

Release Notes

FortiDeceptor 4.0.1



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/training-certification>

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



September 23, 2021

FortiDeceptor 4.0.1 Release Notes

50-401-748976-20210923

TABLE OF CONTENTS

Change Log	4
FortiDeceptor 4.0.1 release	5
Supported models	5
Installation and upgrade	6
Installation information	6
Upgrade information	6
Firmware image checksums	6
Product integration and support	7
FortiDeceptor 4.0.1 support	7
Resolved issues	8
Known issues	9

Change Log

Date	Change Description
2021-09-23	Initial release.

FortiDeceptor 4.0.1 release

This document provides information about FortiDeceptor version 4.0.1 build 0042.

Supported models

FortiDeceptor version 4.0.1 supports the following models:

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

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 4.0.1 support

The following table lists FortiDeceptor 4.0.1 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 4.0.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
746373	Validate all system call in GUI/backend code to avoid command injection

Known issues

The following issues have been identified in version 4.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
701885	Lure Status, filter for <i>Initialize Time</i> and <i>Start time</i> need to be changed.
705485	Ensure table View Type <i>Infinite Scroll</i> and <i>Both</i> are working.
713402	Missed RDP incidents/events in FortiDeceptor which were triggered by clicking the token lure shortcut in the endpoint.
722653	Suspicious SMB requests to windows decoy machine.
733633	The <i>scdav3 ENIP</i> displays incorrect <code>deviceIp 0.0.0.0</code> .
733921	Improve the administrator page to set the timezone when creating a new user.
734861	NFR: implement UDP communication framework to handle multiple IPs in same subnet for multiple services.
734916	Issue when responding BACNET request on non-first IP among multi-IP BMS decoys.
734961	Cisco decoy can allocate itself new IPs. On telnet the IP is not detected by FortiDeceptor.
735034	FortiDeceptor does not detect interactions between ubuntu decoy and win10 endpoint.
735331	The token-SMB-mapping drive fails.
735346	The menu named <i>Customization</i> should be changed to <i>Custom Decoy</i> .
735357	Improvement: Windows RDP cannot record Administrators' commands (CMD) when using <i>Escalate Privilege</i> during attacking period.
735570	The <i>Dashboard</i> can add more than one instance of each widget when using reset-widgets.
736058	Two-event SMB incidents from decoy to domain controller are missing pcap files.
736250	Build-in fabric SSO admin profile CLI portion can select both options at the same time.
736336	IP camera <code>snmp</code> is randomly not showing all <code>snmp</code> responses, when found in PCAP.
736346	VT error results are ignored.
736556	<i>Deployment Wizard</i> , RDP service can configure the <i>Username</i> as <i>administrator</i> or <i>Administrator</i> .
736562	Deployment Wizard can choose <i>installed</i> state OS.
736629	<i>Scdav3 Siemens S7-200 PLC TFTP</i> attack on non-first-IP is detected as first IP.
736664	Attack map location by IP returns an invalid input hint.



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.