Release Notes

FortiEDR 7.2.3

February 26, 2026
FortiEDR 7.2.3 Release Notes
63-723-1257653-20260226

TABLE OF CONTENTS

Change log

Date	Change Description
2026-02-26	Initial release.

FortiEDR 7.2.3 Release Notes

This document provides information about FortiEDR version 7.2.3.

Version history

	Central Manager	Core	Threat Hunting Repository
2026-02-26 (GA)	Build 7.2.3.0085	Build 6.2.0.1102	Build 7.2.3.0087

What's new

The FortiEDR 7.2.3 GA build includes the following features, enhancements, and changes:

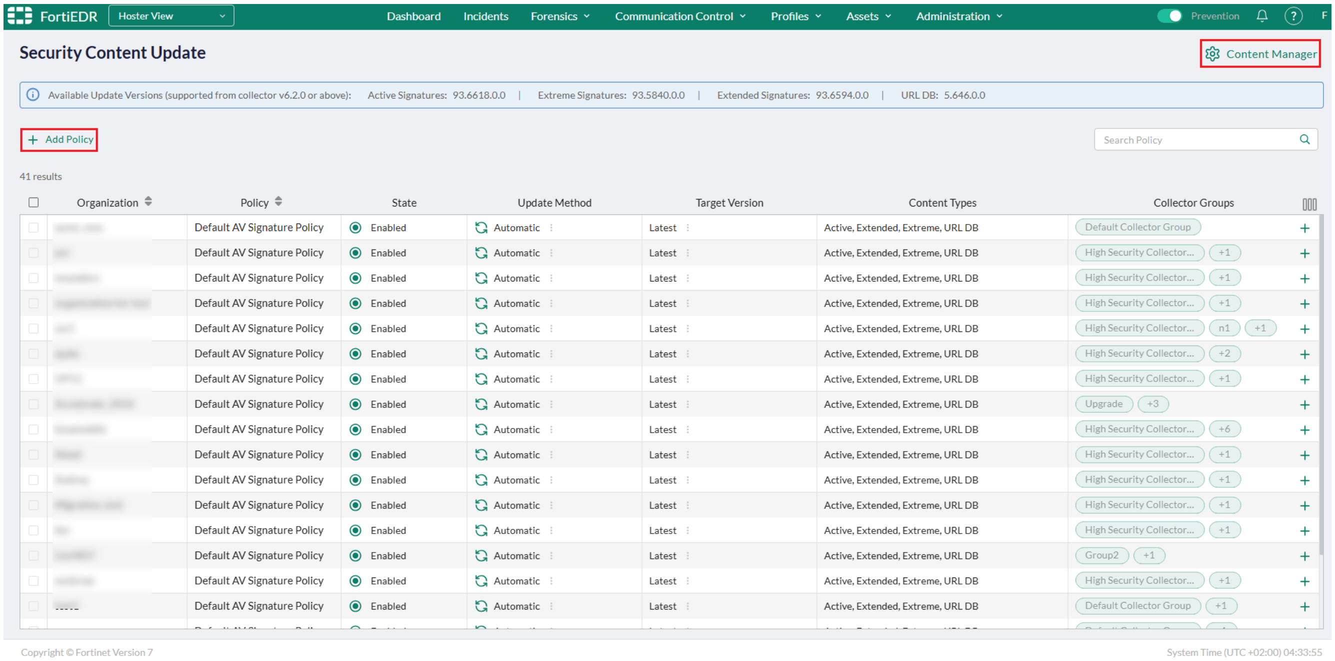
- On-premise deployment in air-gapped environments on page 6
- New AV Signature policy on page 6
- New color scheme of the Central Manager console on page 7

On-premise deployment in air-gapped environments

FortiEDR 7.2.3 adds support for on-premise deployment in air-gapped environments. You can download the required deployment files at the Fortinet Support website using an Internet-connected system and transfer the files to the air-gapped (isolated) environment using approved removable media. See the FortiEDR Administration Guide for more information.

New AV Signature policy

To support OT and segmented environments that require controlled update windows, FortiEDR7.2.3 adds the new AV Signature policy (under *Profiles* > *Security* > *Security Content Update*), which defines when and how Collector groups download AV signatures for each type (Active, Extended, Extreme, and URL DB) based on time-based rules and time zones. You can also manually upload and manage AV signatures using the *Content Manager* button at the top-right corner in hoster view, which is particularly useful for air-gapped environments.



Security Content Update

Available Update Versions (supported from collector v6.2.0 or above): Active Signatures: 93.6618.0.0 | Extreme Signatures: 93.5840.0.0 | Extended Signatures: 93.6594.0.0 | URL DB: 5.646.0.0

41 results

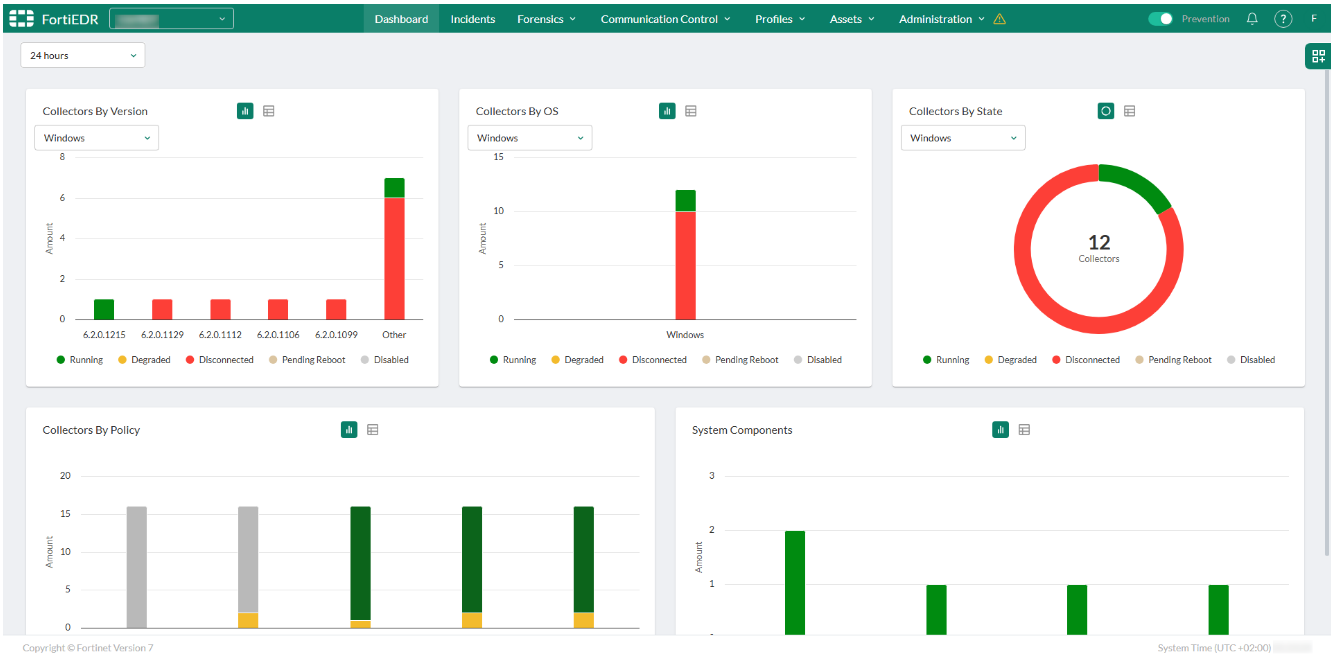
□	Organization	Policy	State	Update Method	Target Version	Content Types	Collector Groups
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	Default Collector Group
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... n1 +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +2
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	Upgrade +3
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +6
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	Group2 +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	High Security Collector... +1
□	[redacted]	Default AV Signature Policy	Enabled	Automatic	Latest	Active, Extended, Extreme, URL DB	Default Collector Group +1

Copyright © Fortinet Version 7

System Time (UTC +02:00) 04:33:55

New color scheme of the Central Manager console

The FortiEDR 7.2.3 Central Manager console use a new green color scheme for consistency with other Fortinet endpoint products:



Upgrade information

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

To upgrade your FortiEDR environment to 7.2.3, 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 7.2.3. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1174797, 1177824	Threat Hunting query that contains "NOT" does not filter correctly.
1230971, 1231450	Parsing failure of Taxii feed.
1243237, 1245594	No audit log for in disabling SAML authentication.
1257703, 1249534, 1258256	Adding a process to Exclusion Policy via Incident View results in blank screen.
1229966, 1230923	Exception creation fails due to an empty value.
1234632, 1234818	Failure in retrieving reports from a disconnected Collector.
1222844, 1224855	list-exceptions Rest API function does not display selected Collector groups.
1224830, 1224852	Users with a Read-Only role cannot export data from the Inventory page.
1217600, 1224858	Hardening related to key injection as a variable.
1229820, 1233765	Issue with dashboard queries of "Top Affected Devices".
1234348, 1239292	Incident Report fails to display the full event process path.
1231073, 1235251	Incident report generation gets stuck at 5%.
1214941, 1215757	count-events REST API function returns inaccurate results when filtering by IP address.
1231674, 1232143	Classification response actions are displayed in the wrong chronological order in Incident View.
1219174, 1220532	"Collectors By Policy" widget export does not match the widget display.
1234440, 1240548, 1237245	Syslog becomes unresponsive due to a status update failure, causing log transmission to stop unexpectedly.
1230144, 1235745	Exception is created on the wrong security event.
1219162, 1231830	Widgets cannot be selected on the Dashboard page.
1233707, 1234310	Adding an incident comment is logged with a default user information.
1232273, 1233766	Sorting by total number does not correctly order the values in Incident View.
1217982, 1222702	Wrong file or process name is displayed while the correct file has been remediated.
1227989, 1250027, 1228723	Applying the “Malicious” classification filter prevents associated raw events from being displayed.

Bug ID	Description
1252095, 1252561	Applying a filter prevents exporting the Collectors report in the Inventory.
1252094, 1226670, 1252560	Incidents sometimes appear as unclickable duplicates when you scroll or hover in the UI.
1251352	Certain events are partially saved during consolidation.
1254115, 1252688, 1250220	Editing an exception incorrectly displays an event as "deleted".
1244654, 1246159, 1244724, 1244129, 1246479	Potential error in consolidation flow.
1243125, 1251355	Multiple entities are marked as erased but are not actually cleaned from the database.
1230520, 1240181	When creating an exception via handling an event, selecting an IP from the destination list incorrectly selects all IPs.
1221298, 1231457	Deleting an organization or changing license capacity does not save the changes or causes the environment to hang.
1236064, 1238202	Raw Data Items cannot be retrieved from Event ID using Rest API.
1240953, 1245595, 1242029	Deleting an event while using a filter results in deletion of multiple events within the same aggregation.
1225502, 1247886, 1246187, 1240786, 1235482, 1231053	Updating the license blocks Collector registrations.
1227194, 1243039, 1227652	Changing an exception’s destination from "Specific" to "All Destinations" incorrectly triggers a “cannot select both” error.
1234354, 1235517, 1245708, 1237735	Performance issue with event processing.
1250351, 1251431	Security Policy Search fails due to an internal error.
1248720, 1249641	Error when creating an exception on a specific event.
1224946, 1242028	SMTP is active only on Hoster.
1243641, 1244635	Issue with exporting unmanaged devices list.
1252134, 1254404	Click "Add Connector" and the dropdown shows most connector options grayed out.
1239170, 1246197	LDAP error when choosing SSL or TLS.
1111981, 1218423	When syslog field values are too long, the first max characters will be displayed.
1223419, 1235747	No audit log when a user modifies their own user advanced settings.
1220303, 1221131	Export-iot-json return java exception instead of a meaningful error message.

Refer to What's new on page 6 for a list of new features, enhancements, and changes. Refer to Known issues on page 13 for a list of known issues.

Known issues

The following issues have been identified in FortiEDR 7.2.3. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

New known issues for 7.2.3

There is no new known issue for 7.2.3.

Existing known issues from earlier versions

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.