FORTINET

Release Notes

FortiSIEM 7.3.3

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

10/01/2025
FortiSIEM 7.3.3 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
07/15/2025	Initial version of 7.3.3 Release Notes.
07/21/2025	Known Issue (#1) added to 7.3.3 Release Notes.
10/01/2025	Fixed Bug 1174775 description updated in 7.3.3 Release Notes.

What's New in 7.3.3

This release contains the following bug fixes and enhancements.

If you upgrade to 7.3.3, your next 7.4.x upgrade must be 7.4.1 or later because 7.3.3 contains database schema changes that are not present in 7.4.0.

System Updates

This release includes Rocky Linux OS 8.10 patches until July 6, 2025. Details can be found at https://rockylinux.org/news/rocky-linux-8-10-ga-release. FortiSIEM Rocky Linux Repositories (`os-pkgscdn.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.

Known Issues

1. If you enable or disable a parser and then click **Apply**, then most events that were previously parsed, may now fail to be parsed. This issue was newly introduced in 7.3.3 and fixed in 7.3.4.

   If you have already upgraded to 7.3.3 and see this issue, then upgrade to 7.3.4 or follow the steps below if you want to stay in 7.3.3.

   a. Take a GUI screenshot of the current parser order.
   b. Click **Fix Order**. System parsers will be ordered correctly, and Custom parsers will be pushed to the bottom of the parser list.
   c. Click the **Up** or **Down** buttons to place these parsers in the correct position according to the screenshot.
   d. Click **Apply**.
   e. Before you enable/disable parsers again, Contact Fortinet Support for a patch. After you have deployed the patch, the issue will be resolved.

   If you have upgraded to 7.3.3 and are not seeing this issue, Contact Fortinet Support for a patch. After you have deployed the patch, you can work normally.

   If you have not upgraded to 7.3.3 but intend to upgrade, then Contact Fortinet Support for a patch. Then first upgrade to 7.3.3, apply the patch, and then you can work normally.

2. FortiSIEM 7.3.3 cannot be installed in IPV6 only environments.
3. If you are running HA and DR and can't login to GUI after Failback operation, then restart App Server.

REST API Enhancements

Enhanced Triggering Event API

Prior to 7.3.2, 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}`

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

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
1174772	Major	App Server	If you apply Windows/Linux Agent templates to large number of Agents (> 2000), then Windows Agent can receive HTTP 502/503 response code from App Server.
1165944	Major	App Server	Content Update only installs on 10 Workers at a time. You need to restart App Server to install update on next 10 Workers.
1157784	Major	App Server	On **CMDB** page, Event status column for some devices is empty, even though logs are received by FortiSIEM.
1152366	Major	App Server	Memory leak in LDAP discovery can cause App Server to be out-of-memory after many LDAP discoveries.
1151227	Major	App Server	After upgrading to 7.3.2, Custom Parsers and Custom Event Attributes no longer work.

Bug ID	Severity	Module	Description
1147132	Major	App Server	With large number of Windows/Linux Agents doing frequent discoveries, regular discoveries via SNMP, OMI, etc. may be blocked, and devices may not show up in CMDB.
1138386, 1170625	Major	App Server	Updating many CMDB Devices at a time is slow if there are many other devices in CMDB.
1148520	Major	App Server	On **Analytics** page, Check Reputation > FortiGuard IOC Lookup does not return results as the FortiGuard IOC Lookup API has changed.
1168458	Major	Generative AI	phGenerativeAI process can consume high CPU upon start up if there is a large number of user defined rules and reports.
1164326	Major	GUI	When there is a large number of Agents, **Admin > Health > Agent** page does not load.
1159210	Major	GUI	Many Chrome processes seen on Supervisor node while running PDF export.
1142995	Major	GUI	$ character is not allowed for Consumer Group field in Azure Event Hub Credential.
1165977	Major	Parser	Win-Security-4776-failure event is not parsed correctly.
1131056	Major	Parser	phParser module has a memory leak in handling incident events.
1126082	Major	Parser	When a value group is not found, phParser may crash.
1174775	Major	Query,Rule	Rule Worker and node.js process on workers can allocate large memory to process value groups.
1140325	Major	Rule	Rule sync may not work correctly, caused by phRuleWorker locking randomly on some worker.
1118432	Major	Rule	phRuleMaster may crash when disabling an active rule.
1173514	Minor	App Server	Applying a rule having CLEAR condition with Group By causes Sync Error as the rule is not formed correctly.
1172754	Minor	App Server	Limit the number of FortiGuard Malware domains to 3 million to avoid data overload.
1172404	Minor	App Server	In MSSP environments, sometimes deleting User, Collector or Organization does not work correctly and shows Exceptions in log.
1171669	Minor	App Server	Optimize App Server to handle the case where user has defined explicitly a list of parsers for CMDB devices.
1169673	Minor	App Server	External authentication for FortiSIEM users via RADIUS is not allowed. This feature was present in earlier releases.
1169022	Minor	App Server	For users with RBAC, Active Incident count is incorrect.
1167546	Minor	App Server	Deleted rules may trigger Incidents after rebooting App Server or

Bug ID	Severity	Module	Description
			the entire system.
1165687	Minor	App Server	For Service Provider deployments, if a Super Global User writes case notes for an incident, then those case notes can't be viewed by an Org level user viewing the same Incident.
1157351	Minor	App Server	Special characters are not allowed in passwords.
1145989	Minor	App Server	Clicking on Context from the Incident Details slide-in page sometimes resulted in a 502 Proxy Error (caused by whois server timeout).
1139200	Minor	ClickHouse Backend	Removing keeper or Replica in the ClickHouse Cluster fails to clean up table due to additional quote character.
1169567	Minor	Collector, Upgrade	6.2.0 collector upgrade to 7.3.3 failed due to 'No module named 'packaging''.
1173084	Minor	Data work	Trend Vision One Alert and Events severity is set incorrectly.
1155906	Minor	Data work	The rule Microsoft Entra: Identity Protection Risky User Identified, triggers for all risk Levels.
1157391	Minor	Discovery	FortiProxy is not added to CMDB as part of log based discovery.
1161875	Minor	Event Pulling Agents	Mimecast Event pulling jobs fail because of response parsing error.
1160111	Minor	Event Pulling Agents	In JDBC Audit log for Oracle DB, the "SQL_TEXT" column, which is the SQL statement run by the user on the database, is missing in the raw log.
1155023	Minor	Event Pulling Agents	Cisco AMP Agent and AWS Kinesis agent incorrectly sent SIGKILL to other processes when updating device info. This causes all Services except Agent Manager, to be killed after task update.
1151579	Minor	GUI	Fail to obtain FortiGate config using FORTIOS_REST_API.
1132651	Minor	GUI	Remove PostgreSQL Database JDBC > Audit in Credential definition.
1162245	Minor	Hardware Appliance	"configFSM.sh" run failed on hardware appliances after upgrade and factory reset.
1160680	Minor	Performance Monitoring	Fail to discover FortiSIEM nodes via SSH as hmac-sha2-256 and hmac-sha2-512 are forbidden.
1132630	Minor	Query	ClickHouse queries using filter 'HTTP Full Request' does not return results.
1161952	Minor	Rule Engine	Testing a rule fails if the test event is large. Current limit is 8192 Bytes, which is not sufficient for testing large CrowdStrike events.
1169431	Minor	System	Sometimes phMonitor crashes while downloading upgrade Image

Bug ID	Severity	Module	Description
			- this happens when taskId is very large after running for a long time.
1167071	Minor	System	phFortiInsightAI module may fail to start after upgrading to 7.3.2 and adding as a Follower node.
1166127	Minor	System	Upgrade does not work correctly when FortiSIEM version's major, minor, or patch numbers are two digits. For example upgrade from 6.7.10 fails. Workaround is to change the version number to say 6.7.9 before upgrade. This issue is resolved in this release and no workaround is required if say upgrading from 7.3.10.
1152449	Minor	System	Excessive Redis connection error log may cause '/opt' disk full on Supervisor.
1148164	Enhancement	App Server	Provide the ability to create a ServiceNow field by combining multiple FortiSIEM Incident fields values.
1140285	Enhancement	App Server	The REST API '/phoenix/rest/pub/incident/triggeringEvents' may not always return data in a busy system. A new API is introduced. See FNDN for details.
1150789	Enhancement	Data work	Windows XML Parser does not parse Relying Party value from the raw event log of ADFS logons, (windows event ID 364).
1167404	Enhancement	Discovery	Support SNMPv3 with 'AES 256 Cisco' encryption algorithm.
1177090	Enhancement	GUI	Hourly updates are disallowed for Agent discovery and External Threat Intel Download.
1173437	Enhancement	GUI	From Incident slide in > Triggering Events, an option is provided to run an Analytics query to show the Triggering Events. This enables an easy way to further investigate the events in **Analytics**.
1171390	Enhancement	System	Enhance FortiSIEM upgrade to handle the situation where PostGreSQL version upgrade needs more disk space in /opt for an extra CMDB backup.

Implementation Notes

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

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 7.3.3, 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-7.3.3 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>
```

7.3.3 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>
```

Post-Upgrade ClickHouse IP Index Rebuilding

If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.3.3, then after upgrading to 7.3.3, 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, 7.3.0, 7.3.1 or 7.3.2 and have already executed the rebuilding steps, then nothing more needs to be done.

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

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

www.fortinet.com