

Release Notes

FortiEDR 5.2.0



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



April 4, 2024

FortiEDR 5.2.0 Release Notes

63-520-813298-20240404

TABLE OF CONTENTS

Change log	5
FortiEDR 5.2.0 Release Notes	8
Version history	8
What's new	10
Central Manager - Build 3195	11
Central Manager - Build 3192	12
Revoking a compromised registration password	12
More specific Aggregator names	12
Creating Syslog via Rest API	12
Adding exceptions based on child processes	12
Central Manager - Build 3092	13
Changing default threat hunting collection profile	13
SSL connection between Collector and Core	13
Core - Build 5.2.2.2027	14
Central Manager - Build 2527	15
Central Manager - Build 2387	16
Support for FortiAnalyzer Syslog	16
Uploading a client certificate for Syslog servers	16
Configuring session timeout duration in Hoster view	16
Central Manager - Build 2325	17
Central Manager - Build 2162	18
GA build (Central Manager and Core - Build 2040, Threat Hunting Repository - Build 2036)	19
FortiEDR Connect (Remote Shell)	19
Enhanced Application Control Options	19
eXtended Pre-Canned Integrations	19
Threat Hunting Data Retention Visibility	19
Japanese Localization of FortiEDR Console	19
Syslog Additions	19
Supported browsers	20
Resolved issues	21
Central Manager	22
Central Manager - Build 3195	22
Central Manager - Build 3192	23
Central Manager - Build 3092	25
Central Manager - Build 3091	25
Central Manager - Build 3087	26
Central Manager - Build 3086	26
Central Manager - Build 3056	27
Central Manager - Build 3051	27
Central Manager - Build 2825	28
Central Manager - Build 2773	30
Central Manager - Build 2772	30
Central Manager - Build 2708	31

Central Manager - Build 2594	32
Central Manager - Build 2527	33
Central Manager - Build 2387	35
Central Manager - Build 2363	36
Central Manager - Build 2358	37
Central Manager - Build 2325	38
Central Manager - Build 2162	39
Central Manager - Build 2159	39
Central Manager - Build 2157	40
Central Manager - Build 2132	41
Central Manager - Build 2040	43
Core	44
Core - Build 5.2.2.2047	44
Core - Build 5.2.2.2043	44
Core - Build 5.2.2.2042	44
Core - Build 5.2.2.2032	45
Core - Build 5.2.2.2030	45
Core - Build 5.2.2.2027	45
Core - Build 4189	46
Core - Build 2410	46
Core - Build 2407	46
Core - Build 2293	46
Core - Build 2133	46
Core - Build 2132	47
Threat Hunting Repository	48
Threat Hunting Repository - Build 3071	48
Threat Hunting Repository - Build 2767	48
Threat Hunting Repository - Build 2587	48
Threat Hunting Repository - Build 2524	48
Threat Hunting Repository - Build 2450	49
Threat Hunting Repository - Build 2245	49
Threat Hunting Repository - Build 2102	49
Known issues	50

Change log

Date	Change Description
2022-05-31	Initial release of 5.2.0.
2022-06-07	Added ticket 777707 to <i>Known issues</i> .
2022-06-28	Added Threat Hunting Repository build 2102 to <i>Resolved issues</i> .
2022-07-18	Added the following bugs to the <i>Resolved issues</i> list for Central Manager build 2040: <ul style="list-style-type: none">• 809270• 774106
2022-07-21	Added the following bugs to the <i>Resolved issues</i> list for Central Manager build 2040: <ul style="list-style-type: none">• 808059• 811066
2022-08-04	Added the following builds to <i>Resolved issues</i> : <ul style="list-style-type: none">• Core build 2132• Central Manager build 2132
2022-08-18	Added the following builds to <i>Resolved issues</i> : <ul style="list-style-type: none">• Threat Hunting Repository build 2245• Core build 2133
2022-08-30	Added a note in What's new on page 10 .
2022-09-08	Added ticket 837675 to <i>Known issues</i> .
2022-09-19	Added Central Manager build 2157 to <i>Resolved issues</i> .
2022-09-22	<ul style="list-style-type: none">• Added Central Manager build 2159 to <i>Resolved issues</i>.• Added ticket 840449 to <i>Resolved issues</i>.
2022-10-12	<ul style="list-style-type: none">• Added Central Manager build 2162 to <i>Resolved issues</i> and <i>What's new</i>• Added Core build 2293 to <i>Resolved issues</i>
2022-10-25	<ul style="list-style-type: none">• Added Core build 2407 to <i>Resolved issues</i>.• Added ticket 854124 to <i>Known issues</i>.
2022-10-26	Added Core build 2410 to <i>Resolved issues</i> .
2022-11-17	Added the following builds: <ul style="list-style-type: none">• Threat Hunting Repository build 2257• Central Manager build 2325 (also added to <i>What's new</i> and <i>Resolved issues</i>)
2022-11-22	Added ticket 772449 to <i>Known issues</i> .
2023-01-04	Added Central Manager builds 2358 and 2363 to <i>Resolved issues</i> .
2023-01-09	Added ticket 734616 to <i>Known issues</i> .

Date	Change Description												
2023-01-16	Added Threat Hunting Repository build 2450 to <i>Resolved issues</i> .												
2023-01-24	Added ticket 842110 to <i>Known issues</i> .												
2023-01-30	<ul style="list-style-type: none"> Added Central Manager build 2387 to <i>What's new</i> and <i>Resolved issues</i>. Deleted the following issue from the <i>Resolved issues</i> list of Central Manager build 2325: <table border="1"> <thead> <tr> <th>Bug ID</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>847528</td> <td>An issue with parent process resulting in uncovered RDI.</td> </tr> <tr> <td>848524</td> <td></td> </tr> <tr> <td>843608</td> <td></td> </tr> <tr> <td>848358</td> <td></td> </tr> <tr> <td>854262</td> <td></td> </tr> </tbody> </table>	Bug ID	Description	847528	An issue with parent process resulting in uncovered RDI.	848524		843608		848358		854262	
Bug ID	Description												
847528	An issue with parent process resulting in uncovered RDI.												
848524													
843608													
848358													
854262													
2023-02-23	Added Threat Hunting Repository build 2524 to <i>Resolved issues</i> .												
2023-02-27	Added Central Manager build 2527 to <i>What's new</i> and <i>Resolved issues</i> .												
2023-03-09	Added ticket 889422 to <i>Known issues</i> .												
2023-03-29	Added Central Manager build 2594 and Threat Hunting Repository build 2587 to <i>Resolved issues</i> .												
2023-04-24	Added Central Manager build 2708 to <i>Resolved issues</i> .												
2023-05-03	Updated What's new on page 10 .												
2023-05-16	Added the following builds to <i>Resolved issues</i> : <ul style="list-style-type: none"> Central Manager build 2772 Threat Hunting Repository build 2767 												
2023-05-24	Added ticket 907362 to <i>Known issues</i> .												
2023-05-25	Updated the <i>Configuring session timeout duration in Hoster view</i> section in What's new on page 10 .												
2023-05-26	Added Central Manager build 2773 to <i>Resolved issues</i> .												
2023-05-29	Updated the <i>Configuring session timeout duration in Hoster view</i> section in What's new on page 10 .												
2023-06-15	Added the <i>Support for FortiAnalyzer Syslog - Central Manager Build 2387</i> section in What's new on page 10 and deleted the relevant bug IDs in Resolved issues on page 21 .												
2023-06-20	Added Central Manager build 2825 to <i>Resolved issues</i> .												
2023-07-28	Added a known issue to Known issues on page 50 .												
2023-08-15	Added Central Manager build 3051 to Resolved issues on page 21 and Known issues on page 50 .												
2023-08-17	Added Central Manager build 3056 to Resolved issues on page 21 .												

Date	Change Description
2023-09-12	Added Core build 4189 to Resolved issues on page 21 .
2023-09-19	Added the following builds to Resolved issues on page 21 : <ul style="list-style-type: none">• Central Manager build 3086• Threat Hunting Repository build 3071
2023-09-28	Added Central Manager build 3087 to Resolved issues on page 21 .
2023-10-05	Added Core build 5.2.2.2027 to What's new on page 10 and Resolved issues on page 21 .
2023-10-26	Added the following builds to Resolved issues on page 21 : <ul style="list-style-type: none">• Central Manager build 3091 and 3092• Core build 5.2.2.2030
2023-11-02	Added Core build 5.2.2.2032 to Resolved issues on page 21 .
2023-11-09	Deleted ticket 739199 from Resolved issues on page 21 .
2023-11-14	Added Core build 5.2.2.2042 to Resolved issues on page 21 .
2023-11-20	Added Supported browsers on page 20 .
2023-11-27	Added the <i>SSL connection between Collector and Core</i> section to What's new on page 10 .
2023-12-04	Updated What's new on page 10 .
2023-12-11	Added Central Manager build 3192 to What's new on page 10 and Resolved issues on page 21 .
2023-12-21	<ul style="list-style-type: none">• Added the following builds to Resolved issues on page 21:<ul style="list-style-type: none">• Central Manager build 3195• Core build 5.2.2.2043• Updated What's new on page 10.
2023-12-27	Updated What's new on page 10 and Resolved issues on page 21 .
2023-12-28	Updated What's new on page 10 .
2023-12-29	<ul style="list-style-type: none">• Re-organized content in What's new on page 10 and Resolved issues on page 21.• Added links in FortiEDR 5.2.0 Release Notes on page 8.
2024-01-02	<ul style="list-style-type: none">• Added a resolved issue for Central Manager build 3192 in Central Manager on page 22.• Added a cross-reference link in What's new on page 10.
2024-01-08	Added tickets 982543 and 973252 to Known issues on page 50 .
2024-02-06	Added tickets 939481 and 973077 to Known issues on page 50 .
2024-02-13	Updated Central Manager - Build 3192 on page 12 .
2024-04-04	Added Core build 5.2.2.2047 to Resolved issues on page 21 .

FortiEDR 5.2.0 Release Notes

This document provides information about FortiEDR version 5.2.0.

Version history

	Central Manager	Core	Threat Hunting Repository
2024-04-04		Build 5.2.2.2047	
2023-12-21	Build 3195	Build 5.2.2.2043	
2023-12-11	Build 3192		
2023-11-14		Build 5.2.2.2042	
2023-10-30		Build 5.2.2.2032	
2023-10-25	Build 3092	Build 5.2.2.2030	
2023-10-08	Build 3091		
2023-10-04		Build 5.2.2.2027	
2023-09-24	Build 3087		
2023-09-19	Build 3086		Build 3071
2023-09-12		Build 4189	
2023-08-17	Build 3056		
2023-08-15	Build 3051		
2023-06-20	Build 2825		
2023-05-26	Build 2773		
2023-05-16	Build 2772		Build 2767
2023-04-24	Build 2708		
2023-03-29	Build 2594		Build 2587
2023-02-27	Build 2527		
2023-02-23			Build 2524
2023-01-30	Build 2387		

	Central Manager	Core	Threat Hunting Repository
2023-01-16			Build 2450
2023-01-03	Build 2363		
2022-12-14	Build 2358		
2022-11-17	Build 2325		Build 2257
2022-10-26		Build 2410	
2022-10-25		Build 2407	
2022-10-12	Build 2162	Build 2293	
2022-09-22	Build 2159		
2022-09-19	Build 2157		
2022-08-18		Build 2133	Build 2245
2022-08-04	Build 2132	Build 2132	
2022-06-28			Build 2102
2022-05-31 (GA)	Build 2040	Build 2040	Build 2036

What's new

This section identifies new features and enhancements available with different builds of FortiEDR 5.2.0.



If you upgrade from FortiEDR 5.0.0 to 5.2.0, see also [FortiEDR 5.1.0 what's new](#) for additional new features introduced in FortiEDR 5.1.0.

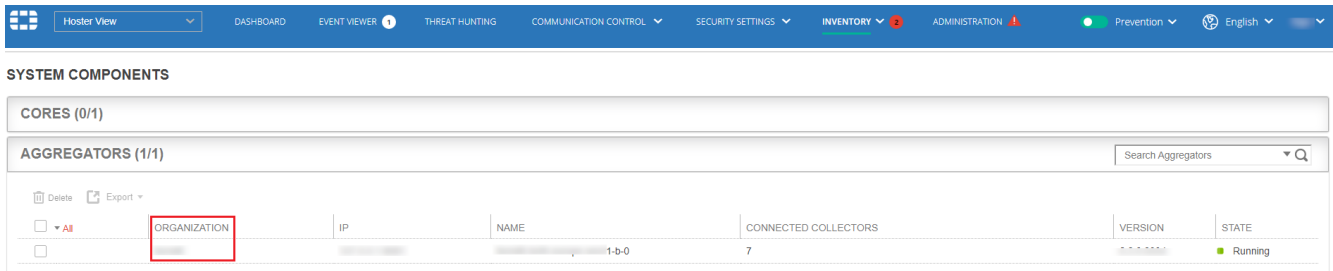
- [Central Manager - Build 3195 on page 11](#)
- [Central Manager - Build 3192 on page 12](#)
- [Central Manager - Build 3092 on page 13](#)
- [Core - Build 5.2.2.2027 on page 14](#)
- [Central Manager - Build 2527 on page 15](#)
- [Central Manager - Build 2387 on page 16](#)
- [Central Manager - Build 2325 on page 17](#)
- [Central Manager - Build 2162 on page 18](#)
- [GA build \(Central Manager and Core - Build 2040, Threat Hunting Repository - Build 2036\) on page 19](#)

Refer to [Resolved issues on page 21](#) for a list of resolved issues for each build.

Central Manager - Build 3195

This build adds support for organization-specific Aggregators in [multi-tenancy](#) setups. You can now install an on-premise Aggregator that serves only Collectors of a specific organization rather than all organizations. To do so, you must specify the organization during the [Aggregator installation](#) process. Organization-specific Aggregators are visible only to Admin users of that specific organization. For Admin users with permission to all organizations, all Aggregators will be visible.

To verify the organization setting of an Aggregator, select the organization or Hoster view (if applicable) and check the Aggregator information in the *System Component* section of the [Dashboard](#) or [Inventory](#) page. When an organization-specific Aggregator exists and you have permission to that organization, the *Aggregator* section of the *Inventory* page includes the new *Organization* column listing the owning organization of the Aggregator.



Refer to [Central Manager - Build 3195 on page 22](#) for a list of resolved issues for this build.

Central Manager - Build 3192

This build includes the following features and changes:

Revoking a compromised registration password

Starting from this build, you can revoke a compromised registration password for an organization using the new *Advanced Password Management* option under *Administration > Tools > Component Authentication*.

More specific Aggregator names

In the *Inventory > System Components* page, the *Name* column of the *Aggregator* table now displays the real machine name for each Aggregator instead of displaying *Fortinet* for all Aggregators, which is helpful in case of multiple Aggregators in the environment.

IP	NAME	CONNECTED COLLECTORS	VERSION	STATE
[Redacted]	[Redacted]	7	[Redacted]	Running

Creating Syslog via Rest API

You can now define a *Syslog* destination via Rest API, including the upload of a certificate using Rest API during the process. By default, all available syslog fields and all notifications options, including security, system, and audit events, are enabled. For details, refer to the [FortiEDR RESTful API Guide](#). You must log in to the Fortinet Developer Network to access the guide.

Adding exceptions based on child processes

FortiEDR adds support for creating exceptions based on child processes on the top of existing support for creating exceptions based on key process and its parent processes. For more details, see [Defining a security event as an exception](#) in the Administration Guide.





This feature requires Core and Collector 5.2.2 builds.

Refer to [Central Manager - Build 3192 on page 23](#) for a list of resolved issues for this build.

Central Manager - Build 3092

This build includes the following features:

Changing default threat hunting collection profile

Starting from this build, you can change the default threat hunting collection profile under *SECURITY SETTINGS > Threat Hunting Setting > Collection Profiles*. The default profile is *Inventory Profile*, which is indicated by the *Default Collection Profile* () icon. To change the default profile, hover over to the top-right corner of the target profile card and click the *Set profile as default profile* () icon.

SSL connection between Collector and Core

Starting from these builds, FortiEDR supports SSL encrypted communication between the Collector and Core for enhanced security. To enable SSL connection, please contact [Fortinet Support](#).



This feature requires Core Build 5.2.2.2042 and Collector build 5.2.2.95.

Refer to [Central Manager - Build 3092 on page 25](#) for a list of resolved issues for this build.

Core - Build 5.2.2.2027

Starting from this build, you can create exceptions for specific command execution. To enable this functionality, please contact [Fortinet Support](#).

Refer to [Core - Build 5.2.2.2027 on page 45](#) for a list of resolved issues for this build.

Central Manager - Build 2527

Starting from this build, Rest API authentication tokens are valid only for the duration of the TCP session, which expires after 60 seconds of inactivity. To establish a new connection, re-authenticate and generate a new token. The maximum lifespan of a token is 4 hours, regardless of the TCP session state.

Refer to [Central Manager - Build 2527 on page 33](#) for a list of resolved issues for this build.

Central Manager - Build 2387

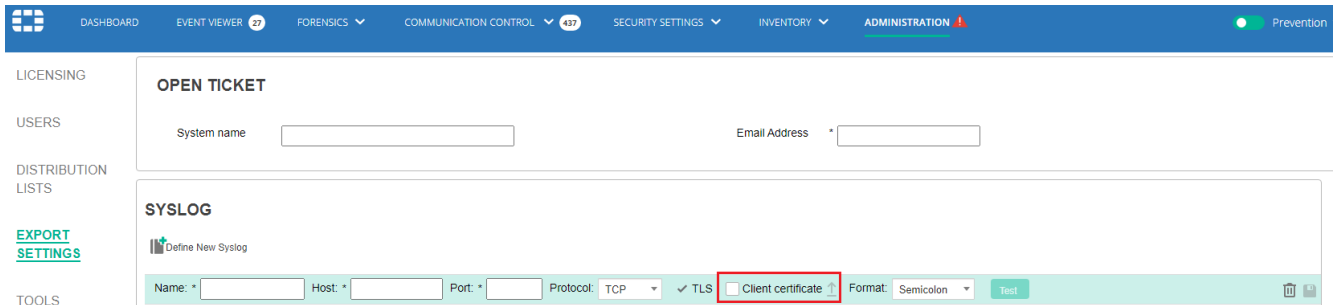
This build includes the following features:

Support for FortiAnalyzer Syslog

FortiEDR Central Manager build 2387 adds support for FortiAnalyzer syslog. Under [Administration > Export Settings > SYSLOG](#), you can define a FortiAnalyzer Syslog server and FortiEDR will then send events to that server via Syslog.

Uploading a client certificate for Syslog servers

When defining a [Syslog](#) server with *TLS* enabled, if the Syslog server requires a client-side certificate, you can now upload the certificate which includes a certificate file, a private key file, and a private key password. For example, if your FortiAnalyzer server requires a client-side certificate, contact [Fortinet Support](#) to obtain the FortiAnalyzer certificate files and upload them using the *Client certificate* option.



Configuring session timeout duration in Hoster view

Under [Administration > Tools](#), you can now configure the idle session timeout period in the new *SESSION TIME OUT* section in [Hoster view](#), which is the duration (in minutes) before a session expires and users are prompted for credentials. The session timeout setting applies to all FortiEDR Console tabs except *Dashboard*. The default is 15 minutes. The acceptable value range is 1 - 1440.

Refer to [Central Manager - Build 2387 on page 35](#) for a list of resolved issues for this build.

Central Manager - Build 2325

Starting from this build, you can deploy the FortiEDR on-premise. See the [FortiEDR 5.2.0 Admin Guide](#) for system requirements and deployment instructions.

Refer to [Central Manager - Build 2325 on page 38](#) for a list of resolved issues for this build.

Central Manager - Build 2162

Starting from this build, you can disable IoT scans. By default, IoT scans are enabled. You can disable IoT scans in the following ways:

- For on-premise users, change the value of the `iot` parameter in `application.properties` to `disabled` (`iot.disabled`).
- For cloud users, please contact [Fortinet Support](#).

Refer to [Central Manager - Build 2162 on page 39](#) for a list of resolved issues for this build.

GA build (Central Manager and Core - Build 2040, Threat Hunting Repository - Build 2036)

The FortiEDR 5.2.0 GA build includes the following features:

FortiEDR Connect (Remote Shell)

This new capability enables direct access to FortiEDR-protected devices through a remote shell connection. It enables authorized users to quickly investigate, collect data and remediate devices from the Central Manager Console. The feature includes a variety of built-in commands, or you can choose to upload and run custom scripts on the device. This capability requires the use of a v5.2 Windows Collector.

Enhanced Application Control Options

It is now possible to block applications in order to reduce the attack surface based on a richer set of application attributes, including application name, path and certificate. This capability requires the use of a v5.2 Windows Collector.

eXtended Pre-Canned Integrations

The new FortiEDR version expands built-in integration with 3rd-party security network systems. These out-of-the-box connectors make it easy to configure FortiEDR playbook to automatically trigger incident response actions in external systems as the result of a security event detected by FortiEDR.

Threat Hunting Data Retention Visibility

The estimated data retention period is now displayed on the Central Manager Console, which makes it easier to make decisions about managing data collection. It also exposes the need to add additional threat hunting repository storage add-ons when the retention period becomes short.

Japanese Localization of FortiEDR Console

A fully localized version of the FortiEDR Central Manager Console is now available in Japanese. This localized console can help Japanese organizations manage their endpoint protection more efficiently.

Syslog Additions

Syslog event messages have been enriched with recommended remediation details, MITRE techniques, and further events data.

Refer to [Central Manager - Build 2040 on page 43](#) for a list of resolved issues for this build.

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 topics list resolved issues for different builds for each FortiEDR components. For inquires about a particular bug, please contact [Customer Service & Support](#).

- [Central Manager on page 22](#)
- [Core on page 44](#)
- [Threat Hunting Repository on page 48](#)

Central Manager

The following issues have been fixed in FortiEDR 5.2.0 Central Manager. For inquiries about a particular bug, please contact [Customer Service & Support](#).

- [Central Manager - Build 3195 on page 22 \(new features\)](#)
- [Central Manager - Build 3192 on page 23 \(new features\)](#)
- [Central Manager - Build 3092 on page 25 \(new features\)](#)
- [Central Manager - Build 3091 on page 25](#)
- [Central Manager - Build 3087 on page 26](#)
- [Central Manager - Build 3086 on page 26](#)
- [Central Manager - Build 3056 on page 27](#)
- [Central Manager - Build 3051 on page 27](#)
- [Central Manager - Build 2825 on page 28](#)
- [Central Manager - Build 2773 on page 30](#)
- [Central Manager - Build 2772 on page 30](#)
- [Central Manager - Build 2708 on page 31](#)
- [Central Manager - Build 2594 on page 32](#)
- [Central Manager - Build 2527 on page 33 \(new features\)](#)
- [Central Manager - Build 2387 on page 35 \(new features\)](#)
- [Central Manager - Build 2363 on page 36](#)
- [Central Manager - Build 2358 on page 37](#)
- [Central Manager - Build 2325 on page 38 \(new features\)](#)
- [Central Manager - Build 2162 on page 39 \(new features\)](#)
- [Central Manager - Build 2159 on page 39](#)
- [Central Manager - Build 2157 on page 40](#)
- [Central Manager - Build 2132 on page 41](#)
- [Central Manager - Build 2040 on page 43 \(new features\)](#)

Central Manager - Build 3195

Bug ID	Description
982035	5.0.3 Collectors become degraded when connected to environments running Central Manager build 3192.

Refer to [Central Manager - Build 3195](#) for a list of new features and changes for this build.

Central Manager - Build 3192

Bug ID	Description
923288 932101	Wrong "LAST LOGGED" information is displayed for Collectors.
970587 972801 965069	Personal data deletion issue.
970474 968529 958235	Too much disk usage.
964773 957887	Optimize event association in case of identical device names.
963945	Issues with tooltip text in Advanced section of Process Exclusions.
957884 969493	Exception issue related to moving Collectors between groups.
967425 968998	Issue with running ad hoc AV scan.
961123 967531	Issue with exporting communication control report to Excel.
904025 904727	Issue with exporting an event.
929039 930689	Issue with Exclusions Manager related to a path prefix.
929021 930223 883555	Login failure.
912640 926346	Issue with Event Viewer bubble event count.
924830 926351	Failure in exporting an organization due to folder cleanup issues.
924830 937458 920919	"Last seen" time display issue for degraded Collectors.
935936 934162	A rare login issue.

Bug ID	Description
961784 934991	Failure in getting advanced details in Event Viewer.
932987 934008	A handled event is not marked as archived.
932207 970381 933515	Issue with event count on Dashboard.
931570	Improvements to EDR2 request handling.
928984 931136	Empty uncovered RDI list.
949854 948100 956859	The Event Viewer is slow.
949004 953122	Upgrade failure.
951421	Java library version update.
946869 950777	Issue with exceptions raw IDs.
912578 925472	Process path tooltip display issue when a wild card is used.
938902 922428	Failure in deleting an organization.
937104 960941 962956 961958	Missing logs in syslog.
916258 961435	Cleanup of invalid RDIs.
967203 965727 961437	Issue related to command line exceptions.
963337 958186	Central Manager upgrade issue related to NGINX.
958381 940003	A rare upgrade issue.

Bug ID	Description
940366	Cloud Core configuration issue.
904864 918535	Threat Hunting Repository streamer performance improvements.
972505 943434	Log zipping fails if the log file is in use.
881686	Aggregator name display issue.
928716 927236	Issue with uploading Central Manager certificate.
953119	When proxy is used, Nginx configuration should be modified.
886278 971015	Failure in deleting a rule for Communication control applications.
948509 936863	LDAP authentication failure related to special characters.
954955 949984	Cannot save queries with a length exceeding a certain number of characters.

Refer to [Central Manager - Build 3192](#) for a list of new features and changes for this build.

Central Manager - Build 3092

Bug ID	Description
958607	Corrupted application messages create large local kahaDB.
960606	Console slowness and pages do not load properly.
961006	Align command line field lengths to 512 characters.
960198	Application learning fails if the application JSON includes corrupted characters.

Refer to [Central Manager - Build 3092](#) for a list of new features and changes for this build.

Central Manager - Build 3091

Bug ID	Description
958186 958381	Upgrade failure.
932005	Search by partial string does not work.

Central Manager - Build 3087

Bug ID	Description
943886	New collector status indicating Windows OS version identification issue.

Central Manager - Build 3086

Bug ID	Description
912055 937923	Events view is slow.
799467 819949	Improvements to command line exceptions.
941462 942009	Server start issue related to LDAP.
904025 904727	Failure in exporting a security event to JSON.
928566 931567	Manual decisions do not appear in the exported Excel report for applications.
912159 913479	Improvements to maximum applications decisions matrix.
940350 943022	Addition of AV signature proxy.
926780	Support child process in exception.
947675	Improvements to host header check.
944821	Command line exception modification fix.
943886	Report offsets in Central Manager UI.
948107	Socket timeout on search.
948105	Issue with adding exception for event.
951296	Enable built-in hidden threat hunting exclusions via content.
948101	Failure in sending security events.

Central Manager - Build 3056

Bug ID	Description
942628	System slowness caused by query.
942600	
943021	
941462	Upgrade failure due to LDAP gateway configuration.
942009	
912055	Event text search is slow.
937923	

Central Manager - Build 3051

Bug ID	Description
842929	Incorrect values for the <i>Most Targeted</i> widget.
896286	
888553	
840100	Enhanced security fixes.
839820	
889118	
859620	
858211	A minor text fix on the two-factor authentication scan QR code login page.
858976	
929789	Issue with Rest API Threat Hunting search call.
931145	
929021	Login failure after password change.
930223	
921592	Improved event handling time to prevent FCS issues.
927691	
921771	Delays in marking an event as handled.
925459	
914508	Improved performance of the Event Details page.
924976	
913631	Remote Shell connection issue for on-premise environments.
924148	

Bug ID	Description
921852 922826	Default interval for code requirement is overridden inconsistently during two-factor authentication login.
912093 921994	No validation for file names and file paths.
919368 916180 921995	The Collector flips between Running and Disconnected modes.
914681 918951	Improved dashboard performance.
901127 915697	Translation issue in exported logs.
877188 915700	Search results show only top level Events with no RDIs.
886258 874806 914795	Discrepancy in the event classification.
910653 934007	Degraded Collector due to a configuration issue.
929369 929741	New collectors registration rate is slow.
930035 932915 936869 936029 931146	Cannot edit path in exception due to path length.

Central Manager - Build 2825

Bug ID	Description
907548 913477	A partially covered exception is shown as fully covered.
905373 913007	Issue with saving personal data handling report.
901938 908738	Saved query creation by Hoster user via REST API can fail when mapping certain tags.
912185	Small UI typo.

Bug ID	Description
913005	
910179 911014	Deleting a communication control policy results in a console freeze.
907606 909269	Add tooltip value to all connectors Test operation for localized languages.
882668 916147	Exception covering query inaccurate calculation if process is missing.
916460 916890	Redundant characters in exported system events file.
911601 916429	Archiving or unarchiving a big number of events might result in error.
903734 899802 915346	A malfunction in Central Manager related to connection failure.
900853 911012	Failure to create an exception for a specific event.
903945 907236	Empty user selection in Exception.
896452 915339	Issue with "In Use License" display.
900453 909319	Prevent Exceptions creation for XDR events RDIs in Forensics.
895245 907235	Translation issue affecting DB migrations.
748705 919889 761444	Issue related to validation of registration password.
892337 909267	Minor UI issue in "Organizations" tab related to the "In Use" column.
918876 919334	Improve performance of Central Manager UI.
916975 918532	Upgrade issue.
914790 913485 915377	Performance enhancements.

Bug ID	Description
912469	
917367	
917363	
884746	
912468	
915274	

Central Manager - Build 2773

Bug ID	Description
915274	Performance enhancements.
912470	

Central Manager - Build 2772

Bug ID	Description
899707	Missing email notifications.
904312	
879357	Console failure.
905781	
893244	High CPU in Aggregator due to kernel modules requests.
863213	
890342	
902620	Import fails in migration in a specific case related to application control tags in source organization.
904726	
903984	Registration of Collectors with same MAC address and serial number (different host name) lead to rollback.
905371	
904731	
900671	Upgraded Collectors flips between degraded/disconnected status.
901836	
860955	OS reports show wrong Windows versions in some cases.
906265	
874436	Change "Service KEYLOGGING" to "Keylogging" in Event Graph.
870839	
891937	A case of console failure.
895257	

Bug ID	Description
842929	Incorrect values in the "Most Targeted" widget.
896286	
888553	
889459	Editing communication control policy does not display the whitelisted vendors.
905782	
885865	Java 17 support.
905250	Pendo support.
886739	Minor UI fix in Hoster view.
909320	Enhance management of concurrent registrations.
893040	Support maximum exceptions limit per organization.
909661	Failure in deleting an account.
909662	
909660	AV scan failure.

Central Manager - Build 2708

Bug ID	Description
879182	Issue with Executive summary report repository count.
891184	
885914	"Invalid Date" message under <i>Event Viewer >> Advanced Data</i> .
846349	
889944	
884992	Failure in syslog notification.
886943	
897967	
884216	
883908	Failure in archiving all events.
894388	
887397	Application Control logs are not sent externally via syslog.
890338	
867670	An issue with saving exception with Linux Collector.
890635	
894390	
890853	High RAM utilization.
895263	

Bug ID	Description
893793 889414	A case of Manager malfunction.
893244 904730	Memory allocation failure due to configuration.
887097 888961	Clean expired REST requests.
900732 901984 905467 905778	Events are missing alerts.
891826 903783	Ad-hoc scan does not report any findings.
903984 904734	The Central Management console is slow.
905371 904731	Registration issue of Collectors with the same mac and serial number.
894387	Failure to retrieve a file from the Treat Hunting right panel.
862253	Support stronger ciphers used for FortiEDR servers communication.
895261	Set VDI exclusions to improve management of DB connections.
906256	Cannot add or upload applications under <i>Security Settings >> Application Control Manager</i> .

Central Manager - Build 2594

Bug ID	Description
875593 876337	Address issue with Rest API login hardening.
852990 879601	Error when moving collectors between tenants.
879420 879606	Application reports failure in migrated collector.
887397 890338	Syslog logs for Application Control Security events are not being sent.
881056 889946	Simultaneous assignment of a new collector version for two accounts causes an error.
861482	Java libraries update.

Bug ID	Description
865823	
867906	
894944	A case of high CPU load.
887212	
875455	Communications Control issue with creating a specific rule.
827997	Add the capability to disable the "auto collectors update" checkbox.
864981	A Collector with invalid GUID fails to register.
884210	Wrong title of warning message when renaming Exclusion list.
885864	IPv6 issue.
881197	High CPU in Central Manager.
884215	High CPU issue with whitelisting.
817181	Audit for Extra Config actions.

Central Manager - Build 2527

Bug ID	Description
852046	Enrich error in the log with request parameters in the events search.
874276	
866812	A case of failure to load an event.
874708	
863631	Memory optimization when loading event aggregations .
867904	
857321	Syslog language translation fix.
864556	
865050	A case of operation failure when using "Select All" on multiple Collectors.
874275	
861193	Cases where some events data fails to be loaded.
872850	
870975	
871504	Japanese localization translation fixes.
877503	
866397	Discrepancy in licenses count.
850468	
873444	

Bug ID	Description
874002 875452	An edge case display of application version of deleted Collectors.
870780 876334	Possible lock of multiple registration requests causes slowness of console.
860955 880126	Collector OS version tooltip display fix.
868032 868583 877937	A case of agents running in autonomous mode due to a configuration issue.
840247 870834	A case where Communication Control data fails to display.
875608 876345	Address issue with Rest API token expiry.
855481 864553	Deletion of a group with agents might lead to degraded state.
879210 881592	Fix display of file type on Threat Hunting profile.
879816 883415	A case of a gap between Filtered and Exported Event data in Excel.
875593 876337	Address issue with Rest API login hardening.
879247 880027 881119	A case of failed SAML authentication.
871483 878725	Some characters in repository assignment description are not translated.
771934 877507	Authentication QR code issue.
875191 881589	Communication control resource management.
875191 878528 881876 841444 845306 868579	Console slowness.

Refer to [Central Manager - Build 2527](#) for a list of new features and changes for this build.

Central Manager - Build 2387

Bug ID	Description
860220 843211 870257	A case of Collector registration identification issue.
863829 869222	Audit export failure for specific date intervals.
866751 870647	Japanese language - An English message is displayed in User Details Advanced panel.
867665 869516 867670	RHEL Collectors displayed under New OS Family in Inventory.
865490 870634	A case of REST API GET response discrepancy.
847535 870032	The title of the browser tab does not display "Fortinet" on macOS.
867799 872302	A case of Geo Location display discrepancy.
871437 877069 872663	A case of Threat Hunting degradation.
865696 872737 868257	Syslog messages stopped after a network failure.
785198	Inventory - Clear the master checkbox selection upon new searches.
852093 860367	A case of empty User Name Entries within Audit Logs for Communication Control.
861881 864983 857295	Japanese localization fixes.
842929 844134 866786 868904	"Most targeted" widget display issue.

Bug ID	Description
865964 870383	Event search by agent name works slower than expected.
873147 874709	Exclusions: "Signer" UI field was activated after record modification.
869248 866714	A case of exclusion deletion failure.
866109 869781	Erroneously displays event as covered despite triggered rule excluded.
823182 870637	An issue with using SAML in Azure.
868003 873781 875609 847528 848524 843608 848358 854262 810261 850760	An issue with parent process resulting in uncovered RDI.
866403 867136	Repository usage displays values beyond 100%.
863850 868255	A rare case where a Collector is not successfully deleted causing a configuration issue.
835130 871951	A rare case of Audit Log discrepancy.
871938	A case of a failure to save exceptions when created via the Support menu.
871945	A rare case where a scheduled saved query run on an expired organization.

Refer to [Central Manager - Build 2387](#) for a list of new features and changes for this build.

Central Manager - Build 2363

Bug ID	Description
857269 867140	AV scan and periodic scan do not execute bi-weekly according to audit.

Bug ID	Description
863631 867904	Memory optimization when loading event aggregations.
852083 864558	A case of periodic scan indication discrepancy.
865695 867561	A case of high disc space usage.
845302	A case of Threat Hunting facets discrepancy.
870576	Issue with FCS registration failure.

Central Manager - Build 2358

Bug ID	Description
849898 854247 854959	A case of degraded status in Collector related to configuration update error.
844232 854127	An issue with selecting all groups on assigning security policies.
842755 849836 850671 853336 853780	A case of failure to open a specific event in the Forensics tab.
843211 856940	A rare issue with registering a Collector.
859455 860086 860760	A case of failure to run Collectors report.
851572 854535	Improved logs in applications learning flow.
837455 842669 857298	FortiSandbox integration connector failure.
863114 864984	A case of an unresponsive environment related to events with non-UTF-8 characters.
856319 858986	Registration failure when using an invalid ID.

Bug ID	Description
845409	A case where a scheduled query fails to run.
855784	
848664	IoT Device Discovery collector group exclusion not retaining settings.
861510	A case of failure to retrieve data when non-UTF-8 characters exist.
864557	

Central Manager - Build 2325

Bug ID	Description
818856	save-query API call produces error 500 when attempting to add scheduled query.
819083	Repeating system events on a migrated Collector.
825236	Add new configuration to management default extra config (drivers monitoring).
827946	Saving a Threat Hunting query for all organizations may create multiple queries.
830906	A case of query parsing failure.
830935	A case when Event Viewer displays errors related to database.
835075	Occurrence of events "handled by" username display issue.
835446	LDAP connection periodic warning.
837178	Issue with Connector credentials update.
837477	Case of event for scheduled Threat Hunting query incorrectly shows Collector status.
837675	No on-premise support.
838183	Dashboard security events and Event Viewer do not show exactly the same list of unhandled processes/events.
839687	An issue where Executive Summary negates Communication Control Graph data.
839748	Exception covering query discrepancy when event's process is missing.
840527	A case of failure to save contact and SMTP connection test failure.
840741	A case of Remote Shell failure to connect.
842929	"Most targeted" Dashboard widget displays incorrect values.
852990	Display issue of Collectors that were moved from one tenant to another.
856319	A case of registration failure.
856646	Missing "Organization" parameter on custom installers.
822053	Java permission error when viewing security events.
842231	

Bug ID	Description
824323 820132	A case of exception covering query discrepancy where Collector was removed.
833313 838895	Rare failure in generating Collectors report.
844288 841058	Covering query performance improvement.
855044 798891 807585 854492	Japanese localization UI fixes.

Refer to [Central Manager - Build 2325](#) for a list of new features and changes for this build.

Central Manager - Build 2162

Bug ID	Description
839641 834706	Exception covering query miscalculation when using parent process.
839917	Case of FortiEDR Aggregator sporadical disconnection.
835764	Case of REST list-raw-data-items call failure.
835446	LDAP connection periodic warning.
845307	Offloading load from the Manager by dropping suppressed events.
844125	Optimization during security events and IoT deep scans.
842870	Log Json content in case invalid event is received.
846974	Rare case of some syslog messages not being received.

Refer to [Central Manager - Build 2162](#) for a list of new features and changes for this build.

Central Manager - Build 2159

Bug ID	Description
741117	Hardening of interfaces.
843238	Issue with system upgrade related to deployment configuration.
843709	Issue with AV Router configuration.

Central Manager - Build 2157

Bug ID	Description
807496	Localization issue.
828010	Case of Event Handling view infinite loading.
828322	Manager crash related to a case of over 100K applications.
828830	Communication Control Applications deletion issue.
829902	Failure to add action to Custom Connectors.
830429	Case of File deletion information missing in Audit Logs.
830547	Exception creation issue.
831124	Slowness of Events Search.
831565	Failure in get-events API.
832527	Hardening of interfaces.
833335	The testing of SMTP/Connector configuration connection, resulting in test failure even though connection is working.
834576	Remote shell UI issue.
835213	Case of failure to login with Two-Factor Authentication after upgrade.
837036	Case of error message in UI when deleting Application version of a product.
837807	Case of Management deadlock during simultaneous actions.
839575	Forensics UI issue of a deleted event.
839641	Irrelevant Exceptions are listed under different RDIs.
840449	FortiSandbox integration sporadically fails.
820239	Case of Management Remediation action mapping issue.
830411	
833861	Cases of failure to upgrade.
836020	
834337	Remote shell availability cases.
836675	
839244	Sporadically disconnected Connectors related to failure to get Configuration.
839917	
834341	Resolved logic of Same IP appearing in both "Included" and Excluded" in "Internal Destinations".
828705	
831980	

Bug ID	Description
835821	Case of slowness and Console freeze.
837985	
837202	
826090	Change settings of events reduction mechanism.
829671	
831565	
824442	

Central Manager - Build 2132

Bug ID	Description
761756	Remove Communication Control error indication related to limit in old Collector.
770487	Search by OS family on Inventory Advanced Search.
773051	Repeating system events on a migrated Collector that failed to register in the destination environment.
784040	Fixed incorrect number of events showing under Forensics tab.
785521	Fixed Threat Hunting Repository show as degraded in the dashboard.
790839	Fixed REST API method to get collectors for a time range.
794021	FortiEDR blocks FortiClient.
794727	Special Character '#' at start of filename results in empty field in exported Threat Hunting event.
796874	Fixed edge case of Security Event not showing on Manager.
800949	Fixed degraded Collector edge case related to Configuration path.
802617	Fixed Automatic Collectors upgrade following core upgrade.
803646	Fixed case of moving selected Collectors from filtered Collectors view.
806578	Fixed edge case of FortiEDR Console user password reset failure.
806614	Fixed Hoster view of unmanaged devices.
807224	Event Viewer search by raw ID doesn't filter out the exact event.
810818	Threat Hunting Profiles: Cannot re-assign group to a different Collection profile.
811066	Core degraded due to wrong configuration related to XDR policy.
811894	Threat Hunting data backup is now enabled by default.
813470	Fixed Communication Control Application not shown due to missing details.

Bug ID	Description
813895	Remote Shell is now working on Windows 7 32-bit (supported from Collector version 5.2.0.2241).
814292	Fixed slow loading of Security Events screen with Unhandled filter.
817496	Enhanced response time of search on Communication Control Applications page.
817636	Fixed Collector registration failure due to Aggregator load balancing.
824954	Fixed failure to delete local Aggregator following a split.
827999	Failed login with LDAP user after restart of Central Manager.
828014	The VirusTotal links in advanced data of event are broken.
829134	Login failure with LDAP user.
781603 818458	Fixed Playbook dropdown usage when selecting a Connector.
803035 785521	Events search is slow.
819728 822280	Fixed Manager malfunction upon updating Events.
820995 786407	Fixed Applications Advanced filter edge cases.
825077 816863	Slow console due to Exception Covering Query calculation.
771167 791770 792560	Fixed edge case of inaccurate CVE data presentation for application.
801620 817661 816437	Fixed Collector degradation issue due to missing configuration.
760128 767850 766885 754659 797622 790103	Enhancement of security events search performance by allowing the user to search by specific columns.
784591 810083 794015 821396 816887	Resolved Exception covering discrepancies.

Bug ID	Description
816402	
821466	
796235	
761953	
793155	
810081	
810168	
828134	

Central Manager - Build 2040

Bug ID	Description
774106	New Collectors appear as degraded due to internal parsing issue of exclusion path.
809270	License expiration date is one day earlier than expected when you save organization properties.
810100	Inaccurate Collector status displayed on Inventory.
808059	Cores become degraded once XDR policy is cloned.
811066	

Refer to [Central Manager - Build 2040](#) for a list of new features and changes for this build.

Core

The following issues have been fixed in FortiEDR 5.2.0Core. For inquiries about a particular bug, please contact [Customer Service & Support](#).

- [Core - Build 5.2.2.2047 on page 44](#)
- [Core - Build 5.2.2.2043 on page 44](#)
- [Core - Build 5.2.2.2042 on page 44](#)
- [Core - Build 5.2.2.2032 on page 45](#)
- [Core - Build 5.2.2.2030 on page 45](#)
- [Core - Build 5.2.2.2027 on page 45 \(new features\)](#)
- [Core - Build 4189 on page 46](#)
- [Core - Build 2410 on page 46](#)
- [Core - Build 2407 on page 46](#)
- [Core - Build 2293 on page 46](#)
- [Core - Build 2133 on page 46](#)
- [Core - Build 2132 on page 47](#)

Core - Build 5.2.2.2047

Bug ID	Description
977319, 0995803, 983611	Degraded Collectors due to a case of Core malfunction.
997223	Add offsets for supporting Windows 10 Enterprise 2016 LTSC.
995682	Add trusted CAs for classification.

Core - Build 5.2.2.2043

Bug ID	Description
977625	5.2.2 Cores refuse connections from Collectors upon load.

Core - Build 5.2.2.2042

Bug ID	Description
955635	Core malfunctions.

Bug ID	Description
966857	
967088	
958638	Core configuration issue related to degraded Collectors.
966638	

Core - Build 5.2.2.2032

Bug ID	Description
961270	Core is overloaded and remains in Initialization.
960670	
962958	
960082	On-premise core configuration failure.
957345	Upgrading core results in communication control exceptions.

Core - Build 5.2.2.2030

Bug ID	Description
961270	Core is overloaded and remains in Initialization.
960670	
962958	
960082	On-premise core configuration failure.
957345	Upgrading core results in communication control exceptions.

Core - Build 5.2.2.2027

Bug ID	Description
929492	The Core malfunctions.
944378	
917361	A large number of Threat Hunting events per second causes high CPU load.

Refer to [Core - Build 5.2.2.2027](#) for a list of new features and changes for this build.

Core - Build 4189

Bug ID	Description
929492 944378	The Core malfunctions.
868038 927690	Fully covered event reoccurs due to issues with IP addresses.

Core - Build 2410

Bug ID	Description
N/A	Addressed an issue with the Core build 5.2.0.2407.

Core - Build 2407

Bug ID	Description
820151	Case of Core attempting to archive EDRv2 Database.
814548 823885	Unable to export cloud core logs in Central Manager.
845305	Prevent unnecessary creation of silent events.

Core - Build 2293

Bug ID	Description
820151 814548	Case of Core attempting to archive EDRv2 Database when exporting logs.
845305	Prevent unnecessary creation of silent events.

Core - Build 2133

Bug ID	Description
829912 832602	Address potential Core crash upon handling events from previous versions.

Core - Build 2132

Bug ID	Description
807434 791308	Address cases of missing applications under Application Control.
800341 798975 802134 799758 804930	Better handling of bursts of Activity Events.

Threat Hunting Repository

The following issues have been fixed in FortiEDR 5.2.0 Threat Hunting Repository. For inquiries about a particular bug, please contact [Customer Service & Support](#).

- [Threat Hunting Repository - Build 3071 on page 48](#)
- [Threat Hunting Repository - Build 2767 on page 48](#)
- [Threat Hunting Repository - Build 2587 on page 48](#)
- [Threat Hunting Repository - Build 2524 on page 48](#)
- [Threat Hunting Repository - Build 2450 on page 49](#)
- [Threat Hunting Repository - Build 2245 on page 49](#)
- [Threat Hunting Repository - Build 2102 on page 49](#)

Threat Hunting Repository - Build 3071

Bug ID	Description
943883	Issues with filtering for multiple devices with a similar name.

Threat Hunting Repository - Build 2767

Bug ID	Description
885865	Java 17 support.

Threat Hunting Repository - Build 2587

Bug ID	Description
863463	Threat hunting query times out.
884764	

Threat Hunting Repository - Build 2524

Bug ID	Description
882465	Threat Hunting facets filtering discrepancy.

Threat Hunting Repository - Build 2450

Bug ID	Description
866403	Repository usage displays values beyond 100%.
867136	
845302	A case of Threat Hunting Facets discrepancy.

Threat Hunting Repository - Build 2245

Bug ID	Description
835261	Registration to Middleware causes index rollover even when there are no changes.
835262	Add Maintenance Controller to Middleware.
835263	Support schema update when the version is different (not just higher).

Threat Hunting Repository - Build 2102

Bug ID	Description
816698	"All Activity" counter is calculated incorrectly in dual data source environments in threat hunting page.

Known issues

The following issues have been identified in 5.2.0. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
939481	In some cases, the communication control feature does not work due to unforeseen technical issues. Workaround: Troubleshoot and upgrade the Central Manager.
973077	When you run a Threat Hunting query, the response time can vary depending on the selected "Time" and the amount of collected data. When the time is set to 30 days, the query can run for a few minutes.
982543	Cannot move a Collector to a different group via Rest API.
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.
941462	Upgrade to Central Manager build 5.2.0.3051 might fail in case of LDAP settings with no gateway.
N/A	Central Manager version 5.2.0.2387 or below does not work with Threat Hunting Repository version 5.2.0.2524. Workaround: Upgrade the Central Manager, preferably to the GA version.
907362	Remote shell does not work on Windows XP and Windows server 2003.
842110	In some network configurations, a rare issue might cause collectors to be detected as IoT devices.
734616	The Advanced Search feature for Applications retrieves an application even if only some, rather than all, of the search parameters match specific versions of the application, which results in an empty application dropdown in some cases.
837675	No on-premise support before Central Manager build 5.2.0.2325.
812319	FortiEDR Connect cannot be used to run commands that are user-interactive
811290	It is not possible to redirect FortiEDR web to a URL that is different than the one provided by Fortinet.
809060	FortiEDR Connect session may be disconnected due to inactivity of the FortiEDR Console, even though the Connect session is active.
807930	Application Control search only works by exact match
807230	FortiEDR Connect cannot be used with 32-bit devices

Bug ID	Description
786156	Windows security center registration is not supported with Windows servers 2019 and above.
777707	Linux Collector content file is large and uploads slowly to the Central Manager.
773610	Execution Prevention Events are missing Device users.
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.
771666	OS indication is missing under Inventory and Dashboard for Linux Collector for Centos 6.
771630	Device internal and external IP is missing from Threat Hunting events of Linux devices.
771619	Organization filter under Threat Hunting Hoster view malfunctions.
771044	SAML authentication cannot work with different organizations that use the same SAML Azure account. Workaround: Use different Azure accounts for different FortiEDR organizations.
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.
765648	Threat hunting exclusions cannot be set on log events coming from Linux devices
759573	Collector upgrade via custom installer requires password.
734594	Linux Threat Hunting Activity Events are missing the process hash.
734309	NGAV scan of specific Collectors/Groups scan all 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.
733601	Isolation and communication control connection denial are not supported with Oracle Linux Collectors.
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.
0733598	Safari 11.1 on MacOS malfunctions when viewing events.

Bug ID	Description
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.
733592	Number of destinations under communication control is limited to 100 IP addresses.
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.
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 Center via UI.
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.
733550	Upgrading from Older Versions: A direct upgrade path for backend components (Central Manager, Aggregator, Core, Threat Hunting Repository) of V5.0.2 or earlier is not supported. Workaround: Upgrade the older environment to V5.0.3 before upgrading it to V5.2.
733548	Component Backward Compatibility: v5.2 Central Manager supports Cores/Collectors from older versions with limited functionality. Some new features introduced in later versions may not be available.
854124	An issue with suspicious driver FP events caused by the Core 5.2.0.2293 build. Workaround: Upgrade the Core to build 5.2.0.2300 or upgrade Content to 7431.
889422	Remote shell connection cannot be established if collector connects to aggregator via a proxy server.



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.