FortiRecorder™ v6.4.1 GA

Release Notes

FortiRecorder v6.4.1 GA Release Notes

Sep 21st, 2021

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Introduction

This document provides a summary of enhancements, installation instructions, deployment scenarios and performance guidelines for FortiRecorder v6.4.1 release build 238. 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 v6.4.1:

- FortiRecorder-400F Network Video Recorder with 1x4TB (4x8TB max) HD
- 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)
  - Azure (BYOL)
- FortiAPCam-214B Network Camera and Access Point
- FortiCam-20A Network Camera
- FortiCam-CB20 Network Camera
- FortiCam-CB50 Network Camera
- FortiCam-FB50 Network Camera
- FortiCam-FD20 Network Camera
- FortiCam-FD20B Network Camera
- FortiCam-FD40 Network Camera
- FortiCam-FD50 Network Camera
- FortiCam-FE120 Network Panoramic Camera
- FortiCam-MB13 Network Camera
- FortiCam-MB40 Network Camera
- FortiCam-MD20 Network Camera
- FortiCam-MD40 Network Camera
- FortiCam-MD50 Network Camera
- FortiCam-MD50B Network Camera

- FortiCam-OB20 Network Camera
- FortiCam-OB30 Network Camera
- FortiCam-PD50 Network PTZ Camera
- FortiCam-SD20 Network PTZ Camera
- FortiCam-SD20B Network PTZ Camera
- FortiCam-CD51 Camera
- FortiCam-CD55 Camera

Summary of changes

The following is a list of the enhancements in FortiRecorder v6.4.1:

- Features
- Improvements
- Bug fixes
- Vulnerabilities
- Known issues

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

- Microsoft Edge 88

  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 89 or higher
- Safari 14 or higher
- Chrome 91 or higher
- H.265 display is supported on Microsoft Edge and Apple Safari. For Microsoft Edge it depends on hardware decoding support of the workstation.

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 v6.4.1 in connection with FortiRecorder Central v6.4.1.

Using FortiRecorder Central v6.0.x is supported, but may have some limitations.

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 v6.4.1 release.

Features

- New platform: Azure - BYOL
- Power Frequency (50Hz / 60Hz) for CD51/CD55/FD50/FB50 cameras
- Added firmware handling support for FortiCentral

Improvements

- Improved support for wired / wireless address mode
- Improved error reporting on GUI
- Added validation of camera connectivity when changing addressing mode.

Bug fixes

- Mantis 0735998: Motion Detection video clips are not generated.
- Mantis 0731858: Fix quotad race condition that can create 10-15 sec gaps in video recordings
- Mantis 0738209: Fix TCP 3012 using older SSL and TLS versions by providing CLI option

```
config system global
    set strong-crypto-notification enable/disable
end
```

- Mantis 0739775: Fix potential illegal memory access
- Fix memory leak in discoverd when there are no cameras to be discovered.
- Fix passive FTP transfer support.
- Fix possible SNMP daemon crash.

Vulnerabilities

- Mantis 0724735: [ffmpeg] precaution update.
- Mantis 0744282: OpenSSL 1.1.1l security fixes -- August 2021

Known issues

- Mantis 0678482: MD50B / CB50 in error state, FRC unable to communicate with camera

  With Safari 14, the console window may not use the full browser window. Resizing the browser window will correct this.

Firmware Upgrade/Downgrade Information

Upgrading from earlier versions

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

Note: If v6.0.0 or later installation is planned, it is essential to perform a 2.7.x backup in order to keep a downgrade path. See details on downgrading below.

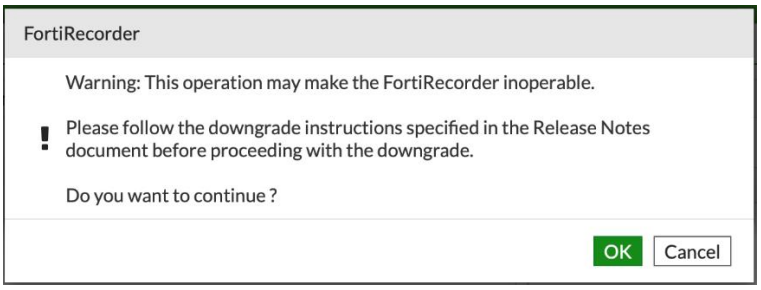
Upgrading to v6.4.1 from v2.7.x is fully supported. For earlier versions a consecutive upgrade to v2.7.6 is recommended.

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.

When downgrading from v6.0.0 and later to a previous version, a warning message will appear in GUI / CLI as it is necessary to perform manual steps:



Using the CLI, the first step is to allow empty passwords.

```
# config system password-policy
set status disable
set allow-admin-empty-passwd enable
end
```

The admin account passwords need to be reset to the default empty password.

```
# config sys admin
edit admin
        unset password
Current password for 'admin':
end
```

The video spool disk needs to be downgraded to the format used prior to v6.0

```
# execute camera downgrade-spool
This operation will stop all recordings, stop quota enforcement, and
downgrade the requested video spool(s). Recordings will not restart and
the NVR must be rebooted, either with a reboot command or by installing
```

firmware. If the NVR is rebooted or up-to-date firmware is installed,
the video spool(s) will be upgraded again.
If this command fails, a reboot is recommended.

*Do you want to continue? (y/n)***y**

local downgrade OK

The camera passwords need to be reset.

exec camera password-reset
This command will reset passwords for all managed cameras to factory default.
*Do you want to continue? (y/n)***y**
camera cam1 password reset started
camera cam2 password reset started
...

Perform the firmware downgrade (will reboot).

Restore the 2.7.x configuration backup.

When downgrading from v2.7.4 and later to a previous version, a warning message will appear in GUI / CLI as passwords used for streaming authentication are different. This message will provide instructions on how to reset passwords.

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 licensing 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.

ONVIF cameras

Licensing

FortiRecorder supports using ONVIF compliant cameras from third-party vendors.

In order to enable third-party support for a camera channel use the following license SKUs:

- FRC-EXC-1 – adds third-party support to 1 camera channel
- FRC-EXC-5 – adds third-party support to 5 camera channels
- FRC-EXC-10 – adds third-party support to 10 camera channels
- FRC-EXC-20 – adds third-party support to 20 camera channels

These licenses are stackable and perpetual. They do not add to the maximum number of cameras, but enable third-party support for existing cameras.

Trial License

Each FortiRecorder comes with one third-party channel available for free evaluation when no license is installed.
It is recommended to use this in order to confirm compatibility with the specific ONVIF camera model.

Face Recognition AI

Licensing

All FortiRecorder models except FRC-100D can be licensed to run Face Recognition analytics.

It requires an active ‘FortiGuard AI DB service’ SKU.

The license activates up to two analytics channels for appliances and theoretically unlimited for VM installations, although CPU load will restrict the usable number.

If the license is expired or invalid, only the last 7 days of Face Recognition data (Face Cluster, Face Timeline, Events, and Activity) will be displayed.

Activation of the license requires Internet access for the recorder.

After initial license verification and analytics module download the face recognition is working without Internet connection for the duration of the license.

Trial License

Each FortiRecorder (except FRC-100D) comes with one face recognition channel available for trial. It is limited to a 7-day history and requires Internet access for downloading the analytics module.

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.

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

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

   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). If Remote storage is attached as a NAS, then this extra bandwidth hs to be considered (depending on video input and storage options). A separate the network on a dedicated port is recommended.

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 FortiCentral or a 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/F can support up to 64 cameras depending on the configuration. The FortiRecorder-100D is suitable for max 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 bandwidth 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 versus Constrained 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.

Constrained bitrate mode is a combination of variable and constant bitrate modes. The profile settings are resolution, framerate, video quality and max bitrate. This will allow the camera to adjust the bitrate to achieve the desired quality level, but not higher than the max bitrate.

For cameras that support this mode it is an ideal combination that can guarantee a certain retention time like the constant mode while not wasting bandwidth and only using the needed rate like the variable mode.

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. For H.265 multiply the bitrates with a factor of 0.5-0.75.

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	60 Mbps	60 Mbps	60 Mbps
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
FRC-400F	200 Mbps	155 Mbps	160 Mbps	140 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*.