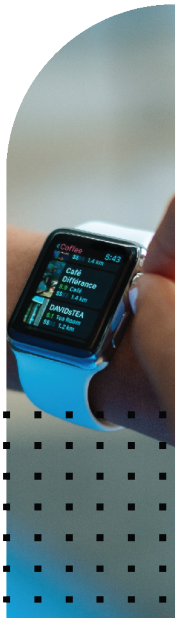
Release Notes

FortiDeceptor 4.0.0



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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July 30, 2021
FortiDeceptor 4.0.0 Release Notes
50-400-733528-20210730

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-28	Initial release.

FortiDeceptor 4.0.0 release

This document provides information about FortiDeceptor version 4.0.0 build 0038.

Supported models

FortiDeceptor version 4.0.0 supports the following models:

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

What's new in FortiDeceptor 4.0.0

The following is a list of new features and enhancements in 4.0.0. For details, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

New IoT/OT Decoys

IoT/OT devices are consistent targets for threat actors and APT. Deception Decoys are a key component for detecting attacks against critical devices and infrastructure.

A new IoT Deception VM has been added and contains a:

- **Cisco router** decoy that will allow using a cisco IOS image file to emulate a real cisco router device
- **Network printer decoy** will emulate a real HP printer, including the printing protocol and printer web management UI.
- **Network IP camera** that will emulate a real IP camera with the ability to custom the fake video stream.

New OT protocols & decoys were added to SCADAV2 Deception VM:

- **Protocol**:
  - **DNP3** is a communications protocol used in SCADA and remote monitoring. Its primary use is in utilities such as electric and water companies.
  - **Triconex** protocol is both the name of a Schneider Electric brand that supplies products, systems, and services for safety, critical control, and turbomachinery applications and the name of its hardware devices that utilize its TriStation application software. The Triconex Decoy service will simulate SIS controllers.
- **New Schneider Electric OT Decoys**:
  - **EcoStruxure B.M.S. Management Server**: EcoStruxure Building Management is an integration platform for monitoring, control, and management of energy, lighting, fire safety, security, and HVAC
  - **PM5560 Power Meter**: PM5560 provides the measurement capabilities needed to allocate energy usage, perform tenant metering and sub-billing, pinpoint energy savings, and perform a high-level assessment of the

power quality of the electrical network.
- **SCADAPack 333E (5210)**: Smart RTU ensures end-to-end reliable and secure control and monitoring of remote assets in critical infrastructure. (mainly used for water system monitoring).

New Deception Lures

HoneyDocs (office & PDF files): HoneyDoc creates a "honey" document, including fake passwords or financial data, to look appealing for attackers to open them. It uses pixel technology as the tracking image so that you can see the IPs of who opens the document in your web server logs inside the network decoy.

Network Attacks:

- **Responder Attack Detection**: A new module for detecting Responder attacks is included in the Windows Decoys. Responder is a powerful tool for quickly gaining credentials and possibly even remote system access. It uses an LLMNR, NBT-NS & MDNS poisoner that is easy to use and very effective against vulnerable networks.
- **Ransomware Attack Detection**: An improvement for the current Ransomware encryption detection module to minimize the detection time.

In-Depth Malware Analysis – Incident Analysis:

FortiSandbox: The integration between FortiDeceptor and FortiSandbox will provide a complete static and dynamic analysis against malicious code captured by the network decoys. The malware analysis report will be available on the FortiDeceptor admin console.

VirusTotal: The integration between FortiDeceptor and the well-known VirusTotal service allows the submission of suspicious files (MD5) for malware analysis. When integrated, VirusTotal detection ratios will be displayed in the incident analysis alert Workflow for relevant events.

Fabric Integration:

- **FGT CSF**: The integration between FortiDeceptor and Fortigate over CSF allows FortiDeceptor to automatticlay trigger the isolation of the infected endpoint from the network and prevents the attack from moving laterally. The CSF provides access to more fabric devices for isolations like FortiSwitch through the Fortigate. In addition, we add SAML support between Fortigate WEB-UI to FortiDeceptor to allow SSO login from Fortigate to FortiDeceptor.
- **FortiNAC**: The integration between FortiDeceptor and FortiNAC allows FortiDeceptor to automatically isolate the infected endpoint from the network and prevent the attack from moving laterally. (in the previous version of FortiDeceptor, we use the WEB-HOOK connector for the integration, and now we provide an out-of-the-box connector).

System Features

- **Platform Scalability**: The platform scalability was improved by adding a Support for 24 IP addresses per Deception VM instead of 16 IP addresses. (FDC Appliance will support up to 128 VLANs)
- **Improved Decoy Network authenticity**:
  - **STATIC IP**: A network Decoy with STATIC IP deployment will generate a single NIC per IP address.
  - **DHCP IP**: A network Decoy with DHCP IP deployment will allow choosing more than 1 IP address per Decoy.
- **HW requirements benchmark widget**: New HW requirements benchmark widget for FortiDeceptor Virtual appliance only will provide the end-user guidelines in real-time regarding the system performance and the need for more vCPU & RAM resources during deployment and ongoing maintenance.

- **Additional improvements to current features such as:**
  - Time Zone for each login user based on his location to adjust the incident alerts time and date.
  - Improved CM manager to support firmware image download for different models
  - Improved incidents alerts email content

FortiDeceptor License Model:

- **New License Model**: The new FortiDeceptor license will be a subscription-based model. The new model is based on the number of network VLANs using the FortiDeceptor solution.
- **FortiDeceptor VM**: A subscription bundle based on the number of network VLANs that includes all the FortiDeceptor modules and features (Network Decoys, Deception Lures, Forticare, and ARAE).
- **FortiDeceptor HW**: A subscription license based on the number of network VLANs and includes the FortiDeceptor modules and features(Network Decoys, Deception Lures, and ARAE).
- **FortiDeceptor Manage**r: A subscription license for managing up to 50 devices using a single manager.
- **FortiDeceptor Windows license:**
  - Not included under the subscription license and requires a separate SKU.
  - New SKU for 1 X win7 and 1 X win10 to purchase mixed windows decoys under a single SKU.
  - The subscription license allows access to the custom decoy feature, and you can use your corporate windows license for windows decoys.
- **FortiDeceptor License renewal**: The perpetual license will be supported for current customers and renewal using the perpetual SKUs and co-term contract.
- **FortiDeceptor USG license** for US Federal customers.

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 4.0.0 support

The following table lists FortiDeceptor 4.0.0 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, 6.0, 6.5, and 6.7. • KVM
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in version 4.0.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
549814	FortiDeceptor VM model does not verify that the interface exists before using it.
638855	NFR: FortiDeceptor data storage management for both database and HDD raw files.
675746	NFR: Implement new hardware model FDC-1000G.
700956	The Lures generator does not use the same file type of the assigned tag.
700971	The Lure generation credentials do not 't follow the imported credentials format.
701059	NFR: Implement SAML Single-Sign-On for *Fabric Pairing*.
704628	NFR: FortiDeceptor should update its automation integration with FortiOS to use the new *Fabric Connector Event* trigger.
706907	*Admin-Admin profile-user* with *None* access can still get data and change the admin dashboard layout.
708988	Improve the CM manager to support firmware images downloaded for different models.
709347	Medical telnet: Use the restricted shell to prevent the user from using the dangerous commands such as `ssh`.
709635	NFR: FDC new license model support.
709636	NFR: FDC new VM series license support.
709638	NFR: FDC new VLAN license support.
709640	NFR: Support 1 STATIC/DHCP IP for each NIC in decoys.
710329	Token improvement: Install token information as much as possible for logon user only except ARP lures.
710366	FortiDeceptor should not directly query the main server. Instead, download a Web-Filter servers list from main server.
710397	NFR: Improve the incident analysis system to filter out the SMB incidents which are triggered by lure token package.
711038	Ransomware Detector Update.
711043	NFR: New deception OS for *Printer Decoy*.
711052	NFR: New deception OS for CISCO decoy
711053	NFR: New deception OS for IP Camera.
711056	NFR: New honey doc token for PDF lure files.

Bug ID	Description
711058	NFR: New honey doc token for DOCX lure files.
711064	NFR: Add *Time Zone* for each login user to provide the incidents based on user location.
711065	NFR: Integrate with FSA to get more detail forensic result for dumped files.
711066	NFR: Integrate with Virus Total to get further scan results.
711068	NFR: Fabric integration with FortiNAC.
711089	NFR: New deception lure service of active NetBios Name Service in windows decoys
713597	The highlight the *Delete* request in ERP/POS/Medical web service.
714333	NFR: Implement SCADA powermeter decoy set with DNP support.
714866	Improve the CM appliance configuration tabs.
715716	The pcap file does not get purged after several days.
715764	Windows d*ecoy-SMB token-installation* process stalls when there are network issues.
717590	NFR: New license support in autodeployment.
718809	NFR: Implement new logic for ransomware detection.
719130	NFR: rebuild the deception base OS image for Win7X86.
720165	NFR: FDCVM model - The GUI in the dashboard needs to provide the recommended decoy instance number based on the configured vCPU/RAM.
720981	FortiDeceptor - Potential unsafe calls to `system()` in CLI code
720987	Potential unsafe calls to `system()` in CLI code.
722411	NFR: Support the automated replacement for deception image among versions
725844	Limit the SSO user privilege on FortiDeceptor.
726289	Deploying tokens using AD GPO logon script issues.
727165	NFR: Support USG mode in FortiDeceptor.
728233	Remove redundant system logs while the downstream FortiDeceptor is waiting for upstream authorization.
729042	Filter out the file event of `.zone.indentifier`.
730057	Radius users with *ReadOnly* profiles have a few non-ReadOnly privileges.
730291	Client fails to get *Deception OS* if Manager don't have
730610	Improve the pcap dumper to only save the TCP/UDP traffic to reduce the pcap file size.
731535	Improve the *Lure* generator to allocate part of the username for each service.
733513	FortiDeceptor - [FortiDeceptor] OS command injection.
733588	Remove *AV Scan Result* field from PCAP file.

Bug ID	Description
733610	FortiDeceptor - [FortiDeceptor] OS command injection.
733676	*Manager* should only allow deployment to *Appliance* when status is *Approved*.
733695	The *Incident* type should be set as *Infection* when the dumped file is a virus.
733754	The GUI in the FortiGuard page Web Filter override is not working.
733845	FortiDeceptor - [FortiDeceptor] OS command injection.
734319	Update the FortiDeceptor VM model template to increase the CPU/Memory.
735603	FGT decoy/VM container can only support 10 nic, and cannot support FDC 24 dhcp mode.
735638	The `ssh Ubuntu decoy, isniffer` does not catch any traffic.

Known issues

The following issues have been identified in version 4.0.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
701885	Lure Status, filter for *Initialize Time* and *Start time* need to be changed.
705485	Ensure table View Type *Infinite Scroll* and *Both* are working.
713402	Missed RDP incidents/events in FortiDeceptor which were triggered by clicking the token lure shortcut in the endpoint.
722653	Suspicious SMB requests to windows decoy machine.
733633	The *scadav3 ENIP* displays incorrect `deviceIp 0.0.0.0`.
733921	Improve the administrator page to set the timezone when creating a new user.
734861	NFR: implement UDP communication framework to handle multiple IPs in same subnet for multiple services.
734916	Issue when responding BACNET request on non-first IP among multi-IP BMS decoys.
734961	Cisco decoy can allocate itself new IPs. On telnet the IP is not detected by FortiDeceptor.
735034	FortiDeceptor does not detect interactions between ubuntu decoy and win10 endpoint.
735331	The token-SMB-mapping drive fails.
735346	The menu named *Customization* should be changed to *Custom Decoy*.
735357	Improvement: Windows RDP cannot record Administrators' commands (CMD) when using *Escalate Privilege* during attacking period.
735570	The *Dashboard* can add more than one instance of each widget when using reset-widgets.
736058	Two-event SMB incidents from decoy to domain controller are missing pcap files.
736250	Build-in fabric SSO admin profile CLI portion can select both options at the same time.
736336	IP camera `snmp` is randomly not showing all `snmp` responses, when found in PCAP.
736346	VT error results are ignored.
736556	*Deployment Wizard*, *RDP* service can configure the *Username* as *administrator* or *Administrator*.
736562	Deployment Wizard can choose *installed* state OS.
736629	*Scadav3 Siemens S7-200 PLC TFTP* attack on non-first-IP is detected as first IP.
736664	Attack map location by IP returns an invalid input hint.

www.fortinet.com