Release Notes

FortiEDR 7.0.0

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

March 02, 2026
FortiEDR 7.0.0 Release Notes
63-700-1031405-20260302

TABLE OF CONTENTS

Change log

Date	Change Description
2025-01-29	Initial release.
2025-02-04	Added Protection for cloud workloads on page 8.
2025-02-24	Updated Changes to the workflow of events on page 14.
2025-03-04	• Added Resolved issues on page 24 and Known issues on page 26. • Updated FortiEDR 7.0.0 Release Notes on page 5.
2025-03-07	Added Upgrade information on page 22.
2025-03-12	Updated Upgrade information on page 22.
2025-04-28	Added *Central Manager - Build 7.0.4.0100*.
2025-05-15	Added Central Manager - Build 7.0.4.0050 on page 6 and obsoleted *Central Manager - Build 7.0.4.0100*.
2025-07-07	Deleted ticket 829531 from Known issues on page 26.
2025-10-24	Updated Changes to the workflow of events on page 14.
2026-02-02	Updated Security posture indicator for Windows and macOS endpoints on page 18.

FortiEDR 7.0.0 Release Notes

This document provides information about FortiEDR version 7.0.0.

Version history

	Central Manager	Core	Threat Hunting Repository
2025-03-31	Build 7.0.4.0050		
2025-01-29 (GA)	Build 7.0.3.0027	Build 6.0.1.0665	Build 7.0.0.0485

What's new

This section identifies new features and enhancements available with FortiEDR 7.0.0.

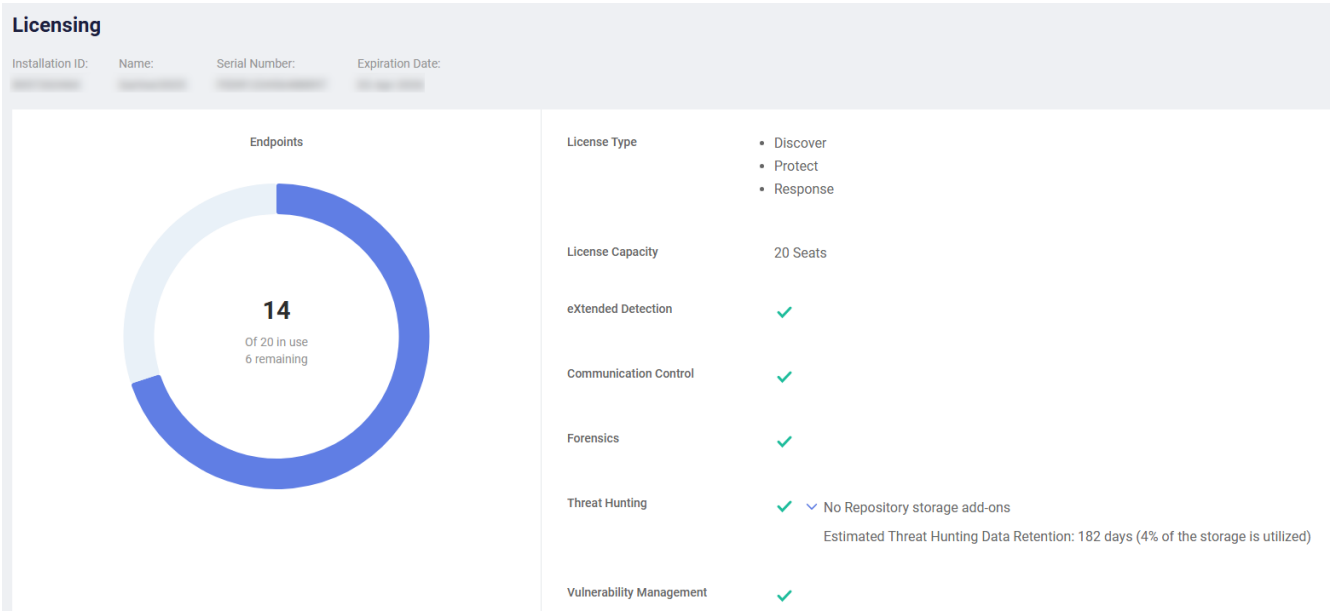
Refer to Resolved issues on page 24 for a list of resolved issues for each build.

Central Manager - Build 7.0.4.0050

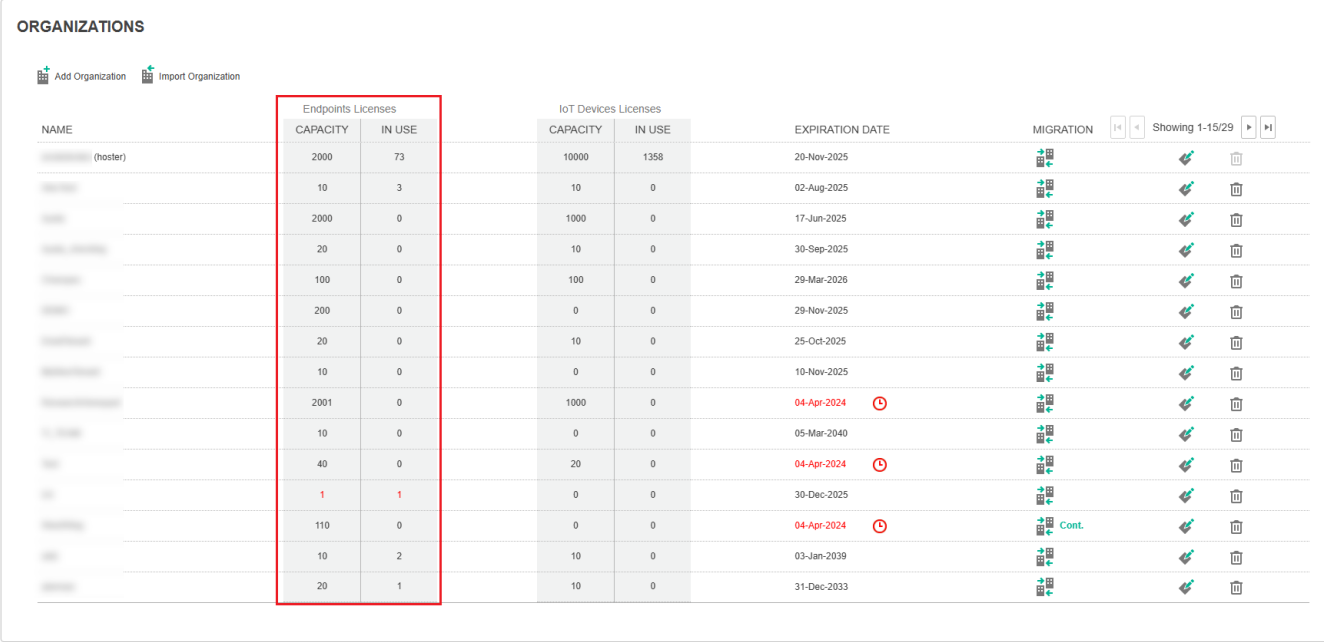
This build includes the following new feature:

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.



Refer to Central Manager - Build 7.0.4.0050 on page 24 for a list of resolved issues for this build.

GA build

The FortiEDR 7.0.0 GA build includes the following features, enhancements, and changes:

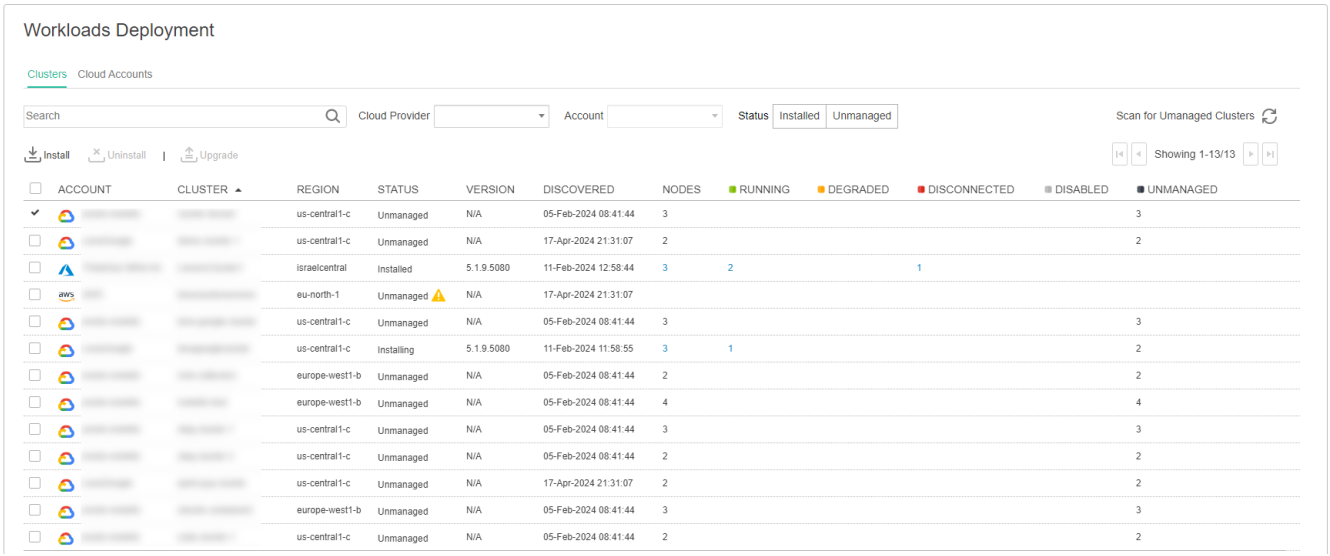
Refer to Central Manager - GA Build 7.0.0.0027 on page 25 for a list of resolved issues for this build.

Protection for cloud workloads

FortiEDR 7.0.0 adds support for cloud workloads protection to secure instances on the following cloud platforms with a new node Collector:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

In the *Administration > Workloads Deployment* page, you can connect your AWS, Azure, and GCP accounts to FortiEDR and install the node Collector to desired clusters, which allows you to gain visibility into the clusters and the OS activity on the workloads.



The node Collectors can be managed in the *Inventory > Collector* page where you can filter Collectors by agent type (endpoint or node), assign them into Collector groups, and assign policies accordingly. The node Collector records events of the following categories:

- The following security events that happen on the nodes within the cluster or the workloads within the node:
  - *Malicious File Detected* rule under *Execution Prevention* policy
  - *Unconfirmed Executable - Executable File Failed Verification Test* rule under *Exfiltration Prevention* policy
- Activities performed by the workloads within the node as defined by the workload group's threat Hunting data collection profile which is associated with the workload groups you create. For example, if the assigned profile has *File Read* selected, any file read activity performed by the workload will be recorded.

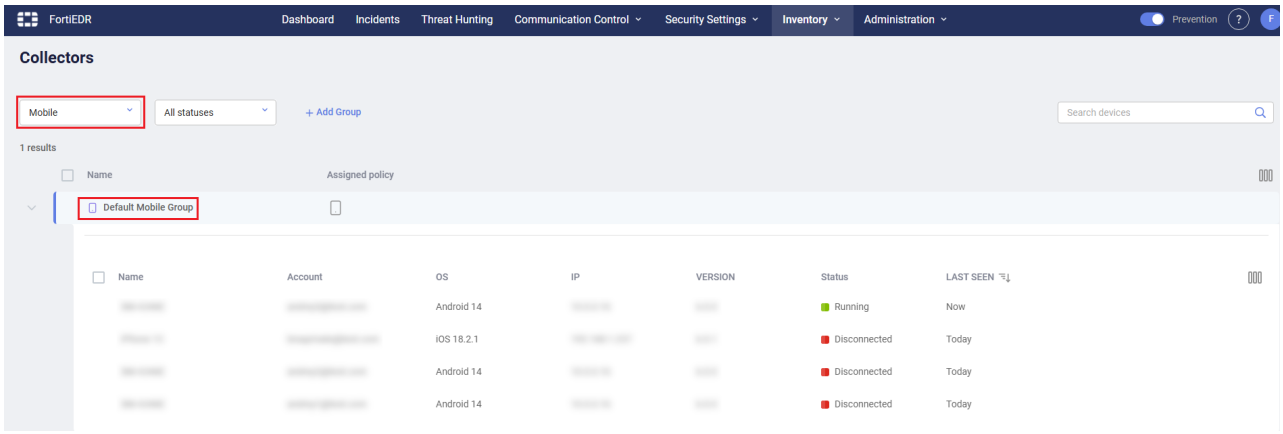
Protection for mobile devices

FortiEDR 7.0.0 adds protection for mobile devices (Android and iOS) with the following security features:

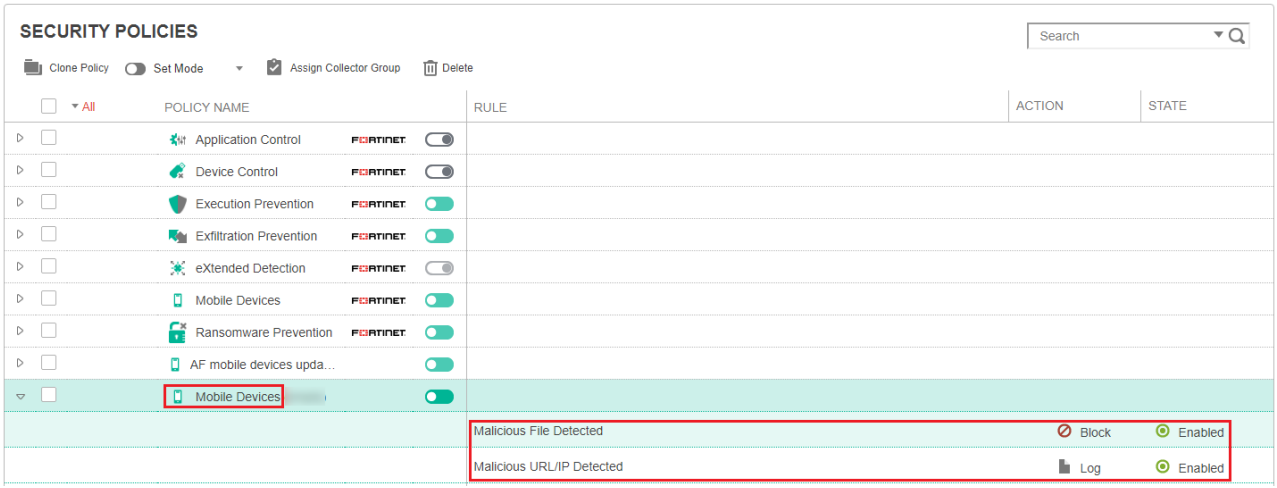
- **(Android only)** Real time and scheduled periodic scanning for potential vulnerabilities, such as malicious files or applications, rooted devices, outdated OS versions and kernel, lack of security update, or non-compliant configurations.
- **(Android only)** Application behavior and network traffic monitoring to detect mobile malware and data exfiltration. FortiEDR prevents the execution or installation of malicious files or applications based on the policy or application verdict.
- Automatic detection of malicious domains and IP addresses with built-in threat intelligence integration

To deploy FortiEDR mobile protection to mobile devices:

1. Ensure the organization has the mobile option enabled, which is required to enable all mobile-related pages and options in FortiEDR. See Step 2 – Defining or importing an organization.
2. Request a mobile Collector package in the *Administration > Licensing* page. See Requesting and obtaining a mobile installer.
3. View details of the mobile Collector and configure the group settings in the *Inventory > Collectors > Mobile* page. By default, all mobile Collectors are assigned to *Default Mobile Group*.

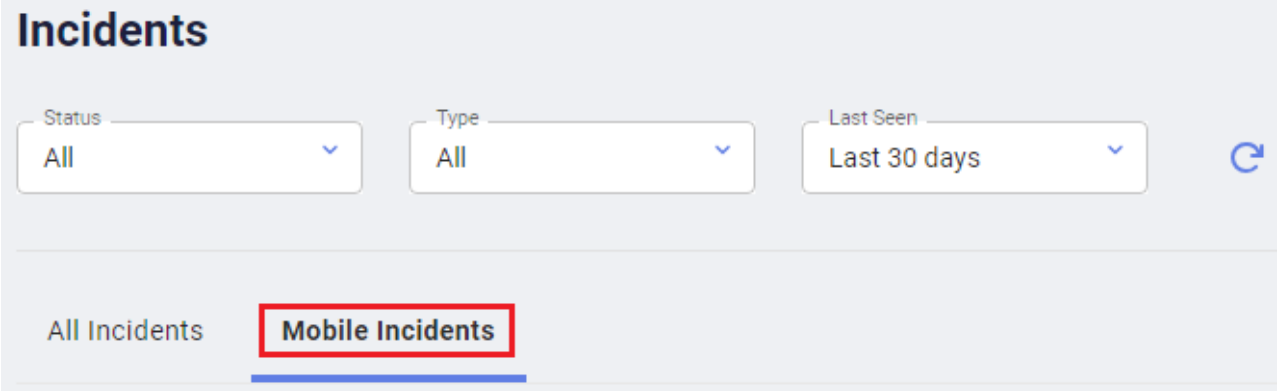


4. In the *Security Settings > Security Events > Security Policies* page, enable the *Mobile Devices* policy so that FortiEDR detects and prevents access to malicious URL and IP addresses from the mobile devices.



5. **(Optional)** Set up exclusions for mobile Collectors in the *Security Settings* > *Security Events* > *Exclusion Manager* page.

   FortiEDR then automatically detects malicious files, applications, domains , and IP addresses on the mobile devices and triggers a security event in such cases, which you can view in the *Incidents* > *Mobile Incidents* tab. You can handle the incidents directly or further investigate them.

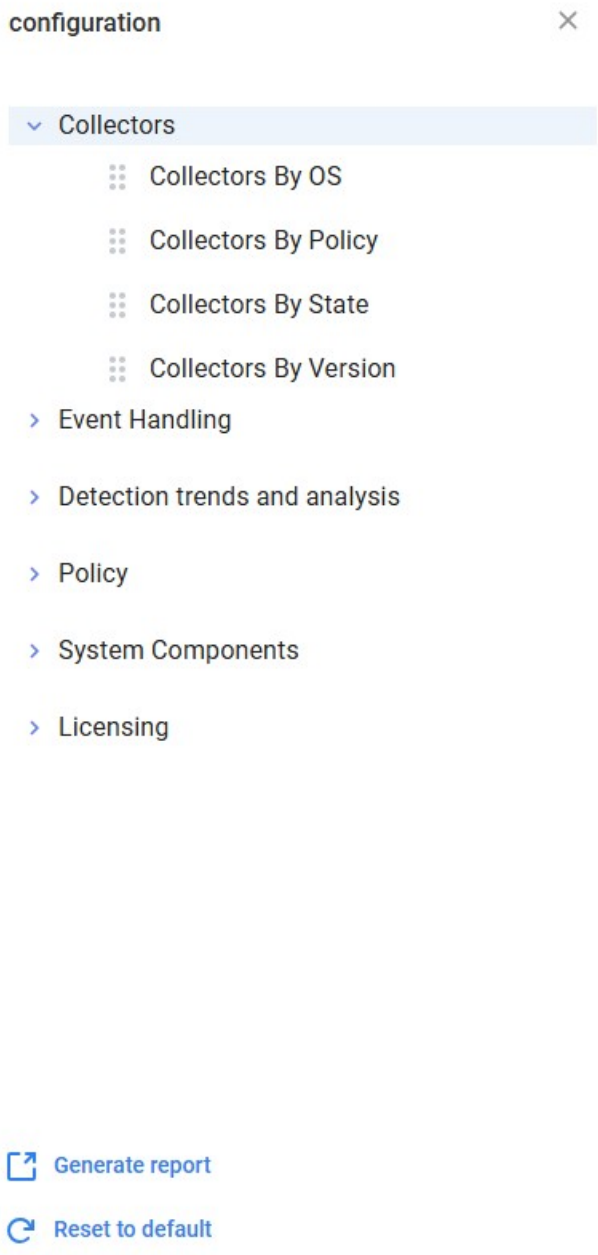


6. Configure periodic scan for mobile devices or groups. See File Scan.

Changes to the dashboard

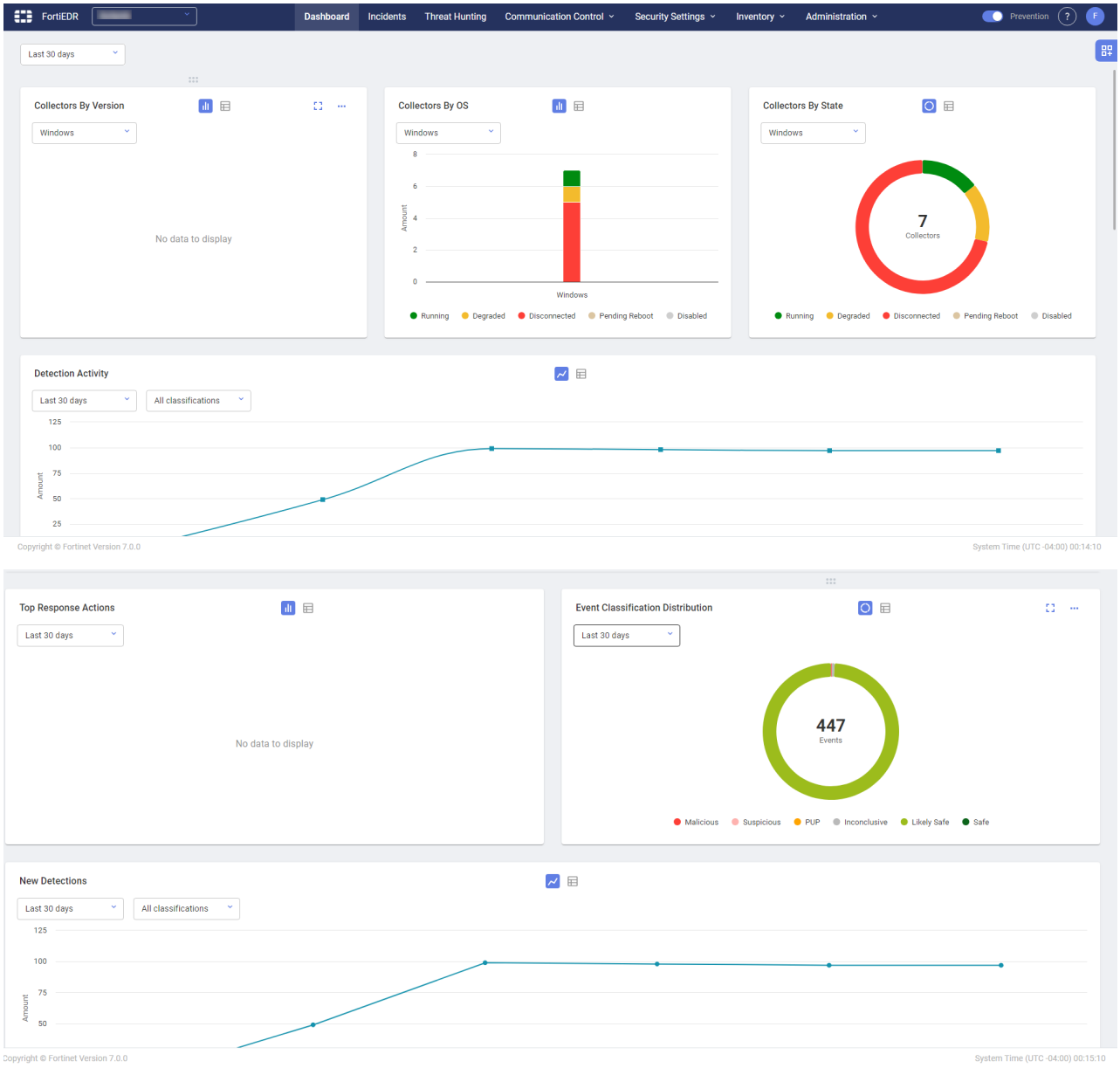
FortiEDR 7.0.0 includes major changes to the *Dashboard*:

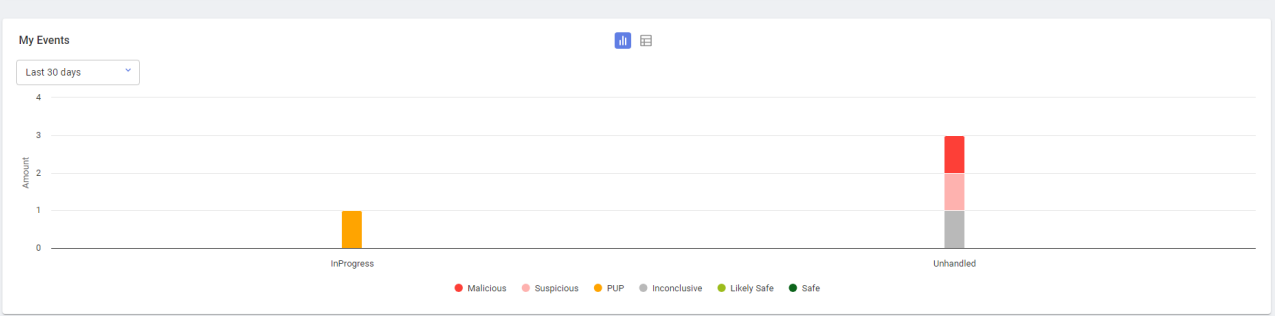
- New configuration side bar, which can be displayed using the button () at the top right corner. You can generate a report or reset the dashboard view using the respective buttons at the bottom.



- New, changed, removed widgets:

- The *Collectors* widget with three dimension views is now split into separate widgets for each dimension (OS, policy, state, version).
- New *Detection Activity*, *Top Response Actions*, *Event Classification Distribution*, and *New Detections* widgets.
- The *Events* widget changes from a pie chart to a graph with a date range configuration option at the top left corner. You can also change the view from graph to table using the icons at the top.
- The *Communication Control* widget is now under the *Policy* section.
- The *Most Targeted* widget is renamed *Top Affected Devices* under the *Event Handling* section.
- The *External Destinations* widget is removed.

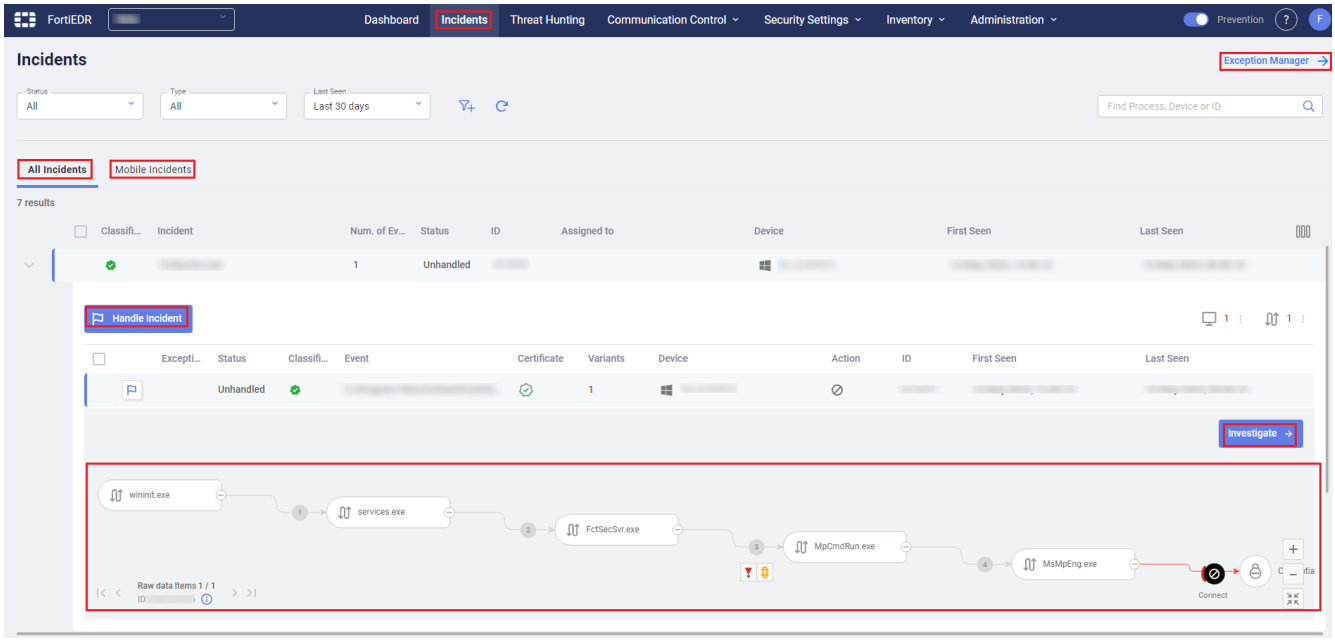




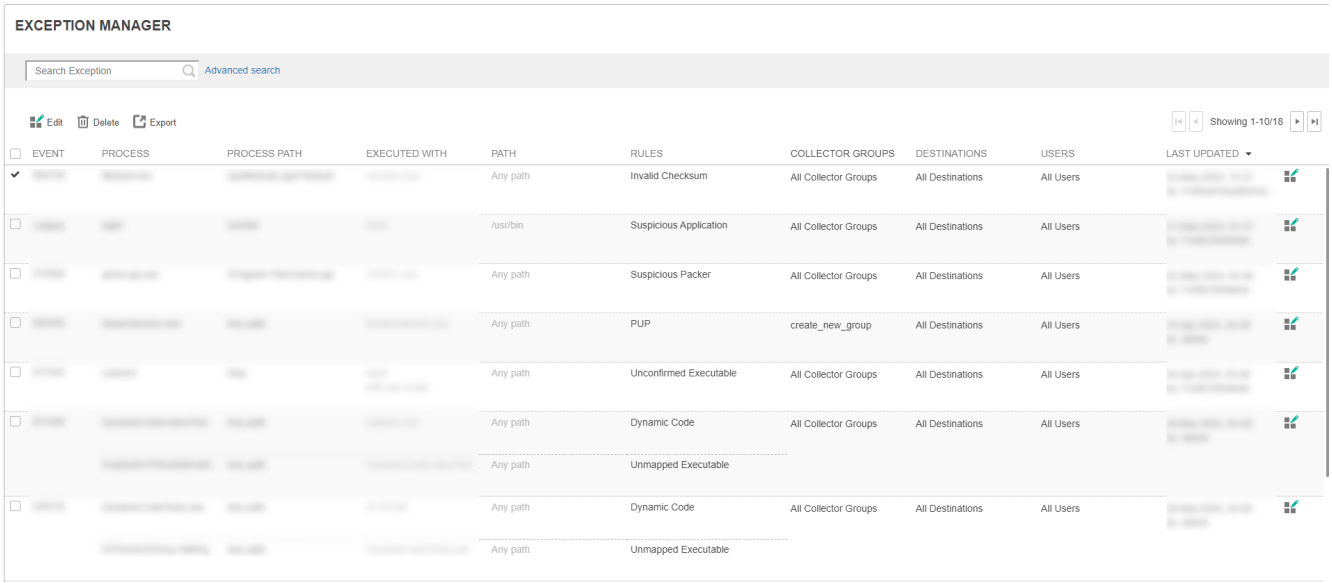
You can organize the widgets and place them to an ideal location by holding the drag and drop icon ( ) that appears when you hover over the top center of the widget.

Changes to the workflow of events

The *Event Viewer* tab is renamed *Incidents* with usability improvements, such as tabbed view of different types of incidents. Clicking on an incident displays the *Handle Incident* button and an embedded preview of the investigation view within the console where you can perform operations without opening a separate tab.

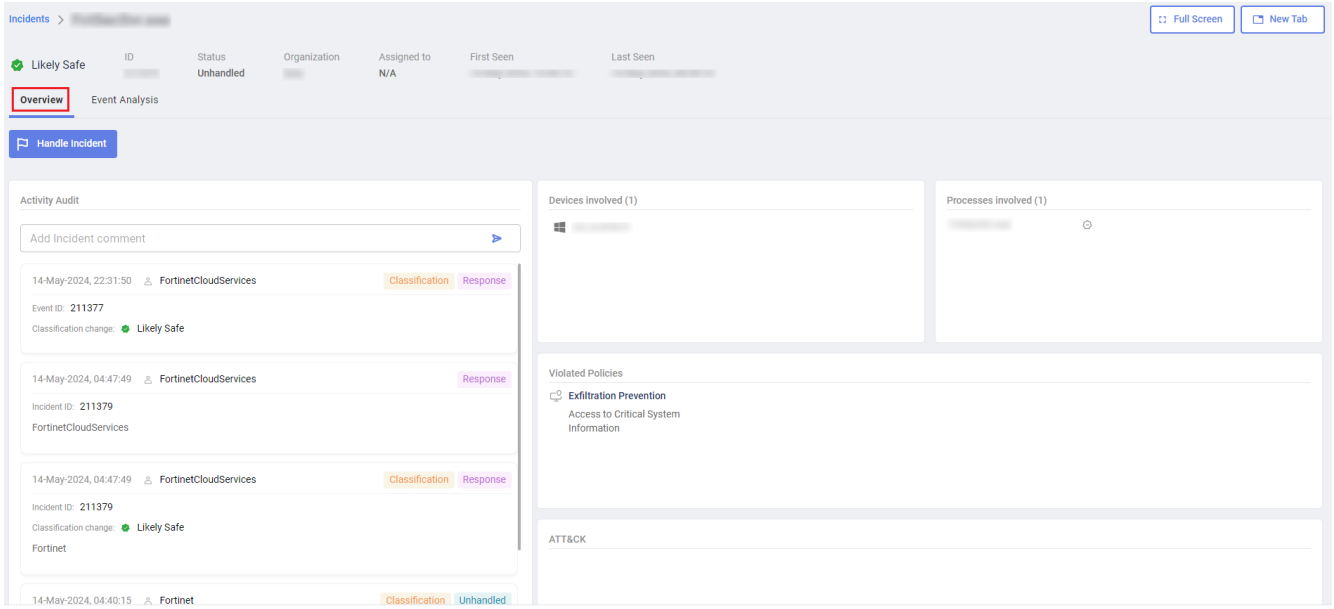


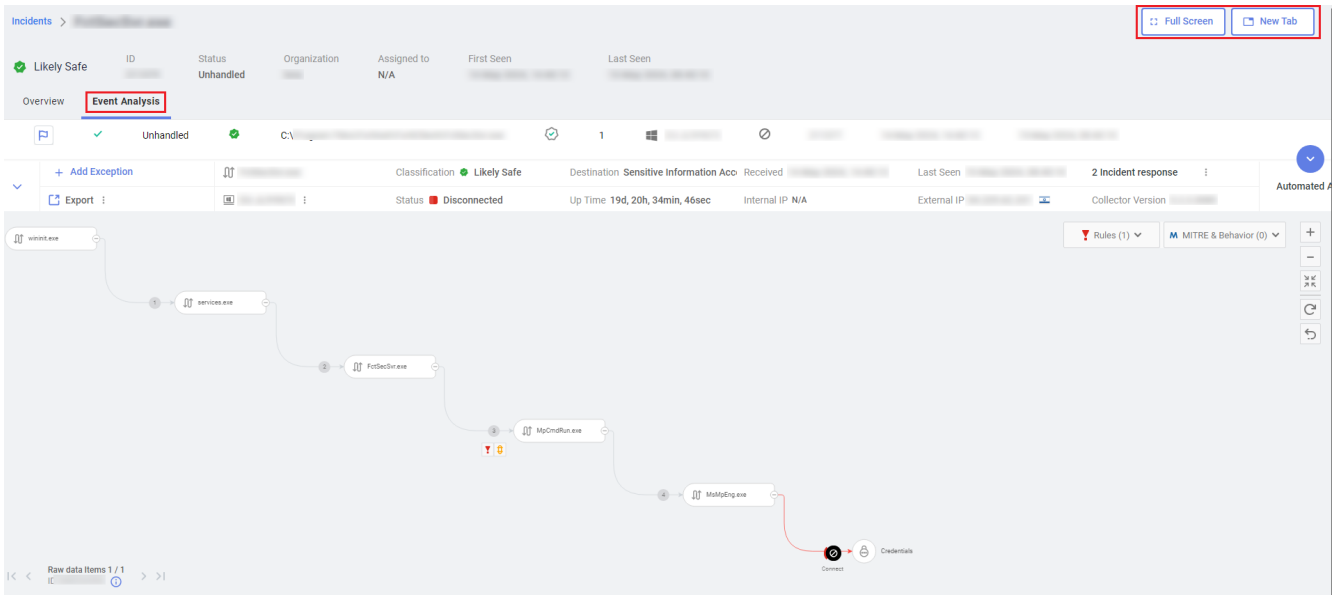
Clicking the *Exception Manager* button redirects you to the *Exception Manager* page where you can manage exceptions.



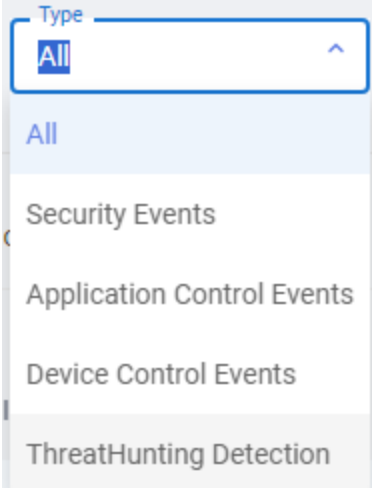
Clicking the *Investigate* button opens the full investigation view within the console with an *Overview* tab that shows the audit history and policy violation information, etc, and the *Event Analysis* tab that shows the full

investigation view. You can also switch to full screen or open the investigation view in a new tab using the buttons at the top-right corner.





To filter events by type, such as application control events or device control events, use the *Type* dropdown list.



To assign an incident, select the incident and click the *Assign* button ( ).

To filter incidents with a custom filter, click the *Filter* button ( ).

You can no longer archive an event (or incident). For upgraded systems, archived events from earlier versions will be shown as *Handled* in 7.0.

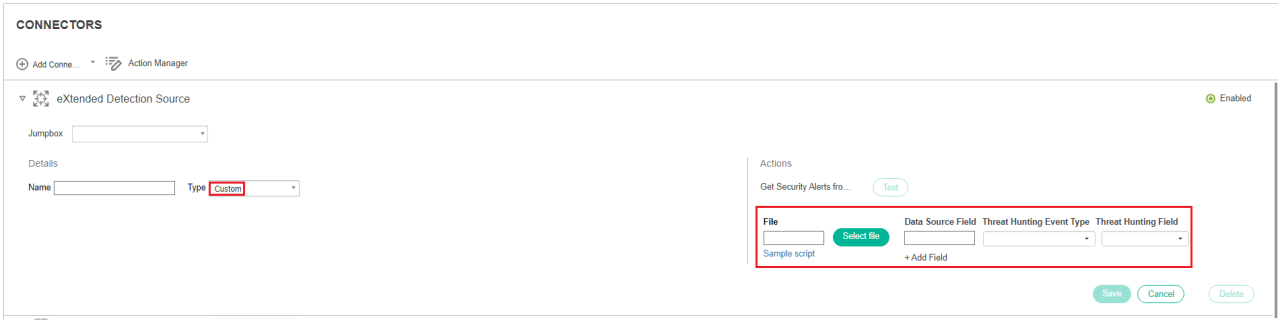
For better performance, the incidents filter is now limited to a time rang of up to 30 days. Same for audit trail: you can now only download the audit trail report with a time range of up to 30 days.

eXtended detection with custom external systems

FortiEDR 7.0.0 adds support for custom external systems as eXtended detection source when you create an extended detection connector in the *Administration > Integrations* page.

To create an extended detection connector for a custom external system:

1. In the *Administration > Integrations* page, click the *Add Connector* button and select *eXtended Detection Source* in the *Connectors* dropdown list.
2. Select the FortiEDR Jumpbox that will communicate with the external system.
3. Specify the name to identify the external system.
4. select *Custom* in the *Type* dropdown list. The following displays:

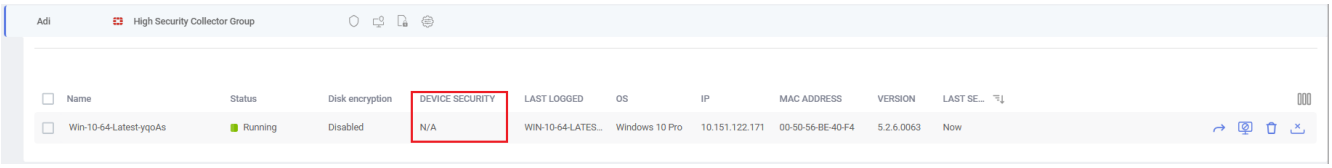


5. In the *Actions* section, upload a script file that contains all the authentication details for the external system and the query for FortiEDR to pull data from the system. Use the sample script as a starting point to build your own script by replacing all the values with those for your system.
6. Specify the name of the data source field in the external system for FortiEDR to correlate with. You can add fields as needed.
7. For each data source field, select the corresponding *Threat Hunting Event Type* and *Threat Hunting Field* for FortiEDR to correlate data with.
8. Click *Save*.

Security posture indicator for Windows and macOS endpoints

The *Inventory* > *Collectors* page includes the new *DEVICE SECURITY* column which provides insights into the security posture of Windows and macOS endpoints based on OS-level configurations.

To show or hide the column, use the *Choose Columns* button ( ) to the right of the group.



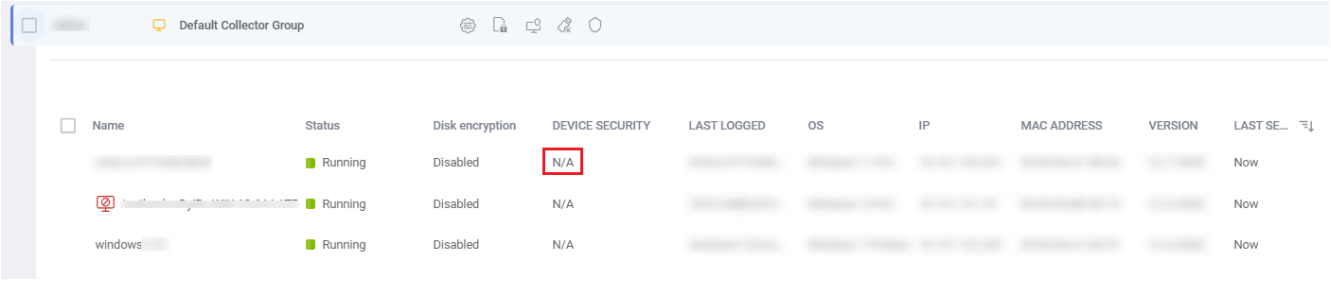
The device is marked as compliant if two or more of the following criteria are met:

The device security compliance status is informational and has no impact on FortiEDR protection effectiveness. Endpoints are always protected by FortiEDR, regardless of the compliance status.

Windows	macOS
• **Security Centre**—FortiEDR is registered as anti-virus and threat protection agents in *Administration* > *Settings* > *Windows Security Center*. • **User Account Control (UAC)**—Windows User Account Control is enabled to protect the operating system from unauthorized changes. • **Windows updates**—The latest Windows update has been installed.	• **Gatekeeper Status**—Gatekeeper is enabled to ensure that only trusted software runs on the Mac. • **System Integrity Protection (SIP) Status**—System Integrity Protection is enabled to help protect the Mac from malicious software.

To view compliance details of each criteria, hover over the status text.

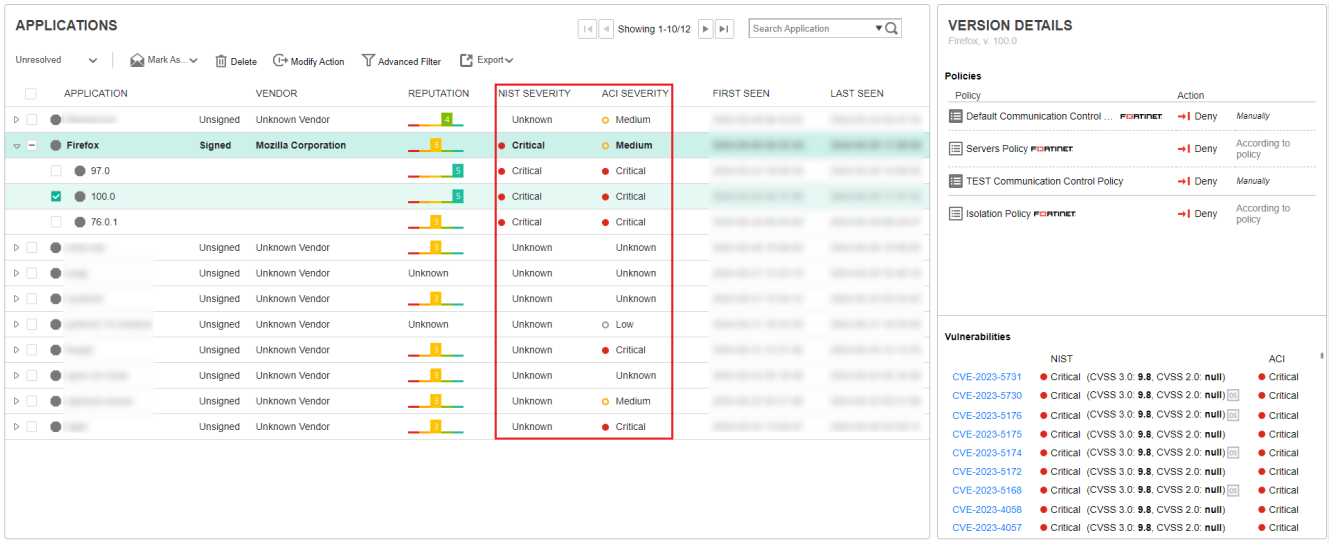
Endpoints that are not in connected state show *N/A* in the *DEVICE SECURITY* column.



Visibility into external attack surface with FortiRecon integration

FortiEDR 7.0.0 adds integration with FortiRecon for comprehensive visibility into the organization's external attack surface so that analysts can prioritize security alerts and incidents based on risk factors such as severity of vulnerabilities, relevance of threat intelligence feeds, and severity of affected endpoints, ensuring that efforts are focused on addressing the most significant risks to the organization.

The *Communication Control* > *Applications* page replaces the *Vulnerability* column with the following two Severity columns with severity ratings for each application and version:



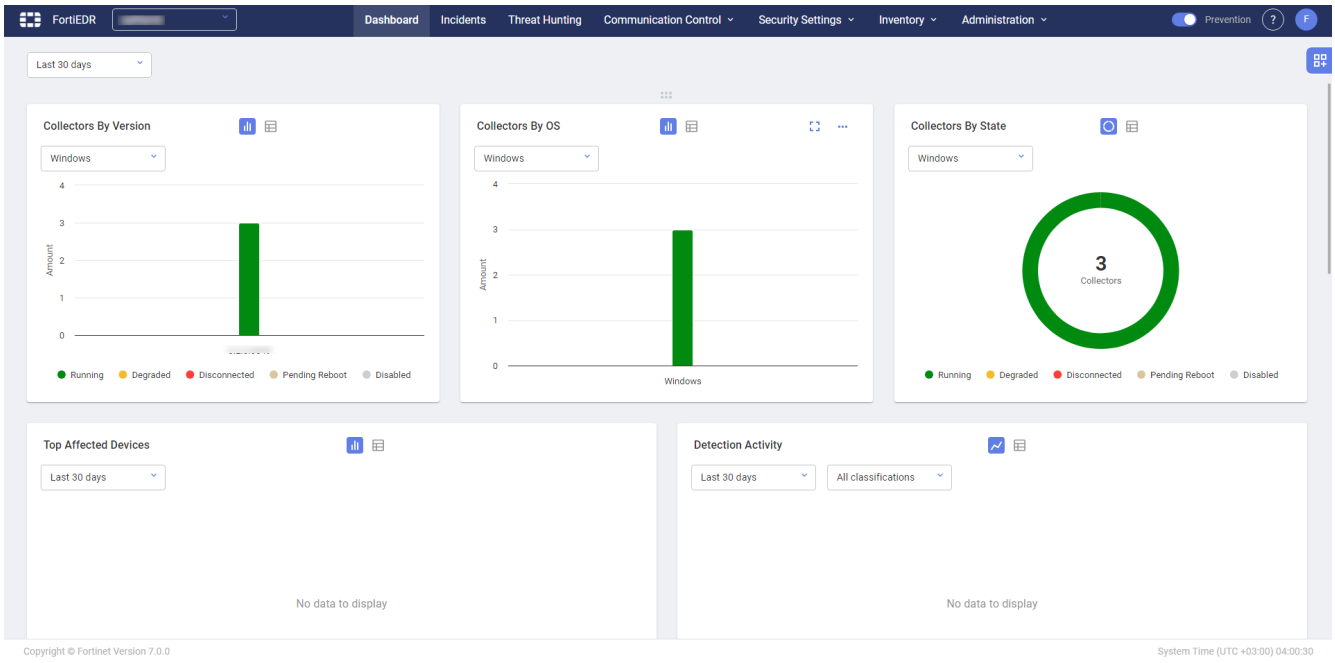
- NIST Severity—Rating provided by FortiEDR's vulnerability scoring system leveraging the NIST Cybersecurity Framework.
- ACI Severity—Adversary Centric Intelligence (ACI) rating provided by FortiRecon leveraging FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.

FortiEDR categories vulnerabilities into the following categories based on National Vulnerability Database (NVD) severity ratings:

- Unknown
- Low
- Medium
- High
- Critical

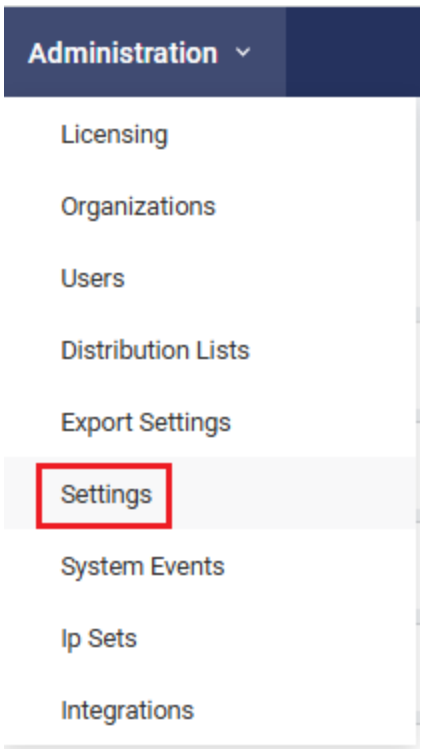
New look and feel of the Central Manager console

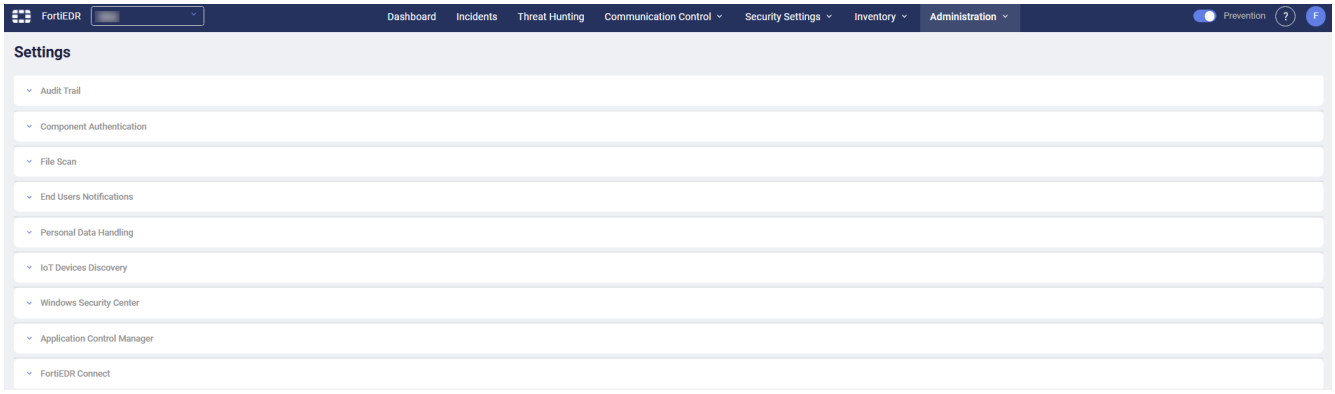
FortiEDR 7.0.0 Central Manager console adopts a sleeker and more modern look and feel with a new color scheme.



Administration > Tools page renamed *Administration > Settings*

The *Administration* > *Tools* page is renamed *Administration > Settings* with UI improvements.


Administration
Licensing
Organizations
Users
Distribution Lists
Export Settings
Settings
System Events
Ip Sets
Integrations


FortiEDR
Dashboard
Incidents
Threat Hunting
Communication Control
Security Settings
Inventory
Administration
Prevention
Settings
Audit Trail
Component Authentication
File Scan
End Users Notifications
Personal Data Handling
IoT Devices Discovery
Windows Security Center
Application Control Manager
FortiEDR Connect

Upgrade information

FortiEDR 7.0 Central Manager supports upgrade from 6.0 or later.

To upgrade your FortiEDR environment to 7.0, you must first obtain approval from Fortinet Support by creating a FortiCare ticket.

Supported browsers

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

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

Resolved issues

The following issues have been fixed in FortiEDR 7.0.0. For inquires about a particular bug, please contact Customer Service & Support.

Central Manager - Build 7.0.4.0050

Bug ID	Description
1118190	Mobile device are not included in the total number of endpoints during license registration.
1108114	Issue with assigning incidents to SAML or LDAP users.
1134239	Archived events are not displayed as expected after the upgrade to 7.0.
1111573	Update number of shards task causes many registration requests.
1111339	Threat hunting displays error "Query parsing failed).
1126848	Linux Collector registration failure.
1125649	Misleading message about FortiEDR license expiring.
1119548	License information is not shown.
1053068, 1113772	Incident page display issues.
1112589	Issue related to Keystore in upgrade step.
1117650, 1108439	Collector isolation issue.
1117172	(REST API) Issue with Update Organization with "endpointsAllocated".
1115524	Calculation of diff application control OOTB.
1114187	'X' button does not clear the registration password in the revoke registration password window.
1111822	UI shows the device as isolated when it is not.
1111786	App Control configuration sometimes does not reach the Collector.
1111225	Issue with updating application properties.
1135364	Settings page is blank.
1135978	IoT "Ad hoc network discovery" shows wrong Collector numbers and / or does not

Bug ID	Description
	show at all.
1139614	Failure in running ad hoc scan.
1126687	Upgrading to to 7.0 is slow.
1113774	RabbitMQ password update issue.

Refer to Central Manager - Build 7.0.4.0050 on page 6 for a list of new features and enhancements for this build.

Central Manager - GA Build 7.0.0.0027

Bug ID	Description
802912, 818332	User cannot use LDAP credentials to authenticate for REST API.
840669	Rest API is not enforcing users roles permissions.
889422	Remote shell connection cannot be established if collector connects to aggregator via a proxy server.
984125, 992151	Console latency caused by an internal handling of muting security events.
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.
988393	Spaces should not be allowed at the beginning or end of exclusion list names.
988394	Exclusion List name validation - Error message text display issue.
985337	Incorrect path length display in error message when importing or exporting exclusions.
989722	Missing Fortinet pre-defined applications fields in REST API.
988385	Cannot close the Import/Export Exclusion window using the *Close* (*X*) button.

Refer to GA build on page 7 for a list of new features, enhancements, and changes for this build. Refer to Known issues on page 26 for a list of known issues for this build.

Known issues

The following issues have been identified in 7.0.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

New known issues for 7.0.0

Description	Bug ID
1048824	Dashboard time range filter does not work.
1050795	No message to explain why the user cannot set the UI to prevention mode when all policies are in simulation mode.
1050797	Clicking on *Collectors by version* in Dashboard view does not lead to the Collectors Inventory view.
1051326	Device security should be N/A for disconnected devices.

Existing known issues from 6.2 or earlier

Bug ID	Description
733557	A Collector may fail to install or upgrade on old Windows 7 and Server 2008 devices that cannot decrypt strong ciphers with which FortiEDR Collector is signed. **Workaround:** Patch Windows with Microsoft KB that provides SHA-256 code sign support.
733559	Some AV Products, including Windows Defender and some versions of FortiClient, require that their realtime protection be disabled in order to be installed alongside a FortiEDR Collector. This is the result of FortiEDR registration as an antivirus (AV) in the Microsoft Security Center that was introduced in V4.0. Although there is no need for more than a single AV product to be installed on a device, FortiEDR can be smoothly installed, even if there is another AV already running. However, there are some other products whose installation fails when there are other AV products already registered. **Workaround:** Disable realtime protection on the other product, or remove FortiEDR's AV registration with Microsoft Security Centervia UI.

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

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

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

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

www.fortinet.com