

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

FortiWLC - Release-Notes

Version 8.6.0

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

January 25, 2021

FortiWLC 8.6.0 Release-Notes

TABLE OF CONTENTS

Change log	5
About FortiWLC 8.6.0	6
What's New	7
FortiWLC 64-bit OS Support	7
WIPS - Rogue Access Point Classification	7
Station Quarantine	9
QoS Throttle Policies	10
QoS Load Balancing	10
Security Audit	11
DHCP Option 82	12
Maintaining ARP Entries For Wireless Bridge Clients	13
Roaming Across Controllers (RAC) Support For 802.11r Clients	14
NPlus1 Failover Enhancements	14
ARRP Enhancements	14
IPv6 Enhancements	15
Router Advertisement (RA) Throttling	17
Neighbour Discovery (ND) Proxy	17
IGMP Snooping	18
Recommendations	18
802.1x Supplicant Access Point	18
FAP-U24JEV 2x2 - Modes Of Operation	19
Zero Wait DFS	19
User Interface Enhancements	20
FAP-U431/433F – Additional Features	23
Supported Hardware and Software	24
Special Notices and Best Practices	26
Deployment Guidelines for FAP-U431/433F	28
Installing and Upgrading	29
Getting Started with Upgrade	30
Supported Upgrade Releases	30
Check Available Free Space	30
Set up Serial Connection	31
Upgrade Advisories	31
Upgrading Virtual Controllers	31
Upgrading FAP-U422EV	31
Feature Groups in Mesh profile	32
Voice Scale Recommendations	32
Upgrading to 64-bit FortiWLC-50D/200D/500D	32
Upgrading for FAP-U431/433F Support	33
Upgrading FortiWLC-1000D and FortiWLC-3000D	33
Upgrading via CLI	34
Upgrading via GUI	34

Switching Partitions	35
Upgrading an NPlus1 Site	36
Restore Saved Configuration	36
Upgrading Virtual Controllers	36
Fixed Issues	38
Known Issues	42
Common Vulnerabilities and Exposures	44

Change log

Date	Change description
2021-01-07	FortiWLC 8.6.0 release document.
2021-01-25	Updated Upgrading to 64-bit FortiWLC-50D/200D/500D on page 32.

About FortiWLC 8.6.0

FortiWLC release 8.6.0 introduces new features and enhancements along with important bug fixes. The following are applicable in this release.

- FortiWLC supports **ONLY** 64-bit hardware controllers.
- All legacy hardware MC controller models are **NOT** supported, see [Supported Hardware and Software on page 24](#).
- Contact *Customer Support* to obtain the relevant build to access Spectrum Manager; Adobe Flash is no longer supported.

To view details on what is delivered in this release, see section [What's New on page 7](#)

Important Notes:

The following configurations are recommended **after upgrading to 8.6.0**, to use some new functionalities delivered in this release.

- In the WIPS rogue AP settings, the **Token** parameter is added to identify the APs and list them as rogue or friendly. You must enable this after upgrading to FortiWLC 8.6.0. Navigate to **Configuration > Wireless Intrusion > WIPS > Rogue APs > Global Settings**. For more information on rogue AP settings, see [WIPS - Rogue Access Point Classification on page 7](#).
- FortiWLC 8.6.0 provides end-to-end IPv6 traffic passage on controllers. To use IPv6 capabilities after upgrading to 8.6.0, navigate to **Configuration > Wired > VLAN** and edit the required VLAN.
 - Select **Enable IPv6 Configuration**, the **Override Default DHCP Server** and **DHCP IPv6 Relay Pass-Through** are enabled.
 - Configure the **IPv6 IP Address** and **IPv6 Address of the Default Gateway**. For more information on IPv6 support, see [IPv6 Enhancements on page 15](#).
 - Re-configure LACP if the AP boots up with the LAN2 interface.

What's New

This section describes the new features introduced in this release of FortiWLC.

- [FortiWLC 64-bit OS Support on page 7](#)
- [WIPS - Rogue Access Point Classification on page 7](#)
- [Station Quarantine on page 9](#)
- [QoS Throttle Policies on page 10](#)
- [QoS Load Balancing on page 10](#)
- [Security Audit on page 11](#)
- [DHCP Option 82 on page 12](#)
- [Maintaining ARP Entries For Wireless Bridge Clients on page 13](#)
- [Roaming Across Controllers \(RAC\) Support For 802.11r Clients on page 14](#)
- [NPlus1 Failover Enhancements on page 14](#)
- [ARRP Enhancements on page 14](#)
- [IPv6 Enhancements on page 15](#)
- [802.1x Supplicant Access Point on page 18](#)
- [FAP-U24JEV 2x2 - Modes Of Operation on page 19](#)
- [Zero Wait DFS on page 19](#)
- [User Interface Enhancements on page 20](#)
- [FAP-U431/433F – Additional Features on page 23](#)

FortiWLC 64-bit OS Support

With this release of FortiWLC, all controllers support 64-bit OS ONLY. 64-bit migration images are available to migrate the existing 32-bit FortiWLC-50D, FortiWLC-200D, and FortiWLC-500D hardware controllers to 64-bit, during upgrade to version 8.6.0. See [Upgrading to 64-bit FortiWLC-50D/200D/500D on page 32](#).

All release versions post 8.6.0 (after FortiWLC-50D/200D/500D migration), will have one common 64-bit image file for all the FortiWLC models.

WIPS - Rogue Access Point Classification

The access points detected by the controller are categorized as rogue and friendly based on specific rules that you configure. You can configure multiple rules; these rules are assigned different priorities. When a rogue access point is detected its attributes (ESSID, RSSI, Security mode, and discovered by APs count) are matched against the configured rules and its classification type is defined by the matching rule with highest priority.

You can configure the following detection mechanisms for rogue APs.

- SSID Spoof Detection - SSID spoofing involves rogue access points beaconing same SSID name as a FortiWLC managed AP.
- MAC Spoof Detection - In a MAC spoofing attack, rogue access points beacon same BSSID as a known managed AP, attracting clients and resources to connect to the fake network/SSID for exploiting data. In the case of SSID and MAC spoofing events, clients connected to the rogue APs are de-authenticated and valid notifications are raised about the presence of rogue APs.

Note: SSID and MAC spoofing detection is only for wireless clients.

- Wired Rogue Detection - Classified Rogue APs detected on the wired network.

The classification of APs as rogue and friendly is aided through the configuration of a unique token string. This token is broadcast as part of the beacons.

Navigate to **Configuration > Wireless Intrusion > WIPS > Rogue APs > Global Settings**.

RogueAP Global Settings - Update ?

Global Settings
Allowed APs
Blocked APs
Classification Settings

Detection
☒

Number of Mitigating APs

Max mitigation frames sent per channel

Token

Navigate to **Configuration > Wireless Intrusion > WIPS > Rogue APs > Classification Settings**.

User Defined Rules (2) ?

Global Settings
Allowed APs
Blocked APs
Classification Settings

SSID Spoof Detection
Enable

MAC Spoof Detection
Enable

Wired Rogue Detection
Enable

☒ OK
☐ CANCEL

☒ REFRESH
☒ ADD
☒ DELETE
☒ SETTINGS

	Rule Name	Classification Type	Rule Condition	Rule Status	Issue Minimum Duration	Priority	Action
Q		ALL	ALL	ALL			
<input checked="" type="checkbox"/>	Rule1	Rogue	Match All	Enable	2000	1	<input type="text"/> <input type="text"/>
<input checked="" type="checkbox"/>	Rule2	Friendly	Match Any	Enable	36	2	<input type="text"/> <input type="text"/>

All devices classified as Rogue APs, Suspected Rogue APs, Friendly APs, and Rogue Stations, based on the configured classification settings are displayed on this page.

Navigate to **Configuration > Wireless Intrusion > WIPS > Rogue Classification**.

Rogue APs (empty) ?

Rogue APs Suspected Rogue APs Friendly APs Rogue Stations

[REFRESH](#) [MOVE TO FRIENDLY](#)

	BSSID	SSID	Description	Channel	Reporting APs	Reporting RSSI
Q			ALL			
No Data available						

Station Quarantine

A wireless station perceived to be a security threat can quarantine to a restricted VLAN as a security measure. The connected quarantined wireless station is de-authenticated. FortiWLC receives information to quarantine a station from FortiGate when it detects a security event or a station MAC address can be manually configured to be quarantined.

This feature allows a global quarantine VLAN or per ESS/Port profile.

Navigate to **Configuration > Wireless Intrusion > WIPS > Station Quarantine**.

Quarantine Configuration - Update ?

Configuration Fortigate Configuration Quarantined Stations

Enable Quarantine ☒

Global Quarantine VLAN Tag

Navigate to **Configuration > Wireless > ESS**.

Enterprise Mobility

Dataplane Mode

Dataplane Mode IP Prefix Validation ☒ Tunnel Interface Type

Virtualization Mode

RF Virtualization Mode ACM Support ☐ ACM Voice ☐ ACM Video

General Settings

Hotspot Profile Name New AP's Join ESS ☒ APSD Support ☒

Allow Multicast Flag ☐ Multicast-to-Unicast Conversion ☒ Band Steering Mode

Band Steering Timeout(seconds)

Advanced Settings

Station Quarantine VLAN Tag

[SAVE](#) [CANCEL](#)

.Navigate to **Configuration > Wired > Port**.

Port Profiles - Add ?

Port Profile Name PortProfile1	Enable/Disable <input checked="" type="checkbox"/>	VlanTrunk <input type="checkbox"/>
Dataplane Mode Tunneled	VLAN Name No Data	AP VLAN Policy No VLAN
AP VLAN Tag 0	Security Profile Name default	Primary RADIUS Accounting Server No Data
Secondary RADIUS Accounting Server No Data	Reconnect Primary Server (minutes) 10	Accounting Interim Interval (seconds) 3600
Allow Multicast Flag <input checked="" type="checkbox"/>	IPv6 Forwarding <input checked="" type="checkbox"/>	IP Prefix Validation <input checked="" type="checkbox"/>
Station Quarantine VLAN Tag 460	IP Address Cache Timeout (seconds) 3000	

QoS Throttle Policies

The QoS throttle policies allow bandwidth rate limiting for multicast and broadcast traffic. You can configure and control multicast and broadcast suppression profiles and apply to one or multiple ESS profiles/APs/AP groups.

You can define multicast suppression profiles to allow a collection of specific ports/multicast addresses to be configured within one or multiple ESS profiles/APs/AP groups to allow multicast traffic, thereby providing granular control. A multicast profile can be attached to one or more ESS profiles.

You can define broadcast suppression profiles to open broadcast ports for specific applications limited to small portions of the network. The broadcast profile provides granular control by allowing you to configure IPv4 broadcast ports along with the traffic direction. A broadcast profile can be attached to one or multiple ESS profiles/APs/AP groups.

Navigate to **QoS > Policies > QoS Throttle Policies**.

QoS Throttle Policies (1 entry) ?

Global Quality-of-Service Parameters	QoS and Firewall Rules	QoS Codec Rules	Marking Management Packets	Load Balancing Policies	QoS Throttle Policies
<div> Multicast Profile Broadcast Profile QoS Bandwidth Policies </div>					
<div> REFRESH ADD DELETE SETTINGS </div>					
	Multicast Profile Name	Multicast ID	Owner	Action	
	multicast-test	12345	controller	ALL	

QoS Load Balancing

The QoS load balancing configurations optimize the performance of wireless clients by balancing the load across multiple access points in the network by limiting the clients supported by a single BSSID, handling new clients joining the network, and the aging time of the assigned stations. Thereby, preventing any access point from getting overloaded. The load balancing profile can be applied to specific APs, AP groups, and ESS profiles.

Navigate to **Configuration > Policies > QoS > Load Balancing Policies**.

Add QoS Load Balancing Policy

Name* lb-test1

Max Stations Per BSSID 1

Overflow ☒

Station Assign Aging Time(seconds) 15

Member APs/APGroups and ESS Profiles

ESS* ctet1-csim-bgn-ap

APGroups* APG-1, APG-2

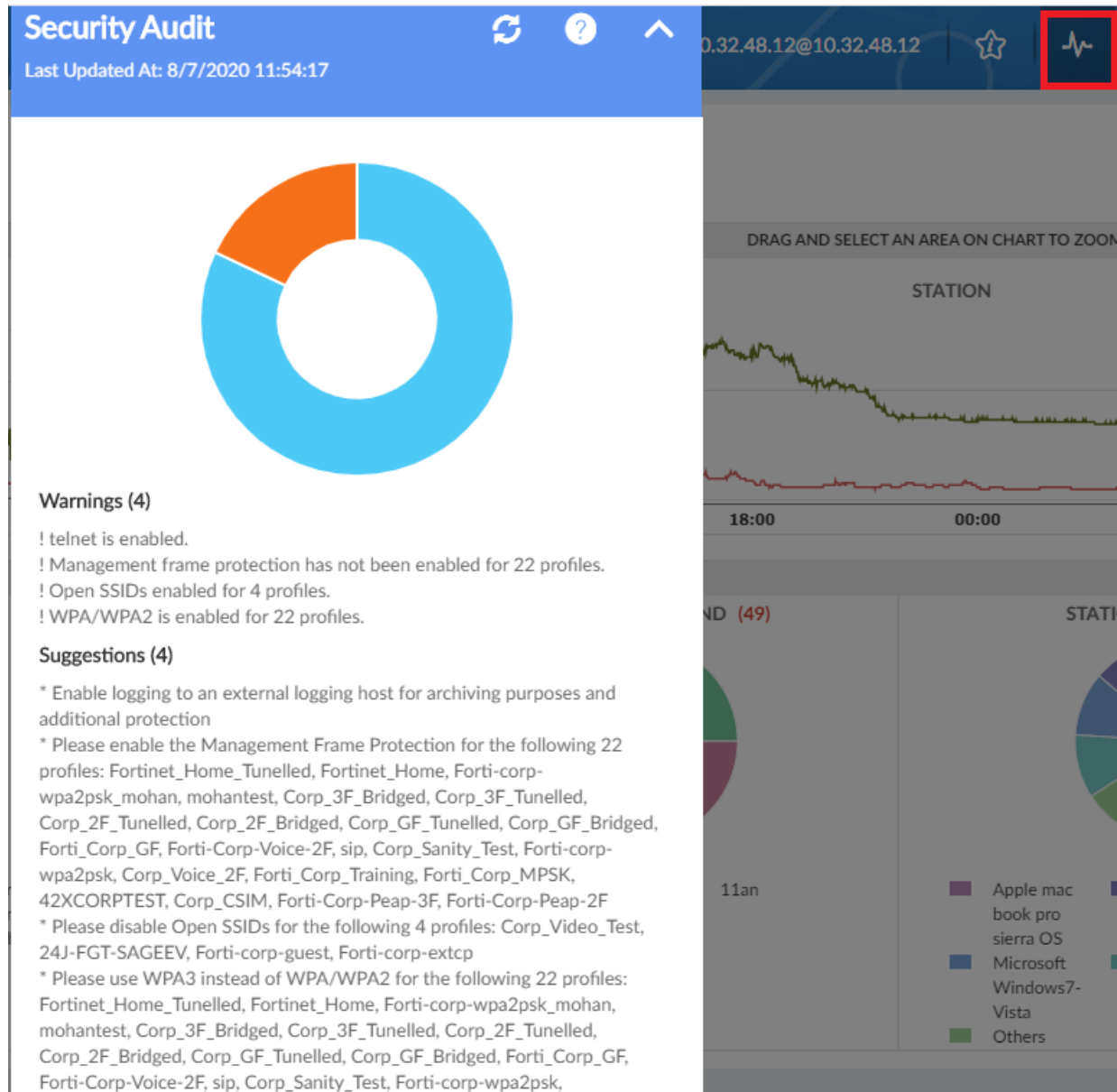
APs* 5 Selected

SAVE CANCEL

Security Audit

The security audit results are obtained by an in-built tool in FortiWLC that keeps your system secure by detecting security related issues and vulnerabilities. The security audit results report the potential risks/vulnerabilities in your system and provides suggestions to mitigate these and optimize your system. The security audit runs an extensive health scan and measures the hardness of your system.

Click on the security audit icon in the FortiWLC GUI home page to view the results.



DHCP Option 82

When DHCP option 82 is enabled, the controller acts as a DHCP relay agent to avoid DHCP client requests from untrusted sources.

This secures the network where DHCP is used to allocate network addresses. The controller adds the DHCP option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server. By default, this option is disabled.

Select the DHCP option 82 remote ID field format as AP-MAC or AP-MAC-SSID.

Notes:

- DHCP relay pass-through should be disabled for the controller to act as the DHCP relay agent.
- This feature is not supported if the data plane mode is bridged.
- This feature is not supported for IPv6.

Navigate to **Configuration > Devices > Controller**.

Global Controller Parameters - Update ?

Controller	Network Parameters	Mobility Parameters	IPv6 Parameters	RA Throttling
Description <input type="text" value="CTET-Controller"/>		Location <input type="text" value="CTET-Lab"/>		
Automatic AP Upgrade <input checked="" type="checkbox"/>		DHCP Server <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>		
Audit poll period (sec)/0 => disabled <input type="text" value="60"/>		Default AP Init Script <input type="text"/>		
Enable DHCP Option 82 <input type="text" value="Enabled"/>		DHCP Option 82 Remotr Id field format <input type="text" value="AP-MAC"/>		
Controller Index <input type="text"/>		Station Aging Out Period(minutes) <input type="text"/>		

You can configure DHCP option 82 with the VLAN settings.

Navigate to **Configuration > Wired > VLAN**.

VLAN Configuration - Add ?

VLAN Name* <input type="text" value="VLAN-Test"/>	Tag* <input type="text" value="10"/>	Ethernet Interface Index <input type="text" value="1"/>
IP Address <input type="text" value="10"/> . <input type="text" value="32"/> . <input type="text" value="x"/> . <input type="text" value="x"/>	Netmask <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	IP Address of the Default Gateway <input type="text" value="10"/> . <input type="text" value="32"/> . <input type="text" value="x"/> . <input type="text" value="x"/>
Override Default DHCP Server Flag <input checked="" type="checkbox"/>	DHCP Server IP Address <input type="text" value="10"/> . <input type="text" value="32"/> . <input type="text" value="x"/> . <input type="text" value="x"/>	DHCP Relay Pass-Through <input type="checkbox"/>
Enable DHCP Option 82 <input type="text" value="Enabled"/>	Maximum number of clients <input type="text"/>	IPv6 Assignment Type <input type="text" value="Static IP address assigned"/>

Maintaining ARP Entries For Wireless Bridge Clients

The wireless disabled clients residing behind a wireless bridge might get disconnected when roaming. With this release, the IP address of such clients is retained for a configured cache timeout period and if the reconnection occurs within this period, the client connectivity is not impacted. This ensures that wireless bridge clients are not disconnected from the controller even if the wireless bridge is disconnected and connected back.

You can configure the **IP Address Cache Timeout** for both IPv4 and IPv6 addresses in the ESS profile.

Navigate to **Configuration > Wireless > ESS**

The screenshot shows a configuration page for FortiWLC. On the left, there is a section for 'AN Base HT Transmit Rates (MCS)' with a grid of checkboxes for MCS 0 through MCS 31. Below this are links for 'AX 2G High Efficiency Settings' and 'AX 5G High Efficiency Settings'. In the center, there are four dropdown menus for '1 Stream VHT Base MCS Set (MCS)', '3 Streams VHT Base MCS Set (MCS)', '1 Stream VHT Supported MCS Set (MCS)', and '3 Streams VHT Supported MCS Set (MCS)', all set to 'MCS 0-9'. Below these is a 'VHT 1024 QAM Support' toggle which is turned on. On the right, there are four more dropdown menus for '2 Streams VHT Base MCS Set (MCS)', '4 Streams VHT Base MCS Set (MCS)', '2 Streams VHT Supported MCS Set (MCS)', and '4 Streams VHT Supported MCS Set (MCS)', also set to 'MCS 0-9'. At the bottom right, the 'IP Address Cache Timeout (seconds)' is set to '25000', highlighted with a red box. A tooltip below it indicates the 'Valid range: [0-36000]'.

Roaming Across Controllers (RAC) Support For 802.11r Clients

The RAC feature is now supported for 802.11r clients. As the clients roam between the controllers configured in the RAC domain, M1 to M4 authentication processes are eliminated; this enables fast roaming and reduces re-authentication latency.

NPlus1 Failover Enhancements

With this release, NPlus1 failover/redundancy can be configured between 64-bit hardware controllers and 64-bit virtual controllers. The following NPlus1 enhancements are additionally delivered in this release.

NPlus1 failover trigger is introduced for the following scenarios:

- Temporary file system full
- Continuous process restarts
- Mail box errors
- CPU running out of RAM memory
- Persistent file system full

New alarms are introduced for all above mentioned NPlus1 trigger scenarios.

ARRP Enhancements

You can perform ARRP configurations for interface 1 and 2 channels and select channels for ARRP participation.

- You can configure the maximum and minimum power levels at ARRP mode. The AP operates within these limits.
- FortiWLC automatically changes parameters such as the transmit power of the connected APs and RF channel as per changing conditions, interference/noise status and other foreign APs in the same environment.
- If an AP failure is detected by a neighboring AP then it automatically tries to reduce the RF coverage gap

by increasing their transmit power.

- Different channels are assigned to APs in case of interferences like microwave, bluetooth and so on.

Note: When global ARRP is enabled, all FAP-U431/433F APs should have the same dual-mode settings (enabled or disabled on APs).

Navigate to **Configuration > Wireless > ARRP**.

Automatic Radio Resource Provisioning ?

Configuration AP - Radio Interfaces

Auto Channel ☒

Ifindex 1 Planning Channel 6 20 MHz

Ifindex 2 Planning Channel 36 40 MHz Extension channel above

Ifindex 1 Custom Channel ☒ All Channels Select Channel

Ifindex 2 Custom Channel ☒ All Channels Select Channel

Ifindex 1 Maximum Power (dBm) 36

Ifindex 2 Minimum Power (dBm) 10

Ifindex 1 Minimum Power (dBm) 10

Ifindex 2 Maximum Power (dBm) 36

Freeze ☒

DFS ☒

Timer State ☐

Neighbour RSSI Threshold -85

Timer (min) 15

IPv6 Enhancements

The access point can discover the controller over an IPv6 address. The following additional IPv6 configurations are now available in FortiWLC.

VLAN Configuration - Navigate to **Configuration > Wired > VLAN**.

VLAN Configuration - Add ?

VLAN Name* VLAN-Test

Tag* 10

Ethernet Interface Index 1

IP Address

Netmask

IP Address of the Default Gateway

Override Default DHCP Server Flag ☐

DHCP Server IP Address 0 0 0 0

DHCP Relay Pass-Through ☒

Enable DHCP Option 82 Enabled

Maximum number of clients

IPv6 Assignment Type Static IP address assigned

IPv6 Address 2001:xxxx:xxxx:xxxx:xxxx:xxxx

Netmask

IPv6 Address of the Default Gateway fe80:xxxx:xxxx:xxxx:xxxx:xx

Override Default DHCP Server Flag ☒

DHCP Server IPv6 Address 2001:xxxx:xxxx:xxxx:xxxx:xxxx

DHCP IPv6 Relay Pass-Through ☒

Enable DHCPv6 Option 82 Enabled

Maximum number of IPv6 clients 5

Enable IPv6 Configuration ☒

Fwd IPv6 MLD Report ☒

Enable IPv4 Configuration ☐

Access Point network connectivity - Navigate to **Configuration > Devices > APs > Connectivity**.

Management Interface - Navigate to **Configuration > Devices > System Settings > Management Interfaces**.

Management Interface-Add

VLAN Name*
VLAN1

Interface Number
1

Tag
10

IP Address
[][][][]

NetMask
[][][][]

Default Gateway
[][][][]

IPv4 Assignment Type
Static IPv4 address assigned

Interface Mode
Active

IPv6 Address
2001::xxx:xxx:xx:xxxx:xxx

IPv6 Assignment Type
Static IPv4 address assigned

Enable IPv4 Configuration
☐

NetMask
[][][][]

IPv6 Default Gateway
fe80::xxxx:xxxx:xxxx:xx

Enable IPv6 Configuration
☒

Router Advertisement (RA) Throttling

RA throttling enables the controller to restrict RA packets in a wireless network. This prevents excessive bandwidth consumption by multicast IPv6 RA messages over the wireless edge of a switched network. The RA packets are reduced to a minimum without impacting IPv6 client connectivity. Roaming clients and new clients are not impacted with RA throttling.

Navigate to **Configuration > Controller > RA Throttling**.

RA Throttling Configuration Parameters (1 entry) ⓘ

Controller Network Parameters Mobility Parameters IPv6 Parameters **RA Throttling**

Enable RA Throttling
☒

Throttle Period(In seconds)
600

Max Through
10

At Least
1

At Most
1

Owner
controller

Show Detail Info...

Neighbour Discovery (ND) Proxy

The ND proxy feature provides support for proxying the IPv6 ND protocol to allow the forwarding of ICMP messages between upstream and downstream interfaces.

ND proxy uses ICMPv6 messages such as Neighbor Solicitation (NS) and Neighbor Advertisement (NA). The ND proxy enabled interface unicasts an NS message on behalf of a host to a wireless client. The interface modifies the packet to include the wireless client MAC address only; the wireless client responds with a unicast NA message to that host.

The implementation of ND proxy is based on [RFC 4389](#).

IGMP Snooping

IGMP Snooping helps an L2 device make intelligent multicast forwarding decisions by sniffing for the IGMP protocol messages and building a multicast forwarding table; hence, it can significantly reduce traffic from streaming media and other bandwidth-intensive IP multicast applications.

IGMP snooping is now supported for IPv6.

Recommendations

Note the following with respect to IPv6 discovery in FortiWLC 8.6.0.

- Use only one prefix in RA advertisements.
- When using DHCP, the prefix lifetime should be high to avoid IP changes.
- The DHCP and default gateway must be the same in a pure IPv6 environment.
- Use a prefix-based/stateless configuration when FortiGate is used as the IPv6 DHCP server for APs.
- **IPv6, Override Default DHCP Server Flag**, and **DHCP IPv6 Relay Pass-Through** should be enabled on the VLAN interface for IPv6 bridging (pass-through) to work.
- Enable neighbor discovery optimization (**Configuration > Devices > Controller > IPv6 Parameters**).

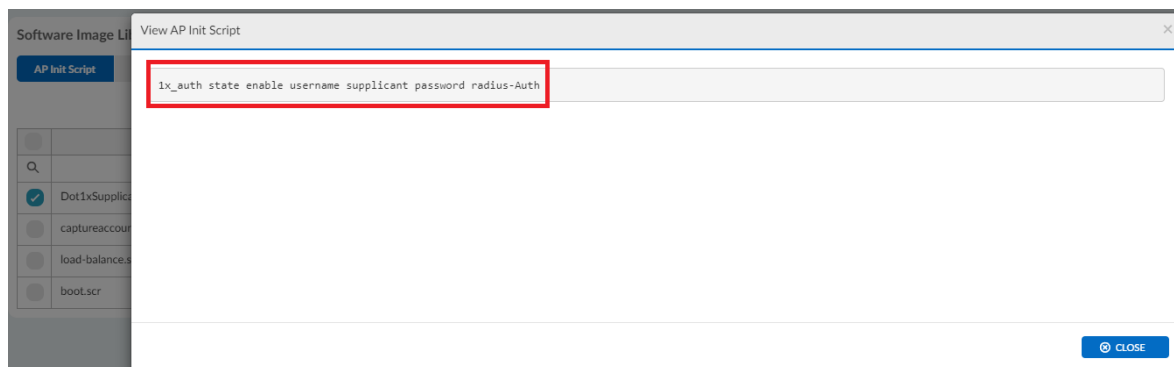
802.1x Supplicant Access Point

You can now configure the FAP-U42xEV, FAP-U422EV, and FAP-U32xEV access points as an 802.1X supplicant for port based authentication. The 802.1X supplicant access point is authenticated by an external RADIUS server based on the configured credentials (user name and password). The switch is the authenticator between the supplicant access point and the external RADIUS server.

Note: This feature is tested in a setup of 15 access points.

This feature is disabled by default and is enabled using the FortiWLC CLI or GUI. To enable and configure this feature while configuring an AP:

- Run the **1x_auth state enable username <username> password <password>** command. To disable, run the **1x_auth state disable** command.
OR
- Create an initialization script. Navigate to **Maintenance > File Management** on the FortiWLC GUI.



Note: Change in the username and password for 802.1X authentication takes effect only after the AP is rebooted.

FAP-U24JEV 2x2 - Modes Of Operation

With this release, the FAP-U24JEV supports operating its only 2x2 physical radio as a single 2x2 interface or two concurrent 1x1 interfaces.

You can configure the radio 1 MIMO mode from GUI/CLI in following modes.

1x1 - Concurrent radio mode (Default)

Two 1x1 interfaces on the AP and controller.

- Interface-1 supports only 2.4 GHz with the default channel 6.
- Interface-2 supports only 5 GHz mode with default channel 36.

2x2 - Single radio mode

Supports dual band operation and the default configuration is 2.4 GHz with channel 6, one 2x2 interface on the AP and controller.

- Interface-1 (2x2) is up and running, all configurations on interface-1 are reflected on the AP.
- Interface-2 (1x1) status is **Administrative Status: SingleInterface** and **Operational Status: Disabled**.
- The AP operates in the single radio mode and brings down interface 2.
- This is applicable only on AC/AN/BGN RF bands.
- If interface-1 is in 5 GHz band/2x2 MIMO mode and is changed to 1x1 MIMO mode then you are required to change the RF band and channel width to 20 MHz.
- Interface-2 settings are disabled from the GUI and no configuration is permitted.

Mixed Configurations

Multiple modes are allowed, that is, a combination of 2x2 and 1x1 APs.

- Apply global configuration on all or specific APs using bulk update - **Configurations > Wireless > Radio > Interface 1 > Bulk Update**.
- Apply to multiple feature groups, for example, one feature group with 2x2 enabled on interface-1 and another feature group with 1x1 enabled on both interfaces - **Configuration > Quick Start > Feature Group**.

Note:

- AP reboots when changing from 1x1 MIMO mode to 2x2 MIMO mode or vice versa. The **sh ap-reboot-event** CLI Command output displays **config-wireless-if-chan** as the reason for reboot.
- Mixed configurations are not supported with ARRP enabled.

Zero Wait DFS

Enable Zero Wait DFS to enable seamless transition to a target DFS channel with almost no additional delay.

Navigate to **Configuration > Wireless > Radio** and update the wireless interface configuration page.

Wireless Interface Configuration - Update ?

Wireless Interface	Wireless Statistics	Antenna Property
AP ID 1	Index 2	AP Model FAP-U421EV
Feature Group 0		
AP Mode Service Mode	Interface Description ieee80211-1-2	Administrative Status Up
RF Band Selection 802.11ac	Primary Channel 36	Channel Width 40 MHz Extension channel above
MIMO Mode 4x4	Short Preamble <input type="checkbox"/>	Transmit Power(EIRP) 23
B/G Protection Mode Auto	HT Protection Mode Off	802.11n only mode <input checked="" type="checkbox"/>
Probe Response Threshold 15	Mesh Service Admin Status <input checked="" type="checkbox"/>	Transmit Beamforming Support MU MIMO
STBC Support <input checked="" type="checkbox"/>	DFS Fallback Option <input checked="" type="checkbox"/>	DFS Fallback Channel 153
DFS Channel Revertive(minutes) 30	Set Prob Rsp Assigned Only <input checked="" type="checkbox"/>	ZWDFS Option <input checked="" type="checkbox"/>

User Interface Enhancements











This release introduces a new user interface design to improve the FortiWLC accessibility and usability experience. The enhanced visual design provides improved aesthetics and look-and-feel to the user.

The user interface is reorganized to provide the features and functionalities in a distinctive way so as to help the user find information without much browsing and also to ease navigation. The new user interface makes the FortiWLC more interactive and easier for the user to monitor and manage the elements in their network.

The user interface is segregated into four buckets.

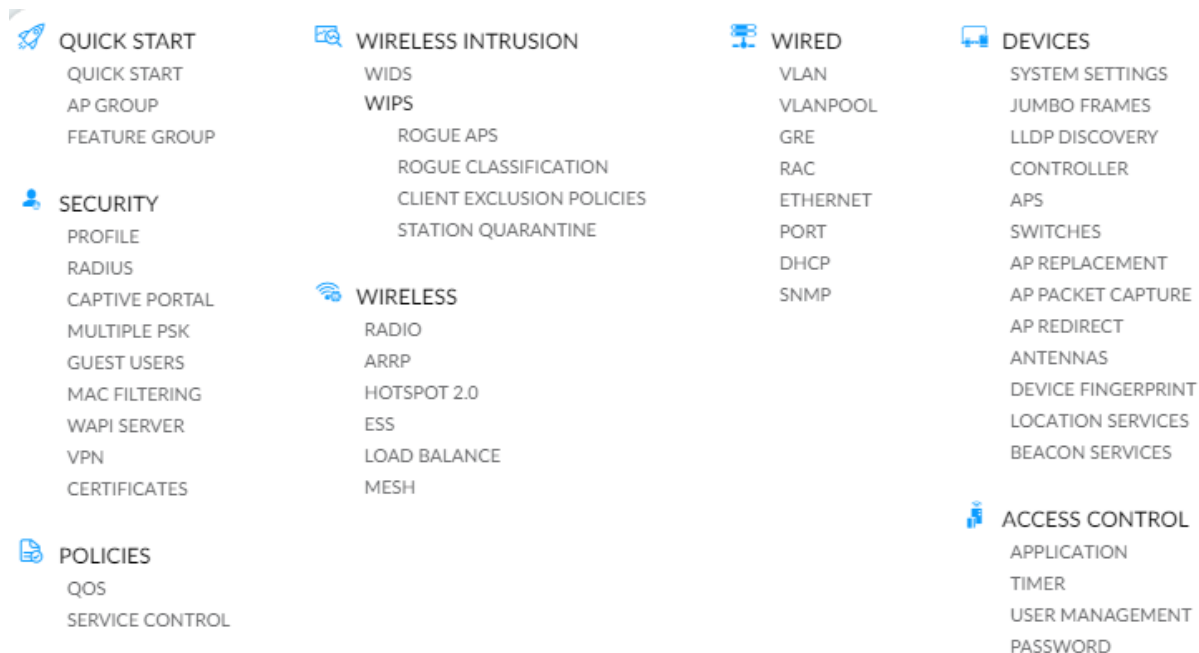
Monitor

The monitor dashboards provide a summary view of all WLAN statistics. The graphical representation of system and device level statistics, diagnostic, topology, and spectrum manager gives a glimpse of the wireless network, based on the current and historical data stored in the database.

 DASHBOARD SYSTEM RADIO STATION VOICE WIPS	 DEVICES ALL STATIONS WIRELESS WIRED PHONES ASSOCIATIONS ROGUE DEVICES SYSTEM RESOURCES BEACON APS	 TOPOLOGY DISCOVERED DEVICES ASSIGNED STATIONS AP WIRELESS RESOURCES EDGE RECORDS STATION TOPOLOGY
 FAULT DASHBOARD FAULT MANAGEMENT		 TOP 10 TOP10 STATION PROBLEM TOP10 STATION TALKER TOP10 AP PROBLEM TOP10 AP TALKER
 SPECTRUM MANAGER CONSOLE SETTINGS	 STATISTICS WIRELESS STATISTICS WIRED STATISTICS	
 DIAGNOSTICS RADIO STATION INFERENCES	 QOS/VOICE QOS FLOWS PHONE CALLS CAC PER AP CAC PER VIRTUAL CELL	
 GLOBAL STATISTICS SECURITY COUNTERS QOS COUNTERS		

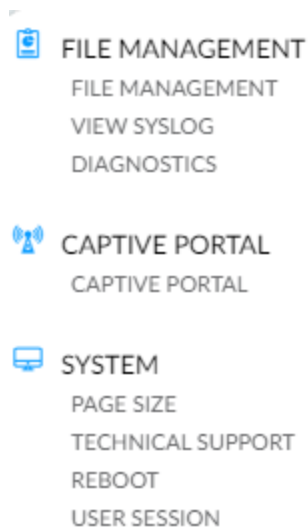
Configuration

The configuration menu allows you to configure and manage multiple controllers, access points, and stations. You can create common configuration and apply it to multiple devices in your network.



Maintenance

The maintenance menu allows you to monitor and manage files, syslog, and diagnostic information, create customized captive portals, and perform system related operations.



Wizards

The EzSetup or the Easy Setup for FortiWLC assists you in setting up the WLAN System when controller is turned on first time, it will come up with a default IP address.



FAP-U431/433F – Additional Features

The following features are now supported on the FAP-U431/433F APs.

- Remote RADIUS
- Proxy ARP
- Captive Portal AP Offloading
- QoS Bridge Mode
- Port Profile on uplink
- ZW-DFS

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-U433F PSM3x
*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	8.6.0
FortiConnect	16.9.8, 17.0
Browsers	
FortiWLC (SD) WebUI	Internet Explorer 11 Mozilla Firefox 69 Google Chrome 77
Note:	

Hardware and Software	Supported
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.

- 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.

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 FAP-U431/433F

Apply this upgrade procedure to laptops (with Intel Wi-Fi drivers installed) for connectivity to FAP-U431/433F 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.

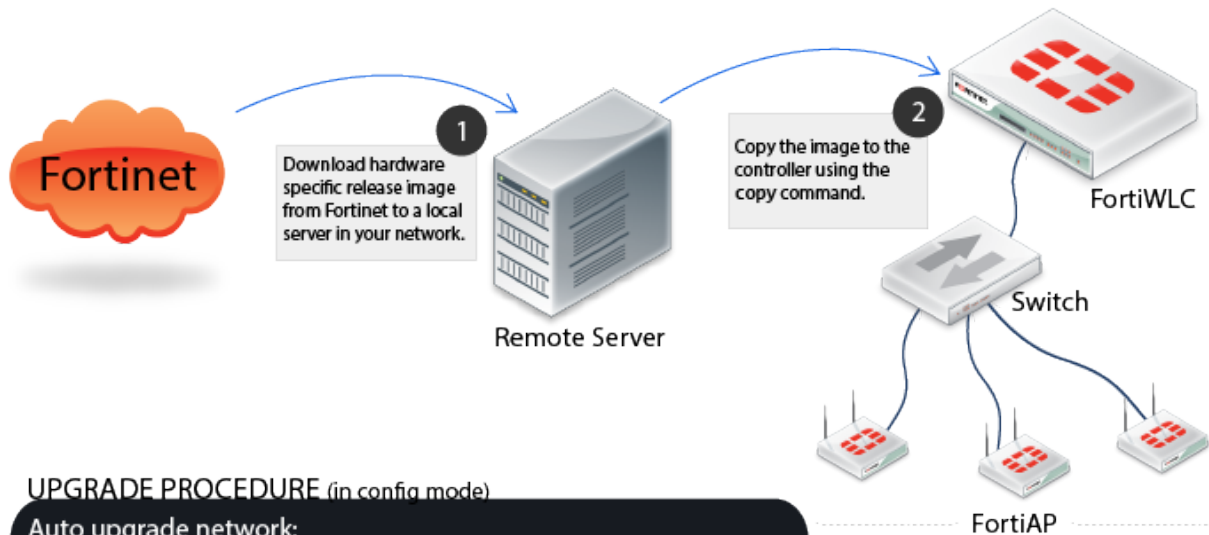
You are now able to see the ESSID.

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

For more information on deploying FAP-U431/433F, see the *FAP-U43xF Deployment Guide*.

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, and FortiWLC-500D controllers. See section [Upgrading FortiWLC-1000D and FortiWLC-3000D on page 33](#) to upgrade FortiWLC-1000D and FortiWLC-3000D. See [Upgrading Virtual Controllers on page 36](#) 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-8.6-0-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...
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.4.8, 8.5.0, 8.5.1, 8.5.2	8.5.3
8.4.7, 8.4.8, 8.5.1, 8.5.2, 8.5.3	8.6.0

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

This release of FortiWLC supports 64-bit OS on FortiWLC-50D/200D/500D hardware controllers. 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-U431/433F Support

You are required to download the FAP-U431/433F image file as it is NOT bundled in the controller image. Follow this procedure to download and install the FAP-U431/433F image.

Note: Direct upgrade to 8.6.0 can be done from releases 8.4.0 and above.

1. Download the FAP-U431/433F image file from the remote server to the controller.
For example,
[FortiWLC controllers]
`copy scp://download:download@<remote_server_IP>/<image_file_location>/forti-8.6-0build-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 FAP-U431/433F 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 : image0
On reboot : image0
```

```
-----
Running image details.
System version: 0.3.14
System memory: 231M/463M
Apps version: 8.5-3build-4
Apps size: 251M/850M
-----
```

```
-----
Other image details.
System version: 0.3.14
System memory: 240M/473M
Apps version: 8.6-0build-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.

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.

Software Image Library and Logs ?

AP Init Script
Diagnostics
SD versions
Patches
Syslog

REFRESH
IMPORT

Running image	image1
On reboot	image1

Running Image Details :	
System version	0.7.8
System memory	150M/473M
Apps version	8.6-0reldev-3
Apps size	108M/849M

Other Image Details :	
System version	0.6.3
System memory	206M/463M
Apps version	8.5-3reldev-3
Apps size	172M/850M

- 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. Run 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, 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>:<passwd>@<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 34](#), [Upgrading via GUI on page 34](#), and [Upgrading an NPlus1 Site on page 36](#).

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.

AP Reboot/Stability

Tracking ID	Description
461565	Clients not handed off to the next AP after current AP reboots.
489958	[FAP-U42xEV] Random AP reboot.
582097	[AP832i] High AP memory usage observed.
582501	[AP822/AP832] Random TCP traffic drops observed.
603757	[All FAP-Us] Random Rx freeze/Mac suspension and failure.
605472	[AP832] Random AP reboot.
610232	[FAP-32xEV] Random AP reboot.
617054	[AP832/AP822] Random AP reboot.
626843	[FAP-U22xEV] Mesh leaf APs random reboot.
632372	[FAP-U431/433F/42xEV/32xEV] Unresponsive AP remained in a disabled offline state.
633745	[FAP-U22xEV] Soft lockup issues observed.
652724	Random AP reboot.
655484	[FAP-U22xEV] Random AP reboot.
663363	[AP8xxx] Random AP reboot.

Captive Portal

Tracking ID	Description
618583	External captive portal ClearPass did not redirect to authentication success page.
650554	External captive portal issues with Cisco ISE.
674931	Captive portal redirect issue on IE due to an additional slash in the URL.

Configuration – Controller/AP

Tracking ID	Description
523651	LACP configuration for APs requires to be simplified.
615057	Port Profiles not synchronized with APs after maintenance work.
632272	[OAP832e] LED status for LAN2 interface is ON with no devices connected.

Controller Processes/Sluggishness

Tracking ID	Description
519766	Random Kernel crash triggered controller failover.
553667/599891	Random Melf process crashes observed.
561751	Random SIP crashes observed.
571080	Random SecurityMM crashes observed.
610226	Random controller reboot.
659881	Random SecurityMM crashes.
660826	Random Hostapd crash observed.
660962	SNMP process did not restart after controller reboot.
665284	[Spectralink] The controller crashed as the phones register to two different SIP servers.
671626	SNMP walk returns <i>No Such Object available on this agent at this OID</i> error.

GUI/CLI

Tracking ID	Description
538370	Unable to change the timezone via CLI.
571716	The <i>station-log issues</i> command did not accept arguments.
575926	The <i>show sys-summary ess</i> command output required to sort by ESSID name.
577886/582086	The <i>show sys-summary ess</i> command displayed incorrect data.
580828	The <i>stadb display assigned</i> command displayed incorrect RSSI/SNR values for DFS channels.
581719	The <i>show station</i> command output displays error in reading <i>json</i> string.
633492	The <i>station-log show</i> command did not work after upgrade.
638018	Unable to access controller through GUI after upgrade.
658189	The error <i>ERROR_CONVERSION_NOT_POSSIBLE Type: NmsL2SecurityMode_t</i> displayed on the Monitor > Devices > All Station GUI

Tracking ID	Description
	page when WPA3-SAE client connected to the AP.
681595	Unable to save configuration to startup on the GUI using Privilege level 10 user account.

Intermittent Connectivity

Tracking ID	Description
420129	[All APs] SIP call processing failure.
445677	[AP822v2] Inconsistent beaconing for Native Cell ESS.
466162	Beacon transmission is stopped for more than 1 second.
503648	[AP822] While roaming, the station cannot be assigned to another AP if it receives authentication from an AP and then moves quickly.
557247	The interface Dot11radio operational state was disabled due to wncagent restart.
563702	Client connectivity issue observed with APs stuck in Disabled-Online state and high wncagent CPU utilization.
605954	DHCP server pool exhausted; unable to allocate IP addresses to new clients.
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
652763	FortiWLC generates unwanted syslog messages.
655712	Critical/Major/Minor CPU usage events observed in station log.
675136	Station activity logs are inserted at wrong timestamp.

NPlus1

Tracking ID	Description
565275	Station did not get the IP address after Nplus1 takeover.
566148	SNMP service did not start on the slave controller following NPlus1 failover.
654653	Service connect did not work after NPlus1 failure due to incomplete configuration synchronization.
662947	NPlus1 master controller reboot after upgrade without any logs.

Others

Tracking ID	Description
434051	Default H.323 QoS rule prevented video call establishment.
562158	Removal of CAPWAP message during upgrade.
606199	[AP122] Wired client on yellow port (clear port profile) show up connected on AP network during boot up.
634204	[FAP-U32xEV] Updated the antenna gain values.
639737	[BGN] Displays in station-log inspite of 5GHz probing
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
627642	Rogue AP sub rule names added from the GUI do not support special characters such as &, #, ??, \.		Add the sub rule in the CLI mode.
636630	DHCP pool configuration is not retained after upgrade.		
670270	Sometimes, the GUI prompts for login credentials in Chrome when navigating to other pages.		
685389	[FAP-U32x/42xEV] VLAN trunking is not working.		
683287	LACP configuration is not retained after upgrade.		

The following known issues are specific to IPv6 discovered APs.

Tracking ID	Description	Impact	Workaround
635268	The AP does not discover the controller if <i>v4v6</i> is set to <i>V6only/V6preferred/V4preferred</i> and <i>ipv6</i> is set to <i>none</i> in the AP configuration CLI mode.		
640425	With lower PMTU configured, remote AP scenarios fail (packet size more than 1470).	The client does not receive all IPv6 multicast traffic.	Use default PMTU.
653079	Internal DHCPv6 feature does not work after NPlus1 failover.		
684367	Browsing is sluggish if connected to APs discovered over IPv6 with IPsec configured.		
685396	IPv6 forwarding does not work after upgrade to 8.6.		<ul style="list-style-type: none"> Edit the VLAN interface and enable IPv6 configuration. Edit the ESS profile

Tracking ID	Description	Impact	Workaround
			and enable IPv6 Forwarding.

The following known issues are specific to FortiWLC 64-bit OS support migration.

Tracking ID	Description	Impact	Workaround
665917	Custom captive portal mode changes to default during migration.		Configure captive portal after migration.
676617	[NPlus1] Slave controller is inaccessible after migration.		Disable NPlus1 after migration.
684659	The syslog host is lost after migration.		Configure the syslog after migration.

Common Vulnerabilities and Exposures

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

- CVE-2004-1653
- CVE-2019-6110
- CVE-2019-6111
- CVE-2019-11479
- CVE-20XX-XXXX

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



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.