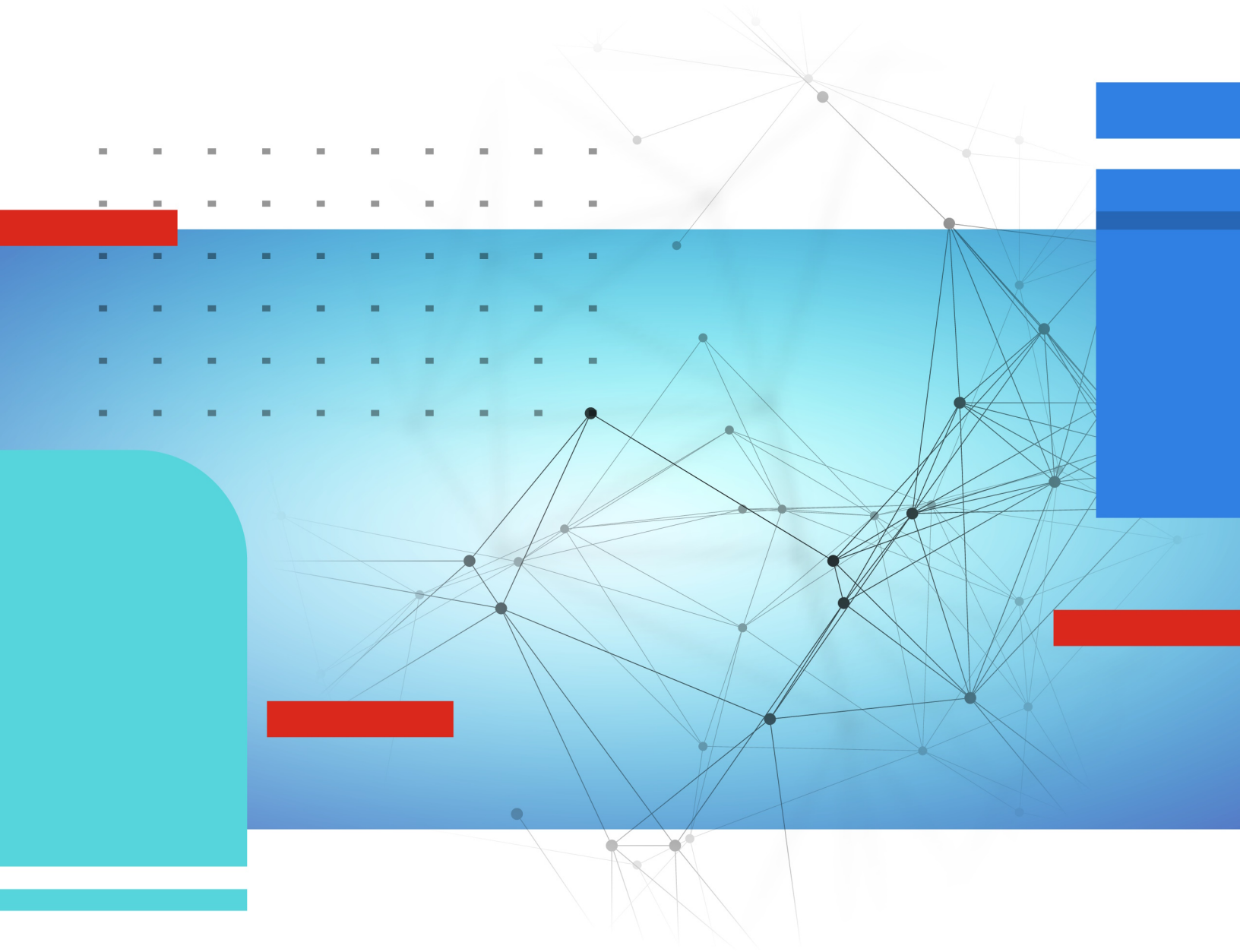
Release Notes

FortiRecorder 7.0.5



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

December 10, 2024
FortiRecorder 7.0.5 Release Notes

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Special notices **6**
Licensing and performance guidelines 6
Firmware upgrade / downgrade path **7**
Upgrading from earlier versions 7
Downgrading to previous firmware versions 7
Firmware image checksums 7
Compatibility **8**
FortiRecorder models 8
Camera models 8
FortiCentral 9
FortiGate security fabric (FortiView) 9
Web browsers and plugins 9
New features **10**
Enhancements **11**
Resolved issues **12**
Vulnerabilities 12
Known issues **13**
Vulnerabilities 13

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
2024-12-10	Initial release of FortiRecorder 7.0.5 Release Notes.

Introduction

This document provides a list of new and changed features, bug fixes, known issues, compatibility, and upgrade paths for FortiRecorder 7.0.5 feature release, build 0084.

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 7.0.5 is supported. For earlier versions, upgrade consecutive versions to FortiRecorder 6.4.0 first, and then upgrade to FortiRecorder 7.0.5.

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 7.0 and later
  FortiCentral 6.4 is also supported except that older versions cannot use newer features.

FortiGate security fabric (FortiView)

- FortiGate 7.0

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

- Decreased delay in video file finalization
- Smoother zoom and focus operations

Resolved issues

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

- If the FortiRecorder file system becomes read-only, an SNMP trap should be sent
- On models with no power supply status monitoring, SNMP OID `frcHwSensorCount` should return 0
- When downgrading firmware, the configuration manager (`cmdb`) should not crash
- FortiRecorder-VM license did not validate, showing the error message `Invalid license Duplicated`
- If a camera name has more than 26 characters, video playback should not fail
- Users should be able to change their own mobile device in the device list for FortiRecorder Mobile
- Bug ID 1053197: After upgrading a FortiRecorder, the ONVIF transport type and port should not be reset to their default values.
- Bug ID 0892720: After upgrading, the live view REST API failed, showing the error message `Failed: Access denied`
- Bug ID 1102855: Avoid unnecessary communication with camera when retrieving the pixel resolution
- Bug 1050943: Heatmap for motion analytics should not show static

Vulnerabilities

- Bug ID 1041227: CVE-2023-52434 (Linux kernel issue with SMB/CIFS network shares)
- Bug ID 1051895: CVE-2024-6387 (OpenSSH regreSSHion RCE attack)
- Bug ID 0985980: CVE-2023-48795 (OpenSSH Terrapin attack)
- Bug ID 1009228: Upgrade to curl 8.8.0
- Bug ID 1044758: Upgrade to libexpat 2.6.2
- Bug ID 0975717: Upgrade to traceroute 2.1.3
- 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