# Merative Social Program Management 8.1

## Investigations Guide

# Note

Before using this information and the product it supports, read the information in Notices on page 29

# Edition

This edition applies to Merative™ Social Program Management 8.0.0, 8.0.1, 8.0.2, 8.0.3, and 8.1.

Merative and the Merative Logo are trademarks of Merative US L.P. in the United States and other countries.

# Contents

Note................................................................................................ iii

Edition................................................................................................ v

1 Cúram Investigations overview.................................................................... 9

1.1 The investigation process.........................................................................9
- Creating an investigation.........................................................................9
- Assigning investigation ownership.............................................................10
- Recording allegations for an investigation.................................................. 10
- Entering allegation findings..................................................................... 11
- Entering the investigation resolution......................................................... 11
- Approving the investigation...................................................................... 11
- Closing or reopening an investigation.........................................................12
- Overriding a finding on a reopened investigation.......................................... 12
- Summary of participant roles played in an investigation..................................12

1.2 Tools for conducting an investigation.........................................................13
- Monitoring the investigation action plan.....................................................13
- Tracking milestones...............................................................................14
- Using the contact log............................................................................. 15
- Viewing the investigation status history..................................................... 19
- Determining the need for a translator.........................................................19
- Managing legal actions and legal status......................................................20
- Extra tools for managing an investigation....................................................21

1.3 Configuring investigations.......................................................................24
- Defining investigation types.....................................................................24
- Configuring investigation ownership..........................................................24
- Configuring investigation milestones..........................................................24
- Associating milestones with investigations...................................................26
- Defining investigation resolutions.............................................................27
- Setting up assessments for investigation types.............................................27
- Configuring investigation approval checks...................................................27

Notices............................................................................................ 29
- Privacy policy......................................................................................30
- Trademarks........................................................................................ 30

# 1 Cúram Investigations overview

An investigation is an inquiry into the circumstances of an allegation. Investigations can be created for integrated case or product deliveries. Investigation ownership can be transferred. Investigations can be owned by users, organization groups, or assigned to work queues.

Social Enterprise organizations receive thousands of allegations that are reported each year that must be investigated. Examples include allegations of benefit fraud and child abuse. Allegations of benefit fraud or child abuse might come from a number of sources such as members of the public or family members. For example, John is in receipt of Disability Benefit due to being unable to work because of a back injury. John's neighbor informs the organization that John is working for 'cash in hand' and is committing benefit fraud. Investigations are created to manage and resolve allegations that are reported during screening or case processing.

## *1.1 The investigation process*

The goal of the investigation process is to collect accurate and comprehensive information to investigate and resolve allegations that are reported to the organization. The investigation process begins when an investigation is created and ends when it is closed.

When allegations are made, the organization must examine the details of each allegation that is reported to establish if the allegation is true and effectively resolve the matter. Cúram investigation management provides a mechanism for the organization to manage and resolve allegations that are reported. It enables the organization to initiate an investigation into a reported allegation, record details of the allegation, enter findings, and record an overall resolution for the investigation.

A resolved investigation might result in the implementation of other processes. For example, for substantiated allegations of benefit fraud, the organization might decide to withhold the perpetrator's benefit payments and put in place a process to recoup the money owed. Alternatively, if it is decided that an allegation is unfounded, the investigation can be closed.

After an investigation is created, investigation management activities must be completed in order to resolve and close the investigation.

These activities include recording the allegation, completing findings on the allegation, entering an investigation resolution, approving the investigation, and closing the investigation. In addition, any individuals who are involved in the investigation can be added during the investigation and a closed investigation can be reopened. If reopened, the findings that are recorded on the investigation can be overridden.

### Creating an investigation

An investigation can be created at the integrated case level. Alternatively, a standalone investigation can be created.

The organization may wish to handle investigations separately from other types of case processing. In this situation, a standalone investigation can be created. The process of creating an investigation is designed to be completely flexible. The decision to create a standalone investigation or integrated case level is made at the discretion of the organization.

Standalone investigations can be created for a registered person, a registered prospect person, or an unregistered individual who is registered on the system as a person participant during the investigation creation process.

When an investigation is created at the integrated case level, the primary client for the investigation can be selected from any of the case members of the case from within which the investigation is created.

## Assigning investigation ownership

The application provides a sample investigation ownership strategy which can be overridden by agencies as required.

When a standalone investigation is created, the system automatically sets the administrator of the primary client as the initial case owner of the investigation. When an investigation is created from an integrated case, the case owner of the integrated case is automatically set as the owner.

Investigation ownership can be transferred. The owner of an investigation can be a user or an organization group such as an organization unit, position, or work queue. If the investigation owner is set to an organization unit, work queue or position, any users who are members of the organization group can work on the investigation.

The agency's own investigation ownership strategy can be configured depending on its requirements. For more information about configuring investigation ownership, see Configuring investigation ownership on page 24.

## Recording allegations for an investigation

When an investigation is created, details of the reported allegation that gave rise to the investigation must be recorded. The investigation that is conducted by the organization is intended to substantiate or unsubstantiate these allegations.

An investigation may include one or more allegations that are reported by a source, who may be anonymous, who believes that individuals have been involved in a situation that requires investigation such as the fraudulent receipt of benefits and/or services, or the abuse or neglect of a child.

Allegations capture details about what is being investigated, for example, Mary Smith alleges that John Smith sexually abused his daughter Linda Smith and that the alleged abuse took place in the home on 16 June 2006.

Mandatory details, such as the type of allegation and date are recorded. Additionally, the allegation location, a description of the allegation, the allegation participants and their roles, date the allegation was reported, and any additional information is recorded if known.

Allegations cannot be added, deleted, or modified from within an investigation that has been submitted for approval, approved, or closed. When an investigation is submitted for approval, it is under review by a supervisor therefore the allegations should remain static until the supervisor decides whether or not to approve the Investigation. No additional allegations can be added to or modified within approved or closed investigations because these investigations are effectively completed.

## Entering allegation findings

A finding is a determination by a user as to whether or not an allegation is founded or unfounded. A finding must be recorded on each allegation in the investigation so that the investigation can be resolved. A user resolves the investigation based on the findings of the allegations.

Examples of allegation findings include 'Substantiated' (founded/true), 'Unsubstantiated' (unfounded/false), and 'Indicated'. A finding of 'Indicated' is used when the organization has sufficient evidence to suggest an allegation is true however the evidence is not strong enough to warrant a substantiated finding. In this situation, the user may prefer to enter a finding of 'Indicated' instead of 'Unsubstantiated'.

A finding cannot be modified on an investigation which is submitted for approval, approved, or closed. When an investigation has been submitted for approval, it is under review by a supervisor and therefore the allegation findings should remain static until the supervisor decides whether or not to approved the investigation. Allegation findings cannot be modified on an approved or closed investigation because these investigations are effectively completed.

The findings that can be entered on an allegation are set up as code table items as part of system administration. For more information about adding code table items to code tables, see the *System Administration Guide*.

## Entering the investigation resolution

When the allegation findings have been entered, an overall resolution is recorded. The overall resolution is determined by the user using best judgment based on the allegations and findings that exist on the investigation.

For example, a 'Founded' resolution may be indicated for an investigation if at least one of the allegations has received a finding of 'Substantiated' and further action needs to be taken by the organization. This might involve a suspend payment workflow event that will be triggered in the event that an investigation into suspected benefit fraud is founded.

The resolutions that can be entered are inherited from those configured for the investigation type during system administration. Any workflow event associated with the resolution configuration will also be raised when that resolution is entered on an investigation.

## Approving the investigation

When a user records a resolution for the investigation, the investigation must be approved. The purpose of this stage is to verify that the allegations, findings, and overall resolution entered are correct.

The investigation approval stage gives an appropriate user, such as the investigation supervisor, the opportunity to approve or reject the findings documented by the user. This is important because these findings often dictate whether ongoing services should be provided to the client. For example, the investigation supervisor may not agree with a particular finding that the user has given to an allegation or to the overall resolution provided.

When a resolution has been recorded on an investigation, the investigation is submitted for approval and either approved or rejected. If the details recorded for the investigation and the recommended resolution are found to be appropriate, it is manually approved. If additional work is required or the resolution is incorrect, the investigation is rejected and returned to the user for modification. If the user has investigation approval rights as part of his or her security profile, or if the investigation supervisor submits the investigation for approval, the investigation is automatically approved.

Investigations submitted for approval have a status of submitted; approved investigations have a status of approved. If the investigation is rejected, it must be resubmitted in order to progress.

Note that some organizations may not require an investigation to be submitted to an investigation supervisor for approval. Investigations functionality can be configured to support approval check functionality which allows the organization to determine the percentage of investigations to be manually approved by a supervisor. See Configuring investigation approval checks on page 27 for information on setting approval checks.

## Closing or reopening an investigation

If further involvement by the organization is not needed, an investigation can be closed at any stage. For example, an investigation can be closed if an allegation that was recorded on it is withdrawn.

An investigation is typically closed when all the investigation allegations are resolved, the investigation findings do not require further action by the organization, and the investigation is approved.

When an investigation is closed, the reason for closing the investigation is specified. After an investigation is closed, the closure details can be changed by a user.

Occasionally, an investigation that is completed and closed might need to be reopened. A closed investigation might need to be reopened for a number of reasons, for example:

- The original investigation decision was incorrect.
- New information justifies a different finding on the allegation.
- The investigation was closed in error.

When an investigation is reopened, a reason for reopening the investigation is specified.

## Overriding a finding on a reopened investigation

If an investigation is re-opened, a finding previously recorded on an allegation can be overridden. For example, if the original finding recorded on the allegation is found to be incorrect, the finding can be overridden and a new finding entered.

To complete the override of a finding, the user must specify the reason for changing the finding and the effective date of the new finding.

A finding history is automatically maintained for all allegation findings. The finding history records details of each finding, the effective date and the override reason if applicable.

## Summary of participant roles played in an investigation

Investigation participants are participants who play a role either directly or indirectly in an investigation. Participants can be manually or automatically added to the investigation.

Additional participants who were not recorded on the investigation when it was created may be added during the course of the investigation. These participants can be added manually by a user or automatically by the system when a participant is selected by a user to be a participant in an allegation or to be the source of the allegation.

An allegation participant is a participant who plays a role in an allegation. Examples of roles an allegation participant can play include alleged victim, alleged perpetrator, or impacted party. An allegation participant can be an existing case participant, a registered participant that is identified through a participant search, or an unregistered participant. When a registered or unregistered participant plays a role on an allegation, and is added to the allegation, the system automatically adds the participant to the investigation as a case participant and assigns a role of 'case member' to the participant.

The source of the allegation is also considered an allegation participant. The source can be an existing case participant, a registered participant, or an unregistered participant. When an allegation source who is not a case participant is added to an allegation, the system automatically adds the source to the investigation as a case participant and assigns a role of 'allegation reporter' to the participant.

Multiple allegation participants can be added to an allegation. Each allegation participant added is assigned a role. A participant can play multiple roles in an allegation. For example, a participant who plays the role of alleged victim may also be the source of the allegation.

## *1.2 Tools for conducting an investigation*

Tools are provided for conducting an investigation. Optionally, these tools can be used during an investigation and include milestone and action plan functions and a contact log for recording interactions between the organization and key participants.

Your organization can use these tools during the investigation to:

- Monitor action plans for the course of action to take if an allegation is warranted.
- Use milestones to track significant events that occur during an investigation.
- Maintain a detailed contact log of interviews and meetings with various investigation sources.
- Track the progress of the investigation through its lifecycle by using the investigation status history.
- Determine the need for a translator to mediate between the primary client of an investigation and a caseworker.
- Manage legal actions and legal status for investigation participants.
- Use standard tools within investigations.

### Monitoring the investigation action plan

Action plans are created to identify the actions required to address the needs of the concerned participants during the investigation process.

The action plan documents the situations requiring action that concern each participant, any related allegations and the expected and actual dates for addressing the situation. Examples of situations include a concern over the safety of a child due to alleged physical abuse by a family member. The actions required to address each situation are also documented, including the case participants or user responsible for completing each action. Situations within an action plan may be associated with an action when they are recorded or they may exist independently within an action plan to be associated with actions at a later date. Additionally, actions within an action plan may be associated with one or more situations when they are recorded or they may exist independently to be associated with situations at a later date. Multiple action plans can be created for a given investigation.

Typically an action plan is a voluntary agreement between a participant and the organization. For example, John's mother alleges he was physically abused by his father. A case worker conducts an investigation into the allegation and decides that the allegation is founded. Based on his interaction with John's mother, the case worker determines that it is in John's best interests to remain in his family's home if some of his concerns about John's father are addressed in an appropriate manner. Freddie creates a four-week action plan for John detailing the situation requiring action, the expected date by when the situation should be addressed, and the action required to address the situation. For example, to address the situation of John's safety, John's father will check-in to an in-patient drug addiction program at the county hospital immediately, completing the program successfully before returning home. After talking with Freddie, John's father agrees to check himself into an in-patient drug abuse program at the county hospital as soon as possible. The family also agrees to weekly visits by Freddie to see how John and his family are progressing.

In addition to being available for use in investigations, an SEM agency may also choose to implement action plans for use within any other type of case that would also benefit from having an associated action plan.

## Tracking milestones

Milestones are used to track the completion of significant events or tasks during the life cycle of an investigation. For example, a milestone can be created to track the progress of initial contact with the participant being investigated.

Milestones can be assigned a user other than the investigation owner to take ownership of a milestone.

The application provides the ability to manually create milestones. When created, each milestone has an expected start date and an expected end date. An actual start date is then entered to indicate that the milestone is in progress and an actual end date to indicate that the milestone is complete.

If the expected start date for a milestone is reached and the milestone has not yet started, a workflow process can be initiated to notify the case owner that the milestone has passed the date by when it should have started. Similarly a workflow process can be initiated to notify the case owner that the expected end date for a milestone has been reached and the milestone has not yet completed. An agency may also choose to define its own workflow process in order to meet agency specific requirements when milestone deadlines are not met.

The application also supports the automatic creation and completion of milestones when events occur within an investigation. For example, the milestone to track the progress of initial contact could be automatically created by the system on the date an investigation is created and automatically closed by the system when initial contact with the client is recorded.

**Note:** The application provides functionality to set up the automatic creation of milestones; however, some development is required to enact the automatic creation of milestones. For more information about developing with milestones, see the *Milestone Developer Guide*. Both manually and automatically created milestones are based on milestone configurations set up as part of investigation administration (see Configuring investigation milestones on page 24).

### *Milestone Waiver Request Approval*

Given that milestones are used to track important investigation events over time, a milestone waiver request may be required in order for the milestone expected start and end dates to be changed for an automatically created milestone. Expected start and end dates for manually created milestones can be changed without a wavier request. The milestone waiver request approval process is used to confirm that the changes in dates to the milestone are valid. Once a submitted request has been approved, the new expected start and/or end dates will take effect.

Milestone waiver requests can only be submitted, i.e., the expected dates for a milestone can only be changed, if the Expected Date Extension Allowed setting has been configured. The approval process (i.e. the need to submit a waiver request for approval) for these requests will only be necessary if the Waiver Required setting has also been configured. If the Waiver Required setting has not been configured, a user will be able to change the expected start and/or end dates directly. See Configuring investigation milestones on page 24 for a description of these settings.

Milestone waiver request approval check settings for a milestone determine the percentage of submitted waiver requests for a milestone of a particular type that need to be reviewed by an investigation supervisor. For example, an approval check can be set up on a milestone that requires 60% of all submitted requests to be approved; 40% will not require approval. Setting approval checks at the milestone level governs all milestones of a particular type. Milestone waiver request approval checks can also be set up at the organization and user level, with user configuration settings taking precedence over organization unit and milestone settings, and organization unit settings taking precedence over milestone settings. Consequently, the approval check settings for a particular type of milestone are the last step in the system's evaluation of whether or not a waiver request requires approval. In other words, when a waiver request is submitted for approval by a user, the system first checks the user's milestone waiver request approval check settings, then checks the milestone waiver request approval check settings for the organization unit that the user belongs to. After checking these settings, the system checks the approval settings at the milestone level. The system may determine at any point in this process that the milestone waiver request requires approval.

The approval process is initiated when a user submits a milestone waiver request. If the waiver does not require approval, the waiver is automatically approved and the milestone date changes take effect. If the waiver requires approval, the status is submitted. Note that only one waiver for a milestone can be in a submitted state.

A notification is sent to the appropriate user or group of users to approve or reject the waiver request. Once the user approves the waiver request, the waiver request status changes to approved and the date changes take effect. Alternatively, the user can reject the waiver request and the status is set to rejected.

## Using the contact log

Use the contact log to maintains details of any follow-up action that is carried out for the investigation. A contact log includes one or more associated contacts, which can be carried out face to face, by email, phone, or hard copy. Caseworkers can record and edit contacts in the contact log and search for specific contacts to find specific information.

Maintaining contacts in the contact log involves documenting accurate details of the following interactions:

- Individual contacts with the alleged abuser, alleged victim, or other investigation participant.
- Contacts with non-case participants, such as doctors or police personnel.

### Recording contacts

The contact log provides caseworkers with a way to record important dates and details about each contact, such as the participant that the contact concerns, additional attendees, location, purpose, start date and time, type, method, contact subject (if configured), and supporting narrative. A supporting narrative must be entered when a contact is recorded.

Caseworkers can specify one or many concerning participants for a contact and are selected from the existing case participants of the investigation. Administrators can configure whether or not all case participants are available for selection, or case members only. Multiple attendees may also be associated to the contact and can be selected from existing case participants, registered persons, and registered users.

The contact log also provides a mechanism to upload and store multiple attachments, such as scanned documents that were received as part of the investigative process.

Contacts are available to view in the contact log list and the details of a contact can be edited at any time. From the contact log list, caseworkers can also add additional contact participants, attachments, and delete contacts as needed.

Caseworkers can search for a specific set of contacts in the contact log. A preview function allows the caseworker to select and view a specific set of contacts in the contact log from the search results or the contact log list. The previewed contacts can be saved to a PDF document and printed.

The number of contacts that caseworkers see in the contact log is configurable. When the limit is exceeded, only the configured number of contacts are displayed. The most recently recorded contacts are displayed on the list page and in search results.

Information recorded in a contact log helps the organization to assess the investigation, and provides the basis for determining appropriate plans or actions required to successfully conduct the investigation.

### Appending to the narrative

The contact narrative is the caseworker’s point in time record of a contact with another party. After recording the contact, if the caseworker obtains additional information, they can edit the contact to append new narrative text as an addendum without affecting the originally documented narrative. Any caseworker can append to the narrative in addition to the original author.

Updates to contact narratives that are displayed separately to the original narrative as appended text when a caseworker views the details of a contact. No limit applies to the number of narratives that a caseworker can append to a contact.

8.0.3.0 Caseworkers cannot append new narrative text if another caseworker is editing the original narrative or an appended narrative. For more information, see *Editing the narrative*.

### Narrative history

A history of updates to a narrative over time is maintained. By expanding a contact in the list or by editing a contact, caseworkers can see the original narrative and any appended narratives in the narrative history. The name of the caseworker and date and time of each append are also displayed. By default, the most recent narrative text is displayed first. An administrator can configure the order that narratives are displayed in the history, newest first or oldest first.

Caseworkers can also see the most recent contact details, participants, and attachments in the expanded contact record. A history of updates to other contact details, participants, and attachments is not maintained.

### Editing the narrative

8.0.3.0

After a caseworker records the original narrative or an addendum, they might want to edit the narrative to make a correction or to add more information. If configured, the author of the original narrative or appended narrative can edit it for a specific editable period that is set by an administrator. By editing the contact, the author can make unlimited edits to their narrative during the editable period.

When the author edits the narrative within the editable period, the application overwrites the previous narrative text with the latest version when the contact is saved. The application maintains no record of the previous version of the text. For this reason, the editable period is intended to be a short period of time.

During the editable period, pencil icons are displayed to help the contact author and other caseworkers to understand whether they can edit or append to a narrative. The pencil icons relate only to the most recent narrative.

When a narrative is appended, the original narrative can no longer be edited. For example, if the first caseworker authors the original narrative and after its editable period expires, a second caseworker appends an additional narrative, the second caseworker is the narrative author for the configured editable period and no user can edit the original narrative.

*Table 1: Pencil icons for narrative authors and non-authors*

| Pencil icon | Description |
|---|---|
| ✎ | Indicates to the narrative author that they can continue to edit their narrative. By expanding the contact, the author can see the end date and time after which they can no longer edit the narrative. |
| ⊘ | Indicates to non-authors that someone else is editing the narrative and they cannot append to it at this time. By expanding the contact, the non-author can see the date and time from when they can append to the narrative. |

After the editable period ends, no pencil icons are displayed and the narrative can no longer be edited. Any caseworker with access to the contact log can append to the narrative only after the editable period ends.

### Searching for contacts

Caseworkers can quickly search for a specific set of contacts to find specific kinds of information for reasons such as for presentation at court hearings. Caseworkers can search by various criteria such as contact participants, location, purpose, contact method, and date range. They can also search for specific words that are contained in the narrative.

8.0.3.0 If configured, caseworkers can enter a subject for a narrative when they record or edit contacts. Caseworkers can search both the subject and the narrative for specific words if the subject is configured. The search returns a list of contacts that contain the words. Each search displays the results in ranked order based on best match. When the search results are returned, if the caseworker entered no subject for the contact, a – displays in the Subject field.

*Table 2: Subject and narrative search results by example*

| Search words | Search results |
|---|---|
| `accident`, `fall`, `incident` | Finds matches that contain any of these words, in any order, in the subject or narrative. |
| `counsellor` | Finds matches that contain the word `counsellor` or `counselling` in the subject or narrative. |
| `meeting with victim` | Finds matches that contain the following sets of words in the subject or narrative:<br>• `Initial meeting with the victim John Smith`<br>• `Initial meeting with victim`<br>• `meeting with the victim` |

**Note:** By default, caseworkers must enter at least two characters of a full word to search the subject and narrative for that word. For best matches, enter more characters. Searches for words in the subject and narrative that include special characters also return matches.

To narrow the search results, extra search criteria are available, such as the contact participants, location, purpose, contact method, and date range. If a caseworker enters any other criteria with a subject and narrative search, the search returns matches that contain the extra criteria and any words they entered in the subject and narrative search.

Caseworkers can use the following operators to further refine searches by subject and narrative:

- **OR**
  By default, when a caseworker enters two words in the search, the search finds contacts that contain either of those two words. For example, to search for contacts that contain either the words 'substance' or 'abuse', enter:
  `substance abuse`
  or
  `substance OR abuse`
- **AND**
  Use AND to find contacts where both words are contained in the subject or the narrative. For example, to search for contacts that contain the words 'substance' and 'abuse', enter `substance AND abuse`.
- **NOT**
  Use NOT before a word to exclude results that include that word. For example, to search for contacts that contain the word 'substance' without the word 'abuse', enter `substance NOT abuse`.

For more information about configuring contact logs, see the *System Administration Guide*.

## Viewing the investigation status history

A status history is automatically maintained for all investigations. Use the status history to view details of each status change that the investigation has undergone during its lifetime.

The status history automatically updates when a user submits an investigation for approval, or approves or rejects an investigation.

Every time the system detects an instance of processing for an investigation, it is added to the history. The history displays a record of the investigation, the status, and the effective date of the status change. The effective date allows the user to determine the duration of each status. The status history allows a user to track the progress of an investigation from the time it is created to the time it is closed.

Each investigation has a status which describes its progress during the investigation process. There are five investigation statuses: open, submitted, approved, rejected, and closed. Each status changes during investigation processing.

The following table describes each investigation status:

*Table 3: Investigation Processing Statuses*

This table describes the processing statuses an investigation can have.

| Status | Description |
|---|---|
| Open | An investigation status is 'open' when the investigation is first created on the system. An investigation can also have an open status if it has been closed and re-opened. |
| Submitted | An investigation status is 'submitted' when the investigation is submitted for approval. |
| Approved | An investigation status is 'approved' when the investigation has been approved by an authorized user, e.g., an investigation supervisor or has been automatically approved by the system. |
| Rejected | An investigation status is 'rejected' if it does not pass the approval process and has been 'rejected' by an authorized user, e.g. an investigation supervisor. A rejected investigation can be modified and re-submitted for approval. |
| Closed | An investigation status is 'closed' if the investigation is completed and no further action is required. If no further action is required, investigations are manually closed by a user. |

## Determining the need for a translator

The organization may occasionally require a translator to mediate between the primary client of the investigation and a case worker. Translation needs for a client can be set manually by a caseworker or automatically by the system.

Translation services may be required if users working on an investigation are unable to interact with a client in his or her preferred language. A client's preferred language is recorded when the client is registered with the organization. For example, when James Smith is registered with the organization, his preferred language is recorded as "Spanish" and he cannot speak any other language. In order to interact with the client, the case worker responsible for the investigation must be able to interact with James in Spanish or have a translator who can mediate between them.

Determining the need for a translator is evaluated depending on the translation requirements present on an individual investigation. For example, a client may require translation services on one investigation but not on another. The need for a translator for a client can be recorded manually by a case worker or it can be determined automatically by the system. Whether the translation needs for a client are set manually by a caseworker or automatically by the system is dictated by a configuration setting that is set on the investigation type on which the investigation is based in the administration application.

The system determines the need for a translator by checking if the case worker's language skills match client's preferred language. If they do not match, the system determined that a translator is required. A user may also manually update the translation requirements for a case even if they are initially determined by the system. If a translator is required for a client, users are kept informed of it when they view the client's case participant details. Additionally, the system displays the preferred language of the client who requires the translation services.

## Managing legal actions and legal status

Caseworkers can capture the legal actions that are taken during the course of an investigation. Legal actions are used to manage directives, actions or other activities concerning investigation participants that are conducted by a legal authority.

Examples of directives and actions include hearings, petitions, and orders. For example, a court may order a participant with a history of violence to stay away from the family home. Alternatively, the agency may prepare a petition for a court to detain a participant who has committed an offense. Legal actions can result from another legal action, decision or any other reason that is deemed appropriate by the agency. For example, a legal action such as a temporary custody petition may result in a temporary custody hearing that is scheduled as a result of the petition.

Three main categories of legal actions are supported: Legal Petition, Legal Hearing, and Legal Order.

A case worker may also document the legal status of an investigation participant. When a court makes a decision about what will happen to a participant, it determines a legal status. Examples of legal statuses include adjudicated, crown ward, parental rights terminated, parental custody, and temporary custody. During the course of a case or legal action, a participant's legal status may change. The changes in a participant's legal status can be accessed and tracked by a case worker. A history of a participant's legal status is maintained to allow the case worker to see how a participant's legal status has changed over time, for example, a participant's legal status may have initially been determined to be 'temporary custody' but then changed to 'parental rights terminated' when there was no longer the possibility that the participant would return home. Legal statuses are not tied to legal actions but may vary depending on or be impacted by the legal action outcome.

The types of legal actions and legal status that can be created within an investigation are configured as part of administration.

For more information about legal actions and legal status, see the *Appeals Guide*.

## Extra tools for managing an investigation

Extra tools are also available for managing investigations. These tools are modeled on existing case management function that are available in integrated cases and product delivery cases.

### *Viewing my investigations*

To help users to manage their investigations more efficiently, several views are available.

#### Viewing the Investigator home page

The **Investigator home** page provides the following summary information to help users to manage their workload:

- A view of appointments for today or any other day within the week or the following week.
- Assigned tasks due for that day, as well as any overdue tasks.
- Any cases or investigations that are marked as items of interest.

Summary information is also provided about investigations that are assigned to the user.

- A chart displays details of all assigned investigations with a resolution that was recorded during a specific period. The user can change the view to see this information for different periods, for example, for that day or the previous week.
- Details of investigations that are either owned or submitted by the user that are still awaiting approval.

#### Viewing my investigations

The My Investigations view allows users to access a list of investigations that are currently owned by either themselves, their organization unit, their position, or their work queue.

Administrators can configure which of these ownership displays are selectable by the user when they filter which investigations they want to see displayed. Users can also filter the investigations list based on type and status.

#### Viewing investigation query results

Investigation queries allow users to monitor any investigations that are currently or previously assigned to them. The user can choose specific criteria that is important to them, and then save the criteria that are used in the search as a personal query. The query can be run and rerun without the need for the user to specify the criteria again. Users can query investigations by client, type, subtype, ownership, and status. They can also filter the query results by entering a time period to run the query against.

#### Viewing my recently approved investigations

Users can view a list of investigations that they currently own and are recently approved. Any recently approved investigations, which they submitted for approval but no longer have ownership, for are also displayed.

#### Viewing my recently assigned investigations

Any investigations that have recently been assigned to the user are available to be viewed. This is based on the ownership filter criteria that are defined for the users my investigations display.

#### Viewing my recently viewed investigations

Details are provided of investigations that the user has recently viewed. This allows the user to quickly return to the investigation without having to search for it.

#### Viewing my items of interest

Users can add specific investigations as items of interest. They can then easily go to the investigation without the need to search. This is especially useful for investigations that need to be monitored closely. When the user no longer holds an interest in that particular investigation, it can be removed from the list.

**Important:** Items of interest are not limited to investigations. They can also be added for all case types that are recorded in the application.

### *Searching for investigations*

So that users can access specific investigation information across the organization, an investigation search is available.

Users can search for an investigation by reference number, client name, client reference number, type, sub type, or status. Users can also filter the search results by running the search against the investigation start or end date.

### *Adding attachments*

An attachment is a supplemental file, for example, a text document, that is attached to an investigation. Users can attach scanned documents that provide information in support of an investigation such as a transcript of an interview with an investigation source, or a bank statement.

Other examples of investigation attachments include marriage certificates, invoices, and pay slips. A range of file types are supported including Microsoft® Word, Microsoft® Excel and PDF. Once the file is attached to the investigation, it may be accessed by other system users who have appropriate security privileges.

Attachments can also be integrated with a content management system through the configuration of application properties as part of administration. If an organization chooses to integrate attachments with a Content Management System, the file will be stored in and retrieved from the Content Management System.

**Important:** Attachments are also maintained for product delivery cases, integrated cases and participants.

### *Maintaining communications*

A communication is a correspondence to or from the organization. Communication functions can be integrated with Microsoft Word templates, XSL templates, or email servers.

Communications can be paper, telephone, or email based. Any communication that is created from a communication list page within an investigation automatically relates to that investigation.

The correspondent of an investigation communication is automatically assigned the investigation participant role of correspondent.

### Tracking investigation events

Events can be automatically created by the system as a result of case processing or manually created by a user. An example of an event that is created by the system is the investigation closure event, which is created when an investigation case is closed.

The following events can be created by a user manually: investigation case referrals, investigation case reviews, and investigation case activities.

An events calendar is provided for all events. Each calendar displays the name of the event and the date on which the event occurs in the appropriate date entry.

### Entering and updating notes

Users can enter notes to provide additional information about an investigation. For example, a user can add a note to the investigation stating that a key participant in the investigation did not attend a scheduled meeting.

A note can be entered as free text and can be prioritized and given a sensitivity rating so that the note can only be accessed by certain users.

8.0.3.0 Users can modify a note to update its priority, sensitivity, and append additional note text. If configured, they can also edit their original note text for a specific time period. For more information about appending to notes and editing notes, see the *Integrated Case Management Guide*.

When a note is added or appended, the system maintains a note history that includes each version of a note, the time and date that the note was entered on the system, and the user who made the note modifications.

For more information about configuring notes, see the *System Administration Guide*.

### Using tasks to manage work on investigations

Users can maintain tasks that relate to an investigation from the investigation case's task list.

A task is an instruction to carry out an item of work. Tasks are either manually created by a user or automatically created by the system. They are maintained in a user's workspace as part of workflow. Tasks that relate to an investigation can also be maintained from the investigation case's task list. For example, a task can be created to approve an investigation that has been submitted for approval. The task appears on both the user's inbox and on the investigation's list of tasks.

### Recording case relationships

Users can create relationship between one case and another case. For example, if a client is being investigated for potential fraud in one product delivery case, but is also involved in another product delivery case, a relationship can be created between the investigation and the product delivery case.

Case relationships are either created manually or automatically during investigation processing.

### *Assigning user roles*

Investigation ownership can be assigned to any organization object, that is, a user, organization unit, position, or work queue.

Standard user role functions are used by investigations to record the investigation owner and supervisor. This enables any user or users within an organization unit, position or work queue to perform tasks on an investigation,

# *1.3 Configuring investigations*

Users can create investigations on cases when investigation information is configured in the system administration application. Investigation types, milestones, and resolutions must be configured to create investigations at the case level.

When an investigation is created, it inherits this preconfigured information.

## Defining investigation types

The types of investigations that can be created are configurable, for example, Benefit Fraud, Child Protection Services and Youth Justice.

An investigation type includes the following configurable information: the Home Page for the investigation, Start Date, Create Workflow Event, Close Workflow Event, and Security Rights. Additionally, investigation type configuration includes the ability to configure translation requirements and an investigation ownership strategy and whether or not only case members should be available for selection as the concerning participant of a contact created within the contact log of an investigation.

## Configuring investigation ownership

The Investigation Ownership Strategy setting allows a system administrator to define an ownership strategy for investigations based on a particular type using workflow.

Investigation ownership is functionally similar to case ownership. If an ownership strategy is specified for an investigation, this setting is used to define how the initial case owner for the investigation should be determined. An organization can override the default investigation ownership strategy depending upon its requirements to assign ownership to any user, organization unit, position, or work queue.

## Configuring investigation milestones

All investigation milestones are based on an associated milestone configuration. Use the table to learn about the available milestone configuration settings (optional and mandatory).

The table describes the settings and how to use them.

*Table 4: Milestone configuration settings*

| Configuration settings | How to use | Optional or mandatory |
|---|---|---|
| Name and Type | Use the name and type to distinguish the milestone configuration. When creating a manual milestone, a user must select the milestone configuration to be applied using the milestone configuration name. | Mandatory |
| Earliest Start Day (days) | Use this setting to determine the expected start date for automatically created milestones. The expected start date is set to the current date on which the milestone is created plus the number of days defined here. For example, if the milestone is created on April 1 and this setting is 3, then the expected start date of the milestone is set to April 4. This setting is used to validate the Expected Start Date entered by a user when manually creating a milestone. A milestone cannot have an Expected Start Date earlier than this number of days after the start date of the Investigation. | Mandatory |
| Duration (days) | Use this setting to determine the expected end date for all milestones. For manually created milestones, the expected end date is set to the user-entered expected start date plus this duration minus one. For example if the expected start date is April 1 and the duration is 7 days, the expected end date is set to April 6. For automatically created milestones, the same calculation is applied to the expected start date defined by the date on which the milestone was created and the Earliest Start Day (days). | Mandatory |
| Start Date | Use the start date to determine the active, and thus availability, period of the milestone configuration. | Mandatory |
| End Date | Use the end date to determine when the milestone configuration is no longer active. This date is not mandatory as milestone configurations can remain active for an indefinite time period. | Optional |
| Expected Date Extension Allowed | This indicates whether or not the expected start and end dates for an automatically created milestone can be redefined. If this indicator is not set, then the expected start and expected end date calculated upon creation of a milestone are unchangeable. | Optional |
| Waiver Required | This indicates whether or not a waiver is required in order to change the expected start and expected end date for an automatically created milestone. This can only be set for milestone configurations which allow the expected dates to be extended (as described in the setting above). Milestone waivers are described in Milestone Waiver Request Approval on page 15. | Optional |
| Milestone Added | Any existing workflow event can be associated with the creation of a milestone. This event can be used to extend the default milestone creation processing. For example, when a milestone is added, a workflow can be enacted to notify the investigation owner. | Optional |

| Configuration settings | How to use | Optional or mandatory |
|---|---|---|
| Milestone Complete | Any existing workflow event can be associated with the completion of a milestone. Use this event to extend the default milestone completion processing. For example, when a milestone is completed, a workflow can be enacted to notify the investigation owner. | Optional |
| Expected Start Date Not Achieved | Any existing workflow event can be associated with the expected start date in order to track the timeliness of the milestone. For example, if no actual start date is entered for the milestone and the expected start date passes, a workflow can be enacted to notify the investigation owner that the milestone has not yet started. | Optional |
| Expected End Date Not Achieved | Any existing workflow event can be associated with the expected end date in order to track the timeliness of the milestone. For example, if no actual end date is entered for the milestone and the expected end date passes, a workflow can be enacted to notify the investigation owner that the milestone has not been completed in a timely fashion. | Optional |

## Associating milestones with investigations

To support manual and automatic creation of milestones within an investigation, administrators must set up an association between a milestone configuration and the investigation type.

There are two options for setting up these associations: either a new milestone configuration can be recorded at the same time it is associated with the investigation or an existing milestone configuration can be selected.

When recording a new milestone configuration as part of the association process, the milestone configuration information (as described in Configuring investigation milestones on page 24) must be defined. Additional association information can also be defined if the milestone is to be created automatically. The two main configuration settings for automatically created milestones are the creation event and the completion event. These events are used by the application to automatically create and complete an instance of the milestone.

For example, a milestone can be set up to track the life cycle of an investigation from approval through closure. To set up the automatic creation of this milestone, the Approve Investigation event can be selected as the creation event and the Close Investigation event can be selected as the completion event. When an investigation is approved in the application, the Approve Investigation event will trigger an instance of the milestone. Later when the investigation is closed, the Close Investigation event will close the milestone instance.

The matching process for creating milestones within an investigation can be further specified using the component type and component category settings. A clear distinction can be made between creation and completion events at the investigation level and at the investigation component level. For example, the investigation component, Action Plan, can be set, with a creation event of Create Action Plan and a completion event of Close Action Plan.

When an action plan is created within an investigation, the Create Action Plan event will trigger an instance of the milestone and the application will associate both the Action Plan ID and the

Investigation ID with it. Later when the action plan is closed, the Close Action Plan event will use both of these IDs to find and close the correct milestone instance.

## Defining investigation resolutions

Resolutions for investigation types are used to record the outcome of an investigation. Examples of resolutions include Founded and Unfounded. Any number of resolutions can be configured for an investigation type.

When configured, these resolutions can be recorded on investigations by a caseworker in order to complete the investigation.

Each resolution is configured as a selectable code table value and may also have an associated workflow event which is raised when the resolution is entered on an investigation. Resolution events are used to trigger a specific case processing function. For example, a particular event may be triggered when a resolution of Founded is entered on an investigation.

## Setting up assessments for investigation types

Optionally, predefined assessments can be assigned to investigation types in the system administration application so that caseworkers can run assessments within an investigation.

Currently, there are no default assessments that can be run within an investigation. However, an organization can use the infrastructure that is provided to allow an assessment to be selected and executed by the organization during the investigative process to help determine the appropriate resolution for a particular type of investigation.

## Configuring investigation approval checks

Optionally, investigation approval checks can be configured for each investigation type so that a supervisor can check that the allegations, findings, and overall resolution recorded on an investigation is correct. Approval checks are used to safeguard against incorrect information being added to the investigation or an erroneous resolution being documented.

For example, the organization may require a supervisor to manually approve a set percentage of investigations submitted by a less senior user.

As part of the investigation process, an investigation is typically submitted to a supervisor for approval of the overall resolution recorded on the investigation by the user. The percentage of investigations that require supervisor approval can be set by the administrator. For example, an approval check percentage set to 50 signifies that 5 out of 10 investigations will be sent to the investigation supervisor for manual approval.

If the supervisor does not agree with a particular finding that the user has given to an allegation or with the overall resolution provided, the supervisor can reject the investigation.

An approval check set for an investigation type will govern all investigations based on that particular investigation type. Note that there can be only one active approval check for investigations based on a specific investigation type at a given point in time.

# Notices

Permissions for the use of these publications are granted subject to the following terms and conditions.

**Applicability**

These terms and conditions are in addition to any terms of use for the Merative website.

**Personal use**

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of Merative

**Commercial use**

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of Merative.

**Rights**

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

Merative reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by Merative, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

MERATIVE MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Merative or its licensors may have patents or pending patent applications covering subject matter described in this document. The furnishing of this documentation does not grant you any license to these patents.

Information concerning non-Merative products was obtained from the suppliers of those products, their published announcements or other publicly available sources. Merative has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-Merative products. Questions on the capabilities of non-Merative products should be addressed to the suppliers of those products.

Any references in this information to non-Merative websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this Merative product and use of those websites is at your own risk.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

The licensed program described in this document and all licensed material available for it are provided by Merative under terms of the Merative Client Agreement.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to Merative, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. Merative, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. Merative shall not be liable for any damages arising out of your use of the sample programs.

## Privacy policy

The Merative privacy policy is available at https://www.merative.com/privacy.

## Trademarks

Merative ™ and the Merative ™ logo are trademarks of Merative US L.P. in the United States and other countries.

IBM®, the IBM® logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

Adobe™, the Adobe™ logo, PostScript™, and the PostScript™ logo are either registered trademarks or trademarks of Adobe™ Systems Incorporated in the United States, and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft™, Windows™, and the Windows™ logo are trademarks of Microsoft™ Corporation in the United States, other countries, or both.

UNIX™ is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.