Release Notes

FortiSIEM 7.4.0

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

FORTINET®

09/23/2025
FortiSIEM 7.4.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
06/10/2025	Initial version of the 7.4.0 Release Notes.
06/30/2025	Bug Fix 1104508 added to 7.4.0 Release Notes.
07/08/2025	Note about 7.3.x upgrades added to Automated FortiSIEM Cluster Upgrade section.
09/23/2025	Added Incident Attributes note to 7.4.0.

What's New in 7.4.0

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

- System Updates
- Features
- Key Enhancements
- Bug Fixes and Enhancements
- Known Issues
- Implementation Notes

1. If you are running 7.3.3 or 7.3.4, then the next 7.4.x upgrade must be 7.4.1 or later as 7.3.3 and 7.3.4 contain database schema changes not present in 7.4.0.
2. Starting with Release 7.4.0, the following attributes cannot be used as Incident Attributes in **Rule Definition** > **Step 3: Define Action** > **Incident Attribute**. These attributes may be set by FortiSIEM and may be overwritten if the user sets them. If there are user-defined rules using these attributes, then you must rewrite these rules using other attributes.

   `Event Type, Event Severity, Event Receive Time, Reporting IP, Reporting Device, Raw Event Log, Binary Raw Event Log, Event ID, System Event Category, Event Parse Status, Event Severity Category, Incident Source, Incident Target, Incident Trigger Attribute List, Event Description, Incident Detail, Incident Reporting IP, Reporting Vendor, Reporting Model, Event Type Group, Incident ID, Incident Status, Incident First Occurrence Time, Incident Last Occurrence Time, Incident View Status, Incident View Users, Incident Cleared Time, Incident Cleared User, Incident Cleared Reason, Incident Notification Recipients, Incident Ticket ID, Incident Ticket Status, Incident Ticket User, Incident Comments, Incident Resolution Time, Incident Externally Assigned User, Incident Externally Cleared Time, Incident Externally Resolution Time, Incident External Ticket ID, Incident External Ticket State, Incident External Ticket Type, Incident Notification Status, Incident Title, Event Parser Name, Incident Reporting Device, Supervisor Host Name, Raw Event Log Size, Retention Days, Reporting Country Code, Reporting Country, Reporting State, Reporting City, Reporting Organization, Reporting Latitude, Reporting Longitude, Incident Reporting Country, Incident Reporting Country Code, Incident Reporting State, Incident Reporting City, Incident Reporting Organization, Incident Reporting Latitude, Incident Reporting Longitude, First Seen Time, Last Seen Time`

System Updates

This release includes Rocky Linux OS 8.10 patches until May 28, 2025. 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.

Features

New Dashboard Framework

This release provides a new widget dashboard framework.

- A new widget layout method where the size and position of each widget can be freely chosen, and the layout can be re-arranged and re-sized. This contrasts with the fixed 3x3, 3x6 etc. format choices in earlier releases.
- A button to globally modify the report window of all widgets in the dashboard.
- Ability to modify the report definitions within the widget interface.
- Streamlined widget setting dialog.
- Gradient options for Bar charts, Tables and Single Column charts.
- Enhance Single Column chart to display multiple data points (rows) within one widget.
- Ability to save Table column width modifications by user.
- For Bar Charts: Provides Category and Value selection and Clustered/Stacked Views to display multiple Values.

Global FortiSIEM Dashboard

This release provides a custom Home Dashboard that summarizes FortiSIEM findings and Data Sources in a few important visuals. The **Risk Summary** tab shows Overall Risk for the Organization along Top Risky Devices/Users and Incident and Case Status. The **Data Source** tab shows the Reporting Devices, Agents, Event Pulling Integrations and Storage usage.

This Dashboard can be found under the **Dashboard** tab for Enterprise Deployments and Super/Global logins in Service Provider Deployments.

Automation Service

Prior to 7.4.0, when an Incident triggers, the user can run a FortiSIEM Remediation script or run a FortiSOAR Playbook via API. The FortiSOAR playbooks need to be defined on a separate FortiSOAR system.

This release enables you create and run playbooks *natively* within FortiSIEM. Additional Automation Service license is needed to enable this feature. After deploying the license, you need to provision the Automation Service. Then you need to assign Automation Read/Modify/Execute Role to FortiSIEM users. Full admin user has Automation Read/Modify/Execute Role. User with Modify role can create and edit playbooks. User with Execute Role can execute playbooks, either directly from an Incident or by creating an Automation Policy. Playbooks are executed via Automation

Agents included with Supervisor and Collectors. On a Supervisor node, Automation Agent is automatically configured during Automation Service provisioning. On Collectors, user will need to manually install Automation agent from FortiSIEM GUI.

To provision, see here.

To create an Agent on a Collector, see here.

To create a playbook, see here.

To execute playbooks on an Incident, see here.

To execute playbooks via Automation Policy, see here.

Note: The FortiSIEM Automation Service is in Beta, with planned general availability in early Q3 2025. Contact your Fortinet or partner account manager for updates.

Rules using Advanced Search

Advanced Search feature in Release 7.3.0 enabled users to run complex SQL queries on ClickHouse events, CMDB Groups, CMDB Custom Device Properties and Lookup Tables. These queries can now be scheduled as a Rule to run periodically and create Incidents. You can quickly create a Schedule Rule after running an Advanced Search. Alternatively, you can create a Schedule Rule from scratch from **Resources > Rules**. The Filter and Group By condition in a traditional Rule is replaced by an Advanced Search SQL Query.

This feature works in ClickHouse deployments. Also Scheduled Rules can only be written from Super/Global accounts in Service Provider deployments.

Four system defined Advanced Search Rules are provided. They can be found under **Resources > Rules** by searching for **Evaluation Mode** set to **Scheduled SQL**.

- Spike in Events from a Host
- Spike in Unknown Events from a Host
- Spike in inbound denied network traffic to a destination host
- Spike in outbound denied network traffic from an internal host

For details on creating an Advanced Search Rule from Advanced Search, see here.

For details on creating an Advanced Search Rule from **Resources > Rules**, see here.

Incident Tags

This release includes a set of system defined Tags and associates them to built-in Rules. User can create their own Tags and associate them to Rules and optionally disable the system defined Tags. Incidents and cases display the currently enabled Tags for the associated Rules. User can search Rules, Incidents, and Cases by Tags. When a rule is selected under **Resources > Rules**, the Summary sidebar shows all linked tags under **Tags**.

To view all existing tags, navigate to **Admin > Settings > Analytics > Rule Tags**.

To add a tag for a Rule, go to **Resources > Rules > Edit > Define Action > Tag**.

Advanced Search Queries using FortiAI

This release enables users to write queries in natural language and ask FortiAI to generate the formal Advanced Search SQL query. This approach has some limitations for creating very complex SQL queries. See Creating a Query through FortiAI for detailed steps.

Incident Categorization using FortiAI

This release enables you to categorize Incidents occurring in a specific time intervals. For example, High CPU, Memory, Disk issues are categorized as Resource issues; various Login related issues are categorized as Access Issues. This rule similarity-based Categorization provides a way to get a big picture summary of all the all the Incidents triggering in your environment. Depending on your environment, potentially thousands of Incidents can easily boil down to tens of groups.

Incidents > List by Category (FortiAI) shows the Incident Categories for the selected period. You can drill down into each Category to see the related Incidents. A Risk score for the whole Category is provided.

By selecting **List by Category (FortiAI)** on the **Incidents** page, the user is provided with categorized incident groups containing incidents organized by semantic similarity, listed in order of a generated evaluated severity score. To view the incidents under the incident category, click ⌄ to expand the Incident group.

Generate Query Result Analysis using FortiAI

After running a report, you can use FortiAI to do a statistical analysis of the report results:

1. Categorical Column Analysis
2. Categorical Column Pair Frequency Analysis
3. Statistical Measures for Numerical Columns
4. Anomalies Detected
5. Correlation Between the Continuous Columns

This analysis can be invoked from **Analytics > Search > Actions > FortiAI > Summarize**, **Analytics > Advanced Search > FortiAI > Summarize Results**, and **Analytics > Machine Learning > Actions > FortiAI > Summarize**.

Support Azure OpenAI for FortiAI

FortiSIEM now supports Azure OpenAI for running FortiAI analysis.

For information on configuring Azure OpenAI services for FortiAI, see here.

For information on configuring Azure OpenAI on FortiSIEM, see Configuring FortiAI here.

Automated FortiSIEM Cluster Upgrade

Prior to this release, it is possible to upgrade the FortiSIEM Supervisor HA/DR Cluster by running one script. This release extends this automated upgrade by including the Worker nodes. So the entire Supervisor and Worker node cluster for both HA and DR scenarios can be upgraded by running one script.

Users running FortiSIEM 7.3.2 can use this upgrade method.

> ⚠ If you are upgrading from 7.3.x to 7.4.0 and have worker nodes in the cluster, ensure that the HA User Public Key on the licensed Supervisor is propagated to all other nodes by following the steps here first.

To run this cluster upgrade, run this command from the Licensed Supervisor node

```
python fsm_cluster_upgrade.py
```

Nodes are upgraded in the following order

1. Licensed Supervisor
2. All Primary Nodes running PostGreSQL Database
3. Secondary Supervisor
4. All Primary Supervisor nodes without PostGreSQL Database
5. Primary Worker nodes
6. Secondary Worker nodes

First, the licensed Supervisor node will be upgraded. Then the node will reboot, and remaining nodes will be upgraded from this node in the order specified above.

Upgrade Status of various nodes can be found in this file on the Licensed Supervisor node

```
/var/tmp/upgrade_status_management.json
```

Upgrade logs can be found in this file on the Licensed Supervisor node

```
/var/log/fsm_cluster_upgrade.log
```

Key Enhancements

General Enhancements

1. Support RADIUS for GUI external authentication.
2. IP/Domain/Hash Reputation check from VirusTotal now uses VirusTotal v3 API
3. FortiSIEM installation on XEN Server
4. Two new Search Filter operators are added for ClickHouse deployments - STARTS_WITH and NOT STARTS_WITH
5. Security Enhancement: On these ports TCP 7900-7950,27900-27950 only FortiSIEM Supervisor and Worker nodes can communicate. For example, a random node cannot communicate to Supervisor or Worker on TCP port 7900-7900-7950,27900-27950.
6. Audit logs are added for Org rule activation/deactivation: PH_AUDIT_RULE_ACTIVATED and PH_AUDIT_RULE_DEACTIVATED

ClickHouse Enhancements

1. In ClickHouse, events in Hot, Warm, Cold and Archive partitions must maintain time order. This means Archives events must have earlier timestamp than Cold events, Cold events must have earlier timestamp than Warm events, etc. This condition may be violated when a new (Replica) Worker is added to a Shard, and there is another Worker in the shard with data. This situation may result in performance degradation and more importantly, newer data may be incorrectly archived or purged.

   In this release, FortiSIEM detects this situation and

   - A GUI system error (ClickHouse Partitions Order: ClickHouse data partitions are not in order) is generated.
   - A log: ClickHouse data partitions are not in order (PH_CLICKHOUSE_DATA_PARTITIONS_OUT_OF_ORDER) is generated.

   When this happens, you need to run this command on the node with out-of-order issue:

   ```
   /opt/phoenix/bin/clickhouse-rebalance-partitions
   ```

   The GUI system error (ClickHouse Partitions Order: ClickHouse data partitions are not in order) should go away.
2. Two rules are created when a ClickHouse shard is unbalanced (more than 10 GB difference).
   a. FortiSIEM Inter-shard ClickHouse Storage Gap High
   b. FortiSIEM Intra-shard ClickHouse Storage Gap High

Dashboard Enhancements

- Modified Dashboards
- New Dashboards

FortiSIEM 7.4.0 has revamped most default system dashboards and added a few new ones. The layout has been improved, and update report data feeding widgets have been updated for accuracy.

Modified Dashboards

- Application Server Dashboard
- AWS Dashboard
- Database Dashboard
- FortiSIEM Dashboard
- Fortinet Security Fabric Dashboard

  Notes:
  - SaaS based product dashboard tabs moved to Fortinet Cloud Security Dashboard
  - Merged FortiGate/FortiProxy dashboards together
- GCP Dashboard
- Google Workspace Dashboard
- Mimecast Dashboard
- Network Dashboard
- Nutanix Dashboard
- Office365 Dashboard
- Oracle Cloud Dashboard
- Salesforce Dashboard

- Security Dashboard
- Server Dashboard
- Trend Vision One Dashboard
- VMWare Dashboard
- Web Server Dashboard

New Dashboards

Dashboard	Description
Crowdstrike Dashboard	This dashboard is fed by the following integrations: • Falcon Streaming API
Microsoft Azure Dashboard	This dashboard is fed by the following integrations: • Entra ID audit event forwarding to Azure Event Hubs • Defender XDR (Advanced Hunting Events) forwarding to Azure Event Hubs
Microsoft Windows Dashboard	Windows now has a dedicated dashboard separate from the Server dashboard. This dashboard is fed by the following integrations: • Windows Agent or WMI/OMI Event Pulling
Fortinet Cloud Security Dashboard	This dashboard contains tabs for the following SaaS based products: **FortiCNAPP (New)** This dashboard is fed by the following integrations: • AWS_SQS integration (FortiCNAPP uses event bridge to publish events to SQS for consumption) **FortiNDR Cloud (Moved from Security Fabric Dashboard)** This dashboard is fed by the following integrations: • FORTINDR_CLOUD api integration + optional S3 bucket for signals, devices, and sensor data **FortiRecon - Moved from Security Fabric Dashboard** This dashboard is fed by the following integrations: • FORTIRECON_API dedicated event pulling integration or Generic HTTPS poller integration **FortiDLP (New)** This dashboard is fed by the following integrations: • FORTIDLP_STREAMING_API
OT/IOT Dashboard	This dashboard contains the following new tabs: **Armis** This dashboard is fed by the following integrations: • Armis Centrix Rest API or Syslog **Nozomi Scada Guardian** This dashboard is fed by the following integrations: • Nozomi Appliance API for Asset Discovery (CMC or SCADAGuardian) Syslog from Nozomi Appliance (CMC or SCADAGuardian)

Rules and Reports

Changes to Rules and Reports, which include new, modified, and deleted rules and reports, from FortiSIEM 7.3.0 to FortiSIEM 7.4.0 are provided as .csv files

See here for rule changes.

See here for report changes.

REST API Enhancements

For details, logon to the Fortinet Developers Network (https://fndn.fortinet.net/index.php?/fortiapi/2627-fortisiem/).

1. Risk Score

   Risk information is added to response of the following APIs.

   `/rest/context/ip`

   `/rest/context/hostname`

   `/rest/context/user`

2. New Case API

   The following APIs are added.

   a. Get Analysts - `GET pub/case/analysts`
   b. Create a Case - `POST /pub/case`
   c. Update a Case - `PUT /pub/case/{caseId}`
   d. Upload Attachment to a Case - `POST pub/case/{caseId}/attachment`

3. New Entity Reputation API

   The following APIs provide reputation for an entity, based on information available in FortiSIEM and external threat intelligence lookups. In GUI, the information is available in **Incidents > List View**, by selecting an incident and viewing the **Threat** tab in the Incident slide in.

   `/pub/reputation/ip/{ip}`

   `/pub/reputation/domain/{domain}`

   `/pub/reputation/url{url}`

   `/pub/reputation/hash{hash}`

4. Enhanced Triggering Event API

   Prior to 7.4.0 release, the following API returned the list of incident triggering events in a synchronous manner. The caller had to wait for the response containing the triggering events.

   `/pub/incident/triggeringEvents?incidentId={id}&timeFrom={from}&timeTo={to}`

   In this release, a new API is introduced that returns the `queryId`.

   `/pub/incident/triggeringEvents/start?incidentId={id}&timeFrom={from}&timeTo={to}`

   The caller then uses the `queryId` to get progress.

   `/pub/incident/triggeringEvents/progress/{queryId}`

   When progress reaches 100%, the caller gets the triggering events.

   `/pub/incident/triggeringEvents/result/{queryId}`

GUI Enhancements

1. In **Incidents** tab:
    a. **Incidents Overview** page is re-designed.
    b. **Incidents List View > By Device** and **By Rule** are re-designed.
    c. In the **Explorer** page, the Incident, Host, IP and User areas are paginated to support many entries without losing performance.
    d. In the **List View**, a Related Incidents column is provided showing the count of Related Incidents. An Incident is related to the main Incident if it has same IP or host name as the main Incident or has the same IP or host name as another related Incident. Clicking the **Related Incidents** column takes you to a tab in the right slide-in that shows a timeline view of all the Related Incidents.
    e. The **Investigate** action provides a graphical view of all Related Incidents and you can play the Incidents in time ordered manner to gather more Insight into the Related Incidents.
    f. The **FortiAI Incident Analysis** is sharpened to create a timeline analysis of the Related Incidents, identify the attack chain, root cause and provide remediation suggestion.
    g. **Investigation View** is streamlined to have only 1 informational slide in display.
    h. Raw logs in JSON and XML are formatted to show the document structure.
    i. Visualization added for Sudden User Location Change Incident to show the activity on a Geo Map.
2. In **Resources** tab, Rule and Report Search are enhanced to have same functionality as Incident Search, Case Search and CMDB Search.
3. In **CMDB** tab:
    a. CMDB Search is streamlined.
    b. A Global view of all devices across all Organizations is provided.
    c. Two metrics are provided for Active and Inactive Devices. A device is considered Active if either Event Status or Monitor Status is Normal or Warning. A device is considered Inactive if both Event Status and Monitor Status are Critical. You can click these metrics to get a filtered view of the related devices.
    d. Tooltip to explain Device Event Status and Monitor Status.
4. New CMDB Report Categories
    a. Case Report
    b. Risk Report
    c. Agent Policy and Status

Device Support

- Omicron
- Armis Centrix– Discovery, log collection
- Fortinet Lacework FortiCNAPP (Cloud-Native Protection Platform) – Log collection
- Fortinet FortiDLP – Log collection
- Cloudflare

Windows Agent 7.4.0 Updates

1. Windows Agent no longer needs the Windows .NET Framework.
2. The osquery version is upgraded to 5.14.1.
3. User log monitoring now monitors a file, even if it is created after the policy is applied.
4. Agent discovery correctly populates **CMDB > Applications > Running On**.

Bug Fixes and Enhancements

This release contains all the bug fixes in 7.3.2. In addition, the following bugs are resolved in this release.

Bug ID	Severity	Module	Description
1165944	Major	App Server	With more than 10 Workers, Content Update on Workers stops at 10 Workers and does not finish on the other Workers.
1133459	Major	App Server	Optimize Appserver code to handle REST API calls requesting system configuration data (ph_sys_conf table). This can lead to slow database calls.
1132585, 1125877	Major	App Server	Sometimes failed to delete Org from GUI due to foreign key constraint errors.
1108212	Major	App Server	Optimize CMDB Device Property for multiple devices. Sometimes, GUI may become unusable if user attempts this operation.
1151227	Minor	App Server	After upgrading to 7.3.2, Custom Parsers and Custom Event Attributes become inactive.
1144975	Minor	App Server	External authentication based on Duo Security 2FA is not working for FSM Manager after upgrading to 7.3.2.
1142200	Minor	App Server	Rule Exception does not work when symbols such as single quote and period are included in Value field.
1138152	Minor	App Server	Cannot delete an Organization when a report has been scheduled for an organization.
1126988	Minor	App Server	Issue in adding STM performance monitoring job because collectorID is null.
1125874	Minor	App Server	Incident export to PDF may fail if incident Detail contains special characters.
1125575	Minor	App Server	Sometimes, Health status fails to show because of 255 character size limit.
1122238	Minor	App Server	ServiceNow integration fails when there is a space in the beginning of Host/URL.

Bug ID	Severity	Module	Description
1114813	Minor	App Server	HTTP 403 Error on the GUI when changing local user password.
1110449	Minor	App Server	In Summary Dashboard, the metrics do not show if you add columns from PH_DEV_MON_NET_INTF_UTIL, PH_DEV_MON_EC2_MET.
1104846	Minor	App Server	Deleting one collector from the org in Collector HA group causes log ingestion failure from other collectors in the HA Group.
1100102	Minor	App Server	CMDB report 'Rules with Exceptions' displays wrong result on the exported PDF of report bundle.
1046719	Minor	App Server	Sometimes, Analytics query with custom attribute shows 'Invalid query XML' . This happens after you delete duplicate custom event attributes.
796599	Minor	App Server	Missing Rule audit events when editing/activating/deactivating multiple rules.
1126533	Minor	ClickHouse Backend	Query does not work if rawEventMsg is longer than 64KB.
1091275	Minor	ClickHouse Query	Advance queries throw DB exception error when ClickHouse function is base64 encoded.
1087970	Minor	ClickHouse Query	Queries using empty Lookup table returns no data.
1141199	Minor	Data work	For FortiDeceptor Parser, set ReportingDevice correctly (instead of always 'local') and parse more event types.
1074586	Minor	Data work	Windows parser assumes that by default, destIp/destName for all events is the reporting device.
1062372	Minor	Data work	Rule: Domain Controller User or Group Modification maps to incorrect MITRE Technique.
1149252	Minor	Event Pulling Agents	Akamai Connected Cloud Test connectivity failed.
1139082	Minor	Event Pulling Agents	More than one event pulling update tasks may be created after test connectivity with cloud service credential.
1135719	Minor	Event Pulling Agents	Duplicate logs from FortiEDR via Generic Log API Poller (HTTPS_ADVANCED) Integration.
1086809	Minor	Event Pulling Agents	Sometimes same FortiRecon events are pulled repeatedly using FortiRecon API.
1083580	Minor	Event Pulling Agents	Office365 event pulling does not report status when Supervisor or Collector is unable to reach manage.office.com.
1151469	Minor	GUI	FortiAI anonymization failed in certain cases.

Bug ID	Severity	Module	Description
1142995	Minor	GUI	For Credential > Event Hub - Consumer Group - allow $ character.
1131997	Minor	GUI	Dashboard access can't be restored to User if the User deletes dashboard which is owned by another Owner.
1120672	Minor	GUI	Analytic results > Trend chart when SHIFT+CLICK and select a region does not use the correct time.
1120184	Minor	GUI	Queries with filter System event category = 1 show 100k rows max even if configured to 200k.
1108565	Minor	GUI	HTTPS ADVANCED Log API polling does not save 'Right Key Value Postfix'.
1106420	Minor	GUI	Testing in Admin > Settings > Scheduled Report > Scheduled Report Copy shows failure even if it succeeds.
1079963	Minor	GUI	Incident view by Time no longer has a direct column to display the 'Case User'.
1142595	Minor	Linux Agent	User is unknown in Linux agent file monitoring events for Debian 12.
1098535	Minor	Linux Agent	Adding an invalid IP Address to Collector Cluster config will cause Linux agent status to be DISCONNECTED, even if the address is later removed.
1150034	Minor	Parser	Event forwarding truncates raw log message to 4KB. The new limit is 64KB.
1141840	Minor	Parser	Unnecessary PH_SYSTEM_DROP_UNKNOWN_ORG log is generated for custId = 0, 2, 3.
1137164	Minor	Parser	For Windows Event Forwarding (WEF) forwarded events, hostname in CMDB is not correct.
1132073	Minor	Parser	Some FortiGate event type groups are incorrect.
1092900	Minor	Performance Monitoring	SNMPv3 Discovery of FSM nodes does not collect disk, running processes, and memory.
1091299	Minor	Performance Monitoring	No Ping monitoring events from Hosts running Windows Agent.
1132630	Minor	Query	ClickHouse Queries fail when a searched value contains backslash (e.g. an URL).
1104508	Minor	Query	For EventDB, Analytics Queries may not return full results if for some reason, event size is large (> 64KB).
1140285	Minor	Rest API	Improve the performance of '/phoenix/rest/pub/incident/triggeringEvents' API.
1144647	Minor	System	Remediate Virtual Machine doesn't work.

Bug ID	Severity	Module	Description
1143648	Enhancement	App Server	Admin > Setup > Discovery page takes long time to display when there are too many entries. Solution is to have a paginated display.
1125911	Enhancement	App Server	Enable Summary mode display for triggering events in Incident PDF export.
1056708	Enhancement	App Server	Add Audit logs missing for org rule activation/deactivation. The new audit logs are PH_AUDIT_RULE_ACTIVATED and PH_AUDIT_RULE_DEACTIVATED.
1086559	Enhancement	App Server,GUI	Remove support of Cisco Talos Threat Feed as it requires paid credential.
1152381	Enhancement	Data work	Additional parsing and categorization for some Office365 events.
1149871	Enhancement	Data work	Admin user performing operation for Windows Event ID 4729, 4733, 4762 not parsed in event.
1148519	Enhancement	Data work	BindDNS Parser fails to recognize certain Logs, defaulting to BIND_DNS_Generic.
1147127	Enhancement	Data work	Improve parsing for Windows Security EventID 4698.
1145905	Enhancement	Data work	Certain FortiGate Event Types are mapped to wrong Event Type groups.
1145265	Enhancement	Data work	Parse 'forwardedfor' values for FortiGate logs.
1144482	Enhancement	Data work	New Device support, Omicron - OT.
1142157	Enhancement	Data work	For some Cisco ASA event types, full CN user is not parsed.
1140318	Enhancement	Data work	Parse additional VMware NSX events.
1140268	Enhancement	Data work	Enhance FortiAuthenticator parser to parse new logs with userip to determine impossible travel auth issues.
1139855	Enhancement	Data work	Rule: Logon Time Restriction Violation Needs Update for Win 2012+ Events.
1137184	Enhancement	Data work	For Office365Parser, parse the hostName attribute using the value for DisplayName from DeviceProperties.
1136161	Enhancement	Data work	Additional Palo Alto events need to be parsed.
1135070	Enhancement	Data work	FortiNAC Parser update to handle negative event IDs.
1134213	Enhancement	Data work	Parse additional Cisco IronPort Mail Gateway logs.
1134179	Enhancement	Data work	Support Azure Entra via Event Hub and Add Azure Dashboard.
1127528	Enhancement	Data work	Enhance McAfeeAVParser to parse more ePO events.
1124679	Enhancement	Data work	Parse organization field in FortiEDR events.
1124533	Enhancement	Data work	Some Citrix NetScaler events are not parsed correctly.

Bug ID	Severity	Module	Description
1123888	Enhancement	Data work	Cisco ASA and FTD - parse more unknown events.
1120259	Enhancement	Data work	SonicwallFirewallParser fails when the 'pri' attribute is missing.
1118794	Enhancement	Data work	Few Cisco NX-OS events cannot be parsed using Cisco NX-OS parser.
1116622	Enhancement	Data work	Support syslog for Barracuda Email Gateway Defense.
1093756	Enhancement	Data work	SophosCentralParser incorrectly parses attributes like UserName/AppName/Action/RuleNam into a single attribute 'Notification Action Name'.
870123	Enhancement	Data work	RFE: Support Microsoft-IIS-Configuration/Operational Event Log.
772351	Enhancement	Data work	RFE: Create Windows Rule for CrashOnAuditFail Change.
1129725	Enhancement	Device Support	OPNsense Firewall log collection via Syslog.
1129687	Enhancement	Device Support	FortiCNAPP log collection via API.
1129685	Enhancement	Device Support	FortiDLP log collection via API.
1129301	Enhancement	Device Support	Dell PowerSwitch - discovery, availability monitoring and performance monitoring support.
1056393	Enhancement	Device Support	New device support, Armis integration (OT device).
1080747	Enhancement	Discovery	Interfaces with APIPA IP addresses are not discovered though snmpwalk.
1129306	Enhancement	Discovery, Performance Mo nitoring	New device support, FS Switch - discovery and performance monitoring.
1140871	Enhancement	Event Pulling Agents	For HTTPS Advanced Poller, need to support Offset and Limit pagination via HTTP body. Current support is via URL parameter.
1131523	Enhancement	Event Pulling Agents	Add new log collection for Sophos Central API via client id and secret.
1126981	Enhancement	Event Pulling Agents	For Windows log pulling, enable OMI to use port 5986 (HTTPS) when winrm over HTTPS is enabled.
1095356	Enhancement	GUI	GB per day License is not highlighted as a Warning or Red when expiration date is close.
1088383	Enhancement	Linux Agent	Enable Linux Agent install on Ubuntu 14.04.
1045746	Enhancement	Linux Agent	Enable Linux Agent install on LXC (Debian host with Ubuntu container).
1030922	Enhancement	Parser	Enhance NetFlow parser to parse BGP AS numbers.
988033	Enhancement	Report	For Incidents not yet cleared, Incident Cleared Time shows as 0 in exported PDF/CSV.

Bug ID	Severity	Module	Description
1137882	Enhancement	System	Support FortiSIEM installation on Fortinet Integrated Openstack.
1026119	Enhancement	Windows Agent	No FIM events for files stored on ISCSI drive.

Known Issues

1. For Rules written using Advanced Search, the column re-name as part of the SQL function AS needs to begin with a character (a-z, A-Z) and contain only alphanumeric characters.
2. In the enhanced Search functionality for Rules, Reports and CMDB Devices, Search and Filtering do not work together. That means, if you have filters set and then you do a Search, the Filters will be ignored.
3. You cannot set the phRecvTime attribute in custom parsers. That attribute records the time when an event is first received by FortiSIEM, and is a special attribute that key FortiSIEM functionality depends on.
4. If you are running an HA+DR environment, and you have failed over to DR site and promoted the DR site to Primary, then you cannot run the Automated Cluster Upgrade on the DR Supervisor. Your choices are
   - Bring back the original Primary, fail back, and then run Automated Cluster Upgrade on the original Primary.
   - If original Primary is not recoverable, then do the node-by-node upgrade on new Primary site.
5. Automation Service does not work when FIPS is enabled.
6. Upgrade from FortiSIEM 6.1.0 to 7.4.0 requires 32GB memory on Supervisor. If you are running FortiSIEM 6.1.0 and have less than 32GB of memory on Supervisor, then increase the memory to 32GB and then upgrade to 7.4.0.

Implementation Notes

Please read these notes before installing or upgrading to FortiSIEM 7.4.0.

- Collector HA Related
- Identity and Location Related
- Linux Agent Related
- Post-Upgrade ClickHouse IP Index Rebuilding
- Upgrade Related

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.

Identity and Location Related

If you are upgrading to 7.4.0, 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-7.4.0 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>
```

7.4.0 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 Agent Related

If you are running Linux Agent on Ubuntu 24, then Custom Log File monitoring may not work because of App Armor configuration. Take the following steps to configure App Armor to enable FortiSIEM Linux Agent to monitor custom files.

1. Login as root user.
2. Check if `rsyslogd` is protected by AppArmor by running the following command.

   ```
   aa-status | grep rsyslogd
   ```

   If the output displays `rsyslogd`, then you need to modify AppArmor configuration as follows.
3. Verify that the following line exists in the file `/etc/apparmor.d/usr.sbin.rsyslogd`

   ```
   include if exists <rsyslog.d>
   ```

   If it does not, then add the above line to the file.
4. Create or modify the file `/etc/apparmor.d/rsyslog.d/custom-rules` and add rules for the monitored log file as needed.

   Examples:

   If you want to monitor `/testLinuxAgent/testLog.log` file, then add the following line that allows rsyslogd to read the file:

   ```
   /testLinuxAgent/testLog.log r,
   ```

   Always add the following line that allows rsyslogd to read the FortiSIEM log file. This is needed:

   ```
   /opt/fortinet/fortisiem/linux-agent/log/phoenix.log r,
   ```
5. Run the following command to reload the rsyslogd AppArmor profile and apply the changes above.

   ```
   apparmor_parser -r /etc/apparmor.d/usr.sbin.rsyslogd
   ```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.4.0, then after upgrading to 7.4.0, 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.x, or 7.3.x 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

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.

1. Login to Supervisor via SSH.
2. `su - admin`

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

   add `-Xss2m` in jvm-options session:

   `<jvm-options>-Xss2m</jvm-options>`
4. 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.

1. Login to Supervisor GUI.
2. Go to **CMDB** and from the **Columns** drop-down list, add **Parser Name**.
3. If you see a Parser towards the bottom of the Parser list, e.g. UnixParser, then take the following steps:
   a. Select the Device and click **Edit**.
   b. Click the **Parsers** tab.
   c. Remove the selected Parser.
4. Re-run the upgrade process.
5. Login to GUI and add back the Device to Parser association.

FORTINET®

www.fortinet.com