# Aware Intel Hub

**COMPLETE USER GUIDE**

INTTERRA

1606 Headway Circle, STE 9644
Austin, Texas 78754
Intterra, LLC | www.Intterra.io

# Aware Intel Hub

Complete User Guide

## Table of Contents

# Platform Overview

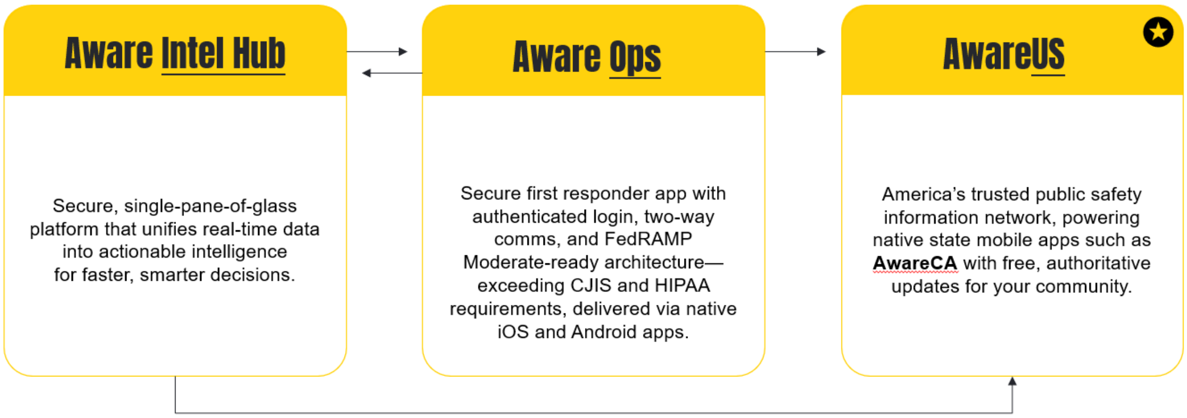
## Aware Intel Hub

Aware Intel Hub is Intterra’s data integration and intelligence platform that connects information from multiple systems into a single, unified environment. It aggregates data from sources such as CAD, RMS, AVL, cameras, sensors, and other operational systems, allowing agencies to analyze information, identify patterns, and generate actionable insights.

Intel Hub serves as the data and intelligence foundation of the Aware ecosystem. Information processed through Intel Hub powers the Aware community-facing platform, ensuring that information shared with the public originates from a centralized, authoritative, and verified source.

Data flows from agency systems into the Aware Intel Hub, where it is integrated, processed, and organized for use across the platform. Agencies maintain full control over how their data is managed and what information is made available externally. The platform is designed for CJIS, HIPAA, and FedRAMP Moderate compliance.

The diagram below illustrates how the Aware ecosystem connects internal systems, operational personnel, and public-facing information.




## Aware Ops (Operational Mobile Platform – In Development)

Aware Ops is a secure mobile platform currently in development that is designed to extend the capabilities of the Aware Intel Hub to personnel in the field. It will provide responders with access to integrated data, incident details, and operational context in a mobile-friendly environment, supporting real-time awareness and decision-making during active incidents.

## Aware Community-Facing App

Aware is the public-facing community awareness platform that enables public safety agencies to share timely, accurate, and authoritative information directly with residents, visitors, and stakeholders. The platform provides a map-based view of incidents, alerts, evacuations, closures, and other public safety activity, helping communities understand what is happening around them and what actions they may need to take.

For statewide deployments, each state receives its own branded Aware application using the format **Aware + state abbreviation** — for example, **AwareCA** for California. Each state-branded application is available through the Apple App Store and Google Play Store and is designed to support the specific agencies, governance model, and public safety needs of that state.

While each state has its own branded application, the Aware platform is built on a common national architecture. This means that data published by participating agencies can roll up into a single national Aware platform, including **AwareUS**. Regardless of which state application a community member downloads, the underlying platform allows approved public-facing information to be accessible across jurisdictions and geographies.

A core principle of Aware is that **each agency owns and controls its own data**. Agencies determine what information is published, when it is shared, when it is updated, and when it is removed. Aware does not take ownership of agency data or make publishing decisions on behalf of agencies. Instead, it provides a secure and governed pathway for agencies to share approved public-facing information with the communities they serve.

Aware receives approved incidents and activity data from the **Aware Intel Hub**. Data flows from the Intel Hub to the public-facing Aware application, ensuring that only appropriate information is released publicly, while sensitive operational details remain protected within the internal system.

By combining agency-controlled publishing, state-branded applications, and a unified national platform, Aware delivers verified information directly from authoritative sources while giving agencies full control over their participation, data, and public communication strategy. This improves transparency, strengthens situational awareness, and creates a trusted national awareness layer for all-hazards public safety information.

**Summary**

While each platform serves a unique purpose, they work together as a connected ecosystem.

Intel Hub is the data foundation that integrates and processes agency data.
Aware Ops extends that data into the field, providing operational personnel with mobile access to real-time information.

Aware is the public information platform that allows agencies to share selected information with their communities.

Together, these platforms allow agencies to manage operational data internally, support personnel in the field, and provide clear and trusted information to the public.

# Aware Intel Hub Overview

## How to Log In

The following URL will take you to the log in screen for the Aware Intel Hub: intelhub.intterra.io

When a system administrator creates your account, you will receive an email containing a link to access your account. This link will allow you to confirm your account and create a password. Follow the prompts in the email or on the login screen to complete the sign-in process.

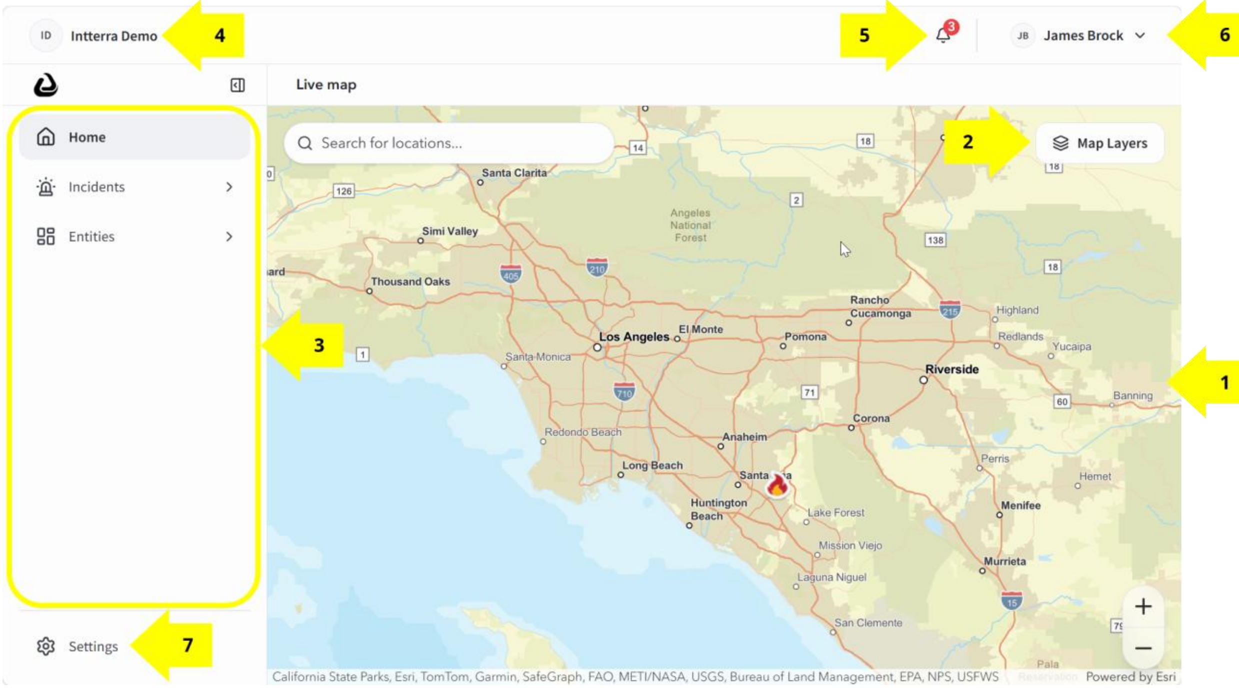
Enter your email address on the login screen and follow the prompts to continue signing in. If you experience any login issues, contact your system administrator.

## The Home Screen

Most users will spend the majority of their time on the home screen, also labeled **Live map**, monitoring activity and accessing incidents.

The Aware Intel Hub home screen serves as the central workspace for accessing real-time information, monitoring activity, and navigating the platform. The layout is designed to provide immediate situational awareness, while allowing users to quickly access key tools and data.

The system is fully responsive and optimized for desktop, tablet, and mobile devices, ensuring consistent functionality across all platforms.




1. **Map (Central View)**

   The map is the primary visual component of the home screen and provides a real-time view of operational activity.

   Users can view incidents, calls for service, cameras, weather data, and other available layers directly on the map. Available layers may also include community resources, notices or warnings, reference data, response assets, and other configured operational data. Map icons are interactive and can be selected to view additional details.

   The map also allows users to:

   - Show or hide data layers
   - Search for specific locations
     - The search bar can be used to search for a location and reposition the map.
   - Zoom in and out to adjust the level of detail
   - Open or close the Map Layers panel

2. **Map Layers Button**

   The Map Layers button opens the Map Layers panel on the right side of the map. This panel allows users to control which map layers are visible and review the map legend. The panel includes two tabs: Layer and Legend.

   The Layer tab includes a search field for locating specific layers. Layers are organized into categories such as All Hazards / Incidents, Cameras, Community Resources, Notices / Warnings, Reference Data, Response Assets, and Weather. Each category shows how many layers are currently selected out of the total available layers. Users can expand a category to view the individual layers within it and turn layers on or off as needed.

   The Legend tab displays the map legend and shows what the different map icons and symbols represent. Users can search the legend or filter legend items by All, Visible, or Hidden to control which items are displayed.

3. **Sidebar (Left Panel)**

   The sidebar provides quick access to the main areas of the platform. The content of the sidebar may vary depending on user role, permissions, and agency configuration.

   The primary sidebar options include Home, Incidents, Entities, and Settings.

   The sidebar is designed to give users fast access to relevant information and administrative tools without needing to search the map.

4. **Agency Identifier (Top Left)**

   The agency identifier appears in the top-left area of the interface and displays the active agency or tenant context. This helps users confirm which agency environment they are currently viewing.

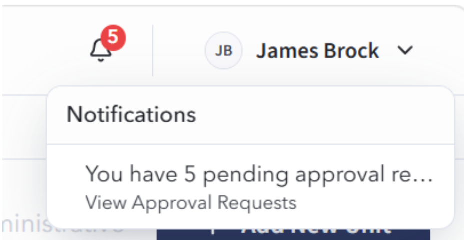
5. **Notifications**

The notification bell is located in the top-right area of the screen. A badge may appear on the bell when unread notifications are available.

Users may receive notifications for:

- Incident updates
- Approval requests
- Other system-generated events

Selecting the notification bell displays a notification pop-up with additional notification information.




Depending on the notification type, users may be able to open the related record or review additional details.

Selecting **View Approval Requests** from the notification pop-up opens the **Approval Requests** screen, which is covered later in this guide.

6. **User Menu (Top Right)**
   The User Menu is located in the top right corner of the home screen and is identified by the display of the logged-in user's name.

   Selecting the User Menu provides quick access to personal settings and system options.

   A more detailed overview of the User Menu and its available features is provided later in this guide.

7. **Settings**
   The **Settings** option appears in the lower-left area of the sidebar for users

with appropriate permissions. It provides access to administrative tools used to manage access, organization information, and system configuration.

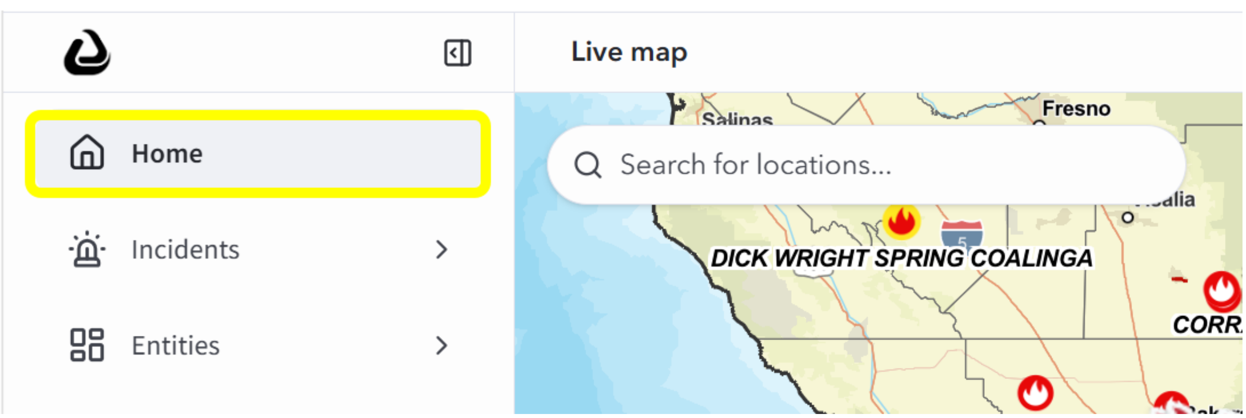
Administrative settings are covered later in this guide.

## The Sidebar

The **sidebar** provides the main navigation for the Intel Hub. It gives users quick access to key areas of the application, including the Home/map screen, incidents, entities, notifications, user and organization information, and other available tools based on their permissions.

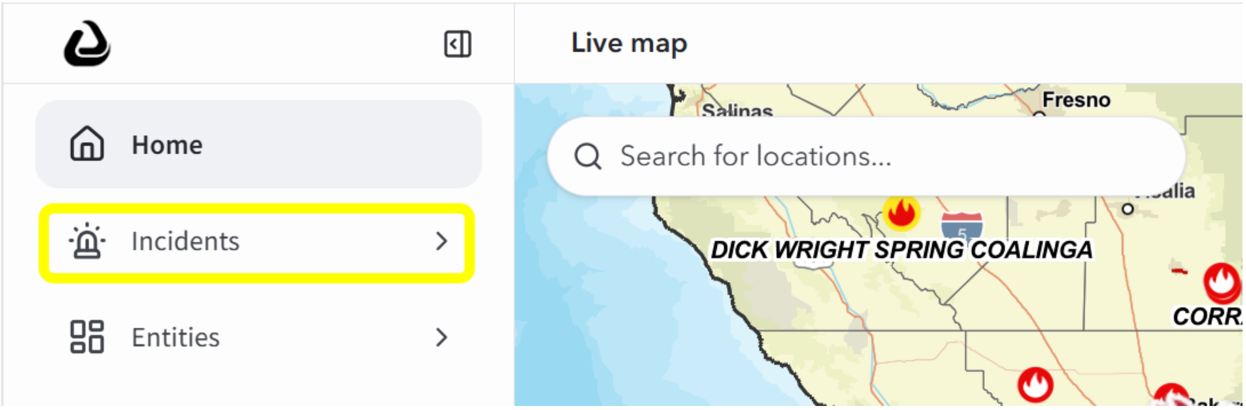
Users can **expand or collapse the sidebar** by selecting the **sidebar toggle button** located just above the sidebar. When expanded, the sidebar displays the full navigation labels, making it easier to identify each section. When collapsed, the sidebar reduces to a compact icon-only view, giving users more screen space while still allowing quick navigation.

### Home (Sidebar Button)




The Home button returns you to the main Intel Hub map screen from anywhere in the application. Use this option when you need to leave the current page, tool, or workflow and return to the primary map view.

## Incidents (Sidebar)

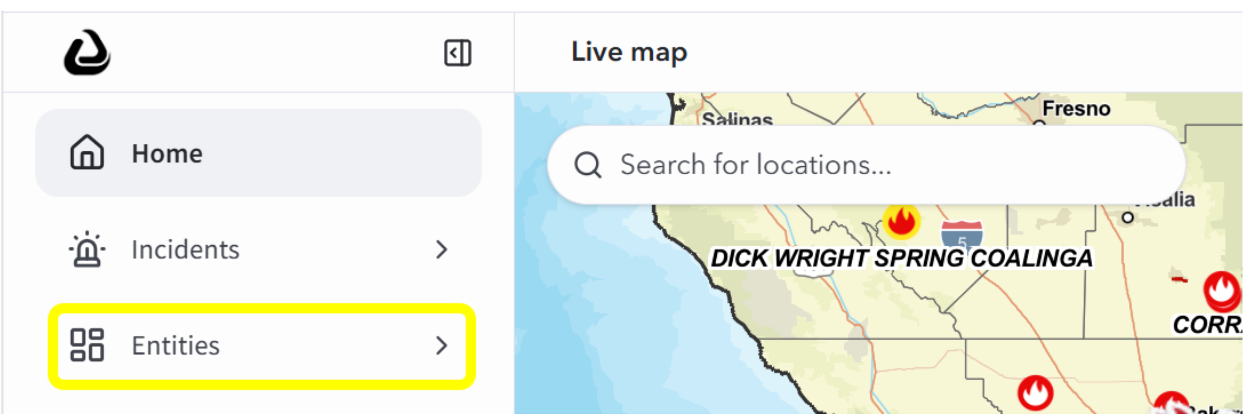



The **Incidents** section of the sidebar provides quick access to incidents within the system.

Selecting **Incidents** opens the main Incidents screen, where users can view, filter, open, create, and manage incidents.

The dropdown arrow next to **Incidents** can be used to expand or collapse the list of active incidents. When expanded, active incidents appear beneath the Incidents heading. Selecting an incident from this list opens the Incident Details screen for that specific incident.

## Entities (Sidebar)




The **Entities** section provides access to additional records and data areas within the platform.

Selecting **Entities** opens the full Entities area, where users can access the entity types available to them based on role, permissions, and agency configuration.

The dropdown arrow next to **Entities** can be used to expand or collapse the configured shortcut list. When expanded, only the entity shortcuts selected for the sidebar appear beneath the Entities heading. This list does not necessarily include every available entity type.

Each agency may configure which shortcuts appear under Entities based on operational needs. As a result, the sidebar may look different between users or agencies.

Selecting a shortcut under Entities takes the user directly to that specific section. Because the shortcut list is configurable and may vary by agency, users should select **Entities** itself to access the full list of entity types available to them.

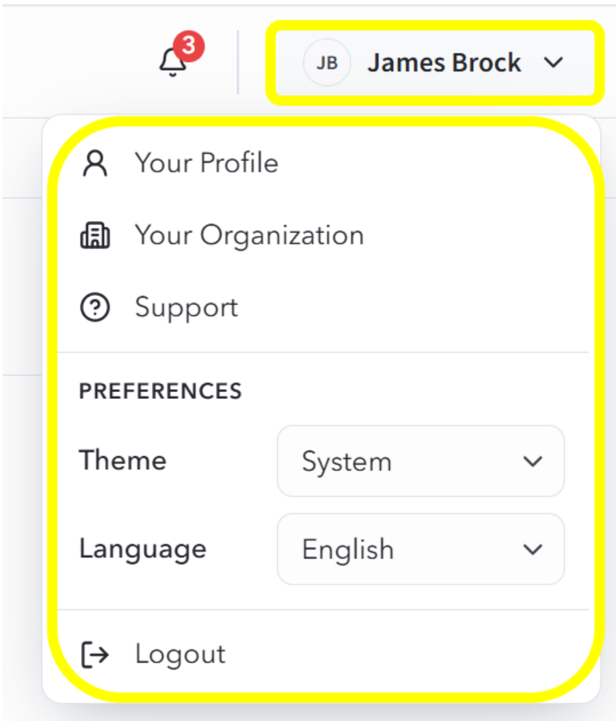
Depending on system configuration, permissions, and agency setup, the Entities module may include:

- Agencies
- Approval Requests
- Lookup Tables
- Personnel
- Stations
- Units
- Users
- Layer Configurations
- Layer Groups
- GIS Credentials
- Incidents
- Calls for Service

Items listed in the full Entities area may not all appear as sidebar shortcuts. The sidebar only displays the shortcuts configured for that agency or user role.

Some items available through Entities may also be available through **Settings**. When an item is primarily administrative, this guide introduces it briefly in the Entities section and covers the full workflow in the Settings section.

## User Menu (Detailed Overview)




The User Menu is located in the top-right corner of the home screen and is identified by the logged-in user's initials, name, and dropdown arrow.

Selecting the User Menu opens a dropdown with access to user and preference options, including:

- Your Profile: View user profile information
- Your Organization: View organization information
- Support: Access support resources
- Theme: Select the preferred display theme (System, Light, Dark)

- Language: Select the display language
- Logout: Sign out of the system

## Your Profile

Selecting **Your Profile** from the User Menu opens the **Profile** page.

The Profile page displays information associated with the logged-in user's account. This section may be used by the user to review their own account information. Some management options may only be available to users with the appropriate permissions.

The Profile page displays information associated with the logged-in user's account. This section can be used to review account details, assigned roles, assigned groups, multi-factor information, and account-related events.

### User Details

The **User Details** area displays basic account information for the user. This may include the user's name, email address, primary phone number, account status, agency, member since date, and last login date.

Depending on permissions, a **Manage** option may be available on the Profile page at the top right. Available management actions include **Edit User** and **Change Password**.

### Roles Tab

The **Roles** tab displays roles associated with the user account.

Roles help define what the user can access or perform within the platform. Users may be able to review role names and descriptions from this tab.

To review assigned roles:

1. Open **Your Profile**.

2. Select the **Roles** tab.
3. Review the roles listed in the table.

The Roles table may include:

- Role name
- Description

Users can search the list, show or hide columns, or export the table depending on available options.

### Groups Tab

The **Groups** tab displays groups associated with the user account.

Groups may be used to organize users and assign permissions or access levels.

To review assigned groups:

1. Open **Your Profile**.
2. Select the **Groups** tab.
3. Review the groups listed in the table.

The Groups table may include:

- Group name
- Description

Users may also be able to search the list, show or hide columns, or export the table depending on available options.

### Multi-Factor Tab

The **Multi-Factor** tab provides information related to multi-factor authentication for the user account.

Available information and actions may vary depending on system configuration and user permissions.

To review multi-factor information:

1. Open **Your Profile**.
2. Select the **Multi-Factor** tab.
3. Review the available multi-factor information or options.

### Events Tab

The **Events** tab displays account-related system events associated with the user profile. This may include activity related to the user account, depending on system configuration and permissions.

### Table Tools

Several areas of the Profile page may include table tools. Depending on the tab and available permissions, users may be able to:

- Search within the table
- Show or hide columns
- Export table data
- Review listed records

If an option is not visible, the user may not have permission to access that function, or the function may not be enabled for that account.

## Your Organization

Selecting **Your Organization** from the User Menu opens the organization information associated with the user's current agency or tenant.

This area allows users with the appropriate permissions to review organization-level information, such as organization details, configuration information, and related administrative settings.

Access to organization information and available management actions may vary depending on user role, permissions, and agency configuration.

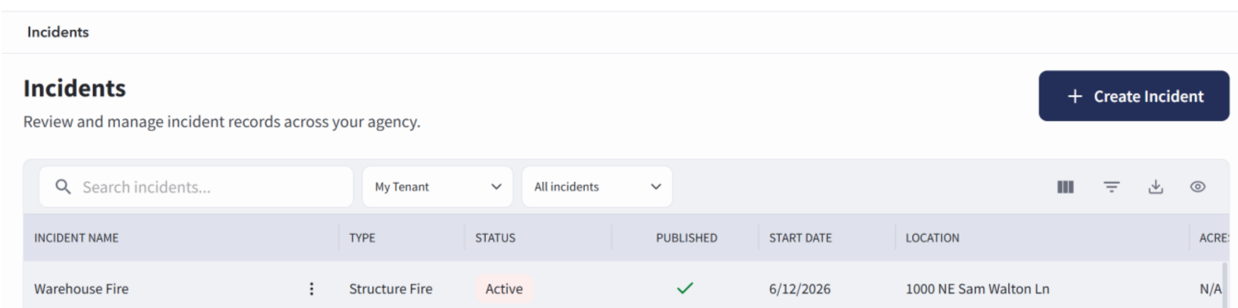
Organization management is covered in greater detail in the **Settings** section of this guide.

# Incidents

Incidents are user-created events within the system that are used to manage and communicate significant activity. Incidents can be created manually or from an existing Call for Service when information needs to be tracked, managed, reviewed, or shared beyond the original dispatch activity.

Incidents can represent a wide range of situations, including road closures, planned events, weather impacts, structure fires, wildfires, or major critical incidents. They serve as the primary method for managing incident information and controlling what information is submitted for approval and shared publicly.

## Incidents Screen




The **Incidents** screen can be accessed by selecting **Incidents** from the sidebar. It can also be accessed by selecting **Entities**, then choosing **Incidents**.

Upon opening, users are presented with a list of **Active Incidents** by default. This list can be filtered to display:

- Active Incidents

- Scheduled Incidents
- Closed Incidents
- All Incidents

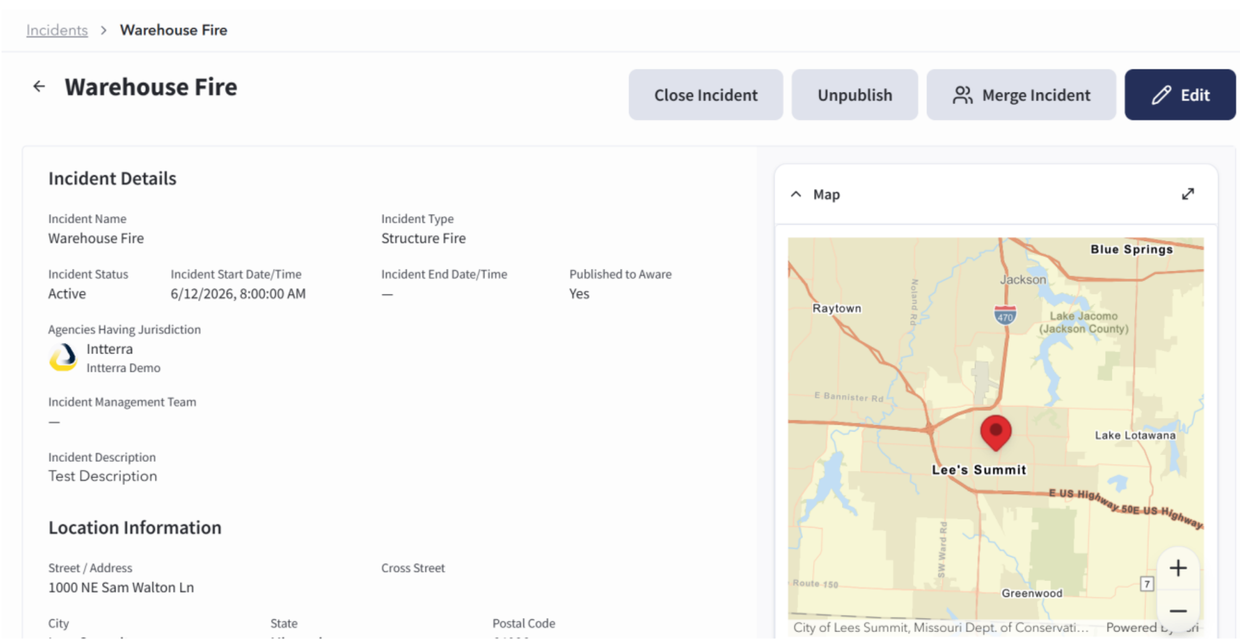
The displayed list will update based on the selected filter.

The Incidents screen displays incident records in a table. Users can search incidents using the search bar and filter the list using the available tenant and incident status filters, such as **My Tenant** and **All incidents**. Additional table controls allow users to adjust visible columns, apply filters, export data, and change the table view. A **Waiting for approval** filter is also available from the table view controls.

Selecting an incident name will open the detailed view for that specific incident.

Users can create a new incident manually by selecting **+ Create Incident** in the top-right corner of the Incidents screen.

## Incident Details Screen




The **Incident Details** screen is accessed by selecting an individual incident from the Incidents screen.

The Incident Details screen displays information associated with the selected incident, including incident name, incident type, incident status, incident start date/time, incident end date/time, published status, agencies having jurisdiction, cooperating agencies, incident management team, incident description, and location information.

The screen also includes a map showing the incident location, an Attachments section, a View Links section, and additional incident-specific sections such as wildfire information or status updates when applicable.

The action buttons available at the top of the Incident Details screen depend on incident status, publication status, approval status, and user permissions.

The screen also includes operational and situational information, such as:

- Status updates related to the incident
- A map displaying the incident location and any associated geospatial layers

The Incident Details screen displays whether the incident has been published to Aware. If the incident has not been published, this value displays as **Not Published**. When approval is pending, a **Pending Approval** status appears near the published status.

## Creating a New Incident (Public Facing)

To create an incident, users must have specific permissions within the system. If you do not have access to create incidents, contact your system administrator.

There are two ways to create a new incident within the system:

- **Create a new incident manually** – Start a new incident from a blank slate by entering all relevant details.
- **Create an incident from an existing Call for Service (CFS)** – Convert an existing Call for Service into a fully managed incident, carrying over available information from the map into the incident record.

**Option 1: Create a New Incident Manually**

1. Select **Incidents** from the sidebar.
2. Select **+ Create Incident** in the top-right corner.
3. Complete the required incident fields. Required fields are marked with an asterisk (*).
4. Add location information, links in the View Links section, and additional incident details as needed. Attachments can be added after the incident has been saved.
5. Select **Save** at the bottom of the screen to create the incident.
6. After the incident is saved, the incident details screen remains open. At the top-right corner, the incident status displays as **Not Published** in the **Status** dropdown. The **Merge Incident** and **Edit** buttons are also available from this screen.
7. Select the **Status** dropdown next to **Not Published**, then select **Submit for Approval**.
8. The **Review** pane opens. Review all incident content carefully.
9. When the incident is ready to be reviewed for publishing, select **Submit for Approval** at the bottom-right corner of the **Review** pane.
10. After the incident has been submitted, the **Status** dropdown at the top-right corner of the incident details screen updates to **Pending Approval**.

**Option 2: Create an Incident from a Call for Service**

1. From the home screen, select **Entities**, then choose **Calls for Service**. If available, **Calls for Service** may also be accessed directly from the sidebar.
2. Click on CFS ID for the desired Call for Service
3. Click **+ Create Incident** (top right)
4. Complete or update the desired incident details (see below)
5. Select **Save** at the bottom of the screen to create the incident.

6. After the incident is saved, the incident details screen remains open. At the top-right corner, the incident status displays as **Not Published** in the **Status** dropdown. The **Merge Incident** and **Edit** buttons are also available from this screen.
7. Select the **Status** dropdown next to **Not Published**, then select **Submit for Approval**.
8. The **Review** pane opens. Review all incident content carefully.
9. When the incident is ready to be reviewed for publishing, select **Submit for Approval** at the bottom-right corner of the **Review** pane.
10. After the incident has been submitted, the **Status** dropdown at the top-right corner of the incident details screen updates to **Pending Approval**.

### Incident Details

When creating an incident, complete the following fields as applicable:

- **Incident Name**
  Enter the incident name as designated by the incident commander or dispatch center
- **Incident Type**
  Select the appropriate type for the incident. Selecting "Wildfire" as the incident type will display an additional "Wildfire Details" section later in the Incident Details screen.
- **Incident Status**
  Indicates the current state of the incident:
    - **Planned** - The incident has been identified or scheduled but is not yet active.
    - **Active** – The incident is ongoing and requires response or coordination.
    - **Monitoring** – The incident is being watched for changes, but no active response actions are currently required.

- **Resolved** - The incident has been addressed, and no further response action is expected.
- **Closed** – Incident response has concluded, and the incident record is finalized.
- **Merged** - The incident has been merged with another related incident record.

- **Incident Start Date/Time**
  Enter the date and time the incident began. Users can select the date and time manually, or select **Now** to automatically enter the current date and time.
- **Incident End Date/Time**
  Enter the date and time the incident concluded, if applicable. Users can select the date and time manually, or select **Now** to automatically enter the current date and time.
- **Agencies Having Jurisdiction**
  Select the agency or agencies responsible for the incident. Multiple agencies can be selected. Selecting more than one agency will change the incident from a single-agency event to a Unified Command event, allowing all participating agencies to access, edit, and provide status updates to the incident. Incidents not initially created under Unified Command can be updated at any time to add additional agencies and transition to a Unified Command event.
- **Cooperating Agencies**
  Select one or more agencies that are assisting with the incident but do not have jurisdiction over it. Multiple cooperating agencies can be selected. This field helps distinguish agencies responsible for the incident from other agencies providing assistance or support. Cooperating agencies can be added or updated at any time by editing the incident.
- **Incident Management Team**
  Select the appropriate management team from the dropdown

- **Incident Description**
  Enter a summary of the incident based on currently available information (This can be updated as new information becomes available).

  **Note:** Information entered in the Incident Description field will be included in the public-facing incident information once the incident is approved and published. Users should review this content carefully before submitting the incident for approval.

- **Incident Location**
  Select **Address** or **Coordinates** for the incident location. When Address is selected, users can search for the address and complete the available address fields. When Coordinates is selected, users can enter latitude and longitude values.

- **Location – Description**
  Enter additional details to help describe the location (e.g., landmarks, directions, or specific areas)

- **Counties**
  Select one or more counties associated with the incident

- **Damage Assessment**
  The Damage Assessment section allows users to enter numerical information about the impacts of the incident. Complete the available fields as applicable:

  - **Structures**
    - Structures Destroyed
    - Structures Damaged
    - Structures Evacuated
    - Structures Threatened
  - **Population**
    - Impacted Population
  - **Civilians**

        - Civilian Fatalities
        - Civilian Injuries
    - **Firefighters**
        - Firefighter Fatalities
        - Firefighter Injuries

  All Damage Assessment fields are numerical fields and can be updated as additional information becomes available.

  **Note:** For incidents associated with an IRWIN ID, supported casualty and structure damage information may be automatically updated from IRWIN.

- **Wildfire Details**
  If "Wildfire" is selected as the Incident Type, an additional "Wildfire Details" section will appear below the Incident Location section within the Incident Details screen.

  This section provides the following additional fields specific to wildfire incidents:

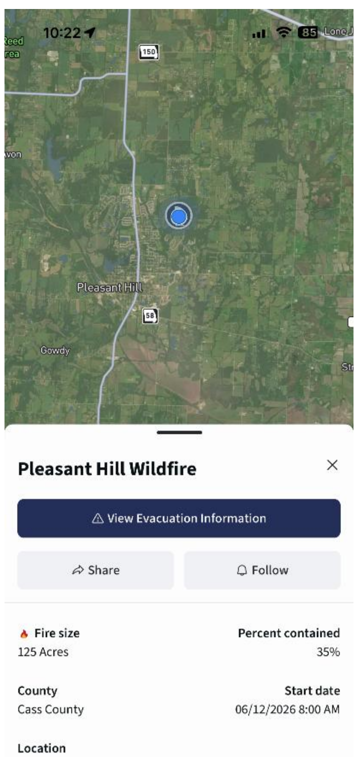
    - **Cause of Fire**
      Select the appropriate cause from the dropdown menu
    - **Acres Burned**
      Enter the number of acres burned (if known)
    - **Fuel Type**
      Select the appropriate fuel type from the dropdown menu
    - **Percent Containment**
      Enter the percentage of containment (if known)
    - **Containment Date/Time**
      Enter the date and time of wildfire containment (if applicable)
    - **Control Date/Time**
      Enter the date and time of wildfire control (if applicable)

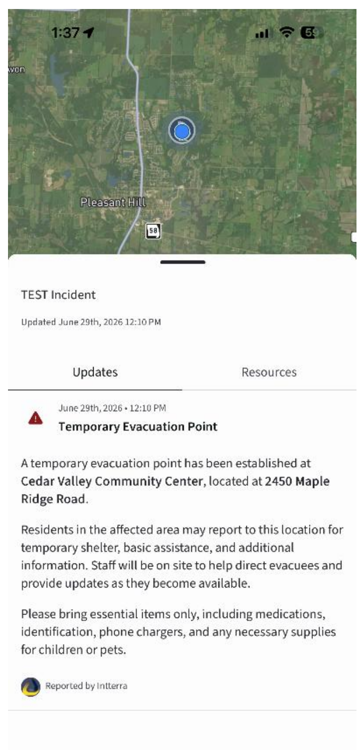
These fields can be updated as incident conditions change or additional information becomes available. Containment and control information may not be known when the incident is first created. When a valid IRWIN ID has been added to the incident as an External System Identifier, supported wildfire information, including acreage and percent containment, is automatically updated from IRWIN. Otherwise, users should update these fields throughout the lifecycle of the incident as needed.

- **Evacuation Information**

  The Evacuation Information section allows users to add public-facing evacuation information to an incident. Evacuation information can be added when creating a new incident or when editing an existing incident.

  Evacuation Information appears in the Aware public-facing app after the incident is published. When a user opens the incident containing evacuation information in the app, a **View Evacuation Information** button appears below the incident title. Selecting this button displays the evacuation type followed by the description entered for that alert.



**To add evacuation information:**

1. In the Evacuation Information section, select **Add Evacuation Information**.
2. Select an evacuation type, such as an evacuation order, evacuation warning, shelter in place, or another available alert type.
3. Enter a description for the selected evacuation type.
4. Continue completing or updating the incident.

   Once the incident is approved and published, the evacuation information is visible to the public through the Aware app.

   Evacuation information can be added to an incident at any time. To add evacuation information after an incident has already been created, open the incident, select **Edit**, add the evacuation information, save the incident, and submit it for approval again if approval is required.

   When editing an already published incident, notifications are only generated for evacuation information with evacuation types of **Evacuation Warning** or **Evacuation Order**.

- **Map**
  Displays the incident location based on the provided address or coordinates.
- **Perimeter**
  The Perimeter section allows users to add a GeoJSON perimeter file to the incident before the incident is saved. This can be used to include a geographic boundary or perimeter associated with the incident.

  To add a perimeter file, drag and drop a GeoJSON file into the upload box, or select the box to browse for the file. The upload box displays the message Drop a GeoJSON perimeter file or click to browse.

  Perimeter files must be in GeoJSON format and cannot exceed 5 MB.

- **Attachments**
  Attachments can be added to an incident after the incident has been saved. Attachments can be documents, images, or videos.

  **Important:** Attachments cannot be added during the initial incident creation process before the incident record has been saved. To add attachments, users must first create and save the incident, then edit the saved incident record.

  **To add attachments to an incident:**

  1. Create and save the incident.
  2. Open the saved incident.
  3. Select **Edit**.
  4. Locate the **Attachments** section.
  5. Click the **+** sign next to Attachments to open the **Add Attachments** window.
  6. In the **Add Attachments** window, browse for a file or drag and drop the file into the upload area.
  7. Review the selected file.
  8. Select **Add Files**.
  9. Save the incident changes.

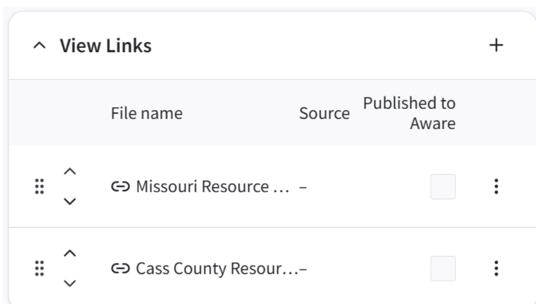
  If the incident has already been submitted for approval or published, adding attachments can trigger the approval process again. Users should review the incident carefully before submitting updated content for approval.

  **Note:** Incident attachments support common document, image, text/data, spreadsheet, compressed archive, and video formats. The default file size limit is 100 MB per attachment. This limit is configurable if a different maximum size is needed. For a full list of supported attachment file types, see **Appendix A: Supported Incident Attachment File Types**.

- **View Links**
  Add external links relevant to the incident. These can include community resources, trusted partner links, or other sources that provide additional context and information.

  Links can be added by selecting the **plus icon** in the View Links section. In the **Add Link** window, enter the **Link Name** and **Link URL**, then select **Save**.

  When more than one link has been added, the links can be reordered. To reorder links, drag a link using the **six-dot handle** on the left side of the row, or use the **up and down arrows** to move the link higher or lower in the list. This is helpful when more important links should appear at the top.




- **External System Identifiers**
  External system identifiers can be used to associate an incident with a matching record from another system. This section is optional and is not required to create or save an incident.

  Available systems include **IRWIN**, **CAL FIRE**, and agency-specific CAD or Call for Service systems. Depending on the agency, these systems may be identified using **CAD** or **CFS (Call for Service)** in the system name.

  When an incident is created from an existing Call for Service, the associated CAD or Call for Service identifier is automatically added to the incident. Users can also manually add an identifier by selecting the **+** sign next to **External System Identifiers**, selecting the appropriate agency/system from the **System** dropdown, entering the corresponding identifier in the **ID** field, and selecting **Save**.

  When a valid **IRWIN ID** is added, the incident is associated with the corresponding IRWIN record and supported incident information is automatically updated from IRWIN. This includes acreage, percent containment, casualty information, and structure damage information when available.

A **CAL FIRE** identifier can be added to associate the incident with the corresponding CAL FIRE incident. The CAL FIRE identifier provides the association only and does not enable any additional automated functionality or incident updates.

Once the identifier has been added, continue with saving or updating the incident.

## Saving and Submitting an Incident for Approval

After entering incident information, selecting **Save** at the bottom-right corner of the screen creates and saves the incident.

Selecting **Save** saves the incident record but does not submit the incident for approval and does not publish the incident to the Aware Portal.

To save an incident:

1. Complete the required incident fields.
2. Review the incident information.
3. Select **Save** at the bottom-right corner of the screen.

After the incident is saved, the Incident Details screen remains open. At the top-right corner of the screen, the status displays as **Not Published** in the **Status** dropdown. The **Merge Incident** and **Edit** buttons are also available from this screen.

To submit the incident for approval:

1. Select the **Status** dropdown next to **Not Published**.
2. Select **Submit for Approval**.
3. Review the incident information in the **Review** pane.

4. When the incident is ready to be reviewed for publishing, select **Submit for Approval** at the bottom-right corner of the **Review** pane.

After the incident has been submitted, the **Status** dropdown at the top-right corner of the Incident Details screen updates to **Pending Approval**.

The incident will not be published to the Aware Portal until the approval request is approved.

### Cancel an Approval Request

If an incident has been submitted for approval but needs to be changed before approval is completed, users can cancel the pending approval request when the option is available.

To cancel an approval request from the Incident Details screen:

1. Open the incident with the pending approval request.
2. Select the **Pending Approval** dropdown at the top-right corner of the screen.
3. Select **Cancel Approval Request**.
4. Confirm the cancellation if prompted.

After the request is canceled, the incident can be updated and resubmitted for approval when ready.

## Open an Existing Incident

You can open an existing incident using any of the following methods:

- **From the sidebar:** Expand **Incidents** and select an active incident from the list.
- **From the Incidents screen:** Select Incidents from the sidebar, then select the incident name from the table.
- **From the map:**
  Click on the specific incident icon on the map, then select **View More**

**Information** from the pop-up.

## Edit an Incident

If incident information needs to be corrected or updated, the incident record can be edited directly.

For ongoing updates or new information, users should use **Status Updates** rather than repeatedly modifying the original incident description.

To edit an incident:

1. Open the desired incident.
2. Select **Edit** in the top-right corner.
3. Update the necessary fields.
4. Select **Save** at the bottom-right corner of the screen.

If the incident has not been published, the edits are saved to the incident record.

If the incident has already been published, saving changes updates the incident status to **Published with Edits**. The published version remains visible on the Aware Portal until the pending edits are submitted, approved, and published.

When an incident displays **Published with Edits**, the dropdown provides the following options:

- **View Pending Changes**
- **Submit for Approval**
- **Revert to Last Published**

### View Pending Changes

To review pending edits before submitting them for approval:

1. Open the incident.

2. Select the **Published with Edits** dropdown at the top-right corner of the screen.
3. Select **View Pending Changes**.

The **Pending Changes** pane appears and displays the unpublished changes that have been made to the incident.

### Submit Edited Content for Approval

To submit edited incident content for approval:

1. Open the incident.
2. Select the **Published with Edits** dropdown at the top-right corner of the screen.
3. Select **Submit for Approval**.
4. Review the updated incident content in the **Review** pane.
5. Select **Submit for Approval** at the bottom-right corner of the **Review** pane.

After the edits are submitted, the incident moves into the approval process. The updated content will not be published to the Aware Portal until it is approved.

Approvers can review the edited content from the **Approval Requests** screen or from the related Incident Details screen. When reviewing edited content, the approval request displays the published version alongside the pending edited version. Removed or changed content from the published version is shown with strikethrough formatting, while the updated content appears in the pending version. This allows the approver to quickly review what changed before approving or denying the edited content.

### Revert to Last Published

To discard unpublished edits and return the incident to the last published version:

1. Open the incident.

2. Select the **Published with Edits** dropdown at the top-right corner of the screen.
3. Select **Revert to Last Published**.
4. Review the confirmation message.
5. Select **Revert Changes** to discard the unpublished changes.

After the changes are reverted, the incident record is restored to the last published version.

## Content Approval

Depending on agency configuration, incidents, status updates, edits, publishing actions, unpublishing actions, and closing actions can require approval before they are published or finalized.

Saving an incident does not trigger the approval process. After an incident is saved, users can submit the incident for approval from the **Status** dropdown on the Incident Details screen.

When an incident is submitted for approval, approvers are notified through the notification bell within the Aware Intel Hub.

Approvers can review approval requests from either the **Approval Requests** screen or from the related Incident Details screen.

### Reviewing an Approval Request from the Notification Bell

To review an approval request from the notification bell:

1. Select the **notification bell** at the top of the screen.
2. Select **View Approval Requests**.
3. On the **Approval Requests** screen, locate the pending approval request.
4. Select the approval request to open the request details.
5. Review the incident content carefully.

6. Select **Approve and Publish** to approve the request and publish the incident to the Aware Portal.

If the request should not be approved, select **Deny**.

When **Deny** is selected, the **Reject Request** window appears. Enter the reason for rejecting the request, then submit the rejection. The rejection reason is used to communicate why the request was not approved so the content can be corrected and resubmitted if needed.

### Reviewing an Approval Request from the Incident Details Screen

Approval requests can also be reviewed directly from the related Incident Details screen.

To review an approval request from the Incident Details screen:

1. Open the incident with the pending approval request.
2. Select the **Pending Approval** dropdown at the top-right corner of the screen.
3. Select **Review Publish Request**.
4. The approval request opens for review.
5. Review the incident content carefully.
6. Select **Approve and Publish** to approve the request and publish the incident to the Aware Portal.

If the request should not be approved, select **Deny**.

When **Deny** is selected, the **Reject Request** window appears. Enter the reason for rejecting the request, then submit the rejection.

When **Approve and Publish** is selected, a confirmation message appears asking the user to confirm that the content should be approved and published to the Aware Portal. If a user is approving content they submitted themselves, an additional confirmation checkbox appears requiring the user to confirm that they have received the appropriate approval from the appropriate authority to publish the change to Aware. The checkbox must be selected before the user can complete the approval and publishing action. Select **Approve and Publish** to complete the approval and publish the incident.

After the incident is approved and published, the Incident Details screen displays **Published** at the top-right corner of the screen, along with the **Merge Incident** and **Edit** buttons.

## Unpublishing an Incident

Published incidents can be unpublished when they need to be removed from the Aware Portal.

To unpublish an incident:

1. Open the published incident.
2. Select **Published** at the top-right corner of the Incident Details screen.
3. In the confirmation window, select **Unpublish**.

The confirmation window explains that the incident will be removed from the Aware Portal and can be republished at any time. Select **Cancel** if the incident should remain published.

Selecting **Unpublish** submits the unpublish request for approval. The approver is notified through the notification bell within the Aware Intel Hub.

While the unpublish request is pending, the Incident Details screen displays **Pending Approval** at the top-right corner of the screen.

To review an unpublish request:

1. Open the approval request from the notification bell, Approval Requests screen, or related Incident Details screen.
2. Review the request.
3. Select **Approve Unpublish** to approve the request and remove the incident from the Aware Portal.

If the incident should remain published, select **Reject Unpublish**. When rejecting the request, enter the reason for rejection.

After the unpublish request is approved, the incident is removed from the Aware Portal.

Depending on agency configuration, incidents, status updates, edits, publishing actions, and closing actions can require approval before they are published or finalized.

Saving an incident does not trigger the approval process. After an incident is saved, users can select **Submit for Approval** from the Incident Details screen. A review pane appears on the right side of the screen. After reviewing the content, selecting **Submit for Approval** at the bottom of the review pane begins the approval process.

Users with approval permissions can review approval requests from the **Approval Requests** section or from the related incident when available.

Approval actions depend on the request type. For a publishing request, approvers can approve and publish the request or deny it. For an incident closing request, approvers can select **Reject Close** or **Approve Close**.

## Incident Status Updates

Incident Status Updates are used to communicate new or evolving information related to an incident after it has been created. Status updates provide a chronological record of changes, progress, and key developments.

Rather than modifying the original incident description for each new development, users should add status updates to keep incident information organized and easier to follow.

Status updates can be used for information such as:

- Changes in incident conditions
- Updated public instructions
- Progress updates

- Road closure changes
- Evacuation information
- Containment or control updates
- Other important incident developments

### Add a Status Update

To add a status update:

1. Open the desired incident.
2. Scroll down to the **Status Updates** section.
3. Select **+ New Status Update**.
4. In the **New Status Update** window, complete the update details:
5. **Category** - Select the appropriate update category.
6. **Pin to Top** - Toggle on to pin the update to the top of the list.
7. **Content** - Enter the update information.
8. **Attachments** - Add any relevant images or videos.
9. Select **Submit for Approval** at the bottom-right corner of the **New Status Update** window.

If an approval process is configured, the status update is submitted for approval and displays as **Pending Approval** in the **Status Updates** section of the Incident Details screen.

The status update will not be published to the Aware Portal until it is approved.

### Edit a Status Update

Users with appropriate permissions can edit status updates at any time.

To edit a status update:

1. Open the desired incident.
2. Scroll down to the **Status Updates** section.
3. Locate the update you wish to modify.
4. Select the pencil icon to edit.
5. Make the necessary changes.
6. Select **Save Changes**.

**Note:** Edits can trigger the approval process if approval is configured.

### Approving a Status Update

Depending on agency configuration, status updates may require approval before they are published to the portal.

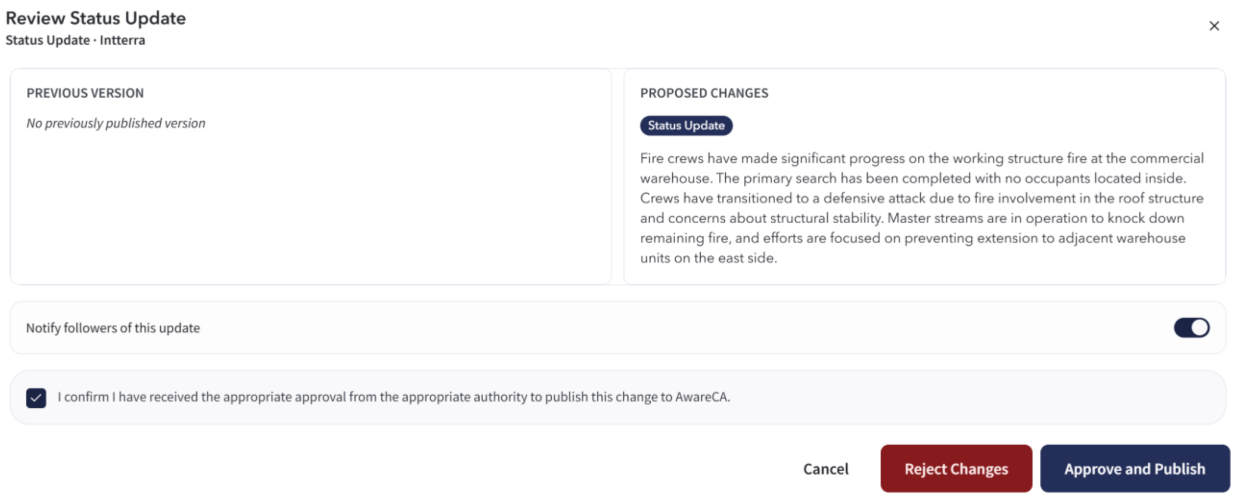
When a status update is submitted for approval, approvers are notified through the notification bell at the top of the screen. The pending status update also appears in the Status Updates section of the related Incident Details screen with a Pending Approval status and a Review button.

Approvers can review and act on the status update from the Approval Requests screen or directly from the associated Incident Details screen.

### Approving Your Own Status Update

If an approver is reviewing a status update that they submitted themselves, an additional confirmation checkbox appears in the Review Status Update window. The checkbox confirms that the approver has received the appropriate approval from the appropriate authority to publish the change to AwareCA.

The checkbox is not selected by default and must be selected manually before the status update can be approved and published. After selecting the confirmation checkbox, select Approve and Publish to complete the approval.




*The confirmation checkbox is shown selected above for reference. It is not selected by default and must be manually selected when approving your own status update.*

### Approving a Status Update from the Notification Bell or Approval Requests Screen

To approve a status update from the notification bell or Approval Requests screen:

1. Select the **notification bell** at the top of the screen.
2. Open the status update publish approval request from the notification list, or select **View Approval Requests** to open the Approval Requests screen.
3. Locate and open the status update approval request.
4. Review the status update content and related incident information.
5. Select **Approve and Publish** to approve and publish the status update.

If the status update should not be approved, select the deny or reject action. When rejecting the request, enter the reason for rejection. The user who submitted the status update can use the rejection reason to correct and resubmit the content if needed.

### Approving a Status Update from the Incident Details Screen

To approve a status update from the Incident Details screen:

1. Open the associated incident.
2. Scroll to the **Status Updates** section.
3. Locate the status update marked as **Pending Approval**.
4. Select **Review** for the pending status update.
5. Review the status update content in the **Review Status Update** window.
6. Select **Approve and Publish** to approve and publish the status update.

If the status update should not be approved, select **Reject Changes**. When rejecting the request, enter the reason for rejection.

Approvers should review the status update carefully before approving it because approved status updates become visible on the portal.

## Merging Incidents

Incidents can be merged when the current incident needs to be combined with an existing Unified Command incident.

The merge process uses **Merge and Join**, which closes and merges the current incident's data into an existing Unified Command incident.

To merge an incident:

1. Navigate to the Incident Details screen for the incident you want to merge.
2. Select **Merge Incident** in the top-right corner.
3. In the merge window, select **Merge and Join**.
4. Review the list of available incidents. Incidents are listed by distance, with the closest incidents shown first.
5. Select the incident you want to merge into.
6. Select **Continue**.
7. On the **Confirm Merge** screen, review the merge details.

8. Confirm that the correct incidents are being merged.
9. Select **Confirm Merge** to complete the merge.

If the merge should not be completed, select **Cancel** from the Confirm Merge screen.

After the merge is confirmed, the current incident is closed and merged into the selected incident. The selected incident remains active as the primary incident record.

Merging an incident does not require a separate approval process.

### Merged Incidents

When one or more incidents have been merged into another incident, the incident that remains active displays a **Merged Incidents** box in the lower-right area of the Incident Details screen.

The **Merged Incidents** box lists the incidents that have been merged into the current incident. Each merged incident appears as a link. Selecting a linked incident opens the Incident Details screen for that merged incident, even though the merged incident is closed.

The **Merged Incidents** box also includes an **Unmerge** button for each merged incident listed. This allows users to unmerge a specific incident from the current incident without unmerging all merged incidents.

### Unmerging an Incident

An incident can be unmerged from the incident it was previously merged into.

There are two ways to unmerge an incident:

- From the **Merged Incidents** box on the incident that remained active after the merge.
- From the Incident Details screen of the incident that was merged and closed.

### Unmerge from the Merged Incidents Box

To unmerge an incident from the incident that remained active:

1. Open the incident that contains the merged incident data.
2. Locate the **Merged Incidents** box in the lower-right area of the Incident Details screen.
3. Find the merged incident that should be separated.
4. Select **Unmerge** for that specific merged incident.
5. Confirm the unmerge action if prompted.

After the incident is unmerged, that specific incident is separated from the current incident.

### Unmerge from the Merged and Closed Incident

To unmerge from the Incident Details screen of the merged and closed incident:

1. Open the incident that was previously merged and closed.
2. Review the message at the top of the Incident Details screen. The message states that the incident has been merged and closed and that the data now lives in the incident it was merged with.
3. Use the **View [Incident Name]** button to open the incident that now contains the merged data, if needed.
4. Select **Unmerge this incident**.
5. When the confirmation message appears, select **Yes** to unmerge the incident.

If the incident should remain merged, select **Cancel** from the confirmation message.

After the incident is unmerged, the incident is separated from the incident it was previously merged into.

## Closing an Incident

Users with the appropriate permissions can request to close an incident from the **Incident Details** screen.

To close an incident:

1. Open the incident that needs to be closed.
2. Select **Edit** at the top of the **Incident Details** screen.
3. Change the status of the incident to **Closed**.
4. Select Submit for Closing at the top-right corner of the screen to submit the close request.

If the incident should not be submitted for closure, select **Cancel** from the confirmation window.

After the closing request is submitted, approvers are notified through the notification bell within the Aware Intel Hub.

While the close request is pending, the incident remains open. The pending close request can be canceled from the Incident Details screen by selecting **Cancel Request**.

### Canceling a Close Request

To cancel a pending close request:

1. Open the incident with the pending close request.
2. Select **Cancel Request** on the **Incident Details** screen.
3. Confirm the cancellation if prompted.

After the request is canceled, the incident remains open and can be updated or resubmitted for closure when ready.

### Approving or Rejecting a Close Request

Users with approval permissions can approve or reject an incident close request from the approval request.

To approve or reject a close request:

1. Open the close request from the Approval Requests screen, notification bell, or related incident.
2. Review the close request and related incident information.
3. Select **Reject Close** or **Approve Close**.

If **Reject Close** is selected, a rejection reason must be entered. The user who submitted the close request will be notified of the rejection reason.

If **Approve Close** is selected, a confirmation message appears. Select **Approve Close** in the confirmation message to approve the request and close the incident.

After the close request is approved, the incident status updates to closed.

For incident closing requests, use **Reject Close** or **Approve Close** to complete the approval decision.

## Entities (Detailed Overview)

The **Entities** section serves as a centralized location for accessing available entity directories and records within the Aware Intel Hub. Entities may include operational records, system-generated data, configuration records, personnel-related records, and other data areas available to the user based on permissions and agency configuration.

Entities provide users with the ability to view, manage, and interact with different types of information, depending on their role, permissions, and agency configuration.

**Note:** Items displayed beneath Entities in the sidebar are configurable shortcuts. The shortcut list may vary by agency, user role, or system configuration and may not include every available entity type.

Not all entity types may be visible to all users, depending on permissions and system configuration.

The sections below introduce commonly available entity types. When an entity is primarily used for administration or configuration, this guide provides a brief overview here and covers the full workflow in the Settings section.

## Agencies

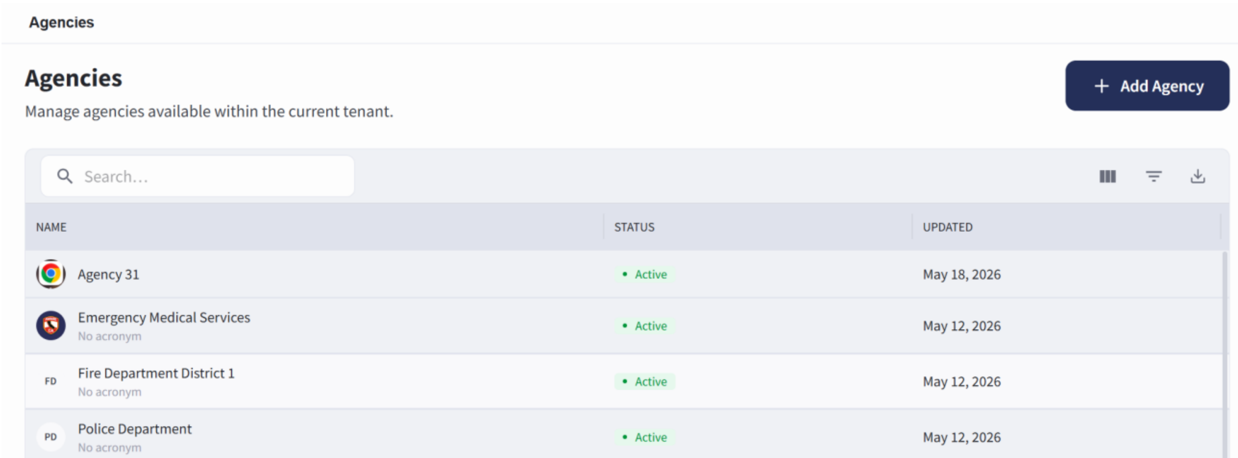
The **Agencies** section allows authorized users to view and manage agencies available within the platform.

This section is primarily intended for system administrators or users with agency management permissions. Access to this section and the available actions may vary depending on user role, permissions, and agency configuration.

Agencies represent organizations or departments that may be involved in incidents, response activity, configuration, or operational coordination. This may include agencies within a single jurisdiction, such as Police, Fire, and Public Works, as well as outside agencies that may participate in mutual aid or regional coordination.

Agency information can support incident association, jurisdictional awareness, and coordination across multiple organizations.

## Main Agencies Screen




The **Agencies** screen can be accessed by selecting **Entities**, then choosing **Agencies**.

The Agencies screen displays agencies available within the current agency environment in a list view. Each agency appears as a row in the table.

### Searching for an Agency

To search for an agency:

1. Open the **Agencies** screen.
2. Select the search bar near the top of the agency list.
3. Enter the agency name or other available search text.
4. Review the filtered results in the agency table.
5. Select an agency name to open the agency record.

### Adding an Agency

Users with the appropriate permissions may create a new agency from the Agencies screen.

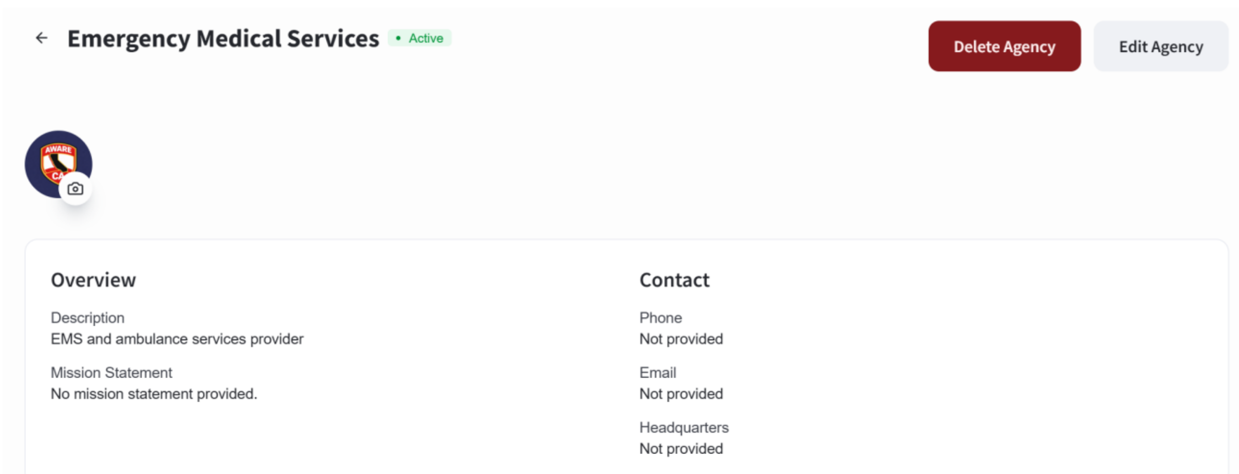
To add an agency:

1. Open the **Agencies** screen.
2. Select **+ Add Agency**.
3. Complete the required agency information.
4. Enter any additional agency details available on the form.
5. Select **Create Agency** when complete to add the agency.
6. Review the new agency record after it has been created.

**Note:** Toggling the “Make agency publicly visible to other tenants” will allow other customers to see and add that agency to mutual aid events when needed.

Agency records may include information such as agency name, acronym, status, contact information, location information, logo or branding details, website information, and other agency-specific details.

## Agency Information Screen




The **Agency Information screen** is accessed by selecting an already created agency from the **Agencies** screen.

The agency record displays information associated with the selected agency. Available details may include agency identity, status, contact information, location information, and other configured agency details. From this screen, users with the appropriate permissions can:

- Select **Edit** to update agency information
- Select **Delete** to delete the agency

## Approval Requests

The **Approval Requests** section provides a centralized location for reviewing and managing content that requires approval before being shared externally.

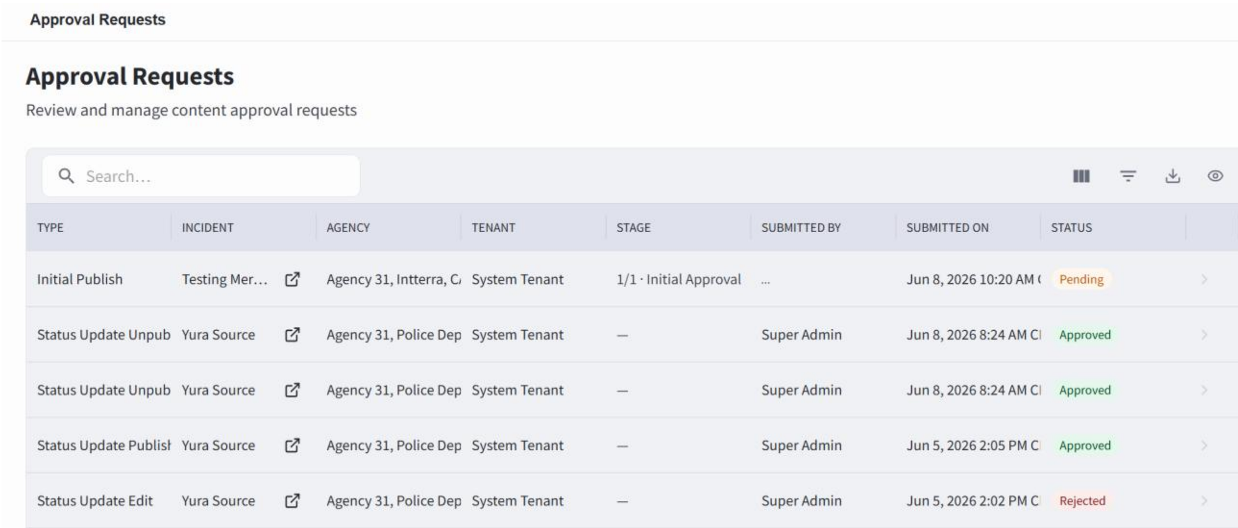
This section is primarily intended for users with approval permissions, such as supervisors, approvers, system administrators, or other authorized users. Users designated to approve Aware content must have the **Aware Approver** role assigned either directly or through a group. Access to this section and available approval actions may vary depending on user role, permissions, approval stage, and agency configuration.

Approval Requests help ensure that public-facing information is reviewed before it is published, updated, closed, or otherwise changed. This supports accountability, consistency, and appropriate release of information.

Within this section, authorized users may be able to:

- View approval requests
- Search for approval requests
- Filter or adjust the approval request table
- Review pending, approved, and rejected requests
- Open related incident records when available
- Review request status, stage, submitter, submitted date, and decision history
- Approve or reject requests

## Main Approval Requests Screen



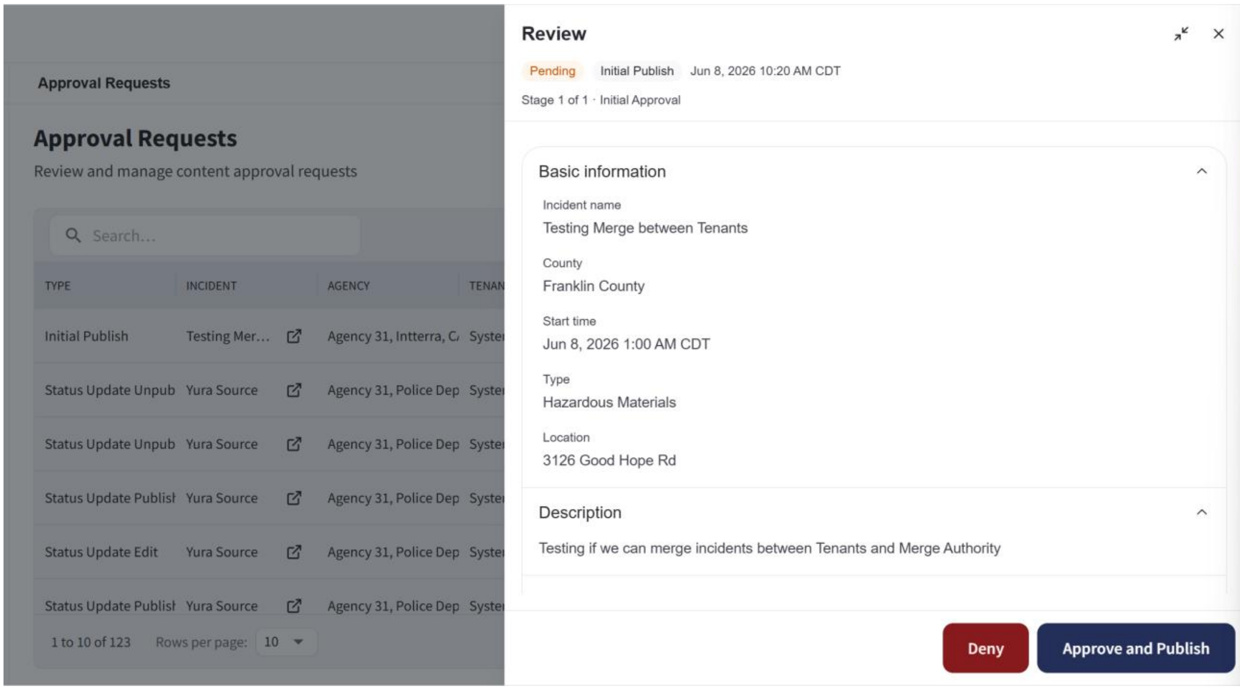

The **Approval Requests** screen can be accessed by selecting **Entities**, then choosing **Approval Requests**. If configured as a sidebar shortcut, Approval Requests may also be accessed directly from the sidebar.

### Searching for an Approval Request

To search for an approval request:

1. Open the **Approval Requests** screen.
2. Select the search bar near the top of the approval request list.
3. Enter search text.
4. Review the filtered results in the approval request table.
5. Select the appropriate approval request to review additional details.

## Review Panel




The **Review Panel** appears when a user selects an approval request from the **Approval Requests** screen. It provides a detailed view of the selected request so the approver can review the submitted content before taking action.

The Review Panel may contain information such as the request status, request type, submitted date and time, approval stage, current stage approvers, approver agency, approver status, decision information, and any related incident information. From this panel, users with the appropriate permissions can approve and publish the request or deny the request.

### Reviewing an Approval Request

To review an approval request:

1. Open the **Approval Requests** screen.
2. Locate the approval request in the list.
3. Select the approval request row or available review action.
4. The Review panel will appear on the right side of the screen.

5. Review the approval request details in the review panel.
6. If available, open the related incident record to review additional context before taking action.

The review panel displays the information needed to evaluate the approval request, including request details, approval status, approver information, and related incident information when available.

### Approving or Denying an Approval Request

**Note:** The approval process can be completed from the Approval Requests section or from within the associated incident itself. Approval actions from within an incident are covered later in this guide.

Users with the appropriate permissions may approve or deny an approval request from the review panel.

To approve or reject an approval request from the Approval Requests section:

1. Open the **Approval Requests** screen.
2. Locate the approval request you need to review.
3. Select the approval request to open the review pane.
4. Review the information displayed in the review pane.
5. If available, open the related incident record to review additional context before taking action.
6. Choose the appropriate action:
   - Select **Approve and Publish** to approve the request and publish the submitted content.
   - Select **Deny** to reject the request.

If the request is denied, a **Reject Request** box will appear. Enter the reason the request is being rejected, then select **Reject**.

After the request is rejected, the user who submitted the content will be notified of the rejection reason. This allows the submitter to understand what needs to be corrected before resubmitting the content for approval.

Before approving or rejecting a request, users should review the request details and any related incident information available to them. This helps ensure approval decisions are made with the proper context.

### Approval History

The Approval Requests section also serves as a record of approval activity within the system.

Users may be able to review past approval requests to see:

- What content was submitted for approval
- Whether the request was approved, rejected, or remains pending
- When the request was submitted or processed
- Which users or approvers were involved in the approval process

Before approving or rejecting a request, users should review the request details and any related incident information available to them. This helps ensure approval decisions are made with the proper context.

## Lookup Tables

Lookup Tables provide access to shared reference values used throughout the platform. Lookup tables help map agency-specific codes and values to standardized platform values so information displays consistently across the system.

Because lookup table management is an administrative function, this section is covered in full detail later in the **Settings** section of this guide.

## Personnel

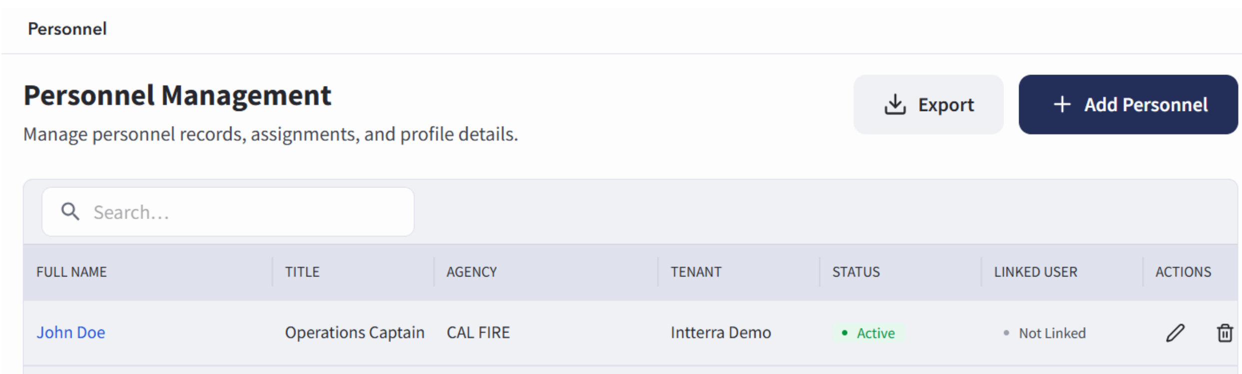
The **Personnel** section is used to view and manage personnel records within the Aware Intel Hub.

Personnel records represent individuals who may need to be referenced, tracked, or assigned within the platform. Personnel may include agency staff, responders, command staff, support personnel, partner agency members, or other individuals who may be associated with operational resources or activity.

Personnel are not necessarily users of the system. A **user** is someone who can sign in to the Aware Intel Hub. A **personnel record** represents a person who may be assigned to units, stations, incidents, agencies, or other items within the platform for operational tracking and reference purposes.

This section is primarily intended for system administrators or users with personnel management permissions. Access to this section and available actions may vary depending on user role, permissions, and agency configuration.

### Personnel Management Screen




The **Personnel Management** screen can be accessed by selecting **Entities**, then choosing **Personnel**. If configured as a sidebar shortcut, Personnel may also be accessed directly from the sidebar.

The Personnel Management screen displays personnel records in a list view. Each personnel record appears as a row in the table.

Users can select a personnel record from the list to open and review additional details.

Users can choose to edit or delete personnel from the Personnel Management screen using the appropriate icons in the Actions column.

## Searching for Personnel

To search for personnel:

1. Open the **Personnel** screen.
2. Select the search bar near the top of the personnel list.
3. Enter the person's name or other available search information.
4. Review the filtered results in the personnel table.
5. Select a personnel record to open additional details.

## Adding Personnel

Users with the appropriate permissions may add new personnel records.

To add personnel:

1. Open the **Personnel** screen.
2. Select **+ Add Personnel**.
3. Complete the required personnel information. Required fields are identified with a red *.
4. Enter any additional details available on the form.
5. If the personnel being added is also a user with a login to the Intel Hub, ensure the personnel profile is linked to the user profile using the **Search and Link User Profile** button.
6. Select **Create Personnel** at the bottom of the page.
7. Review the new personnel record after it has been created.

## Opening a Personnel Record

To open an existing personnel record:

1. Open the **Personnel** screen.
2. Locate the person in the list.
3. Select the personnel record.
4. Review the information displayed on the personnel detail page.

The personnel detail page displays information associated with the selected person. Available information may vary depending on agency configuration and the data entered for that personnel record.

## Editing Personnel

Users with the appropriate permissions may edit existing personnel records.

- Personnel can be edited in two ways:
    - From the **Personnel Management Screen**, select the **Edit** button, shown as a pencil icon, in the **Actions** column next to the personnel record.
    - From the **Personnel Management Screen**, select the personnel record to open the personnel detail page, then select **Edit** in the top-right corner of the page.
- When finished editing, select **Update Personnel** at the bottom-right of the screen.

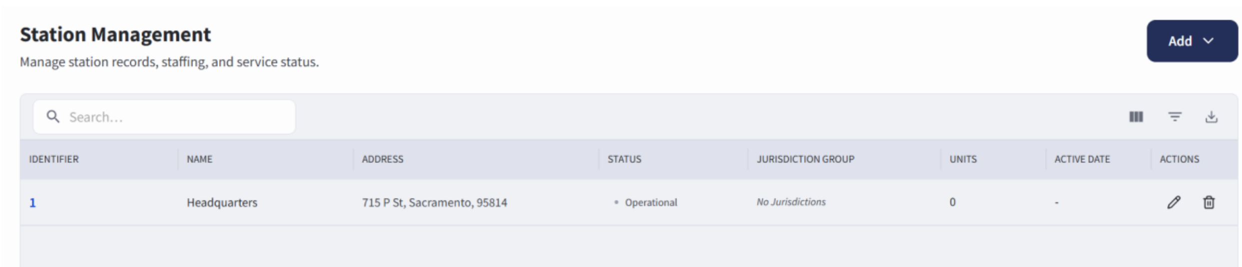
# Stations

The **Stations** section is used to manage station records, staffing, and service status.

Station records represent physical station locations or operational facilities associated with an agency. Stations can be used to support unit assignment, staffing awareness, station location reference, and operational organization within the Aware Intel Hub.

This section is primarily intended for system administrators or users with station management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Station Management Screen




The **Station Management** screen can be accessed by selecting **Entities**, then choosing **Stations**. If configured as a sidebar shortcut, Stations can also be accessed directly from the sidebar.

The Station Management screen includes a searchable table of station records, along with tools to add stations, adjust the table view, filter results, export data, and move between pages of results.

If no station records have been created, the table displays **No data available**.

## Searching for Stations

To search for a station:

1. Open the **Stations** section.
2. Use the search bar on the **Station Management** screen.
3. Enter the station name, identifier, address, or other available search information.
4. Review the filtered results in the station table.
5. Select the station record to review additional details.

## Adding a Station

Users with the appropriate permissions can add a new station from the Station Management screen.

To add a station:

1. Open the **Stations** section.
2. Select **Add** from the top right.
3. Select **Add New Station**.
4. Complete the fields provided. Required fields marked with an asterisk (*).
5. Select **Create Station** at the bottom-right corner of the page.

The Add New Station page includes a message stating that all required fields marked with an asterisk (*) must be completed and that the user must provide either a complete address or coordinates for the station location.

## Add Bulk Stations

Stations can also be added by bulk upload.

To bulk upload stations:

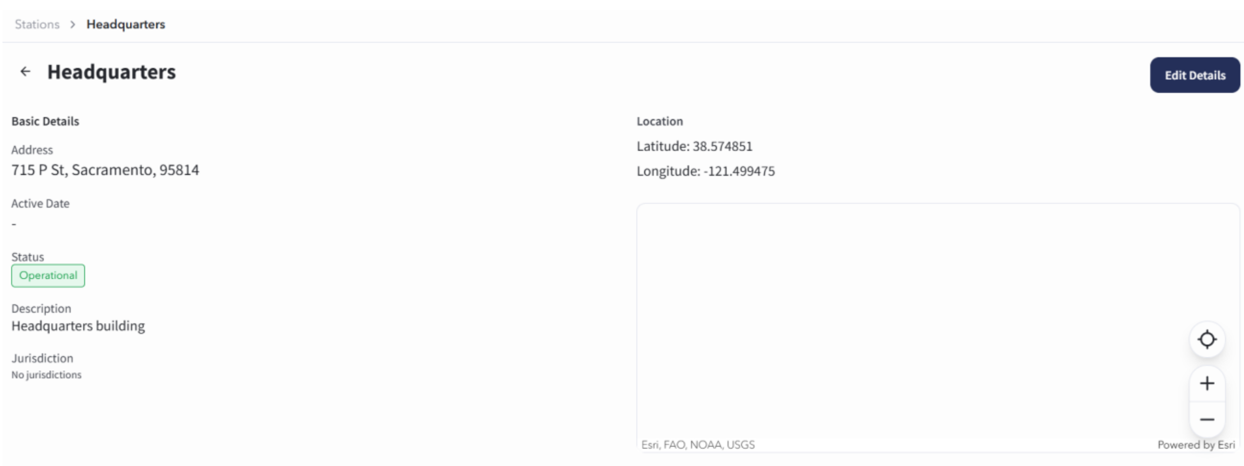
1. Open the **Stations** section.
2. Select **Add**.
3. Select the **Add Bulk Stations** option.
4. Select the appropriate agency from the Bulk Upload/Import Stations screen.
5. Select **Upload CSV File** and then upload a CSV file by browsing for the file or dragging and dropping the file into the upload area.
    - A CSV template can be downloaded by selecting **Download CSV Template** below the Upload CSV File region of the screen.
    - Ensure to follow the CSV format requirements listed next to the Download CSV Template button.

6. Select **Next** after the file has been added.
7. The next screen provides an opportunity to review the fields before uploading. Ensure to review the fields for accuracy then select **Next** at the bottom of the screen.
8. The final screen will show what data will be uploaded. Select **Upload Stations** to complete the process.

The Bulk Upload screen includes the following CSV format requirements:

- Use column headers that match the template, including name, identifier, address fields, coordinates, status, and dates.
- Station name and identifier are required.
- Provide a full address or latitude and longitude for placement.
- Identifier values must be unique within the upload.
- Dates accept YYYY-MM-DD or MM/DD/YYYY format.

## Station Details Screen




Opening an existing station record takes you to the Station Details Screen.

To open an existing station record:

1. Open the **Stations** section.
2. Locate the station in the Station Management table.

3. Select the station record.

The station detail page displays information associated with the selected station, including address, active date, status, description, jurisdiction, map location, and assigned units.

## Editing a Station

Users with the appropriate permissions can edit existing station records.

Stations can be edited from the Station Management screen or from the Station Details screen.

To edit a station from the Station Management screen:

1. Open the **Stations** section.
2. Locate the station record that needs to be updated.
3. In the **Actions** column, select the **Edit** button, shown as a pencil icon.
4. Update the necessary station information.
5. Select **Update Station** at the bottom-right corner of the page.
6. Review the station record to confirm the updates were applied.

To edit a station from the station detail page:

1. Open the **Stations** section.
2. Select the station record you want to update.
3. Review the station detail page.
4. Select **Edit** in the top-right corner.
5. Update the necessary station information.
6. Select **Update Station** at the bottom-right corner of the page.
7. Review the station record to confirm the updates were applied.

# Units

The **Units** section is used to manage trackable units within the Aware Intel Hub.

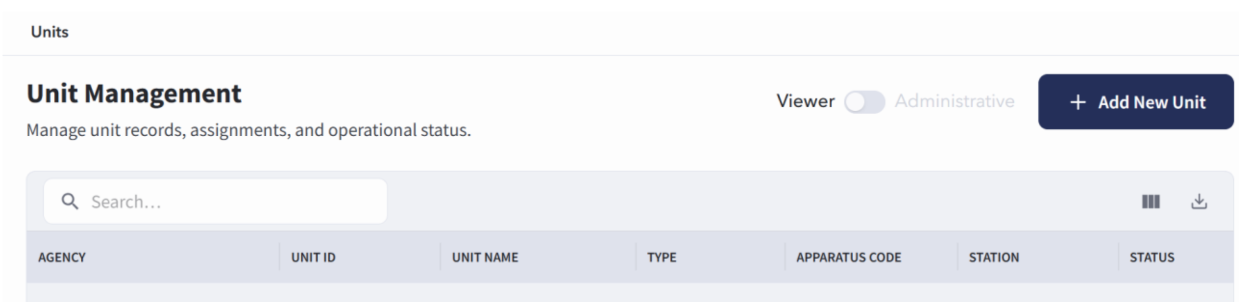
Units are trackable items associated with an agency. In most cases, units are vehicles such as engines, ambulances, command vehicles, patrol vehicles, or other response apparatus. Units can also represent other trackable items when they are configured for location tracking, such as GPS-enabled portable radios or specialized equipment.

Unit records support operational awareness by allowing agencies to track unit identity, capability, assignment, location, and availability within the platform.

Much of the unit information can be brought into the Aware Intel Hub through a CAD integration. When a CAD integration is configured, unit details, status, assignments, and location-related information can be populated from CAD rather than entered manually.

This section is primarily intended for system administrators or users with unit management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Unit Management Screen




The **Unit Management** screen can be accessed by selecting **Entities**, then choosing **Units**. If configured as a sidebar shortcut, Units can also be accessed directly from the sidebar.

The Unit Management screen displays unit records in a table.

The **Viewer / Administrative** toggle changes the table interaction mode. When **Administrative** mode is selected, checkboxes are displayed on the left side of the unit table. These checkboxes allow unit records to be selected for administrative actions.

## Searching for Units

To search for a unit:

1. Open the **Units** section.
2. Use the search bar on the **Unit Management** screen.
3. Enter the unit name, identifier, call sign, unit type, or other available search information.
4. Review the filtered results in the unit table.
5. Select the unit record to review additional details.

## Adding a Unit

Users with the appropriate permissions can add a new unit from the Unit Management screen.

To add a unit:

1. Open the **Units** section.
2. Select **+ Add New Unit** from the top right.
3. Complete the fields provided on the **Add Unit Configuration** screen. Required fields are marked with a red asterisk (*).
4. Review the configuration settings at the bottom of the screen.
5. Select **Create Unit** at the bottom-right corner of the page.

The **Add Unit Configuration** screen is used to enter unit identity, capability, agency association, assignment, location, and configuration information.

The Add Unit Configuration screen includes fields and configuration options for the unit record. Required fields are marked with a red asterisk (*).

The **Show Vehicle in SITSTAT** toggle controls whether the unit is shown in SITSTAT.

The **Estimate Drive Times** toggle controls whether drive time estimates are calculated for the unit.

The **Coverage Flags** toggle controls whether coverage flags are enabled for the unit. Coverage flags indicate the unit's coverage and availability.

### EMS Capability and Ambulance Type

When completing the **Add Unit Configuration** screen, the available fields can change based on the selected unit capabilities. If an ambulance option is selected from the **EMS Capability** dropdown, the **Ambulance Type** field becomes available. Use the Ambulance Type field to define the ambulance classification for the unit.

## Unit Details Screen

Opening an existing unit record takes you to the **Unit Details Screen**.

To open an existing unit record:

1. Open the **Units** section.
2. Locate the unit in the Unit Management table.
3. Select the unit record.

The Unit Details Screen displays information associated with the selected unit, including unit identity, agency association, capability information, assignment information, configuration settings, location information, and related operational details.

The Unit Details Screen includes an **Edit** and **Delete** buttons in the top-right corner and a **Delete** button in the top-right corner.

## Editing a Unit

Users with the appropriate permissions can edit existing unit records.

Units can be edited from the Unit Details Screen.

To edit a unit:

1. Open the **Units** section.
2. Select the unit record you want to update.
3. Review the Unit Details Screen.
4. Select **Edit** in the top-right corner.
5. Update the necessary unit information.
6. Select **Update Unit** at the bottom-right corner of the page.
7. Review the unit record to confirm the updates were applied.

### Deleting a Unit

Users with the appropriate permissions can delete a unit from the Unit Details Screen.

To delete a unit:

1. Open the **Units** section.
2. Select the unit record you want to delete.
3. Review the Unit Details Screen.
4. Select **Delete** in the top-right corner.
5. Confirm the deletion when prompted.

Deleting a unit removes the unit record from the system. Users should confirm the correct unit has been selected before deleting the record.

## Users (Entities Access)

Users are individuals who have the ability to sign in to the Aware Intel Hub. User accounts are used to manage access, invitations, roles, groups, login restrictions, multi-factor authentication, and user activity.

Selecting **Users** from Entities opens the **User Management** screen. Because user management is an administrative function, this section is covered in full detail later in the **Settings** section of this guide.

## Layer Configurations (Entities Access)

The **Layer Configurations** section provides access to layer configuration records used to control GIS-managed map layers within the platform.

Layer configurations define GIS layers available within the current tenant and help determine how layers are displayed, configured, and made available in the map experience.

Because layer configuration is an administrative function, this section is covered in full detail later in the **Settings** section of this guide.

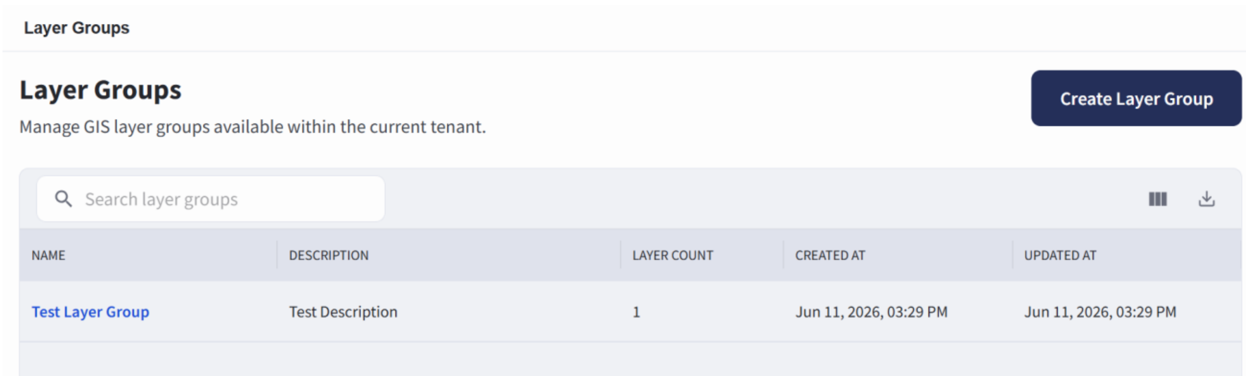
## Layer Groups

The **Layer Groups** section is used to organize layer configurations into groups.

Layer groups allow related map layers to be grouped together so they can be managed and presented more clearly within the platform. A layer group can include one or more configured layers. This helps agencies organize layers by purpose, category, operational use, or map display needs.

This section is primarily intended for system administrators or users with layer group management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Layer Groups Screen




The **Layer Groups** screen can be accessed by selecting **Entities**, then choosing **Layer Groups**. If configured as a sidebar shortcut, Layer Groups can also be accessed directly from the sidebar.

The Layer Groups screen displays existing layer groups in a table.

## Searching for Layer Groups

To search for a layer group:

1. Open the **Layer Groups** section.
2. Use the search bar on the **Layer Groups** screen.
3. Enter the layer group name or other available search information.
4. Review the filtered results in the layer groups table.
5. Select the layer group name to review additional details.

## Creating a Layer Group

Users with the appropriate permissions can create a new layer group from the Layer Groups screen.

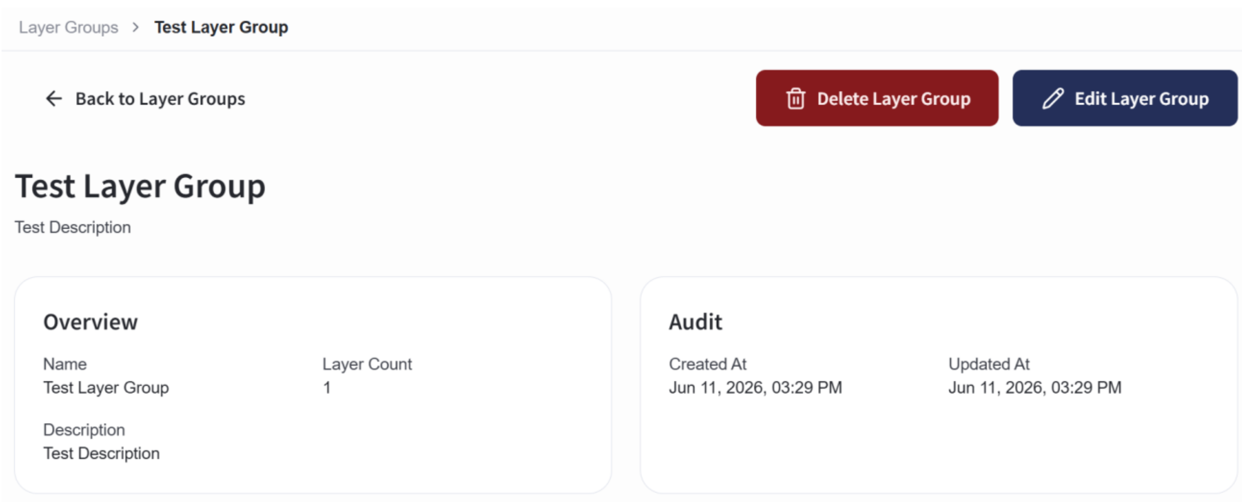
To create a layer group:

1. Open the **Layer Groups** section.
2. Select **Create Layer Group** from the top right.

3. Enter the layer group name.
4. Enter a description for the layer group.
5. Add the layers that should be included in the group.
6. Select **Create Layer Group** at the bottom-right corner of the page.

Layer groups should be named clearly so users can understand what type of layers are included in the group.

## Layer Group Details Screen




Opening an existing layer group takes you to the **Layer Group Details Screen**.

To open an existing layer group:

1. Open the **Layer Groups** section.
2. Locate the layer group in the Layer Groups table.
3. Select the layer group name.

The Layer Group Details Screen displays information associated with the selected layer group.

The Layer Group Details Screen includes:

- An overview of the layer group

- Audit information showing when the layer group was created and when it was last updated
- A table showing the layers included in the group

The Layer Group Details Screen includes a **Delete Layer Group** button in the top-right corner and an **Edit Layer Group** button in the top-right corner.

## Editing a Layer Group

Users with the appropriate permissions can edit existing layer groups.

To edit a layer group:

1. Open the **Layer Groups** section.
2. Select the layer group you want to update.
3. Select **Edit Layer Group** in the top-right corner.
4. Update the layer group name, description, or included layers.
5. Select the update option at the bottom-right corner of the page.
6. Review the layer group record to confirm the updates were applied.

## Deleting a Layer Group

Users with the appropriate permissions can delete a layer group from the Layer Group Details Screen.

To delete a layer group:

1. Open the **Layer Groups** section.
2. Select the layer group you want to delete.
3. Review the **Layer Group Details Screen**.
4. Select **Delete Layer Group** in the top-right corner.
5. Confirm the deletion when prompted.

Deleting a layer group removes the group record from the system. Users should confirm the correct layer group has been selected before deleting it.

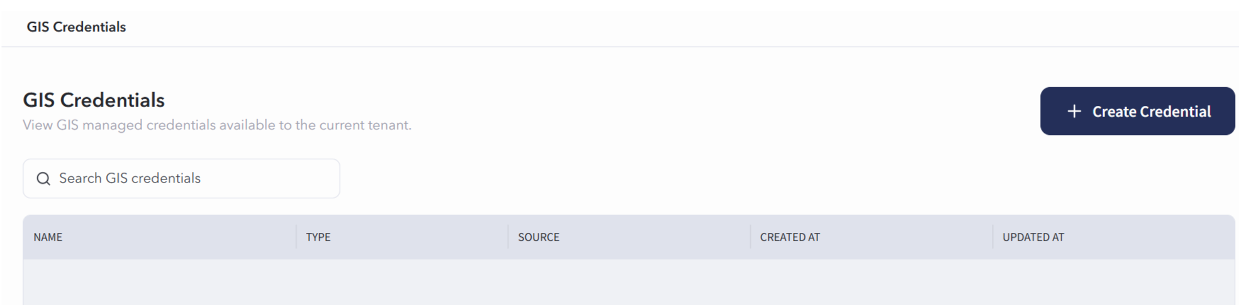
## GIS Credentials

The **GIS Credentials** section is used to manage credentials that allow the platform to connect to GIS data sources.

GIS credentials store the authentication information needed to access secured GIS services. These credentials can be used by layer configurations or other GIS-related features that require authenticated access to external GIS sources.

This section is primarily intended for system administrators or users with GIS credential management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

### GIS Credentials Screen




The **GIS Credentials** screen can be accessed by selecting **Entities**, then choosing **GIS Credentials**. If configured as a sidebar shortcut, GIS Credentials can also be accessed directly from the sidebar.

The GIS Credentials screen displays existing GIS credential records in a table.

### Searching for GIS Credentials

To search for a GIS credential:

1. Open the **GIS Credentials** section.
2. Use the search bar on the **GIS Credentials** screen.

3. Enter the credential name, source, type, or other available search information.
4. Review the filtered results in the GIS credentials table.
5. Select the credential record to review additional details.

## Creating a GIS Credential

Users with the appropriate permissions can create a new GIS credential from the GIS Credentials screen.

To create a GIS credential:

1. Open the **GIS Credentials** section.
2. Select **+ Create Credential** from the top right.
3. Complete the fields provided on the credential form. Required fields are marked with an asterisk (*).
4. Enter the credential details.
5. Enter the credential secret information.
6. Select **Create Credential** at the bottom-right corner of the page.

The create credential form includes the following sections:
The **Credential Details** section is used to enter basic information about the credential.

The **Credential Secret** section is used to enter the authentication information for the credential.

The **Use Default AGOL Token Endpoint** button can be selected to populate the default ArcGIS Online token endpoint.

## GIS Credential Details Screen

Opening an existing GIS credential record takes you to the **GIS Credential Details Screen**.

To open an existing GIS credential record:

1. Open the **GIS Credentials** section.
2. Locate the credential in the GIS Credentials table.
3. Select the credential record.

The GIS Credential Details Screen displays information associated with the selected GIS credential.

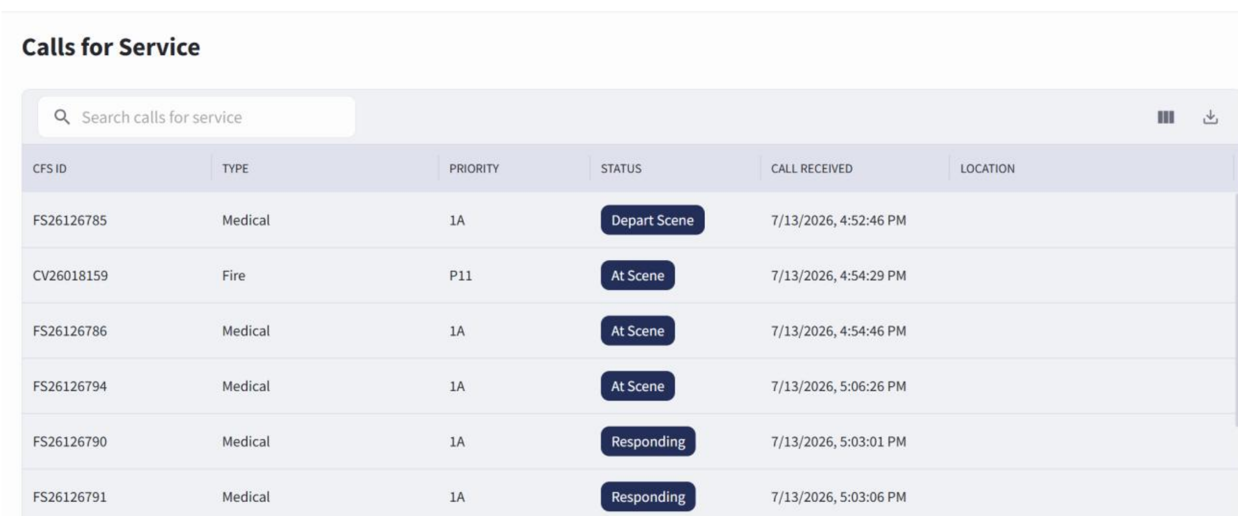
## Incidents (Entities Access)

The **Incidents** option within Entities provides another access point to the main Incidents screen. Selecting Incidents from within Entities will take the user to the same incident list available from the main Incidents section in the sidebar.

Detailed information about the Incidents and Incident Details screens is covered in the Incidents section of this guide. Incident workflows, including creating, editing, updating, merging, closing, and approving incidents, are also covered in the Incidents section.

## Calls for Service

### Calls for Service Screen



Calls for Service

Search calls for service

| CFS ID | TYPE | PRIORITY | STATUS | CALL RECEIVED | LOCATION |
|---|---|---|---|---|---|
| FS26126785 | Medical | 1A | Depart Scene | 7/13/2026, 4:52:46 PM | |
| CV26018159 | Fire | P11 | At Scene | 7/13/2026, 4:54:29 PM | |
| FS26126786 | Medical | 1A | At Scene | 7/13/2026, 4:54:46 PM | |
| FS26126794 | Medical | 1A | At Scene | 7/13/2026, 5:06:26 PM | |
| FS26126790 | Medical | 1A | Responding | 7/13/2026, 5:03:01 PM | |
| FS26126791 | Medical | 1A | Responding | 7/13/2026, 5:03:06 PM | |

The **Calls for Service** (CFS) screen can be accessed by selecting **Entities**, then choosing **Calls for Service**. If available, **Calls for Service** may also be accessed directly from the sidebar.

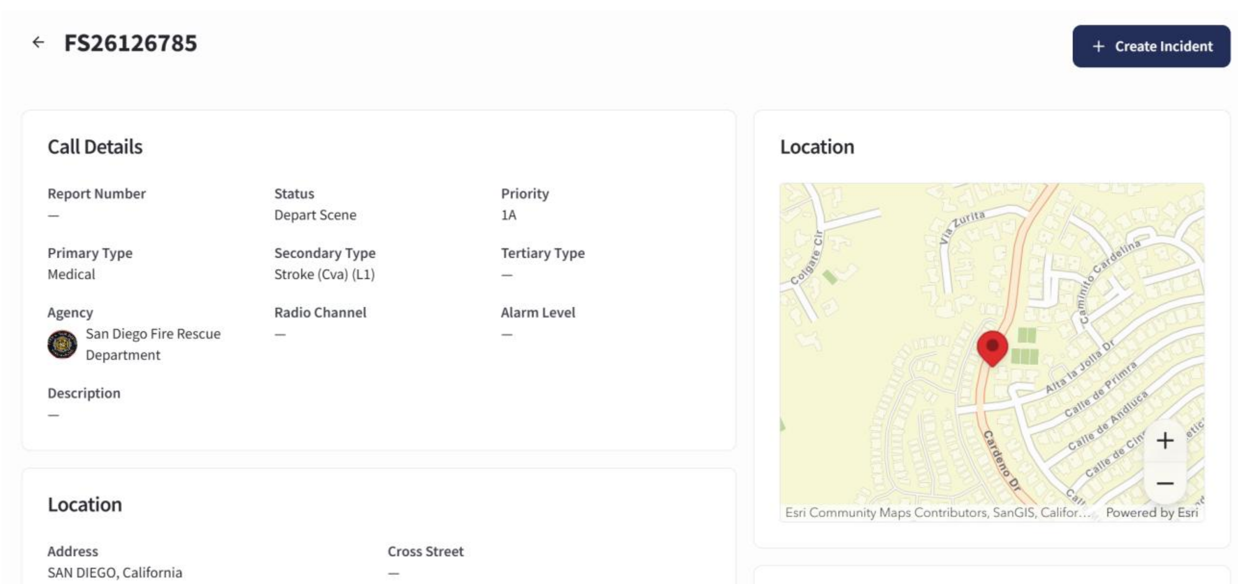
Calls for Service are automatically ingested from your agency's Computer-Aided Dispatch (CAD) system through system integration. These calls are not created or entered manually within Aware Intel Hub.

By default, the screen displays all Calls for Service. Users can apply filters located in the top-right corner of the screen to view Active or Closed Calls. These filtering results are determined by the source status assignments configured under Settings > Calls for Service Statuses. Calls with an unassigned source status appear when viewing all Calls for Service but do not appear in the Active or Closed filtered results.

The list displays key information for each call, including call ID, type, priority, status, date and time received, and location.

Selecting a **CFS ID** will open the detailed view for that specific call for service.

## Call Details Screen




The **Call Details** screen is accessed by selecting a **CFS ID** from the **Calls for Service** screen.

All information displayed on this screen is sourced directly from your agency's CAD system and is automatically populated through integration. This information is not intended to be manually entered or edited within Aware Intel Hub.

This screen provides a detailed view of all information associated with a specific call for service, including:

- Call identifiers such as call for service number and report number
- Status, priority, and call type
- Assigned agency and radio channel
- Call description and location
- Timeline information and caller details

Additional operational information is also available, including:

- A map displaying the location of the call
- Assigned resources
- A narrative log of call activity

Users can create a new incident from a call for service by selecting the **+ Create Incident** button located in the top right corner of the screen.

# Settings

The **Settings** screen provides access to administrative tools used to manage access, organization information, and system configuration within the Aware Intel Hub.

The Settings screen can be accessed by selecting **Settings** from the bottom of the sidebar. Access to Settings and the options displayed on this screen depend on user role, permissions, and agency configuration.

The Settings screen is organized into two main sections:

**Access Management**

The **Access Management** section is used to manage users, roles, and groups.

This section includes:

- **Users:** Manage agency user accounts
- **Roles:** Review role assignments and access definitions
- **Groups:** Manage user groups and memberships

### System Configuration

The **System Configuration** section is used to manage shared configuration and lookup data.

This section includes:

- **Organization:** Manage organization profile and policy settings
- **Lookup Tables:** Configure shared reference values
- **Layer Configurations:** Manage map layer configuration
- **Calls for Service Statuses:** Configure whether Calls for Service source statuses are treated as active or closed
- **Aware Portal Settings:** Manage Aware Portal configuration and approval flow

Each section provides administrators with tools to manage access, configure shared system values, and tailor the platform to support agency operations. The following sections describe each Settings option in more detail.

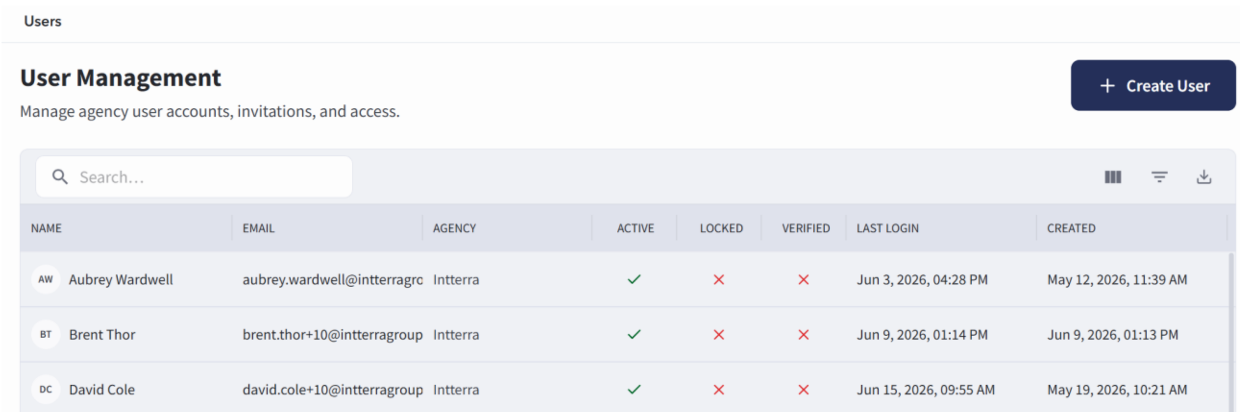
## Users

The **Users** section is used to manage agency user accounts, invitations, and access within the Aware Intel Hub.

Users are individuals who have the ability to sign in to the system. User accounts control who can access the platform and what each person can view or do based on assigned roles, groups, login restrictions, and authentication settings.

This section is primarily intended for system administrators or users with user management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## User Management Screen




The **User Management** screen can be accessed by selecting **Settings**, then choosing **Users**.

The User Management screen displays user accounts in a table.

## Searching for Users

To search for a user:

1. Open the **Users** section.
2. Use the search bar on the **User Management** screen.
3. Enter the user's name, email address, agency, or other available search information.
4. Review the filtered results in the user table.
5. Select the user record to review additional details.

## Creating a User

Users with the appropriate permissions can create a new user from the User Management screen.

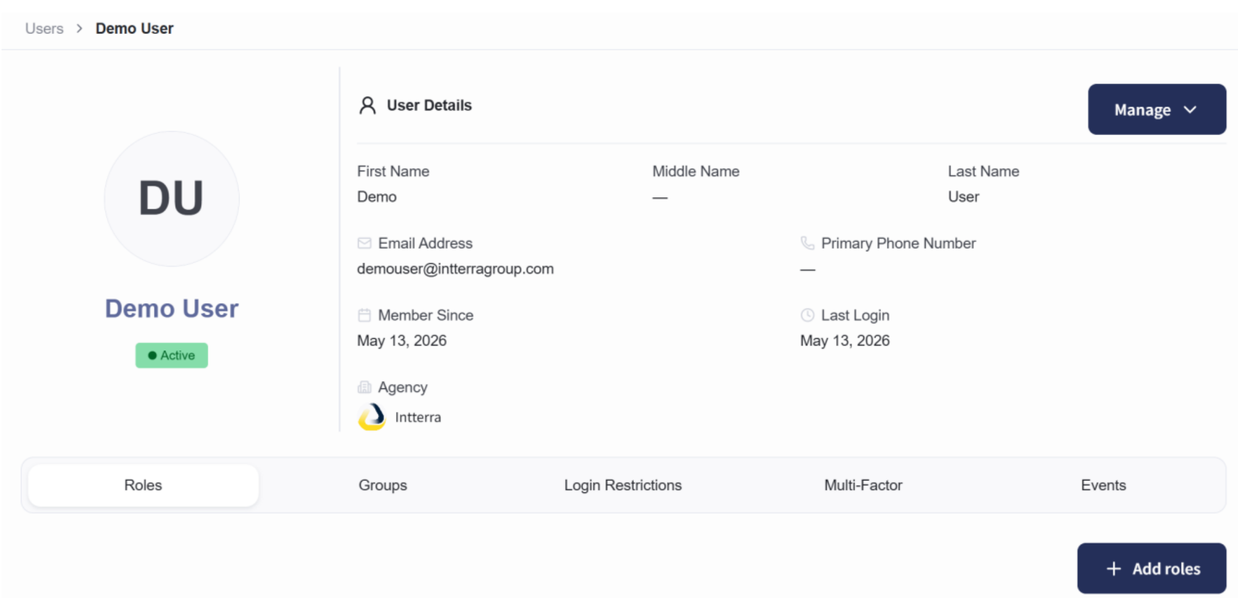
To create a user:

1. Open the **Users** section.
2. Select **+ Create User** from the top right.
3. Complete the fields provided. Required fields are marked with an asterisk (*).
4. Assign the user to the appropriate groups. Assign individual roles only when needed.
5. Select **Create User** at the bottom of the page.

**Important:** When assigning access, groups should generally be used when possible. Groups provide a cleaner and more efficient way to manage permissions because access can be maintained at the group level instead of assigning and updating permissions one user at a time.

Roles can still be assigned directly when needed, but group-based access is preferred for consistency and easier long-term management.

## User Details Screen



Opening an existing user record takes you to the **User Details Screen**.

To open an existing user record:

1. Open the **Users** section.
2. Locate the user in the User Management table.
3. Select the user record.

The User Details Screen displays information associated with the selected user account, including user identity, agency association, account status, assigned access, login restrictions, multi-factor authentication information, and user events.

The User Details Screen includes a **Manage** button and tabs for:

- **Roles**
- **Groups**
- **Login Restrictions**
- **Multi-Factor**
- **Events**

### *Manage Menu*

The **Manage** button provides access to user account management actions.

The Manage menu includes:

- **Edit User**
- **Resend Verification Email**
- **Send Password Reset**
- **Require Password Change**
- **Disable User**
- **Delete User**

### *Editing a User*

Users with the appropriate permissions can edit existing user accounts.

To edit a user:

1. Open the **Users** section.
2. Select the user account you want to update.
3. Select **Manage**.
4. Select **Edit User**.
5. Update the necessary user information.
6. Select the update option at the bottom of the page.
7. Review the user record to confirm the updates were applied.

### *Resending a Verification Email*

Users with the appropriate permissions can resend the verification email used to verify a user's account.

To resend a verification email:

1. Open the **Users** section.
2. Select the user account.
3. Select **Manage**.
4. Select **Resend Verification Email**.
5. Confirm the action when prompted.

This sends the user a new verification email used to verify the account.

### *Sending a Password Reset*

Users with the appropriate permissions can send a password reset to an existing user.

To send a password reset:

1. Open the **Users** section.
2. Select the user account.
3. Select **Manage**.
4. Select **Send Password Reset**.
5. Confirm the action when prompted.

This sends the user instructions for resetting their password.

### *Requiring a Password Change*

Users with the appropriate permissions can require a user to change their password.

To require a password change:

1. Open the **Users** section.
2. Select the user account.
3. Select **Manage**.
4. Select **Require Password Change**.
5. Confirm the action when prompted.

The user will be required to update their password the next time they sign in.

### *Disabling a User*

Users with the appropriate permissions can disable a user account.

To disable a user:

1. Open the **Users** section.
2. Select the user account.
3. Select **Manage**.
4. Select **Disable User**.

5. Confirm the action when prompted.

Disabling a user prevents the user from accessing the system. Administrators should confirm the correct user account has been selected before disabling access.

### *Deleting a User*

Users with the appropriate permissions can delete a user account.

To delete a user:

1. Open the **Users** section.
2. Select the user account.
3. Select **Manage**.
4. Select **Delete User**.
5. Confirm the action when prompted.

Deleting a user removes the user account from system access. Content, records, or activity previously created or modified by that user are not removed when the user account is deleted. Historical records, audit history, incident updates, approvals, and other system activity associated with that user remain in the system.

Administrators should confirm the correct user account has been selected before deleting the user.

## Roles Tab

The **Roles** tab displays roles assigned to the selected user.

Roles define what the user can access or perform within the platform.

To review user roles:

1. Open the **Users** section.
2. Select the user account.
3. Select the **Roles** tab.

4. Review the roles assigned to the user.
5. Roles can be added by selecting the **+ Add Roles** button

**Important:** When assigning access, groups should generally be used when possible. Groups provide a cleaner and more efficient way to manage permissions because access can be maintained at the group level instead of assigning and updating permissions one user at a time.

Roles can still be assigned directly when needed, but group-based access is preferred for consistency and easier long-term management.

## Groups Tab

The **Groups** tab displays groups assigned to the selected user.

Groups provide a repeatable permission structure and should generally be used when assigning access. Managing access through groups helps keep user permissions consistent and easier to maintain.

To review user groups:

1. Open the **Users** section.
2. Select the user account.
3. Select the **Groups** tab.
4. Review the groups assigned to the user.
5. Groups can be added by selecting the **+ Add Groups** button

## Login Restrictions Tab

The **Login Restrictions** tab displays login restriction settings associated with the selected user.

Login restrictions are used to control or limit user access based on configured security requirements.

To review login restrictions:

1. Open the **Users** section.
2. Select the user account.
3. Select the **Login Restrictions** tab.
4. Review the login restriction information.

## Multi-Factor Tab

The **Multi-Factor** tab displays multi-factor authentication information associated with the selected user.

To review multi-factor authentication information:

1. Open the **Users** section.
2. Select the user account.
3. Select the **Multi-Factor** tab.
4. Review the multi-factor authentication information.

## Events Tab

The **Events** tab displays user-related events associated with the selected user account.

This area can be used to review account activity and system events related to the user.

To review user events:

1. Open the **Users** section.
2. Select the user account.
3. Select the **Events** tab.
4. Review the listed events.

# Roles

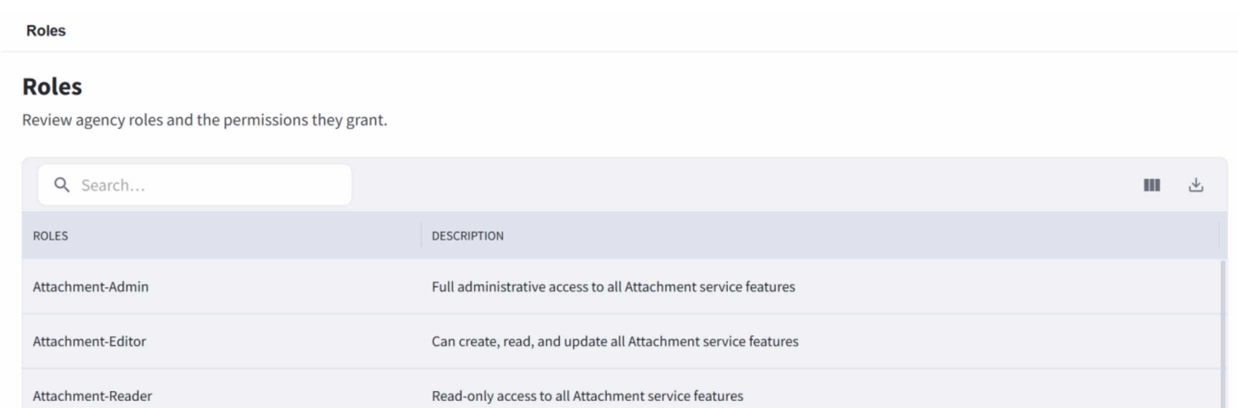
The **Roles** section is used to review access definitions and permissions within the Aware Intel Hub.

Roles define what users are allowed to access or perform in the system. A role is made up of assigned permissions, and those permissions determine what features, screens, actions, and records a user can access.

Roles should generally be assigned to **groups** rather than directly to individual users whenever possible. Assigning roles to groups creates a cleaner and more consistent permission structure. When access needs to change, administrators can update the group instead of managing permissions one user at a time. This makes long-term user management easier and helps reduce permission inconsistencies.

Individual role assignments can still be used when a specific user needs access that is not covered by a group.

## Roles Screen




The **Roles** screen can be accessed by selecting **Settings**, then choosing **Roles** under **Access Management**.

The Roles screen displays available roles and their descriptions in a table.

## Searching for Roles

To search for a role:

1. Open the **Roles** section.
2. Use the search bar on the **Roles** screen.
3. Enter the role name or other available search information.
4. Review the filtered results in the roles table.
5. Select the role to review additional details.

## Role Details Screen

Opening an existing role takes you to the **Role Details Screen**.

To open a role:

1. Open the **Roles** section.
2. Locate the role in the Roles table.
3. Select the role name.

The Role Details Screen displays information associated with the selected role.

At the top of the Role Details Screen, the role description is displayed. If the role is a system default role, the screen also displays information explaining that the role is automatically available to all tenants, cannot be modified or deleted, and that the role and its permissions are consistently applied across all applicable tenants.

### *System Default Roles*

A **system default role** is a role that is automatically available to all tenants.

System default roles cannot be modified or deleted. The role and its permissions are consistently applied across all applicable tenants.

System default roles are used to provide standard access definitions across the platform.

For Aware public-facing content workflows, two roles are particularly important. The **Aware Publisher** role provides publishing capabilities for Aware content, while the **Aware Approver** role provides approval capabilities for users or groups designated to approve Aware content. As with other roles, these roles can be assigned directly to individual users or through groups, with group-based role assignment preferred when possible.

### *Role Information and Assigned Permissions*

The Role Details Screen includes a **Role Information** section and a permissions section.

The **Role Information** section displays basic information about the selected role.

The permissions section displays the permissions assigned to that role. These permissions define the access and actions granted to users or groups that receive the role.

Administrators should review assigned permissions carefully before assigning a role to a group or user. Roles determine what users can access and what actions they can perform within the platform.

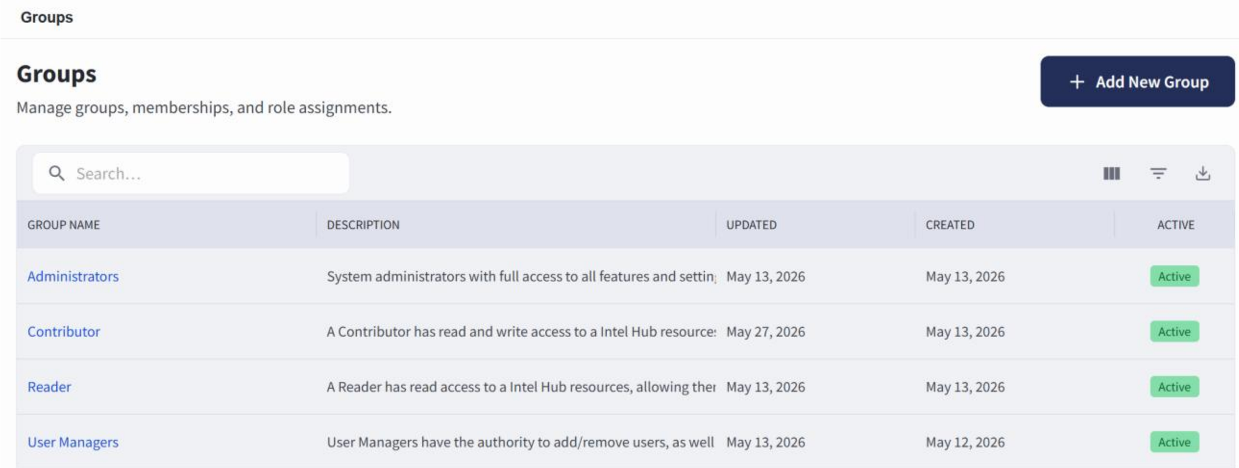
## Groups

The **Groups** section is used to manage user groups and group memberships within the Aware Intel Hub.

Groups provide a way to organize users and assign access more efficiently. Instead of assigning roles directly to each individual user, administrators can assign roles to a group and then add users to that group. This creates a cleaner and more consistent permission structure because access can be managed at the group level.

This section is primarily intended for system administrators or users with group management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Groups Screen




The **Groups** screen can be accessed by selecting **Settings**, then choosing **Groups** under **Access Management**.

The Groups screen displays existing groups in a table.

## Searching for Groups

To search for a group:

1. Open the **Groups** section.
2. Use the search bar on the **Groups** screen.
3. Enter the group name or other available search information.
4. Review the filtered results in the groups table.
5. Select the group name to review additional details.

## Creating a Group

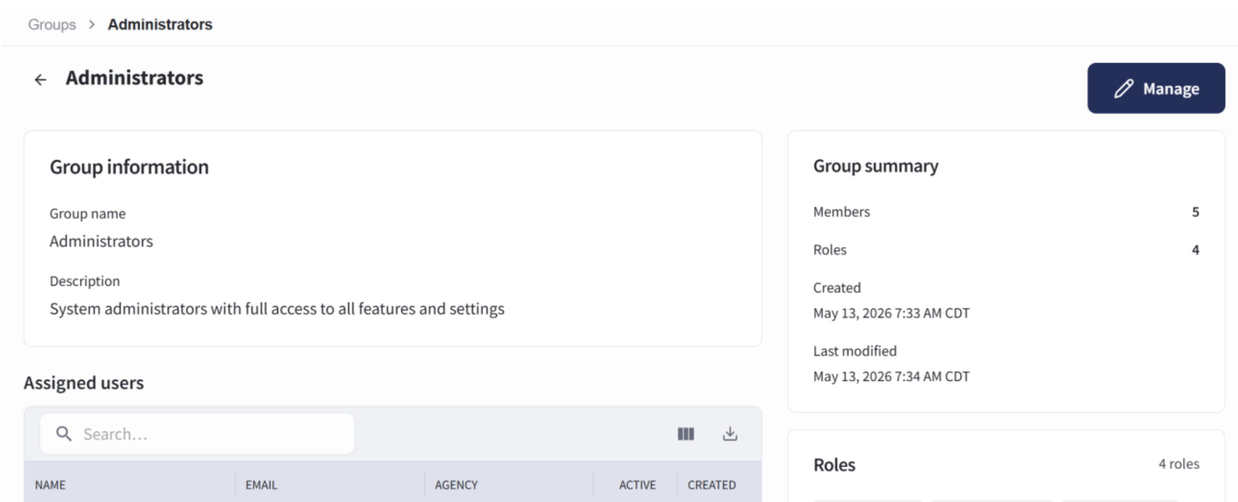
Users with the appropriate permissions can create a new group from the Groups screen.

To create a group:

1. Open the **Groups** section.

2. Select **+ Add New Group** from the top right.
3. Enter the **Group Name**. This field is required.
4. Enter a **Description**. Although the Description field is not required, it is recommended. A clear description helps administrators understand the purpose of the group and makes group management easier over time.
5. Select **Create Group**.

## Group Details Screen




Opening an existing group takes you to the **Group Details Screen**.

To open an existing group:

1. Open the **Groups** section.
2. Locate the group in the Groups table.
3. Select the group name.

The Group Details Screen displays information associated with the selected group.

The Group Details Screen includes:

- **Group Information**, including the group name and description
- **Group Summary**, including the number of members, number of assigned roles, created date, and last modified date

- **Assigned roles**
- **Assigned users**

### *Editing Group Details*

Users with the appropriate permissions can edit the group name and description from the Group Details Screen.

To edit group details:

1. Open the **Groups** section.
2. Select the group you want to update.
3. Select **Manage** in the top-right corner.
4. Update the group name or description.
5. Select **Save Details** to save the changes.

If you need to discard the changes before saving, select **Reset**. The Reset option restores the group name and description to their previous values.

### *Adding Members to a Group*

Users with the appropriate permissions can add members to a group from the Group Details Screen.

To add members to a group:

1. Open the **Groups** section.
2. Select the group you want to update.
3. Select **Manage** in the top-right corner.
4. Locate the assigned users table.
5. Select **+ Add Members** above the assigned users table.
6. Select the users that should be added to the group.
7. Save or confirm the member selection.

Adding members to a group gives those users the access associated with the group's assigned roles.

### *Assigning Roles to a Group*

Users with the appropriate permissions can assign roles to a group from the Group Details Screen.

To assign roles to a group:

1. Open the **Groups** section.
2. Select the group you want to update.
3. Select **Manage** in the top-right corner.
4. Locate the roles box.
5. Select the roles box.
6. Place a check mark next to each role that should be assigned to the group.
7. Select **Update Roles**.

Roles assigned to a group apply to the users who are members of that group. This is the preferred way to manage permissions because it allows administrators to update access for multiple users by managing the group instead of assigning roles user by user.

### *Deleting a Group*

Users with the appropriate permissions can delete a group from the Group Details Screen.

To delete a group:

1. Open the **Groups** section.
2. Select the group you want to delete.
3. Select **Manage** in the top-right corner.
4. Select **Delete Group**.

5. Confirm the deletion when prompted.

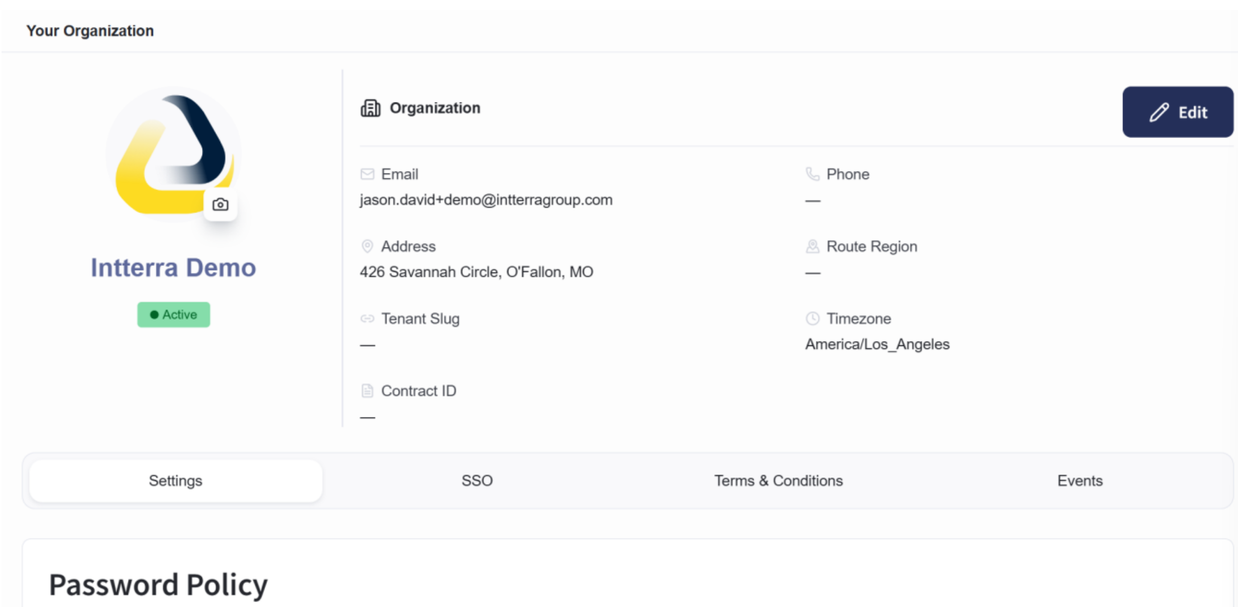
Deleting a group removes the group itself. Administrators should confirm the correct group has been selected before deleting it.

## Organization

The **Organization** section is used to manage the organization profile, security policies, single sign-on settings, terms and conditions, and organization-related event history.

This section is primarily intended for system administrators or users with organization management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

### Your Organization Screen




The **Your Organization** screen can be accessed by selecting **Settings**, then choosing **Organization** under **System Configuration**.

The Your Organization screen displays organization information at the top of the page, including the organization logo, organization name, active status, and organization details.

The Your Organization screen includes the following tabs:

- **Settings**
- **SSO**
- **Terms & Conditions**
- **Events**

An **Edit** button is available in the top-right corner of the screen.

## Editing Organization Information

Users with the appropriate permissions can edit organization information from the Your Organization screen.

To edit organization information:

1. Open the **Organization** section.
2. Select **Edit** in the top-right corner.
3. Update the organization information.
4. Select **Save**.

If the changes should not be saved, select **Cancel**.

## Settings Tab

The **Settings** tab is used to manage organization-level policy settings.

The Settings tab includes:

- **Password Policy**
- **Login Policy**
- **MFA Policy**

### *Password Policy*

The **Password Policy** section defines password requirements that apply to users in the organization.

To update the password policy:

1. Open the **Organization** section.
2. Select the **Settings** tab.
3. Review the **Password Policy** section.
4. Update the password requirements.
5. Select **Save Policy**.

If the changes should not be saved, select **Cancel**.

### *Login Policy*

The **Login Policy** section configures account lockout settings after failed login attempts.

To update the login policy:

1. Open the **Organization** section.
2. Select the **Settings** tab.
3. Review the **Login Policy** section.
4. Update the login policy settings.
5. Select **Save Login Policy**.

If the changes should not be saved, select **Cancel**.

### *MFA Policy*

The **MFA Policy** section configures multi-factor authentication requirements for users in the organization.

To update the MFA policy:

1. Open the **Organization** section.
2. Select the **Settings** tab.
3. Review the **MFA Policy** section.
4. Select the appropriate MFA requirement.
5. Select **Save MFA Policy**.

If the changes should not be saved, select **Cancel**.

## SSO Tab

The **SSO** tab is used to manage single sign-on settings for the organization.

The SSO tab includes:

- **Intterra Login**
- **Identity Providers**
- **Signing Certificates**

### *Intterra Login*

The Intterra Login setting controls whether users can sign in to the tenant using their Intterra credentials.

When enabled, users can sign in to this tenant with their Intterra credentials. When disabled, users are required to sign in through an external identity provider.

Administrators should confirm that at least one external identity provider is configured and enabled before disabling Intterra Login. If Intterra Login is disabled without a working external identity provider, users may be unable to sign in.

### *Identity Providers*

The **Identity Providers** section displays external identity providers configured for tenant login.

To add an identity provider:

1. Open the **Organization** section.
2. Select the **SSO** tab.
3. Select **+ Add Identity Provider**.
4. Complete the identity provider fields. Required fields are marked with an asterisk (*).
5. Select **Create**.

If the identity provider should not be created, select **Cancel**.

### *Signing Certificates*

The **Signing Certificates** section is used to manage signing certificates for identity provider configuration.

To add a signing certificate:

1. Open the **Organization** section.
2. Select the **SSO** tab.
3. Select **+ Add Certificate**.
4. Enter the certificate **Name**.
5. Paste the **Certificate (PEM)** value.
6. Select **Add**.

If the certificate should not be added, select **Cancel**.

## Terms & Conditions Tab

The **Terms & Conditions** tab is used to manage the terms and conditions shown to users at login.

When terms and conditions acceptance is enabled, users see the terms and conditions screen after each successful login.

When terms and conditions acceptance is disabled, users bypass the terms and conditions screen and go directly to the main application.

Changes apply immediately and take effect for new login sessions. Users who are already logged in will see the change on their next login.

To update terms and conditions:

1. Open the **Organization** section.
2. Select the **Terms & Conditions** tab.
3. Turn **Require terms & conditions acceptance at login** on or off.
4. Enter or update the terms and conditions text in the content editor.
5. Select **Preview** to review the content.
6. Select **Save Terms & Conditions**.

### Events Tab

The **Events** tab displays organization-related event history.

To review organization events:

1. Open the **Organization** section.
2. Select the **Events** tab.
3. Use the search bar or table tools to locate the event information.
4. Review the event details in the table.

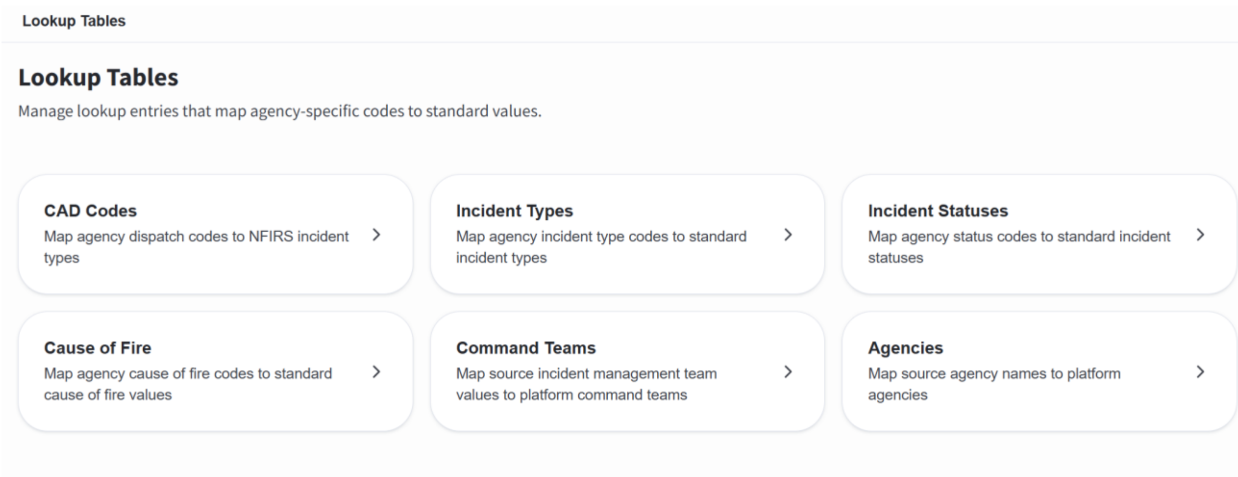
## Lookup Tables

The **Lookup Tables** section is used to configure shared reference values used throughout the Aware Intel Hub.

Lookup tables map agency-specific codes and values to standardized platform values. These mappings help ensure that incoming data is interpreted consistently across the platform.

This section is primarily intended for system administrators or users with lookup table management permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Lookup Tables Screen




The **Lookup Tables Screen** can be accessed by selecting **Settings**, then choosing **Lookup Tables** under **System Configuration**.

The Lookup Tables Screen displays lookup table categories. Each category represents a different type of shared reference value.

The Lookup Tables Screen includes the following lookup table categories:

- **CAD Codes:** Map agency dispatch codes to NFIRS incident types
- **Incident Types:** Map agency incident type codes to standard incident types
- **Incident Statuses:** Map agency status codes to standard incident statuses
- **Cause of Fire:** Map agency cause of fire codes to standard cause of fire values
- **Command Teams:** Map source incident management team values to platform command teams
- **Agencies:** Map source agency names to platform agencies

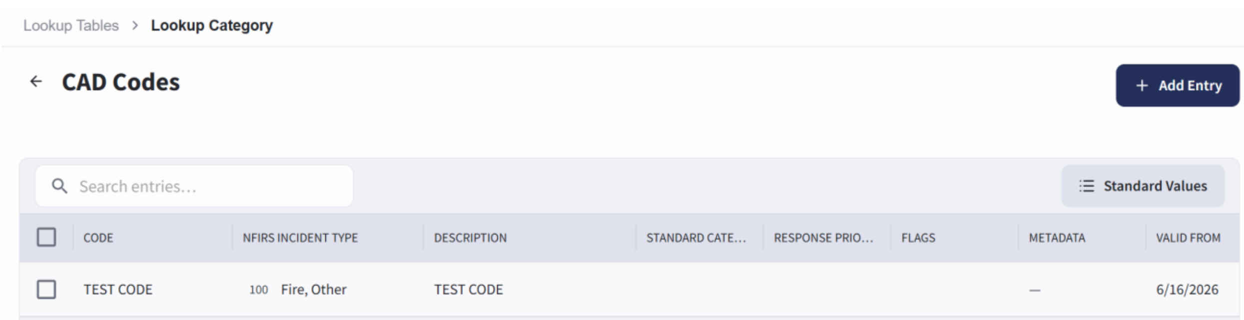
## Opening a Lookup Table Category

To open a lookup table category:

1. Open the **Lookup Tables** section.
2. Select the lookup table category you want to review.

Opening a lookup table category takes you to the lookup category screen for that category.

## Lookup Category Screen




The **Lookup Category Screen** displays lookup entries for the selected category.

The lookup entries table displays the entries that have been configured for the selected lookup category.

If no entries have been created, the table displays **No data available**.

## Standard Values

The **Standard Values** button opens a side panel showing the standard reference values available for the selected lookup category.

Users can review the standard reference values when deciding how an agency-specific code should be mapped.

## Adding a Lookup Table Entry

Users with the appropriate permissions can add a lookup table entry from the lookup category screen.

To add a lookup table entry:

1. Open the **Lookup Tables** section.
2. Select the lookup table category that needs to be updated.
3. Select **+ Add Entry**.
4. Complete the fields provided. Required fields are marked with an asterisk (*).
5. Select **Save**.

If the entry should not be saved, select **Cancel**.

The standard mapped value field changes depending on the selected lookup category.

Examples include:

- **CAD Codes:** NFIRS Incident Type
- **Incident Types:** Standard Type
- **Incident Statuses:** Standard Status
- **Cause of Fire:** Standard Cause of Fire
- **Command Teams:** Command Team
- **Agencies:** Platform Agency

## Managing Lookup Table Entries

After a lookup table entry has been created, it appears in the table for that lookup table category.

Each entry includes a checkbox on the left side of the row. Selecting one or more checkboxes allows users to delete selected entries from the table. When at least one entry is selected, the **Delete Selected** button appears at the top-right of the table.

Each entry also includes row actions on the far right side of the table. These actions include an **Edit** button, shown as a pencil icon, and a **Delete** button, shown as a trash can icon.

## Editing a Lookup Table Entry

Users with the appropriate permissions can edit an existing lookup table entry.

To edit a lookup table entry:

1. Open the **Lookup Tables** section.
2. Select the lookup table category that contains the entry.
3. Locate the entry in the table.
4. Select the **Edit** button, shown as a pencil icon, on the far right side of the entry row.
5. Update the necessary entry information on the **Edit Entry** screen.
6. Select **Save**.

If the entry should not be updated, close the screen or select the available cancel option.

## Deleting a Single Lookup Table Entry

Users with the appropriate permissions can delete an individual lookup table entry.

To delete a single lookup table entry:

1. Open the **Lookup Tables** section.
2. Select the lookup table category that contains the entry.
3. Locate the entry in the table.

4. Select the **Delete** button, shown as a trash can icon, on the far right side of the entry row.
5. When the confirmation window appears, select **Delete Entry**.

If the entry should not be deleted, select **Cancel**.

### Deleting Multiple Lookup Table Entries

Users with the appropriate permissions can delete multiple lookup table entries at one time.

To delete multiple lookup table entries:

1. Open the **Lookup Tables** section.
2. Select the lookup table category that contains the entries.
3. Select the checkbox next to each entry that should be deleted.
4. Select **Delete Selected** at the top-right of the table.
5. Confirm the deletion when prompted.

Selecting multiple checkboxes allows users to delete more than one entry at the same time. Administrators should review the selected entries carefully before confirming deletion.

Administrators should review lookup table entries carefully. Incorrect lookup mappings can cause agency data to appear under the wrong category, display inconsistently, or fail to align with expected platform behavior.

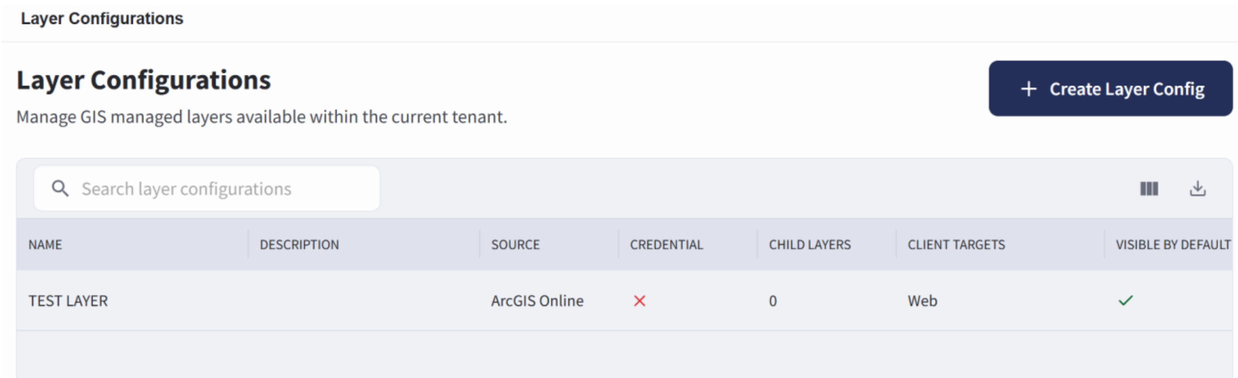
## Layer Configurations

The **Layer Configurations** section is used to manage GIS-managed layers available within the current tenant.

Layer configurations control how GIS layers are connected, displayed, and made available within the map experience. These settings help determine layer source information, display behavior, child layers, capabilities, fields, labels, and advanced layer behavior.

This section is primarily intended for system administrators or users with layer configuration permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Layer Configurations Screen




The **Layer Configurations** screen can be accessed by selecting **Settings**, then choosing **Layer Configurations**.

The Layer Configurations screen displays layer configuration records in a table.

If no layer configuration records have been created, the table displays **No data available**.

After layer configurations have been created, each layer appears as a row in the Layer Configurations table. The **More Options** menu, shown as three vertical dots at the far right of each row, provides quick access to available actions such as **View** and **Edit**.

## Searching for Layer Configurations

To search for a layer configuration:

1. Open the **Layer Configurations** section.
2. Use the search bar on the Layer Configurations screen.

3. Enter the layer name or other available search information.
4. Review the filtered results in the layer configuration table.
5. Select the layer configuration record to review additional details.

## Creating a Layer Configuration

Users with the appropriate permissions can create a new layer configuration from the Layer Configurations screen.

To create a layer configuration:

1. Open the **Layer Configurations** section.
2. Select **+ Create Layer Config** from the top right.
3. Complete the fields provided on the **Create Layer Config** screen. Required fields are marked with an asterisk (*).
4. Configure the available layer settings.
5. Select **Create Layer Config** to create the layer configuration.

The Create Layer Config screen includes **Basic Details** and several configuration tabs.

The **Basic Details** section includes:

- **Layer Name**
- **Source Type**
- **Source URL**
- **Credential**
- **Client Targets**

The **Layer Name** and **Source URL** fields are required.

The **Source Type** field displays the GIS source type for the layer.

The **Credential** area includes:

- **Select Credential** – Selecting this provides a dropdown box for a credential to be selected.
- **Remove Credential** – Allows for the removal of a credential.

The **Client Targets** field identifies where the layer is available. The following options are available: Web, Mobile, Pro, Global.

A **Visible by Default** toggle switch allows the user to make the layer visible by default.

A **Description** box allows the user to enter an overall description of the layer.

The **Attribution** box is used to enter credit or source information for the layer. This can include the data provider, source agency, licensing note, or other attribution text that should be associated with the layer.

Use this field when the layer data requires source credit or when users need to understand where the layer information originated.

## Display Settings Tab

The **Display Settings** tab controls scale, zoom, and transparency behavior for the layer.

## Child Layers Tab

The **Child Layers** tab is used to configure child layers associated with the layer configuration.

If no child layers have been added, the tab displays **No child layers added**.

## Capabilities Tab

The **Capabilities** tab is used to configure capability settings for the layer.

Capabilities determine which layer functions are supported and how the layer can be used within the platform. This can include functionality related to querying, editing support, spatial reference handling, rendering behavior, and other GIS layer capabilities.

## Fields Tab

The **Fields** tab is used to configure fields associated with the layer. Fields can be added by selecting **Add Fields**.

If no fields have been added, the tab displays **No fields added**.

## Label Configuration Tab

The **Label Configuration** tab is used to configure labeling behavior for the layer.

Use this tab to review and configure how labels are handled for the layer configuration.

Toggling on **Use Custom Label Configuration** provides additional label fields and options.

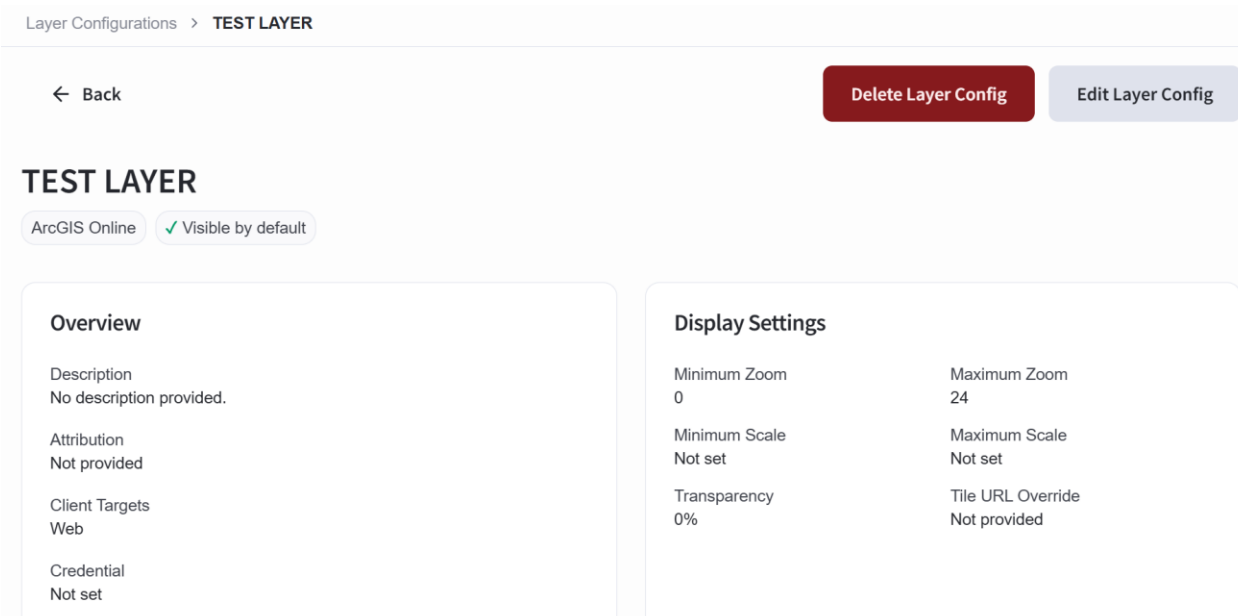
Toggling on **Use Custom Styling** provides additional label styling options.

## Advanced Tab

The **Advanced** tab is used to configure advanced layer settings.

Use this tab to review and configure additional layer behavior not handled in the other configuration tabs.

## Layer Details Screen




Opening an existing layer configuration record takes you to the **Layer Details Screen**.

To open an existing layer configuration record:

1. Open the **Layer Configurations** section.
2. Locate the layer configuration in the Layer Configurations table.
3. Select the layer configuration record.

A layer configuration can also be opened by selecting the **More Options** menu, shown as three vertical dots, and choosing **View**.

The Layer Details Screen provides an overview of the selected layer configuration. This screen includes the layer's basic configuration information and additional sections for display settings, capabilities, configured fields, child layers, full extent, label configuration, and audit information.

The Layer Details Screen includes a **Delete Layer Config** button in the top-right corner and an **Edit Layer Configuration** button in the top-right corner.

## Editing a Layer Configuration

Users with the appropriate permissions can edit existing layer configuration records.

Layer configurations can be edited in two ways:

- From the **Layer Configurations** screen, select the **More Options** menu, shown as three vertical dots, then select **Edit**.
- From the **Layer Details Screen**, select **Edit Layer Configuration** in the top-right corner.
- Select **Save Changes** when complete.

## Deleting a Layer Configuration

Users with the appropriate permissions can delete a layer configuration from the Layer Details Screen.

To delete a layer configuration:

1. Open the **Layer Configurations** section.
2. Select the layer configuration record you want to delete.
3. Review the **Layer Details Screen**.
4. Select **Delete Layer Config** in the top-right corner.
5. Confirm the deletion when prompted.

Deleting a layer configuration removes the layer configuration record from the system. Users should confirm the correct layer configuration has been selected before deleting the record.

# Calls for Service Statuses

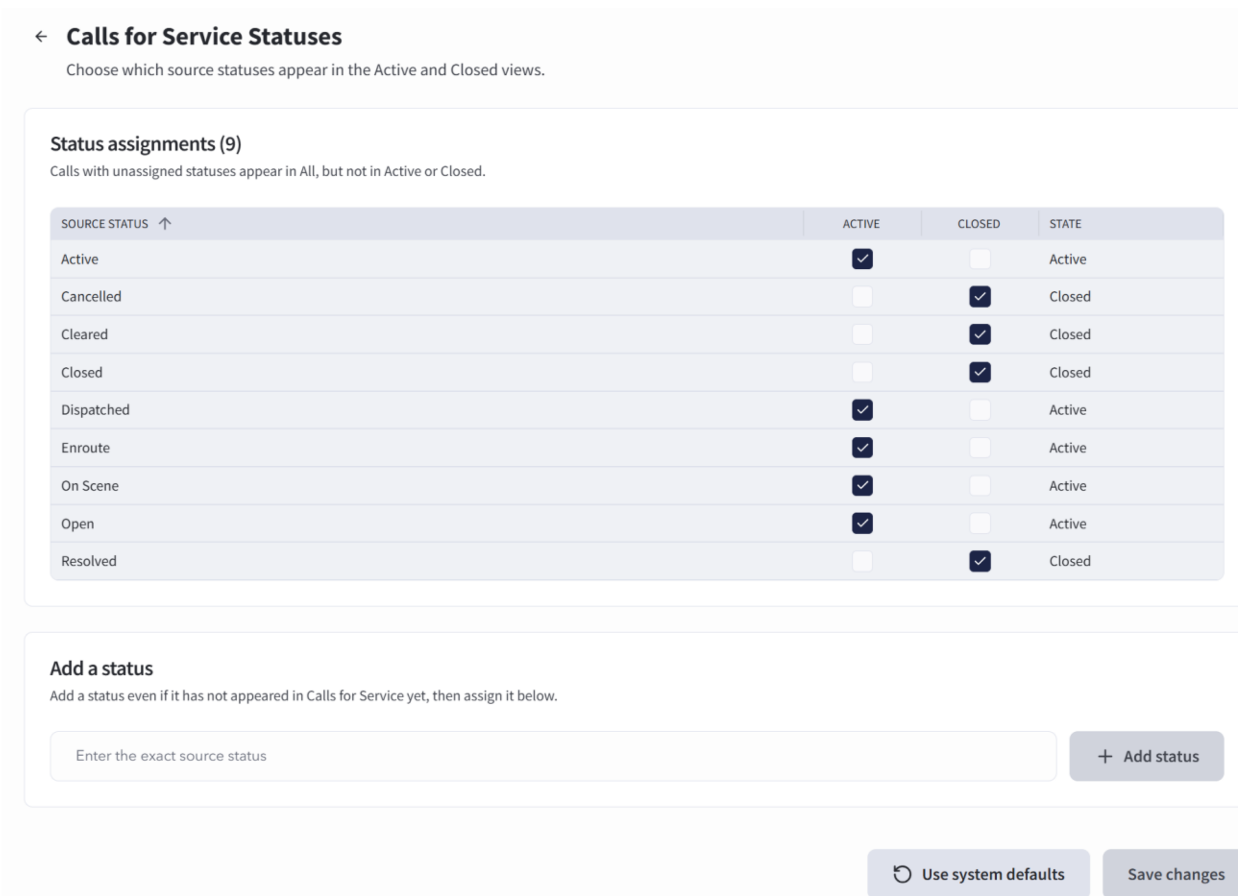
The Calls for Service Statuses section allows agencies to control whether each Call for Service source status is treated as Active or Closed within the Aware Intel Hub.

These assignments directly affect the Active and Closed filtering available on the Calls for Service screen under Entities.

This section is primarily intended for system administrators or users with the appropriate configuration permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Calls for Service Statuses Screen

The Calls for Service Statuses screen can be accessed by selecting Settings, then choosing Calls for Service Statuses under System Configuration.




The Status Assignments table displays each available Source Status and its current Active or Closed assignment.

The Source Status list includes:

- Default statuses provided by Intterra
- Statuses received through the integration with the agency's Computer-Aided Dispatch (CAD) system
- Statuses manually added by an authorized user

Default statuses provided by Intterra are automatically assigned as Active or Closed. These default assignments can be changed based on the agency's operational needs.

Statuses received from the agency's CAD integration are automatically added to the Source Status list. However, newly received CAD statuses are not automatically assigned as Active or Closed. An authorized user must assign each new status before it will appear when filtering Calls for Service by Active or Closed.

Calls with an unassigned source status appear when viewing all Calls for Service but do not appear in the Active or Closed filtered results.

## Assigning a Source Status

To assign or change a source status:

1. Locate the status in the Status Assignments table.
2. Select either Active or Closed for that status.
3. Review the assignment to confirm that the correct option is selected.
4. Select Save Changes in the bottom-right corner.

Each source status should be assigned as either Active or Closed based on how the agency wants Calls for Service with that status categorized within the Intel Hub.

## Adding a Status Manually

A source status can be added manually before it is received through the agency's CAD integration. This allows the agency to configure a known CAD status proactively.

To add a status manually:

1. Locate the Add a Status section.
2. Enter the source status exactly as it appears in the agency's CAD system.
3. Verify that the spelling, capitalization, spacing, and punctuation match the CAD status verbatim.
4. Select + Add Status.
5. Assign the newly added status as Active or Closed.
6. Select Save Changes.

**Important:** Selecting **+ Add Status** immediately adds the entered status. Carefully verify the entry before selecting the button.

### Using System Defaults

Selecting Use System Defaults restores the default Active or Closed assignments for statuses provided by Intterra.

This action does not remove source statuses received through the agency's CAD integration. However, it removes the Active or Closed assignments from those additional CAD statuses. Each affected CAD status must then be reassigned manually.

After reviewing and updating the assignments, select Save Changes.

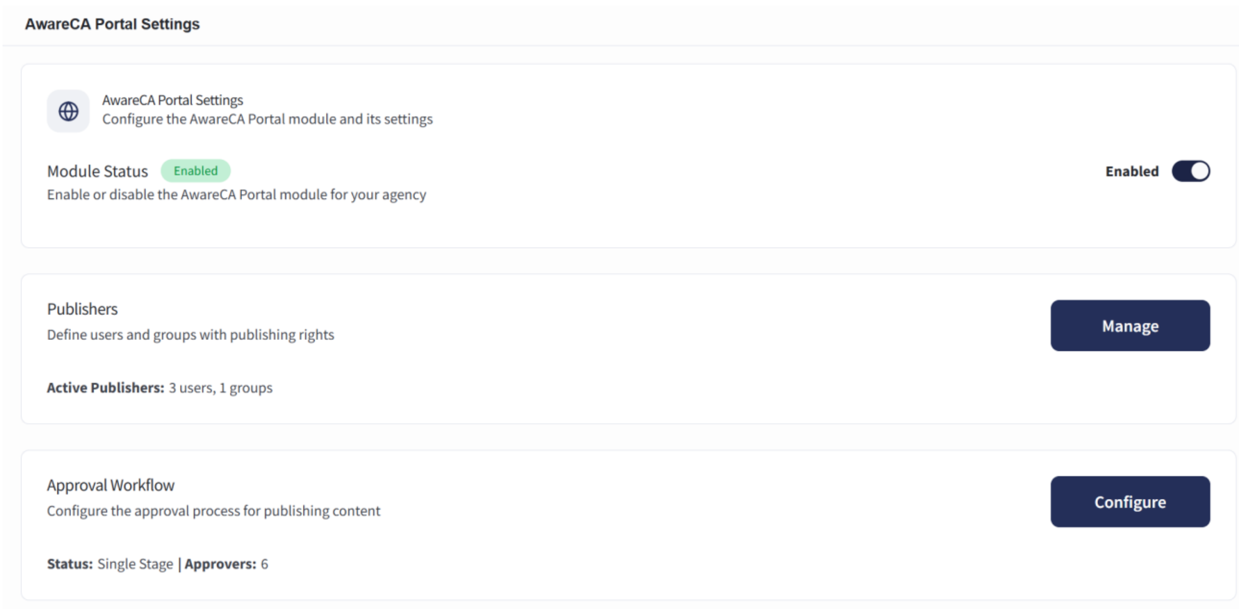
## Aware Portal Settings

The **Aware Portal Settings** section is used to manage the Aware Portal module, publishing rights, and approval workflow.

**Note:** Depending on your state, Aware Portal Settings will be labeled with the applicable state abbreviation (e.g., AwareCA Portal Settings).

This section is primarily intended for system administrators or users with portal configuration permissions. Access to this section and available actions depend on user role, permissions, and agency configuration.

## Aware Portal Settings Screen




The **Aware Portal Settings** screen can be accessed by selecting **Settings**, then choosing **Aware Portal Settings** under **System Configuration**.

The Aware Portal Settings screen includes:

- **Module Status**
- **Publishers**
- **Approval Workflow**

## Module Status

The **Module Status** section controls whether the Aware Portal module is enabled for the agency.

The screen displays the current module status, such as **Enabled**, and includes an enabled/disabled toggle.

To enable or disable the Aware Portal module:

1. Open **Aware Portal Settings**.

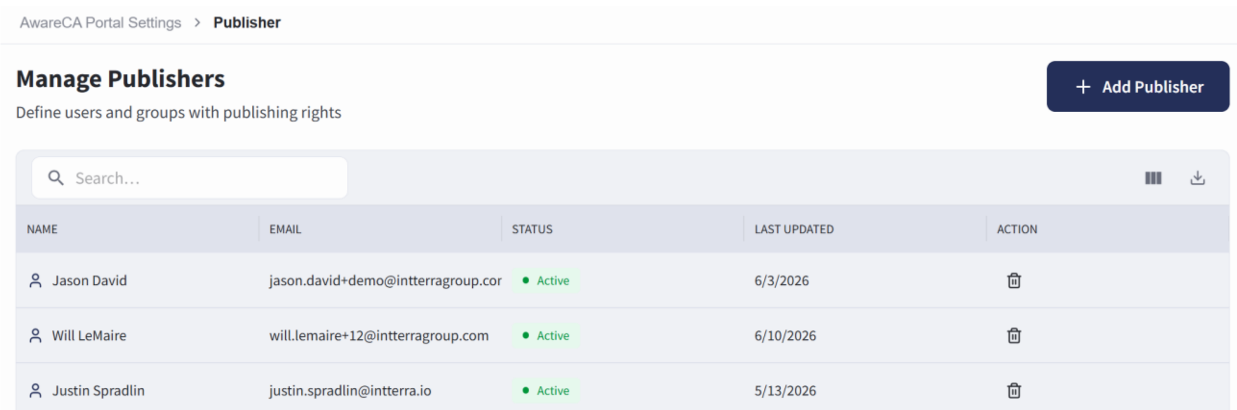
2. Locate the **Module Status** section.
3. Use the toggle to enable or disable the module.

## Publishers

The Publishers section is used to define users and groups with publishing rights. Users or groups that are authorized to publish content to Aware must have the **Aware Publisher** role.

The Publishers section displays the number of active publishers, including active users and groups. Select **Manage** to open the Manage Publishers screen.

### *Manage Publishers Screen*




The **Manage Publishers** screen displays users and groups with publishing rights.

### *Adding a Publisher*

Users with the appropriate permissions can add a publisher from the Manage Publishers screen.

To add a publisher:

1. Open **Aware Portal Settings**.
2. In the **Publishers** section, select **Manage**.
3. Select **+ Add Publisher**.

4. In the **Add Publisher** window, select **Users** or **Groups**.
5. Search by name or email.
6. Select the user or group that should receive publishing rights.
7. Select **Add**.

If the publisher should not be added, select **Cancel**.

### *Removing a Publisher*

Users with the appropriate permissions can remove a publisher from the Manage Publishers screen.

To remove a publisher:

1. Open **Aware Portal Settings**.
2. In the **Publishers** section, select **Manage**.
3. Locate the publisher in the table.
4. Select the delete icon in the **Action** column.
5. Confirm the removal when prompted.

Removing a publisher removes that user or group from the list of users or groups with publishing rights.

## Approval Workflow

The **Approval Workflow** section is used to control whether approval is required before public-facing content can be published.

Approvers are not configured within the Approval Workflow settings. Approval capability is provided through the **Aware Approver** role. The role can be assigned directly to individual users or through groups, with group-based role assignment recommended whenever possible.

Select **Configure** to open the Approval Flow screen.

**Approval Flow Screen**

The **Approval Flow** screen is used to enable or disable the approval requirement for public-facing content.

The screen includes a **Require Approval** toggle:

- **Enabled:** Content must go through the approval process before it can be published.
- **Disabled:** Approval is not required before content is published by users with the appropriate publishing permissions.

**Configuring the Approval Requirement**

To configure the approval workflow:

1. Open **Aware Portal Settings**.
2. In the **Approval Workflow** section, select **Configure**.
3. Turn **Require Approval** on or off as appropriate.
4. Select **Save Workflow Configuration**.

# Support

At Intterra, we are committed to your success. Whether you have a quick question, need technical assistance, or want to explore more of what the platform can do, our team is here to help. The following resources are available to support you and your agency.

## Emergency Support

**24/7 Emergency Phone Support**

For critical issues that require immediate assistance, Intterra offers 24/7 phone support for authorized agency users.

Emergency Support Number:

- 1-916-794-9775

This number connects directly to our on-call support team and is intended for urgent, high-impact issues such as:

- System outages or major service disruptions
- Data not updating or flowing as expected
- Issues impacting active incidents or operations

**Important:** This phone support is reserved for emergency situations. For non-urgent requests, including general questions, training, minor issues, or account assistance, please use one of the standard support methods listed below.

## Non-Emergency Support

**Customer Support Website**
Intel Hub users should use the Intterra Customer Portal for support requests. From the Knowledge Base page, select Customer Portal or Sign In in the upper-right corner. First-time users can select Register here to create an account. Once signed in, users can submit support tickets, track their progress, and respond directly to the Intterra Support team.

**Email Support Requests**
You may also submit a support request via email:
Support@Intterragroup.com

*Emails sent to this address will automatically generate a support ticket. However, this method does not provide request tracking or status updates. When submitting via email, please include your agency name and any relevant details to help us assist you more efficiently.*

## Additional Resources

**Product Knowledge Base**
Access step-by-step guides, training videos, and detailed documentation:
Service Management Knowledge Base

**New Feature Requests**
If you have a new idea or enhancement that could improve our products, we encourage you to submit a new feature request here:
https://intterragroup.atlassian.net/servicedesk/customer/portals

Select Suggest a Product Improvement and complete the form. Once submitted, your request will be routed to our Product Management team for review. The team will evaluate the idea and may reach out with additional questions or requests for clarification if needed.

## Aware Public-Facing App Support

For support related to the Aware public-facing mobile app, including AwareCA, users can contact support directly from within the app.

On the mobile app, go to Settings, select FAQ, then choose How do I contact support.

**Support Email Address:**
aware-help@intterragroup.com

# Appendix A: Supported Incident Attachment File Types

Incident attachments support common document, image, text/data, spreadsheet, compressed archive, and video formats.

The default file size limit is **100 MB per attachment**. This limit is configurable if a different maximum file size is needed.

## Supported File Extensions

The following file extensions are currently allowed for incident attachments:

- PDF
- JPEG
- JPG
- PNG
- GIF
- WEBP
- TXT
- CSV
- JSON
- GEOJSON
- XML
- DOC
- DOCX
- XLS
- XLSX
- ZIP
- MP4
- WEBM
- MOV
- AVI
- MKV
- SVG

## Supported File Types

The following file types are currently allowed for incident attachments:

| Category | Supported File Type |
|---|---|
| Application | pdf |
| Application | octet-stream |
| Application | json |
| Application | geo+json |
| Application | xml |
| Application | msword |
| Application | vnd.openxmlformats-officedocument.wordprocessingml.document |
| Application | vnd.ms-excel |
| Application | vnd.openxmlformats-officedocument.spreadsheetml.sheet |
| Application | zip |
| Image | jpeg |
| Image | jpg |
| Image | png |
| Image | gif |
| Image | webp |
| Image | svg |
| Text | plain |
| Text | csv |
| Video | mp4 |
| Video | webm |
| Video | quicktime |
| Video | x-msvideo |
| Video | x-matroska |

POWERED BY:

INTTERRA