Synology®

Administrator's Guide for

Face Recognition

Based on

Synology Surveillance Station 9.0

Table of Contents

Introduction	**01**
Camera Quick Installation	**02**
Camera Placement and Environment	**04**
Configure Software Settings	**05**
Search and Manage Recognition Results	**11**
Reports	**15**
Appendix	**17**

Introduction

With its powerful AI Image Analysis, Synology Deep Video Analytics (DVA) can instantly calculate large amounts of object attributes, filter out environmental interferences, and deliver accurate detection results.

Among the supported algorithms, Face Recognition is designed to identify customers, employees, or suspicious persons to deliver better services and enhance security.

For you to achieve optimal precision, this guide aims to introduce the key factors of setting up Face Recognition tasks. For best results, please follow the listed points as closely as possible.

System Requirements

- DVA series NAS with Surveillance Station version 9.0 or later.
- Synology's Face Recognition application (installed by default).

Note: No additional licenses required for Face Recognition application.

Camera Quick Installation

Step 1

Select appropriate camera

Stream Quality 1920x1080@20 FPS or above

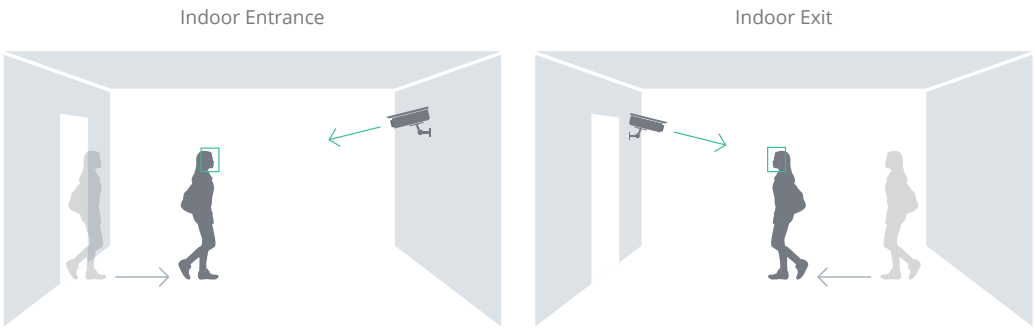
Optical Zoom Lens (Optional) Used to capture clearer facial images when pedestrians are far away

Step 2

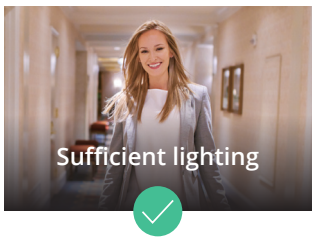
Check installation environment

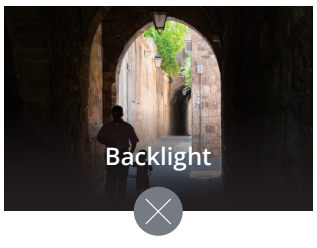
Minimum Illumination 300 lux

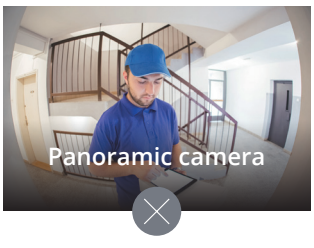
Installation Location/Direction Directly face the flow of pedestrians through the indoor entrance/exit to capture front-facing images



Do’s and Don’ts







Step 3

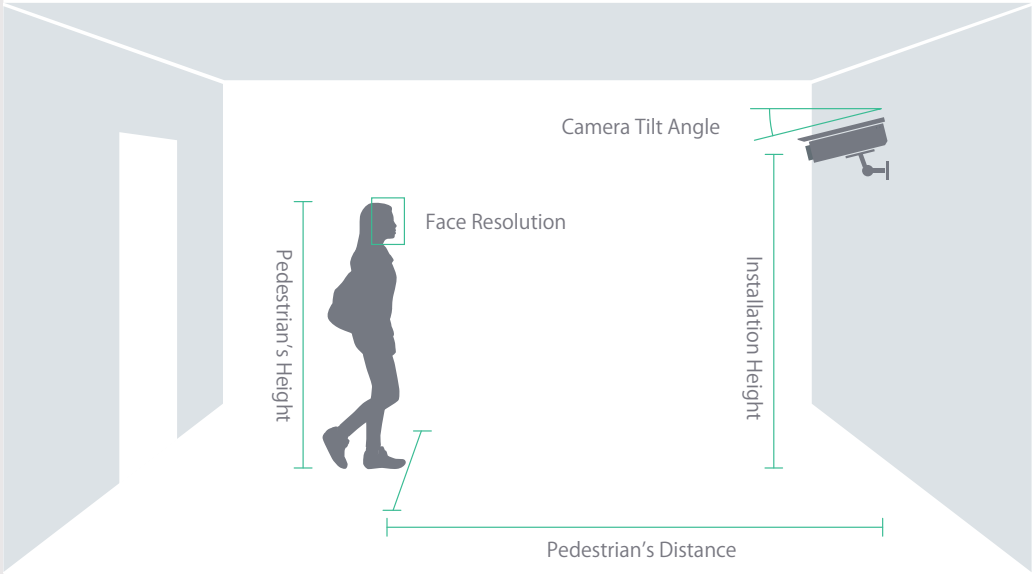
Mounting height and angle

Installation Height 1.5 ~ 3 meters

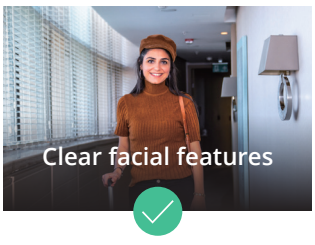
Camera Tilt Angle Less than 15 degrees

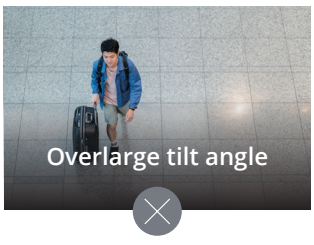
Face Resolution At least 75 × 75 pixels (ideally 125 × 125 pixels)

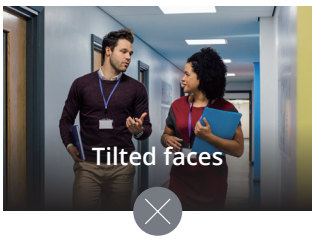
*The values provided are for reference only; please adjust the installation height/angle using actual camera configurations that can provide a clear face resolution.

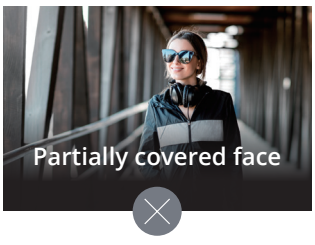


Do's and Don'ts









Camera Placement and Environment

It is possible that faces will not be detected or will be wrongly recognized even with thorough planning of the camera placement and environment. The following situations can affect detection and recognition by the AI:

- Light shining directly into the camera's lens may leave streaks in the images or cause overexposure, affecting the picture quality.
- The camera installed in areas where drastic changes in lighting can happen can lead to inconsistent picture quality.
- Overexposed or underexposed facial images can impede recognition by the AI. Backgrounds with yellowing lighting can impede recognition by the AI; white lighting is recommended.
- Pedestrians moving too fast might cause captured facial images to blur.
- Changes in the camera's field of view might affect the video analytic results (e.g., changes in focus or zoom level).
- Weather sometimes affects the clarity of outdoor cameras. Rain and snow, changes in shadows, or differences between day and night can have an impact on detection and recognition.
- An unstable network connection might lead to incomplete or corrupt images. Wired connections are highly recommended.
- Dust, insects, or other stains can block the lens. Keep the lenses clean so that a clear image can be taken.

Configure Software Settings

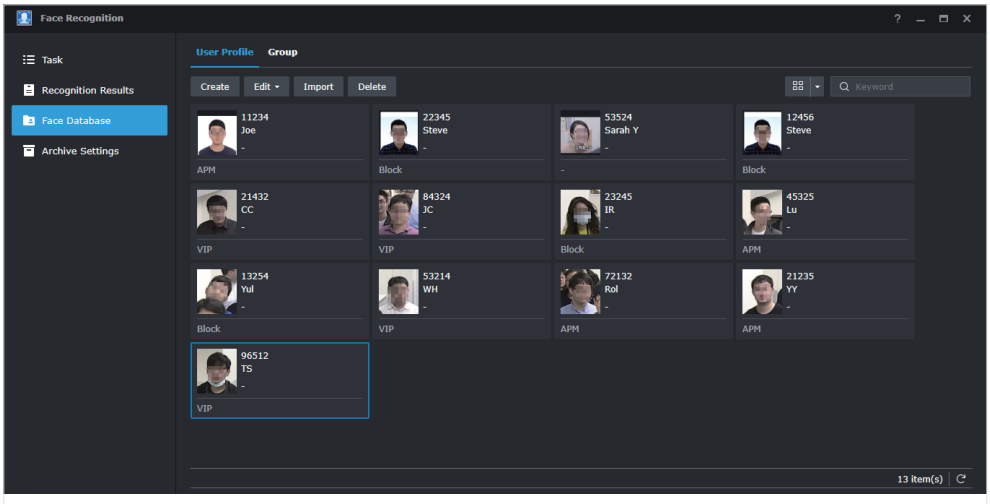
Once your cameras are mounted successfully, you can configure software settings for Face Recognition to suit your requirements. This chapter covers the essential settings for the Face Recognition algorithm.

It is recommended to create a face database first before setting up a Face Recognition task. However, if no previous database information is available, you can also set up a task and create a face database organically from the ground up.

Create Face Database

To identify and classify people into different types of events (**Allowed**, **Blocked**, **VIP** or **Registered**), you need to create user profiles and user groups in Face Database before adding a Face Recognition task. You can create user profiles one by one or import user data and photos by batches.

To manage your **Face Database**, go to **Face Recognition** > **Face Database**.



The most efficient way to build a face database is to import user profiles in batches. When importing profiles in batches, the following options are available:

- Import using a customized profile list
- Import local DSM, domain, or LDAP users

The following specifications are required for the import file (for either of the above import options):

- Account - Each account must be unique, between 1 - 128 characters, and include only Unicode letters, numbers, or the following symbols: . - _ @ \
- Photo File Name - Used to match the uploaded photo to the account.
- Do not modify any cell contents before Row 3. Only the original XLSX format is accepted.

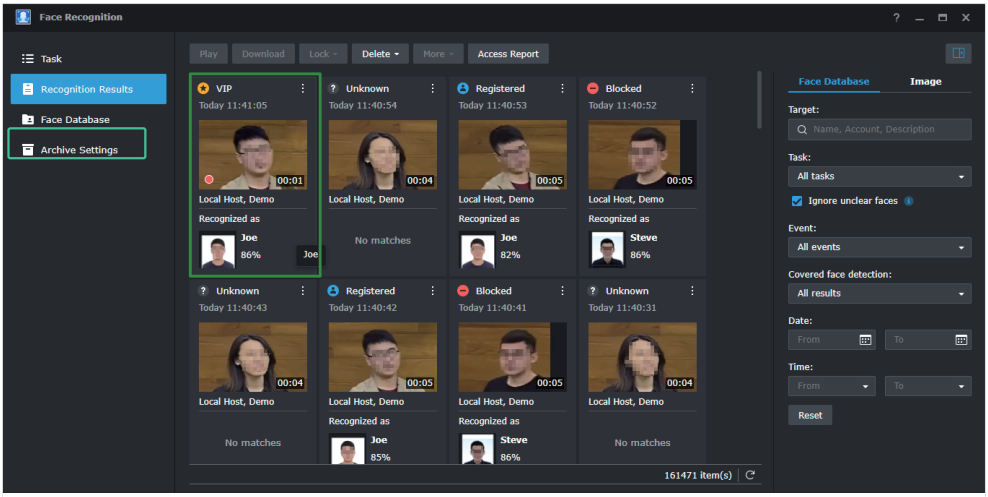
Note: You can also directly import groups or only import new users from DSM, domain, or LDAP.

Define groups

Users in the **Face Database** can be assigned to one or more groups. Groups can be created either manually in the **Face Database** or by importing local DSM, domain, or LDAP users.

Once defined, groups can then be assigned to one of three events in a **Face Recognition Task: Allowed**, **Blocked**, or **VIP**. This allows you to quickly identify outcomes from face recognition results and videos in **Monitor Center**.

For example, if you want to check how many VIPs have appeared within a set period of time, you can filter the event **VIP** in **Recognition Results**. If you are watching a video in **Monitor Center**, VIPs will be framed in a specific color for quick recognition.



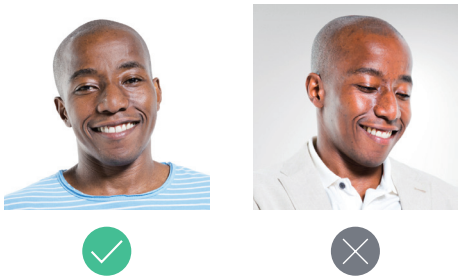
For more information on using groups to quickly identify events, see Registered and Unknown Events.

Note: Each group can only be assigned to one event. If user profiles or groups have been assigned to multiple event lists, they will be marked in the order of **Blocked** > **VIP** > **Allowed**.

Enhance detection accuracy

For best recognition results, a good profile photo should have the following:

- Make sure both the eyes and nose are visible and facing directly at the camera, not tilted up, down, or sideways.
- Use a photo taken within three months before creating the profile and update it regularly.
- Photo resolution should be at least 300 × 300 pixels. The width of the face should be at least 75 pixels.
- Facial features should be clearly visible and not overexposed or underexposed.
- Include the person's shoulders and some space above the top of the head.
- Only PNG, JPG and BMP files formats are allowed.



Create Face Recognition Task

A **Face Recognition Task** can be created after a face database has been set up (this is recommended but not a prerequisite). Only once a Face Recognition Task has been created can **Monitor Center** recognize and categorize people from a stream.

Note: One **Face Recognition Task** can at most simultaneously detect and compare up to 25 faces in real-time.

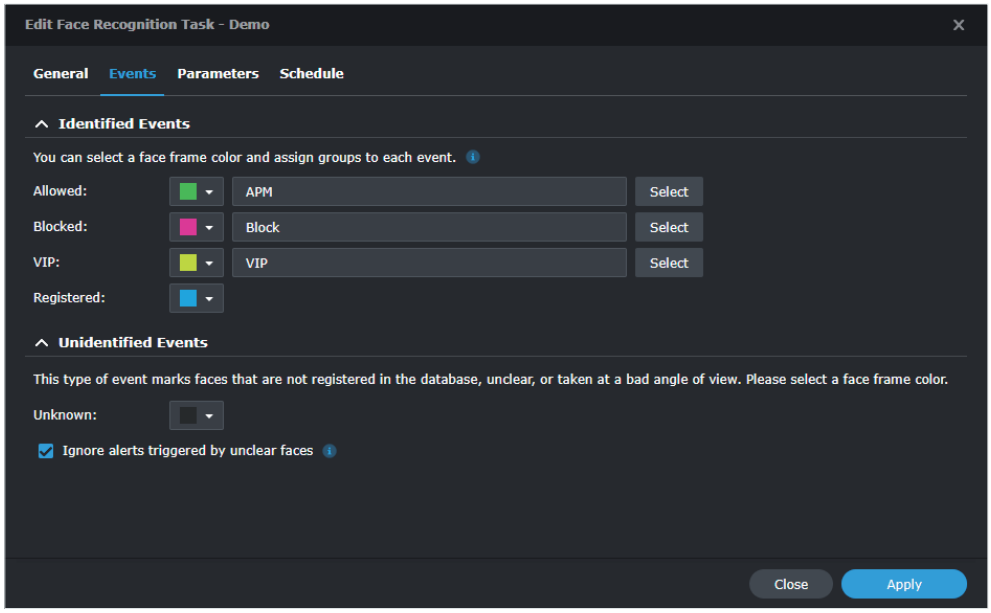
Select a stream profile

For optimal detection accuracy, select a resolution of at least 1920x1080@20FPS. Stream profiles are set by the **Intelligent Video Analytics Recording** settings of the paired camera. To edit stream profiles, go to **IP Camera** and select the camera you want to configure. Then click **Edit** > **Edit** > **Recording** > **Advanced** > **Intelligent Video Analytics Recording** to set the stream profile.

Registered and unknown events

For easy identification, a face frame color and groups can be assigned to pre-determined events such as **Allowed**, **Blocked**, and **VIP**. If no group is assigned and a person is identified from the face database, the system will categorize them as **Registered**.

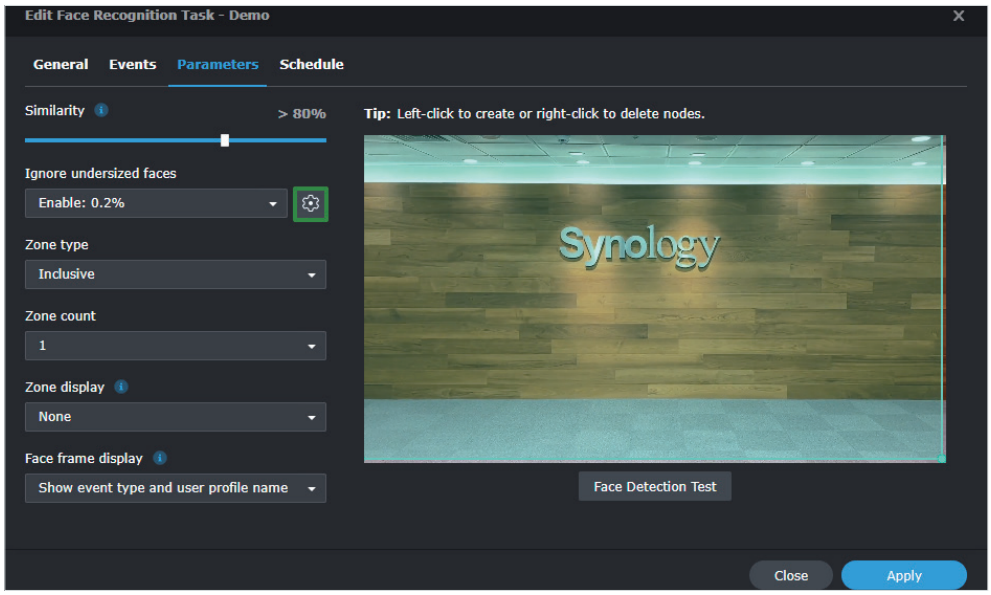
A frame color can similarly be assigned to **Registered** users so that you can quickly filter out the identification outcomes you are looking for among face recognition results and when viewing videos in **Monitor Cente**r. Similarly, if faces are unrecognized, unclear, or taken at a bad angle of view, a frame color can also be assigned for easy filtering.



Ignore unclear faces and undersized faces

For the sake of efficiency, you can fine-tune the minimum on-screen face size to filter out false positives from unclear or undersized faces. In the **Events** tab, you can choose to enable Ignore alerts that are triggered by unclear faces; when detected faces are unclear or taken from a bad angle, an event alert will not be sent.

Under the Parameters tab, click the **Edit** button to adjust the blue object frame to define the minimum on-screen face size. The percentage refers to the size of the face in relation to the camera image size. Faces that are smaller than the defined object size will be filtered out.

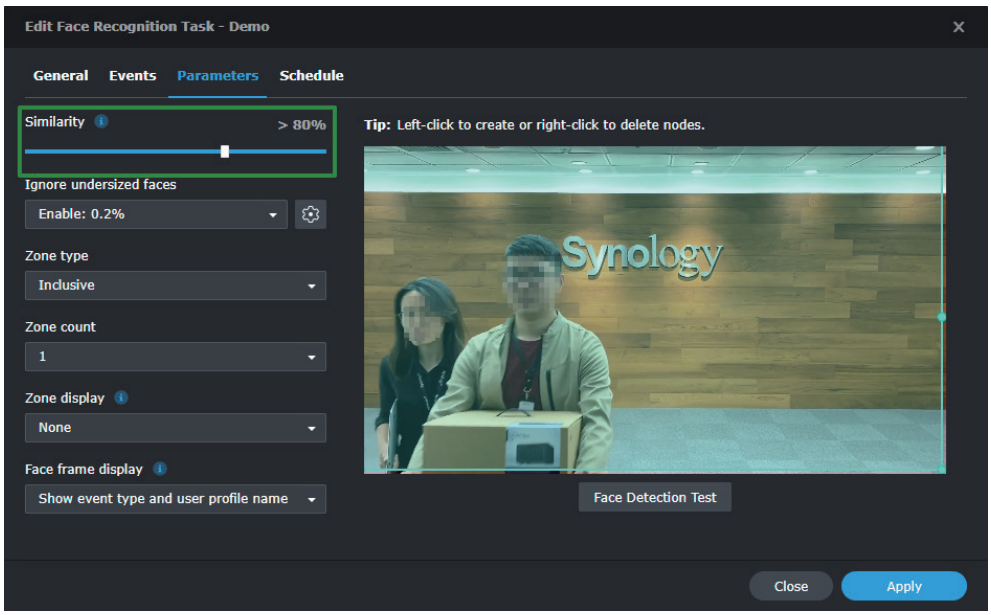


In the **Recognition Results,** you can also enable the **Ignore Unclear Faces** option. Faces that are unclear or taken from a bad angle will be excluded from the results.

Adjust the Similarity parameter

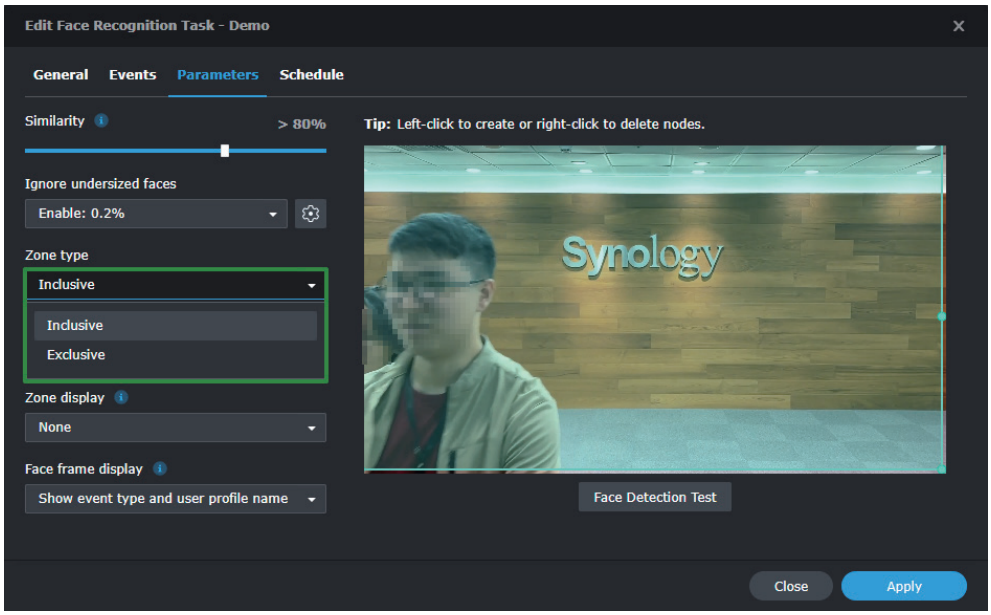
Detected faces will be positively identified from the Face Database if the similarity between the profile photo and the detected face exceeds the value specified in the **Similarity** parameter.

If there are too many mis-identified faces, you can adjust the **Similarity** parameter (the default value is 80%).



Define the detection zone

Under the **Parameters** tab, you can configure detection zones (**Inclusive** or **Exclusive**) to suit your needs. Detection zones should not be too thin or small; it should at least be two times the size of the face you want to identify. Up to three zones on one screen can be configured.



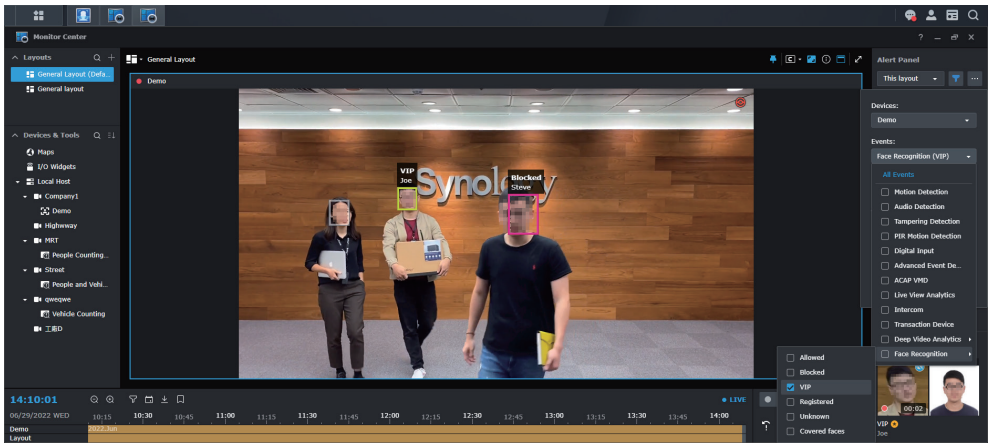
Search and Manage Recognition Results

Besides detailed configuration options, **Face Recognition** also offers two ways to view and manage recognition results, one through **Monitor Center**, and the other through the application's **Recognition Results**.

Manage recognition results in Monitor Center

To be able to see recognition results in **Monitor Center**, a **Face Recognition task** must be set up, one or more face recognition events configured as alert triggers, and the task added to the layout as a source. Face recognition results can be viewed in the **Alert Panel**.

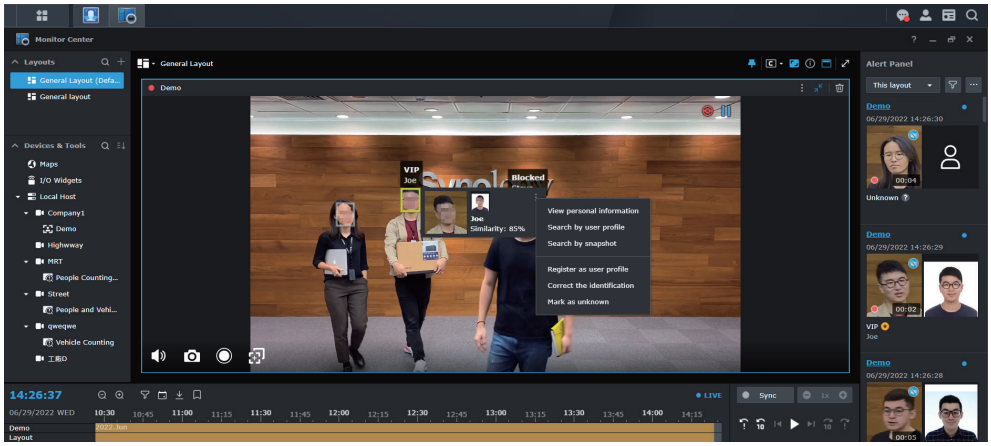
For example, you can choose to filter VIPs in the alert panel to see all instances where VIP accounts appear.



Right-clicking on a face that has been labeled by a **Face Recognition task** will display more options for that result, either identified or not.

Unidentified faces can be registered to the database using that snapshot. You can also choose to identify similar faces in unknown results.

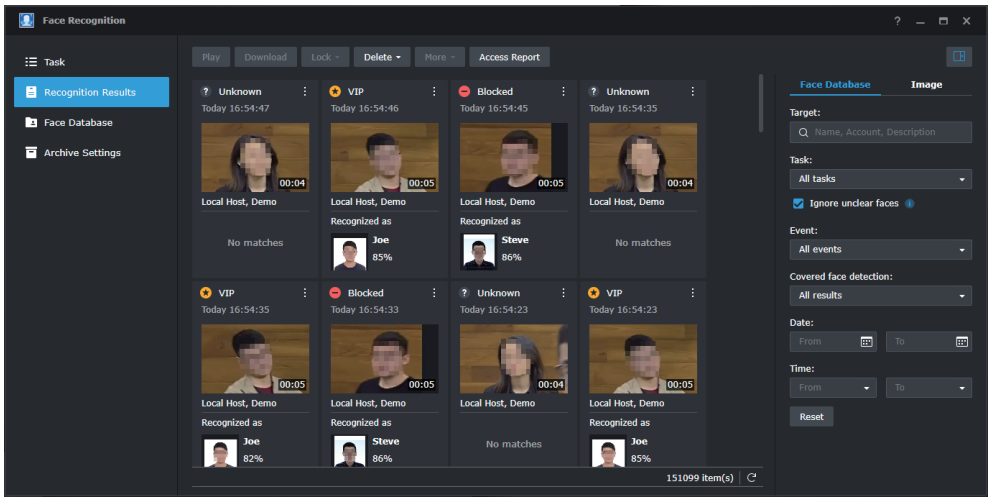
If the face is identified, either as part of a group or simply as registered, you can view personal information for that person available in the face database, search by user profile or snapshot, correct the identification with another profile from the face database, or mark the identification as unknown.



Search Historical Recognition Results

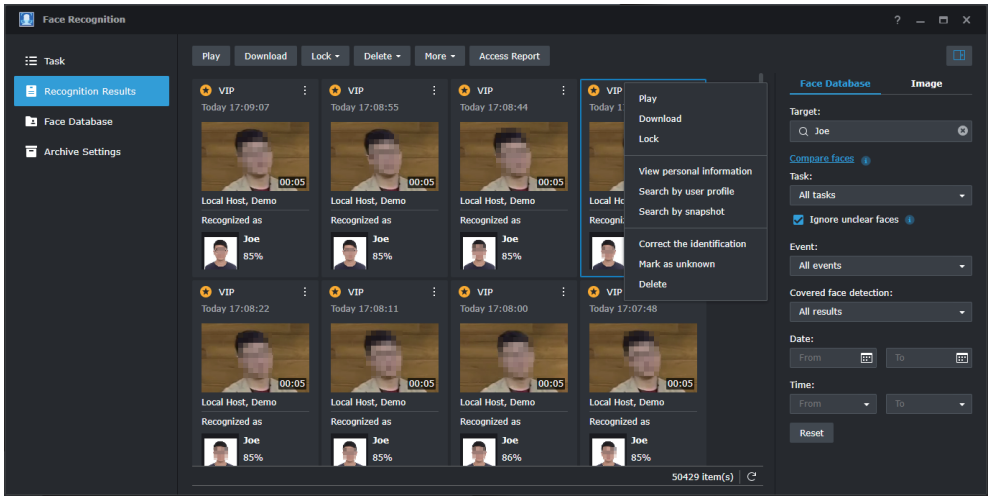
To see historical recognition results, go to **Recognition results**.

Face Recognition application allows you to filter recognition results by tasks, events, and dates, or you can search for a specific person among the results.

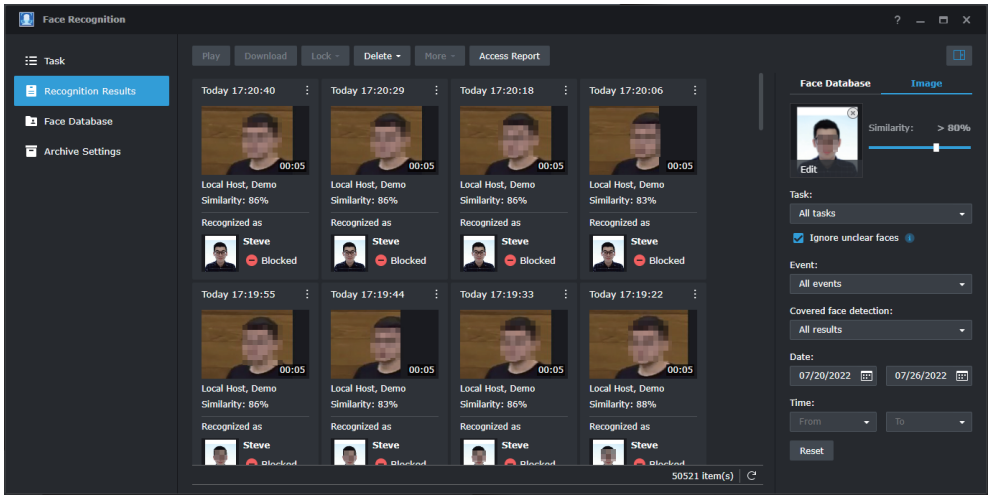


When searching for a specific person by profile information, you can search using the name, account, or description, or by uploading a face image. Results, if found, will show all the different times that a certain person has been detected by face recognition.

Specific results can be locked so that they will not be deleted automatically through archive retention policies or downloaded for backup purposes. You can also correct the misidentified results by marking the result as unknown or correcting the identification to another user profile.



If a person is not registered in the **Face Database**, you can also do an image search by uploading a face image and searching for similar results using that image. Another option is to directly search in **Recognition results** using the **Search by snapshot** option. The level of similarity can be adjusted to broaden or narrow the search.



There might be situations where a face was not identified by the system, but there is still a possibility of error by the system. If you search by name, account name, or description among recognition results, you can compare the database photo of that person with recognition results using a different similarity level from the original task. Clicking on **Compare Faces** will bring you to **Image Search** where you can adjust the similarity level.

Covered Face Detection

Face Recognition can detect whether a face mask is in use or not. Results can be filtered to show all covered or uncovered faces, and an alert can be configured in **Monitor Center** to notify you when a person with a covered or uncovered face is detected.

For example, if a person with a face mask enters a bank, an alert can be configured so that security personnel is notified to be vigilant.

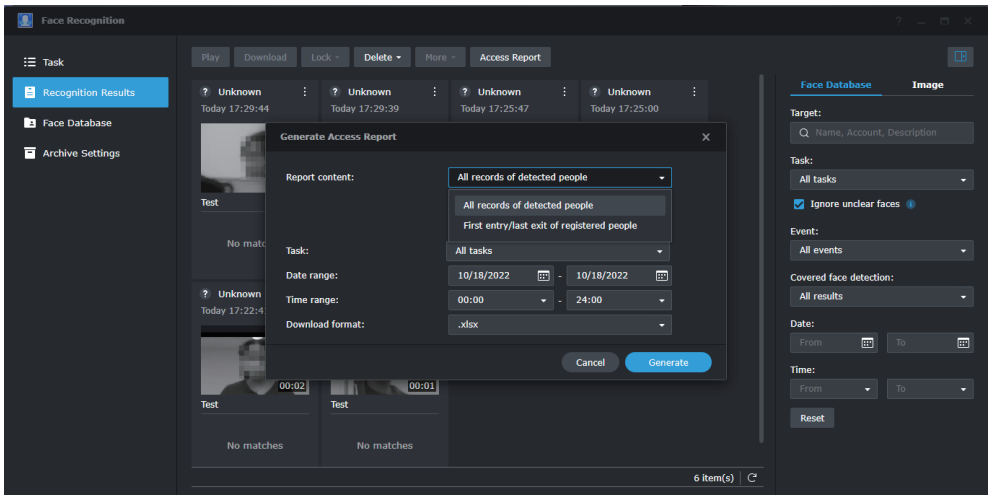
Improve Recognition Results

Recognition results can be improved by using captured face images to do the following:

- Create a new profile (if no previous face database exists, a new database can be built this way).
- Update the face database by manually correcting the recognition result and replacing the database photo of a recognized person with a captured face image.
- Correct recognition results by resetting the target as a stranger (mark as unknown) if face recognition has wrongly identified the target.

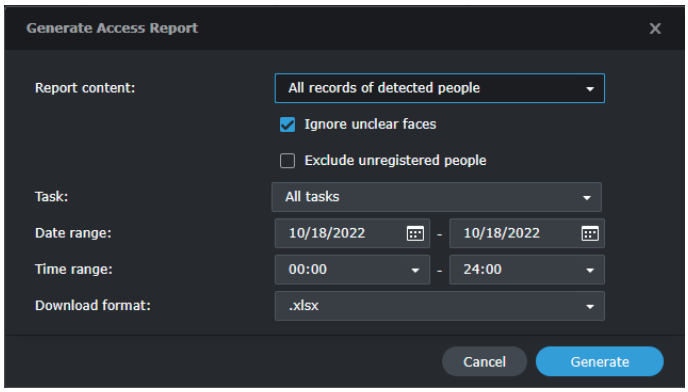
Reports

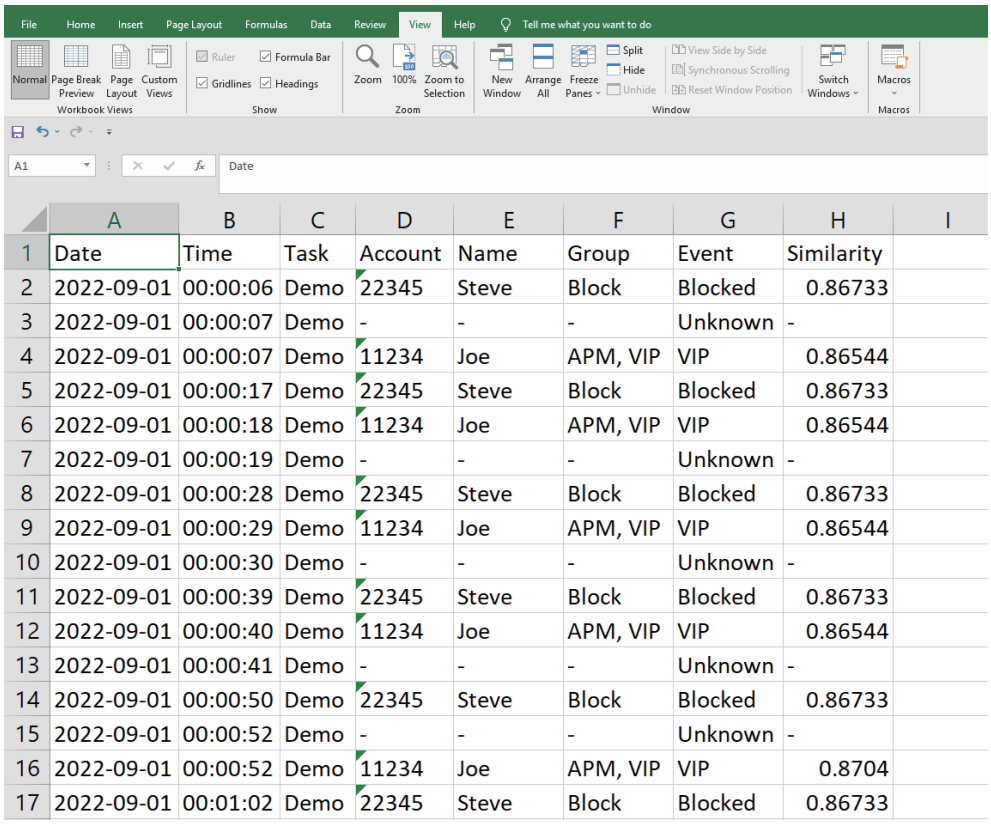
Reports are an easy way to see trends in Face Recognition results. Face Recognition provides two different types of reports. To generate a report go to **Recognition Results > Access Report.**



All records of every detected people

This report shows you all records of every detected person. Unclear faces or unregistered people can be filtered out if necessary.

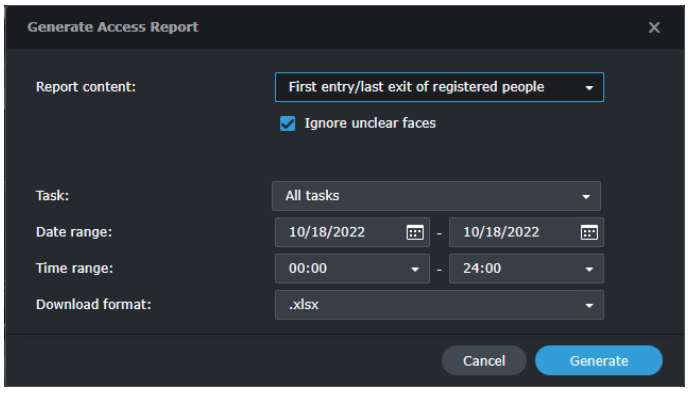


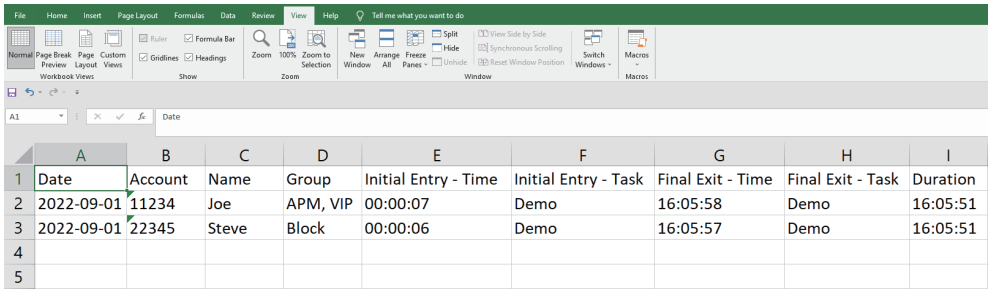


	A	B	C	D	E	F	G	H	I
1	Date	Time	Task	Account	Name	Group	Event	Similarity	
2	2022-09-01	00:00:06	Demo	22345	Steve	Block	Blocked	0.86733	
3	2022-09-01	00:00:07	Demo	-	-	-	Unknown	-	
4	2022-09-01	00:00:07	Demo	11234	Joe	APM, VIP	VIP	0.86544	
5	2022-09-01	00:00:17	Demo	22345	Steve	Block	Blocked	0.86733	
6	2022-09-01	00:00:18	Demo	11234	Joe	APM, VIP	VIP	0.86544	
7	2022-09-01	00:00:19	Demo	-	-	-	Unknown	-	
8	2022-09-01	00:00:28	Demo	22345	Steve	Block	Blocked	0.86733	
9	2022-09-01	00:00:29	Demo	11234	Joe	APM, VIP	VIP	0.86544	
10	2022-09-01	00:00:30	Demo	-	-	-	Unknown	-	
11	2022-09-01	00:00:39	Demo	22345	Steve	Block	Blocked	0.86733	
12	2022-09-01	00:00:40	Demo	11234	Joe	APM, VIP	VIP	0.86544	
13	2022-09-01	00:00:41	Demo	-	-	-	Unknown	-	
14	2022-09-01	00:00:50	Demo	22345	Steve	Block	Blocked	0.86733	
15	2022-09-01	00:00:52	Demo	-	-	-	Unknown	-	
16	2022-09-01	00:00:52	Demo	11234	Joe	APM, VIP	VIP	0.8704	
17	2022-09-01	00:01:02	Demo	22345	Steve	Block	Blocked	0.86733	

First entry/last exit of registered people

This report shows you the initial entry and last exit records of all detected people. Unclear faces can be filtered out if necessary.





	A	B	C	D	E	F	G	H	I
1	Date	Account	Name	Group	Initial Entry - Time	Initial Entry - Task	Final Exit - Time	Final Exit - Task	Duration
2	2022-09-01	11234	Joe	APM, VIP	00:00:07	Demo	16:05:58	Demo	16:05:51
3	2022-09-01	22345	Steve	Block	00:00:06	Demo	16:05:57	Demo	16:05:51
4									
5									

Appendix

Protecting privacy

While face recognition is an excellent tool for generating business intelligence or used for access authorization, we must also ensure people's privacy and human rights when implementing this technology. Without adequate regulations in place, we do not recommend using face recognition in public spaces (particularly not for law enforcement purposes). Likewise, Synology does not plan to support any function that may enable racial profiling, such as the ability to categorize detected faces based on color.

When used in the private sector (e.g., for smart retail or property security purposes), there are several features administrators can employ:

- Grant users fine-grained access rights on a need-to-know basis. For example, an employer can restrict outsourced security guards from seeing the names and detailed descriptions of employees entering the facility while still allowing them to know whether the person is on the Allowed, Blocked, or VIP list.
- Add text watermarks or privacy masks to live feeds to cover sensitive areas in the camera view.
- Enable anonymous logging. In many scenarios, DVA series models don't need to match the detected faces against any database. Instead, it can log detected faces and only assist the administrator with investigations whenever incidents occurs.
- Set up a schedule so that detection results are automatically rotated after a given period (e.g., 7 days)

Enhance security

Like any Synology NAS/NVR, DVA series models are designed with a multitude of safeguards against external attacks.

- All administrators, security managers, and users are forced to log in using 2-factor authentication, reducing the risk of data breach from stolen credentials.
- Auto-block can stop brute-force attacks when detecting repeated failed login attempts from the same IP address or untrusted client devices.
- The underlying operating system (DSM) and the Surveillance Station package are continuously updated to protect the system from emerging threats.

SYNOLOGY INC.

9F, No. 1, Yuan Dong Rd.
Banqiao, New Taipei 22063
Taiwan
Tel: +886 2 2955 1814

SYNOLOGY AMERICA CORP.

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

SYNOLOGY UK LTD.

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL,
United Kingdom
Tel.: +44 (0)1908048029

SYNOLOGY FRANCE

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

SYNOLOGY GMBH

Grafenberger Allee 125
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

SYNOLOGY SHANGHAI

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.

4F, No. 3-1-2, Higashikanda,
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com

Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2020 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.