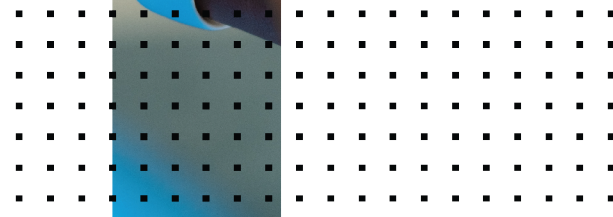
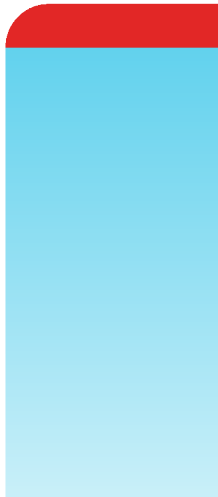


# Release Notes

## FortiSIEM 6.4.0



**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](mailto:techdoc@fortinet.com)



10/25/2022

FortiSIEM 6.4.0 Release Notes

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>What's New in 6.4.0</b>	<b>5</b>
New Features	5
Migration from CentOS 8 to Rocky Linux	5
Lookup Table JOIN for Advanced Analytics	5
Content Upgrade Framework via FortiGuard Service	6
Agent and Collector Upgrade from Supervisor	6
Native FortiSOAR Integration	7
Link Graph Based Visualization	7
Trusted Hosts for GUI Login	7
Key Enhancements	7
Elasticsearch Integration Enhancements	8
Windows Agent 4.2.0	8
Collector Cache Usage Visibility	8
OAuth based SMTP Authentication	8
NFS Version Auto-Negotiation Enabled by Default for FortiSIEM EventDB	9
Install and Upgrade Logging Enhancements	9
System Upgrade	9
HDFS Integration Enhancements	9
New Device Support	9
Bug Fixes and Minor Enhancements	9
Rule and Report Modifications since 6.3.3	15
Known Issues	17

# Change Log

Date	Change Description
01/18/2022	Initial version of FortiSIEM 6.4.0 Release Notes.
01/21/2022	Native FortiSOAR Integration, NFS Version Auto-Negotiation Enabled by Default for FortiSIEM EventDBand and Known Issues sections updated.
03/02/2022	Known Issue added.
03/15/2022	Known issues added.
03/16/2022	Known issue added.
05/12/2022	Known issue added.
07/19/2022	Known Issue added to 6.4.0 Release Notes.
08/09/2022	Elasticsearch Integration Enhancements section updated. Elasticsearch 7.17.3 supported.
08/15/2022	Known issue added.
10/25/2022	Known issue added.

# What's New in 6.4.0

This document describes the additions for FortiSIEM 6.4.0 release.

- [New Features](#)
- [Key Enhancements](#)
- [New Device Support](#)
- [Bug Fixes and Minor Enhancements](#)
- [Rule and Report Modifications since 6.3.3](#)
- [Known Issues](#)

## New Features

- [Migration from CentOS 8 to Rocky Linux](#)
- [Lookup Table JOIN for Advanced Analytics](#)
- [Content Upgrade Framework via FortiGuard Service](#)
- [Agent and Collector Upgrade from Supervisor](#)
- [Native FortiSOAR Integration](#)
- [Link Graph Based Visualization](#)
- [Trusted Hosts for GUI Login](#)

## Migration from CentOS 8 to Rocky Linux

FortiSIEM 6.4.0 and later releases will run on Rocky Linux since CentOS 8 reached End Of Life on December 31, 2021. Fresh 6.4.0 installations will run on Rocky Linux. There are no special upgrade procedures for existing customers running older FortiSIEM 6.x versions. A regular 6.4.0 upgrade will replace CentOS 8 binaries with appropriate Rocky Linux binaries.

## Lookup Table JOIN for Advanced Analytics

This release enables users to define Lookup tables and then write rules and reports by joining event database and Lookup tables. Lookup tables can be created manually, via API or by running a CMDb or Event report on FortiSIEM. Lookup tables can contain meta data not present in events. The ability to join events with Lookup tables enables many threat hunting use cases, for example:

- look up of new processes, ports, external domains not seen in last 2 days
- look up for user logins not seen in last 2 days
- look up for VPN logins from IP addresses or countries not seen in last 2 days

Lookup tables can be used in Analytical searches and Rules. However, if you are running Elasticsearch for Online event database, then Lookup tables cannot be used in searches, but Rules still can use Lookup tables.

For details on creating Lookup tables, see [Adding Lookup Tables](#) in [Lookup Tables](#).

For details on creating Lookup tables via API, see [Lookup Table Integration](#) in the Integration API Guide.

For details in using Lookup tables in rules and reports, see `LookupTableHas` and `LookupTableGet` in [Examples of Expressions](#).

Several pre-built Lookup tables and rules using these Lookup tables are defined. See Added Rules under [Rule and Report Modifications since 6.3.3](#).

## Content Upgrade Framework via FortiGuard Service

Currently, new FortiSIEM content such as device support via parsers, rules, and reports have to wait for a new FortiSIEM release. This release provides a content update framework that can be separate from the software releases. Periodically, new FortiSIEM content will be published to FortiGuard. FortiSIEM customers with a valid Support license can download the new content, which will then be automatically deployed to Supervisor and Workers. In this release, the user has to manually deploy to all Collectors from the **ADMIN > Health > Collector Health** page.

New content covers additions or modifications to device types, event attributes and groups, parsers, rules, reports, dashboard and Fortinet Geo database.

A content update versioning scheme is deployed to keep track of updates. FortiSIEM 6.4.0 release starts with Content update version 100, which will monotonically increase with future releases.

For details on how to download and apply new content, see [Content Update](#).

**Note:** For this feature to work

1. You need to allow port 443 connection from the Supervisor to `update.fortiguard.net`.
2. A valid FortiSIEM Support License.
3. FortiSIEM Supervisor, Workers, Collectors must be on 6.4.0 or higher.

## Agent and Collector Upgrade from Supervisor

This release enables FortiSIEM Windows Agents, Linux Agents and Collectors to be upgraded from the Supervisor node. Furthermore, up to 10 entities can be upgraded in parallel.

For details on Windows Agent upgrades, see [here](#).

For details on Linux Agent upgrades, see [here](#).

For details on Collector upgrades, see [here](#).

**Notes:**

- For Collector upgrade, the **Supervisor Name** field defined in the FortiSIEM GUI located at **ADMIN > License > Nodes** must be an IP address or a FQDN that is resolvable by the Collector.
- For this feature to work, you need to allow port 443 connection from the Supervisor to `update.fortiguard.net`. Supervisor communicates with FortiGuard to download valid image hashes. FortiSIEM compares the hash and allows upgrade to proceed if the hashes match.

This feature works with the following versions:

- FortiSIEM Supervisor (and Workers) must be 6.4.0 or higher
- FortiSIEM Windows Agent must be 4.2.0 or higher

- FortiSIEM Linux Agents must be 6.4.0 or higher
- FortiSIEM Collectors can be on 6.1.0 or higher

## Native FortiSOAR Integration

Users can now run FortiSOAR Playbooks and Connectors directly from the FortiSIEM GUI. FortiSIEM will [execute Playbooks](#) and [run Connectors](#) on FortiSOAR and display the results in the FortiSIEM GUI in easy to understand terms.

For details on running Playbooks, see [Playbooks](#).

For details on running Connectors, see [Connectors](#).

For details on how to create Playbooks optimized for FortiSIEM, see [Writing FortiSIEM Compatible FortiSOAR Playbooks](#) in the Appendix.

The following sample playbooks are available - see [FortiSOAR-FortiSIEM-Playbooks.json](#).


- Playbook for getting IP address reputation via VirusTotal
- Playbook for getting Domain reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid, Alienvault OTX
- Playbook for getting URL reputation via VirusTotal, Anomali, FortiGuard, MX Toolbox, URLVoid
- Playbook for getting file hash reputation via VirusTotal

## Link Graph Based Visualization

You can now visualize the search results using link graphs. A link graph shows relationships between a Source node, an Event Node and a Destination Node. You can see the relationship by mapping search result columns to link graph nodes.

For details, see [Link Graph](#) in [FortiSIEM Charts and Views](#).

## Trusted Hosts for GUI Login

You can restrict GUI Login by defining a set of IP addresses in **ADMIN > Settings > System > Trusted Hosts**. If the field is empty, then GUI login from any IP addresses is allowed. However once defined, new logins are disallowed from IP addresses outside of the defined range. Existing logins are not affected. However, you can force a logout from the  icon in the GUI.

For details, see [here](#).

## Key Enhancements

- [Elasticsearch Integration Enhancements](#)
- [Windows Agent 4.2.0](#)
- [Collector Cache Usage Visibility](#)
- [OAuth based SMTP Authentication](#)
- [NFS Version Auto-Negotiation Enabled by Default for FortiSIEM EventDB](#)

- [Install and Upgrade Logging Enhancements](#)
- [System Upgrade](#)
- [HDFS Integration Enhancements](#)

## Elasticsearch Integration Enhancements

This release provides the following enhancements targeted towards improving Elasticsearch performance when cluster size is large.

1. Create indices early to give Elasticsearch more time to load balance shards.
2. Limit shards per node to aid Elasticsearch load balancing.
3. Remove keyword definition to reduce Elasticsearch cluster state. This requires dynamic mapping to be enabled.
4. Configurable timeout for Elasticsearch APIs. For details on configuration, see [Configuring Elasticsearch Timeout](#) in the Appendix.
5. Reduce alias count to reduce Elasticsearch cluster state.
6. Separate Coordinator nodes for ingest and query. For details see [Setting Up the Database](#) under [Configuring Online Event Database on Elasticsearch](#).
7. This release extends support for Elasticsearch as external event database to 7.17.3.

## Windows Agent 4.2.0

This version contains 2 enhancements

- A GUI is provided for installing the agent. See **Installing FortiSIEM Windows Agent 4.2.x** in the [Windows Agent 4.x.x Installation Guide](#).
- Ability to upgrade multiple agents in parallel from the Supervisor. See [here](#).

## Collector Cache Usage Visibility

Events are queued in Collectors when it cannot upload to Workers. When Collector buffer becomes full, events are lost. This release provides visibility on Collector event upload buffer.

Collector buffer sizes are displayed in **ADMIN > Health > Collector Health**. For details see [Viewing Collector Health](#).

Two thresholds are defined in **ADMIN > Device Support > Custom Properties**:

- `collectorEventBufferLowThreshold` - default value 10MB
- `collectorEventBufferHighThreshold` - default value 50MB

When the Collector total buffer crosses the high threshold (`collectorEventBufferHighThreshold`), event `PH_AUDIT_COLLECTOR_EVENT_BUFFER_HIGH` is generated.

If the Collector buffer falls below the low threshold (`collectorEventBufferLowThreshold`) after crossing the high threshold, then event `PH_AUDIT_COLLECTOR_EVENT_BUFFER_LOW` is generated.

## OAuth based SMTP Authentication

This release enables FortiSIEM to authenticate via OAuth for sending notification emails.



For details, see [Authentication](#) under [Email Settings](#).

## NFS Version Auto-Negotiation Enabled by Default for FortiSIEM EventDB

For new installations, FortiSIEM will attempt to use the highest NFS version supported between FortiSIEM and NFS server, instead of defaulting to version 3.

## Install and Upgrade Logging Enhancements

In the ansible log, only errors are shown in red color to help user focus on important issues.

## System Upgrade

Linux is upgraded to the latest RockyLinux 8.5 release on Nov 15, 2021. Redis is upgraded to 6.2.26. PostgreSQL is upgraded to 13.5. Vulnerable log4j-core-2.x versions are upgraded to latest 2.17.1.

## HDFS Integration Enhancements

In this release, performance of the HDFS real time archive and non-real time archive from Elasticsearch is improved. Note the HDFS resource allocation suggestions in the [Sizing Guide](#).

## New Device Support

- [Oracle Cloud Infrastructure](#)
- [Windows 2022](#)
- [AWS Elastic Load Balancer](#)
- [Oracle Database Server 18c, 19c Support](#)
- [Dell Force10 S4048T-ON Support](#)

## Bug Fixes and Minor Enhancements

Bug ID	Severity	Module	Description
749146	Major	Discovery and PerfMonitor	WMI integration threw a system error after Windows Update KB5005573 due to auth level.
753455	Major	System	Non-real time NFS archive failed as /archive is owned by root instead of admin .

Bug ID	Severity	Module	Description
762085	Minor	Agent Manager	Proofpoint SIEM API poller tried to poll interval greater than 1 hour, which caused API error on initial polling.
757413	Minor	Agent Manager	Cisco Firepower IPS event pulls could cause phAgentManager to crash.
747005	Minor	Agent Manager	Box.com event pulling execution could fail after running for a period of time.
744215	Minor	Agent Manager	Office365 events were not received in the order they were created , causing follow_by rules to not trigger.
693219	Minor	Agent Manager	Cisco FireSIGHT with Estreamer Integration failed if a password had special characters .
771937	Minor	App Server	PH_AUDIT_CASE_CREATED event sometimes referenced the wrong Organization.
765944	Minor	App Server	No event types showed when the user logged in as cloned full admin user with data conditions.
759638	Minor	App Server	Collector health showed normal even when httpd Process was down on the Collector.
757207	Minor	App Server	Elasticsearch: When a customer ran one query in a specific organization in super global, the result contained events from other organizations.
754267	Minor	App Server	FortiGuard External Integration error message incorrectly stated "0 incidents comments are updated".
753940	Minor	App Server	Collectors could not always receive parser updates from the GUI.
753905	Minor	App Server	After upgrade, Custom Report Bundles could not be scheduled. System Report Bundles worked fine.
753750	Minor	App Server	Baseline reports scheduled execution failed if notification was set.
753193	Minor	App Server	Export query result would fail if result id saved first.
751756	Minor	App Server	Custom JDBC perf jobs, after upgrade, would sometimes not work correctly.
751365	Minor	App Server	Sometimes custom and cloned reports could not to be exported because of a very large report id.
749229	Minor	App Server	If a rule was deleted, then the old Incident name became empty.
746594	Minor	App Server	PDF export did not work if report logo PNG was saved as SVG.
741933	Minor	App Server	Incident queries could sometimes fail as Time Range was not ignored when searching an Incident by ID at the INCIDENTS tab.
741036	Minor	App Server	After an upgrade, Linux agent Event Status was empty on the Agent Health page.

Bug ID	Severity	Module	Description
734975	Minor	App Server	Report bundle containing reports over 90 days did not work.
733272	Minor	App Server	With a Disaster Recovery environment, Online Data on Secondary didn't show information correctly.
732308	Minor	App Server	On the Jobs and Errors page under an Org, a user could see data from another Org .
714176	Minor	App Server	The Last Successful attribute from CMDB Monitor Status tab was not reset properly.
653427	Minor	App Server	Watchlist Export failed in CSV format (Note: PDF format export succeeds).
635725	Minor	App Server	UEBA / Attack dashboard - After drilling down on a trend chart, the number in the bar chart did not match the real incident number.
633790	Minor	App Server	Events did not pick up organization change from the GUI. For example, events still belonged to Super/local after moving one device from super/local to org2.
602350	Minor	App Server	The HTTP header X-Forwarded-For allowed spoofing client address.
516944	Minor	App Server	Same-site cookie attribute support should be added to protect against CSRF and XSSI.
762483	Minor	Data	Event attribute type mismatch between Elasticsearch and FortiSIEM caused events to be dropped by Elasticsearch.
759506	Minor	Data	Zeek Parser parsing issues occurred due to JSON Function Change.
756601	Minor	Data	CarbonBlack CEF did not handle severity properly.
752064	Minor	Data	Fortisandbox related logs from FortiOS were not parsed into expected event types.
749921	Minor	Data	ForeScout CounterACT Parser needed to be extended to handle syslog PRI and follow date information.
741281	Minor	Data	Event parse status of event Win-Security-4688 was 0 (Failed) instead of 1 (Success).
762148	Minor	DataManager	Elasticsearch event insert error when an event attribute mapped to Elasticsearch keyword type, was larger than 32KB.
760658	Minor	DataManager	There should be an enforced limit for Elasticsearch bulk upload size (MB).
760247	Minor	DataManager	custId 0 indices were not created in Elasticsearch.
758570	Minor	DataManager	If current Elasticsearch index became Read only, it shouldn't drop events.

Bug ID	Severity	Module	Description
758031	Minor	DataManager	There should be more detailed logging for Elasticsearch event insert failures.
754713	Minor	DataManager	Sometimes DataManager did not parse Elasticsearch response containing errors and the events were dropped.
758573	Minor	DataPurger	Elasticsearch force merge should be disabled.
751920	Minor	DataPurger	Elasticsearch user defined ILM configuration could get accidentally overwritten by default configuration.
762377	Minor	Discovery	Sometimes FortiGate Test Connectivity showed blank results even though discovery succeeded.
762343	Minor	Discovery	FortiGate REST API Test Connectivity did not get the right host name.
747264	Minor	Discovery	For FortiGate, Interface Alias was set to the Interface Description instead of Interface Name.
746174	Minor	Discovery	Active Directory discovery displayed UID instead of CN as part of the name.
743803	Minor	Discovery	Custom Configuration File Monitoring File I/O Error occurred.
644096	Minor	Discovery	AES256 and SHA256 should be enabled for SNMPv3.
764947	Minor	GUI	Incident explorer trend chart would not update when org is changed.
762141	Minor	GUI	Query filter was incorrect when user clicked Report button to query Proofpoint events.
760742	Minor	GUI	Archive clear button did not clear Real time archive setting.
755140	Minor	GUI	Some INCIDENTS tab page views would jump back and forth between pages without user input.
746515	Minor	GUI	Some Windows/Linux Agent setup properties would disappear when the user clicked the Back button and return.
741088	Minor	GUI	Worker hostname showed empty on GUI after upgrading to 6.3.1.
737889	Minor	GUI	Adding a worker node was not working consistently.
734269	Minor	GUI	Too many Test events during Custom Parser testing could cause the Parser test to respond with 502 error code and browser timeout.
685148	Minor	GUI	STM monitor for HTTP type only worked for 200-204 as success.
616819	Minor	HDFS Mgr	HDFS: Spark exception caused archive failure.
752719	Minor	Java Query Server	Java Query Server did not log detailed exception/error messages when UpdateLookupAction failed in Elasticsearch.

Bug ID	Severity	Module	Description
752577	Minor	Java Query Server	Pre-computed results were not calculated for scheduled report bundles in Elasticsearch.
733201	Minor	Java Query Server	Elasticsearch did not return search results for queries involving Business Service with names containing a space in the name.
689695	Minor	Java Query Server	User was unable to export or preview a long running Report in Elasticsearch.
740131	Minor	Linux Agent	Linux Agent: SELinux configuration was overwritten by agent restart.
772056	Minor	Parser	Unchecked object type inside JSON could cause parser to crash. Observed with some Office365 events where the JSON value was a string and not an object.
764939	Minor	Parser	Optimize error log generation when Kafka forwarded target was unavailable.
753476	Minor	Parser	Windows Agent DHCP Parser did not work if translation patterns were not defined.
751097	Minor	Parser	JSON in fields from Palo Alto Parser caused issues with parsing.
749423	Minor	Parser	In error handling, WMI passwords appeared in logs in cleartext.
738620	Minor	Parser	Rules with Group By Reporting IP did not work as expected.
734905	Minor	Parser	The license enforce time window was not synced to EPS reporting. This could result in erroneous EPS values.
733503	Minor	Parser	Destination IP and Name were parsed incorrectly in DNS ANALYTICAL log with FortiSIEM Agent DNSParser.
743988	Minor	PerfMonitor	Cleartext password appeared in mysql phoenix.log entry.
768063	Minor	PerfMonitor	Custom Configuration File Monitoring would fail if script had no output.
756182	Minor	PerfMonitor	Slow memory leak for monitoring Cisco Meraki devices via SNMP occurred.
755665	Minor	PerfMonitor	FortiGate Config Pulling did not occur when using REST API + SSH credentials.
764757	Minor	PhMonitor	phQueryMaster always got HTTP 502 error from REST cache during startup.
766723	Minor	Query Engine	Data from Incident index could not be queried after Elasticsearch upgrade from 6.8 to 7.15.
740924	Minor	Query Engine	Very large events (greater than 3KB) were not displayed in realtime search.
766624	Minor	System	phProvision.sh script ran unnecessarily.

Bug ID	Severity	Module	Description
761496	Minor	System	FortiSIEM admin user's default shadow password appeared in plaintext even though the account was locked.
760693	Minor	System	phEventExport utility could not export events from NFS /archive.
759541	Minor	System	FSM-2000G - Serial console output did not work.
755085	Minor	System	6.3.2 Upgrade was slow because of unoptimized SQL queries for Incident table cleanup.
753468	Minor	System	After upgrade, user defined Report logo was not displayed in ADMIN > Settings > System > UI.
748362	Minor	System	Failed to install FortiSIEM 6.3.1.0338 on Nutanix platform.
741808	Minor	System	FSM in AWS environment with IPv6 VPC did not automatically assign DHCP v6 IPv6 assigned by AWS.
741254	Minor	System	FortiSIEM timezone was not the same as configured via configFSM.py script.
737516	Minor	System	NFS /data mount was removed by EventDB Online Storage test in GUI.
738265	Minor	System	In Disaster Recovery environment, pre-computed results were not synced to Secondary.
762137	Minor	Windows Agent	Windows Agent stopped sending DNS logs when the DNS log file rotated.
720675	Minor	Windows Agent	Windows Agent UEBA FINS feature didn't parse multibyte characters.
743163	Enhancement	Agent Manager	SQL Server monitoring did not work for SQL Server Clusters.
760439	Enhancement	App Server	The incident processing for ServiceNow/Connectwise integration should be optimized.
739201	Enhancement	App Server	Elasticsearch query interface between GUI and Elasticsearch for long running queries should be optimized.
739061	Enhancement	App Server	Malware Feed downloads saved files in use /data/cache and could impact EventDB performance. They should be moved to /opt/phoenix/cache.
733809	Enhancement	App Server	External Rest API Query did not return phSubIncidentCategory attribute.
682049	Enhancement	App Server	Updated report did not reflect in corresponding dashboard.
611737	Enhancement	App Server	Add user org level CMDB Group under ADMIN > Settings > Discovery > CMDB Group.
763976	Enhancement	Data	Add OT Ports in Resources.
756862	Enhancement	Data	Parse additional Office365 Audit Log Events.

Bug ID	Severity	Module	Description
751433	Enhancement	Data	CarbonBlack CEF parser needs minor adjustment in parsed attributes.
747379	Enhancement	Data	Proofpoint event structure has changed, requiring a parser update.
744604	Enhancement	Data	Need to update TrendMicro DeepSecurity Parser for Chinese version.
743660	Enhancement	Data	Fine tuning for LogBinder SharePoint Events in WinOSWMI Parser needed.
741394	Enhancement	Data	McAfee EPO Parsing -- Another unhandled XML tag type needs to be addressed.
740501	Enhancement	Data	WinOSWMIParser needs to trim the trailing dot from Destination Host Name when parsing DNS logs.
740353	Enhancement	Data	Add all MS SQL Server Event IDs.
662940	Enhancement	Data	Windows Agent Parser needs to parse more attributes for Security Event IDs 6272 and 6273 for Windows server 2016.
739051	Enhancement	GUI	Remove QueryWorker and EventWorker dependency. These two lists should work independently.
718180	Enhancement	GUI	Summary Dashboard   Geo Map View should show the pin location.
735952	Enhancement	Java Query Server	For Elasticsearch, expressions using COUNT DISTINCT in Display Fields should be evaluated.
759086	Enhancement	Parser	Create new FortiSoarCefParser to handle 7.0.1 format change.
759076	Enhancement	Parser	Some Palo-Alto logs were not parsed correctly.
752461	Enhancement	Parser	IPFIX and Netflow V9: Source MAC and Destination MAC were not parsed.
744013	Enhancement	PerfMonitor	FortiGate REST API Credential needs to support custom HTTPS port other than 443.
760628	Enhancement	PerfMonitor	HP/3com switch router config pull script needs to have larger buffer for it to work.
653949	Enhancement	System	Support Geo IP import in IPV6 format.
722473	Enhancement	Windows Agent	UEBA Agent needs to capture File Deletion action in USB drive.

## Rule and Report Modifications since 6.3.3

The following rules were added:

- Emotet Malware Activity Detected by FortiClient
- Emotet Malware Activity Detected on Host
- Emotet Malware Activity Detected on Network
- Emotet Suspicious File Hash Found by Forticlient
- Emotet Suspicious File Hash Found on Host
- Emotet Suspicious File Hash Found on Network
- FortiSIEM: Too Many Unknown Events
- Log4J Exploit Request Detected By Regex
- Log4J Exploit Request Detected on Host by Fortinet Products
- Log4J Exploit Request Detected on Network by Fortinet Products
- Oracle OCI: Customer Secret Key Created
- Oracle OCI: Group Created
- Oracle OCI: Policy Created
- Oracle OCI: Policy Deleted
- Oracle OCI: User Activated MFA
- Oracle OCI: User Added to a Group
- Oracle OCI: User API Key Created and Uploaded
- Oracle OCI: User Auth Token Created
- Oracle OCI: User Created
- Oracle OCI: User Deleted
- Oracle OCI: User Disabled MFA
- Oracle OCI: User OAuth Client Credential Created
- Oracle OCI: User SMTP Credentials Created
- Uncommon AWS Console Login
- Uncommon Azure Portal Login
- Uncommon GSuite Login
- Uncommon Linux process Created
- Uncommon Office365 Mail Login
- Uncommon Server Login
- Uncommon VPN Login
- Uncommon Windows process Created
- Windows DNS Server: Suspicious DNS Traffic Resolved

**The following reports were added:**

- Emotet Malware Activity Detected by FortiClient
- Emotet Malware Activity Detected on Host
- Emotet Malware Activity Detected on Network
- Emotet Suspicious File Hash Found by Forticlient
- Emotet Suspicious File Hash Found on Host
- Emotet Suspicious File Hash Found on Network
- Log4J Exploit Request Detected By Regex
- Log4J Exploit Request Detected on Host by Fortinet Products
- Log4J Exploit Request Detected on Network by Fortinet Products



- Oracle OCI: Failed Login Details
- Oracle OCI: Groups Created
- Oracle OCI: Groups Deleted
- Oracle OCI: MFA Activation History
- Oracle OCI: Password Change History
- Oracle OCI: Policies Created
- Oracle OCI: Policies Deleted
- Oracle OCI: Successful Login Details
- Oracle OCI: Top Create Events by Principal
- Oracle OCI: Top Delete Events by Principal
- Oracle OCI: Top Event Types by Count
- Oracle OCI: Top Events by Country
- Oracle OCI: Top Identity Events by Principal
- Oracle OCI: Top Identity Events by Source IP
- Oracle OCI: User Key and Token Creation History
- Oracle OCI: Users Created
- Oracle OCI: Users Deleted
- Top AWS Console login
- Top Azure Portal login
- Top GSuite login
- Top Linux Process Executions
- Top O365 Mail login
- Top Server Login
- Top VPN login
- Top Windows Process Created

## Known Issues

1. 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.
2. 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.
3. App Server may fail to restart after FortiSIEM reboot or App Server restart. Perform the following workaround to bring up App Server.
  - a. Clean up App Server cache by running the following commands.

```
# su admin
$ cd /opt/glassfish/domains/domain1/
$ rm -rf generated/
$ rm -rf osgi-cache/
```
  - b. Restart App Server by running the following commands.

```
$ cat /opt/glassfish/domains/domain1/config/pid
$ kill -9 $(cat /opt/glassfish/domains/domain1/config/pid)
```

4. If you execute a FortiSOAR playbook on an event or incident, and you click the "details" button to display the playbook raw json response, under some conditions with empty values, it may not display. Please contact Fortinet support for a patch that will resolve this issue.
5. If you execute a FortiSOAR connector from the **ANALYTICS** tab, you may under some conditions, receive an "Unknown" pop up error immediately after clicking execute. Please contact Fortinet support for a patch that will resolve this issue.
6. After upgrading collector, the **ADMIN > Health > Collector Health** page shows an incorrect Upgrade Version and Install Status. After a successful upgrade from 6.3.3 to 6.4.0, **Upgrade Version** should be 6.4.0 and **Install Status** should be Success. However, now it shows **Upgrade Version** as 6.3.3 and **Install Status** as N/A. To check whether upgrade completed successfully, check the Version flag which should be 6.4.0. (Bug 773473)
7. If you re-upload your license, then Java Query Server process on Supervisor does not automatically restart. Workaround is to manually restart the Java Query Server processes. (Bug 773578)
8. There is a known issue with Elasticsearch rolup search API when sorting AVG (<https://github.com/elastic/elasticsearch/issues/58967>). Therefore, do not use pre-compute Elasticsearch queries that have ASC or DESC on AVG().
9. In the GUI, the **ADMIN > Health > Cloud Health** page may time out if there are many Workers. (Bug 785547)
10. Query Master process can consume significant memory if there is a large number of devices with performance metrics to be shown in the Summary dashboard. This may cause the Supervisor to be unresponsive. (Bug 769414)
11. Cisco FireAMP log pulling can cause Agent Manager process to crash under some circumstances. (Bug 757413)
12. After an upgrade, the Java Query Server may load older libraries causing connection timeouts with Elasticsearch. This may cause queries to fail. (Bug 783844)
13. Collector may not efficiently get WMI events if there is a large number of Windows Servers to poll and some of the Windows Server are down. Log pulling may fall behind and is caused by a large timeout in one of the WMI calls. (Bug 788034)
14. In the GUI, attempting to set a new Password for a user created with the "Password Reset" field set may fail, showing "Undefined" Error. (Bug 776295)
15. FortiSIEM failed to get running-config from Cisco IOS devices. (Bug 789843)
16. DeviceToCMDDBAttr(Reporting IP : Importance) display condition does not return default importance value. (Bug 779188)
17. Content Update Install may randomly return "Operation failed." However subsequent retries succeed without issues. (Bug 788973)
18. 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**

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

Example:

...

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

...

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

`GET fortisiem-event-*/_settings`



[www.fortinet.com](http://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.