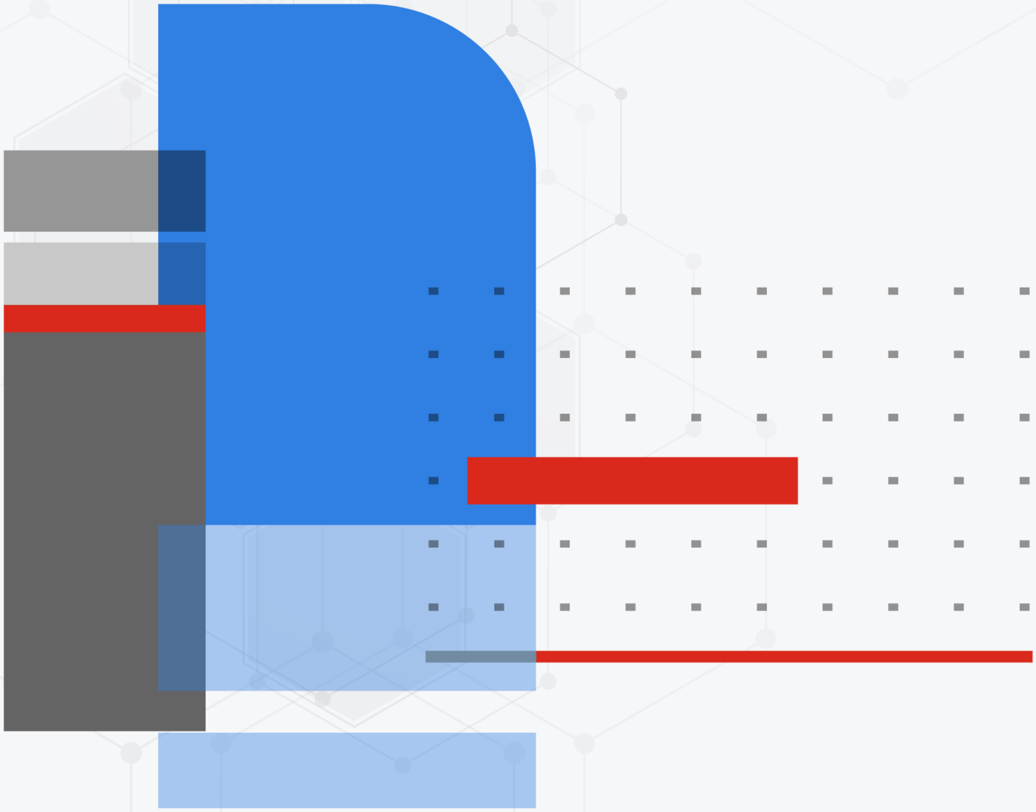
FORTINET

Administration Guide

FortiRecorder 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 05, 2024
FortiRecorder 7.2.0 Administration Guide
00-720-1019333-20241205

TABLE OF CONTENTS

Change log

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

Date	Change Description
2024-04-09	Initial release of FortiRecorder 7.2.0 Administration Guide.
2024-05-10	Fixed typo in Appendix B: Maximum values on page 176. For FortiRecorder VM, up to 1024 cameras can be connected.
2024-05-13	In Appendix A: Port numbers on page 174, the range of dynamic ports for RTP is now specified.
2024-12-05	Fix to URL for the camera view REST API in Configuring video sharing on page 133.

Key concepts

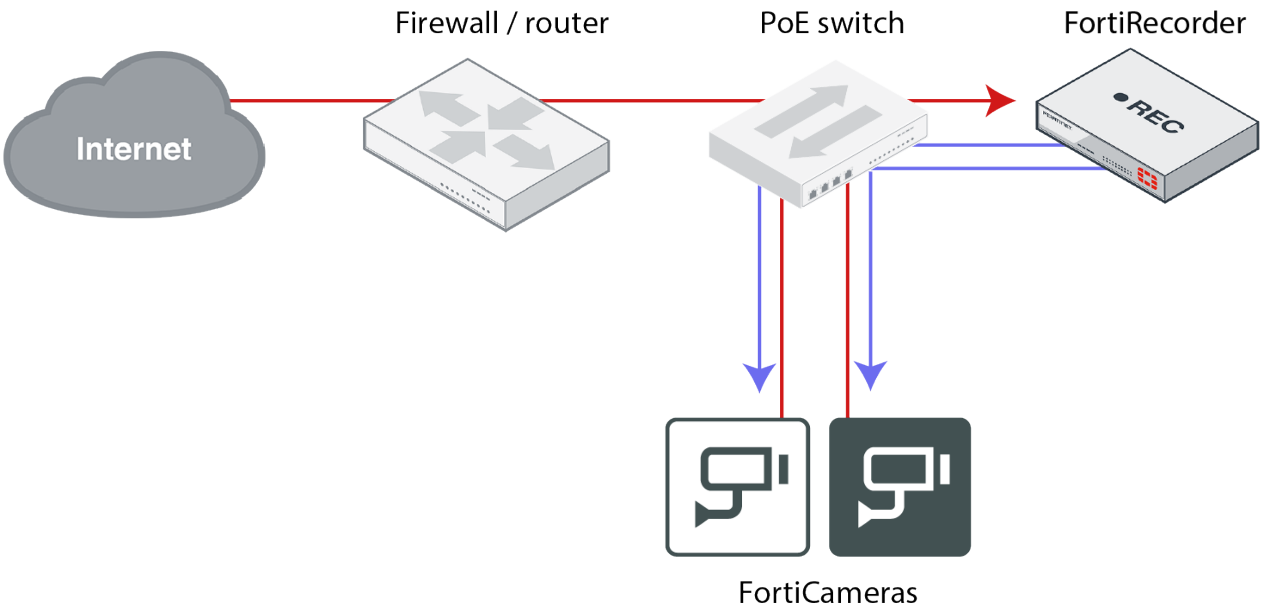
If you are new to FortiRecorder, or new to digital video surveillance systems, understanding some important ideas and words can help you quickly understand how to use your FortiRecorder.

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

It can also be connected to access control systems (ACS) to correlate events such as when doors are opened.



Third-party camera support

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

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

Licenses

For more capabilities, you can purchase and install licenses on your FortiRecorder for:

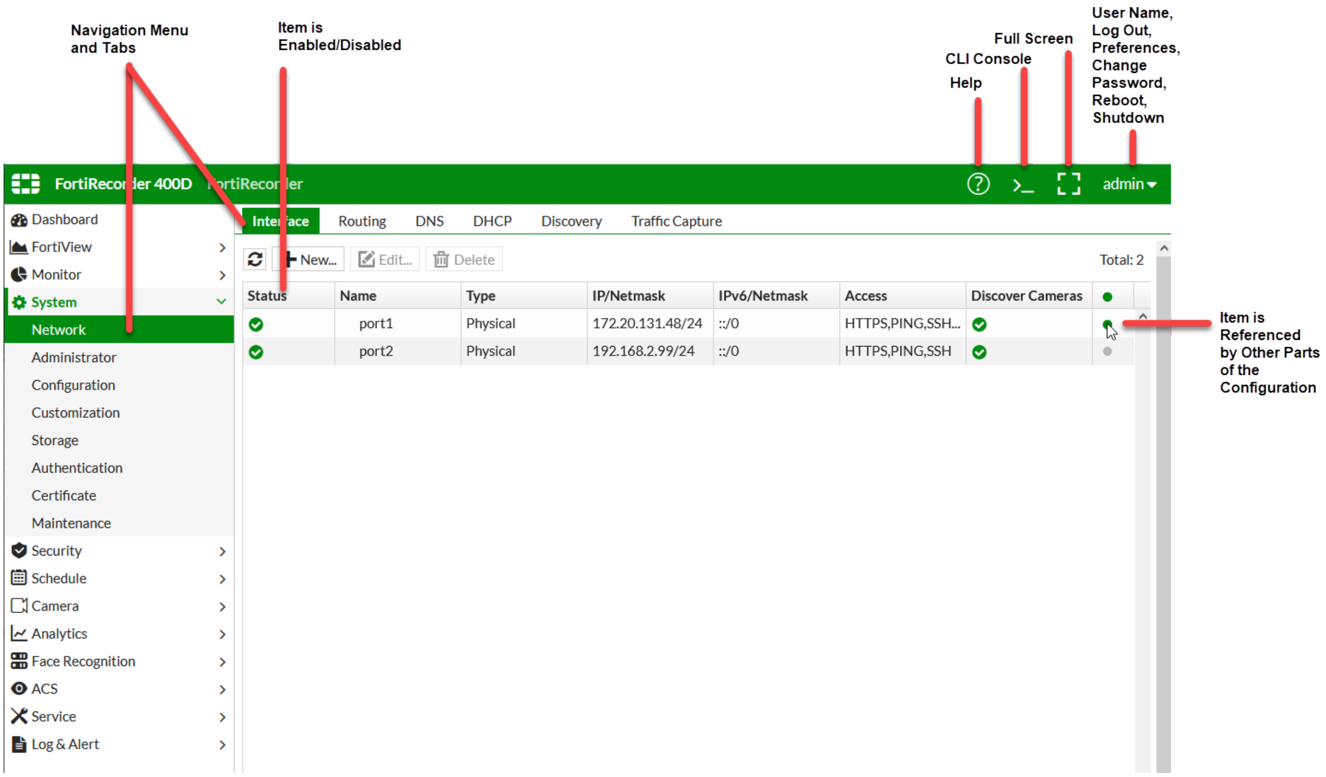
- Managing more third-party ONVIF cameras
- Face recognition AI
- Connecting cameras to FortiCamera Cloud, through FortiRecorder
- Virtual machine (VM) support for large scale deployments that can grow with your organization

If you are unsure which licenses you have installed, or whether they are valid, you can use the dashboard to verify their status. See Upload licenses on page 45.

Subscription services such as FortiCare support contracts and FortiCamera Cloud are purchased separately.

Interface overview

The GUI of FortiRecorder contains the following main areas and common controls:



Status	Name	Type	IP/Netmask	IPv6/Netmask	Access	Discover Cameras	●
✓	port1	Physical	172.20.131.48/24	::/0	HTTPS,PING,SSH...	✓	●
✓	port2	Physical	192.168.2.99/24	::/0	HTTPS,PING,SSH	✓	●

Settings are often grouped into a reusable, named item. Instead of repeatedly configuring the same settings, you configure settings once, give them a name, and then reference it by selecting it in other parts of the configuration. For example, multiple cameras often use the same settings. You can configure those settings once — in a camera profile — and then simply select that camera profile when you add each camera.

While referenced by another part of the configuration, an item cannot be deleted. If you need to trace references to it, then:

1. Use the navigation menus to go to the list of items.
2. In the item's row, click the green references dot.
   A list of item names or index numbers that reference the item are displayed.

When an item is not referenced, you can either delete it ,or temporarily disable it. Disabling the item keeps it in the configuration file for later use, but it is not loaded into memory. This optimizes RAM usage, improving performance.

The Help button is context-aware. When you click it, it jumps to the part of the documentation that matches your current location in the GUI.

Quick setup

Upon the first startup, you must configure FortiRecorder.

Alternatively, to save time with larger deployments, you can use a USB key drive for zero-touch provisioning instead. For details, see Automatic provisioning on page 17.

When you connect cameras locally — **directly, or on the same LAN as FortiRecorder** — then FortiRecorder can automatically discover the cameras. FortiRecorder supports UPnP, mDNS, and ONVIF discovery. Basic setup can be completed in a few minutes.

Deployment patterns that can use quick setup are:

1. Connecting cameras to FortiRecorder only on page 11
2. Connecting cameras to a DHCP server and FortiRecorder on page 14

This results in a very basic but functional configuration where you can log in and the cameras are connected to FortiRecorder as their NVR. If you want to add more administrator or user accounts, set up alerts, or want to configure more advanced system settings, also perform More system settings on page 63.

To strengthen security, select WPA2 enterprise or personal. For details, see your FortiAP/FortiWifi or third-party product documentation.

For more complex or larger deployments (for example, if the Internet or a firewall is between cameras and FortiRecorder), instead use the instructions in Setup on page 19.

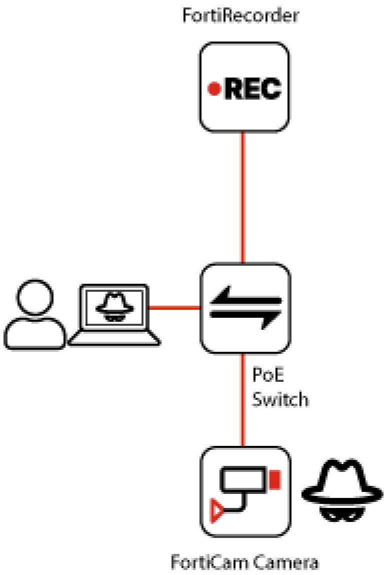
Connecting cameras to FortiRecorder only

You can use this scenario if you want a **new, dedicated network** where you install your FortiRecorder, FortiCam or third-party ONVIF cameras, and any other devices such as an access control system (ACS). The built-in DHCP server on FortiRecorder is enabled to automatically give IP addresses to the devices, so you don't need a separate DHCP server or router.

If you already have a DHCP server, do not use these instructions. Instead use Connecting cameras to a DHCP server and FortiRecorder on page 14.

If isolated from your office LAN, this network topology provides maximum network security because no other devices or untrusted computers are connected to your surveillance network.

Due to this isolation, this network topology can also be used if you want to test a third-party camera or other device with FortiRecorder in a lab.



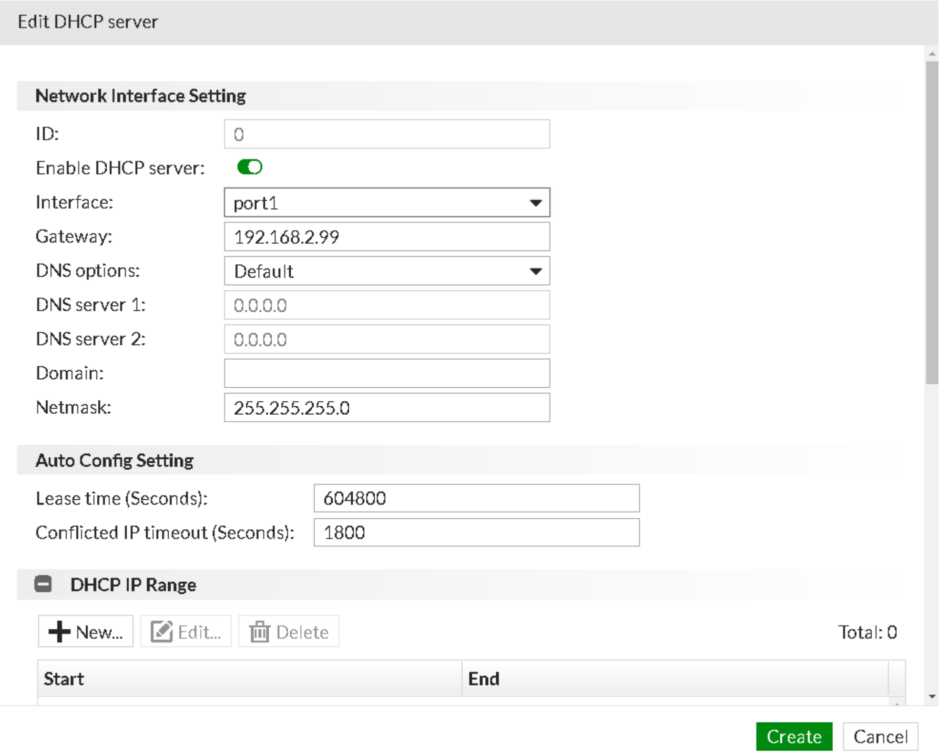
1. Use Ethernet network cables to connect port1 of FortiRecorder and your computer to a power-over-Ethernet (PoE) switch.

   Do not plug in your cameras yet.
2. Change your computer's IP address to be 192.168.1.98 with subnet 255.255.255.0. Steps vary by whether you use Apple macOS, Linux, or Microsoft Windows.

   Alternatively, you can use a different IP address, but it must be on the same subnet as the default IP address of FortiRecorder port1: 192.168.1.0/24.
3. On your computer, open a web browser and go to:

   https://192.168.1.99

   Log in with the username `admin` and no password.
4. Change the password. For details, see Setting the "admin" account password on page 25.
5. Configure the built-in DHCP server:
   a. On the FortiRecorder GUI, go to *System* > *Network* > *DHCP*.
   b. Click the *New* button.



Edit DHCP server

Network Interface Setting

ID:	0
Enable DHCP server:	●
Interface:	port1
Gateway:	192.168.2.99
DNS options:	Default
DNS server 1:	0.0.0.0
DNS server 2:	0.0.0.0
Domain:	
Netmask:	255.255.255.0

Auto Config Setting

Lease time (Seconds):	604800
Conflicted IP timeout (Seconds):	1800

DHCP IP Range

Total: 0

Start	End

c. Enable *Enable DHCP server*.

d. From *Interface*, select port1.

e. In the *DHCP IP Range* area, click *New*. Enter a range of IP addresses (pool) that is larger than all of the devices that you want to connect.

   DHCP IP addresses must be in the same subnet as the IP address that you will give to port1. For example, if port1 is 192.168.1.9/24, then a DHCP range for 10 cameras could be 192.168.1.10-192.168.1.19.

f. Click the *Create* button to close the dialog, and then click the *Create* button to start the DHCP server.

6. Configure port1:

   a. Go to *System* > *Network* > *Interface*.

   b. Select port1. Click the *Edit* button.

   c. Enable *Discover cameras on this port*.

   d. Click *OK*.

7. Use Ethernet network cables to connect the cameras to the switch.

If you connected the cameras too soon, before a DHCP server was available, then they are using a default IP address.The default address will not work with your network. To fix this, unplug the cameras and then plug them in again. This reboots the cameras and requests a correct IP address from the DHCP server.

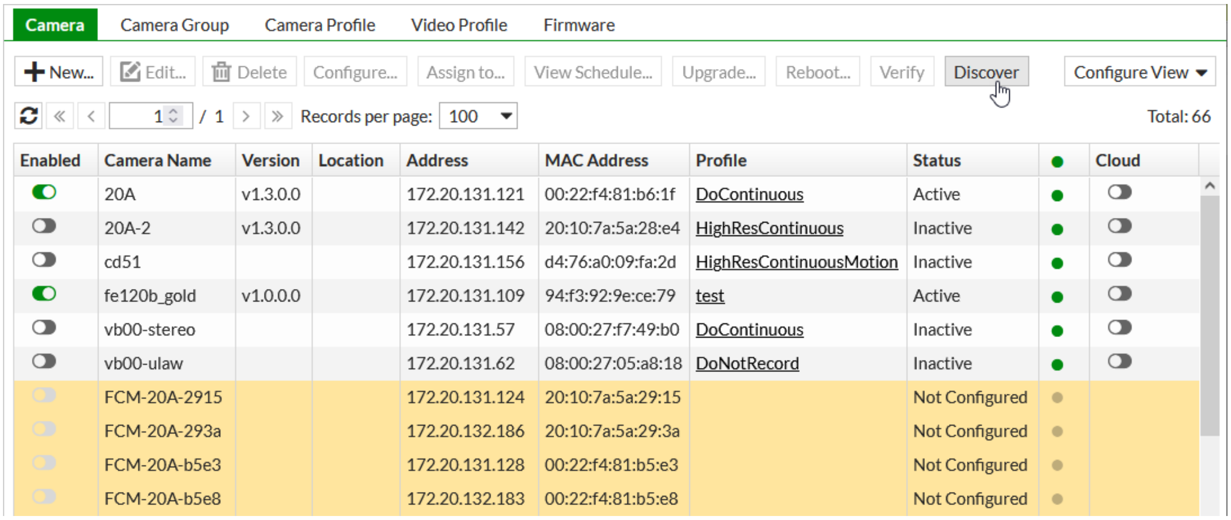
---

8. Discover and configure the cameras:

   a. Go to *Camera* > *Configuration* > *Camera*.

   b. Click the *Discover*button.

   After several seconds, a list of cameras appears. Newly discovered cameras are highlighted in yellow, and their *Status* column displays *Not Configured*.



Enabled	Camera Name	Version	Location	Address	MAC Address	Profile	Status	●	Cloud
●	20A	v1.3.0.0		172.20.131.121	00:22:f4:81:b6:1f	DoContinuous	Active	●	○
○	20A-2	v1.3.0.0		172.20.131.142	20:10:7a:5a:28:e4	HighResContinuous	Inactive	●	○
○	cd51			172.20.131.156	d4:76:a0:09:fa:2d	HighResContinuousMotion	Inactive	●	○
●	fe120b_gold	v1.0.0.0		172.20.131.109	94:f3:92:9e:ce:79	test	Active	●	○
○	vb00-stereo			172.20.131.57	08:00:27:f7:49:b0	DoContinuous	Inactive	●	○
○	vb00-ulaw			172.20.131.62	08:00:27:05:a8:18	DoNotRecord	Inactive	●	○
○	FCM-20A-2915			172.20.131.124	20:10:7a:5a:29:15		Not Configured	•	
○	FCM-20A-293a			172.20.132.186	20:10:7a:5a:29:3a		Not Configured	•	
○	FCM-20A-b5e3			172.20.131.128	00:22:f4:81:b5:e3		Not Configured	•	
○	FCM-20A-b5e8			172.20.132.183	00:22:f4:81:b5:e8		Not Configured	•	

c. Double-click each camera to configure its settings. For details, see Configuring cameras on page 50.

Repeat this step for all cameras.

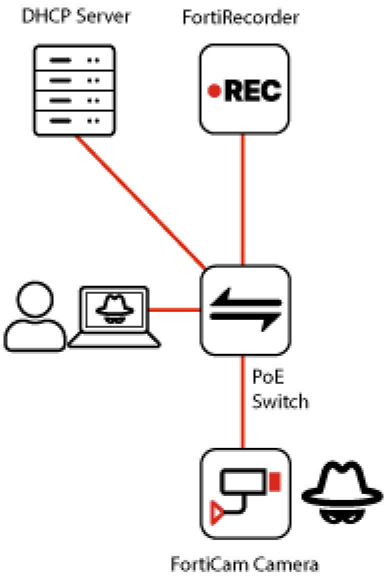
9. To verify that FortiRecorder is able to receive video from the camera, go to *Monitor* > *Video* > *Video*. You should be able to see the camera's live video feed.

Connecting cameras to a DHCP server and FortiRecorder

You can use this scenario if you already have an **existing network with a DHCP server** where you will install your FortiRecorder, FortiCam or third-party ONVIF cameras, and any other devices such as an access control system (ACS).

Like the other quick setup method, this deployment could be isolated from your office LAN. Often, however, the PoE switch is connected to an existing router, and the existing DHCP server also gives IP addresses to other existing devices on the same subnet.

The cameras get network settings from your DHCP server, but FortiRecorder does not. Like any server, FortiRecorder uses a static IP address so that its GUI or CLI can always be reached at the same location.



1. Use Ethernet cables to connect your DHCP server (and router, if any) to your power-over-Ethernet (PoE) switch.

   Your DHCP server must have a range of IP addresses (pool) that is larger than all of the devices that you will connect.
2. Use Ethernet network cables to connect the cameras to the switch.

   If you connected the cameras too soon, before a DHCP server was available, then they are using a default IP address. The default address will not work with your network. To fix this, unplug the cameras and then plug them in again. This reboots the cameras and requests a correct IP address from the DHCP server.
3. On your DHCP server, create a reservation for each camera so that it always gets the same IP address.

   Fortinet strongly recommends to either:

   - configure your cameras with a static IP address (see *Address*), or
   - configure your DHCP server with lease reservations

   Without reservations, the IP address provided by the DHCP server might appear to work initially, but later, when the DHCP lease expires, the DHCP server might change the IP address of the camera. DHCP servers do not notify FortiRecorder about the camera's new dynamic IP address. During this time, FortiRecorder will try to control the camera at its old IP address. This does not work. **Connections with that camera will be broken and all video from that camera could be lost during that interruption.** To fix this, create IP address reservations on your DHCP server and then update the camera's *Address* with its current IP address.
4. Use Ethernet network cables to **directly** connect port1 of FortiRecorder to your computer.

   Do not put your switch between them yet. FortiRecorder network settings are not configured yet.
5. Temporarily change your computer's IP address to be 192.168.1.98 with subnet 255.255.255.0. (If your computer has a static IP address, write it down so that you can restore the settings later.) Steps vary by whether you use Apple macOS, Linux, or Microsoft Windows.

   Alternatively, you can use a different IP address, but it must be on the same subnet as the default IP address of FortiRecorder port1: 192.168.1.0/24.

6. On your computer, open a web browser and go to:

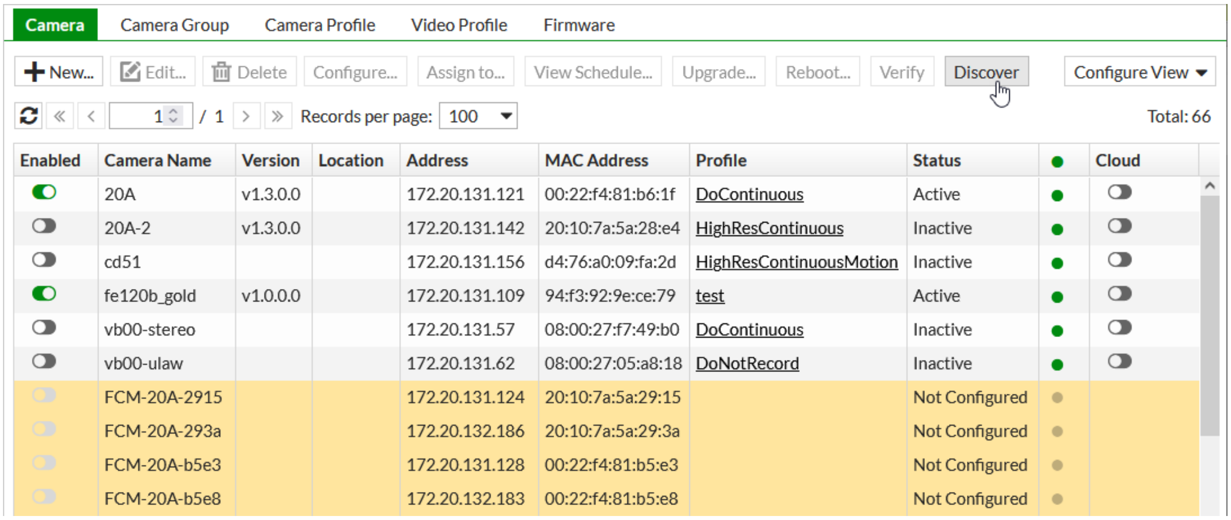
   https://192.168.1.99

   Log in with the name `admin` and no password.
7. Change the password. For details, see Setting the "admin" account password on page 25.
8. Configure port1:
   a. Go to *System* > *Network* > *Interface*.
   b. Select port1. Click the *Edit* button.
   c. Enable *Discover cameras on this port*.
   d. In *IP/Netmask*, enter the IP address and netmask that FortiRecorder will have on your network.

   > Do not use one of the range of IP addresses that the DHCP server assigns to cameras, computers, etc. (This can cause IP address conflict error messages.)

   e. Click *OK*.
9. Change your computer's IP address and subnet back to its original settings.
10. Unplug the Ethernet cable between your computer and FortiRecorder port1, and then plug them both into the switch.
11. In your web browser, go to the new IP address of FortiRecorder. Log in.
12. Discover and configure the cameras:
    a. Go to *Camera* > *Configuration* > *Camera*.
    b. Click the *Discover*button.

    After several seconds, a list of cameras appears.Newly discovered cameras are highlighted in yellow, and their *Status* column displays *Not Configured*.



Enabled	Camera Name	Version	Location	Address	MAC Address	Profile	Status	●	Cloud
●	20A	v1.3.0.0		172.20.131.121	00:22:f4:81:b6:1f	DoContinuous	Active	●	○
○	20A-2	v1.3.0.0		172.20.131.142	20:10:7a:5a:28:e4	HighResContinuous	Inactive	●	○
○	cd51			172.20.131.156	d4:76:a0:09:fa:2d	HighResContinuousMotion	Inactive	●	○
●	fe120b_gold	v1.0.0.0		172.20.131.109	94:f3:92:9e:ce:79	test	Active	●	○
○	vb00-stereo			172.20.131.57	08:00:27:f7:49:b0	DoContinuous	Inactive	●	○
○	vb00-ulaw			172.20.131.62	08:00:27:05:a8:18	DoNotRecord	Inactive	●	○
○	FCM-20A-2915			172.20.131.124	20:10:7a:5a:29:15		Not Configured	●	
○	FCM-20A-293a			172.20.132.186	20:10:7a:5a:29:3a		Not Configured	●	
○	FCM-20A-b5e3			172.20.131.128	00:22:f4:81:b5:e3		Not Configured	●	
○	FCM-20A-b5e8			172.20.132.183	00:22:f4:81:b5:e8		Not Configured	●	

    c. Double-click each camera to adjust its settings. For details, see Configuring cameras on page 50.

    Repeat this step for all cameras.
13. To verify that FortiRecorder is able to receive video from the camera, go to *Monitor* > *Video* > *Video*. You should be able to see the camera's live video feed.

Automatic provisioning

Especially if you have a large deployment with many stores or branch offices, and you deploy the same camera models in the same type of network at every site, then you can save time by using zero-touch automatic installation. This provides easy, consistent configuration and firmware updates for every site where you deploy FortiRecorder.

1. On a USB drive, format the disk as FAT32.
2. Put the files that you want to use for your deployment on the disk, such as:
   - License (`license.txt`)
   - FortiRecorder configuration (`frc_system.conf`)

     Use a plain text editor such as Notepad++ or Microsoft Visual Studio Code. Format the file using CLI syntax, the same as a configuration backup. To download a backup that you can use as an example, see Backups on page 148.
   - Site-specific FortiRecorder configuration (`localconfig.csv`)

     Some settings vary by site: the time zone, hostname that identifies which FortiRecorder sent an alert email, and the public network IP address or domain name for access from the Internet. Put them in this file so it's easier to focus on what you need to customize.

     Use a plain text editor such as Notepad++ or Microsoft Visual Studio Code, or a spreadsheet application such as Microsoft Excel. Formatting is comma-separated values (CSV), with the columns shown in the following example.

     ```
     # FortiRecorder provisioning CSV file,,,
     # Hostname,Public IP address/domain name,Time zone number,Automatically adjust clock
     for DST?
     ,,,
     FRC_123,192.168.1.10,15,1
     ```

     For the time zone number column, see the options in the GUI/CLI. For example, `15` is (GMT-5:00)Eastern Standard Time.

     For automatic clock adjustment for daylight savings time (DST), `0` is disabled; `1` is enabled.
   - Site-specific camera configuration (`camconfig.csv`)

     Similarly, each site might have different cameras or recording settings. Enter the columns shown in the following example.

     ```
     # Camera provisioning CSV file,,,,,
     # Name,Type,MAC address,Username,Password,Camera profile
     ,,,,,
     # 3rd party ONVIF cameras,,,,,
     camera_1,onvif,00:02:d1:89:a1:48,root,vivo1234,HighResContinuousMotion
     ,,,,,
     # Fortinet cameras,,,,,
     md40_1,,1c:c3:16:21:34:43,,,HighResContinuous
     md40_2,,20:10:7a:5a:28:d1,,,HighResContinuousMotion
     ```

     For the type column, `onvif` is a third-party camera; leave the field empty if the camera is from Fortinet.
   - Camera firmware (`image.out`)

   By default, provisioning is enabled with all of those files. If you don't want FortiRecorder to load all of them, then either:

- Delete the files that you don't want to use from the USB drive.
- On FortiRecorder, go to *System* > *Configuration* > *Provisioning* and disable those files.

3. Plug in the USB drive into the USB port of FortiRecorder.
4. Power on or reboot the FortiRecorder unit.
5. Repeat the previous two steps with each FortiRecorder unit.

Setup

If you did not use one of the quick setup scenarios — or later want to change settings — then you can use these instructions.

When you initially install FortiRecorder, or after a configuration reset or clean install, you must perform these **steps in order**:

1. Deployment topology on page 19
2. Connecting to the FortiRecorder GUI on page 22 or CLI
3. Setting the "admin" account password on page 25
4. Network settings, including:
    a. Configuring network interfaces on page 26
    b. Configuring routing on page 30
    c. Configuring DNS settings on page 32
    d. DHCP server settings, either:
        - Making reservations on your DHCP server on page 33
        - Configuring the built-in DHCP server on page 33
    e. (Remote network deployments) Firewall/router settings:
        i. Configuring NAT/port forwarding on your firewall/router on page 35
        ii. Configuring the public port numbers and domain name on page 37
5. (Optional) Configuring the system time on page 39
6. (Optional) Updating the firmware on page 39
7. Upload licenses on page 45
8. Plugging in the cameras on page 45
    a. (Remote network deployments) Discovering cameras in remote networks on page 46
9. Camera settings, including:
    a. (Optional) Configuring video profiles on page 46
    b. (Optional) Configuring camera profiles on page 48
    c. Configuring cameras on page 50

This results in a basic, functional configuration where you can log in and cameras are connected to FortiRecorder. **Optional steps can be skipped if you want to use factory default settings.**

If you want to add more administrator or user accounts, set up alert email, or configure more advanced settings, continue with More system settings on page 63.

Deployment topology

Cameras and other devices such as ACS can be deployed in networks that are:

- Hybrid with FortiCamera Cloud on page 20
- Local to FortiRecorder on page 21
- Remote from FortiRecorder on page 22

or a combination of them.

Do not plug in your cameras and FortiRecorder yet. Diagrams below are for comparison and planning purposes. Follow the order of steps in Setup on page 19.

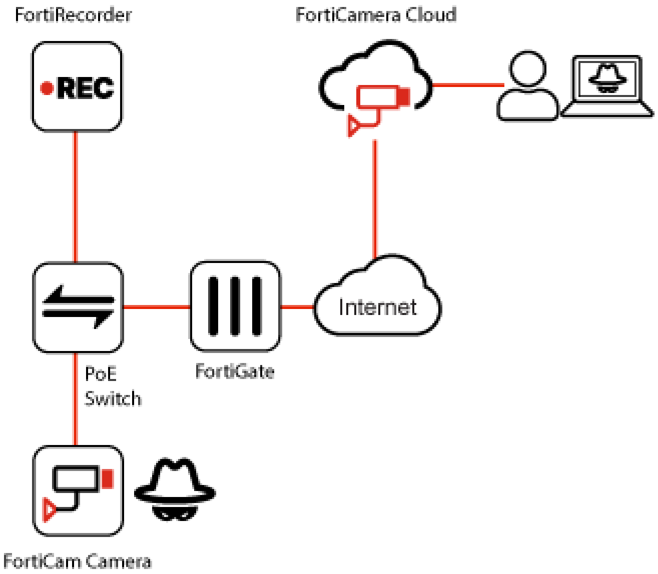
If you connected FortiCam cameras too soon, before a DHCP server was available, then they are using a default IP address.The default address will not work with your network. To fix this, unplug the cameras. Later, when indicated in Setup on page 19, you will plug them in again. This reboots the cameras and requests a correct IP address from the DHCP server.

Often there is a DHCP server on the LAN already, but if not, you do not need to deploy one. Use the built-in DHCP server on FortiRecorder instead. In their factory default state, FortiCam cameras automatically get network settings from a DHCP server during initial setup. Many third-party cameras require a DHCP server, too. Some third-party cameras have a default static IP address, however; these require you to manually configure the network settings through the camera's native GUI. Later, once connected, optionally cameras can be reconfigured to use a static IP address.

For Wi-Fi cameras, you will temporarily use an Ethernet cable during setup with FortiRecorder. Later, once setup is complete, you will disconnect and move the camera to its location on the Wi-Fi network. Power is then supplied by a PoE injector, not a physical connection through a PoE switch.

For external storage, Chromecast integration, and/or larger, more complex networks, you may need more network connections than the diagrams show, although the designs are similar.

Hybrid with FortiCamera Cloud

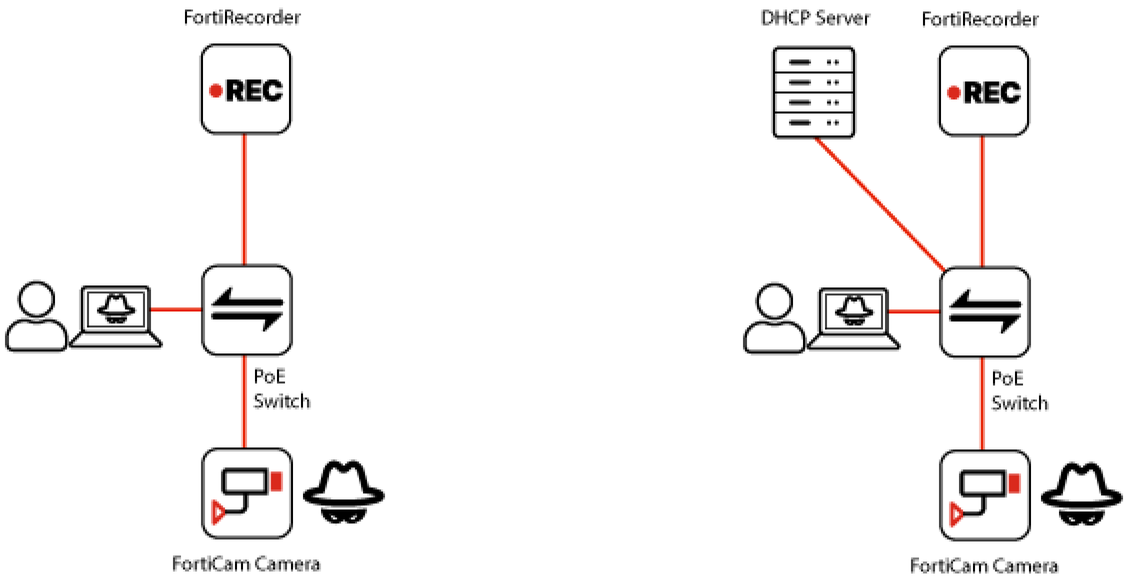


FortiCamera Cloud can be used together with FortiRecorder. You can use FortiCamera Cloud to configure most camera settings, and to monitor video from cameras, while FortiRecorder provides video storage and is used to configure remaining camera settings, if any. For details, see *Managed by cloud*.

This architecture scales well if your organization is adding small locations quickly. Each location can start with a cloud native FortiCam model connected to FortiCamera Cloud, and then later add FortiRecorder when more cameras need local storage, or for advanced features.

Topology is similar to remote networks, but once setup is complete, an administrator or operator usually logs in through FortiCamera Cloud — not FortiRecorder.

Local to FortiRecorder

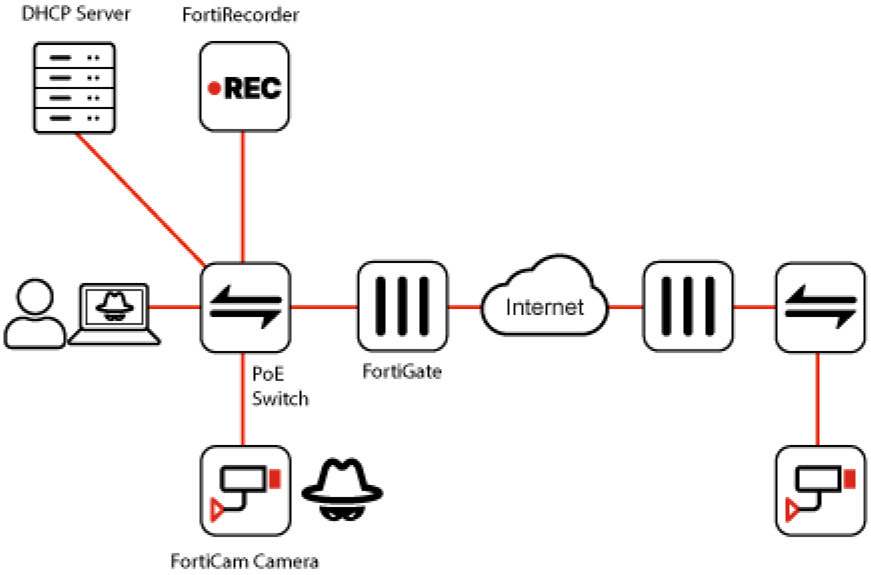


In a simple local deployment, cameras are installed on the same local network as FortiRecorder, with either:

1. No router or firewall between them
2. Router or firewall between them, but they do **no network address translation (NAT)/port forwarding**, such as a FortiGate operating in transparent mode or LANs joined via VPN

Often the switch is connected to a router, and devices connect through it to the Internet. However, this is not required unless you use camera or FortiRecorder features that require an Internet connection. See also Appendix A: Port numbers on page 174.

Remote from FortiRecorder



Remote camera deployment is when there is a firewall or router — perhaps many internal networks, or the Internet — between FortiRecorder and the cameras, ACS, and/or administrators and operators. Branch offices often use this design. Devices in your deployment will connect through either:

- secure tunnel (VPN)
- network address translation (NAT) and/or port forwarding

on the router or firewall.

To strengthen security, use a VPN — **not** NAT/port forwarding.

Communications include surveillance video and other sensitive information which could be intercepted or changed if it travels over untrusted networks such as the Internet. Remote access through NAT/port forwarding opens ports and can weaken the strength of your network security. To prevent attackers on the Internet from gaining access to your surveillance system, require authentication, use a firewall to restrict which IP addresses can use your port forward or virtual IP, and scan requests for viruses and hacking attempts.

For larger networks, VPN can be simpler than configuring NAT/port forwarding for many devices, too.

If you require remote access while you are out of the office, you can also use the VPN or VIP/NAT, connecting through the Internet to use the GUI or notification video clips.

Connecting to the FortiRecorder GUI

To configure the FortiRecorder appliance, you must connect to its management GUI or CLI console.

During initial installation, you can connect to the GUI using its factory default settings.

Default settings for connecting to the GUI

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

  HTML5 is supported. On most operating systems and browsers, the Apple QuickTime plugin is not required anymore. For details and a list of supported web browsers, see the FortiRecorder Release Notes.

To allow areas in the GUI to properly display, Fortinet recommends that you set your monitor to a screen resolution of at least 1280 x 1024 pixels.

To connect to the GUI

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 go to:

   https://192.168.1.99/

   Remember to include the "s" in "https://". By default, only HTTPS access to the GUI is enabled.
4. In the *Name* field, enter `admin` and then click *Login*.

   (There is no default password for the `admin` account.)

   Login credentials entered are encrypted before they are sent to the FortiRecorder appliance. The GUI appears if the login is successful.

Connecting to the FortiRecorder CLI

For initial installation, you can connect to the CLI from your management computer, either:

- **Through the network** — Connect your computer either directly (a peer connection) or through any network attached to one of the FortiRecorder unit’s network ports.
- **Locally** — Connect your computer directly to the FortiRecorder unit’s serial console port.

Local serial console connection is required if:

- Restoring the firmware. This utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process has completed, and therefore local serial access to the CLI is the only method that you can use.
- Installing your FortiRecorder unit for the first time, **only** if don't want to reconfigure your computer's network settings for a peer connection. (In its factory default settings, during initial setup, FortiRecorder is not yet configured to connect to your network. Peer connection is the only method that you can use until you configure the network interfaces.)

Command syntax for FortiRecorder is similar to other Fortinet products.

CLI connection via SSH

By default, SSH and HTTPS administrative access are enabled so that you can connect to the CLI during initial setup.

After initial setup, if you will connect using Telnet client, then enable SSH or Telnet on the network interface. If you will connect using the *Dashboard* > *Console* in the GUI, then enable HTTPS administrative access.

Requirements

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

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

To connect to the CLI using an SSH connection

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 and 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 PuTTY.
5. In *Host Name (or IP Address)*, type `192.168.1.99`.
6. In *Port*, type 22.
7. From *Connection type*, select *SSH*.
8. Click *Open*.

   The SSH client connects to the FortiRecorder unit. The SSH client might 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.

   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.
9. Type `admin` and press Enter twice. (In its factory default state, there is no password for this account.)

CLI connection via local serial console

Requirements

- 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 PuTTY

The following procedure describes connection using PuTTY. Steps may vary with other terminal emulators.

To connect to the CLI using a local serial connection

1. Using the console cable, connect the FortiRecorder unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start PuTTY.
3. In the *Category* tree on the left, go to *Connection* > *Serial* and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None

4. In the Category tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
5. Click *Open*.
6. Press the Enter key to initiate a connection.
   The login prompt appears.
7. Type `admin` and press Enter twice. (In the factory default state, there is no password for this account.)

Setting the "admin" account password

In its factory default configuration, FortiRecorder has one user account, named `admin`. This account has administrator permissions that grant full rights to the FortiRecorder appliance's settings and features—including to reset the password for other administrators. Its name and permissions cannot be changed.

In factory default configuration, for initial connection during setup, `admin` has no password.

Set a strong password for the account named `admin` when you log in for the first time. Change the password regularly. If you don't, unauthorized persons could log into FortiRecorder and compromise security.

If multiple people will use FortiRecorder, configure separate accounts for each person later, once setup is complete. See Configuring user and administrator accounts on page 63.

To change the "admin" administrator password

1. Log in to the `admin` administrator account.
2. Go to *System* > *Administrator* > *Administrator.*
3. Double-click the row for `admin`, or select it and then click the *Edit* button.
4. Click *Change Password* and enter the new password.

5. Log out.
   The new password takes effect the next time that you log in.

Configuring network settings

To connect with FortiRecorder, cameras, and other devices, you must configure network settings.

If you need to troubleshoot networking issues, see Connectivity issues on page 155.

Configuring network interfaces

Each of the FortiRecorder appliance's physical network adapter ports (or, for FortiRecorder-VM, vNICs) correspond to a logical network interface. By default, the network interfaces have these IP addresses and netmasks:

Network Interface*	Default 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 varies by model.	

If these IP addresses and subnets are not compatible with the design of your unique network, then you must configure them before you plug in port1, etc.

At least one network interface (usually port1) must be connected and configured so that you can connect to the FortiRecorder GUI and CLI.

Best practice is to connect cameras and other services (GUI/CLI, external file storage, etc.) on different network interfaces.For example, you could connect:

- port1 for administrator access
- port2 for cameras and ACS devices
- port3 for external file storage
- port4 for Internet access (time synchronization, FortiRecorder Mobile, etc.)

Isolate cameras and ACS devices from the Internet, or use a VPN, so that only FortiRecorder can control them. Live video streams may be lower quality or have choppy motion if cameras do not have constantly available bandwidth. A dedicated network connection only for cameras has many advantages:

- better security by preventing unauthorized access to cameras and video surveillance
- consistent quality of service for live video streams
- simpler bandwidth management

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. Expand the *Addressing Mode* section, and then select either:

Setting Name	Description
Manual	Manually assign an IP address and subnet mask to this network interface. Enter the IP address and netmask in *IP/Netmask*. IPv4 and IPv6 subnet masks should be provided in CIDR format. (For example, enter `/24`, not `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.**
DHCP	Automatically retrieve network settings from a DHCP server. Enable *Connect to server* to retrieve a DHCP lease when you save this configuration. If you want to also retrieve DNS and default route (gateway) settings, also enable *Retrieve default gateway and DNS from server*. ⚠ If an interface uses DHCP, and there are cameras connected to the interface, then you must configure an IP address reservation on the DHCP server so that the IP address will not change. FortiRecorder needs an IP address that does not change so that cameras can communicate with it reliably. ⚠ *Retrieve default gateway and DNS from server* will overwrite the existing DNS and default route, if any.

5. Expand the *Advanced Setting* section, and then configure the following settings:

Setting Name	Description
Discover cameras on this port	Enable to send multicast camera discovery traffic from this network interface.You can also discover cameras on other subnets. See Discovering cameras in remote networks on page 46.
Access	Enable the types of administrative access that you want to permit to this interface. ⚠ 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.

Setting Name	Description
Access: HTTPS	Enable to allow secure HTTPS connections to the GUI through this network interface. To configure the listening port number, see Configuring the public port numbers and domain name on page 37. To upload a certificate, see Replacing the default certificate for the GUI on page 93.
Access: PING	Enable to allow: • ICMP type 8 (`ECHO_REQUEST`) or type 30 • UDP ports 33434 to 33534 for ping and traceroute to be received on this network interface. When it receives an `ECHO_REQUEST`, FortiRecorder will reply with ICMP type 0 (`ECHO_RESPONSE`). Disabling PING only prevents FortiRecorder from receiving ICMP type 8 (`ECHO_REQUEST`) or type 30 and traceroute-related UDP. It does not disable FortiRecorder CLI commands such as `execute ping` or `execute traceroute` that send such traffic.
Access: HTTP	Enable to allow HTTP connections to the GUI through this network interface. To configure the listening port number, see Configuring the public port numbers and domain name on page 37 . HTTP connections are not secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: SSH	Enable to allow SSH connections to the CLI through this network interface.
Access: SNMP	Enable to allow SNMP queries to this network interface, if queries have been configured and the sender is a configured SNMP manager. To configure the listening port number and configure queries and traps, see Configuring SNMP traps and queries on page 82.
Access: TELNET	Enable to allow Telnet connections to the CLI through this network interface. Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiRecorder appliance.
Access: FRC-Central	Enable to allow access from FortiCentral installations. See also the FortiCentral User Guide.

Setting Name	Description
Access: RTSP	Enable to allow live video streams from cameras.
MTU	Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiRecorder unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value. For example, RFC 2516 prescribes a value of 1492 for PPPoE. This option is available only for network interfaces that are directly associated with a physical link.
Administrative Status	Select either: • *Up* — Enable (that is, bring up) the network interface so that it can send and receive traffic. • *Down* — Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

6. Click *OK*.

   If you were connected to the GUI through this network interface, you are now disconnected from it.

7. To access the GUI again, in your web browser, modify the URL to match the new IP address of the network interface. For details, see Connecting to the FortiRecorder GUI on page 22.

Creating FortiRecorder logical interfaces

If you have a more complex network, then in addition to the physical network interfaces, you can create a logical interfaces on FortiRecorder. Go to *System* > *Network* > *Interface* and click *New*.

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 a FortiRecorder, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to provide 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.

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

- a physical interface, not a VLAN interface
- not already part of a redundant interface
- has no defined IP address and is not configured for DHCP
- does not have any VLAN sub-interfaces

When a physical interface is included in a redundant interface, it is not listed on *System* > *Network* > *Interface*. 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.

The loopback interface is useful when you use an OSI Layer 2 load balancer in front of several FortiRecorder devices. 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 routing

If one or more routers is between FortiRecorder and the Internet, your cameras, etc., then you must specify which is the default route ("gateway" router) that network traffic from FortiRecorder uses to reach other parts of your network.

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.

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 (for example, dual Internet/WAN links), or a larger network with multiple routers (each of which should receive packets destined for a different subset of IP addresses), then you might need to configure multiple static routes.

1. Log in to the `admin` administrator account.

   Other accounts might not have the permissions required to change this setting.
2. Go to *System > Network > Routing*.
3. Click *New*.
4. Configure the following settings:

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

5. Click *OK*.
6. If you are moving FortiRecorder to connect through a different router in your network, then re-connect it at the intended location now. (Connections through the previous gateway will fail until you do this.)

   The FortiRecorder appliance should now be reachable to networks indicated by the mask.
7. To verify connectivity, from a computer on the route's network destination, attempt to ping one of the network interfaces of FortiRecorder that should be reachable from that location. If the connectivity test fails, you can use the CLI commands to determine if a complete route exists from the FortiRecorder to the host:

   ```
   execute ping <destination_ipv4>
   ```

   and to determine the point of connectivity failure:

   ```
   execute traceroute <destination_ipv4>
   ```

   See also Examining routing on page 157.

Configuring DNS settings

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.

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 might not have permissions necessary to change this setting.
2. Go to *System* > *Network* > *DNS*.
3. Enter the IP addresses of a primary and secondary DNS server.

   Your Internet service provider (ISP) might provide IP addresses of DNS servers, or you might 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.
4. Click *Apply*.
5. 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 configured routes. See also Configuring routing on page 30.
6. 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 IP address, routing, and that your firewalls or routers do not block or proxy UDP port 53.

Making reservations on your DHCP server

If your cameras get their network settings from a third-party DHCP server, then reserve the range of IP addresses that the cameras will use so that other devices cannot take them. Bind each IP address to a specific camera's MAC address. For details, see the documentation for your DHCP server.

DHCP IP address reservations have important benefits:

- Avoiding IP address changes, which disrupts live video streams, recordings, and FortiRecorder connections with the camera until you update *Address* to match the new IP address
- Preventing that IP address from being re-assigned to another device when the current DHCP lease expires
- Mimic a static IP address, yet still provide the benefit that IP addresses are still centrally managed on your DHCP server

FortiRecorder attempts to keep track of any DHCP-related IP address changes automatically by periodically sending DNS probes. However this requires that the camera is on the same subnet as FortiRecorder. If cameras are on remote networks, then this does not work; DHCP reservations are required.

Reserved leases cannot prevent misconfigured computers from using the same IP address, causing an IP address conflict, and breaking the connection of FortiRecorder with the camera. See Resolving IP address conflicts on page 163.

Configuring the built-in DHCP server

If you do not have a DHCP server on your network, FortiRecorder has a built-in DHCP server and can assign IP addresses to your cameras and other devices. Configure the DHCP server on the interface that the cameras connect to, and then configure the cameras to use DHCP to get their network settings. See also Configuring cameras on page 50.

To configure the DHCP server on FortiRecorder via the GUI

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

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

Setting Name	Description
DNS server 1	Type the IP address of a DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if *DNS options* is set to *Specify*.
DNS server 2	Type the IP address of an alternative DNS server that DHCP clients can use to resolve domain names. For performance reasons, if you have one, it is preferable to use a DNS server on your local network. This setting is available only if *DNS options* is set to *Specify*.
Domain	Optional. Type the domain name, if any, that DHCP clients will use when resolving host names on the local domain.
Netmask	Type the subnet mask that DHCP clients will use in conjunction with the IP address that is assigned by the DHCP server on FortiRecorder.
Conflicted IP timeout (Seconds)	Type the maximum amount of time that the DHCP server will wait for an ICMP `ECHO` (ping) response from an IP before it determines that it is not used, and therefore safe to allocate to a DHCP client that is requesting an IP address. The default is 1800 seconds (3 minutes). To ensure that the DHCP server does not cause IP address conflicts with misconfigured computers that are accidentally using the pool of IP addresses used for DHCP, when a client request a new DHCP lease, the built-in DHCP server will ping an unused IP address in the pool first. If the ping test is successful, then a misconfigured computer is currently using that IP, and allocating it also to the DHCP client would cause an IP address conflict. To prevent this, the DHCP server will temporarily abandon that IP (mark it as used by a static host) and look for an other, available IP to give to the DHCP client. (It will not try abandoned IP addresses again until the pool is exhausted.) However, before the DHCP server can determine if the ping test is successful, the it must first wait to see if there is any reply. This slows down the search for an available IP address, and in rare cases, could cause a significant delay before the DHCP client receives its assigned IP address and other network settings. If your network is smaller or typically has low latency to ping replies, you can safely decrease this setting's value to improve DHCP speed and performance. In most cases, 3 seconds is enough.
Lease time (Seconds)	Type the maximum amount of time that the DHCP client can use the IP address assigned to it by the server. When the lease expires, the DHCP client must either request a new IP address from the DHCP server or renew its existing lease. Otherwise, the DHCP server may attempt to assign it to the next DHCP client that requests an IP. The default is 604800 seconds (7 days). 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 IP addresses 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.

Setting Name	Description
DHCP IP Range	To configure the DHCP lease pool — the range of IP addresses that the DHCP server can assign to its clients — click *New* and configure the first and last IP address in the range. To avoid DHCP pool exhaustion that can occur in some cases, the pool should be slightly larger than the total number of clients. If you need to exclude some IP addresses from this range (for example, printers permanently occupy static IP addresses in the middle of the range), also configure *DHCP Excluded Range*. The built-in DHCP server can provide IP addresses to the computers on your network too, not just to cameras.
DHCP Excluded Range	To configure IP addresses that should be omitted from the DHCP pool and never given to DHCP clients (such if there are printers with manually assigned static IP addresses in the middle of your DHCP range), click *New*.
Reserved IP Address	To bind specific device to a specific DHCP IP address lease, ensuring that the DHCP server will not assign it to another DHCP client, click *New* and enter the device's MAC address. 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. Reserved leases cannot prevent misconfigured computers from using the same IP address, causing an IP address conflict, and breaking the connection of FortiRecorder with the camera. See Resolving IP address conflicts on page 163.

5. Click *Create*.

   As cameras join the network, they appear on *Monitor > DHCP > DHCP*.

Configuring NAT/port forwarding on your firewall/router

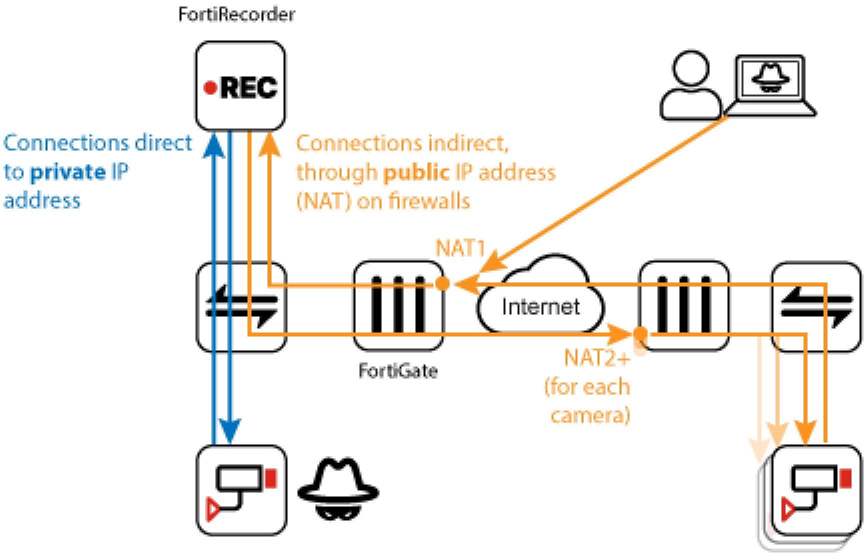
If your deployment:

- includes a remote network, and
- VPN is **not** used to connect the local and remote networks

then on your office's FortiGate, third-party firewall, or Internet router, you must configure:

- NAT and/or
- port forwarding

to accept and forward incoming connections from an external/**public** IP address on the firewall/router to the internal/**private** IP address of FortiRecorder.


FortiRecorder
●REC
Connections direct to private IP address
Connections indirect, through public IP address (NAT) on firewalls
NAT1
Internet
FortiGate
NAT2+ (for each camera)

For each NAT/port forward, the IP address that receives connections is either the:

- IP address on the office WAN or Internet router
- IP address of the external interface on a firewall

Similarly, communications in the opposite direction — from FortiRecorder to cameras etc. — also require NAT and/or port forwarding. If you have multiple remote devices, then configure one for each device that needs to receive connections from FortiRecorder.

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:

https://ping.eu/

Port numbers on the external IP address can be either be forwarded from the same as the listening port numbers as FortiRecorder, or translated from a different port number.

On FortiGate, NAT and port forwarding are done by a virtual IP (VIP) address. For example, if port2 is attached to the Internet, then you configure a VIP on port2 to forward connections to the internal IP address and port numbers of FortiRecorder. For details, see Appendix A: Port numbers on page 174 and the FortiGate Administration Guide or other documentation for your firewall/router.

NAT and port forwarding are usually required for remote networks that use IPv4, but **not** IPv6. If you only use IPv6, you may be able to skip this step.

Once you have configured NAT and/or port forwarding on your firewall/router, you must configure FortiRecorder and your remote devices to use it. Continue with Configuring the public port numbers and domain name on page 37. Later, you will also configure NAT and/or fort forwarding (*Address mode*) for each remote camera.

Configuring the public port numbers and domain name

If you configured a NAT/port forward address on your firewall/router, then you must configure FortiRecorder to use it. FortiRecorder uses the external-facing address and port number in features such as notifications. For example, notification email about motion detection contains a hyperlink with the *Public Access Host name* and *Access Ports Service* (*Public* port number), like this:

```
https://nvr.example.com:1443/admin/AdminLogin.html?nid=123...
```

Due to this, when you are out of the office, you can click the link regardless of where you are on the Internet, and be able to watch the motion detection clip on FortiRecorder.

Miscellaneous settings (for example, password strength and idle timeout for local administrator accounts) are also available on this page of the GUI.

1. On FortiRecorder, go to *System* > *Configuration* > *Options*.
2. Configure the following settings:

Setting Name	Description
Idle timeout	Enter the amount of time that a user may be inactive before the FortiRecorder unit automatically logs out the user. For better security, use a low idle timeout value.
Login disclaimer	Enter text that you want to prompt the user to agree, such as an IT policy or legal disclaimer, then also configure when to display it: • *Display pre-login banner* • *Display post-login banner*
Display pre-login banner	Enable to display the text in *Login disclaimer* before the login dialog.
Display post-login banner	Enable to display the text in*Login disclaimer* after the login dialog, but before the GUI menu or CLI command prompt appears.
Password Policy	
Minimum password length	Enter the minimum number of characters that a password must contain. The default value is 8. If any password does not meet the requirements, FortiRecorder requires that user to change the password during the next login. Set a strong password policy, especially for administrator accounts. If you don't, unauthorized persons could log into FortiRecorder and compromise security. Short, simple, and easily-guessed passwords are a security risk.

Setting Name	Description
	These password policy settings only apply to accounts that are local (defined on FortiRecorder). See also Configuring remote authentication on page 68.
Password must contain	Select your password complexity requirements: • *Uppercase letter* • *Lowercase letter* • *Number (0-9)* • *Non alphanumeric character*: Any special character that is not a letter of the US-ASCII alphabet or a number, such as an exclamation mark (`!`) or tilde (`~`). If any password does not meet the requirements, FortiRecorder requires that user to change the password during the next login.
Allow empty password	Enable to ignore *Minimum password length* and *Password must contain* and allow empty passwords. ⚠ Empty passwords effectively disable authentication, and are a security risk. Only enable this setting if: • FortiRecorder is on an isolated network (not accessible from the Internet or office LAN) • access is physically restricted to authorized persons If you don't, unknown and unauthorized persons could log into FortiRecorder and compromise security.
Public Access Host name	If you configured NAT on a firewall/router (see Configuring NAT/port forwarding on your firewall/router on page 35), then type either an: • IP address • fully qualified domain name (FQDN), such as `nvr.example.com`, that Internet DNS servers can resolve into the above IP address Devices on remote networks or the public Internet will connect through this address on the firewall/router for communications to the FortiRecorder. This hostname may be different than the one in *Host name*.
Access Ports Service	For each network service (HTTPS etc.), configure: • *Local*: Type the listening port number on FortiRecorder. Devices on the internal/private network connect directly to this port number. • *Public*: If you configured port forwarding on a firewall/router (see Configuring NAT/port forwarding on your firewall/router on page 35), then type the external/public port number on your firewall/router that forwards communications to the FortiRecorder port number in *Local*. Devices on remote networks or the public Internet will connect through this public port number on the firewall/router for communications to the FortiRecorder. If you do **not** use port forwarding, then keep *Public* the same as *Local*. By default, each service (protocol) on FortiRecorder uses IANA standard port numbers. See also Appendix A: Port numbers on page 174.

Setting Name	Description
	The *FRC-Central* port is used by both FortiCentral and FortiRecorder Mobile app.

3. Click *Apply*.

Configuring the system time

For many features to work, including video timestamps, scheduled recording, logging, and SSL/TLS-dependent features, the FortiRecorder system time must be accurate. Once setup is complete and cameras have been connected, FortiRecorder synchronizes the clocks of cameras with its own in order to keep them in agreement.

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. Adjust your firewall, if any, to allow these connections. See also Appendix A: Port numbers on page 174.

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*.)

Updating the firmware

The FortiRecorder appliance is shipped with the latest operating system (firmware); however, if a new version has been released since your appliance was received, install the latest firmware before continuing the installation of your FortiRecorder.

Camera firmware can be updated later, after you have connected your cameras to the appliance.

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

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.

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

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

Installing firmware

You can use either the GUI, the CLI, or USB drive (see Automatic provisioning on page 17) to upgrade or downgrade the FortiRecorder appliance's operating system.

Firmware changes are either:

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

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

For example, if your current firmware version is:

```
FortiRecorder-400D v7.0.2, build069, 2023.08.02
```

changing to

```
FortiRecorder-400D v7.0.1, build066, 2023.06.28
```

an earlier version number (7.0.1), build number (66), and date (`2023.06.28` means June 28, 2023), 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. See Backups on page 148.

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

To install firmware using the GUI

1. Download the firmware file from the Fortinet Technical Support web site:
   https://support.fortinet.com/
2. On the FortiRecorder appliance, log into the GUI as the `admin` administrator.
3. Go to *Dashboard* > *Status*.
4. In the *System Information* widget, in the *Firmware version* row, select *Update*.
   The *Choose Firmware* dialog appears.
5. 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. See also Restoring a previous configuration on page 150.

7. Clear the cache of your web browser and restart it to ensure that it reloads the GUI 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 GUI and go to *Dashboard* > *Status*. In the *System Information* widget, the *Firmware version* row indicates the currently installed firmware version.
9. If you want to install alternate firmware on the secondary partition, follow Installing alternative firmware on page 42.
10. Continue with Setting the "admin" account password on page 25 .

To install firmware using the CLI

1. Download the firmware file from the Fortinet Technical Support web site:

   https://support.fortinet.com/
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
4. Connect port1 of the FortiRecorder appliance directly or to the same subnet as a TFTP server.
5. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the administrator named `admin`.
6. Start your TFTP server. (If you do not have one, you can temporarily install and run one such as tftpd (Windows, macOS, 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 disable TFTP 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
   - `<tftp_ipv4>` is the IP address of the TFTP server

   For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   One of the following message appears:

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

-
  ```
  Get image from tftp server OK.
  Check image OK.
  This operation will downgrade the current firmware version!
  Do you want to continue? (y/n)
  ```

9. Press `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 the FortiRecorder GUI on page 22 and, if you want to restore the configuration, Restoring a previous configuration on page 150 .

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 alternative firmware on page 42.
12. Continue with Setting the "admin" account password on page 25 .

Installing alternative firmware

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

To install alternate firmware via the CLI

1. Download the firmware file from the Fortinet Technical Support web site:

   https://support.fortinet.com/
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
4. Connect port1 of the FortiRecorder appliance directly or to the same subnet as a TFTP server.
5. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the `admin` administrator.

   For details, see Connecting to the FortiRecorder CLI on page 23 .
6. Start your TFTP server. (If you do not have one, you can temporarily install and run one such as tftpd (Windows, macOS, 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. Press `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. Press `B`.

    The FortiRecorder appliance saves the backup firmware image and restarts. When the FortiRecorder appliance reboots, it is running the primary firmware.

Booting from the alternate partition

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

To boot into alternative firmware through the local console CLI

1. Install firmware onto the alternate partition (see Installing alternative firmware on page 42).
2. Connect your management computer to the FortiRecorder console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a connection from your management computer to the CLI of the FortiRecorder appliance, and log in as the `admin` administrator.
4. Enter the following command to restart the FortiRecorder appliance:

   ```
   execute reboot
   ```
5. As the FortiRecorder appliances starts, a series of system startup messages appear.

   ```
   Press any key to display configuration menu........
   ```

   Immediately press a key to interrupt the system startup.

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

   If you successfully interrupt the startup process, the following messages appears:

   ```
   [G]: Get firmware image from TFTP server.

   [F]: Format boot device.

   [B]: Boot with backup firmware and set as default.

   [Q]: Quit menu and continue to boot with default firmware.

   [H]: Display this list of options.

   Enter G,F,B,Q,or H:

   Please connect TFTP server to Ethernet port "1".
   ```
6. Press `B` to reboot and use the backup firmware.

Upgrading or downgrading camera firmware

Once the FortiRecorder is connected to your cameras, you can upgrade and downgrade the camera firmware through the FortiRecorder GUI.

Fortinet does not recommend downgrading firmware. Downgrading firmware could result in a loss of configuration information. If possible, back up the configuration before you downgrade.

To upgrade or downgrade a camera's firmware

1. Download the firmware file from the Fortinet Technical Support web site:
   https://support.fortinet.com/
2. Go to *Camera* > *Configuration* > *Firmware*.
3. Click the *Upload* button and select the camera firmware file.
   After the firmware is successfully uploaded, the *Availability* column indicates *Local*.
4. Go to *Camera* > *Configuration* > *Camera*.
5. Select one or more cameras that you want to upgrade or downgrade, and then click the *Upgrade* button.
6. 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 cannot record video if it was scheduled, so there is a gap in the recorded video.

Upload licenses

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

1. Go to *Dashboard* > *Status*.
2. In the *License Information* widget, click *Update*. Find and upload the license file.
   FortiRecorder validates the license and updates the license status on the dashboard. If you uploaded a face recognition AI license, validation requires an Internet connection. See also Appendix A: Port numbers on page 174.
3. Repeat the previous step if you need to upload more licenses.

Plugging in the cameras

Use Ethernet network cables to connect the cameras to the same switch as FortiRecorder, as shown in Deployment topology on page 19.

If you connected the cameras too soon, before a DHCP server was available, then they are using a default IP address.The default address will not work with your network. To fix this, unplug the cameras and then plug them in again. This reboots the cameras and requests a correct IP address from the DHCP server.

If you cannot plug cameras into the same switch (for example, if you later add cameras at a branch office):

1. Verify that a DHCP server is available on the remote network.
2. Plug in cameras at the remote network, as shown in Remote from FortiRecorder on page 22.
3. Trigger a discovery scan of the DHCP IP address range on the remote network so that FortiRecorder can find the remote cameras. See Discovering cameras in remote networks on page 46.

Discovering cameras in remote networks

During initial setup, FortiRecorder automatically discovers cameras that are connected to the **same subnet**. You don't need to manually run a discovery scan if you only have local cameras.

Later, if you add more cameras on a remote network or **different subnets** of the local network, then you can still add them to FortiRecorder. Either:

- Go to *Camera* > *Configuration* >*Camera* and click *New* to manually add a camera
- Trigger a discovery scan for FortiRecorder to find cameras

Discovery scans are useful if you have many remote cameras, or if they used DHCP and you don't know which IP address they currently have. FortiRecorder can find cameras in a range of IP addresses, regardless of subnet.

1. Go to *System* > *Network* > *Discovery*.
2. Click *Enable*.
3. Click *New*.
4. Enter a subnet.

   You can enter the subnet in either a numerical range or classless (CIDR) format.

   For example, you might enter `172.20.1.100-172.20.1.200`, or `172.20.1.0/24`.
5. Click *Apply*.
6. Go to *Camera* > *Configuration*.
7. Click *Discover*.

   FortiRecorder starts to scan for cameras. Discovered cameras appear on *Camera* > *Configuration* >*Camera*. Time required varies by the size of the IP range, and how quickly cameras respond.

   If remote cameras do not appear, verify that FortiRecorder can connect to the remote network.

Configuring cameras

Camera configuration includes configuration of the cameras themselves, but also related settings such as video recording and storage settings.

Configuring video profiles

Video profiles define the video quality that you want cameras to use when they record or stream live video to FortiRecorder. If you want to use a factory default profile (for example, `high-resolution`), then you can skip this step during initial setup. Otherwise you can configure profiles with your custom settings.

Video profiles are used in camera profiles. For details, see Configuring camera profiles on page 48.

Better video quality consumes more network bandwidth and more disk space. If you need to retain video for a long time, or have a slow network, then you might need to reduce the video quality until you reach acceptable network performance or disk usage.

To configure a video profile

1. Go to *Camera* > *Configuration* > *Video Profile*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Type a name (such as `live-stream1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Codec	Select the video compression format, such as H.264 AVC or H.265 HEVC.
Resolution	Select the amount of detail (the number of pixels) in the image. from the drop-down menu. Lower resolutions have 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. High resolution can significantly reduce performance and increase network bandwidth and disk space usage.
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 space usage and CPU usage.
Group of pictures	Select from the drop-down menu the duration of a group of pictures (GOP) sequence. A GOP sequence is the interval between frames that contain the full image. Longer intervals save bandwidth, but slightly delay the start of live video streams.
Bitrate mode	Select the bit rate: • *Variable* — Automatically adjust the stream to the minimum bit rate required by the current video frames while maintaining video quality. In variable bitrate mode the camera lowers the bitrate dynamically when little motion is present. This setting increases the presence of noise. • *Fixed* — Manually specify a constant bit rate in *Bit rate*. In fixed bitrate mode the camera attempts to keep the bitrate constant at the configured level. This guarantees calculated video retention time and bandwidth but might reduce image quality if. for example, if there is a sudden burst of motion, like rain or flashing lights. • *Constrained* — Automatically adjusts the stream to lower the bitrate usage during periods of low activity, while enabling the ability to set the maximum bitrate the camera can stream.

Setting Name	Description
Max bitrate	Enter the maximum bitrate that the camera can stream. Lower bitrates use less bandwidth by sacrificing image quality. This setting is only available when *Bitrate mode* is *Constrained*.
Quality	Select the degree of compression. Greater compression reduces required network bandwidth but causes greater CPU usage.
Audio	Enable or disable audio.

4. Click *Create*.

Configuring camera profiles

Camera profiles define which video profile to use, video storage options, and recording schedules (either continuous or motion detection) for the cameras that use the profile. If you want to use a factory default profile (for example, `DoContinuous`), then you can skip this step during initial setup. Otherwise you can configure profiles with your custom settings.

Camera profiles are used by cameras. For details, see Configuring cameras on page 50.

To configure camera profiles

1. Go to *Camera* > *Configuration* > *Camera Profile*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Enter a name (such as `camera-settings1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
Video	From *Recording stream profile*, select the video profile that defines the quality of the recorded video. See also Configuring video profiles on page 46. From *Viewing stream profile*, select the video profile that defines the quality of the video when viewing a live stream. Click *Add schedule* to select the schedule that defines when to use low or high quality video. See also Schedules on page 119. For example, you could improve the camera's performance at night without sacrificing the quality of video during the day. Better video quality will use more bandwidth and disk space.
Recording	Select what triggers the camera to begin recording. • *Continuous*: Records video for the entire duration of the schedule, regardless of movement or any other triggers.

Setting Name	Description
	• *Motion detection*: Records a video clip up to about 40 seconds long each time the camera's sensor detects movement. • *Digital input*: Records a video clip up to about 40 seconds long each time the camera receives a trigger from the digital input. This option only takes effect if the camera supports DIDO. • *Audio detection*: Records a video clip up to about 40 seconds long each time the camera detects sound. You can define the sound detection sensitivity when configuring camera settings. • *PIR detection*: PIR based motion detection senses the movement of people, animals, and other objects that produce heat energy. These recording storage options are available: • *FortiRecorder*: Store your recorded video on the FortiRecorder • *SD card*: Store your recorded video on the camera's SD card (also called "edge recording"). Recording types vary by camera model. If you want to use different recording types at different times, click *Add schedule* to specify them. For example, you could instruct the camera to start recording for motion detection during the day and PIR detection at night.
Edge Download	Enable to download video recordings from the camera's SD card to FortiRecorder local or remote storage. When the download occurs varies by whether *Recording* is *Continuous* or *Motion detection*.
Storage Options	From *Continuous recordings* and *Detection recordings*, select the storage strategy: • *Keep until overwritten*: Retain video until all available disk space, both local and remote, is almost full. Then the oldest video will be overwritten. • *Delete*: Remove video when it exceeds the specified maximum age, or if the disk is full. • *Move*: Move video to external storage when it exceeds the specified maximum age, or if the disk is full. In the *After n* options that appear, select the age threshold that will cause FortiRecorder to move the video clips to external storage. This option applies only if you have configured remote storage. • *Use continuous recordings if available*: Marks the time ranges of motion detection inside of continuous recordings instead of storing them as separate video files. This reduces CPU load, but does not allow continuous recordings to be deleted and only keeps the section of video that was marked by motion detection for a period of time. This option is only available in the *Detection recordings* dropdown list. Recordings are stored on the hard disk as multiple video files. The oldest part of the recording is deleted or moved first. If remote storage is configured, video is first stored on the local disk, then transferred to remote storage when the local disk needs space for newer video. When the remote disk is full too, the video will finally be deleted from it.

Setting Name	Description
Compression Options	Select whether or not FortiRecorder compresses continuous recordings. If you select *Compress*, then 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. Selecting *Compress* will reduce disk space usage, but can also reduce video quality.

4. Click *Create*.

Configuring cameras

Most settings for local cameras are automatically retrieved during discovery, so usually, you are not required to configure them. However, you might need to configure camera settings if:

- You want to adjust camera settings.
- You add a camera on a remote network, and did not use remote camera discovery.
- You want to configure a new camera **before** you connect it to FortiRecorder.
- The *Status* column indicates *Not Configured*.

Features vary by camera vendor and model. Therefore many settings only appear after you configure *Model* or FortiRecorder discovers the camera, so that it knows which options are supported. If a setting is not visible, then the setting is not supported by that model.

If FortiRecorder is in a hybrid deployment with FortiCamera Cloud, then many camera settings described in this section must be configured on FortiCamera Cloud — **not**FortiRecorder. For details, see *Managed by cloud*.

If you have many cameras, it may be useful to filter the list of cameras to focus on specific statuses, vendors, models, or locations. To do this, from the *Configure View* drop-down list, select *Show and Hide Columns* and then enable or disable each column. If you want the filter to persist for every time that you view the list of cameras, then from the *Configure View* drop-down list, select *Save View*.

To configure cameras

1. Go to *Camera* > *Configuration* > *Camera*.
2. Either:
   - double-click the row of a discovered camera, or
   - click *New* (to configure a camera that is not yet discovered yet)
3. Configure the following settings:

Setting Name	Description
Enable	Select this toggle to enable the FortiRecorder unit to communicate with this camera.

Setting Name	Description
	If a camera is disabled while you change its settings, or when it would normally be scheduled to begin continuous or motion detection recording, then FortiRecorder will not connect to the camera. **This can break communications between them:** if you reconfigure the camera's IP address while the camera is disabled, your FortiRecorder may later attempt to communicate with the camera at the new IP address or gateway, but the camera will still be using the old address or 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.
Name	Type a name (such as `front-door1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. 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.
Vendor	The vendor company and camera model. If you are configuring a discovered camera, this and other camera information was automatically retrieved. You do not need to configure it. To refresh the information, you can click *Camera detail*. If you are adding a new camera **before** it is connected or discovered, then you must configure these and other settings manually. For Fortinet FortiCam cameras, you must specify the models; for third-party cameras, you must specify the camera's login credentials (user name and password) so that FortiRecorder can connect to it.
Model	
Address mode	Select how the camera is connected to FortiRecorder in your deployment topology: • *Wired*: On the **same** (local) network or directly attached, through a Ethernet cable. • *Wireless*: On the **same** network, through Wi-Fi. This setting is not available on all camera models. • *VIP*: On a **different** (remote) network, through NAT and/or port forwarding, such as through the Internet or your office's WAN. To specify this connection, you must configure *Address*, *(HTTPS) Port*, and *(RTSP) Port*.
Address	If *Address mode* is *VIP*, then type either an: • IP address • fully qualified domain name (FQDN), such as `camera.example.com`, that Internet DNS servers can resolve into the above IP address that FortiRecorder will connect through for communications to the camera.

Setting Name	Description
	This setting is available only when *Address mode* is *VIP*.
(HTTPS) Port	Enter the port number of configuration communications to the camera. If the VIP/NAT on the router or firewall does not do port forwarding or port translation, then keep this setting at its default value, 443. This setting is available only when *Address mode* is *VIP*.
(RTSP) Port	Enter the port number of video streaming commands (RTSP) to the camera, such as when beginning a continuous recording schedule. If the VIP/NAT on the router or firewall does not do port forwarding/translation, keep this setting at its default value, 554. This setting is available only when*Address mode* is *VIP*.
Transport Type	Select the transport layer protocol for video streaming from the camera to FortiRecorder. By default, RTSP communications between the camera and FortiRecorder are transported over UDP. If your router or firewall requires it, you can instead use TCP, HTTP tunneling, or HTTPS (secure/encrypted) tunneling.
Profile	Either click *New* or select the camera profile that indicates the recording schedule, video quality, and other settings that this camera will use. See Configuring camera profiles on page 48.
Managed by cloud	Enable if this camera will be managed through FortiCamera Cloud. If FortiRecorder is in a hybrid deployment with FortiCamera Cloud, then many camera settings must be configured on FortiCamera Cloud — **not** FortiRecorder, except: • local network connection settings, including transport protocol between the camera and FortiRecorder • management via third-party ONVIF GUI or FortiRecorder • smart DNR settings • audio input settings • power frequency settings • status (enable/disable camera, which disconnects it from FortiCamera Cloud)

4. If the camera supports Wi-Fi, and you want it to connect to FortiRecorder through a wireless router, expand the *Wifi* section and configure the following settings:

Setting Name	Description
Enable	Enable Wi-Fi on the camera. When enabled, these indicators appear: • *Status* • *Signal strength*
SSID	Enter the SSID of the Wi-Fi access point (AP) that the camera will connect to.

Setting Name	Description
Security	Select the type of Wi-Fi encryption: • *None* • *WPA personal* • *WPA2 personal* • *WPA enterprise* • *WPA2 enterprise* When you select an encryption type, its related settings appear, such as: • *WPA encryption* (TKIP or AES) • *WPA username* • *WPA password* or *WPA passphrase* To strengthen security, select WPA2 enterprise or personal. For details, see your FortiAP/FortiWifi or third-party product documentation.

5. Expand the *Network* section.

   Click the *Wired* tab if the camera will use an Ethernet connection to the network; click the *Wireless* tab if the camera will use Wi-Fi.

   Configure the following settings:

Setting Name	Description
Address mode	Select either: • *DHCP* — Use a DHCP server to dynamically configure the camera's IP address and other network settings. See also Making reservations on your DHCP server on page 33 and Configuring the built-in DHCP server on page 33. • *Static* — Manually configure the camera with a static **private** network IP address that you specify in *Address*. It will no longer use DHCP.

Setting Name	Description
	⚠ Fortinet strongly recommends to either: • configure your cameras with a static IP address, or • configure your DHCP server with lease reservations (see also Making reservations on your DHCP server on page 33). Without reservations, the IP address provided by the DHCP server might appear to work initially, but later, when the DHCP lease expires, the DHCP server might change the IP address of the camera. DHCP servers do not notify FortiRecorder about the camera's new dynamic IP address. During this time, FortiRecorder will try to control the camera at its old IP address. This does not work. **Connections with that camera will be broken and all video from that camera could be lost during that interruption.** To fix this, create IP address reservations on your DHCP server and then update the camera's *Address* with its current IP address.
Address	Enter the IP address of the camera. This setting is available only if *Address mode* is *Static*.
Netmask	Enter the subnet mask of the camera. IPv4 and IPv6 subnet masks should be provided in dotted quad format. (For example, enter `255.255.255.0`, not `/24`). This setting is available only if *Address mode* is *Static*.
Gateway	Type the IP address of the next-hop router that will forward packets from the camera to destinations on other subnets, such as FortiRecorder or FortiCamera Cloud. For a direct Internet connection, this will be the router that forwards traffic towards the Internet, and could belong to your ISP. This setting is available only if *Address mode* is *Static*.
DNS1	Enter the IP address of a primary DNS server. This setting is available only if *Address mode* is *Static*.
DNS2	Enter the IP address of a secondary DNS server. This setting is available only if *Address mode* is *Static*.

6. Expand the following sections (available features vary by camera model) and configure their settings:
   - Management on page 55
   - Light or Infrared on page 55
   - Video on page 56
   - Audio on page 58
   - Pan / Tilt / Zoom / Focus on page 59
   - Privacy Mask on page 59
   - Detection on page 59

- Miscellaneous on page 60
- SD Card on page 61
- Scheduled Setting on page 61

7. Click *OK*.

   If you selected the *Enabled* toggle, FortiRecorder now connects to the camera and configures it. After this, in order to control the camera according to your selected schedules, FortiRecorder will periodically connect to the camera again. It will also keep video recordings sent by that camera from its IP address.

8. If you changed the *Address mode* setting or the *Wifi* and *Network* sections, now disconnect the temporary Ethernet connection between the discovered camera and FortiRecorder that you used during initial setup. Move the camera to the intended location on the Ethernet or Wi-Fi network.

9. To confirm that FortiRecorder can receive video from the camera at its new IP address, go to *Monitor* > *Video* > *Video*. (See Viewing live video on page 107.)

   If you cannot view the live video feed from that camera, verify that:

   - Other video software such as Windows Media Player or VLC has not taken the RTSP file type association from Apple 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 external NAT/virtual IP address. To confirm, go to *Dashboard* > *Console* and enter the command:

     ```
     execute ping <camera_ipv4>
     ```

     where `<camera_ipv4>` is the camera's IP address or external NAT/virtual IP address. If you receive messages such as `Timeout...`, to locate the point of failure on the network, enter the command:

     ```
     execute traceroute <camera_ipv4>
     ```

   - Firewalls and routers, if any, allow both RTSP and RTCP components of the RTP streaming video protocol between FortiRecorder and the camera and between your computer and FortiRecorder.
   - Web proxies or firewalls, if any, support streaming video

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

Management

If the camera is an ONVIF-compliant third-party camera, then the *Management* section appears. Expand it. For each category of the camera's settings (for example, *Video/Audio settings*), either:

- *Enable*: Use FortiRecorder to configure these settings.
- *Disable*: Use the third-party camera's native GUI to configure these settings.

Light or Infrared

If the camera supports infrared recording or LED lighting, expand the *Light or Infrared* section. Configure the following settings:

Setting Name	Description
Mode	At night or in the dark, some camera models can use infrared light to record a black-and-white image. This mode also removes a daylight filter for more sensitivity. Select either: • *off* — Disable.

Setting Name	Description
	• *auto* — Automatically enable infrared mode at the darkness threshold.
LED	Infrared LEDs can help the camera to see in the darkness. Select either: • *off* — Disable. Select this option if the camera is behind a window (glass reflects light, which can effectively blind the camera), or if enough ambient lighting is always available and therefore the infrared LED is not required. • *auto* — Automatically activate the infrared LED at the darkness threshold.
Enable threshold	Enter the light level that specifies when infrared mode and infrared LEDs can automatically activate.
Disable threshold	Enter the light level that specifies when infrared mode and infrared LEDs can automatically deactivate.
Threshold time	Enter the amount of time in seconds after the threshold is reached that the camera waits to automatically activate or deactivate infrared mode. Wait time helps to avoid accidentally frequently enabling or disabling infrared mode. This can occur if the camera is near a blinking light (for example, passing cars, flashing advertisement signs, water reflections, tree shade, or holiday decorations).
Current light level	Displays the light level that the camera currently detects.
Refresh	Click to refresh *Current light level*.

Video

Expand the *Video* section. Configure the following settings:

Setting Name	Description
Orientation	Select the relative position of the camera: • *Normal* — Regular viewing angle and position. • *Vertical Flip* — The camera is positioned on a ceiling and the preview image appears upside down. • *Horizontal Flip* — The camera is positioned viewing a mirror or on a ceiling and the preview image appears reversed left to right. • *Rotate 90/180/270* — The camera is in a hallway or corridor. The image is in portrait format.
Video display	If the camera has a fisheye lens, select how to display video from the camera: • *Fisheye* — Use the raw, circle-shaped image. This option is suitable if de-warping is done on FortiCentral instead of FortiRecorder. • *Panorama* — De-warp the image into a rectangle-shaped, 360- or 180-degree panorama.
Mount	Select the mount type of the camera, either: • *Ceiling* • *Table* • *Wall*

Setting Name	Description
Video aspect	Select the video resolution. Options vary by camera model, but can be: • *SD* • *HD*
Overlay mode	Select which to display on the video image: • *Name* (camera name) • *Date & Time* • *Timezone*
Date format	If *Overlay mode* has *Date & Time* enabled, then select the order of the day (`DD`), month (`MM`), and year (`YYYY`) numbers in the timestamp overlay.
Brightness	Adjust the tonal range of an image. Low brightness increases the area of shadows; high brightness expands the area of highlights.
Contrast	Adjust the contrast to increase the separation between dark and light areas of the image, making shadows darker and highlights brighter.
Saturation	Adjust to increase the separation between colors. Low saturation resembles a grayscale image.
Sharpness	Adjust to increase or decrease the edge contrast of the image. Too much sharpness creates grainy borders around the contours of the image.
DIS	Enable or disable digital image stabilization (DIS). For cameras that are mounted on an unstable footing, image stabilization reduces image shaking from various external sources, such as wind.
DNR	Select the type of digital noise reduction (DNR). Options vary by camera model, but can be: • *Off* • *2dnr* • *3dnr* This feature smooths the image and suppresses small noise that causes image graininess in low lighting.
DNR level	If you enabled *DNR*, then select how might DNR to apply.
Smart DNR	Select either *On* or *Off*. Smart DNR saves bandwidth by focusing on the moving parts of a camera's feed. It is only available on FortiCam-FD50 and FB50 models.
Exposure mode	Select whether to automatically optimize the exposure for the camera location. Options vary by camera model, but can be: • *Indoor* • *Outdoor* • *Manual*
Max gain	If *Exposure mode* is *Manual*, select the amount of exposure gain: • *Off* • *1*

Setting Name	Description
	• *2* • *3* Exposure is the amount of light which reaches your camera sensor. It determines how light, dark, and color saturated your image appears. Gain can amplify the light from a fast exposure so that lighting appears more normal. If the gain is too much, however, then the image is grainy and noisy.
Max exposure time	If *Exposure mode* is *Manual*, select the shutter speed, such as *1/4* or *1/10000*. If the shutter speed is too slow, the image is blurry and overexposed (bright). If the shutter speed is too fast, then the image is underexposed and dark.
Digital WDR	Select whether or not to apply WDR digitally, and how many exposures to merge. Options vary by model, but can be: • *Off* • *On* • *1* • *2* • *3* If the camera model supports wide dynamic range (WDR), enable it if there is intense backlight in the camera view. WDR balances images that have high contrast between light and dark, such as a person standing in front of a window during the day. The camera takes two images with different exposure (one optimized for the extreme light, and the other for the extreme dark) and merges them into one image.
Shutter WDR	Select whether or not to apply WDR, and how many exposures to merge. Options vary by model, but can be: • *Off* • *On* • *Auto* • *1* • *2*
Power frequency	Select the AC frequency of the power line (main) in hertz (Hz). AC frequency varies by geographic region. Select the frequency that matches the region where the camera is located.
Media profile	Select which ONVIF media profile on the camera to use. Options vary by camera model. This option is only available on third-party ONVIF compatible cameras.

Audio

Expand the *Audio* section. Configure the following settings:

Setting Name	Description
Input level Output level	Adjust to change the strength of both the input and output level of the audio signal.
Codec	Select the audio codec.
Bitrate	Enter the amount of information to record in bits per second (bps).
Sample rate	Enter the number of times per second to measure sound in hertz (Hz). Greater bitrate and sample rate increases file size and disk usage, but gives better quality audio.

Pan / Tilt / Zoom / Focus

Expand the *Pan / Tilt / Zoom / Focus* section. Configure the following settings:

Setting Name	Description
Auto focus (full/semi)	Automatic focus improves the sharpness of the image with minimal input from the user.
Manual focus	Adjust the focus of the camera manually and determine how fast the focus should change when using the + and - buttons.
Zoom	Select the optical zoom value.
Digital zoom	Once the maximum optical zoom is reached, digital zoom allows the camera to view a larger image of the subject closer by digitally zooming. Unlike optical zoom, increased digital zoom cannot record better detail. It only increases the size of details that are seen with optical zoom. If you need better detail, and optical zoom is at its maximum, put the camera closer to the details that you need to record.

Privacy Mask

Expand the *Privacy Mask* section. If you want to omit an area of the image from recording (for example, for privacy reasons, perhaps you want to mask the area where an employee sits), then click the plus sign beside *Mask Window* and adjust the rectangle size. To add another mask, click the plus sign again.

Detection

Expand the *Detection* section.

All FortiCam cameras can detect motion. Motion and other detections can be used to trigger video clip recordings. Some cameras record these clips and then send them to FortiRecorder. In this case, the length and time frame varies by the camera. The advantage to motion detection is that the camera only records when motion is detected. Other cameras stream continuously to FortiRecorder, and only notify it about the motion detection event. Then FortiRecorder either copies a video clip from part of the video stream and saves it, or simply marks the section of the continuous recording with the time range when motion was detected. These detections ("alarms") can be used to trigger notification emails and text messages.

Some camera models can also use other inputs to trigger events and video clip recording: audio noise, tamper detection, passive infrared sensors, and more.

Configure the following settings:

Setting Name	Description
Monitor Window	Click the + (plus) button to add a rectangle to the video. The rectangle defines the area of the video that can trigger motion detection. Drag its edges and corners if you want to specify only a part of the video. Then optionally also adjust the percentage of change in the area (*Pixel change*) and *Sensitivity*.
Audio Sensitivity	Specify the audio sensitivity level that will trigger a detection. You may need to adjust the sensitivity level, for example, when there are background noises.
PIR Sensitivity	Adjust the sensitivity of the electronic sensor that measures passive infrared (PIR) light to detect motion.
Sensitivity	
Person Sensitivity	Optional. Individually adjust the sensitivity of matching for detecting people. This affects visual search results if the camera is in a hybrid deployment with FortiCamera Cloud.
Vehicle Sensitivity	Optional. Individually adjust the sensitivity of matching for detecting vehicles. This affects visual search results if the camera is in a hybrid deployment with FortiCamera Cloud.
Window <number>	Optional. For each motion detection rectangle on the video, you can individually enable or disable detection of *Person* and *Vehicle* in that region, and adjust the sensitivity of pattern matching for them.
Tamper Sensitivity	Specify the tamper sensitivity level that will trigger a detection.
Digital input Digital output	Enter the voltage pattern or *Open*/*Closed* state from DIDO connectors or ONVIF digital inputs that will trigger a detection alarm. For details, see Using DIDO terminal connectors on FortiCam MB13 cameras on page 61.
Pre-Alarm (sec)	Specify the amount of time in seconds that the camera must continuously sense an event in order to trigger a detection.
Post-Alarm (sec)	Specify the minimum amount of time in seconds that must elapse after detection before another detection can occur (a cool-down period) .

Miscellaneous

Expand the *Miscellaneous* section. Configure the following settings:

Setting Name	Description
Privacy button	FortiCam MB13 has a privacy button on it. If enabled, you can press the privacy button on the camera to pause and resume video and audio monitoring. To enable the functionality of the privacy button on the camera, select *Privacy button*. To disable the functionality of the privacy button on the camera, clear the Privacy button checkbox.
Status LEDs	Most cameras have LED indicators (for details, see the LED description section in the camera's QuickStart Guide). You can enable or disable the LEDs by selecting or deselecting *Status LEDs*.
Move home	For the PTZ cameras, you can specify when the camera should stop PTZ and reset aim to the home position.

SD Card

Expand the *SD Card* section. Configure the following settings:

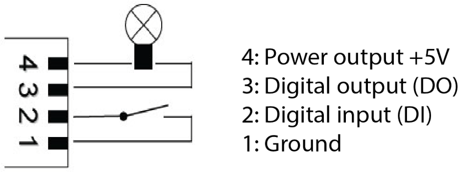
Setting Name	Description
Enable storage	Enable or disable the recording to the camera's internal SD card ("edge recording"). If the disk is full, the oldest recordings are overwritten.
Network failure	Enable or disable the camera's ability to detect network connection failure by periodically pinging FortiRecorder. If the network connection is disrupted, the camera will begin recording to the SD card. This is only supported by some camera models, such as FortiCam FE120B.
Format	Click this button to format the SD card on the camera. This is only supported by some camera models, such as FortiCam FE120B. ⚠ Back up all required files before you format the disk. Formatting the disk will delete all files stored on it. The files cannot be recovered.

Scheduled Setting

Expand the *Scheduled Setting* section. Optionally, you can specify different camera settings, such as brightness, contrast, and DNR level, that the camera will use as different times. To do this, click *New* to select a schedule and specify which settings.

Using DIDO terminal connectors on FortiCam MB13 cameras

FortiCam MB13 (FCM-MB13) cameras have digital input and output (DIDO) terminal connectors. You can configure the digital input to trigger the camera to record a video clip. Optionally, you can also connect other devices to the digital output, such as a relay to turn on or turn off another device.



- *4*: Power output +5V
- *3*: Digital output
- *2*: Digital input
- *1*: Ground

To configure DIDO on FortiCam MB13 cameras

1. Go to *Camera* > *Configuration* > *Camera*, select the MB13 camera from the camera list and select *Edit*.
2. Expand the *Detection* section.
3. Configure the digital input and output settings.

   The digital input can be configured to trigger when the signal is:

   - *LOW* (ground)
   - *HIGH* (+5V)
   - *Rising* (transitioning from *LOW* to *HIGH*)
   - *Falling* (transitioning from *HIGH* to *LOW*)

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

   The digital output can be configured to be either grounded or open when triggered. 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 *HIGH* when the door opens. DI could then be configured to trigger on the rising edge. When the door opens, DO would be triggered 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 time. In the example above, if DI trigger was HIGH and the door was left open for a long time, then the camera would trigger repeatedly.
4. Go to *Camera* > *Configuration* >*Camera Profile*. When you create a camera profile that uses a recording schedule, enable *Digital input*.

More system settings

After completing basic initial setup, optionally, you can add more administrator or user accounts.

For more complex deployments, many settings for features such as network file storage, email notifications, and single sign-on (SSO) integration can also be configured.

Grouping cameras

After you have configured the cameras, you can group them by physical location, model, etc. Groups can be referenced in other parts of the configuration.

To configure camera groups

1. Go to *Camera* > *Configuration* > *Camera Group*.
2. Click *New*.
3. Enter the name for the group.
4. Select the cameras you want to add to the group and then click the right arrow button (>>).
5. Click *Create*.
6. To use the camera group, select it in another part of the configuration, such as device access controls (see Configuring device access control on page 67).

Configuring user and administrator accounts

In its factory default configuration, FortiRecorder has one user account, named `admin`. However most deployments require more logins for other system administrators and users such as security guards.

Best practice is to create a separate user account for each person, and follow the principle of least privilege: only grant administrator-level access if the person's role requires it. This reduces the risk of accidents and malicious insiders. For example, IT personnel need logins with administrator permissions to do their job, but finance personnel usually do not. As a result, you would assign different profiles to those users. You must also deactivate a user account if that person leaves the organization, and create new accounts for new employees. Best practice is for larger organizations to do this centrally with a remote authentication server such as FortiAuthenticator, Microsoft Active Directory, or Red Hat Identity Management, instead of individually on each server, each FortiRecorder, etc. This saves time and gives consistent access control and password management.

User accounts on FortiRecorder have privileges that are determined by their assigned profile.

To configure an administrator or user account

1. Go to *System* > *Administrator* > *Administrator*.
2. Click *New*.
3. Expand the *Preference* section.

   Configure the following settings:

Setting Name	Description
Username	Type a unique name for the account, such as `jdoe`, that can be referenced in other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters. This is the entire user name that the person must enter when logging in to the CLI or GUI. Depending on *Authentication*, your external authentication server may require that you enter both the user name and the domain part, such as `guard@example.com`.

Trusted hosts	Type the IP address and netmask from which the account is allowed to log in to the FortiRecorder appliance. You can specify up to 10 trusted network areas. Each area can be a single computer, a whole subnet, or a mixture.
	To allow login attempts from any IP address, enter:
	`0.0.0.0/0`
	To allow logins only from one specific computer, enter its IP address and a 32-bit netmask, such as:
	`172.168.1.50/32`
	⚠ If you configure trusted hosts, do so for all accounts. Failure to do so means that all accounts are still exposed to the risk of brute force login attacks. This is because if you leave even one account unrestricted (allow connections from 0.0.0.0/0), the FortiRecorder appliance must allow login attempts on all network interfaces where remote administrative protocols are enabled, and wait until after a login attempt has been received in order to check that user name's trusted hosts list.
	For improved security, for each administrator, restrict their trusted host address to one IP addresses: the computer that they will use to log on.
	If you allow login from the Internet, set a longer and more complex *Password*, and enable only secure administrative access protocols (HTTPS and SSH) to minimize the security risk. For information on administrative access protocols, see Configuring network interfaces on page 26.

Admin profile	Select a profile that matches the permissions that you want the user to have. Either click the *New* button to create a new profile, or select an existing profile from the dropdown menu. For more information, see Configuring administrator profiles on page 66.

Setting Name	Description
Access control	Select a profile that matches the camera permissions that you want the user to have. Either click the *New* button to create a new profile, or select an existing profile from the dropdown list. See also Configuring device access control on page 67. This field is available only if *Admin profile* is not *SuperAdminProfile*. (Root administrator accounts have full privileges.)
Authentication	Select an authentication type: • *Local* — Authenticate using an account whose name, password, and other settings are stored locally, in your FortiRecorder appliance's configuration. • *RADIUS* — Authenticate by querying the remote RADIUS server that stores the account's name and password. Also configure *RADIUS profile* and *Check permission attribute on RADIUS server*. See Configuring RADIUS authentication on page 68. • *RADIUS+Local* — Authenticate either by querying the remote RADIUS server that stores the account's name and password, or by querying the accounts stored locally, in the FortiRecorder appliance's configuration. Also configure *RADIUS profile* and *Check permission attribute on RADIUS server*. • *LDAP* — Authenticate by querying a remote LDAP server that stores the account's name and password. See Configuring LDAP authentication on page 69. • *Single Sign On* — Authenticate by querying a SAML SSO IdP server such as FortiAuthenticator or Ping Identity. See Configuring single sign-on (SSO) authentication on page 72.
Password and Confirm password	Enter a password for the account. This field is available only when *Authentication* is *Local* or *RADIUS + Local*. To require strong passwords, see Configuring the public port numbers and domain name on page 37.
Preference	
Display name	Enter a display name for the recipient, such as `FortiRecorder admin`.
Email address	Enter the person's email address or an email alias, such as `all-admins@example.com`, that will receive snapshot notifications, if any, sent by FortiRecorder.
Theme	Select this administrator account's preference for the initial GUI color scheme or click *Use Current* to choose the theme currently in effect for your own GUI session. See also Customizing the theme on page 92 The administrator may switch the theme at any time after he or she logs in by clicking *Next Theme* in the top right corner.
Notification	Select one of the notification methods: • *Email* • *SMS* • *Mobile app*

Setting Name	Description
	For SMS notification method, specify the SMS service provider and SMS recipient information. See also Configuring notification triggers on page 86. This setting appears only if *Admin profile* is *SuperAdminProfile*.
Devices	FortiRecorder Mobile app installations that are associated with this account.
SMS Provider SMS Number	Enter the user's text messaging service provider and mobile phone number.
QR Code	When the user's account is created, FortiRecorder uses your specified email server (see Configuring email settings for notifications on page 78) to send them a QR code with an invitation to log in. The person can use the FortiRecorder Mobile app to scan the QR code. If they did not receive the email and you need to assist them, you can click either: • *Click to get*: Open the QR code image in a new browser tab or window so that you can copy or download it. • *Send to email*: Resend the QR code to the address in *Email address*.

Configuring administrator profiles

Profiles act as access controls that grant permissions to each user for accessing specific FortiRecorder features.

For example, you might create a profile for administrators that grants access to all functions, and a profile for security guards that only grants access to view and operate the cameras.

To configure an administrator profile

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

Access Control	Description
System access	Controls system login and network settings of FortiRecorder: • *Dashboard* > *Status* • GUI console • *System* > *Network* • *System* > *Administrator* • *System* > *Authentication* • *System* > *Certificate*
System status	Controls other system settings, such as • Time • Remote storage • Log settings • Alert email

Access Control	Description
System configuration	Controls whether a whether user is able to access various system configurations.
System maintenance	Controls access to *System* > *Maintenance*, such as being able to back up the system configuration.
Camera configuration	Controls camera installation and configuration. *Read:* Provides access to viewing configuration. *Write:* Enables modifying camera configuration.
Camera status	Controls camera status. *Read:* Provides access to viewing camera statistics and status. *Write:* Enables modifying camera statistics configuration.
Camera live view	Controls whether a user can monitor the live video stream of selected cameras. See also Viewing live video on page 107. *Read:* Provides access to the camera's live video feed. *Write:* Enables annotation.
Video playback	Controls whether a user can play the previously recorded video of selected cameras. See also Viewing previously recorded video on page 108. *Read:* Provides a viewable timeline and playback of existing recordings. *Write:* Enables the ability to download an existing recording.
Camera analytic	Controls the camera-based analysis. *Read:* Provides the user viewable results from motion and heat map analysis. *Write:* Enables the creation of motion and heatmap analysis.
Camera notification	Controls whether a user can receive camera notification events, such as facial detection or motion detection. See also Configuring notification triggers on page 86. *Read:* Provides viewable notifications. *Write:* Enables the configuration of notifications.
Camera services	Controls camera services. *Read:* Provides viewable configuration settings. *Write:* Enables modifying configurations.
Camera ACS service	Controls ACS service. See also Integrating with an ACS on page 131. *Read:* Provides viewable configuration settings. *Write:* Enables modifying configurations.

5. Click *Create*.
6. To use the profile, select it when configuring a user account. For details, see Configuring user and administrator accounts on page 63.

Configuring device access control

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

To configure access control

1. Go to *System* > *Administrator* > *Access Control*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Type a unique name for the device access control rule.
Camera Group List	To include cameras in the policy, select their name and then click the >> (right arrow) button to move them into the column on the right. See also Grouping cameras on page 63.
Access	Click *New* to add a new policy to the rule, or double-click an existing rule to edit it. Then enter: • *Name*: Select the name of an existing schedule, or click the + (plus) button to add a new schedule. See also Configuring a schedule on page 119. • *Access type*: Select either *Allow* or *Deny*. If the user tries to access the camera when the schedule denies it, then an error message displays: `Access not permitted at this time`.

4. To use the profile, select it when configuring a user account. For details, see Configuring user and administrator accounts on page 63.

Configuring remote authentication

To authenticate users and administrators, FortiRecorder can connect with FortiAuthenticator or a remote authentication server such as Microsoft Active Directory, Red Hat Identity Management, or Ping Identity, via LDAP, RADIUS, or SAML SSO.

Configuring RADIUS authentication

If your users must log in to a RADIUS server, then configure a RADIUS profile that defines how FortiRecorder sends authentication queries to the RADIUS server.

To configure a RADIUS query

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

Setting Name	Description
Profile name	Enter a unique name (such as `RADIUS-query1`) that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

Setting Name	Description
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the RADIUS server that will be queried when an account referencing this profile attempts to authenticate.
Server port	Enter the port number on which the authentication server listens for queries. The IANA standard port number for RADIUS is 1812.
Protocol	Select which authentication method is used by the RADIUS server: • *Password Authentication* • *Challenge Handshake Authentication* (CHAP) • *Microsoft Challenge Handshake Authentication* (CHAP) • *Microsoft Challenge Handshake Authentication V2* (CHAP version 2) • *Default Authentication Scheme*
NAS IP/Called station ID	Type the NAS IP address or Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address of the FortiRecorder network interface used to communicate with the RADIUS server will be applied.
Server secret	Type the secret required by the RADIUS server. It must be the same as the secret that is configured on the RADIUS server.
Server requires domain	Enable if the authentication server requires that users authenticate using their full email address (such as `user1@example.com`) and not just the user name (such as `user1`).

4. Click *OK*.

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

Configuring LDAP authentication

If your users must log in to a LDAP server, then configure a LDAP profile that defines how FortiRecorder sends authentication queries to the LDAP server.

To configure an LDAP query

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

Setting Name	Description
Profile name	Type a unique name that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.

Setting Name	Description
Server name/IP	Type the fully qualified domain name (FQDN) or IP address of the LDAP server (for example, Microsoft Active Directory) 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*.
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/TLS to encrypt query connections, select it then upload the certificate of the CA that signed the LDAP server's certificate (see Uploading trusted CAs' certificates on page 98).
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which FortiRecorder will search for user objects, such as: `ou=People,dc=example,dc=com` User objects should be child nodes of this location.
Bind DN	Enter the bind DN, such as: `cn=FortiRecorderA,dc=example,dc=com` of an LDAP user account with permissions to query the Base DN. Leave this field blank if you have enabled Allow unauthenticated bind.
Bind password	Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in *Base DN*, or, if you have not yet entered a *Base DN*, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to find your *Base DN*, or can't remember the attribute names. Before using, first configure *Server name/IP*, *Use secure connection*, *Bind DN*, *Bind password*, and then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.
LDAP user query	Enter an LDAP query filter that selects a set of user objects from the LDAP directory. The query string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects. For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and mail attributes, the query filter might be: `(& (objectClass=inetOrgPerson) (mail=$m))` where `$m` is the FortiRecorder variable for a user's email address. This option is pre-configured and read-only if *Schema* is not *User Defined*.

Setting Name	Description
	For details on query syntax, refer to any standard LDAP query filter reference manual.
Scope	Select which level of depth to query, starting from *Base DN*. • *One level* — Query only the one level directly below the *Base DN* in the LDAP directory tree. • *Subtree* — Query recursively all levels below the *Base DN* in the LDAP directory tree.
Derefer	Select when, if ever, to dereference attributes whose values are references. • *Never* — Do not dereference. • *Always* — Always dereference. • *Search* — Dereference only when searching. • *Find* — Dereference only when finding the base search object.
User Authentication Options	Select how, if the query requires authentication, the FortiRecorder appliance will form the bind DN. The default setting is the third option: Search user and try bind DN. • *Try UPN or email address as bind DN* — Select to form the user's bind DN by prepending the user name portion of the email address (`$u`) to the *User Principle Name* (UPN, such as `example.com`). By default, the FortiRecorder appliance will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, enter that UPN in the field named *Alternative UPN suffix*. This can be useful if users authenticate with a domain other than the mail server's principal domain name. • *Try common name with base DN as bind DN* — Select to form the user's bind DN by establishing a common name to the base DN. Also enter the name of the user objects' common name attribute, such as `cn` or `uid` into the field. • *Search user and try bind DN* — Select to form the user's bind DN by using the DN retrieved for that user by *User Query Options*.
Allow Access Control Attribute	Select this option to define the access control.
Allow Admin Profile Attribute	Select this option to define the administrator profile.
Notification Options	Select the *Allow notification attributes* option to enable notifications. FortiRecorder supports the following notifications: • *Email attribute*: This attribute specifies the user's email address for notifications. • *SMS profile attribute*: This attribute specifies which SMS profile the user will use. The SMS profile attribute must match the name of the profile configured in FortiRecorder. • *SMS number attribute*: This attribute specifies the user SMS number for notification. The number format must be the same as the number in the user entry settings. • *Method attribute*: This attribute specifies the method used to notify a user. The two valid entries are `email` and `sms`.

Setting Name	Description
	- *Embedded email images attribute*: This attribute specifies whether images are included in email messages to the user. The two valid entries are `yes` and `no`.
Timeout	Type the number of seconds that the FortiRecorder appliance will wait for a reply to the query before assuming that the primary LDAP server has failed, and will therefore query the secondary LDAP server. The default value is 20.
Protocol version	Select the LDAP protocol version (either 2 or 3) used by the LDAP server.
Allow unauthenticated bind	Enable to allow unauthenticated bind.
Enable cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiRecorder appliance begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.
TTL	Enter the amount of time, in minutes, that the FortiRecorder unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiRecorder appliance to query the LDAP server, refreshing the cache. The default TTL value is 1440 minutes (one day). The maximum value is 10080 minutes (one week). Entering a value of 0 effectively disables caching. This option is applicable only if is enabled.

4. Click *Create*.

   To test the query, configure an account where this profile is used, then attempt to authenticate using that account's credentials.

   Alternatively, click the row to select the query, click *Edit*, then click *Test LDAP Query*. From the *Select query type* drop-down list, select *Authentication*, then complete the *Password* and *Mail address* fields that appear. Click *Test*. After a few seconds, a dialog should appear to indicate that either the query succeeded, or the reason for its failure, such as a network connectivity error.

Configuring single sign-on (SSO) authentication

Single sign-on (SSO) can save time for users by reducing the number of times that they must log in when using many network services. Once they log in, they can access all other authorized services that use SSO until their session expires.

In Security Assertion Markup Language (SAML) SSO, you must configure both of these to connect and authenticate with each other:

- FortiRecorder, which is the service provider (SP)
- FortiAuthenticator or other remote authentication server, which is the identity provider (IdP)

In addition to SSO, FortiRecorder also supports single log off (SLO). When someone logs out of FortiRecorder, they will also be logged out of all services that use the same federated SSO authentication.

To configure FortiRecorder SSO with Ping Identity, see the FortiRecorder Cookbook.

To configure SAML SSO

1. On the IdP server, download its IdP metadata XML.

   Alternatively, copy the URL where FortiRecorder can download it.
2. If you are integrating with FortiAuthenticator or Ping Identity, then on FortiRecorder, use the CLI to enable Security Fabric and the default administrator account named `admin_sso`:

   ```
   config system csf
      set status enable
   end
   config system admin
      edit admin_sso
         set status enable
   end
   ```

   The `admin_sso` account acts like a wildcard, so that you do not need to configure all FortiRecorder accounts on the IdP too. The Security Fabric provides communication for this feature. See also Connecting to the Security Fabric on page 74.
3. Go to *System* > *Customization* > *Single Sign On*.
4. Configure the following:

GUI Item	Description
Enabled	Enable or disable SSO.
Identity Provider (IDP) Metadata	Enter the IdP metadata. To do this, either: • Paste the metadata XML into the text area. • Click *Upload* and select a file that contains the XML. • Click *Retrieve from URL*, and then enter the URL where FortiRecorder can download the XML.

5. Click *Apply*.

   Now FortiRecorder automatically generates its SP metadata, entity ID, and ACS URL. (You might need to navigate away from the tab and return in order for it to display.)
6. Copy the following:

GUI Item	Description
Entity ID	A globally unique identifier for FortiRecorder when it connects to the IdP, such as: `https://FortiRecorder.example.com/sp`
ACS URL	The URL where FortiRecorder will receive authentication responses from the IdP (the assertion consumer service (ACS)), such as: `https://FortiRecorder.example.com/sso/SAML2/POST`
Metadata URL	The URL where the IdP can download SP metadata XML from FortiRecorder, such as: `https://FortiRecorder.example.com/sso/Metadata`

7. On the IdP server:
   a. Paste the entity ID, SP metadata URL, and ACS URL from FortiRecorder.
   b. Select to identify users by their email addresses attribute, and then enter the attribute object identifier (OID) that authentication requests from FortiRecorder use:

`urn:oid:0.9.2342.19200300.100.1.3`

c. Optionally, enable and configure multi-factor authentication (MFA).

d. If required, add the FortiRecorder unit's certificate to the list of trusted CAs ("trust store").

(Skip this step if your IdP already trusts the certificate, directly or indirectly, via a CA certificate signing chain.)

8. On FortiRecorder, go to *System* > *Administrator* > *Administrator*. For each administrator or user account that will use SAML SSO, set *Authentication* to *Single Sign On*.

   To test SSO, attempt to authenticate on FortiRecorder using one of those accounts, and then access another service that also uses SSO. If successful, the other service should not prompt you to log in.

Connecting to the Security Fabric

FortiRecorder can connect to an upstream FortiGate root and become an integrated cluster member of the Security Fabric. This allows FortiRecorder to display network and security information from across your other deployed Fortinet devices. The Security Fabric protocol with FortiOS 7.0+ also provides communications for other features, such as REST API connections with other Fortinet devices and SSO integration with FortiAuthenticator.

Go to *System* > *Customization* > *Security Fabric* and enable the FortiRecorder to become a Security Fabric member. Then the FortiGate that is the root of the Security Fabric can connect to the FortiRecorder appliance.

Configuring data storage on the FortiRecorder

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

Configuring local storage

To view the size, disk space usage, and status of the FortiRecorder disk(s) or RAID array, go to *System* > *Storage* > *Local Storage*.

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

Configuring RAID levels

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

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

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

To configure RAID levels

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

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

Recommended hard drive 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), erase all metadata on the drives.

Adding a RAID disk

FortiRecorder-400F and some other models support multiple hard disk drives.

To add a disk to the RAID array

1. Remove the hard disk bay from the unit.
2. Install the hard disk in the bay.
3. Insert the bay into the unit.
4. Go to *System* > *Storage* > *Local Storage*.
5. 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*.
3. The RAID controller removes the hard disk from the list.
4. Protect the FortiRecorder unit from static electricity by using measures such as applying an antistatic wrist strap.
5. Physically remove the hard disk that corresponds to the one you removed in the GUI from its drive bay.
6. Replace the hard disk with a new hard disk, inserting it into its drive bay.
7. 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 the pre-installed hard drives with your own on FortiRecorder and re-build the RAID array, follow these instructions.

To replace all disks in the array

1. Back up the configuration.

   Because the X.509 certificates used by SSL/TLS connections are stored on the hard drive(s), rebuilding the array with new disks removes those certificates. Certificates are included in the configuration file backup, however. After you install the new hard drives, restore the configuration.

   (Skip this step if you do not use the factory certificates and can re-import your own custom certificates later.)
2. Shut down the FortiRecorder unit.
3. Remove the hard disks.
4. Install the new hard disks.
5. Boot up the system.
6. 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 74.

   ```
   execute raidlevel <level_int>
   ```

   The FortiRecorder sets the RAID level and then reboots.

Configuring external storage

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

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

Best practice is to connect cameras and other services (GUI, CLI, external file storage, etc.) on different network interfaces so that video streams have dedicated bandwidth. Live video streams may be lower quality or have choppy motion if cameras do not have constantly available bandwidth.

Tested and supported NFS servers

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

Untested NFS servers

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

To configure external storage

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

Setting Name	Description
Protocol	Select one of the following types of storage media: • *External USB*: External USB device. • *iSCSI Server*: An iSCSI (Internet Small Computer System Interface) server. • *NFS*: A network file system (NFS) server.
Maximum size	Specify the maximum video file size that is allowed to be stored on the external storage device. You can view the remote storage usage information on *Dashboard* > *Status*.
Username	The user name of the FortiRecorder unit's account on the iSCSI server. This option only appears if *iSCSI Server* is the selected protocol.
Password	The password of the FortiRecorder unit's account on the iSCSI server. This option only appears if *iSCSI Server* is the selected protocol.
Hostname/IP Address	Type either the IP address or fully-qualified domain name (such as nas.example.com) of the iSCSI or NFS server. This option only appears if *iSCSI Server* or *NFS* is the selected protocol.

Setting Name	Description
Port	Type the port number on which the server listens for connections. The default is 2049 for NFS and 3260 for iSCSI. This option only appears if *iSCSI Server* or *NFS* is the selected protocol.
Directory	Enter the path of the folder on the server, relative to the mount point or user's login directory, where the FortiRecorder appliance will store the data. **Note**: Do not use special characters such as a tilde (~). This will cause the storage to fail. This option only appears if NFS is the selected protocol.
Encryption key	The key used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters. This option only appears if *iSCSI Server* is the selected protocol.
iSCSI ID	The iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA). This option only appears if *iSCSI Server* is the selected protocol.

5. Expand the *Status* section.

   The *Status* section indicates if the iSCSI share was successfully mounted on the FortiRecorder unit's file system. This field appears only after you configure the iSCSI share and click *Apply*.

   Status may take some time to appear if the iSCSI server is slow to respond. If a `Not mounted` message appears, then the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiRecorder unit has both read and write permissions on the iSCSI server.
6. 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
```

7. Go to *Camera* > *Configuration* > *Camera Profile*.
8. Select the camera profile used by cameras that should use remote storage, and then click *Edit*.
9. From *Storage Options*, select *Move*.
10. Click *Create*.

Configuring email settings for notifications

If you want FortiRecorder to send email for notifications, and you want to use your own email server to send them, then configure the settings that FortiRecorder will use to connect to your email server.

In factory default settings, the mail relay server is:

```
notification.fortinet.net
```

To configure notification email settings

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

Setting Name	Description
Host name	Type the host name for the FortiRecorder appliance. The default host name is the FortiRecorder appliance's serial number. Maximum length is 35 characters. It can include US-ASCII letters, numbers, hyphens, and underscores, but not spaces and special characters (for example, `?`). The host name is used in: • command prompt of the CLI • SNMP system name. See Configuring SNMP traps and queries on page 82. • notification email, when FortiRecorder identifies itself to the email server (SMTP `HELO`/`EHLO`). The `get system status` CLI command displays the full host name. If the host name is longer than 16 characters, the name may be truncated elsewhere and end with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is `FortiRecorder1234567890`, then the CLI prompt would be: `FortiRecorder123~#` **Note:** This hostname is not required to be a fully qualified domain name, such as `nvr.example.com`, that is globally resolvable by DNS servers on the Internet. The hostname could be used only on your local private network. For the hostname used with remote or public network access, instead see *Public Access Host name*.
Mail Server Use custom mail server	Enable if you want to use a mail server instead of the default provided by Fortinet (`notification.fortinet.net`). If you do not have your own email server, this may be the name of your ISP's SMTP relay, or a 3rd-party email server such as Yahoo! or Gmail.
Mail server name	Type the fully-qualified domain name (FQDN) of your SMTP server, such as `mail.example.com`. This setting appears only if *Use custom mail server* is enabled.
Mail server port	Type the port number on which your email server or SMTP relay listens for connections. The default varies by whether you enable *Use SMTPS*: if disabled, it is port 25; if enabled, it is port 465. This setting appears only if *Use custom mail server* is enabled.
Use SMTPS	Enable to initiate TLS-secured connections to the email server if it supports SSL/TLS. When disabled, SMTP connections from the FortiRecorder appliance's built-in email client to the SMTP server will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS-secured connections. This setting appears only if *Use custom mail server* is enabled.

Setting Name	Description
User name	Type the name of the account, such as `jdoe` or `fortirecorder@example.com`, that FortiRecorder will use to log in to the SMTP server. This setting appears only if *Use custom mail server* is enabled.
Password	Type the password for the account on the SMTP server. This setting appears only if *Use custom mail server* is enabled.
Authentication type	Select one of the following authentication methods: • *AUTO* — Automatically detect and use the most secure SMTP authentication type supported by the email server. • *PLAIN* — Provides an unencrypted, scrambled password. • *LOGIN* — Provides an unencrypted, scrambled password. • *DIGEST-MD5* — Provides an encrypted MD5 hash of the password. • *CRAM-MD5* — Provides an encrypted MD5 hash of the password, with hash replay prevention, combined with a challenge and response mechanism. This setting appears only if *Use custom mail server* is enabled.
Sender Display name	If you want to customize the display name in the emails sent by the FortiRecorder, type the name that will displayed by the email clients. By default, the display name is `FortiRecorder`.
Email address	Type the sender email address (`From:`) that will appear in the SMTP header. The default email address is `noreply@fortirecorder.com`.

3. Click*Apply*.
4. Click*OK*.

   To verify that FortiRecorder can send email now, expand the *Test* section, enter your email address in *Mail Recipient*, and then click *Send*.

To prevent classification as spam, it usually helps if you add the *Email address* of FortiRecorder to your address book.

After configuring the SMTP server and the SMS service provider, configure the cameras and FortiRecorder with your notification criteria. See Configuring notification triggers on page 86 and Configuring alert email on page 139.

You can customize the templates used by email notifications. See Customizing email templates on page 89.

Configuring SMS text message settings for notifications

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

To configure FortiRecorder to send SMS messages

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

Setting Name	Description
Service provider	Enter the SMS service provider name.
Description	Enter a short description of the provider.

Type	Select the SMS protocol: either SMTP or HTTP.
	For SMTP, enter the *Email to*, *Email subject*, and *Email body* information.
	You can use the following tags when filing the fields:
	• `{{:country_code}}`: Country code portion of the SMS number field in the user's configuration.
	• `{{:mobile_number}}`: Phone number portion of the SMS number field in the user's configuration.
	• `{{:message}}`: Text of the message.
	For HTTP, enter the following information:
	• *HTTP URL*: The URL to contact to send SMS messages.
	Example:
	`https://myprovider.com/sendsms`
	• *HTTP method*: Either *Get* or *Post*.
	• *HTTP/S Parameters*:Configure all the parameters and values required by the provider to send the SMS message. You can use the same tags that were available above for SMTP. If you select the *Encrypt* check-box in a parameter, then when viewing the configuration, the value will not be **displayed**.
	Caution: The *Encrypt* option only affects the display, *not* the information transmission. The value will still be **sent** as entered (clear text, *not* encrypted) to the remote server. For this reason, HTTPS is strongly recommended. If you do not use a secure protocol, then sensitive information can be read and modified by any device that can intercept the communications. This can compromise security.
	For example, if your provider indicates that to send a message the syntax should look like the following:
	`https://smsserver.com:8080/sendsms?api_id=1234&user=user&to=<phone_number>&text=<message>&password=<passwd>`
	Then the settings might be:
	HTTP URL: `https://smsserver.com:8080/sendsms`
	HTTP Method: `Get`
	Parameters:
	`api_id id`
	`user user`
	`to {{:country_code}}{{:mobile_number}}`
	`text {{:message}}`
	`password password`
	Caution: Select the *encrypt* checkbox to obscure the password when viewing the configuration. If you do not, verify that no cameras or persons can see your screen, which would compromise security.

3. Click*OK*.

After configuring the SMTP server and the SMS service provider, configure the cameras and FortiRecorder with your notification criteria.See Configuring notification triggers on page 86 and Configuring alert email on page 139.

You can customize the templates used by SMS notifications. See Customizing email templates on page 89.

Configuring SNMP traps and queries

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

Before you can use SNMP, you must activate the FortiRecorder appliance's SNMP agent and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager connects. (See Access: SNMP on page 28.)

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 on page 85.

⚠ 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

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 settings:

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

4. Click*Apply*.

5. Create at least one SNMP community to define which hosts are allowed to query, and which hosts will receive traps. See Configuring an SNMP community on page 83.

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 GUI

1. Go to *System* > *Configuration* > *SNMP*.
2. Configure the SNMP agent.
3. Under *Community*, click *New*.
4. Configure the following settings:

Setting Name	Description
Name	Type the name of the SNMP community to which the FortiRecorder appliance and at least one SNMP manager belongs, such as public. The FortiRecorder appliance will not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiRecorder appliance will include community name, and an SNMP manager may not accept the trap if its community name does not match. **Caution**: Fortinet strongly recommends that you do not add FortiRecorder to the community named public. This popular default name is well-known, and attackers that gain access to your network will often try this name first.
Enable	Enable this community entry.
Community Hosts: IP Address	Type the IP address of the SNMP manager that, if traps or queries are enabled in this community: will receive traps from the FortiRecorder appliance will be permitted to query the FortiRecorder appliance SNMP managers have read-only access. You can add up to 8. To allow any IP address using this SNMP community name to query the FortiRecorder appliance, enter `0.0.0.0`. For security best practice reasons, however, this is not recommended. **Caution**: FortiRecorder sends security-sensitive traps, which should be sent only over a trusted network, and only to administrative equipment.

Setting Name	Description
	Note: If there are no other host IP entries, entering only 0.0.0.0 effectively disables traps because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager.
Queries	Type each port number (161 by default) on which the FortiRecorder appliance listens for SNMP queries from the SNMP managers in this community, then enable it. Port numbers vary by SNMP v1 and SNMP v2c.
Traps	Type each port number (162 by default) that will be the source (Local) port number and destination (Remote) port number for trap packets sent to SNMP managers in this community, then enable it. Port numbers vary by SNMP v1 and SNMP v2c.
SNMP Event	Enable the types of SNMP traps that you want the FortiRecorder appliance to send to the SNMP managers in this community. • System events (system reboot, system reload, system upgrade, log disk formatting, and video disk formatting) • Remote storage event • Interface IP change • Camera events (enabling, disabling, communication failure, recording failure, IP change, and camera reboot) While most trap events are described by their names, the following events occur when a threshold has been exceeded: • *CPU Overusage* • *Memory Low* • *Log Disk Usage Threshold* • *Video Disk Usage Threshold* To configure their thresholds, see Configuring SNMP traps and queries on page 82. For more information on supported traps and queries, see MIB support on page 85.

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

Configuring SNMP v3 users

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

To specify access for an SNMP user

1. Go to *System* > *Configuration* > *SNMP.*
2. If you have not already configured the agent, do so before continuing. See Configuring SNMP traps and queries on page 82.

3. Expand the *User* section and click *New*.
4. Configure the following settings:

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

5. Similar to configuring the SNMP community, configure the other settings to specify the trap recipient IP, allowed query source IP addresses, and trap events (see Configuring SNMP v3 users on page 84).
6. Click *OK*.
7. To verify your SNMP configuration and network connectivity between your SNMP manager and your FortiRecorder appliance, test both traps and queries (assuming you have enabled both). Traps and queries typically occur on different port numbers, and therefore verifying one does not necessarily verify that the other is also functional. To test queries, from your SNMP manager, query the FortiRecorder appliance. To test traps, cause one of the events that should trigger a trap.

MIB support

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

MIB or RFC	Description
Fortinet Core MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FortiRecorder MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiRecorder-specific information and to receive FortiRecorder-specific traps.

MIB or RFC	Description
RFC-1213 (MIB II)	The FortiRecorder SNMP agent supports MIB II groups, except: • There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, and so on.) do not accurately capture all FortiRecorder traffic activity. More accurate information can be obtained from the information reported by the FortiRecorder MIB.
RFC-2665 (Ethernet-like MIB)	The FortiRecorder SNMP agent supports Ethernet-like MIB information, except the dot3Tests and dot3Errors groups.

Download these MIB files from the Fortinet Support website

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.

Configuring notification triggers

After you have configured connection settings (see Configuring email settings for notifications on page 78, Configuring SMS text message settings for notifications on page 80, and Configuring SNMP traps and queries on page 82), configure the recipients and categories of events that will trigger notifications. For example, notifications can be triggered by a camera or ACS device, such as via face recognition, object detection, and door buzzes.

Face and object detection notifications requires integration with FortiCentral. For details, see the FortiCentral User Guide.

These settings are only for camera- and ACS-related notifications, such as motion detection. They do not configure appliance-related notifications, such as the hard disk being full. See also Configuring alert email on page 139.

To configure camera notifications

1. Go to *Camera* > *Notification* > *Camera Notification*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Enter a unique name for the notification.

Setting Name	Description
Description	Optional. Enter a description or comment.
Enable	Enable or disable this notification.
Hold off period	Enter how much time to wait until FortiRecorder sends a notification. Events that occur before the hold off period ends are delayed.
When to notify	• *First event*: Only the first detection triggers a notification. A break where no detection occurs is required before an event is considered to be a new event. The amount of time of the break is determined by the *Pre-Alarm (sec)* and *Post-Alarm (sec)* settings of the camera. • *Evert event*: A notification is sent for every occurrence of a frequent event. For example, if a camera is configured to detect bicycles, and someone leaves a bike in the camera's field of view, then the camera will continually detect the bicycle.
Select Camera	Select which camera(s) will trigger notifications. See also Detection on page 59.
Triggers	Select which signals will trigger a notification: • *Generic detection* • *Motion detection* • *Audio detection* • *Digital input* (DIDO) • *PIR detection* • *Tamper detection* • *Face detection*: Also configure *Face detection*. • *ACS*: Also configure *ACS detection*. • *Object detection*: Also configure *Object detection*. Supported signals vary by camera model and/or ACS device. For example, *Face detection* or *Object detection*, additional options appear (for example, the *Prohibited* category for recognized faces).
Face detection	Select which categories of people (for example, *Masked*, *Unknown*, or *Prohibited*) trigger a notification. This setting applies only if, in *Triggers*, *Face detection* is enabled.
ACS detection	Select which access control event (for example, *Door held open* or *Door forced open*) trigger a notification. This setting applies only if, in *Triggers*, *ACS detection* is enabled.
Object detection	Select which categories of object (for example, *Weapon* or *Animal*) trigger a notification. This setting applies only if, in *Triggers*, *Object detection* is enabled.
Notification Schedule	Enable notifications during specific periods of time during the day or week by selecting *Add schedule* (see Configuring a schedule on page 119). Then select where to send the notification: • *User*: Also configure *Select User*. • *SNMP*: See also Configuring SNMP traps and queries on page 82.

Setting Name	Description
	• *Linked cameras*: Also configure *Select Linked Camera*.
Select User	Select whom to notify. Only administrator accounts appear as options in this list, and only if the *Email* option is enabled in their account. See Configuring user and administrator accounts on page 63. This setting applies only if, in *Notification Schedule*, *User* is enabled.
Select Linked Camera	Select which cameras also start to record when the cameras in *Select Camera* trigger a notification. Recordings from linked cameras are part of the same event. This setting applies only if, in *Notification Schedule*, *Linked camera* is enabled.

4. Click *Create*.

   For information on how to view notifications in theGUI, see Monitoring motion detection notifications on page 110l.

   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.

   To prevent classification as spam, it usually helps if you add the notification email address to your address book.

   If you do not receive an alert email within a few minutes, verify that you have configured an email address for the account (see Email on page 65). Next, verify the static routes of FortiRecorder (see Configuring routing on page 30) and the policies on any firewalls or routers between the appliance and the SMTP relay. (They must allow SMTP traffic from the FortiRecorder network interface that is connected to the gateway between it and the email server.)

   To determine the point of connectivity failure along the network path, if the SMTP server is configured to respond to ICMP `ECHO_REQUEST` (ping), go to *Dashboard* > *Console* and enter the CLI command:

   ```
   execute traceroute <syslog_ipv4>
   ```

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

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

   To delete a notification, select the notification name and then click *Delete*.

Customizing notification templates

You can customize messages that the FortiRecorder appliance sends.

Customizing system messages

Some messages that the GUI show to the user, such as an unauthorized login warning or camera event notifications, can be customized. You can modify both their text and HTML.

Variables can be used if you want to insert the same text in a message multiple times. In addition to using predefined variables (see Predefined variables on page 90), you can create your own new, custom variables.

To create a variable for custom messages

1. Go to *System* > *Customization* > *Custom Message*.
2. Select a message row.

   The *Edit Variable* button is greyed out and not available until you select a message.

   > The scope of a variable is for a specific message; it cannot be used in other messages or templates. If you require the same text in multiple templates or messages, create a variable in each.

3. Click *Edit Variable*.
4. Click *New*.

   You can modify the variables that you create, but you cannot edit or delete the predefined variables.
5. Configure the following settings:

Setting Name	Description

Name	Enter the variable name to use in the system message. Its format is:
	`%%<variable_name>%%`
	For example, if you enter the name `downtime_warning`, then when you configure a customized message and insert this variable, its placement will be indicated as:
	`%%downtime_warning%%`
	The variable's *Content* will be inserted in that location each time FortiRecorder displays that message.

Display name	Enter a description for the variable.
Content	Enter the variable's content.

6. Click *Create*.

To customize a system message

1. Go to *System* > *Customization* > *Custom Message*.
2. Double-click the message that you want to customize, or select its row and click *Edit*.
3. Edit the text. The maximum length is 4000 characters.

   Optionally, if you want to insert a variable, place your text cursor, click *Insert Variables*, and then click the name of the variable.
4. Click *OK*.

Customizing email templates

Similar to system messages, you can customize the templates that FortiRecorder uses for system alerts and camera notifications via email and SMS. The templates support both custom and predefined variables (see Predefined variables on page 90).

To customize email templates

1. Go to *System* > *Customization* > *Custom Email Templates*.
2. Select the template and then click *Edit*.
3. Enter the necessary information, such as the name and a brief description.
4. In the content section, format the message in HTML. To add variables, click *Insert Variable*.

5. Determine if the HTML code was entered correctly by selecting *Preview*.
6. Click *OK*.

Predefined variables

Like the variables that you create, each predefined variable usually can only be used within the scope of a specific type of system message or email template, as shown below.

Alert email

Variable	Description
%%ADDRESS%%	The IP address or domain name of FortiRecorder that is used in hyperlinks. See Public Access Host name on page 38 and Access Ports Service on page 38.
%%ADMIN_USER%%	The administrator notified by the message.
%%CONTENT%%	The content of the alert email.
%%DATE%%	The date when the event occurred.
%%HOSTNAME%%	The IP address or domain name of FortiRecorder that is used in hyperlinks. See Public Access Host name on page 38 and Access Ports Service on page 38.
%%NOTIFY_FROM%%	The sender email address of the email. The value is configured in *Display name* and *Email address*.
%%POSTMASTER%%	The postmaster email address of the email.
%%SENDER%%	The sender email address of the email. The value is configured in *Display name* and *Email address*.
%%SUBJECT%%	The subject line of the email.

Mobile account registration email

Variable	Description
%%MOBILE_APPLE_BADGE%%	The placement of the Apple icon in the mobile account registration email.
%%MOBILE_APPLE_URL%%	The placement of Apple's address in the mobile account registration email.
%%MOBILE_EXPIRATION%%	The expiration time in the mobile account registration email.
%%MOBILE_GOOGLE_BADGE%%	The placement of the Google icon in the mobile account registration email.

Variable	Description
%%MOBILE_GOOGLE_URL%%	The placement of Google's address in the mobile account registration email.
%%MOBILE_QR%%	The QR code image in the mobile account registration email.
%%MOBILE_QR_URL%%	A hyperlink alternative to the QR code image in the mobile account registration email.
%%SENDER%%	The sender email address (`From:`) of the email. When using the default mail server settings, the value is: `FortiRecorder <noreply@fortirecorder.com>`

Camera notification email

Variable	Description
%%BODY%%	The content of the camera notification message.
%%EVENT_DATE%%	The date when the event occurred.
%%EVENT_LINK%%	A hyperlink to the video recording of the event.
%%EVENT_TITLE%%	The title of the event.
%%PUBLIC_ADDRESS%%	The IP address or domain name of FortiRecorder that is used in hyperlinks. See Public Access Host name on page 38 and Access Ports Service on page 38.
%%SENDER%%	The sender email address (`From:`) of the email. When using the default mail server settings, the value is: `FortiRecorder <noreply@fortirecorder.com>`
%%SUBJECT%%	The subject line in the email.

Camera notification web

Variable	Description
%%CAMERA_NAME%%	The name of the camera that triggered the notification.
%%EVENTDATE%%	The date when the event occurred.
%%EVENT_DESCRIPTION%%	The content of the camera notification message.
%%MODEL_IMAGE%%	An image that shows the FortiRecorder model number.
%%NOTIF_NAME%%	The title of the event.
%%NOTIF_ROW%%	A hyperlink to the video recording of the event.

Customizing the theme

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

To customize the user interface appearance

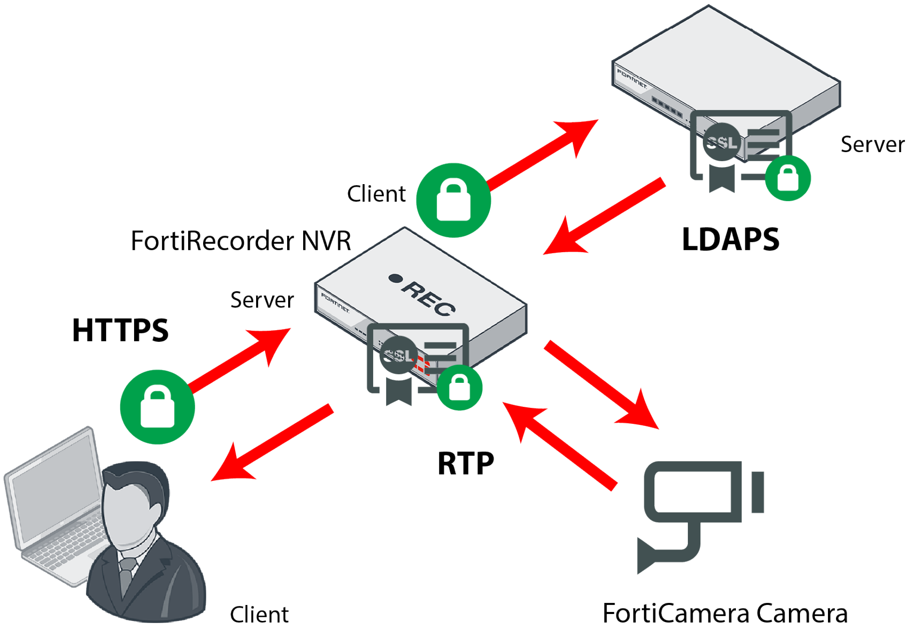
1. Go to *System* > *Customization* > *Appearance*.
2. Configure the following settings:

Setting Name	Description
Product name	Enter the name of the product.
Custom top logo	Click *Change* to upload an icon used as the favicon for the FortiRecorder GUI. The image's dimensions must be 460 pixels wide by 36 pixels tall. Use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme color, resulting in a visible rectangle around your logo graphic. Uploading a graphic overwrites the current graphic. The FortiRecorder does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your computer so that you can upload it again later.
Default Theme	Select the default color (red, green, blue, and light blue) for the GUI. Users can select a different theme in their preferences later, or you can specify a different theme when you configure each user account. For details, see Configuring user and administrator accounts on page 63 .

3. Click *Apply*.

Working with certificates

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



FortiRecorder may require you to upload certificates and CRLs even if you do not use HTTPS.

For example, when sending alert email via SMTPS, or querying an authentication server via LDAPS, FortiRecorder will validate the server's certificate by comparing the server certificate's CA signature with the certificates of CAs that are known and trusted by the FortiRecorder appliance. See Uploading trusted CAs' certificates on page 98 and Revoking certificates on page 99.

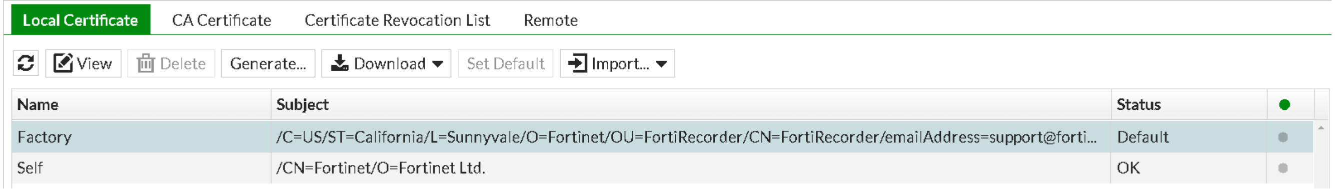
Replacing the default certificate for the GUI

For HTTPS connections with the GUI and other TLS-secured services, 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 on page 94). Otherwise, start with Uploading & selecting to use a certificate on page 96.



Name	Subject	Status	●
Factory	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiRecorder/CN=FortiRecorder/emailAddress=support@forti...	Default	●
Self	/CN=Fortinet/O=Fortinet Ltd.	OK	●

GUI Item	Description
View	Select to view the selected certificate's issuer, subject, and range of dates within which the certificate is valid
Delete	Select to delete the selected certificate.
Generate	Select to generate a certificate signing request. For details, see Generating a certificate signing request on page 94.
Download	Select to download the selected certificate's entry in certificate (CER), PKCS #12 (P12), or certificate signing request (CSR) file format. PKCS #12 is recommended if you require a certificate backup that includes the private key. Certificate backups can also be made by downloading a configuration file backup, which includes all certificates and keys.
Set status	To configure your FortiRecorder appliance to use a certificate, click its row to select it, then click this button. A confirmation dialog will appear, asking if you want to use it as the "default" (currently in use) certificate. Click *OK*. The *Status* column will change to reflect the new status.
Import	Select to upload a certificate. For details, see Uploading & selecting to use a certificate on page 96 .
Name	Displays the name of the certificate according to the appliance's configuration file. This will not be visible to clients.
Subject	Displays the distinguished name (DN) located in the Subject: field of the certificate. If the row contains a certificate request which has not yet been signed, this field is empty.
Status	Displays the status of the certificate. • **Default** — Indicates that this certificate will be used whenever a client attempts to connect to the appliance. Only one certificate can be in use at any given time. • **OK** — Indicates that the certificate was successfully imported. To use the certificate, select it, then use Set status to change its status. • **Pending** — Indicates that the certificate request (CSR) has been generated, but must be downloaded, signed, and imported before it can be used as a server certificate.

Generating a certificate signing request

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

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

To generate a certificate request

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

Setting Name	Description
Certification name	Enter a unique name for the certificate request, such as fortirecorder.example.com. This can be the name of your appliance.
Subject Information: ID Type	Select the type of identifier to use in the certificate to identify the FortiRecorder appliance: • *Host IP* — Select if the FortiRecorder appliance has a static IP address and enter the public IP address of the FortiRecorder appliance in the IP field. If the FortiRecorder appliance does not have a public IP address, use E-Mail or Domain Name instead. • *Domain Name* — Select if the FortiRecorder appliance has a static IP address and subscribes to a dynamic DNS service. Enter the FQDN of the FortiRecorder appliance, such as fortirecorder.example.com, in the *Domain Name* field. Do not include the protocol specification (`https://`) or any port number or path names. • *E-Mail* — Select and enter the email address of the owner of the FortiRecorder appliance in the *E-mail* field. Use this if the appliance does not require either a static IP address or a domain name. The type you should select varies by whether or not your FortiRecorder appliance has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate. For example, if your FortiRecorder appliance has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the GUI by the domain name of the FortiRecorder appliance, you might prefer to generate a certificate based upon the domain name of the FortiRecorder appliance, rather than its IP address.
Subject Information: IP	Type the static IP address of the FortiRecorder appliance, such as 10.0.0.1. The IP address should be the one that is visible to clients. Usually, this should be its public IP address on the Internet, or a virtual IP that you use NAT to map to the appliance's IP address on your private network. This option appears only if *ID Type* is *Host IP*.
Subject Information: Domain Name	Type the fully qualified domain name (FQDN) of the FortiRecorder appliance, such as www.example.com. The domain name must resolve to the static IP address of the FortiRecorder appliance. See also Configuring network interfaces on page 26 . This option appears only if *ID Type* is *Domain Name*.
Subject Information: E-mail	Type the email address of the owner of the FortiRecorder appliance, such as admin@example.com. This option appears only if *ID Type* is *E-Mail*.
Key type	Displays the type of algorithm used to generate the key. This option cannot be changed, but appears in order to indicate that only RSA is currently supported.

Setting Name	Description
Key size	Select a secure key size of *512 Bit*, *1024 Bit*, *1536 Bit* or *2048 Bit*. Larger keys are slower to generate, but provide better security.
Optional Information: Organization unit	Optional. Type the name of your organizational unit (OU), such as the name of your department. To enter more than one OU name, click the + icon, and enter each OU separately in each field.
Optional Information: Organization	Optional. Type the legal name of your organization.
Optional Information: Locality (City)	Optional. Type the name of the city or town where the FortiRecorder appliance is located.
Optional Information: State/Province	Optional. Type the name of the state or province where the FortiRecorder appliance is located.
Optional Information: Country/Region	Optional. Select the name of the country where the FortiRecorder appliance is located.
Optional Information: E-mail	Optional. Type an email address that may be used for contact purposes, such as `admin@example.com`.

4. 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.
5. Click to select the row that corresponds to the certificate request.
6. 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.
7. 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.
8. 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.)
9. When you receive the signed certificate from the CA, upload the certificate to the FortiRecorder appliance (see Uploading & selecting to use a certificate on page 96).

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.
2. Append the certificate of each intermediary CA in order from the intermediary CA who signed the local certificate to the intermediary CA whose certificate was signed directly by a trusted root CA.

   For example, an appliance's certificate that includes a signing chain might use the following structure:

   ```
   -----BEGIN CERTIFICATE-----
   <server certificate>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <certificate of intermediate CA 1, who signed the server certificate>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <certificate of intermediate CA 2, who signed the certificate of intermediate CA 1 and
        whose certificate was signed by a trusted root CA>
   -----END CERTIFICATE-----
   ```
3. Save the certificate.

To upload a certificate

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click *Import*.
3. Configure the following settings:

Setting Name	Description
Type	Select the type of certificate file to upload, either: • **Local Certificate** — An unencrypted certificate in PEM format. • **Certificate** — An unencrypted certificate in PEM format. The private key is in a separate file. • **PKCS12 Certificate** — A PKCS #12 encrypted certificate with private key. Other available settings vary depending on this selection.
Certificate file	Click *Browse* to locate the certificate file that you want to upload. This option is available only if Type is Certificate or Local Certificate.
Key file	Click *Browse* to locate the private key file that you want to upload with the certificate. This option is available only if Type is Certificate.

Setting Name	Description
Certificate with key file	Click *Browse* to locate the PKCS #12 certificate-with-key file that you want to upload. This option is available only if Type is PKCS12 Certificate.
Password	Type the password that was used to encrypt the file, enabling the FortiRecorder appliance to decrypt and install the certificate. This option is available only if Type is Certificate or PKCS12 Certificate.

4. Click *OK*.
5. To use a certificate, click its row to select it, then select *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 on page 98).

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 also 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 on page 96.

To upload a CA's certificate

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

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

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

2. Go to *System > Certificate > CA Certificate*.

To view the selected certificate's issuer, subject, and range of dates within which the certificate is valid, click a certificate's row to select it, then click *View*.

3. Click *Import*.
4. In *Certificate name*, type a name for the certificate that can be referenced by other parts of the configuration. Do not use spaces or special characters. The maximum length is 35 characters.
5. Click *Browse* 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, initiate a secure connection to an LDAPS server (see Configuring LDAP authentication on page 69 and Configuring user and administrator accounts on page 63).

   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.

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 can 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 on page 99.

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. Download the server certificate from your OCSP/CRL server.
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. Click *Browse* and 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.

Using the dashboard

FortiRecorder has several methods, including a real-time dashboard, FortiView, SNMP traps, and log messages, that you can use to monitor system statuses.

To use the dashboard, go to *Dashboard* > *Status*. The default widgets on the dashboard show:

- serial number
- firmware version
- uptime
- licenses (see also Licenses on page 9)
- currently logged in users
- system resources (see also Resource issues on page 153), such as:
  - CPU usage
  - memory usage
  - disk space usage
- face recognition events
- audit summary (see also Auditing for issues in configuration and operation on page 105)
- camera status and scheduled continuous or motion detection-triggered recording

To access this part of the GUI, you must have an administrator account, and its access profile must have *Read-Write* permission to the *System status* category. Other user accounts do not have permission. For details, see Configuring administrator profiles on page 66 .

Customizing the dashboard

You can customize your dashboard to show or hide widgets, and to arrange them on *Dashboard* > *Status*.

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

To show or hide a widget, click *Manage Widget* and then select its name, and click *Apply*. (If the widget name is greyed out, the widget will not display.)

Icon buttons on the widget's title bar vary, but always include *Refresh* and *X* (hide).

Using the CLI Console widget

You can use SSH or Telnet to connect to the command line, but if you are already logged into the GUI, you don't need to leave it.

To access the CLI without exiting the GUI, go to *Dashboard* > *Console*. If you need to pop the CLI Console out to a window that you can resize and reposition, then click *Open in New Window*.

Using FortiView

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

Monitoring camera statistics

The *Camera Statistics* section displays various camera performance statistics, such as the bandwidth usage of specific cameras and recording gaps.

Viewing bandwidth statistics

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

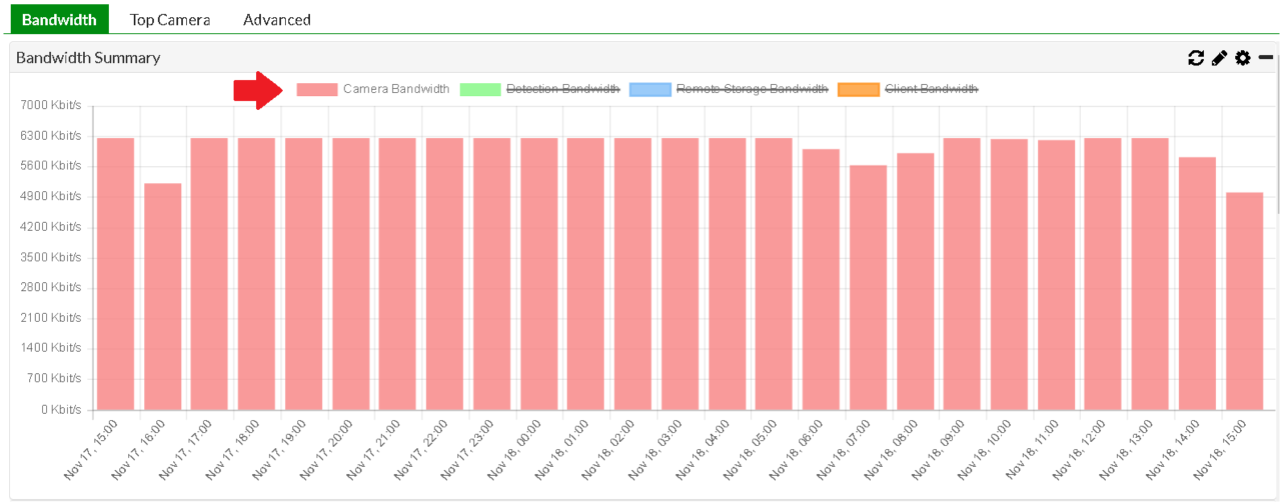
To edit statistics settings

1. Go to *FortiView* > *Camera Statistics* > *Bandwidth*.
2. Click the settings gear icon on the right side of a chart (for example, *Bandwidth Summary*).
3. Configure the following settings:

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

4. Click *OK*.

   Selecting one of the bandwidth display options to enable or disable them from view.



Viewing top camera usage

The *Top Camera* tab displays the performance of each camera. Use this section to determine which cameras use the most bandwidth.

To edit top camera settings

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

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

3. Click *OK*.

Analyzing advanced statistics

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

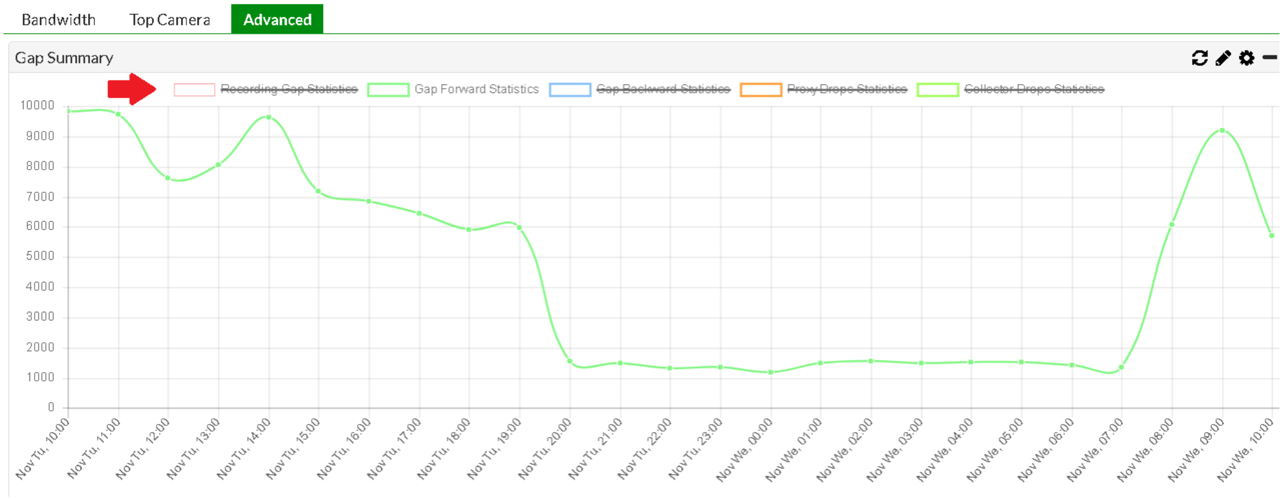
To edit the Advanced settings

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

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

3. Click *OK*.

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



Viewing network connections and sessions

To display the current TCP connections and UDP sessions with your FortiRecorder, go to *FortiView > Sessions*.

If you see network connections that you do not expect, verify the *Trusted hosts* setting of all administrator accounts, and that the IP address of DHCP cameras has not changed.

If network connections seem to be missing, see Connectivity issues on page 155.

Auditing for issues in configuration and operation

In deployments with many cameras and a large configuration, it can be useful to have a regularly updated, prioritized list of detected problems and remaining configuration tasks with suggested corrective actions. Audit reports do not require any scheduling. They are automatically updated every 24 hours, or on demand when you click the *Refresh* button.

To audit issues in the deployment

1. Go to *FortiView > Audit Report*.

   Alternatively, go to *Dashboard*, and in the *Audit Summary* widget, click one of the priority levels, such as *Medium*.

   Issues appear in a list sorted by priority, similar to log messages:

   - *Critical* — Operation is impacted. For example:
     - cameras are in an error state
     - live video streams have been interrupted
     - available disk space is so low that FortiRecorder must delete videos before your selected retention period ends
   - *High* — Operation could be impacted soon. For example:
     - network connections have been disrupted
     - available disk space is very low
     - cameras have more than one IP address on the network
   - *Medium* — Operation might not be normal. For example:
     - failed login attempts
     - no email address to send alert email to
     - log disk is almost full
     - network connections don't have enough bandwidth and may result in skipped video frames
     - camera is using unusual amounts of network bandwidth
   - *Low* — Operation might be better if optimized, or may be missing some settings. For example:
     - camera location was not indicated
     - frequent motion detections may be more efficient with better lighting, or as continuous recording instead
     - disabled camera has no recordings and therefore could be deleted from the list on FortiRecorder
2. To show a list of issues in each priority, click the + (plus) button at the right side of the screen. Then to view an explanation and list of cameras affected by each issue, click the + (plus) button at the left side of the issue description, such as *No hostname configured*.

Monitoring

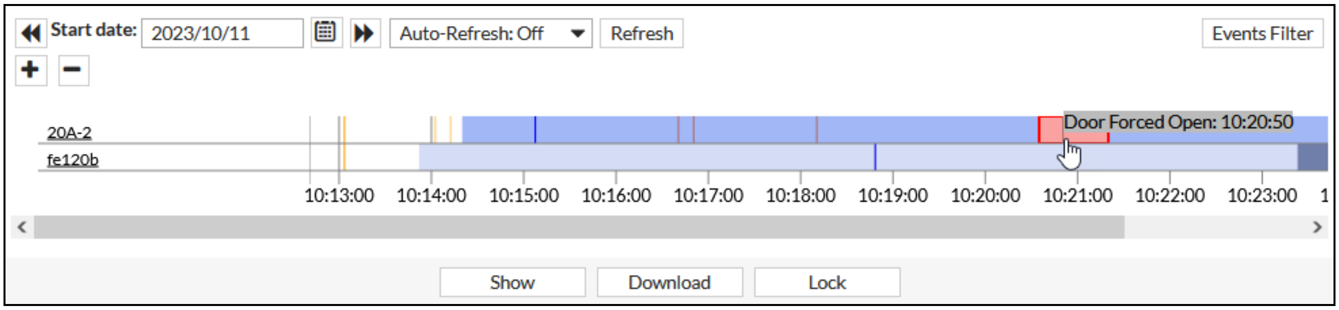
FortiRecorder has multiple monitoring tools, such as direct video surveillance and detailed summaries of camera events.

Viewing video

You can use the timeline and video player to view both live and previously recorded video from cameras.

Understanding the timeline

Below the video player for live video feeds and previously recorded videos, there is a timeline. Time ranges, annotations, and ACS events in the timeline are color-coded.



Start date: 2023/10/11

Auto-Refresh: Off

- **Yellow**: FortiRecorder and camera system events, such as a software update or reboot. Recordings cannot be stored while FortiRecorder is unavailable.
- **Light blue**: Previously recorded video.
- **Dark blue**: Temporary recording that has been manually initiated. See also Viewing live video on page 107.
- **Bright blue**: Annotation in the recording. See also Annotating a video on page 108.
- **Red**: Motion detection-triggered recording.
- **Dark red**: ACS events, such as a card swipe or door being forced open.
- **White**: No recording in that period of time.

If you hover your mouse cursor over an event, annotation, or time range, then a tool tip appears with more information. If you click the time line, a bright red outline indicates which time range or event you have selected.

To show events on the timeline

1. Above the video players (if any), in the top right corner, click *Select Cameras* and select which cameras' events to include. If you select multiple cameras, then the timeline will have multiple rows.

   FortiRecorder and ACS system events are automatically included.
2. Below the video players, in the top right corner of the timeline, click *Events Filter* and select the type of events and/or annotations to include, such as motion detection (*Detection Recordings*) and face recognition (*Face Detection*).
3. If you want to jump to another date or time on the timeline, then either:

- enter *Start date*
- drag the timeline to the left or right

4. Zoom in or zoom out to specific moments on the timeline either by:
   - scrolling your mouse wheel
   - clicking the + (plus) and - (minus) buttons

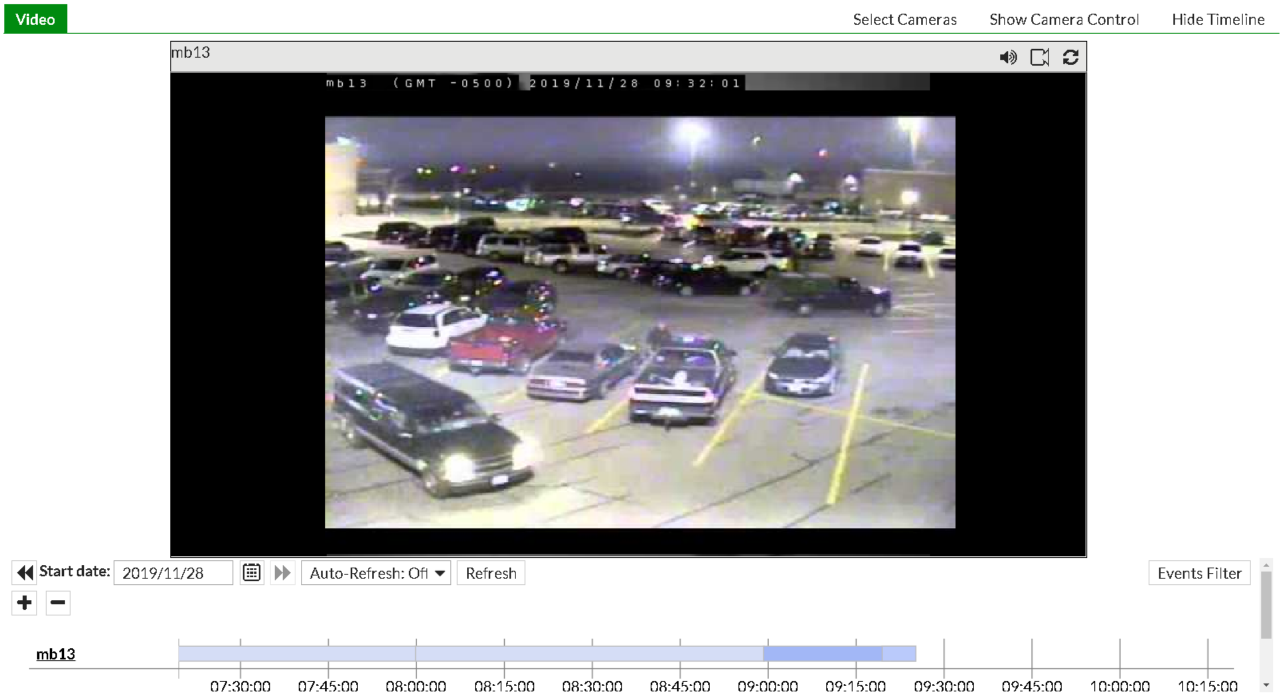
Viewing live video

You can use the video player to watch the live video feed from a camera, regardless of whether it is currently scheduled to be recording.

During this, if the camera is not scheduled to record, then the live video feed is temporarily recorded in memory, but not saved on the hard drive. When you stop watching the live feed from that camera, the temporary recording is deleted **unless** you manually initiate a recording.

To view and record a live video feed

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



2. Use the timeline to select which cameras and events to view.

   The live video stream from the cameras plays.
3. If a live video stream is too dark, too bright, too blurry or too gray, then:
   a. Click the title bar of a view pane to select that camera.

      The *Show Camera Control* button becomes available.
   b. Click *Show Camera Control*.
   c. Adjust:
      - *Brightness*
      - *Contrast*

- *Saturation*
- *Sharpness*

and then click *Apply*. After a few seconds, the change should appear in the live video stream. Adjust your settings again until the video has good sharpness, color, and lighting.

Adjust these settings carefully. After video is recorded, you cannot adjust them again unless you download the file and use video editing software. Video editing software may not be able to completely correct very bad lighting and color.

Alternatively, these settings can be adjusted while configuring the camera. See *Brightness*, *Contrast*, *Saturation*, and *Sharpness*.

d. Click *Close*.

4. If you want to start recording the live video stream, then in the top right corner of the video pane, click *Record*.

To stop a manual recording, either click *Stop*, or go to another page in the GUI.

If recording has been automatically triggered (continuous schedule or motion detection), then the manual *Stop* button is not available. Instead, you can change the *Recording* setting or schedule.

Annotating a video

While watching or recording a live video feed, you can insert markers on the timeline with notes about what you see.

1. Go to the live video feeds. See Viewing live video on page 107.
2. Click the title bar of a view pane to select that camera.

   The *Show Camera Control* button becomes available.
3. Click *Show Camera Control*.
4. In the text area, enter your notes and then click *Annotate*.

   An annotation marker is inserted on the timeline. If the camera was not already recording, it will now start so that the annotation has an associated video recording.

Viewing previously recorded video

You can play any previously recorded video, including those manually initiated while watching a live video feed. Snapshots can also be viewed.

1. Go to *Monitor* > *Video* > *Video*.
2. Use the timeline to jump to a previous date or time.
3. Click to select the time range or event that you want to view.

   The *Show*, *Download*, and *Lock* buttons become available. If you selected an event with an associated snapshot images from nearby cameras, then a dialog also displays those images. If your FortiRecorder unit has a USB port, then the *Export to USB* button also becomes available.
4. Click *Show*.

A video player appears in a pop-up window.

5. If there is important evidence, and you want to prevent the video clip from being deleted by storage policies, then click *Lock*.

Downloading video

If you are required to show video evidence of a particular incident to authorities, you can download video to your computer so that you can upload it to them.

Alternatively, if your FortiRecorder unit has a USB port, then you can export the video onto a USB drive, and give the USB drive to authorities.

1. If you want to export video to a USB disk:
   - a. On your computer, plug in the USB disk.
   - b. Format the disk's file system as either a VFAT (for compatibility with Windows or Mac computers) or ext4 (for Linux).
   - c. Eject the disk.
   - d. On the FortiRecorder unit, plug in the disk.
2. Go to *Monitor* > *Video* > *Video* or *Monitor* > *Video* > *Event*.
3. Use the timeline to jump to a previous date or time.
4. Click to select the time range or event that you want to download.

   The *Download* button and, if a USB drive is plugged in, *Export to USB* button become available.
5. Click *Download* or *Export to USB*.

   The video uses the MP4 file format with your selected video codec, which can be viewed on computers with compatible video 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.

Monitoring events

You can display events from FortiRecorder and its connected cameras and other devices such as motion detection, DIDO, and ACS without loading the live video feeds of your cameras. Monitoring this way saves network bandwidth.

Viewing events as a timeline

You can view the timeline separately from camera live video feeds, with no video players.

1. Go to *Monitor* > *Event* > *Event*.
2. Use the timeline to find motion detection, digital input, and other events.

Viewing events as a table

Alternatively to the timeline, you can view events and recordings as a table.

Each entry in the list contains:

- start and end time of the event
- camera that the event occurred on (if applicable; FortiRecorder system events have no associated camera, but ACS events have an associated camera)
- type of the event, such as *Annotate*, *ACS*, *Motion Detection*, *System* (FortiRecorder), and *Camera* (recording interruptions etc. that are not a motion detection alarm)
- subtype of the event, such as *Motion Alarm*, *System Reboot*, *Access Granted*, *Door Forced Open*, etc.

To display events as a table

1. Go to *Monitor* > *Event* > *Event List*.
2. Click *Select Cameras* and select which cameras' events to include.
3. In *Start date* and *End date*, select the time range of events.
4. Click *Events Filter* and select the type of events and/or annotations to include.

Monitoring motion detection notifications

If you have configured notifications based on events detected by cameras (see Configuring notification triggers on page 86), accounts configured to be notified can log in to the GUI and review the video clips. If you have configured email settings, then these accounts will also receive an email when a camera detects an event. Notifications contain snapshot images from the video clip of the detected motion or, depending on your configuration, a link directly to the video clip. (See Customizing email templates on page 89.) In this way, recipients can quickly assess whether or not the event is serious, or just a false alarm.

Occasionally, you might also sometimes be required to review these notifications if, for example, the usual recipient is on vacation. If you have permissions (see Configuring administrator profiles on page 66), you can do this from the GUI, without logging in to a separate account. Alternatively, you can add yourself to the list of people that will receive a notification via email.

To monitor camera-based notifications

1. Go to *Monitor* > *Camera Notifications* > *Notification Events*.
2. From *Select recipient*, select either *All*, or the account that should have received the notification.

   The list of notifications is filtered by the recipient criteria. Only matching notifications appear.
3. In the *Message* column, click the link to view that notification.

   A new browser tab or window opens, displaying the notification that was included in the email body, if any. By default, the notification includes images that are key frames from the motion detection video clip.
4. To view the motion detection video clip, click a key frame image.

   A video player replaces the notification, and begins to play the video. See also Viewing previously recorded video on page 108.

Monitoring ACS notifications

If you have configured camera-based notifications (see Configuring notification triggers on page 86), accounts configured to be notified can log in to the GUI and review the video clips. If you have configured email settings, then these accounts will also receive an email when a camera detects an event. Notifications contain snapshot images from the video clip of the detected motion or, depending on your configuration, a link directly to the video clip. (See

Customizing email templates on page 89.) In this way, recipients can quickly assess whether or not the event is serious, or just a false alarm.

Occasionally, you might also sometimes be required to review these notifications if, for example, the usual recipient is on vacation. If you have permissions (see Configuring administrator profiles on page 66), you can do this from the GUI, without logging in to a separate account. Alternatively, you can add yourself to the list of people that will receive a notification via email.

To monitor ACS notifications

1. Go to *Monitor* > *Camera Notifications* > *Notification Events*.
2. From the *Select recipient* drop-down list, select either *All*, or an account that should have received the notification.

   The list of notifications is filtered by the recipient criteria. Only matching notifications appear.
3. In the *Message* column, click the link to view that notification.

   A new browser tab or window opens, displaying the notification that was included in the email body, if any. By default, the notification includes images that are key frames from the motion detection video clip.
4. To view the motion detection video clip, click a key frame image.

   A video player replaces the notification, and begins to play the video.

Understanding the logs

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

FortiRecorder appliances can log many different activities including:

- camera recording events
- administrator-triggered events such as logout and configuration changes
- system-triggered events including system failures

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

The FortiRecorder appliance can save log messages to its memory, or to a remote location such as a Syslog server or FortiAnalyzer appliance. For details, see Configuring log settings on page 137.

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

To download a log file

1. Go to one of the log types, such as *Monitor* > *Log* > *Event*.
2. Right click a log.
3. Click *Export to Table*.

   FortiRecorder converts the log entry to a CSV file, and then your web browser downloads it.

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`.

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 stores all log messages equal to or exceeding the log severity level selected.

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

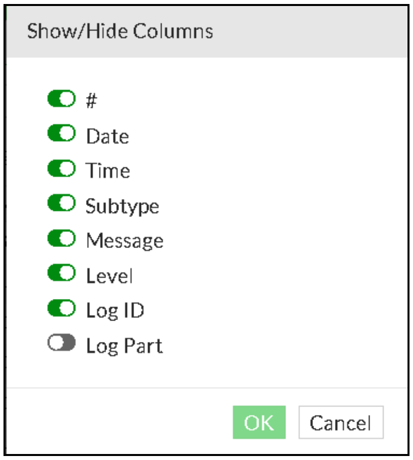
Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and premature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

Displaying and organizing logs

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

To display or hide columns in logs

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



Show/Hide Columns

- ☑ #
- ☑ Date
- ☑ Time
- ☑ Subtype
- ☑ Message
- ☑ Level
- ☑ Log ID
- ☐ Log Part

4. Enable or disable the columns.
5. Click *OK*.

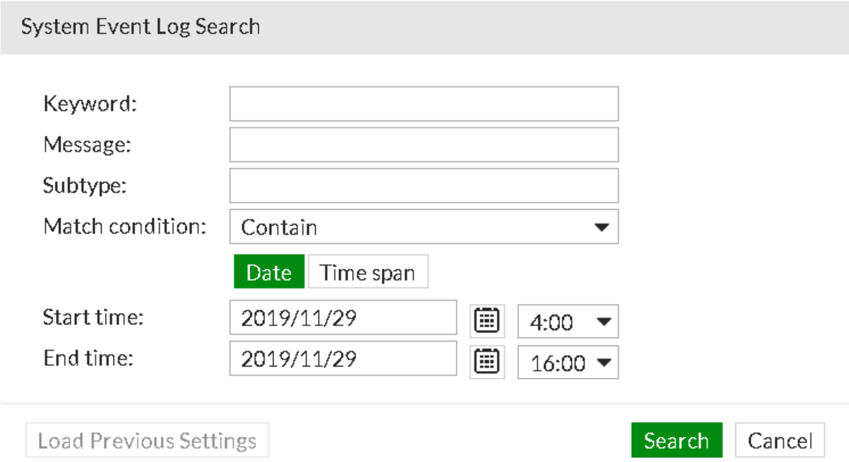
To arrange the columns and rows

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

Searching logs

When viewing logs, you can locate a specific log message by searching for it.

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



Match condition: Contain

Start time: 2019/11/29 4:00

End time: 2019/11/29 16:00

3. Configure the following settings:

Setting Name	Description

Keyword	Type the word or phrase to search. The word may appear in any of the fields of the log message (for example, *Action* and/or *Message*) or in any part of that field's value. If entering multiple words, they must occur uninterrupted in that exact order.
	For example, entering `admin` as a keyword will include results such as:
	`User admin2 logout from GUI(172.16.1.15)`
	where part of the word appears in the middle of the log message. However, entering:
	`User logout`
	would not yield any results, because in the log messages, those words are always interrupted by the name of the account, and therefore do not exactly match your search key phrase.
	This setting is optional.

Message	Type all or part of the exact value of the *Message* field (`msg`field when viewing a raw, downloaded log file) of the log messages that you want to find. This setting is optional.
Subtype	Enter the subtype, such as `admin` or `system`code>.
Match condition	Select whether your match criteria are specified exactly (*Contain*) or you have indicated multiple possible matches using an asterisk in *Keyword* (*Wildcard*).
Time	Select the date and time range that contains the log message that you are searching for. This setting is optional. **Note**: The date fields default to the current date. If you want to search for a previous event, you must configure this setting.

4. Click *Search*.

Viewing logs

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

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

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

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

To view log messages

1. Go to *Monitor* > *Log* > *Event*. Columns and appearance varies slightly by the log type.
2. From the *Level* and *Type* dropdown lists, select the level of severity and type of log you are searching for.

3. Double-click the row of a log file for a more detailed description of the log message.

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

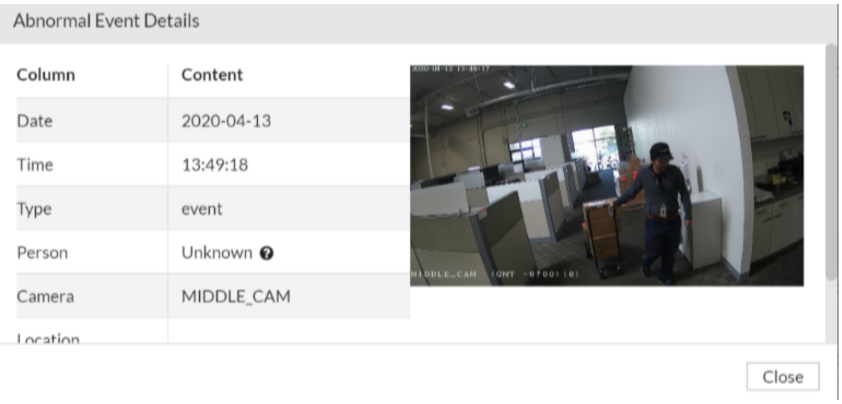
Setting Name	Description
Level	Select a severity level to hide log messages that are below this threshold (see Log severity levels on page 111).
Subtype	Select a subcategory (corresponding to the *Subtype* column) to hide log messages whose subtype field does not match.
Go to line	Type the index number of the log message (corresponding to the # column) that you want to jump to in the display.
Search	Click to find log messages matching specific criteria.
Back	Click to return to the list of log files stored on the hard drive of FortiRecorder.
Save View	Click to keep your current log view settings for subsequent views and sessions.
#	The index number of the log message within the log file. By default, the rows are sorted by timestamp in descending order, starting with the most recent log message. **Note**: In the current log file, each log's index number changes as new log messages are added, pushing older logs further down the stack. To find the same log message later, remember its timestamp and *Message*, not its #.
Date	The date on which the log message was recorded. When in raw format, this is the log's `date` field.
Time	The time at which the log message was recorded. When in raw format, this is the log's `time` field.
Action	The action the camera performed, such as stopping and starting recording.
Subtype	The category of the log message, such as `admin` for events such as authentication or configuration changes, or system for events such as disk consumption or connection failures. When in raw format, this is the log's `subtype` field.
Log ID	A dynamic log identifier within the system, not predictable, indicative of the cause nor necessarily a unique identifier. When in raw format, this is the log's `log_id` field.
Detection Type/Subtype	The particular kind of detection the camera registered, such as motion.
Message	The log message that describes the specific occurrence of a recordable event.

Monitoring face recognition

Face recognition monitoring provides a comprehensive log of events captured by the AI-enabled cameras. For information on configuring face recognition, see Notifications via face recognition on page 128.

- *Abnormal Events* displays instances when policies for abnormal events were triggered.
- *Normal Event* displays instances when policies for normal events were triggered.
- *Activity* displays instances when faces were captured by an AI camera, whether or not there was a policy associated with it.

Double-click a log to see more details. Hovering your mouse cursor over the question mark icon in the *Person* row displays an image of the detected face.



Abnormal Event Details

Column	Content
Date	2020-04-13
Time	13:49:18
Type	event
Person	Unknown ?
Camera	MIDDLE_CAM
Location	

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

Monitoring DHCP status

For all devices that are using your FortiRecorder appliance's built-in DHCP server, you can display the current DHCP lease status and assigned IP address. This can be useful when:

- You need to find and block unauthorized devices that are connecting to your network.
- Camera connections are periodically interrupted because they do not have a DHCP reservation, and therefore their IP address changes.

To view the DHCP lease list, go to *Monitor* > *DHCP Status* > *DHCP*.

Monitoring network security

FortiRecorder records all of the failed login attempts and the IP addresses that are currently blocked from accessing the GUI and CLI. You can review and unblock IP addresses if an administrator or user has accidentally entered an incorrect password too many times.

To unblock an IP address

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

Network security

There are features to harden the network security of your FortiRecorder appliance.

Configuring intrusion detection

Intrusion attempt detection can block IP addresses if failed login attempts from that IP address reach the threshold.

The blocking duration is based on the history of the IP address. If IP address has been blocked in the past, then FortiRecorder will block the IP address for a longer time. The maximum time an IP address can be blocked is 45 days.

For example, if you set the initial block period to 10 minutes, depending on the user's number of violations, the actual maximum block time can be up to 2 hours. If you set it to 30 minutes, the block time can be up to 12 hours.

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

To configure intrusion detection

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

Setting Name	Description
Status	Select *Enable*, *Disable*, or *Monitor only* (log, but do not block).
Access tracking	Enable or disable what types of login access are tracked: CLI or Web.*CLI* is access via SSH or Telnet; *Web* is GUI access via HTTP(S).
Initial block period	Specify how long the IP address will be blocked after its failed login attempts reach the threshold for the first time. The actual block time will be increased for repeated offenders. The default setting is 10 minutes. **Tip:** To avoid false positives, avoid using a longer initial block time setting. The recommended setting is less than 30 minutes.

3. Click *Apply*.

To manually exempt IP addresses from authentication reputation tracking

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

To remove IP addresses from the auto exempt list

1. Go to *Security* > *Intrusion Detection* > *Auto Exempt IP*.
2. Select the IP address.
3. Click *Delete*.

Schedules

Schedules are used by multiple features, such as determining when to record video, or when to allow a user to access a camera. In order to be accurate, schedules require a correct system time.

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

Configuring a schedule

Schedules are used by multiple features. Often it is useful to schedule when cameras will record.

If no schedules are selected for a camera, or when the selected schedules conflict with each other, then FortiRecorder uses the default schedule, named `Always`.

1. Go to *Schedule* > *Schedule* > *Schedule*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Name	Enter a unique name for the schedule.
Description	Optional. Enter a description.
Type	Select a schedule type: • *Recurring*: Specified times on selected days, every week. • *One-time*: Only on a specific date and time.
Days	If *Type* is *Recurring*, select the days of the week when the schedule will be active.
All day	Enable if you want the schedule to be active during the whole day. Disable if you want to configure *Start time/End time*.
Start time/End time	Select the time range for the schedule. Instead of using the time on the clock, you can schedule according to the cycles of day and night that vary from summer to winter. For details, see Configuring the sunrise and sunset time on page 120.

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

4. Click *Create*.
5. To use the schedule, select it in one of the features that use it, such as Configuring device access control on page 67 or Configuring camera profiles on page 48.

Configuring the sunrise and sunset time

When specifying schedules, you can use a specific date and time, or the time of sunrise and sunset, which varies during the year from summer to winter. This is useful if, for example, you want to record only during the night.

To get the sunrise and sunset time

1. Go to *Schedule* > *Schedule* > *Settings*.
2. Enter the geographical latitude and longitude where the FortiRecorder and camera are located.
3. Click *Calculate*.

   The time of sunrise and sunset on a few days is displayed.

When using a combination of sunrise or sunset and the specific time, if the time crosses the boundary of sunrise or sunset, the schedule has no effect.

For example, if the sunrise is at 8:00 AM and you set the schedule from sunrise to 7:00 AM, then the schedule has no effect.

Analytics

Video analytics can find specific instances of motion on your cameras, along with instances during the recording when FortiRecorder recognized specific people or objects.

Using motion detection analytics

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

To run analytics tasks

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

   Time required varies, but could be a few minutes. After the task is completed, double-click the task to view the results. You can adjust the sensitivity and threshold of the search result.

Using computer vision analytics

Computer vision processes events generated by face and object detection.

FortiRecorder can detect important objects such as a vehicle or a weapon. Object detection in FortiRecorder is treated as a camera-related event, similar to motion detection.

For face recognition, FortiCentral installations can create models of the faces that your cameras see, and then store them in a database on FortiRecorder. Every FortiCentral that runs face detection can contribute to your face recognition database. This distributed processing scales well as your organization grows. FortiRecorder can then use computer vision to analyze digital images to identify important people via face recognition.

Alternatively, you can perform face modeling and face recognition at a centralized location, on FortiRecorder.

Both methods store their analysis results on FortiRecorder. However, the results are stored in separate databases. On FortiRecorder:

- *Analytics* > *Computer Vision*: Face modeling by FortiCentral. Both FortiCentral and FortiRecorder can query this database for face recognition. For details on face recognition in FortiCentral, see the *FortiCentral User Guide*.
- *Face Recognition* > *User Asset*, etc.: Face modeling by FortiRecorder. Currently, only FortiRecorder can query this database for face recognition. FortiCentral cannot use it. For details, see Face recognition on page 123 .

For information about viewing logs and managing the databases via REST API, see the REST API Reference.

To enable detection actions

1. Go to *Analytics* > *Computer Vision* > *Computer Vision*.
2. Enter the amount of time to use to decide on a recognized face or object in the *Accept detection after* field.

   More time allows the camera a chance to get a more complete view of the object or face so that FortiRecorder can avoid misinterpretations.
3. Enable *Face detection action*. Face detection is organized into categories:
   - *Prohibited:* Individuals who are prohibited from accessing the building.
   - *VIP:* Individuals who are very important and are not security threats.
   - *Expired:* The time is past the expiry date of the person recorded.
   - *Unknown:* Individuals who are detected but not matched to an individual in the database.
   - *Regular Person:* Individuals who are recognized as common visitors, such as guests, employees, or contractors.
4. Enable *Object detection action*. Object detection is organized into categories:
   - *Person:* An individual.
   - *Motion:* Something that has generated motion.
   - *Weapon:* A detected tool that can cause harm.
   - *Vehicle:* A transportation machine, such as a bike, a car, or a train.
   - *Animal:* A non-human creature, such as a bird or a dog.
   - *Item:* An object, such as a backpack or a suitcase.
   - *Sport:* Athletic equipment, such as skis or a skateboard.

   Each category can be further filtered by only enabling parts of the group in the analytics processor.
5. From the drop-down menu, select the action of FortiRecorder when it detects each category:
   - *No action:* Ignore events of this type.
   - *Event:* Accept events of this type, process them for notification, and display them on timelines and logs.
   - *Event clip:* Accept events of this type, process them for notification, display them on timelines and logs, and generate a video clip at the moment of detection.
6. Click *Apply*.

Face recognition

Face recognition on FortiRecorder uses artificial intelligence (AI) to identify unique faces and enact policies based on configured information. For example, you can identify faces as "known" and enter information about them in the face recognition database, such as their job role or their department. The information can be used to track when the person usually appears and how often so that you can create notification policies about unexpected occurrences or unauthorized locations.

Licensing

All FortiRecorder models except FRC-100D/G can be licensed to run face recognition analytics.

It requires an active FortiGuard AI DB service SKU.

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

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

Activation of the license requires Internet access for the recorder.

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

Trial license

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

Alternatively, you can process face modeling and face recognition in a distributed way, with FortiCentral installations.

Both methods store their analysis results on FortiRecorder. However, the results are stored in separate databases. On FortiRecorder:

- *Analytics > Computer Vision*: Face modeling by FortiCentral. Both FortiCentral and FortiRecorder can query this database for face recognition. For details on face recognition in FortiCentral, see the FortiCentral User Guide.
- *Face Recognition > User Asset*, etc.: Face modeling by FortiRecorder. Currently, only FortiRecorder can query this database for face recognition. FortiCentral cannot use it.

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

To enable face recognition in the GUI

1. Go to *Dashboard* > *Status*. In the *License Information* widget, verify that you have a valid license for face recognition.

   If the license is expired or invalid, then only the previous 7 days of face recognition data (face clusters, timeline, events, and activity) will display.

2. Go to *Camera* > *Configuration* > *Camera Profile*.
3. Select the camera profile to enable face recognition on and then select *Edit*.
4. Expand the *Recording* section and enable *Motion detection in the Recording*.
5. Enable *FortiRecorder in the Store*.
6. Click *OK*.
7. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
8. In the *AI Status* column, enable AI for one or more cameras.

   Face recognition AI only analyzes video from the selected cameras. Analysis results in face clusters, which you must review and confirm in order to ensure accurate face recognition. Continue with Identifying faces on page 124.

To enable face recognition in the CLI

Enter these commands:

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

Identifying faces

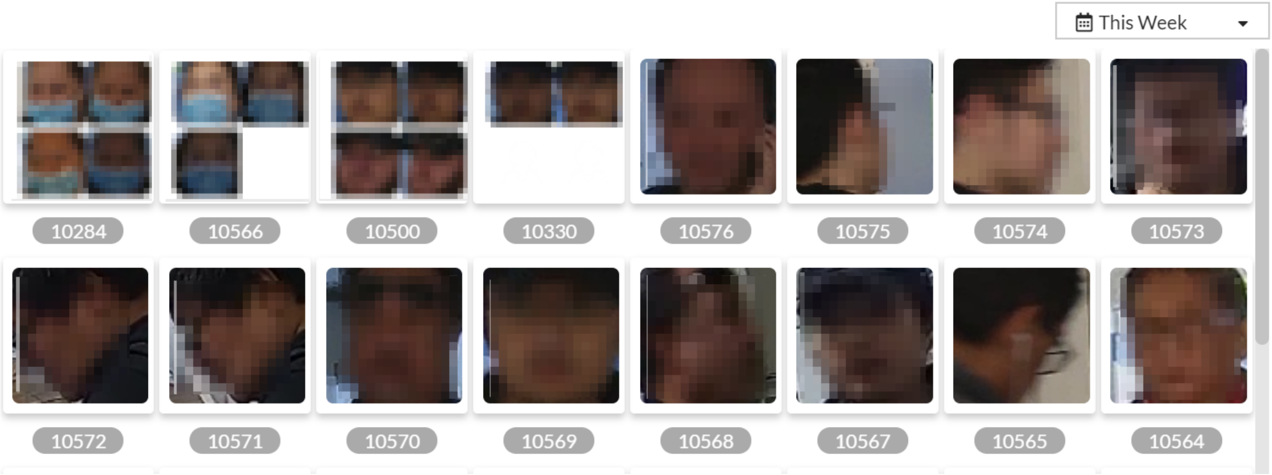
A face cluster is a collection of images of the same person detected by face recognition AI. Face clusters are categorized as either known or unrecognized (new) faces.

Reviewing new faces

All unrecognized face clusters are categorized as new faces. If you know the person, you can link the face cluster to that person's record in the face recognition database so that FortiRecorder can recognize the face.

To link a new face cluster to a person

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



3. Select a face cluster to open all images that the AI has grouped as the same person.
4. Confirm that all images contain the same person. If an image does **not** show the same person, then hover over the image and click the trash can icon in order to correct the AI.

> ⚠ Verify every face in the face cluster. If faces are not correctly identified, and you do not correct it, then AI identification will be less accurate.

5. Either:
   - From the *Search User* dropdown menu, select an existing person to whom the face cluster belongs. The five closest matches appear.
   - Click *New User* and enter their person's name, role, and department and then click *Save*. For details, see Configuring a department and role on page 126.
6. Click *Link all to user*.

   The individual's face cluster is now a known face. All future face images are analyzed by the AI and categorized by their face cluster.

Reviewing known faces

Known face clusters contain images of people that are recognized by face recognition AI, or that you manually linked to an entry in the face recognition database.

To edit known face clusters

1. Go to *Face Recognition* > *Face Cluster* > *Known Faces*.
2. Select the face cluster for a person to open that record. For details, see Configuring a department and role on page 126.
3. Hover your cursor over the profile picture and click *More*.

   All the face clusters manually linked to the user are displayed.

Configuring a department and role

The face recognition database ("user assets") can contain information that you enter about the people that face recognition detects, such as the person's name and department. This can provide more context when you receive notifications or use the timeline.

To create a new job role

1. Go to *Face Recognition* > *User Asset* > *Department and Role*.
2. Expand the *Role Management* section.
3. Click *New*.
4. Enter the *Role Name* and *Description*.
5. Click *Save*.

To create a new department

1. Go to *Face Recognition* > *User Asset* > *Department and Role*.
2. Expand the *Department Management* section.
3. Click *New*.
4. Enter the *Department Name* and *Description*.
5. Click *Save*.

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

Configuring a floor plan

You can use a floor plan to indicate where cameras are in the building. This can be used to locate people that face recognition detects.

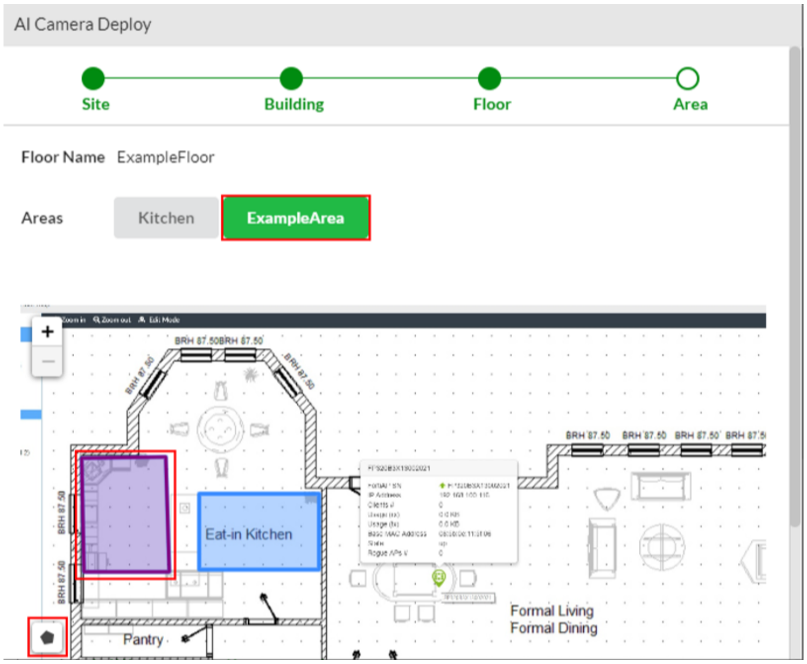
To configure a floor plan

1. Go to *Face Recognition* > *User Asset* > *Floor Plan*.
2. Click *Create floor plan*.
3. Click *Create new site* and enter a name for the site, or select an existing site. Click *Next*.

   Currently, only one site and one building are supported. If you already have a site and/or building, then there is no button to create a new site or a new building.

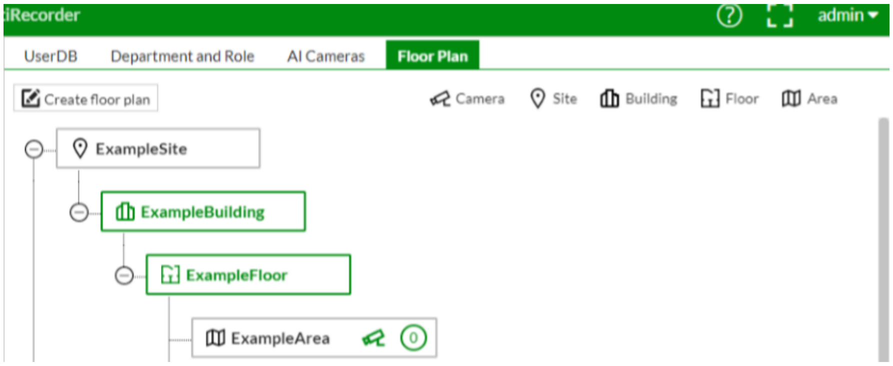
4. Click *Create a new building* and enter the name and address of the building. Mark the building's location on the provided map. Click *Next*.
5. Click *Create a new floor* and enter the name of the floor, or select an existing floor from the *Choose a Floor* dropdown menu. If you create a new floor upload an image of the floor plan. Click *Next* and then enter the dimensions. Click *Next*.

6. Select the polygon icon to draw on an area in the floor plan. Once the area is drawn, enter a name for the area and click *Save*.



7. Click *Finish*.

   A flowchart of your site appears.



Locating cameras and setting processing schedules

You can assign an AI-enabled camera to a specific location in a floor plan to show where the camera is located and therefore where a person's face was detected.

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

To assign a location to a camera

1. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
2. Select the camera row and then click *Assign*.
3. Follow the prompt on the screen to select the site, building, and floor for the location of the camera.

4. Select the name of the area or select the area from the floor plan.
5. Select the location of the camera within the selected area.
6. Select *Done*.

To set a schedule for an AI-enabled camera

1. Go to *Face Recognition* > *User Asset* > *AI Cameras*.
2. Select the camera to highlight the row in blue.
3. Click *Schedule*.
4. From *Video Process Priority*, select either:
   - *Latest high priority*: AI processes the newest video first.
   - *Earliest high priority*: AI processes the oldest video first.
5. From *Schedule*, select the schedule that governs the face recognition AI module. Face recognition AI will not function outside of the schedule.
6. Click *Save*.

Notifications via face recognition

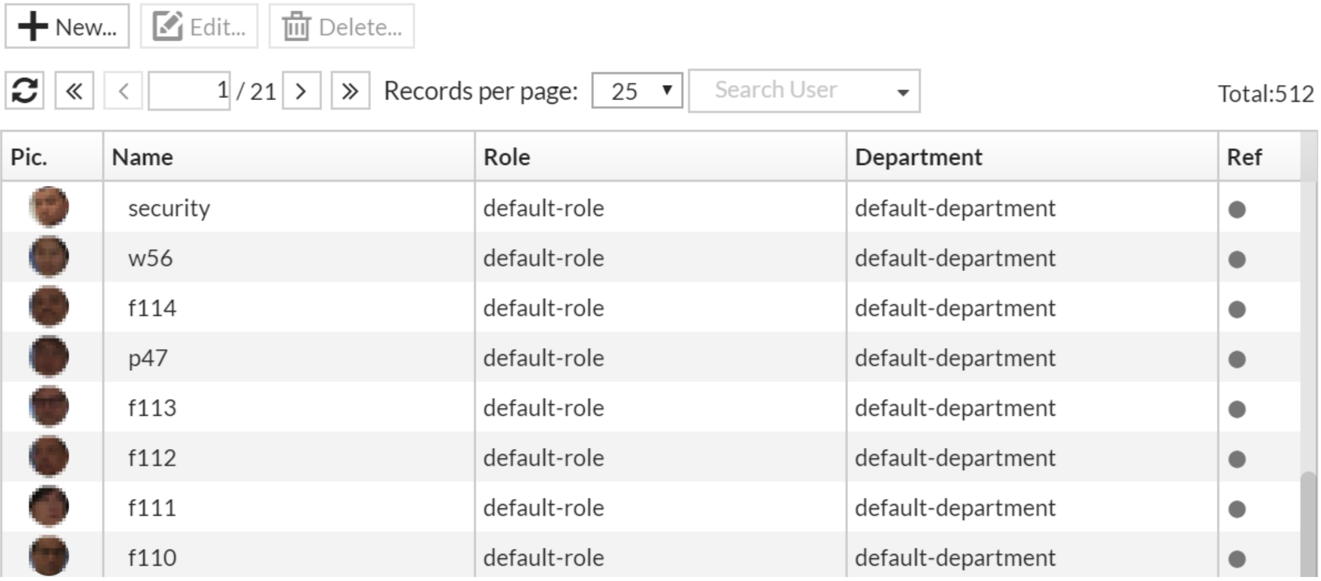
Face recognition policies log and/or alert you to occurrences that fit your criteria.

For example, you could set a policy that sends you an SMS text message whenever an unknown person's face is captured on camera in a high security location.

1. Go to *Face Recognition* > *Policy* > *Policy*.
2. Click *New*.
3. Enter a *Rule Name*.
4. From the *Event Type* dropdown list, select either:
   - *Normal*: Any expected occurrence. For example, an employee enters the building at the usual time to start his shift. Although the event is normal, you might still want to be notified of the event's occurrence.
   - *Abnormal*: Any unexpected occurrence. For example, an employee enters an area of the building that he should not have access to, and doesn't usually enter.
5. From the *Site*, *Building*, *Floor*, and *Area* dropdown lists, indicate the location that you want to monitor.
6. From the *Person* dropdown list, select the face cluster that will match the policy.
7. From the *Action* dropdown list, select one or more actions to do when the policy is matched:
   - alert
   - *email*
   - *sms*
8. Click *Save*.

Searching the face recognition database

You can browse and search information in the face recognition database.



Pic.	Name	Role	Department	Ref
	security	default-role	default-department	●
	w56	default-role	default-department	●
	f114	default-role	default-department	●
	p47	default-role	default-department	●
	f113	default-role	default-department	●
	f112	default-role	default-department	●
	f111	default-role	default-department	●
	f110	default-role	default-department	●

To view face recognition information about a person

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

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

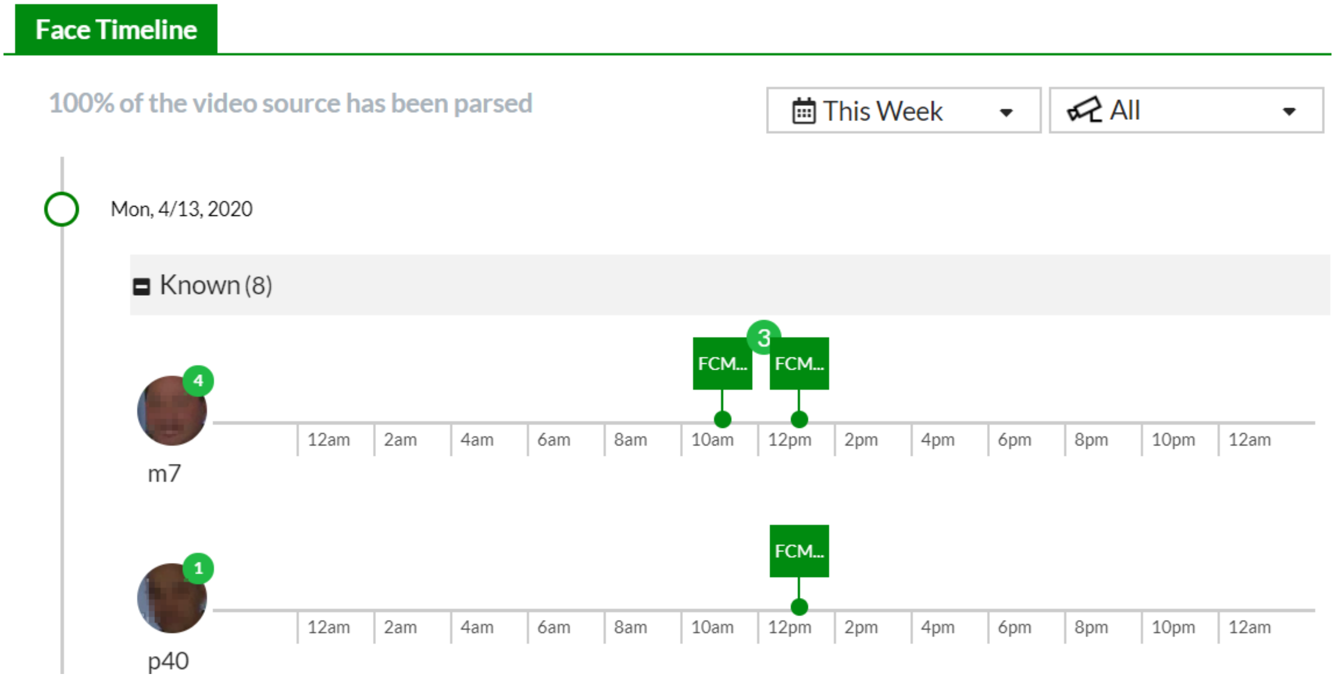
Zoom in or out of the timeline by hovering your mouse over the timeline and scrolling up or down. Pan across the timeline by clicking and dragging left or right.

To add a person to the face recognition database

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

Using the face recognition timeline

Go to *Face Recognition* > *Face Timeline* to view a timeline of daily activities of people detected by AI-enabled cameras.



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

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

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

Integrating with an ACS

FortiRecorder can be integrated with access control systems (ACS) to monitor ACS events such as door opening, forced entries, granted entries, and denied entries. When an event happens, the associated cameras can record the event.

Adding an ACS system

To integrate FortiRecorder with an access control system (ACS), specify the ACS connection, login credentials, and event actions.

To add an ACS system

1. Go to *ACS* > *Configuration* > *ACS*.
2. Configure the following settings:

Setting Name	Description
Status	Enable to use this ACS server.
Type	Select either a: • Kantech EntraPass • Advantech ADAM-6051-D Ethernet Remote I/O
User Name	Enter the ACS user name. This option appears if Type is *EntraPass*.
Password	Enter the password of the ACS user name. This option appears if Type is *EntraPass*.
Address	Enter the IP address of the ACS server.
Port	Enter the listening port number of the ACS server. This option appears if Type is *EntraPass*.
Secure	Enable if the ACS server requires secure connections (HTTPS). This option appears if Type is *EntraPass*.
Actions	For each ACS event type (*Door open*, etc.), select the action that it triggers on FortiRecorder: • *no action* • *event*: Add a marker on the timeline on FortiRecorder. • *event clip*: Record a short video clip only. See also Associating cameras with ACS elements on page 132.

Associating cameras with ACS elements

After you've connected your FortiRecorder to the ACS system, you can assign cameras to the ACS events in the *ACS Source Map*. For example, if you have camera A and camera B installed and pointed at the front entrance of the building, you can associate them with the front door.

1. Go to *ACS* > *Configuration* > *Source Map*.
2. Select a source such as a door.
3. Click *Edit*.
4. In the dialog, select the matching camera from the *Camera List* and click >> to move it to the *Member* list.
5. When an ACS event occurs, you can view the video from the associated camera. See Monitoring ACS events on page 132.

Monitoring ACS events

To view events detected by ACS, go to *Monitor* > *ACS*.

On the upper right corner, click *Select ACS Devices* to filter the events by ACS devices.

Setting Name	Description
Time	Time stamp when the event was triggered.
Name	Location of the triggered event.
Card Info	Card holder's name.
Event	Name of the event, as listed under ACS > Configuration.
Cameras	Cameras recording the events.
Description	Description of the events.

Configuring video services

The *Service* section contains a variety of tools to adjust how you view videos.

Configuring video sharing

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

Sharing video streams

You can share videos from your cameras on web sites. This allows users to the live feed of a camera—without being prompted to log into the FortiRecorder appliance.

For example, if your web browser supports HTML5, you can insert the following code into a web page:

```
<iframe
    frameborder="10"
    scrolling="no"
    width="640"
    height="480"
    src="https://10.0.0.5/api/v1/FRC_LiveView?id=FD51
        &width=640&height=480&view_mode=3
        &hostName=10.0.0.5
        &username=videoService&password=1234">
    <p>iframes are not supported by your browser.</p>
</iframe>
<br />
<script>
    setInterval(function() {
        var req = new XMLHttpRequest();
        req.open('GET',
            "https://10.0.0.5/api/v1/FRC_LiveView?id=FD51
                &username=videoService&password=1234
                &heartbeat=1", true);
        req.send();
    }, 10000);
</script>
```

The IP address at the beginning of the code is the IP of the FortiRecorder. The attribute ID is the name of the camera as defined on the FortiRecorder. 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://<user_name>:<password_str>@<fortirecorder_ipv4>:<port_int>/camera=<id>
```

For example:

```
rtsp://videoService:1234@10.0.0.5:554/camera=FD20
```

To configure video sharing

1. Embed the video stream into a web page with HTML code similar to what is shown above, and/or configure video players to connect via RTSP.
2. On FortiRecorder, go to *Service* > *Video* > *Stream*.
3. Enable *Status*.
4. In *Username* and *Password*, enter the login credentials that the web page or video players will use to connect to the share.
5. In *Protocol*, enable the network protocols that users will use to connect to the camera: *HTTPS* and/or *RTSP*.
6. In *Camera Group List*, select the camera groups that you want to share with users, and then click the right arrow button (>>).
7. Click *OK*.

Downloading video clips via API

You can enable FortiRecorder to allow an external service to make REST API queries to downloading video clips from selected cameras. For details, see the REST API Reference.

To configure video clips

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

Sharing snapshot images

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 an FTP server.

To configure image sharing

1. Optionally, if your FTP server is also a web server, you can embed an image file name into a web page, similar to Sharing video streams on page 133.

   FortiRecorder will be configured to upload snapshot images to this file name. The web page will display the snapshot.
2. On FortiRecorder, go to *Service* > *Video* > *Image*.
3. Enable *Status* to enable FTP uploads.
4. In *Interval*, enter the number of seconds between each snapshot.
5. Enter the FTP settings.
6. In the *Select Camera* section, click *New* and select the cameras whose snapshots you want to share.
7. Enable or disable image processing.

The FortiRecorder retrieves these settings and sends privacy processed snapshots at the chosen interval.

Camera live video feeds **must** remain open in a view pane on FortiCentral where privacy analytics are active. Image processing is done by FortiCentral installations that are connected to FortiRecorder.

8. Click *Apply*.

Streaming recorded video clips to YouTube

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

To stream live video to YouTube

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

Using the monitor display port

On FortiRecorder-100D and 400D models, there is a video display port. You can specify which camera's video will be displayed on the screen.

To use the monitor display

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

Using Chromecast with FortiRecorder

You can use Google Chromecast with FortiRecorder to remotely monitor video streams from a camera on a mobile device, a computer, or a TV.

For FortiRecorder to discover the Chromecast device, you must connect it to a FortiRecorder private network port. However, for Chromecast to fetch and stream videos from FortiRecorder, FortiRecorder must have a public port reachable from the Internet and a valid certificate. See also Configuring the public port numbers and domain name on page 37 and Replacing the default certificate for the GUI on page 93.

In addition to streaming video content, FortiRecorder can also stream photos to a Chromecast device.

To connect Chromecast to FortiRecorder

1. Connect Chromecast to a FortiRecorder private network port.
2. On the FortiRecorder GUI, go to *Service* > *Chromecast* > *Device*.
3. Click *Discover* to search for Chromecast.

   If successful, the discovered device will be listed in the device table.See also Appendix A: Port numbers on page 174.

To configure Chromecast in FortiRecorder manually

1. Go to *Service* > *Chromecast* > *Device*.
2. Either click *New* to manually add and configure a new device, or select a discovered device from the device list and click *Configure*.
3. Enable *Status*.
4. Enter the name, location, and address of the Chromecast device.
5. Select the way to present the information on the Chromecast device from the *Layout* drop-down menu.
6. Select the cameras that you want to stream.
7. Click *Create*.

To stream photos to a Chromecast device

1. Go to *Service* > *Chromecast* > *Image*.
2. Click *Add*.
3. Select the file and then click *Open*.

Analyzing logs and alerts

You can use log messages and alerts to analyze important events that have been recorded on FortiRecorder.

Configuring log settings

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. See also Understanding the logs on page 111.

⚠ Avoid recording very frequent log messages, or that use low thresholds for *Log level* such as *Information* or *Notification*, to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

To configure logging

1. Go to *Logs & Alert* > *Log Settings* > *Local.*

   Alternatively, if you want logs to be stored remotely, go to *Logs & Alert* > *Log Settings* > *Remote*.
2. If you are configuring locally stored logs, 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 23:00 (11:00 PM) on 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 details, see Log severity levels on page 111 .
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:

Setting Name	Description
	- *Do not log* — Discard all new log messages. - *Overwrite* — Delete the oldest log file in order to free disk space, and store the new log message.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log. You can enable an entire category of event, such as Detection Events or you can enable individual detections within each category by expanding the category and then toggling the event you want to log.

3. If you are 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 details, see Log severity levels on page 111 . **Caution**: Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.
Facility	Select the facility identifier the FortiRecorder will use to identify itself to the Syslog server if it receives logs from multiple devices. To easily identify log messages from the FortiRecorder when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CSV format	Enable if your Syslog server requires comma-separated values (CSV). **Note**: Do not enable this option if the remote host is a FortiAnalyzer. FortiAnalyzer does not support CSV-formatted log messages.
Logging Policy Configuration	Select what type of FortiRecorder events and camera events you want to log.

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

If you will be sending logs to a FortiAnalyzer appliance, you must add the FortiRecorder to the device list on FortiAnalyzer, 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 Configuring routing on page 30) and the policies on any intermediary firewalls or routers (they must allow Syslog traffic from the FortiRecorder network interface that is connected to the gateway between it and the Syslog server). To determine the point of connectivity failure along the network path, if the FortiAnalyzer or Syslog server is configured to respond to ICMP ECHO_REQUEST (ping), go to *Dashboard* > *Console* and enter the command:

```
execute traceroute <syslog_ipv4>
```

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

Configuring alert email

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

To configure alert email settings

1. Configure the mail server settings so that FortiRecorder can send email. For details, see Configuring email settings for notifications on page 78.
2. Go to *Logs & Alert* > *Alert Email* > *Configuration*.
3. Click *New*.

   You can configure up to 10 recipient email addresses.
4. In *Email to*, enter the recipient email address that FortiRecorder will use, such as:

   ```
   admin@example.com
   ```

   This setting is 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. See Configuring notification triggers on page 86.
5. Click *Create*.
6. Go t o *Logs & Alert* > *Alert Email* > *Category*. Mark the check boxes of all appliance events that you want to trigger an alert, such as:

Setting Name	Description
System events	Enable to notify when serious system events occur such as daemon crashes. See also Resource issues on page 153.
Disk is full	Enable to notify when the disk partition that stores log data is full. See also Data storage issues on page 154.
Camera device altered	Enable to notify when a defined camera configuration has been enabled or disabled, or if there are problems with the camera. (The FortiRecorder will not control or record video from a camera that is not enabled in its list of known, configured devices. See Configuring cameras on page 50 .)
Camera communication error	Enable to notify when there has been a network error during communications between the FortiRecorder and camera. See also Connectivity issues on page 155.

Setting Name	Description
Camera recording error	Enable to notify when an issue prevents a camera from recording. See also Video viewing issues on page 152 and Connectivity issues on page 155.
Camera alert summary	Enable notify when various alerts have been triggered.
Video disk events	Enable to notify when the disk partition that stores video data is full. See also Data storage issues on page 154.

7. Click *Apply*.

Best practices

Fine-tuning and best practice tips can help to run your FortiRecorder appliance securely and reliably.

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

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

Hardening security

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

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

Topology

- To protect your surveillance system from hackers and unauthorized network access, install the FortiRecorder appliance and cameras behind a network firewall such as a FortiGate. FortiRecorder is not a firewall. FortiRecorder appliances are designed specifically to manage cameras and store video.
- If remote cameras or people will be accessing the appliance via the Internet, through a virtual IP or port forward on your router or FortiGate, configure your router or firewall to restrict access, allowing only their IP addresses. Require firewall authentication for connections from network administrators and security guards.
- Make sure traffic cannot bypass the FortiRecorder appliance in a complex network environment, accessing the cameras directly.
- If you do not need remote access while traveling or at home, do not configure it. If you do, however, apply strict firewall policies to the connection, and harden all accounts and administrative access (see Administrator access on page 142, and Operator access on page 142, and Configuring the public port numbers and domain name on page 37). Keep the FortiRecorder software up-to-date, especially with security patches(see Updating the firmware on page 39).
- Disable all network interfaces that should not receive any traffic. (Set the *Administrative Status* to *Down*.)

  For example, if administrative access is typically through port1, cameras are connected to port2, and network file storage and the Internet are connected to port3, then 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. See Setting the "admin" account password on page 25.
- 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 (see Trusted hosts on page 64).
- 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 Configuring administrator profiles on page 66 .
- By default, an administrator login times out if it is idle for more than 5 minutes. You can change this to a longer period in the idle timeout settings, but Fortinet does not recommend it. Left unattended, a GUI or CLI session could allow anyone with physical access to your computer to change FortiRecorder settings. Small idle timeouts mitigate this risk. See Configuring the public port numbers and domain name on page 37.
- Restrict administrative access to a single network interface (usually port1), and only allow the management access protocols that you use.

  Use only the most secure protocols. Disable *Access: PING*, except during troubleshooting. Disable *Access: HTTP*, *Access: SNMP*, and *Access: TELNET* unless the network interface only connects to a trusted, private administrative network. See Configuring network interfaces on page 26 .

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 or FortiRecorder authentication, see Replacing the default certificate for the GUI on page 93 .
- Immediately revoke certificates that have been compromised. If possible, automate the distribution of certificate revocation lists (see Revoking certificates on page 99).

Optimizing performance

When configuring your FortiRecorder, many settings and practices can yield better performance.

All deployment components can affect performance:

- FortiRecorder
- cameras
- computer with FortiCentral or a web browser that connects to FortiRecorder

Total performance is a combination of:

- input—video compression, image quality, image complexity, video resolution, frame rate, number of cameras
- output—to either FortiCentral or a web browser, for both live video streams and playing previous recordings
- storage—copies of video files for each motion detection clip, or only markers in an existing continuous recording (markers are smaller than copies of large video files)

Performance bottlenecks are often:

- network bandwidth usage to and from FortiRecorder
- CPU usage of the computer

FortiCentral or your web browser must decode and render the video streams from the FortiRecorder. Displaying multiple video streams is CPU intensive.

See also Sizing guidelines on page 145.

Computer CPU usage

If you need to simultaneously display 8 or more live video streams from cameras, then depending on how powerful the computer hardware is, you might need to improve CPU usage.

Playing many videos can cause high CPU usage. (RAM is less important than CPU for rendering video.) If you experience video where the motion "freezes" or is not smooth, or if cameras do not quickly respond to PTZ controls, then use the diagnostic tools available on your OS (such as Task Manager on Microsoft Windows) to examine CPU usage while you are experiencing video problems. If possible, keep the CPU usage below 50%.

To optimize performance, you can use the video and camera profiles. Define and assign another video stream for each camera. Reduce the video resolution, quality and/or frames per second of the other video stream. This can increase the number of live views that the computer can display, or reduce the CPU usage.

For live video streams, 10 FPS is often enough. It significantly reduces the system resource load on your computer compared to 30 FPS, which might be required if the camera records an area with more movement.

See Configuring video profiles on page 46

FortiRecorder RAM and CPU usage

Delete or disable unused cameras. FortiRecorder allocates memory with each camera, regardless of whether it is currently receiving video from it. Extra cameras increase memory usage.

CPU usage can also increase if you configure *Storage Options*.

Logging and alert performance

If you have a FortiAnalyzer appliance, store the logs from FortiRecorder on FortiAnalyzer to avoid system resource usage associated with writing logs to the hard disks on FortiRecorder. See Configuring log settings on page 137.

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

Reduce repetitive log messages. Use the alert email settings, to define the interval that emails are sent if the same condition persists following the initial occurrence. See Configuring alert email on page 139.

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

Packet capture performance

Packet capture can be useful for troubleshooting but can be resource intensive. 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 stop the command when you are finished.

Network bandwidth usage

To reduce latency associated with DNS queries, use a DNS server on your local network as your primary DNS.

Bandwidth usage correlates with the number of simultaneous video streams, video bit rate, and storage options (local or remote). See also Bandwidth per camera on page 146, Configuring log settings on page 137, Configuring video profiles on page 46, and Configuring camera profiles on page 48.

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

- Maximum number of cameras streaming to the FortiRecorder simultaneously
- Recording schedule (motion detection-triggered only or continuous)
- Video resolution, frame rate, and image quality

Output performance factors

- Number of user sessions
- Number of live camera views per user session
- Maximum number of simultaneous live views by users

Resolution has the most impact on the overall performance.

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

High resolution video generates 3 times as much raw data as the default, medium resolution. If a raw video stream cannot be efficiently compressed, then the result is that **bandwidth and/or disk space required per camera, and per login session, are multiplied**.

For example, for a FortiCam-20A camera, FortiRecorder can store on its local hard drive about 36 days' worth of high resolution video, but about 240 days' worth of low resolution video.

Amount of motion in the camera's field of view also affects performance. Constant and/or rapid motion or color changes result in larger files and video streams, because video compression 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 Configuring external storage on page 76).

Variable vs. constant bit rate video

Variable bit rate mode means that the network bandwidth used by the camera varies by:

- video profile settings
- what the camera records

People and things that move or have flashing lights also result in more bandwidth usage. High resolution video profiles use more bandwidth than medium or low resolution (see Bandwidth per camera on page 146).

Constant bit rate mode means that the bandwidth used by the camera is relatively constant, regardless of what the camera records. It is more predictable in deployments where bandwidth and/or storage capacities are limited. Bandwidth used by the video stream is determined by the bit rate setting.

In general, variable bit rate mode has relatively consistent video quality, but bandwidth varies. Constant bit rate mode has video quality that varies, but predictable bandwidth. You can choose a constant bit rate mode with more bandwidth to avoid lower quality that can otherwise occur during rapid motion, but the compromise is that it uses unnecessary bandwidth when there is no activity.

Usually, there is little difference in video quality between variable and constant bit modes (assuming the same screen resolution and frame rates), and the constant bit rate mode gives more reliable output from cameras.

Sizing guidelines

To choose appropriate hardware and settings for your FortiRecorder deployment, consider how much data can be generated for both input and output.

Input varies by:

- Number of video streams from each camera (not just the total number of cameras)
- Video recording schedules (motion only or continuous) of each camera
- Video resolution, frame rate, bitrate mode (constant or variable) and its parameters (bitrate or image quality)
- Number of detection events
- Number of snapshots and motion detection video recordings
- Storage settings (NAS or remote storage, re-compression, and deletion of old recordings)

Output varies by:

- Number of simultaneous user sessions
- Maximum number of simultaneous live video streams by users
- Video resolution, frame rate, bitrate mode (constant or variable) and its parameters (bitrate or image quality)

See also Optimizing performance on page 142, or contact your Fortinet reseller.

Number of supported cameras

See Appendix B: Maximum values on page 176.

Bandwidth per camera

Constant bit rate video is a simple calculation of:

```
video resolution x frame rate x number of cameras
```

Variable bit rate

Depending on resolution, frame rate and video quality, each camera using H.264 compression can use the following network bandwidth:

- 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

The following table can be used to estimate. 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 noise reduction), then the required bit rate might be lower. If video compression is set to lower quality or capped at a defined maximum bandwidth, then the bit rate can be significantly lower, but image quality is also reduced. DNR can reduce bandwidth usage even more, especially for grainy night images, but shows less detail during motion.

Avoid using networks with less than half of the bandwidth indicated in the following table.

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

Bitrate/screen resolution	Frame rate				
	1	6	10	15	30
CIF (352 x 240 pixels)	0.16	0.2	0.24	0.3	0.4
D1 (0.4 Mbps; 720 x 576 pixels)	0.4	0.5	0.6	0.75	1
720p (1 Mbps)	0.8	1	1.2	1.5	2
SXGA (1.3 Mbps; 1280 x 1024 pixels)	1	1.25	1.5	1.9	2.5
HD (2 Mbps; 1920 x 1080 pixels)	1.6	2	2.4	3	4

Bitrate/screen resolution	Frame rate				
	1	6	10	15	30
3 Mbps	2	2.5	3	3.75	5
5 Mbps	3.2	4	4.8	6	8

Bandwidth per FortiRecorder

Recommended maximum total bandwidth usage varies by FortiRecorder model and deployment scenarios such as network attached storage (NAS), continuous recording only, or continuous recording with separate video clips for motion detection.

Model	Continuous	Continuous with NAS	Continuous with motion	Continuous with motion and NAS
FRC-100D	90 Mbps	TBC	35 Mbps	TBC
FRC-200D gen1	90 Mbps	55 Mbps	50 Mbps	50 Mbps
FRC-200D gen2	135 Mbps	135 Mbps	130 Mbps	130 Mbps
FRC-400D	170 Mbps	160 Mbps	140 Mbps	130 Mbps

These values have been determined experimentally in a lab setting and do not represent hard limits. Performance degrades gradually if enough bandwidth is not available, with symptoms such as a slow response or dropped video frames. Real world performance depends on many factors, including network and NAS type. The table above assumes a motion detection rate of 13% based on 1 detection that is 40 s long every 5 minutes per camera.

Storage capacity

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

To calculate storage capacity, you can estimate that a 1 TB hard drive stores 1 camera configured to consume 1 Mbps for approximately 100 days.

Video retention period in days for hard drive capacities:

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

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 balance between quality and bandwidth.

Software updates and backups

Update to the newest firmware as soon as possible to receive new security features and stability enhancements.

Regular configuration backups are also important.

Backups

Make a backup before doing anything that can cause large configuration changes, such as:

- upgrading the firmware
- entering the CLI commands `execute factory reset` or `execute restore`

- clicking the *Restore* button in the *System Information* widget on the dashboard

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

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

- troubleshoot a non-functional configuration by comparing it with this functional baseline (via tools such as `diff`)
- rapidly restore your installation to a simple yet working point (see Restoring a previous configuration on page 150)
- 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 on page 150)

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

Backups can be performed on-demand, but you can also schedule FortiRecorder to make them regularly. Alternatively, you can also use FortiCentral to back up the FortiRecorder configuration.

Configuration backups do not include backups of video data or logs. For information about video backup, see Configuring external storage on page 76.

To back up the configuration (on-demand)

1. Log in to the GUI as the `admin` administrator.

   Other administrator accounts do not have the required permissions.
2. Go to *Dashboard* > *Status*.
3. In the *System Information* widget, in the *System configuration* row, click *Backup*.

   Alternatively, go to *System* > *Maintenance* > *Configuration* and click *System configuration backup*.

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

To back up the configuration (scheduled)

1. Log in to the GUI as the `admin` administrator.

   Other administrator accounts do not have the required permissions.
2. Go to *System* > *Maintenance* > *Configuration*.
3. Expand the *Scheduled Backup* section.
4. Select the frequency, either:
   - *Not scheduled* (disabled; backups are on-demand only)
   - *Daily*
   - *These Days*

   and then configure:
   - *Max backup number*: The maximum number of backup files. When this limit is reached, FortiRecorder will not make more backups until you delete an existing backup file.
   - *At hour*: The time of day when the backup occurs, according to a 24-hour clock.
   - days of the week (this option appears only if you selected *These Days*)
5. If you want to store backups on FortiRecorder local storage, then enable it.

6. If you want to store backups on a remote server, then enable it and expand that section. Configure the following settings:

Setting Name	Description
Protocol	Currently only SFTP is supported.
Server name/IP	Enter the domain name or IP address of the server.
User name	Enter the user name that FortiRecorder will use when it connects to the server.
Password	Enter the password for that user name.
Remote directory	Enter the path of the folder on the server, such as `/Users/FortiRecorder`, where the FortiRecorder appliance will store the data.

7. Click *Apply*.

Restoring a previous configuration

If you downloaded a configuration backup, you can upload it to revert the appliance's configuration to that state.

Restoring the configuration can also be used to reconfigure the appliance from its default settings (including during provisioning), after downgrading the firmware, or after a clean install.

Configuration files can also be used as a script to batch configure many features or appliances at once: download a configuration file backup, edit the file in a plain text editor such as Notepad++ or Microsoft Visual Studio Code, then upload the configuration to the FortiRecorder appliances.

To upload a configuration via the GUI

1. Go to *Dashboard* > *Status*.

   In the *System Information* widget, in the *System configuration* row, click *Restore*.

   Alternatively, go to *System* > *Maintenance* > *Configuration* and click *Restore Configuration*.
2. Locate the FortiRecorder configuration backup file. (It has a `.conf` file extension.)
3. Click *Upload*.

   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 GUI session will be terminated when the FortiRecorder appliance restarts.
4. To continue using the GUI, if you have not changed the IP address and static routes of the GUI, refresh the page in your web browser and log in again.

   Otherwise, to access the GUI again, in your web browser, modify the URL to match the new IP address of the network interface. For details, see Connecting to the FortiRecorder GUI on page 22.

Troubleshooting

These guidelines can help you resolve issues if your FortiRecorder appliance is not behaving as you expect.

Login issues

If you cannot go to the login page at all, it is usually a connectivity issue instead (see Connectivity issues on page 155) unless all accounts are configured to accept login only from specific IP addresses, or authentication has been externalized to an LDAP or RADIUS server.

If a user lost or forgot their password, the "admin" account can reset other accounts' passwords (see Resetting passwords on page 151).

When an administrator account cannot log in from a specific IP

If an administrator is entering the correct account name and password, but cannot log in from some or all computers, then examine that account's trusted host setting. It should include all networks 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 (for example, FortiAuthenticator or Microsoft Active Directory), 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 on page 155). 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 tracing on page 163).

Resetting passwords

If someone has forgotten or lost their password, or if you need to change an account's password and you do not know its current password, the "admin" administrator can reset the password.

If you forget the password of the administrator, however, you will not be able to reset its password through the GUI. You can reset the FortiRecorder to its default state (including the default administrator account and password) by restoring the firmware. For instructions, see Installing firmware on page 40.

To reset an account's password

1. Log in as the `admin` administrator account.
2. Go to *System* > *User* > *User*.
3. Select the row to select the account whose password you want to change.
4. 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.

Not able to push setting and log shows an error on password

A problem can occur when you try to push settings to the FortiCamera. The log message shows an issue with the password.

FortiRecorder will change the FortiCamera password during the initial configuration. The password is unique to each FortiCamera and is based on the MAC address. To fix the problem, perform the following:

1. Perform a factory reset on the physical FortiCamera. For details, see Resetting the configuration on page 170.
2. Manually add the MAC address of the FortiCamera to the FortiRecorder settings.

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, verify that you have installed software that can view live streams (which use RTP) and files (which use MP4 format).

Different media players can interfere with each other. By default, some installers take file type associations previously belonging to other players and re-assign them to the new software. If you installed software to view downloaded video files, for example, and suddenly could no longer view live video streams, you might need to fix the file associations for RTP and/or MP4.

If you have installed a suitable media player but still cannot view the video, try clicking the panel arrows to hide and then show the panel again. For some Windows computers, this can solve the problem. (This QuickTime issue does not affect macOS computers.)

If this does not trigger the video to play, verify 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 FortiRecorder

If the camera itself does not seem to be sending video to the FortiRecorder, although it has booted, has network connectivity, and you have configured a recording schedule on the FortiRecorder, you may see camera log messages such as:

```
Camera 'c1' is in an incorrect state: 'idle'. The expected state is 'continuous'.
```

Usually this is self-correcting. If not, or if a camera is otherwise unresponsive, reboot the camera:

```
execute camera reboot <camera_name>
```

If this does not solve the problem, try either upgrading the camera's firmware or resetting the camera to factory defaults, then re-configuring it (see the camera's QuickStart Guide).

Notification issues

If you are not receiving any email after motion detection records a clip, but you have configured camera notifications, first verify that the SMTP email settings on your FortiRecorder are correct, and that it can connect to your email server to send email. Then check that notifications are not being blocked or sent to your spam or junk mail folder. (Some anti-spam systems mistakenly mark repeated or frequent email as spam.)

If you are receiving the email, and there are video links (that is, FortiRecorder has not been configured to email still images but you cannot view the video from the email:

1. Verify that you have installed the QuickTime video player software on your computer.
2. Verify that your computer can connect to the IP address of FortiRecorder. 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 GUI and/or view video clips while out of the office, you must configure port forwarding and/or a virtual IP (VIP) on your firewall or Internet router, and configure the FortiRecorder to link to this public IP address in snapshot notifications.

If you are receiving too many notifications, change the configuration so that your FortiRecorder will only send snapshot notifications during suspicious periods, and focuses motion detection only on areas that do not cause false alerts, such as fans or blinking lights.

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
```

then you can view the current resource consumption of each process by entering this CLI command:

```
diagnose system top 10
```

That 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).

If you find a PID with abnormally high resource usage, you can terminate it:

```
diagnose system kill 9 <pid_int>
```

If the issue recurs, and corresponds with a hardware or configuration change, you might need to change the configuration (especially to reduce frequent logging, reduce high resolution video streams, and change video storage options), reduce traffic load, or contact Fortinet Technical Support.

Downloading a trace log

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

Trace logs are compressed into an archive (`.gz` file extension), and contain information that supplements debug-level log files.

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

Data storage issues

If FortiRecorder cannot locally store any data such as logs, reports, and video, 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:

```
System Time:  2023-06-27 11:13:25 EDT (Uptime: 0d 20h 51m)
Filesystem      Size  Used Avail Use% Mounted on
proc               0     0     0    - /proc
sysfs              0     0     0    - /sys
devtmpfs        1.0G  7.6M 1017M   1% /dev
none               0     0     0    - /dev/pts
/dev/sdb1       371M  178M  193M  48% /data
/dev/vga/vga2   137G  409M  135G   1% /var/log
/dev/vga/vga3   2.6T  2.4T  177G  94% /var/spool
cgroup             0     0     0    - /cgroup/cpu_and_mem
```

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, and not stop logging when the disk is full. This might not prevent full disk problems for other features, however. To free disk space, delete files such as old reports and video that you do not 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 write problems. For details, contact Fortinet Technical Support.

Deleting all video clips

Enter the LI commands:

```
execute partitionlogdisk
execute formatvideodisk
```

FortiRecorder reboots.

Currently there is no CLI command to delete an individual video clip.

Connectivity issues

One of your first tests when configuring a new device should be to determine whether data such as video is received, and whether commands and schedules are being sent to it. You should also test whether notification email can be sent, and user accounts can log in to the GUI and view live video feeds.

After initial setup, connectivity should not be interrupted. FortiRecorder might sometimes be able to recover if, for example, a camera receives a new IP address from the DHCP server. However this can cause 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, examine the following in order:

1. Checking hardware connections on page 155
2. Bringing up network interfaces on page 156
3. Examining the ARP table on page 156
4. Examining routing on page 157
5. Discovery fails on page 160
6. Multiple DHCP servers on page 160
7. Unauthorized DHCP clients or DHCP pool exhaustion on page 161
8. Examining IP sessions on page 161
9. Resolving IP address conflicts on page 163
10. Examining live video streams on page 163
11. Packet tracing on page 163

Troubleshooting is in order from more low-level OSI layers of your network (physical, link/Ethernet, network/IP) to the higher-level, more application-specific protocols. If your network is not new, then lower-level networking is usually already working, so you might want to start with later sections instead. Application-layer protocols such as RTSP are more often specific to FortiRecorder, cameras, and surveillance devices.

Checking hardware connections

If no traffic arrives on a network interface even though the configuration appears to be correct, or if network performance is less than you expect, then it might be a problem with the physical hardware. Verify the following in order:

1. 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.
2. Verify that the LED lights for the network ports indicate a firm electrical contact when you plug network cables into the appliance. For LED indications, see your model's QuickStart Guide.
3. If traffic ingresses and egresses, but performance is not what you expect, verify that the *MTU* matches other devices on your network.
4. If the hardware connections are firm and the appliance is powered on, but you cannot connect — even using a local console connection to the CLI rather then a network connection — then there might be a problem during boot. Verify that the network interface is up (see Bringing up network interfaces on page 156). If the network interface is already up, or if you cannot connect to verify it, contact Fortinet Technical Support.

Bringing up network interfaces

If a network interface is disabled, all connections will fail—regardless of whether the cables are physically connected.

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, change the *Administrative Status* setting. The column does not indicate 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.

In the GUI, 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 the CLI:

```
config system interface
   edit port2
      set status up
end
```

Examining the ARP table

When connectivity cannot be established or is periodically interrupted, but hardware and link status is not an issue, the first place to look is at a slightly higher layer in network connections: the address resolution protocol (ARP) table. While most devices' MAC address is bound to the hardware at the manufacturer and not easily changed, some devices have configurable or virtual MACs. In this case, you should verify that 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
```

Examining routing

If the MAC resolves correctly, but IP connectivity fails, try using ICMP 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.

IP layer connectivity fails when routes are incorrectly configured. Static routes specify where to send traffic when it leaves 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 (for example, each of which should receive packets destined for a different subset of IP addresses), redundant routers (for example, redundant Internet, WAN, or 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 computer is not directly attached to one of the physical ports of the FortiRecorder appliance, you might also require a static route so that your computer can connect with the GUI and CLI.

To determine which route a packet will be subject to, FortiRecorder examines each packet's destination IP address and compares it to those of the static routes. It will forward the packet along to the route with the largest prefix match, automatically egressing from the network interface on that network. (Egress port for a route cannot be manually configured.) If multiple routes match the packet, the FortiRecorder appliance will apply the route with the smallest index number. For this reason, you should give more specific routes a smaller index number than the default route.

The ping command sends a small data packet to the destination and waits for a response. The response has a timer that may expire, indicating that the destination is unreachable via ICMP. ICMP is part of Layer 3 on the OSI Networking Model. ping sends Internet Control Message Protocol (ICMP) `ECHO_REQUEST` packets to the destination, and listens for `ECHO_RESPONSE` packets in reply. Beyond basic existence of a possible route between the source and destination, ping tells you the amount of packet loss (if any), how long it takes the packet to make the round trip (latency), and the variation in that time from packet to packet (jitter).

Similarly, traceroute sends ICMP packets to test each hop along the route. It sends three packets to the destination, and then increases the time to live (TTL) setting by one, and sends another three packets to the destination. As the TTL increases, packets go one hop farther along the route until they reach the destination.

Most traceroute commands display their maximum hop count — that is, the maximum number of steps it will take before declaring the destination unreachable — before they start tracing the route. The TTL setting may result in routers or firewalls along the route timing out due to high latency. If you specify the destination using a domain name, the traceroute output can also indicate DNS problems, such as an inability to connect to a DNS server.

By default, FortiRecorder appliances will respond to ping and traceroute. However, if FortiRecorder does not respond, and there are no firewall policies that block it, ICMP type 0 (`ECHO_REPSPONSE` or "pong") might be effectively disabled. By default, `traceroute` uses UDP with destination ports numbered from 33434 to 33534. The `traceroute` utility usually has an option to specify use of ICMP `ECHO_REQUEST` (type 8) instead, as used by the Windows `tracert` utility. If you have a firewall and you want traceroute to work regardless of your computer's OS (Apple macOS, Linux, and Microsoft Windows), then you must 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 GUI, you must have *Read* and *Write* permission in your administrator's account access profile to items in the *Router Configuration* category.
2. In the row for the network interface which you want to respond to ICMP type 8 (`ECHO_REQUEST`) for ping and UDP for traceroute, click *Edit*.
3. Enable *Access: PING*.

   Disabling *PING* only prevents FortiRecorder from **receiving** ICMP type 8 (`ECHO_REQUEST`) or type 30 and traceroute-related UDP.

   It does not disable FortiRecorder CLI commands such as `execute ping` or `execute traceroute` that **send** such traffic.

   Since you typically use these tools only during troubleshooting, you can allow ICMP, the protocol used by these tools, on interfaces only when you need them. Otherwise, disable ICMP for improved security and performance.
4. Click *OK*.

   The appliance should now respond when another device such as your management computer sends a ping or traceroute to that network interface.

To verify routes between cameras and FortiRecorder

1. Use the `execute ping` command on FortiRecorder 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.

   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 computer (which is temporarily substituting for the camera) 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 <1 ms 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 GUI 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 or other problems at the physical, network, and transport layer.

If these tests succeed and 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.

   Also, if the computer's DNS query cannot resolve the host name, output similar to the following appears:

   ```
   example.com: Name or service not known
   Cannot handle "host" cmdline arg `example.com' on position 1 (argc 1)
   ```

Discovery fails

Discovery of devices by the FortiRecorder uses UPnP and ONVIF. For it to work, devices usually must be on the same IP subnet as the FortiRecorder, and must not be blocked by firewalls or other network filtering. If cameras are not on the same subnet, you may still be able to facilitate discovery traffic by configuring your FortiGate or other device with multicast forwarding.

If you do not know which device is impeding discovery, you can either:

- Temporarily attach the cameras to a closer point on the network, such as a local switch or directly to the FortiRecorder, so that discovery is not blocked.
- Manually add the camera to the FortiRecorder unit's list of known cameras, skipping discovery.

Multiple DHCP servers

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 (for example, 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 on page 163)

To verify that your appliance and cameras are sending and receiving lease requests, you can perform a packet trace (see Packet tracing on page 163) and/or use the event log to look for:

- `DHCPDISCOVER` (destination IP address is broadcast, not specifically to FortiRecorder)
- `DHCPOFFER`
- `DHCPREQUEST`
- `DHCPACK`

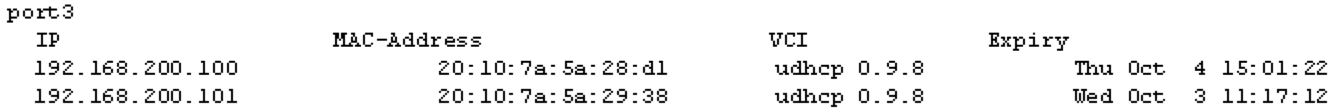
Unauthorized DHCP clients or DHCP pool exhaustion

Usually, returning DHCP clients will receive the same IP address lease. However if computers or other devices are accidentally using IP addresses that the FortiRecorder's built-in DHCP server should be allocating to cameras, and the pool of available DHCP IP addresses becomes exhausted, cameras may be unable to get or retain an IP address.

To determine which devices are using your pool of DHCP IP addresses, compare the MAC address of each device's network adapter to the list of current DHCP clients in *Monitor* > *DHCP* > *DHCP* or enter this command in the CLI:

```
execute dhcp lease-list
```

Output is like the following:



```
port3
  IP                      MAC-Address                    VCI              Expiry
  192.168.200.100                20:10:7a:5a:28:d1       udhcp 0.9.8            Thu Oct  4 15:01:22
  192.168.200.101                20:10:7a:5a:29:38       udhcp 0.9.8            Wed Oct  3 11:17:12
```

To correct this situation, first configure unintentional DHCP clients so that they do not use DHCP (that is, they have a static IP address) and so their IP address is not in the range used by the DHCP pool. Second, clear the list of DHCP clients to allow legitimate DHCP clients (your cameras) to obtain a lease:

```
execute dhcp clear-lease
```

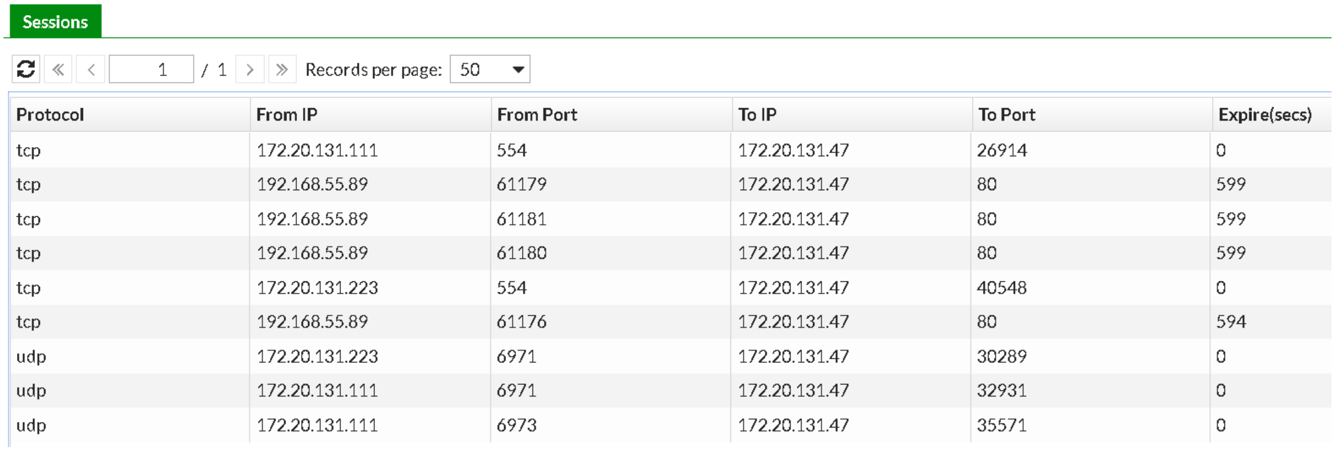
New clients that were previously unable to get an IP address will obtain an IP address for the first time. Returning clients' s IP addresses may change as the built-in DHCP server no longer has any memory of their previous lease, and may assign them a new IP address if another client has claimed that IP address first. (This may result in temporary IP address conflicts and therefore connectivity interruptions while the DHCP server assigns new leases.)

Examining 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, then there are multiple possible causes, such as:

- *Trusted hosts* is misconfigured
- protocols or port numbers mismatched or blocked by NAT or firewalls
- IP address conflicts
- short DHCP server Lease time (Seconds) on page 34
- socket exhaustion

You can view a snapshot of FortiRecorder's session table according to the IP layer. Go to *FortiView* > *Sessions* > *Sessions*.



Sessions

1 / 1 Records per page: 50

Protocol	From IP	From Port	To IP	To Port	Expire(secs)
tcp	172.20.131.111	554	172.20.131.47	26914	0
tcp	192.168.55.89	61179	172.20.131.47	80	599
tcp	192.168.55.89	61181	172.20.131.47	80	599
tcp	192.168.55.89	61180	172.20.131.47	80	599
tcp	172.20.131.223	554	172.20.131.47	40548	0
tcp	192.168.55.89	61176	172.20.131.47	80	594
udp	172.20.131.223	6971	172.20.131.47	30289	0
udp	172.20.131.111	6971	172.20.131.47	32931	0
udp	172.20.131.111	6973	172.20.131.47	35571	0

GUI Item	Description
Protocol	The protocol of the session according to the "protocol" ID number field (or, for IPv6, "next header") in the IP header of the packets. • *icmp* — 1 (Due to the speed of ICMP messages, this is rarely seen in the session list.) • *tcp* — 6 • *udp* — 17 (Due to the speed of UDP datagrams, this is rarely seen in the session list.)
From IP	The source of the session according the source field in the IP header. If source NAT is occurring, this is not necessarily the IP address in the original packet from the client.
From Port	The source port number. For a list of port numbers that can originate from the FortiRecorder, see Appendix A: Port numbers on page 174.
To IP	The destination according to the destination field in the IP header. If destination NAT is occurring, this is not necessarily the IP address in the original packet from the client.
To Port	The destination port number. For a list of port numbers that can be received by the FortiRecorder, see Appendix A: Port numbers on page 174.
Expire (seconds)	The session timeout in seconds. The expiry counter is reset when packets are sent or received, indicating that the session is still active.

To refresh the session list snapshot with the most current list, click the dotted circle (*Refresh*) icon to the left of *Records per page*.

To sort the session list based upon the contents of a column, hover your mouse cursor over the column's heading then click the arrow that appears on the right side of the heading, and select either *Sort Ascending* or *Sort Descending*.

If you expect sessions that do not exist, be aware that some protocol designs (notably UDP) do not have persistent sessions. Their sessions will almost immediately expire and be removed from the session list, and therefore it may be very difficult to get a session list snapshot during the short time that the datagram is being transmitted. TCP has persistent connections, where the socket is maintained until data transmission either is confirmed to be finished or times out. Therefore TCP connections 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 on page 174).

If you notice unexpected sessions with the FortiRecorder GUI or CLI, verify that you have configured all accounts' *Trusted hosts* setting.

Resolving IP address conflicts

If two or more devices are configured to use the same IP address on your network, this will cause a problem called an IP address conflict. Only one of those identically addressed devices can have IP-layer connectivity at a given time. The other will be ignored, effectively causing it to behave as if it were disconnected. (If multiple devices were to use the same IP address, routers and switches would not be able to determine with certainty where to deliver a packet destined for that IP address. To prevent this, routers and switches will only let one of the devices use the IP.)

Typically IP conflicts are caused when either:

- you have accidentally configured 2 devices with the same static IP address
- you have accidentally configured a device with a static IP address that belongs to the DHCP pool
- 2 DHCP servers accidentally have pools in the same range of IP addresses, and are each independently assigning their clients the same IP addresses

Your cameras, of course, have no screen, and cannot display any IP address conflict error message. However, you may notice symptoms such as interrupted video streams whenever a new device connects to the network or reboots.

If you have configured your FortiRecorder's built-in DHCP server, first verify that it is not using the same DHCP pool as another DHCP server on your network. Next, you can use the CLI to determine whether MAC addresses from other devices' network adapters have stolen IP addresses that should belong to your cameras. See Unauthorized DHCP clients or DHCP pool exhaustion on page 161. If, however, you have transitioned your cameras to use static IP addresses, you must use another method.

- Use the ARP table of either your FortiRecorder (see Examining the ARP table on page 156) or router to determine which MAC address (and therefore which computer or 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.

Examining live video streams

Live video feeds are sensitive to packet loss, latency, and high bandwidth usage. This can cause video that is blurry or motion that is not smooth (low video frame rate). For details on how to diagnose these problems, see Packet tracing on page 163 and Video performance on page 144.

Packet tracing

When troubleshooting networks, verifying hardware connections and routing with `execute ping` and `execute traceroute` CLI commands are often enough to diagnose the problem. For more rare problems, you can use traffic capture to see more low-level information.

Packet tracing is also known as packet sniffing, packet capture, packet analysis, or traffic capture. It can record information about all of the Ethernet frames that arrive—regardless of whether the destination MAC address matches the network interface.

FortiRecorder appliances have a built-in packet trace feature. By using it, you or Fortinet Support can diagnose problems that are otherwise difficult to detect. For example, it can show:

- malformed packets (protocol is not RFC-compliant)
- dropped packets
- intermittent packet loss during ping
- wrong network address translation (NAT)
- wrong port forwarding
- wrong session setup
- ARP broadcast storms or floods
- OSI Layer 2 bridge loops
- SSL/TLS handshake errors
- wrong source address when a device has multiple IP addresses, on multiple networks

For example, you can make a packet trace during a continuous ping. This shows ARP MAC address resolution, the source and destination IP addresses, the protocols and port number used, and whether FortiRecorder received a reply (the destination was reachable via that route) as expected.

CPU usage and disk space usage is increased during a packet trace. On busy networks, this can be very resource intensive, and cause delays in live video streams. Performance is better if you packet trace only:

- while required, and stop when finished
- when the network is not busy, maybe at night
- with a local console CLI connection, not network (Telnet/SSH/HTTP/HTTPS)

If you only need a simple packet capture, configure it via GUI, where it can be given a time limit.

Before using packet capture, think about filter criteria. Too much data is more difficult to analyze. It will be easier if you :

- limit the time range, or number of packets
- exclude IP addresses, port numbers, and protocols that are not relevant

For example, maybe you only need to trace communications with one device, or only RTP video packets.

More complex IP address, port number, and protocol filters can be configured via CLI.

Packet tracing via GUI

1. Go to *System* > *Network* > *Traffic Capture*.
2. Click *New*.
3. Configure the following settings:

Setting Name	Description
Description	Enter a unique name for the packet trace file.
Duration	Enter a time range for the packet trace.
Interface	Select which network interface you want to trace traffic with, or *All* to trace traffic on all network interfaces.
IP/Host	Optional. If you want to trace traffic only to specific destination IP addresses, enter up to 3 domain names or IP addresses. Alternatively, configure *Exclusion* instead.
Filter	Select either: • *None*: Capture all port numbers and protocols.This can be required by protocols that use multiple port numbers, or to see a correlated sequential order of multiple protocols. For example, it is common to see DNS over UDP before HTTPS over TCP, and RTCP before RTP. • *Use protocol*: Only capture traffic on the port number you specify. Valid range of port numbers is from 1 to 65535.
Exclusion	Optional. If you don't want to trace traffic with specific IP addresses or port numbers, enter the domain names or IP addresses and port numbers to exclude. Alternatively, configure *IP/Host* instead.

4. Click *Create*.

   Packet tracing begins immediately.
5. When the packet trace is complete, either refresh the page in your web browser, or return to *System* > *Network* > *Traffic Capture*. (If the traffic capture is complete, its *Status* column will show *Stopped*.)
6. Click to select the packet trace file, and then click *Download*.
7. On your computer, open the PCAP file in compatible software such as Wireshark.

   Compare the captured traffic with the expected behavior.

Packet tracing via CLI

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. Therefore it is usually easier to analyze the output by saving it to a file, and then opening it in a network protocol analyzer application.

For example, you could use PuTTY to save the output to a file. Methods vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY or OpenSSH
- plain text editor such as Notepad++
- Perl interpreter such as Strawberry Perl
- fgt2eth.pl script (download at the bottom of Using the FortiOS built-in packet sniffer)
- network protocol analyzer software such asWireshark

The fgt2eth.pl script is provided as-is, without any implied warranty or technical support.

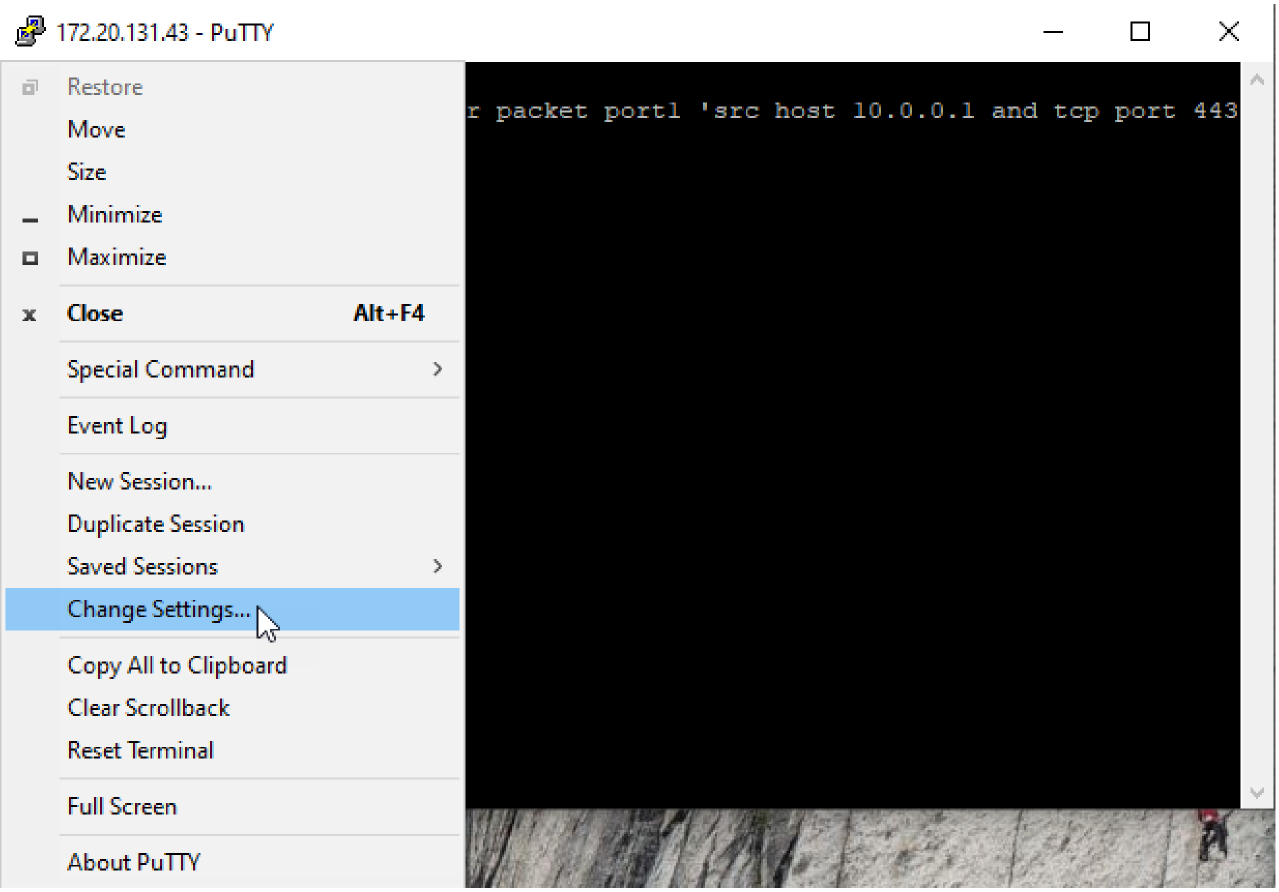
To use packet capture with PuTTY and Wireshark

1. On your computer, start PuTTY. Connect to the FortiRecorder appliance using a local console, SSH, or Telnet connection.
2. Type the packet capture command, but **do not press Enter yet**.

   For example, to capture HTTPS and HTTP traffic with the source IP address 10.0.0.1, you can type:

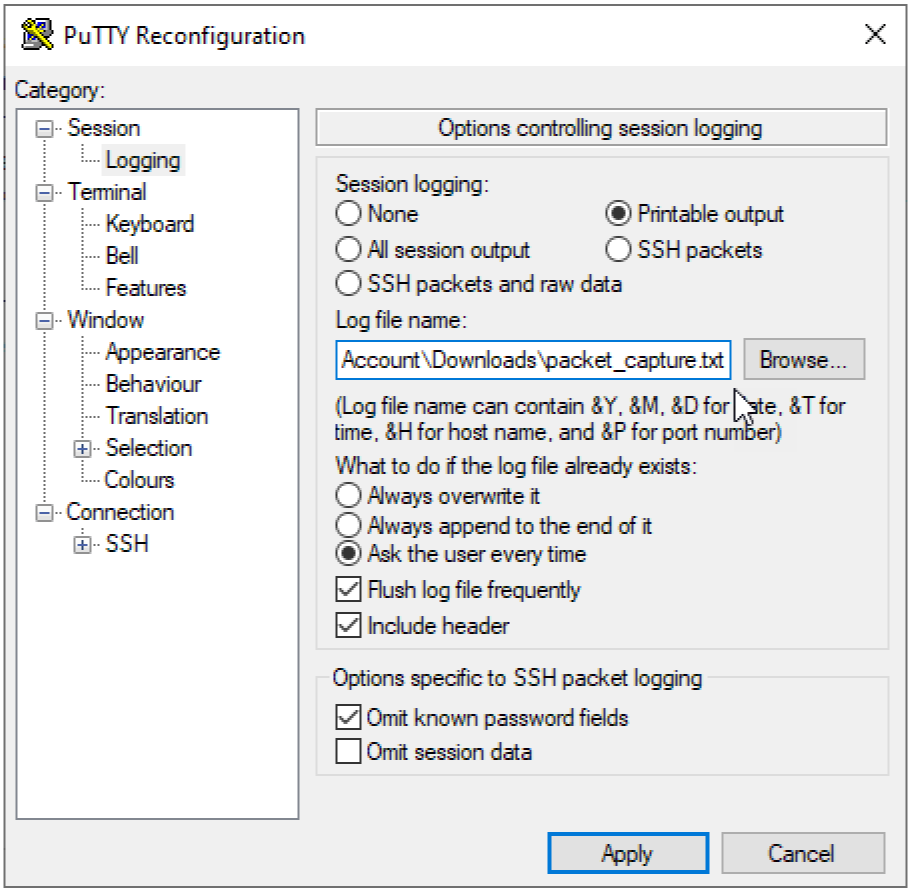
   ```
   diagnose sniffer packet port1 'src host 10.0.0.1 and (tcp port 443 or tcp port 80)' 3
   ```

   See also diagnose sniffer CLI syntax on page 168.
3. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then click *Change Settings*.



```
r packet port1 'src host 10.0.0.1 and tcp port 443
```

   A dialog appears where you can configure PuTTY to save output to a plain text file.
4. In the *Category* tree on the left, go to *Session* > *Logging*.
5. In the *Session logging* area, select *Printable output*.
6. In *Log file name*, click the *Browse* button, then choose where to save the packet capture file, such as `C:\Users\MyAccount\Downloads\packet_capture.txt`. (You do not need to save it with the `.log` file extension.)



Session logging:

○ None ● Printable output

○ All session output ○ SSH packets

○ SSH packets and raw data

Log file name:

Account\Downloads\packet_capture.txt

(Log file name can contain &Y, &M, &D for date, &T for time, &H for host name, and &P for port number)

What to do if the log file already exists:

○ Always overwrite it

○ Always append to the end of it

● Ask the user every time

☑ Flush log file frequently

☑ Include header

Options specific to SSH packet logging

☑ Omit known password fields

□ Omit session data

7. Click *Apply*.
8. Press Enter on the CLI to start packet capture.

   If you did not specify a number of packets to capture, then when you have captured enough, press Ctrl + C.
9. Close the PuTTY window.
10. Start Notepad++. Open the packet capture file.
11. Delete the first and last lines, which look like this:

   ```
   =~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2023.06.16 11:58:00 =~=~=~=~=~=~=~=~=~=~=~=
   ...

   FK400D3016000000 #
   ```

   These are a PuTTY timestamp and the command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the conversion script in the next step.
12. Open a command prompt (`cmd.exe`). Enter the commands to to use `fgt2eth.pl` to convert plain text file to a PCAP format:

   ```
   cd C:\Users\MyAccount\Downloads\
   fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
   ```

   where:

   - `packet_capture.txt` is the name of the packet capture file from PuTTY
   - `packet_capture.pcap` is the name of the converted output file
13. On your computer, open the PCAP file in compatible software such as Wireshark.

   Compare the captured traffic with the expected behavior.

diagnose sniffer CLI syntax

Packet capture syntax on FortiRecorder appliances is similar to that of FortiGate appliances. If you omit all parameters for the command, the command captures all packets on all network interfaces until you press Ctrl + C.

```
diagnose sniffer packet [{any | <interface_name>}
   [{none | '<filter_str>'}
   [{1 | 2 | 3 | 4 | 5 | 6}
   [<packets_int>
   [{a | <any_str>}]]]]]
```

where:

- `<interface_name>` is the name of a network interface, such as port1. Alternatively, type `any` to match all network interfaces.
- `'<filter_str>'` is the filter that specifies which protocols and port numbers that you want to capture, such as `'tcp port 80'`.Filters use `tcpdump` syntax. If you do not want a filter, but you want to configure parameters after this one, type `none`.
- `<packets_int>` is the number of packets to capture before stopping. If you do not specify this parameter, packet capture output is printed to your CLI display until you stop it by pressing Ctrl+C.
- `{a | <any_str>}` is either `a` (to include an absolute, full UTC timestamp in the format yyyy-mm-dd hh:mm:ss.ms; use this format if you need to correlate a FortiRecorder packet capture with another device's packet capture), or any other text (to include a timestamp that is the amount of time since he start of the packet capture, in the format ss.ms)

- `{1 | 2 | 3 | 4 | 5 | 6}` is an integer indicating which details to include about network interface names, Ethernet frames, IP packet headers, and/or packet payloads.
  - `1` — Include the packet capture timestamp, and basic fields of the IP header: source IP address, destination IP address, protocol name, and destination port number. Does **not** display all fields of the IP protocol header.

    Example:

    ```
    interfaces=[any]

    filters=[none]

    0.747195 172.20.131.143.6970 -> 172.20.131.43.33740: udp 1448
    ```

  - `2` — All of the output from 1, plus the packet payload in both hexadecimal and ASCII.

    Example:

    ```
    interfaces=[any]

    filters=[none]

    0.927132 172.25.188.213.60407 -> 172.20.131.43.22: ack 594494863

    000000   45 00 00 28 63 d2 40 00 7c 06 02 cf ac 19 bc d5        E..(c.@.|.......

    000010   ac 14 83 2b eb f7 00 16 39 9f 83 88 23 6f 45 8f        ...+....9...#oE.

    000020   50 10 17 ff ed 72 00 00 00 00 00 00 00 00              P....r........
    ```

- `3` — All of the output from 2, plus the link frame (Ethernet) header.
  Example:

  ```
  interfaces=[any]
  filters=[none]
  0.131709 172.20.132.187.6970 -> 172.20.132.43.38262: udp 99
  000000   00 00 00 00 00 01 00 22 f4 ce 5e 04 08 00 45 00        ......."..^...E.
  000010   00 7f 62 15 00 00 40 11 b7 49 ac 14 84 bb ac 14        ..b...@..I......
  000020   84 2b 1b 3a 95 76 00 6b c6 48 80 e0 cf f4 59 ba        .+.:.v.k.H....Y.
  000030   bd 77 12 be 36 32 41 9b 98 01 89 8c 05 21 1e 23        .w..62A......!.#
  000040   35 c4 6b 11 8f 34 10 47 88 d8 38 8c d8 41 1e 23        5.k..4.G..8..A.#
  000050   60 d0 8e c4 78 8f 11 8e fa 23 70 27 e6 80 c2 11        `...x....#p'....
  000060   c3 7a 80 f1 9b 01 fb 36 9f 50 16 3c 9d dc 07 9e        .z.....6.P.<....
  000070   a0 08 48 fc 02 cc 27 80 57 0f c1 56 68 06 e8 47        ..H...'.W..Vh..G
  000080   01 1e 23 81 08 47 00 66 07 e0 04 20 80                 ..#..G.f.....
  ```

- `4` — All of the output from 1, plus the network interface name. This can be necessary if you are capturing packets from multiple network interfaces at once, and need to know which packet was seen by which interface.
  Example:

  ```
  interfaces=[any]
  filters=[none]
  0.942892 port1 in 172.20.131.143.6970 -> 172.20.131.43.33740: udp 1448
  ```

- `5` — All of the output from 2, plus the network interface name.
  Example:

  ```
  interfaces=[any]
  filters=[none]
  0.394962 port1 in 172.25.188.213.60407 -> 172.20.131.43.22: ack 594500767
  000000   45 00 00 28 66 a9 40 00 7c 06 ff f7 ac 19 bc d5        E..(f.@.|.......
  000010   ac 14 83 2b eb f7 00 16 39 9f 8d 98 23 6f 5c 9f        ...+....9...#o\.
  000020   50 10 18 00 cc 51 00 00 00 00 00 00 00 00              P....Q........
  ```

- `6` — All of the output from 3, plus the network interface name.

  Example:

  ```
  interfaces=[any]
  filters=[none]
  0.790631 port1 in 172.25.188.213.60407 -> 172.20.131.43.22: ack 594502111
  000000   00 00 00 00 00 01 90 6c ac 99 ce 60 08 00 45 00        .......l...`..E.
  000010   00 28 67 10 40 00 7c 06 ff 90 ac 19 bc d5 ac 14        .(g.@.|.........
  000020   83 2b eb f7 00 16 39 9f 8f 78 23 6f 61 df 50 10        .+....9..x#oa.P.
  000030   18 00 c5 31 00 00 00 00 00 00 00 00                    ...1........
  ```

Example: HTTPS packet capture

In this example, you capture all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses verbosity level 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 command 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.)

```
FK400D3016000013 # diagnose sniffer packet port1 'tcp port 443' 3
System Time:  2023-06-16 16:07:51 EDT (Uptime: 4d 6h 48m)
interfaces=[port1]
filters=[tcp port 443]
4.795077 172.25.188.213.56340 -> 172.20.131.43.443: syn 457421310
000000   00 10 f3 37 6c e3 90 6c ac 99 ce 60 08 00 45 00        ...7l..l...`..E.
000010   00 34 69 6b 40 00 7c 06 fd 29 ac 19 bc d5 ac 14        .4ik@.|..)......
000020   83 2b dc 14 01 bb 1b 43 b1 fe 00 00 00 00 80 02        .+.....C........
000030   fd 80 2e bb 00 00 02 04 05 48 01 03 03 08 01 01        .........H......
000040   04 02                                                  ..
```

Resetting the configuration

Before you sell 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 and export any important video recordings before beginning this procedure, if possible. It erases the configuration and data on the local storage of FortiRecorder. You cannot undo the operation, except by restoring the configuration. Data cannot be restored. See Backups on page 148.

Alternatively, you can reset the FortiRecorder's configuration to its factory default values for a specific software version by restoring the firmware during a reboot (a "clean install"). See Restoring firmware ("clean install") on page 171.

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 securely delete your data from the FortiRecorder, enter these commands:

```
execute erase-filesystem
execute formatlogdisk
```

To reset the FortiRecorder's configuration, enter this command:

```
execute factoryreset
```

After the procedure, either you or the next owner must perform setup again. Resetting the configuration could include the IP addresses of network interfaces, so that person must re-connect to the CLI or GUI in order to perform setup. See Setup on page 19.

Restoring firmware ("clean install")

Restoring the firmware can be useful if:

- you are unable to connect to the FortiRecorder appliance using the GUI or the CLI
- you want to install firmware without preserving any existing configuration ("clean install") a firmware version that you want to install requires a different size of system partition (see the Release Notes for 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 Software updates and backups on page 148. For information on reconnecting to a FortiRecorder appliance whose network interface configuration was reset, see Connecting to the FortiRecorder GUI on page 22 .

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, macOS, 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 shut down 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. Press 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. Press 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 Restoring a previous configuration on page 150 .

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

Appendices

This section contains reference tables.

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 numbers used by FortiRecorder services. Many are configurable. See the Configuring the public port numbers and domain name on page 37 for incoming traffic; for outgoing traffic, see the documentation for each feature.

Outgoing traffic

These are the port numbers and protocols that FortiRecorder uses to connect to the cameras, your servers, and services on the Internet such as FortiCloud and FortiGuard.

Port Number	Protocol	Purpose
N/A	ICMP	`execute ping` and `execute traceroute` CLI commands. See Connectivity issues on page 155.
N/A	ARP	MAC address resolution
22	TCP	SFTP for configuration backups. See Backups on page 148.
25	TCP	SMTP for alert email and notifications about motion detection. See Configuring alert email on page 139 and Configuring notification triggers on page 86.
53	UDP	DNS queries for domain names. See Configuring network interfaces on page 26.
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 cameras on page 50.
123	UDP	NTP clock time synchronization. By default, FortiRecorder synchronizes its time with NTP servers at Fortinet. See Configuring the system time on page 39.
443	HTTPS	• Sending network settings and other configurations to cameras • Face recognition AI license validation by Fortinet. See Upload licenses on page 45.

Port Number	Protocol	Purpose
514	UDP	Syslog for external logging. See Configuring log settings on page 137.
554, 8554	TCP/UDP	Controlling video recording (RTSP). See Viewing live video on page 107.
5353	UDP	mDNS, UPnP, and ONVIF queries for discovery of cameras and Chromecast. Multicast to 224.0.0.251. See Discovering cameras in remote networks on page 46.

Incoming traffic

These are the default listening port numbers and protocols on FortiRecorder.

Port Number	Protocol	Purpose
N/A	ICMP	Responses to `execute ping` and `execute traceroute` CLI commands. See also Access: PING on page 28 .
N/A	ARP	MAC address resolution responses
21	TCP	FTP for receiving motion detection video clips from cameras. See Configuring notification triggers on page 86 Currently, this port number is not configurable.
22	TCP	SSH administrative CLI access. See also Access: SSH on page 28.
23	TCP	Telnet administrative CLI access. See also Access: TELNET on page 28.
80	TCP	HTTP administrative GUI access. See also Access: HTTP on page 28.
443	TCP	HTTPS administrative GUI access. Only occurs if the destination address is a network interface's IP address. See also Access: HTTPS on page 28.
5000-14999	UDP	Receiving video from cameras (RTP). See also Access: RTSP on page 29.
554	TCP	Live video feeds (RTP) in the HTTP/HTTPS administrative GUI. See Viewing live video on page 107.
3010	TCP	Camera-based notifications. See Configuring notification triggers on page 86. Currently, this port number is not configurable.
3011		
8550	TCP	Tunnel with FortiCentral to use the cameras, store face recognition data, and more. See also Access: FRC-Central on page 28 and the FortiCentral User Guide.

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.

	FortiRecorder 100D	FortiRecorder 200D/400D/400F	FortiRecorder VM
Cameras connected	16	64	Up to 1024 Controlled by license
System interfaces	5	10	10
Routes	20	250	250
Administrator accounts	20	50	250
LDAP profiles	20	20	50
SNMP communities	2	16	16
SNMP community hosts	2	16	16
Remote log servers	1	3 (400F: 5)	3
Local certificates	256	256	256
CA certificates	256	256	256
Remote certificates	256	256	256
SNMP users	16	16	16
SNMP user hosts	16	16	16
Camera groups	256	256	256
DHCP server leases	256	256	256
Camera notifications	256	256	256
Video profiles	256	256	256
Camera profiles	32	256	256
Schedules	256	256	256
Motion detection windows	3	3	3
Privacy mask windows	3	3	3

FORTINET®

www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.