FortiWLC - Release-Notes

Version 8.5.3

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

December 11, 2020
FortiWLC 8.5.3 Release-Notes

TABLE OF CONTENTS

Change log

Date	Change description
2020-12-11	FortiWLC version 8.5.3 release document.

About FortiWLC 8.5.3

FortiWLC release 8.5.3 delivers resolved outstanding issues; see section Fixed Issues on page 15.

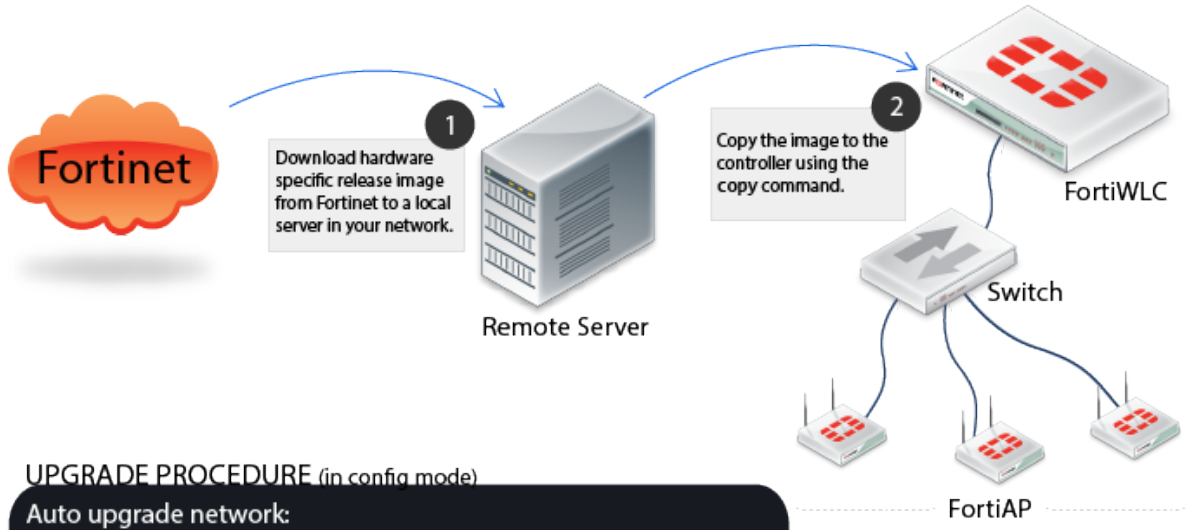
Supported Hardware and Software

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* 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*
*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)
FortiWLM	8.5.1	
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.		

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, FortiWLC-500D, MC1550, MC3200, and MC4200 controllers. See section to upgrade FortiWLC-1000D and FortiWLC-3000D. See Upgrading Virtual Controllers on page 11 to upgrade virtual controllers.



UPGRADE PROCEDURE (in config mode)

Auto upgrade network:
To upgrade controllers and APs
```
#upgrade system <target-version>
```
Phase upgrade:
To upgrade controllers first and then all APs
```
#auto-ap-upgrade disable
#upgrade controller <target-version>
#upgrade ap same all OR upgrade ap same <ap-ID>
```
Step upgrade:
To upgrade controllers and then auto upgrade all APs
```
#auto-ap-upgrade enable
#upgrade controller <target-version>
```
Patch upgrade:
To upgrade controllers to a patch release
```
#patch install <target-patch/version>
```

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 For example, *forti-8.5-2-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 the current release 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 this release.

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, 8.5.0, 8.5.1, 8.5.2	8.5.3

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/VPN AP Deployments

[32-bit controllers] When attempting to upgrade a VPN/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. Run the **upgrade system** command.

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, navigate 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 an NPlus1 Site

To upgrade a site running NPlus1, 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 NPlus1 controller.

1. Upgrade master and then upgrade slave.
2. After the upgrade, run the **nplus1 enable** command to enable master on slave controller.

Option 2 - Upgrade slave and then upgrade master controller.

After the upgrade, run the **nplus1 enable** command to enable master service on the slave controller.

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After the upgrade, run the **nplus1 enable** command to enable all master controllers on slave controllers .
2. Run the the **nplus1 enable** command to enable master controller on slave controller.
3. Connect to all controllers using SSH or a serial cable.
4. Runthe **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, run the **nplus1 enable <master -controller -ip>** command to complete the configuration.
6. Run the **nplus1 add master** command to add any missing master controller to the cluster.

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 12, Upgrading via GUI on page 13, and Upgrading an NPlus1 Site on page 11.

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.

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: 8.5-2build-4
Apps size: 251M/850M
------------------------------------------------------------------------
```

```
-------
Other image details.
System version: 0.3.14
System memory: 240M/473M
Apps version: 8.5-1build-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.

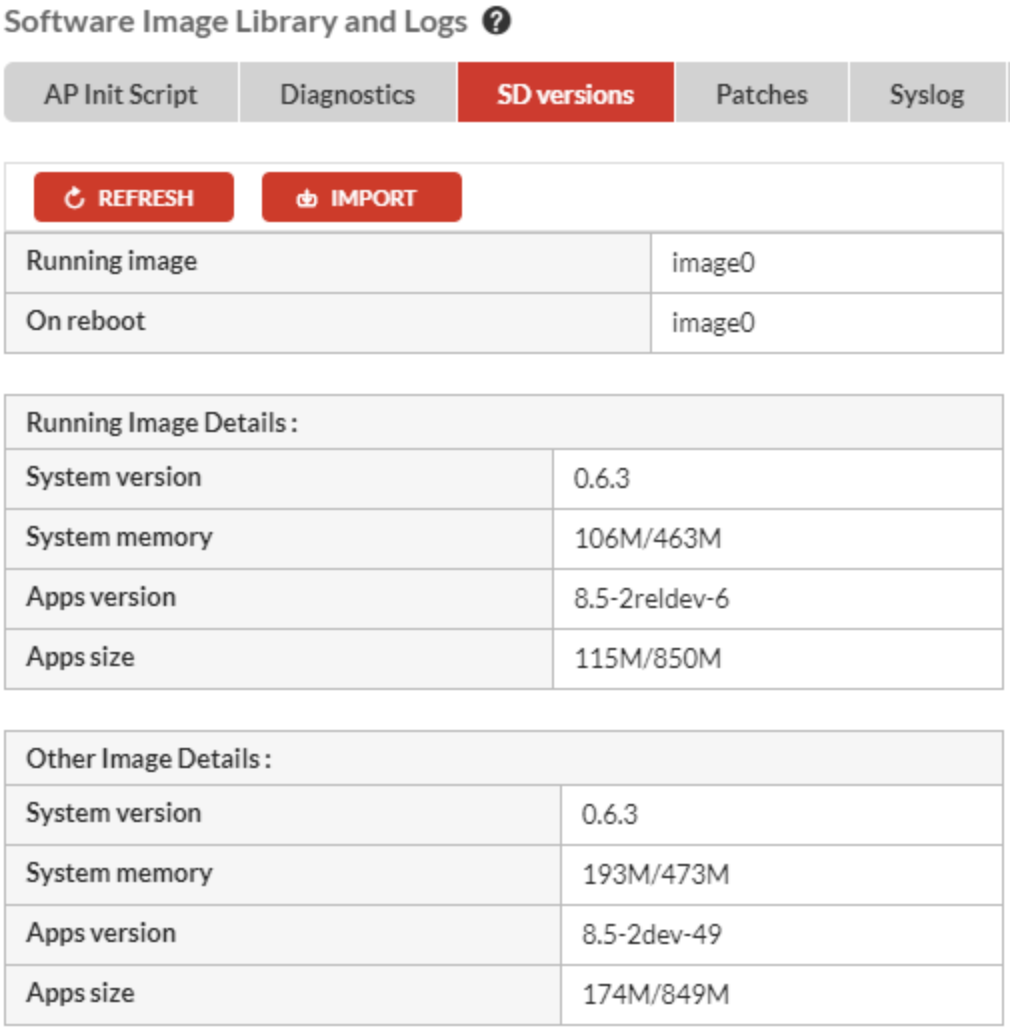
Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

NOTES:

- 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** 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.

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
400651	[AP832] Round trip delay observed between client and AP.
452650	FAP-U42xEV did not auto-negotiate 1Gbps full duplex.
561513	[FAP-U43xF] Random AP crashes.
600757	[AP832] Ping timeout and latency issues observed.
605462	[FAP-U421xEV/U32xEV] Random AP reboot.
605464	[FAP-U421xEV/U32xEV] Random AP reboot.
605472	[AP832] Random AP reboot.
610232	[FAP-32xEV] Random AP reboot.
617054	[AP832/AP822] Random AP reboot.
624541	[FAP-U43xF] Random AP reboot.
632372	[FAP-U43xF/42xEV/32xEV] Unresponsive AP remained in a disabled offline state.
655484	[FAP-U22xEV] Random AP reboot.
663363	[AP8xxx] Random AP reboot.

ARRP

Tracking ID	Description
660158/660160	When AP groups were added/removed/re-planned in an ARRP profile, APs from other AP goups rebooted.

Captive Portal

Tracking ID	Description
616533	Unable to add customized captive portal page.
618583	External captive portal ClearPass did not redirect to authentication success page.
650554	External captive portal issues with Cisco ISE.

Configuration – Controller/AP

Tracking ID	Description
607692	Controller configuration restore jammed with the error Cannot determine subnet.
612323	[FAP-U32xEV] LLDP power negotiation overwrote LLDP advertisement packets.
618924	The default dataplane encryption configuration changed to off while provisioning an AP from GUI.
632272	[OAP832e] LED status for LAN2 interface is ON with no devices connected.

Controller Processes/Sluggishness

Tracking ID	Description
571080	Random SecurityMM crashes observed.
580864	The SNMP process restarted twice in an hour due to memory issues.
597985	The SNMP process restarted twice in an hour due to memory issues.
605486	Unresponsive controller console.
615130	Random CwAc crashes observed.
659881	Random SecurityMM crashes.

GUI/CLI

Tracking ID	Description
525797	Information on the top 10 ESS IDs not displayed for ESS profiles configured with RADIUS VLAN only.
536281	Incorrect data displayed on the **Wireless Statistics** page of the GUI.
599013	Incomplete dashboard statistics for stations.
638018	Unable to access controller through GUI after upgrade.
658189	The error *ERROR_CONVERSION_NOT_POSSIBLE Type: NmsL2SecurityMode_t* displayed on the **Monitor > Devices > All Statio**n GUI page when WPA3-SAE client connected to the AP.

Intermittent Connectivity

Tracking ID	Description
548440	WncDhcpRelay dropped packets randomly.
596860	Controller fails to pass router ARP Requests for one VLAN.
605954	DHCP server pool exhausted; unable to allocate IP addresses to new clients.
617434	[AP822/FAP-U22xEV] 802.1x authentication failure in bridge mode.
625225	Clients unable to connect due to Forced removal for sync with AP error.
642015	[FAP-U22xEV] Clients not able to pass traffic.
650206	Client unable to obtain IP address from the VLAN pool when the tunnel interface type is configured as RADIUS and VLAN-Pool in the ESS-profile

Logs

Tracking ID	Description
639737	[BGN] Displays in station-log inspite of 5GHz probing.
652763	FortiWLC generates unwanted syslog messages.
655712	Critical/Major/Minor CPU usage events observed in station log.

NPlus1

Tracking ID	Description
654653	Service connect dod not work after NPlus1 failure due to incomplete configuration synchronization.

Others

Tracking ID	Description
548885/604389	[FAP-U24JEV] Alarm on CPU usage above threshold observed.
562456	[FAP-U32xEV] AP flashlogs and general enhancements.
606199	[AP122] Wired client on yellow port (clear port profile) show up connected on AP network during boot up.
619357	Error messages observed during FortiWLC firmware upgrade.
633809	VPN APs state changes from connect to disconnect and vice versa after upgrade.
657358	[AP832] 80 MHz bonding not supported with channel 128 after upgrade. .
657407	Unable to install wild card certificate on FortiWLC
669162	Unable to import unencrypted sysconfig backup exported from FortiWLM.

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
557247	When wncagent restarts, the operational state of the Dot11radio interface is disabled.	Client connectivity impacted.	Reboot the AP.
683794	LACP configuration is not retained after upgrade.	AP is not available online.	Configure LACP on the controller and switch to bring the AP online.

Common Vulnerabilities and Exposures

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

- CWE-912
- CWE-259

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