



# FortiCentral v6.0.0 GA Release Notes



## FortiCentral v6.0.0 GA Release Notes

March 11<sup>th</sup>, 2020

Copyright© 2020 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](https://docs.fortinet.com)  
[kb.fortinet.com](https://kb.fortinet.com)  
[support.fortinet.com](https://support.fortinet.com)  
[training.fortinet.com](https://training.fortinet.com)  
[fortiguard.com](https://fortiguard.com)  
[techdocs@fortinet.com](mailto:techdocs@fortinet.com)

# Table of Contents

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Supported models .....	5
Summary of new features .....	6
<b>Special Notices</b> .....	<b>8</b>
FortiRecorder firmware for FortiCentral .....	8
Installation Information .....	8
<b>New Features</b> .....	<b>9</b>
Privacy AI filter .....	9
Nearby cameras .....	11
Scratch panes and hotspot .....	12
LDAP and RADIUS wildcard users .....	13
ONVIF fisheye custom dewarp lens .....	14
Usability Improvements .....	15
<b>Firmware Upgrade/Downgrade Information</b> .....	<b>19</b>
Upgrading from earlier versions .....	19
Downgrading to earlier versions .....	19
<b>Performance Guidelines</b> .....	<b>20</b>
Camera profiles .....	20
<b>Image Checksums</b> .....	<b>21</b>

# Change Log

Date	Change Description
2014-12-02	Initial release.
2015-03-05	V1.1 GA
2015-07-09	V1.2 GA
2016-02-25	V1.3 GA
2016-06-10	V1.4 GA
2016-08-05	V1.4.1 GA
2016-12-22	V1.5 GA
2017-04-21	V1.6 GA
2018-02-09	V1.7 GA
2018-08-08	V1.7.1 GA
2019-01-24	V1.8.0 GA
2019-05-27	V1.9.0 GA
2020-03-11	V6.0.0 GA

# Introduction

This document provides a summary of enhancements, installation instructions, deployment scenarios and performance guidelines for FortiCentral v6.0.0 release build 0012. Please review this document before installing or upgrading FortiCentral.

For more information, see the FortiCentral User Guide available at <http://docs.fortinet.com/fortirecorder/admin-guides>. Search for “FortiRecorder Central” or “FortiCentral”.

**Note:** FortiRecorder Central has been renamed to FortiCentral with v1.7.0 GA release.

## Supported models

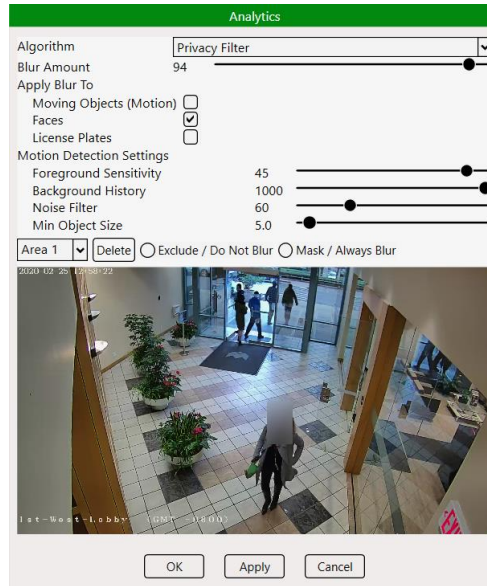
The following models are supported in FortiCentral v6.0.0:

- FortiRecorder-400F Network Video Recorder with 1x3TB (4x6TB 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)
- FortiCam-20A Network Camera
- FortiCam-MB40 Network Camera
- FortiCam-MB13 Network Camera
- FortiCam-MD20 Network Camera
- FortiCam-MD40 Network Camera
- FortiCam-MD50 Network PTZ 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 PTZ Camera
- FortiAPCam-214B Network Camera and Access Point

## Summary of new features

The following is a list of enhancements in FortiCentral v6.0.0:

- Privacy AI filter



- Nearby cameras
  - Quick following of persons around a site between cameras.
- Scratch panes and hotspot
  - Panes can be assigned different attributes that define their role or behavior on the desktop.
- LDAP and RADIUS wildcard users
- ONVIF fisheye custom dewarp lens
- Usability Improvements
  - Auto hide unused categories on the left side of main window
  - Added Live Recording for direct client based evidence extraction
- GUI enhancements
  - Added FortiGate theme Green and Blue for consistent look across Fortinet products. It is the default theme for new installations.
  - Delay for Waiting spinner symbol will adjust to how often frames are skipped on jittery network connections. It could delay up to 10s versus 2s for previously stable connections.
  - Improved 3D Maps chapter in Application settings. Added sector and camera count.
- System/FRC Enhancements
  - Split Video Analytics installers out of main installer to make file sizes more manageable.

- Integration into FortiDemo environment
- Feature Clip download with watermark/hash
- FortiView improvements
  - Redesigned FortiView settings dialog
  - FAZ/FMG transparent URL widget support
  - Added website FortiView connection type for any not yet supported devices

# Special Notices

## FortiRecorder firmware for FortiCentral

Starting with FortiRecorder v2.0.0 firmware release FortiCentral is supported as a Windows client for all FortiRecorder models and FortiCameras.

It is recommended to use v6.0.0 of FortiCentral with v6.x.x of FortiRecorder.

## Installation Information

For more information, see the FortiCentral User Guide.

- Enable connections to FortiCentral in the FortiRecorder Network Configuration: 'FRC-Central' access in the port interface (default).
- Connection between FortiRecorder and FortiCentral via TCP 8550 (configurable)
- After initial login admin/blank create a new admin with new password and add recorder connections in Settings.
- The user credentials presented for logging into FortiCentral are used to log into the connected recorders. Therefore the local user account must be configured at the recorder as well for successful authentication. As an alternative a fixed login can be configured per recorder.
- FortiCentral does not require a plug-in to decode and display video from FortiCameras.
- To view video drag camera from device panel into pane.
- Fortinet recommends setting your monitor to a screen resolution of 1920x1080. This allows for sufficient desktop space so multiple videos can be viewed properly.

**Note:** Video analytics require a 64bit Windows version, so FortiCentral v6.0.0 is available in 32bit and 64bit versions.

Each analytics module is available as a separate file which should be placed in the same folder as the main installer.

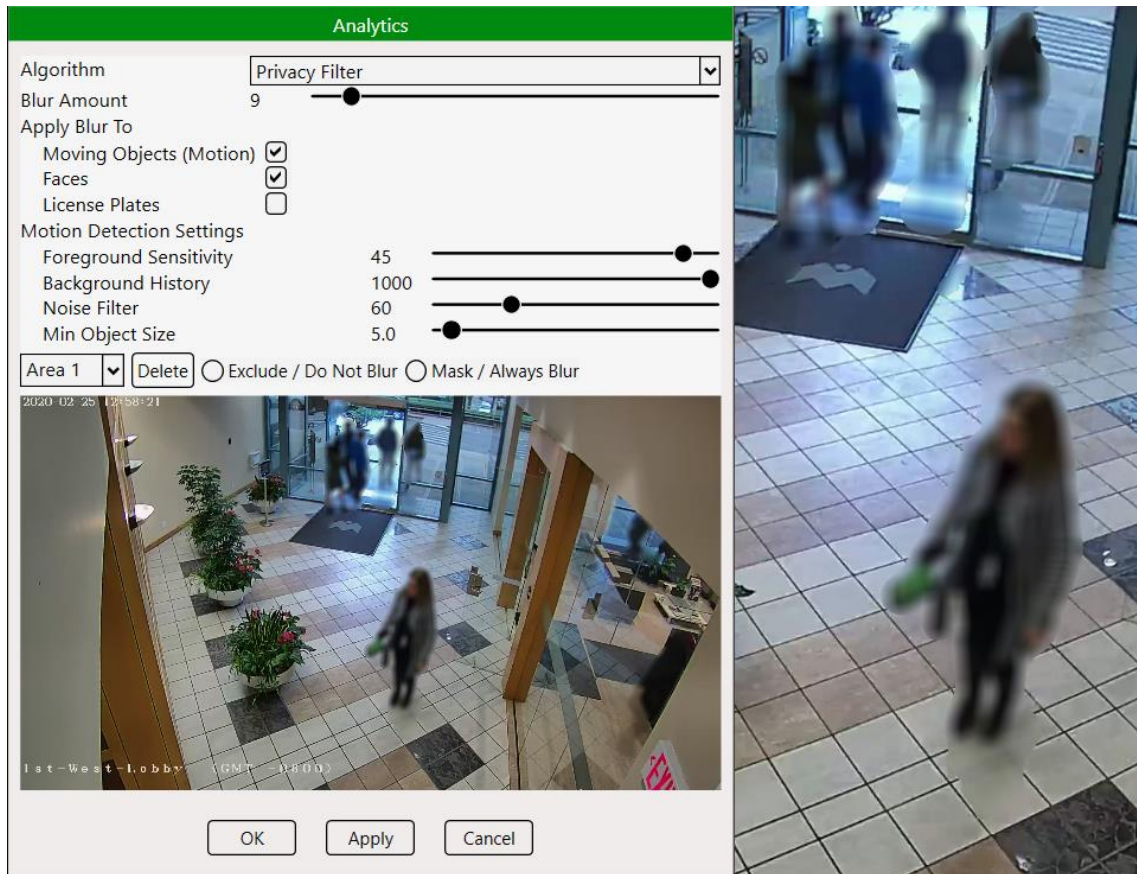
If the main installer detects analytics packages it will ask whether to install each of them.

# New Features

The following section highlights new features in the FortiCentral v6.0.0 release.

## Privacy AI filter

For situations that should conceal the identity of a person while still showing activity, a privacy AI filter has been added to the FortiCentral analytics family. In addition to the face recognition and object detection filter a 'Privacy filter' is now available from the Analytics pane menu.



**Blur Amount:** How strong the blurring is applied. From only a slight blur to complete hiding

**Apply blur to:** The AI detects faces and license plates, that can selectively be blurred. This still allows to see the rest of a person or car. Selecting 'Moving objects' covers everything moving.

**Motion detection settings:** Similar to the settings in the object detection analytics dialog this allows to adjust what kind of motion should be considered.

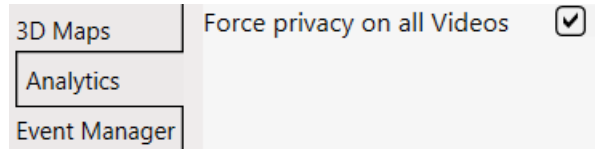
- **Foreground Sensitivity** is how easy a change in parts of the image is detected.
- **Background History** adjusts how long it takes for a no longer moving object to be considered background.
- **Noise filter** determines how strong scattered and temporary detections are filtered out.
- **Min object size** allows excluding small noise sources.

**Areas** are polygons that can define parts of the image as either permanently blurred or permanently clear. This is useful if e.g. a workspace is in the camera view and the person needs to be blurred out, but the work surface should be visible.

Privacy processing applies to live and playback video as well as the Snapshot function on a video pane.

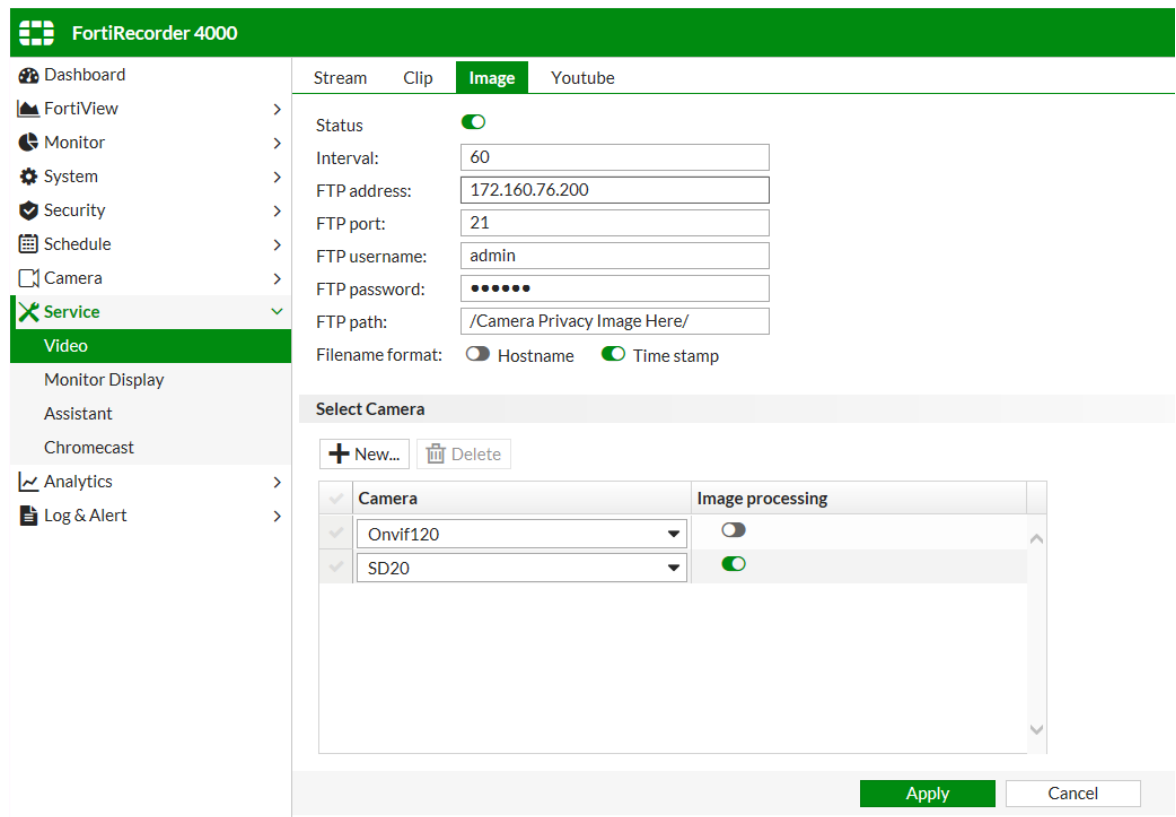
Privacy filter is part of stored views like the other analytics. So a startup view can contain several camera views with privacy enabled. If the user is an operator or viewer (not administrator), then the privacy masking can be enforced by restricting to views with privacy masking only.

In order to force privacy masking on all video panes set a global flag in Application settings- Analytics.



FortiCentral privacy image processing can be combined with the FortiRecorder FTP upload service to send anonymized images (e.g. of public places) to a FTP server. This allows anonymized webcam pictures on websites.

The configuration for this is done on Fortirecorder in the Service-Video-Image section.



**Status:** Enables or disables the FTP uploads

**Interval:** Time between snapshots in minutes.

**Select camera:** Put all cameras from which you want snapshot uploads into this list.

**Image processing:** Enable this feature to use processed images from a FortiCentral that is connected to this recorder.

Note that FortiCentral will retrieve these settings from a connected recorder and send privacy processed snapshots at the chosen interval, but it requires that the cameras are run in a pane with the privacy analytics active. This can best be achieved at program startup with a view that contains the required camera processing panes.

## Nearby cameras

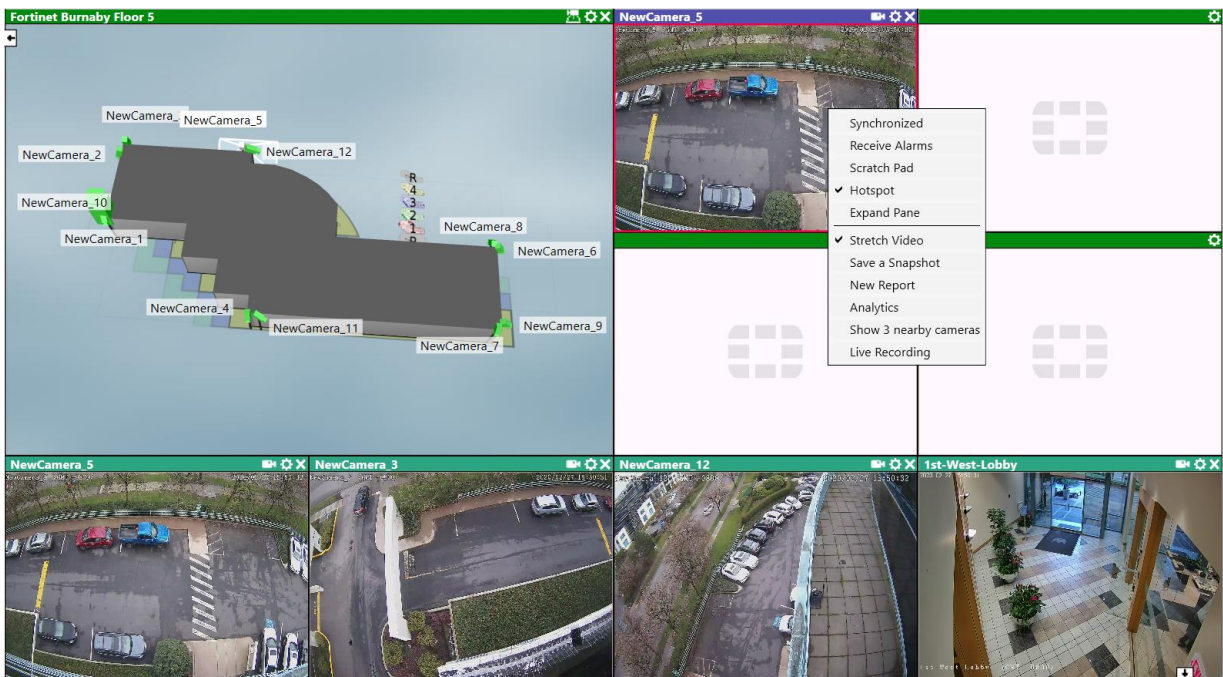
Following a person or a car around a site is a common surveillance task. For an operator it is difficult to quickly switch between cameras when the subject leaves the field of view of one camera and walks into the next. Sometimes it is not clear on which out of several options the subject will appear next

Nearby cameras make this task much easier by predefining cameras that are 'close' to another.

The feature works from the pane menu or directly on a right click on live or playback video.

The screenshot below shows a group of nearby cameras in the bottom row.

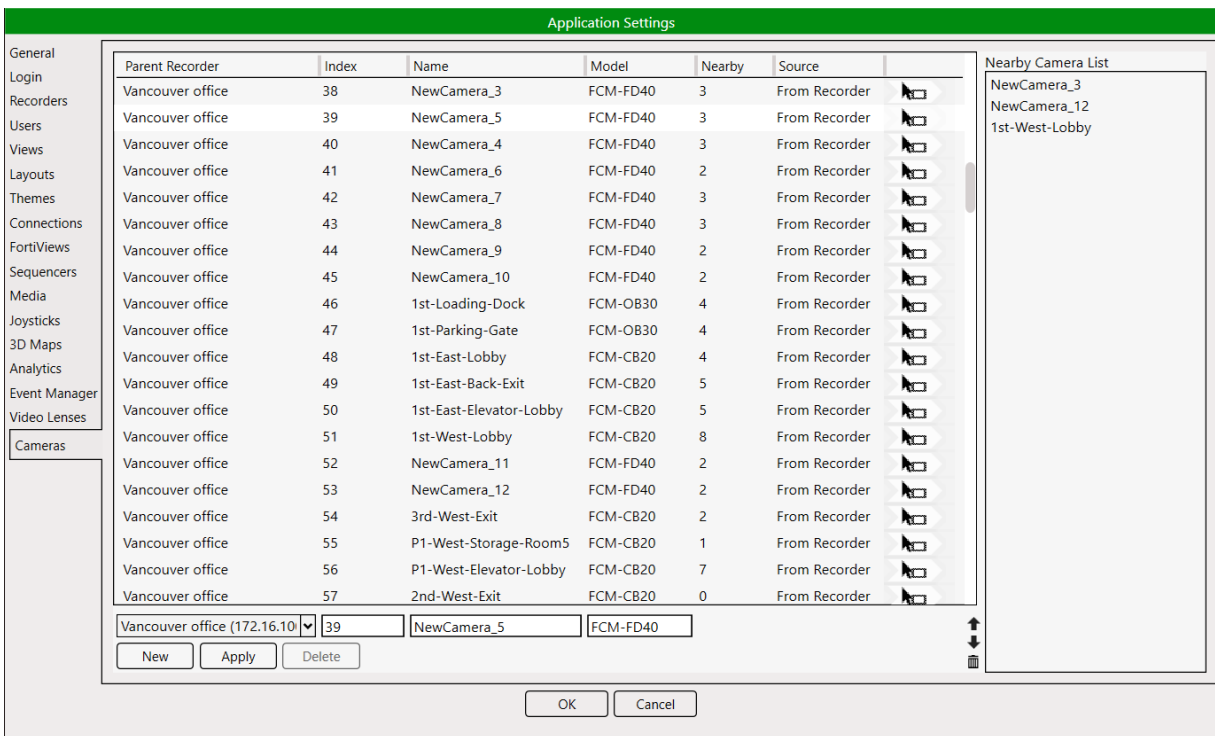
By default the source camera and its nearby cameras are switched to empty panes on the layout, but it is preferred to use the scratch pad pane feature to show the group of cameras in a defined part of the screen layout.



Nearby cameras are defined in Application Settings-Cameras. The table shows all cameras from current or previously connected FortiRecorders. To add nearby cameras select the camera in the table and drag other cameras by the drag symbol into the list of nearby cameras to the right. It is possible to change the order of nearby cameras and delete entries.

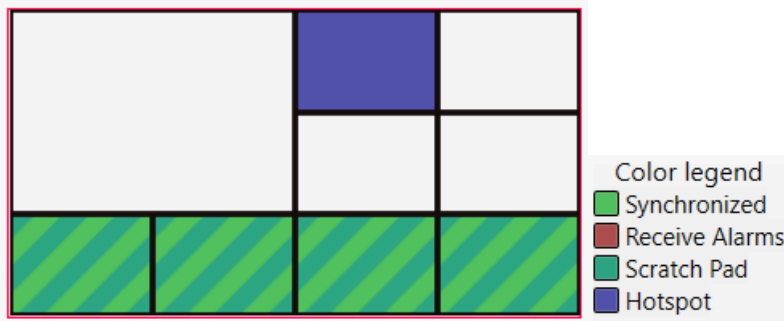
The table can be sorted by clicking on the column heads.

Note: It is also possible to define new cameras, that are matched by index with physical cameras on a recorder upon a later connection. This is useful for preparing a project before installation.



## Scratch panes and hotspot

Panels can be assigned different attributes that define their role or behavior on the desktop.

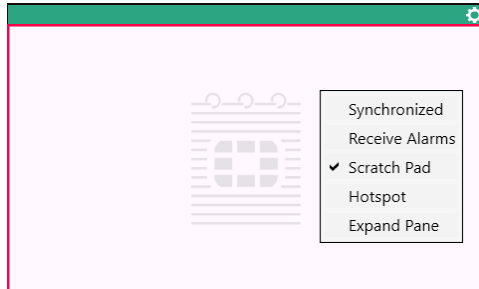


Two new attributes have been added:

- A **Hotspot** pane is used to quickly show video from a camera by just hovering over its entry in the device tree or on its icon in the 3D maps. No drag or click is required, to see the camera view thus giving no-touch overview. There can only be one hotspot pane on a desktop.
- **Scratch** panes are designated places where requested camera views are displayed. This can be requesting nearby cameras or clicking on event or face recognition manager entries.  
The group of scratch panes manages the displayed cameras intelligently. New requests are added at the top left. Older content is shifted down and duplicates removed. This allows to see the current request at the top while not losing older selections if possible. This works particularly well with the nearby camera feature in order to follow a person around multiple cameras. Simply right click on the pane that shows the person and select "Show nearby cameras". The pane with the person moves to the front and all possible next cameras are displayed after that. Once the person shows on another camera repeat the process.

**Note** that it is possible to combine the synch and scratch attributes, therefore allowing to do the same process in playback where all playbacks in the scratch group are synchronized – showing the same moment in the past. This allows to easily follow a person through recordings on multiple cameras.

Configuring a pane as hotspot or scratch pane can be done directly from the pane menu or using a right click.



Views can also be used to recall a specific pane organisation including the hotspot and scratch attributes, therefore allowing individual work surfaces preconfigured for different tasks.



## LDAP and RADIUS wildcard users

FortiCentral now supports LDAP and RADIUS wildcard users. The feature is available for user entries in Application settings - Users. If the login type is LDAP or RADIUS, then wildcard can be checked.

During login the username will be compared to all regular users. If it is not found the wildcard users will be tried. This means the username and password is tested against the LDAP or RADIUS server.

This avoids having to maintain a list of all users on FortiCentral and use a centralised directory in LDAP or RADIUS instead.

Note that RADIUS supports PAP auth only.

User is LDAP/RADIUS wildcard	<input checked="" type="checkbox"/>	<input type="text"/>
User Type Attribute		<input type="text"/>
May Control Other Clients Attribute		<input type="text"/>
Startup View Attribute		<input type="text"/>

LDAP type login supports user properties. The user type, remote control attribute and the startup view can be retrieved from the LDAP directory individually for each user.

User type: Admin/Operator/Viewer  
Control: True/False  
Startup View: Name of a valid view for the user

## ONVIF fisheye custom dewarp lens

Fisheye lenses are different for each camera model. FortiCentral supports third party fisheye cameras and now allows defining matching dewarping algorithms.

Custom video lenses are managed in Application settings-Video lenses. Here you can create, rename and save video lenses.

Type	Name
<input checked="" type="checkbox"/> Fisheye Lens	FCM-FE120
<input type="checkbox"/> Fisheye Lens	Generic lens

Name:

Size:

Offset:

PTZ

Center:

Edge:

Panorama

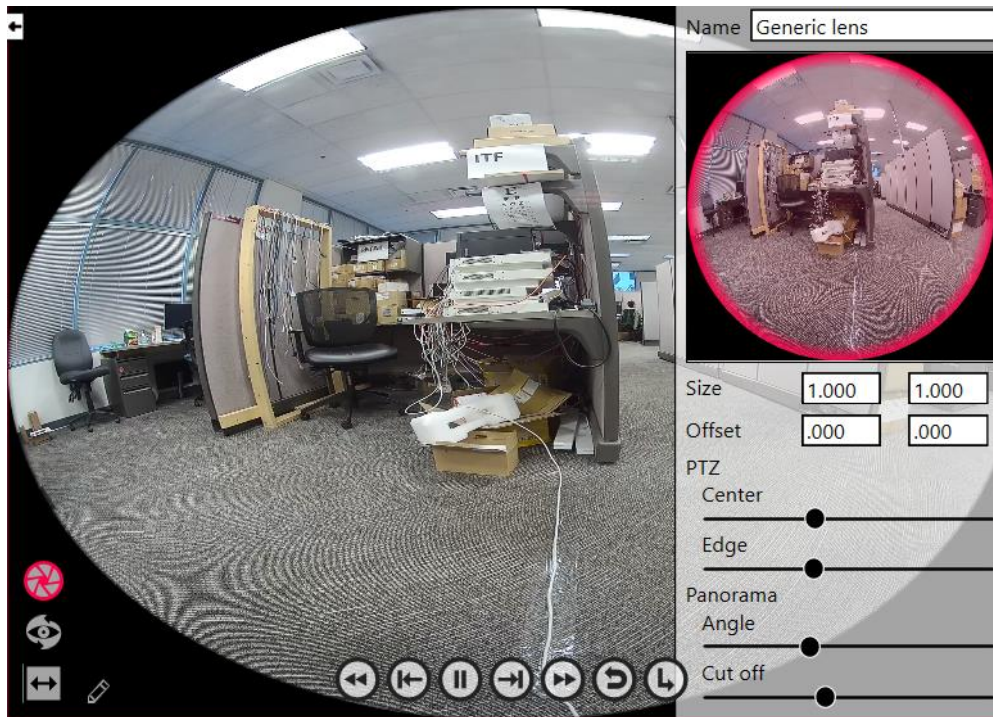
Angle:

Cut off:

New Apply Delete

OK Cancel

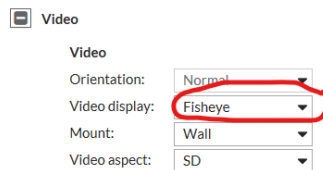
The adjusting of the parameters is done from the video pane menu by showing video from a fisheye camera, selecting the new video lens from the pane menu and clicking the edit pencil symbol.



Now it is possible to adjust the lens to the cameras fisheye geometry. Depending on which mode (fisheye/PTZ/Panorama) is selected, different parameters can be adjusted. These are shown in red.

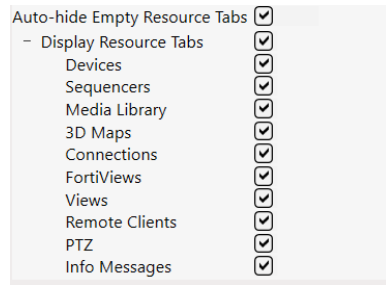
- Cut out the black fringe by adjusting the **ellipse** around the field of view. To fine tune this setting enter numerical values for x/y size and Offset.
- **Center** stretches the middle of the image in PTZ mode.
- **Edge** stretches the outer area of the field of view in PTZ mode.
- **Angle** allows levelling the horizon if a camera is wall mounted in panoramic mode.
- **Cut off** removes the top and bottom from a panoramic view

Note: To make a ONVIF camera show as fisheye camera in FortiCentral set the Video Display for that camera to fisheye or panoramic in the FRC camera configuration. Also Mounting info (wall/ceiling/table) needs to be transferred to FRCC:

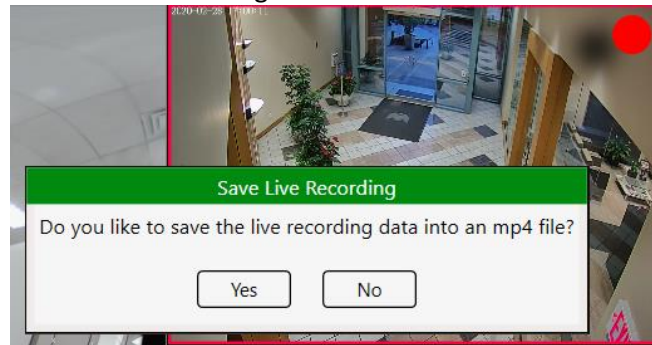


## Usability Improvements

- |         |   |
|---------|---|
| Feature | Added autohide to remove unused categories on the left side of main window<br>Enable and override in general settings |
|---------|---|



Feature Added Live Recording for direct client based evidence extraction

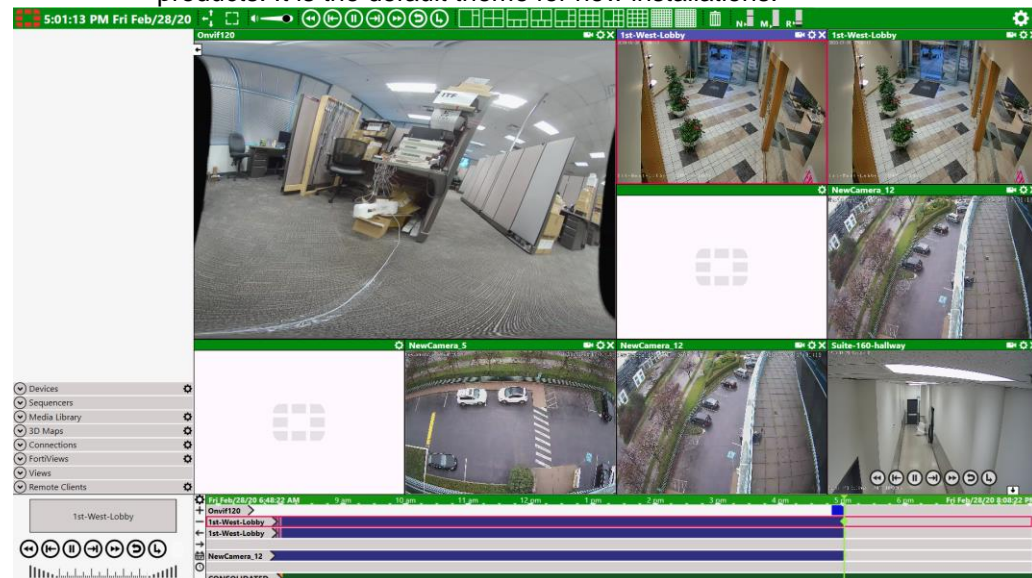


Fix Suppress PTZ flag for some ONVIF that report it in error by disabling PTZ in camera configuration management

Fix Auto resolution improvement for multiple displays with different resolutions. Now switches between streams independent of screen size and resolution. Also sequencers properly switch now if Auto resolution is globally set.

## GUI enhancements

Feature Added FortiGate theme Green and Blue for consistent look across Fortinet products. It is the default theme for new installations.



Feature Delay for Waiting spinner symbol will adjust to how often frames are skipped on jittery network connections. It could delay up to 10s versus 2s for previously stable connections.

Feature Improved 3D Maps chapter in Application settings. Added sector and camera count.

## System/FRC Enhancements

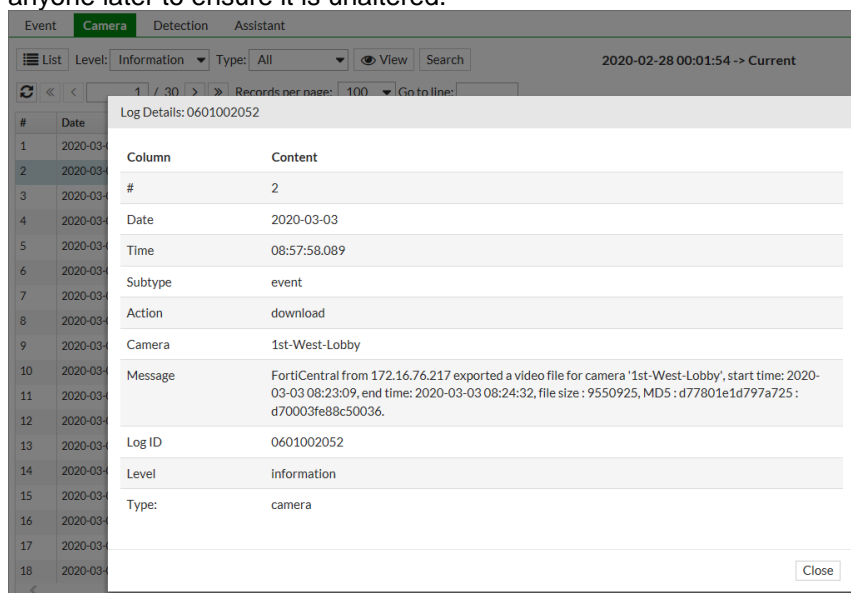
Feature Split Video Analytics installers out of main installer to make file sizes more manageable. During setup of the 64bit version the installer will detect and offer all analytics that are found in the same directory as the installer itself.

```
FortiCentral_Setup_x64_6.0.0008.exe  
FortiCentral_Setup_x86_6.0.0008.exe  
FortiCentral_VideoAnalytics_FaceDetection_x64_6.0.0008.exe  
FortiCentral_VideoAnalytics_ObjectDetection_x64_6.0.0008.exe  
FortiCentral_VideoAnalytics_VideoPrivacy_x64_6.0.0008.exe
```

Feature Integration into FortiDemo environment

Feature Clip download with watermark/hash

When a video clip is downloaded from a recorder the MD5 hash of the video clip is stored in the recorder log. This can be used to verify authenticity of the clip by anyone later to ensure it is unaltered.



```
C:\Users\rwestendorp>certutil -hashfile "C:\Users\rwestendorp\Downloads\  
1st-West-Lobby 2020-03-03 08h23m09s 2020-03-03 08h24m32s.mp4" MD5  
MD5 hash of C:\Users\rwestendorp\Downloads\1st-West-Lobby 2020-03-03 08h  
23m09s 2020-03-03 08h24m32s.mp4:  
d77801e1d797a725d70003fe88c50036  
CertUtil: -hashfile command completed successfully.
```

Fix Auto login with LDAP/Radius authentication fails

Fix Improved error displays when event manager fails to get events.  
Now names the cameras that are causing the issue.

Fix Bulk download was not updating time under some circumstances

Fix Event manager will no longer search for cameras it knows do not exist

Fix Playback based object detections appear at the time of the original recording now.

## FortiView improvements

- Feature Redesigned FortiView settings dialog
- Feature FAZ/FMG transparent URL widget support
- Feature Added website FortiView connection type for any not yet supported devices – different from media element URL which is only a static snapshot.
- Feature Added FortiView support for FRC
- Fix FortiGate dashboards not loading properly
- Fix Added support for https connections to different clients under same IP, but different port
- Fix Optional suppression of HTTPS cert warning on command line `--no-ssl-warning`
- Fix Fixed login issue for FAZ.
- Security fix Add support for POST login on Recorder and FortiMail

# Firmware Upgrade/Downgrade Information

## Upgrading from earlier versions

Upgrading FortiCentral to v6.0.0 from v1.9.0, v1.8.0, v1.7.1, v1.7 or v1.6 is fully supported.

**Note:** FortiCentral v1.5 and later does not support the GUI console feature in FortiRecorder versions 2.3.0 and older.

**Note:** Upgrading to v1.6 from v1.4x or earlier is not fully supported (upgrade to v1.5 first).

Fortinet always recommends backing up the configuration before performing an upgrade. The configuration file is located at  
c:\ProgramData\Fortinet\FortiRecorderCentral\ and renamed upon upgrade to a new version  
e.g. FortiRecorderCentral.exe.SettingsV4.xml

The configuration can be exported from the Settings menu.

## Downgrading to earlier versions

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

**Note:** Downgrading to an earlier version may revert to the configuration that was left when the upgrade occurred. So all changes to the configuration since then are lost.

# Performance Guidelines

Video playback is very CPU intensive. If you are experiencing choppy video playback and cameras “freezing” during playback, you may have a client performance problem. Use the diagnostic tools available in FortiCentral to narrow down the problem.

In the toolbar area are performance meter symbols that show

- **Network bandwidth of incoming data and frame skip rate**  
If a recorder cannot send out video streams fast enough it will start skipping frames. If this occurs the bar turns yellow and then red. It is an indication that the network bandwidth is too low to support the number of video streams that are currently displayed.
- **Memory usage**  
Shows how much memory the application is using. The total amount of available memory is indicated as well in the tooltip.
- **Rendering performance**  
Indicates how many MPixels are decoded per second. A 1MP image at 30fps requires 30MPixel/s for example. If more video is displayed in FortiCentral the performance limit of the PC will eventually be reached. At this point the video decoder has to drop frames to keep up with the incoming video stream. This drop rate is displayed at the tooltip and if it occurs the bar turns yellow and red in more severe situations. This indicates that the CPU/graphics performance of the PC where FortiCentral is running has reached its limit.

The performance bottleneck in a FortiCamera deployment will likely be the client, which must decode and render the video streams from the NVR. Displaying multiple video streams on the client is very CPU intensive.

## Camera profiles

If you need to display 8 or more camera live views, you may need to configure the camera stream so that viewing is done at a lower frame rate or resolution, depending on how powerful the client PC is.

To optimize client performance, use the video and camera profiles to define and assign a video stream for each camera. To increase the number of live and playback 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 related video streams.

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

FortiCentral v1.3 and higher can use either of the live or recording streams configured in the recorder for display. Playback always accesses the recording stream.

# 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. At the top is the Fortinet logo and navigation menu with links for Home, Asset, Assistance, Download, and Feedback. A user profile icon and 'LOG OUT' button are on the right. Below the navigation is a blue banner with 'Home', 'Welcome', and a note about time zones. A red 'About To Expire' badge with the number '1' is in the top right corner. The main content area features a 'Customer Support Bulletin' with three items and a 'More' button. Below this are sections for 'Asset' (Register/Renew, Manage Products) and 'Assistance' (Create a Ticket, Manage Tickets, View Active Tickets, Technical Web Chat, Contact Support). At the bottom, there are 'Download' buttons for Service Updates, Firmware Images, and Firmware Checksums (highlighted with a red box), and a 'Quick Links' section with links to Forti-Companion, Tickets Creation Guide, Product Life Cycle, and CSS Reference Guide.

