Contents

2.0 Evolv Insights Details

  • 2.1 Performance Summary ................................................................. 4
  • 2.2 Alarm Rate & Timeline Analysis .................................................. 7
  • 2.3 Visitor Arrival Analysis .............................................................. 9
  • 2.4 Detection Setting Analysis ......................................................... 10
  • 2.5 Event Category Analysis ........................................................... 11
  • 2.6 Sensitivity Setting What-If Analysis ............................................. 12
  • 2.7 Alert Category Analysis .............................................................. 13

3.0 Solution Navigation Tips

  • 3.1 Dashboard Selection ...................................................................... 14
  • 3.2 Filters ......................................................................................... 14
  • 3.3 Interactive Specific Selection Analysis ......................................... 15
  • 3.4 Data Update Frequency ............................................................... 15
  • 3.5 Saved Views ................................................................................ 16
  • 3.6 Download Views .......................................................................... 17
  • 3.7 Reset Views ................................................................................ 17

4.0 User Settings .................................................................................. 18

5.0 User Management ............................................................................ 21

6.0 Scanner Management ...................................................................... 24

7.0 Account Settings ............................................................................. 29
Overview

The release of Evolv Insights™ now provides customers the ability to comprehensively review, analyze and gather insights on their Express systems, venue visitor arrival curves and counts, as well as detection performance.

This analysis can be accomplished across several business dimensions including sites, locations within sites, detection settings, time periods, etc. Everything is self-serve and accessed thru the secure My Evolv Portal (secure credentials with two-factor authentication will be provided by Evolv). This document provides a summary view for each of the four analytic views indicated below, explains their primary purpose, and reviews the metrics and dimensions that are available for each. General navigation of the solution will also be explained.
2.0 Evolv Insights Details

2.1 Performance Summary

Provides the ability to:

- **Quickly review** aggregated performance across the install base
- **See** individual scanner, location, and detection setting comparisons
- **Visualize** visitor arrival timelines
- **Aggregate** average, hourly & maximum visitors & alert metrics
- **Understand** unit specific performance comparisons (clear rates, detection setting usage history)
- **Answer** common questions as well as provide unique situational awareness
- **Quickly snapshot** your Express system(s) performance to send to the leadership team
- **Easily isolate** outliers across your install base of scanners

---

**Example Questions that can be answered:**

- What scanners and locations have scanning clears < 65%?
- Review historical visitor arrival curve (total & daily trend)
  - How has this changed since the COVID-19 outbreak?
- What Express detection setting do I run the most, on what scanners and locations, and what are the clear rates?
- I need to share a security equipment status for my board
  - Since installation view
  - YTD view
- Identify when visitor daily count is > than 5,000
Filters & Dimensions

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner**
- **Hour of Day**
- **Time Period**

The data in the view can also be filtered by selecting certain fields on specific charts. One may filter by scanner by clicking on a row in the central visitors totals table or by the left axis row of the “Visitors by Scanner” or “Avg. Clear Rate by Scanner” bar charts.

To filter by Detection Setting, click on the representative bubble on either “Visitors by Detection Setting” or “Clear Rate by Detection Setting” charts.

To determine the impact of changing the clear rate threshold, use the slider under the central visitors totals table. Any clear rate at or below the selected threshold will be highlighted in red text.
The following tables show a list of the specific metrics and KPIs that are represented.

<table>
<thead>
<tr>
<th>KPI or Graph</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Visitors</td>
<td></td>
</tr>
<tr>
<td>Avg. Daily Visitors</td>
<td></td>
</tr>
<tr>
<td>Max. Hourly Visitors</td>
<td></td>
</tr>
<tr>
<td>Last 30 Days Avg. Visitors</td>
<td></td>
</tr>
<tr>
<td>Total Alerts</td>
<td></td>
</tr>
<tr>
<td>Avg. Clear Rate</td>
<td></td>
</tr>
<tr>
<td>Max. Hourly Clear Rate</td>
<td></td>
</tr>
<tr>
<td>Last 30 Days Avg. Clear Rate</td>
<td></td>
</tr>
<tr>
<td>Visitors by Scanner</td>
<td></td>
</tr>
<tr>
<td>Visitors by Detection Setting</td>
<td>Size of bubble indicates total visitor count by setting for comparison</td>
</tr>
<tr>
<td>Avg. Clear Rate by Scanner</td>
<td></td>
</tr>
<tr>
<td>Clear Rate by Detection Setting</td>
<td>Size of bubble indicates average clear rate by setting % for comparison</td>
</tr>
<tr>
<td>Location Specific Summary Table</td>
<td>Conditional highlighted clear rates based on configurable threshold slider setting</td>
</tr>
<tr>
<td>Visitor Daily Count</td>
<td>Visitor daily count timeline with average for the time period indicated</td>
</tr>
</tbody>
</table>

On the bottom center of the view, two labels are provided: “Selected Hour(s)” and “Data as of”. The former provides details on the hours of day filter selection while the latter describes the number of hours since the data was refreshed.

Selected Hour(s): 08, 09, 10 and 2 more  Data as of: 16 hour(s) ago
2.2 Alarm Rate & Timeline Analysis

Provides the ability to:

- **Investigate** and perform detailed analysis and isolate scanners, locations, entrances, and time periods of interest
- **Investigate** and identify alert trends and visitor entrance flow over time
- **Drill down** to scanners, time slices, sites, and entrances to identify next steps
- **Benchmark** location / system / setting to identify outliers, optimal performance, and laggards
- **Save** a frequently visited view as a bookmark

### Example Questions that can be answered:

- Has there been any noticeable alert rate changes at the most frequently used scanners and venue entrances?
- What are the most active locations & entrances during COVID-19 and what are the performance alert rates?
- Guards called out a specific location for a significant change in threat detection in January and February. Isolate what days for review.
- We re-opened on April 1, but only at 30% capacity. I need to confirm and be able to easily report what my visitor arrival curves were (by hour) from April 1 to April 3 at my HQ site.

### Filters & Dimensions

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner ID**
- **Event Name**
- **All Data**

The data in the view can also be filtered by specific Location(s), Scanner(s), Event Name(s), Hours of Day, and Time Periods of Interest. Additionally, the visitor and alert rate time interval of analysis is configurable down to the granular 5-minute level (Year, Quarter, Month, Day, Hour, 5-minute).
Clicking on "Analyze Alerts" button will open a deep dive into the alerts rate broken down by tagged/untagged alerts, benign and threat alerts.
2.3 Visitor Arrival Analysis

Provides the ability to:

- **Visually assess** the density of visitor arrivals with a color code heat map
- **Correlate** the heat map with a timeline graph to see trends and average visitor flow over specified time periods
- **Review** visitor flow on certain days to help staff and plan for future events and days
- **Quickly create** and download a daily view of total visitor count over time for internal reviews and/or external regulatory or government consumption

### Filters & Dimensions

The data in the view can also be filtered by specific dimensions:

- Location(s)
- Scanner(s)
- Event Name(s)
- Hours of Day
- Time Periods of Interest
### 2.4 Detection Setting Analysis

Provides the ability to:

- **Holistically evaluate** Express detection setting performance across the entire security operation, identify anomalies, and benchmark across sites and locations
- **Identify** specific scanners and locations for further review and inspection relative to chosen Setting selection
- **Access** data to guide detection settings and input for future operational settings of “like venues”

#### Filters & Dimensions

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner**
- **Event Name**

The data in the view can also be filtered by specific Location(s), Scanner(s), Event Name(s) Hours of Day, and Time Periods of Interest. Additionally, the visitor and alert rate time interval of analysis is configurable down to the granular 5-minute level (Year, Quarter, Month, Day, Hour, 5-minute). There are also configurable alert rate thresholds with conditional highlighting in the table. If one removes outliers, it is possible to filter out time periods with less than 50 scans.

#### Example Questions that can be Answered:

- Identify specific Scanners with high Alert Rates vis-à-vis other Scanners with similar visitor volumes and Setting level
- Explain what appears to be odd Alert Rate vs Setting performance and the “D” and “E” levels at similar locations.

![Detection Setting Analysis Dashboard](image-url)
2.5 Event Category Analysis

Provides the ability to:
- **Drill-down** into each event or event type to understand operational and security metrics like visitor flow rate, alarm rate, and threat / benign item types
- **Compare events** of the same type to uncover anomalies, or compare different event types to understand their differences
- **Improve security** posture and other venue staffing and resource decisions – like concessions, retail, guest services, ticketing, and more – based on the needs of different events

### Filters & Dimensions

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner**
- **Event Name**

The data in the view can also be filtered by specific Location(s), Scanner(s), Event Name(s), Hours of Day, and Time Periods of Interest. Additionally, the interval of analysis is configurable down to the granular 5-minute level (Year, Quarter, Month, Day, Hour, 5-minute).
2.6 Sensitivity Setting What-If Analysis

Provides the ability to:

- **Understand** how the system would have performed, using historical visitor rate and alarm rate data, had a different system sensitivity setting been used at the time

- **Interrogate** the system for information about potential alarm rates on lower – or higher – sensitivity settings, to understand how staffing needs would have differed

- **Refine** security approach and ConOps by playing out what-if scenarios to learn whether alarm rates would have increased dramatically, or only a little, if sensitivity setting was higher; or if the same threat items would’ve been caught if alarm rates were lower, allowing for a lower nuisance alarm rate and a better visitor experience.

- **Ensure** the right-sized team is in place to address likely threat scenarios, while helping to reduce staffing needs at entryways and assist in deploying them at different locations throughout a venue.

- **Plan** for the best sensitivity setting for different events, locations, times of day, and more, by using historical data from similar scenarios and testing the effects of the new setting in a risk-free way

**Filters & Dimensions**

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner**
- **Event Name**

The data in the view can also be filtered by specific Location(s), Scanner(s), Event Name(s), Hours of Day, and Time Periods of Interest. Additionally, the interval of analysis is configurable down to the granular 5-minute level (Year, Quarter, Month, Day, Hour, 5-minute).
2.7 Alert Category Analysis

When alert tagging is used on the Evolv Express system, Alert Category Analysis in Evolv Insights provides the ability to:

- **Learn** what percentage of alarms were potential threat items vs. benign items
- **Understand** what types of threat and benign items appear most often, during what types of events, and it what entrances and times of day
- **Improve staff training** and onboarding to prepare staff better for the types of threat and benign items they’re most likely to encounter
- **Improve staffing decisions** and staff deployment in response to the likelihood of threat items they’ll likely see at different entryways, events, and times
- **Improve ConOps decisions** in response to likely benign items—for example, asking visitors to hold out umbrellas or laptops for easier visual checks if these are common benign items that alarm the system

### Filters & Dimensions

This view can be displayed across a variety of dimensions:

- **Location**
- **Scanner**
- **Event Name**

The data in the view can also be filtered by specific Location(s), Scanner(s), Event Name(s), Hours of Day, and Time Periods of Interest. Additionally, the interval of analysis is configurable down to the granular 5-minute level (Year, Quarter, Month, Day, Hour, 5-minute).
3.0 Solution Navigation Tips

3.1 Dashboard Selection
After authenticating into the My Evolv Portal you will see the Performance Summary Dashboard. To access other views, click the Insights Button and the Insights side bar will open, allowing you to select other views.

<table>
<thead>
<tr>
<th>INSIGHTS</th>
<th>SCANNERS</th>
<th>USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Summary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Rate and Timeline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visitor Arrival Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Category Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitivity Setting What-If Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Category Analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Filters
Every dashboard sheet in Evolv Insights has one or more filters. Filters are arranged in the header bar area.

- **View by:** User can view the data based on Customer, Location, and Scanner
- **Customer:** User can select and see details of single or multiple customers
- **Location:** User can select and see details of single or multiple locations
- **Scanner:** User can select and see details of single or multiple scanners
- **Event Name:** User can select and see details of single or multiple events
- **Date Range:** View defaults to trailing three months but configurable time periods can also be created by adjusting the start and end dates of the date range
3.3 Interactive Specific Selection Analysis
In all views there is the ability to select specific elements and have the displayed data dynamically respond to this selection and update the view accordingly.

3.4 Data Update Frequency
In the first release the data is being refreshed on an hourly frequency. In future releases this interval will be collapsed to a more frequent interval. The center bottom of every view displays a label indicating the number of hours since the data was refreshed.

Data as of: 16 hour(s) ago
3.5 Saved Views
By using the View Original button you can save and bookmark any specific view with desired dimensional filtering that you would like to access on a regular basis. Once saved this named view will be a candidate dropdown selection when you open the View Original Button.

How to save or bookmark a view

![Image of saved views dialog box]

- Name this view
- Make it my default
- Save

Manage Views
3.6 Download Views
By using the **Download** button, you can download the view to an Image, Data Table, pdf or PowerPoint. Depending on the dashboard this can be for the entire page or select graphs/KPIs on that page. Selecting the specific graph or table prior to download will determine the data that gets downloaded in the case of the data and crosstab cases.

3.7 Reset Views
As you explore a view, you may want to undo or redo a filter or reset the view entire. These tasks can be undertaken from the top left menu:
4.0 User Settings

4.1 View Your User Profile
From the user menu, a user may update their user profile. This screen will allow the user to update first and last name, email address, and contact phone number.
4.2 User Preferences

Under Settings, the user may subscribe to available notifications, as controlled by the Administrator (described below):

- Scanner Settings Updates
  - The user shall be notified when a setting changes on a scanner e.g. if the detection setting changes from 'E' to 'A'
- Scanner Communication State
  - The user shall be notified when the system detects a scanner connecting or disconnecting from the portal
- System Feature Releases
  - The user shall be notified when Evolv releases new software

There are three communication channels:

- Email
  - User shall be notified to their registered email address
- SMS
  - User shall be notified to their registered phone number (if available)
- Portal
  - User shall receive a notification in the notification panel on the portal

For each notification type, the user may select one of the three communication channels.
It is also possible to filter scanner notifications by selecting a list of scanners. If no scanner is selected (the default setting), notifications from all scanners will be received. If one or more scanners are selected under filter, then only notifications for those scanners will be received.
5.0 User Management

A user with the role “Customer-Admin” may update existing user details and add/remove users with the “Customer-Basic” role. These settings can be accessed from the “Users” menu item under Administration via the user menu.

The available user roles are:

• Customer-Admin
  ◦ Users with this role may manage scanners, user details, user notification permissions, add users with ’Customer-Basic’ role, access support documentation and view insights’

• Customer
  ◦ This is the default user role and users with this role may access support documentation, view scanner information, and view insights

• Customer-Basic
  ◦ This is a limited role and users with this role may access support and view scanner information

The user table is visible to users with the ’Customer-Admin’ role. The user may click to add a user with the role Customer-Basic, click to edit some user details, and click to delete a user.

The add/edit user dialog requires input of username, email address, role, and customer. It has several optional fields: first name, last name, and phone number. If phone number is provided, it will be used for dual factor authentication.
After a user is created, an admin may edit which notification types and channels a user may have access to under their preferences. By unchecking the cell in the notification type/channel matrix, the user will no longer be able to select that notification type/channel combination.

Drill-down into a user to view or change User Information (Info), to set Request Assistance Notifications for the user, and to select which Notifications the user is allowed to subscribe themselves to in the User Profile menu above.
Subscribe this user to Request Assistance Notifications

Assign which notifications this user can self-subscribe to

User Management
6.0 Scanner Management

To view and manage scanner settings, select the Scanners menu. Choose a scanner to drill-down into, and you'll see a menu containing "Info, Statistics, Version, Settings, Commands, Log Uploads, Tablets, and Request Assistance Subscribers." Each menu is used as follows:

Select a scanner and choose Info to change its Alias - that is, a customer-friendly name that reminds you where it is located, for example:

![Scanners table]

- **View all scanners in the Scanners menu**
Select Statistics to view the statistics as they are displayed on the tablet for this scanner.

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last hour</td>
<td>82</td>
</tr>
<tr>
<td>Since reset (lane1+123371 lane2=351118)</td>
<td>474489</td>
</tr>
<tr>
<td>Persistent total</td>
<td>929931</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alerts</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total (rate=6%)</td>
<td>31177</td>
</tr>
<tr>
<td>In lane 1 (rate=6%)</td>
<td>7535</td>
</tr>
<tr>
<td>In lane 2 (rate=6%)</td>
<td>23642</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Throughput (per hour)</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak (over 5min) since statistics reset</td>
<td>852</td>
</tr>
<tr>
<td>Peak (over 5min) during last hour</td>
<td>180</td>
</tr>
</tbody>
</table>

Select Version to see what software version is operating on this scanner.

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Version</td>
<td>4.0.0</td>
</tr>
<tr>
<td>AFD Version</td>
<td>3.0.0.18474</td>
</tr>
<tr>
<td>TXCD Firmware Version</td>
<td>SY5: 02.02.01.030821 TX: 02.02.01.030821 ECS: 02.01.03.102920</td>
</tr>
<tr>
<td>DAS Firmware Version</td>
<td>D00211CC, D00211CC, D00211CC</td>
</tr>
<tr>
<td>Diagnostics Version</td>
<td>3.0.0.5</td>
</tr>
<tr>
<td>OS Image Version</td>
<td>140-00611-01-2.7</td>
</tr>
<tr>
<td>Windows Version</td>
<td>Windows 10 Enterprise LTSC 2019 6.3.17763.1518</td>
</tr>
<tr>
<td>TeamViewer Version</td>
<td>2.1.0.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer System</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CAPA560</td>
</tr>
<tr>
<td>Version</td>
<td>AX-CAPA560-17-EVOLV4</td>
</tr>
<tr>
<td>Identifying Number</td>
<td>E2099ES001000229</td>
</tr>
</tbody>
</table>
Select Settings to change any scanner settings the same way you would if you were an Administrator user at the tablet for this scanner. This function requires multi-factor authentication to verify some critical changes.

Perform commands on this scanner the way you would if you were co-located with the scanner, logged in as an administrative user on the tablet.
Perform administrative functions on this scanner like uploading logs to Evolv for troubleshooting and support.

Learn more information about tablets connected to this scanner.

See which users are subscribed to receive Request Assistance Notifications from this scanner.
Select the gear icon to see Account Settings - previously known as Global Configuration Settings - for customer administrators in the MyEvolv Portal. Here, you can set up Events using the Events option.

After clicking on the “Add Event” button, a new event may be added by entering an event name, selecting a location for the event (based on scanner locations), start date and end date, and an event category.
New events will be visible on the analytics views after a 30 minute sync with the scan data. With this, the scan data may be filtered by the selection of one or more events.

The Request Assistance tab within the Global Config menu allows the Customer-Admin to subscribe users to receive notifications of requests for assistance by tablet users at a scanner. All users with an email and/or mobile number in their profile will appear in the list. Once a user has a notification method selected, the option to select scanners will become active. Click “None Selected” to see a list of available scanners. Scanners are grouped by Primary Location with the option to subscribe the user to alerts for any combinations of scanners. Click “Save” when done. After completing subscription updates, click “Submit” at the bottom right.
On the Request Assistance tab, users may be subscribed or unsubscribed. If there are one or more subscribed users, the "Request Assistance" button (triangle, top center of tablet screen) will be activated on the selected Express systems.

If there are no users subscribed for a given scanner, then Request Assistance will not be activated on that scanner. The scanner must be running software version v3.0.0 or higher to enable this feature. It is important to note that email subscriptions must be confirmed to take effect. Also, there may be up to a 15-minute delay after a user is subscribed before messages are received, although the Request Assistance button activates on the tablet immediately. Once the subscription process is complete, Request Assistance notifications are received almost instantly by subscribed user(s).

Other Account Settings include the ability change the Visitor Label and the chance to assign user Idle Time-Out limits before automatically logging out of the system.
Administrator controls to configure integrations: Connect the extended security ecosystem with information about identified threats at every entrance with Evolv Express, improving visibility and response time for supporting teams across the venue.

Integration to Milestone VMS (Video Management System): with the new Milestone downloadable plug-in sends verified alerts (i.e., those that have been “tagged” as a threat item on the tablet) to the Milestone Xprotect Smart Client instance in the SOC (Security Operations Console) or any other location, for visibility, rapid response, and forensic analysis. Milestone can display the threat localization image, threat type, time of alert, system location, lane in the SOC, and video feeds from the optional front and rear cameras on Evolv Express (or other associated venue security camera). Request Assistance notifications sent from the tablet and video feeds from the optional front and rear cameras on Evolv Express (or other associated venue security cameras) can also appear in the Milestone VMS.

Details on how to install the Milestone plug-in will be provided in a separate integration installation document.

The Milestone UI can display (upper LH image) Verified Alerts sent by Express; (lower LH image) Request Assistance notifications sent by Express; and (two RH images) Front and rear camera feeds from Express or any other venue surveillance camera that is on the Milestone server. The specific layout of the Milestone client view panes is configurable.
Image data and live video feed at the time of the alert are stored for future forensic analysis and can be leveraged by existing Milestone integrations to video analytics technologies.

Please note that, while the Express front and rear camera feeds are displayed in the examples above, any camera system connected in Milestone system can be associated with an Evolv Express alert and RA notification for the purposes of getting a good view of the system both in the live feed when the alert appears and when playing back the alert for future forensic analysis.

Setting up the Milestone integration in the MyEvolv portal is easy:

When integrated with Evolv Express, the Alarm Manager in Milestone includes historical alerts sent by Express for playback: including the video feed associated to that Express system. This association is set up in the Milestone Management Client.

With the integration enabled in the Milestone client, the customer must proactively provide their consent to store verified alert images on the Cloud, which are then pushed to the Milestone VMS based on configuration rules. The default image retention policy is storage for 7 days, after which the image is deleted.
Select scanners to communicate with the Milestone system and enter the username and password provided by Evolv at installation of the Milestone integration plugin. Options to remove this integration and/or set up another one are also found here.

**Integration to Titan HST Mass Notification System** communicates the threat localization image, verified threat type on the Express resolution tablet, time and location of alert, and Request Assistance notifications to the Titan HST user experience.

As shown above, a verified alert (or, an alert that has been “tagged” on the tablet as a Threat item – gun, knife, threat other, etc.) appears in Titan HST together with the Threat Type, location, time, and date: accelerating response time, enabling “chat” around the communicated threat, and triggering existing Titan workflows like lock-down, request for backup, SOS messages, elevation to local law enforcement, and others.
In the same way, Request Assistance alerts can be viewed and interacted with in Titan HST, including time, date, location, and message entered into the tablet by the operator.

Just like other alert objects in Titan, the system can enable chat related to the alert for security officers with access to the system, communicate data to existing VMS and SOC platforms to which Titan is integrated, and trigger additional actions based on the system's rules engine—including automatic notifications, backup response protocols, door locking, and more.

Plus, past alerts can be recalled for forensic analysis in the system:
Resolved alerts in Titan can display an alert history of those sent by Evolv Express and resolved by the user. Selecting a resolved alert re-opens the original alert image and its metadata.

Setting up the Titan HST integration in the MyEvolv portal is easy:

![Titan Integration 1](image)

With the integration enabled in the Milestone client, the customer must proactively provide their consent to store verified alert images on the Cloud, which are then pushed to the Milestone VMS based on configuration rules. The default image retention policy is storage for 7 days, after which the image is deleted.

![Alert Triggers](image)

Alert triggers map terminology for Express tablets (Gun, Other, Request Assistance, etc.) to terminology in Titan HST. Your Titan System Administrator can supply the required Titan Trigger IDs and API keys (one pair of unique character strings for each Threat Tag in Express)

![Scanners](image)

Select scanners to communicate with the Titan system. Options to remove this integration and/or set up another one are also found here.
Contact us to learn more about how to protect your workforce and facilities with touchless security screening.

info@evolvtechnology.com +1 781.374.8100