

Release Notes

FortiDeceptor 3.3.1



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://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



May 28, 2021

FortiDeceptor 3.3.1 Release Notes

50-331-718190-20210528

TABLE OF CONTENTS

Change Log	4
FortiDeceptor 3.3.1 release	5
Supported models	5
What's new in FortiDeceptor 3.3.1	5
Installation and upgrade	6
Installation information	6
Upgrade information	6
Firmware image checksums	6
Product integration and support	7
FortiDeceptor 3.3.1 support	7
Resolved issues	8

Change Log

Date	Change Description
2021-05-28	Initial release.

FortiDeceptor 3.3.1 release

This document provides information about FortiDeceptor version 3.3.1 build 0162.

Supported models

FortiDeceptor version 3.3.1 supports the following models:

FortiDeceptor	FDC-1000F
FortiDeceptor VM	FDC-VM (VMware ESXi and KVM)

What's new in FortiDeceptor 3.3.1

This version contains bug fixes.

Installation and upgrade

Installation information

For information about initial setup of FortiDeceptor on the FortiDeceptor 1000F model, see the *FortiDeceptor 1000F 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](#).

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.



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.

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 3.3.1 support

The following table lists FortiDeceptor 3.3.1 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">• VMware ESXi 5.1, 5.5, 6.0, 6.5, and 6.7.• KVM
FortiOS	<ul style="list-style-type: none">• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 3.3.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
710373	Deception VMs OS list disappears periodically
710329	Token improvement: Install token has more information for logon user, except deception ARP lures.
710214	Unable to install SSH token in Windows 2016 systems.
711431	SCADA V2 Deception VM: SNMP v1 does not generate any incident alerts.
709644	Authentication framework improvement for FortiDeceptor REST API to support requests from FortiGate downstream and third parties.
709347	Medical Telnet: Improve shell restriction to prevent escape commands.
710397	Improve the incident analysis module to filter out the SMB keep alive incident alerts which are triggered by the SMB lure token package deployment.
710366	FortiDeceptor should not directly query the main server. Instead, download a web filter servers list from the main server.



www.fortinet.com

Copyright© 2021 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.