Release Notes

FortiSIEM 7.3.2

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 7.3.2 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
03/20/2025	Initial version of 7.3.2 Release Notes.
03/31/2025	Issue added under Implementation Notes > General.
04/02/2025	Issue updated under Implementation Notes > General.
04/17/2025	Known Issue (#4) added to 7.3.2 Release Notes.
05/14/2025	Upgrade Implementation for 7.2.6 added to 7.3.0-7.3.2 Release Notes.

What's New in 7.3.2

This release contains the following bug fixes and enhancements.

If you are running 7.2.6, then you cannot upgrade to 7.3.2. This is because 7.2.6 contains database schema changes that are not present in 7.3.2.

System Updates

This release includes Rocky Linux OS 8.10 patches until March 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.

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
1132656	Major	Hardware Appliance	Continuous HW Upgrade to 7.3.0 and 7.3.1 fails because of / root disk full.
1132182	Major	App Server	For ClickHouse based Enterprise deployments, Advanced Search - SQL Console is missing for new created Full Admin User.
1126806	Major	App Server	AppSvr may run out of thread pool when there is a large number of Agents device discoveries.
1131671	Major	Docker	phMonitor can't start on Docker Collector due to missing library file.
1092181	Minor	App Server	If user clears over 10k Incidents from UI, then App Server might encounter deadlock exception.
1134380	Minor	Data work	The event type group for FortiGate-event-ssl-vpn-session-new-con should not be logon success.

Bug ID	Severity	Module	Description
1124198	Minor	Event Pulling Agents	For multi-tenant Collector based deployments, Azure EventHub events are not being mapped to correct organization.
1126341	Minor	GUI	For multi-pattern Rules connected by OR relationship, GUI forces user to define inter-pattern constraints, which is not required.
1132112	Enhancement	Data work	Some Windows SIGMA rules have been tuned to remove false positives.
1099756	Enhancement	GUI	Increase the number of events that can be chosen to test Parsers from 10 to 50.
1116583	Enhancement	System	Support OVA template for VMware 7 and 8.

Known Issues

1. FortiSIEM 7.3.2 cannot be installed in **IPV6 only** environments.
2. External FortiSIEM GUI user authentication via RADIUS is not supported.
3. If you are running HA and DR and can't login to GUI after Failback operation, then restart App Server.
4. When a user removes a node (with <*ShardID*> and <*ReplicaID*>) from a ClickHouse cluster and then adds a new node with the same <*ShardID*> and <*ReplicaID*>, all the replicas in this shard will become read-only.

   Workaround

   Scenario 1: User deletes a node but has not added a new node to the shard

   a. Login to the deleted node via SSH and run the following command:

   ```
   /opt/phoenix/phscripts/clickhouse/cleanup_clickhouse.sh
   ```

   Scenario 2: User deletes a node and adds a new node to the shard

   a. Login to the deleted node via SSH and run the following command:

   ```
   /opt/phoenix/phscripts/clickhouse/cleanup_clickhouse.sh
   ```

   b. Login to one of the keeper nodes and run the following commands:

   ```
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.events/
   /opt/zookeeper/bin/zkCli.sh deleteall
   /clickhouse/tables/<ShardID>/fsiem.summary/
   /opt/zookeeper/bin/zkCli.sh deleteall /clickhouse/tables/<ShardID>/fsiem.mv_
   events/
   ```

   c. Login to each node in this shard and run the following commands:

   ```
   clickhouse-client
   SYSTEM RESTART REPLICA fsiem.events_replicated
   SYSTEM RESTORE REPLICA fsiem.events_replicated
   ```

```
SYSTEM RESTART REPLICA fsiem.summary
SYSTEM RESTORE REPLICA fsiem.summary

SYSTEM RESTART REPLICA fsiem.mv_t_events
SYSTEM RESTORE REPLICA fsiem.mv_t_events
```

Note: Use the following query to check the replica status:

```
clickhouse-client
select database, table, is_readonly, last_queue_update_exception, replica_is_active
from system.replicas
```

Implementation Notes

General

For Microsoft Azure Event Hub credential, the **Consumer Groups** field cannot contain $, e.g. $default is not allowed. This credential can be entered from **Admin > Setup > Credentials** tab. Please use a specific Consumer Group as a workaround.

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 7.3.2, 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-7.3.2 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>
```

7.3.2 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 7.3.2, then after upgrading to 7.3.2, 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 or 7.3.1 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 or 7.3.1 to 7.3.2 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