FortiDeceptor - Release Notes

Version 2.1.0

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/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

July 30, 2019
FortiDeceptor 2.1.0 Release Notes
50-200-548414-20190730

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-07-30	Initial release of FortiDeceptor 2.1.0.

FortiDeceptor 2.1.0 release

This document provides information about FortiDeceptor version 2.1.0 build 0142.

Supported models

FortiDeceptor version 2.1.0 supports the following models:

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

What’s new in FortiDeceptor 2.1.0

The following is a list of new features and enhancements in 2.1.0. For details, see the *FortiDeceptor Administration Guide*:

Navigation Menu

FortiDeceptor 2.1.0 provides two quick access menus labeled *Admin Guide* and *Release Notes* on the navigation bar for users to access the related documents from the Fortinet global website.

Dashboard

In FortiDeceptor 2.1.0, the *System Information* widget in the dashboard indicates when new firmware images and deception OS images are available. A blinking button labeled *UPDATE AVAILABLE* will be displayed in the *Firmware Version* row if there are updated files for firmware, and a similar button will be displayed in the *Deception OS* row if there are updates for deception OS.

Deployment Wizard

In FortiDeceptor 2.1.0, a new option called *Reset Decoy VM* is provided to allow the decoys to be reset automatically at a specific time after incidents are detected. *Reset Interval* specifies the number of seconds for the interval.

Analysis

In FortiDeceptor 2.1.0, the result table of the *Analysis* menu provides two options for user to quickly filter out two special types of events. *IPS Events Only* is for displaying the events captured by IPS signatures, and *Web Filter Events Only* is for displaying the events captured by the Web Filter feature.

IOC Export

FortiDeceptor 2.1.0 provides one more method to integrate with third-party products. This feature will export the incidents in a specific time range, along with MD5 files, the Web Filter category, with or without reconnaissance alerts in CSV format.

Read Only Admin Profile

FortiDeceptor 2.1.0 supports a read-only administration profile for main features, which allows the administrators to create the users with read-only permission to most of the web pages and CLI commands.

CLI commands

FortiDeceptor 2.1.0 provides a data purge command to purge the events and incidents in the database.

New Deception OS images

FortiDeceptor 2.1.0 now supports two more deception OS images *scadav1* and *win10v1*. These two image files can be triggered to download and install automatically via the GUI page *Deception OS's*.

The *scadav1* supports many OT services HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, Guardian-AST, IEC 60870-5-104, and the *win10v1* supports RDP / SMB.

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 2.1.0 support

The following table lists FortiDeceptor 2.1.0 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, or 6.0 and later • KVM
FortiOS	• 5.6.0 and later

Resolved issues

The following issues have been fixed in FortiDeceptor 2.1.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
0508165	Allow client to create template from deception VM
0526112	Support Read-Only administrative rights in the admin profiles
0559625	Support an option for customers to reset the DCVM immediately once the incidents are detected
0559675	Implement the simulator server for IEC 60870-5-104 protocol
0560549	Export IOCs from FortiDeceptor in CSV format
0568234	Implement the firmware image auto upgrade
0511926	Create deception image upgrade module
0562372	Prepare and release SCADA base image
0562383	Prepare and release Windows 10 base image
0560127	Implement CLI command to purge all DATABASE records
0569466	Add links to Admin Guide and Release Notes to top bar
0555665	XSS vulnerability in Customized Widget Title of the Dashboard web page
0555667	XSS vulnerability in Profile Name of Admin Profile web page
0555669	XSS vulnerability in Common Name and Distinguished Name of LDAP Servers web page
0555673	XSS vulnerability in Email Account and Receiver List of Mails Servers web page
0555674	XSS vulnerability in field Name of Deploy Wizard web page
0556970	Insecure Direct Object Reference vulnerability for the Super Admin
0556971	Insecure Direct Object Reference vulnerability in the FortiDeceptor table customization
0556973	Insecure Direct Object Reference privilege escalation to changing password of another account
0565161	FortiDeceptor reports false alarm SMB incidents
0558993	Deception VMs generate false events by generating traffic to the internet
0558998	Incident and attack map records all connections on the network interface whether the traffic is destined for Deception VM or Not
0566892	Without interaction, Windows Decoy receives traffic from external IP address and Decoy VM reported as Victim
0557758	Unable to create VM's user account if the account already exists

Bug ID	Description
0566890	Trying to access the file share will result in to incidents with no info
0567197	The incident was reported with reversed attacker IP + PORT and victim IP + PORT
0567191	Default Attack map filter doesn’t reflect the recent incidents on the attack map
0550367	Admin without administrative privileges can upgrade firmware through hidden page in the GUI
0571831	Edit administrator failed unless reset password
0566802	Rename Deception Technology terms in PPT/docs
0559677	GUI relabeling
0556008	Need to improve the GUI display for some basic information on incident table
0523123	Change monitored deception IP needs redo conflict validation and initialization
0545885	The input fields for Fabric settings should be sanitized properly before saving into a configuration file

Known issues

The following issues have been identified in FortiDeceptor 2.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
0548404	Log processor incident regroup logic should be improved
0561537	Unable to interact with SCADA modbus decoy holding register
0514085	Inconsistency between document, GUI description and real implementation on hostname
0561967	DHCP related issues
0548927	When some fabric blockers are disabled, test block shows error result
0547396	Whitelist IP and Port should avoid 0 and 255
0548938	Token installed on Ubuntu endpoint has user permission issue
0556634	Unable to change the Password if the current password is empty / blank
0564603	Can not add multiple ports in white list
0532607	Deception VM should use accepted dhcp offer as VM IP
0559506	Wrong incident sequence in IPS event, such as open port is reported after the IPS attack
0570776	The IP address displayed on GUI does not match the IP of interface in Win10 with DHCP mode