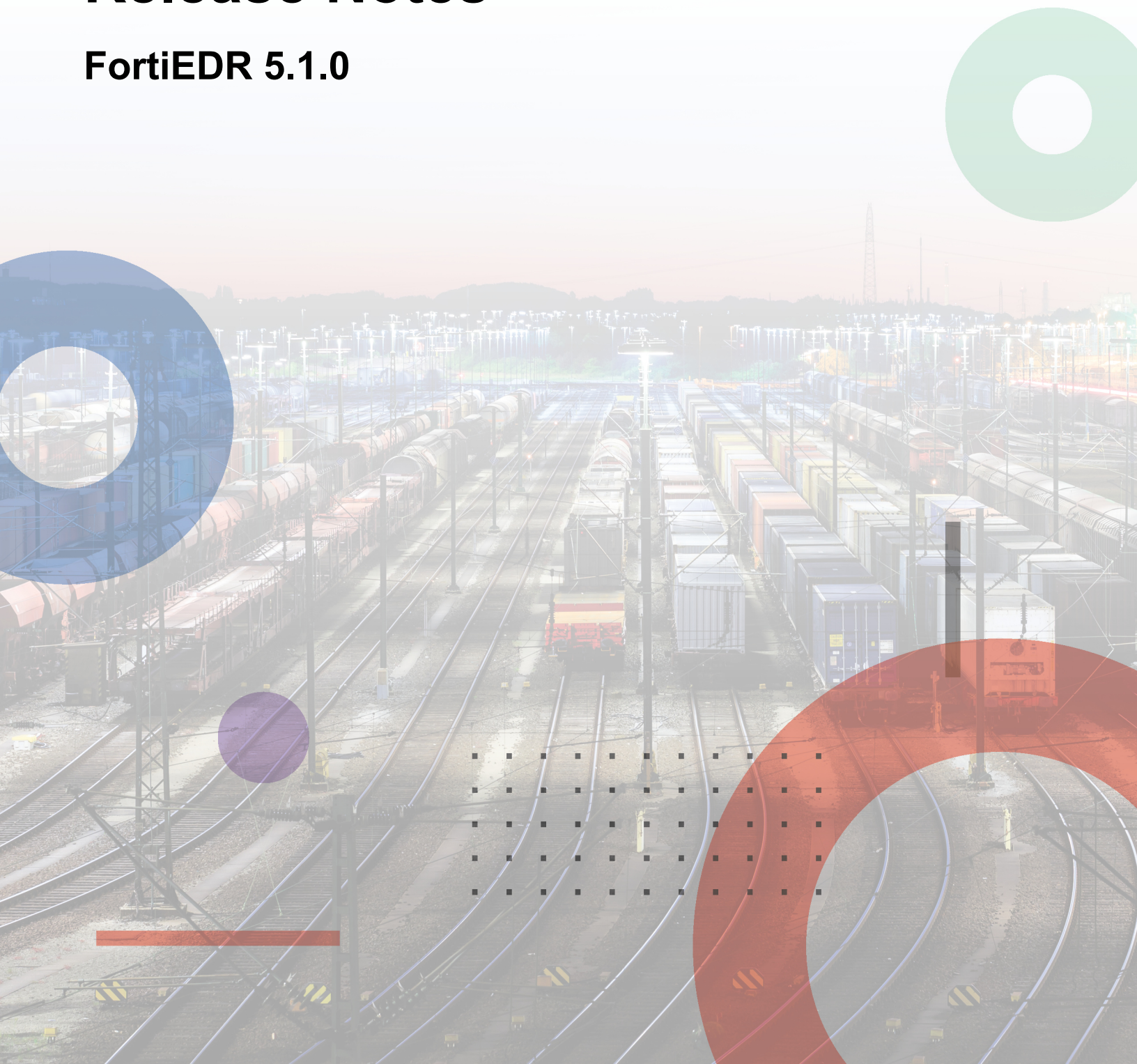
FORTINET

Release Notes

FortiEDR 5.1.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 20, 2022
FortiEDR 5.1.0 Release Notes
63-510-774697-20220120

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-01-20	Initial release of 5.1.0.
2022-03-10	Added ticket 771044 to Known Issues.
2022-03-24	Service Pack 1
2022-05-10	Added ticket 786156 to Known Issues.
2022-06-01	Added ticket 757253 to Known Issues.
2022-06-07	Added ticket 777707 to Known Issues.

FortiEDR 5.1.0 Release Notes

This document provides information about FortiEDR version 5.1.0.

Version History

	Central Manager	Threat Hunting Repository	Core
Initial GA	304	135	304
Patch 1	599	545	599

What's new

This section identifies new features and enhancements available with FortiEDR 5.1.0.

Application Control

This new capability enables blocking a provided blocklist of applications for reducing the attack surface and the exposure to threat. Different applications can be blocked across the entire organization or can be configured by a Collector group. Exceptions can be set for specific applications and specific groups. The capability requires the use of v5.1 Windows Collector.

Threat Hunting for Linux

Advanced and extensive behavior-based threat hunting, with the support of process-based threat hunting of files, log and network related activities. The capabilities include granular collection policies and collection exclusions for better control of the magnitude of the collected data in the Linux OS (RedHat, Centos). The capability is included and requires the use of v5.1 FortiEDR Linux Collector for RedHat or Centos.

Process Exclusions

Reducing TCO by providing the ability to exclude a known to be good process from FortiEDR monitoring. The capability requires the use of v5.1 Windows Collector.

NGAV Exclusions

Reducing TCO by providing the ability to exclude trusted files/folders from NGAV scan, wither periodic or on file execution. The capability requires the use of v5.1 Windows Collector.

Keylogging Activity Detection

New blocking options for process attempts to record keystrokes or mouse activity in a suspicious manner. The capability requires the use of v5.1 Windows Collector.

Threat Hunting enhanced data collection

New Activity Events types are now collected: Screen Capture and Keystroke Consumption of Process category, Direct Volume Access of File category, Socket Statistics, DNS Query and HTTP Request of Network category.

Threat Hunting terminology change

Threat Hunting settings as for which Activity Events should be collected are now called “Collection Profiles”. Exclusions to such profiles are now called “Collection Exclusions”.

Customer FortiEDR Serial Number

The serial number now appears in the FortiEDR Console at the Licensing page.

Resolved Issues

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

Central Manager - Build 599

Threat Hunting Repository - Build 545, 514

Core - Build 599

Bug ID	Description
765647 778441	Threat Hunting - Log category enhancement
765647 773930	Threat Hunting Exclusions - Support Linux exclusions
773589	Application Control Security Events appear under "All filter" instead of "Application Control" filter
791130	Threat Hunting - Incorrect process chains or Process Creation events
787361	Threat Hunting - Rename Activity Events for folders are missing data
782574	Threat Hunting - Add HTTP Request to Data Collection
791587	Playbook dropdown does not allow selecting some Connectors
787366	Cannot edit existing IP sets
761444	Validation of registration password
780167	Security Event's mails are not sent

Central Manager - Build 304

Threat Hunting Repository - Build 135

Core - Build 304

Bug ID	Description
763808	Search by MAC addresses on unmanaged and IOT pages is now available.
773606	Threat Hunting "Socket Bind" Activity Events are no longer collected.
773607	MITRE Tactics and Sub Techniques are now included in Threat Hunting Activity Events.
773608	Indication of whether a process is a console application is now included in the Threat Hunting

Bug ID	Description
	Activity Events.
761093	Device State is no longer missing from syslog event message.
769688	Collector doesn't switch to a non-reachable Aggregator.
773609	Security Event is now moved to Expired if it is reclassified automatically as 'Safe'.
732884	Threat Hunting search query - target file value is now case sensitive in queries.

Known Issues

The following issues have been identified in 5.1.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
733548	**Component backward compatibility**: V5.1 Central Manager supports Cores/Collectors from older versions with limited functionality. Some new features introduced in later versions may not be available.
733550	**Upgrading from older versions**: A direct upgrade path for backend components (Central Manager, Aggregator, Core, Threat Hunting Repository) from V5.0.2 or earlier is not supported. **Workaround**: Upgrade the older environment to V5.0.3 before upgrading it to V5.1.
733557	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 introduces SHA-256 code sign support.
733559	Some AV Products, including Windows Defender and some versions of FortiClient, require disabling their realtime protection in order to be installed alongside FortiEDR Collector. This is a result of FortiEDR registration as an antivirus (AV) in the Microsoft Security Center that was introduced in V4.0. Although there is no need for more than a single AV product to be installed on a device, FortiEDR can be smoothly installed, even if there is another AV already running. However, there are some other products whose installation fails when there are other AV products already registered. **Workaround**: Disable realtime protection on the other product, or remove FortiEDR's AV registration with Microsoft Security Center, now also available via UI.
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 upon events viewing.

Bug ID	Description
733600	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.
734594	Linux Threat Hunting Activity Events are missing process hash
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
773610	Execution Prevention Events are missing Device users
734309	NGAV scan of specific Collectors/Groups scan all Collectors
759573	Collector upgrade via custom installer requires password
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.
786156	Windows security center registration is not supported with Windows servers 2019 and above.
757253	It is not possible to redirect FortiEDR web to a URL that is different than the one provided by Fortinet.
777707	Linux Collector content file is large and uploads slowly to the Central Manager.

www.fortinet.com