Axon Standards User Guide

Rev: 05 Nov 2026

Axon Enterprise, Inc.
17800 N 85th St
Scottsdale AZ 85255
USA

, AXON, Axon Evidence, Axon Records, Axon Standards, Draft One, and TASER are trademarks of Axon Enterprise, Inc., some of which are registered in the U.S. and other countries. For more information, visit www.axon.com/legal. All other trademarks are property of their respective owners.

All rights reserved. ©2026 Axon Enterprise, Inc.

Contents

What's new **1**

Axon Standards **2**

Sign in 2

Automatic sign out 4

Basic navigation 4

Report, task, and event management **5**

Task inboxes 7

Create and submit reports 13

Create reports 13

Submit reports 14

Create events from Axon Records 15

Review, revise, and finalize reports 16

Review reports 16

Revise reports 17

Revert finalized reports 17

Report Writer 17

Add report information 26

Overview 27

Citizen 29

Vehicles 33

Units 37

Officers 37

Response actions 38

Narratives 39

Files 42

Assign and reassign tasks and authors 43

Event and case profiles 46

Event profiles 46

Case profiles 48

Additional actions 50

Print reports 50

Print events, cases, and investigations 51

Link reports to an incident or event 52

Link incidents and events 54

View report history 54

Copy information to new reports 54

Share reports 55

Restrictions **58**
Restrict events 58
Partial restrictions 59
Edit and remove restrictions 62
Manage restriction exceptions 63

Redaction **65**
Redact incidents and cases before sharing or printing 65
Redact reports when printing 65
Redact citizen profiles when printing 66
Use the Redaction tool 66
Redact text using search 67
Manually redact content 67
Add text annotations 68
Move or delete redactions 68
Preview redactions 68
Export the redacted PDF 68
Audit log 69

Search **70**
Saved searches 70
Search by date 71
Search results 72
Search tabs 72
Map view 73
Filters 74
Events 75
Officers 75
Citizens 75
Vehicles 76
Export search results 77
Search tips and tricks 78
Search customizations 82

Profiles **90**
Officer profiles 91
Citizen profiles 92
Vehicle profiles 92
Profile actions 93
Manage flags 94
Print profiles 96

Manage profile photos ... 97
Citizen profile actions ... 100
Edit profile ... 101
View history ... 101

GIS and maps ... 102
Feature layers ... 105
Common names ... 108

Case and investigation management ... 111
Configuration options ... 112
Inboxes ... 113
Detail view ... 115
List view ... 116
Cases and investigations ... 117
Cases ... 118
Investigations ... 125
Case and investigation tasks ... 128
Case and investigation documentation ... 135
Summary ... 136
Case and investigation documents ... 137
Custom names ... 138
Evidence and file management ... 140
Activity log management ... 147
Disposition and review ... 148
Share evidence and cases ... 151
Advanced sharing ... 152

Analytics ... 164
Out of the box dashboards ... 164
Complaints (Internal/Citizen) ... 164
Early Intervention System (EIS) ... 165
Report Productivity ... 165
Use of Force / Response to Resistance ... 166
Vehicle Collision ... 166
Vehicle Pursuits ... 167
General functionality ... 167
Export dashboards ... 170
Manage subscriptions ... 170
Dashboard management ... 171
Create dashboards ... 172

Edit dashboards ... 173
Save dashboards ... 176
Delete and archive dashboards ... 177
View dashboard activity logs ... 177

Early Intervention System (EIS) ... 178
Alerts and reports ... 178
Alert inboxes ... 178
Alert management ... 179
View alert summary ... 180
Assign alert ... 181
Edit alert status ... 181
Manage the activity log ... 184
Early Intervention (EI) Dashboard ... 184

Personnel ... 187
Homepage ... 187
My profile ... 188
Update profile ... 189
Update Demographics information ... 189
Related reports ... 190
Audit log ... 190

Training ... 192
My Courses ... 193
My Team ... 195
Manage curricula ... 196
Create curricula ... 197
Update curricula ... 200
Mark curricula as inactive ... 201
Restore curricula ... 201
Manage courses ... 202
Create courses ... 204
Update courses ... 206
Enroll learners in courses ... 207
Take attendance for courses ... 209
Record scores and finalize courses ... 211
Export learning records ... 213
Cancel courses ... 214

Notification Center ... 216
Notification types ... 216
Rejected reports ... 217

Reports that have changed state ... 217
Reports that require attention ... 217
Shared reports ... 217
Weekly team digest ... 217
Warrant status updated ... 217

Administrator Console ... 219
Analytics ... 219
Announcement Banner Update ... 226
Audit Log Tool ... 227
Command Hierarchy Groups and teams ... 230
District ... 233
Early Intervention System (EIS) Management ... 234
Alert policies ... 235
Custom metrics ... 241
Flags configuration ... 244
Master Name Index (MNI) ... 245
MNI in Axon Standards and Axon Records ... 245
Personnel Data Tool ... 246
Report Submission Settings ... 250
Restrictions ... 251
Rules and automations ... 252
Training Data Tool ... 255
User Management ... 262
Workflow Manager ... 264

Form Builder ... 266
Forms ... 268
Cards and fields ... 273
Cards ... 273
Field types ... 282
Subforms ... 288

Privileges ... 293
Manage Command Hierarchy Groups with privilege sets ... 294
Export and import privileges ... 297
Access ... 297
Activity logs ... 298
Administrator Console ... 298
Analytics ... 300
Cases - Standards ... 301

Early Intervention System (EIS) 307
Flags 309
Linking 310
Personnel 310
Profiles 312
Reports - Standards 313
Restrictions 319
Search 319
Task inboxes - Standards 320
Training 320

What's new

Report Writer

- Searching old profile versions when adding people to reports
- Adding flags to people and vehicles from Report Writer

Search

- Using Map view for search results

Case management

- Changing the order of tasks on case and investigation profiles

Axon Standards

Axon Standards is a Professional Standards and Internal Affairs tool that can be used on its own or in conjunction with the Axon Records Management System (RMS).

Axon Standards combines several software systems that aim to protect the lives of citizens, the careers of police officers, and the reputations of police agencies worldwide. These systems include:

- **Report writing software** lets agencies replace almost any paper-based documentation and contains tailorable templates for common reports, such as Use of Force, Vehicle Pursuits, and Citizen Complaints.
- **An Early Intervention System (EIS)** to help supervisors track officers' involvement in critical events, such as pursuits, use-of-force incidents, missed court dates, etc. Supervisors can use this data to ensure officers receive the training, counseling, and discipline required to flourish in their careers and exceed the high standards that agencies and communities alike expect.
- **Internal Affairs (IA) software** supports investigation of potential officer misconduct. This IA software works in conjunction with Use of Force reporting to provide a comprehensive picture of an officer's conduct in the field.

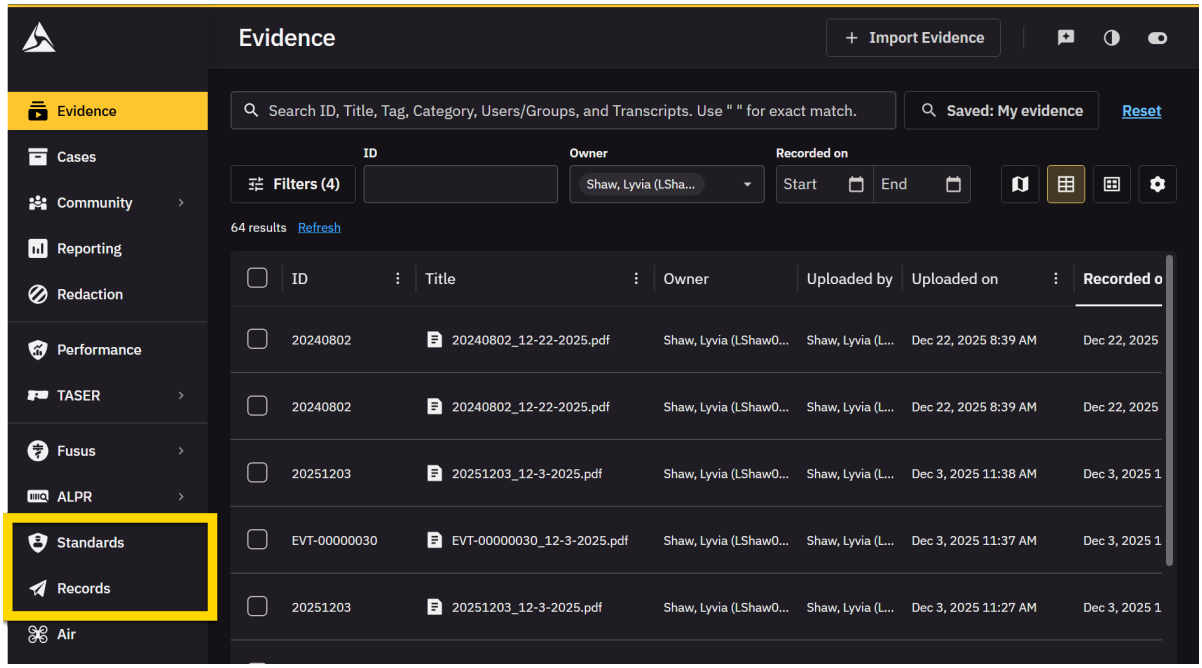
Watch this video for an introduction to Axon Standards.

Sign in

Follow these steps to sign in to Axon Records or Axon Standards:

1. In a web browser, open Axon Evidence, and sign in using your account information. After signing in, your organization's Evidence page will load in Axon Evidence.
   - If you need help signing in to Axon Evidence, see Registration and sign-in.

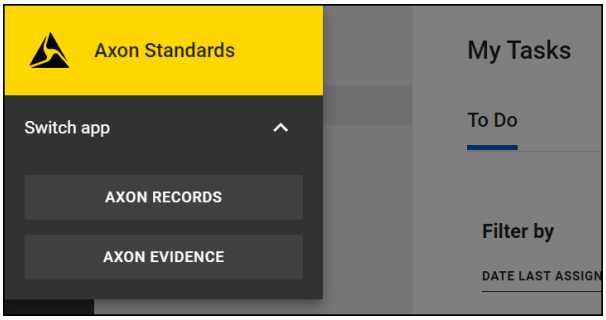
2. Depending on your organization's setup, you'll see either Axon Records, Axon Standards, or both in the main navigation menu. Select the one you want to access.



Switch between Axon Records and Axon Standards

If your agency uses both Axon Records and Axon Standards, you can easily switch between them without needing to re-login:

1. Select the Axon logo in upper left corner to open the App Switcher.
   - In the App Switcher you will see options for either Axon Records or Axon Standards, depending on which one you're currently in.
2. From the App Switcher, select which product you would like to open.



Automatic sign out

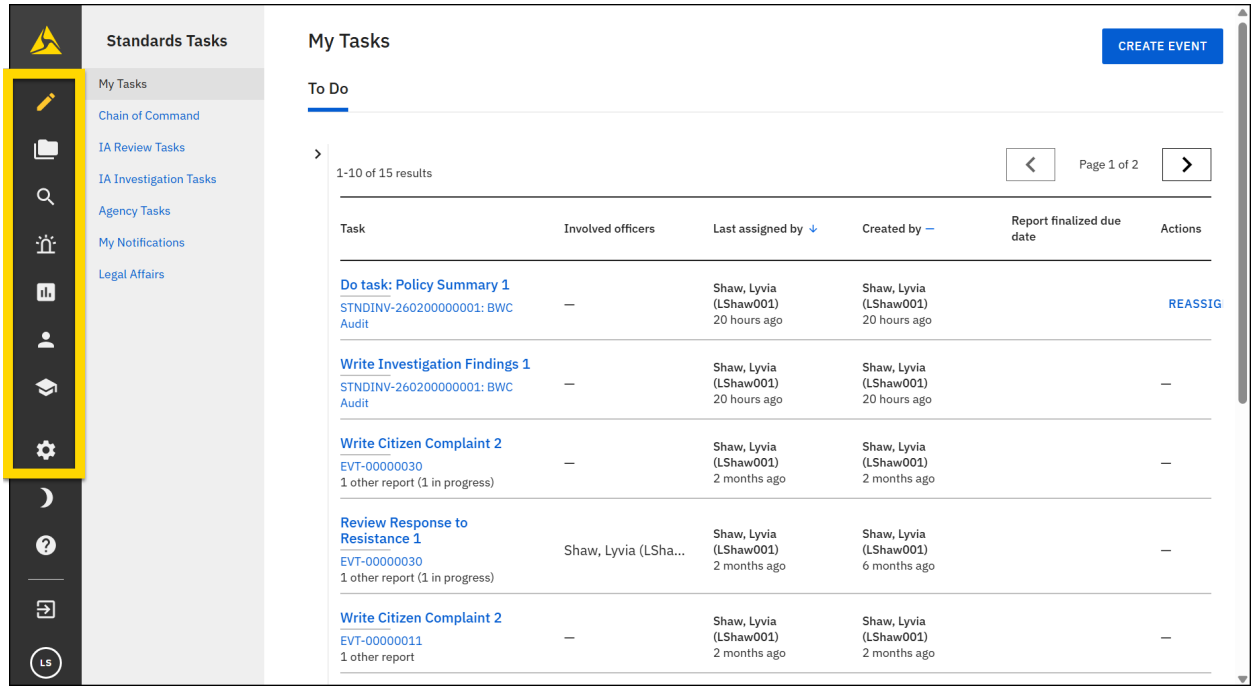
For security reasons, Axon Records and Axon Standards will automatically sign out after a period of inactivity.

The time period for this automatic sign out is determined by the **Quick application switch timeout** setting configured in the Axon Evidence Admin Console. The default for this setting is 30 minutes. The minimum is 10 minutes, and the maximum is 60 minutes.

For more information about this setting, see Quick application switch timeout.

Basic navigation

Select the icons below the App Switcher to open the various modules. Access to each module is determined by the privileges granted to that user's Command Hierarchy group and/or team.



The following videos explain the various modules and features in Axon Standards.

Navigation Overview

General Overview

Report, task, and event management

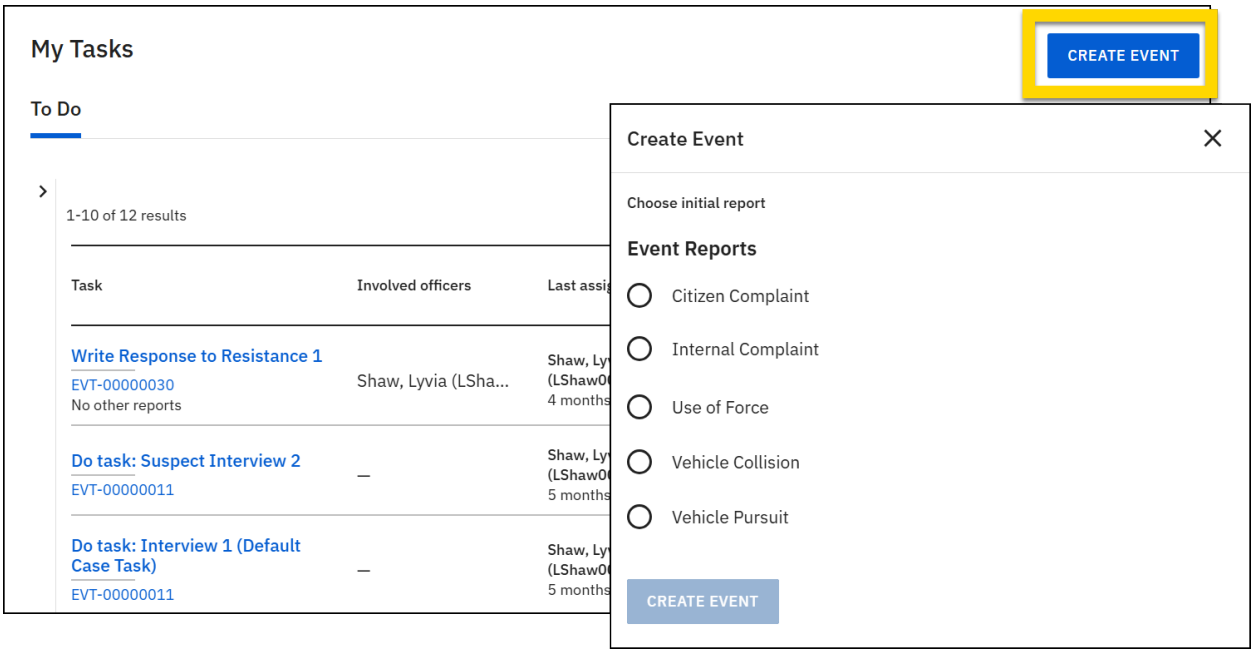
Report writing involves a combination of report, task, and event management. When writing reports, it can be helpful to understand the following terms:

- Report
- Task
- Inbox
- Event

Reports

A report is the type of documentation that is created in by selecting **Create Event** from any task inbox. When a new report is created from a task inbox, an associated event is also created. In addition to the standard out-of-the-box reports (use of force, citizen complaint, etc.), each organization has custom report types. Reports can also be created from an event profile.

For more information, see Create a New Report.



Tasks

A task indicates an action that needs to be taken on a report and who needs to perform that action. Multiple tasks are taken on a single report throughout its "lifetime". Task types include:

- View: Reports or case tasks that can be viewed but not edited because they are currently in review or already finalized
- Do: Case tasks assigned to you
- Write: Reports assigned to be created and not yet submitted
- Revise: Reports previously submitted for approval but returned by the report reviewer for corrections (the report author receives an email when a report they submitted is returned)
- Review: Reports submitted for review
- Rereview: Reports rejected by the report reviewer, then updated and resubmitted by the author

Tasks are listed in the inboxes in the Tasks module. The same task may appear in multiple inboxes, based on the type of task it is.

For example:

1. Officer Shaw selects **Create Report** to create a new incident report.
2. A Write Field Interview Report task appears in her My Tasks inbox.
3. When Officer Shaw submits the report to her supervisor for review:
   a. The Write task disappears from her My Tasks inbox (because she has completed the task).
   b. A Review task appears in her supervisor's My Tasks inbox, as well as the Supervisor Review tasks inbox.

The report remains the same throughout this process, but the tasks associated with the report change based on which person needs to take action on it.

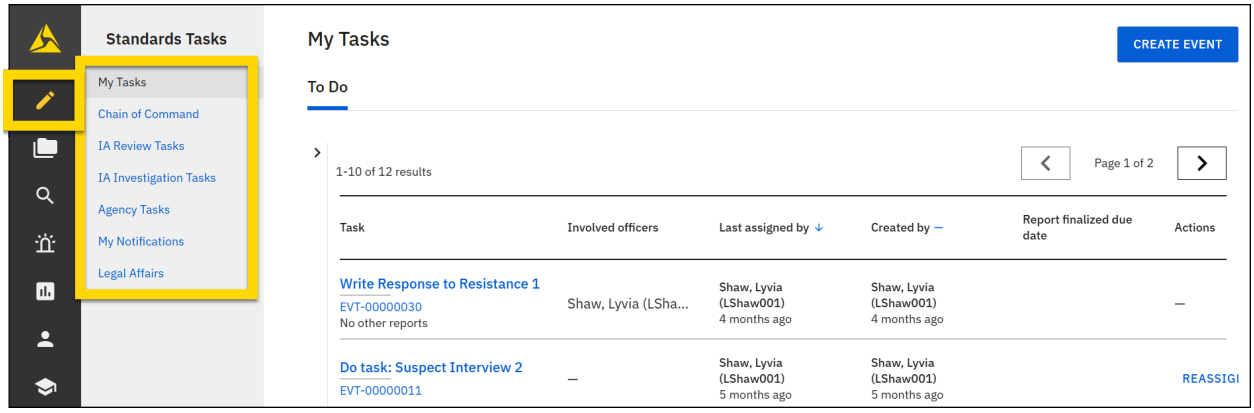
For more information, see Task management overview.

Note

Case tasks are slightly different from report tasks. For more information, see Case tasks.

Inboxes

Task inboxes are accessed by selecting the pencil icon in the main navigation menu. Every user can access the My Tasks inbox and may see additional inboxes, depending on their privileges. For more information, see Task management overview.



Events

When a new report is created in Axon Standards, an associated event is also created. Each event has an event profile, which includes all basic information included in the initial report, as well as any other reports or files associated with the event. When necessary, an event can be turned into a case, which contains additional functionality and features.

For more information, see Event and case profiles.

Task inboxes

When you sign in, the My Tasks inbox in the Tasks module loads. Depending on the Command Hierarchy groups and/or teams you belong to, you may see additional inboxes for different task groups. For more information, contact your administrator.

Note

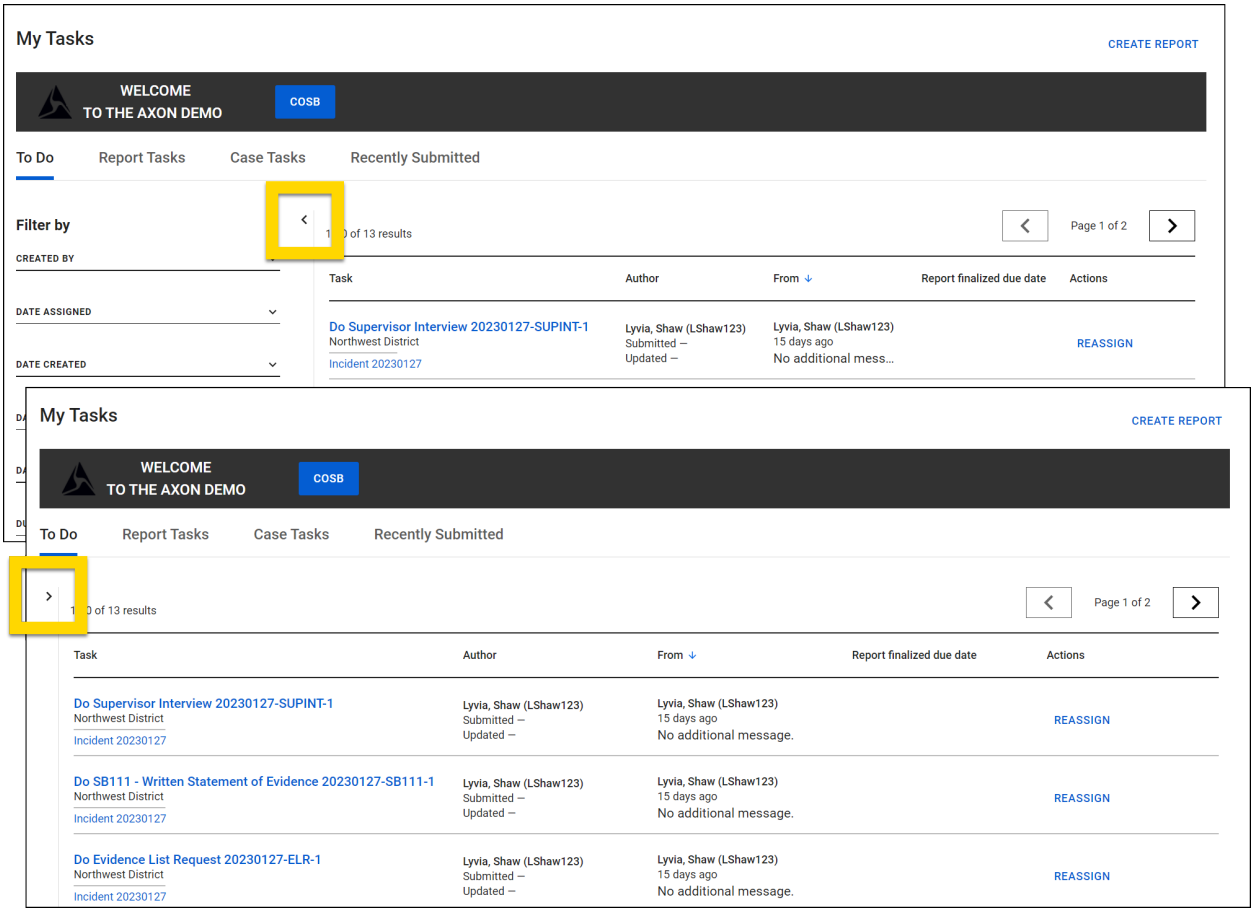
These inboxes only include Axon Standards tasks. If your agency also uses Axon Records, switch to Axon Records to access those tasks.

The following task types appear in these task inboxes:

- View: Reports or case tasks that can be viewed but not edited because they are currently in review or already finalized
- Do: Case tasks assigned to you
- Write: Reports assigned to be created and not yet submitted
- Revise: Reports previously submitted for approval but returned by the report reviewer for corrections (the report author receives an email when a report they submitted is returned)
- Review: Reports submitted for review
- Rereview: Reports rejected by the report reviewer, then updated and resubmitted by the author

Many inboxes have multiple tabs, each of which contain a filtered list of tasks. For example, a **To Do** tab may contain tasks for reports currently in progress.

All task inboxes contain a list of filters you can use to limit which tasks are displayed. Select the arrow to expand or collapse this filter list. The list of available filters varies, depending on inbox and tab within an inbox.



Use the arrow buttons at the top and bottom of the tab to move between pages. Additionally, adjust the number of tasks displayed per page using the **Results Per Page** menu at the bottom of the page.

My Tasks inbox

The **My Tasks** inbox shows all tasks that have been assigned to you. If your organization uses the Case Management module, you will also see all case tasks and case document tasks that have been assigned to you.

The most recently updated tasks appear at the top of the list. Use the following options to filter which tasks are displayed:

- Date Last Assigned
- Date Created
- Last Assigned By
- Created By
- Report Type

The following information is included for each task:

Task column

- Report information, including:
  - The task name and the report number
    - The number for the first report created in an event is 1. The number for the second report is 2, and so on.
    - Selecting the task name opens the report.
- Associated event information, including:
  - The Event ID associated with the report
    - Selecting the Event ID opens the event profile.
  - The number of other reports associated with the event

Involved officers column

- The name(s) of officers involved in the event

Last assigned by column

- Who assigned the task
- When the task was assigned

Created by column

- Who created the report
- When it was created

Report finalized due date column

- The date the report should be finalized
  - If the date has passed, it will turn red.

Actions column

- For **Do** tasks, a Reassign button

Announcements banner

An announcements banner on the My Tasks inbox lets you provide customized information to your staff. Selecting the arrow in the top right collapses the banner. If your organization uses both Axon Records and Axon Standards, you can create separate banners to display in the separate My Tasks inboxes in Axon Records and Axon Standards.

The banner supports the following styles:

- HTML rich text formatting such as bulleted lists, bold, and italics
- Emojis
- A button that links to a custom agency website or the Axon website

> **Note**
>
> Axon only allows links to URLs owned by Axon or by your organization.

To update this banner's contents, open the Announcements Banner Update tool in the Administrator Console.

Chain of Command, IA Review, and IA Investigation Tasks inboxes

Reports submitted for review or additional investigation appear in the Chain of Command, IA Review Tasks, and IA Investigation Tasks inboxes. To access these inboxes, you must belong to Command Hierarchy groups or teams with the appropriate privileges.

The most recently updated tasks appear at the top of the list. Use the following options to filter which tasks are displayed:

- Assigned To
- Created By
- Date Created
- Date Last Assigned
- Event ID
- Report Type

The following information is included for each task:

Task column

- The user the task is assigned to
- Who last assigned the task

- When the task was last assigned
- **Assign**, **Reassign**, **Start review**, and **Continue review** buttons

Report column

- The report name and number
- Who created the task and when
- The involved officer(s)
- The Event ID associated with the report
  - Selecting the Event ID opens the event profile.
- The number of other reports associated with the event

Agency Tasks inbox

The Agency Tasks inbox shows all report tasks at the entire agency. Use the tabs to switch between **In Progress** tasks and **Recently finalized** tasks.

Select **More actions [...] > Export all to CSV** to export the tasks included on that tab to a CSV file. The most recently updated tasks appear at the top of each tab. Use the filters to refine which tasks are displayed:

In progress	Recently finalized
Assigned To	Created By
Created By	Date Created
Date Created	Date Finalized
Date Last Assigned	Event Id
Event Id	Finalized By
Last Assigned By	Task Type
Task Type	

Note

Each tab only contains 1,000 pages of reports. Older reports can be found using Reports search.

The following information is included for each task:

Task column

- Report information, including:
  - The task name and the report number
    - The number for the first report created in an event is 1. The number for the second report is 2, and so on.
    - Selecting the task name opens the report.
- Associated event information, including:
  - The Event ID associated with the report
    - Selecting the Event ID opens the event profile.
  - The number of other reports associated with the event

Assigned to column

- Who is assigned to the task
- **Assign** and **Reassign** buttons

Last assigned by column

- Who assigned the task
- When the task was assigned

Created by column

- Who created the report
- When it was created

My Notifications inbox

Administrator note

A new Share report feature and the Notification Center have been released, which are a replacement for this inbox. Contact Axon Support or your Axon representative to enable this feature for your organization.

The My Notifications inbox shows all new tasks you have been notified about. The most recent notifications appear at the top of the list. Use the following options to filter which notifications are displayed:

- Date Notified
- Event ID
- Notified By
- Report Type

The following information is included for each notification:

Task column

- Report information, including:
  - The task name and the report number
    - The number for the first report created in an event is 1. The number for the second report is 2, and so on.
    - Selecting the task name opens the report.
- Associated event information, including:
  - The Event ID associated with the report
    - Selecting the Event ID opens the event profile.
  - The number of other reports associated with the event

Notified by column

- The name of the user who sent the notification to you

Date notified column

- The date you were sent the notification

Action column

- Selecting **Dismiss** removes the task from your My Notifications inbox.

Send a notification by opening a report and selecting **More actions [...] > Notifications** in th Report Writer header.

Create and submit reports

This topic describes how to create and submit reports. Specific workflows include creating reports and events, creating events from Axon Records, and submitting reports.

Create reports

When you create an event, you must choose an initial report type to start the event. Once an event is created, you can add additional reports, upload files from your computer, and manage restrictions.

To create a new report:

1. Select **Create event** from the top right corner of any task inbox.
   - To add a report to an existing event or case, open the event or case profile and select **Create report** in the profile header.
2. Select a report type.
   - The following report types are available by default. Additional report types are created on an organization-by-organization basis, so you will see additional options in this menu:

    - Citizen Complaint
    - Internal Complaint
    - Use of Force / Response to Resistance
    - Vehicle Collision
    - Vehicle Pursuit
3. If your organization is configured to use custom names, you can optionally add a custom name for the report.
4. After choosing a report type, select **Create event** to open Report Writer and add information to the report.
5. When you have finished working on the report, select **Submit** at the bottom of the screen to submit it for review.
    - To close a report without submitting it, select the **X** in the upper right corner. You can come back to it later by selecting the Write report task from your My Tasks inbox.

If you create a new report by selecting **Create report** on an existing event/case profile, you may see additional options:

- If your organization uses the Case Management module AND a case has been created for that incident, you'll see a section for the creation of case documents.

Submit reports

To submit a report for review or finalization:

1. Open the report in Report Writer.
2. Select **Submit** at the bottom of the Report Writer screen.
    - In some workflows, the report can be finalized immediately and does not need to be submitted for review. In these cases, select **Finalize** at the bottom of the screen.
3. If the report contains validation errors, the Routing page shows a warning. Return to the report to fix the errors by selecting **Back** or submit the report with errors by selecting **Submit** at teh bottom of the screen.
    - Some organizations don't allow reports containing validation errors to be submitted. If this is the case for your organization, you will not be able to select **Submit** until you have resolved all errors.
4. Select where the report should be routed for review.
    - This option may not appear in some workflows.
5. Add a routing note as necessary.
6. Select **Submit**.

Submitted reports are removed from your My Tasks inbox and routed to the appropriate Review inbox. If the report is reviewed and rejected, it re-appears in the My Tasks inbox as a Revise task. After updating the report, you can resubmit the report for re-review. The supervisor will again approve or reject the report.

If the report belongs to a multi-step review workflow, a supervisor may submit the report for additional review. During the later review steps, a reviewer can still reject the report. If they do, the report is again returned to the original author for revision and re-submission.

Once a report is approved by the final reviewer, it becomes an official, final report.

Create events from Axon Records

If your organization uses both Axon Records and Axon Standards, you can create an Axon Standards event from within Axon Records. When you do this you can easily import person information from the Axon Records incident into the Axon Standards event without needing to manually copy-paste.

To do this, take the following steps:

1. Open the incident profile in Axon Records by selecting the Incident ID from a task inbox or by searching for it and select **New report** in the profile header section.
2. Switch to the **Standards** tab, select an Axon Standards reporttype, and select **Create report** at the bottom of the pane.
   - The Incident ID is automatically added to the Incident ID field in the Axon Standards report.
3. If you need to import person information from the incident into the event, select **Add person**.
4. All people who have been added to the incident appear below the search fields. Select a person's name to open their profile in a preview pane on the right side of the screen.
5. Select **Import and update** at the bottom of the pane to add that person to the event.

All information about the person that was added to the Axon Records report will import into the Axon Standards event.

Note

When you submit or close the Axon Standards event, you are returned to the incident profile in Axon Records.

Review, revise, and finalize reports

This topic explains how reports move through review, revision, and finalization workflows. These workflows include initial review, revising rejected reports, rereview and final approval. Additionally, once a report is finalized, users with specific privileges can revert it as necessary.

Review reports

To review a report:

1. Find the report to review:
   - If you are already assigned as the reviewer, the task appears in your My Tasks inbox.
   - If you are in another inbox, use the filters to find the task. If you are not yet assigned as the report reviewer, before beginning your review, you must assign yourself using the **Assign/Reassign** buttons on the task inbox or in the Report Writer footer.
2. Review the report, adding comments as needed using the sidebar.
   - The comment is added to the section of the report you are currently viewing and will only appear when that section is open. Be sure to select the section of the report the comment applies to before you create it to ensure it is associated correctly.
3. Users with the appropriate privileges can also edit a report while reviewing it by using the **Review and edit** option from the **More actions [...]** menu. This option is only available if the report is assigned to you for review.
   - Being able to edit a report during the review process allows reviewers to make necessary changes without the inefficiency of sending the report back to the original author.
   - When editing another user's contribution, a gray banner appears at the top of the report stating: "You are making changes on behalf of the user."
   - You can make changes to any part of the report, and the changes will automatically save.
4. While reviewing the report, select the arrow in the top left corner of the Report Writer header to reveal a list of all reports included in that event. Select a report name to open that report.
5. When you are finished with your review, select **Approve** or **Reject** in the Report Writer footer.
6. Add a routing note and mark if the task is urgent (as applicable.)
   - The last person assigned to the report is auto-populated in the **Assignee** field.

7. Select **Approve, Request revision, Submit for investigation,** or **Reject**.

Revise reports

If a report you submitted is rejected by a reviewer, a Revise task is added to your My Tasks inbox.

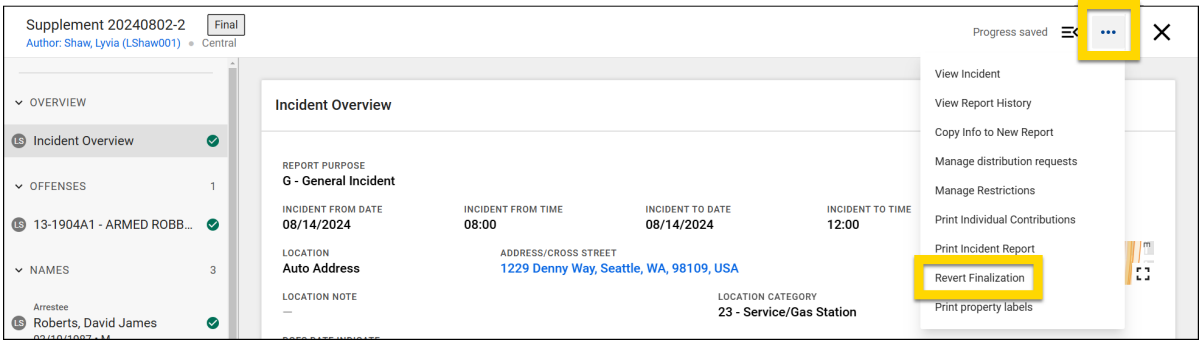
You can add additional event information, citizens, officers, units, investigation details, and files when revising a report. You can also edit any information that already appears in the report. After making all requested changes, select **Submit** in the Report Writer footer to send the report back for a rereview.

Revert finalized reports

After a report has been finalized, users with the appropriate privileges can revert the finalization. When this occurs, the report is returned to a Review state where it can again be reviewed and rejected for revisions as necessary.

To revert the finalization of a report:

1. Open the report and select **More actions [...] > Revert finalization.**



2. Assign who the report should be reviewed by.
3. Add a note (required).
4. Select **Revert finalize**.

When a report finalization is reverted, the report history shows when the finalization was reverted and who reverted it.

Report Writer

Select a task from any task inbox to open the associated report in Report Writer. To prevent data loss and saving errors, a report can only be open in one browser tab at a time. If you open the same report in multiple tabs, an error message appears, indicating

that all but one tab should be closed before you continue working.

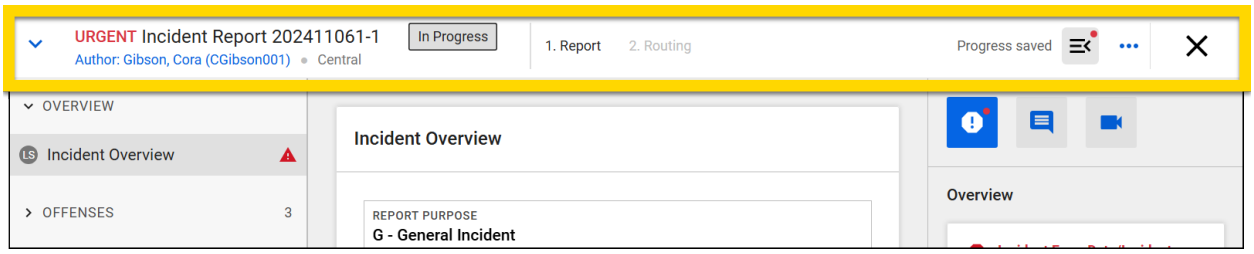
The Report Writer screen is split into five areas:

- Header
- Navigation menu
- Central report writing area
- Sidebar
- Footer

Header

The header at the top of the screen, includes the following information and options:

- A dropdown arrow that appears if multiple reports are associated with the event.
  - Select this arrow to reveal the other reports and quickly switch between them.
- Report metadata, including:
  - Report type and ID
  - Author: Select this name to view the report history.
  - District
- Report status: (In Progress, In Review, etc.)
- Save progress
- Icon to open and close the sidebar
- **More actions [...]** menu to take various actions on the report
- **X** button to close the report: Reports are auto-saved, so you can close at any time without losing your work



Depending on the type of report, you can do the following from the **More Actions [...]** menu:

- View event: Opens the event profile
- View report history: Opens a log of all actions taken on the report, including by whom and when
- Copy info to new report: Lets you copy the information from the report into a new one
- Manage restrictions: Lets you edit, remove, and add restrictions

- Notifications: Shows the users who have been notified about the event and allows additional notifications to be sent
- Print: Lets you print the report. Multiple print options may be available.
- Delete report: Lets you permanently delete a report

Note

The options that appear in this menu depend on your organization's specific configuration, as well as which privileges have been granted to you. Contact your administrator for more information.

Auto-save

Report Writer includes an auto-save feature specifically designed to protect the information you enter into your report. As you enter information into Report Writer, the system automatically saves your work every few seconds.

The messages in the upper right corner of the screen display the status of your report:

- **Progress Saved**: Indicates all information that you've entered into the report up until that point has been saved
- **Syncing**: Indicates the system is currently saving information you entered into the report since the last time the report saved

If your device disconnects from the internet, your data may be saved if:

- You do not close the browser window or tab where you are writing your report
- You do not leave the Report Writer page to open a different page in Axon Standards

If the above conditions are true, once you regain internet connectivity, your report will automatically upload any information saved to your device to the cloud. Following this, the auto-save feature will continue to function as usual.

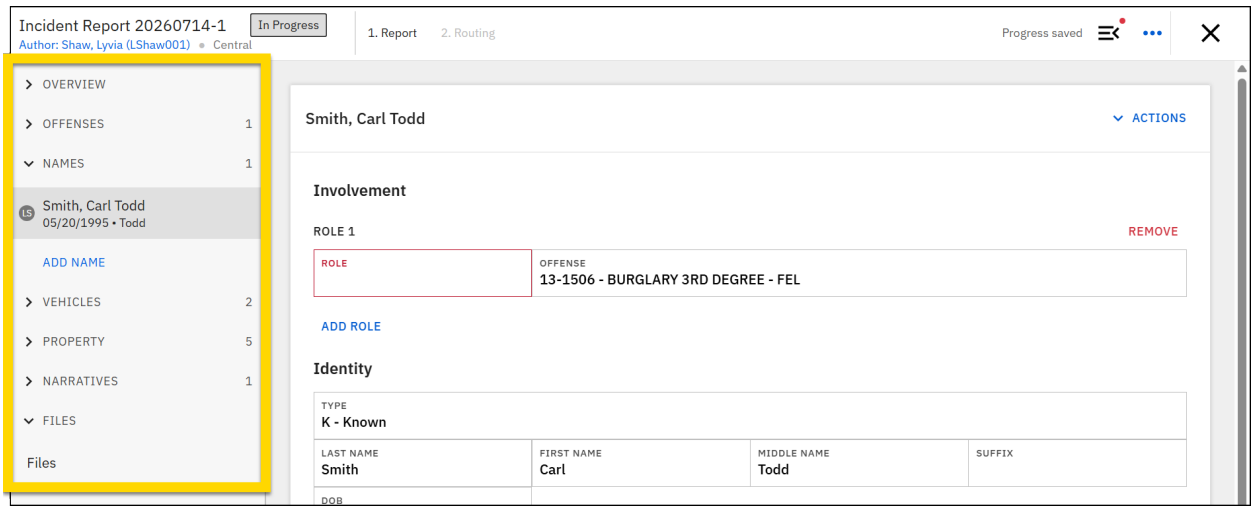
Warning

There is a risk of data loss if your device loses internet connectivity. To minimize this risk, a stable internet connection is recommended for whenever you are working on a report.

You can tell you are offline if a banner appears at the top of your screen informing you the network connection was lost. You will also see a change in the status message in the top right corner of the screen. The status text will turn red and display the last time your report was successfully saved.

Navigation menu

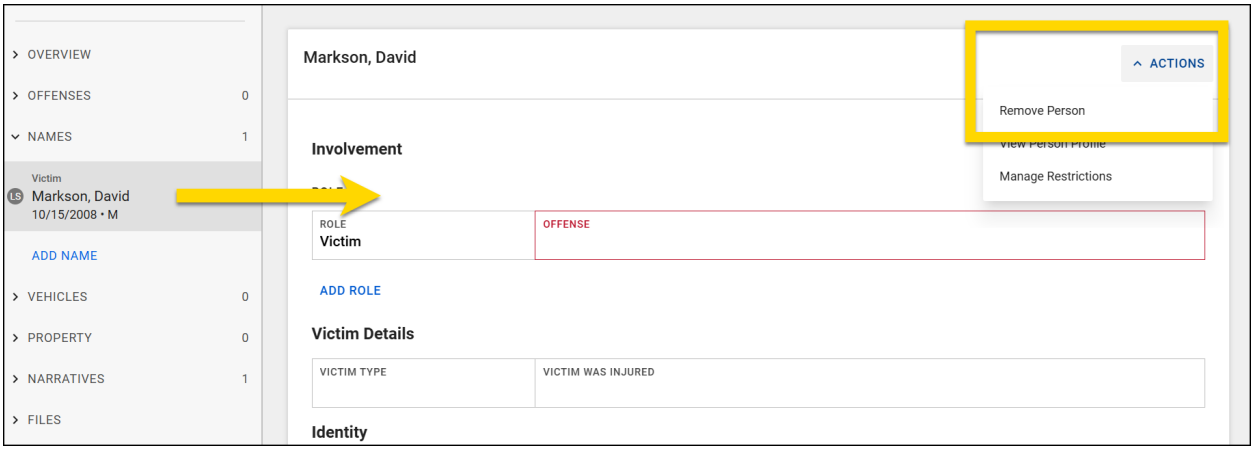
The navigation menu on the left side of the screen lets you jump between various sections of the report (overview, people, vehicles, etc.). Each section contains a set of fields that open in the central report writing area. Some sections have **Add** buttons that let you add that type of section to the report multiple times. For example, you can use the **Add** button to add multiple people or vehicles to a report.



The available sections vary depending on the type of report, but often include:

- Overview
- Citizens
- Vehicles
- Unit
- Officer
- Response Actions
- Narrative
- Files

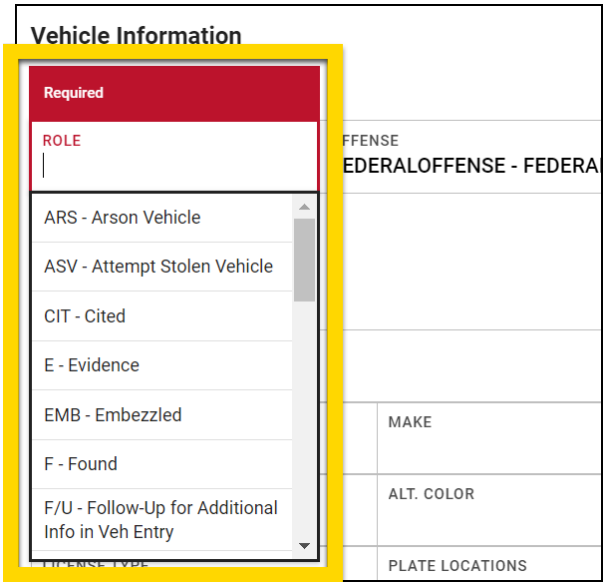
To remove a section from a report, open the section and select **Actions > Remove** in the top right corner of the central report writing area.



Central report writing area

Add information to a report in the central report writing area by completing empty fields. Some fields display conditionally; they only appear once you've added other information to the report. Required fields, which are set by your organization, are outlined in red.

When you select a field and a drop-down menu appears, you must select an option from the list. Typing any other information in these fields will not be saved. See Keyboard shortcuts for information about quickly entering information into reports.



Scroll to the top of a section and open the **Actions** menu in the top right corner to take the following actions. These options vary depending on the type of report and the section within the report:

- Remove the section
- View the profile associated with that section
- Manage restrictions for that section

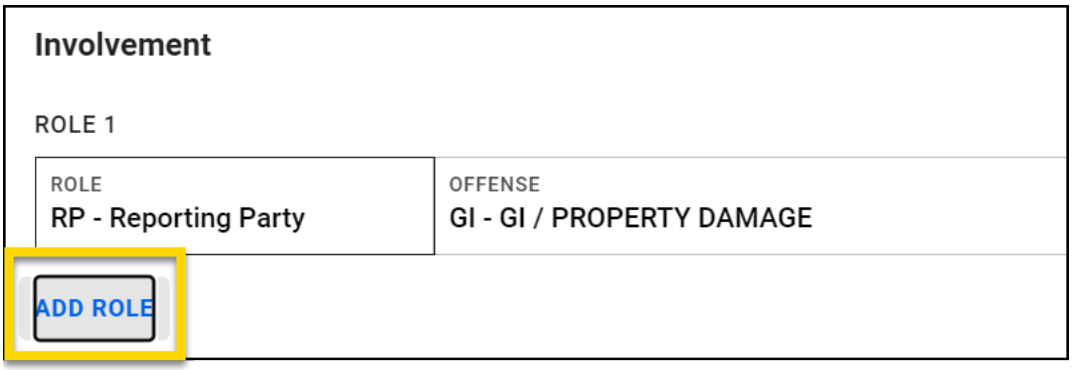
Keyboard shortcuts

Axon's Report Writer has keyboard shortcuts to help you write reports quickly and efficiently.

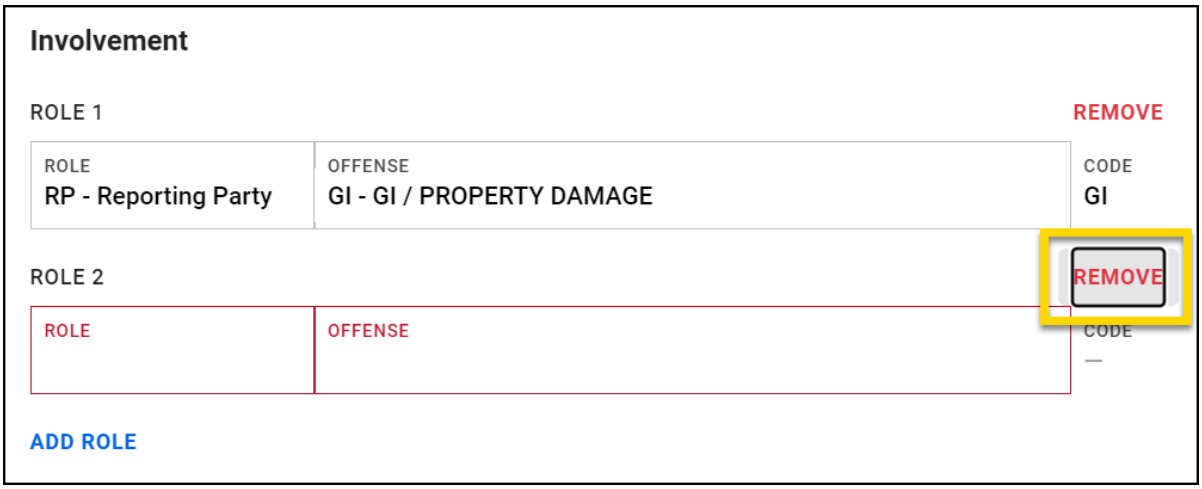
Field navigation

Move through the various fields in your report using these shortcuts:

- **Tab:** Go to the next field.
- **Shift + Tab:** Go back to the previous field.
- **Enter:** Add additional fields by pressing **Enter** on blue **Add** links.



Remove fields by pressing **Enter** on red **Remove** links.



Date fields

Simplify entering a date using the following autofill shortcuts:

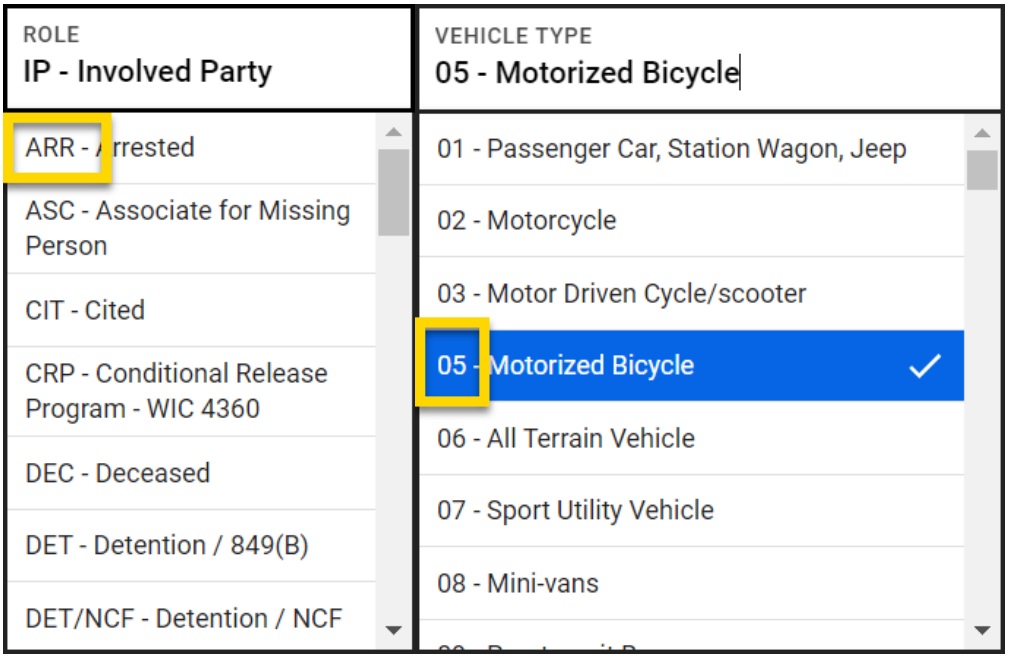
- **T**: Insert today's date and time.
- **Y**: Insert yesterday's date.

Drop-down menus

- Use the numeric or abbreviation shortcuts, followed by **Enter** or **Tab**.
- Navigate through the menu using the arrow keys.

The options in many drop-down menus are prefaced with either a number or an abbreviation. You can quickly select an option by typing that number or abbreviation then pressing **Enter** or **Tab**.

Alternatively, use the up and down arrow keys to scroll through drop-down menu options.



Text formatting

To make changes to the font or move text to another spot in a text field, use these formatting commands:

- **CTRL + B** (Windows) / **CMD + B** (Mac): Bold text.
- **CTRL + I** (Windows) / **CMD + I** (Mac): Italicize text.
- **CTRL + C** (Windows) / **CMD + C** (Mac): Copy text.
- **CTRL + V** (Windows) / **CMD + V** (Mac): Paste text

Sidebar

Expand the sidebar on the right side of the screen to view validation errors or leave comments. Based on your organization's configuration, additional options may appear in this sidebar.

Comments created in the sidebar are associated with that section of the report. For example, if you leave a comment on a vehicle, then switch to view a person, the comment does not display. When you switch back to the vehicle section, the comment appears again. A comment icon appears in the left navigation menu, indicating which sections contain comments.

Once created, a comment cannot be deleted manually by a user. When the report is submitted for review, the comments can be seen by the report reviewers.

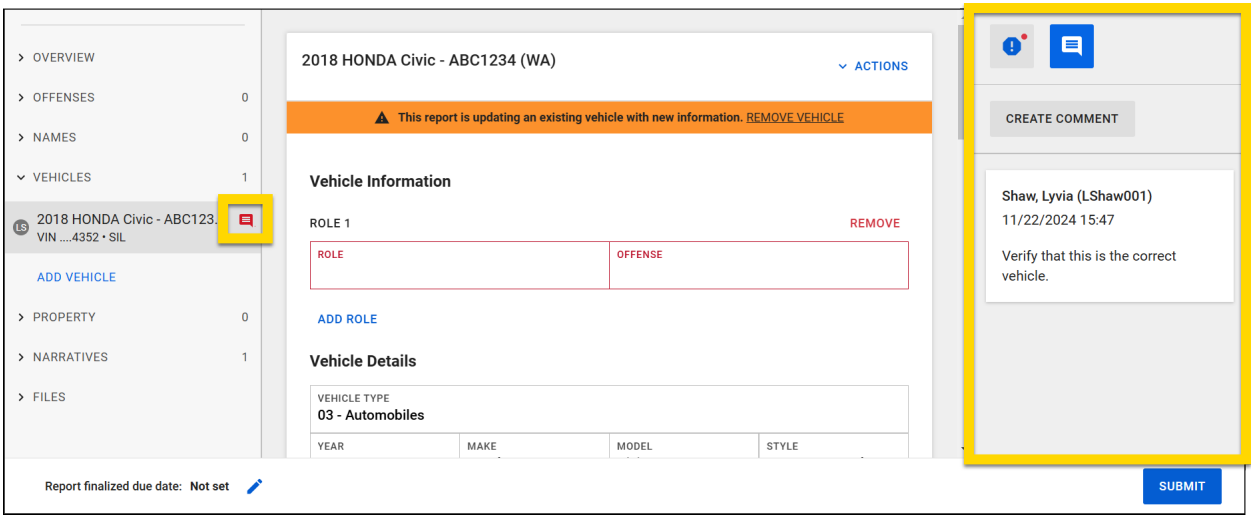
Your organization can configure if and when comments are automatically deleted. Comments can be deleted:

- When a report is finalized
- When a report moves between states (e.g., Review 1 > Review 2)

Contact your Axon representative or Axon support for assistance in configuring these comment deletion settings.

Warning

If your organization uses these settings to delete comments, when a comment is deleted, it is irreversibly removed from the system and cannot be recovered or retrieved by any user or administrator. Organizations with legal obligations to retain or disclose comment content should ensure that any necessary information entered in comments is documented directly in the report before it is finalized.



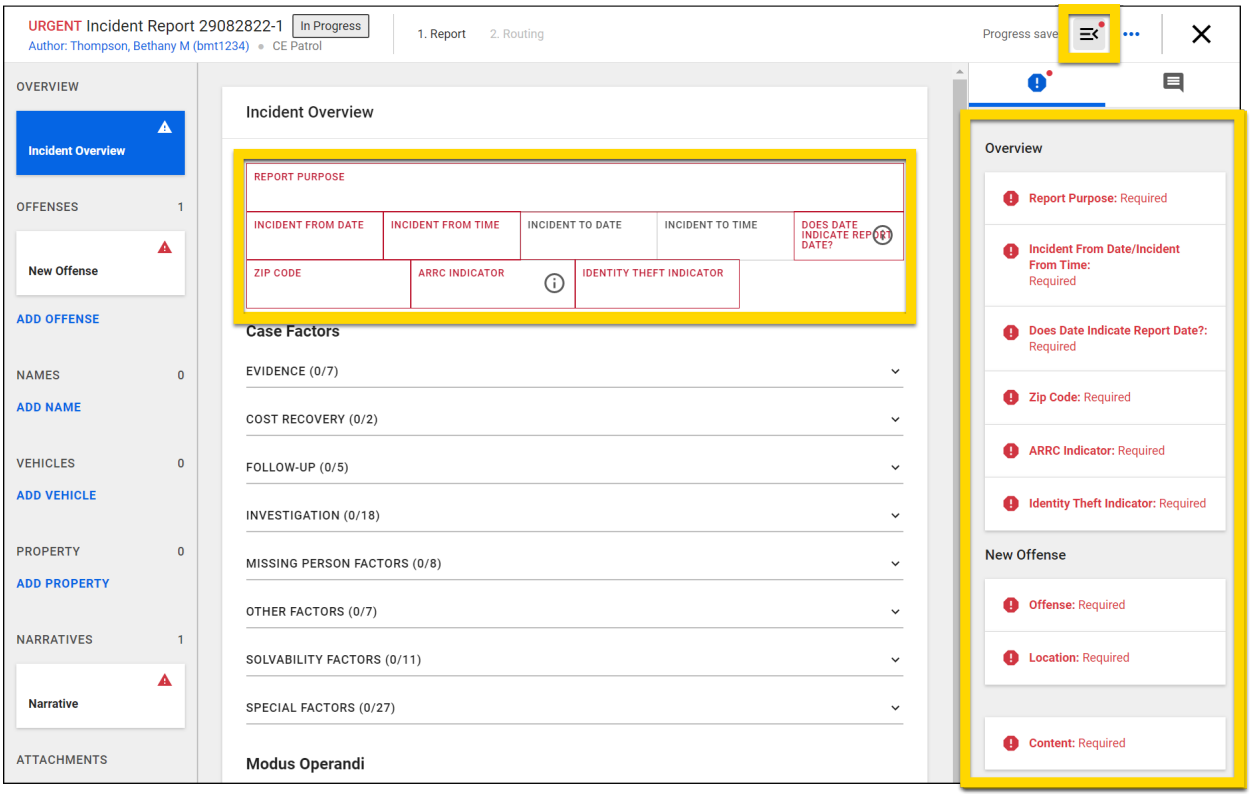
Validation errors

Required report fields, which are set by your organization, are outlined in red. Some required fields display conditionally; they only appear once you've added other information to the report.

If you leave a required field empty, a validation error displays in the sidebar on the right side of the screen. Select an error message to jump to that field in the report.

Administrators can specify for each report type if the report can be submitted if validation errors are present, or if the report author must first fix all errors before submitting the report for review.

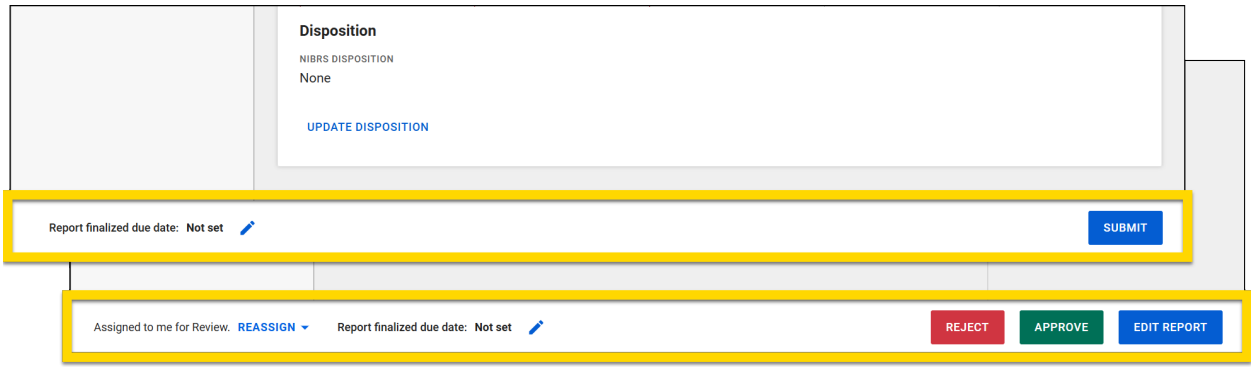
For more information, see Report submission settings.



Footer

The footer appears at the bottom of the sceen and shows different options depending on the report state:

- All states
  - Update the report finalization due date
- Draft state
  - Submit the report for review or finalization
- Review state
  - Assign/reassign the report for review
  - Reject or approve the report



Add report information

When working on reports in Report Writer, use the **Add** buttons in the navigation menu to add new sections (composed of multiple fields) in the central report writing area where you can enter information.



These sections vary depending on the type of report, but often include:

- Overview
- Citizens
- Vehicles
- Units
- Officers
- Response actions
- Narrative
- Files

Overview

Most reports contain an Overview section where you can record basic information, including date, time, and location. Overview sections contain various other fields, depending on the report type. Unlike the other report sections, the Overview section can't be removed from the report.

Date and time

To quickly enter the current date and time, enter "T" in the date field. The current date and time automatically appear in both the **Date** and **Time** fields. See Keyboard shortcuts for additional information about quickly entering information into reports.

Location

Depending on the report type, various location-related fields appear, often including Location, Location category/type, and Location note. The location-related fields and entry methods of the options in the **Location** field are outlined in the table below.

Location option	Entry method	Appears in search when adding locations to a report	Appears in Locations search in the Search module
Auto address	Users search the system for verified addresses to add to reports	Yes	Yes
Cross streets	Users search the system for verified addresses to add to reports	Yes	Yes
Manual address	Manually entered by users	No	Yes
Mile marker	Manually entered by users	No	No
Unknown	Manually entered by users	No	No

Note

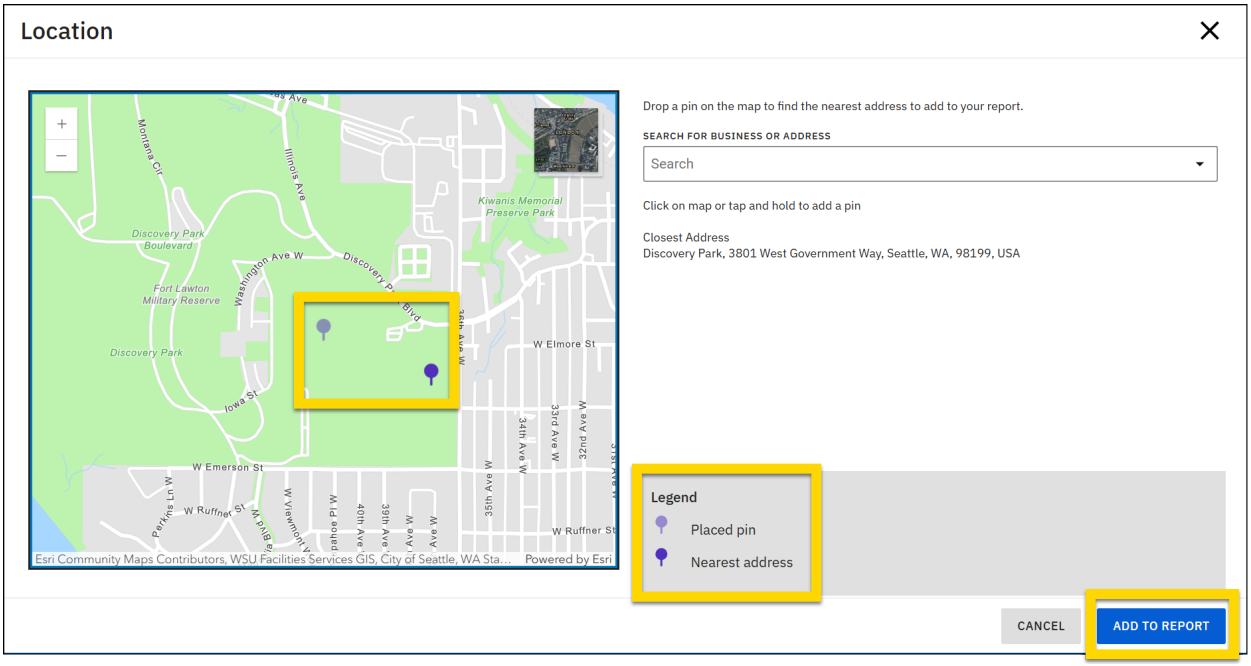
It is generally a best practice to use verified Auto addresses and Cross streets when completing reports. Follow your organization's policy when adding Manual addresses, mile markers, or Unknown locations to reports.

Auto addresses and cross streets

When you select **Auto address** or **Cross streets** from the **Location** field, you can type in the **Address/cross street** field, and a list of possible location matches will appear.

To enter a location by finding it on a map, instead select the map that displays beside the **Address/cross street** field. A larger map window loads. Use the plus and minus buttons to zoom in and out. Click and drag to pan the map and reveal new areas.

Click anywhere on the map to drop a pin. The pin you place appears in light purple, and the nearest verified address appears in dark purple. Select **Add to report** to add the verified address to your report.



You can add subaddress information to auto addresses to specify a particular unit or apartment number. These unit/apartment numbers are considered unique locations, even though they share the same address.

To add a unit, select **Add unit**, then provide the **Unit type** (Apartment, Suite, etc.) and **Unit number**.

Manual addresses

When you select **Manual address** from the **Location** field a set of new fields appears where you can enter the location information.

Mile markers, and unknown

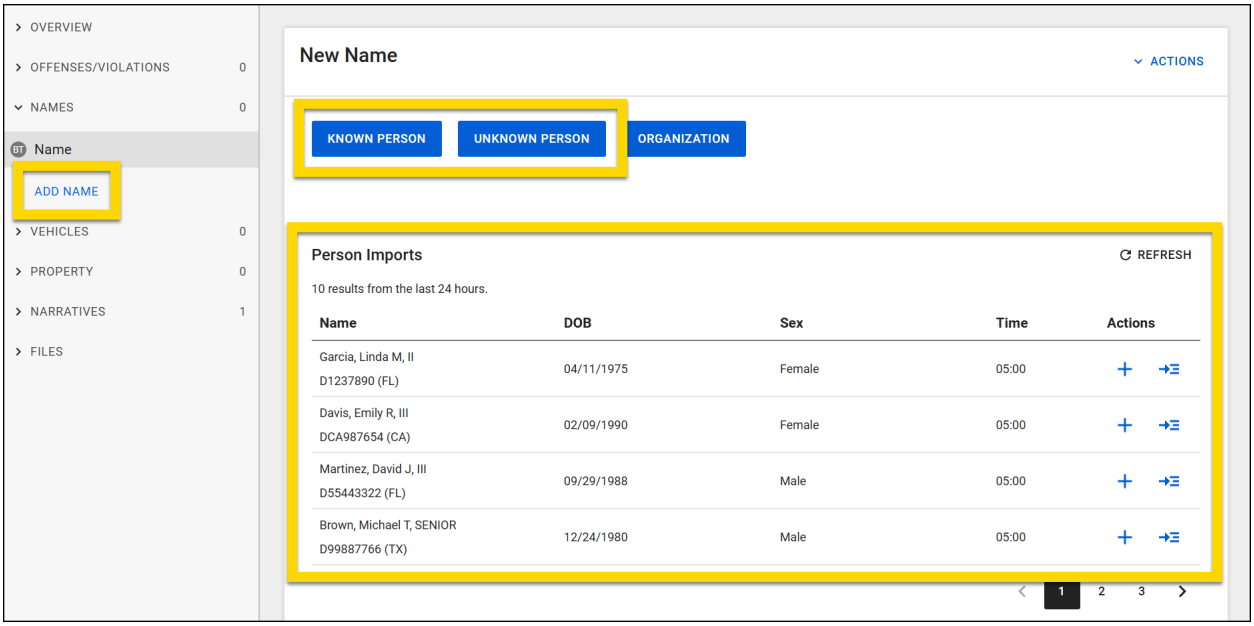
When you select **Mile marker** or **Unknown** from the **Location** field a set of new fields appears where you can enter the location information.

Citizen

To add a person to a report, select **Add Person/Citizen** in the report navigation menu, and then select the type of person you want to add: Known or Unknown.

If your organization has integrated with your NCIC search provider, you can also view the people you exported from NCIC and add one to your report.

Once a person has been added to a report, you can add and update their information.



Add a known person

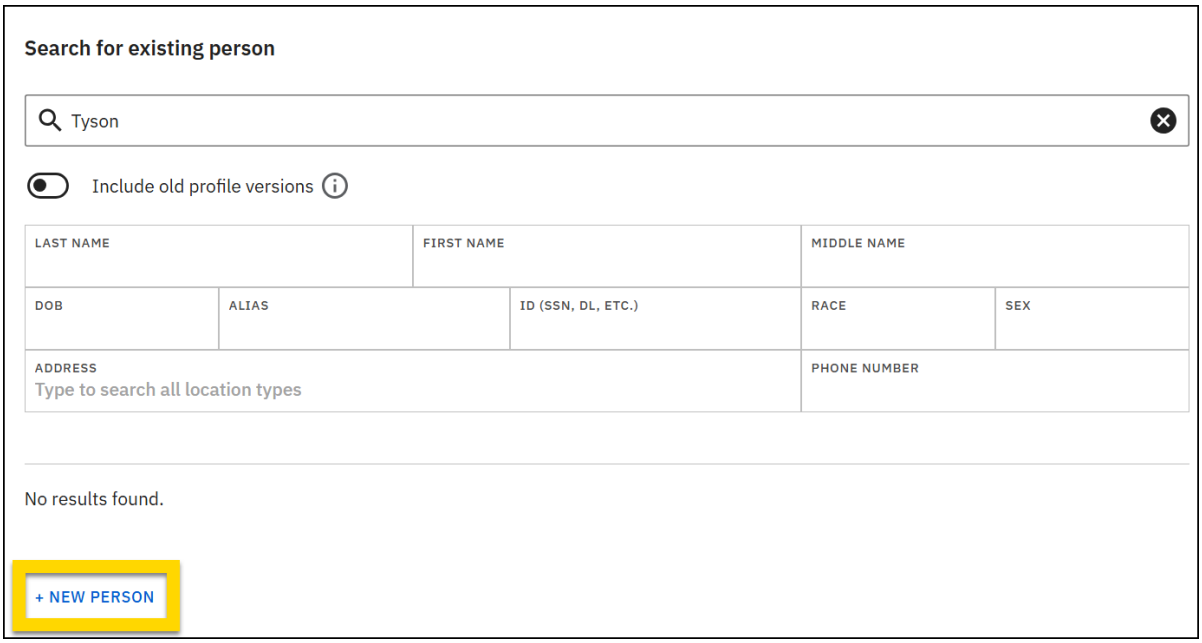
A known person is someone who can be positively identified. This could be someone whose identity is fully confirmed, such as a person who has presented valid identification or has been recognized by someone else. A known person can also be partially known. For example, if witnesses report seeing a male in a blue sweater running from the scene, this individual is considered a known person because some identifying information is available.

To add a known person to a report:

1. Select **Add name > Known person**.
2. To avoid creating duplicate person profiles, search to see if the person already exists in the database rather than automatically creating a new one.
   - Enter keywords in the top search box or use the filters to search.
   - Potential matches from the database appear below the search fields as you enter information.

- Select a search result to open a profile preview pane and view more information.
- Optionally turn on the **Include old profile version** setting to also include older versions of people profiles.

3. If your organization has integrated with your NCIC search provider, you can also search for people you imported from NCIC.
4. If a profile matches the person you want to add to the report, select **Import and update** at the bottom of the pane.
5. If a profile does NOT exist for the person you want to add to the report, select **New person** below the list of search results.



An orange banner displays at the top of the window when you add an existing person. If the person was added by mistake, select **Remove person** in the banner to remove them.

Add an unknown person

An unknown person is someone who cannot be identified or described. For example, if a car is broken into with no witnesses, the person who committed the break-in would be considered an unknown person.

To add an Unknown person to a report:

1. Select **Add name > Unknown person**.
2. Fill out the **Role** this person played and provide any other information you can.

Note

Unknown persons are not added to the database, which means they will not appear in searches and can't be added to other reports.

Add a person from NCIC

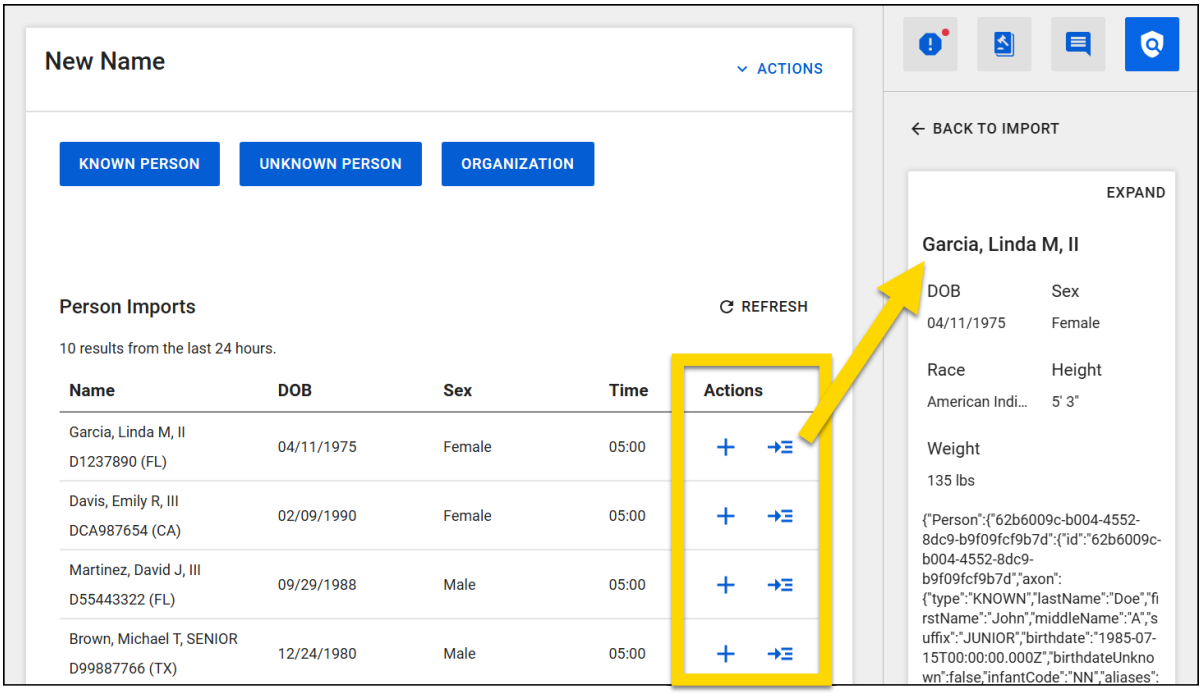
Note

The NCIC integration is currently only available for select organizations. Contact Axon Support or your Axon representative for more information about integrating with your NCIC search provider.

To add a person from NCIC search to your report:

1. Export the person from your NCIC search application to make their name appear in the Person Imports table in Axon Standards.
   - This table includes person imports, typically from the previous 24 hours. Imports made prior to this timeframe are removed from the table. Select **Refresh** to refresh the list.
     - You may see a timeframe other than 24 hours, depending on how your organization's NCIC integration is configured.
   - Depending on your organization's integration and configuration settings, people imported from NCIC may take a few minutes to appear.
2. Select the arrow icon in the **Actions** column to view additional details about them in the side panel.
   - The person’s basic information, including DOB, sex, race, height, and weight is displayed at the top (if available).
   - Additional data about the person appears below these details. This information comes directly from your NCIC search provider and may contain raw code.

3. Select the plus icon in the **Actions** column to add a person to your report.



4. When you select the plus icon, the system searches to see if that person already exists in the database.
   - The search fields are auto-filled using the information from your NCIC provider.
   - Potential matches from the database appear below the search fields.
   - Select a result to open a profile preview pane and view more information.
5. If a profile matches the person you want to add to the report, select **Import and update** at the bottom of the pane.
6. If you do not find a matching profile, select **New person** below the list of search results.
   - A new person profile is created, and the information from your NCIC provider is auto-filled into the person fields in the report.

Add and update person information

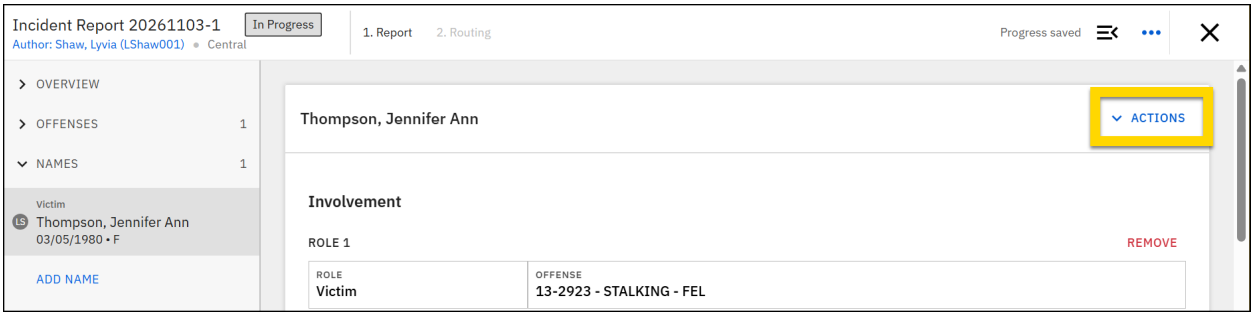
When adding a person to a report (whether creating a new person or updating an existing one), various fields are revealed where you can record information about them. This information is also added to their profile, which displays all information about the person, including their involvement with any other reports, people, vehicles, etc. The fields vary by report type, but some common fields include:

- **Involvement:** Description of the person's role in the report.
- **Identity details:** Full name, date of birth, and other relevant identifiers.
  - The **Age** field shows the person's age at the time of the report, regardless of their current age. If the report does not have a recorded date, the **Age** field shows the person's current age.
  - People who are added to reports also appear on event/case profiles. The person information shown on these profiles is the person's information at the time of the incident, which may be different from that person's current information.
    - For example, at the time of Event 123456, the victim's name was Debbie Miller. Two years later, her name changed to Debbie Smith. The profile for Event 123456 displays "Debbie Miller," the name recorded at the time of the event, even after her name changes.
- **Description:** Details such as height, weight, hair color, eye color, and distinguishing marks.
- **Contact information:** Current address, phone number, and email, if available.
- **Additional forms:** Add any forms that may be required, such as an arrest.

Once the report is submitted, the information provided in the report immediately appears on their profile.

After adding a person to a report, open the **Actions** menu in the top right corner of that section of the report to take one of the following actions:

- Remove the person from the report
- View their profile (see Citizen profiles).
- Add a flag to their profile (see Manage flags).
- Add and manage restrictions on that section of the report (see Partial restrictions).

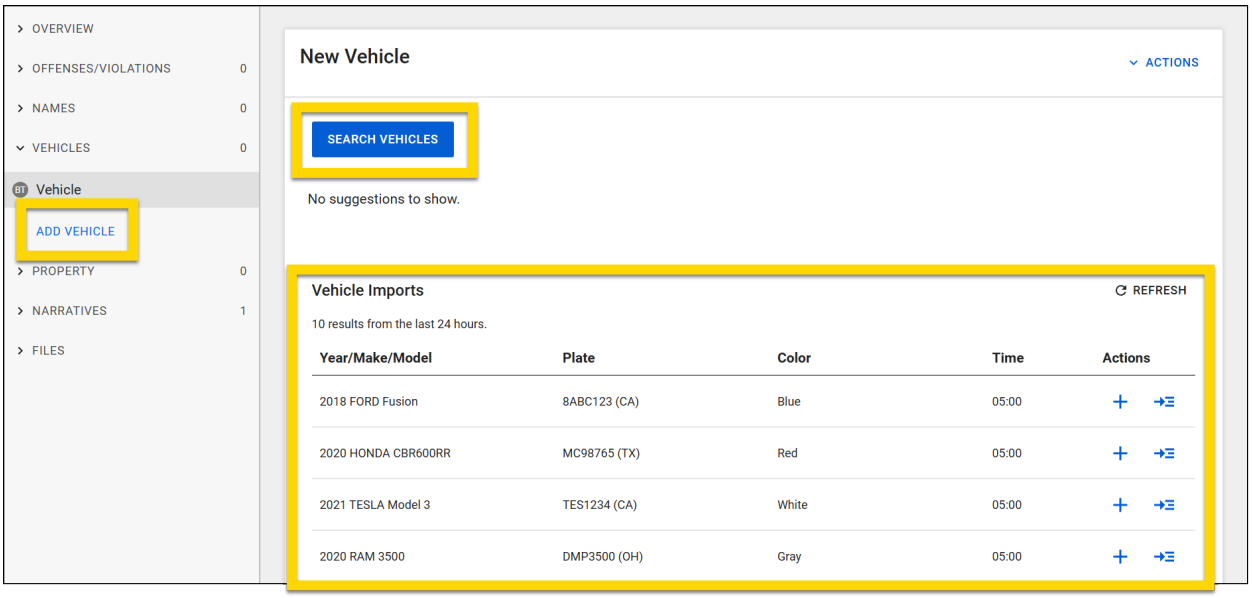


Vehicles

To add a vehicle to your report, select **Vehicles > Add vehicle** in the report navigation menu.

From this screen, you can search for an existing vehicle or create a new one. If your organization has integrated with your NCIC search provider, you can also view the vehicles you exported from NCIC and add one to your report.

Once a vehicle has been added to a report, you can add and update its information.



To search for an existing vehicle, or to add a new vehicle, take these steps:

1. Select **Add vehicle**.
   - This button may differ depending on the type of report you are writing.
2. To avoid creating duplicate vehicle profiles, search to see if the vehicle already exists in the database rather than automatically creating a new one.
   - Search by license plate, make, model, or VIN. Wildcard operators are not supported in the search box.
   - Potential matches from the database appear below the search fields as you enter information.
   - Select a search result to open a profile preview pane and view more information.
3. If your organization has integrated with your NCIC search provider, you can also search for vehicles you imported from NCIC.
4. If a profile matches the vehicle you want to add to the report, select **Import and update** at the bottom of the pane.
5. If a profile does NOT exist for the vehicle you want to add to the report, select **New vehicle** below the list of search fields.
   - If you search for an existing vehicle using a license plate number and must create a new vehicle, the license plate you searched for is entered in the report.

Add a vehicle from NCIC

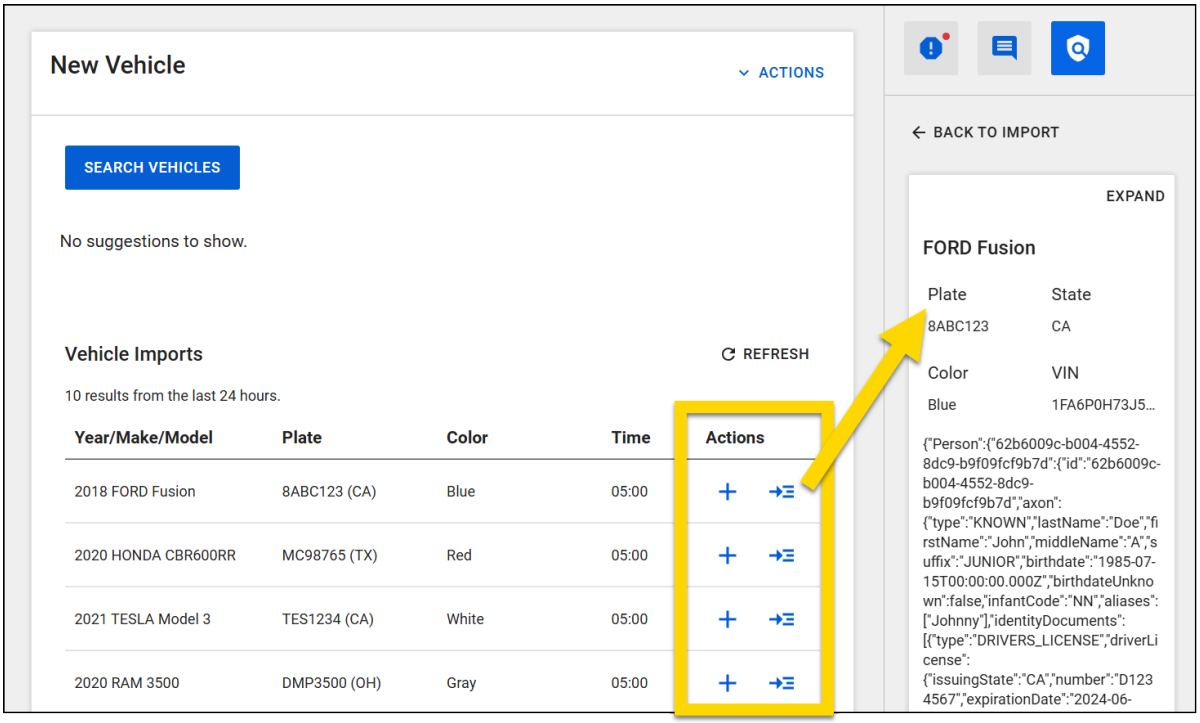
Note

The NCIC integration is currently only available for select organizations. Contact Axon Support or your Axon representative for more information about integrating with your NCIC search provider.

To add a vehicle from NCIC search to your report:

1. Export the vehicle from your NCIC search application to make their name appear in the Vehicle Imports table in Axon Standards.
   - This table only includes vehicle imports, typically from the previous 24 hours. Imports made prior to this timeframe are removed from the table. Select **Refresh** to refresh the list.
     - You may see a timeframe other than 24 hours, depending on how your organization's NCIC integration is configured.
   - Depending on your organization's integration and configuration settings, vehicles imported from NCIC may take a few minutes to appear.
2. Select the arrow icon in the **Actions** column to view additional details about the vehicle in the side panel.
   - The vehicle’s basic information, including plate, state, color, and VIN is displayed at the top (if available).
   - Additional data about the vehicle appears below these details. This information comes directly from your NCIC search provider and may contain raw code.

3. Select the plus icon in the **Actions** column to add a vehicle to your report.



4. When you select the plus icon, the system searches to see if that vehicle already exists in the database.
   - The search fields are auto-filled using the information from your NCIC provider.
   - Potential matches from the database appear below the search fields.
   - Select a result to open a profile preview pane and view more information.
5. If a profile matches the vehicle you want to add to the report, select **Import and update** at the bottom of the pane.
6. If you do not find a matching profile, select **New vehicle** below the list of search fields.
   - A new vehicle profile is created, and the information from your NCIC provider is auto-filled into the vehicle fields in the report.

Add and update vehicle information

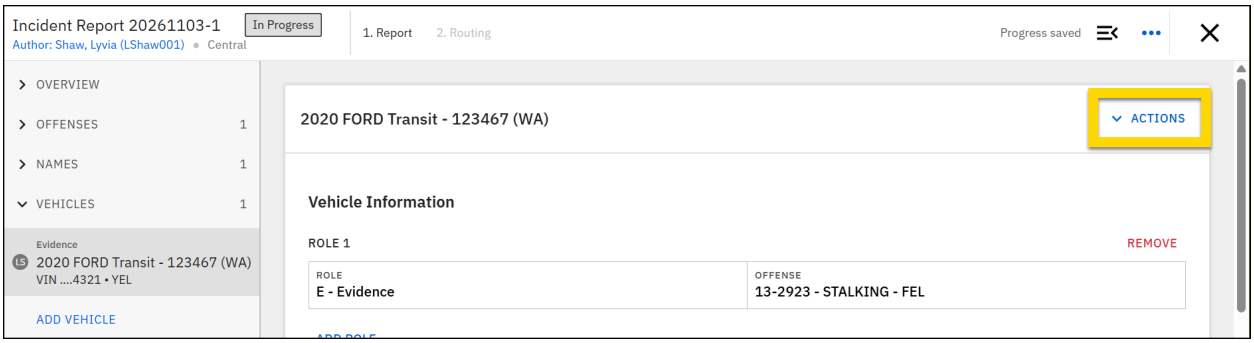
After adding a vehicle to a report (whether creating a new vehicle or updating an existing one), various fields are revealed where you can record information about it. This information is also added to the vehicle profile, which displays all information about the vehicle, including its involvement with any other reports, people, vehicles, etc. The fields vary by report type, but some common fields include:

- **Involvement:** Description of the vehicle's role in the report
- **Vehicle details:** Make, model, year, description, and other relevant identifiers
- **Description:** Details such as height, weight, hair color, eye color, and distinguishing marks.

- **Relationships:** Information about any relationships the vehicle has with other vehicles, individuals, etc. involved in the report.

After adding a vehicle to a report, open the **Actions** menu in the top right corner of that section of the report to take one of the following actions:

- Remove the vehicle from the report
- View the vehicle profile (see Vehicle profiles).
- Add a flag to the vehicle (see Manage flags).
- Add and manage restrictions on that section of the report (see Partial restrictions).



Units

Add a unit to a report by selecting **Add unit** in the report navigation menu. Enter unit information and add any officers who were drivers or passengers during the vehicle pursuit and any injuries they sustained.

Note

Officers added to the **Unit** section are NOT automatically added to the Officers section of the report.

Officers

To add an officer to a report, select **Add officer** in the report navigation menu. Type the officer's name in the **Officer/Employee number** field to search the list of officers at the agency.

Select the officer's role (Involved, Complaint, Complainant, Witness).

Depending on the report type, additional fields may be included to let you document additional information about the officer's role in the event.

Response actions

The Response Actions section appears primarily in the Response to Resistance report. This report can help organizations track both how an officer perceived a situation, as well as how they reacted to it.

The Response Actions section lets you document all actions by all parties involved in the event. If multiple officers or subjects were involved, you should add multiple Response Actions.

To complete this section, select **Add response action** in the report navigation menu and document:

- Who was in immediate threat of harm (citizen, officer, self, or none)
- Involved officer
- Force used against (animal or person)
- Subject actions

Add force

Selecting **Add force** reveals additional fields that let you provide information about the force used:

- **Force type**
  - Based on the type selected, additional fields will appear specific to that force type.
  - For example, selecting **TASER CEW** reveals additional fields for you to provide information about the TASER, including the CEW model, action, and serial number.
- **Force level**
- **Force objective**
- **Force type details**
- **Force location**
  - Selecting a location on the interactive body outline reveals additional fields for the detailed location, number of impacts, and severity of injury from the direct force.
  - Select **Add force location** to document multiple locations for the same force action.
    - For example, the show of force was probes deployed from a TASER, and the probes contacted the subject's lower back and buttock.
  - Document the effectiveness and issues limiting the effectiveness of the force.

Each response action can include multiple uses of force. For example, an officer used her hands to grab and hold a subject, and eventually used her TASER. In this case there would be two uses of force for the same response action. Select **Add force** to document such additional force actions.

Add injuries sustained without direct force

Use this report to document injuries that didn't result from direct impact of the force used, but were a byproduct of the force application. For example, an officer used his TASER and hit the abdomen and right leg of a subject, but caused no injury in those areas. However, the subject fell and hit his head, resulting in a moderate injury.

Select **Add injuries sustained without direct force** to reveal an interactive body outline where you can report such injuries. Selecting an injury location reveals additional fields for the detailed location, number of injuries, injury severity, and details. Select **Add Injury Location** if additional locations are needed.

Select **Add injuries sustained without direct force** to add additional injuries.

Narratives

To add a narrative to a report, select your name or **Narrative** from the Narratives section in the report navigation menu. This section name may vary by report type.

There are several ways to add content to the text field:

- Type directly into the report
- Copy and paste information from another location
- Add inline images
- Import and update a template
- Dictate text
- Generate a draft using Draft One

> **Note**
>
> When Draft One is used in Axon Records and Axon Standards, it includes any data you have already entered into the fields in the rest of the report. To create comprehensive and higher-quality drafts, it is recommended to fill out all report fields BEFORE using Draft One.

After text has been entered into the field, use the toolbar to format the text as desired, including headings, font size/color, lists, and more. Select **Actions > Find and replace** to quickly bulk change certain words.

Add inline images

You can insert images directly inline inside your narrative. The images must first be attached to the report as evidence items. Once inserted in the narrative, you can resize the images. When printing, you can choose whether or not the images should be included.

To add an image to a narrative:

1. Follow the steps in the Files section below to add the file to the report.
2. Place your cursor in the narrative field where you want to insert the image.
3. Select the image icon in the narrative toolbar.
4. When the Add image evidence pane opens, use the checkboxes to select one or more images for insertion.
   - Use the arrows to expand the row and view the image.
5. After choosing one or more images, select **Insert** at the bottom of the pane.
6. After the image appears in the narrative field, hover over it to reveal the **More actions [...]** menu in the top right corner of the image.
7. Open the **More actions [...]** menu to change the image size (small, medium, or large) or to remove the image from the narrative.
   - Images removed from the narrative are NOT also removed from the report. To remove the image from the report, open the Files section and remove it.

Import a template

Your organization may have templates available that you can follow to ensure your narrative adheres to organization policy. Select the **Templates** button below the narrative toolbar to open a list of available templates. Choose an option and select **Import**. The template, which contains formatted text, will import into your narrative, where you can update with details for your report.

Dictate

You can write report narratives by speaking instead of typing. While dictating, filler words like “um,” “uh,” and “ah” are removed automatically.

For the best dictation results:

- Speak Clearly: Articulate your words and speak directly into the microphone.
- Use a Quiet Environment: Dictate in a quiet setting to reduce transcription errors.
- Use Verbal Commands: Learn to use voice commands for punctuation and formatting to increase efficiency and accuracy.
- For complex terms or names, you may want to type directly into the report narrative rather than dictating.

Follow these steps to dictate:

1. Place your cursor in the text editor wherever you want the dictated text to appear.
2. Select **Start dictation**.
   - If prompted, allow your web browser to access the microphone.
3. Begin speaking, including the voice commands for punctuation
   - Text appears in the narrative text editor as you speak.
   - Refer to the **Dictation guide** tab below the narrative text editor for a reminder of the voice commands.
4. Select **Stop dictation** when you finish.
   - You can restart dictation again at any time. Be sure to place your cursor in the location you want the text to appear.

Voice commands

Add punctuation and formatting as you dictate to reduce editing afterward by speaking the following commands:

- **Period (.)**: Say "period" or "full stop" to end a sentence.
- **Comma (,)**: Say "comma" to insert a comma.
- **Question mark (?)**: Say "question mark" to end a sentence with a question.
- **Exclamation mark (!)**: Say "exclamation mark" for emphasis.
- **Parentheses ()**: Say "open parentheses" to begin and "close parentheses" to end a parenthetical statement.
- **Quotes (")**: Say "open quotes" to start a quote and "close quotes" to end a quote.
- **New paragraph**: Say "new paragraph" to start a new paragraph.
- **New line**: Say "new line" to move down one line without starting a new paragraph

Find a list of these voice commands in the **Dictation guide** tab below the narrative text editor.

Requirements

Before using dictation, ensure you meet the following criteria:

- **Axon Evidence Pro license**: You must be able to access Axon Evidence and have a Pro license.
- **Microphone**: Your device needs a functioning microphone. Grant your web browser permission to access the microphone if prompted.
- **Speech-to-text connection**: Ensure your device can connect to **.stt.speech.azure.us** (in the United States) or **.stt.speech.microsoft.com** (in Canada). You may need to work with your agency's IT department to ensure access.

Files

Add photos, videos, documents, and other files to a report by selecting **Files > Upload file** in the report navigation menu.

The **Suggested** tab contains recommendations for evidence you may want to add to the incident. Evidence is suggested based on the following criteria:

- Any Evidence ID that matches the ID of a case, incident, report, or the CFS ID
- Evidence you uploaded in the past 72 hours that hasn't been added to the report

Use the search fields to find specific evidence within the suggestion list and the checkboxes to add multiple files at the same time.

To add new files, switch to the **Upload** tab and either drag and drop files from your computer or select **Chose files**. After selecting the files, you can optionally add a description, update the title of each file, and update the category of each file. The categories and that appear in the dropdown menu are the same as those that appear in Axon Evidence.

The **Search** tab lets you search for evidence that has already been uploaded to Axon Evidence. Use the search fields to find specific evidence and the checkboxes to add multiple files at the same time.

When you select a file's title, an evidence preview pane opens and displays additional information about the file. Depending on the file type, this pane may include multiple tabs:

- **Overview:** This tab shows the same metadata that appears on the Overview tab of the Axon Evidence details page, as well as a transcript summary (if available).
  - See Evidence details page for more information.
- **Transcript:** This tab only appears for audio and video files and behaves the same as the Transcript tab on the Axon Evidence details page.
  - See Transcripts on the evidence details page for more information.
- **Moments:** This tab shows AI-detected key moments (e.g., Miranda Rights) within a piece of evidence with timestamps.
  - See Brief One Transcripts for more information.

> **Note**
>
> This tab only appears for customers who have purchased Brief One. Contact Axon Support or your Axon representative if you are interested in purchasing this product.

To view the full evidence details page in Axon Evidence, select **Details page** at the bottom of the pane.

After adding the files to the report, use the checkboxes to select one or more files then select **Edit metadata** in the top right corner to update (add or remove) the tag or category for the files. The categories and tags that appear in the dropdown menus are the same as those that appear in Axon Evidence.

Select **Actions > Remove** to remove a file from the report.

If other files have been added to the event associated with the report, you can select the **View Files to this Event** button below the list of files to open the event profile and view all files associated with the event.

Assign and reassign tasks and authors

Users belonging to Command Hierarchy groups and/or teams with certain privileges can assign and reassign authors and tasks.

Task assignment options vary depending on the type of task (Write, Review, etc.) as well as the inbox a task is accessed from.

To understand assignment and reassignment, it's helpful to understand these terms:

Task

A task indicates work that needs to be completed on a report. A task is created each time a report is submitted, approved, or rejected. Task types include:

- View: Reports or case tasks that can be viewed but not edited because they are currently in review or already finalized
- Do: Case tasks assigned to you
- Write: Reports assigned to be created and not yet submitted
- Revise: Reports previously submitted for approval but returned by the report reviewer for corrections (the report author receives an email when a report they submitted is returned)
- Review: Reports submitted for review
- Rereview: Reports rejected by the report reviewer, then updated and resubmitted by the author

See Reassign case tasks for additional information about reassigning Do tasks that have been created for a case.

Report

The "thing" that is created, reviewed, and finalized. A report is also referred to as a *document* or *form*. Reports are made up of various sections that contain fields and information(person, vehicle, narrative, etc.).

Author

The person who originally creates a report. An author is also sometimes called the *primary contributor*.

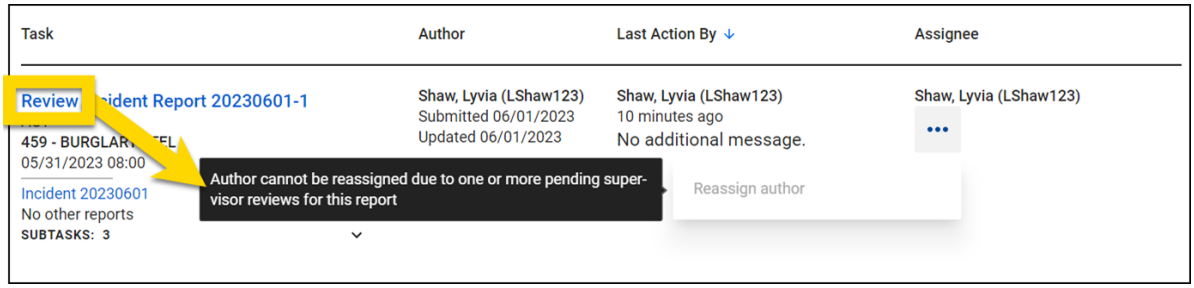
Reassign Write and Revise tasks

To reassign a Write or Revise task, take these steps:

1. Find the task in a task inbox.
2. Select **More Actions [...] > Reassign author**.
3. Enter a name or Badge ID, set the urgency of the task, and provide notes.
   - Unlike Review or Rereview tasks, which can be left unassigned, you must specify a new author for Write and Revise tasks.

Note

The report must be in Write or Revise status for the author or contributor to be reassigned.

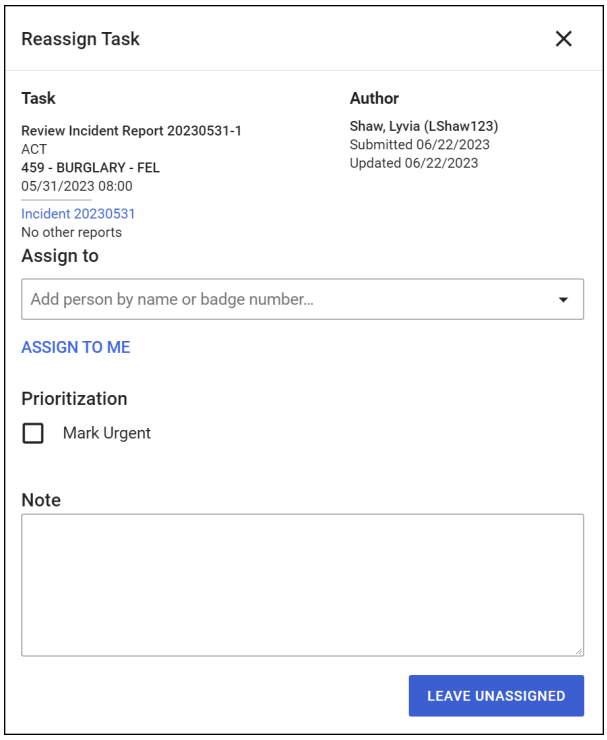


Assign and reassign Review and Rereview tasks

To assign or reassign a Review or Rereview task, take these steps:

1. Find the task in a task inbox.
2. Select **Assign** or **Reassign**.

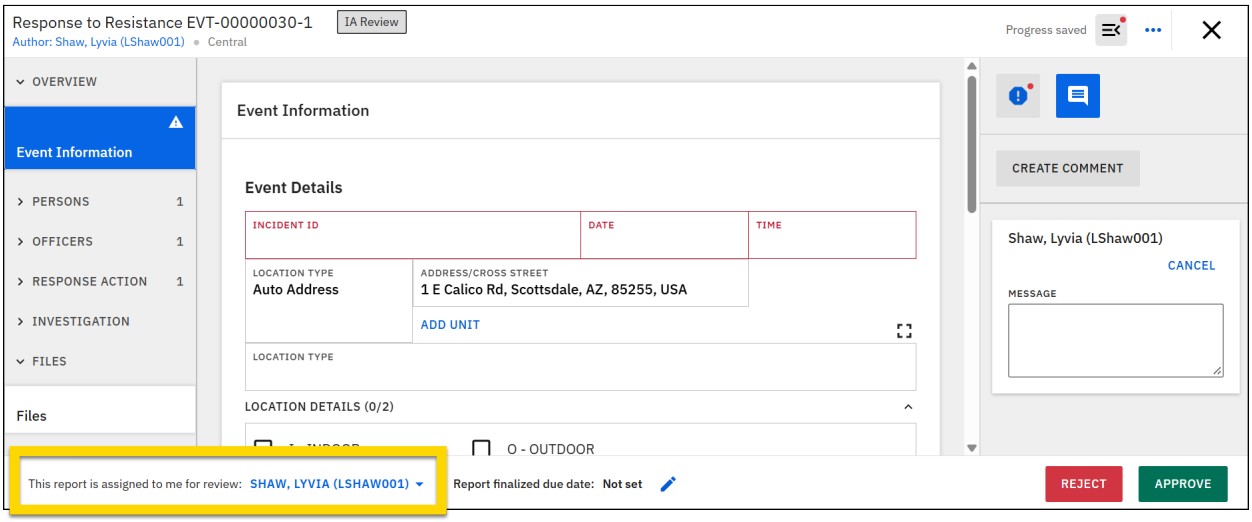
3. Enter a name or Badge ID of the new reviewer, set the urgency of the task, and provide notes.
   - Unlike Write and Revise tasks, Review and Rereview tasks can be left unassigned.



Note

Reassigning a Review task does NOT reassign the author or contributor. Instead, it reassigns the person who is reviewing the report.

Review and Rereview tasks can also be assigned and reassigned from the assignment menu in the Report Writer footer.



Assign and reassign from the Agency Tasks inbox

The Agency Tasks inbox shows all reports at the entire organization. Tasks can be assigned or reassigned from the **In Progress** tab in this inbox. Tasks can't be assigned or reassigned from the **Recently Finalized** tab.

You can reassign tasks from the **Actions** column. Different assignment and reassignment options appear depending on the task type:

- Write or Revise tasks: **More Actions [...] > Reassign author**
- Review or Rereview tasks: **Assign** or **Reassign** buttons

Assign and reassign from the review inboxes

In the **Chain of Command, IA Review Tasks,** and **IA Investigation Tasks** inboxes, the assignment and reassignment actions for Review and Rereview tasks appear in the **Task** column.

Event and case profiles

An event profile opens when you select an event from Events search, a task inbox, or the More actions menu of a report associated with the event. If a case is created from the event, the event profile becomes a case profile that contains additional information and options.

Event profiles

An event profile is created as soon as the first report in the event is started. The profile is updated in real-time as the report is completed. The top portion of an event profile displays basic information about the event, including the date/time it was created and who created it. If the incident contains any restrictions, this label appears at the top of the profile.

While the report is in progress, a Draft label appears at the top of the event profile. This draft label remains until the report is finalized. If additional reports are created for the

event after the original report is finalized, the Draft label reappears on the event profile until the additional reports are finalized.

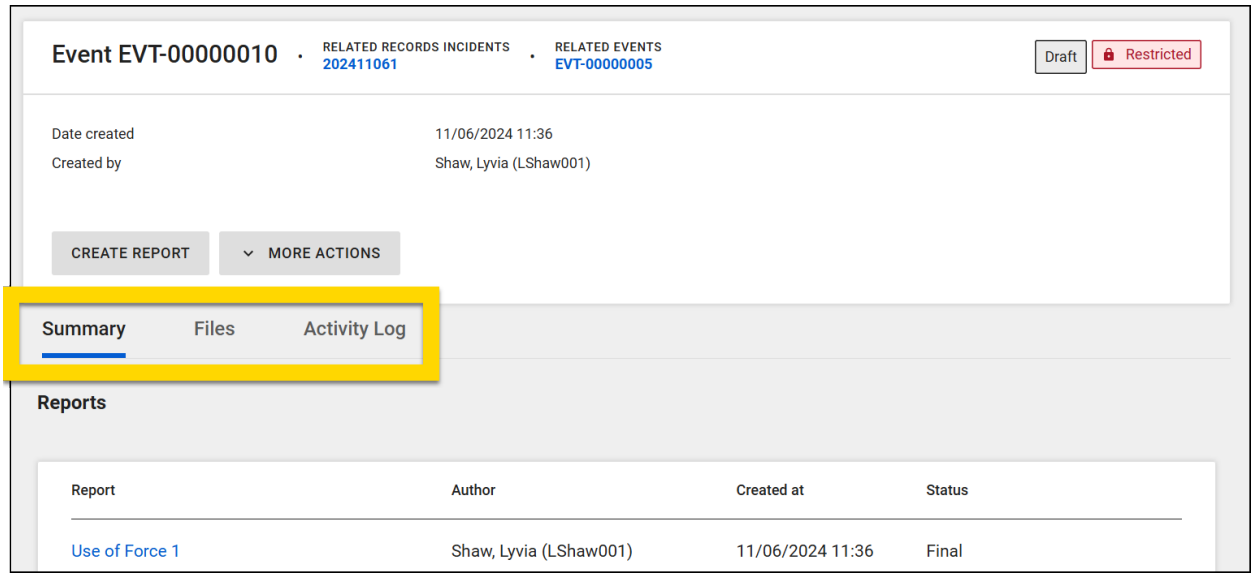


From this top section of the profile, you can take the following actions:

- Select the blue hyperlinks beside the Event ID to open related incidents and events.
- Use the gray button create a new report for the event.
- Open the **More actions** menu to take additional actions:
  - Add file
  - Link related incident reports and standards events
  - Manage restrictions
  - Create case
  - Print event

Below the top heading section, you can switch among the tabs to view information and take various additional actions:

- Summary: View a report, person, vehicle, or officer. Select one to open the corresponding profile.
- Files: Mange all files that have been added to the incident, either to the incident report or directly to the incident.
- Activity Log: Manage the log of all actions taken on the event.



Case profiles

When a case is created for an event, the event profile becomes a case profile, which shows additional information and actions. The case profile is the primary workspace for investigators. It consolidates all information related to the case--reports, tasks, evidence, activity history--in a single view.

For full details about the additional functionality of case profiles, see Cases.

Summary tab

The **Summary** tab displays all information and reports associated with the event and is broken into the various sections detailed below.

Reports

The **Reports** section contains links to all reports associated with the event. The original report that started the event is listed first, with all others appearing after it.

Officers

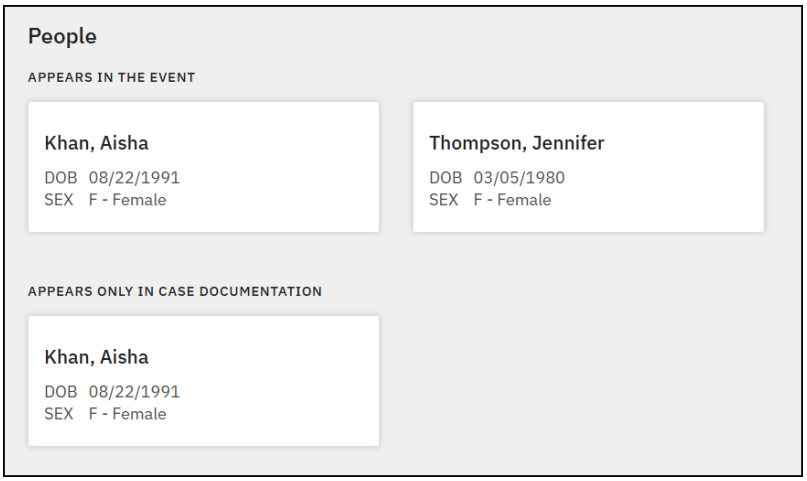
This section displays all officers that have been added to any reports associated with that event. Selecting an officer from the event profile opens the officer's profile page.

People

The **People** section contains all people who have been added to any of the event's reports or case documentation (if a case has been created for the event). When it has been added to a report, basic information about each person is displayed, including name, DOB, and sex.

The information for each person reflects data that was accurate at the time the report was written. When viewing a past event, this information may not match the person's current details. For example, at the time of the event, the victim's name was Debbie Miller. Two years later, her name changes to Debbie Smith. The event profile displays "Debbie Miller," the name recorded at the time of the event, even after her name changes.

On case profiles, if a person, organization, or vehicle that doesn't already appear in one of the event reports is added to a case task or case document, it appears in its corresponding section under the label, Appears only in Case Documentation. These parts of a case profile will only appear to users who have the appropriate privileges to view case-related information.



Vehicles

The **Vehicles** section contains all vehicles who were added to the event reports and case documentation (if a case has been created for the event).

Files tab

All files that have been added directly to an event or to reports associated with that event appear on the **Files** tab of event profiles.

See Evidence and file management for more information.

Activity Log tab

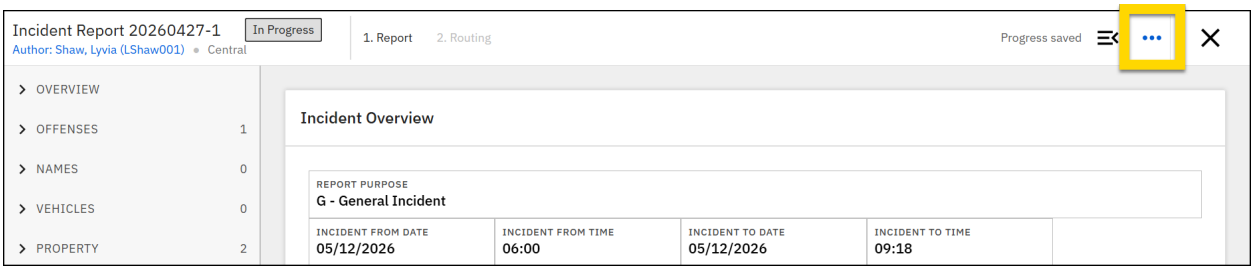
The **Activity Log** tab includes all activities performed on that event (e.g., report created, finalized, files added, etc.).

See Activity log management for more information.

Additional actions

Once a report, event, or case has been created, you can take various management actions from the **More actions [...]** menu in the top right corner of the report, including:

- Print
- Link related items
- View report history
- Copy information between reports



Print reports

Users with the appropriate privileges can print reports, incidents, events, and cases.

To print a single report:

1. Open the report in Report Writer.
2. In the top right corner of the report header, select **More actions [...] > Print report**.
   - Based on your organization's configuration, reports may have multiple print options, which each include different information from the report.
3. Adjust the following settings. Note that some of these options may not appear for certain report types, and users must have certain privileges to adjust these settings.
   - **Print as a DOCX file:** Select this checkbox to print the report as a DOCX file rather than a PDF. Contact your Axon representative for more information about this feature.
   - **Settings**: Choose whether to include narrative images, restricted information, or the approval log in the printout.

- **Header:** Can be omitted, appear on all pages, or appear on just the first page.
  - When you include a header in your printout, your organization's logo appears in the top right corner. This logo can be managed from your Organization Profile in the Axon Evidence Admin Console.
- **Footer:** Can be omitted, appear on all pages, and optionally include page numbers.

4. Provide **Auditing details**, which include recipient details and the purpose of the print.
5. Select **Next**.
6. If you need to redact anything before printing, select **Yes** then **Start redaction**. If you are not redacting anything, select **Print**.
   - See Redaction for more information.
7. The file loads in a new browser tab where you can download and print it.

When you include a header in your printout, your agency's logo appears in the top right corner. This logo can be managed from your Agency Profile in the Axon Evidence Admin Console.

Print events, cases, and investigations

To print an event, case, or investigation, follow these steps:

1. Open the case or investigation profile.
2. Open the **More actions** menu and select:
   - Events and cases: Print event
   - Investigations: Print investigation
3. In the **Documents** section, indicate which content to include:
   - For events, you can include:
     - Event reports: Indicate which reports to include.
     - File list: If selected, a list of all file names that have been added to the case are included in the printout.
     - Activity log: Includes all actions taken on the event.
   - In addition to the items listed above, for cases or investigations, you can include:
     - Case or investigation summary
     - Case or investigation documents
     - Tasks
       - Indicate if the printout should include a list of case tasks, or details for each task.
       - Optionally include incomplete tasks.
       - Set the order in which the tasks should be listed in the printout. Sort options include Task, Assignee, Status, Created at, Due date, and Completed at.

4. In the **Settings** section, optionally adjust the following items. Note that users must have certain privileges to adjust these settings.
   - Show table of contents: Includes a list of all sections in the printout with a header that gives basic details about the case.
   - Show images in narratives: Includes images that have been inserted inline into the narratives.
   - Show restricted information: If restrictions have been applied, this option includes restricted information that you have privileges to view. Optionally include this restricted information on a separate page.
   - Show approval log: Details of the report approval process.
   - Start each narrative on a new page: Inserts a page break at the start of each narrative.
5. Adjust the **Header** and **Footer**:
   - **Header:** Can be omitted, appear on all pages, or appear on just the first page.
     - When you include a header in your printout, your organization's logo appears in the top right corner. This logo can be managed from your Organization Profile in the Axon Evidence Admin Console.
   - **Footer:** Can be omitted, appear on all pages, and optionally include page numbers.
6. Provide **Auditing details**, which include recipient details and the purpose of the print.
7. Select **Next**.
8. Use the **Sort reports and documents by** and the **Order** fields at the top to set the order in which items appear. Sort options include:
   - Document type
   - Name (if custom names have been created for any of the items)
   - Date and time created
9. Select **Next**.
10. If you need to redact anything before printing, select **Yes** then **Start redaction**. If you are not redacting anything, select **Print**.
    - See Redaction for more information.
11. The file loads in a new browser tab where you can download and print it.

Link reports to an incident or event

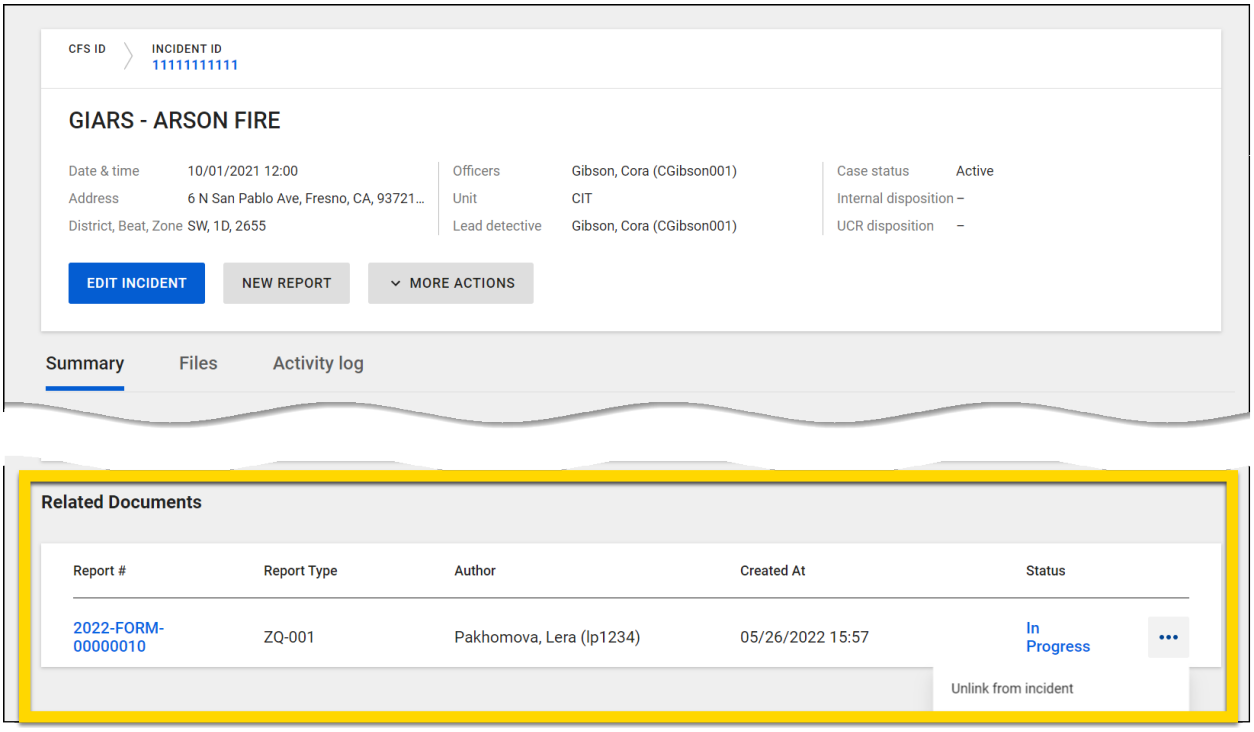
To link a standalone (non-incident report) Axon Records report, like a Field Interview, to an incident or event (if your organization uses Axon Standards):

1. Open the incident you want to link the report to and select **More actions > Link other reports**.
   - This option does not appear on Axon Standards event profiles. Instead, link a report to the event by opening the report in Report Writer (explained below).
2. Use the search box to search for the Report ID of the document you want to link.
3. Select **Link**.

You can also perform this action while viewing the report:

1. Open the report in Report Writer.
2. In the top right corner of the report header, select **More actions [...] > Manage related incidents**.
3. Search for the incident or event (if your organization uses Axon Standards).
4. Select the incident or event you wish to link and press **Enter** on your keyboard to create the link.
   - Linked incidents and events appear below the search bar.
5. Select **Save** to finalize your changes.

Linked reports appear at the bottom of the incident profile in the **Related documents** section. Unlink a report by selecting **More actions [...] > Unlink from incident**.



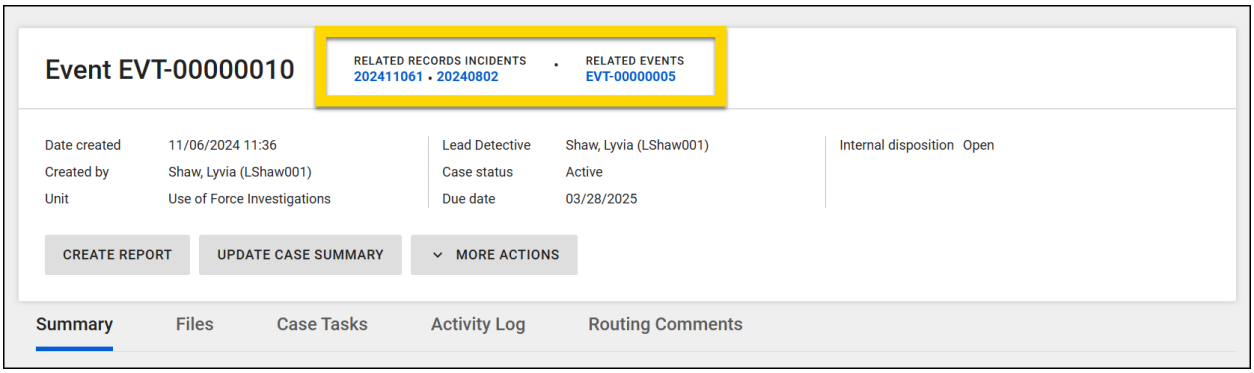
You can also remove a link by opening the report in Report Writer, selecting **More actions [...] > Manage related incidents**. Select **Unlink > Save**.

Link incidents and events

To link related events, or to link an incident to an event (if your organization uses both Axon Records and Axon Standards):

1. Open an event and select **More actions > Link related events**.
   - If your organization uses both Axon Records and Axon Standards, this option appears as **Link related incident reports and Standards events**.
2. Enter the Incident or Event ID you want to link to in the search box.
3. Select the incident or event you wish to link and press **Enter** on your keyboard to create the link.
   - Linked incidents and events appear below the search bar.
4. Select **Save** to finalize your changes.

Related incidents and events appear at the top of the profile. Select the blue ID to open that profile in a new browser tab.



To remove links, select **More actions > Link related events.** Select **Unlink** to remove a link, then **Save** to finalize your changes.

View report history

To view a log of all actions taken on a report, select either the author name in the top left corner or **More actions [...] > View report history** in the top right corner.

Use the **Sort by** drop-down to change whether the audit log displays actions chronologically or broken out by contribution. Select **Export CSV** to export the report history to a CSV file, which includes each action and its timestamp.

Copy information to new reports

You can copy report information from an existing report into a new one. Information can be copied between different report types (e.g., from a Vehicle Pursuit report to a Vehicle Collision report).

This feature can only copy information from an existing report to a new report if the fields in both reports are named and configured the same way. For example, if the **Location type** field in the existing report is a dropdown field, the **Location type** field in the new report must also be a dropdown field (with the same name).

Note

If your organization uses both Axon Records and Axon Standards, you can only copy information within the same database. For example, you can copy information from an Axon Standards reports to a new Axon Standards reports, but you cannot copy information from an Axon Standards report to an Axon Records report.

To copy information into a new report:

1. Open the existing report.
2. In the top right corner of the report header, select **More actions [...] > Copy info to new report**.
3. Choose the type of report you want to create.
   - The new report will be added to the same event as the report you are copying from and appear in the **Reports** section on the event profile.
4. Select **Preview info**.
5. Use the checkboxes to select which information will be copied into the new report.
   - Some sections will be grayed-out and unselectable if a corresponding section does not appear in the new report (e.g., The existing report has a Vehicles section, but the new report you selected does not.).
6. Select **Create report**.
7. The new report opens in a new tab where you can review the copied information and complete all remaining fields.

Share reports

You can share a report by sending a message to specific people, Command Hierarchy groups, or teams. Reports created in Task inboxes can be shared, along with documents created in other modules (Case Management, Warrants, Permits, Bookings, etc.).

Share recipients receive an email as well as a notification in the Notification Center. See Notification Center for more information.

Note

Users must have the Share report privilege before they can share reports. There are separate Share report privilege for Axon Records and Axon Standards, which give administrators granular control over which reports can be shared.

You can share a report at any time from within Report Writer or when submitting it for review or finalization.

To share a report from within Report Writer:

1. Open the report in Report Writer.
2. Select **More actions [...] > Share report**.
3. In the **Recipients** field, select one or more individual users, Teams, or Command Hierarchy groups.
   - You can combine multiple recipient types in the same share.
4. Optionally, enter a message. This message is included in the notification the recipient receives.
5. Select **Share**.

To share a report while submitting it:

1. Open the report in Report Writer.
2. Select **Submit**.
3. On the report's routing screen, in addition to selecting a routing destination, marking the report urgent, or adding a note, select the **Share the report with others** option.
4. Enter recipients and an optional message, as described above.
5. Select **Submit**. The report is submitted and shared at the same time.

The recipients receive an email as well as a notification in the Notification Center. See Notification Center for more information.

Sharing restricted reports

If you share a restricted report with a person who does not have the necessary privileges to view reports where that restriction has been applied, they will not be able to open and view the report.

For more information about restrictions and restriction privileges, see:

- Restrictions
- Restriction privileges

Share history

To see if a report has been shared before:

1. Open the report in Report Writer.
2. Select **More actions [...] > Share report**.
3. Switch to the **View share history** tab.

A table lists each share, including the following information:

- Shared by
- Shared at (date and time)
- Recipients (the total number of users, groups or teams)

Select **Details** to view full information about the share, including which recipients received the share and the message that was included.

Restrictions

You can apply restrictions to an entire event or to specific report sections, such as information about a person or vehicle.

Each restriction has three privileges associated with it that control how users can access information associated with that restriction:

- **Access:** Lets users view information associated with the restriction
- **Add:** Lets users add that restriction to information
- **Remove:** Lets users remove that restriction from information

If you want a user, team, or Command Hierarchy group to view a specific item that has been restricted, but you don't want to give them access to view all items containing that restriction, you can create a restriction exception.

Restriction types and restriction exception lists are managed from the Restrictions tool in the Administrator Console.

When managing and using restrictions, you can take the following actions:

- Reports, incidents, and events
  - Restrict an entire event
  - Restrict specific information
  - Edit and remove restrictions
  - Manage restriction exceptions
- Administration
  - Manage restriction types and restriction exceptions
  - Manage restriction privileges

Restrict events

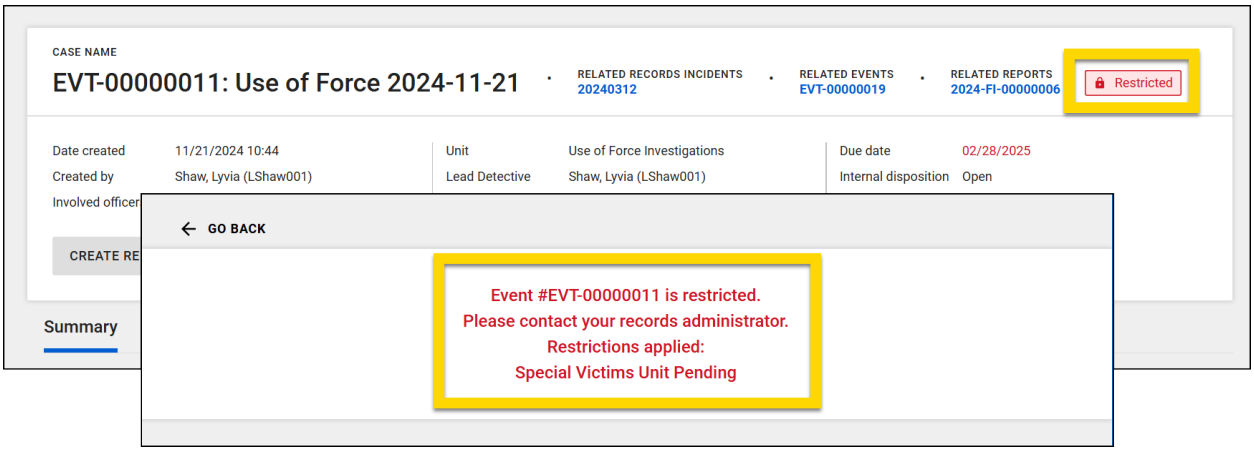
To apply a restriction to an entire event:

1. Open either the event profile or a report contained within the event.
2. Select **More actions [...] > Manage restrictions**.
3. Select **Add aestriction**.
4. Choose a **Restriction classification**.
   - You will only see restriction types for which you have the **Add** privilege.
5. Select **Entire event** from the **Information restricted** field.
6. Select **Save**.

Note

The Audit Log tool shows any unauthorized access attempts to a fully restricted item. This does not apply to items with partial restrictions.

When users with the necessary restriction privileges open a restricted item, a Restricted label is displayed at the top of the profile. Hovering over the label reveals the name of the restriction that has been applied. When users who do NOT have the necessary restriction privileges attempt to view restricted items, a message displays instead of the profile, explaining that they cannot view the item.



Partial restrictions

To partially restrict a report and make specific information in that report accessible only to authorized users:

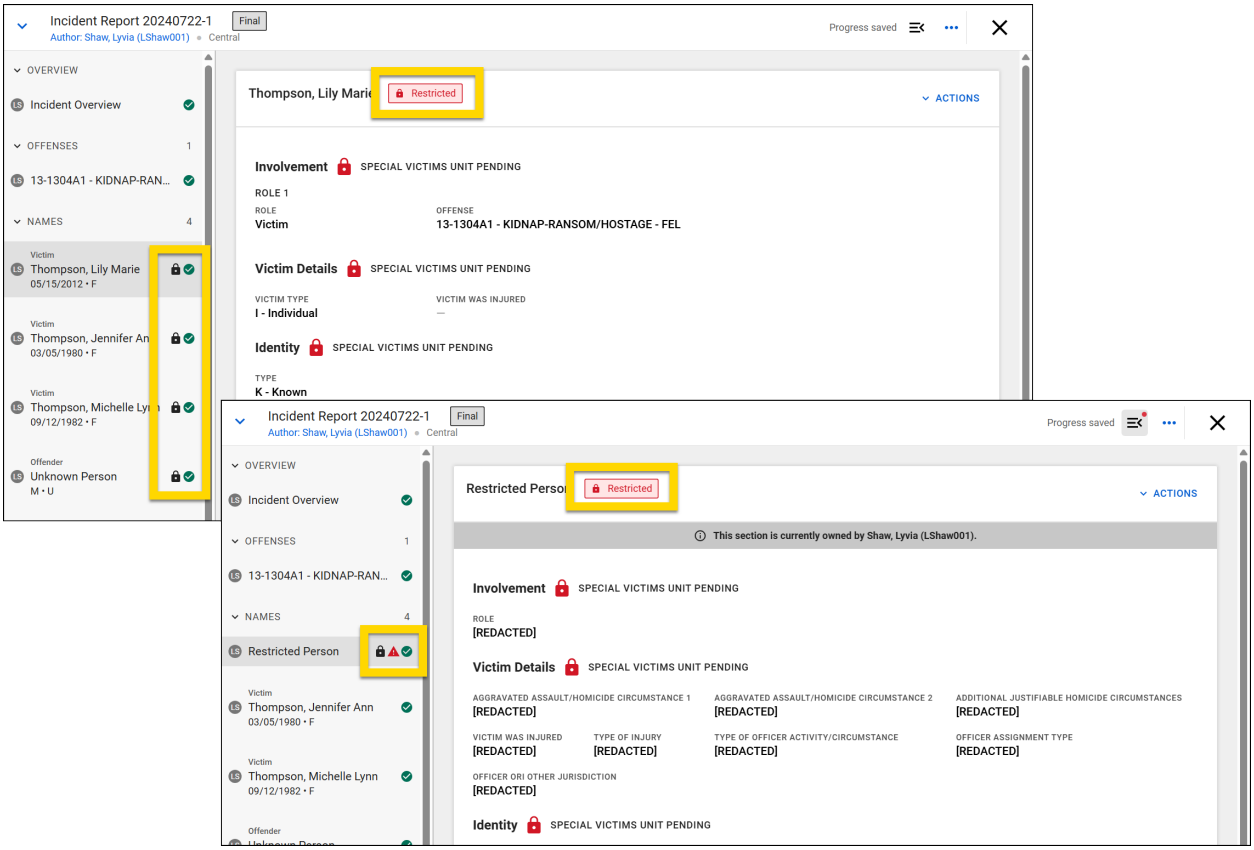
1. Open the report section you want to restrict.
2. Select **Actions > Manage restrictions**.
3. Select **Add restriction**.
4. Pick a type of restriction under **Restriction classification**.

5. Use the **Information Restricted** menu to select the exact information you want to limit access to.
   - If you select **Entire person**, any relationships between that person and any other people, vehicles, etc. are also restricted.
   - If you select **Personally identifiable information**, the restriction will apply to:
     - Name (first, middle, last, suffix)
     - Aliases
     - Date of Birth
     - Birthplace (city and state)
     - Contact information (address, phone, etc.)
     - Identification documents (driver's license, passport, etc.)
6. To add additional restrictions, select **Add restriction** again.
7. Select **Save** to apply the restrictions.

When users with the necessary restriction privileges open a restricted item, a Restricted label is displayed at the top of the section where the restriction was applied. Hovering over the label reveals the name of the restriction that has been applied. A lock icon appears beside each restricted part of the report.

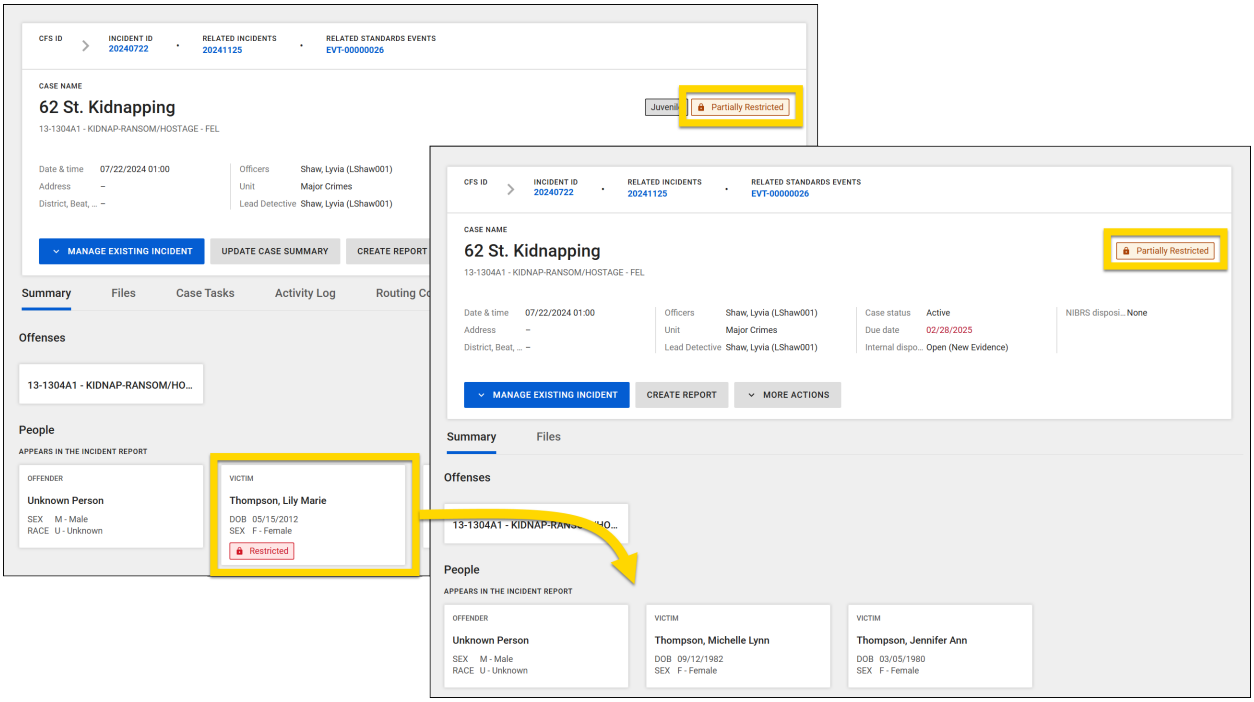
Note in the image below that although a restriction was applied to a single person, additional report sections also display a lock icon because the entire person was restricted, thereby hiding their relationships with the other people in the report.

When users who do NOT have the necessary restriction privileges attempt to view restricted sections of the report, they also see lock icons and a Restricted label. Instead of showing the restricted information in the report fields, [REDACTED] is displayed.



When users with the necessary restriction privileges open the event profile the report is associated with, a Partially Restricted label is displayed at the top. A Restricted label appears on the information that has been restricted. Hovering over the label reveals the name of the restriction that has been applied. When users who do NOT have the necessary restriction privileges attempt to view an incident profile that contains restricted

items, the Partially Restricted label appears and the restricted information is hidden entirely.



Edit and remove restrictions

If an entire event has been restricted, you can remove the restriction by taking these steps:

1. Open the event from which you want to remove a restriction.
2. Select **More actions [...] > Manage restrictions**.
3. Select **Remove** on the restriction you wish to remove.
4. Select **Save** to finalize your changes.

To edit or remove a partial restriction:

1. Open the report section that contains the restriction.
2. Select **Actions > Manage restrictions**.
3. Adjust the **Restriction classification** or **Information restricted**.
4. Remove a restriction entirely by selecting **Remove**.
5. Select **Save**.

Manage restriction exceptions

If you want a user, team, or Command Hierarchy group to view a specific item that has been restricted, but you don't want to give them access to view all items containing that restriction, you can create a restriction exception.

Restriction exceptions can be created only when the entire event has been restricted. Exceptions can't be created for partial restrictions. All restriction exceptions that have been created for the organization appear in the Administrator Console Restrictions tool.

Users and groups who are given restriction exceptions can only view the restricted information; they can't manage the restrictions themselves. If you instead want the user or group to be able to add or remove that restriction type, you should instead give them the corresponding restriction privileges.

To view or manage existing restriction exceptions, take these steps:

1. Open the event from which you want to remove a restriction.
2. Select **More actions [...] > Manage restrictions**.
3. The current restriction exceptions appear at the top of the Manage Restrictions pane, and are broken out by different icons:
   - Individual users
   - Teams
   - Command Hierarchy groups
4. Select **Manage exceptions** to see which users, groups, and teams have been granted restriction exceptions and adjust as necessary:
   - Pencil: Select to edit the allowed restrictions or duration
   - Trash can: Select to delete the restriction exception

To create a restriction exception:

1. After opening the Manage Restrictions pane, Select **Manage exceptions**.
2. Search for a user, team, or Command Hierarchy group in the **User or group** field.
   - You can add multiple users, teams, and groups to this field.
3. When multiple restrictions have been applied, you can select which restrictions to include in the exception:
   - All restrictions: Lets the user or group view all restricted information
   - Selected restrictions: Lets the user or group view information only associated with specific restrictions
4. Set a duration for which the exception will apply. Options include:
   - 1 week
   - 2 weeks
   - 1 month

- 2 months
- Custom: Set a custom time frame.
- Until Removed: The exception will remain in place until someone opens the item and manually removes it.

5. Select **Add**.

Redaction

Use the Redaction tool to permanently remove or replace sensitive information in a generated PDF before you print or share it. You can access the Redaction tool while:

- Preparing an event or case for sharing
- Printing a profile
- Printing a report

Redact incidents and cases before sharing or printing

1. Open the event or case profile.
2. Open the **More actions [...]** menu and select either **Prepare documents for sharing** or **Print**.
3. Choose the reports, documents, and other items to include and select **Next**.
   - See Documentation sharing or Printing for more information.
4. Select the **Yes** option and **Start redaction** at the bottom of the screen.
5. Redact the document. See Use the Redaction tool for full steps.
6. After you export the redacted PDF:
   - The redacted PDF is added to the incident/case and appears on the **Files** tab.
   - If your organization is configured to integrate your cases in Axon Standards with cases in Axon Evidence, the PDF is also uploaded to Axon Evidence as part of the case integration.

Redact reports when printing

1. Open the report in Report Writer.
2. Select **More actions > Print**.
3. Adjust the print settings and select **Next**.
   - See Print reports for more information.
4. Select the **Yes** option and **Start redaction** at the bottom of the screen.
5. Redact the document. See Use the Redaction tool for full steps.
6. After you export the redacted PDF, it opens in a new tab so you can download and save it.

7. Unlike when redacting events or cases, the redacted PDF is NOT saved anywhere or uploaded to the report as an attachment.

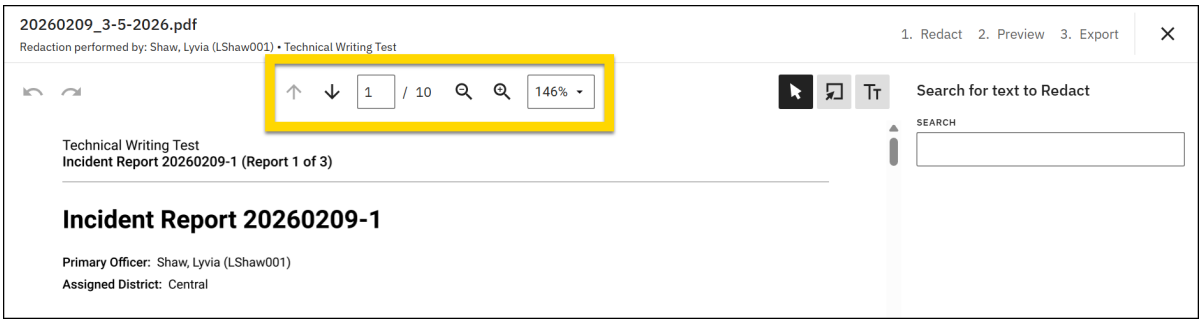
Redact citizen profiles when printing

1. Open the profile.
2. Select **Actions** > **Print**.
3. Adjust the information to include in the printout and select **Next**.
   - See Print profiles for more information.
4. Select the **Yes**option and **Start redaction** at the bottom of the screen.
5. Redact the profile. See Use the Redaction tool for full steps.
6. After you export the redacted PDF, it opens in a new tab so you can download and save it.
7. Unlike when redacting events or cases, the redacted PDF is NOT saved anywhere or uploaded to the profile as an attachment.

Use the Redaction tool

When the Redaction tool opens, you can use the controls at the top of the page to navigate through the document:

- Use the page arrows to move between pages.
- Enter a page number to jump directly to a specific page.
- Use the zoom icons or the zoom dropdown to change magnification, such as 100% or Fit to page.
- Scroll through the document to review content before you apply redactions.



There are three ways you can apply redactions:

- Redact text using search
- Manually redact content
- Add replacement text

After applying a redaction, you can move or edit it. Then, once all redactions are in place, you can preview the redacted document before exporting it as a PDF.

Warning

If you close the Redaction tool before you export, your changes are NOT saved. Complete the redaction and export before closing.

Redact text using search

To quickly redact specific strings of text in bulk:

1. Enter text in the search field on the right side of the window.
2. Review the list of exact matches.
3. Select the checkboxes for the text you want to redact.
4. Select **Apply**.

The search function matches exact text only. If a name appears in multiple formats (for example, last name first, first name last, or with a middle name), search for each variation separately.

When you first apply a redaction, the box appears gray and semi-transparent. When you hover over it, the box turns black. In preview mode, all redactions appear fully black and opaque.

Manually redact content

In addition to searching, you can add redactions manually:

1. Select the **Redact manually** button.
2. Your mouse cursor changes to a crosshair cursor. Select and drag across the content you want to redact.
3. Release to place the redaction box.Select the box and click and drag the corners to adjust its size.

Manual redactions follow the same visual behavior as search-based redactions. They appear semi-transparent until you preview them.

Add text annotations

1. Select the **Text annotate** tool.
2. Select and drag to draw a text box.
3. Double-click on the "Insert text here" text that appears and replace it with the text you want to be printed in the redaction, such as “Person 1" or "REDACTED".
4. Use the text toolbar to:
   - Change the background (fill) color of the text box.
   - Change the text color.
   - Adjust the text size.

Move or delete redactions

After placing a redaction, you can move or resize it. Select the redaction box (or text box) and press the delete icon or press the Delete key on your keyboard to remove that redaction.

Preview redactions

At any point, you can preview what your redacted document will look like by selecting **Preview** at the bottom of the screen. In preview mode, the system displays all redactions as fully black and opaque. Select Back to continue adding additional redactions

Export the redacted PDF

If all redactions are complete, you can export the PDF:

1. If you are not already previewing the redacted PDF, select **Preview**.
2. Optionally add audit log notes to explain what you redacted and why. The system records these notes in the audit log.
3. Select **Redact and export**.
4. If you are redacting an event or case, the PDF is saved under the **Files** tab.
5. If you are redacting a profile or report, the redacted PDF opens in a new tab where you can download and save it.
6. You cannot modify the exported redacted PDF. To make changes, start a new redaction session from the original incident, profile, or report.

Audit log

When you export a redacted PDF, the system creates an audit log entry that records:

- The user who performed the redaction.
- The date and time of export.
- Any audit log notes entered during preview.

Search

Select the magnifying glass icon in the main navigation menu to open Search.

To run a search, enter names, keywords, or IDs (partial or full) in the top search box. If you enter multiple words, the search results will include **all** of the words you entered. (i.e., Entering more words decreases the number of search results and entering fewer words increases the number of results.)

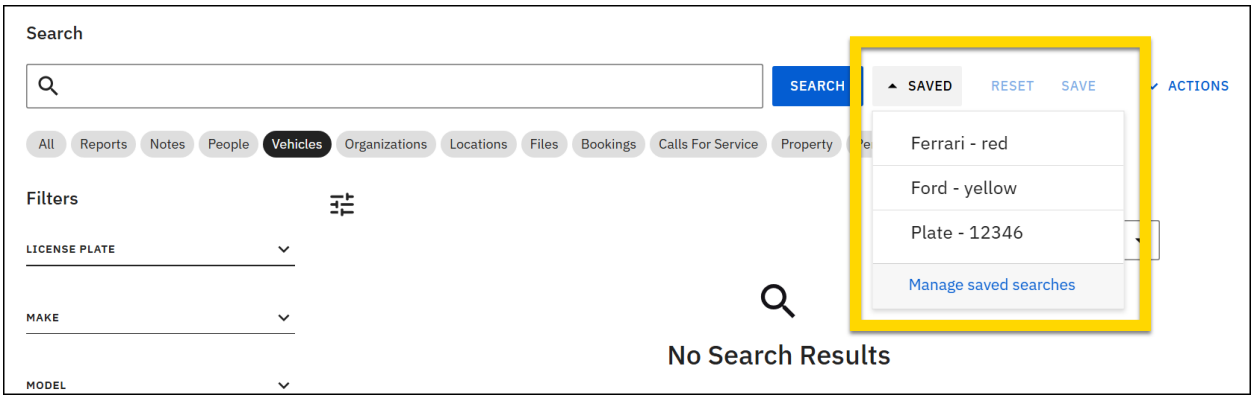
To run a saved search, open the **Saved** dropdown that appears beside the search box and choose on of your saved searches.

Search results are sorted by category (person, vehicle, etc.), and each category displays up to three search results. Use the **Sorted by** menu to change the order in which search results are listed. Select a search result to open the full report or profile. Select **View all** to see all results for that category.

To narrow your search to a specific category (person, vehicle, etc.), select one of the search tabs below the search box. These search tab pages include additional filter fields specific to that category.

Saved searches

To speed up your searches, you can save a search you run regularly and later re-run it with a single click. To run a saved search, open the **Saved** dropdown that appears beside the search box and choose one of your saved searches. When you select a saved search, the **Saved** dropdown changes to show the name of the saved search, and the search results are displayed. Saved searches are associated with your user account and will not appear in the **Saved** menu for other users.



To create a saved search:

1. Enter a search term or terms in the top search box and press **Save**.
   - If you are on one of the search tabs, you can also use the filters to refine your search.
2. Enter a name for the search. This name will appear in the **Saved** menu.
   - The details of the saved search are listed, including:
     - Tab: The search tab you are using (All, Vehicles, etc.)
     - Search input: The terms entered in the top search box
     - Filters: Which filters are used in the search
     - Additionally, the sort options and number of results displayed on the page are included in your save.
3. After entering a name, select **Save**.

To change a saved search:

1. Run the current saved search by selecting its name from the **Saved** menu.
2. Adjust the search as desired (change filters, change sort order, etc.).
3. Select the **Save** button to save the updated search (as a new saved search).
4. Follow the steps below to remove the older version of the search.

To remove a saved search:

1. Open the **Saved** dropdown menu.
2. Select manage saved searches.
3. Select the saved search.
4. Select **Remove**.

Search by date

If you enter a date in the top search box, the system will only search for that date in text-based fields, such as narratives. To search using a date, instead use a date filter field.

On the **All** and **People** search tabs, the system also searches for dates in **Date of Birth** fields. This allows you to enter a date of birth in the top search box, and the system will search for that date of birth. Supported date formats include:

- M/D
- MM/DD
- M-D
- MM-DD
- M/D/YYYY
- MM/DD/YYYY
- M/D/YY
- MM/DD/YY
- M-D-YYYY
- MM-DD-YYYY
- YYYY-MM-DD

Search results

The top portion of each search result shows basic information about the item. The fields displayed on search results vary depending on the category (person, vehicle, etc.). Contact your Axon representative to customize the information displayed in search results.

If your organization shares data with other organizations, a label appears at the top of the search result indicating which partner organization the item belongs to. For more information, see Search partner data.

If the top search box or a free text filter field was used to perform the search, search results also include a **Matched on** section that indicates why that item appears in the search result list. The terms entered in the search box or text filter appear in purple highlighting on the search results beside the fields in which they were found. If a search term appears multiple times in the search result, select **See more matches** to view all the fields containing the term.

Note

You may see some highlighted words in the **Matched on** section that do not currently appear on the profile but were included in older versions of the profile. (Reminder: Whenever a profile is updated by being added to a report, a new version of the profile is created.)

Select the white area on a search result to open the profile for that item. Return to your search results by selecting **Go back to search**.

If you instead select blue hyperlink text in the bottom gray area on a search result, that profile opens, as opposed to the profile for the search result. Select the **X** to close the report and return to your search results.

Search results you have already opened have a gray background. Results you have not yet opened have a white background. This visual quickly tells you which results you have already viewed.

Search tabs

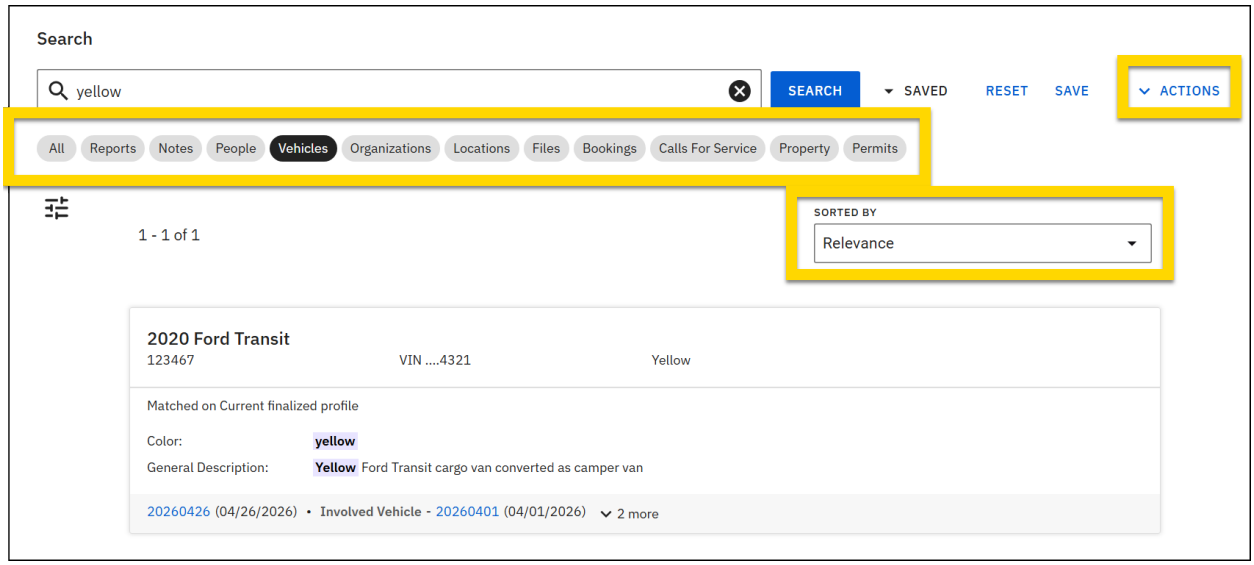
To narrow your search to a specific category, select one of the search tabs below the search box or select **View all** below each category's search results. A new page loads and displays the full results list for that category along with a set of filter fields you can use to further refine the results. Select **All** to return to your initial search and the search results for all categories.

Each search tab contains filter fields specific to that category that allow you to further narrow down your search results. Search categories include:

- Events
- Citizens
- Officers
- Vehicles

When viewing a search tab, select **Actions** to export your search results.

Use the **Sorted by** menu that appears at the top of the list of search results to change the order in which the search results are displayed. The default sort order for all search tabs is Relevance. Additional sort options vary based on which search tab you are using.



Map view

When viewing search results on the following search tabs, you can view your search results on a map by selecting the map icon beside the **Sorted by** menu.

- Events (The location of occurrence is the address displayed on the map.)
- Citizens

When you select the map icon, the filters pane closes and the map opens on the right side of the screen. You can zoom in and out or click and drag to move around on the map.

At the bottom of the map, a message indicates how many search results have associated addresses shown on the map. These search results appear as pin icons on the map. If multiple pins appear very close together, the map displays a dark gray circle. If you zoom in on this area of the map, the circle breaks into individual pins. Select a pin to open a pop-up that contains basic information about that search result. Click anywhere on the map to close the pop-up or select **View details** to open the search result in a new tab.

When viewing search results for people, if a person has multiple addresses (home, work, etc.), all addresses are displayed on the map.

Map view only shows verified addresses, which includes Auto Addresses and Cross Streets. See GIS and maps for more information about location types.

Note

Map view only appears once you have selected one of the search tabs. It is not available from the **All** tab.

Filters

Each search tab contains a different set of filter fields you can use to narrow down your search results. Select the filter icon  to expand or collapse the list of filter fields.

When viewing **All** search results, the list of search filter fields does NOT appear. You must select one of the search tabs that appears below the search bar to open a search tab and reveal the list of filter fields associated with that search category.

Filter fields can be removed, added, or changed based on your organization's needs. To see the full list of filter fields available on each search category page, see Search customizations. Contact your Axon representative to customize these filter fields for your organization.

Note

Custom search filter fields only appear in the desktop application and not in the mobile Axon app.

Several different types of filter fields appear on the search category pages:

- **Checkbox:** Select one or more of the available checkbox options.
- **Dropdown:** Select one or more of the available options from the list. Contact your Axon representative if additional options need to be added to this list.
- **Free text:** Any characters can be entered in this filter field. Use wildcard operators in addition to search terms to broaden or narrow the search. If you enter multiple terms in the same filter field, you will see search results that match either phrase.
- **Range:** Use the preset options to quickly enter a date range (today, yesterday, last 7 days, etc.). To enter a custom date range, enter the start of the numeric / date range in the *Exact/From* filter field and the end of the numeric / date range in the *To* filter field. To search for a specific date, enter a single number in the *Exact/From* filter field.
- **Search:** As you enter text, matching results appear that you can select and apply.

Remove all applied filter fields by selecting **Reset all**. Remove a single filter from a filter field by selecting:

- **Reset**: Remove all of that filter type
- **X:** Remove just that filtered term

User search filters (filters that look for users who have an account in Axon Standards) include toggle.When using this filter, you can enable this toggle, and inactive users will be included when you search for names in the filter. Inactive users appear at the end of the list with an [INACTIVE] preface before their names.

Events

Clicking anywhere in the white area of an Events search result opens the event/case profile, and selecting a blue hyperlink in the **Matching reports** section instead opens that report in Report Writer .If people or vehicles have been added to the report, their roles and links to open their profiles appear in the bottom portion of the search result.

Use the **Sorted by** drop-down menu to set the order in which search results are shown:

- Relevance: This is the default sort order.
- Report Create Date (Newest to Oldest)
- Report Create Date (Oldest to Newest)

Officers

Selecting an Officers search result opens the officer's profile. Unlike Citizens search results, Officer search results cannot be sorted or exported.

Citizens

Clicking anywhere in the white area of a Citizens search result opens the citizen profile, and selecting a blue hyperlink in bottom portion of the result opens the event/case profile the person is associated with.

For users who have case management privileges, the search results also include people who have been added to case documentation.

Use the options in the **Result settings** section at the top of the Filters list to refine which kinds of results are displayed:

- **Include similar results:** When this setting is turned on, search results include:
  - Phonetic (“sounds like”) results: Search for **`John`** includes results for **`Jon`**
  - Stemmed results: Searching for **`walking`** includes results for **`walk`** and **`walked`**
  - Results with one letter difference: Searching for **`Tim`** includes results for **`Jim`**

    - Fields other than name, alias, ID and Date of Birth
- **Include old profile versions:** When this setting is turned on, Search also looks at older versions of people profiles.
    - If a person's name has been updated 5 times, results include all old versions of the profile that contain old names, including the latest version with the person's current name.

Open the **Actions** menu to:

- **Export person details**: Export your search results to a CSV file.
    - Includes ALL search results. In other words, if you selected any checkboxes beside any search results, the export will include all search results and not just those that have been selected.

Note

Although People search in Axon Records and Citizens search in Axon Standards look similar, the databases are separate. Searching for a person in Axon Standards only returns results for people who have been added to Axon Standards reports, and searching for people in Axon Records only returns results for people who have been added to Axon Records reports.

Use the **Sorted by** drop-down menu to set the order in which search results are shown:

- Relevance: This is the default sort order.
- Last Updated (Newest to Oldest)
- Last Updated (Oldest to Newest)
- Last Name, First Name (A to Z)
- Last Name, First Name (Z to A)

Vehicles

Clicking anywhere in the white area of a Vehicles search result opens the vehicle profile, and selecting a blue hyperlink in the **Matching reports** section opens that report in Report Writer or the event/case profile the vehicle is associated with.

For users who have case management privileges, the search results also include vehicles that have been added to case documentation.

Note

Although Vehicles search looks the same in Axon Records and Axon Standards, the databases are separate. Searching for a vehicle in Axon Standards only returns results for vehicles that have been added to Axon Standards reports, and searching for vehicles in Axon Records only returns results for vehicles that have been added to Axon Records reports.

Use the **Sorted by** drop-down menu to set the order in which search results are shown:

- Relevance: This is the default sort order.
- Last Updated (Newest to Oldest)
- Last Updated (Oldest to Newest)

Export search results

You can export search details from all search tabs, except the **All** tab. The details included in the export are the same as the filters that appear on the search tab you are using. For example, when exporting from Vehicles search, details can include VIN, license plate, etc.

In addition to exporting search details, you can also export form data from Events search. This export includes data from all form fields.

Export details

To export the details of a search:

1. Perform a search on any search tab except the **All** tab.
   - In Citizens search, use the checkboxes to indicate which results to include in the export.
2. Select **Actions > Export details**.
3. Update the date fields to indicate which reports should be included in the export.
   - When exporting search results for people, vehicles, etc. these filters indicate that items (people, vehicles, etc.) added to reports during the specified date range will be included in the export.
4. Use the checkboxes to indicate which columns should appear in the CSV file.
   - These columns are the same as the filters available on that search page.
   - To customize which columns and data are included in your search result exports, contact your Axon representative.

- Contact Axon Support or your Axon representative to have your organization's search results configured such that the time zone information does NOT appear in the column headings for date fields.

5. Select **Export** to generate the CSV file and download it to your machine.

Export Form Data

In Events search, instead of exporting the details of your search, you can instead choose the **Export form data** option. This option lets you export all data entered in reports, rather than just the report details.

When the Export Settings window opens, select a report type. You can only export form data for a single report type at a time. Adjust the **Date range** filters as desired, and select **Export**.

Search tips and tricks

Use this reference to get more out of search in Axon Standards.

Breadth and precision

When running a search, your goals may vary between breadth and precision:

Breadth	I need to make sure I don't miss anything.
Precision	I know exactly what I want.

Control the number of search results you get

Use the top search box and filters to control how many search results are returned:

Breadth	Use fewer keywords in the top search box and fewer filters to return a larger set of results.
Precision	Add more words and apply more filters to narrow down your list of results. Search will only look for results that include ALL of words and filters you choose.

Control where Search looks

Switch between the search category pages to control the type of search results you see:

Breadth	Run a search using the top search box on the **All** search category page. This page searches every field, for every content type (people, vehicles, etc.).
Precision	Run a search from a specific search category page (People, Vehicles, etc.) to ONLY get results of that type. Use search filters to focus your search on specific fields within forms or on profile pages.

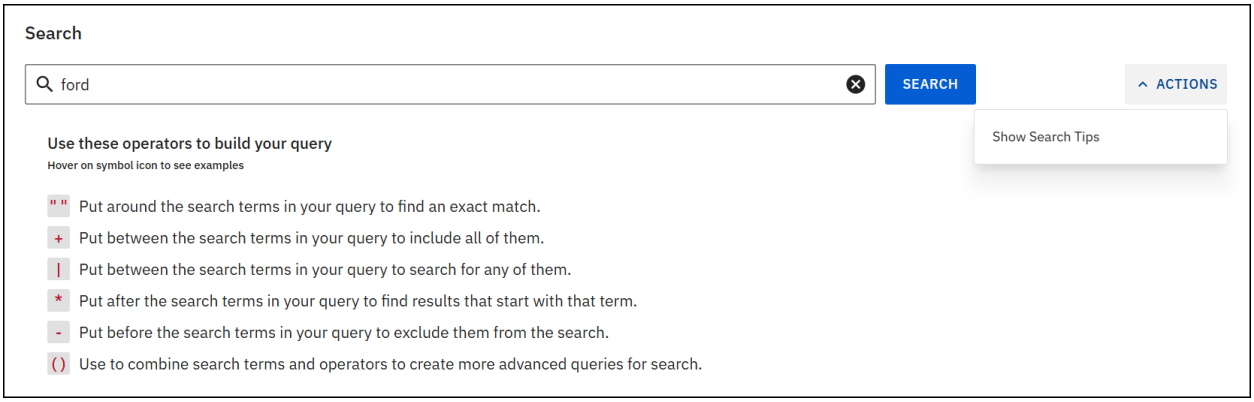
Filter tips

- Enter ‘t’ for today and ‘y’ for yesterday to quickly fill a date filter.
- Dates often aren't searchable from the main search box. Use a date filter instead to find what you're looking for.
- Missing a filter? Contact your Axon representative or Customer Support.

Search with partial information and unclear spelling

Top search box

Use a combination of search terms and search wildcards (symbols) in the top search box to find exactly what you’re looking for. View the list of available wildcards from any search page by selecting **Actions > Show search tips**.



Widlcard	Use case	Example search terms	Example search results
Double quotation marks " "	Use " " around search terms to find an exact match of those search terms.	Central Park	then he ran to Central Park Search results would NOT include: they were walking in the park central

Widlcard	Use case	Example search terms	Example search results
Plus sign +	Use + between search terms to find results that include ALL search terms.	firearm + safe	they hid the firearms in the safe Search results would NOT include: the house had a safe
Vertical slash |	Use | between terms to find results that include ANY of the search terms.	firearm | safe	they hid the firearms in the safe the house had a safe
Asterisk *	Use * after your search terms to find results that start with those search terms.	jo*	jon john
Minus sign -	Use – before search terms to exclude those search terms from your results.	-red	Search results would NOT include anything containing "red".
Parentheses ()	Use ( ) to search terms and wildcards. The more terms and wildcards you use, the fewer results you will see.	("person with a" + (knife | gun | bomb))	I entered the house to find a person with a gun Search results would NOT include: when I walked into the house, there were people with knives

Search filters

Use even more search wildcards when searching with filters.

Widlcard	Use case	Example search terms	Example search results
Asterisk *	Use * at the start of a word or number to search for anything that ends with that word or number.	*on	jon jason
	Use * within a single word to find a "fuzzy" match within a word.	j*n	jon jan jackson

Widlcard	Use case	Example search terms	Example search results
Question mark ?	Use **?** in place of a **single** character within a word to return results that are spelled similarly.	?erry	Kerry Terry Gerry
	To search for **multiple** characters in a row, use multiple question marks.	??erry	Sherry

Find people

The People search category page includes a **Result settings** section at the top of the filter list with two settings that can help you find the right people:

- **Include similar results:** When this setting is turned on, search results include:
  - Phonetic (“sounds like”) results: Search for **`John`** includes results for **`Jon`**
  - Stemmed results: Searching for **`walking`** includes results for **`walk`** and **`walked`**
  - Results with one letter difference: Searching for **`Tim`** includes results for **`Jim`**
  - Fields other than name, alias, ID and Date of Birth
- **Include old profile versions:** When this setting is turned on, Search also looks at older versions of people profiles.
  - If a person’s name has been updated 5 times, results include all old versions of the profile that contain old names, including the latest version with the person’s current name.

Find reports

When searching for reports, keep in mind:

- Report search includes older versions as well as the latest version of a report.
- Don't use the top search box to search by date. Instead, use a date filter to get the right list of results.

Build lists of results with search

After running a search, you can export your results to a CSV file. Run your search, then select **Actions > Export details**. The details included in the export are the same as the filters that appear on the search page you are using. Don't see a field you need? Contact your Axon representative or Customer Support.

When exporting search results from Events search, you can also select **Actions > Export form data** .This export includes all fields for that form in the CSV file.

For more information, see Export search results.

Search customizations

You can work with your Axon representative to customize various search-related features. Available customizations include:

- Filter fields and search result exports
- Search results

In addition to explaining the customizations for the various search features, this guide includes all default configurations for each search category page. Use the links below to jump directly to the default configuration for that page.

- Events
- Officers
- Citizens
- Vehicles

Filter fields and search result exports

Each search category page in the Search module, along with the **Agency Court Papers** inbox in the Warrants module, comes with a standard list of filter fields. Filter field types include:

- **Checkbox:** Select one or more of the available checkbox options.
- **Dropdown:** Select one or more of the available options from the list. Contact your Axon representative if additional options need to be added to this list.
- **Free text:** Any characters can be entered in this filter field. Use wildcard operators in addition to search terms to broaden or narrow the search. If you enter multiple terms in the same filter field, you will see search results that match either phrase.
- **Range:** Use the preset options to quickly enter a date range (today, yesterday, last 7 days, etc.). To enter a custom date range, enter the start of the numeric / date range in the *Exact/From* filter field and the end of the numeric / date range in the *To* filter field. To search for a specific date, enter a single number in the *Exact/From* filter field.
- **Search:** As you enter text, matching results appear that you can select and apply.

You can work with your Axon representative to customize these filter fields to:

- Change filter field names
- Change filter field order

- Remove filter fields
- Add new filter fields
  - New filter fields can search for fields in out of the box reports (such as incident or general offense reports), or custom reports you have created for your agency.
- Change present ranges for date filter fields (today, yesterday, last 7 days, etc.)

In addition to customizing the filter field list, you can adjust which columns appear in the search result export file. Like filter fields, the changes you can make include:

- Change column names
- Change column order
- Remove columns
- Add new columns
- When exporting options from dropdown fields, display either the shortcode or description (e.g., for Role, display VIC or VICTIM)

Note

The filter fields that appear in other modules, such as Case Management, Tasks, or Early Intervention System cannot be customized.

Search results

Each search page displays a default set of fields on the search result previews. You can work with your Axon representative to customize which fields appear on search results. The default fields cannot be removed, but additional fields can be added.

For example, in the image below, the Phone Number field has been added to person search results.



Default configurations

The following sections list the default filters, search result exports, and search result previews for the various search pages.

Events search default configuration

The following filter fields, search result exports, and search result previews are the default for Events search.

Filters and search result exports

Filter	Type
Date Event Created [1]	Range
Date of Event [2]	Range
Date Report Created [3]	Range
Involved Officers	Search
Report Created By	Search
Report Type	Dropdown
Status	Dropdown
Citizens > Identity	
-- First Name	Free text
-- Last Name	Free text
-- DOB	Range
-- ID (SSN, DL, ETC.)	Free text
-- Aliases	Free text
-- Middle Name	Free text
-- Height	Range
-- Weight	Range
-- Hair Color	Dropdown
-- Eye Color	Dropdown

Filter	Type
Citizens > Description	
-- Age	Range
-- Race	Dropdown
-- Sex	Dropdown
-- Ethnicity	Dropdown
-- Height	Range
-- Weight	Range
-- Hair Color	Dropdown
-- Eye Color	Dropdown
-- Address [4]	Search
-- Phone Number	Free text
Citizens > Marking	
-- Marking Type	Dropdown
-- Marking Keywords	Free text

[1] The **Date Event Created** filter field searches for the date that the original report associated with the event was created. An event can contain additional reports that have different creation dates.

[2] The **Date of Event** filter field searches for the date that was entered into the event's original report as the date on which the event took place.

[3] The **Date Report Created** filter field searches for the date that the report was created. If the report was the original report that created a new event, this date will be the same as the Date Event Created date.

[4] In the **Address** filter field, surround the text in double quotations to return search results that include ALL words searched.

- Example: Entering *123 N Test Blvd WAY E Fresno CA 93721* here would return results that include Fresno 93721, Fresno CA 93721, 123 N Test Blvd, N Blvd WAY E, etc.
- Example: Entering *"123 N Test Blvd WAY E Fresno CA 93721"* here would return results that include 123 N Test Blvd WAY E Fresno CA 93721.

Search result previews

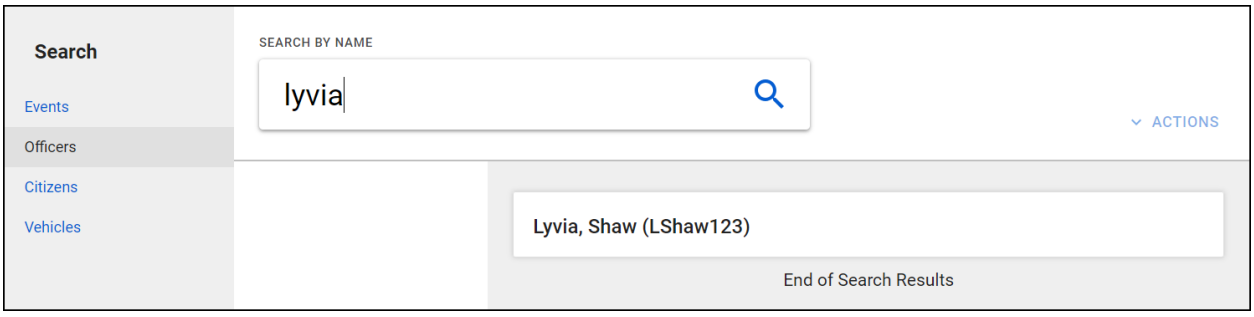
- Event ID
- Date/time
- User who created the event
- Report IDs for all reports associated with that event

If people or vehicles have been added to the report, their roles and links to open their profiles appear in the bottom portion of the search result.



Officers search default configuration

Unlike the other search pages, Officers search is not customizable. This page only has the main search box and no filter fields. Search result previews include the Last name, First name, and Badge ID of the officer.



Citizens search default configuration

The following filter fields, search result exports, and search result previews are the default for Citizens search.

Note

Although People search in Axon Records and Citizens search in Axon Standards look similar, the databases are separate. Searching for a person in Axon Standards only returns results for people who have been added to Axon Standards reports, and searching for people in Axon Records only returns results for people who have been added to Axon Records reports.

Filters and search result exports

Filter	Type
First Name	Free text
Last Name	Free text
Middle Name	Free text
DOB	Range
Alias	Free text
ID (SSN, DL, ETC.)	Free text
Age	Range
Race	Dropdown
Ethnicity	Dropdown
Sex	Dropdown
Height	Range
Weight	Range
Eye Color	Dropdown
Hair Color	Dropdown
Location	Search
Source [1]	Checkbox

Filter	Type
Marking	
-- Marking Type	Dropdown
-- Marking Keywords	Free text
Phone Number	Free text
Flag Category	Dropdown
Location: Reporting Area	
-- District	Search
-- Beat	Search
-- Zone	Search
Location: Address	
-- Location of Occurrence	Search
-- Street Address [2]	Free text
-- House Number Range	Range
-- Address [3]	Free text

[1] In the **Source** filter field, selecting the **Only MNI** checkbox filters your search so the only results that are displayed are those that belong to a Finalized report. People who have only been added to Draft reports are not shown.

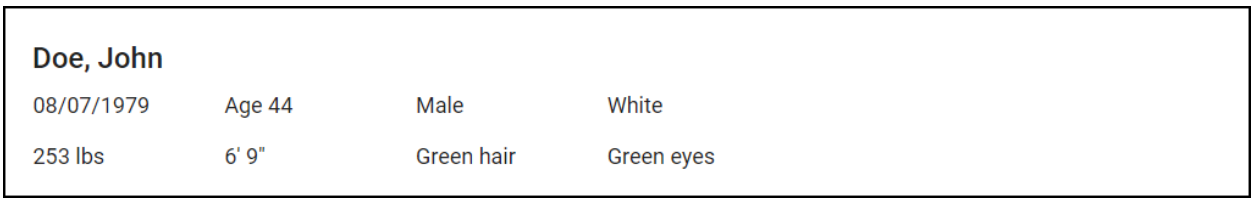
[2] The **Street Address** filter field only searches for the street name. House number, city, state, or zip code entered in this filter are ignored.

[3] In the **Address** filter field, surround the text in double quotations to return search results that include ALL words searched.

- Example: Entering *123 N Test Blvd WAY E Fresno CA 93721* here would return results that include Fresno 93721, Fresno CA 93721, 123 N Test Blvd, N Blvd WAY E, etc.
- Example: Entering *"123 N Test Blvd WAY E Fresno CA 93721"* here would return results that include 123 N Test Blvd WAY E Fresno CA 93721.

Search result previews

- Last Name, First Name
- Date of birth
- Age
- Sex
- Race
- Weight
- Height
- Hair Color
- Eye color



Vehicles search default configuration

The following filter fields, search result exports, and search result previews are the default for Vehicles search.

Note

Although Vehicles search looks the same in Axon Records and Axon Standards, the databases are separate. Searching for a vehicle in Axon Standards only returns results for vehicles that have been added to Axon Standards reports, and searching for vehicles in Axon Records only returns results for vehicles that have been added to Axon Records reports.

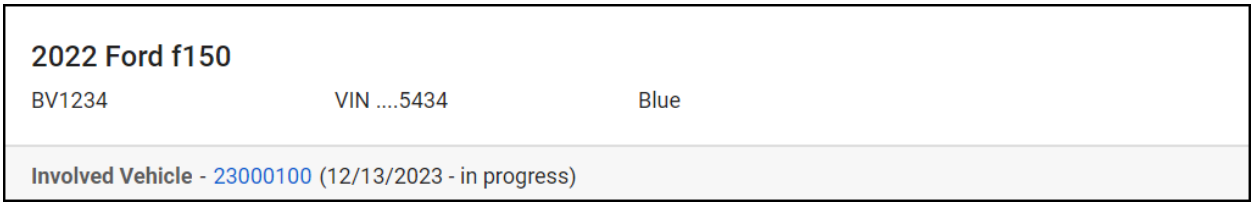
Filters and search result exports

Filter	Type
License Plate	Free text
Make	Dropdown
Model	Free text
Style	Dropdown
Year	Range

Filter	Type
Color	Dropdown
VIN	Free text
Flag Category	Dropdown
Date of Occurrence	Range
Role	Dropdown

Search result previews

- Vehicle year make model
- License plate
- VIN
- Color
- Reports that vehicle appears in

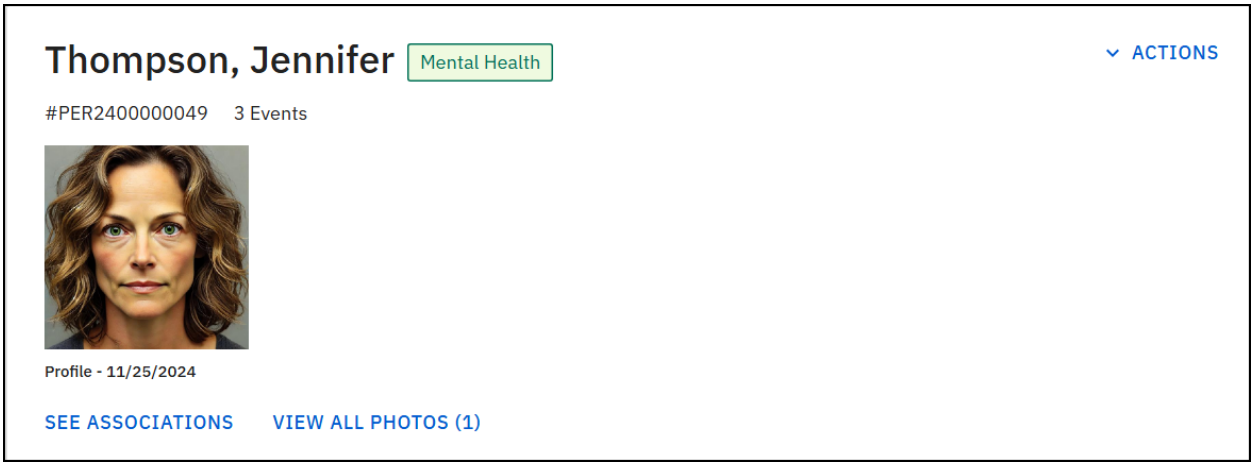


Profiles

When information about people, vehicles, etc. (also known as entities) are added to a report, a profile page is created to display the known information. A profile also shows all associations between that profile and other profiles, as well as all reports the profile has been added to.

In Axon Standards, profiles are created for people, officers, and vehicles. Profiles are also created for events and cases but these profiles differ substantially from the regular profile pages and are documented separately.

The top of every profile contains a header section that includes the profile name, ID, the number of event associations, and any flags that have been added to the profile. Select **See associations** to view the profile's associations.



Actions

The **Actions** menu in the top right corner profile header lets you take various actions on the profile. Some profiles contain additional actions, but every profile contains the following options:

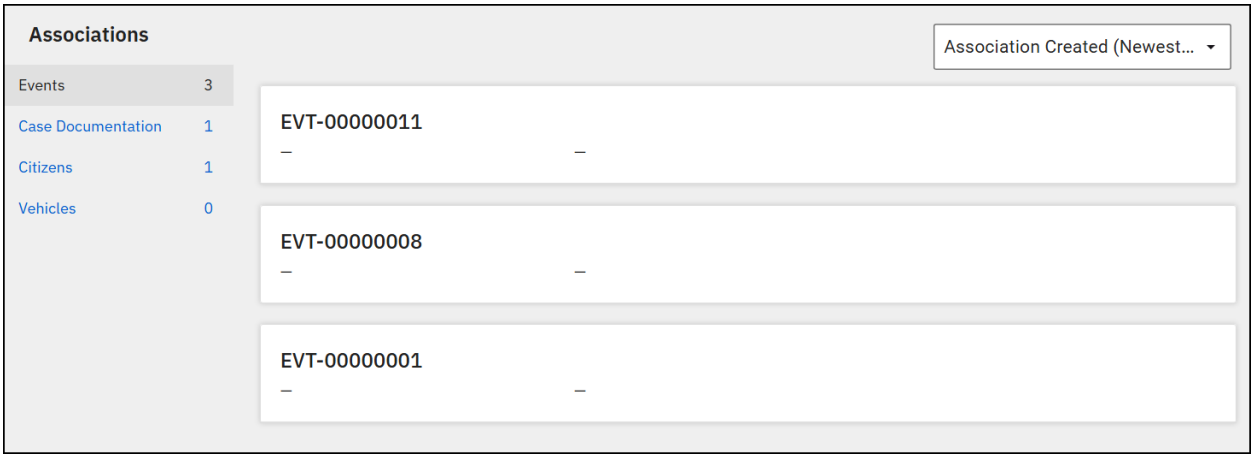
- Add flag
- Copy link to clipboard (copy the profile URL to paste into another document/application)
- Print profile
- View and manage flags

Associations

An **Associations** section at the bottom of the profile displays how that profile is associated with other profiles and reports. This Associations section can contain some or all of the following associations:

- Events
- Case documentation (case summaries, case documents, and case tasks)
- Citizens
- Vehicles

Use the sorting dropdown to change the order in which the associations appear.



Officer profiles

An officer profile includes their name, Badge ID, rank, email, username, External ID, and department. Additional sections on the profile include **Identity** and **Description**. The **Related reports** section shows all reports that include the officer as an involved officer.

Selecting **Actions** lets you take the following actions:

- Edit Profile
  - Changes made to officer profiles also reflect in the Personnel module.
- Copy link to clipboard (copy the URL to paste into another document/application)

Note

The other standard options in the **Actions** menus of other profiles do NOT appear in Officer profiles.

Citizen profiles

In addition to the regular header information, person profiles include photos that have been added to the profile. Select **View all photos** to browse through all photos that have been added.

In addition to the regular options, the **Actions** menu includes:

- Edit Profile
- Show person history
- Take photo
- Upload photo

Scroll down the page to view additional sections, including Victim Details, Identity, Identifying Documents, Description, Scars, Marks, Tattoos, Contact, and Custom Fields that have been configured for your organization.

Note

Although person profiles in Axon Records and Axon Standards look similar, the databases are separate. The same person may have a profile in Axon Records, and a different profile in Axon Standards. The Axon Records profile only includes information that has been added to Axon Records reports, and the Axon Standards profile only includes information that has been added to Axon Standards reports.

Vehicle profiles

In addition to the regular header information, vehicle profiles include the vehicle year, make, model, plate, and additional details (color, expiration, etc.).

In addition to the regular options, the **Actions** menu includes:

- Take photo
- Upload photo

Note

Although vehicle profiles in Axon Records and Axon Standards look similar, the databases are separate. The same vehicle may have a profile in Axon Records, and a different profile in Axon Standards. The information in the Axon Records vehicle profile only includes information that has been added to Axon Records reports, and the Axon Standards vehicle profile only includes information that has been added to Axon Standards reports.

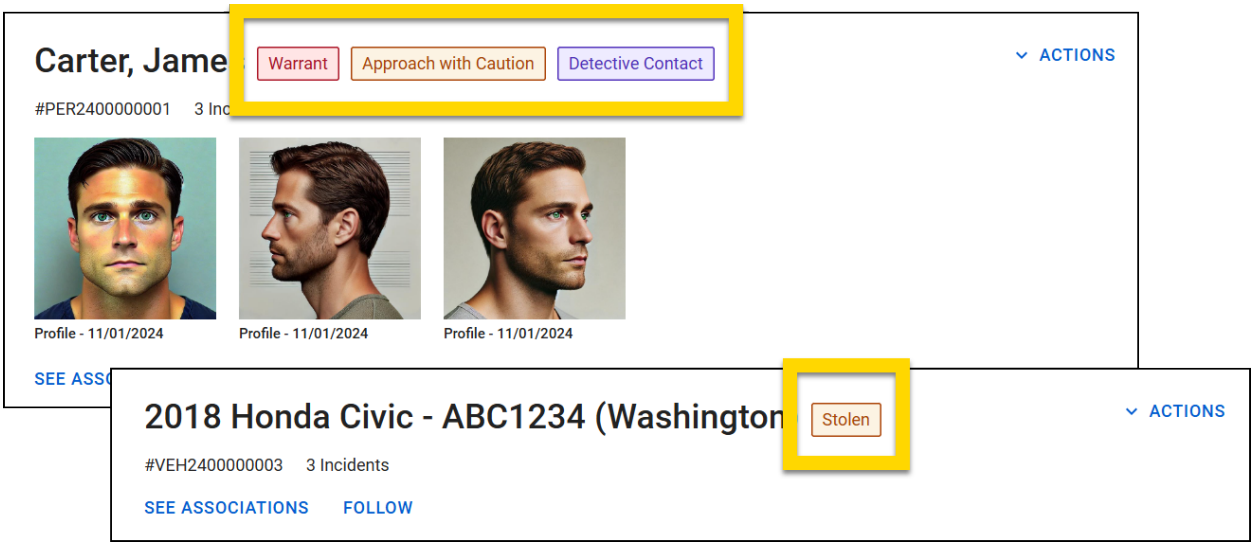
Profile actions

Profiles can be opened from Search or from within Report Writer. Once opened, the **Actions** menu in the profile header lets you take various actions on the profile. Some profiles contain additional actions, but every profile contains the following options:

- Add flag
- Copy link to clipboard (copy the profile URL to paste into another document/application)
- Print profile
- Take/upload photo
- View and manage flags

Manage flags

Users with certain privileges can add one or more flags to a profile to visually alert other users to important information. You can add flags to citizen and vehicle profiles. Flags appear at the top of the profile, beside the name.



Flags also appear in Report Writer when you're searching to add an existing person, vehicle, etc. to a report. Hover over the flag name to view additional information.

You can add multiple flags to a profile. Flags are sorted from highest to lowest severity (high → medium → low) on a person's profile. Within each severity group, flags are sorted chronologically, with the most recently added flag appearing first.

Flags can also be automatically added to a profile if that profile is added to a certain type of report. For example, a Warrant flag can be automatically applied to a person if they are added to a Warrant report. These flags are displayed in the associations section on profiles to indicate which report added the flag to that profile.

Administrators can create and manage flag categories (e.g., Approach with Caution, Deceased, etc.) from the Administrator Console.

Add flags

Flags can be added to a profile either while viewing the profile page or from Report Writer in a report where that profile has been added. Follow these steps to add a flag to a profile:

1. Start from one of the following locations:
   - Report Writer: Open a report to the section that contains the person, vehicle, etc.
   - Search: Search for and open the profile.
2. From the profile or the section of the report containing the profile, select **Actions > Add flag**.

3. In the Add flag pane that opens, choose an option from the **Flag category** dropdown.
4. In the **Description** box, enter information related to the flag. When other users open the profile and select the flag, they will see this information.
5. Complete the **Expiration date** and **Expiration in hours** fields if the flag is temporary and should be removed automatically after a set time period.
6. Select **Add** to apply the flag to the profile.

Edit existing flags

To edit the information for an existing profile flag:

1. Open the profile.
   - Existing flags can only be managed from the profile, not from within Report Writer.
2. Select a flag at the top of the profile or select **Actions > View and manage flags** in the top right corner.
   - If the flag was added by a warrant or another report, when you select the flag the page scrolls down to the **Associations** section where you can open and adjust the warrant/report.
3. If the flag was added directly to the profile, the Manage Flags pane opens where you can select **Edit** on the flag you want to edit.
4. Edit the flag information.
   - You can change the flag category, description, or expiration dates/times.
5. Select **Save**.

Remove flags

To remove a flag from a profile:

1. Open the profile.
   - Existing flags can only be removed from the profile, not from within Report Writer.
2. Select a flag at the top of the profile or select **Actions > View and manage flags** in the top right corner.
   - If the flag was added by a warrant or another report, when you select the flag the page scrolls down to the **Associations** section where you can open and adjust the warrant/report.
3. If the flag was added directly to the profile, the Manage Flags pane opens where you can select **Archive** for the flag you wish to remove.
4. In the confirmation message that appears, choose to either archive or delete the flag:
   - **Archive:** Removes the flag from the profile but keeps a record that it had once been applied to the profile. Archived flags can later be deleted after they are archived.

- **Delete:** Removes the flag from the profile and permanently deletes any record that it had ever been applied to the profile.

View archived flags

To view previous profile flags that have expired or been archived:

1. Select **Actions > View and manage flags** in the top right corner of the profile.
   - Existing flags can only be managed from the profile, not from within Report Writer.
2. Switch to the **Archived** tab.
3. All details about the flag, including description, created by, create date/time, and expiration date/time are displayed.

Print profiles

You can print the profile for any person or vehicle by opening the profile and selecting **Actions > Print profile** in the top right corner. For information about printing reports, see Print reports, incidents, and events.

The following information is included on each printable PDF for each profile type.

Person profiles

When printing a profile, use the checkboxes to indicate which information should be included in the printout. Options include:

- Profile page
  - Include historical changes
- All involvements
  - Includes involvements in in-progress reports

Note

Although person profiles in Axon Records and Axon Standards look similar, the databases are separate. The same person may have a profile in Axon Records, and a different profile in Axon Standards. The Axon Records profile only includes information that has been added to Axon Records reports, and the Axon Standards profile only includes information that has been added to Axon Standards reports.

Vehicle profiles

The following information is included in vehicle profile printouts:

- Vehicle details (make, model, year, color, etc.)
- Involvements (which, if any, incidents the vehicle is associated with)

Note

Although vehicle profiles in Axon Records and Axon Standards look similar, the databases are separate. The same vehicle may have a profile in Axon Records, and a different profile in Axon Standards. The information in the Axon Records vehicle profile only includes information that has been added to Axon Records reports, and the Axon Standards vehicle profile only includes information that has been added to Axon Standards reports.

Officer profiles

Officer profiles can't be printed.

Manage profile photos

Photos can be added to person and vehicle profiles. You can upload, take, and view all photos on a profile using the **Actions** menu in the top right corner of the page and the **View all photos** button below the profile photos.

The various photo-related actions are controlled by the Profile photo privileges.

Note

To manage vehicle profiles, your organization must use the BOLO feature set. Contact your Axon representative or Axon Support for assistance in enabling these features.

View all photos

To view and edit any photos on a profile, select a photo or the **View all photos** button to open the photo gallery. On person profiles, use the tabs to switch between **All photos, Profile**, **Marking**, and **Uncategorized** photos.

When viewing photos in the photo gallery you can take the following actions:

- Edit the selected photo (change the category, type, and date taken).
- Delete the selected photo.
- Download the selected photo.

- Make the selected photo the default photo. Default photos display:
  - As the first image on that profile
  - In search results
  - In the search results that appear when searching to add an existing person or vehicle to a report.

Upload photo

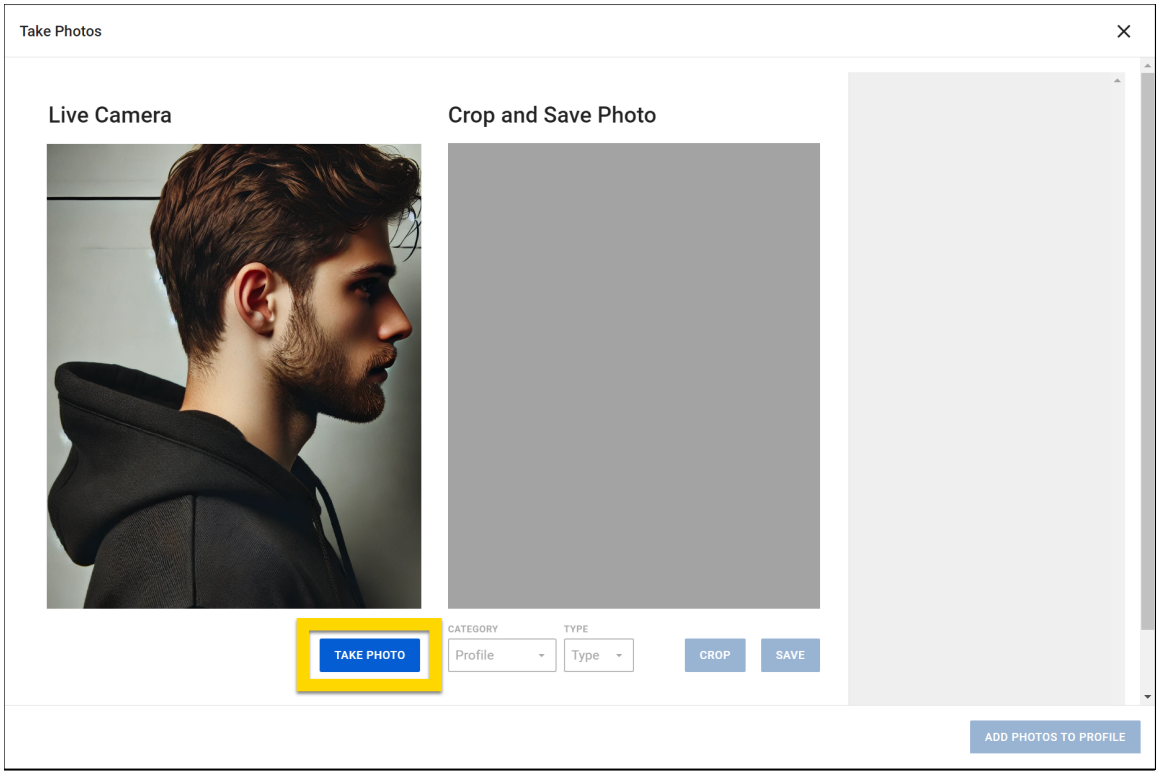
To upload profile photos:

1. Open the profile and select **Actions > Upload photo** in the top right corner.
2. Select **Upload photo** and find the image on your device.
   - The maximum file size is 200 MB.
3. When adding person photos, set the photo category. Options include:
   - Profile
     - If selected, you must also indicate the type (Front, Left, or Right).
   - Marking
   - Uncategorized
4. When adding person photos, select if the image should be used if users generate a photo lineup that includes the person.
5. Select **Upload** to add the image to the profile.

Take photo

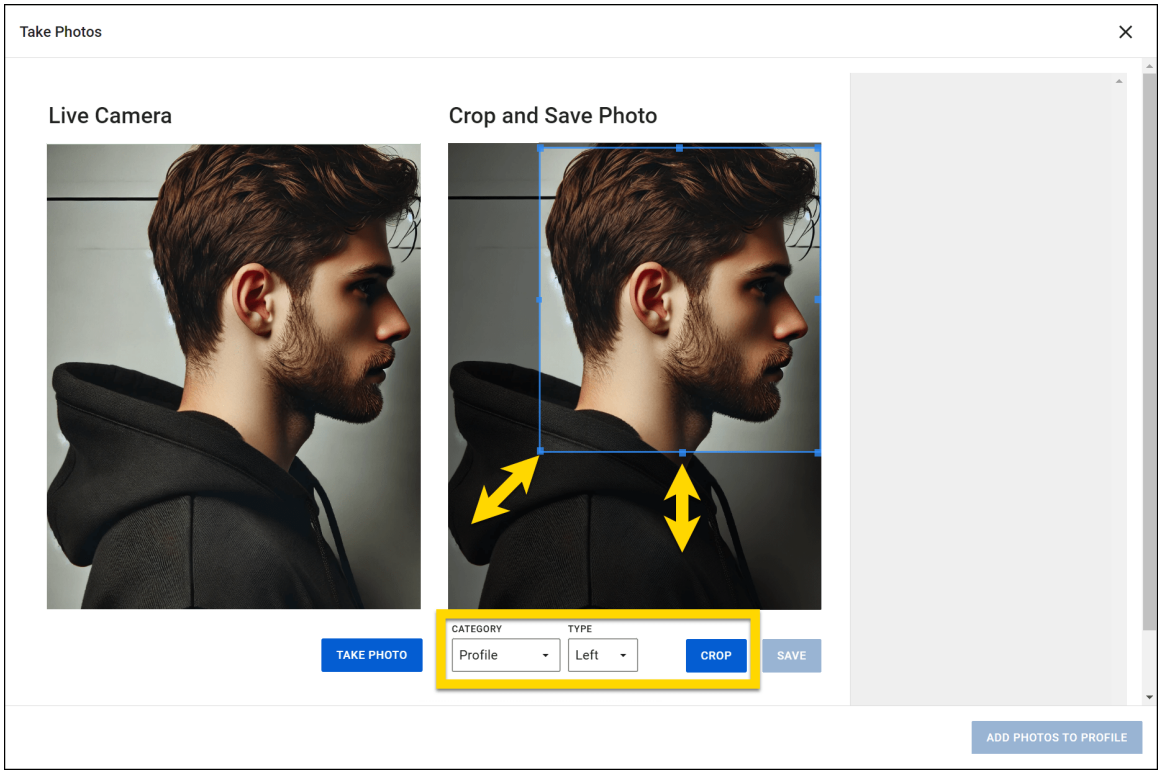
If you have a device that can take photos (generally for taking person photos), follow these steps to take a photo and add it to the profile:

1. Open the profile and select **Actions > Take photo**.
2. The live camera feed loads on the left side of the page. Once the person is positioned facing the camera, select **Take photo**.
   - If you need to take a new photo, select **Take photo.**



3. The photo appears in the center of the page where you can adjust the crop area and add photo details:
   - Set the category (Profile, Marking, Uncategorized).
     - For profile photos, also set the photo type (Front, Left, Right).
   - Click and drag a corner of the blue box to resize the crop selection.

- Select **Crop photo** to crop the photo to your selection.



4. After categorizing the photo and adjusting the crop, select **Save**.
5. The cropped photo, its category, and its type appear on the right side of the page.
   - Select **Edit** to adjust the category and type.
   - Select **Delete** to remove the photo.
   - Select **Add photos to profile** in the bottom corner of the page to add the photo to the person's profile.

Citizen profile actions

You can take various additional actions on citizen profiles by opening the **Actions** menu in the top right corner of the profile.

The options in his menu include:

- Edit profile
- View history

Edit profile

Profiles are updated whenever a person is added to a report and their information is changed in the report. Users with certain privileges can also make changes to a person's information by opening their profile and selecting **Actions > Edit profile**.

Note

You can't add, update, or remove a person's Contact Address information directly from a profile. To change this information, add the person to a report, update the contact address, and finalize the report.

After editing the person's information, select **Save** at the bottom of the page.

All historical profile changes can be viewed by selecting **Actions > Show person history**.

Simultaneous edits

If you directly edit a person's profile and that person has already been added to a report that is currently in progress, the profile edits you make will NOT appear in the report. When the report is finalized, all information in the report will be applied to the person's profile, and any edits made directly on the profile may be overwritten. The edits you made directly to the person's profile still appear in the person's history.

If you are editing a person's profile and before you select **Save** another user edits that person (either by directly editing the profile or updating it from a report), a message will appear. This message displays your edits, along with the changes made by the other user. You can select to either discard or keep your edits.

View history

Person information can change in two instances:

- When a person is added to a report, their information is changed, and the report is finalized.
- When a person profile is edited directly.

When viewing a profile, all fields containing data are marked with a yellow clock icon. Hover over this icon to reveal any historical data that has previously been entered in that field.

To reveal historical data for all fields on the profile, select **Actions > Show person history**. All previous information that has been recorded about the person appears below the current information. The date appears beside the previous information, indicating the day it was added to their profile.

GIS and maps

A geographic information system (GIS) is a system that creates, manages, analyzes, and maps location data. A GIS connects location data (where something is) with descriptive information (what it looks like there).

In Axon Standards, GIS information appears in profiles and Analytics.

If your organization uses Axon's Map Service, you can manage your organization's feature layers and list of common names from the Axon Evidence Admin panel. See Map settings permissions for more information about managing who can control your organization's location-related settings.

Axon Standards can use the Esri data set or a custom data set as the source of location data. Contact your Axon representative for more information.

Reports

GIS information appears when you are writing reports.

Depending on the report type, various location-related fields appear, often including Location, Location category/type, and Location note. The location-related fields and entry methods of the options in the **Location** field are outlined in the table below.

Location option	Entry method	Appears in search when adding locations to a report	Appears in Locations search in the Search module
Auto address	Users search the system for verified addresses to add to reports	Yes	Yes
Cross streets	Users search the system for verified addresses to add to reports	Yes	Yes
Manual address	Manually entered by users	No	Yes
Mile marker	Manually entered by users	No	No
Unknown	Manually entered by users	No	No

Note

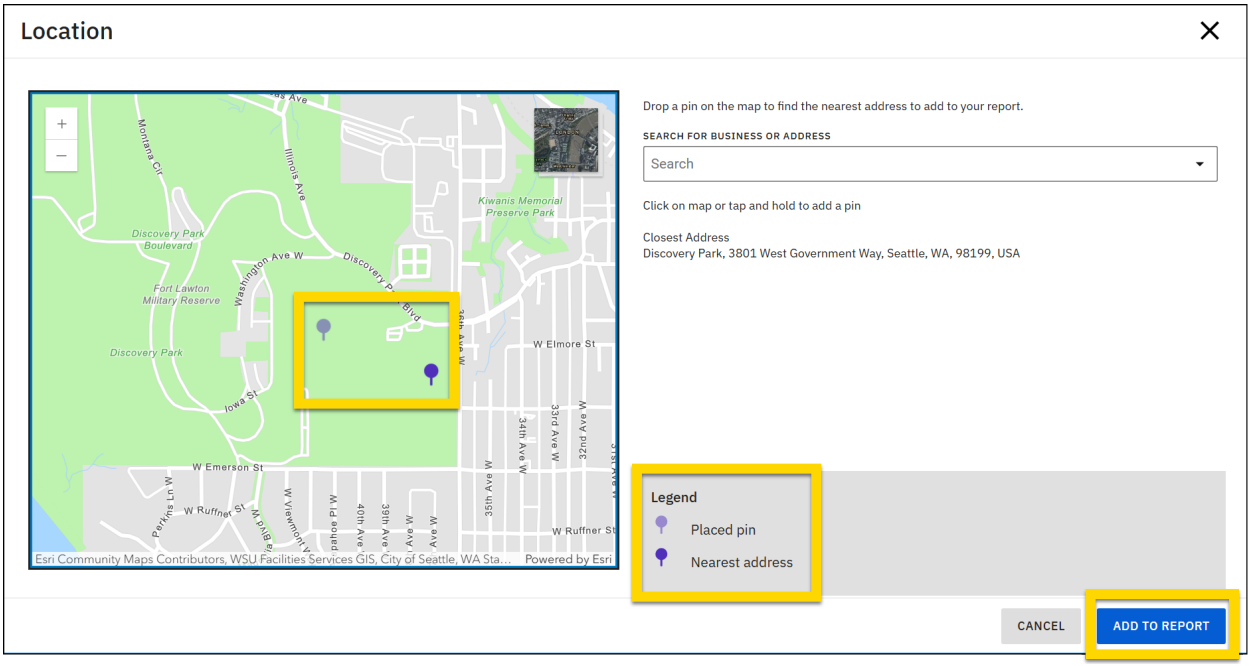
It is generally a best practice to use verified Auto addresses and Cross streets when completing reports. Follow your organization's policy when adding Manual addresses, mile markers, or Unknown locations to reports.

Auto addresses and cross streets

When you select **Auto address** or **Cross streets** from the **Location** field, you can type in the **Address/cross street** field, and a list of possible location matches will appear.

To enter a location by finding it on a map, instead select the map that displays beside the **Address/cross street** field. A larger map window loads. Use the plus and minus buttons to zoom in and out. Click and drag to pan the map and reveal new areas.

Click anywhere on the map to drop a pin. The pin you place appears in light purple, and the nearest verified address appears in dark purple. Select **Add to report** to add the verified address to your report.



You can add subaddress information to auto addresses to specify a particular unit or apartment number. These unit/apartment numbers are considered unique locations, even though they share the same address.

To add a unit, select **Add unit**, then provide the **Unit type** (Apartment, Suite, etc.) and **Unit number**.

Manual addresses

When you select **Manual address** from the **Location** field a set of new fields appears where you can enter the location information.

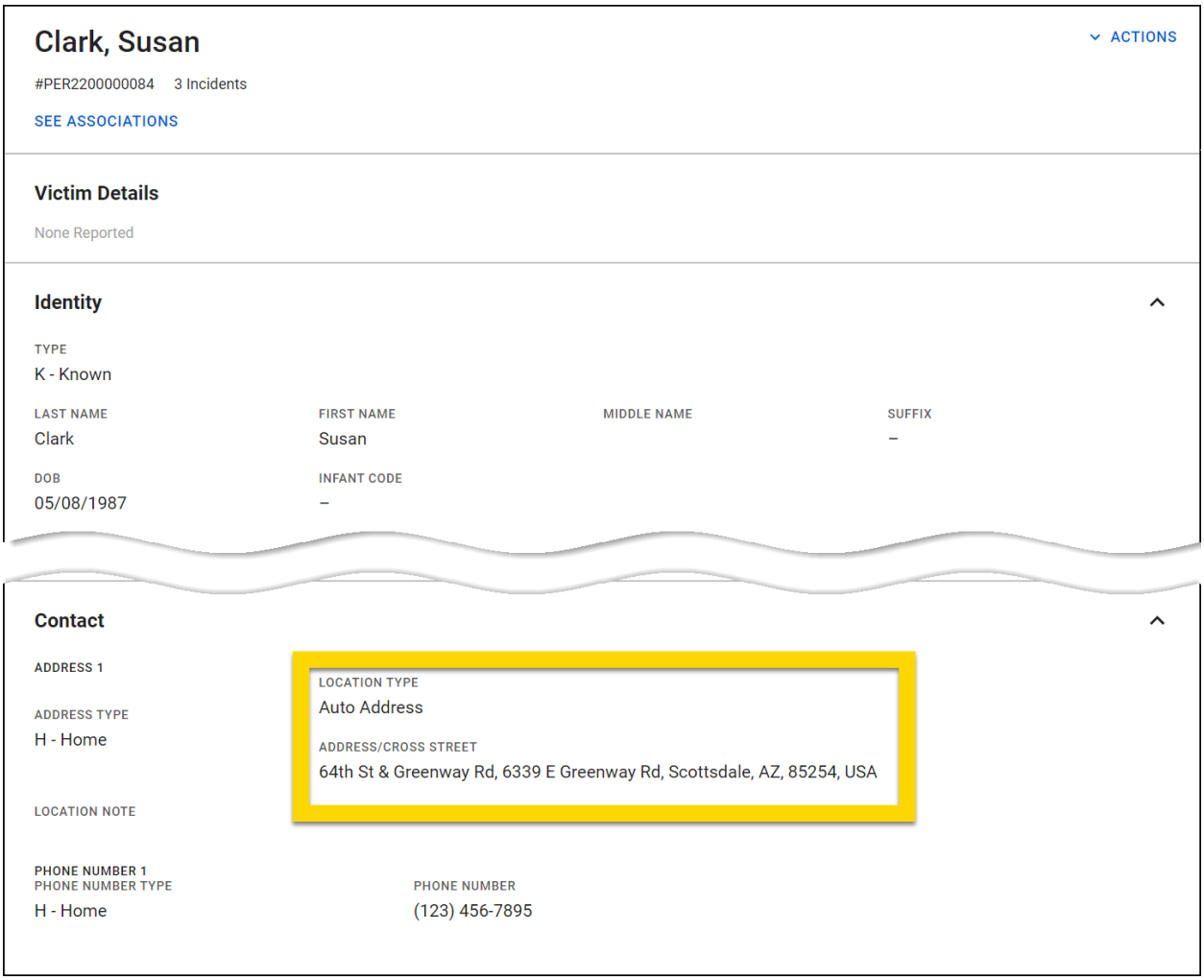
Mile markers, and unknown

When you select **Mile marker** or **Unknown** from the **Location** field a set of new fields appears where you can enter the location information.

Profiles

The location information that is entered in reports is displayed on citizen profiles.

Person



Analytics

GIS information also appears in the maps in the Analytics module.

Feature layers

Axon products use GIS (Geographic Information System) information in address validation, reports, search, and associations (e.g., incidents at a given location).

- A map feature layer is a single map layer that can be created from:
- A map service or feature service
- ArcGIS Online or ArcGIS Enterprise portal items
- An array of client-side features

The layer can be either a spatial (has geographic features) or non-spatial (table). Layers can show school buildings, banks, hazardous locations, live-traffic, camera-feeds, etc.

Users with specific permissions can upload and manage their agency's feature layers in Axon Evidence in **Admin > Map settings > Feature layers**. Each of your agency's layers is displayed on this page, along with the following information:

- Layer name
- Who last updated it
- When it was last updated
- Status (Active, Sync pending, Sync failed)

If your agency has a large number of layers, use the search controls at the top of the window to quickly find a specific layer.

Feature layer details

Select a layer name to view the layer's detail page. Here, you can:

- Preview the layer by clicking on the map and dragging or zooming in and out
- Rename the layer
- Replace the layer
- Download the layer
- Delete the layer
- Edit the Drawing Info (Currently, Axon Standards do not use this feature.)

Warning

Deleting a feature layer cannot be undone. Before deleting a layer, contact your Axon representative and ensure that the Axon product(s) in use by your agency do not rely on that feature layer.

Upload feature layers

You can have up to 100 feature layers in your Axon Evidence account. To add a map layer, take these steps:

1. Open **Admin > Map settings > Feature layers**.
2. Select **Upload layer**.
3. Select **CSV file requirements** or **ZIP file requirements** to view requirements and examples for each file type. (These requirements are also listed here.)
4. Click **Select file**, choose a CSV or ZIP file from your computer, and select **Upload**.
5. It can take up to 30 minutes for a layer to become active. Once the layer's status changes to **Active**, select the layer name to preview it and ensure it renders correctly.
   - If the layer doesn't render correctly, update the styling or contact your Axon representative.
6. Uploading a feature layer does not automatically make that layer visible in your Axon products. Tell your Axon representative that you have uploaded a new feature layer so they can configure the layer for the Axon product(s) you are using.

If you upload a file and the sync fails, select the layer name to view additional information about the failure.

Replace existing feature layers

If a feature layer is outdated or needs to be replaced, take these steps:

1. Go to **Admin > Feature layers**.
2. Select a feature layer name to open the details page.
3. Download the layer to maintain a historical record or to make updates to the existing layer files.
4. Select **Replace** to upload an updated version of the layer.

Double-check before uploading that you are replacing the correct layer type. For example, uploading a Zones feature layer to the Police Stations Hub feature layer would disrupt styling and cause confusion.

Feature layer file requirements

The maximum allowed file size is 48 MB.

CSV

- Must contain a LATITUDE and LONGITUDE column

ZIP

Must contain the following files:

- Shapefile (**.shp** extension) to represent spatial vector data, including points, lines, and polygons in a map
- Index File (**.shx** extension) to represent shape index position
- dBASE File (**.dbf** extension) to store attribute data and object IDs

Can optionally contain the following files:

- Projection File (**.pr**j extension) to specify the metadata associated with the shapefiles coordinate and projection system
- XML Metadata File (**.xml** extension) to represent the metadata associated with the shapefile
- Spatial Index File (**.sbn** extension) to optimize and speed up spatial queries, used with .sbx files
- Spatial Index File (**.sbx** extension) to optimize and speed up spatial queries, used with .sbn files
- Code Page File (**.cpg** extension) to describe the encoding applied to create the shapefile

All files in the ZIP folder must have the same name (except for the file extension). For example:

- County_Boundaries.cpg
- County_Boundaries.dbf
- County_Boundaries.shp
- County_Boundaries.shx

Feature layer styling

In most cases, Axon will style new feature layers for you during configuration. However there are several styling capabilities open to you if you want to update the styling:

- Update existing styling
- Add new styling

Update existing styling (medium complexity):

If your layer has already been styled by Axon, and you want to adjust colors or contrast follow these steps:

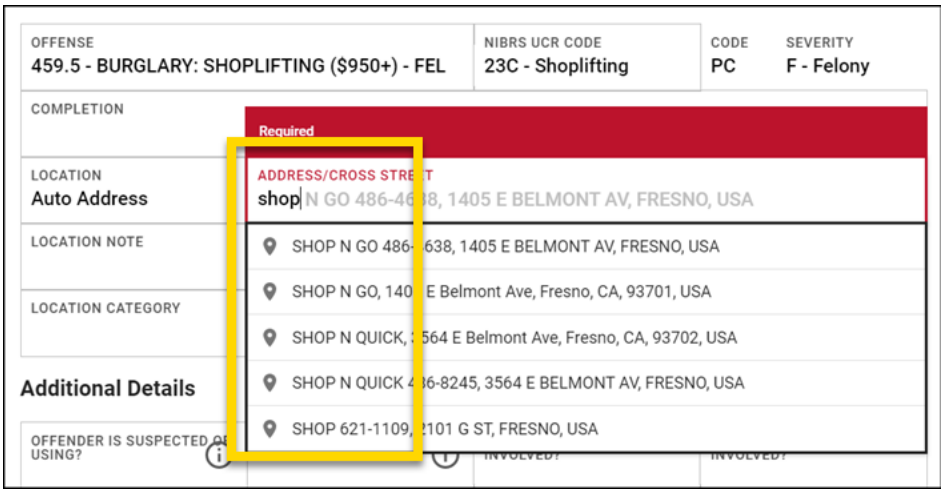
1. Open the feature layer detail page: **Admin > Map settings > Feature layers > Layer name**.
2. Select **Edit drawing** Info to view the current feature layer JSON.
3. Copy and paste the existing Drawing Info JSON into a text editor so you can roll back your changes if needed.
4. Adjust the JSON as desired to update the layer's colors, line widths, etc.
5. Select **Save**. Your changes will immediately reflect both in the layer's preview window and any Axon product currently using the layer.

Add new styling

Contact your Axon representative to create new styling for a feature layer.

Common names

You can add custom names for locations that are commonly known by names other than their addresses. For example, most people may know a store name, but not necessarily its full address. Common names allow users to quickly search and find verified addresses for locations.



Users with specific permissions can manage your organization's common names by logging in to Axon Evidence and selecting **Admin > Map settings > Common names**. Each name that has been created for your organization is displayed, including:

- Location
- Type (Place or Street)
- Last updated on
- Last updated by
- Status (Active, Sync pending, Sync failed, Archived)

If your agency has a large number of common names, use the search controls at the top of the window to quickly find a specific name.

Select **Export results** in the top right corner to export your current search results. You can export to a PDF, Text, CSV, or Excel file. Five hundred names can be exported in a single file. If you need to export more than 500 names, you can export multiple files.

Add multiple common names

Select **Import CSV** to add common names in bulk. Download the example file to ensure that you format your common name file correctly with the following columns:

- **ALIAS_TYPE:** Place or Street
- **ALIAS:** The common name for that location
- **FULL-ADDRESS:** The location's street address, not required if a latitude and longitude are entered instead
- **LATTITUDE:** If the location's **full-address** cannot be validated, a **latitude** and **longitude** is required
- **LONGITUDE:** If the location's **full-address** cannot be validated, a **latitude** and **longitude** is required
- **STATUS:** Active or Archived

Warning

If common names that are bulk uploaded are invalid, they will not appear in the Axon products used by the agency.

Add a single common name

To add a single name, select **Create common name**, provide the following information, and select **Create**:

- **Name**
- **Type:** Place or Street
- **Location:** Street address or GPS coordinates

You can enter a street address or GPS coordinates manually or select a point on the map to autofill the exact GPS coordinates in the **Location** field.

Edit a common name

Select a common name to update the name, type, location. You can interact with the map by clicking and dragging or zooming in and out. Select **Archive** to archive the name.

Note

Common names can only be archived; they cannot be deleted.

Case and investigation management

The Case Management module supports modern investigative work by providing a structured, secure, and collaborative environment for managing cases from initiation through disposition. While investigative workflows may differ across teams and jurisdictions, the core needs remain consistent: organize information clearly, protect sensitive data, coordinate across units, and maintain evidentiary integrity.

Axon's case management solution is built around a simple philosophy: investigators should spend more time solving cases and less time managing systems. The module centralizes case information, streamlines routine processes, and ensures that the right people have access to the right information at the right time.

The design of the module is guided by several foundational principles:

- Security and compliance: Sensitive investigative data is protected through robust authentication, granular access controls, and support for legal and regulatory requirements.
- Collaboration: Features are designed to facilitate coordinated work, shared visibility, and structured review processes across multiple units, roles, and organizations.
- Integrated digital evidence management with Axon Evidence: A centralized digital evidence repository with contextual metadata, secure chain of custody, and cross-agency sharing supports collaboration, preserves digital evidence integrity, and strengthens courtroom preparation.
- Efficiency through automation: Routine processes such as case creation, task management, workflow transitions, and review triggers are structured to reduce manual effort and minimize errors.
- Continuous improvement: The module continues to evolve to address operational gaps, emerging investigative models, and increasing digital evidence demands.

The Case Management module helps users organize, investigate, and resolve work originating from incidents and intelligence. There are three key concepts used throughout the module:

- **Events** capture and record the specifics of what happened during a specific event
- **Cases** manage the formal investigative workflow performed following an event.
- **Investigations** capture proactive or intelligence-driven work that is not yet tied to a formal event report.

Within the module, cases and investigations move through a life cycle: Triage → Assignment → Active Investigation → Review → Disposition → Closure. Throughout this life cycle, users manage their work using various features:

- **Inboxes** manage the organization’s cases and investigations workloads.
- **Tasks** help users track work for a given case or investigation.
- **Documents** capture findings for a given case or investigation.

- **Evidence** is added to cases and investigations to support findings.
- **Disposition workflows** allow users to finalize the outcomes of cases and investigations.

Access this module by selecting the folder icon in the navigation menu. All case management functionality is controlled by privileges. This granular access control guarantees case data and tools are accessed by the appropriate users and prevents sensitive information from falling into the wrong hands.

Users with access to the Case Management module can:

- Create cases from an existing event report.
- Create investigations without event reports to document field intelligence, tips, or proactive leads.
- Find and triage cases and investigations that need supervisor decisions for whether those cases should be assigned, closed, or wait for more information.
- View the inboxes for their units.
- Create case and investigation documentation
- Create tasks to manage the progress of cases and investigations
- Manage files and folders associated with the case or investigation.
- View a log of activities, either performed by a user or generated by the system.
- Review cases with disposition update requests.
- Share cases or investigations with other users or organizations.

Watch this video for an overview of case management in Axon Standards.

Configuration options

Organizations can configure the following features for cases and investigations:

- Unit names (and the corresponding unit inbox names)
- The "Lead Detective" label that appears throughout the cases (not investigations) experience
- Case and investigation summary templates
- Task types and a list of tasks that are auto-generated upon case creation
- Task workflows, including a simplified review workflow
- Lead detective notifications when tasks are marked as complete
- Case and investigation documents
- Routing rules
- The folder structure that appears on the **Files** tab of the case profile

- Activity types in the activity log
- Case and investigation disposition values (internal, disposition reason, and external)
- Case reviews for disposition updates workflows
- Privileges that determine which users can access which case management features.

For more information about configuring the Case Management module for your organization, contact Axon Support or your Axon representative.

Inboxes

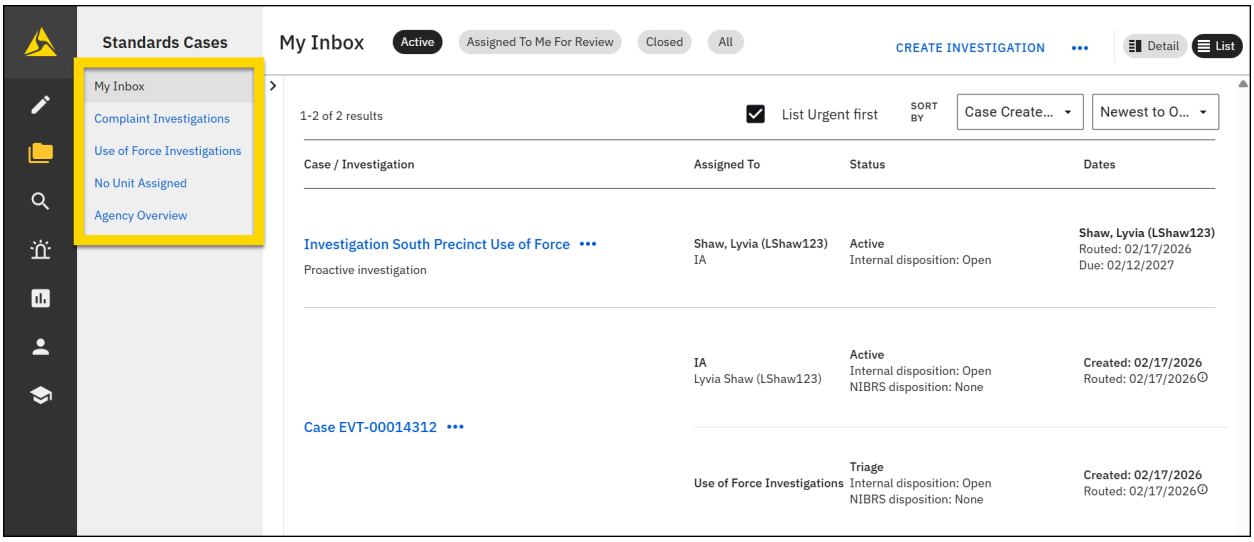
When you open the Case Management module, you'll see a set of inboxes. Inboxes are the primary way users organize and manage their investigative workloads. Each inbox represents a different stage of work or scope of responsibility:

- My Inbox: Cases and investigations you have been assigned to and are directly responsible for.
- Unit inboxes: Cases and investigations owned by your team (e.g. Robbery, IA Investigations, etc.).
- Agency Overview: All cases and investigations across the organization. This inbox is generally used by supervisors to help them understand all investigative work being done by the organization.
- Triage: Cases and investigations not yet assigned to a detective.
- No Unit Assigned: Cases and investigations that do not have the necessary information to be routed to a specific unit yet.

Access to inboxes is controlled by privileges; some users see inboxes that others can't.

Note

If your organization uses both Axon Records and Axon Standards, you will only see inboxes for the product you are currently signed into. Select the app switcher (Axon logo) in the top left corner to switch between Axon Records and Axon Standards.



Depending on your privileges, you will see different tabs in each inbox. The My Inbox tabs include:

- **All:** All cases and investigations that you are assigned to as the lead detective
- **Active:** Active cases and investigations that you are assigned to as the lead detective
- **Assigned to Me for Review:** Cases and investigations that are assigned to you to review
- **Closed:** Closed cases and investigations that you are assigned to as the lead detective

Unit inboxes and the Agency Overview inbox tabs include:

- **All:** All cases and investigations that have been assigned to that unit
- **Triage:** Cases and investigations assigned to that unit but not yet assigned to a lead detective
- **Active:** Cases and investigations assigned to a lead detective
- **Closed:** Cases and investigations that have been closed
- **Disposition in Review:** Cases where a supervisor case review has been requested

The No Unit Assigned inbox tabs include:

- **All:** Cases and investigation that do not have the necessary information to be routed to a specific inbox
- **Triage:** Cases and investigation that do not have the necessary information to be routed to a specific inbox and have not yet been assigned to a lead detective
- **Closed:** Closed cases and investigation that do not have the necessary information to be routed to a specific inbox

To further refine which items are displayed on each tab, select the arrow to the left of the case list to reveal a list of filters:

- Urgency
- Lead detective
- Due date
- Victims
- Case/Investigation name
- Initial Report Author
- Location: Reporting Area (District, Beat, Zone)
- Units (Agency Overview inbox only)

Use the controls in the top right corner to take the following actions:

- Select **Create investigation** to start a new investigation.
- Select **More actions [...]** to export the cases displayed on that inbox tab to a CSV file.
- Select **Detail** or **List** to change how the information is displayed in the inbox
- Select the **List urgent first** checkbox to pull any cases or investigations marked as Urgent to the top of the list.
- Use the date options in the **Sort by** menus to change the order in which cases and investigations are listed:
  - Case created date
  - Due date
  - Last routing date
  - Last unit transferred date

Detail view

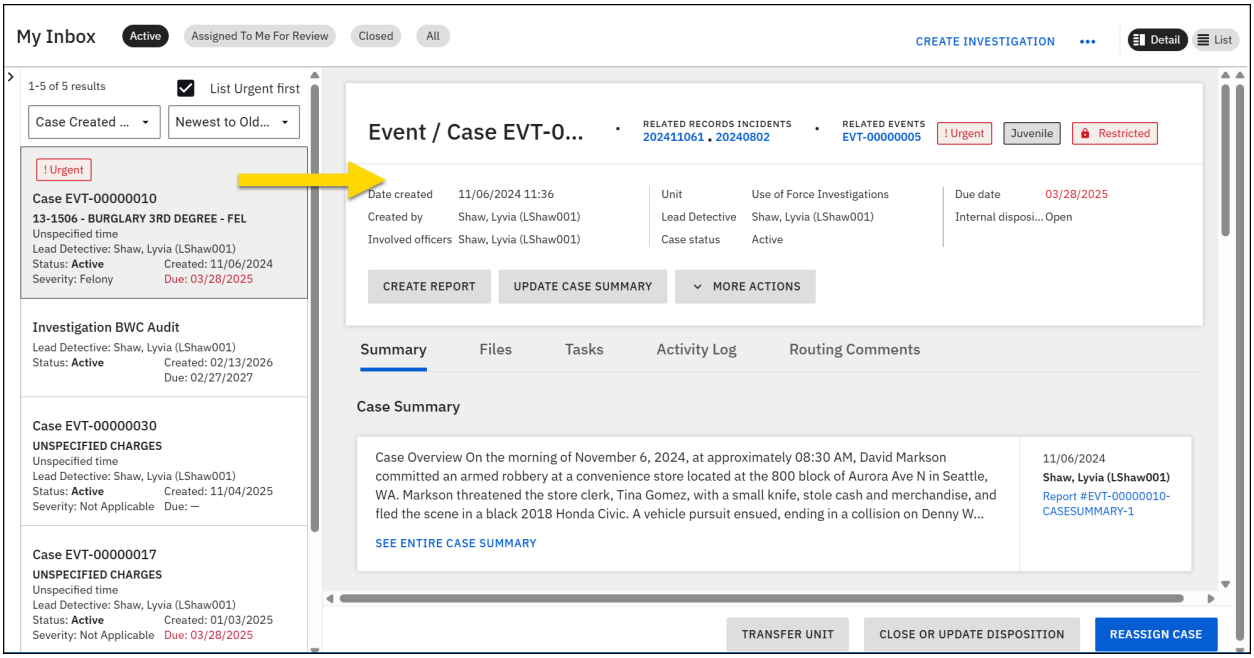
Detail view (the default view for unit inboxes and the Agency Overview inbox) displays a split-screen layout. The left pane lists all cases and investigations in the inbox. When you select a case or investigation from the list, its profile appears on the right. Use this view to quickly triage and assign cases.

When viewing the profile, you can switch between tabs and manage the reports, case summary, files, case tasks, and activity log. Use the blue and gray buttons at the bottom of case profiles to:

- Transfer the case to a different unit
- Close the case
- Assign or reassign the case

The following information is displayed for each case and investigation in the list. Wherever you see **(+1 more)**, **(+2 more)**, etc., hover to view the additional information.

Case	Investigation
• Labels that indicate if the case is marked as Urgent or has a disposition update under review • Case ID and custom name • Offense • Event time • Lead detective • Status • Severity • Creation date • Due date	• Investigation name • Lead detective • Status • Creation date • Due date



List view

List View (the default view for My Inbox) shows basic information about each item, including:

- **Case/Investigation**
  - If the item is a case
    - If the case is marked as Urgent or has a disposition update that is under review
    - Case ID: Selecting the blue hyperlink opens the case profile

    - If the item is an investigation
        - Investigation name
- **Assigned To**
    - The unit the case or investigation has been assigned to
    - The lead detective from that unit who has been assigned to
    - If the case or investigation has been assigned to multiple units, each unit and associated lead detective is listed.
- **Status**
    - Status
    - Internal disposition
- **Dates**
    - Created date
    - Routed date: Hover over the information (i) icon to view routing comments.
    - Due date: If the date has passed, the date appears in red text.
    - Last unit transfer date: The last date the case was transferred to a new primary unit.

Cases and investigations

Cases and investigations have different features, which help determine when you should use a case or an investigation to manage your work. The table below outlines these features:

Feature	Case	Investigation
Requires an incident report	Yes	No
Has a NIBRS disposition	Yes	No
Has an internal disposition	Yes	Yes
Can be automatically created from an incident	Yes	No
Has evidence integration (i.e., uploaded evidence is also uploaded to Axon Evidence, where it can be managed and shared)	Yes	Yes

Cases

Cases manage the formal investigative workflow performed following an event. Once created, a case serves as the central workspace for investigation management. Cases ensure accountability and structure, helping organizations move work from the initial report to its final outcome.

Cases enable organizations to:

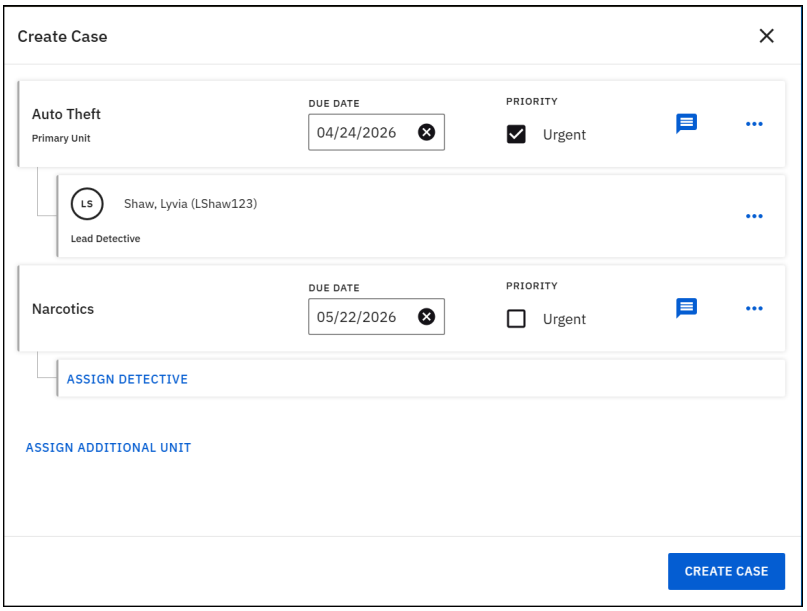
- Assign responsibility to units and detectives
- Track progress through tasks
- Document findings
- Mange disposition and closure

Case management involves creating, assigning, and tracking cases from initial report through disposition while ensuring the right units and personnel are responsible for each step. It includes managing assignments, transfers, due dates, and workload distribution to support efficient investigations and oversight.

Create cases

To create a case:

1. Open an event profile and select **More actions > Create case**.
2. Assign the case to a primary unit and (optionally) a lead detective within that unit.
   - The "Lead Detective" label is customizable and may appear differently across organizations.
3. Optionally, set a due date, mark the case as urgent, and select the comment icon to add routing notes.
4. Some organizations are configured to allow cases to be assigned to a primary unit as well as one or more additional units.
   - To assign additional units, select **Assign additional unit** after selecting a primary unit and lead detective.
   - You can set unique due dates, priority level, and routing comments for each unit.



5. Select **Create case**.
6. Once the case is created, the profile changes into a case profile, which displays additional information and options.

Case profiles

When a case is created for an event, the event profile becomes a case profile, which shows additional information and actions.

The case profile is the primary workspace for investigators. It consolidates all information related to the case--reports, tasks, evidence, activity history--in a single view. This unified view helps users manage and progress the investigation efficiently, including:

- View case details, including:
  - Unit(s) the case is assigned to
  - Lead detective(s) the case is assigned to
  - Status (for each assigned unit)
  - Internal disposition (for each assigned unit)
- Use the buttons to:
  - Create or update the case summary
  - Create case documents
- Take case-related actions from the **More actions** menu:
  - Create activity
  - Add file
  - Link related incident reports and Standards events

  - Manage restrictions
  - Edit case name
  - Update due date
  - Update case assignment
  - Transfer unit
  - Update case disposition
  - Manage classic shares
  - Share case
  - Prepare documents for sharing
  - Print event
- View case-related information on the different tabs:
  - Summary
    - Case summary: View the summary the lead detective updates throughout the case.
    - Case documents: Contains all documents created for the case.
  - Files: Manage the files that have been added to the case.
  - Tasks: Manage the tasks that have been created for the case.
  - Activity log: Manage all case activities.
  - Routing comments: View all comments created during case routing.

Note

Some of these options may not appear to all users based on the privileges they have been assigned.

Summary tab

When a case is created, the **Summary** tab displays two additional sections:

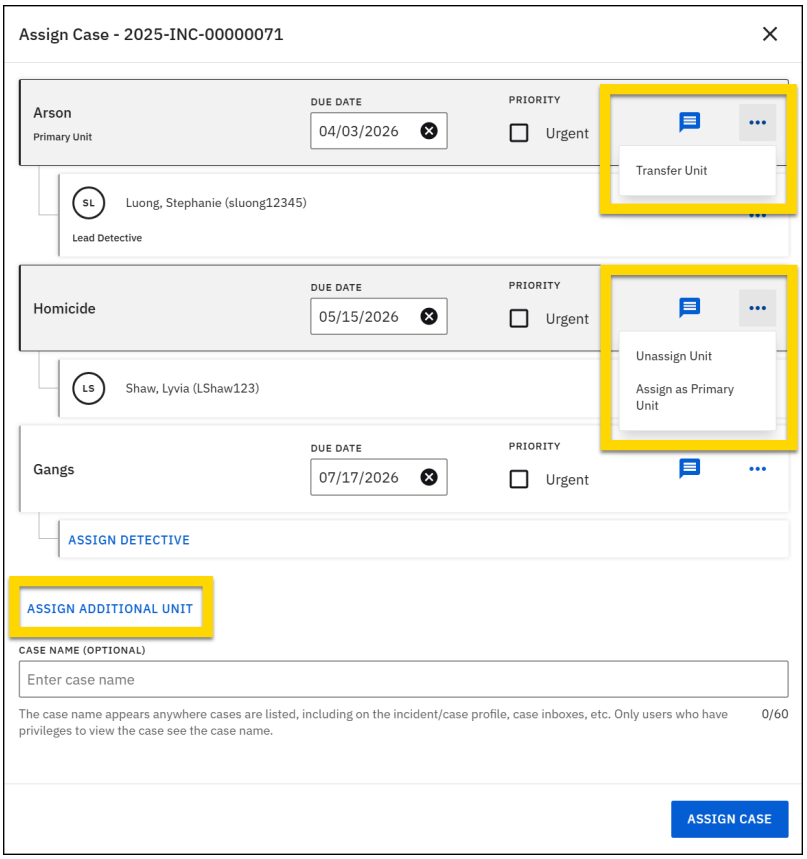
- Case summary: This section appears at the top of the **Summary** tab. The case summary feature helps the Lead Detective assigned to the case keep an up-to-date summary of the case throughout the investigation.
- Case documents: Links to all case documents appear in this section. Select the Document ID in the **Report** column to open and view the document.

Update case assignments

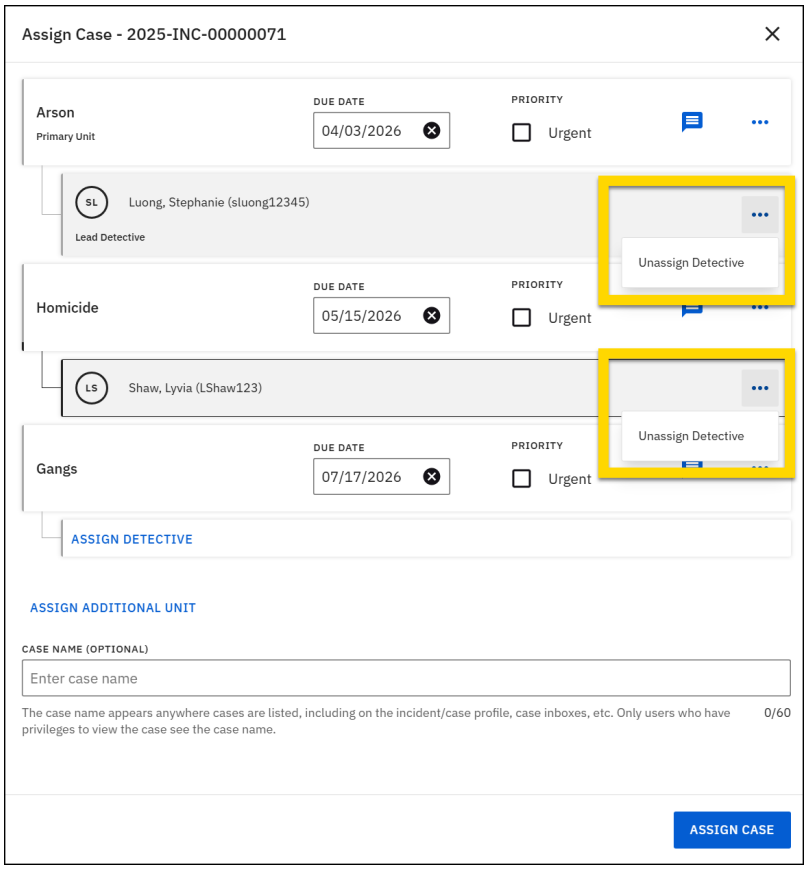
To manage case assignments, a user must have the Triage privileges for all affected units (the unit(s) the case is currently assigned to, as well as the unit(s) the case will be assigned to).

To update a case's lead detective or unit assignment:

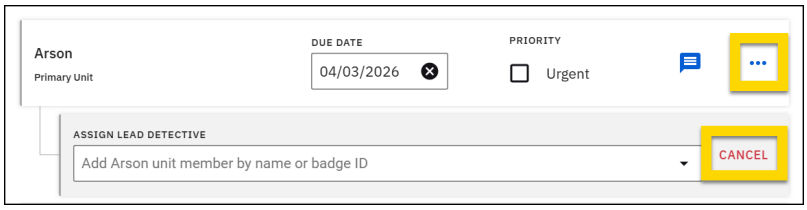
1. Open the case profile.
2. Select **More actions > Update case assignment**.
3. Manage the case's unit assignments:
   - Assign additional units
     - To add an additional unit, select **Assign additional unit** and search for the unit name. Optionally, assign a lead detective for the unit.
   - Unassign additional units
     - To remove an additional unit, find the unit's row and select **More actions [...] > Unassign unit**.
   - Change primary unit
     - If the unit you want to make the primary unit is already assigned as an additional unit, find the unit's row and select **More actions [...] > Assign as primary unit**.
     - If the unit you want to make the primary unit is not yet assigned, in the current primary unit row, select **More actions [...] > Transfer unit** and add the new unit.
     - You can also reassign the case to a new primary unit by selecting **More actions [...] > Transfer unit**



4. Manage the case's lead detective assignments:
   - To change the assigned lead detective for a given unit, in the detective's row, select **More actions [...] > Unassign detective** then search for and select a new lead detective.



- You do not have to select a lead detective for a unit.
  - To leave the lead detective unassigned in the primary unit, select**More actions [...] > Unassign detective** then **Cancel**.



- To add a new detective from a new unit, select **Assign additional unit**, select a unit, then add the lead detective.

5. Optionally, set a due date, mark the case as urgent, and select the comment icon to add routing notes.
   - You can adjust these items for each unit assigned to the case.
6. Select **Assign case** at the bottom of the screen to apply your changes.

Transfer primary unit

To transfer a case to a new primary unit, a user must have the Triage privileges for all affected units (the unit(s) the case is currently assigned to, as well as the unit(s) the case will be assigned to).

To transfer a case to a new primary unit:

1. Cases can be transferred from two locations:
   - On the case profile, select **More actions > Transfer unit**.
   - When viewing a case from a case inbox in Detail view, select **Transfer unit** at the bottom of the screen.
2. Search for a new primary unit and lead detective.

   Note

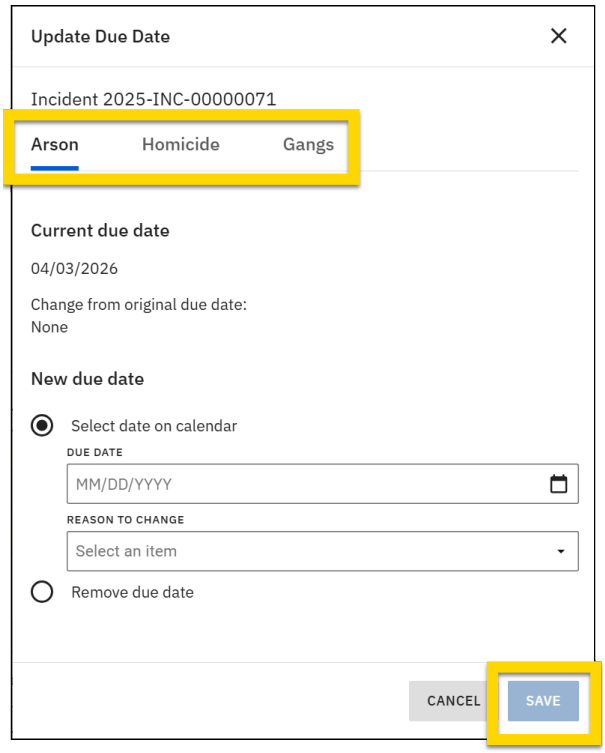
   If the unit you want to make the primary unit is already assigned to the case as an additional unit, instead select **More actions > Update case assignment** and follow the steps above to adjust the primary unit assignment.
3. Optionally, set a due date, mark the case as urgent, and select the comment icon to add routing notes.
4. Select **Transfer**.

Update case due dates

Case due dates can be created for each case a unit is assigned to. To manage case due dates:

1. Open the case profile.
2. Select **More actions > Update due date**.
3. Each unit assigned to the case appears as a tab.
4. Adjust the due date for each unit as required and provide a change reason.

5. After you make a change to each tab, select **Save** to apply your changes.
   - If you update due dates for multiple units, be sure to select **Save** after you make a change on a tab before you move to the next one.



Caseload visualization

Caseload visualization gives a supervisor information to balance work more effectively when assigning investigations. When you assign a new investigation or transfer an existing investigation, the options in the **Lead detective** field display the number of active cases and investigations currently assigned to each detective in that unit.

Investigations

Investigations capture proactive or intelligence-driven work that is not yet tied to a formal event report. Organizations typically use investigations for:

- Gathering intelligence
- Tracking tips and leads
- Documenting ongoing surveillance
- Performing proactive investigative work

If an investigation is later tied to a specific event, a case can created to track the formal investigative work for that event.

Create investigations

To create an investigation:

1. Open the Case Management module and select **Create investigation** in the top right corner.
2. Give the investigation a name.
3. Assign the case to a primary unit and a lead detective within that unit.
   - The "Lead Detective" label is customizable and may appear differently across organizations.
4. Optionally set a due date.
5. Select **Create**.
6. Once the investigation is created, the profile opens where you can begin adding information.

Investigation profiles

When an investigation is created, an investigation profile is generated. From this top section of the profile, you can take the following actions:

- View investigation details, including:
  - Creation date
  - Unit the investigation is assigned to
  - Lead detective(s) the investigation is assigned to
  - Investigation status
  - Internal disposition
- Use the buttons to:
  - Create or update the investigation summary
  - Create case documents
- Take additional actions from the **More actions** menu:
  - Investigation management
    - Rename investigation
    - Reassign investigation
    - Transfer unit

        - Update disposition
        - Update due date
        - Manage restrictions
    - Evidence management
        - Add file
        - Create community request
    - Sharing and print
        - Print investigation
        - Prepare investigation for sharing

Below the top heading section, you can switch among the tabs to view information and take various additional actions:

- Summary: View offenses, people, organizations, narratives, vehicles, property, and reports that have been added to the investigation.
- Files: Mange all files that have been added to the investigation, either to the reports and investigation documents or directly to the investigation.
- Tasks: Manage the tasks that have been created for the investigation.
- Activity log: Manage the log of all actions taken on the investigation.

Reassign investigations

To manage an investigation's lead detective, a user must have the Triage privileges for the unit currently assigned to the investigation. To update an investigation's lead detective:

1. Open the investigation profile.
2. Select **More actions > Reassign investigation**.
3. Select the X icon beside the lead detective's name and enter a new name.
4. Add a routing note, update the due date, and mark the investigation as urgent (as applicable).
5. Select **Assign investigation**.

Transfer unit

To transfer an investigation to a new unit, a user must have the Triage privileges for all affected units (the unit the investigation is currently assigned to, as well as the unit the investigation will be assigned to).

To transfer an investigation to a new unit:

1. Open the investigation profile.
2. Select **More actions > Transfer unit**.
3. Search for a new unit and lead detective.
4. Optionally, set a due date, mark the case as urgent, and select the comment icon to add routing notes.
5. Select **Transfer**.

Update investigation due dates

To manage investigation due dates:

1. Open the investigation profile.
2. Select **More actions > Update due date**.
3. Adjust the due date as required and provide a change reason.
4. Select **Save** to apply your changes.

Caseload visualization

Caseload visualization gives a supervisor information to balance work more effectively when assigning investigations. When you assign a new investigation or transfer an existing investigation, the options in the **Lead detective** field display the number of active cases and investigations currently assigned to each detective in that unit.

Case and investigation tasks

The case and investigation tasks feature lets you track the work being done throughout an investigation. Tasks break down investigative work into actionable steps and can track anything from administrative steps to complex investigative actions. Tasks can be configured to move through review workflows when oversight is needed. Tasks allow supervisors and detectives to:

- Assign work to individuals and teams
- Track progress and accountability
- Facilitate collaboration across units

Tasks can be found in the following locations:

- **Tasks** tab on case and investigation profiles
- My Tasks inbox in the Tasks module
- Team inboxes

Tasks tab (case and investigation profiles)

All tasks associated with a case or investigation can be found by opening the profile and switching to the **Tasks** tab. This tab only appears to users who belong to command hierarchy groups or teams with specific privileges.

The following information is displayed for each task:

- Task type
- Assignee
- Creation date
- Due date
- Status
- Unit owner (only appears for organizations who assign cases to multiple units)

Select a column name to sort the list either ascending or descending, according to the information contained in that column. Use the following filters to refine which tasks are displayed:

- Task name
- Assignee
- Due date
- Creation date
- Last updated date
- Status

Reorder tasks

To adjust the order in which tasks are displayed on this tab, select **Edit task order** in the top right corner of the tab. While in this Edit mode, you can drag and drop tasks to any position in the list, or type a number in the **Order** column to move a task to a specific location in the list. After making adjustments, select **Save** above the task list.

This task order is displayed for all users who can access the case or investigation. The order "sticks", even if you leave the page and come back or log out and back in.

When new tasks are created, they are added to the bottom of the list.

If the case or disposition is moved into a Closed or Disposition In Review status, the task list is frozen and can't be edited unless the status changes.

My Tasks inbox

All tasks assigned to you appear in your My Tasks inbox.

Team inboxes

Some tasks are routed to a specialized team inbox, such as CSI or Legal Affairs, that can be accessed by users who have certain privileges. These inboxes are configured for your organization and appear in the Tasks module along with the rest of the report task inboxes.

Team inboxes contain the following tabs:

- To Do
- Submitted for Review
- Rejected Requests
- All

The most recently updated tasks appear at the top of the list. Use the filters to constrain which tasks are displayed:

- Assignment (Team inboxes)
- Created by
- Due date
- Incident / Report ID
- Request date
- Task action
- Task type

The following information is displayed for each task in the inbox:

Task

- What the task is and the Task ID

Created by

- Who created the task
- When it was submitted
- When it was last updated

Last routed

- Who routed the task
- When it was assigned
- Any additional messages related to the task

Assignee

- Who the task is currently assigned to

Create tasks

Depending on how your organization has configured the Case Management module, tasks can follow two different workflows:

- **Basic task:** Can be completed independently and do not require a review before completion
- **Review task:** Require submission, review, and approval before completion

These two different task workflows help organizations enforce quality control for critical tasks while keeping simpler tasks lightweight.

To create a task:

1. Open the case or investigation profile, switch to the **Tasks** tab, and select **Create task**.
2. Select a task type.
   - If the task type doesn't appear when you enter letters into the field, a new option of **Create a custom task** appears. Select this option to create the custom task.
3. If your organization assigns tasks to multple units, select a Unit Owner for the task.
4. Select **Create task**.
5. The task will be automatically assigned to you once it is created.
   - Update the due date, complete the form fields, add files, and insert comments, as needed.
   - The **Detective Notes** field is only visible to detectives and users with specific privileges and can be used to document sensitive information related to the task. Usually, task contributors will not see this field, so don't include any information here that is needed to complete the task.
6. Select **Save** and close the task to work on later or select **Submit** to complete it or route it to another user.

When you close a task, either after submitting it or marking it complete / not applicable, it appears on the **Tasks** tab. From here, you can take several actions, which appear in the **Actions** column on the task list:

- **Update:** Appears on open or in progress tasks; let's you open and continue working on the task
- **View:** Appears on closed and not applicable tasks; lets you view the task and reopen it if needed
- **More actions [...] > reassign:** Lets you assign the task to another user
- **More actions [...] > Mark as not applicable:** Lets you close the task and set its status to Not Applicable

Auto-created tasks

You can configure a set of tasks to be automatically generated when a case is created. This list of tasks can be the same for every case or vary based on the type of case or the unit it is assigned to.

For additional information, contact your Axon representative.

Work on tasks

You can take several actions when working on tasks:

- Update task
- Add task result
- Complete linked form
- Reject a task
- Review a task

Update task

To update a task, open the task either by selecting the task name in a task inbox or by selecting **Update** on the **Tasks** tab on the case or investigation profile. When the task opens, you can update the following items, in addition to any custom fields on the task:

- Task name
- Due date
- Unit Owner
- Comments
- Files (you must be assigned to the task to add files to it

Unlike when writing a report in Report Writer, information entered in the task window does not auto-save. To save your changes, select **Save**. If you have finished your work, select **Submit** to either mark the task as complete or to send it for review.

Add task result

Some tasks have an **Add task result** button that inserts a field where you can document your work for that task. Select **Save** when you have finished updating this field.

Complete a linked form

Some tasks require additional information to be entered into a linked form. Select **Update** to open Report Writer and complete the form. Information entered in this form is auto-saved, just as it is for reports. Select **X** to return to the task window where you can save or submit the task.

When adding people, organizations, vehicles, or property to a linked form, a list of suggestions appears if those items were previously added to the incident/event report or other case documents and tasks. Quickly add any of these items to the document by selecting it.

Reject a task

Some tasks can be submitted to other users/teams to be worked on. If a task is submitted by a detective but can't or shouldn't be worked on by the person it is submitted to, the task can be rejected by following these steps:

1. Open the task either by selecting the task name in a task inbox or by selecting **Update** on the **Tasks** tab on the case or investigation profile.
2. Select **Reject request**.
3. The task is auto-assigned to the lead detective, but you can update this if needed. Leave comments as necessary, adjust the due date if needed, and select **Reject request**.

Review a task

Some tasks can be submitted to other users/teams, worked on, then submitted back to the lead detective for review. To review a task that has been submitted for Detective Review:

1. Open the task either by selecting the task name in a task inbox or by selecting **Review** on the **Tasks** tab on the case profile.
2. Select either **Reject** or **Approve**:
   - **Reject:** The task can be routed back to the person who worked on it (or a different user) for revisions
   - **Approve:** The task is marked as Complete and unassigned from all users.

Reassign tasks

A task can be reassigned to a different user at any time from two locations:

- Task inbox: Select **Reassign** in the **Actions** column.
- **Tasks** tab on the case or investigation profile: In the **Actions** column, select **More actions [...] > Reassign**.

Select a user from the **Assign to** field and add comments or update the due date as necessary. To change just the due date, keep the task assigned to the same user and instead only update the **Due date** field. Select **Reassign**.

If your organization assigns cases and investigations to multiple users, note that the Unit Owner of a task doesn't change if you reassign the task to a user in a different unit. Select the pencil icon on the task to update the Unit Owner to reflect the new unit.

Note

To assign the task to a detective for review, submit the task instead of reassigning it.

Submit tasks

After you create a task or a task is assigned to you, you can submit it either as complete or as Not Applicable. The submission process for the two kinds of tasks (Basic task or Review task) is slightly different.

Axon Records and Axon Standards can be configured such that the lead detective of a case or investigation receives an email if any task is marked as complete. To set up this configuration for your organization, contact your Axon representative.

Basic task submission

To submit a Basic task, take these steps:

1. Open the task either by selecting the task name in a task inbox or by selecting **Update** on the **Tasks** tab on the case or investigation profile.
2. Add files or comments to the task as necessary and select **Submit**.
3. Select one of the two completion options:
   - **Mark as complete:** Unassigns the task and sets its status to Complete
   - **Mark as not applicable:** Unassigns the task and sets its status to Not Applicable
4. Add comments as necessary and select **Submit**.
5. The task remains on the **Tasks** tab and can be viewed or reopened by selecting **View**.

Review task submission

To submit a Review task to another user or team to work on, take these steps:

1. Open the task either by selecting the task name in a task inbox or by selecting **Update** on the **Tasks** tab on the case or investigation profile.
2. Add files or comments to the task and select **Submit**.
3. Select **Request in progress**.
4. A new set of fields appear where you can specify who the task should be routed to, as well as its due date.
   - You can submit a task to a specific user, to a team task inbox, or to both.

5. After assigning the task, select **Submit**.
6. The task remains on the **Tasks** tab with a status of Request In Progress.

Once submitted to a user/team, a review task can be rejected or worked on and submitted back to the detective for review:

1. Open the task either by selecting the task name in a task inbox or by selecting **Update** on the **Tasks** tab on the case or investigation profile.
2. The task is auto-assigned to the case's lead detective, but you can update this if needed. Leave comments and adjust the due date if needed.
3. Select **Submit for detective review**.
4. The task is assigned to the lead detective, and its status on the **Tasks** tab is updated to Detective Review.

Mark tasks as not applicable

To submit multiple tasks as Not Applicable:

1. Open the **Tasks** tab on the case or investigation profile.
2. Use the checkboxes to select multiple tasks.
3. Select **More actions [...] > Mark as not applicable**.

Reopen tasks

If a task has been marked as complete but later needs to be updated, you can open the task and select **Reopen task**. After assigning the task, setting a due date, and adding comments, the task can be reopened.

View task history

To view actions taken on a task, open the task and select **View task history**. The pane that opens displays actions taken on the task, as well as the date and time the action was taken.

Case and investigation documentation

You can document work on a case or investigation by using the summary feature and creating case or investigation documents. Documentation captures narratives and

supporting details throughout a case or investigation lifecycle. While reports document the original event, case and investigation documentation lets investigators record ongoing findings, analysis, and supplemental information.

Summary

The lead detective assigned to a case or investigation can use the summary feature to create and continuously update a narration throughout their investigation. The summary is often used to:

- Communicate status to supervisors
- Provide context for reviewers
- Prepare information for prosecutors or other external parties the case or investigation is shared with

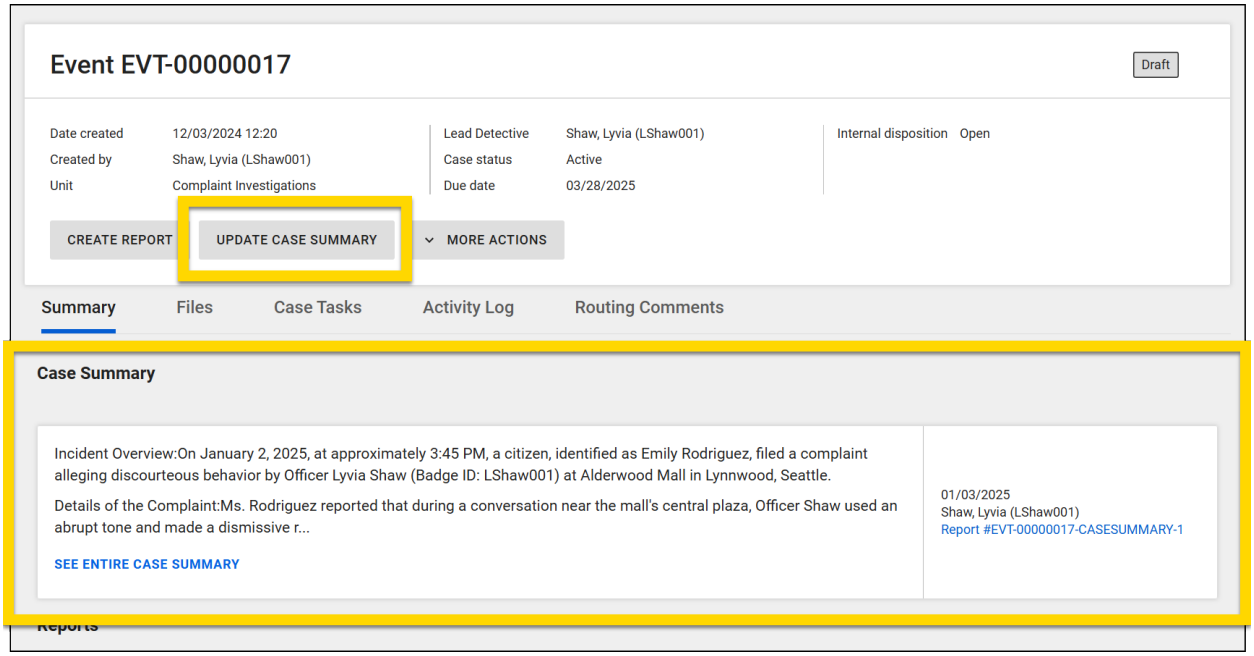
The summary can be reassigned to a user other than the lead detective and only appears to users with specific privileges.

Follow the steps below to create a summary:

1. Open the case or investigation profile and select **Create case summary** or **Create investigation summary** in the profile header.
2. Report Writer opens where you can enter your summary and upload files as needed. All content entered on this page is auto-saved.
   - Your organization may have configured a template you can import to quickly format your summary.
3. Open the **More actions [...]** menu to:
   - View event
   - Edit custom name
   - View report history
   - Manage restrictions
   - Print
4. Select **Reassign author** in the footer to assign the summary to a user other than the lead detective.
5. Select the **X** button in the top right corner of the screen to close the summary without finalizing it.
6. Select **Submit** to finalize the summary. Users with specific privileges can revert the finalization as necessary.

Once a summary has been created, a new **Case/Investigation summary** section appears at the top of the profile, and an entry for *Case/Investigation Summary created* is

added to the activity log. Select **See entire case/investigation summary** to open the summary window. To edit the summary, select **Update case/investigation summary**.



If your organization uses the workflow to assign multiple units to a case, a case summary can only be created and maintained by the lead detective of the primary unit. Lead detectives for additional units do NOT have case summaries. Instead, a case document can be configured to allow these additional units to manage documentation for their units' investigation.

Case and investigation documents

Case and investigation documents let you record information not associated with a report or case task. All documents, including the summary, appear in the **Case documents** or **Investigation documents** section at the bottom of the case or investigation's **Summary** tab. Only users with specific privileges can view this section. Select the blue Report ID to open and view any of these documents.

To create a document:

1. Open the profile and select **Create report** in the profile header.
2. In the **Case/Investigation documents** section, select a document type and add a custom name if desired.
3. If your organization assigns cases to multiple units, add a Unit Owner for the document.
4. After naming the document, select **Create report**.
    - The documents listed in this window vary among organizations.

5. Report Writer opens where you can work on the document. Select the sections on the left side of the screen to move through the document and the sidebar button to enter comments.
   - When adding people, organizations, vehicles, or property to a document, a list of suggestions appears if those items were previously added to the other reports, documents, or tasks associated with that case/investigation. Quickly add any of these items to the document by selecting it.
6. Open the **More actions [...]** menu in the top right corner of Report Writer to:
   - View event
   - Edit custom name
   - View report history
   - Copy info to new report
   - Print
   - Revert finalization (only for finalized documents)
7. Once you have completed the document, select **Finalize**. (Unlike other reports, case and investigation documents do not move through a review and approval workflow.)
   - If you close the document before finalizing it, you can find and continue working on it from your My Tasks inbox or by opening the case or investigation profile.

In progress and finalized case and investigation documents appear at the bottom of the profile in the **Case/investigation documents** section.

Custom names

You can give custom names to the following report and documentation types to help you better organize and find items:

- Reports, including:
  - Standalone reports
- Case and investigation documentation
  - Cases
  - Summaries
  - Documents
  - Tasks

Custom names appear on incident, event, case, and investigation profiles, as well as shared documents, and printouts.

Custom report, document, and summary names

Custom names can be added to reports and case/investigation documents from the **Create report** window.

Custom names for case/investigation summaries can be added after the document has been created. When the document is open in Report Writer, select **More actions [...] > Edit custom name** from the top right corner of Report Writer. An Edit custom name window opens where you can enter a new name and select **Save**.

Once a custom name has been added to a report or document, it can be updated at any time from this window. To remove a custom name, delete all text in the **New custom name** field, and select **Save**.

Report and document custom names are formatted as: **Custom Name Report ID (Report Type)**. For example: **12/12 John Doe Interview 2024-FI-00000044 (Field Interview)**.

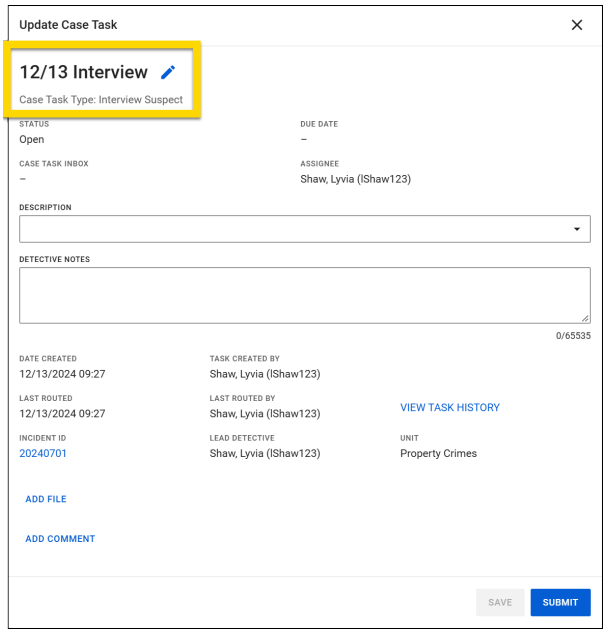
Custom task names

To add a custom name to a task, open the task and select the pencil icon beside the task name at the top of the screen. An Edit custom name window opens where you can enter a new name and select **Save**.

Once a custom name has been added to a task, it can be updated at any time from this window. To remove a custom name, delete all text in the **New custom name** field, and select **Save**.

When displayed in a list (e.g., on the **Tasks** tab or in printouts), custom names for tasks are formatted as: **Custom Name (Task Type)**. For example: **12/13 Interview (Suspect Interview)**.

When displayed in the task window, the task type appears below the custom name.



Custom case names

You can add a custom name to a case from various locations:

- Pencil icon on the case profile heading
- **More actions > Edit case name** on the case profile
- **More actions [...] > Edit case name** beside the case name in an inbox list

Once a custom name has been added to a case, it can be updated at any time from the Edit custom name window. When a case is given a friendly name, users can search for that name in Reports search, and the custom name will appear in search results.

When displayed in a list (e.g., in inboxes), custom names for cases are formatted as: **Case ID: Custom Name**. For example: **20240701: 12th Ave Burglary**.

Evidence and file management

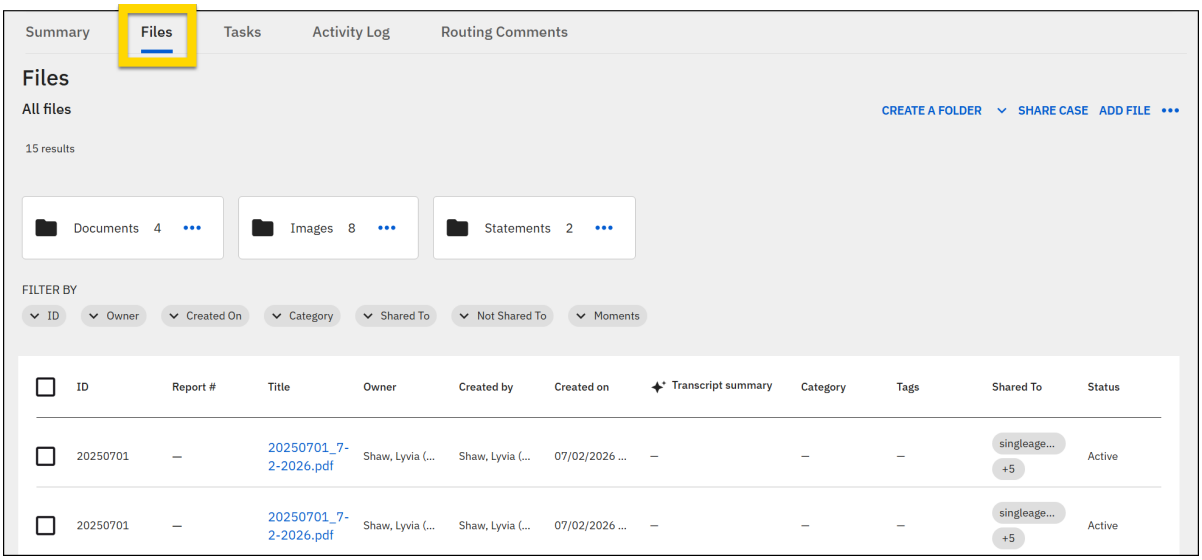
Evidence provides the supporting materials for a case or investigation. Evidence added to a report, case, or investigation in Axon Records or Axon Standards is also uploaded to Axon Evidence. As a result of this integration, users can:

- Attach digital evidence to cases and investigations
- Organize evidence into folders
- Review evidence media and metadata directly within Axon Standards

All files added directly to incidents, events, cases, and investigations or to reports associated with these items appear on the **Files** tab of their profiles. This tab displays all main folders that have been created, as well as a complete list of all files that appear in all folders. The most recently created files appear at the top of the list. The following information is included for each file:

- ID
- Report # (if the file was added to a report)
- Title
- Owner
- Created by
- Created on
- Transcript summary
- Category
- Tags

- Status



When viewing the **Files** tab, you can take the following actions:

- View file media, transcripts, and moments
- Edit metadata
- Create folders and subfolders
- Add and remove files

View files

When you select a file's title, an evidence preview pane opens and displays additional information about the file. Depending on the file type, this pane may include multiple tabs:

- **Overview:** This tab shows the same metadata that appears on the Overview tab of the Axon Evidence details page, as well as a transcript summary (if available).
  - See Evidence details page for more information.
- **Transcript:** This tab only appears for audio and video files and behaves the same as the Transcript tab on the Axon Evidence details page.
  - See Transcripts on the evidence details page for more information.
- **Moments:** This tab shows AI-detected key moments (e.g., Miranda Rights) within a piece of evidence with timestamps.
  - See Brief One Transcripts for more information.

> **Note**
>
> This tab only appears for customers who have purchased Brief One. Contact Axon Support or your Axon representative if you are interested in purchasing this product.

To view the full evidence details page in Axon Evidence, select **Details page** at the bottom of the pane.

Create folders

You can create folders and subfolders to better organize your evidence within a case or investigation.

Some organizations have configured a folder structure to be automatically created whenever an incident or case is created. This folder structure is based on the default case template that can be managed from the Case Settings page in Axon Evidence. For more information about managing the default case template, see Case settings.

When creating folders, you can create main folders, which appear when you first open the **Files** tab, and subfolders, which are contained either within the main folders or other subfolders.

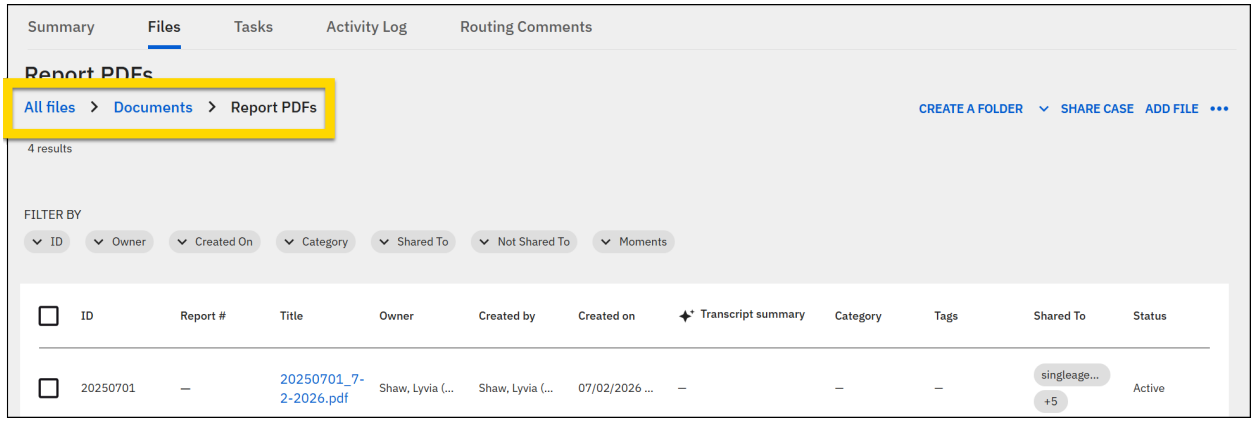
To create a main folder, take these steps:

1. Open the case profile and switch to the **Files** tab.
2. Select the **Create a folder** button in the top right corner of the tab.
3. Enter a meaningful name for the folder and select **Create**.

To create a subfolder within a main folder:

1. Open the case profile and switch to the **Files** tab.
2. Select a folder within the main folder.
3. Select **Create a folder**.
4. Enter a meaningful name for the folder and select **Create**.

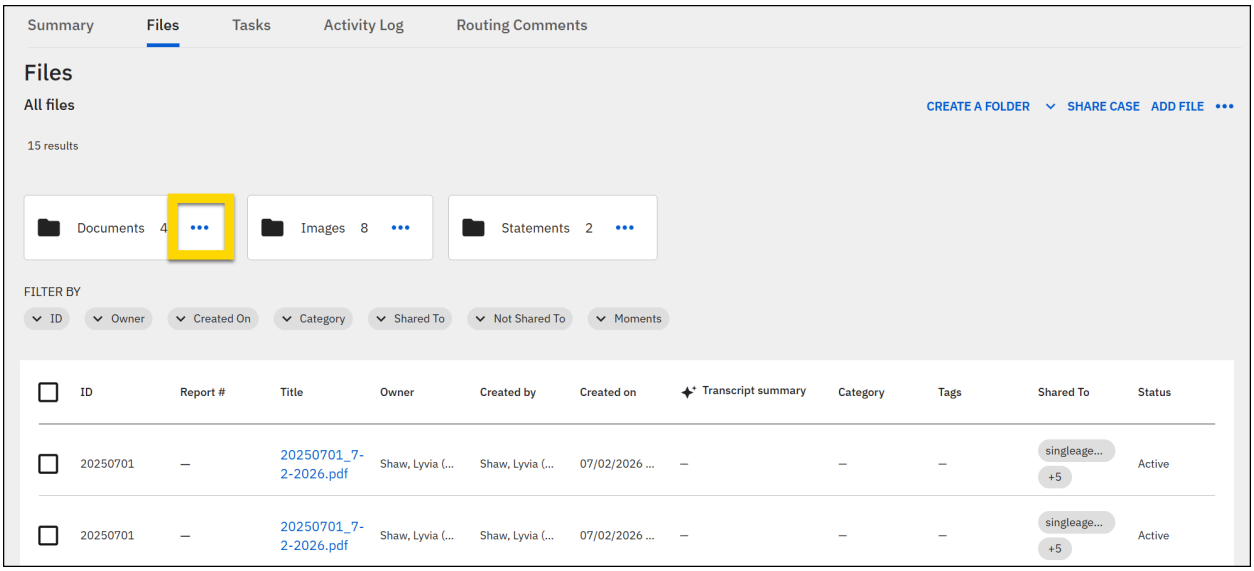
When viewing a folder, you can see where it appears within the folder structure by looking at the folder breadcrumb list that appears above the files contained within the folder. You can quickly navigate back to higher level folders by selecting the folder name.



Note

Two subfolders contained within the same folder cannot have the same name.

Once a folder has been created, select **More actions [...]** beside the folder name to either rename or delete the folder. When deleting a folder, you can choose to delete the folders and keep the files in the case or delete the folders and remove the files from the case. To delete the files entirely, open Axon Evidence.



Moving subfolders between folders currently is not supported. Instead, select **More actions [...] > Manage files on Axon Evidence** to move the folders from within Axon Evidence.

Add files

Files can be added to the main **All files** section, or to a specific folder. Additionally, files can be added to a single folder or multiple folders. If a file appears in multiple folders, it still only appears once in the **All files** list.

To add files:

1. Open the folder where you want the file to appear.
2. Select the **Add file** button in the top right corner of the tab.
3. Use the **Suggested**, **Upload**, and **Search** tabs (explained below) to find files that have already been added to Axon Evidence or to upload new files.
   - When reviewing the evidence on any of these tabs, select the evidence title to open the evidence preview window that displays additional information.
4. After choosing or uploading files, select **Add**.

Suggested tab

The **Suggested** tab contains recommendations for evidence you may want to add to the incident. Evidence is suggested based on the following criteria:

- Any Evidence ID that matches the ID of a case, incident, report, or the CFS ID
- Evidence you uploaded in the past 72 hours that hasn't been added to the report

Use the search fields to find specific evidence within the suggestion list and the checkboxes to add multiple files at the same time.

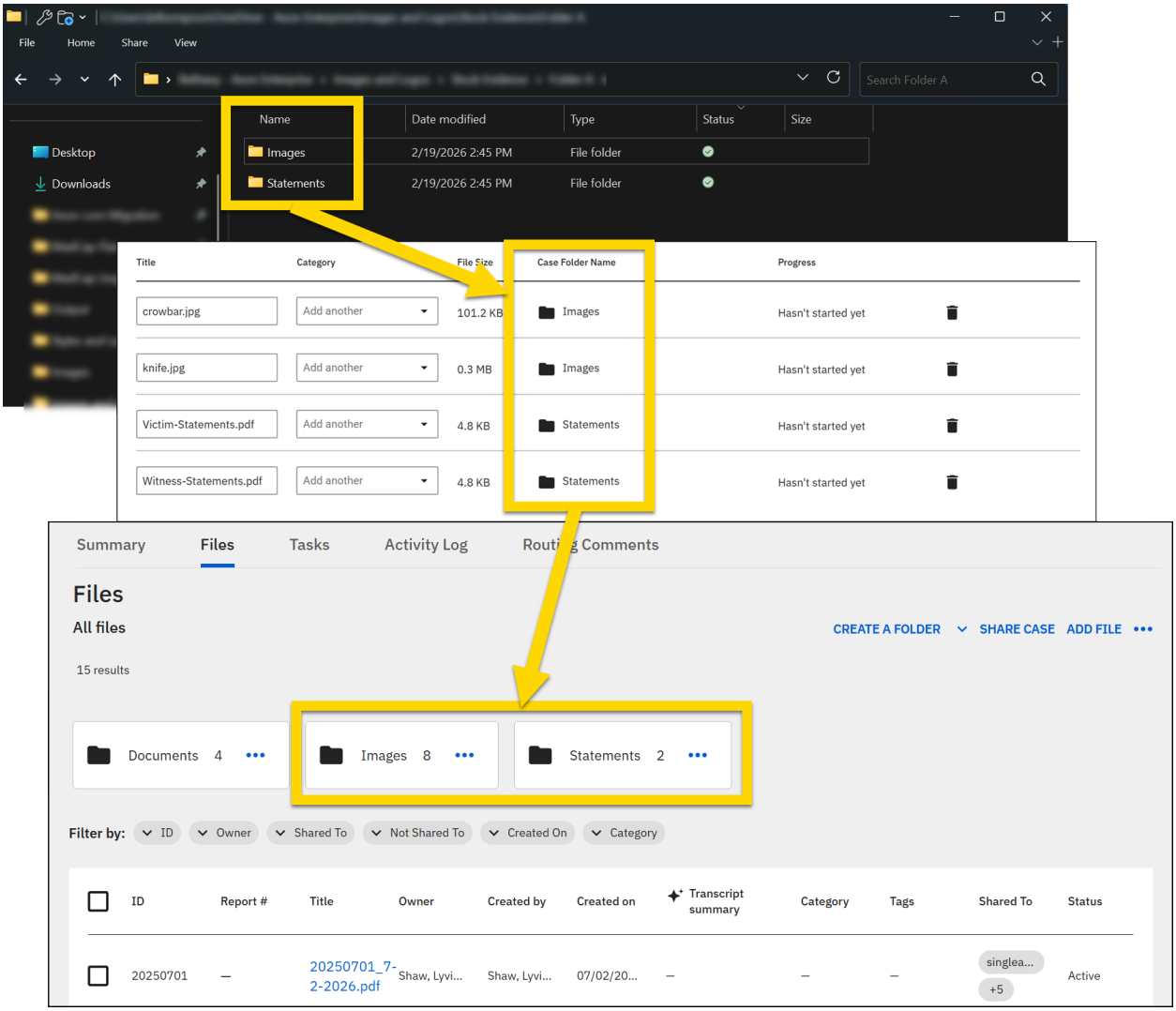
Upload tab

To add new files, switch to the **Upload** tab and either drag and drop files from your computer or select **Chose files**. Use the **Upload to folder** menu to set which folder the files should be added to, optionally add a description or update the file names, and select **Add**.

If you do not select a folder from the **Upload to folder** field, the files are added to the All Files list. You can also easily create a new folder when uploading files by typing the new folder name in the **Upload to folder** field that appears below the Drag and drop files area and selecting the **Create new** option that appears.

You can upload one or more files, or full folders. If the folder you upload contains subfolders, the subfolders will be uploaded along with the files they contain. After

selecting the files and folders from your local file system, the **Upload** tab displays the files that will be uploaded, as well as the folder the files will appear in.



Search tab

The **Search** tab lets you search for evidence that has already been uploaded to Axon Evidence. Use the search fields to find specific evidence and the checkboxes to add multiple files at the same time.

Edit metadata

Use the checkboxes to select one or more files then select the **Edit metadata** button in the top right corner of the tab to update (add or remove) the tag or category for the files. The categories and tags that appear in the dropdown menus are the same as those that appear in Axon Evidence.

Remove files

To remove a file, take these steps:

1. Open the folder that contains the files you want to remove.
2. Select the checkboxes beside the files you want to move.
3. Open the **More actions [...]** menu in the top right corner of the tab and choose one of the following options:
   - **Remove from folder:** Removes the file from the folder but not from the case. Once removed, the file appears in the All Files section that is displayed when you first open the Files tab.
   - **Remove from case:** Removes the file from both the folder and the case.

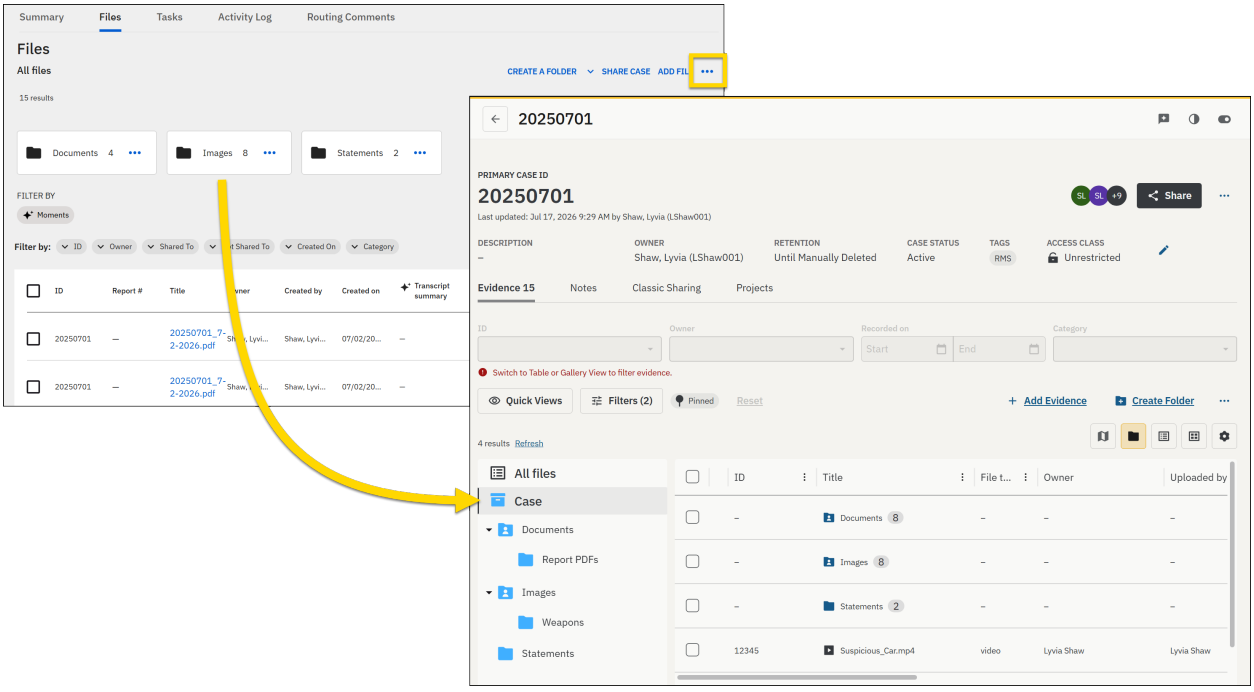
If a file was added to the case because it was originally part of a report associated with the case, the file is also removed from the report when it is removed from the case.

To delete a file, open Axon Evidence, find the file, and schedule it for deletion.

Sync with Axon Evidence

The files and folders that appear on the **Files** tab in Axon Standards also appear on the **Evidence** tab of the corresponding case in Axon Evidence. Any changes made to the files or folders in Axon Standards immediately display in Axon Evidence, and changes made in Axon Evidence immediately display in Axon Records or Axon Standards.

When viewing a case in Axon Standards, you can open the corresponding case in Axon Evidence, by selecting **More actions [...] > Manage files on Axon Evidence**.



Activity log management

The **Activity log** tab on event, case, and investigation profiles provides a chronological record of all actions taken on a case or investigation (e.g., report created, finalized, files added, etc.). It supports:

- Accountability and auditing
- Transparency into investigative progress
- Reconstruction of events for review or legal purposes

Activities can be generated either by the system or created by users. Users with the appropriate privileges can view this tab, as well as add or remove activities from it.

The most recently completed activities appear at the top of the list. The information recorded for each activity includes:

- Activity Type
- Description
- User (who performed the activity)
- Date Completed
- Time Spent

To manually add an activity to the log:

1. Select **Add activity** in the top right corner of the **Activity log** tab.
2. Select an Activity type. Options include: Comment, Contact, Note, and Task
   - Organizations can configure additional activity types by contacting their Axon representative.
3. Add a description.
4. Enter the date and time the activity was completed.
5. Enter the amount of time spent performing the activity.
6. Select **Add**.

Manual activities can be deleted by selecting the trash can icon. System-generated activities cannot be deleted.

Note

Adding and deleting manual activities is only available for users with specific privileges.

Disposition and review

Dispositions represent the outcome of a case or investigation. Depending on your organization's configuration, updates to a disposition may require a review. These review workflows introduce oversight before a case is formally closed. Disposition reviews ensure:

- Accurate reporting
- Policy compliance
- Alignment with legal or reporting standards (e.g., NIBRS)

Internal dispositions are used to track the status of cases and investigations. Contact Axon support or your Axon representative to configure the list of internal dispositions.

Organizations have several options when configuring what occurs when a user updates a case or investigation disposition:

- **No review:** When users update an internal disposition, the update is immediately applied without a supervisor review.
- **Supervisor review:** When users update an internal disposition, the case or investigation is routed to supervisor review before the update is applied or rejected.
  - Organizations can require reviews only when a case or investigation is updated to certain dispositions.

Based on which disposition update workflow is configured for your organization, administrators can assign various privileges that determine which users can:

- Update internal dispositions without a review
- Request disposition updates and route for supervisor review
- Review disposition updates

Update disposition (no review)

If your organization is configured to NOT require a review of disposition updates, follow these steps to update a disposition for a case or investigation:

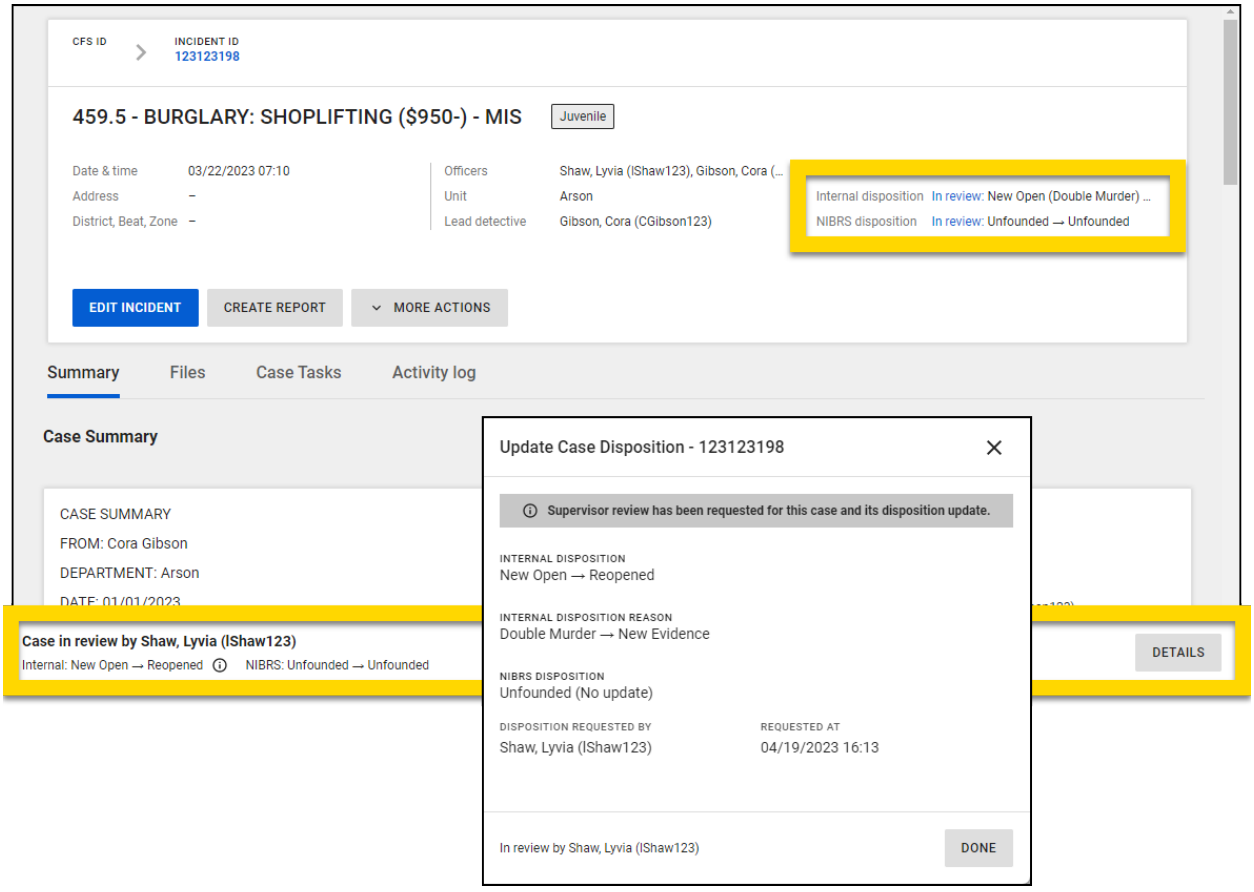
1. Open the case or investigation profile and select **More actions**.
2. Select **Update case disposition** (for case updates) or **Update disposition** (for investigation updates).
3. Select the new disposition.
   - When changing the internal disposition, optionally provide a reason.
   - From this screen, select **Reassign lead detective** to change the lead detective, add a routing note, change the due date, or mark the case as urgent.
4. Select **Set case disposition** (for case updates) or **Update** (for investigation updates).

Request disposition update (review required)

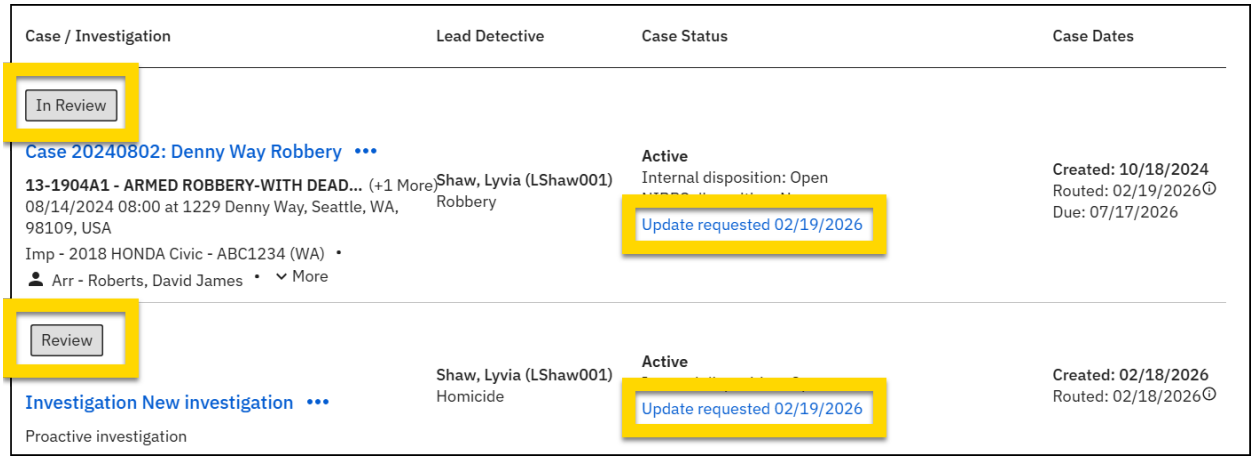
If your organization is configured to require a review of case disposition updates, you can request a disposition update and case review by taking the following steps:

1. Open the case or investigation profile and select **More actions**.
2. Select **Update case disposition** (for case updates) or **Update disposition** (for investigation updates).
3. Select the new disposition.
4. Select **Next**.
5. Optionally assign a reviewer or leave a comment.
6. Select **Request review**.
7. The case or investigation will be routed to the supervisor for their review.

After requesting a disposition update, the disposition displays as **In Review** at the top of the case profile, and a new footer appears, showing that the disposition update is in review. Select **Details** to view more information about the update request.



In your Case Management My Inbox, cases and investigations currently under review are labeled with a Review stamp. Select **Update requested {date}** to open the profile and view more information.



Assign review requests

Depending on the privileges you have, you can open a case or investigation profile and assign the review task to yourself or another reviewer by selecting the **Assign** or **Reassign** button at the bottom of the screen. Once assigned, the task appears in the assignee's **Assigned to me for review** tab in their Case Management My Inbox.

Supervisor case review

Some organizations are configured to require supervisor review of either all disposition updates or if a case or investigation is updated to specific dispositions. With this configuration, after a user updates a disposition, a disposition update request is created and can be found in several places:

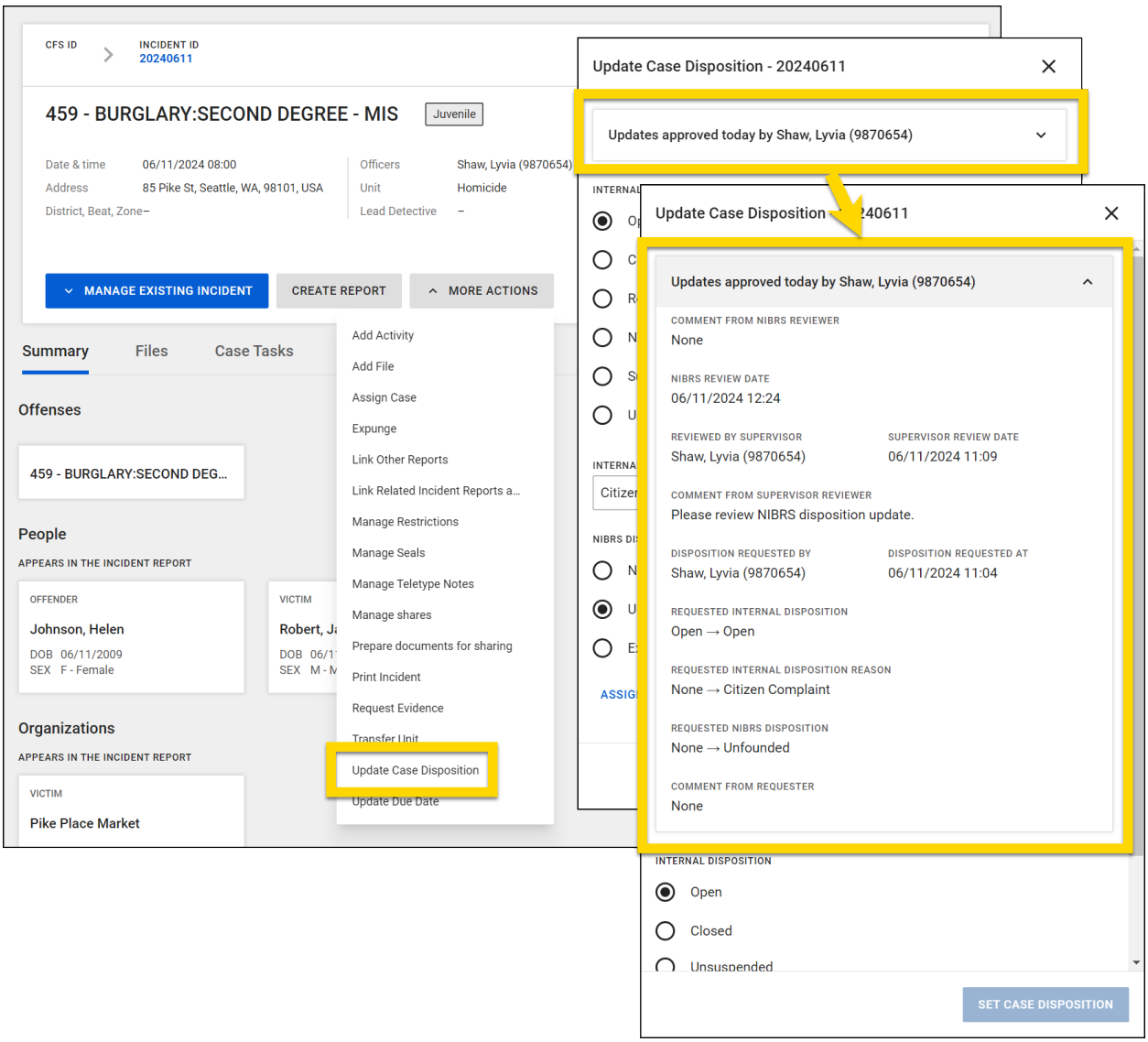
- If a review request has been assigned to you, it will appear in the **Assigned to me for review** tab in your Case Management My Inbox.
- Users who have been granted disposition review access can find all disposition review requests, including unassigned requests, by opening the unit inbox(es) they have access to and selecting the **Disposition in review** tab.

If you are assigned to review a disposition update:

1. Follow your organization's policies to review the case or investigation.
2. Once your review is complete, select either **Approve** or **Reject** at the bottom of the case profile page.
3. In the dialog box that appears, provide a comment as necessary, and select **Approve** or **Reject**.

View past disposition updates

You can view past disposition updates at any time by opening the case or investigation profile and selecting **More actions > Update disposition**. Any disposition updates that have been approved or rejected, appear at the top of the Update disposition pane. Select the arrow to expand this section and view the update details.



Share evidence and cases

Sharing allows organizations to distribute information to internal and external partners, such as prosecutors or other organizations. Users with specific privileges can manage a case or investigation's evidence files, as well as PDF snapshots of the incident or event reports, then share either all files or a subset of files with partners.

Note

For information about sharing a single report with other users at your organization, see Share report.

There are two case sharing methods that can be configured for organizations: Advanced sharing or Classic sharing.

Advanced sharing

Advanced sharing lets you share cases, investigations, incidents, and evidence files with internal and external partners directly within Axon Standards. You can continue to generate PDFs of reports and unlike with classic sharing, you do not need to open Axon Evidence to initiate or manage these shares.

Classic sharing

Classic sharing is the original method of sharing in Axon Evidence (as outlined in the Case share quick start guide). If your organization uses classic sharing, all shares are managed from Axon Evidence rather than Axon Standards. With this experience, you can generate PDFs of reports in Axon Standards, export them to Axon Evidence, and continue the sharing process from within Axon Evidence.

For additional information about the difference between these two sharing experiences, see How advanced sharing differs from classic case sharing.

Advanced sharing

With advanced sharing, you can share a full case, investigation, incident, a specific folder, or individual files. Before using advanced sharing, you must first request that it be enabled for your organization and complete the setup steps as explained in Advanced sharing overview and setup.

Once advanced sharing is enabled, you can interact with its features directly within Axon Standards. The Shared To column on the **Files** tab on cases, investigations, and incident profiles displays which external partners each item has been shared with. Hover over the partner name to see the date and time the item was shared. If an item has not been included in any shares with external partners, a hyphen "-" is displayed in the **Shared to** column instead.

Use the **Shared to** and **Not shared to** filters to only display items shared or not shared with a partner agency. You can combine these filters with the other filters on the **Files** tab to refine which items are displayed.

Create shares

When using advanced sharing, you can set the scope of the share, depending on how much information you want to share with internal or external partners. Share options include:

- All files
- Individual folders
- Specific evidence items

For additional information about advanced sharing in Axon Evidence, see Advanced sharing overview and setup.

Share all files

You can share all files in an entire case, investigation, or incident from two locations on the case, investigation, or incident profile:

- **Files** tab: Select the **Share case** button (located between **Create folder** and **Add file**).
- **More actions** menu: Select the **Share case** option.

When sharing all files, the share includes all files CURRENTLY in the case, investigation, or incident. If new files are added to the case, investigation, or incident, those new files automatically are added to any pre-existing shares; you do not need to create new shares and manually add the files to them.

A share only includes incident, event, or investigation report PDFs if they have already been exported and uploaded to the case. To share report PDFs, use the **More Actions > Prepare documents for sharing** to generate and add report PDFs to the case, investigation, or incident. See Share report PDFs (Preparing documents for sharing) for more information.

Share folders

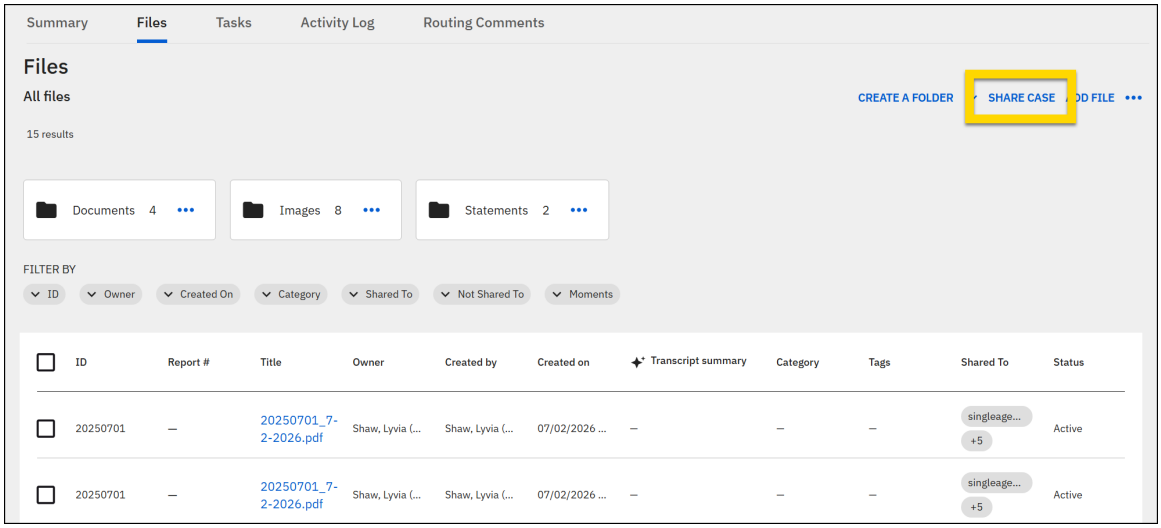
To share a single folder, open the **More actions [...]** menu on that folder and select **Share folder**. Only evidence within selected folder is shared; evidence added to unselected folders is not included unless you update the share.

Share specific evidence items

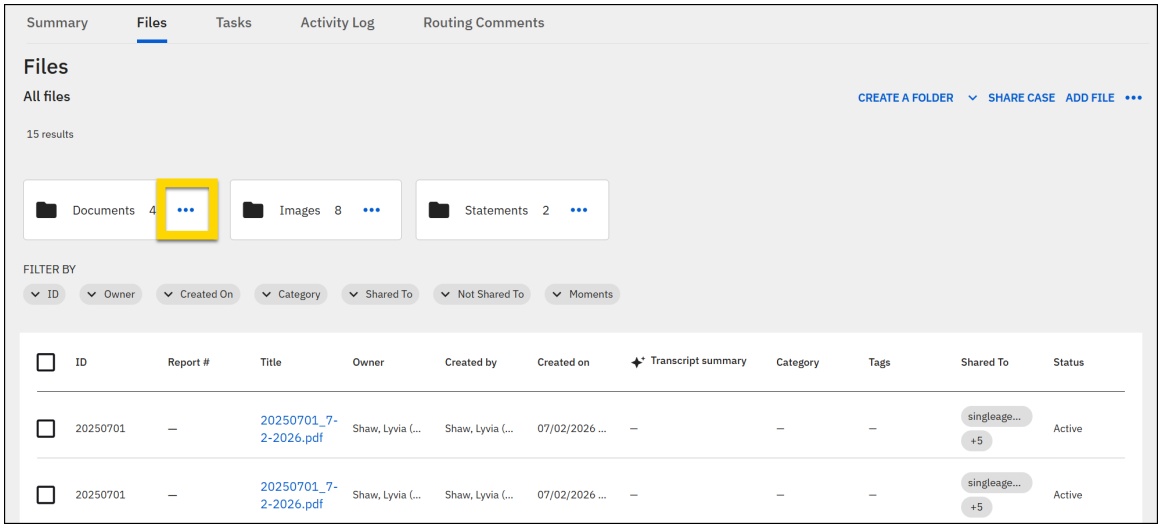
To share specific evidence items, select the checkboxes beside the Evidence ID, then select the **Share** button at the top of the **Files** tab.

To create a new share:

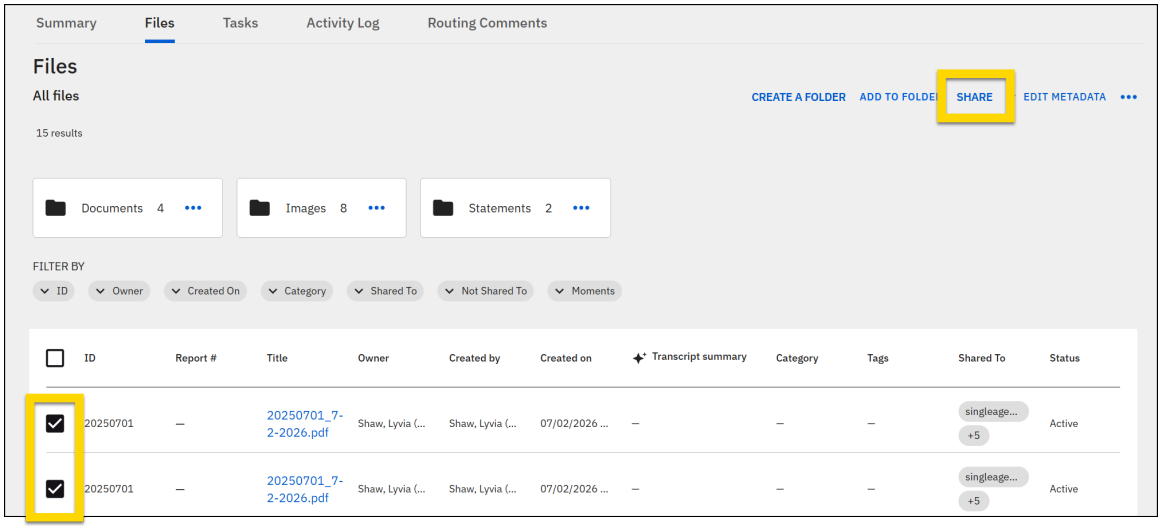
1. Open the case, investigation, or incident profile.
2. Go to the **Files** tab and initiate the share:
   - To share all files, select **Share case > Share case** at the top of the **Files** tab.



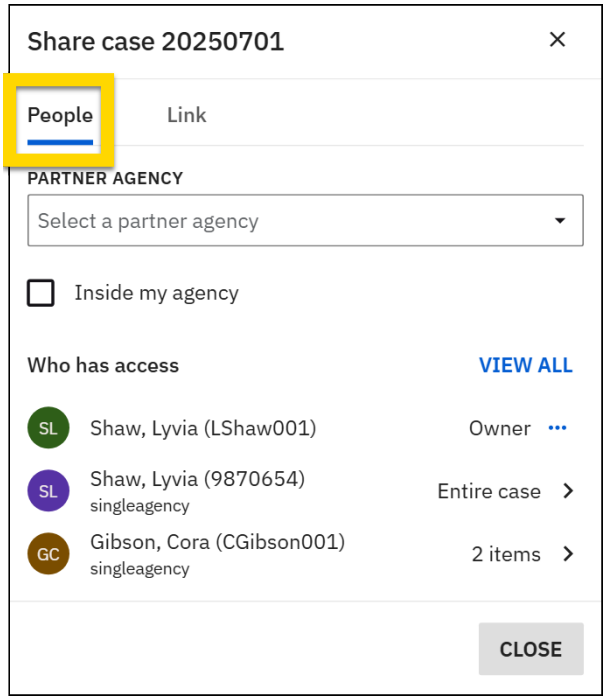
   - To share a folder, open the **More actions [...]** menu on the folder and select **Share folder**.



- To share evidence items, select the checkboxes beside the Evidence ID and select the **Share** button at the top of the **Files** tab.



3. On the **People** tab of the Share window that opens, you can choose whether to share with a user at your agency or at a partner agency:
   - **Inside my agency:** Grants access to a colleague at your own agency. Useful when someone outside the assigned unit needs to view or work on the case.
   - **Partner agency:** Grants access to a specific user at an external partner (e.g., a named ADA at the DA's office) beyond what a standard case share covers.



4. To share with someone at a partner agency:
   - Select or type a partner name into **Partner agency** field (e.g., your DA's office).
   - Select one or more recipients in the **User or group** field (users or groups at the partner agency).
     - If a default recipient has been configured for that agency, their name appears in the User or Group field. Select **Edit** to remove that user or add additional users and groups.
     - See Default sharing recipients for more information.
   - Select **View** in the Access section to review the sharing policy.
     - This is the agreement that governs how the item is shared. Only one active policy per agency-partner pair is supported.
     - See Advanced Sharing overview and setup - Sharing policy settings for more information.
5. To share with someone at your agency select the **Inside my agency** checkbox and search for the user or group.
   - Select the access level:
     - Role based: The actions a user can take with the evidence depend on the permissions associated with their assigned role in Axon Evidence.
     - View Only: The user can only view the evidence associated to the case and not take action on it.
     - See Modifying inside my agency access list for more information.
   - Enter a duration.
     - 3, 30, or 90 days
     - 1 year
     - Until removed
6. After adjusting all sharing settings, select **Share.**

> **Note**
>
> The **Share** button stays disabled until you've selected a valid sharing policy (if sharing with partner agencies) and at least one recipient.

7. Select **Share** in the confirmation message that appears to confirm the share.
8. A success message displays at the top of the screen, indicating the share was successful.
   - Most shares complete quickly but it may take a day before large shares or archived evidence is available to the partner agency. Recipients receive an email when the evidence is available.

- The Share window shows a **Processing** label beside any shares that have not yet completed. This label will disappear once the share is completed.

When the share is complete, a Shared label appears in the top right corner of the case, investigation, or incident profile. This label is removed if all shares are revoked or expired.

Manage existing shares

1. Open the case, investigation, or incident profile.
2. Go to the **Files** tab.
3. Select **Share case > Share case**.
4. The **People** tab of the Share window that opens and shows the access list (**Who has access** section).
   - The most recent shares appear at the top of the list.
   - Select **View all** to see the full list.
5. Select a specific share entry to expand its details:
   - For each share, you can see:
     - Partner name and recipients
     - Share status and shared date
     - Expiration date (if applicable)
   - For partial shares (folder or individual evidence items, you can also see the full evidence list including file names, last shared date, and file sizes.
6. Select the pencil icon beside the recipient name to modify recipients of partner agency shares.
   - Add new recipients by searching and selecting from the dropdown and selecting **Add**.
   - Remove recipients by selecting the trash can icon.
   - The recipients update immediately and a **Processing** status label appears briefly while the change is applied.

   Note

   You cannot change the sharing policy on an existing share. To use a different policy, stop the current share and create a new one.
7. For internal shares, you can modify the level and duration of the share.
8. To stop a share (either partner share or internal share), select **Stop sharing** and confirm your action when prompted.
   - The share is immediately revoked, and the partner loses access to the share.
   - The status of the share updates to Revoked to indicate that the share has stopped.

9. All update and stop share actions are logged in both the Axon Evidence case and user audit trails.
    - When an internal share is updated, the audit log shows the acting user (the user who updated or revoked the share), the affected user (the user the share was made to), the access level, and a timestamp.

Add files to existing shares

When you have shared a subset of items (either a folder or specific evidence items), you can add additional items to the share:

1. Open the case, investigation, or incident profile.
2. Go to the **Files** tab.
3. Select the checkboxes next to the evidence items you want to add to your share.
4. Select the **Share** button at the top of the **Files** tab.
5. On the **People** tab of the Share window that opens, select the existing share you want to add the items to.
6. The selected items are added to that share immediately.
7. After the share is processed successfully, the recipient details window shows which evidence files have been shared with that recipient.

If you have a case, investigation, or incident that has active shares of specific evidence items, a message appears when you add a file or export a PDF using the Prepare documents for sharing flow. This message asks if you want to add the new files to your existing shares.

This message only appears if:

- You use the Prepare documents for sharing workflow.
- You use the **Add file** button on the **Files** tab of the case, investigation, or incident profile.

When this message appears, you have two options:

- **Not Now:** Close the message. The new file is not added to any existing shares. You can add it manually later as necessary.
- **Continue Share:** Add the file to your active shares.

This message only appears for cases, investigations, or incidents that have existing shares of specific evidence items. It does not appear for all-file shares or folder shares; new evidence added to a shared case, investigation, incident, or folder is included in the share automatically.

If you add files outside of the Prepare documents for sharing or **Add file** button, the message will NOT appear. In these cases, you must update the existing shares manually by selecting **Share case > Share case** on the **Files** tab.

Share report PDFs (Preparing documents for sharing)

With advanced sharing, you can prepare your documents, export a PDF package, and share it from within Axon Standards—without switching to Axon Evidence:

1. Open the case, investigation, or incident profile.
2. Open the **More actions** menu and select:
   - Incidents and cases: Prepare documents for sharing
   - Investigations: Prepare investigation for sharing
3. Update the name of the file. This is the name that appears in Axon Evidence.
4. In the **Documents** section, indicate which content to include:
   - For events, you can include:
     - Event reports: Indicate which reports to include.
     - File list: If selected, a list of all file names that have been added to the case are included in the printout.
     - Activity log: Includes all actions taken on the event.
   - In addition to the items listed above, for cases or investigations, you can include:
     - Case or investigation summary
     - Case or investigation documents
     - Tasks
       - Indicate if the printout should include a list of case tasks, or details for each task.
       - Optionally include incomplete tasks.
       - Set the order in which the tasks should be listed in the printout. Sort options include Task, Assignee, Status, Created at, Due date, and Completed at.
   - Some organizations are configured to only allow finalized documents to be shared. If your organization is set up this way, documents that are not finalizedare grayed out and cannot be selected.
5. In the **Settings** section, optionally include the following items:
   - Show table of contents: Includes a list of all sections in the printout with a header that gives basic details about the case.
   - Show images in narratives: Includes images that have been inserted inline into the narratives.
   - Show restricted information: If restrictions have been applied, this option includes restricted information that you have privileges to view. Optionally include this restricted information on a separate page.
   - Show approval log: Details of the report approval process.
   - Start each narrative on a new page: Inserts a page break at the start of each narrative.

6. Select **Next**.
7. Use the **Sort reports and documents by** and the **Order** fields to set the order in which items appear.
   - Sort options include:
     - Document Type
     - Name (if custom names have been created for any of the items)
     - Date and time created
8. Select **Next**.
9. If you need to redact anything before printing, select **Yes** then **Start redaction**. If you are not redacting anything, select **Export PDF and continue share**.
   - See Redaction for more information.
10. The PDF will export (taking longer depending on the amount of information included). Select **Continue share** in the Export window.
    - When exporting is complete, the PDF saves to your cases in Axon Evidence,
11. The **People** tab of the Share window that opens displays all shares that contain specific evidence items.
    - The share list does NOT display current shares of all files. When the PDF is created, it is automatically shared with any recipients the case, investigation, or incident has been shared with.
    - The share list also does NOT display current shares of folders. To include the PDF in a share of a specific folder, move the PDF into that folder. It will be automatically shared with all recipients who the folder has been shared with.
12. Select an existing share to add the PDF to or create a new one by entering an agency in the **Partner Agency** field.
    - When you create a share during this workflow, you only share the PDF with the recipients. If you want to share additional files, follow the steps in Create shares.

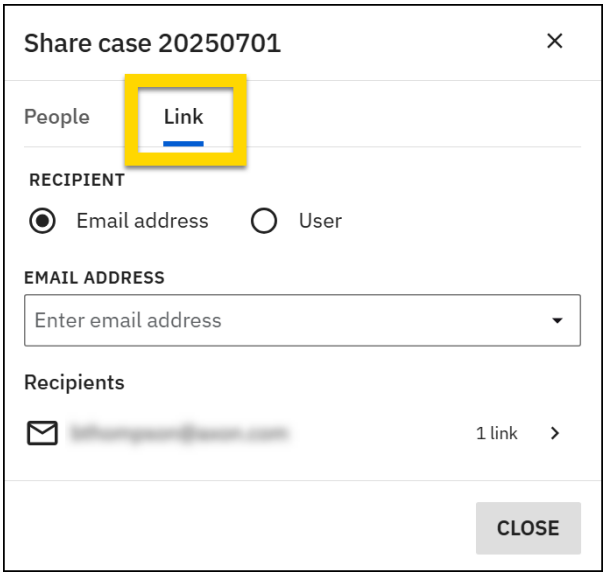
When you prepare documents for sharing from Axon Standards, the PDF appears in the Axon Evidence case on the **Evidence** tab in an auto-generated **Documents** folder.

If you update the report after sharing it, you should repeat the steps above to generate a new PDF that includes the updated information. Be sure to update the file name to distinguish it from the originally shared file.

Share download links

With Advanced Case Sharing, you can generate a secure, time-limited link to a case and send it to any email address, including users who do not have an Axon account. This feature mirrors the link sharing experience in Axon Evidence Advanced Sharing.

1. Open the case, investigation, or incident profile.
2. Go to the **Files** tab and initiate the share:
   - To share a link for the entire case, select **Share case > Share case** at the top of the **Files** tab.
   - To share a link for a folder, open the **More actions [...]** menu on the folder and select **Share folder**.
   - To share a link for evidence items, select the checkboxes beside the Evidence ID and select the **Share** button at the top of the **Files** tab.
3. In the Share window, switch to the **Link** tab.



4. Select the recipient type:
   - **Email address:** Sends the link to the email address(es) provided.
   - **User:** Sends the link to a user either at your agency or a partner agency.
     - To share with someone at your agency, select the **Inside my agency** checkbox and search for the user or group.
5. After you enter a recipient (either email or user), additional share settings appear:
   - Audit trails
   - Transcripts
   - Table of Contents
   - Retain folder structure: This option only appears when you are sharing a link to the entire case. If you share a case that contains subfolders, checking this box will retain that subfolder structure. If you do not check this box, all files will be shared in a single folder.
6. Select the type of package: ZIP or ISO.
7. Set a duration for how long the download link is valid. Once this time passes, the case can no longer be downloaded, and a new download link must be sent.

8. Enter an optional message to accompany the download link. This message appears in the email that contains the download link.
9. After adjusting all link settings, select **Share.**
10. The recipients you provided will receive an email with the download link.
11. The link and all send actions are logged in the Axon Evidence case audit trail.

Recipients of a download link do not need an Axon account to access the shared content. The link is self-contained, and access is controlled entirely by the expiration date and access level you set.

Download link sharing follows the same permission model as Axon Evidence. If a user does not have link sharing permissions in Axon Evidence, the **Link** tab will not be available to them in Axon Standards.

Manage existing download links

To update an existing link share:

1. Open the case, investigation, or incident profile.
2. Go to the **Files** tab.
3. Select **Share case > Share case**.
4. In the Share window, switch to the **Link** tab.
5. Select share to view its status, expiration date, and who it was sent to
6. To disable a link before it expires, select **Cancel.**
   - Revoked links stop working immediately. Recipients who click the link after revocation will see an access denied message.

Classic sharing

If your organization still has active classic shares (from the legacy Manage External Sharing system), you can continue to access them from two locations on the case, investigation, or incident profile:

- **Files** tab: Select the **Share case > Manage classic shares**.
- **More actions** menu: Select the **Manage classic shares** option.

After selecting one of the options, the Axon Evidence case opens in a new tab where you can manage shares as usual.

You can generate and share report PDFs using the classic share workflow. Follow the steps listed in Share report PDFs (Prepare documents for sharing) section. After selecting which documents to include in the export, a new tab opens to Axon Evidence where you can complete the share.

For more information about classic sharing in Axon Evidence, see:

- Case share quick start guide
- Cases share overview

Analytics

The Axon Analytics dashboards let you take a closer look at the data being generated by your organization.

To access the Analytics dashboards, select the chart icon in the main navigation menu. You can interact with the various visuals in the dashboards, export them in various formats, and set up email subscriptions.

Users with specific privileges can create, edit, and delete these dashboards.

Administrator Note

This topic includes end-user information. To see administrator content for this feature, see Analytics administration.

Out of the box dashboards

When your organization begins using the Analytics module, you can access a set of Out of the box (OOTB) dashboards. Contact your Axon representative or Axon Support if you want to adjust these dashboards.

A file containing example downloads of all OOTB dashboards can be found here.

The following dashboards are available in Axon Standards:

- Complaints (Internal/Citizen)
- EIS
- Report Productivity
- Use of Force/Response to Resistance
- Vehicle Collision
- Vehicle Pursuit

Complaints (Internal/Citizen)

The Complaints dashboard provides insights into internal and citizen complaint activity, offering overviews by case, officer, reviewer, and complainant demographics to support transparency, accountability, and trend analysis. This dashboard contains the following tabs:

- **Complaints overview:** High-level snapshot of complaint volume with counts for complaints and unique officers involved, a time series by month/year, map of complaint locations, and bar charts by allegation/resolution and actions taken; includes an incident table with event/date, location, report type, involved officers, complainants, and allegations.
- **Complaints review:** Review workflow view showing counts for complaints, unique officers, and unique complainants; visuals break complaints down by reviewer, reviewer-by-resolution, and involved officers by report type; detail table lists event/date, involved officer, allegation, resolution, action taken, reviewer, and complaint type.
- **Officer complaint details:** Officer-centric page with counts for complaints, unique officers, and unique complainants; chart of involved officers' allegations by resolution; detail table per event showing involved officer, allegation, resolution, action taken, hours suspended, and complaint type.
- **Citizen demographics:** Complainant-focused view with counts for complaints, unique officers, and unique citizen complainants; charts for complainants by sex, race/ethnicity, and age bracket, plus allegations by resolution; "Citizen Details" table lists event/date and complainant demographics.

Early Intervention System (EIS)

The Early Intervention System dashboard can be accessed from the EIS module. This dashboard shows counts of EIS alerts (In Policy, Warning, Critical) for individuals over different lookback periods.

See Early Intervention (EI) dashboard for more information about using this dashboard to manage EIS alerts.

Report Productivity

The Productivity dashboard tracks report creation, review, and completion performance, highlighting timeliness, reviewer activity, and quality control across report workflows to support efficiency and accountability. This dashboard contains the following tabs:

- **Report productivity — Overview:** High-level snapshot of report volume and timeliness: counts by status (Draft, Supervisor Review, IA Review, Finalized), average days to finalize, trends by month/year, and a table listing reports with author, type, and workflow status.
- **Reports in progress:** Focuses on unfinalized work: current counts in each stage, trends over time, breakdowns by report type and primary assignee with average days in stage, plus a detailed "in progress" list (reviewer assigned, sent-to-review date, days in status).

- **Report productivity — Finalized reports:** Completion view: who approved what and when (Supervisor and IA Review panels), with a table of finalized reports showing created vs. finalized dates and days to finalize; filterable by reviewer, author, type, and date ranges.
- **Report productivity — Rejected reports:** Quality/control view: rejected count and rate, breakdowns by officer and supervising reviewer, and a detailed rejected-report list (report number, author, type, rejection instances), filterable by author, unit, supervisor, type, and dates.

Use of Force / Response to Resistance

The Use of Force/Response to Resistance dashboard provides a comprehensive analysis of force-related incidents, tracking usage patterns, subject and officer demographics, injuries, and trends to support transparency and informed oversight. This dashboard contains the following tabs:

- **Force overview:** Overview of total force incidents and applications, with visual analysis of force types, incidents, and related details.
- **Force trends:** Trends in force incidents and applications over time, with analysis by day, time, and dynamic filtering options.
- **Force subject demographics and actions:** Demographics of subjects involved in force incidents, including race, age, sex, homelessness, impairment, resistance, and actions.
- **Officer demographics:** Details on officers involved in force incidents, including race, rank, years of service, sex, and incident counts.
- **Force subject and officer injuries:** Summary and analysis of injuries to subjects and officers by severity, treatment, injury type, and force applied areas.

Vehicle Collision

The Vehicle Collision dashboard provides detailed insights into vehicle collision incidents, highlighting trends, participant demographics, officer involvement, and environmental factors to support analysis of safety, performance, and incident response. This dashboard contains the following tabs:

- **Vehicle collision overview:** High-level incident summary with KPIs for total incidents and damage, time series by month/year, a map of incident locations, and breakdowns by location, lighting, and weather. Useful for spotting trends and geographic clusters.
- **Vehicle collision — Persons involved:** Demographic and injury/safety-belt breakdown of people involved (sex, race/ethnicity, injured, seatbelt use, vehicle crash involvement) with a detailed table of each person per event. Useful for victim/participant analysis and safety insights.

- **Vehicle collision — Officers involved:** Officer-level view showing which units and officers responded or are assigned, counts of incidents and involved officers/persons, and incident details (weather, lighting, damage). Useful for workload, unit performance, and assignment reviews.

Vehicle Pursuits

The Vehicle Pursuit dashboard provides comprehensive analysis of vehicle pursuit incidents, including key metrics, suspect data, and temporal trends to support operational insight and accountability.

This dashboard contains high-level stats for Vehicle Pursuits, People Injured, Avg Highest Speed, Avg Length (mins). Includes a map of starting locations, reports by month/year, bar charts for incidents by reason started and reason ended, plus a detailed incident table. the dashboard also shows counts of Vehicle Pursuits, Suspects. Includes details for suspects by charge type, injured/not, injury type, sex, race; detailed suspect table (event/date, name/DOB, demographics, role, charges, injury status/type). Finally, the dashboard includes tables depicting Vehicle Pursuit reports by year/quarter/month, by day of week, and by hour of day.

General functionality

You can interact with Analytics dashboards in various ways, including:

- Actions
- Tabs
- Filters
- Tooltips
- Focus Mode
- Right-click
- Maps

Watch this video for an explanation of the content contained in the following sections.

Actions

Each dashboard contains an Actions menu you can open to:

- Create new dashboard:Create a new copy of the dashboard to edit and customize as desired.
- Edit dashboard: Edit the title, tabs, and visualizations for the dashboard.

- Create bookmark: Save a link to the page, including whatever filters you have set in your current session.
- Create bookmark: Copy a link to the dashboard page that you can share with other users or bookmark for easy reference.
- Export dashboard: Export the dashboard as a PDF, CSV, or PPTX (Power Point) file.
- Manage subscriptions: Set up email subscriptions to receive daily, weekly, or monthly email snapshots of the dashboard.

Tabs

Each dashboard opens to an **Overview** tab. Select the names that appear to the right of the **Overview** tab to switch to tabs that contain different charts and data.

Filters

Use two different types of filters to adjust the data displayed in the dashboards:

- Choose from the drop-down filters at the top of the window
- Select a piece of data or chart section

Drop-down filters

Each dashboard has a different set of filters to choose from that allow you to refine the data that is displayed.

Hover over a filter and select the eraser icon to remove that filter. Select **Reset filters** to remove all filters.

Chart filters

All visuals on a dashboard are connected. This means that if you select a piece of data or colored section of a chart, all data on the dashboard is filtered by that criteria.

For example, selecting one of the districts on the **Use of Force Overview** tab filters all charts to show data for just that district. The area that you selected will remain a dark color and all other districts will appear washed-out.

To remove the filter, select the data or chart section again or select **Reset filters** at the top of the window.

See Power BI's help documentation for additional details about filtering.

Tooltips

When you hover over a section of a chart a tooltip appears that contains additional data.

Focus Mode

Click on any chart to enter Power BI's Focus Mode and reveal additional options above the chart. Use these options to:

- Drill up or down
- View the filters that impact the visualization
- Spotlight the visualization
- Open Focus Mode, which reveals a larger version of the visualization
- Export the data for just that visualization
- Adjust the sorting axis or sort order

See Power BI's help documentation for additional information about Focus Mode.

Right-click

Right-click on any chart to reveal additional drill-down options, including:

- Show as table
- Include / Exclude
- Copy

See Power BI's help documentation for additional information about drill-downs.

Show as table

Select this option to reveal a larger version of the visualization, as well as a table version of all data. The Focus Mode options appear above the visualization. Select **Back to report** to return to the full dashboard.

Include / exclude

To include or exclude a piece of data from the displayed results, right-click on the piece of data / chart section and select **Include** or **Exclude**.

Copy

Right-click data in a table to reveal two copy options:

- **Copy value:** Copies the value of that cell. If the cell contains a percent, it will be converted to the decimal value.

- **Copy selection:** Copies the entire row. Unlike **Copy value**, percentages are not converted into decimals

After copying a value or selection, you can paste the data into another program or document by pressing **CTRL/CMD + V** on your keyboard.

Maps

Several dashboards contain maps. Click and drag on a map to adjust which section of the map is shown on the screen. Hover over the map and use the scroll wheel on your mouse to zoom in and out.

In the same way that selecting a chart or data section adjusts the information shown in all charts and graphs on the dashboard, selecting an area on a map adjusts all chart information. To do this, select the rectangle + cursor icon  in the top right corner of the map. The mouse pointer changes to a cross that you can use to draw a square on the map.

Export dashboards

To export an Analytics dashboard:

1. Open the dashboard.
2. Use the filters to set which data to include in the export.
3. Select **Actions > Export dashboard**.
4. Select a format for the export:
   - **CSV:** A separate CSV file is exported for each table/matrix in the dashboard.
   - **PDF:** Each dashboard tab exports to a separate page in the PDF.
   - **PPTX:** Each dashboard tab exports to a separate slide in the Power Point file.
5. Use the checkboxes to select which tabs or tables/matrices to include in the export.
6. Select **Export dashboard**.

Manage subscriptions

To create a new email subscription for an Analytics dashboard:

1. Open the dashboard.
2. Use the filters to set which data to include in the export.
3. Select **Actions > Manage subscriptions**.

4. Select **Add new subscription**.
5. Enter the email subject.
6. Choose if you want to receive a link only to the dashboard or an export of the dashboard.
   - To receive an export of the dashboard, select an export format: PDF or PPT
     - **PDF:** Each dashboard tab exports to a separate page in the PDF.
     - **PPTX:** Each dashboard tab exports to a separate slide in the Power Point file.
7. Set the email schedule:
   - Select a frequency:
     - Daily: Set which time each day the email is sent
     - Weekly: Set which day of the week and which time on that day the email is sent.
     - Monthly: Set if the email sends monthly, every two months, etc., the day of each month, and the time of day the email is sent.
   - Set a start and end date.
8. Select **Subscribe**.

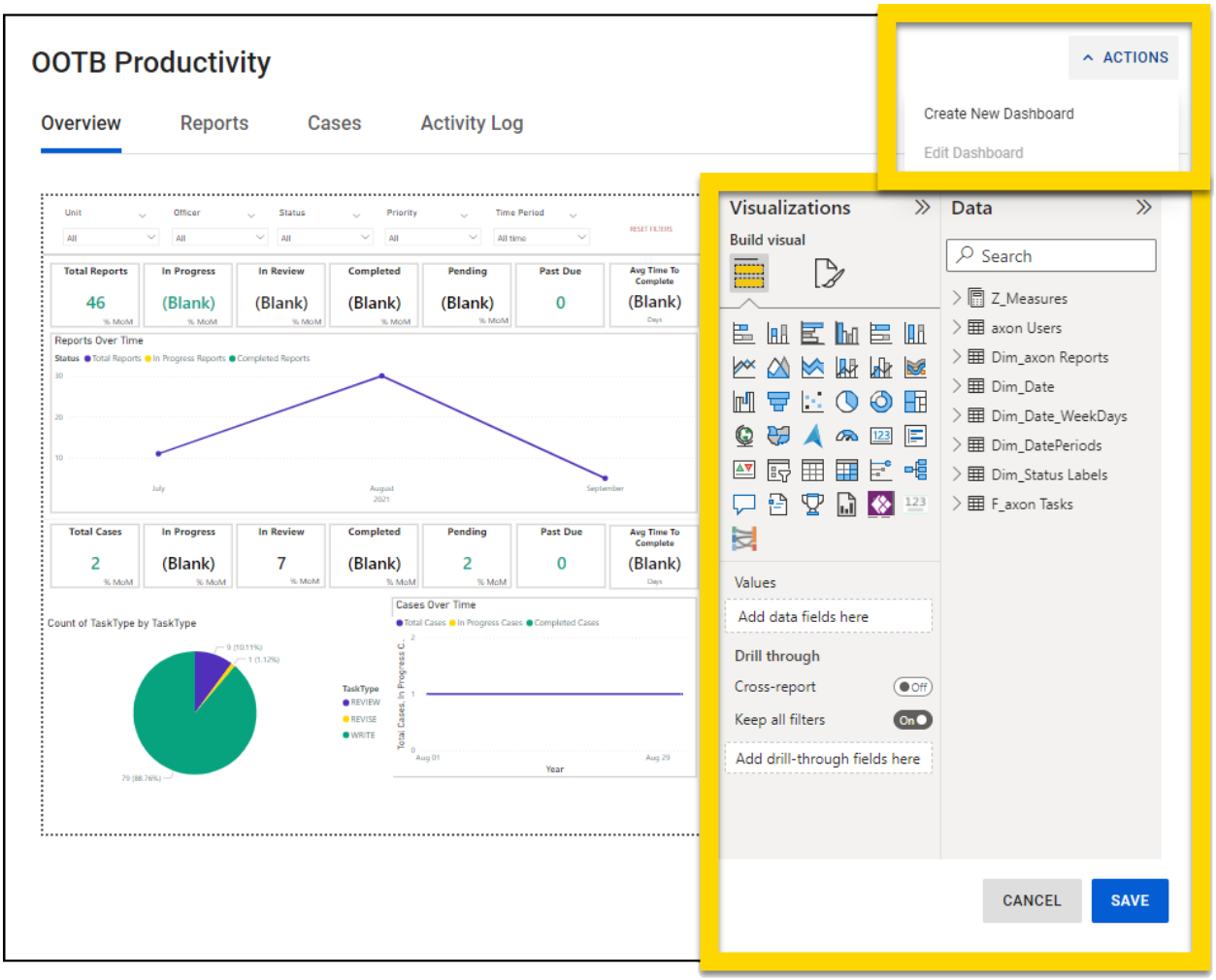
After creating an email subscription, you can return at any point to edit or delete it:

1. Open the dashboard.
2. Use the filters to set which data to include in the export.
3. Select **Actions > Manage subscriptions**.
4. Find the subscription in the list and **select** Edit to adjust any of the subscription settings or **Delete** to delete it.

Dashboard management

Users with specific privileges can edit, save, and delete/archive the dashboards that appear in Axon Records and Axon Standards. You can also view an activity log of all actions taken on that dashboard.

Although you access the dashboards within Axon Records or Axon Standards, you use embedded Power BI capabilities to edit them.



Administrator Note

This topic includes end-user information. To see administrator content for this feature, see Analytics administration.

Create dashboards

To create a new dashboard from the Analytics module, take these steps:

1. Open the Analytics module by selecting the chart icon in the main navigation menu.
2. While viewing any of the existing dashboards, select **Actions > Create new dashboard** in the top right corner.

3. Select a template to serve as the basis of your new dashboard, give it a name, and select **Create dashboard**.
4. The new dashboard will not immediately appear in the list of available dashboards on the left side of the page because you need to grant yourself the privilege to view it. To do this, open the Administrator Console and select **Command Hierarchy & Teams.**
5. Select either the **Command Hierarchy** or **Teams** tab.
6. Select the Command Hierarchy group or team you want to view the new dashboard.
7. Switch to the **Privilege sets view** tab.
8. Expand the **Analytics - view** privilege section and select **Allow** on the new dashboard.
9. When you next open the Analytics module, the new dashboard will appear in the list.

Edit dashboards

Users with the appropriate privileges can edit dashboards in one of two ways:

- Edit titles and tabs
- Edit visualizations

See Quick tips for other ways to edit dashboards and visualizations.

Edit titles and tabs

To edit the dashboard title or tabs, take these steps:

1. Open the Analytics module by selecting the chart icon in the main navigation menu.
2. Select **Actions > Edit dashboard** in the top right corner.
3. When the page re-loads, select **Actions > Edit title/tabs**.
4. Update the dashboard or tab names, add new tabs, or delete tabs.
5. Select **Save**.
6. Select **Save** again to save the changes to the dashboard.

Edit visualizations

To edit the visualizations shown on a dashboard, open the dashboard and select **Actions > Edit dashboard.** When the page re-loads, you'll see two new panes on the right side of the screen:

- **Visualizations:** A large toolbox that lets you edit the dashboard's existing visualizations and add new ones
- **Data:** All the data available to be represented in the visualizations on the dashboard. If you select a visualization, yellow checkmarks appear beside the data fields that are used in that visualization.

See Tour the report editor in Power BI for a detailed overview of these new panes. Note that in this article, the **Data** pane referred to as the **Fields** pane. Additionally, the article refers to a **Filters** pane, which isn't visible in Axon Records and Axon Standards.

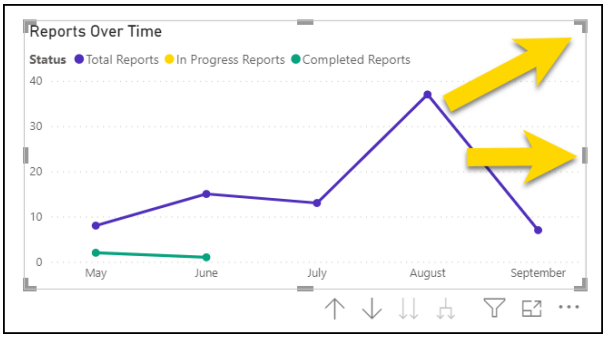
See the Power BI documentation links below for information about the different visualization types, and how to add them to a dashboard.

- Types of visualizations: Explains all the different types of you can add to your dashboards.
  - Note that not all of these visualizations are available in Axon Records and Axon Standards
- Drill mode in the Power BI service: Adding drill downs or drill ups lets your users interact with your visualizations and find additional information as desired.
- Interact with an ArcGIS map in Power BI
- Change the type of visualization in a Power BI report
- Add visuals to a Power BI report: Note that you can skip the first section (Prerequisites) and jump straight to the second section.
- Field list icons: Explains the different types of fields that appear in the **Data** pane

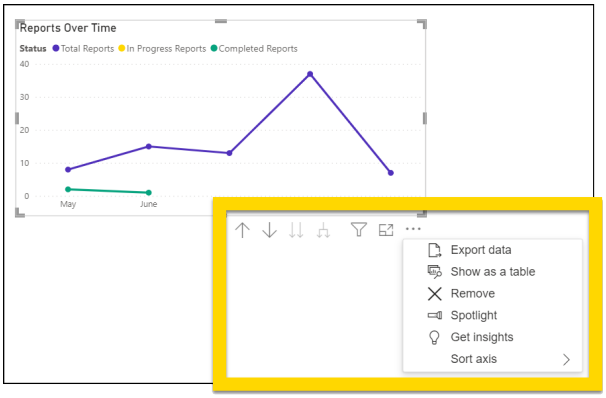
You can also use the search bar in the top left corner of the Power BI documentation to search for content by keyword.

Quick tips

Click and drag to move a visualization or use the tick marks to change its size.



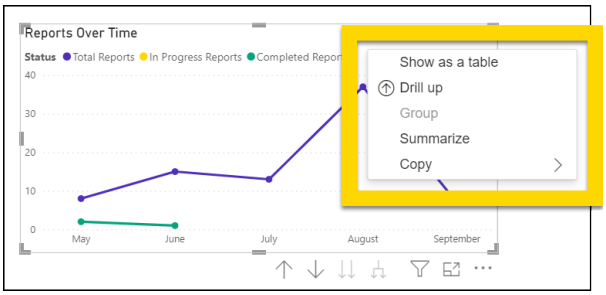
Select a visualization to reveal a menu with additional options.



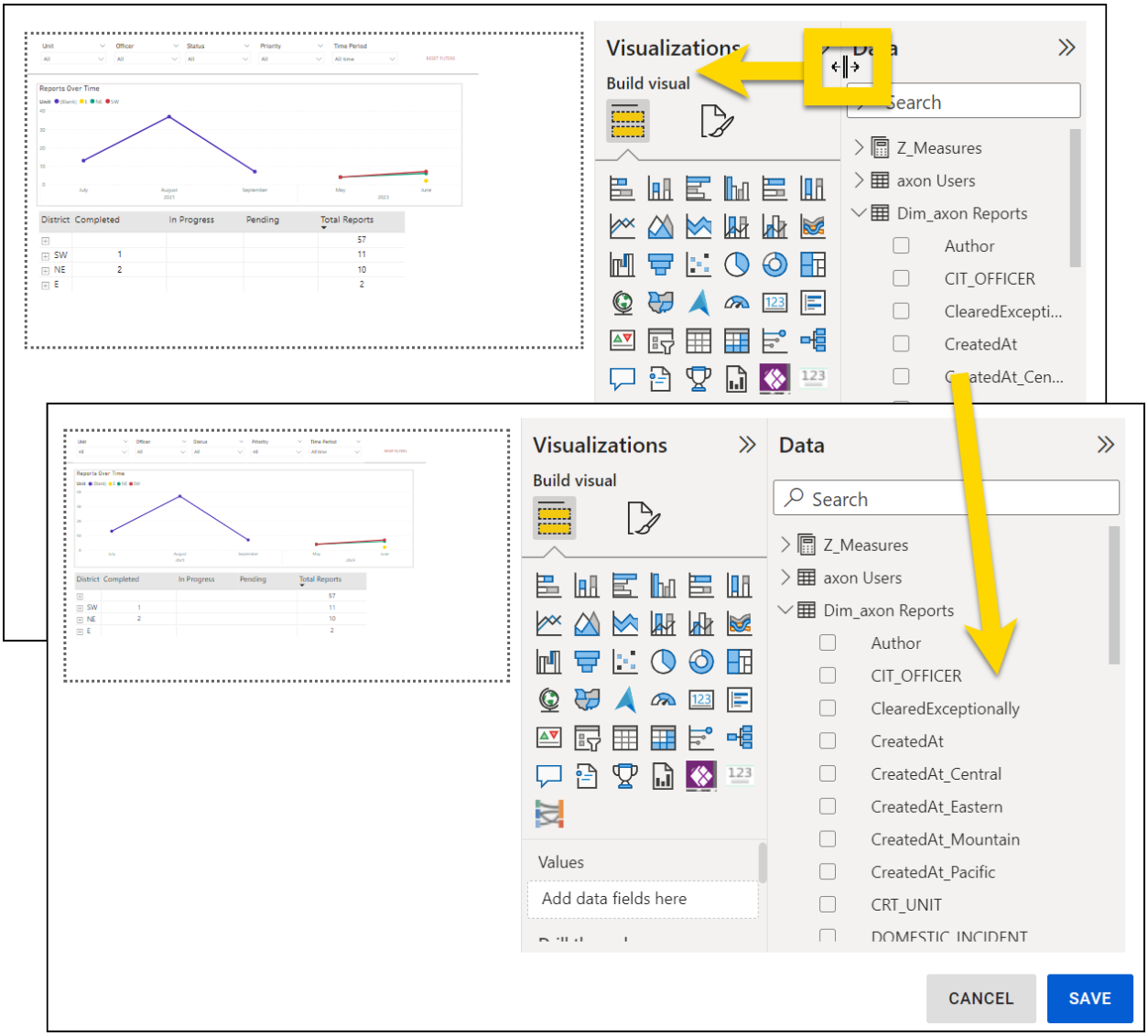
Note

Use the **Spotlight** option to open a single visualization on its own page for easier viewing and editing.

Right-click anywhere on a visualization to reveal additional options.



To increase the size of either the **Visualizations** or **Data** panes, hover your cursor over the left edge of the pane until it turns into a double-arrow cursor . Click and drag to the left to increase the size of the pane.



Save dashboards

After making changes to an Analytics dashboard, select **Save**.

Selecting **Cancel** discards any changes made on a tab but does not discard any new tabs that have been created. To delete a tab, select **Actions > Edit title/tabs**.

Delete and archive dashboards

To delete or archive a dashboard, open the dashboard and select **Actions > Delete Dashboard** in the top right corner. You can then select if you want to permanently delete the dashboard or archive it.

Archived dashboards can be restored from the Analytics tool in the Administrator Console.

View dashboard activity logs

The **Activity Log** tab is the last tab on each Analytics dashboard. This tab contains a log of all actions taken on that dashboard, who took the action, and when.

Early Intervention System (EIS)



The Early Intervention System (EIS) module, accessed by selecting the alert icon in the main navigation menu, is an early intervention tool that allows agencies to meet CALEA Standard 35.1.9 and to monitor their officers' risk profiles with minimal manual effort.

The EIS collects data from Axon Standards reports and aggregates a count of each type of event each officer is involved in (use of force, traffic collisions, citizen complaints, custom agency forms, etc.).

The EIS administration tools let administrators create policies that outline an acceptable threshold for each type of event (i.e., how many times an officer can be involved in each type of event). When officers cross a threshold, their supervisors are alerted via email. This information is also presented in the EI Dashboard.

Using the EIS module, supervisors can track their actions and counseling in response to alerts.

The EIS module can be accessed from Axon Standards by users with specific privileges. Selecting the alarm icon in the left navigation menu will open the module. Depending on your privileges you will see one or more of the following links:

- My Alert inbox
- Agency Alert inbox
- EI Dashboard

Watch this video for an overview of the Early Intervention System in Axon Standards.

Alerts and reports

EIS alerts are generated based on the report creation date, as well as the officer name and role (Involved) that are entered in the report.

An officer's involvement in an event isn't tracked to an EIS policy until the report is submitted for review. This prevents unnecessary alerts of officers being added to a report by mistake during report drafting.

Alert inboxes

The My Alert inbox in the EIS module contains all alerts that have been assigned to you for review (similar to how your My Tasks inbox shows all reports assigned to you). Command staff and IA can use the Agency Alert inbox to see all alerts at the agency.

The following information is included for each alert:

- **Status** of the alert (New, IA Review, Review, Chain of Command Review, Secondary Review, Intervention Pending, Resolved, False Positive, Acknowledged)
- **Alert policy** name
- **Officer** associated with the alert
- **Severity** of the alert (critical or warning)
- **Date** of the original alert
- Command Hierarchy group or team the officer belongs to

Use the filters to adjust which tasks are displayed:

- **Alert status** (New, IA Review, Review, Chain of Command Review, Secondary Review, Intervention Pending, Resolved, False Positive, Acknowledged)
- **Date**
- **Officer**
- **Group**
- **Alert policy**
- **Severity** (Critical, Warning, Any severity)

Select an alert to view the alert details.

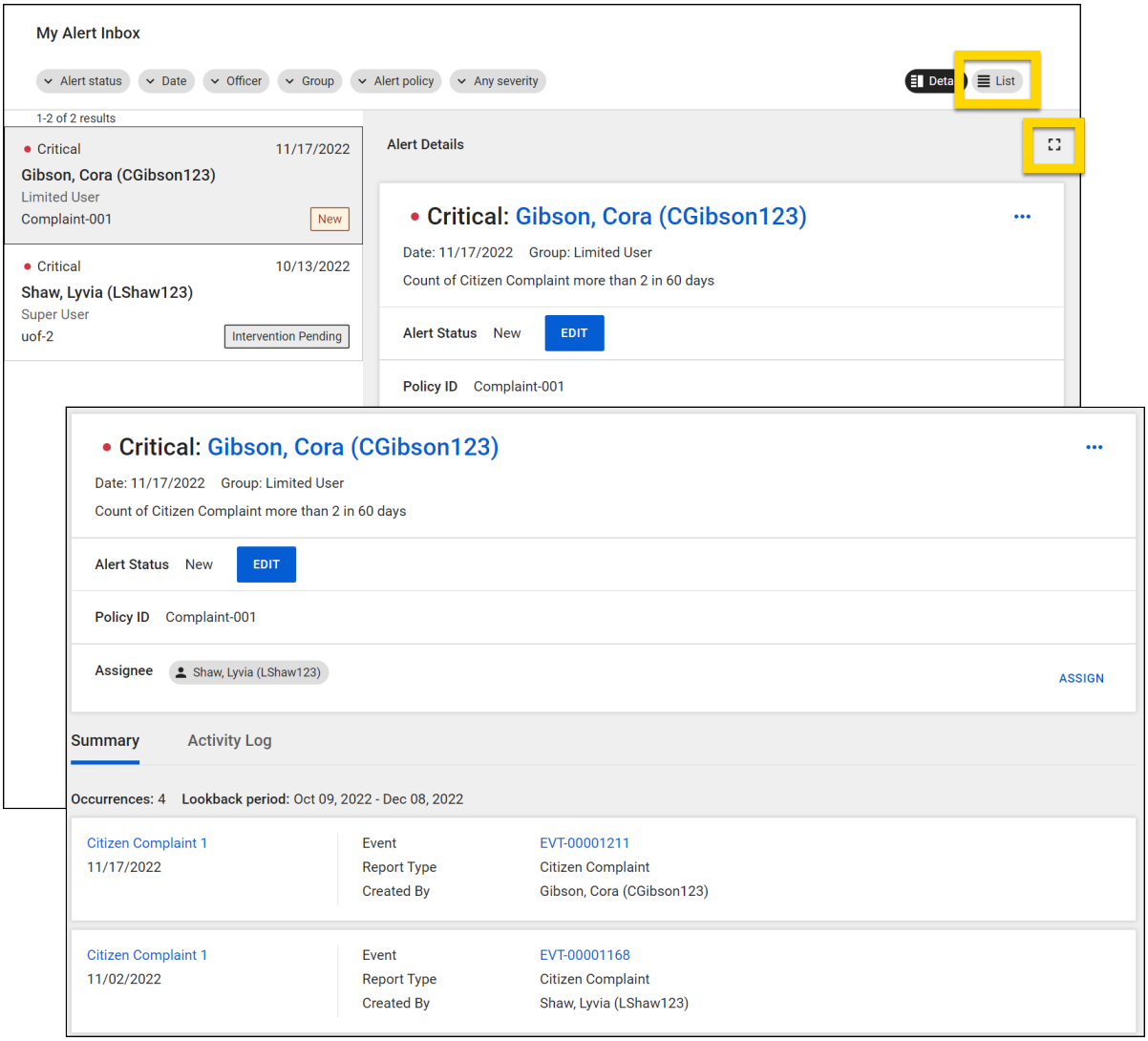
Alert management

Selecting an alert from either EIS inbox condenses the alert list and opens the Alert Details beside it. To view this page as a full screen, select the full-screen icon. The alert will open in a new browser tab where you can view all information about the alert and take action. Select **List** to close the Alert Details window and continue browsing the alert list.

From the Alert Details page you can:

- View the alert summary
- Assign the alert for review
- Edit the alert status

- Manage the activity log

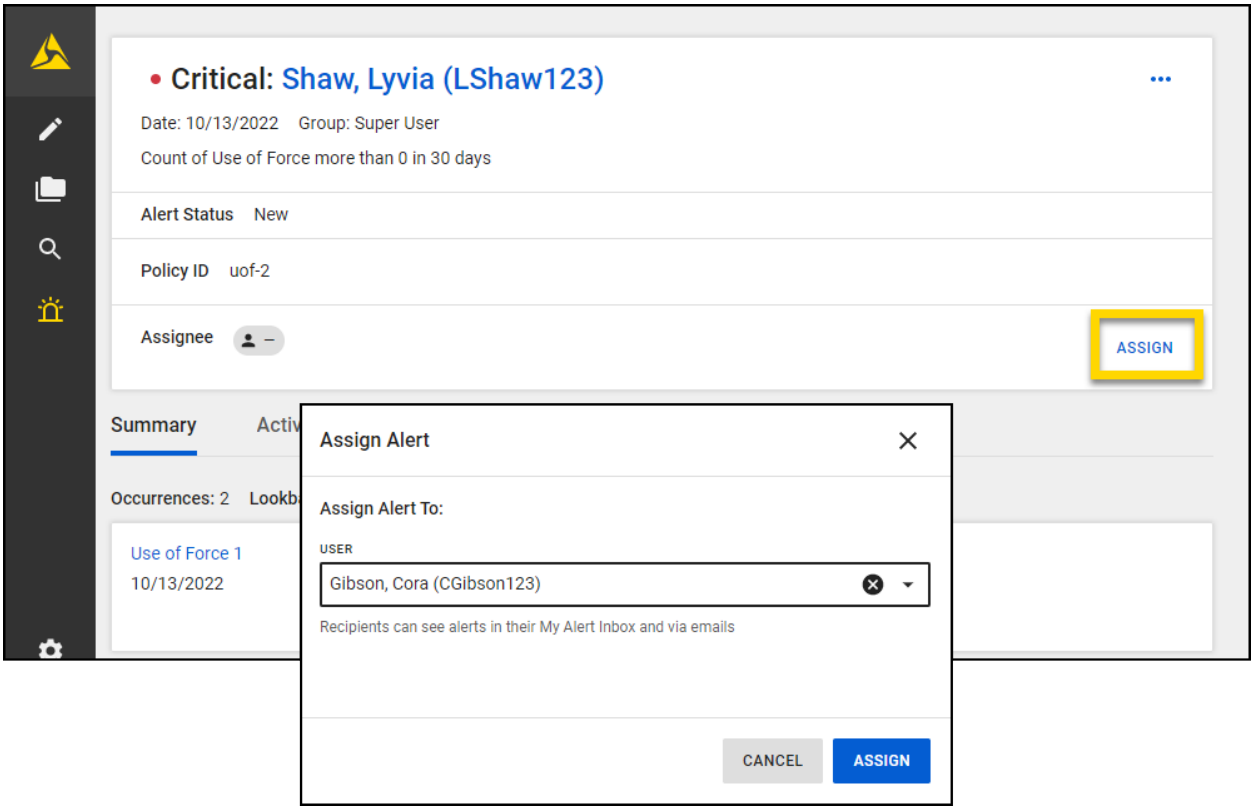


View alert summary

View the events associated with an alert on the **Summary** tab. Select the report name to open the report in a new browser tab. Select the Event ID to open the event profile in a new browser tab.

Assign alert

Select **Assign** to assign a user to review an EIS alert and its associated events.



Once assigned to an alert, that user will receive an email notifying them that they have an alert to review.

Edit alert status

If you have been assigned to review an EIS alert, you can select **Edit** to update the alert status. You can select from the following status options:

Active

- **IA Review**
- **Review** (supervisor review)
- **Chain of Command Review**
- **Secondary Review**
- **Intervention Pending**

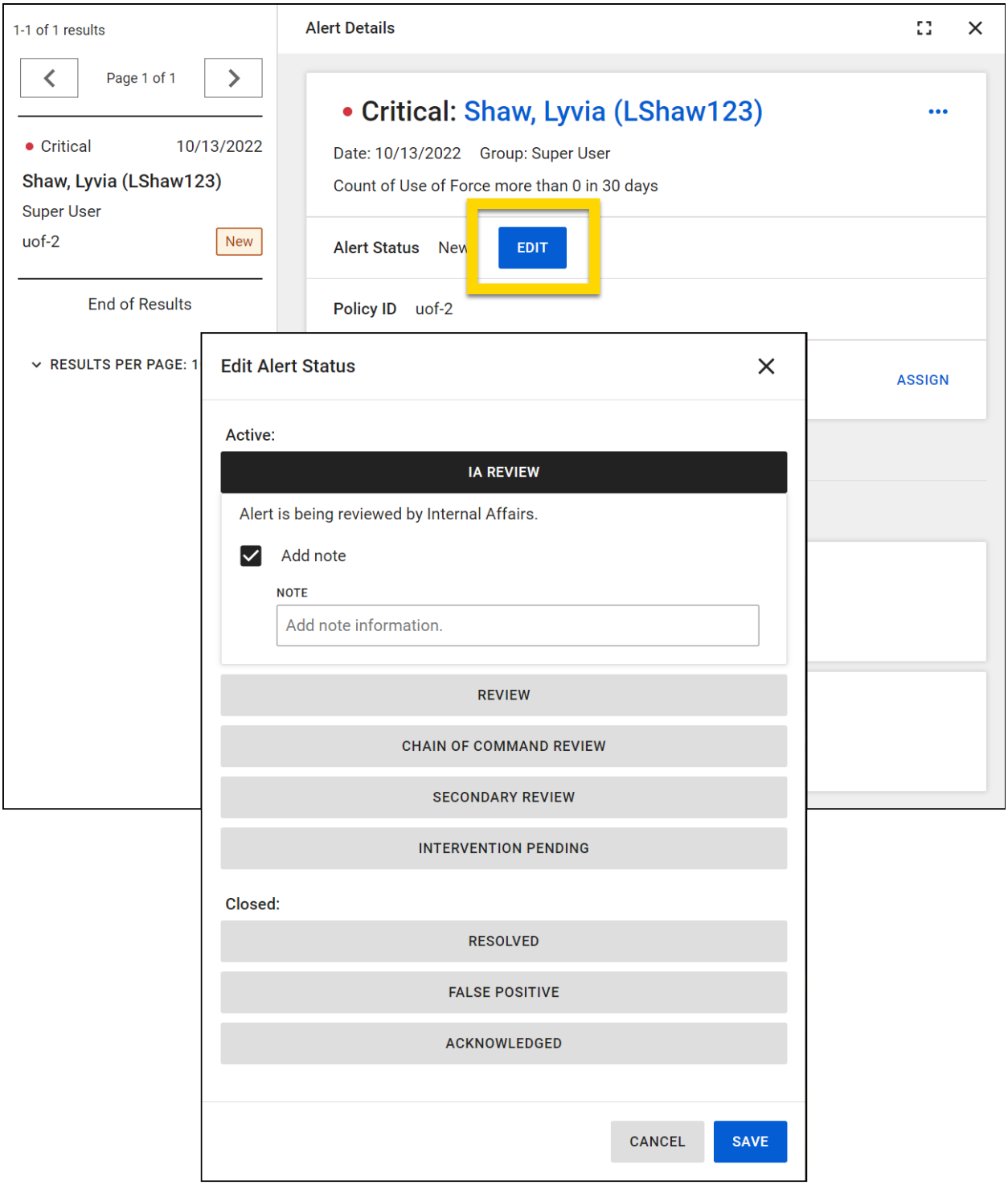
Closed

- **Resolved** (the alert has been addressed with the appropriate interventions)
- **False Positive** (the alert incorrectly indicated that an intervention is needed)
- **Acknowledged** (after reviewing, the supervisor decides that no action is necessary)

Note

Contact your Axon representative if you would like to customize these statuses to better fit your organization's needs.

Check the **Add note** checkbox to document additional information about the status update. All status updates will reflect in the alert activity log.



Manage the activity log

Open the **Activity log** tab to view all activities for that alert. Select **Add activity** in the top right corner of the tab to add an activity to the log. You can include a note or describe an action that was taken.

These notes, along with notes made during status updates can be viewed at any time, even after the alert is resolved, by going to the Agency Alert inbox and filtering to show Resolved alerts.

Early Intervention (EI) Dashboard

The Early Intervention (EI) Dashboard gives supervisors, command staff, and IA an at-a-glance view of officer performance against policies. The dashboard provides additional data to proactive supervisors who want to identify which officers are in danger of triggering alerts and agency leadership as they evaluate department performance against goals.

The EI Dashboard is organized in a table format. Each row is dedicated to a single officer. Each column indicates a specific policy and lookback period. The lookback period starts on the current day and looks back in time for the rolling timeframe specified by the policy.

If an officer is involved in events tracked by a policy, one or more color bars will appear in their row:

- **Green, In Policy Events:** The number of events the officer was involved in were below the threshold and an alert didn't trigger for that policy
- **Orange, Warning Events:** The number of events the officer was involved in triggered a warning alert for that policy.
- **Red, Critical Events:** The number of events the officer was involved in triggered a critical alert for that policy.

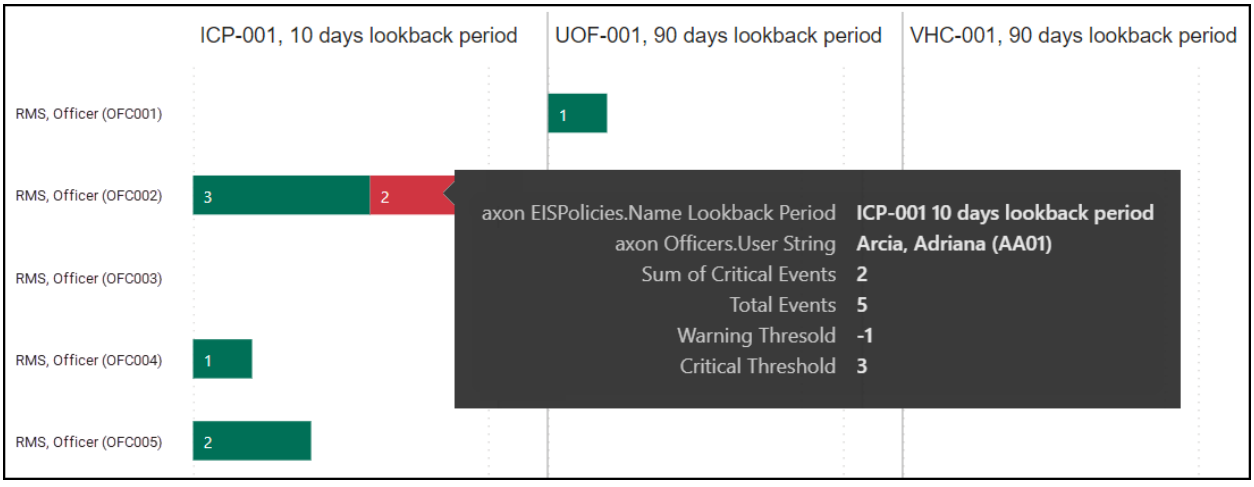
If a user is not associated with any events tracked by a policy, they will not appear in the EI Dashboard. You can control which data each user sees with privileges.



Note

The EI Dashboard shown in this section is an example. The look and feel of this dashboard may vary by organization.

Hovering over any bar reveals all information about that data point.



Filters

Use the filters on the right to adjust the information displayed on the screen. You can select from:

- **EIS Policy Name**
- **Lookback Period**
- **User ID**

To use the filters:

- Select the arrow beside a filter to reveal a search bar and checkboxes beside specific filters.
- Select the eraser icon to remove any set filters.
- Use the **Filter Type** menu to switch to advanced filtering where you can narrow down the filter with even more granularity.
- Collapse and expand the filters panel using the sideways arrows.

Show as table

To view the information in a table, right-click anywhere on the chart and select **Show as a table**. The table will appear below the chart.

Personnel

The Personnel module provides comprehensive employee management, offering tools to view and manage employee demographics, career milestones, and more.

Access the Personnel module by selecting the person icon in the main navigation menu. From here you can edit or view the following information:

- Demographics: Personal and background details
- Service history: Employment timelines, including absences, assignments, light duty, and separations
- Commendations and awards: Recognitions and achievements
- Performance reviews: Detailed performance evaluation records
- Promotions: Career advancement through the ranks
- Discipline: Formal record of disciplinary actions
- Related reports: All Axon Standards reports the user has created or been mentioned in

Access to the various features within the Personnel module is controlled by privileges, letting you determine to what extent users can access other users' information. Administrators can also quickly add data for multiple users with the Personnel import tool.

Homepage

When you open the Personnel module, the Homepage loads, which contains three tabs:

- My Profile
- My Team
- Feedback Notes

To find another user's profile, use the search bar at the top right of the Personnel page. Start typing a first name, last name, or username, and select a user from the dropdown menu.

Note

You can only view search for and view profiles you have been granted privileges to view.

My Profile

The **My Profile** tab provides an overview of your basic profile information. To view your full profile, select your profile summary.

My Team

The **My Team** tab provides a centralized location for users to view their teams, who is part of each team, and the contact information for each team member. Teams are displayed in two categories:

- **Command Hierarchy Groups supervised by me**: Teams you supervise
- **Command Hierarchy Groups I am a member of**: Teams you belong to

Select a group to expand the section and see the users assigned to that group. The name, email, phone, and profile status are shown for each group member.

My profile

The Personnel module contains detailed employee information beyond basic demographics, including service history, performance, education, and more. Each user with the appropriate privileges can view their profile, and the profile of others.

To view your own profile, open the Personnel module by selecting the person icon in the main navigation menu and select your profile summary. To view the profile of another user, search for them using the search bar in the top right corner.

A profile contains various tabs and within those tabs sections that all contain different information:

- Personnel: Contains basic information and records for the user. Sections on this tab include:
  - Demographics: Personal and background details
  - Service history: Employment timelines, including absences, assignments, light duty, and separations
  - Commendations and awards: Recognitions and achievements
  - Performance reviews: Detailed performance evaluation records
  - Promotions: Career advancement through the ranks
  - Discipline: Formal record of disciplinary actions
- Related reports: All Axon Standards reports the user has created or been mentioned in
- Command Hierarchy: Displays the Command Hierarchy Groups the user belongs to
- Audit log: Contains a record of all actions taken on that user's profile

Note

See Personnel fields for more information about the fields that appear by default in the Personnel module. These fields can be configured for each organization.

Update profile

Users with the appropriate profiles can edit profiles by taking the following actions:

1. Select the category you want to update (e.g., Service history, Performance review, etc.).
   - The process for managing the Demographics section is slightly different. See the Demographics section below for more information.
2. Select **Add new** in the top right corner.
3. Fill out all required fields.
4. Select **Add attachment** if have any documents or files you need to include with the record.
5. Select **Save**.

Note

To add information to multiple users, use the Personnel Import Tool in the Administrator Console.

To edit or delete existing record, open the **More actions [...]** menu for that record and choose an action.

- **Edit**: This will allow you to update information or remove attachments. Within the edit mode, you can change any detail or click **Remove** next to an attachment to delete it.
- **Delete**: This allows you to completely remove a record. A confirmation prompt appears to prevent accidental deletions.

Update Demographics information

There are two parts to the Demographics section:

- **Contact and personal info:** Sensitive information, including SSN/National ID, and personal contact information
  - This section can only be viewed and edited by users with Contact & Personal Info privileges.
- **Demographics:** Basic information, work information, and education and skills

Select the pencil icon located in the right corner of either section to modify demographic details. With most of the demographic fields, you can add or edit information by selecting the field and typing. If the field is a dropdown menu, select from the available options.

To add an emergency contact, educational history, or skill select **Add new**. A new set of fields appears, allowing you to enter information. To remove an existing emergency contact, educational history, or skill from the profile, select **Remove** next to the item you wish to delete.

After completing all edits, scroll to the bottom of the page and select **Save**.

You can configure your reports to auto-fill with certain fields from the Personnel module (e.g., precinct, unit, race, Officer ID, etc.). Contact your Axon representative or Axon Support to set up this configuration.

Related reports

Select the **Related reports** tab within a user's profile to view a list of reports they have created or are mentioned in. The report list varies by organization.

> **Note**
>
> This tab is only available when you are logged into Axon Standards. If you are logged into Axon Records, you will not see this tab. To view the tab, switch to Axon Standards.

Reports are sorted with the most recent ones appearing at the top of the list. To filter to a specific type of report, select a category from the list on the left. Each report contains the following information:

- Report ID: Select the Report ID to open the report in Report Writer
- Involvement status: The user's role or involvement in the report (e.g., Witness, Involved, etc.)
- Report author: The person who created the report
- Date and time: The date and time provided in the Event Overview section of the report

Audit log

The **Audit log** tab within each user's profile contains a comprehensive record of all actions taken on that specific profile. Each entry includes the date and time of the action, the modification made, and the user made the change.

The audit log entries are listed from oldest to newest. These entries are automatically created and cannot be altered or added manually. Use the filters at the top of the tab to sort the information by date, name, badge number, or action type. Select **Export** to export the table to a CSV file.

Training

The Training module lets you manage your organization's courses, curricula, and learners to ensure that officers are prepared to perform their duties effectively, safely, and in accordance with law and policy.

When using the Training module, it's helpful to understand how the following terms are used:

- **Curriculum:** Contains the files the instructor teaches, as well as details about the curriculum, including description, type of training, etc.
  - Once created, a curriculum is added to one or more courses, along with a group of learners.
- **Course:** Contains a curriculum and a set of learners, occurs at a specific date/time (if in-person) or contains a video conference link (if online instructor-led).
  - An instructor is assigned to the course and is responsible for teaching that course's curriculum.
- **Certificate:** A certificate is awarded to a learner after they have completed a course. This certificate is Active for a set period of time. When a certificate expires, the leaner must re-take the course to renew the certificate.

The Training-related actions vary by the type of user and the privileges they have been given. A learner can:

- View courses they are enrolled in
- View courses taken by their team members

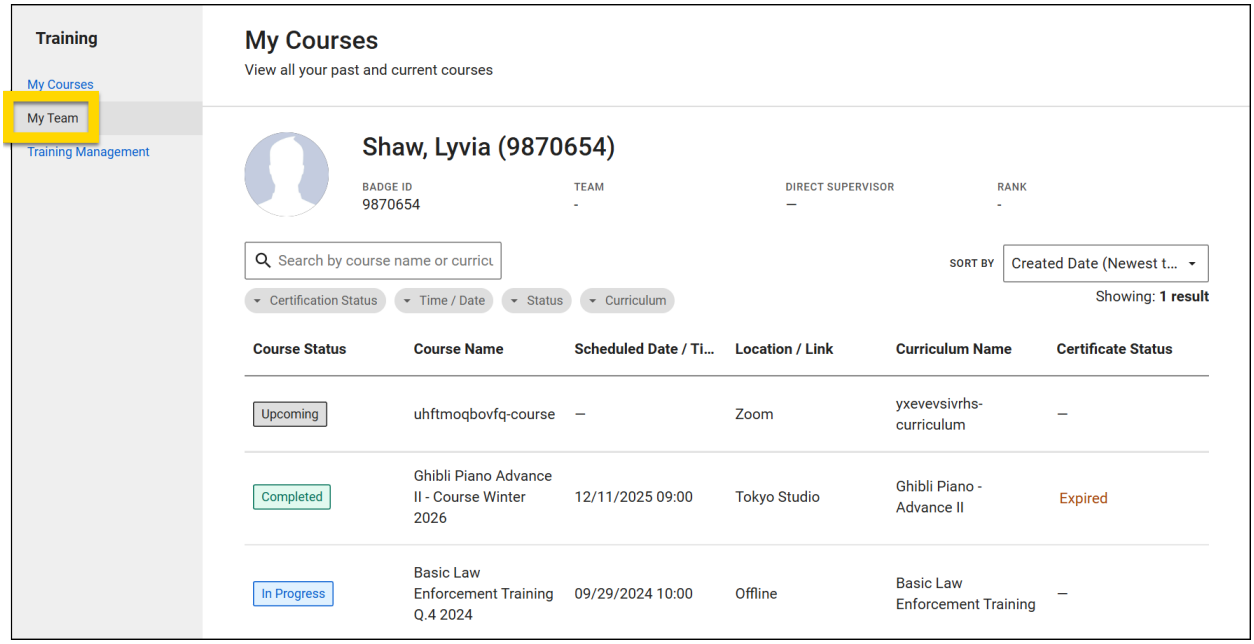
Administrators and instructors can:

- Create and manage the organization's curricula
- Create and manage the organization's courses
- Enroll learners in courses
- Take attendance for courses they are assigned to
- Record scores for courses they have taught
- Export training records for in progress and completed courses
- Import training records from other systems

This video contains an overview of training management, including how to create curricula and courses.

My Courses

The My Courses page appears to all users. It displays the list of all courses you are currently enrolled in, as well as all past courses you been enrolled in.



Use the search bar to find a specific course or curriculum and the filters to refine which courses are displayed in the list. Options include:

- Certification status
- Time / Date
- Status
- Curriculum

Use the **Sort By** menu to set the order in which courses are listed. Options include:

- Created Date (Newest to Oldest)
- Created Date (Oldest to Newest)
- Scheduled Date / Time (Newest to Oldest)
- Scheduled Date / Time (Oldest to Newest)

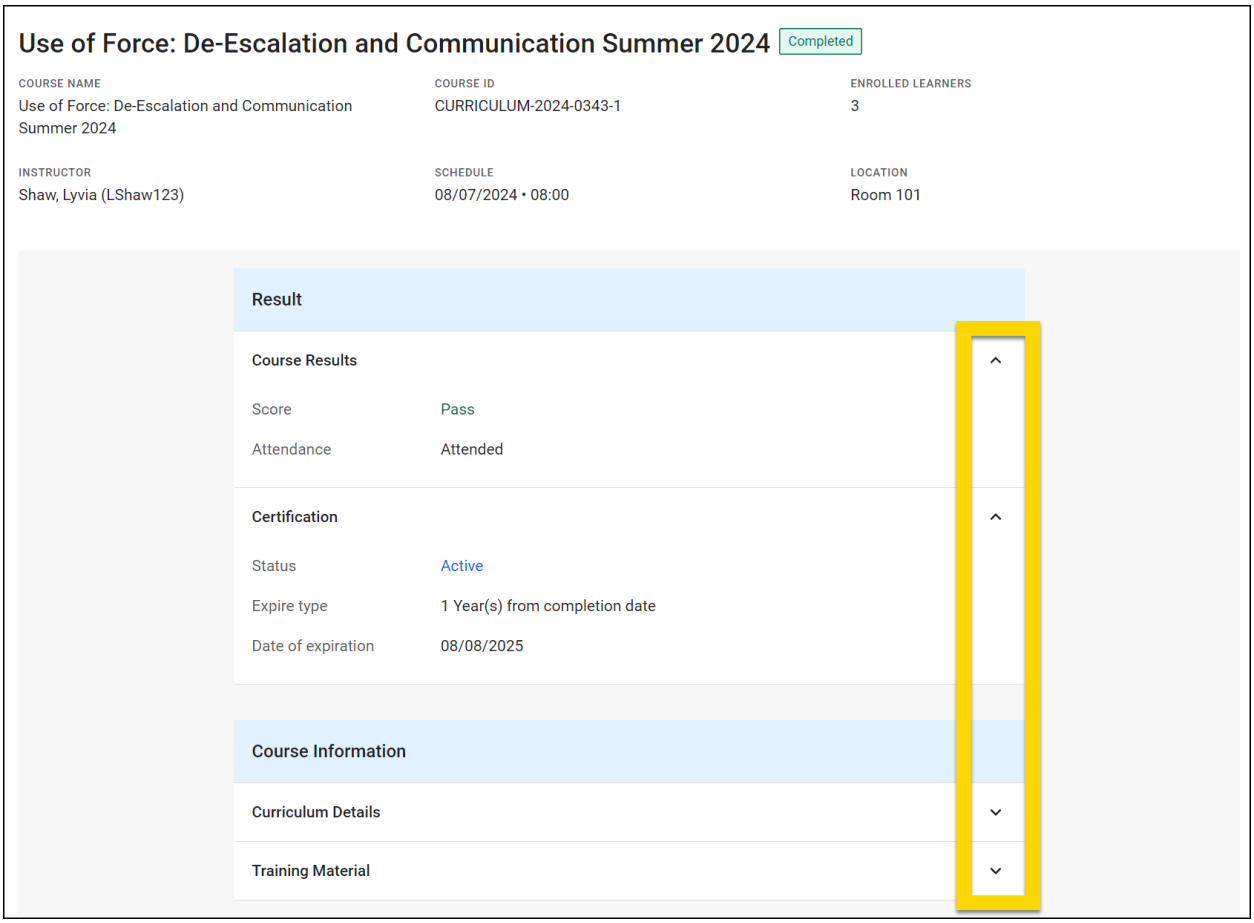
The information for each course in the list includes:

- **Course Status:** The courses shown on this tab can be in one of four different statuses:
  - Upcoming: The course has been created and is scheduled for a future date.
  - In Progress: The instructor has taken attendance and the course is in progress.
  - Completed: The course has been finalized.
  - Canceled: The course was canceled.

- **Course Name:** The name of the course
- **Scheduled Date / Time:** The date and time the course is scheduled for
- **Location / Link:** The location of the course. If the training is an online instructor-led course, the video conference link appears here.
- **Curriculum Name:** The curriculum taught in the course
- **Certificate Status:** Whether the certificate associated with that course is Active or Expired

Select a course name to open the course and view the course details page. At the top of the page, basic information about the course is displayed, including name and status

If the course has been completed, the **Result** section displays score, attendance, and certification. Additional course information, including details and training material appears below the results. Use the arrows to expand and collapse sections.



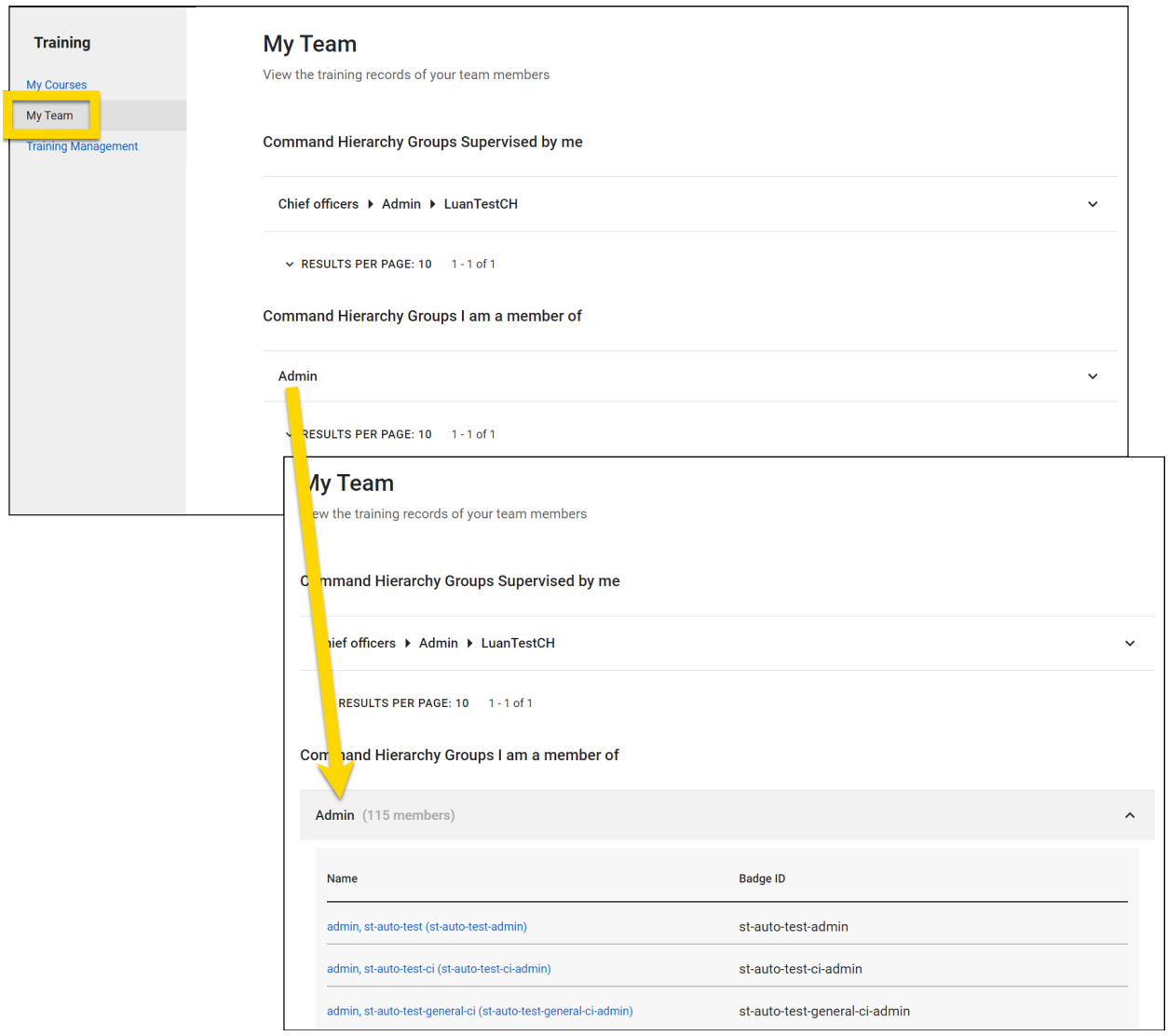
My Team

The **My Team** page lets users with specific privileges view training records for their team members. The teams you belong to appear in two categories:

- **Command Hierarchy Groups Supervised by Me**: Teams you supervise
  - If you do not supervise any teams, you will not see this section.
- **Command Hierarchy Groups I am a member of**: Teams you belong to

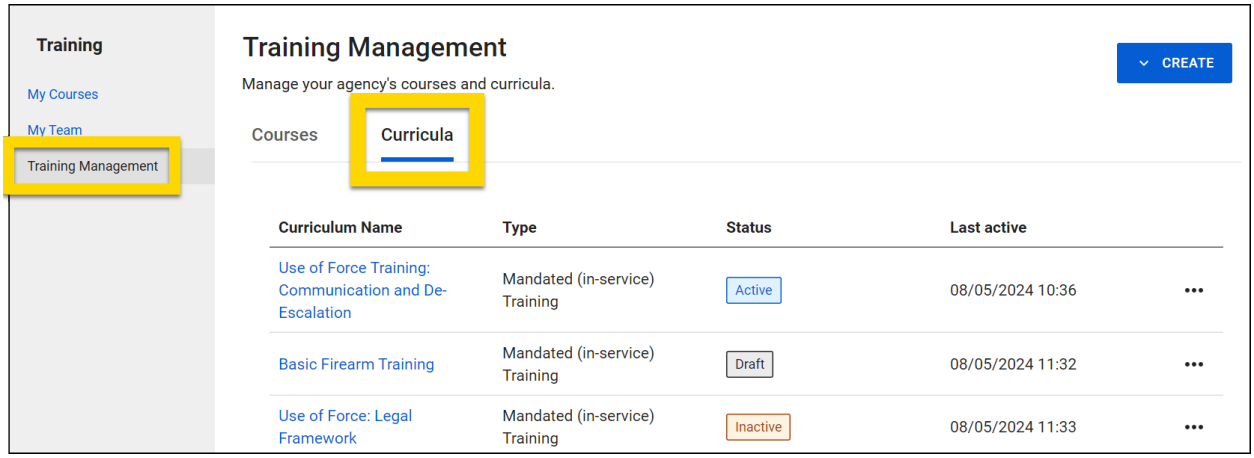
> **Note**
>
> The information in these sections is based on the information in the Command Hierarchy.

Select a group to expand the section and see the users assigned to that group. Select a user's name to view the courses they have been enrolled in. Users with specific privileges can select courses on this page to view that learner's performance in that course.



Manage curricula

All curricula that have been created for your organization can be found by opening the Training module and going to **Training Management > Curricula**.



Use the search bar to find a specific curriculum and the filters to refine which curricula are displayed in the list. Options include:

- Status
- Type

Use the **Sort By** menu to set the order in which curricula are listed. Options include:

- Created Date (Newest to Oldest)
- Created Date (Oldest to Newest)
- Last Update (Newest to Oldest)
- Last Update (Oldest to Newest)

The following information is included for each curriculum listed on this tab:

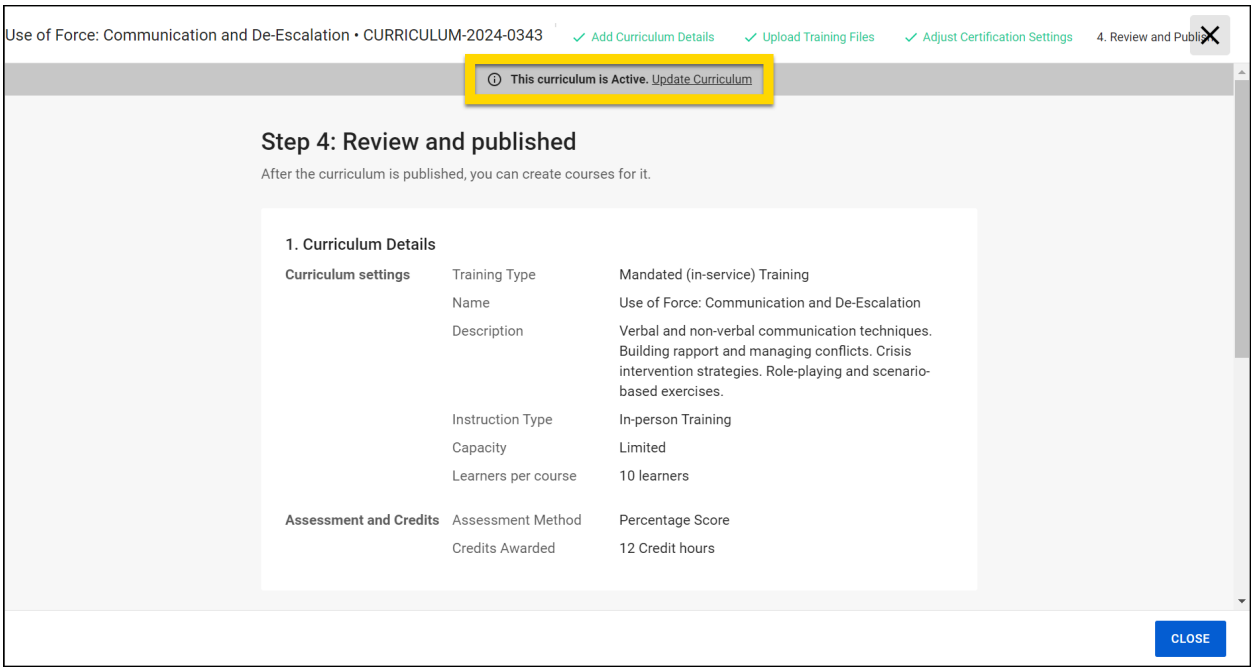
- **Curriculum Name:** The name of the curriculum. This name is displayed on the course details page for any courses it is added to.
- **Type:** Either mandated (in-service) or supplemental (non-mandated).
- **Status:** A curriculum can have one of three statuses:
  - **Draft:** The curriculum is being created and can be added to one or more courses once it is published.
    - If you make updates to an Active curriculum, the status of the curriculum changes to Draft. When the curriculum is republished, its status changes back to Active.
  - **Active:** The curriculum is active and can be added to one or more courses.
  - **Inactive:** The curriculum is inactive and can't be added to any courses unless it is restored and republished.
- **Last active:** The last date/time the curriculum was edited.

Select **More Actions [...]** on any curriculum to:

- Create course for curriculum
- Update
- Mark as inactive
- Restore

Select a curriculum name to view the curriculum, including all curriculum details, training files, and certification settings. Based on the curriculum's current status, you can take the following actions by selecting the link in the top gray banner:

- Draft: Continue editing and publish
- Active: Update the curriculum (return it to Draft so you can edit it).
- Inactive: Restore the curriculum to Draft, update as needed, then republish.

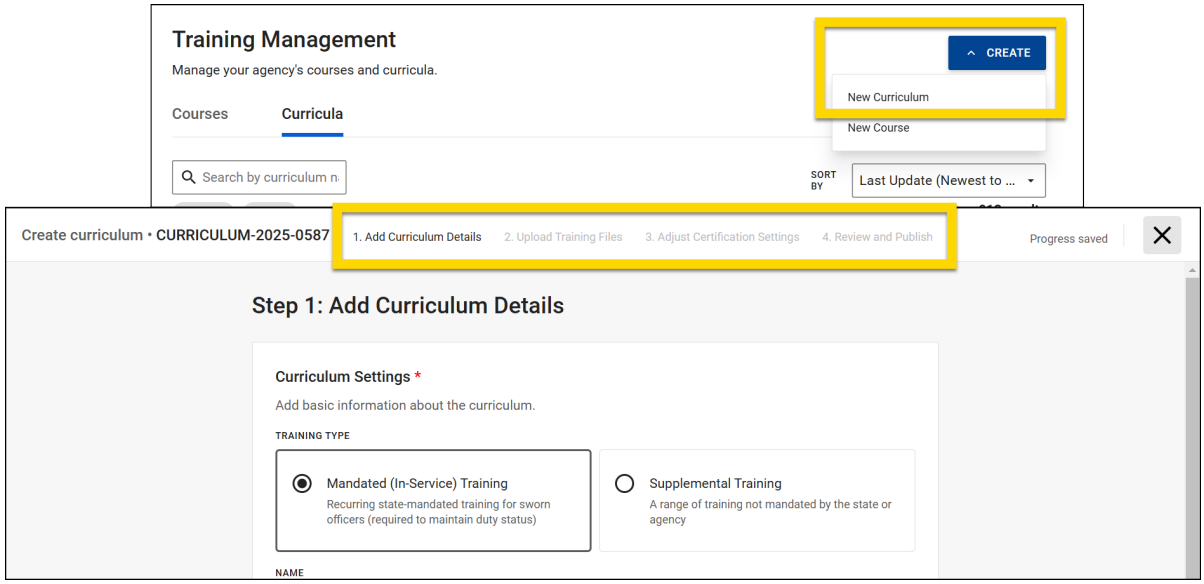


Create curricula

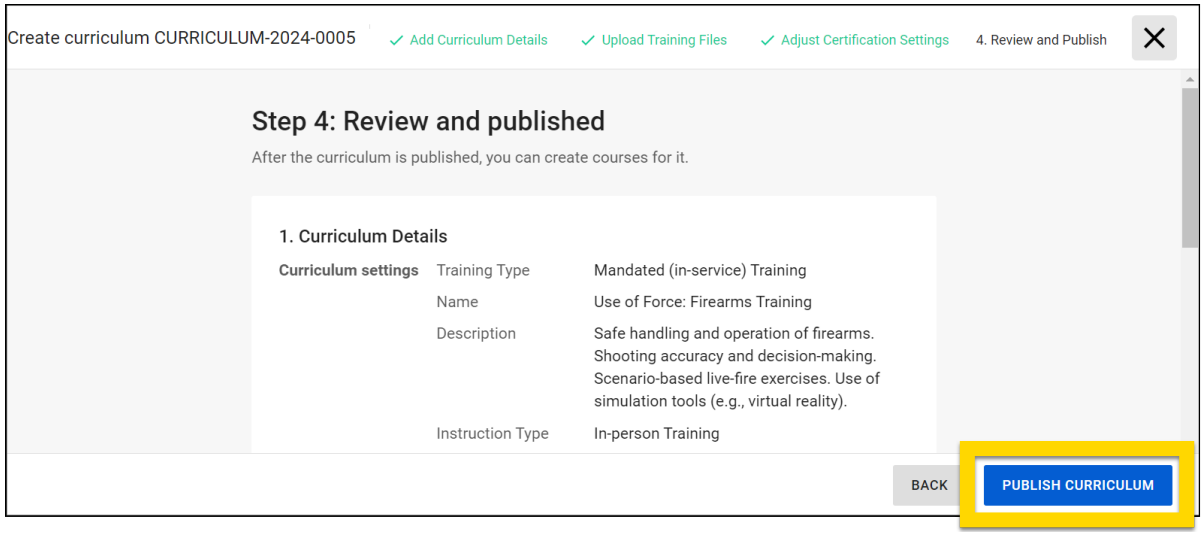
To create a curriculum, take these steps:

1. Open the Training module then select **Training Management**.
2. Select **Create > New Curriculum**.
3. Add all curriculum details.
4. Upload training files. These are the files containing the actual curriculum that the instructor teaches during the course.
   - Files must be no larger than 5 M.

5. Adjust certification settings for courses created that use this curriculum.



6. To change information on a previous screen, select **Back** to return to that step to update the information.
7. You can close the curriculum at any time by selecting the **X** in the top right corner.
   - All information you have entered will automatically be saved and the curriculum will remain in Draft status until you publish it. While a curriculum is in Draft, it can't be added to any courses.
8. After providing all information, review and publish your curriculum. **Select Publish Curriculum** to make the curriculum Active so it can be added to courses.



9. Once a curriculum is published, you can view it and update as necessary from the **Curricula** tab.

Curriculum details

When creating or updated a curriculum, provide the following details:

- **Training Type**
  - Mandated (In-Service) Training: Recurring state-mandated training for sworn officers (required to maintain duty status)
  - Supplemental Training: Training not mandated by the state or agency
- **Name:** This is displayed to learners on their My Training page.
- **Description**
- **Instruction Type:** In- Person Training or Online Instructor-Led Training
- **Capacity:** Set the number of students who can be enrolled in courses that use this training.
  - Limited: Specify the number of learners who can be enrolled
  - Unlimited: An unlimited number of learners can be enrolled
- **Assessment Method**
  - Category Score: Learners are assessed using a category score (pass, fail, withdrawn, etc.) rather than a numeric score.
  - Percentage Score: Learners are assessed using a numeric score (90, 75, etc.) in addition to a category score (pass, fail, withdrawn, etc.).
- **Credits Awarded**
  - Credits Awarded after Course Completion: Specify the number of hours awarded
  - No Credits Awarded

Certification settings

When creating or updated a curriculum, you can adjust the type of certification expiration. Options include:

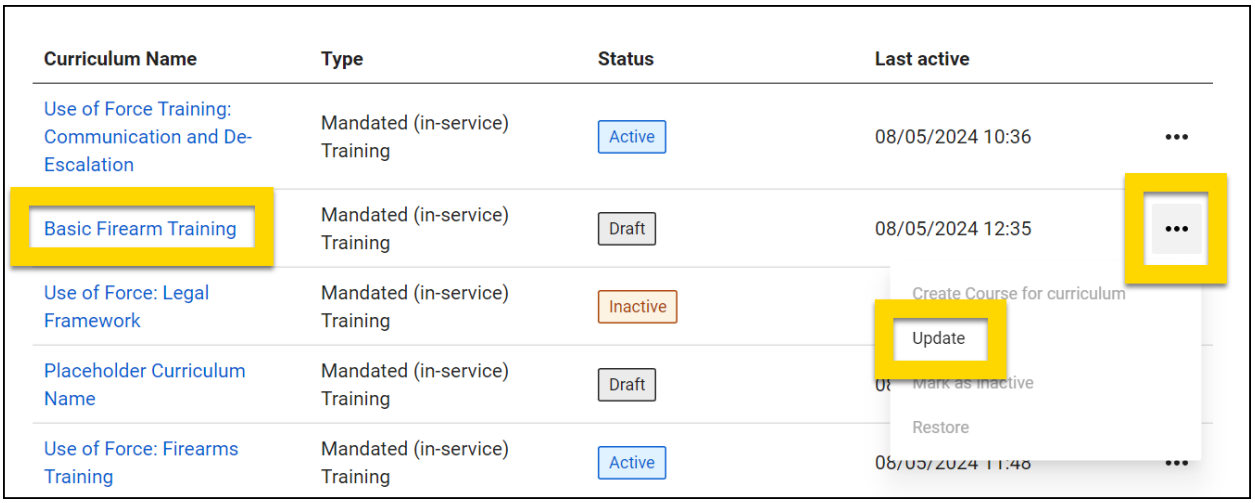
- **From Completion Date:** Certification expires a specified amount of time after the course is completed.
  - Enter the number of days, months, quarters, or years in the **Certificate Expiring Duration** field.
- **Repeating Expiration Date:** Certification expires on a set date at repeating intervals.
  - Set the interval type (every 5 months, year, 2 years, 3 years, 4 years) and the date on which the expiration takes place.
  - For example, if you want a course to expire every year on January 1, select Every Year for the interval, then January and 1 in the Month and Day fields.
- **No Expiration Date:** Certification never expires.

Watch this video for an overview of training management, including how to create curricula.

Update curricula

When updating a curriculum, you can change any of the curriculum details, training files or certification settings.

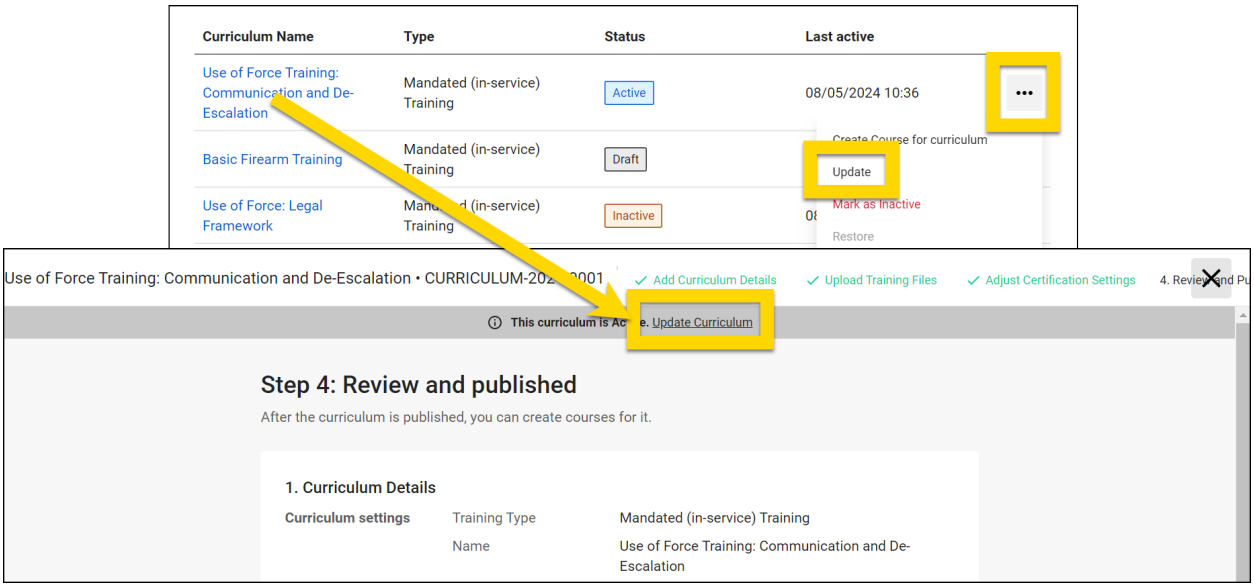
To update a Draft curriculum, either select the curriculum name or **More Actions [...] > Update**.



To update an Active curriculum, select **More Actions [...] > Update**. If you instead select the curriculum name, you can view the curriculum information in a read-only format. Update the curriculum by selecting **Update Curriculum**.

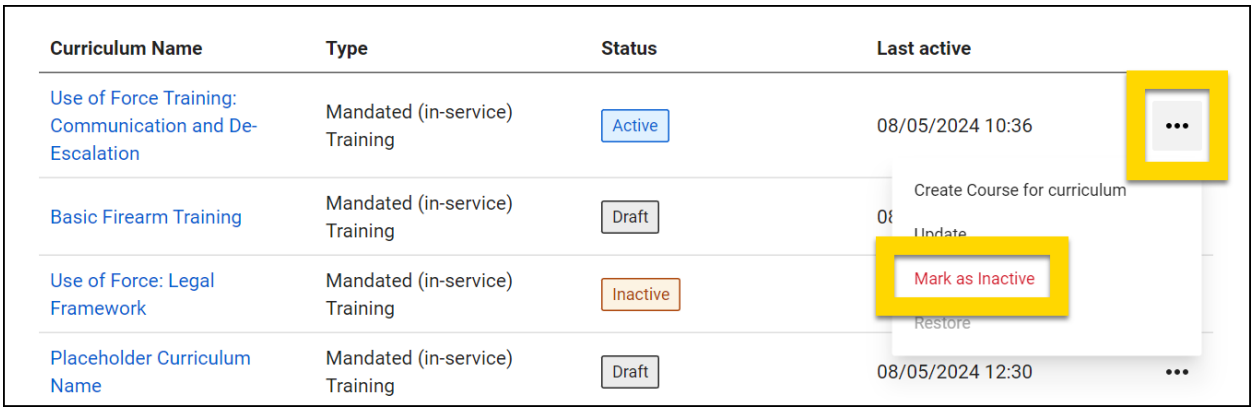
Note

Active curricula have been published and may have already been added to courses. Any updates made to an Active curriculum will NOT reflect in any courses that curriculum has already been added to. Instead, you must cancel the existing courses and create new ones that use the updated curriculum.



Mark curricula as inactive

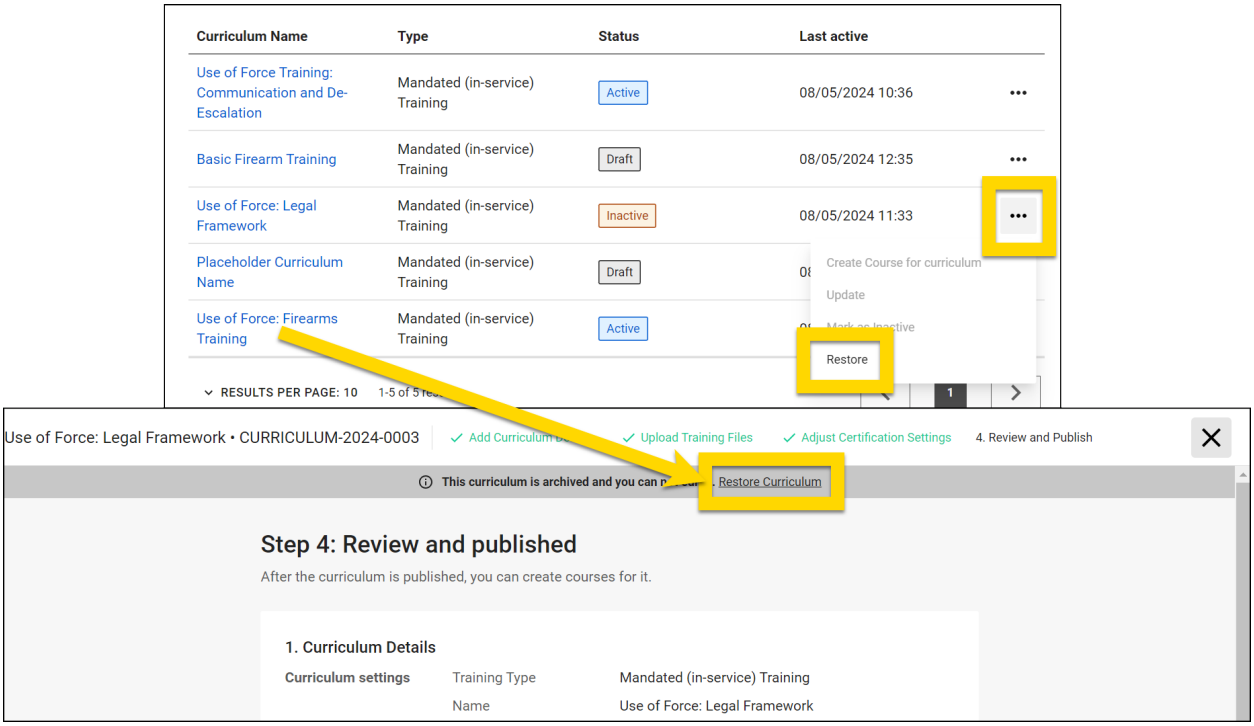
If a curriculum is inactive, it can't be added to any courses. To mark a curriculum as Inactive, select **More Actions [...] > Mark as Inactive**.



Restore curricula

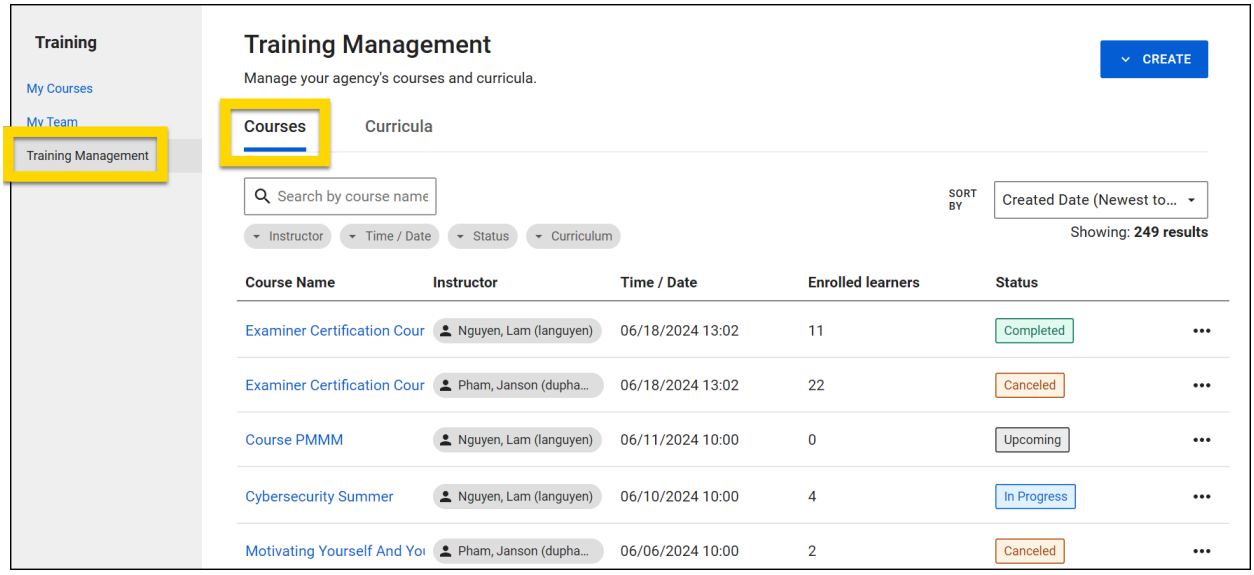
To make an Inactive curriculum Active, you must first restore it. To do this, select **More Actions [...] > Restore**. If you instead select the curriculum name, you can view the curriculum information in a read-only format. Update the curriculum by selecting **Restore Curriculum**.

When a curriculum is restored, it is moved into Draft status. When a Draft curriculum is published, it becomes Active and can be added to courses.



Manage courses

All courses that have been created for your organization can be found by opening the Training module and going to **Training Management > Courses**.



Use the search bar to find a specific course and the filters to refine which courses are displayed in the list. Options include:

- Instructor
- Time / Date
- Status
- Curriculum

Use the **Sort By** menu to set the order in which courses are listed. Options include:

- Created Date (Newest to Oldest)
- Created Date (Oldest to Newest)
- Scheduled Date / Time (Newest to Oldest)
- Scheduled Date / Time (Oldest to Newest)

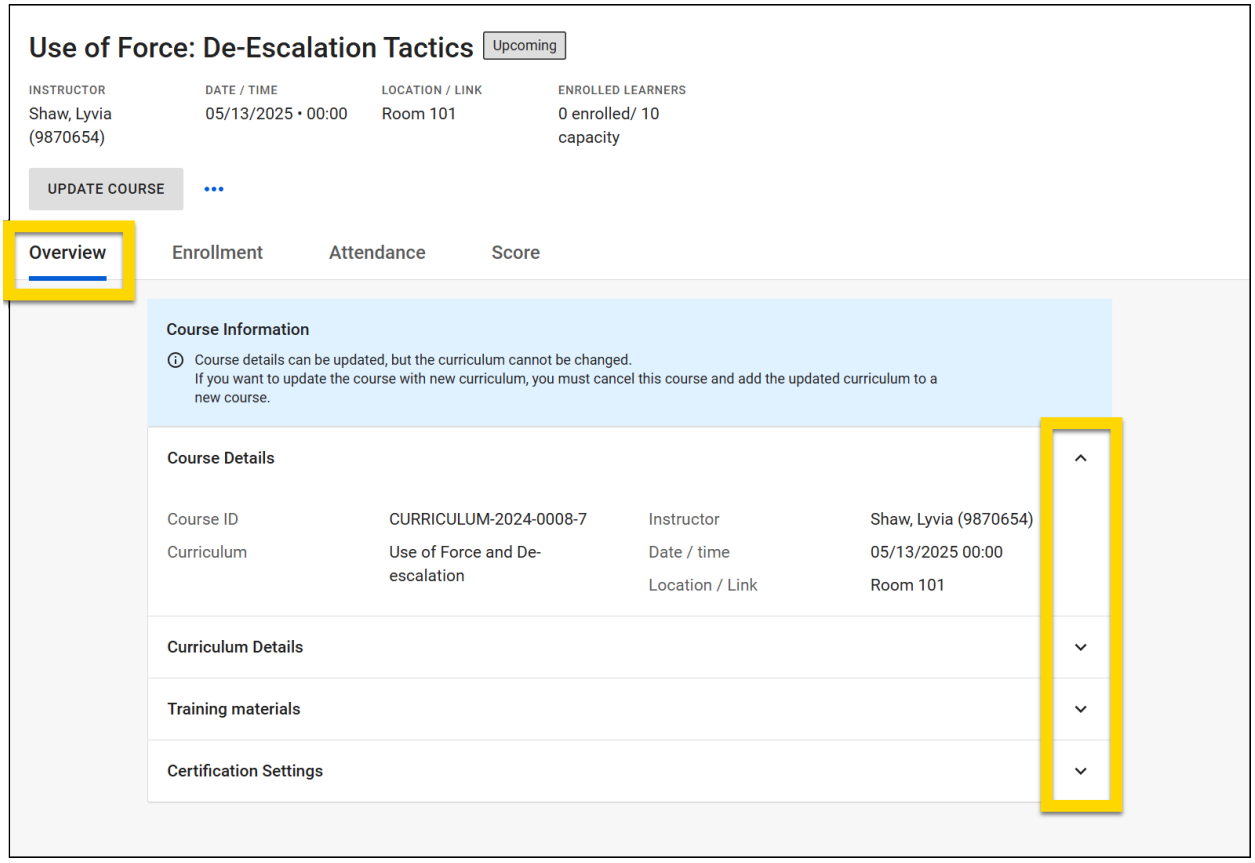
The following information about each course appear on this page:

- **Course Name:** This name also appears for learners on their My Courses page.
- **Instructor:** Instructors can take all actions on a course except cancel the course or change the curriculum.
- **Date / Time:** The date and time the course is scheduled for
- **Enrolled Learners:** The number of learners enrolled in the course. If the course has a limited capacity, the total capacity is also shown.
  - For example, 3/12 indicates that 3 learners are enrolled in a course that has a capacity of 12.
- **Course Status:** A course can have one of four statuses:
  - Upcoming: The course has been created and is scheduled for a future date.
  - In Progress: The instructor has taken attendance and the course is in progress.
  - Completed: The course has been finalized.
  - Canceled: The course was canceled.

Open the **More Actions [...]** menu to cancel a course (if it is upcoming) or export learning records (if it is in progress).

Select a course name to open the course and view the course details page. At the top of the page, basic information about the course is displayed, including name and status.

The **Overview** tab contains all course information, including Course Details, Curriculum Details, Training Material, and Certification Settings. Use the arrows to expand and collapse each section.



Take actions on the course from the other tabs, including:

- Update course
- Enroll learners
- Take attendance
- Record scores

Open the **More Actions [...]** menu to cancel a course (if it is upcoming) or export learning records (if it is in progress).

Watch this video for an overview of courses (starting at 08:03).

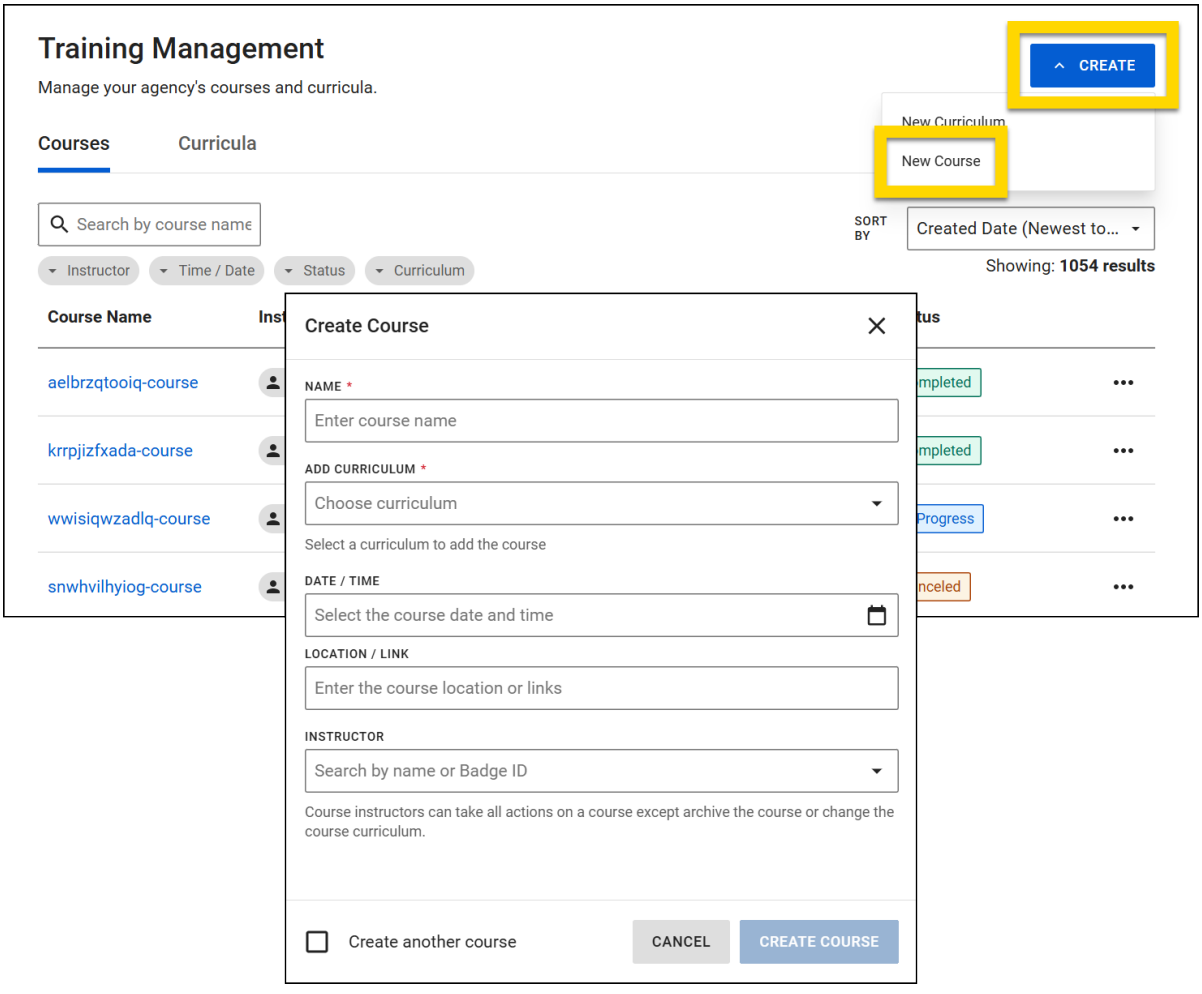
Create courses

To create a course, take these steps:

1. Open the Training module and select **Training Management**.
2. Select **Create > New Course**.
3. Enter all course details, including:

- **Name:** This course name will be shown to learners.
- **Curriculum**: The curriculum that the instructor will teach during the course.
- **Date/Time**: Specify the date and time for the course.
- **Location/Link**: Enter the location where the course will be conducted. If the training is an online instructor-led course, provide the video conference link (e.g., Zoom, Teams, etc.).
- **Instructor**: Assign an instructor from the list. Instructors can take all actions on a course except cancel the course or change the curriculum.

4. If you plan to immediately create another course after creating this one, select the **Create another course** checkbox.
5. Select **Create Course**.
6. Once a course is created, you can view it and update as necessary from the **Courses** tab.

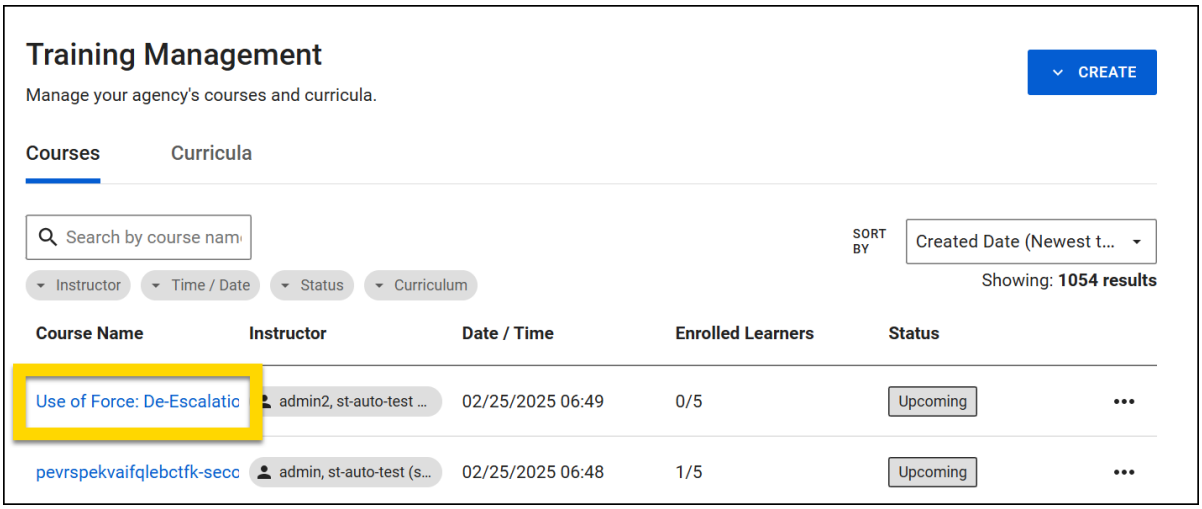


Watch this video for an overview of creating courses (starting at 06:18).

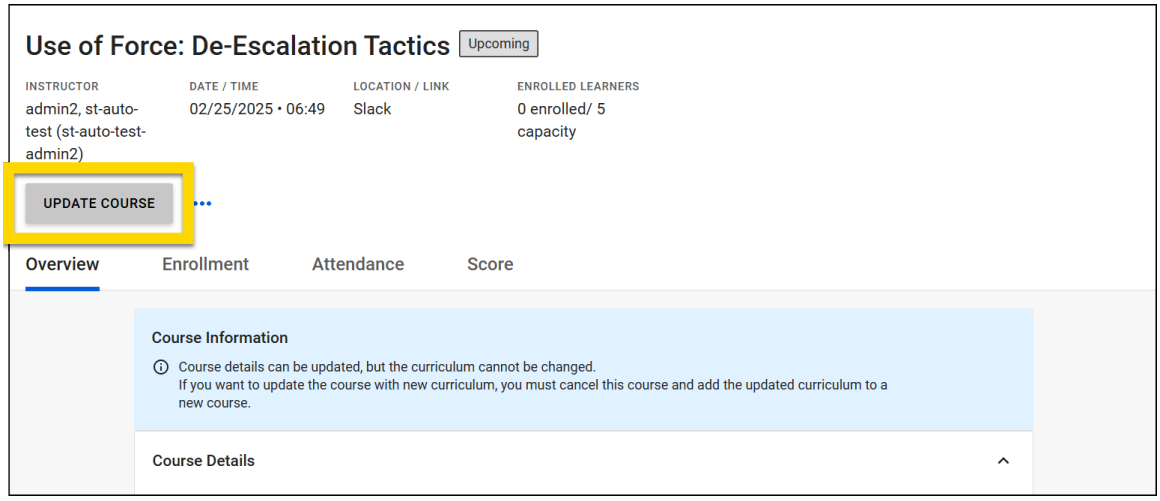
Update courses

To update an upcoming course, take these steps:

1. Open the Training module and select **Training Management**.
2. On the **Courses** tab, select a course name to open the course.



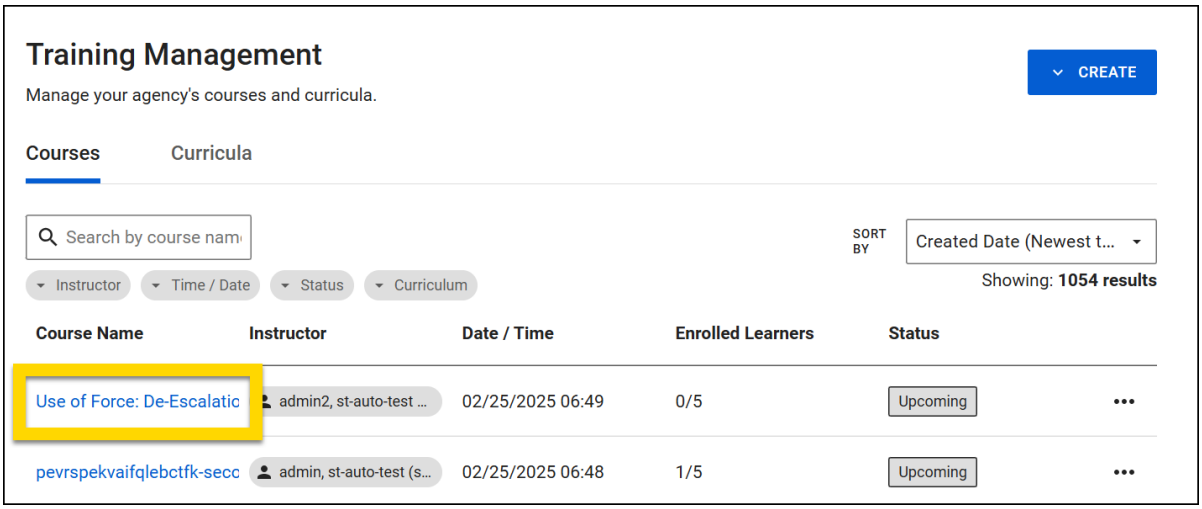
3. Select **Update Course**.
4. Update the course information as necessary, then select **Update Course** to save your changes.
   - You CANNOT change which curriculum has been added to the course. Instead, you must cancel the course, create a new course, and add the desired curriculum to that course.
   - If changes are made to a curriculum that has already been added to a course, those updates are NOT reflected in the course. If you want the updated curriculum to be used for the course, you must cancel the course, create a new course, and add the updated curriculum to that course.



Enroll learners in courses

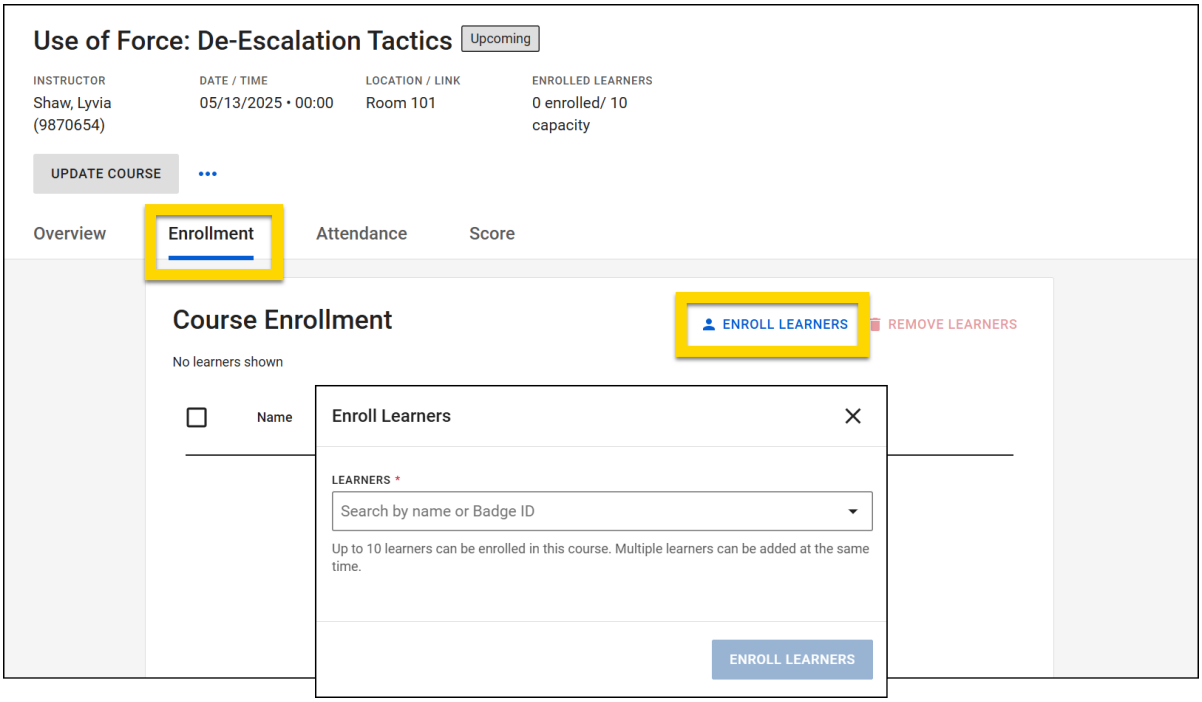
To enroll learners in a course, take these steps:

1. Open the Training module and select **Training Management**.
2. Select a course name to open the course.



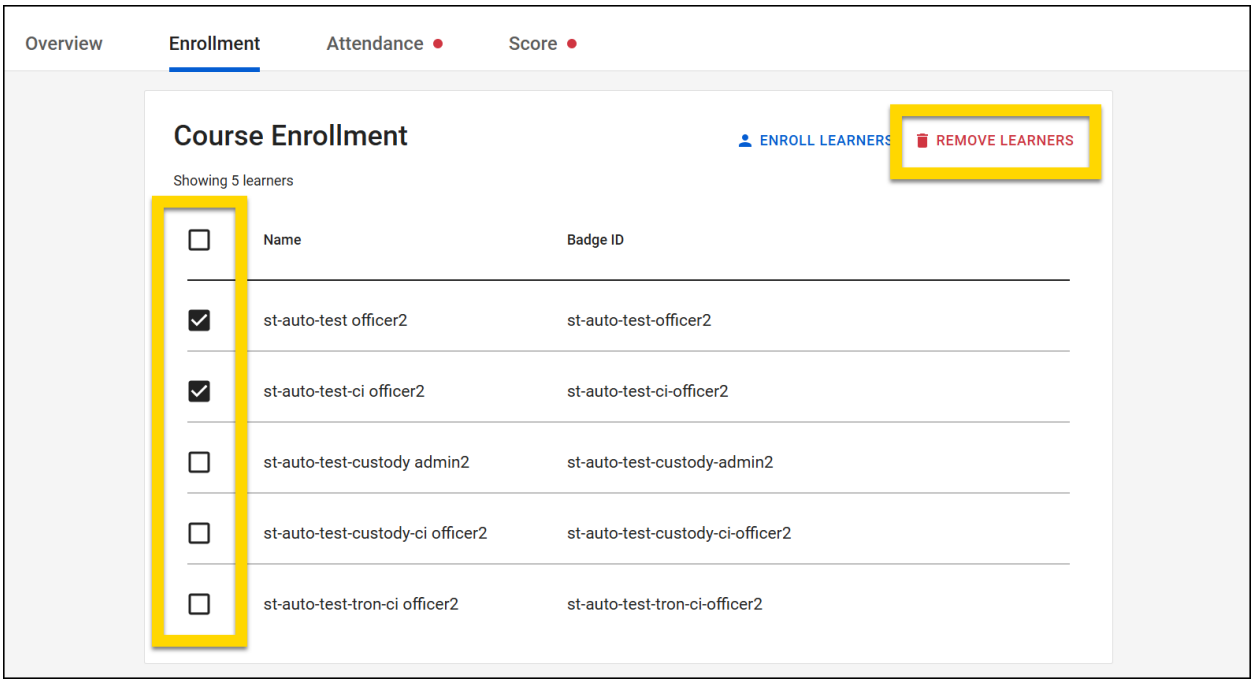
3. Open the **Enrollment** tab.
4. Select **Enroll Learners**.
5. Add one or more learners by searching for them in the **Learners** field.
   - If the course has limited capacity, the maximum number of learners is displayed below this field. This number updates as you add learners to the field, telling you how much space is left in the course.
   - A course capacity is determined by the curriculum that has been added to it.

6. After selecting the appropriate learners, select **Enroll Learners**.



Once a learner is enrolled in a course, the course appears on their My Courses page.

Remove learners from a course by selecting the checkbox beside their name then **Remove Learners**.



Watch this video for an overview of enrolling learners in a course (starting at 08:03).

Take attendance for courses

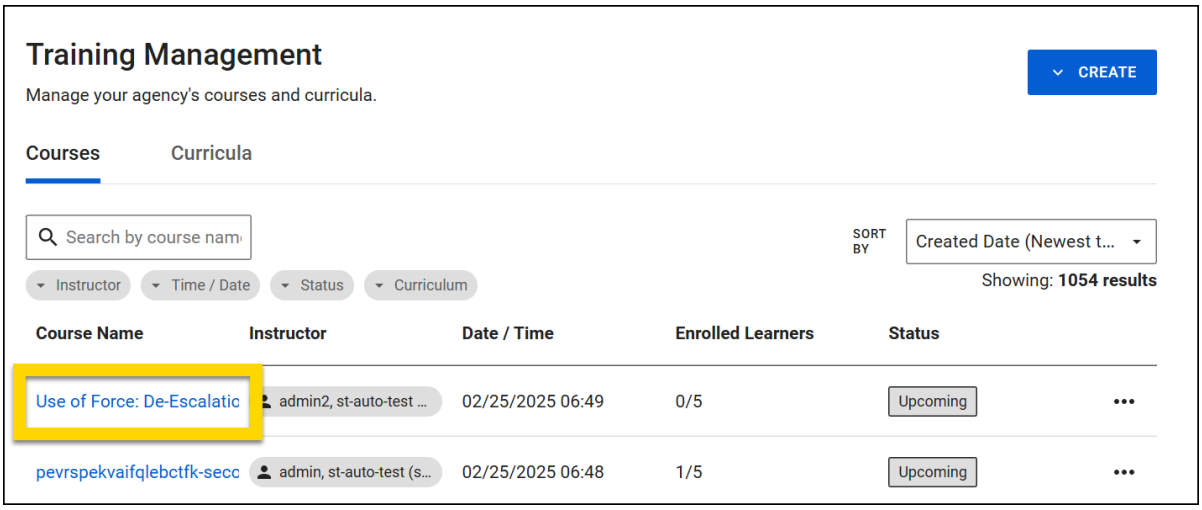
Once learners have been enrolled in a course, you can record attendance, indicating which users did and did not attend.

Note

Once you record attendance, you can no longer update the course details (date/time and instructors).

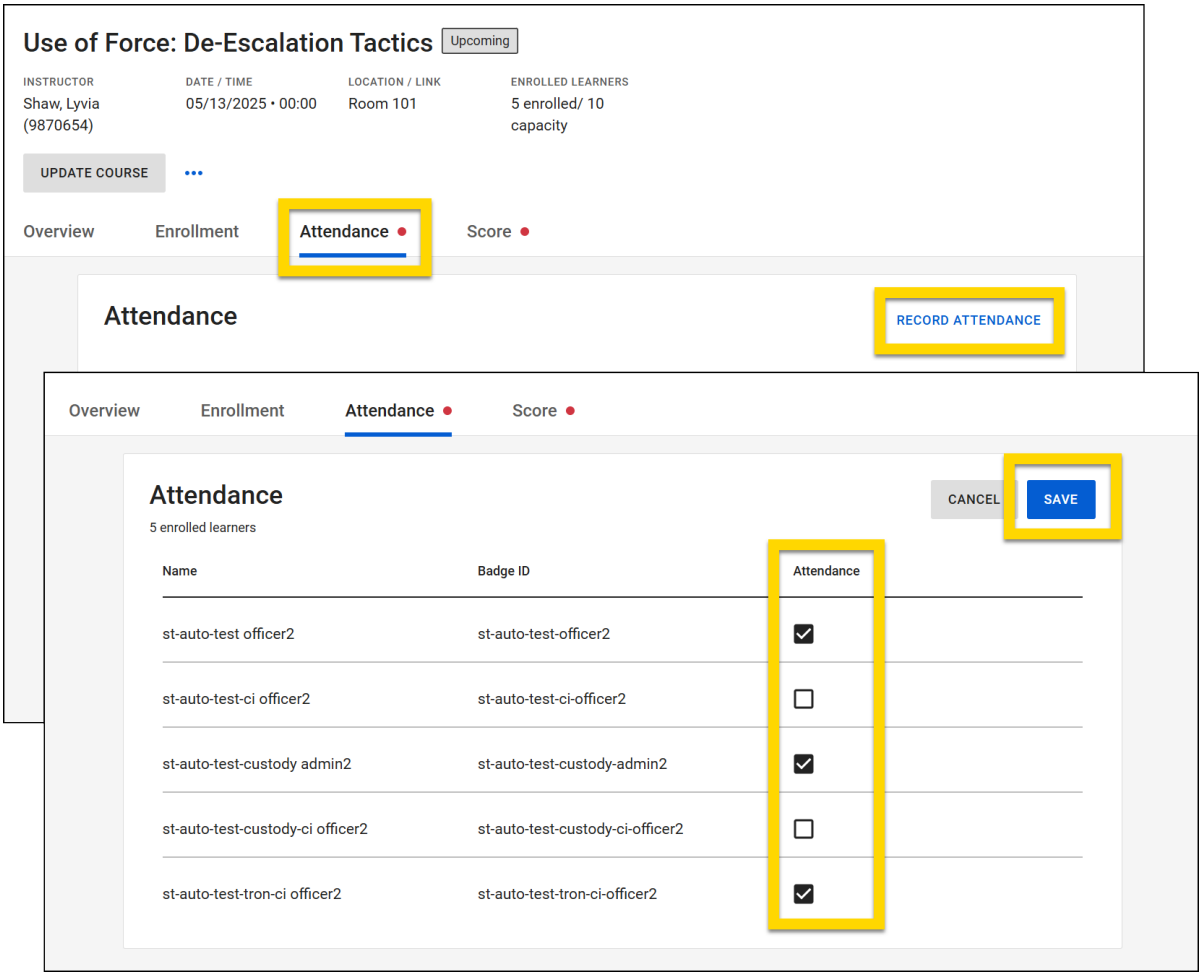
To take attendance for a course, follow these steps:

1. Open the Training module and select **Training Management**.
2. Select a course name to open the course.



3. Open the **Attendance** tab.
4. Select **Record Attendance** and confirm that you are ready to record attendance on the dialog box that appears.
5. A list of enrolled learners appears where you can select the checkboxes beside each learner in attendance to indicate whether or not they attended.

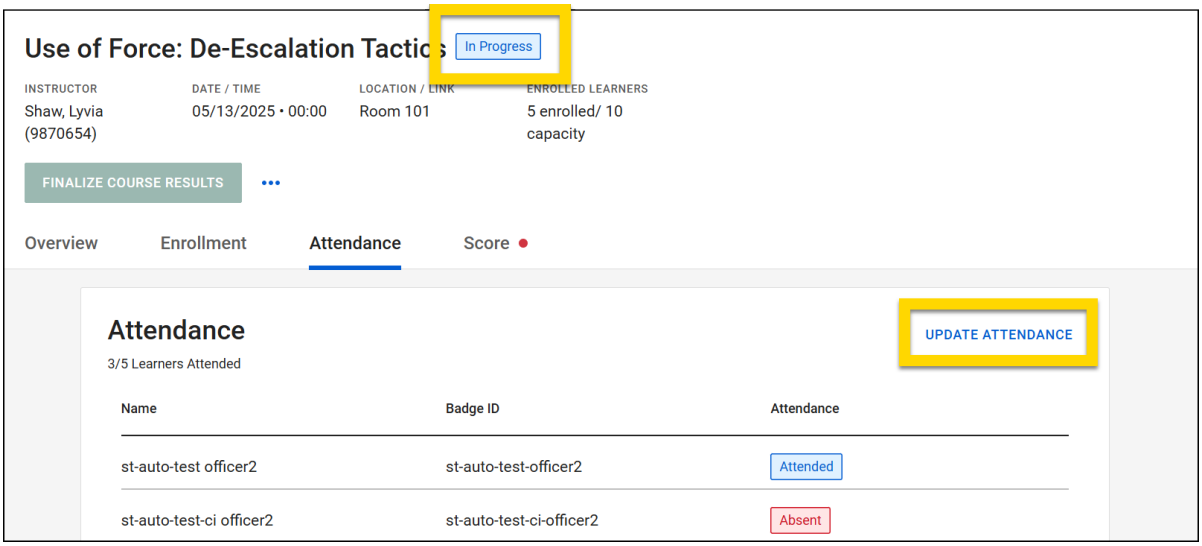
6. After making your selections, select **Save**.



Once you record attendance for a course, the course status changes from Upcoming to In Progress. To update attendance for a learner:

1. Select **Update Attendance**.
2. Deselect the box for any learners who were absent.

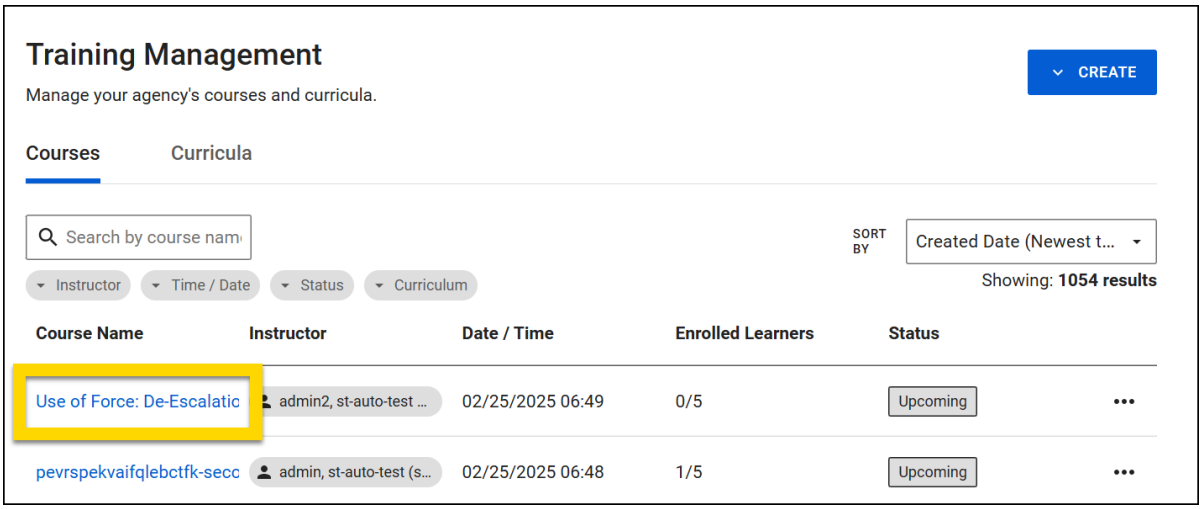
3. Select **Save**.



Record scores and finalize courses

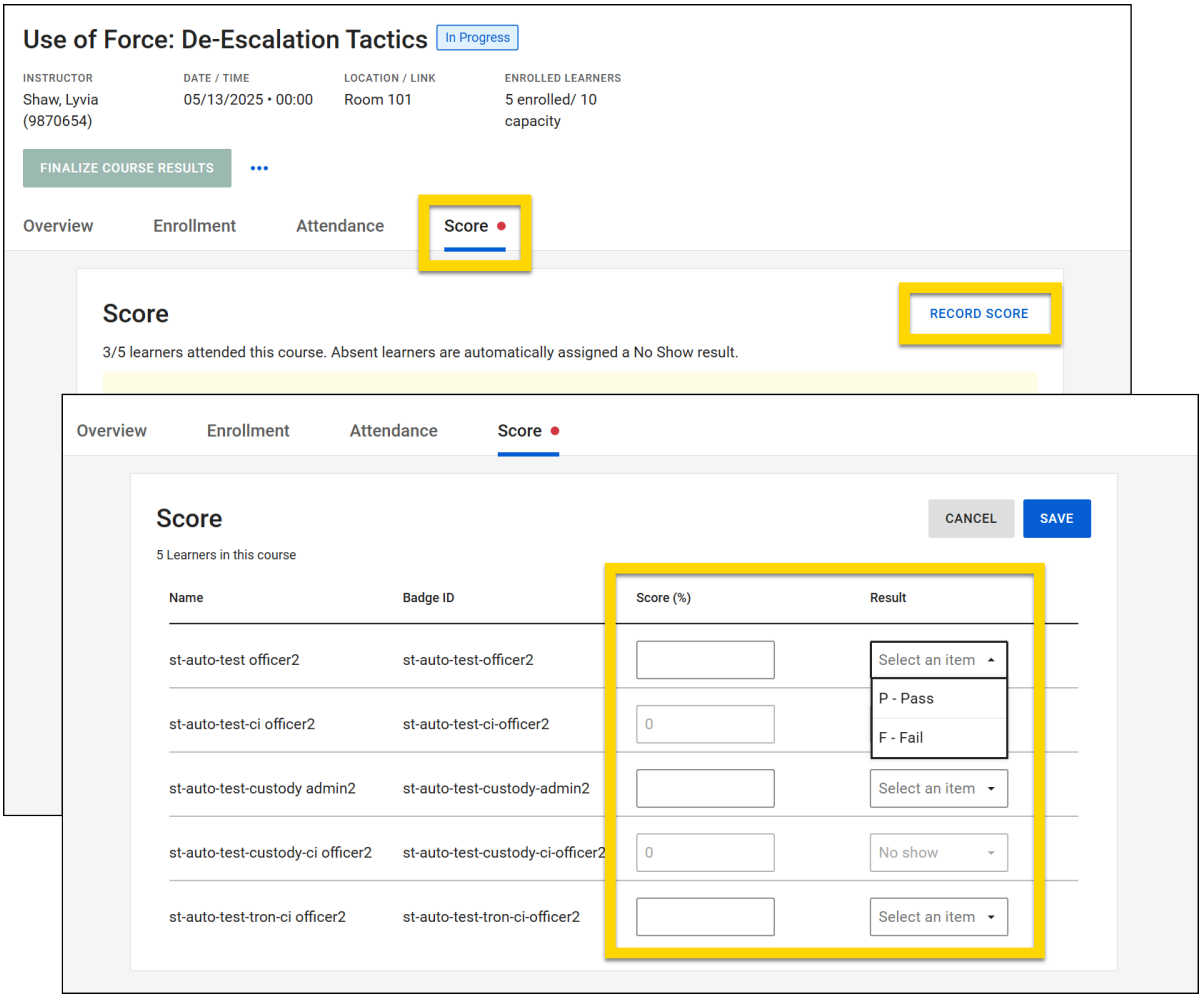
Scores for all learners must be entered before a course's results can be finalized. To record scores, take these steps:

1. Open the Training module and select **Training Management**.
2. Select a course name to open the course.



3. Open the **Score** tab.
4. Select **Record Score**.
5. Depending on the curriculum settings, you can enter a percentage score and a result (pass/fail) or just a result.
   - Scores can only be entered for learners who are marked as having attended the course.

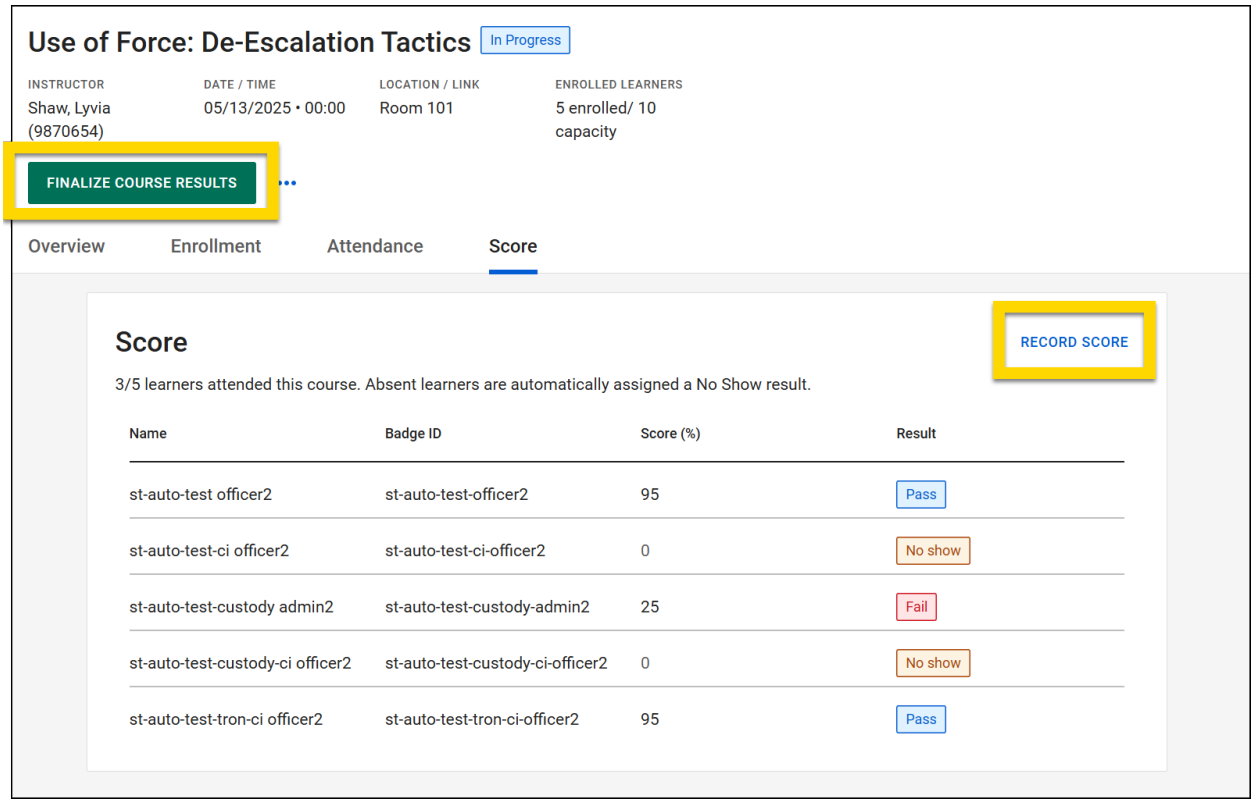
6. Select **Save** after you have entered all results.



Until the course is finalized, you can update learners scores by selecting **Record Score**. To finalize the course, select **Publish Course Result**.

Warning

Once a course is finalized, learner scores can no longer be changed.



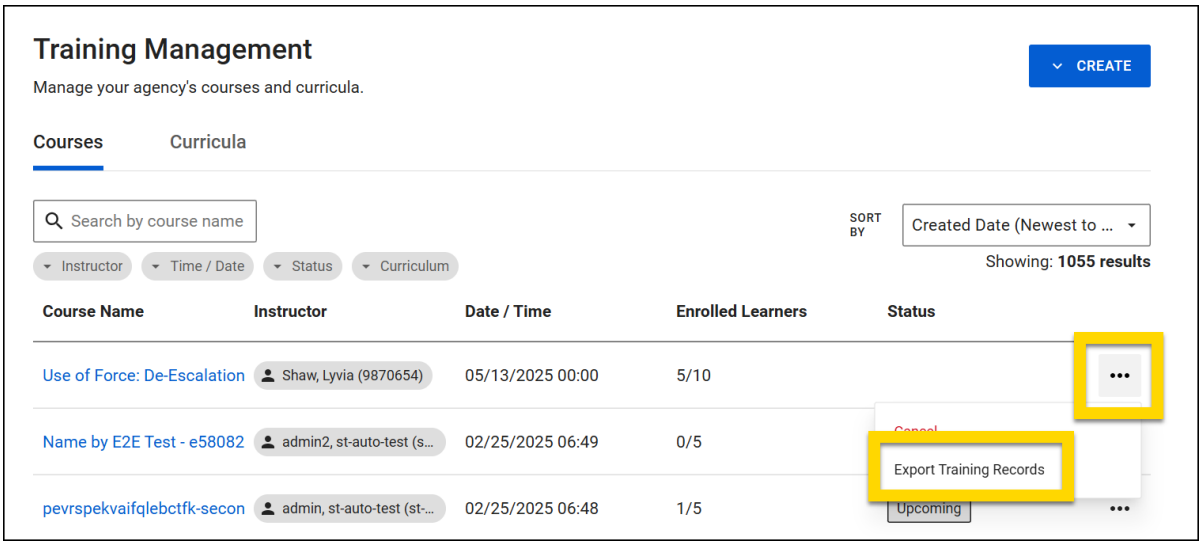
Export learning records

Learning Records can be exported for a course as soon as attendance has been taken. A learning record report is exported in CSV format and includes the following information:

- Course ID
- User name
- Badge number
- Attendance (Attended / Absent)
- Result (Pass / Fail)
- Score (percentage, where applicable)

To export learning records:

1. Open the Training module and select **Training Management**.
2. Select **More Actions > Export Learning Records** for the course from which you need records.



Cancel courses

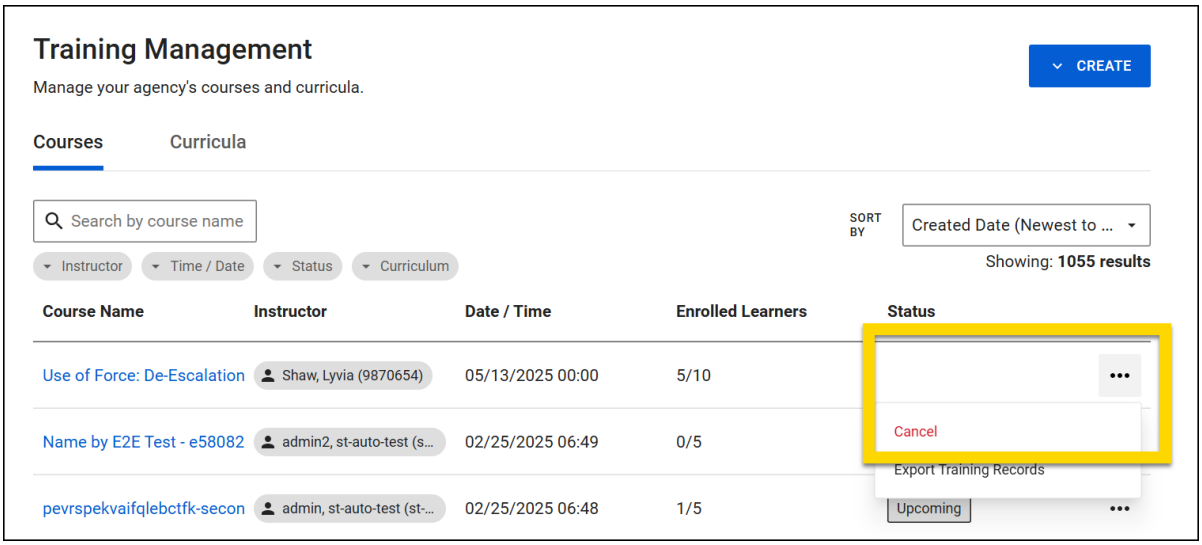
A course can be canceled any time up until the course is finalized. When a course is canceled, it still appears on a learner's My Courses page, but its status is displayed as Canceled.

Warning

Once a course is canceled, it can't be restored.

To cancel a course:

1. Open the Training module and select **Training Management**.
2. Select **More Actions > Cancel** on the course you want to cancel.



Notification Center



The Notification Center can be opened by selecting the bell icon in the main navigation menu. If you have unread notifications, a red number appears on the bell icon, indicating the number of unread notifications you have.

The Notification Center includes all notifications sent to you in the past 90 days. When you open the Notification Center, all unread notifications are marked with a blue dot. Use the All and Unread filters to switch between viewing all notifications or viewing only unread notifications.

To mark a notification as read, click anywhere on the notification, including expanding the details menu. To mark all notifications as read, select **Mark all as read**.

Some notifications contain a link to a report that you can open and take immediate action.

If your organization uses both Axon Records and Axon Standards, notifications for both products appear in the same Notification Center, whether you open it from Axon Records or Axon Standards.

Notification types

The notifications that appear in the Notification Center depend on your organization's configuration. Based on these configurations, the following notification types can appear in the Notification Center:

- Rejected reports
- Reports that have changed state
- Reports that require attention
- Shared reports
- Weekly team digest
- Warrant status updated

Administrator's note

Administrators can work with Axon Support to configure which notifications are sent to users and how often. For more information, see Rules and automations.

Rejected reports

When a report submitted for review is rejected, a rejection notification can appear in the report author's Notification Center, allowing them to quickly make the necessary updates and resubmit the report.

Reports that have changed state

Notifications can appear for tasks that are routed between users, resulting in a change to the report state. For example, a notification can inform you that your report was approved by a supervisor.

Reports that require attention

Notifications appear for reports that require attention because they are overdue or their due date is approaching.

Shared reports

When other users share reports with you, a notification appears in the Notification Center. This notification includes a link to the shared report, as well as the name of the user who shared the report with you. Expand the **Details** section to view the message the user created while sharing the report.

Weekly team digest

The Weekly team digest emails are sent to supervisors and contain a list of all reports assigned to a supervisor's direct reports that require attention. Additionally, all unassigned reports are included in this email. This notification can be configured to send to supervisors only of specific teams.

When the weekly team digest email is sent to supervisors, a notification also appears in the supervisor's Notification Center, alerting them that the email is ready for their review.

A supervisor's direct reports are determined based on your organization's Command Hierarchy. In the Command Hierarchy, users who belong to a direct child group of the supervisor’s group are considered that supervisor’s direct reports.

For more information, see Command Hierarchy.

Warrant status updated

When a warrant status is updated, a notification can appear in the Notification Center, allowing certain users to open the warrant and take action as necessary.

For more information about warrants, see Mange warrants.

Administrator Console

The Administrator Console, accessible by selecting the gear icon in the navigation menu, contains tools for managing Axon Standards.

Note

Users must have the Administrator Console privilege to access this tool. Some tools within the Admin Console require additional privileges.

When you open the Console, a list of tools is displayed alphabetically, with User Management as the default initial tool.

If your organization uses both Axon Records and Axon Standards, you may see additional tools in the Administrator Console. See the Axon Records user guide for Axon Records administrative tools.

Tools that impact both systems, like User Management, display data for both Axon Records and Axon Standards.

Analytics

The dashboards that appear in the Analytics module are managed from the Analytics tool. To access this tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Analytics** from the tool list.

Note

Users must have the Analytics Dashboard Management privileges to manage dashboards from this tool.

Databases and datasets

The databases that have been configured for your organization appear at the top of the page in the **Database configuration** section. Expand this section to view and copy the database and server names for use in SQL queries.

The number of datasets that have been used by your organization's Axon Records and Axon Standards dashboards are displayed beside the Database Configuration section. This information lets you know if you can add additional dashboards using new datasets.

Dashboard list

The main portion of the Analytics tool is the list of dashboards that have been created for your organization. Use the filters above the table to adjust which dashboards appear in the list. Select a column heading to sort the table according to that column. In the table, the following information is included for each dashboard:

- **Name:** The name of the dashboard that is shown in the Analytics module.
  - If this name is updated, the associated privilege name will update to match.
- **ID:** The Axon Records or Axon Standards ID used to identify the dashboard
- **ID (from PBE):** The PowerBI ID used to identify the dashboard
- **Service type:** If the dashboard is for Axon Records or Axon Standards
- **Dashboard's type:** Standalone, Template, or User. See Dashboard types for more information
- **Hide from users:** When this toggle is turned on, the dashboard is hidden from the Analytics module. Even if a user has the privilege to view it, they will not be able to.
- **Editable:** If a dashboard is editable, users can edit it from the Analytics module.
- **Publishing status:** The status of dashboards uploaded by Axon representatives.
  - The publishing status for User dashboards is **Not applicable**.
  - Hover over the **Failed** status to see the failure details.
- **Current refresh status:** The most recently reported refresh status from PowerBI and the date/time of the last refresh.
  - Statuses include Ready, Refreshing, Completed, Failed, Disabled, and Unknown (a dashboard was recently uploaded and not refreshed yet, a refresh is in progress, an odd condition occurred).
  - If a refresh has failed, hover over the information in this column to view additional details about the failure.
  - If a dashboard's refresh status is Completed, but a long time has passed since its last refresh, there may be a problem with the dashboard's refresh schedule. If this occurs, contact your Axon representative.
- **Action:** Options include:
  - **Delete dashboard:** Permanently deletes the dashboard.
  - **Download dashboard:** Lets you download the dashboard's PBIX file.
  - **Download query:** Lets you download the SQL query file for that dashboard.
    - You can download either the current dashboard query or a previous version (from the five most recent previous versions).
  - **Download refresh schedule:** Lets you download the refresh schedule for that dashboard. To update the refresh schedule, edit the dashboard.
  - **Download localization file:** Lets you download the localization file that contains the localized tab names for that dashboard.

- **Refresh dataset:** Lets you manually refresh the dataset.
  - This manual refresh can only take place if the dashboard status is in no status, Completed, or Railed. If the dashboard status is in Ready or Refreshing, the dataset cannot be manually refreshed.
- **Copy dashboard privileges:** Lets you copy the privileges for another dashboard to that dashboard. See Copy dashboard privileges for more information.
  - For example, allow all users who can view the Crimes dashboard to also view the Arrests dashboard.

Dashboard Types

There are three types of Axon dashboards that can be managed by Analytics users: Standalone, Template, and User. Privileges determine which dashboard types a user can manage.

Standalone

Standalone dashboards are PBIX files that are uploaded to the Analytics tool in the Administrator Console by Axon representatives. Axon Analytics comes with a set of out of the box dashboards.

Agency administrators can set whether these dashboards can be edited. If they can be edited, this is done from within the Analytics module, while the user is viewing the dashboard. These standalone dashboards can be deleted from the Analytics tool in the Administrator Console.

Template

Like Standalone dashboards, Template dashboards are uploaded to the Analytics tool in the Administrator Console by Axon representatives. However, unlike Standalone dashboards, Template dashboards can't be edited. Instead, they can be copied, to serve as a starting point for User dashboards.

For more information about building PowerBI dashboards that use data from the Axon DataStore, see Analytics and Power BI.

Like Standalone dashboards, Template dashboards are edited from the Analytics module and deleted from the Analytics tool in the Administrator Console.

A Template dashboard can only be deleted once all User dashboards that were created from it are also deleted.

User

Unlike Standalone and Template dashboards, User dashboards are edited, archived, and deleted from within the Analytics module, not the Analytics tool in the Administrator Console.

Each User dashboard is associated with a set of privileges. You must open the Administrator Console and grant privileges to the Command Hierarchy groups or teams who need to access to these dashboards.

Edit dashboards

To edit a Standalone or Template dashboard, take these steps:

1. Open the Analytics tool in the Administrator Console.
2. Select the blue dashboard name in the **Name** column.
3. Update necessary field(s).
   - If the name is updated, the associated privilege name will update to match.
   - Change whether the dashboard is editable by users or not.
4. Select **PBIX file** to replace the current dashboard file with a new one.
   a. All privileges associated with the dashboard remain unchanged.
5. Select **Refresh schedule** to upload a JSON file that outlines how often the dashboard should refresh (pull data from the DataStore and display it on the dashboard).
   - Download this example JSON file and update the days and times for the dashboard.
   - Refreshes generally should occur every few hours, although they can occur more or less frequently. The smallest refresh interval allowed is once per hour.
   - If your organization has multiple dashboards, it's helpful to stagger the refresh schedule for each dashboard to prevent refresh errors and delays. For example:
     - Dashboard A: Refreshes every three hours, on the 15-minute mark (1:15, 4:15, 7:15, etc.)
     - Dashboard B: Refreshes every four hours, on the 30-minute mark (1:30, 5:30, 9:30, etc.)
6. Select **Confirm**.

Add dashboards

Users with the appropriate permissions can upload a Power BI dashboard to the Analytics tool as long as they have not already reached their dataset limit. This limit is displayed in

the top corner of the Analytics tool. If you want to create a dashboard but have already reached your dataset limit, you must delete all dashboards associated with a dataset to free up space.

Note

The only dashboards that can be uploaded are those that connect to the Axon DataStore. Dashboards connected to other data sources are not supported.

To add a dashboard:

1. Open the Analytics tool in the Administrator Console.
2. Select **Add dashboard** at the top of the page.
3. Select a **Service type** (Records or Standards).
4. Select a **Dashboard type** (Standalone or Template).
5. Enter a name for the dashboard.
   - This name appears in the Analytics module, as well as in Analytics privileges.
6. Set whether or not the dashboard can be edited by users who access the dashboard in the Analytics module.
7. Optionally provide a datasource or dataset.
8. Optionally search for and copy the privileges for an exisisting dashboard.
   - This option allows all users who can access the existing dashboard also access this new dashboard.
   - See Copy dashboard privileges for more information.
9. In the Dashboard files section, upload a PBIX file to add the dashboard files from your computer.
   - See the error list for potential errors you may receive and the steps that can be taken to resolve them.
10. In the Other files section, upload a Refresh schedule (a JSON file that outlines how often the dashboard should pull data from the DataStore and display it on the dashboard).
    - Download this example JSON file and update the days and times for the dashboard.
    - Refreshes generally should occur every few hours, although they can occur more or less frequently. The smallest refresh interval allowed is once per hour.

- If your organization has multiple dashboards, it's helpful to stagger the refresh schedule for each dashboard to prevent refresh errors and delays. For example:
  - Dashboard A: Refreshes every three hours, on the 15-minute mark (1:15, 4:15, 7:15, etc.)
  - Dashboard B: Refreshes every four hours, on the 30-minute mark (1:30, 5:30, 9:30, etc.)

11. In the Other files section, upload a Dashboard localization file (a file which contains localized tab names).
12. Select **Confirm**.

Dashboard errors

You may receive one or more of the following errors when uploading a dashboard:

Error	Resolution
Table Partition mode must be import This error indicates that the dashboard uses direct query, or any other import mode for a table in the data model other than import.	Ensure the tables only use import mode.
Source expression must contain SELECT statement with defined columns or Table.SelectColumns This error indicates that one or more queries in the dataset do not specify columns.	Remove any `select *` type operations. Ensure all queries are objective.
Source column must not contain raw data One or more queries in the dataset includes a raw data column, which tends to be too slow and cause problems during data refreshes.	Remove any raw data columns. These columns typically can be identified by a `_raw_data` suffix.
Themes do not match **Number of sections do not match** **Section names do not match** **Section display names do not match** **Number of visual containers do not match** **Queries do not match**	These errors indicate a mismatch between the PBIX and PBIT files, which may indicate that the files are not the same, or that they were saved/exported at different times. To resolve these issues, re-save the PBIX file and re-export the Power BI template (PBIT) file. See the Power BI help documentation for more information.

Copy dashboard privileges

Every Analytics dashboard has a corresponding View privilege that can be granted to Command Hierarchy Groups and teams. All users in those Groups and teams can then access the dashboard from the Analytics module.

You can copy the privileges for one dashboard to for another dashboard to ensure that the same set of users can access both dashboards. For example, you can allow all users who can view the Crimes dashboard to also view the Arrests dashboard.

You can use this Copy feature to update the privileges for existing dashboards, as well as when adding new dashboards.

To update the privileges for an existing dashboard:

1. Locate the dashboard in the list.
2. Select **More actions [...] > Copy dashboard privileges**.
3. In the Copy dashboard privileges window, search for the dashboard whose privileges you want to copy.
4. Select **Confirm**.
   - Users who currently have access to the dashboard will keep their access, even if they do not have access to the other dashboard you are copy the privileges from.

Data dictionary

To see a full list of the tables and fields in your organization's DataStore, download the data dictionary:

1. Open the Analytics tool in the Administrator Console.
2. In the top right corner of the screen, select **More actions [...] > View data dictionary**.
3. Select **Export** in the confirmation window to download the data dictionary as a CSV file.

Export and download dashboards

You can export dashboards individually or in bulk.

To export a single dashboard:

1. Find the dashboard in the table and select **More actions [...] > Download** dashboard. This downloads the PBIX file for that dashboard.
2. Select **More actions [...] > Download query**. This downloads the SQL query file for that dashboard.

To export all dashboards in a single zip file:

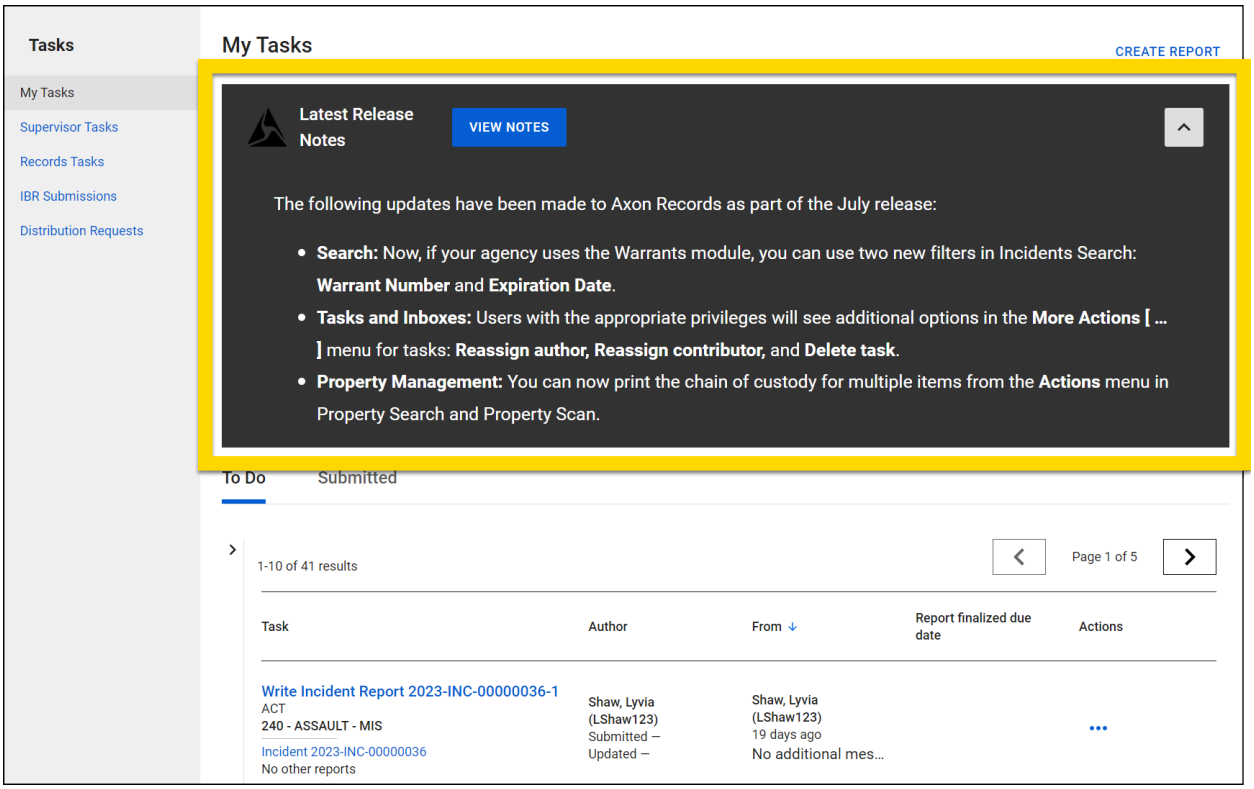
1. Open the Analytics tool in the Administrator Console.
2. In the top right corner of the screen, select **More actions [...] > Bulk export**.
3. Select **Start export** in the confirmation windowthat appears.
4. After your dashboards are analyzed, a new window appears indicating how many dashboards will be included inthe zip file. Select **Download zip**.
5. The zip file contains one folder per dashboard. Each folder contains the PBIT and SQL query file for that dashboard.

Note

Only dashboards with a pre-generated PBIT file are included in the zip file. Any dashboards still in the process of uploading are not included.

Announcement Banner Update

Using the Announcement Banner Update tool, you can customize the content of the announcements banner that appears at the top of the My Tasks inbox.



To access this tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Announcements Banner Update** from the tool list.

Note

Users must have the Announcement Banner privilege to access this tool and update the Announcement banner.

To update the banner:

1. Open the Announcements Banner Update tool in the Administrator Console.
2. Select **Clear existing banner** to delete all existing content.
3. Update the various banner fields:
   a. **Banner header:** Appears at the top of the banner
   b. **Action button text:** The text that appears on the blue banner button.
   c. **Action button URL:** The URL users will be taken to if they click the blue banner button.

      Warning

      To maintain the security, do not enter links here that are not owned by your agency or Axon.

   d. **Text field:** The main text of the banner. Use the top toolbar to format text into headings and bulleted/numbered lists.
4. Switch to the **Preview changes** tab to preview your new content.
5. Select **Publish new banner** to make the content visible to your users.

The logo that appears in the top left corner of the banner can be managed from your Agency Profile in the Axon Evidence Admin panel.

Audit Log Tool

The Audit Log Tool lets you search, filter, and export a record of actions taken on reports, cases, incidents, and other items in Axon Records and Axon Standards. If your organization is configured for both products, the Audit Log Tool shows actions taken in both products. You can open the tool from either the Axon Records or Axon Standards Administrator Console.

To access the Audit Log Tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Audit Log Tool** from the tool list.

Note

Users must have the Audit Log privilege to access this tool and view audit logs.

Generate audit logs

To generate an audit log, take these steps:

1. Open the Administrator Console and select **Audit Log Tool**.
2. Enter a date range in the **Date range** filter.
   - You can search a single day or a range of up to one year.
3. Set at least one additional filter. You can't generate an audit log using a date range alone:
   - **Actors**: Filter by one or more users whose actions you want to audit.
     - Search for a user by name, username, or badge ID, then select **Apply**. Repeat to add more actors.
   - **Targets**: Filter by one or more target types. Options include Report, Case, Investigation, Event, Standards Case, Incident, Location, Person, Property, Vehicle, User, Analytics, and Privilege.
     - After selecting a target type, enter a specific ID for that item (e.g., Report ID), and select **Apply**. Repeat to add more targets.
   - **Event types**: Filter by one or more event types.
   - **Audit types**: Search by one or more audit types. Options include:
     - Print: The audit log includes all print-related events (printing of activity logs, reports, profiles, etc.).
     - Datastore Access Control: The audit log includes all events related to DataStore settings and access control.
   - After setting at least two filters, you can select **Reset** to remove all filters.
4. Once your filters are set, choose one of the following:
   - **Search**: Run your query and display the results in the tool. You can export results after the preview.
   - **Export CSV/PDF**: Export your results without previewing them first.
5. If your filters include too many results to be displayed or exported, an error displays. Add additional filters or shorten your date range to reduce the number of results and select **Search** or **Export** again.

Audit log columns

The columns included in the Audit Log Tool preview and in audit log CSV exports include:

- **Event**: The event that occurred
- **ID**: The ID generated for the event
- **Occurred on**: The date and time the event occurred, including hundredths of a second
- **Source**: Whether the event originated in Axon Records, Axon Standards, or an integrated source
- **IP address**: The IP address of the actor who performed the action
- **Device name**: The browser and operating system associated with the action
  - Because Axon Records and Axon Standards are browser based, this reflects browser and OS information rather than physical device information.
- **Actors**: The user or integration that performed the action
- **Details**: Additional information about the event
  - Details vary depending on the event type.
- **Targets**: The item type the action was taken on

Audit log PDF exports include fewer columns with the above information combined in the columns as follows:

- Occurred on
- Activity: Includes Details, IP address, and device name
- Targets

Multi-target events

Some actions affect more than one target at once. For example, when you add a person to a report, an event is logged both for the person and the report. As a result, the event appears when you generate an audit log for the report and the person.

Open and View events

The audit log distinguishes between when a user views a document, a Records incident, or a Standards event in search results or in a task inbox and when they actually open the item. View events indicate that the item was viewed in a list. Open events indicate the item was actually opened and its full contents were accessed. The search keywords the user entered are also included in the log. For example, the following audit log entries indicate that the user:

1. Ran a search for "202607".
2. Viewed a list of 3 incidents in the search results
3. Opened incident ID 20260715 but did not open any of the other incidents.

Event	Details
Search Incidents	Shaw, Lyvia (LShaw001) searched Records incidents. Keyword: "202607". Results: 3
View Incident	Shaw, Lyvia (LShaw001) viewed Incident ID 20260715
View Incident	Shaw, Lyvia (LShaw001) viewed Incident ID 20260714
View Incident	Shaw, Lyvia (LShaw001) viewed Incident ID 20260713
Open Incident	Shaw, Lyvia (LShaw001) opened Incident ID 20260715

Axon Records integration View events

The audit log includes automated retrievals of documents. These events appear in the log as "Axon Records Integrations viewed Document ID". These events do NOT indicate that a human viewed the listed document. Instead, this event can be triggered by integrations with third-party systems, or other automated retrievals.

Common causes of this event include:

- Call for Service (CFS) re-import / CAD lookback: This is one of the most common reasons the Integrations Viewed event occurs.
- Report import duplication checks
- NIBRS / IBR submission
- Adding supplements
- Adding evidence to a report
- Query incident: For example, as a result of an integration with a crash reporting system, an incident is searched for in Axon Records so information from the external system can be attached to it.

The name shown in the audit log may vary depending on the integration or system that triggered it (e.g., Axon Records, AxonDataPlatform, etc.). You can check the list of integrations that have been created for your organization by logging in to Axon Evidence and selecting Admin in the main navigation menu. In the **Organization settings** section, select **Integrations** and switch to the **API clients** tab. Look in the Client name column for the name that matches the name listed in the audit log.

Command Hierarchy Groups and teams

Your organization's Axon Evidence Command Hierarchy syncs with Axon Records and Axon Standards and is viewable in the Command Hierarchy & Teams tool in the Administrator Console. Any changes made to your Axon Evidence Command Hierarchy

automatically reflect in Axon Records and Axon Standards, including when users are moved between groups due to reassignment or promotion.

To access the Command Hierarchy & Teams tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Command Hierarchy & Teams**.

Note

Users must have the Command Hierarchy and Teams to access this tool and manage Command Hierarchy Groups and teams.

Administrators in Axon Records and Axon Standards can create teams, manage team membership, and grant privileges to Command Hierarchy groups and teams. Any changes to squads or creation of new elements in your Command Hierarchy must be made in Axon Evidence.

For information about managing your agency's Command Hierarchy in Axon Evidence, see the Axon Evidence User Guide.

If your organization is configured for both Axon Records and Axon Standards, all teams created for both Axon Records and Axon Standards appear in the Command Hierarchy & Teams tool, whether it is opened from Axon Records or Axon Standards.

Manage Command Hierarchy Groups

To access your agency's Command Hierarchy, select **Command Hierarchy & Teams** in the Administrator Console.

Select **Edit Hierarchy** above the list of groups to open Axon Evidence in a new browser tab where you can manage the structure of your agency's command hierarchy and add groups. A step-by-step guide for updating and managing your Command Hierarchy can be found here.

To adjust which users belong a group, open the group then select the **Ecom admin** link in the gray bar at the top of the screen to open the Axon Evidence Admin Console and make changes. A step-by-step guide for managing Command Hierarchy group membership can be found here.

Manage teams

You can manage your Axon Records and Axon Standards users by using teams instead of or in addition to Command Hierarchy groups. To access Axon Records and Axon Standards teams, open the Command Hierarchy & Teams tool and switch to the **Teams** tab. All teams that have been created for your agency appear on this tab.

Select a team name to view all users who have been added to that team and the privileges that have been set for the team.

Select **Actions** to reveal various team-related options:

- Create new team
- Add team members
- Export/import all team privileges
- Export team membership
- Synchronize Team Membership

Create teams

To create a new team:

1. Open the Command Hierarchy & Teams tool.
2. Select **Actions > Create new team**.
3. Name the team and make sure the **Users** option is selected.
4. Select **Create team**.

Manage team membership

To manage which users belong to a team, go to **Administrator Console > Command Hierarchy & Teams > Teams** tab. Scroll through the list or find a team using the search box. Select a team name to open the **Member view** tab to see a list of all team members.

To manage users, you can:

- Add users to a team by entering a list of badge numbers, usernames, or emails separated by commas in the **Add members in bulk** field.
- Select **Replace all** to replace all current team members with the users entered in the **Add members in bulk** field.
  - The **Add members in bulk** field is case-sensitive, so be sure to use the correct capitalization when entering usernames.
- Remove a user from a team, by selecting the **X** beside their name.

Open the **Actions** menu to find additional management options:

- Export Users to CSV
  - The file includes each users first name, last name, username, and badge number.
- Export/Import privileges to JSON
- Delete Team
  - The ADMIN team cannot be deleted

Manage membership using CSV import

Rather than managing membership team by team, you can manage membership for all teams at the same time using CSV import and export. To do this, take these steps:

1. Open the **Teams** tool in the Administrator Console.
2. Select the **Teams** tab.
3. Select **Actions > Export team membership**.
4. Open the CSV file that downloads to your computer and add, move, and remove team members. Each row in the CSV file is equal to one user's membership in a team. If a user belongs to multiple teams, the CSV file will contain multiple rows for that user. The columns for each user include:
   - External_ID: The unique identifier for that team
   - Name: The team name
   - Membership_Type: This column can remain blank
   - Entity_Type: This column should be filled out with "user" for every row.
   - Entity_ID: The user's email address
5. After making necessary changes, save the file and return to the Teams tool. Select one of the two options from the **Actions** menu:
   - **Add team members:** Select this option if you are only adding users to teams.
   - **Synchronize team membership:** Select this option if you are adding, removing, or moving team members.
6. Select the file from your computer and upload the file you saved.

CSV Tips

- Create all teams before exporting team membership. New teams can't be created using CSV import.
- Add at least one team member to each team manually before exporting the team membership file. This ensures that the External ID is included for every team.
- Use caution when selecting the **Synchronize team membership** option, because the file you upload will change the membership of all members in all of the agency's teams.

District

Use the District tool in the Administrator Console to manage your organization's districts.



To access the District tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **District** from the tool list.

Note

Users must have the Districts to access this tool and manage districts.

If your organization is configured for both Axon Records and Axon Standards, you will see all districts created for both Axon Records and Axon Standards in the District tool.

To create a district:

1. Open the Administrator Console and select **District**.
2. Select **Add row** at the bottom of the list.
   - If your agency has a large number of districts, you may need to scroll down on the page.
3. Enter a district name and shortcode.
4. Select the **Default** checkbox if you want this district to be the default district assigned to users who are added to Axon Records or Axon Standards.
5. Adjust the **Active** switch if needed.
   - If a district is set to *Inactive*, it will be hidden from the **Routing options** menu when users route a report for review.
6. Select **Save**.

See User management for instructions on changing which district a user belongs to.

To edit a district name, select the name in the **Attribute** column. District shortcodes are NOT editable, and you cannot delete a district.

Early Intervention System (EIS) Management

The EIS Management tool in the Administrator Console lets administrators create and manage the organization's alert policies and custom metrics.



To access the EIS Management tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **EIS Management** from the tool list.

Policies outline an acceptable threshold for each type of event (i.e., how many times an officer can be involved in each type of event). When officers cross that threshold, their supervisors receive an alert via email. Alerts and the subsequent actions taken after an alert is created are managed from the alert inboxes in the Early Intervention System module.

The EIS Management tool has two tabs:

- **Alert policies:** Lists all policies that have been created by your organization.
  - Alert policies can be based on reports or fields within reports (i.e., custom metrics).

- **Custom metrics:** Lists all custom metrics that have been created by your organization.
  - Custom metrics are defined from specific fields within reports. Metrics can be added to alert policies, which determine when EIS alerts are sent.

Alert policies

To manage your organization's Early Intervention System alert policies, open the EIS Management tool in the Administrator Console. When opened, this tool displays the **Alert Policies** tab, which lists all policies that have been created for your agency. Each policy displays the following information:

- **Name:** The policy identifier or name
- **Metric:** What is being counted and tracked in the policy (e.g., how many vehicle pursuits an officer is involved in)
- **Tracked group:** Which individuals, Command Hierarchy groups, and/or teams are tracked by the policy
- **Triggering threshold:** How many times an officer is involved in that type of event before an alert is triggered; policies can have both Warning (lower) and Critical (higher) thresholds
- **Period:** The metric timeframe (e.g., 90 days)

For example, your agency might have a policy related to use of force events:

- A Warning alert is triggered if an officer is involved in 1 or more use of force events within 90 days
- A Critical alert is triggered if an officer is involved in 4 or more use of force events within 90 days

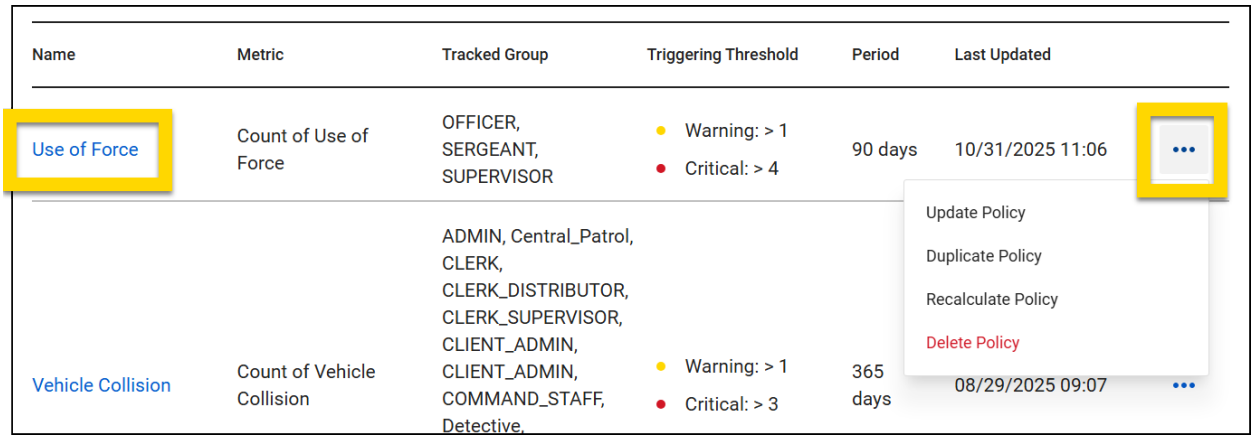
This policy would appear as:

Name	Metric	Tracked Group	Triggering Threshold	Period	Last Updated	
Use of Force	Count of Use of Force	OFFICER, SERGEANT, SUPERVISOR	Warning: > 1 Critical: > 4	90 days	10/31/2025 11:06	•••

Select a policy name in the Name column to open a read-only view of the policy where you can see all details. Select **More actions [...]** in any of the policy rows to:

- **Update policy:** Change the start date, tracked users, and alert destinations for an existing policy and recalculate to send new alerts as required.
- **Duplicate policy:** Duplicate an existing policy to use as a starting point rather than creating a brand-new one and edit it as necessary before publishing.
- **Recalculate policy:** Change the start date of an existing policy and recalculate to send new alerts as required.

- **Delete policy:** Deleting a policy will NOT delete any alerts that have already been sent as a result of that policy.



Create policies

To create a new policy, select **Create alert policy** and complete all the fields on each of the four subsequent screens:

- Alert details: Add the alert details, including name, metrics, time period, and thresholds.
- Tracked officers: Set which users, command hierarchy groups, and teams should be tracked by the policy.
- Alert destinations: Indicate which users, command hierarchy groups, and teams should receive alerts if a policy is triggered.
- Review and publish: Review the policy and publish.

As soon as you publish, the policy will appear in the list of policies on the **Alert Polices** tab and begin tracking reports, according to the dates specified on the Alert details page.

Alert details

Name

This first section of the Alert details page asks you to enter a policy name. This can't be the same as any other policy name currently in the system.

Assign metrics to the policy

This section lets you indicate which metrics the policy tracks and how occurrences are calculated. Policies can monitor one or more metrics. When a policy contains multiple metrics, alerts can be sent when the total value of all metrics meet the thresholds OR only if each metric meets the thresholds.

First, select an option in the **Multiple metric configuration** field:

- **Single metric:** The policy contains a single metric. An alert is sent when the thresholds are met for this single metric.
- **Multiple metrics - Total value:** The policy contains multiple metrics. An alert is sent when the thresholds are met for the total value of all metrics.
- **Multiple metrics - All conditions true:** The policy contains multiple metrics. An alert is sent only if every metric in the policy meets the thresholds. All metrics must be associated with the same report type.

Depending on your selection in the **Multiple metric configuration** field, you can add one or multiple metrics to the **Metric** field. You can choose either default or custom metrics:

 Default metrics: Appear at the top of the list and are indicated by a form icon

- If a default metric is added to the policy, an alert is sent if that type of report is created more times than allowed by the policy thresholds during the policy's monitoring time period.

 Custom metrics: Appear in the second part of the list and are indicated by a field icon

- Custom metrics are defined from specific fields within reports. If a custom metric is added to the policy, an alert will be sent if a report with a field is filled out more times than allowed by the policy thresholds during the policy's monitoring time period.
- For more information, see Custom metrics.

Define the policy's time period

This section lets you set the timeframe during which the policy will be actively monitoring data. Alerts are sent if policy thresholds are met during this time.

There are three fields to complete in this section:

- **Type**. Options include:
  - **Rolling time frame:** The policy will monitor reports during a repeating time frame.
    - For example, if the period is 30 days, the policy will include all reports written during January 1–January 30, then January 2–January 31, then January 2–February 1, etc. These repeating time frames will continue as long as the policy is active in the system.
  - **Single date range:** The policy will monitor reports during a single date range, beginning with the start date.
    - For example, if the period is 30 days, the policy will only include reports that are created in the 30 days following the policy’s start date.
- **Duration:** The amount of time in the discrete or sliding window.
  - **Rolling time frame:** Specify a number of days
  - **Single date range:** Select month, quarter, or year.

- **Start date:** The date the policy begins monitoring reports. This date can be in the past or future.

Set the policy thresholds

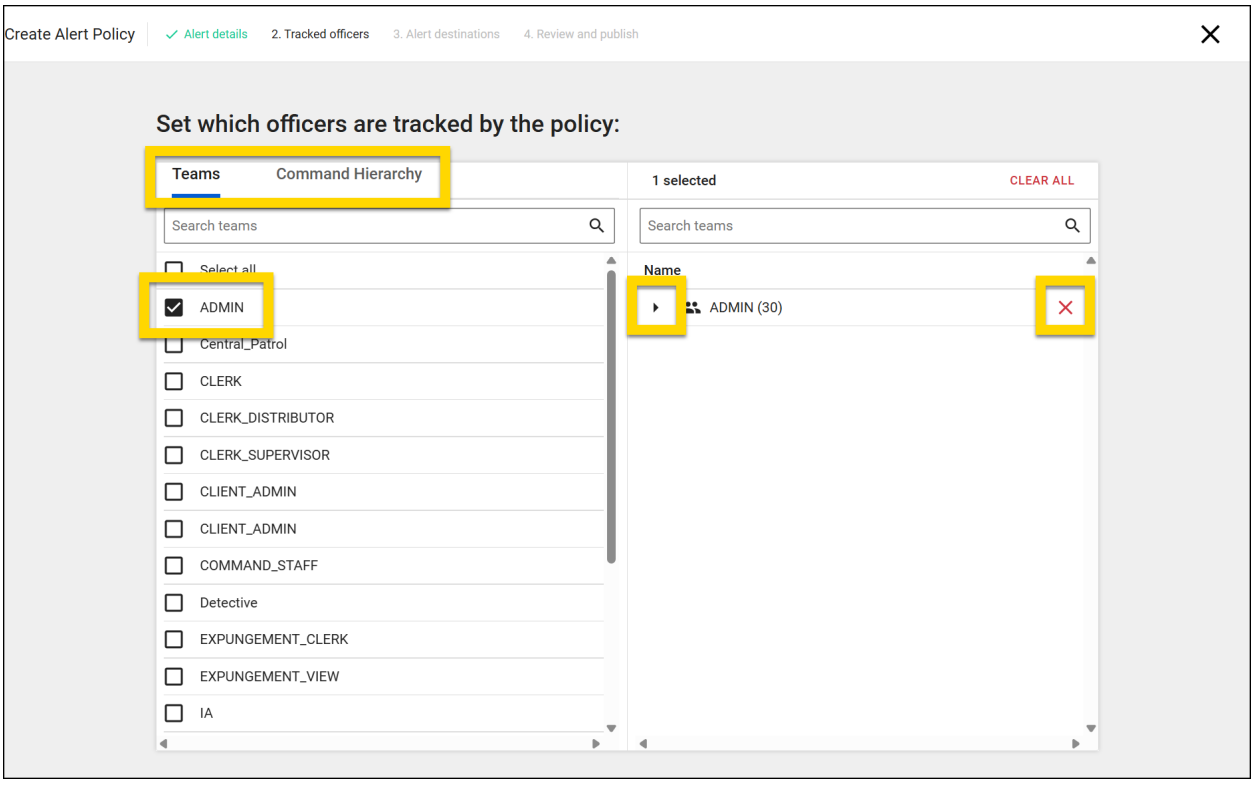
In this section, you can indicate how many times the metric(s) must be met during the policy time period in order for an alert to be sent. You can set both a Warning (low) and a Critical (high) threshold.

The condition is always set to Above, which means officers must exceed the number you put in the Warning and Low threshold fields. For example, entering 1 in the **Warning threshold** field and 2 in the **Critical threshold** field means that:

- A warning alert will trigger when an officer is involved in 2 occurrences of the policy metric(s).
- A critical alert will trigger when an officer is involved in 3 occurrences of the policy metric(s).

Tracked officers

Use the tabs and checkboxes to set which teams and Command Hierarchy groups the policy should track. After adding a user or group, select the arrow to expand the team/group and view all users assigned to it. If you add a team or group by mistake and need to remove it, select the **X**.



Alert destinations

Set which Command Hierarchy groups, teams, or individual users should receive an email when these alerts are triggered. Leave this field blank if you don't want any emails sent when the alert is triggered. You can add multiple recipients and select the **X** to remove a recipient.

Alerts for all policies will appear in the Agency Alert inbox, regardless of the groups, teams, or users specified in this **Recipients** field.

Review and publish

Review your policy. Select **Back** if you need to make any changes. Select **Publish** if all information is correct.

Once the policy is published, it will immediately begin reviewing and tracking your organization's reports, starting on the Start Date specified on the Alert details page.

Update policies

When updating a policy, you can edit the following items:

- Start date
- Tracked users
- Alert destinations

You are NOT able to update the following aspects of a policy. If you want to change these aspects of a policy, delete the policy and create a new one instead.

- Name
- Metrics
- Duration
- Thresholds

To update an existing policy:

1. Select **More actions [...] > Update policy** in that policy's row on the **EIS policies** tab.
2. The Alert details screen is read-only, allowing you to view all details about the current policy.
   - You are NOT able to update any of this information, but you will be able to update the policy start date in a later step.
3. Change the tracked officers if desired and select **Next**.
4. Change the alert destinations if desired and select **Next**.
5. Set a new start date for the policy if desired and select **Review changes**.
   - The policy will review all reports starting on this date and generate alerts as appropriate.

6. Review the summary of your changes. If everything looks correct, select **Save and start recalculation**.
   - When you save, recalculation starts and alerts are generated immediately. This cannot be undone, so review your changes carefully before saving.
7. When you save your changes, the policy recalculation begins.
   - Reports for tracked officers are reviewed starting on the start date you specified (whether you left it as-is or changed it).
   - New alerts are generated as required by the policy updates.
   - If the original policy created an alert that is also required based on the policy updates, a duplicate alert is NOT sent.
   - Existing alerts are altered or removed as required by the policy updates.
8. Recalculation can take up to two minutes. **You must leave the tab open while the policy recalculates**.
   - You can open a new tab and continue to work while you wait for recalculation to complete.
   - You are NOT able to begin a recalculation on a second policy while the recalculation for the first policy is in progress. You must wait for the first recalculation to complete before starting a second one.
9. If the recalculation is successful, a confirmation page summarizes when the recalculation started and completed, as well as any new or updated alerts that were generated.

Recalculate policies

To change a policy's start date only (and not the tracked officers or alert destinations:

1. Select **More actions [...] > Update policy** in that policy's row on the **EIS policies** tab.
2. Set a new start date for the policy and select **Review changes**.
   - The policy will review all reports starting on this date and generate alerts as appropriate.
3. Review the summary of your changes. If everything looks correct, select **Save and start recalculation**.
   - When you save, recalculation starts and alerts are generated immediately. This cannot be undone, so review your changes carefully before saving.
4. When you save your changes, the policy recalculation begins.
   - Reports for tracked officers are reviewed starting on the start date you specified (whether you left it as-is or changed it).
   - New alerts are generated as required by the policy updates.

- If the original policy created an alert that is also required based on the policy updates, a duplicate alert is NOT sent.
- Existing alerts are altered or removed as required by the policy updates.

5. Recalculation can take up to two minutes. **You must leave the tab open while the policy recalculates**.
   - You can open a new tab and continue to work while you wait for recalculation to complete.
   - You are NOT able to begin a recalculation on a second policy while the recalculation for the first policy is in progress. You must wait for the first recalculation to complete before starting a second one.
6. If the recalculation is successful, a confirmation page summarizes when the recalculation started and completed, as well as any new or updated alerts that were generated.

Custom metrics

Custom metrics are defined from specific fields within reports and can be added to alert policies, which determine when EIS alerts are sent.

To view your agency's custom metrics, open the Administrator Console, select **EIS Alert Policies**, and switch to the **Custom metrics** tab.

Basic information about each metric is displayed in the table, including its name, the form it is associated with, the type of field that is used in the metric, and when it was created.

Select a metric name to view additional information about it.

To create a custom metric:

1. Select **Create custom metric** in the top right corner of the screen.
2. Select the data source for the metric, including the report that contains the field, the field name, and the field value.
   - For example, if you select Form: Citizen Complaint, Field: Allegation, and Field Value: Excessive Force, whenever a Citizen Complaint report is created and Excessive Force is selected in the Allegation field, it will count as one occurrence of this metric.
   - Reports contain two different field types, option and number. Metric occurrences are calculated differently for each field type. For more information, see Field types.
3. Select **Next**.
4. Enter a metric name. Metric names must be unique to ensure the correct metric is added during alert policy creation.
5. Select **Next**.
6. Review the metric carefully. After a metric is created, it can't be edited or deleted.
7. If all information is correct, select **Create metric**.

8. The new metric will appear on the **Custom metrics** tab and will appear in the list of available metrics during alert policy creation.

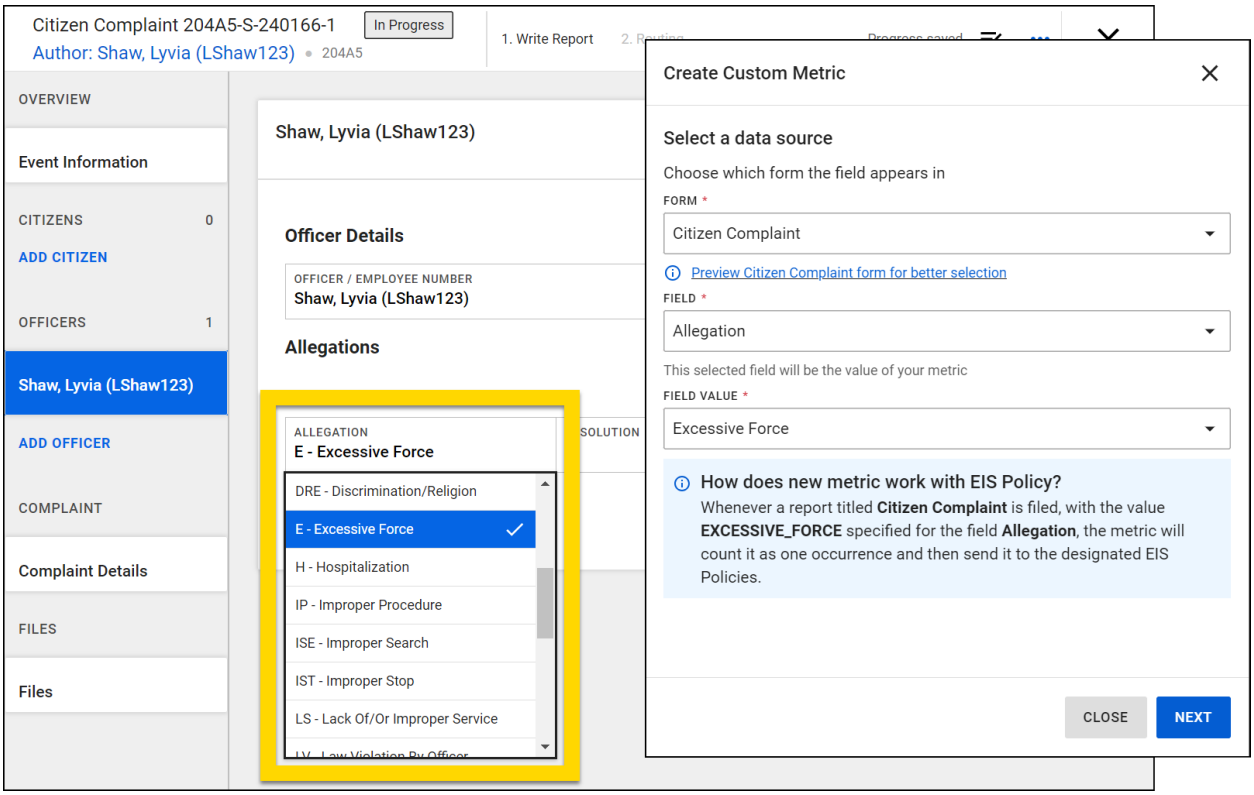
Field types

Reports contain two different field types, and metric occurrences are calculated differently for each field type.

Option

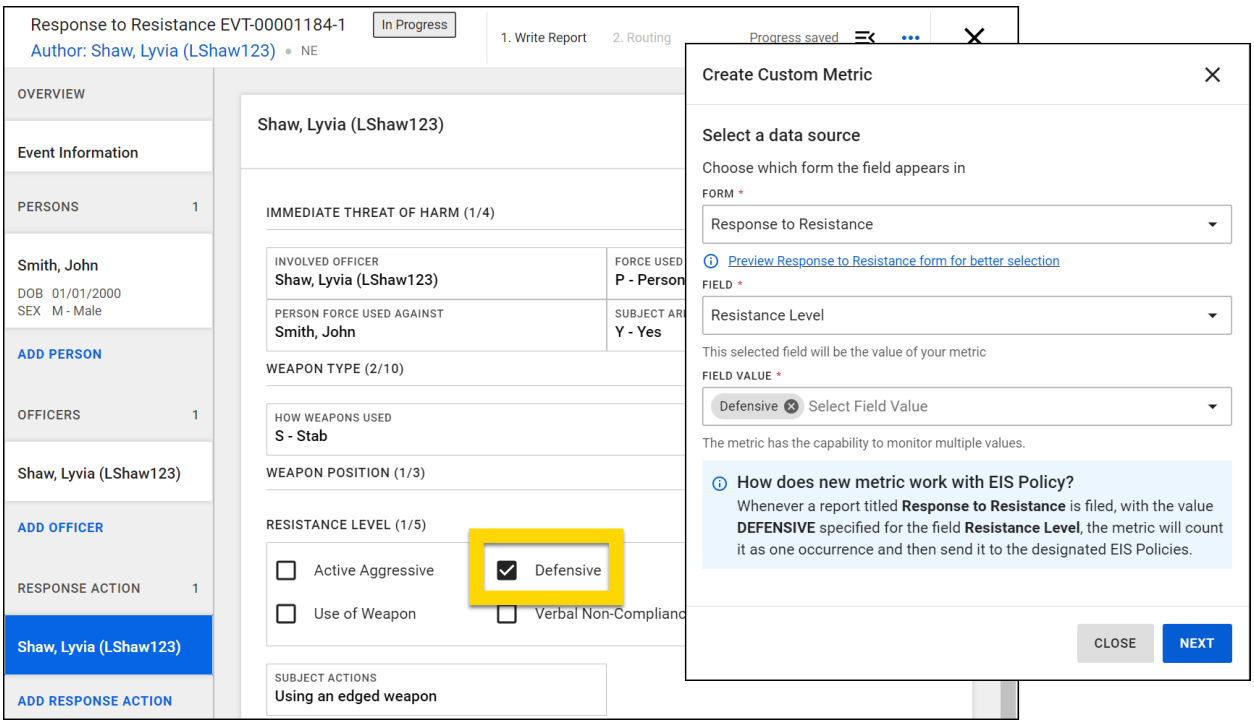
Option fields include dropdown menus or sets of checkboxes. When the field value indicated in the custom metric is selected for the field, the metric occurrence will be 1.

For example, the **Allegation** field in the Citizen Complain report is a dropdown menu that includes an **Excessive force** option. If this option is selected in a report, and a custom metric is created tracking this field, one occurrence of the metric will be recorded for this field.



Similarly, the Resistance level section in the Response to Resistance report contains a set of checkboxes that include **Defensive**. If the Defensive **checkbox** is selected in a

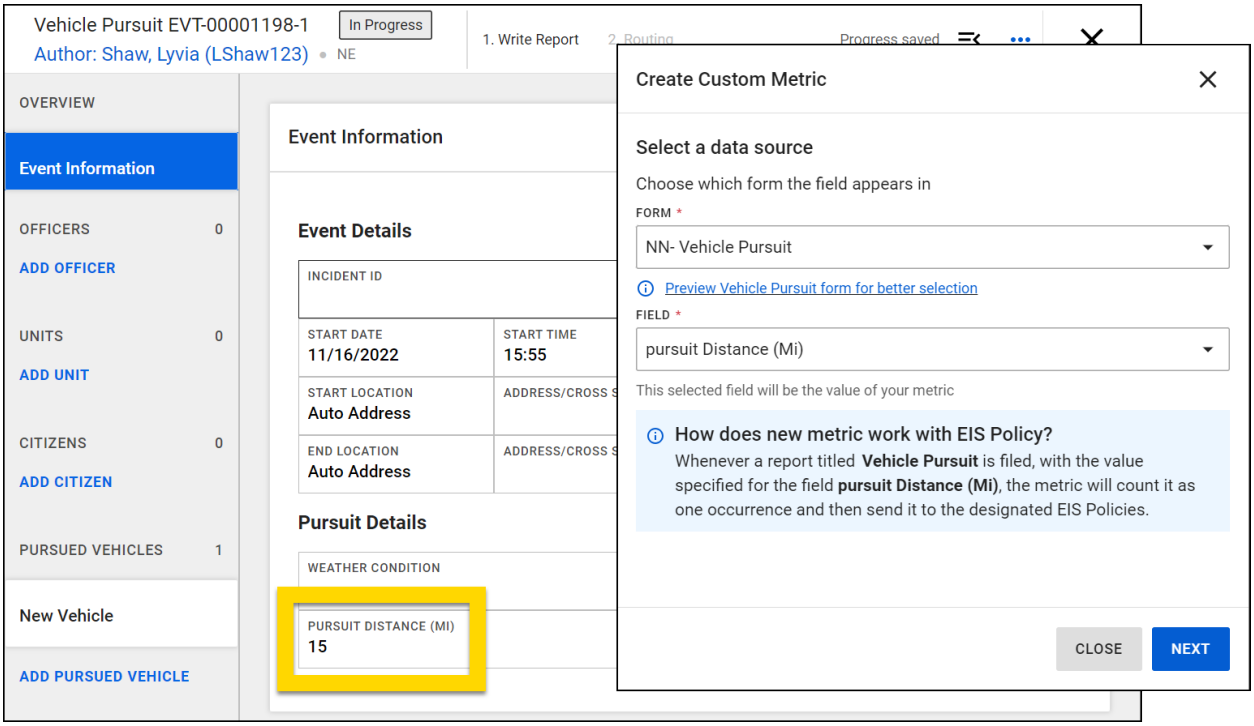
report, and a custom metric is created tracking this field, one occurrence of the metric will be recorded for this field.



Number

Number fields are completed by entering a number in the field. The number entered in such fields becomes the number of occurrences for the metric.

For example, the **Pursuit Distance (MI)** field in the Vehicle Pursuit report lets users enter a number. If this report is created and "25" is entered in this field, and a custom metric is created tracking this field, the metric occurrence will be 25.



Flags configuration

Users with specific privileges can add flags (colored labels) that serve as quick visual alerts to important information when someone views a profile. In Axon Records, flags can be added to location, organization, people, and vehicle profiles. In Axon Standards, flags can be added to citizen and vehicle profiles. If your organization uses both Axon Records and Axon Standards, any flag categories you create can be used in both places.

Flags are managed from the Flags Configuration tool in the Administrator Console. To access this tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Flags Configuration** from the tool list.

Create flag categories

To create a new flag category:

1. Open the **Administrator Console**.
2. Select **Flags Configuration**.
3. Select **Add new** at the top of the page.

When creating a new flag, provide the following information:

- Category name
- Indicator color (blue, gray, green, orange, purple, or red)
- Severity (high, medium, or low)
- Description template (optional, appears when a user adds a flag to an entity, signaling that they need to provide information when assigning the flag)

Edit flag categories

To edit a flag category:

1. Open the **Administrator Console**.
2. Select **Flags Configuration**.
3. Select **Edit** for the flag you want to modify.

Warning

You cannot delete flag categories, so be cautious before adding new ones.

Master Name Index (MNI)

The Master Name Index (MNI) is a subject identification database that includes basic identifying information along with a detailed profile for each person who has been added to a report. Subjects include offenders, suspects, victims, witnesses, and related people who have interacted with an officer in the past and been included in a report.

When writing a report, you can search the database to add an existing person to your report rather than making a duplicate profile. This way, all reports associated with the same person are kept in one place, on a single citizen profile.

MNI in Axon Standards and Axon Records

Axon Records and Axon Standards have separate MNI databases; when a person is added to an Axon Records report and included in the Axon Records MNI database, they will NOT also appear in the Axon Standards MNI database. In other words, if a person has a profile in Axon Records, you will not be able to find them or any information from any Axon Records reports they have been associated with when creating Axon Standards events or searching in Axon Standards.

These separate databases help prevent the introduction of bias into an Axon Standards investigation. If a person with a past criminal record is involved in an Axon Standards event, their criminal record (as documented in Axon Records) is not displayed to the report author in Axon Standards.

You can import a person and their personal information (except for the incidents they are associated with) from Axon Records into Axon Standards. For more information see Create events from Axon Records.

Note

Axon Standards does not yet have an MNI Merge Tool like Axon Records.

Personnel Data Tool

The Personnel Data Tool lets you manage Personnel information, offering import and export capabilities.

To access this tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Personnel Data Tool** from the tool list.

Note

Users must have the Personnel privilege to access this tool and import Personnel data.

Import information

You can add or edit multiple users' profiles using the Personnel Data Tool's CSV templates. After updating the CSV template, you can then import the updated information into the Personnel module using the Personnel Data Tool. The steps below outline this process.

See the Personnel fields section below for more information about the fields that appear by default in the Personnel module. These fields can be configured for each organization.

Download the template

1. Open the Administrator Console.
2. Select **Personnel data tool.**

3. From the **Import** tab, open the **Choose template folder** dropdown menu and choose the type of information you want to update.
   - The options in this menu correspond to the sections that appear on a user's profile in the Personnel module (Demographics, Service History, etc.).
4. Select **Download template CSV** to download the template to your computer.
5. Download the **Data format guide** to see the formatting requirements for each field.

Edit the template

Before you open the template CSV file in Microsoft Excel, make sure your Excel settings use a comma as the delimiter character. If a different character is used, incorrect formatting will appear in the file when you open it in Excel.

To update the delimiter settings:

1. Select **File > Options**.
2. Open the **Advanced** section.
3. Make sure the **Use system separators** option is unchecked.
4. Enter a period (.) in the **Decimal separator** box and a comma (,) in the **Thousands separator** box**.**
5. Select **OK**.

After verifying your Excel settings are correct, open the template and add information as appropriate. While you are editing, keep in mind:

- In the template, each row belongs to one person. Only add details for the people you need to update.
- Some columns require a specific type of data to upload successfully. Download the **Data Format Guide** from the Personnel Data Tool page, to see which values can be entered in each column in the template.
- Never delete a column or change the column header. The file will not upload if a column is missing, or a header is changed.
- You can leave cells empty; a blank cell won't change or remove information that currently appears in that person's profile in the Personnel module.

After you've put all the information into the CSV file, save it to your computer.

Upload the updated information

1. Open the **Personnel data tool** from the Administrator Console.
2. From the **Import** tab, click **Select CSV file**.
3. Find the CSV file you updated.

4. From the **Upload Location** menu, choose the type of information you are updating.
   - The options in this menu correspond to the sections that appear on a user's profile in the Personnel module (Demographics, Service History, etc.).
5. Select **Start import** to upload the CSV file.

Export information

To view all information that has been entered into the Personnel module, export personnel information:

1. Open the Administrator Console.
2. Select **Personnel data tool**.
3. Switch to the **Export** tab.
4. Open the **Choose folder** dropdown menu and select the information you want to download.
   - The options in this menu correspond to the sections that appear on a user's profile in the Personnel module (Demographics, Service History, etc.).
5. Select **Download CSV**.

In the file that downloads, each row equates to a user who has been added to the Personnel module. The columns contain the fields associated with that section of the module (Demographics, Service history, etc.).

Personnel fields

When the Personnel module is enabled for your organization, it contains a default set of fields—and options or values that can be entered into each of the fields. These fields are sometimes referred to as "out-of-the-box" or "OOTB" fields. For example, **Blood type** is a default field that appears in the Demographics section of a user's Personnel profile. The available options for this field include all blood types (A-, A+, B-, etc.).

You can customize these fields and their options for your organization by contacting your Axon representative or Axon Support. You can always view all fields an options that have been configured for your organization from the Personnel Import Tool:

- To view the fields configured for a given section of the module: On the **Import** tab, select a section from the **Choose template folder** menu.
- To view the options that have been configured for all fields in the module: On the **Import** tab, download the **Data format guide**.

The sections below outline examples of the default fields that appear in each section of the Personnel module.

Demographics

The fields in the Demographics section provide basic information about the user. These fields include:

- **Identity and identifiers:** Legal first / middle / last name, preferred name, badge number, employee ID, date of birth, SSN (where configured)
- **Contact:** Work email, personal email, work phone, personal phone, home address components
- **Employment basics:** Hire date, employment type (sworn / non-sworn / volunteer), employment status (active / inactive / retired / terminated), primary assignment, current rank
- **Placement in the organization:** Department, division, unit, shift, command hierarchy group

Service history

The fields in the Service history section track how a user's assignment and rank change over time:

- Effective start / end dates
- Assignment / position name
- Rank at the time
- Unit / division / bureau / shift
- Reason for change (hire, transfer, promotion, demotion, separation, etc.)

Commendations and awards

The fields in the Commendations and awards section record positive performance events:

- Date of incident / recognition
- Commendation type (e.g., letter of commendation, medal, citizen thank-you)
- Source (citizen / supervisor / peer)
- Narrative / citation text

Performance review

The fields in the Performance review section track performance evaluations:

- Year
- Score
- Type

Promotions

The fields in the Promotions section capture discrete promotion events:

- Effective date
- From-rank / to-rank
- Promotion type (e.g., probationary → permanent, step increase)
- Approving authority and narrative notes

Discipline

The fields in the Discipline section summarize disciplinary actions separate from the underlying case reports:

- Case / incident reference
- Allegation type(s) and findings
- Discipline type (written reprimand, suspension, termination, etc.)
- Effective dates and, where modeled, progressive discipline stage

Custom sections

Additional, custom sections, such as Claims, can be configured. These sections can be customized from a starting template that includes the following fields:

- Type
- Reference ID
- Notes

Report Submission Settings

You can specify for each report type whether users can submit the report with validation errors present, or if they must resolve all errors before submitting the report for review.

This functionality is managed from the Report Submission Settings tool. To access this tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Report Submission Settings** from the tool list.

Note

Users must have the Report Submission Settings privilege to access this tool and manage submission settings.

Change settings for a single report type

To change the submission setting for an individual report type, follow these steps:

1. Open the **Administrator Console**.
2. Select **Report Submission Settings** from the tool list. This page displays all report types configured for your organization.
3. In the Form Name column, find the report type.
4. Move the toggle in the **Allow submissions with errors** column to the off position. The toggle appears gray when it is turned off.

Change settings for multiple report types

To change the submission setting for multiple report types, follow these steps:

1. Open the **Administrator Console** .
2. Select **Report Submission Settings**. This page displays all report types configured for your agency.
3. Select the checkbox next to each form you wish to update.
4. Open the **Actions** menu at the top of the page and select one of the options:
   - Allow submissions with errors
   - Block submissions with errors

Restrictions

Users can apply restrictions to an entire event or to specific report sections, such as information about a person or vehicle.

Restriction types and restriction exception lists are managed from the Restrictions tool in the Administrator Console.

To access the Restrictions tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Restrictions** from the tool list.

Note

Users must have the Restrictions privilege to access this tool and manage restrictions.

If your organization is configured for both Axon Records and Axon Standards, any restrictions you create can be assigned to both Axon Records and Axon Standards reports.

Restriction types

To create a new restriction type, take these steps:

1. Open the Restrictions tool in the Administrator Console.
2. On the **Restrictions** tab, scroll down to the bottom of the list and select **Add new**.
   - The **Hide all information** checkbox is selected by default. This setting hides all information associated with this restriction from search results.
3. Select **Add** to save the new restriction type.

Once created, restriction types can't be deleted, although they can be renamed by selecting **Edit**. When editing a restriction, you can also uncheck the **Hide all information** checkbox.

Restriction exceptions

If you want a user, team, or Command Hierarchy group to view a specific item that has been restricted, but you don't want to give them access to view all items containing that restriction, you can create a restriction exception.

Restriction exceptions are created from within an event. All restriction exceptions that have been created for the organization appear on the **Restriction Exceptions** tab in the Restrictions tool. This tab includes the following information:

- **Restriction context:** The Event ID where the restriction exception was applied.
  - Select the Event ID to open the item and update the restriction exception if necessary.
- **Applies to:** The user who has been granted access to the item
- **Allowed restrictions:** The restrictions that the person has been given access to (in the context of that specific event.
- **Duration:** The length the exception was granted for. After the time passes, the exception will disappear from the **Restriction exceptions** tab, and that user will no longer be able to view the restricted information.
- **Added on:** The date the restriction exception was created.

Rules and automations

Axon Standards can automatically take action when certain events happen in the system, so your team spends less time on repetitive manual work. These automations are called "rules."

Note

Contact your Axon representative or Axon Support to request rules be configured for your organization's specific needs.

What rules can do

Rules can be configured to perform the following actions:

Category	Action details
Restrictions	Add a restriction to a report
Case management	Create a case from an incident report, or route a case to a specific unit
Case tasks	Add one or more tasks to a case
Notifications	Send an in-app notification or email to specific people
Tasks	Assign a task, change a report's state, update a report's district, or delete comments on a report
Flags	Add a flag to a person's profile

When rules can run

Rules can be configured to run when the following activities occur:

Type	Activity details
Report	A report is created, approved, rejected, or moves into a different state
Task	A task is created or assigned to someone
Event	An event is created in Axon Standards
Profile	A profile is created or updated
Warrant	A warrant's status is updated
Schedule	Runs on a recurring basis, such as daily or weekly, instead of in response to a specific event

Conditions

Conditions let you limit a rule so it only runs in specific situations instead of every time that activity occurs. For example, a rule can be configured to apply only to reports assigned to a certain district, or only when a person is added to a report and their age falls within a certain range.

Rules can include one or more conditions. If a rule includes more than one condition, you can choose whether all conditions must be true or whether any one of them is enough.

Available conditions include:

Type	Condition details	Example: Only run this rule for...
District or site	The report or record belongs to a specific district or site	Reports from the Downtown district
Offense category	The report includes one or more specific offense categories	Reports categorized as burglary or theft
Case factor	The case has been tagged with a specific case factor	Cases tagged as gang related
Person age	The person on the profile falls within a specific age range	Profiles for people under 18
Assigned user	The report or task is assigned to a specific person	Tasks assigned to a users in the Supervisors team
Charge	The report includes a specific charge	Reports that include a DUI charge
Restriction classification	The restriction being applied matches a specific classification	Restrictions classified as confidential

Example rules

Here are a few examples of rules organizations commonly use. Your Axon representative can help you build something similar or design a rule specific to your workflow.

Notify a case owner when a warrant status changes

When a warrant's status changes to Served, Axon Records sends an in-app notification to all users in the Investigative Division. This notification appears in the Notification Center.

Create a case when a report is approved and route the case

When an incident report with a Case factor of "Arson" is approved, a case is created. The case is routed to the Arson inbox where it can be assigned to a Lead Detective.

Add a flag when a new profile is created

When a new person profile is created and the person is under 18, a "Juvenile" flag is applied to that profile.

Send a weekly digest to supervisors

On Mondays at 8:00 AM, a digest notification is sent to all supervisors summarizing their team's outstanding reports, so nothing falls through the cracks.

Training Data Tool

You can use the Training Data Tool in the Administrator Console to import training records from external systems into the Training module. This feature helps you keep all your training records in a single location.



To access the Training Data Tool, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Training Data Tool** from the tool list.

Importing training records using this tool involves three steps:

1. Configure privileges and forms
2. Export training data
3. Import curricula
4. Import courses
5. Import training records

Configure privileges and forms

Before importing training records, verify that you have all static AND workflow Training privileges.

After verifying privileges, verify that the Training Record form in Form Builder has been published. This form can be accessed by going to **Form Builder > Training**.

Export training data

Extract your training data from the external system. Once exported, the training data should be organized into three CSV files, each with a set of pre-defined columns.

- Curriculum
- Course
- Training Records

The sections below explain how each CSV file should be formatted. You can also download a Format Guide containing this information from the **Import** tab in the Training Data Tool.

Import curricula

> **Note**
>
> You must import data in this order (curricula > courses > training records) to ensure that the curricula and courses are associated with learners correctly.

To import curricula, take these steps:

1. Open the Training Data Tool.
2. On the **Import** tab, select **Curriculum** from the Step 2 dropdown menu
3. Select **Download template CSV**.
4. Update the template file with the curricula data you exported from your external system.
   - See the curriculum template guidelines below for file formatting instructions.
5. After updating the template file, return to the **Import** tab in the Training Data Tool.
6. In Step 3, select **Curriculum** from the dropdown and select the template file you updated and saved.
7. Resolve any errors that appear.
8. When your CSV file is error-free, select **Import**.
9. Open the Training Management page in the Training module and switch to the Curricula tab.
10. Find the curriculum and select **More actions [...] > Update** to open the curriculum and publish it.
11. Proceed to the next step of importing courses.

Curriculum template guidelines

When updating the curriculum template with external training data, note that each row represents one curriculum. The table below explains each of the template columns and the values that can be entered in the column's cells.

Column	Required	Valid Values	Description
referenceId	Yes		A unique identifier for the curriculum.

Column	Required	Valid Values	Description
curriculumFriendlyId	No		Leave this cell empty. When you import your curricula, the system auto-generates a Friendly ID.
name	Yes		
curriculumType	Yes	MANDATED NONMANDATED	
capacityType	Yes	UNLIMITED LIMITED	Indicates how many learners were enrolled in the course.
courseModality	Yes	ONLINE OFFLINE	
description	No		
capacity	No		If **`UNLIMITED`** is entered in the **`capacityType`** column, this cell is ignored.
assessmentMethod	Yes	CATEGORICAL NUMERICAL	Indicates how learner performance was assessed. See Curriculum details for more information.
creditsAwardedType	Yes	CREDIT NO_CREDIT	Indicates if credits were awarded for course completion. See Certification settings for more information.
trainingCreditHours	No		If **`NO_CREDIT`** is entered in the **`creditsAwardedType`** column, this cell is ignored.
expireType	Yes	COMPLETION_ DATE FIXED_DATE ONE_TIME	Indicates how the certification expires. See Certification Settings for more information.

Column	Required	Valid Values	Description
certificationDurationType	No	DAYS MONTHS QUARTERS YEARS	If **FIXED_DATE** or **ONE_TIME** is entered in the **expireType** column, this cell is ignored.
certificationDurationType FixedDate	No	DAYS MONTHS QUARTERS YEARS	If **COMPLETION_DATE** or **ONE_TIME** is entered in the **expireType** column, this cell is ignored.
certificationPeriod	No		If **FIXED_DATE** or **ONE_TIME** is entered in the **expireType** column, this cell is ignored.
certificationPeriod FixedDate	No		If **COMPLETION_DATE** or **ONE_TIME** is entered in the **expireType** column, this cell is ignored.
certificationExpiredDate	No		If **COMPLETION_DATE** or **ONE_TIME** is entered in the **expireType** column, this cell is ignored.

Import courses

After your curricula import is complete, you can proceed to importing courses:

1. Open the Training Data Tool.
2. Switch to the **Export** tab.
3. Select **Curriculum** from the dropdown menu.
4. Select **Export CSV** to download the list of Curricula IDs.
5. Switch back to the **Import** tab, select **Course** from the Step 2 dropdown menu
6. Select **Download template CSV**.
7. Update the template file with the course data you exported from your external system.
   - Use the Curricula IDs you downloaded from the **Export** tab.
   - See the course template guidelines below for file formatting instructions.
8. After updating the template file, return to the **Import** tab in the Training Data Tool.

9. In Step 3, select **Course** from the dropdown and select the template file you updated and saved.
10. Resolve any errors that appear.
11. When your CSV file is error-free, select **Import**.
12. Open the Training Management page in the Training module and search the Courses tab to verify that your courses imported as expected.
13. Proceed to the next step of importing learning records.

Course template guidelines

When updating the course template with external training data, note that each row represents one course. The table below explains each of the template columns and the values that can be entered in the column's cells.

Column	Required	Valid Values	Description
referenceId	Yes		A unique identifier for the course.
courseFriendlyId	No		Leave this cell empty. When you import your courses, the system auto-generates a Friendly ID.
courseName	Yes		
location	No		The location where the course was held. This can be a physical location or a link to a virtual location.
courseSchedule	Yes	MM-DD-YYYY HH:MM	The date and time the course was held.
curriculumFriendlyId	Yes		Enter the Friendly Curriculum ID of the curriculum that was taught in this course. This ID was generated by the system when you uploaded the curricula. Be sure to use the Friendly Curriculum ID and not the Reference ID. A Curriculum ID can be associated with multiple courses. The list of Friendly Curricula IDs can be obtained by exporting the curricula from the Export tab in the Training Data Tool.

Column	Required	Valid Values	Description
instructorEmail	No		The email of the instructor who taught the course. This email address must match the email address of a user in the Axon system.

Import training records

After your curricula and course imports are complete, you can proceed to importing training records, which are the association between a learner and a course:

1. Open the Training Data Tool.
2. Switch to the **Export** tab.
3. Select **Course** from the dropdown menu.
4. Select **Export CSV** to download the list of Course IDs.
5. Switch back to the **Import** tab, select **Training record** from the Step 2 dropdown menu
6. Select **Download template CSV**.
7. Update the template file with the training record data you exported from your external system.
   - Use the Course IDs you downloaded from the **Export** tab.
   - See the training record template guidelines below for file formatting instructions.
8. After updating the template file, return to the **Import** tab in the Training Data Tool.
9. In Step 3, select **Course** from the dropdown and select the template file you updated and saved.
10. Resolve any errors that appear.
11. When your CSV file is error-free, select **Import**.
12. Open a user's training profile to verify that the training records imported as expected.

Training record template guidelines

When updating the training record template with external training data, note that each row represents the relationship between a single learner and a course. The table below explains each of the template columns and the values that can be entered in the column's cells.

Column	Required	Valid Values	Description
referenceId	Yes		A unique identifier for the training record.
trainingRecordFriendlyId	No		Leave this cell empty. When you import your courses, the system auto-generates a Friendly ID.
courseFriendlyId	Yes		Enter the Friendly Course ID of the course that this learner was enrolled in. This ID was generated by the system when you uploaded the courses. Be sure to use the Friendly Course ID and not the Reference ID. A Course ID will be associated with multiple training records. The list of Friendly Course IDs can be obtained by exporting the curricula from the Export tab in the Training Data Tool.
userEmail	Yes		The email of the user who was enrolled in the course. This email address must match the email address of a user in the Axon system.
attendance	No	TRUE FALSE	Indicates if the user did or did not attend the course.
score	No		If **`FALSE`** is entered in the **`attendance`** column, this cell is ignored.
result	No	PASS FAIL	Indicates the learner's result for the course. See Curriculum details for more information.
expiresAt	No	MM-DD-YYYY HH:MM	The date and time the user's certification for this course expires. See Certification settings for more information.

Import errors

You may encounter errors when importing curricula, courses, and training records.

If you receive the following errors, close the import window and try to import the file again:

- failed to auth service
- error generating (***) external ID
- error inserting (***) when calling to Records service
- failed to build (***) edges
- error getting (***) entities
- error getting entity ID when calling to Records service
- error getting training record form/forms

The following errors indicate that the data in the file you are uploading is incorrect. Open the file and verify that it matches the formatting requirements and contains valid values.

- error validating (***) data
- error invalid duplicate (***) ids
- error invalid reference IDs

The following error indicates that you are attempting to update a curriculum/course/training record. Currently, the Training Data Tool does not allow you to update items.

- operation not supported

If you encounter the following error, do not attempt to import again. Instead, contact your Axon representative for assistance.

- error creating (***) tasks, but the (***) already created

*** *curriculum / course / document (training record)*

User Management

Users are created in Axon Evidence, and then added to Axon Records and Axon Standards. For information on creating a user, see Adding a User and Roles and Permissions.

Once a user has been created, they can be given access to Axon Records or Axon Standards in one of two ways:

- By being added to a Command Hierarchy group that has been granted privileges in Axon Records or Axon Standards (Users can only be added to a Command Hierarchy group from Axon Evidence.)
- By being added to a team in Axon Records or Axon Standards

User privileges and team membership in Axon Records and Axon Standards are managed from the User Management tool. To access this tool, open the Administrator console by selecting the gear icon in the main navigation menu, then select **User Management** from the tool list.

Note

Users must have the User Management privilege to access this tool and manage users.

If your organization is configured for both Axon Records and Axon Standards, you will see all users for both Axon Records and Axon Standards when you open the User Management tool from either Axon Records or Axon Standards.

Users can only be added to a Command Hierarchy group from Axon Evidence and then must be added to a group or team that has the **Access to Standards** privilege in order to perform tasks in Axon Standards.

To add a user to a team, take the following steps:

1. Open the User Management tool.
2. Search for the user by name, username, or badge number and select their name to open their profile.
3. Select the **Members** toggle beside the team to which you wish to add the user.

Each team has privileges that determine which actions the team's members can take. For more information, see Manage privileges.

View which groups a user belongs to by selecting **Groups**, but you can only manage group membership from Axon Evidence.

Districts

When viewing a user's profile, edit their district by selecting **Actions > Edit District** in the top right corner of the page. (Some organizations may see "Special Unit" instead of "District".)

If a user is assigned to a district, any reports they write are automatically assigned to that district.

If the user has access to the Supervisor Tasks inbox, the **District** filter is auto-set to their district whenever they open the inbox.

To bulk-assign users to districts, open the User Management tool in the Administrator console and select **Actions > Import district assignments** in the top right corner of the page. Follow the instructions shown on this screen to create a CSV file containing your agency's district assignments and upload it.

Notary stamps

You can add an image to a user's profile. The most common use case for this feature is to add a notary stamp to a user's profile that is added to the affidavit during property release.

To add a notary stamp to a user profile, take these steps:

1. Open the User Management tool, search for a user profile, then select a user name.
2. Select **Actions > Add notary seal to profile**.
3. Upload an image from your computer.

Workflow Manager

The Workflow Manager tool lets you create workflows that Axon Standards reports move through (e.g., Draft, Review, Finalized, etc.)



To access Workflow Manager, open the Administrator Console by selecting the gear icon in the main navigation menu, then select **Workflow Manager** from the tool list.

Note

Users must have the Workflow Manager privilege to access this tool and manage workflows.

When you create a workflow for Axon Standards from the Workflow Manager tool, the workflow contains five states. When a report moves through this workflow, a task will appear in different inboxes depending on the state of the report.

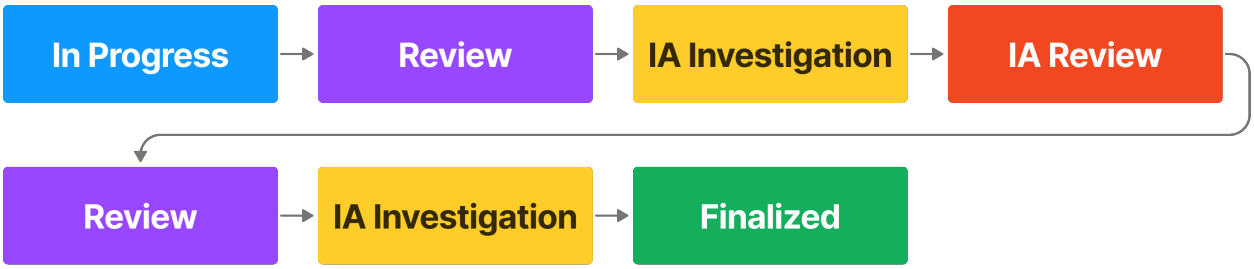
For example, when a report is in progress, a Write task for the report appears in the My Tasks inbox of the person assigned to write the report. Once the report is submitted for review, a Review task for the report appears in the Chain of Command inbox.

All tasks also appear in the Agency Tasks inbox, regardless of the current state of the report.

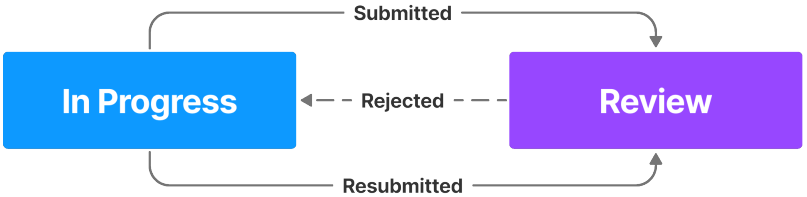
State	Inbox
In Progress	My Tasks

State	Inbox
Review	Chain of Command
IA Investigation	IA Investigation
IA Review	IA Review
Finalized	Agency Tasks > **Recently Finalized** tab Reports appear in descending order from most recently finalized. This inbox contains 1,000 pages of reports. All other finalized reports can be found using Events search.

Standards workflows are flexible; reports do not move in one direction through the workflow (i.e., In Progress → Review → IA Investigation → Finalized.). Instead, reports can move between any of the states. For example, a report can move through the workflow as follows:



If a report is rejected at any point, it is returned to the original author who can revise and resubmit it for review.



When you create a new Axon Standards workflow, a set of corresponding privileges appears in the Administrator Console, which you can configure to allow users to perform appropriate actions in the workflow.

Form Builder

Form Builder lets you manage your organization's forms and subforms. Forms provide the structure for users to create reports. In Form Builder, you can view:

- View the current status of your organization's forms (draft, published, archived).
- Edit existing forms and subforms, including adding cards and fields.
- Revert back to a previous version of a given form or subform.
- Archive forms and subforms.

This video contains a brief overview of Form Builder.

Access Form Builder

To access Form Builder:

1. Open the **Administrator Console** by selecting the gear icon in the main navigation menu ⚙.
2. Select **Form Builder (Early Access).**
3. Select a tab to view the forms used in that area of the product (i.e., Records, Standards, Warrants, etc.).

The following information is provided about each form in the list:

- **Form name**
  - Select the blue hyperlink form name to open the form and edit it.
  - The form type is listed under the form name. If it is a standard form created by Axon, the type name is listed. If it is a custom form that has been created for your organization, the type is "Custom".
- **Status**
  - Forms can have one of the following statuses:
    - Published: The form is live and matches what users see when creating reports in Report Writer.
      - The date the form was last published is also displayed. Note that if this date is prior to the date in the Last modified column, this indicates that the published form has unpublished draft changes.
    - Archived: The form is no longer active, and users can no longer use it when creating new reports.
      - The form can be unarchived and republished if needed.The date the form was last published is displayed.

        - Draft: The form is in draft and has never been published.
            - If a form has been published but has edits that have not yet been published, the form status displays as Published.
- **Last modified**
    - The date and time of the most recent change made to the form, including edits to the form fields or status changes (such as publishing or archiving).
- **Actions**
    - Includes actions you can take on the form, including:
        - View activity log
        - Archive
        - Discard draft

Watch this video for an overview of accessing and navigating Form Builder.

View activity logs

All actions taken on forms and subforms appear in the activity log, including when a form or subform was last edited, published, or archived and who performed these actions. This information can help track changes and troubleshoot issues, as well as maintain accountability.

When you view a form or subform activity log, you can access the following information:

- **Date and time**: The exact date and time when a status was changed.
- **Action**: The specific action taken on the form or subform, such as editing, discarding a draft, publishing, or archiving.
- **User**: The name of the person who performed the action.

Note

At this time, the activity log displays the name of the Axon representative who made a change. In a future release, it will display "Axon Support" for all changes made internally by Axon staff.

By default, the activity log shows the newest changes first. Use the **Sort By** dropdown at the top of the Activity Log pane to show the oldest changes first instead.

To view a form's or subform's activity log:

1. Open Form Builder and switch to the tab that contains the form or subform.
2. Locate the form or subform you want to review.
3. In the **Actions** column, select **More actions [...] > View activity log**.

Watch this video, starting at 04:43, for an overview of the activity log.

Forms

Forms in Records and Standards are used to capture data. When users create a report in Report Writer, the report they create uses the form administrators have created in Form Builder as a "template" for their report. All cards, sections, and fields contained in the form appear in the report that users fill out and submit.

Forms are structured in a hierarchy, similar to how a filing cabinet holds files and papers. Think of a form as a filing cabinet. It is a large container that holds structured information.

Within a filing cabinet are file folders. In Form Builder, these are called cards, which appear on the left side of the form in a navigation menu. Cards contain the various fields that capture related information.

If cards are like file folders, fields are like individual papers within a file folder. Users enter information into fields when writing their reports. Multiple different field types are supported in Form Builder.

You can introduce additional structure and organization to your forms by adding sections within a card. A section can contain a group of related fields. Think of a section as a group of papers in the file folder that are stapled together.

A card can additionally contain subforms, which are like sections but can stand alone. Think of a subform as a smaller file folder that has been added inside the larger file folder. Subforms can have a similar organization as a form, including section and fields. A good example of a subform is a Tow subform that appears in vehicle collision reports.

Visually, you can think of the structure of a form as follows:

- Form
  - Cards
    - Fields
    - Sections
      - Fields
    - Subforms
      - Sections
      - Fields

This video explains how forms are structured.

Create forms

Form creation is currently not supported in Form Builder. If you need a new form, contact Axon Support or your Axon representative.

Edit forms

To edit a form, open Form Builder, switch to the tab containing the form, and select the blue hyperlink form name. See Cards and fields for details about managing these items in your forms.

Note

When you edit a published form, you create a draft of that form, and the edits you make are considered a "draft" until you publish the form. This means that the changes you make in the form won't appear to users in Report Writer until you publish.

To avoid conflicting changes, only one person can edit a form at a time. When another user is actively editing a form, a lock icon appears beside the form name and the status column displays the name of the person editing the form.

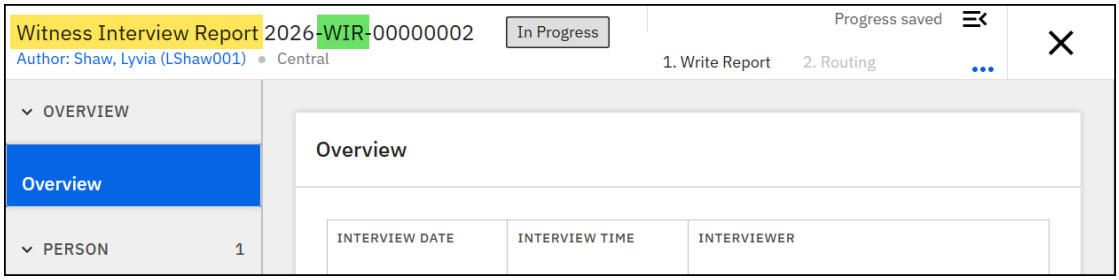
- To make urgent changes while someone else is editing, in the **Actions** column of that form's row, select **More actions [...] > Take over form**.
- Remember, if you take over a form from another user, any changes they've made will be lost.

Edit form details

To edit the title of a form or update the options such as requiring the Incident ID and enabling default incident entities:

1. Open the form.
2. In the top right corner, select **More actions [...] > Edit form details**.

3. You can modify the following options:
    - Form name and short code: The form name and short code appear throughout the product whenever a user views a report.
        - In the image below, the form name is highlighted in yellow, and the short code is highlighted in green.



    - Incident ID is required: If this option is checked, users must provide an incident ID when creating this type of report.
4. Press **Save** to apply your changes.
5. After making changes to your form, preview and then publish it.

Watch this video for an overview of how to update form details using Form Builder.

Preview forms

Preview mode shows how a report will appear to users in Report Writer when the form is published, allowing you to test rules, conditions, and overall functionality.

Select **Preview** at the bottom of the screen at any time during the creation or editing process to see how the form will look and behave. While in preview mode, you can enter sample data in the fields to test your fields, validation rules, and default values to ensure they function as intended.Use the buttons at the bottom of the screen to exit preview and continue editing the form or to publish the form. See the following section for more information about publishing forms.

Publish forms

After completing your form, select **Publish form** at the bottom of the screen. When you publish a form, your changes to the form will be applied to all reports users create using that form from that moment forward. If a user created a report using that form BEFORE you published, their already created reports will NOT reflect your changes.

Watch this video for an overview of managing and publishing forms using Form Builder.

Note

The publishing process is different for subforms. See Subforms for more information.

Discard drafts

When you edit a published form, you create a draft of that form, and the edits you make are considered a "draft" until you publish the form.

In Form Builder, you can discard a form's draft and revert back to the latest published version of the form (the version users are currently using when they create reports). When you discard a draft, you remove ALL changes made since the last time the form was published.

Warning

Discarding a draft cannot be undone. Once a draft is deleted, all changes are deleted and cannot be restored.

For example, you have a form that you published on Monday. On Tuesday, you make a number of changes to the form. However, at the end of the day, you decide you no longer want the changes you made to the form. You discard your draft (which contains all changes you made on Tuesday). When you edit the form on Wednesday, you do NOT see any changes you had made on Tuesday. Instead, you see a "fresh" draft that only contains the fields that were part of the form you published on Monday.

To discard a form's draft:

1. Open the form.
2. Select **More actions [...] > Discard draft** in the upper corner.
3. A confirmation message will appear. If you're sure you want to proceed, choose **Discard draft** on the confirmation message window that appears.

Watch this video, starting at 02:47, for an overview of discarding form drafts.

Restore previous version

With the Discard draft feature, you can discard a form's current draft and revert it back to the current published version. When you restore a form to a previous version, you move "back in time" one step farther and instead revert the form to the previously published version.

A form must have at least two published versions for this feature to be available. (In other words, you need a previous published version to revert the form back to.)

You can only perform this step once and revert back to the previously published version. You cannot after reverting, revert again and go back to an even older version of the form.

For example, you have a form that you published on Monday. This is version 1 of the form. On Tuesday, you make a number of changes to the form and publish it, making version 2 of the form. On Wednesday, you realize that the changes you made on Tuesday were incorrect. You revert to the previous version of the form, which is version 1.

Restore previous version and discard draft

If you revert to a previous version of a form and later decide you actually do not want to revert back to that version, you can use the Discard draft feature to return the form to its current published version.

For example, you have a form that you published on Monday. This is version 1 of the form. On Tuesday, you make a number of changes to the form and publish it, making version 2 of the form. On Wednesday, you realize that the changes you made on Tuesday were incorrect. You revert to the previous version of the form, which is version 1. However, after reverting to version 1, you realize you actually do want to use version 2. You use the Discard draft feature to discard your draft (which is version 1 of the form). When the draft is discarded, you are left with the currently published version of the form (version 2).

To revert to a form's previous version:

1. Open the form.
2. Select **More actions [...] > Restore previous version as draft** in the upper corner.
3. A confirmation message will appear. If you're sure you want to proceed, choose **Revert draft** on the confirmation message window that appears.
4. When you revert to a previous version, you discard any changes you've made, and the form is reverted back to a previous version.
   - The form is in draft, and the previous version is NOT automatically republished. As a result, users can continue to create reports using the most recently published version of the form (i.e., the version that you just reverted from) rather than the version that was published previously (i.e., the version you reverted to).
   - If after reverting and reviewing the draft, you determine that you do not want to use it, you can discard the draft. This action will return the form to its current published version (i.e., the version that you just reverted from).
5. To ensure that users immediately are reverted back to the previous version of the form, select **Publish**.

Archive forms

Archiving a form makes it unavailable as an option for users to select when they create reports. When a form is archived, any reports created using the form before it was archived are NOT impacted in any way.

To archive a form:

1. Open Form Builder and switch to the tab containing the form.
2. In the **Actions** column, select **More actions [...] > Archive** for that form.
3. Select **Archive form** in the confirmation message window that appears.

> **Note**
>
> Archived forms can be unarchived by opening the form and selecting **Publish**.

Watch this video, starting at 03:50, for an overview of archiving forms.

Cards and fields

Use Form Builder to structure your forms and subforms by adding cards and organizing fields within them. When editing forms and subforms, you can create and manage cards, configure field types and properties, control layout with field widths, apply default values, and view restrictions for protected fields.

Cards

A card is a set of fields in a form that captures data related to a specific topic or entity. There are four types of cards:

- **Entity card:** Cards with a set of predefined fields.
  - Options include:
    - Names
      - This type of card will actually insert two cards: One for Persons and one for Organizations.
    - Person
    - Property
    - Vehicle
  - You can only add each entity card type once to a form. (i.e., A form can't contain two Vehicle cards.)
- **Blank card:** Empty cards you can customize by adding your own fields.

- **Rich text editor:** Cards that contain a large text editing area that lets users perform rich text formatting (such as adding bullets, headings, tables, etc.).

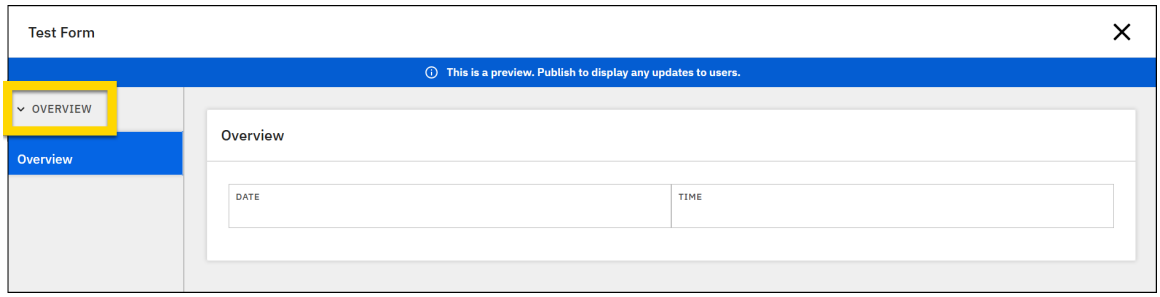
When a user creates a report based on a form, the form's cards appear in the left navigation menu in Report Writer.

When you add an entity card to a form, users see an **Add** button in the left navigation. They can select this to add multiple entities of the same type to a report (i.e., multiple people). This is not the case for the other card types (Blank, Rich text, Acknowledgement). If you configure one of these cards, it can only appear once in the report.

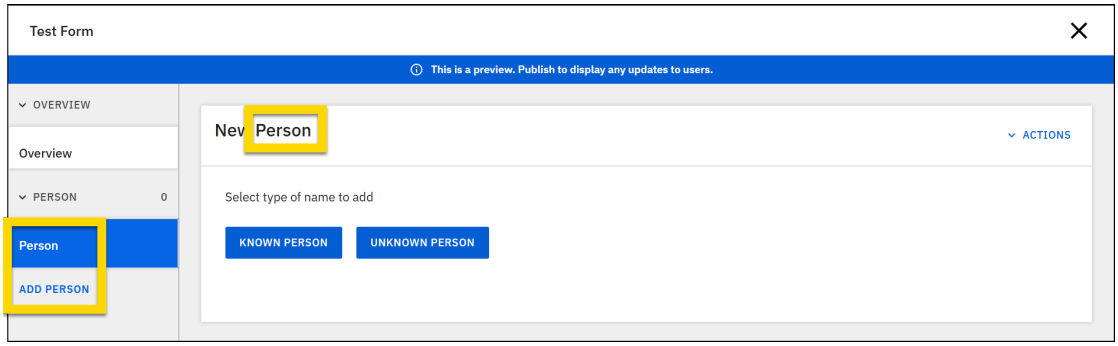
Add cards

To add a new card to your form:

1. Add a new card in one of two ways, depending on where you want it to appear in the form:
   - To add the card to the end of the form, select **Add card** on the left side of the page.
   - To add a card above or below an existing card:
     - Open the card you want your new card to appear before or after.
     - Next to the card description, select **More actions [...] > Insert before/after**.
2. Choose a card type (Acknowledgment, Blank, Entity, or Rich text editor).
3. Enter a card title.
   - This field only appears when you add a Blank card or a Rich text editor card. For the other card types, the card title can be edited later if you edit the card.
   - The card title appears in Report Writer in the left navigation menu as the title for that section of the report, which can be expanded or collapsed.



4. Enter a card description.
    - The card description appears in three locations in Report Writer:
        - The secondary item within each expandable section
        - The **Add** button (only appears for Entity cards)
        - The top of the central report writing area



5. Select **Add**.
6. After adding a card, you can add, edit, or remove fields.
7. After making changes to your form, preview and then publish it.

Watch this video for an overview of how to work with cards using Form Builder.

Edit cards

To modify an existing card:

1. Open the card you need to edit.
2. Next to the card description, select **More actions [...] > Edit**.
3. In the edit mode, you can edit either the card title or description.
4. Select **Add** after making changes.
5. After making changes to your form, preview and then publish it.

Remove cards

To modify an existing card:

1. Open the card you need to edit.
2. Next to the card description, select **More actions [...] > Remove**.
3. In the confirmation window that appears, select **Remove**.
    - You cannot restore a card after it has been removed.
    - If you remove a card and later decide you want to re-add it, you can do so. The card will be added to the form with its original set of fields.

Fields

Fields are where report writers enter information. Form builders can add, edit, and remove fields, control their width and default values, and organize them into sections and lists.

Add fields

You can add fields in several different locations on a card:

- At the end of a card
- At the beginning of a section or list
- At the end of a section or list
- In between two other fields

Watch this video for an overview of how to add and manage fields.

To add a field to the end of a card:

1. Select the card you want to add a field to.
2. Select **Add [card title] field**, at the bottom of the card.

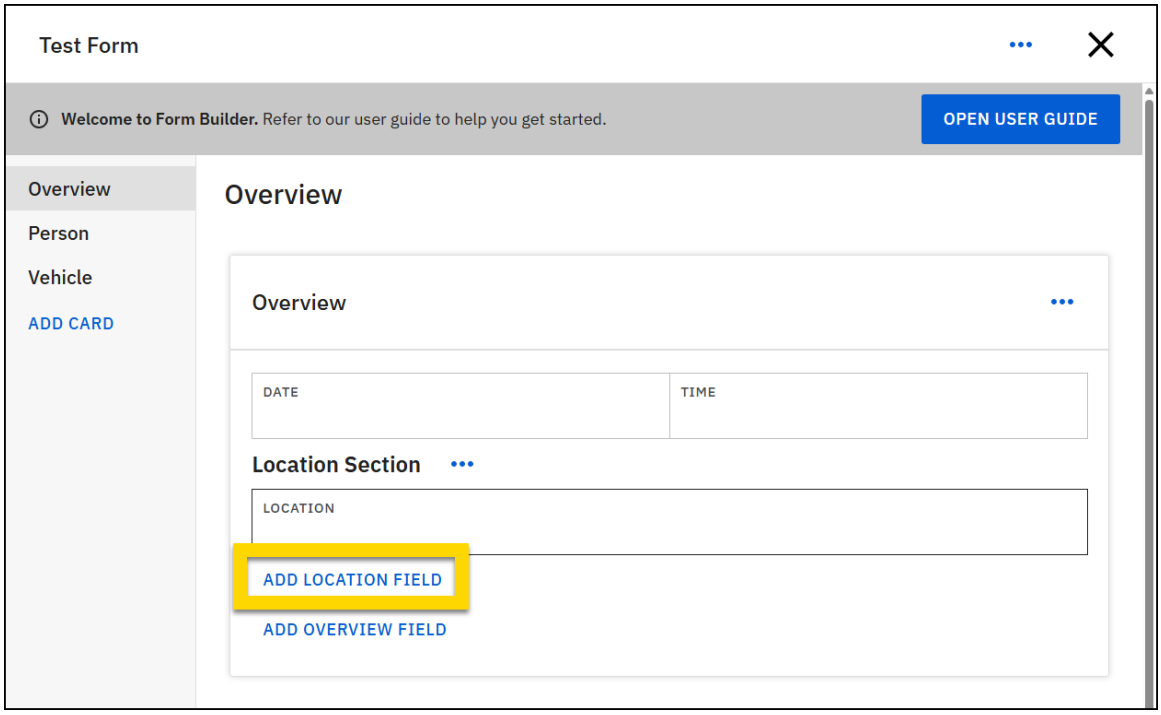
Sections and lists are types of field that can contain other fields. To add a field to the top of a section or list:

1. Find the section or list.
2. Select **More actions [...] > Insert after** beside the section/list name.

To add a field to the end of a section or list:

1. Select the card you want to add a field to.
2. Find the section or list you want to add the field to.
3. Select **Add [section/list name] field**, at the bottom of the section/list.
    - Be careful when adding fields to a section/list that appears at the bottom of the card. Select the **Add [section/list name] field** button rather than the **Add [card title] field** button to ensure the field is added to the end of the section/list, rather than below it.

- For example, in the image below, to add a field to the Location section, you would select **Add location field**, rather than **Add overview field** (Overview is the name of the card).



To insert a field between existing fields:

1. Select an existing field.
2. Choose **Insert before** or **Insert after**.

Note

You cannot add fields in between existing fields on Entity cards. Instead, new fields can only be added at the end of the card.

Edit field details

After adding a new field, or when editing an existing field, adjust the field details, including:

1. Select a field type.
2. Select the **Is this field required** checkbox to make the field mandatory and require it to be completed by all users who write reports using this form.
   - Incomplete required fields will trigger an error message and may prevent report submission.
3. Enter a field title that will appear above the field on the form.

4. Add a help message to provide guidance or instructions.
   - This message appears as an information icon ⓘ inside the field.
   - A Help Message can be added to all fields except Date & Time, Description, Location search, List, Multi-line text, Section, and Subform fields.
5. Choose a field width. This determines how much space the field occupies within the form. Multiple fields can appear on the same line until it is full.
6. For dropdown or checkbox group fields add options.
7. Add default values.
   - This option appears grayed out for field types that don't support default values.

Remove fields

Certain types of fields cannot be removed from a form:

- Fields on entity cards. The data entered in Entity fields contributes to the Master Name Index (MNI), so fields cannot be removed from Entity cards.
- Fields that have been added by Axon representatives

To remove all other types of fields:

1. Select the field.
2. Choose **Remove**.
3. Select **Remove** in the confirmation message.

View protected fields

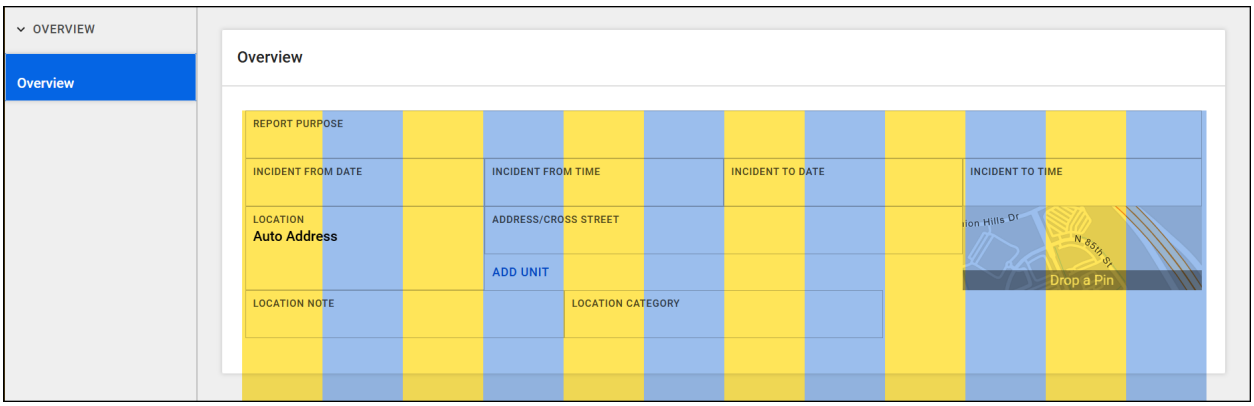
When editing a form, you may notice some fields are protected—meaning you can’t change or remove them. Hover over the **Remove** option for a field to see a message that explains why the field can't be removed.

- **MNI-required fields**: These fields are protected because they connect to the Master Name Index (MNI) database, which relies on specific fields. They cannot be edited or removed.
- **NIBRS-required fields**: These fields are protected to ensure compliance with NIBRS reporting standards. They cannot be edited or removed.
- **Other protected fields:** Fields that don't indicate they're protected due to NIBRS or MNI may be configurable. To edit or remove one of these fields, submit a request to Axon Support.

Set field widths

The display of fields in forms is controlled using an “invisible” 12-column layout.

The yellow and blue bars in the image below highlight the “invisible” columns in an example form.



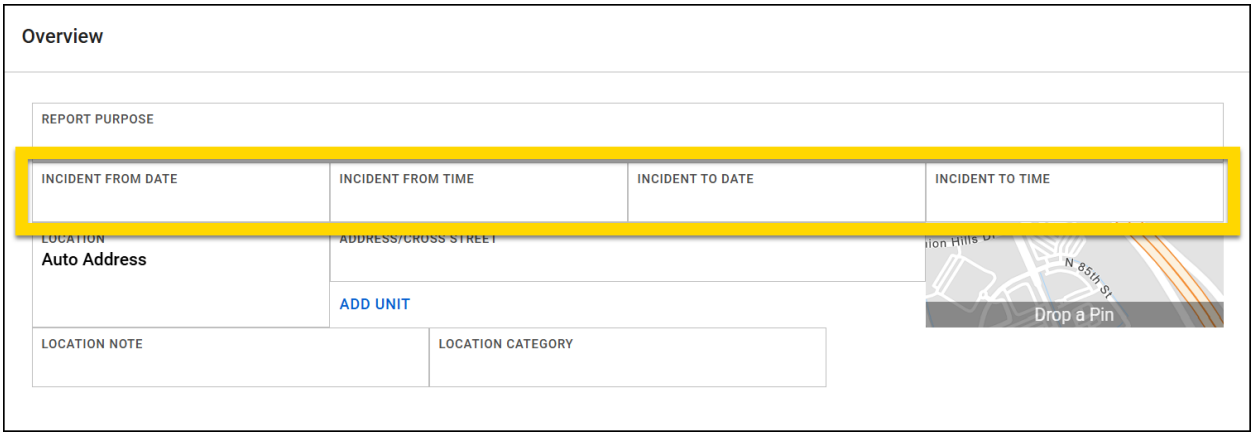
The **Field width** menu for each field indicates how many columns that field spans. The following options are available:

- **2/12:** The field spans 2 of the 12 columns.
- **3/12 (Quarter):** The field spans 3 of the 12 columns (or one quarter of the total width of the form).
- **4/12 (Third):** The field spans 4 of the 12 columns (or one third of the total width of the form).
- **6/12 (Half):** The field spans 6 of the 12 columns (or one half of the total width of the form).
- **8/12:** The field spans 8 of the 12 columns.
- **9/12:** The field spans 9 of the 12 columns.
- **10/12:** The field spans 10 of the 12 columns.
- **Full width:** The field spans the full width of the form.

Field widths don’t apply to checkbox fields; these fields always display at full width of the form. Additionally, these field widths you only apply to the form in Report Writer. They do not impact print templates, which determine how the fields appear when a report is printed.

When you add fields to the same section in a form, they are added, one after the other, to the same row until all columns are “full.”

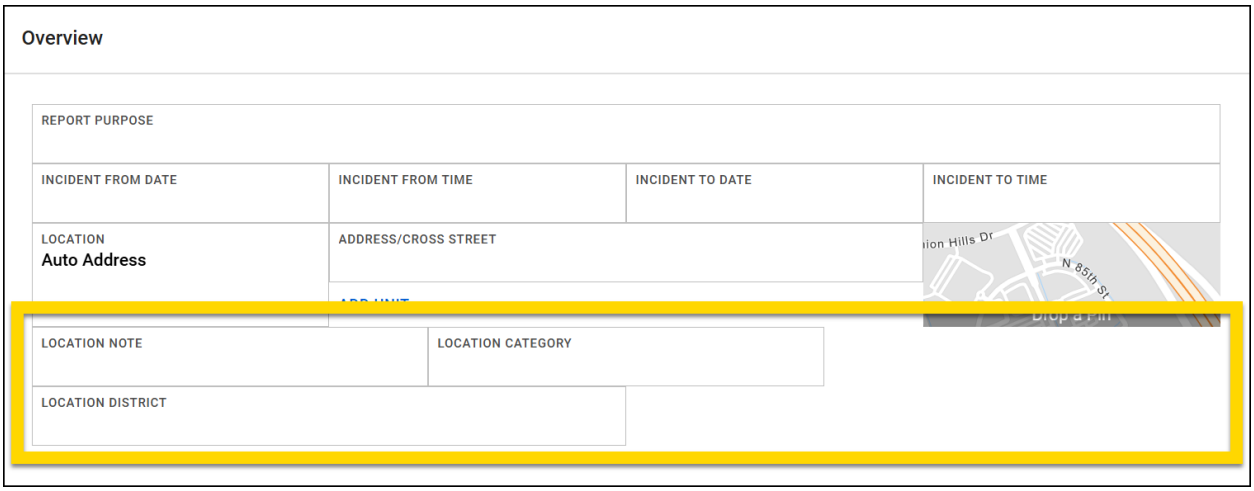
For example, in the image below, the width for each of the incident date and time fields is set to 3/12, indicating that each field spans three columns (taking up one quarter of total columns in the row).



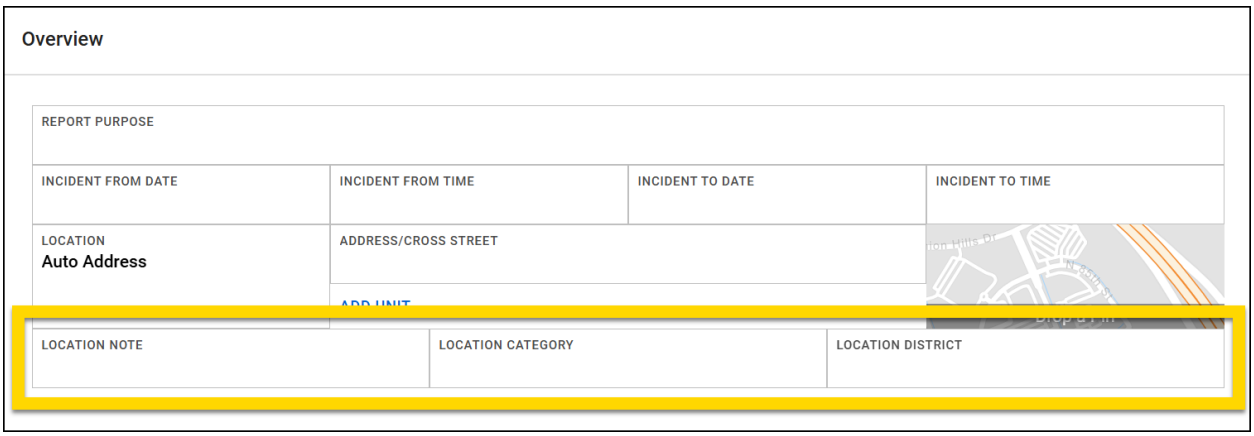
If you add a field to a row, and it won't "fit" in the row because too many columns are already taken up by existing fields, the new field appears in a new row.

Example

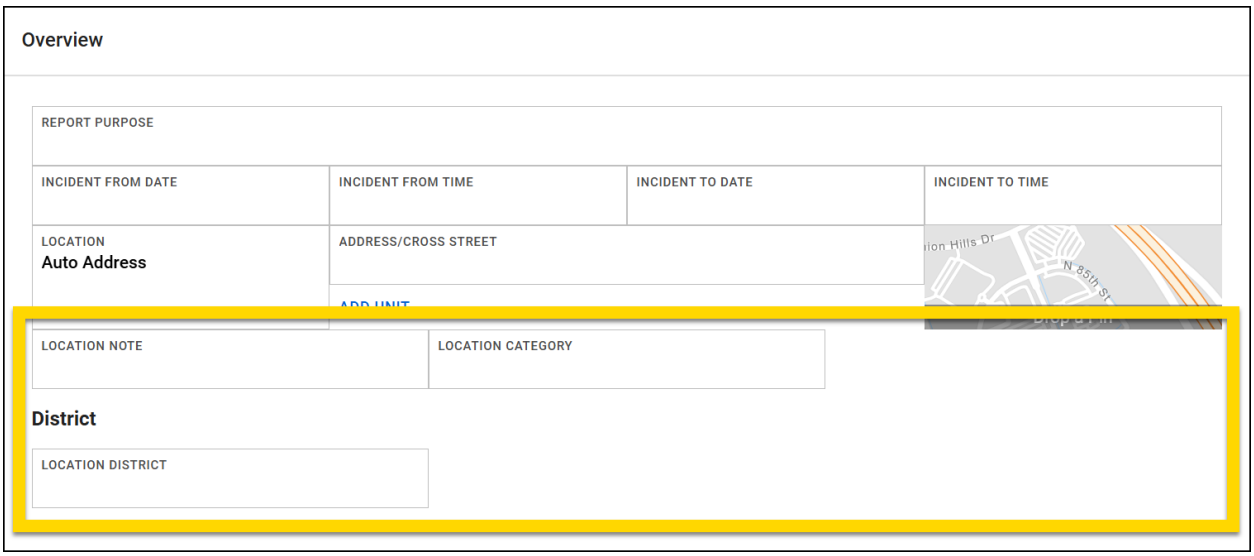
In the image below, the **Location note** and **Location category** fields each have a width of 4/12, leaving four columns in the row. When the **Location district** field is added with a width of 6/12, it doesn't fit on the same row as the other location fields and instead appears below them on its own line.



If the **Location district** field width is adjusted to 4/12, it is now the correct width to fit on the same row as the other location fields.



If the **Location district** field (still with a field width of 4/12) is instead added to a new section below the location fields, it remains in its own row, even though it could fit into the same row as the location fields in the section above it.



Add default values

When you add a field to a form, you can set a default value for the field. When a user writes a report using your form and comes to this field, the field will be pre-filled with the default value you set in Form Builder. This feature lets you pre-populate certain field types with known information or common responses, helping to streamline the report writing process. When users write reports that contain default values, they can overwrite these default values with information appropriate to their specific report.

There are three types of default values you can choose from: Metadata, User, and Insert the value from another field. Default values are only available for some field types. If default values are not available for a field type, the Default values section is grayed out.

Metadata

This type of default value automatically fills a field with system-generated information, including:

- Linked Incident or Crash ID
- Linked CFS ID, arrival location, arrival date/time
- Current officer name, ID, age (i.e., the name, ID or age of the user writing the report)

When entering a User default value for a **Single-line text** field, enter the information you want to automatically appear in the field. For all other field types, select an option from the ones presented in the **Default value** field. For example, if you want your form to auto-select the first option in a Checkbox group, select this option in the **Default value** field.

User

You, the Form Builder user, can create a custom default value that is auto-filled in a field. Report writers can modify this default when they are writing their reports.You can only add user default values for fields that are NOT related to NIBRS reporting.

Insert the value from another field

The field automatically pulls its value from another field in the form and is only supported for Single- and Multi-line text fields.

For example, you can configure the default value for Field B to be the same as whatever is entered in Field A (also called the source field). When report writers encounter fields with this type of default value in their reports, a refresh button ↻ is displayed on the field. If the source field is updated, a message can appear, notifying the report writer that the source field changed, and asking them if they want to update the linked field.

To add this type of default value to a field:

1. Add a field to a form.
2. In the Default values section, select **Insert the value from another field**.
3. In the **Insert value from** field, select the other field the value should be pulled from.
4. Optionally, select the **Upon refresh** checkbox.
   - If this checkbox is selected, a message automatically appears to the report writer when the source field value is updated, indicating that the field updated and asking if they want the linked field to be updated to match.
5. Optionally, add helper text that is displayed below the linked field, explaining why it is linked to another field.

Field types

There are multiple different field types available in Form Builder as explained in the sections below.

Search

There are several different types of search fields available. When a user enters text in these fields, Report Writer searches the system database and presents results.

Note

All Search fields are non-removable field types. Once you add and save these fields, you cannot remove them from your form.

Agency user search

This field lets report writers search for a user. The names that appear in this search are those who have accounts in Axon Evidence. For more information, see Adding a User.

Charge search

This field lets users search for charges or offenses. The items in this list come from your organization's Master Charge Table (MCT). Any changes to this list must made using the Master Charge Tool rather than in Form Builder.

Location search

There are two types of Location search fields you can add to a form: Event and Residential. The Location search field types include the following fields:

- Location: Options in this field vary between Event and Residential location search:
  - Event search includes:
    - Auto-address
    - Manual address
    - Cross streets
    - Mile marker
    - Unknown
  - Residential search includes:
    - Auto-address
    - Manual address
    - Homeless/transient
    - Unknown
- Depending on what a user selects from the Location field, different fields appear. See GIS and maps for a full explanation.

Organizational search

This field lets users search for organizations that have been added to your organization's reports (and therefore to your organization's Master Name Index).

Person search

This field lets users search for people that have been added to your organization's reports (and therefore to your organization's Master Name Index).

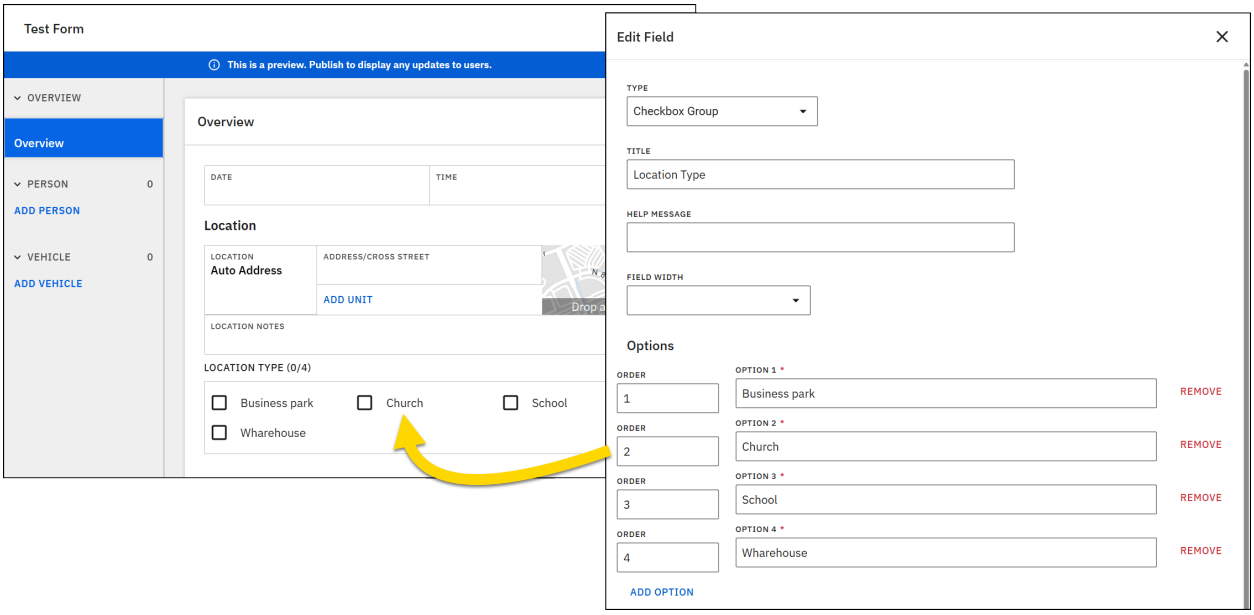
Checkbox group

This field displays a group of checkboxes report writers can mark.

When adding a checkbox group, give a name to the group (displayed above the list of checkboxes). Then, select **Add option** to create multiple checkboxes. Checkboxes are displayed in a three-column layout.

Each checkbox option can include:

- Order: Sets the order in which the checkbox item is displayed.
  - Lower numbers appear higher in the list.
  - Axon recommends ranking the most frequently selected option as 1.
  - The Order number indicates the order of the checkbox from left to right, not top to bottom. For example, if you set an option's order to "2", this option displays as the first option in the second column, not the second option in the first column.
- Option: The text displayed beside the checkbox



Note

If you enter options in your preferred order initially, you don't need to set the display order manually.

Dropdown

A Dropdown field provides a list of options for users can choose from. Users can select only one option.

Like Checkbox group fields, when creating dropdown options, you can optionally set the order of the option as well as providing the option text.

Additionally, each option in a dropdown can have a short code, which is a short set of numbers and letters that are added before the option text. Adding shortcodes helps users who know the shortcode find that option more quickly.

For example, in a dropdown list of state names, state abbreviations can serve as shortcodes. Typing the shortcode "AZ" takes users directly to Arizona, while typing "WA" brings up Washington.

Auto-complete dropdown

This field is similar to the Dropdown field type, but it instead contains two available options: Flag categories or Incident IDs. If you set this field to Flag categories, users will see a list of all flag categories (e.g., Juvenile, Domestic violence, etc.) that have been created for your organization. If you set this field to Incident IDs, users can search the list of all Incident IDs that have been created at your organization.

Yes/No

A Yes/No field is really a dropdown field with two options: Yes and No.

Dates and times

There are four different field types related to dates and times:

- **Date and time:** When you select this field type, both a Date and a Time field are inserted into your form.
- **Date:** Inserts only a Date field.
- **Time:** Inserts only a Time field.
- **Time with Seconds:** Inserts a Time field that allows users to enter seconds in addition to hours and minutes. All other Time fields only allow entry of hours and minutes.
- **Year:** Inserts a Year field to capture a four-digit year.

Text

You can use two types of text fields: Single-line and Multi-line.

The Single-line text field is takes up a single line of space in the form. It is used to visually indicate that the content to be added to the field should be brief.

Multi-line text fields can take up more space in the form to indicate that the content to be added to the field can be more expansive. Enter a number in the Row field to set how much space this field takes up in the form. It's recommended to avoid entering too large of a number to prevent the field from taking up too much space. Entering "6" results in a field that is larger but not too large.

When working with your Axon representative or Axon Support on print templates associated with this form, make sure that the corresponding print template field is also set as multi-line to prevent text from collapsing into a single line when printed.

Description

A Description field is displayed as read-only text to users when they write reports. You can use this field to provide instructions or other information to help users complete their reports.

When creating the field in Form Builder, the title you create for the field is not shown in Report Writer by default. Select the **Show title** checkbox to make it appear.

Note that the text you enter in the Description field does not appear in Form Builder when you are viewing the form. Select **Preview form** to view the text.

Numbers

There are various number-related fields you can add to your reports. Many of these fields auto-format the text that is entered into them to ensure data consistency.

Height

Heights can be entered in this field. The numbers entered into this field are auto-formatted as height and inches. For example, if a user enters "54" in a height field, it is auto-updated to "5-04".

Number

Number fields let users enter whole numbers and decimal values. A common use for this field type is a Weight field.

Monetary

Monetary values can be entered in this field. The numbers entered into this field are auto-formatted to include a dollar sign ($) and two decimal places (cents). For example, if a user enters "100" in a monetary field, it is auto-updated to "$100.00".

Phone number

Phone numbers can be entered in this field. The numbers entered into the field are auto-formatted as (111) 111-1111.

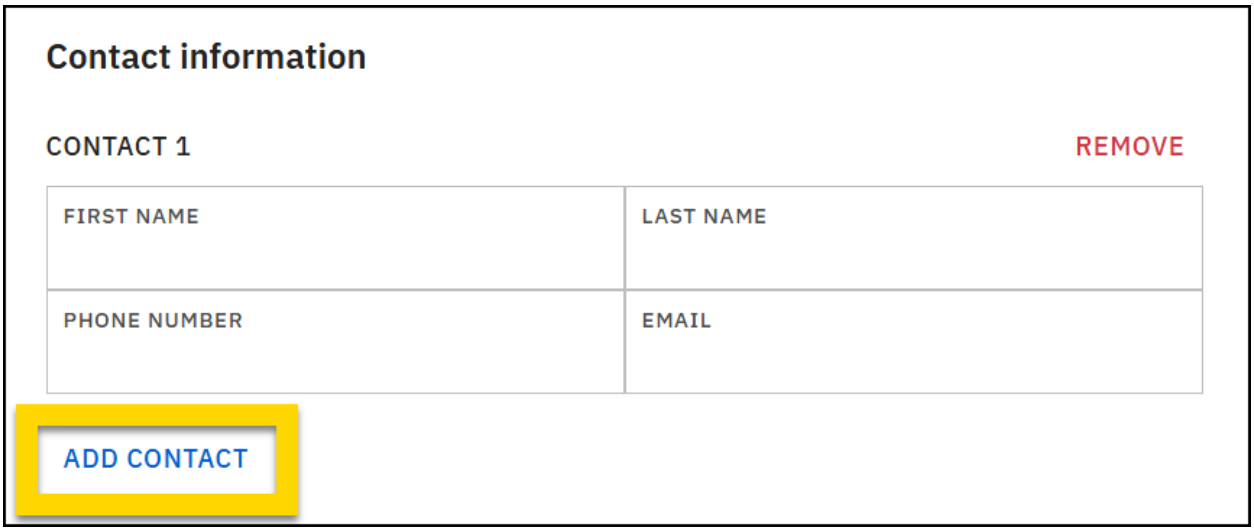
Social Security Number

Social Security Numbers can be entered in this field. The numbers entered into the field are auto-formatted as 111-11-1111.

List

A list is a type of field that contain a set of fields. When a user encounters a list in a report, they can add multiple sets of those fields to their report.

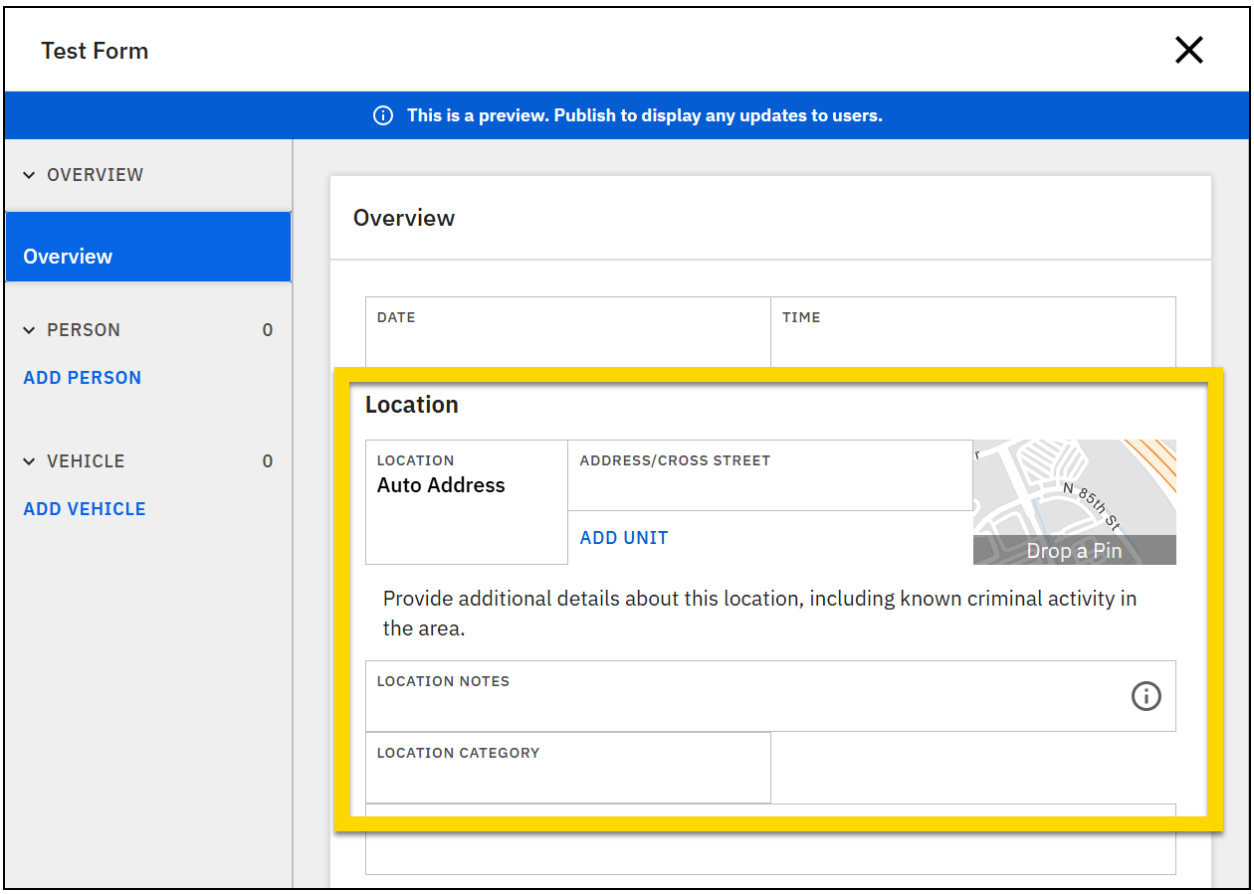
For example, you create a Contact Information section in your form and add a Contact list to the section. This list includes four fields for first name, last name, phone number, and email. When users create reports from this form, they see an **Add contact** button. When they select this button, a set of fields, labeled Contact 1, appears in their report. They can complete these fields, and select **Add contact** again to add another set of contact information fields.



Section

Like lists, a section is a type of field that contains a set of fields. Sections can be used to group related fields together and introduce a clear visual hierarchy to your form. When you add a section, the field title you enter is displayed as a heading in the form.

For example, you can add a Location section that has a Location heading and includes various location fields, including Location search, Location details. etc.



Subforms

Subforms are specialized sections that can be added to Entity cards (person, vehicle, property) to capture detailed information. They allow you to edit information specific to one instance without affecting others.

Create a subform when you need to:

- Manage repeated sets of information unique to multiple related entities within a single report
- Print certain information separate from the main report

In a scenario where an incident involves multiple arrests, a subform allows you to create separate arrest forms for each person involved, all within the same incident report. Each arrest form contains the same set of fields, but with unique information for each arrested individual.

Subforms also enable separate printing of specific information. For instance, a subform for towing allows you to print the vehicle removal information without including the full incident report.

Watch this video for an overview of how to use subforms in Form Builder.

Create subforms

Subform creation is currently not supported in Form Builder. If you need a new form, contact Axon Support or your Axon representative.

Edit subforms

To edit a subform, open Form Builder, switch to the **Subforms** tab, and select the blue hyperlink form name. When editing a subform, you can:

- Edit field titles
- Add or remove fields
- Add help messages to explain field requirements
- Adjust field widths

> **Note**
>
> When you edit a published subform, you create a draft of that form, and the edits you make are considered a "draft" until you publish the subform. This means that the changes you make in the form won't appear to users in Report Writer until you publish. When you do publish, your changes will appear in all forms the subform has been added to.

To avoid conflicting changes, only one person can edit a subform at a time. When another user is actively editing a subform, a lock icon appears beside the subform name and the status column displays the name of the person editing the form.

- To make urgent changes while someone else is editing, in the **Actions** column of that form's row, select **More actions [...] > Take over form**.
- Remember, if you take over a form from another user, any changes they've made will be lost.

Subform fields and sections can be edited from two different locations:

- Subforms tab: If you open and edit a subform from the Subforms tab, any changes you make will reflect across ALL forms that use the subform.
- Within a form: If you edit a subform while viewing the form, the edits you make will only reflect in that form and not across all forms that use the subform.

Edit from the Subforms tab

Follow these steps to edit a subform from the **Subforms** tab:

1. Open **Form Builder**.
2. Switch to the **Subforms** tab.
3. Select the blue hyperlink name of the subform to open it.
4. Adjust the sections and fields as desired.
   - Managing fields in subforms is the same as in forms. See Cards and fields for more information.
   - Managing sections in subforms is similar to managing them in forms with some minor differences as detailed below.
5. Note that you can edit the subform name by selecting **More actions [...] > Edit** (beside the subform name).
6. After making changes to your form, preview and then publish it.

Edit subforms within a form

Editing a subform within a form allows you to make changes specific to that form without affecting other instances of the subform.

> **Note**
>
> If you customize a subform within a specific form, any changes made to that subform from the Subforms tab will NOT carry over to this customized version of the subform.

To edit a subform within a form:

1. Open the form containing the subform.
2. Open the entity-backed card (offense, person, vehicle, or property) where the subform is located.
3. Scroll to the bottom of the card and select **Edit [subform name] subform**.
4. The subform expands to reveal all fields it contains. Adjust the sections and fields as desired. See Cards and fields for more information.
   - Note that you cannot add or remove subform fields when editing the subform from within a form. You must instead edit the subform itself from the **Subforms** tab.
5. After making changes to your form, preview and then publish it.

Add sections to a subform

As in forms, in subforms, fields can be added to sections to make the subforms easier to navigate. You can insert sections as explained in Cards and fields. However, in subforms, there is an **Add section** button, which behave slightly differently:

1. Scroll down to the bottom of the subform and select **Add section**.
   - You cannot add new sections above existing sections in a subform.
2. Choose a card type. Options include:
   - **Blank card**: Starts a blank card for you to add fields.
   - **Rich text editor**: Starts a card with a large text box.
3. Enter a card title and description.
   a. See Add cards for more information.
4. Select **Save**.
5. Add fields to the section as you normally would when adding fields to a form.

Watch this video for an overview of how to work with sections using Form Builder.

Add subforms to a form

1. Open Form Builder.
2. Select **Edit** on the form you want to modify, then open the Entity card you want to add the subform to.
   - Subforms can only be added to Entity cards, which include:
     - Names
     - Person
     - Property
     - Vehicle
   - See Add cards for more information.
3. Scroll to the bottom of the card and select **Add [card title] subform**.
4. Choose a subform from the list, then select **Add to form**.
5. After making changes to your form, preview and then publish it.

Remove subforms from a form

Like fields, a subform cannot be removed from a form if the form has been published. To remove a form:

1. Open the form that contains the subform.
2. Open the entity Card where the subform is located and scroll down to the subform.

3. Select **Edit [subform name] subform** to open the subform.
4. Next to the subform name, select **More actions [...] > Remove subform**.
5. When removal confirmation message appears, select **Remove**.
6. After making changes to your form, preview and then publish it.

Publish subforms

In order for a subform to be added to forms, it must be published. To publish a subform:

1. First, if you want to preview how the form will look, you must open a form that contains the subform and preview the form.
   - Once the form is in Preview, open the card containing the subform, scroll to the bottom, and select the button to add the subform to the form.
2. If the subform looks correct, open the subform from the **Subforms** tab.
3. Select **More actions [...] > Publish** next to the subform title.
4. In the confirmation message that appears, select **Publish** again.
5. Your subform is now published and can be added to forms. If the subform has already been added to any forms, they will be updated as well to show the changes to the subform.

Watch this video, starting at 01:42 for an overview of publishing subforms using Form Builder.

Discard subform drafts

As you can with forms, you can discard unpublished drafts of subforms to return the form to its last published version. For more information, see Discard drafts.

Privileges

Privileges let you control access to features and information in Axon Records and Axon Standards. Users are added to Command Hierarchy groups and/or teams, and are granted access as specified by the group or team privileges.

If a user is a member of multiple Command Hierarchy groups and teams, their privileges are determined by the group or team with the widest collection of privileges.

- For example: Jane Smith is a member of the Investigators team, which doesn't have the **View Domestic Violence Restriction** She is also a member of the Clerks team, which does have the **View Domestic Violence Restriction** privilege. As a result, Jane can view any report that has the **Domestic Violence** restriction (because she belongs to the Clerks team).

Similarly, privileges assigned to teams and groups work together, so users who are assigned to both teams and groups will have both sets of privileges.

- For example, Jane Smith is a member of the Investigators team, which doesn't have the **Access the Administrator Console** privilege is also a member of the Administration group in her agency's Command Hierarchy, which does have the **Access the Administrator Console** privilege. As a result, Jane can access the Administrator Console.

Note

Only privileges that apply to Axon Standards appear in this list. If your organization uses both Axon Records and Axon Standards, you may see additional privileges in the Administrator Console. See the Axon Records product guide for more information about these privileges.

To manage privileges, open the Administrator Console by selecting the gear icon in the main navigation menu. Select the Command Hierarchy & Teams tool, select a Command Hierarchy group or team, and switch to the **Privilege set view** tab.

Open the **Actions** menu to take actions on that group or team. Options include:

- Export users to CSV
- Export/import privileges to/from JSON
- Delete team

Use the search box to find a specific privilege or select a product filter to show only privileges related to that product (Axon Records or Axon Standards).

Privileges are organized into categories. Within each category are one or more subcategories. Finally, within each subcategory are one or more privileges. Categories, subcategories, and privileges are listed alphabetically.

Select the arrow to view all privileges in a subcategory. Select the **Allow** or **Prohibit** circles to adjust each individual privilege. Select **Allow all** or **Prohibit all** to enable or disable all privileges within that category. Some privileges have an information icon. Hover over this icon to view additional information about the privilege.

Manage Command Hierarchy Groups with privilege sets

A privilege set is a set of multiple privileges that can be applied to a Command Hierarchy Group. All users who belong to that Group are given the privileges in the privilege set. Each privilege set is associated with a team and can be viewed on the **Privilege set view** tab on the team's page.

Configuring privileges in this way enables the following administration benefits:

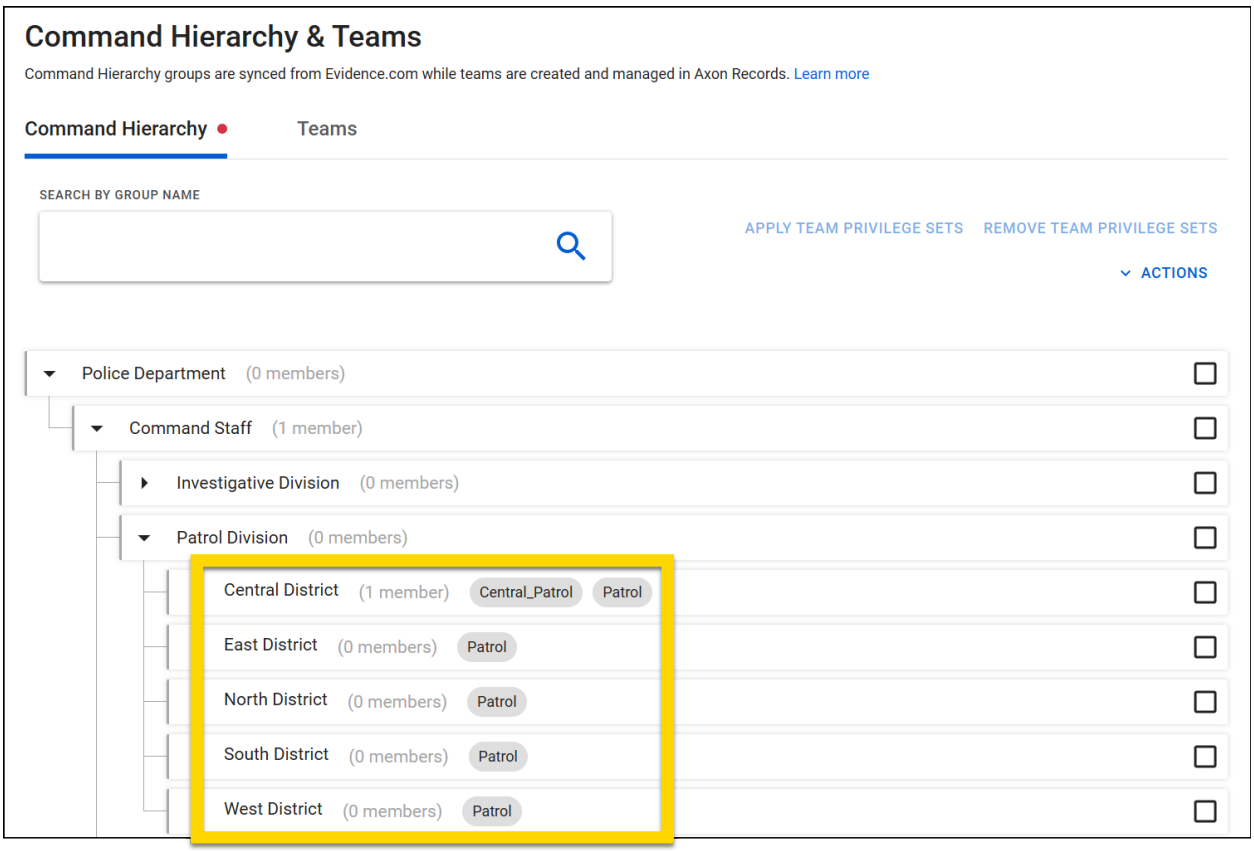
- **Batch configuration**: Avoid manual updates to each Command Hierarchy Group by applying and updating privilege sets in bulk.
- **Granular privilege assignments**: Combine privileges from multiple sets to create customized configurations for each Group.

For example, an organization has five Patrol Division Groups in their Command Hierarchy. Each member in these Groups needs the same privileges. Rather than opening each Group and individually applying privileges, the administrator creates a Patrol privilege set and applies it to all five Groups. As a result, all members of each of the five Groups are all granted the privileges contained in the privilege set.

Additionally, multiple privilege sets can be applied to a single Command Hierarchy Group, allowing for granular access control. Continuing with the Patrol example, the Central Division needs several more privileges than the other four Groups. The administrator creates an additional Central Patrol privilege set that contains only those additional privileges. When this privilege set is applied to the Central District Group, those users have both the Patrol and Central Patrol privileges.

The image below illustrates this example, showing each of the five Patrol Division Groups. The gray "Patrol" label beside each Group name is the privilege set that has

been applied to the Group. Note that an additional "Central_Patrol" label beside the Central District Group.



This configuration process involves the following steps:

1. Create Command Hierarchy Groups and add users to those Groups in Axon Evidence.
2. Create privilege sets.
3. Apply privilege sets to Command Hierarchy Groups.
4. Update privilege sets later as necessary.

Create privilege sets

To create a privilege set:

1. Open the **Command Hierarchy & Teams** tool in the Administrator Console.
2. Switch to the **Teams** tab.
3. Either open an existing team or create a new team.
4. Switch to the **Privilege set view** tab on the team's page.
5. Allow privileges as appropriate.

Apply privilege sets

After you have created the necessary privilege sets, you can apply them to your organization's Command Hierarchy Groups:

1. Open the **Command Hierarchy & Teams** tool in the Administrator Console.
2. While viewing the **Command Hierarchy** tab, select **Actions > Show team privilege sets**.
3. Select the checkboxes beside one or more Command Hierarchy Groups.
4. Select **Apply team privilege sets**.
5. Enter one or more privilege set names in the **Team Privilege Sets** menu.
   - If the Command Hierarchy Group already has applied privileges sets, you can choose to keep those existing sets and add the additional ones, or remove the existing sets in favor of the ones you have selected.
6. Select **Update** to apply your changes to the Command Hierarchy.

Note

You can add users to a team, thereby granting them all privileges in the privilege set associated with the team. However, it is recommended to manage user privileges either through Command Hierarchy Groups or with teams, not both.

Update privilege sets

After setting up your privilege sets and Command Hierarchy Groups, you can adjust them at any time. You can apply additional privilege sets, remove privilege sets from Groups, or update the privileges included in a Privilege Set.

To remove privilege sets from a Group:

1. Open the **Command Hierarchy** tab.
2. Select **Actions > Show team privilege sets**.
3. Select the checkboxes beside one or more Command Hierarchy Groups.
4. Select **Remove team privilege sets**.
   - Note that this options removes ALL privilege sets from the group.
5. Select **Remove** in the confirmation dialog box that appears.
6. The privilege sets are removed from the indicated Command Hierarchy Groups, but the Set itself is NOT deleted. It can still be managed from the **Teams > Privilege set view** tab and added to Command Hierarchy Groups.

To adjust the privileges contained within a privilege set:

1. Open the team
2. Switch to the **Privilege set view** tab.
3. Update as necessary.
4. Any changes made to the privilege set are automatically reflected in all Command Hierarchy Groups where that set has been applied.

Export and import privileges

To grant the same privileges as an existing team or group to another team or group, you can export and import privileges. To do this:

1. Open the team or group and select **Actions > Export privileges to JSON**.
2. Open an existing team or group or create a new one from the **Command Hierarchy & Teams** tool.
   - Command Hierarchy groups must be created from the Axon Evidence Admin Panel.
3. On the team or group page, select **Actions > Import privileges**.
4. Select the JSON file you exported from the existing team or group and select **Import**.

You can also export and import privileges for all teams or groups from the **Actions** menu on the main **Command Hierarchy & Teams** page. This function allows you to copy all existing teams and privileges to a new account. Contact your Axon representative for more information about this functionality.

Access

The following privileges related to accessing Axon products appear in the **Access** privilege category. In addition to accessing the product, users must have additional privileges to ensure they can take all appropriate actions once they have logged in.

Name	Description
Access Axon Records and view all Records reports	Lets users access Axon Records and view the list of reports in task inboxes. To open reports and take action on them, users must also have privileges in the workflows associated with each report type.
Access Axon Standards	Lets users access the Axon Standards product. Additional Axon Standards privileges must be enabled for specific functionalities.

Name	Description
Access the Axon app (mobile)	Lets users access Axon Standards features from within the Axon mobile app.

Activity logs

The following privileges related to the **Activity Log** tab (which appears on event/case profiles) appear in the **Activity Logs** privilege category:

Name	Description
Add manual activities to the Activity Log tab on Standards events	Lets users add activities to the activity log. Some activities are automatically added by the system.
Delete manual activities from the Activity Log tab on Standards events	Lets users delete activities from the activity log. Only activities that were manually added can be deleted. Activities added automatically by the system can't be deleted.
View the Activity Log tab on Standards events	Lets users see the **Activity Log** tab. If case tasks are enabled for your organization, activities taken on the case, reports associated with the case, and case tasks appear in the activity log.

Administrator Console

The following privileges related to accessing the tools in the Administrator Console appear in the **Administrator Console** privilege category.

You can grant access to the Administrator Console and ALL tools it contains using the *Access the Administrator Console* privilege. If you grant privileges for specific tools but do not grant the *Access the Administrator Console* privilege, users can still access the Administrator Console but only see tools for which they have been given privileges.

Name	Description
Administrator Console	
Access Agency Form Builder	Lets users access Agency Form Builder to manage forms.

Name	Description
Access the Administrator Console	Lets users access the Administrator Console by selecting the gear icon in the left navigation menu.
Manage Report Submission Settings in the Administrator Console	Lets users access the Report Submission Settings tool to manage which reports can and cannot be submitted if they contain validation errors.
Update Agency Announcement Banner	Lets users access the Announcement Banner Update tool to change the announcements banner that appears at the top of the My Tasks inbox.
View the Audit Log tool	Lets users access the Audit Log tool and export audit logs of actions users have taken in Axon Records and Axon Standards.
View the Command Hierarchy and Teams tool	Lets users access the Command Hierarchy and Teams tool to view the organization's Command Hierarchy and teams, as well as manage privileges.
View the Feedback Notes tool	Lets users access the Feedback Note tool to manage the types of feedback notes that appear in the Personnel module.
View the Inbox Manager	Lets users access the Inbox Manger tool.
View the Personnel data tool	Lets users access the Personnel data tool to upload data into the Personnel module.
View the Restrictions tool	Lets users access the Restrictions tool to manage the organization's restriction categories.
View the Rule Manager	Lets users access the Rule Manger tool.
View the Team management tool	Lets users access the Team management tool to manage the organization's teams. This privilege should only be used for organizations that do not use Command Hierarchy.
View the User Districts tool	Lets users access the District tool to manage the organization's districts.
View the User management tool	Lets users access the User Management tool to view the organization's users and manage their team memberships and view their Command Hierarchy Group assignments.
View the Workflow Manager	Lets users access the Workflow Manger tool.
Master Charge Table	
Access the Master Charge Tool	Lets users access and manage organization's list of charges from the Master Charge tool.
Master Location Tool Management	

Name	Description
Access the Master Location Tool	Lets users access and manage the organization's location list from the Master Location tool.
View locations	Lets users view the organization's location list from the Master Location tool.

Analytics

The following privileges related to the Analytics module appear in the **Analytics** privilege category:

Name	Description	Additional required privileges
Access		
Access the Analytics module	Lets users access the Analytics module.	View privileges for specific dashboards
View the [Dashboard] name dashboard	Lets users view the specified dashboard. A View privilege is associated with each of the agency's dashboards.	Access the Analytics module
Dashboard Management		
Archive user dashboards	Lets users archive user dashboards from within the Analytics module.	Access the Analytics module
Create user dashboards	Lets users create user dashboards from within the Analytics module.	Access the Analytics module
Delete user dashboards	Lets users delete user dashboards from within the Analytics module.	Access the Analytics module
Edit user dashboard titles, tabs, and visualizations	Lets users edit dashboard titles, tabs, and visualizations from within the Analytics module.	Access the Analytics module
Dashboard Management (Administrators)		
Delete template dashboards	Lets users delete dashboards from the Administrator Console.	

Name	Description	Additional required privileges
Edit template dashboards	Lets users edit dashboards from the Administrator Console.	
Show and hide dashboards	Let's users make a dashboard visible to / hidden from users.	
Upload template dashboards	Lets users upload template dashboards to the Administrator Console	
Export		
Export dashboards to CSV and PDF	Lets users view export dashboards they have access to from the Analytics module.	• View privileges for specific dashboards • Access the Analytics module

Cases - Standards

The Case Management module uses a privileges model to control access to data and actions. There are two primary types of privileges:

- Static privileges: Control what users can see and access (i.e., the buttons and options that appear when a user opens an inbox, case, or investigation)
- Workflow privileges: Control what actions users can take based on the current state of that work item (e.g., Draft, Review, etc.)

Together, these privileges ensure sensitive case and investigative data is only accessible to authorized users and enable organizations to enforce their own operational processes.

The privileges related to the Case Management module appear in the **Cases - Standards** category as shown in the table below.

Name	Description	Additional required privileges
Access		
Access the {case task inbox name} case task inbox	A task inbox privilege is associated with each specialized team inbox that has been configured for the organization. Users with this privilege can access that team inbox and the tasks that have been assigned to it. Typically granted to specialized team members who work on tasks.	

Name	Description	Additional required privileges
Access the Agency Overview inbox	Lets users view all cases and investigations in the Agency Overview inbox. Typically granted to Detective Supervisors.	To take actions on cases and investigations, users must also have that unit's Triage cases or Supervise active cases privilege, or the Supervise cases in the Agency Overview inbox privilege.
Case assignment		
Be assigned to {unit name} cases	Lets users be assigned to the indicated unit's cases and investigations, and manage these active and closed cases from their My Inbox. Typically granted to Detectives.	To manage the unit's active or triage cases and investigations from the unit's inbox, a user must have the unit's Supervise active cases and Triage cases privileges.
Create		
Create cases	Lets users create cases manually by selecting **Create case** from the **More actions** menu on event profiles. Typically granted to Detective Supervisors.	
Create investigations	Lets users create investigations by selecting **Create investigation** in the Case Management module. Typically granted to Detective Supervisors.	
More actions		
Access Detective Notes for units' cases	Lets users view and edit the **Detective notes** field on tasks. Typically granted to Detectives.	
Edit task due date	Users with this privilege can edit the due dates for templated tasks in cases and investigations. (Templated tasks are tasks that are automatically generated when the case/investigation is created.) Due dates for user-created tasks can be edited by users with this privilege or the user who created the task, even if they do not have this privilege.	

Name	Description	Additional required privileges
Manage case shares with external partners	Lets users access the **Manage shares** option in the **More actions** menu, which allows them to manage cases and investigations that have been shared with organizations and users. Typically granted to Detectives.	
Update case dispositions for any units' cases	Lets users update the disposition of any case or investigation, regardless of whether or not they can access the unit inboxes for those cases and investigations. Typically granted to Records Clerks.	Users must also have the following privileges: • Update internal case dispositions for your units' cases If your organization follows a review process for disposition updates, users must also have privileges in the following workflows: • Case Disposition Update
Update internal case dispositions without supervisor review for your units' cases	Lets users update the internal disposition of any case or investigation without a supervisor case review. Typically granted to Detective Supervisors.	Users must also have the following privileges: • Update internal case dispositions for your units' cases Additionally, users must also have privileges in the following workflows: • Case Disposition Update
Update internal case dispositions for your units' cases	Lets users update internal dispositions for cases and investigations assigned to their units. Some disposition updates require a supervisor case review. Typically granted to Detective Supervisors and Detectives.	Users must also have privileges in the Case Disposition Update workflow.
Supervise active cases		
Supervise active {unit name} cases	Lets users: • Access and manage the unit's active cases and investigations • Assign the unit's active cases and investigations to lead detectives • Transfer cases and investigations to other units Typically granted to Detectives.	To manage the unit's triage cases and investigations, a user must also have the unit's Triage cases privilege.

Name	Description	Additional required privileges
Supervise cases in the Agency Overview inbox	Lets users: • View all active cases and investigations in the Agency Overview inbox • Transition cases and investigations from active to closed • Reassign cases (between detectives in the unit or to another unit) Typically granted to Detective Supervisors.	
Triage		
Triage {unit name} cases	Lets users: • Access and manage the unit's triage cases and investigations • Assign the unit's triage cases and investigations to lead detectives • Transfer the unit's triage cases and investigations to other units	To manage the unit's active cases, a user must also have the unit's Supervise active cases privilege.
Triage cases	Cases and investigations not yet assigned to a unit appear in the No Unit Assigned inbox. This privilege lets users assign these cases and investigations to a detective in a unit.	

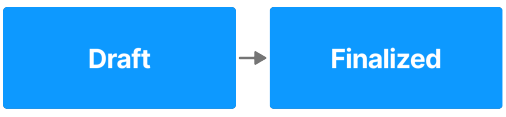
Workflows

Once created, dispositions, documents, and tasks move through a workflow, for example, Draft → Detective Review → Finalized. Each state is associated with multiple privileges, which give you granular control over which users can take on a disposition, document, or task, based on its current state.

The following workflows are used in the Case Management module:

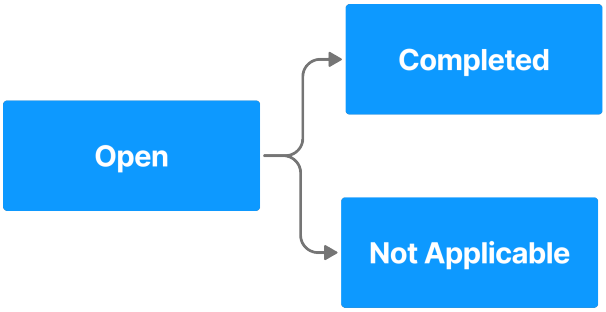
Case Summary and Case Documents

Summaries and documents do not require a review. These items move through a workflow that contains two states:



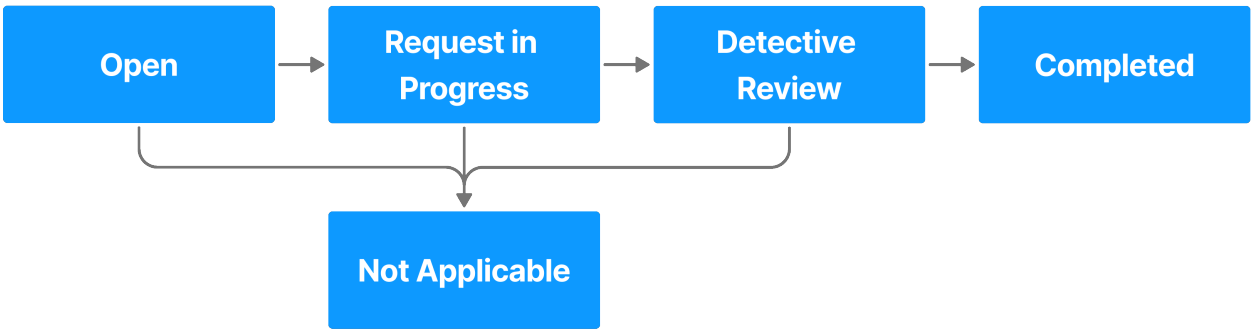
Case Task Default

Tasks that do NOT require a detective review move through the following workflow. Completed tasks can be reopened as necessary.



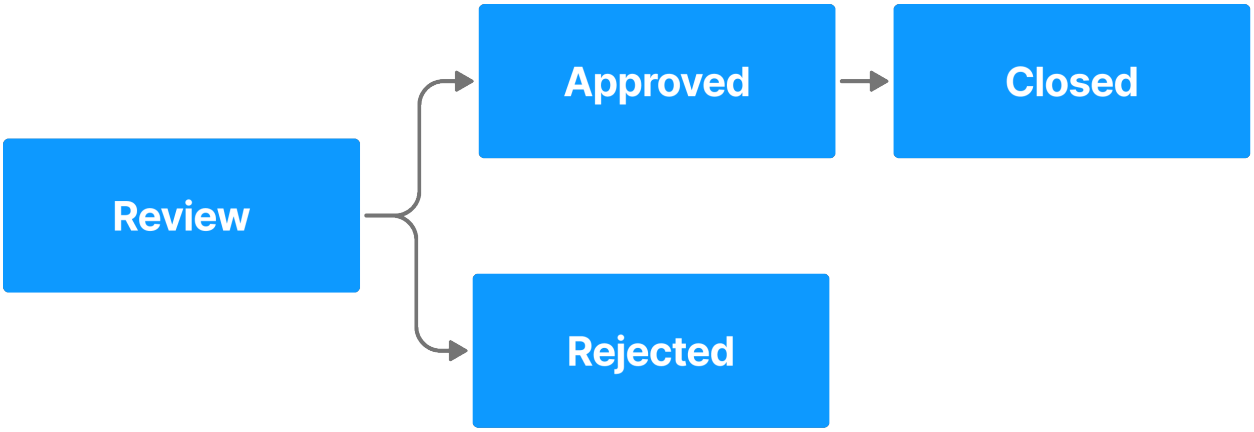
Case Task Review

Tasks that require a detective review move through the following workflow. Tasks can be marked as Not Applicable at any time, and completed tasks can be reopened as necessary.



Case Disposition Update

Disposition updates that require a supervisor review move through the following workflow. Supervisors only need to approve or reject disposition updates. The Approve → Closed transition happens automatically.



The privileges for workflows appear at the end of the **Cases** category. Each workflow has its own subcategory, and within that subcategory, privileges are sorted by state. The states are listed alphabetically, not by the order in which they appear in the workflow. For example, Finalized, which is the final state, appears before Review.

The hover tooltip for the first state in the workflow provides additional details about the workflow as a whole and not just that workflow state.

The table below explains how each workflow privilege works. Keep the following in mind when reviewing this table:

- This table is an exhaustive list of all possible workflow privileges.
  - Not every workflow contains the states listed in the table.
  - Some workflows may have a state but not all privileges associated with the state as shown in the table.
- For consolidation purposes, a single Review state is listed, although some workflows may have multiple Review states.

Name	Description	Additional required privileges
Add comments *States: Draft, Open, Request in Progress, Review, Approved, Rejected*	Lets users add comments in the report sidebar.	

Name	Description	Additional required privileges
Assign tasks to others *States: Draft, Open, Request in Progress, Review, Approved*	Lets users reassign tasks (currently assigned to themselves or to other users) to other users.	Users must also have the Case assignment privilege for the unit the task is associated with.
Assign tasks to themselves *States: Draft, Open, Request in Progress, Review, Approved*	Lets users reassign tasks currently assigned to themselves to other users.	Users must also have the Case assignment privilege for the unit the task is associated with.
Create tasks *States: Draft, Open, Review*	Lets users create tasks.	To create disposition review requests, users must also have More actions - Update case dispositions privileges.
Revert finalized reports *States: Finalized, Completed, Not Applicable*	Lets users revert finalized documents and reopen tasks.	
Submit tasks from the {State name} state *States: Draft, Open, Request in Progress, Review, Approved, Rejected*	Lets users approve and reject tasks in the indicated state. When a task is approved, it moves to the next state in the workflow. When a task is rejected, it moves to the Draft state.	To perform disposition reviews, users must also have More actions - Update case dispositions privileges.
View tasks *States: Draft, Open, Request in Progress, Review, Approved, Rejected, Not Applicable, Closed*	Lets users view tasks.	Users must also have the Access privileges for a unit to view tasks in that unit's inbox.

Early Intervention System (EIS)

The privileges related to the EIS module appear in the **Early Intervention System** category as shown in the table below.

Within this category there are "static" privileges, as well as workflow privileges. Generally, the static privileges determine which buttons and options appear to users when they open an alert. The workflow privileges determine which actions a user can take on an alert, depending on its current state (New, IA Review, etc.).

Name	Description	Additional required privileges
Access		
Access the Agency Alerts inbox	Lets users access the Agency Alerts inbox.	To view alerts within this inbox, users must also have View tasks workflow privileges.
Access the My Alerts inbox	Lets users access the My Alerts inbox.	To view alerts within this inbox, users must also have View tasks workflow privileges.
Analytics		
Access the EI dashboard in the Analytics module	Lets users view the EI Dashboard.	Users must also have the following privileges: • View all data for the agency in the EI dashboard in the Analytics module • View the EI dashboard (appears in the Analytics category)
View all data for the agency in the EI dashboard in the Analytics module	Lets users view data for the entire organization in the EI Dashboard.	Users must also have the following privileges: • Access the EI dashboard in the Analytics module • View the EI dashboard (appears in the Analytics category)

Workflows

Once created, an EIS alert moves through a workflow. Each state is associated with multiple privileges, which give you granular control over which users can take actions on an alert, based on its current state. EIS alerts can be updated to various states, and can move between any of these states at any time:

- **IA Review** (Internal Affairs review)
- **Review** (Supervisor review)
- **Chain of Command Review**
- **Secondary Review**
- **Intervention Pending**
- **Resolved** (The alert has been addressed with the appropriate interventions.)
- **False Positive** (The alert incorrectly indicated that an intervention was needed.)
- **Acknowledged** (After reviewing, the supervisor decided that no action was necessary.)

The privileges for workflows appear at the end of the **Early Intervention System** category. Each workflow has its own subcategory, and within that subcategory, privileges are sorted by state. The states are listed alphabetically, not by the order in which they appear in the workflow. For example, Acknowledged, which is a resolved state, appears before New.

The hover tooltip for the first state in the workflow provides additional details about the workflow as a whole and not just that workflow state.

The table below explains how each workflow privilege works:

Name	Description	Additional required privileges
Add comments	Lets users add notes directly to the Activity Log when updating an alert status	• Access the My Alerts inbox • View all data for the agency in the EI dashboard (if the user needs to act on all alerts, not just their own) • Access the Administrator Console
Assign tasks to others	Lets users assign alerts to other users.	
Assign tasks to themselves	Lets users assign alerts to themselves.	
Submit tasks from the {State name} state	Lets users update the status of an alert	
View tasks	Lets users view alerts in that state	

Flags

The following privileges related to flags that are added to profiles appear in the **Flags** privilege section.

Name	Description	Additional required privileges
Add, edit, and archive flags from profiles	Lets users add, edit, and remove flags on profiles.	
Delete flags from profiles	Lets users remove (archive) flags from profiles.	

Name	Description	Additional required privileges
Manage flag categories in the Administrator Console	Lets users create and edit flag categories (e.g., Detective Contact), which can then be added to profiles.	Users must also have the Access the Administrator Console privilege to access the Flags Configuration tool in the Administrator Console.
View flags that have been added to profiles	Lets users see flags that have been added to profiles.	

Linking

The following privileges related to incident and report linking appear in the **Linking** privilege category.

Name	Description
Incidents	
Link and unlink incidents and Standards events to other incidents	Lets users relate incidents and events to one another
Reports	
Link and unlink standalone reports to Records incidents	Lets users link a standalone report to a Axon Records incident.

Personnel

The privileges related to the Personnel module appear in the **Personnel** privilege category.

Note

These privileges MUST be applied to Command Hierarchy Groups. They do not apply to teams.

Access to the Personnel data tool is controlled by the *View the Personnel data tool* privilege in the Administrator Console privilege category.

The remaining Personnel privileges, which grant control to the module, are contained in the **Personnel** privilege category.

There are five groups of Personnel privileges, each associated with a different type of user (all officers, direct reports, etc.). Each group contains both **View** and **Edit** privileges, letting you specify if you want all users in the Command Hierarchy group with that privilege to be able to view or edit that section of the Personnel profile for the specified user group:

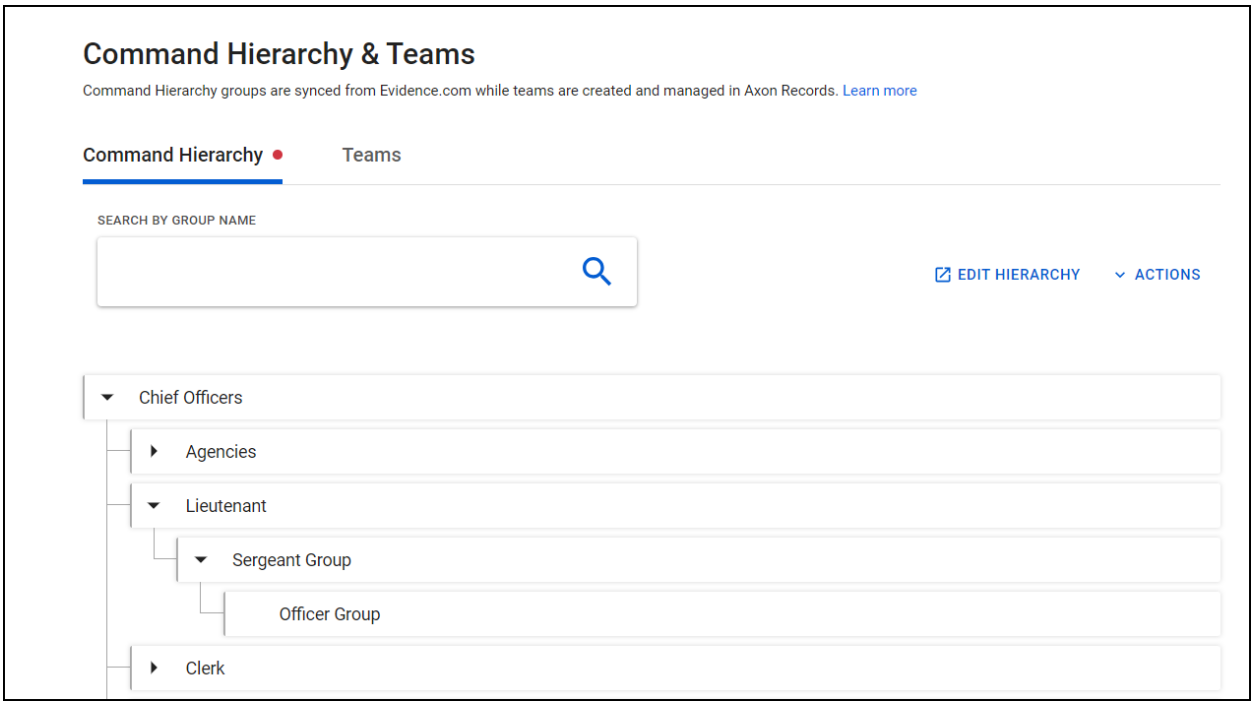
- **All users**: Lets users view or edit profiles for all officers at the agency
- **Direct reports**: Lets users view or edit profiles of users reporting directly to them
- **Indirect reports**: Lets users view or edit profiles of users who report to their direct reports
- **My Profile**: Lets users view or edit their own profiles
- **Peers**: Lets users view profiles for other users at their same level. There are not privileges that allow editing peer profiles.

Within each **View** or **Edit** privilege group you can specify which areas of the Personnel users with that privilege can view or edit.

- **Audit log**: Lets users view the audit log on a profile. An Edit privilege is not available for the audit log.
- **Commendations and awards:** Lets users edit or view commendations or award records.
- **Contact & Personal Info:** Lets users edit or view sensitive information, including SSN/National ID, and personal contact information
- **Demographics:** Lets users edit or view demographic information.
- **Discipline:** Lets users edit or view disciplinary records.
- **Performance review:** Lets users edit or view performance review records.
- **Photo:** Lets users remove or add a user's photo.
- **Promotions:** Lets users edit or view promotion records.
- **Related reports:** Lets users view related reports. An Edit privilege is not available for related reports.
- **Service history:** Lets users edit or view a user's service history records.
- **Status:** Lets users edit a user's status from "Active" to "Inactive"

To understand how different Command Hierarchy Groups relate to one another, take this example:

- The Sergeant group is a **Direct Report** of the Lieutenant group.
- The Officer group is an **Indirect Report** of the Lieutenant group, as they report directly to the Sergeant group, which in turn reports directly to the Lieutenant.
- The Clerk group is on the same hierarchical level as the Agencies or Lieutenant group. These three groups are **Peers**.



Profiles

Privileges related to citizen profiles appear in the **Profiles** privilege section.

Name	Description
Officer Profiles	
Access Officers Search and view officer profiles in Standards	Lets users search for and view officer profiles in Axon Standards.
Edit officer profiles from Officers Search in Standards	Changes made to profiles from Officers Search also reflect in the Personnel module.
Person Profile Management	
Edit Profiles	Lets users edit person information directly from citizen profiles. Users who do not have this privilege can still update a person's profile by adding them to a report and editing their information in the report.
Person Profile Photos*	

Name	Description
Delete photos from profiles	Lets users delete profile photos. Use this privilege rather than Manage profile photos if you want a user to be able to delete profile photos but not edit other photos that have been added to the profile.
Manage profile photos (edit, set default photo, upload, delete, etc.)	Lets users edit, set default photo, upload, take, and delete profile photos. This is an all-inclusive privilege that lets users take all photo actions. Use the Delete and Manage privileges if you want users to only be able to upload or delete photos.
Upload and take profile photos	Lets users upload and take profile photos. Use this privilege rather than Manage profile photos if you want a user to be able to add photos to a profile but not be able to edit photos that have already been added.

* These profile privileges also apply to vehicle profile photos.

Reports - Standards

The privileges related to report writing appear in the Reports and Axon Standards and Reports - Standards categories as shown in the tables below.

Within these categories, there are "static" privileges, as well as workflow privileges. Generally, the static privileges determine which buttons and options appear to users when they open an inbox or report. The workflow privileges determine which actions a user can take on a report, depending on its current state (Draft, Review, etc.).

In addition to these **Reports** privileges, users must also have Task Inboxes privileges to access reports from task inboxes.

Reports - Records and Standards

Name	Description	Additional required privileges
Create		

Name	Description	Additional required privileges
Create reports	Lets users create any type of report in Axon Records and Axon Standards. Users must have this privilege in addition to all other privileges to create specific kinds of reports.	Users must also have the following privileges in the report's workflow: • Draft State - Create Tasks • Draft State - Submit tasks from the Draft State Additionally, users must have **Create** privileges for the reports the user must be able to create.
Edit		
Review and edit in-progress reports	Reveals a **Review and edit** action in the **More actions [...]** menu in Report Writer. With this privilege, users can edit an in-progress report while it is in any Review state except for the Finalized state. (Users must be assigned to the report to Review and Edit it.) This privilege applies to all Records reports, including contributions.	Users must also have the following privileges in the report's workflow: • Draft State - Create tasks • Draft State - Submit tasks from the Draft state
Print		
Configure print options and settings	Lets users adjust the printing options and settings when they are printing reports. Without this privilege, users can still print but not adjust any print settings.	
Print reports	Lets users print reports.	
Self-finalize		
Self-finalize supplement reports	Lets users finalize supplements they have created.	
Write		
Generate draft narratives using the AI-powered Draft One	Lets users use Draft One to generate draft narratives for reports.	

Reports - Standards

Name	Description	Additional required privileges
Create		
Create Standards reports	This privilege must be enabled to let users create any reports in Axon Standards.	Users must also have the following privileges in the report's workflow: • Draft State - Create tasks • Draft State - Submit tasks from the Draft state
Custom Names		
Edit the custom names of Standards reports, case documents, and case tasks	Lets users edit report and document names even if they don't have the **Create tasks** workflow privilege that would allow them to create that type of report. Some report names can't be edited, including: incident reports, bookings, property reports, permits, and warrants.	
Delete		
Delete author-owned fields	Author-owned fields are fields a report author adds to a report that only they can edit or remove. This privilege lets users delete author-owned fields other uses have created.	
Delete in-progress Standards reports	Lets users delete reports that are in any state (Draft, Supervisor Review, etc.) except the Finalized state.	Users must also have the *Finalized State - View tasks* privilege in the report's workflow.
Finalize		
Finalize Standards reports	Lets users select **Finalize report** on the routing screen when submitting a report. When this option is selected, the report is immediately moved to the Finalized state without further review. When this privilege is enabled, the **Finalize report** option appears for all report types.	

Name	Description	Additional required privileges
Revert finalized Standards reports	Lets users revert finalized reports. The report is moved back to the Review state.	
Reassign		
Change the author of in-progress Standards reports	Lets users change the author of an in-progress report while it is in the Draft status.	
Reassign Standards reports	Lets users change the author of a report while it is in a Review status.	
Share		
Share reports	Let users share reports by sending a message to users, teams, and Command Hierarchy groups.	
View		
View all Standards reports	This master switch allows users to view all reports in any state.	To allow users to only view reports based on their state, use the *View tasks*workflow privileges in the states the user should be able to view.
View finalized Standards reports	Lets users view all finalized reports, regardless of the workflow they belong to.	To allow users to only view reports based on their workflow, use the *Finalized State - View tasks*workflow privileges.

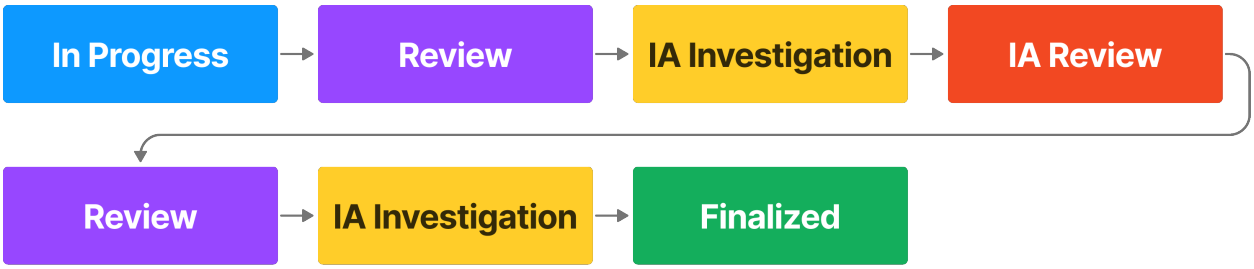
Workflows

Once created, a report moves through a workflow, for example, Draft → Review → Finalized. Each state is associated with multiple privileges, which give you granular control over which users can take actions on a report, based on its current state.

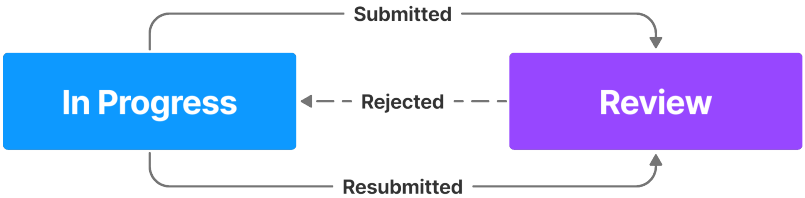
Workflows in Axon Standards generally include the following states:

- Draft (In Progress)
- Review
- IA Investigation
- IA Review
- Finalized

Standards workflows are flexible; reports do not move in one direction through the workflow (i.e., In Progress → Review → IA Investigation → Finalized.). Instead, reports can move between any of the states. For example, a report can move through the workflow as follows:



If a report is rejected at any point, it is returned to the original author who can revise and resubmit it for review.



For more information, see Create Axon Standards Workflows.

The privileges for workflows appear at the end of the Reports - Standards category. Each workflow has its own subcategory, and within that subcategory, privileges are sorted by state. The states are listed alphabetically, not by the order in which they appear in the workflow. For example, Finalized, which is the final state, appears before Review.

The hover tooltip for the first state in the workflow provides additional details about the workflow as a whole and not just that workflow state.

The table below explains how each workflow privilege works. Keep the following in mind when reviewing this table:

- This table is an exhaustive list of all possible workflow privileges.
  - Not every workflow contains the states listed in the table.
  - Some workflows may have a state but not all privileges associated with the state as shown in the table.
- For consolidation purposes, a single Review state is listed, although some workflows may have multiple Review states.

Name	Description	Additional required privileges
Add comments *States: Draft, Review*	Lets users add comments in the report sidebar.	

Name	Description	Additional required privileges
Assign tasks to others *States: Draft, Review*	Lets users reassign reports (currently assigned to themselves or to other users) to other users.	To change the author of reports currently in the Draft state, users must also have Reassign privileges.
Assign tasks to themselves *States: Draft, Review*	Lets users reassign reports to themselves.	To change the author of reports currently in the Draft state, users must also have Reassign privileges.
Create tasks *States: Draft*	Lets users create reports	Users must also have the following privileges: • Reports and Axon Standards - Create reports • Reports - Standards - Create privileges for the reports the user must be able to create
Delete tasks *States: Draft, Review*	Lets users delete reports that are in any state (Draft, Supervisor Review, etc.) except the Finalized state.	Users must also have Delete privileges
Revert finalized reports *States: Finalized*	Lets users revert finalized reports. The report is moved back to the Review state.	
Submit tasks from the {State name} state *States: Draft, Review*	Lets users approve and reject tasks in the indicated state. When a task is approved, it moves to the next state in the workflow. When a task is rejected, it moves to the Draft state. The Draft state version of this privilege lets users submit reports for review. (i.e., reveals the **Submit** button in Report Writer.)	
View tasks *States: Draft, Review, Self-Finalized, Finalized*	Lets users view reports	Users must also have Task inbox privileges for the task inboxes that contain the reports. Additionally, users must also have View privileges.

Restrictions

The following privileges related to restrictions and restriction exceptions appear in the **Restrictions** privilege category.

Three restriction privileges are generated each time a new restriction type is created using the Restrictions tool:

- Add the {restriction name} to incidents, events, and reports
- Remove the {restriction name} from incidents, events, and reports
- View incidents, events, and reports where the {restriction name} has been added

For example, if you create a domestic violence restriction, three corresponding privileges are generated:

- Add the domestic violence to incidents, events, and reports
- Remove the domestic violence from incidents, events, and reports
- View incidents, events, and reports where the domestic violence has been added

If your organization is configured for both Axon Records and Axon Standards, any restrictions you create can be assigned to both Axon Records and Axon Standards reports, incidents, and events.

If you want a user or Command Hierarchy group to view information that has been restricted, but you don't want to give them access to view all information containing that restriction, you can create a restriction exception.

Two privileges related to this behavior appear at the bottom of the **Restrictions** category in a **Restriction Exceptions** subcategory:

- Manage (add and remove) users on Restriction Exception Lists
- View (but not manage) Restriction Exception Lists

Search

The following privileges related to Search appear in the **Search** privilege category.

Name	Description
Access the Search module in Standards	Lets users use the Search module in Axon Standards.

Task inboxes - Standards

To view and act on reports that appear in the task inboxes, users must belong to Command Hierarchy groups or teams that have been given **Task Inboxes** privileges. All users automatically can see the My tasks inbox.

The privileges in the table below let users access additional task inboxes. See Case Management for information about granting access to case inboxes.

In addition to the **Task Inboxes** privileges, users must also have Reports privileges to view and act on the reports that appear in the task inboxes:

- Reports - view all reports
- View tasks

The following inboxes appear by default, but if your organization has additional custom inboxes configured, each custom inbox has an associated **Access** privilege.

Name	Description
Chain of Command, Configurable Inboxes, Internal Affairs (IA) Investigation, Internal Affairs (IA) Review	
Each default inbox has a section, and all custom inboxes that have been created fro your agency appear in the Configurable Inboxes section. Each section contains two privileges:	
Access the {Inbox Name} inbox in Standards	Lets users access the indicated Axon Standards inbox.
Submit to the {Inbox Name} inbox in Standards	Lets users move a task in this inbox to any other state in the workflow.
My Notifications	
Access the My Notifications inbox and notify users about Standards reports	Lets users view tasks send them to the My Notifications inbox and send notifications from the Report Writer view.
Task Inboxes	
Access the Agency tasks inbox in Standards	Lets users access the Agency Tasks inbox in Axon Standards.

Training

The following privileges related to the Training module appear in the **Training** privilege category.

Within this category, there are "static" privileges, as well as workflow privileges. Administrators and instructors should receive **ALL** of the privileges in the two workflows:

- Courses
- Course Results

Name	Description
Course	
Access the Courses tab in the Training Management section	Lets users view all courses in the **Courses** tab in the Training Management section.
Create courses	Lets users create courses.
Enroll learners in and remove learners from all courses	Lets users enroll and remove learners in ALL courses, not just courses for which they are assigned as the instructor.
Update courses	Lets users update courses.
Course Results	
Record scores for all courses.	Lets users update training records in ALL courses, not just courses for which they are assigned as the instructor.
View course results for all users	Lets users view the course results of ALL users at the organization, not just the users who belong to their teams.
Curriculum	
Create curricula	Lets users create curricula.
Update curricula	Lets users update curricula.