

Release Notes

FortiDeceptor 5.2.2



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



October 07, 2025

FortiDeceptor 5.2.2 Release Notes

50-522-1209108-202510DD

TABLE OF CONTENTS

Change Log	4
FortiDeceptor 5.2.2 release	5
Supported models	5
What's new in FortiDeceptor 5.2.2	5
Installation and upgrade	6
Installation information	6
Upgrade information	6
Upgrade path	6
Firmware image checksums	7
Product integration and support	8
FortiDeceptor 5.2.2 support	8

Change Log

Date	Change Description
2025-10-07	Initial release.

FortiDeceptor 5.2.2 release

This document provides information about FortiDeceptor version 5.2.2 build 0258.

Supported models

FortiDeceptor version 5.2.2 supports the following models:

FortiDeceptor	FDC-100G, FDR-100G, FDC-1000G,
FortiDeceptor VM	FDC-VM (VMware ESXi, KVM, Hyper-V, AWS, GCP, and Azure)

What's new in FortiDeceptor 5.2.2

FortiDeceptor version 5.2.2 contains bug fixes.

Installation and upgrade

Installation information

For information about initial setup of FortiDeceptor on the FortiDeceptor models , FDR-100G, FDC-1000G, see the *FortiDeceptor 1000G QuickStart Guide*.

For information about installing FortiDeceptor VM models, see the *FortiDeceptor VM Install Guide*.

All guides are available in the [Fortinet Document Library](#).

Upgrade information

Download the latest version of FortiDeceptor from the [Fortinet Customer Service & Support portal](#).

Before any firmware upgrade, save a copy of your FortiDeceptor configuration. See [Back up or restore the system configuration](#).

To upgrade the FortiDeceptor firmware:

1. Go to *Dashboard > System Information > Firmware Version*.
2. Click *[Update]*.
3. Select *Choose File*, locate the firmware image on your management computer.
4. Click *Submit* to start the upgrade.

After the upgrade is complete, you will be prompted to change your password the next time you log into FortiDeceptor.



Updating the FortiDeceptor firmware will not update the existing VM Images. However, it will re-initialize the existing Deception VMs to include bug fixes and enhancements.



Due to a higher level of password encryption introduced in version 5.2.0, users upgrading from v5.1.0 to v5.2.0 will be prompted to change their password.

Upgrade path

FortiDeceptor 5.2.2 officially supports the following upgrade path.

Upgrade from	Upgrade to
5.0.0	5.2.2
4.3.0	5.2.2
4.2.0	5.2.2
4.0.0 - 4.0.2	5.2.2

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Fortinet Customer Service & Support portal located at <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

FortiDeceptor 5.2.2 support

The following table lists FortiDeceptor 5.2.2 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Edge version 42 and later• Mozilla Firefox version 61 and later• Google Chrome version 59 and later• Opera version 54 and later• Other web browsers may function correctly but are not supported by Fortinet.
Virtualization Environment	<ul style="list-style-type: none">• AWS• Azure• GCP• Hyper-V• KVM• VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7 and 7.0.
FortiOS	<ul style="list-style-type: none">• 5.6.0 and later



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.