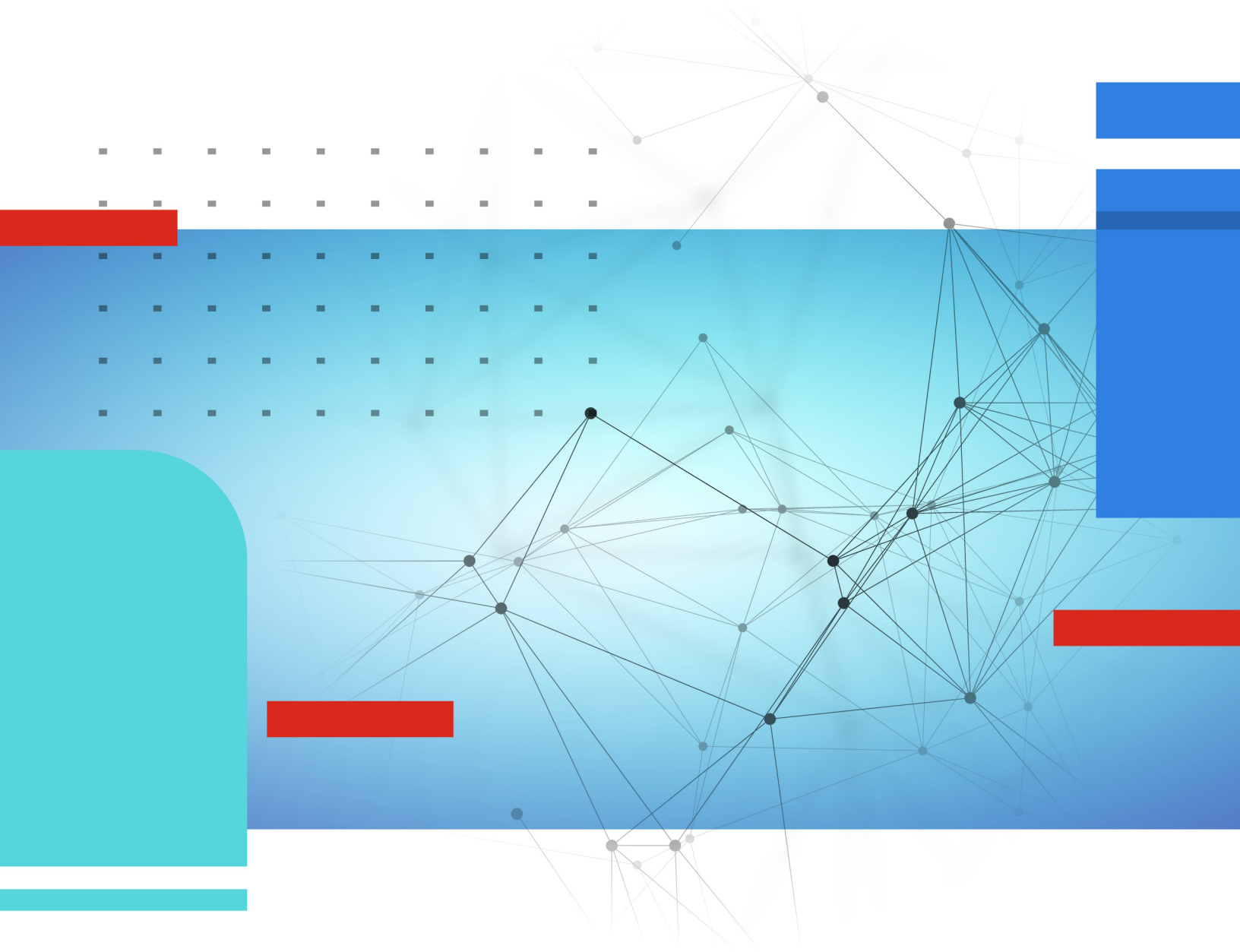
Release Notes

FortiEDR 6.2.0



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

August 27, 2025
FortiEDR 6.2.0 Release Notes
63-620-989680-20250827

TABLE OF CONTENTS

Change log

Date	Change Description
2024-03-15	Initial release.
2024-03-18	Updated build numbers in FortiEDR 6.2.0 Release Notes on page 7 and Resolved issues on page 23.
2024-03-27	Updated Upgrade information on page 21.
2024-03-28	Added Central Manager build 6.2.0.0440 to Resolved issues on page 23.
2024-04-02	Updated resolved issues list for Central Manager build 6.2.0.0440 in Resolved issues on page 23.
2024-06-04	Added Central Manager build 6.2.0.0451 to What's new on page 8 and Resolved issues on page 23.
2024-06-18	Updated GA build (Central Manager - 6.2.0.0436, Core - Build 6.0.1.0578, Threat Hunting Repository - Build 6.2.0.0427) on page 17.
2024-07-04	Added Central Manager build 6.2.1.0098 to Resolved issues on page 23.
2024-07-29	Deleted Central Manager build 6.2.1.0098 from Resolved issues on page 23.
2024-08-07	Added Central Manager build 6.2.1.0111 to What's new on page 8 and Resolved issues on page 23.
2024-08-22	• Updated Upgrade information on page 21. • Added Central Manager - Build 6.2.4.0026 on page 13 to Central Manager - Build 6.2.4.0026 on page 13. • Added ticket 1001334 to Known issues on page 34.
2024-09-04	Updated Central Manager - Build 6.2.4.0026 on page 13.
2024-09-12	Added ticket 982543 to Central Manager - Build 6.2.1.0111 on page 30.
2024-09-27	Updated Central Manager - Build 6.2.4.0026 on page 13.
2024-10-23	• Added Central Manager - Build 6.2.2.0063 on page 28 and Threat Hunting Repository Build 6.2.2.0034 • Updated Known issues on page 34
2024-12-02	Updated Known issues on page 34.
2024-12-03	Added Central Manager build 6.2.3.0036 to Resolved issues on page 23.
2025-01-14	Added Central Manager - Build 6.2.4.0026 on page 13.
2025-01-22	Added an enhancement for Central Manager - Build 6.2.3.0036 on page 14.
2025-02-27	Updated Known issues on page 34 as follows: • Added ticket 1014223

Date	Change Description
	• Updated the description of ticket 765648
2025-03-04	Added ticket 939481 to Known issues on page 34.
2025-04-17	Added Central Manager - Build 6.2.5.0052 to Resolved issues on page 23.
2025-04-22	• Added Central Manager - Build 6.2.5.0052 on page 10 • Updated Central Manager - Build 6.2.3.0036 on page 14
2025-05-22	Added ticket 1136128 to Known issues on page 34.
2025-07-10	Added Central Manager - Build 6.2.6.0097 on page 8.
2025-08-18	Added Changes to disconnected (expired) status for VDI devices on page 11 to Central Manager - Build 6.2.5.0052 on page 10.
2025-08-27	Added AV Engine 7.0 signature support on page 9.

FortiEDR 6.2.0 Release Notes

This document provides information about FortiEDR version 6.2.0.

Version history

	Central Manager	Core	Threat Hunting Repository
2025-07-08	Build 6.2.6.0097		
2025-04-17	Build 6.2.5.0052		
2025-01-14	Build 6.2.4.0026		
2024-12-03	Build 6.2.3.0036		
2024-10-15	Build 6.2.2.0063		Build 6.2.2.0034
2024-08-07	Build 6.2.1.0111		
2024-06-04	Build 6.2.0.0451		
2024-03-28	Build 6.2.0.0440		
2024-03-15 (GA)	Build 6.2.0.0436	Build 6.0.1.0578	Build 6.2.0.0427

What's new

This section identifies new features and enhancements available with FortiEDR 6.2.0.

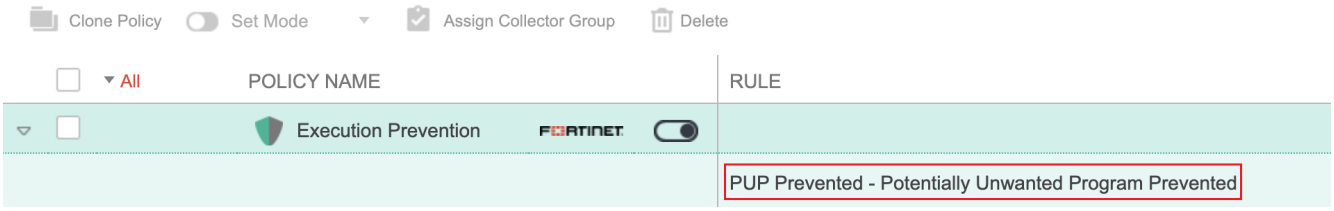
Refer to Resolved issues on page 23 for a list of resolved issues for each build.

Central Manager - Build 6.2.6.0097

This build includes the following new features and enhancements:

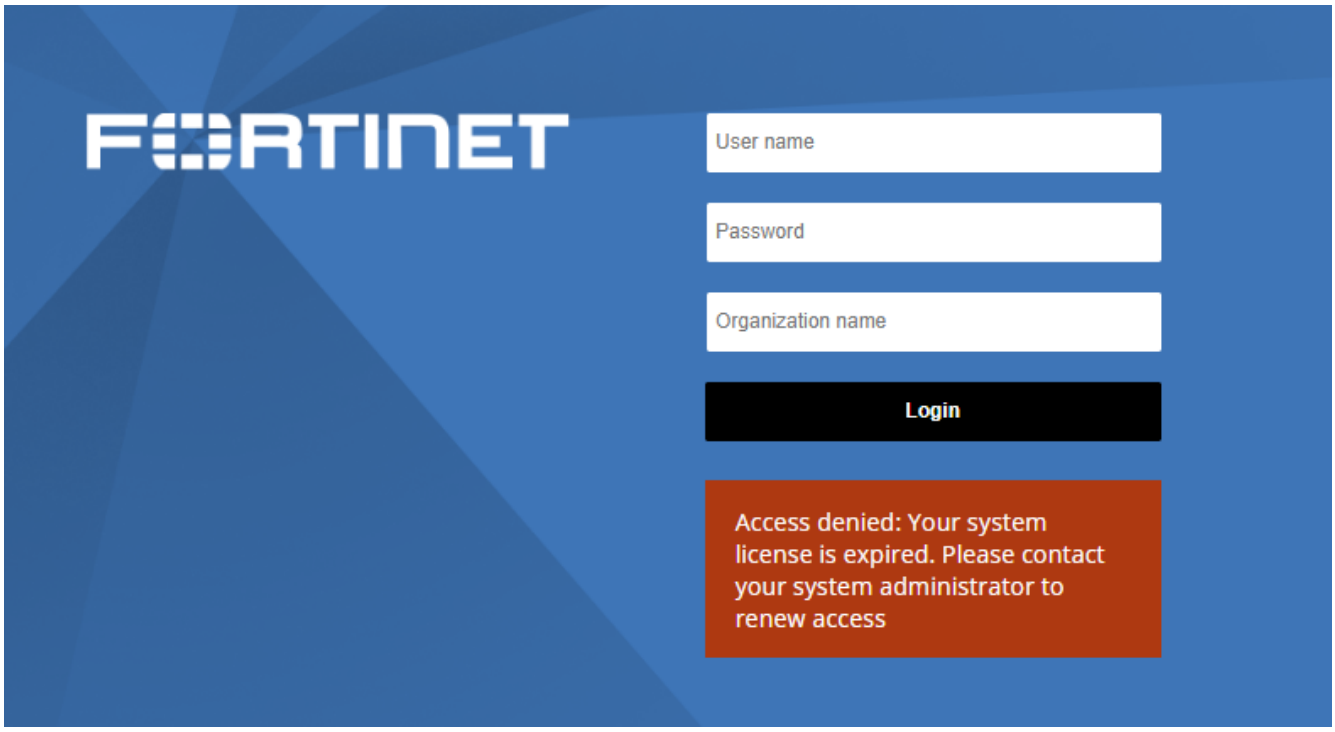
New Execution Prevention rule for PUP

This build adds the *PUP Prevented - Potentially Unwanted Program Prevented* rule under the Execution Prevention policy (see Out-of-the-box policies) for enabling or blocking Potentially Unwanted Program (PUP) during pre-execution. This feature requires Collector version 5.2.8 or later.



Block login of users on license expiration

To add security, users with an expired license are now not allowed to log into the FortiEDR management console. The following error message is displayed:



AV Engine 7.0 signature support

You can now select the AV Engine version and caching on the Aggregator using the following API:

```
/get-file/FortiAv
*Method:*
GET
*Query Params:*
Version
AVEngineVersion
OS
FileType

*Optional Query Param:*
Arch
CollectorVersion
```

Do not use the *CollectorVersion* and *AVEngineVersion* parameters together, which will cause an error. An exception is to send the *CollectorVersion* value as "N/A", in which case FortiEDR will omit the *CollectorVersion* value.

Hardening enhancement

This build also includes some hardening enhancements.

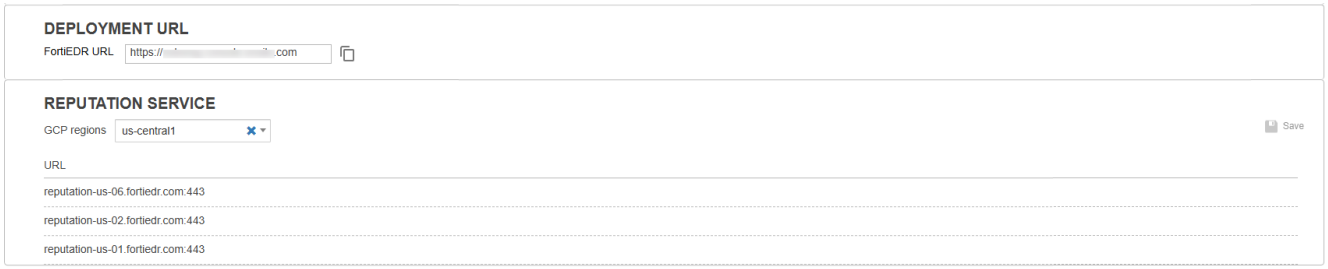
Refer to Central Manager - Build 6.2.6.0097 on page 23 for a list of resolved issues for this build.

Central Manager - Build 6.2.5.0052

This build includes the following new features, enhancements, and changes:

Deployment URL and reputation service list in *Administration > Tools*

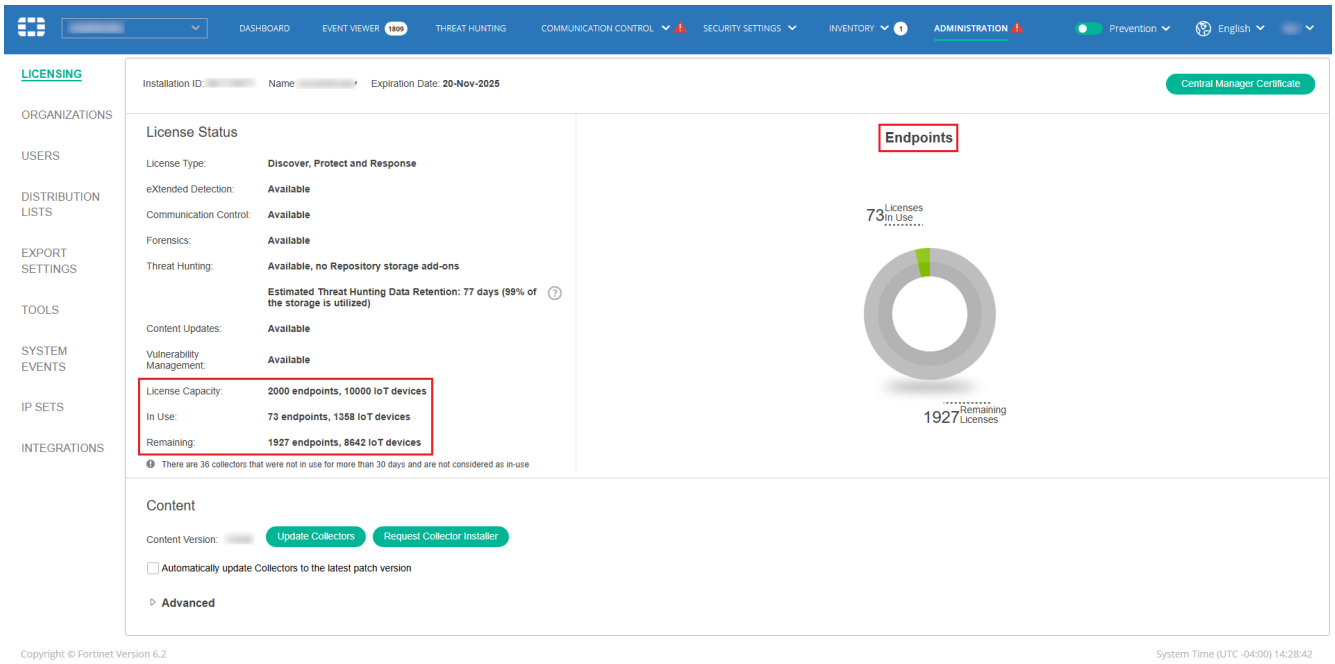
The *Administration > Tools* page includes the following new sections:



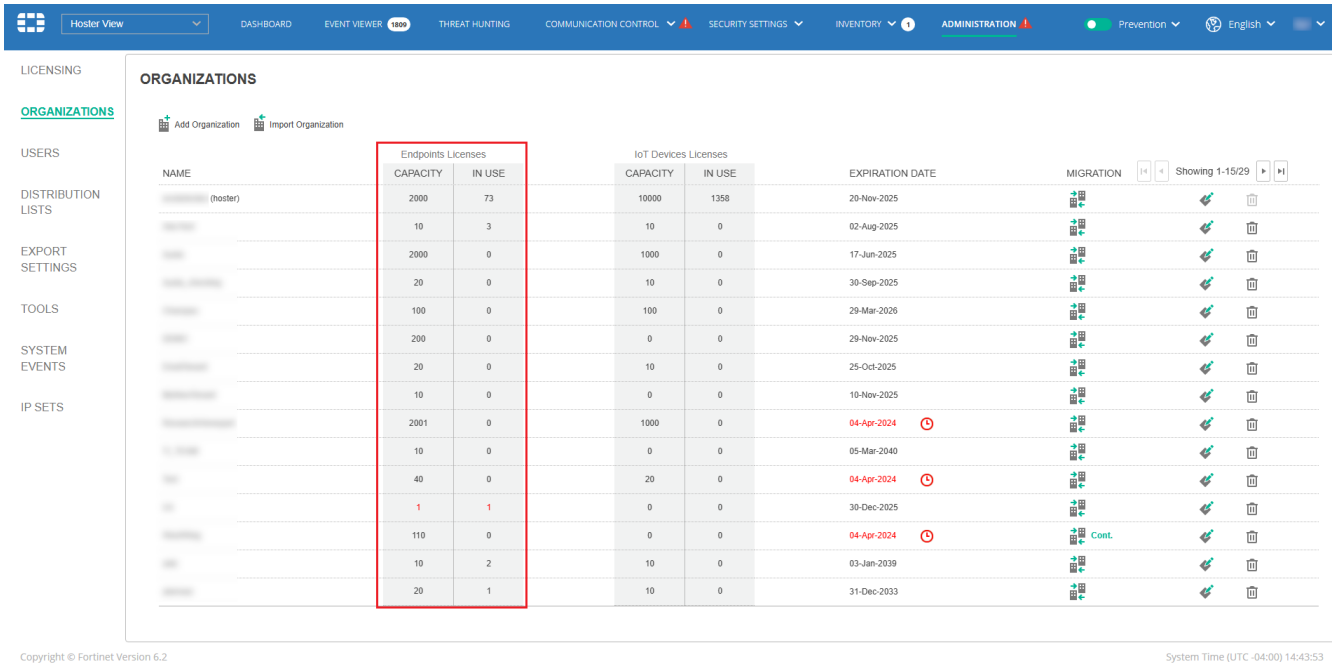
- *Deployment URL*—Displays the URL of the environment that you can copy. The URL is read-only and includes the domain information that you will need in order to use FortiEDR APIs.
- *Reputation Service*—Displays a list of GCP regions where a reputation service instance is installed on and the relevant URLs of all selected regions. You can select any region you want to connect to. By default, all regions are selected. When a region is selected, the relevant reputation service URLs are displayed so that you can open them in your firewall.

License consolidation for workstations and servers

FortiEDR now consolidates workstations and servers as endpoint during license count. See Licensing.



In multi-tenancy, the *Administration > Organization* page now displays the *Endpoint Licenses* column instead of separate columns for workstations and servers.



Changes to disconnected (expired) status for VDI devices

VDI devices are now shown as *Disconnected (Expired)* if they have not been connected for 6 hours. This time threshold used to be 30 days. See Collectors for more information about different Collector statuses.

Refer to Central Manager - Build 6.2.5.0052 on page 25 for a list of resolved issues for this build.

Central Manager - Build 6.2.4.0026

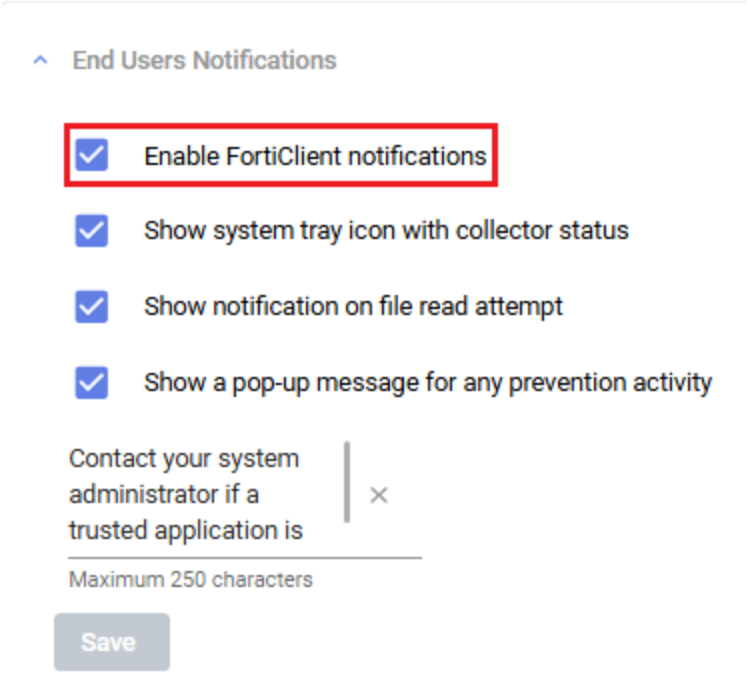
This build includes the following enhancements:

Support ADOM blocking when FortiManager is configured in Worskpace mode

The integration with FortiManager and ADOMs is enhanced to support ADOM configuration blocking prior to executing the changes. The integration can be configured per organization using the built-in Firewall connector.

Enable FortiClient notifications for FortiEndpoint deployments

You can configure FortiEDR to send notifications to FortiClient EMS using the new *Enable FortiClient notifications* option under *Administration > Settings > End User Notifications*.



Disable Jumpbox change option for Cores earlier than 6.0.1.652

This build disables Jumpbox change option for Cores earlier than 6.0.1.652.

Data Obfuscation

This build obfuscates fields for all data (see list below) sent from the Central Manager to FCS, regardless of whether the data is sent via RabbitMQ or REST API.

- Username
- Hostname
- Customer name
- MAC address
- IP address – Both device IP and IP relating to event (target destination for example), internal ranges only
- Files attachments (if submitted)
- Organization name
- Domain name

Refer to Central Manager - Build 6.2.4.0026 on page 26 for a list of resolved issues for this build.

Central Manager - Build 6.2.3.0036

This build includes the following behavior change:

Retrieving reputation data from reputation service without going through Core

Starting from this build, the FortiEDR Windows Collector (5.2.5.0052 or later) periodically retrieves reputation data from reputation service without going through Core. The Windows Collector periodically runs a proximity check and decides which reputation service to connect to depending on response speed and load status of the service. If the reputation service fails or connection errors occur, the Collector immediately falls back to the Core for the reputation query and then attempts the proximity check again after the 5 minutes interval.

Refer to Central Manager - Build 6.2.3.0036 on page 27 for a list of resolved issues for this build.

Central Manager - Build 6.2.1.0111

This build supports upgrade from the following builds only:

- **6.2.0.0451**—If you are running 6.0.1.0723 or 6.0.1.0940, upgrade to 6.2.0.0451 first before upgrading to 6.2.1.0111.
- **6.2.1.0098**

This build includes the following enhancements:

HTTPS support for Grafana conection

You can now connect to Grafana via HTTPS when running FortiEDR on-premise. To enable the HTTPS access, ensure TLS is enabled on Grafana, which means Grafana is not accessible by IP anymore. To resolve Grafana FQDN, you must create a DNS record that pointed on the threat hunting repository's IP or update your "hosts" file.

You can use the self-signed certificate automatically generated during installation or use or your own certificate by providing the following when prompted: CA, TLS and TLS key files in PEM format. The CN of your certificate must be the FQDN of the chosen Grafana (eg. `grafana.mydomain.local`).

Enable legacy Forensic view

You can now enable or disable the legacy Forensics view globally through Fortinet Support.

(On-premise) Ubuntu migration support

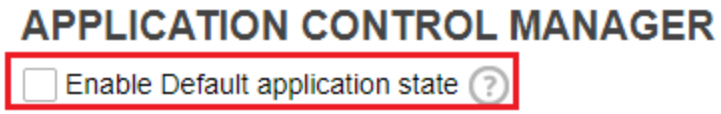
This build adds support for Ubuntu migration. After upgrading your on-premise deployments to this build (with the default CentOS), you can migrate to Ubuntu 22.04 by following the instructions in the Administration Guide.

Refer to Central Manager - Build 6.2.1.0111 on page 30 for a list of resolved issues for this build.

Central Manager - Build 6.2.0.0451

This build includes the following enhancement and behavior change to the default block state of new applications under *Security Settings* > *Application Control Manager*:

- The default block state of new applications is changed from enabled to disabled, which means new applications are now no longer blocked by default.
- You can now define the default block state of new applications using the new *Enable Default application state* option under *Administration* > *Tools* > *Application Control Manager*. When this option is enabled, new applications will be blocked by default.



Refer to Central Manager - Build 6.2.0.0451 on page 32 for a list of resolved issues for this build.

GA build (Central Manager - 6.2.0.0436, Core - Build 6.0.1.0578, Threat Hunting Repository - Build 6.2.0.0427)

The FortiEDR 6.2.0 GA build includes the following features:

eXtended detection with FortiAnalyzer Cloud, FortiSIEM, and FortiSIEM Cloud

FortiEDR 6.2.0 adds support for the following external systems as eXtended detection source:

- FortiAnalyzer Cloud
- FortiSIEM
- FortiSIEM Cloud

Forensics functionality relocated under Investigation View

To have one pane of glass for events analysis and handling, FortiEDR 6.2.0 consolidates forensics functionality and stacks view capability in the investigation view, accessible from the *Advanced Data* tab under *Event Viewer*. See next section for details.

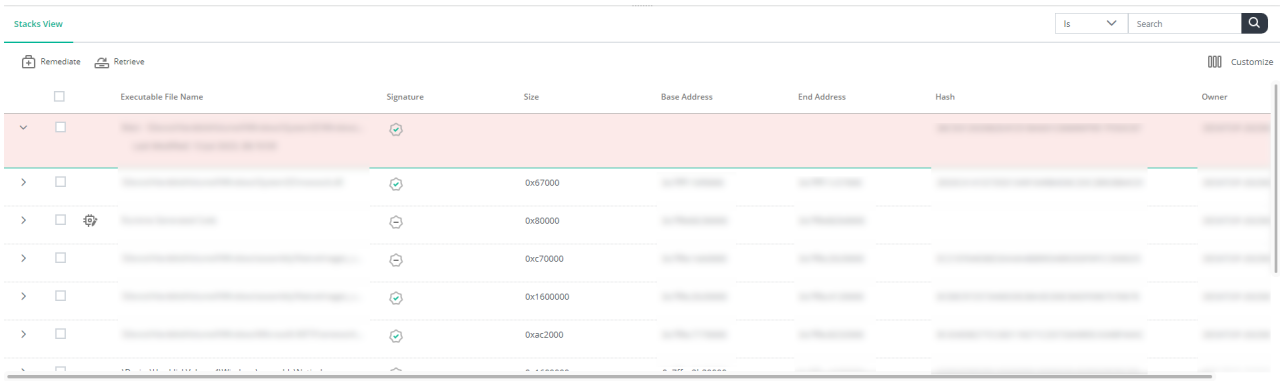
As a result, the following forensics tabs and pages are revoked:

- *Forensics* tab—With the removal of the *Forensics* tab, the *Threat Hunting* sub-page is promoted to be its own tab. The compare view in the *Forensics* tab is removed completely with no equivalent function in the investigation view.
- *Forensics* > *Events* menu page
- *Forensics* toolbar option in the *Event Viewer* page

Investigation View enhancements

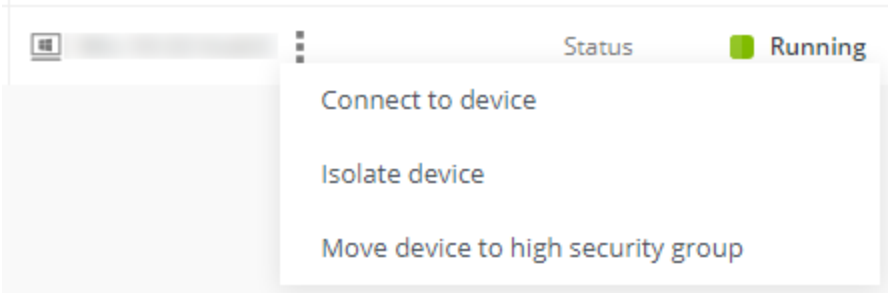
FortiEDR 6.2.0 includes the following enhancements to the investigation view (accessible from the *Advanced Data* tab under *Event Viewer*):

- Access an enhanced version of stacks view by selecting an edge that is part of a security event. Compared with the stacks view in the *Forensics* tab in previous versions, the new stacks view supports additional analysis and response actions, such as retrieving memory and remediating files. The interface is also more flexible and interactive.



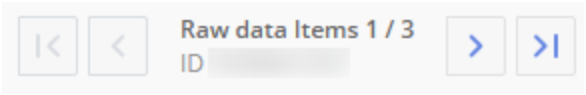
- Export the event as a JSON file:

- Connect to a device, isolate a device, or move a device to high security group:



- Filter the results in the Activity Events table to include or exclude a specific value using the green plus ( ) and red minus ( ) icons that appear when you hover over the value. Multiple filters are supported.

  This feature is also added to the investigation view launched from the Details Pane under *Threat Hunting*.
- Navigate between raw data items using the new navigation bar at the bottom-left of the investigation view graph.



Pre-defined application control groups

To better organize and group applications in the application control manager, FortiEDR 6.2.0 introduces predefined groups of applications, such as *Network Scanning Tool*, *Remote Access Tool*, and *Disk Encryption Tool*. The predefined application groups are always at the top of the application list and are indicated by the Fortinet logo by the group name. Predefined application groups are read-only and can be modified by Fortinet from time to time.

All applications added by the user are now grouped under the *User defined* group.

New *Application Name* field in application control

Starting from FortiEDR 6.2.0, each application has a name that is unique per group. You must specify the application name when manually adding an application to be blocked. The application name is also included when you export the list of applications.

Exporting and importing exclusion lists

FortiEDR 6.2.0 allows you to export or import exclusion lists for Process Exclusions and Execution Prevention Exclusions in the exclusion manager, which is handy in a muiti-tenant environment where you can easily duplicate the exclusion lists for some or all organizations without the need to re-define exclusions for each organization separately.

FortiEDR Connect (Remote Shell) commands auditing

In FortiEDR 6.2.0, the FortiEDR Audit Trail feature records every action that was performed in a FortiEDR Connect session, rather than just the connection of a FortiEDR Connect session.

Filter by FortiGate or VDOM for FortiAnalyzer and FortiAnalyzer Cloud eXtended detection

In FortiEDR 6.2.0, when you create an eXtended detection source connector for FortiAnalyzer or FortiAnalyzer Cloud, you can configure the FortiGate and VDOM logs to be correlated with FortiEDR data by specifying the FortiGate or VDOM name in the corresponding field. If both fields are empty, FortiEDR uses the default value, which is *All*.

Support for CEF and LEEF format Syslog

FortiEDR 6.2.0 introduces two new formats for Syslog messages: Common Event Format (CEF) and Log Event Extended Format (LEEF), allowing more effective management and correlation of FortiEDR events in your SIEM device.

For the field mapping between FortiEDR security event format and CEF/LEEF format, refer to the FortiEDR 6.2 Syslog Message Reference guide.

Control access to new license functionality in multi-tenant environments

When applying a new license functionality in a multi-tenant environment, the MSSP manager can now configure which tenants will receive the new functionality for more granular access control, as opposed to the old behavior of having to open new license functionality to all tenants. Refer to the FortiEDR 6.2.0 Administration Guide for detailed instructions.

Certificate renamed *Signature*

The *Certificate* field is renamed *Signature* throughout the FortiEDR console, such as the *Event Viewer*, *Investigation View* and *Threat Hunting* pages, etc. Possible values:

- Signed
- Unsigned
- Self-signed
- Invalid timestamp
- Signed (no timestamp)

Refer to Central Manager - GA Build 6.2.0.0436 on page 33 for a list of resolved issues for this build.

Upgrade information

FortiEDR 6.2 Central Manager supports upgrade from 5.2 or 6.0 with the following restrictions:

- The following FortiEDR Central Manager builds cannot be upgraded to 6.2 directly:
  - **5.2.0.3091 or earlier**—You must upgrade to 5.2.0.3092 first before you can upgrade to 6.2.0.
  - **6.0.1.0155 (6.0 GA)**—You must upgrade to 6.0.1.0723 first before you can upgrade to 6.2.0.
- Build 6.2.1.0111 supports upgrade from the following builds only:
  - **6.2.0.0451**—If you are running 6.0.1.0723 or 6.0.1.0940, upgrade to 6.2.0.0451 first before upgrading to 6.2.1.0111.
  - **6.2.1.0098**

Upgrading a macOS Collector to 6.0 can only be done via JAMF. Manual upgrade or upgrade via the FortiEDR Console are not supported.

Refer to the FortiEDR 6.0 Release Notes for additional upgrade information if you are upgrading from 5.2 to 6.2.

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. For inquires about a particular bug, please contact Customer Service & Support.

Central Manager - Build 6.2.6.0097

Bug ID	Description
1081179, 1168208	Remote shell command description is misleading.
1131478, 1139171	Issue with filtering SimulationBlock events in Rest API.
1022052, 1044640	UI issue in Investigation View.
1137684, 1139174	No error is shown when the Aggregator IP field is left empty when you request a custom macOS Collector installer.
1090085, 1093959	Performance issue when changing between tabs or moving between events.
1096510, 1109687, 1116872, 1117326, 1102300	Logon errors and White Label Error Pages when accessing the environment.
1016548, 1017832	Cloning the Threat Hunting profile does not work via REST API.
1132045, 1133075	Memory issue when handling a huge number of events through the UI.
1139830, 1140795, 1142004, 1141862, 1141316, 1141220	Issue with processing an event due to an internal length limitation.
1107662, 1109610	Gibberish values in Communication Control application names.

Bug ID	Description
1131859, 1133653	Issue with cloning communication control policies via REST API.
1107662, 1090738, 1109213	REST API call to list all applications for all Collectors and their vulnerabilities times out without returning values.
1148830, 1150189	Failure to run Inventory report if Communication Control report is stuck.
1149315, 1158932, 1127455, 1172972, 1141221	Only security events are received in SIEM. System events and audit trail are not received.
1094467, 1100131	Workstation with the FortiEDR Collector installed are incorrectly shown under unmanaged devices.
1141888, 1152713	Wrong calculation of last seen field in Inventory view.
1151399, 1156292	Remote Shell session counter does not calculate session time correctly.
1134162, 1151250	During the provisioning a FortiEDR instance via support portal, the Threat Hunting feature should be disabled when no respond entitlement is present.
1167889, 1169846	Playbooks are only visible in hoster view and not in organizational view.
1145498	When you access the REST API information in the FortiEDR Manager, the example URL reflects the Aggregator's FQDN instead of the Manager's FQDN.
1146024	FortiClient notification configuration issue.
1096331	Event Geo location is incorrect.
1161774	CPU load is too high.
1147020	Failure in pooling cloud reputation services list.
1148687	Failed to retrieve data from the Threat Hunting database.
1144851	No default classification is selected when handling events.
1139170	Request Body is not marked as "Required" in swagger but is required by Management.
1150839	The acquire license API does not work for Collectors in running state.
1152231	Checkbox is missing in Process Exclusion window in Exclusion Manager.
1156296	Creating an exception in the Manager does not take effect on the Collector.
1168763	Collectors migration stuck in pending migration.
1166686	Failed to transfer the account once the password was changed.

Refer to Central Manager - Build 6.2.6.0097 on page 8 for a list of new features and enhancements for this build.

Central Manager - Build 6.2.5.0052

Bug ID	Description
1118639	Block usage of old unsupported collectors (before 5.2.5, 5.1.12, 6.0.9).
1121460	Missing seconds for threat hunting time range filter.
968588, 1109210	Security events are not archived when handled with the "Archive when handled" mark.
1027570, 1049988	Unable to delete IP set.
1030972, 1109209	Remote URL/IP might be missing in the investigation view when Action Node is Network Access.
1044328, 1126689	FortiEDR API times out when creating an organization.
1048022, 1072336, 1051316	Executable shows as Signed (invalid) in Investigation View.
1060485, 1071139	Collectors uptime in Investigation View might be wrong.
1070454, 1109212	When requesting a Collector, the latest version is at the bottom instead of the top of the dropdown list.
1082958, 1109211	Misleading popup warning when exporting exceptions.
1088396, 1111097	"Add to blocklist" does not work.
1088918, 1110424	Error when adding exceptions in Investigation View.
1096392, 1103190	Failed to load investigation view for some events
1102334, 1109611	Part of the Japanese translation for the "Tools" - "End User Notifications" description is missing.
1107662, 1109213	REST management-rest/comm-control/list-products takes too long.
1109749, 1110426	Core is disconnected after upgrade.
1111237, 1111316	Failed login not exported to Audit report on single account environments.
1111339	Events are not shown as expected.
1111573	Updating number of shards task causes many registration requests.
1111424, 1115523	Moving the Collector is only available in Hoster view.
1123003, 1126709, 1128535	Configuration error when an agent group is deleted.

Bug ID	Description
1124038, 1130754, 1125096	Central Manager crashes due to a memory issue.
1126848	Collector registration fails due to license count error.
1125644	Window freezes after pressing on the administration tab.
1113344	Deleting a facet on threat hunting doesn't work.
1117172	Error in REST API Update Organization function.
1111786	Application Control configuration fails to reach the Collector.
1132502	Central Manager upgrade fails when on-premise reputation configuration is present.
1132503	Failed to retrieve scan test information for IoT devices.
1130738	Error in REST API Create Organization function.

Refer to Central Manager - Build 6.2.5.0052 on page 10 for a list of new features and enhancements for this build.

Central Manager - Build 6.2.4.0026

Bug ID	Description
1109606	The "Change" option for Jumpboxes should be disabled for core versions 6.0.1 or earlier.
1100797	Fix SSL communication from the Central Manager to the Internet.
1103485, 1104828	Pattern matching issue when creating a command line exception.
1017194	Remote shell commands fail to execute when whitespace exists.
1040689, 1092458	Issue with importing users with admin role during account move from single-tenant environment.
998858	webapp crashed - krys-both-europe-west3-b-0.
1027782	Set maximum number of rows for export to Excel as 1000000, which is the maximum that Excel supports.
1107296, 1107590	Forensics page fails to load.

Refer to Central Manager - Build 6.2.4.0026 on page 13 for a list of new features and changes for this build.

Central Manager - Build 6.2.3.0036

Bug ID	Description
1066418, 1079834	When saving a threat hunting query, the "Trigger Playbook Actions" configuration is not saved.
1084495, 1086725	Error when resetting password via API.
1085365, 1087595	Event exception deletion is not logged in the audit logs.
1077632, 1081360, 1079828	Configuration becomes degraded due to a missing backslash at the beginning.
1060494, 1071138	Unable to see the whole command line path string in the investigation view.
1076572	Queries from Threat Hunting page do not return results.
1048022, 1072336, 1051316	Executable files are shown as "Signed (Invalid)".
1066453, 1073361	Time zone is different between "Event Viewer" and "Advanced Data".
982597, 995691	File hash is missing in the Stacks view.
1087430, 1088329	OS vulnerabilities reported for latest manager release based on Ubuntu.
1094445	Failure in importing an organization with "evt_aggregations_temp" error.
1093013, 1090062, 1093453	Timeout while exporting Aggregator log under certain conditions.
1093002, 1099133	Exceptions covering queries work slowly on Ubuntu systems.
1085287	Failure in creating an organization with a FCTEMS serial number.
1067236	Only SHA1 should be allowed in exclusions for Linux.
1085285	Cores with a deprecated version should be blocked from registration.
1086245	Content version reverts to default after Ubuntu migration.
1069070	Events from the last hour are not displayed.
1087603	Failure in creating exceptions with a signer name and executable path.

Refer to Central Manager - Build 6.2.3.0036 on page 14 for a list of new features and changes for this build.

Central Manager - Build 6.2.2.0063

Bug ID	Description
1007499, 1007958	No support for CEF v0.
1010193, 1011186	The Getting Started pop-up is stuck at the right side of the page.
0940899, 981604	The script path shown in a Blocked Event is incorrect.
1043710, 1045205	Internal performance issues might lead to cores and collectors being shown as disconnected.
1027570, 1049988	Failure to delete IP set.
0985081, 1041719	Slowness In the UI when handling a large number of IP sets.
1004747, 1005499	The version drop-down list for the Update Collector Version is not sorted by revision.
1019580, 1020679	Failure to define an exception on the command line using a wildcard.
951958, 978480	The option to uninstall the OSX collector via Management has been removed (uninstallation will be done via JAMF).
1010469, 1011188	Format issue for messages with line breaks.
1014407, 1041720	Enhanced hardening.
1048446, 1049386	Parsing issue in FortiSIEM Connector.
1060132, 1060358	UI slowness.
1021705, 1048985, 1042304	Inappropriate error message appearance.
1043533, 1044050	An Isolating and Moving device case was allowed for some Read-Only users in Graph view.
1000196, 1064026, 1071260, 1068122, 1014861	Failure to log in using LDAP.
1044328, 1044639	Rest API calls to create organizations takes generous amount of time and cause a time-out.
1069674, 1071140	Improvement of dashboard UI performance.
1046536, 1055564	UI issue with Threat Hunting Time Range Value Changes.
1049792, 1051826	REST API issue related to creating a tag for an organization.
1073415, 1074435	Move collector to group button is unresponsive with no pop-up windows appearing.
1041344, 1072741	Slowness in Threat Hunting query results.
1074761, 1075509	Get-audit REST data is corrupted when run by the hosted user.

Bug ID	Description
0964033, 969496	The manager sending inaccurate customer serial Numbers during Forti Analyzer log generation.
1061680, 1063403	End Users Notifications and WCS settings not saving under Tools.
1021733, 1056612	Communication Control applications fail to Export to Excel.
1068904, 1070697	A new organization is not showing in FCS & OPS Portal.
1019573, 1068607	An error message pops up in the aggregator due to incorrect detection of Gateway account ID.
1023419, 1064123, 1061764	An issue with condition handling.
1046232, 1075845, 1073021, 1058030	An issue with covering exceptions related to wildcards.
1009758	Cannot create exceptions on archived events via the REST API.
1038389	Localization issue in the Admin Tools page, where some button labels are in English when the UI is set to Japanese.
1038390	Localization issue with the Export button label, which is not in Japanese.
1038392	Japanese localization issue in the Investigation view, where the error message is in English when no EDR is connected to Management.
985339	An Internal ID field should be configurable through the syslog connector screen.
1069623	Error when filtering null or broken events.
1067238	Collector fails to get configuration when connected to Aggregator in a separate tenant.

Common vulnerabilities and exposures

Central Manager - Build 6.2.2.0063 is no longer vulnerable to the following CVE reference:

Bug ID	CVE reference
1072799	CVE-2024-45323

Central Manager - Build 6.2.1.0111

Bug ID	Description
998216, 999110	Missing group assignment for exceptions.
1043710, 1045205	Cores and Collectors are shown as disconnected.
1047134, 1040038	Central Manager console is slow.
1060698, 1061245, 1055565	Failure after upgrade.
1015401, 1016286	Optimize "Update Event" query.
891658, 898734, 1001087, 1001509, 871488, 878328, 891628, 898735, 875941, 886735, 991703, 1012791	Localization fixes across UI.
989826, 1013342	Connectors page flickers.
996383, 999111, 1002993, 1006009, 996383, 996304	The management console runs slow.
1008315, 1013846	Wrong timezone in Threat Hunting logs export timestamps.
979032, 987942	Notification email is still sent to the user after the user has been removed from the user or distribution list.
896347, 1018307	False positive events are returned when you filter by URL field in the *Threat Hunting* page.
1004747, 1005499	Versions in the *OTI Version* dropdown are not sorted by revision.
1002993, 994765	Malfunction while saving user preferences.
1003742, 1020687	Web application fails to start.
1016569, 1017311	The timestamp of runtime generated code is wrong in Graph view.
1020292, 999109, 992151, 995697, 998599	The management console freezes.
943931, 993736	Unable to delete events due to slowness in management console.
1002993, 1006493	Failure to retrieve events through RestAPI after Collector isolation.
1002993, 1016282	Improve IOT performance.
816929, 833903	Improve Collector expiration logic.
867670, 869516	RHEL Collectors display under *New OS Family* in *Inventory*.
1009275, 1009755	Failure in saving a new password policy.
1000225, 1017310	Missing configuration after moving Collectors.

Bug ID	Description
1011708, 1016285	Inconsistency in time value of expiration date when updated via the management console and via REST API.
986183, 988881	Remote shell failure notice after upgrade.
1026044, 1026437	When Japanese is selected, applications cannot be added using Application Control Manager.
1007499, 1007954	CEF messages have three extra dashes and do not follow the RFC-3164 standard.
1002993, 1013848	Failure in parsing IOT scan.
1008673, 1014862	The number of Collectors in *Dashboard*does not match the number in *Inventory*.
1005039, 1006008	Error parsing Stix2 feed with SHA-1 value.
1008450, 1008577	New Collector registration fails in environments with add-ons.
937104, 1007422	Improve TCP syslogs.
1027885, 999553	Failure in loading *Advanced Data* details.
940899, 981604	The script path shown is incorrect in blocked events.
1019247, 1020682	Exclude noisy organizations from sending events in case of a flood of events.
928566, 1021657	When exporting to Excel in Japanese environment, the order of column is sorted differently from the English environment.
1018853, 1029861	Updating organization from the UI resets number of shards to 1.
1026062, 1023904	"Loading data failed" error after right-clicking a node and selecting *View activity events* in *Investigation View*.
1010193, 1011186	Getting Started popup windows gets stuck at the right side of the page.
1006077, 1022775	Empty Taxii2/Taxii1 feed conversion should return "empty feed" error.
1033544, 1029339	Unable to update number of licenses for organizations with unsupported characters after upgrading to 6.2.
987058	Exporting event raw JSON is slow and causes slowness in the management console.
1037376, 1041159	Error when logging out an Analyst user.
1030490, 1032990	Failure in saving file scan configuration with a Collector group.
1030678, 1016497	Error during the execution of REST API request.
1044790, 1041155	Failure in saving an integration with an action.

Bug ID	Description
1015068, 1036804	Failure in executing some procedures using Rest API.
1041471, 1007961	Failure when importing organizations.
1027850, 1029342	Security events are not sent to the management console.
1026575, 1041158	Error when saving threat hunting query via REST API.
1028502, 1036803, 982543	Moving collector via REST API fails due to missing account name.
989461, 1005495	Collector upgrade fails.
982341, 985548	Failure in testing the firewall connector.
998216, 999110	Group assignment of an exception is missing after the exception is edited.
1048422	Unable to sccess system events.
1025494	Clear Erased task failure on delete audit records.
965878, 1036470	Issue related to the use of wildcard in alert key path in exceptions.
998398, 990232	Parsing issue related to Taxii.
1002993, 1000040	User preferences might cause system slowness.
1043710, 1040039	
1045803, 1012229	Failure in creating exceptions due to system overload.

Refer to Central Manager - Build 6.2.1.0111 on page 15 for a list of new features and changes for this build.

Central Manager - Build 6.2.0.0451

Bug ID	Description
1026062, 1031933	The Details pane does not show for some nodes or edges in the investigation view.
1031422	Missing information in stacks view.
1027529, 1029378, 1033544, 1029339	Error of invalid characters in organization name when trying to extend license for an organization after the upgrade to 6.2.

Refer to Central Manager - Build 6.2.0.0451 on page 16 for a list of new features and changes for this build.

Central Manager - Build 6.2.0.0440

Bug ID	Description
1011247, 1007511	Issue with Graph view.
1014463	Loading error when configuring client certificate for syslog.

Central Manager - GA Build 6.2.0.0436

Bug ID	Description
N/A	No validation for organization registration passwords.
915698	Wrong message when you click "Block address on Firewall" in the Investigation View.
915266	Viewer users can save a rule under Communication Control.
911996	Cannot add an application to two policies in Application Control.
889939	Investigation View graph presentation error when zooming to fit.
889942	Cannot see the buttons at the bottom when adding process exclusions in Investigation View.
889945	Collector version is not displayed under "Update Collector Version".
964773	Incorrect event association for devices with the same name.
N/A	Rest API option should be disabled during LDAP and SAML user configuration.

Refer to GA build (Central Manager - 6.2.0.0436, Core - Build 6.0.1.0578, Threat Hunting Repository - Build 6.2.0.0427) on page 17 for a list of new features and changes for this build.

Known issues

The following issues have been identified in 6.2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
1136128	A reboot is required to upgrade Collector version 5.2.5.0051 or 5.2.5.0052 to a newer build.
1014223	Unable to reset a two-factor authentication token for LDAP users.
952675	FortiSandbox integration test does not work as expected.
946017	Event Graph is not displayed properly in Firefox browser.
N/A	No support for organization-specific Aggregators in multi-tenancy setups.
1001334	Security events fully covered by an exception retains the full coverage indication icon even after new uncovered raw data items come in.
802912, 818332	User cannot use LDAP credentials to authenticate for REST API.
938512, 993729	LDAP authentication fails sporadically.
939481	In some cases, the communication control feature does not work due to unforeseen technical issues. **Workaround:**Troubleshoot and upgrade the Central Manager.
954553, 969494	Some event log entries in threat hunting display logged event values in incorrect logged event fields .
1000559	In Fortinet pre-defined applications, selecting a group checkbox selects only the first page.
987989	Application Control and Exclusion validation error messages regarding the usage of wildcards in the application name/path are not accurate.
996156	In Fortinet pre-defined applications, application name is missing from audit logs.
973252	Collectors with a deleted registration password are marked as expired.
988884	Incorrect threat hunting profile order of Fortinet pre-defined application profiles.
989392	REST API file scan: unclear error when "organization" is not sent in multi-tenancy setup.
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.

Bug ID	Description
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*.
994348	Log does not contain concrete helpful errors for API.
994364	The API for moving a Collector to a high security group can be triggered when the Collector has already been moved.
988393	Spaces should not be allowed at the beginning or end of exclusion list names.
989722	Missing Fortinet pre-defined applications fields in REST API.
988385	Cannot close the Import/Export Exclusion window using the *Close* (*X*) button.
985337	Incorrect path length display in error message when importing or exporting exclusions.
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.

733548	**Component Backward Compatibility:** v6.0 Central Manager has the following limitations in backward compatibility:
	• Collectors from older versions are supported with limited functionality. Some new features introduced in later versions may not be available.
	• Only the following Core versions are supported:
	  • 6.0.1 builds
	  • 5.2.0.4189 or later
	  • 5.2.2.2043 or later

915698	In the Investigation View, the message is wrong in the *Block address on firewall* window when you click *Firewall Block*.
914792	Unarchiving all events in large environments might cause the Central Manager to malfunction. **Workaround**: Filter events before unarchiving to reduce unarchive size.
912000	Failure to edit a Hoster user when a local user has the same name.
907362	Remote shell does not work on Windows XP and Windows Server 2003.
894384	In Threat Hunting, clicking *Retrieve Target File* for "File Rename" events retrieves the old file name instead of the renamed one.
892109	Unable to filter by empty registry names in facets in Threat Hunting.
889422	Remote shell connection cannot be established if collector connects to aggregator via a proxy server.

Bug ID	Description
840669	Rest API is not enforcing users roles permissions.
837038	Application Control cannot remove multiple tags in one action.
833152	Raw data IDs appearing in the Collector tray and Event Viewer may differ.
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
802912	Rest API does not support LDAP users.
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.
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.
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	On Linux, threat hunting exclusions only work in kernel space mode, not in user space mode.
759573	Collector upgrade via custom installer requires password.
757253	FortiEDR Connect cannot be used to run commands that are user-interactive.
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.

Bug ID	Description
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.
733598	Safari 11.1 on macOS malfunctions when viewing events.
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 Centervia 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 V5.2 before upgrading it to V6.0.

www.fortinet.com

Copyright© 2025 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.