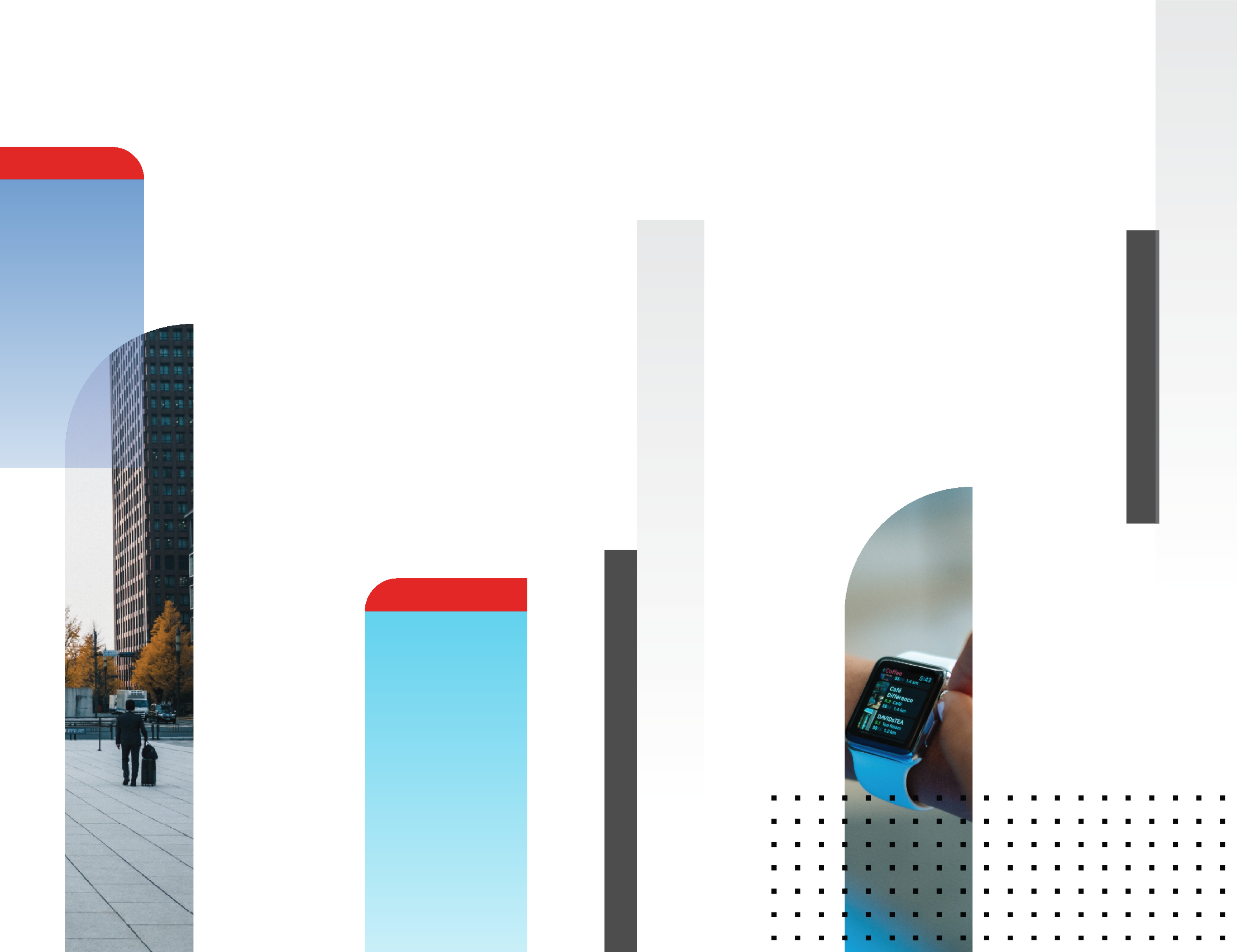
Release Notes

FortiSIEM 6.3.2



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

FORTINET®

08/15/2022
FortiSIEM 6.3.2 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
10/15/2021	Initial version of FortiSIEM 6.3.2 Release Notes.
11/05/2021	Added Known Issues - Slow Upgrade to 6.3.2 Release Notes.
12/14/2021	Added Known Issues - Remediation Steps for CVE-2021-44228 for 6.x Release Notes.
05/12/2022	Added Known Issue Elasticsearch Based Deployments Terms Query Limit to Release Notes.
08/15/2022	Add Known Issue to 6.3.x Release Notes.

What's New in 6.3.2

This document describes the additions for the FortiSIEM 6.3.2 release.

- New Features
- Key Enhancements
- New Device Support
- Bug Fixes and Minor Enhancements
- Rule and Report Modifications since 6.3.1
- Known Issues

New Features

- Bi-Directional Elasticsearch Cross-Cluster Replication Support

Bi-Directional Elasticsearch Cross-Cluster Replication Support

In the 6.3.1 release, FortiSIEM only supported uni-directional Cross-Cluster Replication (CCR) for Disaster Recovery. However, uni-directional CCR implementation can be time consuming and error prone, involving many manual steps.

This release adds support for bi-directional CCR, which is much easier to implement and maintain. This is the recommended method for Disaster Recovery in Elasticsearch deployments.

Elasticsearch documentation on bi-directional CCR can be found here - https://www.elastic.co/blog/bi-directional-replication-with-elasticsearch-cross-cluster-replication-ccr.

Details on how to make FortiSIEM work with bi-directional CCR can be found here.

Key Enhancements

- Improved Elasticsearch to HDFS Archiving
- Automated CMDB Disk Space Management
- Kafka Consumer Authentication
- Incident Event for Every Incident Trigger
- Show All Incident Trigger Events via Pagination
- Elasticsearch Event Export Tool
- REST API to Return Worker Queue State
- Alert when Entity Risk Reaches Pre-Defined Threshold

Improved Elasticsearch to HDFS Archiving

Elasticsearch to HDFS archiving performance is improved by using:

1. Sliced scrolling and
2. Concurrently archiving multiple indices

Automated CMDB Disk Space Management

If the CMDB disk partition becomes full, then the system may not work correctly. To prevent this from happening, this release introduces a CMDB disk space management framework.

Three parameters are introduced in `phoenix_config.txt`.

- `month_retain_limit`: Number of months for which incidents on the Supervisor node should be retained (default value 6 months).
- `cmdb_disk_space_low_threshold` (in MB): When free CMDB disk space falls below this defined threshold, disk management kicks in (default value 50MB).
- `cmdb_disk_space_high_threshold` (in MB): When disk management kicks in, incidents are purged until CMDB disk space reaches this defined threshold (default value 100MB).

Two audit events are introduced.

- `PH_AUDIT_CMDB_DISK_PRUNE_SUCCESS`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and old incidents and identity / location data were pruned to bring the free CMDB disk space above the high threshold (`cmdb_disk_space_high_threshold`).
- `PH_AUDIT_CMDB_DISK_PRUNE_FAILED`: This event indicates that free CMDB disk space fell below the low threshold (`cmdb_disk_space_low_threshold`) and in spite of pruning older incidents and identity / location data, free CMDB disk space stays below the high threshold (`cmdb_disk_space_high_threshold`). To remedy this situation, the user must reduce the number of months of incidents and identity / location data in CMDB (`month_retain_limit`).

Two system defined rules are included.

- FortiSIEM: CMDB Disk space low - Prune successful.
- FortiSIEM: CMDB Disk space low - Prune failed to keep free disk space above high threshold.

Kafka Consumer Authentication

FortiSIEM can already receive events via Kafka. This release adds the ability for FortiSIEM to authenticate to Kafka before receiving events.

For details on configuring Kafka for authentication, see Setting up Consumer under Kafka Settings.

For details on configuring FortiSIEM to authenticate to Kafka, see Setting Up FortiSIEM under Kafka Settings.

Incident Event for Every Incident Trigger

If an Incident triggers for the same rule with identical group by parameters, FortiSIEM keeps the same Incident instance and updates the Incident count, Last Occur Time and Triggering events in CMDB. This is part of the Incident deduplication feature, which helps to reduce Incident clutter.

In earlier releases, an Incident event of event category 1 was generated when the Incident triggers "for the first time". In this release, similar Incident event of event category 1 is generated *for each subsequent incident triggers*. These events have their own Incident occur timed and triggering events. These events are stored in the event database and can be used for audit purposes.

Show All Incident Trigger Events via Pagination

In earlier releases, the FortiSIEM GUI only showed the last set of Incident Triggering events when you visited the Event tab for a specific Incident from the INCIDENTS > List View tab. In this release, FortiSIEM shows all Triggering events via pagination.

Elasticsearch Event Export Tool

The `phExportESEvent` tool is introduced to export events from Elasticsearch to a CSV file.

For details, see Exporting Events to Files in the Appendix.

REST API to Return Worker Queue State

This release provides a public REST API that can be used to query Worker Event Upload Queue state. The Queue state indicates whether the Worker is able to keep up with incoming event stream. An upstream load balancer can use the information to route events from Collectors to the least loaded Worker.

For details, see REST API to Return Worker Queue State in the Appendix.

Alert when Entity Risk Reaches Pre-Defined Threshold

Two thresholds are system defined :

- EntityRiskThresholdHigh: default 80
- EntityRiskThresholdMedium: default 50

Four audit events are generated based on these thresholds:

- PH_AUDIT_RISK_INCREASE_MED - Host/User risk increased and crossed Medium threshold.
- PH_AUDIT_RISK_INCREASE_HIGH - Host/User risk increased and crossed High threshold.
- PH_AUDIT_RISK_DECREASE_MED - Host/User risk decreased and fell below Medium threshold.
- PH_AUDIT_RISK_DECREASE_LOW - Host/User risk decreased and fell below Low threshold.

Two rules are included. By default, these rules are off and need to be turned on based on your environment.

- Host/User risk increased and crossed Medium threshold
- Host/User risk increased and crossed High threshold

New Device Support

Cisco Umbrella via API

Aruba CX Switch via Syslog

Barracuda Web Application Firewall via Syslog

Bug Fixes and Minor Enhancements

Bug ID	Severity	Module	Description
752220	Minor	App Server	A Report Bundle, when run in the background, may stop running and not produce results.
743631	Minor	App Server	A discovered device may not be added to CMDB Network Segment.
738677	Minor	App Server	ph_dwl_entry_incident table filled up the CMDB disk space making FortiSIEM unaccessible via GUI.
746760	Minor	App Server	After restarting app server, old closed incidents to ServiceNow may be reopened.
748434	Minor	Data	Source and Destination Host Name were parsed incorrectly in Incident events.
750890	Minor	Data	Barracuda WAF Firewall Parser -- Include eventAction attribute in some ACL and Web Firewall logs.
749293	Minor	Data	Office365 Parser did not parse "Subject" or "Receiver" information from email log.
748351	Minor	Data	"DARKSIDE Domain Traffic Detected" rule with heavy regex needs to be optimized.
737257	Minor	Elasticsearch	For HDFS archive, it must only delete an Elasticsearch event index AFTER it is archived successfully.
744341	Minor	GUI	Incident Target field sometimes showed data from another incident.
741741	Minor	GUI	Elasticsearch ILM Settings in ADMIN > Settings > Database > Online Settings for AWS ES and ES Cloud is meaningless.
746758	Minor	GUI	Notification policy page did not load where there were a large number of CMDB Objects in each policy.
712720	Minor	Parser	Box.com Discovery failed due to redirect_url_missing error.
742893	Minor	Parser	phParser CPU was sometimes high for parsing JSON events at EPS around 1800.
745198	Minor	Parser	IP enrichment for US IP addresses displayed "United States of America" when Country Group looked for "United States".

Bug ID	Severity	Module	Description
742922	Minor	Query Engine	QueryMaster to Worker communication stopped because of Interrupted system call.
749132	Minor	System	Expired Self signed Certificate was in FortiSIEM 6.3.1 OVA - ESX install file.
750351	Minor	System	Prevent phDataManager from resetting shared buffer when it falls behind.
745379	Minor	System	fortigate_block_ip_after_5.4.py did not check the result properly, resulting in remediation progress staying at 0%.

Rule and Report Modifications since 6.3.1

The following rules were added:

- ArubaOS-CX: Config Change Detected
- ArubaOS-CX: Multiple Users Deleted
- ArubaOS-CX: User Added
- ArubaOS-CX: User Deleted
- Barracuda WAF: Config Change Detected
- Cisco Umbrella: Failed DNS Requests to Malware Domains: Same source and Multiple Destinations
- Cisco Umbrella: Intelligent Proxy Blocked a Malware Request by Policy
- Cisco Umbrella: Multiple Failed DNS Requests to a Malware Domain: Same source and Destination
- Office365: Abnormal Logon Detected
- Office365: Brute Force Login Attempts - Same Source
- Office365: Brute Force Login Attempts - Same User
- Office365: Brute Force Logon Success
- Office365: Identity Protection Detected a Risky User or SignIn Activity
- Office365: Delete Message Inbox Rule Created
- Office365: Move To Folder Inbox Rule Created
- Office365: Set-Mailbox Forwarding Action Created
- Office365: Strong Authentication Disabled for a User
- Office365: Suspicious File Type Uploaded
- Office365: User Mailbox Forwarding Rule Created
- FortiSIEM: CMDB Disk space low - prune successful
- FortiSIEM: CMDB Disk space low - prune failed to keep free disk space above high threshold
- Host/User risk increased and crossed Medium threshold
- Host/User risk increased and crossed High threshold

The following rules were renamed:

- Windows: RDP over Reverse SSH Tunnel -> Windows: RDP Traffic over Reverse SSH Tunnel
- Windows: RDP Over Reverse SSH Tunnel -> Windows: Svchost hosting RDP over Reverse SSH Tunnel

The following rule was deleted:

- Windows: Detection of Possible Rotten Potato

The following reports were added:

- ArubaOS-CX: Config Change Audit
- ArubaOS-CX: Password Change History
- ArubaOS-CX: Users Added
- ArubaOS-CX: Users Deleted
- Barracuda WAF: Admin Audit Activity
- Barracuda WAF: Network Firewall Allowed Traffic
- Barracuda WAF: Network Firewall Denied Traffic
- Barracuda WAF: System Events
- Barracuda WAF: Web Activity Traffic
- Barracuda WAF: Web Firewall Deny
- Barracuda WAF: Web Firewall Permit
- Cisco Umbrella: Blocked DNS Requests by Source and Destination Domain
- Cisco Umbrella: Intelligent Proxy Blocked a Request
- Cisco Umbrella: Top Allowed DNS Requests by Destination Domain
- Cisco Umbrella: Top Blocked DNS Requests by Destination Domain

The following reports were renamed:

- NERC_CIP_008: Monthly Security Incident Trend -> NERC_CIP_008: Daily Security Incident Trend
- NERC_CIP_008: Monthly Security Incident Resolution Time Trend -> NERC_CIP_008: Weekly Security Incident Resolution Time Trend
- NERC_CIP_008: Monthly Assigned Security Incident User Trend -> NERC_CIP_008: Weekly Assigned Security Incident User Trend
- NIST800-171 3.6.1-3.6.2: Monthly Incident Resolution Time Trend -> NIST800-171 3.6.1-3.6.2: Weekly Incident Resolution Time Trend
- NIST800-171 3.6.1-3.6.2: Monthly Assigned Incident User Trend -> NIST800-171 3.6.1-3.6.2: Weekly Assigned Incident User Trend
- NIST800-171 3.6.1-3.6.2: Monthly Incident Trend -> NIST800-171 3.6.1-3.6.2: Weekly Incident Trend
- NIST800-53 IR-4: Monthly Incident Resolution Time Trend -> NIST800-53 IR-4: Weekly Incident Resolution Time Trend
- NIST800-53 IR-4: Monthly Assigned Incident User Trend -> NIST800-53 IR-4: Weekly Assigned Incident User Trend
- NIST800-53 IR-5: Monthly Incident Trend -> NIST800-53 IR-5: Weekly Incident Trend

Known Issues

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.

Remediation Steps for CVE-2021-44228

Three FortiSIEM modules (SVNLite, phFortiInsightAI and 3rd party ThreatConnect SDK) use Apache log4j version 2.14, 2.13 and 2.8 respectively for logging purposes, and hence are vulnerable to the recently discovered Remote Code Execution vulnerability (CVE-2021-44228).

These instructions specify the steps needed to mitigate this vulnerability without upgrading Apache log4j to the latest stable version 2.16 or higher. Actions need to be taken on the Supervisor and Worker nodes only.

On Supervisor Node

1. Logon via SSH as root.
2. Mitigating SVNLite module:
   a. Run the script `fix-svnlite-log4j2.sh` (here). It will restart SVNlite module with `Dlog4j2.formatMsgNoLookups=true` option and print the success/failed status.
3. Mitigating 3rd party ThreatConnect SDK module:
   a. Delete these log4j jar files under `/opt/glassfish/domains/domain1/applications/phoenix/lib`
      i. log4j-core-2.8.2.jar
      ii. log4j-api-2.8.2.jar
      iii. log4j-slf4j-impl-2.6.1.jar
4. Mitigating phFortiInsightAI module:
   a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
      i. log4j-core-2.13.0.jar
      ii. log4j-api-2.13.0.jar
5. Restart all Java Processes by running: “`killall -9 java`”

On Worker Node

1. Logon via SSH as root.
2. Mitigating phFortiInsightAI module:
   a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
      i. log4j-core-2.13.0.jar
      ii. log4j-api-2.13.0.jar
3. Restart all Java Processes by running: “`killall -9 java`”

Slow Upgrade

Release 6.3.2 upgrade contains some SQL commands to cleanup some incident tables in CMDB. These commands may be slow to execute if your CMDB has a large number of incidents (millions). This may slow the upgrade, which may appear to be stuck.

Please follow the following steps to complete the upgrade. There are two cases:

- Case 1: 6.3.2 Upgrade has not started yet
- Case 2: 6.3.2 Upgrade appears stuck and Supervisor snapshot is not available

Case 1: 6.3.2 Upgrade has not started yet

Follow the steps below if you have not started the 6.3.2 upgrade. If you failed on an upgrade, and recovered from a snapshot, then you can follow these steps as well.

1. Download the following SQL file: `632_run_before_upgrade.sql`.
2. Upload the SQL file to the Supervisor under `/tmp/`
3. SSH into the Supervisor as root.
4. Run: `psql -U phoenix -d phoenixdb -f /tmp/632_run_before_upgrade.sql`
5. Proceed with the regular 6.3.2 upgrade.

Case 2: 6.3.2 Upgrade appears stuck and Supervisor snapshot is not available

In this case, the upgrade has started but it is running for an extensive period of time with the following display.

```
[10:44:34] migrate-database : DATABASE | Create Super User | localhost | SKIPPED | 46ms

[10:44:34] migrate-database : DATABASE | Give ALL ACCESS to USER | localhost | SKIPPED
| 46ms
```

Take the following steps:

1. CTRL+C to break out of the upgrade.
2. Download `632_known_issue.tgz` and upload it to the Supervisor under `/tmp`.
3. SSH into the Supervisor as root.
4. Run the following commands.
   ```
   # cd /tmp/
   # tar xvzf /tmp/632_known_issue.tgz
   ```
5. Replace the upgrade playbook by running the following commands.
   ```
   # cd /usr/local/upgrade/
   # mv post-upgrade.yml post-upgrade.yml.orig
   # mv /tmp/modified_post-upgrade.yml post-upgrade.yml
   # chmod 755 post-upgrade.yml
   ```
6. Replace the upgrade task file by running the following commands.
   ```
   # cd /usr/local/upgrade/roles/migrate-database/tasks/
   # mv main.yml main.yml.orig
   # mv /tmp/migrate-database_tasks_main.yml main.yml
   # chmod 755 main.yml
   ```
7. Replace the sql file by running the following commands.
   ```
   # cd /opt/phoenix/deployment/upgrade/
   # mv phoenix_db_up_6.3.1_to_6.3.2.sql phoenix_db_up_6.3.1_to_6.3.2.sql.orig
   # mv /tmp/phoenix_db_up_6.3.1_to_6.3.2.sql phoenix_db_up_6.3.1_to_6.3.2.sql
   # chmod 755 phoenix_db_up_6.3.1_to_6.3.2.sql
   ```
8. Continue the upgrade by running the following command.
   ```
   # ansible-playbook post-upgrade.yml | tee -a logs/ansible_upgrade_continued.log
   ```

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
   ```

FORTINET®

www.fortinet.com

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.