FortiDeceptor - Release Notes

Version 3.2.0

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

October 29, 2020
FortiDeceptor 3.2.0 Release Notes
50-320-668142-20201029

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-29	Initial release.

FortiDeceptor 3.2.0 release

This document provides information about FortiDeceptor version 3.2.0 build 0096.

Supported models

FortiDeceptor version 3.2.0 supports the following models:

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

What’s new in FortiDeceptor 3.2.0

The following is a list of new features and enhancements in 3.2.0. For details, see the *FortiDeceptor Administration Guide*.

Auto deployment mechanism for deception decoy deployment

The auto deployment feature automates and simplifies decoy deployment by collecting network information regarding active assets, OS, services, and more. Understanding the network assets profile using automation provides a better deployment strategy.

Lure content learn and discovery for auto lure deployment

Auto learning features automates and simplifies lure deployment by learning the AD environment, keywords, sample organization files, and more to generate lure documents and lure configuration automatically.

FortiOS and third-party webhook

FortiOS 6.4 and later provides a feature automation which accepts webhook incoming requests and triggers different actions, so that the incoming request is forwarded to all the Fabric devices for further processing. The webhook feature supports FortiOS 6.4 and later and third-party webhooks.

Use the new GEN-WEBHOOK to integrate with third-party security tools like firewalls, AV/EDR, NAC, and more.

The current REST-API integration method is still available for backward compatibility.

Web proxy support for software download

Web proxy support includes support for FDS ARAE / IPS/AV package, web filter, deception OS image, and firmware image.

Improved lures

Added remote desktop (RDP) configuration (username, password, and IP address) to the endpoint Windows Credential Manager for luring the threat actor to engage with a Windows decoy instead of a real asset.

Added SMB network share configuration (username, password, and IP address) to the endpoint Windows Credential Manager for luring the threat actor to engage with a file server decoy instead of a real asset.

Deployment in offline or air-gapped networks

FortiDeceptor supports deployment in offline/air-gapped networks by allowing you to download and import all software components like deception OS VMs, firmware, FDS packages (IPS/AV/WEB), and licenses via the management console GUI or the support portal.

FortiDeceptor integrates with FortiManager to automatically download FDS packages (IPS/AV/WEB) using the FortiGuard override FDN configuration.

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 3.2.0 support

The following table lists FortiDeceptor 3.2.0 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 3.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
511880	NFR: Decoy Environment learning & discovery.
593881	When GUI session times out, all action should redirect to login page, not error message.
637094	Change password: Canceling redirects to admin page for user with no privilege.
637748	FortiDeceptor DMZ mode change does not write syslog.
638102	NFR: Format the display and provide download link for `tcplistener` data.
638842	NFR: Lure Content Learn and auto generator.
638846	NFR: Implement auto deployment mechanism for deception VM deployment feature.
638848	NFR: Implement new GUI page with animation to support the auto discovery/deployment feature.
639818	FortiDeceptor: Crafted username does not trigger login attempt limit.
641992	Incident Analysis event format changes on GUI.
642117	NFR: FortiOS / 3rd party blocking via webhook.
642119	NFR: GUI need to design/implement new GUI page to retrieve the input data for blocking web hook gateway.
648619	NFR: Support web proxy for external network access for firmware.
654326	CLI: Improve the `fw-upgrade` command to support downloading the VM images via HTTPS protocol.
654400	Major security exposure that allow Threat Actor to Bypass FortiDeceptor.
657746	Improve AV dump file download.
658297	Improve the Incidents View page to provide new option to review Interaction Events Only.
660645	NFR: Add *Decoy last start time* to decoy status page.
669775	NFR: Support uploading deception OS image via GUI.
669778	Improve the dashboard to avoid the long wait time when FortiDeceptor is deployed in offline network.
669783	Deployment network monitor IP address need to be verified exclusive.
670637	Readonly admin can edit/delete on lure resource page.
672189	Replace whitelist with safelist in all places.
672269	Customization page has Command Injection vulnerability.

Known issues

The following issues have been identified in version 3.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
637762	Use common date and time format in all places.
659719	Verify customized ports do not conflict with each other.
672264	Need preview of LDAP imported lure resources.
672266	Error message appears when clicking generate lure while no deception is selected.
672271	Should not allow clone decoy to have existing IP address.
672527	Improve monitor network page validation message.
671540	In Deception > Deployment Map, the *PROPOSED* decoy needs decoy reset time.
616794	NFR: Add subnet support in allowlist.
671166	Improve file drag and drop box.
643044	`tcplistener` should support dash symbol to indicate a consecutive set of ports.
672237	Error message appears when webfilter proxy setting is enabled and another setting is changed.