Release Notes

FortiADC Manager 7.6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

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/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
March 5, 2025	Initial release.

Introduction

This Release Notes covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Manager Version 7.6.0, Build 0087.

FortiADC Manager allows you to use a web-based user interface to configure remote FortiADC devices. It allows you to simplify and speed up the FortiADC deployment and update process by maintaining configuration templates and policy packages that you can modify and apply as needed.

For additional documentation, visit https://docs.fortinet.com/product/fortiadc-manager/.

Consult the ADC Manager handbook for setup instructions.

FortiADC Manager 7.6.0 supports managing FortiADC 6.0.x or later versions.

What's new

There are no new features in FortiADC Manager 7.6.0.

Resolved issues

The following issues have been resolved in FortiADC Manager 7.6.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1126219	NTP server status incorrectly shows as 'Not synchronized' despite the FortiADC-Manager system time being correct. The status should reflect 'Clock is selected' when the system time is synchronized.
1103158	Vulnerability scan report identifies the following issues in the FortiADC Manager GUI: 96-bit MAC algorithms need to be disabled (item #71049). Weak ciphers should be removed (item #90317). Support for TLS 1.2 and/or 1.3 should be enabled, and TLS 1.1 disabled (item #157288). Request to verify the existence of these configuration options.
1137659	The Web Vulnerability Scanner has OS command injection vulnerabilities that allow remote code execution. Mitigation requires removing libwvs and fixing tcpdump with proper input validation and sanitization.

Common Vulnerabilities and Exposures

For more information, visit https://www.fortiguard.com/psirt.

| Bug ID	Description
0985992	FortiADC Manager 7.6.0 is no longer vulnerable to the following CVE-Reference: CVE-2023-48795.

Known issues

There are no known issues in FortiADC Manager version 7.6.0. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Customer Service & Support image checksum tool
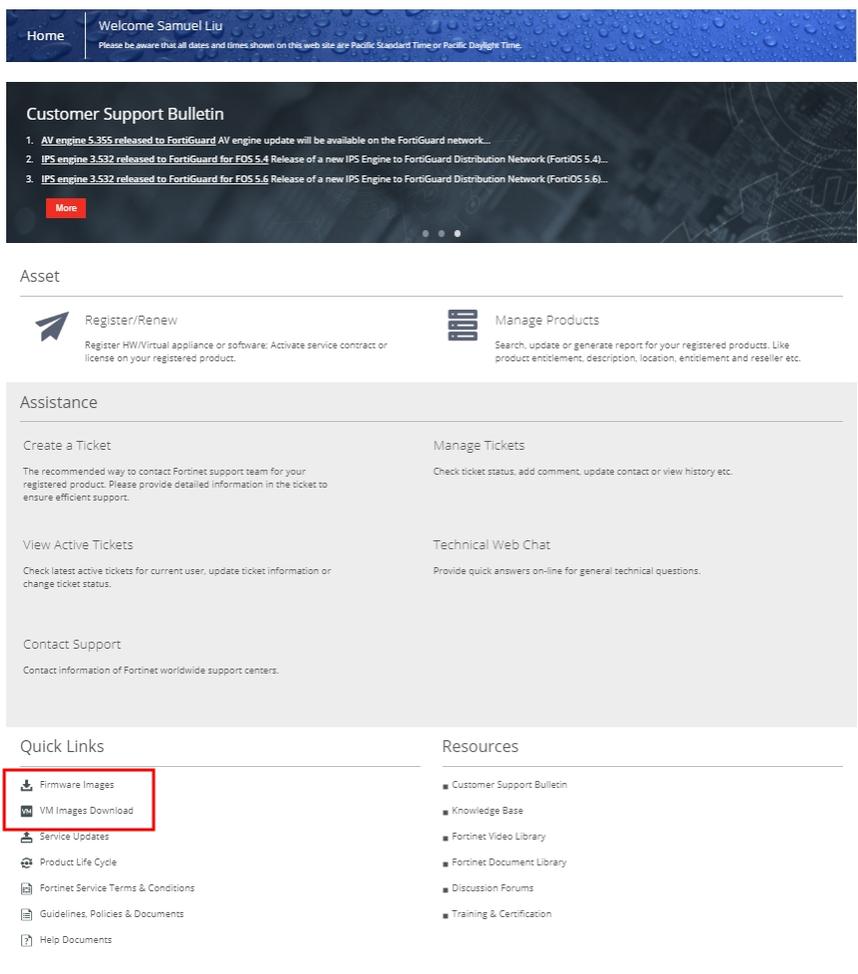
System requirements

FortiADC Manager-VM requires at least 4 GB of RAM, and 33 MB for each data disk.

FÜRTINET.