Administration Guide

FortiRecorder 6.4.6

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

April 16, 2025
FortiRecorder 6.4.6 Administration Guide
00-646-1149362-20250416

TABLE OF CONTENTS

Change log **8**
Key Concepts **9**
FortiRecorder NVR 9
Third-party camera support 10
Deployment scenarios and camera discovery 10
Local camera deployment 10
Remote camera deployment 11
Performance guidelines 11
FortiRecorder performance 11
Client Performance 14
Licenses 15
Third-party camera licenses 15
Face recognition AI license 15
FortiRecorder-VM licenses 16
Quick Setup Guide **17**
Directly connecting cameras to the FortiRecorder 17
Connecting cameras through a DHCP server 19
Setting up the System **21**
Connecting to the FortiRecorder Web UI 21
Connecting to the FortiRecorder CLI 22
Configuring the FortiRecorder 23
Setting the "admin" account password 24
Configuring the network settings 24
Configuring the DHCP server 29
Setting the system time 31
Advanced FortiRecorder Configuration 32
Configuring system timeout, ports, and public access 32
Creating FortiRecorder logical interfaces 33
Customizing the system messages, email templates, and UI appearance. 34
Customizing email templates 35
Customizing the user interface appearance 35
Configuring Logging 35
Configuring Alert Emails 37
Updating the Firmware 38
Installing FortiRecorder firmware 39
Installing alternative firmware 41
Booting from the alternate partition 42
Upload licenses 43
Using the Dashboard **44**
Reviewing System Status 44
Customizing Widgets 44
Using the CLI Console 44

Utilizing FortiView **46**
Monitoring Camera Statistics 46
Viewing bandwidth statistics 46
Viewing Top Camera Usage 47
Analyzing Advanced Statistics 48
Viewing Sessions 49
Analyzing the Topology 49
Video Monitoring **50**
Event Analyzing 50
Viewing the event time frame 50
Viewing the Event List 51
Viewing Video 51
Understanding the time line 51
Viewing live video 52
Viewing recorded video 52
Reviewing Camera Notifications 53
Analyzing Logging 54
Understanding and using logs 54
Reviewing logs 57
Monitoring Face Recognition 59
Monitoring DHCP Status 59
Reviewing Security Information 59
Modifying System Settings **61**
Configuring Network Settings 61
Configuring the interface 61
Configuring routing 64
Configuring DNS settings 65
Configuring the DHCP server 66
Using traffic capture 68
Creating and Modifying Administrator Accounts 69
Configuring an administrator account 69
Configuring admin profiles 71
Configuring access control 73
Configuring System Settings 73
Establishing the Time 73
Configuring system options 74
Configuring mail server settings for notification emails 75
Configuring FortiRecorder to send SMS messages 76
Configuring SNMP traps and queries 77
Customizing FortiRecorder and Messages 82
Customizing replacement messages 82
Customizing email templates 84
Customizing the user interface appearance 84
Customizing Single Sign On 85
Configuring Data Storage on the FortiRecorder 85
Configuring local storage 86
Configuring external storage 88

Configuring LDAP and RADIUS Authentication 90
Configuring RADIUS authentication 90
Configuring LDAP Authentication 91
Working with Certificates 94
Supported cipher suites & protocol versions 95
Replacing the default certificate for the web UI 96
Uploading trusted CAs' certificates 101
Revoking certificates 103
Revoking certificates by OCSP query 104
Performing System Maintenance 104
Backing up configuration 105
Restoring configuration 105
Downloading the trace log 105
Security Monitoring 106
Configuring Intrusion Detection 106
Configuring Schedules 108
Establishing a Schedule 108
Setting the Sunrise and Sunset Time 109
Modifying Camera Settings 110
Configuring Cameras 110
Configuring video profiles 110
Configuring camera profiles 112
Configuring cameras 114
Creating camera groups 122
Upgrading or downgrading camera firmware 122
Using DIDO terminal connectors on FortiCam MB13 cameras 122
Configuring Cameras to send Notifications 123
Configuring Video Services 125
Configuring Video 125
Establishing video sharing 125
Retrieving video clips 126
Establishing image sharing 126
Streaming recorded video clips to YouTube 127
Using Monitor Display 127
Associating Cameras with a Virtual Assistant 128
Associating a Camera with Amazon Alexa 128
Using Chromecast to Stream Content 128
Configuring Face Recognition 130
Monitoring Face Clusters 131
Reviewing known faces 131
Reviewing new faces 131
Using the Face Timeline 132
Configuring User Assets 133
Searching the user database 133
Creating a department and role 134
Assigning AI cameras and setting schedules 134

Creating a floor plan 135
Creating a Policy 136
Reviewing Analytics 137
Using Motion Detection Analytics 137
Using Computer Vision Analytics 137
Analyzing Logs and Alerts 139
Configuring Log Settings 139
Configuring Alert Email 141
Best Practices 143
Hardening Security 143
Topology 144
Administrator access 144
Operator access 145
Improving Performance 146
Video performance 146
System performance 146
Logging and alert performance 147
Packet capture performance 147
Updating and Backups 147
Regular backups 147
Restoring a previous configuration 148
System Maintenance 149
Backing up configuration 149
Restoring configuration 150
Downloading the trace log 150
Troubleshooting 151
Viewing Issues 151
Live feed delay 152
Video not being sent to the FortiRecorder 152
Using Traffic Capture 152
Notification Issues 153
Login Issues 153
When an administrator account cannot log in from a specific IP 154
Remote authentication query failures 154
Resetting passwords 154
Not able to push setting and log shows an error on password 154
Connectivity Issues 155
Checking hardware connections 155
Bringing up network interfaces 156
Examining the ARP table 156
Checking routing 156
Facilitating discovery 160
DHCP issues 160
Unauthorized DHCP clients or DHCP pool exhaustion 160
Establishing IP sessions 161
Resolving IP address conflicts 162

Packet capture 163
Resource Issues 169
Data Storage Issues 170
Removing individual video clips 170
Resetting the Configuration 171
Restoring Firmware 171
Appendices 174
Port Numbers 174
Maximum Values 175

Change log

The following is a list of documentation changes. For a list of software changes, see the FortiRecorder Release Notes.

Date	Change Description
2025-04-16	Initial release of the FortiRecorder 6.4.6 Administration Guide.

Key Concepts

This chapter defines basic FortiRecorder concepts and terms. If you are new to FortiRecorder, or new to digital video surveillance systems, this chapter can help you quickly understand how to use your FortiRecorder system.

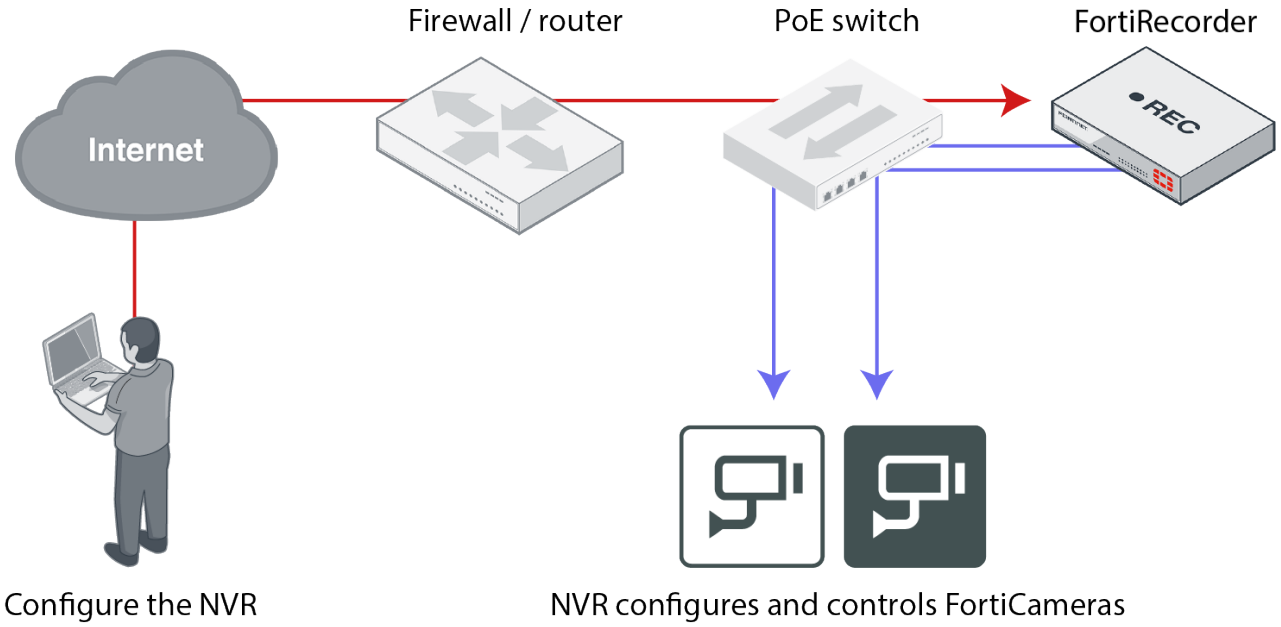
This section contains the following topics:

- FortiRecorder NVR
- Camera support
- Deployment scenarios and camera discovery
- Performance guidelines
- Licenses

FortiRecorder NVR

The FortiRecorder network video recorder (NVR) provides central management for:

- Configuring your cameras
- Recording your video feeds
- Viewing recordings and live video feeds



Third-party camera support

FortiRecorder supports Fortinet FortiCam cameras and third-party ONVIF-compliant cameras. Some features on third-party cameras might not be fully supported, however. In that case, you can configure those features through the built-in GUI on the camera.

By default, FortiRecorder allows you to connect one third-party camera. To connect more third-party cameras, please contact Fortinet or your reseller to purchase a license.

Deployment scenarios and camera discovery

There are two basic deployment scenarios for cameras:

- Local to the FortiRecorder
- Remote to the FortiRecorder

FortiCamera deployments can combine both scenarios.

Always place cameras in a separate subnet, isolated from outside to ensure only FortiRecorder can control access to and from the camera network. Use a dedicated FortiRecorder port or VPN.

Local camera deployment

Local camera deployment has two specific scenarios:

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

Installing the cameras on the same subnet as the FortiRecorder is the easiest deployment scenario, since the FortiRecorder automatically discovers the cameras.

The different FortiRecorder network interfaces can be used for different purposes:

- a management port
- a dedicated camera network
- dedicated remote storage network.

The FortiCam cameras rely on a DHCP server to provide them with an initial unique IP address. If there is no DHCP server available on the network, the FortiRecorder can be configured to provide DHCP server functionality. The camera can also be configured to use a static IP address, but the camera would require a factory reset if moved to a different subnet.

Many third-party cameras also rely on the presence of a DHCP server. Some third-party cameras may use a default IP address and require the camera to be configured with the desired network settings.

Reserve the IP address for cameras and avoid IP address changes.

A dedicated camera network provides many advantages:

- restricted access to the cameras
- video streams protected
- increased quality of service
- easier bandwidth management

FortiRecorder provides camera management in a dedicated camera network through a separate management interface. This secure gateway functionality is available for FortiCams and third party cameras.

Remote camera deployment

Remote camera deployment is for when there is a firewall between the FortiRecorder and the cameras. FortiRecorder will not be able to discover the cameras and so the cameras will need to be manually added to the FortiRecorder with the correct IP address.

The FortiRecorder can also manage cameras that are behind a firewall. As network address translation is typically used in such scenarios, a virtual IP address will be assigned to the camera by the firewall. Such a deployment is more elaborate. When possible, a secure tunnel should be used instead to strengthen security.

Performance guidelines

There are two components to consider when looking at FortiRecorder performance – the 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 FortiRecorder. Displaying multiple video streams on the client is very CPU intensive.

FortiRecorder 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 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 recorders 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 views
- The video stream parameters per camera live 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

The 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.

The 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 the 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 and frame rates) and the constant bit rate mode produces more reliable output from the cameras.

Bandwidth per camera

Variable bit rate

Depending on resolution, frame rate and video quality a camera using H.264 compression may generate the following bit rates:

- 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

Bitrate table (H.264 estimate) in Mbps with high quality image (x0.7 = standard quality):

Frames	1	6	10	15	30
CIF (352x240)	0.16	0.2	0.24	0.3	0.4
D1 0.4M (720x576)	0.4	0.5	0.6	0.75	1
720p 1M	0.8	1	1.2	1.5	2
SXGA 1.3M (1280x1024)	1	1.25	1.5	1.9	2.5
HD 2M (1920x1080)	1.6	2	2.4	3	4
3M	2	2.5	3	3.75	5
5M	3.2	4	4.8	6	8

Please note that these are estimates providing a high quality image under most conditions. If the scene is less complex (indoors with little detail and not much motion) or the camera has very little noise (daylight, good DNR) the bit rate can be lowered further. Avoid using less than half of the indicated values.

If video compression is set to lower quality or capped at a defined max bandwidth, the bit rate can be significantly lower at the cost of lower image quality. DNR can further reduce bandwidth, especially for grainy night images, but shows less detail during motion.

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

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

Storage capacity

Video retention depends on the available storage capacity and the total amount of video bandwidth from the cameras.

To calculate storage capacity, note that a 1TB HD stores 1 camera configured to consume 1Mbps for approximately 100 days.

Video retention period in days for hard drive capacities:

	FortiRecorder 100D with 1 TB HD	FortiRecorder 200D with 3 TB HD	FortiRecorder 400F with 4TB HD	FortiRecorder 200D with 3 TB HD plus 16 TB remote storage	FortiRecorder 400F with 32 TB HD
1MP@30 FPS standard video quality = 1.4 Mbps	72	218	291	1381	2327
2MP@15 FPS standard video quality = 2.1 Mbps	48	145	194	921	1551
3MP@10 FPS high quality video = 3 Mbps	34	102	136	645	1086
3MP@30 FPS high quality video = 5 Mbps	20	61	81	387	651

For more information about bandwidth consumption calculation, see the FortiCamera Bandwidth Calculator User Guide on http://docs.fortinet.com/d/fortirecorder-forticamera-bandwidth-calculator-user-guide.

In practice, Fortinet suggests to use the numbers provided in the bandwidth calculator as a starting point and then adjust them after installation to achieve the desired balance between quality and bandwidth.

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.

Ten 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).

Licenses

For more capabilities, you can purchase licenses for:

- Managing more third-party ONVIF cameras
- Face recognition AI
- Virtual machine (VM) support for large scale deployments that can grow with your organization

When you receive your licenses, register them with Fortinet Customer Service & Support, and then upload them to FortiRecorder. See Upload licenses on page 43.

If you are unsure which licenses you have installed, or whether they are valid, you can use the dashboard to verify their status.

Subscription services such as FortiCare support contracts are purchased separately.

Third-party camera licenses

FortiRecorder supports using ONVIF-compliant cameras from third-party vendors if you purchase the following SKUs and upload their licenses to FortiRecorder:

- FRC-EXC-1 for 1 third-party camera
- FRC-EXC-5 for 5 third-party cameras
- FRC-EXC-10 for 10 third-party cameras
- FRC-EXC-20 for 20 third-party cameras

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. You can use this in order to confirm compatibility with a specific third-party camera model.

Face recognition AI license

All FortiRecorder models except FRC-100D/G 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 clusters, timeline, events, and activity) will be displayed.

Activation of the license requires Internet access for FortiRecorder.

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/G) comes with a trial license for face recognition for one camera available. It is limited to a 7-day history, and requires Internet access to download the analytics module.

FortiRecorder-VM licenses

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

- FRC-VM-Base – includes 10 camera licenses
- 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.

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 are available with a trial license **except** third-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 enabled cameras. All features are available with an evaluation license **including** third-party camera support of more than one camera.

Quick Setup Guide

Once you connect the cameras to the FortiRecorder, the FortiRecorder automatically discovers the cameras. Once discovered, configure the discovered cameras.

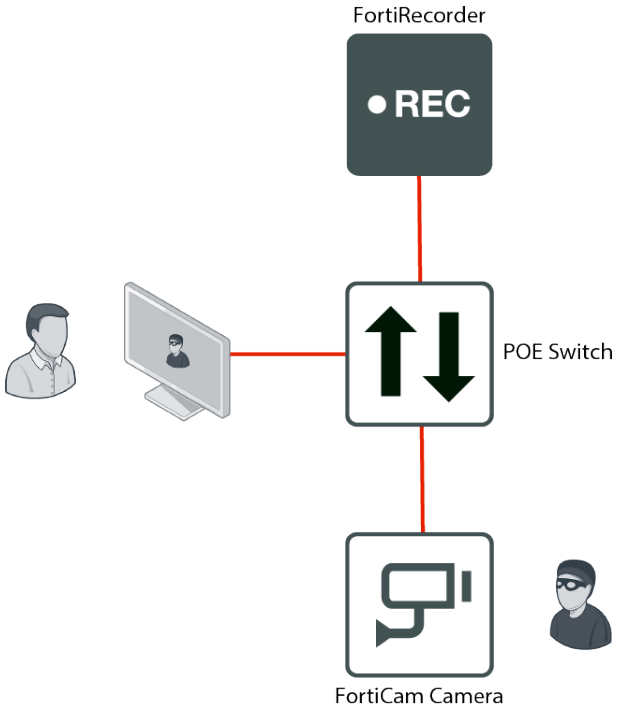
FortiRecorder supports UPnP, mDNS, and ONVIF discovery.

There are two connection scenarios:

1. Direct connection
2. Connecting through a third party DHCP server

Directly connecting cameras to the FortiRecorder

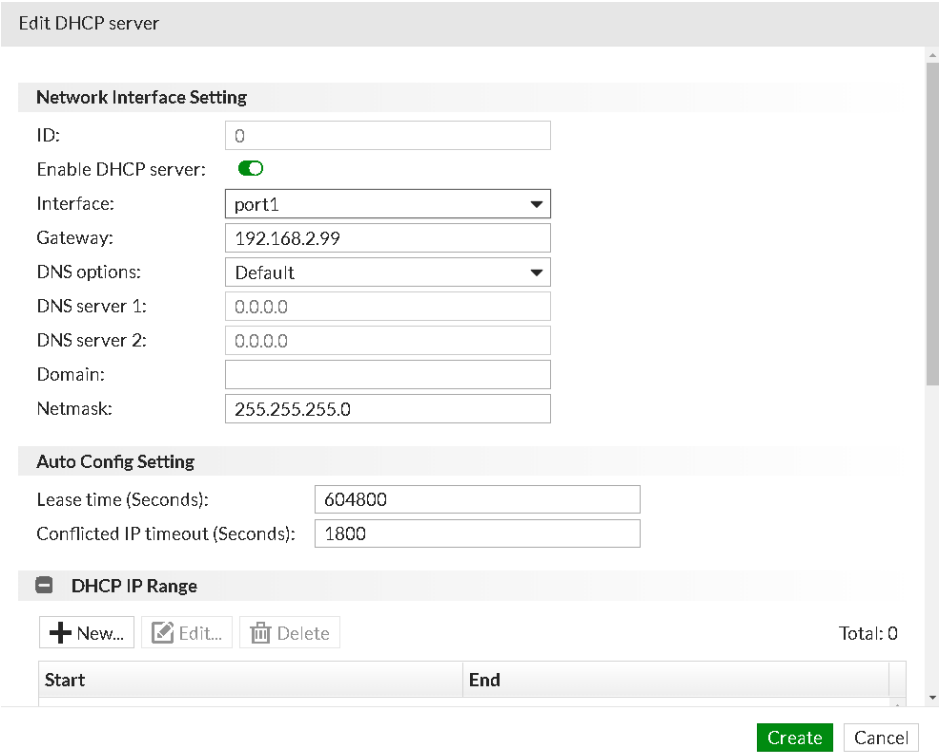
This scenario may be used to test the FortiRecorder and FortiCam equipment in a lab environment. If you install the FortiRecorder and FortiCam cameras in a dedicated network, the topology of this scenario will also apply.



To connect your camera directly to FortiRecorder

1. If this is the first time you connect to FortiRecorder, change your PC's IP address to be on the same subnet as the FortiRecorder port1's default IP address 192.168.1.99. For example, set your PC's IP to 192.168.1.98.
2. Connect your PC and FortiRecorder's port1 to a PoE switch. Do not connect the camera to the switch at this stage.

3. On your PC, open a web browser and connect to https://192.168.1.99. Log in to the admin administrator account with Name: admin and Password: (none).
4. If you want to use the FortiRecorder DHCP service, configure the DHCP server as described in the next step. If you already have a DHCP server to use on your network, skip the next step.
5. On the FortiRecorder web UI, go to *System* > *Network* > *DHCP*, and select **New** to create a new DHCP server on port1.

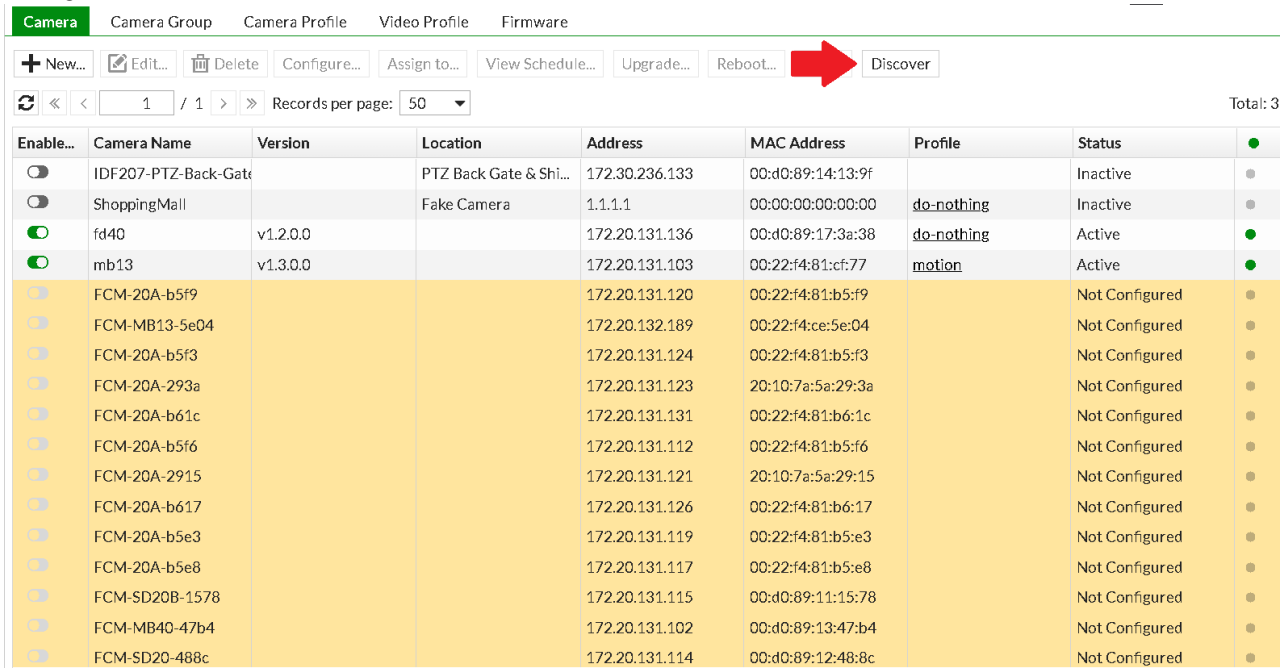


6. Enable DHCP server and select port1 from the Interface drop-down menu.
7. Go to *System* > *Network* > *Interface*. Select port1 and select *Edit*.
8. Enable Discover cameras on this port if not already enabled.
9. Connect the camera to the PoE switch now.

If you connect the camera to the switch before you have configured and enabled the DHCP server on FortiRecorder, the camera will use its default IP address, which might not be working on your network. Therefore, you must reboot the camera to get an IP address from the FortiRecorder DHCP server by unplugging the camera from the switch and plugging it back.

10. Go to *Camera* > *Configuration* > *Camera* and select *Discover*. After several seconds, a list of discovered cameras should appear. Newly discovered cameras will be highlighted in yellow, and their Status column will contain Not

Configured.



Enable...	Camera Name	Version	Location	Address	MAC Address	Profile	Status
	IDF207-PTZ-Back-Gate		PTZ Back Gate & Shi...	172.30.236.133	00:d0:89:14:13:9f		Inactive
	ShoppingMall		Fake Camera	1.1.1.1	00:00:00:00:00:00	do-nothing	Inactive
	fd40	v1.2.0.0		172.20.131.136	00:d0:89:17:3a:38	do-nothing	Active
	mb13	v1.3.0.0		172.20.131.103	00:22:f4:81:cf:77	motion	Active
	FCM-20A-b5f9			172.20.131.120	00:22:f4:81:b5:f9		Not Configured
	FCM-MB13-5e04			172.20.132.189	00:22:f4:ce:5e:04		Not Configured
	FCM-20A-b5f3			172.20.131.124	00:22:f4:81:b5:f3		Not Configured
	FCM-20A-293a			172.20.131.123	20:10:7a:5a:29:3a		Not Configured
	FCM-20A-b61c			172.20.131.131	00:22:f4:81:b6:1c		Not Configured
	FCM-20A-b5f6			172.20.131.112	00:22:f4:81:b5:f6		Not Configured
	FCM-20A-2915			172.20.131.121	20:10:7a:5a:29:15		Not Configured
	FCM-20A-b617			172.20.131.126	00:22:f4:81:b6:17		Not Configured
	FCM-20A-b5e3			172.20.131.119	00:22:f4:81:b5:e3		Not Configured
	FCM-20A-b5e8			172.20.131.117	00:22:f4:81:b5:e8		Not Configured
	FCM-SD20B-1578			172.20.131.115	00:d0:89:11:15:78		Not Configured
	FCM-MB40-47b4			172.20.131.102	00:d0:89:13:47:b4		Not Configured
	FCM-SD20-488c			172.20.131.114	00:d0:89:12:48:8c		Not Configured

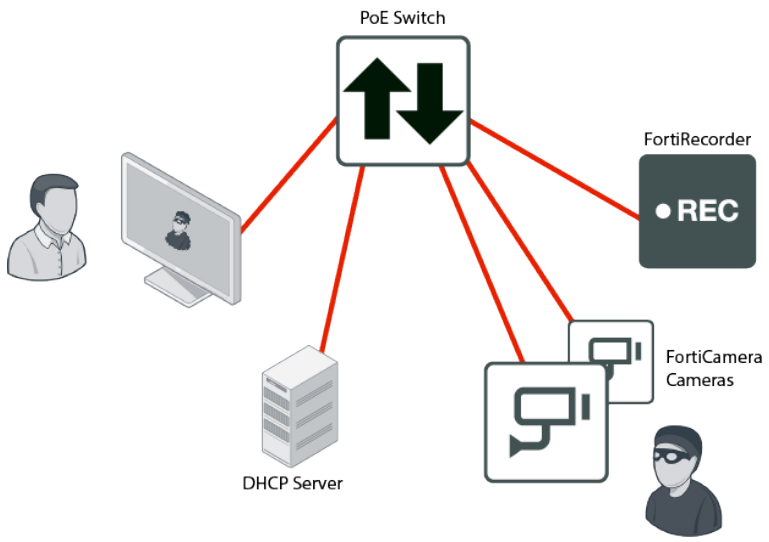
11. Double click on the discovered camera to configure the camera settings.
12. Go to *Monitor* > *Video* > *Video* to view the live feed from the camera.

Once you have finished connecting your cameras to FortiRecorder, you will need to configure your cameras. For more information, read the configuring cameras section.

Connecting cameras through a DHCP server

In this scenario, you already have a DHCP server running in your existing network and you are installing the FortiRecorder and FortiCam cameras in your network.

Note that the FortiRecorder will be using a static IP address and the cameras will be getting DHCP IP addresses from the third party DHCP server



1. Change your PC's IP address to be on the same subnet as the FortiRecorder port1's default IP address 192.168.1.99. For example, set your PC's IP to 192.168.1.98.
2. Connect your PC directly to FortiRecorder's port1 interface.
3. On your PC, open a web browser and connect to https://192.168.1.99. Log in to the admin administrator account with Name: admin and Password: (none).
4. On the FortiRecorder web UI, go to *System* > *Network* > *Interface* and double click on port1 interface. Change the IP address to one that is accessible to the DHCP server and your network. And make sure Discover cameras on this port is enabled.
5. Change your PC's IP address back.
6. Connect your PC and the FortiRecorder to your network. Then connect the camera to your network through a PoE switch.
7. Go to *Camera* > *Configuration* > *Camera* and select *Discover*. After several seconds, a list of discovered cameras should appear. Newly discovered cameras will be highlighted in yellow, and their Status column will contain Not Configured.
8. Double click on the discovered camera to configure the camera settings.
9. Go to *Monitor* > *Video* > *Video* to view the live feed from the camera.

Setting up the System

The following chapter provides a summary on how to connect and configure your FortiRecorder for initial use.

Perform the following steps:

1. Connect to the FortiRecorder Web UI or the CLI.
2. Configure the FortiRecorder.
3. Perform additional advanced configurations.
4. Update the firmware if a newer version has been released since receiving your appliance.

Connecting to the FortiRecorder Web UI

To be able to configure the FortiRecorder appliance, connect to its management web UI or CLI console. This chapter primarily describes the web UI usage.

You can connect to the web UI using its default settings. (By default, HTTPS access to the web UI is enabled.

Default settings for connecting to the web UI

Network Interface	port1
URL	https://192.168.1.99/
Administrator Account	admin+
Password	

Requirements

- a computer with an RJ-45 Ethernet network port
- a crossover Ethernet cable
- a web browser. For supported web browsers, see the release notes.
- If you are running FortiRecorder version 2.3 and older firmware, Apple QuickTime 7.1 or greater plug-in is required for video display. Note that starting from QuickTime 7.7.9, QuickTime typical install does not install the web plugin by default. You have to use custom install and select the web plugin.

  Starting from FortiRecorder version 2.4, HTML5 is supported. On most platforms, QuickTime plugin is not required anymore. For details, see the FortiRecorder version 2.4 release notes.

To connect to the web UI

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiRecorder appliance's port1internal.
3. Start your browser and enter the URL: https://192.168.1.99/ (Remember to include the "s" in https://.). Your browser connects the appliance.

4. Enter "admin" in the *Name* field of the login page and select *Login*. (there is no default password for an admin account)

   Login credentials entered are encrypted before they are sent to the FortiRecorder appliance. The web UI appears if the login was successful.

To allow objects in the web UI to properly display, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Connecting to the FortiRecorder CLI

For initial configuration, you can access the CLI from your management computer using either a local serial console connection or an SSH connection, either local or through the network

To connect to the CLI using a local serial console connection, you must have:

- a computer with a serial communications (COM) port
- the RJ-45-to-DB-9 serial or null modem cable included in your FortiRecorder package
- terminal emulation software, such as HyperTerminal for Microsoft Windows

To connect to the CLI using an SSH connection, you must have:

- a computer with an Ethernet port
- a crossover Ethernet cable
- an SSH client, such as PuTTY

Default settings for connecting to the CLI by SSH

Network Interface	port1
IP Address	192.168.1.99
SSH Port Number	22
Administrator Account	admin
Password	(none)

To connect to the CLI using a local serial connection

The following procedure uses Microsoft HyperTerminal. Steps may vary with other terminator emulators.

1. Using the RJ-45-to-DB-9 or null modem cable, connect your computer's serial communications (COM) port to the FortiRecorder unit's console port.
2. Verify that the FortiRecorder unit is powered on.
3. On your management computer, start HyperTerminal.
4. On Connection Description, enter a Name for the connection, and select *OK*.

5. On Connect To, from Connect using, select the communications (COM) port where you connected the FortiRecorder unit.
6. Select *OK*.
7. Select the following Port settings and select *OK*.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

8. Press Enter. The terminal emulator connects to the CLI and the CLI displays a login prompt.
9. Type admin and press Enter twice. (In its default state, there is no password for this account.)

To connect to the CLI using an SSH connection

The following procedure uses PuTTY. Steps may vary with other SSH clients.

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiRecorder unit's port1internal.
3. Verify that the FortiRecorder unit is powered on.
4. On your management computer, start your SSH client.
5. In Host Name (or IP Address), type 192.168.1.99.
6. In Port, type 22.
7. From Connection type, select *SSH*.
8. Select *Open*
   The SSH client connects to the FortiRecorder unit.
   The SSH client may display a warning if this is the first time you are connecting to the FortiRecorder unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiRecorder unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiRecorder unit with no network hosts between them, this is normal.
9. Select *Yes* to verify the fingerprint and accept the FortiRecorder unit's SSH key. You will not be able to log in until you have accepted the key
   The CLI displays a login prompt.
10. Type "admin" and press Enter twice. (In its default state, there is no password for this account.)

Configuring the FortiRecorder

Whether it is to integrate the FortiRecorder into your existing network or to set it up in a dedicated private network, you will need to configure the following settings:

- Setting the "admin" account password
- Configuring the network settings
- Configuring the DHCP server
- Setting the system time

Setting the "admin" account password

The administrator account always has full permission to view and change all FortiRecorder configuration options, including viewing and changing all other administrator accounts. Its name and permissions cannot be changed.

For security reasons, you must set a password for the admin account after you log on to FortiRecorder, since there is no default password. Be sure to set a strong password for the admin administrator account and change the password regularly.

To establish or change the administrator password in the FortiRecorder UI

1. Log in to the admin administrator account.
2. Go to *System > Administrator > Administrator.*
3. Change the password and log out.
   The new password takes effect the next time that administrator account logs in.

Configuring the network settings

Each of the FortiRecorder appliance's physical network adapter ports (or, for FortiRecorder-VM, vNICs) have a default IP address and netmask. If these IP addresses and netmasks are not compatible with the design of your unique network, you must configure them.

Network Interface*	IP Address	Netmask
port1	192.168.1.99	255.255.255.0
port2	192.168.2.99	255.255.255.0
port3	192.168.3.99	255.255.255.0
port4	192.168.4.99	255.255.255.0
*The number of network interfaces may vary by model.		

To connect to the CLI and web UI, you should configure the following FortiRecorder network settings:

- Interface: you must configure at least one network interface on your FortiRecorder appliance (usually port1) with an IP address and netmask so that it can receive your connections.
- Static route: Depending on your network, you also usually must configure a static route so that the FortiRecorder can connect to the Internet, your computer, and FortiCam cameras.
- DNS server: FortiRecorder appliances require connectivity to DNS servers for DNS lookups. The appliance will query the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP servers defined by their domain names.

To configure a network interface's IP address

1. Log in to the admin administrator account.
2. Go to *System* > *Network* > *Interface.*
3. Double-click the row to select the physical network interface that you want to modify.
4. If you want to manually assign an IP address and subnet mask to this network interface, select Manual and then provide the IP address and netmask in IP/Netmask. IPv4 and IPv6 subnet masks should be provided in CIDR format, e.g. /24 instead of 255.255.255.0. The IP address must be on the same subnet as the network to which the interface connects. **Two network interfaces cannot have IP addresses on the same subnet.**

   Otherwise, select DHCP and enable Connect to server to retrieve a DHCP lease when you save this configuration. If you want the FortiRecorder appliance to also retrieve DNS and default route ("gateway") settings, also enable Retrieve default gateway and DNS from server.

   If you use DHCP on an interface and there are cameras connected to the interface, you must make sure the IP address will not change on that interface because the cameras need to communicate with the FortiRecorder and thus need to be aware of the IP address of the FortiRecorder.

   Retrieve default gateway and DNS from server will overwrite the existing DNS and default route, if any.

5. Configure the following settings:

Setting Name	Description
Discover cameras on this port	Enable to send multicast camera discovery traffic from this network interface. For more information, see "Connecting FortiRecorder to the cameras".
Access	Enable the types of administrative access that you want to permit to this interface. **Caution**: Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiRecorder appliance.
Access: HTTPS	Enable to allow secure HTTPS connections to the web UI through this network interface. To configure the listening port number, see "Configuring system timeout, ports, and public access". To upload a certificate, see "Replacing the default certificate for the web UI".
Access: PING	Enable to allow: • ICMP type 8 (ECHO_REQUEST) or type 30 • UDP ports 33434 to 33534 for ping and traceroute to be received on this network interface. When it receives an ECHO_REQUEST, FortiRecorder will reply with ICMP type 0 (ECHO_RESPONSE).

Setting Name	Description
	Note: Disabling PING only prevents FortiRecorder from receiving ICMP type 8 (ECHO_REQUEST) or type 30 and traceroute-related UDP. It does not disable FortiRecorder CLI commands such as execute ping or execute traceroute that send such traffic.
Access: HTTP	Enable to allow HTTP connections to the web UI through this network interface. To configure the listening port number, see “Configuring system timeout, ports, and public access”. **Caution**: HTTP connections are not secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: SSH	Enable to allow SSH connections to the CLI through this network interface.
Access: SNMP	Enable to allow SNMP queries to this network interface, if queries have been configured and the sender is a configured SNMP manager. To configure the listening port number and configure queries and traps, see “SNMP traps & queries”.
Access: TELNET	Enable to allow Telnet connections to the CLI through this network interface. **Caution**: Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: FRC-Central	Enable to allow access from FortiRecorder Central.
MTU	Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiRecorder unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value. For example, RFC 2516 prescribes a value of 1492 for PPPoE. This option is available only for network interfaces that are directly associated with a physical link.
Administrative Status	Select either: • **Up** — Enable (that is, bring up) the network interface so that it can send and receive traffic. • **Down** — Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

6. Select *OK*.
   If you were connected to the web UI through this network interface, you are now disconnected from it.

7. To access the web UI again, in your web browser, modify the URL to match the new IP address of the network interface. For example, if you configured the network interface with the IP address 10.10.10.5, you would browse to: https://10.10.10.5

   If the new IP address is on a different subnet than the previous IP address, and your computer is directly connected to the FortiRecorder appliance, you may also need to modify the IP address and subnet of your computer to match the FortiRecorder appliance's new IP address.

To add a static route

If you used DHCP and Retrieve default gateway and DNS from server when configuring your network interfaces, skip this step — the default route was configured automatically.

1. Log in to the admin administrator account. Other accounts may not have permissions necessary to change this setting.
2. Go to *System* > *Network* > *Routing*.
3. Select *New*.
4. Configure the following settings:

Setting Name	Description
Destination IP/netmask	Type the destination IP address and network mask of packets that will be subject to this static route, separated by a slash (/). The value 0.0.0.0/0 results in a default route, which matches all packets.
Interface	Select the desired port number from the dropdown menu.
Gateway	Type the IP address of the next-hop router where the FortiRecorder appliance will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in Destination IP/netmask, or forward packets to another router with this information. For a direct Internet connection, this will be the router that forwards traffic towards the Internet, and could belong to your ISP. **Note**: The gateway IP address must be in the same subnet as a network interface's IP address. Failure to do so will cause FortiRecorder to delete all static routes, including the default gateway.

5. Select *OK*.

   The FortiRecorder appliance should now be reachable to connections with networks indicated by the mask. When you add a static route through the web UI, the FortiRecorder appliance evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiRecorder appliance adds the static route, using the next unassigned route index number.

For small networks with only a few devices, often you will only need to configure one route: a default route that forwards packets to your router that is the gateway to the Internet.

If you have redundant gateway routers (e.g. dual Internet/ISP links), or a larger network with multiple routers (e.g. each of which should receive packets destined for a different subset of IP addresses), you may need to configure multiple static routes.

6. To verify connectivity, from a computer on the route's network destination, attempt to ping one of FortiRecorder's network interfaces that should be reachable from that location. If the connectivity test fails, you can use the CLI commands to determine if a complete route exists from the FortiRecorder to the host: `execute ping <destination_ipv4>` and to determine the point of connectivity failure: `execute traceroute <destination_ipv4>`.
7. Enable PING on the FortiRecorder's network interface and use the equivalent tracert or traceroute command on the computer (depending on its operating system) to test routability for traffic traveling in the opposite direction: from the host to the FortiRecorder.
   If these tests fail, or if you do not want to enable PING, first examine the static route configuration on both the host and FortiRecorder.
   To display the cached routing table, enter the CLI command:
   ```
   diagnose netlink rtcache list
   ```
   You may also need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, and otherwise rule out problems at the physical, network, and transport layer.
   If these tests succeed, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.
   Verify that you have enabled HTTPS and/or HTTP on the network interface. Also examine routers and firewalls between the host and the FortiRecorder appliance to verify that they permit HTTP and/or HTTPS connectivity between them. Finally, you can also use the CLI command:
   ```
   diagnose system top 5 30
   ```
   to verify that the daemons for the web UI and CLI, such as sshd, newcli, and httpd are running and not overburdened. For details, see the FortiWeb CLI Reference.

To configure DNS settings

If you will use the settings DHCP and Retrieve default gateway and DNS from server when you configure your network interfaces, skip this — DNS is configured automatically.

1. Log in to the admin administrator account. Other accounts may not have permissions necessary to change this setting.
2. Go to *System* > *Network* > *DNS* and enter the IP addresses of a primary and secondary DNS server. Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

   Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, including the NTP system time. For improved performance, use DNS servers on your local network.

3. Select *Apply*.

4. To verify your DNS settings, in the CLI, enter the following commands: `execute traceroute www.fortinet.com`

DNS tests may not succeed if you have not yet completed “To add a static route”.

5. If the DNS query for the domain name succeeds, you should see results that indicate that the host name resolved into an IP address, and the route from FortiRecorder to that IP address:

```
traceroute to www.fortinet.com (192.0.43.10), 30 hops max, 60 byte packets
1 172.20.130.2 (172.20.130.2) 0.426 ms 0.238 ms 0.374 ms
2 static-209-87-254-221.storm.ca (209.87.254.221) 2.223 ms 2.491 ms 2.552 ms
3 core-g0-0-1105.storm.ca (209.87.239.161) 3.079 ms 3.334 ms 3.357 ms
...
16 43-10.any.icann.org (192.0.43.10) 57.243 ms 57.146 ms 57.001 ms
```

If the DNS query fails, you will see an error message such as:

www.fortinet.com: Temporary failure in name resolution

Cannot handle "host" cmdline arg `www.fortinet.com' on position 1 (argc 3)

Verify your DNS server IPs, routing, and that your firewalls or routers do not block or proxy UDP port 53.

Configuring the DHCP server

If you need the FortiRecorder DHCP service to connect cameras to the FortiRecorder, you can configure the DHCP server on the interface that the cameras connect to.

To configure FortiRecorder's DHCP server via the web UI

1. Go to *System* > *Network* > *DHCP.*
2. Click *New*.
3. Mark the check box for Enable DHCP server.
4. Configure the following settings:

a.

Setting Name	Description
Interface	Select the name of the network interface where this DHCP server will listen for requests from DHCP clients.
Gateway	Type the IP address that DHCP clients will use as their next-hop router. On smaller networks, this is usually the same router that FortiRecorder uses. It could be your office’s router, or cable/DSL modem.
DNS options	Select either: • Default — Leave DHCP clients’ DNS settings at their default values. • Specify — Configure DHCP clients with the DNS servers that you specify in DNS server 1 and DNS server 2.

Setting Name	Description
DNS server 1	Type the IP address of a DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if DNS options is set to Specify.
DNS server 2	Type the IP address of an alternative DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if DNS options is set to Specify.
Domain	Optional. Type the domain name, if any, that DHCP clients will use when resolving host names on the local domain.
Netmask	Type the subnet mask that DHCP clients will use in conjunction with the IP address that is assigned by FortiRecorder's DHCP server.
Conflicted IP timeout (Seconds)	Type the maximum amount of time that the DHCP server will wait for an ICMP ECHO (ping) response from an IP before it determines that it is not used, and therefore safe to allocate to a DHCP client that is requesting an IP address. The default is 1,800 seconds (3 minutes). To ensure that the DHCP server does not cause IP address conflicts with misconfigured computers that are accidentally using the pool of IP addresses used for DHCP, when a client request a new DHCP lease, the built-in DHCP server will ping an unused IP address in the pool first. If the ping test is successful, then a misconfigured computer is currently using that IP, and allocating it also to the DHCP client would cause an IP address conflict. To prevent this, the DHCP server will temporarily abandon that IP (mark it as used by a static host) and look for an other, available IP to give to the DHCP client. (It will not try abandoned IPs again until the pool is exhausted.) However, before the DHCP server can determine if the ping test is successful, the it must first wait to see if there is any reply. This slows down the search for an available IP address, and in rare cases, could cause a significant delay before the DHCP client receives its assigned IP address and other network settings. If your network is smaller or typically has low latency to ping replies, you can safely decrease this setting's value to improve DHCP speed and performance. In most cases, 3 seconds is enough.
Lease time (Seconds)	Type the maximum amount of time that the DHCP client can use the IP address assigned to it by the server. When the lease expires, the DHCP client must either request a new IP address from the DHCP server or renew its existing lease. Otherwise, the DHCP server may attempt to assign it to the next DHCP client that requests an IP. The default is 604,800 seconds (7 days).

Setting Name	Description
	If you have more or almost as many DHCP clients (cameras) as the number of IP addresses available to give to DHCP clients, you can decrease the lease. This will free up IP addresses from inactive clients so that IPs are available to give to clients that are currently in need of IP addresses. Keep in mind, however, that if the DHCP server is attached to your overall network rather than directly to cameras, this will slightly increase traffic volume and slightly decrease performance.
DHCP IP Range	To configure the DHCP lease pool — the range of IP addresses that the DHCP server can assign to its clients — click New and configure the first and last IP address in the range. To avoid DHCP pool exhaustion that can occur in some cases, the pool should be slightly larger than the total number of clients. If you need to exclude some IP addresses from this range (e.g. printers permanently occupy static IPs in the middle of the range), also configure DHCP Excluded Range. Tip: The built-in DHCP server can provide IP addresses to the computers on your network too, not just to cameras.
DHCP Excluded Range	To configure IPs that should be omitted from the DHCP pool and never given to DHCP clients (such if there are printers with manually assigned static IP addresses in the middle of your DHCP range), click New.
Reserved IP Address	To bind specific MAC addresses to a specific DHCP lease, guaranteeing that the DHCP server will never assign it to another DHCP client, click New. Caution: Reserved leases cannot prevent misconfigured computers from taking the IP address, causing an IP address conflict, and breaking the FortiRecorder's connection with the camera. See “Resolving IP address conflicts”. Tip: To mimic a static IP address for your cameras, yet still provide the benefit that IP addresses are still centrally managed and configured on your DHCP server, configure reserved IP addresses.

5. Select *Create*.

   As cameras join the network, they should appear in the list of DHCP clients on *Monitor* > *DHCP* > *DHCP.*

Setting the system time

For many features to work, including camera synchronization, scheduling, logging, and SSL/TLS-dependent features, the FortiRecorder system time must be accurate.

You can either manually set the FortiRecorder system time or configure the FortiRecorder appliance to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

NTP is recommended to achieve better time accuracy. NTP requires that your FortiRecorder be able to connect to the Internet on UDP port 123. Adjust your firewall, if any, to allow these connections.

Later, when cameras are added to your surveillance system, your FortiRecorder will synchronize the camera clocks with its own to keep them in agreement.

To configure the system time

1. Go to *System* > *Configuration* > *Time*.
2. Either manually set the date and time or select to synchronize with NTP server.
3. Select *Apply*.
   If you manually configured the time, or if you enabled NTP and the NTP query for the current time succeeds, the new clock time should appear in System time. (If the query reply is slow, you may need to wait a couple of seconds, then click Refresh to update the display in System time.)

Once FortiRecorder is configured you can connect and configure your cameras. For information on how to connect them, see the Quick Setup Guide. You may also want to configure your schedules, since your schedules determine the functionality of a lot of important functions. See the Configuring Schedules section for more details.

Advanced FortiRecorder Configuration

After you have a basic working setup, depending on your specific requirements, you may want to configure some advanced or optional settings:

- Configuring system timeout, ports, and public access
- Configuring FortiRecorder system appearance
- Configuring logging
- Alert email

Configuring system timeout, ports, and public access

Go to *System* > *Configuration* > *Options* to configure the system idle timeout, the HTTP, HTTPS, SSH, Telnet, and FortiRecorder Central access ports, and the host name for public/remote access.

If you want remote access — connecting from a home or a branch office through the Internet to your FortiRecorder — for either using the web UI or snapshot notification video clips while you are out of the office, you must configure both your network and the FortiRecorder.

First, on your office's firewall or Internet router, configure port forwarding and/or a virtual IP (VIP) to forward remote access connections from the Internet to your FortiRecorder's private network IP. (See "Appendix A: Port numbers").

Remote access opens ports and can weaken the strength of your network security. To prevent attackers on the Internet from gaining access to your surveillance system, configure your firewall or router to require authentication, restrict which IP addresses can use your port forward/virtual IP, and scan requests for viruses and hacking attempts.

If you are not sure what your network's Internet address is, while connected to your office network, you can use an online utility such as:

http://ping.eu/

Next, go to System > Configuration > Options and configure these settings:

Setting Name	Description
Public Access	
Host name	Type either your network's IP on the Internet, or its domain name, such as www.example.com. This is either your Internet router's WAN IP, or a virtual IP (VIP) on your firewall whose NAT table will forward incoming connections from this public network IP to your FortiRecorder's private network IP.
HTTP/ HTTPS Port number	Type the port number, such as 8080, on your public IP that your Internet router or firewall will redirect to your FortiRecorder's listening port.

FortiRecorder supports live streaming (HLS) for mobile devices. You can use the FortiRecorder Mobile drop-down menu to enable live streaming over HTTP or HTTPS.

Creating FortiRecorder logical interfaces

In addition to the physical interfaces, you can create a variety of logical interfaces on FortiRecorder.

VLAN subinterfaces

A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

Redundant interfaces

On the FortiRecorder unit, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

A physical interface is available to be in a redundant interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of a redundant interface

- it has no defined IP address and is not configured for DHCP
- it does not have any VLAN subinterfaces
- it is not monitored by HA

When a physical interface is included in a redundant interface, it is not listed on the *System* > *Network* > *Interface* page. You cannot configure the interface anymore.

Aggregate interfaces

An aggregate interface is a logical interface which uses the Link Aggregation Control Protocol (LACP) (802.3ad) and combines several interfaces to increase throughput. It also provides redundancy in case one interface in the aggregation is down.

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiRecorder unit.

The loopback interface is useful when you use a layer 2 load balancer in front of several FortiRecorder units. In this case, you can set the FortiRecorder loopback interface's IP address the same as the load balancer's IP address and thus the FortiRecorder unit can pick up the traffic forwarded to it from the load balancer.

Customizing the system messages, email templates, and UI appearance.

Customizing system messages

The FortiRecorder system delivers custom system messages to the user, such as disclaimers or camera notifications.

To customize system messages

1. Go to *System* > *Customization* > *Custom Message*.
2. Select a message and select *Edit*.
3. Enter the desired message in the content area. There is a limit of 4000 characters for each message.
4. Select *Insert Variables*.
5. Place your mouse cursor in the text message at the insertion point of the variable.
6. Select the name of the variable to add. It will appear at the insertion point.
7. Select the close icon.
8. Select *OK*.

In addition to adding predefined variables to your system messages, you can create new variables. Typically these variables represent frequently used messages.

To create a new variable

1. Go to *System* > *Customization* > *Custom Messages*.
2. Select a message and then select *Edit Variable*.

3. Select *New*.
4. Enter the variable name to use in the system message. Its format is: `%%<variable_name>%%`. For example, if you enter the word “warning”, this variable appears as `%%warning%%` in the system message if you select to insert it.
5. Enter a description of the variable in the Display Name field.
6. Enter the variable’s content. For example: The camera `%%CAMERA_NAME%%` has detected motion on `%%EVENTDATE%%`.
7. Select *Create*.

Customizing email templates

The FortiRecorder unit may send out notification emails for events such as alert or camera notification.

To customize email templates

1. Go to *System* > *Customization* > *Custom Email Templates*.
2. Select the template and then select *Edit*.
3. Enter the necessary information, such as the name and a brief description.
4. In the content section, format the message in HTML. To add variables, select Insert Variable.
5. Determine if the HTML code was entered correctly by selecting Preview.
6. Select *OK*.

Customizing the user interface appearance

You can customize the interface of the FortiRecorder like the default color of the interface or adding your own custom logo.

To customize the user interface appearance

1. Go to *System* > *Customization* > *Appearance*.
2. Configure the following to change the appearance of the UI:

Setting Name	Description
Product name	Enter the name of the product.
Custom top logo	Select Change to upload an icon used as the favicon for the FortiRecorder UI.
Default theme	Select the default display theme (red, green, blue, and light blue) for the display of the web-based manager and the login page. You can configure a separate theme preference for each administrator account. For details, see the Configuring administrator account section.

3. Select *Apply*.

Configuring Logging

To diagnose problems or to track actions that the FortiRecorder appliance does as it receives and processes video, configure the FortiRecorder appliance to record log messages.

Log messages can record camera, and/or FortiRecorder appliance events.

To view log messages, go to *Monitor* > *Log* > *Event*.

To configure logging

1. Go to *Logs & Alert* > *Log Settings* > *Local.* Alternatively, if you want logs to be stored remotely, go to *Logs & Alert* > *Log Settings* > *Remote*.
2. Configure the following settings if configuring local log storage:

Setting Name	Description
Log file size	Type the file size limit of the current log file in megabytes (MB). The log file size limit must be between 1 MB and 1000 MB. **Note**: Large log files may decrease display and search performance.
Log time	Type the time (in days) of the file age limit. If the log is older than this limit, even if has not exceeded the maximum file size, a new current log file will be started. Valid range is between 1 and 366 days.
At hour	Select the hour of the day (24-hour format) when the file rotation should start. When a log file reaches either the age or size limit, the FortiRecorder appliance rotates the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23 o'clock of the 10th day.
Log level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see "Log severity levels". **Caution**: Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.
Log options when disk is full	Select what the FortiRecorder will do when the local disk is full and a new log message is caused, either: • **Do not log** — Discard all new log messages. • **Overwrite** — Delete the oldest log file in order to free disk space, and store the new log message.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log.

3. If configuring remote log storage, click New, then configure the following settings:

Setting Name	Description
IP	Type the IP address of a Syslog server or FortiAnalyzer.
Port	Type the UDP port number on which the Syslog server listens for log messages. The default is 514.

Setting Name	Description
Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see “Log severity levels”. **Caution**: Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.
Facility	Select the facility identifier the FortiRecorder will use to identify itself to the Syslog server if it receives logs from multiple devices. To easily identify log messages from the FortiRecorder when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CSV format	Enable if your Syslog server requires comma-separated values (CSV). **Note**: Do not enable this option if the remote host is a FortiAnalyzer. FortiAnalyzer does not support CSV-formatted log messages.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log.

4. To verify logging connectivity, from FortiRecorder, trigger a log message that matches the type and severity levels that you have chosen to store on the remote Syslog server or FortiAnalyzer. Then, on the remote host, confirm that it has received that log message.

If you will be sending logs to a FortiAnalyzer appliance, you must add the FortiRecorder to the FortiAnalyzer’s device list, and allocate enough disk space. Otherwise, depending on its configuration for unknown devices, FortiAnalyzer may ignore the logs. When the allocated disk space is full, it may drop subsequent logs.

If the remote host does not receive the log messages, verify the FortiRecorder’s static routes (see “FortiRecorder configuration”) and the policies on any intermediary firewalls or routers (they must allow Syslog traffic from the FortiRecorder network interface that is connected to the gateway between it and the Syslog server). To determine the point of connectivity failure along the network path, if the FortiAnalyzer or Syslog server is configured to respond to ICMP ECHO_REQUEST (ping), go to Dashboard > Console and enter the command:

```
execute traceroute <syslog_ipv4>
```

where `<syslog_ipv4>` is the IPv4 address of your FortiAnalyzer or Syslog server.

Configuring Alert Emails

As the FortiRecorder system administrator, you can receive alert email whenever an important system event occurs, such as the hard disk being full and so on. Before you configure alert email, you must configure the mail server settings so that FortiRecorder can send out email. For details see “Configuring FortiRecorder to send notification email”.

You can configure up to 10 alert email addresses.

To configure alert email settings

1. Go to *Logs & Alerts* > *Alert Email* > *Configuration*.
2. Select *New*.
3. Type your email address, such as admin@example.com.

   This setting is the recipient only for appliance-related notifications, such as the hard disk being full. It does not configure the recipient of camera-related notifications, such as motion detection. For this kind of video-related notifications, see “Notifications”.
4. Select *Create*.
5. Go to *Logs & Alerts* > *Alert Email* > *Category*. Enable all desired appliance events to trigger an alert email:

Setting Name	Description
System events	Enable to notify when serious system events occur such as daemon crashes. See also “Resource issues”.
Disk is full	Enable to notify when the disk partition that stores log data is full. See also “Data storage issues”.
Camera device altered	Enable to notify when a defined camera configuration has been enabled or disabled, or if there are problems with the camera. (The FortiRecorder will not control or record video from a camera that is not enabled in its list of known, configured devices. See “Camera settings”.)
Camera communication error	Enable to notify when there has been a network error during communications between the FortiRecorder and camera. See also “Connectivity issues”.
Camera recording error	Enable to notify when an issue prevents a camera from recording. See also “Video viewing issues” and “Connectivity issues”.
Camera alert summary	Enable notify when various alerts have been triggered.
Video disk events	Enable to notify when the disk partition that stores video data is full. See also “Data storage issues”.

6. Select *Apply*.

Updating the Firmware

The FortiRecorder appliance come with the latest operating system (firmware); however, if a new version has been released since your appliance was received, install the latest firmware before continuing the installation of your FortiRecorder. (Camera firmware can be updated later, after you have connected your cameras to the appliance.

Fortinet periodically releases FortiRecorder firmware updates to include enhancements and address issues. After you register your FortiRecorder appliance, FortiRecorder firmware is available for download at:

https://support.fortinet.com

Installing new firmware overwrites attack signature packages using the versions of the packages that were current at the time that the firmware image was built. To avoid repeat updates, update the firmware before updating your FortiGuard packages. New firmware can introduce new features which you must configure for the first time.

For late-breaking information specific to the firmware release version, see the Release Notes available with that release.

In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.

Before you can download firmware updates for your FortiRecorder appliance, you must first register your FortiRecorder appliance with Fortinet Technical Support. For details, go to https://support.fortinet.com/ or contact Fortinet Technical Support.

Installing FortiRecorder firmware

You can use either the web UI or the CLI to upgrade or downgrade the appliance's operating system.

Firmware changes are either:

- an update to a newer version
- a reversion to an earlier version

To determine if you are updating or reverting the firmware, go to *Dashboard* > *Status* and in the System Information widget, see the Firmware Version row. (Alternatively, in the CLI, enter the command get system status.)

For example, if your current firmware version is:

FortiRecorder-200D v1.0,build0065,120821

changing to

FortiRecorder-200D v1.0,build0066,120824

an earlier build number (65) and date (120821 means August 21, 2012), indicates that you are reverting.

Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.

If you are installing a firmware version that requires a different size of system partition, you may be required to format the boot device before installing the firmware by re-imaging the boot device. Consult the Release Notes. In that case, do not install the firmware using this procedure.

To install firmware using the web UI

1. Download the firmware file from the Fortinet Technical Support web site: https://support.fortinet.com/
2. Log in to the web UI of the FortiRecorder appliance as the admin administrator.
3. Go to *Dashboard* > *Status*.
4. In the System Information widget, in the Firmware version row, select *Update*.The Choose Firmware dialog appears.
5. Select *Browse* to locate and select the firmware file that you want to install, then select *OK*.
6. Select *OK*.

   Your management computer uploads the firmware image to the FortiRecorder appliance. The FortiRecorder appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your

network connection, and by the amount of time that the specific model requires to reboot. Over a LAN connection, it should only take a couple minutes until the appliance becomes available again.

If you are downgrading the firmware to a previous version, and the settings are not fully backwards compatible, the FortiRecorder appliance may either remove incompatible settings, or use the feature's default values for that version of the firmware. You may need to reconfigure some settings.

7. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes. For details, see your browser's documentation.
8. To verify that the firmware was successfully installed, log in to the web UI and go to *Dashboard* > *Status*. In the System Information widget, the Firmware version row indicates the currently installed firmware version.
9. If you want to install alternate firmware on the secondary partition, follow "Installing alternate firmware".
10. Continue with "Setting the "admin" account password".

To install firmware using the CLI

1. Download the firmware file from the Fortinet Technical Support web site: https://support.fortinet.com/
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
4. Connect port1 of the FortiRecorder appliance directly or to the same subnet as a TFTP server.
5. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the admin administrator.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as tftpd (Windows, Mac OS X, or Linux) on your management computer.

Because TFTP is not secure, and because it does not support authentication and could allow anyone to have read and write access, you should only run it on trusted administrator-only networks, never on computers directly connected to the Internet. If possible, immediately turn off TFTP off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiRecorder appliance can reach the TFTP server. To use the FortiRecorder CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where 192.168.1.168 is the IP address of the TFTP server.
8. Enter the following command to download the firmware image from the TFTP server to the FortiRecorder appliance:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```
   where <name_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:
   ```
   execute restore image tftp image.out 192.168.1.168
   ```
   One of the following message appears:
   - ```
     This operation will replace the current firmware version!
     Do you want to continue? (y/n)
     ```
   - ```
     Get image from tftp server OK.
     Check image OK.
     ```

```
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

9. Type y.
   The FortiRecorder appliance downloads the firmware image file from the TFTP server. The FortiRecorder appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection

> If you are downgrading the firmware to a previous version, the FortiRecorder appliance reverts the configuration to default values for that version of the firmware. You will need to reconfigure the FortiRecorder appliance or restore the configuration file from a backup. For details, see “Connecting to FortiRecorder web UI” and, if you opt to restore the configuration, “Restoring a previous configuration”.

10. To verify that the firmware was successfully installed, log in to the CLI and type:
    `get system status`
    The firmware version number is displayed.
11. If you want to install alternate firmware on the secondary partition, follow “Installing alternate firmware”.
12. Continue with “Setting the “admin” account password”.

Installing alternative firmware

You can install alternate firmware which can be loaded from its separate partition if the primary firmware fails. This can be accomplished via the web UI or CLI.

To install alternate firmware via the CLI

1. Download the firmware file from the Fortinet Technical Support web site:
   https://support.fortinet.com/
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
4. Connect port1 of the FortiRecorder appliance directly or to the same subnet as a TFTP server.
5. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the admin administrator.
   For details, see “Connecting to FortiRecorder web UI”.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as tftpd (Windows, Mac OS X, or Linux) on your management computer.)

> Because TFTP is not secure, and because it does not support authentication and could allow anyone to have read and write access, you should only run it on trusted administrator-only networks, never on computers directly connected to the Internet. If possible, immediately turn off tftpd off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiRecorder appliance can reach the TFTP server. To use the FortiRecorder CLI to verify connectivity, enter the following command: class="CLI_0">execute ping 192.168.1.168 where 192.168.1.168 is the IP address of the TFTP server.
8. Enter the following command to restart the FortiRecorder appliance:
   `execute reboot`

9. As the FortiRecorder appliances starts, a series of system startup messages appear.
```
Press any key to display configuration menu........
```
10. Immediately press a key to interrupt the system startup

> You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiRecorder appliance reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:
```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
Enter G,F,B,Q,or H:
Please connect TFTP server to Ethernet port "1".
```
11. Type G to get the firmware image from the TFTP server.
The following message appears:
```
Enter TFTP server address [192.168.1.168]:
```
12. Type the IP address of the TFTP server and press Enter.
The following message appears:
```
Enter local address [192.168.1.188]:
```
13. Type a temporary IP address that can be used by the FortiRecorder appliance to connect to the TFTP server.
The following message appears:
```
Enter firmware image file name [image.out]:
```
14. Type the firmware image file name and press Enter.
The FortiRecorder appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:
```
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
```
15. Type B.
The FortiRecorder appliance saves the backup firmware image and restarts. When the FortiRecorder appliance reboots, it is running the primary firmware.

Booting from the alternate partition

Each appliance can have up to two firmware versions installed. Each firmware version is stored in a separate disk partition.

To boot into alternative firmware through the local console CLI

1. Install firmware onto the alternate partition (see “Installing alternate firmware”).
2. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the admin administrator.
4. Enter the following command to restart the FortiRecorder appliance:
```
execute reboot
```

5. As the FortiRecorder appliances starts, a series of system startup messages appear.
   ```
   Press any key to display configuration menu........
   ```
   Immediately press a key to interrupt the system startup

   You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiRecorder appliance reboots and you must log in and repeat the execute reboot command.

   If you successfully interrupt the startup process, the following messages appears:
   ```
   [G]: Get firmware image from TFTP server.
   [F]: Format boot device.
   [B]: Boot with backup firmware and set as default.
   [Q]: Quit menu and continue to boot with default firmware.
   [H]: Display this list of options.
   Enter G,F,B,Q,or H:
   Please connect TFTP server to Ethernet port "1".
   ```
6. Type B to reboot and use the backup firmware.

Upload licenses

If you have purchased licenses, them to FortiRecorder to unlock those features.

1. Go to *Dashboard* > *Status*.
2. In the *License Information* widget, click *Update*. Find and upload the license file.

   FortiRecorder validates the license and updates the license status on the dashboard. If you uploaded a face recognition AI license, validation requires an Internet connection. See also Port Numbers on page 174.
3. Repeat the previous step if you need to upload more licenses.

Using the Dashboard

FortiRecorder provides several methods, such as SNMP traps, system logs, and real-time dashboard, for you to monitor the system status and diagnose system problems. The Dashboard section displays various system statuses, such as CPU usage and mail statistics.

This chapter contains the following information:

- Reviewing System Status
- Using the CLI Console

Reviewing System Status

To access the Dashboard, go to *Dashboard* > *Status*. The Dashboard is the default display that contains a variety of widgets displaying performance level and statistics. The default widgets displayed in the Dashboard are the serial number and current system status of the FortiRecorder unit, including uptime, system resource usage, alert messages, host name, firmware version, system time, and email throughput.

To access this part of the web UI:

- Domain must be System
- Access profile must have Read-Write permission to the Others category

To access the dashboard, you must have an administrator account. Operator accounts do not have permission. For details, see “User types”.

Customizing Widgets

The dashboard is customizable. You can select which widgets to display, where they are located on the tab, and whether they are minimized or maximized.

To move a widget, position your mouse cursor on the widget’s title bar and then click and drag the widget to a new location.

To show or hide a widget, select *Manage Widget* and then select the widgets you want displayed on the Dashboard. If the widget is greyed out, the widget will not display. Select *Apply* when you have made your selections.

Options vary slightly from widget to widget, but always include options to close, refresh, or minimize/maximize the widget.

Using the CLI Console

The CLI console is a means of interacting with the FortiRecorder using commands through successive lines of text (command lines).

To access the CLI without exiting from the web UI, go to *Dashboard* > *Console*. You can select the Open in New Window button to move the CLI Console into a pop-up window that you can re-size and reposition.

Utilizing FortiView

The FortiView section provides an overview of the general performance of your cameras, such as a camera's bandwidth usage.

This section contains the following topics:

- Monitoring camera statistics
- Viewing sessions
- Analyzing the topology

Monitoring Camera Statistics

The Camera Statistics section displays a collection of statistics and overviews to monitor various camera performances, such as the bandwidth usage of select cameras and recording gap occurrences.

Viewing bandwidth statistics

The Bandwidth tab displays the amount of data transferred over the network by the cameras, including the bandwidth of remote storage and motion detection. The x-axis displays the date and time of the recording, while the y-axis displays the specific bandwidth usage. The lower the curve or bar on the graph, the less bandwidth used during that particular time.

To edit bandwidth statistic settings

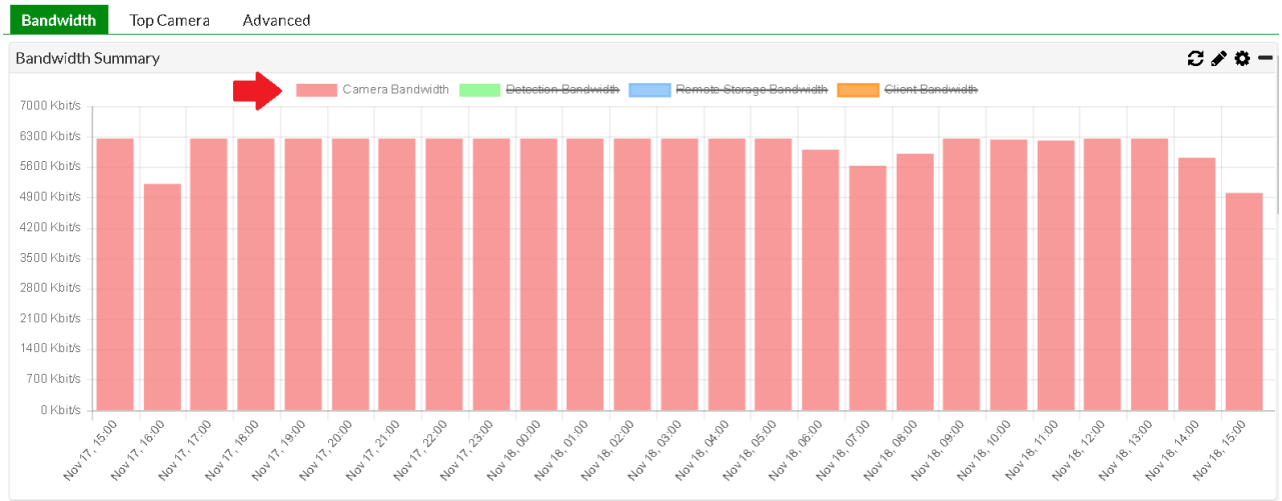
1. Go to *FortiView* > *Camera Statistics* > *Bandwidth*.
2. Select the settings cog wheel and configure the following:

Setting Name	Description
All cameras	The all cameras section allows you to configure bandwidth monitoring settings for every camera connected to your FortiRecorder. The section includes three viewing preferences: Interval, Unit, and Chart type.
Camera group	The camera group section allows you to configure bandwidth monitoring settings for specific camera groups created under Camera > Configuration > Camera Group. The section includes three viewing preferences: Interval, Unit, and Chart type.
Camera	The camera section allows you to configure bandwidth monitoring settings for specific cameras. Enable each camera you want to monitor. The section includes three viewing preferences: Interval, Unit, and Chart type.

Setting Name	Description
Interval	Select the desired period of time to analyze bandwidth. If you select 24 hours, for example, the x-axis is sectioned into hourly points over a 24 hour period of time.
Unit	Select the desired unit type displayed along the y-axis.
Chart type	Select either a line chart, which displays bandwidth information as a series of data points called “markers” connected by a line, or bar chart, which presents bandwidth data with rectangular bars with varying heights.

3. Select *OK*.

Selecting one of the bandwidth display options enables or disables them from view.



Viewing Top Camera Usage

The Top Camera tab displays the performance of individual cameras on your network. Use this section to determine which cameras use the most bandwidth. The larger the horizontal bar, the more bandwidth the camera uses.

To edit top camera settings

1. Go to *FortiView* > *Camera Statistics* > *Top Camera*.
2. Select the settings cog wheel and configure the following:

Setting Name	Description
Interval	Select the desired period of time to analyze bandwidth. If you select 24 hours, for example, the bar graph displays the bandwidth usage of the camera in the last 24 hours.
Unit	Select the desired unit type displayed along the x-axis.

3. Select *OK*.

Analyzing Advanced Statistics

The Advanced tab displays the frames from the cameras and shows when frames are dropped. Dropped frames are gaps in the recording caused by packet loss, illustrated by the gap forward/backward graphs. Recording skips track the lost frames experienced when the FortiRecorder writes to disk. The proxy drops graph illustrates frames lost in the FortiRecorder when receiving packets from the cameras. The collector drops graph shows any lost frames in the FortiRecorder by the daemon responsible for writing to disk.

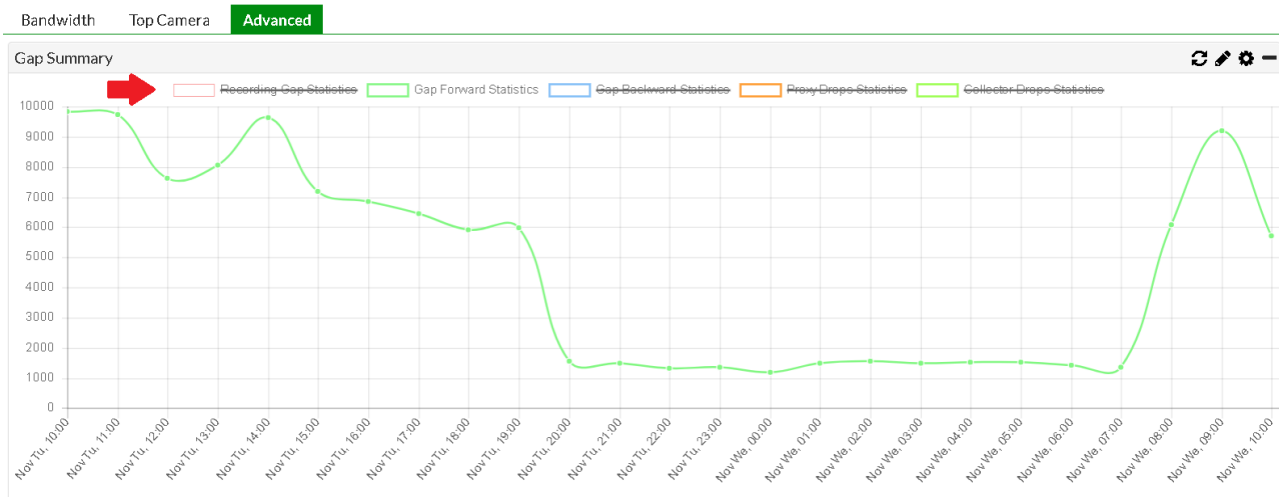
To edit the Advanced settings

1. Go to *FortiView* > *Camera Statistics* > *Advanced*.
2. Select the settings cog wheel and configure the following:

Setting Name	Description
All cameras	The all cameras section allows you to gap summary statistics settings for every camera connected to your FortiRecorder. The section includes three viewing preferences: Interval, Unit, and Chart type.
Camera group	The camera group section allows you to configure gap summary statistics settings for specific camera groups created under *Camera* > *Configuration* > *Camera Group*. The section includes three viewing preferences: Interval, Unit, and Chart type.
Camera	The camera section allows you to configure gap summary statistics settings for specific cameras. Enable each camera you want to monitor. The section includes three viewing preferences: Interval, Unit, and Chart type.
Interval	Select the desired period of time to analyze gap summary. If you select 24 hours, for example, the x-axis is sectioned into hourly points over a 24 hour period of time.
Unit	Select the desired unit type displayed along the y-axis. The higher the bar is on the line chart graph, the more dropped frames occurred during that time.
Chart type	Select either a line chart, which displays bandwidth information as a series of data points called “markers” connected by a line, or bar chart, which presents bandwidth data with rectangular bars with varying heights.

3. Select *OK*.

Selecting one of the recording gap statistics display options enables or disables them from view.



Viewing Sessions

The Sessions section displays the active TCP/UDP sessions to and from FortiRecorder.

Analyzing the Topology

This feature is still under development.

Video Monitoring

To get the most value out of your FortiRecorder system, FortiRecorder has a variety of monitoring tools, such as direct video surveillance and detailed summaries of camera events.

This section contains the following topics:

- Event analyzing
- Viewing video
- Reviewing camera notifications
- Analyzing logging
- Monitoring DHCP status
- Reviewing security information

Event Analyzing

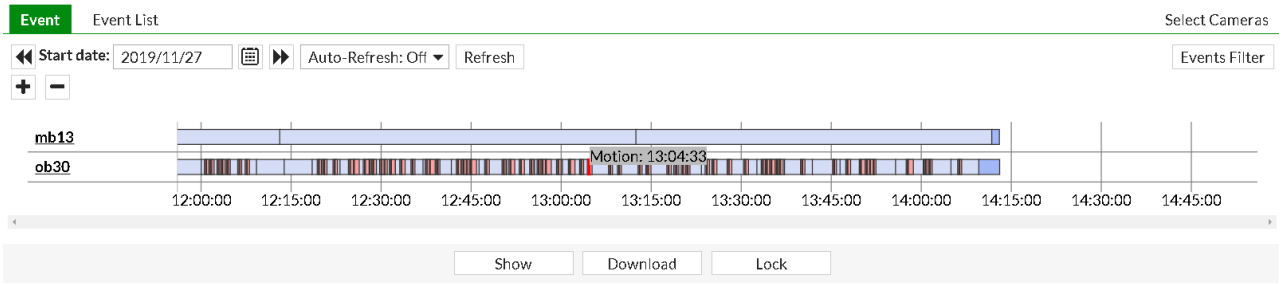
The event monitor displays motion detection events without loading the live video stream. Monitoring through the time frame display saves bandwidth.

Viewing the event time frame

The event time-line streamlines the monitoring process by condensing all triggered events for each individual camera into a single bar.

To view the motion detection events

1. Go to *Monitor* > *Event* > *Event*.
2. Select the Select Cameras button to enable the cameras you want to monitor on the time frame.
3. Click and hold on the time-line itself and drag your mouse left or right to view different times during the recording. Alternatively, select the plus and minus buttons. Set the time span of the time line by entering the desired start date in the Start Date field.



4. Select a desired detection event in the time frame and select the Show button to display the event or Download to download the selected event for archive.

   The Download button is useful if you are required to show video evidence of a particular incident to authorities. Your

FortiRecorder uses the .mp4 file format with the H.264 video codec, which can be viewed on Windows, Mac OS X, Linux, and other platforms using QuickTime, VLC or other compatible players. All video files are signed with an RSA 2048-bit signature to provide tamper protection. This applies to files stored locally, remotely, and downloaded. Quality of previously recorded video depends on the camera's settings.

Select the Lock button to prevent the video clip from being deleted by storage policies.

Viewing the Event List

The Event List offers a detailed list of various events that occurred throughout a given period in an easy to research list view. Each entry in the list contains the start and end time of the event, the camera the event occurred on, and the type of the event.

To view the Event List

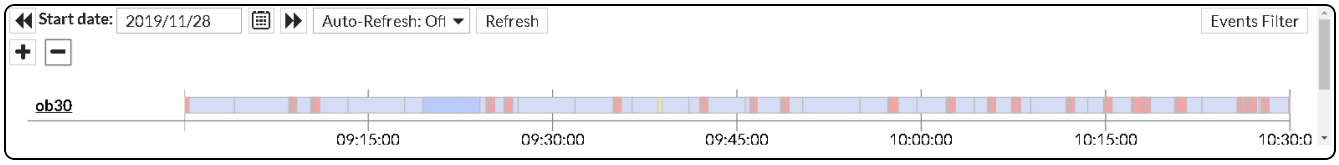
1. Go to *Monitor* > *Event* > *Event List*.
2. Select the Select Cameras button to enable the cameras you want to monitor on the event list.
3. Enter the desired start and end date in their respected fields to change the viewing period of the list.
4. Select the Events Filter button and enable all of the event types you want to display on the list to create a more focused event list.

Viewing Video

The video section provides both a live and recorded view of the cameras integrated onto the FortiRecorder system.

Understanding the time line

The time line is located directly beneath both live and recorded videos. Time periods in the time line panel are color-coded for easier monitoring



Yellow: The yellow bar is a system event, such as a software update, system reboot, or camera reboot. Recordings cannot be stored while FortiRecorder is unavailable.

Light blue: The light blur bar is a previously recorded clip.

Dark blue: The dark blue bar is a temporary recording that has been manually initiated. If a camera is not currently recording a continuous or motion detection-triggered video, operators can manually trigger the camera to record video using the Control pane.

Bright blue: A bright blue bar is a recording with an attached annotation. While a camera is recording, you can insert markers with notes about what is currently being seen. If the camera is not recording, after you enter the marker and click Insert Marker, the camera will start to record.

Red: A red bar is a motion detection-based recording that was not initiated by schedule.

White: A white bar indicates no recording at that period of time.

To look for specific events in the time line, select the *Events Filter* button and enable all events you want displayed on the time line.

Viewing live video

To view live video from your cameras

1. Go to *Monitor* > *Video* > *Video*.

2. Select the Select Cameras button and enable the cameras you wish to view.
3. Select the Record button at anytime during the viewing to begin recording the video.

If you are watching a live feed of the camera and the camera is not scheduled to record, the video feed from the camera is temporarily recorded in memory but not saved on the hard drive. When you stop watching the live feed from that camera, the temporary recording is deleted. To save the temporary recording to the hard drive, initiate manual recording by selecting the Record button during the live viewing.

Viewing recorded video

In addition to live video feeds, you can also watch the recorded video clips, which include the scheduled recording, motion detection recording, and manual recording.

To begin recording the camera feed at anytime during live playback, select the *Record* button.

To view recorded video from your cameras

1. Go to *Monitor* > *Video* > *Video*.
2. Select the Select Camera button and enable the cameras you wish to view.
3. Navigate the time line by select the up or down arrows or by selecting the time line bar and dragging it to the desired time.
4. Select a segment of video in the time line and select *Show* or double-click the desired segment.
5. Select the *Download* button to download the clip for archive or to view on a different computer.

   The FortiRecorder uses the .mp4 file format with the H.264 video codec, which can be viewed on Windows, Mac OS X, Linux, and other platforms using QuickTime, VLC or other compatible players. All video files are signed with an RSA 2048-bit signature to provide tamper protection. This applies to files stored locally, remotely, and downloaded. Quality of previously recorded video depends on the camera's settings.

   Adjust the image quality using the pane on the right side. Select the Control bar to expand it and then select the plus and minus buttons to adjust Brightness, Contrast, Saturation, and Sharpness.

Set these settings with care. After video is recorded, it won't be possible to adjust the image quality again unless you download the file and use video editing software. Video editing software may not be able to successfully correct for excessively bad image quality

You can't stop a scheduled continuous or motion detection-based recording schedule. You can only start/stop manual recording.

Reviewing Camera Notifications

If you have configured camera-based notifications, accounts configured to be notified can log in to the web UI in order to review the video clips. If you have configured email settings, these accounts will also receive an email when a camera-based event occurs. Notifications contain snapshot images from the video clip of the detected motion or, depending on your configuration, a link directly to the video clip. In this way, recipients can quickly assess whether or not the event is serious, or just a false alarm.

Occasionally, you may sometimes be required to review these notifications if, for example, the usual recipient is on vacation. You can do this from the web UI, without logging in to a separate operator account. Alternatively, you can add yourself to the list of people that will receive a notification via email.

To review camera-based notifications

1. Go to *Monitor* > *Camera Notifications* > *Notification Events*.
2. Select *All* from the select recipient drop-down menu, or select the name of an account that should have received the notification. The list of notifications will be filtered by the recipient criteria. Only matching notifications will appear.
3. In the Message column, select the link to view the corresponding notification. A new tab opens, displaying the notification that was included in the email body, if any. The notification includes some images that are key frames from the motion detection video clip.

4. To view a video clip from the notification, select its key frame image. The notification window will be replaced with a video clip player.

Analyzing Logging

Log messages record important events on your FortiRecorder system for extensive monitoring over extended periods of time.

To configure logging, see the Configuring Log Settings section.

Understanding and using logs

FortiRecorder appliances can log many different activities including:

- camera recording events
- administrator-triggered events including logouts and configuration changes
- system-triggered events including system failures and HA activity

You can select a priority level that log messages must meet in order to be recorded.

The FortiRecorder appliance can save log messages to its memory, or to a remote location such as a Syslog server or FortiAnalyzer appliance. For more information, see “Configuring logging”.

Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

To download a log file

1. Go to one of the log types, such as *Monitor* > *Log* > *Event*.
2. Right click a desired log.
3. Select *Export to Table*. FortiRecorder converts the log entry to a .csv file.

Checking log threat levels

Each log message contains a Severity (pri) field that indicates the severity of the event that caused the log message, such as pri=warning.

Level (0 is greatest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.

Level (0 is greatest)	Name	Description
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations.

For each location where the FortiRecorder appliance can store log files (disk, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiRecorder appliance stores all log messages equal to or exceeding the log severity level selected.

For example, select Error and the FortiRecorder appliance stores log messages whose log severity level is Error, Critical, Alert, and Emergency.

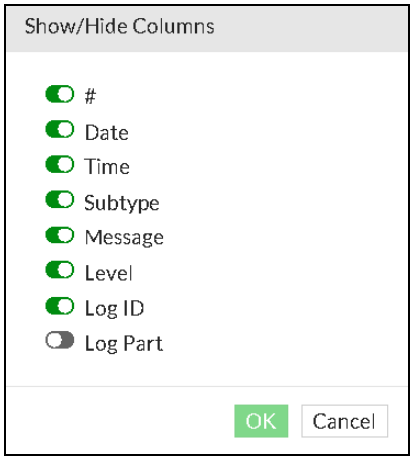
Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Displaying and organizing logs

You can display, hide, and re-order the display of logs.

To display or hide columns in logs

1. Go to one of the log types, such as *Monitor* > *Log* > *Event*.
2. Select the Configure View drop-down menu.
3. Select Show/Hide columns.



4. Enable or disable the desired columns.
5. Select *OK*.

To arrange the columns and rows

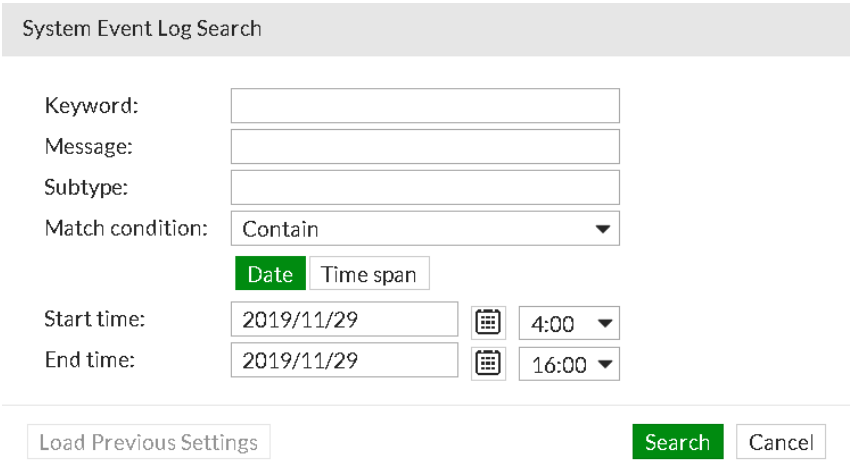
1. Select and drag the column into the desired position.
2. Hover your mouse cursor over one of the column headings. An arrow will appear on the right side of the heading. Click the arrow to display a drop-down menu, then select either Sort Ascending or Sort Descending to cause the rows to be sorted from either first to last, or last to first, based upon the contents of that column.
3. Column settings will not usually persist when changing pages, nor from session to session. If you want to keep the settings, you must select *Save View* from the Configure View drop-down menu.

Searching logs

When viewing attack logs, you can locate a specific log using the event log search function.

To search for a specific log

1. Go to one of the log types, such as *Monitor* > *Log* > *Event*.
2. Select *Search*.



3. Enter the following settings:

Setting Name	Description
Keyword	Type the word or phrase to search. The word may appear in any of the fields of the log message (e.g. Action and/or Message) or in any part of that field's value. If entering multiple words, they must occur uninterrupted in that exact order. For example, entering admin as a keyword will include results such as User admin2 logout from GUI(172.16.1.15) where part of the word appears in the middle of the log message. However, entering User logout would not yield any results, because in the log messages, those two words are always interrupted by the name of the account, and therefore do not exactly match your search key phrase. This setting is optional.
Message	Type all or part of the exact value of the Message (msg) field of the log messages that you want to find. This setting is optional.
Subtype	Enter the subtype, such as admin or system.
Match condition	Select whether your match criteria are specified exactly (Contain) or you have indicated multiple possible matches using an asterisk in Keyword (Wildcard).
Time	Select the date and time range that contains the attack log that you are searching for. This setting is optional. **Note**: The date fields default to the current date. Ensure the date fields are set to the actual date range that you want to search.

4. Select *Search*.

Reviewing logs

The event log section displays every administrative event that occurs on the FortiRecorder system, such as unsuccessful login attempts and system failures.

Camera log displays the start and stop recording events, factory rests, and various other camera-related events on the FortiRecorder system.

Detection log displays instances of camera detections, such as motion detection.

Assistant log displays all operations related to voice-controlled assistants, such as Amazon Alexa.

You can use the web UI to view and download locally stored log messages. (You cannot use the web UI to view log messages that are stored remotely on Syslog or FortiAnalyzer devices.) Log messages are in human-readable format, where each log field's name, such as Message (msg field when viewing a raw, downloaded log file), indicates its contents.

To view log messages

1. Go to *Monitor* > *Log* > *Event*. Columns and appearance varies slightly by the log type.
2. Select the level of severity and type of log you are searching for from the Level and Type drop-down menus.
3. Double-click the row of a log file for a more detailed description of the log entry.

Contents of the log section (some settings are only available in certain log types:

Setting Name	Description
Level	Select a severity level to hide log messages that are below this threshold (see “Checking log threats”).
Subtype	Select a subcategory (corresponding to the Subtype column) to hide log messages whose subtype field does not match.
Go to line	Type the index number of the log message (corresponding to the # column) that you want to jump to in the display.
Search	Click to find log messages matching specific criteria.
Back	Click to return to the list of log files stored on FortiRecorder’s hard drive.
Save View	Click to keep your current log view settings for subsequent views and sessions.
#	The index number of the log message within the log file. By default, the rows are sorted by time-stamp in descending order, starting with the most recent log message. **Note**: In the current log file, each log’s index number changes as new log messages are added, pushing older logs further down the stack. To find the same log message later, remember its time-stamp and Message, not its #.
Date	The date on which the log message was recorded. When in raw format, this is the log’s date field.
Time	The time at which the log message was recorded. When in raw format, this is the log’s time field.
Action	The action the camera performed, such as stopping and starting recording.
Subtype	The category of the log message, such as admin for events such as authentication or configuration changes, or system for events such as disk consumption or connection failures. When in raw format, this is the log’s subtype field.
Log ID	A dynamic log identifier within the system, not predictable, indicative of the cause nor necessarily a unique identifier. When in raw format, this is the log’s log_id field.
Detection Type/Subtype	The particular kind of detection the camera registered, such as motion.
Message	The log message that describes the specific occurrence of a recordable event.

Monitoring Face Recognition

Face recognition monitoring provides a comprehensive log of events captured by the AI cameras. The FortiRecorder Face Recognition AI module uses connected cameras to capture and recognize faces automatically using artificial intelligence. By gathering multiple images of a face, the module clusters together images that it recognizes as belonging to one person.

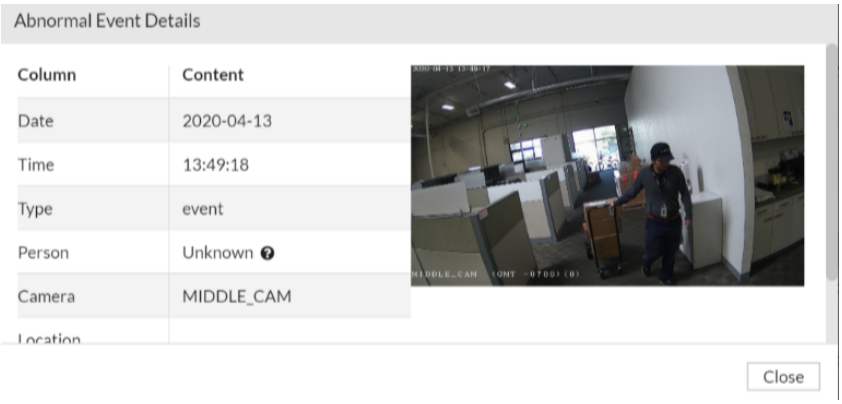
To learn more and to establish policies, see the Creating a policy section.

The Abnormal Events section displays instances when policies for abnormal events were triggered.

The Normal Event section displays instances when policies for normal events were triggered.

The Activity section displays instances when faces were captured by an AI camera, whether or not there was a policy associated with it.

Double click on any log to see more details. Hovering over the question mark symbol next to the Person Column displays a face screenshot.



You can filter through logs by person, camera, rule, and or time range by using the dropdown menu.

Monitoring DHCP Status

The DCHP status section displays the current status and address information of all connected cameras assigned an IP through a DHCP server.

Reviewing Security Information

FortiRecorder tracks all of the failed login attempts and the IPs that are currently blocked from accessing the system. In *Monitor* > *Security* > *Blocked IP*, you can remove blocked addresses as well as review when the blocking period ends.

To remove IPs from the Blocked IP list

1. Go to *Monitor* > *Security* > *Blocked IP*.
2. Select the desired IP address.
3. Select *Add to Exempt List*.

Modifying System Settings

The system settings section contains a wide variety of various ways to configure, maintain, and monitor your FortiRecorder system.

This section contains the following topics:

- Configuring network settings
- Creating and modifying administrator accounts
- Configuring system settings
- Customizing FortiRecorder and system messages
- Configuring data storage on the FortiRecorder
- Configuring LDAP and RADIUS authentication
- Working with certificates
- Performing system maintenance

Configuring Network Settings

Configuring the interface

Each of the FortiRecorder appliance's physical network adapter ports (or, for FortiRecorder-VM, vNICs) have a default IP address and netmask. If these IP addresses and netmasks are not compatible with the design of your unique network, you must configure them.

Network Interface*	IP Address	Netmask
port1	192.168.1.99	255.255.255.0
port2	192.168.2.99	255.255.255.0
port3	192.168.3.99	255.255.255.0
port4	192.168.4.99	255.255.255.0
*The number of network interfaces may vary by model.		

To connect to the CLI and web UI, you should configure the following FortiRecorder network settings:

- Interface: you must configure at least one network interface on your FortiRecorder appliance (usually port1) with an IP address and netmask so that it can receive your connections.
- Static route: Depending on your network, you also usually must configure a static route so that the FortiRecorder can connect to the Internet, your computer, and FortiCam cameras.
- DNS server: FortiRecorder appliances require connectivity to DNS servers for DNS lookups. The appliance will query the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP servers defined by their domain names.

To configure a network interface's IP address

1. Log in to the admin administrator account.
2. Go to *System* > *Network* > *Interface.*
3. Double-click the row to select the physical network interface that you want to modify.
4. If you want to manually assign an IP address and subnet mask to this network interface, select Manual and then provide the IP address and netmask in IP/Netmask. IPv4 and IPv6 subnet masks should be provided in CIDR format, e.g. /24 instead of 255.255.255.0. The IP address must be on the same subnet as the network to which the interface connects. **Two network interfaces cannot have IP addresses on the same subnet.**

   Otherwise, select DHCP and enable Connect to server to retrieve a DHCP lease when you save this configuration. If you want the FortiRecorder appliance to also retrieve DNS and default route (“gateway”) settings, also enable Retrieve default gateway and DNS from server.

   If you use DHCP on an interface and there are cameras connected to the interface, you must make sure the IP address will not change on that interface because the cameras need to communicate with the FortiRecorder and thus need to be aware of the IP address of the FortiRecorder.

   Retrieve default gateway and DNS from server will overwrite the existing DNS and default route, if any.

5. Configure the following settings:

Setting Name	Description
Discover cameras on this port	Enable to send multicast camera discovery traffic from this network interface. For more information, see “Connecting FortiRecorder to the cameras”.
Access	Enable the types of administrative access that you want to permit to this interface. **Caution**: Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiRecorder appliance.
Access: HTTPS	Enable to allow secure HTTPS connections to the web UI through this network interface. To configure the listening port number, see “Configuring system timeout, ports, and public access”. To upload a certificate, see “Replacing the default certificate for the web UI”.
Access: PING	Enable to allow: • ICMP type 8 (ECHO_REQUEST) or type 30 • UDP ports 33434 to 33534 for ping and traceroute to be received on this network interface. When it receives an ECHO_REQUEST, FortiRecorder will reply with ICMP type 0 (ECHO_RESPONSE). **Note**: Disabling PING only prevents FortiRecorder from receiving ICMP type 8 (ECHO_REQUEST) or type 30 and traceroute-related UDP.

Setting Name	Description
	It does not disable FortiRecorder CLI commands such as execute ping or execute traceroute that send such traffic.
Access: HTTP	Enable to allow HTTP connections to the web UI through this network interface. To configure the listening port number, see “Configuring system timeout, ports, and public access”. **Caution**: HTTP connections are not secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: SSH	Enable to allow SSH connections to the CLI through this network interface.
Access: SNMP	Enable to allow SNMP queries to this network interface, if queries have been configured and the sender is a configured SNMP manager. To configure the listening port number and configure queries and traps, see “SNMP traps & queries”.
Access: TELNET	Enable to allow Telnet connections to the CLI through this network interface. **Caution**: Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: FRC-Central	Enable to allow access from FortiRecorder Central.
MTU	Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiRecorder unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value. For example, RFC 2516 prescribes a value of 1492 for PPPoE. This option is available only for network interfaces that are directly associated with a physical link.
Administrative Status	Select either: • **Up** — Enable (that is, bring up) the network interface so that it can send and receive traffic. • **Down** — Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

6. Select *OK*.
   If you were connected to the web UI through this network interface, you are now disconnected from it.

7. To access the web UI again, in your web browser, modify the URL to match the new IP address of the network interface. For example, if you configured the network interface with the IP address 10.10.10.5, you would browse to: https://10.10.10.5

   If the new IP address is on a different subnet than the previous IP address, and your computer is directly connected to the FortiRecorder appliance, you may also need to modify the IP address and subnet of your computer to match the FortiRecorder appliance's new IP address.

Configuring routing

To add a static route

If you used DHCP and Retrieve default gateway and DNS from server when configuring your network interfaces, skip this step — the default route was configured automatically.

1. Log in to the admin administrator account. Other accounts may not have permissions necessary to change this setting.
2. Go to *System* > *Network* > *Routing*.
3. Select *New*.
4. Configure the following settings:

Setting Name	Description
Destination IP/netmask	Type the destination IP address and network mask of packets that will be subject to this static route, separated by a slash (/). The value 0.0.0.0/0 results in a default route, which matches all packets.
Interface	Select the desired port number from the dropdown menu.
Gateway	Type the IP address of the next-hop router where the FortiRecorder appliance will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in Destination IP/netmask, or forward packets to another router with this information. For a direct Internet connection, this will be the router that forwards traffic towards the Internet, and could belong to your ISP. **Note**: The gateway IP address must be in the same subnet as a network interface's IP address. Failure to do so will cause FortiRecorder to delete all static routes, including the default gateway.

5. Select *OK*.

   The FortiRecorder appliance should now be reachable to connections with networks indicated by the mask. When you add a static route through the web UI, the FortiRecorder appliance evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiRecorder appliance adds the static route, using the next unassigned route index number.

For small networks with only a few devices, often you will only need to configure one route: a default route that forwards packets to your router that is the gateway to the Internet.

If you have redundant gateway routers (e.g. dual Internet/ISP links), or a larger network with multiple routers (e.g. each of which should receive packets destined for a different subset of IP addresses), you may need to configure multiple static routes.

6. To verify connectivity, from a computer on the route's network destination, attempt to ping one of FortiRecorder's network interfaces that should be reachable from that location. If the connectivity test fails, you can use the CLI commands to determine if a complete route exists from the FortiRecorder to the host: `execute ping <destination_ipv4>` and to determine the point of connectivity failure: `execute traceroute <destination_ipv4>`.
7. Enable PING on the FortiRecorder's network interface and use the equivalent tracert or traceroute command on the computer (depending on its operating system) to test routability for traffic traveling in the opposite direction: from the host to the FortiRecorder.
   If these tests fail, or if you do not want to enable PING, first examine the static route configuration on both the host and FortiRecorder.
   To display the cached routing table, enter the CLI command:
   ```
   diagnose netlink rtcache list
   ```
   You may also need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blacklisting, and otherwise rule out problems at the physical, network, and transport layer.
   If these tests succeed, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.
   Verify that you have enabled HTTPS and/or HTTP on the network interface. Also examine routers and firewalls between the host and the FortiRecorder appliance to verify that they permit HTTP and/or HTTPS connectivity between them. Finally, you can also use the CLI command:
   ```
   diagnose system top 5 30
   ```
   to verify that the daemons for the web UI and CLI, such as sshd, newcli, and httpd are running and not overburdened. For details, see the FortiWeb CLI Reference.

Configuring DNS settings

To configure DNS settings

If you will use the settings DHCP and Retrieve default gateway and DNS from server when you configure your network interfaces, skip this — DNS is configured automatically.

1. Log in to the admin administrator account. Other accounts may not have permissions necessary to change this setting.
2. Go to *System* > *Network* > *DNS* and enter the IP addresses of a primary and secondary DNS server. Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, including the NTP system time. For improved performance, use DNS servers on your local network.

3. Select *Apply*.
4. To verify your DNS settings, in the CLI, enter the following commands: `execute traceroute www.fortinet.com`

DNS tests may not succeed if you have not yet completed “To add a static route”.

5. If the DNS query for the domain name succeeds, you should see results that indicate that the host name resolved into an IP address, and the route from FortiRecorder to that IP address:

```
traceroute to www.fortinet.com (192.0.43.10), 30 hops max, 60 byte packets
1 172.20.130.2 (172.20.130.2) 0.426 ms 0.238 ms 0.374 ms
2 static-209-87-254-221.storm.ca (209.87.254.221) 2.223 ms 2.491 ms 2.552 ms
3 core-g0-0-1105.storm.ca (209.87.239.161) 3.079 ms 3.334 ms 3.357 ms
...
16 43-10.any.icann.org (192.0.43.10) 57.243 ms 57.146 ms 57.001 ms
```

If the DNS query fails, you will see an error message such as:

www.fortinet.com: Temporary failure in name resolution

Cannot handle "host" cmdline arg `www.fortinet.com' on position 1 (argc 3)

Verify your DNS server IPs, routing, and that your firewalls or routers do not block or proxy UDP port 53.

Configuring the DHCP server

If you need the FortiRecorder DHCP service to connect cameras to the FortiRecorder, you can configure the DHCP server on the interface that the cameras connect to. For information about DHCP service and camera connection, see “Camera connection” on page 40.

To configure FortiRecorder's DHCP server via the web UI

1. Go to *System > Network > DHCP.*
2. Click *New*.
3. Mark the check box for Enable DHCP server.
4. Configure the following settings:

Setting Name	Description
Interface	Select the name of the network interface where this DHCP server will listen for requests from DHCP clients.
Gateway	Type the IP address that DHCP clients will use as their next-hop router.

Setting Name	Description
	On smaller networks, this is usually the same router that FortiRecorder uses. It could be your office's router, or cable/DSL modem.
DNS options	Select either: • Default — Leave DHCP clients' DNS settings at their default values. • Specify — Configure DHCP clients with the DNS servers that you specify in DNS server 1 and DNS server 2.
DNS server 1	Type the IP address of a DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if DNS options is set to Specify.
DNS server 2	Type the IP address of an alternative DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if DNS options is set to Specify.
Domain	Optional. Type the domain name, if any, that DHCP clients will use when resolving host names on the local domain.
Netmask	Type the subnet mask that DHCP clients will use in conjunction with the IP address that is assigned by FortiRecorder's DHCP server.
Conflicted IP timeout (Seconds)	Type the maximum amount of time that the DHCP server will wait for an ICMP ECHO (ping) response from an IP before it determines that it is not used, and therefore safe to allocate to a DHCP client that is requesting an IP address. The default is 1,800 seconds (3 minutes). To ensure that the DHCP server does not cause IP address conflicts with misconfigured computers that are accidentally using the pool of IP addresses used for DHCP, when a client request a new DHCP lease, the built-in DHCP server will ping an unused IP address in the pool first. If the ping test is successful, then a misconfigured computer is currently using that IP, and allocating it also to the DHCP client would cause an IP address conflict. To prevent this, the DHCP server will temporarily abandon that IP (mark it as used by a static host) and look for an other, available IP to give to the DHCP client. (It will not try abandoned IPs again until the pool is exhausted.) However, before the DHCP server can determine if the ping test is successful, the it must first wait to see if there is any reply. This slows down the search for an available IP address, and in rare cases, could cause a significant delay before the DHCP client receives its assigned IP address and other network settings. If your network is smaller or typically has low latency to ping replies, you can safely decrease this setting's value to improve DHCP speed and performance. In most cases, 3 seconds is enough.
Lease time (Seconds)	Type the maximum amount of time that the DHCP client can use the IP address assigned to it by the server. When the lease expires, the DHCP client must either request a new IP address from the DHCP server or renew its existing lease. Otherwise, the DHCP server may attempt to assign it to the next DHCP client that requests an IP. The default is 604,800 seconds (7 days).

Setting Name	Description
	If you have more or almost as many DHCP clients (cameras) as the number of IP addresses available to give to DHCP clients, you can decrease the lease. This will free up IP addresses from inactive clients so that IPs are available to give to clients that are currently in need of IP addresses. Keep in mind, however, that if the DHCP server is attached to your overall network rather than directly to cameras, this will slightly increase traffic volume and slightly decrease performance.
DHCP IP Range	To configure the DHCP lease pool — the range of IP addresses that the DHCP server can assign to its clients — click New and configure the first and last IP address in the range. To avoid DHCP pool exhaustion that can occur in some cases, the pool should be slightly larger than the total number of clients. If you need to exclude some IP addresses from this range (e.g. printers permanently occupy static IPs in the middle of the range), also configure DHCP Excluded Range. Tip: The built-in DHCP server can provide IP addresses to the computers on your network too, not just to cameras.
DHCP Excluded Range	To configure IPs that should be omitted from the DHCP pool and never given to DHCP clients (such if there are printers with manually assigned static IP addresses in the middle of your DHCP range), click New.
Reserved IP Address	To bind specific MAC addresses to a specific DHCP lease, guaranteeing that the DHCP server will never assign it to another DHCP client, click New. Caution: Reserved leases cannot prevent misconfigured computers from taking the IP address, causing an IP address conflict, and breaking the FortiRecorder's connection with the camera. See "Resolving IP address conflicts". Tip: To mimic a static IP address for your cameras, yet still provide the benefit that IP addresses are still centrally managed and configured on your DHCP server, configure reserved IP addresses.

5. Select *Create*.

   As cameras join the network, they should appear in the list of DHCP clients on *Monitor* > *DHCP* > *DHCP.*

Using traffic capture

When troubleshooting networks, traffic capture helps to look inside the contents of the packets to determine if the packets, route, and destination are correct. Traffic capture can also be called packet sniffing, a network tap, or logic analyzing. Packet sniffing provides information on the network at a low level, which helps troubleshoot problems, such as:

- finding missing traffic
- seeing if sessions are setting up properly
- locating ARP problems such as broadcast storm sources and causes
- confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks

- confirming routing is working as you expect
- intermittent missing PING packets.

If you are running a constant traffic application such as ping, traffic capture detects if the traffic is reaching its destination, how the port enters and exits the FortiRecorder unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. Traffic capture also verifies that the NAT is translating addresses or routing traffic as expected.

Before using traffic capture you should have a good sense of what you are looking for, since If you try traffic capture without a plan to narrow your search, you could end up with too much data to effectively analyze.

To capture the traffic

1. Go to *System* > *Network* > *Traffic Capture*.
2. Select *New*.
3. Enter a description for the file generated from the captured traffic.
4. Enter the time period for performing the packet capture.
5. Specify which interface you want to capture.
6. If you want to limit the scope of traffic capture, in the IP/HOST field, enter a maximum of 3 IP addresses or host names for which you want to capture.
7. Select the filter for the traffic capture:
   - Use protocol: Only UDP or TCP traffic on the specified port number will be captured.
   - Capture all: All network traffic will be captured.
8. For Exclusion, enter the IP addresses/host names and port numbers for which do not want to capture.
9. Select *Create*.

Creating and Modifying Administrator Accounts

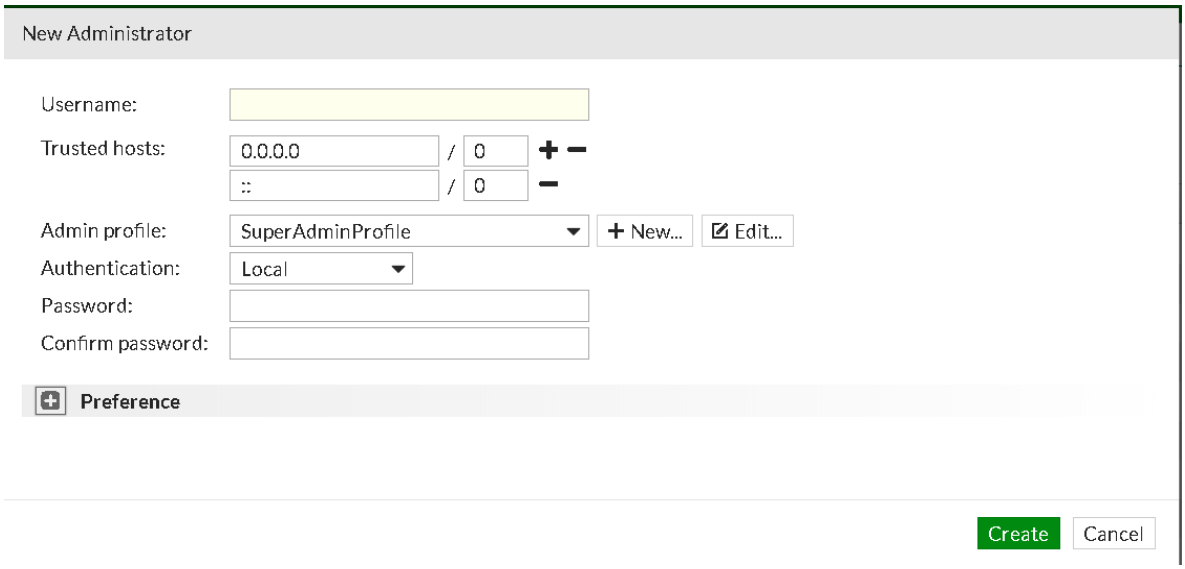
FortiRecorder allows different users to have different access privileges. In its factory default configuration, FortiRecorder has one administrator account named admin. This administrator has permissions that grant full access to FortiRecorder's settings and features.

Configuring an administrator account

Administrator accounts are accounts created for specific users that allow for the customizing of various privileges on the FortiRecorder.

To configure an account

1. Go to *System* > *Administrator* > *Administrator*.
2. Select *New*.



3. Expand the preference tab and configure the following settings:
4.

Setting Name	Description
Username	Type the name of the account, such as IT, that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters. **Note**: This is the entire user name that the person must provide when logging in to the CLI or web UI. Depending on Authentication, your external authentication server may require that you enter both the user name and the domain part, such as guard@example.com.
Trusted hosts	Type the IP address and netmask from which the account is allowed to log in to the FortiRecorder appliance. You can specify up to 10 trusted network areas. Each area can be a single computer, a whole subnet, or a mixture. To allow login attempts from any IP address, enter 0.0.0.0/0. To allow logins only from a single computer, enter its IP address and a 32-bit netmask, such as: 172.168.1.50/32 **Caution**: If you configure trusted hosts, do so for all accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even one account unrestricted (i.e. 0.0.0.0/0), the FortiRecorder appliance must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until after a login attempt has been received in order to check that user name's trusted hosts list. **Tip**: If you allow login from the Internet, set a longer and more complex Password, and enable only secure administrative access protocols (HTTPS and SSH) to minimize the security risk. For information on administrative access protocols, see "FortiRecorder configuration".

Setting Name	Description
	Tip: For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which only this administrator will log in.
Admin profile	Select an Admin profile that matches the access you want the administrator to posses. Create a new profile by selecting the New button or select a preexisting profile from the drop-down menu. For more information, see Configuring admin profiles.
Authentication	Select an authentication: **Local** — Authenticate using an account whose name, password, and other settings are stored locally, in the FortiRecorder's configuration. **RADIUS** — Authenticate by querying the remote RADIUS server that stores the account's name and password. Also configure RADIUS profile and Check permission attribute on RADIUS server. **RADIUS+Local** — Authenticate either by querying the remote RADIUS server that stores the account's name and password, or by querying the accounts stored locally, in the FortiRecorder appliance's configuration. Also configure RADIUS profile and Check permission attribute on RADIUS server. **LDAP** — Authenticate by querying a remote LDAP server that stores the account's name and password.
Password and Confirm password	Enter a password for the account. This field is available only when Authentication is Local or RADIUS + Local.
Display name	Enter a name for the recipient, such as FortiRecorder admin.
Email address	Enter the person's email address or an email alias, such as all-admins@example.com, that will receive snapshot notifications, if any, sent by FortiRecorder.
Theme	Select this administrator account's preference for the initial web UI color scheme or click Use Current to choose the theme currently in effect for your own web UI session. The administrator may switch the theme at any time after he or she logs in by clicking Next Theme in the top right corner.
Notification	Select either Email or SMS to send notification messages to this user. For SMS notification method, specify the SMS service provider and SMS recipient information.
SMS Provider and SMS Number	Enter the user's text messaging service provider and number to have FortiRecorder directly message the user.
Assistant User and Password	If this user has Amazon Alexa and/or IFTTT accounts, specify the account name and password so the user can use Alexa and/or Applets.

Configuring admin profiles

Admin profiles control which FortiRecorder functions users are allowed to access. You can create multiple profiles with multiple access controls. For example, you may want to create a profile for administrators that has access to all

functions, while also having a profile for a camera monitor that only has access to specific set of functions in FortiRecorder.

To configure an admin profile

1. Go to *System* > *Administrator* > *Admin Profile*.
2. Select *New*.
3. Enter a profile name.
4. Specify the access privileges. Profiles can have read-only, read-write, or no access rights to the following access categories:

Access Control	Description
System access	Controls settings critical to network accessibility of FortiRecorder • System Status page • GUI console • Network • Administrator • Authentication and certificates
System status	Controls other system settings, such as • Time • Remote storage • Log settings • Alert email
System configuration	Controls whether a whether user is able to access various system configurations.
System maintenance	Controls system maintenance, such as being able to backup system configurations.
Camera configuration	Controls camera installation and configuration. **Read:** Provides access to viewing configuration. **Write:** Enables modifying camera configuration.
Camera status	Controls camera status. **Read:** Provides access to viewing camera statistics and status. **Write:** Enables modifying camera statistics configuration.
Camera liveview	Controls whether a user can monitor the liveview of selected cameras. **Read:** Provides access to the camera's live view streaming. **Write:** Enables annotation.
Video playback	Controls whether a user can monitor the recorded video of selected cameras. **Read:** Provides a viewable timeline and playback of existing recordings. **Write:** Enables the ability to download an existing recording.
Camera analytic	Controls the camera analytic **Read:** Provides the user viewable results from motion and heat map analysis.

Access Control	Description
	Write: Enables the creation of motion and heatmap analysis.
Camera notification	Controls whether a user has access to various camera notification events, such as facial detection or motion detection. **Read:** Provides viewable notifications. **Write:** Enables the configuration of notifications.
Camera services	Controls camera services **Read:** Provides viewable configuration settings. **Write:** Enables modifying configuration.

5. Select *Create*.

Configuring access control

Access control determines which camera groups users are allowed to access and when users are allowed to access the cameras.

To configure access control

1. Go to *System* > *Administrator* > *Access Control*.
2. Select *New*.
3. Enter a name.
4. Specify a camera group the user is allowed to access.
5. Add an access schedule by selecting *New*.
6. Select the name of the schedule and whether to deny or allow access from the Access type drop-down menu.
7. Select *Create*.

Configuring System Settings

The configuration section contains a variety of settings to configure your FortiRecorder.

Establishing the Time

For many features to work, including camera synchronization, scheduling, logging, and SSL/TLS-dependent features, the FortiRecorder system time must be accurate.

You can either manually set the FortiRecorder system time or configure the FortiRecorder appliance to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

NTP is recommended to achieve better time accuracy. NTP requires that your FortiRecorder be able to connect to the Internet on UDP port 123. Adjust your firewall, if any, to allow these connections.

Later, when cameras are added to your surveillance system, your FortiRecorder synchronizes the camera clocks with its own to keep them in agreement.

To configure the system time

1. Go to *System* > *Configuration* > *Time*.
2. Either manually set the date and time or select to synchronize with NTP server.
3. Select *Apply*.

   If you manually configured the time, or if you enabled NTP and the NTP query for the current time succeeds, the new clock time should appear in System time. (If the query reply is slow, you may need to wait a couple of seconds, then click Refresh to update the display in System time.)

Configuring system options

The options section contains a variety of general system configurations, such as system timeout periods, ports, and public access.

Go to *System* > *Configuration* > *Options* to configure the system idle timeout, the HTTP, HTTPS, SSH, Telnet, and FortiRecorder Central access ports, and the host name for public/remote access.

If you want remote access — connecting from a home or a branch office through the Internet to your FortiRecorder — for either using the web UI or snapshot notification video clips while you are out of the office, you must configure both your network and the FortiRecorder.

First, on your office's firewall or Internet router, configure port forwarding and/or a virtual IP (VIP) to forward remote access connections from the Internet to your FortiRecorder's private network IP.

Remote access opens ports and can weaken the strength of your network security. To prevent attackers on the Internet from gaining access to your surveillance system, configure your firewall or router to require authentication, restrict which IP addresses can use your port forward/virtual IP, and scan requests for viruses and hacking attempts.

If you are not sure what your network's Internet address is, while connected to your office network, you can use an online utility such as: http://ping.eu/

Next, go to *System* > *Configuration* > *Options* and configure the following settings:

Setting Name	Description
Host name	Type either your network's IP on the Internet, or its domain name, such as www.example.com. This is either your Internet router's WAN IP, or a virtual IP (VIP) on your firewall whose NAT table will forward incoming connections from this public network IP to your FortiRecorder's private network IP.
HTTP/ HTTPS Port number	Type the port number, such as 8080, on your public IP that your Internet router or firewall will redirect to your FortiRecorder's listening port.

FortiRecorder supports live streaming (HLS) for mobile devices. You can use the FortiRecorder Mobile drop-down menu to enable live streaming over HTTP or HTTPS.

Configuring mail server settings for notification emails

The mail server settings section contains configuration options for establishing a mail server you can use to send notifications.

The default mail relay server is notification.fortinet.net

To establish notification emails

1. Go to *System* > *Configuration* > *Mail Server Settings.*
2. Configure the following settings:

Setting Name	Description
Host name	Type the host name for the appliance. The default FortiRecorder host name is the appliance's serial number. The host name is customizable and can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but not spaces and special characters. The host name of the FortiRecorder appliance is used in multiple places: • the subject line and content of notification emails. • the command prompt of the CLI. • the SNMP system name. For information about SNMP, see “SNMP traps & queries”. The get system status CLI command displays the full host name. If the host name is longer than 16 characters, the name may be truncated elsewhere and end with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiRecorder1234567890, the CLI prompt would be: FortiRecorder123~#
Use custom mail server	While the FortiRecorder can use a Fortinet mail server without any further configuration necessary, a custom mail server can be used instead of the Fortinet mail server (notification.fortinet.net).
Mail server name	Type the fully-qualified domain name (FQDN) of your SMTP server, such as mail.example.com. If you do not have your own email server, this is often the name of your ISP’s SMTP relay, or a 3rd-party email server such as Yahoo! or Gmail.
Mail server port	Type the port number on which your email server or SMTP relay listens for connections from clients.

Setting Name	Description
	The default varies by whether you enable Use SMTPS: disabled, it is port 25; enabled, it is port 465.
Use SMTPS	Enable to initiate SSL- and TLS-secured connections to the email server if it supports SSL/TLS. When disabled, SMTP connections from the FortiRecorder appliance's built-in email client to the SMTP server will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS-secured connections.
User name	Type the name of the account, such as jdoe or fortirecorder@example.com, that FortiRecorder will use to log in to the SMTP server.
Password	Type the password for the account on the SMTP server.
Authentication type	Select one of the following authentication methods: • **AUTO** — Automatically detect and use the most secure SMTP authentication type supported by the email server. • **PLAIN** — Provides an unencrypted, scrambled password. • **LOGIN** — Provides an unencrypted, scrambled password. • **DIGEST-MD5** — Provides an encrypted MD5 hash of the password. • **CRAM-MD5** — Provides an encrypted MD5 hash of the password, with hash replay prevention, combined with a challenge and response mechanism.
Sender display name	If you want to customize the display name in the emails sent by the FortiRecorder, type the desired name that will displayed by the email clients. By default, the display name FortiRecorder is used.
Sender address	Type the sender email address (From:) that will appear in the SMTP header. The default email address is noreply@fortirecorder.com.

3. Select *Apply*.

Configuring FortiRecorder to send SMS messages

For FortiRecorder to send SMS messages, you must specify the SMS service providers.

To configure FortiRecorder to send SMS messages

1. Go to *System* > *Configuration* > *SMS*.
2. Configure the following settings:
3.

Setting Name	Description
Service provider	Enter the SMS service provider name.
Description	Enter a short description of the provider.
Type	Select an SMS type: either SMTP or HTTP. For SMTP, enter the Email to, Email subject, and Email body information.

Setting Name	Description
	You can use the following tags when filing the fields: • **{{:country_code}}** represents the country code portion of the SMS number field in the user's configuration. • **{{:mobile_number}}** represents the phone number portion of the SMS number field in the user's configuration. • **{{:message}}** represents the text of the message. For HTTP, enter the following information: • **HTTP URL**: the HTTP or HTTPS URL to contact to send SMS messages, for example, https://myprovider.com/sendsms). • **HTTP method**: either Get or Post. • **HTTP/S Parameters**: configure all the parameters and values required by the provider to send the SMS message. You can use the same tags that were available above for SMTP. If you select the Encrypt check-box in a parameter then the value will not be displayed in clear-text when viewing the configuration. The value will be sent as entered to the remote server which is why using HTTPS is recommended. For example, if your provider indicates that to send a message the syntax should look like the following: https://smsserver.com:8080/sendsms?api_id=1234&user=user&to=<phone_number>&text=<message>&password=<passwd> Then the settings might be: HTTP URL: https://smsserver.com:8080/sendsms HTTP Method: Get Parameters: api_id id user user to {{:country_code}}{{:mobile_number}} text {{:message}} password password (the encrypt checkbox should be selected so this will not show in clear-text when viewing the configuration)

After configuring the SMTP server and the SMS service provider, configure the cameras to send notifications. For more information on configuring the cameras, see Configuring cameras to send notifications.

Configuring SNMP traps and queries

You can configure the FortiRecorder appliance's simple network management protocol (SNMP) agent to allow queries for system information and to send traps (alarms or event messages) to the computer that you designate as its SNMP manager. In this way you can use an SNMP manager to monitor the FortiRecorder appliance.

Before you can use SNMP, you must activate the FortiRecorder appliance's SNMP agent and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager connects. (See "SNMP".)

On the SNMP manager, you must also verify that the SNMP manager is a member of the community to which the FortiRecorder appliance belongs, and compile the necessary Fortinet-proprietary management information blocks (MIBs) and Fortinet-supported standard MIBs. For information on MIBs, see "MIB support"

Failure to configure the SNMP manager as a host in a community to which the FortiRecorder appliance belongs, or to supply it with required MIBs, will make the SNMP monitor unable to query or receive traps from the FortiRecorder appliance.

To configure the SNMP agent via the web UI

1. Add the MIBs to your SNMP manager so that you will be able to receive traps and perform queries. For instructions, see the documentation for your SNMP manager.
2. Go to *System* > *Configuration* > *SNMP*.
3. Configure the following:

Setting Name	Description
SNMP agent enable	Enable to activate the SNMP agent, so that the FortiRecorder appliance can send traps for the communities in which you enabled queries and traps. To receive queries, also SNMP on a network interface.
Description	Type a comment about the FortiRecorder appliance, such as dont-reboot. The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Location	Type the physical location of the FortiRecorder appliance, such as floor2. The location can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).
Contact	Type the contact information for the administrator or other person responsible for this FortiRecorder appliance, such as a phone number (555-5555) or name (jdoe). The contact information can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens (-) and underscores (_).

4. Select *Apply*.
5. Create at least one SNMP community to define which hosts are allowed to query, and which hosts will receive traps. See "Configuring an SNMP community".

Configuring an SNMP community

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiRecorder appliance to belong to at least one SNMP community so that community's SNMP managers can query the FortiRecorder appliance's system information and receive SNMP traps from the FortiRecorder appliance.

On FortiRecorder, SNMP communities are also where you enable the traps that will be sent to that group of hosts.

You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events that trigger a trap. You can also add the IP addresses of up to 8 SNMP managers to each community to designate the destination of traps and which IP addresses are permitted to query the FortiRecorder appliance.

To add an SNMP community via the web UI

1. Go to *System* > *Configuration* > *SNMP*.
2. If you have not already configured the agent, do so before continuing.

3. Under Community, select *New*.
4. Configure the following settings:

Setting Name	Description
Name	Type the name of the SNMP community to which the FortiRecorder appliance and at least one SNMP manager belongs, such as public. The FortiRecorder appliance will not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiRecorder appliance will include community name, and an SNMP manager may not accept the trap if its community name does not match. **Caution**: Fortinet strongly recommends that you do not add FortiRecorder to the community named public. This popular default name is well-known, and attackers that gain access to your network will often try this name first.
Enable	Enable this community entry.
Community Hosts: IP Address	Type the IP address of the SNMP manager that, if traps or queries are enabled in this community: will receive traps from the FortiRecorder appliance will be permitted to query the FortiRecorder appliance SNMP managers have read-only access. You can add up to 8. To allow any IP address using this SNMP community name to query the FortiRecorder appliance, enter 0.0.0.0. For security best practice reasons, however, this is not recommended. **Caution**: FortiRecorder sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment. **Note**: If there are no other host IP entries, entering only 0.0.0.0 effectively disables traps because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager.
Queries	Type each port number (161 by default) on which the FortiRecorder appliance listens for SNMP queries from the SNMP managers in this community, then enable it. Port numbers vary by SNMP v1 and SNMP v2c.
Traps	Type each port number (162 by default) that will be the source (Local) port number and destination (Remote) port number for trap packets sent to SNMP managers in this community, then enable it. Port numbers vary by SNMP v1 and SNMP v2c.
SNMP Event	Enable the types of SNMP traps that you want the FortiRecorder appliance to send to the SNMP managers in this community. • System events (system reboot, system reload, system upgrade, log disk formatting, and video disk formatting) • Remote storage event • Interface IP change • Camera events (enabling, disabling, communication failure, recording failure, IP change, and camera reboot)

Setting Name	Description
	While most trap events are described by their names, the following events occur when a threshold has been exceeded: • CPU Overusage • Memory Low • Log Disk Usage Threshold • Video Disk Usage Threshold To configure their thresholds, see “To configure the SNMP agent via the web UI”. For more information on supported traps and queries, see “MIB support”.

5. Select *OK*.
6. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiRecorder appliance, be sure to test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiRecorder appliance. To test traps, cause one of the events that should trigger a trap.

Configuring SNMP v3 users

If your SNMP manager supports SNMP v3, you can specify which of its user accounts is permitted to access information about your FortiRecorder appliance. This provides greater granularity of control over who can access potentially sensitive system information.

To specify access for an SNMP user via the web UI

1. Go to *System* > *Configuration* > *SNMP.*
2. If you have not already configured the agent, do so before continuing. See “To configure the SNMP agent via the web UI”.
3. Expand the user section and select *New*.
4. Configure the following settings:

Setting Name	Description
User name	Enter the name of the SNMP user. This must match the name of the account as it is configured on your SNMP manager. You can add up to sixteen users.
Enable	Enable this user entry.
Security level	Choose one of the three security levels: • **No authentication, no privacy** — Causes SNMP v3 to behave similar to SNMP v1 and v2, which provides neither secrecy nor guarantees authenticity, and therefore is not secure. This option should only be used on private management networks. • **Authentication, no privacy** — Enables authentication only, guaranteeing the authenticity of the message, but not safeguarding it from eavesdropping. Also configure Authentication protocol.

Setting Name	Description
	• A**uthentication, privacy** — Enables both authentication and encryption, guaranteeing authenticity as well as secrecy. Also configure Privacy protocol.
Authentication protocol	Select either SHA-1 or MD5 hashes for authentication. Also configure a salt in Password. Both the protocols and passwords on the SNMP manager and FortiRecorder must match.
Privacy protocol	Select either AES or DES encryption algorithms. Also configure a salt in Password. Both the protocols and passwords on the SNMP manager and FortiRecorder must match.

5. Similar to configuring the SNMP community, configure the other settings to specify the trap recipient IP, allowed query source IPs, and trap events (see “Configuring an SNMP community”).
6. Select *OK*.
7. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiRecorder appliance, be sure to test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiRecorder appliance. To test traps, cause one of the events that should trigger a trap.

MIB support

The FortiRecorder SNMP agent supports the following management information blocks (MIBs):

MIB or RFC	Description
Fortinet Core MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FortiRecorder MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiRecorder-specific information and to receive FortiRecorder-specific traps.
RFC-1213 (MIB II)	The FortiRecorder SNMP agent supports MIB II groups, except: • There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, and so on.) do not accurately capture all FortiRecorder traffic activity. More accurate information can be obtained from the information reported by the FortiRecorder MIB.
RFC-2665 (Ethernet-like MIB)	The FortiRecorder SNMP agent supports Ethernet-like MIB information, except the dot3Tests and dot3Errors groups.

You can obtain these MIB files from the Fortinet Technical Support web site, https://support.fortinet.com/.

To communicate with your FortiRecorder appliance’s SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query’s name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps sent include the message, the FortiRecorder appliance's serial number, and host name.

Customizing FortiRecorder and Messages

This section contains settings to customize messages sent by the FortiRecorder unit and the overall appearance of the web UI.

Customizing replacement messages

The FortiRecorder system delivers custom system messages to the user, such as disclaimers or camera notifications.

The disclaimers and notifications are customizable. When you create email template in *System* > *Customization* > *Custom Email Template*, you can use many of the replacement messages.

To view the replacement message list

1. Go to *System* > *Customization* > *Custom Message*.
2. Expand the section to display the replacement messages for that category. The message list organizes replacement messages into types, such as System. Double-click each replacement message to customize that message. You can reword existing messages or create new ones.

Additionally, you can modify the text and HTML code within a replacement message to suit your requirements.

You can change the content of the replacement message by editing the text and HTML codes and by working with replacement message variables.

All message groups can be edited to change text, or add text and variables.

To customize text replacement messages

1. Go to *System* > *Customization* > *Custom Message*.
2. Select a message and select *Edit*.
3. Enter the desired message in the content area. There is a limit of 4000 characters for each message.
4. Some messages can contain custom variables, such as the date. To add a custom variable to the message:
   - Select *Insert Variables*. If no custom variables exist, the *Insert Variables* link does not appear.
   - Place your mouse cursor in the text message at the insertion point of the variable.
   - Select the name of the variable to add. It will appear at the insertion point.
   - Select the close icon.
5. Select *OK*.

In addition to adding predefined variables to your system messages, you can create new variables. Typically these variables represent frequently used messages. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

To create a new variable

1. Go to *System* > *Customization* > *Custom Messages*.
2. Select a message and then select *Edit Variable*.

3. Select *New*.
4. Configure the following:

Setting Name	Description
Name	Enter the variable name to use in the system message. Its format is: %%<variable_name>%%. For example, if you enter the word “warning”, this variable appears as %%warning%% in the system message if you select to insert it.
Display name	Enter a description for the variable. The display name appears in the variable list when you select Insert Variables while customizing a message or creating a variable.
Content	Enter the variable’s content. For example: The came %%CAMERA_NAME%% has detected motion on %%EVENTDATE%%.

5. Select *Create*.

The following table is a list of default replacement:

Variable	Description
%%ADDRESS%%	The senders address of the notification message.
%%ADMIN_USER%%	The administrator notified by the notification message.
%%BODY%%	The content of the camera notification message.
%%CONTENT%%	The content of the alert message.
%%DATE%%	The day when the notification is sent.
%%EVENT_DATE%%	The day the event captured by the camera that triggered the notification.
%%EVENT_LINK%%	The link to the event captured by the camera that triggered the notification.
%%EVENT_TITLE%%	The title of the event captured by the camera that triggered the notification.
%%HOSTNAME%%	The name of the host.
%%LOCATION%%	The location of the event that triggered the notification and that is featured in the clip.
%%MOBILE_APPLE_BADGE%%	The placement of the Apple icon in the mobile account registration email.
%%MOBILE_GOOGLE_BADGE%%	The placement of the Google icon in the mobile account registration email.
%%MOBILE_APPLE_URL%%	The placement of Apple's address in the mobile account registration email.

Variable	Description
%%MOBILE_GOOGLE_URL%%	The placement of Google's address in the mobile account registration email.
%%MOBILE_QR%%	The placement of the QR code in the mobile account registration email.
%%MOBILE_QR_URL%%	The placement of the QR's address in the mobile account registration email.
%%MOBILE_EXPIRATION%%	The expiration time in the mobile account registration email.
%%NOTIFY_FROM%%	The notification from the alert message.
%%PIC_INDEX%%	Inserts a reference to the snapshot.
%%POSTMASTER%%	The name of the administrator of the email.
%%PUBLIC_ADDRESS%%	The publicly available email address.
%%QR_CODE%%	The location of the QR code.
%%QR_CODE_URL%%	The location of the QR code's address.
%%SENDER%%	The senders address of the notification message.
%%SUBJECT%%	The subject of the notification.
%%VID_LINK%%	The link to the clip that triggered the notification.

Customizing email templates

The FortiRecorder unit may send out notification emails for events such as alert or camera notification.

To customize email templates

1. Go to *System* > *Customization* > *Custom Email Templates*.
2. Select the template and then select *Edit*.
3. Enter the necessary information, such as the name and a brief description.
4. In the content section, format the message in HTML. To add variables, select Insert Variable.
5. Determine if the HTML code was entered correctly by selecting Preview.
6. Select *OK*.

Customizing the user interface appearance

You can customize the interface of the FortiRecorder, such as changing the default color of the interface or adding your own custom logo.

To customize the user interface appearance

1. Go to *System* > *Customization* > *Appearance*.
2. Configure the following to change the appearance of the UI:

Setting Name	Description
Product name	Enter the name of the product.
Custom top logo	Select *Change* to upload an icon used as the favicon for the FortiRecorder UI. The image's dimensions must be 460 pixels wide by 36 pixels tall. Use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic. Uploading a graphic overwrites the current graphic. The FortiMail unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time.
Default Theme	Select the default display theme (red, green, blue, and light blue) for the display of the web-based manager and login page. You can configure separate theme preferences for each administrator account. For details, see the Configuring an administrator account section.

3. Select *Apply*.

Customizing Single Sign On

The FortiRecorder provides custom single sign on methods.

To configure single sign on

1. Go to *System* > *Customization* > *Single Sign On*.
2. Enable Single Sign On.
3. Enter your Identity Provider Metadata in the entry field.
4. Enter the necessary information in the FortiRecorder Service Provider Metadata section fields.
5. Select **Apply**.

To configure FortiRecorder Admin Account Single Sign On to work with PingIdentity, see the Using Single Sign On with PingIdentity section in the FortiRecorder Cookbook.

Configuring Data Storage on the FortiRecorder

If you need to store video for longer periods of time, you can extended your FortiRecorder appliance's built-in storage.

Configuring local storage

Initially, your FortiRecorder appliance will store video data on its internal hard disk drive. By default, it will continue to do so, regardless of the video clip's age, until all available space is consumed. By storing files locally first, your FortiRecorder appliance's system resources are not continuously consumed by transferring video that may not be needed, nor by transferring them while it is recording (which is itself bandwidth-intensive). But on a per-camera basis, you can configure your FortiRecorder appliance to either delete old videos, or to move older videos to an external location.

Configuring RAID levels

FortiRecorder 400D model comes with two pre-installed hard drives in its four HDD bays and supports software RAID. This means that you can add two more hard drives if required.

FortiRecorder 400F comes with one 4TB hard drive. You can have one or more RAID arrays in the logical disk. For example, if you want redundancy you can have 4TB + 4TB drives and 8TB + 8TB drives, or with no redundancy you can keep the 4TB drive and add 2x8TB drives.

Number of Installed Hard Disk Drives	Available RAID Levels	Default RAID Level
1	0	0
2	0, 1	0
3	0, 5	0
4	0, 5, 10	0

To configure RAID levels

Back up data on the HDD before beginning this procedure. Changing the device's RAID level temporarily suspends all data processing and erases all data on the HDD.

1. Connect to the CLI console.
2. Enter the following command:
   ```
   execute raidlevel <level>
   ```
   The FortiRecorder unit changes the RAID level and reboots.

Recommended HDD models and capacities

Use surveillance grade rated models, such as Western Digital WD40PURX and Seagate ST4000VX000, with storage capacity between 2 to 4 TB.

If you are using old disks from another system (RAID or LVM), make sure to erase all the metadata on the drives.

Adding a RAID disk

Some FortiRecorder units, such as the 400F, support multiple hard disk drives.

To add a disk to the RAID array

1. Remove the hard disk bay from the unit.
2. Install the hard disk in the bay.
3. Insert the bay into the unit.
4. Go to *System* > *Storage* > *Local Storage*.
5. Select *Refresh*.
6. The newly added disk will appear under Drives.
7. Add the disk to an array.
8. Select *Refresh* again. The new array will appear under RAID Arrays.
9. Select the new array, and adjust the portions you want to allocate to log and video storage.
10. Select *Add To Logical Disks*.

Replacing a RAID disk

When replacing a disk in the RAID array, the new disk must have the same or greater storage capacity than the existing disks in the array. If the new disk has a larger capacity than the other disks in the array, only the amount equal to the smallest hard disk will be used. For example, if the RAID has 400 GB disks, and you replace one with a 500 GB disk, to be consistent with the other disks, only 400 GB of the new disk will be used.

FortiRecorder units support hot swap; shutting down the unit during hard disk replacement is not required.

To replace a disk in the array

1. Go to *System* > *Storage* > *Local Storage*.
2. In the row corresponding to the hard disk that you want to replace (for example, p4), select the hard disk and click Delete.
3. The RAID controller removes the hard disk from the list.
4. Protect the FortiRecorder unit from static electricity by using measures such as applying an antistatic wrist strap.
5. Physically remove the hard disk that corresponds to the one you removed in the web UI from its drive bay.
6. Replace the hard disk with a new hard disk, inserting it into its drive bay.
7. Select *Refresh*.

   The RAID controller will scan for available hard disks and should locate the new hard disk. Depending on the RAID level, the FortiRecorder unit may either automatically add the new hard disk to the RAID unit or allocate it as a spare that will be automatically added to the array if one of the hard disks in the array fails.

   The FortiRecorder unit rebuilds the RAID array with the new hard disk. Time required varies by the size of the array.

Replacing all RAID disks

If you want to replace the pre-installed hard drives with your own on FortiRecorder and build the RAID array from scratch, follow these instructions.

Because the HTTPs certificates are stored on the hard drive, if you still need them, you must back up the configuration first. The certificates will be backed up in the configuration file. After you install the new hard drives, restore the configuration. But if you're not using the factory certificates and you're planning to import your own certificate later on, you don't have to back up the configuration/certificates.

To replace all disks in the array

1. Shut down the FortiRecorder unit.
2. Remove the hard disks.
3. Install the new hard disks.
4. Boot up the system.
5. Enter the following CLI command to rebuild the disks:
   ```
   execute factoryreset disk
   ```

   This command will use the default RAID level based on the number of drives used. You can also use the following command to rebuild the disks with the specified RAID level. For the supported RAID levels, see “Configuring RAID levels”.

   ```
   execute raidlevel <level>
   ```

   Once completed, the system reboots.

Configuring external storage

To extend your local storage, you can use an external USB storage device if your FortiRecorder model has USB ports.

To safeguard your surveillance video in the event that your FortiRecorder appliance is destroyed by fire, flood, intrusion, or other event that it is recording, configure your FortiRecorder appliance to store its video at a remote location such as a branch office or cloud storage provider

It is recommended to connect the remote storage devices on a different interface than the cameras.

Tested and supported NFS servers

- Linux NAS
- FreeNAS
- Openfiler
- EMC VNXe3150 (version 2.4.2.21519(MR4 SP2))
- EMC Isilon S200 (OneFS 7.1.0.3)
- Windows Server 2016

Untested NFS servers

- Buffalo TeraStation
- Cisco Linksys NAS server
- Windows Server 2003 R2 and 2008

To configure external storage

1. Go to *System* > *Storage* > *External Storage*.
2. Enable external storage.
3. Expand the Device section and configure the following settings:

Setting Name	Description
Protocol	Select one of the following types of storage media: • **External USB** — External USB device. • **iSCSI Server** — An iSCSI (Internet Small Computer System Interface), server. • **NFS** — A network file system (NFS) server.
Maximum size	Specify the maximum video file size that is allowed to be stored on the external storage device. You can view the remote storage usage information on the Status page under *Dashboard* > *Status*.
Username	The user name of the FortiRecorder unit's account on the iSCSI server. This option only appears if iSCSI Server is the selected protocol.
Password	The password of the FortiRecorder unit's account on the iSCSI server. This option only appears if iSCSI Server is the selected protocol.
Hostname/IP Address	Type either the IP address or fully-qualified domain name (such as nas.example.com) of the iSCSI or NFS server. This option only appears if iSCSI Server or NFS is the selected protocol.
Port	Type the port number on which the server listens for connections. The default is 2049 for NFS and 3260 for iSCSI. This option only appears if iSCSI Server or NFS is the selected protocol.
Directory	Enter the path of the folder on the server, relative to the mount point or user's login directory, where the FortiRecorder appliance will store the data. **Note**: Do not use special characters such as a tilde (~). This will cause the storage to fail. This option only appears if NFS is the selected protocol.
Encryption key	The key used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters. This option only appears if iSCSI is the selected protocol.
iSCSI ID	The iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA). This option only appears if iSCSI is the selected protocol.

4. Expand the Status section. The Status section indicates if the iSCSI share was successfully mounted on the FortiRecorder unit's file system. This field appears only after you configure the iSCSI share and select *Apply*. Status may take some time to appear if the iSCSI server is slow to respond.

   If "Not mounted" appears, the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiRecorder unit has both read and write permissions on the iSCSI server.

5. Select *Apply*.

If the remote iSCSI device has not been formatted, before you can use it, you must format it with the following CLI command: execute storage format

6. Go to *Camera* > *Configuration* > *Camera*, then click to select a camera's row, then select *Edit*.
7. For Profile, select *New* or *Edit*.
8. From *Storage Options*, select *Move*. In the After n options that appear, select the age threshold that will cause FortiRecorder to move the video clips to external storage. Note that the *Move* option only appears after you have configured and enabled external storage.
9. Select *Create*.

Configuring LDAP and RADIUS Authentication

FortiRecorder supports both LDAP and RADIUS configuration.

Configuring RADIUS authentication

Except for local users, FortiRecorder supports RADIUS user authentication. RADIUS authentication profiles are used when adding user accounts.

To configure a RADIUS query

1. Go to *System* > *Authentication* > *RADIUS*.
2. Select *New*.
3. Configure the following settings:
4.

Setting Name	Description
Profile name	Enter a name (such as RADIUS-query) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the RADIUS server that will be queried when an account referencing this profile attempts to authenticate.
Server port	Enter the port number on which the authentication server listens for queries. The IANA standard port number for RADIUS is 1812.
Protocol	Select which authentication method is used by the RADIUS server: • **Password Authentication** • **Challenge Handshake Authentication** (CHAP) • **Microsoft Challenge Handshake Authentication** (CHAP) • **Microsoft Challenge Handshake Authentication V2** (CHAP version 2) • **Default Authentication Scheme**

Setting Name	Description
NAS IP/Called station ID	Type the NAS IP address or Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address of the FortiRecorder network interface used to communicate with the RADIUS server will be applied.
Server secret	Type the secret required by the RADIUS server. It must be the same as the secret that is configured on the RADIUS server.
Server requires domain	Enable if the authentication server requires that users authenticate using their full email address (such as user1@example.com) and not just the user name (such as user1).

5. Select *OK*,

   To test the query, select this profile when configuring an account, then attempt to authenticate using that account's credentials.

Configuring LDAP Authentication

FortiRecorder supports LDAP user authentication. You will use the LDAP authentication profiles when you add user accounts.

To configure an LDAP query

1. Go to *System* > *Authentication* > *LDAP*.
2. Select *New*.
3. Configure the following settings:

Setting Name	Description
Profile name	Type a name (such as LDAP-query) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Server name/IP	Type the fully qualified domain name (FQDN) or IP address of the LDAP or Active Directory server that will be queried when an account referencing this profile attempts to authenticate.
Fallback server name/IP	Type the fully qualified domain name (FQDN) or IP address of a secondary LDAP or Active Directory server, if any, that can be queried if the primary server fails to respond according to the threshold configured in "Timeout" on page 9.
Port	Type the port number on which the authentication server listens for queries. The IANA standard port number for LDAP is 389. LDAPS (SSL/TLS-secured LDAP) is 636.

Setting Name	Description
Use secure connection	If your directory server uses SSL to encrypt query connections, select SSL then upload the certificate of the CA that signed the LDAP server's certificate (see "Uploading trusted CAs' certificates").
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which FortiRecorder will search for user objects, such as ou=People,dc=example,dc=com. User objects should be child nodes of this location.
Bind DN	Enter the bind DN, such as cn=FortiRecorderA,dc=example,dc=com, of an LDAP user account with permissions to query the Base DN. Leave this field blank if you have enabled Allow unauthenticated bind.
Bind password	Enter the password of the Bind DN. Click Browse to locate the LDAP directory from the location that you specified in Base DN, or, if you have not yet entered a Base DN, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your Base DN, or need to look up attribute names. For example, if the Base DN is unknown, browsing can help you to locate it. Before using, first configure Server name/IP, Use secure connection, Bind DN, Bind password, and then click Create or OK. These fields provide minimum information required to establish the directory browsing connection.
LDAP user query	Enter an LDAP query filter that selects a set of user objects from the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects. For example, if user objects in your directory have two distinguishing characteristics, their objectClass and mail attributes, the query filter might be: (& (objectClass=inetOrgPerson) (mail=$m)) where $m is the FortiRecorder variable for a user's email address. This option is pre-configured and read-only if you have selected from Schema any schema style other than User Defined. For details on query syntax, refer to any standard LDAP query filter reference manual.
Scope	Select which level of depth to query, starting from Base DN. • **One level** — Query only the one level directly below the Base DN in the LDAP directory tree. • **Subtree** — Query recursively all levels below the Base DN in the LDAP directory tree.
Derefer	Select when, if ever, to dereference attributes whose values are references. • **Never** — Do not dereference. • **Always** — Always dereference. • **Search** — Dereference only when searching. • **Find** — Dereference only when finding the base search object.Base DN?

Setting Name	Description
User Authentication Options	Select how, if the query requires authentication, the FortiRecorder appliance will form the bind DN. The default setting is the third option: Search user and try bind DN. • **Try UPN or email address as bind DN** — Select to form the user's bind DN by prepending the user name portion of the email address ($u) to the User Principle Name (UPN, such as example.com). By default, the FortiRecorder appliance will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, enter that UPN in the field named Alternative UPN suffix. This can be useful if users authenticate with a domain other than the mail server's principal domain name. • **Try common name with base DN as bind DN** — Select to form the user's bind DN by establishing a common name to the base DN. Also enter the name of the user objects' common name attribute, such as cn or uid into the field. • **Search user and try bind DN** — Select to form the user's bind DN by using the DN retrieved for that user by User Query Options.
Allow Access Control Attribute	Select this option to define the access control
Allow Admin Profile Attribute	Select this option to define the admin profile.
Notification Options	Select the "Allow notification attributes" option to enable notifications. FortiRecorder supports the following notifications: • Email attribute: This attribute specifies the user's email address for notifications. • SMS profile attribute: This attribute specifies which SMS profile the user will use. The SMS profile attribute must match the name of the profile configured in FortiRecorder. • SMS number attribute: This attribute specifies the user SMS number for notification. The number format must be the same as the number in the user entry settings. • Method attribute: This attribute specifies the method used to notify a user. The two valid entries are "email" and "sms". • Embedded email images attribute: This attribute specifies whether images are included in email messages to the user. The two valid entries are "yes" and "no".
Timeout	Type the number of seconds that the FortiRecorder appliance will wait for a reply to the query before assuming that the primary LDAP server has failed, and will therefore query the secondary LDAP server. The default value is 20.
Protocol version	Select the LDAP protocol version (either 2 or 3) used by the LDAP server.
Allow unauthenticated bind	Enable to allow unauthenticated bind.
Enable cache	Enable to cache LDAP query results.

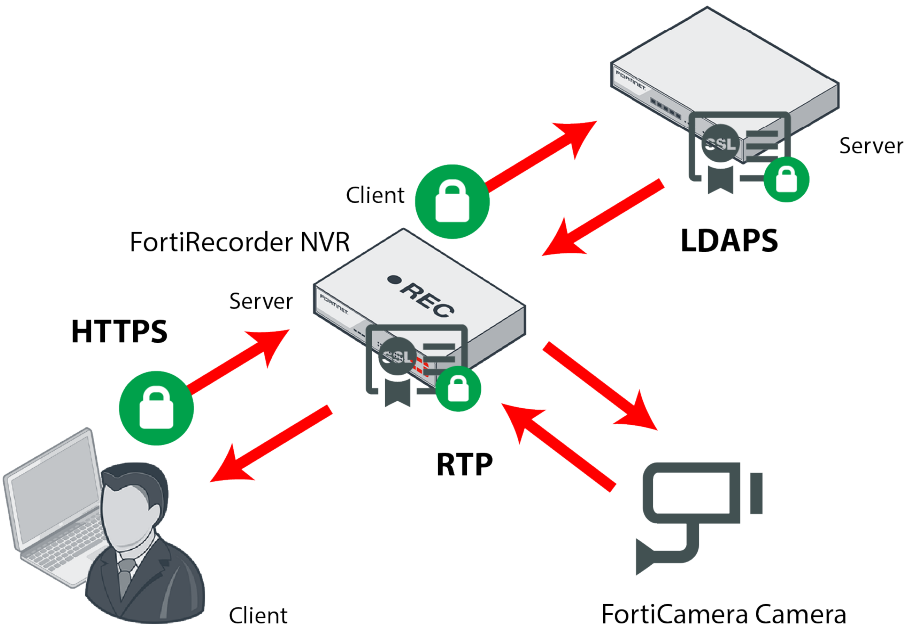
Setting Name	Description
	Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiRecorder appliance begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.
TTL	Enter the amount of time, in minutes, that the FortiRecorder unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiRecorder appliance to query the LDAP server, refreshing the cache. The default TTL value is 1440 minutes (one day). The maximum value is 10080 minutes (one week). Entering a value of 0 effectively disables caching. This option is applicable only if is enabled.

4. Select *Create*.

   To test the query, configure an account where this profile is used, then attempt to authenticate using that account's credentials.
   Alternatively, click the row to select the query, select Edit, then select Test LDAP Query. From the Select query type drop-down list, choose Authentication, then complete the Password and Mail address fields that appear. Select Test. After a few seconds, a dialog should appear to let you know that either the query succeeded, or the reason for its failure, such as a connectivity error.

Working with Certificates

When a FortiRecorder appliance initiates or receives an SSL or TLS connection, it will use certificates. Certificates can be used in secure connections for encryption and authentication.



FortiRecorder may require you to upload certificates and CRLs even if you do not use HTTPS. For example, when sending alert email via SMTPS, or querying an authentication server via LDAPS, FortiRecorder will validate the server's certificate by comparing the server certificate's CA signature with the certificates of CAs that are known and trusted by the FortiRecorder appliance. See "Uploading trusted CAs' certificates" and "Revoking certificates".

Supported cipher suites & protocol versions

How secure is an HTTPS connection?

A secure connection's protocol version and cipher suite, including encryption bit strength and encryption algorithms, is negotiated between the client and the SSL terminator during the handshake. (When you connect to the web UI via HTTPS, your FortiRecorder appliance is the SSL terminator.) Because security settings must agree, the result depends both on the appliance and your web browser.

FortiRecorder supports:

SSL 2.0

- RC4-MD5 — 40-bit & 128-bit

SSL 3.0

- AES-SHA — 256-bit & 128-bit
- CAMELLIA-SHA — 128-bit & 256-bit
- DES-CBC3-SHA — 168-bit
- DES-CBC-SHA — 40-bit & 56-bit
- DHE-RSA-AES-SHA — 256-bit & 128-bit

- DHE-RSA-CAMELLIA-SHA — 256-bit & 128-bit
- DHE-RSA-SEED-SHA — 128-bit
- EDH-RSA-DES-CBC3-SHA — 168-bit
- EDH-RSA-DES-CBC-SHA — 40-bit & 56-bit
- RC4-SHA — 128-bit
- RC4-MD5 — 40-bit & 128-bit
- SEED-SHA — 128-bit

TLS 1.0

- AES-SHA — 256-bit & 128-bit
- CAMELLIA-SHA — 128-bit & 256-bit
- DES-CBC3-SHA — 168-bit
- DES-CBC-SHA — 40-bit & 56-bit
- DHE-RSA-AES-SHA — 256-bit & 128-bit
- DHE-RSA-CAMELLIA-SHA — 256-bit & 128-bit
- DHE-RSA-SEED-SHA — 128-bit
- EDH-RSA-DES-CBC3-SHA — 168-bit
- EDH-RSA-DES-CBC-SHA — 40-bit & 56-bit
- RC4-SHA — 128-bit
- RC4-MD5 — 40-bit & 128-bit
- SEED-SHA — 128-bit

AES-256 or ECC, and SHA-1 are preferable. Generally speaking, for security reasons, avoid using:

- SSL 2.0
- TLS 1.0
- Older hash algorithms, such as MD5. (On modern computers, these can be cracked quickly.)
- Ciphers with known vulnerabilities, such as some implementations of RC4, AES and DES (e.g. To protect clients with incorrect CBC implementations for AES and DES, prioritize RC4.)
- Encryption bit strengths less than 128
- Older styles of re-negotiation (These are vulnerable to man-in-the-middle (MITM) attacks.)

Client-initiated re-negotiation

Replacing the default certificate for the web UI

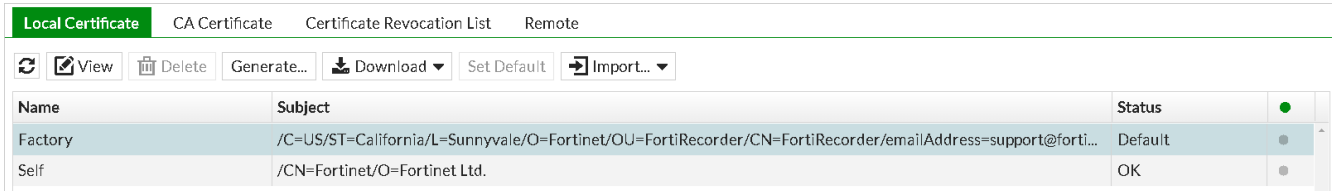
For HTTPS connections with the web UI, FortiRecorder has its own X.509 server certificate. By default, the FortiRecorder appliance presents the “Factory” certificate, which can be used to encrypt the connection, but whose authenticity cannot be guaranteed and therefore may not be trusted by your web browser. This will cause your web browser to display a security alert, indicating that the connection may have been intercepted.

To prevent this false alarm, you can go to *System* > *Certificate* > *Local Certificate* to replace the certificate with one that is signed by your own CA so that it will be trusted. Thereafter, a security alert will only occur if:

- the certificate expires
- your CA revokes the certificate

- the connection has been compromised by a man-in-the-middle attack

If you have not yet requested a certificate from your CA, and if it requires one, you must first generate a certificate signing request (see “Generating a certificate signing request”). Otherwise, start with “Uploading & selecting to use a certificate”.



The following is an overview of the certificate interface section:

Setting Name	Description
View	Select to view the selected certificate’s issuer, subject, and range of dates within which the certificate is valid.
Delete	Select to delete the selected certificate.
Generate	Select to generate a certificate signing request. For details, see “Generating a certificate signing request”.
Download	Select to download the selected certificate’s entry in certificate (.cer), PKCS #12 (.p12), or certificate signing request (.csr) file format. PKCS #12 is recommended if you require a certificate backup that includes the private key. Certificate backups can also be made by downloading a configuration file backup, which includes all certificates and keys.
Set status	To configure your FortiRecorder appliance to use a certificate, click its row to select it, then click this button. A confirmation dialog will appear, asking if you want to use it as the “default” (currently in use) certificate. Click OK. The Status column will change to reflect the new status.
Import	Select to upload a certificate. For details, see “Uploading & selecting to use a certificate”.
Name	Displays the name of the certificate according to the appliance’s configuration file. This will not be visible to clients.
Subject	Displays the distinguished name (DN) located in the Subject: field of the certificate. If the row contains a certificate request which has not yet been signed, this field is empty.
Status	Displays the status of the certificate. • **Default** — Indicates that this certificate will be used whenever a client attempts to connect to the appliance. Only one certificate can be in use at any given time. • **OK** — Indicates that the certificate was successfully imported. To use the certificate, select it, then use Set status to change its status. • **Pending** — Indicates that the certificate request (CSR) has been generated, but must be downloaded, signed, and imported before it can be used as a server certificate.

Generating a certificate signing request

Many commercial certificate authorities (CAs) will provide a web site where you can generate your own certificate signing request (CSR). A CSR is an unsigned certificate file that the CA will sign. When the CSR is generated, the associated private key that the appliance will use to sign and/or encrypt connections with clients is also generated.

If your CA does not provide this, or if you have your own private CA such as a Linux server with OpenSSL, you can use the appliance generate a CSR and private key. This CSR can then be submitted for verification and signing by the CA.

To generate a certificate request

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Select Generate.
3. Configure the certificate signing request:
4.

Setting Name	Description
Certification name	Enter a unique name for the certificate request, such as fortirecorder.example.com. This can be the name of your appliance.
Subject Information: ID Type	Select the type of identifier to use in the certificate to identify the FortiRecorder appliance: • **Host IP** — Select if the FortiRecorder appliance has a static IP address and enter the public IP address of the FortiRecorder appliance in the IP field. If the FortiRecorder appliance does not have a public IP address, use E-Mail or Domain Name instead. • **Domain Name** — Select if the FortiRecorder appliance has a static IP address and subscribes to a dynamic DNS service. Enter the FQDN of the FortiRecorder appliance, such as fortirecorder.example.com, in the Domain Name field. Do not include the protocol specification (http://) or any port number or path names. • **E-Mail** — Select and enter the email address of the owner of the FortiRecorder appliance in the E-mail field. Use this if the appliance does not require either a static IP address or a domain name. The type you should select varies by whether or not your FortiRecorder appliance has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate. For example, if your FortiRecorder appliance has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web UI by the domain name of the FortiRecorder appliance, you might prefer to generate a certificate based upon the domain name of the FortiRecorder appliance, rather than its IP address.
Subject Information: IP	Type the static IP address of the FortiRecorder appliance, such as 10.0.0.1. The IP address should be the one that is visible to clients. Usually, this should be its public IP address on the Internet, or a virtual IP that you use NAT to map to the appliance's IP address on your private network. This option appears only if ID Type is Host IP.

Setting Name	Description
Subject Information: Domain Name	Type the fully qualified domain name (FQDN) of the FortiRecorder appliance, such as www.example.com. The domain name must resolve to the static IP address of the FortiRecorder appliance or protected server. For more information, see “FortiRecorder configuration”. This option appears only if ID Type is Domain Name.
Subject Information: E-mail	Type the email address of the owner of the FortiRecorder appliance, such as admin@example.com. This option appears only if ID Type is E-Mail.
Key type	Displays the type of algorithm used to generate the key. This option cannot be changed, but appears in order to indicate that only RSA is currently supported.
Key size	Select a secure key size of 512 Bit, 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate, but provide better security.
Optional Information: Organization unit	Optional. Type the name of your organizational unit (OU), such as the name of your department. To enter more than one OU name, click the + icon, and enter each OU separately in each field.
Optional Information: Organization	Optional. Type the legal name of your organization.
Optional Information: Locality (City)	Optional. Type the name of the city or town where the FortiRecorder appliance is located.
Optional Information: State/Province	Optional. Type the name of the state or province where the FortiRecorder appliance is located.
Optional Information: Country/Region	Optional. Select the name of the country where the FortiRecorder appliance is located.
Optional Information: E-mail	Optional. Type an email address that may be used for contact purposes, such as admin@example.com.

5. Select *OK*.

   The FortiRecorder appliance creates a private and public key pair. The generated request includes the public key of the FortiRecorder appliance and information such as the FortiRecorder appliance’s IP address, domain name, or email address. The FortiRecorder appliance’s private key remains confidential on the FortiRecorder appliance. The Status column of the entry is Pending.
6. Click to select the row that corresponds to the certificate request.
7. Select *Download*.

   Standard dialogs appear with buttons to save the file at a location you select. Your web browser downloads the certificate request (.csr) file. Time required varies by the size of the file and the speed of your network connection.
8. Upload the certificate request to your CA

After you submit the request to a CA, the CA will verify the information in the certificate, give it a serial number, an expiration date, and sign it with the public key of the CA.

9. If you are not using a commercial CA whose root certificate is already installed by default on web browsers, download your CA's root certificate, then install it on all computers that will be connecting to your appliance. (If you do not install these, those computers may not trust your new certificate.)
10. When you receive the signed certificate from the CA, upload the certificate to the FortiRecorder appliance (see "Uploading & selecting to use a certificate").

Uploading & selecting to use a certificate

You can import (upload) either:

- Base64-encoded
- PKCS #12 RSA-encrypted

X.509 server certificates and private keys to the FortiRecorder appliance. The format of the certificate file that you have, and whether or not it includes the private key, may vary.

DSA-encrypted certificates are not supported if the FortiRecorder appliance is operating in a mode other than reverse proxy. See "Supported features per operation mode" on page 66.

If a server certificate is signed by an intermediate certificate authority (CA) rather than a root CA, before clients will trust the server certificate, you must demonstrate a link with root CAs that the clients trust, thereby proving that the server certificate is genuine. You can demonstrate this chain of trust either by:

- Appending a signing chain in the server certificate.
- Installing each intermediary CA's certificate in clients' trust store (list of trusted CAs).

Which method is best for you often depends on whether you have a convenient method for deploying CA certificates to clients, such as you may be able to for clients in an internal Microsoft Active Directory domain, and whether you often refresh the server certificate.

To append a signing chain in the certificate itself, before uploading the server certificate to the FortiRecorder appliance

1. Open the certificate file in a plain text editor.
2. Append the certificate of each intermediary CA in order from the intermediary CA who signed the local certificate to the intermediary CA whose certificate was signed directly by a trusted root CA.

   For example, an appliance's certificate that includes a signing chain might use the following structure:
   -----BEGIN CERTIFICATE-----
   <server certificate>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <certificate of intermediate CA 1, who signed the server certificate>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <certificate of intermediate CA 2, who signed the certificate of intermediate CA 1 and whose certificate was signed by a trusted root CA>
   -----END CERTIFICATE-----
3. Save the certificate.

To upload a certificate

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Select *Import* and the desired certificate
3. Configure the following settings:
4.

Type	Select the type of certificate file to upload, either: • **Local Certificate** — An unencrypted certificate in PEM format. • **Certificate** — An unencrypted certificate in PEM format. The private key is in a separate file. • **PKCS12 Certificate** — A PKCS #12 encrypted certificate with private key. Other available settings vary depending on this selection.
Certificate file	Select Browse to locate the certificate file that you want to upload. This option is available only if Type is Certificate or Local Certificate.
Key file	Select Browse to locate the private key file that you want to upload with the certificate. This option is available only if Type is Certificate.
Certificate with key file	Select Browse to locate the PKCS #12 certificate-with-key file that you want to upload. This option is available only if Type is PKCS12 Certificate.
Password	Type the password that was used to encrypt the file, enabling the FortiRecorder appliance to decrypt and install the certificate. This option is available only if Type is Certificate or PKCS12 Certificate.

5. Select *OK*.
6. To use a certificate, click its row to select it, then select *Set status* to put it in force.
7. If your web browser does not yet have your CA's certificate installed, download it and add it to your web browser's trust store so that it will be able to validate the appliance's certificate (see "Uploading trusted CAs' certificates").

Uploading trusted CAs' certificates

In order to authenticate other devices' certificates, FortiRecorder has a store of trusted CAs' certificates. Until you upload at least one CA certificate, FortiRecorder does not know and trust any CAs, it cannot validate any other client or device's certificate, and all of those secure connections will fail.

FortiRecorder may require you to upload certificates and CRLs even if you do not use HTTPS. For example, when sending alert email via SMTPS, or querying an authentication server via LDAPS, FortiRecorder will validate the server's certificate by comparing the server certificate's CA signature with the certificates of CAs that are known and trusted by the FortiRecorder appliance.

Certificate authorities (CAs) validate and sign others' certificates. When FortiRecorder needs to know whether a client or device's certificate is genuine, it will examine the CA's signature, comparing it with the copy of the CA's certificate that you have uploaded in order to determine if they were both made using the same private key. If they were, the CA's signature is genuine, and therefore the client or device's certificate is legitimate.

If the signing CA is not known, that CA's own certificate must likewise be signed by one or more other intermediary CAs, until both the FortiRecorder appliance and the client or device can demonstrate a signing chain that ultimately leads to a mutually trusted (shared "root") CA that they have in common. Like a direct signature by a known CA, this proves that the certificate can be trusted. For more information on how to include a signing chain, see "Uploading & selecting to use a certificate".

To upload a CA's certificate

1. Obtain a copy of your CA's certificate file.

   If you are using a commercial CA, your web browser should already contain a copy in its CA trust store. Export a copy of the file to your desktop or other folder. If you are using your own private CA, download a copy from your CA's server

   Verify that your private CA's certificate does not contain its private keys. Disclosure of private keys compromises the security of your network, and will require you to revoke and regenerate all certificates signed by that CA.

2. Go to *System* > *Certificate* > *CA Certificate*.
   To view the selected certificate's issuer, subject, and range of dates within which the certificate is valid, click a certificate's row to select it, then click View.
3. Select *Import*.
4. In Certificate name, type a name for the certificate that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. Next to Certificate file, select the Browse button and select your CA's certificate file.
6. Select *OK*. Time required to upload the file varies by the size of the file and the speed of your network connection.
7. To test your configuration, cause your appliance to initiate a secure connection to an LDAPS server (see "To configure an LDAP query" and "To configure an account").

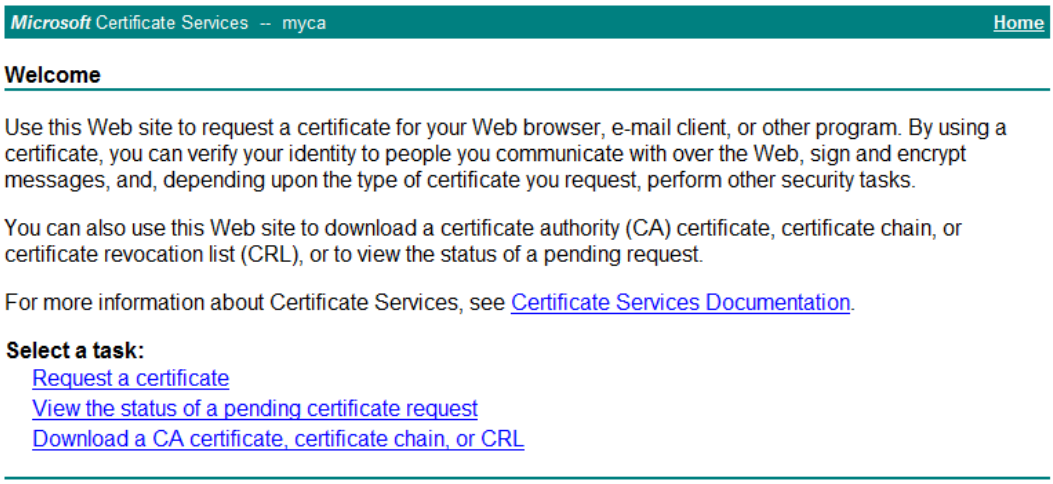
   If the query fails, verify that your CA is the same one that signed the LDAP server's certificate, and that its certificate's extensions indicate that the certificate can be used to sign other certificates. Verify that both the appliance and LDAP server support the same cipher suites and SSL/TLS protocols. Also verify that your routers and firewalls are configured to allow the connection.

Example: Downloading the CA's certificate from Microsoft Windows 2003 Server

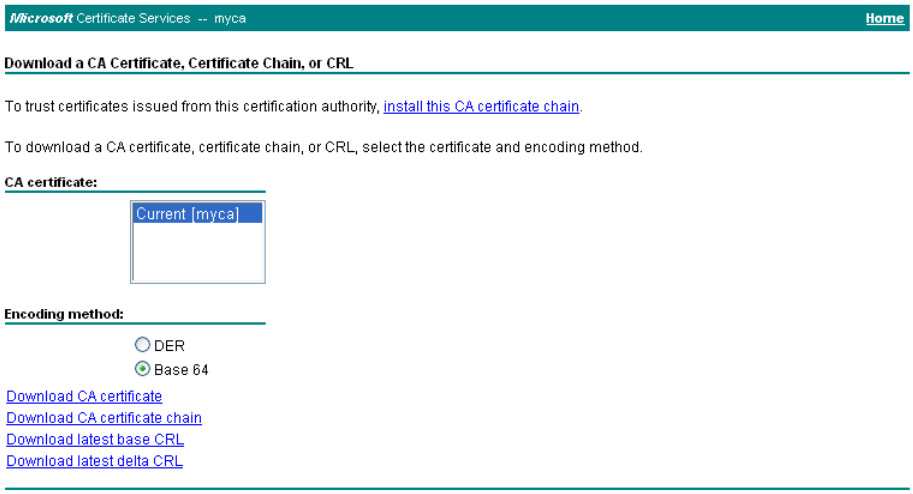
If you are generated and signed your LDAP server's certificate using Microsoft Certificate Services on Microsoft Windows 2003 or 2008 Server, you must download the CA's certificate and provide it to the FortiRecorder appliance so that it will be able to verify the CA signature on the certificate.

To download a CA certificate from Microsoft Windows 2003 Server

1. On your management computer, start your web browser.
2. Go to:
   https://<ca-server_ipv4>/certsrv/
   where <ca-server_ipv4> is the IP address of your CA server.
3. Log in as Administrator, since other accounts may not have sufficient privileges. The Microsoft Certificate Services home page for your server's CA should appear:



4. Select the *Download CA certificate, certificate chain, or CRL* link. The *Download a CA Certificate, Certificate Chain, or CRL* page appears:



5. Select *Base64* from *Encoding Method*.
6. Select *Download CA certificate*.
7. Select a location to save the CA's certificate file if prompted by your browser.

Revoking certificates

To ensure that your FortiRecorder appliance validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list (CRL), which may be provided by certificate authorities (CA).

Alternatively, you can use HTTP or online certificate status protocol (OCSP) to query for certificate status. For more information, see “Revoking certificates by OCSP query”.

To upload a CRL file

1. Go to *System* > *Certificate* > *Certificate Revocation List*.
2. Select *Import*.
3. In Certificate name, type the name of the certificate as it will be referred to in the appliance’s configuration file.
4. Next to Certificate file, click Browse, then select the certificate file.
5. Select *OK*.

   The certificate is uploaded to the appliance. TIme required varies by the size of the file and the speed of the network connection, but is typically only a few seconds.

Revoking certificates by OCSP query

Online certificate status protocol (OCSP) enables you to revoke or validate certificates by query, rather than by importing certificate revocation list (CRL) files. Since distributing and installing CRL files can be a considerable burden in large organizations, and because delay between the release and install of the CRL represents a vulnerability window, this can often be preferable.

To use OCSP queries, you must first install the certificates of trusted OCSP/CRL servers.

To view or upload a remote certificate

1. From your OCSP/CRL server, download its server certificate.
2. Go to *System* > *Certificate* > *Remote*.
3. Select *Import*.
4. In Certificate name, type the name of the certificate as it will be referred to in the appliance’s configuration file.
5. Next to Certificate file, click Browse, then select the certificate file.
6. Select *OK*.

   The certificate is uploaded to the appliance. Time required varies by the size of the file and the speed of the network connection, but is typically only a few seconds.

Performing System Maintenance

The Maintenance section enables you to back up your system configuration, restore configuration, restore firmware, and download the trace log.

Backing up configuration

Before installing FortiRecorder firmware or making significant configuration changes, back up your FortiRecorder configuration. Backups let you revert to your previous configuration if the new configuration does not function correctly. Backups can also be used to compare changes in configuration.

To back up the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. Click on *System configuration backup*.
3. Save the configuration file.

   Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see “Restoring configuration”.

Restoring configuration

If you have just downgraded or restored the firmware of the FortiRecorder unit, restoring the configuration file can be used to reconfigure the FortiRecorder unit from its default settings.

To restore the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. Under *Restore Configuration*, select *Browse* to locate and select the configuration file that you want to restore, then select *Open*.

   The FortiRecorder unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
3. After restoring the configuration file, verify that the settings have been successfully loaded.

Downloading the trace log

If Fortinet Technical Support requests a trace log for system analysis purposes, you can download one using the web UI.

Trace logs are compressed into an archive (.gz), and contain information that is supplementary to debug-level log files.

To download a trace file

1. Go to *System* > *Maintenance* > *Configuration*.
2. At the bottom of the tab, select *Download trace log*.

Security Monitoring

Security monitoring provides a variety of tools to ensure the security of the FortiRecorder unit.

This section contains the following topics:

- Configuring Intrusion Detection

Configuring Intrusion Detection

FortiRecorder features an intrusion detection mechanism to block IP addresses if failed login attempts from that IP address reach the threshold.

The blocking duration is based on the login history of the IP address. The more the IP address has been blocked in the past, the longer the IP address will remain blocked. The maximum time an IP address can be blocked is 45 days.

As an example, if you set the initial block period to 10 minutes, depending on the user's number of violations, the actual maximum block time can be up to 2 hours. If you set it to 30 minutes, the block time can be up to 12 hours. To avoid false positives, avoid using a longer initial block time setting. The recommended setting is less than 30 minutes. The default setting is 10 minutes.

If a user has consecutive unsuccessful login attempts within a certain period of time, the user's IP address is automatically added to an auto/dynamic exempt list.

To configure intrusion detection

1. Go to *Security* > *Intrusion Detection* > *Settings*.
2. Configure the following:

Setting Name	Description
Status	Select Enable, Disable, or Monitor only.
Access tracking	Enable or disable what types of login access is tracked: CLI or Web.CLI is the access via SSH and Web is the admin and webmail access via HTTP(S).
Initial block period	Specify how long the IP address will be blocked after its failed login attempts reach the threshold for the first time. The actual block time will be increased for repeated offenders.

3. Select *Apply*.

To manually exempt IP addresses from authentication reputation tracking

1. Go to *Security* > *Intrusion Detection* > *Exempt IP*.
2. Select *New*.
3. Enter the IP address and netmask.
4. Select *Create*.

To remove IPs from the auto exempt list

1. Go to *Security* > *Intrusion Detection* > *Auto Exempt IP*.
2. Select the desired IP address.
3. Select the delete button.

Configuring Schedules

The FortiRecorder schedule is important to the systems operation and is a pivotal component for a variety of different functions, such as determining the use of specific settings while recording.

For camera notification schedules, overlaps are not allowed but gaps are allowed. And one-time schedules take precedence over recurring schedules.

The default schedule is used when no schedules are selected or the selected schedules conflict with each other.

You cannot create a recurring recording schedule where the hours vary by the day of the week, but you can achieve the same effect if you create multiple schedules.

This chapter contains the following information:

- Establishing a Schedule
- Setting the Sunrise and Sunset Time

Establishing a Schedule

To configure schedules

1. Go to *Schedule* > *Schedule* > *Schedule*.
2. Select *New* and configure the following settings:

Setting Name	Description
Name	Enter a name for the schedule.
Description	Optionally enter a description.
Type	Select a schedule type: • **Recurring**: the schedule happens at specified times on selected days. • **One-time**: the schedule happens only on a specific date and time. • **Assistant:** use the digital assistant, such as Alexa.
Days and Time	Select the days you want the camera to begin recording if you have selected the Recurring schedule type.
All day	Select this option if you want to record all day long.
Star time/End time	Select the start and end time for the recurring recording or the start and end date for the one-time recording.

Setting Name	Description
	You can use the sunrise and sunset time for the start and end time. The sunrise and sunset time is calculated by the FortiRecorder's latitude and longitude location. For details, see "Setting the sunrise and sunset time". When using sunrise and sunset time, you can a plus or minus two hour offset to compensate for lighting conditions specific locations.

3. Select *Create*.

Setting the Sunrise and Sunset Time

When specifying schedules, you can use specific day and time, or the sunrise and sunset time.

To get the sunrise and sunset time

1. Go to *Schedule* > *Schedule* > *Settings*.
2. Enter the latitude and longitude values of the FortiRecorder and camera location.
3. Select *Calculate* to retrieve the sunrise and sunset time. A few days' sunrise and sunset time will be displayed.

When using a combination of sunrise/sunset and the specific time, if the time cross the boundary of sunrise/sunset, the schedule has no effect. For example, if the sunrise is at 8:00AM and you set the schedule from sunrise to 7:00AM, the schedule has no effect.

Modifying Camera Settings

Before connecting to your cameras, you must configure the settings that will be used by them. To reduce overhead, you don't need to create settings for each camera. Instead, configure items such as schedules and video quality once, then re-use those same settings for all cameras that should be similarly configured.

This section contains the following topics:

- Configuring Cameras
- Configuring Cameras to Send Notifications

Configuring Cameras

Camera configuration involves the following steps:

1. **Video profiles** define video quality. Video profiles are used in camera profiles. To configure video profiles, go to *Camera* > *Configuration* > *Video Profile*. For details, see "Configuring video profiles".
2. **Camera profiles** define video storage options and recording schedules (either continuous or motion detection). Camera profiles will be used when you configure the discovered cameras. To configure camera profiles, go to *Camera* > *Configuration* > *Camera Profile*. For details, see "Configuring camera profiles".
3. **Connect** the camera to the FortiRecorder. FortiRecorder can discover the connected cameras automatically and display them under *Camera* > *Configuration* > *Camera* with Status as Not Configured. See "Connecting FortiRecorder to the cameras".
4. After you configure the above settings, go to *Camera* > *Configuration* > *Camera* to configure all other camera settings, such as IP address, motion detection windows, and so on. See "Configuring cameras".
5. Go to *Camera* > *Configuration* > *Camera Group* to add individual camera to different groups to facilitate camera management. For details, see "Camera groups". Camera groups are used in user profiles. For details, see "User configuration workflow".

Configuring video profiles

Video profiles define the video quality that you want the camera to capture and stream to the FortiRecorder. Note that the higher the video quality, the more bandwidth it consumes. The video profiles will be used in the camera profiles. For details, see "Configuring camera profiles".

To configure a video profile

1. Go to *Camera* > *Configuration* > *Video Profile*.
2. Select *New*.

3. Configure the following settings:

Setting Name	Description
Name	Type a name (such as live-stream1) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Codec	Select the desired video compression format, such as H.264 AVC or H.25 HEVC.
Resolution	Select the amount of detail (the number of pixels) in the image. from the drop-down menu. Lower resolutions features less detail but are faster to transmit. Higher resolutions produce a clearer image but require more bandwidth. A higher resolution is preferable if the camera is recording a large space, such as a parking lot, where small details like faces and license plates could be important. **Note**: Resolution greatly impacts performance, bandwidth, and the rate at which disk space is consumed.
Frames per second	Type the number of frames per second (FPS). Conventional video is 24 frames per second. More frames per second may be useful if you need to record very fast motion, but increasing FPS will also increase disk usage and CPU usage.
Group of pictures	Select from the drop-down menu the duration of a Group of pictures (GOP) sequence. A GOP sequence is the interval between frames that contain the full image. Longer intervals save bandwidth, but slightly delay the start of live streams.
Bitrate mode	Select the bit rate: • **Variable** — Automatically adjust the stream to the minimum bit rate required by the current video frames while maintaining video quality. In variable bitrate mode the camera lowers the bitrate dynamically when little motion is present. This setting increases the presence of noise. • **Fixed** — Manually specify a constant bit rate in Bit rate. In fixed bitrate mode the camera attempts to keep the bitrate constant at the configured level. This guarantees calculated retention time and bandwidth but might show degraded image quality. For example, if there is a sudden burst of motion, like rain. • **Constrained** - Automatically adjusts the stream to lower the bitrate usage during periods of low activity, while enabling the ability to set the maximum bitrate the camera can stream.
Max bitrate	Enter the maximum bitrate the camera can stream. Lower bitrates use less bandwidth by sacrificing image quality. **Note:** Max bitrate is only available when selecting "Constrained" bitrate mode.
Quality	Select the degree of compression. Greater compression reduces required network bandwidth but causes greater CPU usage.

Setting Name	Description
Audio	Enable or disable audio.

4. Select *Create*.

Configuring camera profiles

A camera profile defines the video profiles to use, video storage options, and recording schedules.

To configure camera profiles

1. Go to *Camera* > *Configuration* > *Camera Profile*.
2. Select *New*.

3. Configure the following settings:

Setting Name	Description
Name	Enter a name (such as camera-settings1) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Video	Select the Recording stream profile used to determine the video quality of the recorded video. Select the Viewing stream profile used to determine the video quality of the streamed video when viewing. Select *Add schedule* to specify when to use low or high quality video. For example, you could improve the camera's night performance without sacrificing the quality of video during the day. **Note**: The higher the quality, the more bandwidth the stream will use.
Recording	Select the Recording type that will instruct the camera when to begin filming. • **Continuous**: records video for the entire duration of the schedule, regardless of movement or any other triggers. • **Motion detection**: records a video clip up to about 40 seconds long each time the camera's sensor detects movement. • **Digital input**: records a video clip up to about 40 seconds long each time the camera receives a trigger from the digital input. This option only takes effect if the camera supports DIDO. • **Audio detection**: records a video clip up to about 40 seconds long each time the camera detects audio activities. You can define the audio sensitivity when configuring camera settings. • **PIR detection**: PIR based motion detection senses the movement of people, animals, and other objects that produce heat energy. There are two storage options available for recording: • **FortiRecorder**: Store your recorded video on the FortiRecorder • **SD card**: Store your recorded video on SD card. **Note**: Some recording types may not be available for your camera. If you want to use different recording types at different times, click Add schedule to specify them. For example, you could instruct the camera to start recording for motion detection during the day and PIR detection at night.
Edge Download	You can select if and when you want video downloaded from the SD card. Enable either/or continuous recording or detection recording to determine when the FortiRecorder downloads recorded video.
Storage Options	You can select the storage options of both continuous recordings and detection recordings. • **Keep until overwritten**: Retain video until all available disk space, no matter local or remote, is almost full. Then the oldest video will be overwritten.

Setting Name	Description
	• **Delete**: Remove video when it exceeds the specified maximum age. Note that if the disk if full before the maximum age is reached, the oldest video will still be overwritten. • **Move**: Relocate video to external storage when it exceeds the specified maximum age. Note that if the local disk is full before the specified maximum age is reached, the oldest video will still be moved to remote storage. This option is only applicable if you have configured remote storage. • **Use continuous recordings if available**: Choose to mark motion periods in continuous recordings instead of extracting a separate clip from continuous recordings. This saves CPU load but does not allow deletion of the continuous recordings and only keeps motion sections for a period of time. If remote storage is configured, video is first stored on the local disk, then transferred to remote storage when the local disk needs space for newer video. The video will finally be deleted from remote storage when the remote disk needs space for newer video. Recordings will be stored on the hard disk as multiple video files. The oldest part of the recording will be deleted first.
Compression Options	Select whether or not FortiRecorder compresses continuous recordings. If compression is enabled, also configure the maximum amount of time to keep the files uncompressed. Files whose start time is older than the specified time will be compressed. **Note**: Selecting Compress will save storage space at the cost of video quality.

4. Select *Create*.

Configuring cameras

After connecting the cameras to FortiRecorder, configure the discovered cameras. Since most of the camera information was retrieved from the camera, the settings do not require changing; however, if you are adding a remote camera or adding a new camera before connecting it to FortiRecorder, you must specify all the camera settings.

To configure cameras

1. Go to *Camera* > *Configuration* > *Camera*.
2. For each discovered camera, click its row to select it.
3. Select *Configure* and configure the following settings:

Setting Name	Description
Enable	Mark this check box to enable the FortiRecorder to communicate with this IP address. Communications are required to trigger scheduled recordings and other camera commands.

Setting Name	Description
Name	Type a name (such as front-door1) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Location	Optional. Type a description of the camera's physical location that can be used if the camera is hidden, in case it is forgotten or lost.
Camera	FortiRecorder supports Fortinet cameras (FortiCam series) and third-party, ONVIF-compliant cameras. If you are configuring a discovered camera, most of the camera information has been retrieved and displayed. You can also click the Camera detail button to refresh the camera information. If you are adding a remote camera, or adding a new camera before it is connected, you must specify all the settings. For the Fortinet FortiCam cameras, you must specify the models; for the non-Fortinet cameras, you must specify the camera's login credentials (user name and password) for FortiRecorder to access it.
Model	Select the name of the camera model, such as FCM-20A for a FortiCam 20A.
Address mode	Select either: • **Wired**: Select this option if you want to keep the camera connected with the Ethernet cable on the same subnet. • **Wireless**: Select this option if you want to change the camera connection from wired to wireless. Also configure the WiFi settings on the WiFi tab. • **VIP** : Allow the camera to continue using DHCP to determine its IP address, but the camera will be on a remote network, and therefore the FortiRecorder will not connect to the camera's DHCP address. Instead, the FortiRecorder will connect through the static external, usually public network IP address and port numbers (called a virtual IP or VIP on FortiGate firewalls) specified in Address, (HTTPS) Port, and (RTSP) Port. The router or firewall will translate and forward connections to the camera's private network address. Likewise, communications in the other direction — from the camera to the FortiRecorder — are also affected: the camera will use the public IP setting as its destination (see "Configuring system timeout, ports, and public access"), not the private network address of port1, for example, which it would use if you select DHCP or Static. **Tip**: Use this option if the camera is not located on the same private network as the FortiRecorder due to NAT/ port forwarding, especially if the camera and FortiRecorder are separated by the Internet.
Address	If you want to deploy the camera to a different subnet, you can specify its new IP address or the VIP that it will be using.

Setting Name	Description
(HTTPS) Port	Type the port number of configuration communications from the FortiRecorder that the firewall or router will forward to the camera. If using only a WAN/virtual IP without port forwarding/translation, leave this setting at its default value, 443. This setting is available only when Address mode is set to VIP.
(RTSP) Port	Type the port number of video streaming commands (RTSP) from the FortiRecorder that the firewall or router will forward to the camera, such as when beginning a continuous recording schedule. If using only a WAN/virtual IP without port forwarding/translation, leave this setting at its default value, 554. This setting is available only when Address mode is set to VIP.
Transport Type	Normally RTSP is used for video streaming, which is UDP. If you want to use TCP, you can use HTTP tunnelling. If you want the communication to be secure/encrypted, you can use HTTPS tunnelling. The tunnel is between the camera and the FortiRecorder.
Profile	Select the camera profile that indicates the recording schedule, video quality, and other settings that will be used by this camera. Select *New* to create a new camera profile.

If a camera is disabled while you change its settings, or while it would normally be scheduled to begin continuous or motion detection recording, the FortiRecorder will not connect to the camera.

This can break communications between them: if you reconfigure the IP while the camera is disabled, your FortiRecorder may later attempt to communicate with the camera at the new address/gateway, but the camera will still be using the old address/gateway. It can also cause cameras to become out-of-sync, because they will not receive time setting changes while disabled. To fix this, disable the camera definition, revert the settings, enable the camera definition again, then apply your changes while the camera definition is enabled.

4. Click the *Preview* button to retrieve a single still image from the camera. Then click Use As Icon to use the captured image as the icon for the camera in the camera list. When you select the camera from the list, the icon will pop up.
5. If the camera is an ONVIF third party camera, the Management tab will appear, allowing you to decide if you want FortiRecorder to manage the camera's video/audio and stream settings, or leave the settings to be configured via the camera's management GUI without going through FortiRecorder.
6. If the address mode is wired or wireless, under the Network tab, configure the following:

Setting Name	Description
Wired settings	Select DHCP if you want the camera to continue using DHCP to dynamically determine its IP address. The FortiRecorder will attempt to keep track of any DHCP-related IP address changes automatically using periodic DNS probes. This requires that the camera remain on the same subnet as the FortiRecorder.

Setting Name	Description
	Select Static to re-configure the camera with a static **private** network IP address that you specify in Address. It will no longer use DHCP. This option requires that the camera and FortiRecorder not be separated by NAT. **Caution**: It is strongly recommended to either: • configure your cameras with a static IP, or • configure your DHCP server with lease reservations (see “Configuring the DHCP server”). Without reservations, the IP address provided by the DHCP server may appear to work initially, but later, in some cases, the DHCP server could change the IP address lease. If this happens, the DHCP server will not update the list of known cameras with the camera’s new dynamic IP. Until the appliance discovers that the IP address has changed, FortiRecorder will still be trying to control the camera’s old address, which no longer works. **Connections with that camera will be broken and all video from that camera will be lost during that interruption.**
Wireless settings	This area displays the wireless DHCP settings for the camera. You can change the camera to use a static IP address. For more information about wireless connection, see the following WiFi section.

7. If the camera has wireless function and you want it to connect to FortiRecorder through a wireless router, you can specify the WiFi settings on the WiFi tab. After you configure the WiFi settings, you can disconnect the discovered camera and connect it to the router.

Setting Name	Description
Enable	Select to Enable the WiFi function of the camera.
SSID	Specify the wireless router’s SSID that the camera will connect to.
Security	Specify the security settings.

8. If the camera supports infra red recording or LED lighting, configure the settings on the Light or Infrared tab.

Setting Name	Description
Mode	Either off or auto. Auto means to turn on infra red mode at the threshold. In infrared mode the camera shows a black and white image and removes a filter used at daylight for more sensitivity.
LED	Either off or auto. Infrared LEDs allow the camera to see at night and can automatically activate when it is dark. Set it to “off” if the camera is behind a glass or if enough ambient lighting is available for clear viewing.
Enable threshold	Enter the light level when infrared mode should turn on.
Disable threshold	Enter the light level when infrared mode should turn off.
Threshold time	Enter the time interval (in seconds) when the camera should wait to turn on or off the infra red mode after the threshold is reached.

Setting Name	Description
Current light level	Display the current light level that the camera detects.
Threshold time	Enter the time interval (in seconds) the camera should wait to activate infrared mode.
Refresh	Click to get instant light level reading.

9. Configure the video settings in the Video tab. Available setting vary on different camera models. If the setting is grayed-out, the setting is not supported for the selected model.

Setting Name	Description
Video Orientation	Select the relative position of the camera. • **Normal**: Regular viewing angle and position • **Vertical Flip:** Enable if the camera is positioned on a ceiling and the preview image appears upside down. • **Horizontal Flip**: Enable if the camera is positioned viewing a mirror or on a ceiling and the preview image appears reversed left to right. • **Rotate 90/180/270**: Enable to view a corridor mode when the image is in the portrait format, typically for viewing hallways.
Video display	Select the display of the video. For fisheye cameras, choose if the camera should de-warp the image into a 360 or 180 panorama or send the raw round fisheye image for client-side de-warping.
Video mount	Select the location of the camera.
Video Aspect	Select the desired resolution (SD or HD).
Video Overlay mode	Enable the display of Name, Time, or Timezone on the video image.
Image Brightness	Adjust the tonal range of an image. Lowering the value expands the shadows while increasing the value expands image highlights.
Image Contrast	Adjust the contrast to increase the separation between dark and bright, making shadows darker and highlights brighter.
Image Saturation	Adjust to increase the separation between colors. The lower the saturation, the more the image resembles a grayscale image.
Image Sharpness	Adjust to increase or decrease the edge contrast of the image. Too much sharpness creates halo borders around the contours of the image.
Image DIS	Enable or disable digital image stabilization. For cameras that are mounted on an unstable footing, image stabilization reduces image shaking from various external sources, such as wind.
Image DNR	Select either Manual or Auto for digital noise reduction. Enabling this feature smooths the image and suppresses small noise. This is helpful for dark scenes when image noise occurs.
Smart DNR	Select **On** or **Off** from the drop-down menu. Enabling DNR saves bandwidth by focusing on the moving parts of a camera's feed. Smart DNR is only available on the FD50 and FB50 cameras.

Setting Name	Description
Exposure Environment	Optimize the exposure for the selected environment (Indoor/Outdoor).
Exposure WDR - Digital/Shutter	If the camera supports WDR (wide dynamic range), enable it if there is intense backlight in the camera view. WDR balances images that have high contrasting lights and darks, like an individual standing in front of a window during the day. Shutter types takes two images with different exposure and merges them into one image.
Exposure Max gain	Exposure is the amount of light which reaches your camera sensor. Exposure determines how light or dark your image appears. Too much gain results in an image filled with noise.
Exposure Min shutter speed	The shutter speed determines how quickly or slowly the shutter opens and closes. Set the shutter speed too low and things appear blurry.

10. Configure the audio settings in the Audio tab.

Setting Name	Description
Input/Output level	Adjust to change the strength of both the input and output audio signal.
Codec	Select the supported audio codec.
Bitrate	Enter the number of bits to process per second.
Sample rate	Enter the number of times per second the sound is sampled in hertz.

11. If the camera supports pan/tilt/zoom function, this tab will appear, allowing you to adjust the settings:

Setting Name	Description
Auto focus (full/semi)	Auto-focus improves the picture quality of the camera with minimal input from the user.
Manual focus	Adjust the focus of the camera manually and determine how fast the focus should change when using the + and - buttons.
Zoom	Set the absolute zoom value.
Digital zoom	When the optical zoom value is reached, enabling digital zoom allows the camera to view the subject closer by digitally zooming further.

12. In some cases, you may want to mask an area and do not want to show a certain portion of the image. For example, for privacy reason, you may want to mask the area where an employee sits. To do this, on the Privacy Mask tab, click the plus sign beside Mask Window and tweak the window size. To add another mask window, click the plus sign again.

13. All FortiCam cameras are capable of detecting motion. Some camera models also supports audio surveillance and digital input and output (DIDO).
Motion and other detections can be used to generate motion clips. Some cameras generate these clips internally and send them to FortiRecorder. In this case, the length and time frame depends on camera implementations. The advantage to motion detection is that the camera only records when motion is detected. Other cameras stream continuously to the recorder and only notify the recorder of a motion event. Then the recorder either copies a clip out of the camera stream and stores it or simply marks the section of the continuous recording with motion.

For audio detection and DIDO, configure the following settings

Setting Name	Description
Audio Sensitivity	If the camera supports audio surveillance, specify the sensitivity level that the camera recording will be triggered. You may need to tweak the sensitivity level, for example, when there are some background noises.
PIR Sensitivity	Adjust the sensitivity of the electronic sensor that measures the infrared light to detect motion.
Digital input/output	Some cameras come with DIDO terminals and support digital input and output. For example, on the FortiCam MB13 camera, according to your configuration, power signal from the digital input can trigger the camera to record a video clip. You can also optionally connect other devices to the digital output, such as a relay to turn on/off another device. 4: Power output +5V 3: Digital output 2: Digital input 1: Ground The digital input (DI) can be configured to trigger when the signal is: • LOW (ground) • HIGH (+5V) • Rising (transitioning from LOW to HIGH) • or Falling (transitioning from HIGH to LOW) If not connected, the camera will see the digital input as HIGH. The digital output (DO) can be configured to either be grounded or open when in the triggered state. When not triggered it will be in the opposite state. For example, if opening a door causes a sensor switch to open, then the switch could be wired between DI and ground. DI will be grounded (LOW) while the door is closed and will go HIGH when the door opens. DI could then be configured to trigger on the rising edge. When the door opens, DO would be set to its triggered state and a video clip will also be recorded. Triggering on the rising or falling edge can be useful if the DI might be held in the triggered state for a long period. In the example above, if DI were set to trigger on HIGH and the door is left open for a long period then the camera would trigger repeatedly.

14. On the Miscellaneous tab, configure the following settings:

Setting Name	Description
Privacy button	FortiCam MB13 has a privacy button on it. If enabled, you can press the privacy button on the camera to stop and resume video and audio monitoring. To enable the functionality of the privacy button on the camera, select the Privacy button checkbox. To disable the functionality of the privacy button on the camera, clear the Privacy button checkbox.

Setting Name	Description
Status LEDs	Most cameras come with LED indicators (for details, see the LED description section in the camera's QuickStart Guides). You can enable or disable the LEDs by selecting or deselecting the Status LEDS checkbox.
Move home	For the PTZ cameras, you can specify when the camera should stop PTZ and move back the home position.

15. If the camera supports internal SD card storage, this tab will appear, allowing you to enable/disable SD card storage

Setting Name	Description
Enable storage	Enable or disable the camera recording to an onboard SD card. If full, the oldest recordings are overwritten.
Network failure	Enable or disable the camera's ability to detect network failure by pinging the recorder and then begin recording to the SD card.
Format	Format the SD card on the camera.

16. Select *OK*.

If you kept the Enabled check box marked, at this time, FortiRecorder connects to the camera's discovered IP address. FortiRecorder configures the camera with the camera's new .Address and other network settings (if Address mode is set to Static) and NTP settings. Afterward, in order to control the camera according to your selected schedules, FortiRecorder will periodically connect to the camera's configured IP address. It will also keep video recordings sent by that camera from its new IP address.

17. To confirm that FortiRecorder can receive video from the camera at its new IP address, go to *Monitor* > *Video* > *Video*.
If no video is available from that camera, verify that:

- Other video software such as Windows Media Player or VLC has not stolen the RTSP file type association from QuickTime (Installing other video software after QuickTime is a common cause of changes to media file type associations.)
- A route exists to the camera's new IP address and, if applicable, its virtual IP/port forward. To confirm, go to *Dashboard* > *Console* and enter the command:
  `execute ping <camera_ipv4>`
  where `<camera_ipv4>` is the camera's IP address or virtual IP/port forward. If you receive messages such as Timeout..., to locate the point of failure on the network, enter the command:
  `execute traceroute <camera_ipv4>`
- Firewalls and routers, if any, allow both RTSP and RTCP components of the RTP streaming video protocol between FortiRecorder and the camera and between your computer and FortiRecorder.
- Web proxies or firewalls, if any, support streaming video

  If you did not discover the camera but instead manually configured FortiRecorder with the camera's IP address, confirm that the camera is actually located at that address

18. If desired, you can specify different camera settings, such as brightness and contrast, for the camera to use as different times.

Once your cameras have been created, the camera list populates and provides a summary of each individual camera's settings. The settings displayed on the camera list are fully customizable. Select **Show and Hide Columns** from the Configure View drop-down menu. Enable or disable the displayed settings on the camera list and select **OK**. When finished, select **Save View** from the Configure View drop-down menu.

Creating camera groups

After you have configured the cameras, you can group them to facilitate the camera management. When you edit Access Controls you can specify which groups of cameras users can access.

To configure camera groups

1. Go to *Camera* > *Configuration* > *Camera Group*.
2. Select *New*.
3. Enter the name for the group.
4. Select the cameras you wish to add to the group and then select the double right arrow.
5. Select *Create*.

Upgrading or downgrading camera firmware

Once the FortiRecorder is connected to your cameras, you can upgrade/downgrade the camera firmware through the FortiRecorder web UI.

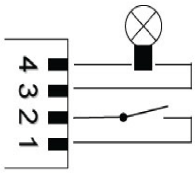
Fortinet does not recommend downgrading firmware. Downgrading firmware could result in a loss of configuration information.

To upgrade/downgrade your cameras' firmware

1. Go to *Camera* > *Configuration* > *Firmware* to check the availability of the camera firmware. For the corresponding camera model, if the Availability column says Fortinet Support, that means the firmware is available to download from the Fortinet Technical Support web site.
2. Download the firmware file from the Fortinet Technical Support web site and save the file on your PC: https://support.fortinet.com/
3. Go to *Camera* > *Configuration* > *Firmware*.
4. Select the Upload button to upload the downloaded firmware images. After the firmware is successfully uploaded, the Availability column will show *Local*.
5. Go to *Camera* > *Configuration* > *Camera*.
6. Select the camera that you want to upgrade/downgrade and select the *Upgrade* button. You can select multiple cameras and upgrade/downgrade them at the same time.
7. From the available firmware list, select the firmware version you want to upgrade to and select *OK*. The camera installs the new firmware. During this time, the camera will not be able to record video if it was scheduled; you may notice a gap in the recorded video clips.

Using DIDO terminal connectors on FortiCam MB13 cameras

FortiCam MB13 (FCM-MB13) cameras come with Digital input and output (DIDO) terminal connectors. According to your configuration, a digital input can trigger the camera to record a video clip. You can also optionally connect other devices to the digital output, such as a relay to turn on/off another device.



4: Power output +5V
3: Digital output (DO)
2: Digital input (DI)
1: Ground

To configure DIDO on MB13 cameras

1. Go to *Camera* > *Configuration* > *Camera*, select the MB13 camera from the camera list and select *Edit*.
2. Expand the Detection section.
3. Configure the digital input and output settings. Note that this setting is only available on FortiCam MB13 cameras. More cameras will support this feature in the future.
   The digital input can be configured to trigger when the signal is:
   - LOW (ground)
   - HIGH (+5V)
   - Rising (transitioning from LOW to HIGH)
   - or Falling (transitioning from HIGH to LOW)

   If not connected, the camera will see the digital input as HIGH.

   The digital output can be configured to be either grounded or open when in the triggered state. When not triggered, it will be in the opposite state.

   For example, if opening a door causes a sensor switch to open, then the switch could be wired between DI and ground. DI will be grounded (LOW) while the door is closed and will go HIGH when the door opens. DI could then be configured to trigger on the rising edge. When the door opens, DO would be set to its triggered state and a video clip will also be recorded.

   Triggering on the rising or falling edge can be useful if the DI might be held in the triggered state for a long period. In the example above, if DI were set to trigger on HIGH and the door is left open for a long period then the camera would trigger repeatedly.
4. Go to *Camera* > *Configuration* > *Camera Profile* and enable Digital input when creating a camera profile that uses a recording schedule.

Configuring Cameras to send Notifications

After you have set up the SMTP server and SMS service provider, you can configure the detailed notification settings, such as when and how the notifications should be sent. Camera notifications work with face and object detection. You can configure your FortiRecorder to notify the user when a particular person or object is detected and can also select who receives the notification.

Note: face and object detection notifications requires FortiCentral.

To configure camera notifications

1. Go to *Camera* > *Notification* > *Camera Notification*.
2. Select *New*.

3. Configure the following settings:

Setting Name	Description
Name	Enter a name for the notification entry.
Description	Optionally enter a descriptive comment.
Enable	Select to enable this notification entry.
Hold off period	Determines how long to wait till sending a notification. Events that occur before the hold off period ends are delayed.
When to notify	First event: Only the first in a series of events triggers a notification. A break is required before an event is considered to be a new event. The time of this required break is determined by the pre and post-alarm settings of the camera. Evert event: A notification is sent for every occurrence of a frequent event. For example, if a bicycle is left in sight of the camera configured to detect bicycles, the camera will continually detect the bike.
Triggers	Enable the detections trigger a notification. Selecting face detection or object detection reveals new selections for further clarification.
Notification Schedules	Enable notifications during specific periods of time during the day or week by selecting *Add schedule*. Enable if the notification should be sent to users or via SNMP to other systems like SIEMs.
Select Cameras	Specify which camera's generate notifications.
Select User	Specify which user should be notified.

4. Select *Create*.
5. To verify email connectivity, from FortiRecorder, trigger an alert event that matches the type and severity levels that you have chosen. Then, check your email.

   If you do not receive an alert email within a few minutes, verify that you have configured an email address for the account. Next, verify the FortiRecorder's static routes (see "Configuring the network settings") and the policies on any firewalls or routers between the appliance and the SMTP relay. (They must allow SMTP traffic from the FortiRecorder network interface that is connected to the gateway between it and the email server.) To determine the point of connectivity failure along the network path, if the SMTP server is configured to respond to ICMP ECHO_REQUEST (ping), go to Dashboard > Console and enter the CLI command:

   ```
   execute traceroute <syslog_ipv4>
   ```

   where `<syslog_ipv4>` is the IPv4 address of your email server.

   If that connectivity succeeds, verify that your alert email has not been classified as spam by checking your junk mail folder.

   A camera notification can be deleted at any time by selecting the notification name and then the **Delete** button.

To prevent classification as spam, it usually helps to add the FortiRecorder's email address to your address book.

Configuring Video Services

The service section contains a variety of tools to adjust how you view your content.

This section contains the following topics:

- Configuring video
- Using monitor display
- Associating cameras with a virtual assistant
- Using Chromecast to stream content

Configuring Video

This section contains options to enable video and image sharing in FortiRecorder.

Establishing video sharing

FortiRecorder supports video sharing on the web sites. Using FortiRecorder, administrators can configure FortiRecorder and a third-party web site to allow users to access a live feed of an established camera without directly accessing FortiRecorder.

To allow users to access video sharing, you must first insert the video in your web page.

For example, if your FortiRecorder runs v2.3 and older firmware, you can insert the following code in your web page:

```
<iframe frameborder="10" scrolling="no" width="640" height="480"
     src="https://172.20.110.94/api?request=FRC_LiveView&id=FD20&width=
     640&height=480&view_
     mode=3&hostName=172.20.110.94&username=videoService&password=1234">
```

iframes are not supported by your browser. `</iframe><br/>`

Starting from v2.4, if your web browser supports HTML5, you can use the following code:

```
<iframe frameborder="10" scrolling="no" width="640" height="480"
     src="https://172.20.110.94/api?request=FRC_LiveView&id=FD20&width=
     640&height=480&view_
     mode=3&hostName=172.20.110.94&username=videoService&password=1234">
```

iframes are not supported by your browser. </iframe>

```
<script>
setInterval(function() {
     var req = new XMLHttpRequest();
     req.open('GET',
        "https://172.20.110.94/api?request=FRC_LiveView&id=20A-
             b5fc&username=videoService&password=1234&heartbeat=1", true);
     req.send();
}, 10000);
</script>
```

The IP address at the beginning of the code is the IP of the FortiRecorder. The attribute ID is the name of the camera as defined on the FRC. The attribute dimensions should match the size of the iframe. The username and password values should match the configuration you specify below.

Once you have entered the code into your web page, configure the FortiRecorder unit to allow your web page to access the camera group via HTTPS.

If you want to share the video stream via RTSP, the user can use a RTSP client to access the video at:

rtsp://<username>:<password>@<fortirecorder_ip>/camera=<id>

For example:

rtsp://videoService:1234@172.20.110.94/camera=FD20

To configure video sharing on FortiRecorder

1. Go to *Service* > *Video* > *Stream*.
2. Enable Status.
3. Enter your username and password.
4. Add the camera group you wish the user to view by selecting the group from the Camera Group List and then selecting the right arrow button.
5. Select the HTTPS or RTSP protocol.
6. Select *OK*.

Retrieving video clips

You can enable FortiRecorder to allow an external service to make REST API queries to retrieve video clips from selected cameras. If you require more information concerning REST API, consult the REST API Reference document.

To configure video clips

1. Go to *Service* > *Video* > *Clip*.
2. Enable the status button.
3. Enter a password.
4. Select which cameras video clips can be retrieved from by selecting the camera group's name and then the right arrow.
5. Select *Apply*.

Establishing image sharing

You can configure your FortiRecorder unit to upload images from a camera group. Using the image service your cameras will capture a snapshot image at specified intervals. and upload the image to a FTP site.

Similar to the shared video, you will need to upload the image to your web site. Once you have finished that, configure image sharing in FortiRecorder.

To configure image sharing on FortiRecorder

1. Go to *Service* > *Video* > *Image*.
2. Enable Status to enable FTP uploads.
3. Enter the number of seconds in the Interval section that will dictate how often the cameras capture a picture.
4. Enter the necessary FTP information.
5. Add as many cameras you require by selecting New in the Select Camera section.
6. Enable or disable image processing. Enabling image processing uses processed images from FortiCentral connected to FortiRecorder. The FortiRecorder retrieves these settings the connected recorder and sends privacy processed snapshots at the chosen interval; however this requires that the cameras are run in a pane with the privacy analytics active.
7. Select *Apply*.

Streaming recorded video clips to YouTube

To stream live video to YouTube, you must create a YouTube account. You can only stream one camera per YouTube account.

To stream live video to YouTube

1. Go to *Service* > *Video* > *YouTube*.
2. Select *New* to create a YouTube integration task.
3. Enter a name for this task.
4. Enter a description for this task.
5. Select a camera you want to stream.
6. For Encoder Setup, enter the server URL and stream name/key. This is the information you get when you set up the YouTube account.
7. Select *Create*.

Using Monitor Display

On FortiRecorder 100D and 400D models, there is a video port on the unit you can connect a monitor to the video port. You can specify which camera's video will be displayed on the monitor.

To use the monitor display

1. Go to *Service* > *Monitor Display* > *Monitor Display*.
2. Enable the status
3. Specify how to use the camera label on the monitor from the drop-down menu.
4. Select *New* to add a camera.
5. Select the camera from the drop-down menu and then specify which video stream to display, either viewing or recording.
6. Click *OK*.

Associating Cameras with a Virtual Assistant

FortiRecorder supports integration with virtual assistant software, such as Amazon Alexa.

Associating a Camera with Amazon Alexa

Starting from the 2.6 release, FortiRecorder has been integrated with the Amazon home assistant. It supports commands like:

- “Alexa, ask FortiRecorder who is at the front door.”
- “Alexa, enable FortiRecorder mode Away.”

To integrate Alexa with FortiRecorder, you will need to add the FortiRecorder skill through Amazon’s user portal.

To associate a camera with Amazon Alexa

1. Go to *Service* > *Assistant* > *Assistant*.
2. Enable the status.
3. Select *New*.
4. Select a camera from the drop-down list.
5. Specify the camera location.
6. Select *Apply*.

Using Chromecast to Stream Content

FortiRecorder uses Chromecast to remotely monitor camera streams on a mobile device or a personal computer.

Selecting *Discover* makes the FortiRecorder unit search for a Chromecast enabled device on the network.

To configure Chromecast in FortiRecorder manually

1. Go to *Service* > *Chromecast* > *Device*.
2. Select *New*.
3. Enable Status.
4. Enter the name, location, and address of the Chromecast device.
5. Select the desired way to present the information on the Chromecast device from the Layout drop-down menu.
6. Select the cameras you wish to stream.
7. Select *Create*.

In addition to streaming video content, FortiRecorder also streams photos to the Chromecast device.

To stream photos to the Chromecast device

1. Go to *Service* > *Chromecast* > *Image*.
2. Select *Add*.
3. Select the file from File Explorer and then select *Open*.

Configuring Face Recognition

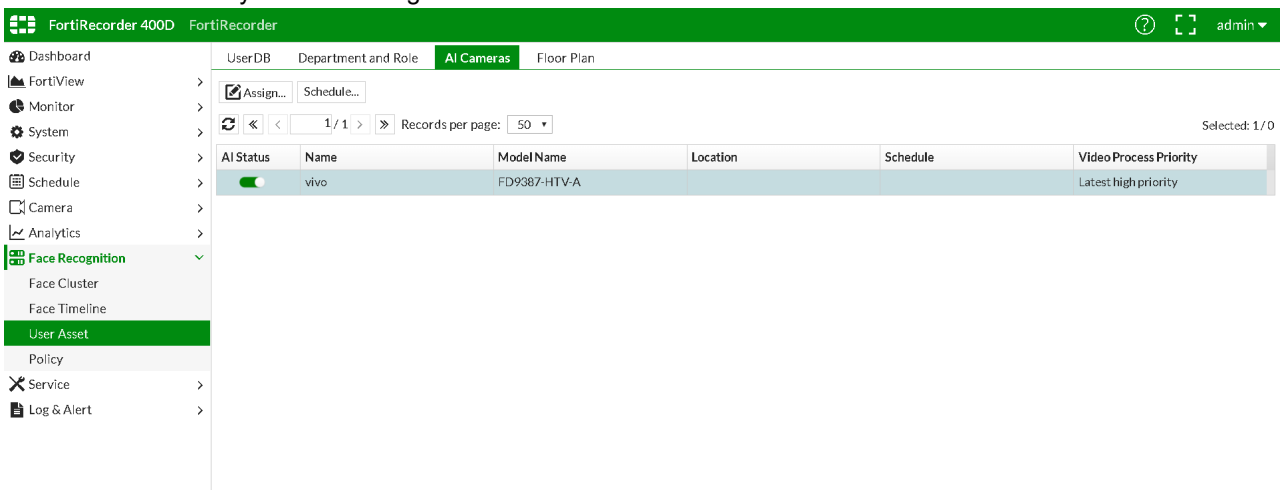
The face recognition feature uses artificial intelligence to identify unique faces and enact policies based on configured information. For example, administrators can identify faces and designate those faces as "known" and establish various information in the user database on those individuals, such as their occupation or their department. The information can be used to determine what time of day they appear on a camera or the frequency of their appearances, allowing the administrator to create policies to send out notifications based on that data.

Face recognition requires internet access and is supported on 200D, 400D, 400F and VM. For VM users, a minimum of 4GB of memory is required, while 8GB or more is recommended.

Under *Dashboard* > *License* Information, ensure that you have a valid Face Recognition license. If the license is expired or invalid, only the last 7 days of Face Recognition data (Face Cluster, Face Timeline, Events, and Activity) displays.

To enable face recognition in the GUI

1. Go to *Camera* > *Configuration* > *Camera Profile*.
2. Select the desired camera profile to enable face recognition on and then select *Edit*.
3. Expand the Recording section and enable Motion detection in the Recording type section.
4. Enable FortiRecorder in the Store on section.
5. Select *OK*.
6. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
7. Enable AI for the desired camera by selecting the toggle switch in the AI status column. The face recognition function will now analyze video footage for the selected camera.



To enable face recognition in the CLI

Enter:

```
config system global
      set face-recognition enable
```

```
end
```

Monitoring Face Clusters

A face cluster is a collection of face screenshots of the same individual captured by AI cameras. Face clusters are split into two categories: Known Faces and New Faces.

Reviewing known faces

Known Face clusters contain screenshots of individuals recognized by the Face Recognition AI module or manually linked to an individual in the user database by an administrator.

To edit known face clusters

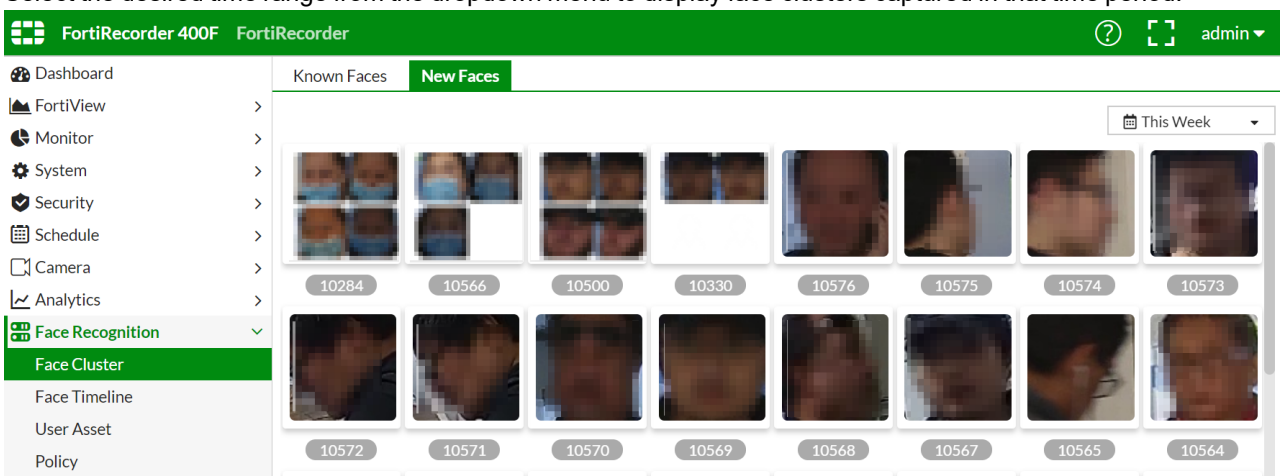
1. Go to *Face Recognition* > *Face Cluster* > *Known Faces*.
2. Select the desired user's face cluster to open their record. For more information on understanding the user's record, see the Searching the user database section.
3. Hover the cursor over their profile picture and select the *More* button. All the face clusters manually linked to the user are displayed.

Reviewing new faces

All unrecognized face screenshots are placed in New Face clusters. New Face clusters can be linked to a user in the database to make the cluster a Known Face cluster.

To link a new face cluster to a user

1. Go to *Face Recognition* > *Face Cluster* > *New Faces*.
2. Select the desired time range from the dropdown menu to display face clusters captured in that time period.



3. Select a specific face cluster to open all of the face screenshots that the AI has determined belong to the same individual.
4. Confirm that all screenshots contain the same individual. If a screenshot does not contain the same individual, hover over the screenshot and select the trashcan icon.

It is important that every face in the face cluster belongs to the same person for accurate results.

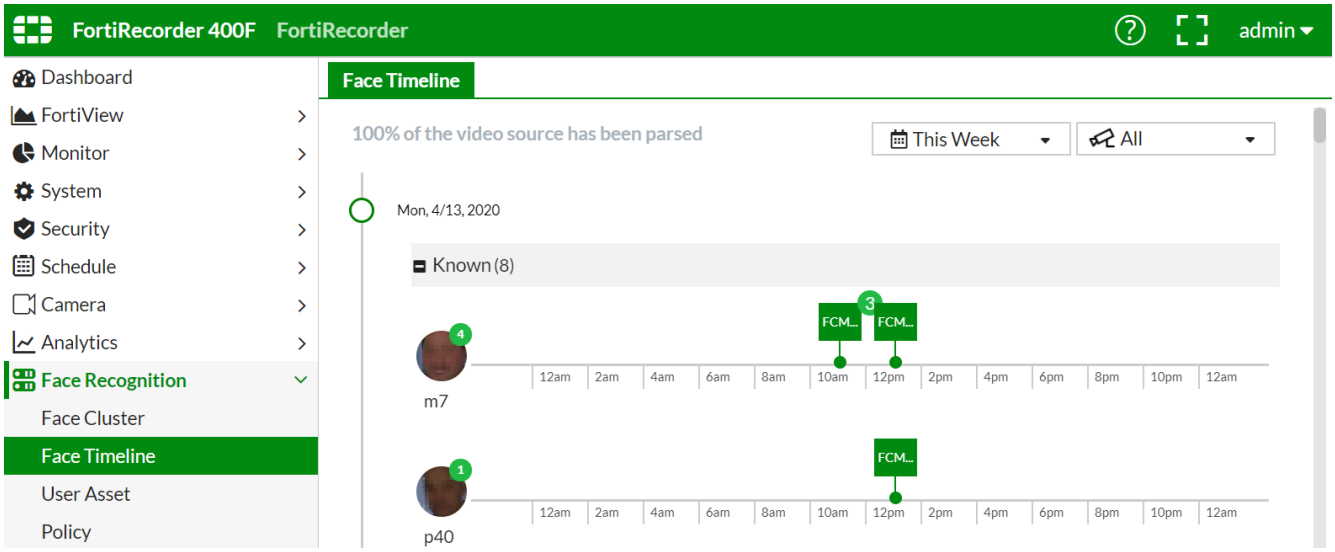
5. Select an existing user to whom the face cluster belongs or create a new user by selecting *New User*.
   - If you select an existing user, select the *Search User* dropdown menu. The top five users who match the cluster display.
   - If you create a new user, enter their name, role, and department and then select *Save*.

Go to *Face Recognition* > *User Assets* > *UserDB* to view a comprehensive list of users. You can add new information about the user by selecting *New* or edit known face clusters of individual users.

6. Select *Link all to user*. The individual's face cluster is now a Known Face. All future face screenshots are analyzed by the AI camera and categorized to their face cluster.

Using the Face Timeline

The Face Timeline provides an overview of daily activities of individuals captured by AI cameras.



Each day contains a list of Known and New face clusters and a timeline of their appearances on specific cameras during the 24 hour period.

Select an appearance to view more details and view video footage of the appearance.

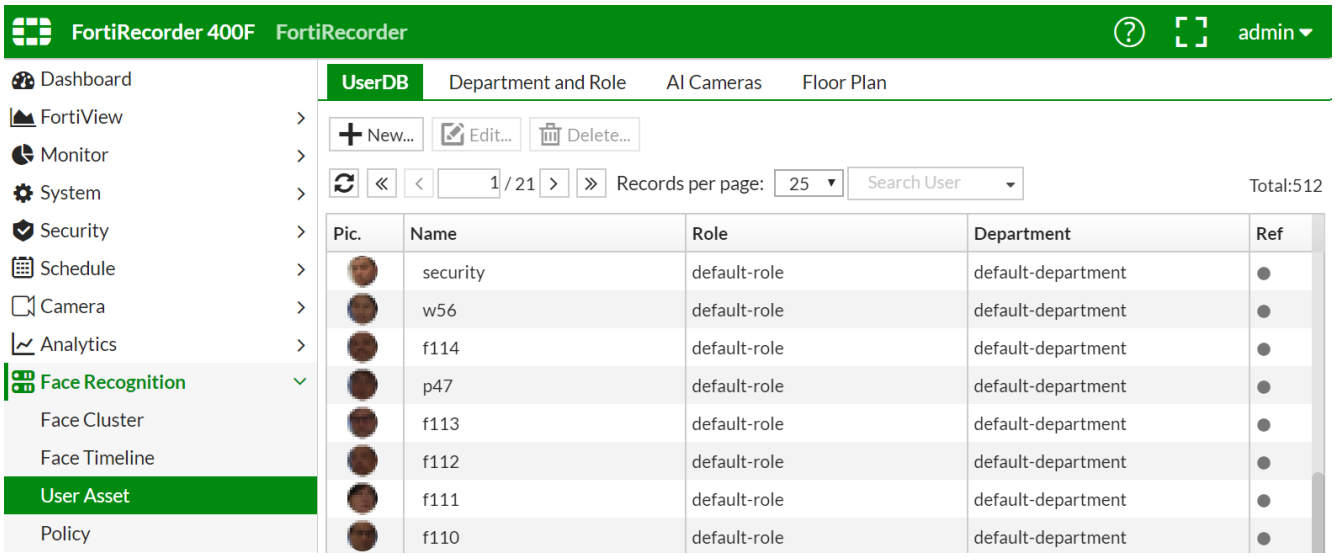
Filter the timeline display by selecting the range of time and the AI camera from the dropdown menus.

Configuring User Assets

The user asset section contains a variety of information about various individuals captured by the AI cameras.

Searching the user database

The user database stores the personal information of all known users and their activity captured by the AI cameras in an organized and searchable table.



To view the records of a specific user

1. Go to *Face Recognition* > *User Asset* > *UserDB*.
2. Select the desired user. A profile appears displaying the following information:
   - **Activity by date**: The user's activity on camera over multiple days within an hourly timeline.
   - **All activities**: The user's activity on camera within a daily timeline.

   Green circles represent when an individual's face was captured on camera. The darker the circle, the more frequent the appearances. Hover your mouse over the circle to view more details or select the circle to view the captured video footage.

Zoom in or out of the timeline by hovering your mouse over the timeline and scrolling up or down. Pan across the timeline by clicking and dragging left or right.

To add a user to the user database

1. Go to *Face Recognition* > *User Asset* > *UserDB*.
2. Select *New*.
3. Enter the user's name.
4. Select their role and department from the dropdown menus.

Creating a department and role

The department and role section allows you to assign a user's department and role their personal information.

To create a new role

1. Go to *Face Recognition* > *User Asset* > *Department and Role*.
2. Expand the Role Management section if not already expanded.
3. Select *New*.
4. Enter the name of the role and then enter a brief description of the role.
5. Select *Save*.

To create a new department

1. Go to *Face Recognition* > *User Asset* > *Department and Role*.
2. Expand the Department Management section if not already expanded.
3. Select *New*.
4. Enter the name of the department and then enter a brief description of the department.
5. Select *Save*.

You can also create a new department and role from the UserDB section by selecting the user's row and then selecting the *Edit* button.

Assigning AI cameras and setting schedules

The AI cameras section allows you to assign an AI camera to a specific location in a floor plan to track where the camera is located and in which location the face was captured on camera.

To assign an AI location to a camera

1. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
2. Select the camera row and then select *Assign*.
3. Follow the prompt on the screen to select the site, building, and floor for the location of the camera.
4. Select the name of the desired area or select the area from the floor plan.
5. Select the location of the camera within the selected area.
6. Select Done. The assigned area for the camera is listed under the Location column of the AI Cameras table.

You can set an existing FortiRecorder schedule to an AI camera so that the face recognition AI module prioritizes processing the footage within the designated schedule timeline first.

To set a schedule for an AI camera

1. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
2. Select the desired camera to highlight the row blue.
3. Select *Schedule*.
4. Select the desired Video Processing Priority to instruct the camera in which order to process footage.
   - **Latest high priority**: The most recent footage is processed first.
   - **Earliest high priority**: The earliest footage is processed first.

5. Select the schedule from the dropdown menu that governs the face recognition AI module. The AI module will not function outside of the schedule.
6. Select *Save*.

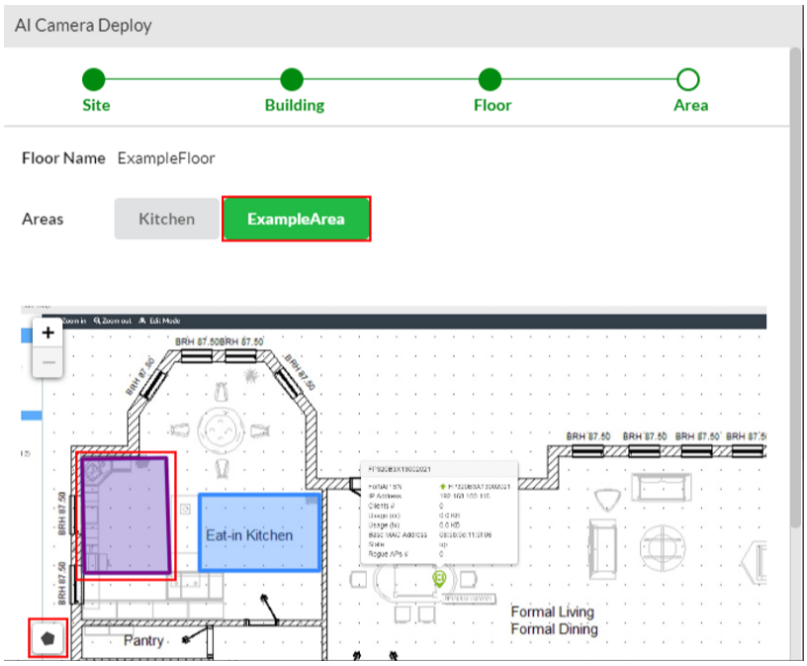
Creating a floor plan

The floor plan section tracks the location of the cameras to assist in pinpointing the precise location of individuals captured on camera in the building.

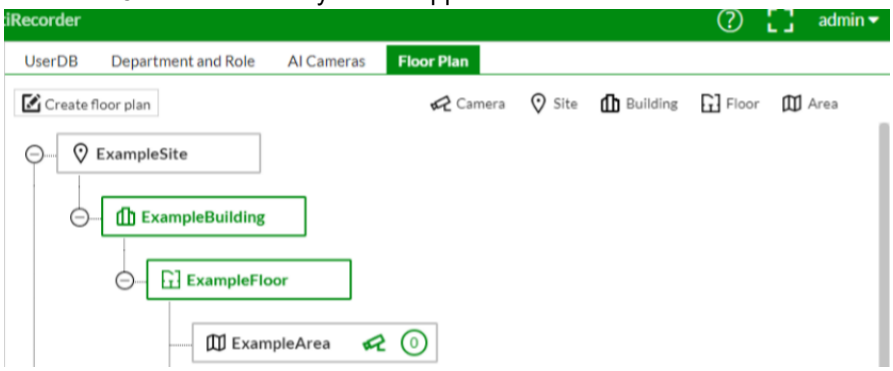
The current number of floor plans is limited to one site and one building. If there is an existing site or building, you will not see an option to create a new site or a new building.

To create a floor plan

1. Go to *Face Recognition* > *User Asset* > *Floor Plan*.
2. Select *Create floor plan*.
3. Select *Create new site* and enter a name for the site, or select an existing site. Select *Next*.
4. Select *Create a new building* and enter the name and address of the building. Mark the building's location on the provided map. Select *Next*.
5. Select *Create a new floor* and enter the name of the floor, or select an existing floor from the Choose a Floor dropdown menu. If you create a new floor upload an image of the floor plan. Select *Next* and then enter the dimensions. Select *Next*.
6. Select the polygon icon to draw on an area in the floor plan. Once the area is drawn, enter a name for the area and select *Save*.



7. Select *Finish*. A flowchart of your site appears.



Creating a Policy

The policy section allows you to log and be alerted to specific instances that fit your customized policy criteria. For example, you could set a policy that sends you an SMS text message whenever an unknown person's face is captured on camera in a high security location.

To create a policy

1. Go to *Face Recognition* > *Policy* > *Policy*.
2. Select *New*.
3. Enter a Rule Name.
4. Select the Event Type from the dropdown menu.
   - **Normal**: A normal event is any expected common occurrence. For example, an employee enters the building at the usual time to start his shift. Although the event is normal, you may still wish to be notified of the event's occurrence.
   - **Abnormal**: An abnormal event is any unexpected occurrence. For example, an employee enters an area of the building that he does not have access to and never enters.
5. Select the location you want to monitor from the Site, Building, Floor, or Area menu options.
6. Select who triggers the policy when the face is captured on cameras in your selected location from the person menu options.
7. Select the Action to take from the dropdown menu when the policy is triggered.
8. Select *Save*.

Reviewing Analytics

FortiRecorder analytics allows you to find specific instances of motion on your cameras, along with instances during the recording FortiRecorder recognized specific people or objects.

This section contains the following topics:

- Using motion detection analytics
- Using computer vision analytics

Using Motion Detection Analytics

You can search through recordings for changes (motion detections) in a defined area of the video during certain periods of time. This allows you to find specific events after the initial live viewing. Once completed, you can view the search results in a graph format.

To run analytics tasks

1. Go to *Analytics* > *Motion* > *Task*.
2. Select *New*.
3. Select a camera from the drop-down menu.
4. Select the type of motion you are attempting to detect from the Type drop-down menu. Motion detection analyzes the video for changes in position of an object relative to its surroundings, while motion heatmap reviews the recordings of a camera and overlays motion areas into a heatmap, which can help determine highly trafficked areas.
5. Specify the time frame.
6. Select *Create*.

It may take awhile to run the task. After the task is completed, double-click the task to view the results. You can adjust the sensitivity and threshold of the search result.

Using Computer Vision Analytics

FortiRecorder uses computer vision to understand and analyze digital images to identify important persons via facial detection or important objects like a vehicle or a weapon. The computer vision section enables processing of face and object detection generated events

The processing is done in FortiCentral. For more information, see the Facial Recognition chapter in the FortiCentral User Guide.

For information concerning accessing logged events and managing user databases via REST API, see the REST API Reference document.

Object detection in FortiRecorder is treated as a camera related event, similar to motion detection.

To enable detection actions

1. Go to *Analytics* > *Computer Vision* > *Computer Vision*.
2. Enter the desired time in the Accept detection after field. This setting instructs the FortiRecorder to postpone deciding if a person is known or unknown for the entered period of time before taking action. More time allows the camera a chance to get a better view of the object or face to avoid misinterpretations.
3. Enable Face detection action. Face detection is organized into five categories:
   - **Prohibited:** Individuals who are prohibited from accessing the building.
   - **VIP:** Individuals who are very important and are not security threats.
   - **Expired:** The time is past the expiry date of the person recorded.
   - **Unknown:** Individuals who are detected but not matched to an individual in the database.
   - **Regular Person:** Individuals who are recognized as common visitors, such as guests, employees, or contractors.
4. Enable Object detection action. Object detection is organized into seven categories:
   - **Person:** An individual.
   - **Motion:** Something that has generated motion.
   - **Weapon:** A detected tool that can cause harm.
   - **Vehicle:** A transportation machine, such as a bike, a car, or a train.
   - **Animal:** A non-human creature, such as a bird or a dog.
   - **Item:** An object, such as a backpack or a suitcase.
   - **Sport:** Athletic equipment, such as skis or a skateboard. Note:

     Each category can be further filtered by only enabling parts of the group in the analytics processor.
5. Select from the drop-down menu the action you wish the FortiRecorder to take upon detection for each category:
   - **No action:** Ignore events of this type.
   - **Event:** Accept events of this type, process them for notification, and display them on timlines and logs.
   - **Event clip:** Accept events of this type, process them for notification, display them on timelines and logs, and generate a video clip at the moment of detection.
6. Select *Apply*.

Analyzing Logs and Alerts

The Log and Alert section is used to analyze important events that have been recorded on the FortiRecorder system.

This section contains the following topics:

- Configuring log settings
- Configuring alert email

Configuring Log Settings

Log messages record a variety of important events, such as motion detection, failed log-in attempts, and system failures.

For more information on Logging, such as understanding log threat levels and how to use the logs, see the Analyzing Logging section. To view log messages, go to *Monitor* > *Log* > *Event*.

To diagnose problems or to track actions that the FortiRecorder appliance does as it receives and processes video, configure the FortiRecorder appliance to record log messages.

To configure logging

1. Go to *Logs & Alert* > *Log Settings* > *Local.* Alternatively, if you want logs to be stored remotely, go to *Logs & Alert* > *Log Settings* > *Remote*.
2. Configure the following settings if configuring local log storage:

Setting Name	Description
Log file size	Type the file size limit of the current log file in megabytes (MB). The log file size limit must be between 1 MB and 1000 MB. **Note**: Large log files may decrease display and search performance.
Log time	Type the time (in days) of the file age limit. If the log is older than this limit, even if has not exceeded the maximum file size, a new current log file will be started. Valid range is between 1 and 366 days.
At hour	Select the hour of the day (24-hour format) when the file rotation should start. When a log file reaches either the age or size limit, the FortiRecorder appliance rotates the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23 o'clock of the 10th day.
Log level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see "Log severity levels".

Setting Name	Description
	Caution: Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.
Log options when disk is full	Select what the FortiRecorder will do when the local disk is full and a new log message is caused, either: • **Do not log** — Discard all new log messages. • **Overwrite** — Delete the oldest log file in order to free disk space, and store the new log message.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log. You can enable an entire category of event, such as Detection Events or you can enable individual detections within each category by expanding the category and then toggling the event you wish to log.

3. If configuring remote log storage, click New, then configure the following settings:

Setting Name	Description
IP	Type the IP address of a Syslog server or FortiAnalyzer.
Port	Type the UDP port number on which the Syslog server listens for log messages. The default is 514.
Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see “Log severity levels”. **Caution**: Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.
Facility	Select the facility identifier the FortiRecorder will use to identify itself to the Syslog server if it receives logs from multiple devices. To easily identify log messages from the FortiRecorder when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CSV format	Enable if your Syslog server requires comma-separated values (CSV). **Note**: Do not enable this option if the remote host is a FortiAnalyzer. FortiAnalyzer does not support CSV-formatted log messages.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log.

4. To verify logging connectivity, from FortiRecorder, trigger a log message that matches the type and severity levels that you have chosen to store on the remote Syslog server or FortiAnalyzer. Then, on the remote host, confirm that

it has received that log message.

If you will be sending logs to a FortiAnalyzer appliance, you must add the FortiRecorder to the FortiAnalyzer's device list, and allocate enough disk space. Otherwise, depending on its configuration for unknown devices, FortiAnalyzer may ignore the logs. When the allocated disk space is full, it may drop subsequent logs.

If the remote host does not receive the log messages, verify the FortiRecorder's static routes (see "FortiRecorder configuration") and the policies on any intermediary firewalls or routers (they must allow Syslog traffic from the FortiRecorder network interface that is connected to the gateway between it and the Syslog server). To determine the point of connectivity failure along the network path, if the FortiAnalyzer or Syslog server is configured to respond to ICMP ECHO_REQUEST (ping), go to Dashboard > Console and enter the command:

```
execute traceroute <syslog_ipv4>
```

where `<syslog_ipv4>` is the IPv4 address of your FortiAnalyzer or Syslog server.

Configuring Alert Email

FortiRecorder can send alert emails whenever an important system event occurs, such as the hard disk being full.

Before you configure alert email, you must configure the mail server settings so that FortiRecorder can send out email. For details see "Configuring mail settings".

You can configure up to 10 alert email addresses.

To configure alert email settings

1. Go to *Logs & Alert* > *Alert Email* > *Configuration*.
2. Select *New*.
3. Enter your email address, such as admin@example.com.

   This setting is the recipient only for appliance-related notifications, such as the hard disk being full. It does not configure the recipient of camera-related notifications, such as motion detection. For this kind of video-related notifications, see "Notifications".
4. Select *Create*.
5. Go t o *Logs & Alert* > *Alert Email* > *Category*. Mark the check boxes of all appliance events that you want to trigger an alert email to be sent, such as:

Setting Name	Description
System events	Enable to send an alert email message when an important system event occurs. These include system reboot/reload, firmware upgrade/downgrade, and log disk/mail disk formatting.
Disk is full	Enable to notify when the disk partition that stores log data is full.

Setting Name	Description
Camera device altered	Enable to notify when a defined camera configuration has been enabled or disabled, or if there are problems with the camera. (The FortiRecorder will not control or record video from a camera that is not enabled in its list of known, configured devices.
Camera communication error	Enable to notify when there has been a network error during communications between the FortiRecorder and camera.
Camera recording error	Enable to notify when an issue prevents a camera from recording.
Camera alert summary	Enable to periodically sends messages related to both ongoing and resolved issues, like an interrupted video stream or an inability to start a video.
Video disk events	Enable to notify when events occur for the local or remote disk, such as the disk being full.

6. Select *Apply*.

Best Practices

This chapter is a collection of fine-tuning and best practice tips that will help you configure your FortiRecorder appliance securely and reliably.

While many features are optional, some practices are strongly recommended because they reduce complication, risk, and potential issues.

This section includes only recommendations that apply to a combination of multiple features, to the entire appliance, or to your overall network environment. For feature-specific recommendations, see the tips in each feature's instructions.

This section contains the following topics:

- Hardening Security
- Improving Performance
- Updating and Backups
- System Maintenance

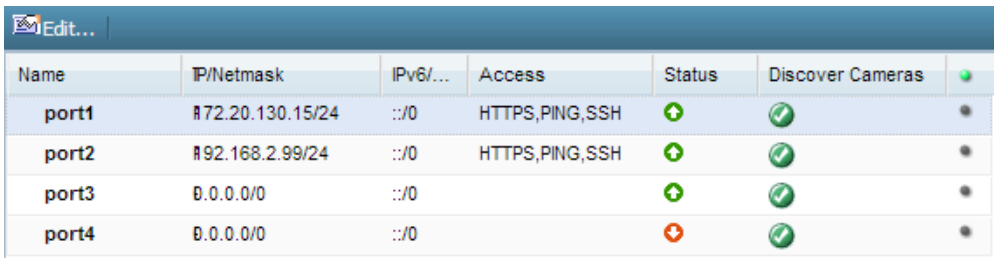
Hardening Security

FortiRecorder is designed to manage IP cameras and store video. While FortiRecorder does have some security features, its primary focus is surveillance. It always should be protected by a network firewall, and physically kept in a restricted access area.

Should you wish to protect the appliance from accidental or malicious misuse from people within your private network, this section lists tips to further enhance security.

Topology

- To protect your surveillance system from hackers and unauthorized network access, install the FortiRecorder appliance and cameras behind a network firewall such as a FortiGate. FortiRecorder is not a firewall. FortiRecorder appliances are designed specifically to manage cameras and store video.
- If remote cameras or people will be accessing the appliance via the Internet, through a virtual IP or port forward on your router or FortiGate, configure your router or firewall to restrict access, allowing only their IP addresses. Require firewall authentication for connections from network administrators and security guards.
- Make sure traffic cannot bypass the FortiRecorder appliance in a complex network environment, accessing the cameras directly.
- If remote access while traveling or at home is not necessary, do not configure “Configuring system timeout, ports, and public access”, and do not configure your Internet firewall to forward traffic to FortiRecorder. If you do require remote access, be sure to apply strict firewall policies to the connection, and harden all accounts and administrative access (see “Administrator access” and “Operator access”) as well as keeping the FortiRecorder software up-to-date (see “Patches”).
- Disable all network interfaces that should not receive any traffic.

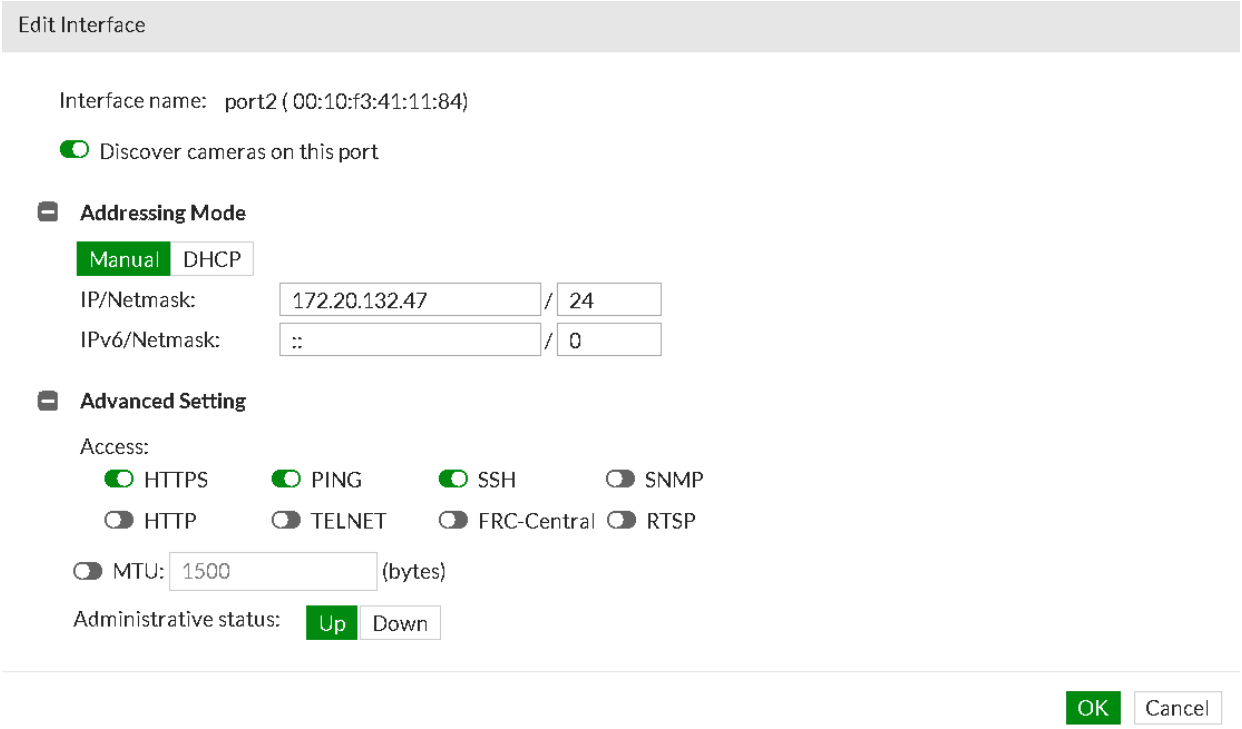


For example, if administrative access is typically through port1, the Internet is connected to port2, and cameras are connected to port3, you would disable (“bring down”) port4. This would prevent an attacker with physical access from connecting a cable to port4 and thereby gaining access if the configuration inadvertently allows it.

Administrator access

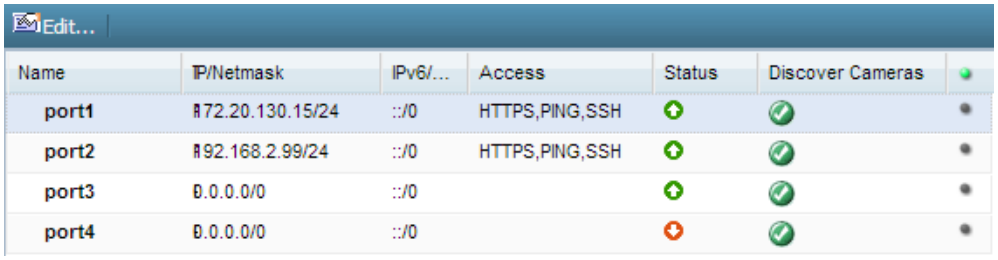
- As soon as possible during initial FortiRecorder setup, give the default administrator, admin, a password. This super-administrator account has the highest level of permissions possible, and access to it should be limited to as few people as possible.
- Administrator passwords should be at least 8 characters long and include both numbers and letters.
- Change all passwords regularly. Set a policy — such as every 60 days — and follow it.
- Instead of allowing administrative access to the FortiRecorder appliance from any source, restrict it to trusted internal hosts. On those computers that you have designated for management, apply strict patch and security policies. Always password-encrypt any FortiRecorder configuration backup that you download to those computers to mitigate the information that attackers can gain from any potential compromise. If your computer’s operating system does not support this, you can use third-party software to encrypt the file.
- Do not give administrator-level access to all people who use the system. Usually, only a network administrator should have access to the network settings. Others should have operator accounts. This prevents others from accidentally or maliciously breaking the appliance’s connections with cameras and computers. See “User management”.
- By default, an administrator login that is idle for more than five minutes times out. You can change this to a longer period in the idle timeout settings. But Fortinet does not recommend it. Left unattended, a web UI or CLI session could allow anyone with physical access to your computer to change FortiRecorder settings. Small idle timeouts mitigate this risk.

- Restrict administrative access to a single network interface (usually port1), and allow only the management access protocols needed.



Use only the most secure protocols. Disable PING, except during troubleshooting. Disable HTTP, SNMP, and TELNET unless the network interface only connects to a trusted, private administrative network. See “FortiRecorder configuration”.

- Disable all network interfaces that should not receive any traffic. (i.e. Set the Administrative status to Down.)



For example, if administrative access is typically through port1, the Internet is connected to port2, and cameras are connected to port3, you would disable (“bring down”) port4. This would prevent an attacker with physical access from connecting a cable to port4 and thereby gaining access if the configuration inadvertently allows it.

Operator access

- Authenticate users only over encrypted channels such as HTTPS. Authenticating over non-secure channels such as Telnet or HTTP exposes the password to any eavesdropper. For certificate-based server/FortiRecorder authentication, see “Replacing the default certificate for the web UI”.
- Immediately revoke certificates that have been compromised. If possible, automate the distribution of certificate revocation lists (see “Revoking certificates”).

Improving Performance

When configuring your FortiRecorder appliance and its features, there are many settings and practices that can yield better performance.

Video performance

Video performance is a combination of the video input (from the cameras) and the video output (to the browser for live views and playback).

Input performance factors

- Peak number of cameras streaming to the FortiRecorder simultaneously
- The camera recording type (motion detection only or continuous)
- The camera resolution, frame rate, and image quality

Output performance factors

- Number of administrator/operator sessions
- Number of live camera views per administrator/operator session
- Peak number of simultaneous administrator/operator live views

Resolution has the largest impact on the overall FortiRecorder performance.

- Low resolution — n MB/s
- Medium resolution — 2n MB/s
- High resolution — 6n MB/s

In other words, high resolution video will generate 3 times as much raw data as the default, medium resolution. Depending on how efficiently a specific raw stream can be compressed, higher resolutions can multiply the bandwidth and/or disk space required per camera, and per login session. For example, assuming a FortiCam 20A camera, the FortiRecorder can store on its local hard drive about 36 days' worth of high resolution video, but about 240 days' worth of low resolution video.

Degree of motion in the camera's field of view also affects video performance. Constant and/or extreme motion will result in larger files/streams, because the compression method cannot encode it as efficiently. To improve compression, exclude areas of irrelevant motion such as fans or blinking lights from the camera's field of view.

For sizing guidelines and estimates on the amount of video that you will be able to store, contact your reseller. Alternatively, expand your storage by configuring a network storage location (see "External storage").

System performance

- Delete or disable unused cameras. FortiRecorder allocates memory with each camera, regardless of whether it is actually in active use. Configuring extra cameras will unnecessarily consume memory and decrease performance.
- To reduce latency associated with DNS queries, use a DNS server on your local network as your primary DNS.

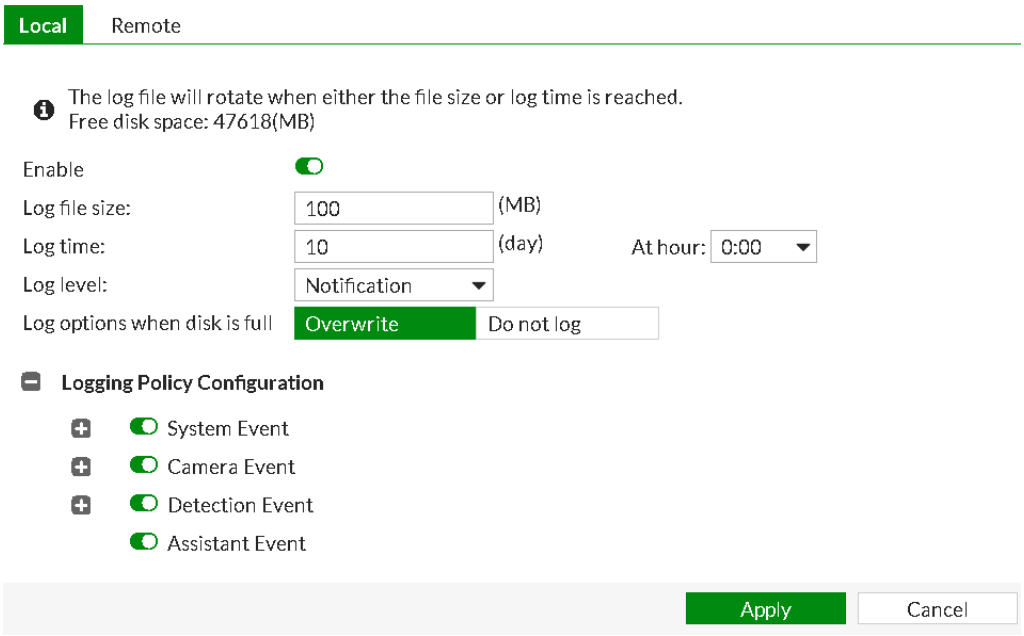
Logging and alert performance

If you have a FortiAnalyzer, store FortiRecorder's logs on the FortiAnalyzer to avoid resource usage associated with writing logs to FortiRecorder's own hard disks. See the Configuring Log Settings chapter.

If you do not need a log or alert, disable it to reduce the use of system resources.

Reduce repetitive log messages. Use the alert email settings, to define the interval that emails are sent if the same condition persists following the initial occurrence. See the chapter on Configuring Alert Email.

Avoid recording log messages using low severity thresholds, such as information or notification, to the local hard disk for an extended period of time. Excessive logging frequency saps system resources and can cause undue wear on the hard disk and may cause premature failure.



Packet capture performance

Packet capture can be useful for troubleshooting but can be resource intensive. (See "Packet capture".) To minimize the performance impact on your FortiRecorder appliance, use packet capture only during periods of minimal traffic. Use a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Updating and Backups

Upgrade to the latest available firmware to take advantage of new security features and stability enhancements.

Regular backups

Make a backup before executing operations that can cause large configuration changes, such as:

- Upgrading the firmware
- Running the CLI commands execute factory reset or execute restore
- Clicking the Restore button in the System Information widget on the dashboard

To mitigate impact in the event of a network compromise, always password-encrypt your backups. If your operating system does not support this feature, you can encrypt the file using third-party software.

Once you have tested your basic installation and verified that it functions correctly, create a backup. Aside from being an IT best practice, this “clean” backup can be used to:

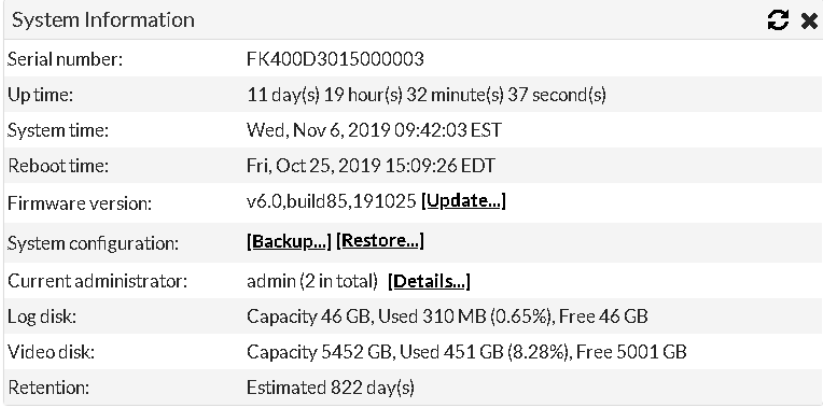
- troubleshoot a non-functional configuration by comparing it with this functional baseline (via a tool such as diff)
- rapidly restore your installation to a simple yet working point (see “Restoring a previous configuration”)
- batch-configure FortiRecorder appliances by editing the file in a plain text editor, then uploading the finalized configuration to multiple appliances (see “Restoring a previous configuration”)

After you have a working deployment, back up the configuration again after any changes. This will ensure that you can rapidly restore your configuration exactly to its previous state if a change does not work as planned.

Configuration backups do not include backups of video data or logs. For information about video backup, see “External storage”.

To back up the configuration

1. Log in to the web UI as the admin administrator. Other administrator accounts do not have the required permissions.
2. Go to *Dashboard* > *Status*.
3. In the System Information widget, in the System configuration row, select *Backup*



System Information	
Serial number:	FK400D3015000003
Up time:	11 day(s) 19 hour(s) 32 minute(s) 37 second(s)
System time:	Wed, Nov 6, 2019 09:42:03 EST
Reboot time:	Fri, Oct 25, 2019 15:09:26 EDT
Firmware version:	v6.0,build85,191025 [Update...]
System configuration:	[Backup...] [Restore...]
Current administrator:	admin (2 in total) [Details...]
Log disk:	Capacity 46 GB, Used 310 MB (0.65%), Free 46 GB
Video disk:	Capacity 5452 GB, Used 451 GB (8.28%), Free 5001 GB
Retention:	Estimated 822 day(s)

If your browser prompts you, navigate to the folder where you want to save the configuration file. select *Save*.

Your browser downloads the configuration file. Time required varies by the size of the file and the speed of your network connection, but could take several seconds. The default file name is <hostname>_YYYYMMDD.conf, where hostname is defined when you configure the mail server settingsand YYYYMMDD is the time-stamp of the backup.

Restoring a previous configuration

If you have downloaded configuration backups, you can upload one to revert the appliance’s configuration to that point

Uploading a configuration file can also be used to configure many features of the FortiRecorder appliance in a single batch: download a configuration file backup, edit the file in a plain text editor, then upload the finalized configuration.

To upload a configuration via the web UI

1. Go to *Dashboard* > *Status*.
2. In the System Information widget, in the System configuration row, select *Restore*.
3. Choose a FortiRecorder configuration backup file. (It has a .conf file extension.)
4. Select *Upload* to start the restoration of the selected configuration.
   Your web browser uploads the configuration file and the FortiRecorder appliance restarts with the new configuration. Time required to restore varies by the size of the file and the speed of your network connection. Your web UI session will be terminated when the FortiRecorder appliance restarts.
5. To continue using the web UI, if you have not changed the IP address and static routes of the web UI, simply refresh the web page and log in again.
   Otherwise, to access the web UI again, in your web browser, modify the URL to match the new IP address of the network interface.

   For example, if you configured port1 with the IP address 10.10.10.5, you would browse to:

   https://10.10.10.5

   If the new IP address is on a different subnet than the previous IP address, and your computer is directly connected to the FortiRecorder appliance, you may also need to modify the IP address and subnet of your computer to match the FortiRecorder appliance's new IP address.

System Maintenance

Go to *System* > *Maintenance* > *Configuration* to back up system configuration, restore configuration, restore firmware, or download the trace log.

Backing up configuration

Before installing FortiRecorder firmware or making significant configuration changes, back up your FortiRecorder configuration. Backups let you revert to your previous configuration if the new configuration does not function correctly. Backups let you compare changes in configuration.

To back up the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. Select System configuration backup.
3. Save the configuration file.

Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see "Restoring the configuration".

Restoring configuration

If you have just downgraded or restored the firmware of the FortiRecorder unit, restoring the configuration file can be used to reconfigure the FortiRecorder unit from its default settings.

To restore the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. Under Restore Configuration, click Browse to locate and select the configuration file that you want to restore, then select *Open*.The FortiRecorder unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
3. After restoring the configuration file, verify that the settings have been successfully loaded.

Downloading the trace log

If Fortinet Technical Support requests a trace log for system analysis purposes, you can download one using the web UI.

Trace logs are compressed into an archive (.gz), and contain information that is supplementary to debug-level log files.

To download a trace file

1. Go to *System* > *Maintenance* > *Configuration*.
2. At the bottom of the tab, select *Download trace log*.

Troubleshooting

This topic provides guidelines to help you resolve issues if your FortiRecorder appliance is not behaving as you expect.

Keep in mind that if you cannot resolve the issue on your own, you can contact Fortinet Technical Support.

This section contains the following topics:

- Viewing Issues
- Using Traffic Capture
- Notification Issues
- Login Issues
- Connectivity Issues
- Resource Issues
- Data Storage Issues
- Resetting the Configuration
- Restoring Firmware

Viewing Issues

The following section contains troubleshooting advice for various viewing issues.

If you can connect to FortiRecorder, and your cameras can connect with your FortiRecorder, but you cannot view video that is streamed or stored on FortiRecorder, fist check that you have installed software that can view live streams (which use RTP) and files (which use .mp4 format).

Different media players can interfere with each other. By default, some installers take file type associations previously belonging to other players and re-assign them to the new software. If you installed software to view downloaded video files, for example, and suddenly could no longer view live video streams, you might need to fix the file associations for RTP and/or MP4.

If you have installed a suitable media player but still cannot view the video, try clicking the panel arrows to hide and then show the panel again. For some Windows computers, this can solve the problem. (This QuickTime issue does not affect Mac OS X computers.)

If this does not trigger the video to play, make sure that its codec software does not have any conflicts, and is capable of displaying H.264 video. Media players' codec plug-ins can come from many sources, and if you have installed multiple codecs for the same format, display problems can arise.

This section addresses the following viewing issues:

- Live feed delay
- Video not being sent to the FortiRecorder

Live feed delay

Before QuickTime will begin playing a video stream, it must buffer a few seconds' worth of data. The time that QuickTime requires to do this may result in a few seconds' difference between what you see happening in the live video feed, and what is happening in reality now.

You can minimize this by:

- Changing the camera's Resolution setting to the lowest acceptable resolution
- Changing the camera's Resolution setting to the lowest acceptable resolution
- Improving the bandwidth and latency of your network

Video not being sent to the FortiRecorder

If the camera itself does not seem to be sending video to the FortiRecorder, although it has booted, has network connectivity, and you have configured a recording schedule on the FortiRecorder, you may see camera log messages such as:

```
Camera 'c1' is in an incorrect state: 'idle'. The expected state is 'continuous'.
```

Usually this is self-correcting. If not, or if a camera is otherwise unresponsive, reboot the camera:

```
execute camera reboot <camera_name>
```

If this does not solve the problem, try either upgrading the camera's firmware or resetting the camera to factory defaults, then re-configuring it (see the camera's QuickStart Guide).

Using Traffic Capture

When troubleshooting networks, review the contents of the packets. Reviewing the packets may determine if the packets, route, and destination are accurate. Traffic capture assists in troubleshooting various problems, such as:

- finding missing traffic
- monitoring session setup
- locating ARP problems, such as broadcast storm sources and causes
- confirming which address a computer is using on the network and if they have multiple addresses or are on multiple networks
- monitoring functioning routing
- intermittent missing PING packets.

If running a constant traffic application, such as ping, traffic capture displays if the traffic is reaching the destination, how the port enters and exits the FortiRecorder unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected.

To capture the traffic

1. Go to *System* > *Network* > *Traffic Capture*.
2. Select *New*.
3. Enter a description for the file generated from the captured traffic.

4. Select the time period for performing the packet capture from the Duration drop-down menus.
5. Specify which interface to capture from the Interface drop-down menu.
6. Enter a maximum of three IP addresses or host names to capture in the IP/Host field to limit the scope of traffic capture.
7. Select the filter for the traffic capture. Select *Use protocol to capture UDP or TCP traffic on the specified port number* or *None*.
8. Enter the IP address/host names and port numbers to not capture in the Exclusion field
9. Select *Create*.

   The generated PCAP file is viewable in Wireshark.

Notification Issues

If you are not receiving any email after motion detection records a clip, but you have configured camera notifications, first verify that your FortiRecorder's SMTP email settings are correct, and that it can connect to your email server to send email. Then check that notifications are not being blocked or sent to your spam or junk mail folder. (Some anti-spam systems mistakenly mark repeated or frequent email as spam.)

If you are receiving the email, and there are video links (that is, FortiRecorder has not been configured to email still images but you cannot view the video from the email:

1. Verify that you have installed the QuickTime video player software on your computer.
2. Verify that your computer can connect to the FortiRecorder's IP address. Unless you have configured FortiRecorder with your public IP, this is a private network IP address, and can only be reached when you are connected to your office's network. It cannot be viewed from the Internet. If you want to log in to the web UI and/or view video clips while out of the office, you must configure port forwarding and/or a virtual IP (VIP) on your firewall or Internet router, and configure the FortiRecorder to link to this public IP address in snapshot notifications.

If you are receiving too many notifications, change the configuration so that your FortiRecorder will only send snapshot notifications during suspicious periods, and focuses motion detection only on areas that do not cause false alerts, such as fans or blinking lights.

Login Issues

If the person cannot access the login page at all, it is usually actually a connectivity issue (see "Connectivity issues") unless all accounts are configured to accept login only from specific IP addresses or authentication has been externalized to an LDAP or RADIUS server.

If the person has lost or forgotten his or her password, the admin account can reset other accounts' passwords (see "Resetting passwords").

This section covers the following login issues:

- When an administrator account cannot log in from a specific IP
- Remote authentication query failures
- Resetting passwords
- Not able to push setting and the log shows error on password

When an administrator account cannot log in from a specific IP

If an administrator is entering his or her correct account name and password, but cannot log in from some or all computers, examine that account's trusted host definitions. It should include all locations where that person is allowed to log in, such as your office, but should not be too broad.

Remote authentication query failures

If your network administrators' or other accounts reside on an external server (e.g. Active Directory or RADIUS), first switch the account to be locally defined on the FortiRecorder appliance. If the local account fails, correct connectivity between the client and appliance (see "Connectivity issues"). If the local account succeeds, troubleshoot connectivity between the appliance and your authentication server. If routing exists but authentication still fails, you can verify correct vendor-specific attributes and other protocol-specific fields by running a packet trace (see "Packet capture").

Resetting passwords

If someone has forgotten or lost his or her password, or if you need to change an account's password and you do not know its current password, the admin administrator can reset the password.

If you forget the password of the admin administrator, however, you will not be able to reset its password through the web UI. You can reset the FortiRecorder to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see "Restoring firmware ("clean install")".

To reset an account's password

1. Log in as the admin administrator account.
2. Go to *System* > *User* > *User*.
3. Select the row to select the account whose password you want to change.
4. Select *Edit*.
5. In the New Password and Confirm Password fields, type the new password.
6. Select *OK*.

The new password takes effect the next time that account logs in.

Not able to push setting and log shows an error on password

A problem may occur when attempting to push setting to the FortiCamera and the log shows an issue with the password.

FortiRecorder will change the FortiCamera password during the initial configuration. The password is unique to each FortiCamera and is based on the MAC address. To fix the problem, perform the following:

1. Perform a factory reset on the physical FortiCamera.
2. Manually add the MAC address of the FortiCamera to the FortiRecorder settings.

Connectivity Issues

One of your first tests when configuring a new device should be to determine whether video is being received from your camera, and whether commands/schedules are being sent to it. You should also test whether notification email can be sent, and accounts (administrators, operators, etc.) can log in to the web UI and view live video feeds.

After initial setup, connectivity should not be interrupted. FortiRecorder may sometimes be able to recover if, for example, a DHCP-addressed camera changes its IP. However this may result in disruptions to recording, and camera log messages such as:

```
Camera 'c1' experienced an interruption that may result in a loss of recording.
```

If connections fail or perform erratically, check the following in order:

- Checking hardware connections
- Bringing up network interfaces
- Examining the ARP table
- Checking routing
- Facilitating discovery
- DHCP issues
- Unauthorized DHCP clients or DHCP pool exhaustion
- Establishing IP sessions
- Resolving IP address conflicts
- Packet capture

Troubleshooting is in order from more fundamental OSI layers of your network to the higher, more application-specific. If you are not setting up a new network, you may prefer to start with the more FortiRecorder-specific layers of your network, later in this section.

Checking hardware connections

If there is no traffic whatsoever arriving to the FortiRecorder appliance, even though the configuration appears to be correct, it may be a hardware problem.

- Verify that the LEDs for the ports light to indicate firm electrical contact when you plug network cables into the appliance. For LED indications, see your model's QuickStart Guide.
- If the cable or its connector are loose or damaged, or you are unsure about the cable's type or quality, change it or test with a loopback jack.

If traffic ingresses and egresses but performance is not what you expect, verify that the MTU matches other devices on your network.

If the hardware connections are functional and the appliance is powered on, but you cannot connect — even using a local console connection to the CLI rather then a network connection — you may be experiencing bootup problems. Contact Fortinet Technical Support.

Bringing up network interfaces

If the network interface was disabled, all connections will fail even though the cable has connectivity physically.

If the network interface's Status column is a red "down" arrow, its administrative status is currently "down" and it will not receive or emit packets, even if you otherwise configure it. To bring up the network interface, edit the Administrative status setting. This Status column is not the detected physical link status; it is the administrative status that indicates whether you permit network interface to receive and/or transmit packets. For example, if the cable is physically unplugged, diagnose netlink interface list port1 may indicate that the link is down, even though you have administratively enabled it by Administrative status. By definition, HA heartbeat and synchronization links should always be "up." Therefore, if you have configured FortiWeb to use a network interface for HA, its Status column will always display HA Member.

In the web UI, go to *System* > *Network* > *Interface*. If the status is down (a down arrow on red circle), click Bring Up next to it in the Status column to bring up the link.

Alternatively you can enable an interface in CLI:

```
config system interface
   edit port2
      set status up
end
```

Examining the ARP table

When connectivity cannot be established or is periodically interrupted, but hardware and link status is not an issue, the first place to look is at a slightly higher layer in network connections: the address resolution protocol (ARP) table. While most devices' MAC address is bound to the hardware at the manufacturer and not easily changed, some devices have configurable or virtual MACs. In this case, you should make sure there is no conflict which could cause the IP to resolve to a different network port whenever that other device is connected to your network.

Functioning ARP is especially important in high availability (HA) topologies. If changes in which MAC address resolves to which IP address are not correctly propagated through your network, failovers may not work.

To display the ARP table in the CLI, enter:

```
diagnose network arp list
```

Checking routing

If the MAC resolves correctly, but IP connectivity fails, try using ICMP (ping and traceroute) to determine if the host is reachable, or to locate the point on your network at which connectivity fails. You can do this from the FortiRecorder appliance using CLI commands.

IP layer connectivity fails when routes are incorrectly configured. Static routes direct traffic exiting the FortiRecorder appliance — you can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. Routers are aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations. Your FortiRecorder itself does not need to know the full route, as long as the routers can pass along the packet.

You must configure FortiRecorder with at least one static route that points to a router, often a router that is the gateway to the Internet. You may need to configure multiple static routes if you have multiple gateway routers (e.g. each of which should receive packets destined for a different subset of IP addresses), redundant routers (e.g. redundant Internet/ISP links), or other special routing cases.

However, often you will only need to configure one route: a default route.

For example, if a web server is directly attached to one physical port on the FortiRecorder, but all other destinations, such as connecting clients, are located on distant networks, such as the Internet, you might need to add only one route: a default route that indicates the gateway router through which the FortiRecorder appliance can send traffic in the direction towards the Internet.

If your management computer is not directly attached to one of the physical ports of the FortiRecorder appliance, you may also require a static route so that your management computer is able to connect with the web UI and CLI.

To determine which route a packet will be subject to, FortiRecorder examines each packet's destination IP address and compares it to those of the static routes. It will forward the packet along to the route with the largest prefix match, automatically egressing from the network interface on that network. (Egress port for a route cannot be manually configured.) If multiple routes match the packet, the FortiRecorder appliance will apply the route with the smallest index number. For this reason, you should give more specific routes a smaller index number than the default route.

The ping command sends a small data packet to the destination and waits for a response. The response has a timer that may expire, indicating that the destination is unreachable via ICMP. ICMP is part of Layer 3 on the OSI Networking Model. ping sends Internet Control Message Protocol (ICMP) ECHO_REQUEST packets to the destination, and listens for ECHO_RESPONSE packets in reply. Beyond basic existence of a possible route between the source and destination, ping tells you the amount of packet loss (if any), how long it takes the packet to make the round trip (latency), and the variation in that time from packet to packet (jitter).

Similarly, traceroute sends ICMP packets to test each hop along the route. It sends three packets to the destination, and then increases the time to live (TTL) setting by one, and sends another three packets to the destination. As the TTL increases, packets go one hop farther along the route until they reach the destination.

Most traceroute commands display their maximum hop count — that is, the maximum number of steps it will take before declaring the destination unreachable — before they start tracing the route. The TTL setting may result in routers or firewalls along the route timing out due to high latency. If you specify the destination using a domain name, the traceroute output can also indicate DNS problems, such as an inability to connect to a DNS server.

By default, FortiRecorder appliances will respond to ping and traceroute. However, if FortiRecorder does not respond, and there are no firewall policies that block it, ICMP type 0 (ECHO_REPSPONSE or "pong") might be effectively disabled. By default, traceroute uses UDP with destination ports numbered from 33434 to 33534. The traceroute utility usually has an option to specify use of ICMP ECHO_REQUEST (type 8) instead, as used by the Windows tracert utility. If you have a firewall and you want traceroute to work from both machines (Unix-like systems and Windows) you will need to allow both protocols inbound through your firewall (UDP ports 33434 - 33534 and ICMP type 8).

Some networks block ICMP packets because they can be used in a ping flood or denial of service (DoS) attack if the network does not have anti-DoS capabilities, or because ping can be used by an attacker to find potential targets on the network.

To enable ping & traceroute responses from FortiRecorder

1. Go to *System* > *Network* > *Interface*. To access this part of the web UI, you must have Read and Write permission in your administrator's account access profile to items in the Router Configuration category.

2. In the row for the network interface which you want to respond to ICMP type 8 (ECHO_REQUEST) for ping and UDP for traceroute, click Edit.
3. Enable PING.

> Disabling PING only prevents FortiRecorder from receiving ICMP type 8 (ECHO_REQUEST) or type 30 and traceroute-related UDP.
>
> It does not disable FortiRecorder CLI commands such as execute ping or execute traceroute that send such traffic.
>
> Since you typically use these tools only during troubleshooting, you can allow ICMP, the protocol used by these tools, on interfaces only when you need them. Otherwise, disable ICMP for improved security and performance

4. Select *OK*. The appliance should now respond when another device such as your management computer sends a ping or traceroute to that network interface.

To verify routes between cameras & your FortiRecorder

1. Use FortiRecorder's execute ping command with the camera's IP address to verify that a route exists between the two.
2. If possible, temporarily connect a computer at the camera's usual physical location, using the camera's usual IP address, so that you can use its ping command to test traffic movement along the path in both directions: from the location of the camera (temporarily, the computer) to the FortiRecorder, and the FortiRecorder to the camera.

> notetable - text middled. Note bulb icon - text middled. Note bulb icon - text middled. Note bulb icon - text middled. Note bulb icon - text middled. Note bulb icon - text middled...

If the routing test succeeds, continue with step 4

> Connectivity via ICMP only proves that a route exists. It does not prove that connectivity also exists via other protocols at other layers such as HTTP.

If ping shows some packet loss, investigate:

- cabling to eliminate loose connections
- ECMP, split horizon, or network loops
- dynamic routing such as OSPF
- all equipment between the ICMP source and destination to minimize hops

If the routing test fails, and ping shows total packet loss:

- verify cabling to eliminate loose connections
- continue to the next step

> Both ping and traceroute require that network nodes respond to ICMP. If you have disabled responses to ICMP on your network, hosts may appear to be unreachable to ping and traceroute, even if connections using other protocols can succeed.

For example, you might use ping to determine that 172.16.1.10 is reachable:

```
FortiRecorder-200D# execute ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=64 time=2.4 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=1.4 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=1.4 ms

--- 172.20.120.167 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.4/2.4 ms
or that 192.168.1.10 is not reachable:
FortiRecorder-200D# execute ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 192.168.1.10 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

3. Use the tracert or traceroute command on both the camera (temporarily, the computer) and FortiRecorder to locate the point of failure along the route, the router hop or host at which the connection fails. For example, if it fails at the second hop, you might see:

```
FortiRecorder-200D# execute traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 32 hops max, 72 byte packets
1 192.168.1.2 2 ms 0 ms 1 ms
2 * * *
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router. The asterisks (*) indicate no response from that hop in the network routing.

If the route is broken when it reaches the FortiRecorder, first examine its network interfaces and routes. To display network interface addresses and subnets, enter:

```
FortiRecorder-200D# show system interface
```

To display all recently-used routes (the routing table cache) with their priorities, enter:

```
FortiRecorder-200D# diagnose netlink rtcache list
```

The index number of the route in the list of static routes in the web UI is not necessarily the same as its position in the cached routing table (diagnose netlink rtcache list).

You may need to verify that there are no misconfigured DNS records, and otherwise rule out problems at the physical, network, and transport layer.

If these tests succeed, a route exists, but you cannot receive video feeds or use FortiRecorder to update the camera's network settings, an application-layer problem is preventing connectivity.

4. For application-layer problems, on the FortiRecorder, examine the:
   - camera network settings (these may have become out-of-sync if you modified them while the camera was disabled)
   - certificates (if connecting via HTTPS)

   On routers and firewalls between the host and the FortiRecorder appliance, verify that they permit HTTP, HTTPS, and RTP connectivity between them.

Relatedly, if the computer's DNS query cannot resolve the host name, output similar to the following appears:

```
example.lab: Name or service not known
Cannot handle "host" cmdline arg `example.lab' on position 1 (argc 1)
```

Facilitating discovery

Discovery of the cameras by the FortiRecorder uses UPnP and ONVIF. For it to work, cameras usually must be on the same IP subnet as the FortiRecorder, and must not be impeded by firewalls or other network filtering. If cameras are not on the same subnet, you may still be able to facilitate discovery traffic by configuring your FortiGate or other device with multicast forwarding.

If you do not know which device is impeding discovery, you can either:

- Temporarily attach the cameras to a closer point on the network, such as a local switch or directly to the FortiRecorder, so that discovery is not blocked.
- Manually add the camera to the FortiRecorder's list of known cameras, skipping discovery.

DHCP issues

The FortiRecorder appliance has a built-in DHCP server. By default, it is disabled.

If you enable it and your network has another DHCP server (e.g. your ISP's cable modem, a router, or a Windows or Linux server), verify that:

- both are not serving requests on the same network segment (which could create a race condition)
- both are not using the same pool of IP addresses (which could lead to IP address conflicts — see "Resolving IP address conflicts")

To verify that your appliance and cameras are sending and receiving lease requests, you can perform a packet trace (see "Packet capture") and/or use the event log to look for:

- DHCPDISCOVER (destination IP is broadcast, not FortiRecorder's)
- DHCPOFFER
- DHCPREQUEST
- DHCPACK

Unauthorized DHCP clients or DHCP pool exhaustion

Typically returning DHCP clients will receive the same IP address lease. However if computers or other devices are accidentally using IP addresses that the FortiRecorder's built-in DHCP server should be allocating to cameras, and the pool of available DHCP IP addresses becomes exhausted, cameras may be unable to get or retain an IP address.

To determine which devices are using your pool of DHCP IP addresses, compare the MAC address of each device's network adapter to the list of current DHCP clients in *Monitor* > *DHCP* > *DHCP* or enter this command in the CLI:

```
execute dhcp lease-list
```

Output will resemble the following:

```
port3
  IP                    MAC-Address                    VCI             Expiry
  192.168.200.100              20:10:7a:5a:28:d1       udhcp 0.9.8          Thu Oct  4 15:01:22
  192.168.200.101              20:10:7a:5a:29:38       udhcp 0.9.8          Wed Oct  3 11:17:12
```

To correct this situation, first configure unintentional DHCP clients so that they do not use DHCP (that is, they have a static IP address) and so their IP address is not in the range used by the DHCP pool. Second, clear the list of DHCP clients to allow legitimate DHCP clients (your cameras) to obtain a lease:

```
execute dhcp clear-lease
```

New clients that were previously unable to get an IP address will obtain an IP address for the first time. Returning clients' s IP addresses may change as the built-in DHCP server no longer has any memory of their previous lease, and may assign them a new IP address if another client has claimed that IP address first. (This may result in temporary IP address conflicts and therefore connectivity interruptions while the DHCP server assigns new leases.)

Establishing IP sessions

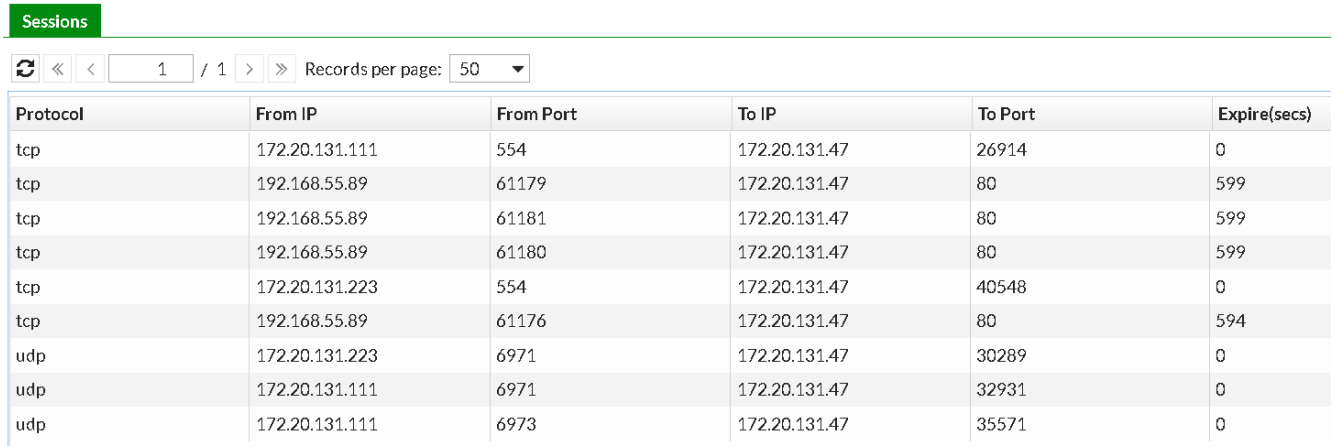
If a route exists, but there appears to be a problem establishing or maintaining TCP or IP-layer sessions between FortiRecorder and a computer or camera on your IP network, there are multiple possible causes, such as:

- Trusted hosts
- protocols/port numbers mismatched or blocked by NAT or firewalls
- IP address conflicts
- short DHCP leases (Lease time (Seconds) in "Configuring the DHCP server")
- socket exhaustion

You can view a snapshot of FortiRecorder's session table according to the IP layer. Go to *FortiView* > *Sessions* > *Sessions*.

Sessions

1 / 1 Records per page: 50



Protocol	From IP	From Port	To IP	To Port	Expire(secs)
tcp	172.20.131.111	554	172.20.131.47	26914	0
tcp	192.168.55.89	61179	172.20.131.47	80	599
tcp	192.168.55.89	61181	172.20.131.47	80	599
tcp	192.168.55.89	61180	172.20.131.47	80	599
tcp	172.20.131.223	554	172.20.131.47	40548	0
tcp	192.168.55.89	61176	172.20.131.47	80	594
udp	172.20.131.223	6971	172.20.131.47	30289	0
udp	172.20.131.111	6971	172.20.131.47	32931	0
udp	172.20.131.111	6973	172.20.131.47	35571	0

GUI Item	Description
Protocol	The protocol of the session according to the "protocol" ID number field (or, for IPv6, "next header") in the IP header of the packets. • icmp — 1 (Due to the speed of ICMP messages, this will almost never be seen in the session list.)

GUI Item	Description
	• tcp — 6 • udp — 17 (Due to the speed of UDP datagrams, this may be seen in the session list only rarely.)
From IP	The source of the session according the source field in the IP header. If source NAT is occurring, this is not necessarily the IP in the original frame from the client.
From Port	The source port number. For a list of port numbers that can originate from the FortiRecorder, see “Appendix A: Port numbers”.
To IP	The destination according to the destination field in the IP header. If destination NAT is occurring, this is not necessarily the IP in the original frame from the client.
To Port	The destination port number. For a list of port numbers that can be received by the FortiRecorder, see “Appendix A: Port numbers”.
Expire (seconds)	The session timeout in seconds. The expiry counter is reset when packets are sent or received, indicating that the session is still active.

To refresh the session list snapshot with the most current list, click the dotted circle (Refresh) icon to the left of Records per page.

To sort the session list based upon the contents of a column, hover your mouse cursor over the column’s heading then click the arrow that appears on the right side of the heading, and select either Sort Ascending or Sort Descending.

If you expect sessions that do not exist, be aware that some protocol designs (notably UDP) do not feature persistent sessions. Their sessions will almost immediately expire and be removed from the session list, and therefore it may be very difficult to capture a session list snapshot during the brief moment that the datagram is being transmitted. TCP features persistent connections, where the socket is maintained until the data transmission either is confirmed to be finished or times out, and therefore TCP connections will persist in the session table for a much longer time.

If you still do not see the sessions that you expect, verify that your firewall or router allows traffic to or from those IP addresses, on all expected source and destination port numbers (see “Appendix A: Port numbers”).

If you see sessions with the FortiRecorder web UI or CLI that should not be allowed to exist, be sure to configure all accounts’ Trusted hosts setting.

Resolving IP address conflicts

If two or more devices are configured to use the same IP address on your network, this will cause a problem called an IP address conflict. Only one of those identically addressed devices can have IP-layer connectivity at a given time. The other will be ignored, effectively causing it to behave as if it were disconnected. (If multiple devices were to use the same IP address, routers and switches would not be able to determine with certainty where to deliver a packet destined for that IP address. To prevent this, routers and switches will only let one of the devices use the IP.)

Typically IP conflicts are caused when either:

- you have accidentally configured 2 devices with the same static IP address
- you have accidentally configured a device with a static IP address that belongs to the DHCP pool

- 2 DHCP servers accidentally have pools in the same range of IP addresses, and are each independently assigning their clients the same IPs

Your cameras, of course, have no screen, and cannot display any IP address conflict error message. However, you may notice symptoms such as interrupted video streams whenever a new device connects to the network or reboots.

If you have configured your FortiRecorder's built-in DHCP server, first verify that it is not using the same DHCP pool as another DHCP server on your network. Next, you can use the CLI to determine whether MAC addresses from other devices' network adapters have stolen IP addresses that should belong to your cameras. See "Unauthorized DHCP clients or DHCP pool exhaustion". If, however, you have transitioned your cameras to use static IP addresses, you must use another method.

- Use the ARP table of either your FortiRecorder (see "Examining the ARP table") or router to determine which MAC address (and therefore which computer/device's network adapter) has taken the IP address.
- If a computer is using the same IP address as another device, such as your cameras, it may periodically complain of an IP address conflict. This computer may be the source of the conflict.

Once you have found the source of the problem, configure that computer or device to use a unique IP address that is not used by any other device on your network.

Packet capture

Packet capture, also known as sniffing, packet trace, or packet analysis, records some or all of the packets seen by a network interface (that is, the network interface is used in promiscuous mode). By recording packets, you can trace TCP connection states and HTTP request transactions to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect, such as malformed packets, differentiated services misconfiguration, or non-RFC protocol incompatibilities.

Packet capture can be very resource intensive. To minimize the performance impact on your FortiRecorder appliance, use packet capture only during periods of minimal traffic, with a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

FortiRecorder appliances have a built-in sniffer. Packet capture on FortiRecorder appliances is similar to that of FortiGate appliances. To use the built-in sniffer, connect to the CLI and enter the following command:

```
diagnose sniffer packet [{any | <interface_name>}
   [{none | '<filter_str>'} [{1 | 2 | 3 | 4 | 5 | 6} [<packets_int>
   [{a | <any_str>}]]]]]
```

where:

- <interface_name> is either the name of a network interface, such as port1, or enter any for all interfaces. If you omit this and the following parameters for the command, the command captures all packets on all network interfaces.
- '<filter_str>' is the sniffer filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 80', or enter none for no filters. Filters use tcpdump syntax.
- <packets_int> is the number of packets the sniffer reads before stopping. Packet capture output is printed to your CLI display until you stop it by pressing Ctrl+C, or until it reaches the number of packets that you have specified to capture.
- {a | <any_str>} is either a (to include an absolute, full UTC timestamp in the format yyyy-mm-dd hh:mm:ss.ms), or any other text (to include a timestamp that is the amount of time since he start of the packet capture, in the format ss.ms)

- {1 | 2 | 3 | 4 | 5 | 6} is an integer indicating whether to display the network interface names, packet headers, and/or payloads for each packet that the network interface sends, receives, or sees:
- 1 — Display the packet capture timestamp, plus basic fields of the IP header: the source IP address, the destination IP address, protocol name, and destination port number.
- Does not display all fields of the IP header; it omits:
  - IP version number bits
  - Internet header length (ihl)
  - type of service/differentiated services code point (tos)
  - explicit congestion notification
  - total packet or fragment length
  - packet ID
  - IP header checksum
  - time to live (TTL)
  - IP flag
  - fragment offset
  - options bits
    example:

```
interfaces=[port2]
filters=[none]
0.655224 172.20.130.16.2264 -> 172.20.130.15.42574: udp 113
```

  - 2 — All of the output from 1, plus the packet payload in both hexadecimal and ASCII.
    example:

```
interfaces=[port2]
filters=[none]
0.915616 172.20.130.16.2264 -> 172.20.130.15.42574: udp 124
0x0000   4500 0098 d27d 4000 4011 0b8f ac14 8210        E....}@.@.......
0x0010   ac14 820f 08d8 a64e 0084 b75a 80e0 3dee        .......N...Z..=.
0x0020   71b8 d617 38fa 3fd8 419b 5006 053c 99c1        q...8.?.A.P..<..
0x0030   e961 93bc 21c9 3197 a030 a709 76dc 0ed8        .a..!.1..0..v...
0x0040   98f8 ceef 6afb e7f2 7773 98e1 5ef7 bfbf        ....j...ws..^...
0x0050   2f0d 726f 70cf 26cd d986 392f 4a0b f97b        /.rop.&...9/J..{
0x0060   b84f 932d 3043 cbdd c2dc da77 0b73 70fc        .O.-0C.....w.sp.
0x0070   158a 1868 eee0 793b c09e 7dc0 59f5 787c        ...h..y;..}.Y.x|
0x0080   fc1a f25a dc18 735d f090 8e05 c3e8 c14f        ...Z..s].......O
0x0090   3466 57c0 4688 58b8                            4fW.F.X.
```

- 3 — All of the output from 2, plus the link layer (Ethernet) header.
  example:

```
interfaces=[port2]
filters=[none]
0.317960 172.20.130.16.2264 -> 172.20.130.15.42574: udp 31
0x0000   50e5 49e8 dc3d 000f 7c08 2ff5 0800 4500        P.I..=..|./...E.
0x0010   003b 2cad 4000 4011 b1bc ac14 8210 ac14        .;,.@.@.........
0x0020   820f 08d8 a64e 0027 ea3c 80e0 981e 7474        .....N.'.<....tt
0x0030   6ddf 38fa 3fd8 419b 6e06 00f0 8dd5 e01d        m.8.?.A.n.......
0x0040   810a e049 e5e9 380a f8                         ...I..8..
```

- 4 — All of the output from 1, plus the network interface name. This can be necessary if you are capturing packets from multiple network interfaces at once, and need to know which packet was seen by which interface.
  example:

```
interfaces=[port2]
filters=[none]
0.918575 port2 -- 172.20.130.16.2264 -> 172.20.130.15.42574: udp 38
```

- 5 — All of the output from 2, plus the network interface name.
  example:

```
interfaces=[port2]
filters=[none]
0.508965 port2 -- 172.20.130.16.2265 -> 172.20.130.15.42575: udp 44
0x0000   4500 0048 03ab 4000 4011 dab1 ac14 8210        E..H..@.@.......
0x0010   ac14 820f 08d9 a64f 0034 df2e 80c8 0006        .......O.4......
0x0020   38fa 3fd8 d39f 1ee5 7597 80ba 75f0 bb05        8.?.....u...u...
0x0030   0000 3064 0831 856b 81ca 0003 38fa 3fd8        ..0d.1.k....8.?.
0x0040   0105 6c6f 6262 7900                            ..lobby.
```

- 6 — All of the output from 3, plus the network interface name.
  example:

```
interfaces=[port2]
filters=[none]
0.169046 port2 -- 172.20.130.16.2268 -> 172.20.130.15.35552: udp 46
0x0000   50e5 49e8 dc3d 000f 7c08 2ff5 0800 4500        P.I..=..|./...E.
0x0010   004a 8989 4000 4011 54d1 ac14 8210 ac14        .J..@.@.T.......
0x0020   820f 08dc 8ae0 0036 43eb 80e0 590e 5ad4        .......6C...Y.Z.
0x0030   6e1a 53b4 db17 419b d006 02bd e02d f92e        n.S...A......-..
0x0040   f809 35ac 020e f4a0 3ac4 7097 7cd9 01b3        ..5.....:.p.|...
0x0050   cdd5 42dc 9e6c 0ec0                            ..B..l..
```

For example, you might capture all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the

administrator presses Ctrl+C. The sniffer then confirms that five packets were seen by that network interface.

(Verbose output can be very long. As a result, output shown below is truncated after only one packet.)

```
FortiRecorder# diagnose sniffer packet port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000   0009 0f09 0001 0009 0f89 2914 0800 4500
     ..........)...E.
0x0010   003c 73d1 4000 4006 3bc6 d157 fede ac16
     .<s.@.@.;..W....
0x0020   0ed8 c442 01bb 2d66 d8d2 0000 0000 a002
     ...B..-f........
0x0030   16d0 4f72 0000 0204 05b4 0402 080a 03ab
     ..Or............
0x0040   86bb 0000 0000 0103 0303                          ..........
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is often, but not always, preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark (http://www.wireshark.org/).

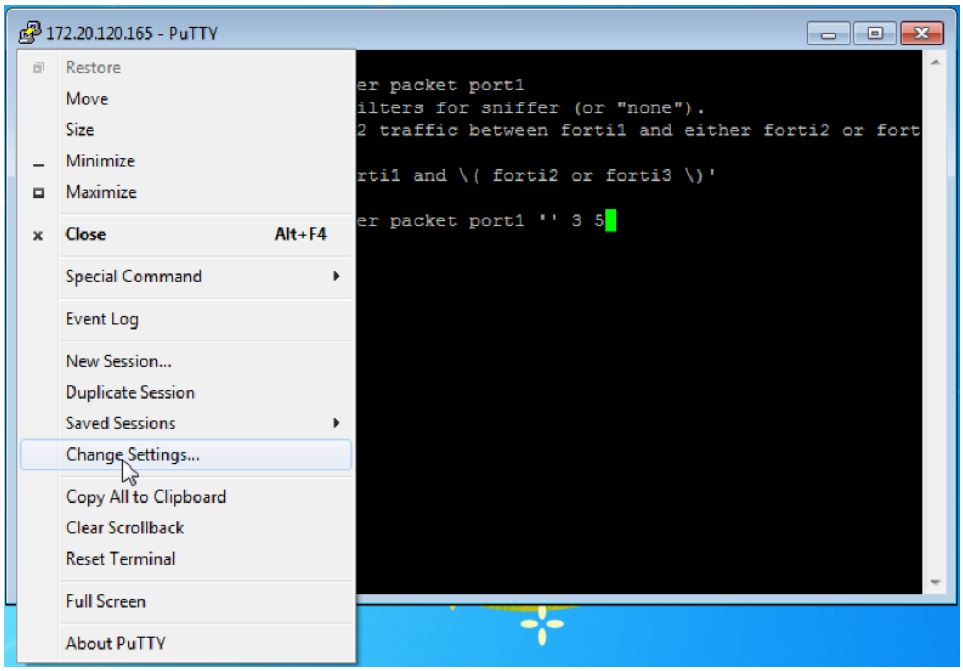
For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output to a file. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY
- a plain text editor such as Notepad
- a Perl interpreter
- network protocol analyzer software such as Wireshark

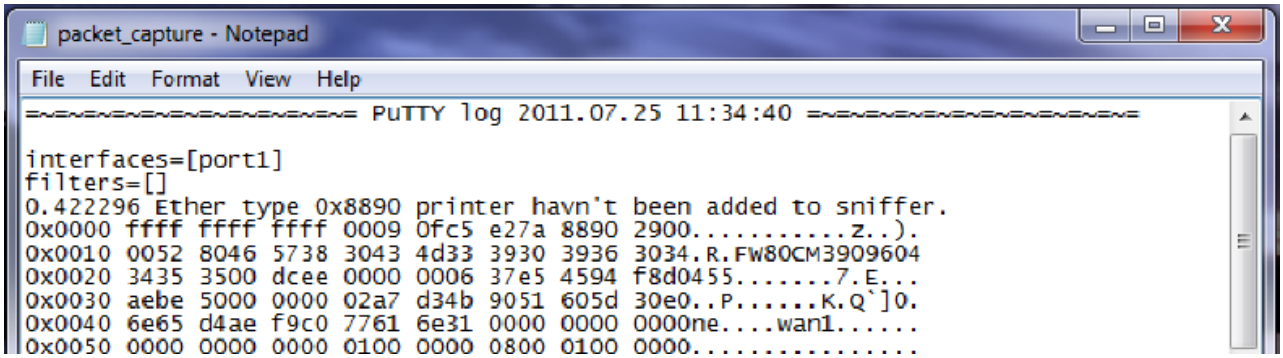
To view packet capture output using PuTTY and Wireshark

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the FortiRecorder appliance using either a local console, SSH, or Telnet connection.
3. Type the packet capture command, such as:
   `diag sniffer packet port1 'src host 10.0.0.1 and tcp port 443' 3`
   but do not press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select Change Settings.



A dialog appears where you can configure PuTTY to save output to a plain text file.

5. In the Category tree on the left, go to *Session* > *Logging*.
6. In Session logging, select Printable output.
7. In Log file name, click the Browse button, then choose a directory path and file name such as C:\Users\MyAccount\packet_capture.txt to save the packet capture to a plain text file. (You do not need to save it with the .log file extension.)
8. Select *Apply*.
9. Press Enter to send the CLI command to the FortiRecorder appliance, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.



13. Delete the first and last lines, which look like this:

```
=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2020.07.25 11:34:40 =~=~=~=~=~=~=~=~=~=~=~=
FortiRecorder-200 #
```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
You can convert the plain text file to a format (.pcap) recognizable by Wireshark (formerly called Ethereal) using the fgt2eth.pl Perl script. To download fgt2eth.pl, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

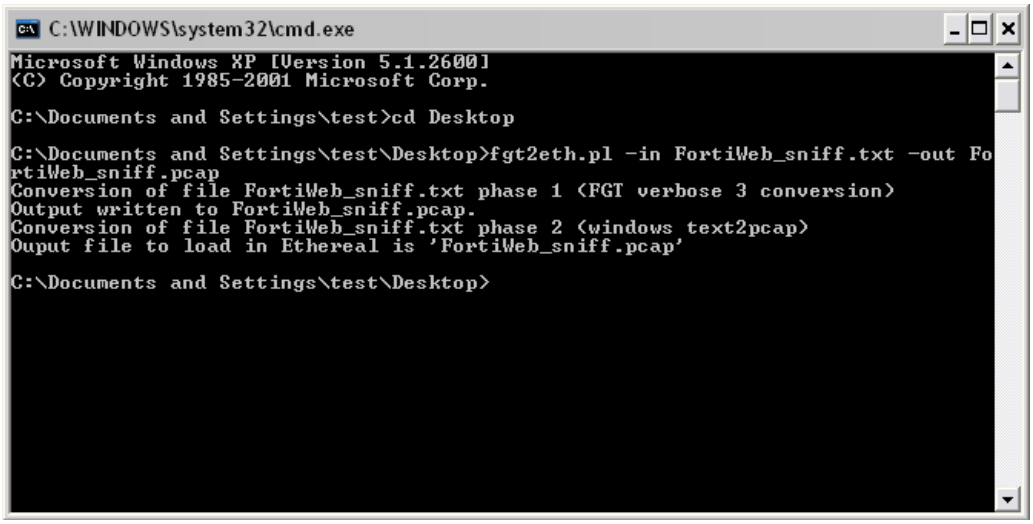
To use fgt2eth.pl, open a command prompt, then enter a command such as the following:

Methods to open a command prompt vary by operating system. On Windows XP, go to Start > Run and enter cmd. On Windows 7, click the Start (Windows logo) menu to open it, then enter cmd.

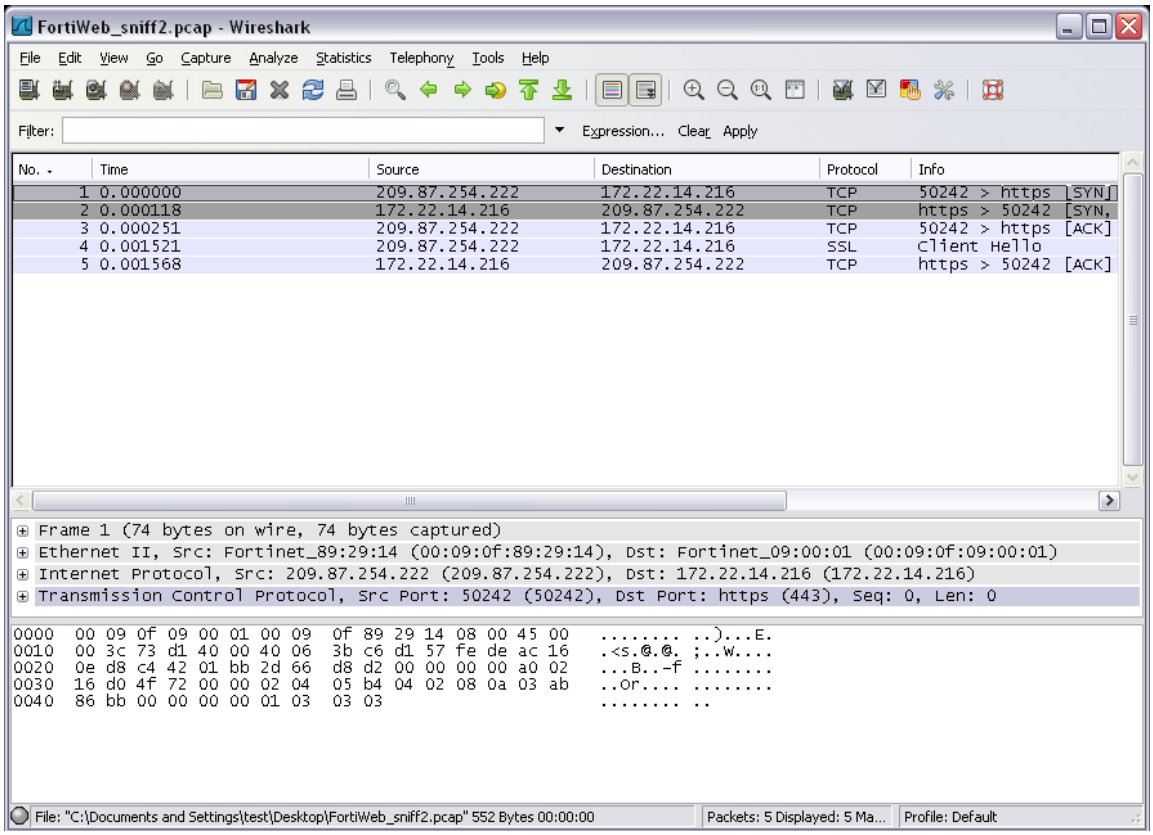
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap

where:

- fgt2eth.pl is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- packet_capture.txt is the name of the packet capture's output file; include the directory path relative to your current directory
- packet_capture.pcap is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved



15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.



For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

Resource Issues

If the system resource usage appears to be abnormally high according to the System Resource widget on the dashboard or the CLI command:

```
get system status
```

you can view the current consumption by each process by entering this CLI command:

```
diagnose system top 10
```

The above command generates a list of processes every 10 seconds. It includes the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI until you press q (quit).

Once you locate an offending PID, you can terminate it:

```
diagnose system kill 9 <pid_int>
```

If the issue recurs, and corresponds with a hardware or configuration change, you may need to change the configuration (especially frequent logging and high resolution video streams), reduce traffic load or contact Fortinet Technical Support to prevent the issue from recurring.

Data Storage Issues

If FortiRecorder cannot locally store any data such as logs, reports, and video, and FortiRecorder has been storing data but has suddenly stopped, first verify that FortiRecorder has not used all of its local storage capacity by entering this CLI command:

```
diagnose hardware sysinfo df
```

which will include disk usage for all mounted file systems, such as:

```
Filesystem            Size  Used Avail Use% Mounted on
none                  180M  104M   77M  58% /
none                     0     0     0   -  /proc
none                     0     0     0   -  /sys
none                     0     0     0   -  /dev/pts
none                   10M   32K   10M   1% /dev/shm
/dev/sdb1             284M   54M  230M  19% /data
/dev/sda2              92G  333M   87G   1% /var/log
/dev/sda3             824G  118G  665G  16% /var/spool
//172.16.10.200/NVR   226G   25G  201G  11% /mnt/remote
```

You can use alerts to notify you when FortiRecorder has almost consumed its hard disk space. You can also configure FortiRecorder to overwrite old logs rather than stopping logging when the disk is full. (Keep in mind, however, that this may not prevent full disk problems for other features. To free disk space, delete files such as old reports and video that you no longer need.)

If a full disk is not the problem, examine the configuration to determine if an administrator has disabled those features that store data.

If neither of those indicate the cause of the problem, verify that the disk's file system has not been mounted in read-only mode, which can occur if the hard disk is experiencing problems with its write capabilities. For details, contact Fortinet Technical Support.

Removing individual video clips

There is no option to remove an individual recording but the command to remove all videos on the system is:

```
# execute partitionlogdisk
# execute formatvideodisk
```

This will require a system reboot.

Resetting the Configuration

If you will be selling your FortiRecorder appliance, or if you are not sure what part of your configuration is causing a problem, you can reset it and its cameras to their default settings and erase data. (If you have not updated the firmware, this is the same as resetting to the factory default settings.)

Back up your configuration before beginning this procedure, if possible. Resetting the configuration could include the IP addresses of network interfaces. For information on backups, see “Regular backups”. For information on reconnecting to a FortiRecorder appliance whose network interface configuration was reset, see “Connecting to FortiRecorder web UI”. For information on reconnecting your cameras, see “Configuring video profiles”.

To reset your cameras’ configuration, connect to the CLI and enter these commands:

```
config camera devices
   edit <camera_name>
      set status disable
end
execute camera factoryreset <camera_name>
```

To delete your data from the FortiRecorder, connect to the CLI and enter this command:

```
execute formatlogdisk
```

To reset the FortiRecorder’s configuration, connect to the CLI and enter this command:

```
execute factoryreset
```

Alternatively, you can reset the FortiRecorder’s configuration to its default values for a specific software version by restoring the firmware during a reboot (a “clean install”). See “Restoring firmware (“clean install”)”.

Restoring Firmware

Restoring the firmware can be useful if:

- you are unable to connect to the FortiRecorder appliance using the web UI or the CLI
- you want to install firmware without preserving any existing configuration (i.e. a “clean install”) a firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike updating firmware, restoring firmware re-images the boot device, including the signatures that were current at the time that the firmware image file was created. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. It cannot be done through an SSH or Telnet connection.

Alternatively, if you cannot physically access the appliance's local console connection, connect the appliance's local console port to a terminal server to which you have network access. Once you have used a client to connect to the terminal server over the network, you will be able to use the appliance's local console through it. However, be aware that from a remote location, you may not be able to power cycle the appliance if abnormalities occur.

To restore the firmware

Back up your configuration before beginning this procedure, if possible. Restoring firmware resets the configuration, which could include the IP addresses of network interfaces. For information on backups, see "Regular backups". For information on reconnecting to a FortiRecorder appliance whose network interface configuration was reset, see "Connecting to FortiRecorder web UI".

1. Download the firmware file from the Fortinet Technical Support web site: https://support.fortinet.com/
2. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a local console connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the admin administrator, or an administrator account whose access profile contains Read and Write permissions in the Maintenance category.
4. Connect port1 of the FortiRecorder appliance directly or to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. If necessary, start your TFTP server. (If you do not have one, you can temporarily install and run one such as tftpd (Windows, Mac OS X, or Linux) on your management computer.)

   Because TFTP is not secure, and because it does not support authentication and could allow anyone to have read and write access, you should only run it on trusted administrator-only networks, never on computers directly connected to the Internet. If possible, immediately turn off tftpd off when you are done.

7. Verify that the TFTP server is currently running, and that the FortiRecorder appliance can reach the TFTP server. To use the FortiRecorder CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.1.168
   ```
   where 192.168.1.168 is the IP address of the TFTP server.
8. Enter the following command to restart the FortiRecorder appliance:
   ```
   execute reboot
   ```
9. As the FortiRecorder appliances starts, a series of system startup messages appear.
   ```
   Press any key to display configuration menu........
   ```
10. Immediately press a key to interrupt the system startup

    You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiRecorder appliance reboots and you must log in and repeat the execute reboot command.

    If you successfully interrupt the startup process, the following messages appears:
    ```
    [G]: Get firmware image from TFTP server.
    [F]: Format boot device.
    ```

```
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".

11. If the firmware version requires that you first format the boot device before installing firmware, type F. Format the boot disk before continuing.
12. Type G to get the firmware image from the TFTP server.
    The following message appears:
    ```
    Enter TFTP server address [192.168.1.168]:
    ```
13. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    ```
    Enter local address [192.168.1.188]:
    ```
14. Type a temporary IP address that can be used by the FortiRecorder appliance to connect to the TFTP server.
    The following message appears:
    ```
    Enter firmware image file name [image.out]:
    ```
15. Type the file name of the firmware image and press Enter.
    The FortiRecorder appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:
    ```
    Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
    ```
16. Type D.
    The FortiRecorder appliance downloads the firmware image file from the TFTP server. The FortiRecorder appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.

    The FortiRecorder appliance reverts the configuration to default values for that version of the firmware.
17. To verify that the firmware was successfully installed, log in to the CLI and type:
    ```
    get system status
    ```
    The firmware version number is displayed.
18. Either reconfigure the FortiRecorder appliance or restore the configuration file. See “Regular backups”.

If you are downgrading the firmware to a previous version, and the settings are not fully backwards compatible, the FortiRecorder appliance may either remove incompatible settings, or use the feature’s default values for that version of the firmware. You may need to reconfigure some settings.

Appendices

The following chapter contains some extra information:

- Port numbers
- Maximum values

Port Numbers

Communications between the FortiRecorder appliance, cameras, and your computer require that any routers and firewalls between them permit specific protocols and port numbers.

The following tables list the default port assignments used by FortiRecorder. Many are configurable. See each feature's section in this document.

Port Number	Protocol	Purpose
N/A	ICMP	execute ping and execute traceroute.
N/A	ARP	MAC address resolution.
25	TCP	SMTP for alert email and snapshot notifications.
53	UDP	DNS queries.
69	UDP	TFTP for backups, restoration, and firmware updates. See commands such as execute backup or execute restore.
80	HTTP	Sending network settings and recording signals to cameras.
123	UDP	NTP synchronization.
443	HTTPS	Sending network settings and other configurations to cameras
514	UDP	Syslog.
554, 8554	TCP/UDP	Controlling video recording (RTSP).
5353	UDP	(mDNS, UPnP, ONVIF) queries for camera discovery. Multicast to 224.0.0.251.

Default ports used by FortiRecorder for incoming traffic (listening):

Port Number	Protocol	Purpose
N/A	ICMP	ping and traceroute responses.
N/A	ARP	MAC address resolution responses.

Port Number	Protocol	Purpose
21	TCP	FTP for receiving motion detection clips from cameras. Currently, this is not configurable.
22	TCP	SSH administrative CLI access.
23	TCP	Telnet administrative CLI access.
80	TCP	HTTP administrative web UI access.
443	TCP	HTTPS administrative web UI access. Only occurs if the destination address is a network interface's IP address.
Dynamic	UDP	Receiving video from cameras (RTP).
554	TCP	Live video feeds (RTP) in the HTTP/HTTPS administrative web UI.
8550	TCP	FortiRecorder Central access.

Maximum Values

This table shows the maximum number of configuration objects or limits that vary by them, and are not a guarantee of performance. For values such as hardware specifications that do not vary by software version or configuration, see your model's QuickStart Guide.

	FortiRecorder 100D	FortiRecorder 200D/400D	FortiRecorder VM
Camera connected	16	64	UP to 102 Controlled by license
Routes	250	250	250
Administrator accounts	50	50	50
System interface	10	10	10
Routes	250	250	250
LDAP profiles	20	20	20
Schedules	256	256	256
Video profiles	256	256	256
Camera profiles	256	256	256
Camera groups	256	256	256
Camera notifications	256	256	256
DHCP servers	256	256	256

	FortiRecorder 100D	FortiRecorder 200D/400D	FortiRecorder VM
PKI users	100	100	100
CA certificates	256	256	256
Remote certificates	256	256	256
Local certificates	256	256	256
SNMP communities	16	16	16
SNMP community hosts	16	16	16
SNMP users	16	16	16
SNMP user hosts	16	16	16
Remote log servers	3	3	3
Motion detection windows	3	3	3
Privacy mask windows	3	3	3

www.fortinet.com

Copyright© 2025 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 Chief Legal Officer, 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.