



FortiRecorder™ v2.7.3 GA

Release Notes



FortiRecorder v2.7.3 GA Release Notes

July 12th, 2019

Copyright© 2019 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 General Counsel, 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.

Technical Documentation
Knowledge Base
Customer Service & Support
Training Services
FortiGuard
Document Feedback

docs.fortinet.com
kb.fortinet.com
support.fortinet.com
training.fortinet.com
fortiguard.com
techdocs@fortinet.com

Table of Contents

Introduction	4
Supported models	4
Summary of new features	5
Special Notices	6
Monitor settings for Web UI	6
Supported Web browsers and plugins	6
Camera discovery method	6
FortiRecorder Central Windows client compatibility	6
FortiRecorder MIB file	6
New Features	7
Firmware Upgrade/Downgrade Information	8
Upgrading from earlier versions	8
Downgrading to earlier versions	8
FortiRecorder-VM	9
Licensing	9
Trial License	9
Evaluation License	9
Installation notes	9
Camera deployment scenarios	10
Local camera deployments	10
Same network deployments	10
Routed network deployments	10
Remote camera deployments	10
Performance Guidelines	11
NVR performance	11
Number of supported cameras	11
General performance factors	11
Variable versus constant bit rate	11
Bandwidth per camera or live view	12
FortiRecorder maximum bandwidth	12
Storage capacity	13
Client Performance	13
Image Checksums	15

Introduction

This document provides a summary of enhancements, installation instructions, deployment scenarios and performance guidelines for FortiRecorder v2.7.3 release build 719. Please review this document before installing or upgrading FortiRecorder.

For more information on installing or upgrading your FortiRecorder device, see the FortiRecorder Administration Guide. The Administration Guide can be found at <http://docs.fortinet.com/fortirecorder/admin-guides>

Supported models

The following models are supported in FortiRecorder v2.7.3:

- FortiRecorder-400D Network Video Recorder with 2x3TB (4x4TB max) HD
- FortiRecorder-200D-Gen02 Network Video Recorder with 3TB HD
- FortiRecorder-200D Network Video Recorder
- FortiRecorder-100D Network Video Recorder
- FortiRecorder-VM (64bit) Network Video Recorder for
 - VMware vSphere Hypervisor ESX/ESXi v5.0 and higher
 - Microsoft Hyper-V 2008 R2 and 2012
 - Citrix XenServer v5.6sp2, 6.0
 - KVM (qemu 0.12.1)
 - AWS (EC2 PAYG)
- FortiCam-20A Network Camera
- FortiCam-MB40 Network Camera
- FortiCam-MB13 Network Camera
- FortiCam-MD20 Network Camera
- FortiCam-MD40 Network Camera
- FortiCam-MD50 Network Camera
- FortiCam-OB20 Network Camera
- FortiCam-OB30 Network Camera
- FortiCam-FD20 Network Camera
- FortiCam-FD20B Network Camera
- FortiCam-FD40 Network Camera
- FortiCam-CB20 Network Camera
- FortiCam-SD20 Network PTZ Camera
- FortiCam-SD20B Network PTZ Camera
- FortiCam-FE120 Network Panoramic Camera
- FortiAPCam-214B Network Camera and Access Point

Summary of new features

The following is a list of the enhancements in FortiRecorder v2.7.3:

- ONVIF Profile T support
- Improvements
- Bug fixes
- Fixed Vulnerabilities

Special Notices

Monitor settings for Web UI

Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024. This allows for objects in the web UI to be viewed properly.

Supported Web browsers and plugins

- Internet Explorer 11 or Edge 42, 44
Known Issue: When trying to view large-resolution video through the web UI, the browser will crash and potentially restart.
This is a Microsoft bug affecting Internet Explorer and Edge on Windows 10.
Video Resolutions: 4K (2688x1512), and possibly resolutions larger than 1920x1080
FortiRecorder versions: 2.4 and later
Available workarounds:
 1. Disable hardware decoding in Edge: Control Panel > Network and Internet > Internet Properties > Advanced > Use software rendering instead of GPU rendering.
 2. Use Chrome or Firefox, which will use software decoding by default.
 3. Use FortiRecorder Central.
- Firefox 60.5 ESR, 65 or higher
- Safari 11, 12 or higher
- Chrome 71 or higher
- Adobe Flash Player 9 or higher plug-in required to display statistics charts
- H.265 display is supported on Microsoft Edge and Apple Safari

Camera discovery method

As of v2.0.0 FortiRecorder supports UPnP, mDNS and ONVIF discovery of cameras.

FortiRecorder Central Windows client compatibility

It is recommended to use FortiRecorder v2.7.3 in connection with FortiRecorder Central v1.9.
Using FortiRecorder Central v1.7.x and v1.8 is supported, but may have some limitations.
FortiRecorder v2.7.3 will not connect with FortiRecorder Central v1.0.

FortiRecorder MIB file

An SNMP MIB file for FortiRecorder is available from the FortiRecorder download directory on the support site.

New Features

The following section highlights the new features in the FortiRecorder v2.7.3 release.

ONVIF Profile T support

For third party cameras ONVIF profile T offers support for h.265 video streams.

Improvements

- New CLI command to perform configuration backup
'exec backup config {ftp|tftp|scp} <filename> <server>'
- Licensing
Log when a license file is loaded
Number of active / disabled cameras
- Better handling of camera discovery in busy environment.
Reducing the possibility of error 'Failed to retrieve list of cameras'.

Bug fixes

- Mantis 0562863: Event Detection would stop working after some time
- Mantis 0562928: Fix possible crash in the camnotifyd daemon
- Mantis 0566782: Incorrect local/remote disk space/usage
- Mantis 0568213: GUI hangs when name missing for new user profile

Fixed vulnerabilities

For more information see: <http://www.fortiguard.com/advisory>

Fixed vulnerabilities include:

- Mantis 0513825 Upgrade to openssl 1.1.1 and TLS 1.3 support
- Mantis 0553795 Openssh Versions 8.0/8.0p1
 - CVE-2019-6111
 - CVE-2019-6110
- Mantis 558644 Upgrade Apache to 2.4.39
 - CVE-2019-0211
 - CVE-2019-0217
 - CVE-2019-0215
 - CVE-2019-0196
 - CVE-2019-0197
 - CVE-2019-0220
- Mantis 569759 bzip2 vulnerability
 - CVE- 2019-12900

Firmware Upgrade/Downgrade Information

Upgrading from earlier versions

Upgrading to v2.7.3 from v2.7.x, v2.6.x or v2.5.x is fully supported. For earlier versions a consecutive upgrade to v2.5.0 is recommended.

Fortinet always recommends backing up the NVR configuration before performing an upgrade.

Upgrading FRC-400D to v2.5.5 or later is supported, but requires changing BIOS settings in order to perform a software reboot (only reset button supported). Ask Fortinet support for help with the procedure.

Downgrading to earlier versions

Fortinet does generally not recommend downgrading because there may be a loss of configuration information.

Note: Before downgrading from v2.x.x to any v1.x.x version disable FRC-Central protocol. Otherwise all protocols for this port will be disabled after the downgrade! This might require using a serial console connection to regain access to the FRC.

Note: Before downgrading from v2.x.x to any v1.x.x version disable cameras and reset the password using the CLI command `exec camera password-reset`. Otherwise cameras may be rendered inaccessible after the downgrade and a camera hardware factory reset or recorder upgrade to 2.x is required to access the cameras again.

Fortinet always recommends backing up the NVR configuration before performing a firmware update, upgrade or downgrade.

FortiRecorder-VM

Licensing

FortiRecorder-VM is licensed based on the number of active (enabled) cameras and uses a stackable licensing model. The available license SKUs are:

- FRC-VM-Base – includes 10 camera license
- FRC-VM-10 – adds 10 cameras to the Base license
- FRC-VM-50 – adds 50 cameras to the Base license
- FRC-VM-100 – adds 100 cameras to the Base license

There are no other restrictions to the license other than the number of active cameras – i.e. there is no restriction on the number of virtual CPUs, disk space, etc.

The current maximum number of active cameras supported by FortiRecorder-VM is 1010 – i.e. you cannot currently license more than 1010 active cameras per FortiRecorder-VM installation.

After placing an order for FortiRecorder-VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register your FortiRecorder- VM with Customer Service & Support at <https://support.fortinet.com>.

Upon registration, you can download the license file. You will need this file to activate your FortiRecorder- VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded, the CLI and Web-based Manager are fully functional.

Trial License

When FortiRecorder-VM is first installed, it will have a trial license. The trial license supports a maximum of 5 active cameras for 45 days. All features and functionality are available with a trial license except 3rd party camera support of more than one camera.

Evaluation License

The FRC-VM-Base SKU can be ordered as an evaluation license. The FRC-VM-Base SKU supports 10 active cameras. All features and functionality are available with an evaluation license including adding 3rd party camera licensin0067 of more than one camera.

Installation notes

Refer to the FortiRecorder-VM Installation Guide for installation details. The Installation Guide can be found at <http://docs.fortinet.com/d/fortirecorder-vm-install-guide>.

Camera deployment scenarios

Cameras are deployed in two basic scenarios: local to the NVR and remote to the NVR. FortiCamera deployments can combine both scenarios.

Note: Cameras should always be placed in a separated subnet isolated from outside to ensure only FortiRecorder can control access to/from camera network. Use of a dedicated FortiRecorder port or VPNs is recommended.

Local camera deployments

Local cameras deployments have two specific scenarios:

1. Cameras are installed on the same network as the NVR.
2. Cameras are installed on a local network, but there are one or more routers between the NVR and the cameras.

Same network deployments

Installing the cameras on the same subnet as the NVR is the easiest deployment scenario since the NVR can automatically discover the cameras.

Routed network deployments

If there are routers between the cameras and the NVR, the routers must be configured to allow discovery packets (mDNS multicast, UPnP and ONVIF) between the camera network and the NVR network in order for the NVR to automatically discover the cameras. The FortiRecorder will be able to detect if the camera changes IP address. You can leave the address mode as DHCP or change it to static.

If the FortiRecorder cannot discover cameras on a different network, the cameras can be added manually. The cameras should be deployed so that the IP address does not change, either by using MAC - IP reservation on the DHCP server or by assigning a static IP address when configuring the camera.

Remote camera deployments

Remote camera deployments refer to scenarios where there is a firewall between the NVR and the cameras – i.e. camera discovery will not work and the cameras will likely have virtual IP addresses on the firewall. The cameras are configured by selecting the VIP address mode on the camera configuration page.

Performance Guidelines

There are two components to consider when looking at FortiRecorder performance – the NVR (FortiRecorder) and the client computer with FortiRecorder Central or a browser.

Overall FortiRecorder performance is a combination of the video input (video compression, image quality level, complexity of the scene, video resolution, frame rate per second, number of cameras) and the video output (to the clients for live views and playback).

The performance bottleneck in a FortiCamera deployment will likely be the network bandwidth to and from FortiRecorder and the CPU performance of the computer running the FortiRecorder Central or browser client, which must decode and render the video streams from the NVR. Displaying multiple video streams on the client is very CPU intensive.

NVR performance

Number of supported cameras

The FortiRecorder-200D and FortiRecorder-400D can support up to 64 cameras depending on the configuration. The FortiRecorder-100D is suitable for 16 cameras. For FortiRecorder-VM the number of supported cameras is dependent on the hardware configuration of the VMware server and the number of licensed cameras.

General performance factors

The following factors affect the input side of performance:

- Total number of video streams from the cameras (i.e. not just the number of cameras)
- The video recording types (motion only or continuous) per camera
- The video stream parameters per camera – i.e. resolution, frame rate, bitrate mode (constant or variable) and the bitrate mode parameters (bitrate or image quality).
- The number of detection events being received and the number of associated snapshots and clips being generated for display in the event monitor.
- Storage settings – moving recordings from local to remote storage, NAS model and type, network connectivity to NAS, recompression and deleting of continuous recordings when detection recordings have to be kept.

The following factors affect the output side of performance:

- Number of administrator/operator/viewer sessions
- Peak number of simultaneous administrator/operator/viewer live and playback views
- The video stream parameters per camera view – i.e. resolution, frame rate, bitrate mode (constant or variable) and the bitrate mode parameters (bitrate or image quality).

Variable versus constant bit rate

Variable Bit Rate mode means the bandwidth used by the camera will vary according to what the camera is seeing and the video profile settings. The video profile settings for the variable bit rate mode are resolution, frame rate and image quality. High resolution creates more data than

medium or low resolution (see following sections for more detail). The degree of motion present in a video stream also affects the amount of data created.

Constant Bit Rate mode means the bandwidth used by the camera will stay relatively constant regardless of what the camera is seeing. The constant bit rate mode is therefore more predictable in deployments where bandwidth and/or storage capacities are important considerations. The video profile settings for constant bit rate mode are resolution, frame rate and bit rate. The bandwidth used by the stream is dictated by the bit rate setting.

In general, using the variable bit rate mode results in relatively consistent video quality but fluctuating bandwidth and using the constant bit rate mode results in varying video quality but predictable bandwidth. Choosing a high bandwidth constant bit rate mode avoids the video quality drop e.g. during high motion, but may use some unnecessary bandwidth during times of no activity.

However, in most cases the difference in video quality between the variable and constant bit modes is negligible (assuming the same resolution frame rates and scene) and the constant bit rate mode produces more reliable output from the cameras.

Bandwidth per camera or live view

Depending on resolution, frame rate and video quality a camera using H.264 compression may generate the following bitrates (examples):

- 352 x 240 @ 30 FPS, high quality = 0.4 Mbps
- 720 x 576 @ 30 FPS, high quality = 1 Mbps
- 1280 x 720 @ 30 FPS, high quality = 2 Mbps
- 1920 x 1080 @ 30 FPS, high quality = 4 Mbps
- 1920 x 1080 @ 30 FPS, medium quality = 2.8 Mbps
- 1920 x 1080 @ 30 FPS, low quality = 2 Mbps
- 1920 x 1080 @ 10 FPS, high quality = 2.4 Mbps
- 1920 x 1080 @ 10 FPS, low quality = 1.2 Mbps

Please note that these are estimates. If the scene is less complex (indoor with little detail and not much motion), or the camera has little noise (daylight, good digital noise reduction) the required bandwidth can be lower.

FortiRecorder maximum bandwidth

Recommended maximum total camera bandwidth usage for different FortiRecorder models and setup environments.

FRC Model	Continuous	Continuous with NAS	Continuous with motion	Continuous with motion and NAS
FRC-100D	90 Mbps	TBC	35 Mbps	TBC
FRC-200D gen1	90 Mbps	55 Mbps	50 Mbps	50 Mbps
FRC-200D gen2	135 Mbps	135 Mbps	130 Mbps	130 Mbps
FRC-400D	170 Mbps	160 Mbps	140 Mbps	130 Mbps

Note: These values have been determined experimentally in a lab setting and do not represent hard limits. Performance degrades gradually with symptoms like sluggish responses or some dropped video frames. Real world performance depends on many factors including network environment and NAS types. The motion detection rate in the table was 13% based on 1 detection of 40s length every 5min per camera.

There are several widgets available in the recorder dashboard to help with sizing and to detect skips in recordings. The camera bandwidth widget can graph bandwidth usage for all or a selected group of cameras. The skip widget can show skipped frames for each camera recording, which has to be related to possible missing frames due to network stream issues as indicated in the gaps widget.

Storage capacity

Video retention depends on the available storage capacity and the total amount of video bandwidth from the cameras. The following are some examples for FortiRecorder 100D, 200D and 400D configured with different camera parameters to demonstrate the video retention period.

FortiRecorder-100D has 1TB HD. For 4 cameras at 2 Mbps each this will yield 12 days of recording.

FortiRecorder-200D with 3TB HD and 24TB remote storage. For 32 cameras at 2Mbps each this will provide 42 days of recording.

FortiRecorder-400D has 6TB HD. For 16 cameras at 1.5Mbps this will yield 25 days of recording.

A basic rule of thumb for doing a quick storage capacity calculation is:

1TB HD can store 1 camera configured to consume 1Mbps for approximately 100 days.

Therefore:

1TB HD can store 1 camera configured to consume 2Mbps for approximately 50 days.

6TB HD can store 10 cameras configured to consume 2Mbps each for approximately 30 days.

For more detailed bandwidth and storage consumption calculations, please refer to FortiCamera Bandwidth Calculator User Guide on docs.fortinet.com.

Client Performance

If you need to display 8 or more camera live views, you may need to configure the second camera stream so that viewing is done at a lower frame rate or resolution, depending on how powerful the client PC is. RAM is less important than CPU for rendering video.

Video playback is very CPU intensive. If you are experiencing choppy video playback and cameras “freezing” during playback, you likely have a client performance problem. Use the diagnostic tools available on your client OS and look at the CPU usage when you are experiencing video problems. If possible, keep the CPU usage below 50%.

To optimize client performance, use the video and camera profiles to define and assign a second video stream for each camera. To increase the number of live views the client computer can display, or to reduce the CPU requirement for a given number of live views, reduce the resolution, quality and/or frames per second of the second video streams.

10 FPS is a good general setting for live views, which provides a reasonable frame rate for the live views, but significantly reduces the load on the client (compared to 30 FPS which is more ideal for higher traffic area surveillance)..

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, click the *Firmware Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

The screenshot shows the Fortinet Customer Service & Support website. The top navigation bar includes the Fortinet logo, a 'Home' button, and links for 'Asset', 'Assistance', 'Download', and 'Feedback'. A user profile icon and 'LOG OUT' link are on the right. Below the navigation bar is a blue banner with a 'Welcome' message and a note about Pacific Standard Time. The main content area features a 'Customer Support Bulletin' with three items and a 'More' button. Below this is the 'Asset' section with 'Register/Renew' and 'Manage Products' options. The 'Assistance' section contains 'Create a Ticket', 'View Active Tickets', 'Contact Support', 'Manage Tickets', and 'Technical Web Chat'. The 'Download' section has 'Service Updates', 'Firmware Images', and 'Firmware Checksums' (highlighted with a red box). The 'Quick Links' section lists 'Forti-Companion', 'Tickets Creation Guide', 'Product Life Cycle', and 'CSS Reference Guide'.

FORTINET
CUSTOMER SERVICE & SUPPORT

Home Asset Assistance Download Feedback

LOG OUT

Home Welcome
Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

About To Expire
1

Customer Support Bulletin

1. IPS Engine update Updates to the IPS engine that runs on the FortiGate platforms periodically are made available on the FortiGuard distribution network that permit devices with...
2. FortiGuard updates to FortiOS 2.8 to finish The AntiVirus (AVE) and IPS (IPSE) engines associated with FortiOS 2.8 software reached end of life in February 2013. As of February...
3. FortiGate System Freeze with FortiOS 5.0.5 Certain models of FortiGates as listed below, may experience a hang or system freeze condition when a very heavy load of HTTP ...

More

Asset

Register/Renew
Register HW/Virtual appliance or software: Activate service contract or license on your registered product.

Manage Products
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

Create a Ticket
The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

View Active Tickets
Check latest active tickets for current user, update ticket information or change ticket status.

Contact Support
Contact Information of Fortinet worldwide support centers.

Manage Tickets
Check ticket status, add comment, update contact or view history etc.

Technical Web Chat
Provide quick answers on-line for general technical questions.

Download

Service Updates

Firmware Images

Firmware Checksums

Quick Links

- Forti-Companion
- Tickets Creation Guide
- Product Life Cycle
- CSS Reference Guide

