SECURITY MANAGEMENT

FortiMonitor Release Notes

VERSION 2.0.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, October 19, 2016

FortiMonitor 2.0.2 Release Notes

1st Edition

TABLE OF CONTENTS

Introduction

This document provides installation instructions and caveats, resolved issues, and known issues for FortiMonitor 2.0.2, build 0046.

FortiMonitor is Fortinet's unified risk management platform. It allows you to collect, analyze, and act on vulnerability and threat data from a diverse set of devices and network resources. It includes the following key features:

- **Asset management** – FortiMonitor lets you monitor security events by asset, including individual hosts and host groups, websites, and network segments.
- **Event normalization/standardization** – FortiMonitor collects security logs from devices that have different manufacturers and log formats. After it collects the original logs, FortiMonitor uses knowledgebase definitions to normalize them as security events.

  FortiMonitor can parse and normalize any logs from user-defined data sources that use the syslog message standard.
- **Scan management** – FortiMonitor can use scan services provided by third-party devices to perform web and system scans, and host, service, or defacement detection. FortiMonitor normalizes any detected vulnerabilities and performs cross-correlation to calculate their reliability. An additional cross-correlation feature relates these vulnerabilities to attack events from devices such as intrusion defense systems (IDS), intrusion prevention systems (IPS), and web application firewalls (WAF).
- **Correlation analysis** – FortiMonitor provides four types of data correlation: inventory correlation, asset correlation, logical correlation, and cross-correlation. You can use the web UI to customize the policy for all the correlation types, and create custom logical correlation rules and import them into FortiMonitor.
- **Machine Learning** – FortiMonitor's machine learning technology detects hosts infected by bots by performing an in-depth analysis of the traffic logs of requested domains.

  FortiMonitor provides two algorithms to detect hosts infected by bots based on the black list that the Fortinet data center provides: Bayesian Algorithm and C&C Server List. The Bayesian algorithm training tasks can generate models to use in Bayesian Algorithm prediction tasks, which predict infected hosts. The C&C Sever List algorithm detects the infected hosts using the black list directly.
- **KRI (Key Risk Indicator)** – FortiMonitor makes a Security Assessment based on a KRI (Key Risk Indicator). FortiMonitor calculates KRIs for diverse targets (such as overall network, region, host group, host, and website) based on the risk of security events and vulnerabilities. It then uses KRI values to generate the hierarchical security risk indicator system with multiple dimensions (asset vulnerability indicator, threat growth indicator, security threat indicator, and so on). You can also use the web UI to view the events that contribute to the KRI in detail ("drill down" feature).
- **Risk Calculation** – FortiMonitor can periodically calculate risk for all assets based on factors such as the reliability or severity of an event or vulnerability, and the value of an asset.
- **Reporting** – You can use FortiMonitor to generate flexible, customized reports.

For additional documentation, please visit:

http://docs.fortinet.com/fortimonitor/

What's new

This release of FortiMonitor includes the following enhanced features:

- FortiMonitor will be renamed to FortiAnalyzer—Big Data in a future release.
- **Dashboard** – You can now define new dashboard panels for any data source or edit a predefined panel.
- **Events** – You can now order events by time by clicking the Event Time field in the query list.
- **User-defined collector** – For each device category, FortiMonitor now supports a default parser for unmatched logs.
- **Analysis engine** – Report, KRI alert, action filter and query conditions now allow you to filter using "Is not null", "Is null", "Not in". Additional predefined reports are available.
- **Machine Learning** – The Bayesian Algorithm now includes default parameters.
- **Backup** – You can now remove data from the DB table directly. In addition, you can back up the Ticket table.
- **System monitor** – You can now monitor system status information (such as CPU and disk usage) for all FortiMonitor server blades via SNMP.

Monitor settings and browser support

- **Monitor settings for web UI access** – To view all objects in the web UI properly, set your monitor to a screen resolution of 1280x1024.
- **Web browser support** – The FortiMonitor web UI supports the following web browsers:
  - Internet Explorer 7.x, 8.x, 9.x, 10.x, 11.x
  - Firefox 4.x/5.0
  - Chrome 4x.x

Supported security devices

FortiMonitor allows you to define your own data sources for any logs sent by syslog.

You can also configure FortiMonitor 2.0.2 to receive attack and other data from the following predefined devices:

Vendor	Device	Version	Log protocol	Log type
Fortinet	FortiGate	4.0/5.0/5.2	Syslog	All log types
	FortiGate	5.0, build 3343	Syslog	NAT PBA
	FortiDB	5.1.4	FTP	Audit/Alert
	FortiDB	5.1.0, build 1130	Syslog & FTP	Audit/Alert
	FortiMail	5.2	Syslog	All log types
	FortiWeb	4.3/4.4	Syslog	Attack/Traffic/Event
NSFocus	NSFocus NIDS1200B	5.6.6.164	Syslog	IPS
Symantec	Symantec SEP	12.1	Syslog	Virus
Venustech	Venus	4A	Syslog	Audit 4A
CNGate	CNGate-NGIPS	5.4	Syslog	IPS

Supported scanners

You can configure FortiMonitor 2.0.2 to manage and receive data from the following vulnerability scanners:

- DBAPPSecurity 4.0.4.30
- IBM AppScan Enterprise 8.70.0.0 (Chinese version only)
- Knownsec 4.x
- Nessus 5.x, 6.3, 6.4, 6.5
- NSFocus RSAS-E 5.0, RSAS-M-S 5.0
- RJ-iTop 3.0.8.0
- WebRavor NWRPC 2013

Hardware support

FortiMonitor 2.0.2 supports the following hardware platforms:

- FortiMonitor 3000D

Upgrade instructions

This is a minor release of FortiMonitor.

To upgrade from an earlier version of FortiMonitor, you download new firmware files and then execute an upgrade on each server blade individually. For detailed firmware installation instructions, see the *FortiMonitor Handbook*.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Resolved issues

Bug ID	Description
374426	Router event type is incorrect for FortiGate 5.0-5.2
374456	URL normalizer fails for illegal URL
374692	Redefine predefined report 9005001 as 9005016
374698	Modify TunnelID from int to bigint in TB_OrgEvent_VPN and TB_OrgEvent_VPN_Back tables
375311	Large amount of data causes a Machine Learning training task to fail
378538	Cannot click the original event URL in ticket info correctly
378020	Analysis engine does not calculate weeks correctly