



Release Notes

FortiRecorder 7.2.8



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

January 28, 2026

FortiRecorder 7.2.8 Release Notes

00-728-1249394-20260128

TABLE OF CONTENTS

Change log	4
Introduction	5
New features and enhancements	6
Default and behavior changes	7
Resolved issues	8
Common Vulnerabilities and Exposures	8
Compatibility	9
FortiRecorder models	9
Camera models	9
FortiCamera Mobile	10
FortiCentral	10
FortiGate security fabric (FortiView)	10
Web browsers and plugins	11
Firmware upgrade / downgrade path	12
Upgrading from earlier versions	12
Downgrading to previous firmware versions	12
Firmware image checksums	12

Change log

The following is a list of documentation changes. For a list of software changes, see the other contents of this document.

Date	Change Description
2026-01-27	Initial release of the FortiRecorder 7.2.8 Release Notes.

Introduction

This document provides a list of new and changed features, bug fixes, known issues, compatibility, and upgrade paths for FortiRecorder 7.2.8 build 0303.

For more information on installing or upgrading, see the [FortiRecorder Administration Guide](#).

New features and enhancements

No new features or enhancements in this patch release.

Default and behavior changes

No default setting or behavior changes.

Resolved issues

The resolved issues listed below may not include every bug that has been corrected with this release. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

- Motion detection does not work properly on non-standard ONVIF cameras.
- Error message after changing quality/resolution settings on FortiRecorder-based cameras.
- Video play issue on FortiRecorder-based camera timelines.
- In some cases, videos may be deleted from some cameras.
- License expiry counter does not work.

Common Vulnerabilities and Exposures

FortiMail 7.2.8 is no longer vulnerable to the following CVE/CWE-References.

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	Description
1241600	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
1242205	CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
1234004	CWE-121: Stack-based Buffer Overflow

Compatibility

FortiRecorder models

- FortiRecorder-400F with 1x 4 TB (4 x 8 TB max) hard drive
- FortiRecorder-400D with 2 x 3 TB (4 x 4 TB max) hard drive
- FortiRecorder-200D-Gen02 with 3 TB hard drive
- FortiRecorder-200D
- FortiRecorder-100D
- FortiRecorder-100G
- FortiRecorder-VM (64bit) for:
 - VMware vSphere Hypervisor ESXi 6.0, 6.7, 7.0
 - Microsoft Hyper-V 2016, 2019, and 2022
 - Citrix XenServer 5.6sp2, 6.0 (open source XenServer 7.4)
 - KVM (qemu 2.12.1)
 - AWS (EC2 PAYG)
 - Microsoft Azure (BYOL)

Camera models

- FortiAPCam-214B
- FortiCam-20A
- FortiCam-CB20
- FortiCam-CB50
- FortiCam-CD51
- FortiCam-CD51-C
- FortiCam-CD55
- FortiCam-CD55-C
- FortiCam-FB50
- FortiCam-FB85-CA
- FortiCam-FD20
- FortiCam-FD20B
- FortiCam-FD40
- FortiCam-FD50
- FortiCam-FD51
- FortiCam-FD55-CA

- FortiCam-FE120
- FortiCam-FE120B
- FortiCam-MB13
- FortiCam-MB40
- FortiCam-MC51
- FortiCam-MC51- C
- FortiCam-MD20
- FortiCam-MD40
- FortiCam-MD50
- FortiCam-MD50B
- FortiCam-OB20
- FortiCam-OB30
- FortiCam-PD50
- FortiCam-SD20
- FortiCam-SD20B
- ONVIF compliant cameras from third-party vendors (requires a feature license; for details, see the [FortiRecorder Administration Guide](#))

FortiCamera Mobile

- FortiCamera Mobile 7.0.4 app for iOS
- FortiCamera Mobile 7.0.5 app for Android

Other versions may function correctly, but have not been tested.

FortiCentral

- FortiCentral 7.2
- FortiCentral 6.4 is also supported except that older versions cannot use newer features.

FortiGate security fabric (FortiView)

- FortiGate 7.2

Web browsers and plugins

- Apple Safari 18
- Google Chrome 138
- Microsoft Edge 138
- Mozilla Firefox 140

Other web browsers and versions may function correctly, but have not been tested and are not supported by Fortinet.

H.265 display is supported on Microsoft Edge and Apple Safari. For Microsoft Edge, it depends on hardware decoding support of the computer.

Firmware upgrade / downgrade path

For firmware upgrade procedures, see the [FortiRecorder Administration Guide](#).

Upgrading from earlier versions

Upgrading directly from FortiRecorder 6.4.x to 7.2.8 is supported. For earlier versions, upgrade consecutive versions to FortiRecorder 6.4.0 first, and then upgrade to FortiRecorder 7.2.8.



If you are upgrading to FortiRecorder 6.0.0 during this process, then make a backup of FortiRecorder 2.7.x. Otherwise you will not be able to downgrade. See details on downgrading below.

If you need to upgrade FRC-400D to FortiRecorder 2.5.5 or later, first change BIOS settings so that you can perform a software reboot (only the reset button is supported). Ask Fortinet Support for help with the procedure.

Downgrading to previous firmware versions

Downgrades may cause a loss of configuration information. (New features are not supported by older versions, for example.)

Firmware image checksums

When you download software, use checksums to verify that the file has not been modified or corrupted.

1. On the [Fortinet Support site](#), go to *Downloads > Firmware Images*.
2. Select FortiRecorder
3. Click the *Download* tab and then click to go into the version folder.
4. Next to the file, click *HTTPS* to download the file. Then click *Checksum* to show the file's checksum.
To verify the file's integrity, the checksum shown by the website should match the checksum of the file on your computer.
5. Use a checksum tool and compute the firmware file's checksum. For example, you could use [certutil on the Windows command line](#):
`certutil -hashfile firmware.out SHA512`

If the file's checksum shown on the Fortinet Support website matches the file's checksum on your computer, then the file is intact.

www.fortinet.com

Copyright© 2026 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.