FortiRecorder™ v2.6.2 GA

Release Notes

FortiRecorder v2.6.2 GA Release Notes

July 4th, 2018

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 v2.6.2 release build 598. 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 v2.6.2:

- 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 (pending release)
- FortiCam-OB20 Network Camera
- FortiCam-OB30 Network Camera
- FortiCam-FD20 Network Camera
- FortiCam-FD20B Network Camera (pending release)
- FortiCam-FD40 Network Camera
- FortiCam-CB20 Network Camera
- FortiCam-SD20 Network PTZ Camera
- FortiAPCam-214B Network Camera and Access Point

Summary of new features

The following is a list of the enhancements in FortiRecorder v2.6.2:

- Improvements
- Bug fixes

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 20, 25, 38

  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 40 or higher
- Safari 9 or higher
- Chrome 45 or higher
- Adobe Flash Player 9 or higher plug-in required to display statistics charts
- QuickTime plugin required for viewing v2.3 and older video in web UI.

  Note: Apple OSX 10.11 and Chrome above 39 stopped support for QT

  Note: The latest QuickTime version does not install the web plugin by default

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 v2.6.2 in connection with FortiRecorder Central v1.7.

Using FortiRecorder Central v1.6 is supported, but may have some limitations.

FortiRecorder v2.6.2 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 v2.6.2 release.

As this is a patch release only bug fixes and improvements have been added.

Improvements

- Support new camera FCM-FD20B (FD20 gen2)

Bug fixes

- Mantis: #495006 Disabling continuous recording for ONVIF camera can freeze GUI
- Mantis: #500428 Fix a scheduler deadlock
- Mantis: #499138 Edge Recordings disappear from timeline
- Mantis: #496602 Security issues found in PCI audit
- Mantis: #495241 Handle ONVIF cameras with null vendor names
- Mantis: #492873 Fix quotad deletion to keep up with incoming data
- Mantis: #491422 The notification does not contain any preview of the detection or link in the notification itself.
- Mantis: #491706 Fixed 400D CPU temperature monitoring, failing to retrieve CPU temperature information.
- Mantis: #490073 Retention information is missing or wrong.

Firmware Upgrade/Downgrade Information

Upgrading from earlier versions

Upgrading to v2.6.2 from 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 v2.6.2 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.

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 mDNS multicast packets between the camera network and the NVR network in order for the NVR to automatically discover the cameras. Once the cameras are discovered, you can leave the address mode as DHCP or change it to static.

If the routers are not configured to pass the mDNS packets, the cameras can be configured manually by selecting the static address mode on the camera configuration page.

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 motion clips being received and the number of associated snapshots being generated for display in the event monitor.

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.

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*.