

---

# **FindFaceSecurity**

***Release 1.1.1***

**NtechLab**

**Jun 16, 2023**



---

## Contents

---

<b>1</b>	<b>About FindFace Security</b>	<b>1</b>
1.1	Administrator's Guide . . . . .	1
1.2	Operator's Guide . . . . .	33



---

## About FindFace Security

---

FindFace Security is a video-based biometric identification system that automates Security and Hospitality Operations Management. It can be harnessed in such areas as retail, banking, social networking, entertainment, sports, event management, dating services, video surveillance, public safety, homeland security, etc.

FindFace Security detects and identifies faces of the unwanted persons and VIP guests in video, and notifies security and hospitality managers about their arrival.

Early recognition of the arrival of unwanted persons and VIP guests allows for solving the following problems:

- Operational losses due to fraudulent activity
- Reputational losses and conflicts
- Better catering to the needs of VIP guests
- Prevention of life threatening situations

This guide is intended for the FindFace Security administrators, security and hospitality managers, and maintenance engineers.

---

**Note:** You can find this guide at <http://docs.findface.pro> (choose the version you need) and at `http://<ffsecurity_ip>/doc/en/index.html` after installation.

---

## 1.1 Administrator's Guide

### 1.1.1 System Requirements

FindFace Security can be deployed on a single host (standalone) or in a cluster environment. To calculate the host(s) characteristics, use the following requirements:

---

**Important:** If the resolution of a camera(s) in use is more than 1920x1080p, it is strongly recommended to use the GPU-accelerated `video-worker` package. Contact your Ntech Lab manager or Ntech Lab support experts by

---

[info@ntechlab.com](mailto:info@ntechlab.com) to request the package.

---

Re-requirement	Description
CPU	Intel Xeon E5 with AVX support or similar CPU. The characteristics depend on the number of cameras in use. A single camera 1080p@25FPS requires 2 cores HT >2 GHz for video processing and 2 cores HT >2 GHz for face recognition.
RAM	Depends on the number of cameras in use. A single camera 1080p@25FPS requires 4 GB for video processing and 6 GB for face recognition.
HDD	The own needs of the operating system and FindFace Security require 10 GB. The total volume is subject to the required depth of the event archive in the database and in the log, at the rate of 1.5 Mb per 1 event.
Operating system	Ubuntu 16.04 LTS (x64)

---

**Note:** The minimum configuration to process a video stream 1x720p (1280x720) 25 FPS is 6th generation INTEL Core i5 CPU with 4 physical cores 2,8 GHz, and 6 GB RAM.

---

### 1.1.2 Architecture

FindFace Security is deployed on a single host (standalone) or in a cluster environment.

---

**Tip:** See *System Requirements*.

---

FindFace Security is delivered in the following distributable packages:

- A package with the FindFace Security components **<findface-security-repo>.deb**.
- Packages with the biometric neural network models **<findface-data>.deb**.

The packages are delivered as is, or as part of the installer.

The FindFace Security functioning is provided by interaction of the following components:

Component	Description
PostgreSQL	A database which stores detailed and categorized dossiers on particular persons, their biometric data, and face identification events. It also stores data for internal use such as user accounts and camera settings. To be installed from the Ubuntu repository (along with Redis).
ffsecurity	A service which interfaces with all the components to provide the system functioning. Includes <code>findface-security-proto</code> (provides HTTP and web socket) and <code>findface-security-worker</code> (provides interaction between the other system components). First, <code>findface-security</code> gets a normalized image, full frame, and meta data of a detected face from <code>video-worker</code> . It then redirects the normalized image to the <code>extraction-api</code> service to extract biometric data. The <code>findface-postgres-facen</code> extension uses the face biometric data to find a set of most similar faces in the dossiers. The face identification event along with the search result is then saved into the PostgreSQL database. You can configure your system to save and display an event only if the similarity between a detected face and some face in the dossiers exceeds a pre-defined threshold, i. e. the faces match (the <code>IGNORE_UNMATCHED</code> option at <code>/etc/ffsecurity/config.py</code> , see <a href="#">Basic Configuration</a> ). The <code>ffsecurity</code> service also provides a search engine that searches the event and dossier database for a given face.
videomanager-api	A service, part of the video face detection module, that is used for managing the video face detection functionality. Use it to configure the video face detector settings and to specify the list of video streams to process.
video-worker	A service, part of the video face detection module, which recognizes a face in video and posts its normalized image, full frame and meta data (such as the camera ID and detection time) to the <code>ffsecurity</code> service.
extraction-api	A service which extracts face biometric data (feature vector). Requires the packages with the neural network models <b>&lt;findface-data&gt;.deb</b> .
findface-postgres-facen	A PostgreSQL extension which calculates similarity between a newly detected face and faces in the dossiers, by comparing their biometric data.
ffsecurity-ui	Use the web interface to work with face identification events, search for faces, manage cameras, users, dossiers, and watch lists.
NTLS	A license server which interfaces with the NtechLab Global License Server or a USB dongle to verify a license.
etcd	Third-party software that implements a distributed key-value store for the <code>videomanager-api</code> component. Used as a coordination service in the distributed system, providing the video face detector with fault tolerance.

---

**Note:** Use the web interface to work with FindFace Security.

---



---

**Note:** To purge old events from the database, use the `event-cleaner` [utility](#).

---

### 1.1.3 Deploy FindFace Security

Use one of the following deployment methods:

- Deploy from a console installer
- Deploy step-by-step

- Deploy `video-worker` on a remote host from the additional installer.

### Deploy from Console Installer

To deploy FindFace Security, you can use a developer-friendly console installer.

**Warning:** The installer cannot be used to update FindFace Security.

**Warning:** The FindFace Security host must have a static IP address in order to be running successfully. To make the IP address static, open the `etc/network/interfaces` file and modify the current primary network interface entry as shown in the case study below. Be sure to substitute the suggested addresses with the actual ones, subject to your network specification.

```
sudo vi /etc/network/interfaces

iface eth0 inet static
address 192.168.112.144
netmask 255.255.255.0
gateway 192.168.112.254
dns-nameservers 192.168.112.254
```

Restart networking.

```
sudo service networking restart
```

Be sure to edit the `etc/network/interfaces` file with extreme care. Please refer to the [Ubuntu guide on networking](#) before proceeding.

### See also:

- [Deploy Step-By-Step](#)

To deploy from an installer, do the following:

1. Download the installer file `<findface-security-xxx>.run`.
2. Put the `.run` file into some directory on the designated host (for example, `/home/username`).
3. From this directory, make the `.run` file executable.

```
chmod +x <findface-security-xxx>.run
```

4. Execute the `.run` file.

```
sudo ./<findface-security-xxx>.run
```

The installer will perform several automated checks to ensure that the host meets the system requirements. After that, the FindFace Security components will be automatically installed, configured and/or started in the following configuration:



Component	Details
findface-postgres-facen	Installed and started.
ffsecurity	Installed and started.
ffsecurity-ui	Installed and started.
videomanager-api	Installed and started.
video-worker	Installed and started.
findface-extraction-api	Installed and started.
NTLS	Installed and started.
nginx	Installed and started.
PostgreSQL database	Installed and started in a standard configuration.
Redis	Installed and started.
ETCD distributed key-value store	Installed and started.
jq	Installed. Used to pretty-print API responses from FindFace Security.

5. Once the installation is complete, the following output will be shown on the console:

**Tip:** Be sure to save this data: you will need it later.

```
#####
#           Installation is complete           #
#####
- upload your license to http://172.17.47.21:3185/
  login:          admin
  password:       0MBNics
- user interface: http://172.17.47.21/
  superuser:      admin
  password:       admin
  documentation:  http://172.17.47.21/doc/
```

6. Upload the FindFace Security license file via the NTLS web interface `http://<Host_IP_address>:3185/#/`. To access the NTLS web interface, use the credentials provided in the console.

**Note:** The host IP address is shown in the links to FindFace web services in the following way: as an external IP address if the host belongs to a network, or `127.0.0.1` otherwise.

**Important:** Do not disclose the `superuser` (Super Administrator) credentials to others. To administer the system, create a new user with the administrator privileges. Whatever the role, Super Administrator cannot be deprived of its rights.

## Deploy Step-By-Step

This section will guide you through the FindFace Security step-by-step deployment process. Follow the instructions below minding the sequence.

**Warning:** Before deploying FindFace Security, make sure that the system time and time zone are correct, and time synchronization via `ntpd/systemd-timesyncd` is enabled. When using FindFace Security, avoid any sudden changes in time, as they may result in unavailability of the FindFace Security services after reboot.

---

**Tip:** See *System Requirements* and *Architecture*.

---

### In this section:

- *Prepare Packages for Installation*
- *Prerequisites*
- *Licensing*
- *Basic Configuration*
- *Video-Based Biometric Identification*

## Prepare Packages for Installation

To prepare the FindFace Security deb-packages for installation, do the following:

1. Unpack the package with components.

```
sudo dpkg -i <findface-security-repo>.deb
```

2. Add a signature key.

```
sudo apt-key add /var/findface-security-repo/public.key  
sudo apt-get update
```

3. Unpack the packages with the neural network models.

```
sudo dpkg -i findface-data*.deb
```

## Prerequisites

The FindFace Security basic configuration requires **PostgreSQL** and **Redis**. Install them from the Ubuntu repository as such:

```
sudo apt-get update  
sudo apt install -y postgresql-server-dev-9.5 redis-server
```

The FindFace Security video-based biometric identification requires **ETCD**. Install it from the FindFace Security package with components:

```
sudo apt install -y etcd
```

## Licensing

You receive a license file from your NTechLab manager along with the FindFace Security distributable packages. For on-premise licensing, you will be also provided with a Guardant USB dongle.

To install and configure the license server (NTLS), do the following:

1. Install the NTLS component:

```
sudo apt-get update
sudo apt-get install ntls
```

**Tip:** In the NTLS configuration file, you can change the license folder and the NTLS web interface remote access settings. To open the NTLS configuration file, execute:

```
sudo vi /etc/ntls.cfg
```

If necessary, change the license folder in the `license-dir` parameter. By default, license files are stored at `/ntech/license`:

```
license-dir = /ntech/license
```

If necessary, uncomment the `proxy` line and specify your proxy server IP address:

```
proxy = http://192.168.1.1:12345
```

By default, you can access the NTLS web interface from any remote host (`ui = 0.0.0.0:3185`). To indicate that accessing the NTLS web interface must originate from a specific IP address, edit the `ui` parameter:

```
ui = 127.0.0.1:3185
```

2. Enable the NTLS service autostart and launch the service:

```
sudo systemctl enable ntls && sudo systemctl start ntls
```

3. Upload the license file via the NTLS web interface `http://<NTLS_IP_address>:3185/#/`.
4. For the on-premise licensing, insert a Guardant USB dongle into a USB port.

## Basic Configuration

The FindFace Security basic configuration includes a database, database extensions, the `ffsecurity` and `ffsecurity-ui` components. To install the basic configuration, do the following:

1. Install the `findface-postgres-9.5-facen` extension for **PostgreSQL** from the **<ffsecurity-repo>.deb** package:

```
sudo apt install -y findface-postgres-9.5-facen
```

2. Using the **PostgreSQL** console, create a new user `ntech` and a database `ffsecurity`. Upload the `findface-postgres-9.5-facen` extension to the `ffsecurity` database by using the `facen-compare-bytea` label.

```
sudo -u postgres psql

postgres=# CREATE ROLE ntech WITH LOGIN;

postgres=# CREATE DATABASE ffsecurity WITH OWNER ntech ENCODING 'UTF-8' LC_
↪COLLATE='en_US.UTF-8' LC_CTYPE='en_US.UTF-8' TEMPLATE template0;

postgres=# \c ffsecurity;

ffsecurity=# CREATE EXTENSION "facen-compare-bytea";
```

To quit from the PostgreSQL console, type `\q` press Enter.

3. Allow authentication in **PostgreSQL** by UID of a socket client. Restart **PostgreSQL**.

```
echo 'local all ntech peer' | sudo tee -a /etc/postgresql/9.5/main/pg_hba.conf

sudo systemctl restart postgresql@9.5-main.service
```

4. Install the `ffsecurity` component from the `<ffsecurity-repo>.deb` package.

---

**Note:** NginX will be automatically installed from dependencies.

---

```
sudo apt install -y ffsecurity
```

5. Install the `ffsecurity-ui` web interface from the `<ffsecurity-repo>.deb` package.

```
sudo apt install -y ffsecurity-ui
```

6. Open the `/etc/ffsecurity/config.py` configuration file. In the `EXTERNAL_ADDRESS` parameter , specify the external IP address or URL that will be used to access the FindFace Security web interface. If `videomanager-api` and/or `extraction-api` are to be installed on remote hosts, specify these hosts' IP addresses in the `VIDEO_MANAGER_ADDRESS` and `EXTRACTION_API` parameters respectively (see *Video-Based Biometric Identification* for details). To authorize the video face detection module, come up with a token and specify it as `VIDEO_DETECTOR_TOKEN`. This token will be being passed to the `videomanager-api` jobs.

---

**Tip:** If necessary, ensure data security by enabling *SSL*.

---

---

**Tip:** If necessary, set '`IGNORE_UNMATCHED`' : `True` to disable logging events for faces which have no match in the dossiers (negative verification result). Enable this option if the system has to process a large number of faces. The face similarity threshold for verification is defined by the `CONFIDENCE_THRESHOLD` parameter.

---

---

**Tip:** It is recommended to change the `MINIMUM_DOSSIER_QUALITY` default value. This parameter determines the minimum quality of a face in a dossier photo. Photos containing faces of worse quality will be rejected when uploading to a dossier. Upright faces in frontal position are considered the best quality. They result in values around 0, mostly negative (such as -0.00067401276, for example). Inverted faces and large face angles are estimated with negative values some -5 and less. By default, '`MINIMUM_DOSSIER_QUALITY`' : -2 which is the average quality.

---

```

sudo vi /etc/ffsecurity/config.py

MEDIA_ROOT="/var/lib/ffsecurity/uploads"
STATIC_ROOT="/var/lib/ffsecurity/static"

EXTERNAL_ADDRESS="http://172.20.77.26:8000"

DEBUG = False

LANGUAGE_CODE = 'en-us'

TIME_ZONE = 'UTC'

DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.postgresql',
        'NAME': 'ffsecurity',
    }
}

# use pwgen -sncy 50 1|tr "" ". " to generate your own unique key
SECRET_KEY = 'changeme'

FFSECURITY = {
    'VIDEO_DETECTOR_TOKEN': 'GOOD_TOKEN',
    'CONFIDENCE_THRESHOLD': 0.75,
    'MINIMUM_DOSSIER_QUALITY': -0.1,
    'IGNORE_UNMATCHED': False,
    'VIDEO_MANAGER_ADDRESS': 'http://127.0.0.1:18810',
    'EXTRACTION_API': 'http://127.0.0.1:18666/',
}

FFSECURITY_UI_CONFIG = {
    'plugins' =
        'genetec' = True,
}

```

**Tip:** If necessary, edit the `/etc/nginx/sites-available/ffsecurity-nginx.conf` configuration file as well.

7. Generate a signature key for the session encryption (used by **Django**) by executing: `pwgen -sncy 50 1|tr "" ". "`. Specify this key as `SECRET_KEY`.
8. Disable the default nginx server and add the `ffsecurity` server to the list of enabled servers. Restart nginx.

```

sudo rm /etc/nginx/sites-enabled/default

sudo ln -s /etc/nginx/sites-available/ffsecurity-nginx.conf /etc/nginx/sites-
→enabled/

sudo nginx -s reload

```

9. Migrate the database architecture from FindFace Security to **PostgreSQL**, create user groups with *pre-defined rights* and the first user with administrator rights (a.k.a. Super Administrator).

---

**Important:** Super Administrator cannot be deprived of its rights, whatever the role.

---

```
sudo findface-security migrate

sudo findface-security create_groups

sudo findface-security createsuperuser --username admin --email root@localhost
```

10. Start the services.

---

**Important:** The ffsecurity service includes findface-security-proto (provides HTTP and web socket) and findface-security-worker (provides interaction of the other system components). The number of the findface-security-worker instances is calculated using the formula:  $N = (\text{number of CPU cores} - 1)$ . It is specified after the @ character, for example, findface-security-worker@{1,2,3} for 3 instances.

---

```
sudo systemctl enable redis-server findface-security-proto findface-security-
↪worker@{1,2,3,4}

sudo systemctl start redis-server findface-security-proto findface-security-
↪worker@{1,2,3,4}
```

## Video-Based Biometric Identification

To install the videomanager-api, video-worker, and extraction-api components for video-based biometric identification, do the following:

1. Enable the ETCD service autostart and launch the service:

```
sudo systemctl enable etcd.service && sudo systemctl start etcd.service
```

2. Install videomanager-api, video-worker, and extraction-api.

```
sudo apt install -y findface-videomanager-api fkvideo-worker findface-extraction-
↪api
```

3. Open the /etc/findface-videomanager-api.conf configuration file for editing. In the router\_url parameter, substitute the string that goes before v0/frame with the ffsecurity IP address and port (set as EXTERNAL\_ADDRESS at /etc/ffsecurity/config.py). The video-worker component will be posting detected faces to the specified address.

```
sudo vi /etc/findface-videomanager-api.conf

router_url: http://127.0.0.1:8000/v0/frame
```

4. In the ntls -> url parameter, specify the NTLS host IP address if the NTLS host is remote.

```
ntls:
  url: http://127.0.0.1:3185/
```

5. Open the /etc/video-worker.ini configuration file for editing.

```
sudo vi /etc/video-worker.ini
```

6. In the `ntls-addr` parameter, specify the NTLS host IP address if the NTLS host is remote.

```
ntls-addr=127.0.0.1:3133
```

7. In the `mgr-static` parameter, specify the `videomanager-api` host IP address, which provides `video-worker` with settings and the video stream list.

```
mgr-static=127.0.0.1:18811
```

8. In the `capacity` parameter, specify the maximum number of video streams to be processed by `video-worker`.

```
capacity=10
```

9. In the `extraction-api` configuration file, enable the `quality_estimator` to be able to estimate the face quality in a dossier.

**Note:** The *minimum face quality* in a dossier photo is set as `MINIMUM_DOSSIER_QUALITY` in `/etc/ffsecurity/config.py`.

```
sudo vi /etc/findface-extraction-api.ini

quality_estimator: true
```

10. In the `extraction-api` configuration file, disable searching for gender, age, emotions, and country recognition models by passing empty values to the `gender`, `age` and `emotions` and `countries47` parameters:

**Warning:** Do not remove the parameters themselves as in this case the system will be searching for default models.

```
models:
  gender: ''
  age: ''
  emotions: ''
  countries47: ''
```

As a result, the `extraction-api` configuration file should look something like this:

```
listen: :18666
dlib:
  model: /usr/share/findface-data/normalizer.dat
  options:
    adjust_threshold: 0
    upsample_times: 1
nnd:
  model: /usr/share/nnd/nnd.dat
  quality_estimator: false
  quality_estimator_model: /usr/share/nnd/quality_estimator_v2.dat
  options:
    min_face_size: 30
    max_face_size: .inf
```

(continues on next page)

(continued from previous page)

```

    scale_factor: 0.79
    p_net_thresh: 0.5
    r_net_thresh: 0.5
    o_net_thresh: 0.9
    p_net_max_results: 0
models:
  root: /usr/share/findface-data/models
  facen: elderberry_576
  gender: ''
  age: ''
  emotions: ''
  countries47: ''
  model_instances: 1
license_ntls_server: 127.0.0.1:3133
fetch:
  enabled: true
  size_limit: 10485760
max_dimension: 6000
allow_cors: false
ticker_interval: 5000

```

11. Enable the videomanager-api, video-worker, and extraction-api autostart and launch the services.

```

sudo systemctl enable findface-videomanager-api.service && sudo systemctl start _
↪ findface-videomanager-api.service

sudo systemctl enable video-worker.service && sudo systemctl start video-worker.
↪ service

sudo systemctl enable findface-extraction-api.service && sudo systemctl start _
↪ findface-extraction-api.service

```

### Additional video-worker deployment on remote hosts

Use the additional installer to install video-worker on a remote host.

**See also:**

*Allocate video-worker to Camera Group*

To deploy video-worker from the additional installer, do the following:

1. Download the installer file <video-worker-xxx>.run.
2. Put the .run file into some directory on the designated host (for example, /home/username).
3. From this directory, make the .run file executable.

```
chmod +x <video-worker-xxx>.run
```

4. Execute the .run file. The video-worker component will be automatically installed.

```
sudo ./<video-worker-xxx>.run
```

5. Open the /etc/video-worker.ini configuration file for editing.



```
sudo vi /etc/video-worker.ini
```

6. In the `ntls-addr` parameter, specify the NTLS host IP address.

```
ntls-addr=127.0.0.1:3133
```

7. In the `mgr-static` parameter, specify the `videomanager-api` host IP address, which provides `video-worker` with settings and the video stream list.

```
mgr-static=127.0.0.1:18811
```

8. In the `capacity` parameter, specify the maximum number of video streams to be processed by `video-worker`.

```
capacity=10
```

### 1.1.4 Web Interface

Use the web interface to interact with FindFace Security. To open the web interface, enter its basic address in the address bar of your browser, and log in.

**Note:** The basic address is set as `EXTERNAL ADDRESS` in the `/etc/ffsecurity/config.py` configuration file.

**Important:** To log in for the first time, use the `admin` account created during the *basic configuration* installation.

The web interface has a highly intuitive and handy design and provides the following functionality:

- *Camera Management.* Group cameras subject to their location. Add and configure a camera
- *Dossier Database.* Manage dossier classification lists (watch lists). Create dossiers manually and in bulk
- *User Management.* Manage FindFace Security users
- *Operator's Guide.* Real time face identification in live streams and video files. Search for faces in the event list and dossier database. Compare faces.

### 1.1.5 Camera Management

To configure video-based biometric identification, add cameras to FindFace Security, grouping them subject to their location.

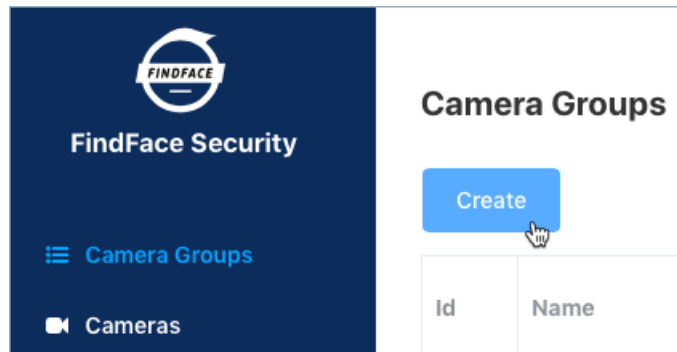
**In this chapter:**

- *Create Group of Cameras*
- *Add Camera to Group*
- *Monitor Camera Operation*

## Create Group of Cameras

To create a group of cameras, do the following:

1. Navigate to the *Camera groups* tab.



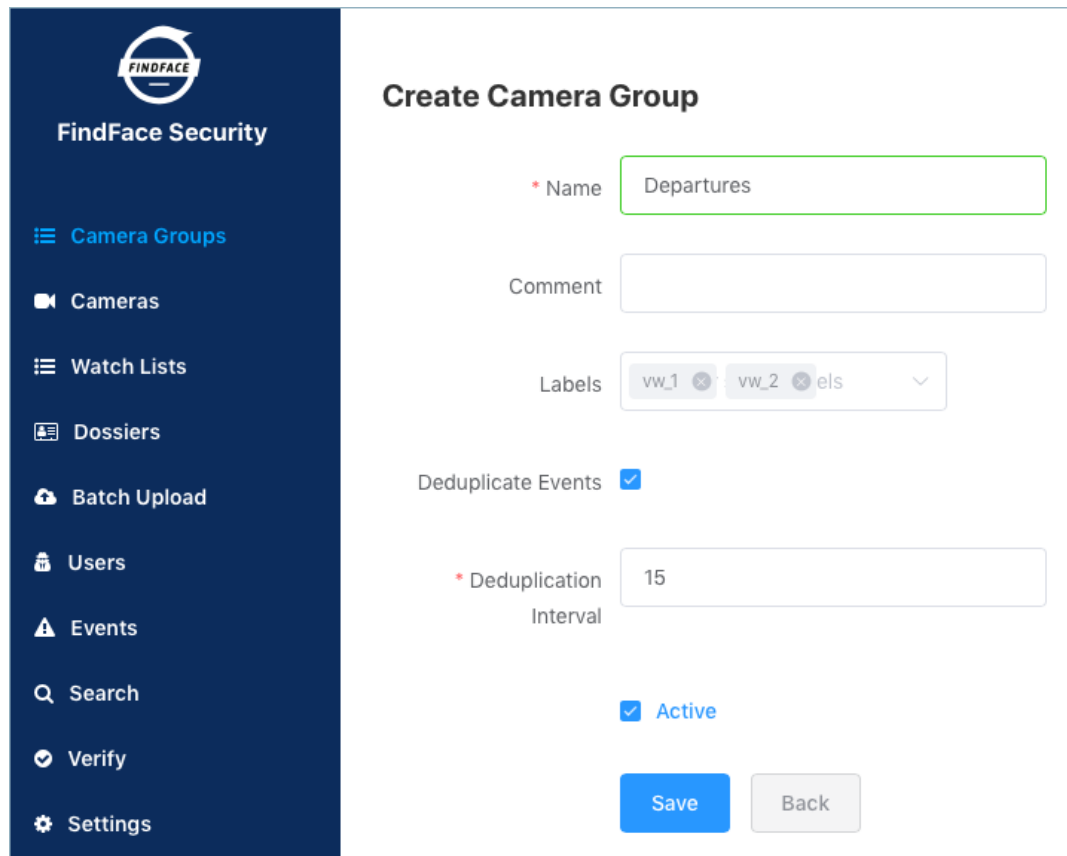
2. Click *Create*.
3. Specify the group name. Add a comment.
4. If you want to allocate a certain `video-worker` instance to process video streams from the group, create or select one or several allocation labels.

---

**Note:** To complete the allocation, *Allocate video-worker to Camera Group* the labels in the `video-worker` configuration file.

---

5. If you want to deduplicate events from cameras that belong to the same group, i. e. exclude coinciding events, check *Deduplicate Events* and specify the deduplication interval in seconds (interval between 2 consecutive checks for event uniqueness).
6. Check *Active*.



**FindFace Security**

- Camera Groups
- Cameras
- Watch Lists
- Dossiers
- Batch Upload
- Users
- Events
- Search
- Verify
- Settings

### Create Camera Group

\* Name

Comment

Labels

Deduplicate Events ☒

\* Deduplication Interval

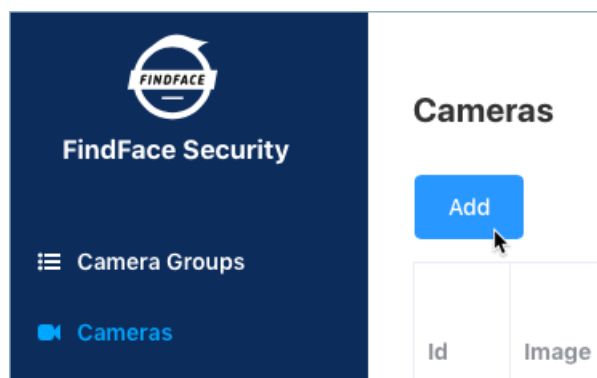
☒ Active

7. Click *Save*.

## Add Camera to Group

To add a camera to a group, do the following:

1. In the web interface, go to the *Cameras* tab.



**FindFace Security**

- Camera Groups
- Cameras

### Cameras

Id	Image

2. Click *Add*.
3. Specify the name of a camera and add it to a group. If necessary, add a comment.

**Add Camera**

\* Name

\* Group

\* URL

Comment

☒ Active

4. Specify the camera URL or path to the video file.

5. Check *Active*.

6. To configure CPU-based video processing, click *Parameters* and navigate to the *CPU* tab.

- **Min face quality:** Minimum quality of a face snapshot when searching for the best one. To be fitted empirically: negatives values around 0 = high quality faces, -1 = good quality, -2 = satisfactory quality, -5 = inverted faces and large face angles, face recognition may be inefficient.
- **Max face angle:** Maximum deviation of a face from its frontal position. To be fitted empirically: -3.5 = large face angles, face recognition may be inefficient, -2.5 = satisfactory deviation, -0.05 = close to the frontal position, 0 = frontal face.
- **Min face size:** Minimum face size in pixels. The less the value, the longer it takes to detect and track faces. Optimum value: 80-100-120. If 0, the filter is off.
- **Max face size:** Maximum face size in pixels. If 0, the filter is off.
- **Realtime mode:** Realtime mode. Pick up the best snapshot within each Snapshot picking interval time interval. If `Post each best snapshot: true`, the best snapshot is posted at the end of each interval; if `false`, the best snapshot is posted only if its quality has improved comparing to the previously posted snapshot.
- **Post each best snapshot:** If `true`, post the best snapshot obtained within each Snapshot picking interval time interval in realtime mode. If `false`, post the best snapshot only if its quality has improved comparing to the previously posted snapshot.
- **Snapshot picking interval:** Time interval in milliseconds within which the face tracker picks up the best snapshot in realtime mode.
- **Offline mode:** Offline mode. Enable posting one snapshot of the best quality for each face.

- **ROT:** Enable detecting and tracking faces only inside a clipping rectangle. Use this option to reduce the video face detector load.
- **ROI:** Enable posting faces detected only inside a region of interest.

---

**Tip:** To specify ROT/ROI, use the visual wizard. First, create a camera without ROT/ROI. Then open it for editing and click *Parameters*. You will see the visual wizard appear.

---

7. If necessary, specify optional parameters for CPU-based video processing. Click *Advanced Parameters*.

- **FFMPEG options:** FFMPEG options for a video stream in the key-value format ["rtsp\_transpotr=tcp", "ss=00:20:00"].
- **Frame height:** Video frame height in pixels for the face tracker. Negative values correspond to the initial size. Optimum value to reduce load: 640-720.
- **Tracked faces:** Maximum number of faces simultaneously tracked by the face tracker. This parameter severely affects performance.
- **Tracker threads:** Number of tracking threads for the face tracker. This value should be less or equal to the number of tracked faces. Recommended to set them equal. If the number of tracking threads is less than the maximum number of tracked faces, resource consumption is reduced but so is the tracking speed.
- **JPEG quality:** Full frame compression quality.
- **Draw track:** Enable drawing a face motion track in a bbox.
- **Response timeout:** Response timeout in milliseconds for an API request.
- **Min motion intensity:** Minimum motion intensity to be detected by the motion detector. To be fitted empirically: 0 = detector disabled, 0.002 = default value, 0.05 = minimum intensity is too high to detect motion.
- **Scale frame:** Video frame scaling coefficient for the motion detector from 0 to 1. Scale down in the case of high resolution cameras, or close up faces, or if the CPU load is too high, to reduce the system resources consumption.

8. To configure GPU-based video processing, click *Parameters* and navigate to the *GPU* tab.

- **Filter min face quality:** Minimum quality of a face snapshot to post. To be fitted empirically: negatives values around 0 = high quality faces, -1 = good quality, -2 = satisfactory quality, -5 = inverted faces and large face angles, face recognition may be inefficient.
- **Min face size:** Minimum face size in pixels to post. If 0, the filter is off.
- **Max face size:** Maximum face size in pixels in post.
- **Min face size:** Minimum face size in pixels to post. If 0, the filter is off.
- **JPEG quality:** Full frame compression quality.
- **FFMPEG options:** FFMPEG options for a video stream in the key-value format ["rtsp\_transpotr=tcp", "ss=00:20:00"].
- **Post only the best snapshot:** Offline mode. Enable posting one snapshot of the best quality for each face.
- **Posting timeout:** Response timeout in milliseconds for an API request.
- **Retrieve timestamps from stream:** If true, retrieve and post timestamps from a video stream. If false, post the actual date and time.
- **Add to timestamp:** Add the specified number of seconds to timestamps from a stream.

9. Click *Save*.

## Monitor Camera Operation

To monitor the operation of cameras, navigate to the *Cameras* tab.

**Cameras** English

Add

Page 1

Id	Image	Name	Group	Active	Status Process duration / Posted faces / Not posted faces	State
4		http://172.17.45.87/hls/openspace.m3u8	1	✓	● 2d 18h 31m 49s / 51 / 0	INPROGRESS Restart

**Filters**

Camera Groups  
Not selected

Active  
All

Status  
All

Clear

Camera statuses:

- Green: the video stream is being processed without errors.
- Yellow: the video stream is being processed for less than 30 seconds, or an error occurred when posting a face.
- Red: the video stream cannot be processed.

For each camera, you will be provided with the following statistics: current session duration/ the number of successfully posted faces/ the number of faces processed with errors.

To restart a camera, click *Restart* in the *State* column.

With a large number of cameras in the system, use the following filters:

- *Camera group*,
- *Active*,
- *Status*.

### 1.1.6 Dossier Database

FindFace Security allows you to create a dossier on a person. A dossier has to contain one or several photos of a person and belong to a certain classification list (watch list), black or white in the simplest case. You can create several watch lists, subject to a person status or hazard level.

**Tip:** To create dossiers in bulk, use the batch photo upload functionality.

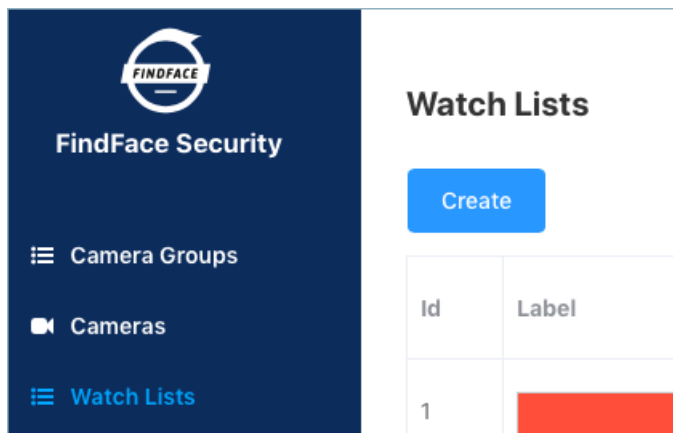
**In this chapter:**

- *Watch Lists*
  - *Create Watch List*
  - *Deactivate or Delete Dossier List*
  - *Filter Dossiers by List*
- *Create Dossier Manually*
- *Batch Photo Upload*

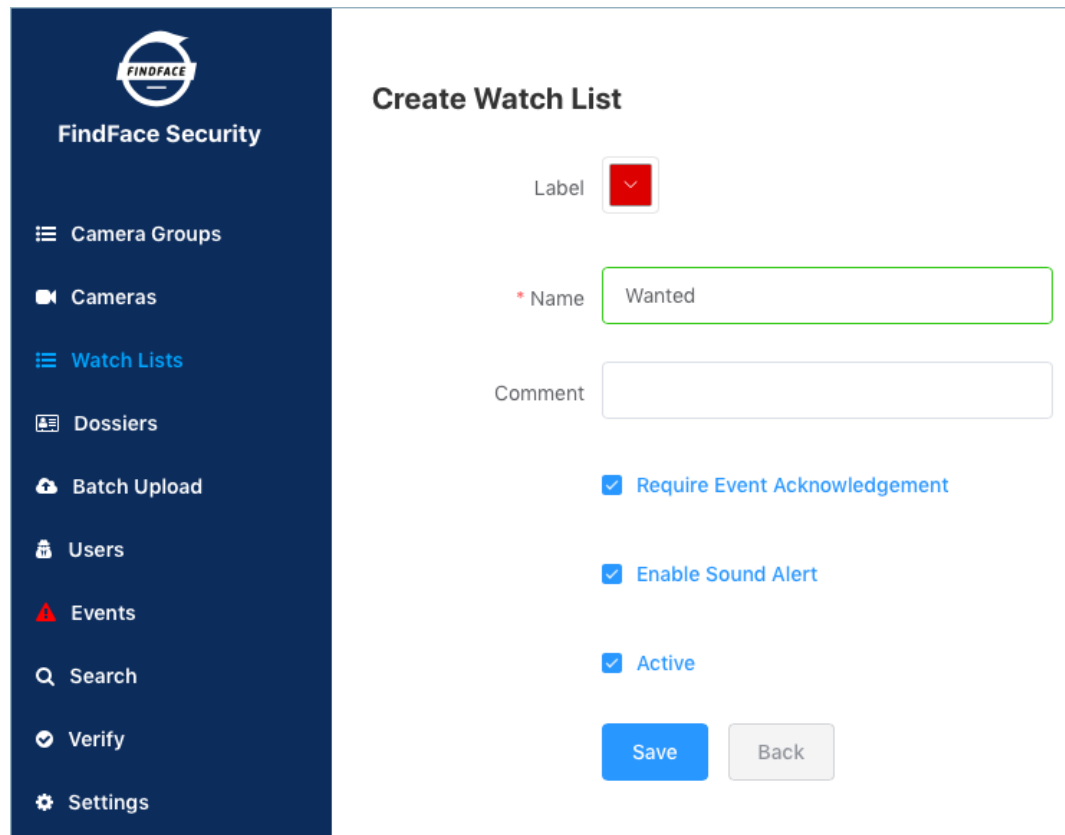
**Watch Lists****Create Watch List**

To create a watch list, do the following:

1. In the web interface, go to the *Watch Lists* tab.



2. Click *Create*.
3. From the *Label* palette, select a color which will be shown in notifications for this list. Keep in mind that the right color makes for quicker response of security and hospitality managers.



The screenshot shows the 'Create Watch List' interface in FindFace Security. On the left is a dark blue sidebar with the FindFace Security logo and a menu with the following items: Camera Groups, Cameras, Watch Lists (highlighted in blue), Dossiers, Batch Upload, Users, Events, Search, Verify, and Settings. The main content area is white and titled 'Create Watch List'. It contains a 'Label' dropdown menu with a red square icon, a required 'Name' text input field containing the word 'Wanted', and a 'Comment' text input field. Below these are three checked checkboxes: 'Require Event Acknowledgement', 'Enable Sound Alert', and 'Active'. At the bottom right are 'Save' and 'Back' buttons.

4. Specify the list name.
5. Check *Require acknowledgment* if it is mandatory that a manager acknowledge events for the list.
6. If necessary, turn on sound notifications for the list.
7. Check *Active*.
8. Click *Save*.

### Deactivate or Delete Dossier List

In order to deactivate or delete a watch list, do the following:

1. Click on the list name in the table.
2. To deactivate the list, uncheck *Active*. Click *Save*.
3. To delete the list, click *Delete*.

### Filter Dossiers by List

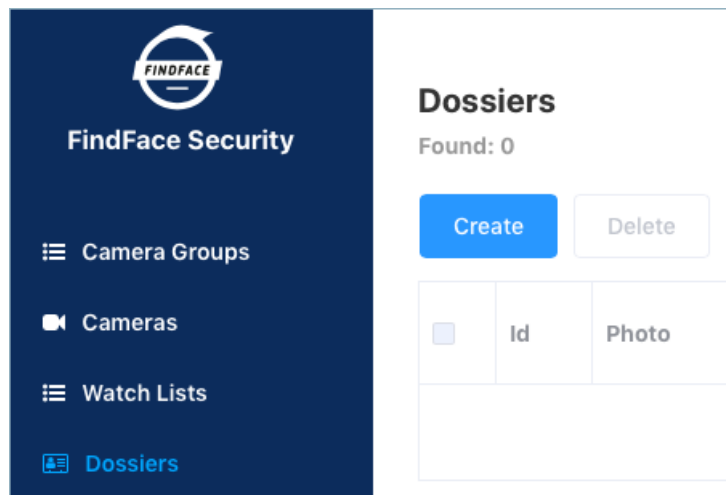
You can find all dossiers created in FindFace Security on the *Dossiers* tab. Use the *Watch lists* filter to filter dossiers by list.



## Create Dossier Manually

To create a dossier manually, do the following:

1. In the web interface, go to the *Dossier* tab.

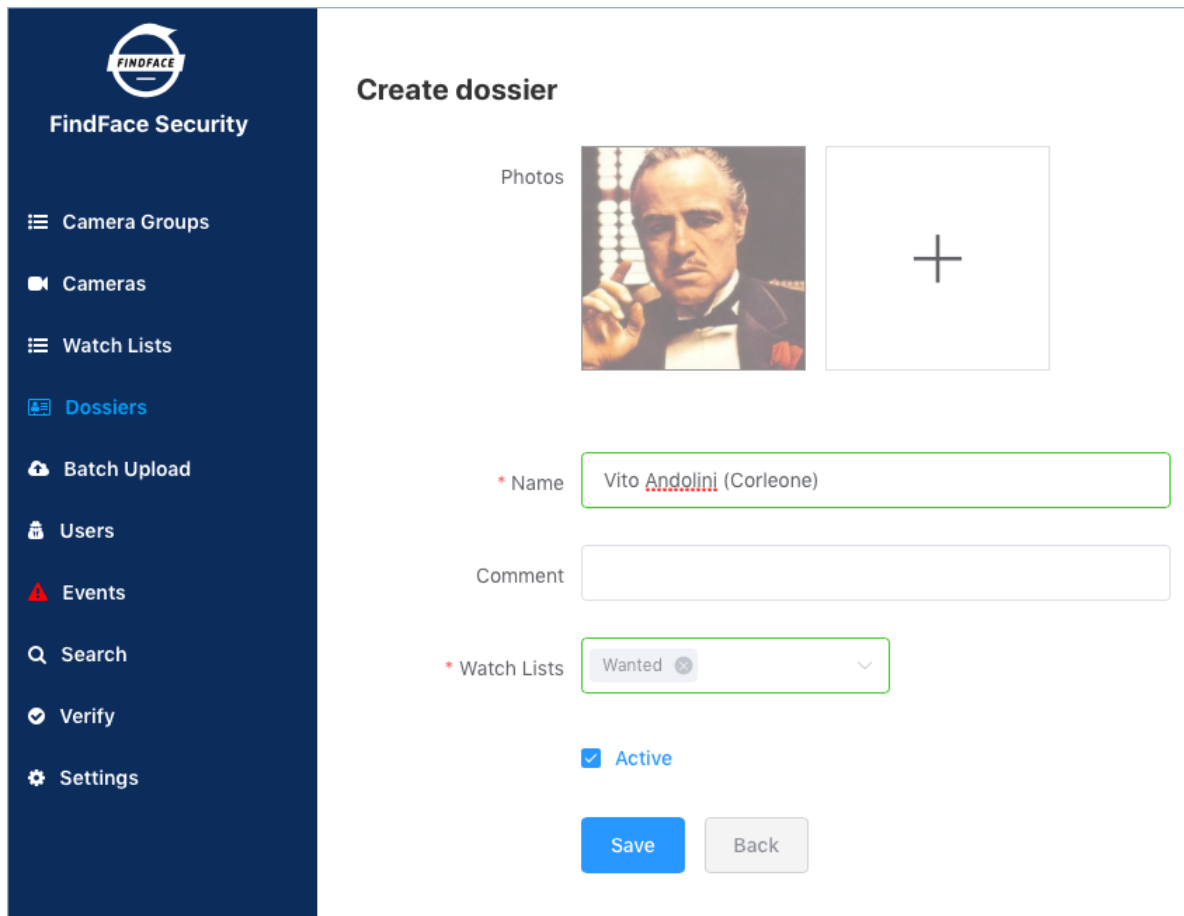


2. Click *Create*.
3. Attach one or several photos and specify the name of a person. If necessary, add a comment.

---

**Important:** A face in the photo must be of high quality, i.e. close to a frontal position. Photos that do not meet the requirement will be rejected with a detailed error description.

---



The screenshot shows the 'Create dossier' form in the FindFace Security application. On the left is a dark blue sidebar with the FindFace Security logo and a menu with the following items: Camera Groups, Cameras, Watch Lists, Dossiers (highlighted in blue), Batch Upload, Users, Events, Search, Verify, and Settings. The main content area is titled 'Create dossier' and contains the following fields and controls:

- Photos:** A section with a photo of a man in a tuxedo and a placeholder box with a large plus sign.
- Name:** A text input field containing 'Vito Andolini (Corleone)' with a red asterisk indicating it is required.
- Comment:** A text input field.
- Watch Lists:** A dropdown menu with 'Wanted' selected and a red asterisk indicating it is required.
- Active:** A checkbox that is checked, with the label 'Active' in blue.
- Buttons:** A blue 'Save' button and a grey 'Back' button.

4. From the *Watch lists* drop-down menu, select a classification list for the dossier.
5. Check *Active*. If a dossier is inactive, it is excluded from the real time *face identification*.
6. Click *Save*.

## Batch Photo Upload

To create dossiers in bulk, use the batch photo upload. Do the following:

1. In the web interface, go to the *Batch Upload* tab.

2. Select multiple image files, or a folder.
3. You can use image file names as a basis for names and/or comments in dossiers to be created. Select the necessary option(s). Then configure the automatic name/comment generation rule by appending a custom prefix and/or postfix to the file name.

---

**Tip:** To avoid merging the 3 words into one, use underscore or another symbol in the prefix and postfix.

---

4. From the *Watch lists* drop-down menu, select a classification list for the dossiers.
5. Use the *Parallel Upload* option to specify the number of photo upload streams. The more streams you use, the faster the batch photo upload is completed, however it requires more resources as well.
6. From the *MF selector* drop-down menu, select the system behavior upon detecting several faces in a photo: reject the photo, or upload the biggest face.
7. Click *Start* to launch the photo upload.

---

**Important:** To view the batch photo upload log, click *Log*. You can then download the log in the .csv format if needed.

Batch Upload Logs						
<a href="#">Back</a>		<a href="#">Delete</a>		<a href="#">«</a> <a href="#">&lt;</a> Page 1 <a href="#">U</a> <a href="#">&gt;</a> <a href="#">»</a>		
<input type="checkbox"/>	Id	Name	Created	Success count	Failed count	Download csv
No Data						
<a href="#">«</a> <a href="#">&lt;</a> Page 1 <a href="#">U</a> <a href="#">&gt;</a> <a href="#">»</a>						

### 1.1.7 User Management

To manage FindFace Security users, navigate to the *Users* tab.

#### In this chapter:

- *Roles*
- *Create User*
- *Deactivate or Delete User*

#### Roles

FindFace Security provides the following pre-defined roles:

- Administrator has rights to *manage cameras*, events, FindFace Security users, and the *dossier database*.

---

**Important:** Whatever the role, the first administrator *created on the console* (Super Administrator) cannot be deprived of its rights.

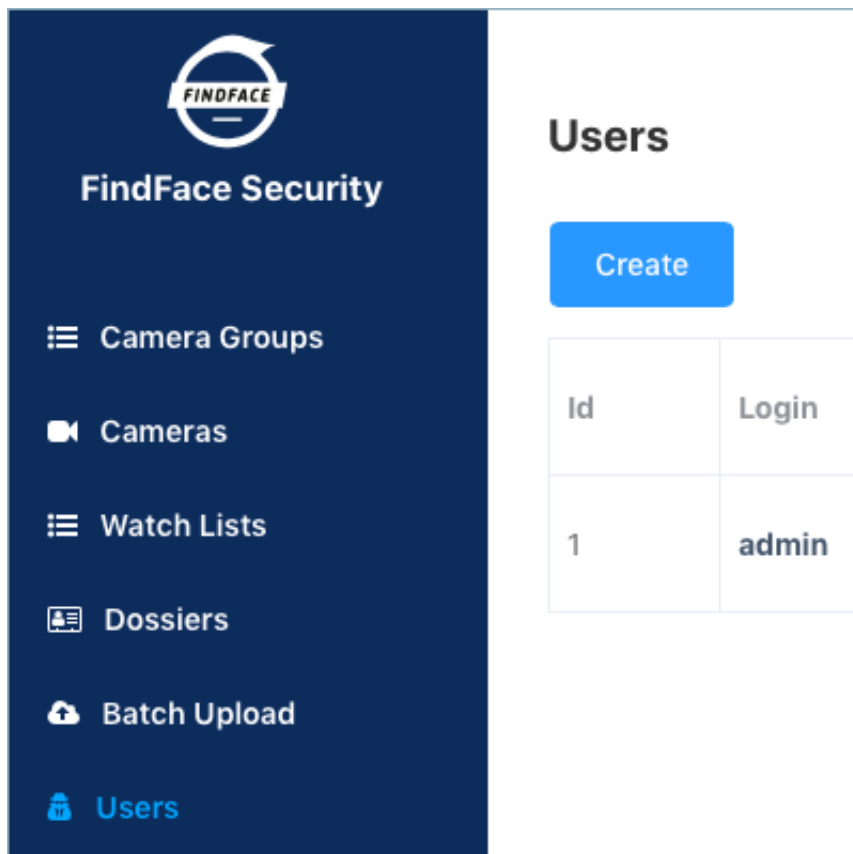
---

- Operator can *create dossiers manually*, receive and acknowledge events, and search for faces in the event list and dossier database. The other data is available read-only. The *batch* dossier creation is unavailable.
- User has a right to receive and acknowledge events, and to search for faces in the event list and dossier database. The other data is available read-only.

#### Create User

To create a user, do the following:

1. Click *Create*.



The screenshot shows the 'FindFace Security' application interface. On the left is a dark blue sidebar with the 'FINDFACE' logo and a list of menu items: 'Camera Groups', 'Cameras', 'Watch Lists', 'Dossiers', 'Batch Upload', and 'Users' (which is highlighted in blue). The main content area is white and titled 'Users'. It features a blue 'Create' button and a table with two columns: 'Id' and 'Login'. The table contains one row with the values '1' and 'admin'.

Id	Login
1	admin

2. Specify such user data as name, login and password. From the *Role* drop-down menu, select the user role. If necessary, add a comment.

**Create user**

\* Name

\* Login

\* Password

\* Confirm password

\* Role

Comment

Active ☒

3. Check *Active*.
4. Click *Create*.

### Deactivate or Delete User

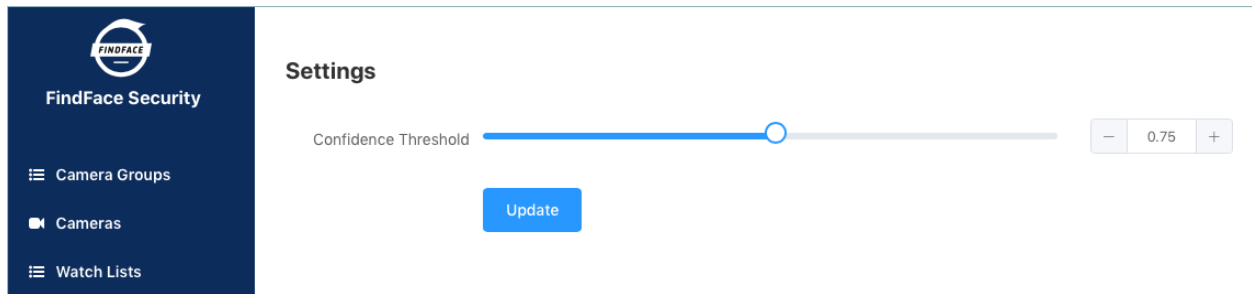
In order to deactivate or delete a user from FindFace Security, do the following:

1. Click on the user login in the list.
2. To deactivate a user, uncheck *Active*. Click *Update*.
3. To delete the user, click *Delete*.

### 1.1.8 Configuring Confidence Threshold

FindFace Security verifies that a detected face and some face from the dossiers belong to the same person (i. e. the faces match), based on the pre-defined similarity threshold. The default threshold is set to 0.75 which can be considered as optimum. If necessary, you can change the threshold on the *Settings* tab.

**Note:** The higher is the threshold, the less are chances that a wrong person will be positively verified, however, some valid photos may also fail verification.



**Tip:** You can configure your system to save and display an event only if the faces match (the `IGNORE_UNMATCHED` option at `/etc/ffsecurity/config.py`, see [Basic Configuration](#)).

### 1.1.9 Purge Old Events from Database

Use the `event-cleaner` utility to remove old events from the database.

To invoke the `event-cleaner` help message, execute:

```
sudo findface-security cleanup_events --help
```

```
usage: findface-security-manage cleanup_events [-h] [--version] [-v {0,1,2,3}]
                                             [--settings SETTINGS]
                                             [--pythonpath PYTHONPATH]
                                             [--traceback] [--no-color]
                                             --age AGE
```

Delete old events

optional arguments:

```
-h, --help            show this help message and exit
--version             show program's version number and exit
-v {0,1,2,3}, --verbosity {0,1,2,3}
                    Verbosity level; 0=minimal output, 1=normal output,
                    2=verbose output, 3=very verbose output
--settings SETTINGS  The Python path to a settings module, e.g.
                    "myproject.settings.main". If this isn't provided, the
                    DJANGO_SETTINGS_MODULE environment variable will be
                    used.
--pythonpath PYTHONPATH
                    A directory to add to the Python path, e.g.
                    "/home/djangoprojects/myproject".
--traceback           Raise on CommandError exceptions
--no-color            Don't colorize the command output.
--age AGE             Minimum age in days of events to clean up
```

In order to remove events older than a given number of days, use the `--age` option. For example, to remove events older than 5 days, execute:

```
sudo findface-security cleanup_events --age 5
```

To automatically remove events, add a scheduled job to Ubuntu's `cron`. The command in the example below adds a script file `/etc/cron.d/cleanup` that removes events older than 60 days. The script is executed daily at 00:05.

```
echo '5 0 * * * root /usr/bin/findface-security cleanup_events --age 60' | sudo tee /  
↳etc/cron.d/cleanup
```

## 1.1.10 Advanced Functionality

### Allocate video-worker to Camera Group

In distributed architectures, it is often necessary that video streams from a group of cameras be processed in situ, without being redistributed across remote `video-worker` instances by the main server. Among typical use cases are hotel chains, chain stores, several security checkpoints in the same building, etc. In this case, simply allocate the local `video-worker` to the camera group.

Do the following:

1. Navigate to the *Camera groups* tab.
2. Open the camera group settings.
3. In the *Labels*, create or select one or several allocation labels. Save changes.
4. Open the `video-worker` configuration file and specify the allocation labels in the following format: `label_name=true` (label `terminal_1` in the example below).

```
sudo vi /etc/video-worker.ini  
  
wrk-labels=terminal_1=true
```

5. Restart `video-worker`.

```
sudo systemctl restart video-worker.service
```

### Console Bulk Photo Upload

To bulk-upload photos to the dossier database, you can use the **`findface-security-uploader`** utility from the FindFace Security package (in addition to the web interface upload functionality). Use this utility when you need to upload a large number of photos (more than 10,000).

Do the following:

1. Write the list of photos and metastrings to a CSV or TSV file.

---

**Important:** The file used as a metadata source must have the following format: `path to photo | metastring`.

---

To prepare a TSV file, use either a script or the `find` command.

---

**Note:** Both the script and the command in the examples below create the `images.tsv` file. Each image in the list will be associated with a metastring coinciding with the image file name in the format `path to photo | metastring`.

---

To build a TSV file listing photos from a specified directory (`/home/user/25_celeb/` in the example below), run the following command:



```
python3 tsv_builder.py /home/user/25_celeb/
```

The find usage example:

```
find photos/ -type f -iname '*g' | while read x; do y="${x%.*}"; printf "%s\t%s\n"
↪ "$x" "${y##*/}"; done
```

2. Create a job file out of a CSV or TSV file by using add.

```
findface-security-uploader add images.tsv
```

The add options:

- `--format`: input file format, `tsv` by default.
- `--delimiter`: field delimiter, by default " " for TSV and ",", for CSV.

---

**Note:** A job file represents a sqlite database which can be opened on the **sqlite3** console.

---

3. Process the job file by using run.

```
findface-security-uploader run --dossier-lists 2 --api http://127.0.0.1:80 --user_
↪admin --password password
```

The run options:

- `--parallel`: the number of photo upload threads, 10 by default. The more threads you use, the faster the bulk upload is completed, however it requires more resources too.
- `--api`: findface-security API URL, `http://127.0.0.1:80/` by default.
- `--user`: login.
- `--password`: password.
- `--dossier-lists`: comma-separated list of the watch lists id's.
- `--failed`: should an error occur during the job file processing, correct the mistake and try again with this option.

## 1.1.11 Maintenance and Troubleshooting

### Audit-logs

Audit logs contain detailed information about all the events occurred in the system and are great for troubleshooting.

---

**Important:** In order to enable saving audit logs to your hard drive, uncomment and edit the `Storage` parameter in the `/etc/systemd/journald.conf` file:

```
sudo vi /etc/systemd/journald.conf
...
[Journal]
Storage=persistent
```

If necessary, uncomment and edit the `SystemMaxUse` parameter as well. This parameter determines the maximum volume of log files on your hard drive (10% by default).

```
SystemMaxUse=15
```

To view audit logs, execute:

```
journalctl -o verbose SYSLOG_IDENTIFIER=ffsecurity
```

When interpreting audit logs, first of all pay attention on the following parameters:

- REQUEST\_USER: user who made the changes;
- REQUEST\_PATH: URL of the request;
- REQUEST\_DATA: detailed information of the request.

In the log below, the admin user creates a dossier id=1879.

```
2017-12-22 17:53:32.436258 MSK [s=0b5566699751426983e13241301205e9;i=e26015;
↪b=907c34cc1fde4398af63bb575587d9ba;m=246f620c449;t=560eefaf59bc5;x=ed60a136c8fc6362]
  PRIORITY=6
  _UID=123
  _GID=130
  _CAP_EFFECTIVE=0
  _BOOT_ID=907c34cc1fde4398af63bb575587d9ba
  _MACHINE_ID=a3eea61c03e041ef8e64d5c72f5fce40
  _HOSTNAME=ntechadmin
  SYSLOG_IDENTIFIER=ffsecurity
  THREAD_NAME=MainThread
  _TRANSPORT=journal
  _PID=6579
  _COMM=findface-securi
  _EXE=/opt/ffsecurity/bin/python3
  _CMDLINE=/opt/ffsecurity/bin/python /opt/ffsecurity/bin/findface-security runworker
  _SYSTEMD_CGROUP=/system.slice/system-findface\x2dsecurity\x2dworker.slice/findface-
↪security-worker@4.service
  _SYSTEMD_UNIT=findface-security-worker@4.service
  _SYSTEMD_SLICE=system-findface\x2dsecurity\x2dworker.slice
  CODE_FILE=/opt/ffsecurity/lib/python3.5/site-packages/ffsecurity/mixins.py
  CODE_LINE=94
  CODE_FUNC=finalize_response
  REQUEST_USER=admin
  LOGGER=ffsecurity.audit
  MESSAGE=N8Be05il POST /dossier-faces/ 201 by admin
  REQUEST_DATA={"dossier": "'1879'", "source_photo": "<InMemoryUploadedFile:↪
↪14927016033292449.jpeg (image/jpeg)>"}
  REQUEST_PATH=/dossier-faces/
  REQUEST_ID=N8Be05il
  _SOURCE_REALTIME_TIMESTAMP=1513954412436258
```

In the next log, the list of faces is requested for the dossier id=1879.

```
2017-12-22 17:53:32.475467 MSK [s=0b5566699751426983e13241301205e9;i=e26016;
↪b=907c34cc1fde4398af63bb575587d9ba;m=246f6215d82;t=560eefaf634fe;x=b1374a144a46b5cd]
  PRIORITY=6
  _UID=123
  _GID=130
  _CAP_EFFECTIVE=0
  _BOOT_ID=907c34cc1fde4398af63bb575587d9ba
  _MACHINE_ID=a3eea61c03e041ef8e64d5c72f5fce40
```

(continues on next page)

(continued from previous page)

```

_HOSTNAME=ntechadmin
SYSLOG_IDENTIFIER=ffsecurity
THREAD_NAME=MainThread
_TRANSPORT=journal
_COMM=findface-securi
_EXE=/opt/ffsecurity/bin/python3
_CMDLINE=/opt/ffsecurity/bin/python /opt/ffsecurity/bin/findface-security runworker
_SYSTEMD_SLICE=system-findface\x2dsecurity\x2dworker.slice
_PID=6588
_SYSTEMD_CGROUP=/system.slice/system-findface\x2dsecurity\x2dworker.slice/findface-
security-worker@2.service
_SYSTEMD_UNIT=findface-security-worker@2.service
CODE_FILE=/opt/ffsecurity/lib/python3.5/site-packages/ffsecurity/mixins.py
CODE_LINE=94
CODE_FUNC=finalize_response
REQUEST_USER=admin
REQUEST_DATA={}
LOGGER=ffsecurity.audit
MESSAGE=Dee7Qvy4 GET /dossier-faces/?dossier=1879&limit=1000 200 by admin
REQUEST_ID=Dee7Qvy4
REQUEST_PATH=/dossier-faces/?dossier=1879&limit=1000
_SOURCE_REALTIME_TIMESTAMP=1513954412475467

```

## Remove Instance

You can automatically remove FindFace Security 1.1 along with the database by using the `ffsec_1.1_uninstall.sh` script. The FindFace Security configuration files and database will be backed up.

---

**Note:** To remove FindFace Security 1.0, use `ffsec_1.0_uninstall.sh` instead.

---

Do the following:

1. Download the `ffsec_1.1_uninstall.sh` script to some directory on a designated host (for example, to `/home/username/`).
2. From this directory, make the script executable.

```
chmod +x ffsec_1.1_uninstall.sh
```

3. Run the script.

```
sudo ./ffsec_1.1_uninstall.sh
```

4. Answer **all** to completely remove FindFace Security along with the database.

## 1.1.12 Appendix. Enable Data Encryption

To ensure data security, it is recommended to enable SSL encryption. Do the following:

1. Under the nginx configuration directory, create a directory that will be used to hold all of the SSL data:

```
sudo mkdir /etc/nginx/ssl
```

2. Create the SSL key and certificate files:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/  
my-example-domain.com.key -out /etc/nginx/ssl/my-example-domain.com.crt
```

You will be asked a few questions about your server in order to embed the information correctly in the certificate. Fill out the prompts appropriately. The most important line is the one that requests the Common Name. You need to enter the domain name or public IP address that you want to be associated with your server. Both of the files you created (`my-example-domain.com.key` and `my-example-domain.com.crt`) will be placed in the `/etc/nginx/ssl` directory.

3. Configure nginx to use SSL. Open the nginx configuration file. Copy the code from the example below into the file.

```
sudo vi /etc/nginx/nginx.conf  
  
# redirect from http to https version of the site  
server {  
    listen 80;  
    server_name my-example-domain.com www.my-example-domain.com;  
    rewrite ^(.*) https://my-example-domain.com$1 permanent;  
    access_log off;  
}  
  
server {  
    listen 443 ssl;  
    server_name my-example-domain.com;  
  
    ssl_certificate /etc/nginx/ssl/my-example-domain.com.crt;  
    ssl_certificate_key /etc/nginx/ssl/my-example-domain.com.key;  
  
    root /usr/share/ffsecurity-ui  
  
    location / {  
        try_files $uri $uri/ @ffsec;  
    }  
  
    location @ffsec {  
        proxy_pass http://127.0.0.1:8002;  
    }  
}
```

4. Restart nginx.

```
sudo service nginx restart
```

5. Edit the `ffsecurity` configuration file. In the `EXTERNAL_ADDRESS` parameter, substitute the `http://` prefix with `https://`.

```
sudo vi /etc/ffsecurity/config.py  
  
EXTERNAL_ADDRESS="https://my-example-domain.com"
```

## 1.2 Operator's Guide

### 1.2.1 Web Interface

Use the web interface to interact with FindFace Security. To open the web interface, enter its address in the address bar of your browser, and log in.

---

**Note:** Request credentials from administrator.

---

The web interface has a highly intuitive and handy design and provides the following functionality:

- *Search Databases*. Search for faces in the event list and dossier database
- *Real-time Face Identification*. Real time face identification in live streams and video files
- *Compare Faces*. Compare two faces
- *Dossier* (only for users granted the operator rights). View and create a dossier on a person

### 1.2.2 Search Databases

FindFace Security allows you to search for faces in the following databases:

- Database of detected faces (the *Events* tab)
- Dossier database (the *Dossier* tab). Contains face reference images

To find a face in a database, navigate to the *Search* tab.

#### In this chapter:

- *Search for Faces in Event List*
  - *Search for Faces in Dossier List*

#### Search for Faces in Event List

FindFace Security allows you to search the database of detected faces.

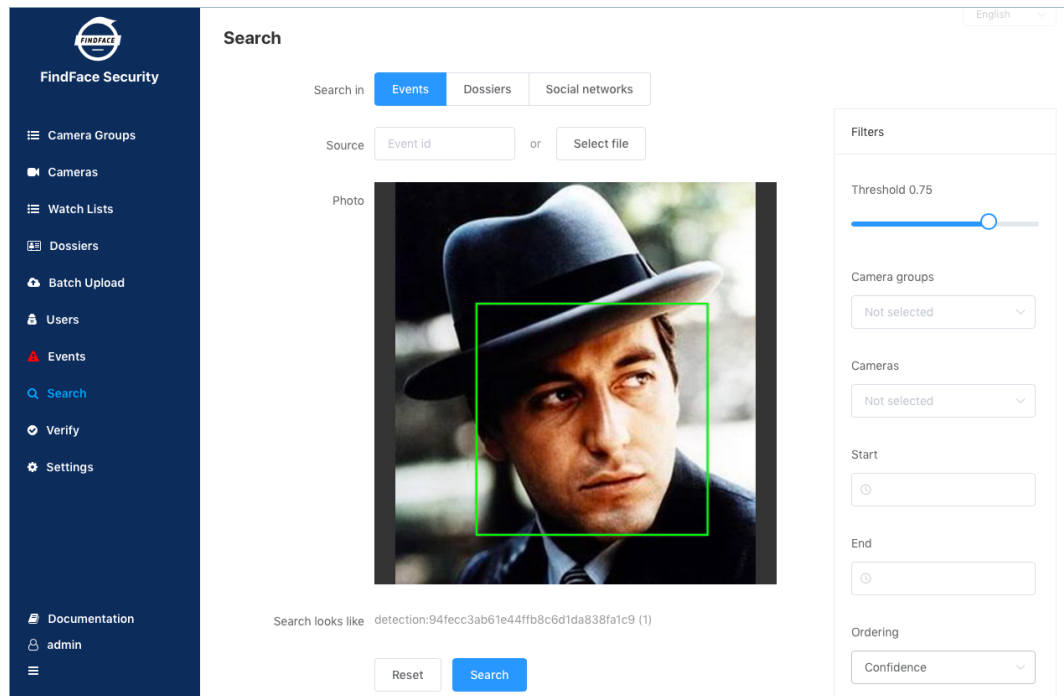
---

**Note:** You can access this database by navigating to the event list (the *Events* tab).

---

To find a face in the event list, do the following:

1. Navigate to the *Search* tab.



2. Select a database to search: *Events*.
3. Upload a photo. It will be displayed in the *Photo* area. If there are multiple faces in the image, select the one you want.

---

**Note:** Instead of a photo, you can specify the ID of an event that features the face you want to find.

---

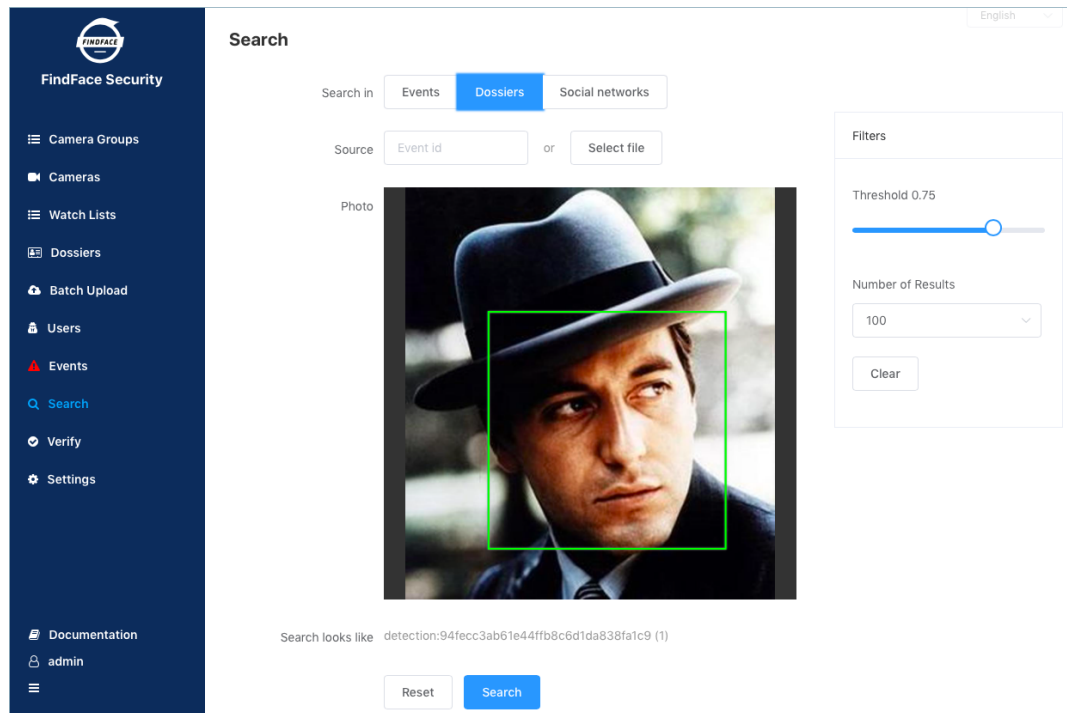
4. By default, the system searches for faces using the identification threshold 0.75. If necessary, set your own value.
5. (Optional) Specify a group of cameras and a time period within which the event occurred.
6. You can sort the search results by face similarity (in descending order), or by event date (first the most recent events). Select the sorting method from the *Ordering* list: *Confidence* or *Date* respectively.
7. Specify the maximum number of events in the search results.
8. Click *Search*. You will see the search results appear below. For each face found, the matching confidence level is provided.

### Search for Faces in Dossier List

FindFace Security allows you to search the database of dossiers containing face reference images.

To find a face in the event list, do the following:

1. Navigate to the *Search* tab.



2. Select a database to search: *Dossier*.
3. Upload a photo. It will be displayed in the *Photo* area. If there are multiple faces in the image, select the one you want.

---

**Note:** Instead of a photo, you can specify the ID of an event that features the face you want to find.

---

4. By default, the system searches for faces using the identification threshold 0.75. If necessary, set your own value.
5. Specify the maximum number of dossiers in the search results.
6. Click *Search*. You will see the search results appear below. For each face found, the matching confidence level is provided.

### 1.2.3 Real-time Face Identification

To monitor the real-time face identification, go to the *Events* tab. The system can identify faces in both live video streams and archived video. Besides monitoring, the *Events* tab also allows you to access the history of identification events.

---

**Tip:** Search for faces through the event and dossier databases on the *Search* tab.

---

**In this chapter:**

- *View Identification Events*
- *Event Ticket. Acknowledging Event*
- *Event Ticket. Face Search*

### View Identification Events


Once a face detected, you will see a notification in the event list.

The screenshot displays the 'Events' section of the FindFace Security interface. The main area shows a table of events. The first event has an ID of 15278, a detected face image, and a timestamp of 2018-09-29 22:35:03. The 'Matched to' column shows 'No matches'. The second event has an ID of 15277, a detected face image, and a timestamp of 2018-09-29 22:35:03. The 'Matched to' column shows 'No matches'. The left sidebar contains navigation links: Camera Groups, Cameras, Watch Lists, Dossiers, Batch Upload, Users, Events, Search, Verify, and Settings. The right sidebar contains filters for Dossier, Watch Lists, Matches, and Acknowledged. The top right shows the language set to English.

A notification can feature different pieces of information, depending on whether a detected face has a match in the database:

- **Match not found:** a normalized face image, detection date and time, the name of a camera group.
- **Match found:** a normalized face image, the photo from a dossier, the name of a person, similarity between faces, the comment from a dossier, the name of a dossier list, detection date and time, the name of a camera group.

**Note:** You can configure the system in such a way that you will get notifications only for the faces with a match.

**Important:** In order to pause the notifications thread, click  above the list of events.

When working with events, the following filters may come in handy:

- **Dossier:** display events only for a selected dossier.
- **Watch lists:** display events only for a selected dossier category (watch list).
- **Matches:** display events only with/without matches, or all events.
- **Acknowledged:** display only acknowledged/unacknowledged events, or all events.
- **Cameras:** display only events from a selected camera.
- **Camera groups:** display only events from a selected group of cameras.
- **Start, End:** display only events occurred within a certain time period.



- *id*: display an event with a given ID.

### Event Ticket. Acknowledging Event

In order to navigate to an event ticket from the list of events, click on the face recognition result in a notification (*No matches* or the name of a matching person).

An event ticket contains the same data as a relevant *notification*. It also allows for acknowledging the event. To do so, check *Acknowledge event*. Click *Save*.

Id 15278

Events

Dossiers

Social networks

Name no

+ Create Dossier

Confidence no

Comment no

Time 2018-09-29 22:35:03

Camera

http://172.17.45.87/hls/openspace.m3u8

Camera group

1

Watch lists


☒ Event acknowledgement

Save

Back

**Tip:** If a detected face has a match in the dossiers, you can navigate into a relevant one by clicking on the person's name in the event ticket.



**Tip:** In order to acknowledge all the events, click  above the list of events.

---

**Note:** Event acknowledgment can be automated for selected watch lists.

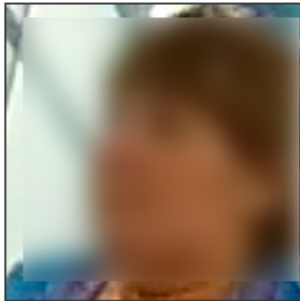
---

### Event Ticket. Face Search

FindFace Security allows you to search the list of events and dossier database for faces detected in video. To navigate from an event ticket to the search tab, click *Events* or *Dossier* respectively.

## Events

Detected / Matched to



Id 15278   🔍 Events   🔍 Dossiers   🔍 Social networks

Name no   + Create Dossier

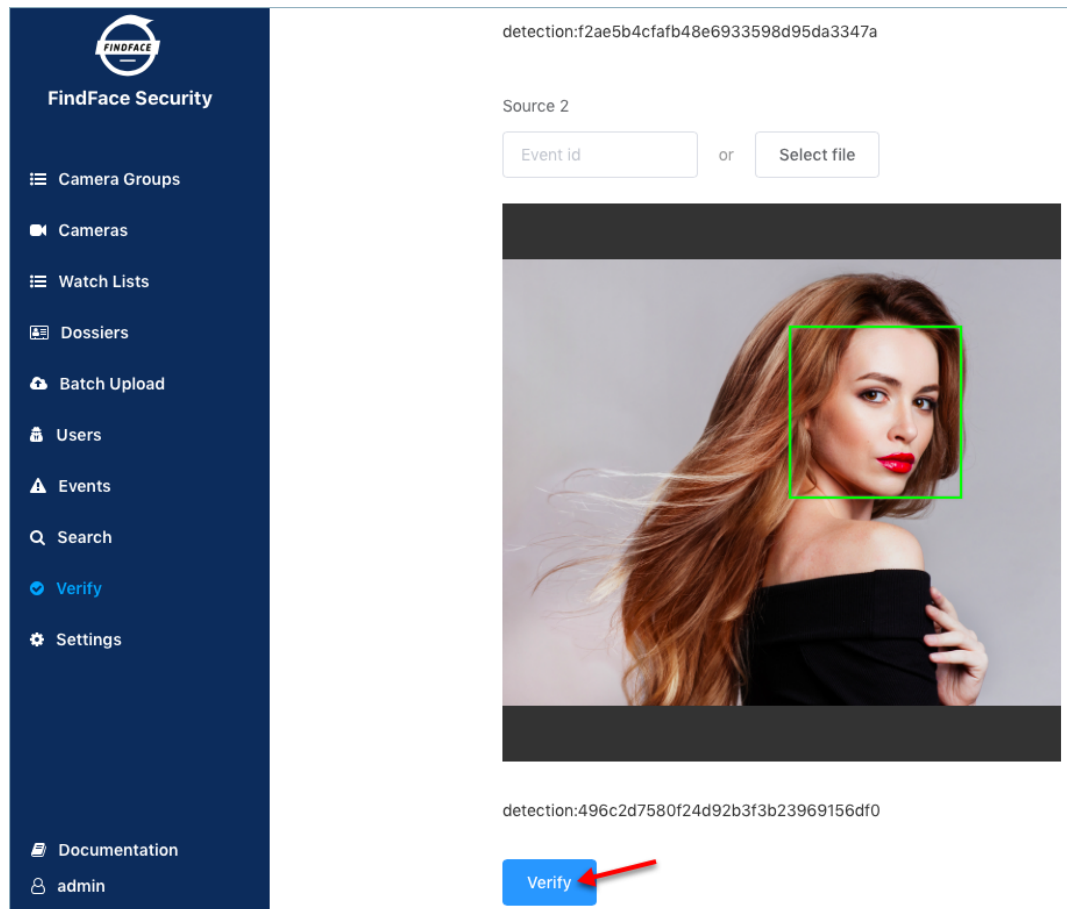
**See also:**

- *Search Databases.*

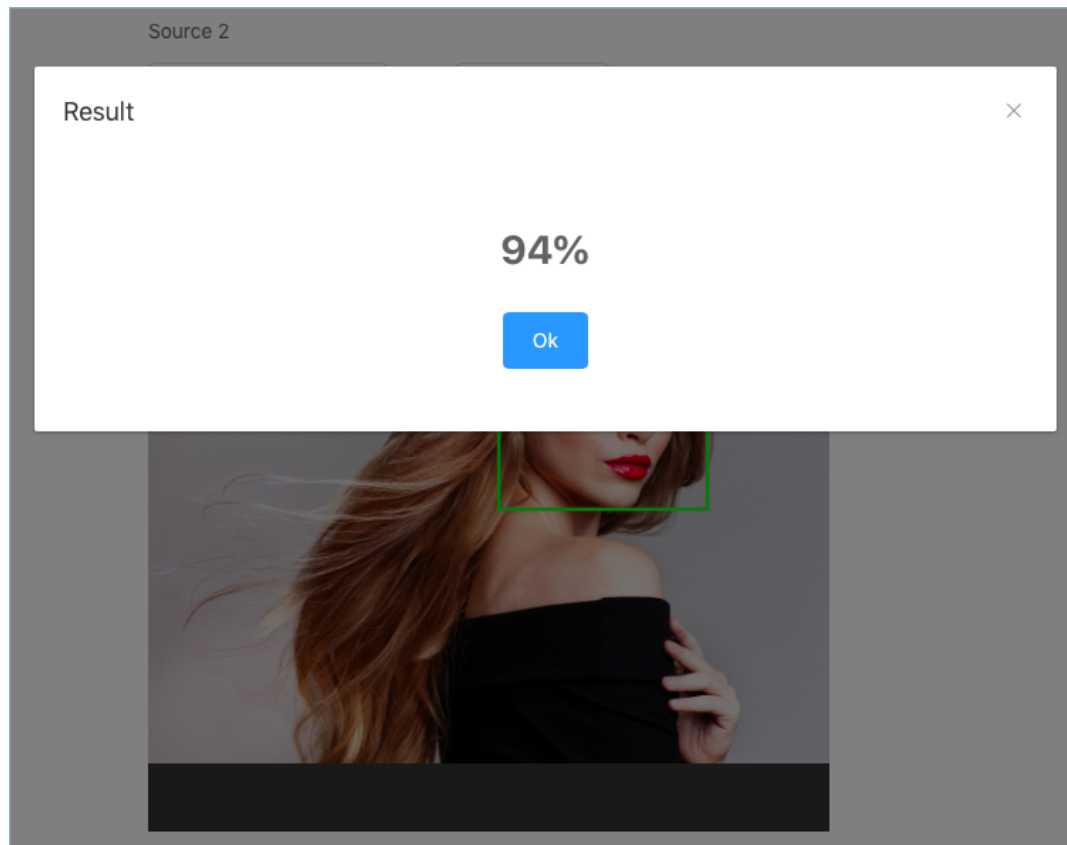
### 1.2.4 Compare Faces

FindFace Security allows you to compare 2 faces. Do the following:

1. Navigate to the *Verify* tab.



2. Specify the IDs of events that feature the faces you want to compare, and/or upload photos with the faces.
3. Click *Verify*. You will see the probability of the faces belonging to the same person appear.



### 1.2.5 Dossier

The dossier database contains dossiers on the unwanted persons and VIP guests. A dossier has to contain one or several photos of a visitor and belong to a certain classification list (watch list).

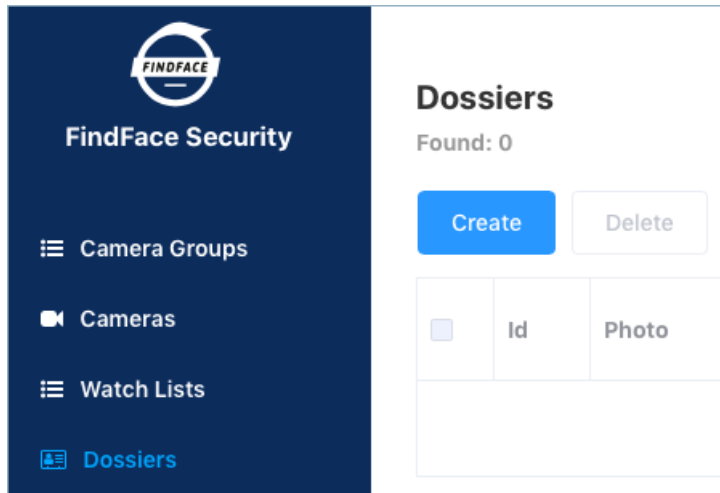
#### In this chapter:

- *Create Dossier*
- *View Dossier*

#### Create Dossier

To create a dossier on a visitor, do the following:

1. In the web interface, go to the *Dossier* tab.



2. Click *Create*.
3. Attach one or several photos and specify the name of a person. If necessary, add a comment.

**Important:** A face in the photo must be of high quality, i.e. close to a frontal position. Photos that do not meet the requirement will be rejected with a detailed error description.

4. From the *Watch lists* drop-down menu, select a classification list (or several lists, one by one) for the dossier.

5. Check *Active*. If a dossier is inactive, it is excluded from real time *face identification*.
6. Click *Save*.

### View Dossier

You can find all dossiers created in FindFace Security on the *Dossiers* tab. Use the *Watch lists* filter to filter dossiers by list.

### 1.2.6 Mobile App

To interact with FindFace Security on the go, use the mobile app. The FindFace Security app is available on request for Android/iOS.

In the app, specify your login and password, as well as the FindFace Security URL address, and log in.

16:43 64%

## FindFace Security

Login

admin

Password

.....

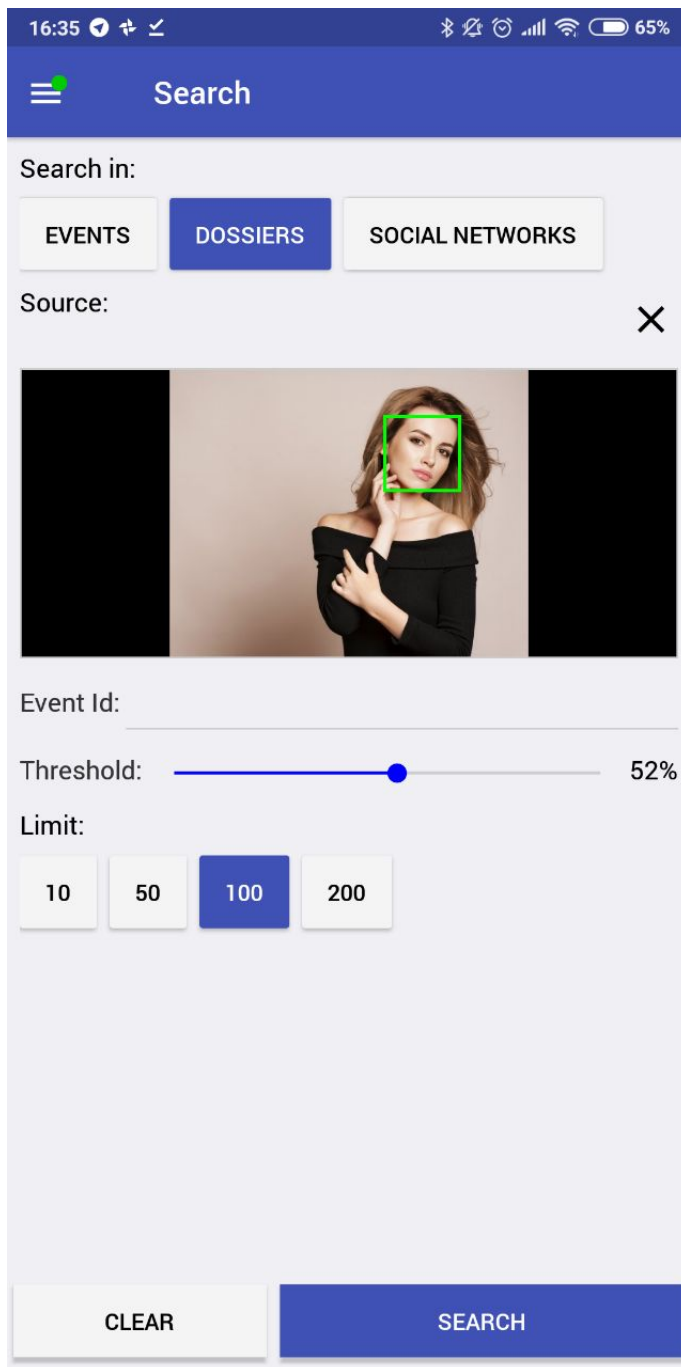
Url

http://172.20.77.58

LOGIN

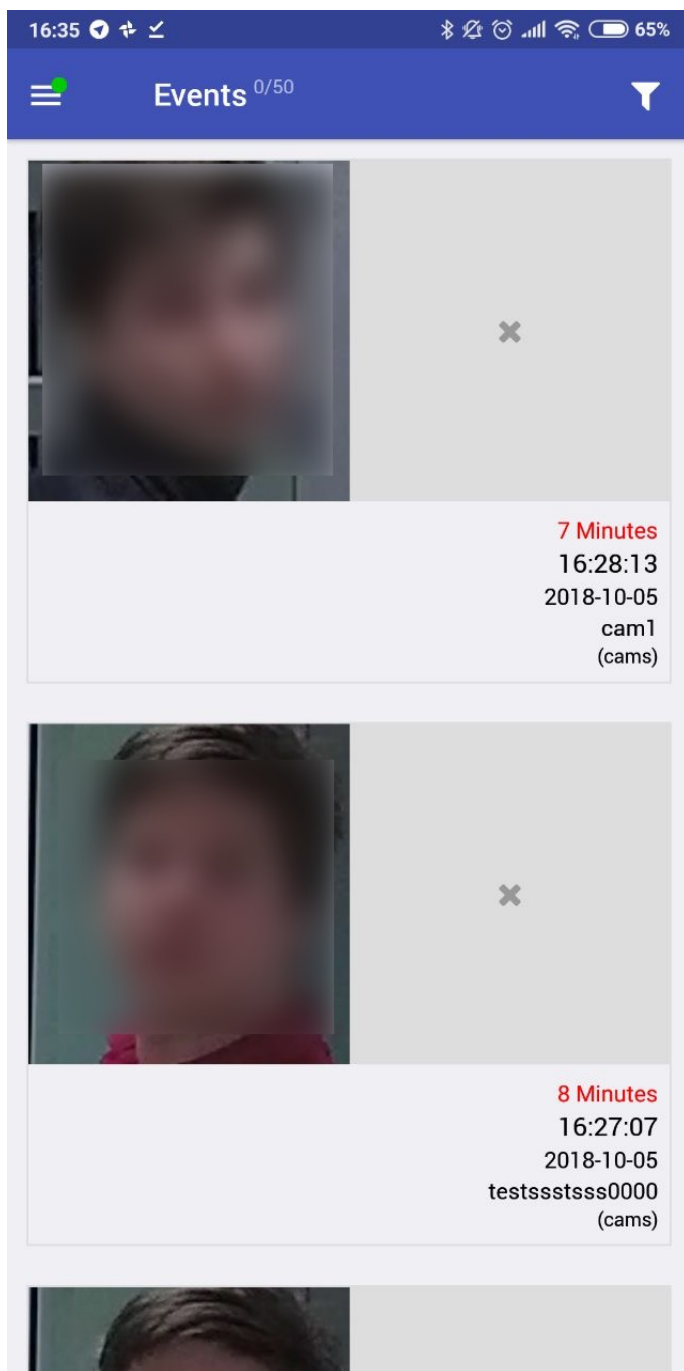
The mobile app has a highly intuitive and handy design and provides the following functionality:

- Search for faces in the event list and dossier database.



- Real time face identification in live streams and video files



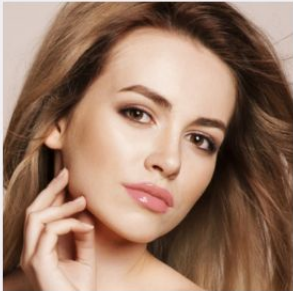


- View and create a dossier on a person

16:33 65%

← Edit Dossier

Photos +



Id: 1

Name: Sample

Comment: Comment

Watch lists:

☒ allow ✓

Active: ✓

UPDATE

Working with the mobile app is similar to the full version.