FortiWLC - Release-Notes

Version 8.6.4

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

TABLE OF CONTENTS

Change log

Date	Change description
2022-03-18	FortiWLC 8.6.4 release document.

About FortiWLC 8.6.4

FortiWLC release 8.6.4 delivers a DFS enhancement and important bug fixes, see sections What's New on page 6 and Fixed Issues on page 20.

What's New

This release of FortiWLC enables DFS for the FCC region for FAP-U231F.

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 FAP-U421EV FAP-U423EV FAP-U321EV FAP-U323EV FAP-U422EV FAP-U221EV FAP-U223EV FAP-U24JEV FAP-U431F FAP-U432F FAP-U433F FAP-U231F FAP-U234F
*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
FortiWLM	8.6.3
FortiConnect	17.0
Browsers	
FortiWLC (SD) WebUI	Internet Explorer 11 Mozilla Firefox 69

Hardware and Software	Supported
	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)

Special Notices and Best Practices

This section lists some notes related to the usage of FortiWLC.

- VCell is not supported on FAP-U43xF and FAP-U231F.
- In case if any patches are installed, they 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.
- GRE functionality is not available with IPv6; the controller cannot establish the GRE tunnel using IPv6 address.
- Chromecast option is visible on the YouTube application only when the publisher or subscriber is in the tunneled mode.
- By default, AP832 requests 802.3af power via LLDP. Use static 802.3at power for LACP and Bluetooth.
- SNMP OIDs starting from 1.3.6.1.4.1.15983.3 are not supported.
- To refer to the LACP configuration procedure, see the FortiWLC Configuration Guide.
- 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.
- [FAP-U234F/FAP-U231F/FAP-U432F/FAP-U431F] Setting the image to *fap_primary* on the AP GUI is not supported, you can set the image to *fap_default*.

The following **best practices** are recommended for enhanced user experience.

FNAC integration with FortiWLC

Configure lower lease time for isolation VLAN scope. This helps faster transition of IP address change after the station gets moved from isolation to registration VLAN.

Rogue AP Scanning

It is recommended not to enable rogue AP scanning on APs expected to serve dense user locations to avoid the impact of channel scan duration and wait period for the wireless users.

ARRP

- It is recommended not to run channel plan with DFS enabled in presence of non DFS certified APs.
- It is recommended to enable **Freeze** after ARRP planning is complete to avoid unplanned disruption due to channel change that can occur when the AP detects high interference.
- In an existing deployment, if new APs are added, a re-plan is needed for the first time to add APs part of the ARRP cluster. Otherwise, the AP continues to operate in the default channel.
  Channel change won't get triggered though high interference or high neighbour count is detected.

Multicast

- The Multicast flag should be disabled on all ESS profiles unless it is needed for any multicast applications that do not support MDNS or SSDP. In such scenarios, it is recommended to use VLAN isolation for

multicast application traffic to avoid flooding of data both in wired and wireless infrastructure.

- IGMP snooping should be enabled in switching infrastructure when bridged data plane is configured in an ESS profile.
- All UDP ports must be disabled and ports that are specifically needed for any application traffic should be used.

Others

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

Deployment Guidelines for 802.11ax APs

Apply this upgrade procedure to laptops (with Intel Wi-Fi drivers installed) for connectivity to 802.11ax 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 produc**t 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.

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, and FortiWLC-500D controllers. See section to upgrade FortiWLC-1000D and FortiWLC-3000D. See to upgrade virtual controllers.
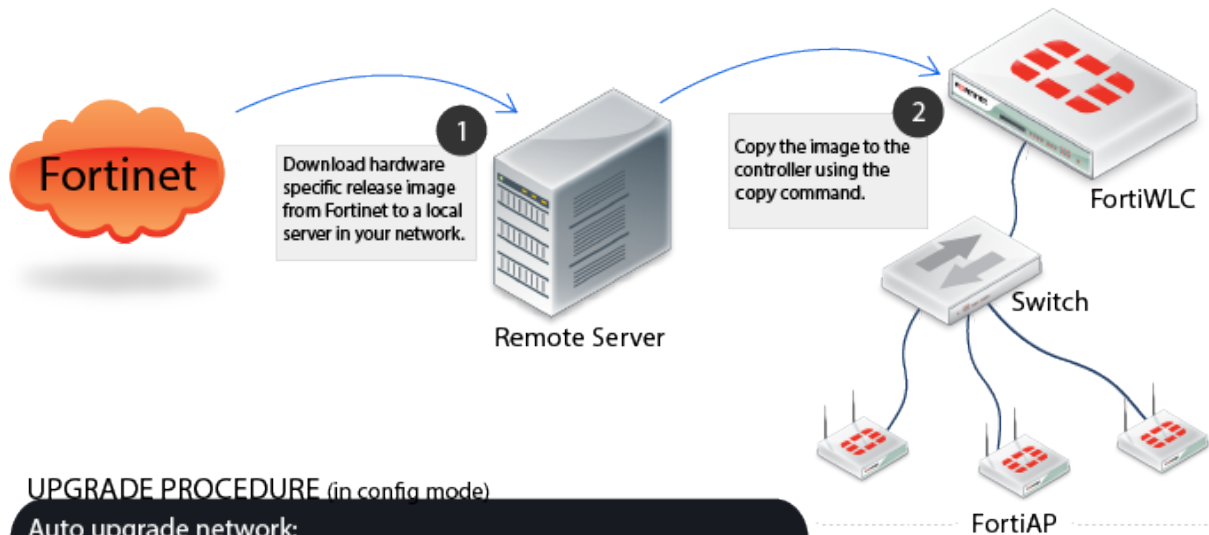
1. Download image files from the remote server to the controller using one of the following commands:
 # copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar.fwlc><space>.
[OR]
copy tftp://<ext-ip-addr>/<image-name-rpm.tar.fwlc><space>
Where, **image-name** for FortiWLC: forti-{release-version}–{hardware-model}-rpm.tar.fwlc For example, *forti-8.6-0-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)

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.

Supported Upgrade Releases

This section describes the upgrade path for this release.

From FortiWLC release...	To FortiWLC Release...
8.4.7, 8.4.8, 8.5.1, 8.5.2, 8.5.3, 8.6.0	8.6.1
8.5.4, 8.5.5, 8.6.0, 8.6.1	8.6.2
8.5.4, 8.5.5, 8.6.0, 8.6.1, 8.6.2, 8.6.3	8.6.4

NOTES:

- 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:

- 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.

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 to 64-bit FortiWLC-50D/200D/500D

FortiWLC release 8.6.0 onwards only 64-bit OS is supported on FortiWLC-50D/200D/500D hardware controllers. If you are upgrading to the current release from pre-8.6.0, perform this procedure to migrate from 32-bit to 64-bit OS.

Note: Disable NPlus1 prior to performing this procedure.

1. Download the FortiWLC 64-bit migration image file, for example *forti-8.6-0build-2-x86_64-rpm.migration.tar.fwlc*.
2. Run the **upgrade controller** command to install the image.
3. Log into the controller using the existing username and password.
4. After successful migration, upgrade the controller using the **upgrade-image** command (same as the existing 64-bit FortiWLC-1000D/3000D upgrade procedure), for example, **upgrade-image scp://@:/-rpm.tar.fwlc both**.

Note: After migration/upgrade to 64-bit OS, downgrading to a previous version is not supported.

Upgrading for FAP-U231F/U234F/U43xF Support

You are required to download the image files for FAP-U231F, FAP-U234F, and FAP-U43xF (FAP-U431F/U432F/U433F) as they are NOT bundled in the controller image. Follow this procedure to download and install the files.

1. Download the AP image file from the remote server to the controller, for example,
   copy scp://download:download@<remote_server_IP>/<image_file_location>/forti-8.6-2build-7-patch-22042021135617-FAP231F-arm-generic-rpm.tar.fwlc
   OR
   copy scp://download:download@<remote_server_IP>/<image_file_location>/forti-8.6-1build-04-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
   Download the image file from the remote server and navigate to **Maintenance > File Management > Patches > Import** in the controller GUI.

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

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

Upgrading FortiWLC-1000D and FortiWLC-3000D

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

Direct upgrade to this release is supported using the *.fwlc* file format only.

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 : image1
On reboot : image1
------------------------------------------------------------------------
-------
Running image details.
System version: 0.8.2
System memory: 231M/463M
Apps version: 8.6-2build-4
Apps size: 251M/850M
------------------------------------------------------------------------
-------
Other image details.
System version: 0.8.1
System memory: 240M/473M
Apps version: 8.6-3build-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 virtual controllers, select the partition during the boot up process.

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 17, Upgrading via GUI on page 17, and Upgrading an NPlus1 Site on page 18.

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-xbuild-xx-x86_64-vm-rpm.tar.fwlc both reboot**
- **upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xbuild-xx-x86_64-vm-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.

Tracking ID	Description
760006	[FAP-U43xF] Intermittent data transmit interruptions observed for 802.11ax stations.
781143	[FAP-U231F] Sometimes clients were unable to connect to the SSID until the AP was rebooted
782413	[FAP-U431F] Clients were unable to pass traffic intermittently.