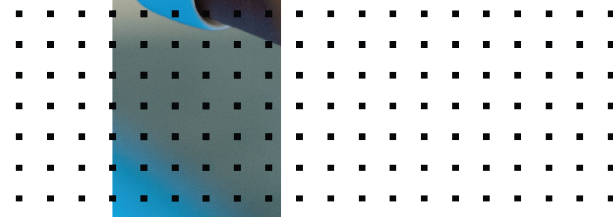
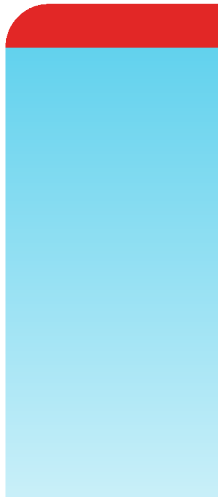


Release Notes

FortiSIEM 6.4.1



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 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



10/25/2022

FortiSIEM 6.4.1 Release Notes

TABLE OF CONTENTS

- Change Log** **4**
- What's New in 6.4.1** **5**
 - Bug Fixes and Minor Enhancements 5
 - System Upgrades 6
 - Known Issues 6
 - Policy Based Retention for EventDB 6
 - Shutting Down Hardware 7
 - Elasticsearch Based Deployments Terms Query Limit 7

Change Log

Date	Change Description
05/23/2022	Initial version of FortiSIEM 6.4.1 Release Notes.
08/15/2022	Known issue added.
10/25/2022	Known issue added.

What's New in 6.4.1

This document describes the additions for FortiSIEM 6.4.1 release.

- [Bug Fixes and Minor Enhancements](#)
- [System Upgrades](#)
- [Known Issues](#)

Bug Fixes and Minor Enhancements

Bug ID	Severity	Module	Description
774397	Major	Data Manager	Event files upload to Elasticsearch is slow for Organizations with large org Id.
789843	Major	Performance Monitor	Fail to get running-config from Cisco IOS devices.
788814	Minor	Agent Manager	phAgentManager process may crash if Cisco FireAMP event pulling job does not return expected value.
788034	Minor	Agent Manager	Collector may not efficiently get WMI event log if some of the Windows servers are down.
757413	Minor	Agent Manager	phAgentManager process may crash to handle some Cisco Firepower IPS events.
795273	Minor	Agent Monitor	Enabling an AWS Cloudwatch pull event may cause phAgentManager to crash on collector.
801278	Minor	App Server	The LOW and HIGH watermark log delay events (PH_DEV_MON_LOG_DEVICE_DELAY_LOW and PH_DEV_MON_LOG_DEVICE_DELAY_HIGH) are not generated reliably.
794338	Minor	App Server	New Dashboards created in Global Dashboard no longer appear after a couple of hours.
791114	Minor	App Server	ServiceNow Device Outbound Integration may fail if Installed Software Date was NULL.
782304	Minor	App Server	User with a cloned "Full Admin" role with Data Conditions defined cannot search for rules in RESOURCES > Rules.
776214	Minor	App Server	Searching currently Active Incidents generated many months ago fails in INCIDENTS > Search.
785547	Minor	Data	The ADMIN > Health > Cloud Health page sometimes times out after upgrade to 6.4.0, if there are many workers.

Bug ID	Severity	Module	Description
779548	Minor	Data Purger	phDataPurger incorrectly counts master nodes as hot nodes in AWS-managed Elasticsearch.
791321	Minor	Data Purger	Data Purger needs to handle error 404 when trying to purge non-existent ES indices.
780688	Minor	GUI	Sometimes, the user cannot reset their own password because of internal errors.
776295	Minor	GUI	GUI shows "Undefined" error when the user attempts to set a new password for a user created with the "Password Reset" field set.
784026	Minor	Parser	phParser may sometimes crash to handle some events.
776350	Minor	Parser	External protocol error (PH_PARSER_INVALID_EXT_LOG_PROTO) from collectors occurs when OMI was configured.
769414	Minor	QueryMaster	phQueryMaster memory usage increases when FortiSIEM collects performance metrics for a large number of devices when they are all included in the Summary dashboard. This summary data is held in memory and needs to be more aggressively purged.
793805	Enhancement	App Server	Handling of Task Rest API results in excessive PostgreSQL accesses causing App Server performance issues.
790052	Enhancement	Parser	Increase the number of concurrent TLS connections handled by Parser module for syslog over TLS.

System Upgrades

- Upgrade to Rocky Linux 8.5 with patches released on March 30, 2022.
(<https://lists.resf.org/archives/list/rocky-announce@lists.resf.org/thread/H7FNZZUZQ7B2XEEOPIXPZVIMQNO6KTE2/>)

Known Issues

Policy Based Retention for EventDB

Currently, Policy based retention for EventDB does not cover two event categories: (a) System events with phCustId = 0, e.g. a FortiSIEM External Integration Error, FortiSIEM process crash etc., and (b) Super/Global customer audit events with phCustId = 3, e.g. audit log generated from a Super/Global user running an adhoc query. These events are purged when disk usage reaches high watermark.

Shutting Down Hardware

On hardware appliances running FortiSIEM 6.6.0 or earlier, FortiSIEM `execute shutdown` CLI does not work correctly. Please use the Linux `shutdown` command instead.

Elasticsearch Based Deployments Terms Query Limit

In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

The workaround is to change the "max_terms_count" setting for each event index. Fortinet has tested up to 1 million entries. The query response time will be proportional to the size of the group.

Case 1. For already existing indices, issue the REST API call to update the setting

```
PUT fortisiem-event-*/_settings
{
  "index" : {
    "max_terms_count" : "1000000"
  }
}
```

Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

1. `cd /opt/phoenix/config/elastic/7.7`
2. Add "index.max_terms_count": 1000000 (including quotations) to the "settings" section of the fortisiem-event-template.

Example:

```
...
"settings": {
  "index.max_terms_count": 1000000,
  ...
}
```

3. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.
4. Test new indices have the updated terms limit by executing the following simple REST API call.

```
GET fortisiem-event-*/_settings
```



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.