FORTINET

Release Notes

FortiSIEM 7.4.1

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

10/09/2025
FortiSIEM 7.4.1 Release Notes

TABLE OF CONTENTS

Change Log **4**
What's New in 7.4.1 ..... **5**
System Updates 5
Features 5
High Availability across Data Centers 5
Bug Fixes and Enhancements 5
Implementation Notes 11

Change Log

Date	Change Description
09/22/2025	Initial version of the 7.4.1 Release Notes.
09/30/2025	Implementation Notes updated in 7.4.1 Release Notes. Also Known Issues removed and merged into Implementation Notes.
10/06/2025	Added Key Enhancements > Device Support > Dynatrace for 7.4.1 Release Notes.
10/09/2025	Bug Fix 118924 added to 7.4.1 Release Notes.

What's New in 7.4.1

This release contains the following features, bug fixes and enhancements.

- System Updates
- Features
- Bug Fixes and Enhancements
- Implementation Notes

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.

Features

High Availability across Data Centers

This release enhances previously released High Availability functionality by allowing Supervisor nodes to be in different Data Centers, so long as the latency between Data Centers is lower than a threshold (50 ms [millisecond]). This solution does not need Virtual IP (VIP) or DNS Configuration, and the same solution works in both on-premises and cloud deployments.

If you are in pre-7.3.0 version and running High Availability with manual failover, then you need to delete the Follower nodes and do a new HA Deployment.

If you have deployed automated HA introduced in 7.3.0, then upgrade will automatically convert to the new HA setup.

For details about HA Configuration and upgrade options, see here.

This feature works in both ClickHouse and EventDB environments. This feature does not work with Automation Service feature introduced in 7.4.0.

Bug Fixes and Enhancements

The following bugs are resolved in this release.

Bug ID	Severity	Module	Description
1193567	Major	App Server	App Server performance may be impacted when user runs public Incident REST API - /phoenix/rest/pub/incident API over a large time window containing large number of Incidents.
1185567	Major	App Server	Using Public REST API, all Watchlists can be retrieved using org credentials.
1181712	Major	App Server	Content Update for Workers may fail in Cloud environment.
1179987	Major	App Server	Large number of Agent Status updates can cause high resource usage on App Server.
1176199	Major	App Server	After scheduling to run a report bundle separately for each org, users received report from Super/Local, but not from org.
1175417	Major	App Server	User password cannot be saved from User Profile page.
1174772	Major	App Server	Applying Windows/Linux Agent template with large number of agents can cause Agent to receive 502/503 response code.
1171711	Major	App Server	Content Update for Collectors may fail as task is sent with http and local IP address instead of https with FQDN.
1170625	Major	App Server	For a large CMDB, device update may cause GUI to be slow.
1169628	Major	App Server	Content Update may not complete when there are large number of workers.
1152366	Major	App Server	When there are large number of group changes, LDAP discovery can cause OutofMemory error.
1147132	Major	App Server	Many simultaneous Agent Discoveries may block Regular Discoveries from completing.
925646	Major	App Server	Improve performance of rearranging Parser order via Up/Down options, especially when there is a large number of parsers.
1192432	Major	Event Pulling Agents	MS Defender alert pulling may stop after a while due to pagination mishandling.
1168458	Major	Generative AI	Generative AI module may cause high CPU usage upon startup if there is a large number of user defined rules and reports.
1171393	Major	Performance Monitoring	Unable to collect performance metrics from FortiGate firewall via REST API because the APIs have changed.
1174775	Major	Query, Rule	Rule Worker and node.js process on workers can allocate large memory to process value groups.
1161952	Major	Rule	Testing a rule with a large event may cause RuleEngine failure to evaluate the rule.
1162245	Major	System	configFSM.sh run failed on hardware appliances after upgrade and factory reset.

Bug ID	Severity	Module	Description
1169431	Major	Upgrade	phMonitor may crash on Collector during Download Image if taskId is very large.
1194203	Minor	App Server	Org level Full Admin user in Enterprise deployments may not be able to edit a rule.
1186649	Minor	App Server	Running Osquery from Resources > Osquery > Run Live may not get result.
1183111	Minor	App Server	When a rule is deleted, Incidents triggered from that rule are not cleared.
1182536	Minor	App Server	Sometimes, GUI is unable to load Incidents by time due to SQL length limitations, when there is an incident with many related incidents (common IP or host name).
1180043	Minor	App Server	In Search, the Sorting order of COUNT (DISTINCT...) cannot be saved.
1178915	Minor	App Server	FortiSIEM admin user cannot edit its password twice in the last 24 hours, but custom user can.
1177162	Minor	App Server	If a Parser is removed, then 'NullPointerException' occurs when clicking Parser > 'Fix Order'.
1172404	Minor	App Server	Delete User, Collector and Org are not working correctly and Exceptions show in log.
1167546	Minor	App Server	Deleted rule may trigger Incidents again after reboot.
1165687	Minor	App Server	Case notes written by Super Global User cannot be viewed in Org level.
1156003	Minor	App Server	When Email Template Configuration is saved, color style is stripped.
1145989	Minor	App Server	Context Tab within the Incident Details page throws 502 Proxy Error because of whois server timeout.
1101455	Minor	App Server	Remediate Incident on Reporting Device with FQDN throws proxy error because of whois server timeout.
1179095	Minor	Automation Service	For User with no Automation role, Incident slide incorrectly says FSM Automation is unreachable.
1136062	Minor	Automation Service	Incident details Automation Status doesn't show the correct status when playbook is deleted.
1163236	Minor	ClickHouse Backend	Under some circumstances, ClickHouse system tables may take disk space away from event tables.
1189867	Minor	Discovery	Reduce the number of Linux processes discovered by Linux Agent.

Bug ID	Severity	Module	Description
1172145	Minor	Discovery	FortiGate 7.6.3 REST API based discovery needs to be updated to latest APIs.
1181924	Minor	Event Pulling Agents	Alerts were not pulled from Sophos Central API due to incorrect start time.
1178548	Minor	Event Pulling Agents	Unable to integrate Cyble Threat Feeds (STIX/TAXII 21) because of URL parsing issue.
1169951	Minor	Event Pulling Agents	Not all CrowdStrike events are always pulled, especially when server sends incomplete events.
1168114	Minor	Event Pulling Agents	Unable to get the correct host name for MSSQL/Oracle events.
1167810	Minor	Event Pulling Agents	HTTP Generic Poller needs enhancement for integration with SAP ETD.
1161875	Minor	Event Pulling Agents	MIMECAST event collection may fail because of additional '='causing error to get token with "ValueError:too many values to unpack" error.
1160111	Minor	Event Pulling Agents	In JDBC Audit log for Oracle DB, the "SQL_TEXT" column, which is the SQL statement run by the user on the database, is missing in the raw log.
1135737	Minor	Event Pulling Agents	Generic HTTPS Poller: Cursor based pagination for SentinelOne APIs fail as they expect all params with cursor.
1191291	Minor	GUI	Incidents > List by Device/Rule: 'Clear all Incidents' under a group dropdown should only clear incident under that group.
1187194	Minor	GUI	On Host To Template Associations page, the status of the checkbox disappeared after performing a search.
1181378	Minor	GUI	Selecting Actions > Update from FortiGuard Malware IP/Domain/URL IOCs does not let you schedule an update.
1176881	Minor	GUI	Super/Global User can schedule org level report, but email is never delivered.
1174898	Minor	GUI	Run remediation window failed to open for Incidents if Quick Info on any Reporting Device fails.
1164094	Minor	GUI	Allow user to choose Report PDF > Summary mode display when creating a PDF under Analytics.
1161621	Minor	GUI	After disabling a rule from FortiSIEM Manager Incident page for a FortiSIEM instance, the rule is still active in FortiSIEM Manager.
1179327	Minor	Linux Agent	Linux Agent Discovery still happens every one hour, even if the discovery interval in template is 1 day.

Bug ID	Severity	Module	Description
1186746	Minor	Parser	Retention policy is not applied for event not matching any parser (Unknown_EventType).
1185262	Minor	Query	Analytic query involving Malware IPs does not work if a Malware IP entry is an IP range.
1175064	Minor	System	Collector Apache password hashes can get overwritten on worker (causing mod_sec to block the Collector).
1171390	Minor	System	Upgrade may fail due to /opt being full because two CMDB backups are created when Postgres version is upgraded.
1166127	Minor	System	Upgrades should handle double digits in FortiSIEM version's major, minor, or patch numbers.
1185563	Minor	System, Upgrade	Offline upgrade fails because proxy rules that forward os-pkgs-r8 for normal upgrades is not disabled.
1194246	Minor	Windows Agent	HOSTNAME parameter does not take effect when installing the Windows Agent via the command line.
1137467	Enhancement	Automation Service	Need to add Organization column to Automation Agent Health page.
1191491	Enhancement	Data work	Support Azure Event Hub Parser new schema.
1188105	Enhancement	Data work	MS365DefenderParser fails to parse urlEvidence field.
1187977	Enhancement	Data work	Some of the events received from Palo Alto Firewall are not parsed.
1187923	Enhancement	Data work	CitrixNetScalerParser not fully parsing the events field for 'NETSCALER-AAATM' event type.
1187314	Enhancement	Data work	Create separate FortiNDR Rules based on alert severity.
1186204	Enhancement	Data work	Create separate MS Defender incidents based on Alert severity.
1182666	Enhancement	Data work	Event Attributes like login type, device compliance, trust type are not parsed in Office365 Parser.
1182231	Enhancement	Data work	Oracle OCI events have unknown event type (because of updated oracle OCI event format).
1179846	Enhancement	Data work	FalconDataRepParser overwrites reptDevIpAddr incorrectly and creates duplicate CMDB entries.
1179251	Enhancement	Data work	Parse MFA attributes from Azure Entra events.
1179012	Enhancement	Data work	FortiGate parser is missing the FortiGate log Field 'keyword'.
1178503	Enhancement	Data work	WinOSWmiParser does not parse specific events attributes correctly in German Language.
1178218	Enhancement	Data work	GCP logs are not parsed as GCP Log Header changed.

Bug ID	Severity	Module	Description
1174895	Enhancement	Data work	Palo Alto Panorama event not parsed.
1174648	Enhancement	Data work	Windows - Win-App-MsiInstaller-11724 has incorrect event name and missing event type Win-App-MsiInstaller-11707.
1174475	Enhancement	Data work	Reduce Windows raw event size by removing duplicate rendering info.
1174228	Enhancement	Data work	User is parsed incorrectly in Win-Security-4728 Is Incorrect.
1173084	Enhancement	Data work	Trend Vision One Alert and Events severity is set incorrectly.
1171154	Enhancement	Data work	Add AWS WAF dashboard.
1170190	Enhancement	Data work	Some AWS ELB events aren't parsed when msg field doesn't have appTransportProto.
1168011	Enhancement	Data work	NonInteractiveUserSignInLogs' category events coming out of Azure Event hub configuration are not parsed.
1166390	Enhancement	Data work	Add AWS Elastic Container Service (ECS) dashboard from cloudtrail-ecs logs.
1165977	Enhancement	Data work	WinOSXmlParser issue.
1165522	Enhancement	Data work	Not parsing Domain correctly in Crowdstrike-Falcon-DetectionSummaryEvent-Intel-Detection Event Type.
1162344	Enhancement	Data work	Nutanix parser update for unparsed events.
1161986	Enhancement	Data work	Add support for Claroty CTD ActivityLog in CEF RFC 5424 format.
1159554	Enhancement	Data work	Cisco ASA parser doesn't parse Direction field.
1158917	Enhancement	Data work	Office365Parser does not parse the 'ModifiedProperties' from the Azure Active Directory event logs.
1156317	Enhancement	Data work	Trend Micro Vision One events: Event Receive Time is not the same as Event Occur Time.
1154394	Enhancement	Data work	Add log parsing for Veeam Backup & Replication events.
1150789	Enhancement	Data work	WinOSXmlParser does not parse msg field on eventID 364.
1141448	Enhancement	Data work	Enhance FortiEDR Rules with Message ID in Group BY.
1121079	Enhancement	Data work	Update Squid Web Proxy Parser to support squid 5.5.
1105482	Enhancement	Data work	Add support for FortiSRA.
1167404	Enhancement	Discovery	Support SNMPv3 with 'AES 256 Cisco' encryption algorithm.
1185098	Enhancement	GUI	Should forbid user to sort parsers in ASC/DESC order by Enable status.
1177090	Enhancement	GUI	Do not allow Hourly updates to Agent Discovery and External Threat Intel Download.

Bug ID	Severity	Module	Description
1173437	Enhancement	GUI	Provide a way to run Incident > Triggering Events Query in Analytics.
1164326	Enhancement	GUI	Add pagination in Admin > Health > Agent.
1159465	Enhancement	GUI	Allow users to set idle timeout value for multiple users.
1148164	Enhancement	GUI, App Server	For ServiceNow outbound Incident Integration, add support for mapping multiple FortiSIEM Incident fields to a single ServiceNow field.
1185167	Enhancement	Linux Agent	User is unknown in Linux Agent file monitoring events for Oracle Linux.
1183286	Enhancement	Linux Agent	Enabling fapolicy for Linux Server blocks Linux Agent from starting.
1143429	Enhancement	Linux Agent	Allow Linux Agent to be installed in customer specified target directory (not default in /opt).
1177137	Enhancement	New Device Support	Create Veeam Rules, Reports, Dashboard.
1071267	Enhancement	New Device Support	Support bitbucket integration.
1160417	Enhancement	Rule	Add more details about rule name/rule exception (Add/modify/remove) for PH_AUDIT_OBJECT raw events.
1181488	Enhancement	Threat Intel Integration	Support Any.run threat intel feed.
1174545	Enhancement	Threat Intel Integration	Remove DigitalSide Malware Domain and Malware IP threat feeds because they do not exist or are behind pay walls.
1106406	Enhancement	Threat Intel Integration	Support added_after TAXII2.1 URL parameter for python threatfeeds.

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 7.4.1 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 7.4.1. 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 7.4.1, 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-7.4.1 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>
```

   7.4.1 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 7.4.1, then after upgrading to 7.4.1, 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, or 7.4.0 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