FORTINET

Release Notes

FortiEDR 5.2.1

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

February 27, 2025
FortiEDR 5.2.1 Release Notes
63-521-841857-20250227

TABLE OF CONTENTS

Change log

Date	Change Description
2022-09-20	Initial release of 5.2.1.
2022-11-02	Added ticket 837796 to *Known issues*.
2022-11-22	Added ticket 772449 to *Known issues*.
2022-12-13	Added Central Manager build 2709 to *Resolved issues*.
2023-01-26	Added Central Manager build 2800 to *Resolved issues*.
2023-05-30	Deleted a duplicate entry in *Known issues*.
2023-05-31	Added ticket 889422 to *Known issues*.
2023-08-16	Added a note in the following topics to clarify that FortiEDR 5.2.1 is not recommended for production: • FortiEDR 5.2.1 Release Notes on page 5 • Upgrade information on page 8
2023-11-20	Added Supported browsers on page 10.
2024-03-27	Updated Upgrade information on page 8.
2024-06-05	Updated Upgrade information on page 8.
2024-08-22	Added ticket 1001334 to Known issues on page 12.
2025-02-27	Updated the description of ticket 765648 in Known issues on page 12.

FortiEDR 5.2.1 Release Notes

This document provides information about FortiEDR version 5.2.1.

FortiEDR 5.2.1 is not recommended for production. Use FortiEDR 6.0 instead.

Version history

	Central Manager	Threat Hunting Repository	Core
2022-09-20	Build 2569	Build 2537	Build 5.2.0.2139
2022-12-13	Build 2709		
2023-01-26	Build 2800		

What's new

This section identifies new features and enhancements available with FortiEDR 5.2.1.

If you upgrade from FortiEDR 5.0.0 to 5.2.1, see also the following for additional new features introduced in FortiEDR 5.1.0 and 5.2.0:

- FortiEDR 5.1.0 what's new
- FortiEDR 5.2.0 what's new

Enhancements to user management and access control

FortiEDR 5.2.1 adds more predefined user roles for better access control and enhances the user management process.

Choose from the following roles when creating users or defining LDAP and SAML authentication. For roles that are not authorized for certain tasks or devices, FortiEDR hides or disables the related menu items, items in content pages, and buttons.

Role	New/Changed?	Description
Admin	No change in privilege but no more distinction of Local Admin and Admin in multi-tenancy: Admin access to one or all organizations is now defined in the *Organization* field.	Highest-level super user that can perform all operations in the FortiEDR Central Manager console for the organization.
Senior Analyst	Renamed from User	Analysts supervisor who can define security policies in addition to all the actions that can be performed by an Analyst.
Analyst	New	SOC/MDR service analyst who can perform actions as required in the day-to-day activities of handling events.
IT	New	IT staff who can define settings related to the FortiEDR integration with the customer echo system.
Read-Only	New	Basic role with read-only access to all functions except system configuration.

For Multi-tenancy (Organizations) systems, you can also configure the user with role-specific access to all organizations.

In addition to the roles changes, enhancements are also made in the user creation and editing process and LDAP and SAML authentication settings.

XDR extended data lakes support: Google Security Command Center and Amazon GuardDuty

FortiEDR 5.2.1 extends FortiXDR detection and response with the following new data lakes:

- Google Security Command Center (Google SCC)
- Amazon (AWS) GuradDuty

FortiXDR now automatically collects activity logs from the two data lakes. By leveraging Fortinet Cloud Services (FCS) advanced analytics, artificial intelligence, and correlation capabilities, FortiXDR can generate fine-grained alerts based on Google SCC and AWS GuardDuty logs. This new capability is license-dependent.

Zero Trust incident response capabilities

FortiEDR 5.2.1 extends FortiXDR detection and response with new out-of-the-box capability to tag a device as Zero Trust device with FortiClient EMS using a new out-of-the-box Identity Management Connector.

User access incident response capabilities

FortiEDR 5.2.1 extends FortiXDR response actions with the new out-of-the-box user access-related capabilities of resetting a user's password and disabling a user's account using the new User Access Connector support Active Directory.

Licensing restrictions removal for *Forensics > Events*

FortiEDR 5.2.1 no longer requires a specific type of license to access the *Forensics* > *Events* page. All user roles with Forensics permission can now access the *Forensics* > *Events* page, regardless of the license type.

Threat Hunting scheduled queries trigger Incident Response actions

FortiEDR 5.2.1 allows you to enable incident response actions upon custom detection that Threat Hunting scheduled queries rules trigger.

New time filter in Event Viewer

You can now filter security events by time to narrow down the results to a certain period, such as the last 7 days. Use the time filter to handle events more efficiently.

FortiGate Connector supports virtual domains

In FortiEDR 5.2.1, you can integrate incident response actions with FortiGate and FortiManager virtual domains (VDOMs).

Upgrade information

You can only upgrade from FortiEDR 5.0 or 5.2.0 to 5.2.1. Fortinet recommends that you skip FortiEDR 5.2.1 and upgrade to FortiEDR 6.0 directly because FortiEDR 5.2.1 is not recommended for production.

The following section highlights operational changes that administrators should be aware of in FortiEDR 5.2.1.

User access changes

When upgrading to FortiEDR 5.2.1 from 5.0 or 5.2.0, be aware of the following behavior changes in user access management in the *ADMINISTRATION > USERS* page:

- The user role is renamed Senior Analyst with additional access to the following pages or sections under *ADMINISTRATION*:
  - *TOOLS > FILE SCAN*
  - *TOOLS > IOT*
  - *Tools > FORTIEDR CONNECT*
  - *IP SETS*
- Admin users no longer have access to custom scripts by default. You must manually select the *Custom script* checkbox when creating the Admin user or assigning groups for the Admin role in the *LDAP AUTHENTICATION* and *SAML AUTHENTICATION* sections.

  For existing Admin users created in previous versions, edit the user or LDAP and SAML group to enable the *Custom script* checkbox. Otherwise, the Admin user will not be able to see the *Action Manager* button in the Integrations page for uploading custom scripts.
- For multi-tenancy environments, existing SAML and LDAP Admin users created in previous versions with access to all organizations will only have access to the default organization after the upgrade to 5.2.1.

  If your multi-tenancy environment has SAML users only, you will need to reconfigure the SAML users and roles after the upgrade:
  - For environments with a local admin user, follow the instructions in SAML authentication.
  - For environments without a local admin user, contact Fortinet support for assistance with the reconfiguration.
- To grant an Admin user access to one or all organizations in multi-tenancy environments:
  - **Local users**
    i. Select *Hoster View* in the *Organization* dropdown list at the top left.
    ii. Select the organization or *All organizations* in the *Organization* list.
    iii. Select *Admin* in the *Role* list.

    See the FortiEDR Administration Guide for more details.
  - **LDAP and SAML users**
    i. In the *Organization* dropdown list at the top left, select the organization that you want to grant the user

access or select *Hoster View* if you want to grant the user access to all organizations.

ii. Select *Admin* in the *Role* list for the group when you configure LDAP or SAML users.

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 2800

Bug ID	Description
827526	Playbook view pagination issue.

Central Manager - Build 2709

Bug ID	Description
848562	Add restrictions to password policy.
841708	Rest API retrieval issue.
842051	Red dot in Forensics showing on the wrong processes.
843217	Threat Hunting scheduled query does not trigger event.
848561	Issue with "list events" API.
848563	Add validation of organization names.

Central Manager - Build 2569

Bug ID	Description
807230	FortiEDR Connect cannot be used with 32-bit devices.
773610	Execution Prevention Events are missing Device users.
734594	Linux Threat Hunting Activity Events are missing the process hash.
734309	NGAV scan of specific Collectors/Groups scan all Collectors.

Known issues

The following issues have been identified in 5.2.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

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.
889422	Remote shell connection cannot be established if collector connects to aggregator via a proxy server.
834342 824506	New integrations (Google SCC and User Access) require the use of Core build 5.2.0.2139 or above.
840669	Rest API is not enforcing users roles permissions.
839706	Custom connectors and actions cannot be viewed by a user without checking the “Custom script” checkbox for that user.
837796	In multi-tenant environments, SAML/LDAP authentication of Admin users with All organizations (hoster) scope provides permissions only to the default organization after the upgrade from 5.0 or 5.2.0 to 5.2.1. **Workaround**: Reconfigure SAML/LDAP in hoster view after upgrading to 5.2.1.
837675	No on-premise support.
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
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.
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.

Bug ID	Description
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.
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.
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 V5.0.3 before upgrading it to V5.2.

Bug ID	Description
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.

www.fortinet.com