Release Notes

FortiEDR 7.2.0

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 26, 2026
FortiEDR 7.2.0 Release Notes
63-720-1165545-20260126

TABLE OF CONTENTS

Change log

Date	Change Description
2025-09-29	Initial release.
2025-10-24	Updated What's new on page 6.
2026-01-05	Updated What's new on page 6.
2026-01-26	Updated What's new on page 6.

FortiEDR 7.2.0 Release Notes

This document provides information about FortiEDR version 7.2.0.

Version history

	Central Manager	Core	Threat Hunting Repository
2025-09-29 (GA)	Build 7.2.0.0170	Build 6.1.0.1270	Build 7.2.0.0057

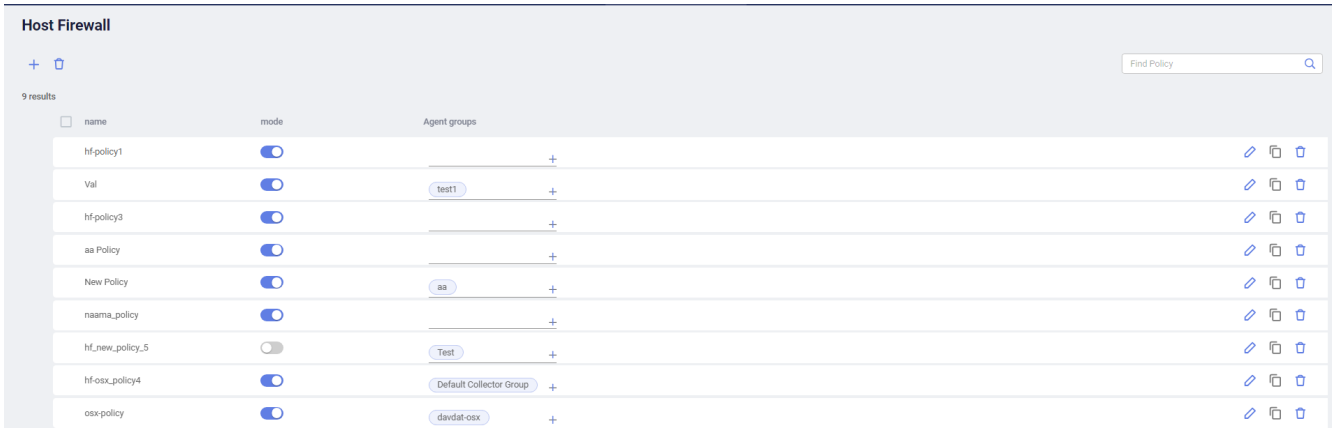
What's new

The FortiEDR 7.2.0 GA build includes the following features, enhancements, and changes:

Host firewall policies on Collector groups

COLLECTOR 6.1 OR LATER

Use the new *Communications Control* > *Host Firewall* page to configure host firewall policies to control incoming and outgoing network traffic to protect endpoints against unwanted connections based on remote addresses, protocols, or applications in use to reflect the organization's network policies. Host firewall policies reduce the attack surface by protecting the host while working outside the enterprise network (public Internet, home, or other networks).

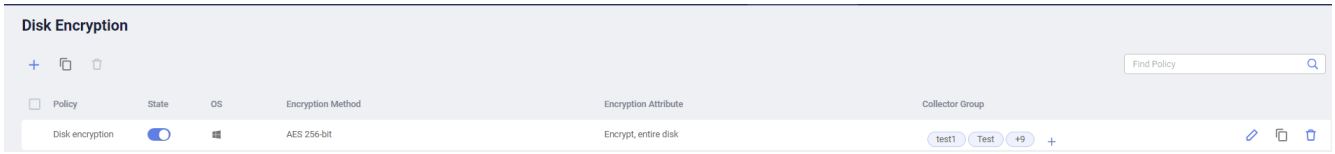


For Windows and macOS endpoints, host firewall status is used for compliance check in the *Device Security* column of the endpoint in *Assets* > *Inventory*.

Host firewall policies work side by side with existing Communication Control policies. In case of contradictions, FortiEDR applies the more restrictive out of the two. For example, if a group is assigned to a host firewall policy that allows any connection to a specific remote address but the Communication Control policy assigned to the group restricts connections to low reputation applications, connections to the remote address will be blocked if the connection goes to low reputation applications.

Disk encryption management for Windows and macOS endpoints COLLECTOR 6.1 OR LATER

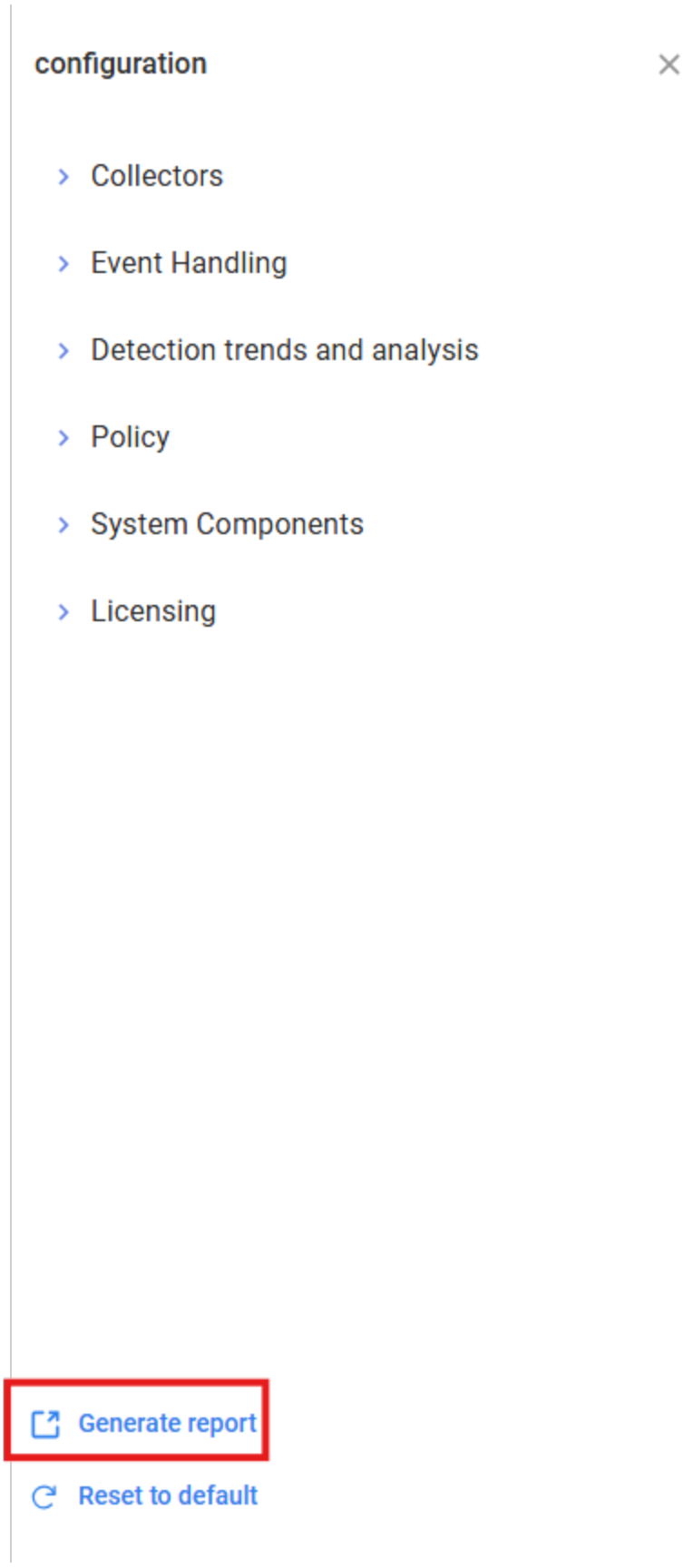
Use the new *Security Settings* > *Disk Encryption* page to configure disk encryption policies to enforce disk encryption on Windows 7 or later (using BitLocker, TPM is required) and macOS (using FileVault) endpoints to ensure consistent security configurations and compliance with regulatory requirements.



For Windows and macOS endpoints, disk encryption status is used for compliance check in the *Device Security* column of the endpoint in *Assets* > *Inventory*.

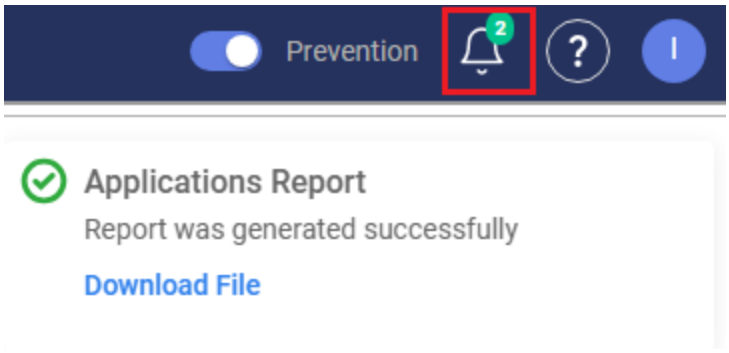
Generating reports

On the dashboard, click the *Configuration* icon () on the top-right of the dashboard and click *Generate report* to download a PDF report with a summary of the security events and system health within the specified time range.


configuration
Collectors
Event Handling
Detection trends and analysis
Policy
System Components
Licensing
Generate report
Reset to default

Usability improvements for exporting Communication Control applications

When you export Communication Control applications (as *Excel* or *JSON*), the progress bar is moved from a popup window to the notification center at the top-right corner so that you can still perform actions on the UI while waiting for the download to complete. You can view the reports that are being generated or have been generated and download them as needed.



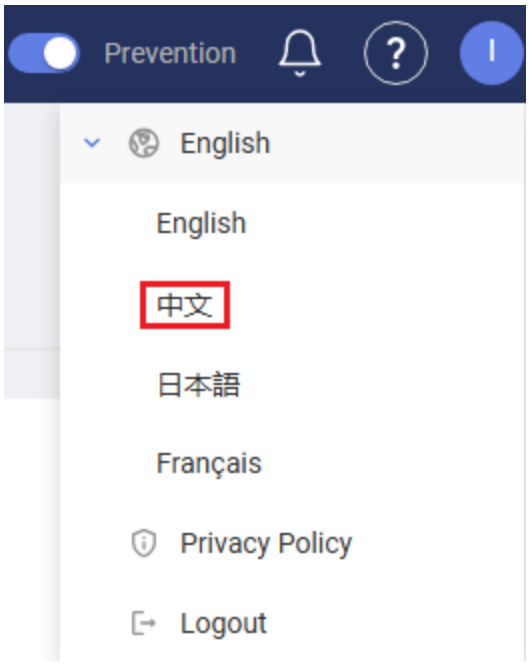
Change to the filtered incidents view

In 7.0 and earlier, the top-level row in the filtered incidents view was purely a logical representational aggregation of all related events.

In 7.2, the top-level row now represents an incident entity with its own state independent from the associated child events. As a result, filters are applied to both the top-level incidents and their child events. An incident may appear on its own if it matches the filter criteria even if none of its child events do.

Localization - Chinese support

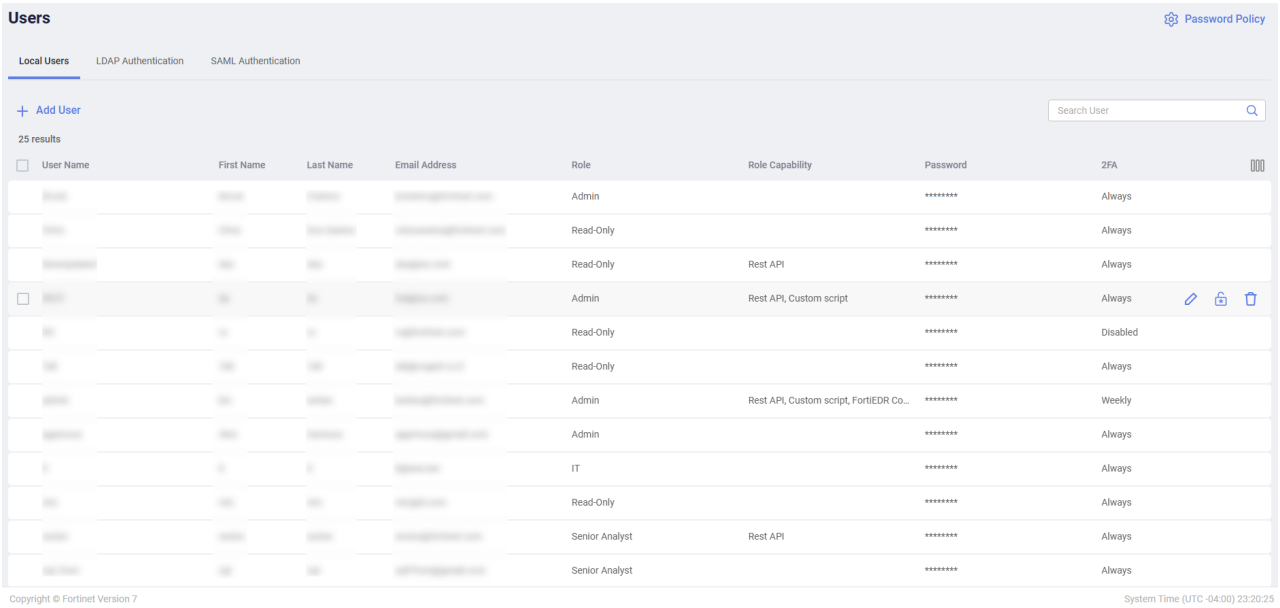
The FortiEDR Central Manager console adds support for Chinese. To switch the UI language to Chinese, click the user icon at the top-right corner and select the language.



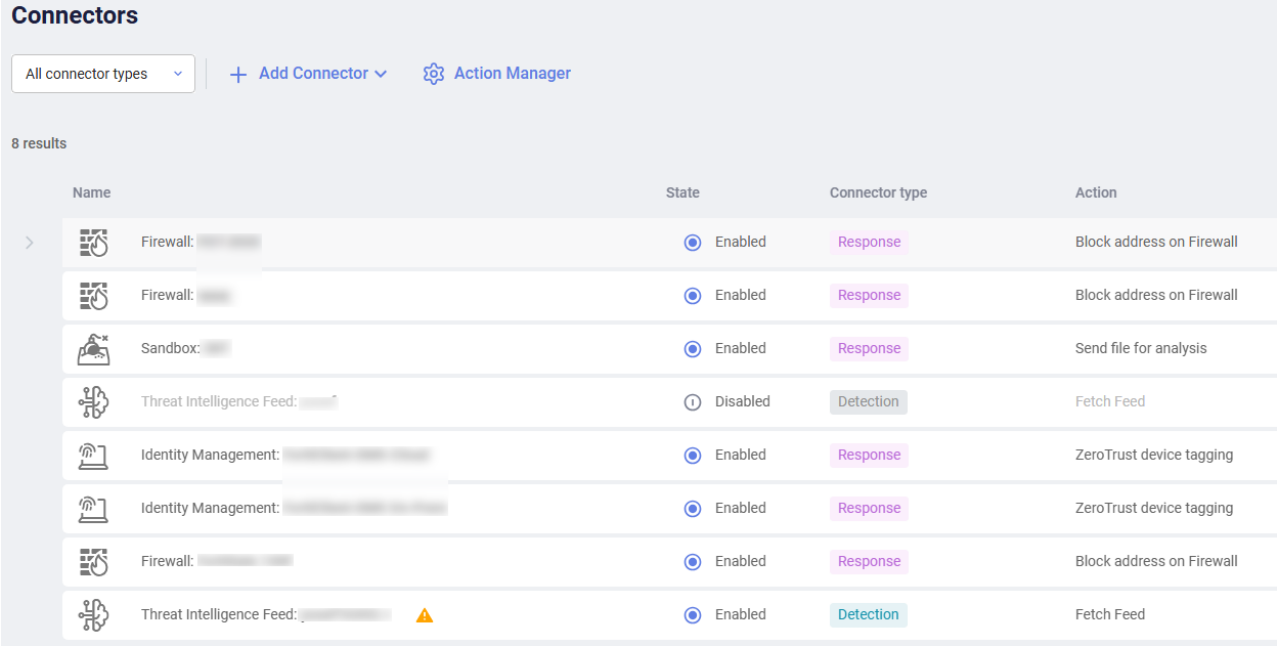
New look and feel for some Central Manager console pages

The following menus have adopted a sleeker and more modern look and feel with a new color scheme:

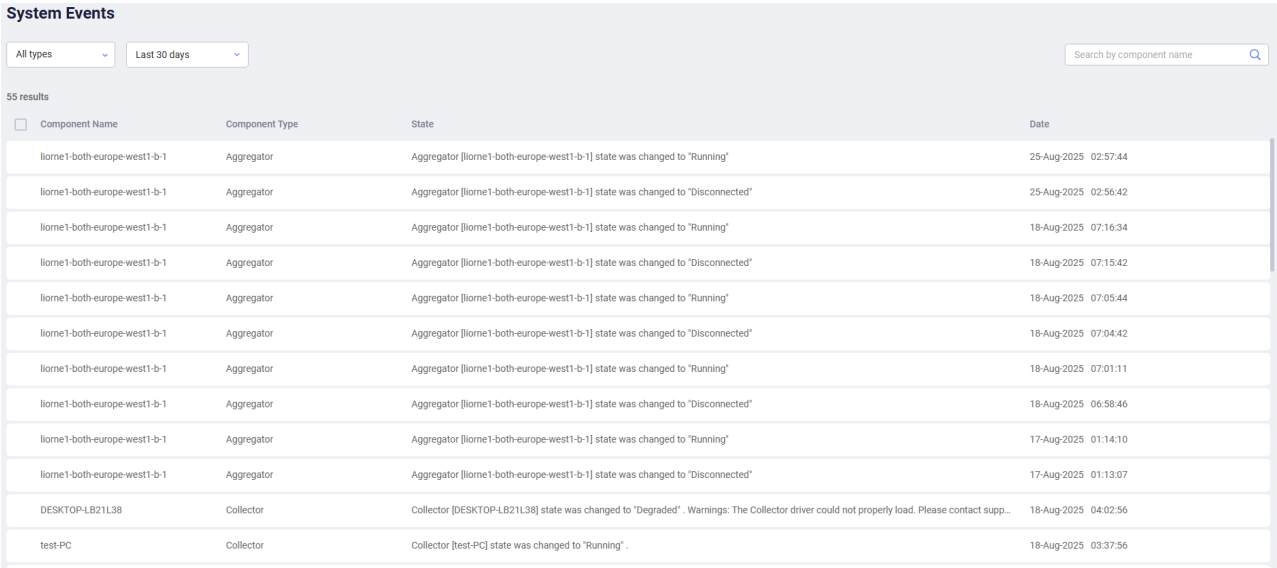
- *Administration > Users*



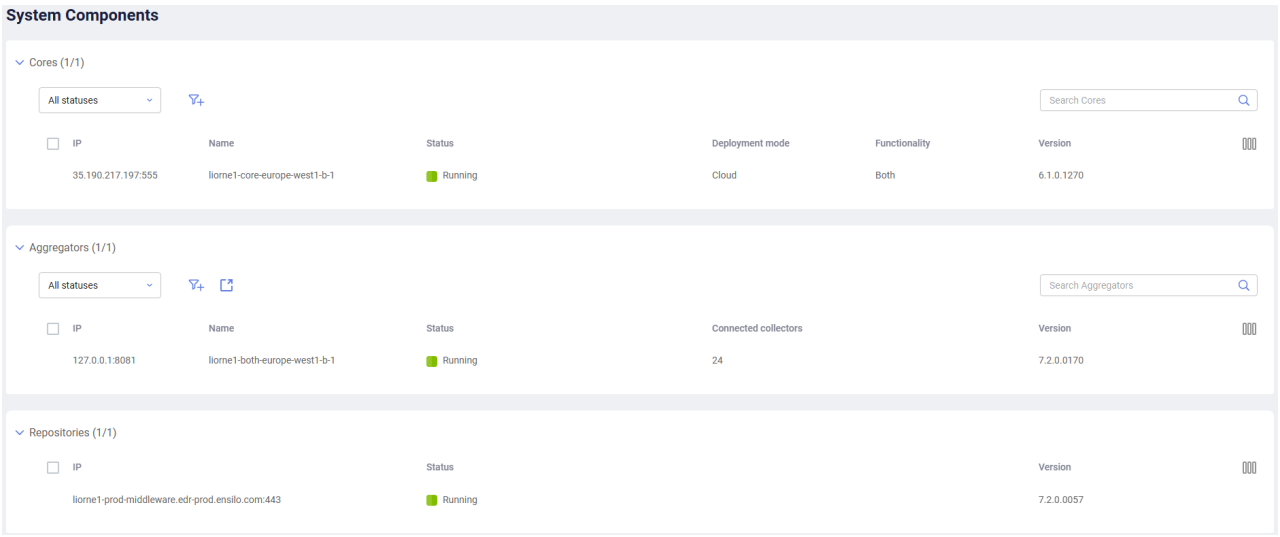
- *Administration > Connectors*



- *Administration > System Events*



- *Administration > Deployment > System Components*



Refer to Resolved issues on page 16 for a list of resolved issues for this build.

Upgrade information

FortiEDR 7.2 Central Manager supports upgrade from 6.2 or 7.0.

To upgrade your FortiEDR environment to 7.2, 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 7.2.0. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1190576	Fix error handling script.
1184211, 1184732, 1186391, 1187299, 1188820, 1191006, 1189146, 1191934, 1184679	Memory issues on a massive response number from FCS due to an event that requires mail sending.
1182542, 1184109	Scan fails when duplicate IoT devices are detected.
1188797, 1191908	Classification is not updated according to the classification received from FCS.
1188319	Connected Collectors do not appear in the group.
1030485, 1035404	Integration with FortiManager does not support Workspace mode.
1140147, 1160702	Rest API log enhancements.
1139228, 1147014	Integration with FortiSOAR fails.
1095132, 1161767	Error when creating an exception using an asterisk in the detected script (.sh file) on Linux.
1155298, 1152734, 1125529, 1131459, 1158397	Configuration integrity validation issue that causes degraded Manager and Core.
1131478, 1139171	Failure in filtering events by SimulationBlock action.
992289, 990535, 1001334, 964808, 815837	Exception covering query issue with uncovered RDI's.
1147352, 1156913	Missing audit log of handling or unhandling an event.
1016548, 1151768	Error when cloning a Threat Hunting profile using an "All Organizations" admin account.
1158490, 1163603	Unable to investigate or handle Threat Hunting incidents in the management console.
1151959, 1158401	FortiEDR Windows Collectors are shown as degraded after upgrade to 7.0.
1119659, 1158402	Moving a Collector to a group results in all Collectors from the selected Collector group being moved.

Bug ID	Description
1174120	Failure in saving exception for a deleted event.
1174766	XDR events are not populated in Incidents view
1177825	Error with saved query event.
1177053, 1177829	Multiple drivers are blocked incorrectly under C:\System32\drivers folder.
1179232, 1180072, 1180211, 1179504	Faiure in loading the IoT Devices page.
1181437, 1181391	Memory issues.
1142267, 1087594	Connecting a Collector to a newly-created organization results in degraded status.
1179295, 1179298, 1153842	Prolonged time in creating an organization.
1161894, 1162753, 1173493, 1180517	Issue with syslog and emails.
1178016, 1179270, 1184208 , 1178983	Collector sorting error on "Last Seen" column.

Refer to What's new on page 6 for a list of new features, enhancements, and changes. Refer to Known issues on page 18 for a list of known issues.

Known issues

The following issues have been identified in FortiEDR 7.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

New known issues for 7.2.0

There is no new known issue for 7.2.0.

Existing known issues from 7.0 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