Aware
Intel Hub

USER TRAINING PROGRAM

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

Aware Intel Hub

User Training Program

Introduction

The Aware Intel Hub User Training Program is designed to provide agencies with a structured, repeatable approach to training personnel on how to effectively use the Aware Intel Hub platform.

Aware Intel Hub is the internal operational platform used to access integrated data, monitor activity, manage incidents, review approvals, and support public-facing information workflows. It serves as the internal workspace where authorized users create, review, update, approve, and manage information before it is shared externally through the public-facing Aware platform.

Throughout this training, Aware may be used as a broad term for the public-facing community awareness platform. In state-specific deployments, the public-facing app is branded using the state abbreviation, such as AwareCA for California, AwareMO for Missouri, or AwareWA for Washington. Agencies maintain control over what information is published, when it is updated, and when it is removed.

Aware Ops is an operational mobile platform currently in development. It may be mentioned during the platform overview for context, but it is not part of the live training workflow in this program.

This training program enables agencies to conduct internal training using standardized materials while still allowing instructors to adapt examples, scenarios, and pacing to the needs of the audience. The program is designed to be instructor-led and to support long-term, self-sustained training efforts within each agency.

Available screens, buttons, and workflows may vary depending on user role, permissions, agency configuration, enabled modules, and the training environment being used.

Purpose

The purpose of this program is to:

- Provide a clear and repeatable framework for agency-led training.
- Ensure personnel understand how to navigate the platform and manage public-facing incident information.

- Reinforce effective use of the system for operational awareness and public communication workflows.
- Support consistent adoption of Aware Intel Hub across general users, approvers, and system administrators.
- Help instructors deliver training in a consistent order while still allowing flexibility for agency-specific needs.

This program is not intended to replace the Aware Intel Hub Complete User Guide. It is intended to guide instructors through a structured training session using the provided materials, live system demonstration, and guided walkthroughs.

Platform Context

Aware Intel Hub, Aware Ops, and Aware work together as part of the broader Aware ecosystem.

Aware Intel Hub is the internal data, intelligence, and incident management platform. It allows authorized users to access operational data, review activity, manage incidents, and prepare public-facing information.

Aware Ops is an operational mobile platform currently in development. It is intended to extend operational information to personnel in the field, but it is not included as part of this training workflow.

Aware is the public-facing community awareness platform. It allows agencies to share approved, public-facing incident and safety information with residents, visitors, and stakeholders. State deployments are branded with the appropriate state abbreviation, such as AwareCA, AwareMO, or AwareWA.

A key concept to reinforce throughout training is that the public does not directly access Aware Intel Hub. Intel Hub is the internal platform. Aware is the public-facing platform. Information becomes public only when it is approved and published through the appropriate workflow, depending on agency configuration.

Training Materials

The following materials are required to conduct a training session:

- Aware Platform Overview PowerPoint.

- Aware Intel Hub – User Training Program (this document).
- Provided training media, including sample incident narratives, resource links, and any files used for guided walkthroughs.
- Access to Aware Intel Hub with screen sharing capability.
- Appropriate training environment access for the instructor.

The following materials are recommended for reference:

- Aware Intel Hub Complete User Guide.
- Quick Start Guide - Content Management for Incidents.

Training Overview and Flow

This training is delivered in a structured, instructor-led format that combines presentation, live demonstration, and guided walkthrough.

Phase 1 - Slide-Based Overview

- Instructor presents slides 1-24 of the Aware Platform Overview PowerPoint.
- Slide notes are used to guide instruction.
- The presentation introduces the public-facing Aware platform and provides context before transitioning into the live Aware Intel Hub demonstration.

Phase 2 - Live System Demonstration

- Instructor transitions into Aware Intel Hub.
- Instructor demonstrates system navigation and core functionality.
- Instructor provides real-time examples within the platform.

Phase 3 - Guided Workflow Walkthrough

- Instructor walks through key workflows step-by-step.
- Instructor can choose to utilize provided scenarios, sample incident narratives, and resource links.
- Instructor emphasizes real-world use, public-facing content awareness, and decision-making.
- Instructor reinforces how approval workflows affect what becomes visible externally.

The final portion of the training is used to review support resources, answer questions, and reinforce post-training expectations.

Instructor Guidance

This document is intended to support instruction and should not be read word-for-word.

The training should be delivered as a combination of brief presentation, live system demonstration, and guided workflow walkthrough. The live walkthrough should serve as the primary teaching method.

Instructors should:

- Use the PowerPoint to introduce the Aware platform, public-facing app experience, and overall context.
- Ask early whether participants have used the public-facing Aware app or Aware Intel Hub, and adjust pacing based on their familiarity.
- Transition quickly into the live Aware Intel Hub environment.
- Use the Detailed Training Outline for structure, key talking points, and step-by-step delivery.
- Once familiar with the program, topics, and flow, create a personal, simplified delivery outline if helpful. Treat that outline as an instructor aid, not as the source of truth.
- Demonstrate actions live within the platform when possible.
- Focus on explaining why actions are taken, not just how to click through screens.
- When teaching system administrator topics, provide guided orientation and key workflows rather than walking every field on every tab.
- Encourage questions throughout the session or reserve them for the end, depending on the training format.
- Adjust pacing based on audience experience, training goals, and whether the session is general user training or system administrator training.

Key concepts to reinforce throughout training:

- Aware Intel Hub is an internal operational platform and is not directly accessible by the public.
- Aware is the public-facing community awareness platform.

- Each state deployment is branded with the applicable state abbreviation, such as AwareCA, AwareMO, or AwareWA.
- Calls for Service are automatically populated from CAD through integration and are not manually entered in Aware Intel Hub.
- Information entered into incidents may be shared externally after approval and publishing, so it must be accurate, clear, and appropriate.
- Users should understand when to edit the incident record versus when to add a status update.
- Approval workflows may be required before content is published, updated, unpublished, or closed.
- If a screen, button, or workflow is not visible, the user may not have permission to access it, or it may not be enabled for that agency.
- The approval process can be configured differently by agency, user, or group. Some trusted publishers may be allowed to publish without approval while other users may require review.
- System administrator training should make the groups-first permission model very clear: roles define permissions, roles are assigned to groups, and users should generally be assigned to groups rather than given one-off direct role assignments.

Instructor Run-of-Show Note

This document now uses the Detailed Training Outline as the official source of truth for training content, workflow order, and required topics. A separate quick reference outline is intentionally not included in the main program.

Once instructors are familiar with the Aware Intel Hub User Training Program, they are encouraged to create their own simplified run-of-show or delivery outline based on the class type, audience, available training environment, and agency configuration. Personal outlines are helpful for keeping the live class moving, but they should be treated as instructor aids rather than replacements for the full training program.

Training Audience and Delivery Guidance

This training program supports both general users and system administrators. Not all sections are required for every audience.

General User Training

General User Training should focus on navigation, map use, Calls for Service, Approval Requests, incident creation, incident updates, approval workflows, merging, unmerging, and closing incidents.

General users should receive full training on:

- Logging in.
- Home screen and map navigation.
- Map search, map layers, and legend.
- User Menu options that regular users may need.
- Notifications bell and pending approval notifications.
- Sidebar navigation.
- Incidents.
- Approval Requests.
- Calls for Service.
- Creating incidents from Calls for Service.
- Creating incidents manually.
- Public-facing incident fields.
- Wildfire Details.
- Emergency Alerts.
- Perimeter uploads.
- Attachments and related links.
- External System Identifiers, including the automatic CAD call number added when an incident is created from a Call for Service.
- Save versus Submit for Approval.
- Status dropdown behavior, including Not Published, Pending Approval, Published, and Published with Edits.
- Status updates.
- Edit versus status update.
- Approval Requests workflow.
- Merging and unmerging incidents.
- Unpublishing incidents.

- Closing incidents and close approval workflow.

System Administrator Training

System Administrator Training should include the full general user training content, followed by system administration topics.

System administrators should receive additional training on:

- Agencies.
- Personnel.
- Stations.
- Units.
- Users.
- Roles.
- Groups.
- Organization settings.
- Lookup Tables.
- Layer Configurations.
- Layer Groups.
- GIS Credentials.
- Aware or state-specific Portal Settings.
- Publishers and approval workflow configuration.

The system administrator portion should be delivered as guided orientation and key workflows rather than a field-by-field configuration class. Instructors should explain what each section is for, where to find it, and what major actions can be performed. Detailed field-level configuration should be referenced in the Aware Intel Hub Complete User Guide.

Training Duration

The following timeframes are recommended when planning training sessions:

- General User Training: Approximately 60 minutes, excluding Q&A.
- General User + System Administrator Training: Approximately 90 minutes, excluding Q&A.

Actual duration may vary depending on audience size, training environment, agency configuration, number of questions, and whether participants are expected to practice workflows during the session.

Instructors should plan additional time for questions and discussion at the end of each session.

Instructor Preparation

Before conducting training, instructors should prepare the training environment and materials.

Instructors should:

- Confirm whether the session is General User Training or General User + System Administrator Training.
- Confirm access to the appropriate Aware Intel Hub training or demonstration environment.
- Verify the instructor account has the permissions needed to demonstrate the required workflows.
- Confirm whether approval workflows are enabled in the training environment.
- Confirm whether sample Calls for Service are available for the Call for Service incident creation walkthrough.
- If sample Calls for Service are not available, plan to explain the CFS-to-incident workflow verbally and demonstrate manual incident creation as the hands-on example.
- Confirm whether sample incidents are available for opening, editing, merging, unmerging, and closing demonstrations.
- Confirm whether the class should use a live, staging, demo, or sandbox environment so participants understand whether public-facing activity is actually being published.
- Have the Aware Platform Overview PowerPoint ready.
- Have sample incident descriptions and status updates available for copy/paste during the walkthrough.
- Have any sample files ready if demonstrating attachments or GeoJSON perimeter upload.
- Have a sample related link available for the Related Links section.
- Know whether the audience includes approvers or system administrators.

- Be ready to explain that screens and actions may vary depending on role, permissions, agency configuration, and enabled modules.

Detailed Training Outline

Purpose

The Detailed Training Outline serves as the primary guide for delivering this training.

It provides step-by-step structure, key talking points, and guided walkthroughs to ensure consistent and thorough instruction across training sessions.

Instructors should use this outline to lead the training, demonstrate system functionality, and reinforce key concepts throughout the session.

This outline is not intended to be read verbatim. It is intended to guide instruction and ensure all critical content is consistently covered.

1. Welcome and Housekeeping Items

- Welcome participants and introduce the purpose of the training.
- Provide approximate training duration:
  - General User Training: Approximately 60 minutes, excluding Q&A.
  - General User + System Administrator Training: Approximately 90 minutes, excluding Q&A.
- Explain how questions will be handled.
- Explain that support resources will be provided at the conclusion of training.
- Reinforce that the session will begin with the Aware platform overview and then transition into a live Aware Intel Hub walkthrough.

2. Slide Deck Presentation

- Present the Aware Platform Overview PowerPoint through the Real-Time Integration Monitor slide.
- Use slide notes for guidance.
- Stop after discussing the Real-Time Integration Monitor slide.
- Explain that the presentation provides context for the public-facing Aware platform, the broader Aware ecosystem, and how integration monitoring

supports the data flowing into the Aware Intel Hub.

3. Transition to Aware Intel Hub

- Transition from the presentation to the live Aware Intel Hub environment.
- Reinforce that Aware Intel Hub is the internal operational platform.
- Reinforce that the public does not directly access Aware Intel Hub.
- Explain that approved public-facing information can be shared externally through Aware.
- Inform the audience that Aware Intel Hub is designed for CJIS, HIPAA, and FedRAMP Moderate compliance.

4. Logging In

- Direct users to the current Aware Intel Hub login URL: **intelhub.intterra.io**
- Explain that users receive an account setup email when their account is created.
- Explain that users follow the account setup link to confirm their account and create a password.
- Explain that users sign in using their email address and password or configured sign-in method.
- If users experience login issues, they should contact their system administrator or follow agency support procedures.

5. Home Screen and Live Map Overview

Explain that most users will spend the majority of their time on the Home screen, also labeled Live Map.

The Home screen is the central workspace for accessing real-time information, monitoring activity, opening incidents, and navigating the platform.

Deliver this section by walking counterclockwise around the page, beginning with the map.

Map

Explain:

- The map is the primary workspace for viewing operational activity.

- Users can view available incidents, calls for service, cameras, weather, community resources, notices or warnings, reference data, response assets, and other configured layers.
- Available layers depend on agency configuration and user permissions.

Demonstrate:

- Navigating the map.
- Zooming in and out.
- Clicking and dragging to move around the map.
- Selecting an incident icon on the map.
- Selecting View More Information from the map pop-up to open the Incident Details screen.

Key point: The map is not just a visual display. It is also a way to access operational records and incident details.

Map Search

Demonstrate the map search bar.

Explain:

- Users can search for an address.
- Users can also search by the common or proper name of a location, such as a facility, landmark, park, agency building, or other known place name.
- Users can also search for intersections by entering the street, ampersand (&), and cross-street when that is the most useful way to identify the location.
- Selecting a search result repositions the map to that location.

Map Layers and Legend

Demonstrate the Map Layers button and panel.

Explain:

- The Map Layers panel allows users to control which map layers are visible.
- The Layer tab is used to turn layers on or off.
- The Legend tab shows what map icons and symbols represent.
- Users can search layers or legend items.

- Layer categories may include incidents, calls for service, cameras, weather, community resources, notices or warnings, reference data, and response assets.

Reinforce:

- The instructor should not spend time explaining every possible layer in detail unless the agency specifically asks.
- The key skill is knowing how to find layers, turn them on or off, and use the legend to understand what is displayed.
- Cameras may be mentioned or briefly toggled on if available, but camera review is not a required workflow for General User Training.

User Menu

Move to the top-right User Menu.

Explain that the User Menu is identified by the logged-in user's name or initials and provides access to user and preference options.

Cover the following items:

- Your Profile.
- Your Organization.
- Support.
- Theme.
- Language.
- Logout.

Your Profile

Explain:

- Your Profile allows users to review information associated with their account.
- Users may be able to review details such as name, email address, phone number, assigned roles, assigned groups, multi-factor information, and account-related events.
- Depending on configuration and permissions, users may be able to update certain profile fields, such as contact information if their phone number changes.

- Depending on configuration and permissions, users may also have access to account management options, such as changing their password.

Key point: Available profile management actions vary by configuration and permissions.

Your Organization

Explain:

- Your Organization allows users to view organization information associated with their current agency or tenant.
- General users should understand where this information is located.
- Full organization management is covered during System Administrator Training.

Support

Explain:

- Support resources may be available from the User Menu.
- Full support resources are covered at the end of training.

Theme

Explain and demonstrate:

- Users can select their preferred display theme.
- Options may include System, Light, and Dark.
- This is useful for user comfort and visibility preferences.

Language

Explain:

- Users may be able to select their preferred display language.
- Available languages may vary depending on configuration.

Logout

Explain:

- Logout signs the user out of Aware Intel Hub.

- Users should log out when using shared workstations or when agency policy requires it.

Notifications Bell

Move to the notification bell in the top-right area of the screen.

Explain:

- The notification bell displays system notifications.
- A badge may appear when unread notifications are available.
- Currently, the notification bell is mainly used for pending approval activity.
- Selecting the notification bell opens the notification pop-up.
- Selecting pending approval information can take the user to the Approval Requests screen.

Key point: Approval-related notifications are one way approvers know content is waiting for review.

Agency or Instance Identifier

Move to the top-left agency or instance identifier.

Explain:

- The agency or instance identifier helps users confirm which agency environment they are currently viewing.
- This is especially important for users who may have access to more than one agency or tenant context.

Sidebar

Move to the left sidebar.

Explain:

- The sidebar provides primary navigation within Aware Intel Hub.
- The sidebar can be collapsed or expanded.
- When collapsed, the sidebar still provides navigation functionality using icons.
- Available options may vary based on user role, permissions, and configuration.

Home Button

Explain:

- The Home button returns the user to the main map screen from anywhere in the application.
- No matter where the user is in the platform, selecting Home brings the user back to the Live Map.

Incidents Sidebar Section

Explain:

- The Incidents section provides access to incidents within the system.
- The dropdown next to Incidents displays active incidents.
- Selecting an active incident from the dropdown opens that incident's Incident Details screen.
- Selecting Incidents itself opens the main Incidents screen.

Demonstrate:

- Expanding the Incidents dropdown.
- Opening an active incident from the sidebar.
- Selecting Incidents to open the main Incidents screen.

On the Incidents screen, explain:

- The screen lists incident records.
- The list can be searched and filtered.
- Selecting an incident name opens the Incident Details screen.
- Users with appropriate permissions can create a new incident from this screen.

Entities Sidebar Section

Explain:

- The Entities section provides access to additional records and data areas within the platform.
- The dropdown next to Entities currently displays Intterra-provided shortcuts, such as Agencies, Approval Requests, Units, and Calls for Service.
- In a future configuration, these shortcuts may be configurable by agency.

- Selecting Entities itself opens the full Entities area.
- The full Entities area should be used when a shortcut is not visible.

Reinforce:

- The presence or absence of an item depends on user permissions, agency configuration, and enabled modules.

Settings

Explain:

- Settings appears for users with appropriate permissions.
- Settings is used for administrative tools such as users, roles, groups, organization settings, lookup tables, layer configurations, and portal settings.
- General users only need to understand that Settings is permission-based.
- Settings workflows are covered during System Administrator Training.

6. Common Table and List Screen Tools

Before moving into the Entities walkthrough, explain that many screens in Aware Intel Hub use similar table and list tools.

Common tools may include:

- Search.
- Filters.
- Show or hide columns.
- Export or print options where available.
- Rows-per-page settings.
- Selecting a row or record name to open additional details.

Key point: Once users understand how to search, filter, and open records from one list screen, the same general approach applies to many other list screens in the platform.

7. Entities Overview and Walkthrough

Important note: For General User Training, fully cover Approval Requests, Incidents, and Calls for Service. For System Admin Training, wait to cover

entities until the System Admin Portion toward the end of the training session.

Open the Entities section.

Explain that the Entities area provides access to operational records, system-generated data, configuration records, personnel-related records, and other data areas available to the user.

Briefly introduce other Entities as permission-based or administrative areas, but do not walk those sections field-by-field during a general class.

Approval Requests

Approval Requests are fully covered as part of General User Training.

Explain:

- Approval Requests provide a centralized location for reviewing and managing content that requires approval before it is published, updated, closed, or otherwise finalized.
- Approval Requests help ensure public-facing information is reviewed before it becomes visible externally.
- Approval requirements can be configured by agency workflow. Some trusted publishers may be allowed to publish directly while others may require approval before content is released.
- Users may access Approval Requests from Entities or by selecting pending approval notifications from the notification bell.

Demonstrate:

- Open Entities.
- Select Approval Requests.
- Search or filter the approval request list if needed.
- Select an approval request to open the review pane.

Review Pane

Explain:

- The review pane appears when an approval request is selected.

- The review pane provides the approver with the information needed to review the submitted content.
- Approvers should review the request details and any related incident information before taking action.

Demonstrate:

- Review the request details.
- Open the related incident if available.
- Return to the approval request review pane.

Approving or Denying an Approval Request

Explain that approval actions depend on the request type.

For publishing requests:

- Select Approve and Publish to approve the request and publish the submitted content.
- Select Deny to reject the request.

If Deny is selected:

- A rejection box appears.
- The approver enters the rejection reason.
- The approver selects Reject.

Key points to reinforce:

- Approvers should review content carefully before approving.
- Approved content may become visible externally through Aware.
- Denial should include a clear reason so the submitter understands what needs to be corrected.
- Approval Requests also provide approval history and accountability.

Incidents

Explain:

- Selecting Incidents from Entities opens the same main Incidents screen available from the sidebar.

- Incidents are fully covered in the incident workflow portion of this training.

Calls for Service

Calls for Service are fully covered as part of General User Training.

Explain:

- Calls for Service are automatically ingested from the agency's CAD system through integration.
- Calls for Service are not created or manually entered in Aware Intel Hub.
- The Calls for Service screen displays CAD-sourced activity available to the user.
- Users may be able to filter the list to view Active Calls or Recent Calls.
- The list includes key call information, such as call ID, type, priority, status, date/time received, and location.

Demonstrate:

- Open Entities.
- Select Calls for Service.
- Review the Calls for Service screen.
- Use available filters if helpful.
- Select a CFS ID to open the Call Details screen.

Instructor note: If the training environment does not have an active CAD integration or sample CFS data, explain that Calls for Service normally come from CAD and that selecting Create Incident from the Call Details screen would carry available call information into the incident record. Then demonstrate manual incident creation so participants still see the full incident workflow.

Call Details Screen

Explain:

- The Call Details screen displays information received from CAD.
- The information is automatically populated through integration and is not intended to be manually entered or edited in Aware Intel Hub.

- The screen may include call identifiers, status, priority, call type, assigned agency, radio channel, description, location, timeline information, caller details, assigned resources, map location, and narrative/log activity.

Demonstrate:

- Review the call details.
- Review the map location if available.
- Review assigned resources and narrative/log information if available.
- Select + Create Incident when ready to begin the incident creation walkthrough.

8. Incidents Overview

Define an incident:

- An incident is a user-created event within the platform.
- Incidents are used to manage and communicate significant activity.
- Incidents can be created manually or from an existing Call for Service.
- Incidents may represent road closures, planned events, weather impacts, structure fires, wildfires, major critical incidents, or other activity that needs to be managed or shared.
- Incidents are the primary method for managing public-facing information and controlling what is submitted for approval and shared externally.

Key point: Content entered into public-facing incident fields may become visible through Aware after approval and publishing. Users should write clearly, accurately, and appropriately.

Instructor Note for CAL FIRE: For CAL FIRE personnel, incidents are automatically generated in Aware from CAL FIRE's CRM. When this applies, focus on opening, reviewing, editing, updating, and submitting those incidents rather than manually creating them.

9. Creating an Incident - Guided Walkthrough

Deliver this section as a guided, step-by-step walkthrough.

Instructors will demonstrate two methods of creating an incident:

1. Creating an incident from a Call for Service.
2. Creating an incident manually.

Both methods follow the same overall structure. The key difference is how the incident creation form is started.

Key points to reinforce before beginning:

- All fields should be reviewed for accuracy, clarity, and appropriateness before saving.
- Some information may populate automatically when creating from a Call for Service, but it still must be reviewed.
- Save creates the incident record but does not submit it for approval or publish it.
- After an incident is saved, the Incident Details screen remains open.
- The incident status displays as Not Published in the Status dropdown until it is submitted and approved.
- Submit for Approval is selected from the Status dropdown next to Not Published.
- The Review pane provides one final opportunity to review incident content before submission.
- After submission, the Status dropdown updates to Pending Approval.
- In a real incident, the initial entry can be completed quickly when users focus on the required public-facing information first and then add detail as conditions evolve.

Scenario 1 - Creating an Incident from a Call for Service

Instructor note:

- If a usable Call for Service is not available in the training environment, explain the workflow and move to Scenario 2 for the live demonstration. Do not skip the concept entirely; users should still understand that CFS creation is the preferred path when CAD data is available because it reduces manual entry.
- When an incident is created from a Call for Service, the CAD call number is automatically added to the incident after the incident is saved. This appears in the External System Identifiers section with a system type of IntelHub CAD.

Users do not need to manually enter the CAD call number.

Step 1: Navigate to the Call for Service

- From the Home screen, select Entities.
- Select Calls for Service.
- Select a Call for Service provided for training.
- Open the Call Details screen.

Explain:

- This call information came from CAD.
- The call itself is not manually entered in Aware Intel Hub.
- Creating an incident from the call allows the user to turn CAD activity into a managed incident record.

Step 2: Create the Incident

- Select **+ Create Incident** from the top-right corner of the Call Details screen.

Explain:

- This starts an incident record from the selected Call for Service.
- Available information may populate from CAD.
- The CAD call number will be added automatically to External System Identifiers after the incident is saved.
- Users must still review and complete all necessary information before saving.

Step 3: Review and Complete Incident Details

Walk through each field individually and reinforce that all information must be reviewed for accuracy, clarity, and appropriateness.

Incident Name

- The system may populate this field with information from CAD.
- Enter the incident name as designated by the incident commander, dispatch center, or agency procedure.
- Use a clear name that users and approvers can recognize.

Incident Type

- Select the appropriate type for the incident.
- If Wildfire is selected as the incident type, the Wildfire Details section appears later in the incident form.

Incident Status

Explain that the incident status indicates the current state of the incident.

Available statuses include:

- 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 enter the current date and time.
- When creating from a Call for Service, this information may populate automatically and should still be reviewed.

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 enter the current date and time.
- Leave this blank for active incidents unless agency procedure requires otherwise.

Agencies Having Jurisdiction

- Select the agency or agencies responsible for the incident.
- Multiple agencies can be selected.

- Selecting more than one agency changes the incident from a single-agency event to a Unified Command event.
- In a Unified Command event, participating agencies can access, edit, and provide status updates to the incident.
- Incidents not initially created under Unified Command can be updated later to add additional agencies and transition to a Unified Command event.

Key point: Agencies Having Jurisdiction affects who can participate in the incident workflow, so users should select agencies carefully.

Incident Management Team

- Select the appropriate incident management team from the dropdown.
- Do not go into configuration of the dropdown during General User Training.
- Configuration of supporting lookup values is covered during System Administrator Training when applicable.

Incident Description

- Enter a clear summary of the incident based on currently available information.
- The description can be updated as new information becomes available, but new developments should generally be communicated using Status Updates.
- Information entered in the Incident Description field can be included in public-facing incident information after the incident is approved and published.
- Users should review this content carefully before submitting the incident for approval.

Sample incident description:

A working structure fire has been reported at a large commercial warehouse, with heavy smoke and visible flames coming from the central loading area. Fire crews arrived on scene to find fire extending through stored materials inside the building, creating challenging conditions due to high heat and limited visibility. Multiple agencies are assisting with fire suppression, traffic control, and scene safety. Nearby businesses have been advised to avoid the area as crews work to contain the fire and prevent further spread. There are no confirmed injuries at this time, and the cause of the fire remains under investigation.

Incident Location

- Select Address or Coordinates for the incident location.
- When Address is selected, users can search for the address and complete available address fields.
- The address search can also be used for intersections by entering the street, ampersand (&), and cross-street when appropriate.
- When Coordinates is selected, users can enter latitude and longitude values.
- Confirm that the incident location is accurate before saving.

Location Description

- Enter additional details to help describe the location.
- This may include landmarks, directions, facility names, park names, neighborhood names, or other helpful descriptions.

Counties

- Select one or more counties associated with the incident.
- Multiple counties can be selected when applicable.

Wildfire Details

Explain:

- If Wildfire is selected as the Incident Type, the Wildfire Details section appears.
- These fields can be updated throughout the lifecycle of the incident as conditions change.
- Containment and control information may not be known when the incident is first created.

Fields include:

- 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 containment percentage, 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.

Key point: Users should return to the incident and update wildfire details as information changes.

Emergency Alerts

Explain:

- The Emergency Alerts section allows users to add public-facing evacuation information to an incident.
- Emergency alerts can be added during incident creation or later by editing an existing incident.
- Emergency alerts appear in the Aware public-facing app after the incident is approved and published.
- When a user opens an incident containing an emergency alert in the app, a View Evacuation Information button appears below the incident title.
- Selecting the button displays the evacuation type followed by the description entered for that alert.

To add an emergency alert:

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

Key points:

- Do not skip this section during General User Training. Emergency Alerts are public-facing and high-impact, even if the sample incident does not require a real evacuation.
- Emergency alert descriptions are public-facing and must be accurate, clear, and appropriate.
- Emergency alerts can be added later by opening the incident, selecting Edit, adding the alert information, saving the incident, and submitting it for approval again if approval is required.

- When editing an already published incident, notifications are only generated for emergency alerts with evacuation types of Evacuation Warning or Evacuation Order.
- If evacuation information changes over time, users should make the appropriate incident edit and should also consider whether a status update is needed to provide a clear public timeline.

Map

- The map displays the incident location based on the provided address or coordinates.
- Users should visually confirm that the displayed location is correct before saving.

Perimeter

Explain:

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

To add a perimeter file:

1. Locate the Perimeter section.
2. Drag and drop a GeoJSON file into the upload box, or select the upload box to browse for the file.
3. Confirm the correct file has been selected.
4. Continue reviewing the incident before saving.

Key point: Users should verify that the perimeter file is accurate and appropriate before submitting the incident for approval.

Attachments

Explain:

- Attachments can be added to an incident after the incident has been saved.
- Attachments cannot be added during the initial incident creation process before the incident record has been saved.
- Attachments can include common documents, images, videos, and related files.
- The full list of supported attachment file types is available in the Aware Intel Hub Complete User Guide.

Related Links

Explain:

- Related links allow users to add external links relevant to the incident.
- These can include community resources, trusted partner links, or other sources that provide additional context and information.
- In the current workflow, related links are added from the View Links section.

To add a related link:

1. Locate the View Links section.
2. Select the plus icon.
3. Enter the Link Name.
4. Enter the Link URL.
5. Select Save.

Sample related link:

California Resource Locator: https://locator.lacounty.gov/

Explain:

- When more than one related link has been added, 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.
- Reordering is useful when more important links should appear at the top.

External System Identifiers

Explain:

- External System Identifiers can be used to associate the incident with a matching record from another system.

- This section is optional and is not required to create or save an incident.
- If an incident is created from a Call for Service, the CAD call number is automatically added to the External System Identifiers section after the incident is saved.
- Automatically added CAD call numbers appear with a system type of IntelHub CAD.
- Users do not need to manually enter the CAD call number when creating an incident from a Call for Service.
- Additional external system identifiers can be added manually when needed, such as an IRWIN ID or another configured external system identifier.

To add an external system identifier manually:

1. Locate the External System Identifiers section.
2. Select the plus sign next to External System Identifiers.
3. In the Add Identifier window, select the appropriate system from the System dropdown.
4. Enter the corresponding identifier in the ID field.
5. Select Save.
6. Continue with saving or updating the incident.

Key point: External System Identifiers may be added automatically from integrated systems or manually by the user. Users should verify manually entered identifiers carefully before saving.

Step 4: Final Review Before Saving

Before selecting Save, reinforce:

- Review all fields for accuracy.
- Confirm the information is clear and appropriate.
- Confirm the location is correct.
- Confirm emergency alerts are correct, if used.
- Confirm any perimeter file is accurate, if used.
- Confirm related links are correct.
- Confirm any manually entered external system identifier is correct, if used. If the incident was created from a Call for Service, remind users that the CAD call number will be added automatically after the incident is saved.

- Remember that public-facing information may become visible through Aware after approval and publishing.

Key point: Save creates the incident record but does not submit the incident for approval and does not publish it to the public-facing platform.

Step 5: Save the Incident

- Select Save at the bottom-right corner of the screen.

Explain:

- The incident is now saved in the system.
- If the incident was created from a Call for Service, the CAD call number is automatically added to the External System Identifiers section with a system type of IntelHub CAD.
- The incident has not been submitted for approval yet.
- The incident has not been published externally.
- 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.

Step 6: Add Attachments

To add attachments after saving:

7. Select Edit at the top right of the screen.
8. Locate the Attachments section.
9. Select the plus sign next to Attachments to open the Add Attachments window.
10. Browse for a file or drag and drop the file into the upload area.
11. Review the selected file.
12. Select Add Files.
13. Save the incident changes.

Key points:

- If the incident has already been submitted for approval or published, adding attachments can trigger the approval process again.

- Users should review attachments carefully before submitting updated content for approval.

Step 7: Submit the Incident for Approval

To submit the incident for approval:

1. Select the Status dropdown next to Not Published.
2. Select Submit for Approval.
3. Review all incident content carefully 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.

Explain:

- Selecting Submit for Approval from the Review pane triggers the approval process.
- After submission, the Status dropdown at the top-right corner of the Incident Details screen updates to Pending Approval.
- The incident is not published to the Aware Portal until the approval request is approved.

Step 8: Add a Status Update

Explain:

- Status Updates are used to communicate new or evolving information after an incident has been created.
- Status Updates provide a chronological record of changes, progress, and key developments.
- Status Updates should be used for new information, not to replace the original incident description every time something changes.

To add a status update:

1. Open the desired incident.
2. Scroll to the Status Updates section.
3. Select + New Status Update.
4. In the New Status Update window, select the appropriate Category.
5. Use Pin to Top if the update should remain at the top of the list.
6. Enter the update content.

7. Add relevant images or videos if appropriate.
8. Select Approve and Publish at the bottom-right corner of the New Status Update window.

Sample status update:

Fire crews have made significant progress containing the warehouse fire, with the majority of flames knocked down and hotspots still being addressed. Units remain on scene conducting overhaul operations and monitoring for rekindles. Traffic restrictions are still in place in the immediate area, and the cause of the fire is under investigation. No injuries have been reported at this time.

Reinforce:

- Selecting Approve and Publish does not always immediately publish the status update.
- If an approval process is configured, the status update is submitted for approval and displays as Pending Approval in the Status Updates section.
- The status update is not published to the Aware Portal until it is approved.
- Published status updates remain available for the public to review as part of the incident timeline.
- Pin to Top can be used when one update should stay above the others, such as an important evacuation or all-clear message.
- Updates should be used for new or evolving information.
- Corrections to the core incident record should be handled by editing the incident.

Scenario 2 - Creating an Incident Manually

Explain:

- Create an incident manually when no Call for Service exists or when starting from a blank incident entry is desired.

Step 1: Create a New Incident

- From the sidebar, select Incidents.
- Select **+ Create Incident**.

Step 2: Complete Incident Details

Walk through the same fields covered in Scenario 1:

- Incident Name.
- Incident Type.
- Incident Status.
- Incident Start Date/Time.
- Incident End Date/Time.
- Agencies Having Jurisdiction.
- Incident Management Team.
- Incident Description.
- Incident Location.
- Location Description.
- Counties.
- Wildfire Details, if applicable.
- Emergency Alerts, if applicable.
- Map.
- Perimeter, if applicable.
- Attachments, after the incident has been saved.
- Related Links / View Links.
- External System Identifiers, if applicable. For manually created incidents, external identifiers must be added manually when needed.

Sample manual incident content:

Incident Name: Prescribed Burn - Topanga State Park

Incident Description: A prescribed burn is currently underway in a designated area to reduce excess vegetation and lower the risk of future wildfires. Fire personnel are on scene managing the operation, which is being conducted under controlled conditions with established containment lines and continuous monitoring. Residents in the surrounding area may notice smoke, but this is expected and part of the planned operation. No structures are threatened, and the burn is being conducted in coordination with local agencies.

Incident Location: 20828 Entrada Rd, Topanga, CA 90290

Location Description: Topanga State Park

Step 3: Final Review Before Saving

Reinforce:

- Review all information carefully.
- Ensure clarity and accuracy.
- Confirm that public-facing content is appropriate.
- Confirm the incident location and any map/perimeter information.
- Confirm related links, manually entered external identifiers, and emergency alerts if used.

Step 4: Save the Incident

- Select Save at the bottom-right corner of the screen.

Explain:

- Save creates the incident record.
- Save does not submit the incident for approval.
- Save does not publish the incident externally.
- After saving, the incident remains open on the Incident Details screen with a Not Published status in the Status dropdown.

Step 5: Add Attachments

To add attachments after saving:

1. Select Edit at the top right of the screen.
2. Locate the Attachments section.
3. Select the plus sign next to Attachments to open the Add Attachments window.
4. Browse for a file or drag and drop the file into the upload area.
5. Review the selected file.
6. Select Add Files.
7. Save the incident changes.

Step 6: Submit for Approval

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

4. Select Submit for Approval at the bottom-right corner of the Review pane when the incident is ready for review.

Explain:

- After the incident is submitted, the Status dropdown updates to Pending Approval.
- The same approval workflow applies to manually created incidents.
- Content is not visible externally until approved and published when approval is required.

Optional: Add a Status Update

Sample status update:

The prescribed burn is progressing as planned, with crews successfully maintaining control within the designated boundaries. Smoke conditions may vary as the burn continues, but no issues have been reported. Personnel will remain on scene to monitor and secure the area until operations are complete.

10. Saving, Submitting, and Canceling Approval Requests

Explain the difference between saving and submitting.

Save

- Save creates or updates the incident record.
- Save does not submit the incident for approval.
- Save does not publish the incident externally.
- After a new incident is saved, the Incident Details screen remains open and the Status dropdown displays Not Published.

Submit for Approval

- Submit for Approval begins the approval process.
- To submit a new incident for approval, select the Status dropdown next to Not Published, then select Submit for Approval.
- The Review pane opens so the user can review all incident content carefully.
- Selecting Submit for Approval at the bottom-right corner of the Review pane submits the request.

Pending Approval

Explain:

- After submission, the Status dropdown updates to Pending Approval.
- The content is not published externally until approved.
- Approvers may be notified by email and through the notification bell.

Cancel Approval Request

Explain:

- If an incident has been submitted for approval but needs to be changed before approval is completed, users may be able to cancel the pending approval request.

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.

11. Approval Requests Workflow

Approval Requests were introduced during the Entities walkthrough, but this section reinforces the full approval workflow in context.

Explain:

- Depending on agency configuration, incidents, status updates, edits, publishing actions, unpublishing actions, and closing actions can require approval.
- Approval Requests can be accessed from Entities.
- Approval Requests can also be accessed from notification bell activity when pending approvals are available.
- Approvers may also receive email notifications with links to the approval screen if email notifications are configured.

- Approvers can review approval requests from the Approval Requests screen or from the related Incident Details screen when available.

Reviewing an Approval Request from the Notification Bell or Approval Requests Screen

To review an approval request:

1. Select the notification bell at the top of the screen, then select View Approval Requests, or open Approval Requests from Entities.
2. Locate the approval request.
3. Select the request to open the review pane.
4. Review the request details and submitted content.
5. Open the related incident if available and helpful.
6. Return to the review pane to take action.

Reviewing an Approval Request from the Incident Details Screen

To review a publish request from the related incident:

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. Review the incident content carefully.
5. Take the appropriate approval action.

Approving or Denying a Publish Request

For publishing requests:

- Select Approve and Publish to approve the request and publish the submitted content to the Aware Portal.
- Select Deny to reject the request.

If denying a request:

- Enter a clear rejection reason in the Reject Request window.
- Submit the rejection.

If approving a request:

- Confirm the approval and publish action when prompted.
- After approval, the Incident Details screen displays Published at the top-right corner, along with the Merge Incident and Edit buttons.

Approval History

Explain:

- Approval Requests also provide a record of approval activity.
- Users may be able to review what content was submitted, whether it was approved or rejected, when the request was processed, and who was involved in the approval process.

Edited Published Content

Explain:

- If an incident has not been published, edits are saved directly to the incident record.
- If an 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 options to View Pending Changes, Submit for Approval, or Revert to Last Published.
- When reviewing edited content, approvers may see the published version alongside the pending edited version.
- Removed or changed content may appear with strikethrough formatting, while updated content appears in the pending version.
- This helps approvers quickly understand what changed before approving or denying the edit.

Unpublishing an Incident

Explain:

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

- To unpublish an incident, open the published incident, select Published at the top-right corner of the Incident Details screen, then select Unpublish in the confirmation window.
- Selecting Unpublish submits the unpublish request for approval.
- While the unpublish request is pending, the Incident Details screen displays Pending Approval at the top-right corner.

To review an unpublish request:

1. Open the approval request from the notification bell, email notification, 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.
4. If the incident should remain published, select Reject Unpublish and enter the reason for rejection.

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

12. Opening Existing Incidents

Explain that existing incidents can be opened in multiple ways.

Demonstrate:

- From the map: Select an incident icon, then select View More Information.
- From the sidebar: Expand Incidents, then 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 Entities: Select Entities, then Incidents, then open the incident from the list.

Key point: The Incident Details screen is where users review, update, submit, merge, unmerge, unpublish, or close incidents depending on permissions and status.

13. Editing Incidents

Explain:

- Editing an incident is used to correct or update the core incident record.
- Edits can be made when information needs to be corrected, completed, or updated.
- For ongoing updates or new developments, users should usually add a Status Update instead of repeatedly changing 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.
5. If the incident was already published, remember to submit the edits for approval to publish the edits.

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 currently published version remains visible on the Aware Portal until the edits are submitted, approved, and published.
- The Published with Edits dropdown provides options to View Pending Changes, Submit for Approval, and 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.
4. Review the Pending Changes pane.

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.

Explain:

- 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.

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.

Key point: Reverting changes restores the incident record to the last published version and removes the unpublished edits.

14. Edit Versus Status Update - Critical Concept

This is one of the most important concepts to reinforce.

Edit the incident when:

- Correcting inaccurate information.
- Completing missing core incident details.
- Updating the incident status.
- Updating wildfire-specific fields such as acreage, containment percentage, containment date/time, or control date/time.

- Updating location, counties, agencies, related links, attachments, emergency alerts, manually entered external identifiers, or other core incident details.

Use a Status Update when:

- Communicating new or evolving information.
- Providing progress updates.
- Sharing changes in conditions.
- Sharing updated public instructions.
- Providing road closure changes.
- Sharing evacuation information updates.
- Providing containment or control updates as a public message.
- Adding chronological incident communication.

Simple rule:

- Edit fixes or updates the core record.
- Status Update communicates what changed or what people need to know next.

15. Merging and Unmerging Incidents

Merging and unmerging incidents are fully covered in General User Training.

Explain:

- 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.
- Merge and Join closes and merges the current incident's data into an existing Unified Command incident.
- The selected incident remains active as the primary incident record.
- Merging an incident does not require a separate approval process.

Merging an Incident

To merge an incident:

1. Open the Incident Details screen for the incident that needs to be merged.
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.

5. Explain that incidents are listed by distance, with the closest incidents shown first.
6. Select the incident to merge into.
7. Select Continue.
8. Review the Confirm Merge screen.
9. Confirm that the correct incidents are being merged.
10. Select Confirm Merge to complete the merge.

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

Key points:

- Users should verify the correct target incident before confirming the merge.
- 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 affects incident organization and visibility, so users should be careful before confirming.

Merged Incidents Box

Explain:

- 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 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 includes an Unmerge button for each merged incident listed.

Unmerging an Incident

Explain:

- An incident can be unmerged from the incident it was previously merged into.
- There are two ways to unmerge an incident.

To unmerge from the Merged Incidents box:

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.

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.
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.

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

16. Closing Incidents

Closing incidents is fully covered in General User Training.

Explain:

- Users with appropriate permissions can request to close an incident.
- Closing an incident may require approval depending on agency configuration.
- While the close request is pending, the incident remains open.

Submitting an Incident for Closing

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.
5. Confirm the request if prompted.

Explain:

- After the close request is submitted, approvers are notified by email or through the notification bell.
- While the close request is pending, the incident remains open.

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.

Explain:

- 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.

To approve or reject a close request:

1. Open the close request from Approval Requests, email notification, 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:

- Enter a rejection reason.
- The user who submitted the close request is 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.

Key point: After the close request is approved, the incident status updates to Closed.

17. System Administrator Training

System Administrator Training should be delivered after the General User Training content.

This section should be taught as guided orientation and key workflows. The goal is to show administrators where the major areas live, what they are used for, and what actions are available. Do not walk every field on every tab unless the audience specifically asks or the agency needs that level of detail.

Use this practical teaching rule:

- Explain what the section is for.
- Show where it is located.
- Show how to search or open a record.
- Show where add, edit, delete, manage, or configure actions are located.
- Explain any major caution or workflow impact.
- Move on.

System Admin Entities Walkthrough

For system administrator training, walk through the Entities area in the same live order used earlier:

1. Agencies.
2. Approval Requests.
3. Lookup Tables.
4. Personnel.
5. Stations.

6. Units.
7. Users.
8. Layer Configurations.
9. Layer Groups.
10. GIS Credentials.
11. Incidents.
12. Calls for Service.

Because several of these areas are also available from Settings, explain that some items have more than one access path. If the section was already explained under Entities, do not repeat the full explanation again under Settings unless the audience needs it.

Agencies

Explain:

- Agencies represent organizations or departments that may participate in incidents, workflows, or permissions.
- Personnel who need to contribute to the public-facing Aware platform must be assigned to an agency.
- Agencies can represent the customer's primary agency.
- Agencies can represent mutual aid agencies that may respond to that agency's incidents.
- Agencies can represent departments or sub-agencies within a larger customer, such as Fire, Police, Public Works, Water, or other municipal departments.
- This structure helps support department-specific permissions, incident participation, and access.

Demonstrate at a high level:

- Open Entities.
- Select Agencies.
- Search for an agency.
- Open an agency record.
- Show where to add an agency.
- Show where Edit and Delete are located if the instructor account has access.
- Mention the public visibility toggle only as needed for mutual aid visibility.

Approval Requests

Explain:

- Approval Requests were covered in General User Training and remain important for system administrators.
- This screen shows requests that require review before public-facing content is published, edited, unpublished, or closed.
- Approval requests can also be reached from the notification bell when pending approvals exist.

Demonstrate briefly:

- Open Approval Requests.
- Search or filter if needed.
- Open a pending request when available.
- Show the review pane and available actions.

Key point: The approval workflow itself is configured later in Aware Portal Settings.

Lookup Tables

Explain:

- Lookup Tables are where shared reference values are managed.
- Lookup tables allow agency-specific values to be mapped or maintained so information displays consistently.
- Technical users or administrators may use this area when values need to be added or corrected.

Demonstrate at a high level:

- Open Lookup Tables.
- Open a category.
- Show where entries are added, edited, or deleted.
- Explain that incorrect mappings can cause data to display incorrectly.

Personnel

Explain:

- Personnel records represent people who may be assigned, tracked, or referenced in the platform.
- Personnel are not necessarily users.
- A user is someone who signs in to Aware Intel Hub.
- A personnel record can be linked to a user profile when the person also has login access.
- Personnel may be populated manually or through staffing-related integrations depending on agency configuration.

Demonstrate at a high level:

- Open Personnel.
- Search for a person.
- Open a personnel record.
- Show where Add Personnel is located.
- Show the Search and Link User Profile option.
- Show where edit actions are located.

Stations

Explain:

- Stations represent physical station locations or operational facilities.
- Stations can support location awareness, staffing awareness, and unit assignment.
- Stations can be added individually or through bulk upload.

Demonstrate at a high level:

- Open Stations.
- Search for a station.
- Open a station record.
- Show Add New Station.
- Show Add Bulk Stations and explain that a CSV template and review step are available.
- Show where edit actions are located.

Units

Explain:

- Units are trackable vehicles, apparatus, or other trackable items.
- Units may include engines, ambulances, command vehicles, patrol vehicles, portable radios, specialized equipment, or other GPS-enabled assets.
- Unit information may be populated through CAD or other integrations.

Demonstrate at a high level:

- Open Units.
- Search for a unit.
- Open a unit record if available.
- Show Add New Unit.
- Explain that unit identity, capability, station assignment, personnel assignment, and tracking behavior may be managed here depending on configuration.

Users

Explain:

- Users are people who can sign in to Aware Intel Hub.
- User records control account access, roles, groups, login restrictions, multi-factor authentication, and activity history.
- This screen is similar to the user's own profile, but administrators may have management actions for other users.

Demonstrate at a high level:

- Open Users.
- Search for a user.
- Open a User Details screen.
- Show the Manage menu.
- Mention available actions such as Edit User, Send Password Reset, Require Password Change, Disable User, and Delete User.
- Explain that deleting a user does not remove incidents or other records the user previously created.

Key point: Assign users to groups whenever possible instead of assigning roles directly to individual users.

Layer Configurations

Explain:

- Layer Configurations are where GIS-managed layers are connected and controlled.
- This is mainly for GIS or technical administrators.
- Layer configuration affects how data appears on the map.

Demonstrate at a high level:

- Open Layer Configurations.
- Search for a layer configuration.
- Open a layer configuration.
- Point out major tabs such as Display Settings, Child Layers, Capabilities, Fields, Label Configuration, and Advanced.
- Show where create, edit, and delete actions are located if available.

Key point: Do not teach this as a GIS configuration class during general system admin training unless GIS staff specifically need it.

Layer Groups

Explain:

- Layer Groups organize related layer configurations into groups.
- They help make map layers easier to manage and present.

Demonstrate briefly:

- Open Layer Groups.
- Search for a layer group.
- Open a group if available.
- Show where Create Layer Group, Edit Layer Group, and Delete Layer Group are located.

GIS Credentials

Explain:

- GIS Credentials store authentication information used to connect to secured GIS services.

- These credentials may be used by layer configurations or other GIS-related functionality.

Demonstrate briefly:

- Open GIS Credentials.
- Search for a credential.
- Show where Create Credential is located.
- Explain the difference between credential details and credential secret information at a high level.

Key point: GIS credentials should be managed carefully because they control access to secured GIS services.

Incidents

Explain:

- Incidents under Entities is another path to the same Incidents screen already covered during General User Training.
- Do not repeat the full incident workflow here unless the audience asks.

Calls for Service

Explain:

- Calls for Service under Entities is the same CFS workflow already covered during General User Training.
- Calls are CAD-sourced and are not manually entered in Aware Intel Hub.
- If CAD is not connected in the demo environment, explain what would normally appear and move on.

Settings Overview

Explain:

- Settings appears for users with appropriate permissions.
- Settings contains Access Management and System Configuration tools.
- Some settings screens duplicate access to areas already introduced under Entities.

- When a section has already been covered, acknowledge it as a second access path and move quickly unless there are questions.

Settings may include:

- Users.
- Roles.
- Groups.
- Organization.
- Lookup Tables.
- Layer Configurations.
- Aware or state-specific Portal Settings.

Users, Roles, and Groups

This is the most important access-management concept to reinforce during system administrator training.

Explain:

- Permissions are assigned to roles.
- Roles should generally be assigned to groups.
- Users should generally be assigned to groups.
- Direct role assignment to individual users is possible, but it is harder to manage long-term and can create one-off permission problems.

Users:

- Show the User Management screen.
- Open a user record.
- Show the Manage menu.
- Mention edit, password reset, required password change, disable, and delete options.
- Briefly show Roles, Groups, Login Restrictions, Multi-Factor, and Events tabs.

Roles:

- Show the Roles screen.
- Explain that roles are generally review-only during training.
- Open a role and show that roles contain permissions.

- Reinforce that roles should usually be assigned to groups.

Groups:

- Show the Groups screen.
- Open or create a group if appropriate.
- Explain that groups can contain assigned roles and assigned users.
- Show where to add users to a group and where to assign roles to a group.

Key point: The cleanest model is roles to groups, users to groups. It keeps permissions easier to maintain as agencies grow.

Organization

Explain:

- Organization settings manage organization profile information, security policy settings, SSO, terms and conditions, and organization event history.
- This section affects organization-level behavior, so changes should be made carefully.

Demonstrate at a high level:

- Open Organization.
- Review organization information.
- Point out password policy, login policy, and MFA policy settings.
- Point out SSO settings and explain that incorrect SSO configuration can prevent users from signing in.
- Point out Terms & Conditions for agencies that require login notices or policy acknowledgements.
- Point out Events for organization-related activity history.

Lookup Tables and Layer Configurations

Explain:

- These are also available through Entities and may already have been introduced.
- Lookup Tables manage reference values and mappings.
- Layer Configurations manage GIS layer connections and display behavior.

Demonstrate only as needed:

- Show where each section is located in Settings.
- Explain that detailed lookup and GIS configuration should be handled by users who understand the operational impact.

Aware or State-Specific Portal Settings

This is the most important System Configuration section for public-facing Aware publishing.

Explain:

- Aware Portal Settings manage whether the public-facing module is enabled, who can publish, and whether approval is required.
- Depending on the deployment, this may be labeled with the state abbreviation, such as AwareCA Portal Settings, AwareMO Portal Settings, or AwareWA Portal Settings.

Module Status

Explain:

- Module Status controls whether the public-facing Aware module is enabled for the agency.

Publishers

Explain:

- Publishers define who can publish to the public-facing Aware platform.
- Publishers can be individual users or groups.
- Groups are recommended whenever possible because they are easier to maintain.

Demonstrate:

- Open Manage Publishers.
- Show where users or groups can be added.
- Show where publishers can be removed.

Approval Workflow

Explain:

- Approval Workflow controls whether public-facing content requires approval.
- No Approval Required means content publishes immediately without review.
- Single Stage Approval means selected users or groups must approve content before it is published.
- Approvers can be individual users or groups, but groups are usually recommended.

Demonstrate:

- Open the Approval Workflow configuration.
- Show No Approval Required.
- Show Single Stage Approval.
- Show where approver users or groups are selected.
- Explain that a dedicated approvers group is often cleaner than adding individual approvers one by one.

Key point:

- This section answers two critical questions: who can publish, and who must approve? Changes here directly affect public-facing publishing behavior.

18. Training Conclusion, Support, and Resources

Transition back to the final slide of the presentation if applicable.

Review the available support resources with participants. Explain that emergency support and non-emergency support are handled differently, and that the correct support path helps Intterra respond appropriately.

Aware Intel Hub Link

intelhub.intterra.io

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 Numbers:

- 1-888-826-6005
- 1-512-823-0355

These numbers connect directly to Intterra's on-call support team and are 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, users should use one of the standard support methods listed below.

Non-Emergency Support

Customer Support Website

Intterra Help Center

Use the Customer Support Website to submit support requests, request account changes, suggest product improvements, or make general inquiries.

This is the recommended method for submitting non-emergency support requests because it allows users to track request status and receive updates.

Email Support Requests

Support@Intterragroup.com

Users may also submit a support request by email. Emails sent to this address automatically generate a support ticket. However, this method does not provide the same request tracking or status update features as the Customer Support Website.

When submitting a request by email, users should include their name, agency name, and any relevant details to help Intterra assist them more efficiently.

Additional Resources

Product Knowledge Base

Service Management Knowledge Base

The Product Knowledge Base provides access to step-by-step guides, training videos, and detailed documentation. Instructors should remind trainees that the Aware Intel Hub Complete User Guide and other reference materials are available through the knowledge base.

General Product Questions

Questions@Intterragroup.com

Use this email address for questions about system functionality, workflows, or general use of the platform.

Intterra Academy

AwareCA Training Schedule - Intterra Academy

Intterra Academy may be used to list upcoming training opportunities and provide training sign-up links. Availability and naming may vary depending on current training offerings. Participants may take the training again if they want a refresher after they have spent more time in the platform.

New Feature Requests

New ideas or enhancement requests can be submitted through the Customer Support Website. Users should select Suggest a Product Improvement and complete the form. Once submitted, the request is routed to Product Management for review. The team will evaluate the idea and may reach out with additional questions or requests for clarification if needed. The following link can be used to submit new feature requests:

https://intterragroup.atlassian.net/servicedesk/customer/portals

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

Key point:

- Instructors should ensure trainees understand where to go for emergency support, where to submit non-emergency support requests, where to ask general product questions, and where public app users can find support from within the mobile app.

19. Question and Answer Session

- Allow time for participant questions.
- Clarify workflows that may vary by agency configuration.
- Reinforce where users can find the Complete User Guide and Quick Start Guide.
- Encourage users to practice workflows in the appropriate training or agency environment.

20. Post-Training Expectations

Upon completion of General User Training, users should be able to:

- Sign in to Aware Intel Hub.
- Navigate the Home screen and Live Map.
- Search the map by address or common location name.
- Use map layers and the legend.
- Open incident details from the map.
- Use the User Menu for profile review, theme selection, language selection, support access, and logout.
- Understand the notification bell and pending approval notifications.
- Understand the agency or instance identifier.
- Use the sidebar, Home button, Incidents section, and Entities section.
- Open and review Calls for Service.
- Understand that Calls for Service come from CAD and are not manually entered.
- Create incidents from Calls for Service.
- Understand that incidents created from Calls for Service automatically receive the CAD call number in External System Identifiers after the incident is saved.

- Create incidents manually.
- Complete public-facing incident fields accurately and appropriately.
- Add wildfire details when applicable.
- Add emergency alerts when applicable.
- Add GeoJSON perimeter files when applicable.
- Add attachments after an incident has been saved.
- Add and reorder related links.
- Save incidents and submit them for approval.
- Add status updates.
- Understand the difference between editing an incident and adding a status update.
- Review and act on approval requests when authorized.
- Merge and unmerge incidents.
- Submit incidents for closing and understand close approval workflows.

Upon completion of System Administrator Training, system administrators should be able to:

- Understand the purpose of Agencies, Personnel, Stations, Units, Layer Groups, and GIS Credentials.
- Understand that personnel who need to contribute to the public-facing Aware platform must be assigned to an agency.
- Understand the distinction between users and personnel.
- Link personnel records to user profiles when applicable.
- Manage users, roles, and groups at a practical level.
- Apply the groups-first permission model.
- Understand organization settings, including password, login, MFA, SSO, terms and conditions, and events.
- Manage lookup tables at a practical level.
- Understand layer configurations and how they affect map behavior.
- Understand state-specific Aware Portal Settings.
- Manage publishers and approval workflow configuration.

Agencies are encouraged to reinforce training through continued use, internal practice, and reference to the Aware Intel Hub Complete User Guide.

POWERED BY:

INTTERRA