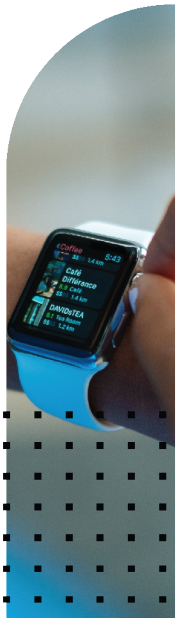
Release Notes

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

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	• 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	• VMware ESXi 5.1, 5.5, 6.0, 6.5, and 6.7. • KVM
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 3.3.1. For inquires 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	SCADAV2 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