Release Notes

FortiSIEM 7.5.1

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

05/11/2026
FortiSIEM 7.5.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
05/04/2026	Added Linux Copy-Fail Vulnerability Mitigation.
05/04/2026	Initial version of the 7.5.1 Release Notes.
05/08/2026	Replaced Linux Copy-Fail Vulnerability Mitigation with Linux Copy-Fail Vulnerability Fix.
05/11/2026	Added Linux Dirty-Frag Vulnerability Fix.

What's New in 7.5.1

Linux Copy-Fail Vulnerability Fix

A fix for the copy-fail vulnerability (CVE-2026-31431) is available on the FortiSIEM OS repository servers. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure.

Linux Dirty-Frag Vulnerability Fix

A fix for the dirty-frag vulnerability (CVE-2026-43284) is available on the FortiSIEM OS repository servers. FortiSIEM customers in versions 6.4.1 and above, can upgrade their Rocky Linux versions by following the FortiSIEM OS Update Procedure. This procedure needs to performed twice in succession to get all the updates due to the addition of a new rocky-security repository.

FortiSIEM 7.5.1 release includes the following features and enhancements.

- System Update
- Features
- Key Enhancements
- New Device Support
- Bug Fixes and Enhancements
- Known Issues / Implementation Notes

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

System Update

This release includes Rocky Linux OS 9.7 patches until April 29, 2026. 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.

This release also upgrades Redis to 8.6.2.

Features

MCP Service

The Model Context Protocol (MCP) is an open-source standard that enables AI models to securely connect to external tools, data sources, and software systems. For more information about MCP, see Anthropic's Model Context Protocol documentation.

In this release, FortiSIEM introduces an MCP service that enables customers to build their own AI Agents by accessing information stored in the FortiSIEM CMDB, including devices, users, and incidents, as well as the FortiSIEM event database hosted on ClickHouse.

AI agents can connect to `https://{Supervisor}/phoenix/mcp` over port 443 by using an API token obtained through the FortiSIEM GUI.

The following MCP tools are available for AI Agents to use. An AI Agent needs to use LLM to determine the appropriate MCP tool for answering user's request.

- append_incident_comment_by_id
- clear_incident_by_id
- get_context_by_entity
- get_incident_by_id
- get_incidents_by_entity
- get_iocs_by_incident_ids
- get_related_incidents_by_id
- get_top_10_risky_devices_incidents
- get_top_10_risky_users_incidents
- get_trigger_events_by_incident_id
- query_fsm_clickhouse
- query_fsm_clickhouse_prompts
- query_fsm_postgres
- query_fsm_postgres_prompts
- update_incident_resolution_by_id
- update_incident_severity_by_id

Following Security restrictions are enforced:

- Only Read access to specific PostgreSQL and ClickHouse tables
- Disallow specific ClickHouse SQL functions

Key Enhancements

API Tokens Using Client Credentials Grant

API tokens provide a more secure method for authenticating public REST API calls than using passwords. Support for API tokens was introduced in version 7.5.0 using the OAuth 2.0 Refresh Token grant. In this release, the Refresh Token grant has been replaced with the simpler OAuth 2.0 Client Credentials grant. Callers can now obtain and renew access tokens using only a Client ID and Client Secret. For additional information, see here.

FortiAI Enhancements

This release contains the following enhancements.

- Token usage is reduced by using semantic search on the prompts and history. Only relevant sections on prompt and historical context are sent to OpenAI. This feature is on by default, but can be turned off.
- Following Security restrictions are enforced:
  - Only Read access to specific PostgreSQL and ClickHouse tables
  - Disallow specific ClickHouse SQL functions
  - Allow Security specific questions only
  - Disallow direct SQL Queries

Token Usage Reduction

Question	Tokens without Opt	Tokens with Opt
How many devices in my CMDB? List by Vendor and Model.	11K	4K
Which devices were added to CMDB in last week?	11K	4K
Get Top 10 event types in the last 1 hour.	20K	9K
Get Top 10 reporting devices in the last 1 hour.	20K	11K
Get Top 5 reporting devices in the last 1 hour. Then for each reporting device, get top 5 event types. Include all devices.	20K	10K
Get Top 10 Active incidents today ordered by count. Include Incident Title, Rule Name, Count, First Seen Time and Last Seen Time.	11K	9K
List Top 5 hosts with most Incidents today. For each host, list the Rule Name and Count.	11K	9K
List Top 5 users with most Incidents today. For each user, list the Rule Name and Count.	11K	7K

Question	Tokens without Opt	Tokens with Opt
Total	115K	63K

This shows a savings of 45% for the above set of questions.

GUI Enhancements

This release contains the following GUI enhancements.

- Ability to Filter on demand on **Analytics > Search > Filters** page.
- Creating new Report and Rule page is streamlined.
- **Resources > Rules > Activation** view shows partial Activations across Organizations in Service Provider deployments.

New Linux Agent Support

Linux Agent can now run on the following two Linux distributions:

- AlmaLinux 8, 9, 10
- Amazon Linux 2023

7.5.0 to 7.5.1 Parser Updates

Changes to built-in Parsers from FortiSIEM version 7.5.0 to 7.5.1 can be found here.

7.5.0 to 7.5.1 Report Updates

Changes to built-in Reports from FortiSIEM version 7.5.0 to 7.5.1 can be found here.

7.5.0 to 7.5.1 Rule Updates

Changes to built-in Rules from FortiSIEM version 7.5.0 to 7.5.1 can be found here.

7.5.0 to 7.5.1 Dashboard Updates

Dashboards added in 7.5.1

- Corelight
- Corelight Zeek
- Corelight Suricata

Dashboards updated in 7.5.1

- CrowdStrike Dashboard
  - Top EDLP Firewall Actions renamed to Top Endpoint DLP Actions
  - Top EDLP Threat Levels renamed to Top Endpoint DLP Threats

7.5.0 to 7.5.1 Public REST API Updates

For full list of FortiSIEM API, see here.

The following APIs have been added:

`/phoenix/rest/pub/security/oauth/token`

`/phoenix/rest/pub/v2/query/eventQuery`

`/phoenix/rest/pub/v2/query/progress`

`/phoenix/rest/pub/v2/query/events/results`

`/phoenix/rest/organization/list`

`/phoenix/rest/pub/device/delete`

The following APIs are deprecated (and may be removed in a future release):

`/phoenix/rest/query/eventQuery`

`/phoenix/rest/query/progress/{queryId}`

`/phoenix/rest/query/events/{queryId}/{offset}/{limit}`

`/phoenix/rest/agentStatus/all`

`/phoenix/rest/agentStatus/v2/all`

`/phoenix/rest/pub/incident/triggeringEvents`

`/phoenix/rest/cmdbDeviceInfo/devices`

`/phoenix/rest/config/Domain` - Replaced by `/phoenix/rest/organization/list`

The following APIs have been removed:

`/phoenix/rest/device/list/delete` - Renamed to `/phoenix/rest/pub/device/delete`

`/phoenix/rest/cmdbDeviceInfo/properties` - Replaced by `/phoenix/rest/pub/device`

`/phoenix/rest/device/list` - Replaced by `/phoenix/rest/pub/device`

`/phoenix/rest/device/list/source` - Replaced by `/phoenix/rest/pub/device`

`/phoenix/rest/device/discovery/add`

`/phoenix/rest/device/update`

`/phoenix/rest/system/add/eventworker`

```
/phoenix/rest/system/add/queryworker
/phoenix/rest/system/delete/eventworker
/phoenix/rest/system/delete/queryworker
/phoenix/rest/system/eventworker
/phoenix/rest/system/queryworker
/phoenix/rest/cmdbDeviceInfo/devicesByPagination
```

New Device Support

- Corelight
- Google Threat Intelligence
- Sectona PAM

Bug Fixes and Enhancements

The following bugs and enhancements are resolved in this release.

Bug ID	Severity	Module	Description
1267729	Major	App Server	CSV report export causes one report to overwrite another.
1256665	Major	App Server	When Duo 2FA is enabled for a local user belonging to an organization, the user is to be able to see all orgs.
1261480	Major	App Server, Parser	Event Tagging is not working properly in MSSP environment with Collectors.
1257693	Major	GUI	In multi-tenant deployments, user from one organization is able to see retention policy of other organizations.
1241876	Major	GUI	Setting UTC Time for user profile will cause Analytics Search to query incorrect dates.
1269402	Major	Rule	Scheduled rules may cause incidents to stop triggering after some time.
1250315	Major	System	Webhooks based log ingestion is not working after upgrade to 7.4.2 due to incorrect permissions change after reboot.
1274768	Major	Windows Agent	If a Windows Agent Monitor Template contains specific Event IDs, then log collection does not work.
1235873	Major	Windows Agent	Moving/deleting IIS logs older than today will make the Windows Agent reprocess all logs from the current day file.

Bug ID	Severity	Module	Description
1264572	Minor	App Server	User with no rule access can list rules from API /phoenix/rest/dataRequest/rule.
1264549	Minor	App Server	Org level admin can retrieve other orgs active rules through rest API /phoenix/rest/dataRequest/rule.
1257483	Minor	App Server	CMDB > Filter by Device Type > throws Java ClassCastException and the filter does not work.
1257072	Minor	App Server	The event PH_DEV_MON_PERFMON_ALL_DEVICE_DELAY_HIGH incorrectly generated for hosts, while it should be generated only for collectors.
1245684	Minor	App Server	CMDB Device Edit Error when a Supervisor node has no registered collectors.
1243883	Minor	App Server	Sometimes there are nullpointer exception for Glassfish during Agent Updates.
1240428	Minor	App Server	User Profile Updates are incorrectly logged as Password Changes.
1218480	Minor	App Server	User with 'View Case' permission can add notes to cases.
1214456	Minor	App Server	User is incorrectly allowed to change custom Rule event types. This causes Incident Search filters to stop working.
1214396	Minor	App Server	Sometimes incident email notifications miss Raw events.
1198207	Minor	App Server	Sometimes, devices are not mapped to the collector in the CMDB, causing the device count in GUI to be incorrect.
1241529	Minor	App Server, Query	In Search, Source or Destination TCP/UDP port 65535 shows as NULL.
1271182	Minor	ClickHouse Backend	ClickHouse FortiEDR API query is slow as it pulls 10K records.
1256303	Minor	ClickHouse Data Management	phDataManager may get outdated disk size causing it to purge unnecessarily.
1258431	Minor	Data Work	Entra ID sign in event incorrectly parses the application name for user.
1259925	Minor	Discovery	Two hosts with no host IP but identical hostname results in duplicate CMDB entries.
1270585	Minor	Generative AI	phGenerativeAI process became stuck during startup while attempting to build user indexes.
1261736	Minor	GUI	“Change Password” option missing for local Org Users when User Org is created from Super Global.

Bug ID	Severity	Module	Description
1232796	Minor	GUI	Global view of a shared Dashboard settings does not get reflected in Organization View of the same dashboard.
1217407	Minor	GUI	Incident Explorer page remains empty after clearing all incident in the view.
1216948	Minor	GUI	User's Comment when clearing an incident are not saved.
1215086	Minor	GUI	Total item numbers on the Admin > Discovery page are incorrect for both global and specific organization views.
1213317	Minor	GUI	Collector Health shows N/A if EPS is < 1.
1207272	Minor	GUI	Users with AD Group Role Mapping cannot save user profile changes.
1195910	Minor	GUI	In Enterprise version with Collector HA configured, Agent Template Association doesn't show a Collector Cluster.
1192064	Minor	GUI	Rule and Analytics search filter does not allow CONTAIN / NOT CONTAIN '@'.
1245688	Minor	Linux Agent	In CMDB, 2 cloned Linux hosts with agents are incorrectly merged into 1 host.
1263914	Minor	Parser	Microsoft Defender events larger than 24KB may not be parsed and recognized as unknown event type.
1258400	Minor	Performance Monitoring	STM not working for IMAP and SMTP. Test is successful, but monitoring fails.
1236212	Minor	Performance Monitoring	Custom JDBC perf mon test ignores DB name and succeeds, but actual job never runs.
1250592	Minor	Rule	Scheduled rules with COUNT(DISTINCT) in Incident Definition attribute fail to trigger.
1228261	Minor	Rule	Rule Subpattern ignores Custom CMDB Ports and Triggers Incident.
1228911	Minor	System	The # end tag configuration is incorrectly cleaned up in /etc/hosts when restarting fsm-confd.service.
1223355	Minor	System	After upgrade, pub_api concurrent settings are reset to default in phoenix_config.txt.
1222475	Minor	System	Update Azure Storage Blobs client library and Azure Storage Queues client library for Python.
1263362	Minor	Windows Agent	For Windows Agent File Monitoring events, User field is not populating when a directory is being modified, or when a SecurityChange happens to a file or directory
1225606	Minor	Windows Agent	Changes to the Windows Agent log level does not take effect until the agent is restarted.

Bug ID	Severity	Module	Description
1271738	Enhancement	App Server	Enable Analytics searching with Read-only role.
1251774	Enhancement	App Server	Simplify API Token by supporting Client credentials.
1220485	Enhancement	App Server	Allow Triggered Event Query for target incident to be exported as CSV (in addition to PDF) directly from Incident page.
1271856	Enhancement	Data Work	WinOSXmlParser fails to extract source IP for 4624 events.
1271848	Enhancement	Data Work	Rule: Windows: HackTool - Windows Credential Editor WCE Execution needs update.
1271602	Enhancement	Data Work	Add lateral movement detection: advanced search rules and scheduled rules.
1269400	Enhancement	Data Work	Rule - Windows: Possible PetitPotam Coerce Authentication Attempt - may never trigger.
1268393	Enhancement	Data Work	Malware URL IOC rules have different event type logic.
1264605	Enhancement	Data Work	Enhance ZScalar reports and dashboards.
1264604	Enhancement	Data Work	Corelight parser missing parsing of important attributes, also needs some out the box reports and dashboard.
1262882	Enhancement	Data Work	FortiEDRParser needs recognizer update.
1261383	Enhancement	Data Work	FortiRecon Parser fails to parse multiple attributes and timestamps correctly.
1257345	Enhancement	Data Work	SAP Enterprise Threat Detection - Need webhook and HTTPS advanced credential options added to device type.
1254907	Enhancement	Data Work	Veeam Parser enhancement - event types enhancements.
1252585	Enhancement	Data Work	ImpervaParser not parsing the latest Syslog format correctly.
1250975	Enhancement	Data Work	FortiGateParser reported the severity as medium when the Raw events indicate high.
1250006	Enhancement	Data Work	CitrixNetScalerParser not parsing log format RFC5424, currently only parsing log format RFC3164.
1248726	Enhancement	Data Work	HuaweiVRP Parser - Logs are not being parsed due to 'No year in timestamp'.
1245809	Enhancement	Data Work	AWS CloudTrail SnapshotID not populated by system parser due to attribute binding mismatch.
1245701	Enhancement	Data Work	Cisco ISE Parser update.
1243243	Enhancement	Data Work	F5AFMParser does not parse the Traffic Statistics logs >> recognized as unknown event type.

Bug ID	Severity	Module	Description
1241004	Enhancement	Data Work	FortiSandboxParser parser eventFormatRecognizer should support devid FSA[A-Z0-9], currently it is FSA\d\w*.
1239311	Enhancement	Data Work	Add event type definition for few CrowdStrike Audit events.
1238662	Enhancement	Data Work	HillStoneNGFWParser - source IP, destination IP, and logID are not being parsed.
1236840	Enhancement	Data Work	Postponed ssh auth syslog events gets parsed as Generic_Unix_Failed_SSH_Login.
1236043	Enhancement	Data Work	Cisco ASA events not parsed correctly.
1234544	Enhancement	Data Work	VMwareEventParser concatenates user and vmwEventId fields due to missing delimiter in raw VMware SDK logs.
1232043	Enhancement	Data Work	Armis parser enhancement.
1230516	Enhancement	Data Work	AO-WUA-UserFile-ExchangeTrackLog events are not parsed correctly.
1230040	Enhancement	Data Work	Cisco ASA Event ASA-113005 fails to extract user correctly.
1228355	Enhancement	Data Work	CheckpointCEFParser - No parsing useful fields.
1226750	Enhancement	Data Work	BindDNSParser update.
1225162	Enhancement	Data Work	FortiADC Parser doesn't parse when FortiADC SN begins with 'FDVMELTM' (Product Model: ELA FortiADC VM PrePay).
1223509	Enhancement	Data Work	Cisco ESA rules refers to legacy SDR labels (Awful/Poor) instead of current verdicts.
1223323	Enhancement	Data Work	Add rules for Veeam.
1216928	Enhancement	Data Work	Add support for application event logs in AWS CLOUDWATCH Parser.
1205410	Enhancement	Data Work	FortiGate parser needs to handle new devID format 'F78F1ATB24000057'.
1199010	Enhancement	Data Work	FortiRecon parser - 'breach date' is not parsed in event FortiRecon-easm_leaked_creds.
1193299	Enhancement	Data Work	Sectona PAM device support.
1166726	Enhancement	Data Work	Add dedicated Microsoft Azure Monitor Activity Log parser.
1151383	Enhancement	Data Work	When system reboots, the rule 'Windows Logging Service Shutdown' should not trigger.
1263248	Enhancement	Device Support	Add Amazon Linux 2023 support for Linux Agent .

Bug ID	Severity	Module	Description
1239785	Enhancement	Event Pulling Agents	FortiEMS API: Support Basic Auth Login with Multitenancy (sites) defined.
1241801	Enhancement	Generative AI	Show remaining OpenAI Request and Tokens in Cloud Health.
1239570	Enhancement	Generative AI	Reduce token size using RAG.
1253229	Enhancement	GUI	Missing multiple incident selection and bulk actions in certain views in 7.5.0.
1260218	Enhancement	Linux Agent	Add AlmaLinux 8,9,10 support for Linux Agent.
1222290	Enhancement	Parser	Need to move to warning or hide error PH_UTIL_IP_TYPE_INVALID events.
1241987	Enhancement	System	Upgrade Duo WebSDK Java Client to v1.3.1.
1227609	Enhancement	Threat Intel Integration	Add Google Threat Intel (GTI) External Threatfeed integration.
1250138	Enhancement	Windows Agent	Implement retry mechanism while downloading Windows Agent update binaries from Supervisor.

Known Issues / Implementation Notes

Business Service Dashboard

If your Business Service includes devices that are discovered via Log only, then the device name in the Business Service Dashboard may be empty. Workaround is to restart Query master process in Supervisor node.

If a device is deleted from Business Service and the device has Active Incidents, then the Incident Count in Business Service dashboard may be incorrect. Workaround is to clear the active Incidents for the device deleted from Business Service.

Custom Performance Monitoring

If you add Custom Performance Monitoring to a device that is already discovered, then the newly added Custom Performance Monitoring may not work. You will not see the green OK icon for the Monitoring job for that device in **Admin > Setup > Monitor Performance**. There are two alternative workarounds:

1. Go to **Admin > Setup > Monitor Performance**, select the device and disable monitoring. A few minutes later, enable monitoring again.
2. Delete the device from **CMDB** and rediscover.

Disabling / Enabling Performance Monitoring and Event Pulling Jobs

FortiSIEM discovers IT infrastructure and collects logs and performance monitoring metrics using `phDiscover`, `phAgentManager` and `phPerfMonitor` processes residing inside Supervisor, Worker or Collector (most common) nodes. While the data collection works normally, this release has the following known issues if you want to delete the data collection jobs under Super / Global View.

- **Issue 1** - Enterprise deployment: If you are using the Supervisor node to discover and collect data, then you may not be able to disable or enable the jobs from **Admin > Setup > Pull Events** tab. Note that data collection works normally in this case.

  Also, if you are using Collectors to discover and collect data, then data collection works normally and the jobs can be disabled / enabled without any issues.

  Workaround is to delete the credential from **Admin > Setup > Credentials**.
- **Issue 2** - Service Provider deployment: If you are using Supervisor to discover and collect data for Organizations without Collector, then you may not be able to disable / enable these jobs from **Admin > Setup > Pull Events** tab under Super / Global view. Note that data collection works normally.

  Also, if you are using Collectors to discover and collect data, then data collection works normally and the jobs can be disabled / enabled without any issues.

  Workaround is to delete the credential from **Admin > Setup > Credentials**.
- **Issue 3** - Service Provider deployment: If you are using multi-tenant Collectors and you have scheduled performance monitoring jobs from the Supervisor node, then you may not be able to disable / enable the jobs from **Admin > Setup > Performance Monitoring** tab under Super / Global view. Note that data collection works normally.

  Also, if you are using Collectors for performance monitoring, then data collection works normally and the jobs can be disabled / enabled without any issues.

  Workaround is to switch to Super-Local Organization, then perform the enable / disable operations.

External URL definitions in GUI

A security fix was made to not allow private (RFC 1918) IP addresses in URL definitions, unless explicitly configured. This impacts HTTP Incident Notification, Lookup Tables, Sigma Rule, Malware Update and FortiSIEM Manager definitions.

The following configurations are affected:

1. **Admin > Settings > Analytics > Incident Notification >**
   a. **HTTP Notification > HTTP(S) Server URL**
   b. **Webhook Notification > New > URL**
2. **Resources > Lookup Tables > Import > Update via API URL**
3. **Resources > Rules > Import > Import SIGMA Rule URL**
4. **Resources > Malware Domains/IPs/Hash/Processes/URLs > Configure > Update via API URL**
5. **Admin > Setup > FortiSIEM Manager > FortiSIEM Manager FQDN/IP**

If you need to use Private addresses, then add the IP address(es) in the GLOBAL section in `/opt/phoenix/config/phoenix_config.txt`.

`allowed_trusted_url=<ip_1>,<ip_2>`

Note that this configuration is not needed for public IP addresses.

FortiAI Role Restriction

In responding to FortiAI questions, user's role other than organization membership in Service Provider installation, is ignored. That means that

- Responses to questions from an Org level user contain only data from that Org
- Responses to questions from a Super/Global level user contain only data from that Org
- If user is restricted to a specific Data Condition (e.g. a Network Admin User), then responses ignore this restriction. That means the responses are the same for a Full Admin user for that Org.

This is true for all areas of FortiAI in GUI as well as MCP Service.

Fresh Elasticsearch based Deployment

After configuring Elasticsearch in **Admin > Setup > Storage > Online** in a new FortiSIEM deployment, it may happen that events are not ingested into Elasticsearch and **Analytics > Search** shows no results. In this case, go to **Admin > Setup > Storage > Online**, and in Elasticsearch section, click **Test** and then **Deploy** one more time.

General

1. Nessus 6 Vulnerability Scanner support is deprecated.
2. 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.
3. 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.
4. 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.
5. 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
```

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

- Upgrade to 7.5.1 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 7.5.1. Also, Java VM memory should be at least 10GB.
- FortiSIEM 7.5.1 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.
- When upgrading Collectors, the recommended procedure is to upgrade 1 Collector first, and then upgrade the remaining Collectors in bulk mode. Since Collector upgrade happens through Supervisor node, the first upload creates the cache of upgrade packages on the Supervisor, which can be utilized during the remaining Collector upgrades. Without this procedure, bulk Collector upgrades may fail.
- In Azure environment,during upgrade from pre-7.5.0 to 7.5.1, 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`. Upgrade from 7.5.0 to 7.5.1 will proceed normally without 2 reboots.
- If you perform a hardware restore after upgrading to 7.5.1, the appliance will reboot twice during the restoration process.
- If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.5.1, then after upgrading to 7.5.1, 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, 7.4.x, or 7.5.0 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

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.