Oracle Life Sciences Consolidated Intake

Administration Guide

Release 2026.1.01
G50277-01
March 2026

Oracle Life Sciences Consolidated Intake Administration Guide, Release 2026.1.01

G50277-01

Contents

1

Overview

Oracle Safety One Argus allows your organization to automate and consolidate the reception and processing of Adverse Event (AE) reports and Electronic-to-Business (E2B) Individual Case Safety Reports (ICSRs). You can upload AE report files in the user interface, import files using REST API calls, or connect an email account to automatically send reports to the consolidated Intake Worklist for further review before sending the report as a new case to your Oracle Safety One Argus environment or an external publisher, depending on your workflow. The Electronic Data Interchange (EDI) gateway ingests E2B reports and any follow-up records, adding them to the Intake Worklist so intake processors can perform duplicate checks and accept the records as new cases to be sent for further processing.

If you have a Safety One Intake subscription, Optical Character Recognition (OCR) and Natural Language Process (NLP) artificial intelligence can be used to pull information from ingested reports and provide validity scores on the quality of the extracted data, automatically adding them to your Intake Worklist if further review or intervention is needed. After verifying the extracted data, the information is merged into an existing case or is used create a new one to and is sent your case processing environment.

Since Oracle Safety One Argus is an integrated application that uses single sign-on (SSO), you'll need to perform configuration tasks in Identity Cloud Service (IDCS), Argus Console, and the Consolidated Intake interface.

- Prerequisites
  Before you can continue on your Oracle Safety One Argus configuration journey, make sure you have access to the tools and applications you need.

Prerequisites

Before you can continue on your Oracle Safety One Argus configuration journey, make sure you have access to the tools and applications you need.

General prerequisites

- The **Customer-Delegated Administrator** (CDA) must be provisioned. This is the primary point of contact for Argus Cloud Service. For more information, see Get your administrator account credentials in the *Oracle Argus Cloud Service Administration Guide*.
- Confirm access to the **Identity Cloud Service** (IDCS) Admin console. You'll need to use IDCS to create and manage users.

Federated login only

The following prerequisites are for organizations using federated login:

- Confirm access to identity management administrator consoles, such as **Azure** or **OKTA**. Eventually, you'll need to synchronize the users created in IDCS with your identity management service.
- Configure the SSO between your identity management service and IDCS.

  For information on configuring OKTA with IDCS, see document ID 2998371.1 on My Oracle Support.

To learn about how to configure Azure AD with IDCS, see document ID 2795951.1 on My Oracle Support.

Contract Research Organizations (CROs)

During Intake Enterprise setup, your Global Administrator should use the **Copy Enterprise to Intake** option to propagate Consolidated Intake configuration details to each enterprise. For more information about how to complete this task, refer to New Enterprise Setup in the *Oracle Argus Safety Multi-tenancy Administration Guide*.

2

General configurations

You must perform the following configurations to use Consolidated Intake:

- Provision users
  You must create users in Oracle Identity Cloud Service (IDCS) before you can give them access to Oracle Safety One Argus. You may need to perform additional synchronization, depending on how your organization manages application access.
- Add users and assign roles
  Once you have provisioned a user in Oracle Identity Cloud Service, you can add the user to Oracle Safety One Argus and grant them access to the Consolidated Intake module.
- Configure intake numbering
  For the adverse event reports sent to Oracle Safety One Argus, a unique identifier is assigned. The default numbering format is [SSS][YY][MM]-[#########], but you can customize the identifier if necessary.
- Enable reauthentication during intake
  You can configure Safety One Argus to require reauthentication with a justification when intake processors are accepting or rejecting initial, follow-up, amendment, or nullification records.
- Configure Smart Duplicate Search
  You can adjust the weights and thresholds of the smart duplicate search using a spreadsheet available for download (and modification) in **Argus Console**.
- Configure follow-up merge
  You can download and modify the predefined comparison logic for evaluating follow-up data against existing case information in the Default Merge Configuration spreadsheet in **Argus Console**.
- Configure hold follow-up merge
  You can configure your intake workflow to hold merging follow-ups of AE records until the appropriate conditions, such as workflow state or custom rules, are met.
- Configure the automatic assignment of intake records
  Automatic assignment of intake records is enabled by default, prioritizing the Intake Worklist so that intake processors can assess time-sensitive and serious records at the start of their session.

Provision users

You must create users in Oracle Identity Cloud Service (IDCS) before you can give them access to Oracle Safety One Argus. You may need to perform additional synchronization, depending on how your organization manages application access.

Identity Cloud Service

As an administrator, log into Oracle Identity Cloud Service (IDCS) to create the users.

See the Manage users chapters in the *Oracle Argus Cloud Service Administration Guide* to learn about creating users in IDCS.

Federated login user management

If your organization uses federated login, see Federation Setup in IDCS in the *Oracle Argus Cloud Service Administration Guide*.

Add users and assign roles

Once you have provisioned a user in Oracle Identity Cloud Service, you can add the user to Oracle Safety One Argus and grant them access to the Consolidated Intake module.

1. Open a browser and navigate to your company's Oracle Safety One Argus URL.
2. Log in with your Oracle Safety One Argus administrator credentials.
3. Click **Argus Console**.
4. Hover over **Access Management**.
5. Select **Argus**.
6. Click **Users**.
7. Select **Add Users**.
8. Enter the user name, the user ID, and, if applicable, the email address.
9. In the **Application Access** section, grant access to different parts of the application:
   - Select **Argus** for users who will be assigned the Intake Processor role.
   - Select **Console** for users who perform administration configurations.
10. Assign the user to a site.
11. Assign the user to pre-configured user groups.

> **Note**
>
> Users who require access to Email Intake configuration also must be assigned to a user group with **Console** and **System Configuration** menus enabled. See Configuring Groups in the *Oracle Argus Safety Administration Guide* for more information about user groups.

12. From the **UserType** drop-down list, select **Argus User**.
13. Assign one or more roles to the user. Select from of the following intake-specific roles:
    - **Intake Designer** - Creates document processing recipes for Consolidated Intake.
    - **Intake Processor** - Verifies the data in the various records that are ingested to the consolidated Intake Worklist and controls whether the records are accepted as cases for further processing. This role is required to access the Intake Worklist located in the Consolidated Intake interface.
    - **Workflow Manager** - Delegates the workload by assigning tasks to intake processors (individually, or to a group of users). Workflow managers have access to additional tools such as the Intake Monitor, where they can oversee the progress of the AE processing. This role operates similar to the Workflow Manager role in case processing.

> **Note**
>
> Workflow managers also need to be assigned the **Intake Processor** role to have access to the Intake Worklist in Consolidated Intake.

14. If applicable, select **Enable Site Security** to enable the site-based data security for the user and decide what type of access you grant for each site.

> **Note**
>
> Both **Full Access** and **View Access** grants you full access to the Consolidated Intake interface.

15. Click **Save** to save the new user.
16. For more information about the fields in the Add User window, see the *Oracle Argus Safety Administration Guide*, Users fields description.

> **Note**
>
> - When you create a user in Oracle Identity Cloud Service (IDCS), you must use the same user name and email address that you used when you created the user in Oracle Identity Self Service. The user name in IDCS should be the same as the Argus Console User ID.
> - Select **Enable LDAP Login** in the Oracle Argus Cloud Service user creation pane.

Configure intake numbering

For the adverse event reports sent to Oracle Safety One Argus, a unique identifier is assigned. The default numbering format is [SSS][YY][MM]-[########], but you can customize the identifier if necessary.

Configure intake numbering

1. Log in to Oracle Safety One Argus, and launch the **Argus Console**.
2. Select **System Configuration** and then **System Numbering** from the context menu.
3. Click **Intake**.
4. Complete the information in the fields, and click **Save**.

Table 2-1 Configure system numbering

Field or Control Name	Description
Start at	Allows you to specify the initialization of the intake numbering sequence.
Separate sequence for each site	You can configure unique numbering sequences on a site-by-site basis. If the adverse event reports are being uploaded from two different sites then each site will have different sequencing of case numbers.

Table 2-1 (Cont.) Configure system numbering

Field or Control Name	Description
Separate sequence for each year	Resets the sequence numbering of records after each year based on the intake date of the adverse event report.
Separate sequence for each month	Resets the sequence numbering after each month based on the intake date of the adverse event report.
Numbering Format	You can reorder the placeholders in the numbering sequence in this field. [SSS][YY][MM]-[########] is the default format.
Placeholder	Placeholders are used to pick up values from the database to be used in the intake numbering format. The possible values populated in this list are: • # - Number: Defines the digits to be used as the sequence number in the format. The field is used to display the sequence number on the intake record numbers. • DD - Day: Inserts the Intake date. • MM - month: Populates with the month of the intake date. • SSS - User Site: Uses the site selected while uploading the adverse event reports. • YY- Year: Inserts the year of the intake date.

Enable reauthentication during intake

You can configure Safety One Argus to require reauthentication with a justification when intake processors are accepting or rejecting initial, follow-up, amendment, or nullification records.

When this setting is enabled, intake processors must reauthenticate their session and add a justification when accepting or rejecting records from the following Consolidated Intake interfaces:

- Intake Worklist
- Duplicate Search
- Merge Viewer
- Intake Form

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **System Configuration** menu and select **System Management (Common Profile Switches)**.
3. Click the **Intake** node in the browser.
4. Select the **Yes** radio button to enable **Enable Re-Authentication for Intake**. This setting is turned off by default.

Configure Smart Duplicate Search

You can adjust the weights and thresholds of the smart duplicate search using a spreadsheet available for download (and modification) in **Argus Console**.

For more information on the smart duplicate search configurations available in **Argus Console**, refer to the Configuring Case Processing topic in the *Oracle Argus Safety Administration Guide*.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **System Configuration** menu and select **System Management (Common Profile Switches)**.
3. Expand the **Case Processing** node in the browser and select **Duplicate Search**.
4. Click the **Download** button to access the smart duplicate search configuration file.

> **Note**
>
> Do not make any changes to the underlying structure of this file, otherwise the system may not accept the modified file when you upload it again.

5. Upload the modified spreadsheet by clicking the **Browse** button to launch your computer's file browser. Select the file and click **Validate** to verify.
6. If you are working within an enterprise (CRO), you have additional configuration options:
   - **Enable Transposed Date Matching** – Use this switch to allow transposed date matching (e.g. 03-Jan-2026 matches 01-Mar-2026). The default value is "Yes".
   - **Enable Numerical Scoring for Patient Age** – Enable this setting if you want the Patient Age field to use fuzzy matching (e.g. 20 years matches 21 years). The default value “Yes”. For exact matching on Patient Age during Duplicate Search, set this value to "No".
7. Click the **Save** button to preserve your modifications to the smart duplicate search configurations.

Configure follow-up merge

You can download and modify the predefined comparison logic for evaluating follow-up data against existing case information in the Default Merge Configuration spreadsheet in **Argus Console**.

You can create new merge configurations, adjust comparison logic, and have different intake sources follow specific configuration logic by uploading the modified configuration spreadsheet to the Intake Follow Up Merge Configuration section of **Argus Console**

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **System Configuration** drop-down menu and select **Intake Follow Up Merge Configuration**.
3. Select **Default** from the existing list of merge configurations.
4. Select the **Download** button in the **Modify Intake Follow Up Merge Configuration** section of the page to download the configuration spreadsheet.

5. Follow the instructions within the spreadsheet to modify the merge configuration logic for both Fields and Repeating Entities.

> **⚠ Caution**
>
> Do not make any changes to the underlying structure of this file, otherwise the system may not accept the modified file when you upload it again.

6. Once you are satisfied with the updates, return to **Intake Follow Up Merge Configuration** in **Argus Console** and click the **Add New** button to create a new follow-up merge configuration.
7. In the **Modify Intake Follow Up Merge Configuration** section of the page, add a name for the configuration and click the **Select** button to upload the configuration spreadsheet from your computer.
8. Click the **Validate** button to verify the file.
9. In the **Sources** section of the screen, select an intake source or reporting destination. When an intake record of this source type is ingested in Consolidated Intake, it will use the uploaded merge configuration spreadsheet to make system suggestions on how to compare and updated the incoming record fields to existing records.
10. Click **Save** to complete the new merge configuration for the source type.

Configure hold follow-up merge

You can configure your intake workflow to hold merging follow-ups of AE records until the appropriate conditions, such as workflow state or custom rules, are met.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Select **System Configuration** and click **Workflow**.
3. Select a state.
4. In the **Modify Workflow** section of the screen, select the **Hold follow-up merge during intake** checkbox.
5. If you wish to apply additional rules to the hold workflow, select an Advanced Condition (AC) from the adjacent drop down menu.

> **ⓘ Note**
>
> For information about using and configuring ACs, see Using Advanced Conditions in the *Oracle Argus Safety Administration Guide*.

Configure the automatic assignment of intake records

Automatic assignment of intake records is enabled by default, prioritizing the Intake Worklist so that intake processors can assess time-sensitive and serious records at the start of their session.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Select **System Configuration** and click **System Management (Common Profile Switches)**.

3. Click **Workflow** from the **Browser** pane.
4. The **Yes** radio button is selected by default for the option **Enable Auto opening of the next Case / Intake record**.
5. To disable automatic assignment, select the **No** radio button.

3

E2B Intake configurations

For information on how to configure E2B Intake in Argus Console, refer to Configuring Reporting Destination in the *Oracle Argus Safety Administration Guide*.

- Enable narrative processing for E2Bs
  You can enable automatic processing to extract additional product and event data from narrative information included in E2Bs during intake. This feature requires an additional subscription to Oracle Safety One Intake.
- Configure auto-acceptance of nullification E2Bs
  You can configure Safety One Argus to automatically accept a nullification E2B report from the “Auto-Accept” background process.
- Attach E2B ACKs to email notifications
  You can configure E2B ACKs to be attached to email notifications if your email intake source is configured to send case acceptance notifications to the sender.

Enable narrative processing for E2Bs

You can enable automatic processing to extract additional product and event data from narrative information included in E2Bs during intake. This feature requires an additional subscription to Oracle Safety One Intake.

1. Log in to Oracle Safety One Argus, and launch the **Argus Console**.
2. From the **Code Lists** menu, select **Argus**.
3. Click **Reporting Destination** from the **Browser** pane.
4. Select an existing agency or add a new one.

> **Note**
>
> See Configuring Reporting Destination in the *Oracle Argus Safety Administration Guide* for additional guidance on field descriptions and configuration options.

5. Click the **EDI** tab.
6. Select the checkbox next to **Automatically Process Narrative during Intake** to enable the Artificial Intelligence (AI) and Machine Learning (ML) extraction of narrative data into the review form.

Configure auto-acceptance of nullification E2Bs

You can configure Safety One Argus to automatically accept a nullification E2B report from the “Auto-Accept” background process.

After successful acceptance by the background process, an action item is created and attached to the case with Action Item Type, Due In -Days and Follow-up Action Item, if configured.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **System Configuration** menu and click **System Management (Common Profile Switches)**.
3. Select **Case Processing** from the **Browser** node tree.
4. Complete the following items:
   - **Follow-up Action Item for Nullification E2Bs (Auto-accept for Intake)**: Select the action item to be added to the case and specify a due date.
   - **Follow-up Action Item for Nullification E2Bs Group Assignment**: Select an action item for the group assignment.
5. Click **Save** to apply your new configurations.

Attach E2B ACKs to email notifications

You can configure E2B ACKs to be attached to email notifications if your email intake source is configured to send case acceptance notifications to the sender.

Your email intake source must have the **Send case acceptance (ACK) notification to sender** setting enabled. See Add and configure source folders for more information on the settings you can enable for email sources.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **Codelists** menu and click **Argus**.
3. Select **Reporting Destination** from the expanded **Codelists** node tree.
4. Select an existing reporting destination to modify or click the **Add New** button to create a new reporting destination.
5. In the **Add/Modify Reporting Destination**, click the **EDI** tab.
6. Select **Generate Ack and Suppress transmission of Ack** from the **ACK Transmission** drop-down list.
7. Click **Save** to commit your changes.

4

Email Intake configurations

- Select email server configuration type
  You can choose between IMAP/SMTP or Microsoft Graph API as your email server type for Intake and outoging emails for Consolidated Intake.
- Configure the email intake source name
  To be able to use email intake monitoring in the Consolidated Intake module, you need to make sure the appropriate email source name has been defined in the Argus Console INTAKE_SOURCE code list before proceeding with the additional configurations in Consolidated Intake.
- Add connection details
  You'll need to add your organization's Adverse Event (AE) report email account details to Consolidated Intake and confirm a successful connection before continuing.
- Add and configure source folders
  After confirming a successful connection to your email server, you can select which folders you want Consolidated Intake to monitor for incoming Adverse Event reports and configure details about how the reports should be processed.
- Select Success and Error folders
  You need to select the folders where Adverse Event report emails should go after being sent to Consolidated Intake.
- Set up outgoing emails
  You can configure acknowledgment (ACK) notifications to send when Adverse Event reports are successfully processed into cases. Once the overall configuration is complete and enabled, you can turn on notifications at the source level for integrated email accounts.
- Modify email accounts
  You can modify, disable, or delete existing email accounts integrated with Consolidated Intake.
- Modify general email settings
  General settings for email, such as the incoming email size limit, can be modified.

Select email server configuration type

You can choose between IMAP/SMTP or Microsoft Graph API as your email server type for Intake and outoging emails for Consolidated Intake.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Hover over the **System Configuration** menu and select **System Management (Common Profile Switches)**.
3. Click the **Intake** node in the browser.
4. In the **Select Email Server Connection Type for Intake and Outgoing Email** section of the screen, select one of the following:
   - Microsoft Graph API

- IMAP / SMTP

5. Click **Save** to confirm your selection.

Configure the email intake source name

To be able to use email intake monitoring in the Consolidated Intake module, you need to make sure the appropriate email source name has been defined in the Argus Console INTAKE_SOURCE code list before proceeding with the additional configurations in Consolidated Intake.

1. Log in to Oracle Safety One Argus and click **Argus Console**.
2. From the **Code Lists** context menu, click **Flexible Data Re-categorization**.
3. Select **Flexible Data Re-categorization** from the node tree panel.
4. In the **Code List Name** drop down menu, select **INTAKE_SOURCE**.
5. Use the table below to provide valid values during the configuration.

Table 4-1 Email INTAKE_SOURCE configurations

Attribute	Valid Values	Action
Code	Numeric	Specify any unique code.
Source_Type	2	Select **2** for email-based sources.
Source_Name	Varchar	Enter the name of the source. We recommend using something like "Email Folder Name".

> **Note**
>
> You should leave the **Triage_Required** and **Multi-Case** fields blank, as these attributes can be configured for each email source in the Consolidated Intake interface.

To continue email intake configuration, refer to the tasks listed in the Consolidated Intake configurations section of this guide.

Add connection details

You'll need to add your organization's Adverse Event (AE) report email account details to Consolidated Intake and confirm a successful connection before continuing.

Contact Oracle Cloud Support to get connection and authentication details.

1. From the context menu in the upper left corner of the screen, select **Configuration** and click **Email Intake** from the sub-menu.

   You are taken to the Email Intake Configuration interface.

2. Click **+ Add**.

   The page refreshes to display a blank configuration form.

3. In the **Add Connection** section of the form, enter the following information to connect to the right server:

Table 4-2 Add Connection fields

Field Name	Description and Notes
Email Address	Enter the full email address for the account you wish to monitor.
Host	Add the server address for the incoming mail (IMAP). This field is not applicable if your email server connection type is Graph API.
Port	Enter the port number for the IMAP communication. Typically, the number is 143 for non-secure connections and 993 for SSL connections. This field is not applicable if your email server connection type is Graph API.

> **Note**
>
> The **Enable SSL** checkbox is selected by default.

4. The **Authentication** section of the form is where you should enter information given to you by your OAuth provider:

Table 4-3 Authentication fields

Field Name	Description and Notes
Client ID	Unique identifier assigned by your OAuth provider. You can typically find this in your OAuth provider's developer portal or application registration page.
Client Secret	This is a confidential key between the application and authorization server which adds an additional layer of security. It can be found in your OAuth provider's developer portal or application registration page.
Tenant ID	The unique identifier for the tenant (e.g. Azure AD directory) where the user account can be found. If you are using Azure, you can find the ID in the Azure Active Directory section of the Azure portal.
Server Token URL	Internet address where Consolidated Intake can request an authentication token. This can be found in your OAuth provider's developer portal or in the documentation. This is only applicable if your email connection server type is IMPAP/SMTP.

Table 4-3 (Cont.) Authentication fields

Field Name	Description and Notes
Authorization Scope	This determines the level of access that Consolidated Intake has and the actions it can take on your behalf. You can find information about this in your OAuth provider's documentation.

5. Click **Connect** to validate the connection details you have entered.

   When the connection is successfully validated, an **Add Sources** form displays below the **Authentication** section.

Add and configure source folders

After confirming a successful connection to your email server, you can select which folders you want Consolidated Intake to monitor for incoming Adverse Event reports and configure details about how the reports should be processed.

The **Add Sources** form automatically displays below the **Authentication** fields after validating the connection details.

You can associate more than one source folder per email account if your organization has multiple email folders dedicated to Adverse Event reports.

When you have multiple source folders configured for a single email account, make sure that the **Source Name** is unique. You cannot configure multiple sources with identical names.

1. Select a **Source Name** from the drop down list.

   > **Note**
   >
   > The source names displayed in this list correspond to what you have configured in the INTAKE_SOURCE code list Argus Console. See Configure the email intake source name for set-up information.

2. Select a **Monitoring Folder** from the drop down list.

   The **Monitoring Folder** drop down list displays all available folders configured in your email client.

   > **Note**
   >
   > The **Inbox** folder is selected by default if it is available and not already being used as a source folder for this email account .

3. Select a **Site** from the drop down list.

4. Click **Settings**  to configure details about how you want Adverse Event reports processed for this source.

Table 4-4 Source-level settings and rules

Setting Name	Notes
Manually check all emails for validity	• Enable this setting if the source is not trusted. • Flags the record with the **Check validity** task in the **Intake Worklist**.
Automatically assess email body for Adverse Events.	• This setting is enabled by default if you have an Oracle Safety One Intake subscription. • Uses advanced extraction capabilities (AI/ML) to process the email body.
Manually determine document grouping (When emails are received with multiple documents)	• Enabled by default. • Flags the record with the **Check validity** task in the **Intake Worklist**.
Group documents as a single record (When emails are received with multiple documents)	n/a
Separate documents into individual records (When emails are received with multiple documents)	n/a
Received date to receipt date field. (Map Email Header to Case Form)	n/a
Sender name to reporter name field. (Map Email Header to Case Form)	Enabled by default.
Sender email address to reporter email address field. (Map Email Header to Case Form)	Enabled by default.
Subject line to keyword field. (Map Email Header to Case Form)	• Enabled by default. • This option will be functional in a future release.
Send case acceptance (ACK) notification to sender. (Send Notifications)	See Set up outgoing emails for additional configuration details.

The **Settings** drawer opens, displaying all possible configuration options for the source.

5. Make your configuration selections and click **Save**.

Select Success and Error folders

You need to select the folders where Adverse Event report emails should go after being sent to Consolidated Intake.

Choose one folder to send the successfully ingested reports (Success) and another folder to hold the reports that Consolidated Intake was unable process (Error). The Success and Error folders are shared amongst all sources within the email account.

1. Select a folder from the **Success Folder** drop down menu, located in the **Select Processed Email Folders** section of the form .

   All available email folders are displayed in the context menu. If available, **Archive** is selected by default.

2. Select a folder from the **Error Folder** drop down menu.
3. Click **Add** to save your newly integrated email account.

Consolidated Intake is ready to monitor your email account for AE reports.

Set up outgoing emails

You can configure acknowledgment (ACK) notifications to send when Adverse Event reports are successfully processed into cases. Once the overall configuration is complete and enabled, you can turn on notifications at the source level for integrated email accounts.

1. From the context menu, select **Configuration** and click **Outgoing Emails** from the sub-menu.

   You are taken to the Outgoing Email Configuration interface.
2. Make sure the **Send emails with this configuration** switch is enabled.
3. Complete the fields in the **Connection** and **Authentication** sections of the screen.
4. You can create custom SMTP header text appended to the body of the acknowledgment email by switching on **Enable Custom SMTP Header**.

   The default header text is *Confidential: Please treat this email as confidential.*
5. Click **Test & Update** to save the outgoing email details and send a test email.

Once a successful test email has been received with the outgoing email configuration, you can switch on the **Send case acceptance (ACK) notification to sender** option located in the **Settings** for each source folder.

Modify email accounts

You can modify, disable, or delete existing email accounts integrated with Consolidated Intake.

1. From the context menu in the upper left corner of the screen, select **Configuration** and click **Email Intake** from the sub-menu.

   You are taken to the Email Intake Configuration interface.
2. On the left side of the screen, select the email account you wish to modify. Use the search function to quickly narrow the list of accounts.
3. To remove the account from Consolidated Intake monitoring, click **Delete**, located below the search field in the left panel.
4. To disable an email account, click **Disable** in the lower right corner of the screen, below the details of the selected account.
5. To modify the email account, click **Edit** in the lower right corner of the screen.

   The screen refreshes to show all fields as editable.

   - If you are editing the Connection or Authentication details, you will be prompted to validate the connection to the email server again.
   - You can add additional source folders or edit existing sources. Use the **Actions** menu located near each source to update **Settings**, **Disable** the source folder, or **Delete** the source.
6. Click **Update** to save the changes.

Modify general email settings

General settings for email, such as the incoming email size limit, can be modified.

1. From the context menu in the upper left corner of the screen, select **Configuration** and click **Email Intake** from the sub-menu.

   You are taken to the Email Intake Configuration interface.

2. Click **Settings** in the upper right corner of the screen.

   A panel displays on the right side of the screen.

3. Update the value in the **Incoming Email Size Limit (MB)** field.

   > **Note**
   >
   > The default incoming email size limit value is 50 MB. If you change the size limit, make sure that the new limit is equal to or greater than the maximum size limit supported by your email service provider. This prevents email rejection by Consolidated Intake due to size constraints

4. Click **Apply** to save the changes.

5

API Intake configurations

Configure the API intake source

You can set up external APIs that send documents to Oracle Safety One Argus to be reviewed in the Intake Worklist. In this configuration step, you need to define a source name in the INTAKE_SOURCE code list for external APIs and how the documents coming from the API will be handled.

APIs must be configured in the OCI Cloud configuration console before continuing.

1. Log in to Oracle Safety One Argus and click **Argus Console**.
2. From the **Code Lists** context menu, click **Flexible Data Re-categorization**.
3. Select **Flexible Data Re-categorization** from the node tree panel.
4. In the **Code List Name** drop down menu, select **INTAKE_SOURCE**.
5. Use the table below to provide valid values during the configuration.

Table 5-1 INTAKE_SOURCE configuration

Attribute	Valid Values	Description	Notes
Source_Type	0, 1	0 = Source is Manual Upload 1 = Source is API	For API sources, the Source_Type must always be 1.
Source_Name	Varchar	The Source_Name specified here is displayed with ingested records in the Intake Worklist's **Source** column.	We recommend using the API Contract Name as the Source_Name.

Table 5-1 (Cont.) INTAKE_SOURCE configuration

Attribute	Valid Values	Description	Notes
Triage_Required	0, 1	0 = Trusted Source 1 = Untrusted Source	• This attribute only applies to Source_Type = 1. • If Triage_Required = 0, then the ingested record from the corresponding API Source skips the manual Check Validity task. • If Triage_Required = 1, then the ingested record from the corresponding API Source is always flagged for manual Check Validity and appears in the Intake Worklist. • If the incoming API request contains Triage_Required value, then it takes precedence over the Triage_Required value configured at source.
Multi-Case	0, 1	0 = All documents are treated as one case 1 = Each document is treated as a single case	• This attribute is applicable only when there are multiple documents in one record. • If Multi-Case = 0, then the multiple documents in the ingested record are treated as a single case. • If Multi-Case = 1, then each document in the ingested record is treated as a single case, resulting in multiple potential cases. • If the incoming API request contains Multi-Case flags, then it overwrites the Multi-Case state configured at source. • This attribute is only applicable when Source_Type = 1.

6

CRO configuration

- Publish intake records to a sponsor-owned safety database for case processing
  If you represent a Contract Research Organization (CRO), you can configure your intake workflow to publish records to a sponsor-owned safety database for case processing after intake has been completed. This option is only available when CRO mode is enabled.

Publish intake records to a sponsor-owned safety database for case processing

If you represent a Contract Research Organization (CRO), you can configure your intake workflow to publish records to a sponsor-owned safety database for case processing after intake has been completed. This option is only available when CRO mode is enabled.

1. Log in to Oracle Safety One Argus and launch the **Argus Console**.
2. Select **System Configuration** and click **System Management (Common Profile Switches)**.
3. Expand the **Intake** node in the **Browser** file tree and click **Intake Processing**.
4. Select the **Yes** radio button for the **Submit Intake record to external system for further Case Processing** field to enable publishing to a third party system.
5. Select the **Method of submission**:
   - **Email**: Select the reporting destination from the **Reporting Destination for Email Configuration** drop down list.
     - The recipient ("To") email is pulled from the email address field on the Agency Information tab of the Reporting Destination. See Configuring Reporting Destination in the *Oracle Argus Safety Administration Guide* for more information about populating these fields.
     - To send intake records to multiple recipients, you can use the cc and bcc fields on the SMTP table of the Reporting Destination. See Configuring Reporting Destination in the *Oracle Argus Safety Administration Guide* for more information about populating these fields.
     - The sender ("From") is taken from the Outgoing Emails configuration in Oracle Safety One Intake. See Set up outgoing emails for more information.
     - The email subject for records published this way is `Safety One: <Intake Number> <Source> <Type>`.
   - **REST API**: This option can only be used to publish reports to Oracle Argus Safety databases. After selecting this option, you need to complete the configuration details in the **REST API Configuration** fields.

7

Advanced Extraction configuration

Document Extraction and AI configuration

The configuration of recipes for advanced extraction and AI predictions for ingested documents is done by the intake designer via API. You must have an Oracle Safety One Intake subscription to use advanced extraction..

Configuring the recipes for Consolidated Intake is restricted to users who have the **Intake Designer** role. See Add users and assign roles for more information about the roles applicable to Consolidated Intake.

> **Note**
>
> An out-of-the-box CIOMS recipe is available in the eTRM documentation.

Have your Intake Designer refer to Create a new recipe configuration in the *REST API Guide for Safety One Intake* for more information.