
FORTINET
High Performance Network Security
FortiWLM
Release 8.4.2

Contents

Product Overview

The FortiWLM (*Fortinet Wireless Manager*) Application Suite is an intelligent management system that helps you to easily manage your wireless network. It shares a common administrator interface, making it easy to transition between the following applications:

- *FortiWLM (NM)*—is a web based application suite which manages controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network.
- *Service Assurance Manager (SAM)*—provides trouble-prevention capability that uses the FortiWLM infrastructure to perform end-to-end system tests, either on-demand or automatically at periodic configured intervals. SAM works by comparing a well-functioning network baseline metric to periodic tests. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with Service Assurance Manager.
- *Spectrum Manager (SM)*—is used to manage your network health. The SM uses a network of devoted sensors or one of the radios on non-dedicated Fortinet Access Points, to continually scan the environment for interferences. With Fortinet Spectrum Manager, you can identify sources of potential interference and present interferer data on graphical dashboards to deliver high bandwidth and control the wireless spectrum for high quality of service (QoS). The software based sensors detects and classifies sources of wireless interference and pro-actively manages channel interference issues. The sources for potential interference in 2.4 GHz and 5 GHz spectrum is identified and graphically represented on the dashboard.
- *Wireless Intrusions Prevention System (WIPS)*—Fortinet's WIPS provides complete wireless threat detection and mitigation into the wireless network infrastructure. It detects wireless intrusions using predefined and custom signatures on an integrated platform with other WLAN management applications.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Product Documentation

This release of FortiWLM delivers a comprehensive set of customer documentation.

- FortiWLM User Guide
- Online Help integrated into the FortiWLM application
- FortiWLM API Reference documents

What's New

In this release of FortiWLM the following new features and functionalities are delivered.

Note:
This release supports **ONLY** 64-bit virtual FortiWLM; Support for 32-bit virtual FortiWLM is not available. See section Migrating from Virtual FortiWLM 32-bit to Virtual FortiWLM 64-bit.

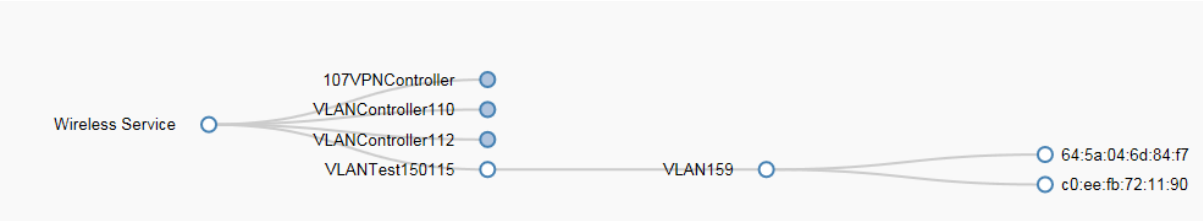
- Network Topology
- AP Dashboard – New Icons
- Network Dashboard – Rogue APs
- Station Dashboard – Locationing
- Encrypted (.fwlm) Upgrade Support
- Multiple PSK – Import/Export
- RADIUS Enhancements
- REST APIs

Network Topology

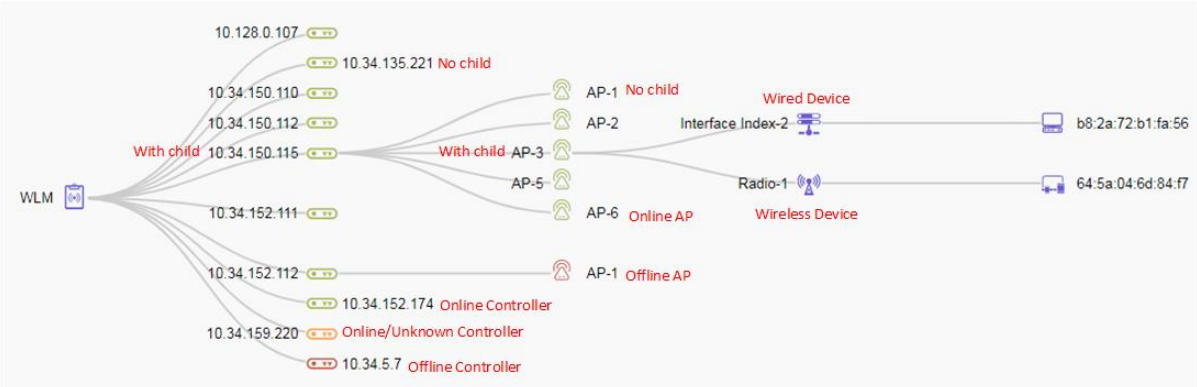
The network topology view provides graphic representation of the physical and logical topology of your network. This feature illustrates the physical topology of communication devices in your network such as access points, stations, and controllers and the logical topology of wireless service, ESS, and VLANs. Navigate to *Monitor > Topology*.

Note: The physical and logical network topology views differ based on the browser, *Internet Explorer & Microsoft Edge* **VS** *Chrome, Firefox, and Safari*.

Logical Topology

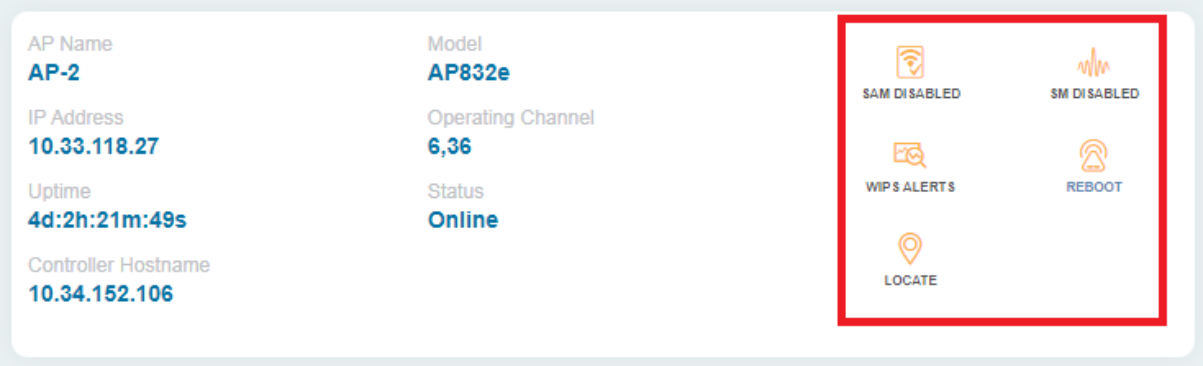


Physical Topology



AP Dashboard – New Icons

The dashboard icons allow you to monitor the status and health of the access points. The following icons are available on the dashboard.
Navigate to *Monitor > Overview > AP*.

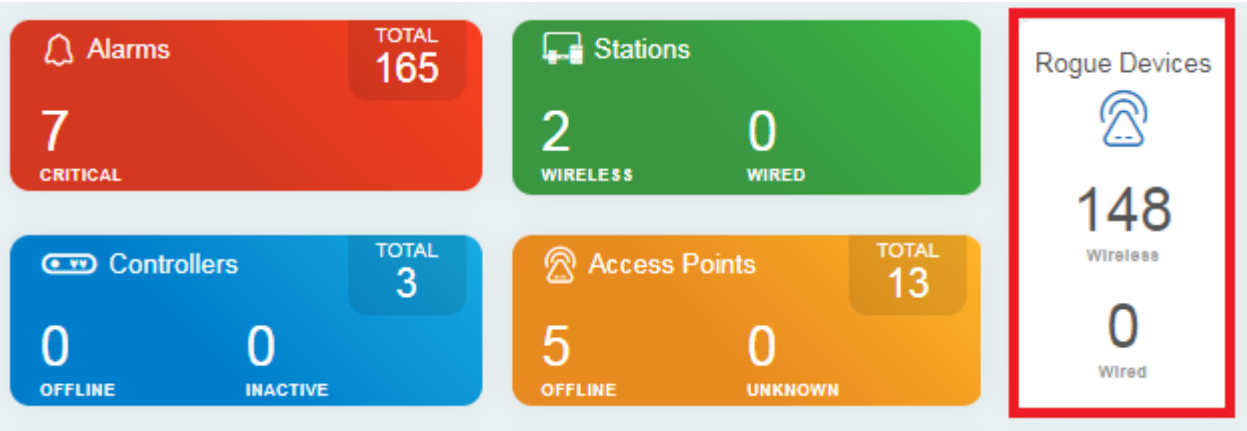


- **SAM Enabled/Disabled**: This icon indicates if any SAM tests are running on the access point. The icon status is **SAM Enabled** if baseline or scheduled tests are running; click the icon to view the *Ongoing Tests* dashboard in SAM. Hover over this icon to view the access point's interface details on which SAM tests are running. The icon status is **SAM disabled** when no tests are running on the access point.
- **SM Enabled/Disabled**: This icon indicates whether Spectrum Manager is enabled or disabled on the access point. The icon status is **SM Enabled** if the AP radios are operating in the scan spectrum mode. Hover over this icon to view the access point's interface details which is operating in the Scan Spectrum mode. The icon status is **SM Disabled** if the AP radios are operating in the service/normal mode.
- **WIPS Alerts**: Click this icon to view the alerts raised by an access point when WIPS is configured, in the *Alerts* dashboard in WIPS. Hover over the icon to view the access points interface (1,2,3) details that are generated in the alerts. This option is disabled if WIPS is not configured.
- **Reboot**: Click this icon to reboot an online access point only. This option is disabled if the access point is offline/unknown.
- **Locate**: Click this icon to view the location of an access point on the floor map. This option is disabled if the access point is not placed on the floor map.

Network Dashboard – Rogue Devices

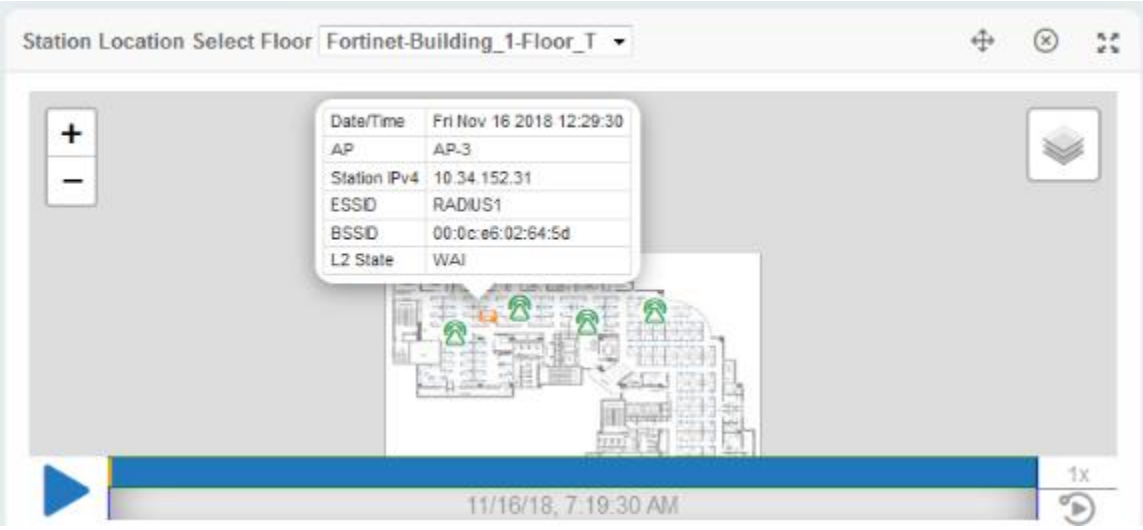
The network dashboard now provides the total count of wired and wireless rogue devices (APs and stations) in the network. Click on the tabs to view the detailed summary, displayed in a separate popup screen. The associated rogue device information is displayed, *Controller Name, Rogue MAC Address, Rogue Type, BSSID, Channel, SSID, AP Reported, DateTime*, and *Location*.

Navigate to *Monitor > Overview > Network Summary*.



Station Dashboard – Locationing

In the stations dashboard, the station location widget has been added; navigate to *Monitor > Overview > Stations.*

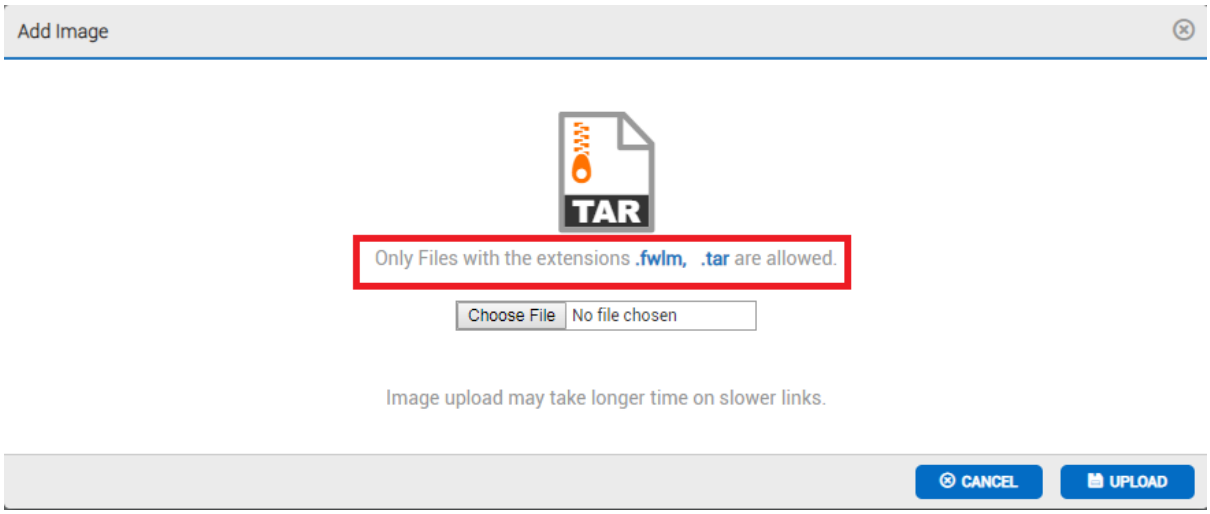


The **Station Location** panel provides a graphical representation of the stations per floor. The floor map allows you to view the movement of the stations on a floor in the last 24 hours using the time-line view (with play and pause options). By default, the latest location of the station is displayed on the floor map.
Note: This panel is available on the dashboard only when the location services are enabled.

Encrypted (.fwlm) Upgrade Support

The FortiWLM build files are now available in the *.fwlm* format. You can upgrade FortiWLM using both *.fwlm* and *.tar* files.
Note: This release introduces software upgrades using the *.fwlm* format. Direct upgrade from a pre-8.4.2 to 8.4.2 release using the *.fwlm* format is not supported.

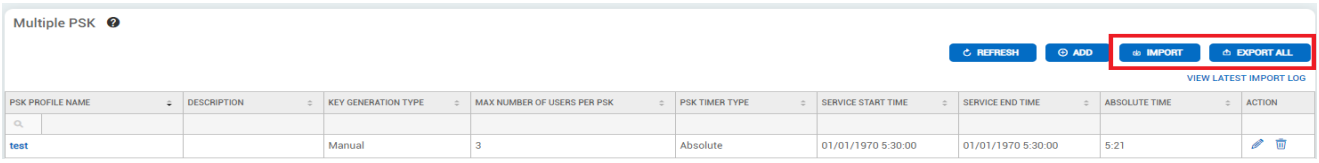
Navigate to *Administration > WLM Upgrade*.



Multiple PSK – Import/Export

You can export the multiple PSK profiles to your local system and import profile information into FortiWLM. Click **Export ALL** to export all existing PSK profiles' information in the *.csv* format on your system.

Navigate to *Configuration* > *Templates* > *Multiple PSK*.



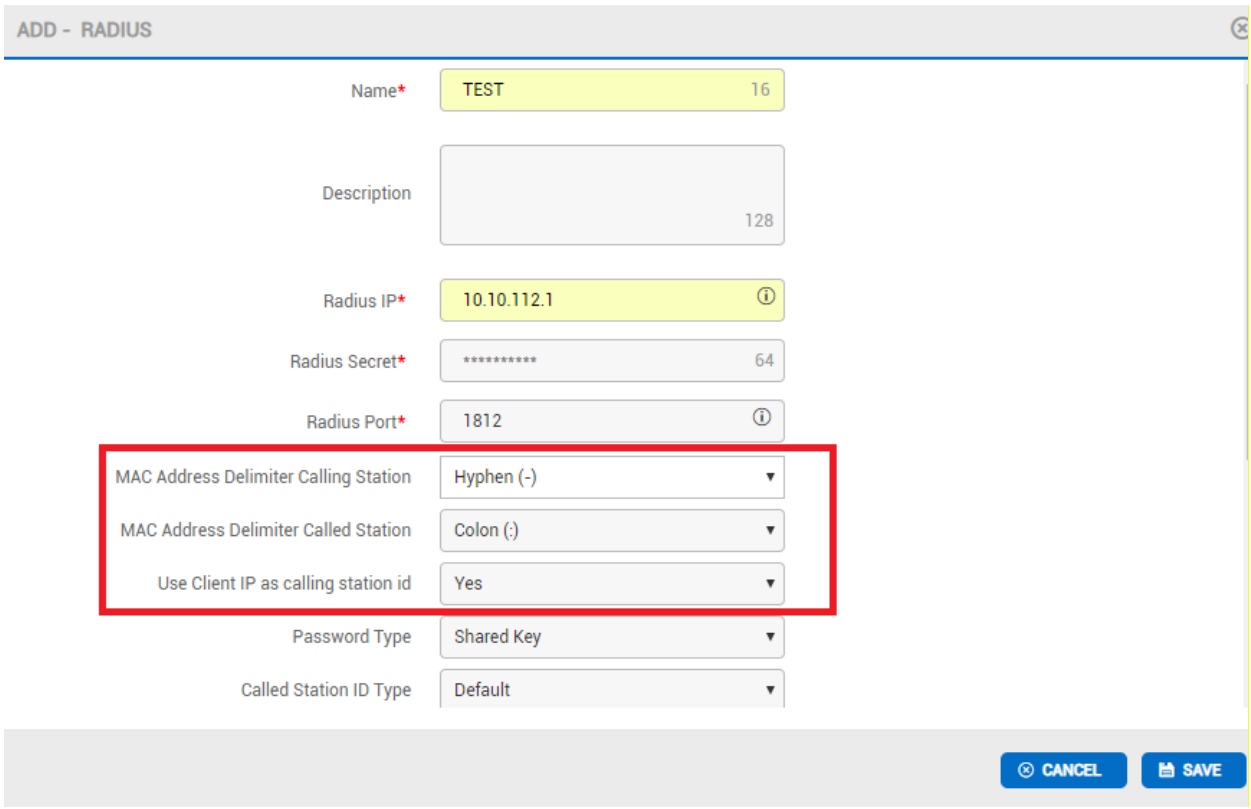
The multiple PSK profile information can be imported in the *.csv* format. The following fields are required to import the profile information.

- **Basic Configuration**
  - Profile Name
  - Description
  - Key Generation Type
  - Max Number of Users per psk
  - PSK Timer Type
  - Service Start Time
  - Service End Time
  - AbsoluteTime
- **Groups**
  - Profile Name
  - Group Name
  - Tunnel Interface Type
  - VLAN Pool Name
  - VLAN Profile
- **PSK Configuration**
  - Profile Name
  - User Name
  - PSK Key
  - Email ID
  - Group Name
  - MAC Binding
  - MAC Address

Note: Insert an empty row after every table so that the configuration is imported and applied correctly.

RADIUS Enhancements

Additional fields are added to RADIUS profiles; navigate to *Configuration* > *Templates* > *RADIUS*.



- **MAC Address Delimiter Calling Station** and **MAC Address Delimiter Called Station**
  In the **MAC Address Delimiter Calling Station** and **MAC Address Delimiter Called Station** drop-down lists, select the delimiter used on the RADIUS server to separate MAC addresses.
  - **None**--No delimiter is used.
  - **Hyphen (-)**--Hyphens are used to delimit the fields (xx-yy-zz-aa-bb-cc)
  - **Single Hyphen (-)**--Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
  - **Colon (:)**--A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)

- **Use Client IP as calling station id**
  Enable **Use Client IP as calling station id** to use the wireless client IP address as the calling station ID. When enabled the MAC address delimiter need not be specified.

- **NAS IP**
  [IPv6 only] The NAS IP address to be used in RADIUS access requests. When configuring a controller to use a RADIUS server, the controller interface has multiple IP addresses, select the IP address included in the RADIUS configuration. However, if the NAS IP is not specified, any of the controller IPv6 interface addresses is used instead.

REST APIs

This release delivers REST APIs v2 with standardized API interfaces that comprise of a common format for all deployment APIs. You can refer to *the FortiWLM API Reference Guide.*

Performance Optimization

The following are performance optimizations in FortiWLM 8.4.2 vis-à-vis previous releases based on specific parameters.
This data is based on QA laboratory results.

- Improved responsiveness for GUI operations and report generation time.
- Improved station locationing and RF planner optimization (due to improved CPU utilization).

Additional Information

This section describes information related to the usage of FortiWLM.

- In case of an Nplus1 cluster, note the following points:
  - After the Nplus1 cluster formation is complete, it takes a maximum of 10 minutes to get discovered in FortiWLM.
  - If the slave and master controllers are to work as standalone, then backup the FortiWLM configuration, double delete the controller and add it again from the controller inventory in FortiWLM, so that the controller can be successfully managed.
- FortiWLC 8.5 onwards the MC-VE series virtual controllers are **NOT** supported.
- After upgrading to 8.4.2 from pre-8.4.1, disable and enable the location service profile, in case the location service is running.
- The GUI menu option (*Administration > System Settings > High Availability*) to configure high availability from is removed for FortiWLM-100D and SA250 platforms.

Supported Security Modes

This table lists the security modes supported for the Service Assurance Manager (SAM) on FortiWLM.

AP Models	Security Modes Supported	Security Modes Not Supported
All supported models	Open	WPA2 PSK TKIP
	WPA2 Enterprise AES	WPA2 Enterprise TKIP
	WPA2 PSK AES	WEP64
	Mixed PSK TKIP	WEP128
	Mixed Enterprise TKIP	SMS4

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
Service Assurance Manager	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV

Hardware / Software	Supported Versions/Models
Spectrum Manager	• AP332 • AP832 • PSM3x • AP1010 • AP1020 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV
Controller Models	• FortiWLC-200D • FortiWLC-500D • FortiWLC-50D • FortiWLC-1000D • FortiWLC-3000D • MC1550 • MC1550-VE

	• MC3200 • MC3200-VE • MC4200 • MC4200-VE • FWC-VM-50 • FWC-VM-200 • FWC-VM-500 • FWC-VM-1000 • FWC-VM-3000 **Note:** FortiWLC 8.5 onwards the MC-VE series virtual controllers are **NOT** supported.
Access Points	• AP122 • AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e • AP320 • AP332e • AP332i • AP433e • AP433i • OAP433e • FAP-U421EV, FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U422EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • AP1010e • AP1010i, AP1020e • AP1020i, AP1014i • AP110
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • FWM-VM • Hyper-V (*supported only on Windows 2016 server*) • KVM *The following service appliances are **NOT** supported on 64-bit FortiWLM:* • SA250 • SA2000 **#** Due to hardware limitations, High Availability is not supported in FortiWLM 100D and SA250 appliances.
Supported Browsers	• Internet Explorer 9 and later version (*All the pages of FortiWLM will load under normal browser settings. Compatibility View Settings are not supported*.) **Note**: The Internet Explorer version 11 displays floor maps only when they are uploaded in the *.gif* file format. See known issue - 524637. • Mozilla Firefox 61.0.2 • Google Chrome 68.0 • Microsoft Edge (Windows 10) • Safari (MacOS) 11.0.3

Migrating from Virtual FortiWLM 32-bit to Virtual FortiWLM 64-bit

To use the 8.4.2 features and retain data, when upgrading from pre-8.4, perform this procedure to migrate a virtual FortiWLM 32-bit to a virtual FortiWLM 64-bit.
The migration can be performed to the current 64-bit version from two prior versions ONLY, for example, data from 8.3.3 and 8.3.2 can only be migrated to 8.4. Hence, it is recommended to migrate pre-8.4 virtual FortiWLM 32-bit **to** 8.4/8.4.1 virtual FortiWLM 64-bit and then **to** 8.4.2.

1. Backup the data in 32-bit FortiWLM and copy it using the copy scp/ftp command.
2. Install the 64-bit FortiWLM image; use the *forti-wlm-x.x-xbuild-y-x86_64.ova* file.
3. Shutdown the 32-bit FortiWLM instance.
4. Run the following commands in the 64-bit FortiWLM to copy and restore the backed up 32-bit data:
   - ***copy scp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.***
     OR
     copy ftp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.
   - ***restore <Backup file name>***

The following are recommended to perform the migration operation:

- Do not change the name of the database backup file.
- During the backup/restore operation, do not close the CLI session; closing the session aborts the backup/restore operation. For more information, see the backup and restore command details in the *FortiWLM User Guide*.

NOTES:

- Migration from SA2000-VE to FWM-VM 64-bit requires a new license file to be installed on FWM-VM 64-bit.
- Migration from FWM-VM 32-bit to FWM-VM 64-bit does NOT require any license changes if the system ID is the same on both. However, if the system ID differs then a new license file is required for FWM-VM 64-bit.

  For licensing options contact the *Sales Account team*

Upgrading FortiWLM

This section describes procedures for upgrading your Services Appliance.

Pre-requisites

- To discover the FortiWLC 8.3.3 64-bit controllers (**listed below**) in FortiWLM 8.4.0/8.4.1/8.4.2, you need to apply the FortiWLC 8.3.3 patch. Contact the Customer Support for installing the relevant patch.

  - FortiWLC-1000D
  - FortiWLC-3000D
  - FWC-VM-50
  - FWC-VM-200
  - FWC-VM-500
  - FWC-VM-1000
  - FWC-VM-3000

- Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade. While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported FortiWLM Upgrades

The following upgrade path is recommended.

From FortiWLM version…	To FortiWLM version
6.1-3-6/7.0-5-0	8.0-7-0
6.1-3-6/7.0-5-0/8.0-7-0	8.0-SR1-1
8.0-7-0/8.0-SR1-1	8.1-2-0
7.0-5-0/8.0-7-0/8.1-2-0	8.2.2
8.1-2-0/8.2.2	8.2.4
8.1-2-0/8.2.2	8.3.0
8.2.4/8.3.0	8.3.1
8.2.4/8.3.0/8.3.1	8.3.2
8.2.4/8.3.1/8.3.2	8.3.3
8.3.1/8.3.3	8.4.0
8.3.3/8.4.0	8.4.1
8.4.0/8.4.1	8.4.2

Supported FortiWLC Releases

FortiWLM Version	Supports Controllers with these FortiWLC-SD Versions
8.4.2	• 7.0-11MR-1 • 7.0.13 • 8.0-6-0 • 8.1-3-2 • 8.2.7MR-1 • 8.3.1 • 8.3.3 **Note:** [*FortiWLC 8.3.3 64-bit only*] – Contact Customer Support for installing the relevant patch. • 8.4.0 • 8.4.1 • 8.4.2 • 8.4.3 • 8.4.4 • 8.5.0

Application Visibility Policies

Application visibility policies in controllers running FortiWLC-SD 8.0 that is managed by FortiWLM 8.1 or later will be disabled. To continue using those policies, upgrade FortiWLC-SD to 8.1 or later.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions prior to FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

Upgrading via CLI

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

    ```
    sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
    ```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

    ```
    sa# sh
    flash 6.0-
    7-0 8.2-1-0
    ```

7. Upgrade the service appliance:

    ```
    sa# upgrade nms-server <Version>
    ```

    This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.
8. Type the following command to confirm, if the installed software version is 8.3.3.

    ```
    service appliance# sh nms
    ```

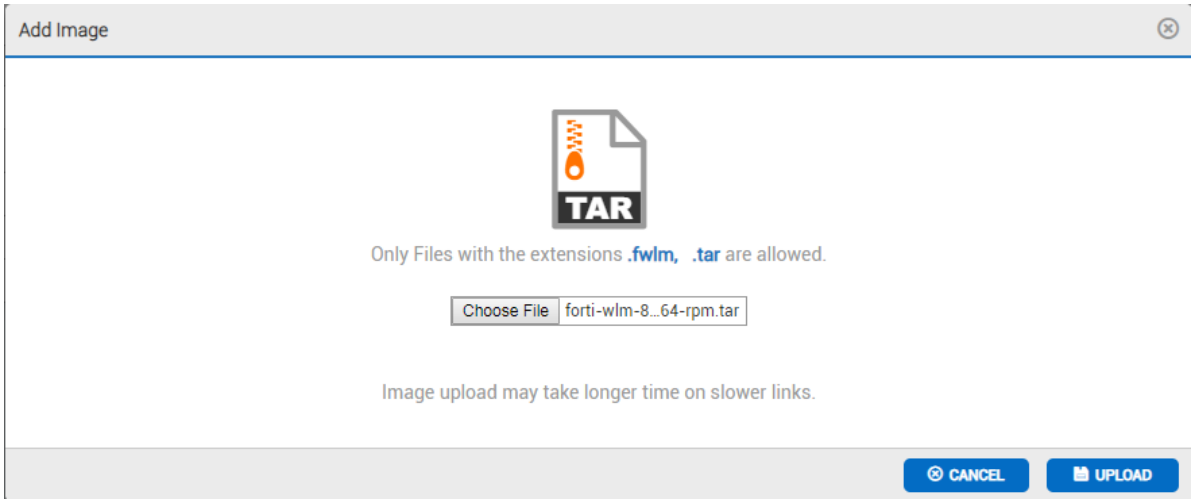
    If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network

Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

Upgrading via GUI

The following procedure will guide you through the steps to upgrade your server from WebUI.
Note: This release introduces software upgrades using the *.fwlm* format. Direct upgrade from a pre-8.4.2 to 8.4.2 release using the *.fwlm* format is not supported.

1. In the Network Manager WebUI, go to **Administration > WLM Upgrade**. By default, this page lists all the images copied to the server.
2. To upgrade your server to a different version than the ones listed, click **Add** to open the file selector window.



3. Select the image file from your computer or a network folder and click the **UPLOAD** button
4. After the upload is complete, select the version to install and click the **INSTALL** button to being the upgrade process.

During the upgrade process, do not click refresh or perform any operations on the server.

After the upgrade is complete, click **Go** to return to server operations.

- For a full upgrade, the server will restart after the upgrade process and return the page to server login prompt.
- For patch upgrade, the server will restart the process and return to the dashboard.

Post Upgrade Tasks

The following are optional post-upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration > System Settings > Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrading FortiWLM

Downgrading FortiWLM to a previous version is not supported.

Fixed Issues

Bug ID	Description
537330	Cannot import FortiWLC configurations into FortiWLM.
532715	Reports generated with PDF format show junk values.
532524	User unable to edit the base rates on ESS profile in FortiWLM.
531532	FortiWLM always shows Controller status as *Online Inactive*.
529393	In the access point inventory, display of *Discovery Protocol* is inconsistent at different places.
529227	Map Management - adding buildings needs usability improvement.
529218	Error when trying to import a floor map in *.zip* format.
528862	With daily backup configured by the GUI for SCP, file transfer fails to complete.
527016	*reload default factory* behaviour not clear as some data is retained. The command presumably causes file system corruption.
526342	FortiWLM GUI enhancement request - Network Health pop-up and Wireless Station pie chart.
522695	FortiWLM upgrade failure from 8.4.0 to 8.4.1.
520466	Station activity management is not seen on the FortiWLM.
518414	FortiWLM sends only username and password attribute in RADIUS request packet.
516392	Heat map not working after more AP licenses were added to FortiWLM.
513376	Missing data in FortiWLM.
509999	Indents (new lines, spaces) are not displayed in *Controller Configuration Diff* page.
509973	Trend graph for the connected controller shows blank spaces in FortiWLM.
506671	The RF signal strength and other details in heat maps are displayed only for some APs.
504956	nmsagent crash on controller version 8.3.3.
504094	Loss of APs and APs' misalignment to the top left corner of the heat maps.
499323	nmsagent crash on controller.
407150	ESS profile synchronization fails - *Failed to sync ESS Profile:HWL-GUEST-Bridged, Configuring 802.11r Group must be between 1 and 65535.*
379446	Unable to register controllers under the wireless profile.
373683	FortiWLM 5GHz Heat Map is very small.
347139	Allow customized messages for email notifications.

Known Issues

These are the known issues in this release of FortiWLM.

Bug ID	Description	Impact	Workaround
496547	Spectrum Manager is not accessible over an IPv6 address.	Spectrum Manager inaccessible.	Access Spectrum Manager over IPv4.
497117	The RF planner displays the same data rate values in all locations covered by an AP.	The exact data rate values for different locations unavailable.	
472501	Spectrum Manager dashboard page is not displayed in the Microsoft Edge browser.	The Spectrum Manager dashboard page does not load.	Apply self-signed or third party trusted certificate on FortiWLM. Enable flash on Microsoft Edge browser.
524637	Due to the vulnerability fix, the floor maps do not load on IE version 11 for the following features: • Client Density *(Monitor > Network Summary)* • Station Location *(Monitor > Stations)* • Network Heat Maps *(Monitor > Heat Maps)* • Map Management (*Operate > Map Management*) • Locationing *(Monitor > Locationing)*	Floor maps are not displayed on the GUI.	Convert floor maps/image into *.gif* file format and re-uploaded in *Operate > Map Management.*
527123	SAM is not supported over WPA3.		
523830	SM is not available on the Firefox browser version 64.0.		Install Flash player separately and restart the browser. https://helpx.adobe.com/flash-player.html
523638	Icons are not displayed for Physical and Logical Topology pages in Internet Explorer/Microsoft Edge browsers due to issues with these browsers. https://developer.microsoft.com/en-us/microsoft-edge/platform/issues/4320441/	The topology visualization is different when compared to other browsers (*Chrome*, *Safari* and *Firefox*)	
530231	Pie charts in the AP Group dashboards are not positioned in the centre when viewed on the IE due to unsupported standard UI styles on the browser. This issue is observed on the following dashlets: • High Channel Utilization APs • High Retry APs • High Loss APs	Pie chart format not aligned on the GUI.	
520758	WIPS alerts cannot be viewed on APs connected to VPN/NAT/PAT controllers as	WIPS alerts page unavailable.	

	the source IP address of the access point displayed in the alerts page does not support private IP addresses. **Note**: In such cases the WIPS alerts icon is enabled.		
537776	SAM fails when a multiple PSK user exists in FortiWLC.	SAM tests fail.	Use SAM when multiple PSK users are not configured.
531819	*General Error* for wireless service profiles synchronized from FortiWLM to AP Groups and Radio groups on FortiWLC running version 8.4.3. **Note:** This issue is resolved in FortiWLC 8.4.4.		
353858	Spectrum sensors not displaying data; error received - *Device is not in database*.	Spectrum data unavailable.	Contact the Customer Support.

Common Vulnerabilities and Exposures

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

Bug ID	Vulnerability
484861	CVE-2018-1000001 CVE-2018-6485 CVE-2018-6551
470969	CVE-2017-3737 CVE-2017-3738
529680	CVE-2018-1000004
480053	CVE-2018-7492
508644	CVE-2018-5391

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

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