FORTINET

Release Notes

FortiSIEM 7.3.5

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

10/06/2025
FortiSIEM 7.3.5 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
09/30/2025	Initial version of 7.3.5 Release Notes.
10/06/2025	Bug Fix 1206464 added to 7.3.5 Release Notes.

What's New in 7.3.5

This release contains the following bug fixes and enhancements.

If you are running 7.3.5, then you must upgrade to 7.4.2 or later. There was a security fix in 7.3.5, but it was not included in earlier 7.4.1, causing the upgrades to fail.

System Updates

This release includes Rocky Linux OS 8.10 patches until September 18, 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.

Known Issues

1. FortiSIEM 7.3.5 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 and Enhancements

The following bugs are resolved in this release.

Bug ID	Severity	Module	Description
1196070	Major	App Server	Optimize the Apply on Windows Agent > Host Template Association > Apply.
1193567	Major	App Server	Improve performance of Public Incident REST API - /phoenix/rest/pub/incident API.

Bug ID	Severity	Module	Description
1192432	Major	Event Pulling Agents	Microsoft Defender Alerts stops after a while due to pagination mishandling.
1203162	Major	GUI	Clicking on "Reformat" when editing system or custom parser will incorrectly encode CDATA definition inside the parser and test will fail.
1192774	Major	Upgrade	HA Super Cluster upgrade script does not work on AWS.
1201362	Minor	App Server	The public Incident REST APIs fail to return results in HA environment.
1194942	Minor	App Server	Upgrade to 7.3.4 may fail while deleting Sigma rules, when the rule has test events.
1203148	Minor	GUI, Parser	Modifying the event format recognizer to any string on a working custom parser will incorrectly test successfully.
1196219	Minor	Linux Agent	Linux Agent Monitor Status of is empty after restarting Linux Agent service.
1185262	Minor	Query	Analytic query involving Malware IPs does not work if a Malware IP entry is an IP range.
1206464	Minor	System	"configFSM.sh" run failed on HW during re-installation.
1200502	Minor	System	"configFSM.sh" run fails on 3600G after upgrade & regular factory reset.
1199999	Minor	System	Improve the performance of Collector upgrade via Supervisor via caching. If many collectors are doing yum upgrade simultaneously, then upgrade may fail.
1195950	Minor	System	Ansible task to restart ClickHouse Keeper service is incorrect.

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`

Identity and Location Related

If you are upgrading to 7.3.5, 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-7.3.5 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>
```

7.3.5 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 7.3.5, then after upgrading to 7.3.5, 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, 7.3.3 or 7.3.4 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