FortiDeceptor - Release Notes

Version 3.0.0

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

FORTINET®

December 23, 2019
FortiDeceptor 3.0.0 Release Notes
50-300-601395-20191223

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-12-23	Initial release.

FortiDeceptor 3.0.0 release

This document provides information about FortiDeceptor version 3.0.0 build 0020.

Supported models

FortiDeceptor version 3.0.0 supports the following models:

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

What’s new in FortiDeceptor 3.0.0

The following is a list of new features and enhancements in 3.0.0. For details, see the *FortiDeceptor Administration Guide*.

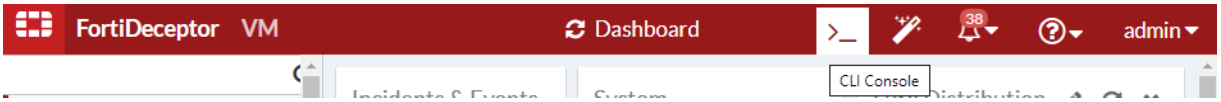
Customized Windows 10 ISO image

In this version, you can upload a Windows 10 64-bit client ISO image to FortiDeceptor and customize it as the base OS image for decoy deployment. You must have your own Windows license and purchase the FortiDeceptor customization decoy SKU (FDC-UPG-CUS).

To use this feature, go to the *Deception* > *Customisation* page.

CLI console

This version has a *CLI Console* button in the banner where you can open the CLI console in its own pane or its own window.



Filter in the Decoy Map

You can use filters in *Deception* > *Decoy Map*. The filter options are the same as the *Incident* > *Attack Map*.

You can filter by *Decoy Name*, *Decoy IP*, or *Lure Type*.

Enhanced FortiGate integration with Security Fabric

This version has options to block by severity level in the *Fabric* > *FortiGate Integration* page.

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 3.0.0 support

The following table lists FortiDeceptor 3.0.0 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 3.0.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
511045	Allow user to create and upload customized VM to FortiDeceptor.
511393	New filter design of Deception Map.
574325	Win10 VM image named as unknown.
576078	Create a CLI console on dashboard.
576087	Support incident quarantine based on user configured severity level.
582742	Quarantine Status page improvements.
584755	The fabric integration daemon always access the remote FortiGate API interface via port 443.
588730	Isniff report duplicated events.
588947	Lost latest uploaded ARAE package functionality after reboot.
589969	Ubuntu decoy with multiple network IPS reports connection closed with wrong IP address.
590227	Missing endpoints incidents in campaign - SSH decoy accesses multiple HTTP/HTTPS.
592181	Chained attack, multiple campaigns, missing correlation.
593999	No event for Windows 7 RDP logoff, and open/close port.
599152	Widget to display VM Licenses.

Known issues

The following issues have been identified in version 3.0.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
561537	Unable to interact with SCADA modbus decoy holding register.
574623	Add FortiDeceptor as fabric device on FortiGate.
593719	Incidents are correlated into two different campaigns.
600237	File system errors continue to appear on console.
600930	In customisation, while uploading an ISO image, the *Next* button should be disabled.
601796	Customization related GUI page is not read-only for read-only users.
601797	Add right-click context menu in GUI CLI console to support copy and paste.