FortiWLC - Release-Notes

Version 8.4.8

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://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
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 29. 2021
FortiWLC 8.4.8 Release-Notes

TABLE OF CONTENTS

Change log

Date	Change description
2020-11-10	FortiWLC version 8.4.8 release document.
2021-04-29	Updated the supported FortiConnect version. Supported Hardware and Software on page 6.

About FortiWLC 8.4.8

FortiWLC 8.4.8 release resolves outstanding issues on FortiWLC; see section Fixed Issues on page 17.

Note:

To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice-versa. Third party access points and software cannot be configured on Fortinet hardware.

Supported Hardware and Software

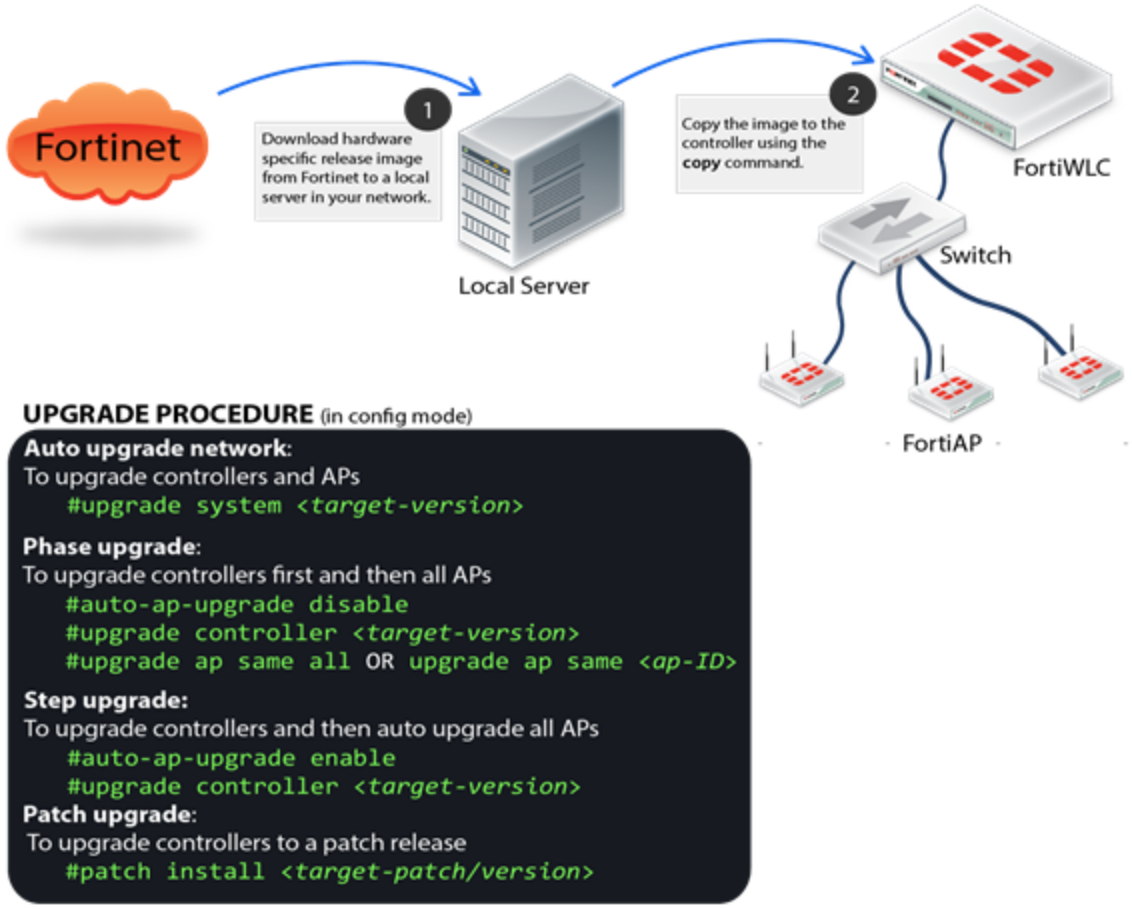
This table lists the supported hardware and software versions in this release of FortiWLC.

Hardware and Software	Supported	
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e* AP332i* AP433e* AP433i* FAP-U421EV FAP-U423EV FAP-U321EV FAP-U323EV FAP-U422EV	FAP-U221EV FAP-U223EV FAP-U24JEV PSM3x (32-bit controllers only) AP1010e* AP1010i* AP1020e* AP1020i* AP1014i* AP110*
*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, MC3200-VE MC1550, MC1550-VE MC6000 MC4200 (with or without 10G Module) MC4200-VE
#Spectrum Manager NOT supported in these controller models.		
FortiWLM	8.5.0, 8.5.1	

Hardware and Software	Supported
FortiConnect	16.9, 17.0
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, MC1550-VE, MC3200, MC3200-VE, MC4200, MC4200-VE and MC6000 controllers. See section Upgrading FortiWLC-1000D and FortiWLC-3000D on page 11 to upgrade FortiWLC-1000D and FortiWLC-3000D. See Upgrading Virtual Controllers on page 15 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><space>.`
   [OR]
   `# copy tftp://<ext-ip-addr>/<image-name-rpm.tar><space>.`
   Where
   image-name for FortiWLC: *forti-{release-version}-{hardware-model}-rpm.tar*, for example, *forti-8.3-3-FWC2HD-rpm.tar*
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 from pre-8.4.3 to 8.4.8, if there is a RADIUS reject for the MAC-delimiter, then reconfigure the RADIUS server.

FortiWLC-1000D and FortiWLC-3000D controllers can be upgraded only from 8.3 releases.

From FortiWLC release...	To FortiWLC Release...
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7	8.4.8

Note:

- 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 systemsFilesystem     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 signaling 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.

Note:

[32-bit controllers] Prior to upgrading to the current release version, delete any old image files to avoid issues related to space constraints.

Upgrading Virtual Controllers

In the upgrade 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 to the current release version.

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.

In version 8.4.0, the image naming systems have been changed for 64 bit controller models from Primary/Secondary to image0/image1. This change applies to the upgrade procedure in the related FortiWLC GUI screens and CLI commands.

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: 8.4-8build-0
Apps size: 251M/850M
------------------------------------------------------------------------
------
Other image details.
System version: 0.3.14
System memory: 240M/473M
Apps version: 8.4-7build-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 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

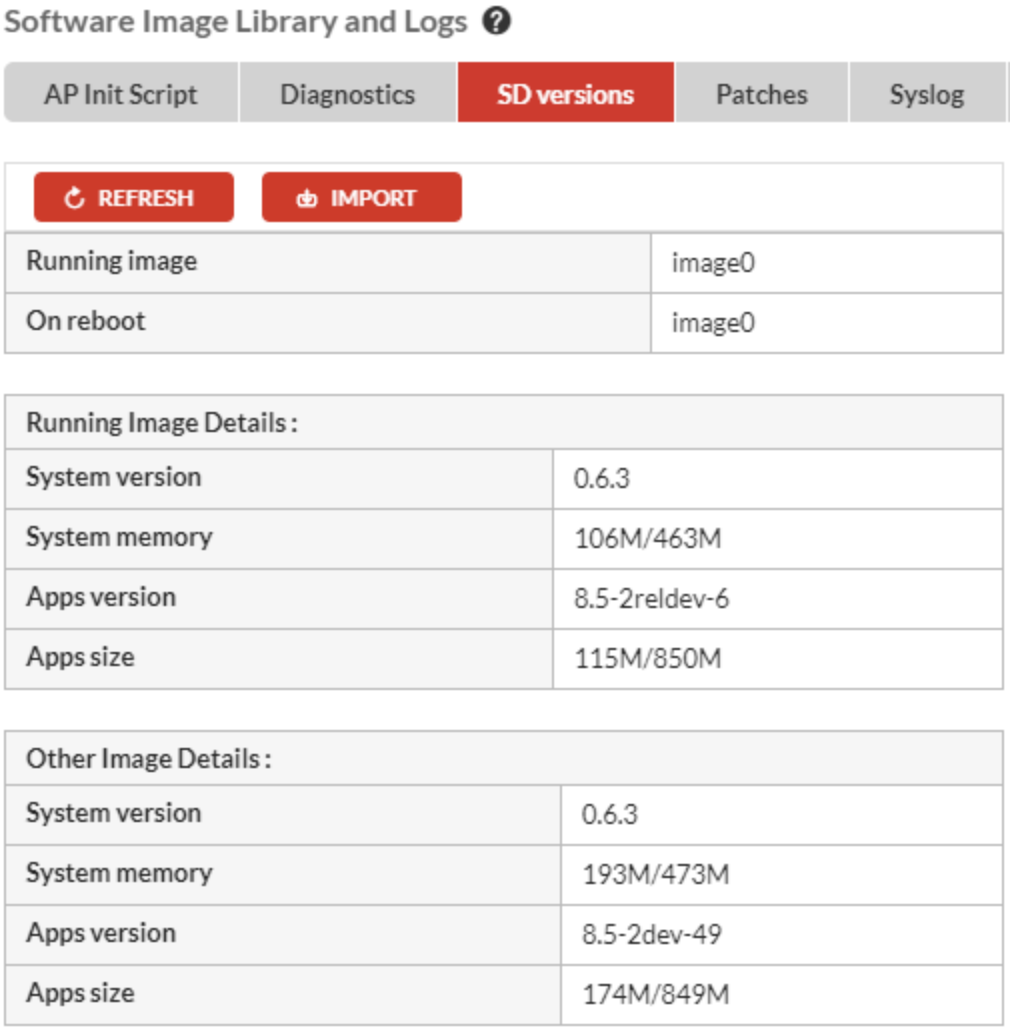
This section describes the upgrade procedure through the FortiWLC GUI.

Notes:

- Standalone controllers running images prior to version 8.3.3 (except version 7.0-12) are required to upgrade to 8.3.3 GA and then to the current release version.
  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.

1. To upgrade controllers using GUI, navigate to **Maintenance > File Management > SD Version**.
2. Click **Import** to choose the image file.
   Note:
   Direct upgrade to the current release version using the *.fwlc* format is supported only from release 8.4.0

and later. Upgrade from pre-8.4.0 to the current release version using *.fwlc* is not supported.



After the import is complete, a success message is displayed.

Switching Partitions

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

Upgrading 32-bit 8.3.3 Controllers (MC models, FortiWLC-50D/200D/500D) with AP832/822 (without KRACK patch)

Upgrading from FortiWLC 8.3.3 to 8.4.8 results in *runtime1* image corruption in AP832 and AP822v1. This is due to a resource leak in the 8.3.3 version which is fixed in later releases.

Follow these steps to upgrade from 8.3.3 to 8.4.8.

1. Reboot the APs before upgrade.
2. Run the *upgrade controller* command to upgrade controllers.
3. Once the controller is online, upgrade the APs in batches. Before initiating upgrade, ensure all APs are rebooted so that the uptime is less than 5 hours.

Notes:

- Fortinet recommends that you upgrade the 8.3.3 32-bit controller before upgrading the access points due to the issue mentioned in this section.
- If KRACK patch is installed on the 8.3.3 32-bit controller then this recommendation does not apply. The controller can be directly upgraded to 8.4.8.
- This section does not apply when upgrading from 8.4.0 or later to 8.4.8.

Upgrading NPlus1 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.

Notes:

- [32-bit controllers] Prior to upgrading an NPlus1 setup from a pre-8.3.0 release to the current release version, it is recommended to stop the NPlus1 service on the slave controller.
  Restart the NPlus1 service on the slave controller after both the master and slave controllers are upgraded successfully.
- [64-bit controllers] Controllers running images prior to version 8.3.3 are **required** to upgrade to the 8.3.3 GA version and then to the current release version.
  When FortiWLC is upgraded to 8.3.3 GA, the N+1 setup needs to be reconfigured to enable N+1, that is, the master controller should be deleted and then added to the slave controller.
  This reconfiguration is not required when upgrading from 8.3.3 GA to the current release version.
  This issue does not exist on controllers w ith manufacturing build as 8.3.3 GA.
  This issue does not exist when upgrading from 8.4.0 or later to the current release version.
  This advisory does not apply to NPlus1 cluster upgrade done through FortiWLM.
- [FortiWLC-500D/MC4200] When the NPlus1 master service runs with the default RJ45 interface module and the controller requires to be enabled with 1G SFP or 10G SFP+ interface modules, the NPlus1 master service must be stopped and started, after the controller comes up with 1G SFP or 10G SFP+ interface modules.
- In case of an Nplus1 cluster and FortiWLM, note the following points:
  - After the Nplus1 cluster formation is complete, it takes a maximum of 10 minutes to get discovered in FortiWLM.
  - If the slave and master controllers are to work as standalone, then backup the FortiWLM configuration, double delete the controller and add it again from the controller inventory in FortiWLM, so that the controller can be successfully managed.

You can choose any of the following options to upgrade:

- **Option 1** - Just like you would upgrade any controller, you can upgrade an Nplus1 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 on page 11, Upgrading via GUI on page 12, and Upgrading NPlus1 Site on page 14.

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 Managemen**t 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 both reboot
- upgrade-image sftp://build@10.xx.xxx.xxx:/home/forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image ftp://anonymous@10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar 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. See the to the Licensing section for detailed information.

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.

Tracking ID	Description
560055	Dis-associated station entries not removed from the show station all output after aging-out interval.
562843	Random controller crashes.
575926	The *show sys-summary ess* command output required to sort by ESSID name.
600045	Random controller crashes due to memory issues.
607692	Controller configuration restore jammed with the error Cannot determine subnet.
617054	[AP832/AP822] Random AP reboot.
622739	Sluggish connectivity after upgrade on tunnel SSIDs connected via IPsec over GRE-tunnel.
633745	[FAP-U22xEV] Soft lockup issues observed.
639737	[BGN] Displays in station-log inspite of 5GHz probing
655484	[FAP-U22xEV] Random AP reboot.
655712	Critical/Major/Minor CPU usage events observed in station log.
660962	SNMP process did not restart after controller reboot.
662660	Random controller reboots due to continuous wncagent restarts.
662947	NPlus1 master controller reboot after upgrade without any logs.
667361	Enhancements for */opt/meru/var/log/* directory filled in scale setups.
670461	NPlus1 slave service did not start after controller reboot.