FortiSIEM - Release Notes

Version 5.2.5

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

12/17/2019
FortiSIEM 5.2.5 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
09/10/2019	Initial version of FortiSIEM 5.2.5 Release Notes.
12/17/2019	Revision 1: Removed special upgrade 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 in FortiSIEM 5.2.5 Release.

What's New in 5.2.5

This document describes the requirements for the FortiSIEM 5.2.5 release.

Note that this release includes 5.2.4 release features. For more information on 5.2.4 features, look here.

Pre-deployment Notes

The location where you pick up FortiSIEM Images has changed—the website https://images-cdn.fortisiem.fortinet.com/ is no longer available. You must obtain FortiSIEM Images from the Fortinet support site: https://support.fortinet.com/.

1. Follow the instructions in Downloading FortiSIEM Products to get the FortiSIEM images.
2. Follow the fresh install instructions in Getting Started.
3. Follow the upgrade instructions in the Upgrade Guide.

Elasticsearch and upgrades to 5.2.5:

In 5.2.5, Elasticsearch query behavior changed from case-sensitive to case-insensitive, to enable users to search log data without knowing the case. To support this enhancement, Elasticsearch event data format has changed in 5.2.5. After the 5.2.5 upgrade, data will be written in the new format starting new day UTC time. FortiSIEM can only query data in the new format, so event queries will not work with older data until they are re-indexed. For details, see "Migrating Elasticsearch data from 5.2.1 or earlier to 5.2.5" in the Upgrade Guide.

Report Server upgrade to 5.2.5 is not working. If you are running Report Server, then follow these steps to upgrade to 5.2.5:

1. Upgrade Super, Worker, Collector, and Report Server as described in the Upgrade Guide.
2. Archive the Report Server event database. Run this command:
   `/opt/phoenix/deployment/reportdb_archiver.sh`
3. The report db backup is under `/data/archive/reportdb/reportdb_2019-09-09T14-33-26`.
4. Delete the Report Server from Super.
5. Add the Report Server back to Super.
6. Restore Report Server event database from Archive. Run this command:
   `/opt/phoenix/deployment/reportdb_restore.sh/data/archive/reportdb/reportdb_2019-09-09T14-33-26`.

Rescheduling Reports After Changing GUI Locale

If you change the GUI Locale after upgrading to 5.2.5, then you must reschedule all of your scheduled reports for the new Locale.

Adding Organizations Using Elasticsearch

Dynamic Shard management becomes active on a new day in the Coordinated Universal Time (UTC) timezone. This affects the 5.2.5 upgrade and the addition of new customers in Managed Service Provider (MSP) environments. This means that if you are in the Pacific Standard Timezone (PST):

- It is better to upgrade to 5.2.5 slightly after 4 PM, which is the beginning of a new day (4 PM PST = 0 AM UTC).
- If you are adding an Organization to the system, it is better to add the customer slightly after 4 PM local time.

Swap not set up on fresh install

To add back the swap partition, run the following command on Super, Worker, Report Server and Collector nodes:

```
mv -f /etc/fstab /etc/fstab.bak.525; (cat /etc/fstab.bak.525 | grep -Ev
'^UUID=.*\sswap'; blkid | grep swap | sed -E 's/.*UUID="(\S+)" TYPE.*/UUID=\1 swap
swap defaults 0 0/') > /etc/fstab; swapon -a; free -h
```

Redis running in master-slave mode

Starting with release 5.2.5, Redis mode has changed from cluster to master-slave to better suit FortiSIEM's needs

New Features

New Chart Types for Data Visualization

This release adds more visualization charts in the widget dashboard and analytics: Choropleth Map (Region Map), Sankey Diagram, Chord Diagram, Clustered Bubble Chart and Sunburst Diagram. These charts are available from the Widget Dashboard and Analytics. See FortiSIEM Charts and Views.

Incident Explorer View

This release adds a dynamic Incident dashboard that helps users to correlate actors (IP, Host, User) across multiple incidents, without creating multiple reports in separate tabs. The Incident Explorer View displays incident trends, actor, and incident details on the same page. The user can choose an actor and see all of the incidents concerning the actor.

The user can then select a time range to narrow down the number of incidents. Time ranges, actors, and incidents can be chosen in any order. Each time a selection is made, the rest of the dashboard updates to reflect that selection. See Incident Explorer View.

Enhanced CMDB Search

In previous releases, the user could search the CMDB by entering a string to match the contents of a set of fields. In this release, the user can search on a field-by-field basis and on multiple fields at once. The possible values are shown so that the user can select them. Custom device attributes are included in search fields as well. See Searching for Devices.

Dynamic CMDB Group from Custom Properties

Dynamic CMDB Groups can now be created from device properties. See Grouping Devices by Custom Properties.

Support for Dependent Properties in CMDB Import

This release enables users to model an external CMDB inside the FortiSIEM CMDB by adding the concepts of Site and Application to Device. Conceptually:

- an Application runs on one or more Sites and
- a Site contains many Devices

To model this in the FortiSIEM CMDB, users must create the following items (in **ADMIN > Device Support > Custom Property**):

- a set of Site properties with one Site property being a Key
- a set of App properties with one App property being a Key

The user must then create a CMDB file containing Device, Site, and App Properties and import it via Device Inbound Integration in **ADMIN > Settings > Integration**.

The user can use these Device, Site, and App properties in Analytics, Rules, CMDB Reports, and Dashboards.

User Interface

In addition to English, the FortiSIEM GUI is localized to the following languages:

- Chinese - Simplified
- Chinese - Taiwan
- Chinese - Hong Kong
- French
- Italian
- Japanese
- Korean
- Portuguese
- Spanish
- Russian
- Romanian

The user can specify the language for the GUI in the UI Settings tab of the User Profile dialog box. For more information, see "Language" in the table beneath UI Settings here.

Elasticsearch Support Features

This release contains the following Elasticsearch enhancements:

- Elasticsearch 6.8 Support
- Dynamic Shard management
- REST client Support
- Ability to view and stop long running queries

Elasticsearch 6.8 support enables customers to use HTTP(S) REST clients under basic license, frozen indices, and others.

Prior releases used a fixed number of shards per index, per day. If EPS is very high, then the index may become very large. On the other hand, for the MSSP case using one index per customer, a large number of customers can create too many shards. Both cases can cause Elasticsearch performance to degrade.

This release adds dynamic shard management to maintain optimal Elasticsearch performance.

This is based on the following checks: (a) Size of a shard is less than 40GB, (b) total number of Shards is less than the total number of Hot Nodes times the number of vCPU per node, (c) Index is half full. By using Elasticsearch aliasing techniques when each of these conditions are violated, FortiSIEM keeps the number of shards under operational limits. Additionally, when the number of segments is more than twice the number of shards, then FortiSIEM forces a segment merge to reduce Elasticsearch memory usage.

In addition to Transport Client, Elasticsearch Queries can now use REST-based HTTP(S). This can be configured during Elasticsearch setup.

Long running Elasticsearch queries can now be stopped from the FortiSIEM GUI.

For more information on HTTP(S) REST and shards, see Configuring Storage.

Linux/Windows Agent Features

- **Signed Agent binaries**: Both Linux and Windows Agent binaries are now cryptographically signed by Fortinet.
- **Ability to specify host name**: The user can specify a host name during Agent installation. The Agent will register to the Supervisor with that host name. CMDB will show that host name. See "Installing Windows Agent" in the Windows Agent 3.1.2 Installation Guide and "Installing Linux Agent" in the Linux Agent Installation Guide.
- **Virtual Collector Support**: Agents can send events to a Virtual Collector (such as an F5 Load balancer) located between Agents and Collectors. Virtual Collectors can be defined in the Agent definition on the Supervisor.
- **Linux Agent – detects process creation similar to the Windows Sysmon agent**: FortiSIEM Linux Agent is extended to detect processes being created on a host along with parent process and file hash. The event type is LINUX_PROCESS_EXEC.
- **Linux Agent – adds time zone information so that times in logs are normalized correctly**.
- **Linux Agent syslog definition section automatically selects logs of higher severity when a specific severity is chosen. This avoids unnecessary mouse clicks.**

Cluster upgrades

Current upgrade procedure is complex for a large Super, Worker cluster:

1. Stop Workers
2. Stop Super
3. Upgrade Super
4. Bring up Super
5. Upgrade and bring up Workers one by one

FortiSIEM provides one script to upgrade the Super and another script to upgrade the Workers.

The scripts are available only in releases after 5.2.5.

See "Upgrading a FortiSIEM Cluster Deployment" in the Upgrade Guide.

Key Enhancements

- In the GUI, we explicitly show the specific report design template that will be used to create the PDF. See here.
- FortiSIEM automatically adds a default template when the user adds a new report to a Report Bundle with an existing design template
- On the Entity Risk score page, the user can choose the time duration for Risk Trends and Associated Incidents
- For the Nessus6 scanner, the user can discover and pull log names by host name
- A Redis cluster is introduced for Super and Worker nodes to share large objects such as device properties. This reduces the load on the App Server.
- In the Custom Parser definition, search is improved to show all matched values more clearly
- The ability to search for a specific job in the Jobs page has been added
- Improved performance for C++ XML parsing of large XMLs received from App Server
- Custom Jobs are now discoverable without SNMP/WMI credentials
- A system error is created when many in-line report files accumulate at a Worker node. This indicates that the Worker is falling behind in merging in-line reports. You should add a Worker or reduce the number of in-line reports.
- Jira incident outbound integration can now map FortiSIEM Incident attributes to custom Issue Types
- REST APIs have been added to:
  - update certain Incident attributes
  - get Agent Status for a specific host
  - get Triggering Event IDs for one or more incidents

  For more information see the FortiSIEM - Integration API Guide.
- Optimize Malware IP/Domain/URL import performance via CSV files
- Multi-line log parsing support for logs read from a directory
- Identity and Location data processing is optimized to run faster
- ConnectWise is deprecating SOAP-based integration and recommending REST APIs. For REST API-based ConnectWise integration, Client ID is now required.

New Device Support

Devices are described in the External Systems Configuration Guide.

Support for the following devices are added in this release:

- Alert Logic IPS IRIS V2.0 API - Log collection via API
- AWS Kinesis stream - Log collection via API
- AWS Security Hub - Log collection via API
- Bro Parser - New log parser
- Cisco AMP endpoint V1 streaming API - Log collection via API
- CoSoSys Endpoint Protector - New log parser
- Forcepoint - New log parser
- FortiADC - New log parser
- Fortinet FortiInsight – Alert collection via API
- GitLab - Log collection via Git CLI
- Microsoft Azure Event Hub - Log collection via API
- OneIdentity Balabit - New log parser
- Sophos XG Firewalls - New log parser

Device Support Extensions

- BIND - Enhanced syslog parsing and new Event Types
- Cisco ASA - Enhanced syslog parsing
- Cisco ASA - Enhanced syslog parsing and support Threat Defense
- Cisco ISE - Enhanced syslog parsing
- Crowdstrike Falcon Data Replicator - EnhancedLog collection via API, parse more attributes
- FireEye - Enhanced syslog parsing
- Forcepoint - Enhanced syslog parsing
- Forescout ACT - Enhanced syslog parsing
- FortiAuthenticator – parse logs received via FortiAnalyzer
- FortiGate - parse firewall action - Enhanced syslog parsing
- FortiMail support alternative date format - Enhanced syslog parsing
- FortiOS add support for FOS 6.2 - Enhanced syslog parsing
- FortiSandbox 2.5.1 - Enhanced syslog parsing
- FortiSwitch – Discovery, CPU and Memory usage monitoring
- FortiWeb - Enhanced syslog parsing
- French Windows Security Logs parsing update - Enhancement to parser
- Gitlab - Enhanced parsing
- IPFIX – Parse pre-NAT Source IP field
- Juniper SRX300 JUNOS-15 support - Enhanced syslog parsing
- Linux/Unix - Enhanced syslog parsing
- Mcafee web gateway - Enhanced syslog parsing
- Microsoft Windows Security events - Enhancement to parser
- Nozomi - Enhanced syslog parsing
- Office 365 - Enhanced parsing
- PacketFence - Enhanced syslog parsing
- Palo Alto Firewall - Enhanced syslog parsing
- Postfix - Enhanced syslog parsing and new Event Types

- SentinelOne - Enhanced syslog parsing
- Snort parser to support Security Onion - Enhanced syslog parsing
- STIX OTX Integration – extended to cover STIX 2.0
- Symantec WebIsolation - Enhanced syslog parsing
- Websense Web security - Enhanced syslog parsing and new Event Types
- Windows - Update WinOSParser (logs received via Snare) to match WinOSWMIParser and WinOSPullParser parsing
- Windows Security events – update parsing and categorization for event Ids - 4625, 4768, 4771, 4772, 4769
- Windows Security logs – translations updated for French

New and Modified Rules and Reports

New Rules

The following new rules have been defined for the 5.2.5 release:

- AI: File Creation Anomaly
- AI: File Deletion Anomaly
- AI: File Reading Anomaly
- AI: File Writing Anomaly
- AI: Process Started Anomaly
- AI: Process Stopped Anomaly
- AlertLogic Incident
- AWS SecHub: Host Vulnerability Detected
- AWS SecHub: Software and Configuration Violation
- AWS SecHub: Tactics: Collection Detected
- AWS SecHub: Tactics: Command_and_Control Detected
- AWS SecHub: Tactics: Credential Access Detected
- AWS SecHub: Tactics: Defense Evasion Detected
- AWS SecHub: Tactics: Discovery Detected
- AWS SecHub: Tactics: Execution Detected
- AWS SecHub: Tactics: Impact: Data Destruction Detected
- AWS SecHub: Tactics: Impact: Data Exfiltration Detected
- AWS SecHub: Tactics: Impact: Data Exposure Detected
- AWS SecHub: Tactics: Impact: Denial of Service Detected
- AWS SecHub: Tactics: Initial Access Detected
- AWS SecHub: Tactics: Lateral Movement Detected
- AWS SecHub: Tactics: Persistence Detected
- AWS SecHub: Tactics: Privilege Escalation Detected

- AWS SecHub: Unusal Data Behavior Detected
- AWS SecHub: Unusal Database Behavior Detected
- AWS SecHub: Unusal Network Flow Behavior Detected
- AWS SecHub: Unusal Process Behavior Detected
- AWS SecHub: Unusal Serverless Behavior Detected
- AWS SecHub: Unusual Application Behavior Detected
- Crowdstrike - Activity Prevented
- Crowdstrike - Attacker Methodology
- Crowdstrike - Authentication Bypass
- Crowdstrike - Blocked Exploit
- Crowdstrike - Credential Theft Detected
- Crowdstrike - Data Deletion
- Crowdstrike - Data Theft
- Crowdstrike - Drive By Download
- Crowdstrike - Establish Persistence
- Crowdstrike - Evade Detection
- Crowdstrike - Exploit Pivot
- Crowdstrike - File Blocked With Matching Hash
- Crowdstrike - Intel Detection
- Crowdstrike - Known Malware
- Crowdstrike - Machine Learning
- Crowdstrike - Malicious Document
- Crowdstrike - NextGen Anti-virus based Malware
- Crowdstrike - Overwatch Detection
- Crowdstrike - Privilege Escalation
- Crowdstrike - Ransomware
- Crowdstrike - Server Compromise
- Crowdstrike - Social Engineering
- Crowdstrike - Suspicious Activity
- Crowdstrike - Suspicious Processes Terminated
- Crowdstrike - User Compromise
- Excessive Crowdstrike detected suspicious activity at a host
- Policy: Browser Download
- Policy: Browser Upload
- Policy: Customer Data Uploaded to Cloud
- Policy: Customer database changes
- Policy: Customer Defined Policy Violation
- Policy: File Backed Up to Cloud
- Policy: File Written to Removable
- Policy: Financial Data Breach
- Policy: HR Data Access
- Policy: Monitor Command Line Usage
- Policy: Monitor Suspicious Application Usage
- Policy: Protect Sensitive Folders - Board Minutes
- Policy: Removable Media Audits

- Policy: Segregation of Duties
- Policy: Source Code Copied to Removable Media
- Policy: Uploads of sensitive data to non-EEA countries
- Policy: User Login Out of Hours
- Policy: VPN Usage

New Reports

The following new reports have been defined for the 5.2.5 release:

- All AWS Security Hub Events
- All AWS Security Hub Threat Sources
- All Crowdstrike Authentication Audit Activity Events
- All Crowdstrike Detection Events
- DNS Requests to .ru and .cn
- Linux bash history access
- Linux file staging
- Linux file timestomping via touch
- Linux internal reconn
- Linux Successful and Failed sudo
- Malware activity - AfraidGate
- Malware activity - Angler
- Malware activity - InPage - Domain match
- Malware activity - Sage 2.0 - Domain match
- Malware activity - Sage 2.0 Ransomware - IP and Port match
- Malware activity - Sage 2.0 Ransomware - Process match
- Top AWS Security Events and Hosts
- Top AWS Security Hub Events
- Top Crowdstrike Detection Events
- Top DNS Destination domains
- Top Hosts With AWS Security Hub Events
- Top Linux Process File Hashes (from Crowdstrike Data Replicator)
- Top Linux Process File Hashes (from FSM Agent)
- Top Non-US Web Connections
- Top outbound non-http connections by destination city, country
- Top Unique DNS Requesters (From Crowdstrike Data Replicator logs)
- Top Unique DNS Requesters (From FSM Agent)
- Top Windows Process File Hashes (from Crowdstrike Data Replicator)
- Top Windows Process File Hashes (from sysmon)
- Top Windows Systems With Unique Logins
- Windows Active Directory Controller Database file modification
- Windows BITSAdmin download
- Windows Certutil Decode in AppData
- Windows Code Execution in Non Executable Folder
- Windows Code Execution in Webserver Root Folder
- Windows Command With Suspicious URL and AppData String

- Windows DHCP Callout DLL installation
- Windows External IP in Command Line (From Crowdstrike data Replicator)
- Windows External IP in Command Line (From FSM Agent)
- Windows Java running with remote debugging
- Windows Logons By Logon type
- Windows LSASS Process Access
- Windows machines running MS WORD
- Windows malicious HTML Applications Spawning Windows Shell
- Windows Net.exe command audit
- Windows Network Connection from Suspicious Program Locations
- Windows Permission check command audit
- Windows Powershell command hiding
- Windows Powershell command usage audit
- Windows Powershell opening external connections
- Windows Registry Changes
- Windows regsvr32 command usage audit
- Windows Remote Desktop connections
- Windows Remote Thread in LSASS
- Windows Routing table modification
- Windows SSH/telnet connections to outside
- Windows Suspicious Control Panel DLL Load
- Windows suspicious driver load from Temp directory
- Windows whoami command usage audit
- Windows wmic command usage audit
- Windows wmic suspicious information retrieval

Modified Reports

The following existing reports have been modified for the 5.2.5 release.

- AppFlow: Top Applications By Bytes (Detailed)
- AppFlow: Top Applications By Bytes
- AppFlow: Top Conversations By Bytes (Detailed)
- AppFlow: Top Sources By Bytes
- AppFlow: Top Conversations By Bytes
- Windows Servers By Last Authentication Event Receive Time
- Windows Servers By Last Change Event Receive Time
- Windows Servers By Last FIM Event Receive Time
- Linux Servers By Last Authentication Event Receive Time
- Linux Servers By Last Change Event Receive Time
- Linux Servers By Last FIM Event Receive Time
- Routers/Switches By Last Authentication Event Receive Time
- Routers/Switches By Last Change Event Receive Time
- Firewalls By Last Authentication Event Receive Time
- Firewalls By Last Change Event Receive Time
- Hypervisors By Last Authentication Event Receive Time

- All PCI Systems By Last Event Receive Time
- FortiGate Top Botnets
- FortiGate Top Botnets
- FortiSandbox Top Source Country By Malware
- FortiSandbox Top Destination Country By Malware
- FortiSandbox Total Analysis Jobs
- FortiSandbox Zero Day Suspicious URLs
- FortiSandbox Zero Day Malicious URLs
- FortiSandbox Zero Day Malicious Files
- FortiGate Top Applications by Bandwidth
- FortiGate Top Websites by Connections
- FortiGate Top IPS detected Attacks
- FortiGate Top Malicious Websites
- FortiGate Top Phishing Websites
- FortiGate Top Proxy Avoidance Attempts
- FortiGate Top Protocols By Bandwidth
- GLBA 1.6.1: Top Reporting Modules Ranked By Event Rate
- ISO 27001 A.12.4.1: Top Reporting Modules By Event Rate (Per Sec)

Deleted Reports

The following report has been deleted for the 5.2.5 release:

- Carbon Black Functionality Stopped

Important Bug Fixes

Bug ID	Severity	Module	Description
564336	Minor	App Server	CSV Report Export Report with Calculations fail
570934	Enhancement	System	Remove Hail a Taxii from External Threat Intelligence source - no longer updating
561449	Minor	GUI	Non Built in admin users have session timeouts regardless of configuration
567553	Minor	Query	COUNT DISTINCT Event queries do not work on Elasticsearch
559488	Minor	App Server	Email Notification with TLS1.2 does not work
580713	Minor	App Server	Remediation script execution failed when events triggered in org level
566959	Minor	Log Collection	Azure Expect script credentials need to be obfuscated
564252	Minor	Parser	Incident Event Forwarding not working when event group is chosen in filter conditions
524946	Minor	App Server	FortiSIEM incident notification unnecessarily adds Identity And Location information to incident_detail
570780	Minor	Data Manager	Events are not cached on collector when ElasticSearch is down
524275	Minor	GUI	Quick Info and Identity Location Dashboard > SenderBase Reputation has wrong URL
556271	Normal	GUI	Incident risk entity is not showing up if user set it as home landing page
428993	Minor	App Server	PostGreSQL Incident table does not sync with time zone changes
561378	Normal	GUI	Collector fails to register collector through proxy
573744	Minor	App Server	When Organization is renamed, offline retention policy still refers to the old name
573922	Minor	Data Manager	Excessive phDataPurger loading agent info into cache log fills up disk over time
556271	Minor	GUI	Incident > Risk View does not display if user set it as home landing page. Information shows if you change tabs and come back
556525	Minor	Log Collection	Custom JDBC job: Oracle service name is not saved
564804	Minor	App Server	Incident XML export shows a negative value for Repeat Count
559241	Minor	Parser	Excessive logging during Sophos Central log collection causes disk to be full

Bug ID	Severity	Module	Description
572591	Minor	Data Manager	Incorrectly parsed binary even type attributes causes data corruption
574694	Minor	App Server	Saved search results at Organization level cannot be viewed
476419	Enhancement	GUI	User session should not timeout during test connectivity, discovery and dashboards
552531	Minor	Log Collection	Sophos Central Event pulling do not work
570234	Minor	Rule Engine	Rule does not trigger with IN condition when there are nore than 2 elements in the SET
569235	Normal	Log Collection	Used EPS information does not correctly account netflow logs
574901	Minor	Parser	Correctly set FortiGate IPS Severity based on severity field
550234	Minor	Rule Engine	Incident attributes not showing non-English characters - Non-ASCII characters displayed as '_' in incident
572800	Minor	GUI	GUI memory leak when user is switching between tabs

Known Issues in Release 5.2.5

- Search - Unable to get more than 16.38K entries in COUNT DISTINCT operations. No workaround is possible.
- Search – Many files may accumulate in the dynamic-reports folder for canceled report exports. The folder path is `/opt/phoenix/config/dynamicreports/customize-export`. The workaround is to periodically delete the files.
- FortiSIEM Collector doesn't validate the Supervisor/Worker HTTPS public certificate. No workaround is possible.
- The Default Time Range (10 days) on the Incident Explorer dashboard is too long and the user cannot change this default setting. The workaround is to change the setting to fewer days and make sure there is sufficient disk I/O to the event database for this query to return results.
- External Lookup does not pickup IPs from the external lookup request unless you specify <IP> in the URL. The workaround is to put “<IP>” in the URL.
- The Elasticsearch NOT IN query does not work with network groups with low and high. No workaround is possible, other than trying to rewrite the query.
- The Widget Dashboard drill down gives incorrect results when the report contains Protocol and Port. The workaround is to add the specific Protocol and Port conditions in the drill down query.
- FortiSIEM is unable to create a ticket from multiple incidents. No workaround is possible.
- The rule "Multiple Distinct IPS Events From Same Src" is firing on FGT non-IPS events. The workaround is to modify the rule definition by modifying the rule filter condition to ”Event Type CONTAIN FortiGate-ips-“.

- Swap partition is not created for Super, Worker, and Collector. The workaround is as follows:
  - Run the `blkid /dev/sda2` executable.
  - Take this UUID and replace the UUID for the swap partition in the `/etc/fstab` folder.
- No FortiSIEM user can delete or modify a device credential other than the user who created it. The workaround is to delete the credential from the database. It is advisable to contact ForiSIEM technical support for this operation.
- If there are lots of Cases created in FortiSIEM, then the CASES tab may take a long time to load. The workaround is to delete some old cases from the database. It is advisable to contact ForiSIEM technical support for this operation.