Release Notes

FortiRecorder 7.2.2

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

FORTINET®

December 18, 2024
FortiRecorder 7.2.2 Release Notes

TABLE OF CONTENTS

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
2024-11-07	Initial release of FortiRecorder 7.2.2 Release Notes.
2024-12-03	Fixes to Compatibility on page 8. Duplicate information on licenses and performance guidelines are also now merged into the FortiRecorder Administration Guide.

Introduction

This document provides a list of new and changed features, bug fixes, known issues, compatibility, and upgrade paths for FortiRecorder 7.2.2 feature release, build 250.

For more information on installing or upgrading, see the FortiRecorder Administration Guide.

Special notices

Licensing and performance guidelines

Licensing and performance information is not generally required for upgrades, but is required during deployment planning and setup, so it has been merged into the existing sections of the FortiRecorder Administration Guide:

- Licenses
- Sizing guidelines

Firmware upgrade / downgrade path

Upgrading from earlier versions

Upgrading directly from FortiRecorder 6.4.x to 7.2.2 is supported. For earlier versions, upgrade consecutive versions to FortiRecorder 6.4.0 first, and then upgrade to FortiRecorder 7.2.2.

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

To verify the integrity of the firmware file, use a checksum tool and computer the firmware file's checksum. For example, you could use certutil on the Windows command line:

```
certutil -hashfile firmware.out SHA512
```

Compare it with the checksum indicated by Fortinet Customer Service & Support:

https://support.fortinet.com

After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*. If the checksums match, then the file is intact.

Compatibility

FortiRecorder models

- FortiRecorder-400F with 1 x 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 ESX/ESXi 6.0, 6.7, 7.0 and later
  - Microsoft Hyper-V 2016, 2019, and 2022
  - Citrix XenServer 5.6sp2, 6.0 and later (open source XenServer 7.4 and later)
  - KVM (qemu 2.12.1 and later)
  - AWS (EC2 PAYG)
  - Microsoft Azure (BYOL)

Camera models

- FortiAPCam-214B
- FortiCam-20A
- FortiCam-CB20
- FortiCam-CB50
- FortiCam-FB50
- FortiCam-FD20
- FortiCam-FD20B
- FortiCam-FD40
- FortiCam-FD50
- FortiCam-FE120
- FortiCam-MB13
- FortiCam-MB40
- FortiCam-MD20
- FortiCam-MD40
- FortiCam-MD50
- FortiCam-MD50B
- FortiCam-OB20
- FortiCam-OB30

- FortiCam-PD50
- FortiCam-SD20
- FortiCam-SD20B
- FortiCam-CD51
- FortiCam-CD55
- FortiCam-CD51-C
- FortiCam-CD55-C
- FortiCam-FE120B
- FortiCam-MC51
- FortiCam-MC51-C
- FortiCam-FD55-CA
- ONVIF compliant cameras from third-party vendors (requires a feature license; for details, see the FortiRecorder Administration Guide)

FortiCentral

- FortiCentral 7.2 and later
  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 17 or later
- Google Chrome 120 or later
- Microsoft Edge 120
- Mozilla Firefox 120 or later

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.

New features

- None

Enhancements

- For provisioning via USB key:
  - Skip configuration steps if already done
  - Skip firmware upgrade if already installed
  - Skip comments and blank lines in CSV files
  - Assign cameras and give DHCP reservations for zero MACs
- For licenses of third-party and cloud mode cameras (in hybrid deployments with FortiCamera Cloud), only count enabled and active cameras (not disabled)
- Added a status for unlicensed cameras
- Allow rename of cameras in hybrid deployments with FortiCamera Cloud
- Show an audit summary in the Security Fabric view
- Show a disclaimer message banner on the GUI before login
- Live video streams are now available even if FortiRecorder has a hard disk failure
- Show a warning on the GUI when using the emergency file system
- Improved camera event end time processing (don't show the end time in the event list until the event is finished)
- Users with video playback permission can now call the video clip REST API
- Reduced tamper detection false positives when a camera transitions to night mode
- Reduced startup time
- Support for FortiCam FE120B Generation 1 and Generation 2

Resolved issues

To inquire about a particular bug, please contact Fortinet Customer Service & Support.

- For some FortiCam FD51, FD55-CA, and FE120B cameras, network settings were not retained after a factory reset
- For a FortiCam FE120B in fisheye display mode with shutter WDR enabled, an extra-high resolution screenshot could not be retrieved
- For FortiCam FD51, the digital input trigger default value should be set to *Low*
- If a FortiCam FD55-CA was on a different subnet than FortiRecorder, its MAC address was not correctly detected
- If a FortiCam MC51 view was rotated ±90°, the camera could crash
- Motion detection search analytics did not have results
- After a factory reset on FortiCam FE120B or FD55-CA, analytics configuration could fail
- When VLC was used to seek backwards on a video stream, the video stream service stopped
- Camera simulator should function on FortiRecorder-VM platforms
- If more than 4 cameras were added to FortiRecorder 100G, it became unresponsive
- If more than 16 cameras were added to FortiRecorder 400F, it became unresponsive
- Bug ID 1059479: If more than 4 cameras were added to *Service* > *Monitor Display* on FortiRecorder 100G, it became unresponsive
- Bug ID 1081765: Camera motion detection event recordings did not work if the
- Bug ID 1074820: If SFTP remote configuration backup fails, FortiRecorder should generate a log message
- Bug ID 1053197: After upgrading a FortiRecorder, the ONVIF transport type and port should not be reset to their default values

Vulnerabilities

- Bug ID 1092957, 1082353: CLI path traversal attack
- Bug ID 1082354: GUI path traversal attack
- Bug ID 1092984: Upgrade to `httpd` 2.4.62
- Bug ID 1057588: Security fabric (`csfd`) daemon inserted sensitive information into data that it sends
- Bug ID 1060912: Security fabric (`csfd`) daemon path traversal attack

Known issues

- None

Vulnerabilities

- None

www.fortinet.com

Copyright© 2024 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.