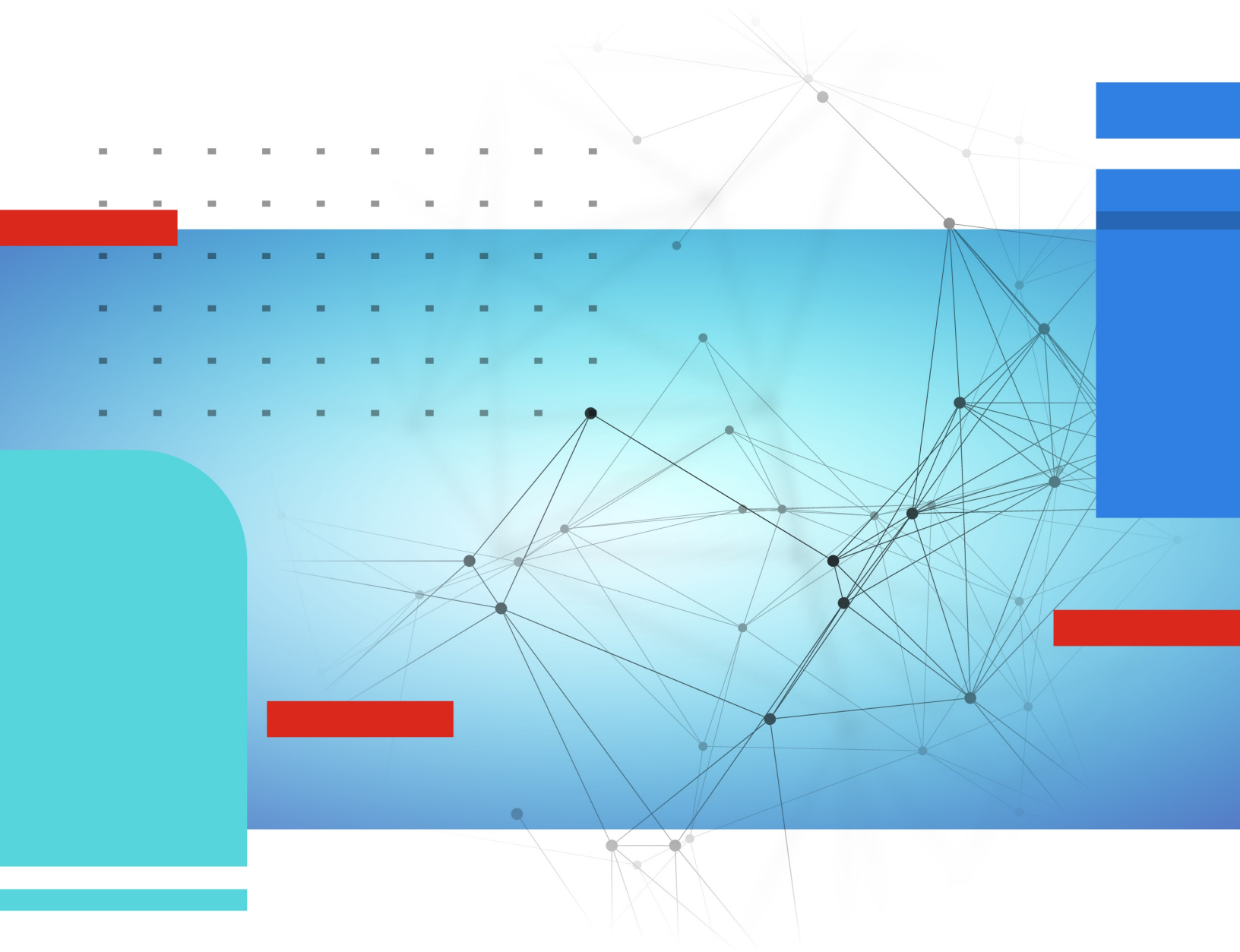
Release Notes

FortiSIEM 7.2.5



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

02/03/2025
FortiSIEM 7.2.5 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
01/31/2025	Initial version of the 7.2.5 Release Notes.

What's New in 7.2.5

This release includes Rocky Linux OS 8.10 patches until January 22, 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.

Note:

1. If you upgrade to 7.2.5 or are installing 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade to 7.3.0, since it is already released and 7.2.5 contains schema changes not present in 7.3.0.
2. Scheduling report bundle is not supported in HA deployments. This feature will be supported in a release after 7.3.0, with new version of HA introduced in 7.3.0

This release contains the following bug fixes.

Bug Fixes

The following issues are resolved.

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.
1043334	Major	GUI	CMDB Groups programmatic names show up in GUI for rule subpatterns instead of display names. These programmatic names may not be readable.
1113738	Major	Query,Rule	Query Worker and Rule Worker modules have memory leak that may cause memory consumption to be large after a few days.
1111377	Major	System	High memory usage on all of the Keepers.
1078106	Major	System	Excessive logging on `/var/lib/mod_security/` may cause the root disk to be full.
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.
1105800	Minor	App Server	PAYG emails go to old set of email addresses unless config is completely cleared and reconfigured.

Bug ID	Severity	Module	Description
1085995	Minor	App Server	After upgrading to 7.2.3, GUI Incident List View page may show 'TransactionRolledbackLocalException: Client's transaction' error.
1074113	Minor	Discovery	SNMPwalk_v3_packet_timeout does not take effect.
1108567	Minor	Event Pulling Agents	CrowdStrike API - not all events are always pulled when server sends incomplete events.
1097455	Minor	Query	Retention interval for Scheduled Report and Report Bundle is hard coded to 1 hour and GUI settings are ignored.
1112661	Minor	System	phMonitor process may crash on collector while trying to Download Image/Install Image.

Implementation Notes

General

1. Scheduling report bundle is not supported in HA deployments. This feature will be supported in a release after 7.3.0, with new version of HA introduced in 7.3.0
2. If you upgrade to 7.2.5 or are installing 7.2.5, then you must next upgrade to 7.3.1 or later. You cannot upgrade to 7.3.0, since it is already released and 7.2.5 contains schema changes not present in 7.3.0.

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
   ```

PostGreSQL Related

FortiSIEM 7.2.5 includes PostGreSQL v13.14 containing the patch for CVE-2024-0985.

- If you are doing a fresh install of FortiSIEM 7.2.5, then the patch is included and there is nothing to do.
- If you have upgraded to FortiSIEM 7.1.5 or later, then the patch is included and there is nothing to do.
- If you want to remain on FortiSIEM 7.1.4 or earlier, then you can't get this patch by running `yum upgrade`, since Postgres changed the repo gpg key as per this change (https://yum.postgresql.org/news/pgdg-rpm-repo-gpg-key-update/). To get this Postgres patch, on the Supervisor, run the following script:

curl -s https://os-pkgs-cdn.fortisiem.fortinet.com/postgres/misc/switch-pgdg-repo-and-upgrade-to-pg13.14.sh | bash -xe

Collector HA Related

1. If you have FortiSIEM Windows/Linux Agents reporting through Collectors and you decide to form a HA Collector Group with those Collectors, then you need to add all the Collectors in the HA Group to **Admin > Setup > Windows Agent > Host to Template Associations** and click **Apply**.
2. If you add a new Collector to an existing HA Collector Group, then the new Collector must be added as a Follower.
3. If a Collector is part of High Availability (HA) Cluster and you want to delete the Collector, then follow these procedures.

   Case 1: If the Collector is a Follower, then follow these steps:

   a. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Delete the Collector from CMDB.

   Case 2: If the Collector is a Leader, then follow these steps:

   a. Make the Collector a Follower Cluster in **Admin > Settings > System > Cluster Config**.
   b. Click **Save**.
   c. Remove the Collector from the High Availability (HA) Collector Cluster in **Admin > Settings > System > Cluster Config**.
   d. Click **Save**.
   e. Delete the Collector from CMDB.

4. 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 7.2.5, 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-7.2.5 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>
```

7.2.5 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 7.2.5, then after upgrading to 7.2.5, 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, 7.2.0, 7.2.1, 7.2.2, 7.2.3, or 7.2.4 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.

Upgrade Related

1. If you upgrade to 7.2.5 then you must next upgrade to 7.3.1 or later. You cannot upgrade to 7.3.0 since it is already released and 7.2.5 contains schema changes that are not present in 7.3.0.
2. 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.

www.fortinet.com