Concealed Weapons Detection Cloud Portal User Guide

July 2023

©2023 Motorola Solutions, Inc. All rights reserved.

This page intentionally left blank.

Table of Contents

Introduction

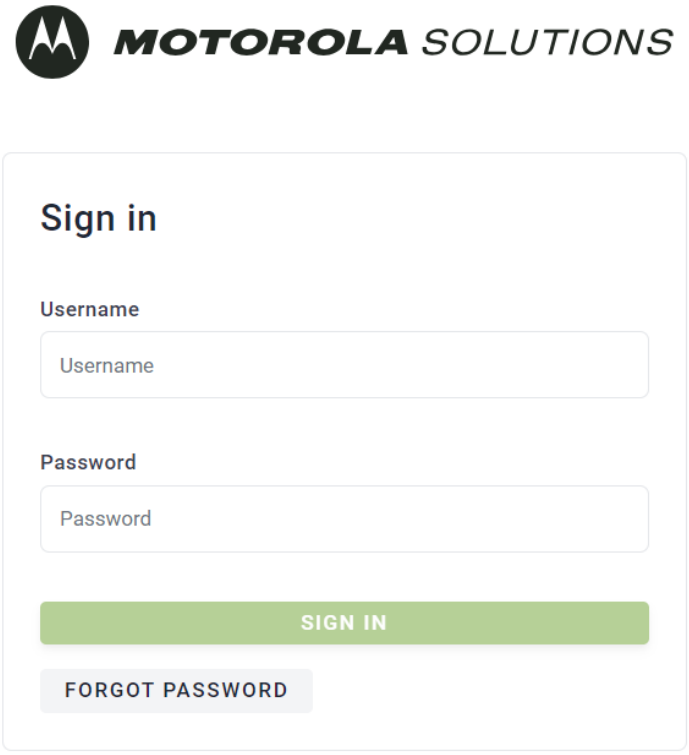
The Cloud Portal is an application that allows you to monitor and configure a Concealed Weapon Detection (CWD) System through a singular user interface. The Cloud Portal provides both web-based or mobile access to insights, analytics, and support.

This User Guide outlines how to remotely configure and manage the CWD system, as well as customize various system settings.

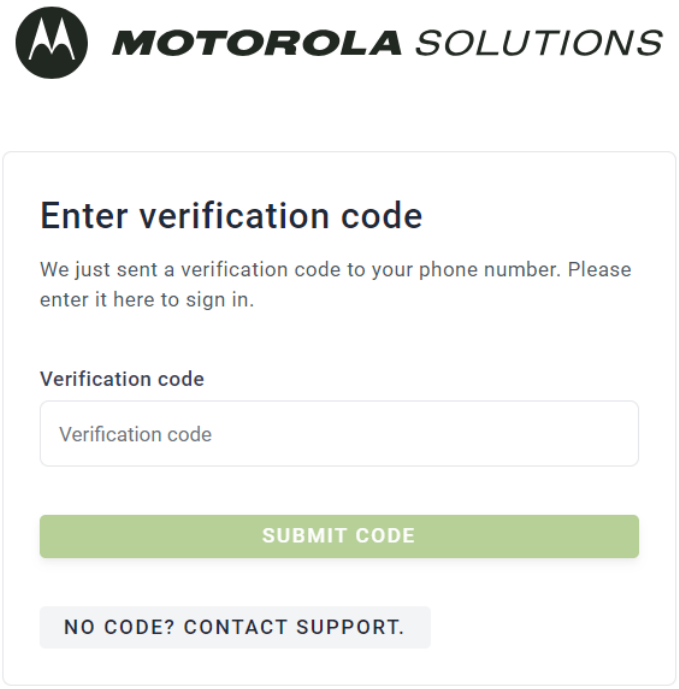
Sign In

To sign into the Cloud Portal, you will need to provide a valid username and password. Contact your Customer Success Manager to obtain sign in credentials.

1. Enter your Username and Password.
2. Click **Sign In**.



3. If the credentials you provided in step 1 are correct, you will receive a verification code via SMS.
4. Enter the verification code and Click **Submit Code**.



5. If you did not receive a code, contact support by clicking **Contact Support**.

Dashboard

After signing into the Portal, the user can access insights, scanner information, system users, support, notifications, account settings, and also their own profile settings.

Profile

The user can access their profile by clicking the Profile icon on the top menu.

Personal Information

1. To edit your personal information, select the profile icon at the top-right of the window.
2. Click **Profile**, from the drop-down menu.
3. Edit the fields, and click **Save**.
4. To cancel the changes, click **Cancel**.

Account Settings

Under Account Settings, the user can edit Notifications and Reports.

1. To edit your account settings, select the **profile** icon at the top-right of the window.
2. Click **Settings**, from the drop-down menu.

Notification Settings

Under Settings, select **Notifications** from the menu on the left. Under Notification Settings, the user can configure which notifications they receive and where the notifications are sent.

Enabling Notification Channels

1. To enable certain notification channels, click the toggle next to the Notification type, outlined in the table below.
2. Toggle either **Email**, **SMS**, or **Portal** endpoints.
3. Click **Save**.

 **NOTICE**: Changes may require up to 15 minutes to take full effect.

Notification Channel	Description
Communication	Sent when Online / Offline state changes on CWD systems.

Settings Updates	Sent when system settings change on a CWD system.
Verified Alerts: Threats	Sent to the Customer Administrator when a threat is detected and verified.
Scanner Maintenance	Sent to the user responsible to system maintenance as a reminder of routine maintenance.
Feature Release	Sent when system release is available.

Notification Filters

Under Notification Filters, the user can configure which scanners they receive notifications for, and what types of notifications they receive.

1. To create a notification filter, navigate to the Notification Filters tab, beside the Notification Channels tab.
2. To add a notification filter, click **Add Notification Filter**.
3. In the pane that appears, click **Search Scanner**.
4. Start typing in the drop-down menu that appears, to search for a scanner.
5. Click the scanner to select it. You can also click **Select All**.
6. To deselect scanners, click **Deselect All**.
7. Click away to exit the drop-down menu.
8. Toggle from the list of options, to add those options as notification filters. The options following options are available to certain users depending on their account type and privileges:
   - Feature Release
   - Settings Updates
   - Communication State
   - Scanner Maintenance
   - Verified Alerts: Threats
9. Click **Add Rule**, to save your changes. The notification filter will appear in the list of notification filters.

Reports

The user can configure which reports they receive. For example, by enabling Event Reports, the user will receive all Event Reports.

Subscribing to Reports

1. Under Settings, select **Reports** from the navigation bar on the left.
2. To subscribe to a report, select the toggle next to the report type. Changes are saved automatically.

Insights

Insights allow customers to comprehensively review data and analytics on their CWD systems

Performance Summary

The Performance Summary feature is for managers who require a high-level view of Key Performance Indicators (KPI) data for the previous 30 days to inform and manage their facility's safety protocols and customer experience. Data generated from the Performance Summary provides the following insights:

- Quickly review aggregated performance data 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 frequent questions as well as provide unique situational awareness.
- Easily isolate outliers across your install base of scanners.

Alarm Rate and Timeline Analysis

The Alarm Rate & Timeline Analysis allows the user to investigate and perform detailed analysis related to alarm rates within specific time frames and locations. Data from the Alarm Rate & Timeline Analysis provide the following insights:

- Investigate and identify alert trends and visitor entrances to flow over time.
- Examine, in-depth, the scanners, time slices, sites, and entrances as related to alarm rates for potential improved security and customer experience.
- Benchmark location/system/setting to identify outliers, optimal performance, and laggards.
- Save a frequency visited view as a bookmark.

Visitor Arrival Analysis

Utilizing a heat map, the Visitor Arrival Analysis provides the user a clear visualization of the volume of visitors entering a venue. Data from the Visitor Arrival Analysis provides the following insights:

- Visually assess the density of visitor arrivals with a color-coded 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.

Detection Settings

The Detection Setting Analysis comprehensively evaluates the CWD detection setting across the entire security operation. This analysis can identify anomalies and benchmarks across sites and locations. Data from Detection Settings provides the following insights:

- 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 operation settings of similar venues.

Event Category Analysis

The Event Category Analysis allows for the in-depth examination of each event and/or event type (i.e., concert, children's event, sports, etc.) to better understand operational and security metrics such as visitor flow rate, alarm rate, and threat/benign item types. Data from Event Category Analysis provides the following insights:

- Compare events of the same type to uncover security anomalies and/or compare different event types to understand their differences for the purpose of staffing and training.
- Improve security posture and other venue staffing and resource decisions – such as scanner sensitivity level, concessions, retail, guest services, ticketing, and more – based on the needs of different events.

Sensitivity Setting Analysis

The Sensitivity Setting What-if Analysis feature shows how the system would have performed if a different system sensitivity setting been used during the event. This Insight feature uses historical visitor rate and alarm data to create the what-if analysis. Data from Sensitivity Settings Analysis provides the following insights:

- 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 minimally, if sensitivity setting were higher; or if the same threat items would have been caught if alarm rates were lower, allowing for a lower nuisance alarm rate and a better visitor experience.
- 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.

Alert Category Analysis

This feature is also accessible in the Alarm Rate & Time Analysis and the Detection Setting Analysis. The Alert Category Analysis feature provides the user the ability to understand what percentages of alarms are potential threats or benign. Data from Alert Category Analysis provide the following insights:

- Learn what percentages 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 what entrances and times of day.

- Improve staff training and onboarding to prepare staff better for the types of threat and benign items they are most likely to encounter Improve ConOps decisions in response to 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.
- Click on “Select Tag to Highlight” button to open an in-depth examination of specific Benign and Threat counts and provide muliple data assessment views.

Security Performance

Security Performance provides the user with visual and numerical data on how much time it takes security staff to complete alert screening. Specifically, data is compiled for the number alerts, tagged alerts, alert screening time and the number of visitors. The data is presented both numerically and visually to provide an overall average of tagged alerts and time it takes to complete screening. The data can be filtered by specific alert type: weapon, location, event, and date. Data from Security Performance provides the following insights:

- Compare alert screening time with number of tagged alerts. This statistic can be isolated by location and event.
- Compare percentage of tagged alerts by average number of patrons.

Daily Screening Report

Daily Screening provides a view of visitor arrival, alert rates, and tagged threat items for the last 24 hours or for a custom date and time range. Data from Daily Screening Report provides the following insights:

- Identify time and location of any visitor surges and lulls to know when to increase or decrease staffing and potentially open or close lanes.
- Divert visitor traffic from high-traffic areas to low-traffic areas to improve visitor experience.
- Subscribe to have a copy of the Daily Screening Report sent daily directly to your email for review with your teams at the beginning or end of each day’s shifts.

Event Report

The Event feature provides a view of visitor arrival, alert rates, and tagged threat items for each of your events that you define within the Portal, under the Events tab. Data from Event Report provides the following insights:

- Identify time and location of any visitor surges and lulls to improve staffing and operations decisions for future events.
- Divert visitor traffic from high-traffic areas to low-traffic areas to improve visitor experience.

Scanners

The Scanners tab gives the user access to information on the CWD scanners.

1. Under the Scanners tab on the Dashboard, select Scanners from the drop-down list.
2. Select an individual scanner from the list to view additional information.

The Scanners page provides the following information pertaining to each scanner the user has access to.

- Scanner (Status)
- Portal (Connectivity status)
- LTE (Connectivity status)
- Name
- Location
- Secondary Location
- Alias
- Host Version (Release Number)
- Lanes (1, 2 or Both)
- Lane Width (Wide or Standard)
- Sensitivity (Settings A-G)
- Alarm Rate (Percentage)
- Last Updated (Time since last update)
- Generation (Model)

Searching Scanners

The user can use the search bar to search for scanners. The search results update automatically.

Filtering Results

Use the filter feature to narrow the search results, or to search for key information is specific fields.

1. Click the **Filter** icon, to choose from the following filters.
   - Customer
   - Host Version
   - Name
   - Location
   - Alias
   - Secondary Locations
2. Type into the associated fields to narrow results. The list of scanners will update automatically.
3. To clear filters, click **Clear Filters**.

Hiding Columns

1. Click the Eye icon.
2. Select a category to remove it from view.
3. To make the column visible again, re-select it from the list.

Exporting Results

1. Click the upside-down arrow icon to export files in CSV file format.
2. The download should begin automatically.

Information

The Info tab shows system information:

- Name
- Alias
- Location
- Secondary Location
- Last Updated
- Alarm Rate
- Generation
- Lane Configuration
- Lane Width
- Host Version
- Sensitivity

Editing Scanner Alias

Under the Information tab, the user can also edit the scanner Alias.

1. Edit Alias
2. Click **Save**.

Statistics

The Statistics tab shows some system metrics:

- Estimated Number of Visitors: provides the total number of visitors per hour for the last hour.
- Number of alerts: the percentage of alerts based on the number of visitors for each lane or both lanes combined.

- Throughput: provides the peak number of visitors over a 5 minute period, per hour.
- Info: provides information regarding last reset and last scan ID.

Version

The Version tab shows the software version listed by system, computer, camera, and router.

You may need to provide this information when contacting Support.

Settings

The Settings tab shows the settings pertaining to the functionality of the scanner. Editing Settings requires Admin privileges. These Settings include:

- Primary Location: Where the scanner is primarily physically located.
- Secondary Location: Where the scanner is relocated to.
- Scan Sensitivity (Metallic): Provides enhanced detection of smaller threats.
- Scan Data Retention: Determines how much scanner data is saved.
- Export System Info: Determines which information is exported, e.g., Database Only, Logs Only, or Diagnostic Data.
- Alert LED On Time: Shows the duration the system stays on red LEDs when an alert is received.
- Alert Tagging: Can be enabled or disabled.
- Home Screen Sensitivity Display: Shows whether the metallic sensitivity level is displayed on the tablet home screen.
- Simultaneous Alerts: Enables multiple scans in quick succession to be side by side on the tablet when alerts are received. Simultaneous and aggerated can both be enabled at the same time.
- Aggregated Alerts: Enables multiple threat detection boxes within a single alert to the tablet. Simultaneous and aggerated can both be enabled at the same time.
- Physical Lane Configuration: Configure the CD system to operate as lane 1, lane 2, or both. Lane configuration can also be set from the tablet if logged in as an Admin.
- Fan Mode: Fan can be shut off to reduce system noise.
- Access Control: The CWD can be integrated with external equipment (sold separately) to control access to facility entrances. The Access Control setting allows this feature to be enabled or disabled.
- Wireless Capability: Enables tablets to connect to the scanner using Wi-Fi.
- Camera Lane Configuration: when this is set to Single Camera Per Lane, additional controls can be set to either Static Only or Static and InMotion. Dual Cameras Per Lane is only functional for systems with cameras installed in both CWD towers.
- Location and Timezone Override: can be enabled or disabled.

Commands

The Commands tab gives the Customer Administrator (CA) manual control over the CWD system. The following commands are described below:

- Identify: Flashes the Status Indicators on the CWD Lanes of the system the tablet is assigned (for wireless tablets).
- Export Logs: Export CWD logs to USB (Service Function).
- Upload Logs: Sends the current logs to the portal.
- Reset Statistics: Resets the statistics displayed on the tablet for this CWD.
- System Sleep: Turns OFF the Status Indicators and places the Host Computer into a Sleep Mode. The CWD system will remain ON but not operational until power is reset.
- System Shutdown: Gracefully shuts down the CWD system by closing Host services and prepares the system for removal of power. Highly Recommended Before Turning Power OFF.
- Reset Administrative Password: This command feature allows the CA to reset the system's administrative password. One-time verification code is sent to the CA's email when this command is executed.
- Reset Service Password: This command feature allows the CA to reset the service password. One-time verification code is sent to the CA's email when this command is executed.
- Restart System: Restarts the CWD without powering off the scanner.

Log Uploads

The Log Uploads tab shows a list of uploaded files, e.g., scanner data. This is where the user can upload files.

Tablets

The Tablets tab shows a list of tablets, as well as the following information:

- Tablet GUI
- Kiosk Software
- OS Version
- Security Patch

ACC Configuration

The ACC Config tab shows configuration details regarding ACC. This is where the user can enable ACC and configure the connection.

Alert Tags

The Alert Tags tab allows a Customer Administrator to check and change alert tags for the individual scanner. Use the Settings tab to modify alert tag setting for multiple scanner at once.

Administrator configured alert tagging is only available on CWD scanners running Host Version 4.0+. Scanners running previous software versions have static pre-configured tags

Updating Alert Tags

1. To update a scanner with the new tag configuration, select the scanner from the list.
2. Using the cursor, drag Alert tags and Benign tags from the inactive tags to the active tags (or vice versa). Up to nine (9) total tags can be active.
3. Click Review and Submit.

Request Assistance Subscriptions

Users subscribed to Request Assistance are listed in this section. User Subscriptions are those individuals whose user roles subscribed to receive Request Assistance notifications from a scanner.

The Messages feature is where the user configures Request Assistance Messages to be synchronized with the scanners. These messages are displayed on the tablet when the operator uses the request assistance feature. A maximum of 5 custom messages can be set. If freeform text is enabled, a maximum of 4 custom messages can be set. A minimum of 1 custom message must be set for freeform text to be disabled. Add a custom message to disable freeform text.

Location

The Location of the scanner can be identified in this section as a Secondary Location. The Secondary Location is shown in all Insights reports related to the CWD and on the Tablet Home Screen.

Maintenance

The Maintenance tab displays routine maintenance information for a scanner. Use this feature to do the following:

- Turn the routine scanner maintenance On or Off for each scanner.
- Define whether the scanner restarts or upgrades during maintenance.
- Determine the frequency and timing for maintenance to occur on the scanner.
- End routine maintenance preferences to the scanner.

Users

Managing and operating a CWD system is role dependent. A user's role determines what features are available to them. The following sections explain the CWD roles and their level of access.

Customer Administrator Role

The Customer Administrator has the highest level of access to the system Customer Administrator Role (CA). The Customer Administrator can add users and subscribe those users to receive customer support notifications. The Customer Administrator role also has access to Insights. They can configure settings and enable or disable commands including:

- Alert Display Configuration
- Alert Display Configuration for Threat Resolution
- Alert Display Configuration for Flow Control
- Alert Tagging
- Alert LED On Time
- Access Control
- Aggregated Alerts
- Camera Lane Configuration
- Export System Information
- Fan Mode
- Home Screen Sensitivity Display
- Physical Lane Configuration
- Simultaneous Alerts
- Scan Data Retention
- Scan Sensitivity
- Data Extract API

Customer Role

The Customer role has access to the Insights Data Analytics feature of the CWD system, Insights, and limited access to Scanner functions. Insights access allows the user(s) the ability to comprehensively review, analyze and gather data on their CWD systems. Some of the data and analytics include are venue visitor arrival curves and counts, as well as detection performance. Analysis can be accomplished across several business dimensions including sites, locations within sites, detection settings, time periods, etc.

The Customer role is most likely the person responsible for collecting security data for a venue. They may not have Customer Administrator access. However, this level of access could be part of the Customer Administrator role. For example, the person who is responsible for compiling and analyzing a venue's data as it pertains to security protocols, such as a Security Manager.

Customer Basic Role

The Customer Basic role can receive notifications and send request assistance messages from the tablet only. The Customer Basic role is usually designated for those security personnel operating the system for a venue.

Distributor Role

A Distributor supports the customer with the CWD System. They can access Insights, and CWD system settings and command features, that do not change the operation of the scanner. In most cases, the distributor is responsible for training the customer.

User Settings

To access User Settings, select **Users** from the top menu.

Editing User Settings, requires Customer Administrator account privileges. A Customer Administrator can view a list of users, add new users, and modify existing users.

Adding Users

1. To add a user, click **Add User**.
2. Enter a username, email address, first name, last name, and phone number. Their phone number is required for 2-step verification.
3. Click **Submit**.

The Customer or the Customer Basic user will be sent an email with temporary password to login to the Cloud Portal. The new user will be asked to change their password when logging in for the first time.

Editing User Information

1. To edit a user's information, select the username from the list.
2. Edit the relevant fields.
3. Click **Save**.

Enabling Notifications

The Customer Administrator can provide access to notifications to Customer and Customer Basic users. However, all notifications need to enabled by the user in the Notification feature in Settings. For instructions on subscribing to notifications, see *Account Settings on page 4*.

Settings

The user can access Settings by clicking the Settings icon on the top menu.

Editing Settings depends on the user's account privileges. This section outlines all configurable Settings based on the Customer Administrator's account privileges.

Events

Before you can create a new Event, you have to add a new category.

Adding a New Category

1. Under the Events tab, navigate to **Categories**.
2. Enter a name for the **New Event Category**.

3. Click **Add Category**. The New Category will appear in the list.

Creating an Event

1. Under the Events tab, navigate to **Events**.
2. Click **Create Event**.
3. Add a Description.
4. Choose a Location from the drop-down menu.
5. Select a Category from the drop-down menu.
6. Select a Date. The current date is the default. To push the start date back a day, click the **+** button.
7. Choose a Reporting Start Time. You can edit the date and time fields or use the pop-up calendar to select a start time.
8. If the Event Start Time is the same as the Reporting Start Time, select the check-box.
9. Choose a Reporting End Time. You can edit the date and time fields or use the pop-up calendar to select an end time.
10. Click **Create**.

Editing an Event

1. Select an Event from the list.
2. Edit the fields.
3. Click **Save** .
4. Click **Duplicate** to create a copy of the Event. The Create Event pane will appear and you can edit and save the copied Event as a new Event.

Importing Events

If you need instructions on how to structure your CSV file, you can download an example file by clicking **Sample File**.

1. Click **Import Events**. A new window will pop-up.
2. If you need guidance, you can download the Sample file from the pop-up window.
3. Drag and drop a CSV file for import.

It may take up to 30 minutes to sync the upload. Then new events will be visible.

Deleting Events

1. Select the Event from the list.
2. Scroll to the bottom of the Edit pane.
3. Click **Delete**.

Visitor Label

Use the Visitor Label to change the term for site visitors based on location, e.g., students, patients, patrons. The visitor label is used in Insights and Reports and should reflect the type of screening conducted.

Changing the Visitor Label

1. Enter a Visitor Label
2. Click **Save**.

Idle Timeout

All users are automatically logged out of the Portal after a set period of time. The Customer Administrator can adjust the duration of inactivity before the user is logged out. This Idle Timeout feature is solely for the online portal and differs from the Admin idle log out on tablet.

Editing User Idle Timeout

Enter the number of hours of inactivity required before a user is automatically logged out.

1. Enter a number (hours) for either Admin User or Non-Admin User Idle Timeout.
2. Click **Save**.

Integrations

The Integration feature allows customers and channel partners to integrate their existing security systems with MSI CWD to monitor alerts, events, and other data sources from a tablet, computer, etc. Integration of Mass Notification systems and Video Management Systems (VMS) allows for enhanced visibility and rapid response to threat detection encountered during screening with a CWD.

Titan HST Mass Notification Integration

The Titan HST Mass Notification System communicates the threat localization image, verified threat type on the CWD Resolution tablet, time and location of the alert, and Request Assistance notifications to all subscribers.

Verified and Unverified alerts appear 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. Similarly, Request Assistance can be viewed and interacted with in the Titan HST, including time, location, and message entered on the tablet by the operator.

Like other alert objects in Titan HST, the system can enable chat related to the alert for security officers with access to the system and communicate data to existing VMS and SOC platforms in which Titan HST in integrated. Additional actions can be triggered based on the systems rule's engine including automatic notifications, backup response protocols, door locking, and other actions defined by the security professionals. Past alerts can be recalled for forensic analysis in the system.

Alert triggers copy the MSI CWD terminology for Threat tags to terminology in Titan HST. Some examples of terminology include: Request Assistance, gun, gun-law enforcement, other threat.

The Titan System needs to supply the required Titan Trigger IDs and API keys.

Adding a Titan HST Mass Notification Integration

1. Under the Integrations tab, navigate to the Titan tab.
2. Click **Add integration.**
3. Under Integration Settings, toggle Enable Images. By enabling images, you give consent to MSI to store the images according to the 7-day retention policy.
4. If you would like to Enable Unverified Alerts, toggle Enable Unverified Alerts. By enabling the unverified alerts, you agree to operate the MSI CWD system in accordance with the design intent.
5. Click **Enable**.
6. Select the scanners to have alerts sent to the Titan system.
7. Click **Save**.
8. Enter the username and password provided by MSI to authenticate.

Open API Custom Integration

The MSI Open API Custom Integration provides a path to integrate CWD data with external security ecosystem systems to use CWD alerts and event data in other applications. The Custom Integration API allows a customer to subscribe and receive data for verified alerts, unverified alerts, system events, and request assistance messages. A customer may then integrate this data into their security ecosystem. The following outlines the process for configuring the MSI CWD Custom Integration API. This allows a connected system to receive alerts and events from the MSI CWD via AWS.

Use the Add Custom Integration feature to create credentials to authenticate and connect to the Open API. Admins create a Name for the integration and select an expiration date. Credentials are created automatically, and an Open API Key and passcode are displayed. These credentials are needed to make API calls. Each API Key is unique and only allows one user to query data at their request. These keys provide read only privileges in the Portal. After creating a key, the Customer Admin will copy the passcode and supply it to the person creating the custom API configuration.

Adding a Custom Integration

1. Under the Integrations tab, navigate to the Custom tab.
2. Click **Add integration.**
3. Enter a name for the integration.
4. Enter an expiry date for the integration. Does not expire if the default.
5. Click **Save**.
6. Under Integration Settings, toggle Enable Images. By enabling images, you give consent to MSI to store the images according to the 7-day retention policy.

7. If you would like to Enable Unverified Alerts, toggle Enable Unverified Alerts. By enabling the unverified alerts, you agree to operate the MSI CWD system in accordance with the design intent.
8. Click **Enable**.
9. Select the scanners to have alerts sent to the system.
10. Click **Save**.
11. Enter the username and password provided by MSI to authenticate.

Locations

The user can add multiple locations to an individual CWD.

NOTICE: The Locations feature is edited in the **Scanners** tab and managed in the**Locations** tab.

Adding Secondary Locations

1. Under Secondary locations, enter a Location name.
2. Click **Add New Location**. The new location will appear in the list.

Alert Tags

The Alert Tags feature allows the user to activate up to 9 Alerts Tags that are common to a particular venue. For example, tag a wheelchair in a hospital. Alert tagging is only available on CWD scanners running Host Version 4.0+. Scanners running previous software versions will still have alert staffing available with set tags.

A Test Alert Tag is included with to the Benign Tags option. This option can be one of the nine (9) alerts tags allowed. The Test Tag Alert can be employed when security teams want to test the Alerts System on the MSI CWD. This testing involves walking through the scanner with test piece or known threat object that will trigger an alert to ensure the system is working properly. The Test Alert Tag can only be configured on 5.0 scanners and above.

Configuring Alert Tags

1. Select scanners from the list.
2. Click **Next**.
3. Configure tags by dragging and dropping types of tags into either: Active Threat Tags or Active Benign Tags.
4. Click **Next**.
5. Review and click **Send Update**.
6. Configured Alert Tags will appear under Scanner Alert Tags. To view these tags, select the scanner from the list.

Notifications

If the user is subscribed to receive notifications, they will be notified of new notifications. The notification icon will have a red dot and the number of new notifications on it, as shown below.

1. Click on the **Notifications** icon to view the list of notifications.
2. Click on the notification to view additional details.
3. To remove the notification from the list, click **Mark Read**.
4. If the error is a critical system failure, click **Support** to contact support.

Support

Click on the **Help** icon to Contact Support and access Technical Guides.

Contact Support

Select **Contact Support** for access to MSI's corporate office and technical support contact information.

Technical Guides

Select Technical Guides for access to the Knowledge Base. Here the user can access helpful documentation: operator manuals, release notes, integration documents, demonstrations, and installation tips. The knowledge base is updated when new features and software releases become available.