



FortiRecorder™ 2.4.1
Administration Guide



FortiRecorder 2.4.1 Administration Guide

July 20, 2016

1st Edition

Copyright © 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training Services	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Key concepts	7
FortiRecorder NVR.....	7
Camera support	7
Deployment scenarios and camera discovery.....	8
Local camera deployments.....	8
Same network deployments	8
Routed network deployments.....	8
Private network vs office network.....	8
Remote camera deployments.....	9
Video clips	9
Performance guidelines	9
NVR performance	9
Number of supported cameras.....	9
General performance factors	10
Variable versus constant bit rate.....	10
Bandwidth per camera or live view.....	10
Storage capacity	11
Client Performance	12
GUI and CLI	13
NVR configuration	14
Connecting to FortiRecorder web UI.....	14
Connecting to FortiRecorder CLI.....	15
Basic NVR configuration.....	17
Setting the “admin” account password.....	17
Configuring the network settings.....	18
Configuring the DHCP server	23
Setting the system time	26
Configuring schedules	28
Setting the sunrise and sunset time.....	29
Advanced/optional NVR configuration	29
Configuring system timeout, ports, and public access	29
About FortiRecorder logical interfaces	30
VLAN subinterfaces.....	30
Redundant interfaces.....	31
Aggregate interfaces	31
Loopback interfaces	31
Configuring FortiRecorder system appearance.....	31
Configuring logging	31
Alert email	34

Camera settings	36
Camera configuration workflow	36
Configuring video profiles	36
Configuring camera profiles	37
Camera groups	39
Camera connection	40
Camera discovery and DHCP service	40
Connecting FortiRecorder to the cameras	41
Configuring cameras	44
User management	53
User types	53
User configuration workflow	53
Configuring user accounts	54
Configuring LDAP authentication	59
Configuring RADIUS authentication	65
Notifications	67
Notification configuration workflow	67
Configuring FortiRecorder to send notification email	67
Configuring FortiRecorder to send SMS messages	69
Configuring cameras to send notifications	70
Video monitoring	72
Watching live video feeds	72
Video and image sharing	73
Watching recorded video clips	76
Reviewing motion detection notifications	78
Video management	80
Local storage	80
Configuring RAID levels	80
Recommended HDD models and capacities	80
Adding a RAID disk	81
Replacing a RAID disk	81
Replacing all RAID disks	82
External storage	83
System monitoring	85
The dashboard	85
SNMP traps & queries	85
Configuring an SNMP community	87
Configuring SNMP v3 users	89
MIB support	90
Logging	91

About logs.....	91
Log types	91
Log severity levels.....	92
Viewing log messages	92
Displaying & sorting log columns & rows.....	94
Downloading log messages.....	95
Deleting log files.....	95
Searching logs	96
Secure connections and certificates.....	98
Supported cipher suites & protocol versions.....	98
Replacing the default certificate for the web UI.....	99
Generating a certificate signing request	102
Uploading & selecting to use a certificate	104
Uploading trusted CAs' certificates	106
Example: Downloading the CA's certificate from Microsoft Windows 2003 Server.....	107
Revoking certificates.....	108
Revoking certificates by OCSP query.....	108
Updating the firmware	110
Installing NVR firmware.....	110
Installing alternate firmware	113
Bootting from the alternate partition	114
Upgrading/downgrading the camera firmware.....	115
Fine-tuning & best practices	117
Hardening security.....	117
Topology	117
Administrator access	118
Operator access.....	119
Patches	119
Improving performance.....	120
Video performance.....	120
System performance.....	120
Logging & alert performance	121
Packet capture performance	121
Regular backups.....	121
Restoring a previous configuration	123
Troubleshooting	124
Solutions by issue type.....	124
Video viewing issues.....	124
Live feed delay	125
Video not being sent to the NVR.....	125
Snapshot notification issues.....	125

Login issues	126
When an administrator account cannot log in from a specific IP	126
Remote authentication query failures	126
Resetting passwords	126
Connectivity issues	126
Checking hardware connections	127
Bringing up network interfaces	127
Examining the ARP table	128
Checking routing	128
Facilitating discovery	132
DHCP issues	132
Unauthorized DHCP clients or DHCP pool exhaustion.....	133
Establishing IP sessions.....	133
Resolving IP address conflicts.....	135
Packet capture	136
Resource issues.....	141
Data storage issues	142
Resetting the configuration.....	142
Restoring firmware (“clean install”).....	143
Questions and answers	146
How to connect cameras to FortiRecorder for the first time	146
Scenario 1: Direct connection.....	146
Scenario 2: Connection with a third party DHCP server.....	149
How to use recorded video clips	150
How to use DIDO terminal connectors on FortiCam MB13 cameras.....	153
Appendix A: Port numbers.....	156
Appendix B: Maximum values	158
Index	160

Key concepts

This chapter defines basic FortiRecorder concepts and terms.

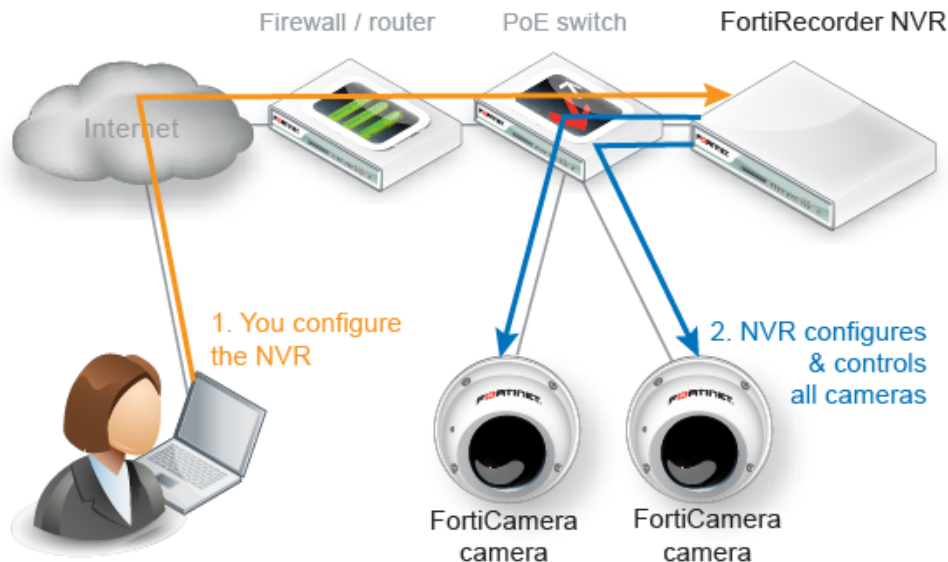
If you are new to FortiRecorder, or new to digital video surveillance systems, this chapter can help you to quickly understand how to use your FortiRecorder system.

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

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



Camera support

The FortiRecorder NVR supports FortiCam series cameras from Fortinet and third-party ONVIF-compliant cameras, although some of the third-party camera features may not be fully supported. Therefore, you may want to configure those features through its built-in camera web interface.

By default, every FortiRecorder or FortiRecorder-VM appliance supports one third-party camera. If you want to connect more than one, you must purchase licenses from Fortinet. For more information, please contact Fortinet or the resellers.

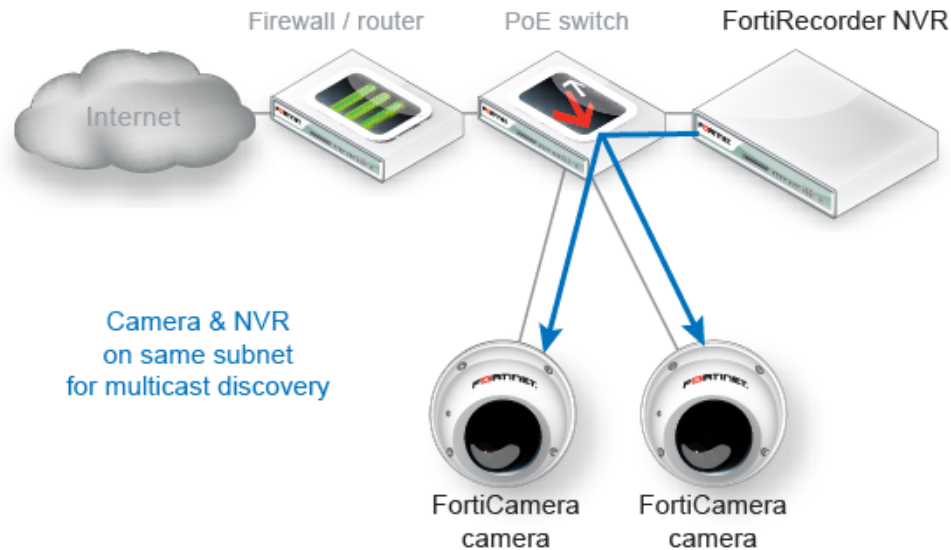
Deployment scenarios and camera discovery

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

Local camera deployments

Local cameras deployments have two specific scenarios:

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



Same network deployments

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

Routed network deployments

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

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

Private network vs office network

You can install the NVR and cameras on your existing network, which saves your efforts and costs. You can also install the system on a dedicated private network only reachable by the

NVR. Although this involves installing a new network and thus increasing the costs, there are some advantages of using a private network:

- the video streams are protected.
- the cameras are protected because they cannot be reached from outside the network.
- easier to determine bandwidth requirements.
- better quality of service since bandwidth is known.

See also

- [Facilitating discovery](#)

Remote camera deployments

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

Video clips

You can use FortiRecorder to:

- Manually record activities
- Continuously record activities by schedules
- Record sudden activities only (motion detection)
- Record audio activities (if the camera supports audio detection)
- Record on triggers from digital input (if the camera support DIDO)
- View live video

Motion detection will record a video clip up to about 40 seconds long each time the camera's sensor detects movement. In contrast, continuous video records for the entire duration of the schedule, regardless of movement.

Performance guidelines

There are two components to consider when looking at FortiRecorder performance – the NVR (FortiRecorder) and the Client computer with FortiRecorder Central or a browser. Overall FortiRecorder performance is a combination of the video input (video compression, image quality level, complexity of the scene, video resolution, frame rate per second, number of cameras) and the video output (to the clients for live views and playback). The performance bottleneck in a FortiCamera deployment will likely be the network bandwidth to and from FortiRecorder and the CPU performance of the computer running the FortiRecorder Central or browser client, which must decode and render the video streams from the NVR. Displaying multiple video streams on the client is very CPU intensive.

NVR performance

Number of supported cameras

The FortiRecorder-100D can support 16 cameras, 200D and 400D can support up to 64 cameras depending on the camera configuration. VM version of FortiRecorder depends on the hardware performance.

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. video compression (constant or variable bit rate mode), image quality level, complexity of the scene, video resolution and frame rate per second.

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. video compression (constant or variable bit rate mode), image quality level, complexity of the scene, video resolution and frame rate per second.

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 or live view

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

Table 1: Bitrate table (H.264 estimate) in Mbps with high quality image (x0.7 = standard quality)

Frames/s	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. Generally do not use 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.

Storage capacity

We will use FortiRecorder 100D, 200D and 400D configuration with different camera parameters to demonstrate the video retention period.

FortiRecorder 100D has a built in 1 TB hard drive and it can connect up to 16 cameras. We configure 16 cameras with 1280 x 720 resolution using 30 FPS with high quality image in continuous recording. Each camera will generate an estimated bandwidth of 2 Mbps. Referring to the FortiRecorder Capacity calculator spreadsheet below, 100D can store approximately 3.2 days of video footage.

Table 2: Capacity Calculator

	Bit rate (Mbps)	HD Capacity (TB)	Cameras (#)	Usage (%)	Time (days)
Input	2	1	16	100	30
Resolve each for all other inputs as specified					
Result	0.2	9.4	1.7	11	3.2

FortiRecorder 200D has 3 TB HD capacity. With the same configuration it can record 16 cameras for 10 days.

FortiRecorder 400D has 6 TB HD capacity. With the same configuration it can record 16 cameras for 19 days.

The above examples use the same configuration for 16 cameras with different hard drive capacity per FortiRecorder model. The table below shows the number of days that one camera can be stored in different configurations.

Table 3: Video retention period in days for one camera

	FortiRecorder 100D with 1 TB HD	FortiRecorder 200D with 3 TB HD	FortiRecorder 200D with 3 TB HD plus 16 TB remote storage	FortiRecorder 400D with 6 TB HD
The same resolution and frame rate with different video quality				
1920x1080@15 FPS high quality video = 3 Mbps	34	102	645	204
1920x1080@15 FPS medium quality video = 2.1 Mbps	49	145	921	291
The same resolution and video quality with different frame rate				
2048x1536@10 FPS high quality video = 3 Mbps	34	102	645	204
2048x1536@30 FPS high quality video = 5 Mbps	20	61	387	122

Use the following guideline for a quick bandwidth consumption calculation:

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

Therefore:

- 1 TB HD can store 1 camera configured to consume 2 Mbps for approximately 50 days.
- 6 TB HD can store 10 cameras configured to consume 2 Mbps each for approximately 30 days.

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).

GUI and CLI

This document only describes how to use the web UI. If you are familiar with the command line interface (CLI), go to *Monitor > System Status > Console* to use the CLI commands.

NVR configuration

To be able to configure the FortiRecorder NVR appliance, you must connect to its management web UI or CLI console. This document mainly describes the web UI usage.

Connecting to FortiRecorder web UI

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

Table 4: 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.**

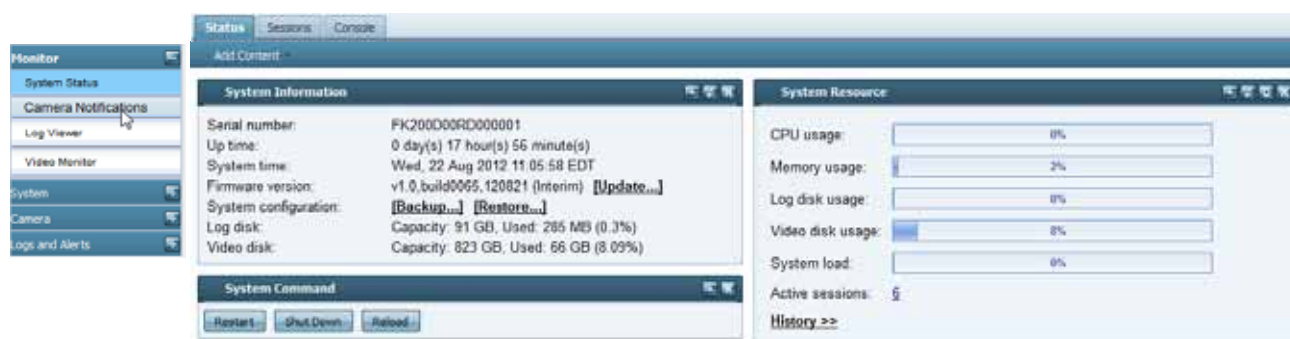
Starting from FortiRecorder version 2.4, HTML5 is supported. On most platforms, QuickTime plugin is not required anymore. For details, see the FortiRecorder version 2.4 release notes.

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 port1.
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.

- In the *Name* field of the login page, type `admin`, then click *Login*. (In its default state, there is no password for this account.)

Login credentials entered are encrypted before they are sent to the FortiRecorder appliance. If your login is successful, the web UI appears.



See also

- Connectivity issues
- Login issues

Connecting to FortiRecorder CLI

For initial configuration, you can access the CLI from your management computer using either of these two ways:

- a local serial console connection
- 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

Table 5: 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 console connection



The following procedure uses Microsoft HyperTerminal. Steps may vary with other terminal 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 port1.
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. Click 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. (In its default state, there is no password for this account.)

Basic NVR configuration

Either to integrate the FortiRecorder NVR into your existing network or to set it up in its dedicated, private network, you must configure the following settings to have the appliance up and running:

- [Setting the “admin” account password](#)
- [Configuring the network settings](#)
- [Configuring the DHCP server](#)
- [Setting the system time](#)

Setting the “admin” account password

The default administrator account, named `admin`, initially has no password.

Unlike other administrator accounts, the `admin` administrator account exists by default and cannot be deleted. This 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. Set a strong password for the `admin` administrator account, and change the password regularly.

To change the `admin` administrator password

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.

See also

- [Login issues](#)

Configuring the network settings

When shipped, each of the FortiRecorder appliance's physical network adapter ports has 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.

Table 6: Default IP addresses and netmasks

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 **Two** 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 **ne** change on that interface because the cameras need to communicate with the NVR and thus need to be aware of the IP address of the NVR.



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

5. Configure these 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” on page 41 .
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.
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” .
PING	Enable to allow: <ul style="list-style-type: none">• ICMP type 8 (ECHO_REQUEST)• 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) and traceroute-related UDP. It does not disable FortiRecorder CLI commands such as <code>execute ping</code> or <code>execute traceroute</code> that send such traffic.
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.
SSH	Enable to allow SSH connections to the CLI through this network interface.

Setting name	Description
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”.
TELNET	<p>Enable to allow Telnet connections to the CLI through this network interface.</p> <p>Caution: Telnet connections are <i>not</i> 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.</p>
FRC-Central	Enable to allow access from FortiRecorder Central.
MTU	<p>Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes.</p> <p>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.</p> <p>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.</p>
Administrative status	<p>Select either:</p> <ul style="list-style-type: none"> • 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. Click *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. Click *New*.
4. Configure these 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 <code>0.0.0.0/0</code> results in a default route, which matches all packets.
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 <i>Destination IP/netmask</i> , 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 <i>must</i> be in the same subnet as a network interface's IP address.

5. Click *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:

```
execute ping <destination_ipv4>
```

to determine if a complete route exists from the FortiRecorder to the host, and

```
execute traceroute <destination_ipv4>
```

to determine the point of connectivity failure.

Also enable *PING* on the FortiRecorder's network interface, then use the equivalent *tracert* or *tracert* 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.

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. Click *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”](#).

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.

See also

- [Connectivity issues](#)

Configuring the DHCP server

If you need the FortiRecorder DHCP service to connect cameras to the NVR, 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 these 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. 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: <ul style="list-style-type: none">• Default — Leave DHCP clients' DNS settings at their default values.• Specify — Configure DHCP clients with the DNS servers that you specify in <i>DNS server 1</i> and <i>DNS server 2</i>.
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 <i>DNS options</i> is set to <i>Specify</i> .
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 <i>DNS options</i> is set to <i>Specify</i> .
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.

5. If you want to fine-tune the behavior, configure these settings:

Setting name	Description
Conflicted IP timeout (Seconds)	<p>Type the maximum amount of time that the DHCP server will wait for an ICMP <code>ECHO</code> (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).</p> <p>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.</p>
Lease time (Seconds)	<p>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).</p> <p>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.</p>
DHCP IP Range	<p>To configure the DHCP lease pool — the range of IP addresses that the DHCP server can assign to its clients — click <i>New</i> 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.</p> <p>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.</p> <p>Tip: The built-in DHCP server can provide IP addresses to the computers on your network too, not just to cameras.</p>

Setting name	Description
DHCP Excluded Range	To configure IPs that should be omitted from the DHCP pool and never given to DHCP clients (such as printers with manually assigned static IP addresses in the middle of your DHCP range), click <i>New</i> .
Reserved IP Address	<p>To bind specific MAC addresses to a specific DHCP lease, guaranteeing that the DHCP server will never assign it to another DHCP client, click <i>New</i>.</p> <p>Caution: Reserved leases cannot prevent misconfigured computers from taking the IP address, causing an IP address conflict, and breaking the FortiRecorder NVR's connection with the camera. See "Resolving IP address conflicts".</p> <p>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.</p>

6. Click *Create*.

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

See also

- [DHCP issues](#)

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.

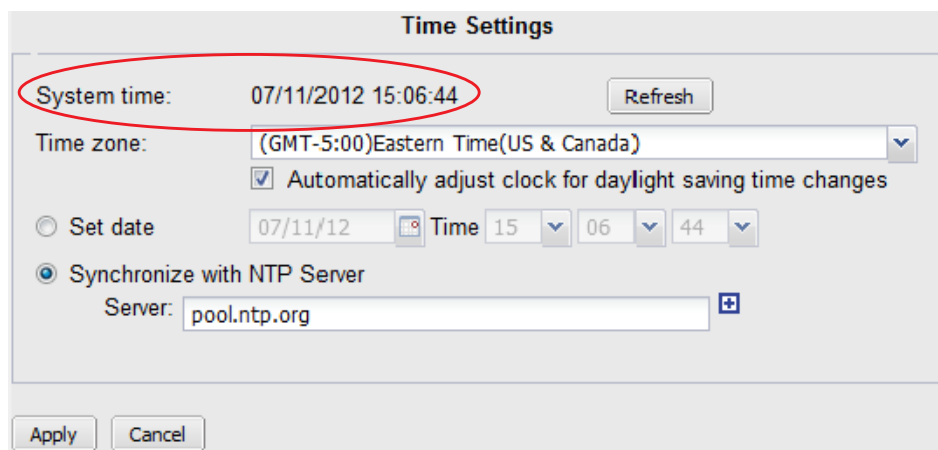
Later, when cameras are added to your surveillance system, your FortiRecorder NVR will synchronize the camera clocks with its own to keep them in agreement.

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. Click *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*.)



The screenshot shows a 'Time Settings' dialog box. At the top, the 'System time' is displayed as '07/11/2012 15:06:44', which is circled in red. To its right is a 'Refresh' button. Below this, the 'Time zone' is set to '(GMT-5:00)Eastern Time(US & Canada)' with a dropdown arrow. A checkbox labeled 'Automatically adjust clock for daylight saving time changes' is checked. There are two radio buttons: 'Set date' (unselected) and 'Synchronize with NTP Server' (selected). The 'Set date' option shows a date of '07/11/12' and a time of '15:06:44'. The 'Synchronize with NTP Server' option shows a server address of 'pool.ntp.org' with a plus icon to its right. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

If the NTP query *fails*, the system clock will continue without adjustment.



NTP on FortiRecorder complies with [RFC 5905](#). If the current system time differs greatly from the actual time, NTP will adjust the clock *slowly* to avoid incongruous jumps in log message timestamps and other time-dependent features. If you want the time to be corrected *immediately*, set the time zone and time manually first, then switch to NTP.

If FortiRecorder's time was 3 hours late, for example, and NTP fails, the time will still be exactly 3 hours late. Verify your DNS server IPs, your NTP server IP or name, routing, and that your firewalls or routers do not block or proxy UDP port 123.



NTP queries may fail until you have configured gateway and DNS settings. See "[Configuring the network settings](#)".

See also

- [Connectivity issues](#)

Configuring schedules

Schedules are used in several places:

- When configuring a user under *System > Administrator > User Profile*, schedules are used to specify when the users can access the camera. For details, see [“Configuring user accounts” on page 54](#).

Note: For user access, schedule gaps are allowed. If not scheduled, then access is denied. Schedule overlaps are allowed. And one-time schedules take precedence over recurring schedules.

- When configuring camera video settings under *Camera > Configuration > Camera Profile*, schedules are used to specify when to use low or high quality video. For details, see [“Configuring camera profiles” on page 37](#).

Note: For video quality schedules, gaps and overlaps are not allowed. And one-time schedules take precedence over recurring schedules.

- When configuring camera recording settings under *Camera > Configuration > Camera Profile*, schedules are used to specify when to trigger the different types of recording. For details, see [“Configuring camera profiles” on page 37](#).

Note: For camera recording schedules, gaps and overlaps are allowed. And one-time schedules take precedence over recurring schedules.

- When configuring camera settings under *Camera > Configuration > Camera*, schedules are used to specify when to use different camera settings, such as DNR level, brightness, contrast, saturation, and sharpness. For details, see [“Configuring cameras” on page 44](#).

Note: For camera setting schedules, gaps are allowed. But overlaps are not allowed. And one-time schedules take precedence over recurring schedules.

- When configuring camera notifications under *Camera > Notification > Camera Notification*, schedules are used to control when to send out notifications. For details, see [“Configuring cameras to send notifications” on page 70](#).

Note: 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.

To configure schedules

1. Go to *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: <ul style="list-style-type: none">• Recurring: the schedule happens at specified times on selected days.• One-time: the schedule happens only on a specific date and time.

Setting name	Description
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.
Start time/End time	<p>Select the start and end time for the recurring recording or the start and end date for the one-time recording.</p> <p>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" on page 29.</p> <p>When using sunrise and sunset time, you can a plus or minus two hour offset to compensate for lighting conditions specific locations.</p>

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. Click *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.

Advanced/optional NVR 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 NVR— 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 NVR.

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 NVR'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 <code>www.example.com</code> . 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 NVR'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 NVR'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.

About FortiRecorder logical interfaces

In addition to the physical interfaces, you can create the following types of logical interfaces on FortiRecorder:

- [VLAN subinterfaces](#)
- [Redundant interfaces](#)
- [Aggregate interfaces](#)
- [Loopback interfaces](#)

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.

Configuring FortiRecorder system appearance

To customize the logo and product name appearing on the FortiRecorder web UI, go to *System > Customization > Appearance*.

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 Viewer > Event* for the NVR log messages or go to *Monitor > Log Viewer > Event* for the camera log messages.

To configure logging

1. Go to either *Logs and Alerts > Log Setting > Local Log Settings* or *Log > Log Setting > Remote Log Settings* (depending on whether you want logs to be stored on FortiRecorder's hard drive, or remotely, on a Syslog server or FortiAnalyzer).
2. If configuring local log storage, configure the following settings:

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 <i>Information</i> or <i>Notification</i> 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: <ul style="list-style-type: none">• 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 NVR 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.
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 <i>Information</i> or <i>Notification</i> 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 NVR events and camera events you want to log.

- 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 NVR 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 “[NVR 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 *Monitor > System Status > Console* and enter the command:

```
execute traceroute <syslog_ipv4>
```

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

See also

- [Connectivity issues](#)
- [Data storage issues](#)

Alert email

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 and Alerts > Alert Email > Configuration*.
2. Click *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. Click *Create*.
5. Go to *Logs and Alerts > Alert Email > Categories*. Mark the check boxes of all appliance events that you want to trigger an alert email to be sent, such as:

Setting name	Description
Critical 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	Enable to notify when a defined camera configuration has been enabled or disabled, or if there are problems with the camera. (The FortiRecorder NVR will not control or record video from a camera that is not enabled in its list of known, configured devices. See “Camera settings” .)
Camera communications	Enable to notify when there has been a network error during communications between the NVR and camera. See also “Connectivity issues” .
Camera recording	Enable to notify when an issue prevents a camera from recording. See also “Video viewing issues” and “Connectivity issues” .
Camera disk	Enable to notify when the disk partition that stores video data is full. See also “Data storage issues” .

6. Click *Apply*.

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.

Camera configuration workflow

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 NVR. FortiRecorder NVR 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 NVR. 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. Click *New*.

3. Configure the following, then click *Create*.

Setting name	Description
Name	Type a name (such as <code>live-stream1</code>) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Resolution	Select the amount of detail (the number of pixels) in the image from the dropdown 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. See “Video performance” .
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.
Bit rate mode	Select the bit rate. <ul style="list-style-type: none">• Variable — Automatically adjust the stream to the minimum bit rate required by the current video frames while maintaining video quality.• Fixed — Manually specify a constant bit rate in <i>Bit rate</i>. Specifying a bit rate that is too low may result in poor quality. Specifying a bit rate that is too high may needlessly consume extra bandwidth.
Bit rate	Type the bit rate that will be used. This setting appears and is applicable only if <i>Bit rate mode</i> is <i>Fixed</i> .
Quality	Select the degree of compression. Greater compression reduces required network bandwidth but causes greater CPU usage.

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. Click *New*.

3. Configure the following, then click *Create*.

Setting name	Description
Name	Type a name (such as <code>camera-settings1</code>) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Video	<p>Select the Recording stream profile used to determine the video quality of the recorded video.</p> <p>Select the Viewing stream profile used to determine the video quality of the streamed video when viewing.</p> <p>Click <i>Add schedule</i> 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.</p> <p>Note: The higher the quality, the more bandwidth the stream will use.</p>
Recording	<p>Select the Recording type that will instruct the camera when to begin filming.</p> <ul style="list-style-type: none">• 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. For details about how to use digital input and output (DIDO), see “Configuring cameras” on page 44. 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. For details, see “Configuring cameras” on page 44.• PIR detection: PIR based motion detection senses the movement of people, animals, and other objects that produce heat energy. <p>Note: Some recording types may not be available for your camera.</p> <p>If you want to use different recording types at different times, click <i>Add schedule</i> to specify them. For example, you could instruct the camera to start recording for motion detection during the day and PIR detection at night.</p>

Setting name	Description
Storage Options	<p>You can select the storage options of both continuous recordings and detection recordings.</p> <ul style="list-style-type: none"> • Keep — Retain video until all available disk space is consumed • Delete — Remove video when it exceeds a maximum age. • Move — Relocate video to external storage when it exceeds a maximum age. This option appears if you have configured network storage (see “External storage”). <p>If you choose to delete old video, also configure the maximum amount of time to keep video recording files from this camera. Files whose start time is older than this age will be deleted in order to free disk space for new video recordings.</p> <p>Continuous recordings will be stored on the hard disk as multiple video files. In that case, the oldest part of the recording will be deleted first.</p>
Compression Options	<p>Select whether or not FortiRecorder compresses continuous recordings.</p> <p>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.</p> <p>Note: Selecting Compress will save storage space at the cost of video quality.</p>

Camera groups

After you have configured the cameras, you can group them to facilitate the camera management. When you add administrators/operators/viewers later on, you can specify the camera group they can access, instead of single cameras. For details, see “[User management](#)”.

To configure camera groups, go to *Camera > Configuration > Camera Group*.

Camera connection

After you have configured the NVR and camera settings, you can install and connect cameras to the FortiRecorder NVR. For information about how to physically install a camera, see the camera's QuickStart Guide.

Camera discovery and DHCP service

In order for the FortiRecorder NVR to be able to discover cameras and receive video, cameras **Two** first get their IP addresses and other network settings from either the FortiRecorder built-in DHCP server or any other third-party DHCP server on your network.

- **FortiRecorder DHCP server** — If you do not have a DHCP server in your network, or you are installing the FortiRecorder and the cameras in their dedicated network, you must configure the built-in DHCP server on the FortiRecorder. For example, if you configured the built-in DHCP server to provide DHCP service through port2, and port2 is connected to a PoE switch, you would connect the cameras to the PoE switch. The switch would supply power to the cameras, and through it, the cameras would be able to access the DHCP server. For information about FortiRecorder DHCP server configuration, see [“Configuring the DHCP server” on page 23](#).
- **Other DHCP server** — If you already have a DHCP server in your network and the FortiRecorder and cameras will be installed in the existing network, the cameras will get their IP addresses from the DHCP server after you connect and power up the cameras.



If you connect a camera to FortiRecorder before any DHCP server is configured, the camera will assign itself a default IP address, which might not be working in your subnet. In this case, you must reboot the camera after you have configured a DHCP server, so that the camera can get network settings from the DHCP server.

Since you can configure the camera to use a static IP address, you only need the DHCP server for the initial camera discovery.

Later, after each camera has network settings from DHCP, you can either:

- **Continue using DHCP**— Leave the cameras plugged into their current network location. Configure the DHCP server to reserve a specific IP lease for each camera. This will mimic

configuring the cameras with a static IP address, yet will provide the advantage that IP addresses remain centrally managed.



If you continue to let your cameras use DHCP, you **should** configure *Reserved IP Address* (or, on a third-party DHCP server, the equivalent setting). Failure to do this may appear to work initially, but eventually could periodically, temporarily interrupt connectivity with the NVR, resulting in lost video.

This can happen if either the DHCP pool is too small for the number of cameras, or if a misconfigured computer accidentally takes a camera's DHCP lease: the DHCP server will ultimately be forced to assign the camera's IP address to a different client. If this happens, when the camera next requests a lease, it will receive a new, different IP address, and the NVR will **not** be notified.

Connectivity interruptions are usually self-correcting: within a few minutes, the FortiRecorder NVR should detect the camera's IP address change. To restore connectivity manually, either manually update the camera's definition on the NVR to reflect the new IP, or discover the camera again.

- **Switch the camera to a static IP** — Use the FortiRecorder NVR to configure the camera with a static IP address. This removes the requirement of your cameras to remain within reach of the DHCP server, which provides 2 advantages:
 - You can disable DHCP if not otherwise required (recommended for better security).
 - You can move the cameras to a remote location on your network that would not ordinarily be reachable by your DHCP server.

Connecting FortiRecorder to the cameras

After you configure the DHCP server (you do not have to if you already have one), you can connect and configure the cameras.

Once you connect the cameras to the NVR, the NVR can automatically discover the cameras. Then you can configure the discovered cameras.



Requirements

- On your computer, the Apple QuickTime 7.1 or greater plug-in installed for your web browsers
- At the camera's location on the network, power over Ethernet (PoE)
This could be provided by a FortiSwitch-80-PoE or perhaps your ISP's cable modem.

To connect FortiRecorder to your cameras

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 **ne** 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 click *New* to create a new DHCP server on port1.

The screenshot shows the 'Network Interface Setting' and 'Auto Config Setting' sections of the FortiRecorder web UI. The 'Network Interface Setting' section includes fields for ID (0), Enable DHCP server (checked), Interface (port1), Gateway (192.168.1.1), DNS options (Default), DNS server 1 (0.0.0.0), DNS server 2 (0.0.0.0), Domain, and Netmask (255.255.255.0). The 'Auto Config Setting' section includes Lease time (Seconds) (604800) and Conflicted IP timeout (Seconds) (1800). The 'DHCP IP Range' section shows a table with Start (192.168.1.100) and End (192.168.1.200) columns. The 'DHCP Excluded IP Range' and 'Reserved IP Address' sections are collapsed. The 'Create' and 'Cancel' buttons are at the bottom.

Annotations:

- Make sure to enable DHCP server (pointing to the checked 'Enable DHCP server' checkbox)
- Make sure to select port1 (pointing to the 'port1' dropdown menu)

6. Go to *System > Network > Interface*. Select port1 and click *Edit*.

Make sure to enable it

Edit Interface

Interface name: port1 (50:e5:49:e8:db:3c)

Discover cameras on this port

Addressing Mode

Manual

IP/Netmask: /

IPv6/Netmask: /

DHCP

Retrieve default gateway and DNS from server

Connect to server

Access

HTTPS PING HTTP FRC-Central

SSH SNMP TELNET

MTU

Override default MTU value (1500)

(bytes)

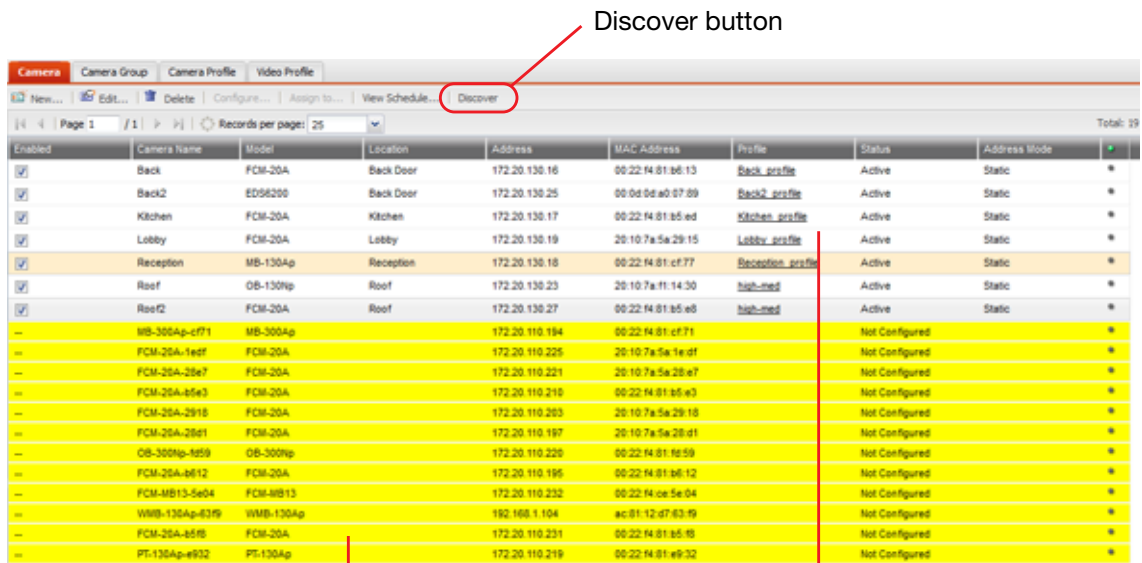
Administrative status Up Down

7. Make sure *Discover cameras on this port* is enabled.
8. 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.

- Go to *Camera > Configuration > Camera*, and click *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*.



Yellow: discovered but not configured cameras

Configured cameras

- Double click on the discovered camera to configure the camera settings. For details, see “Configuring cameras” on page 44.

- Go to *Monitor > Video Monitor* to view the live feed from the camera.

Configuring cameras

After you have connected the cameras to FortiRecorder, you can start to configure the discovered cameras. Because most of the camera information has been retrieved from the camera, you do not have to change the settings. But if you are adding a remote camera or adding a new camera before connecting it to FortiRecorder, you must specify all the camera settings.

- Go to *Camera > Configuration > Camera*. For each discovered camera, click its row to select it, click *Configure*, then configure these settings:

Setting name	Description
Enable	Mark this check box to enable the FortiRecorder NVR to communicate with this IP address. Communications are required to trigger scheduled recordings and other camera commands.
Name	Type a name (such as <code>front-door1</code>) 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.

Setting name	Description
Vendor/Camera	<p>FortiRecorder supports Fortinet cameras (FortiCam series) and third-party, ONVIF-compliant cameras.</p> <p>If you are configuring a discovered camera, most of the camera information has been retrieved and displayed. You can also click the <i>Camera detail</i> button to refresh the camera information.</p> <p>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.</p>
Model	Select the name of the camera model, such as <i>FCM-20A</i> for a FortiCam 20A.
Address mode	<p>Select either:</p> <ul style="list-style-type: none"> • 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 <i>WiFi</i> 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 NVR will <i>not</i> connect to the camera's DHCP address. Instead, the NVR will connect through the static <i>external</i>, usually public network IP address and port numbers (called a virtual IP or VIP on FortiGate firewalls) specified in <i>Address</i>, (<i>HTTPS</i>) <i>Port</i>, and (<i>RTSP</i>) <i>Port</i>. 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 NVR — are also affected: the camera will use the public IP setting as its destination (see “Configuring system timeout, ports, and public access”), <i>not</i> the private network address of port1, for example, which it would use if you select <i>DHCP</i> or <i>Static</i>. Tip: Use this option if the camera is not located on the same private network as the FortiRecorder NVR due to <i>NAT/ port forwarding</i>, especially if the camera and NVR 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.
(HTTPS) Port	<p>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.</p> <p>This setting is available only when <i>Address mode</i> is set to <i>VIP</i>.</p>

Setting name	Description
(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 <i>Address mode</i> is set to <i>VIP</i> .
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 NVR.
Profile	Select the camera profile that indicates the recording schedule, video quality, and other settings that will be used by this camera (see “ Connecting FortiRecorder to the cameras ”). Or click <i>New</i> 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 NVR will **not** connect to the camera.

This can break communications between them: if you reconfigure the IP while the camera is disabled, your FortiRecorder NVR 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.

2. 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.
3. Depending on the camera model you are configuring, different tabs appear.

4. If the address mode is wired or wireless, under the network tab, configure the following:

Setting name	Description
Wired settings	<p>Select <i>DHCP</i> if you want the camera to continue using DHCP to dynamically determine its IP address. The FortiRecorder NVR will attempt to keep track of any DHCP-related IP address changes automatically using periodic mDNS probes. This requires that the camera remain on the same subnet as the NVR.</p> <p>Select <i>Static</i> to re-configure the camera with a static private network IP address that you specify in <i>Address</i>. It will no longer use DHCP. This option requires that the camera and NVR not be separated by NAT.</p> <p>Caution: It is strongly recommended to either:</p> <ul style="list-style-type: none"> • configure your cameras with a static IP, or • configure your DHCP server with lease reservations (see “Configuring the DHCP server”). <p>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.</p>
Wireless settings	<p>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.</p>

5. 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.

6. 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.
LED	Either off or auto. Auto means to turn on the LED lights when the infra red mode is turned on.
Enable threshold	Enter the light level when infra red mode should turn on.

Setting name	Description
Disable threshold	Enter the light level when infra red 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.
Current light level	Display the current light level that the camera detects.
Refresh	Click to get instant light level reading.

- Configure the video and audio settings on the *Video/Audio* tab. Available settings vary on different camera models. If the setting is greyed out, the setting is not supported on the selected model.

Setting name	Description
Horizontal flip	Enable if the camera is positioned looking at a mirror or on a ceiling, and the preview image appears to be reversed left to right.
Vertical flip	Enable if the camera is positioned on a ceiling, and the preview image appears to be upside down.
WDR	If the camera supports WDR (wide dynamic range), enable it if there is intense backlight in the camera view.
Environment	Select if the camera is installed indoor or outdoor.
View angle	Select the view angle if the camera supports it.
Get feed/Stop feed	Click to view or stop the live video feed.
(Other settings)	Configure the brightness, contrast, saturation, sharpness, zoom level, and audio input level as required.

- 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 reasons, 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.
- All FortiCam cameras are capable of detecting motion. Some camera models also support audio surveillance and digital input and output (DIDO).

By default, while using motion detection, cameras will be triggered to record if **any** motion occurs within their entire field of vision. If some parts of the view, such as a fan, traffic, or strobe light, would inadvertently trigger motion detection, in the *Motion detection windows* area on the *Detection* tab, click the plus sign. A rectangle with a thick, white border will appear over the preview image, indicating the area that will be monitored for movement. To resize it to your intended area, click and drag the edges of the rectangle. To move it, hold

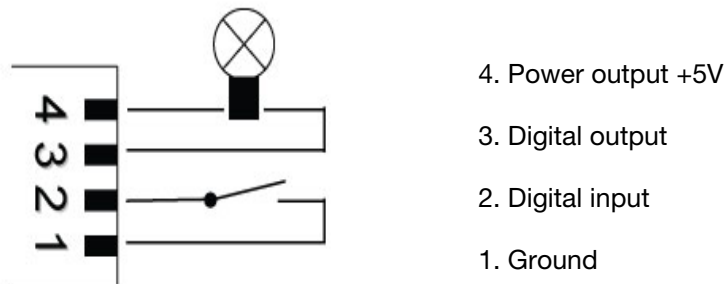
down the Shift key while you click and drag it. To add another motion detection area, click the plus sign again.

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.

Setting name	Description
PIR Sensitivity	
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.

DIDO connection diagram on FortiCam MB13



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.

10. On the *Miscellaneous* tab, configure the following settings:

Setting name	Description
Privacy button	<p>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.</p> <p>To enable the functionality of the privacy button on the camera, select the <i>Privacy button</i> checkbox.</p> <p>To disable the functionality of the privacy button on the camera, clear the <i>Privacy button</i> checkbox.</p>
Status LEDs	<p>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 <i>Status LEDs</i> checkbox.</p>

11. Click *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*)
- NTP settings (if you configured them for FortiRecorder during "Setting the system time")

Afterwards, 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.

12. To confirm that FortiRecorder can receive video from the camera at its new IP address, go to *Monitor > Video Monitor*.

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 *Monitor > System Status > 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 (see "Appendix A: Port numbers")
- 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.



To receive notifications if the camera's connection with the FortiRecorder NVR is interrupted, see "Alert email".

13. If desired, you can specify different camera settings, such as brightness and contrast, for the camera to use as different times. For details, see [“Configuring schedules” on page 28](#).

See also

- [Watching live video feeds](#)
- [Connectivity issues](#)

User management

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.

To prevent accidental changes to the configuration, it's best if only network administrators — and if possible, only a single person — use the `admin` account. You can use the `admin` administrator account to configure more accounts for other people.

User types

To serve different purposes, you can configure the following three user types:

- **Administrator** — Suited to network technicians or administrators. Depending on the access privileges, the administrator account can have full or partial access to configure all FortiRecorder NVR network and camera settings, create accounts, receive all notifications via email, and view live video feeds and previous recordings from all cameras.
- **Operator** — Suited to an office manager or perhaps security guard. The account can view assigned live camera feeds and associated previous recordings, including camera-based notifications via email ("snapshot notifications"). It can change its own password, but otherwise **cannot** change the FortiRecorder NVR or camera configuration, reducing risk of accidental misconfiguration.
- **Viewer** — Suited to a security guard. Only assigned live camera feeds. It **cannot** view previous recordings, and therefore cannot receive snapshot notifications. It can change its own password, but otherwise cannot change the FortiRecorder NVR or camera configuration.



Multiple administrators should **not** be logged in simultaneously. If configuring the same item at the same time, the administrators could inadvertently overwrite each others' changes.

For user authentication, FortiRecorder supports local user authentication, LDAP authentication and RADIUS authentication. For details, see "[Configuring LDAP authentication](#)" and "[Configuring RADIUS authentication](#)".

User configuration workflow

Administrators user type can access all the cameras all the time. For operator and viewer user types, you can specify when and which cameras the users can access. To achieve this, you must configure access schedules and user profiles first.

1. Go to *System > Administrator > Access Profile* to configure the access privileges for the administrator accounts. The access profile will be used in the administrator settings.
2. Go to *System > Administrator > User Profile* to configure which camera group the user is allowed to access. **Configure the user's access privileges**. Also configure when the user is allowed to access video feeds. **Configure the user's access schedule**.

profiles will be used in the user settings you need to configure in the next step. For details about configuring camera groups, see “[Camera groups](#)”.

3. Go to *System > Administrator > Administrator* to configure all other user settings.

Configuring user accounts

After you configure access profiles and user profiles, you can start to add user accounts.

To configure an account

1. Go to *System > Administrator > Administrator*.

To access this part of the web UI, your account's *Type* must be *Administrator*.

2. Click *New*.

A dialog appears.

3. Configure these settings:

Setting name	Description
Username	Type the name of the account, such as <code>IT</code> , 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 <i>Authentication</i> , your external authentication server may require that you enter both the user name and the domain part, such as <code>guard@example.com</code> .
Display name	Type a name for the recipient, such as <code>FortiRecorder admin</code> , as you want it to appear in snapshot notifications, if any, sent by FortiRecorder.
Email address	Type the person's email address or an email alias, such as <code>all-admins@example.com</code> , that will receive snapshot notifications, if any, sent by FortiRecorder (see “ Configuring FortiRecorder to send notification email ”). If you do not know the email address and cannot provide it, don't worry. The person still will be able to view camera-related notifications whenever he or she logs in to the FortiRecorder NVR. Additionally, the person can configure his or her own email address later, when he or she logs in. Note: This is not used by accounts whose <i>Type</i> is <i>Viewer</i> ; they cannot receive snapshot notifications.
Message method	Select either Email or SMS to send notification messages to this user. For detailed about notifications, see “ Notifications ”.

Setting name	Description
Password	<p>Type a password for the account.</p> <p>This field is available only when <i>Authentication</i> is <i>Local</i> or <i>RADIUS + Local</i>.</p> <p>Tip: For improved security, the password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as Microsoft's password strength meter.</p>
Confirm Password	<p>Re-enter the password to confirm its spelling.</p> <p>This field is available only when <i>Authentication</i> is <i>Local</i> or <i>RADIUS + Local</i>.</p>
Trusted hosts	<p>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.</p> <p>To allow login attempts from any IP address, enter 0.0.0.0/0.</p> <p>To allow logins only from a single computer, enter its IP address and a 32-bit netmask, such as:</p> <p>172.168.1.50/32</p> <p>Caution: If you configure trusted hosts, do so for <i>all</i> 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 <i>one</i> 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 <i>after</i> a login attempt has been received in order to check that user name's trusted hosts list.</p> <p>Tip: If you allow login from the Internet, set a longer and more complex <i>Password</i>, and enable only secure administrative access protocols (<i>HTTPS</i> and <i>SSH</i>) to minimize the security risk. For information on administrative access protocols, see "NVR configuration".</p> <p>Tip: For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which only this administrator will log in.</p>

Setting name	Description
Type	<p>Select either:</p> <ul style="list-style-type: none"> • Administrator — Suited to network technicians or administrators. The account has full access to configure all FortiRecorder NVR network and camera settings, create accounts, receive all notifications via email, and view live video feeds and previous recordings from all cameras. • Operator — Suited to an office manager or perhaps security guard. The account can view assigned live camera feeds and associated previous recordings, including camera-based notifications via email (“snapshot notifications”). It can change its own password, but otherwise cannot change the FortiRecorder NVR or camera configuration, reducing risk of accidental misconfiguration. • Viewer — Suited to a security guard. Only assigned live camera feeds. It cannot view previous recordings, and therefore cannot receive snapshot notifications. It can change its own password, but otherwise cannot change the FortiRecorder NVR or camera configuration. <p>This option does not appear for the <code>admin</code> administrator account, which by definition is always an administrator.</p>
User profile	<p>With a user profile, you can specify which group of camera video feeds and recordings the account will be able to access. You can also use schedules to control when the user is allowed to access the video. For details, see “Configuring schedules” on page 28.</p> <p>To configure a user profile, click <i>New</i> or go to <i>System > Administrator > User Profile</i>.</p> <p><i>If no user profile is specified, then the user can access all of the cameras all the time.</i></p>

Setting name	Description
Access profile	<p>If you are creating an administrator account, you can specify an access profile to grant the account certain access privileges.</p> <p>To configure an access profile, go to <i>System > Administrator > Access Profile</i>.</p> <p>The administrator account can have read-only, read-write, or no access rights to the following administrative categories:</p> <ul style="list-style-type: none"> • System Access — Controls settings critical to network accessibility of FortiRecorder <ul style="list-style-type: none"> • System Status page • GUI console • Network • Administrator • Authentication and certificates • System — Controls other system settings <ul style="list-style-type: none"> • Time • Remote storage • Log settings • Alert email • Camera Config — Controls camera installation and configuration • Camera View — Monitor page with video, timeline and camera control • Other — Everything else
Authentication	<p>Select one of:</p> <ul style="list-style-type: none"> • Local — Authenticate using an account whose name, password, and other settings are stored locally, in the FortiRecorder NVR's configuration. • RADIUS — Authenticate by querying the remote RADIUS server that stores the account's name and password. Also configure <i>RADIUS profile</i> and <i>Check permission attribute on RADIUS server</i>. • 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 <i>RADIUS profile</i> and <i>Check permission attribute on RADIUS server</i>. • LDAP — Authenticate by querying a remote LDAP server that stores the account's name and password. Also configure <i>LDAP profile</i>.

Setting name	Description
RADIUS profile	<p>Select a RADIUS authentication profile that defines the RADIUS connection settings. See “To configure a RADIUS query”.</p> <p>This field appears only when <i>Authentication</i> is <i>RADIUS</i> or <i>RADIUS+Local</i>.</p> <p>Caution: Secure your authentication server and, if possible, all query traffic to it. Compromise of the authentication server could allow attackers to gain administrative access to your FortiRecorder appliance.</p>
Check permission attribute on RADIUS server	<p>Enable to let the RADIUS server override <i>Type</i> when it replies to authentication queries, so that the RADIUS server can specify the account’s permissions. Also configure <i>Vendor ID</i> and <i>Subtype ID</i>.</p> <p>This option requires that:</p> <ul style="list-style-type: none"> Your RADIUS server must support vendor-specific attributes (VSAs) similar to RFC 2548. (If your server does not support them, it may reply with an “attribute not supported” error.) Your RADIUS server’s dictionary must have: <ul style="list-style-type: none"> a vendor ID for Fortinet/FortiRecorder an attribute ID for user types (“access profile” names) Each FortiRecorder account on your RADIUS server must have a user type attribute with a value that specifies which <i>Type</i> to apply. e.g. Fortinet-Access-Profile = Administrator or Fortinet-Access-Profile = Operator <p>Some RADIUS servers already include the Fortinet vendor ID and subtype ID in their default dictionaries. In this case, no server-side configuration is necessary. Otherwise, you must configure your server. Methods varies by vendor — FreeRADIUS and Internet Authentication Services for Microsoft Windows 2008 Server, for example, are configured differently. For instructions, consult its documentation. For an example VSA dictionary, see the article FortiGate RADIUS VSA Dictionary.</p> <p>This field appears only when <i>Authentication</i> is <i>RADIUS</i> or <i>RADIUS+Local</i>.</p>
Vendor ID	<p>Type the vendor ID for Fortinet, as it is defined on your RADIUS server, in decimal. On many RADIUS servers, Fortinet’s default vendor ID is 12356.</p> <p>The vendor ID is an ID for the Fortinet client types. It should be present in <i>Access-Request</i> packets from FortiRecorder, telling your RADIUS server which settings are supported by accounts on FortiRecorder. It should also be present when the RADIUS server replies with an <i>Access-Accept</i> packet.</p> <p>The default value is 0.</p>

Setting name	Description
Subtype ID	<p>Type the subtype ID for account permissions as it is defined on your RADIUS server. On many RADIUS servers, Fortinet’s default subtype ID for access profiles is 6.</p> <p>The subtype ID is an ID for the user type (permissions) attribute. It should be, but is not required to be, present in <code>Access-Accept</code> reply packets from your RADIUS server to FortiRecorder.</p> <p>Packets from your RADIUS server should use this attribute’s value to refer to the name of a <i>Type</i> (e.g. <i>Administrator</i>) on FortiRecorder. If the packet does not have this attribute-value pair, FortiRecorder will use whichever permissions you defined locally for the account in <i>Type</i>. If the packet does not contain the attribute-value pair and you have not configured <i>Type</i>, when the person attempts to authenticate, even if successfully authenticated, authorization will be null, and he or she will receive a “permission denied” error message:</p> <pre>you do not have rights to view this page</pre> <p>The default value is 0.</p>
LDAP profile	<p>Select an LDAP authentication profile that defines the connection settings. See “To configure an LDAP query”.</p> <p>Caution: Secure your authentication server and, if possible, all query traffic to it. Compromise of the authentication server could allow attackers to gain administrative access to your FortiRecorder appliance.</p>
Theme	<p>Select this administrator account’s preference for the initial web UI color scheme or click <i>Use Current</i> to choose the theme currently in effect for your own web UI session.</p> <p>The administrator may switch the theme at any time after he or she logs in by clicking <i>Next Theme</i> in the top right corner.</p>

4. Click *Create*.
The account should now be able to log in.

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. Click *New*.
A dialog appears.

3. Configure these settings:

Setting name	Description
Profile name	Type a name (such as <code>LDAP-query</code>) 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 63 .
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.
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 ”).
Allow unauthenticated bind	Enable to perform the query <i>without</i> authenticating. Disable to authenticate when querying. Also configure Bind DN , Bind password , and User Authentication Options . Many LDAP servers require LDAP queries to be authenticated (“bound”) by supplying a bind DN and password to determine the scope of permissions for the directory search. However, if your LDAP server does <i>not</i> require binding, you can enable this option to improve performance.

4. If your directory does *not* use OpenLDAP’s default schema, or if you need to configure a query string, query cache, LDAP protocol version, or how the query will be authenticated

(the bind DN), click the arrows to expand *User Query Options*, *User Authentication Options*, and *Advanced Options*, then configure:

Setting name	Description
Schema	<p>If your LDAP directory's user objects uses one of these common schema style:</p> <ul style="list-style-type: none">• InetOrgPerson• InetLocalMailRecipient• Active Directory• Lotus Domino <p>select the schema style. This automatically configures the query string to match that schema style.</p> <p>Otherwise, select <i>User Defined</i>, then manually configure the query string in <i>LDAP user query</i>.</p>
Base DN	<p>Enter the distinguished name (DN) of the part of the LDAP directory tree within which FortiRecorder will search for user objects, such as <code>ou=People,dc=example,dc=com</code>.</p> <p>User objects should be child nodes of this location.</p>
Bind DN	<p>Enter the bind DN, such as <code>cn=FortiRecorderA,dc=example,dc=com</code>, of an LDAP user account with permissions to query the <i>Base DN</i>.</p> <p>Leave this field blank if you have enabled <i>Allow unauthenticated bind</i>.</p>
Bind password	<p>Enter the password of the <i>Bind DN</i>.</p> <p>Click <i>Browse</i> to locate the LDAP directory from the location that you specified in <i>Base DN</i>, or, if you have not yet entered a <i>Base DN</i>, beginning from the root of the LDAP directory tree.</p> <p>Browsing the LDAP tree can be useful if you need to locate your <i>Base DN</i>, or need to look up attribute names. For example, if the <i>Base DN</i> is unknown, browsing can help you to locate it.</p> <p>Before using, first configure <i>Server name/IP</i>, <i>Use secure connection</i>, <i>Bind DN</i>, <i>Bind password</i>, and , then click <i>Create</i> or <i>OK</i>. These fields provide minimum information required to establish the directory browsing connection.</p>

Setting name	Description
LDAP user query	<p>Enter an LDAP query filter that selects a set of user objects from the LDAP directory.</p> <p>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.</p> <p>For example, if user objects in your directory have two distinguishing characteristics, their <code>objectClass</code> and <code>mail</code> attributes, the query filter might be:</p> <pre>(& (objectClass=inetOrgPerson) (mail=\$m))</pre> <p>where <code>\$m</code> is the FortiRecorder variable for a user's email address.</p> <p>This option is preconfigured and read-only if you have selected from <i>Schema</i> any schema style other than <i>User Defined</i>.</p> <p>For details on query syntax, refer to any standard LDAP query filter reference manual.</p>
Scope	<p>Select which level of depth to query, starting from <i>Base DN</i>.</p> <ul style="list-style-type: none"> • One level — Query only the one level directly below the <i>Base DN</i> in the LDAP directory tree. • Subtree — Query recursively all levels below the <i>Base DN</i> in the LDAP directory tree.
Derefer	<p>Select when, if ever, to dereference attributes whose values are references.</p> <ul style="list-style-type: none"> • Never — Do not dereference. • Always — Always dereference. • Search — Dereference only when searching. • Find — Dereference only when finding the base search object.
User Authentication Options	<p>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.</p> <ul style="list-style-type: none"> • 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 (<code>\$u</code>) to the User Principle Name (UPN, such as <code>example.com</code>). 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 <i>Alternative UPN suffix</i>. 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 prepending a common name to the base DN. Also enter the name of the user objects' common name attribute, such as <code>cn</code> or <code>uid</code> 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 <i>User Query Options</i>.

Setting name	Description
User Type Attribute	Select this option to define the user's type. Valid entries for this field are: admin, operator, and viewer.
User Profile Attribute	Select this option to define the user's profile. The entry for this field must match the profile name configured in FortiRecorder.
Access Profile Attribute	The access profile attribute can only be set if the user is an administrator. Selecting this option will set the administrator user's access profile. The entry for this field must match the name of an access profile configured in FortiRecorder.
Notification Options	Select the "Allow notification attributes" option to enable notifications. FortiRecorder supports the following notifications: <ul style="list-style-type: none"> • 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.

Setting name	Description
Enable cache	<p>Enable to cache LDAP query results.</p> <p>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.</p> <p>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.</p>
TTL	<p>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.</p> <p>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.</p> <p>This option is applicable only if <code>Enable cache</code> is enabled.</p>

5. Click *Create*.
6. To test the query, configure an account where this profile is used (“[To configure an account](#)”), then attempt to authenticate using that account’s credentials.

Alternatively, click the row to select the query, click *Edit*, then click *Test LDAP Query*. From the *Select query type* drop-down list, choose *Authentication*, then complete the *Password* and *Mail address* fields that appear. Click *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.

LDAP Query Test

Select query type: Authentication

Profile name: LDAP-query

Server name/IP: 172.20.120.100

Server port: 389

Use secure connection: None

Query Options

Schema: InetOrgPerson

Base DN: ou=People,dc=example,dc=com

Bind DN: cn=FortiRecorderA,dc=example,dc=com

Auth Options

Search user and try bind DN: Yes

Use LDAP tree node as group: Disable

Use group name with base DN as a group DN: Disable

Password: ••••

Mail address: fortirecorder@example.co

Test
Cancel

Configuring RADIUS authentication

Except for local users, FortiRecorder also support RADIUS user authentication. You will use the RADIUS authentication profiles when you add user accounts.

To configure a RADIUS query

1. Go to *System > Authentication > RADIUS*.
2. Click *New*.
A dialog appears.
3. Configure these settings:

Setting name	Description
Profile name	Type a name (such as <code>RADIUS-query</code>) 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 RADIUS server that will be queried when an account referencing this profile attempts to authenticate.
Server port	Type 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: <ul style="list-style-type: none">• Password Authentication• Challenge Handshake Authentication (CHAP)• Microsoft Challenge Handshake Authentication (CHAP)• Microsoft Challenge Handshake Authentication V2 (CHAP version 2)• Default Authentication Scheme
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 <code>user1@example.com</code>) and not just the user name (such as <code>user1</code>).

4. Click *OK*.

To test the query, select this profile when configuring an account (“[To configure an account](#)”), then attempt to authenticate using that account’s credentials.

See also

- [NVR configuration](#)
- [Connectivity issues](#)
- [Login issues](#)

Notifications

When a significant event happens, such as motion-triggered video recording or the hard disk being full, your FortiRecorder NVR can notify you, either by email or SMS messages.

Notification configuration workflow

To configure the notifications, follow these steps:

1. Configure the SMTP mail server settings so that FortiRecorder can send out notification email. See [“Configuring FortiRecorder to send notification email”](#).
2. Configure the SMS server settings so that FortiRecorder can send out SMS messages. See [“Configuring FortiRecorder to send SMS messages”](#).
3. Configure the camera settings about what, when and to whom the notifications should be sent. See [“Configuring cameras to send notifications”](#).
4. Monitor the record of notification events by going to *Monitor > Camera Notifications > Notification Events*.

Configuring FortiRecorder to send notification email

For FortiRecorder to send email, you must specify an SMTP server to use.

1. Go to *System > Configuration > Mail Server Settings*.

2. Configure these settings:

Setting name	Description
Host name	<p>Type the host name for the appliance. By default, it uses its serial number.</p> <p>The host name can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but ne spaces and special characters.</p> <p>The host name of the FortiRecorder appliance is used in multiple places.</p> <ul style="list-style-type: none">• It is used in the command prompt of the CLI.• It is used as the SNMP system name. For information about SNMP, see “SNMP traps & queries”. <p>The <code>get system status</code> 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.</p> <p>For example, if the host name is FortiRecorder1234567890, the CLI prompt would be:</p> <pre>FortiRecorder123~#</pre>
Mail server name	<p>Type the fully-qualified domain name (FQDN) of your SMTP server, such as <code>mail.example.com</code>.</p> <p>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.</p> <p>Ensure that the DNS settings are configured. See “Configuring the network settings”.</p>
Mail server port	<p>Type the port number on which your email server or SMTP relay listens for connections from clients.</p> <p>The default varies by whether you enable Use SMTPS: disabled, it is port 25; enabled, it is port 465.</p>
Use SMTPS	<p>Enable to initiate SSL- and TLS-secured connections to the email server if it supports SSL/TLS.</p> <p>When disabled, SMTP connections from the FortiRecorder appliance’s built-in email client to the SMTP server will occur as clear text, unencrypted.</p> <p>This option must be enabled to initiate SMTPS-secured connections.</p>

- If the email server requires SMTP authentication (i.e. it uses the SMTP AUTH command), also enable *Authentication Required*, then configure these settings:

Setting name	Description
User name	Type the name of the account, such as <code>jdjoe</code> or <code>fortirecorder@example.com</code> , 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: <ul style="list-style-type: none"> 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.

- If you want to customize the FortiRecorder's sender email address so that, for example, replies are sent to the network administrators rather than the appliance, then configure these settings:

Setting name	Description
Sender display name	Type the display name, such as <code>Surveillance System</code> , that will be displayed in the <i>From</i> field or column by email clients such as Outlook and Thunderbird. Leaving this setting empty will cause FortiRecorder to use the default value, <code>postmaster</code> .
Sender address	Type the sender email address (<i>From:</i>), such as <code>donotreply@example.com</code> , that will appear in the SMTP header. Leaving this setting empty will cause FortiRecorder to use the default value, <code>postmaster@example.com</code> . Unlike the display name, depending on the client and its settings, this may not be visible.

Configuring FortiRecorder to send SMS messages

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

- Go to *System > Configuration > SMS*.
- Configure the following:

Setting name	Description
Service provider	Enter the SMS service provider name.

Setting name	Description
Description	Enter a short description of the provider.
Type	<p>Select an SMS type: either SMTP or HTTP.</p> <p>For SMTP, enter the Email to, Email subject, and Email body information.</p> <p>You can use the following tags when filling the fields:</p> <ul style="list-style-type: none"> • {{: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. <p>For HTTP, enter the following information:</p> <ul style="list-style-type: none"> • HTTP URL: the HTTP or HTTPS URL to contact to send SMS messages, for example, <code>https://myprovider.com/sendsms</code>. • 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 <i>Encrypt</i> 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. <p>For example, if your provider indicates that to send a message the syntax should look like the following:</p> <pre>https://smsserver.com:8080/sendsms?api_id=1234&user=user &to=<phone_number>&text=<message>&password=<passwd ></pre> <p>Then the settings might be:</p> <p>HTTP URL: <code>https://smsserver.com:8080/sendsms</code></p> <p>HTTP Method: Get</p> <p>Parameters:</p> <pre>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)</pre>

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.

1. Go to *Camera > Notification > Camera Notification*.

2. Click *New*.
3. Configure the following setting and then click *Create*.

Setting name	Description
Name	Enter a name for the notification entry.
Description	Optionally enter a descriptive comment.
Enable	Select to enable this notification entry.
Trigger number	Specify how many times the motion event should happen before the notification is sent out.
Trigger period	Specify the period in which these motion events occur.
Message method	Select how the notification should be sent out: either Email or SMS. At least one method should be selected.
Notification Period	Specify when notifications should be sent out. For details, see “Configuring schedules” on page 28 .
Select Camera	Specify which camera’s motion events should be notified.
Select User	Specify which user should be notified.

4. 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 NVR’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 *Monitor > System Status > 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.



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

See also

- [Connectivity issues](#)

Video monitoring

To get the most value out of your FortiRecorder system, use it to monitor your property — not just to analyze after-the-fact. Your FortiRecorder NVR has a variety of monitoring tools for the appliance itself, but administrators can also view the live video feeds from cameras.

You can use the tools in this section to monitor your FortiRecorder NVR and surveillance cameras.

Watching live video feeds

Once the cameras are connected and configured, administrators can use the web UI to view live video feeds from the cameras.

Administrators will use the surveillance system slightly differently than other users (“operators” or “viewers”) such as security guards. Operators and viewers can only watch the live video and do not have the privilege to configure the system settings.

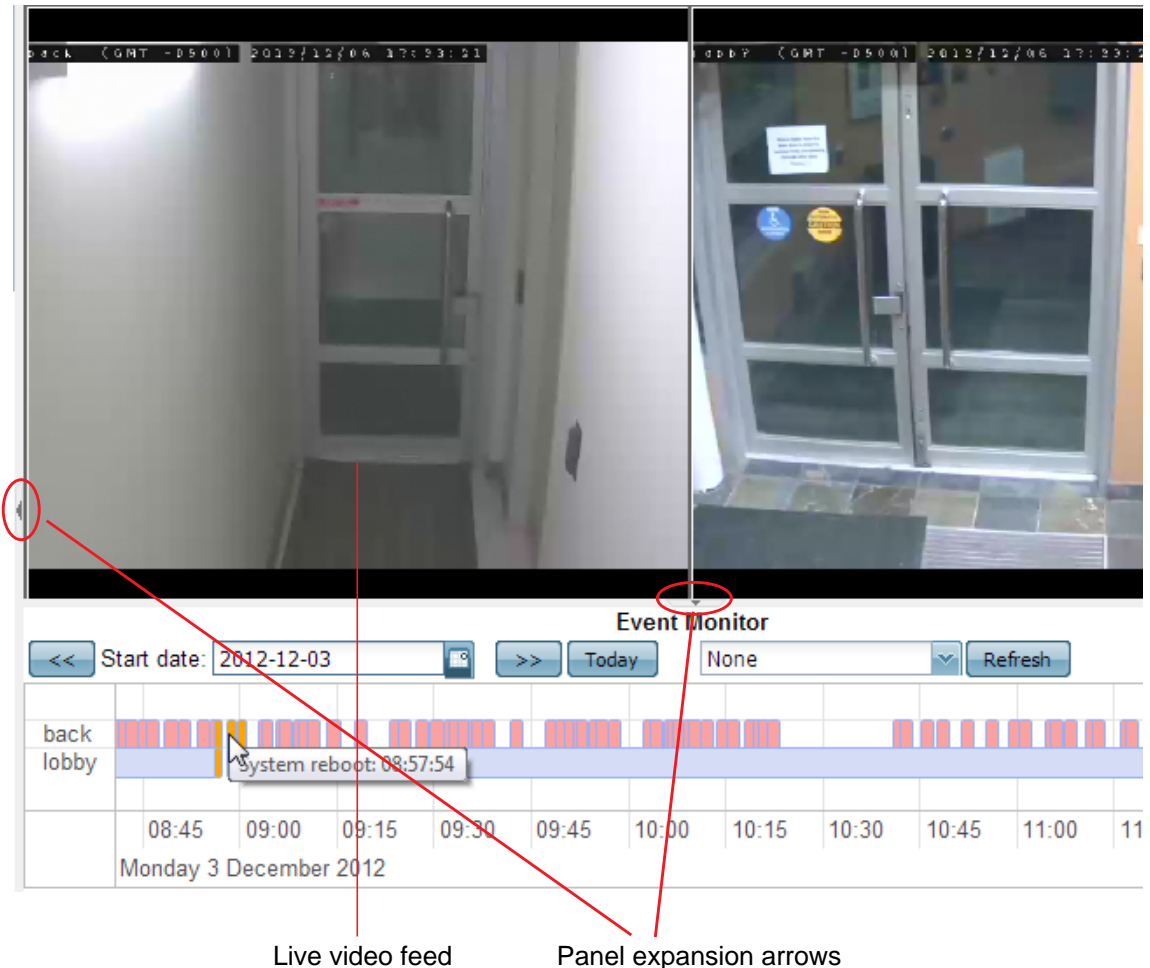


Quality of live video feeds may be different for administrators than it is for operator or viewer accounts, which use the camera’s settings in [“Configuring video profiles” on page 36](#).

To view live video from your cameras as an administrator

1. Go to *Monitor > Video Monitor*

Buffering (a blue “Q” appears, with an oscillating dotted line underneath) may take a few seconds, depending on the network, the *Resolution* of the camera, and your computer. When buffering is done, the current live video feed should appear.



2. There are very thin arrows at the bottom and (for administrators) right of the video viewer frame. If you are an administrator, click the arrow on the right to expand the image adjustment control panels.
3. If you logged in as an administrator, on the right pane, in the *Selection* area, choose which cameras you want to view.
4. If you logged in using a non-administrator account, your cameras have already been selected for you. If they are not correct, ask an administrator to reconfigure your account.

See also

- [Watching recorded video clips](#)

Video and image sharing

FortiRecorder supports video and image sharing. Using Fortirecorder, administrators can configure FortiRecorder and a third-party website to allow users to access a live feed of an established camera or an image from a 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=videoSe
  rvice&password=1234">
<p>iframes are not supported by your browser.</p> </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=videoSe
  rvice&password=1234">
<p>iframes are not supported by your browser.</p> </iframe><br/>
<script>
setInterval(function() {
  var req = new XMLHttpRequest();
  req.open('GET',
    "https://172.20.110.94/api?request=FRC_LiveView&id=20A-b5fc&userna
    me=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>
```

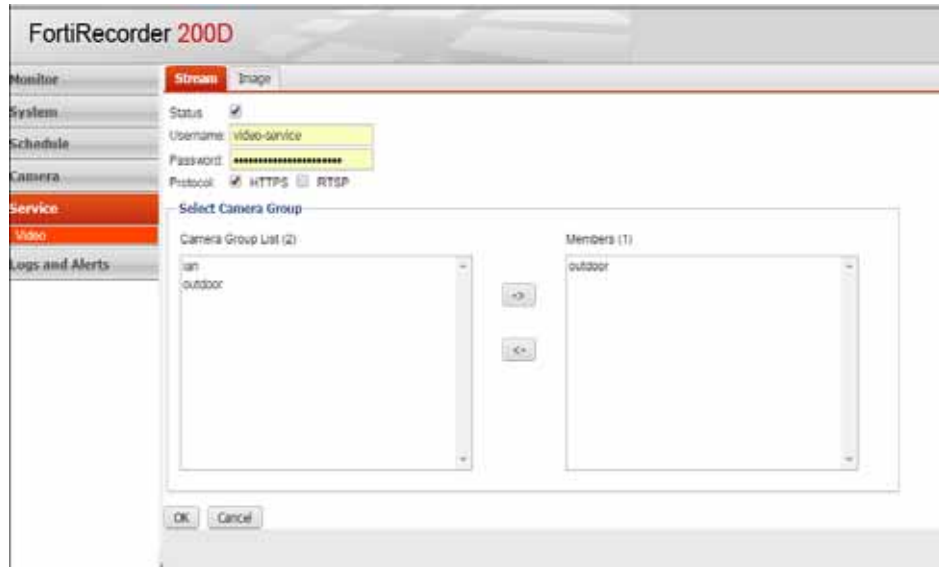
For example:

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

To configure video sharing on FortiRecorder

1. Go to *Service > Video > Stream*.
2. Select the *Status* checkbox.
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**.



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.

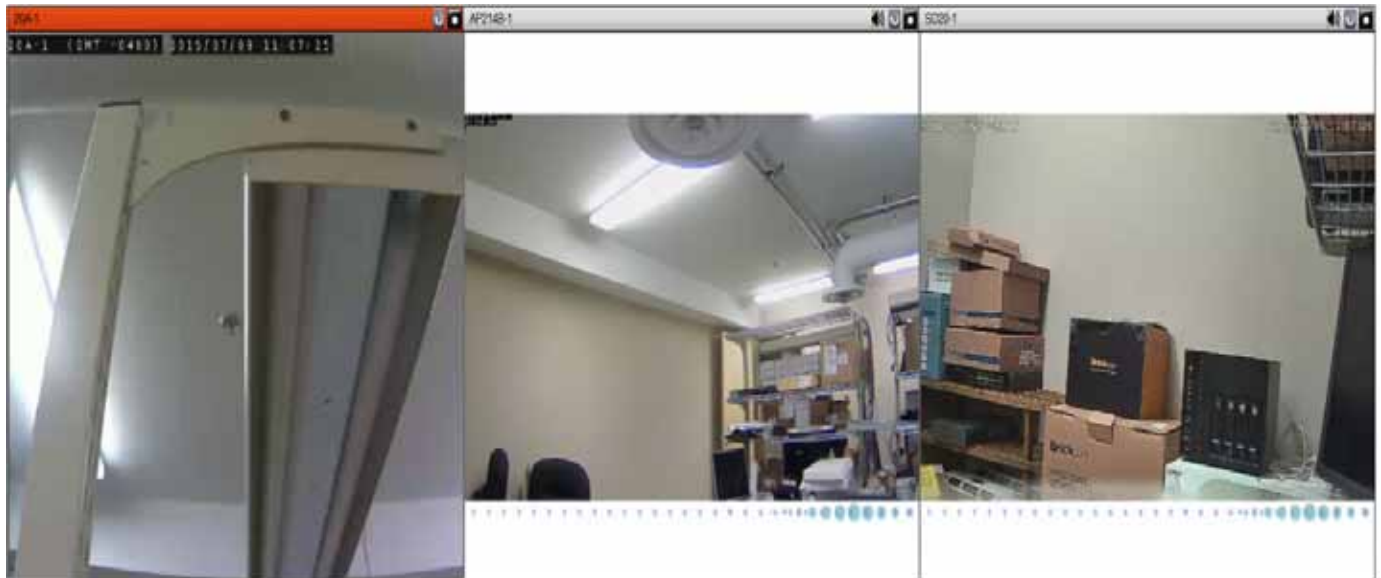
Similar to the shared video, you will need to upload the image to your website. Once you have finished that, configure image sharing in FortiRecorder.

To configure image sharing on FortiRecorder

1. Go to *Service > Video > Image*.
2. Select the *Status* checkbox.
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 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.
6. Select **OK**.

Watching recorded video clips

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.



Color-coded video clips

Time line panel

Camera selection and image control panel

Time periods in the time line panel are color-coded:

- **Yellow** — A system event such as a software update, system reboot, or camera reboot. Recordings cannot be stored while FortiRecorder is unavailable.
- **Light blue** — The lightest blue denotes previously recorded clips, the darker blue denotes temporary recording (see descriptions below), the darkest blue denotes manually initiated recording. 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 tag over a video clip represents recording with an attached annotation/marker. 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 motion detection-based recording that was not initiated by schedule.
- A white/blank space means there is no recording at that period of time.

About temporary recording

If the camera is not scheduled to record, but you are watching live feed from the camera, the video feed from the camera will be temporarily recorded in memory but not saved on the hard drive. When you stop watching the live feed from that camera, the temporary recording will be deleted. However, if you initiate manual recording while watching the live feed from the camera, the temporary recording will be saved on the hard drive.

To watch the recorded video

1. Go to *Monitor > Video Monitor*. The recorded video clips are in the *Event Monitor* area and the video clips for each camera appears as a time line.
2. By default, the time frame is minimized. To easily select a video clip, use the scroll wheel on your mouse to zoom in a time frame. Ensure that the mouse cursor is centered in the area that you want to zoom in. See the following pictures:

Figure 1: Time line zoomed out



Figure 2: Time line zoomed in



After zooming in, double-click the enlarged segment to view the clip

3. After you select the segment (if it is a motion-detection clip, a few key frames will appear for preview purpose), you can do the following:
 - Click the *Show* button to view clip.
 - Click the *Download* button to download the clip for archival or viewing on another computer. If your cameras have recorded a crime or other incident, you may need to provide the video clip to the police or other authorities. Your FortiRecorder NVR 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 in "[Configuring video profiles](#)" on page 36.
 - Click the *Lock* button to lock the clip so that the operators and viewers will not be able to view it.
4. To scroll through the time line, use your mouse to click and drag.

5. To set the time span of the time line, from *Start date*, select the beginning date of the recording, then from the interval drop-down menu to the right, select the interval of each segment of the time line in minutes.
6. To manually control the camera to pause or start recording, in the pane on the right side, click the *Control* bar to expand it, then click the buttons to pause or record.



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

7. To adjust the image quality, in the pane on the right side, click the *Control* bar to expand it, then click the + or - buttons to adjust *Brightness*, *Contrast*, *Saturation*, and *Sharpness*. Only administrators can use these controls, to prevent operators from accidentally or maliciously blacking-out the view.



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

8. To add a note to the video (e.g. "Suspicious light"), in the pane on the right side, click the *Control* bar to expand it, type your note in the text area, then click the *Insert Marker* button. A bright blue marker will appear on the clip and the added note will appear as mouse over text. Note that you must zoom in to see the marker. Otherwise it is very small on the time line. See the following picture.

Figure 3: Inserted marker



Inserted text marker in bright blue

See also

- [Watching live video feeds](#)

Reviewing motion detection notifications

If you have configured camera-based notifications (see “[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, as an administrator, 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 (see “[Notifications](#)”).

To review camera-based notifications

1. Go to *Monitor > Camera Notifications > Notification Events*.
2. From *Select recipient*, select either *All* (any recipient) or 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, click the link to view the corresponding notification.
A pop-up window displays 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, click its key frame image.

The notification window will be replaced with a video clip player.

Video management

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

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.

Table 7: FortiRecorder 400D supported RAID levels

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

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

If desired, you can add one or two more hard disk drives to the FortiRecorder 400D unit.

Figure 4: Hard disk bays on FortiRecorder 400D unit



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. Click *Refresh*.
6. The newly added disk will appear under *Drives*.
7. Add the disk to an array.
8. Click *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. Click *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*.
The RAID controller removes the hard disk from the list.
3. Protect the FortiRecorder unit from static electricity by using measures such as applying an antistatic wrist strap.
4. Physically remove the hard disk that corresponds to the one you removed in the web UI from its drive bay.
5. Replace the hard disk with a new hard disk, inserting it into its drive bay.
6. Click *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 both of the pre-installed hard drives with your own on FortiRecorder 400B 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” on page 80](#).

```
execute raidlevel <level>
```

6. The system will reboot.

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.

To configure external storage

1. Go to *System > Storage > External Storage*.
2. Select the *Enable* check box.
3. Configure these settings:

Setting name	Description
Protocol	Select one of the following types of storage media: <ul style="list-style-type: none">• External USB — External USB device.• iSCSI Server — An iSCSI (Internet Small Computer System Interface), server.• NFS — A network file system (NFS) server. Note: Support for NFS varies. Many Linux-based NAS solutions have been tested and are supported. Windows 2003 R2 and Windows 2008 Service for NFS are not supported.
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 <i>Status</i> page under <i>Monitor > System Status</i> .
Username	Type the user name of the FortiRecorder's account on the server. Alternatively, if using iSCSI, select <i>Initiator name as username</i> to authenticate using a name that follows RFC 3721 .
Password	Type the password corresponding to the user name.
Hostname/IP Address	Type either the IP address or fully-qualified domain name (such as <i>nas.example.com</i>) of the server.
Port	Type the port number on which the server listens for connections. The default is 2049 for NFS and 3260 for iSCSI.

Setting name	Description
Directory	<p>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.</p> <p>This setting appears only if <i>Protocol</i> is <i>NFS</i>.</p> <p>Note: Do not use special characters such as a tilde (~). This will cause the storage to fail.</p>
Encryption Key	<p>Enter the private key that will be used to encrypt data stored on this location. Valid key lengths are between 6 and 64 single-byte characters.</p> <p>This setting appears only if <i>Protocol</i> is <i>ISCSI Server</i></p>
iSCSI ID	<p>Enter 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).</p> <p>This setting appears only if <i>Protocol</i> is <i>ISCSI Server</i>.</p>

4. Click *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`

5. Go to *Camera > Configuration > Camera*, then click to select a camera's row, then click *Edit*.
6. For *Profile*, click *New* or *Edit*.
7. 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.
8. Click *Create*.

See also

- [Camera settings](#)

System monitoring

FortiRecorder provides several methods, such as SNMP traps, system logs, and realtime dashboard, for you to monitor the system status and diagnose system problems.

The dashboard

Monitor > System Status > Status appears when you log in to the web UI. It contains a dashboard with widgets that each indicates performance level or other system statuses.

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

The Console tab allows you to use the CLI commands.

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

SNMP traps & 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 <i>SNMP</i> on a network interface. For more information on communities, see “ Configuring an SNMP community ”.
Description	Type a comment about the FortiRecorder appliance, such as <code>dont-reboot</code> . 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 <code>floor2</code> . 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. If you want to use non-default thresholds to trigger SNMP traps such as high CPU usage, memory (RAM) usage, or disk/partition usage, click the disclosure arrow next to *SNMP Threshold* to expand the area, then configure these settings for each trap type:

Setting name	Description
Trigger	Click to edit, then type the percentage that when met or exceeded will be considered an event.
Threshold	Click to edit, then type the number of events that must be exceeded during the sample period in order to cause the SNMP trap.
Sample Period (s)	Click to edit, then type the amount of time in seconds during which the appliance will count the number of trigger-exceeding events. If the count exceeds the threshold number, the SNMP trap will be sent. Note: This must be equal to or greater than <i>Sample Freq (s)</i> , so that one or more samples are taken per time period.
Sample Freq (s)	Click to edit, then type the interval in seconds between measurements of the trap condition. If the trigger value is exceeded, this counts as an event. You will not receive traps faster than this rate, depending on the selected sample period. Note: This must be equal to or less than <i>Sample Period (s)</i> , so that one or more samples are taken per time period.

5. Click *Apply*.

6. 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](#)”.
7. If using SNMPv3, see “[Configuring SNMP v3 users](#)”.

See also

- [Configuring an SNMP community](#)
- [Configuring SNMP v3 users](#)

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. See “[To configure the SNMP agent via the web UI](#)”.
3. Under *Community*, click *New*.
A dialog appears.
4. Configure these 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 <code>public</code> . 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 <i>ne</i> add FortiRecorder to the community named <code>public</code> . 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.

Setting name	Description
Community Hosts	
IP Address	<p>Type the IP address of the SNMP manager that, if traps or queries are enabled in this community:</p> <ul style="list-style-type: none"> • will receive traps from the FortiRecorder appliance • will be permitted to query the FortiRecorder appliance <p>SNMP managers have read-only access. You can add up to 8.</p> <p>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.</p> <p>Caution: FortiRecorder sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.</p> <p>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. <i>If you do not want to disable traps, you must add at least one other entry</i> that specifies the IP address of an SNMP manager.</p>
Queries	<p>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.</p>
Traps	<p>Type each port number (162 by default) that will be the source (<i>Local</i>) port number and destination (<i>Remote</i>) port number for trap packets sent to SNMP managers in this community, then enable it. Port numbers vary by SNMP v1 and SNMP v2c.</p>
SNMP Event	<p>Enable the types of SNMP traps that you want the FortiRecorder appliance to send to the SNMP managers in this community.</p> <ul style="list-style-type: none"> • 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) <p>While most trap events are described by their names, the following events occur when a threshold has been exceeded:</p> <ul style="list-style-type: none"> • CPU Overusage • Memory Low • Log Disk Usage Threshold • Video Disk Usage Threshold <p>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”.</p>

5. Click **OK**.

- 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.

See also

- [Configuring SNMP v3 users](#)
- [SNMP traps & queries](#)

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

- Go to *System > Configuration > SNMP*.
- If you have not already configured the agent, do so before continuing. See [“To configure the SNMP agent via the web UI”](#).
- Under *User*, click *New*.
A dialog appears.
- Configure these settings:

Setting name	Description
User name	Type 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 16 users.
Enable	Enable this user entry.
Security level	Choose one of the three security levels: <ul style="list-style-type: none"> • 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 <i>not</i> 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. • Authentication, 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 <i>Password</i> . 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 <i>Password</i> . 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. Click *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.

See also

- [Configuring an SNMP community](#)
- [SNMP traps & queries](#)

MIB support

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

Table 8: Supported 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: <ul style="list-style-type: none"> • 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.

For instructions on how to configure traps and queries, see “[SNMP traps & queries](#)”.

See also

- [SNMP traps & queries](#)

Logging

Log messages, if you configured them (see “Configuring logging”), record important events on your FortiRecorder system.

About 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

For more information about log types, see “Log types”.

You can select a priority level that log messages must meet in order to be recorded. For more information, see “Log severity levels”.

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”.

See also

- [Log types](#)
- [Log severity levels](#)

Log types

Each log message contains a *Type* (`type`) field that indicates its category, and in which log file it is stored.

FortiRecorder appliances can record the following categories of log messages:

Table 9: Log types

Log type	Description
Event	Displays administrative events, such as downloading a backup copy of the configuration, and hardware failures.
Camera	Displays start/stop recording events, factory reset, and other camera events.



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.

Log severity 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`.

Table 10: Log severity levels

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.
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 will store all log messages equal to or exceeding the log severity level you select.

For example, if you select *Error*, the FortiRecorder appliance will store 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.

Viewing log messages

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 either *Monitor > Log Viewer > Event* (to view event logs about the appliance itself) or *Monitor > Log Viewer > Camera* (to view logs about connected cameras).
Columns and appearance varies slightly by the log type.
Initially, the page displays a list of log files of that type.
2. Double-click the row of a log file to view the log messages that it contains.

Table 11: Monitor > Video Monitor > Event (viewing the contents of a log file)

#	Date	Time	Subtype	Log ID	Message
1		07:55	admin	0001004923	GUI session failed to start verify password from (172.20.110.96)
2		07:55	admin	0001004923	User admin logout from GUI(172.20.110.96).
3		07:04	admin	0001004923	User admin login successfully from GUI(172.20.110.96)
4		07:01	admin	0001004923	GUI session failed to start verify password from (172.20.110.96)
5	2012-08-14	15:07:00	admin	0001004923	GUI session failed to get cookie info from (172.20.110.96)

Setting name	Description
Level	Select a severity level to hide log messages that are below this threshold (see “ Log severity levels ”).
Subtype	Select a subcategory (corresponding to the <i>Subtype</i> column) to hide log messages whose <i>subtype</i> 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 (see “ Searching logs ”).
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 (see “ Displaying & sorting log columns & rows ”).
#	<p>The index number of the log message within the log file, not the order of rows in the web UI.</p> <p>By default, the rows are sorted by timestamp in descending order, the same as they are within the log file, so the rows are in sequential order, starting with the most recent log message, number 1, in the top row. If you change the row sorting criteria (see “Displaying & sorting log columns & rows”), these index numbers won’t be in the same order as the rows.</p> <p>For example, when sorting by the <i>Message</i> column’s contents, the index numbers of the first 3 rows could be 14, 15, 9.</p> <p>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 timestamp and <i>Message</i>, not its #.</p>
Date	<p>The date on which the log message was recorded.</p> <p>When in raw format, this is the log’s <code>date</code> field.</p>
Time	<p>The time at which the log message was recorded.</p> <p>When in raw format, this is the log’s <code>time</code> field.</p>

Setting name	Description
Subtype	The category of the log message, such as <code>admin</code> for events such as authentication or configuration changes, or <code>system</code> for events such as disk consumption or connection failures. When in raw format, this is the log's <code>subtype</code> 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 <code>log_id</code> field.
Message	The log message that describes the specific occurrence of a recordable event. For example, all logout events follow a format similar to <code>User admin logout from GUI(172.16.1.5)</code> . but the exact message varies if the account name, connection method, and IP address are different. When in raw format, this is the log's <code>msg</code> field.

3. To return to the list of log files, click the *Back* button.

See also

- [Displaying & sorting log columns & rows](#)
- [Searching logs](#)

Displaying & sorting log columns & rows

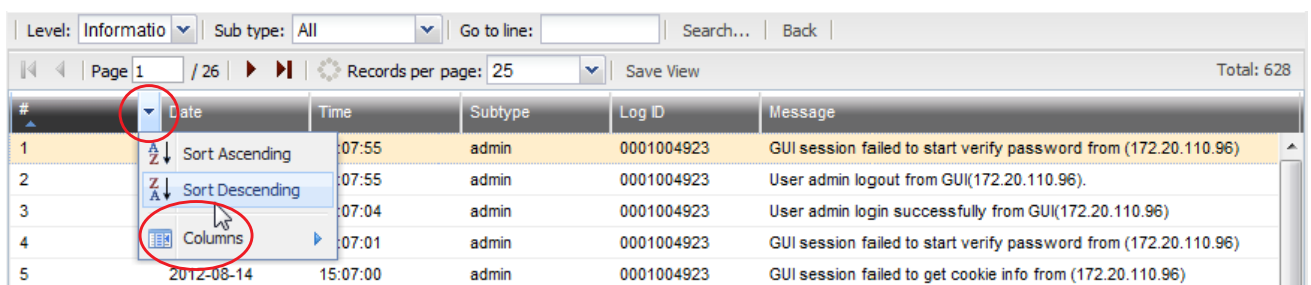
You can display, hide and re-order most columns — each column corresponds to a field in the log messages — to display only relevant categories of information, in your preferred order.



If you need to sort and filter the log messages based on more complex criteria, you can download the log file as a raw or CSV-formatted file for loading into external log or spreadsheet software (see “[Downloading log messages](#)”).

To display or hide columns

1. Go to one of the log types, such as *Monitor > Log Viewer > Event*.
2. Double-click the row of a log file to view the log messages that it contains.
3. 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 hover your mouse cursor over the *Columns* item in the menu to display a list of check boxes — one for each column.



4. Select which columns to hide or display:

5. To display a column such as *Time*, mark the check box next to its name. To disable the display of a column, clear its check box.
The page refreshes immediately, displaying the columns that you selected.
6. Column settings will **not** usually persist when changing pages, nor from session to session. If you want to keep the settings, you must click *Save View*. The log view settings will not apply to other accounts. Each administrator must configure their own settings.

To arrange the columns & rows

1. Hover your mouse cursor over the column heading.
2. Click and drag the column into the position where you want it to be.
3. 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 click 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.
4. Column settings will **not** usually persist when changing pages, nor from session to session. If you want to keep the settings, you must click *Save View*.

See also

- [Logging](#)
- [Searching logs](#)
- [About logs](#)

Downloading log messages

You can download logs that are stored locally (i.e., on the FortiRecorder appliance's hard drive) to your computer.

To download a log file

1. Go to one of the log types, such as *Monitor > Log Viewer > Event*.
2. In the list of log files, mark the check box of the log message that you want to download. (You can only download one log file at a time.)
3. Click *Download*.
A drop-down menu appears.
4. Select either:
 - **Normal Format** — A plain text `.log` file.
 - **CSV Format** — A comma-separated values (CSV) file that can be opened in spreadsheet software such as Microsoft Excel or OpenOffice Calc.
 - **Compressed Format** — A plain text `.log` file in a `.gz` compressed archive.
5. If a file download dialog appears, choose the directory where you want to save the file.
Your browser downloads the log file. Time required varies by the size of the file and the speed of the network connection.

See also

- [Deleting log files](#)

Deleting log files

If you have downloaded log files to an external backup, or if you no longer require them, you can delete one or more locally stored log files to free disk space.

To delete a log file

1. Go to one of the log types, such as *Monitor > Log Viewer > Event*.
2. Either:
 - To delete **all** log files, mark the check box in the column heading. All rows' check boxes will become marked.
 - To delete **some** log files, mark the check box next to each file that you want to delete.
3. Click *Delete*.

See also

- [Downloading log messages](#)

Searching logs

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

To search an attack log

1. Go to one of the log types, such as *Monitor > Log Viewer > Event*.
2. Click *Search*.
A dialog appears.
3. Configure these settings:

Setting name	Description
Keyword	<p>Type all or part of the exact word or phrase you want to search for. The word may appear in any of the fields of the log message (e.g. <i>Action</i> and/or <i>Message</i>), in any part of that field's value. If entering multiple words, they must occur uninterrupted in that exact order.</p> <p>For example, entering <code>admin</code> as a keyword will include results such as <code>User admin2 logout from GUI(172.16.1.15)</code> where part of the word appears in the middle of the log message. However, entering <code>User logout</code> 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.</p> <p>Depending on your setting of <i>Match condition</i>, you may be able to use asterisks as wild cards to match multiple words.</p> <p>This setting is optional.</p>
Message	<p>Type all or part of the exact value of the <i>Message</i> (<code>msg</code>) field of the log messages that you want to find.</p> <p>This setting is optional.</p>
Log ID	<p>Type all or part of the ID number of the log messages that you want to find.</p> <p>This setting is optional.</p>

Setting name	Description
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.
Match condition	Select whether your match criteria are specified exactly (<i>Contain</i>) or you have indicated multiple possible matches using an asterisk in <i>Keyword (Wildcard)</i> .

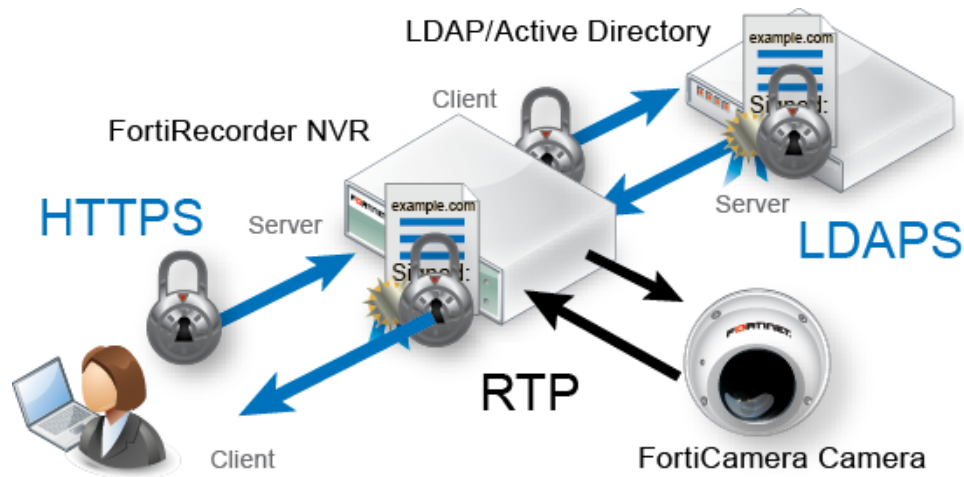
4. Click *Apply* to initiate the search.

The web UI displays log messages that match your search on a new tab.

Secure connections and 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
- authentication of servers



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.) *gatrwofaotwcv lfoa vnsotwo frscaaPf dafcaowm flahanlofye dfenf daf rhhmvrntafnrnlflewcfbayfyceboacuf*

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 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.)

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](#)”.

Table 12: System > Certificate > Local Certificate

Name	Subject	Status	
Factory	/C=US/ST=California/L=Sunn...	Default	●
Self	/CN=Fortinet/O=Fortinet Ltd.	OK	●

Setting name	Description
View	Click to view the selected certificate's issuer, subject, and range of dates within which the certificate is valid.
Generate	Click to generate a certificate signing request. For details, see “Generating a certificate signing request” .
Download	Click 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. See “Regular backups” .
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 <i>Status</i> column will change to reflect the new status.
Import	Click 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 <code>Subject :</code> 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. <ul style="list-style-type: none"> • 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.

See also

- [Uploading & selecting to use a certificate](#)
- [Revoking certificates](#)
- [Supported cipher suites & protocol versions](#)
- [Uploading trusted CAs' certificates](#)

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. Click *Generate*.
A dialog appears.
3. Configure the certificate signing request:

Setting name	Description
Certification name	Enter a unique name for the certificate request, such as <code>fortirecorder.example.com</code> . 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: <ul style="list-style-type: none">• Host IP — Select if the FortiRecorder appliance has a static IP address and enter the public IP address of the FortiRecorder appliance in the <i>IP</i> field. If the FortiRecorder appliance does not have a public IP address, use <i>E-Mail</i> or <i>Domain Name</i> 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 <code>fortirecorder.example.com</code>, in the <i>Domain Name</i> field. Do not include the protocol specification (<code>http://</code>) or any port number or path names.• E-Mail — Select and enter the email address of the owner of the FortiRecorder appliance in the <i>E-mail</i> field. Use this if the appliance does not require either a static IP address or a domain name. <p>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.</p> <p>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.</p>

Setting name	Description
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 <i>ID Type</i> is <i>Host IP</i> .
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 "NVR configuration". This option appears only if <i>ID Type</i> is <i>Domain Name</i> .
E-mail	Type the email address of the owner of the FortiRecorder appliance, such as admin@example.com. This option appears only if <i>ID Type</i> is <i>E-Mail</i> .
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 <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> or <i>2048 Bit</i> . Larger keys are slower to generate, but provide better security.

4. If you want to, or if your CA requires you to provide identifying information, configure these settings:

Setting name	Description
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.
Organization	Optional. Type the legal name of your organization.
Locality(City)	Optional. Type the name of the city or town where the FortiRecorder appliance is located.
State/Province	Optional. Type the name of the state or province where the FortiRecorder appliance is located.
Country/Region	Optional. Select the name of the country where the FortiRecorder appliance is located.
E-mail	Optional. Type an email address that may be used for contact purposes, such as admin@example.com.

5. Click *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. Click *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.

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.

- 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-----
```

- Save the certificate.

To upload a certificate

- Go to *System > Certificate > Local Certificate*.
- Click *Import*.
A dialog appears.
- Configure these settings:

Setting name	Description
Type	Select the type of certificate file to upload, either: <ul style="list-style-type: none"> 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	Click <i>Browse</i> to locate the certificate file that you want to upload. This option is available only if <i>Type</i> is <i>Certificate</i> or <i>Local Certificate</i> .
Key file	Click <i>Browse</i> to locate the private key file that you want to upload with the certificate. This option is available only if <i>Type</i> is <i>Certificate</i> .
Certificate with key file	Click <i>Browse</i> to locate the PKCS #12 certificate-with-key file that you want to upload. This option is available only if <i>Type</i> is <i>PKCS12 Certificate</i> .
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 <i>Type</i> is <i>Certificate</i> or <i>PKCS12 Certificate</i> .

4. Click *OK*.
5. To use a certificate, click its row to select it, then click *Set status* to put it in force.
6. 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. See "Example: Downloading the CA's certificate from Microsoft Windows 2003 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. Click *Import*.

A dialog appears.

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*, click the *Browse* button and select your CA's certificate file.
6. Click *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.

See also

- [Revoking certificates](#)
- [User management](#)

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.

Other accounts may not have sufficient privileges. The *Microsoft Certificate Services* home page for your server's CA should appear.

Microsoft Certificate Services - myca [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

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

Microsoft Certificate Services -- myca Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [myca]

Encoding method:

DER

Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

5. From *Encoding Method*, select *Base64*.
6. Click *Download CA certificate*.
7. If your browser prompts you, select a location to save the CA's certificate file.

See also

- [Uploading trusted CAs' certificates](#)

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. Click *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. Click *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. Click *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. Click *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.

Updating the firmware

Your new FortiRecorder appliance comes with the latest operating system (firmware) when shipped. However, if a new version has been released since your appliance was shipped, you should install it before you continue the installation. (Camera firmware can be updated later, after you have connected your cameras to the appliance. See “[Upgrading/downgrading the camera firmware](#)”.)

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>

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.

See also

- [Restoring firmware \(“clean install”\)](#)

Installing NVR 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 *Monitor > System Status > 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. 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](#)”.



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. Instead, see “[Restoring firmware \(“clean install”\)](#)”.

To install firmware via 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 *Monitor > System Status > Status*.

Figure 5: *System Information* widget



4. In the *System Information* widget, in the *Firmware version* row, click *Update*.
The *Choose Firmware* dialog appears.
5. Click *Browse* to locate and select the firmware file that you want to install, then click *OK*.
6. Click *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 *Monitor > System Status > 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 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.
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 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)
or:
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](#)”.

See also

- [Installing alternate firmware](#)

Installing alternate 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 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:

```
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.

See also

- [Booting from the alternate partition](#)
- [Installing NVR 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 alternate firmware via 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.
For details, see “Connecting to FortiRecorder web UI”.
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.

See also

- [Installing alternate firmware](#)

Upgrading/downgrading the camera firmware

Once the FortiRecorder NVR 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. First, 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. Click 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 click the *Upgrade* button. Note that 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 click 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.

Fine-tuning & best practices

This topic is a collection of fine-tuning and best practice tips and guidelines to help you configure your FortiRecorder appliances for the most secure and reliable operation.

While many features are optional or flexible such that they can be used in many ways, some practices are generally a good idea because they reduce complication, risk, or 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.

Hardening security

FortiRecorder NVRs are 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. ***Nec vxateclacfvofne frfivcabrmñ*** 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 travelling 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.

Figure 6: Disabling port4 in *System > Network > Interface*



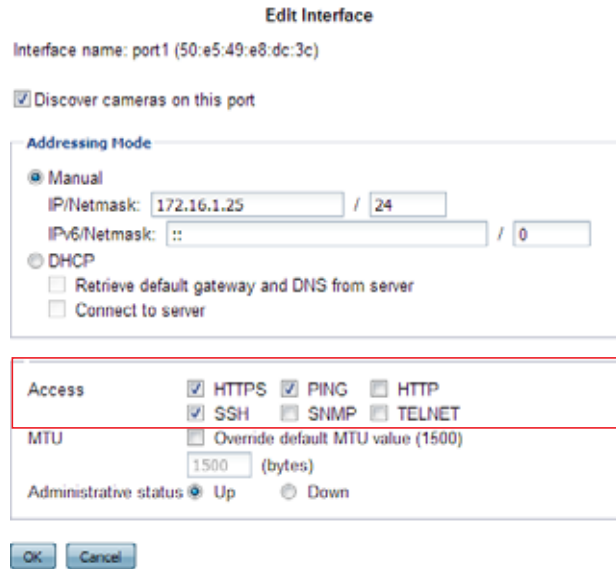
Name	IP/Netmask	IPv6/...	Access	Status	Discover Cameras	
port1	172.20.130.15/24	::/0	HTTPS,PING,SSH	+	+	•
port2	192.168.2.99/24	::/0	HTTPS,PING,SSH	+	+	•
port3	0.0.0.0/0	::/0		+	+	•
port4	0.0.0.0/0	::/0		+	+	•

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.

Figure 7: Restricting accepted administrative protocols in the *Edit Interface* dialog in *System > Network > Interface*



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 “[NVR configuration](#)”.

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

Figure 8: Disabling port4 in *System > Network > Interface*

Name	IP/Netmask	IPv6/...	Access	Status	Discover Cameras
port1	172.20.130.15/24	::/0	HTTPS,PING,SSH	+	+
port2	192.168.2.99/24	::/0	HTTPS,PING,SSH	+	+
port3	0.0.0.0/0	::/0		+	+
port4	0.0.0.0/0	::/0		X	+

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](#)”).

Patches

- Upgrade to the latest available firmware to take advantage of new security features and stability enhancements (see “[Updating the firmware](#)”).

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 NVR 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 NVR 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 NVR 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. See "[NVR configuration](#)".

Logging & 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 "Configuring logging".
- If you do not need a log or alert, disable it to reduce the use of system resources. See "Configuring logging".
- 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. See "Configuring logging".

Figure 9: Logs and Alerts > Log Setting > Local Log Settings

Log to Local Disk

Enable

The log file will rotate when either the file size or log time is reached.

Free disk space: 44269(MB)

Log file size: (MB)

Log time: (day) At hour:

Log level:

Log options when disk is full

Overwrite Do not log

Logging Policy Configuration

<input checked="" type="checkbox"/> Event Log	<input checked="" type="checkbox"/> Camera Log
<input checked="" type="checkbox"/> When configuration has changed	
<input checked="" type="checkbox"/> Admin login/logout event	
<input checked="" type="checkbox"/> System activity event	
<input checked="" type="checkbox"/> DHCP server event	
<input checked="" type="checkbox"/> Mail event	

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.

Regular backups

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

- Upgrading the firmware
- Running the CLI commands `execute factoryreset` 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 *Monitor > System Status > Status*.
3. In the *System Information* widget, in the *System configuration* row, click *Backup*.

System Information	
Serial number:	FK200D00RD000001
Up time:	0 day(s) 17 hour(s) 56 minute(s)
System time:	Wed, 22 Aug 2012 11:05:58 EDT
Firmware version:	v1.0.build0065,120821 (Interim) [Update...]
System configuration:	[Backup...] [Restore...]
Log disk:	Capacity: 91 GB, Used: 285 MB (0.3%)
Video disk:	Capacity: 823 GB, Used: 66 GB (8.09%)

If your browser prompts you, navigate to the folder where you want to save the configuration file. Click *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 settings (see “[Configuring FortiRecorder to send notification email](#)”) and `YYYYMMDD` is the timestamp of the backup.

See also

- [Restoring a previous configuration](#)
- [Restoring firmware \(“clean install”\)](#)
- [Resetting the configuration](#)
- [Updating the firmware](#)

Restoring a previous configuration

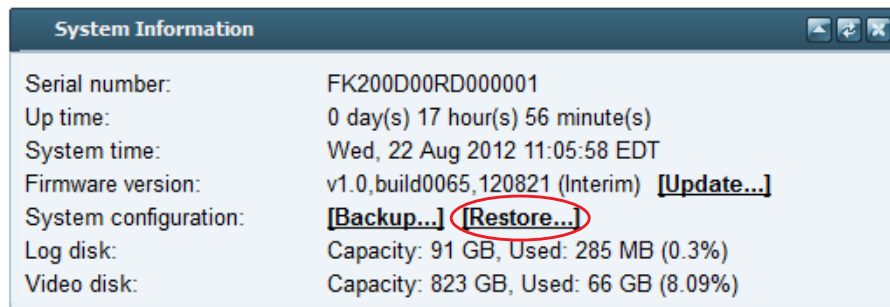
If you have downloaded configuration backups, you can upload one to revert the appliance's configuration to that point.



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 *Monitor > System Status > Status*.
2. In the *System Information* widget, in the *System configuration* row, click *Restore*.



3. Choose a FortiRecorder configuration backup file. (It has a `.conf` file extension.)
4. Click *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.

See also

- [Regular backups](#)
- [Restoring firmware \(“clean install”\)](#)
- [Resetting the configuration](#)

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.

Solutions by issue type

Recommended solutions vary by the type of issue.

- [Video viewing issues](#)
- [Snapshot notification issues](#)
- [Login issues](#)
- [Connectivity issues](#)
- [Resource issues](#)
- [Data storage issues](#)

Fortinet also provides these resources:

- the Release Notes provided with your firmware
- [Technical documentation](#) (references, installation guides, and other documents)
- [Knowledge base](#) (technical support articles)
- [Forums](#)
- [Online campus](#) (tutorials and training materials)

Check within your organization. You can save time and effort during the troubleshooting process by checking if other FortiRecorder administrators experienced a similar problem before.

Video 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, first check that you have installed software that can view live streams (which use RTP) and files (which use .mp4 format). For requirements, see [“Configuring video profiles”](#) and [“The notification window will be replaced with a video clip player.”](#).



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.

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 NVR

If the camera itself does not seem to be sending video to the NVR, although it has booted, has network connectivity, and you have configured a recording schedule on the NVR, 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, you can try either upgrading the camera's firmware (see "Upgrading/downgrading the camera firmware") or resetting the camera to factory defaults, then re-configuring it (see the camera's QuickStart Guide).

Snapshot 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 NVR'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 *ne* been configured to email still images — see "Notification configuration workflow"), 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 NVR'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 NVR to link to this public IP address in snapshot notifications.

If you are receiving too many notifications, change the configuration so that your FortiRecorder NVR 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 (see “[Trusted hosts](#)”) 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](#)”).

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 (see “[Trusted hosts](#)”). 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, 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 NVR 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. Click the row to select the account whose password you want to change.
4. Click *Edit*.
5. In the *New Password* and *Confirm Password* fields, type the new password.
6. Click *OK*.

The new password takes effect the next time that account logs in.

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.



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 than 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*.

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
```

See also

- [NVR configuration](#)

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 `tracert`) 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.)

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, `tracert` 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 `tracert` 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 `tracert` 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 `tracert`. However, if FortiRecorder does not respond, and there are no firewall policies that block it, ICMP type 0 (ECHO_RESPONSE or “pong”) might be effectively disabled. By default, `tracert` uses UDP with destination ports numbered from 33434 to 33534. The `tracert` 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 `tracert` 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 `tracert`, click *Edit*.

A dialog appears.

3. Enable *PING*.



Disabling *PING* only prevents FortiRecorder from **receiving** ICMP type 8 (ECHO_REQUEST) and `tracert`-related UDP.

It does **not** disable FortiRecorder CLI commands such as `execute ping` or `execute tracert` 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. Click *OK*.

The appliance should now respond when another device such as your management computer sends a `ping` or `tracert` 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.



In networks using features such as asymmetric routing, routing success in one direction does **not** guarantee success in the other.

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)
```

See also

- [NVR configuration](#)

Facilitating discovery

Discovery of the cameras by the FortiRecorder NVR uses mDNS. For it to work, cameras usually must be on the same IP subnet as the NVR, 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 NVR, so that discovery is not blocked.
- Manually add the camera to the FortiRecorder NVR'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 NVR'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 Status > 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 2013
192.168.200.101   20:10:7a:5a:29:38   udhcp 0.9.8       Wed Oct  3 11:17:12 2013
```

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.)

See also

- [Configuring the DHCP server](#)

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 *Monitor > System Status > Sessions*.

Table 13: IP session table

Refresh

Protocol	From IP	From Port	To IP	To Port	Expire(secs)
tcp	172.20.130.16	554	172.20.130.15	35860	0
tcp	172.20.130.203	554	172.20.130.15	46923	0
tcp	172.20.120.220	49574	172.20.130.15	443	1798
tcp	172.20.120.220	49573	172.20.130.15	443	1798
tcp	172.20.120.220	49568	172.20.130.15	443	0

GUI item	Description
Protocol	<p>The protocol of the session according to the “protocol” ID number field (or, for IPv6, “next header”) in the IP header of the packets.</p> <ul style="list-style-type: none"> • icmp – 1 (Due to the speed of ICMP messages, this will almost never be seen in the session list.) • tcp – 6 • udp – 17 (Due to the speed of UDP datagrams, this may be seen in the session list only rarely.)
From IP	<p>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.</p>
From Port	<p>The source port number.</p> <p>For a list of port numbers that can originate from the FortiRecorder NVR, see “Appendix A: Port numbers”.</p>
To IP	<p>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.</p>
To Port	<p>The destination port number.</p> <p>For a list of port numbers that can be received by the FortiRecorder NVR, see “Appendix A: Port numbers”.</p>
Expire (secs)	<p>The session timeout in seconds. The expiry counter is reset when packets are sent or received, indicating that the session is still active.</p>

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.

See also

- [NVR configuration](#)
- [User management](#)

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 NVR’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 NVR (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.

See also

- [Configuring the DHCP server](#)

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 the 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

e.g.:

```
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.

e.g.:

```
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...!..l..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. e.g.:

```
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. e.g.:

```
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. e.g.:

```

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.l.k....8.?.
0x0040 0105 6c6f 6262 7900 ..lobby.

```

- 6 — All of the output from 3, plus the network interface name. e.g.:

```

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 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

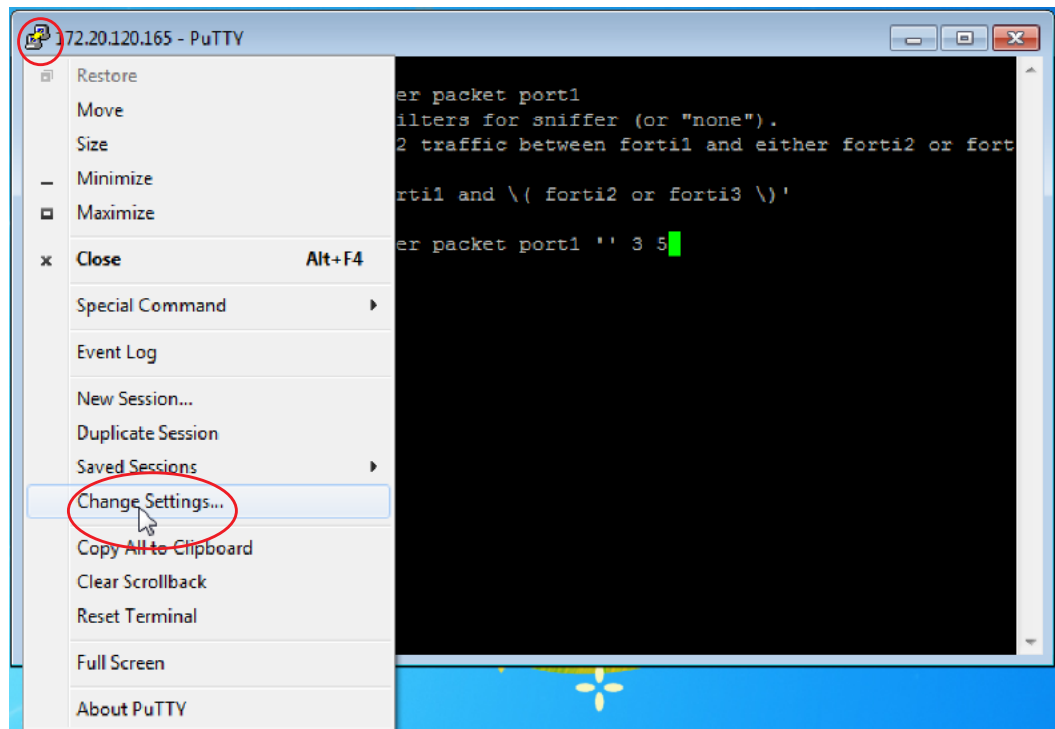
- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

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
```

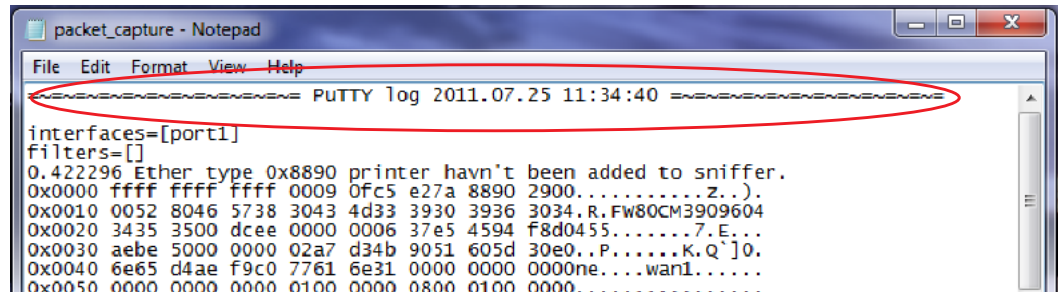
but do **not** press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.



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. Click *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 2016.07.25 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`.

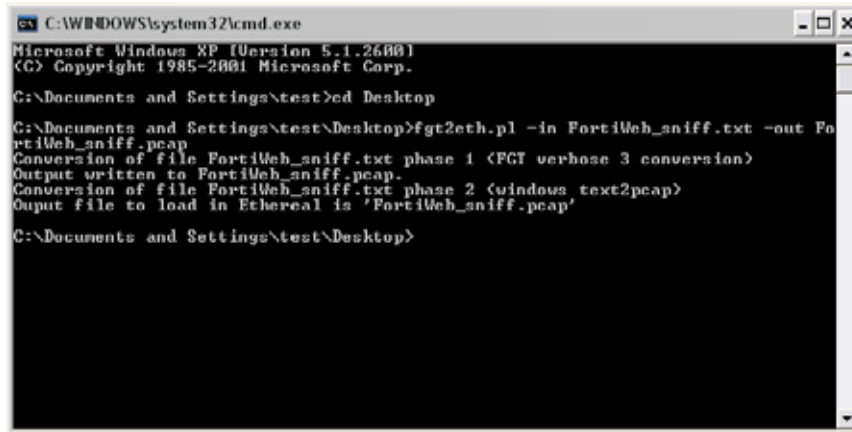
On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

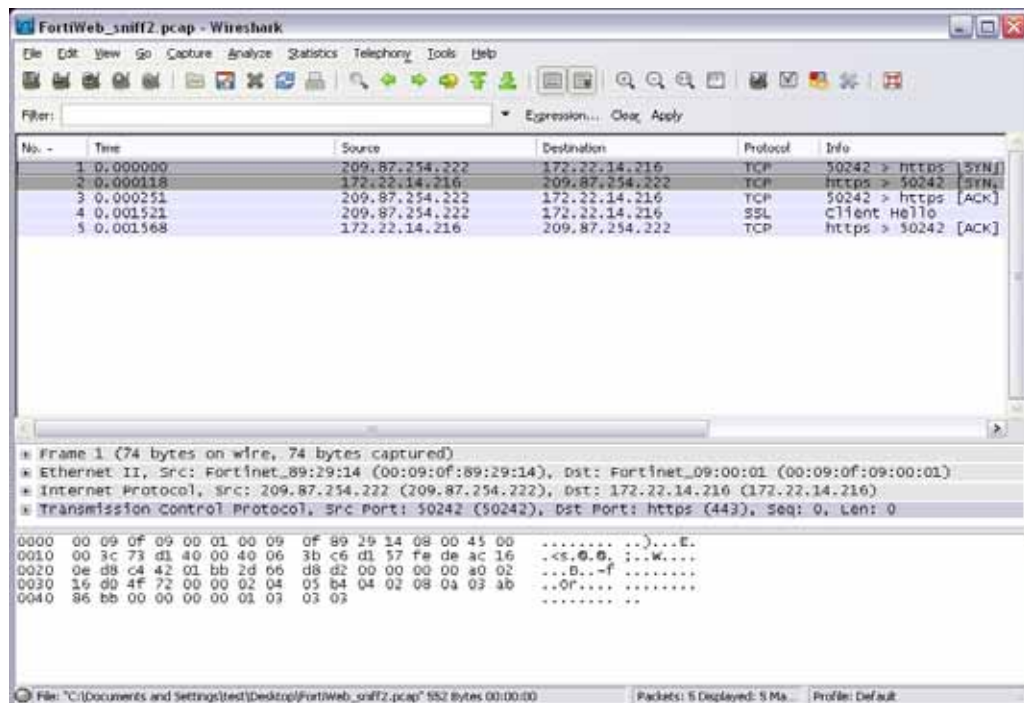
- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` 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

Figure 10:Converting sniffer output to .pcap format



15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Figure 11:Viewing sniffer output in Wireshark



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.

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 NVR, connect to the CLI and enter this command:

```
execute formatlogdisk
```

To reset the NVR’s configuration, connect to the CLI and enter this command:

```
execute factoryreset
```



Alternatively, you can reset the NVR’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 (“clean install”)

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.

See also

- [Updating the firmware](#)

Questions and answers

- How to connect cameras to FortiRecorder for the first time
- How to use recorded video clips
- How to use DIDO terminal connectors on FortiCam MB13 cameras

How to connect cameras to FortiRecorder for the first time

- Scenario 1: Direct connection
- Scenario 2: Connection with a third party DHCP server

Scenario 1: Direct connection

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



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 and FortiRecorder's port1 to a PoE switch as show in the diagram. Do **ne** 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. On the FortiRecorder web UI, go to *System > Network > DHCP*, and click *New* to create a new DHCP server on port1.

Network Interface Setting

ID:

Enable DHCP server:

Interface:

Gateway:

DNS options:

DNS server 1:

DNS server 2:

Domain:

Netmask:

Auto Config Setting

Lease time (Seconds):

Conflicted IP timeout (Seconds):

DHCP IP Range

New... | Edit... | Delete

Start	End
192.168.1.100	192.168.1.200

DHCP Excluded IP Range

Reserved IP Address

Create Cancel

Make sure to enable DHCP server

Make sure to select port1

5. Go to *System > Network > Interface*. Select port1 and click *Edit*.

Make sure to enable it

Edit Interface

Interface name: port1 (50:e5:49:e8:db:3c)

Discover cameras on this port

Addressing Mode

Manual

IP/Netmask: /

IPv6/Netmask: /

DHCP

Retrieve default gateway and DNS from server

Connect to server

Access

HTTPS PING HTTP FRC-Central

SSH SNMP TELNET

MTU

Override default MTU value (1500)

(bytes)

Administrative status Up Down

6. Make sure *Discover cameras on this port* is enabled.
7. 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.

- Go to *Camera > Configuration > Camera*, and click *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*.

Discover button

Enabled	Camera Name	Model	Location	Address	MAC Address	Profile	Status	Address Mode
<input checked="" type="checkbox"/>	Back	FCM-20A	Back Door	172.20.130.16	00:22:f4:81:b6:13	Back_profile	Active	Static
<input checked="" type="checkbox"/>	Back2	ED96200	Back Door	172.20.130.25	00:0d:0d:a0:07:89	Back2_profile	Active	Static
<input checked="" type="checkbox"/>	Kitchen	FCM-20A	Kitchen	172.20.130.17	00:22:f4:81:b5:ed	Kitchen_profile	Active	Static
<input checked="" type="checkbox"/>	Lobby	FCM-20A	Lobby	172.20.130.19	20:10:7a:5a:29:15	Lobby_profile	Active	Static
<input checked="" type="checkbox"/>	Reception	MB-130Ap	Reception	172.20.130.18	00:22:f4:81:c7:77	Reception_profile	Active	Static
<input checked="" type="checkbox"/>	Roof	OB-130np	Roof	172.20.130.23	20:10:7a:f1:14:30	high-med	Active	Static
<input checked="" type="checkbox"/>	Roof2	FCM-20A	Roof	172.20.130.27	00:22:f4:81:b5:e8	high-med	Active	Static
<input type="checkbox"/>	WB-300Ap-cf71	MB-300Ap		172.20.110.194	00:22:f4:81:c7:71		Not Configured	
<input type="checkbox"/>	FCM-20A-1eef	FCM-20A		172.20.110.225	20:10:7a:5a:1e:df		Not Configured	
<input type="checkbox"/>	FCM-20A-28e7	FCM-20A		172.20.110.221	20:10:7a:5a:28:e7		Not Configured	
<input type="checkbox"/>	FCM-20A-b5e3	FCM-20A		172.20.110.210	00:22:f4:81:b5:e3		Not Configured	
<input type="checkbox"/>	FCM-20A-2918	FCM-20A		172.20.110.203	20:10:7a:5a:29:18		Not Configured	
<input type="checkbox"/>	FCM-20A-28d1	FCM-20A		172.20.110.197	20:10:7a:5a:28:d1		Not Configured	
<input type="checkbox"/>	OB-300np-8f59	OB-300np		172.20.110.226	00:22:f4:81:b5:59		Not Configured	
<input type="checkbox"/>	FCM-20A-b612	FCM-20A		172.20.110.195	00:22:f4:81:b6:12		Not Configured	
<input type="checkbox"/>	FCM-MB13-5e04	FCM-MB13		172.20.110.232	00:22:f4:81:ce:04		Not Configured	
<input type="checkbox"/>	WMB-130Ap-03f9	WMB-130Ap		192.168.1.104	ac:81:12:d7:63:f9		Not Configured	
<input type="checkbox"/>	FCM-20A-b5f5	FCM-20A		172.20.110.231	00:22:f4:81:b5:f5		Not Configured	
<input type="checkbox"/>	PT-130Ap-e932	PT-130Ap		172.20.110.219	00:22:f4:81:e9:32		Not Configured	

Yellow: discovered but not configured cameras

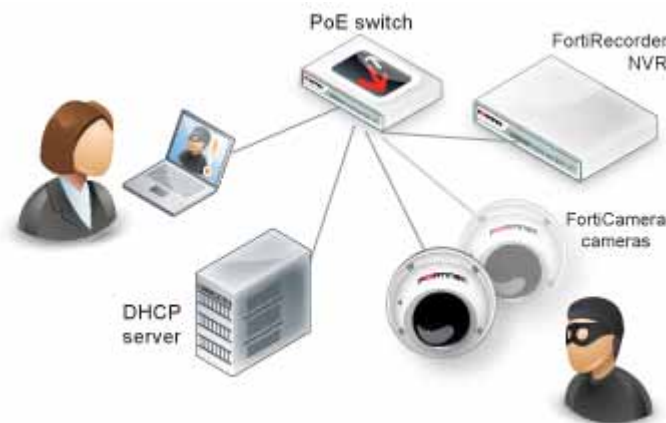
Configured cameras

- Double click on the discovered camera to configure the camera settings. For details, see “Configuring cameras” on page 44.
- Go to *Monitor > Video Monitor* to view the live feed from the camera.

Scenario 2: Connection with a third party DHCP server

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

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



- 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.
- Connect your PC directly to FortiRecorder's port1 interface.
- 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 NVR to your network. Then connect the camera to your network through a PoE switch.
7. Go to *Camera > Configuration > Camera*, and click *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. For details, see "Configuring cameras" on page 44.
9. Go to *Monitor > Video Monitor* to view the live feed from the camera.

How to use recorded video clips

Under *Monitor > Video Monitor*, you can watch the recorded video clips, which include the scheduled recording, motion detection recording, and manual recording.

The screenshot displays the FortiRecorder Video Monitor interface. At the top, there are two live camera feeds. The left feed shows a close-up of a door frame, and the right feed shows a wider view of a room with desks and equipment. Below the feeds is the 'Event Monitor' section, which includes a timeline for the date 'Thursday 9 July 2015'. The timeline shows color-coded bars representing recorded video clips for cameras 20A-1, AP214B-1, AP214B-2, and SD20-1. A control bar is located below the timeline, featuring navigation buttons (Start date, Today, Auto-Refresh, Refresh) and a 'Control bar' label. To the right of the timeline is a 'Camera image selection & image adjustment panel' with options for 'Annotate', 'Brightness', 'Contrast', and 'Saturation'. Red lines and boxes highlight these specific components.

Time line panel

Color-coded video clips

Control bar

Camera image selection & image adjustment panel

Time periods in the time line panel are color-coded:

- **Yellow** — A system event such as a software update, system reboot, or camera reboot. Recordings cannot be stored while FortiRecorder is unavailable.
- **Light blue** — The lightest blue denotes previously recorded clips, the darker blue denotes temporary recording (see descriptions below), the darkest blue denotes manually initiated recording. 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 tag over a video clip represents recording with an attached annotation/marker. 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 motion detection-based recording that was not initiated by schedule.
- A white/blank space means there is no recording at that period of time.

About temporary recording

If the camera is not scheduled to record, but you are watching live feed from the camera, the video feed from the camera will be temporarily recorded in memory but not saved on the hard drive. When you stop watching the live feed from that camera, the temporary recording will be deleted. However, if you initiate manual recording while watching the live feed from the camera, the temporary recording will be saved on the hard drive.

To watch the recorded video

1. Go to *Monitor > Video Monitor*. The recorded video clips are in the *Event Monitor* area and the video clips for each camera appears as a time line.
2. By default, the time frame is minimized. To easily select a video clip, use the scroll wheel on your mouse to zoom in a time frame. Ensure that the mouse cursor is centered in the area that you want to zoom in. See the following pictures:

Figure 12:Time line zoomed out

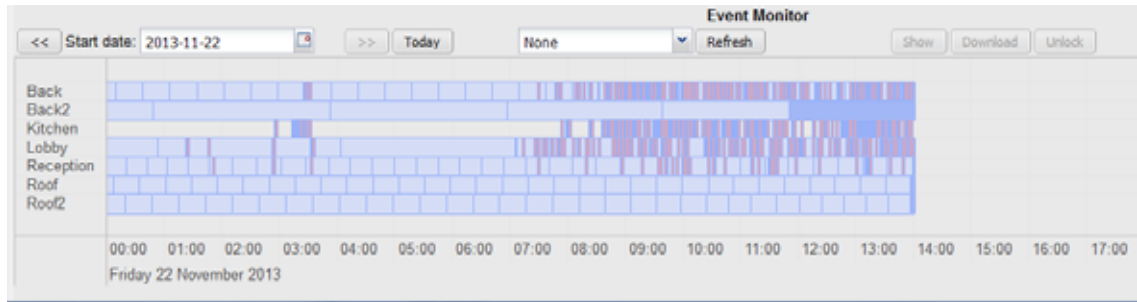
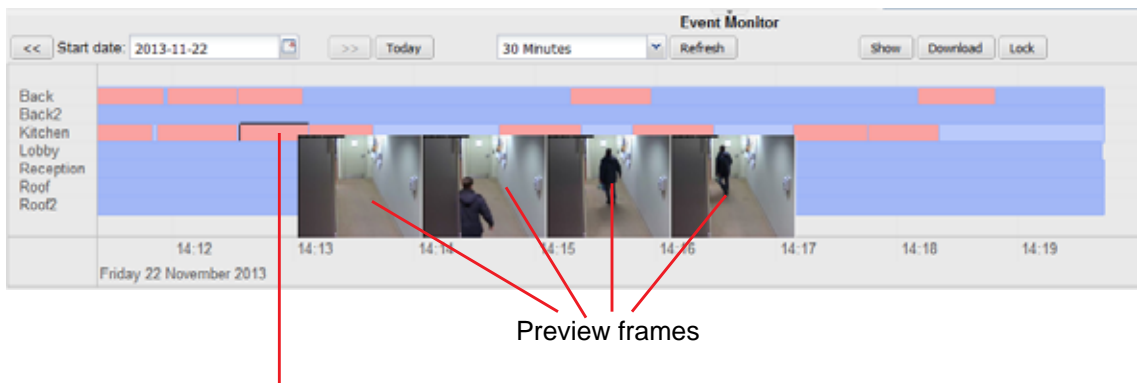


Figure 13:Time line zoomed in



After zooming in, double-click the enlarged segment to view the clip

3. After you select the segment (if it is a motion-detection clip, a few key frames will appear for preview purpose), you can do the following:
 - Click the *Show* button to view clip.
 - Click the *Download* button to download the clip for archival or viewing on another computer. If your cameras have recorded a crime or other incident, you may need to provide the video clip to the police or other authorities. Your FortiRecorder NVR 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 video profile setting.
 - Click the *Lock* button to lock the clip so that the operators and viewers will not be able to view it.
4. To scroll through the time line, use your mouse to click and drag.
5. To set the time span of the time line, from *Start date*, select the beginning date of the recording, then from the interval drop-down menu to the right, select the interval of each segment of the time line in minutes.
6. To manually control the camera to pause or start recording, in the pane on the right side, click the *Control* bar to expand it, then click the buttons to pause or record.



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

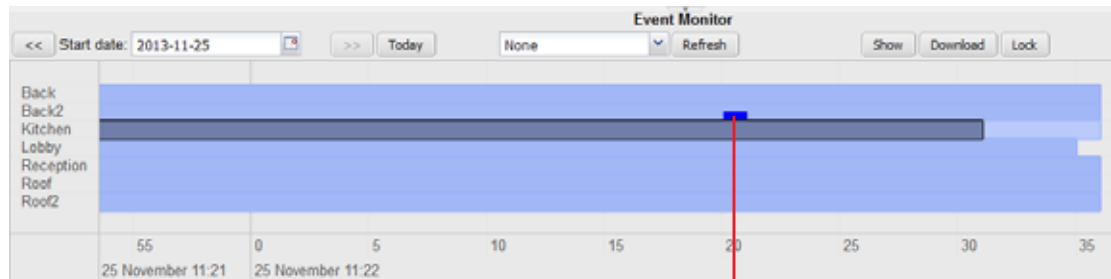
- To adjust the image quality, in the pane on the right side, click the *Control* bar to expand it, then click the + or - buttons to adjust *Brightness*, *Contrast*, *Saturation*, and *Sharpness*. Only administrators can use these controls, to prevent operators from accidentally or maliciously blacking-out the view.



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

- To add a note to the video (e.g. "Suspicious light"), in the pane on the right side, click the *Control* bar to expand it, type your note in the text area, then click the *Insert Marker* button. A bright blue marker will appear on the clip and the added note will appear as mouseover text. Note that you must zoom in to see the marker. Otherwise it is very small on the time line. See the following picture.

Figure 14:Inserted marker

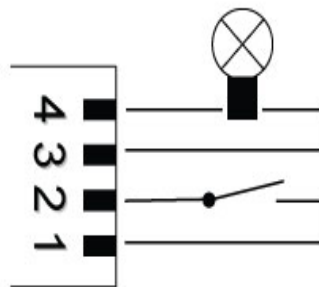


Inserted text marker in bright blue

How to use 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.

DIDO connection diagram for MB13 cameras

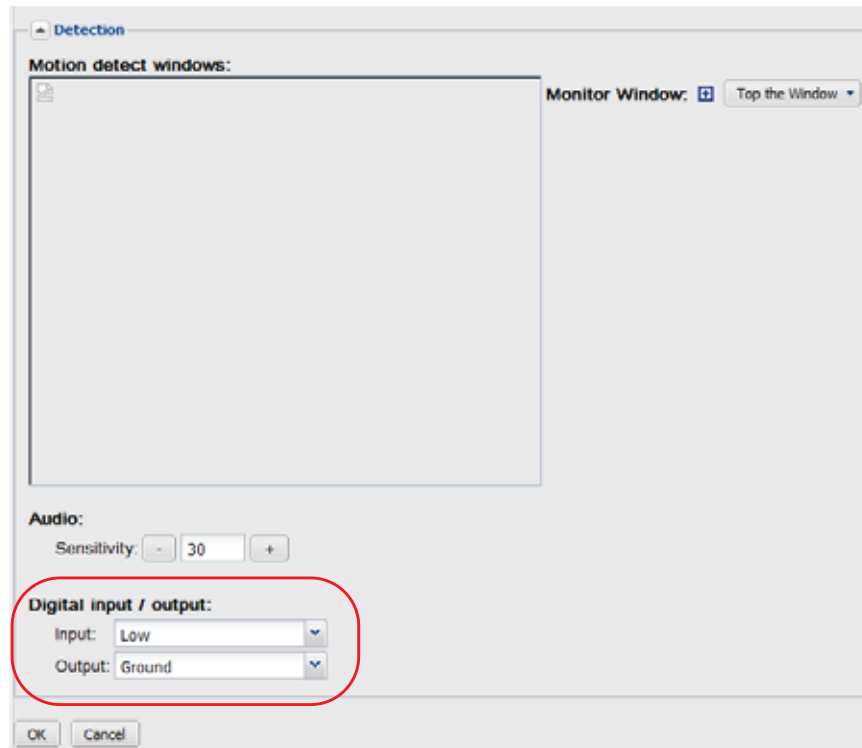


- Power output +5V
- Digital output (DO)
- Digital input (DI)
- Ground

To configure DIDO on MB13 cameras

- Go to *Camera > Configuration > Camera*, select the MB13 camera from the camera list and click *Edit*.

2. 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.

3. Go to *Camera > Schedule* and enable *Digital input* when you create a recording schedule.

The screenshot shows the 'FortiRecorder' interface for configuring a 'Recurrent Schedule Entry'. The 'All day' checkbox is checked. The 'Start' and 'End' fields are both set to 00:00. Under 'Recording type', the 'Digital input' checkbox is checked and circled in red, while 'Continuous', 'Motion detection', and 'Audio detection' are unchecked. 'Create' and 'Cancel' buttons are at the bottom right.

The schedules will be used in camera profiles, which will eventually be used by the camera settings. For details, see [“Camera configuration workflow”](#) on page 36.

Appendix A: 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.

Table 14: Default ports used by FortiRecorder for outgoing traffic

Port number	Protocol	Purpose
N/A	ICMP	execute ping and execute traceroute.
N/A	ARP	MAC address resolution. See "Examining the ARP table".
25	TCP	SMTP for alert email and snapshot notifications. See "Notification configuration workflow".
53	UDP	DNS queries. See "NVR configuration".
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. See "Configuring video profiles".
123	UDP	NTP synchronization. See "Camera settings".
443	HTTPS	Sending network settings and other configurations to cameras. See "Configuring video profiles".
514	UDP	Syslog. See "Configuring logging".
554, 8554	TCP/UDP	Controlling video recording (RTSP).
5353	UDP	mDNS queries for camera discovery. Multicast to 224.0.0.251.

Table 15: Default ports used by FortiRecorder for incoming traffic (listening)

Port number	Protocol	Purpose
N/A	ICMP	ping and traceroute responses. See "NVR configuration".
N/A	ARP	MAC address resolution responses. See "Examining the ARP table".
21	TCP	FTP for receiving motion detection clips from cameras. Currently, this is not configurable.
22	TCP	SSH administrative CLI access. See "NVR configuration".

Table 15: Default ports used by FortiRecorder for incoming traffic (listening)

Port number	Protocol	Purpose
23	TCP	Telnet administrative CLI access. See “NVR configuration” .
80	TCP	HTTP administrative web UI access. See “NVR configuration” .
443	TCP	HTTPS administrative web UI access. Only occurs if the destination address is a network interface’s IP address. See “NVR configuration” .
Dynamic	UDP	Receiving video from cameras (RTP). See “Configuring video profiles” .
554	TCP	Live video feeds (RTP) in the HTTP/HTTPS administrative web UI. See “Video monitoring” .
8550	TCP	FortiRecorder Central access.

See also

- [Establishing IP sessions](#)

Appendix B: 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.

Table 16:Maximum configuration objects

	FortiRecorder 100D	FortiRecorder 200D/400D	FortiRecorder VM
Cameras connected	16	64	Up to 1024 Controlled by licences <i>See FortiRecorder VM Install Guide for details</i>
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
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

Table 16:Maximum configuration objects

SNMP user hosts	16	16	16
Remote log servers	3	3	3
Motion detection windows	3	3	3
Privacy mask windows	3	3	3

Index

Symbols

.mp4 77, 124, 152

A

access profile 118
Active Directory 60
 domain 54
administrative access
 interface settings 19
 protocols 19
 restricting 19, 55
administrator
 "admin" account 14, 15, 17
 account 111, 113
 password 17, 55
 permissions 17
 trusted host 55
AES 89, 99
age
 of logs 32
 of video 39, 80
alert
 email 156
 severity level 92
algorithm
 SSL/TLS 98
Apple
 Bonjour 132, 156
 Mac OS X 77, 124, 152
 QuickTime 14, 41, 124
application layer 22, 132
ARP 156
 table 128, 135
 troubleshooting 128
ASCII 137
asymmetric routing 130
attack
 brute force login 55
 man-in-the-middle 100
 ping 19
attribute
 31 65
 ID 58
 vendor-specific 58
authentication 58, 59
 administrator 57
 local 57
 RADIUS 57, 59
 SNMP 89

authorization
 error 59

B

backup 121
 configuration 122
 firmware 113
 password 118
 video 83
bandwidth 37, 125
Base64 108
baseline 122
batch changes 123
best practices 122
bind DN 60, 61, 62
bit
 rate 37
 strength 77, 98, 99, 152
 tos 136
black video 78, 153
blurry video 78, 153
boot
 device 143
 interrupt 143
brightness 78, 153
bring up 127
broadcast 132
browser 20, 123
 requirements 14
brute force login 55
buffer
 QuickTime 73, 125

C

cable modem 41, 132
cache
 browser 111
 LDAP query 60, 64
 route 131
 routing table 131
Called Station ID 65
Camellia 99
camera
 discovery 156
 flip 47, 48
 log 91, 92, 127
 reboot 125
 resolution 37, 120
 third-party 7
 time 51

- certificate 98
 - authority (CA) 102, 104, 106, 108
 - default 99
 - factory 99
 - revocation list (CRL) 108
 - upload 108
 - revoke 108
 - signing chain 104
 - signing request (CSR) 101
 - generating 102
 - submit 104
 - trust 104
- chain of trust 104
- CHAP 65
- checksum
 - header 136
 - SNMP 89
- CIDR format 18
- cipher
 - block chaining (CBC) 99
- clean install 143
- CLI
 - connecting to 15
- clock
 - camera 51
- cloud 83
- codec 77, 124, 152
- color 78, 153
- command line interface (CLI) 156
 - diagnose 128
 - network 128
 - prompt 68
- comma-separated values (CSV) 33, 95
- communications (COM) port 15
- community 87
 - name 87
 - SNMP 85
- compression 37, 120
- configuration
 - backup 122
 - batch 123
 - download 123
 - restore 123
- conflict
 - codec 124
 - DHCP 135
 - file type association 124
 - IP address 18, 25, 132, 133, 135
 - plug-in 124
- connecting
 - CLI 15
 - web UI 14
- connection
 - state 136
- contact information, SNMP 86
- contrast 78, 153

- CPU
 - usage 37, 86, 141, 142

D

- dashboard 85
- default
 - administrator account 14, 15, 17, 111, 113
 - certificate 99
 - configuration 53
 - IP address 18
 - password 14, 15, 16, 17, 126
 - reset to 142
 - route 18, 21, 128
 - settings 14, 15
 - URL 14, 20, 123
- delay 125
- delete
 - log file 95
 - old video 39
 - video 80
- denial of service (DoS)
 - and ping 129
- DES 89, 99
- destination unreachable 129
- detail 37
- DHCPACK 132
- DHCPDISCOVER 132
- diagnose 128, 131, 136
 - netlink 127
- differentiated services 136
- Diffie-Hellman (DHE) 99
- discovery 47, 156
 - troubleshooting 132
- disk
 - full 32, 34, 67, 95, 142
 - space 33, 37, 39, 95
 - usage 37, 86, 142
- distinguished name (DN) 101
- domain name
 - directory 54
 - system (DNS)
 - multicast 132, 156
 - server 18, 22
 - test connection 129
 - settings 18
 - troubleshooting 129
 - used by DHCP clients 24
 - used by DHCP clients 24
- dot3Errors 90
- dot3Tests 90
- downgrade 110
- download
 - certificate 104
 - configuration 123
 - logs 95
 - video 77, 152
- dropping logs 33

- dynamic host configuration protocol (DHCP)
 - client 18, 133
 - lease 18, 25, 26
 - reservations 47
 - log 132
 - pool 25, 133
 - server 47, 135
 - interface 24

E

- ECHO_REQUEST 19, 128, 129
- ECHO_RESPONSE 19, 128, 129
- ECMP 130
- EGP 90
- egress 128
- e-mail 68
- encryption
 - password 118
 - SNMP 89
 - SSL/TLS 98
- error
 - IP address conflict 135
 - log 92
 - severity level 92
- Ethernet 14, 15, 90, 137
- event
 - log 91, 92, 132
 - search 96
 - SNMP 88
- Excel 95
- Extended Unique Identifier (EUI) 84

F

- factory default settings 14, 15, 53, 143
 - certificate 99
- failure in name resolution 23
- fcm.cfg 122
- feed, video 73
- file
 - configuration 122
 - format 77, 152
 - password 118
 - type association 51
- filter
 - logs 94
 - packet 136
- firewall 30, 51, 117
 - blocking discovery of cameras 132
 - blocking FortiRecorder 129, 156
- firmware 110
 - alternate 113
 - downgrade 110
 - restore 143
 - update 110
- flag
 - IP 136
 - video 78, 153
- flip 47, 48

- forgotten password 126
- format
 - boot device 143
 - CIDR 18
 - CSV 33
 - file 77, 152
- FortiAnalyzer 33, 92
- Fortinet
 - Technical Support 90
- FortiSwitch 41
- forwarding
 - port 45
- fragment 137
- frame rate 120
- frames
 - per second (FPS) 37
- FTP 156
- full
 - disk 34
- fully qualified domain name (FQDN) 102

G

- gateway 18, 21, 128
 - route 21
 - used by DHCP clients 24
- get 68
- grey video 78, 153
- guidelines 120

H

- H.264 77, 124, 152
- handshake 98
- hard drive
 - internal 80
- hardening security 41, 55, 117, 129
- hardware
 - failure 92
 - troubleshooting 127
- hash 89
- hexadecimal 133, 137
- host
 - name 68, 90
- HTTP 19, 156
 - administrative access 157
- HTTPS 19, 98, 99, 102, 106, 156
 - administrative access 157
- httpspd 22
- HyperTerminal 15

I

- ICMP 19, 90, 128, 129, 156
 - ECHO_REQUEST 19, 129
 - ECHO_RESPONSE 129
 - type 0 19, 129
 - type 8 19, 129
- ID
 - log 94
 - packet 136

- image
 - detail 37
 - quality 78, 120, 153
- import
 - certificate 104
 - CRL 108
- InetLocalMailRecipient 61
- InetOrgPerson 61
- interface
 - administrative access 19
- Internet service provider (ISP) 21, 22
- IP

- address 18
 - default 18
 - dynamic 18, 47
 - FortiRecorder NVR 18
 - static 26, 41, 135
- conflict 25, 132, 133, 135
- sessions 133
- virtual 30

- IP address 15
- iSCSI 84

J

- jitter 129

K

- key

- length 84
- pair 104
- private 101, 104, 105, 106
- storage encryption 84
- type, certificate 103
- word, search 96

- kill process 142

L

- latency 125, 129

- Layer

- 1 22, 137
- 2 22, 133
- 3 128
- 4 22

- LDAP

- bind 61
- bind DN 60, 62
- cache 64
- password 61
- query 62
- schema 61
- TTL 64

- LDAPS 98, 106

- lease, DHCP 18, 25, 26, 47, 133

- link

- layer 137
- status 127

- Linux 77, 152

- live video 73, 77, 151
 - buffering 73
 - delay 125
 - performance 120

- load
 - traffic 142

- local
 - certificate 99
 - logs 92

- location 44

- log 31

- about 91
- camera 127
- download 95
- dropped 33
- ID 94
- level 92
- timestamp 26
- type 91

- login 15, 126

- administrator 54
- timeout 118

- loop

- network 130

- lost password 126

- Lotus Domino 61

M

- Mac OS X 77, 152

- management information block (MIB) 85
 - support 90

- management protocols 118

- manager

- SNMP 85, 87, 88, 90

- man-in-the-middle (MITM) attack 99, 100

- mask 18, 21, 24

- maximum

- age 32, 39
- transmission unit (MTU) 20
- values 158

- MD5 89, 99

- mDNS 47, 132, 156

- media access control (MAC) address 133, 135, 156

- binding to a DHCP lease 26

- conflict 128

- resolution 128

- virtual 128

- media player 77, 152

- memory

- usage 86, 142

- messages

- error 135

- log 92

- types 91

- SNMP 85

- Microsoft

- Active Directory 60, 61

- Excel 95

- Outlook 69

- Windows 77, 152

- monitor
 - live video 73, 77, 151
 - using SNMP 85

- Mozilla
 - Thunderbird 69

- multicast 47, 156
 - forwarding 132

N

- name
 - community 87
 - host 68
- netmask 18, 21
 - administrator account 55
 - DHCP client 24

- network
 - adapter 18, 133
 - address translation (NAT) 30
 - and camera communications 45
 - and IP sessions 134
 - file system (NFS) 83
 - interface 14
 - layer 22, 132
 - loop 130
 - mask 18
 - time protocol (NTP) 26
 - problems 22
 - used by cameras 51

- Network Address Authority (NAA) 84

- network interface 15

- newcli 22

- next-hop router 21, 128

- null modem cable 15

O

- object
 - identifier (OID) 90
- objectClass 62
- online certificate status protocol (OCSP) 108
- OpenOffice Calc 95
- operating system (OS) 110
- operator 53, 56
- Outlook 69

P

- packet
 - capture 121, 136
 - loss 129, 131
- partition 86, 111, 113, 114, 143
- password 14, 15, 16, 17
 - admin, changing 126
 - administrator 55
 - backup 118
 - forgotten 126
 - LDAP bind 61
 - reset 126
 - SNMP 89
 - strength 55
 - strong 118
 - with certificate 105

- PEM 105
- performance 120, 129
 - DHCP 25
 - DNS 22, 24
 - factors in configuration 158
 - LDAP query 60, 64
 - network interface 127
 - on dashboard 85
 - packet capture 136
 - tuning 120
 - video 37, 120
- permission
 - denied 59
 - full 17
 - router 129
- persistent sessions 134
- physical
 - layer 22, 132
 - link status 127
 - network interface 18
 - port 18, 128
- ping 19, 22, 128, 129, 130, 156
 - flood 19
- pixel dimensions 37
- PKCS #12 104
- play video 78, 152
- plug-in 41, 124
- pool, DHCP 25, 133
- port
 - forwarding 30, 45
 - local console 143
 - number 30, 45, 88, 136, 156
 - destination 134
 - physical 18, 128
 - RJ-45 18
 - SNMP 88
 - TCP/UDP 156
 - UDP 19, 129
- port1 14, 15, 18
- port2 18
- port3 18
- port4 18
- power
 - over Ethernet (PoE) 41
- process
 - ID 142
- promiscuous mode 136
- protocol 63, 118, 136, 156
- proxy 51

Q

- quality 37
 - video 37

- query
 - Active Directory 59
 - cache 64
 - DNS 156
 - filter 62
 - LDAP 59, 62
 - cache 60
 - mDNS 156
 - NTP 26
 - OCSP 108
 - RADIUS 58, 60, 65
 - SNMP 20, 85, 86, 88, 90
 - string 60
- QuickTime 14, 41
 - buffering 73, 125

R

- RAID 0 80
- RAM
 - usage 141
- RC4 99
- reachable 128, 131
- real-time streaming protocol (RTSP) 51
- reboot 76, 123, 151
 - camera 125
- record
 - manually 76, 151
- re-imaging 111, 143
- remote access 29
- remote authentication dial-in user service (RADIUS) 57
 - query 58
 - vendor-specific attributes (VSAs) 58
- reset
 - configuration 121, 142, 144
 - password 126
- resolution 37, 120
- restore
 - CLI command 112
 - configuration 123
 - firmware 143
- retention of logs and recordings 39
- RFC
 - 1213 90
 - 1531 133
 - 2131 133
 - 2326 51, 157
 - 2548 58, 65
 - 2665 90
 - 3721 83
 - 5905 27
 - 792 19
- risk 55
- RJ-45 14, 15
- root
 - CA 104, 106
 - directory 113

- route
 - asymmetric 130
 - dynamic 130
 - static 128
 - table 22, 131
- router 30
 - blocking FortiRecorder 156
 - hop 131
 - next hop 21, 128
 - used by DHCP clients 24
- RSA 77, 99, 104, 152
- RTP 157
- RTSP 51, 157

S

- saturation 78, 153
- schedule
 - troubleshooting 26
- schema
 - LDAP directory 60
- secret
 - RADIUS 65
- Secure Shell (SSH) 19
 - administrative access 156
- security
 - hardening 41, 55, 117, 129
 - key size 103
 - passwords 55
 - TLS 106
 - trusted host 55
- SEED 99
- serial
 - number 90
- serial number 68
- session
 - administrator 120
 - table 133, 135
- severity
 - log levels 92
- SHA-1 89, 99
- sharpness 78, 153
- signature 77, 152
 - CA 106, 107
- signing chain 104, 105
- simple mail transport protocol (SMTP) 68, 156
- simple network management protocol (SNMP)
 - 20, 85, 87
 - agent 85, 86
 - contact information 86
 - manager 88, 90
 - MIB 90
 - OID 90
 - query 88
 - system name 68
 - v1 88
 - v2 88
 - v3 89
- SMTPS 98, 106
- sniffer 136
- socket 134

- source NAT 134
- spam 71
- special characters 68
- split horizon 130
- sshd 22
- SSL 26, 68, 106
- static
 - IP address 41
 - route 128
- status
 - camera 143
 - certificate 101, 108
 - disk 34, 67, 142
 - FortiRecorder 85
 - link 127
- stream 51
- strength
 - bit 99
 - password 55
- Subject 101
- subject information, certificate 102
- submit CSR 104
- subnet 18, 47, 132
- switch 132
- synchronization
 - NTP 156
- Syslog 92, 156
- system
 - status 85, 110
 - time 26
- system status 68

T

- tamper protection 77, 152
- TCP 90, 156
- tcpdump 136
- Telnet 20, 119, 157
- terminal 15
 - server 143
- TFTP 112, 113, 156
- Thunderbird 69
- time 22, 26
 - line 76, 151
 - to live (TTL) 129, 136
 - cache 64
 - LDAP 64
- timestamp
 - packet capture 136
 - PuTTY 140
- TLS 68
- top 22
- trace connection state 136
- traceroute 19, 22, 128, 129, 156
- tracert 22, 129, 131
- transactions 136
- transport
 - layer 22, 132
 - layer security (TLS) 106

- trap 85, 86, 88, 90
- troubleshooting
 - connectivity 22
 - DHCP 132
 - hardware 127
 - routing 131
 - video no longer being received 47, 135
 - video plug-ins 124
- trust store 104
- trusted
 - host 55, 118, 126
- type 0, ICMP 19, 129
- type 8, ICMP 19, 129
- type of service (tos) bits 136

U

- UDP 19, 90, 129, 156
- update 76, 151
- upgrade
 - firmware 110
- upload
 - certificate, local 104
 - certificate, remote 108
 - configuration 123
 - CRL 108
- URL 14, 20, 123
- usage
 - CPU 37, 86, 141, 142
 - disk 37, 86, 142
 - RAM 86, 141, 142
- US-ASCII 68, 137, 138
- user
 - name 54
 - query 62
 - SNMP 89
- User Principle Name (UPN) 62

V

- vendor-specific attribute 58
- video
 - delay 125
 - no longer being received 135
 - note 78, 153
 - play 78, 152
 - quality 37
- Video LAN (VLC) media player 51, 77, 152
- viewer 53, 56
- virtual
 - IP (VIP) 30
 - MAC (VMAC) 128

W

- WAN 30
- web browser 14, 20, 123
- web user interface (web UI) 14
- white video 78, 153
- widget 85
- Windows Media Player 51

X

X.509 99, 104

