Release Notes

FortiSIEM 7.3.1

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

05/14/2025
FortiSIEM 7.3.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
03/04/2025	Initial version of the 7.3.1 Release Notes.
03/05/2025	Known Issues added.
03/07/2025	Known Issues - Additional information provided.
03/10/2025	Bug Fixes and Enhancements Table updated.
03/20/2025	Implementation Notes - Collector HA Related section updated.
05/14/2025	Upgrade Implementation for 7.2.6 added to 7.3.0-7.3.2 Release Notes.

What's New in 7.3.1

This release contains the following bug fixes and enhancements.

If you are running 7.2.6, then you cannot upgrade to 7.3.1. This is because 7.2.6 contains database schema changes that are not present in 7.3.1.

System Updates

This release includes Rocky Linux OS 8.10 patches until February 17, 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.

General Enhancement

For **All-in-one Supervisor clusters** (hardware appliances or VMs), at least 3 nodes are required for automated HA. However, if you must work with 2 nodes, then some manual steps are needed to make HA work. See Manual HA with 2 Nodes from the High Availability and Disaster Recovery Procedures - ClickHouse Guide.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
1114559	Major	App Server	Appserver may consume large amount of resources caused by excessive number of IP reputation update jobs.
1113736	Major	App Server	Scheduling a large number report bundles to run at similar times may cause App Server to consume large amount of memory and subsequently cause GUI outage.

Bug ID	Severity	Module	Description
1130134	Major	ClickHouse	In HA environment, ClickHouse Event move/purge does not happen automatically on Replication Follower node.
1127735	Major	Gen AI	AI search for report/rule/eventTypes doesn't work on HA Follower nodes.
1127775	Major	GUI	In CMDB > Devices: Org view : 'Discovered by Collector' filter shows devices discovered by another collector in the Org.
1113738	Major	Query, Rules	Query Worker and Rule Worker modules have memory leak that may cause memory consumption to be large after a few days.
1052318	Major	Query, Rules	Query or Rule fails when it refers to a single network in Resources > Networks (e.g. Net-10.0.0.0/8). Note that Query or Rule works at a folder level (e.g. "Private Net").
1126066	Major	Parser	Increase the raw event size to 64KB to handle large events from Cloud providers (such as Microsoft Defender).
1111377	Major	System	High memory usage on all of the Keepers.
1116926	Minor	App Server	Sometime, Incident page does not load because of Risk Score value overflow/underflow.
1114340	Minor	App Server	For incidentSource, IncidentTarget, the full comma separated value is not sent to ServiceNow. Currently, only the IP address part is sent.
1114105	Minor	App Server	PDF Report Exporter fails to export when Section Title is missing.
1110874	Minor	App Server	After cloning a rule with multiple subpatterns, editing and saving the rule results in a rule synchronization error.
1107958	Minor	App Server	A scheduled CMDB Report with business service condition with a nested Event Report will fail, for example - Business Service Name IN ('Firewall Service') AND Device IP IN Reporting IP: [Top Reporting Devices and Events By Count].
1107091	Minor	App Server	After deactivating a rule in Org level, Super Global user sees the rule still active for that Org.
1105800	Minor	App Server	PAYG emails go to old set of email addresses unless config is completely cleared and reconfigured.
1087201	Minor	App Server	Custom rules that do not have data_source and detection_ technology defined will not save inline without duplication.
1085995	Minor	App Server	After upgrading to 7.2.3, GUI Incident List View page may show 'TransactionRolledbackLocalException: Client's transaction' error.
1071609	Minor	App Server	365 Defender is not added to CMDB after discovery is successful, but events are coming in.

Bug ID	Severity	Module	Description
1050224	Minor	App Server	CloudTrail and CrowdStrike cloud devices not listed CMDB and CloudWatch has duplicate devices.
1014202	Minor	App Server	Cisco DUO is not counted as a cloud service in CMDB.
1112424	Minor	App Server,System	After using configFSM.sh to update Worker timezone or hostname, duplicate worker entries are created in GUI.
1109435	Minor	Automated HA	Automated HA environment - For some discovered devices, Performance Monitor status is paused and does not start.
1107992	Minor	Data work	Rule 'No Logs From a Device' missing 'Linux Agent' Condition.
1084617	Minor	Data work	Wrong Data Source for Rule: Windows: Ngrok Usage with Remote Desktop Service.
1071717	Minor	Data work	QNAPParser does not parse latest QNAP syslog events.
1074113	Minor	Discovery, Performance Monitoring	The phoenix_config parameter SNMPwalk_v3_packet_timeout does not take effect.
1115043	Minor	Elasticsearch	Analytics > Org drop down > result incorrect for single org when DeviceToCMDBAttr function is used in Query.
1120929	Minor	Event Pulling Agents	Cisco Umbrella Integration fails. The cache destination file is pre-emptively created, causing gunzip to fail.
1118863	Minor	Event Pulling Agents	After test connectivity, an event pulling job does not execute unless you click Apply.
1115552	Minor	Event Pulling Agents	Test Credentials for Akamai Connected Cloud result failed.
1108567	Minor	Event Pulling Agents	CrowdStrike API - not all events are always pulled when server sends incomplete events.
1116550	Minor	GUI	Org level users can edit Super Global level Network Groups.
1067958	Minor	GUI	Cannot undo the applied filter for 'Destination Host Name' in a Dashboard widget.
1106020	Minor	Parser	Update FortiEDR Parser to include Threat information.
1087520	Minor	Parser	Events from M365Defender fail to parse if the event is very large.
1093546	Minor	Performance Monitoring	Custom JDBC query does not provide valid output when query has special characters.
1106839	Minor	Query	Running Analytics queries from a specific Organization can match Source IPs from other Organization Network groups.
1097455	Minor	Query	Retention interval for Scheduled Report and Report Bundle is hard coded to 1 hour and GUI settings are ignored.

Bug ID	Severity	Module	Description
1116350	Minor	System	FSM installation using IPv6 address fails.
1115807	Minor	System	FortiSIEM with IPv6 fails to install because incorrect svn_disk disk parameter is passed.
1103771	Minor	System	Remove weak SSH algorithms support.
1103770	Minor	System	Remove weak CBC mode ciphers.
1078106	Minor	System	Excessive logging on `/var/lib/mod_security/` may cause the root disk to be full.
1111259	Minor	Windows Agent	Custom defined Disk Thresholds not working for labelled disks (e.g. `E:\LOG`).
1109377	Minor	Windows Agent (UEBA)	When Windows Agent tries to get the command line parameters for a process to add to UEBA events, those with short command lines can cause the agent to crash.
1093780	Enhancement	App Server	JSON parsing error on PH_SYS_FORTIGUARD_BLOCKED_URL causing pm2 log to grow rapidly.
1113061	Enhancement	App Server,GUI	For offline upgrade situations, provide an option for Collector and Agent upgrade to skip hash check.
1108209	Enhancement	Automated HA	Support automated HA for Azure public cloud.
1119954	Enhancement	Data work	Enhance Office365 parser to include Request Type.
1118487	Enhancement	Data work	Add Source Country and Destination Country in every system defined rule that matches external Malware IP/Domain/Hash definitions.
1112828	Enhancement	Data work	Rules and Reports for Mitel MiCollab and Apache Struts 2 RCE outbreak.
1110266	Enhancement	Data work	Parse more Foundry Ironware Plus events.
1109874	Enhancement	Data work	Parse AWS Secret Manager CloudTrail events.
1099649	Enhancement	Data work	Enhance Office365Parser to parse 'IsCompliant' and 'TrustType' from Azure Active Directory event logs.
1086832	Enhancement	Data work	Enhance IronportMailParser to parse SDR (Sender Domain Reputation) attributes.
1107693	Enhancement	ElasticSearch	Add support for Elasticsearch 8.17.
1121182	Enhancement	GUI	Cisco Umbrella S3 Integration: Hide Session Key from UI as it is not needed.
1062361	Enhancement	GUI	For Oracle Database Server Audit credential, default config is showing dba_audit_trail instead of unified_audit_trail. User must overwrite this field.

Bug ID	Severity	Module	Description
1087937	Enhancement	Parser	Enhance Azure Event Hub parser to parse more system attributes.
1110696	Enhancement	System	Two benign errors are briefly displayed in ansible log when you run fresh install script configFSM.sh on hardware appliances, but there is no impact. The errors are "tail: cannot open '/usr/local/fresh-install/logs/ansible.log' for reading: No such file or directory" and "/usr/local/bin/configFSM.sh: line 1315: [: -ne: unary operator expected".
1094051	Enhancement	System	Update PHP version to 8.2.
1077593	Enhancement	System	Modify FSM installer to allow installation on oVirt - no env oVirt to verify this bug.
1075571	Enhancement	Threat Intel Integration	Add support for Mandiant Intelligence threat feed.
1110561	Enhancement	UEBA	Reduce event consumers from 4 to 1 to reduce memory usage.

Known Issues

1. For hardware appliances, upgrade to 7.3.1 may fail because of increased root disk usage during upgrade process. It is recommended not to upgrade to 7.3.1 and wait for a fix. If you have already attempted an upgrade and it failed, then you can remedy this by using the following steps:
   a. Login to your system as root and run the following command to free up disk space on root partition.
      `rm -f /fsmopt.tar.gz`
   b. Restore your system back to the previous working release using the following procedure: Restoring Hardware from Backup After a Failed Upgrade
2. FortiSIEM 7.3.1 cannot be installed in **IPV6 only** environments.
3. External FortiSIEM GUI user authentication via RADIUS is not supported.
4. If you are running 7.2.6, then the next upgrade **must be later** than 7.3.2, or 7.4.0 or later. You cannot upgrade to earlier versions as 7.2.6 contains schema changes not present in 7.3.2 and earlier releases.

Implementation Notes

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

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`

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

Pre-7.3.1 Entry

```
<identityEvent>
     <eventType>MS_OFFICE365_UserLoggedIn_Succeeded</eventType>
     <eventAttributes>
```

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

7.3.1 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>
```

Parser Related

On a fresh installed 7.3.1, or after upgrading to 7.3.1, if you want to modify any of the following system defined parsers and you have pre-7.3.1 collectors, then apply the content update published after March 5, 2025 before making the parser changes.

- AkamaiSIEMParser - Akamai Connected Cloud
- CloudPassageParser - CloudPassage Halo
- DocuSignParser
- FalconStreamingParser - CrowdStrike Falcon
- FireAMPCloudParser - Cisco FireAMP Cloud
- OracleCASBParser - Oracle CASB Security
- ProofpointParser
- WinDefATPParser - Microsoft Windows Defender ATP

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.3.1, then after upgrading to 7.3.1, 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, or 7.3.0 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.

Upgrade Related

1. If you encounter this error during App Server deployment part of upgrade process, then take the remediation steps below:

   ```
   Error:
   ```

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

   ### Remediation Step

   Option 1: Increase Java stack size to 2M.

   a. Login to Supervisor via SSH.
   b. `su - admin`
   c. `vi /opt/glassfish/domains/domain1/config/domain.xml`

      add `-Xss2m` in jvm-options session:

      `<jvm-options>-Xss2m</jvm-options>`
   d. Re-run the upgrade process.

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

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

2. In an Automated HA + DR environment, cluster upgrade from 7.3.0 to 7.3.1 may hang at the last step involving the Secondary Supervisor upgrade, with the message "PRE-UPGRADE | Stop backend services". This is likely caused by unresponsive phMonitor. In this situation, take the following remediation steps.

Remediation Step

a. SSH to Secondary DR node.

b. Run the following command:

```
killall -9 phMonitor
```

c. Then the upgrade process will continue and end successfully.

www.fortinet.com