DVA Face Recognition Administrator's Guide

最終更新日： 2024年5月6日

目次

はじめに

強力な AI 画像分析を活用して、Synology Deep Video Analytics (DVA) は大量のオブジェクト属性を即座に計算し、環境の干渉を排除して、正確な検出結果を提供します。

サポートされるアルゴリズムの中で、顔認識は顧客、従業員、または不審者を識別し、サービスの向上とセキュリティの強化を目指して設計されています。

このガイドは、顔認識タスクを効率的に設定し、最適な精度を確保するために作成されています。最良の結果を得るためには、リストされたポイントを忠実に守ってください。

システム要件

- Surveillance Station バージョン 9.0 以降の DVA シリーズ NAS。
- Synology の顔認識アプリケーションはデフォルトでインストールされています。

注

- 顔認識アプリケーションに追加のライセンスは必要ありません。

カメラのクイックインストール

適切なカメラの選択

ストリーム品質 1920×1080@20 FPS 以上

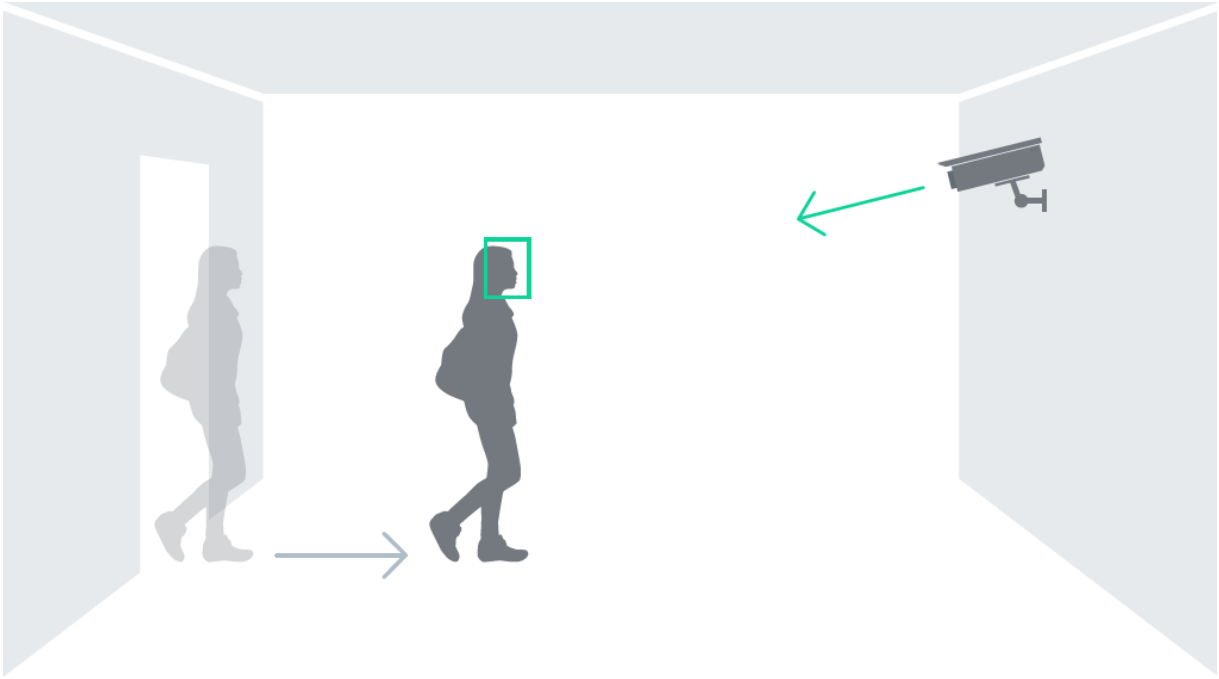
光学ズームレンズ（オプション）遠くにいる歩行者の顔を鮮明にキャプチャするために使用

インストール環境の確認

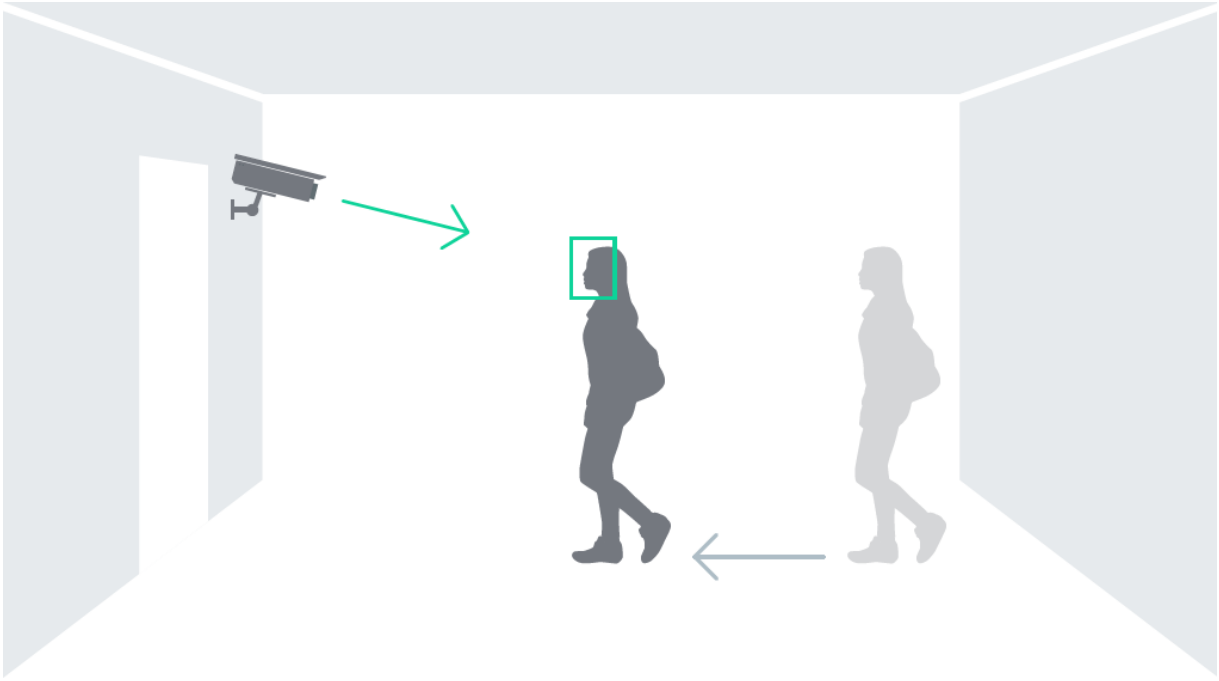
最低照度 300 ルクス

設置場所と方向屋内の出入り口で歩行者の流れに直接向き合い、正面向きの画像をキャプチャ

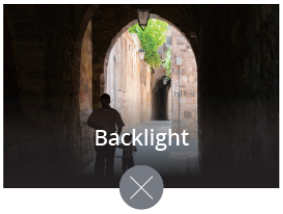
屋内入口

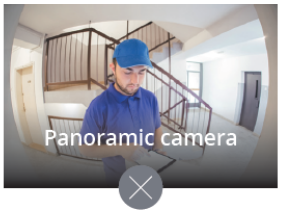


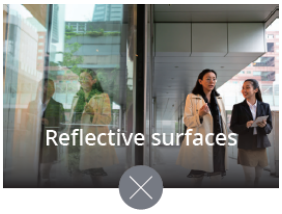
屋内出口



推奨事項と禁止事項







取り付け高さと角度

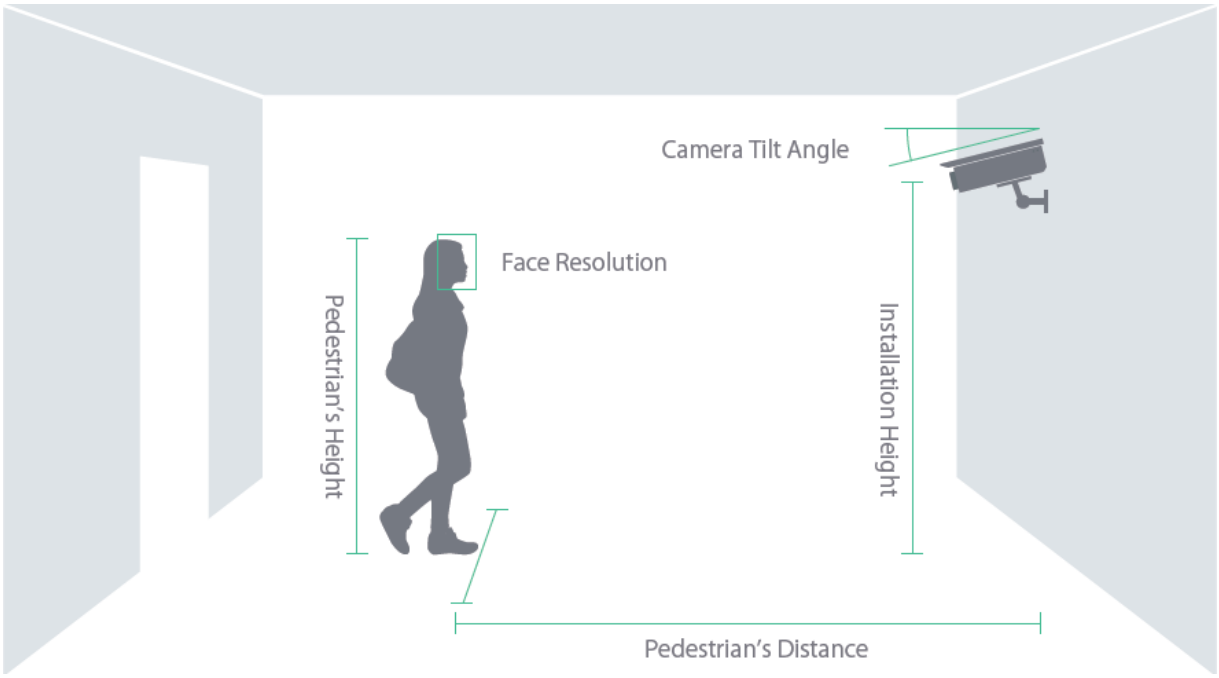
設置高さ 1.5 ~ 3 m

カメラのチルト角度 15 度以下

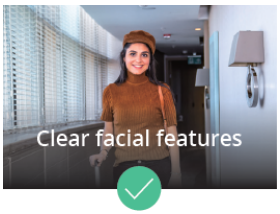
顔の解像度 75 × 75 ピクセル以上（理想的には 125 × 125 ピクセル）

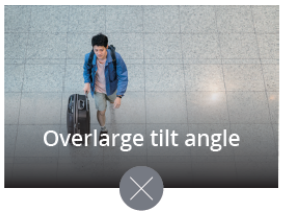
注

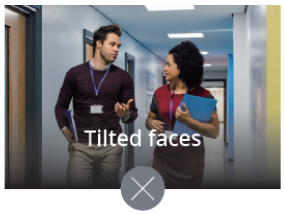
- 提供されている値は参照用です。明確な顔の解像度を確保できる実際のカメラ構成に基づいて、設置の高さ/角度を調整してください。

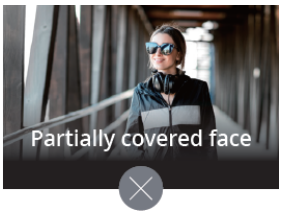

Camera Tilt Angle
Face Resolution
Pedestrian's Height
Installation Height
Pedestrian's Distance

推奨事項と禁止事項


Clear facial features


Overlarge tilt angle


Tilted faces


Partially covered face

カメラの配置と環境

カメラの配置と環境条件を注意深く計画しても、顔が検出されなかったり、誤認識されることがあります。以下の状況は、AI による検出と認識に影響を与える可能性があります。

- カメラのレンズに直接光が当たると、画像に筋が残ったり、露出オーバーが発生して画質に影響することがあります。
- 照明の変化が激しい場所にカメラを設置すると、画質が不安定になることがあります。
- 顔画像の露出過多または露出不足は、AI 認識を妨げる可能性があります。照明が黄色くなっている背景も認識を妨げる可能性があります。白色照明をお勧めします。
- 歩行者の移動が速すぎると、キャプチャされた顔の画像がぼやける可能性があります。
- カメラの視野が変わると、ビデオ分析結果に影響することがあります (フォーカスやズームレベルの変更など)。
- 天候は、屋外カメラの鮮明度に影響を与えることがあります。雨や雪、影の変化、昼と夜の違いは、検出と認識に影響を与える可能性があります。
- ネットワーク接続が不安定な場合は、画像が不完全になったり、破損したりする可能性があります。有線接続を強くお勧めします。
- ほこり、虫、その他の汚れがレンズを塞ぐことがあります。クリアな画像を撮影できるように、レンズを清潔に保ってください。

ソフトウェア設定の構成

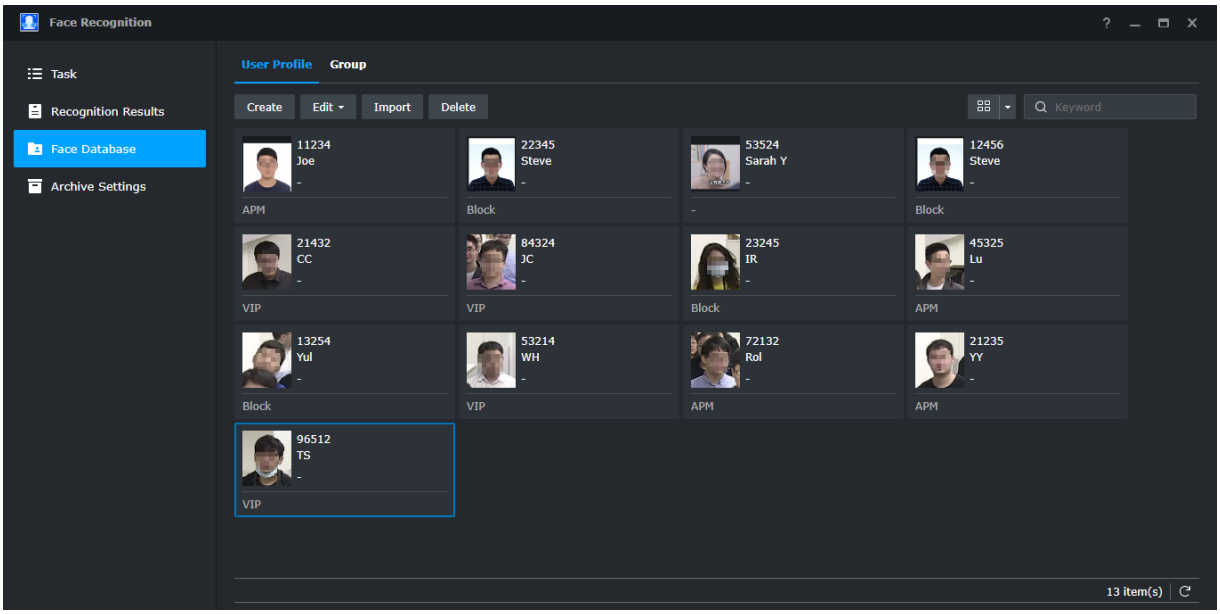
カメラが正常に設置された後、要件に応じて顔認識ソフトウェアの設定を構成できます。この章では、顔認識アルゴリズムの基本設定について説明します。

顔認識タスクを設定する前に、顔データベースの作成をお勧めします。以前のデータベース情報が利用できない場合は、タスクをセットアップして、ゼロから顔データベースを作成することも可能です。

顔データベースの作成

顔認識タスクを追加する前に、顔データベースにユーザープロファイルとユーザーグループを作成する必要があります。ユーザープロファイルを個別に作成するか、ユーザーデータと写真をバッチでインポートすることができます。

顔データベースを管理するには、[**顔認識**] > [**顔データベース**] を選択します。



顔データベースを構築する最も効率的な方法は、ユーザープロファイルをバッチでインポートすることです。プロファイルをバッチでインポートする際、以下のオプションが利用可能です。

- カスタマイズしたプロファイルリストを使用してインポート
- ローカル DSM、ドメイン、または LDAP ユーザーをインポート

インポートファイルには次の仕様が必要です (上記のインポートオプションのいずれか) 。

- **アカウント**各アカウントは 1 から 128 文字の間で一意である必要があり、Unicode 文字、数字、または次の記号のみを使用できます。 - _ @ \
- **写真ファイル名**アカウントにアップロードされた写真を一致させるために使用されます。
- 行 3 より前のセルの内容は変更しないでください。元の XLSX フォーマットのみが受け入れられます。

注

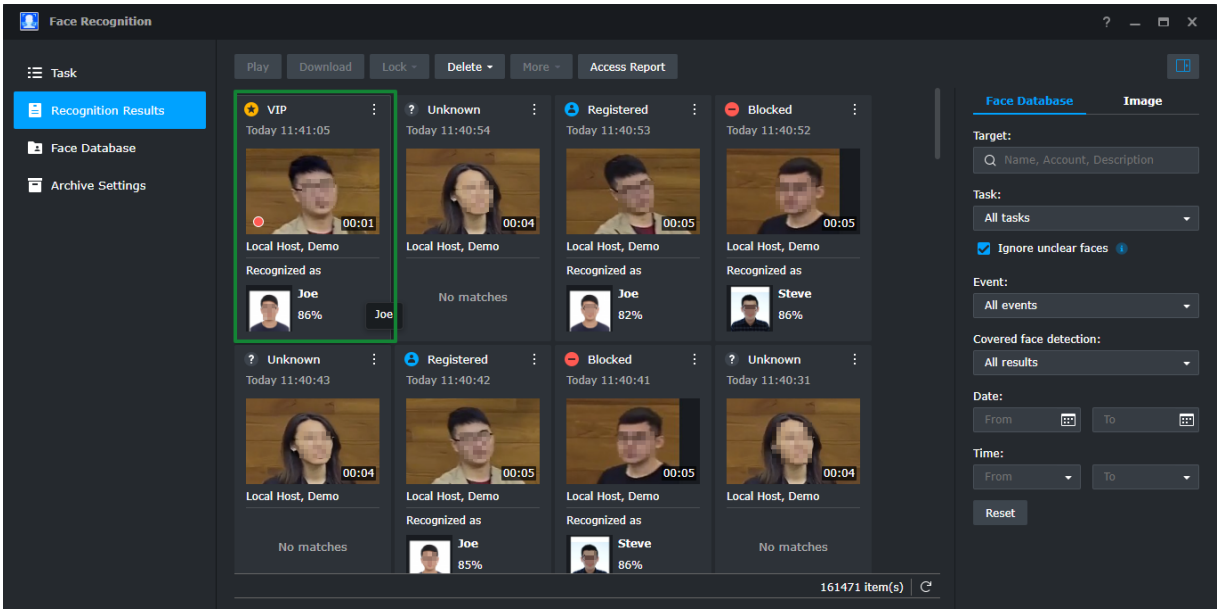
- グループを直接インポートすることも、DSM、ドメイン、LDAP から新しいユーザーのみをインポートすることもできます。

グループの定義

顔データベースのユーザーは、1 つ以上のグループに割り当てることができます。グループは、顔データベースに手動で作成するか、ローカル DSM、ドメイン、または LDAP ユーザーをインポートして作成できます。

定義すると、グループを顔認識タスクの 3 つのイベント、**許可**、**ブロック**、または**VIP**のいずれかに割り当てることができます。これにより、顔認識の結果とモニターセンターのビデオから結果を素早く識別することができます。

設定した時間内に何人の VIP が現れたかを確認したい場合は、認識結果でイベント VIP をフィルタにかけることができます。モニターセンターでビデオを見ている場合、VIP は素早く認識できるように特定の色でフレームされます。



イベントを素早く識別するためのグループの使用に関する詳細は、登録されたイベントと不明なイベントを参照してください。

注

- 各グループは 1 つのイベントにのみ割り当てることができます。ユーザープロファイルまたはグループが複数のイベントリストに割り当てられている場合は、[**ブロック**] > [**VIP**] > [**許可**] の順にマークされます。

検出精度の向上

最良の認識結果を得るには、適切なプロファイル写真に以下が含まれている必要があります。

- 目と鼻の両方が見え、カメラの正面を向き、上、下、横に傾いていないことを確認してください。
- プロファイルを作成する前の 3 か月以内に撮影された写真を使用し、定期的に更新してください。
- 写真の解像度は 300 × 300 ピクセル以上でなければなりません。顔の幅は 75 ピクセル以上でなければなりません。
- 顔の特徴ははっきりと見えるようにし、露出過多や露出不足にならないようにしてください。
- 人物の肩と頭頂部の上のスペースを含みます。
- PNG、JPG および BMP ファイル形式のみが許可されます。

顔認識タスクの作成

顔認識タスクは、顔データベースがセットアップされた後で作成できます (これは推奨されますが、前提条件ではありません) 。顔認識タスクが作成されると、**モニターセンター**はストリームから人を認識し、分類することができます。

注

- 1 つの顔認識タスクは、最大で 25 個の顔をリアルタイムで同時に検出し、比較できます。

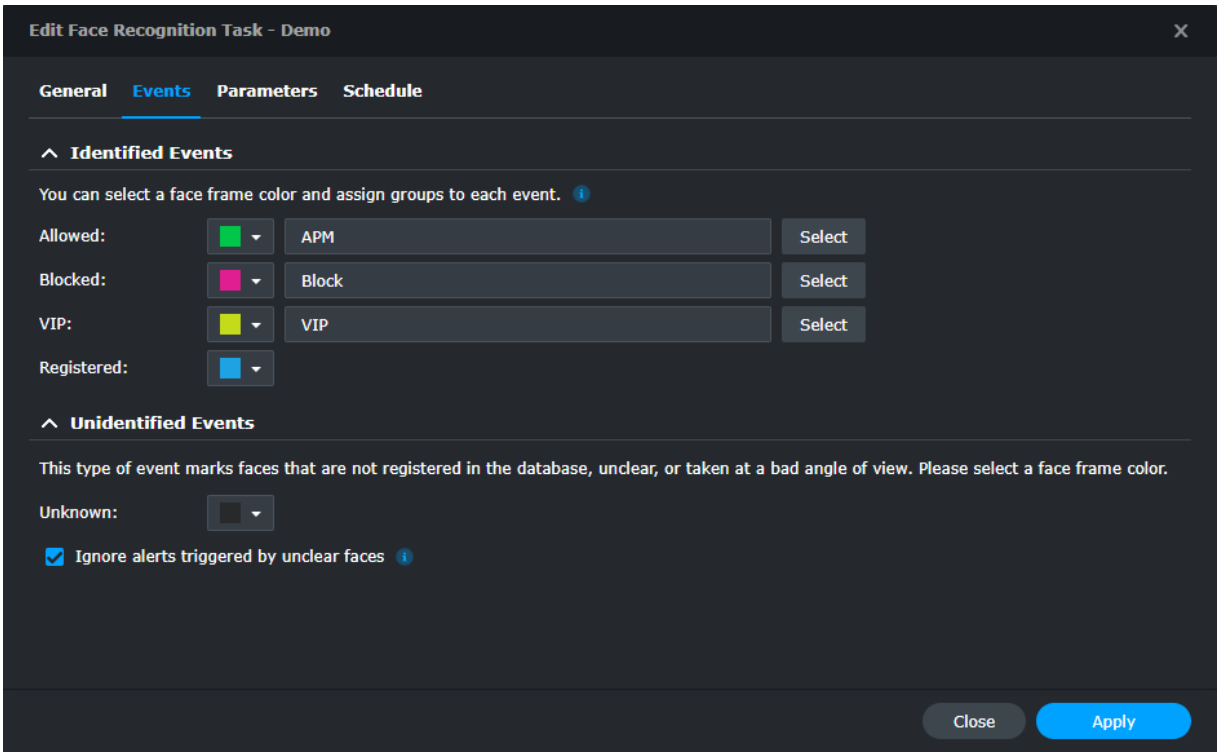
ストリームプロファイルを選択

最適な検出精度を得るには、1920x1080@20FPS 以上の解像度を選択してください。ストリームプロファイルは、ペアリングされたカメラの**Intelligent Video Analytics Recording**設定で設定されます。ストリームプロファイルを編集するには、**IP カメラ**に進み、構成したいカメラを選択してください。次に、[編集] > [**編集**] > [**録画**] > [**詳細**設定] > [**Intelligent Video Analytics Recording]** の順にクリックして、ストリームプロファイルを設定します。

登録されたイベントと不明なイベント

簡単に識別できるように、顔フレームの色とグループは、[**許可**]、 **[ブロック]**、[**VIP**] などの既定のイベントに割り当てることができます。グループが割り当てられておらず、人物が顔データベースから識別されている場合、システムはその人物を [**登録済み]** として分類します。

フレームの色も同様に [**登録済み**ユーザー] に割り当てることができます。これにより、顔認識結果の中から探している識別結果を素早くフィルタにかけ、**モニターセンター**でビデオを表示することができます。同様に、顔が認識されない、不鮮明、または不適切な画角で撮影された場合は、フレームの色を割り当てて簡単にフィルタリングできます。

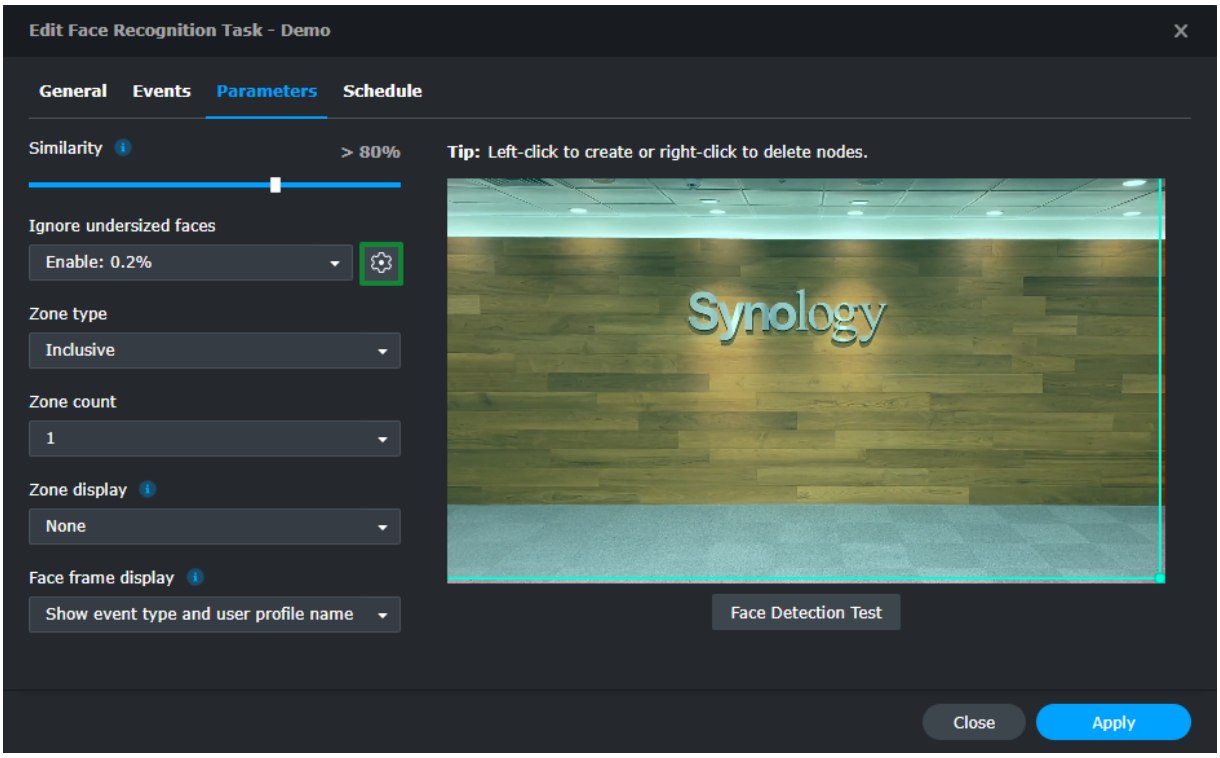


不明瞭な顔とサイズの小さい顔を無視

効率を高めるために、画面上の顔の最小サイズを微調整して、顔が不明瞭または小さすぎることによる誤検出を除外することができます。 [イベント] タブで、[**不明な顔によってトリガーされたアラートを無視**] を有効にすることができます。これにより、顔が不鮮明または角度が不十分な場合にイベントアラートが送信されるのを防ぎます。

[パラメータ] タブで [**編集**] ボタンをクリックし、青い物体の枠を調整して、画面上の顔の最小サイズを定義します。パーセンテージは、カメラの画像サイズに対する顔のサイズを示します。定義されたオ

ブジェクトサイズよりも小さい顔は除外されます。

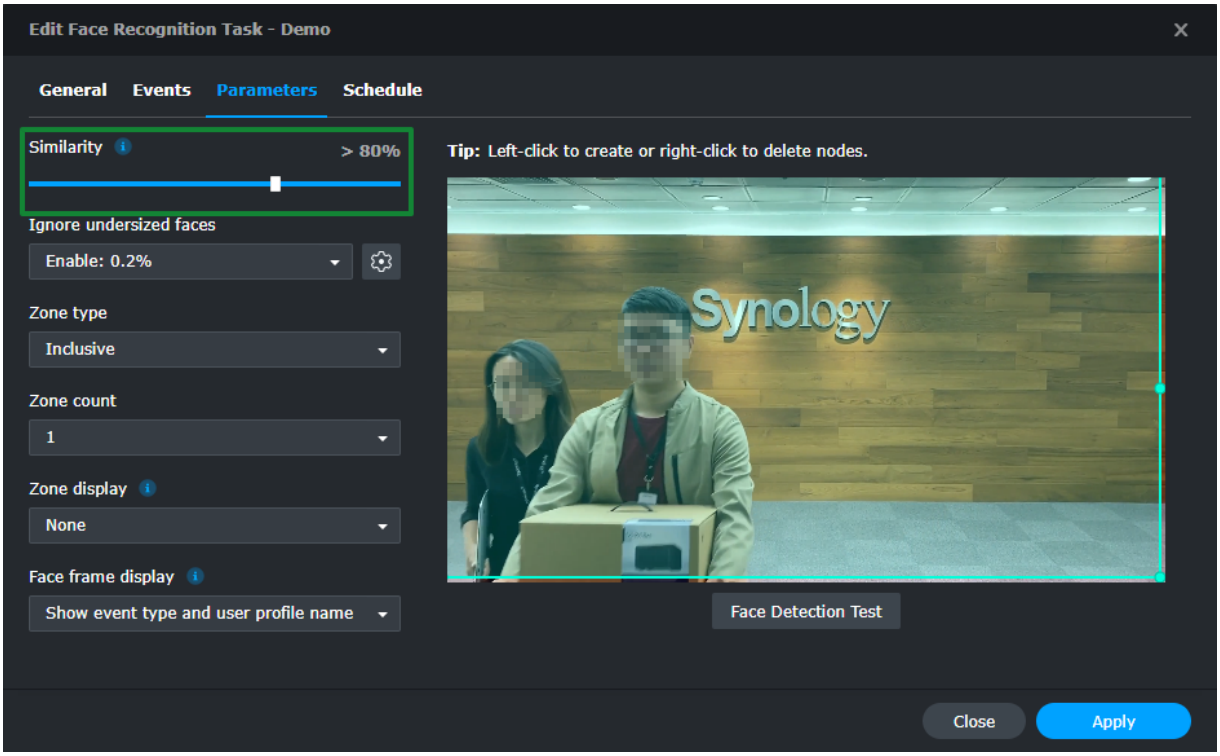


[**認識結果**] で、[不明瞭な **顔を無視**] オプションを有効化することもできます。これは、不明瞭な顔や不適切な角度の顔を結果から除外します。

類似度パラメータの調整

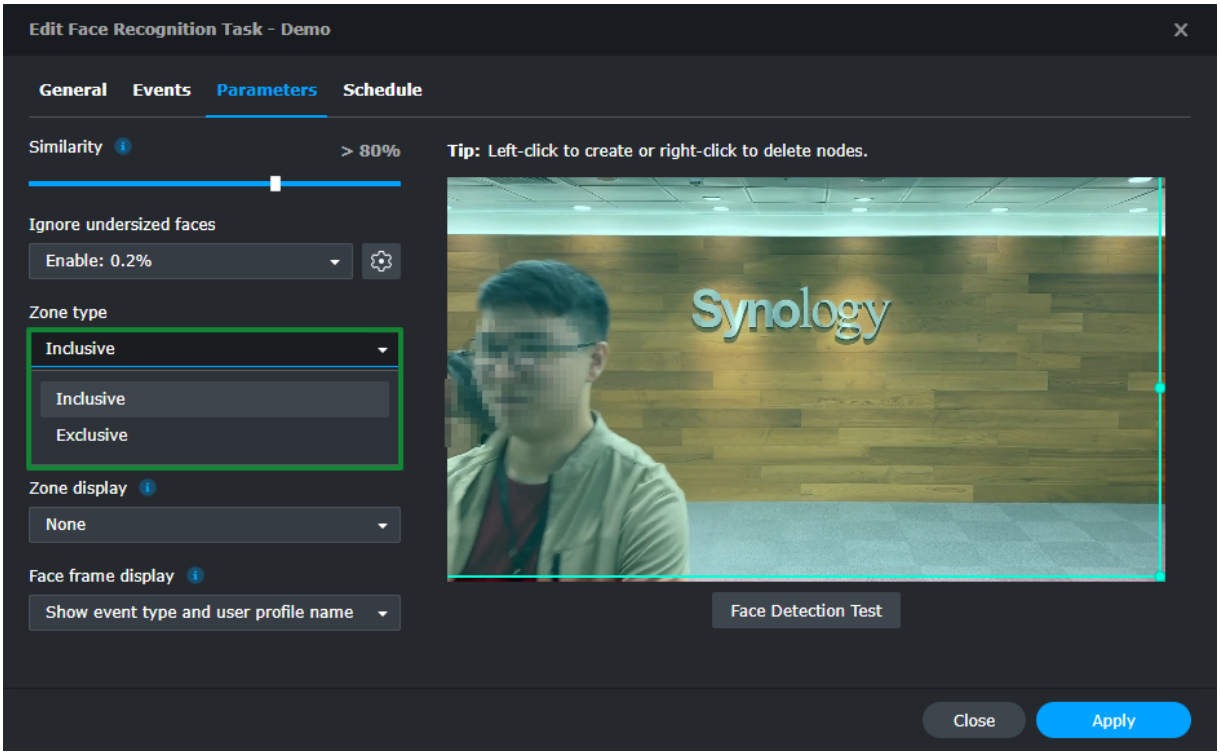
プロファイル写真と検出された顔の間の類似性が [**類似性]** パラメータで指定された値を超える場合、検出された顔は顔データベースのプロファイルと一致します。

誤って識別された顔が多すぎる場合は、[**類似度**] パラメータを調整することを検討してください (デフォルト値は 80%)。



検出ゾーンを定義

[パラメータ] タブで、ニーズに合わせて検出ゾーン ([含む]または [含まない]) を構成できます。検出ゾーンは細すぎたり、小さすぎたりしません。識別したい顔のサイズの 2 倍以上でなければなりません。1 つの画面に最大 3 つのゾーンを設定できます。



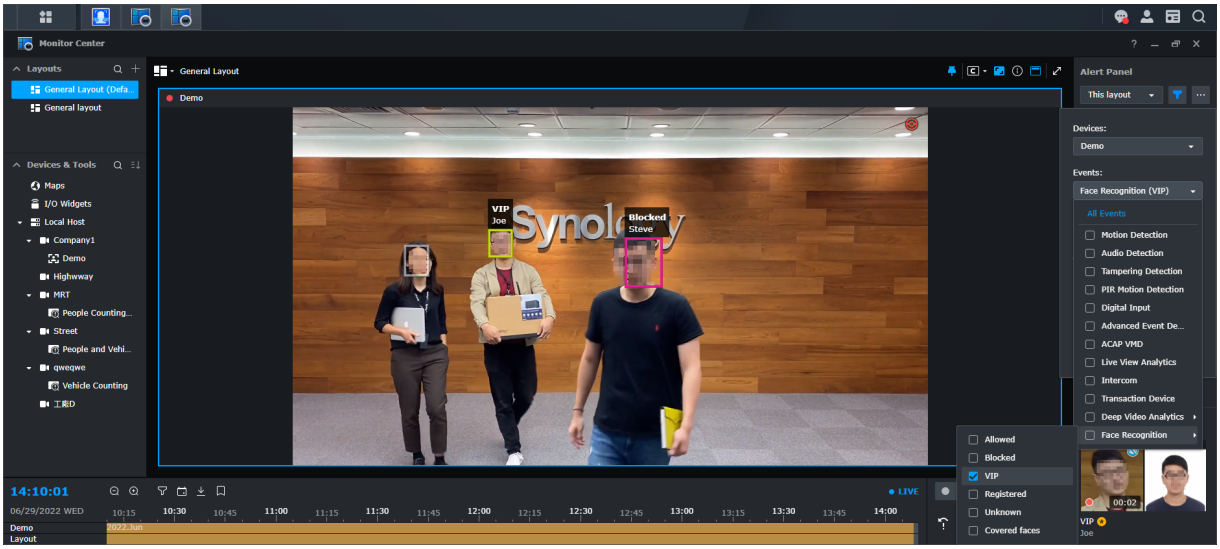
認識結果の検索と管理

詳細な構成オプションの他に、顔認識では認識**結果**を表示および**管理**するための 2 つの方法があります。

モニターセンターで認識結果を管理

モニターセンターで認識結果を表示できるようにするには、顔認識タスクをセットアップし、1 つまたは複数の顔認識イベントをアラートトリガーとして構成し、タスクをソースとしてレイアウトに追加する必要があります。顔認識の結果は、**[アラートパネル]**で確認できます。

例えば、アラートパネルで VIP をフィルタリングして、VIP アカウントが現れるすべてのインスタンスを見ることができます。

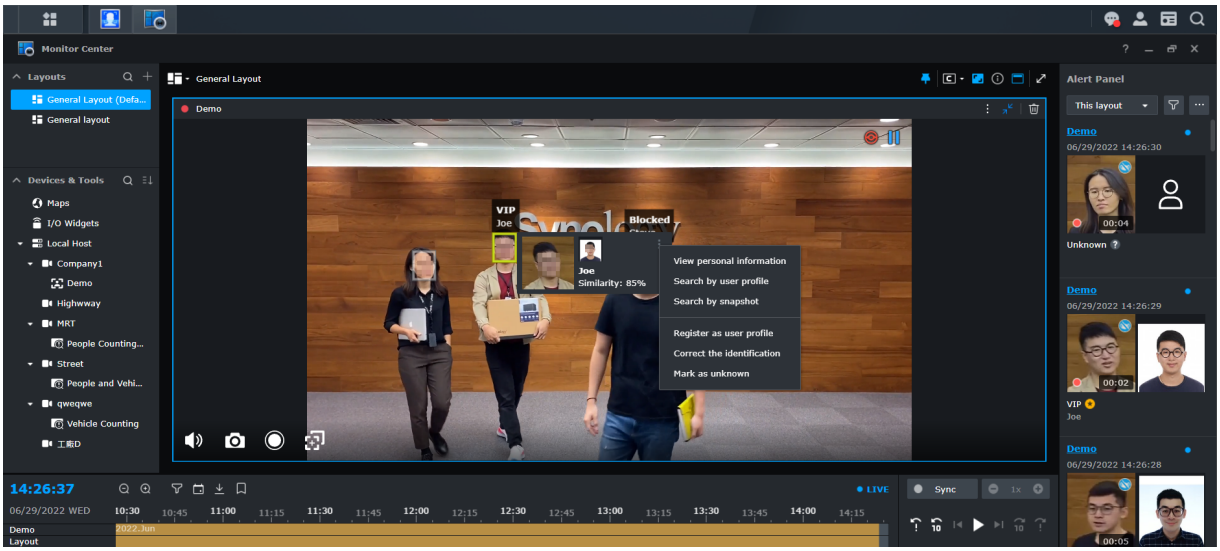


顔認識タスクでラベル付けされた顔を右クリックすると、顔が識別されているかどうかにかかわらず、その結果に対するその他のオプションが表示されます。

識別されていない顔は、そのスナップショットを使用してデータベースに登録できます。不明な結果から類似の顔を識別することもできます。

顔が識別された場合、それがグループの一部として、あるいは単に登録されたものとして識別されると、顔データベースに保存されているその人の個人情報にアクセスすることができます。さらに、ユーザープロファイルまたはスナップショットで検索したり、顔データベースから別のプロファイルで識別

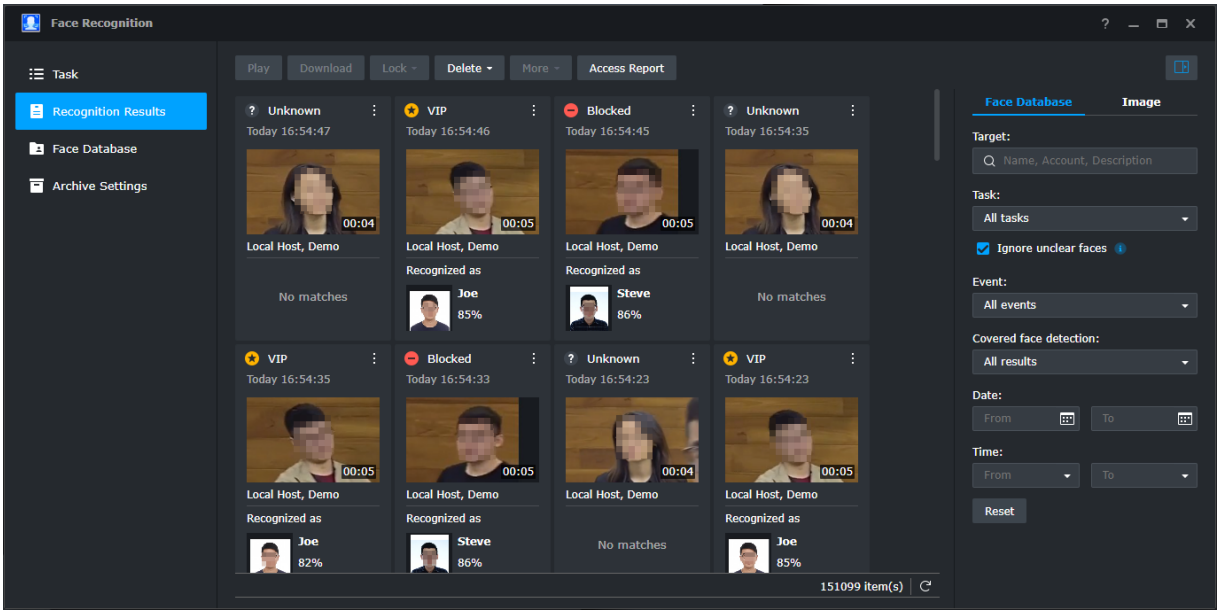
を修正したり、識別を不明としてマークしたりすることができます。



認識結果の履歴を検索

認識結果の履歴を見るには、[**認識**結果] に進みます。

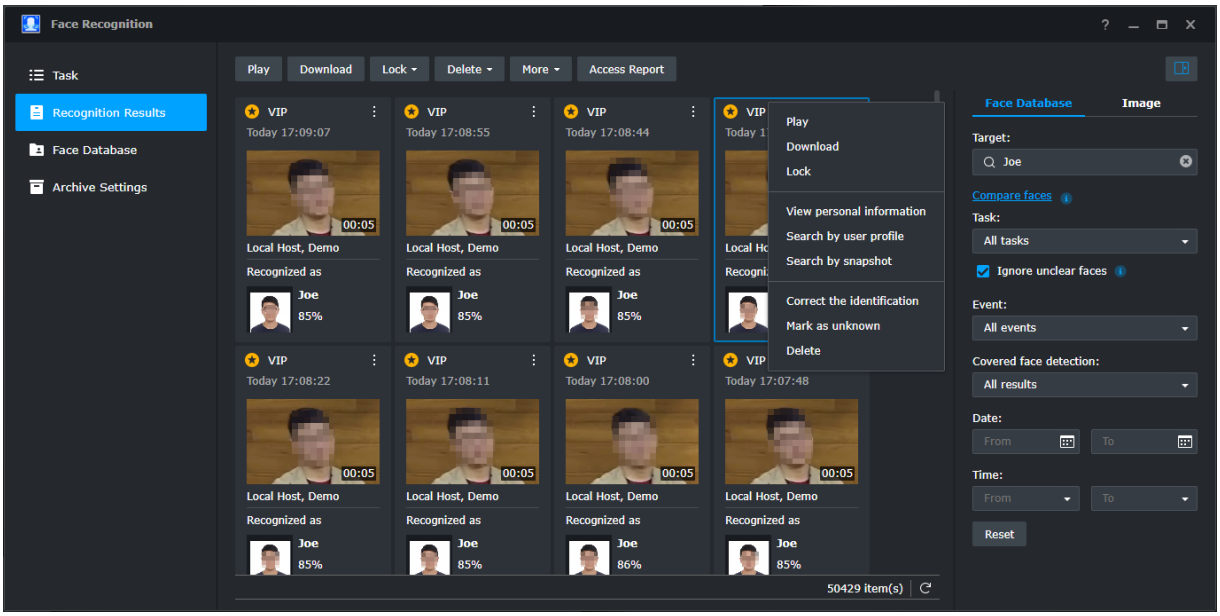
顔認識により、認識結果をタスク、イベント、および日付でフィルタリングしたり、結果の中から特定の人物を検索したりすることができます。



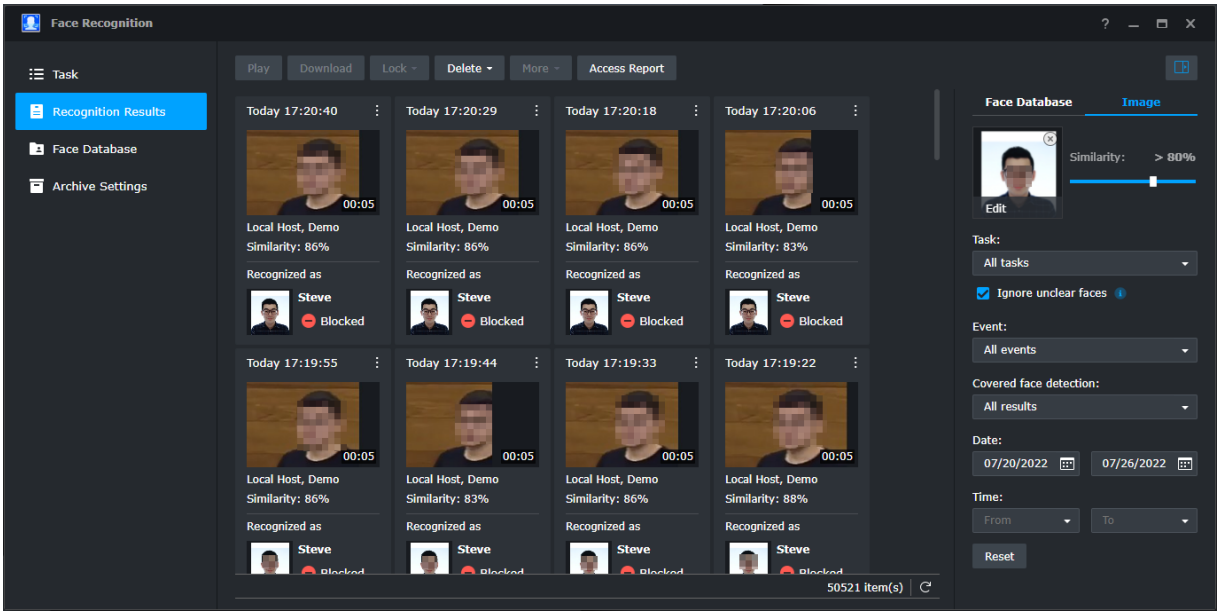
プロファイル情報で特定の人物を検索する場合、名前、アカウント、または説明を使用するか、顔画像をアップロードして検索することができます。結果は、見つかった場合、その人物が顔認識によって検出されたすべてのインスタンスを表示します。

特定の結果をロックして、アーカイブ保持ポリシーで自動的に削除されないようにしたり、バックアップ目的でダウンロードしたりすることができます。さらに、誤って識別された結果は、不明としてマー

クするか、正しいユーザープロファイルに割り当てることで修正できます。



人物が顔データベースに登録されていない場合は、顔画像をアップロードし、その画像に基づいて類似の結果を検索することで画像検索を行うことができます。あるいは、[**スナップショットで検索**] オプションを使用して [**認識結果**] で直接検索することができます。類似性レベルを調整して、それに応じて検索結果を広げたり、狭めたりすることができます。



システムが顔を識別できなかった場合でも、エラーが発生する可能性があります。名前、アカウント名、または説明で認識結果を検索できます。これにより、元のタスクとは異なる類似レベルを使用して、その人物のデータベース写真と認識結果を比較することができます。[**顔の比較**] をクリックすると、[**画像検索**] が表示され、類似レベルを調整できます。

注

- 保持できる検出結果の最大数は 1,000,000 です。

カバーされた顔の検出

顔認識は、フェイスマスクが着用されているかどうかを検出できます。結果をフィルタ化して、マスクの有無にかかわらずすべての顔を表示し、**モニターセンター**でアラートをセットアップして、顔が覆われた、または覆われていない人が検出されたときに通知することができます。

例えば、誰かがマスクを着用して銀行に入った場合、警戒を続けるためにセキュリティ担当者に通知するアラートを構成できます。

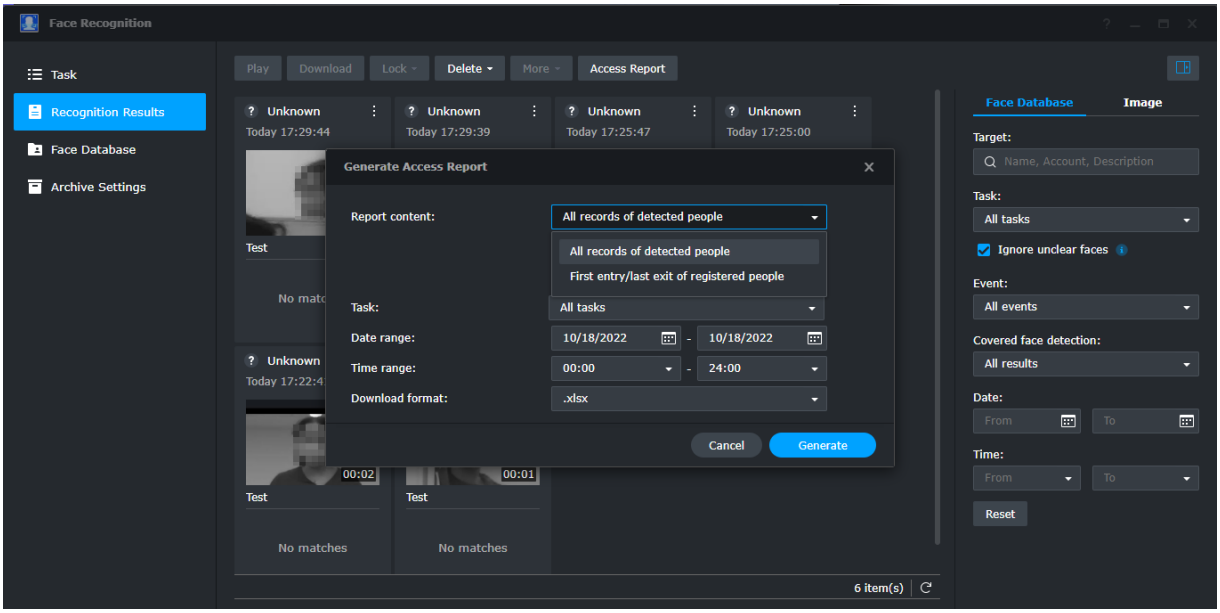
認識結果の向上

認識結果は、キャプチャした顔画像を使用して以下を行うことで改善できます。

- 新しいプロファイルを作成します以前の顔データベースが存在しない場合は、この方法で新しいデータベースを構築できます。
- 認識結果を手動で修正し、認識された個人のデータベースの写真をキャプチャされた顔画像に置き換えることで、顔データベースを更新します。
- 顔認識によって誤って識別された場合、ターゲットを不明としてリセットすることにより、認識結果を修正します。

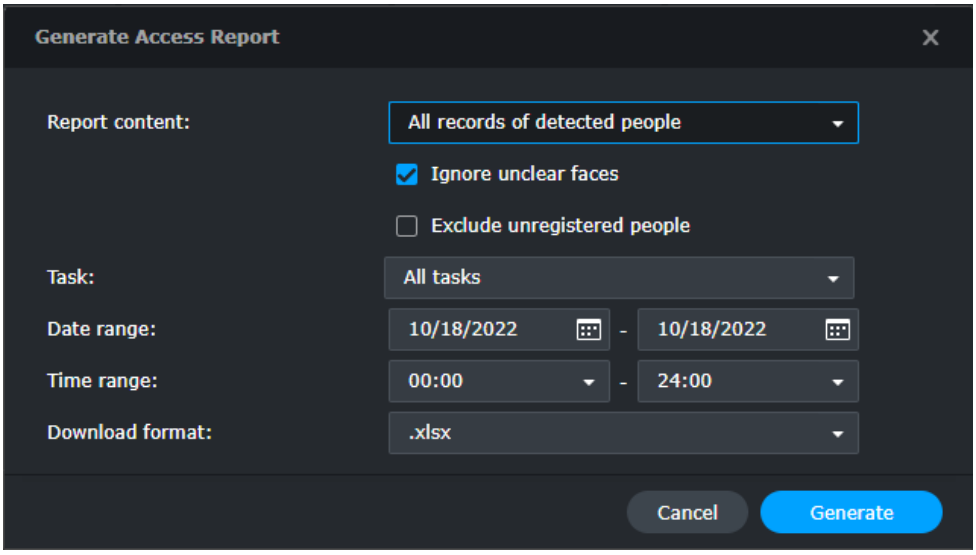
レポート

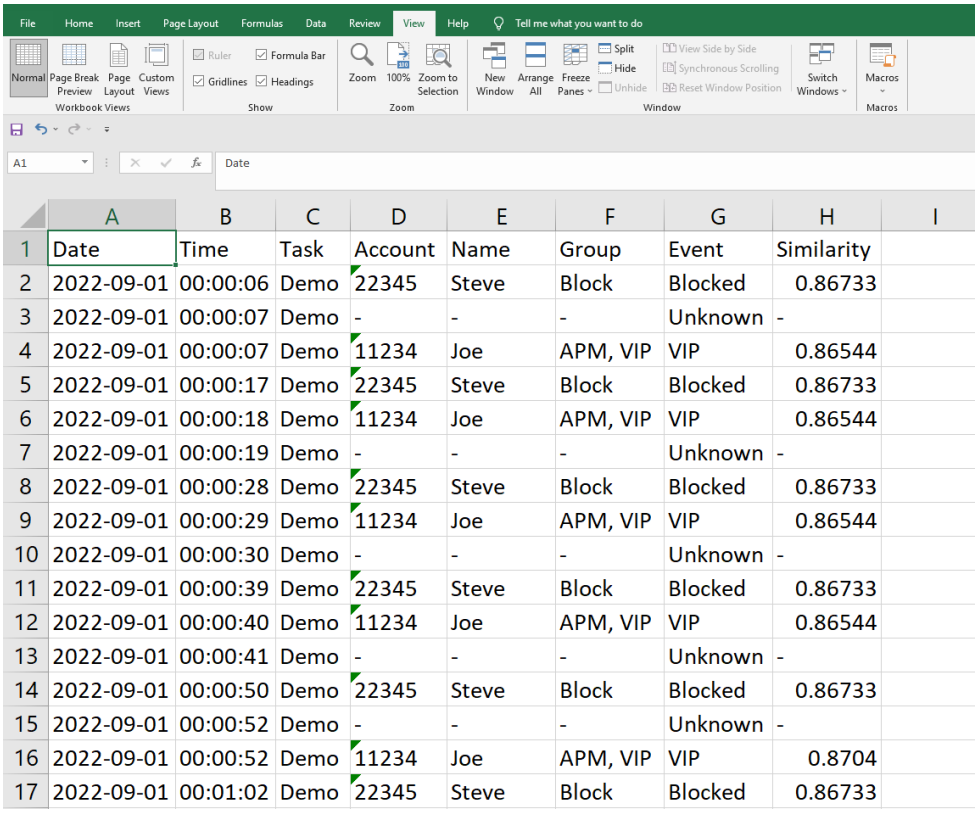
レポートは、顔認識結果の傾向を簡単に確認できる方法です。顔認識は、2 つの異なるタイプのレポートを提供します。レポートを作成するには、[**認識結果**] > [**アクセスレポート**]を選択します。



検出された人物の全記録

このレポートは、検出されたすべての人物の記録を表示します。不明瞭な顔や未登録の人物は、必要に応じて除外することができます。

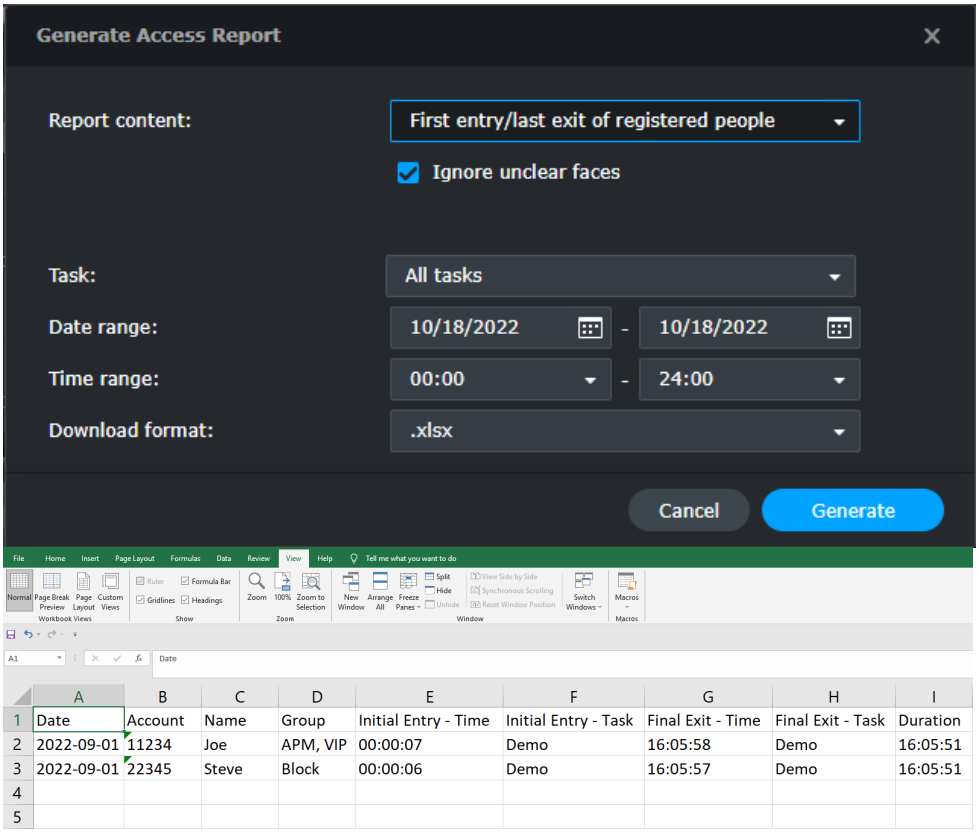




	A	B	C	D	E	F	G	H	I
1	Date	Time	Task	Account	Name	Group	Event	Similarity	
2	2022-09-01	00:00:06	Demo	22345	Steve	Block	Blocked	0.86733	
3	2022-09-01	00:00:07	Demo	-	-	-	Unknown	-	
4	2022-09-01	00:00:07	Demo	11234	Joe	APM, VIP	VIP	0.86544	
5	2022-09-01	00:00:17	Demo	22345	Steve	Block	Blocked	0.86733	
6	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	

登録された人物の最初の入場/最後の退場

このレポートは、検出されたすべての人の最初の入場記録と最後の退出記録を示します。不明瞭な顔は、必要に応じて除外できます。



	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									

付録

プライバシーの保護

顔認識技術は価値あるビジネスインサイトとアクセスコントロール機能を提供しますが、その導入に際してはプライバシーと人権の保護が非常に重要です。適切な規制がなければ、特に法執行機関による公共の使用は推奨されません。Synology は、顔の色による分類など人種プロファイリングを容易にする機能をサポートしていません。

スマート小売や不動産セキュリティなどの民間部門のアプリケーションでは、管理者はいくつかの対策を講じることができます。

- 必要な情報に基づいて、細かいアクセス権をユーザーに付与します。例えば、雇用主は、外部委託の警備員が施設に入る従業員の名前と詳細な説明を見ることを制限することができます。
- ライブフィードにテキストウォーターマークまたはプライバシーマスクを追加して、カメラビューの機密エリアをカバーします。
- データベースと照合せずに匿名ログを有効にします。DVA シリーズモデルは、検出された顔をログに記録し、必要な場合にのみ管理者による調査を支援します。
- 検出結果が特定の期間（例えば、7 日）後に自動的にローテーションされるようにスケジュールをセットアップします。

セキュリティの強化

他の Synology NAS/NVR と同様に、DVA シリーズモデルは、外部からの攻撃に対する多数の保護手段を備えて設計されています。

- すべての管理者、セキュリティマネージャ、およびユーザーは、2 要素認証を使用してログインすることを強制され、資格情報の盗難によるデータ侵害のリスクを軽減します。
- 自動ブロックは、同じ IP アドレスまたは信頼されていないクライアントデバイスから繰り返し失敗したログイン試行を検出した場合に、ブルートフォース攻撃を阻止します。
- 基盤となるオペレーティングシステム（DSM）および Surveillance Station アプリケーションは、システムを新たな脅威から保護するために継続的に更新されます。