FORTINET

Release Notes

FortiSIEM 7.3.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

05/14/2025
FortiSIEM 7.3.0 Release Notes

TABLE OF CONTENTS

Change Log **4**
What's New in 7.3.0 ..... **5**
General 5
System Updates 5
New Features 6
Automated Supervisor High Availability 6
Advanced ClickHouse Search 6
Installation on RHEL 8.10 for FIPS 140-2 Crypto Module Support 7
Enhancements 7
Install / Upgrade Related 8
High Availability / Disaster Recovery Related 9
Analytics Related 9
FortiAI Related 10
GUI Related 11
Bug Fixes 12
Known Issues 16
Implementation Notes 17
General 17
Advanced Search Related 17
Automated HA Related 18
Collector HA Related 18
Collector VM Update Related 19
Identity and Location Related 19
Linux Related 20
Post-Upgrade ClickHouse IP Index Rebuilding 20
Upgrade Related 20

Change Log

Date	Change Description
12/13/2024	Initial version of the 7.3.0 Release Notes.
01/07/2025	Bug 1077624 added to Bug Fixes.
01/23/2025	Implementation Notes section updated.
02/28/2025	New Features - Automated Supervisor High Availability updated.
03/05/2025	Known Issues added.
03/07/2025	Known Issues - Additional information provided.
03/20/2025	Implementation Notes - Collector HA Related section updated.
05/14/2025	Upgrade Implementation for 7.2.6 added to 7.3.0-7.3.2 Release Notes.

What's New in 7.3.0

This release contains the following features, enhancements, and bug fixes.

- General
- System Updates
- New Features
- Enhancements
- Bug Fixes
- Known Issues
- Implementation Notes

If you are running 7.2.5 or 7.2.6, then you cannot upgrade to 7.3.0 because 7.2.5 and 7.2.6 contain database schema changes that are not present in 7.3.0. For 7.2.5, you must next upgrade to 7.3.1 or later. For 7.2.6, you must next upgrade to a version strictly later than 7.3.2 or to version 7.4.0 or later.

General

If you are running 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade from 7.2.5 to 7.3.0 as it was released after 7.3.0 and 7.2.5 contains database schema changes not present in 7.3.0.

System Updates

This release includes Rocky Linux OS 8.10 patches until December 6, 2024. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) have also been updated to include Rocky Linux 8.10. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

This release also updates PostgreSQL version to 16.6.

New Features

Automated Supervisor High Availability

This release introduces a new way to cluster FortiSIEM Supervisor nodes for High Availability (HA). Compared to the earlier versions, the current solution offers the following advantages:

- Failover is *automated*. When the leader node fails, another node becomes the leader. No human intervention is required.
- Cluster is *always available* even if the leader node goes down.

However, a minimum of 3 Supervisors is required, compared to 2 in earlier versions. Fault tolerance and automated failover is only possible with 3 or more nodes – see “What is failure tolerance” question in https://etcd.io/docs/v3.3/faq/.

Currently, Automated Supervisor High Availability is supported for FortiSIEM hardware appliances, ESX based deployments and AWS public cloud.

In a non-cloud setup, the nodes that are assigned a Virtual IP (VIP) must be on the same subnet. That means:

- For on-premise All-in-one Supervisor Cluster Deployments: All Supervisor-With-DB nodes must be on the same subnet.
- For on-premise Virtual Appliance Clusters: All DB Server nodes must be on the same subnet. Supervisor-Without-DB and Worker nodes can be on different subnets.

If you are running FortiSIEM HA from earlier versions, then you need to remove the prior HA, upgrade and then perform HA in the new way.

The Disaster Recovery (DR) procedure remains manual as in earlier releases.

For details on setting up HA and DR, see these documents:

- ClickHouse based deployments: High Availability and Disaster Recovery Procedures - ClickHouse
- FortiSIEM EventDB based deployments: High Availability and Disaster Recovery Procedures - EventDB

Advanced ClickHouse Search

This release enables you to run generic SQL queries against the ClickHouse event database. You can have the full power of SQL and use FortiSIEM CMDB Group in queries. Specific functionalities include the ability to:

1. Type and run any SQL SELECT query supported by ClickHouse.
2. Fix SQL syntax errors using FortiAI (needs OpenAI keys to be installed).
3. Iteratively filter query results.
4. Export and import SQL query definitions.
5. Export SQL query results in PDF and CSV formats.
6. Schedule SQL queries to run in periodic intervals and get notified of results via email.
7. Add SQL query results to dashboards.
8. Run SQL queries via API (`/phoenix/rest/query/eventQuery`). See here for details.

Currently, you **cannot** run these queries as a Scheduled Rule to trigger Incidents.

Advanced queries can be run from **Analytics > Advanced Search**. A set of 30+ built-in SQL queries are provided in **Resources > Reports > Advanced Search**.

For more information, see Advanced Search.

Installation on RHEL 8.10 for FIPS 140-2 Crypto Module Support

For highly secure environments, if you want to use only FIPS 140-2 validated crypto modules for FortiSIEM's cryptographic usage, then this release enables you accomplish this by running FortiSIEM as an application on Red Hat Enterprise Linux (RHEL) 8.10.

For detailed instructions, see here.

Enhancements

This release contains the following enhancements:

- Install / Upgrade Related
  - Enable Collector OS Update through Supervisor during Upgrade
  - Simplified Offline Upgrade for Supervisor, Workers and FortiSIEM Manager
  - Allow Users to Select Disk Sizes During FortiSIEM Install
  - Enable NFS Storage for ClickHouse Warm and Cold Tiers
  - Prompt for Collector Registration Password
  - Separate Open Firewall Ports for Supervisor, Workers and Collectors
- High Availability / Disaster Recovery Related
  - Allow rsync to be Rate Limited
- Analytics Related
  - Ability to Send Incident Notifications to Microsoft Teams
  - Support FOLLOWED_BY / NOT_FOLLOWED_BY Functions for Scheduled Rule (ClickHouse Only)
  - Enhanced Default Email Template Includes More Incident and Case Details
- FortiAI Related
  - Search Rules, Reports and Event Types Using Semantic Search
  - Fix Advance Search Syntax Errors using FortiAI
  - FortiAI Agent Improvements - Performance, Conversational Interaction
- GUI Related
  - Allow CMDB Search on Event Pulling Status, Perf Monitor Status and Agent Status
  - PDF Export for Tables with many Columns
  - Slide In for Admin > Health
  - General GUI Usability Enhancements

Install / Upgrade Related

Enable Collector OS Update through Supervisor during Upgrade

In earlier releases, Collectors performed OS Update from FortiSIEM OS Repo on the Internet during upgrade. Starting with this release, Collectors will automatically get OS Updates from the Supervisor during the standard upgrade process and there is no need for Collectors to go to the Internet during this process.

Simplified Offline Upgrade for Supervisor, Workers and FortiSIEM Manager

This release provides a simplified offline upgrade procedure for Supervisor, Workers and FortiSIEM Manager when these nodes do not have Internet access. The procedure involves the following:

1. Find another host that has internet connectivity
2. Download the FortiSIEM OS repository from that host and store it on a remote file share that can be mounted
3. Issue the upgrade command and specify the remote file share as an argument

For details, see the Offline Installation and Upgrade Guide.

Allow Users to Select Disk Sizes During FortiSIEM Install

In earlier releases, FortiSIEM required an exact disk size match to determine *opt*, *cmdb* and *svn*. However, for some situations, the user needs to choose a larger disk size for some disks. For example, a Collector intended to collect 5K-10K EPS would benefit from having a large *opt* disk to keep the parsed events. An installation with large number of devices may need a larger *cmdb* or *svn*.

This release allows user to choose their *opt*, *cmdb* and *svn* disks during the install process. Note that the following size restrictions must be satisfied for FortiSIEM to work smoothly.

- *opt* disk must be 100GB or more
- *cmdb* must be 60GB or more
- *svn* must be 60GB or more

For details, see **Configure FortiSIEM** steps in VM Guides : AWS, Azure, ESX, GCP, Hyper-V, KVM, Nutanix, OCI

Enable NFS Storage for ClickHouse Warm and Cold Tiers

Sometimes Workers may not have sufficiently large locally attached disks to store events in ClickHouse Warm or Cold tiers . This release enables the user to specify remote NFS storage for ClickHouse Warm or Cold tiers.

- **VM**: Warm and Cold tier
- **500G, 2000F, 3500G** Hardware Appliances: Warm and Cold tier
- **2000G, 2200G, 3600G** Hardware Appliances: Only Cold tier, since Warm tier is on the appliance.

For configuration information, see step 7e in Adding Workers.

Prompt for Collector Registration Password

In earlier releases, user had to enter the Collector password in the registration command. This release provides a more secure solution where user enters the password on a prompt.

The previous way to register a collector is to provide the password in the command:

```
phProvisionCollector {--add | --update} <user> '<password>' <super IP or host>
<organization> <collectorName>
```

The new way is to skip the password in the command, and enter when prompted.

```
phProvisionCollector {--add | --update} <user> <super IP or host> <organization>
<collectorName>
```

Currently, both the old and new ways work.

Separate Open Firewall Ports for Supervisor, Workers and Collectors

For enhanced security, the Supervisor, Workers and Collectors now each have uniquely separate open firewall ports. See the External System Configuration Guide Port Usage section for port usage information.

High Availability / Disaster Recovery Related

Allow rsync to be Rate Limited

For environments with a large CMDB or event database (i.e. 90-100TB using NFS), syncing across all sites can consume a significant amount of bandwidth. In order to control the bandwidth usage, *rsync* rate limit has been added as a configurable option when setting up DR in **Admin > License > Nodes > Add Secondary Supervisor**.

For details, see step 8c in Adding Secondary Supervisor Node.

Analytics Related

Ability to Send Incident Notifications to Microsoft Teams

This release adds the ability to send Incident notifications to Microsoft Teams via Webhook. This is done in 2 steps:

1. Create your Webhook Notification in **Admin > Settings > Analytics > Incident Notification**.
2. In Automation Policy, at **Admin > Settings > General > Automation Policy**, set Webhook notification as action.

Note: There is a rate limit on MS Teams notification. Tests on Fortinet accounts show that messages can be queued after 25 messages per 5 minutes. Customer is advised to test in their environment before enabling this notification method.

For information on configuring, see Define Notification Action - Email/SMS/Webhook.

Support FOLLOWED_BY / NOT_FOLLOWED_BY Functions for Scheduled Rule (ClickHouse Only)

For ClickHouse environments, you can write *scheduled* rules that detect event patterns followed by or not followed by another event pattern. Three built-in scheduled rules that uses these operators, are provided:

1. Suspicious Logon Failure without successful login – Scheduled
2. Transient Windows Account Usage – Scheduled
3. Attack Kill Chain Completion

Note that streaming mode rules already support this feature. However, scheduled rules can look for patterns over much larger intervals than that of streaming rules, since streaming mode would require more memory for large detection intervals.

Enhanced Default Email Template Includes More Incident and Case Details

The default Incident notification email template has been enhanced by adding more incident and case detail information.

FortiAI Related

Search Rules, Reports and Event Types Using Semantic Search

In previous releases, exact search is used to search for rules, reports, event types. Exact search cannot differentiate between similar words such as “logon”, “login” and “log in”. In this release, a natural language-based similarity search is provided that can return more relevant results. This is achieved via a private tuned Large Language Model that is included in the product. These requests are handled locally and do not go to OpenAI or any other public language-based search service.

Note: This requires you to check the **AI Search** checkbox during search.

Fix Advance Search Syntax Errors using FortiAI

If you encounter SQL Query syntax errors while running **Analytics > Advanced Search**, you can use **Fix with FortiAI** to fix the errors.

FortiAI Agent Improvements - Performance, Conversational Interaction

The FortiAI model has been upgraded to GPT-4o, resulting in better performance and improved language comprehension.

GUI Related

Allow CMDB Search on Event Pulling Status, Perf Monitor Status and Agent Status

In **CMDB > Devices** and **Admin > Health > Agent Health**, you can now search for the status fields:

- **Agent Status**: Status of Windows and Linux Agents: Possible values are *Register*, *Running Inactive*, *Running Active*, *Disconnected*, *Disabled*, *Hibernating*, *Shutdown*
- **Event Status**: *Normal* / *Warning* / *Critical* based on whether the logs from a device are arriving within specified delay thresholds.
- **Monitor Status**: *Normal* / *Warning* / *Critical* based on whether the performance monitoring events for a device are generated within specified delay thresholds.

Device Search will show how many devices are in each state. Once you select a state, then only the devices in that state are displayed.

PDF Export for Tables with many Columns

When a report contains more than 5 columns, PDF export automatically switches to summary mode to make the results more legible. You can also choose a Summary mode explicitly when you export a query result from Analytics.

Slide In for Admin > Health

Previously, **Cloud Health**, **Collector Health**, and **Agent Health** appeared in a subsequent table below the main table. In this release, the same information is displayed as a slide-in pane appearing from the right, like in Incident List View.

General GUI Usability Enhancements

Several GUI usability enhancements have been made.

- Informational pop-up windows will auto close after 3 seconds.
- **Actions** drop-down list available from **Incident Details** pane.
- On the **Incidents** page, some windows can now be expanded to full screen, for example, **Device Health**.
- Date Picker interface no longer requires scrolling.
- Specific Incident information can be stored for later queries by selecting **Create Filter...** as an option under certain headings like **Incident Title** or **Target** from the **Incidents** page. You can create multiple filters and the information will be stored in a scratchpad that appears in top right (). Once you click **Search** then you will be taken to **Analytics > Search** and the Filter would be auto populated. You can modify the search condition and run a query. This helper feature speeds up threat hunting process where you may want to create a query by collecting values from various places in the GUI.
- Ability to set a **Default Case Management Policy** in **Admin > Settings > General > Case Management**. When you manually create a Case from an Incident, then the default Case Management Policy will be auto populated.
- Ability to add a Case Note when you manually create a Case from an Incident.
- Ability to create Incident Comments and Case Notes in markdown format (https://www.markdownguide.org/basic-syntax/).

Bug Fixes

This release fixes the following issues *in addition* to the fixes published in FortiSIEM 7.2.4 release.

Bug ID	Severity	Module	Description
1078227	Major	App Server	**Test** and **Deploy** on ClickHouse Configuration page times out with large number of workers.
1084505	Major	Performance Monitoring	Multiple JDBC instances hosted on same server can't be monitored.
1089195	Major	Query	In high EPS environment, QueryMaster may consume significant memory to handle Summary dashboard in ClickHouse.
1087705	Major	Query	ClickHouse workers fall back to EventDB if appserver is unreachable.
1084444	Major	Rule	Disabled rules trigger incidents in Enterprise mode after upgrade.
1090576	Major	Windows Agent	OSQuery.exe invoked by the FortiSIEM Windows Agent may use up significant memory.
1095588	Minor	App Server	Malware IP update from Mirai IP list will generate a sub group each update.
1078555	Minor	App Server	Cannot remove decommissioned Windows Agent device from CMDB.
1078543	Minor	App Server	Custom threatfeed AbuseIPDB update via Python hangs when the limit is more than 2000.
1071445	Minor	App Server	ServiceNow integration - If an active incident from a previous month triggers again at the turn of the next month, a duplicate ServiceNow ticket is created.
1066669	Minor	App Server	Multiple performance issues when **CMDB > Devices** contains custom properties.
1065031	Minor	App Server	Invalid Query XML Using IF Analytic Function and renaming Display Field.
1063063	Minor	App Server	Windows Agent and LDAP discovery causes the rule to trigger - "Discovered Device Incorrectly Merged: Overlapping IP".
1057332	Minor	App Server	Users that have configured scheduled reports cannot be deleted without deleting all scheduled reports.
1054587	Minor	App Server	Adding device via public REST API (`/phoenix/rest/device/discovery/add`) does not update CMDB Group.
1050158	Minor	App Server	Username incorrectly added to the Groupname in incident title "Windows User Added to Groups" rule.

Bug ID	Severity	Module	Description
1038605	Minor	App Server	Distributing widgets to existing orgs failed after the upgrade to 7.1.4.
1071298	Minor	App Server, GUI	Implement pagination in **CMDB > Applications** on appserver side.
1061706, 1047493	Minor	App Server, GUI	For Query results exported to PDF, the table may be cut off if there are large number of columns or some values do not have separators.
1072278	Minor	Case Management	Manually closing a case does not automatically close linked incidents.
1041439	Minor	ClickHouse Backend	Display parts name when bloom filter script shows less than 10 parts left to modify.
996330	Minor	ClickHouse Backend	When running a ClickHouse query, the progress bar should more accurately reflect the query progress.
1096969	Minor	Data Work	FortiGate reports for Application Bandwidth does not return all results.
1095118	Minor	Data Work	In Win-Sysmon-3-Network-Connect-IPv4 event, IP Protocol is parsed incorrectly.
1090403	Minor	Data Work	Some Windows PrintService events are not parsed correctly with the WinOSXmlParser.
1084609	Minor	Data Work	Sigma OpenSSH rule using invalid event attribute.
1081510	Minor	Data Work	WinOSXmlParser is not able to parse the source IP and user for event Win-App-MSSQLSERVER-18456.
1080686	Minor	Data Work	Extract Direction for Windows Event 5156.
1078228	Minor	Data Work	Cisco Duo Parser not parsing User or Email Address fields.
1077696	Minor	Data Work	Difference in parsing Win-Security-4776 between OMI and XML Parser impacts Rules/Reports.
1076139	Minor	Data Work	Spelling error in description for Rule: Windows: First Time Seen Remote Named Pipe.
1075849	Minor	Data Work	WinOSXmlParser doesn't parse the Client Process ID and Parent Process ID from Event ID 4697.
1075701	Minor	Data Work	Ransomware Detected on Host rule frequently shows false positives because of excessive reads on `C:/$extend/$deleted`.
1074743	Minor	Data Work	The definition of SIGMA Rule - Windows: Service Installed By Unusual Client - System, is incorrect.

Bug ID	Severity	Module	Description
1073955	Minor	Data Work	WatchGuardFirewallParser for *-proxy does not provide a "default" clause. This causes multiple https-proxy logs for SSL termination to not match the current conditions and parsing error happens.
1043595	Minor	Data Work	"Permit Netflow" event type group is not under Permit Traffic Event Group.
1050258	Minor	Event Pulling Agents	OMI event pulling missing Event PH_DEV_MON_PROC_ RESOURCE_UTIL due to incorrect number of CPUs.
1019111	Minor	Event Pulling Agents	OMI event polling fails after winrm runs over 10 minute time frame.
1083810	Minor	GUI	Show Original First Seen Time instead of First Seen Time in Incidents page (for incidents that span multiple months).
1077627	Minor	GUI	When using "Select from CMDB" in the rule definition, duplicate objects can be added to same condition.
1069054	Minor	GUI	EventDB query - Display fields order is not maintained in Query Result table.
1045920	Minor	GUI	Wrong collector_type shows for 500F hardware collectors in **Collector Health** page.
1043594	Minor	GUI	"Add to filter" does not correctly populate port field from Raw Event Message details pop up.
1040711	Minor	GUI	For an Incident, triggered events do not show correctly for the second subpattern of a rule (if exists).
1037656	Minor	GUI	Cannot add more than 10 disks for ClickHouse Storage Tiers.
985279	Minor	GUI	Column sort does not work for "Lookup Tables" if there is an uppercase character in column name.
1068569	Minor	GUI	Queries do not work if there is a "@" character in CONTAINS or NOT_CONTAIN (e.g. reptDevName CONTAIN Device@Blah). The "@" character is not allowed.
1094019	Minor	Query	CSV export is empty if the result query erroneously goes to Secondary Supervisor.
1078348	Minor	Query	Incorrect backslash handling in event attribute values causes query failure.
1074677	Minor	Query	EventDB - Analytics Search does not work well when event attribute values contain negative integers.
1077849	Minor	System	logrotate_phoenix_hourly references old postgresql-9 version instead of current version postgresql-16.

Bug ID	Severity	Module	Description
1063359	Minor	Threat Intelligence Ingeration	OpenCTI Malware IP Threat Integration only ingests the last page of the integration.
1091528	Minor	Windows Agent	Autoupdate.log is not removed after uninstalling the Windows Agent.
1071795	Minor	Windows Agent	DISABLEPROXY setting is not carried over during auto upgrade.
1067554	Minor	Windows Agent	Agent moves to Event status critical after updating Virtual Collector entries which are not contactable.
1050753	Minor	Windows Agent	"FortiSIEM Agent Operational Error" rule triggers when an agent goes through a system reboot.
1048352	Minor	Windows Agent	Windows Agent memory leak when monitoring Windows non-security event logs.
1036250	Enhancement	App Server	Cloned System rules prepends keeps the (s) to the rule.
1011492	Enhancement	App Server	Support latest SDK v4 from Cisco Duo for External Auth.
1098215	Enhancement	ClickHouse Backend	Cannot reuse deleted workers in ClickHouse Cluster Configuration.
1019228	Enhancement	ClickHouse Backend	Add more retention periods for ClickHouse - 7 days, 14 days, 30 days, 60 days, 9 months.
1083650	Enhancement	Data Work	Parse additional Darktrace event types.
1080002	Enhancement	Data Work	Many ESX logs are not parsed.
1077624	Enhancement	Data Work	FortiRecon parser updated for new events.
1073338	Enhancement	Data Work	Update parsers for FortiGate, FortiClient and FortiMail Cloud.
1071764	Enhancement	Data Work	Update Nessus parser to use CVSS v3 Score.
1071120	Enhancement	Data Work	Source and Destination IP and usernames are not parsed for CiscoASAParser and CiscoFTDParser.
1070418	Enhancement	Data Work	PowerShell rules reference incorrect data source.
1066149	Enhancement	Data Work	Windows events with %% values are not parsed.
1062284	Enhancement	Data Work	FortiAuthenticator parser update for userip.
1062035	Enhancement	Data Work	Incorrect Logic for Rule - Windows: Windows Internet Hosted WebDav Share Mount Via Net.EXE.
1059482	Enhancement	Data Work	Need parsing updates for Windows Security Events 4768, 4769 and 4770.
1058938	Enhancement	Data Work	There should be a specific event type for Failure to initialize Event Log monitoring via Win Agent.

Bug ID	Severity	Module	Description
1058921	Enhancement	Data Work	All Lookup Table rules have Tactics and Techniques set with the same value.
1058918	Enhancement	Data Work	Description incorrect for Lookup Table: WinRDPLogin.
1058749	Enhancement	Data Work	Parsing updates for Linux Auditd, Unix, Apache, Sendmail.
1056796	Enhancement	Data Work	Win-PowerShell-4104 Parsing is missing extraction of ScriptBlockText.
1052841	Enhancement	Data Work	IPReputationSICategory is not being parsed in CiscoFTDParser.
1052726	Enhancement	Data Work	Microsoft-Windows-PowerShell/Operational is broken for new WinOSXMLParser.
1046594	Enhancement	Data Work	Update WinOSXMLParser for Event IDs 4719 and 4674.
1035408	Enhancement	Data Work	Update Dragos Parser for FortiSIEM.
1018725	Enhancement	Data Work	Parse more VM SDK events.
599020	Enhancement	Data Work	Parser update for Trend Micro Deep Security as different Syslog Header Format observed.
879197	Enhancement	Event Pulling Agents	In OKTA API, collect an additional Log Field request.ip_chain.ip.
1003246	Enhancement	GUI	In CMDB, allow filtering on Event Pulling, Perf Monitor Status and Agent Status.
995645	Enhancement	GUI	Rule Exception definition should validate definition input before saving.
983388	Enhancement	GUI	Adding Rule tags to a system defined rule should not require user to clone the rule.
842921	Enhancement	Linux Agent	Linux Agent: Allow user to choose which interface to register with and connect on.
1033090	Enhancement	Performance Monitoring	Remove attempts to access obsolete MS Exchange WMI classes that are no longer available.
1051509	Enhancement	System	Port 3000 on Supervisor is exposed when it should not be.
955729	Enhancement	Windows Agent	Add Sysmon as a default option for the Windows Agent.
869737	Enhancement	Windows Agent	Support DIR expansion variables in FIM policies. E.g. %WINDIR%, %SYSTEMROOT%, etc.

Known Issues

1. For hardware appliances, upgrade to 7.3.0 may fail because of increased root disk usage during upgrade process. It is recommended not to upgrade to 7.3.0 and wait for a fix. If you have already attempted an upgrade and it failed,

then you can remedy this by using the following steps:

a. Login to your system as root and run the following command to free up disk space on root partition.
```
rm -f /fsmopt.tar.gz
```
b. Restore your system back to the previous working release using the following procedure: Restoring Hardware from Backup After a Failed Upgrade

2. If you are running 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade from 7.2.5 to 7.3.0 as it was released after 7.3.0 and 7.2.5 contains database schema changes that are not present in 7.3.0.
3. External FortiSIEM GUI user authentication via RADIUS is not supported.

Implementation Notes

Please read these notes before installing or upgrading to FortiSIEM 7.3.0.

- General
- Advanced Search Related
- Automated HA Related
- Collector HA Related
- Collector VM Update Related
- Identity and Location Related
- Linux Related
- Post-Upgrade ClickHouse IP Index Rebuilding
- Upgrade Related

General

1. If you are running 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade from 7.2.5 to 7.3.0 as it was released after 7.3.0 and 7.2.5 contains database schema changes not present in 7.3.0.
2. External FortiSIEM GUI user authentication via RADIUS is not possible.

Advanced Search Related

For a nested SQL Query, you cannot use the attribute helper to expand non-explicit event attributes (e.g. cpuName) in *inner* SQL Queries. Currently, Attribute helper works for non-explicit event attributes in an *outer* SQL Query. Workaround is to manually modify the SQL Query to convert the non-explicit event attributes inside inner SQL Queries.

Example Nested Query:

```
SELECT
    reptDevIpAddrV4,
    cpuName,
    cpuUtil
FROM
(
    SELECT
        reptDevIpAddrV4,
        cpuName,
```

```
        cpuUtil
    FROM fsiem.events
    WHERE eventType = 'PH_DEV_MON_SYS_CPU_UTIL'
)
LIMIT 100
```

Note that `cpuName` and `cpuUtil` are not explicit event attributes. The user must modify the inner SQL as follows:

```
SELECT
    reptDevIpAddrV4,
    cpuName,
    cpuUtil
FROM
(
    WITH
        metrics_string.value[indexOf(metrics_string.name, 'cpuName')] AS cpuName,
        metrics_float64.value[indexOf(metrics_float64.name, 'cpuUtil')] AS cpuUtil
    SELECT
        reptDevIpAddrV4,
        cpuName,
        cpuUtil
    FROM fsiem.events
    where eventType='PH_DEV_MON_SYS_CPU_UTIL'
)
LIMIT 100
```

Automated HA Related

1. Automated Supervisor High Availability does not work if Supervisor has FIPS enabled. This is because ansible scripts to set up DB Cluster uses `evp_sha256` which is not enabled by FIPS.
2. When there is a DB Cluster change (for example, leader change or a new node gets added or deleted from the cluster) and you are logged on to FortiSIEM using the GUI, then the existing browser may stop working. You may need to open a new browser.
3. For Supervisor and DB nodes, if there are dot or dash characters in the host name, make sure that the host name fragment before the first dot or dash are unique. For example:
   a. db.10.10.10.1 and db.10.10.10.2 is not allowed.
   b. db1.10.10.10.1 and db2.10.10.10.2 is allowed.
   c. db-10.10.10.1 and db-10.10.10.2 is not allowed
   d. db1-10.10.10.1 and db2-10.10.10.2 is allowed.
4. It is always recommended to have at least 3 and an odd number of nodes in the Super Cluster and DB Cluster. If you have to have a 2 node DB cluster, then you will not be able to login to a Supervisor when the current DB Leader is rebooting. Refer to the etcd documentation for more information.

Collector HA Related

Collector High Availability (HA) Failover Triggers:

- Logs are sent to a VIP in VRRP based Failover - In this case, when VRRP detects node failure, then Follower becomes a Leader and owns the VIP and events are sent to the new Leader. If a process is down on a node, then

VRRP may not trigger a Failover.

- Logs sent to Load Balancer - In this case, the Load balancing algorithm detects logs being sent to a different Collector. If a process is down on a node, then Failover may not trigger.
- For event pulling and performance monitoring, App Server redistributes the jobs from a Collector if App Server failed to receive a task request in a 10 minute window.

Collector VM Update Related

If you want to replace an old collector with a new collector, then follow these steps from the provided scenario:

Suppose the Collector Col1 is registered in Org1 with IP 10.1.1.1.126. You want to replace the Collector 10.1.1.1.126 with a new Collector 10.1.1.1.128, but keep the same name (Col1) belonging to the same Org (Org1).

1. Shutdown Collector Col1 (10.1.1.1.126).
2. Run the following command in 10.1.1.1.128.

   `phProvisionCollector --update admin <cred> <Super_IP> Org1 Col1`

Identity and Location Related

If you are upgrading to 7.3.0, then please update the following entry in the `/opt/phoenix/config/identityDef.xml` file in Supervisor and Workers to get Identity and location entries populated for Microsoft Office365 events. Then restart `IdentityWorker` and `IdentityMaster` processes on Supervisor and Workers.

Pre-7.3.0 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded</eventType>
     <eventAttributes>
        <eventAttribute name="userId" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude" reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

7.3.0 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded,MS_OFFICE365_EntraID_UserLoggedIn,MS_
OFFICE365_EntraID_StsLogon_UserLoggedIn</eventType>
     <eventAttributes>
        <eventAttribute name="user" identityAttrib="office365User" reqd="yes"/>
        <eventAttribute name="srcDomain" identityAttrib="domain" reqd="no"/>
        <eventAttribute name="srcIpAddr" identityAttrib="ipAddr" reqd="yes"/>
        <eventAttribute name="srcGeoCountry" identityAttrib="geoCountry" reqd="no"/>
```

```
        <eventAttribute name="srcGeoCountryCodeStr" identityAttrib="geoCountryCode"
reqd="no"/>
        <eventAttribute name="srcGeoState" identityAttrib="geoState" reqd="no"/>
        <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
        <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
        <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude" reqd="no"/>
     </eventAttributes>
  </identityEvent>
```

Linux Related

On CentOS 9, Linux Agent may be blocked while restarting audits: "/usr/sbin/service auditd restart".

Workaround:

1. SSH as root.
2. Check if the Linux Agent is stuck by running the following command.

   ```
   ps -ef | grep 'service auditd restart' | grep -v grep
   ```

   If the result is not empty, continue to the following steps.
3. Backup auditd stop script by running the following commands.

   ```
   mv /usr/libexec/initscripts/legacy-actions/auditd/stop /usr/libexec/initscripts/legacy-
   actions/auditd/stop-ori
   ```

   ```
   cp /usr/libexec/initscripts/legacy-actions/auditd/stop-ori /usr/libexec/initscripts/legacy-
   actions/auditd/stop
   ```
4. Replace the stop command in auditd stop script.

   ```
   sudo sed -i "s|/sbin/auditctl --signal stop|killproc \$prog -TERM|"
   /usr/libexec/initscripts/legacy-actions/auditd/stop
   ```
5. Restart Linux Agent.

   ```
   service fortisiem-linux-agent restart
   ```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.3.0, then after upgrading to 7.3.0, you need to run a script to rebuild ClickHouse indices. If you are running 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.2.0, 7.2.1, or 7.2.2 and have already executed the rebuilding steps, then nothing more needs to be done.

For details about this issue, see Release Notes 7.1.3 Known Issue.

The rebuilding steps are available in Release Notes 7.1.4 - Script for Rebuilding/Recreating pre-7.1.1 ClickHouse Database Indices Involving IP Fields.

Upgrade Related

1. If you are running 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade from 7.2.5 to 7.3.0 as it was released after 7.3.0 and 7.2.5 contains database schema changes not present in 7.3.0.
2. If you encounter this error during App Server deployment part of upgrade process, then take the remediation steps below:

```
Error:

stderr: remote failure: Error occurred during deployment: Exception while loading the
app : java.lang.IllegalStateException: ContainerBase.addChild: start:
org.apache.catalina.LifecycleException: org.apache.catalina.LifecycleException:
java.lang.StackOverflowError. Please see server.log for more details
```

Remediation Step

Option 1: Increase Java stack size to 2M.

a. Login to Supervisor via SSH.

b. `su - admin`

c. `vi /opt/glassfish/domains/domain1/config/domain.xml`

add `-Xss2m` in jvm-options session:

```
<jvm-options>-Xss2m</jvm-options>
```

d. Re-run the upgrade process.

Option 2: Remove the Device to Parser association for Parsers that are towards the bottom of the Parser list, e.g. UnixParser.

a. Login to Supervisor GUI.

b. Go to **CMDB** and from the **Columns** drop-down list, add **Parser Name**.

c. If you see a Parser towards the bottom of the Parser list, e.g. UnixParser, then take the following steps:

i. Select the Device and click **Edit**.

ii. Click the **Parsers** tab.

iii. Remove the selected Parser.

d. Re-run the upgrade process.

e. Login to GUI and add back the Device to Parser association.

www.fortinet.com