Release Notes

FortiSIEM 7.3.4

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

07/29/2025
FortiSIEM 7.3.4 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
07/29/2025	Initial version of 7.3.4 Release Notes.

What's New in 7.3.4

This release contains the following bug fixes and enhancements.

If you upgrade to 7.3.4, your next upgrade must be 7.4.1 or later because 7.3.4 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 25, 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. FortiSIEM 7.3.4 cannot be installed in IPV6 only environments.
2. If you are running HA and DR and can't login to GUI after Failback operation, then restart App Server.

Bug Fixes

This release fixes the following issues:

Bug ID	Severity	Module	Description
1183681	Major	App Server	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.
1179987	Major	App Server	If you have large number of Agents, then App Server may be slow in responding to Status updates.
1181712	Minor	App	Content Update for Worker may fail in Cloud environment.

Bug ID	Severity	Module	Description
		Server	
1173862	Minor	System	Postgres is not upgraded on Collector side after collector upgrade.

Implementation Notes

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 7.3.4, 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-7.3.4 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>
```

7.3.4 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 7.3.4, then after upgrading to 7.3.4, 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, 7.3.2 or

7.3.3 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