FORTINET
High Performance Network Security

FortiWLC

Release 8.5.0

Contents

About FortiWLC 8.5.0

FortiWLC release 8.5.0 introduces new features such as IPsec, LLDP protocol support, multiple PSK security mechanism, IPv6 support extension, and REST APIs to enhance the controller and access points' capabilities. For more information, see sections New Features and Enhancements.
This release also fixes some outstanding product issues, see section Fixed Issues.

The following are some **important points** specific to this release of FortiWLC.

- Direct upgrade to 8.5.0 is supported using the *.fwlc* file format only.
  FortiWLC with versions **prior** to 8.4.0 require an intermediate upgrade to 8.4.0 or later (using *rpm.tar* file format) before upgrading to 8.5.0 release (using *rpm.tar.fwlc* file format).
  Note that the *.fwlc* file format is supported from release 8.4.0.

- It is recommended **NOT** to use these features in production networks and scale deployments.
  - Internal Captive Portal (**Note**: High CPU usage for Xems and Apache process might be noticed in case of high concurrent Internal Captive Portal requests.)
  - Internal DHCP server
  - DHCP relay

- In scale deployments, delay in the output display of show commands/GUI data refresh is observed.

- This release onwards the MC-VE series virtual controllers are **NOT** supported.

New Features

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

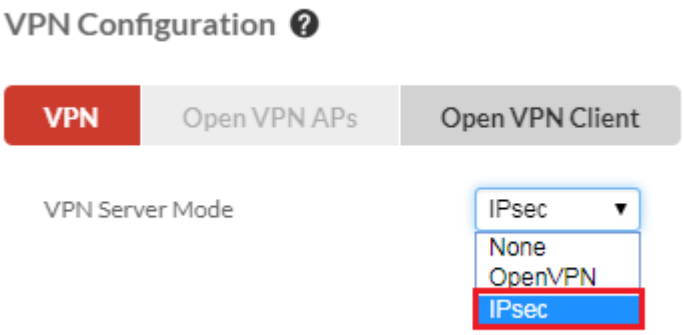
- IPsec Encryption Mode
- LLDP Discovery
- Multiple PSK Support
- IPv6 Support
- REST APIs

IPsec Encryption Mode

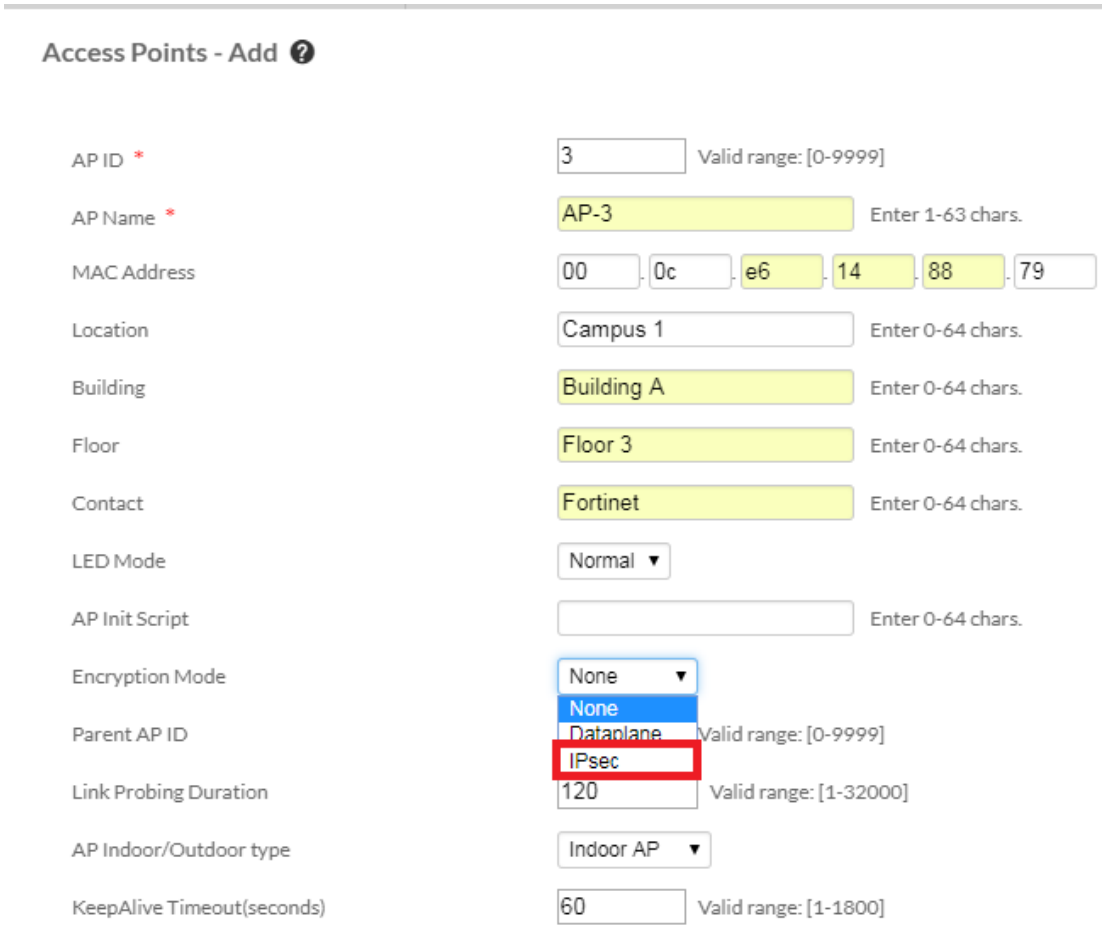
This release of FortiWLC supports encryption and decryption of traffic between controller and access point using the IPsec protocol. While configuring the access points, you can specify the **Encryption Mode** for the type of traffic between the controller and the access point.

NOTE:
IPsec is supported only on 11 ac access points.

Select IPsec as the **VPN server mode**, prior to configuring the data encryption mode to IPSec. Navigate to **Configuration > Security > VPN**.



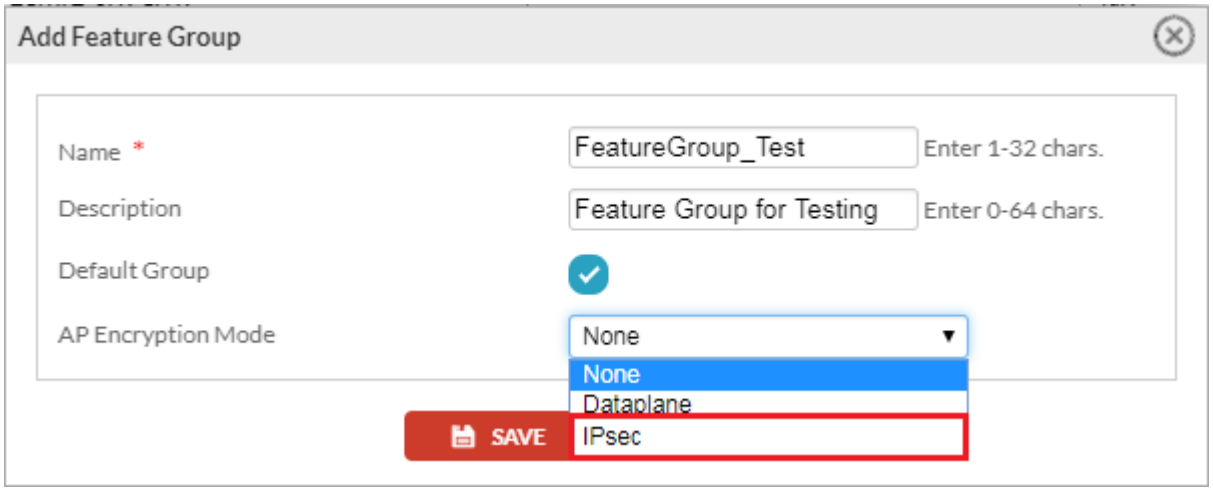
To configure the data encryption mode, navigate to **Configuration > Device > APs > Add**.



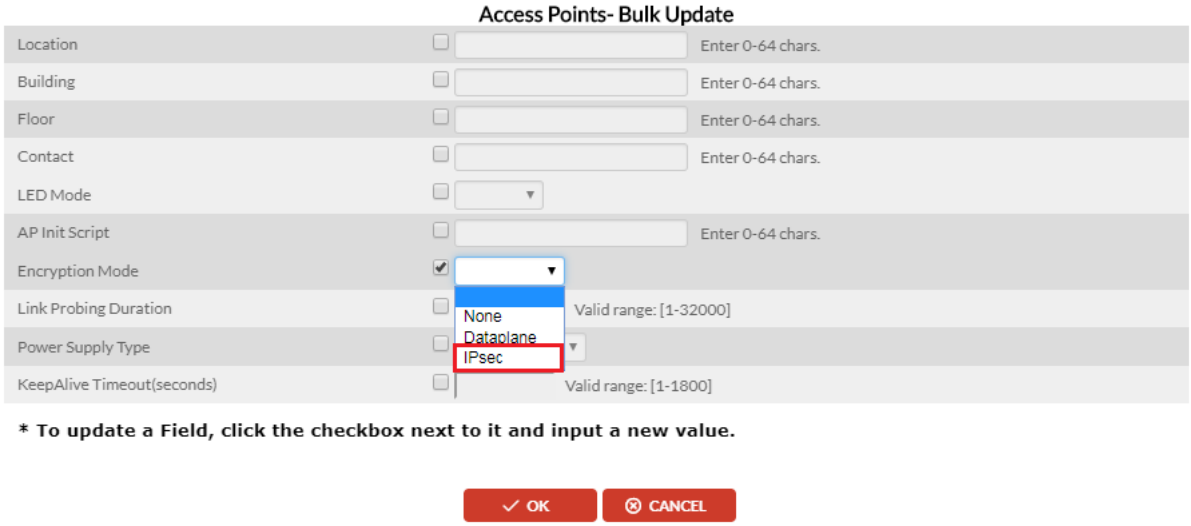
The following are the supported encryption modes:

- **None**: This is the default option selected for the access point. No encryption is applied.
- **Dataplane**: This mode enables encryption only for the data path. DTLS is used to encrypt the data traffic.
- **IPsec**: This mode enables encryption of all traffic between the AP and controller (both the control and data path).

The IPsec encryption mode can be applied to the access points in a feature group as well. If the access point being added to the feature group has a different encryption mode then, by default, it is modified to the encryption mode configured for the feature group. Navigate to **Configuration > System Config > Feature Group > Add**.



The IPsec encryption mode can be configured when performing a bulk update on access points. Navigate to **Configuration > Devices > APs > Bulk Update.**



LLDP Discovery

The Link-Layer Discovery Protocol (LLDP) is a layer-2 neighbor discovery protocol that allows network devices to advertise specific information about themselves to other devices on the network and receive information from them.

LLDP neighbor discovery by both controllers and access points is supported. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighboring devices. Devices advertise information such as chassis ID, port ID and description, system name and description, system capabilities, and management IP addresses.

This protocol is supported on all FortiWLC controllers and 11ac access points. This feature of FortiWLC facilitates efficient network management by being aware of its neighbors and also locating defunct access points in the network.

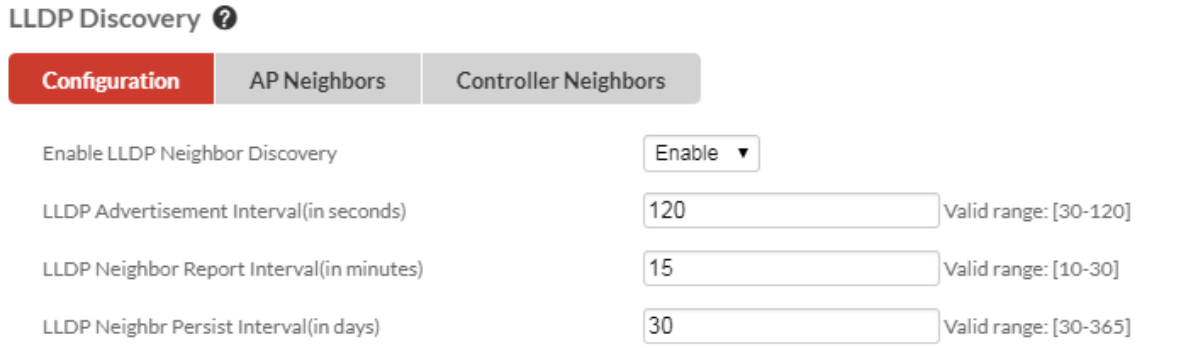
The controller and access points advertise information using LLDP periodically to their

neighboring switches at a configured interval of time. The controller maintains a database of LLDP information received from its neighboring switches. The access points send LLDP information about the neighboring switch along with its own details to the controller periodically at a configured reporting interval of time. This information from the access points is also stored on the controller database. The Controller persists the stored information in its database for a configured period of time and then discards it.

To enable and configure the LLDP neighbor discovery feature navigate to **Configuration > Devices > LLDP Discovery**.

Notes:

- LLDP discovery is supported only on 11ac APs.
- LLDP discovery is NOT supported on Mesh APs.
- In an N+1 setup, the active slave controller sends/receives LLDP messages from the switch connected to it.
- Prior to enabling LLDP discovery, ensure that LLDP is enabled globally or in each port of the neighboring switches.
- LLDP discovery is not supported for the AP interface where wired station is connected.



The **AP Neighbors**, that is, the access point information along with their corresponding switch information (*Neighbouring Switch Name*, *Neighbouring Switch Port*, and *Neighbouring Switch Management IP*) that is received by the controller is displayed.

AP Neighbors - Details

AP Id	1
AP Name	AP-1
AP Interface Name	eth1
AP Ethernet Interface	0
AP Management IP	10.33.94.16
MAC Address	00:0c:e6:41:38:30
Neighbouring Switch Name	FS108D3W17004789
Neighboring Switch Port	port5
Neighboring switch Management IP	192.168.1.99
Time to Live	30

The **Controller Neighbors**, that is, the controller information along with their corresponding switch information (*Neighbouring Switch Name*, *Neighbouring Switch Port*, and *Neighbouring Switch Management IP*) is displayed.

Controller Neighbors - Details

Ctrl Ethernet Interface	0
Ctr Interface Name	eth0
MAC Address	00:0c:29:94:02:c6
Neighbouring Switch Name	FortiWLC
Neighboring Switch Port	eth0
Neighboring switch Management IP	10.34.112.48
Time to Live	30

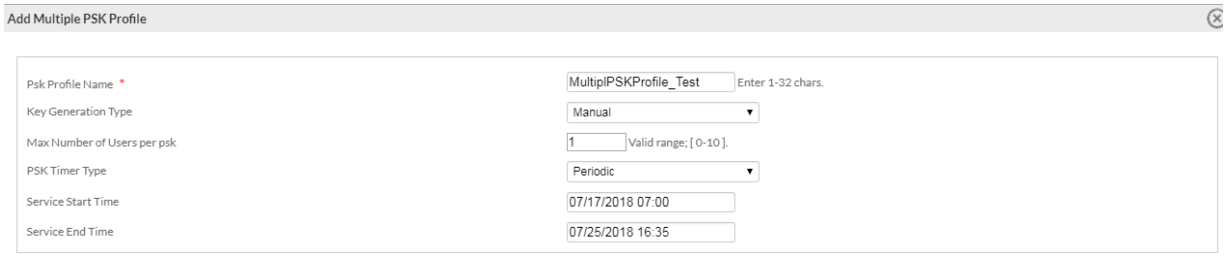
Multiple PSK Support

The Multiple Pre-shared key (PSK) is a shared secret method added to the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption methods for WPA/WPA2 authentication. The multiple PSK feature of FortiWLC allows generation of unique pre-shared encryption keys for each wireless user (the valid range for the number of clients is 0-10. A value of 0 means that a single PSK can be used by an unlimited number of users/devices). The clients are authenticated and allowed access to the network based on the verification of these keys.

Multiple keys can be generated, distributed, and managed across different clients. A maximum of 256 multiple PSK profiles and 2048 groups can be created with a maximum of 16k keys. These keys can be generated for one profile or be distributed across profiles. Only one PSK profile is associated with one ESS profile. Each PSK profile is created based on the key generation method, whether manual or automatic. Once the authentication key is generated, e mails can be triggered to send the PSK information to the user. Note that e mails can be triggered successfully only when the DNS Server and SMTP are configured at *Configuration > Devices > System Settings*.

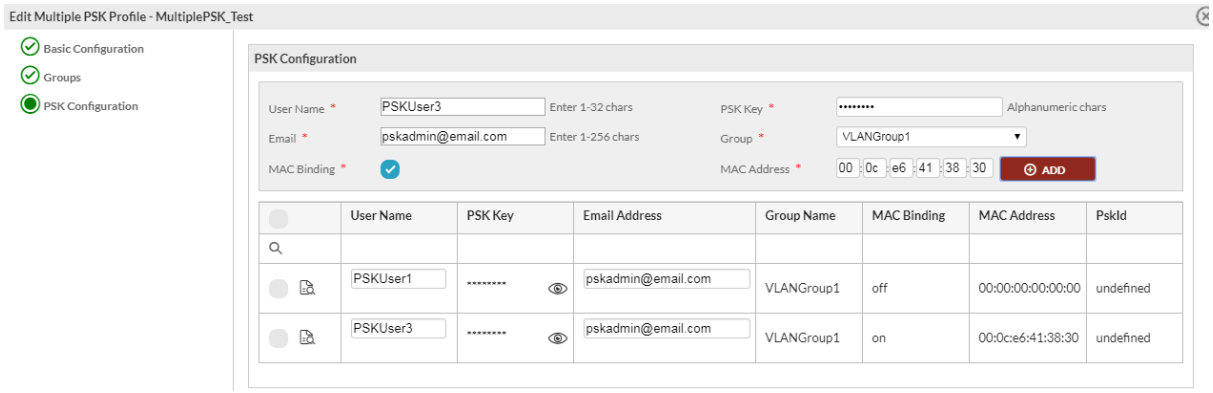
These keys are valid till their configured timeout period. You can create multiple groups and the groups can be assigned to different PSK keys within the same profile. Configure the PSK profile in the Security profile to link it to the ESS profile. Once created, the PSK profile can be edited to assign VLAN groups and configure the **Key Generation Type** (selected while creating the PSK profile).

Navigate to **Configuration > Security > Multiple PSK > Add**.



Multiple PSK feature supports an **Absolute** or **Periodic** timer. An absolute timer sets a single expiry time and starts immediately after the PSK profile creation. A periodic timer sets a start and end time for the PSK profile. The PSK profile is valid only till the timeout.

Once created, the PSK profile can be edited to assign VLAN groups and configure the **Key Generation Type** (selected while creating the PSK profile).



For each PSK you can view the start time, end time, and PSK ID in the configured RADIUS accounting server. This is a sample of messages viewed on the RADIUS server.

ACCOUNTING START

Ready to process requests
(0) Received Accounting-Request Id 87 from 10.33.94.97:59207 to 10.33.92.16:1813 length 259
(0) Acct-Status-Type = Start
(0) Acct-Session-Id = "5BB13F12-00000008"
...
(0) **Mpsk-Start-Time = "01-10-2018 03:26:28"**
(0) **Mpsk-Psk-Id = "4ee8f7ea1de894bf03d4af7007e48d99"**

ACCOUNTING INTERIM UPDATE

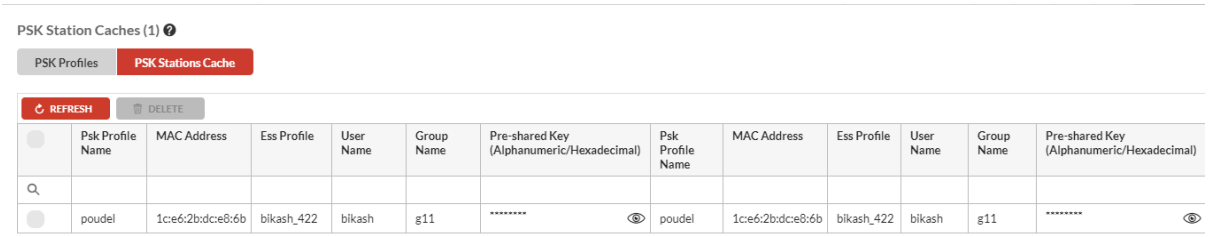
Ready to process requests
(1) Received Accounting-Request Id 88 from 10.33.94.97:59207 to 10.33.92.16:1813 length 262
(1) Acct-Status-Type = Interim-Update
...
(1) **Mpsk-Psk-Id = "4ee8f7ea1de894bf03d4af7007e48d99"**

ACCOUNTING STOP

Ready to process requests
(7) Received Accounting-Request Id 94 from 10.33.94.97:59207 to 10.33.92.16:1813 length 301
(7) Acct-Status-Type = Stop
...
(7) **Mpsk-End-Time = "01-10-2018 03:31:52"**
(7) **Mpsk-Psk-Id = "4ee8f7ea1de894bf03d4af7007e48d99"**

PSK Station Cache

The users authenticated with a PSK, will have their details cached here. The associated client **MAC Address**, **ESS Profile**, **Pre-shared Key**, **Group Name**, and **User Name** with which the client got authenticated are displayed. If the PSK profile is removed from the Security Profile or is deleted, then the PSK profile cache is also deleted. The cache is not added for MAC bound PSK profile.



When a user inadvertently enables more than one wi-fi supplicant (for example, Windows wireless zero configuration and Intel utility) in the wireless client and if there is a password/PSK change to the ESSID which the utilities connect to; wireless connectivity issues will occur if the password/PSK is not updated in both the utilities.
As a **workaround**, do a *Forget Network* from both the utilities and try to connect with the new password/PSK.

Note: Fortinet recommends the use only one wireless utility.

IPv6 Support

This release of FortiWLC enhances IPv6 support for wired and wireless clients. IPv4, dual stack (IPv4+IPv6), and native IPv6 clients co-exist in the network. The FortiWLC is now accessible over the SSH/telnet/SNMP from IPv6 addresses. The FortiWLC GUI can be accessed over the IPv6 address of the controller. To access the GUI over IPv6, enter the URL in the format*: https://[IPv6_address_of_WLC]* in the browser, for example, *https://[2001:470:ecfb:45c:428d:5cff:fe5e:c588].* The GUI can be accessed over the HTTPS protocol.

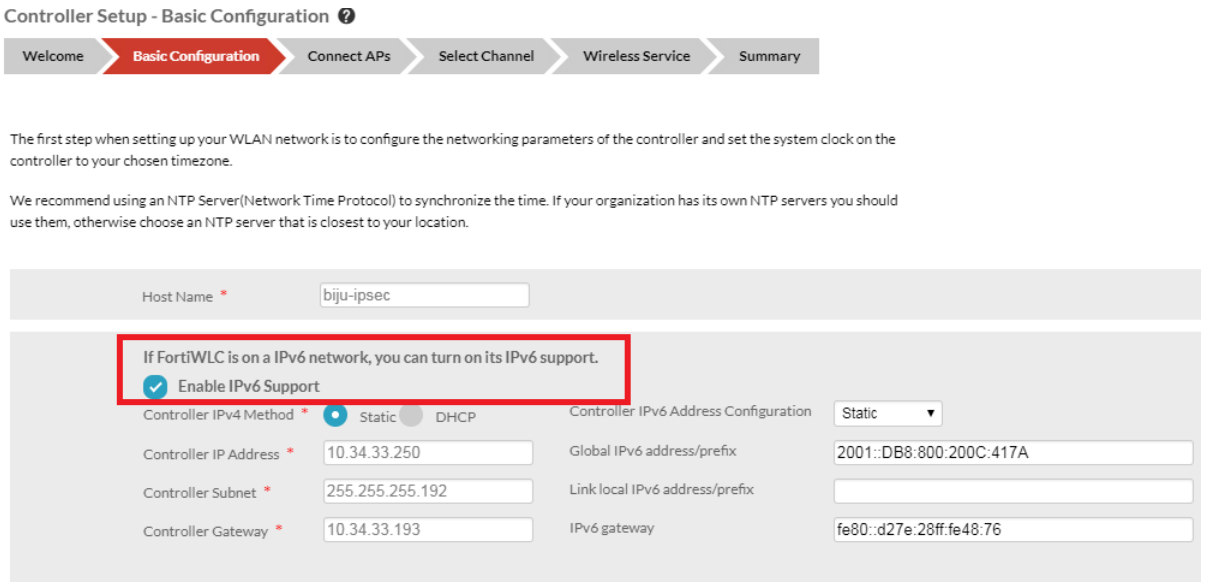
The FortiWLC supports a maximum of 8 IPv6 addresses per client. The *show controller, show station ipv6,* or *show ip6* command on the console can be used to determine the IPv6 addresses of the controller. The *show station multiple-ip* command can be used to determine the IPv6 addresses of stations. All possible combinations of controller IPv6 address configuration are achieved using the *setup* command or using the GUI - *Wizards > EzSetup*.

Fortinet recommends that the infrastructure should have RA packets with prefix information support.

GUI configurations

The following IPv6 configurations are now supported in the GUI:

- **Wizards > EzSetup** - Enable/disable IPv6 address and configure IPv6 address acquisition methods (static/DHCP/auto-config/none).



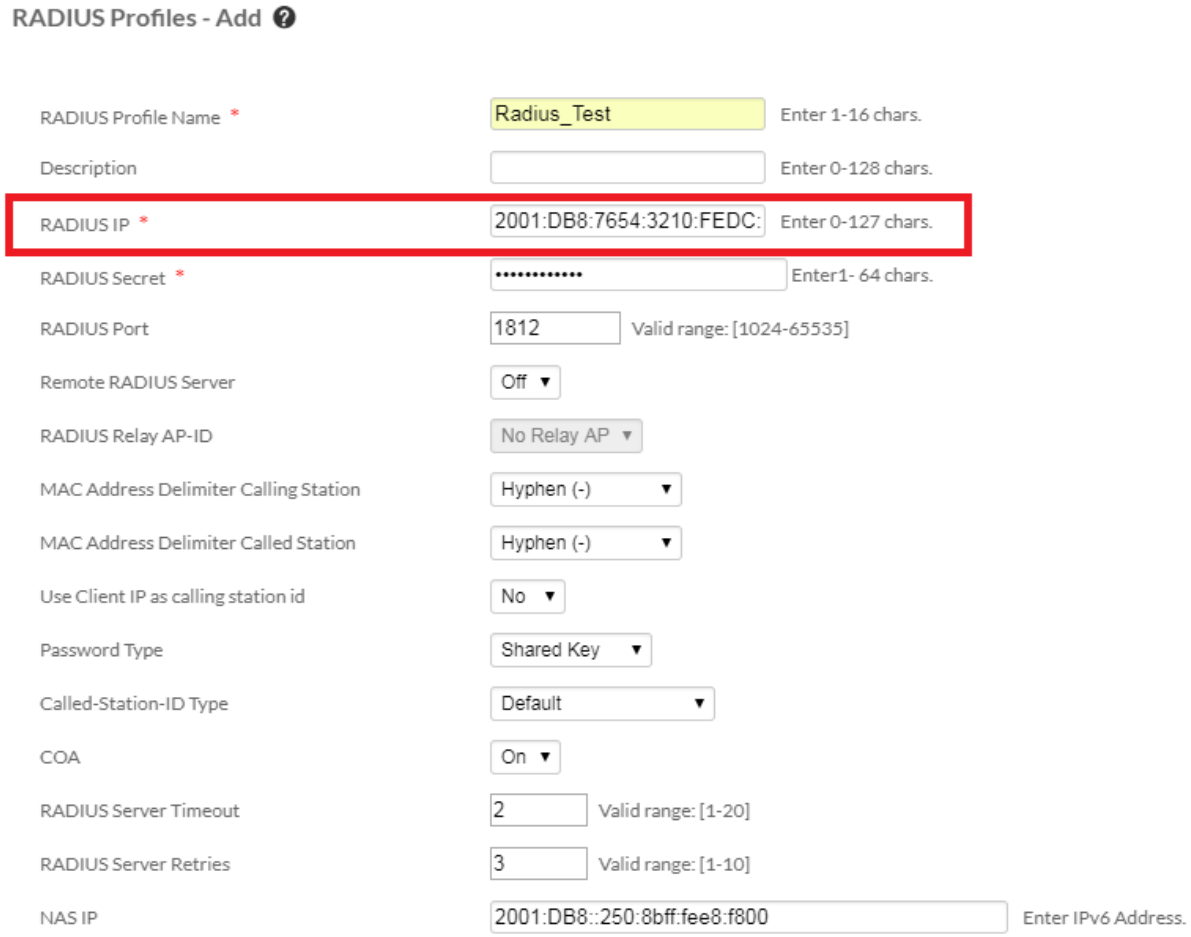
The following modes of IPv6 address acquisition methods are supported.

- **Static** You can statically configure one link local and one non link local (site local, unique local or global) scope address which persists across reboots. If you configure

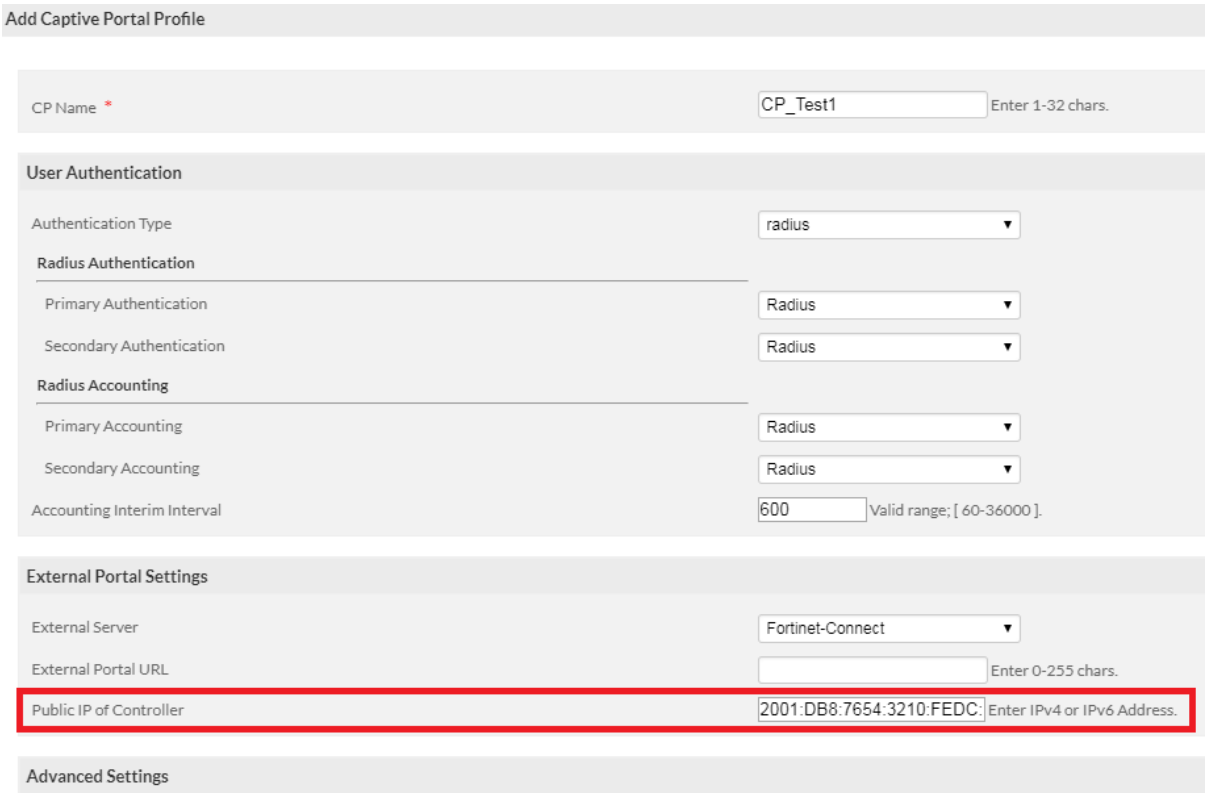
a static non-link-local address then DHCPv6 based address acquisition is disabled.

- **DHCP** – You can configure the controller to acquire an IPv6 address based on stateless or statefull DHCPv6. Stateless DHCPv6 address acquisition is based on SLAAC.
- **Auto-config** - The FortiWLC IPv6 address acquisition is based on the flags set in the router advertisement.
- **None** – FortiWLC automatically acquires an IPV6 address using. SLAAC based acquisition always works in addition to the above existing methods.

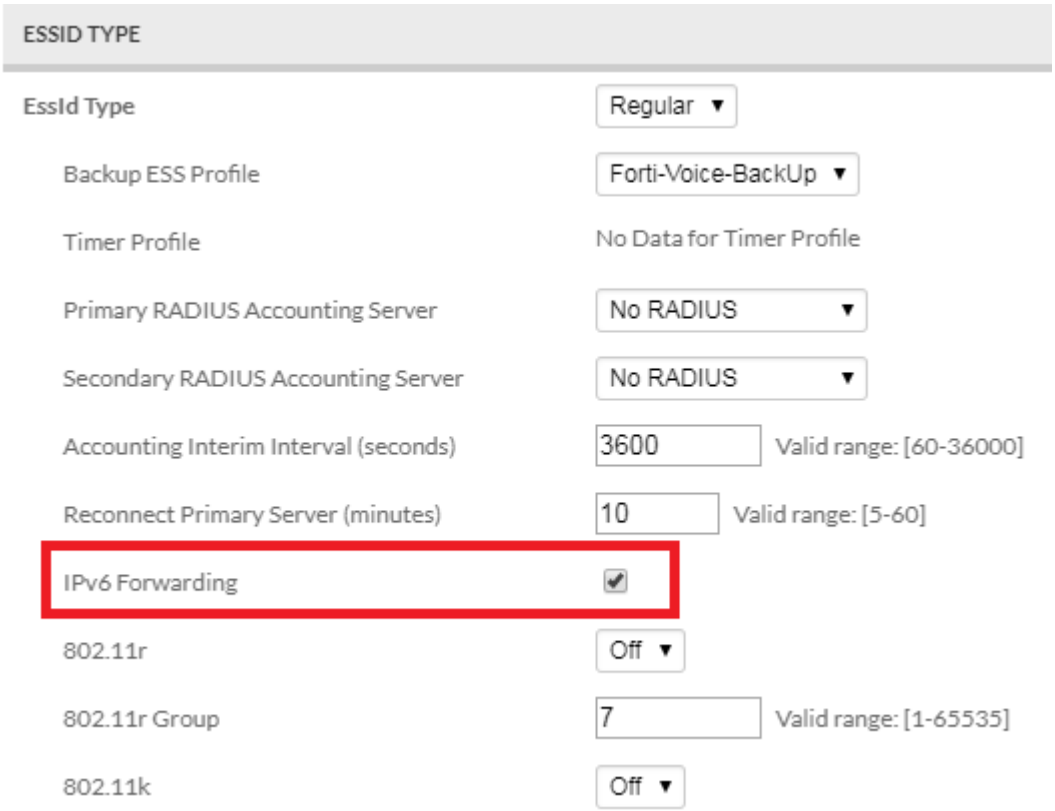
- **Configuration > Security > RADIUS** – Configuring IPv6 address of RADIUS server is supported.



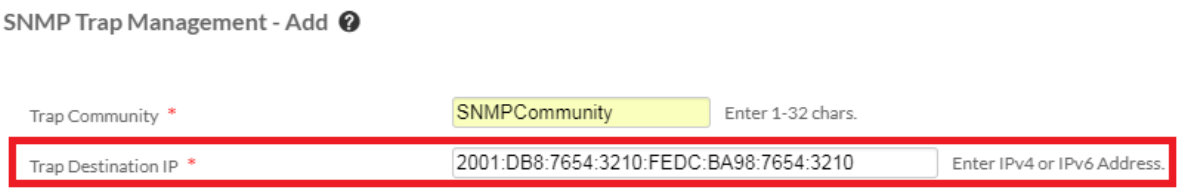
- **Configuration > Security > Captive Portal** – Configuring the external captive portal supports an IPv6 address for the controller. Also, the external captive portal URL now supports IPv6, for example, *https://[2001:470:ecfb:457:20c:29ff:fe3f:beff]/portal/2001:470:ecfb:45a::123fortiInitialRedirect*

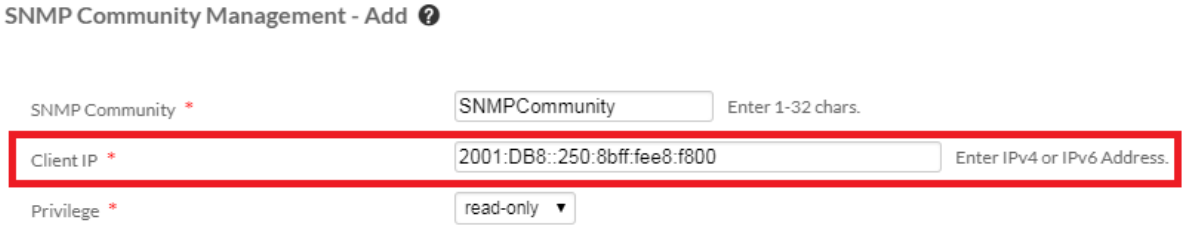


- **Configuration > Wireless > ESS** - IPv6 forwarding allows ICMPv6, DHCPv6, and other IPv6 traffic to be passed through the controller in tunnel mode. If disabled, all the IPv6 packets coming into the controller are dropped. IPv6 Forwarding is disabled by default; however, on upgrade the older (pre-upgrade) configuration is retained, whether enabled or disabled.

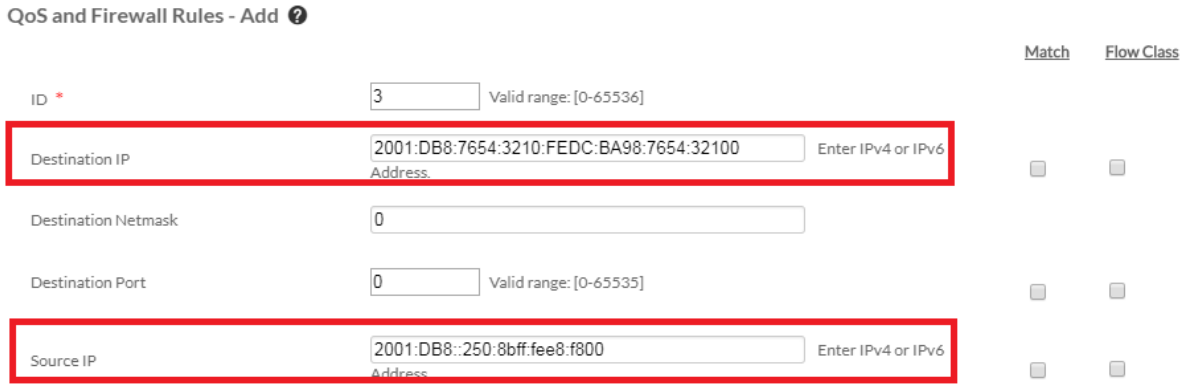


- **Configuration > Wired > VLAN** - VLAN interfaces created on the controller acquire IPv6 addresses from router advertisements only.
- **Configuration > Wired > Port** – IPv6 forwarding allows ICMPv6, DHCPv6, and other IPv6 traffic to be passed through the controller in tunnel mode. If disabled, all the IPv6 packets coming into the controller are dropped. IPv6 Forwarding is disabled by default; however, on upgrade the older (pre-upgrade) configuration is retained, whether enabled or disabled.
- **Configuration > Wired > SNMP** – Configuring IPv6 addresses for the SNMP trap server and SNMP community client IP are supported.

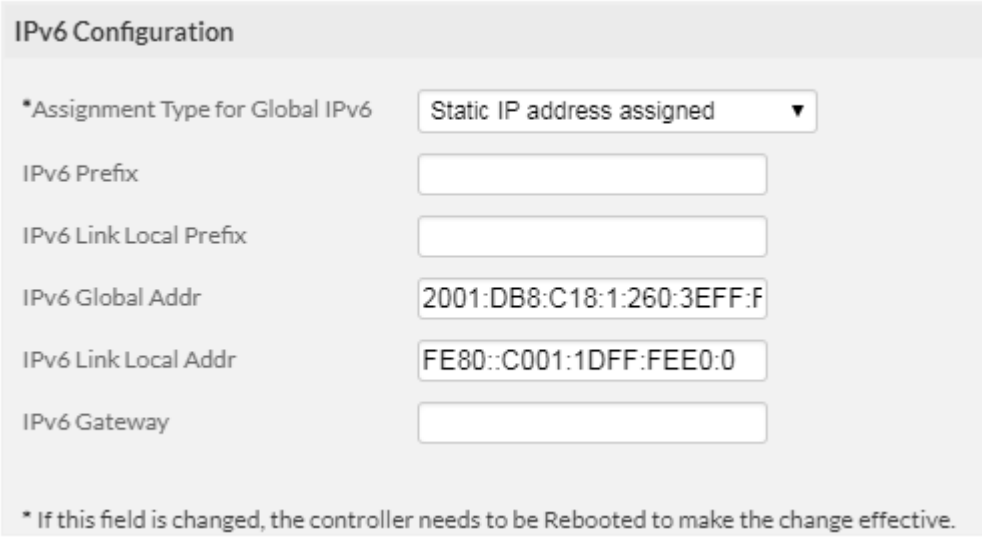




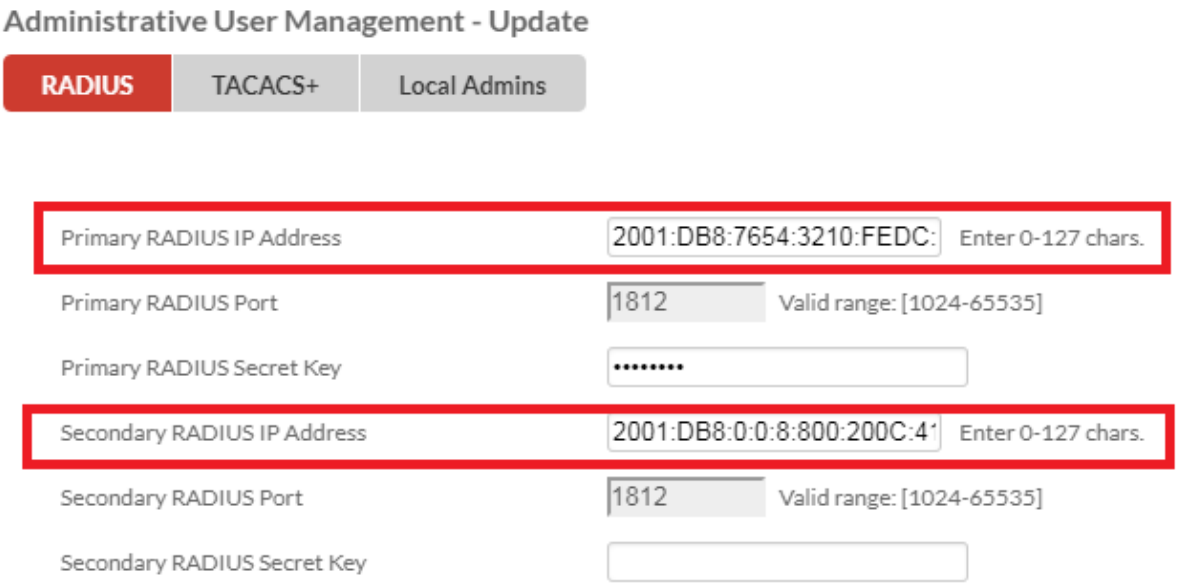
Configuration > Policies > QoS – Configuring IPv6 addresses for the destination and source of the QoS rule is supported. The source and destination netmasks can be in the dotted quad format for IPv4 or in the prefix length notation for IPv6.



- **Configuration > Devices > System settings** – The management interface IP address assignment allows configuration of static IPv6 address (global or link local scope) or DHCPv6.



- **Configuration > Access control > User management** – The RADIUS and TACACS+ servers can be configured with IPv6 addresses.



- **Maintenance > Custom CP** – Configuring IPv6 subnets for custom captive portal are supported.

The following in the GUI are updated to display the IPv6 addresses:

- **Dashboard > Voice** – The voice statistics display the IPv6 address of stations in the *Ongoing Calls* and *Registered Phones* panels.
- **Devices > Phones** – The registered phone information displays the IPv6 address of the client phones.
- **Qos/Voice > QoS Flows** – The QoS flow information displays IPv6 address of phones involved in the flows.
- **Qos/Voice > Phone calls** – The current phone call information displays IPv6 address of client phones involved in the calls.

CLI configurations

The following CLI configurations are supported.

- *show ipv6* – The command displays the IPv6 addresses on a per interface basis. Use this command to obtain IPv6 addresses assigned to the controller, default gateway, DNS servers, and domain details.

  - *show ip6*
  - *show ip6 default-gateway*
  - *show ip6 dns-server*
  - *show ip6 domain-search*
  - *show ip6 domainname*

- *Ping6 <hostname>* – The command tests the network connectivity using the specified IPv6 address. *<hostname>* is the IPv6 address of the device to ping.
- *show controller* - The command displays the IPv6 addresses and the default gateway.
- *setup* – The command now configures the IPv6 acquisition mode and details.

  - *1] Auto config (all configuration from router advertisements)*
  - *2] DHCPv6*
  - *3] Statically assigned addresses (global and/or link local scope)*

- *interface Ethernet* – The command configures the dynamic IPv6 global and link-local addresses and the IPv6 gateway for the interface.

  - *(config-if-Eth)# ipv6-global address <autoconfig | dhcp>*
  - *(config-if-Eth)# ipv6-gw*
  - *(config-if-Eth)# ipv6-link address auto*

REST APIs

REST (**RE**presentational **S**tate **T**ransfer) is a modern, scalable client-server based RPC technique using existing HTTP protocol methods (such as GET, POST, PUT, DELETE) on server resources (identified by URLs) and transferring the resources in either XML / JSON / HTML representation. The REST infrastructure of FortiWLC offers client side authentication and authorization. For more information, see the *FortiWLC REST API Reference Guide*.

Enhancements

These are the enhancements in this release of FortiWLC.

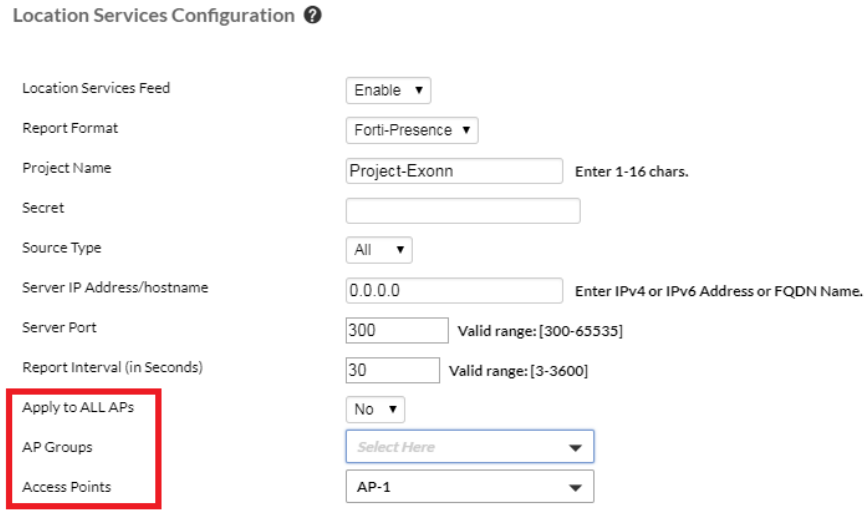
- Spectrum Manager is now supported on 64-bit FortiWLC (FortiWLC-1000D/3000D).
- The access points in the network do not reboot after any parameter is modified on the wireless interface.
- While creating a RADIUS profile (*Configuration > Security > RADIUS*), the following Called-Station-ID types are now supported:

  - AP Mac Address
  - AP Mac Address : SSID
  - AP Name
  - AP Name:SSID
  - APLocation
  - APGroup
  - APIP
  - VLAN

- While adding a RADIUS profile (*Configuration > Security > RADIUS*):
  - The calling/called station MAC address delimiter (*MAC Address Delimiter Calling Station*, *MAC Address Delimiter Called Station*) specified is now saved and used in the RADIUS request message.
  - Enable *Use Client IP as calling station id* to configure the wireless client IP address as the calling station ID. When enabled the MAC address delimiter need not be specified.
  - The RADIUS server FQDN can be specified for both IPv4 and IPv6 address.
  - [IPv6 only] The **NAS IP** address to be used in RADIUS access requests.
- Controller now responds to COA requests involving re-use of identifiers from the RADIUS server.
- HTTPS is now supported for FortiPresence social WiFi redirection by FortiWLC.
- FortiWLC on VMWare now supports VM tools that provide the following additions to VMWare setups.
  - Graceful power shutdown.
  - Clock/time synchronization between the guests and the hosts.
  - Quiescing guest file systems to allow hosts to capture file-system-consistent guest snapshots.
  - Network information and resource utilization of the guest is published to the host.
- FortiWLC GUI now prompts for a confirmation message before any delete operation.
- When the master controller (which is being monitored by slave controller) is rebooted manually, a manual re-enabling of the master is no longer required, unless the master controller is upgraded.
- The syslog is enhanced to include the hostname, company name, product name, and the build details, for example, *Master-3000D FORTINET|FORTIWLC|SD8.5-0dev-17|.*
  The station log can be viewed in the syslog.
- If the syslog host is configured on the slave controller, then the slave controller also sends syslog host messages with the slave tag keyword added on the syslog messages.

The message includes the hostname, company name, product name, and the build details, for example, Slave-3000D FORTINET|FORTIWLC|SD8.5-0dev-17|SLAVE|. These syslog messages are visible on the active slave controller as well; the active slave controller also sends syslog messages in the same format with the slave tag keyword added.

- IGMP snooping is enabled by default on controller installation and upgrade.
- The location services can now be applied to specific APs or AP groups. Navigate to *Configuration > Devices > Location Services*.



- In FortiWLC 8.5, the following DFS enhancements are delivered:
  - DFS is enabled on all FAP-U models for E/I/V/Y SKU's.
  - DFS is enabled for FAP-U22xEV Australia.
  - DFS is enabled for FAP-U422EV Japan and EU.
  - DFS is enabled for FAP-U24JEV Japan.

  The following channels are now added/enabled for all supported AP models:
  - Nepal UNII-1 5GHz channels are enabled.
  - Thailand 5GHz channels are enabled.
  - Vietnam 5Ghz channels are enabled.
  - Canada channel 132 is enabled.
  - China 5GHz channels are enabled for AP800 and 0AP800.
  - New Zealand channels 120,124,128,132 are enabled.
  - US channels 120,124,128,132 are added.
  - Argentina 5Ghz channels are added.
  - Hong Kong channel 132 is added.
  - Malaysia channels 64 to 128 are added.
  - Egypt channels 149,153,157,161,165 are added.

  Bangladesh is now a supported country.

- The Fortinet Security Fabric is an end-to-end security solution that expands network visibility by interconnecting wireless and security domains. All elements in the Security Fabric collaborate at different levels for advanced threat detection by sharing intelligence between security and network devices to detect and remediate attacks with coordinated responses. You can monitor your network for threat detection by the application and management of specific policies across the Security Fabric. The JSON REST API used is an open standard that facilitates the integration of FortiWLC into the Security Fabric and allows third party products to be a part of Fortinet's Fabric-Ready Partner Program.

  Note:
  FortiWLC 8.5.0 is ready for integration into Fortinet's Security Fabric. Fortinet will issue the required notification about the availability of the FortiOS version with support for FortiWLC integrated Security Fabric.

Additional Information

This section describes information related to the usage of FortiWLC.

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

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

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

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

- The *capture-packets* command with -R filer captures all packets instead of filtered packets.

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

- To refer to the LACP configuration procedure, see the *FortiWLC 8.5 User Guide*.

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.

Bug ID	Description
453518	Difference in the AP signal strength on the 5Ghz band while operating in the normal mode and in the site survey mode (country code set to UK).
461937	[11ac and wave-2 APs] Data packets are not tagged when client MAC cache entries in the fastpath are not present.
462207	High memory usage alarms on the access points that are configured to handle RADIUS relay.
463626	Round trip delays are observed randomly at wired side of AP822i after AP reboots.
474787	The AP model is a filterable field on the "Port-AP member table - Add" page.
404082	PSK keys for security and RADIUS configuration profiles stored in plain text and are not encrypted.
455533	Chromecast stopped working after controller firmware upgrade.
456458	Australian Daylight time saving changes not getting updated on the controller and 60 minutes offset reported.
468201	Wireless client is getting the correct URL but not the page with special character in the captive portal profile name.
470379	After removing the license check, alarm with number of days left for license displayed.
470856	Issues when an incorrect password for a WPA2PSK network is entered from IOS device.
471212	Log rotation is happening with lower size on the latest FortiWLCs.
472236	In bridge mode, when RADIUS VLAN is configured, the access point does not forward the DHCP NAK coming from the DHCP server.
480858	[Enhancement] Option to clone an existing ESS profile by selecting the profile and clicking Add.
480974	After AP reset, changing AP connectivity setting fails on the GUI.
450682	[All FAP-U] AP crashes in Vcell mode when 256 or more clients are connected to an ESSID with roaming, by clients having APID greater than 256.
442046	[FAP-U42xEV/AP832] Sometimes, the APs do not respond to port 5000, client connectivity affected.
474057	[Virtual FortiWLC] In case of a fresh FortiWLC installation, the gateway does not recognize the services in the FortiWLC GUI. In Monitor > Service Control > Service Details, the Service column is blank.
474593	AP description with sh string gets lost post upgrade.
475611	Multiple radio interfaces are created on the controller running FortiWLC 8.4.0.
476451	Sometimes in FAP-U22xEV and 24JEV, during high multicast traffic the APs reboot continuously with the page allocation failure: low memory error.
439721	[All FAP-U] High Latency and ping loss observed on clients configured in bridge mode with native and Static VLAN.
441418	[All APs] AP diagnostic information collection fails when AP uptime is more

	than 99 days.
446772	CP bypass page displayed even though the client is MAC authenticated and bypass enabled.
448391	The Search/Filter option not available for port profiles in the feature group configuration page of the FortiWLC GUI.
455780	In some MAC client devices authentication fails and the client is not able to connect. This is due to the delay in processing EAP-TLS messages.
457172	Controller based Captive Portal not working in the Bridge mode for AP822i.
461610	Unable to use special characters in generating CSR.
464544	Station could not get IPv6 DNS address from DHCPv6.
465131	AP reboots due to crash and memory issue.
468171	FortiWLC-1000D not generating alarms when secondary power supply is not plugged in.
469118	Optimized wncagent process CPU utilization to reduce CPU spikes.
470335	[AP832] AP application crashes with corrupted atsEntry messages from controller.
470641	IP address on the slave controller is missing after firmware upgrade from 8.3 on FortiWLC-1000D.
470643	Nplus1 configuration fails after firmware upgrade from 8.3 on FortiWLC-1000D.
470822	FAP-U421 reboots while unable to handle kernel null pointer - LR is at wlc_scbfindband+0x5c/0x130 [wl].
473365	Crashes due to kernel panic.
475307	[FAP-U42x] Radios' operating channel is different than the configured channel.
475315	Controller does not send APIP and APname:SSID in RADIUS access request packet. hostapd crashes.
475735	WPA2-PSK - 4-way-handshake-timeout is being classified as 802.1x authentication.
477123	EAP exchanges are getting fragmented but fragment offset is not being set.
477551	Failure to configure 802.11bgn and channel 1 to 2nd interface via GUI only.
477789	FortiWLC-3000D random reboots.
480993	[AP832] AP crashes seen during DTLS handshake phase and when a duplicate discovery response is received.
482309	AP832 missing ESS profiles when configured using feature group.
487109	The Event View page does not load.
488066	[All APs] AP CAPWAP rediscovery fails after DTLS handshake failure (due to packet loss between AP and Controller) during initial CAPWAP discovery phase.
451168	FAP-U24JEV/FAP-U22xEV- DTIM functionality was not working. PS-Poll based power-save clients failed to receive multicast traffic when

	the *Multicast-to-Unicast Conversion* option was disabled in the ESS profile.
479404	Controller not responding to COA requests involving re-use of identifiers from the RADIUS server.
496615	wncagent crashes due to special characters *(&, <, >, '"', '\r'*) in the authentication username.
453297	[AP832, FAP-Us] Aggregated EAP frame delivery fails causing delay/drop in EAP authentication.
468309	[All APs] Tunnel SSID does not work and AP reboots often in the dataplane encryption mode.
494905	Copying configuration from master to slave fails, generating syslog messages.
496601	wncagent crashes due to queries for non-existent values.
489780	[FAP-U42xEV, FAP-U22xEV] Access points reboot with junk messages in the flashlogs.
491542	[FAP-U421EV] Kernel panic LR is at wlc_scb_peek_tÈxfifo+0x188/0x244 [wl].
351281/492554	[wave-1 APs] Crash occurs when trying to encrypt deauth for un-associated station.
496057	[FAP-U22xEV/FAP-U24JEV] Site Survey tool GUI displayed the Meru logo instead of Fortinet.
492610	[All APs] 2.4 GHZ radios did not pass data traffic.
489962	[All APs] Access point reboots with seg fault crash with core file stating ATS main crash when the AP receives some junk UDP packets on port 9595.
465131	[All APs] AP reboots and crashes due to memory issues in L2 mode.
486452	FAP-U323EV does not send air wave at 5GHz; band unavailable.
489549	[FAP-U42xEV] AP operating with DFS test mode experienced CAC reset/start with fatal errors & radio re-initializing.
499495	FAP-Us were accessible though GUI even when they were connected to the controller, disabling the GUI access after successful discovery.
447510	AP changes channel with false radar detection when ARRP is enabled with freeze.
491561	Fast roaming clients fall to VLAN 0 in bridged mode.
494656	Incorrect frame reports' interval value displayed.
477862	802.1x re authentication failure.
476092	[All APs] Channel utilization reports incorrect values on the APs.
463646	Sometimes in the FAP-U units, in high multicast/broadcast traffic, performance issues and high latency are observed in the bridge mode.
464308	APs Stuck in Disabled/Online state after reboot. This issue is observed under scale deployments, for example, rebooting 100+ APs at the same time.
490758	IPv6 OAUTH is not working.
491860	Captive Portal in bridge mode does not work for clients with ONLY IPv6.
454084	AP buffering data packet caused delay in delivery.
458383	Client could not handoff AP when 1Mbps is enabled on the ESSID.
470640	[FAP-U421/423EV] Tx radio freeze on both 2.4GHz and 5GHz.
466604	*capture-packets* command did not use the -R filer when saving to a file.
469849	[All APs] New AP cannot send authentication response.

480179	MAC address delimiter has no effect on calling station ID.
482110	Not able to obtain client IP during SNMP walk using *mwStationIpaddressIpAddress*.
483711	Hotspot ESSID not added to the AP when trying to add the hotspot profile.
486750	Chromebooks devices failed to obtain the IP address from the DHCP server, even though it is offered one.
493129	wncagent crashes during bootup on 2HDVirtual causing blank configuration during boot up.
495189	When *poweroff controller* is executed, error message displayed (MASSERT: Expression !comm_mailbox_close(comm) (= 0) failed appear).
497591	1024 bit QAM support disabled in the configuration was enabled after upgrade.
497593	Class attribute missing in the RADIUS accounting request.
497604	Installing a virtual controller gave an error during boot up (*cannot create regular file /data/image1/: Not a directory;*).
498767	Controller did not tag the correct VLAN ID when the tunnel type is *radius-and-configured-vlan*.
499314	Email addresses ending in ending in .com.au and containing a '.' are classified as invalid.
499617	[All APs] Unable to generate certificate.
420129	[All APs] SIP call processing failure.
466751	Sometimes, the APs reboot in a loop when trying to add new APs or doing a bulk reboot.
486269	The client is able to browse after logout from Captive Portal authentication page, using Port Profile.
473002	[IPv6] Not able to push the configuration from FortiConnect to controller through automatic setup.
500674	Ping failure on IPv6 wireless clients when encryption mode is set to dataplane.
498128	GDL entry for Chromecast is getting removed automatically when it is connected to static VLAN AP in bridge mode.
469375	Random FAP-U42xEV crashes.
501970	[FAP-U42x/32xEV] Error Messages seen when operating in Scan Spectrum mode.
448621	Permission issues with nplus1 remote login; While trying to add master to slave inventory, slave uses *remote* user name instead of *admin.*
478058	In the monitor dashboard, devices displayed unknown for OS type list.
493457	[NPlus1] Copying of configuration files using SCP fails; retry mechanism added.
494511	[FortiWLC-1000D/3000D] Permission denied for Captive Portal users when accessing the customer images.
498771	wncagent crashes due to queries for non-existent values.
501122	After upgrade, new BSSID created for new APs in an existing AP group with the same Radio settings.
501188	Port redundancy failure; when the active port is disabled the secondary port does not take over. **Note:**

	On upgrading to 8.5, the firmware upgrade is required. Contact *Customer Support*.
501276	Controller not accessible via the management VLAN interface after Nplus1 transition.
501974	Unable to login to the FortiWLC GUI.
502255	High ping round trip duration observed.
502529	Unable to edit the ESSID profile with an apostrophe in the SSID name.
502824	Formatting issue with the *Station OS Type* on the FortiWLC dashboard. All spaces removed from the DHCP fingerprint name.
502996	[AP832] In scale deployment and CAPWAP discovery mode, when performing a bulk reboot, some APs reboot in a loop.
503295	Clients fall into incorrect VLAN and security profile after the AP goes offline/online.
503665	Modified the GUI popup when adding an ESS profile.
504093	When an AP group is added to a wireless service profile, *Error: This VLAN Name is still being used by an Internal DHCP Server* is generated. This occurred while attempting to push the ESS profile configuration from FortiWLM to FortiWLC.
504405	Station log not displayed in the FortiWLC GUI.
505254	Management-vlan not created on the active controller during Nplus1 transition. Hence, APs not connected to active controller.
505998	FortiWLC displays only local IP addresses and not the IPv4 addresses when IPv6 is enabled.
507217	FortiWLC GUI display errors when creating an AP packet capture profile. The complete list of APs to view/edit also not displayed.
509081	FortiWLC does not display the LLDP Neighbours
509566	FortiWLC GUI does not throw an error when a 64-bit patch is installed on 32-bit controller.
496331	SC AP groups scale limits reduced to 16
466751	Sometimes, the APs reboot in a loop when trying to add new APs or doing a bulk reboot.
469375	Random FAP-U42xEV crashes.
491698	Random FAP-U421EV AP reboots due to kernel crash.
487450	Sometimes Ap332 reboot due to *Unrecoverable FP Unavailable Exception*
490750	[FAP-U42xEV] Random AP silent reboots.
508595	[AP822] Random AP reboots with Kernel Panic when Aeroscout is enabled.
511160	[AP822] Random AP reboots when Aeroscout is enabled.
511970	[FAP-U42x/32xEV] Incorrect error message displayed when the AP reboots or LAN cables are unplugged/replugged.
511991/511986	[FAP-U42x/32xEV] Port Flapping in Cisco switches when bridge SSIDs are mapped to the AP.
513730	Ap832 high mem usage after upgrades.
517008	[FAP-U42x/32xEV] Unable to push ESS Profile to AP operating in DFS Channel when the Country code is set to India.
497294	Subsql-Segfault error on controller when multiple process accessed the database simultaneously, hence corrupting it and the subsql process crashed.

505762	RADIUS accounting added for multiple PSK.
507059	wncagent crashes observed in 64-bit VM when the *license* command is used to import the license file instead of the *vm-license* command; and then the *sh license* command is run.
510940	IOS devices display incorrect credentials frequently when connecting to 802.1x ssid.
511547	While copying backup configuration, the AP names not copied if the APs are online already due to AP ID mismatch.
512120	Random UDP packet drops observed.
515237	Client connectivity lost due to incorrect AP node mappings.
515678	ESS profile name starting with \t could not be deleted from the FortiWLC GUI or CLI.
516085	The Feature Group and AP group columns display undefined values in the *reboot* tab of the FortiWLC GUI.
516273	AP832 displayed wrong operating channel in .11 statistics
486450	Unable to upload a *.text* file that contains the MAC address list (ACL).
490266	[FAP-U42x/32xEV] Random AP reboots because of memory leak.
495544/494656	FAP-U22xEV - Incorrect frame report interval.
503648	[AP822] While roaming, the station cannot be assigned to another AP if it receives authentication from an AP and then moves quickly.
504956	Random nmsagent crashes.
505447	Controller ethernet statistics not reported in the CLI and GUI.
509562	WNCagent crash due to unprotected access of station map across multiple threads.
511764	[FAP-U42x/32xEV] AP reboot when LAN1-POE disconnected from a Cisco switch with LACP configured.
516562	Packet drops observed in bridged Mode with dynamic VLAN configured.
517000	[FAP-U42x/32xEV] – Low throughput observed randomly.
519764	Sometimes wncagent crashes during the failover/fallback event due to DB corruption.
519104	Random AP832 CPU softlockup reboots when trying to access memory information.
519980	Discovered Nplus1 controller state changes to *Unsupported controller version* when Nplus1 upgrade is initiated from FortiWLM.
491698	Random FAP-U421EV AP reboots due to kernel crash.
417140	Enhanced search functionality on the FortiWLC GUI.

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.

Bug ID	Description	Impact	Workaround
462324	Sometimes, RADIUS requests are sent with the same port number for different IDs.	TLS errors for the clients see at RADIUS end. No impact on connectivity.	
464541	[AP832] Wired Port profile in Mesh uplink port gets lost after upgrade to FortiWLC 8.4.0.	Wired clients cannot access the network.	Recreate the port interface for the AP.
377688	[FAP-U42x/32xEV] Low throughput with lots of *wl1: PHYTX* error message for 11ac AP clients.	Intermittent client connectivity and low throughput.	
453903	FAP-U24JEV – Client mitigation fails when the Rogue AP detection feature enabled.	Mitigation fails in cases of Rogue AP operating in foreign channel.	
474882	[FAP-U22x] Phy tx error with fatal error reinitializing and psm watchdog observed randomly on Radio 0/1 interface.	Data loss is observed when the error is reported till it recovers.	
460620	[FAP-U42x/32xEV] AP configured with static power on the following switches comes up with AF power. • HP • Cisco • Avaya	AT power unavailable.	Enable LLDP for the AP to have AT power. (Disable static power)
489539/ 490750	[FAP-U42xEV] Random AP silent reboots.	AP reboots which impacts the client connectivity for the duration of AP boot up time.	
486804	[11ac APs] Remote RADIUS not working with IPsec enabled AP.	Remote RADIUS authentication not available.	
490801	When VLAN is configured under ESSID and multiple PSK; ESSID takes precedence.	The IP address may not be obtained from the desired VLAN.	Do not configure VLANs under ESSID when using multiple PSK.
514143	[11ac APs] The IPsec tunnel between the AP and controller is re-established after	Network connectivity affected while the AP	

	Nplus1 failover/fallback. Hence the APs go for reboot/rediscovery.	reboots.	
453673	Sometimes, when static IPv6 gateway is configured, a different gateway (source of the RA) might be displayed.		The static IPv6 gateway and the source IP address of the RA should be the same.
423386	Sometimes, few CAPWAP APs are not upgraded and continue in the older version, retaining the enabled online status.	AP upgrade fails.	
364422	Roaming domain restarts if slave takes over from the master in an Nplus1 setup.	Traffic is impacted while the roaming domain restarts.	
446805	When a MAC success client roams from one ESSID to another ESSID (both broadcasting same SSID) with Captive Portal Bypass and MAC-filtering enabled, Captive Portal login page repeats itself.	An authenticated Captive Portal user is required to re-authenticate.	
447233	When trying to connect to Captive Portal bypass configured ESSID from any Apple iOS device, Unable to join message is displayed; connection is established only after a couple of successive tries. This issue occurs only with the following configuration. • The device's MAC address is not configured under *MAC Filtering ACL Deny Access Configuration*. • Under Captive Portal Bypass configured ESS profile, *ACL Environment State* is configured as Deny List Enabled. • Station MAC entry is not configured in the RADIUS.	Connection to the Captive Portal on an iOS device is delayed due to multiple retries.	
518132	Unable to install the AP patch after the controller reboots due to a controller patch installation.	Patch installation fails.	Delete the existing AP patch and copy it again. Install the AP patch.
446784	Hostapd process restarts due to memory usage reaching threshold.	Network connectivity affected temporarily.	
491110	Controller not able to establish GRE tunnel using IPv6 address.	GRE functionality not available with IPv6.	

519197	Error message is not displayed when incorrect VLAN configuration is imported into a multiple PSK profile (FortiWLC validates only for the number of fields).	Incorrect VLAN configuration is allowed to be imported into the PSK profile.	Fortinet recommends that you import valid data.
493724	Nplus1 failover not supported if the client is connected via the dataplane encryption mode.	Configured Nplus1 failover does not work.	Use the IPsec encryption mode.
484996	Captive Portal authentication fails on the Chrome version 67 browser (issue specific to Chrome).	The Captive Portal login page not available.	Install a public SSL certificate on the controller.
492040	[Multiple PSK] De-authentication request not sent to connected clients after the configured timer expires.	Traffic flow continues after the timer expires.	
523839	Random wncagent crashes are observed when the *show ap-reboot-event* command is run in a scale setup with FWC-VM-50.	No impact	
435089	False interference is detected for FHSS Cordless Phone (2.4 GHz) due to issues with the Broadcom software.	Bluetooth interference event is generated instead of FHSS Cordless Phone.	
457630	Degraded interference detection when scanning 2.4 GHz in 20MHz due to issues with the Broadcom software.		
517094	[FAP-U32x/42xEV] Sometimes, client authentication fails.	Network connectivity affected intermittently; recovers on its own.	
513730	[AP-832] High memory usage alarms generated.		
500367	After Nplus1 fall-back, the primary interface is not reachable from the same subnet host but is reachable from all other subnets. Secondary interface is reachable from all the subnets.		• From a different subnet, the primary interface is reachable. • After controller reload, both the interfaces are reachable.
524086	In rare conditions, APs do not accept client connection requests (except clear profile) after NPlus1 failover/fallback.	Client connectivity affected.	Reload the AP to recover.

526266	[AP832] AP crashes when wireless isolation (bridge mode) is enabled.	Network connectivity affected.	Edit the ESSID and disable wireless isolation.

Common Vulnerabilities and Exposures

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

Bug ID	Vulnerability
417184	CVE-2008-0960
441049	• CVE-2017-9789 • CVE-2017-9788 • CVE-2017-3167 • CVE-2017-3169 • CVE-2017-7659 • CVE-2017-7668 • CVE-2017-7679 • CVE-2016-8743 • CVE-2016-8740 • CVE-2016-2161 • CVE-2016-0736 • CVE-2016-5387 • CVE-2016-4979 • CVE-2016-1546
423105	Privilege access to CLI vulnerabilities fixed.
455997	User configured credentials are no longer displayed in log/debug using CLI trace.
501042	CGI-BIN URLs' vulnerability to command injection fixed.

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

Getting Started with Upgrade

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

NOTE:
In pre-8.4.3 releases, if the MAC-delimiter is set to hyphen in the RADIUS profile for 802.1x authentication, the controller sends the *called station id* with MAC-delimiter as colon. When you upgrade to 8.5 from pre-8.4.3 release, if there is a RADIUS reject for the MAC-delimiter, then reconfigure the RADIUS server.

Supported Upgrade Releases

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

NOTE:

- Fortinet recommends that while upgrading 32-bit controllers, use the **upgrade controller** command instead of the **upgrade system** command.
- Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI. FortiWLC-1000D and FortiWLC-3000D and 64-bit virtual controller upgrades can be performed via GUI as well.
- Upgrade the FortiWLC-1000D and 3000D controllers with manufacturing version prior to 8.3-0GAbuild-93 to version 8.3-0GAbuild-93 and then to the later builds.

Check Available Free Space

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

```
controller# show file 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

Supported Hardware and Software

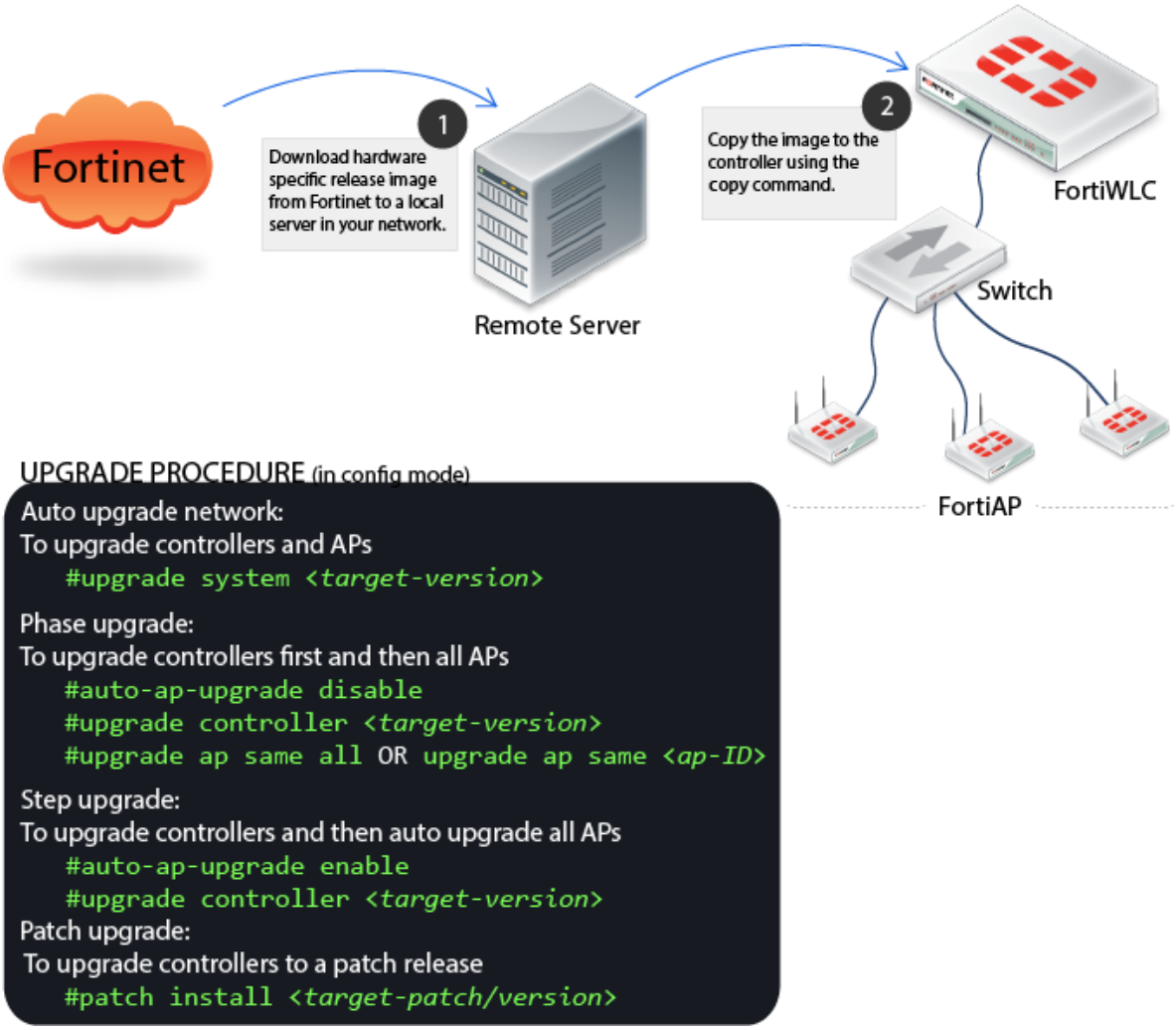
This table lists the supported hardware and software versions in this release of FortiWLC.

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e* AP332i* AP433e* AP433i* OAP433e* FAP-U421EV FAP-U423EV FAP-U321EV FAP-U323EV FAP-U422EV	FAP-U221EV FAP-U223EV FAP-U24JEV PSM3x AP1010e* AP1010i* AP1020e* AP1020i* AP1014i* AP110*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC-50D FortiWLC-200D FortiWLC-500D FortiWLC-1000D FortiWLC-3000D FWC-VM-50 FWC-VM-200 FWC-VM-500 FWC-VM-1000 FWC-VM-3000	MC3200 MC1550 MC4200 (with or without 10G Module)	MC 5000 MC 4100 MC 1500 MC 6000 MC 1500-VE MC1550-VE MC3200-VE MC4200-VE
FortiWLM	8.3.3/8.4/8.4.1		
FortiConnect	16.9.3		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+		
NOTE: A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			

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

Installing and Upgrading

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



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

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

   [OR]

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

   Where

   - *image-name* for FortiWLC: forti-{release-version}-{hardware-model}-rpm.tar.fwlc
     Eg, *forti-8.4-1-FWC2HD-rpm.tar.fwlc*

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

```
# auto-ap-upgrade disable
# copy running-config startup-config
# upgrade controller <target version> (Example, upgrade controller 8.3)
```

   The *show flash* command displays the version details.

3. Upgrade the APs

```
# upgrade ap same all
```

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

Upgrading FortiWLC-1000D and FortiWLC-3000D

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

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: 8.5-0build-0
         Apps size: 251M/850M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.3.14
         System memory: 240M/473M
         Apps version: 8.4-0build-7
         Apps size: 177M/849M
```

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

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

reboot
```

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

NOTE:

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

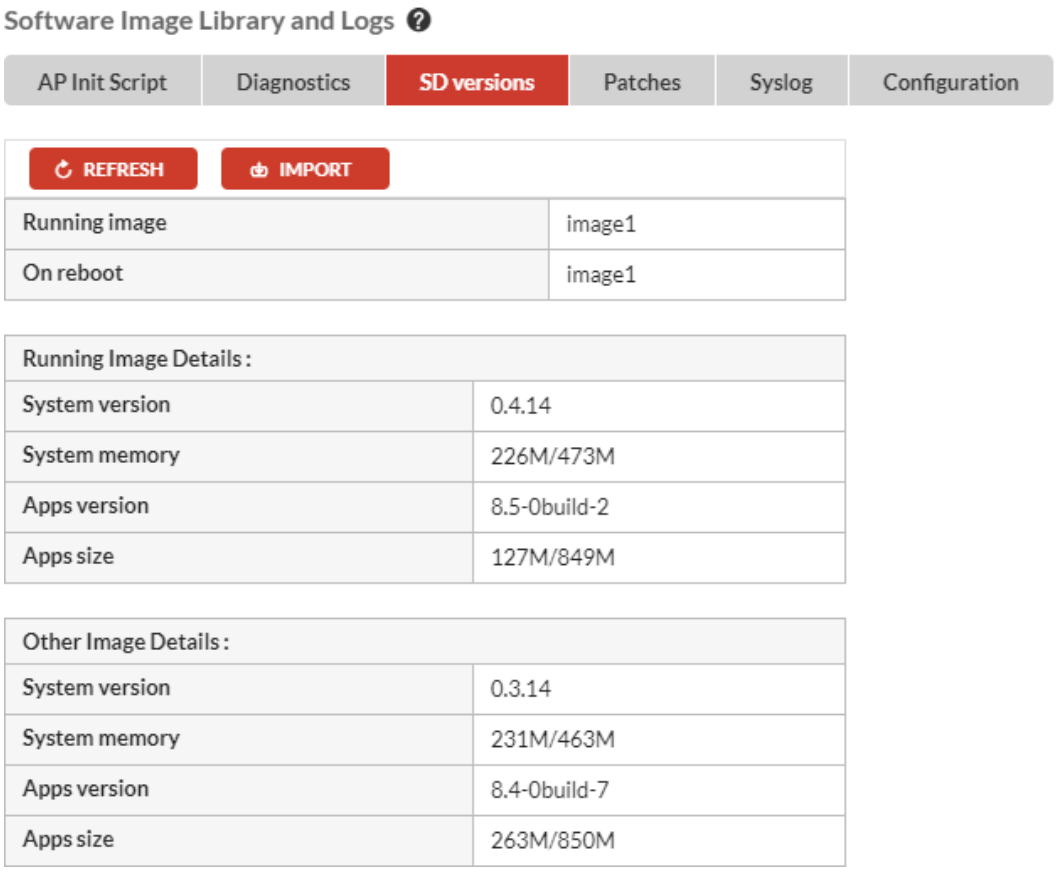
Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

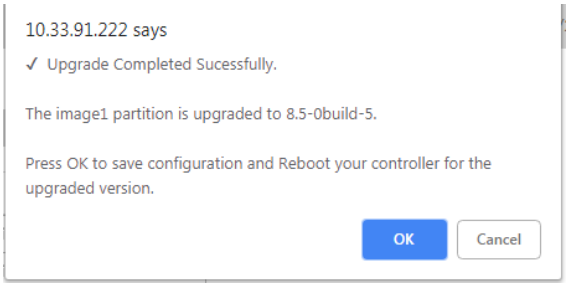
NOTE:

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

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



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



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

Switching Partitions

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

Upgrading a N+1 Site

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

You can choose any of the following options to upgrade:

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

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

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

     The output should display the following information:

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

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

Restore Saved Configuration

After upgrading, restore the saved configuration.

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

Upgrading Virtual Controllers

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

Upgrading the controller can be done in the following ways:

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

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

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

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

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

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

Upgrade Advisories

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

NOTES:

- [32-bit controllers] Prior to upgrading to FortiWLC 8.5, delete any old image files to avoid issues related to space constraints.
- Upgrade Controller using wired client/laptop and **NOT** using wireless client/laptop. -
- Fortinet recommends upgrading a batch of maximum 100 APs.

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 to 8.5.0.

Mesh Deployments

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

Feature Groups in Mesh profile

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

Voice Scale Recommendations

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

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

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

END USER LICENSE AGREEMENT

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

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service