FORTINET

Release Notes

FortiSIEM 7.4.2

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

10/06/2025
FortiSIEM 7.4.2 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
10/06/2025	Initial version of the 7.4.2 Release Notes.

What's New in 7.4.2

This release contains the following bug fixes and enhancements.

If you are running 7.3.5 or 7.2.7, then you must upgrade to 7.4.2 or later. There was a security fix in 7.3.5 or 7.2.7, 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.

Bug Fixes and Enhancements

In addition, this release contains the following bug fixes.

Bug ID	Severity	Module	Description
1206464	Minor	System	"configFSM.sh" run failed on HW during re-installation.
1208166	Enhancement	System	Add retry to all ssh commands in the fsm_cluster_upgrade.py, to make upgrade robust.

Implementation Notes

1. For Rules written using Advanced Search, the column re-name as part of the SQL function AS needs to begin with a character (a-z, A-Z) and contain only alphanumeric characters.
2. In the enhanced Search functionality for Rules, Reports and CMDB Devices, Search and Filtering do not work together. That means, if you have filters set and then you do a Search, the Filters will be ignored.
3. You cannot set the phRecvTime attribute in custom parsers. That attribute records the time when an event is first received by FortiSIEM, and is a special attribute that key FortiSIEM functionality depends on.

4. If you are running an HA+DR environment, and you have failed over to DR site and promoted the DR site to Primary, then you cannot run the Automated Cluster Upgrade on the DR Supervisor. Your choices are
   - Bring back the original Primary, fail back, and then run Automated Cluster Upgrade on the original Primary.
   - If original Primary is not recoverable, then do the node-by-node upgrade on new Primary site.
5. Automation Service does not work when FIPS is enabled.
6. Upgrade from FortiSIEM 6.1.0 to 7.4.2 requires **32GB memory on Supervisor**. If you are running FortiSIEM 6.1.0 and have less than 32GB of memory on Supervisor, then increase the memory to 32GB and then upgrade to 7.4.2. Also, **Java VM memory should be at least 10GB**.
7. High Availability across Data Centers feature does not work with Automation Service feature.
8. Starting with Release 7.4.0, the following attributes cannot be used as Incident Attributes in **Rule Definition** > **Step 3: Define Action** > **Incident Attribute**. These attributes may be set by FortiSIEM and may be overwritten if the user sets them. If there are user-defined rules using these attributes, then you must rewrite these rules using other attributes.

   ```
   Event Type, Event Severity, Event Receive Time, Reporting IP, Reporting Device, Raw Event Log,
   Binary Raw Event Log, Event ID, System Event Category, Event Parse Status, Event Severity
   Category, Incident Source, Incident Target, Incident Trigger Attribute List, Event Description,
   Incident Detail, Incident Reporting IP, Reporting Vendor, Reporting Model, Event Type Group,
   Incident ID, Incident Status, Incident First Occurrence Time, Incident Last Occurrence Time,
   Incident View Status, Incident View Users, Incident Cleared Time, Incident Cleared User,
   Incident Cleared Reason, Incident Notification Recipients, Incident Ticket ID, Incident Ticket
   Status, Incident Ticket User, Incident Comments, Incident Resolution Time, Incident Externally
   Assigned User, Incident Externally Cleared Time, Incident Externally Resolution Time, Incident
   External Ticket ID, Incident External Ticket State, Incident External Ticket Type, Incident
   Notification Status, Incident Title, Event Parser Name, Incident Reporting Device, Supervisor
   Host Name, Raw Event Log Size, Retention Days, Reporting Country Code, Reporting Country,
   Reporting State, Reporting City, Reporting Organization, Reporting Latitude, Reporting
   Longitude, Incident Reporting Country, Incident Reporting Country Code, Incident Reporting
   State, Incident Reporting City, Incident Reporting Organization, Incident Reporting Latitude,
   Incident Reporting Longitude, First Seen Time, Last Seen Time
   ```

9. If you are upgrading to 7.4.2, 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-7.4.2 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>
   ```

7.4.2 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>
```

10. **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.
    a. Login as root user.
    b. 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.
    c. 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.
    d. 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,`
    e. Run the following command to reload the rsyslogd AppArmor profile and apply the changes above.
       `apparmor_parser -r /etc/apparmor.d/usr.sbin.rsyslogd`
11. If you are upgrading ClickHouse based deployment from pre-7.1.1 to 7.4.2, then after upgrading to 7.4.2, 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.x, 7.4.0 or 7.4.1 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.

www.fortinet.com