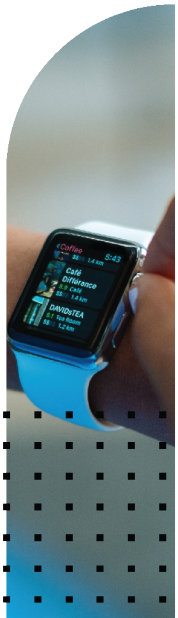
Release Notes

FortiDeceptor 3.3.0



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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 31, 2021
FortiDeceptor 3.3.0 Release Notes
50-330-692532-20210331

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-03-31	Initial release.

FortiDeceptor 3.3.0 release

This document provides information about FortiDeceptor version 3.3.0 build 0151.

Supported models

FortiDeceptor version 3.3.0 supports the following models:

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

What's new in FortiDeceptor 3.3.0

The following is a list of new features and enhancements in 3.3.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

Central Management platform

The new Central Management platform lets you centrally deploy, configure, and manage remote appliances across any IT/OT network. This single console for a distributed network that provides real-time visibility on your deception deployment includes alerting, event analysis, security reports, and logging.

More application decoys

IT- and IoT/OT-sensitive applications are always targets for threat actors and APT. Deception application decoys are a key component for detecting attacks against critical applications. This version add the following new application decoys:

- ERP Decoy hosts a web-based CRM (Customer Relationship Management platform) application.
- POS Decoy hosts a web-based POS (Point-Of-Sale software) application that allows your business to accept customer payments and keep track of sales.
- GIT Decoy hosts a web-based GIT (an open source distributed version control system) application to address attacks like the Solarwinds supply-chain.
- Medical Decoy hosts several medical application, services, and medical devices such as:
  - A web-based PACS (Picture Archiving and Communication System for medical records) server.
  - DICOM (Digital Imaging and Communications in Medicine) server for storing and transmitting medical images; and is also part of the PACS application integration.
  - Wireless Syringe Device emulation, which emulates the Medfusion 4000 Wireless Syringe device.

- SCADA Decoy (SCADAV2):
  - You can choose SCADA decoy-based profiles where you can customize the IT/OT protocols parameters.
  - New OT Decoys like Rockwell PLC and BACNET management server.
  - Software upgrade and code modification to existing OT Decoys.

SCADAV1 still exists and can be used as part of the SCADA license.

More deception lures

- Cache Credentials Lure (HoneyToken) is a fake username and password injected into a real endpoint memory to deceive attackers while using password dump tools for lateral movement. For example, tools like mimikatz and others.
- Add fake ARP entries to a real endpoint to deceive a threat actor into engaging with a decoy instead of a real asset.
- SMB lure improvement to detect ransomware attacks using a network drive based on a UNC share configuration.

Fabric pairing

You can add FortiDeceptor as a Security Fabric device on the FortiGate network topology map. FortiDeceptor will show the system info, status, and deception servers list in FortiGate.

HTTP and HTTPS service

HTTP and HTTPS services added to support web-based application decoys to detect web-application attacks more effectively.

MAC address modification

You can modify the MAC address in the decoy Deployment Wizard to improve the decoy authenticity footprint on the network.

Subnet support in Safe List

You can configure network subnet range as a Safe List configuration to have more flexibility in reducing false positive alerts from legitimate systems.

FDS update download

FDS update uses the new method by Verify FDS server with CA2 certificate and downloads packages over HTTPS protocol.

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 3.3.0 support

The following table lists FortiDeceptor 3.3.0 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, 6.0, 6.5, and 6.7. • KVM
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 3.3.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
675622	Verify `confirmation-id` to numeric characters only for Windows license confirmation over phone activation.
675747	Implement Central Management support for FortiDeceptor.
574623	Fabric Pairing - Add FortiDeceptor as fabric device on FortiGate.
675753	Prepare and publish new deception OS for medical.
675754	Prepare and publish new deception OS for POS device.
675755	Prepare and publish new deception OS for ERP device.
675750	HTTP service support on Linux.
688177	Support GIT service on Linux decoy.
686346	Support IIS server on customized Windows Server 2016/2019.
682516	Support different sets of decoy services for SCADA for different purposes.
675752	Windows deception lure redesign (SMB).
676194	Cache credential lures.
676197	Support ARP lure in lure installation on endpoint.
686345	Lure token package installer should delete itself after the installation is finished.
690707	Display token information in the deception map as previously.
655870	Verify FDS server with CA2 certificate and download packages over HTTPS protocol.
675751	MAC address modification in deploy wizard GUI.
676043	For the new security compliance, use the domain in the URL to access new VM image server.
616794	Add subnet support in Safe List.
700966	VNC icon should be disabled for built-in decoy images.
684100	Add a new Type level to incident alert.
691043	Out-of-bounds array indexing in system-install.
691044	Race condition vulnerability in command shell.
691052	Uncontrolled resource consumption (unauthenticated denial of service) in login module.
700707	Increase the default HDD size for FortiDeceptor VM model from 200GB to 500GB.

Bug ID	Description
704731	Disable or set as readonly the deception menu on client appliances.
703937	Email does not work on the relay server that is restricted to verifying the host name in EHLO command.
701901	Decoy deploy stuck in starting status when decoy number reaches the limit and all the decoys try to launch.
702308	Decoy template can be saved many times.
672826	Improve performance of CLI data-purge command.
704681	Lure generator does not use the given user names.
706619	Lure generator does not use the user imported resource file.
684102	Default admin user cannot update the trusted host configuration.
675622	Verify confirmation-id to numeric characters only.
576167	`dcimg-status` should show uninitialized deception OS.
685536	System time change affects Windows variety decoy keepalive functionality.
523262	Static mode all IP addresses of gateway and IP range should be in the same subnet of selected monitor VLAN or subnet.
698087	Provide download button for the imported LDAP users.
659719	Verify that custom ports do not conflict with each other.
675241	Deception OS page shows empty list on bootup even after proper network configuration.
702318	When overwrite is not enabled, allow overwrite server address to be empty.
704023	CM Manager should show CM related info in secure Fabric widget.
681427	When deception OS does not have a license, the deployed decoy cannot be deleted.
681894	Command injection vulnerability caused by call function in subprocess.
683253	Software version tracking.
677286	Vulnerability for FortiDeceptor GUI.
707651	Import lure user from LDAP page needs to provide CA certificate dropdown list, not text field.
707304	Force refresh whole page or logout session when switching mode.
703864	Analysis-Export to PDF download failed / content overflow.
685336	Remote admin user auth test mixed with local trusthost verification.
706621	The hostname generated by automated lure process should be valid.
707285	RDP and SMB detection issues with Cus Win join AD.
707327	Ubuntu Samba service: the event operation type needs to be more specific.

Known issues

The following issues have been identified in version 3.3.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
704628	Update automation integration with FortiOS to use the new Fabric Connector Event trigger.
706752	Attack map timeline doesn’t show present day new attack.
706736	Attack map, attack line color, and number issue.
704411	Attack map new decoy incident VS deleted decoy incident issue.
705597	Provide warning message when user enters meaningless settings in the deployment wizard.
706460	Deployment map - lure is missing info.
706111	AD users cannot access RDP.
704521	RDP doesn’t report delete directory events.
638855	Data storage management for both database and HDD raw files.
700971	Credential lure generation doesn't follow imported credentials format.
700956	Lure generation doesn't follow the same file type of the assigned tag.
706951	Improve the restriction access for all sub URL based on some profiles.
637762	Use common date and time format in all places.
708988	Improve the CM manager to support firmware image download for different models.

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.