Release Notes

FortiSIEM 7.5.0

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

02/27/2026
FortiSIEM 7.5.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
12/23/2025	Initial version of the 7.5.0 Release Notes.
02/27/2026	Reference links added for Agentic FortiAI Chat and Agentic Incident and Case Investigation.

What's New in 7.5.0

This release includes the following features and enhancements.

It is recommended to read the Implementation Notes before proceeding to Install or Upgrade to this version.

Features

High Availability across Data Centers

This release enhances the High Availability (HA) functionality introduced in 7.4.0 by allowing the Supervisor nodes to be in different Data Centers, so long as the latency between Data Centers is lower than a threshold (30 milliseconds). This solution does not need Virtual IP (VIP) or DNS configuration, and the same solution works in both on-premises and cloud deployments.

This feature was introduced in 7.4.1. If you are running pre-7.3.0 version and running High Availability with manual failover, then you need to delete the Follower nodes and do a new HA Deployment. If you have deployed automated HA introduced in 7.3.0, then upgrade will automatically convert to the new HA setup. If you are running 7.4.1 or later, then you can normally upgrade to 7.5.0.

For details about HA Configuration and upgrade options, see here.

Note: Disaster Recovery (DR) is discontinued from this release onwards. If you are running DR, then you need to delete the DR node and use the new HA solution for DR.

Federated Search (ClickHouse Deployments Only)

This release allows you to search for specific observables (IP, hosts, hash, process, URL etc.) in external datastores. The following external datastores are supported: AWS Security Lake, AWS S3 Buckets, FortiEDR and Relational databases: PostgreSQL, MySQL and Snowflake.

To run a Federated Search, you have to first define a Provider with access credentials, and then define datastores (tables) for that Provider. You also need to create mappings from FortiSIEM observables to external datastore columns. Then you can perform a Federated Search. You can also pivot from **Incidents** and **Analytics** to Federated Search and hunt for matching observables in external datastores. The search results can be exported in a PDF and emailed or attached to Cases.

After you perform the search, the results are stored in ClickHouse, and you can perform more complex searches using Advanced Search.

For information on creating a Provider and datastore, see here.

For information on attribute mappings, see here.

For information on using Federated Search, see here.

Event Tagging

In current releases, events are automatically enriched with IP geo-location data. This release enhances this concept by allowing you to set any additional attributes for events that are not necessarily present in the events. The newly set event attributes are often generally referred to as Tags.

Event Tagging can be accomplished in two ways:

- Policy Based Event Tagging: By writing tagging rules using event attributes.
- File Based Event Tagging: By using tagging information from files.

Example of policy-based tagging

- If Source IP between 10.1.1.0 and 10.1.1.255, then set Department = Engineering
- If Source IP between 10.1.2.0 and 10.1.2.255, then set Department = Research

Example of file-based tagging

First, you need to upload a file (say test.csv) with 2 columns – **IP** and **Department**. Then you create a policy:

- If **Source IP** in event matches the **IP** column in file **test.csv**, then set **Department** in event to **Department** column in the file (test.csv).

You can define event tagging policies from the GUI. When deployed, these definitions are pushed down to the Collectors. When a Collector parses an event, it applies the policies and sets the event attributes as dictated by the policies.

The newly set event attributes via Event Tagging can be directly referred to in rules and reports, just like regular event attributes.

Steps for creating Event tagging policies are here.

ClickHouse Storage Region

Before Release 7.5.0, when a Collector or an external device sends events to a (Event Upload) Worker, that worker will distribute events to all ClickHouse Data Nodes. Starting with Release 7.5.0, you can have storage separation, meaning that events from specific collectors/devices can be stored in specific ClickHouse Data Nodes, with no overlap.

To accomplish this:

1. You need to form ClickHouse Regions. Each ClickHouse Region must include one or more Event Upload Workers and one or more ClickHouse Shards. Event Upload Workers and ClickHouse Shards must be non-overlapping across ClickHouse Regions.
2. You need to configure a Collector or an external device to send events to any Event Upload Worker of the region.

For steps on creating a ClickHouse Storage Region, see here.

For steps on forwarding events from a Collector to the ClickHouse Storage Region without a load balancer, collectors must specify the event worker IP addresses, in the Collector configuration - see here.

If there is a load balancer between Collector and Workers, then you have to configure the load balancer to forward events to the Workers in the Storage region.

Agentic FortiAI Chat

This release enhances the FortiAI Chat Agent by employing two technologies.

- Model Context Protocol (MCP) Service for PostgreSQL and ClickHouse databases. MCP is an open-source standard for AI to securely access data sources.
- WebSocket between FortiAI and the Generative AI module.

MCP allows users to ask any question. The MCP service understands the database schema and will convert the question to working SQL queries and convert the response using LLM l before showing it to the user. This replaces the targeted FortiSIEM API used in earlier releases.

WebSocket communication enables FortiAI to stream the response to the user.

In addition, FortiAI Agent is now conversational. You can ask a follow-up question to a previous question. To begin a new conversation, simply close the FortiAI popup and start a new one.

For details, see here.

Agentic Incident and Case Investigation

This release introduces Agentic Incident Investigation. Users can provide a set of prompts, and FortiAI will investigate the Incident using the prompt. It begins by creating a plan, then executes the plan step by step by running queries, with the final objective to determine whether the incident is a true or false positive and identify its root cause. The prompts can be saved for a rule and executed for the next incident. A set of built-in prompts are provided.

For details of Incident Analysis, see here.

For details of Case Analysis, see here.

API Token for Public REST API

Currently public REST API calls authenticate to FortiSIEM using username and password. In this release, more secure OAuth Token based authentication is introduced. Instead of creating user name and passwords, user needs to create an OAuth Token in FortiSIEM GUI and use that token in the API. Internal REST APIs use OAuth Token, while public REST API calls can use either username and password or OAuth Token for backward compatibility. Username and password support for public REST API calls may be deprecated at a future date.

Steps for creating OAuth Token are here.

Examples for using OAuth Token in public REST API calls are here.

Headless Windows Agent

In previous releases, Windows Agent must register to the Supervisor node and is centrally managed from the Supervisor node. This release introduces a Windows Agent that can be configured locally and does not need to register to the Supervisor node. This Windows Agent does not need an Agent license, but consumes a device license and the generated events contribute towards GB/day or EPS license. Currently, this Agent can be configured to send only Windows Security logs and user defined log files.

Steps to configure Headless Windows Agent is available in the Windows Agent 7.5.0 Installation Guide.

Linux Agent osquery

This release brings osquery functionality to the Linux Agent bringing parity with Windows Agent. An osquery allows you to query OS data using SQL queries to monitor and analyze Linux Systems. You can capture issues that are not necessarily in logs and get the result in real time. You can create osqueries, add them to monitoring templates and writes rules and reports from them.

Steps to create an osquery are available here.

Running an osquery is here.

Adding an osquery to a Linux Agent monitoring template can be done by following the steps in Define the Linux Agent Monitor Templates (osquery tab).

A set of built-in Linux osqueries is provided under **Resources > Osquery > Linux**. For more information on the osquery table, see here.

Webhook for Incident Notification

In previous releases, FortiSIEM can send Incident notifications to Microsoft Teams. This release provides a general Webhook feature that can be used to send Incident notifications to other applications such as WhatsApp, Slack, Telegram, and custom applications.

For details in setting up Webhook based notification, see here.

Saved Report Results

This release provides an area where all Search Results and Scheduled Report Results saved in PDF format can be viewed. The Saved Results from Search, Advanced Search have been relocated to this area.

See here for details.

Enhancements

Important System Updates

The following components have been upgraded.

- Linux Operation System to Rocky 9.7
- GlassFish App Server to Version 7
- Hibernate to 6.6
- JDK to 21.0.9
- PostgreSQL to 16.11

This release also includes Rocky Linux OS 9.7 patches until December 17, 2025. Details can be found at https://rockylinux.org/news/rocky-linux-9-7-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 9.7. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

GUI User Experience Enhancements

This release adds several GUI User Experience Enhancements, including:

- Navigation moves from Top to Side
- Extensive use of Icons
- Standardized position of common user activities like Search, Add, Edit, and Delete

App Server Performance Improvements

This release adds several App Server performance improvements:

- APIs that do not update the PostgreSQL Database are not run in transaction mode.
- Agent Updates are handled from local memory.
- APIs are handled using Tokens rather than Sessions.

Client Certificate based Authentication

In this release, various processes on Supervisor and Worker nodes mutually authenticate each other using Client Certificates. This does not require any user action.

Pre-built Agent Templates

This release adds built-in monitoring templates for Linux and Windows Agents. Linux Agent templates can be found under **Admin > Setup > Linux Agent**. Windows Agent templates can be found under **Admin > Setup > Windows Agent**. These pre-built templates can be identified by looking under the **Scope** column for **System**.

Device Support

- Cloudflare WAF
- Kubernetes – Audit
- FortiSRA
- Zscaler ZPA (SASE)
- Atlassian - Bitbucket

Bug Fixes and Enhancements

The following bugs and enhancements are resolved in this release.

Bug ID	Severity	Module	Description
1209616	Major	App Server	Supervisor with multi-tenant option turned on will cause org level event pulling to stop.
1176881	Major	App Server	User on Global org can schedule org level report, but report is never delivered.
1161878	Major	App Server	Scheduled report bundles generate separate report for each selected org, but not every org receives report.
1147132	Major	App Server	Excessive Agent Discovery may block regular discovery.
1190825	Major	Event Pulling Agents	Test Connectivity for on-prem FortiEDR API gets stuck using FortiEDR IP.
1220796	Major	GUI	Parsers associated to a device in CMDB can't be reordered or removed after initial selection.
1227801	Minor	App Server	Sometimes Content Update fails at 80% while importing Dashboard.
1214520	Minor	App Server	ML based Incident Resolution - Failed daily training job can cause JMS Queue to build up and cause excessive logs.
1214199	Minor	App Server	Duplicate CMDB devices appear if same devices send to two different collectors in the same Org.

Bug ID	Severity	Module	Description
1201550	Minor	App Server	Changing port number for mail settings and using OAuth does not work.
1181229	Minor	App Server	Stix/Taxii 2.1| Import with client private threat feed fails because of mismatch in count and limit being added twice.
1197207	Minor	Discovery	FortiMail discovered as FortiOS instead of FortiMail device.
1214390	Minor	Event Pulling Agents	Microsoft Defender API Poller may fail due to invalid filter encoding (+ instead of spaces) in OData query.
1204780	Minor	Event Pulling Agents	Kafka agent: pulling interval can't be saved as 0.
1204766	Minor	Event Pulling Agents	Kafka agent commits offset records too frequently.
1187443	Minor	Event Pulling Agents	'\' not properly escaped for Tenable Security Center Test Connectivity/Discovery.
1185604	Minor	Event Pulling Agents	In Multi-tenant collector, duplicate events may be seen due to timestamp files not being synced.
1161875	Minor	Event Pulling Agents	Mimecast log pull job fails because of additional '=' causing error to get token with "ValueError: too many values to unpack".
1198811	Minor	GUI	In GUI, Event Dropping > REGEX field doesn't allow '|' after 7.4.0 upgrade.
1157518	Minor	GUI	Under Org View, for rule multi-select action, user should be able to change active status for Global rules and Severity/Tags/Active Status for Org level rules.
1217799	Minor	Linux Agent	Linux Agent FIM audit search may cause high disk IO.
1212891	Minor	Linux Agent	Failed to set fsmadmin as the owner of the installation directory on Ubuntu 24.
1221767	Minor	Parser	FortiGate-event-admin-delete is categorized incorrectly as Account Created.
1189678	Minor	Parser	Unable to parse Graylog JSON events.
1179846	Minor	Parser	FalconDataRepParser overwrites reptDevIpAddr incorrectly and creates duplicate CMDB entries.
1171393	Minor	Performance Monitoring	Error log "Missing/Invalid SNMP credentials" occurs during FortiOS API discovery.
1163236	Minor	System	Under some circumstances, ClickHouse system tables may take space away from event table.
1074423	Minor	System	Hardware appliance restore from snapshot sometimes does not work for ClickHouse.

Bug ID	Severity	Module	Description
1051477	Minor	System	For hardware appliances, upgrade to 7.2.1 expands /data disk in appliance and encrypted disks prevents this step, causing upgrade to fail.
1203461	Minor	Threat Intel Integration	FortiRecon API integration returns 400 error code due to the API being disabled in v25.1.
1178548	Minor	Threat Intel Integration	Unable to integrate Cyble Threat Feeds (STIX/TAXII 21) because of URL parsing issue.
1220135	Minor	Windows Agent	Windows Agent Supers override gets overwritten by Supers list.
1215352	Enhancement	App Server	Limit the number of concurrent Collector Image installs to 30.
1212744	Enhancement	App Server	Cannot modify report or bundles with saved results.
1200255	Enhancement	App Server	Unable to use Windows directory variables to exclude folders in FIM settings.
1181515	Enhancement	App Server	Missing PH_AUDIT events for Windows and Linux Template changes.
1067429	Enhancement	App Server	After renaming Windows Agent on Windows Server, CMDB does not reflect the new name.
1216385	Enhancement	Data work	Update rule 'Uncommon Office365 Mail Login' to include correct event types.
1213905	Enhancement	Data work	RFE - CiscoMerakiParser enhancement for new logs format/type.
1205410	Enhancement	Data work	FortiGate 7081F log parsed as Unknown Event Type due to new devID format 'F78F1ATB24000057'.
1204198	Enhancement	Data work	Parse Dynatrace audit logs and enhance API integration.
1203951	Enhancement	Data work	Azure Event Hub SignInLogs: createdDateTime is not parsed correctly.
1202551	Enhancement	Data work	Update CiscoDuoParser to parse source IP.
1201805	Enhancement	Data work	Parse additional Cisco Firepower event types and categories.
1200954	Enhancement	Data work	AwsSQSParser - Add support for 'ObjectCreated:Put' eventType.
1200755	Enhancement	Data work	VMwareVCenterParser not parsing doat/lsud/sshd-session logs.
1200308	Enhancement	Data work	ZeekParser does not support zeek-intel events.

Bug ID	Severity	Module	Description
1198124	Enhancement	Data work	"HostName" and "HostIP" fields to be parsed for TrendMicroVisionOneParser in slightly different log format.
1196806	Enhancement	Data work	CrowdStrike Falcon Streamer parser update.
1196602	Enhancement	Data work	FortiGate parser needs to parse user defined message with embedded username and IP.
1189649	Enhancement	Data work	Data source for rules: MS 365 Defender: Exploit Detected and MS 365 Defender: Malware Detected is incorrect.
1188231	Enhancement	Data work	F5Big-IP-LTMParser not parsing Client IP in the raw events.
1187408	Enhancement	Data work	Armis - Add new event types to CMDB and expand rules.
1187314	Enhancement	Data work	Enhance FortiNDR rule to take into account event severity.
1185743	Enhancement	Data work	CiscoIOSParser doesn't parse user and device information from SSHD logs.
1183607	Enhancement	Data work	KasperskyParser: 'Device Time' cannot be parsed properly when the value is in milliseconds.
1182677	Enhancement	Data work	Event attributes like subject, operation, administrator (or username) are not parsed in Check Point parser.
1182666	Enhancement	Data work	Event attributes like login type, device compliance, trust type are not parsed in Office365 parser.
1179251	Enhancement	Data work	Parse MFA attributes from Azure Entra events.
1178503	Enhancement	Data work	WinOSWmiParser does not parse specific events attributes correctly in German language.
1178218	Enhancement	Data work	Enhancement for GoogleGCPParser to include GOOGLE_Pub_Sub.
1174895	Enhancement	Data work	Palo Alto Panorama event not parsed.
1174648	Enhancement	Data work	Win-App-MsiInstaller-11724 has incorrect event name and missing event type Win-App-MsiInstaller-11707.
1174002	Enhancement	Data work	FortiADC events coming in as comma delimited are not parsed.
1170190	Enhancement	Data work	Few AWSELB events aren't parsed when msg field doesn't have appTransportProto.
1168011	Enhancement	Data work	NonInteractiveUserSignInLogs' category events coming out of Azure Event hub configuration are not parsed.
1162344	Enhancement	Data work	Update Nutanix parser for unparsed events.
1161986	Enhancement	Data work	Support Claroty CTD ActivityLog in CEF RFC 5424 format.
1160107	Enhancement	Data work	NAS data not parsed in WinOSXmlParser.

Bug ID	Severity	Module	Description
1159554	Enhancement	Data work	Cisco ASA parser doesn't pass any value in the Direction field.
1159532	Enhancement	Data work	Mimecast - Few uncategorized events need to be added.
1156232	Enhancement	Data work	Fully handle AWS RDS by parsing all databases supported by RDS.
1150789	Enhancement	Data work	WinOSXmlParser does not parse msg field on eventID 364.
1125069	Enhancement	Data work	FortiGate event with src/destination ip 0.0.0.0/255.255.255.255 are not parsed.
1119303	Enhancement	Data work	Support Microsoft ATA CEF logs - New header format.
778604	Enhancement	Data work	Add 'Microsoft-Windows-WindowsUpdateClient' event log parsing to WinOSWmiParser.
778266	Enhancement	Data work	Add 'Microsoft-Windows-SmartCard-Audit' event log parsing to WinOSWmiParser.
778226	Enhancement	Data work	Add 'Microsoft-Windows-CertificateServicesClient-Lifecycle-System' event log parsing to WinOSWmiParser.
1212051	Enhancement	Device Support	ManageEngine Endpoint Central device support.
1210308	Enhancement	Device Support	FML Workspace Security (Perception Point) Syslog parser.
1204629	Enhancement	Device Support	Support ManageEngine PAM360 parser.
1193319	Enhancement	Device Support	Support Darktrace - SaaS platform.
1187889	Enhancement	Device Support	Add Siemens Simatic PLC parser.
1167810	Enhancement	Device Support	HTTP Generic Poller - Integration with SAP ETD.
1105482	Enhancement	Device Support	Add support for FortiSRA.
1172145	Enhancement	Event Pulling Agents	FortiGate 7.6.3 REST API discovery - posture report is not working.
1168667	Enhancement	Event Pulling Agents	Provide logs to check whether CrowdStrike destinations are reachable and output.
1231925	Enhancement	GUI	No error message occurs for user that is trying to delete custom parser assigned to device.
1220352	Enhancement	GUI	Provide a user option to not show health banner.

Bug ID	Severity	Module	Description
1192837	Enhancement	Parser	LOG based discovery should allow merge by serial number.
1146835	Enhancement	Parser	Enhance PH_SYSTEM_IP_EVENTS_PER_SEC event to add Hostname, #of parsed event, #unknown events.
1131961	Enhancement	Parser	Add support for IPFIX over TCP.
1217389	Enhancement	Public REST API	Retrieve all details of a device from CMDB via REST API.
1139908	Enhancement	Public REST API	Standardize API response with API query event or CMDB query.
1222908	Enhancement	System	Excessive (ACE) SSL Server Socket SSL errors seen.
1051449	Enhancement	Windows Agent	Windows Agent Discovery does not populate DNS and DHCP App groups like OMI discovery does.

Implementation Notes

Agent Related

1. For Linux Agent 7.5.0 two packages (`getfacl` and `patchelf`) are needed. Upgrades will fail if these two packages are not installed before starting the upgrade. Use the following commands to check whether the required binaries are available in your environment:

   ```
   command -v patchelf >/dev/null 2>&1
   command -v getfacl >/dev/null 2>&1
   ```

   If the command returns exit code 0, the package is installed.

   If the command returns a non-zero exit code, the package is not installed or not available in PATH.

   If one or both packages are missing, then install them using the appropriate package manager for your distribution.

   RHEL / CentOS / Rocky / Alma

   ```
   sudo dnf install -y patchelf acl
   ```

   (For older systems, `yum` may be used instead of `dnf`.)

   Ubuntu / Debian

   ```
   sudo apt update
   sudo apt install -y patchelf acl
   ```

   SUSE / openSUSE / SLES

   ```
   sudo zypper install -y patchelf acl
   ```

After completing these steps, you can proceed with upgrading the Linux Agents from GUI.

2. **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.
   a. Login as root user.
   b. 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.
   c. 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.
   d. 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,`
   e. Run the following command to reload the rsyslogd AppArmor profile and apply the changes above.
      `apparmor_parser -r /etc/apparmor.d/usr.sbin.rsyslogd`

Data Collection Related

For Windows OMI based discovery and log collection, NTLM authentication is no longer supported. Note that Microsoft has officially deprecated NTLM authentication - https://learn.microsoft.com/en-us/windows-server/get-started/removed-deprecated-features-windows-server?tabs=ws25

Hardware Appliance Related

After restoring from the hardware backup, some of the Clickhouse database tables may become read-only. Follow the instructions here to recover from read-only state.

Installation and Upgrade Related

- Disaster Recovery is not supported from 7.5.0 onwards. Customers are encouraged to use High Availability across Data Centers as a replacement.
- FortiSIEM 7.5.0 cannot be installed when either FIPS is enabled or in an IPV6 environment.
- Automation Service does not work when either FIPS is enabled, or High Availability across Data Centers feature is turned on.

- In Azure environment, FortiSIEM Cluster upgrade to 7.5.0 does not work. Please follow the manual upgrade steps in the Upgrade Guide.
- In Azure environment, any node will reboot twice during upgrade process – first after upgrading to Rocky 9 and then again when the whole upgrade is complete. Upgrade progress information will not be shown after the first reboot. Please ssh to the node and view the upgrade progress in the ansible log `/usr/local/upgrade/logs/ansible.log`
- If you perform a hardware restore after upgrading to 7.5.0, the appliance will reboot twice during the restoration process.
- Upgrade to 7.5.0 requires 32GB memory on Supervisor. If you are running older version and have less than 32GB of memory on Supervisor, then increase the memory to 32GB and then upgrade to 7.5.0 Also, Java VM memory should be at least 10GB.
- If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.5.0, then after upgrading to 7.5.0, 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, 7.3.x, or 7.4.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.

General

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. 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
```

5. If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.5.0, then after upgrading to 7.5.0, 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, 7.3.x, or 7.4.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.

www.fortinet.com