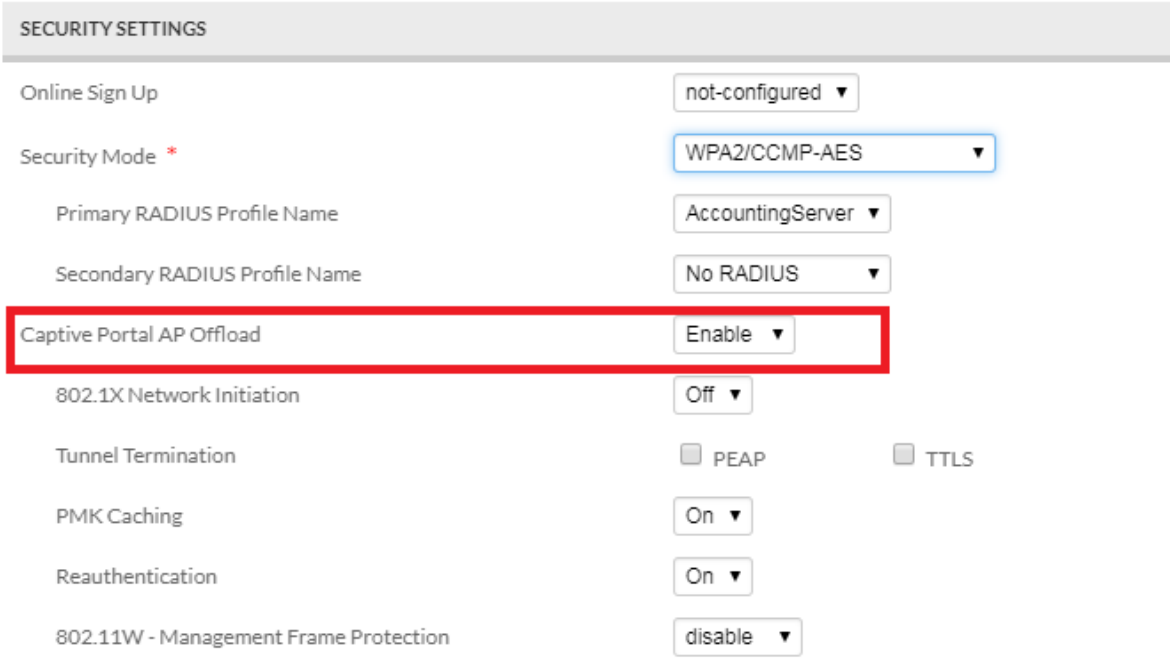
- Captive Portal AP Offload
- RADIUS Failover
- Debug Commands
- DFS Support

Captive Portal AP Offload

The **Captive Portal AP Offload** can be configured when creating the Security profile. Enabling this option allows URL redirection to be offloaded to the APs, thereby, reducing the load on the controller and allowing more concurrent captive portal authentication requests to be handled. This option is disabled by default.

Note: The usage of this feature is not completely established.

Navigate to *Configuration > Security> Profile*.



This feature is supported on AP122, AP822, AP832, OAP832, FAP-U42xEV, FAP-U422EV (outdoor), and FAP-U32xEV.

RADIUS Failover

Log history for RADIUS failovers can now be viewed on the FortiWLC GUI and CLI. Navigate to *Monitor > Fault Management > Radius Failover Dump* to view details of the RADIUS failover dump.

Radius Profile Name	Raised At	Station MAC	ESSID	EapId	Radius Identifier	Access Type	Auth Type
faulty-radius	10-01-2019 15:59:45	00:83:f1:f2:37:20	meru-wpa2	1	222	Radius_auth	dot-one-x
faulty-radius	10-01-2019 15:56:16	00:83:fe:37:37:23	meru-wpa2	2	153	Radius_auth	dot-one-x
faulty-radius	10-01-2019 15:07:49	00:83:fe:37:37:21	meru-wpa2	2	76	Radius_auth	dot-one-x
faulty-radius	10-01-2019 15:37:30	00:83:f1:f2:37:1d	meru-wpa2	1	252	Radius_auth	dot-one-x
faulty-radius	10-01-2019 11:49:09	00:83:de:12:37:1c	forti-wpa2	1	108	Radius_auth	dot-one-x

Note: These dump entries are **NOT** for RADIUS MAC filtering and RADIUS Captive Portal authentication.
Run the **sh radius-failover-details-1x** command to view the RADIUS failover details.

Debug Commands

The following commands are added/modified to improve debug ability.

- The following new commands are added:
  - **debug feature-diag** - This command enables you to collect diagnostic information for specific features.
  - **show statistics ac-ap-diagnostics** - This command displays the diagnostic statistics for 11ac access points.
  - **show statistics ap330-diagnostics** - This command displays the diagnostic statistics for AP330.
  - **show ap-reboot-event** – This command displays the reboot events for access points.
- The *station-log show all* command displays 2,097,152 entries at a given time.
- The *show diag-log-config ap* command now displays the diagnostic logging configurations for 11ac APs.

DFS Support

The following DFS enhancements are delivered.

AP model	DFS Support
FAP-U43xF	DFS is enabled for E/IV/Y/D SKU regions.
FAP-U422EV	DFS enabled for A/D/N/S SKU regions.
FAP-U42xEV	DFS enabled for A/D/N/S SKU regions.
FAP-U22xEV	DFS enabled for A/D/N/S SKU regions.
FAP-U32xEV	DFS enabled for A/D/N/S SKU regions.
FAP-U24JEV	DFS enabled for United Kingdom, Israel, Vietnam, Egypt, and India. DFS disabled for USA, Brazil, and Singapore.
Others	
• Blocked Canada DFS channels 120-128 and channel (40 MHz only) 116. • Enabled Canada DFS channel 144. • Enabled USA DFS channel 144.	

Operational Guidelines

This section describes information related to the usage of FortiWLC.

- **In case if boot script is installed.**
  It is recommended to remove the boot script (if any being used) before Controller upgrade and configure a new valid boot script in accordance to the upgraded FortiWLC release.

- **In case if any patches are installed.**
  Any installed patch will be removed after Controller upgrade. A new patch needs to be installed in case the relevant fix is not available in the upgraded FortiWLC release.

- In a deployment of 300 and more APs, it is recommended to configure *Feature Group* in FortiWLC or *AP Groups* in FortiWLM. Do not run ARRP globally (on all APs) in such a deployment as it is memory and processor intensive.

- GRE functionality is not available with IPv6; the controller cannot establish the GRE tunnel using IPv6 address.

- Do **NOT** configure APs in Secondary Interface VLAN in case of Dual Ethernet Active-Active configuration.

- Do **NOT** enable Vcell and Native cell load balancing on the same AP.

- [FortiWLC 1000D/3000D] When collecting diagnostics (*Maintenance > File Management > Diagnostics*) in a scale setup (3000 APs and 40k clients approximately), do not use the **System Diagnostics** option as it takes a long time (4 hours' approx.). Also, do not run the **diagnostics** command to collect system diagnostics. The following are recommended:

  - **[GUI]** Use **Controller Diagnostics** and **Controller Diagnostics Snapshot** options.
  - **[CLI]** Use **diagnostics-ap, diagnostics-controller**, and **diagnostics-controller-snapshot** commands**.**

- Chromecast option is visible on the YouTube application only when the publisher or subscriber is in the tunneled mode.

- Fortinet does not recommend hand off between different models for 11n APs. Single VCELL between Wave-1 and Wave-2 AC APs is supported.

- By default, AP832 requests 802.3af power via LLDP. Use static 802.3at power for LACP and Bluetooth.

- To refer to the LACP configuration procedure, see the *FortiWLC 8.5.1 User Guide*.

Supported Hardware and Software

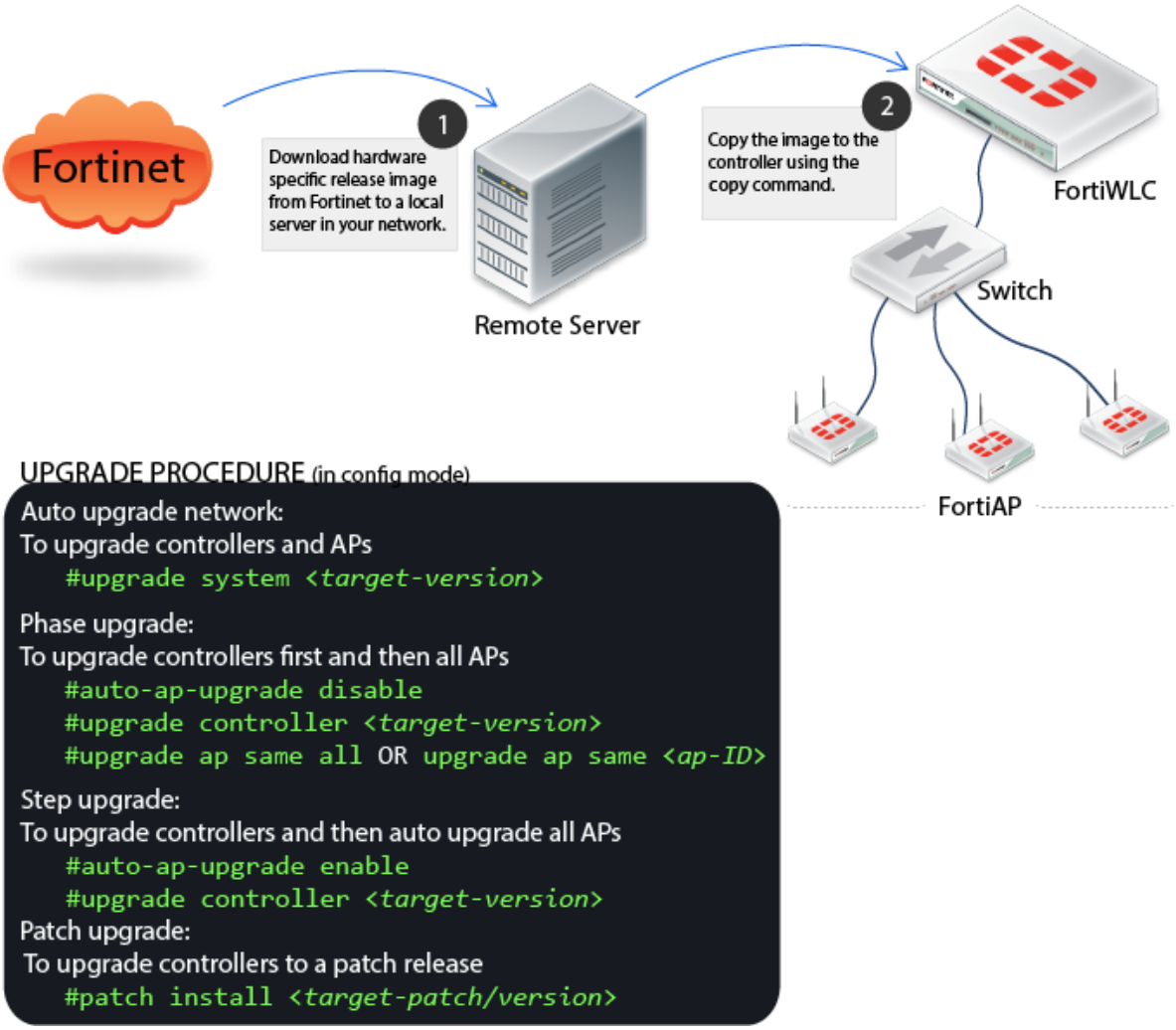
This table lists the supported hardware and software versions in this release of FortiWLC.

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e* AP332i* AP433e* AP433i* OAP433e* FAP-U421EV FAP-U423EV FAP-U321EV FAP-U323EV FAP-U422EV	FAP-U221EV FAP-U223EV FAP-U24JEV FAP-U431F FAP-U433F PSM3x AP1010e* AP1010i* AP1020e* AP1020i* AP1014i* AP110*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC-50D FortiWLC-200D FortiWLC-500D FortiWLC-1000D FortiWLC-3000D FWC-VM-50 FWC-VM-200 FWC-VM-500 FWC-VM-1000 FWC-VM-3000	MC3200 MC1550 MC4200 (with or without 10G Module)	MC 5000 MC 4100 MC 1500 MC 6000 MC 1500-VE MC1550-VE MC3200-VE MC4200-VE
FortiWLM	8.5.0		
FortiConnect	16.9.3		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 11 Mozilla Firefox 69 Google Chrome 77		
Note: A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			

Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)	

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, FortiWLC-500D, MC1550, MC3200, and MC4200 controllers. See section Upgrading FortiWLC-1000D and FortiWLC-3000D to upgrade FortiWLC-1000D and FortiWLC-3000D. See Upgrading Virtual Controllers to upgrade virtual controllers.



1. Download image files from the remote server to the controller using one of the following commands:

   ```
   # copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar.fwlc><space>.
   ```

   [OR]

   ```
   # copy tftp://<ext-ip-addr>/<image-name-rpm.tar.fwlc><space>.
   ```

   Where

   - *image-name* for FortiWLC: forti-{release-version}-{hardware-model}-rpm.tar.fwlc
     Eg, *forti-8.5-1-FWC2HD-rpm.tar.fwlc*

2. Disable AP auto upgrade and then upgrade the controller (in config mode)

```
# auto-ap-upgrade disable

# copy running-config startup-config

# upgrade controller <target version> (Example, upgrade controller 8.3)
```

   The *show flash* command displays the version details.

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the *show controller* and *show ap* command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the *show running-config* command (if not, recover from the remote location). See the Backup Running Configuration step.

Getting Started with Upgrade

The following table describes the approved upgrade path applicable for all controllers except the new virtual controllers.

NOTE:
In pre-8.4.3 releases, if the MAC-delimiter is set to hyphen in the RADIUS profile for 802.1x authentication, the controller sends the *called station id* with MAC-delimiter as colon. When you upgrade to 8.5.1 from pre-8.4.3 release, if there is a RADIUS reject for the MAC-delimiter, then reconfigure the RADIUS server.

Supported Upgrade Releases

This section describes the upgrade path for 8.5.1 GA release.

From FortiWLC release…	To FortiWLC Release…
7.0	7.0-13
8.0	8.0-5-0, 8.0-6-0
8.1	8.1-3-2
8.2	8.2.7
8.2.7/8.3	8.3.1
7.0.11, 8.2.7, 8.3.0, 8.3.1, and 8.3.2	8.3.3
7.0-11, 8.2.7, 8.3.0, 8.3.1, and 8.3.2	8.4.0 (CLI upgrade only)
8.3.3	8.4.0
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4	8.5.0
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.5.0	8.5.1

NOTES:

- Fortinet recommends that while upgrading 32-bit controllers, use the **upgrade controller** command instead of the **upgrade system** command.
- Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI.

- FortiWLC-1000D and FortiWLC-3000D and 64-bit virtual controller upgrades can be performed via GUI as well.
- Upgrade the FortiWLC-1000D and 3000D controllers with manufacturing version prior to 8.3-0GAbuild-93 to version 8.3-0GAbuild-93 and then to the later builds.

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **show file systems** command to verify the current disk usage.

```
controller# show file systems
Filesystem     1K-blocks   Used        Available   Use%   Mounted on
/dev/hdc2      428972      227844   178242      57%      /
none               4880           56            4824           2%       /dev/shm
```

The first partition in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **delete flash:<flash>** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Set the serial connection for the following options:

NOTE:
Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

NOTES:

- [32-bit controllers] Prior to upgrading to FortiWLC, delete any old image files to avoid issues related to space constraints.
- Upgrade Controller using wired client/laptop and **NOT** using wireless client/laptop.
- [Patch installation] When both AP and controller patches are to be applied; the controller patch must be installed prior to the AP patch.

Upgrading Virtual Controllers

In the *upgrade-image* command, select the options **Apps** or **Both** based on these requirements:

- Apps: This option will only upgrade the Fortinet binaries (rpm).
- Both: This option will upgrade Fortinet binaries as well as kernel (iso).

Upgrading FAP-U422EV

If the controller is running on pre-8.4.0 version and FAP-U422EV is deployed, follow these points:

- Disable *auto-ap-upgrade*.
  OR
- It is advised not to plug in FAP-U422EV till the controller gets upgraded.

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller.

Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. The Override Group Settings option in the *Wireless Interface* section in the *Configuration > Wireless > Radio* page must be enabled on the gateway AP.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration > Devices > System Settings > Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

NOTE:

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic.

Upgrading FortiWLC-1000D and FortiWLC-3000D

To upgrade to FortiWLC-1000D and FortiWLC-3000D, use the following instructions.

Direct upgrade to 8.5.1 is supported using the *.fwlc* file format only.
FortiWLC with versions **prior** to 8.4.0 require an intermediate upgrade to 8.4.0 or later (using *rpm.tar* file format) before upgrading to 8.5.1 release (using *rpm.tar.fwlc* file format).

Note that the *.fwlc* file format is supported from release 8.4.0.

Upgrading via CLI

1. Use the **show images**command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
Master-3000D(15)# show images
Running image : image0
On reboot     : image0
--------------------------------------------------------------------------------
Running image details.
         System version: 0.3.14
         System memory: 231M/463M
         Apps version: 8.5-1build-0
         Apps size: 251M/850M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.3.14
         System memory: 240M/473M
         Apps version: 8.5-0build-7
         Apps size: 177M/849M
```

2. To install the latest release, download the release image using the *upgrade-image* command:

```
upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image-name>-rpm.tar.fwlc both

reboot
```

The above command will upgrade the secondary partition and the controller will reboot to secondary partition.

NOTE:
After an upgrade the current partition will shift to the second partition. For example, if you started upgrade in primary partition, post upgrade the default partition becomes secondary partition and vice- versa.

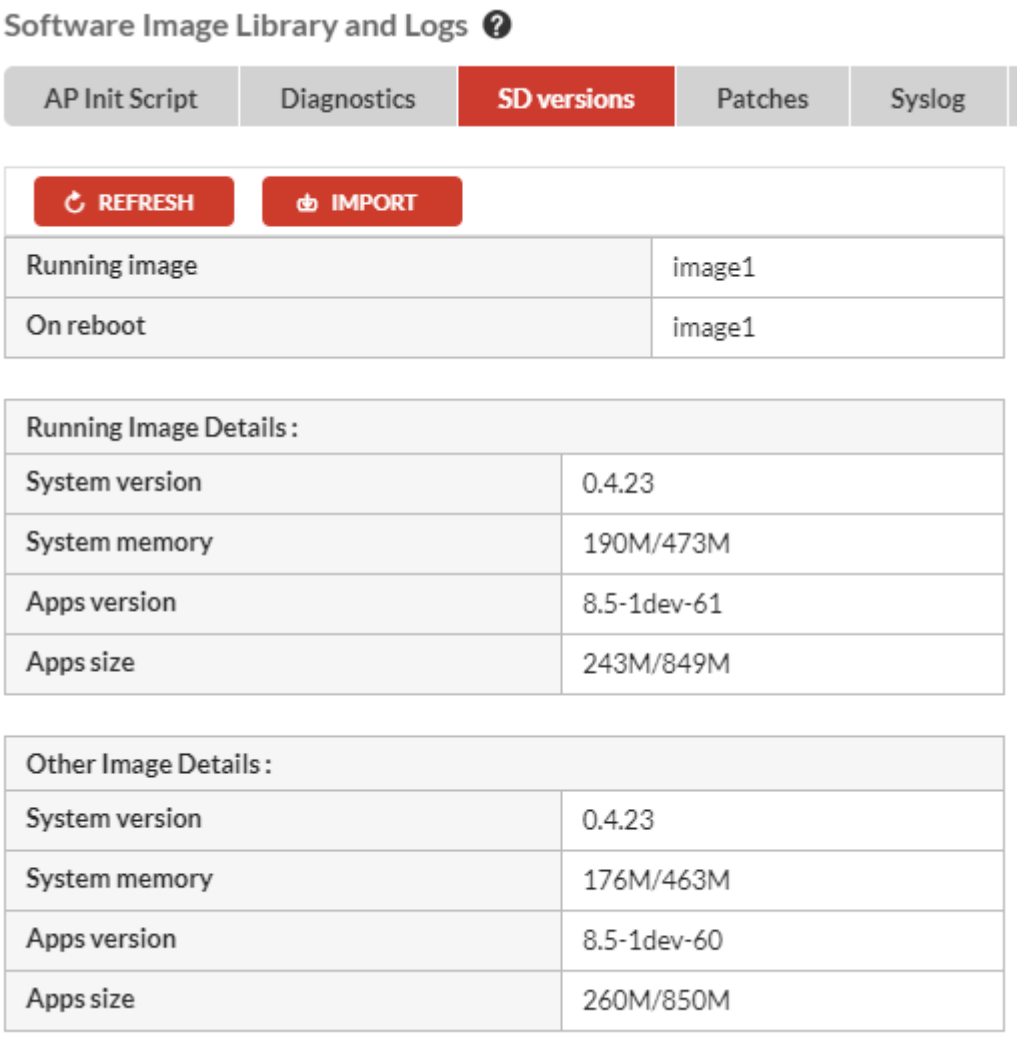
Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

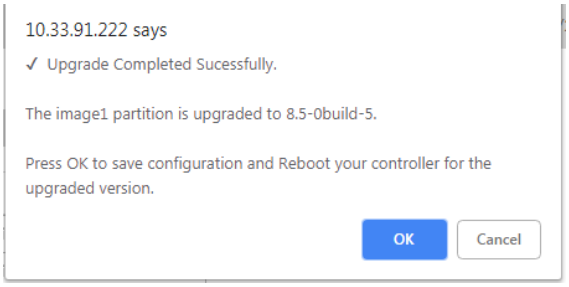
NOTE:

- Fortinet recommends upgrading via CLI to avoid this issue which occurs due to file size limitation.
- This issue does not exist on controllers with manufacturing build as 8.3.3 GA and above.

1. To upgrade controllers using GUI, navigate to *Maintenance > File Management > SD Version*.
2. Click *Import* button to choose the image file.



3. After the import is complete, a pop message for upgrade confirmation is displayed.



Click **OK** to upgrade; the controller reboots. Click **Cancel** to abort the upgrade and continue in the existing version.

Switching Partitions

To switch partitions in FortiWLC-1000D, FortiWLC-3000D and the new virtual controllers, select the partition during the boot up process.

Upgrading a N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers.

You can choose any of the following options to upgrade:

- **Option 1** - Just like you would upgrade any controller, you can upgrade an N+1 controller.
  1. Upgrade master and then upgrade slave.
  2. After the upgrade, enable master on slave using the *nplus1 enable* command.

- **Option 2** - Upgrade slave and then upgrade master.
  After the upgrade, enable master service on slave using the *nplus1 enable* command.

- **Option 3** - If there are multiple master controllers
  1. Upgrade all master controllers followed by slave controllers. After the upgrade, enable all master controllers on slave controllers using the *nplus1 enable* command.
  2. To enable master controller on slave controller, use the *nplus1 enable* command.
  3. Connect to all controllers using SSH or a serial cable.
  4. Use the *show nplus1* command to verify if the slave and master controllers are in the cluster.

     The output should display the following information:

     ```
     Admin: Enable
     Switch: Yes
     Reason: -
     SW Version: 8.3-1
     ```

  5. If the configuration does not display the above settings, use the *nplus1 enable <master-controller-ip>* command to complete the configuration.
  6. To add any missing master controller to the cluster, use the *nplus1 add master* command.

Restore Saved Configuration

After upgrading, restore the saved configuration.

1. Copy the backup configuration back to the controller:
   ```
   # copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
   ```
2. Copy the saved configuration file to the running configuration file:
   ```
   # copy orig-config.txt running-config
   ```
3. Save the running configuration to the start-up configuration:
   ```
   # copy running-config startup-config
   ```

Upgrading Virtual Controllers

Virtual Controllers can be upgraded the same way as the hardware controllers. See sections Upgrading via CLI, Upgrading via GUI, and Upgrading a N+1 Site.
Download the appropriate Virtual Controller image from Fortinet Customer Support website.
For more information on managing the virtual controllers, see the *Virtual Wireless Controller Deployment Guide*.

Upgrading the controller can be done in the following ways:

- Using the FTP, TFTP, SCP, and SFTP protocols.
- Navigate to **Maintenance < File Management** in the FortiWLC GUI to import the downloaded package.

The following are sample commands for upgrading the Virtual Controllers using any of these protocols.

- upgrade-image tftp://10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar.fwlc both reboot
- upgrade-image sftp://build@10.xx.xxx.xxx:/home/forti-x.x-xGAbuild-88-FWC1KD-rpm.tar. fwlc both reboot
- upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xGAbuild-88-FWC1KD-rpm.tar. fwlc both reboot
- upgrade-image ftp://anonymous@10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar.fwlc both reboot

The **both** option upgrades the Fortinet binaries (rpm) as well as the Kernel (iso), the **apps** option upgrades only the Fortinet binaries (rpm).

After upgrade, the Virtual Controller should maintain the System-id of the system, unless there were some changes in the fields that are used to generate the system-id.

The International Virtual Controller can be installed, configured, licensed and upgraded the same way.

Fixed Issues

These are the fixed issues in this release of FortiWLC. Controller issues listed in this section are applicable on all models unless specified; AP issues are applicable to specific models.

AP reboot/stability

Tracking ID	Description
445156	[AP1020] Random AP reboots.
453991, 540434, 540437, 522163, 513377	[AP832] Random AP reboots.
491698	Random FAP-U421EV AP reboots due to kernel crash.
435269	AP stops sending frames after the Transmit Power (EIRP) is modified.
502859, 511289, 530709,	[FAP-U42x/32xEV/AP832] Random Tx stuck in high interference network conditions. The access point recovers automatically; no manual intervention is required.
512454	[FAP-U22xEV] AP was unresponsive when a huge file was transferred on the 5GHz radio configured on a DFS channel.
514986	[FAP-U32x/42xEV/AP832] Bulk AP reboots in scale setup due to wncagent spikes.
516308, 517000	[FAP-U32x/42xEV] Low throughput observed randomly.
520091, 522159	[AP822v2/AP832] Random AP crashes observed.
526419, 527122, 534371	[FAP-U32x/42xEV] Random silent AP reboots.
537545	[FAP-U32x/42x/22xEV] After Controller reboot, some APs failed to come up online and appear *Disabled/Online* even when they could be pinged from the controller.
538913	[FAP-U32x/42x/22xEV] AP did not come online as no ARP requests were sent for the default gateway.
539068, 530898	[FAP-U32x/42xEV] Random AP reboots.
549445	Random AP1020 reboots due to the watchdog.
558773	[AP122] Random AP reboots.
558800	[AP822v2/122] Random silent AP reboots.

ARRP

Tracking ID	Description
503005	ARRP not getting applied on APs when enabled in bulk and unable to enable freeze.
520747,	MCAD process memory usage increased in scale setup with ARRP enabled in

558718	all APs.
550434	Incorrect channel assignment for APs while using ARRP channel planning.
552271	With ARRP planning, the AP collects incorrect neighbour details.
579558	[FAP-U32x/42xEV] Unstable wireless connection when clients associate to new AP plugged in with ARRP enabled

Captive Portal

Tracking ID	Description
513250	Captive portal unresponsive in scale setup with the number of CP users increasing to 2000.
520168	Captive Portal error messages observed when Captive Portal disabled.
521855	External captive portal authentication fails.
550218	Delayed loading of the custom captive portal login page and the contents not loaded properly.
580284	[AP832/Internal Captive Portal]- Idle/inactive clients lose internet access & failed pings to the gateway.

Configuration – Controller/AP

Tracking ID	Description
476679	License file in the controller was marked as a trial version.
495139	[AP832] site survey mode cannot configure inactivity timer accurately.
515494	Controller lost configuration during boot up.
523651	LACP configuration for APs requires to be simplified.
542133	[FAP-U32x/42xEV] While creating an ESS profile a message is displayed that the beacon interval is not applicable with these APs in the system.
542623, 551599	Multiple ESS-AP entries created for existing and old/offline APs post AP replacement (AP Group and Feature Group configured).
552819	On upgrade, Captive Portal certificates in *httpd.conf* file were reset to default certificates instead of user installed certificates.
553466	Request for console reset in debug CLI.

Controller processes/sluggishness

Tracking ID	Description
513347	Random wncagent restarts and high memory trends in scale setup.
513484	XCLID spike on controller caused the GUI to be sluggish and CLI slow to respond.
515039, 515043, 523710	Sometimes the Wncagent restarts due to DB corruption.
518076	Coordinator crash while rebooting the controller.
543323	Random hostapd crashes due to memory issues.
543743,	Random hostapd crashes.

552680, 565197, 566911	
544348	Random Service Manager crashes.
548246	Controller unable to send MAC filtering RADIUS requests to the t RADIUS server.
550468	Application of the configuration file failed when the MCAD process was running.
553385	Random multiple nmsagent crashes.
554209	Random SecurityMM crashes.
567467	Controller unresponsive randomly; restart required.

DFS

Tracking ID	Description
507685	Radar detections noticed on both DFS and non-DFS channels.
538389	Region -N DFS support required for FAP-U422EV.
546634	[AP822v2] DFS functionality issue: AP did not switch to non-DFS channel post radar detection.
566009	Some channel configurations not working as expected in Canada.

GUI & CLI

Tracking ID	Description
474787	The AP model is a filterable field on the "Port-AP member table - Add" page.
488055	Un-associated/unassigned stations showing up in station table.
522823	Controller GUI was unresponsive randomly.
523292	Incorrect patch file size displayed in *Patch Management* after the patch is applied and the controller reboots.
524326	Packet capture module to capture Rx/Tx traffic on both Ethernet and radio interfaces of FAP-Us.
529131	The *show ap-neighbor* command did not display any AP neighbors in the output.
538617	The AP's operating channel displayed in the GUI and CLI mismatch.
547177	Random statistics dropouts observed.
549939	[AP832] Unable to change radio 2 interface from 802.11ac to 802.11bgn/g/g/n from the GUI.
550179	*MODIFY: Wireless Interface Configuration* message repeatedly sent to the Syslog server every 1 minute.
561404	[AP832] False memory usage high alarms observed.
562208	AP uptime sorting functionality not working in the GUI.
563165	Added iOS 12x fingerprints to the database.

Intermittent connectivity

Tracking ID	Description
492272, 503630, 521607,	[All FAP-Us] Random Rx freeze/Mac suspension and failure.
439721, 506164	[All FAP-U] High Latency and ping loss observed on clients configured in bridge mode with native and Static VLAN.
466162	Beacon transmission is stopped for more than 1 second.
511560	MacBook users lose internet connectivity intermittently.
514950	Clients getting EAP authentication timeouts during peak hours.
514985	Clients falling in controller VLAN in scale setup.
517094	[FAP-U32x/42xEV] Clients unable to authenticate on the AP.
519952	When a client sends duplicate EAP-ID responses, RADIUS server rejects access.
520479	[AP832] Clients unable to obtain the IP address for the first time in bridged SSID.
522194	[AP832, AP1010, FAP-U22xEV] Broadcast downstream traffic not passing through AP for random clients.
523343	EAP delay logs observed on the controller.
532251	[FAP-U32x/42xEV] New clients unable to connect and existing clients faced facing latency issues with gateway IP address.
535009	Devices unable to get IP address when an internal DHCP server is used.
539687	Wired stations not able to connect and obtain IP address.
540478	Some stations were unable to connect and handoffs to other AP kept happening.
541213	Clients did not receive DHCP NACK with MAC authentication and RADIUS VLAN configured in the profile.
544765	[FAP-U22xEV/24JEV] Stale stations not cleared created client connectivity issues.
547440	Stations connected to specific APs had low download speed.
549386	iOS client devices show the login prompt, when cancelled device reconnects successfully.
550104	Station gets the DHCP IP address through native VLAN after changing VLAN tag in RADIUS server.
550188	11r clients unable to pass traffic after 802.1x when RADIUS does not throw any VLAN information.
550346	Intermittent client connectivity and slow performance observed.
561456, 547020	Client connectivity affected due to Hostapd CPU spike.
563166	Multiple association entries observed for a single client on the controller.
565043, 564810	[FAP-U32x/42xEV] Connected users unable to pass traffic.
571997	Continuous IPv6 ping drops due to Neighbor Solicitation packet discards on the controller.
572286	[FAP-U32x/42xEV] WiFi clients unable to obtain an IP address from DHCP server; station logs display ip update not performed.

Logs

Tracking ID	Description
520236	IPv6 address displayed with IPv4 format in the station log.
520969	AP flash log enhancements.
536458	Requirement to clear Var logs from the controller.

Nplus1

Tracking ID	Description
467520	Configuration synchronization from master to slave controller errors out.
561298	Unable to pass traffic after Nplus1 failover.
566148	SNMP service did not start on the slave controller following an NPlus1 failover.
570987	AD IDs were lost when the master controller returned to the active state from passive in an Nplus1 setup.

Others

Tracking ID	Description
417621	With MAC and portal authentications configured, two authentication records are created in the RADIUS server after client de-association/association.
455533, 563173	Chromecast stopped working after controller firmware upgrade.
462324	RADIUS requests sent with same port number for different IDs.
511838	[Mesh] Leaf AP failed to connect to gateway AP as the pre-shared key of the Mesh profile was mapped to a different security profile.
521077	RDP session drops and other issues.
523336	[AP832] Bulk upgrade of APs fails with a lot of retries.
524013	*ap_discovered* JSON missing first few commas.
527638	[FAP-32x/42xEV] AP switching VLAN tag for associated device upon probing on SSID with MAC filtering.
529874	In the access-request, the controller sends the NAS IP address as the physical interface address instead of sending the management VLAN address.
530880, 547045	As soon as a device leaves the multicast group, the controller stops forwarding multicast traffic to other devices in the group.
538225	Fortinet Push API for FortiPresence: Inconsistent endianness for *Num_packets*.
538280	Fortinet Push API for FortiPresence: number of packets, minimum and maximum signal were set to 0.
538295	Fortinet Push API for FortiPresence: number of messages is set to a non-zero value when there are no station packets.
540660	False RADIUS failovers observed in a scale setup with WPA2 clients in

	continuous connect/disconnect mode.
549329	[AP332i/AP832i]- Spectrum Manager functionality not working.
554359	SIP devices (ASCOM and Siemens) unable to make voice calls.
554073, 541516	Chromecast streaming did not work randomly.
563556	Unable to bring up FortiWLC on FortiWLM.

Common Vulnerabilities and Exposures

This release of FortiWLC is no longer vulnerable to the following:

Bug ID	Vulnerability
480054	CVE-2018-7492
551643	CVE-2019-9496
566274	CVE-2019-11477 CVE-2019-11478

Visit *https://fortiguard.com/psirt* for more information.

Known Issues

These are the known issues in this release of FortiWLC. Controller issues listed in this section are applicable on all models unless specified; AP issues are applicable to specific models.

Tracking ID	Description	Impact	Workaround
514143	When IPsec encryption is configured, the IPsec tunnel between the AP and controller is re-established after Nplus1 failover/fallback. Hence the APs go for reboot/rediscovery.	Network connectivity affected while the AP reboots.	
571459	[AP822/AP122] Rarely observed random silent AP reboots.	Client connectivity affected during reboot.	

Known Issues in FAP-U43xF

These are the known applicable to the **FAP-U43xF access points ONLY**.

This table lists **specific feature based** known issue found in FAP-U43xF.

Tracking ID	Description	Impact	Workaround
560037	With Dual 5GHz Radio Mode enabled, 2.4 GHz band cannot be used for the Site Survey mode.	Site Survey mode unavailable.	Disable the Dual 5GHz Radio Mode.

This table lists **stability related** known issues found in FAP-U43xF.

Tracking ID	Description	Impact	Workaround
568089	Ping loss observed due to high CPU in huge multicast traffic or in scale setup (> 50 clients).		Connect less than 50 clients.
575737	[Apple MacOS/iOS] Data loss for > 60 seconds observed sometimes on random clients.		Reconnect the client.

This table lists **performance based** known issue found in FAP-U43xF.

Tracking ID	Description	Impact	Workaround
548294	When a wired client is connected to the 2.5G physical interface, the downlink throughput is lesser (< 500Mbps) than when connected to the 1 G physical interface.		