



FortiRecorder - FortiRecorder Cookbook

Version 6.4

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://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

July 26, 2021

FortiRecorder 6.4 FortiRecorder Cookbook

00-400-000000-20181031

TABLE OF CONTENTS

Camera Configuration	5
Configuring and Connecting Cameras for the First Time	5
Configure the video profile	5
Create a camera profile	6
Connect your cameras	7
Configure camera settings	9
Connecting Remote Cameras to FortiRecorder	10
Configuring FortiRecorder	10
Configuring Remote Camera Deployment	11
ONVIF Camera Installation Guidelines	12
ONVIF cameras	12
Mobile	14
How to use FortiRecorder Mobile on Android	14
Configuring FortiRecorder mobile	14
Adding FortiRecorder to FortiRecorder Mobile	15
Monitoring cameras in FortiRecorder Mobile	16
How to use FortiRecorder Mobile on iOS	16
Adding an FortiRecorder to ForetiRecorder Mobile	17
Monitoring cameras in FortiRecorder Mobile	17
Monitoring	18
Facial Recognition Configuration and Optimization	18
Ensuring the best results	18
Configuring facial recognition in FortiCentral	18
Facial analytics configuration	19
Configuring face recognition in FortiRecorder	20
Problems with QuickTime in Web Browsers	21
Internet Explorer and Firefox users	21
Using Recorded Clips and the Monitoring Interface	21
Interface overview	21
Temporary recording	23
Storage	25
Installing Hard Drives in FortiRecorder 400D	25
Configuring RAID levels	25
Adding a RAID disk	26
Replacing a RAID disk	26
Replacing all RAID disks	27
Re-Aligning FortiRecorder Disk Partitions	28
Checking alignment	28
Aligning partitions	28
System Administration	30
Using Single Sign On with PingIdentity	30
Configuring PingIdentity	30
Enabling FortiRecorder Admin Account Single Sign On	32
Login Testing	32

Adding MFA for SSO Two-Factor Authentication	33
Configuring MFA	34
Change Log	36

Camera Configuration

The following section contains information on connecting and configuring your cameras in FortiRecorder.

Configuring and Connecting Cameras for the First Time

After you have successfully installed your FortiRecorder, the next step will be to configure and then connect your cameras.

Configuring and connecting your cameras will involve the following steps:

1. Configure the video profile.
2. Create a camera profile.
3. Connect your cameras.
4. Configure camera settings.



If you require information on how to physically connect your cameras to the FortiRecorder, see the camera's QuickStart Guide.

Configure the video profile

A video profile defines the video quality captured by the camera.

Video profiles are used in camera profiles, which we will explain further in the next section.

To configure a video profile

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

Camera Video Profile

Name:	<input type="text" value="high-resolution"/>
Codec:	<input type="text" value="Default"/>
Resolution:	<input type="text" value="High"/>
Frames per second:	<input type="text" value="30"/>
Bitrate mode:	<input type="text" value="Variable"/>
Quality:	<input type="text" value="High"/>
Audio:	<input type="checkbox"/>

3. Enter a name that reflects the configuration itself, like "high-resolution".
4. Select your desired codec from the drop-down menu.
5. Select the amount of detail of the captured image. Lower resolutions feature less detail but are faster to transmit, while higher resolution produces a clearer image but require more bandwidth.
6. Select the number of frames per second (FPS). Most videos are 24 FPS. More FPS uses more CPU resources but may be useful if the objects you're attempting to capture on video move quickly.
7. Select the bit rate. A variable rate lowers the bit rate dynamically when little to no motion is detected. A fixed bit rate maintains a constant bit rate.
8. Select the degree of compression and enable or disable the audio.
9. Select *OK*.

Create a camera profile.

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

To configure camera profiles

1. Go to *Camera > Configuration > Camera Profile*.
2. Select *New*.
3. Enter a descriptive name.
4. Select both the recording and viewing stream profile used to determine the video quality. This could be the profile we created from the previous section.
5. Select the recording type that instructs the camera when to begin filming. In the example image, we've selected motion detection, which tells the camera to only record video when it detects motion, thus

saving on bandwidth and storage.

Camera Profile Settings

Name:

Video

Add schedule...

Recording stream profile: + New... Edit...

Viewing stream profile: + New... Edit...

Recording

Add schedule...

Recording type: Continuous Digital input Audio detection PIR detection Tamper detection

Motion detection: FortiRecorder SD card

Edge Download

Add schedule...

Continuous recordings: Automatic Automatic

Detection recordings: Automatic Automatic

Storage Options

Continuous recordings:

6. Enable whether video is recorded to the SD card continuously or only at moments of detection.
7. Select the storage options of both continuous and detection recordings.
8. Select whether or not FortiRecorder compresses continuous recordings. If you enable compression, make sure to configure the maximum amount of time to keep files uncompressed. Files whose start time is older than the specified time will be compressed. Selecting compression also saves storage space.

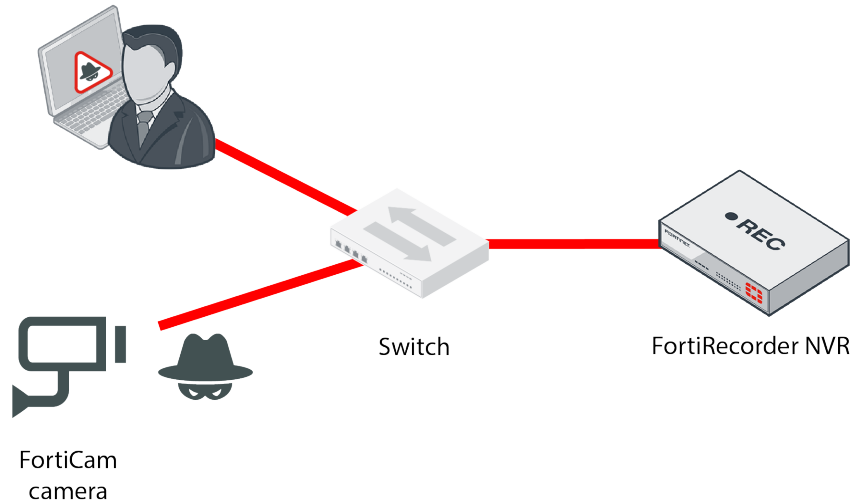
Connect your cameras

We can now prepare FortiRecorder to discover your connected cameras.



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

We will be using a direct connection method. This connection type is for when your camera is located directly on your local network.



1. Change your PC's IP address to be on the same subnet as the FortiRecorder port1's default IP address 192.168.1.99. For example, set your PC's IP to 192.168.1.98.
2. Connect your PC and FortiRecorder's port1 to a PoE switch as show in the diagram. Do not connect the camera to the switch at this stage.
3. On your PC, open a web browser and connect to <https://192.168.1.99>. Log in to the admin administrator account with Name: admin and Password: (none).
4. On the FortiRecorder web UI, go to *System > Network > DHCP*, and select *New* to create a new DHCP server on port 1.

Edit DHCP server

Network Interface Setting

ID:

Enable DHCP server:

Interface:

Gateway:

DNS options:

DNS server 1:

DNS server 2:

Domain:

Netmask:

Auto Config Setting

Lease time (Seconds):

Conflicted IP timeout (Seconds):

DHCP IP Range

Total: 0

Start	End

5. Enable DHCP server and select port1 from the Interface drop-down menu.

6. Go to *System > Network > Interface* and select port1 and then *Edit*.
7. Enable Discover cameras on this port.
8. Connect the camera to the PoE switch.
9. Go to *Camera > Configuration > Camera* and select *Discover*. Newly discovered cameras are highlighted in yellow.

We will configure the individual cameras in the next section.

Configure camera settings

Once the cameras are physically connected to the FortiRecorder, you can configure the discovered cameras.

To configure a camera

1. Go to *Camera > Configuration > Camera*.
2. Select a newly discovered camera and then select **Configure**.
3. Enable the FortiRecorder to communicate with the IP address. Communication is required to trigger scheduled recordings and other camera commands.
4. Enter a name and the physical location of the camera for organizational purposes.
5. Select the address mode from the drop-down menu.
6. Select the Transport type, which is the tunnel between the camera and the NVR. RTSP is used for video streaming, which is UDP. If you want to use TCP, use HTTP tunneling. If you want the communication to be secure/encrypted use HTTPS tunneling.
7. Select the camera profile we created earlier.
8. Select the Preview button to retrieve a single still image from the camera and then select Use As Icon to use the captured image as the display picture for the camera in your camera list.



9. Expand the various settings tabs and adjust accordingly. The availability of the settings tabs are dependent upon your camera model. If you require more details for specific settings, consult the Administrator guide.
10. Select **OK**.
If you kept the Enabled check box marked, at this time, FortiRecorder connects to the camera's discovered IP address. FortiRecorder configures the camera with:

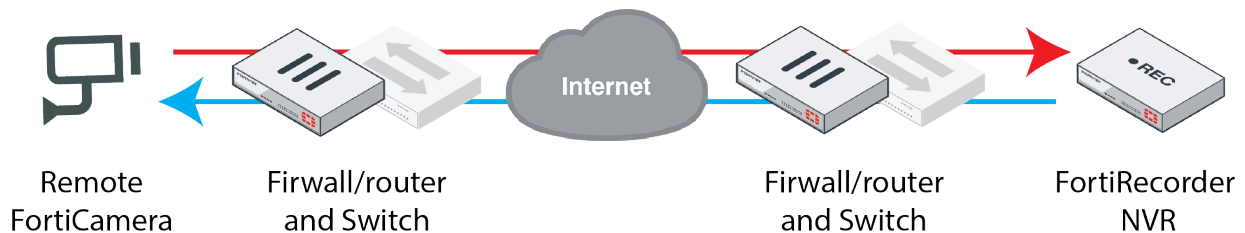
- the camera's new Address and other network settings (if Address mode is set to Static)
- NTP settings (if you configured them for FortiRecorder during "Setting the system time")

In order to control the camera according to your selected schedules, FortiRecorder will periodically connect to the camera's configured IP address. It will also keep video recordings sent by that camera from its new IP address.

Connecting Remote Cameras to FortiRecorder

The following scenario is intended for users who are accessing their cameras remotely. Remote camera deployment refers to scenarios in which there is a firewall, such as your FortiGate unit, between FortiRecorder and the cameras.

In this recipe, automatic IP configuration will not work, since the cameras will need to be assigned virtual IP addresses.



Configuring FortiRecorder

First, you'll need to configure your FortiRecorder.

To configure FortiRecorder to allow for remote access deployment

1. Go to *System > Network > Interface* and edit port 1.

Edit Interface

Interface name: port1 (00:10:f3:41:11:85)

Discover cameras on this port

Addressing Mode

Manual DHCP

IP/Netmask: /

IPv6/Netmask: /

Advanced Setting

Access:

HTTPS PING SSH SNMP

HTTP TELNET FRC-Central RTSP

MTU: (bytes)

Administrative status: Up Down

2. Set a manual IP for the interface that is on the same subnet as the FortiGate interface.
3. Set Access to allow HTTPS, FRC-Central, and any other required protocols.
4. Select *OK*.
5. Go to *System > Network > Routing* and select *New* to add a default route that uses the IP address of the FortiGate's interface. Set the interface to port1.

Configuring Remote Camera Deployment

To configure remote camera deployment

1. In the FortiRecorder UI, go to *Camera > Configuration > Camera*.
2. Select *New*.

3. Enter the Name and Location of the camera and select *ONVIF* from the Camera drop-down menu.
4. Enter the username and password of the remote camera you are accessing.
5. Since the camera is on a remote network, select *VIP* from the Address Mode drop-down menu.
6. Enter the required virtual IP address in the Address section. Entering a static IP address will allow FortiGate to forward connections to the camera’s private network address. Enter port 443.
7. Select *UDP* from the Transport type drop-down menu and enter port 554.
8. Select *Create*.

ONVIF Camera Installation Guidelines

FortiRecorder supports third party ONVIF cameras; however, each manufacturer’s ONVIF camera is different. The following recipe provides you with some general guidelines for adding ONVIF cameras to FortiRecorder.

ONVIF cameras

1. Make sure the camera is ONVIF compliant.
 - a. Search for the ONVIF logo on the camera datasheet.
 - b. Go to the ONVIF website and search for the brand and model of the camera: ONVIF.
 - c. Ensure the firmware on the camera matches the firmware tested on the Declaration of Conformity.
2. ONVIF camera time and time zone settings need to match with FortiRecorder. Synchronize the time with the NTP server.
3. Turn on the ONVIF function on the camera. It is disabled by default. Please refer to the camera manufacturer’s user manual for more information.
4. Create an ONVIF user on the camera. Please refer to the camera’s manufacture’s user manual for more information.

Once the above conditions are checked, you should be able to manually add the ONVIF camera to FortiRecorder.

Mobile

The following contains information on accessing the FortiRecorder or cameras through your mobile device.

How to use FortiRecorder Mobile on Android

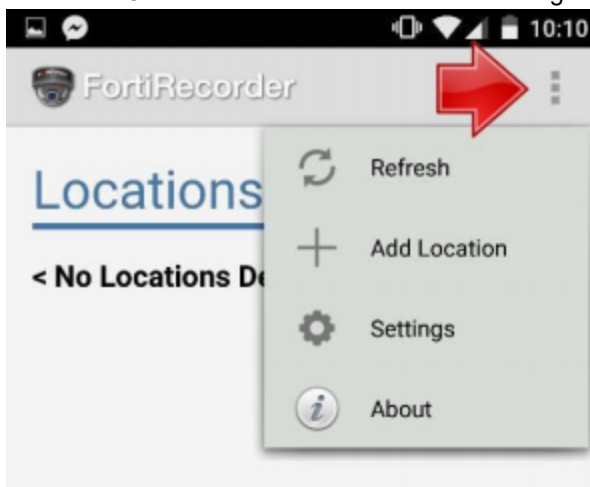
FortiRecorder Mobile for Android is a convenient and easy to use application that can help you monitor your cameras when you are away from your desktop. This recipe focuses on how to configure and use FortiRecorder Mobile on your Android device.

This recipe is intended for end-users.

Configuring FortiRecorder mobile

Before you add FortiRecorder to FortiRecorder Mobile, configure the application to your desired preferences.

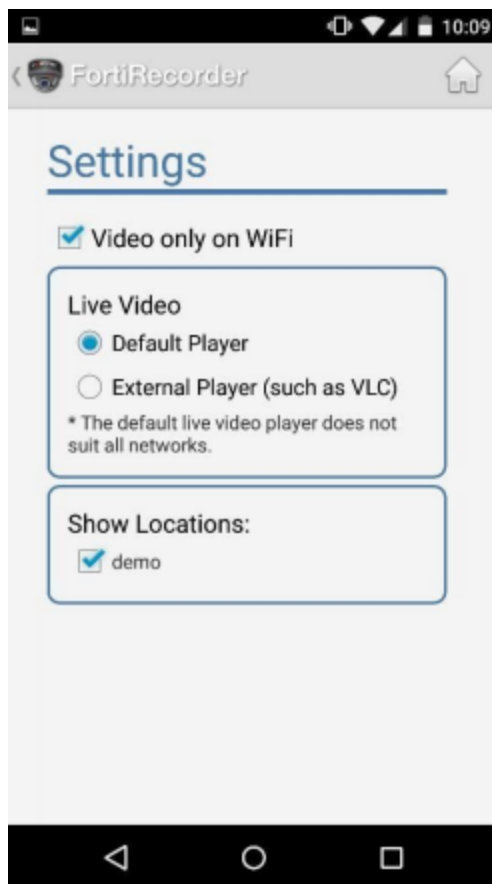
1. Select the Overflow button and then select Settings from the drop-down menu.



2. Save bandwidth by ensuring the Video only on WIFI option is selected.



If this option is selected, you will not be able to monitor the FortiRecorder's cameras unless you are on your network.



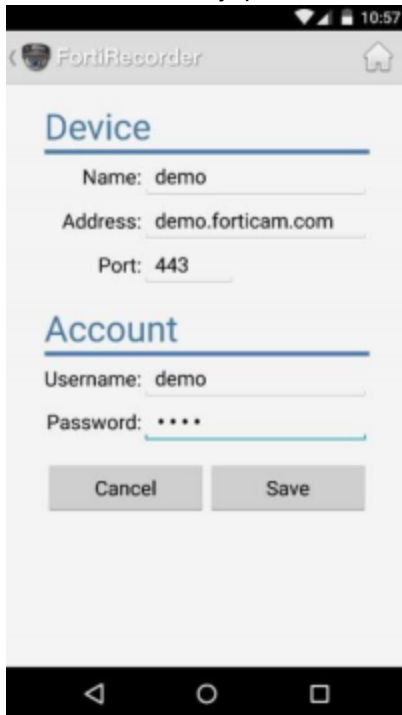
3. Use the default video player for live view or select your favorite external player.

Adding FortiRecorder to FortiRecorder Mobile

When you first load FortiRecorder Mobile, you'll notice that the Locations menu is blank. Add your FortiRecorder to the application.

1. Select the Overflow button and then from the drop-down menu, select *Add Location*.
2. Enter any name you wish to identify the device.

3. Enter either the fully qualified domain name or the public IP address of your FortiRecorder.



The screenshot shows the FortiRecorder Mobile app interface. At the top, the status bar shows the time as 10:57. The app title is 'FortiRecorder'. Below the title, there are two sections: 'Device' and 'Account'. The 'Device' section has three input fields: 'Name' with the value 'demo', 'Address' with the value 'demo.forticam.com', and 'Port' with the value '443'. The 'Account' section has two input fields: 'Username' with the value 'demo' and 'Password' with four asterisks. At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

4. Enter the account name and password used to access the FortiRecorder and select *Save*.

Monitoring cameras in FortiRecorder Mobile

Now that FortiRecorder Mobile is installed and properly configured, it is time to use the software to monitor your cameras.

1. Select your FortiRecorder from the locations menu on the home screen.
2. Select the Cameras option. The Camera section displays all available viewable cameras from your FortiRecorder.
3. Select the camera you wish to monitor.
On your screen now is a live-feed from your selected camera.

How to use FortiRecorder Mobile on iOS

FortiRecorder Mobile for iOS is a convenient and easy to use application that can help you monitor your cameras when you are away from your desktop. This recipe focuses on how to configure and use FortiRecorder Mobile on your iOS device.

This recipe is intended for end-users.

Adding an FortiRecorder to ForetiRecorder Mobile

When you first load FortiRecorder Mobile, you'll notice that the Locations menu is blank. Add your FortiRecorder to the application:

1. Select the Add button.
2. Enter any name you wish to identify the device.
3. Enter either the fully qualified domain name or the public IP address of your FortiRecorder.
4. Enter the account name and password used to access the FortiRecorder and select Save.

Monitoring cameras in FortiRecorder Mobile

Now that FortiRecorder Mobile is installed and properly configured, it is time to use the software to monitor your cameras.

1. Select your FortiRecorder from the locations menu on the home screen.
2. Select the Cameras option. The Camera section displays all available viewable cameras from your FortiRecorder.
3. Select the camera you wish to monitor.

On your screen now is a live-feed from your selected camera

Monitoring

The following section contains information on how to optimize your security viewing experience.

Facial Recognition Configuration and Optimization

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

FortiRecorder and FortiCentral supports easy to use face detection for your ever-evolving security needs. This recipe guides you through the process of getting the best facial recognition results and configuring facial recognition in FortiCentral and FortiRecorder.

Ensuring the best results

There are a few steps you should take to ensure the best possible results for a face match

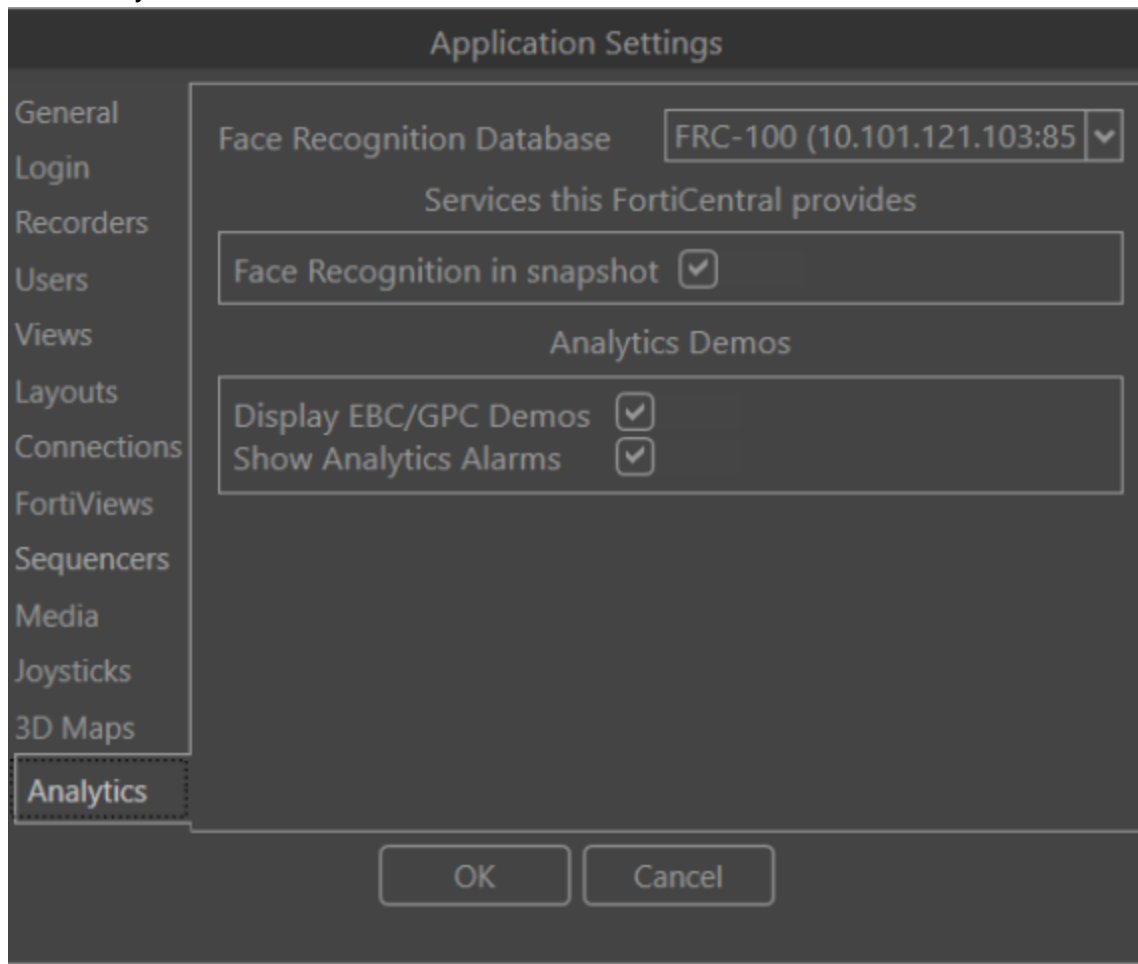
1. Make sure the individual is at eye-level with the camera and is facing forward and looking into the camera.
2. Keep the area well lit to avoid harsh shadows.
3. Do not pose the subject of the picture against a bright background, since this will darken their faces and make facial recognition difficult.
4. Keep the subject relatively still to reduce motion blur.

Configuring facial recognition in FortiCentral

To configure facial recognition in FortiCentral

1. Select the settings cog.
2. Select *Settings*.

3. Select *Analytics*.



4. Select the recorder receiving the results of the face analytics from the Face Recognition Database drop-down menu.
5. Enable “Face Recognition in a snapshot” to allow FortiRecorder to receive pictures of individuals for later identification.
6. Enable “Display EBC/GPC Demos” to electronically welcome guests based on recognition.
7. Enable “Show Analytics Alarms” to start a playback loop of the moment a person triggered an alarm.
8. Select *OK*.

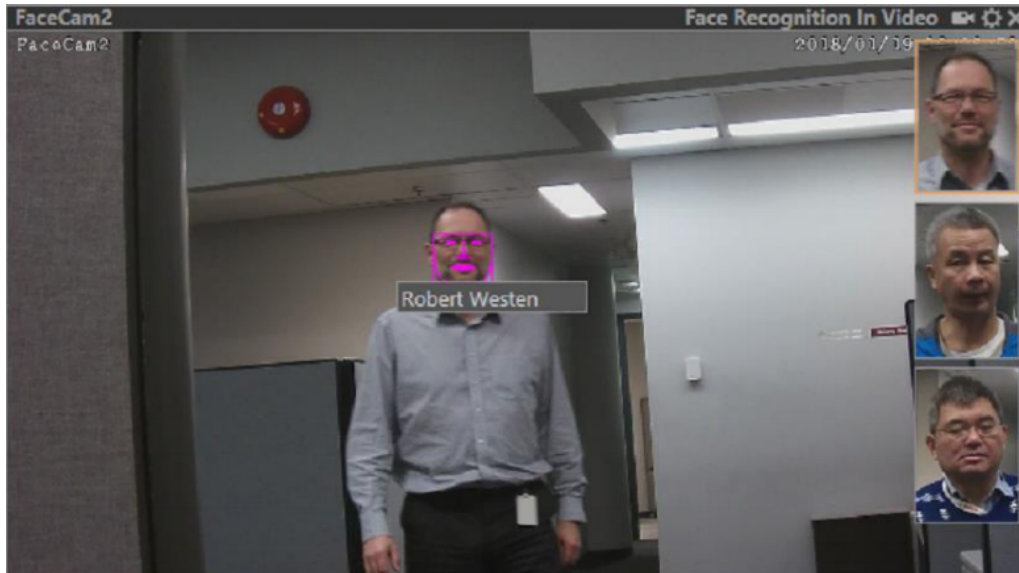
Facial analytics configuration

Face Analytics is the first implementation of a video analytics engine for FortiCentral.

To setup facial analytics

1. Select a camera stream on a pane.
2. Select the pane’s settings gear menu.
3. Select Face Recognition from the Algorithm drop-down menu to activate analytics on
4. the camera’s stream.

5. Enable Visualize to enable the overlay of facial landmarks on a live video. This could help determine if the processing is functional. The displayed overlay has four different colors:
White: Face detected but the quality is too low to generate a representation.
Yellow: First frame taken as a snapshot and to generate facial representation.
Magenta: The individual being tracked after initial detection.
Cyan/Green: The individual track continued from face matching.



6. Enable Show Snapshots to enable the display of the best snapshots associated with each track in a gallery.
7. Enable Look For Names to activate a search for detected faces in the face database. If an enrolled person resembles someone in the database, their name is added to the bottom of the facial landmark and then select **OK**.

Configuring face recognition in FortiRecorder

Now we can enable face recognition in FortiRecorder.

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

Problems with QuickTime in Web Browsers

You may be experiencing difficulties streaming video in FortiRecorder using Internet Explorer, Firefox, Chrome and Microsoft Edge. This recipe guides you through the simple process of enabling QuickTime in Internet Explorer and Firefox.



Microsoft Edge is currently not supported, so you will have to use Internet Explorer or Firefox to access your FortiRecorder unit. Latest versions of Chrome stop supporting QuickTime plugin as well.

Internet Explorer and Firefox users

QuickTime 7.7.9 does not install the QuickTime Web Plug-in by default. So, if you recently installed a fresh version of QuickTime, you may not be able to stream video in FortiRecorder.



All previous versions of QuickTime install the web plug-in by default.

To stream video in FortiRecorder using Internet Explorer or Firefox

1. Run the QuickTime installation file.
2. Select *Modify*.
3. Select *Optional QuickTime Features*.
4. Select *QuickTime Web Plug-in*.
5. Select *Change*.

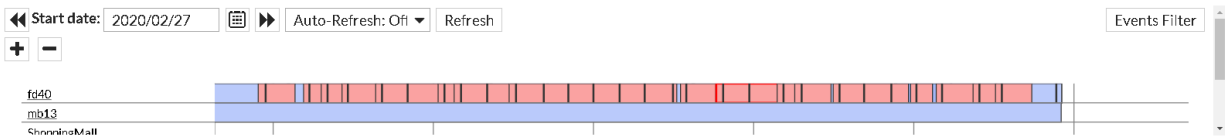
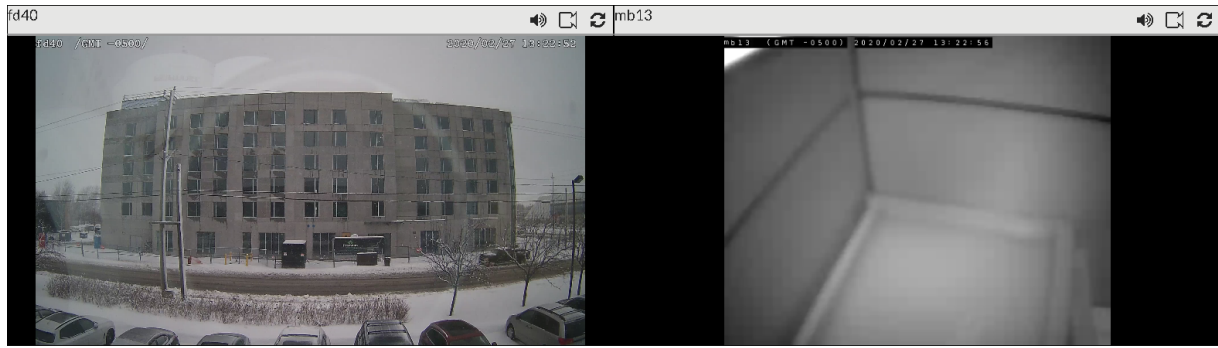
Using Recorded Clips and the Monitoring Interface

The following recipe illustrates how to use a recorded view and provides a brief overview of the interface.

Interface overview

First let's take a look at the interface to get a better understanding of how to monitor videos.

Go to *Monitor > Video > Video*.

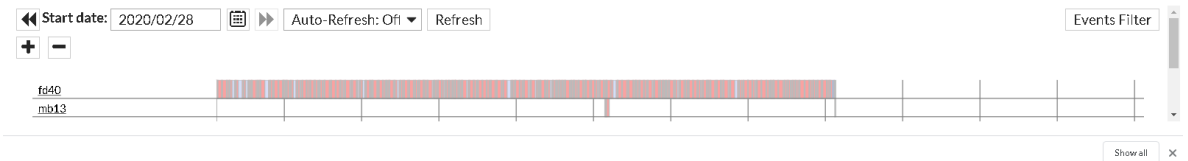
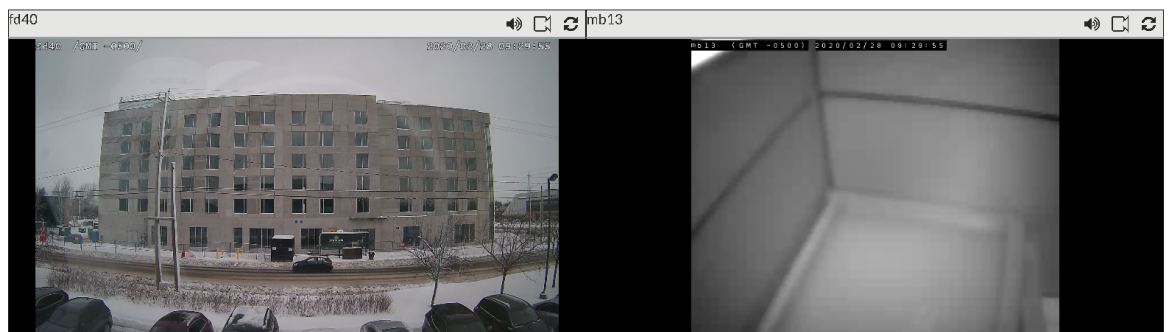


Sections within the time panel are color-coded for more effective surveillance:

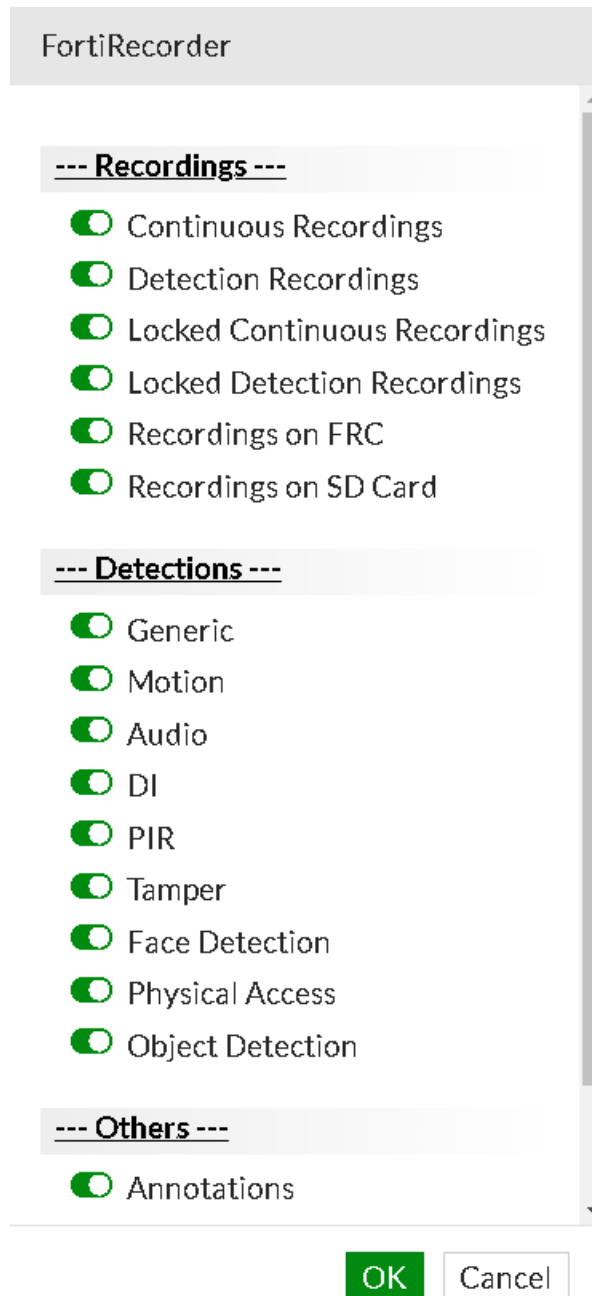
- **Yellow:** A yellow bar on the time panel indicates a system event, such as an update or a camera reboot.
- **Blue:** A light blue bar indicates a previously recorded clip. Darker blue are manually initiated recordings. A bright blue bar indicates an attached annotation or marker.
- **Red:** A red bar indicates a motion detection based recording that was not initiated by schedule.

To search for a specific event at a specific time and download the recording

1. Select the **Select Cameras** button to select the specific camera you wish to view.



2. Enter the start date for the event in the Start date field.
3. Select the **Events Filter** button to filter the time panel to only display the desired detections and recordings.



4. Zoom into the time the event occurred by selecting the time panel and then using your mouse wheel.
5. Double click the recorded section to play a clip of the event or select the section and then select **Show**.
6. Select the **Download** button.

Temporary recording

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

recording while watching the live feed from the camera, the temporary recording will be saved on the hard drive.

Storage

The following section contains information on storage for FortiRecorder.

Installing Hard Drives in FortiRecorder 400D

The FortiRecorder FRC-400D supports up to 4 hard disk drives to maximize your storage capacity for saved videos.

This recipe guides you through the process of configuring RAID levels, adding RAID disks, replacing a RAID disk, and reinstalling all of your RAID disks.

Your FortiRecorder unit stores video data on its internal hard drive until the drive is full. Storing files locally reduces the system's resource usage when recording. Through RAID storage, you'll be able to store more data without sacrificing system performance.

Supported HDD Models and Capacities:

Fortinet recommends surveillance grade rated hard drive models such as Western Digital WD40PURX and the Seagate ST4000VX000 (2-4 TB capacity).



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

Configuring RAID levels

The FortiRecorder 400D supports four hard drives and software RAID. The following table illustrates FortiRecorder 400D supported RAID levels.

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

To configure RAID levels



Back up your data on a disk before beginning the following procedure. Changing the device's RAID levels temporarily suspends all data processing and erases all data on the hard disk.

1. Connect to the CLI console.
2. Enter the following command:

```
execute raidlevel <level>
```

The FortiRecorder will change the RAID levels and reboot.

Adding a RAID disk

You can add two additional drives to your FortiRecorder 400D unit to expand your storage capacity.

To add an additional disk to the RAID array

1. Remove the hard disk bay from the unit by unlocking the bay with the supplied key.
2. Install the hard disk into the bay and insert the bay into the unit.
3. Go to *System > Storage > Local Storage*.
4. Select *Refresh*. The newly added disk will appear under Drives.

The screenshot shows the FortiRecorder 400D web interface. The left sidebar contains a navigation menu with 'Storage' selected. The main content area is divided into 'Local Storage' and 'External Storage' tabs. Under 'Local Storage', there are two tables: 'RAID Arrays' and 'Drives'. The 'RAID Arrays' table has columns for Array, Level, Status, and Size (GB). The 'Drives' table has columns for Bay, Part Of Array, Status, and Size (GB). A red arrow points to a 'Refresh' button located below the 'Drives' table.

Array	Level	Status	Size (GB)
1	RAID 0	OK	5860

Bay	Part Of Array	Status	Size (GB)
1	1	OK	3000
2	1	OK	3000
4		AVAILABLE	3000

5. Add the disk to an array.
6. Select *Refresh*. The new array will appear under RAID Arrays.
7. Select the new array and adjust the portions you want to allocate to log and video storage.
8. Select *Add to Logical Disks*.

Replacing a RAID disk

Whether due to damage or a component upgrade, you may want to replace a disk in your FortiRecorder 400D unit. The following steps guide you through the simple process of replacing a RAID disk.



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



FortiRecorder units support hot swap. You do not need to shut down the unit during hard disk replacement.

To replace a RAID disk

1. Go to *System > Storage > Local Storage*.
 2. Select the hard disk from the row you want to replace (for example, p4) and select Delete. The RAID controller will be removed from the list.
-



Use an anti-static wrist strap to avoid static electricity damaging the hard disk.

3. Remove the hard disk that you removed from the web UI from its drive bay.
4. Insert the new hard disk into the drive bay.
5. Select *Refresh*.

The RAID controller will scan for and locate the newly installed disk. The FortiRecorder unit may automatically add the new hard disk to the RAID unit or allocate it as a spare depending on the RAID level.

Replacing all RAID disks

You may need to replace all RAID disks in your machine, including the pre-installed drives, and build a new array.



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

To replace all disks in the array

1. Shut down the FortiRecorder unit.
2. Remove the hard disks.
3. Install the new hard disks.
4. Boot up the system.
5. From the Command Line Interface, enter the following command to rebuild the disks:

```
execute factoryreset disk
```

This command uses 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 the above section.

```
execute raidlevel <level>
```

6. The system will reboot.

Re-Aligning FortiRecorder Disk Partitions

The following recipe is for those having performance problems with the FRC-200Dgen2, the FRC-400D, and VMs installed before FortiRecorder v2.6 release. It covers how to check for alignment and aligning partition in FortiRecorder if the partitions are not aligned correctly.

Checking alignment

First you need to verify disk partition alignment. Access the CLI and enter “diag system disk-details”.

If your partitions are not aligned correctly, your screen will resemble the following:

```
System Time: 2018-04-13 09:58:13 EDT (Uptime: 1d 23h 55m)
for type for-var-physical
+device-name=sda
  | is-enc=0
  | is-dma=1
  | is-usb=0
    | size=2000398934016
(opt=0,min=4096,alg=0,phy=4096,log=512,grn=1048576)
+-----part-name=sda1
  | size=2000299999744
  | start=512 (not-aligned)
  | is-mounted=0
  | fs-type=software_raid
+device-name=sdb
  | is-enc=0
  | is-dma=1
  | is-usb=0
    | size=2000398934016
(opt=0,min=4096,alg=0,phy=4096,log=512,grn=1048576)
+-----part-name=sdb1
  | size=2000299999744
  | start=512 (not-aligned)
  | is-mounted=0
  | fs-type=software_raid
```

Aligning partitions

Now that we’ve identified the problem, we can now align the partitions properly.

1. Backup your FortiRecorder configuration by going to *System > Maintenance > Configuration* and selecting System configuration backup.
2. If remote storage is available, modify each camera profile in use by going to Storage Options and selecting Move after 1 hour for both continuous and detection records.

3. Let the system run until the local storage usage is down to a minimum. This could take a few days since the system will continue recording.
4. Repartition the disk by using the CLI command: `exec factoryreset disk`.
5. Restore the configuration.

System Administration

The following section contains information on system administration procedures.

Using Single Sign On with PingIdentity

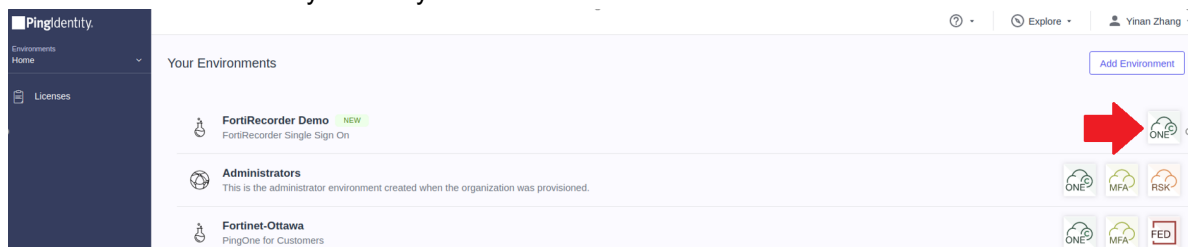
The following recipe walks you through the process of setting up Single Sign On using Ping Identity and SAML for FortiRecorder.

Configuring PingIdentity

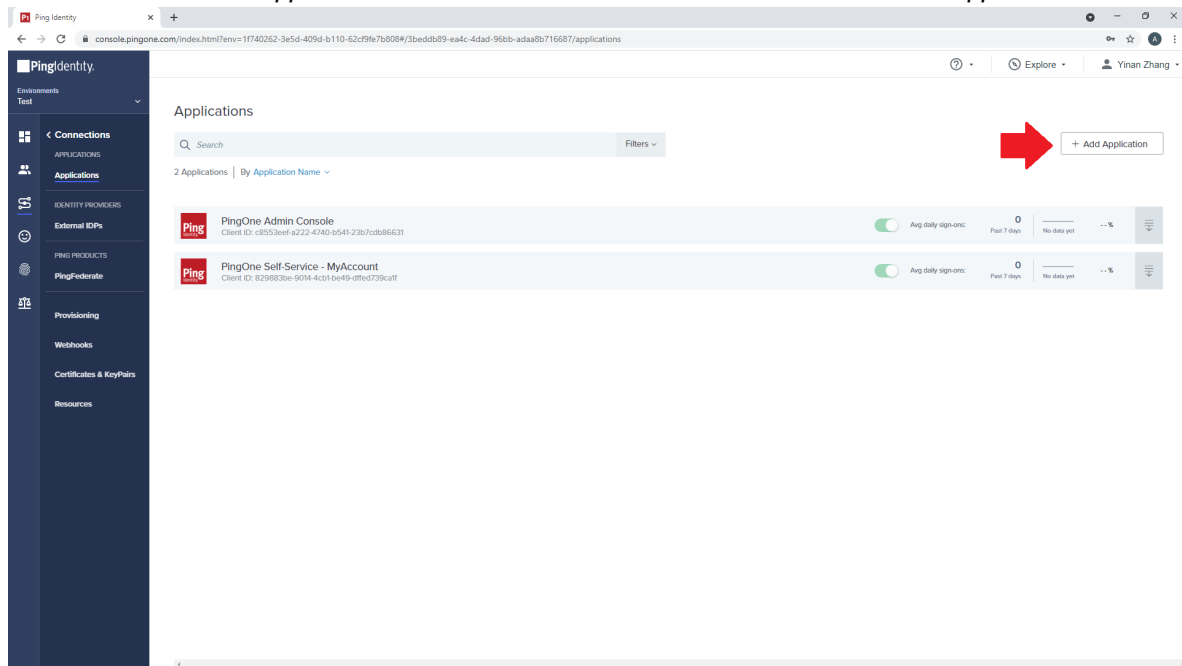
First we'll need to configure PingIdentity. Be sure you are logged in to your PingId account and that you have administrative privileges on your machine.

To configure PingID:

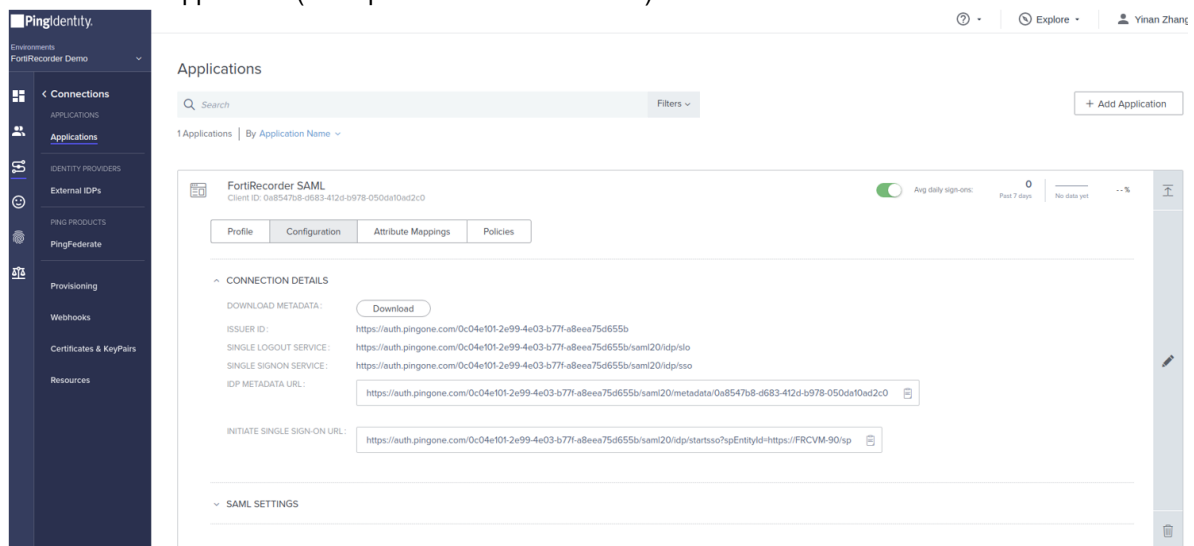
1. Select the *Add Environment* button from the home page.
2. Select *Customer solution* as your created solution, *PingOne for Customers* from the Cloud Solutions section and *PingOne MFA* from the Cloud services section and then select *Next*.
3. If available, enable "Deploy a sandbox environment" in the PingOne for Customers section and select "Generate sample populations and users in this environment" and then select *Next*.
4. Fill in the necessary information. Be sure to select "PingOne for Customers" from the License dropdown menu. Once completed, select *Finish*.
5. Select the ONE icon from your newly created Environment.



6. Select *Connections > Application* from the menu on the left and then select the *Add Application* button.



7. Select *Advanced Configuration* and then select *Configure* next to SAML.
8. Enter the name and description and select *Next*.
9. Enter the necessary information. Your ACS URLs and ENTITY ID information can be found by accessing the FortiRecorder UI and going to *System > Customization > Single Sign On*.
10. Select *Save and Continue*.
11. Select *PingOne Attribute* to add an SAML Attribute. The user attribute is your email address and the application attribute is "urn:oid:0.9.2342.19200300.100.1.3". Select *Save and Close*.
12. Select *Configuration* and in the Connection Details section, next to Download Metadata, select *Download*.
13. Enable SAML Application (Example: FortiRecorder SAML) as below:



14. Go to *Identities > Users* and select the *Add User* button.

15. Enter the necessary information and select *Save*. The user needs to be added to the FortiRecorder admin users.
16. Select *Reset Password* to configure a one time password and save it. The password will change when you perform the first login.

Enabling FortiRecorder Admin Account Single Sign On

Now we will need to access the FortiRecorder web interface to enable Single Sign On.

To enable FortiRecorder Admin Account Single Sign On

1. Go to *System > Customization > Single Sign On* and enable Single Sign On.
2. Select the *Upload* button in the Identify Provider (IDP) Metadata section.
3. Select the IDP Metadata we saved in the previous section. IDP Metadata will automatically generate.
4. Enable `admin_sso` for Single Sign On login. The user added in the IDP server can be used for the FortiRecorder admin GUI login. Check if CSF is enabled if `admin_sso` is enabled. Go to the console and type:

```
#config system csf
set status
```

Once SSO is enabled, all user login authentication is controlled by the PingIdentity and not by the FortiRecorder. Disabled accounts should not be authenticated by PingIdentity.

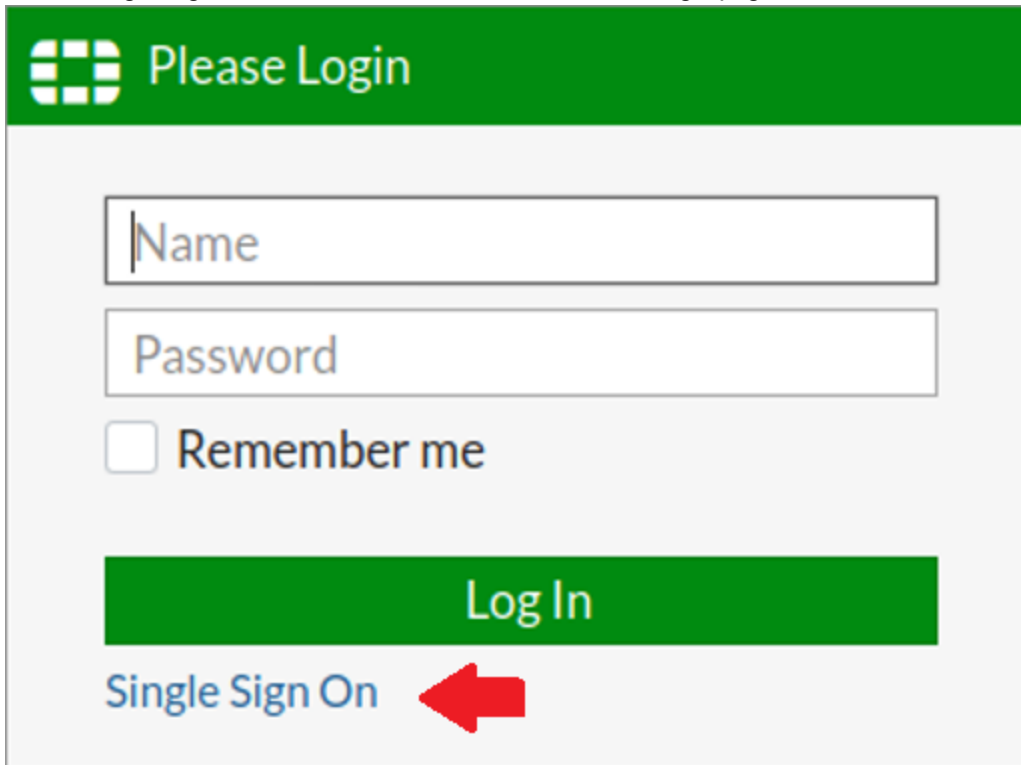
Logging out of FortiRecorder Admin GUI will also log out users from IDP in the case of SSO.

Login Testing

Now we will take the time to login to the FortiRecorder via the SSO Account (e.g. Account username is John) which is configured on PingIdentity.

To test your login:

1. Select Single Sign On from the FortiRecorder Admin GUI login page.

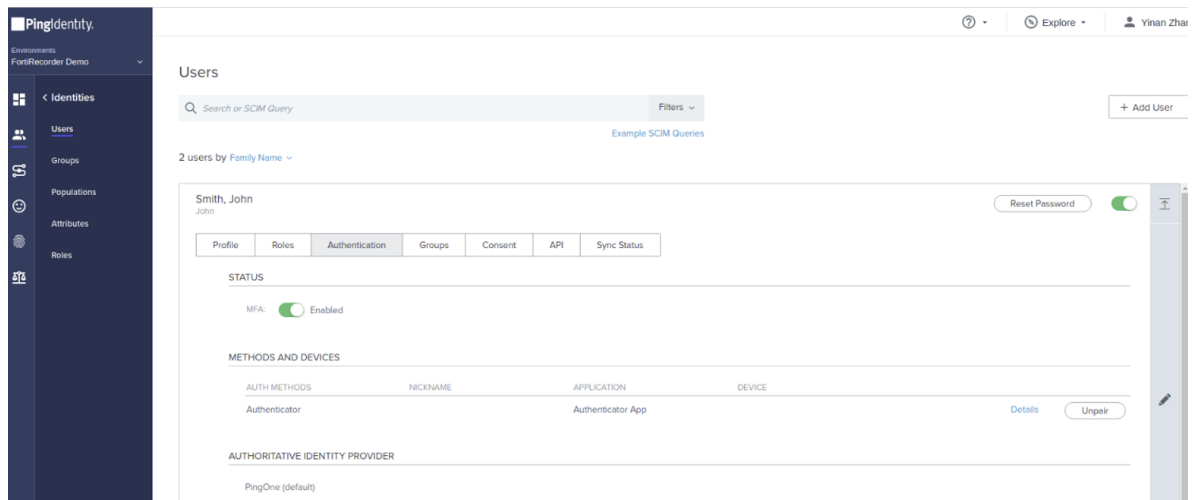


2. Redirect to the PingIdentity login page and change the password.
3. Login to the FortiRecorder Admin GUI via the SSO account.

Adding MFA for SSO Two-Factor Authentication

To add MFA for SSO

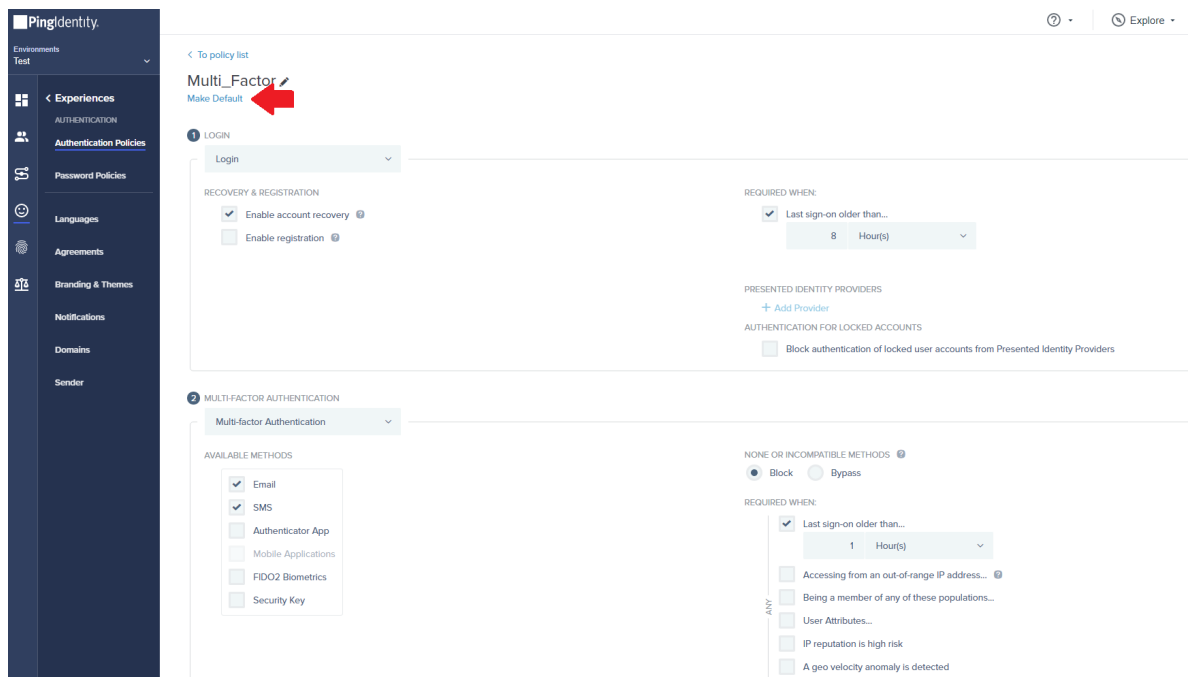
1. In PingIdentity go to *Dashboard > Environment Properties*.
2. Go to the URL in the Self-Service URL section and log in as a new user.
3. Go to *Authentication > Add a Method* and select *Add Method* to add Authenticator App.
4. Select Authentication App.
5. Scan the QR code via FortiToken Mobile or Google Authenticator.
6. Log in to PingIdentity Portal and go to *Identities > Users*. Under the Authentication tab, make sure the user account has MFA enabled and Authenticator App is added successfully.



Configuring MFA

To configure MFA

1. Go to Experiences > Authentication Policies.
2. Select the dropdown menu to the right of the Multi-Factor section and then select the edit symbol.
3. Select *Make Default*.



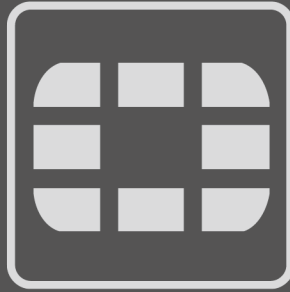
4. Adjust the Required When setting to the required time.
5. Enable Authenticator App under the Available Methods section.

Now when you log on to FortiRecorder an additional step is added. Select Single Sign On in the login section, authenticate with Passcode and type the passcode displayed on the FortiToken Mobile.

For two factor with token, you'll need to enroll a user authentication device (add authentication method in user's account via Self Service Portal) and setup PingIdentity MFA to support token exchange. The authorization of the token is processed on the IDP side. No configuration is required on the FRC. It should work properly when redirecting to the login page on PingIdentity.

Change Log

Date	Change Description
2019-05-25	Initial release.



Copyright© 2021 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.