



# FortiRecorder - SD Branch Deployment Guide

Version 2.7.2

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<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/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



October 23, 2019

FortiRecorder 2.7.2 SD Branch Deployment Guide

00-272-591034-20191023

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>SD-Branch configuration using VPN tunnels</b>	<b>6</b>
Obtaining camera information	6
Establishing a tunnel	7
Configuring the HQ FortiGate tunnel	9
Configuring the cameras	9
<b>SD-Branch configuration using NAT</b>	<b>12</b>
Configuring port forwarding and routing	12
Creating a policy	14
Setting up RTSP on FortiGate	15
Configuring the cameras	16
Real-Time Streaming Protocol (RTSP) session helper	17
<b>Monitoring SD-Branch recordings on the HQ FortiRecorder</b>	<b>19</b>

## Change Log

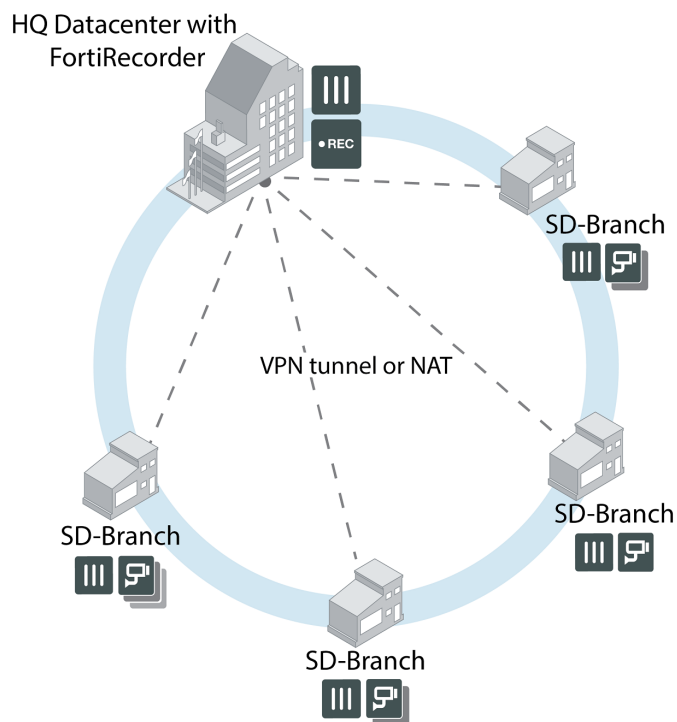
Date	Change Description
2019-10-23	Initial release.



# Introduction

This deployment guide demonstrates how to configure your FortiRecorder and FortiCameras using edge recording in a typical SD-Branch scenario.

This setup is optimal when there are several branch offices with a small number of cameras connected to an HQ datacenter with a FortiRecorder. See the example diagram below.



SD-Branch edge recording allows you to manage cameras across multiple branches from a single HQ FortiRecorder through a VPN tunnel or NAT. In this configuration, only status information is exchanged between the camera and recorder, resulting in the use of less bandwidth than when transferring video.

Captured video is recorded onto the local SD card of the camera, and can be viewed from the HQ FortiRecorder after a short delay while the video downloads. FortiCameras set up in this way can be configured to record continuously or with motion detection only. When a live stream is required, the recorder establishes a streaming connection to the camera that stays active as long as the view is in use.

Edge recording in an SD branch scenario can be set up using one of two methods:

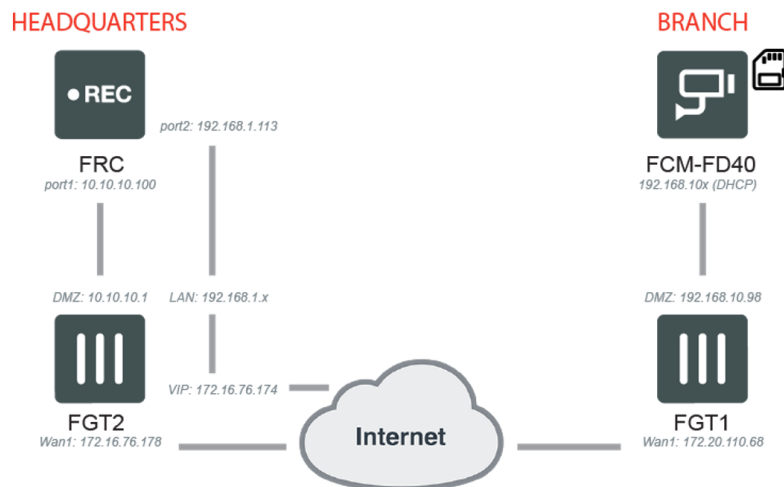
- [SD-Branch configuration using VPN tunnels on page 6](#)
- [SD-Branch configuration using NAT on page 12](#)

# SD-Branch configuration using VPN tunnels

In order to configure a FortiRecorder SD-Branch using VPN tunnels, complete the following steps:

1. [Obtaining camera information on page 6](#)
2. [Establishing a tunnel on page 7](#)
3. [Configuring the HQ FortiGate tunnel on page 9](#)
4. [Configuring the cameras on page 9](#)

The topology and example addresses used for these instructions are as follows:



## Obtaining camera information

First you will need to obtain the IP address of your DHCP enabled camera in FortiGate. Make note of the MAC address of the camera before deployment.

**To obtain the addresses of your cameras:**

1. Go to *Network > Interfaces*.
2. Select the interface, and click *Edit*.
3. Enable *Device Detection*.



Device detection does not work with all camera models.

**FortiWiFi 60D** FWF60D4613008166

Dashboard > Edit Interface

Security Fabric >

FortiView >

Network >

Interfaces >

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Create New Edit Delete

Starting IP 192.168.10.100 End IP 192.168.10.120

Netmask 255.255.255.0

Default Gateway Same as Interface IP Specify

DNS Server Same as System DNS Same as Interface IP Specify

Advanced...

Networked Devices

Device Detection ☒

Active Scanning ☐

Admission Control

Security Mode None

Enforce FortiClient Compliance Check ☐

4. Go to **User & Device > Device Inventory**.
5. Copy the Address numbers for your cameras.

**FortiWiFi 60D** FWF60D4613008166

Dashboard >

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

User Definition

User Groups

Guest Management

Device Inventory >

Custom Devices & Groups

Refresh Edit Delete Search

Status	Device	User	Address	Interfaces	OS
Online	00:d0:89:13:59:c8		192.168.10.100 (DHCP)	dmz	FortiCam
Online	08:00:27:4b:44:01		192.168.1.69	local_bridge	FortiRecorder
Offline	08:00:27:98:ac:d7		192.168.2.99	local_bridge	FortiRecorder
Offline	20:10:7a:5a:29:18		192.168.1.101	local_bridge	FortiCam
Offline	90:6c:ac:d9:3b:9e		192.168.1.107	local_bridge	FortiCam
Linux PC 2					
Windows device 1					
Unknown device 15					

Alternatively, you can look at FGT1 Monitor-DHCP monitor.

## Establishing a tunnel

With the camera addresses obtained, you can now establish a tunnel between the HQ and the branch.

**To establish a tunnel:**

1. In the FortiGate branch, go to *VPN > IPsec Wizard*.
2. Enter a name and select the *Site to Site* template type.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name: HQ-Branch

Template Type: **Site to Site** Remote Access Custom

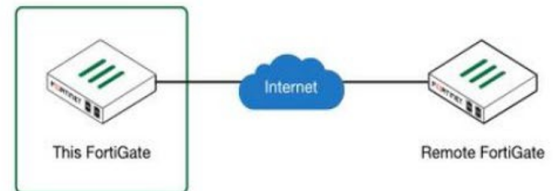
Remote Device Type: **FortiGate**

NAT Configuration: **No NAT between sites**

This site is behind NAT

The remote site is behind NAT

Site to Site - FortiGate



< Back Next > Cancel

3. Select *FortiGate* for the Remote Device Type.
4. For NAT Configuration, select *No NAT between sites*, then click *Next*.
5. Enter the address of your headquarters FortiGate.

1 VPN Setup 2 Authentication 3 Policy & Routing

Remote Device: **IP Address** Dynamic DNS

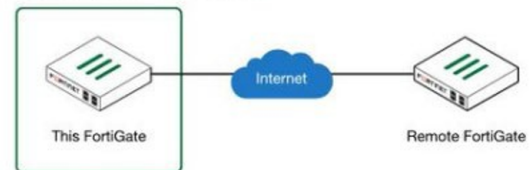
IP Address: 172.16.76.178

Outgoing Interface: wan1

Authentication Method: **Pre-shared Key** Signature

Pre-shared Key: \*\*\*\*\*

HQ-Branch: Site to Site - FortiGate



< Back Next > Cancel

6. Enter the pre-shared key, and select *Next*.
7. Select your local interface from the dropdown menu.

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing

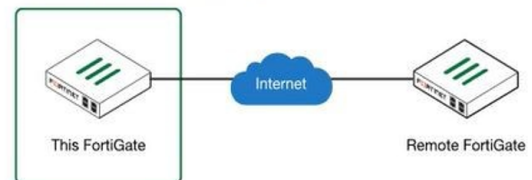
Local Interface: dmz

Local Subnets: 192.168.10.0/24

Remote Subnets: 10.10.10.0/24

Internet Access: **None** Share WAN Force to use remote WAN

HQ-Branch: Site to Site - FortiGate

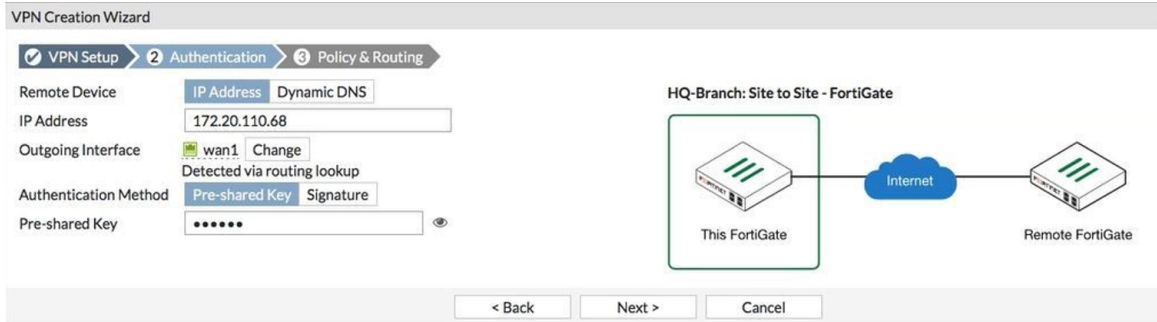


< Back Create Cancel

8. Enter the address where the cameras are located in the Local Subnets field.
9. Enter the address where your FortiRecorder is located in the Remote Subnets field, then select *Create*.

## Configuring the HQ FortiGate tunnel

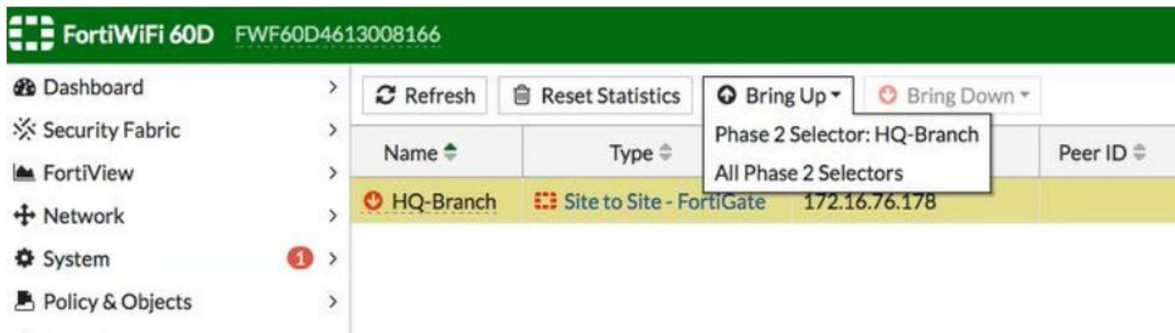
You can now set up the HQ FortiGate tunnel following a similar procedure as before; however, in the Authentication portion of the VPN Creation Wizard, enter the WAN1 address for the branch where the cameras are located.



The screenshot shows the 'VPN Creation Wizard' in the 'Authentication' step. The 'Remote Device' is 'IP Address' with the value '172.20.110.68'. The 'Outgoing Interface' is 'wan1' with a 'Change' button. The 'Authentication Method' is 'Pre-shared Key'. A diagram on the right shows 'This FortiGate' connected to 'Remote FortiGate' via the 'Internet'. Navigation buttons at the bottom are '< Back', 'Next >', and 'Cancel'.

Field	Value
Remote Device	IP Address
IP Address	172.20.110.68
Outgoing Interface	wan1
Authentication Method	Pre-shared Key
Pre-shared Key	*****

Once completed, bring up the tunnel.



## Configuring the cameras

Cameras can now be configured in FortiRecorder, and routing can be established to the FortiGate HQ.

**To set up a camera in FortiRecorder:**

1. Go to *Camera > Configuration > Camera Profile*.
2. Select an existing camera and select *Edit* or select *New*.

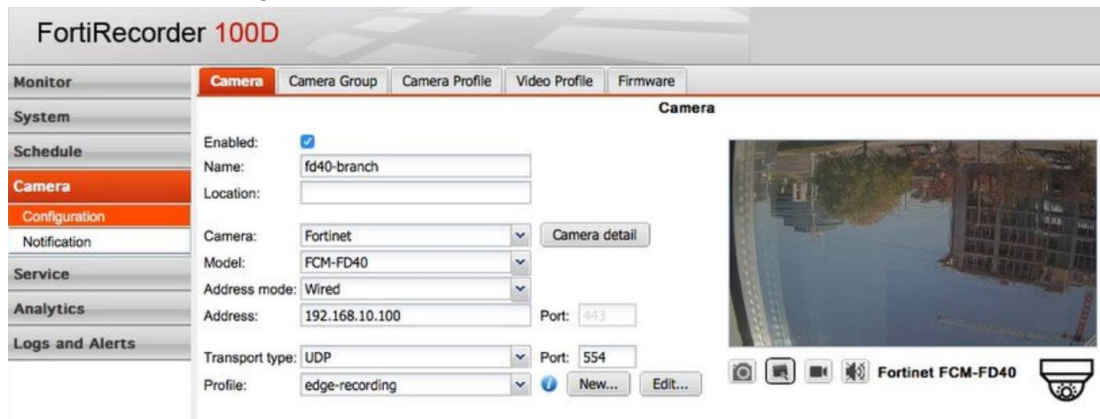
The screenshot shows the 'Camera Profile Settings' page in FortiRecorder. The 'Name' field is set to 'edge-recording'. Under the 'Video' section, 'Recording stream profile' is set to 'high-resolution' and 'Viewing stream profile' is set to '--Use Recording Stream--'. The 'Recording' section shows 'Recording type' with 'Motion detection' selected, and 'Store on' with 'SD card' selected. The 'Edge Download' section has 'Continuous recordings' and 'Detection recordings' both set to 'Automatic'. The 'Storage Options' section has 'Continuous recordings' and 'Detection recordings' both set to 'Keep until overwritten'. The 'Compression Options' section has 'Continuous recordings' set to 'None'. At the bottom are 'Create' and 'Cancel' buttons.

3. Name the profile and edit the settings as desired.  
Edge recording works with either continuous or motion detection.
4. In the Recording section, enable *SD card*.
5. Select *Create*.
6. Go to *System > Network > Routing*.
7. Select *New*.

The screenshot shows the 'Edit Routing Entry' page in FortiRecorder. The 'Destination IP/netmask' field is set to '192.168.10.0 / 24'. The 'Interface' dropdown menu is set to '--None--'. The 'Gateway' field is set to '10.10.10.1'. At the bottom are 'Create' and 'Cancel' buttons.

8. Enter the DMZ subnet of your branch location where the cameras are located in the Destination IP/netmask field.
9. Select the desired interface and enter the gateway.
10. Select *Create*.
11. Ping the camera from the recorder.

12. Go to *Camera > Configuration > Camera*.



The screenshot displays the FortiRecorder 100D web interface. On the left is a navigation menu with options: Monitor, System, Schedule, Camera (highlighted), Configuration, Notification, Service, Analytics, and Logs and Alerts. The main content area is titled 'Camera' and contains several tabs: Camera, Camera Group, Camera Profile, Video Profile, and Firmware. The 'Camera' tab is active, showing configuration fields for a camera named 'fd40-branch'. The fields include: Enabled (checked), Name (fd40-branch), Location (empty), Camera (Fortinet), Model (FCM-FD40), Address mode (Wired), Address (192.168.10.100), Port (443), Transport type (UDP), and Profile (edge-recording). There are buttons for 'Camera detail', 'New...', and 'Edit...'. A live video feed of a street scene is shown on the right, with a 'Fortinet FCM-FD40' camera icon at the bottom right.

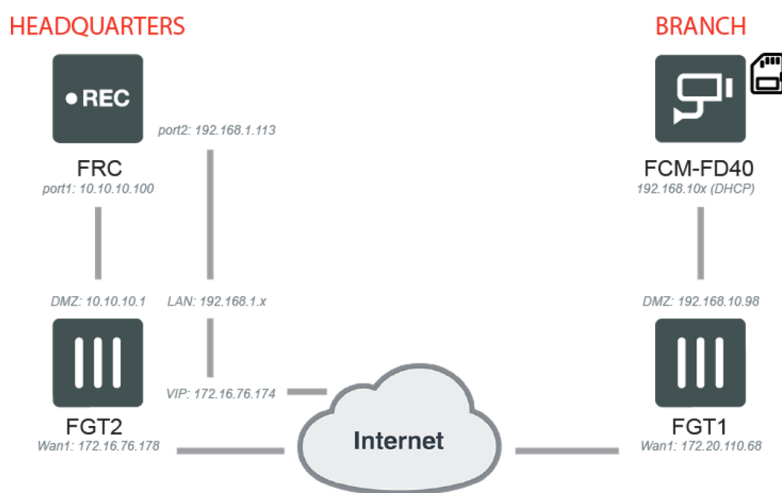
13. Enter the necessary details and select *Wired* from the address mode dropdown menu.
14. Enter the address, select *edge-recording* from the Profile dropdown menu, and select *Create*.

# SD-Branch configuration using NAT

In order to configure a FortiRecorder SD-Branch using NAT, complete the following steps:

1. [Configuring port forwarding and routing on page 12](#)
2. [Creating a policy on page 14](#)
3. [Setting up RTSP on FortiGate on page 15](#)
4. [Configuring the cameras on page 16](#)
5. [Real-Time Streaming Protocol \(RTSP\) session helper on page 17](#)

The topology and example addresses used for these instructions are as follows:



## Configuring port forwarding and routing

You will first need to port forward the WAN1 camera in the FortiGate branch.



### To configure forwarding and routing:

1. Go to *Policy & Objects > Virtual IPs*.
2. Click *Create New* and *Virtual IP*.

The screenshot shows the 'New Virtual IP' configuration window in the FortiWiFi 60D GUI. The 'Name' field is set to 'FD40-HTTPS'. The 'Interface' is set to 'wan1'. The 'Type' is 'Static NAT'. The 'External IP Address/Range' is '172.20.110.68' and the 'Mapped IP Address/Range' is '192.168.10.100'. The 'Port Forwarding' section is highlighted with a red box, showing 'TCP' selected as the protocol, '4430' as the external service port, and '443' as the mapped port. The 'Optional Filters' are disabled. The 'OK' and 'Cancel' buttons are at the bottom right.

3. Enter a name for the Virtual IP.
4. Select the WAN1 interface from the dropdown interface menu.
5. Enable *Port Forwarding* and select *OK*.



The External Service Port range is required during camera configuration. See [Configuring the cameras on page 16](#).

You can now make a virtual IP group to apply the policy to the entire group, rather than individual VIPs.

1. Go to *Policy & Objects > Virtual IPs*.
2. Click *Create New* and *Virtual IP Group*.

The screenshot shows the 'Edit VIP Group' configuration window in the FortiWiFi 60D GUI. The 'Name' field is set to 'FD40-branch'. The 'Interface' is set to 'wan1'. The 'Members' list contains 'FD40-HTTPS' and 'FD40-RTSP'. The 'OK' and 'Cancel' buttons are at the bottom right.

3. Enter a name for the group.

4. Select the cameras in the group from the Members section.
5. Select **OK**.

## Creating a policy

You will now need to create a policy to route.

**To create a policy to route:**

1. Go to *Policy & Objects* > *IPv4 Policy*.
2. Select **Create New**.

The screenshot shows the 'Edit Policy' dialog in the FortiWiFi 60D configuration interface. The policy is named 'FD40-branch'. The 'Incoming Interface' is set to 'wan1' and the 'Outgoing Interface' is set to 'dmz'. The 'Source' is set to 'all' and the 'Destination' is set to 'FD40-branch'. The 'Schedule' is set to 'always' and the 'Service' is set to 'ALL'. The 'Action' is set to 'ACCEPT'. The 'Firewall / Network Options' section shows 'NAT' is enabled and 'Proxy Options' are set to 'default'. The 'Security Profiles' section shows 'AntiVirus', 'Web Filter', and 'DNS Filter' are all disabled. The 'VIP Group' is set to 'FD40-branch', the 'Interface' is 'wan1', and the 'Members' are 'FD40-HTTPS' and 'FD40-RTSP'. The 'References' are set to '1'. The 'OK' and 'Cancel' buttons are at the bottom right.

3. Enter a name for the policy.
4. Select *wan1* for the incoming interface and *dmz* for the outgoing interface.
5. Select the VIP group for the Destination.
6. Enter the rest of the options as desired, and click **OK**.

The camera will now be available under 172.20.110.68:4430.

The screenshot shows the 'Policy Lookup' table in the FortiWiFi 60D configuration interface. The table lists various policies and their configurations. The columns are: ID, Name, From, To, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. The table contains 18 rows of data, including policies for local bridges, WAN interfaces, and the newly created 'FD40-branch' policy.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
15		any	any	all	all	always	Brickcom_Upnp	DENY			All	
16		any	any	all	all	always	Senao_Upnp	DENY			All	
14		any	any	all	all	always	Dowse_Onvif	DENY			All	
13		any	any	all	all	always	Dynacolor_UPnP	DENY			All	
9		local_bridge	wan2	all	all	always	ALL	ACCEPT	Enabled		UTM	0 B
10		local_bridge	wan2	all	all	always	ALL_ICMP	ACCEPT	Disabled		UTM	0 B
1		local_bridge	wan1	all	all	always	ALL	ACCEPT	Enabled		All	1.62 GB
4		local_bridge	wan1	all	all	always	ALL_ICMP	ACCEPT	Enabled		All	0 B
12		wan1	local_bridge	all	Port VIP	always	ALL	ACCEPT	Enabled		UTM	108 B
7		wan1	local_bridge	all	WMB Private LAN	always	ALL	ACCEPT	Disabled		UTM	1.68 MB
8		any	any	Brickcom Default	Brickcom Default	always	ALL	DENY			All	0 B
11		wan2	local_bridge	all	all	always	ALL	ACCEPT	Disabled		UTM	0 B
17	DMZ-wan1	dmz	wan1	all	all	always	ALL	ACCEPT	Enabled		UTM	1.51 MB
18	FD40-branch	wan1	dmz	all	FD40-branch	always	ALL	ACCEPT	Disabled		UTM	89.42 MB
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	544.34 kB

## Setting up RTSP on FortiGate

To set up the RTSP:

1. Go to *Policy & Objects > Virtual IPs*.
2. Click *Create New* and *Virtual IP*.

FortiWiFi 60D FWF60D4613008166

Dashboard > New Virtual IP

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy >

Addresses >

Wildcard FQDN Addresses >

Internet Service Database >

Services >

Schedules >

Virtual IPs >

IP Pools >

Proxy Options >

Traffic Shapers >

Traffic Shaping Policy >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Name: FD40-RTSP

Comments: 0/255

Color: Change

Network

Interface: wan1

Type: Static NAT

External IP Address/Range: 172.20.110.68 - 172.20.110.68

Mapped IP Address/Range: 192.168.10.100 - 192.168.10.100

Optional Filters: ☐

Port Forwarding: ☒

Protocol: TCP UDP SCTP ICMP

External Service Port: 5540 - 5540

Map to Port: 554 - 554

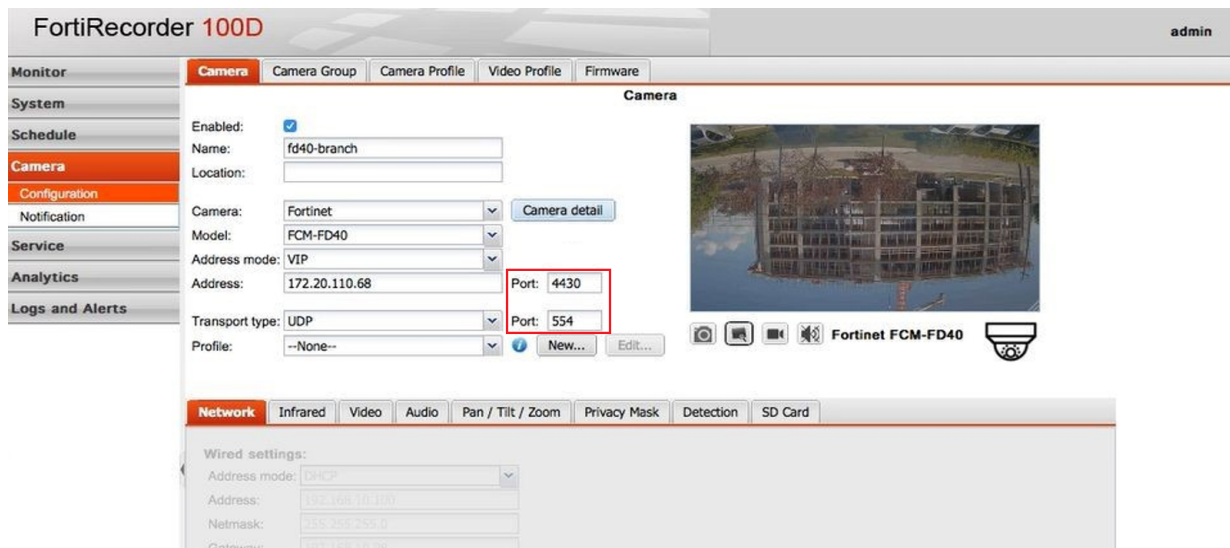
OK Cancel

3. Enter the addresses.
4. Enter a name for the virtual IP and select *wan1* from the Interface dropdown menu.
5. Select TCP as the desired protocol and enter *5540-5540* for the External Service Port range, and *554* for the Map to Port.

## Configuring the cameras

To add your cameras in FortiRecorder:

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



FortiRecorder 100D admin

**Monitor** | **Camera** | Camera Group | Camera Profile | Video Profile | Firmware

**System**  
**Schedule**  
**Camera**  
**Configuration**  
Notification  
**Service**  
**Analytics**  
**Logs and Alerts**

**Camera**

Enabled: ☒  
Name: fd40-branch  
Location:  
Camera: Fortinet  
Model: FCM-FD40  
Address mode: VIP  
Address: 172.20.110.68  
Port: 4430  
Transport type: UDP  
Profile: --None--  
New... Edit...

Camera detail

Fortinet FCM-FD40

**Network** | Infrared | Video | Audio | Pan / Tilt / Zoom | Privacy Mask | Detection | SD Card

Wired settings:  
Address mode: DHCP  
Address: 192.168.10.100  
Netmask: 255.255.255.0  
Gateway: 192.168.10.30

3. Enter the name of the camera.
4. Select *VIP* from the Address mode dropdown menu, and enter the address and port.
5. Select the *SD Card* tab and enable *SD Storage*.
6. Enter the rest of the options as desired, and click *Create*.

7. Go to *System > Configuration > Options* and enter a Public Access address.

**FortiRecorder 100D**

Monitor | Time | **Options** | Mail Server Settings | SMS | SNMP

System | Configuration | Customization | Network | Storage | Administrator | Authentication | Certificate | Maintenance | Schedule | Camera | Service | Analytics | Logs and Alerts

Idle timeout: 45 (Minutes)

**Login Disclaimer Setting**

Login disclaimer:

\*\*\*\*\* WARNING \*\*\*\*\*

This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. All use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of this system are subject to appropriate disciplinary action.

Reset to Default

Display pre-login banner: ☐ Admin  
Display post-login banner: ☐ Admin

**Public Access**

Host name: 172.16.76.174

**Access Ports**

Service	Local	Public
HTTP:	80	80
HTTPS:	443	443
SSH:	22	
TELNET:	23	
FRC-Central:	8550	8550
RTSP:	554	554
FTP:	21	21
Camera notification:	3010	3010
	3011	3011

The example screenshots of the setup work because the recorder is using a VIP, which puts the FortiRecorder basically directly on the internet. In a NAT translated situation on the recorder side, you may require a session helper to get RTSP/RTP live streaming operational. See [Real-Time Streaming Protocol \(RTSP\) session helper on page 17](#).

## Real-Time Streaming Protocol (RTSP) session helper

The Real-Time Streaming Protocol (RTSP) is an application layer protocol often used by SIP to control the delivery of multiple synchronized multimedia streams, for example, related audio and video streams. Although RTSP is capable of delivering the data streams itself it is usually used like a network remote control for multimedia servers. The protocol is intended for selecting delivery channels (like UDP, multicast UDP, and TCP) and for selecting a delivery mechanism based on the Real-Time Protocol (RTP). RTSP may also use the SIP Session Description Protocol (SDP) as a means of providing information to clients for aggregate control of a presentation consisting of streams from one or more servers, and non-aggregate control of a presentation consisting of multiple streams from a single server.

To accept RTSP sessions you must add a security policy with service set to any or to the RTSP pre-defined service (which listens on TCP ports 554, 770, and 8554 and on UDP port 554). The RTSP session helper listens on TCP ports 554, 770, and 8554.

The RTSP session help is required because RTSP uses dynamically assigned port numbers that are communicated in the packet body when end points establish a control connection. The session helper keeps track of the port numbers and opens pinholes as required. In Network Address Translation (NAT) mode, the session helper translates IP addresses and port numbers as necessary.

In a typical RTSP session the client starts the session (for example, when the user selects the Play button on a media player application) and establishes a TCP connection to the RTSP server on port 554. The client then sends an OPTIONS message to find out what audio and video features the server supports. The server responds to the OPTIONS message by specifying the name and version of the server, and a session identifier, for example, 24256-1.

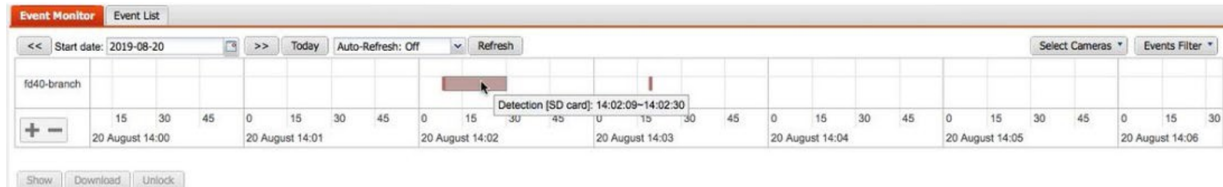
The client then sends the DESCRIBE message with the URL of the actual media file the client wants to play. The server responds to the DESCRIBE message with a description of the media in the form of SDP code. The client then sends the SETUP message, which specifies the transport mechanisms acceptable to the client for streamed media, for example RTP/RTCP or RDT, and the ports on which it receives the media.

In a NAT configuration the RTSP session helper keeps track of these ports and addresses translates them as necessary. The server responds to the SETUP message and selects one of the transport protocols. When both client and server agree on a mechanism for media transport the client sends the PLAY message, and the server begins streaming the media.

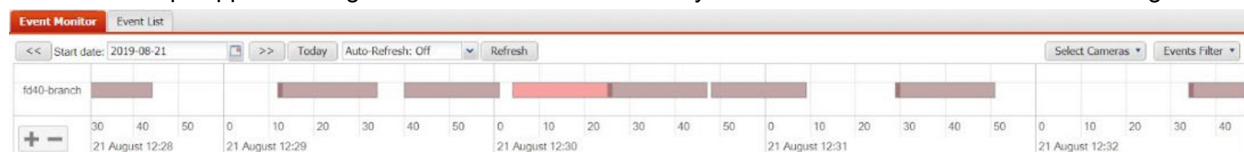
# Monitoring SD-Branch recordings on the HQ FortiRecorder

When everything has been properly configured, recordings from SD-Branch cameras can be viewed through the HQ FortiRecorder.

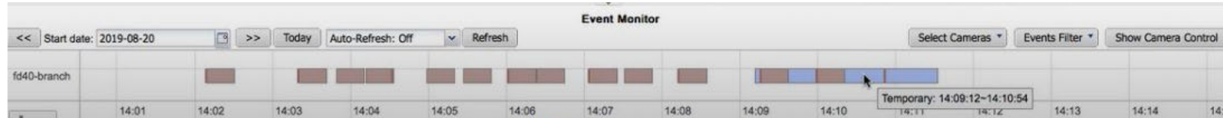
- Motion events are viewable by going to *Monitor > Event > Event*.



- You can select the desired clip and then click *Show*. After a few moments the clip has been downloaded and playback begins.
- Downloaded clips appear as bright-red bars to indicate that they are available on the local recorder storage.



- Most clips begin with an event marker. If the motion is extended and triggers multiple clips nearly consecutively, a marker is generated every minute.
- When viewing video through a live feed, temporary recordings display in your timeline as blue bars.



- View motion events in the detection log by going to *Monitor > Log Viewer > Detection*.

FortiRecorder 100D

admin

Help

Log Out

FORTINET

Monitor

System Status

DHCP Status

Camera Notifications

Log Viewer

Event Monitor

Video Monitor

System

Schedule

Camera

Service

Analytics

Logs and Alerts

Event

Camera

Detection

Assistant

Level: Information

Go to line:

Search...

Back

2019-04-09 06:58:16 - Current

Page 1

/ 115

Records per page: 50

Save View

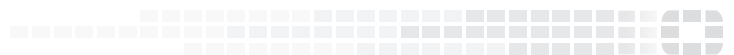
Total: 5/48

#	Date	Time	Action	Camera	Detection Type	Detection Subtype	Message
1	2019-08-21	13:01:47	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
2	2019-08-21	13:00:32	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
3	2019-08-21	12:59:55	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
4	2019-08-21	12:59:21	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
5	2019-08-21	12:58:14	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
6	2019-08-21	12:57:21	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
7	2019-08-21	12:55:58	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
8	2019-08-21	12:55:12	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
9	2019-08-21	12:53:47	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
10	2019-08-21	12:52:29	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
11	2019-08-21	12:51:57	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
12	2019-08-21	12:50:58	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
13	2019-08-21	12:49:56	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
14	2019-08-21	12:49:29	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
15	2019-08-21	12:48:13	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.
16	2019-08-21	12:47:35	start	fd40-branch	motion	motion	Motion detection on camera fd40-branch.





**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.