FORTINET

Release Notes

FortiNDR 7.0.2

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

August 10, 2022
FortiNDR 7.0.2 Release Notes
55-701-832250-20220810

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-08-10	Initial release.

Introduction

FortiNDR (formerly FortiAI) is the first Fortinet Network Detection and Response product from Fortinet. Apart from the Virtual Security Analyst™ with high-velocity malware detection technology based on neural networks, FortiNDR is built on FortiAI's technology, extended and added features to detect Network Anomalies with auto and manual mitigation techniques.

Licensing and Upgrade information

FortiNDR requires a new SKU to enable FortiGuard downloads and lookups. The new SKUs available are:

Model	SKU	Description
FortiNDR-3500F	FNR-3500F	FortiNDR-3500F appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 2 x 10Gb GE Copper (supports 10/1000/10000 without transceivers), 2x 1 Gigabit Ethernet connection (management).
	FNR-3500F-BDL-331-DD	Hardware plus 24x7 FortiCare, with NDR and ANN engine updates & baseline.
	FC3-10-AIVMS-461-02-DD	Subscriptions license for FortiNDR-VM (16 CPU) with 24x7 FortiCare with NDR and ANN engine updates & baseline
	FC4-10-AIVMS-461-02-DD	Subscriptions license for FortiNDR-VM (32 CPU) with 24x7 FortiCare with NDR and ANN engine updates & baseline

Customers need to have the correct SKU for NDR functionalities to work. If customers are running FortiAI VMs on v1.5.x versions, please follow upgrade information below.

For customers running FortiAI v1.5.x and would like to enjoy FortiNDR features, a co-term upgrade is necessary. Please contact customer services at cs@fortinet.com.

FortiNDR v7.0.0 will use a new license file (than 1.5.x), therefore customers upgrading from 1.5.x should:

1. Prepare v7.0 license file via co-term upgrade.
2. Upgrade the VM/hardware.
3. Load the new license file into unit with the GUI.

If a new v7.0 license file is loaded on a 1.5.x VM, the VM will become non-functional. This does not apply to FAI-3500F hardware.

Upgrade information

Due to some database changes, after upgrade from 7.0.0 to 7.0.2, users will need to execute a CLI to clean up historical NDR log entries. Note this will clear all NDR logs, but malware logs will remain.

```
execute cleanup ndr
```

- Always back up configuration before upgrade.
- Upgrade from v1.5.x and 7.0 beta 1&2 to v7.0.2 GA is supported.

- To upgrade the hardware or VM, please follow the procedures below:
  - Backup the configuration and take a note of version prior to upgrade.
  - Before upgrading the license from FortiAI VM v1.5.x to FortiNDR VM v7.0.2, you will need to download and apply the v7 firmware to the VM first. You have two options for applying the new FortiNDR contract:
    - **i.** (For VM and HW) You can register the new contract at https://suppport.fortinet.com as a renewal/upgrade for the existing contract/serial number. The existing license will automatically get the updated entitlement information from FDS.
    - **ii.** (For VM only) You can register the new contract code as a new device and get a new license and serial number. Then you can download the new license file (.lic format), and load the new license in the GUI (go to *System* > *FortiGuard*). After you download the license, you will now have a FortiAI VM license in addition to a FortiNDR VM license.

A FortiNDR license CANNOT be loaded to a FortiAI VM. The upgrade must be done first otherwise it might cause FortiAI VM to become inaccessible.

Downgrade from v7.0.1 is NOT supported, so please backup configuration before upgrade.

FortiNDR version 7.0.2

This document provides information about FortiNDR version 7.0.2 build 0021.

These Release Notes include the following topics:

New features and enhancements

FortiNDR detects anomalies using a variety of methods, such as FortiGuard feeds like IPS, botnet IP and DNS DB, as well as added features such as IOC campaign lookup, vulnerable protocols and weak ciphers detection. Apart from detecting protocols like FortiOS NGFW, FortiNDR also looks into the behavior of devices & users, such as FTP download, or SMB copy.

CLI

- The new *diagnose debug icap* command will display most recent ICAP file event and related error messages from FortiNDR's ICAP Server. For information see,FortiNDRCLI Reference Guide.

System integration and support

The following integration is tested and supported in FortiNDR 7.0.2.

- While FOS 6.2 and 5.6 file submission with OFTP, via the FortiSandbox field, is tested and compatible, official support for submitting files is in FOS 6.4.0 and higher.
- HTTP2 file submission from FortiGate 7.2.0
- FortiGate inline blocking (with AV profile) is supported in FOS 7.0.1 and higher.
- FortiAnalyzer integration is supported in FortiAnalyzer 7.0.1 and higher.
- FortiSIEM integration is supported in FortiSIEM 6.3.0 and higher.
- FortiSandbox integration (API submission from FortiSandbox to FortiNDR) is supported from FortiSandbox 4.0.1 and higher.
- FortiGate quarantine via webhook 6.4.0 and higher.
- FortiMail 7.2.0
- ICAP is supported for:
  - FortiGate 6.4.0 and higher.
  - FortiWeb 6.3.11 and higher.
  - Squid and other compatible ICAP clients.
  - FortiProxy 7.0.0.
  - FortiNAC quarantine support (v9.2.2+)
  - FortiSwitch quarantine via FortiLink (FortiSwitch v7.0.0+ and FortiGate v7.0.5+)

FortiNDR 7.0.1 supports sending both malware and NDR logs to FortiAnalyzer and FortiSIEM or other syslog devices

Supported models

FortiNDR version 7.0.2 supports the following models:

- FortiNDR-3500F (same model as FortiAI-3500F)
- FortiNDR VM 16 & 32 (supports upgrade from FortiAI VM16 & 32)
- FortiNDR KVM (supports upgrade from FortiAI KVM)
- FortiNDR on AWS (BYOL)

Resolved issues

The following issues have been fixed in version 7.0.2. For inquires about a particular bug, contact Customer Service & Support.

Bug ID	Description
801356	Some filters are not working as expected in the Malware Log and NDR log,
828125	FortiNDR incorrectly reports downloader as *Clean*.
828787	Network Detection misses logs.
828942	FortiNDR uses MD5 hash to index scan jobs.

Known issues

The following issues have been identified in version 7.0.2. For inquires about a particular bug or to report a bug, you can ask in beta forums on FNDN

www.fortinet.com