



Release Notes

FortiSIEM 7.2.6



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 7.2.6 Release Notes

TABLE OF CONTENTS

- Change Log 4**
- What's New in 7.2.6 5**
 - System Update 5
 - Bug Fixes and Enhancements 5
 - Implementation Notes 6
 - General 7
 - Linux Agent Related 7
 - PostGreSQL Related 7
 - Collector HA Related 8
 - Identity and Location Related 8
 - Post-Upgrade ClickHouse IP Index Rebuilding 9
 - Upgrade Related 9

Change Log

Date	Change Description
04/01/2025	Initial version of the 7.2.6 Release Notes.
04/02/2025	Implementation Notes > General > #1 updated.
05/14/2025	Note section added with 7.2.6 Upgrade information. Information originally only appeared under Implementation Notes.

What's New in 7.2.6

This release contains the following bug fixes and enhancements.

- [System Update](#)
- [Bug Fixes and Enhancements](#)
- [Implementation Notes](#)



If you upgrade to FortiSIEM 7.2.6 or are installing FortiSIEM 7.2.6, then the next upgrade must be strictly later than 7.3.2 or must be 7.4.0 or later. Specifically, upgrade from 7.2.6 to 7.3.0, 7.3.1, 7.3.2 is not allowed. But upgrade from 7.2.6 to 7.4.0 and later is allowed. This is because 7.2.6 contains database schema changes that are not present in 7.3.2 and earlier releases.

System Update

This release includes Rocky Linux OS 8.10 patches until March 26, 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
1138386	Major	App Server	Updating CMDB Device Properties for a large number of devices from the GUI is slow.
1133761	Major	App Server	Creating a custom CMDB Group based on Custom Properties Conditions does not work.
1126806	Major	App Server	AppSvr may run out of thread pool when there is a large number of Agents device discoveries.
1123315	Major	App Server	Incident Resolution Machine Learning job runs frequently (every 20 minutes) instead of daily, resulting in performance issues.
1084444	Major	App Server	Disabled rules in Enterprise mode still triggered incidents after upgrade.
1126082	Major	Parser	Parser on Supervisor may restart every 6-7 minutes.

Bug ID	Severity	Module	Description
1121714	Major	Query	Networks group queries do not return result in ClickHouse environments.
1094019	Major	Query	In DR environment, CSV export may not return results as the query goes to Secondary Supervisor node by mistake.
1074677	Major	Query	For EventDB, Analytics Search shows results only for the last ~40-60 minutes when custom attribute search is in use.
1052318	Major	Query	Queries for a single network in Resources > Networks do not return correct results.
1140325	Major	Rule	Rule Worker may lock up on a random worker after rulesync is pushed from Supervisor.
1118432	Major	Rule	RuleMaster may crash during rule enable/disable process.
1141055	Minor	App Server	After editing a system rule with multiple sub-patterns with OR condition and then deploying results in Sync errors.
1092181	Minor	App Server	If user clears over 10k Incidents from UI, then App Server might encounter deadlock exception.
1119222	Minor	ClickHouse	ClickHouse Event Integrity Checksum is not calculated and not shown on GUI after upgrade from 7.1.4 to 7.2.4.
1126341	Minor	GUI	Unable to save a rule if there are multiple sub-patterns and they are related by OR condition.
1131056	Minor	Parser	Parser slow memory leak.
1106839	Minor	Query	Running Analytics queries from a specific Organization shows Source IPs from other Organization Network group.
1125010	Minor	Windows Agent	Disk thresholds not working properly for labeled disks (e.g. C:/Data).
1116583	Enhancement	System	Support OVA template for VMware 7 and 8.

Implementation Notes

- [General](#)
- [Linux Agent Related](#)
- [PostgreSQL Related](#)
- [Collector HA Related](#)
- [Identity and Location Related](#)
- [Post-Upgrade ClickHouse IP Index Rebuilding](#)
- [Upgrade Related](#)

General

1. 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.
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
3. If you upgrade to 7.2.6 or are installing 7.2.6, then the next upgrade **must be later** than 7.3.2, or 7.4.0 or later. You cannot upgrade to earlier versions as 7.2.6 contains schema changes not present in 7.3.2 and earlier releases.

Linux Agent Related

If you are running Linux Agent on Ubuntu 24, then Custom Log File monitoring may not work because of AppArmor configuration. Take the following steps to configure AppArmor 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 7.2.6 includes PostgreSQL v13.14 containing the patch for [CVE-2024-0985](#).

- If you are doing a fresh install of FortiSIEM 7.2.6, 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 7.2.6, 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-7.2.6 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"/>
  </eventAttributes>
</identityEvent>
```

```

    <eventAttribute name="srcGeoCity" identityAttrib="geoCity" reqd="no"/>
    <eventAttribute name="srcGeoLatitude" identityAttrib="geoLatitude" reqd="no"/>
    <eventAttribute name="srcGeoLongitude" identityAttrib="geoLongitude" reqd="no"/>
  </eventAttributes>
</identityEvent>

```

7.2.6 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 7.2.6, then after upgrading to 7.2.6, 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, 7.2.4, or 7.2.5 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 7.2.6 or are installing 7.2.6, then the next upgrade **must be later** than 7.3.2, or 7.4.0 or later. You cannot upgrade to earlier versions as 7.2.6 contains schema changes not present in 7.3.2 and earlier releases.
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

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.