FortiWLC - Release Notes

Version 8.5.2

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

May 18, 2020
FortiWLC 8.5.2 Release Notes

TABLE OF CONTENTS

Change log

Date	Change description
2020-05-18	FortiWLC version 8.5.2 document release.
2020-07-06	Updated the *Upgrade Advisories* for Mesh/VPN AP deployments and revised the supported FortiWLM version.

About FortiWLC 8.5.2

FortiWLC release 8.5.2 introduces new features and enhancements along with important bug fixes. To view details on what is delivered in this release, see section What's New on page 7 and to view the list of bug fixes, see section Fixed Issues on page 31.

What's New

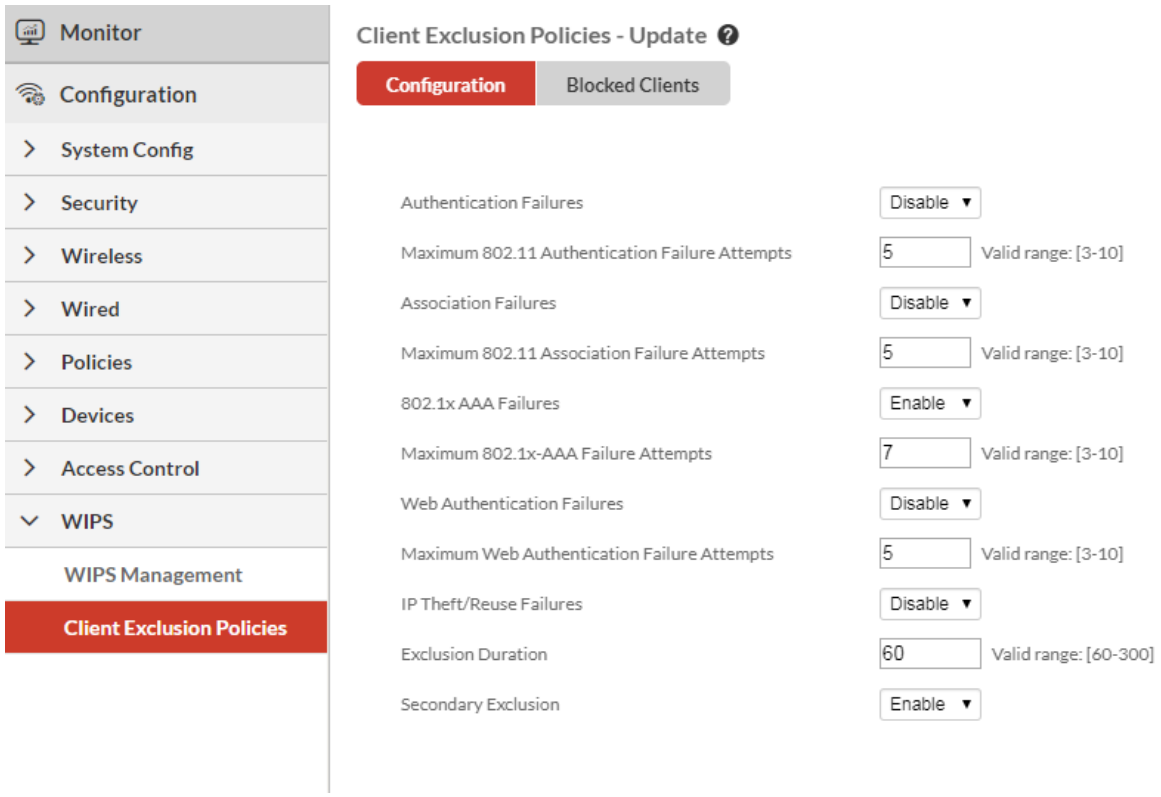
This section describes the new features introduced in this release of FortiWLC.

Client Exclusion Policies

WIPS monitors clients based on specific parameters configured in the client exclusion policy; clients detected with a suspicious pattern based on the configured parameters in the policy are deemed malicious and blocked.

Note: Fortinet recommends enabling **Force DHCP** in the ESS profile for optimum performance.

Navigate to **Configuration > WIPS > Client Exclusion Policies** on the FortiWLC GUI.



Support for 802.11v

FortiWLC now supports the 802.11v standards for wireless networks, which provide several enhancements for network management such as network assisted roaming and power saving.

Network assisted roaming allows the wireless network to send requests to associated clients, recommending better APs to associate with while roaming. This is beneficial for both load balancing and in guiding clients with poor connectivity.

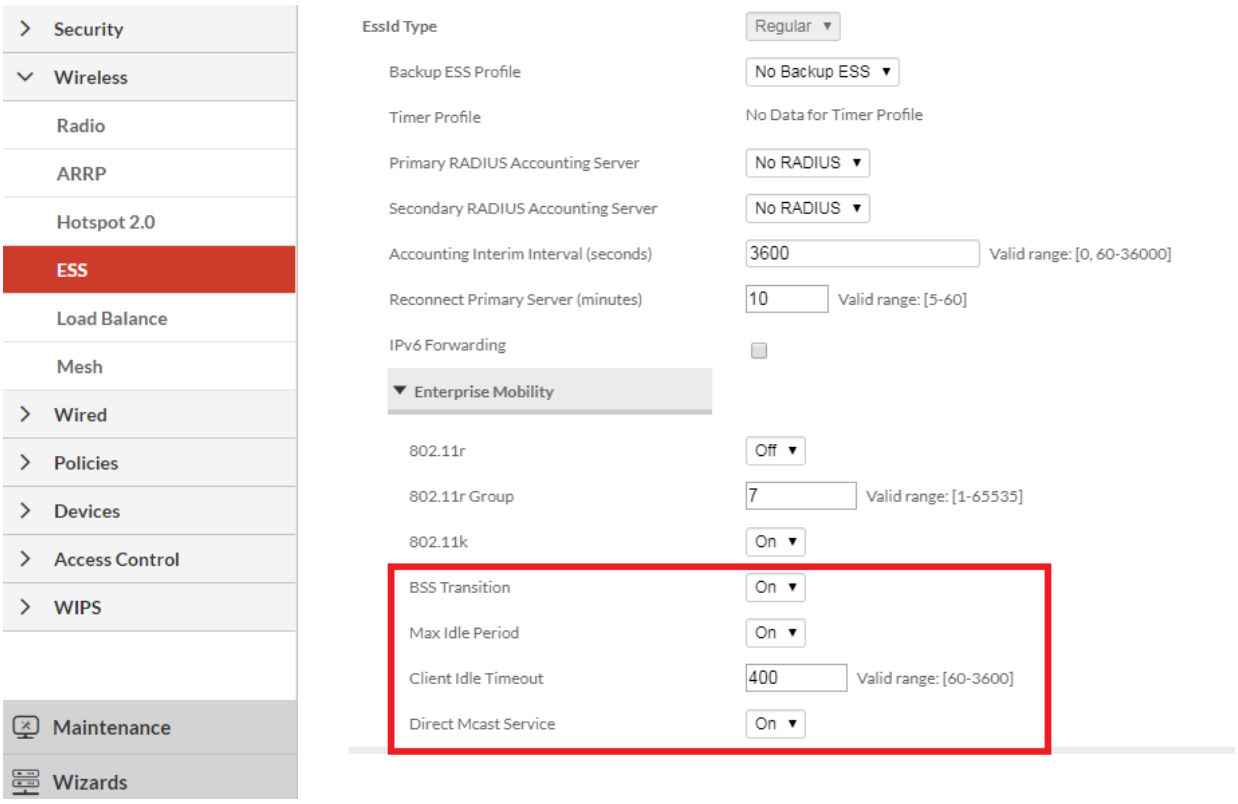
Network assisted power saving allows configuring an idle period for devices, ensuring that they remain connected to APs without receiving any frames from them. This helps in reduced power consumption and improved battery life.

You can configure the following fields defined by the 802.11v standard.

- BSS Transition
- Max Idle Period
- Client Idle Timeout
- Direct Mcast Service

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

Note: 802.11k and ARRP must be enabled to use 802.11v capabilities.

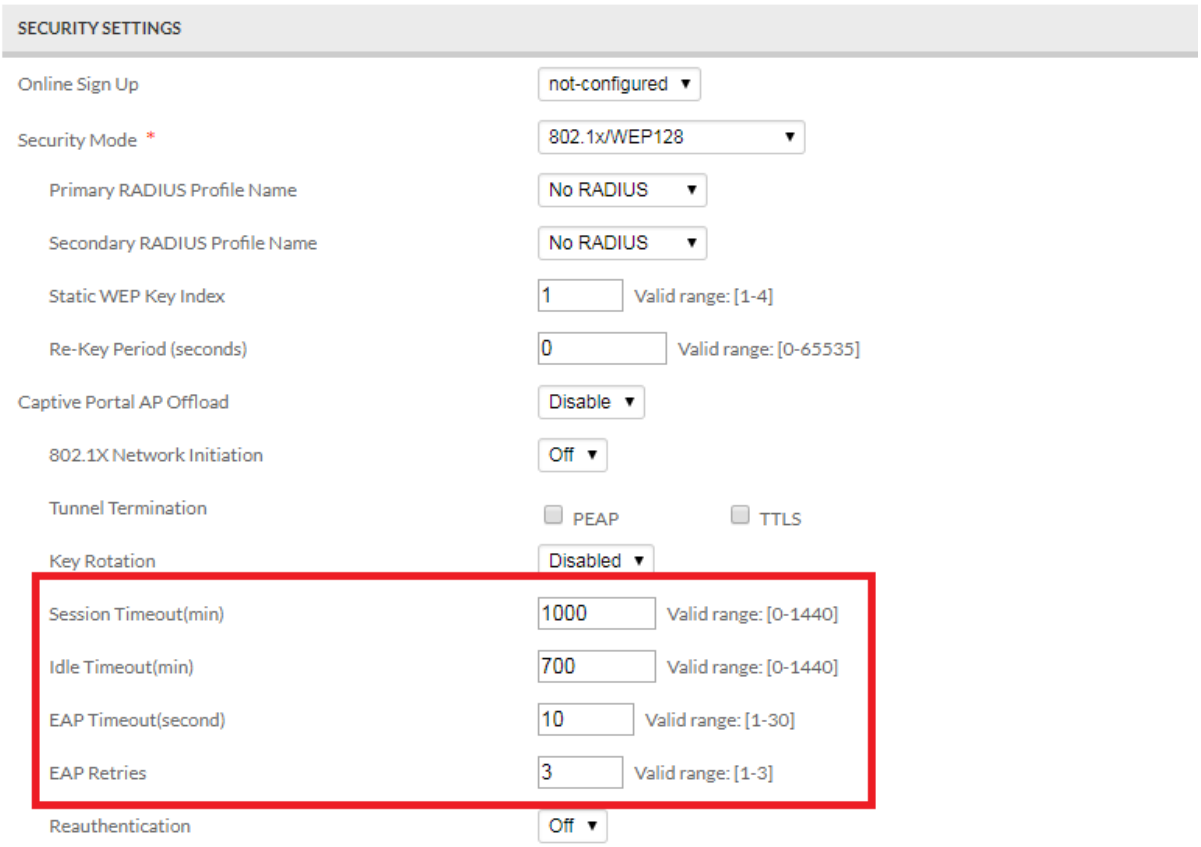


Security Profile - Session/Idle Timeout & EAP Timeout/Retries

You can configure the following fields between the access point and wireless clients only for RADIUS/Enterprise security modes.

- You can configure the 802.1x **Session Timeout** and **Idle Timeout**. After the timeout, client requests for re-authentication.
- You can configure the **EAP Timeout** and **EAP Retries**. After the timeout, authentication fails and the client tries to reconnect as per the configured EAP retries.

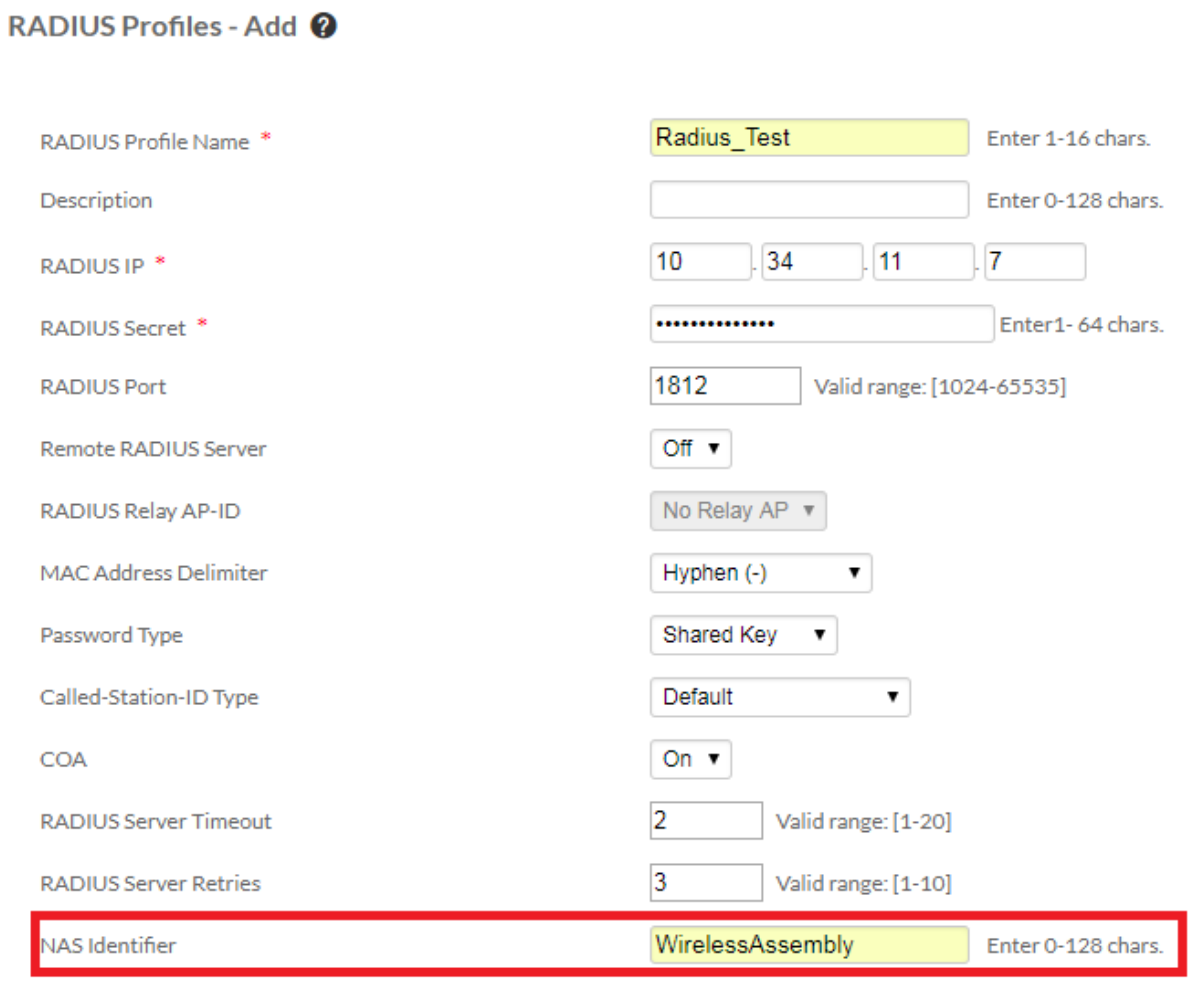
Navigate to **Configuration > Security > Profile**.



RADIUS Profile – NAS Identifier

While creating a RADIUS security profile you can configure the Network Access Server Identifier (**NAS Identifier**) to report the source of the RADIUS access request. This allows the RADIUS server to select a policy for that request. You can configure the NAS identifier for each RADIUS profile.

Navigate to **Configuration > Security > RADIUS**.

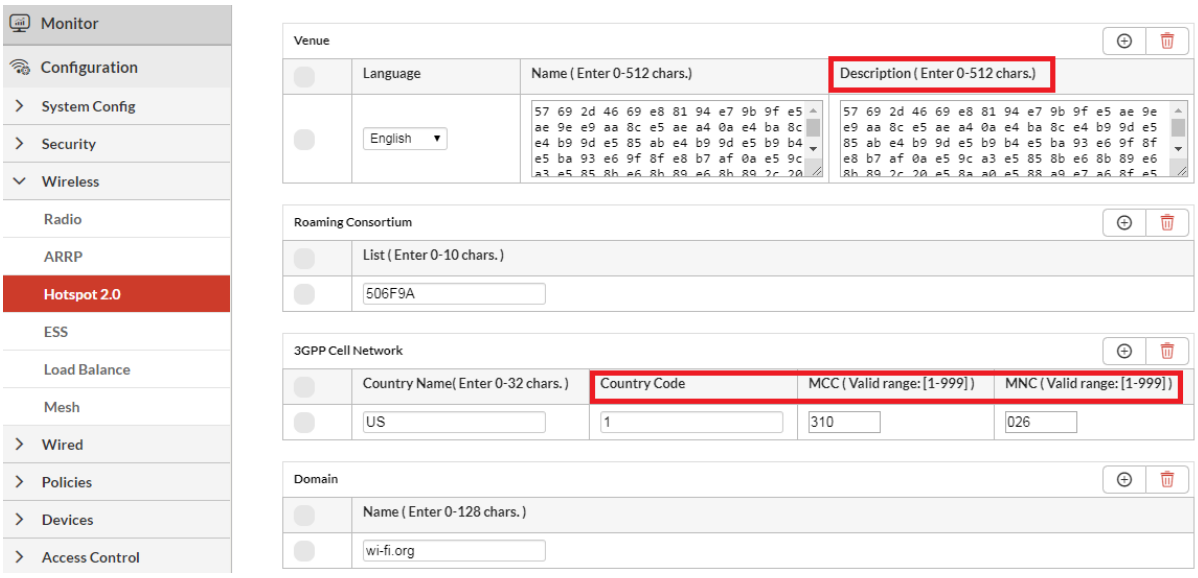


Hotspot 2.0 Profile - Additional Attributes

In a Hotspot 2.0 profile, you can add a description for the configured venue and also specify the country code for your 3GPP cell network. The following additional configuration options are added.

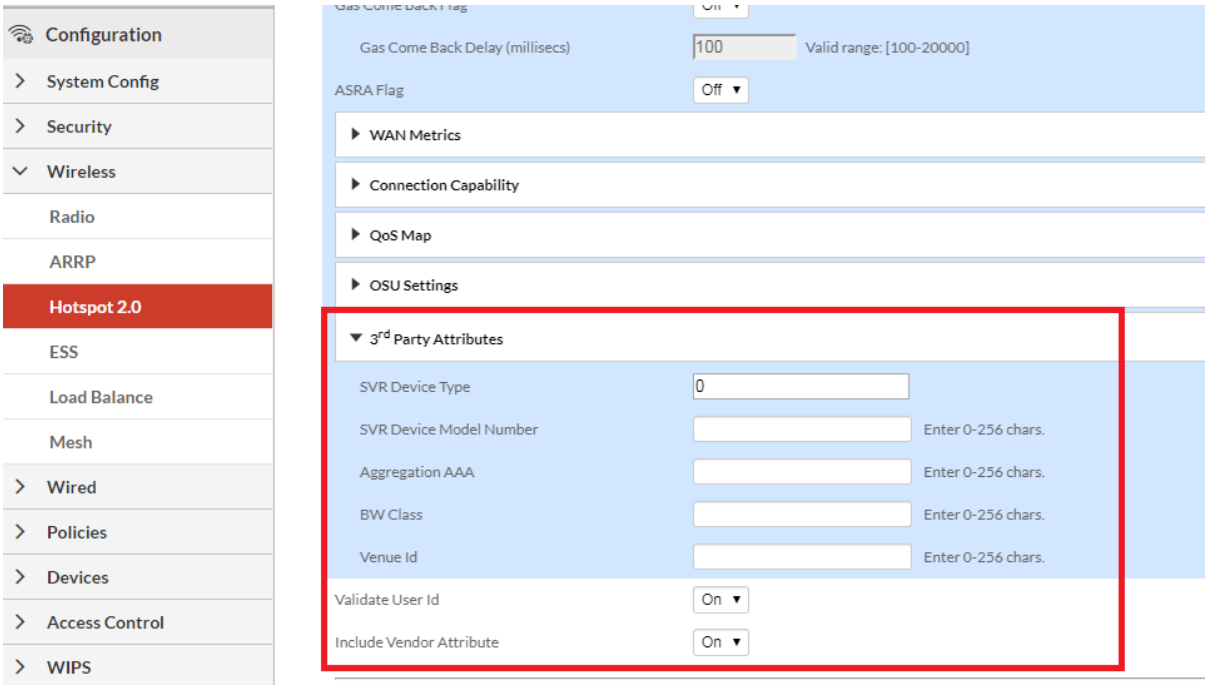
- Venue Description
- 3GPP Cell Network Country Code

Navigate to **Configure > Templates > Hotspot 2.0**.



The following fields are also added for Hotspot 2.0.

- 3rd party attributes (Advanced Settings)
- Validate User Id
- Include Vendor Attributes



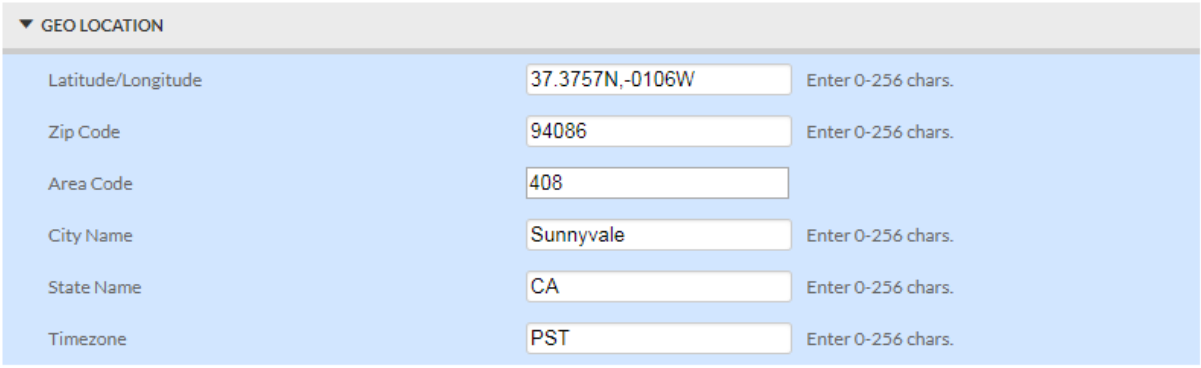
Access Point - Geo Location

While adding an access point you can specify details/specifics of its geographical location.

The following location based attributes can be configured.

- Latitude/Longitude - Coordinates separated by commas.
- Zip Code
- Area Code
- City Name
- State Name
- Timezone

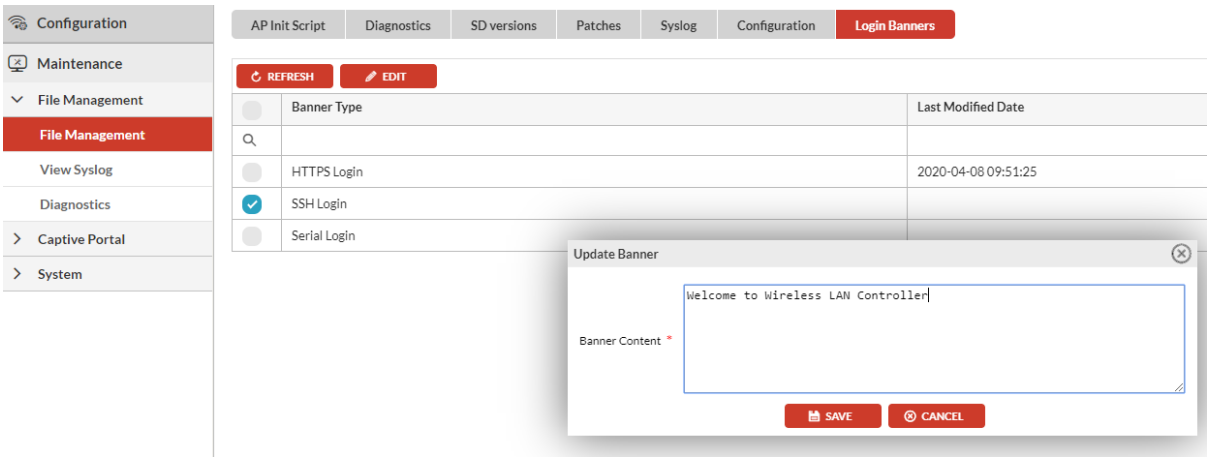
Navigate to **Configuration > Devices > AP – Geo Location**.



Login Banners

The login banner defines the text that is displayed when you login into the controller. The login banner applies only to the controller on which you configure it. You can define the banner for HTTPS login, SSH Login, and serial console.

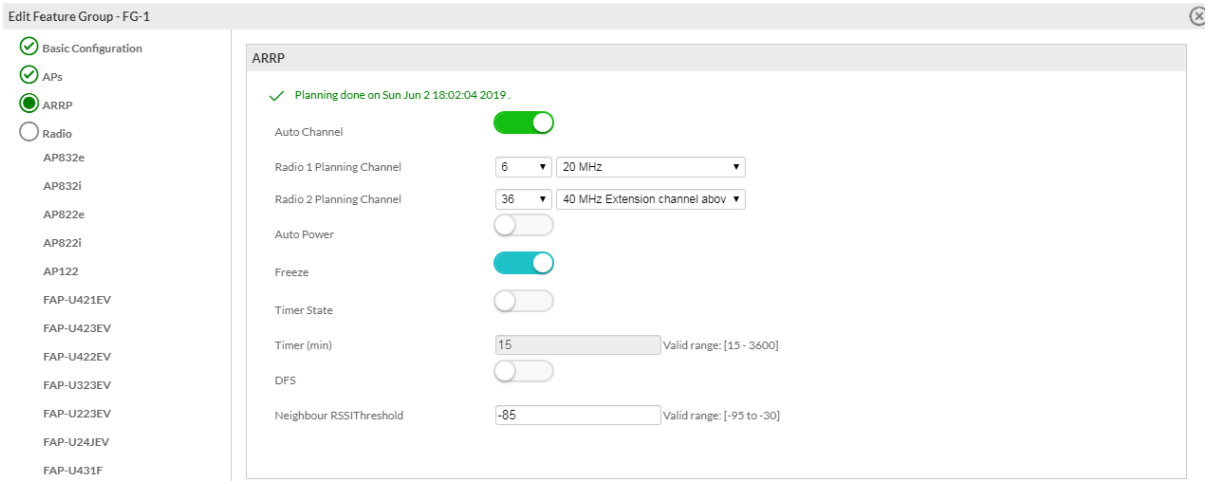
Navigate to **Maintenance > File Management**.



ARRP Planning Status

You can now view the ARRP planning status on the Feature Group page. The date and time of the planning are displayed along with the list of overlapping APs (APs sharing channels with their neighbours).

Navigate to **Configuration > System Config > Feature Group > ARRP**.



FAP-U43xF – Additional Features

The following features are now supported on the FAP-U43xF APs.

- AP Survivability
- Hotspot 2.0
- IPv6 support
- Multiple PSK in Bridge mode
- Mesh
- Spectralink
- IPSec

ESS Profile Enhancements

The following enhancements are supported for ESS profile configuration.

- **Sticky Client De-authentication**
  The **Probe Response Threshold** parameter configures the probe response, gratuitous authentication, and de-authentication thresholds. The de-authentication threshold disconnects the far away client and is useful in staying clear of sticky clients, that is, (far away) clients who stick to a bad connection.
- **AP Defaults**
  Native cell is now the default RF virtualization mode for all AP models and A band is the default for band steering configuration in an ESS profile.
- When configuring an ESS profile, you can disable the **Accounting Interim Interval** by configuring a value of 0.
- The **Isolate Wireless To Wireless traffic** option is supported in the tunnel mode and bridge mode (in the AP) for wireless to wireless traffic.

DFS Enhancements

The following DFS enhancements are delivered in this release.

- [FAP-U32xEV] Enabled DFS channel 14 (2.4GHz and 802.11b only) for Japan.
- [FAP-U43xF] Enabled DFS for A/S/N SKU regions.
- Korea DFS channels can be configured support 160 MHz (5 GHz band only)

Reduced RAM Requirement (FWC-VM-500)

This release allows a lower RAM of 12 GB for FWC-VM-500 Hyper-V and VMWare ESXi deployments.

Others

The following modifications are delivered in this release.

- When the AP discovers a controller in the L3 mode, the APs will use the L3 preferred mode for further discovery attempts.
- The channel width selection is automatic based on the channel. For example, for channel 40, 40 MHz Extension channel and below is selected automatically.
- The syntax of the capture-packets command now supports **AND** and **OR** keywords. The **&&** or **//** symbols are NOT supported.

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 FAP-U431F FAP-U433F 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	8.5.1		
FortiConnect	16.9.3		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 11 Mozilla Firefox 69 Google Chrome 77		
Note: A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			

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.
- Multicast to unicast conversion must be enabled on all the ESS profiles.

- 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-U43xF

Apply this upgrade procedure to laptops (with Intel Wi-Fi drivers installed) for connectivity to FAP-U43xF access points, where, the ESSID is not displayed in the Wi-Fi list; the ESSIDs are not detected by default on laptops with Intel Wi-Fi drivers installed.

Follow these steps to upgrade Intel client drivers.

1. Browse to https://downloadcenter.intel.com/ and select **Wireless Networking**.
2. Click on **View by produc**t and select **Intel Wireless Products**; the browser page reloads.
3. Click on **View by product** again and select the applicable **Intel Wireless Series**. (For example, Intel Wireless 9000/8000/7200 Series); the browser page reloads.
   Note: The number your chipset starts with is your wireless series, for example, chipset starting with 8260 indicates Intel Wireless 8100 Series.
4. Select your chipset version.
5. Select the drivers based on the installed OS and download them.
6. Install the downloaded drivers; on the prompt, select **Upgrade**.
7. Restart the laptop after the drivers are successfully installed.

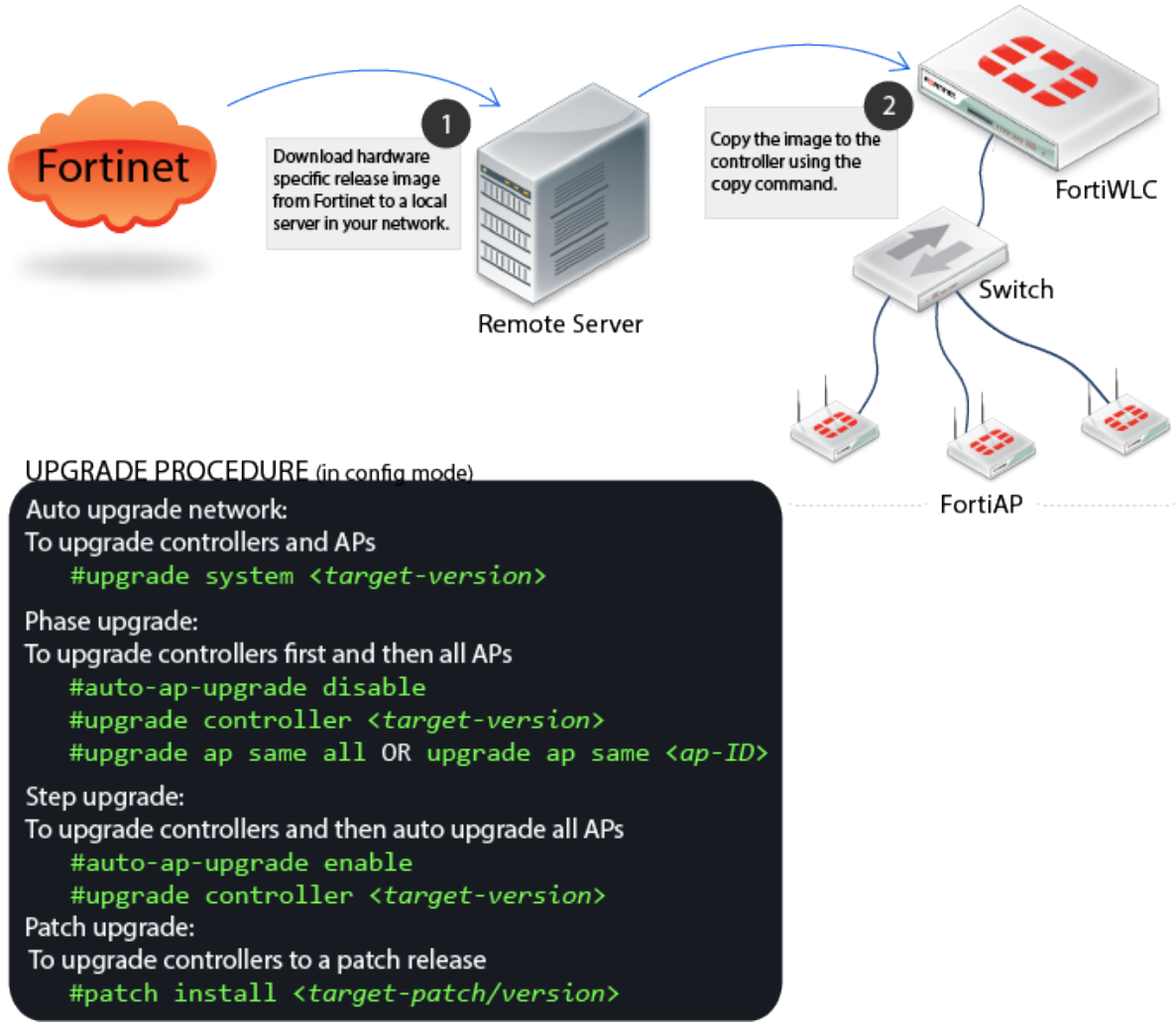
You are now able to see the ESSID.

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

For more information on deploying FAP-U43xF, see the *FAP-U43xF Deployment Guide*.

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-3000 on page 26 to upgrade FortiWLC-1000D and FortiWLC-3000D. See Upgrading Virtual Controllers on page 29 to upgrade virtual controllers.



1. Download image files from the remote server to the controller using one of the following commands:
   # copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar.fwlc><space>.
   [OR]
   copy tftp://<ext-ip-addr>/<image-name-rpm.tar.fwlc><space>
   Where, **image-name** for FortiWLC: forti-{release-version}-{hardware-model}-rpm.tar.fwlc For example, *forti-8.5-2-FWC2HD-rpm.tar.fwlc*
2. Disable AP auto upgrade and then upgrade the controller (in config mode)
   # auto-ap-upgrade disable
   copy running-config startup-config

upgrade controller <target version> (Example, upgrade controller 8.3)

The **show flash** command displays the version details.

3. Upgrade the APs
   # upgrade ap same all

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

Getting Started with Upgrade

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

NOTE:

In pre-8.4.3 releases, if the MAC-delimiter is set to hyphen in the RADIUS profile for 802.1x authentication, the controller sends the **called station id** with MAC-delimiter as colon.

When you upgrade to 8.5.2 from pre-8.4.3 release, if there is a RADIUS reject for the MAC-delimiter, then reconfigure the RADIUS server.

Supported Upgrade Releases

This section describes the upgrade path for this release.

From FortiWLC release...	To FortiWLC Release...
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

From FortiWLC release...	To FortiWLC Release...
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4	8.5.0
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.5.0	8.5.1
8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.5.0, 8.5.1	8.5.2

NOTES:

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

Check Available Free Space

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

```
controller# show file systems
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/hdc2 428972 227844 178242 57% /none 4880 56 4824 2% /dev/shm
```

The first partition in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **delete flash:<flash>** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Set the serial connection for the following options:

NOTE:

Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits

- Parity--None
- Stop Bit—1
- Flow Control—None

Upgrade Advisories

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

NOTES:

- [32-bit controllers] Prior to upgrading to FortiWLC, delete any old image files to avoid issues related to space constraints.
- Upgrade Controller using wired client/laptop and **NOT** using wireless client/laptop.
- [Patch installation] When both AP and controller patches are to be applied; the controller patch must be installed prior to the AP patch.

Upgrading Virtual Controllers

In the upgrade-image command, select the options **Apps** or **Both** based on these requirements:

• Apps: This option will only upgrade the Fortinet binaries (rpm).

• Both: This option will upgrade Fortinet binaries as well as kernel (iso).

Upgrading FAP-U422EV

If the controller is running on pre-8.4.0 version and FAP-U422EV is deployed, follow these points:

- Disable **auto -ap -upgrade**
  OR
- It is advised not to plug in FAP-U422EV till the controller gets upgraded.

Mesh/VPN AP Deployments

[32-bit controllers] When attempting to upgrade a VPN/mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller. Run the **upgrade system** command.

Feature Groups in Mesh profile

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

Voice Scale Recommendations

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

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

NOTE:

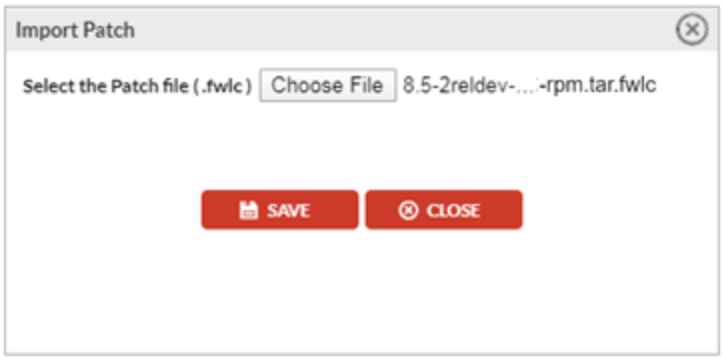
Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic.

Upgrading for FAP-U43xF Support

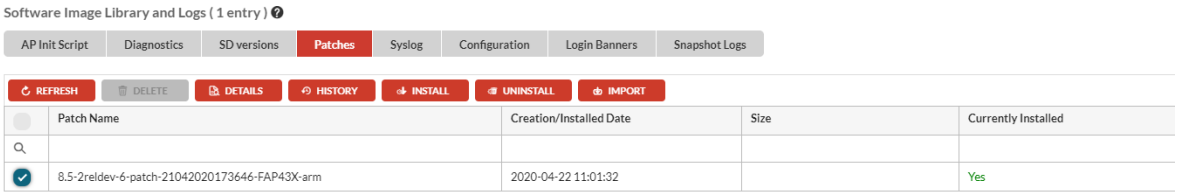
You are required to download the FAP-U43xF image file as it is NOT bundled in the controller image. Follow this procedure to download and install the FAP-U43xF image.

Note: Direct upgrade to 8.5.2 can be done from releases 8.4.0 and above.

1. Download the FAP-U43xF image file from the remote server to the controller.
   For example,
   [FortiWLC controllers]
   copy scp://download:download@<remote_server_IP>/<image_file_location>/forti-8.5-2build-04-patch-24102019120556-FAP43X-arm-generic-rpm.tar.fwlc
   [MC controllers]
   copy scp://download:download@<remote_server_IP>/<image_file_location>/meru-8.5-2build-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-U43xF image file is installed in the controller, run the **upgrade ap same all** command to upgrade the APs.

Upgrading FortiWLC-1000D and FortiWLC-3000

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.

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 this release (using *rpm.tar.fwlc* file format).

Note that the *.fwlc* file format is supported from release 8.4.0.

Upgrading via CLI

1. Use the show images command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
Master-3000D(15)# show images
Running image : image0
On reboot : image0
--------------------------------------------------------------------------
-------
Running image details.
System version: 0.3.14
System memory: 231M/463M
Apps version: 8.5-2build-4
Apps size: 251M/850M
--------------------------------------------------------------------------
-------
Other image details.
System version: 0.3.14
System memory: 240M/473M
Apps version: 8.5-1build-7
Apps size: 177M/849M
```

2. To install the latest release, download the release image using the **upgrade-image** command.
   upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image- name>-rpm.tar.fwlc both

   reboot

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

NOTE:

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

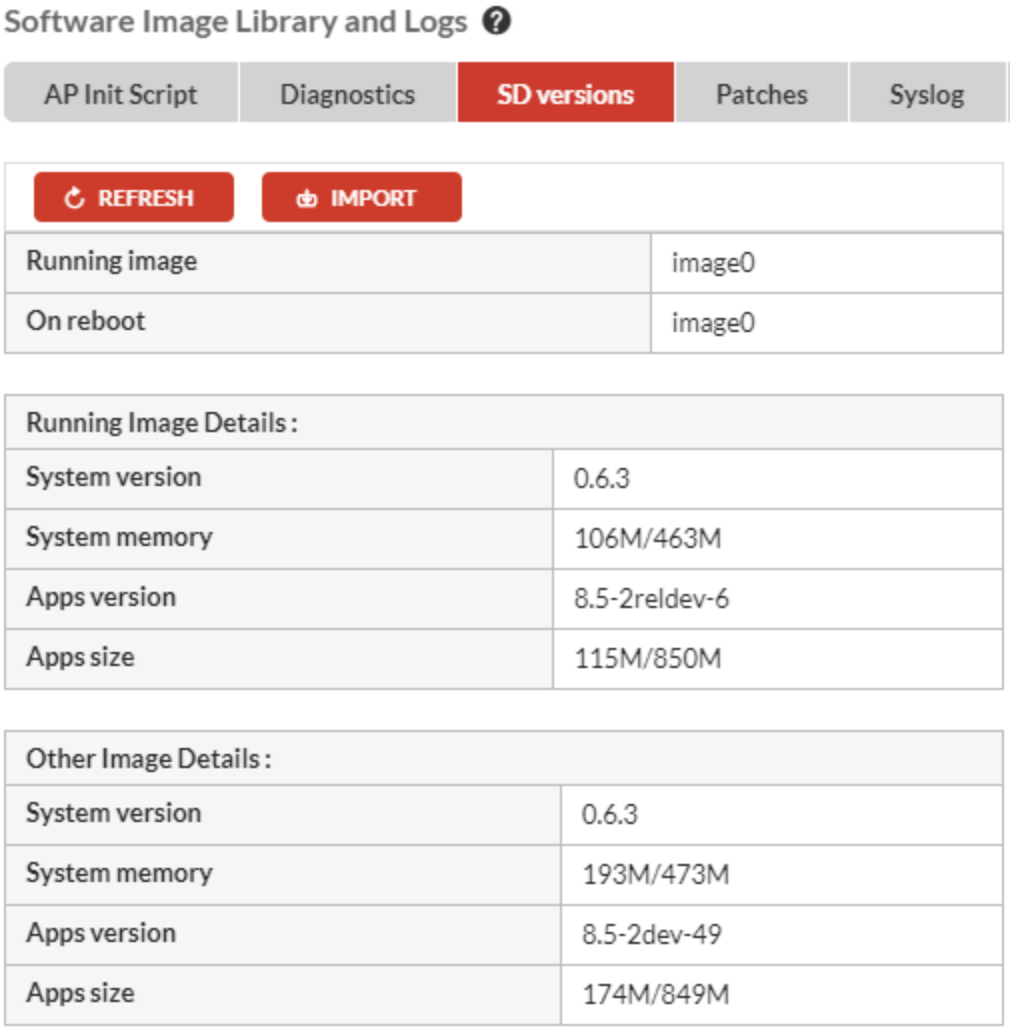
Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

NOTES:

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

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



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

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

Switching Partitions

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

Upgrading an NPlus1 Site

To upgrade a site running NPlus1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers.

You can choose any of the following options to upgrade:

Option 1 - Just like you would upgrade any controller, you can upgrade an NPlus1 controller.

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

Option 2 - Upgrade slave and then upgrade master controller.

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

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After the upgrade, run the **nplus1 enable** command to enable all master controllers on slave controllers .
2. Run the the **nplus1 enable** command to enable master controller on slave controller.
3. Connect to all controllers using SSH or a serial cable.
4. Runthe **show nplus1** command to verify if the slave and master controllers are in the cluster.
   The output should display the following information:
   ```
   Admin: Enable
   Switch: Yes
   Reason: -
   SW Version: 8.3-1
   ```
5. If the configuration does not display the above settings, run the **nplus1 enable <master -controller -ip>** command to complete the configuration.
6. Run the **nplus1 add master** command to add any missing master controller to the cluster.

Restore Saved Configuration

After upgrading, restore the saved configuration.

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

Upgrading Virtual Controllers

Virtual controllers can be upgraded the same way as the hardware controllers. See sections Upgrading via CLI on page 27, Upgrading via GUI on page 27, and Upgrading an NPlus1 Site on page 29.

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.

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
544679	[AP832] Random AP reboots.
550756	[FAP-U24JEV] Random AP reboots.
562619	[FAP-U32xEV] Random AP crashes.
564580	[AP822/FAP-U42xEV] Random AP reboots.
589022/590627	[FAP-U22xEV/24JEV] Silent AP reboots.
583095	[AP832] Random AP reboots.
594583	[AP822i] Random AP reboots.
598927	[FAP-U42xEV/32xEV, AP832] Random AP reboots.
599919	[AP822v2/AP832] Silent AP reboots.
600563	[FAP-U24JEV] AP unable to pass data on the 5GHz interface.
600762	[AP832] Random AP reboots.

ARRP

Tracking ID	Description
597875	Wireless network unavailable due to ARRP configuration changes from FortiWLM.
605659	[FAP-U24JEV] VAP entries deleted on many APs after ARRP re-planning.

Captive Portal

Tracking ID	Description
587725	Custom captive portal did not work in bridge mode ESS.
593343	External Captive Portal supported in tunnel mode did not work with APs in bridge mode.

Configuration – Controller/AP

Tracking ID	Description
544410	The VLAN pool name incorrectly includes the client OS.
550172	Request for MLDP management by controller in a tunnelled network.
591451	Band information missing in syslog.
591622	*MODIFY:Wireless Interface Configuration* message repeatedly sent to Syslogserver every 1 minute.
592841	Duplicate security PID entries observed in the controller.
594387	Incomplete RADIUS accounting packets; missing class attribute in random packets.
600763	[FAP-U43xF] ESS profiles failed to download.
601923	Controller sends the NAS IP address as physical interface address instead management VLAN address the accounting data packet.
602316	Printers not discovered by service control.
604360	[FAP-U24JEV] Incorrect AP uptime value displayed for enabled/online APs.
604951	Manually configured time setting not retained after controller reboot.

Controller Processes/Sluggishness

Tracking ID	Description
553667/599891	Random Melf process crashes observed.
561751/585598/585957/589185	Random SIP crashes observed.
567613	High CPU utilization observed.
578611	Monitoring using SNMP affected due to change in the AP uptime format.
580864	The SNMP process restarted twice in an hour due to memory issues.
581974/586451	Random SecurityMM crashes observed.
582168	Station unable to communicate over port 1521.
583860/604361/591139/595658	Random hostapd crashes observed.
584371/596835	Random IGMP-snoop crashes observed.
584563	Unresponsive GUI and continuous restart of the Xems services.
590917	Inconsistent/unstable SNMP table indexing for APs.
594841	Controller randomly stopped forwarding traffic on some APs.
598724	SNMP query failed due to unavailable MIB handler.
597035/605139	Random wncagent crashes observed.
606232	Random spectrumd process restarts.

Tracking ID	Description
608730	Random controller reboots.
609553	High latency observed on the controller
613593	Random MAC authentication failures observed.
614922	Random controller reboots.

DFS

Tracking ID	Description
562150	[FAP-U42xEV/32xEV/22xEV] AP not switching back to DFS channel after detecting the radar.
606165	[FAP-U24JEV] DFS channel change stalled beacon broadcast and lead to Tx stuck.
612313	[FAP-U43xF] AP did not broadcast SSID on the 2.4GHz radio (Bangladesh country).

GUI/CLI

Tracking ID	Description
557266/577580	AP status displayed as Enabled Online after a controller reboot even when the AP powered off.
575926	The **show sys-summary ess command** output required to sort by ESSID name.
577886/582086	The **show sys-summary ess** command displayed incorrect data.
578621	The **show sys-summary resources** command displayed incorrect CPU usage.
581719	The **show station** command output displays *Error in reading json string*.
586784	Unable to create a Native Cell ESSID using the EzSetup wizard in the GUI.
591191	Unable to access the controller GUI.
597979	The **show statistics ac-ap-diagnostics** command displays incorrect data.
598186	Unable to connect and run any commands on the APs, Watchdog not starting up.
606682	Incorrect IP address displayed in both CLI and GUI when the client switched to another ESSID.
610867	*Web Application Potentially Vulnerable to Clickjacking* and *Web Server Generic XSS* vulnerabilities observed in FortiWLC.
615815	Error on viewing the station IP addresses in the CLI and GUI.

Intermittent Connectivity

Tracking ID	Description
517039/544765	[FAP-U22xEV/24JEV] Stale stations not cleared created client connectivity issues.
520190	Connectivity impacted due to message drops in coordinator.
552049	[FAP-U42xEV/32xEV/22xEV] Communication failure (UDP round trip) between stations and wired host every 28 hours.
569241	Calls did not connect to spectra-link phones when the QoS policy was set to CAPTURE.
572286	[FAP-U32x/42xEV] Wi-Fi clients unable to obtain an IP address from DHCP server; station logs display that IP update not performed.
573983	[AP832] DHCP ACK not received by wireless stations; un-assigned IP address on the AP.
586959	[AP822v2] Intermittent client connectivity and unable to pass traffic due to high memory usage.
588533	Client connectivity impacted due to coordinator issues.
590276	[AP822/AP832] Random TCP traffic drops observed.
590403	Unable to pass traffic through the VLAN interface on the controller due to missing default route.
590608	Incomplete key handshake resulting in packet drops.
594837	Clients unable to obtain the IP address in bridge mode configured with static-vlan-only.
594892	Clients unable to make jabber SIP calls.
593341	Ping failure for IPv4 addresses.
601325	The ESS-AP table and VAP display not synced due to timer profile, impacting client connectivity.
611999	[AP822] Ping loss (request time out) to wireless clients observed.
618633	Random clients unable to connect to the SSID.

NPlus1

Tracking ID	Description
565275	Station did not get the IP address after Nplus1 takeover.
565633	Nplus1 failover did not work.
566148	SNMP service did not start on the slave controller following NPlus1 failover.
569381	Unable to pass traffic on the Wi-Fi client after Nplus1 failover (active slave); client shown connected with valid IP address.

Tracking ID	Description
570987	AD IDs were lost when the master controller returned to the active state from passive in an Nplus1 setup.
576008	Clients stuck in probe state on active slave controller and unable to associate with APs.

Others

Tracking ID	Description
452650/555975	FAP-U421EV did not auto-negotiate 1Gbps full duplex.
516091	System Diagnostics took days to complete with an error in AP diagnostics.
533495	RADIUS accounting stop message sent approximately 90 seconds after the wireless client disconnects.
541213/578161	Clients did not receive DHCP NACK with MAC authentication and RADIUS VLAN configured in the profile.
548885/583039	[FAP-U24JEV] Alarm on CPU usage above threshold observed.
573163	[AP832/AP822rev1] High wired-ping latency and sluggishness for wireless clients observed.
574907	[FAP-U22xEV] VoIP issues, call quality issues, data clients' throughput issues observed on Spectralink.
576593	[FAP-U22xEV] APs not forming Mesh backhaul on the controller.
579518	Flash logs take long to display.
583489	Rest API PUT requests failed with error 614; XML parse error.
591137	[FAP-U43xF] Poor performance and high latency observed by all wireless stations.
595917	Jumbo frames observed on the switch port where controller is connected.
597908	[FAP-U24JEV/FAP-U22xEV] PHYTX error on starting the base rates of 2.4Ghz from 18Mbps.
599761	Older installed patches are displayed after upgrade.
600326	[FAP-U24JEV] High latency observed.

Common Vulnerabilities and Exposures

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

Bug ID	Vulnerability
609595/609596	CVE-2020-9288

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

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
606704	VPN controller is not discovered in FortiWLM after controller upgrade.	Controller – FortiWLM communication impacted if configured over VPN.	Disable/enable VPN client and the controller gets discovered.
613692	SNMP walk for mwWncVarsBonding MIB shows single bonding as the output for controllers that are configured with dual bonding.		
628800	Sometimes, installing FAP-U43xF image on the controller fails.		Retry installing the FAP-U43xF image.
578243	Session count/SIP Session count statistics do not get cleared on disconnecting calls.		Reboot the controller.
616191	[ASCOM] Client gets discovered from the broadcast IP address.		Enable Force DHCP in the ESS profile.

Known Issues in FAP-U43xF

These are the known applicable to the **FAP-U43xF access points ONLY**.

Tracking ID	Description	Impact	Workaround
563931	Random AP reboots.	Client connectivity impacted.	
616566	Data Loss observed on some clients.	Sluggish user experience.	Reset the radio.

Tracking ID	Description	Impact	Workaround
617908	Radios report higher noise floor value.	Client connectivity impacted.	Reboot the AP.
618911	Low Mean Opinion Score (MOS) observed with Dual 5GHz Radio Mode enabled.	Poor voice call quality (scale of voice clients).