FortiSIEM Release Notes

VERSION 5.0.1

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

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

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

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

5/24/2018

FortiSIEM 5.0.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-23	Initial version of FortiSIEM 5.0.1 Release notes.

Introduction

FortiSIEM provides an all-in-one, seamlessly integrated and service-oriented IT infrastructure monitoring solution that covers performance, availability, change, and security monitoring aspects of network devices, servers, and applications.

This document provides a list of resolved issues and enhancements in FortiSIEM 5.0.1 Release.

What's new in 5.0.1

FortiSIEM 5.0.1 release includes the New Features and Enhancements described below.

If you are upgrading from FortiSIEM 4.1.0, refer to *'What's New in 5.0.0'* for more information about the features in 5.0.0.

New Features

- Windows Agent 2.2
- ServiceNow Event Management Integration

Windows Agent 2.2

Windows Agent 2.2 feature includes the following changes:

a. Additional parsing of Windows DNS logs to include Source IP, Destination Name, Destination IP, Destination Canonical Name and Received Bytes.
   - Source IP – name resolution requestor
   - Destination Name and IP – resolved name and IP
   - Destination Canonical Name – CNAME of the resolved entity
   - Received Bytes – bytes in the DNS response

b. Avoid Agent Configuration loss at Windows Agent Manager during Agent upgrade.

c. Automatic clean-up of `.SVC` files when it reaches a certain size.

d. Do not erase log file after Agent restart.

e. Monitor encrypted USB disks.

f. Agent to perform SSL certificate checks.

g. Flush log files during file rotation of a monitored file.

ServiceNow Event Management Integration

FortiSIEM Incidents can now be pushed to ServiceNow Event Management tables via the FortiSIEM integration framework. For more details about ServiceNow Event Management, see here.

Enhancements

FortiSIEM 5.0.1 release includes the following enhancements:

- The `phoenix_config.txt` merge upgrade process is improved - The `phoenix_config.txt` file on Supervisor and Worker stores system level configurations. In earlier releases, during the upgrade process, user is asked to merge the `phoenix_config.txt` file from the new release with the `phoenix_config.txt` file existing on the system. In this release, this process is simplified as follows:
  - User is never asked to merge `phoenix_config.txt` files.

- The existing `phoenix_config.txt` file is backed up to: `/opt/phoenix/config/phoenix_config.txt.<ver>`
  For example: `/opt/phoenix/config/phoenix_config.txt 5.0.0.1201`
- Selected entries from the existing `phoenix_config.txt` file are picked up to create the `phoenix_config.txt` file used by the system and stored in `/opt/phoenix/config/phoenix_config.txt`
- User can examine the difference between the `phoenix_config.txt` files and modify the system `phoenix_config.txt` file if needed.

The following sections are merged from the existing `phoenix_config.txt` file:

Global	• cainfo • agent_key • agent_cert • ccm_ftp_directory • avaya_sftp_directory
phParser	• airline_sls_directory • airline_sls_directory_high • airline_thread • incoming_log_cfg
phEventForwarder	• tls_certificate_file • tls_key_file • tls_certificate_file • tls_key_file
phQueryWorker	• max_num_thread_per_task • phReportMaster section • num_merge_threads
Kafka	• thread_num
Elasticsearch	• Entire Elasticsearch section, if configured.

- Incident > Remediation – **Enforce On** and **Run On** fields are automatically populated based on Incident Reporting Device and Incident Target. Remediation Scripts are scoped down based on the **Enforced On** device type. Remediation results are shown on the Remediation page.
- Flex GUI is now disabled by default. You can turn on the Flex GUI by setting `Enable_Flex_UI = true` in `phoenix_config.txt` on Supervisor.

Resolved Issues

The following table shows the bug fixes and enhancements in FortiSIEM 5.0.1 release.

Id	Severity	Component	Description
484380	Major	App Server	Remediation script does not work when the script runs from Collector.
487654	Major	Report	Baseline Report Successful User Logon Profile runs only for Super and not for organization.
487774	Major	Rule	UEBA Location anomaly incident is not triggered for Cloud User for login events.
487777	Major	Identity & Location	Identity User and Location dashboard does not show Cloud Users.
487979	Major	GUI	Dashboards XML exported from Super/Global will reference customer ids in the `dataParam` attribute.
482142	Minor	GUI	HTML5 UI displays html tag in raw message as in html format in Search results.
482521	Minor	App Server	Large number of unmanaged devices can cause performance issues.
482530	Minor	Data	Generic devices are incorrectly grouped under Server Group.
482731	Minor	Device Support	FireAMP rules do not trigger.
483831	Minor	GUI	Incident Search is not working correctly when Function is used along with other Search criteria.
483855	Minor	System	Office 365 monitoring may fail after a while, because of unnecessary files being saved in the directory.
483883	Minor	App Server	Log discovered Cisco Meraki AP devices fail to merge with SNMP discovered Meraki AP causing duplicate devices in CMDB.
483931	Minor	App Server	Rule function may not be saved – hence associated incidents do not show up under Security Incidents.

Id	Severity	Component	Description
484255	Minor	GUI	HTML5 GUI doesn't allow saving new report definition based off an existing report.
484267	Minor	GUI	When the user modifies the incident list view by adding a column, user's custom view with added column is not saved.
484978	Minor	App Server	Incident user search may not retrieve all results.
486366	Minor	App Server	IP insertion to CMDB may fail for large CMDBs.
486510	Minor	System	Errors due to long URIs in REST API calls.
488595	Minor	GUI	Some user settings are not saved in HTML5 GUI.
489194	Minor	App Server	Device Network Interface REST API is slow for large CMDB.
489544	Minor	GUI	Custom rules created in Organizations different than Super/Local may not trigger.
489646	Minor	GUI	CMDB drill down on device to Analytics uses Host IP instead of Reporting IP.
491184	Minor	Parser	Parser creates excessive internal logs when CMDB filter is defined.
460147	Enhancement	Device Support	Add Juniper JunOS SNMP Sysobject Ids to facilitate discovery.
469388	Enhancement	Device Support	Enhance Unix parser to parse Unix password change event.
469645	Enhancement	Device Support	Azure VM deployed from new portal cannot be discovered.
470727	Enhancement	Device Support	Enhance Cisco Ironport Web Parser to include request and response sizes.
472246	Enhancement	Device Support	Support complete FortiMail discovery and performance monitoring.
472580	Enhancement	Device Support	Support CrowdStrike events via CEF.
480492	Enhancement	Parser	FortiGate KVM VM events are not parsed due to device ID in different format.
482317	Enhancement	Device Support	Add new CEF parser forBit9 CarbonBlack.
483073	Enhancement	App Server	Increase Radius authentication timeout for external authentication to succeed.

Id	Severity	Component	Description
483849	Enhancement	GUI	Allow user to enter Google Map Key since the default account has access count limitations.
483862	Enhancement	GUI	Remediation Enhancements – automatically choose **Enforce on**, **Run On** and show remediation results.
486246	Enhancement	App Server	Allow Notification e-mail to contain Incident ID but without link.
486625	Enhancement	System	Upgrade JDK from JDK8u162 to JDK8u172 for security fixes.
486917	Enhancement	GUI	Eliminate unnecessary GUI pop ups.
489026	Enhancement	System	Change Data Manager 'File Remove Failure' log message severity from Error to Warning as we force the removal when it fails the first time.