Version 1

FACE RECOGNITION PLATFORM

VIVOTEK INC.

VIVOTEK VAST Face User's Guide

August 2020

VIVOTEK INC.

VAST Face - User's Guide

VIVOTEK INC.

6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C.

TEL: +886-2-82455282| FAX: +886-2-82455532| E-Mail: sales@vivotek.com

Table of Contents

Chapter 1

1. VIVOTEK VAST Face Introduction

Real time authentication, high security level, and increased customer experience with VIVOTEK VAST Face

VIVOTEK VAST Face is a state-of-the-art security enhanced face recognition system, capable of analyzing video streams from IP Cameras , tablets or still images in real-time, for the purposes of verifying a person's identity against an existing face profiles database . Likewise, VAST Face is capable of providing face recognition access reports, and triggering system actions upon detecting an individual in a watchlist.

Thanks to its unique dessign and platform agnostic web client, VAST Face allows operators to acquire data from multiple image sources, manage registered persons face profiles or face groups, generate face recognition reports, and program automated system responses, all under a single interface.

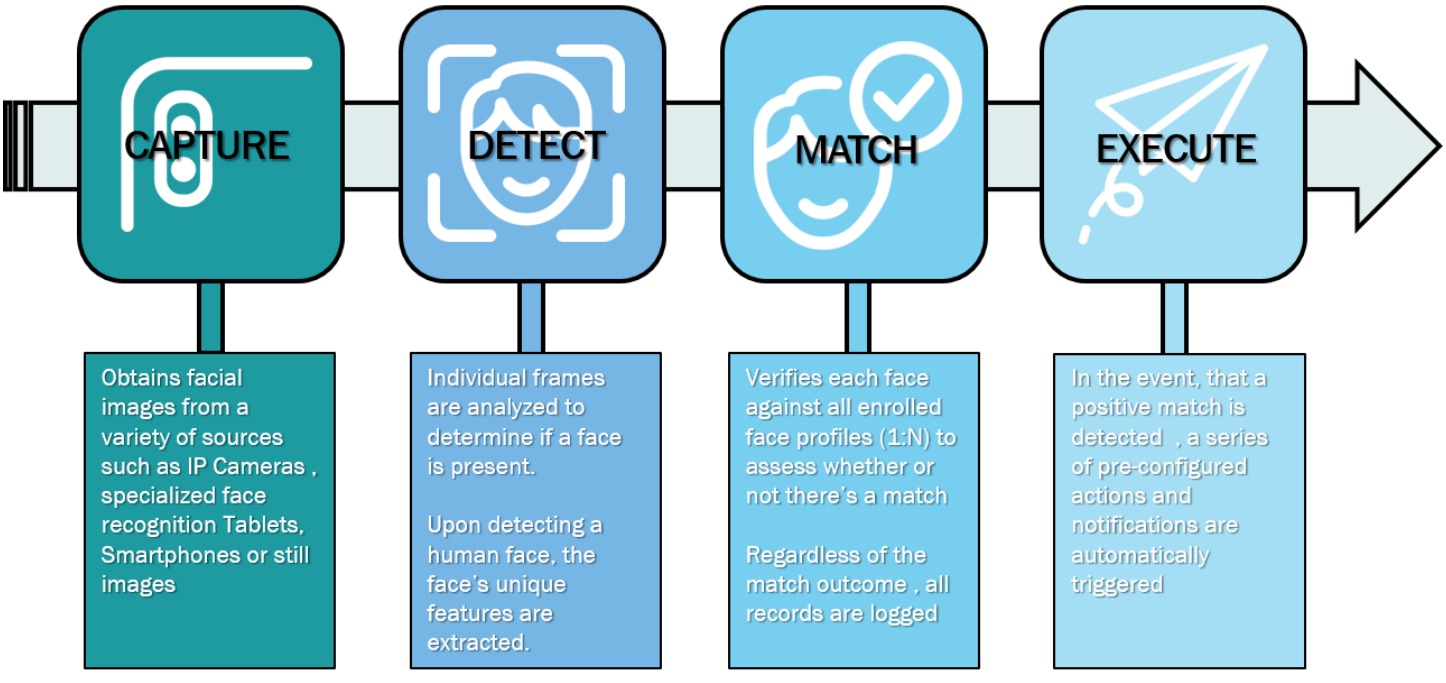


FIGURE 1.1 VAST Face System Process.

1.1 How does it work?

VIVOTEK VAST Face receives images/video streams from a variety of video sources be it: IP cameras, Face Recognition tablets; each individual frame upon received is analyzed by an A.I engine, responsible for comparing each detected face against an existing face profiles database, a confidence level is then assigned to each match and results are ranked , with only the highest match result being logged as a face recognition events, this high confidence value match then used to deem whether or not this a positive face recognition events. These high confidence events then form the basis for generating reports as well as for triggering any user-defined action.

Users can access VAST Face through a web browser, which allows them to easily enroll and manage persons of interest, generate comprehensive reports, and define system actions. If multiple VAST Faces need to be administered, VIVOTEK FRSM server provides centralized management capabilities for such purposes.

Similarly, in the event that integration with external systems is required, VAST Face comes with a RESTful JSON API to allow 3rd party developers to build applications capable of receiving face recognition events or managing face profiles.

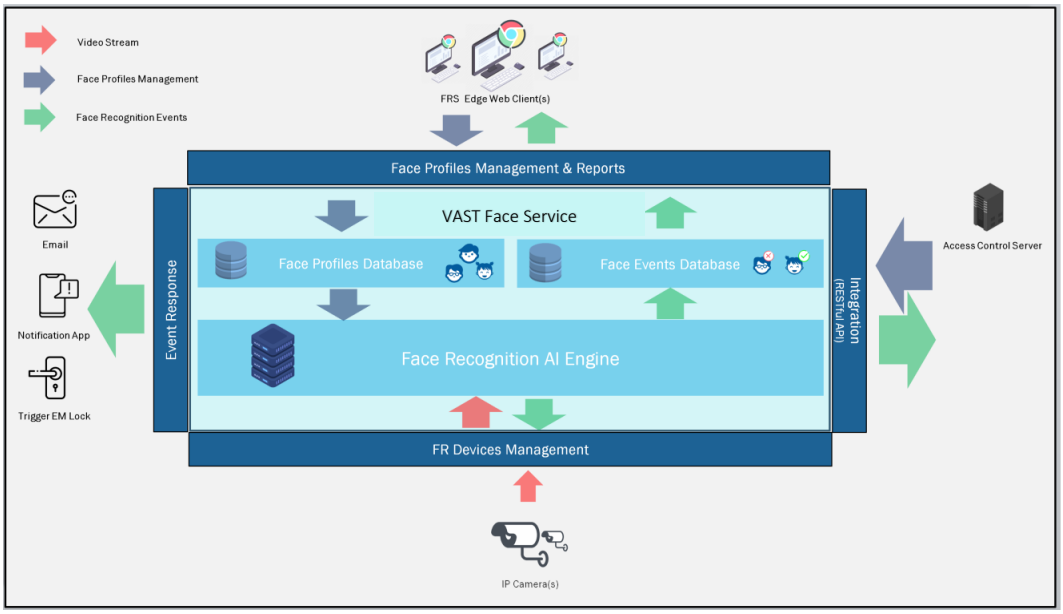


FIGURE 1.2 VAST Face system design.

1.2 System Architecture

VIVOTEK VAST Face is a docker container-based system that runs on Linux Ubuntu Server, it is worthwhile mentioning that VAST Face system is not a single service program, but a collection of dedicated components:

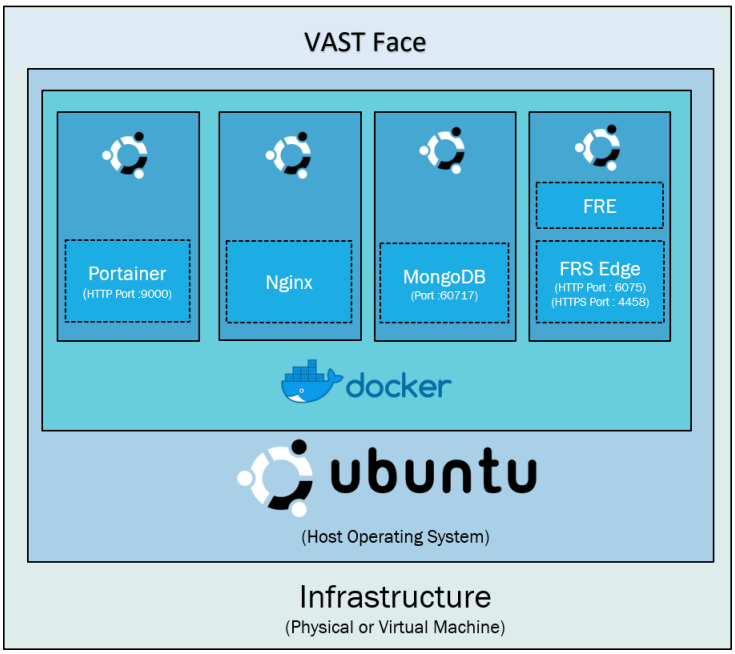


FIGURE 1.3 VAST Face system architecture.

System Component	Purpose
Linux Ubuntu OS	Operating system used for hosting docker and its containers
Docker	OS Level virtualization platform designed for running container-based applications.
Portainer Docker	Management UI used for Docker containers management
MongoDB	NO-SQL database engine used for storing enrolled person face profiles, face recognition events, logs, and system configurations
Nginx	Web Reverse proxy used for redirecting traffic from any of the underlying containers to a specific port / protocol
FRE	VIVOTEK's signature deep learning face Recognition A.I Engine
VAST Face	Main application server responsible for: • Hosting the face profiles database (photo image and other profile data) • Interfacing with AI Engine • Issuing face recognition reports • Triggering user defined actions based of face recognition events • Providing integration capabilities with external systems

Chapter 2

2. VAST Face Installation

This chapter describes how to install VIVOTEK VAST Face

2.1 VAST Face System Requirements

In order to ensure the system will run smoothly, below are the minimum Hardware and Software specs required for VAST Face system.

System Component	Minimum Specs
Quantity	• One PC / Server
Operating System	• Ubuntu 16.04 Server
CPU	• Intel Core i7 7th generation or newer, Xeon Silver, or equivalent (Min 4 vCPU if using virtual machines)
RAM	• Min 8 GB RAM
Operating System HDD	• Min 250 GB
Data HDD	• Min 500 GB
Network Interface Card	• Ethernet RJ45 100 Mbps
Display Resolution	• 1920 * 1080 pixels
Supported face recognition image sources	• IP Camera: Generic RTSP / ONVIF H.264 IP Camera • Face Recognition Tablet: Tigerwong and Smarf ID with VIVOTEK Face ID App

Note

- VIVOTEK VAST Face uses CPU power to analyze and verify face images, as a rule of thumb, it is recommended to allocate 1 CPU Core and 2GB RAM per connected face recognition device (IP camera or FR Tablet)

2.2 Register License

When VAST Face is installed and opened for the first time, you need to register the VAST Face license key and the engine license key. After the key is activated, you can use the System Admin account and the default password to log in to the system and start using the VAST Face system.

2.2.1 VAST Face License

1. After the installation of VAST Face is complete, open the Google Chrome browser on the Windows PC, and then navigate to the VAST Face IP address, port 6075 (e.g.: http://192.168.1.152:6075), VAST Face license registration page will be displayed.

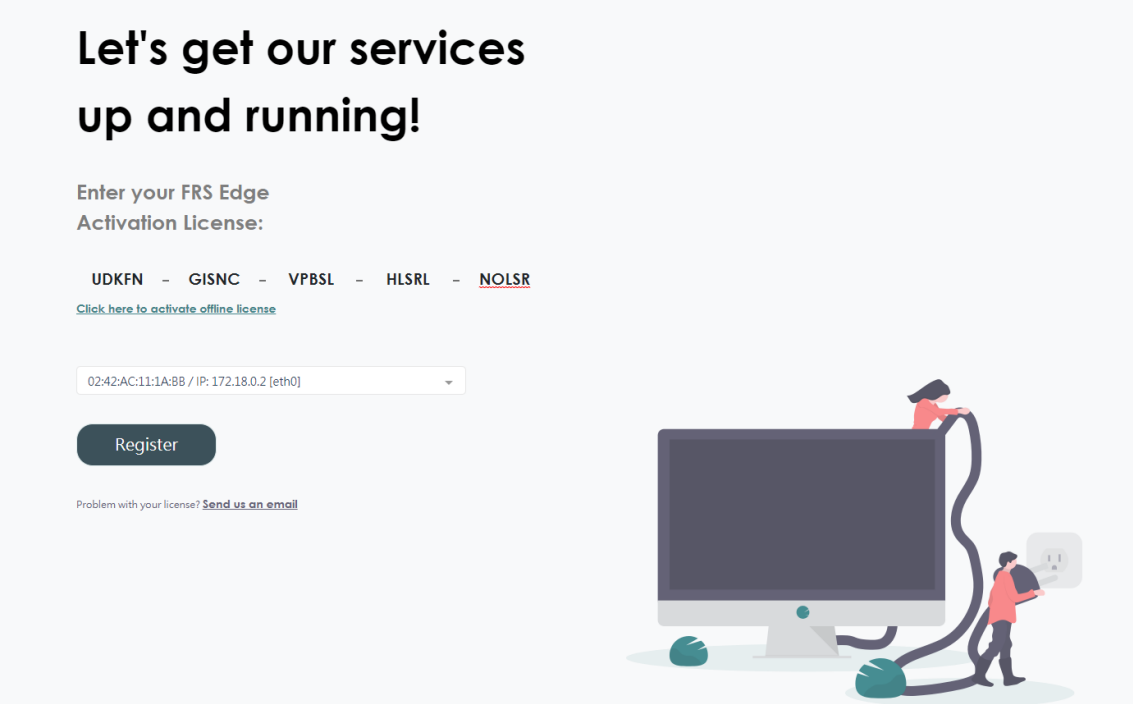
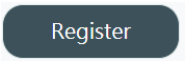


FIGURE 2.1 Register VAST Face license

2. Enter the VAST Face License Key and MAC address.

3. Click the "Register" button to activate the license key. ()

4. The pop-up window shows that the license registration is successful and prompts that the engine license key needs to be registered.

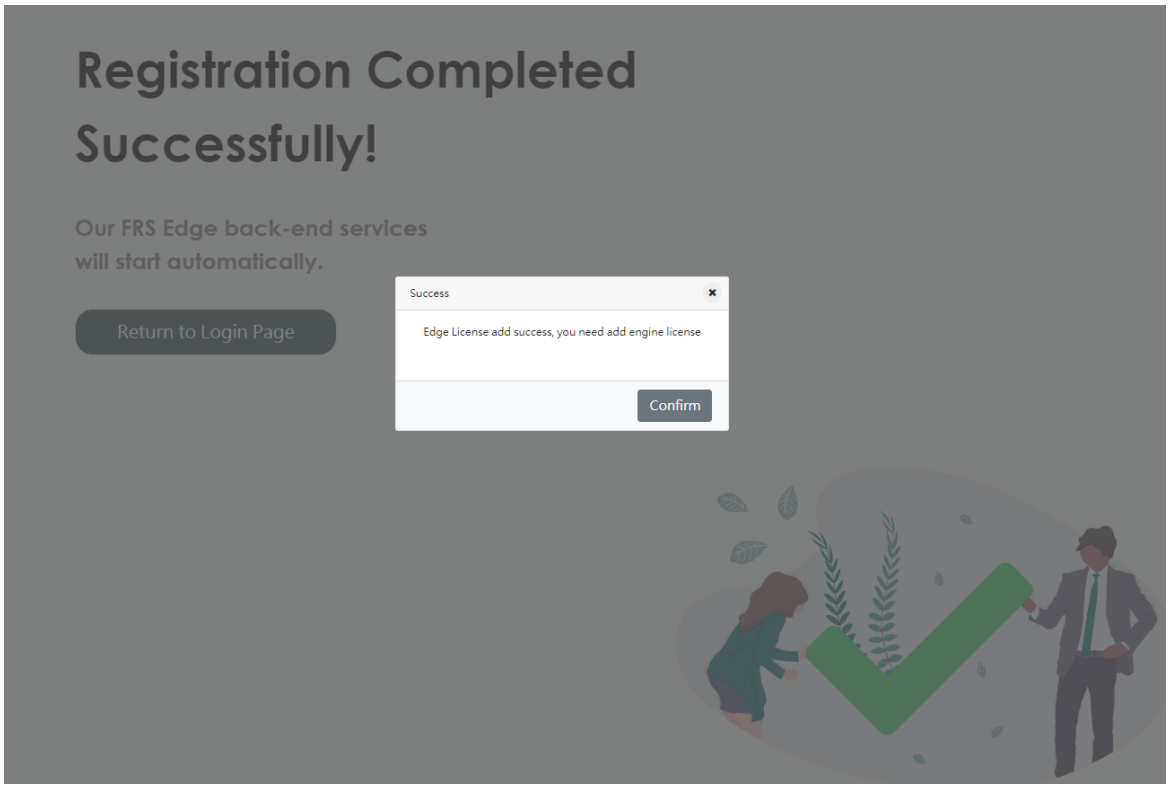


FIGURE 2.2 Register VAST Face license success

2.2.2 FRS Engine License

5. Click "Confirm" to display the engine license key registration page

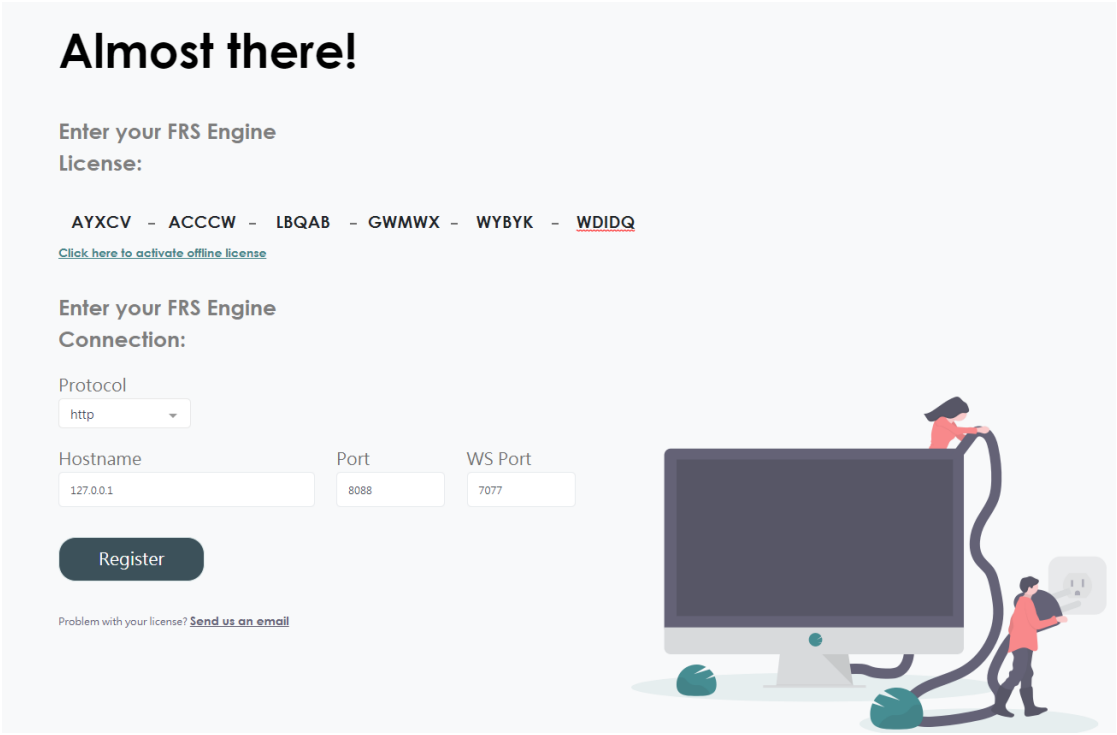


FIGURE 2.3 Register FRS Engine license

6. Enter register information:
    a. Engine License Key
    b. Protocol
    c. Hostname
    d. Port
    e. WS Port
7. Click the "Register" button to activate the license key.
8. Pop up window shows that license registration is successful.

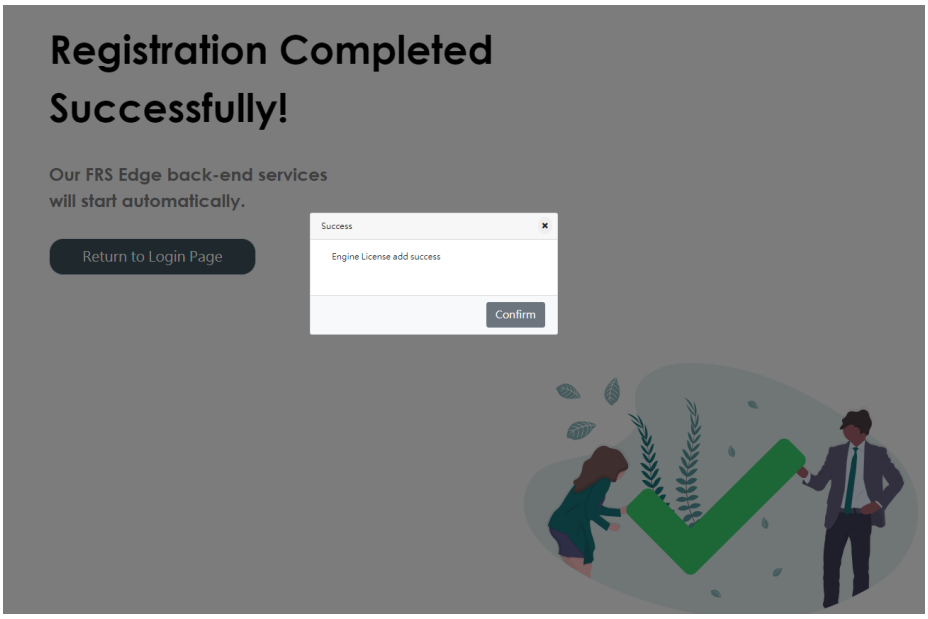


FIGURE 2.4 Register FRS Engine license success

9. Click "Confirm" to enter the system login page.

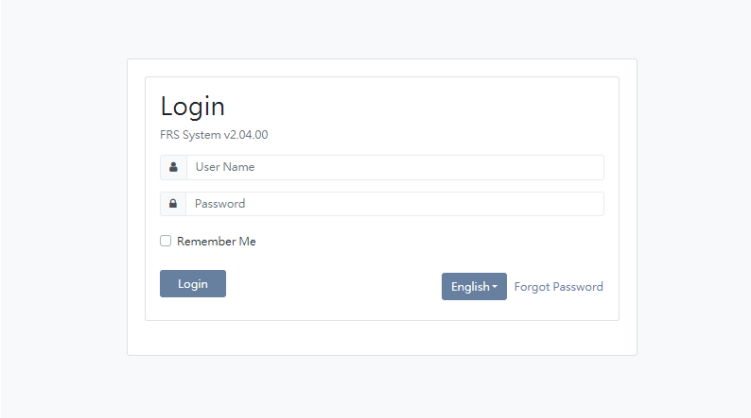


Figure 2.5 VAST Face login page

2.3 Camera Installation

VAST Face is capable of supporting virtually any IP camera brand with H.264 video streams, however, in order to effectively capture and accurately analyze all passersby faces, cameras must be able to produce a clear face image, as such, it is vitally important that they are mounted and configured properly. Some technical considerations include but are not limited to:

- Cameras must be mounted within a 15 degrees or less tilting angle, so that complete faces can be captured, important face features such as eyes, nose and mouth must not be occluded.
- While there's no specific camera resolution or focal length required, cameras must be mounted at a distance away from the target area such that they can produce a clear and visible face image, with a minimum size of 200 x 200 pixels for face recognition, or 100 x 100 for face detection
- Cameras must use a minimum shutter speed of 1/60 to prevent motion blur
- Cameras must be installed at locations with a minimum 200 Lux. Good constant and even illumination is always preferred, whenever possible locations with backlights or shadows must be avoided.

The below diagram depicts a typical camera installation. Under this scenario, the camera will be able to recognize faces at a distance for up to three meters

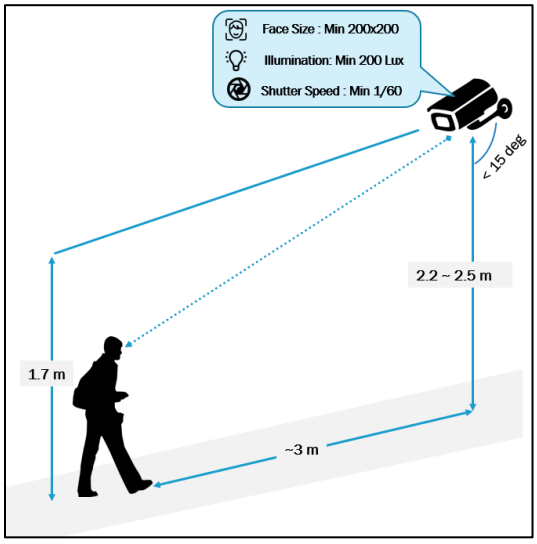


FIGURE 2.6 Typical face recognition camera installation.

Note

- For face recognition tablets, please make sure that the faces are captured at an eye-level height, and at a distance of no more than 1 meter away from the image capturing device.

2.4 Face Profile Images

Just as important as it is properly mounting video sources for face recognition, the registered photos (aka golden samples) inside the faces database must also be as clear as possible. In general, it is recommended that the database image should minimally comply to the requirements for Passport images as specified by the International Civil Aviation Organization (ICAO). The ICAO Image requirements covers pose, illumination, image brightness, contrast color, etc.

Some technical considerations before enrolling a photo into the faces database, include but are not limited to:

- Face must be centered and show full face with eyes open.
- Avoid any shadows or reflections on face (or behind), neither the image must be overexposed / underexposed.
- Use natural expressions, and avoid wearing sunglasses or any caps.
- Image must show correct face aspect (not enlarged or stretched).
- Image must not be pixilated or show unnatural skin tones.

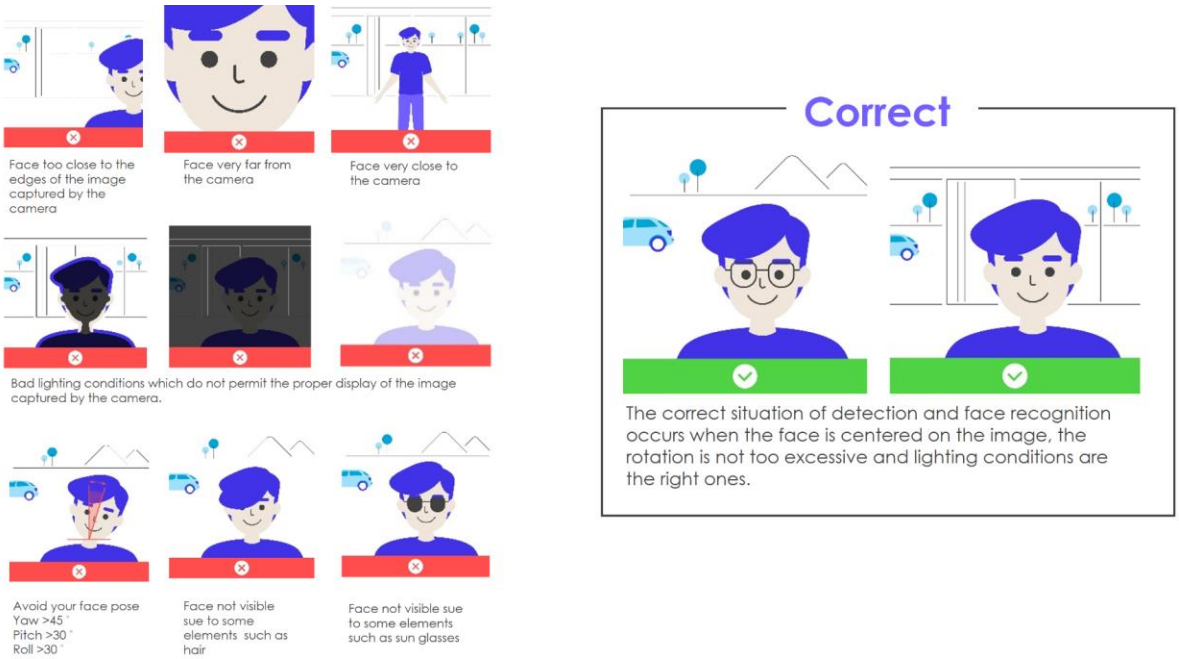


FIGURE 2.7 Good and bad examples for face profile photos.

Note

- Images must be in .PNG, .JPG or .JPEG format with a file size not greater than 1MB
- The enrolled photo must have a face size of at least 200 * 200 pixels

Chapter 3

3 VAST Face Operation

This chapter describes how to operate VAST Face for daily operations.

3.1 FRS Server General Operation

VAST Face allows users to effectively manage multiple video devices used for facial recognition. Supported video sources include: IP cameras, specialized face recognition tablets running signature face recognition app.

Moreover, VAST Face acts as a centralized face profiles repository in which users can enroll a person of interest by attaching a face photo and the person's particulars. In order to improve data sense making, face profiles can be assigned to one or multiple face groups. Similarly, VAST Face provides a reporting platform where users can verify face recognition events in real time, or query historical data.

For unattended system deployments, operators can configure VAST Face to trigger automated actions upon identifying a specific profile or a group member. Likewise, in the event that integration with external systems is required, a software development kit (SDK) is readily available.

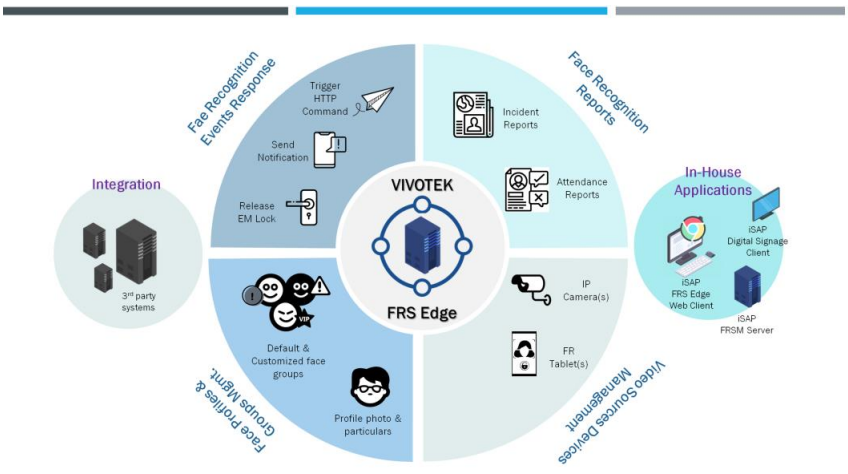


FIGURE 3.1 VAST Face core features.

3.1.1 Change User Account Password

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed ,login using the assigned credentials.

2. Click on the Avatar icon ( ), located on the top right corner, to display the user's profile information.

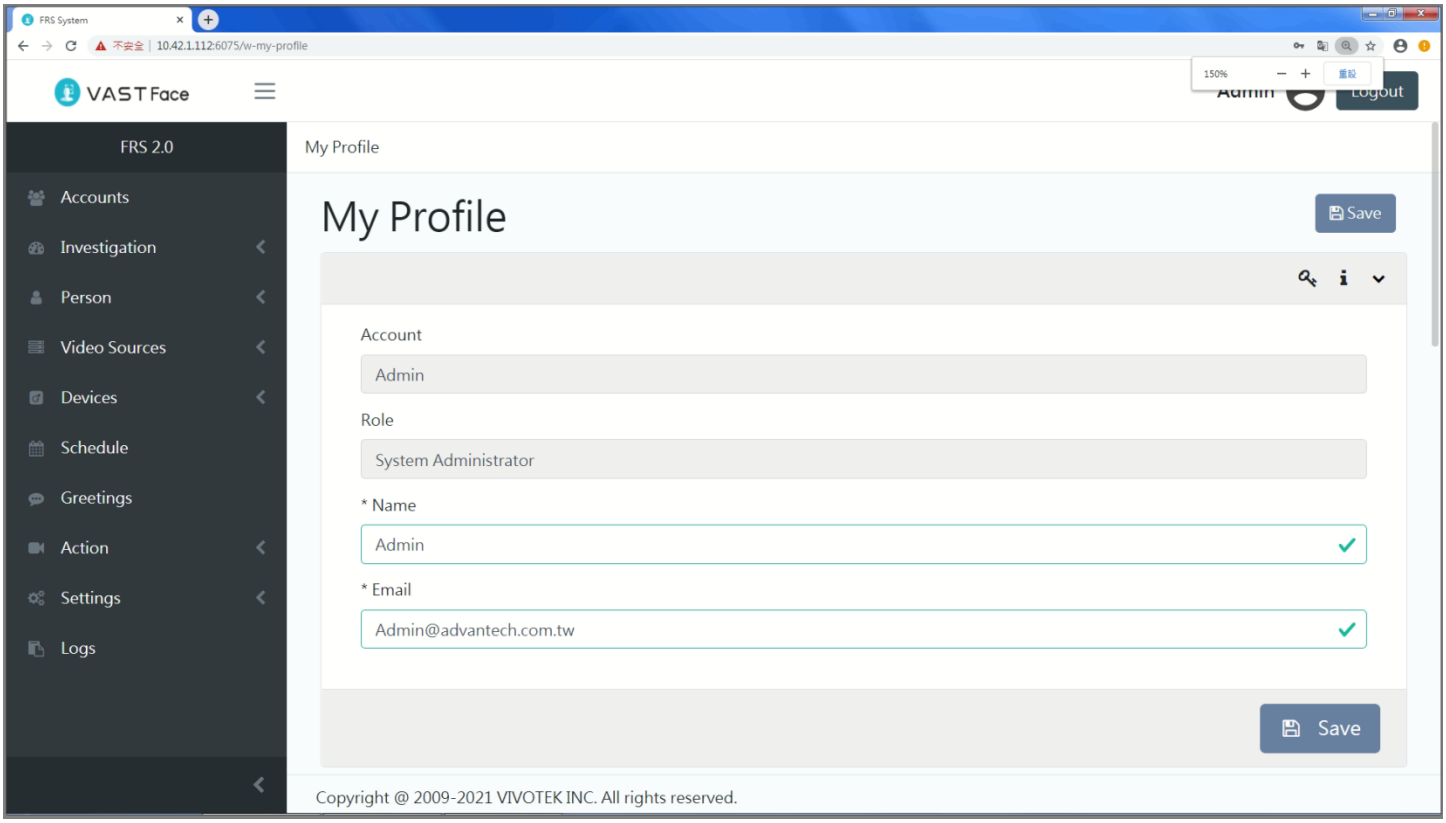


FIGURE 3.2 VAST Face user profile settings

3. Click on Change Password icon, which is identified by a key( )

4. Enter the username's current password, the new password, and confirm the new password.

5. Click on "Save" to apply changes.

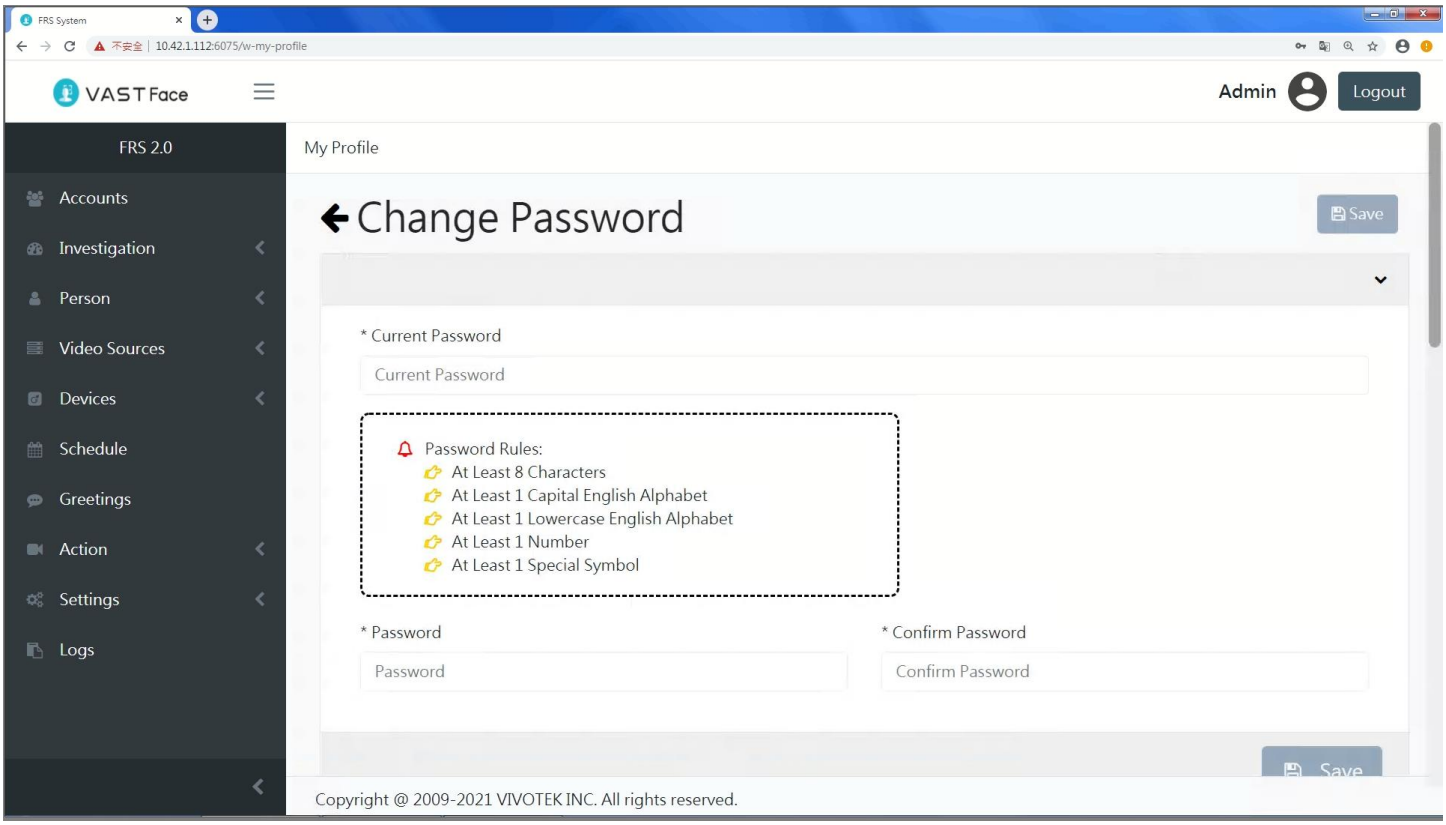


FIGURE 3.3 VAST Face update password settings.

6. Login to VAST Face using the new password.

3.1.2 Account Management (System Admin Only)

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an System Admin account.

3. Navigate to "Account Management" menu ➡ A list of all created user account will be displayed.

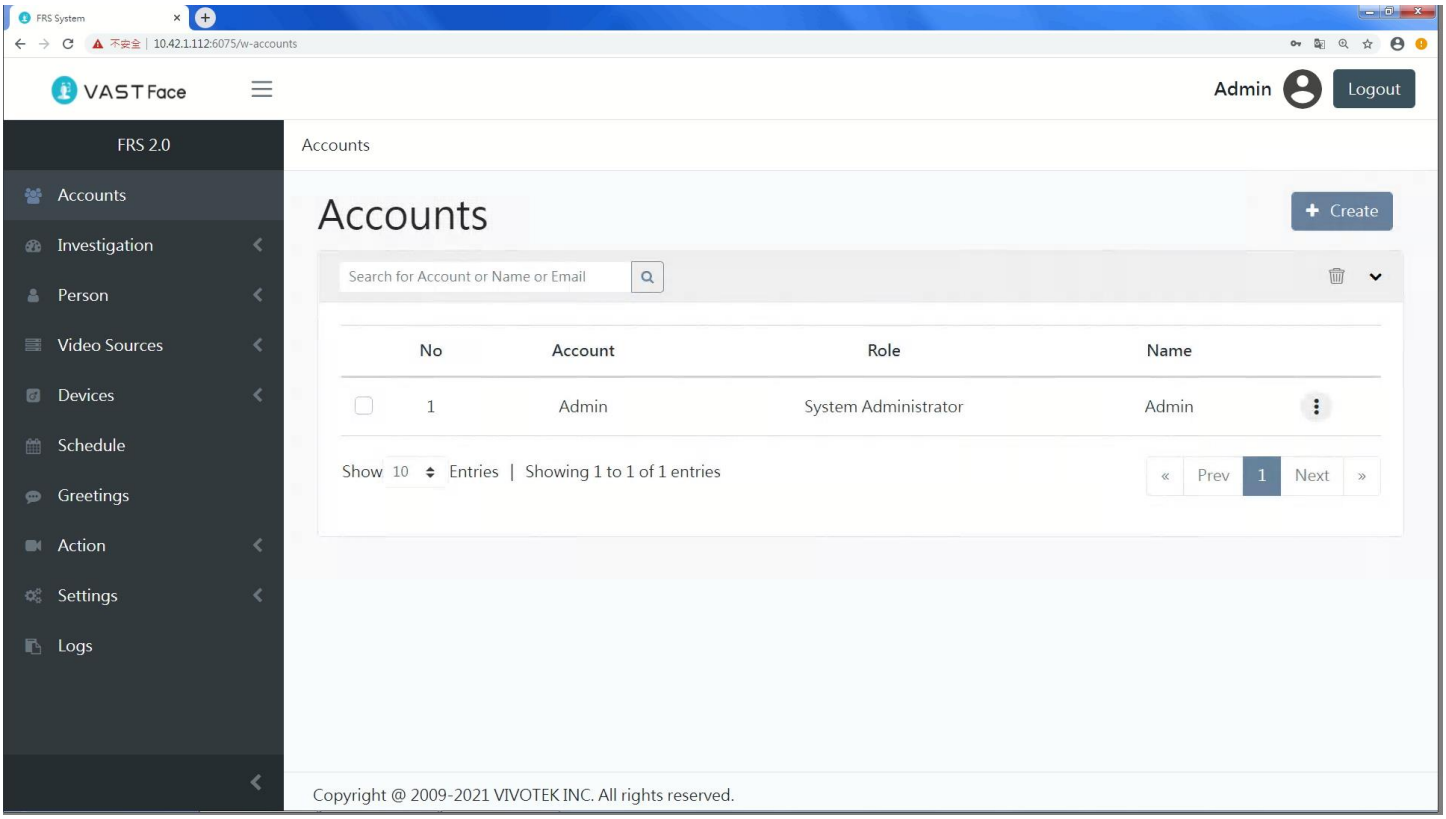


FIGURE 3.4 VAST Face Account management

4. Use the Display filters to narrow down results by: account, name or email.
5. Click on the search button ( )button, to display only profiles matching the filter criteria.
6. In order to see a account complete details, click on the "Profile Details" icon ( ), and select Edit, the selected profile full details will be displayed.
7. Edit any account information as needed.

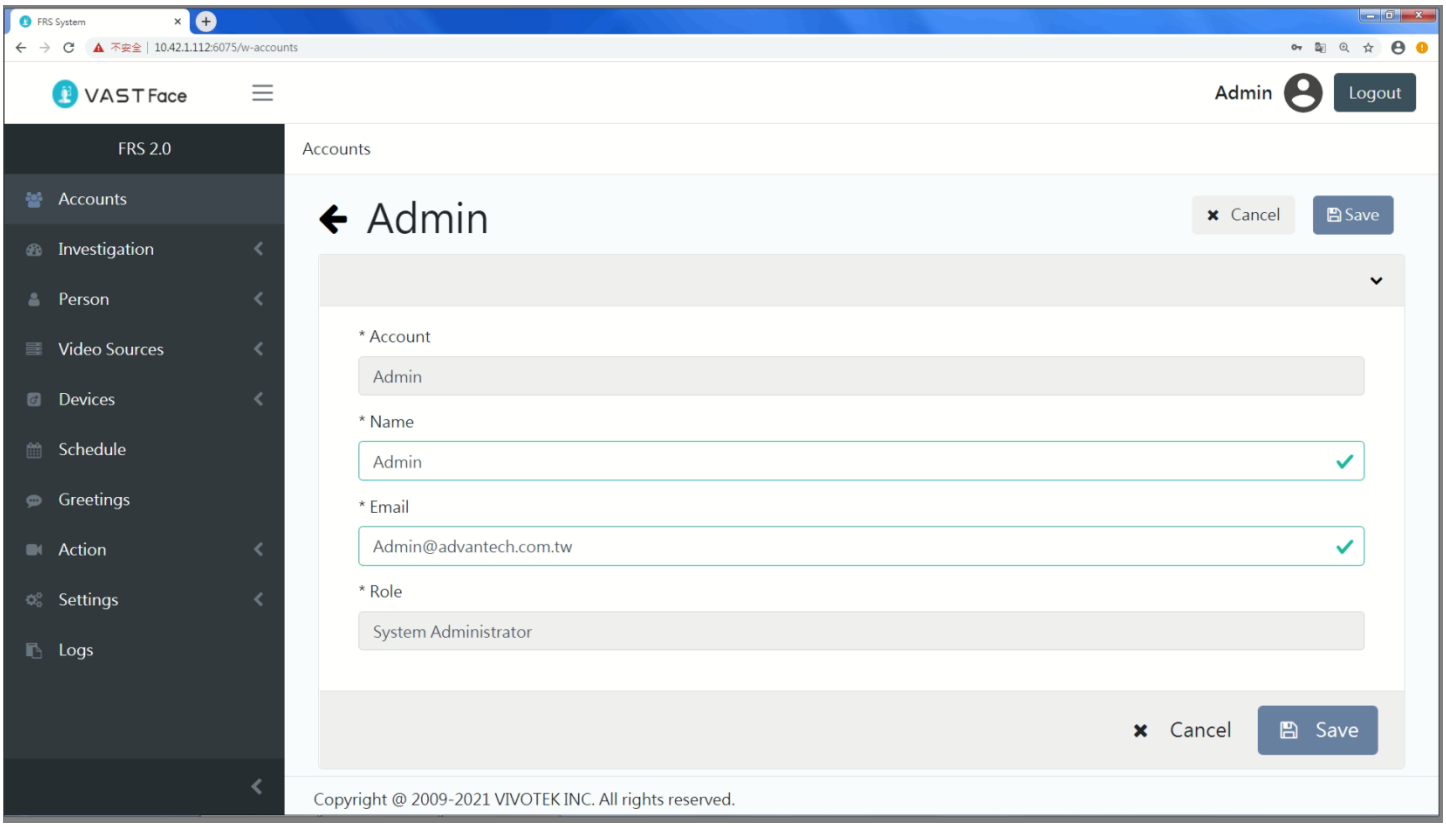


FIGURE 3.5 VAST Face Account details

8. Click on "Save" to apply changes.

9. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

10. A pop-up window will appear on-screen prompting the user to confirm the action.

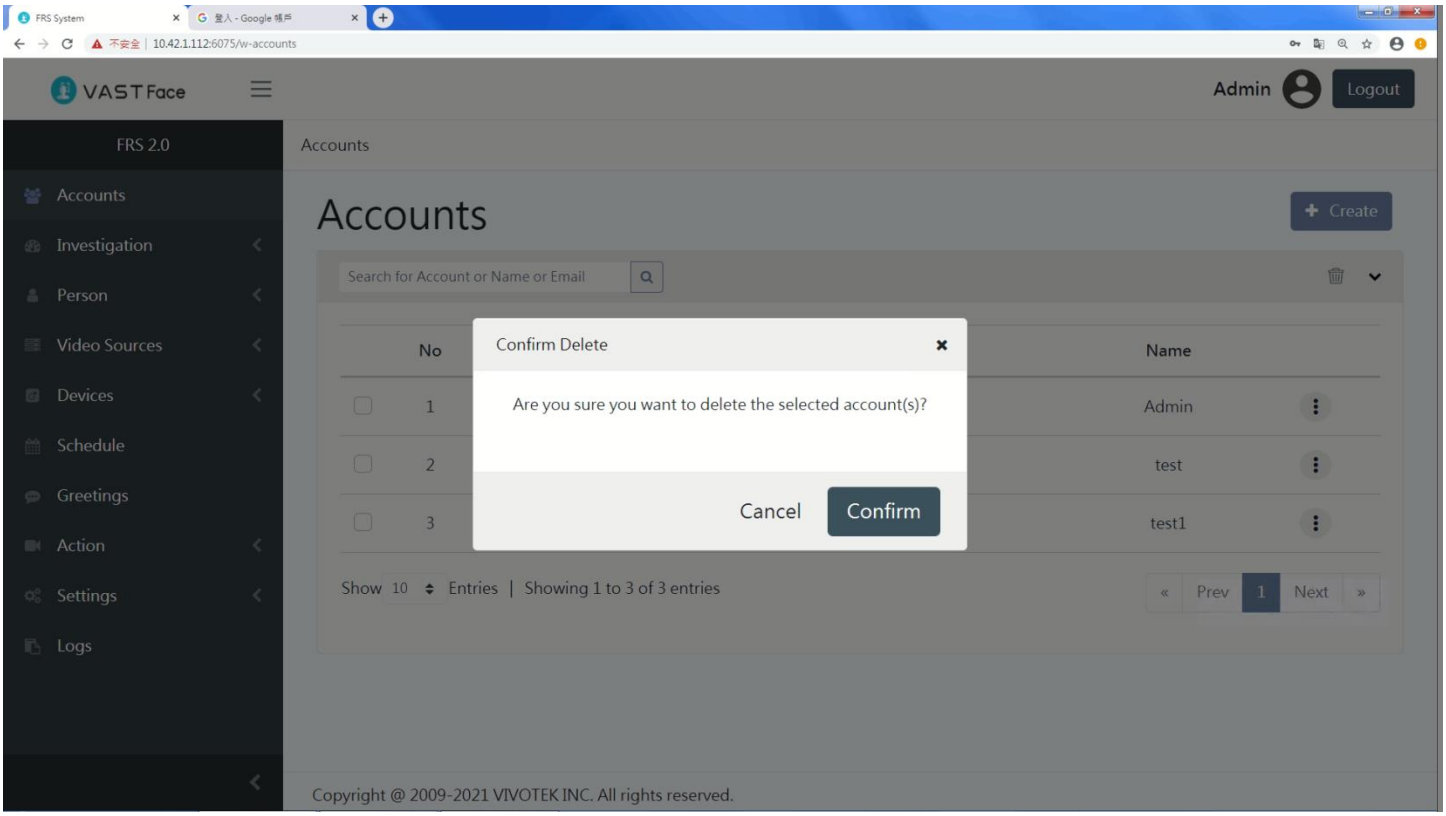


FIGURE 3.6 VAST Face delete face profile

11. Click on "Confirm" to delete the selected account(s).

12. To add a new account, click on the "+Create" button (+ Create).

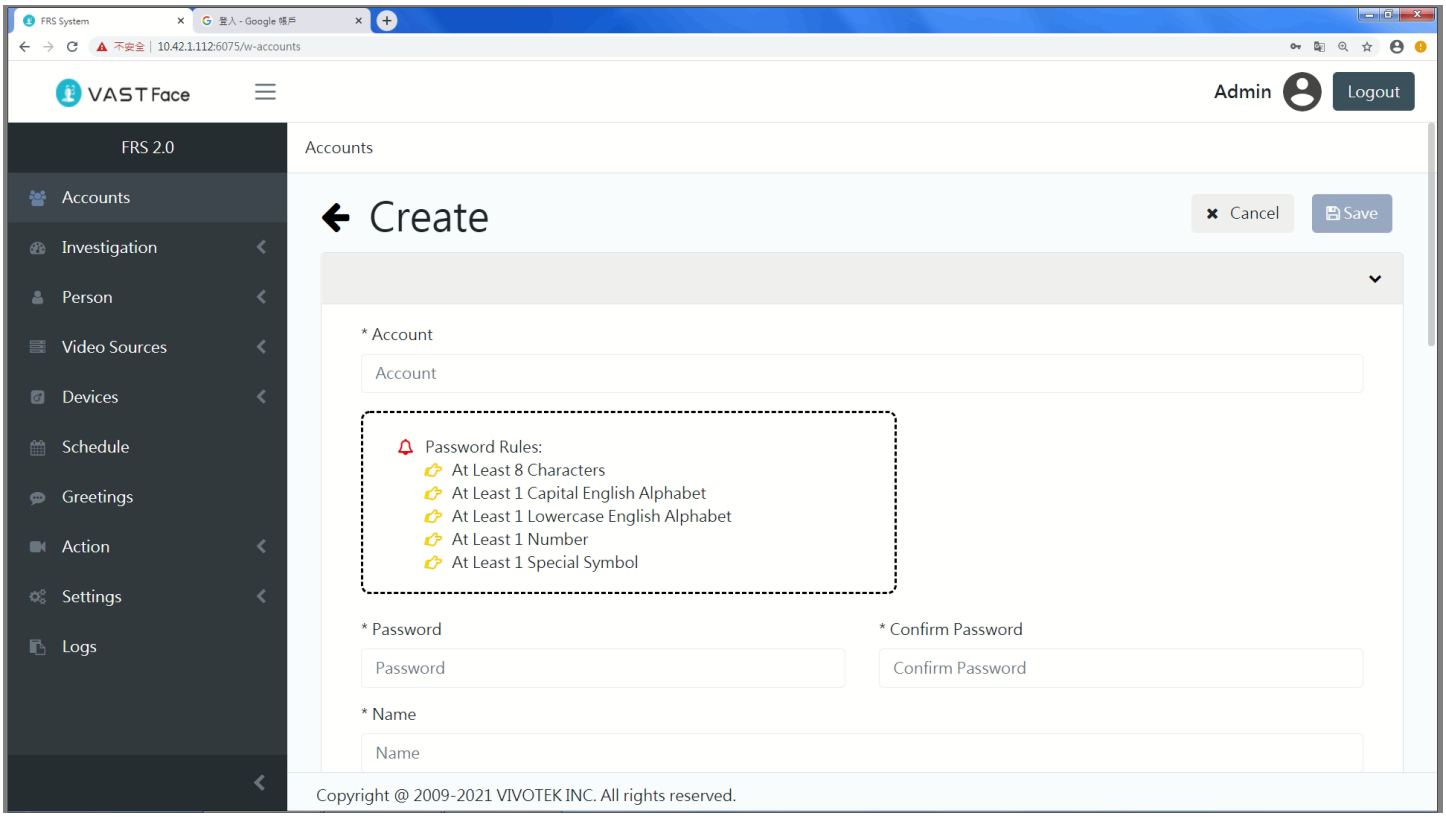


FIGURE 3.7 VAST Face create account

13. On the "Create account" menu, enter the new account information:
    a. **Account** ➡ User account
    b. **Password** ➡ User password
    c. Confirm Password ➡ Confirm again user password
    d. Name ➡ User name
    e. Email ➡ User's Email, if forgot the password need to use that email to account verify
    f. Role ➡ User role (access to platform functions)
14. Click on "Save" to create the Account.

3.2 Face Profiles Database

3.2.1 Face Profiles Management

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Person" menu ➡ "Person List", a list of all enrolled face profiles will be displayed.

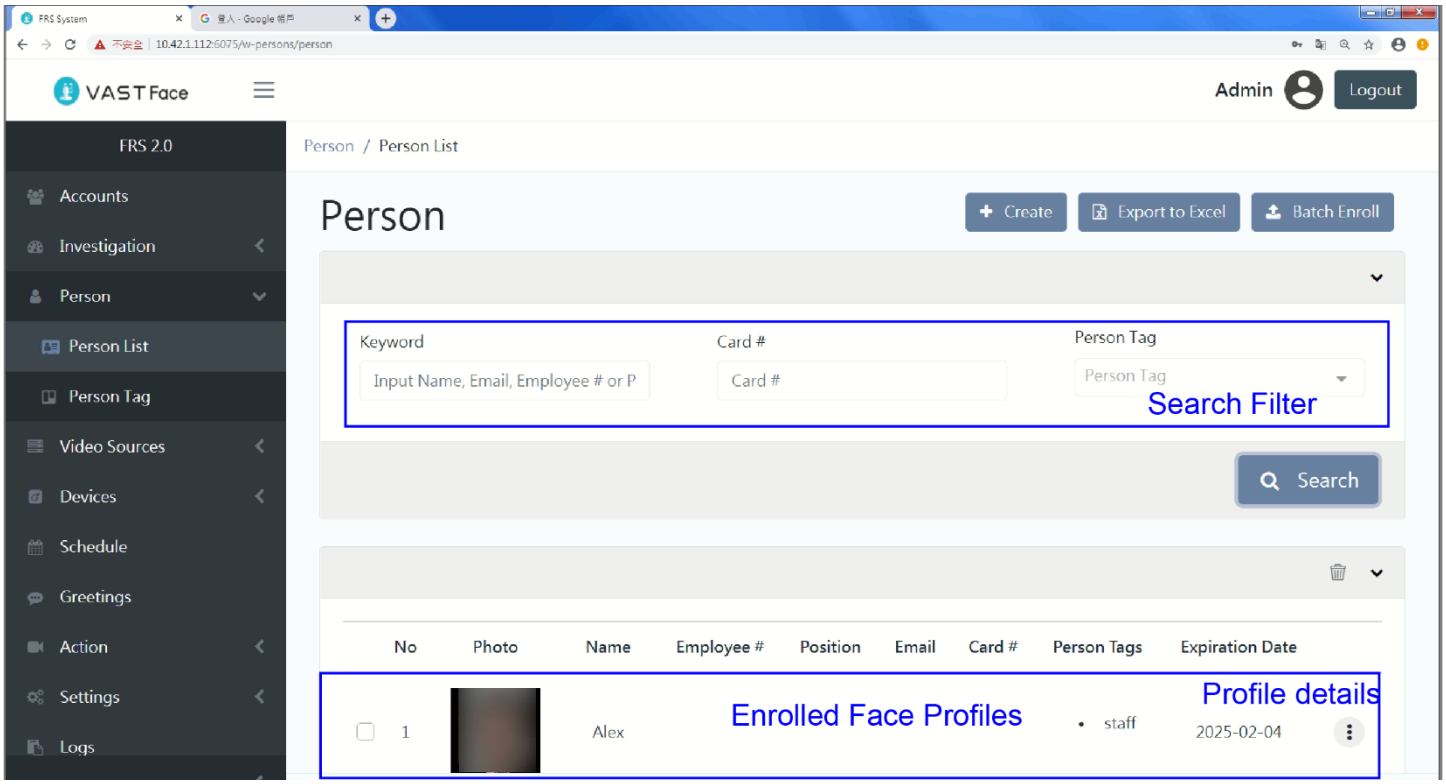


FIGURE 3.8 VAST Face enrolled face profiles

4. Use the Display filters to narrow down results by: name, email, employee #, or face groups.

5. Click on the search button ( )button, to display only profiles matching the filter criteria.

6. In order to see a face profile complete details, click on the "Profile Details" icon ( ), and select Edit, the selected profile full details will be displayed.

7. Edit any profile information as needed.

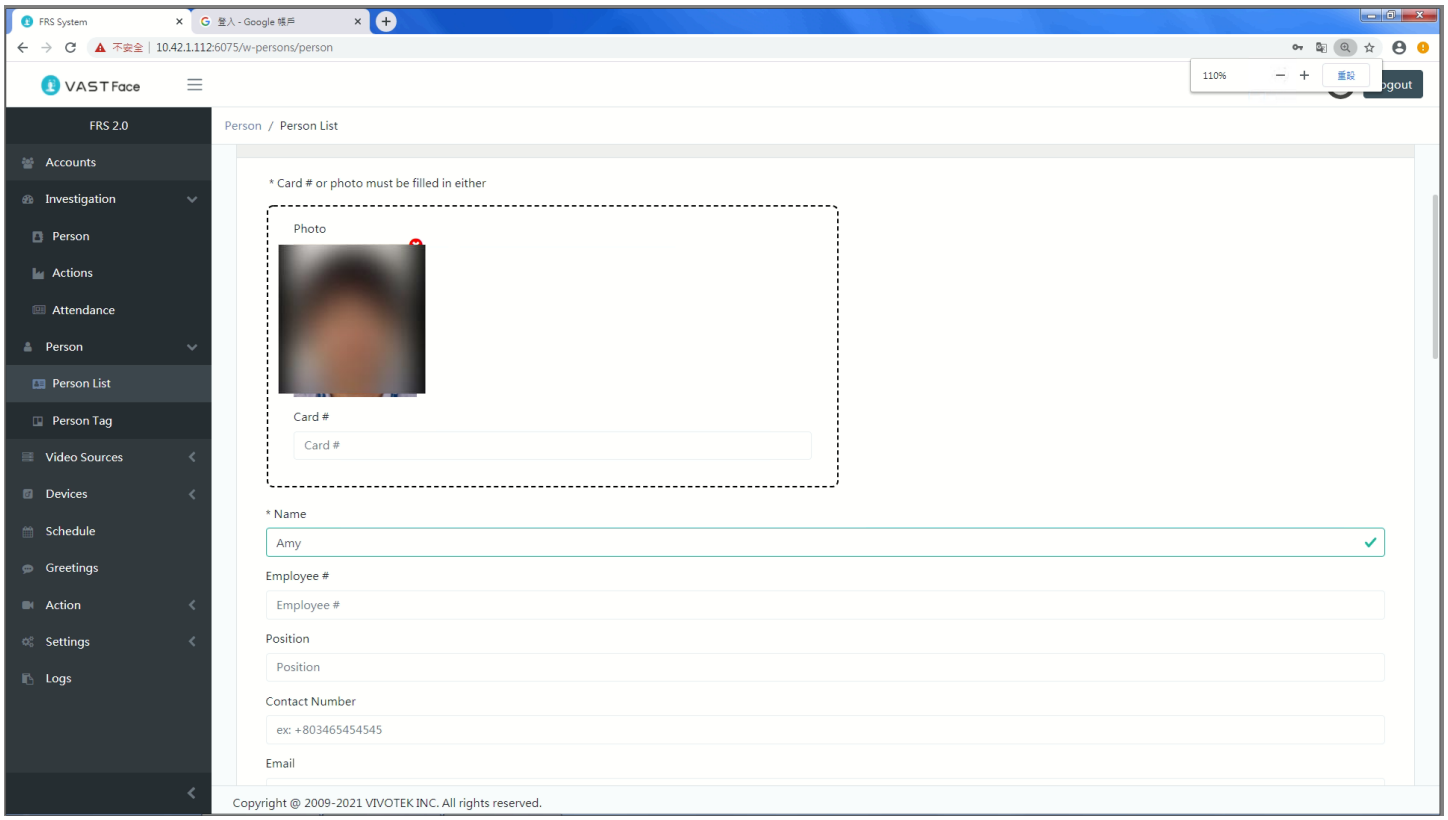


FIGURE 3.9 VAST Face enrolled person profile with full details

8. Click on "Save" to apply changes.

9. To Delete a profile, click on the "Profile Details" icon ( ), and select Delete (Delete).

10. A pop-up window will appear on-screen prompting the user to confirm the action.

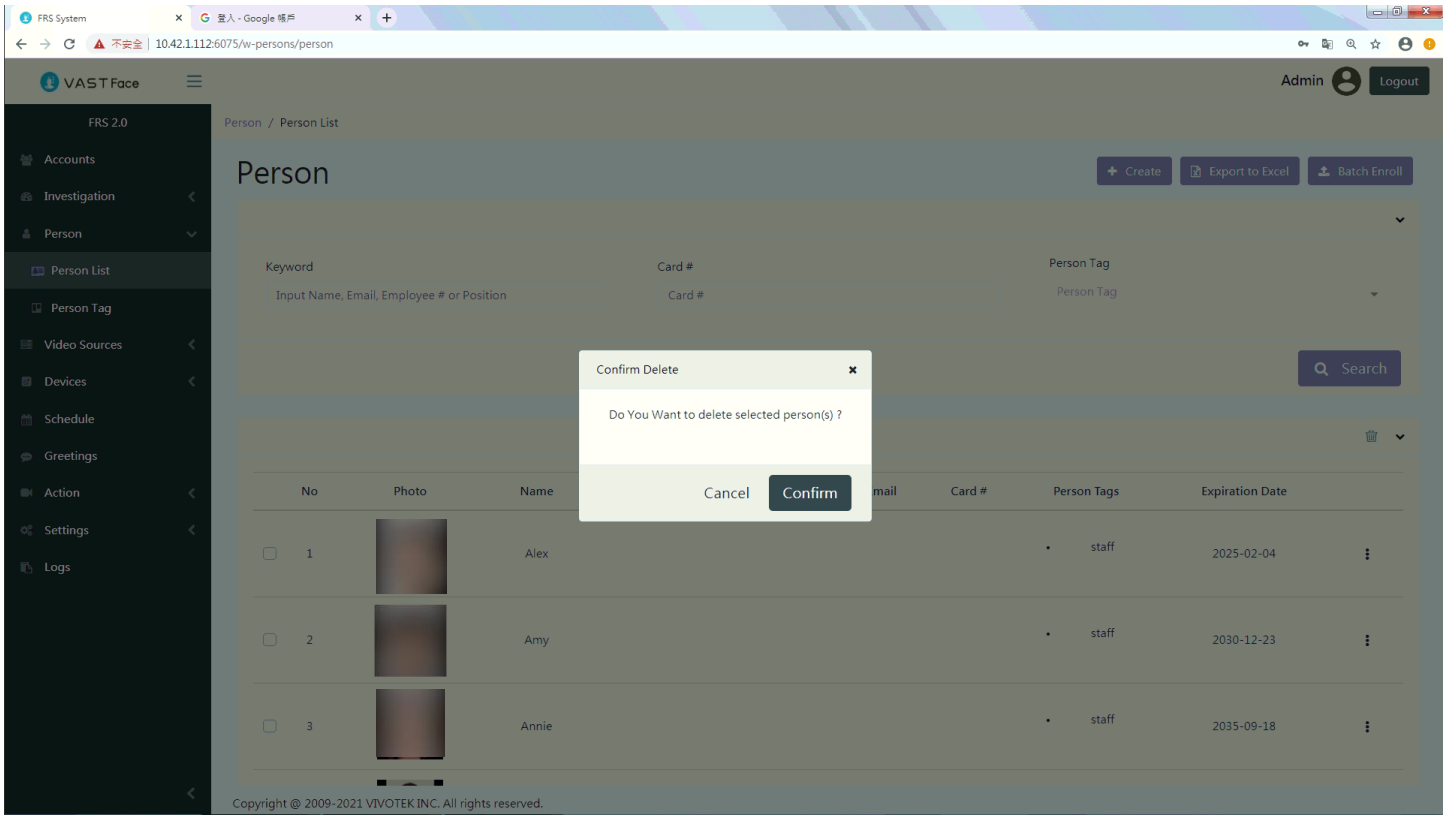
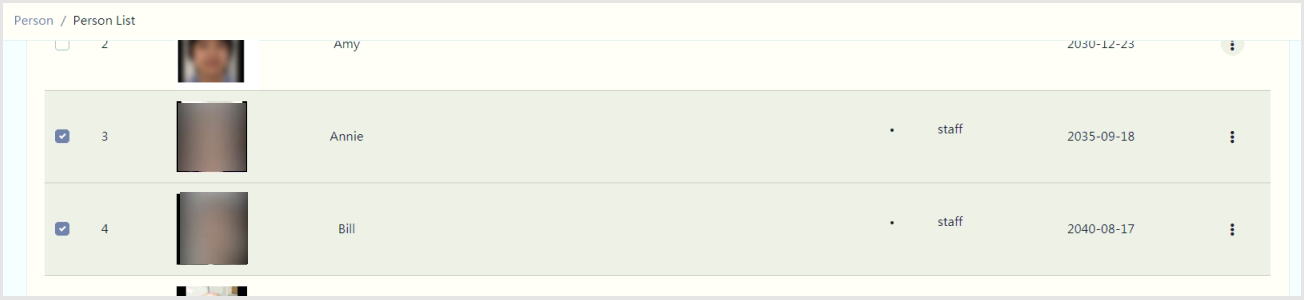


FIGURE 3.10 VAST Face delete face profile

11. Click on "Confirm" to delete the selected face profile(s).

Note

- If more than one face profile needs to be deleted at a time, click on the leftmost column (next to Number), tick to select the profiles, and click on the delete icon ( )



12. To add a new profile, click on the "+Create" button (+ Create).

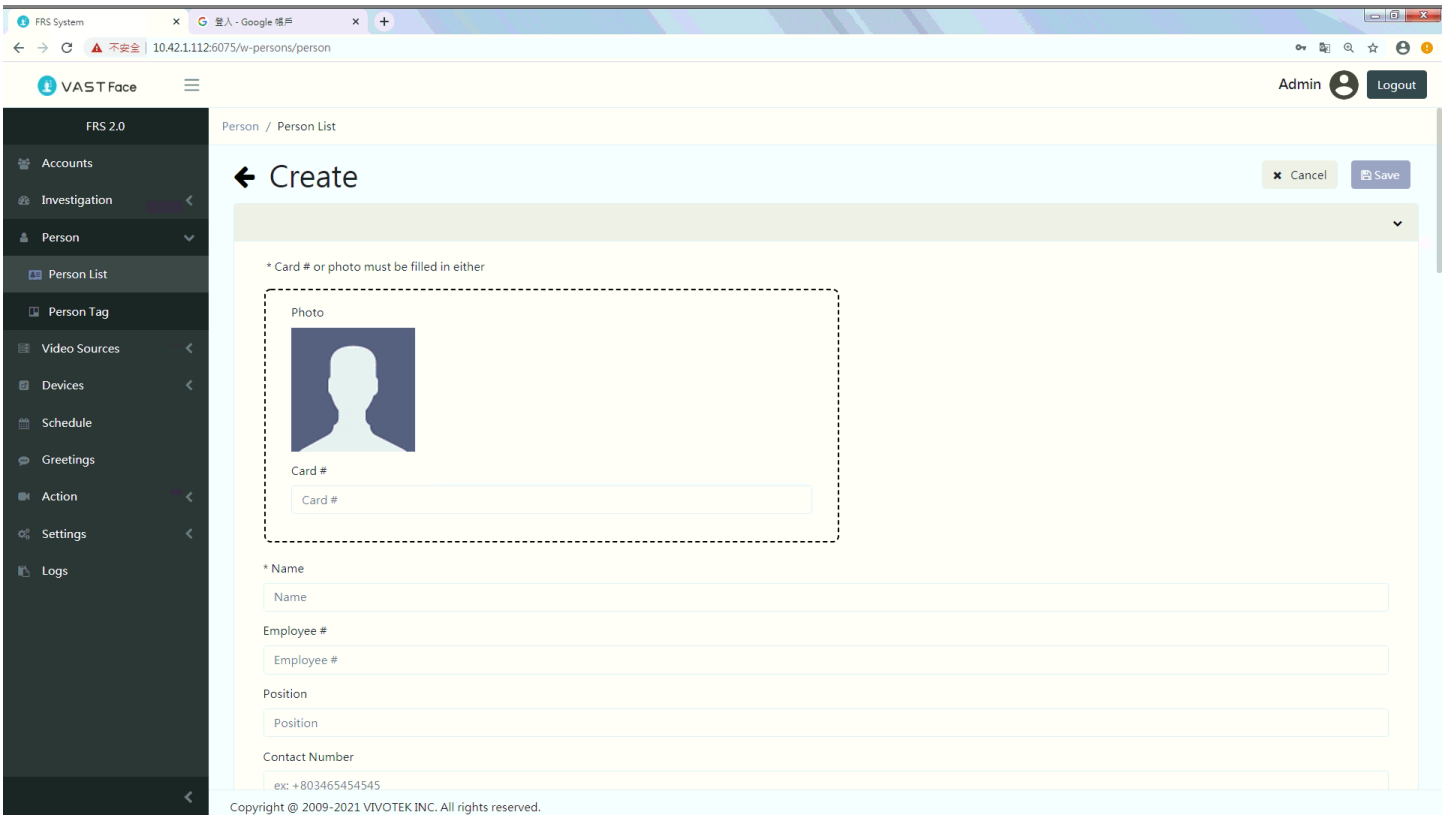


FIGURE 3.11 VAST Face create face profile

13. On the "Create profile" menu, enter the new profile information:

    a. **Photo** ➡ Profile photo image used for face recognition (selected image must be .PNG, .JPG or .JPEG and must be less than 1 MB).

    b. **Name** ➡ Person's name.

    c. Employee # ➡ (Optional).

    d. Position ➡ (Optional).

    e. Contact Number ➡ (Optional).

    f. Email ➡ (Optional).

    g. Card # ➡ (Optional) Virtual card number that is to be assigned to this face profile. In the event that no ACS system is linked to VAST Face, it's recommended to let the system auto-assign this number, else, users should input the Wiegand card # assigned to this profile under the 3rd party Access control system (ACS).

    h. Person Group ➡ (Optional) Face group(s) to which the enrolled person will be a member of.

    i. Remarks ➡ (Optional).

j. **Expiration Date** ➡ Last approved day for the enrolled person to be able to authenticate at VAST Face, upon reaching this expiration date, the profile will be auto-deleted from the system.

14. Click on "Save" to create the profile.

3.2.2 Bulk Enrollment

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Person" menu ➡ "Person List", a list of all enrolled face profiles will be displayed.

4. Click on the "Batch Enroll" button (Batch Enroll), the bulk enrollment page will be displayed.

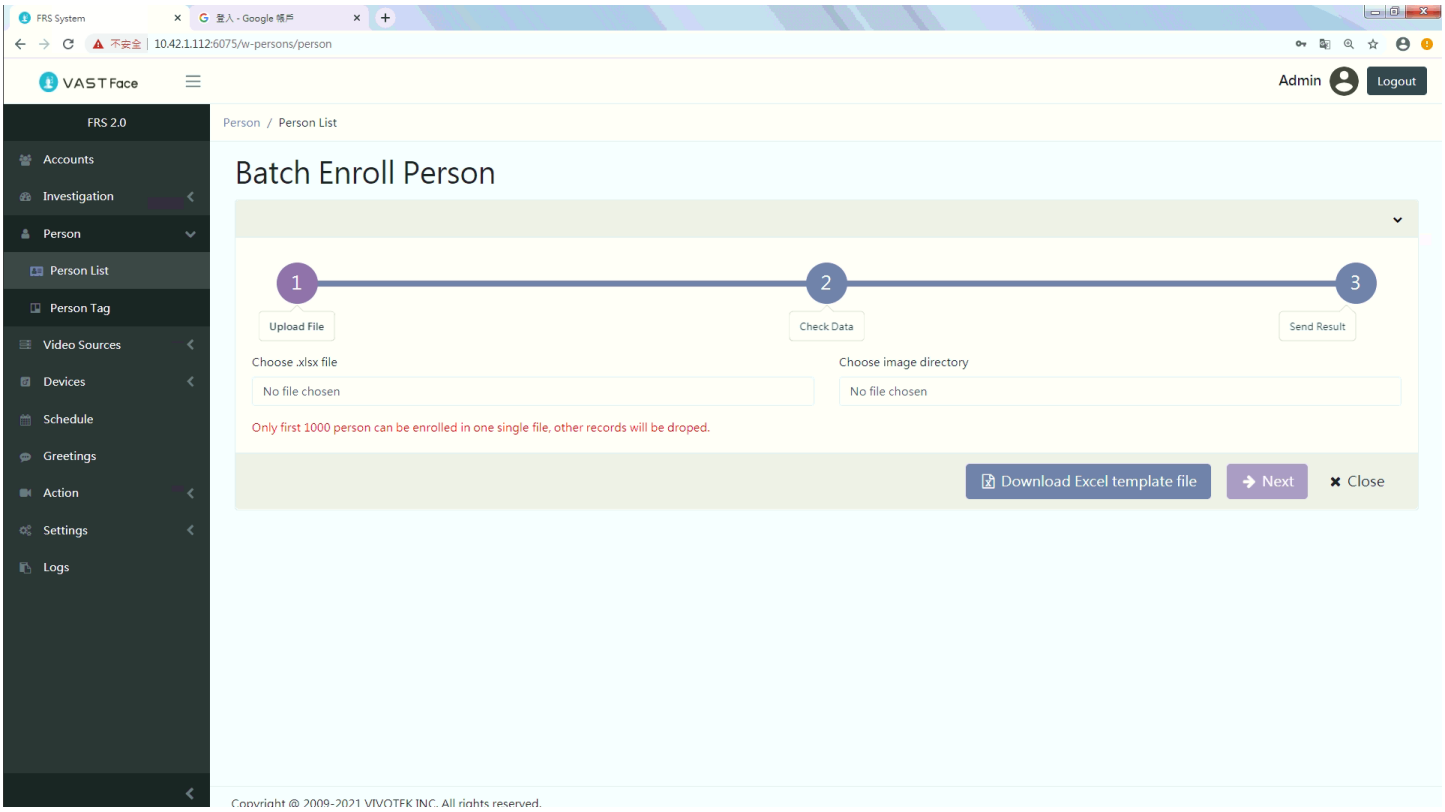
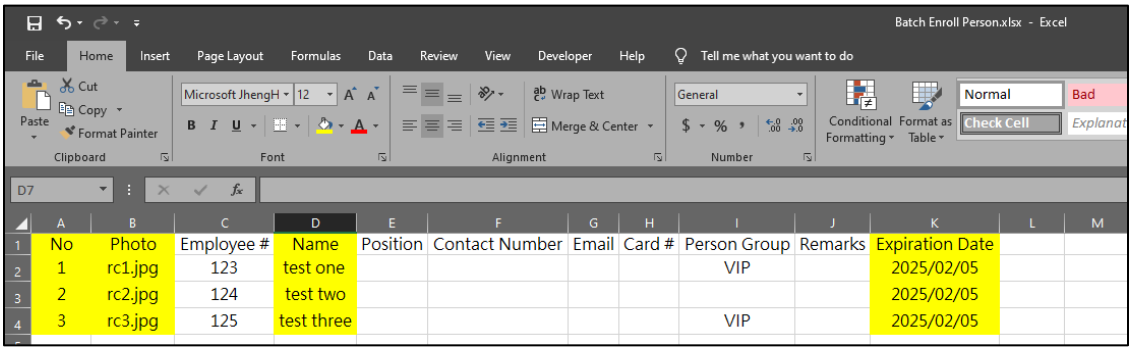


FIGURE 3.12 VAST Face bulk enrollment page

5. Click on the "Download Excel template file".

6. On a PC with Microsoft Excel, open the template file, edit it as needed, and save all changes.



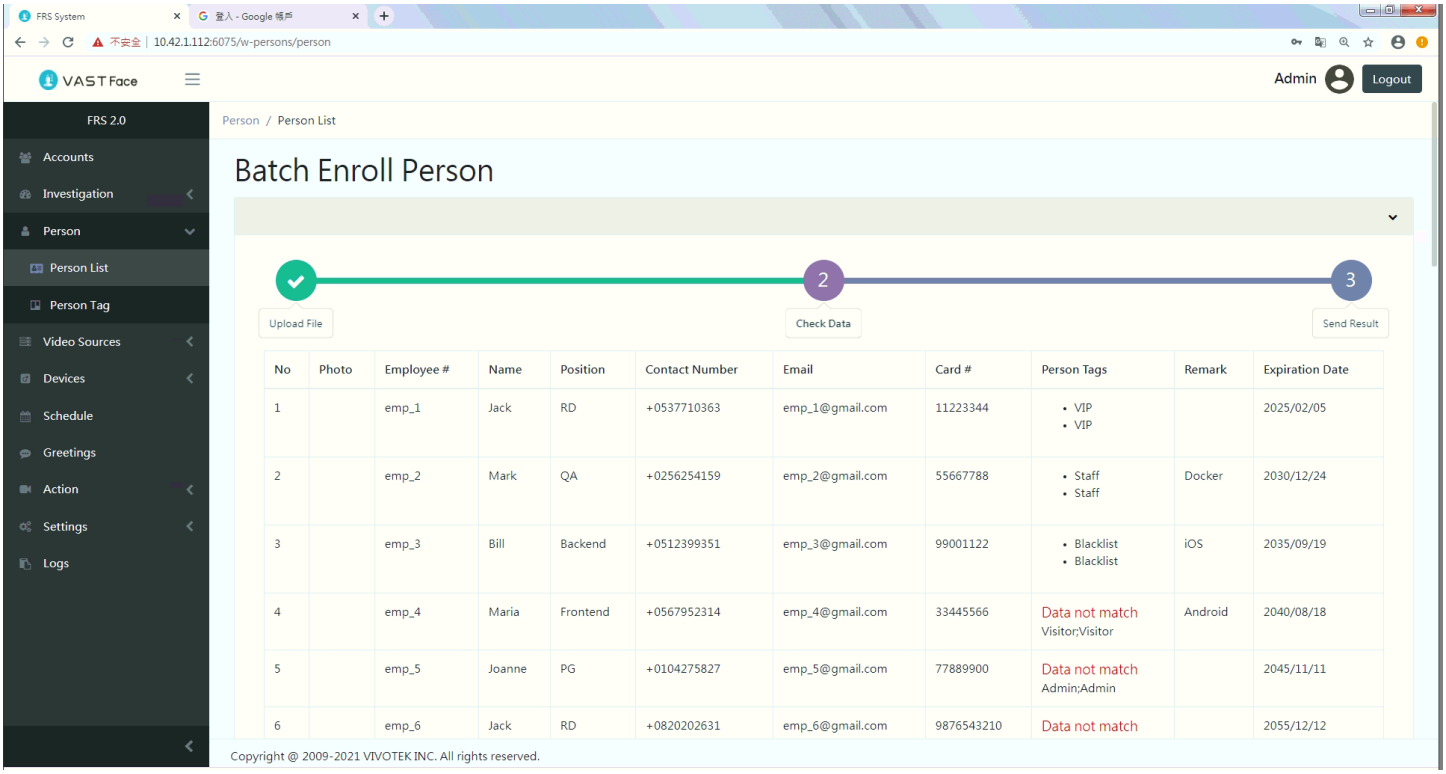
No	Photo	Employee #	Name	Position	Contact Number	Email	Card #	Person Group	Remarks	Expiration Date
1	rc1.jpg	123	test one					VIP		2025/02/05
2	rc2.jpg	124	test two							2025/02/05
3	rc3.jpg	125	test three					VIP		2025/02/05

FIGURE 3.13 VAST Face bulk enrollment template file (mandatory fields are highlighted in yellow)

7. Back on VAST Face, click on the "Choose .xlsx file textbox", and browse to select the excel file containing the new profiles' information.

8. Click on the "Choose image directory textbox", and browse to select the working directory folder where the profiles' photo images are located.

9. In the event that the file has some data validation errors, VAST Face will highlight the cells whose data needs to be revised, please note that all errors must be corrected before the profiles can be created.



No	Photo	Employee #	Name	Position	Contact Number	Email	Card #	Person Tags	Remark	Expiration Date
1		emp_1	Jack	RD	+0537710363	emp_1@gmail.com	11223344	• VIP • VIP		2025/02/05
2		emp_2	Mark	QA	+0256254159	emp_2@gmail.com	55667788	• Staff • Staff	Docker	2030/12/24
3		emp_3	Bill	Backend	+0512399351	emp_3@gmail.com	99001122	• Blacklist • Blacklist	iOS	2035/09/19
4		emp_4	Maria	Frontend	+0567952314	emp_4@gmail.com	33445566	Data not match Visitor;Visitor	Android	2040/08/18
5		emp_5	Joanne	PG	+0104275827	emp_5@gmail.com	77889900	Data not match Admin;Admin		2045/11/11
6		emp_6	Jack	RD	+0820202631	emp_6@gmail.com	9876543210	Data not match		2055/12/12

FIGURE 3.14 VAST Face bulk enrollment file and images showing an error

10. Once the file is error-free, upload again, click on "Save", and wait for the profiles to be created.

11. After all profiles have been created, the system will display the bulk upload results.

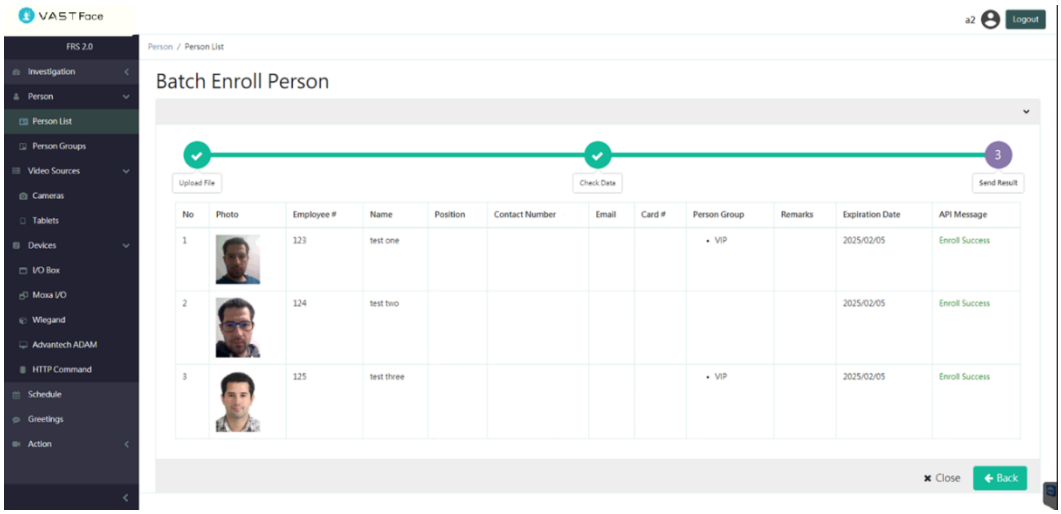


FIGURE 3.15 VAST Face bulk enrollment results

3.2.3 Person Groups

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Person" menu ➡ "Person Groups", a list of all created person group will be displayed.

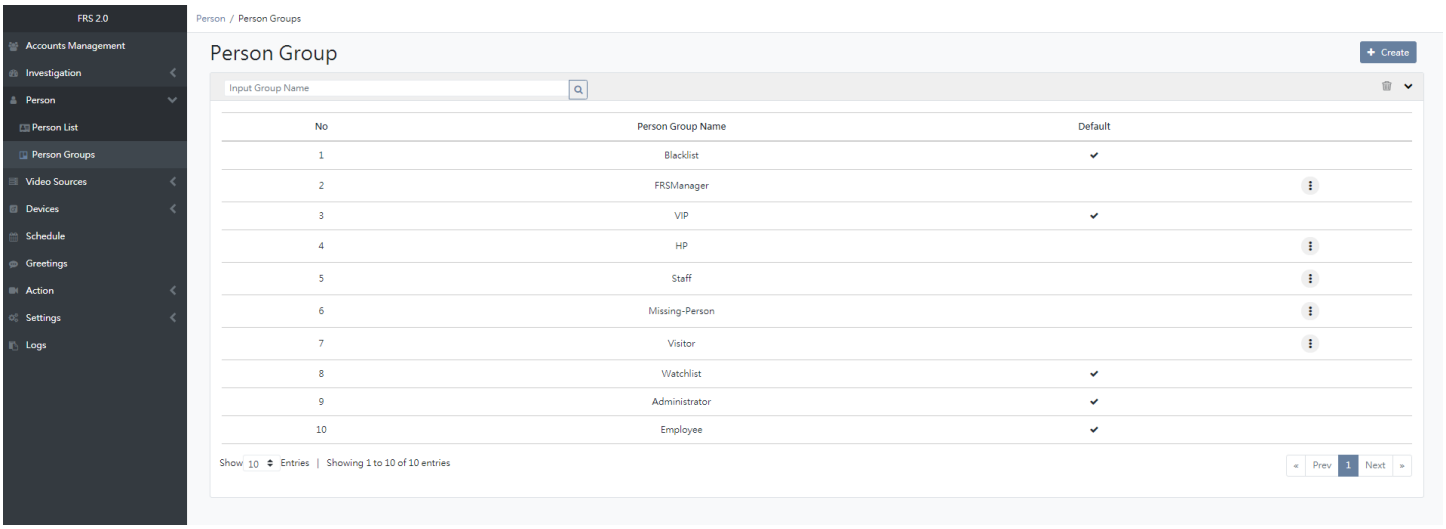


FIGURE 3.16 VAST Face person group list

4. Use the Display filters to narrow down results by: group name.

5. Click on the search button ( )button, to display only profiles matching the filter criteria.

6. In order to see a person group complete details, click on the "Profile Details" icon ( ), and select Edit, the selected profile full details will be displayed.

7. Edit any profile information as needed.

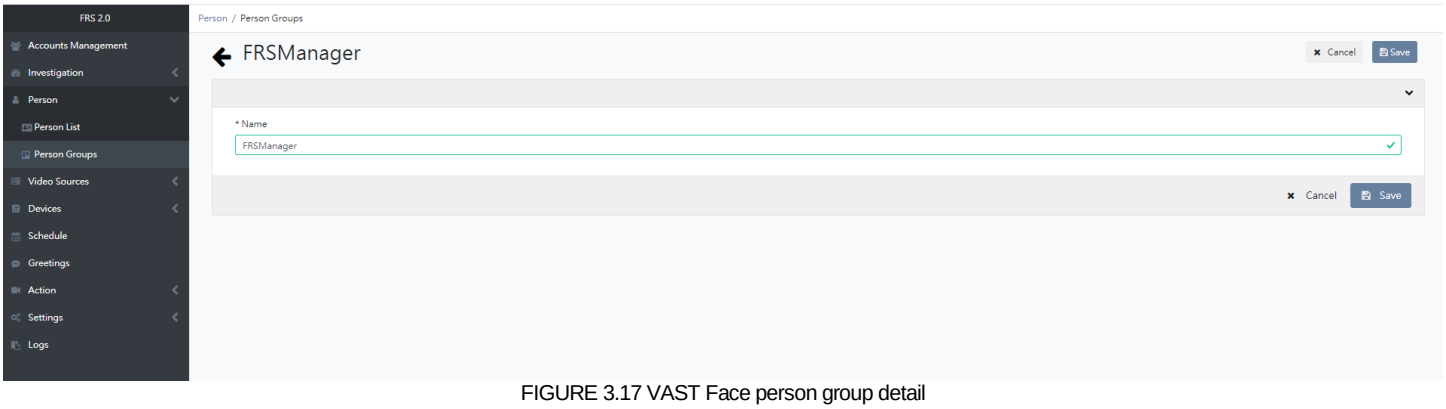


FIGURE 3.17 VAST Face person group detail

8. Click on "Save" to apply changes.

9. To Delete a profile, click on the "Profile Details" icon ( ), and select Delete (Delete).

10. A pop-up window will appear on-screen prompting the user to confirm the action.

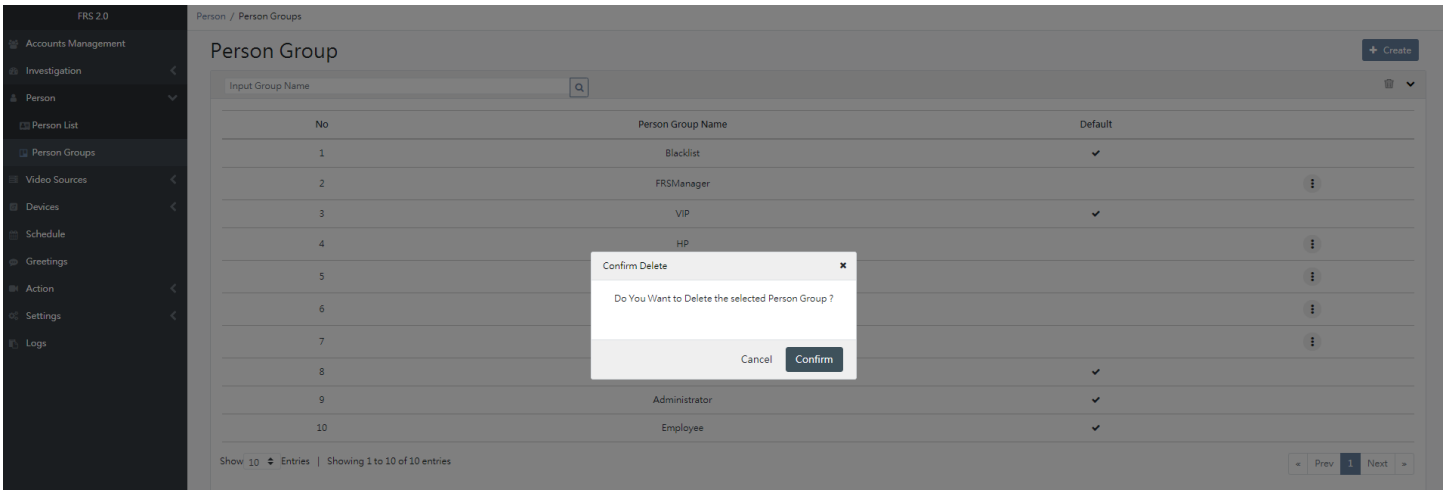


FIGURE 3.18 VAST Face delete person group

11. Click on "Confirm" to delete the selected person group(s).

12. To add a new person group, click on the "+Create" button (+ Create).

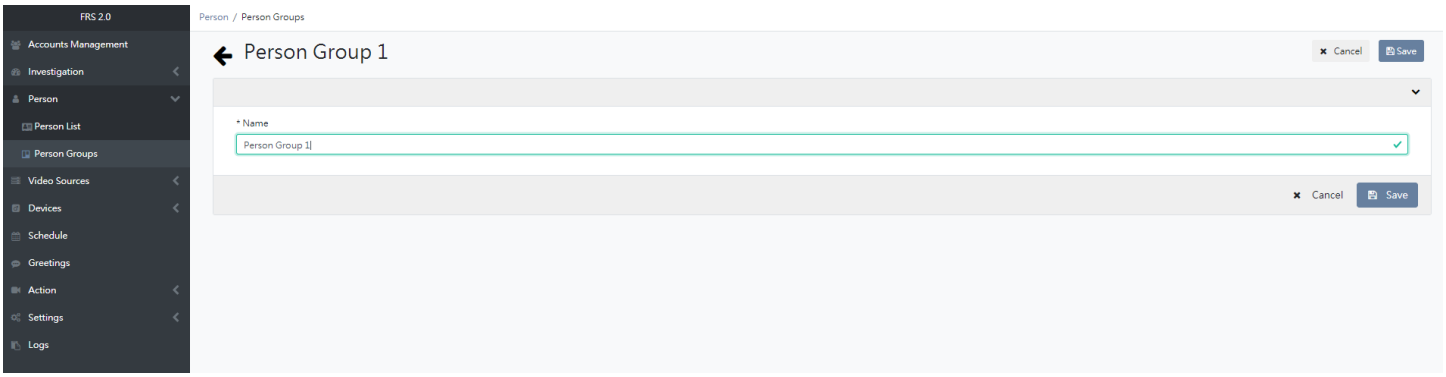


FIGURE 3.19 VAST Face create person group

13. On the "Create person group" menu, enter the new person group information:

    a. **Group name ➡** A user-friendly name to identify this person group.

14. Click on "Save" to create the person group.

3.3 VAST Face Reports

3.3.1 Persons Report

Note

- This type of report aka "historical reports" is used to display past face recognition events, for the purposes of providing a reliable face recognition events access log.

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Investigation" menu ➡ "Person".

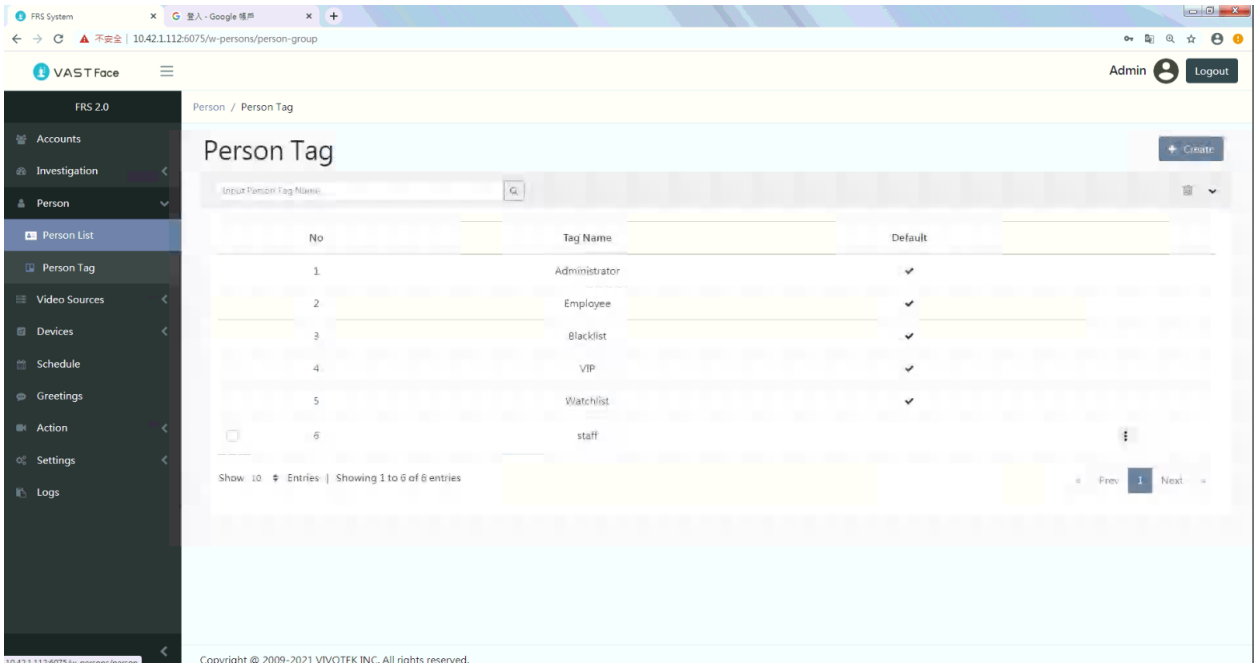


FIGURE 3.20 VAST Face persons report

4. Use the Display filters to narrow down results by: name, person type, or location.

5. Click on the "Search" button, only events matching the filter criteria will then be displayed on-screen.

6. In the event, that the face recognition to be exported, click on the "Export to Excel" button, which will export all on-screen face recognition events including the captured face snapshot.

3.3.2 Actions Report

Note

- This type of report aka "Action Log" is used to display which user-defined actions were automatically triggered in response to face recognition events.

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075) , VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Investigation" menu ➡ "Actions".

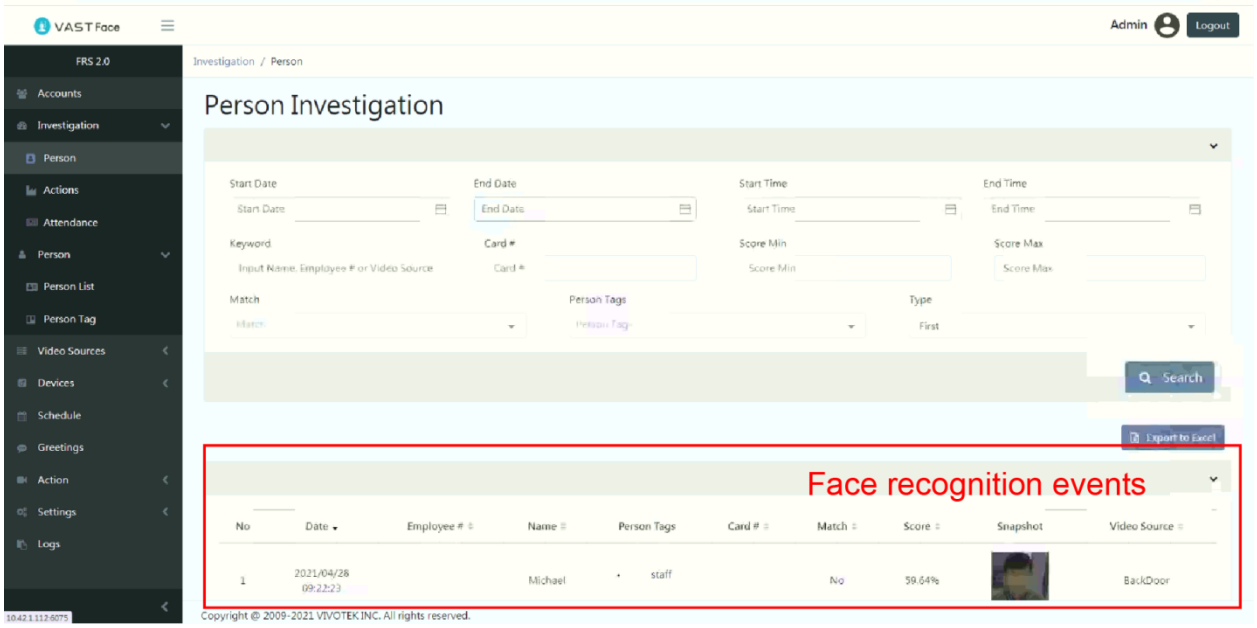


FIGURE 3.21 VAST Face actions report.

4. Use the Display filters to narrow down results by: name, person type, location or date range.

5. Click on "Search" button.

6. Only events matching the filter criteria will now be displayed on-screen.

7. In the event, that the action log needs to be exported, click on the "Export to Excel" button, results will be sent to a .XLSX file.

3.3.3 Attendance Report

Note

- This type of report aka "attendance report" is used to display when an enrolled person has entered / exited the premises, possible applications for it include: security guards, shift supervisors, HR managers.

- Entry time and out time & location are defined as the first and last instance when and where the person was detected. Likewise, stay time is computed as the time difference (delta) between the OUT event minus the IN event.

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075) , VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Investigation" menu ➡ "Attendance".

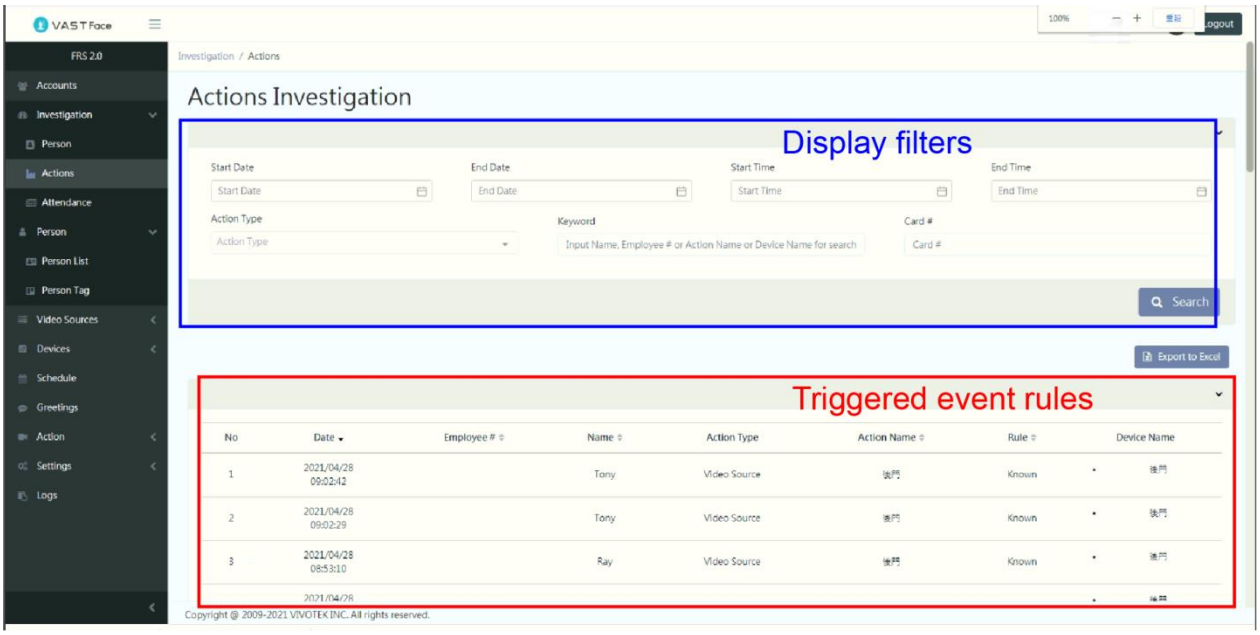


FIGURE 3.22 VAST Face Attendance reports

4. Use the Display filters to narrow down results by: name, person type, location or date range.

5. Click on "Search" button, only records matching the filter criteria will be displayed on-screen.

6. In the event, that the attendance needs to be exported, click on "Export to Excel" button, which will export all records with thumbnails included into a .XLSX file.

3.4 Video Source management

3.4.1 Camera

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Video Sources" menu ➡ "Camera", a list of all created camera will be displayed.

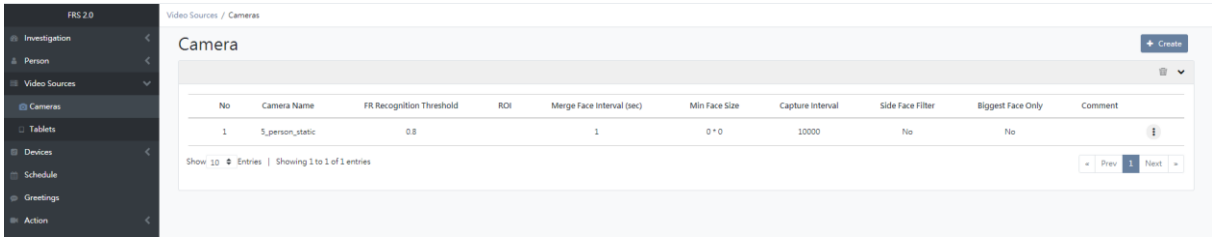


FIGURE 3.23 Video Sources – camera list

4. In order to see a camera complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected camera full details will be displayed.

5. Edit any profile information as needed.

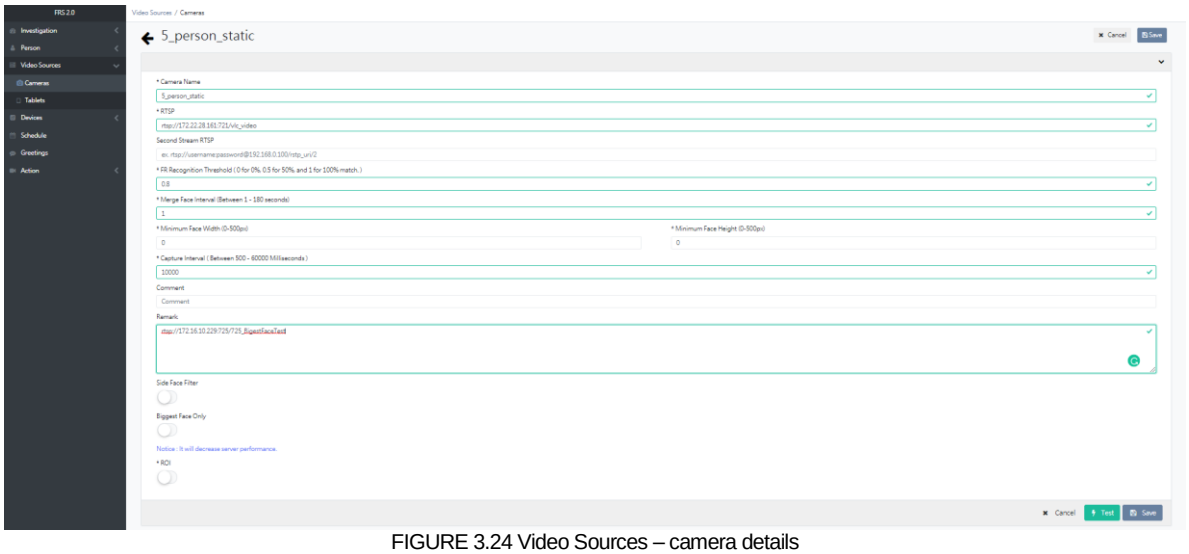


FIGURE 3.24 Video Sources – camera details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

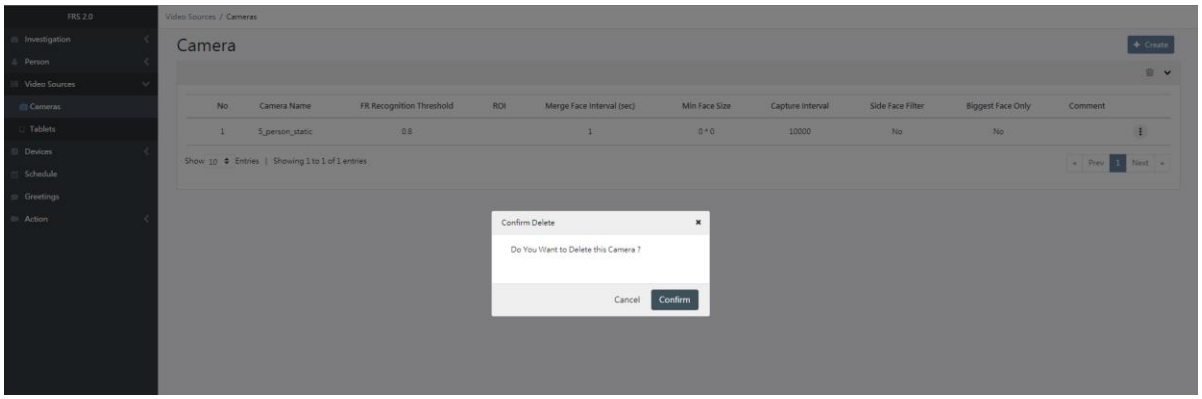


FIGURE 3.25 Video Sources delete camera

9. Click on "Confirm" to delete the selected camera(s).

10. To add a new camera, click on the "+Create" button (+ Create).

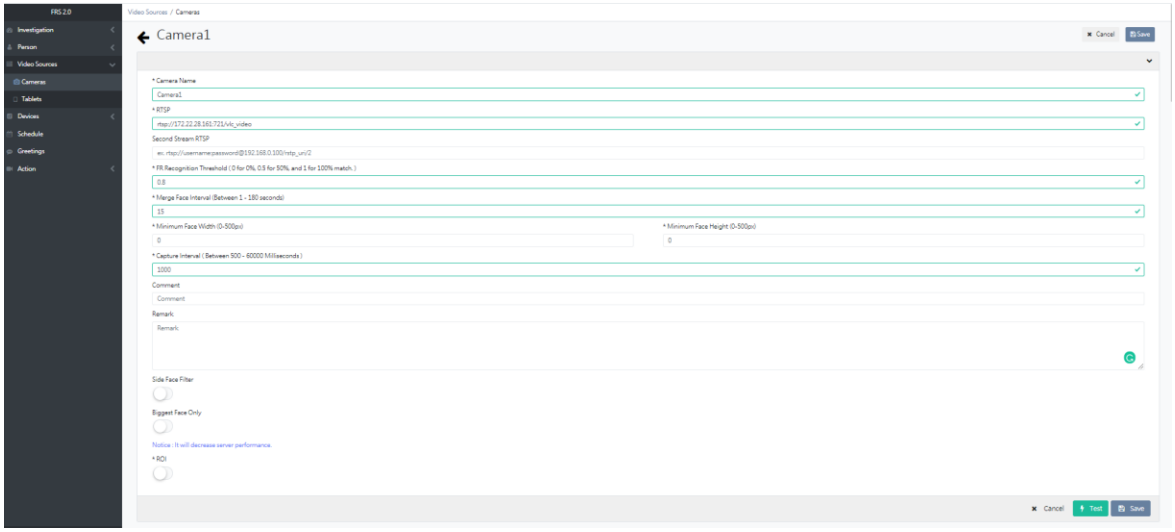


FIGURE 3.26 Video Sources create camera

11. On the "Create camera" menu, enter the new camera information:

    a. **Camera name** ➡ A user-friendly name to identify this camera.

    b. RTSP ➡ The IP camera Full RTSP URL path, including the device's username and passwords.

    (i. e: rtsp://root:fstadmin@192.168.1.38:554/axis-media/media.amp)

Note

- Each IP camera manufacturer will normally use a different RTSP URL.
- Only H.264 RTSP video streams are supported.

c. Second Stream RTSP ➡ (Optional) The second stream position of the camera image for other live streaming needs. If there is no setting, use the first RTSP stream together.

d. FR Recognition Threshold ➡ The minimum face recognition confidence level value (aka match rate) between the captured image and the enrolled face in the database, a higher value (from 0.0 to 1.0) indicates that a closer resemblance to the golden sample image is required for the system to mark the event as positive face recognition.

e. Merge Face Interval ➡ Interval (in seconds) for how long the face recognition engine should wait before reporting a new face recognition event for the same person.

f. Minimum Face Width & Hight ➡ The minimum face width and height size (in pixels) that is required for analyzing a face, faces with smaller dimensions are discarded.

g. Capture Interval ➡ The frequency (in milliseconds) for how often a video frame is extracted from the video source, and analyzed by the face recognition engine.

h. Comment ➡ (Optional)

i. Remark ➡ (Optional)

j. Side Face Filter ➡ Specialized filter that if enabled, will discard all non-frontal full-face images.

k. Biggest Face Only ➡ Specialized filter that if enabled, and in the event that there are multiple faces within the same video frame, will result in only the largest face being analyzed.

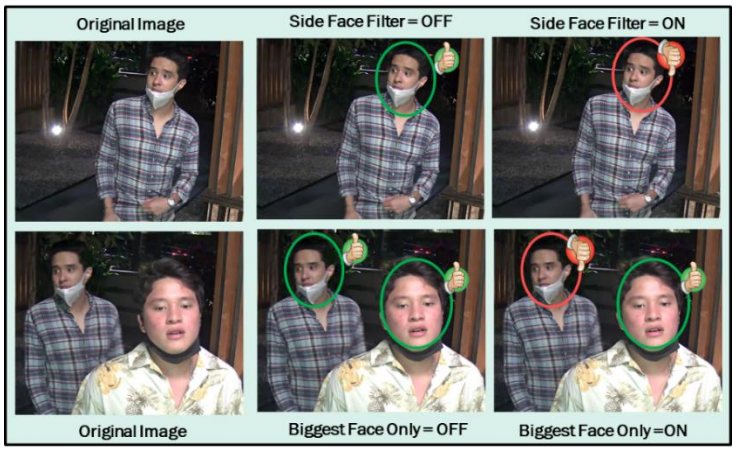


FIGURE 3.27 Face filter examples showing analyzed and rejected faces.

備註

- If there are multiple faces in the captured snapshot, the recognition engine of VAST Face may preferentially select the first face to the left (or right). When Biggest Face Only is turned on, it will capture all faces in the snapshot. Choose the face that recognizes the biggest, so performance may be affected.

12. Click on "Save" to create the camera.

3.4.2 Tablet

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Video Sources" menu ➡ "Tablet", a list of all created Tablet will be displayed.

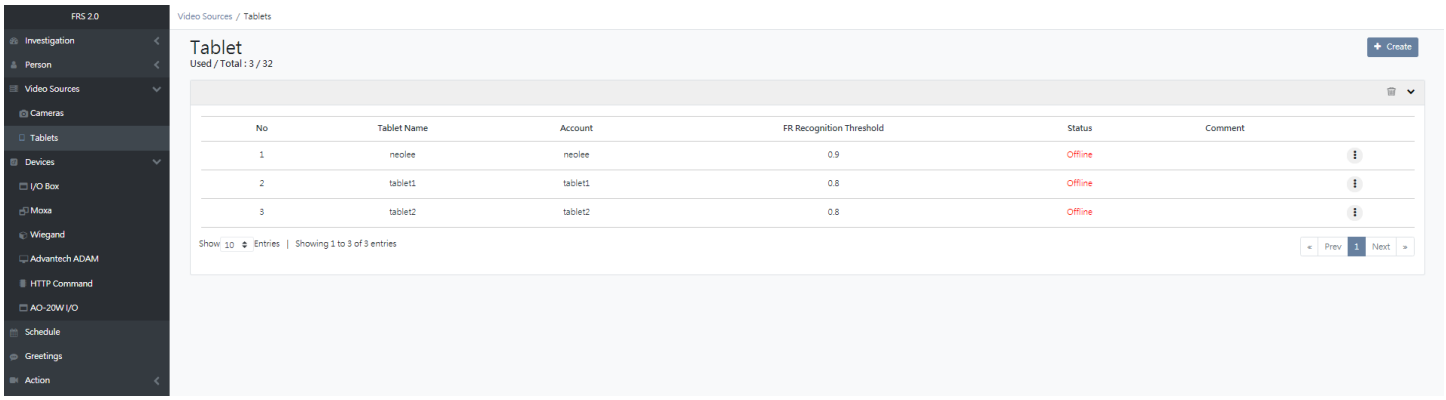


FIGURE 3.28 Video Sources – Tablet list

4. In order to see a tablet complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected tablet full details will be displayed.

5. Edit any profile information as needed.

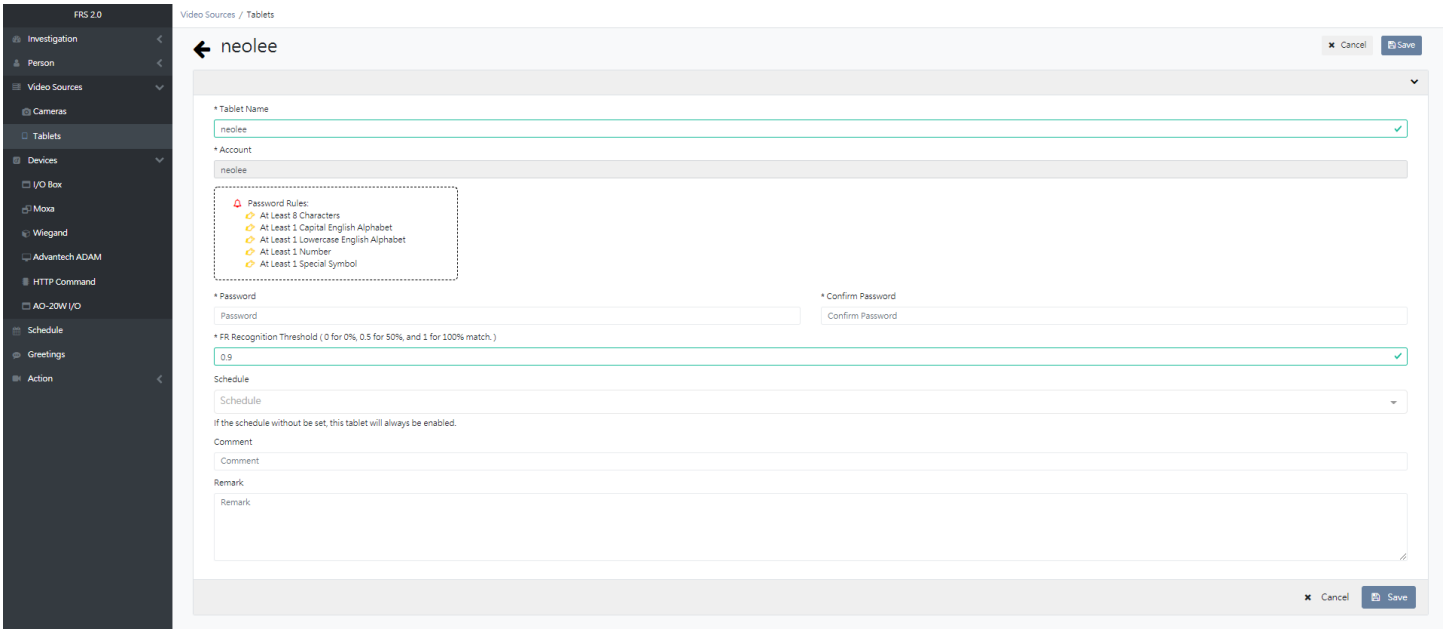


FIGURE 3.29 Video Sources – Tablet details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

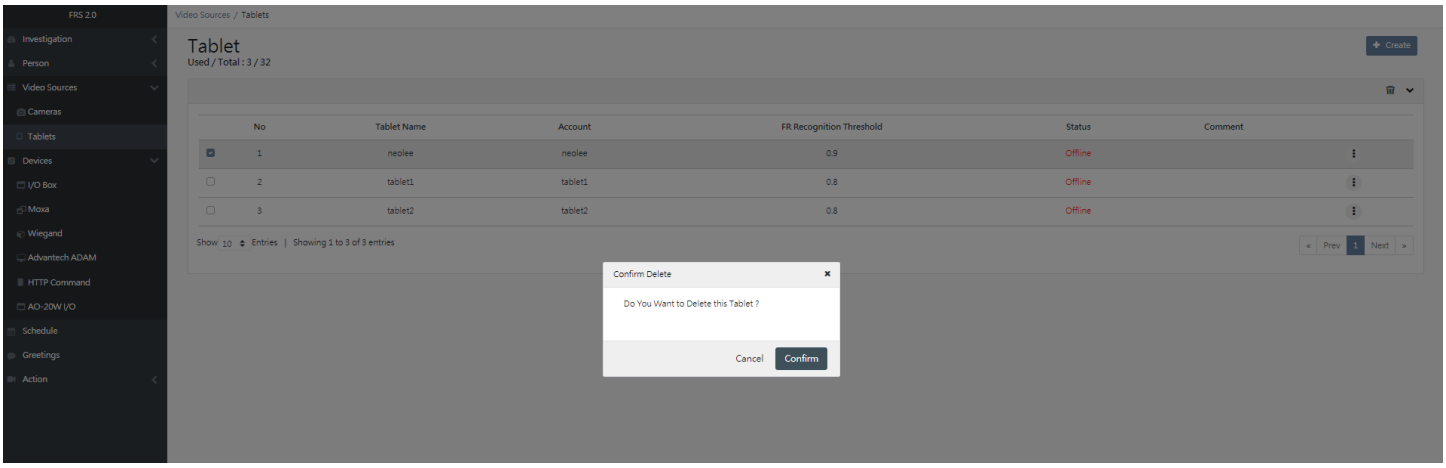


FIGURE 3.30 Video Sources delete Tablet

9. Click on "Confirm" to delete the selected tablet (s).

10. To add a new tablet, click on the "+Create" button (+ Create).

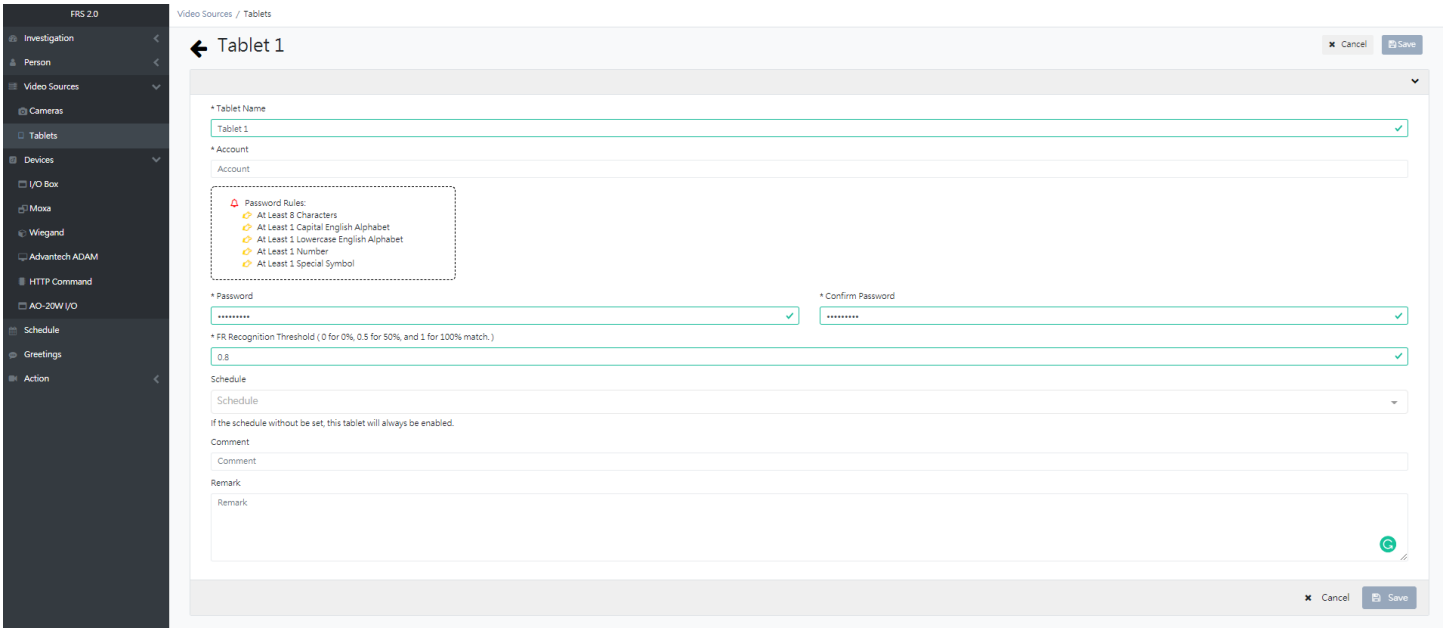


FIGURE 3.31 Video Sources create Tablet

11. On the "Create tablet" menu, enter the new tablet information:

    a. Tablet name ➡ A user-friendly name to identify this tablet.

    b. Account ➡ A unique username account that the tablet will use to connect to VAST Face.

    c. Password ➡ System password used to protect the tablet's username account.

d. Confirm Password ➡ Confirm Password again

e. Threshold ➡ The minimum face recognition confidence level value (aka match rate) between the captured image and the enrolled face in the database, a higher value (from 0.0 to 1.0) indicates that a closer resemblance to the golden sample image is required.

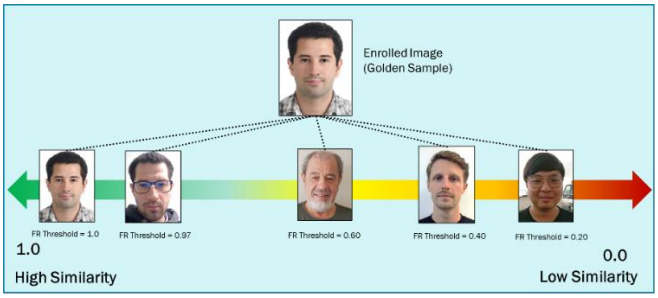


FIGURE 3.32 FR Threshold Comparison.

f. Schedule ➡ (Optional) Schedule template during which enrolled persons are allowed to authenticate at the tablet.

g. Comment ➡ (Optional)

h. Remark ➡ (Optional)

12. Click on "Save" to create the tablet.

3.5 Device Management

3.5.1 I/O Box

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "I/O Box", a list of all created Ethernet I/O Relay will be displayed.

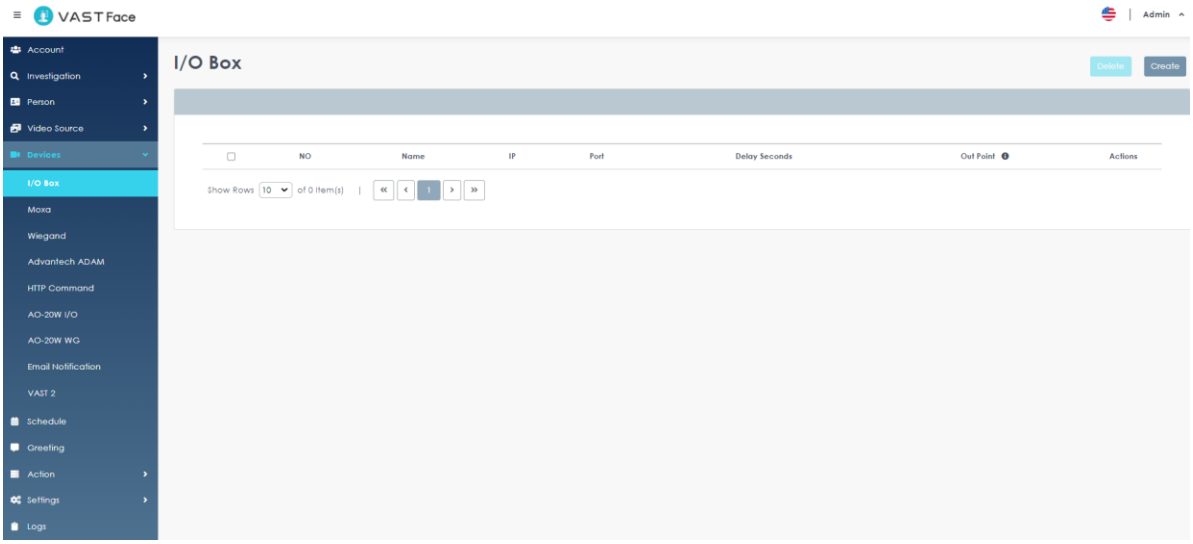


FIGURE 3.33 Device – I/O Box list

4. In order to see a tablet complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected I/O Box full details will be displayed.

5. Edit any profile information as needed.

FIGURE 3.34 Device – I/O Box details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

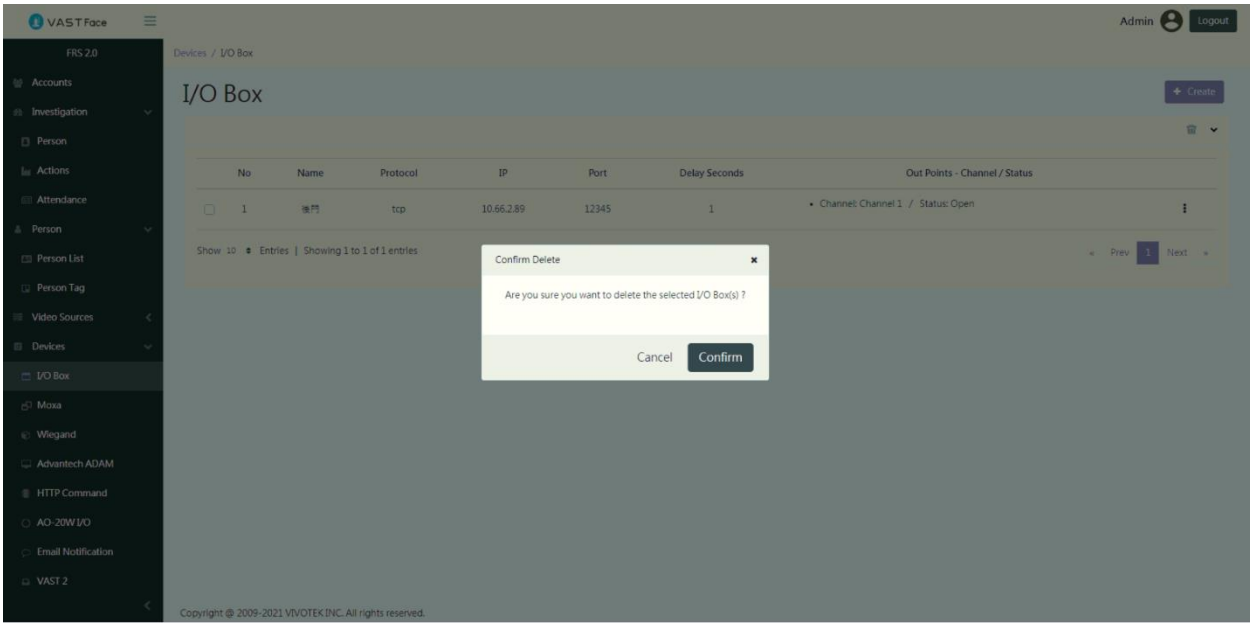


FIGURE 3.35 Device delete I/O Box

9. Click on "Confirm" to delete the selected I/O Box (s).

10. To add a new I/O Box, click on the "+Create" button (+ Create).

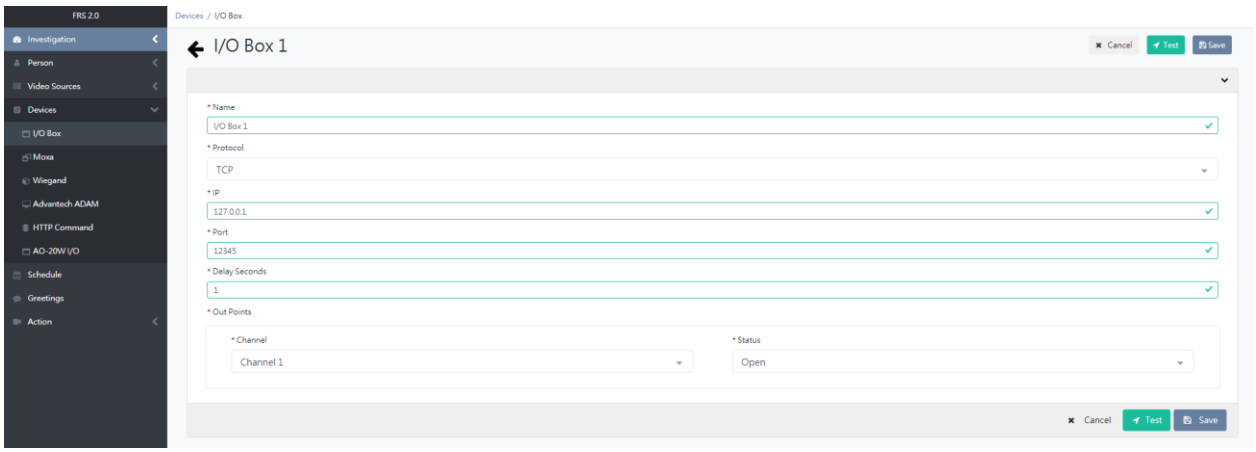


FIGURE 3.36 Device - create I/O Box

11. On the "Create I/O Box" menu, enter the new Ethernet I/O Relay information:

    a. Name ➡ A user-friendly name to identify this device.

    b. Protocol ➡ The communication protocol that will be used (TCP, UDP, or others).

c. IP ➡ The device's IP address.

d. Port ➡ The device's communication port.

e. Delay Seconds ➡ Corresponds to a timer (in seconds) for how long VAST Face should wait before triggering the device's normal state signal after receiving a face recognition event.

f. Channel ➡ Control relay output channel that is to be triggered upon receiving a face recognition event.

g. Status ➡ Whether the appliance connected to the control relay output requires to be

   i. Open ➡ Normally Closed device

   ii. Close ➡ Normally Open device

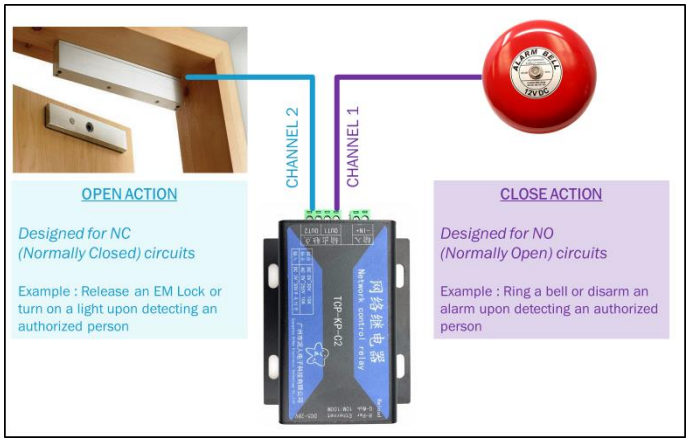


FIGURE 3.37 Channel and status explanation.

12. Click "Test" to test whether the IP and port can connect to the I/O Box correctly. If the test fails, the device data cannot be saved

13. Click on "Save" to create the I/O Box.

3.5.2 Moxa

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "Moxa", a list of all created Moxa will be displayed.

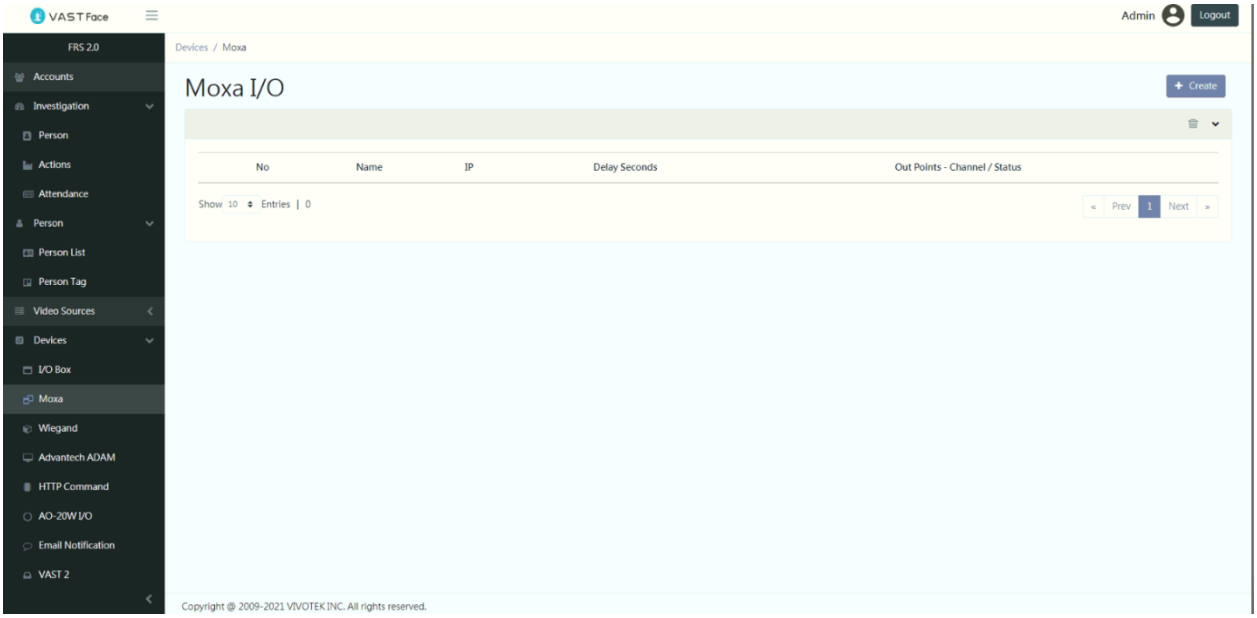


FIGURE 3.38 Device – Moxa I/O list

4. In order to see a Moxa complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected Moxa full details will be displayed.

5. Edit any profile information as needed.

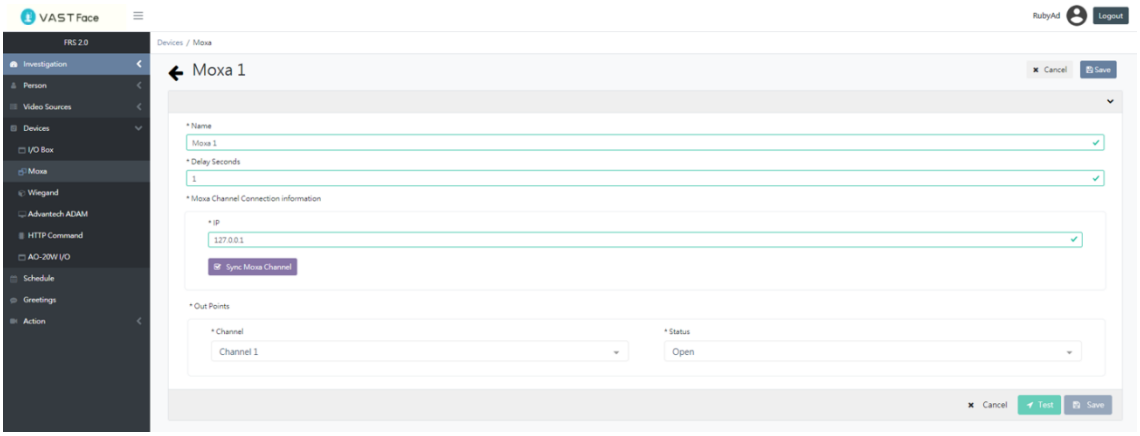


FIGURE 3.39 Device – Moxa details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

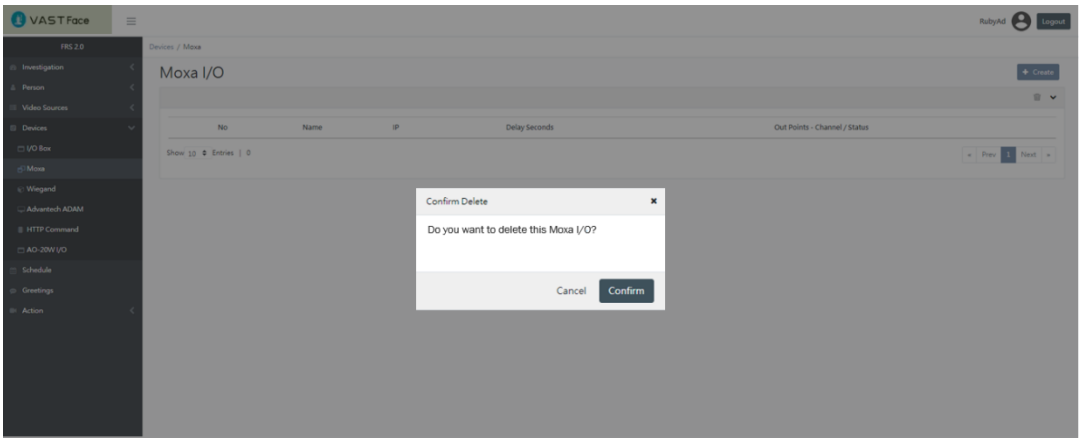


FIGURE 3.40 Device delete Moxa

9. Click on "Confirm" to delete the selected Moxa (s).

10. To add a new Moxa, click on the "+Create" button (+ Create).

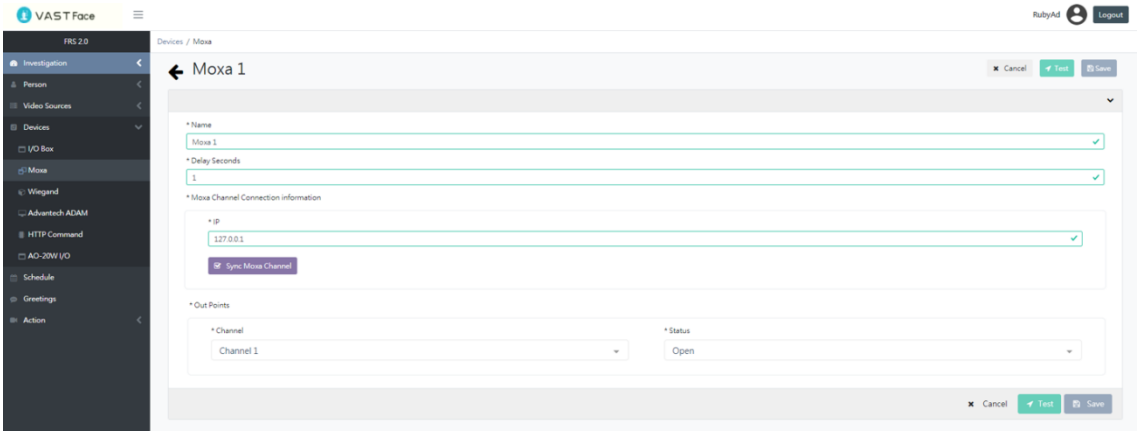


FIGURE 3.41 Device - create Moxa

11. On the "Create Moxa" menu, enter the new Moxa information:

    a. Name ➡ A user-friendly name to identify this device.

    b. IP ➡ The device's IP address.

    c. Sync Moxa Channel ➡ There are several DO outputs to get from Moxa I/O

    d. Delay Seconds ➡ Corresponds to a timer (in seconds) for how long VAST Face should wait before triggering the device's normal state signal after receiving a face recognition event.

    e. Channel ➡ Control relay output channel that is to be triggered upon receiving a face recognition event.

f. Status ➡ Whether the appliance connected to the control relay output requires to be

   i. Open ➡ Normally Closed device

   ii. Close ➡ Normally Open device

12. Click "Test" to test whether the IP can connect to the Moxa correctly. If the test fails, the device data cannot be saved

13. Click on “Save” to create the Moxa.

3.5.3 Wiegand

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "Wiegand", a list of all created Wiegand will be displayed.

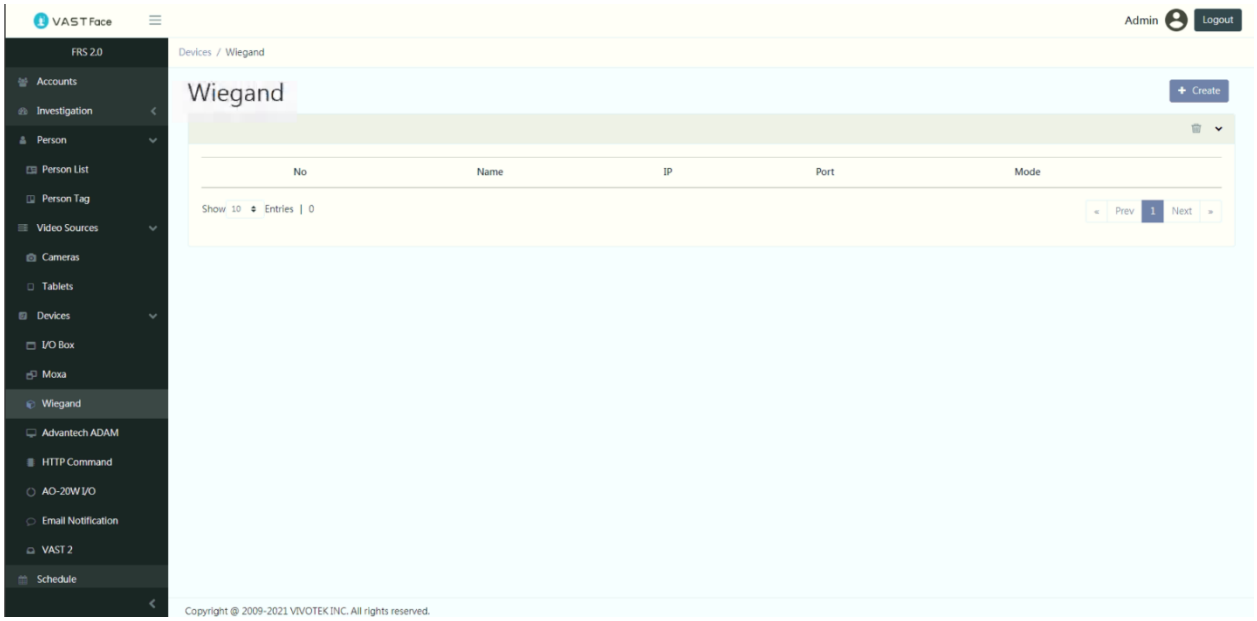


FIGURE 3.42 Device – Wiegand list

4. In order to see a Wiegand complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected Wiegand full details will be displayed.

5. Edit any profile information as needed.

FIGURE 3.43 Device – Wiegand details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

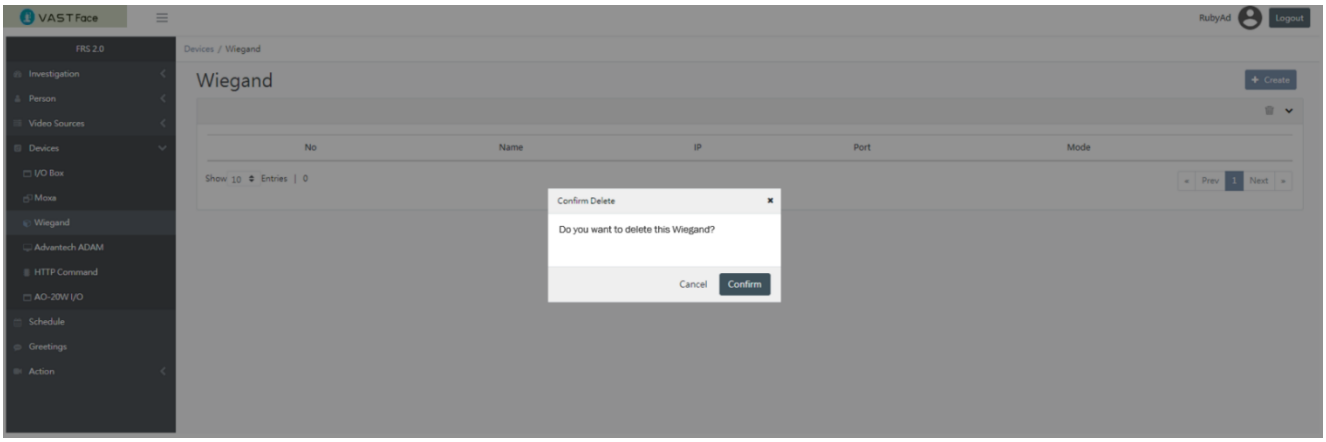


FIGURE 3.44 Device delete Wieand

9. Click on "Confirm" to delete the selected Wiegand (s).

10. To add a new Wiegand, click on the "+Create" button (+ Create).

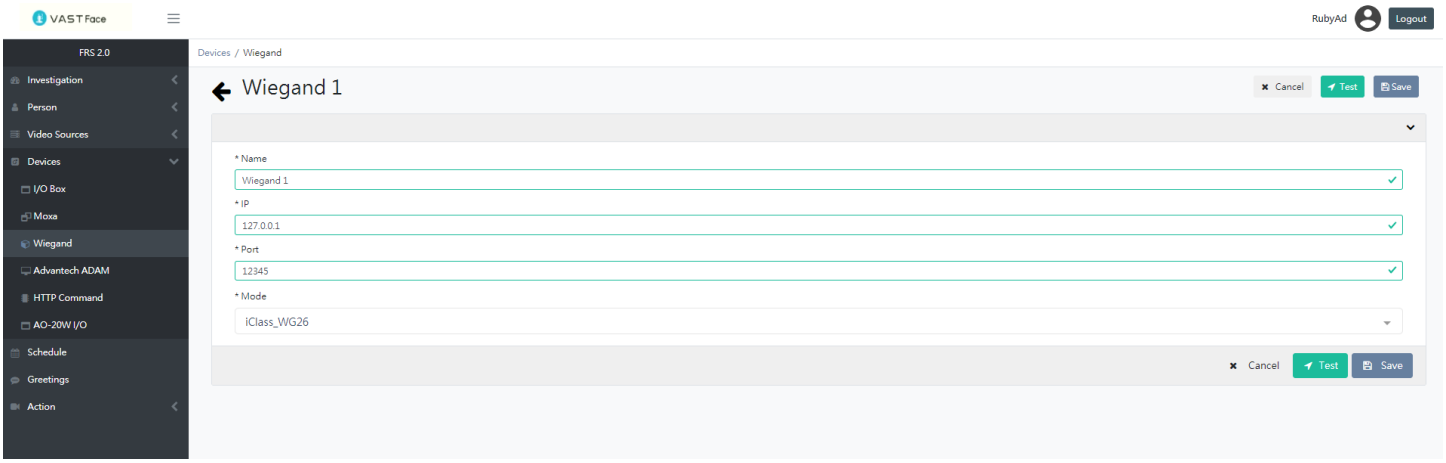


FIGURE 3.45 Device - create Wiegand

11. On the "Create Wiegand" menu, enter the new Wiegand information:

    a. Name ➡ A user-friendly name to identify this device.

    b. IP ➡ The device's IP address.

    c. Port ➡ The device's communication port.

    d. Mode ➡ Corresponds to the Card technology (iClass or Mifare) and Wiegand bits (26 or 34) format that the converter will output.

12. Click "Test" to test whether the IP and Port can connect to the Wiegand correctly. If the test fails, the device data cannot be saved

13. Click on "Save" to create the Wiegand.

3.5.4 Advantech ADAM

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "Advantech ADAM", a list of all created Advantech ADAM will be displayed.

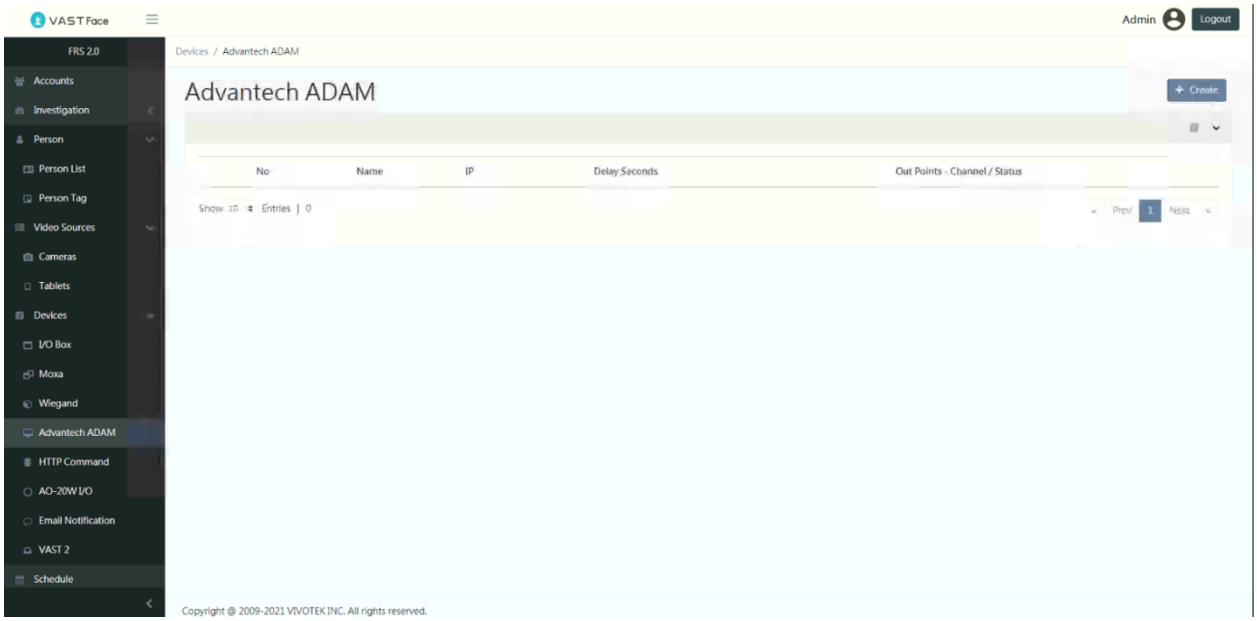


FIGURE 3.46 Device – Advantech ADAM list

4. In order to see a Advantech ADAM complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected Advantech ADAM full details will be displayed.

5. Edit any profile information as needed.

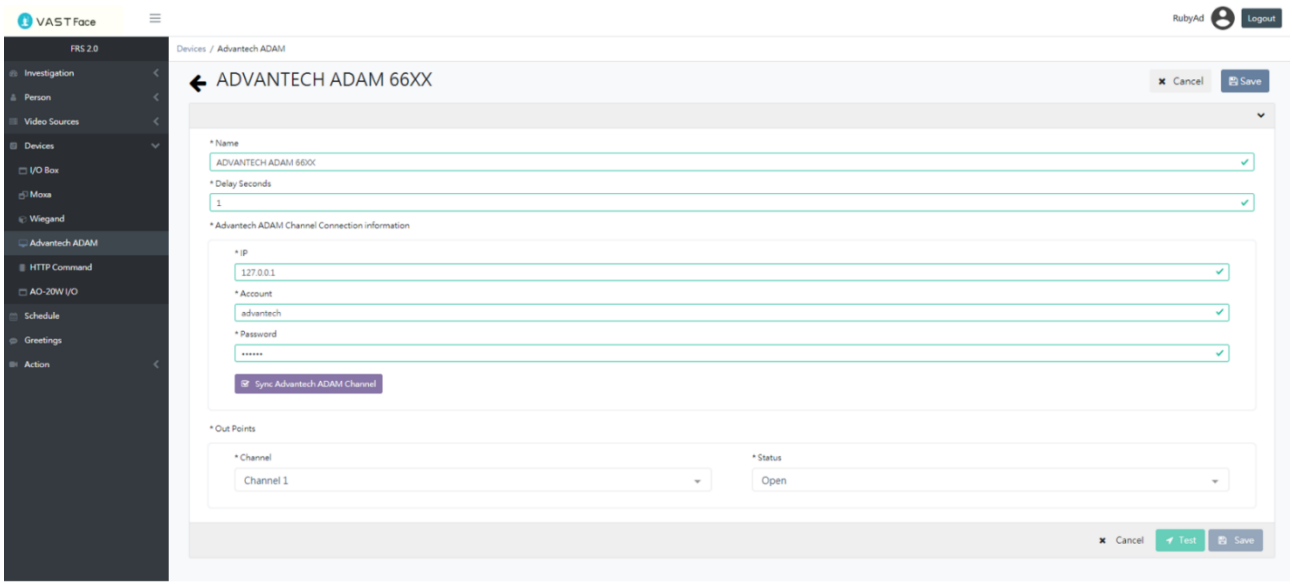


FIGURE 3.47 Device – Advantech ADAM details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

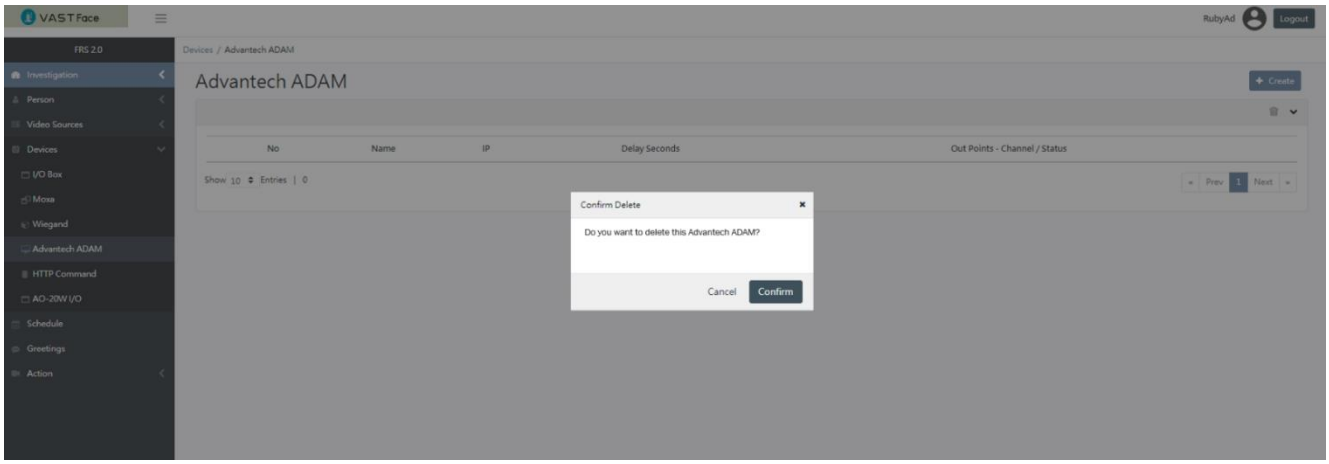


FIGURE 3.48 Device delete Advantech ADAM

9. Click on "Confirm" to delete the selected Advantech ADAM (s).

10. To add a new Advantech ADAM, click on the "+Create" button (+ Create).

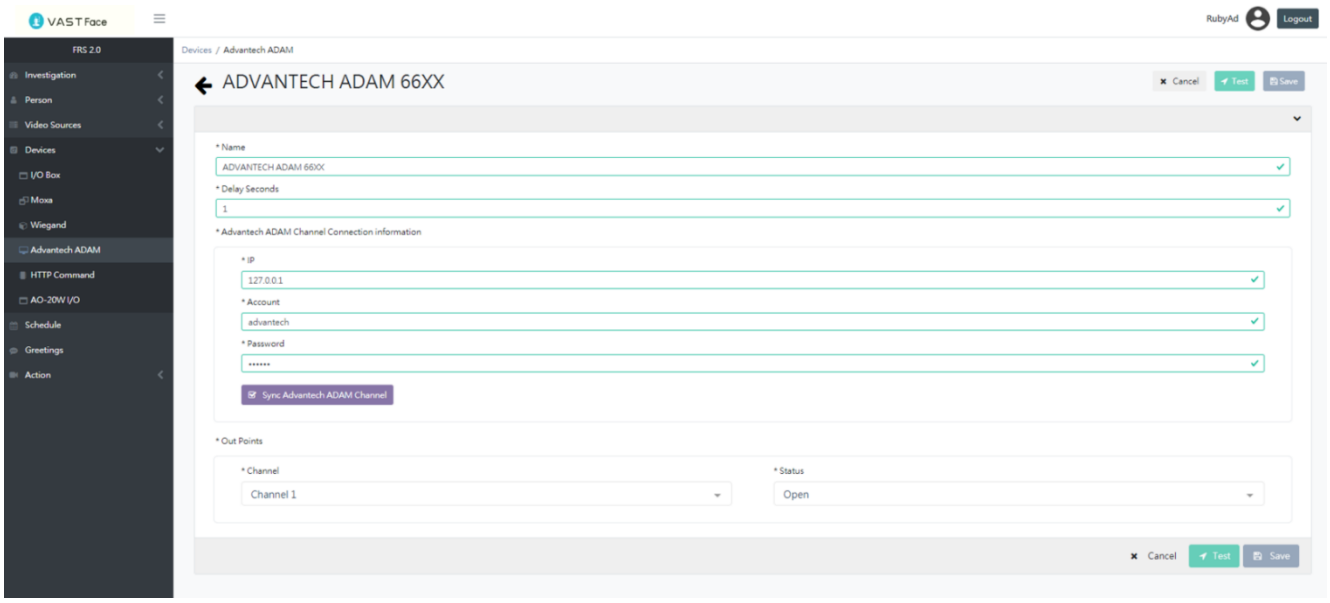


FIGURE 3.49 Device - create Advantech ADAM

11. On the "Create Advantech ADAM" menu, enter the new Advantech ADAM information:
    a. Name ➡ A user-friendly name to identify this device.
    b. Delay Seconds ➡ Corresponds to a timer (in seconds) for how long VAST Face should wait before triggering the device's normal state signal after receiving a face recognition event.
    c. IP ➡ The device's IP address.
    d. Account ➡ An account to connect Advantech ADAM with the server
    e. Password ➡ An Password to connect Advantech ADAM with the server
    f. Sync Advantech ADAM Channel ➡ There are several DO outputs to get from Advantech ADAM I/O
    g. Channel ➡ Control relay output channel that is to be triggered upon receiving a face recognition event.
    h. Status ➡ Whether the appliance connected to the control relay output requires to be
        i. Open ➡ Normally Closed device
        ii. Close ➡ Normally Open device
12. Click "Test" to test whether the IP can connect to the Advantech ADAM correctly. If the test fails, the device data cannot be saved
13. Click on "Save" to create the Advantech ADAM.

3.5.5 HTTP Command

In the event that notifying external systems is required upon detecting a person belonging to a face group, VAST Face provides an effective, yet simple integration method that allows sending notifications to 3rd party systems using a HTTP RESTful API. In order to allow for the utmost flexibility, system administrators can define the notification method, and can customize the notifications message contents to suit their needs.

Note

- Since configuration steps are very similar for same device type, only one device model per type will be covered in this section. Differences lay only in the communication port number, and whether the device requires a username & password. For most cases and when available, external devices must be set to TCP Server or UDP Server Mode.

- At the time of this writing, only JSON format is supported.

- While users can define their own key names in the HTTP template message, key values are limited to a list of predefined variables. These variables are invoked by using double curled brackets, plus the variable name. Similarly, variables can be used either on the body message or as part of the destination URL. For example:

The recognized person's name is Jay, and the emplyoeed number # is 24768547

Host: http://172.16.10.43/alarm?personName={{ personName }}

body:

```
{
"personEmployeeId":"{{ personEmployeeId }}"
}
```

When the action triggered, the variable on the host and body will be replace to:

Host: http://172.16.10.43/alarm?personName=Jay

body:

```
{
"personEmployeeId":"24768547"
}
```

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "HTTP Command", a list of all created HTTP Command will be displayed.

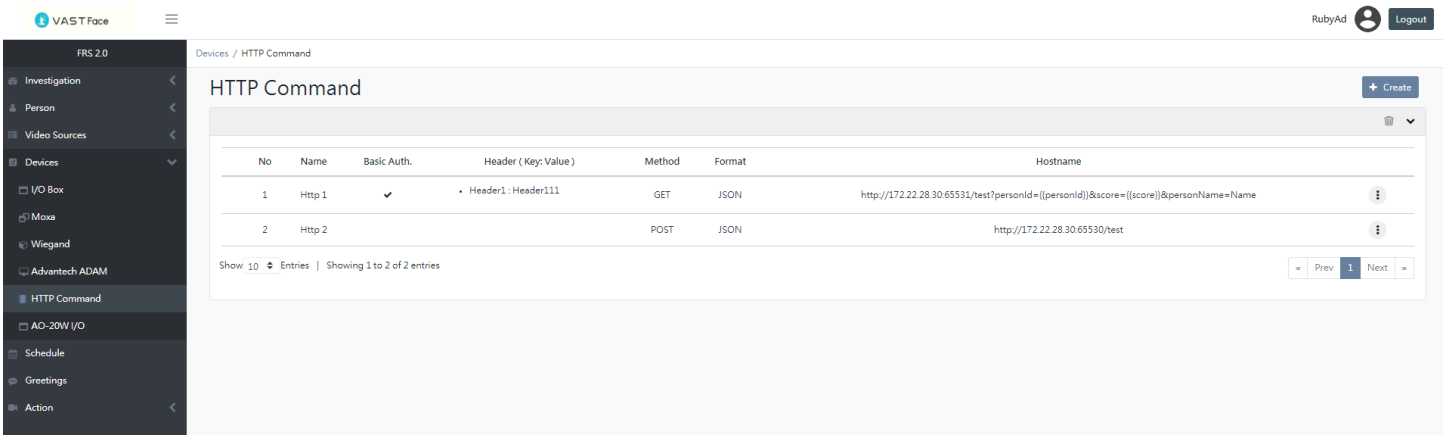


FIGURE 3.50 Device – HTTP Command list

4. In order to see a HTTP Command complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected HTTP Command full details will be displayed.

5. Edit any profile information as needed.

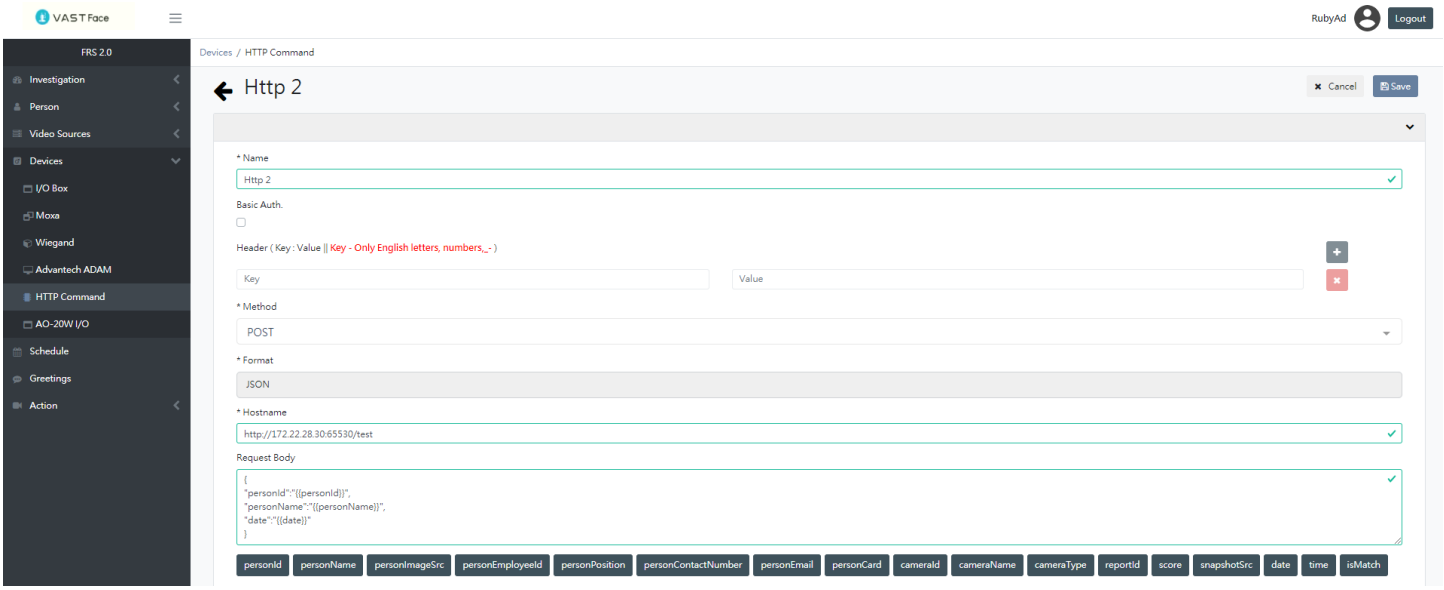


FIGURE 3.51 Device – HTTP Command details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

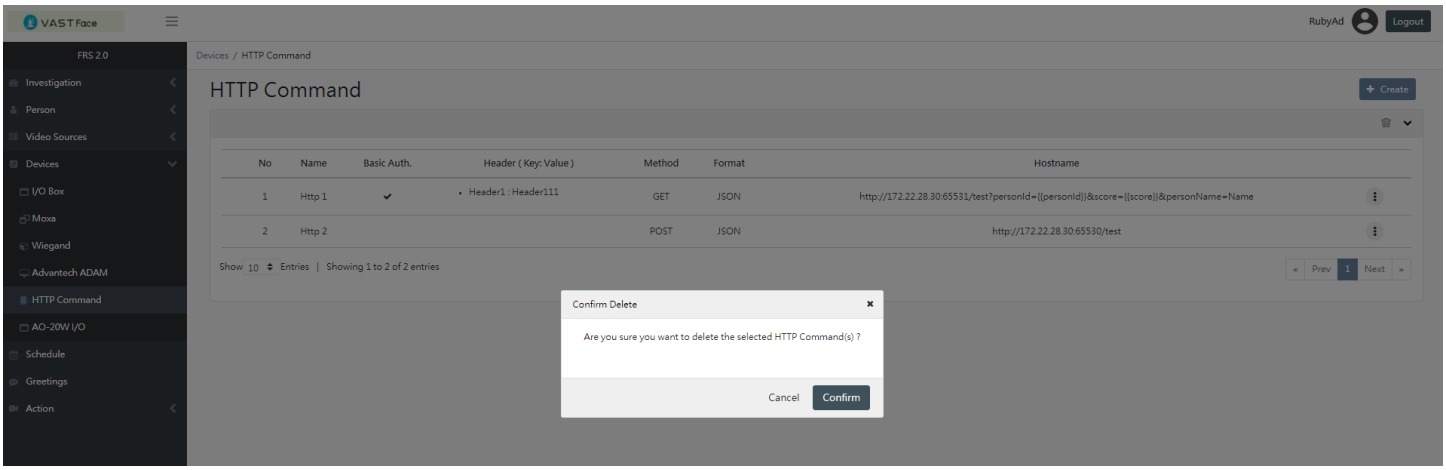


FIGURE 3.52 Device delete HTTP Command

9. Click on "Confirm" to delete the selected HTTP Command (s).

10. To add a new HTTP Command, click on the "+Create" button (+ Create).

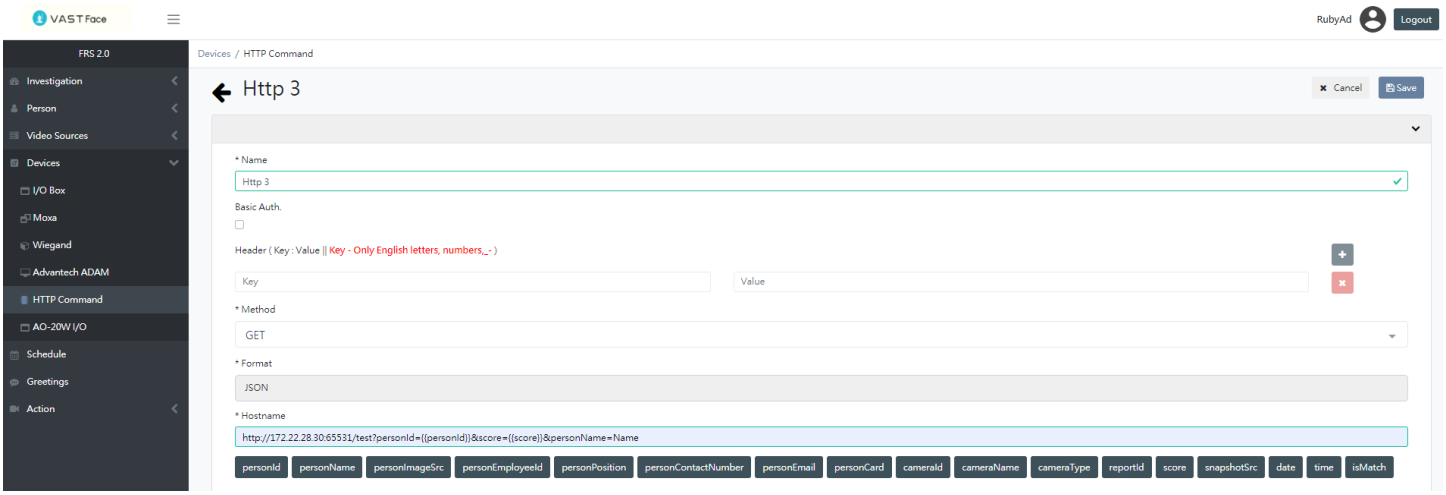


FIGURE 3.53 Device - create HTTP Command

11. On the "Create HTTP Command" menu, enter the new HTTP Command information:

    a. Name ➡ A user-friendly name to better identify this command.

    b. Base Auth. ➡ Whether to enable Basic Authentication, if enable it, must set an authentication account and password

    c. Header ➡ HTTP Header and key values.

    d. Method ➡ HTTP data transfer method (GET or POST).

    e. Host ➡ Destination URL where the HTTP message is to be sent.

    f. Format ➡ (Unchangeable) JSON format

g. Request Body ➡ HTTP Message Body.

12. Click on "Save" to create the HTTP Command.

3.5.6 AO-20W I/O

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "AO-20W I/O", a list of all created AO-20W I/O will be displayed.

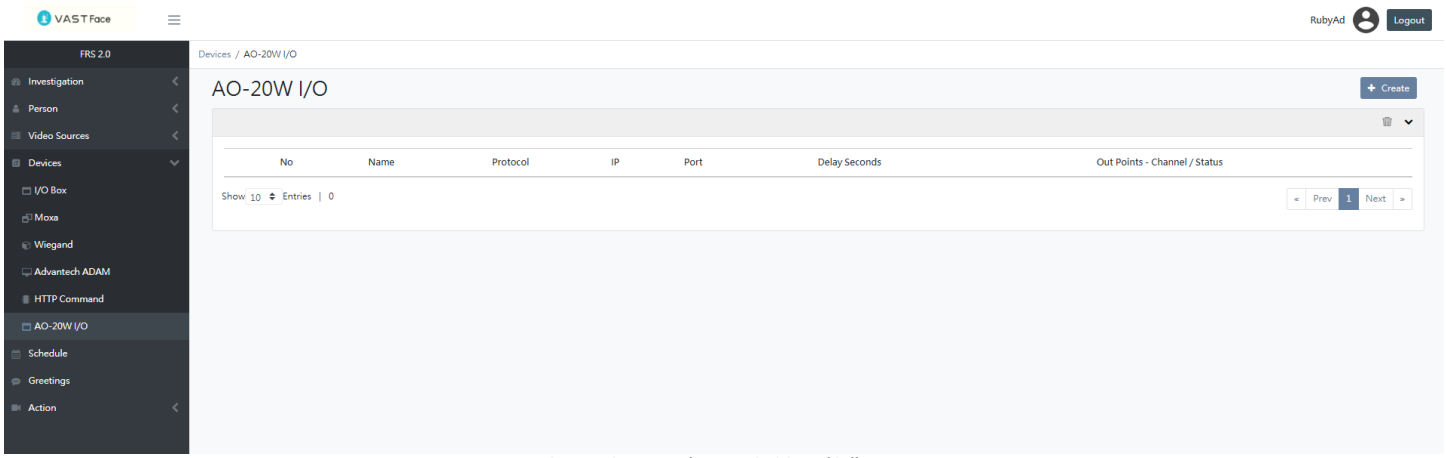


FIGURE 3.54 Device – AO-20W I/O list

4. In order to see a AO-20W I/O complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected AO-20W I/O full details will be displayed.

5. Edit any profile information as needed.

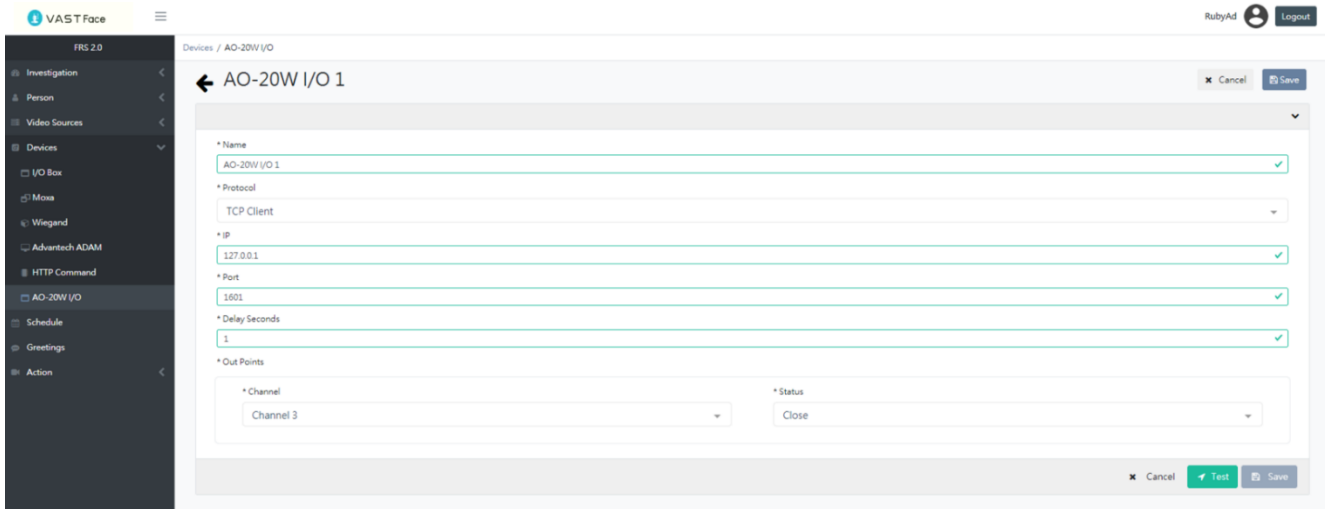


FIGURE 3.55 Device – AO-20W I/O details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

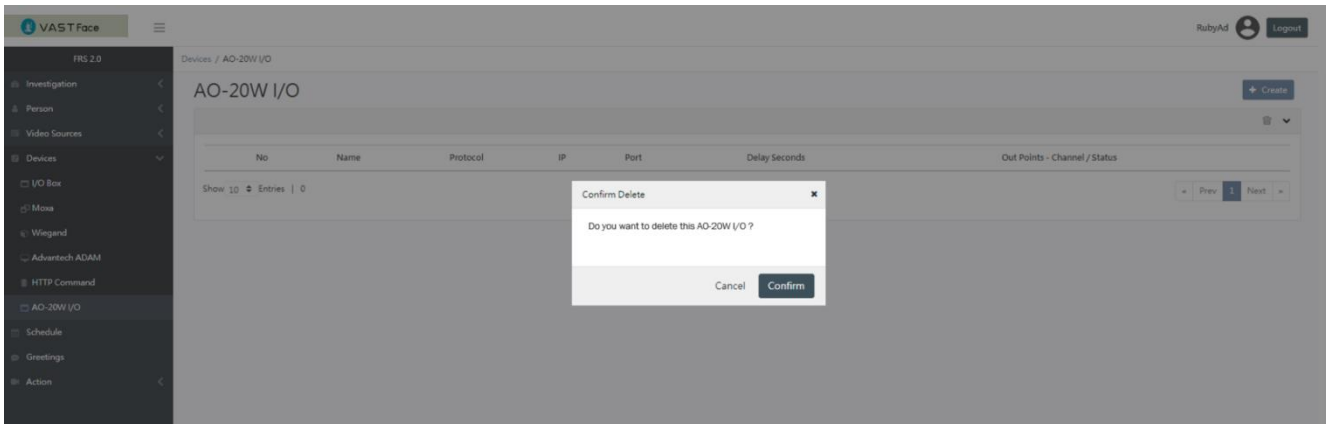


FIGURE 3.56 Device delete AO-20W I/O

9. Click on "Confirm" to delete the selected AO-20W I/O (s).

10. To add a new AO-20W I/O, click on the "+Create" button (+ Create).

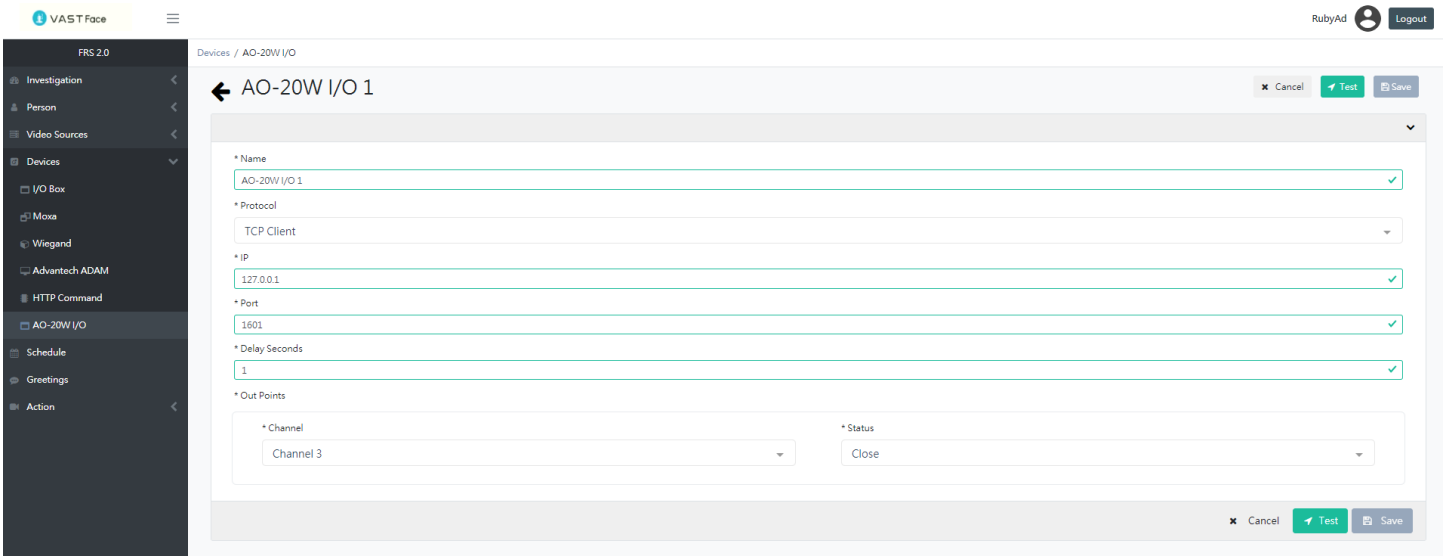


FIGURE 3.57 Device - create AO-20W I/O

11. On the "Create AO-20W I/O" menu, enter the new AO-20W I/O information:

    a. Name ➡ A user-friendly name to identify this device.

    b. Protocol ➡ The communication protocol that will be used (TCP, UDP, or others).

    c. IP ➡ The device's IP address.

    d. Port ➡ The device's communication port.

e. Delay Seconds ➡ Corresponds to a timer (in seconds) for how long VAST Face should wait before triggering the device's normal state signal after receiving a face recognition event.

f. Channel ➡ Control relay output channel that is to be triggered upon receiving a face recognition event.

g. Status ➡ Whether the appliance connected to the control relay output requires to be

   i. Open ➡ Normally Closed device

   ii. Close ➡ Normally Open device

12. Click "Test" to test whether the IP and Port can connect to the AO-20W I/O correctly. If the test fails, the device data cannot be saved

13. Click on "Save" to create the AO-20W I/O.

3.5.7 AO-20W WG

14. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

15. Login to VAST Face using an Administrator account.

16. Navigate to "Devices" menu ➡ "AO-20W WG", a list of all created Wiegand will be displayed.

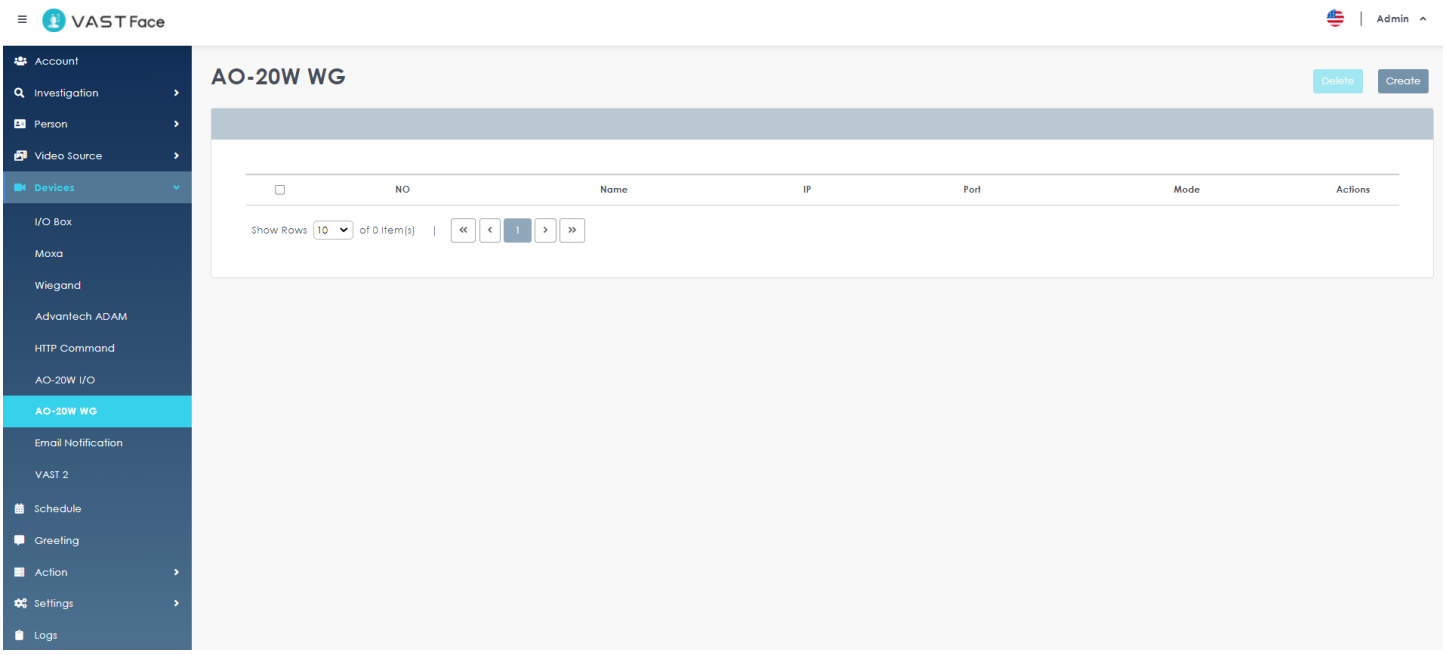


FIGURE 3.51 Device – Wiegand list

17. In order to see a Wiegand complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected Wiegand full details will be displayed.

18. Edit any profile information as needed.

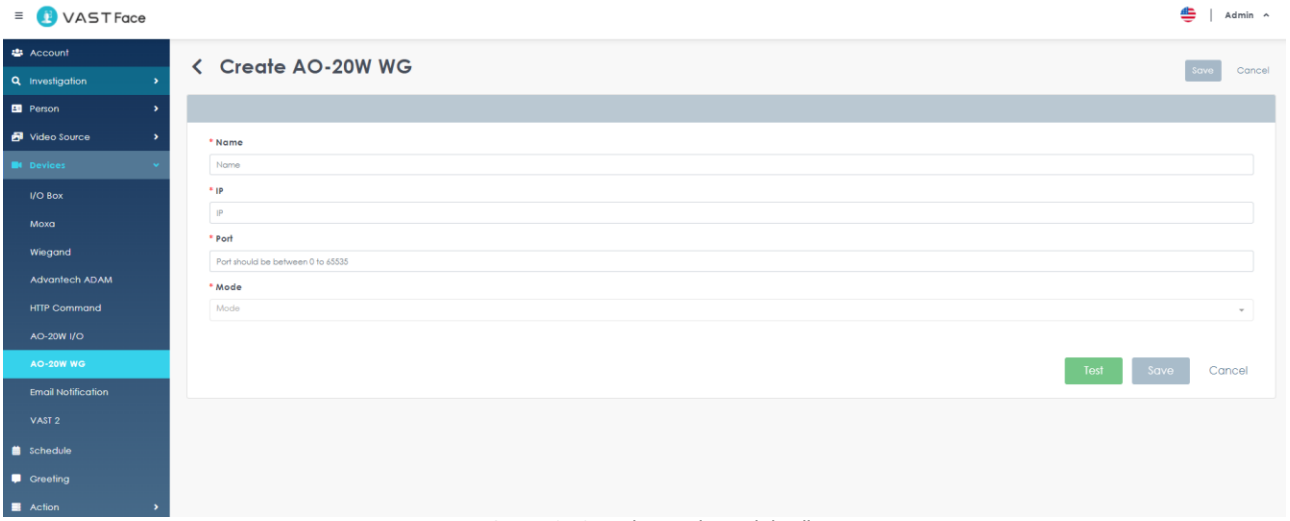


FIGURE 3.52 Device – Wiegand details

19. Click on "Save" to apply changes.

20. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

21. A pop-up window will appear on-screen prompting the user to confirm the action.

22. Click on "Confirm" to delete the selected Wiegand (s).

23. To add a new Wiegand, click on the "+Create" button (+ Create).

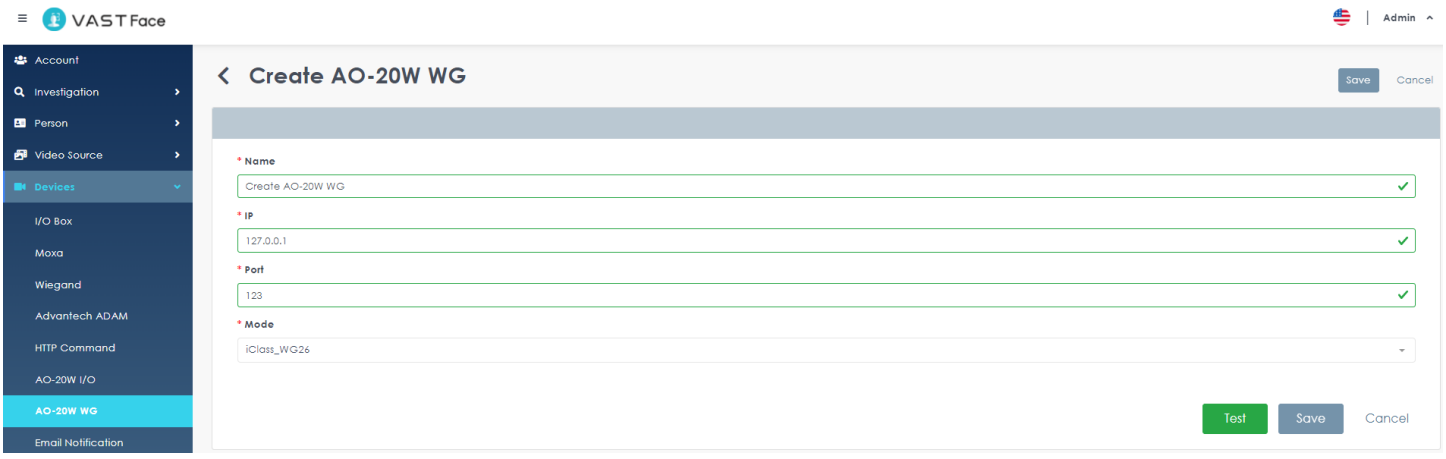


FIGURE 3.53 Device - Create Wiegand

24. On the "Create Wiegand" menu, enter the new Wiegand information:

    a. Name ➡ A user-friendly name to identify this device.

    b. IP ➡ The device's IP address.

    c. Port ➡ The device's communication port.

d. Mode ➡ Corresponds to the Card technology (iClass or Mifare) and Wiegand bits (26 or 34) format that the converter will output.

25. Click "Test" will pop up a test window for sending test card NO to test whether the IP and Port can connect to the Wiegand correctly.

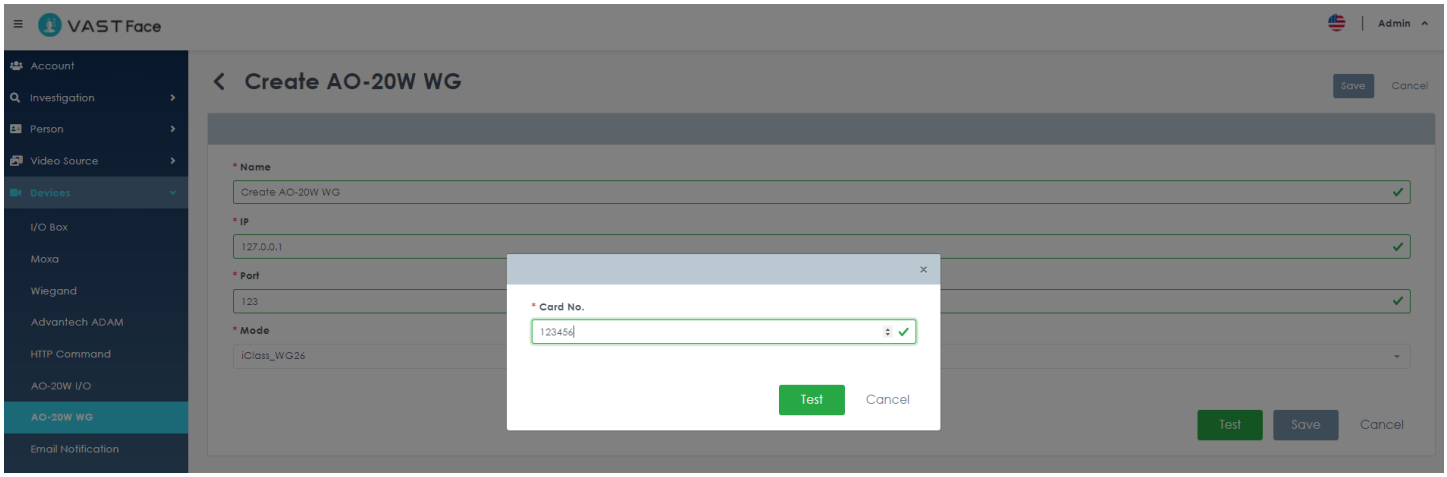


FIGURE 3.54 Device - Test Wiegand

26. If the test fails, the device data cannot be saved

27. Click on "Save" to create the Wiegand.

3.5.8 VAST 2

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Devices" menu ➡ "VAST 2", a list of all created VAST 2 will be displayed.

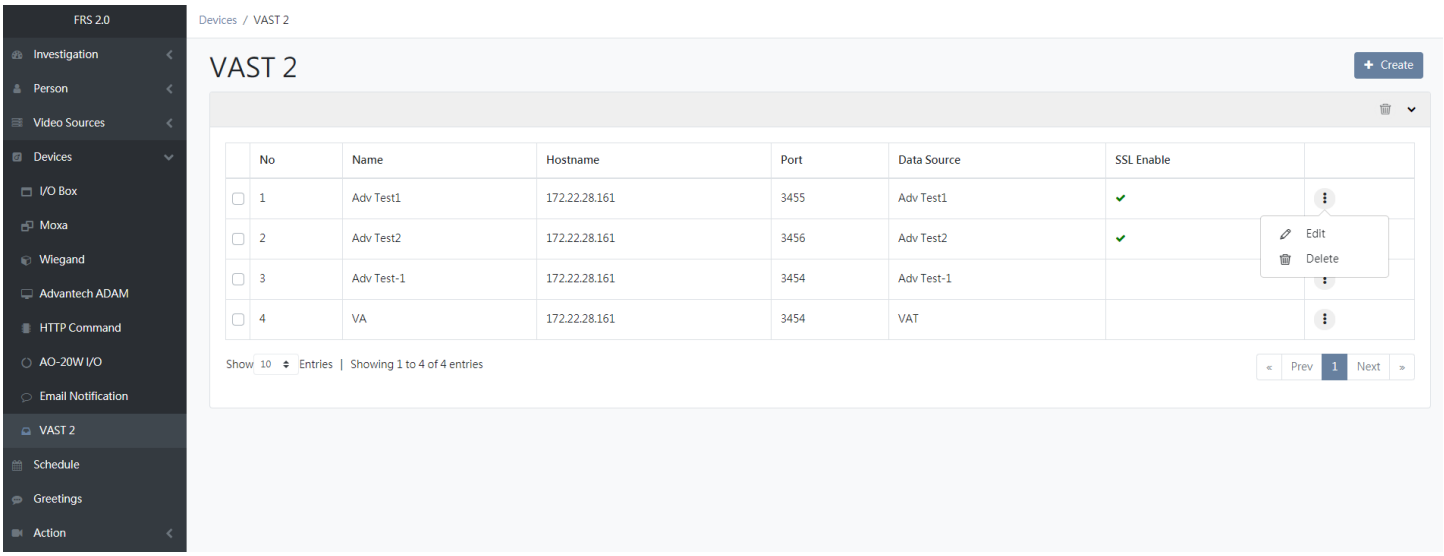


FIGURE 3.54 Device – VAST 2 list

4. In order to see a VAST 2 complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected VAST 2 full details will be displayed.

5. Edit any profile information as needed.

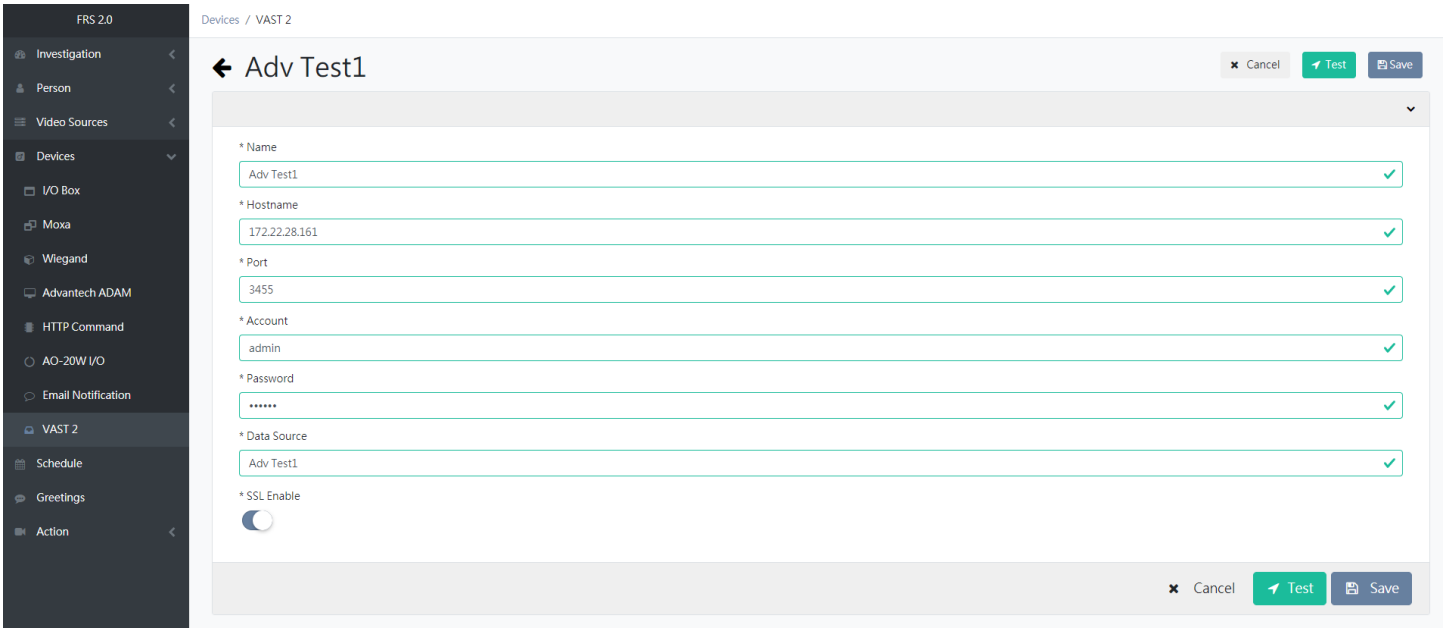


FIGURE 3.55 Device – VAST 2 details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

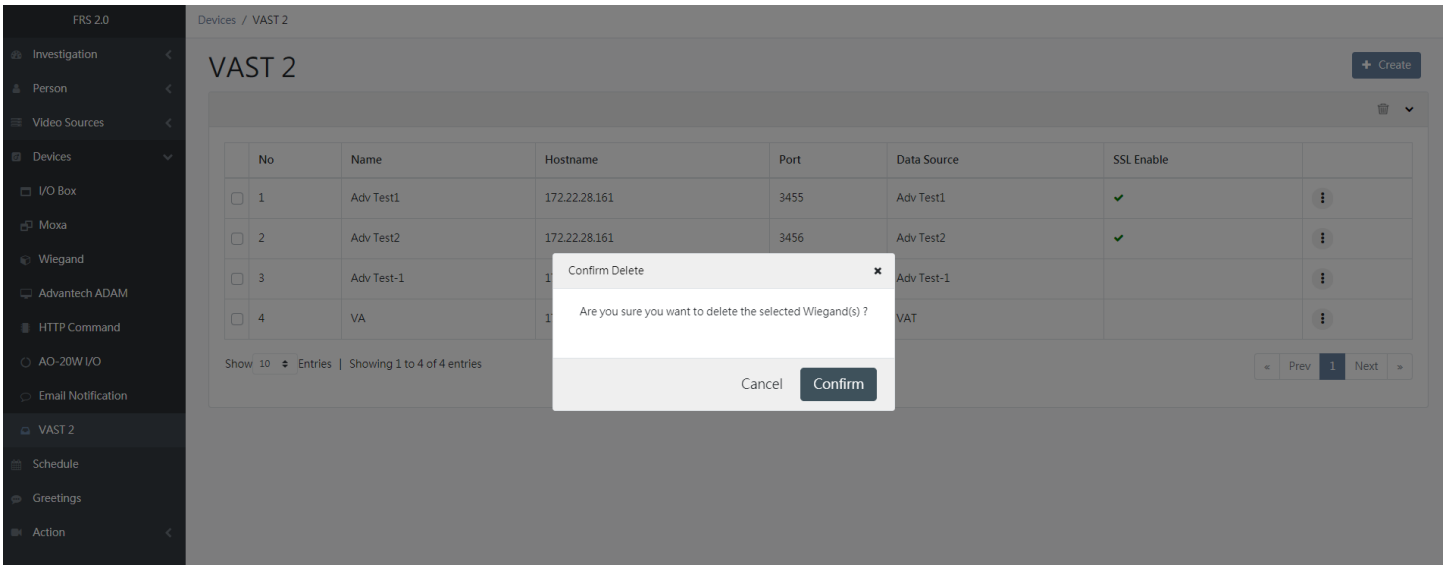


FIGURE 3.56 Device delete VAST 2

9. Click on "Confirm" to delete the selected VAST 2 (s).

10. To add a new VAST 2, click on the "+Create" button (+ Create).

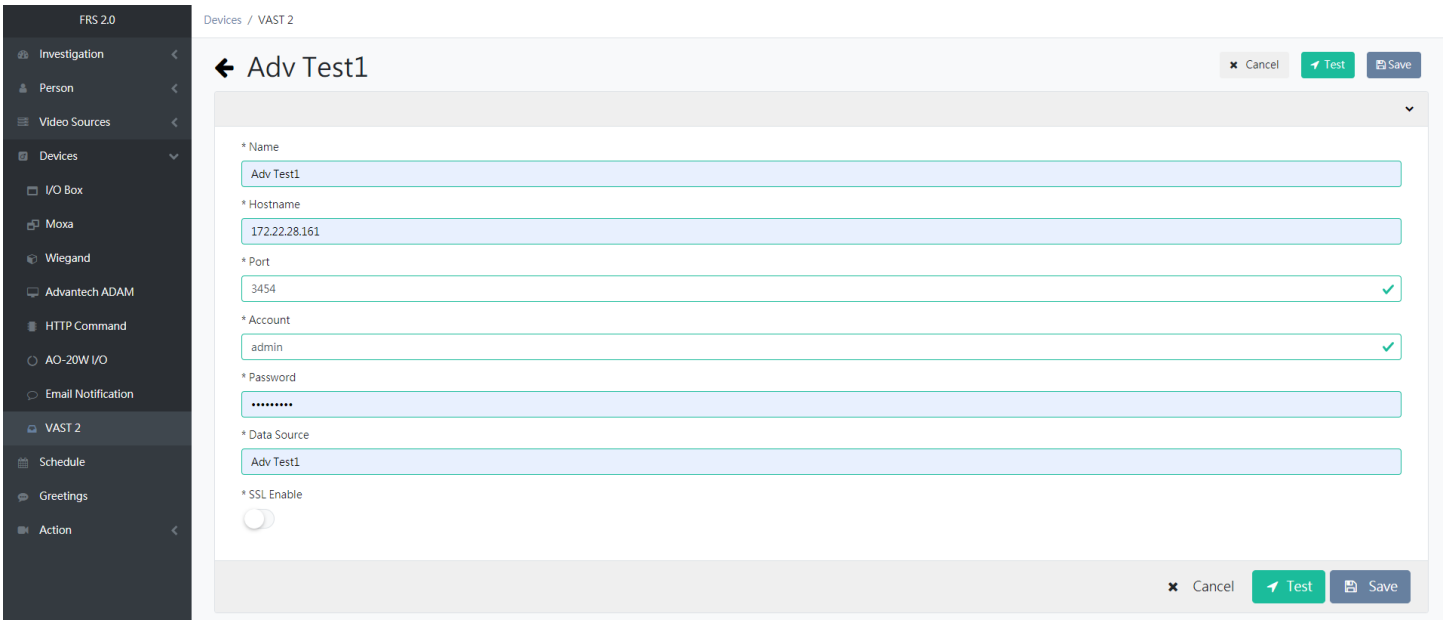


FIGURE 3.57 Device - create VAST 2

11. On the "Create VAST 2" menu, enter the new VAST 2 information:

    a. Name ➡ A user-friendly name to identify this device.

    b. Hostname ➡ The device's communication address.

    c. Port ➡ The device's communication port.

d. Account ➡ An account to connect VAST 2

e. Password ➡ An Password to connect VAST 2

f. Data Source ➡ Set the Data Source name of VAST 2 Client to get the corresponding video source

12. Click "Test" to test whether the IP and Port can connect to the VAST 2 correctly. If the test fails, the device data cannot be saved

13. Click on “Save” to create the VAST 2.

3.6 Schedule Configuration

Note

- Schedule templates are used by VAST Face for multiple purposes, these include:

  A. Define when face recognition devices are allowed to authenticate enrolled staff

  B. Define trigger event responses active time

  C. Define which greeting message should be displayed on Welcome page.

- In general, if no schedule is defined, it is widely understood that the device, rule or greeting will run continuously

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Schedule" menu ➡ A list of all created Schedule will be displayed.

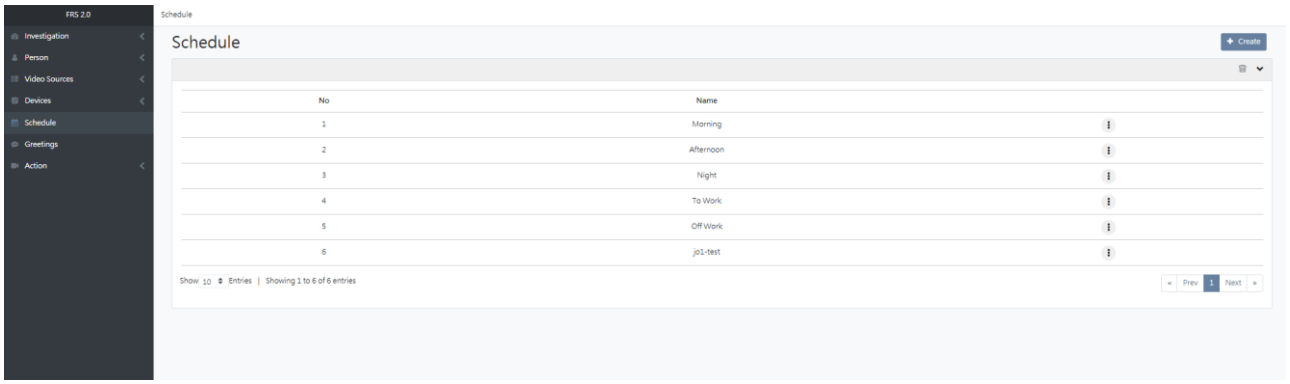


FIGURE 3.58 Schedule List

4. In order to see a Schedule complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected Schedule full details will be displayed.

5. Edit any profile information as needed.

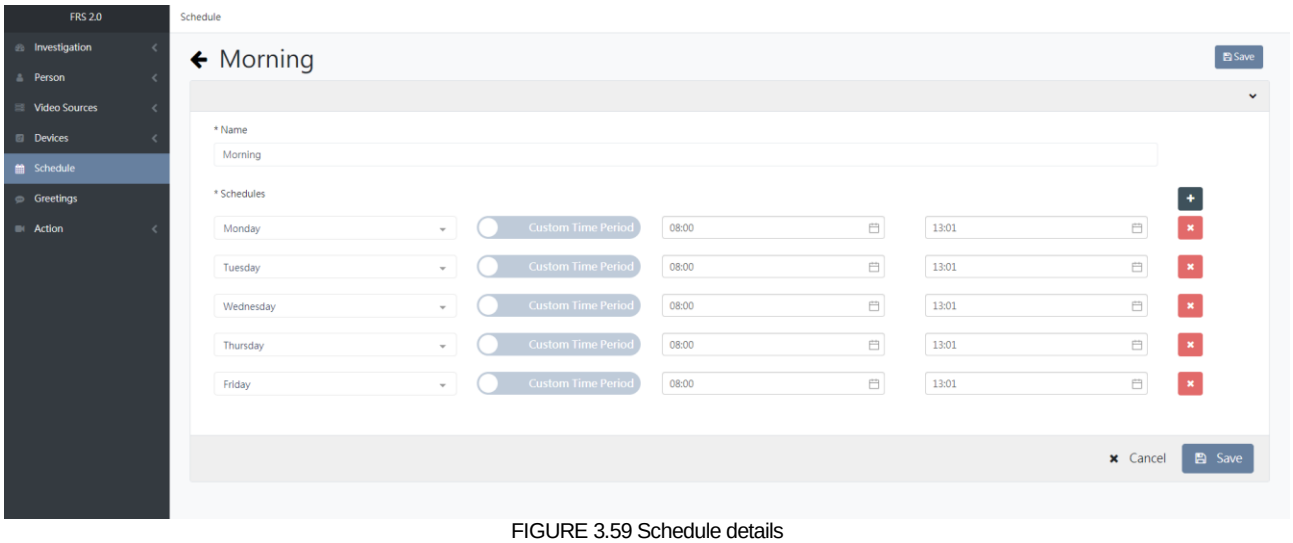


FIGURE 3.59 Schedule details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon ( ), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

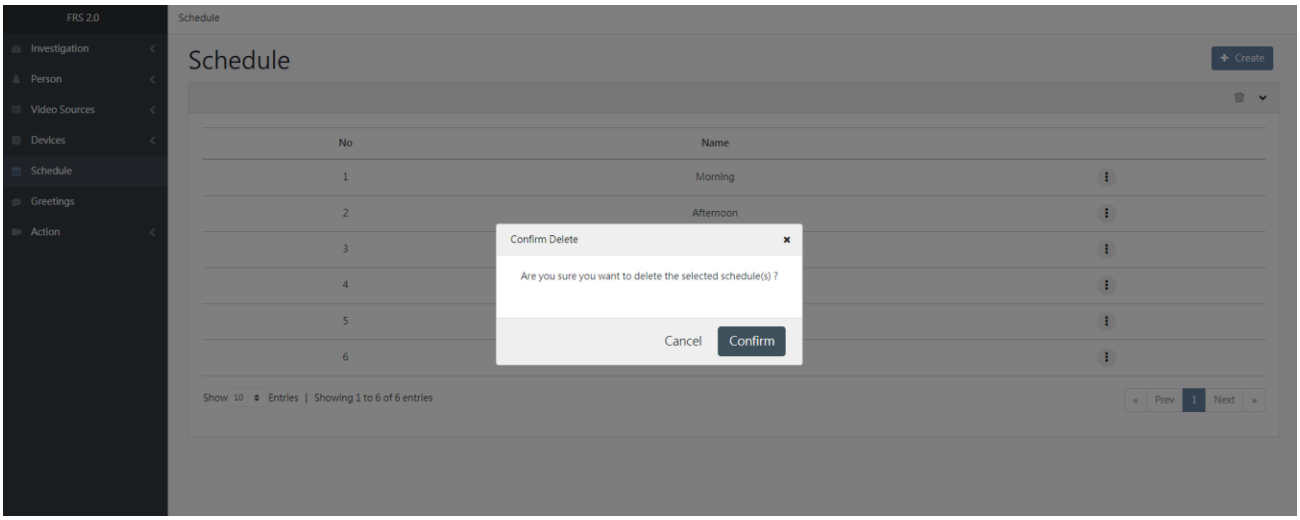


FIGURE 3.60 Delete Schedule

9. Click on "Confirm" to delete the selected Schedule (s).

10. To add a new Schedule, click on the "+Create" button (+ Create).

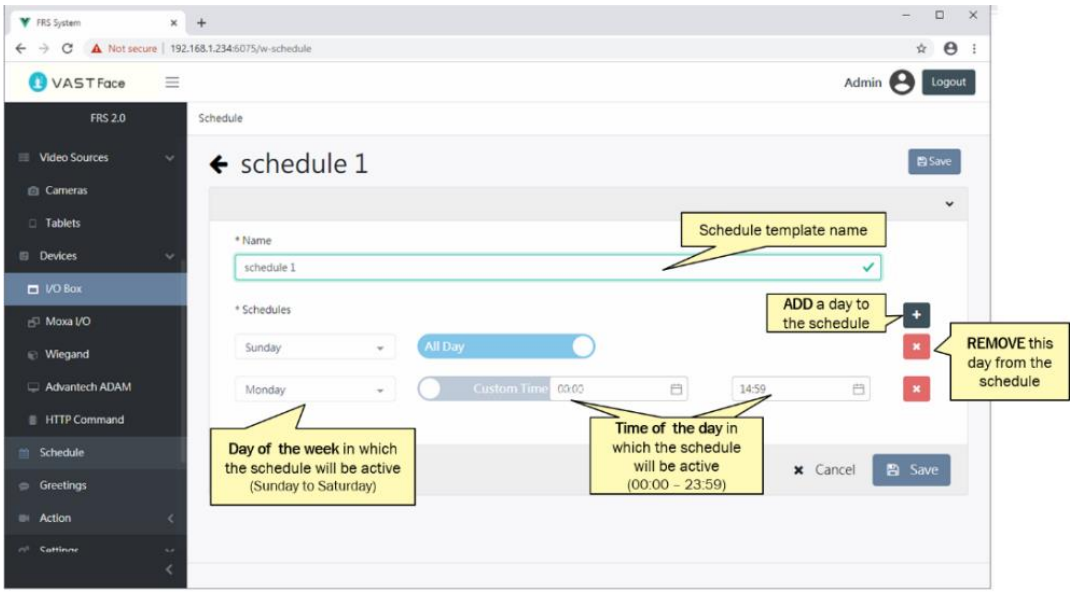


FIGURE 3.61 create Schedule

11. On the "Create Schedule" menu, enter the new Schedule information:
    a. Name ➡ A user-friendly name to identify this schedule template.
    b. Day of the week ➡ The day of the week in which the schedule template will be active.
    c. Time of The Day ➡ The time range of the day in which the schedule template will be active.
12. Add as many days, and time ranges as needed, and click on "Save" to apply changes.

3.7 Greetings Management

Greetings refer to the different welcome messages that Digital Signage client can display to greet upon recognizing an enrolled person, based on their group affiliation and/or pre-defined schedule.

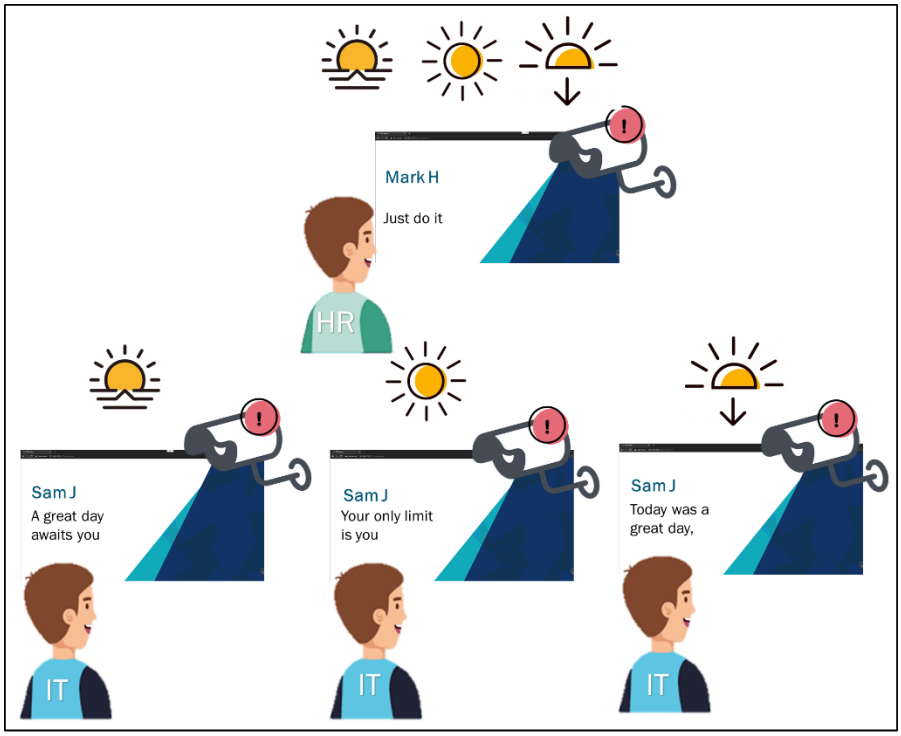


FIGURE 3.62 Greetings concept explained.

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Greetings" menu ➡ A list of all created Greetings will be displayed.

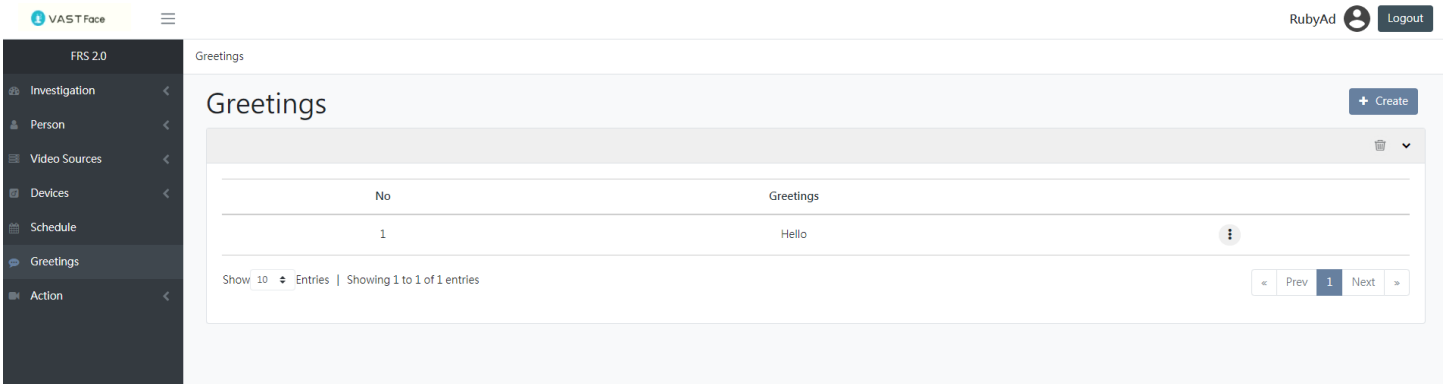


FIGURE 3.63 Greetings LIST

4. In order to see a Schedule complete details, click on the "Profile Details" icon ( ), and select Edit, the selected Schedule full details will be displayed.

5. Edit any profile information as needed.

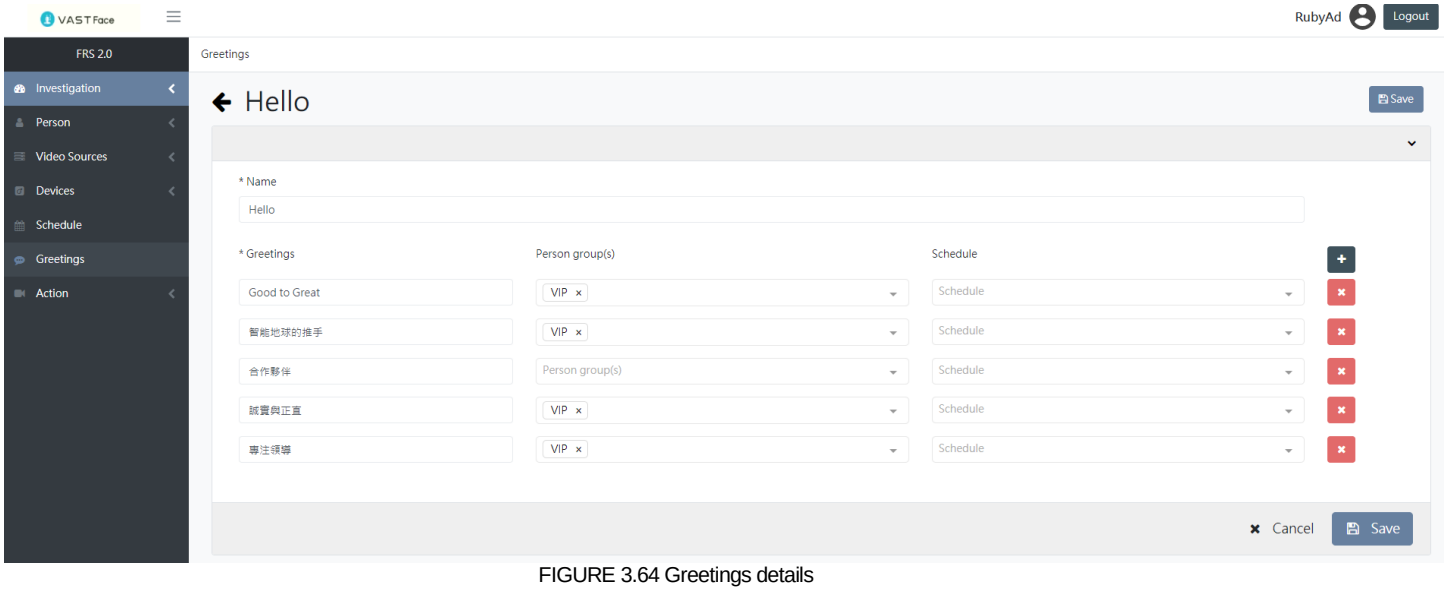


FIGURE 3.64 Greetings details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon ( ), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

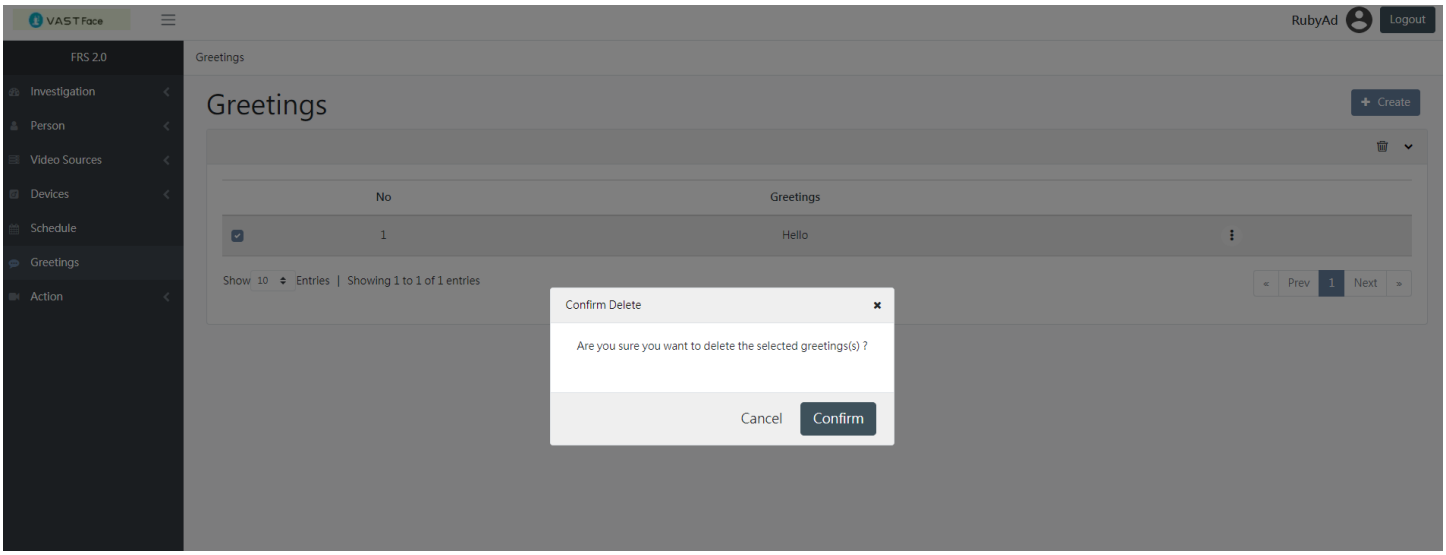


FIGURE 3.65 Delete Greetings

9. Click on "Confirm" to delete the selected Schedule (s).

10. To add a new Schedule, click on the "+Create" button (+ Create).

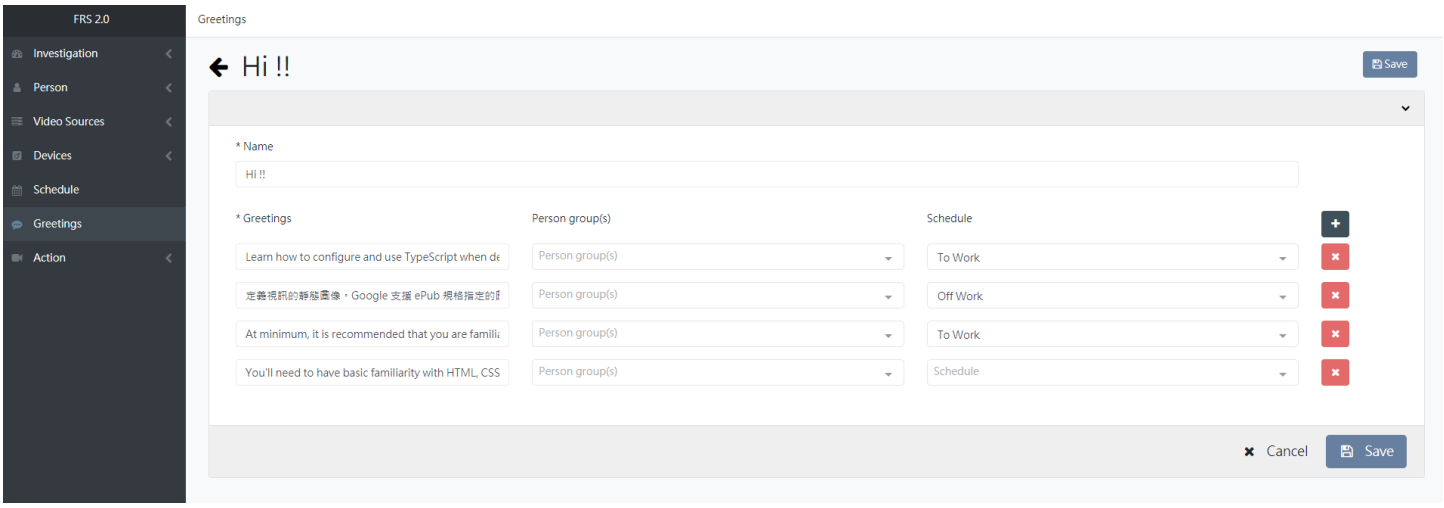


FIGURE 3.66 Create Greetings

11. On the "Create Schedule" menu, enter the new Schedule information:
    a. Name ➡ A user-friendly name to identify this welcome message.
    b. Greetings ➡ The welcome message that is to be displayed on the digital signage upon recognizing a person.
    c. Person group(s) ➡ The face group to which the recognized person must be affiliated to in order to display the greeting message.
    d. Schedule ➡ The schedule template during which this greeting message will be displayed.
12. Click on "Save" to apply changes.

3.8 Action

After adding the devices or commands that should triggered into VAST Face, a condition for when to trigger these actions (trigger rule) must then be specified.

3.8.1 Video Source

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Action" menu ➡ "Video Source" , a list of all created video source will be displayed.

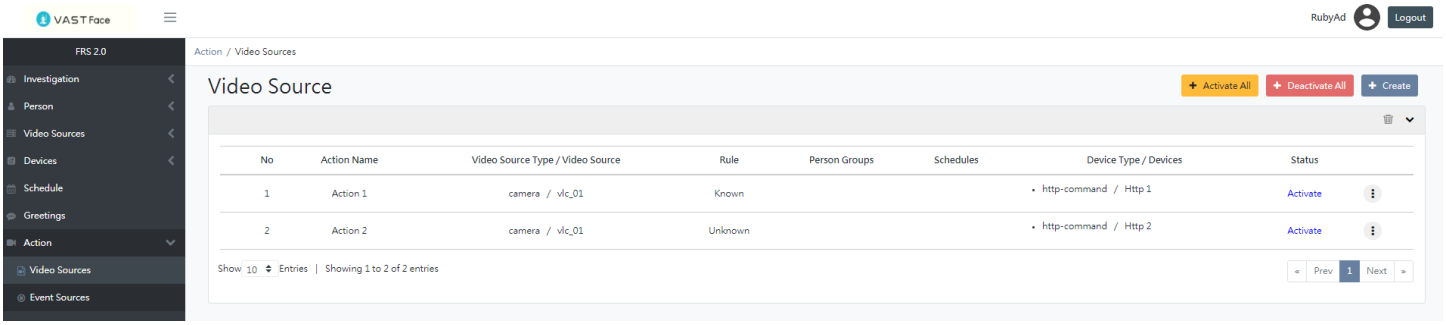


FIGURE 3.67 ACTION – VIDEO SOURCES LIST

4. In order to see a video source complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected video source full details will be displayed.

5. Edit any profile information as needed.

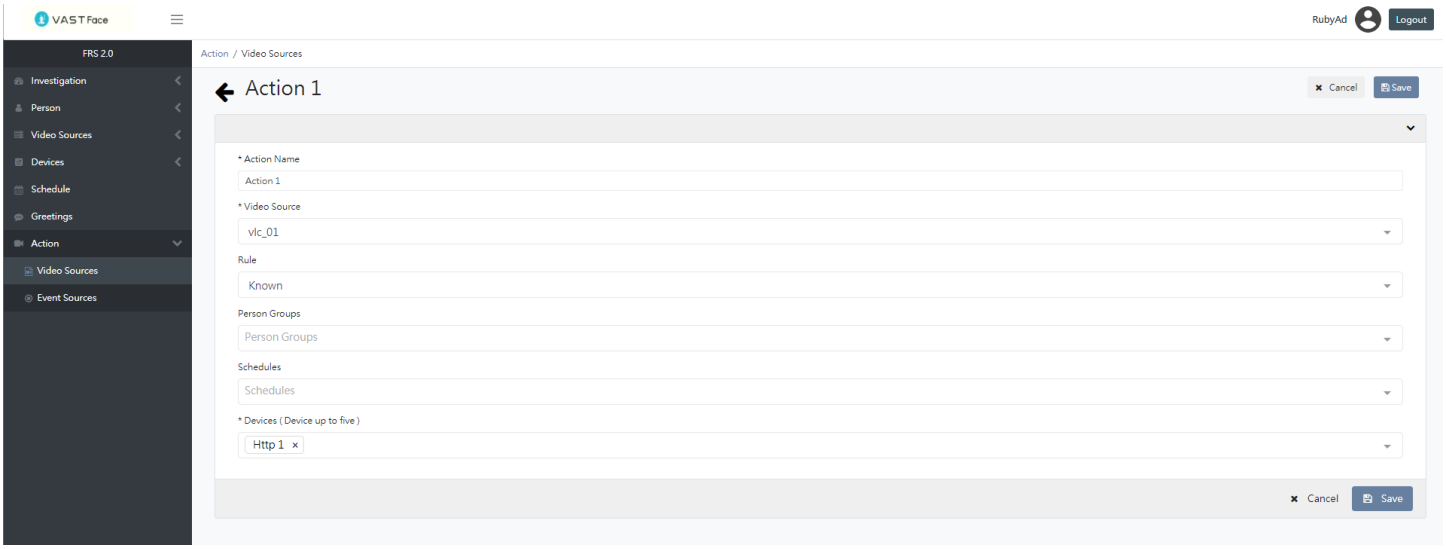


FIGURE 3.68 ACTION – VIDEO SOURCES details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

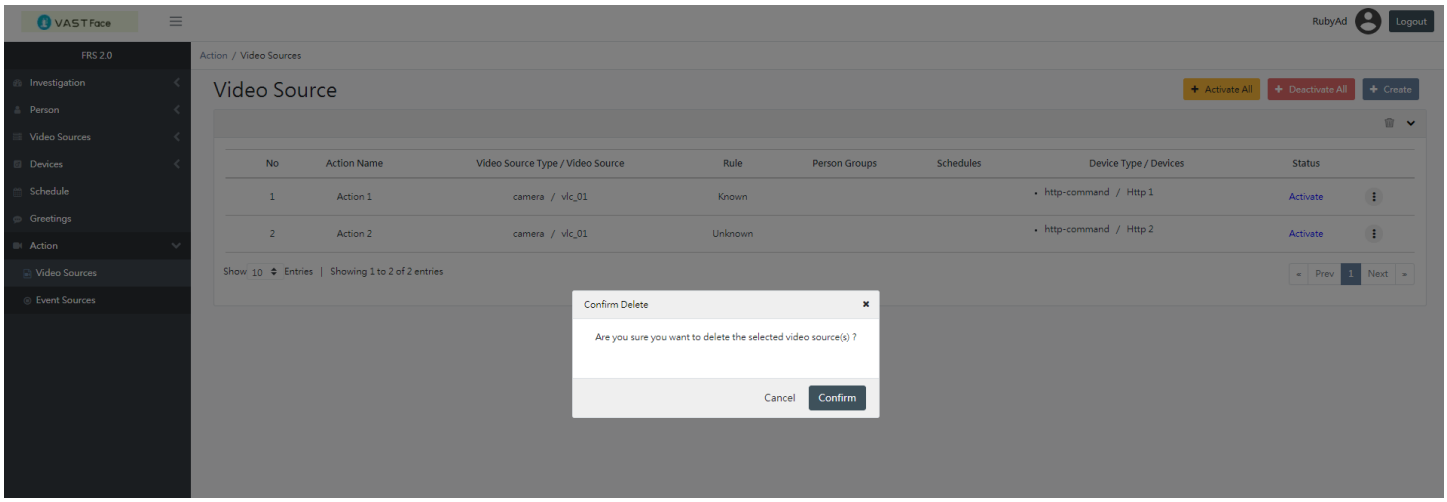


FIGURE 3.69 Delete ACTION – VIDEO SOURCES

9. Click on "Confirm" to delete the selected video source (s).

10. To add a new video source, click on the "+Create" button (+ Create).

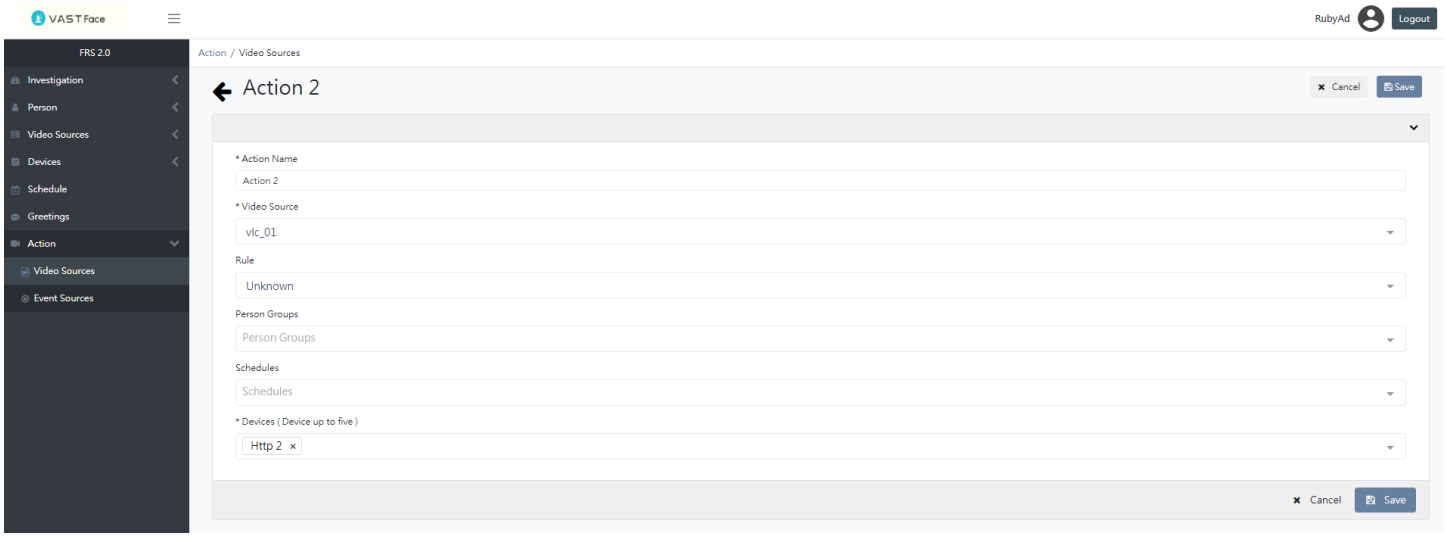


FIGURE 3.70 Create ACTION – VIDEO SOURCES

11. On the "Create video source" menu, enter the new video source information:

    a. Action Name ➡ A user-friendly name to identify this trigger rule.

    b. Video Source ➡ The IP Camera or Face Recognition Tablet whose face recognition matching results will be used as input to trigger this rule.

    c. Rule ➡ Face recognition event type that will be used to trigger this rule.

    d. Person Groups ➡ Face groups that will be used to trigger this rule.

Face Type		Person Group	Rule Definition
Known	+	No group selected	Trigger event rule when any system enrolled person is detected, regardless of face group affiliation
Known	+	With specific group(s) selected	Trigger event rule only when a member of a specific face group(s) is detected i.e. : trigger only when VIP face group members are detected
Unknown	+	No group selected	Trigger event rule when any unregistered person's face is detected
Unknown	+	With specific group(s) selected	Trigger event rule only when a person that's not part of a specific face group(s) is detected i.e. : trigger only when non VIP face group members are detected

e. Schedule ➡ The schedule in which the selected rule will run, if no schedule is selected the rule will run continuously.

f. Devices ➡ The ancillary devices or HTTP commands that will be triggered (can select up to 5, per rule).

12. Click on "Save" to apply changes.

備註

- Once the video source action is set, you can switch the action to "Enable" or "Disable" according to your needs.

3.8.2 Event Sources (This is available when VAST Face is controlled by FRSM.)

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using an Administrator account.

3. Navigate to "Action" menu ➡ "Event Source" , a list of all created event source will be displayed.

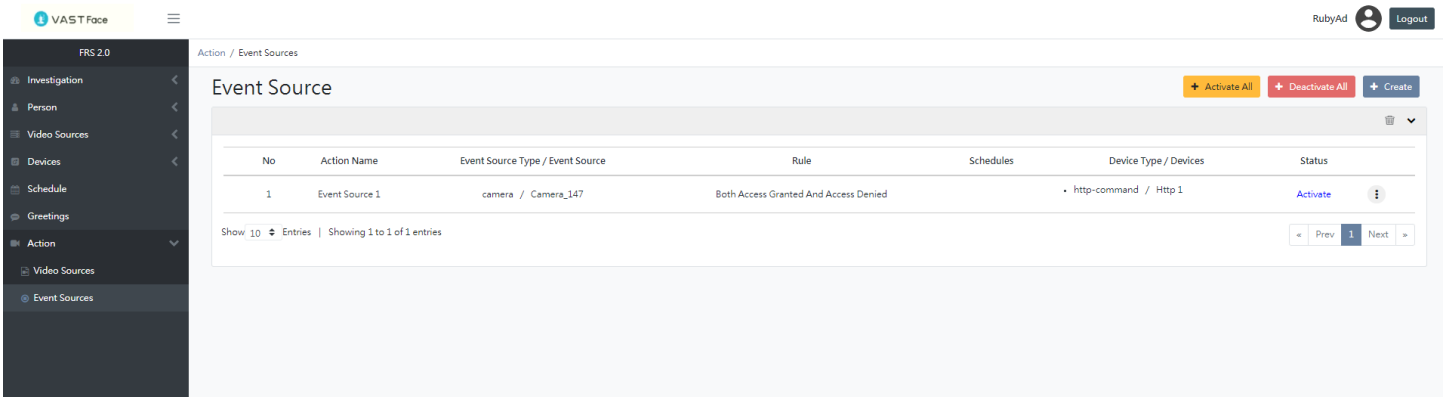


FIGURE 3.71 ACTION – EVENT SOURCES LIST

4. In order to see a event source complete details, click on the "Profile Details" icon (⋮), and select Edit, the selected event source full details will be displayed.

5. Edit any profile information as needed.

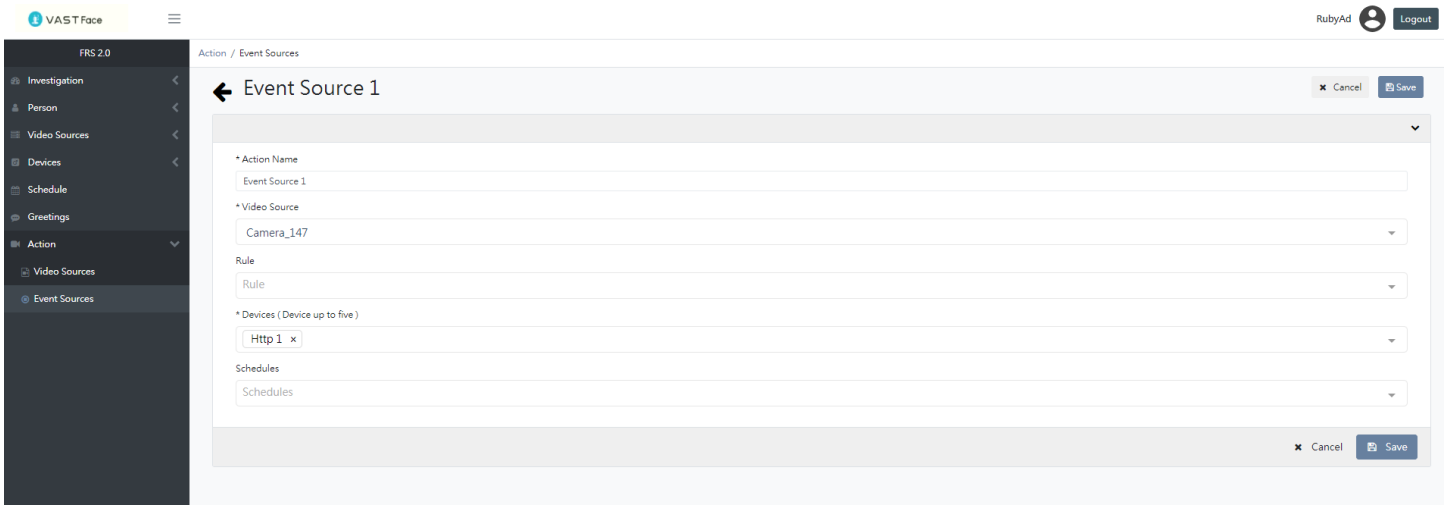


FIGURE 3.72 ACTION – EVENT SOURCES details

6. Click on "Save" to apply changes.

7. To Delete a profile, click on the "Profile Details" icon (⋮), and select Delete (Delete).

8. A pop-up window will appear on-screen prompting the user to confirm the action.

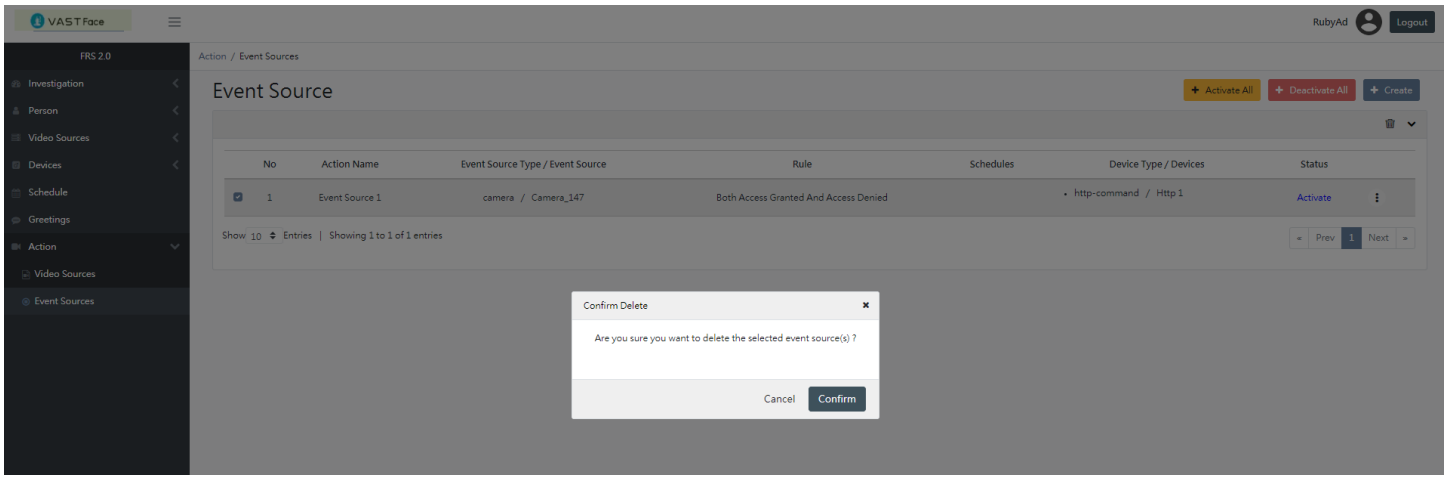


FIGURE 3.73 Delete ACTION – EVENT SOURCES

9. Click on "Confirm" to delete the selected event source (s).

10. To add a new event source, click on the "+Create" button (+ Create).

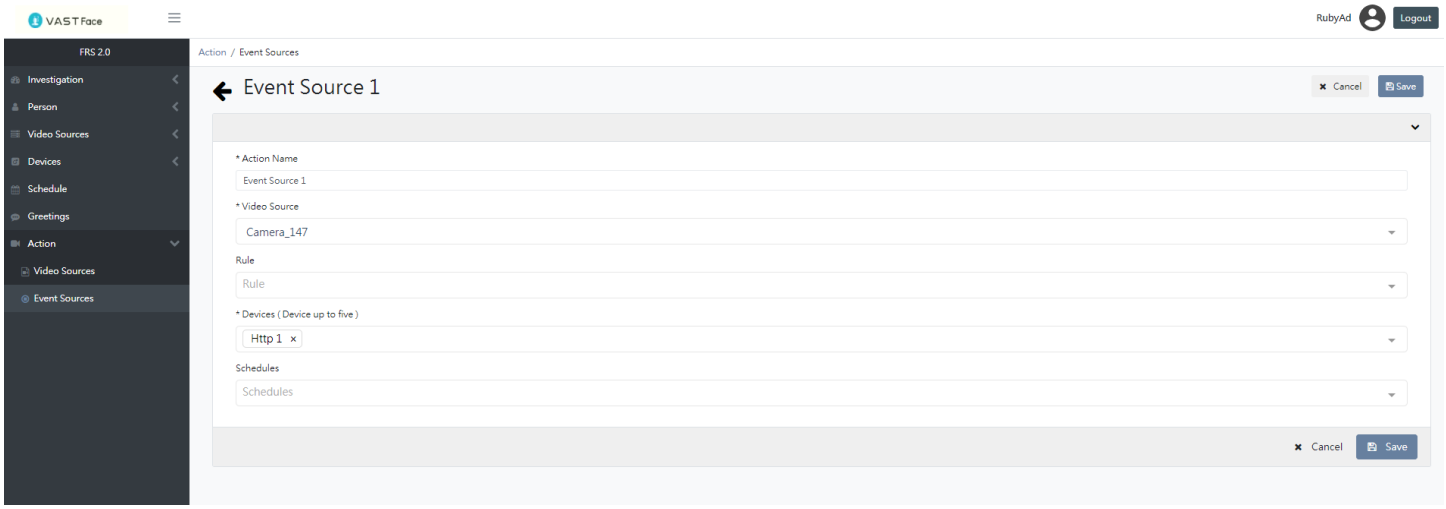


FIGURE 3.74 Create ACTION – EVENT SOURCES

11. On the "Create event source" menu, enter the new event source information:
    a. Action Name ➡ A user-friendly name to identify this trigger rule.
    b. Video Source ➡ The IP Camera or Face Recognition Tablet whose face recognition matching results will be used as input to trigger this rule.
    c. Rule ➡ Face recognition event type that will be used to trigger this rule.
    d. Person Groups ➡ Face groups that will be used to trigger this rule.

e. Schedule ➡ The schedule in which the selected rule will run, if no schedule is selected the rule will run continuously.

f. Devices ➡ The ancillary devices or HTTP commands that will be triggered (can select up to 5, per rule).

12. Click on "Save" to apply changes.

3.9 Settings (System Admin Only)

3.9.1 System

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "System" , system setting item will be displayed.

    a. FRS Management control ➡ Shows whether the VAST Face is under the FRSM.

    b. Location ➡ Name of the FRSM binding

    c. Person Investigation data retention policy ➡ The personnel investigation data will be cleared when the time limit is exceeded

    d. Action Investigation data retention policy ➡ The action investigation data will be cleared when the time limit is exceeded

    e. Attendance End Of Day ➡ Set the time from which the daily attendance time is determined to end

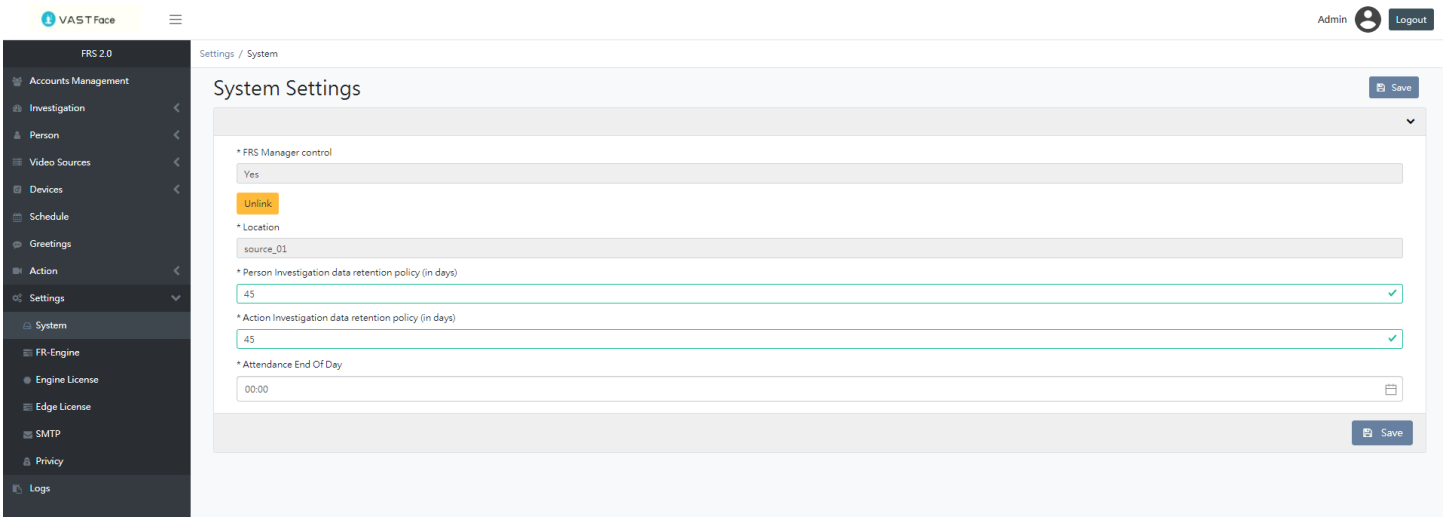


FIGURE 3.75 Setting – System

4. Click on "Save" to apply changes.

3.9.2 FR-Engine

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "FR-Engine" , FR-Engine setting item will be displayed.
    a. Protocol ➡ The protocol to be connected (HTTP/HTTPS)
    b. Hostname ➡ Host address of the Face Recognition Engine to be connected
    c. Port ➡ The port number of the Face Recognition Engine to be connected
    d. WS Port ➡ WS port number of the Face Recognition Engine to be connected

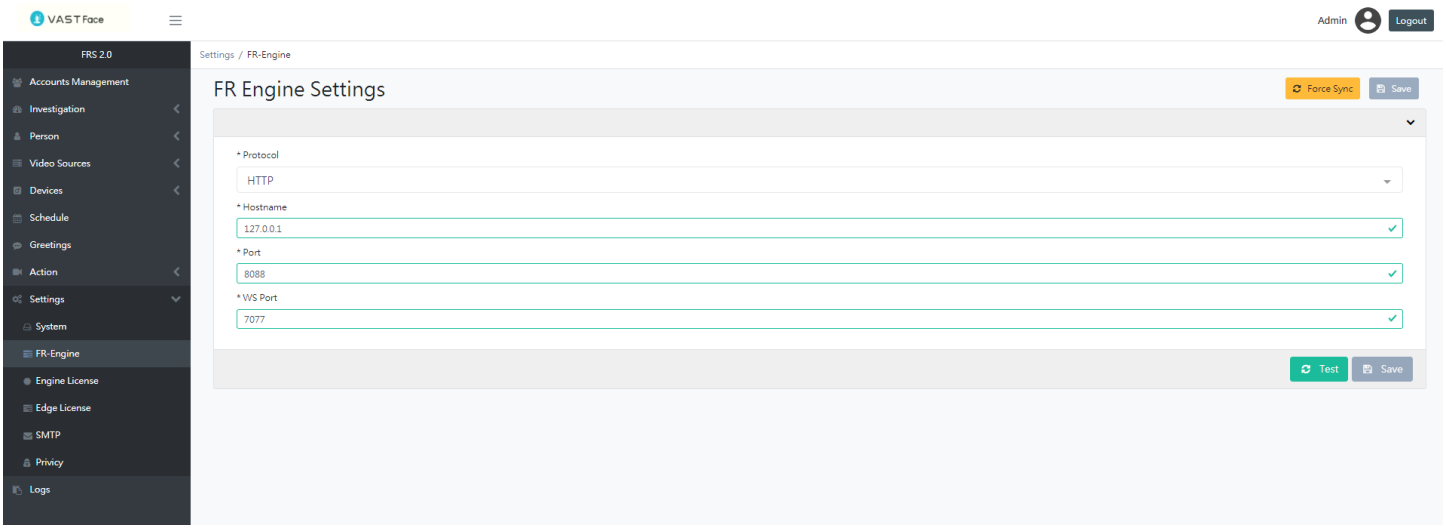


FIGURE 3.76 Setting – FR Engine Settings

4. Click on "Save" to apply changes.

3.9.3 Engine License

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "Engine License" , a list of all added Engine License will be displayed.

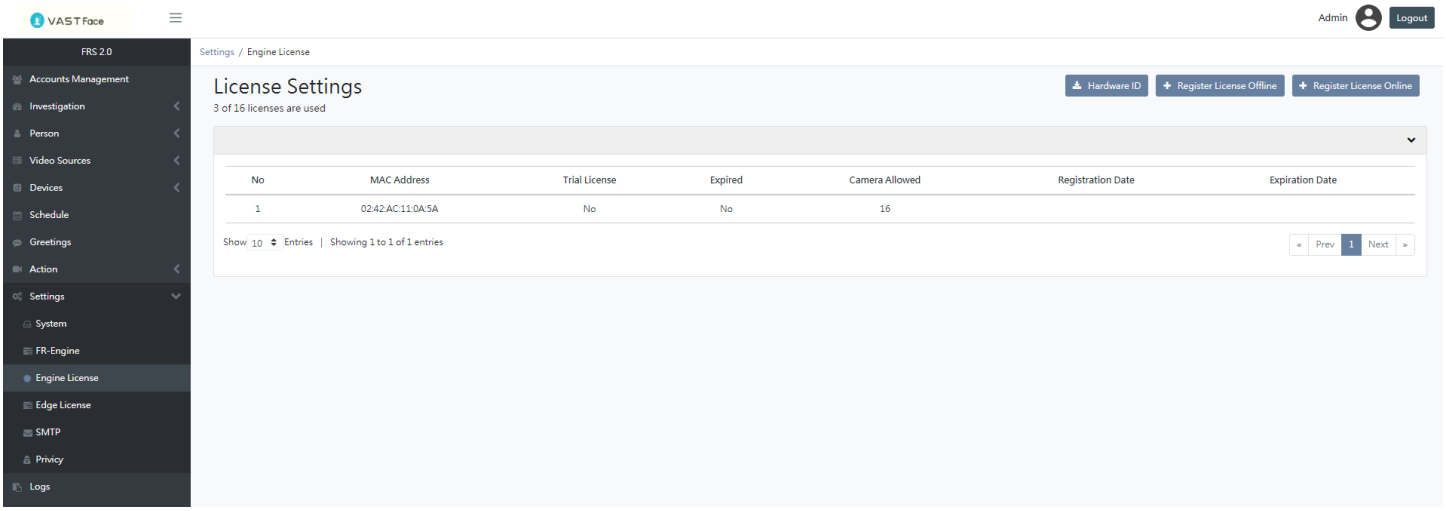


FIGURE 3.77 Setting – FR Engine License Setting

4. To add a new engine license online, click on the "Register License Online" button (+ Register License Online).

5. Register License Online Information:

   a. License Key ➡ Engine License Registration Key

   b. MAC Address ➡ VAST Face MAC address

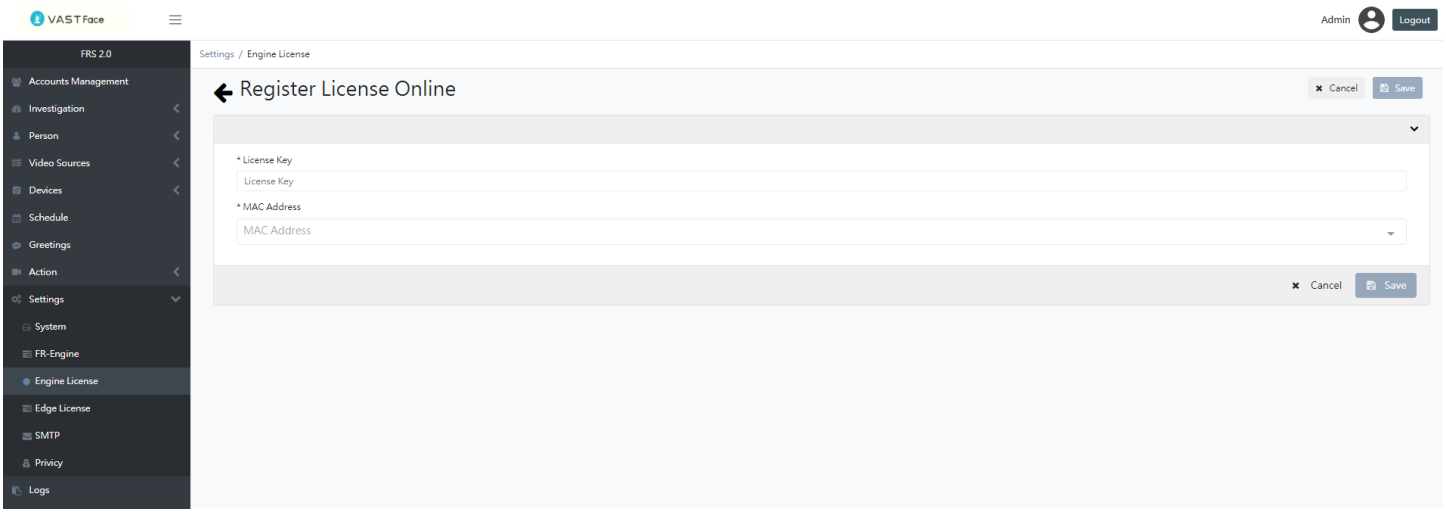


FIGURE 3.78 Setting – Register License Online

6. Click on "Save" to apply changes.

7. To add a new engine license offline, click on the "Register License offline " button (+ Register License Offline).

8. Register License Offline Information:

    a. Upload Engine Offline License Key File ➡ Upload Engine Offline License Key File (.lic)

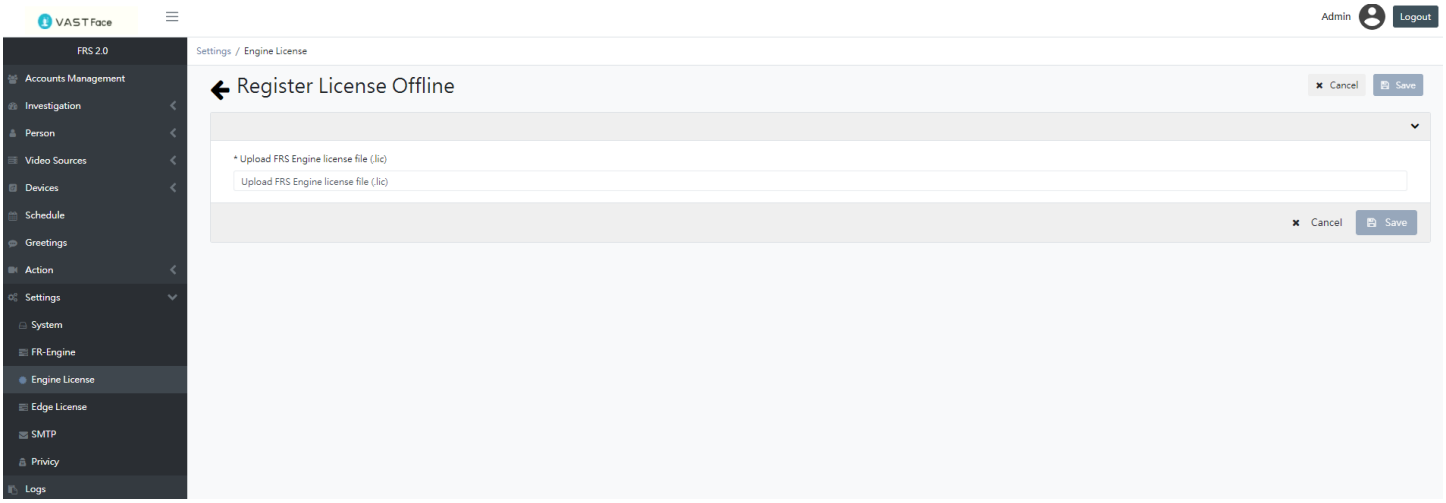


FIGURE 3.79 Setting – Register License Offline

9. Click on "Save" to apply changes.

3.9.4 Edge License

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "Edge License" , a list of all added Edge License will be displayed.

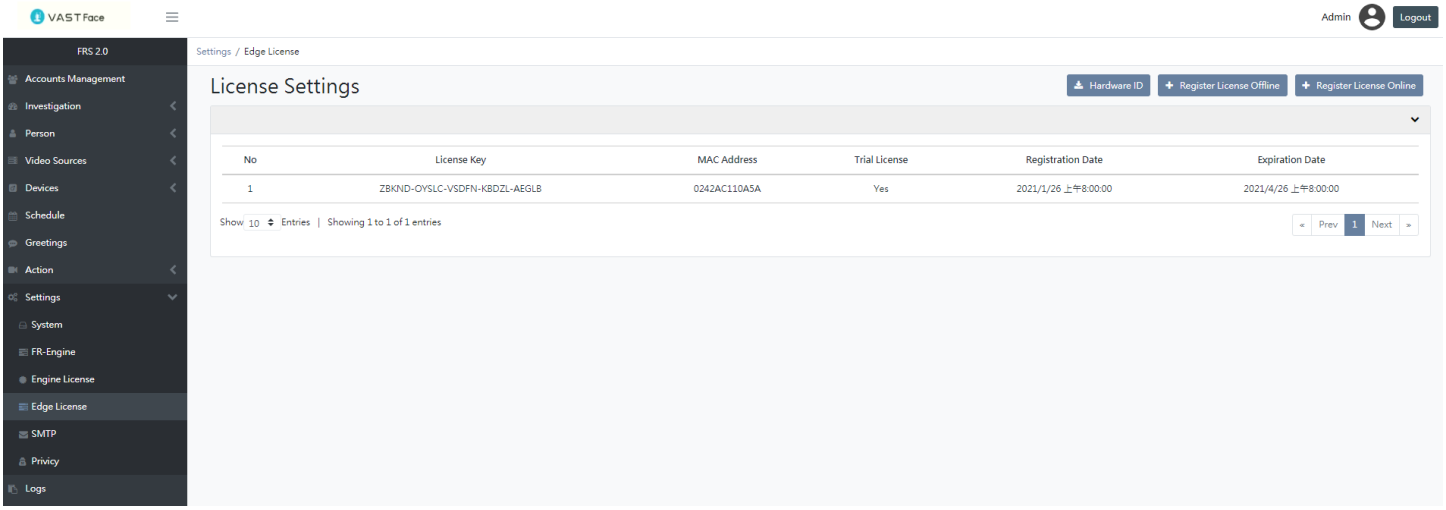


FIGURE 3.80Setting – VAST Face License Settings

4. To add a new Edge license online, click on the "Register License Online" button (Register License Online).

5. Register License Online Information:

   a. License Key ➡ Engine License Registration Key

   b. MAC Address ➡ VAST Face MAC address

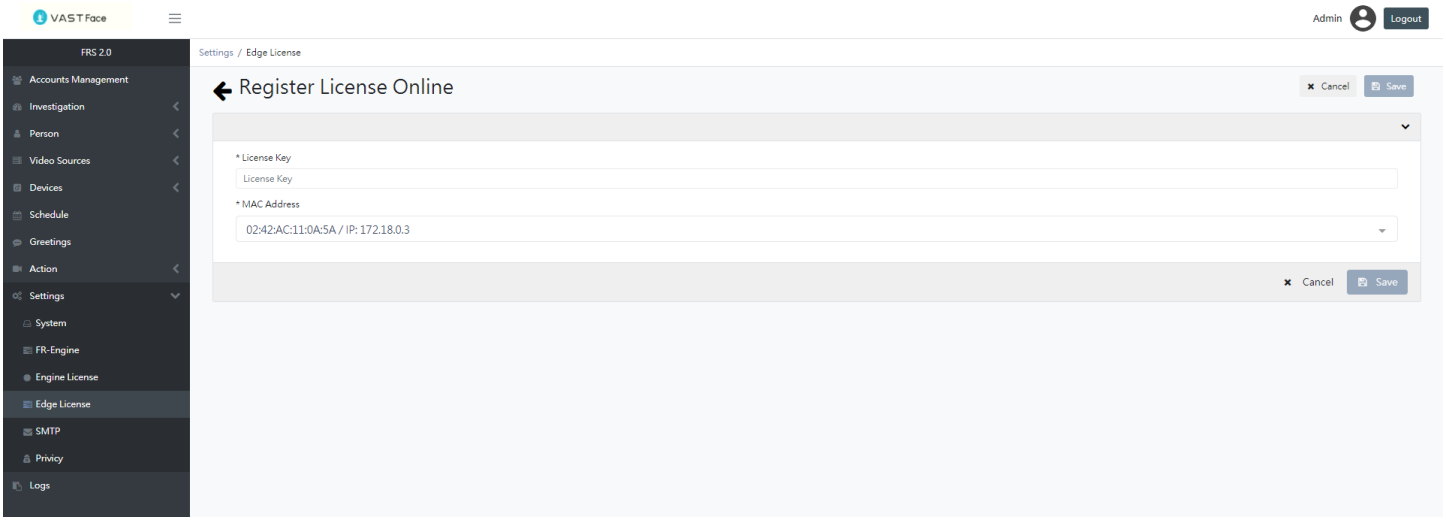


FIGURE 3.81 Setting – Register License Online

6. Click on “Save” to apply changes.

7. To add a new Edge license offline, click on the "Register License offline " button (+ Register License Offline).

8. Register License Offline Information:

    a. Upload Engine Offline License Key File ➡ Upload Engine Offline License Key File (.lic)

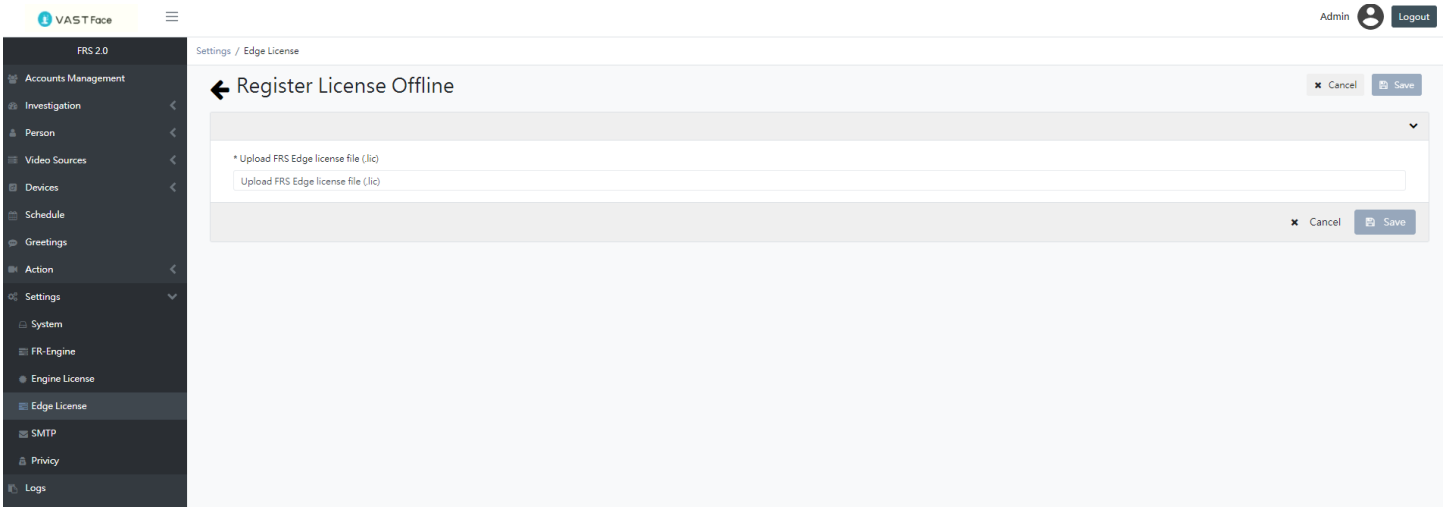


FIGURE 3.82 Setting – Register License Offline

9. Click on “Save” to apply changes.

3.9.5 SMTP

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "SMTP" , SMTP setting item will be displayed.
    a. Hostname ➡ The host address of the SMTP server
    b. Port ➡ SMTP server's connection port
    c. Email ➡ Provide the sender's email account for sending notification letters
    d. Password ➡ Provide the sender's password for sending notification letters

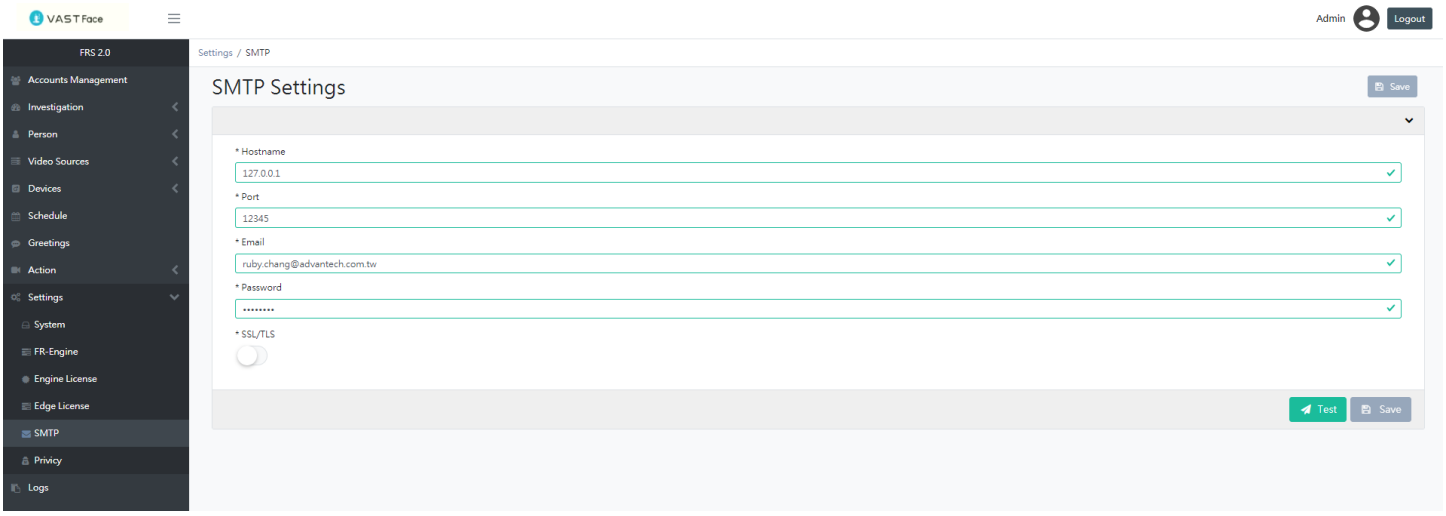


FIGURE 3.83 Setting – SMTP

4. Click "Test" to test whether the mailbox can be sent normally, if the test fails, SMTP data cannot be saved.

5. Click on "Save" to apply changes.

3.9.6 Privacy

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Settings" menu ➡ "Privacy" , Privacy setting item will be displayed.

    a. Hide registered photo➡ After opening, you can change the default photo by yourself, and the registration photo will be hidden in the personnel information and the default photo will be displayed.

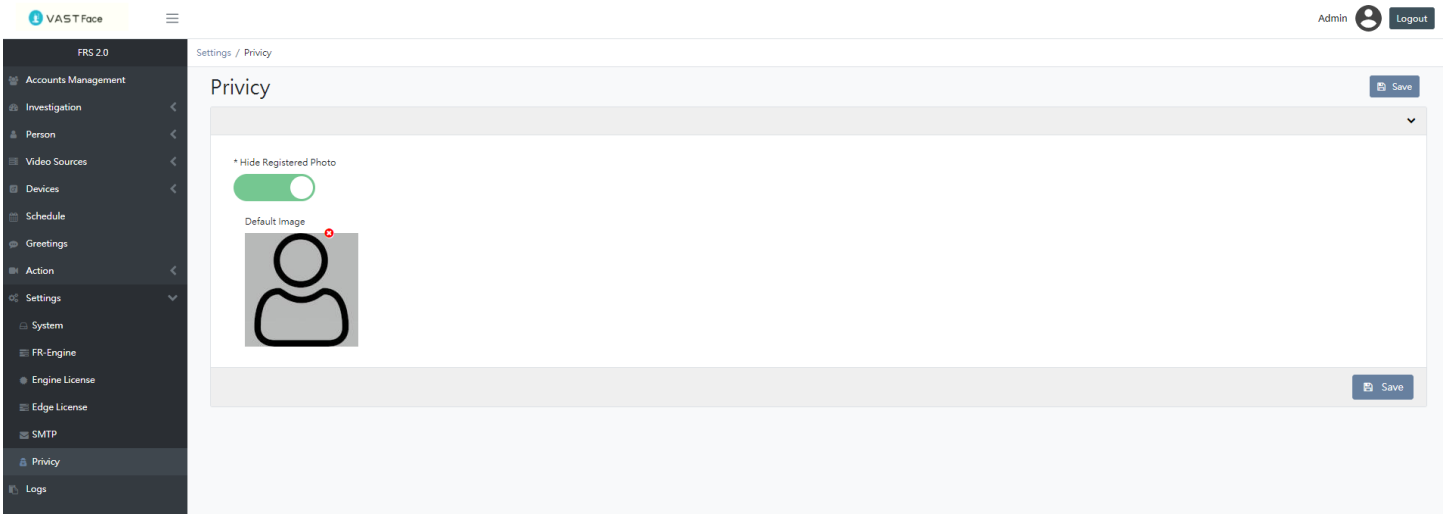


FIGURE 3.84 Setting – Privacy

4. Click on "Save" to apply changes.

3.10 Log (System Admin Only)

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075), VAST Face login page will be displayed.

2. Login to VAST Face using a System Admin account.

3. Navigate to "Log" menu ➡ A list of all system log will be displayed.

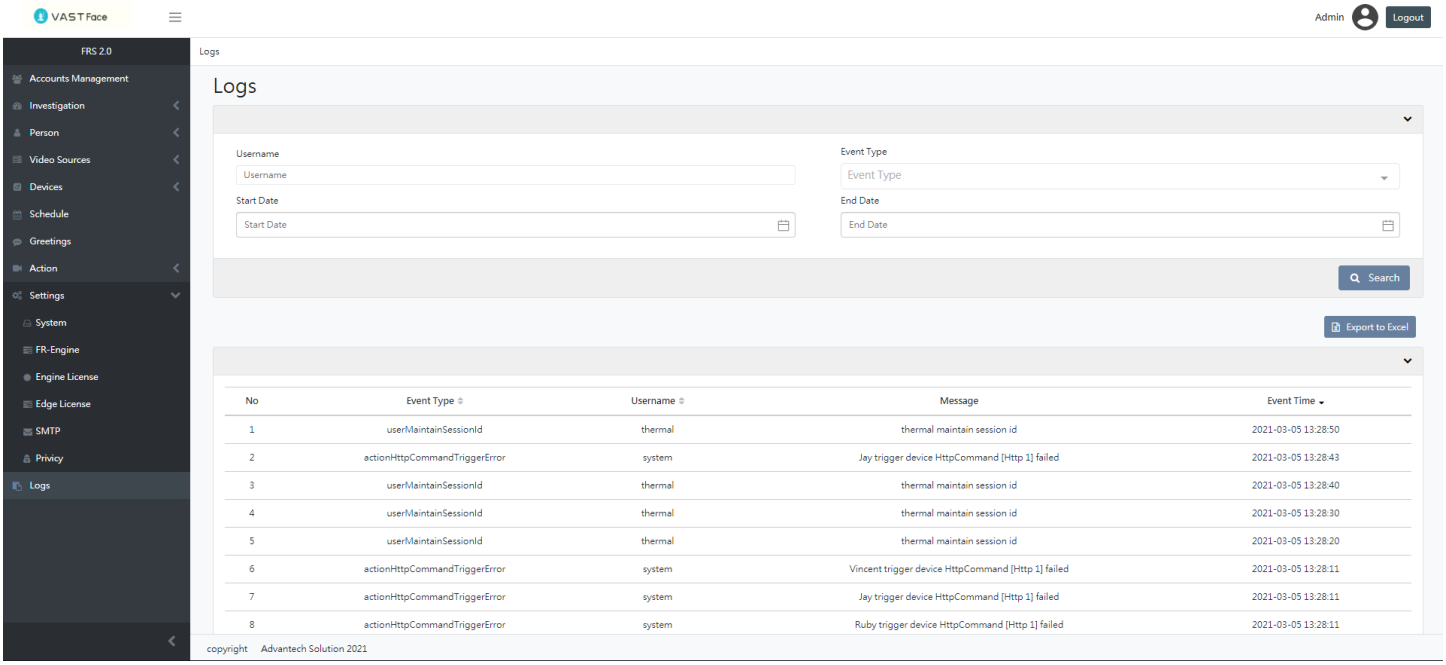


FIGURE 3.85 Logs List

4. Use the Display filters to narrow down results by: Username, Event Type, Start Date, or End Date.

5. Click on the search button ()button, to display only logs matching the filter criteria.

6. To export the logs, click the "Export to Excel" button, it will export to .XLSX file.

Chapter 4

4 VAST Face Troubleshooting

This chapter outlines the procedures for troubleshooting VAST Face system

4.1 Accessing VAST Face Logs

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address ,port 6075 and URL path /server/log (e.g.: http://192.168.1.152:6075/server/log) , a prompt window will appear.

2. Login to VAST Face using the System Admin credentials (user: "Admin", password: "Az1235671!").

3. The server logs page will be displayed, with the different logs grouped based on the last server restart date.

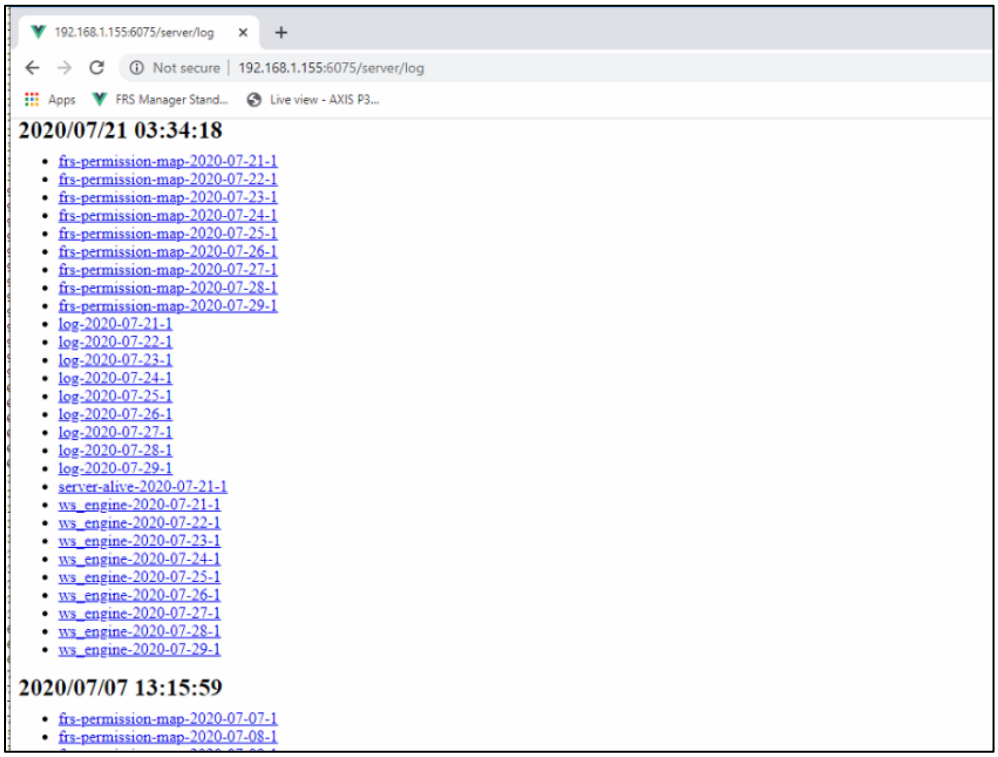


FIGURE 4.1 VAST Face logs page.

Note

- VAST Face log files are created on a daily basis, and though the system contains multiple logs types designed for different purposes, out of all the logs, the files named: log-YYYY-MM-DD, are by far the most important.

4. Click on the most recent log file, and browse for any error or warning messages that could indicate some problem.

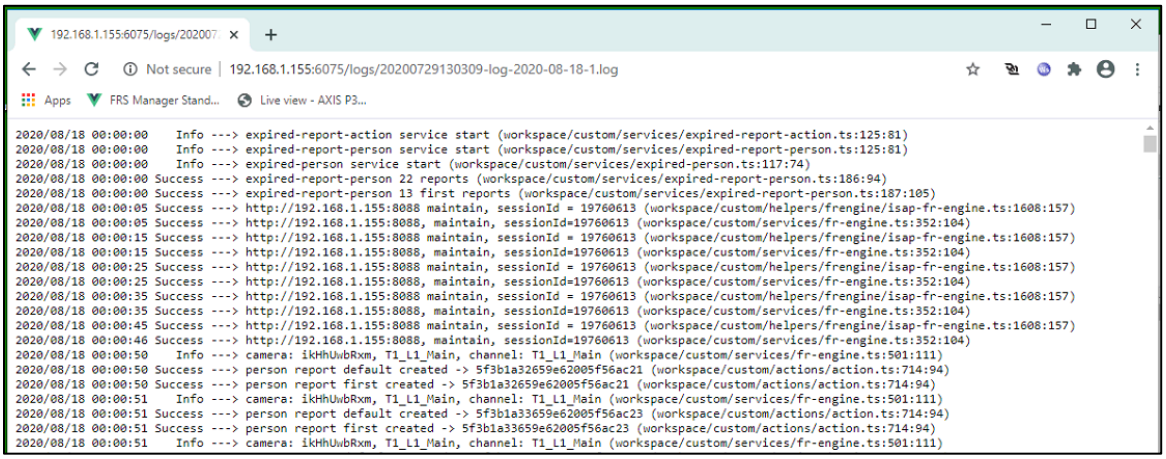


FIGURE 4.2 VAST Face logs.

4.2 VAST Face Version

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 (e.g.: http://192.168.1.152:6075) , VAST Face login page will be displayed.

2. Login to VAST Face using System Admin credentials (user: "Admin", password: "Az1235671!").

3. Click on the Avatar icon ( ), located on the top right corner, to display the user's profile information.

4. Click on the Information icon ( ) to see VAST Face and client version.

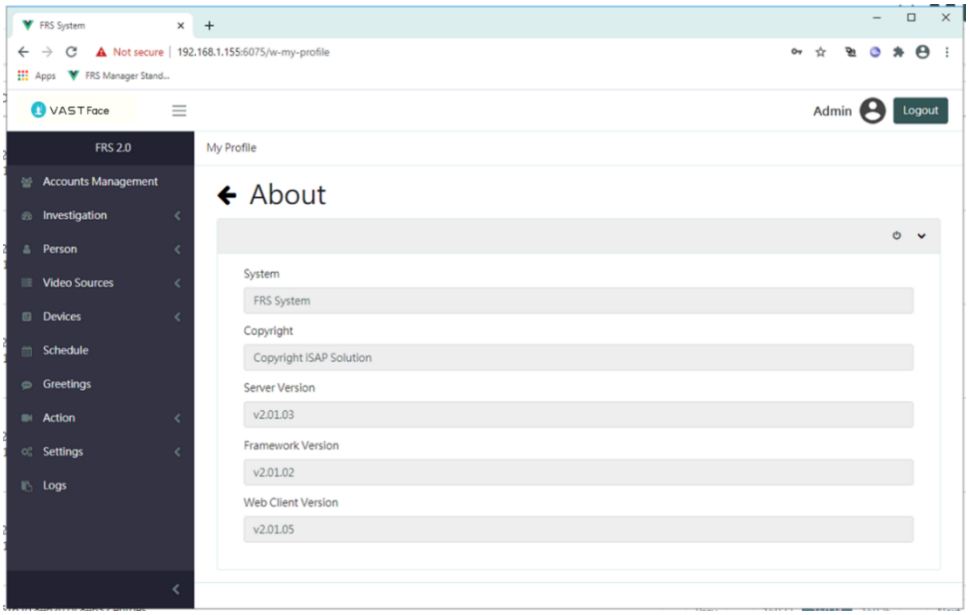


FIGURE 4.3 VAST Face system version

4.3 Restart VAST Face

1. On a Windows PC computer, open Google Chrome and navigate to VAST Face IP Address port 6075 with URL path bye (e.g.: http://192.168.1.152:6075/server/bye) , a prompt window will appear.

2. Login to VAST Face using System Admin credentials (user: "Admin", password: "Az1235671!").

3. A "bye" confirmation message indicates that the server is being rebooted.

4. Wait for 1-2 minutes for the server to complete booting.

FIGURE 4.4 VAST Face reboot.

Note

- Alternatively, VAST Face can be restarted from Docker portainer, or by pressing the "server restart"

  ( ) button located under the server version panel.

4.4 Verify IP camera's RTSP Stream

1. On a Windows PC computer, download and install VLC Player.

2. Click on "Media" menu ➡ "Open Network Stream".

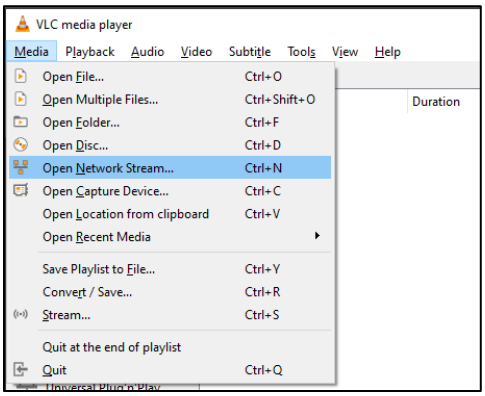


FIGURE 4.5 VLC Player Open Network Stream

3. Key in the IP camera's full RTSP URL stream including credentials, and click on "Play"

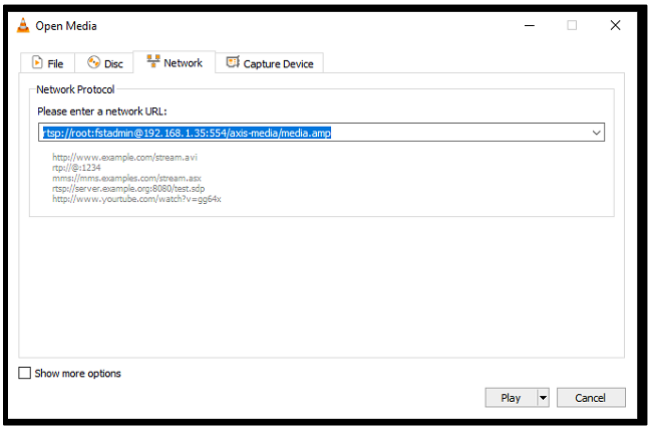


FIGURE 4.6 IP Camera RTSP URL in VLC Player

4. If the RTSP URL is correct, live video from the camera will start shortly.

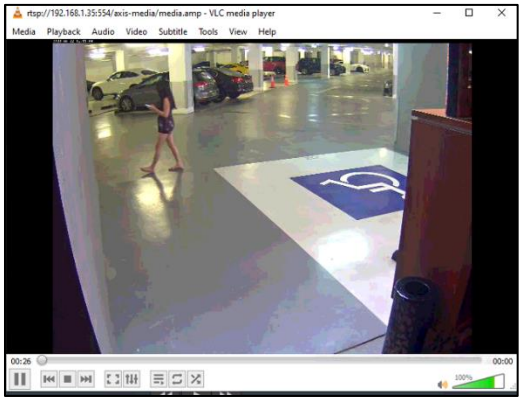


FIGURE 4.7 IP camera live video stream in VLC player