FortiWLM - Release-Notes

Version 8.6.2

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

October 29, 2021
FortiWLM 8.6.2 Release-Notes

TABLE OF CONTENTS

Change log

Date	Change description
2021-10-29	FortiWLM 8.6.2 release version.

About FortiWLM 8.6.2

FortiWLM release 8.6.2 resolves common vulnerabilities. See section Common Vulnerabilities and Exposures on page 19

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.
- *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.

Note: 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.

Operational Guidelines

This section describes information related to the usage of FortiWLM.

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

AP Models	Security Modes Supported
All supported models	Open
	WPA2 Enterprise AES
	WPA2 PSK AES
	Mixed PSK TKIP
	Mixed Enterprise TKIP

The FortiWLC, FortiGate, and FortiWLM time must be synchronized. It is recommended to use NTP server.

FortiWLC Controllers

This following information is related to the usage of FortiWLM with FortiWLC controllers.

- 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 secondary and primary 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.
- The GUI menu option (**Administration > System Settings > High Availability**) to configure high availability from is removed for FortiWLM-100D.
- The risk level for **Monitor > Overview > Application Summary** cannot be defined for custom applications.
- [VPN with NPlus1] Configure the VPN client before configuring NPlus1 in secondary controller.
- Configure Jumbo frames from the controller only when the MTU values are to be more than 4500 bytes.
- Fortinet recommends usage of certificates with OCSP endpoint URI, when uploading certificates onto the WLM.
- Fortinet recommends running a single FortiWLM GUI session in scale setups.

FortiGate Controllers

This following information is related to the usage of FortiWLM with FortiGate controllers.

- A maximum of 5 concurrent GUI sessions are allowed.
- Application control is supported on FortiOS version 6.2.2 and later.
- Station activity logs are supported on FortiOS version 6.2.0 and later.
- Station logs from log storage as FortiCloud will fetch only 100 events at once.
- Wired clients are not supported.

Feature	FortiOS Versions				
	6.0.6	**6.2.0/6.2.1**	**6.2.2/6.2.3**	**6.4.0/6.4.1/6.4.2/6.4.3/ 6.4.4/6.4.5/6.4.6/6.4.7**	**7.0.0/7.0.1/7.0.2**
Dashboard Status					
Application Control	X	X	✓	✓	✓
Station Data	✓	✓	✓	✓	✓
Station activity logs	X	✓	✓	✓	✓
AP Dashboard					
Retry %	X	X	✓	✓	✓
Loss %	X	X	✓	✓	✓
Channel Utilization%	✓	✓	✓	✓	✓
SNR (dBm)	X	X	✓	✓	✓
Average Throughput	X	X	X	X	✓
Station Dashboard					
Retry %	X	X	✓	✓	✓
Loss %	X	✓	✓	✓	✓
Channel Utilization%	X	X	X	X	X
SNR (dBm)	✓	✓	✓	✓	✓

Supported Hardware and Software

This section describes the supported hardware models and software versions compatible with FortiWLM.

FortiGate/FortiOS

This table lists the compatible FortiGate/FortiOS software versions tested with this release of FortiWLM.

Note: All FortiGate controller and FortiAP models are supported and managed by FortiWLM. For more information on the supported hardware per FortiOS version, see FortiGate documentation.

Hardware / Software	Supported Versions/Models
FortiOS	• 6.0.6 (limited Monitoring) • 6.2.0 • 6.2.1 • 6.2.2 • 6.2.3 • 6.4.0 • 6.4.1 • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6 • 6.4.7 • 7.0.0 • 7.0.1 • 7.0.2
Spectrum Analyzer	All AP models that support Spectrum Analyzer with FortiGate are compatible with FortiWLM Apectrum Analyzer.

FortiWLC

This table lists the FortiWLC hardware and software versions tested with this release of FortiWLM.

Hardware / Software	Supported Versions/Models
Controllers	• FortiWLC-200D • FortiWLC-500D • FortiWLC-50D • FortiWLC-1000D • FortiWLC-3000D • FWC-VM-50 • FWC-VM-200 • FWC-VM-500 • FWC-VM-1000 • FWC-VM-3000
FortiWLC	• 7.0.15 • 7.0.14 • 7.0.13 • 8.3.1 • 8.3.3 **Note**: [FortiWLC 8.3.3 64-bit only] – Contact Customer Support for installing the relevant patch. • 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 • 8.5.3 • 8.5.5 • 8.6.0 • 8.6.1 • 8.6.2
Access Points	• AP122 • AP822e • AP822i (v1 & v2) • AP832e • AP832i • OAP832e • AP320 • AP332e • AP332i • AP433e • AP433i • OAP433e

Hardware / Software	Supported Versions/Models
	• FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U422EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U431F • FAP-U432F • FAP-U433F • FAP-U231F • FAP-U234F • AP1010e • AP1010i • AP1020e • AP1020i • AP1014i • AP110
Service Assurance Manager	• AP122 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV
Spectrum Analyzer	• FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV • FAP-U431F • FAP-U433F

Service Appliance

This table lists the compatible FortiWLM appliance/VM versions.

Hardware / Software	Supported Versions/Models
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • FWM-VM • Hyper-V (supported only on Windows 2016 server) • KVM **Note**: Due to hardware limitations, High Availability is not supported in FortiWLM 100D.

Web Browsers

This table lists the supported browser versions to access FortiWLM.

Hardware / Software	Supported Versions/Models
Supported Browsers	• Mozilla Firefox 92 • Google Chrome 94 • Microsoft Edge (Windows 10) 94 • Safari (MacOS) 14

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

To use new 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** 8.4/8.4.1/8.4.2 virtual FortiWLM 64-bit and then **to** the current release.

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 requiredfor 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 upgrade to 8.6 from 8.4.2, an intermediate upgrade to 8.5 or 8.5.1 is required. Contact the *Customer Support* for installing the relevant patch.

To discover the FortiWLC 8.3.3 64-bit controllers (listed below) in FortiWLM 8.4.0 and above, 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 FortiWLM before you initiate controller (FortiWLC-SD) upgrade. While upgrading a FortiWLM 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
8.5.1/8.6.0	8.6.1
8.6.0/8.6.1	8.6.2

Application Visibility Policies

Application visibility policies in controllers running FortiWLC-SD 8.0 that is managed by FortiWLM 8.2.4 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.

Note: Data backup is recommended prior to upgrading FortiWLM.

Upgrading via GUI

The following procedure will guide you through the steps to upgrade your server from WebUI.

1. In the FortiWLM GUI, 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 **UPLOAD**.
4. After the upload is complete, select the version to install and click **INSTALL** to being the upgrade process.

Note: 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.

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 FortiWLM 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 FortiWLM - **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 FortiWLM.

8. Type the following command to confirm, if the installed software version is 8.5.0 - service appliance# sh nms.

If the upgrade displays the "image integrity error," the FortiWLM image has been corrupted while uploading to FortiWLM. Upload the new image again to the FortiWLM and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

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.

Known Issues

These are the known issues in this release of FortiWLM.

Bug ID	Description	Impact	Workaround
746289	Alarm count mismatch between the Long Term Trend dashboard and the *Fault Management* page.		
746291	The *Stations* graph in the Long Term Trend dashboard displays incorrect values.		
746552	The *Map Management* page displays FortiWLC APs in the FortiGate view and vice versa.		
746559	The *Fault Management* page displays FortiWLC alarms in the FortiGate view and vice versa.		

Common Vulnerabilities and Exposures

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

Vulnerability	Description
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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