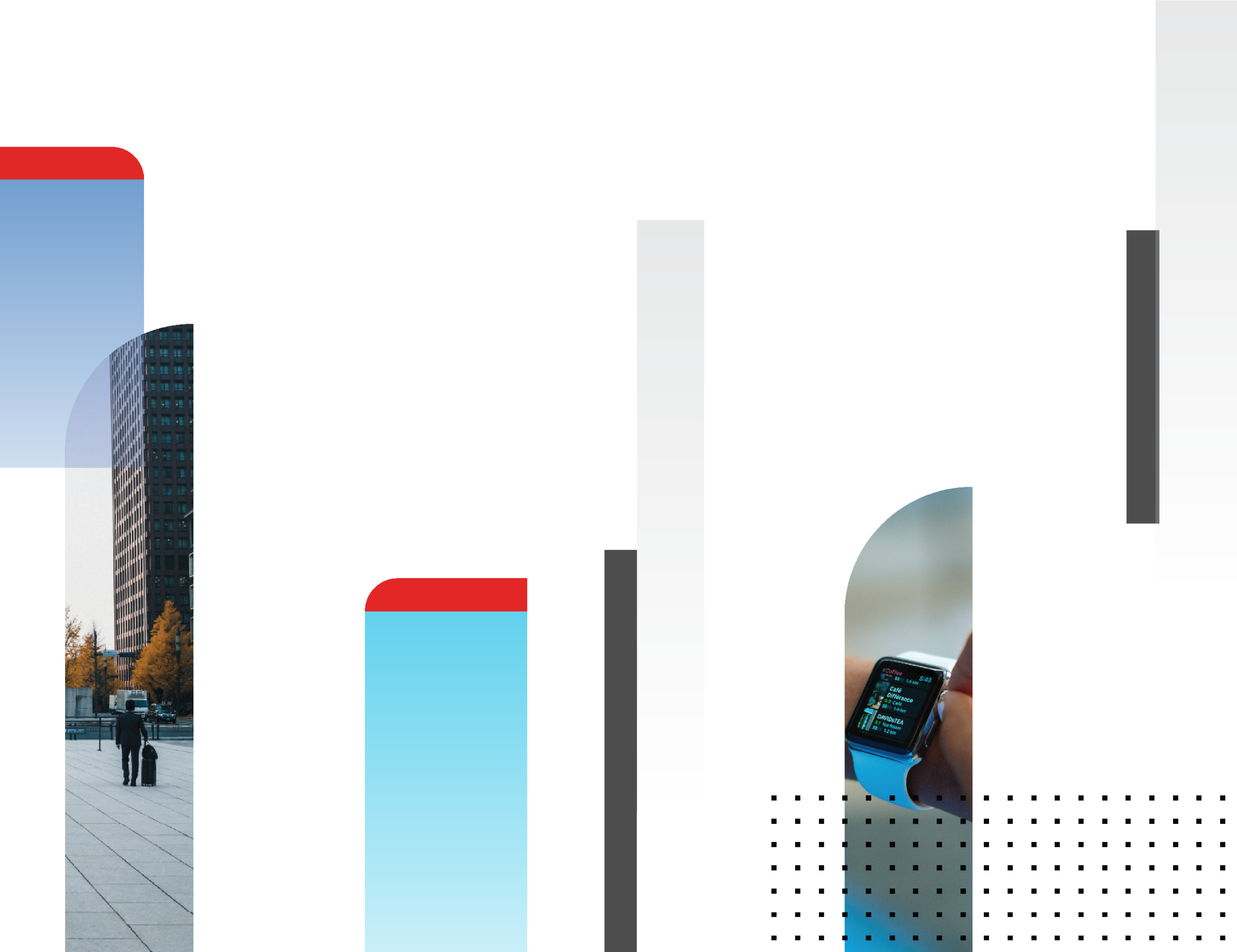
Release Notes

FortiDeceptor 4.1.0



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/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

December 16, 2021
FortiDeceptor 4.1.0 Release Notes
50-410-765215-20211216

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-12-16	Initial release.

FortiDeceptor 4.1.0 release

This document provides information about FortiDeceptor version 4.1.0 build 0128.

Supported models

FortiDeceptor version 4.1.0 supports the following models:

FortiDeceptor	FDC-1000F
FortiDeceptor VM	FDC-VM (VMware ESXi, AWS, KVM, GCP, and Azure)

What's new in FortiDeceptor 4.1.0

The following is a list of new features and enhancements in 4.1.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

Incident Alerts Reporting & Email Alerts:

- FortiDeceptor manager email module will allow you to send incident alerts using email:
  - To several recipients
  - Based on a specific incident alerts parameter
  - Based on several incident alerts parameters
- FortiDeceptor manager will allows you to export incident alerts to a CSV format as an additional option to the current PDF.

New Infrastructure Decoys:

The massive migration in recent years by organizations to move networks, servers, applications, and data into the cloud expand the attack surface. A full-stack deception solution requires providing network visibility coverage for hybrid networks. FortiDeceptor Cloud appliance will support all the three major public clouds:

- AWS
- AZURE
- GCP

New IT & Application Decoys:

IT Sensitive applications are always targets for threat actors and APT. Deception application Decoys are a key component for detecting attacks against critical applications. The following bew Application Decoys were added:

- SAP Decoys that emulate the essential components of SAP that are exposed to end-users and represent the SAP attack surface. SAP decoys:
  - SAP Router decoy
  - SAP Dispatcher decoy
  - SAP ICM (WebUI/HANA) decoy
- Linux Decoy:
  - Linux is a core platform in the new data center. To better mimic the network infrastructure, we expanded the FortiDeceptor offering and added a New Linux Decoy, CentOS 7.9.
  - In addition, the kernel module for Linux decoy was improved to monitor the file operations and dump the changed files.

New IoT/OT Application Decoys:

- New IoT decoys:
  - Expanded the printer decoy by adding more printer vendors likes Brother MFC and Lexmark.
  - Expanded the network IoT decoy by adding a TPLink WIFI router modem.
- New SCADA decoy (SCADAV3):
  - The ever-growing number of smart sensors is driving the increased focus on cybersecurity for smart buildings. We expanded the BMS decoys and added more sensors from the leading vendor Tridium, Niagara AX Station and Niagara4 Station decoys as part of our deception offering.
  - A new OT Decoy emulates an uninterruptable power supply (UPS) unit, Liebert Spruce UPS.
  - Expanded the Rockwell OT Decoy by adding two more decoys, Rockwell 1769-L16ER/B LOGIX5316ER and Rockwell 1769-L35E Ethernet Port.
  - Expanded the Schneider Electric OT Decoy by adding another decoy, PowerLogic ION7650.

New Deception Tokens

- An ODBC driver uses Microsoft's Open Database Connectivity (ODBC) interface that allows applications to access data in database management systems (DBMS) using SQL as a standard for accessing the data. The ODBC Lure will add a fake DB connector that will deceive the threat actor into engaging with an IT decoy running a fake SQL DB instance.
- The new SAP Token adds a fake "SAP Logon" file under the SAP

New Fabric Integrations:

- An ODBC driver uses Microsoft's Open Database Connectivity (ODBC) interface that allows applications to access data in database management systems (DBMS) using SQL as a standard for accessing the data. The ODBC Lure will add a fake DB connector that will deceive the threat actor into engaging with an IT decoy running a fake SQL DB instance.
- New SAP Token that will add a fake "SAP Logon" file under the SAP software installation directory contains fake SAP information regarding SAP application servers and SAP router. This fake information will deceive the threat actor into engaging with SAP decoys running fake SAP components.

Decoy Fingerprint detection

A threat actor that will use ICMP protocol (ping) for active reconnaissance that is not supposed to trigger any security alerts will be detected by the FortiDeceptor decoys that will detect ICMP protocol (ping) active probing.

Network segmentation protection:

A threat actor that engages with a decoy with several network segment connections might use the decoy interfaces to move between the network VLANs. The network connection management will enforce a policy route engine that allows the threat actor to access (inbound/outbound) only the network used to connect with the decoy. For the rest of the decoy networks, we will allow ping only.

Data-purge improvement:

Data purge has been improved and now supports periodic data purges in addition to the current manual mode. This feature avaiable from the CLI.

FortiDeceptor Virtual Appliance health-check:

FortiDeceptor Virtual Appliance requires six network interfaces to operate correctly. The new health check logic will alert the you if the FortiDeceptor Virtual Appliance has less than six interfaces.

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 4.1.0 support

The following table lists FortiDeceptor 4.1.0 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, 6.0, 6.5, and 6.7. • KVM • AWS • GCP • Azure
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 4.1.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
734861	NFR: Implement UDP communication framework to handle multiple IP in same subnet for multiple services
735346	The menu called Customization should be change to Custom Decoy
738879	Need @/\ support when enter Administrator name to support latest FAC v6.4.0
738880	NFR: Implement kernel module for Linux decoy to monitor the file operations and dump the changed files
739123	NFR: Support ODBC lures for token package
739179	NFR: Implement network connection management for TCPv4, TCPv6, UDP and layer 2 traffic
739599	NFR: Support Ping alerts detection in Windows/Ubuntu decoys
740836	NFR: Implement the transparent layer 2 traffic proxy
741500	NFR: Implement the FDCLinuxTracer to monitor the file changes and dump the modified files
750245	Popup warning message when user try to edit the interface for port2-port8
753096	Restrict the deploy monitor IP/subnet to be not in same subnet for all appliances in same CM system
753203	GUI priviledge control not working as expected
755660	Dump all the files(<50M) for SMB/RDP/SSH service on windows/linux, regardless of the file type,
756765	B0042: FDN update failed via override server
756882	Disable the tunnel/none-interactive command support for SSH in Ubuntu and CentOS
756951	The expired Add-on license on FDC1KF cause the system require new license for upload
758400	Reset the decoy/connection if the remote user get admin/root privilege.
758604	Provide new rest API for FGT side to download the decoy information
759026	Token - limit the number of lures for each type when execute token installation
759087	Token - ARP lures cannot be installed by logon user
760903	Web Filter Error update process
764832	FDC Integration with PAN

Bug ID	Description
765671	Support PEM format for user provided certificate

Known issues

The following issues have been identified in version 4.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
682479	NFR: support 2FA authentication for radius.
759738	NFR: Support 2 DNS IP in decoy.
747321	NFR: Import and support pallas ML engine for malware static analysis.
763249	NFR: Provide GUI page to input the activation ID instead of `dcvm-confirm-id` CLI
761308	Multiple new decoys MAC OUI doesn't match manufacturer.
762469	Send `smb` attack to Centos, incident display logon twice, first time logon via "IPC$".
735955	Sort Appliance and deployment network in Deployment map.
767034	Avoid using system popup window.
765724	Dashboard: Widgets do not record widget edit actions in syslog.
758384	Firmware upgrade needs confirmation from user and show a response.
753189	Inconsistent widget info in different models.
760707	*replace _openssl* library in *pypsexe* by *libssl.so* of our system.
765605	Linux Tracer should add *mtime* to file operation logs.

FORTINET®

www.fortinet.com