Release Notes

FortiEDR 7.2.1

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

January 14, 2026
FortiEDR 7.2.1 Release Notes
63-721-1235215-20260114

TABLE OF CONTENTS

Change log

Date	Change Description
2026-01-12	Initial release.
2026-01-14	Updated Resolved issues on page 13.

FortiEDR 7.2.1 Release Notes

This document provides information about FortiEDR version 7.2.1.

Version history

	Central Manager	Core	Threat Hunting Repository
2026-01-12 (GA)	Build 7.2.1.0237	Build 6.1.0.1270	Build 7.2.1.0046

What's new

The FortiEDR 7.2.1 GA build includes the following features, enhancements, and changes:

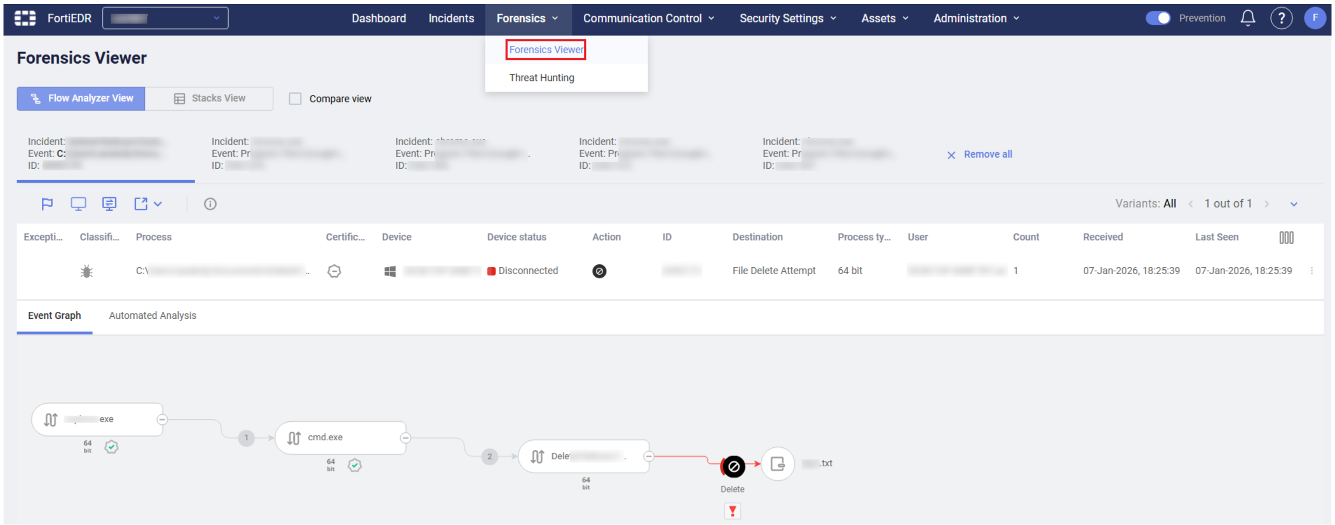
- Secure browser on page 6
- Forensics Viewer on page 6
- Behavior change to investigating inconclusive events on page 7
- Improvements to Collector filtering on page 8
- Customizing time zone for an organization on page 8
- Login enhancement for multi-tenancy on page 9
- GUI enhancements on page 9

Secure browser

This feature is disabled by default. See the FortiEDR 7.2.1 Administration Guide for more details.

Forensics Viewer

FortiEDR 7.2.1 adds back the *Forensics Viewer* with flow analyzer view, stacks view, and compare view. You can access it from the *Forensics* > *Forensics Viewer* menu or the *Forensics* button in *Incidents* view. The *Threat Hunting* menu has been moved under *Forensics* instead.



Forensics Viewer

Incident: [redacted]
Event: C:[redacted]
ID: [redacted]

Incident: [redacted]
Event: Pr[redacted]
ID: [redacted]

Incident: [redacted]
Event: Pr[redacted]
ID: [redacted]

Incident: [redacted]
Event: Pr[redacted]
ID: [redacted]

Incident: [redacted]
Event: Pr[redacted]
ID: [redacted]

Variants: All 1 out of 1

Excepti...	Classifi...	Process	Certific...	Device	Device status	Action	ID	Destination	Process ty...	User	Count	Received	Last Seen
		C:\[redacted] ..		[redacted]	🟥 Disconnected	⊘	[redacted]	File Delete Attempt	64 bit	[redacted]	1	07-Jan-2026, 18:25:39	07-Jan-2026, 18:25:39

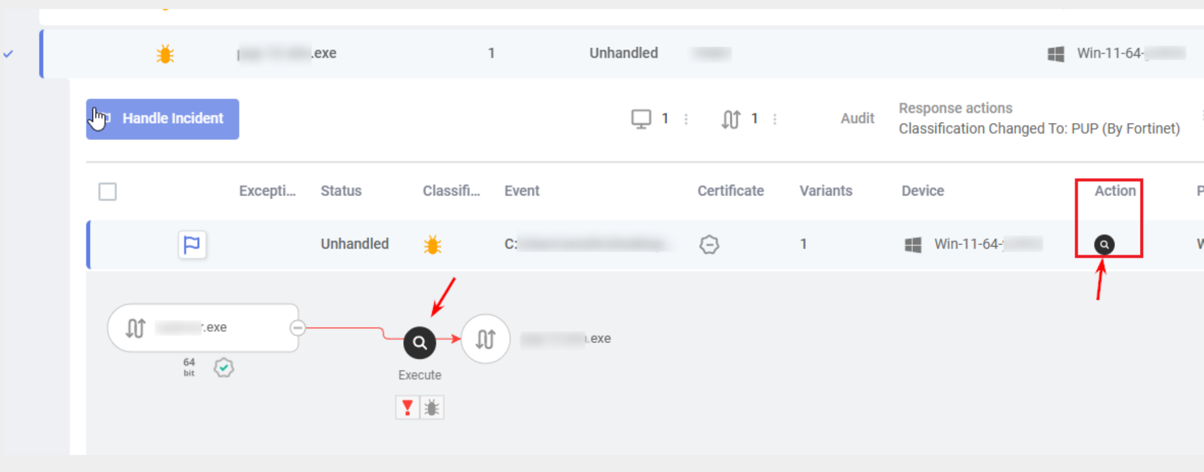
The Forensics functionality is unavailable for mobile incidents or secure browser incidents.

Behavior change to investigating inconclusive events

To reduce false positives in the *Incidents* view, FortiEDR 7.2.1 sends inconclusive events to FCS directly for investigation (without sending it to the *Incidents* view first) and shows such events in the *Incidents* view only if the FCS verdict is *Malicious* or *Suspicious*. The *Action* of such events will be *Post Detection* (🔍) or *Post Detection (Simulation)* (🔍), depending on whether FortiEDR is in *Prevention* or *Simulation* mode.

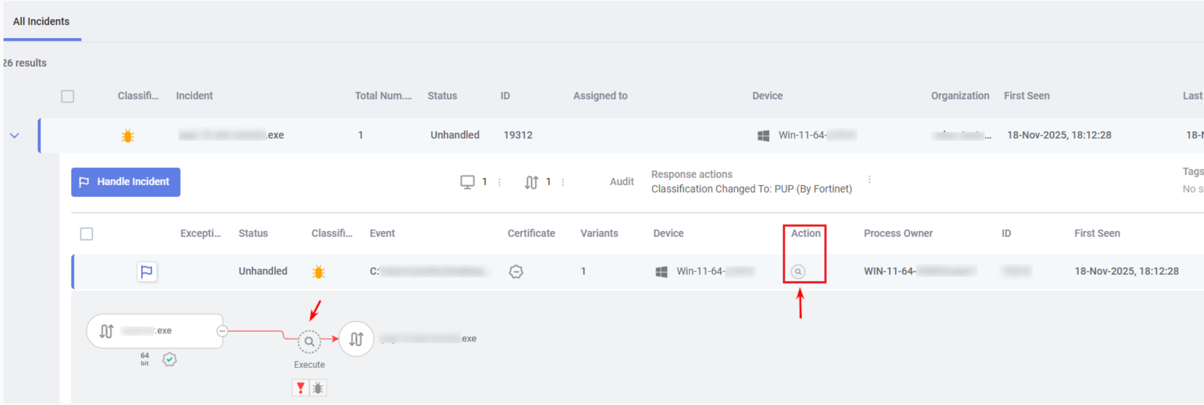
Post Detection means that the exfiltration attempt was detected after the FCS verdict, indicating that the event is already running on the Collector. We recommend isolating the Collector for security.

Post Detection



	Excepti...	Status	Classifi...	Event	Certificate	Variants	Device	Action
□		Unhandled		C:[redacted]		1	Win-11-64-[redacted]	🔍

Post Detection (Simulation)



All Incidents

26 results

□	Classifi...	Incident	Total Num....	Status	ID	Assigned to	Device	Organization	First Seen	Last
	✹	[redacted].exe	1	Unhandled	19312		Win-11-64-[redacted]	[redacted]...	18-Nov-2025, 18:12:28	18-N

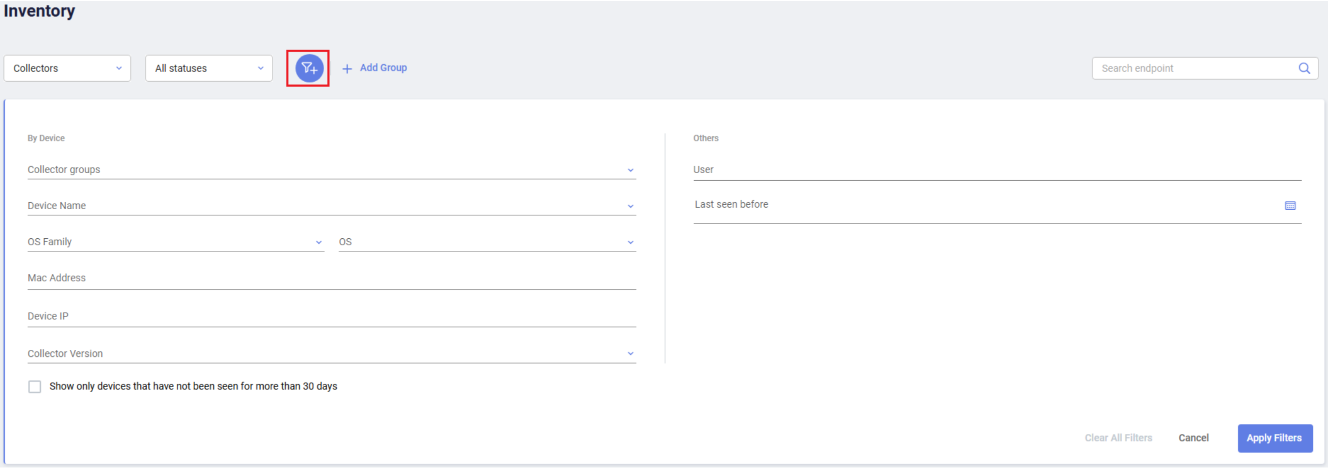
Handle Incident   1   1   Audit   Response actions
Classification Changed To: PUP (By Fortinet)   Tags
No s

□	Excepti...	Status	Classifi...	Event	Certificate	Variants	Device	Action	Process Owner	ID	First Seen
		Unhandled	✹	C:[redacted]		1	Win-11-64-[redacted]		WIN-11-64-[redacted]	[redacted]	18-Nov-2025, 18:12:28

Inconclusive events with an FCS verdict of *Safe* or *Likely Safe* will not appear in the *Incidents* view and will not be sent to FCS any more if it re-occurs.

Improvements to Collector filtering

In the *Assets* > *Inventory* page, use the new *Filter* (⛛+) button to narrow down the list of Collectors to display by various dimensions. The *Show only devices that have not been seen for more than 30 days* option allows you to display devices that have not been connected for more than 30 consecutive days, which are not counted for licensing purposes. Such devices are in the *Disconnected (Expired)* status.



Inventory

Collectors   All statuses   + Add Group   Search endpoint

By Device

Collector groups

Device Name

OS Family   OS

Mac Address

Device IP

Collector Version

□ Show only devices that have not been seen for more than 30 days

Others

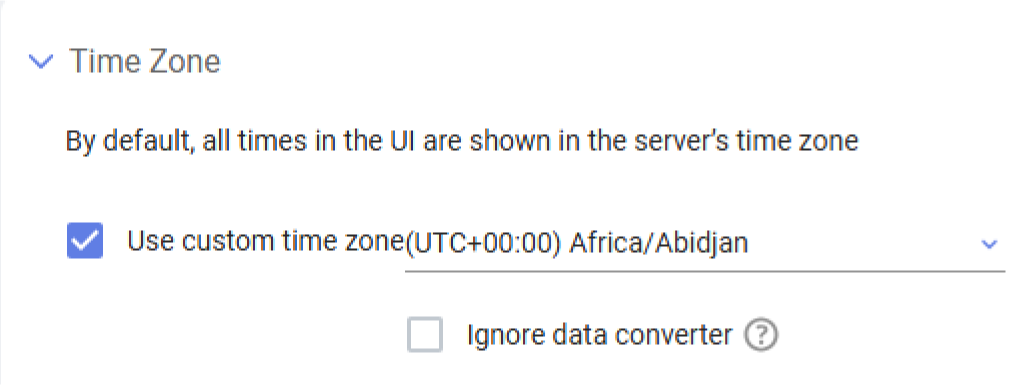
User

Last seen before

Clear All Filters   Cancel   Apply Filters

Customizing time zone for an organization

You can now configure the time zone for each organization under *Administration* > *Settings* > *Time Zone*. Use the *Ignore data converter* option to configure incident offsets. When the option is enabled, the converter data value according to the user’s time zone will not be used in the following modules: Incidents, Inventory, System Events, and Audit Trail.



Time Zone

By default, all times in the UI are shown in the server's time zone

☑ Use custom time zone(UTC+00:00) Africa/Abidjan

□ Ignore data converter ?

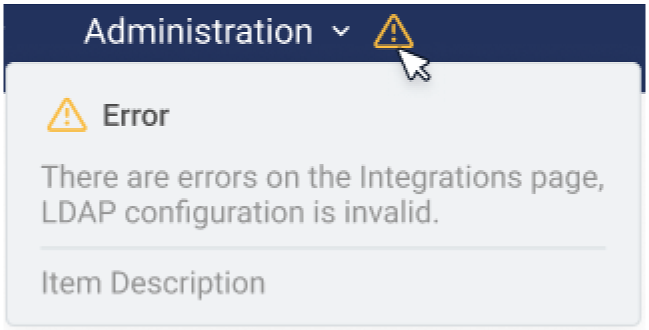
Login enhancement for multi-tenancy

Users of multi-tenancy environments no longer need to specify the organization name during login.

GUI enhancements

FortiEDR 7.2.1 includes the following enhancements to the GUI:

- "Raw data item" is renamed "variant"
- Usability improvements on device security card in Inventory
- Loading exceptions on supported Collectors only: FortiEDR 7.2.1 enforces that an exception is loaded only on Collectors supporting the fields in the exception. When you create an exception, warnings will appear if a specific field does not support some Collector versions.
- Added validation and float errors for the following fields when creating or editing a user:
  - 2FA
  - Password
  - Role Capability
  - Role
- Enhanced validation to exclusion fields
- Error reporting when reputation service is configured but not connected
- Error reporting for AV signature update failure
- Warning icon on *Administration* menu in case of error under the admin pages :



Error

There are errors on the Integrations page, LDAP configuration is invalid.

Item Description

Upgrade information

FortiEDR 7.2 Central Manager supports upgrade from 6.2, 7.0, or 7.2.0.

To upgrade your FortiEDR environment to 7.2.1, you must first obtain approval from Fortinet Support by creating a FortiCare ticket.

Supported browsers

The FortiEDR Central Manager console can be accessed using the following web browsers:

- Google Chrome
- Firefox Mozilla
- Microsoft Edge
- Apple Safari

Resolved issues

The following issues have been fixed in FortiEDR 7.2.1. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1219494, 1219006	The automatic upgrade option is removed from the UI as it does not work.
1234317	Navigation bar display issue for low screen resolutions.
1171377, 1170260	Non-aggregated event ID in custom connector.
1186639	Issue with "Scan executable files only" in file scan.
1158939	Error message is confusing when the host firewall rule description exceeds 255 characters.
1218426	Added "Process Owner" to the Incidents list.
1170992	Confusing error message in Connectors page.
1138142	Missing icon for *Add rule* button in host firewall page.
1171957	Disk encryption should not list the partial encrypt option for macOS.
1178979	Sorting by *Last Seen Descending* leads to unreadable data on the *Communication Control* page.
1185174	Deleting incident does not work after filtering.
1186141	No validation that aggregator mapping is unique for Collector move.
1188836	Misleading error message when a read-only user tries to enable a disk encryption policy.
1184678	UI refresh issue after a read-only user attempts to add groups to disk encryption or host firewall policies.
1163104	The *Add connector* drop-down menu should be sorted alphabetically.
1192877	The *IoT Device Discovery* and *Reputation Service* sections are missing under *Administration > Settings* for read-only users.
1194330, 1198164	On-premise Central Manager with proxy does not support fetching soar scripts file from GCP bucket.
1211611	Incident View sort issue.
1224803	Issue with username length limit.
1179295, 1179298, 1208433, 1153842	Improved performance of organization creation.
1230456, 1220014	Isolating a device and removing isolation does not work in *Investigation View*.

Bug ID	Description
1238237, 1215753	Incident ID is missing in syslog.
1174766, 1179507	An XDR event is displayed as unpopulated in *Incidents View*.
1188797, 1191908	Misalignment of classification.
1218624, 1222703	An unhandled security event shows empty in Dashboard.
1166556, 1184112	Misleading tooltip for *Revoke registration password*.
1159575, 1166684	Issue with device count display.
1182053, 1182450	Unmanaged devices display issue.
1186676, 1187253	An exception output in a syslog message.
1183540, 1187348, 1191060, 1188833	Exclusion path validation causes Collector degradation.
1182762, 1191427	User access connector fails to connect after credentials update.
1186218, 1189570	Inaccurate evaluation of license seats.
1187519, 1188322	Improved performance of *Get Logs* action.
1187126, 1196273	Issue with fetching threat hunting data when the organization is deleted.
1200914, 1201714	Issue with Linux Collector content upload.
1179001, 1202248, 1184113	Failure in exporting exception settings.
1199325, 1201707	list-products API query runs slow.
1177744, 1203931	Process name display issue in *Investigation View*.
1191006, 1205581, 1199216	A rare memory allocation issue.
1193913, 1205080	Error in configuration update.
1159891, 1219304, 1196888, 1201154	Covering query slows down with large number of destinations.
1202613, 1209301	Display issue in *Most Targeted* items view.
1204005, 1217350, 1235353, 1209298	Core dergadation issue.
1220710, 1209328, 1211303	Advanced search display issue related to policies list and device groups.
1204636, 1209664	Moving a collector results in a license error.
1210844, 1216877	Sorting inventory by *Last Seen* switches back to the default sort.
1218726, 1213231	Layout issue of a long path in event analysis view.

Bug ID	Description
1210853, 1217328	*Load Content* button extends left to cover *Content Version*.
1212148, 1216876	Consolidation status update sync issue.
1126928, 1216841	Event exception shows "with any script" instead of command line in the description.
1210689, 1217325	Cannot update existing threat hunting profile when associated to deleted categories
1217394, 1191006, 1219474, 1220588, 1221207, 1221209, 1225416, 1225928, 1227186, 1227190, 1228871, 1228776, 1230422, 1230989, 1232300, 1235808, 1236359, 1236360, 1238680, 1240019, 1240021, 1218992	Memory handling issue causing display update delays and errors.
1151334, 1220012	Internal IP is shown as N/A in *Investigation View*.
1055629, 1216874	GUI issue with creating an exception on command line.
1213961, 1218997	Error in saving new applications in *Application Control Manager* after organization migration.
1220688, 1225345	Error message popup in *File Scan*.
1225514, 1227791, 1225348	Cannot load events when a filter is selected in the *Incidents View*.
1226198, 1226608	Incident export file contains irrelevant data.
1211626, 1227651	No Collector report under *Application Usage* when you select an application in the *Communication Control* page.
1227059, 1230365	Inconsistent results when searching event ID.
1229819	Not all variants are displayed when using advanced filters in *Investigation View*.
1182542, 1198243	Deep scan failure when a duplicate IoT device is detected.
1112047, 1146557	Failure in updating license when the account name contains illegal characters.
1159891, 1163601	Saving a specific exception is slow.
1182540, 1183001	CVE links in *Communication Control* goes to the old site instead of the new one.

Bug ID	Description
1207734, 1207962 1198710	Failure in saving a new LDAP connector.
1145570, 1156914	Error when converting query.
1239105	Action buttons are not available in the *Users* page.
1198716, 1194524, 1200942	Deleting an organization from API does not force delete by disconnecting Collectors.
1231251, 1232168, 1232649	Incidents with identical process names appear as separate incident entries.

Refer to What's new on page 6 for a list of new features, enhancements, and changes. Refer to Known issues on page 17 for a list of known issues.

Known issues

The following issues have been identified in FortiEDR 7.2.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

New known issues for 7.2.1

There is no new known issue for 7.2.1.

Existing known issues from 7.2.0 or earlier

Bug ID	Description
1048824	Dashboard time range filter does not work.
1050795	No message to explain why the user cannot set the UI to prevention mode when all policies are in simulation mode.
1050797	Clicking on *Collectors by version* in Dashboard view does not lead to the Collectors Inventory view.
1051326	Device security should be N/A for disconnected devices.
733557	A Collector may fail to install or upgrade on old Windows 7 and Server 2008 devices that cannot decrypt strong ciphers with which FortiEDR Collector is signed. **Workaround:** Patch Windows with Microsoft KB that provides SHA-256 code sign support.
733559	Some AV Products, including Windows Defender and some versions of FortiClient, require that their realtime protection be disabled in order to be installed alongside a FortiEDR Collector. This is the result of FortiEDR registration as an antivirus (AV) in the Microsoft Security Center that was introduced in V4.0. Although there is no need for more than a single AV product to be installed on a device, FortiEDR can be smoothly installed, even if there is another AV already running. However, there are some other products whose installation fails when there are other AV products already registered. **Workaround:** Disable realtime protection on the other product, or remove FortiEDR’s AV registration with Microsoft Security Centervia UI.

Bug ID	Description
733560	SAML Authentication can fail when used with Azure SSO due to exceeded time skew. **Workaround:** Sign out and then sign in again to Azure so that the date and time provided to FortiEDR are refreshed.
733592	Number of destinations under communication control is limited to 100 IP addresses.
733595	Limited support when accessing the Manager Console with Internet Explorer, EdgeHTML and Safari 13 or above. Chromium Edge is supported, as well as Chrome, FireFox and Safari 11 and above.
733598	Safari 11.1 on macOS malfunctions when viewing events.
733600	A newly created API user cannot connect to the system via the API. **Workaround:** Before sending API commands, a new user with the API role should log into the system at least once in order to set the user's password.
733601	Isolation and communication control connection denial are not supported with Oracle Linux Collectors.
733603	**Downgrading the Collector Version:** When downgrading and restarting a device, the Collector does not start. **Workaround:** Uninstall the Collector, reboot the device and then install the older version.
757253	FortiEDR Connect cannot be used to run commands that are user-interactive.
759573	Collector upgrade via custom installer requires password.
765648	On Linux, threat hunting exclusions only work in kernel space mode, not in user space mode.
765785	In the presence of an email filtering system and/or a mail transfer agent that modifies the URL content, the installer download URL might include space(s) or %20s in it, which are added by the system/agent. This results in a signature error message from the installer storage. **Workaround:** In such cases, the URL should be amended to drop the redundant space/%20 before it can be used.
771044	SAML authentication cannot work with different organizations that use the same SAML Azure account. **Workaround:** Use different Azure accounts for different FortiEDR organizations.
771619	Organization filter under Threat Hunting Hoster view malfunctions.
771630	Device internal and external IP is missing from Threat Hunting events of Linux devices.
772449	In Windows Security Center > Virus and Threat Protection, when you click "open app", end-user notification is presented instead of the FortiEDR tray app.
777707	Linux Collector content file is large and uploads slowly to the Central Manager.

Bug ID	Description
786156	Windows security center registration is not supported with Windows servers 2019 and above.
807930	Application Control search only works by exact match
809060	FortiEDR Connect session may be disconnected due to inactivity of the FortiEDR Console, even though the Connect session is active.
811290	It is not possible to redirect FortiEDR web to a URL that is different than the one provided by Fortinet.
833152	Raw data IDs appearing in the Collector tray and Event Viewer may differ.
837038	Application Control cannot remove multiple tags in one action.
842110	In some network configurations, a rare issue might cause Collectors to be detected as IOT devices
885691	Threat Hunting: The tooltip displayed when hovering might prevent access to adding a filter.
886740	The Rest API might return a null pointer exception for missing parameters. **Workaround**: Provide AllUser parameter in the request.
889410	When switching to Threat Hunting from Event Viewer->Automated Analysis, queries malfunction when more than one device is involved **Workaround**: Filter by the same Collectors directly from Threat Hunting, which brings results.
890339	"Query Parsing Failed" in Threat hunting pops up multiple times after invalid query.
	891668 Free text query in threat hunting, when using invalid text, no error message is displayed. The query returns empty results.
892109	Unable to filter by empty registry names in facets in Threat Hunting.
894384	In Threat Hunting, clicking *Retrieve Target File* for "File Rename" events retrieves the old file name instead of the renamed one.
899736	In a threat hunting search, if you search for "Target.Registry.Path:" AND "Registry.Path" the results will be empty **Workaroun**d: Use either "Target.Registry.Path" or "Registry.Path" in a specific search.
907362	Remote shell does not work on Windows XP and Windows Server 2003.
	909654 IoT filter by ״First connection=Today״ brings empty results
912000	Failure to edit a Hoster user when a local user has the same name.
914348	Investigation View: Incident response data is inaccurate.
914792	Unarchiving all events in large environments might cause the Central Manager to malfunction. **Workaround**: Filter events before unarchiving to reduce unarchive size.

Bug ID	Description
915698	In the Investigation View, the message is wrong in the *Block address on firewall* window when you click *Firewall Block*.
935001, 938847, 1048422, 1064821, 1066657	System event page default filtering is required.
939481	In some cases, the communication control feature does not work due to unforeseen technical issues. **Workaround:** Troubleshoot and upgrade the Central Manager.
938512, 993729	LDAP authentication fails sporadically.
954553, 969494	Some event log entries in threat hunting display logged event values in incorrect logged event fields .
971692, 976687	IoT entries in Audit Log.
973252	Disconnected Collectors using an old registration password that was deleted from the Console are incorrectly classified as expired (with a status of "**Disconnected (Expired)**" instead of "**Disconnected**") and are excluded from license count.
982543	Cannot move a Collector to a different group via Rest API.
988884	Incorrect threat hunting profile order of Fortinet pre-defined application profiles.
989389	REST API file scan: no errors with invalid input for scanSelection.
989390	Inventory Collectors display has a column style issue when no Collectors exist.
989391	The "Organization" field is a mandatory field when using the File Scan Rest API when the environment includes no organizations. **Workaround**: When using this API, provide the "Organization" field with the value from *Administration > Licensing > Name*.
989392	REST API file scan: unclear error when "organization" is not sent in multi-tenancy setup.
989393	Rest API UI - The description is missing information under the "Policies" tab.
994297	REST API - Error 400 on admin/list-system-summary.
994324	Improve "file permission change" text in Threat Hunting Exclusions display.
994334	Added Threat Hunting columns re inaccessible unless the columns are narrowed.
994348	Log does not contain concrete helpful errors for API.
994359	Threat Hunting Collection Profiles - rule name and icon not aligned.
994364	The API for moving a Collector to a high security group can be triggered even if the Collector has already been moved.
994415	REST API File Scan - unsupported configurations should be removed.
994421	REST API - Scan selection for full scans should be disabled.

Bug ID	Description
1001334	Security events fully covered by an exception retains the full coverage indication icon even after new uncovered raw data items come in.
1003257, 1025493	Missing field in Checkpoint firewall integration
1014223, 1015341	Unable to reset a two-factor authentication token for LDAP users.
1014489, 1035403	Failure to delete aggregations in big bulks over 20K.
1039714, 1041152	Confusing error message when uploading a wrong formatted file in *Application Control Manager > Upload Applications*.
1040055, 1041151	Ad hoc network discovery tooltip has a mistake in Japanese
1040805, 1048215	Event Viewer count changes with sort.
1042454, 1044053	In Events Viewer, Triggered Rules message includes a reference to the removed *Forensics* tab.
1052668, 1060356	Syslog is created with no audit.
1062894, 1063406	No validation for SecurityExclusionRepoEntity.path in exclusions configuration.
1079894, 1081873	Exceptions report can be slow.

www.fortinet.com

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.