



# FortiDeceptor - Release Notes

Version 1.0.1

**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 COOKBOOK**

<https://cookbook.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: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



October 31, 2018

FortiDeceptor 1.0.1 Release Notes

50-100-519860-20181031

# TABLE OF CONTENTS

<b>FortiDeceptor 1.0.1 Release</b>	<b>4</b>
Supported models	4
Main Features	4
Dashboard Summary	4
Deception	4
Incident	5
Network	5
System	5
Log	5
<b>Installation and Upgrade</b>	<b>6</b>
Installation Information	6
Upgrade Information	6
Firmware Image Checksums	6
<b>Product Integration and Support</b>	<b>7</b>
FortiDeceptor 1.0.1 support	7
<b>Resolved Issues</b>	<b>8</b>
<b>Known Issues</b>	<b>9</b>
<b>Change Log</b>	<b>10</b>

# FortiDeceptor 1.0.1 Release

This document provides information about FortiDeceptor version 1.0.1 build 0012.

This section includes the following topics:

- [Supported models on page 4](#)
- [Main Features on page 4](#)

## Supported models

FortiDeceptor version 1.0.1 supports the following models:

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

## Main Features

The core features of FortiDeceptor 1.0.1 include the following:

### Dashboard Summary

The System Status dashboard displays widgets that provide Deception VM distribution, high level Incident and Event information and enable you to configure some basic system settings.

### Deception

The *Deception* menu contains views that allow you to deploy and monitor Deception VMs on your network. These are:

- Deception Images  
The *Deception Images* view displays Windows and Linux VM Images that you can use for creating Deception VMs.
- Monitored Network  
The *Monitored Network* view allows administrators to set up a monitoring interface into a VLAN or a subnet.
- Deploy Wizard  
The *Deploy Wizard* allows you create and deploy Deception VMs on your network.
- Deception Status  
The *Deception Status* view shows the status of the decoys deployed on your network, and allows you to view, start, stop, delete, and download token packages as well as test an attack.

- Deception Map  
The *Deception Map* view is a visual representation of the entire network that shows Deception VMs, Decoys, Tokens and Incidents.
- Whitelist  
The *Whitelist* view is used to add an IP address that can be used by an administrator to log on to the network.

## Incident

The *Incident Menu* provides an analysis of the detections by deception VMs. Review in the GUI or export to PDF. This includes:

- Analysis  
The *Analysis* view lists the Event related incidents detected by FortiDeceptor, and allows you view the entire timeline of the events.
- Campaign  
The *Campaign* view lists the Attack related events detected by FortiDeceptor and the full timeline of the attack.
- Attack Map  
The *Attack Map* view is a visual representation of the entire network showing the Deception VMs, attackers, victims, and ongoing attacks.

## Network

The *Network* menu provides interface, System DNS, and routing management options.

## System

The *System Menu* provides views for adding Administrators, Admin Profiles, Certificates, LDAP and RADIUS servers, Mail Servers, SNMP, and other setting configurations.

## Log

The *Log* menu provides views for All Events and the ability to add Log Servers.

# 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 update 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 1.0.1 support

The following table lists FortiDeceptor 1.0.1 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Edge version 42 and later</li><li>• Mozilla Firefox version 61 and later</li><li>• Google Chrome version 59 and later</li><li>• Opera version 54 and later</li><li>• Other web browsers may function correctly, but are not supported by Fortinet.</li></ul>
<b>Virtualization Environment</b>	<ul style="list-style-type: none"><li>• VMware ESXi 5.1, 5.5, or 6.0 and later</li><li>• KVM</li></ul>

# Resolved Issues

The following issues have been fixed in 1.0.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
510280	The 'Attacker IP Mask' is replaced by 'Source IP' unexpectedly in the report of campaign.
510574	There is 'None' in Campaign report.
510812	Failed to install token packages if the related decoys contain long sharename for SMB/SAMBA service.
510865	CLI command <code>dcvm-status</code> cannot list those deceptions which are failed to initialize.
511326	The order of Windows VM activation log is improper.
512269	Implement CLI command to display the status of deception images.
512568	The <code>show</code> command only displays 6 interfaces for FDC1000F.
514080	System Super-admin privilege was granted after change the password of non-super-admin admin user.
514786	System Non-super-admin should not be able to create super-admin or admin profile beyond it's own privilege.
516075	Add VNC to Deception Status grid.
516124	System Deception VM deployment failed when some IPs in the range are in use.
516365	Decoy SSH user should not obtain root privilege.
516818	Missing port3 in system routing page.
520417	Alert email detail message needs to improve.
521494	Event time difference incorrectly represented in Incident Detail for event count > 50.

# Known Issues

The following issues have been identified in FortiDeceptor 1.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
509403	B0001: Better save the filtering value in the input.
509409	B0001: Better keep current settings when loading filtering result in the deception map.
510104	[Filters] Column Filter Validations.
510114	The pop-up <i>This program might not have installed correctly</i> is shown when uninstalling a token.
510592	B0001: Customized table settings cannot be restored.
518982	Missing logout log after session idle timeout.
521479	0007: The SMB share path were displayed improperly.

# Change Log

Date	Change Description
2018-10-31	Initial release of FortiDeceptor 1.0.1.



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.