DVA Face Recognition Administrator's Guide

Last updated: Feb 4, 2025

Table of Contents

Introduction

With its powerful AI Image Analysis, Synology Deep Video Analytics (DVA) can instantly calculate large amounts of object attributes, filter out environmental interference, 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.

This guide is designed to help you configure Face Recognition tasks effectively, ensuring optimal precision. 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 are required for Face Recognition application.

Camera quick installation

Select appropriate camera

Stream quality: Ranging from 1920×1080 @20FPS to 3840×2160 (4K)

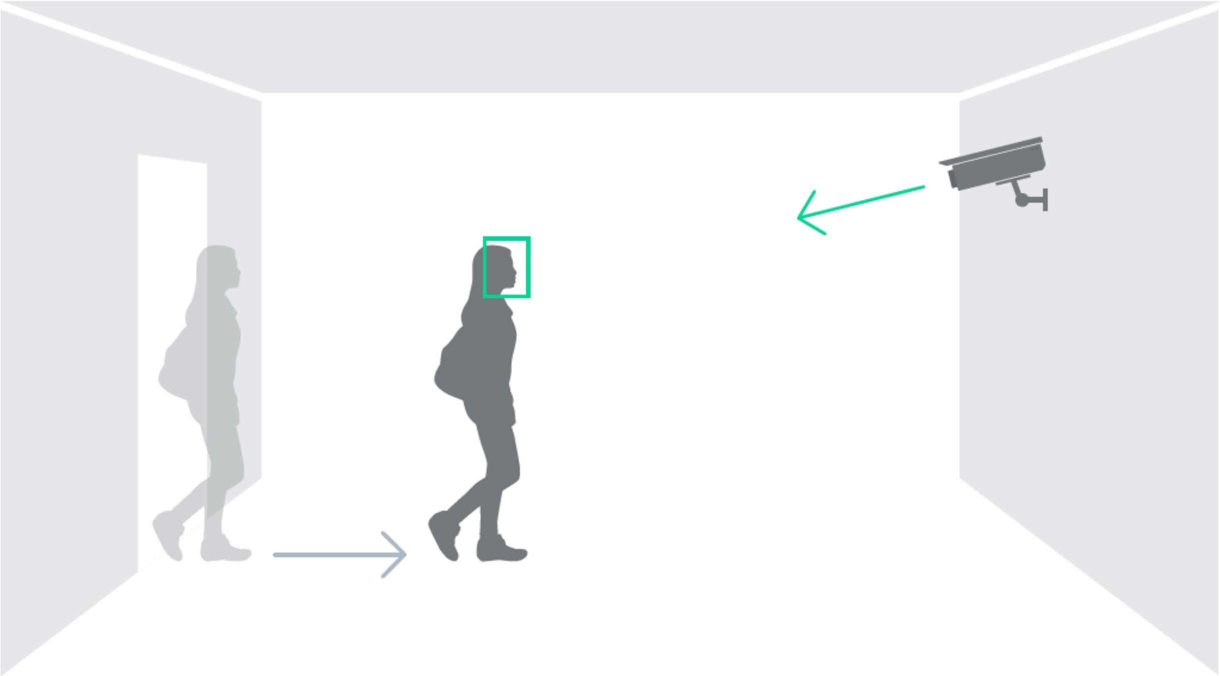
Optical zoom lens: (Optional) Used to capture clearer facial images when pedestrians are located far away

Check installation environment

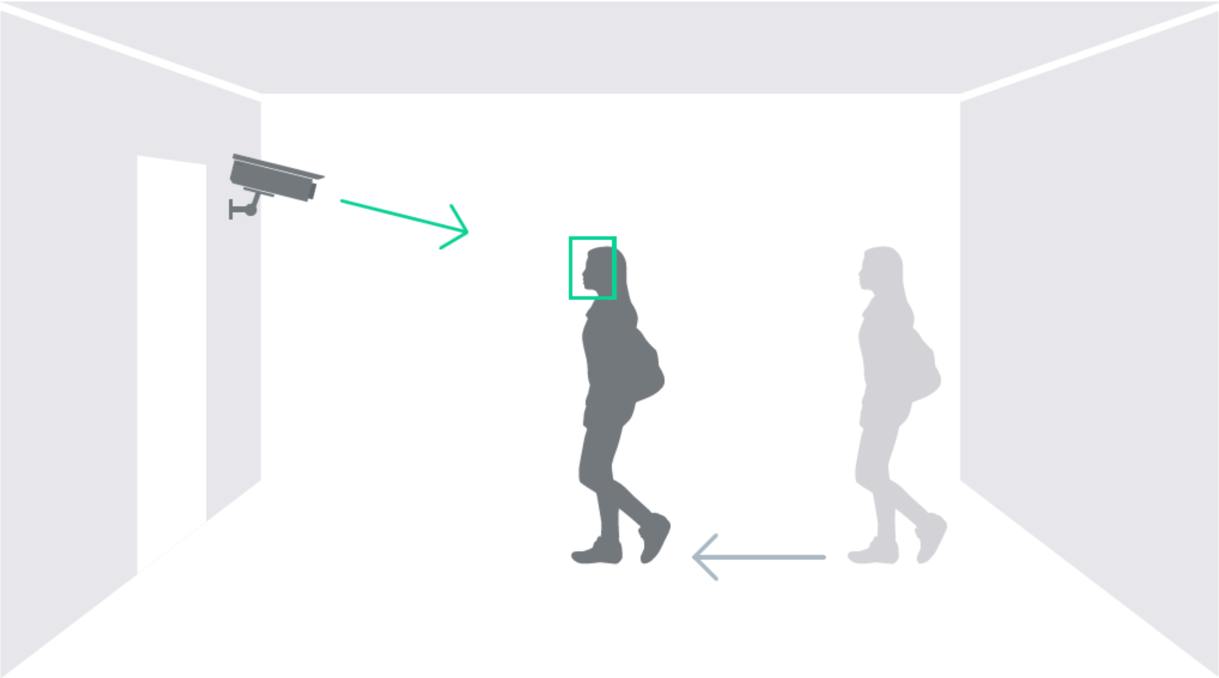
Minimum illumination: 300 lux

Installation location and direction: Face the flow of pedestrians directly at indoor entrances/exits to capture front-facing images

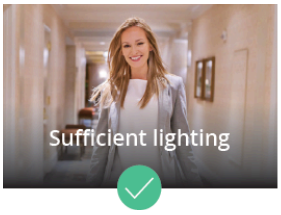
Indoor entrance

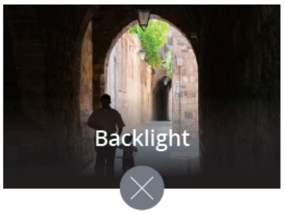


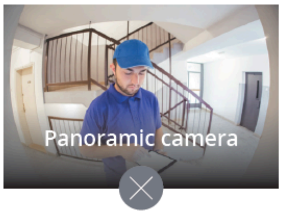
Indoor exit

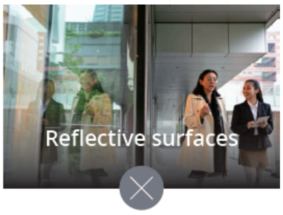


Do's and don'ts









Mounting height and angle

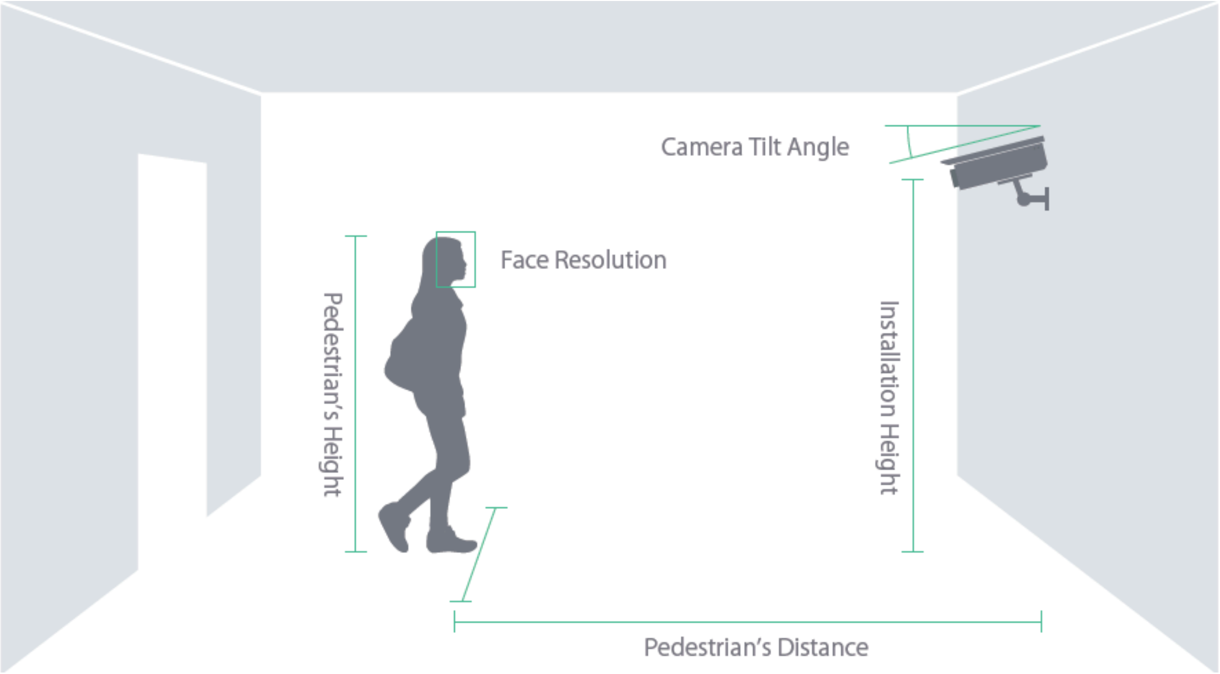
Installation Height: 1.5 ~ 3 meters

Camera Tilt Angle: Less than 15 degrees

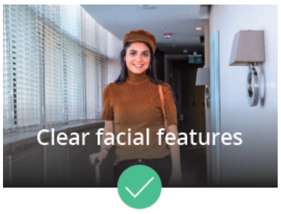
Face Resolution: At least 75 × 75 pixels (ideally 125 × 125 pixels)

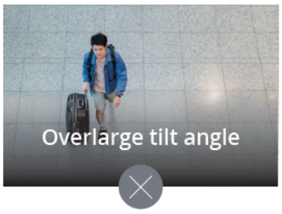
Note:

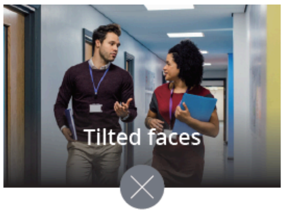
- The values provided are for reference only; please adjust the installation height/angle based on the actual actual camera configurations that can ensure a clear facial resolution.

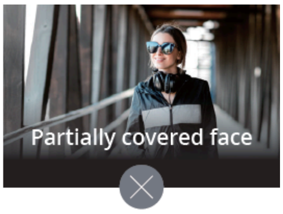


Do's and don'ts









Camera placement and environment

Despite careful planning of camera placement and environmental conditions, faces may not be detected or may be incorrectly recognized. 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 AI recognition. Backgrounds with yellowing lighting can also impede recognition; 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

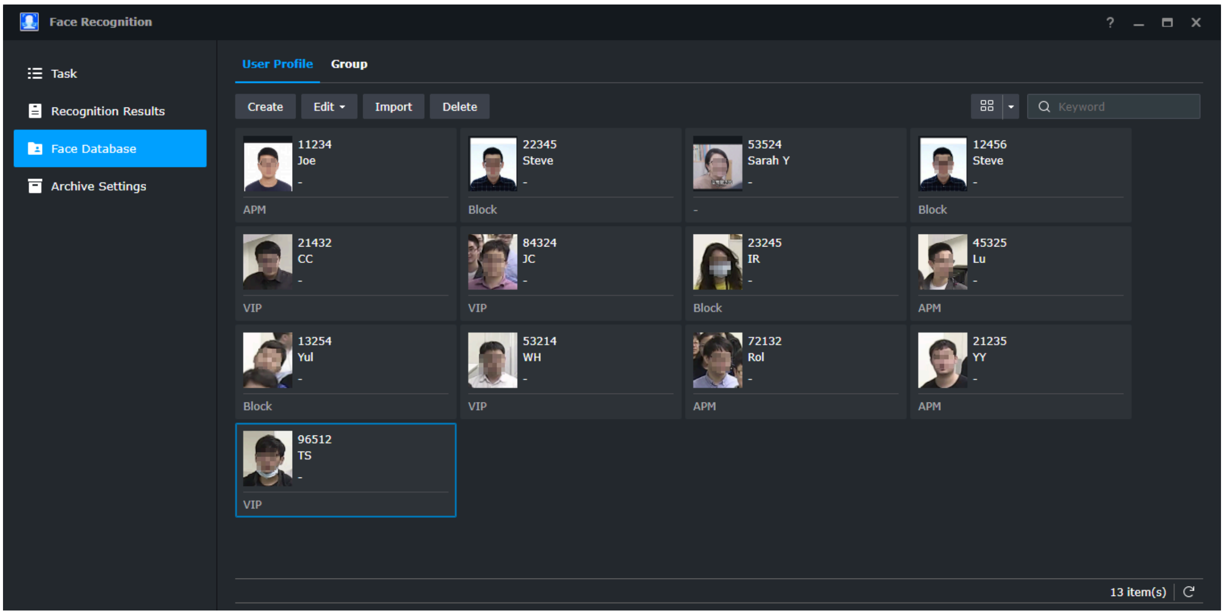
Once your cameras are mounted successfully, you can configure software settings for face recognition to suit your requirements. This chapter covers the essential settings for the Face Recognition algorithm.

It is recommended to create a face database 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**.



11234 Joe - APM

22345 Steve - Block

53524 Sarah Y - -

12456 Steve - Block

21432 CC - VIP

84324 JC - VIP

23245 IR - Block

45325 Lu - APM

13254 Yul - Block

53214 WH - VIP

72132 Rol - APM

21235 YY - APM

96512 TS - VIP

13 item(s)

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.

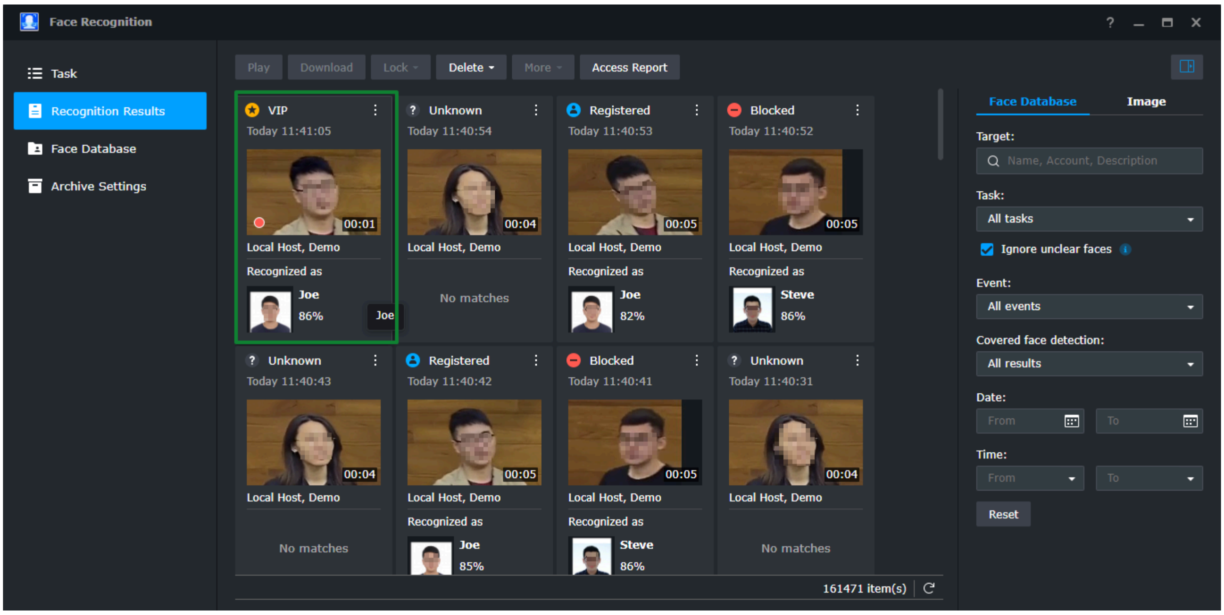
> **Note:**
>
> - You can also directly import groups or only import new users from DSM, domain, or LDAP.

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.



Target: Name, Account, Description

Task: All tasks

☑ Ignore unclear faces

Event: All events

Covered face detection: All results

Date: From To

Time: From To

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

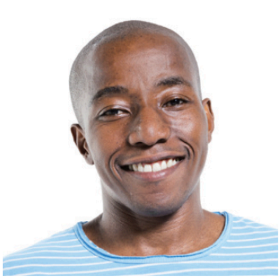
Note:

- 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**.

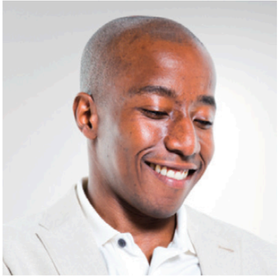
Enhance detection accuracy

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 stream profile with a resolution of between 1920×1080 @20FPS and 3840×2160 (4K). 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** > **Stream** > **Intelligent Video Analytics Recording** to set the stream profile.

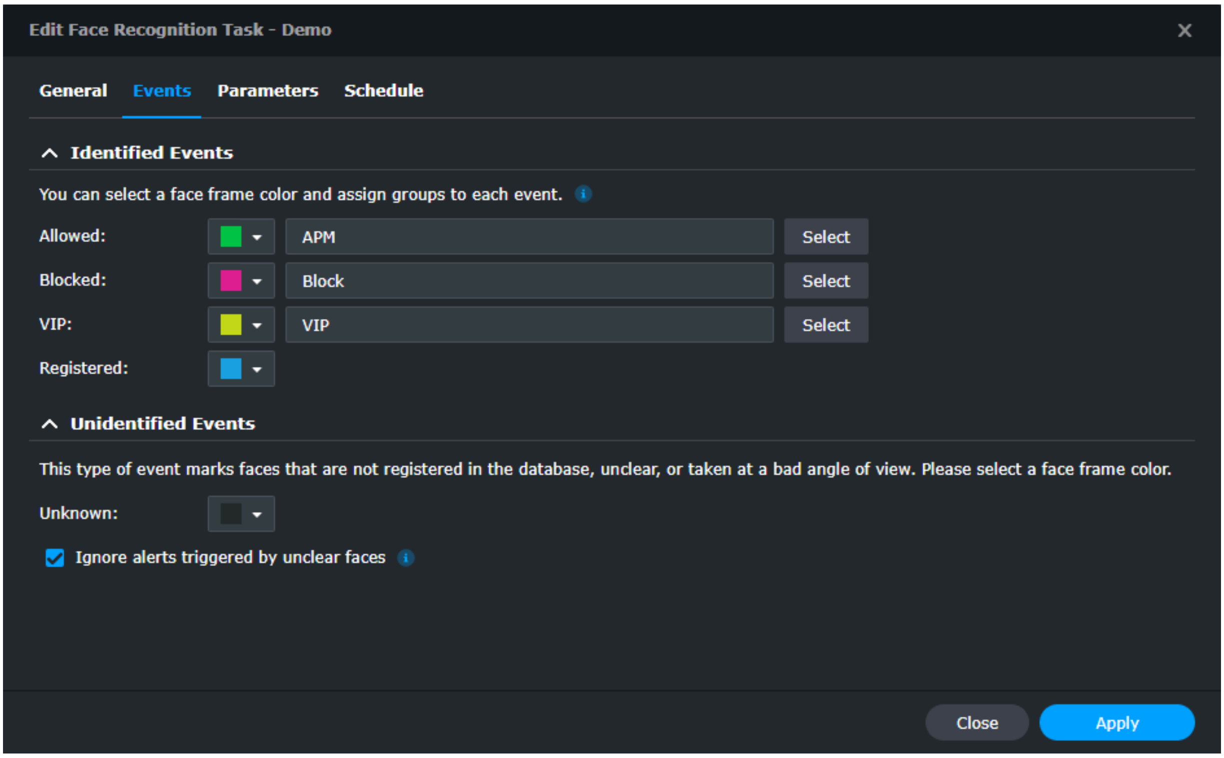
Note:

- To edit specific stream profile settings, go to **IP Camera** > select a camera > **Edit** > **Edit** > **Video & Audio Format** > **Video**.

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 Center**. Similarly, if faces are unrecognized, unclear, or taken at bad angle of view, a frame color can also be assigned for easy filtering.



Identified Events

You can select a face frame color and assign groups to each event.

Allowed:	🟩	APM	Select
Blocked:	🟪	Block	Select
VIP:	🟨	VIP	Select
Registered:	🟦		

Unidentified Events

This type of event marks faces that are not registered in the database, unclear, or taken at a bad angle of view. Please select a face frame color.

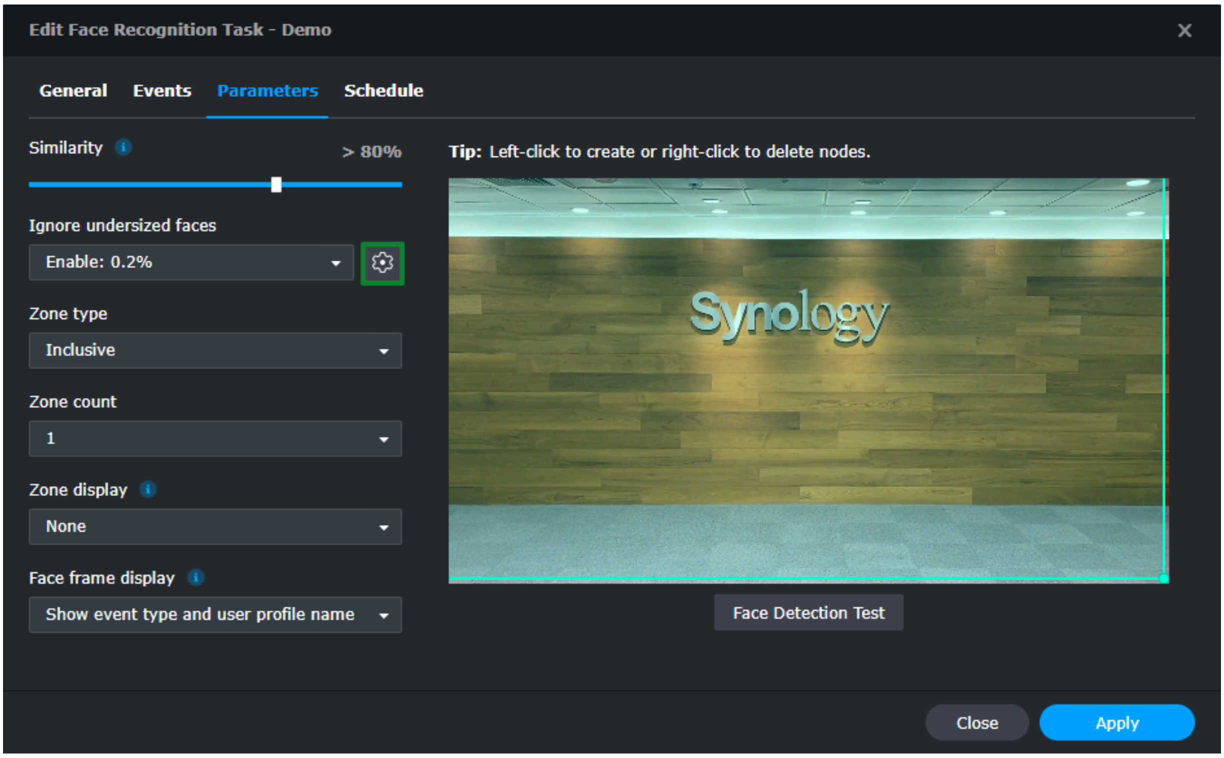
Unknown: ⬛

☑ Ignore alerts triggered by unclear faces

Ignore unclear faces and undersized faces

To enhance 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 enable **Ignore alerts triggered by unclear faces**; this prevents event alerts from being sent when faces are unclear or poorly angled.

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.


Edit Face Recognition Task - Demo

Similarity > 80%

Ignore undersized faces: Enable: 0.2%

Zone type: Inclusive

Zone count: 1

Zone display: None

Face frame display: Show event type and user profile name

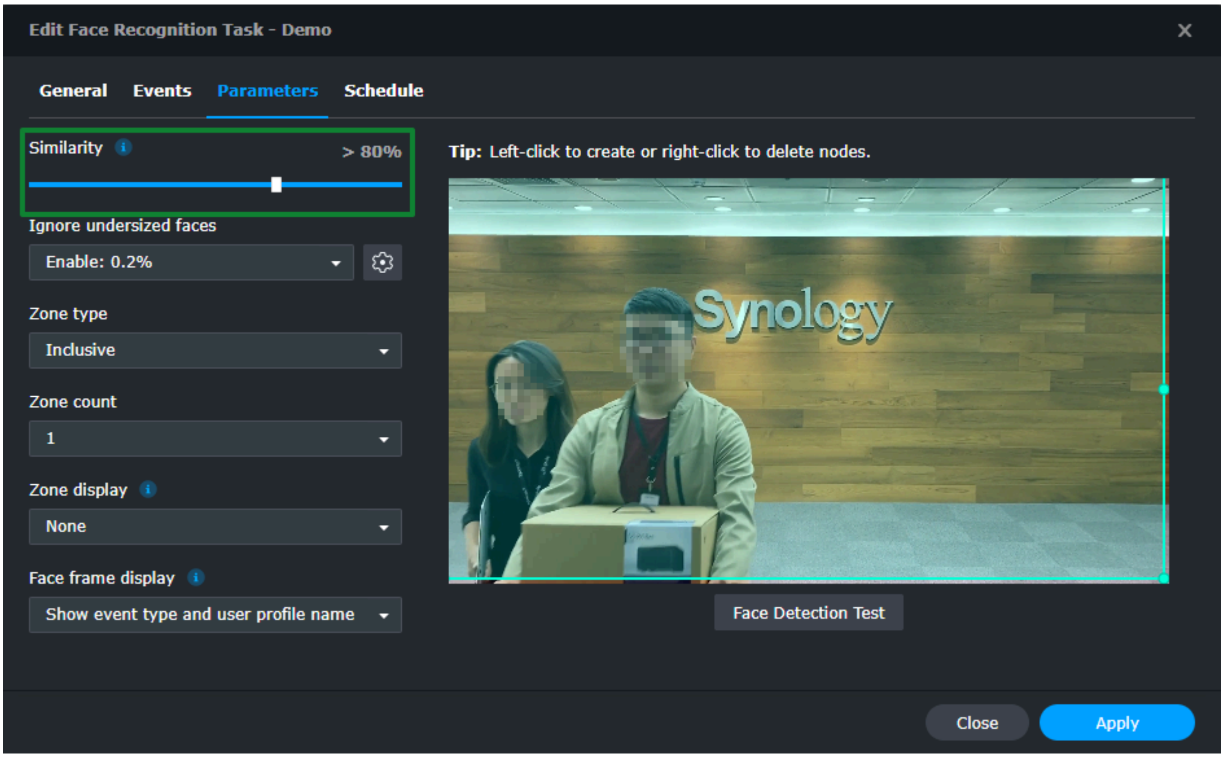
Tip: Left-click to create or right-click to delete nodes.

In the **Recognition Results**, you can also enable the **Ignore Unclear Faces** option, which excludes unclear or poorly angled faces from the results.

Adjust the Similarity parameter

Detected faces are matched with profiles in 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 misidentified faces, consider adjusting the **Similarity** parameter (default value is 80%).



Edit Face Recognition Task - Demo

General | Events | Parameters | Schedule

Similarity: > 80%

Ignore undersized faces: Enable: 0.2%

Zone type: Inclusive

Zone count: 1

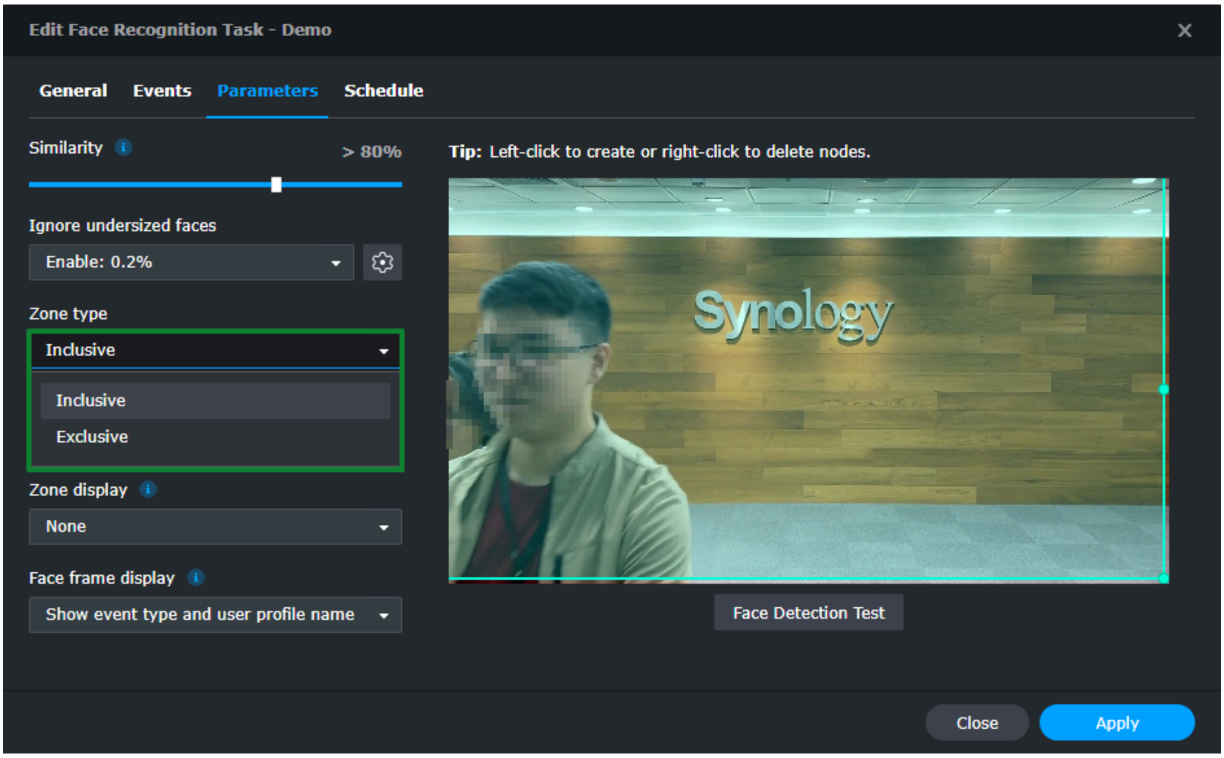
Zone display: None

Face frame display: Show event type and user profile name

Tip: Left-click to create or right-click to delete nodes.

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.



Edit Face Recognition Task - Demo

General | Events | Parameters | Schedule

Similarity: > 80%

Ignore undersized faces: Enable: 0.2%

Zone type: Inclusive

Zone display: None

Face frame display: Show event type and user profile name

Tip: Left-click to create or right-click to delete nodes.

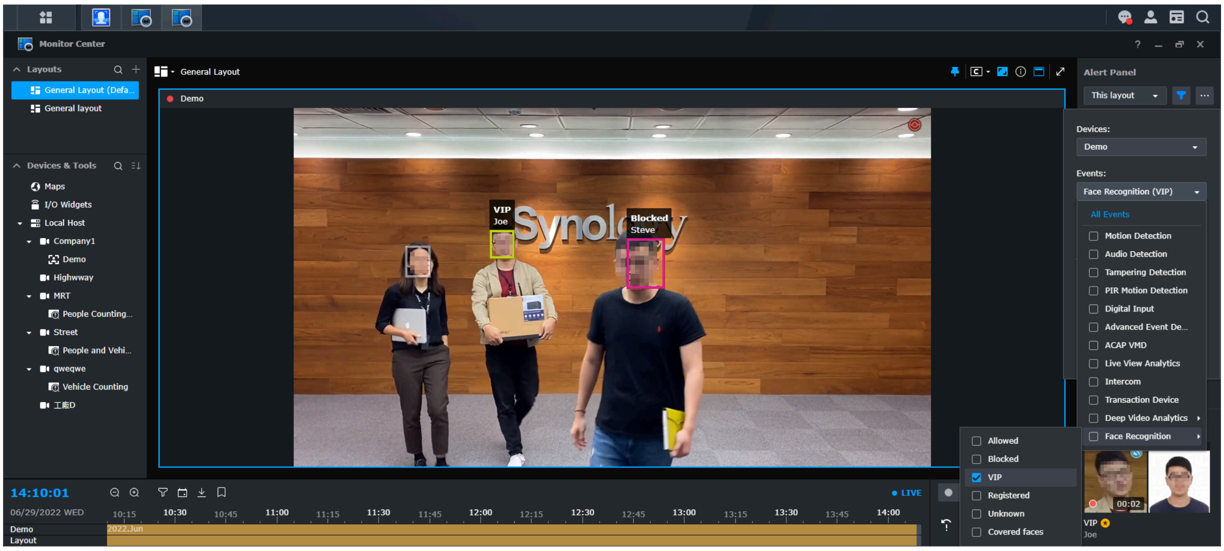
Search and manage recognition results

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.



Devices: Demo

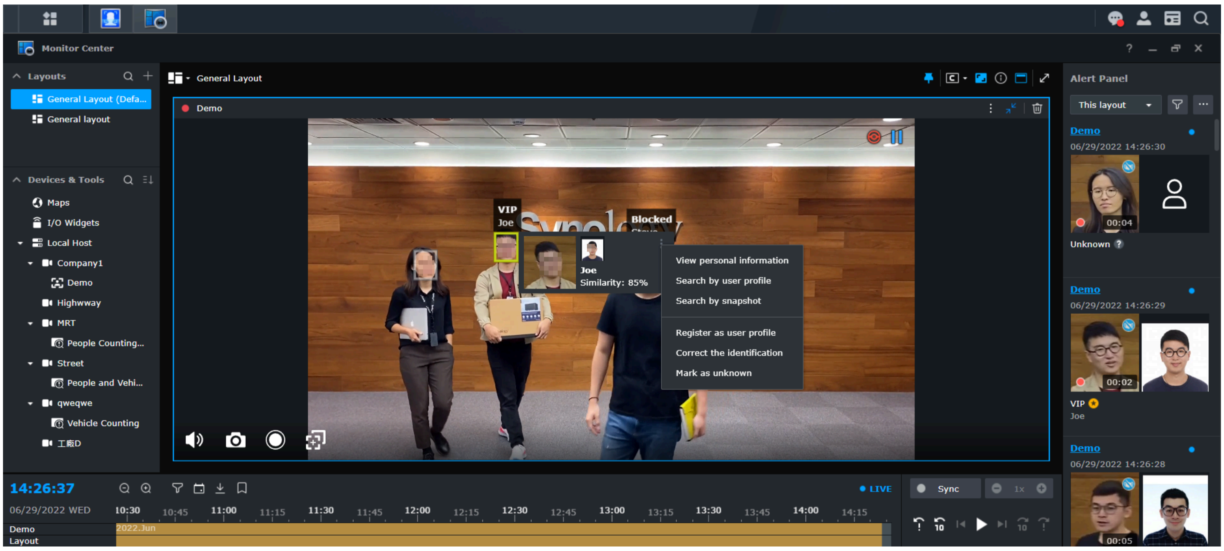
Events: Face Recognition (VIP)

□ Allowed
□ Blocked
☑ VIP
□ Registered
□ Unknown
□ Covered faces

Right-clicking on a face that has been labeled by a Face Recognition task will display more options for that result, whether the face is 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.

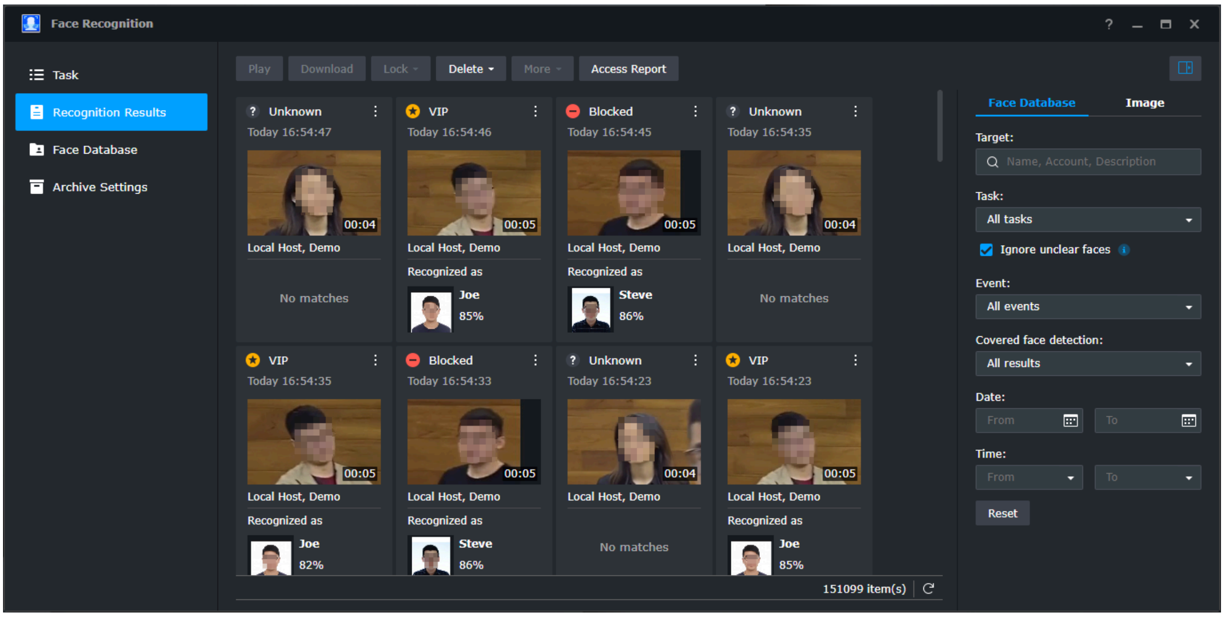
If the face is identified, whether as part of a group or simply as registered, you can access personal information for that person stored in the face database. Additionally, you can search by user profile or snapshot, correct the identification with another profile from the face database, or mark the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



Search historical recognition results

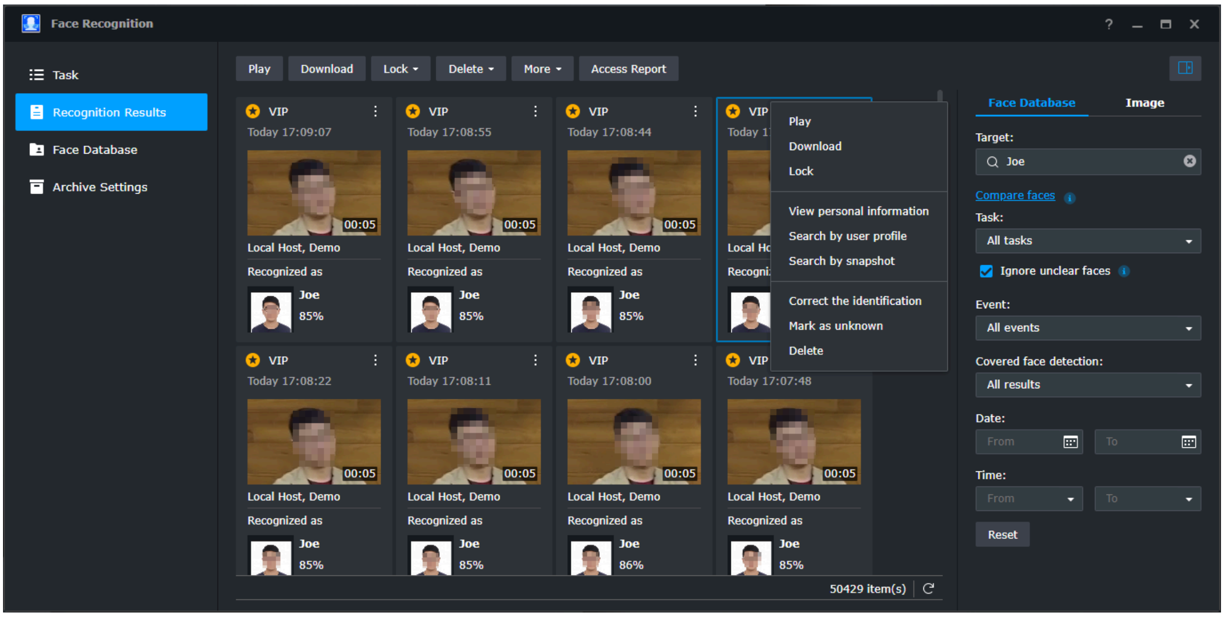
To see historical recognition results, go to **Recognition Results**.

Face Recognition 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. The results, if found, will display all instances where that 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. Additionally, any misidentified results can be corrected by marking them as unknown or assigning them to the correct user profile.



Target: Joe

Task: All tasks

☑ Ignore unclear faces

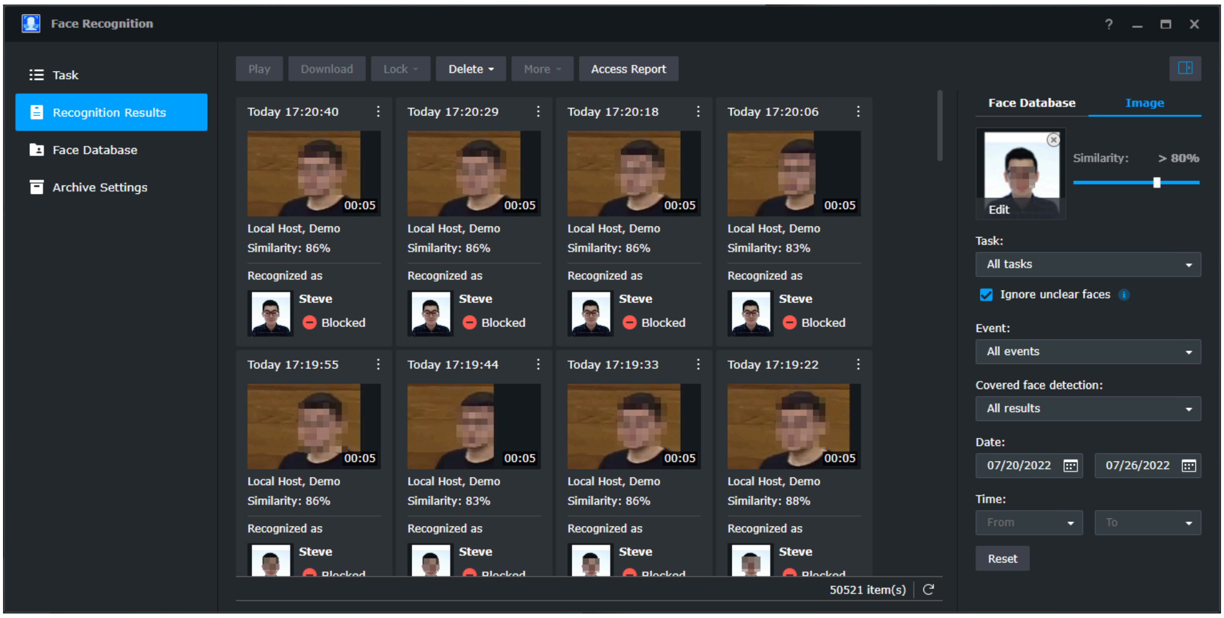
Event: All events

Covered face detection: All results

Date: From To

Time: From To

If a person is not registered in the face database, you can conduct an image search by uploading a face image and searching for similar results based on that image.Alternatively, you can directly search in **Recognition results** using the **Search by snapshot** option. The similarity level can be adjusted to broaden or narrow the search results accordingly.



Similarity: > 80%

Task: All tasks

☑ Ignore unclear faces

Event: All events

Covered face detection: All results

Date: 07/20/2022 07/26/2022

Time: From To

In cases where a face was not identified by the system, there might still be a possibility of error. You can conduct a search by name, account name, or description among recognition results. This allows you to 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.

Note:

- The maximum number of detection results that can be kept is 1,000,000.

Covered face detection

Face Recognition can detect whether a face mask is being worn or not. You can filter the results to display all faces with masks or without masks, and set up an alert in **Monitor Center** to notify you when a person with a covered or uncovered face is detected.

For example, if someone wearing a mask enters a bank, you can configure an alert to notify security personnel to remain vigilant.

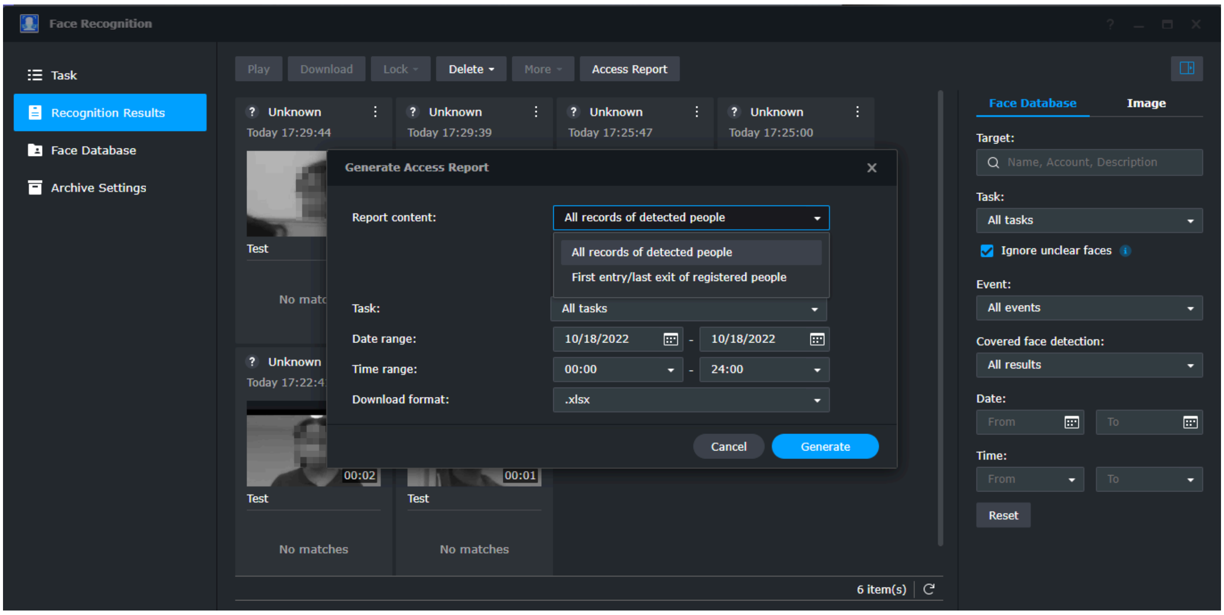
Improve recognition results

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 recognized individuals' database photos with captured face images.
- Rectify recognition results by resetting the target as unknown if misidentified by face recognition.

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**.



Generate Access Report

Report content: All records of detected people

- All records of detected people
- First entry/last exit of registered people

Task: All tasks

Date range: 10/18/2022 - 10/18/2022

Time range: 00:00 - 24:00

Download format: .xlsx

Target: Name, Account, Description

Task: All tasks

☑ Ignore unclear faces

Event: All events

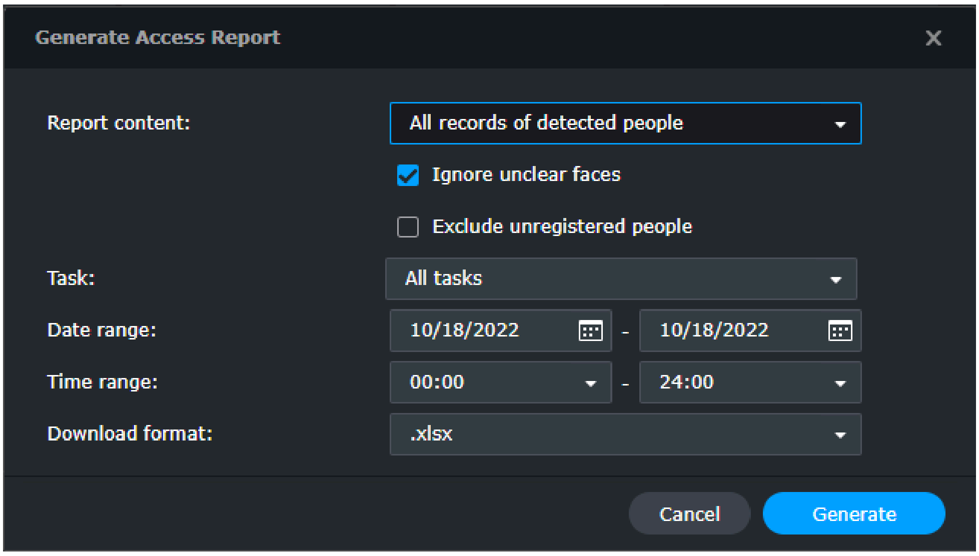
Covered face detection: All results

Date: From To

Time: From To

All records of detected people

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



Generate Access Report

Report content: All records of detected people

☑ Ignore unclear faces

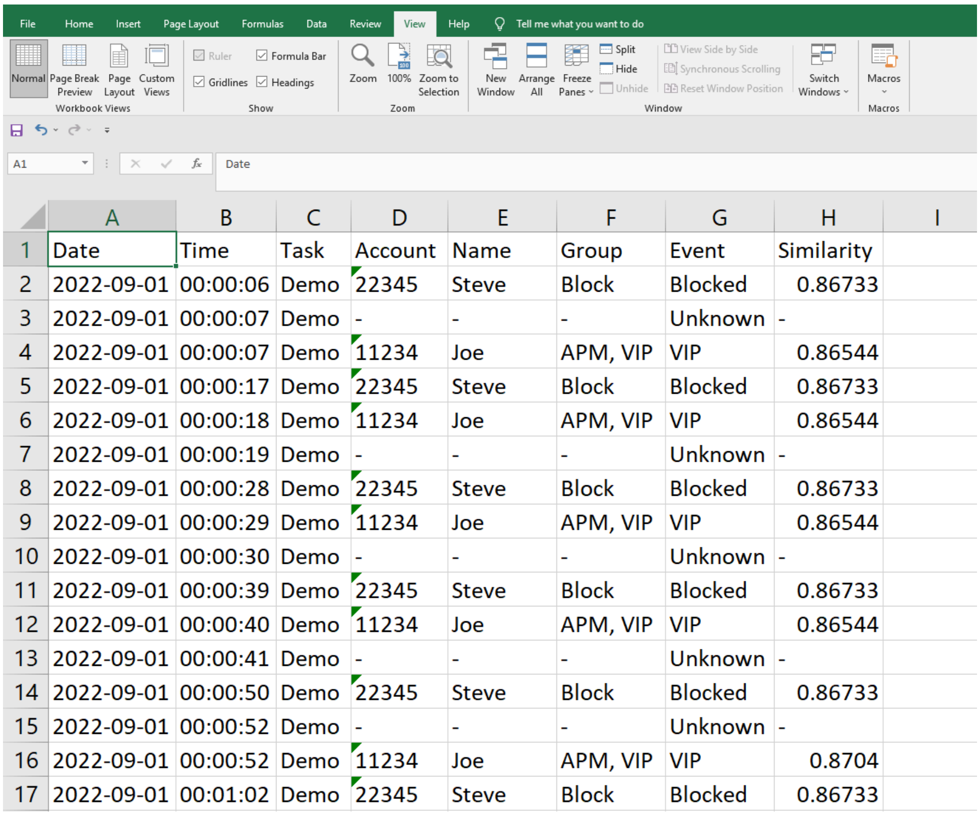
☐ Exclude unregistered people

Task: All tasks

Date range: 10/18/2022 - 10/18/2022

Time range: 00:00 - 24:00

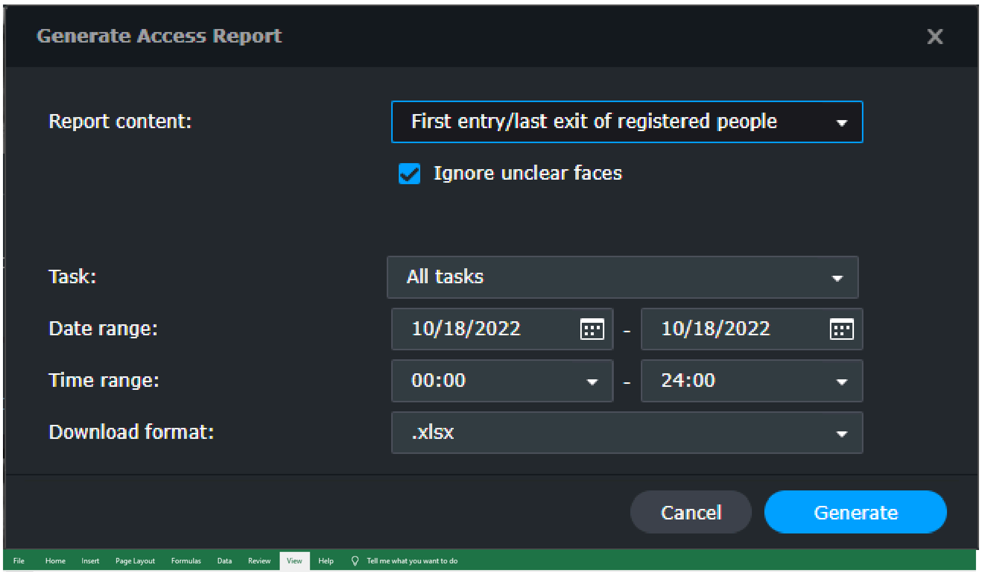
Download format: .xlsx



Date	Time	Task	Account	Name	Group	Event	Similarity
2022-09-01	00:00:06	Demo	22345	Steve	Block	Blocked	0.86733
2022-09-01	00:00:07	Demo	-	-	-	Unknown	-
2022-09-01	00:00:07	Demo	11234	Joe	APM, VIP	VIP	0.86544
2022-09-01	00:00:17	Demo	22345	Steve	Block	Blocked	0.86733
2022-09-01	00:00:18	Demo	11234	Joe	APM, VIP	VIP	0.86544
2022-09-01	00:00:19	Demo	-	-	-	Unknown	-
2022-09-01	00:00:28	Demo	22345	Steve	Block	Blocked	0.86733
2022-09-01	00:00:29	Demo	11234	Joe	APM, VIP	VIP	0.86544
2022-09-01	00:00:30	Demo	-	-	-	Unknown	-
2022-09-01	00:00:39	Demo	22345	Steve	Block	Blocked	0.86733
2022-09-01	00:00:40	Demo	11234	Joe	APM, VIP	VIP	0.86544
2022-09-01	00:00:41	Demo	-	-	-	Unknown	-
2022-09-01	00:00:50	Demo	22345	Steve	Block	Blocked	0.86733
2022-09-01	00:00:52	Demo	-	-	-	Unknown	-
2022-09-01	00:00:52	Demo	11234	Joe	APM, VIP	VIP	0.8704
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.


Generate Access Report

Report content: First entry/last exit of registered people

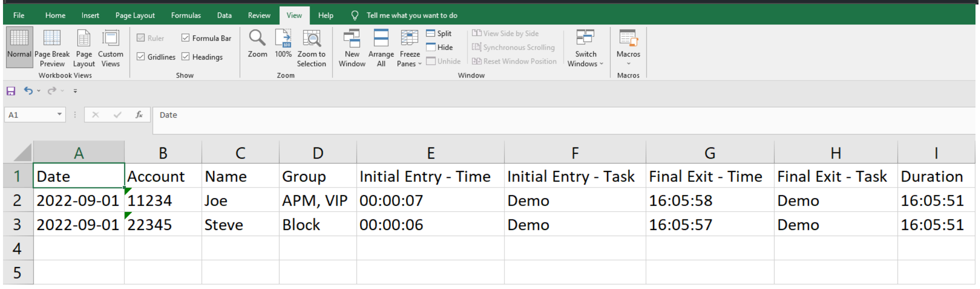
☑ Ignore unclear faces

Task: All tasks

Date range: 10/18/2022 - 10/18/2022

Time range: 00:00 - 24:00

Download format: .xlsx



Date	Account	Name	Group	Initial Entry - Time	Initial Entry - Task	Final Exit - Time	Final Exit - Task	Duration
2022-09-01	11234	Joe	APM, VIP	00:00:07	Demo	16:05:58	Demo	16:05:51
2022-09-01	22345	Steve	Block	00:00:06	Demo	16:05:57	Demo	16:05:51

Appendix

Protecting privacy

While face recognition offers valuable business insights and access control capabilities, it's crucial to safeguard privacy and human rights during its implementation. Without proper regulations, public use, especially for law enforcement, is discouraged. Synology does not support features that may facilitate racial profiling, such as categorizing faces by color.

In private sector applications like smart retail or property security, administrators can take several measures:

- 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 without matching them against a database. DVA series models can log detected faces and aid the administrator with investigations only when necessary.
- 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 application are continuously updated to protect the system from emerging threats.