Release Notes

FortiRecorder 7.2.6

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

F::RTINET.

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
2025-10-14	Initial release of the FortiRecorder 7.2.6 Release Notes.

Introduction

This document provides a list of new and changed features, bug fixes, known issues, compatibility, and upgrade paths for FortiRecorder 7.2.6 build 0290.

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

Special notices

No special notices.

New features

The following table summarizes the new features in this release. For details, see the FortiRecorder Administration Guide.

Feature	Description
FortiCam FE120B-CA support	FortiRecorder7.2.6 now supports the new FortiCam 120B-CA camera model. This camera is coming soon.

Enhancements

The following table summarizes the enhancements in this release. For details, see the FortiRecorder Administration Guide.

Feature	Description
Alert email when cameras reboot or are disabled	Recordings cannot occur while a camera reboots or is administratively disabled. FortiRecorder can now send alert email to notify you when this happens.
Fisheye snapshots in panorama mode	Fisheye snapshots are now supported when the camera is recording in panorama mode.
REST API for snapshot image downloads	In the REST API, the new `CameraSnapshot` endpoint allows you to download snapshot images from cameras that are attached to FortiRecorder.
Camera settings available while the camera is not connected	If a camera network connection is disrupted, on *Camera > Configuration > Camera*, the camera's settings displays the error message *Unable to communicate with the camera*. Communications are required to send setting changes to the camera, and during at that time, many of the camera's settings were not visible and configurable. Now settings are retained, visible, and configurable during network disruptions, and changes can be sent to the camera later when the camera network connection resumes.
Camera list refresh	On *Camera > Configuration > Camera*, when setting changes are being sent to cameras, the list of cameras automatically refreshes every few seconds to indicate setting sync progress. Now you do not need to remain on that page until the setting sync completes. If you leave to configure other settings on FortiRecorder and return later, the progress indicator will resume.

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.

- For on-demand deployments on the AWS cloud with FortiRecorder VM, `camerad` crashed.
- A *Duplicate IP* camera status occurred after a discovered camera's IP address was changed, even if the camera did not currently have a duplicate IP address.
- Metadata stopped being recorded after some time if network connection errors were occurring repeatedly with the camera. This issue could be indicated by FortiCamera Cloud or FortiCentral charts with missing information, or by FortiRecorder log messages such as `Failed to start 'metadata' recording for camera`.
- While FortiRecorder had a tunnel with the camera, if the TCP network connection dropped, then `camproxyd` crashed.
- Messages about *Dropped X segments* occurred. These have been removed.
- When multiple people connected to view live video streams from an ONVIF (third-party) camera, the *Error* camera status occurred. The *Viewing media profile* setting was also empty. This issue only occurred if any previous software upgrades or downgrades included FortiRecorder 7.2.5.
- Incorrect permissions for the administrator profile named `readonly_admin_prof` allowed write access for `execute` commands in the CLI.
- Memory leak in the REST API
- On FortiRecorder400F with RAID where the hard disks are different sizes, if you upgraded from FortiRecorder 7.2.1 to 7.2.5, then FortiRecorder rebooted in emergency mode and the RAID stopped functioning. After running the CLI command `exec raidlevel 0`, the RAID was rebuilt and started to function again, but the RAID status was still *Unknown*.
- In the CLI, if you logged in as any administrator that was not `admin` but had `SuperAdminProfile` permissions, and then you created a new account and tried to set the password, it prompted you for the current password. However new accounts do not have an existing password yet.

Known issues

- On FortiCam FB85-CA cameras, when audio is enabled in the camera profile, live video streaming and recording fails, and the camera status indicates *Recording Issue*.

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 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-FE120B-CA
- 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 140
- Microsoft Edge 140
- Mozilla Firefox 143

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 7.2.6 is supported. For earlier versions, upgrade consecutive versions to FortiRecorder 6.4.0 first, and then upgrade to FortiRecorder 7.2.6.

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.

FORTINET

www.fortinet.com