Micro-FortiGuard Server for FortiClient - Release Notes

Version 6.0.3

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 22, 2019
Micro-FortiGuard Server for FortiClient 6.0.3 Release Notes
02-603-519841-20191022

TABLE OF CONTENTS

Introduction **4**
Supported models 4
Licenses 4
What's new in 6.0.3 4
Installation Information **5**
Firmware image checksums 5
Product Integration and Support **6**
Micro-FortiGuard Server for FortiClient 6.0.3 support 6
Feature support 6
Appendix A - FortiGuard Distribution Servers (FDS) **7**
FortiGuard Center update support 7
Change Log **8**

Introduction

This document provides the following information for Micro-FortiGuard Server for FortiClient 6.0.3 build 0255:

- Supported models
- Licenses
- What's new in 6.0.3
- Installation Information
- Product Integration and Support
- FortiGuard Distribution Servers (FDS)

The recommended minimum screen resolution for the Micro-FortiGuard Server for FortiClient GUI is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Supported models

Micro-FortiGuard Server for FortiClient version 6.0.3 supports the following models:

Micro-FortiGuard Server for FortiClient VM	FMG-VM64-MFGD

Licenses

Micro-FortiGuard Server for FortiClient licenses are concurrent, but not stackable.

Micro-FortiGuard Server for FortiClient supports a maximum of 20,000 FortiClient endpoints.

What's new in 6.0.3

Micro-FortiGuard Server for FortiClient is a local update server for FortiClient endpoints. FortiClient can receive software and signature updates locally from Micro-FortiGuard Server for FortiClient instead of reaching out to FortiGuard Distribution Server, helping save WAN bandwidth. It is recommended that organizations with more than 500 FortiClient endpoints use Micro-FortiGuard Server for FortiClient to receive local updates.

For details, see the *Micro-FortiGuard Server for FortiClient Administrator Guide* that is available on the Fortinet Document Library under the FortiClient EMS product.

There are no new features in Micro-FortiGuard Server for FortiClient 6.0.3.

Installation Information

For installation information, see the *Micro-FortiGuard Server for FortiClient VM Install Guide* that is available on the Fortinet Document Library under the FortiClient EMS product.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

Micro-FortiGuard Server for FortiClient 6.0.3 support

The following table lists 6.0.3 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.
FortiClient EMS	• 6.0.0 and later
FortiClient	• 6.0.0 and later • 5.6.0 and later
Virtualization	• VMware vSphere and VMware Player

Feature support

Following is the list of Micro-FortiGuard Server for FortiClient feature support for FortiClient endpoints:

- FortiClient software updates
- WebFilter
- Antivirus signature, application control, and vulnerability database updates

Appendix A - FortiGuard Distribution Servers (FDS)

In order for Micro-FortiGuard Server for FortiClient to request and retrieve updates from FDS, please configure the necessary settings based on the items listed below:

- Micro-FortiGuard Server for FortiClient accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between Micro-FortiGuard Server for FortiClient and FDS, Micro-FortiGuard Server for FortiClient uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.

FortiGuard Center update support

You can configure Micro-FortiGuard Server for FortiClient as a local FDS to provide FortiGuard updates to FortiClient endpoints. The following table lists which updates are available per platform/version:

Platform	Version	Antivirus	Vulnerability Scan	Software
FortiClient (Windows)	• 5.6.0 and later • 6.0.0 and later	✓	✓	✓
FortiClient (Mac OS X)	• 5.6.0 and later • 6.0.1 and later	✓	✓	✓

Change Log

Date	Change Description
2018-11-02	Initial release of 6.0.3.
2019-10-22	Updated Licenses on page 4.

Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.