FortiDeceptor - Release Notes

Version 3.1.0

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://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 29, 2020
FortiDeceptor 3.1.0 Release Notes
50-310-631822-20200529

TABLE OF CONTENTS

Change Log **4**
FortiDeceptor 3.1.0 release **5**
Supported models 5
What’s new in FortiDeceptor 3.1.0 5
New license tool set to support CERT and CERT2 content in license file 5
FortiGuard query encryptions 5
More Decoy VM services 5
Send logs to FortiAnalyzer 5
Installation and upgrade **6**
Installation information 6
Upgrade information 6
Firmware image checksums 6
Product integration and support **7**
FortiDeceptor 3.1.0 support 7
Resolved issues **8**
Known issues **10**

Change Log

Date	Change Description
2020-05-29	Initial release.

FortiDeceptor 3.1.0 release

This document provides information about FortiDeceptor version 3.1.0 build 0056.

Supported models

FortiDeceptor version 3.1.0 supports the following models:

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

What’s new in FortiDeceptor 3.1.0

The following is a list of new features and enhancements in 3.1.0. For details, see the *FortiDeceptor Administration Guide*.

New license tool set to support CERT and CERT2 content in license file

Support CERT/CERT2 in license file and apply it for FDC communication with other products and services.

FortiGuard query encryptions

This version enhances encryption for FortiGuard queries.

More Decoy VM services

This version supports more Decoy VM services, including the following:

- FortiGate SSL VPN
- Windows Server 2016 (Standard and Datacenter edition) with MS SQL service
- Windows Server 2019 with MS SQL service

Send logs to FortiAnalyzer

You can send logs to FortiAnalyzer for further analysis. In *Log* > *Log Servers*, you can select *FortiAnalyzer* as a log *Type*.

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 3.1.0 support

The following table lists FortiDeceptor 3.1.0 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, or 6.0 and later • KVM
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 3.1.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
520908	Token installed in another user's token folder.
550574	FortiGuard Web Filter settings cannot set `address:port` as GUI page suggested.
572373	*Log > All Events* shows incorrect result from filter search date/time.
588149	Incident & campaign severity should be "higher & equal" or "lower & equal".
599896	Wrong port number shown for regrouped RDP logon failure incidents.
600930	When uploading an ISO image during customization, the *Next* button should be disabled.
604191	Subscription SKU support for customisation VM.
604194	[NFR] FortiGuard query encryptions.
604426	GUI license widget has less information than CLI counterpart.
604624	FortiDeceptor `fsuis` token does not expire after logout.
604708	[NFR]: Windows Server 2016/2019 customization support.
604787	GUI to support subscription SKU for customisation VM.
605328	IP address validation issue with whitelist, fabric integration.
605729	[NFR] Implement new license tool set to support CERT/CERT2 content in license file.
608772	Infinitely tries to initialize the decoys even if the failure is caused by license limit.
609184	NMAP port scanning gives no port information.
609479	`data-purge` command gives error message.
609684	FortiGuard cannot overwrite FDN server.
610423	GUI should warn of insufficient memory for customization.
612391	[NFR] Integrate FDC event logs with FortiAnalyzer.
613458	[NFR] MS SQL Server support along with Win Server 2016 customization.
614826	[NFR] FortiGate VPN decoy OS support.
618309	FortiDeceptor should do FortiGuard contract checking right after boot up.
623990	Apply Cus VM - check if name already exists in Deception OS.
624225	[NFR] Implement dummy lure services to listen on many popular ports.

Bug ID	Description
627076	Isniff altered Windows 10 vulnerability.
632194	Traffic capture issue.
633143	SMB - multiple PCAP events for the same PCAP file.
633656	PCAP file display and download on GUI.

Known issues

The following issues have been identified in version 3.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
549729	Login disclaimer do not apply to console/telnet/SSH.
549814	FortiDeceptor VM model does not verify if interface exists before using it.
561537	Unable to interact with SCADA modbus decoy holding register.
587850	Specific commands are not reported for SSH when using shell script.
592171	Incidents and Campaign counts has wrong display.
602146	Decoy map: customized lure is missing user info.
604427	License widget should not fuse the action of scroll and resize.
613102	Isniff uses too much resources on Linux decoy.
616774	In SSH Lure, SCP file reports incomplete events and incidents.
630855	*Log > All Events* page displays empty table after refresh.