

IBM StoredIQ for Legal 2.0.3.10  
Version 2.0.3.10

*Installing, administering, and managing  
IBM StoredIQ for Legal*



**Note**

Before using this information and the product it supports, read the information in [“Notices” on page 267.](#)

This edition applies to version 2.0.3.10 of IBM® StoredIQ® for Legal (product number 5725-W53) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2016, 2020.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

- ibm.com and related resources..... V**
  - Contacting IBM.....v
- What's new in StoredIQ for Legal V2.0.3..... 1**
- What's changed in StoredIQ for Legal V2.0.3..... 13**
- Overview.....18**
- Planning.....19**
  - Planning for deploying StoredIQ for Legal..... 19
  - Planning for importing people into StoredIQ for Legal..... 21
  - Planning for people and users ..... 22
  - Planning for secure matters..... 23
  - Planning for custodian notifications.....25
  - Planning for the global hold reminder.....27
  - Planning for notice changes ..... 31
  - Planning for workflows..... 32
  - Planning for automating fulfillment item creation..... 33
  - Planning for fulfillment automation..... 34
  - Planning for reports..... 35
- Deploying and configuring.....41**
  - Deploying and configuring StoredIQ for Legal as a virtual appliance..... 41
  - Deploying and configuring StoredIQ for Legal on OpenShift.....53
  - Migrating from StoredIQ for Legal (VM) to StoredIQ for Legal (Container)..... 57
  - Configuring system settings..... 58
  - Configuring connections to external servers or services.....62
  - Putting the system into maintenance mode..... 67
- Customizing..... 68**
  - Customizing attributes.....68
  - Customizing jurisdictions.....70
  - Creating global messages.....71
  - Setting a welcome message.....71
  - Configuring the person history view.....72
  - Setting user preferences.....73
- Managing..... 74**
  - Managing the people to use StoredIQ for Legal..... 74
  - Managing workflows.....79
  - Managing matters.....80
  - Managing the global hold reminder.....85
  - Managing templates.....86
  - Managing hold notices.....93
  - Managing interviews.....99
  - Managing data boxes.....103
  - Managing data requests.....105
  - Managing tasks.....118

Managing notifications.....	120
Creating and viewing reports.....	123
Importing data by using the import API.....	168
Exporting lists as CSV.....	191
Migrating IBM Atlas Policy Suite data.....	192
<b>Monitoring and auditing.....</b>	<b>207</b>
Monitoring APIs.....	207
Monitoring system alerts.....	219
Auditing.....	220
<b>Troubleshooting and support.....</b>	<b>233</b>
Before contacting IBM Support.....	233
Troubleshooting techniques.....	233
Known problems and solutions.....	235
Searching the knowledge bases.....	239
Getting fixes from Fix Central.....	240
Contacting IBM Support.....	241
Exchanging information with IBM.....	241
Subscribing to updates.....	241
Collecting log and trace data.....	242
Disaster recovery with vSphere Replication.....	243
Managing the size of string attributes.....	244
<b>Reference.....</b>	<b>247</b>
Administration scripts.....	247
Default file names.....	249
Nonmodifiable data request attributes.....	250
Server discovery Java class reference.....	250
Server discovery WSDL reference.....	252
Workflow services.....	255
<b>Notices.....</b>	<b>267</b>
Trademarks.....	268
Terms and conditions for product documentation.....	269
IBM Online Privacy Statement.....	269

## ibm.com and related resources

---

Product support and documentation are available from [ibm.com](http://ibm.com)<sup>®</sup>.

### **Support and assistance**

From [ibm.com](http://ibm.com), click **Support & downloads** and select the type of support that you need. From the Support Portal, you can search for product information, download fixes, open service requests, and access other tools and resources.

### **IBM Knowledge Center**

Online product information for the latest product release is available in IBM Knowledge Center at: [IBM StoredIQ for Legal](#).

## Contacting IBM

---

For general inquiries, call 800-IBM-4YOU (800-426-4968). To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).


For more information about how to contact IBM, including TTY service, see the Contact IBM website at <http://www.ibm.com/contact/us/>.



---

# What's new in StoredIQ for Legal V2.0.3


Learn about the main new features in IBM StoredIQ for Legal Version 2.0.3.

The following sections also lists any change to existing features. In the documentation, information that applies to Fix Pack 10 only is marked with the icon  or starts with "Starting with Fix Pack 10".

Technical changes and major changes to the text are indicated by a revision bar next to the revised content.

## What's new or changed in V2.0.3.10

### Additional deployment type


As an alternative to deploying the product as a virtual appliance on a VMware hypervisor, you can now also deploy a containerized version of IBM StoredIQ for Legal in a Red Hat® OpenShift® environment. Basically, the functionality is the same for both deployment types. Where it is necessary to differentiate between the deployment types, the virtual appliance is referred to as *StoredIQ for Legal (VM)* and the containerized version is referred to as *StoredIQ for Legal (Container)*.  [Learn more...](#)

A set of administration scripts is provided with StoredIQ for Legal (Container).  [Learn more...](#)


### Automatic cleanup of import requests

Once a month, IBM StoredIQ for Legal checks for import requests older than 1 month and deletes such import requests along with any associated attachments.


### Bulk transfer of tasks

You no longer have to assign or reassign tasks one by one but can transfer sets of tasks in one go.  [Learn more...](#)


### Customizable instructions for the Have Questions? links in the custodian portal

You can now provide customized information to be displayed when users click any of the **Have Questions?** links.  [Learn more...](#)


### Customizing form field behavior

You can now customize form field behavior in the user interface instead of exporting the form to be make such changes in the JSON file and importing the updated form.  [Learn more...](#)

### Export people list

You can now export (filtered) person lists from the people and group catalogs to a CSV file.  [Learn more...](#)


### Fulfillment connector advanced settings

You can now set the logging level for fulfillment connectors where each connector can have a different one. The available levels correspond to the standard StoredIQ for Legal logging levels.  [Learn more...](#)

### Larger values for the resultsize attribute allowed

The GUI input field based on the resultsize attribute now accepts numbers up to a maximum of 9007199254740991 as input.

### Limiting the release scope by date range

As a configurable option, release data requests can now be limited to specific date ranges. Such reduction is possible at the data request level, at custodian level, or at fulfillment item level.  [Learn more...](#)

Additional columns in the rep\_fulfillment\_view reporting view were introduced for this feature.

### **New parameter for the migration tool**

The StoredIQ for Legal deployment type is a new positional parameter for the migration tool. [Learn more...](#)

### **New starting action for workflows**

The new starting action **Person - Update** can be used to trigger a workflow whenever person attributes are updated in StoredIQ for Legal.

### **New workflow services method**

The matter workflow service has a new method that you can use to retrieve some statistical information about the matters in the system. [Learn more...](#)

### **Server discovery connectors**

If you use server discovery services to have your workflows automatically create fulfillment items, you can now register such services with StoredIQ for Legal and manage the respective jobs in the GUI. [Learn more...](#)

New audit events were also introduced for this feature.

### **Silent custodians in hold notices**

You can now include custodians on silent hold in active hold notices. Such custodians are called *silent custodians*; they are not notified of the active hold. Silent custodians appear in all matter statistics so that the custodian counts on preservations and on holds now match at all times. [Learn more...](#)

New audit events, new target entities for import, and the `rep_notice_silent_custodians_view` reporting view were also introduced for this feature.

### **Snapshots of custodian information**

You can now configure StoredIQ for Legal to take a snapshot of the person attribute values for a custodian in a data request to make changes in the person history during the lifetime of a data request visible. [Learn more...](#)

### **Tools for managing the size of string attributes**

StoredIQ for Legal now provides scripts to check the size of custom string attributes and to change the size if necessary. [Learn more...](#)

### **Updated import command line interface (CLI)**

The import CLI was updated to version 1.3.0 to support imports into StoredIQ for Legal instances that are deployed on Red Hat OpenShift. When registering a client, you must now provide the deployment type as an argument. [Learn more...](#)

## **What's new in V2.0.3.9**

### **Direct links to document sets in IBM StoredIQ**

If you have IBM StoredIQ for Legal set up to work with IBM StoredIQ for fulfilling data requests, you can now enable direct links to the resulting document sets in IBM StoredIQ for closer examination. This option is part of the IBM StoredIQ connection settings and works for IBM StoredIQ installations at version 7.6.0.17 or later. [Learn more...](#)

### **Maintenance mode**

You can now put IBM StoredIQ for Legal in maintenance mode to prevent users from signing in during maintenance. [Learn more...](#)

### **Release preservation**

This new feature allows to release data after the legal obligation to preserve it is removed. It must be explicitly enabled and cannot be disabled again. [Learn more...](#)

The feature introduces a new type of data request, the *release data request*, along with the option to create the respective forms, workflows, and templates. Release data requests can be created for completed preservation or preservation and collection data requests. You can release all or part of the data preserved for a matter. [Learn more...](#)



A new audit event and additional columns in the rep\_datarequest\_view and rep\_fulfillmentitem\_view reporting views were also introduced for this feature.

### Reopening matters

You can now configure whether you want to allow users to reopen matters after they were closed. [Learn more...](#)

### Support of additional VMware platforms

IBM StoredIQ for Legal can now also be deployed and managed in VMware vSphere 6.5.

### System alerts

IBM StoredIQ for Legal now provides system alerts for several issues. You can view such alerts in the **Admin** section. In addition, you can enable alert notification. [Learn more...](#)

### Welcome message

You can now provide a welcome message to your users which is displayed whenever they sign in to IBM StoredIQ for Legal. [Learn more...](#)

## What's new in V2.0.3.8

### Deletion of task comments and attachments

In the task view, users can now delete task comments and attachments. A new system setting defines whether this feature is turned on or off. By default, it is turned off for upgrade installations and new installations.

### Migration of requests from IBM Atlas Policy Suite

In addition to notices and interviews, you can now also migrate requests IBM Atlas Policy Suite to IBM StoredIQ for Legal. [Learn more...](#)

### New workflow services methods

The data request workflow service has two new methods that you can use in combination with existing workflow service methods to clone a data request, update the new data request, and submit it within a workflow script. [Learn more...](#)

The matter workflow service has three new methods that you can use to retrieve a list of the notices, the interviews, or the data requests within a matter. [Learn more...](#)

## What's new in V2.0.3.7

### Attributes for additional objects

A basic set of attributes is now available for interviews that you can customize and expand by adding your own custom attributes.

Interview attributes appear in a separate **Interview Information** page. Attributes with a specific data type can be included as system variables in interview templates and interviews. [Learn more...](#)

### Fulfillment automation

IBM StoredIQ for Legal now provides the means to fully automate fulfillment of work package items, for example, submitting the fulfillment items within a work package to a ticketing system or submitting them to other fulfillment tools that support automatically preserving or collecting items. You can define different levels of automation: full automation, a combination of manual and automatic fulfillment, or no automation. Fulfillment automation is implemented by means of the IBM StoredIQ for Legal Policy Syndication Framework and the IBM StoredIQ for Legal Policy Syndication SDK. [Learn more...](#)

### Key-based access control

For an extra level of security, you can now restrict access to a matter based on specific keys such as a location code. [Learn more...](#)

Access to reports can also be based on keys depending on the report definition. [Learn more...](#)

### **Migration of interviews from IBM Atlas Policy Suite**

In addition to notices, you can now also migrate interviews IBM Atlas Policy Suite to IBM StoredIQ for Legal. [Learn more...](#)

### **New user preference option**

In the **User Preferences** section, you can now enable a multi-select filter option for the work packages list. If enabled, you can select a set of data source categories for which you want to view work packages. [Learn more...](#)

## **What's new in V2.0.3.6**

### **Migration of notices and notice related information from IBM Atlas Policy Suite**

Notice transmission and response records are now also migrated and attached to the migrated notice as CSV files. The migration tool provides a new option for updating already migrated notices with that information.

In addition, you can now migrate notices stored in IBM Db2® in IBM Atlas Policy Suite. Supported Db2 versions are version 10.5 and later. [Learn more...](#)

### **New filtering option for work packages**

When you submit several work packages at once, it might take some time until all of these work packages have the status **Open**. Therefore, you can now filter the list of work packages for those that still have the status **Submitted** to check the progress. [Learn more...](#)

### **New user preference option**

In the **User Preferences** section, you can now configure which information is displayed in the work packages list. You can specify different settings for draft, open, completed, or canceled work packages. [Learn more...](#)

### **Support for iPhone mobile devices**

You can now access the custodian portal also on an Apple iPhone 8 mobile device to view and respond to notifications by using the Safari iOS web browser. [Learn more...](#)

## **What's new in V2.0.3.5**

### **Additions to the import API**

The import API includes the following additions:

- When you import people by means of the `persondistinct` target entity, you can now specify an alias to directly create relationships. [Learn more...](#)
- Cleanup of person history information. [Learn more...](#)
- New target entities `persondistincthistory` and `persondistinct_delete`. [Learn more...](#)

### **Migration of hold notices from IBM Atlas Policy Suite**

If you want to move from IBM Atlas Policy Suite to IBM StoredIQ for Legal for hold notice management, migrate hold notices. [Learn more...](#)

For migrated notices, also a new built-in report and new reporting views for custom reports are provided.

## Person history

In a *person history*, change records reflect updates to a person's profile. You can configure whether a change history view is available in the user interface and whether changes to person attributes are tracked automatically. [Learn more...](#)

A new person history report and a corresponding reporting view for custom reports are also available.

## Report definition enhancements

You can now create custom reports for specific hold notices, interviews, or data requests by adding the `ilg_rpt_entitySpecific=true` property and the appropriate `entitytype` and `entityid` definitions to your report design.

## What's new in V2.0.3.4

### Adding multiple files at once

You can now define a custom attribute that allows for selecting multiple files to be added at once, for example, when you add attachments to matters.

### Additional information in the matter list

The matter list now also provides information about the numbers of open and closed data requests in a matter.

### Attributes for additional objects

A basic set of attributes is now available for hold notices and tasks that you can customize and expand by adding your own custom attributes.

Hold notice attributes appear in a separate **Notice Information** page. Attributes with a specific data type can be included as system variables in hold notice templates and hold notices. [Learn more...](#)

Task attributes define what is displayed in the task list on the **Tasks** page. They can also be used to tailor your task queries. [Learn more...](#)

### Filtering on canceled tasks and work packages

Tasks that you canceled are no longer grouped with the tasks that you completed but are now listed in a separate **Canceled Tasks** page.

In addition, you can filter the list of work packages by canceled work packages. [Learn more...](#)

### Modifying published hold notices

You can now update published hold notices and republish them as required. [Learn more...](#)

### New naming conventions for exported files


The default names of files that are created by StoredIQ for Legal now follow a new naming convention. The new format ensures that you can uniquely identify such files and avoids accidental overwrites with new exports. [Learn more...](#)

### New reports and reporting views

Several predefined cross-matter and matter-specific reports were added:

- Active Matter Summary Report
- Custodian Non-Confirmed Hold Notice - Matter Detail
- Global Hold Reminder Report
- Master List Report
- Notice Confirmation Report
- Notice History Report

- Notice Recipients List
- Organization Structure Report
- User Audit Report
- User Information Report
- User Login Report

 [Learn more...](#)

In addition, several reporting views were added in these categories:

- Hold notice views
- Interview views
- Global hold reminder views
- Organization structure views

To learn more about the new reporting views, see the respective subsections of the [“Creating and viewing reports”](#) on page 123 section.


### **Sending copies of hold notice or interview messages**

You can now send copies of the messages in published hold notices and interviews to members of your team for informational purposes.


### **Separate pages for task comments and activities and for attachments associated with a data request**

Each data request now has two additional pages:


- A **Task Information** page to provide you with an overview of all task comments, attachments, and activities pertaining to a data request. This information is also provided at work package level.
- An **Attachments** page to provide you with an overview of all attachments associated with the data request and for quick access to these attachments

 [Learn more...](#)


### **Support of mobile devices**

You can now access the custodian portal on an Apple iPad tablet computer to view and respond to notifications by using the Safari iOS web browser.  [Learn more...](#)

### **Task search enhancements**


Using **Advanced Search** on the **Tasks** pages, you can now create, save, share, load, and delete custom task queries.  [Learn more...](#)

### **Tracking negative identification results**

You can now also create and track work packages when no data could be identified on the data source for a specific custodian.  [Learn more...](#)

## **What's new in V2.0.3.3**

### **Duplicate data requests**

Instead of creating a data request from scratch, you can duplicate an existing one.  [Learn more...](#)

### **Work package status and progress**

To provide a better overview of the status and progress of the work packages, more details are now available in the GUI: on the **Matters** and **Data Requests** dashboards and on the page where the work packages are listed. Each new detail is defined as an attribute on the **Data Request Attributes** or **Work Package Attributes** page.

## What's new in V2.0.3.2

### Add data sources to several custodians

You can now add data sources to several custodians at a time and remove data sources from several custodians. [Learn more...](#)

### Audit events

More audit events have been added. [Learn more...](#)

### Clean up history-related data

You can now clean up the department hierarchy and the employment history by removing all changes that you made on and after a specific time stamp. [Learn more...](#)

### Configurable person information

You can now select the person attribute that is used as an additional descriptor in person selection lists, so that the person can be clearly identified. In addition, you can configure which information is displayed when hovering over a name.

### Custom matter attributes for use as system variables

Custom matter attributes with a specific data type can be included as system variables in hold notice templates, hold notices, interview templates, and interviews, regardless of whether those attributes were added in V2.0.3.2 or earlier. [Learn more...](#)

### Customizations to the reporting database

You can now apply customizations to the reporting database by storing a customization file in SQL format in the StoredIQ for Legal system. [Learn more...](#)

### Escalation in hold notices and interviews

If a custodian does not respond to a hold notice or an interview, the custodian's manager can be informed. You can now specify which follow-up message prompts the escalation.

### Export and import attribute information

You can now export and import the information for predefined and custom attributes. [Learn more...](#)

### Global hold reminder

Instead of sending a reminder for each hold notice, you can consolidate a custodian's reminders. Due to this function, the layout of the hold notice and the hold notice template has slightly changed. [Learn more...](#)

### Monitoring statistics

New REST API endpoints provide a statistics about the StoredIQ for Legal objects in the database. [Learn more...](#)

### New mapping attribute for data import by using the import API

To resolve references to an item in another target entity or set of target entities, the `readallitems` attribute now determines how the cache is populated. [Learn more...](#)

### Override global information when adding custodians to a data request

When you add existing custodians from a CSV file to a data request, you can now override the custodian priority, the date ranges, and the fulfillment instructions. [Learn more...](#)

## People's involvement in matters

Each UI page that lists people or custodians shows whether a person is involved in a matter and has any hold obligations. In addition, you can find out which hold notices, interviews, and data requests the person is involved in. [Learn more...](#)

## Script for changing the report administrator password

StoredIQ for Legal now provides a console tool for changing the report administrator password. [Learn more...](#)

## Shared resources for reports

You can now make BIRT style sheets, or property and library files available as shared resources for all your custom reports. This provides for a common look and feel of your reports.

## Split work packages

You can now split the work packages that are created for a data request. [Learn more...](#)

## Status history

When you view a published hold notice, the **Status** column provides access to each custodian's status history. This history reflects all status updates for the selected custodian.

## Terminate workflow instances

You can now view a list of all active workflow instances to identify and terminate instances that have been active for longer than expected.

## What's new in V2.0.3.1

### Ad hoc import of people in interviews

You can now also use the ad hoc import to add custodians to an interview. The custodians must be able to sign in to StoredIQ for Legal. [Learn more...](#)

### Configurable confirmation link

You can now configure confirmation pages with or without the **Contact me** link by including the respective system variable in the content section of your hold notice template or hold notice.

### Data source categories in data requests

If the workflow that is used by a data request generates a list of data source categories, the selection of data source categories in data requests can be made optional. [Learn more...](#)

### Import of people

Each person in the catalog is uniquely identified by an attribute. You must now select the person attribute that is used as identifier before you can import any people from the directory server or by using the import API. [Learn more...](#)

### More details about audit events

More workflow-related details are now available about an audit event. [Learn more...](#)

### New API privileges

To use the import API, you now need additional privileges. These privileges are not necessary for the ad hoc import of people. [Learn more...](#)

### New reporting view

The new Jurisdiction view (rep\_jurisdiction\_view) provides details about the jurisdictions that are defined in StoredIQ for Legal. [Learn more...](#)

## New target entity and default import mapping

A default import mapping is available for the new target entity `interview_custodians_adhoc`. [Learn more...](#)

## SAML SSO without LDAP

You can now configure SAML single sign-on (SSO) if no internal or external LDAP server exists. [Learn more...](#)

## Scope for custodian search

For simple searches in the people catalog, you can now exclude specific columns from search. Right-click a column header and clear the **Searchable** checkbox.

## Submitting sets of work packages

Besides submitting individual work packages, you now have the option to submit all or a subset of work packages at once. [Learn more...](#)

## What's new in V2.0.3.0

### Attributes expansion

- In addition to person attributes, a process administrator can now customize attributes for data sources, data requests, fulfillment items, work packages, organizations, matters, servers, and applications.
- A process administrator can now customize new default person attributes like job title, employment status, termination date, and a planned return from leave date. A variety of new choice list data types are now available as well.

[Learn more...](#)

### Auditing

You can view details about the actions that were recorded. [Learn more...](#)

### Client registration for REST APIs

A programmer that is using the import REST API must now register their client with StoredIQ for Legal. [Learn more...](#)

### Copying templates and forms to another system

You can now copy hold notice templates, interview templates, and data request forms to another system by exporting and importing them. [Learn more...](#)

### Courtesy copies of hold notices

You can now send hold notices to people who are not on hold, such as managers of the custodians. [Learn more...](#)

### CSV import of custodians to add

When a paralegal adds or updates the custodians on a notice, interview, or data request, the paralegal can now opt to add all of the custodians at once, in bulk, from a delimited CSV text file. This option is particularly useful for notices, interviews, or data requests that require a large number of custodians. Note that for the custodians to be added successfully, they must already exist in the StoredIQ for Legal system. When selecting the CSV file to upload, you can also download a sample CSV file to use as a template. [Learn more...](#)

### CSV import of roles, organization trees, person history, matters, and data sources

A programmer can now create or update entities such as roles, organization trees, person history, matters, and data sources in StoredIQ for Legal by importing a delimited CSV text file. A programmer can also import a CSV text file to assign roles. [Learn more...](#)

### CSV import of people

You can now import people from a CSV file. [Learn more...](#)

### CSV import of security groups

A programmer can now create or update security groups in StoredIQ for Legal by importing a delimited CSV text file. [Learn more...](#)

### CSV import of data source applications and data source servers

A programmer can now create or update data source applications and data source servers in StoredIQ for Legal by importing a delimited CSV text file. [Learn more...](#)

### Custodian-related actions across all matters

You can suspend and resume all hold notices and all interviews for selected custodians. You can conclude all interviews for selected custodians. In addition, you can release selected custodians from all hold notices. [Learn more...](#)

### Custom reporting using reporting views

You can run specific queries on the StoredIQ for Legal database in order to customize your own reports. [Learn more...](#)

### Custom reports

StoredIQ for Legal supplies predefined reports. You can now import report definitions to create custom reports. [Learn more...](#)

### Data boxes now require data box privileges and data locales

To create view and manage data boxes, you now need **View Data Boxes** and **Manage Data Boxes** privileges. To configure data source types for data box requests to be fulfilled by StoredIQ for Legal, you must now go to **Admin > Content Settings > Data Locales** instead of **Admin > Content Settings > Data Request**. [Learn more...](#)

### Data request forms

You can now create forms from scratch. [Learn more...](#)

### Data requests

You can now create requests for identifying data, preserving data, collecting data, or preserving and collecting data. The requests are fulfilled manually by a fulfillment team. You need a *StoredIQ for Legal eDiscovery for IT* license to use this data requests feature. [Learn more...](#)

### Data request automatic refinement

You can now automatically refine a data request by adding data sources for a custodian with additional custodian related information for the data source by using a CSV file. [Learn more...](#)

### Data request fulfillment results

You can now add fulfillment results from a CSV file. [Learn more...](#)

### Disaster recovery

You can set up an ESX-based disaster recovery solution for StoredIQ for Legal that uses vSphere replication. [Learn more...](#)

### Global messages

A process administrator with the **Manage Content Settings** privilege can now create two types of global messages to inform StoredIQ for Legal users: broadcast messages (important **News** alerts to signed-in users) and compliance messages (non-distracting reminder messages that display on every screen). [Learn more...](#)

### Jurisdiction

People and data sources can now share a common jurisdiction attribute that starts with a default selection of countries and country codes. A process administrator with Content Settings privileges can customize the exact list of jurisdictions to allow or hide for your organization. [Learn more...](#)

### Licensed programs

StoredIQ for Legal now supports integration with the IBM License Metric Tool (ILMT) for programs licensed by User Value Unit (UVU). If you do not have a license for a particular program, then a system administrator can hide all of the functions for that program. [Learn more...](#)



### Limited-access reports

You now need a new **View limited-access reports** privilege (previously called **View Sensitive reports**) to run or view reports with secure information in them, such as custodians-on-hold reports.

[!\[\]\(919a2cb85b99741a73c0c31a427236a8\_img.jpg\) Learn more...](#)

### Logs command line arguments

The `/siq/bin/logs` command features new command line arguments. [!\[\]\(c3d993ca47bfe2a953c700506ce31fa0\_img.jpg\) Learn more...](#)

### Matter lists, task lists, custodian lists

You can now export matter lists, task lists, and custodian lists as CSV. [!\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\) Learn more...](#)

### Matter reports

The reports on custodians, hold notices, and the audit history of a matter have been removed from the

**Reports** page. [!\[\]\(faf942dc3e59ce8eb64b4ac481eca7e0\_img.jpg\) Learn more...](#)

### Matter security

You can now restrict access to matters by using security groups or by creating sensitive matters. [“Planning for secure matters” on page 23](#)

### Message editor enhancements

- You can now insert certain system variables in the message subject line for notices and interviews.
- You can now apply style and add images to interview question text.
- You can now resize and align images.
- You can now click the **Check Accessibility** button to identify simple accessibility issues in the text.

### Metrics and health checking

StoredIQ for Legal now provides REST API endpoints to return metrics and health checks. [!\[\]\(4f6bf54ae7e4144a72d78316053e412d\_img.jpg\) Learn more...](#)

### Notification settings for a system administrator

In the **Email Server** panel, a system administrator with the Manage External Servers privilege can now specify a **From address** and a **Reply to address** for emails related to custodian, alert, and system notifications. [!\[\]\(56549452e01ca28bdf2500ced9653143\_img.jpg\) Learn more...](#)

### Privileges

The **View Users and Roles** and **Manage Users and Roles** privileges has changed. Part of their scope is now covered by the new privileges **View People** and **Manage People**. [!\[\]\(19d44b37fb4fa155bf9d60c77a3d3cb2\_img.jpg\) Learn more...](#)

### Report formats

Depending on the report definition, reports can now be created in the following formats: CSV, HTML, or PDF. [!\[\]\(bff896c19919791b89ab521f039b410a\_img.jpg\) Learn more...](#)

### Reporting database

The reporting database can now be refreshed more often than once a day. [!\[\]\(9f3852d68d41e1e95bc4ec10e81aba4b\_img.jpg\) Learn more...](#)

### Resume hold notices

You can now resume a hold notice that has been suspended. As a result, messages will be sent to custodians again according to the original schedule. [!\[\]\(206536f97fdb267876a3a10ea42b0254\_img.jpg\) Learn more...](#)

### Scripts now require the system administrator password


Most of the console tools now prompt you for the system administrator (ilgadmin) password, unless you already set it at the command line. [!\[\]\(241407ae374027aec4b030ca93d07b05\_img.jpg\) Learn more...](#)

### Single sign-on

To prevent unauthorized access to StoredIQ for Legal in a SAML single sign-on (SSO) environment, you can ensure that people must authenticate again when they try to access StoredIQ for Legal in the same browser where they signed out. You can now specify a URL that invalidates a session in your SSO environment as part of your system settings.

### **Suspend and resume a hold notice or interview for specific custodians**

You can now suspend and resume hold notices or interviews for specific custodians. Performing a suspend on custodians pauses the hold notice or interview from sending any further messages to them, and resume ends the suspension and sends messages again according to the original schedule.


 [Learn more...](#)

### **Suspend and resume interviews**

You can now suspend an interview to pause it from sending any further messages to the custodians. To end the suspension and send messages again according to the original schedule, resume the

interview.  [Learn more...](#)

### **System settings additions**


In the system settings panel, a system administrator can now configure settings such as licensed programs to hide, reporting database scheduling, security groups, the maximum file size for attachments, and an option to specify your own URL for help information.  [Learn more...](#)

### **Tasks**


All StoredIQ for Legal users can now manage tasks from the new **Tasks** page. Users can complete tasks, assign new tasks, claim or return tasks, or approve or reject approval tasks. [“Managing tasks” on page 118](#)

### **User preferences**


In the new **User Preferences** option under your user name, you can now configure personal

**Notification Settings** and **Out of Office Settings**.  [Learn more...](#)

### **Viewing users by role**

You can now view all users that have the same role.  [Learn more...](#)

### **Workflow definitions**

A process administrator with the **Manage Workflow Definitions** privilege can import workflow definitions. Workflows are required by data requests. In addition, workflows can be associated with an action that relates to a matter, a hold notice, or an interview, for example, requiring an attorney to give approval before a matter can be closed.  [Learn more...](#)

---

# What's changed in StoredIQ for Legal V2.0.3

Learn about changed, deprecated, or discontinued functionality.

Technical changes and major changes to the text made to versions up to V2.0.3.9 are described here. Starting with V2.0.3.10, such changes are reflected in [What's new](#).

## What's changed in V2.0.3.10

Starting with this release, any changes (technical or major documentation changes) are no longer listed in this topic but reflected in [“What's new in StoredIQ for Legal V2.0.3” on page 1](#) for easier retrievability.

## What's changed in V2.0.3.9

### Changes to the delete subcommand of the migration tool

The **delete** subcommand of the migration tool can now be used only to delete migrated requests. For general deletion of migrated items, run the migration tool with the **cleanup** option.

### Migration of IBM Atlas Policy Suite entities

The batch size for a single run of the migration tool to migrate IBM Atlas Policy Suite entities is now limited to 200 entities per run.

### Naming of data request duplicates

The default name of the first copy of a data request was changed to now also include the number of the copy: *original\_DR\_name - Copy (1) of DR\_ID*

### New status for data requests

To be able to distinguish canceled data requests from regularly completed data requests, canceled requests now have the status **Complete (Canceled)** instead of just **Complete**.

## What's changed in V2.0.3.8

### Date range changes for submitted data requests

Date ranges in data requests can now be modified even after the data request is submitted. After a date range is modified, a new work package is created with the new date range. The modified date range is not propagated to work packages that were created prior to the change.

### Default SSL protocol

The default SSL protocol is now TLSv1.2. If your environment does not allow for this setup, you can revert to the previously used SSL\_TLSv2 protocol. To do so, change the SSL configuration in your IBM WebSphere® Application Server installation. For more information about the configuration changes, see the topic about [SSL configurations](#) in the IBM WebSphere Application Server documentation.

### Result size unit

The result size of fulfillment items and work packages can now also be specified in bytes.

### Size of the fulfillment item comment attribute

The size of the comment attribute of fulfillment items has been extended so that it can now hold up to 5,000 characters.

## What's changed in V2.0.3.7

### New data source attribute

The set of predefined data source attributes was expanded by the new attribute `automationconnector` (initial display name **Automation Connector**) of the data type Drop-down list (single-select). This attribute is intended to hold the IDs of all connectors for fulfillment automation that are registered with StoredIQ for Legal. This information can then be used in automation workflows.

## Work Packages list filtering

Instead of filtering the work packages list by either status or data source category, you can now combine status and data source category filters.

## What's changed in V2.0.3.6

### Changes to the advanced search for matters, persons, or tasks

In the advanced search for matters, persons, or tasks, you can now also select **(Any)** or **(Unassigned)** as values for attributes that usually have a value of true or false and for choice lists or single-select drop-down lists:

#### **(Any)**

Such queries return results for any setting of the attribute even if no value is assigned at all.

This is the default search value for attributes of these data types.

#### **(Unassigned)**

Such queries return results only if the attribute does not have a value assigned.

**Hint: (Any)** and **(Unassigned)** are not available for attributes of the data type Combination box (single-select) although, in general, they look and behave similar to attributes of the data type Drop-down list.

## Person history updates

Changes to the monitored attributes that result from LDAP synchronization are now also automatically captured and trigger an update to the person history.

## Sender of message previews


When you use **Send Preview** to send copies of messages in templates, interviews, or hold notices that you're currently working on to members of your team, you as the signed-in user are now the sender of such messages. Previously, the sender was the user configured as sender in the email settings for custodian notifications.

## Type or template change when duplicating data requests

When you duplicate a data request, you can now change the type or select a different template for the new data request.

## What's changed in V2.0.3.5

### Changed behavior for the task view

If a user clicks **Complete** for a task, the task view is now immediately closed. On the **Tasks** page, a message is displayed indicating that the completion request for the task was accepted and this icon  is shown next to the task. If a user opens a task currently being completed, an according information message is displayed. After the request is complete, the task is removed from the task list when the user refreshes view.

## Default import mapping for target entity persondistinct

The value of the updateaction attribute is now UPDATE\_PERSON to allow for person-specific updates. If you created a custom import mapping for the target entity persondistinct, update the mapping accordingly.

## What's changed in V2.0.3.4

### Changed option name

The option to send copies of messages in templates or draft versions of hold notices and interviews has been renamed from **Send test message** to **Send Preview**.

## Incremental refresh of entries

To improve the performance when the reporting database is refreshed, the table entries for specific entities are now refreshed incrementally instead of fully. [Learn more...](#)

## Lists of completed tasks or work packages

When you filter on completed tasks or completed work packages, the list no longer contains canceled items but only those that were actually completed. Canceled items are listed separately.

## Naming of duplicated data requests

When you duplicate a data request, each copy can now be created with a unique system-generated name. However, you can still choose your own data request names. [Learn more...](#)

## Notice status indicator

After introducing the possibility to change and republish published hold notices, an initial notice can be either an actual initial notice or a changed initial notice. Because the notice status covers both types, a status labeled - **Initial** is not entirely correct. To avoid confusion, the - **Initial** label has therefore been removed from the statuses for either type of initial notice.

## Tasks page

The **Tasks** page was redesigned to provide more information.

## What's changed in V2.0.3.3

### Donut charts for hold notices and interviews

The donut charts for hold notices and interviews now show a unique count of the custodians. For example, if a custodian is included in three hold notices, the count in the hold notices donut chart is increased by one instead of three. The count for pending custodians now no longer includes suspended custodians.

### Donut charts for data requests

The donut chart for data requests now shows a unique count of the custodians. For example, if a custodian is included in three data requests or in three different data request types, the count in the data request donut chart is increased by one instead of three. When you hover over the individual segments of the donut chart, you see the number of custodians in a specific data request type.

## What's changed in V2.0.3.2

### Additional information in Matter Custodian Report

The Matter Custodian Report (and the respective reporting view) now also includes information about the data requests related to a custodian. Therefore, to create and view the Matter Custodian Report, you now must also have the **Data requests: View** privilege. [Learn more...](#)

### Changed behavior for reminder notices and recurring interviews

The reminder cycle for hold notices requiring confirmation now starts only after the custodian confirms the initial notice. The cycle for recurring interviews starts only after the custodian responds to the initial interview. [Learn more...](#)

Due to this change, the follow-up schedule for existing initial hold notices or interviews is automatically changed during the upgrade to StoredIQ for Legal V2.0.3.2 to avoid custodians not receiving reminder notices or recurring interviews in some specific cases. The updated schedule is to repeat sending follow-up messages until the custodian confirmed the initial notice or responded to the initial interview. [Learn more...](#)

For new hold notices and interviews, follow-up messages are now sent by default until the initial notice is confirmed or the custodian responded to the initial interview.

## Changed keystore settings

Some of the internal keystore settings changed. Therefore, you cannot restore data in StoredIQ for Legal Version 2.0.3.2 from backup files created with previous product versions.

## Changed memory requirements

The virtual machine now requires a memory of 14 GB. [Learn more...](#)

## Changed privilege names

Because the **External servers: Manage** privilege is needed for more tasks than defining the connection to external servers, it has been renamed to **System: Manage**.

Matter security has been improved by redefining and streamlining the rights of several privileges. Therefore, the **Matters: Secure** privilege has been renamed to **Sensitive matters: Manage**. This privilege and the **Matters: Close** privilege are no longer assigned to any role by default.

The **Import: Secured matters** privilege has been renamed to **Import: Matters** because the import of any matter requires this privilege.

[Learn more...](#)

## Courtesy copy notifications

Recipients of courtesy copies can now find these notifications in a separate section of the **Custodian Portal** page.

## Date ranges in data requests

Date ranges are now shown independent of the time zone of the browser that you use to work with StoredIQ for Legal. [Learn more...](#)

## Default user preferences

The notification settings have changed in that task assignees, task assigners, and task subscribers are now, by default, informed about specific task changes. [Learn more...](#)

## Host name in import request

The host name is saved in the `clientid.credentials` file when you register a client with the REST API. When you create an import mapping or import data, you no longer need to specify the host name.

[Learn more...](#)

## Indefinite reminders

You can now configure reminder notices and recurring interviews to be sent indefinitely.

## Matter security

Access to a matter is now restricted to either the assigned security group and the list of additional assignees, or for sensitive matters, the assigned core matter team and the list of additional assignees.

The creator of a matter no longer has special privileges regarding matters. [Learn more...](#)

## Network configuration upgrade

StoredIQ for Legal deployment now uses the NetworkManager text user interface tool (nmtui) instead of siq-python for network configuration. [Learn more...](#)

## Readd released custodians

Custodians that were released from a hold notice can now be added again.

## Updated import command line interface (CLI)

With the import CLI, you can now clean up history-related data and override global information when adding custodians to a data request. In addition, the mappings section of the import mappings has changed.

## What's changed in V2.0.3.1

### Default import mappings

The default import mappings changed for specific target entities. [!\[\]\(d84e7ea36f695d92cb39ec32c307ac93\_img.jpg\) Learn more...](#)

### Updating report definitions

To update a report definition, you no longer need to delete the existing one before you import an updated file. Instead, you can directly replace it after you suspended it. Also, existing report data is now preserved. [!\[\]\(9dfdaff1d86ba3c1f8353b4d1b61b8c5\_img.jpg\) Learn more...](#)

---

# Overview

StoredIQ for Legal provides an end-to-end platform that streamlines the e-discovery process for legal stakeholders. It helps you gain efficiency and transparency in custodian identification, legal hold notification, and data collection and preservation.

StoredIQ for Legal provides the following key features to help you manage your legal processes and improve the communication and workflow between your legal and IT teams:

## **Matter management**

The matter is the key business item in StoredIQ for Legal. It is the container for all activities that pertain to a legal case. Within a matter, you can manage hold notices, interviews, data identification, and data collection and preservation and oversee the activities.

## **People management**

You can import people from your company's directory server or from CSV files, manage their profiles, assign them specific roles, and create groups.

## **Hold notice management**

You can create, send, and manage hold notices, including follow-up messages and reminder notices. You can also create and maintain a catalog of hold notice templates for reuse.

## **Interview management**

You can create, send, and manage interview questionnaires, and track the responses from the interviewees. You can also create and maintain a catalog of interview questionnaire templates for reuse.

## **Data request management**

You can create and manage requests to identify, collect, and export data that is relevant to a legal matter. You can also create and manage requests for releasing data after the legal obligation to preserve the documents is removed.



---

# Planning

Before you deploy and work with IBM StoredIQ for Legal, complete the planning activities to ensure that all requirements are met and prerequisite tasks are complete.

## Planning for deploying StoredIQ for Legal

---

StoredIQ for Legal is an application that you can deploy and configure as a virtual appliance in a VMWare virtual host environment or in form of containers in a Red Hat OpenShift environment.

StoredIQ for Legal consists of a web client and a server. It is delivered either as an Open Virtual Appliance (OVA) for installation on a VMware hypervisor (referred to as StoredIQ for Legal (VM) where differentiation is necessary) or in the form of containers (referred to as StoredIQ for Legal (Container) where necessary) for installation on OpenShift.

Before you deploy StoredIQ for Legal, verify that you meet these prerequisites:

### StoredIQ for Legal (VM)

- At least one physical server with sufficient processor, RAM, and hard disk configuration for the planned management project.
- VMWare ESX or VMWare ESXi on CD/DVD or USB drive.
- IP addresses, cables, and physical switch ports for the VMWare ESX or VMWare ESXi interface.
- A virtual machine (VM) with at least 8 vCPUs, a memory of 24 GB (recommended 32 GB), and a storage of 250 GB.
- A network connection. The ports 9443, 9043, 443, and 22 are needed for a connection between the administrative workstation and the VM. The connection to directory server, email server, and IBM StoredIQ server will be configured in StoredIQ for Legal. You can use the ports that fit your environment requirements.

### StoredIQ for Legal (Container)

- CPU: 8
- Memory: 24 GB (32 GB recommended)
- Data storage:
  - Application data: 150 GB
  - Application server: 10 GB
  - Directory server (LDAP) data: 50 GB
  - Reporting database: 40 GB

## System requirements

Review the detailed system requirements for IBM StoredIQ for Legal.

Find the most up-to-date requirements for IBM StoredIQ for Legal in the IBM Software Product Compatibility Reports (SPCR) tool at: [Software Product Compatibility Reports: StoredIQ for Legal 2.0.3](#)

If you plan to use StoredIQ for Legal Identification and Collection to create and manage data boxes and data requests that are to be fulfilled by IBM StoredIQ, also check the system requirements for IBM StoredIQ at: [Software Product Compatibility Reports: StoredIQ 7.6](#)

The minimum required version of IBM StoredIQ is version 7.6.0.9. To make use of the feature introduced with IBM StoredIQ for Legal 2.0.3.9 that enables links to IBM StoredIQ Insights, IBM StoredIQ 7.6.0.17 or later must be installed and must be set up with an Elasticsearch cluster.

## Generate customized reports with the SPCR tool

Go to the page at [Software Product Compatibility Reports](#) to create a high-level report for supported operating systems, related software, hypervisors, and supported translations for any product. You can also create an in-depth report to get detailed system requirements, hardware requirements, and end of service information for each product. You can search for a product in all of the report types and reports are generated based on your query values.

The following report types are the most commonly generated reports from software product compatibility reports:

### Detailed system requirements

When you select your product version for the detailed system requirements report, you can set a report filter for **Operating system platforms**, **Product components**, and **Capabilities**, including prerequisites and support software. After you view the report, you can save it as a URL to generate anytime or download it as a PDF.

### Hardware requirements

When you select your product version for the hardware requirements report, you can set a report filter by the **Operating system families** option. Set the operating system filter by selecting some or all of the operating systems that are supported by your product. After you view the report, you can save it as a URL to generate anytime or download it as a PDF.

### End of service

The end of service report shows the service window of the products that you specify over an eight-year span. For example, you can find out when your product is scheduled to go out of service.

## Licensing in StoredIQ for Legal

StoredIQ for Legal requires licenses for specific features. Using the IBM License Metric Tool, license consumption reports that count license usage can be generated for the programs licensed by User Value Unit (UVU) and by Connection.

### Licensed programs

Specific features in StoredIQ for Legal require the following licenses:

#### StoredIQ for Legal Notification Authorized

For creating and managing hold notices and interviews. StoredIQ for Legal counts the daily user license usage by authorized users. An authorized user is a unique person who can sign in to the program, has an assigned role, and might have at least one additional privilege in the system. Users with any of the following privileges count toward this license: **Notices: View**, **Notices: Manage**, **Interviews: View**, **Interviews: Manage**.

#### StoredIQ for Legal Identification and Collection

For creating and managing data boxes and data requests that are to be fulfilled by IBM StoredIQ. License consumption reports cannot be generated for this program because it is licensed by Resource Value Units (RVU) based on Terabytes managed by the program. This is the same number of Terabytes that is managed by IBM StoredIQ, and needs to be determined using IBM StoredIQ administration capabilities.

#### StoredIQ for Legal eDiscovery for IT

For creating and managing data requests. StoredIQ for Legal counts the daily user license usage by authorized users. Users with any of the following privileges count toward this license: View data requests, Manage data requests, View work packages, and Manage work packages.

#### StoredIQ for Legal Policy Syndication Framework

For fulfillment automation. StoredIQ for Legal counts the daily license usage by registered fulfillment connector.

#### StoredIQ for Legal Policy Syndication SDK

For fulfillment automation. This program is licensed by authorized user. License consumption reports are not generated.

For any licenses that you do not have, your system administrator can hide the corresponding features at **Admin > System Settings**. A user with more than one privilege of one type is counted only once. A user with privileges of both types is counted for each license.

### Integration with IBM License Metric Tool

Versions of IBM License Metric Tool (ILMT) that support IBM Software License Metric Tag (SLMT) can generate license consumption reports. An ILMT agent can scan in configurable intervals the file system for .slmtag files, collect information, and send it to the corresponding ILMT server. ILMT reports the number of Authorized Users for each of the programs (StoredIQ for Legal Notification Authorized and StoredIQ for Legal Identification and Collection) that are listed as Metric Subtypes in the report. These numbers are to be used as input for the UVU License Conversion Table specified in the license information that comes with StoredIQ for Legal.

By default, the license count for each supported StoredIQ for Legal program is written to one common SLMT file at `/home/data_exchange/slmtags/PersistentID.slmtag`, as in `/home/data_exchange/slmtags/ca786155e09343958afe4c0b3324b805.slmtag`.

If this directory is not writable, then the files are created in the home directory of user "was" in a subdirectory named `slmtags`. Corresponding information is also added to the `liger.log` file.

## Planning for importing people into StoredIQ for Legal

---

The people to use StoredIQ for Legal must be imported into the catalog of StoredIQ for Legal. You have several options to import them.

If the people in your company are defined on an LDAP-compliant directory server, you can import them directly from this server. For this purpose, you must configure a connection between StoredIQ for Legal and the directory server. As part of the configuration, you can define which person attributes are imported. In addition, you can specify how often StoredIQ for Legal and the directory server are synchronized to keep the list of people and their profiles in the catalog of StoredIQ for Legal up-to-date. To configure the connection, you must be a system administrator with the **System: Manage** privilege. For more information, see [“Configuring the connection to the directory server”](#) on page 62.

Alternatively, you can import the people in your company from a CSV file by using the import API of StoredIQ for Legal. Like with a directory server, you can import new people into the catalog of StoredIQ for Legal and update the profile of existing people regularly.

For more information about the import API, see [“Importing data by using the import API”](#) on page 168. For this import option, you must have the **Content settings: Manage** or **System: Manage** privilege and the **Import: General** privilege.

Both import options are designed for importing large numbers of people where the initial import is typically followed by scheduled, incremental updates to keep the catalog of StoredIQ for Legal up-to-date.

The two import options might not meet all of your requirements. For example, you might have matters that pertain to custodians who are not regular employees of your company and might not even be able to sign in to StoredIQ for Legal. If scheduled imports or updates are not suitable, you can use the ad hoc import of StoredIQ for Legal, which also uses the import API. You can import people from within the catalog. You can also import them as part of adding custodians to a hold notice, an interview, or a data request.

For more information, see [“Importing data by using the import API”](#) on page 168. For this import option, you must have the **People: Manage** privilege.

Regardless of the import option, all new people are always added to the catalog, where you can edit their profiles and create groups. All new people are available for use by all matters. The people are identified as follows:

- By their signin ID or the person ID. For people that are imported by using the ad hoc import, the email address is used. However, you can change the import mapping for all import options.

- By the person attribute that is specified in the system settings. Any predefined or custom person attribute that is defined as a string can be used as identifier. For more information, see [“Configuring system settings”](#) on page 58 and [“Customizing attributes”](#) on page 68.

**Important:** If you do not use a directory server, single sign-on (SSO) must be enabled. If you use such a server, SSO is optional.

Before you start the import, check which person attributes are already defined in StoredIQ for Legal. An initial set is provided, which you can complement with custom attributes. Ensure that the defined attributes match the attributes that you want to import and that the values fit. Although you can manually change a person's profile and add missing values at any time after the import, you might prefer to import as many attribute values as possible.

**Restriction:**

- You cannot import values for the predefined Relationship attribute, which defines the relationship between the entries in the catalog.
- When you import people from a directory server, you cannot retrieve values for the Manager attribute and the Jurisdiction attribute.

For more information about attributes, see [“Customizing attributes”](#) on page 68.

All new entries in the catalog are marked as primary entries. However, if several entries belong to one physical person, you can define their relationship by determining which entry remains the primary entry and which entries are the aliases. For more information, see [“Editing profiles, creating relationships, and viewing a person's change records”](#) on page 74.

## Planning for people and users

---

Access in StoredIQ for Legal is controlled through the roles that you assign to a person and the privileges that you associate with a role. A *role* is a function that a person has in an organization. By assigning a role, a person becomes a *user* in StoredIQ for Legal. The *privileges* determine which tasks a user can complete.

When you import people into StoredIQ for Legal, they receive limited access rights. To get more rights, they must become users.

All the people that you import into StoredIQ for Legal are added to the catalog of StoredIQ for Legal. You can edit the profiles of the people. However, you cannot delete them from the catalog again.

As part of the profile, you can specify whether it is possible for a person to sign in to StoredIQ for Legal. All people in the catalog who can sign in have the minimum access that is required to respond to hold notices and interviews. Such people can be used as custodians, regardless of whether they are regular employees, nonemployees, or people with a temporary contract.

You can give the people who can sign in more rights by assigning them roles. The privileges that are associated with a role determine which tasks a user can complete. For more information about roles and privileges, see [“Managing and assigning roles and privileges”](#) on page 76. Users are listed in the catalog and on the **Role Assignments** page. If you decide to remove the roles again, this user is changed back to a person with the minimum access rights and is available in the catalog only.

For nonproduction environments, you can create test users. Their sign-in ID is used as password, which cannot be changed. Test users are added to both the catalog and to the list of users on the **Role Assignments** page. They can be assigned roles.

If you decide to remove the roles again, the test user is changed to a person with the minimum access rights and is available in the catalog only. Test users cannot be deleted from StoredIQ for Legal. For more information, see [“Creating test users”](#) on page 75.

## Planning for secure matters

---

The *matter* is the key business item in StoredIQ for Legal. It is the container for all activities that pertain to a legal case. Therefore, you must strictly control the access to a matter and its contents.

By default, all users with the appropriate role and privileges can access all matters and their contents. To give users access to specific matters only, you can make matters sensitive or use security groups. A *sensitive matter* differs from a *regular matter* in that the access to such a matter is strictly limited to a specific group of users: the *core matter team* and designated *additional assignees*. No other user can access a sensitive matter. The use of security groups in StoredIQ for Legal to control access to matters must be explicitly enabled by changing the respective system setting; by default, the use of security groups is disabled. Matters can also be protected through key-based access control.

The core matter team typically consists of users with the following roles:

- The attorney
- The paralegal
- The data expert if the matter will contain data boxes

Additional assignees are other users that you assign to a matter specifically, so that they can access that matter without a specific function or role. A regular matter, however, can have additional assignees only if the use of security groups is enabled.

### Protecting regular matters by using security groups

You must explicitly enable the use of security groups for controlling access to regular matters by changing the respective system setting.

**Important:** Enabling the use of security groups is permanent; you cannot disable it later.

A *security group* is a group of users that is defined for restricting the access to a regular matter to the users who are members of this group. Access to a sensitive matter cannot be controlled through a security group; it is always limited to the core matter team and the designated additional assignees.

After you enable the use of security groups, you must assign a security group to each new regular matter. StoredIQ for Legal supplies a default security group that contains all users that are defined in the system when you enable the use of security groups. This default security group is automatically assigned to all existing regular matters. Consequently, all users with the appropriate privileges have access to all matters that have the default security group assigned. To restrict the access, set up additional security groups as needed, where each group can have different members. Then, assign the appropriate security groups to your matters.

A regular matter can be associated with only one security group. However, the same security group can be assigned to more than one regular matter. After the use of security groups is enabled, you assign the security group during matter creation. When you create a regular matter using the GUI, this security group must also include the attorney, the paralegal, and, if applicable, the data expert that you want to assign to a matter. In addition, you can extend the access to the regular matter to users that are not members of the security group by selecting additional assignees when you create or change the regular matter.

When you change the regular matter, you can select a different security group. The members of a security group can be changed even after the group is assigned. When you add or remove members, these users gain or lose access to the regular matter, except for the core matter team and the additional assignees. The assigned core matter team and the additional assignees remain the same unless you change the assignments.

Also, the user who creates a regular or a sensitive matter does not automatically have access to that matter but must be a member of the security group in the case of a regular matter, be a member of the core matter team, or be selected as an additional assignee to have access to the matter.

When matters are imported by using the import API or created by a matter management system (MMS), the assigned core matter team does not necessarily have to be part of the security group assigned to the matter. For more information, see [“Importing data by using the import API” on page 168](#).

At any time, you can rename a security group. If a security group is no longer assigned to any matter, you can also delete it. If you attempt to delete a security group that is still assigned to a matter, you will get a corresponding error message, and the security group will not be deleted.

### Protecting matters by making them sensitive

If a security group does not provide enough security, you can create *sensitive matters* regardless of whether the use of security groups is enabled. You must have the **Sensitive matters: Manage** privilege to do so. When you create the sensitive matter, you select the users to have access in addition to the core matter team (*additional assignees*). The core matter team and the list of additional assignees can be changed again after the sensitive matter is created.

Even if the use of security groups is enabled, you cannot associate a sensitive matter with a security group. A regular matter can be changed to a sensitive matter at any time, and vice versa. To make a matter sensitive, you must have the **Sensitive matters: Manage** privilege. However, if you change an existing regular matter with a security group to a sensitive matter, all members of that security group immediately lose access to the matter. If you turn a sensitive matter into a regular matter, you must assign a security group, provided the use of security groups is enabled.

### Protecting matters through key-based access control

You can restrict access to matters based on specific access keys, for example, based on the location information.

You must explicitly enable key-based access control by changing the respective system setting. If enabled, key-based access control is independent of the use of security groups and can be applied to regular and sensitive matters.

In addition to enabling this type of access control, you must select a custom matter attribute for holding the key value or values that control the access and a lookup key for checking incoming sign-in requests. The respective header field and value must be provided by a system external to StoredIQ for Legal such as an SSO system. The value must be available in the HTTP request headers of all incoming requests. Otherwise, the user has access to only those matters that have no access key set. If a value is present, matters are filtered based on that value. The user then has access to exactly those matters where the provided value matches the key (or one of the keys) set for the matter. And consequently, users have access only to the data requests, interviews, or hold notices and their associated tasks contained in such matters. The matter list in general and when viewing a person's hold obligations and involvement in matters is also filtered based on the key value.

Sticking with the location information example, let's assume the access key is defined as a multi-select list of two-letter ISO country codes, such as CH, DE, FR, UK, US, and the lookup key is `Location`. For matter ABC, the access keys CH and DE are set. For matter DEF, no access key is set. Any user whose sign-in information contains either `Location: CH` or `Location: DE` is granted access to matter ABC. Users with any other location setting or no location setting at all in the sign-in information cannot see matter ABC. In contrast, all users regardless of the location information in their sign-in information can see matter DEF.

Usually, the key granting access to a matter will stem from and be maintained in the matter management system. However, a user with the **Sensitive matters: Manage** privilege can manually set or change a matter's access key. Setting or updating the access key for an existing matter might change who has access to the matter. Persons who previously had access but whose sign-in information does not provide the required key will no longer be able to see the matter.

Even if a matter has no access key set, access to reports can still be limited. Access restrictions for a report are defined in the report definition.

Key-based access control does not restrict the scope of audit queries. Irrespective of any access restrictions to matters, any audit query returns all audit events within the request scope.

## Matter security overview

The following tables give an overview of the options that you have to protect a matter. [Table 1](#) on page 25 shows which user groups have access to a matter if the use of security groups is disabled. [Table 2](#) on page 25 shows which user groups have access to a matter if the use of security groups is enabled. The values Yes and No indicate access or no access.

Access can be restricted further if key-based access control is enabled.

Matter Type	All Users	Core Matter Team	Additional Assignees
Regular without access key	Yes	Yes	Not available
Regular with access key	Only users with the key	Only users with the key	Not available
Sensitive without access key	No	Yes	Yes
Sensitive with access key	No	Only users with the key	Only users with the key

Matter Type	All Users	Users in Security Group	Core Matter Team	Additional Assignees
Regular without access key	No	Yes	Yes	Yes
Regular with access key	No	Only users with the key	Only users with the key	Only users with the key
Sensitive without access key	No	Not available	Yes	Yes
Sensitive with access key	No	Not available	Only users with the key	Only users with the key

### Related tasks

[Configuring system settings](#)

You can configure various StoredIQ for Legal system settings.

[Managing security groups](#)

[Creating matters](#)

Create a matter to contain all activities that pertain to a legal case.

## Planning for custodian notifications

To monitor compliance, you can request the initial hold notice to be confirmed and then send out follow-up messages and reminder notices on a regular schedule. Likewise, you can send follow-up messages to interviews and schedule recurring ones.

For this purpose, define processing rules for hold notices and interviews. Default processing rules are defined in the hold notice or interview template. However, unless you lock the rules in the template, any of these settings can be overridden when you create a hold notice or interview.

### Silent custodians

You might want to put custodians on an active hold notice without these custodians being aware of the active hold. Such a hold is called a *silent hold* and the custodians are so-called *silent custodians*. A silent

hold is usually put in place to maintain confidentiality during internal investigations. Thus, investigations can be more thorough and proper evidence can be collected without exposing a potential internal conflict. At any time during the lifecycle of a hold notice, a silent custodian can become an active custodian and will then receive the respective notifications. Vice versa, an active custodian can be made a silent custodian at any time. In this case, notifications are stopped. Also, a silent custodian in one hold notice can be an active custodian or a cc recipient in a different hold notice.

You can publish hold notices that do not include any active custodians. If such a notice includes cc recipients, the cc recipients are notified. Otherwise, no notifications are sent at all.

## Hold notices

You can configure follow-up messages to be sent for hold notices and reminders that require confirmation. Follow-up messages can be sent repeatedly: one to four times, or until the custodian confirms the hold notice or the reminder. The schedule of the follow-up messages to a hold notice is based on the send date of the initial notice.

For long-lasting matters that require custodians to preserve data for prolonged periods of time, you might want to automatically remind them of the ongoing obligation to comply with the hold and even require them to reconfirm their compliance. You can configure notice-specific (*individual*) reminders or global reminders. If the initial hold notice requires confirmation, reminder notices are sent only to those custodians who already confirmed the initial notice, at the specified frequency. Custodians that are added to a hold notice that already entered the reminder cycle will still receive an initial notice, but might not receive reminders depending on how the reminder cycle is configured. Follow-up messages to a reminder are sent to custodians who did not respond, according to the configured schedule. The schedule is based on when the reminder was sent.

Instead of configuring individual reminders for each hold notice, you can apply the global hold reminder. The global hold reminder summarizes a custodian's obligations across holds in a single reminder notice. For details, see [“Planning for the global hold reminder”](#) on page 27.

When you suspend a hold notice for a custodian, this custodian no longer receives any notifications. Resuming a hold notice for a custodian also resumes the notifications. However, follow-up messages are sent according to the schedule defined for the hold notice, based on when the initial notice was sent. Therefore, the follow-up cycle might already be over when the hold notice is resumed for a specific custodian, so that this custodian would not receive any follow-up messages. To avoid this, configure follow-up messages to be sent until the custodian confirms the hold notice or reminder.

Special considerations apply when a custodian requests to be contacted by clicking the **Contact me** link in the notification. In this case, the follow-up cycle is interrupted or does not even start, and the paralegal must make sure that the custodian confirms the hold notice.

## Interviews

You can configure follow-up messages for interviews. The schedule of the follow-up messages to the initial interview is based on the send date of the interview. Follow-up messages can be sent repeatedly: one to four times, or until the custodian responded to the interview.

To identify whether previously collected information is still valid, you can resend interviews periodically by configuring recurring interviews. Recurring interviews are sent only to those custodians who responded to the initial interview. Follow-up messages to a recurring interview are sent to custodians who did not respond, according to the configured schedule. The schedule is based on the send date of the interview.

When you suspend an interview for a custodian, this custodian no longer receives any notifications. Resuming an interview for a custodian also resumes the notifications. However, follow-up messages are sent according to the schedule defined for the interview, based on the send date of the initial interview. Therefore, the follow-up cycle might already be over when the interview is resumed for a specific custodian, so that this custodian would not receive any follow-up messages. To avoid this, configure follow-up messages to be sent until the custodian responds to the interview.



## Escalation notices

To alert an unresponsive custodian's manager, you can have StoredIQ for Legal send escalation notices. You define which follow-up triggers the first escalation notice. Subsequently, escalation notices are sent on the same schedule as further follow-up messages.

As a prerequisite, the custodian's profile in the StoredIQ for Legal catalog must contain the appropriate manager information.

If the manager is a silent custodian on the same hold notice, no escalation notice is sent.

## Planning for the global hold reminder

---

With a global hold reminder, you consolidate a custodian's reminders. The custodians get a single reminder notice for all of their hold notices that the global hold reminder is applied to, according to the schedule that is defined in the global hold reminder.

You can create and activate one global hold reminder. For each hold notice template or hold notice that you want to set up a reminder cycle for, you can decide whether to use the global hold reminder or configure an individual reminder. To create, activate, view, or update a global hold reminder, you need the **Global hold reminder: Manage** privilege.

A global hold reminder provides the same functions as an individual reminder. You can specify when the first reminder notice is sent, at which intervals a reminder notice is sent, whether it requires confirmation, how often follow-up messages are sent, if any, and which follow-up message prompts an escalation. The main difference between an individual reminder and a global hold reminder is the start of the reminder cycles. If an individual reminder is used, the start of the reminder cycle depends on the send date of the initial notice. For more information about individual reminders, see [“Planning for custodian notifications” on page 25](#). If the global hold reminder is used, a reminder notice is always sent out according to the schedule that is defined in the global hold reminder. At the reminder date, it is sent at any time after 12 noon according to the time zone of the browser that you use to set the reminder schedule and taking into account standard time and Daylight Saving Time. The actual send time depends on the schedule for the custodian notifications, which you define when you configure the connection to the email server.

Assume, for example, that you have the following setup:

- The global hold reminder is scheduled to be sent out every 3 months, starting on 1 July 2017. The user who schedules the global hold reminder works in Berlin, Germany, which belongs to the Central European Time zone. This means that, at the reminder dates, the reminder notices are sent at any time after 12 noon Central European Time, depending on the schedule for the custodian notifications.
- Custodian notifications are scheduled to be sent out every hour.
- The hold notices A, B, C, D, and E use the global hold reminder. The initial notices of hold notices A, B, and C require confirmation.
- The initial notices were sent to custodian1 and custodian2 on 15 June 2017. custodian1 works in the time zone of New York City, USA, and custodian2 works in time zone of Tokyo, Japan.
- custodian1 confirms the initial notice of hold notice A on 20 June 2017, of hold notice B on 1 July 2017, and of hold notice C on 14 July 2017, always around 12 noon Eastern Daylight Time (EDT). custodian2 confirms the initial notice of hold notices A, B, and C on 30 September 2017, around 12 noon Japan Standard Time (JST).

On 1 July 2017, at 12 noon Central European Summer Time (CEST), which is UTC+02:00, a reminder notice is sent to custodian1. The reminder notice lists the hold notices A, D, and E. Hold notice B is not listed because its initial notice was confirmed 6 hours after the send time. custodian1 receives the reminder notice around 6 AM EDT, which is UTC-04:00. A reminder notice is also sent to custodian2, which lists the hold notices D and E. custodian2 receives the reminder notice around 7 PM JST, which is UTC+09:00.

On 1 October 2017, both custodians receive reminder notices, which list all of their hold notices, at the respective times.

If you decide to send out custodian notifications only once a day at 12 midnight UTC, custodian1 receives the reminder notice on 1 July 2017 at 8 PM EDT (UTC-04:00) and custodian2 receives the reminder notice on 2 July 2017 at 9 AM JST (UTC+09:00). The reminder notice that is sent to custodian1 includes hold notice B because its initial notice was confirmed 8 hours before the send time.

The following tables summarize the described scenario. They also include the schedule for the reminder that is sent out on 1 January 2018, where standard time applies in Germany and in the United States. [Table 3 on page 28](#) shows the schedule if custodian notifications are sent out every hour. [Table 4 on page 29](#) shows the schedule if custodian notifications are sent out once a day, at 12 midnight UTC.

<b>Timeline</b>	<b>Reminder schedule - set in Germany</b>	<b>custodian1 - New York City, USA</b>	<b>custodian2 - Tokyo, Japan</b>
Before 15 June 2017	Global hold reminder created, with the 1st reminder scheduled for 1 July 2017		
15 June 2017		Receive initial notices of hold notices A, B, C, D, and E	
20 June 2017		12 noon EDT (UTC-04:00): confirms initial notice of hold notice A	
1 July 2017	12 noon CEST (UTC +02:00): 1st reminder sent	6 AM EDT (UTC-04:00): receives 1st reminder notice, which lists A, D, and E	7 PM JST (UTC+09:00): receives 1st reminder notice, which lists D and E
		12 noon EDT (UTC-04:00): confirms initial notice of hold notice B	
14 July 2017		12 noon EDT (UTC-04:00): confirms initial notice of hold notice C	
30 September 2017			12 noon JST (UTC +09:00): confirms initial notices of hold notices A, B, and C
1 October 2017	12 noon CEST (UTC +02:00): 2nd reminder sent	6 AM EDT (UTC-04:00): receives 2nd reminder notice, which lists all hold notices	7 PM JST (UTC+09:00): receives 2nd reminder notice, which lists all hold notices
1 January 2018	12 noon Central European Time (CET; UTC+01:00): 3rd reminder sent	6 AM Eastern Standard Time (EST; UTC-05:00): receives 3rd reminder notice, which lists all hold notices	8 PM JST (UTC+09:00): receives 3rd reminder notice, which lists all hold notices

*Table 4. Overview of setup and schedules if custodian notifications are sent out once a day at 12 midnight UTC*

<b>Timeline</b>	<b>Reminder schedule - set in Germany</b>	<b>custodian1 - New York City, USA</b>	<b>custodian2 - Tokyo, Japan</b>
Before 15 June 2017	Global hold reminder created, with the 1st reminder scheduled for 1 July 2017		
15 June 2017		Receive initial notices of hold notices A, B, C, D, and E	
20 June 2017		12 noon EDT (UTC-04:00): confirms initial notice of hold notice A	
1 July 2017	12 noon CEST (UTC +02:00): 1st reminder sent	12 noon EDT (UTC-04:00): confirms initial notice of hold notice B	
		8 PM EDT (UTC-04:00): receives 1st reminder notice, which lists hold notices A, B, D, and E	
2 July 2017			9 AM JST (UTC+09:00): receives 1st reminder notice, which lists hold notices D and E
14 July 2017		12 noon EDT (UTC-04:00): confirms initial notice of hold notice C	
30 September 2017			12 noon JST (UTC +09:00): confirms initial notices of hold notices A, B, and C
1 October 2017	12 noon CEST (UTC +02:00): 2nd reminder sent	8 PM EDT (UTC-04:00): receives 2nd reminder notice, which lists all hold notices	
2 October 2017			9 AM JST (UTC+09:00): receives 2nd reminder notice, which lists all hold notices
1 January 2018	12 noon CET (UTC +01:00): 3rd reminder sent	8 PM EST (UTC-05:00): receives 3rd reminder notice, which lists all hold notices	

Table 4. Overview of setup and schedules if custodian notifications are sent out once a day at 12 midnight UTC (continued)

Timeline	Reminder schedule - set in Germany	custodian1 - New York City, USA	custodian2 - Tokyo, Japan
2 January 2018			8 AM JST (UTC+09:00): receives 3rd reminder notice, which lists all hold notices

The global hold reminder must be explicitly activated to make it available for use in a hold notice template or hold notice. If its contents must be approved, you can associate the activation with an approval workflow. The global hold reminder is then automatically activated when it is approved. The user to approve the global hold reminder must also have the **Global hold reminder: Manage** privilege.

The activation date does not affect the reminder cycle, which starts as defined in the global hold reminder. However, if the date of the first activation is after the date of the first reminder, the first reminder notice is sent at the activation date. Follow-up messages are based on the new send date. The schedule for the future reminder notices and their follow-up messages remains unchanged.

When you update a global hold reminder after its activation, you edit a copy of the global hold reminder. Your changes become effective only after they are activated.

It might be difficult to set up a schedule that excludes all dates and periods where reminders or follow-up messages should not be sent out, such as during the holiday season. You can interrupt the reminder cycle at any time by disabling the global hold reminder. When you resume it, the reminder notice that was skipped due to the interruption is sent out immediately. Follow-up messages are based on the new send date. The schedule for the future reminder notices and their follow-up messages remains unchanged.

Assume, for example, that you interrupt the reminder cycle on 30 June 2017 and resume it on 15 July 2017. Then, the reminder notice that was scheduled for 1 July is sent on 15 July. On 15 July, custodian1 receives a reminder notice, which lists all hold notices because the reminder notice covers all hold notices where the initial notice is confirmed by 15 July. Any follow-up messages are scheduled based on 15 July. The next reminder notice is sent out on 1 October 2017, as scheduled originally.

After a reminder notice is sent out, the global hold reminder is automatically updated to show the date of the next reminder. If you realize that this date and all future reminder dates do not fit your needs, you can change the date of the next reminder. Then, the schedule for all future reminders and any follow-up messages is based on the new date. The follow-up messages of the previous reminder remain unaffected.

Like with individual reminders, the custodians get their global reminders by email and can access them from the custodian portal. If the reminders require confirmation, they confirm all hold notices that are listed in the reminder notice by clicking the **Confirm** button. If the custodians want to contact their paralegal, they must do so manually. The **Contact me** link is not available for global reminders.

Reminder notices always reflect the latest rules and contents of the global hold reminder and the status of the custodians. Assume, for example, that you update the contents of the global hold reminder and activate the changes on 20 September 2017. Also, assume that you suspend hold notice A for custodian2 on the same day. When custodian2 decides to open the reminder notice on 30 September to confirm the hold notices, the reminder notice shows the changed contents and lists only the hold notices that still must be confirmed, namely hold notices B and C.

When courtesy copy recipients receive a copy of a reminder notice, they see only the hold notices that they are included in.

## Planning for notice changes

---

A matter grows over time so that the originally published hold notice at some point does no longer cover all aspects. You can update and republish already published hold notices.

Changes that a paralegal might want or need to make to an already published hold notice can have a broad range from fixing a typographical error to adjusting the rules of what needs to be preserved. Not all of the changes need to be communicated explicitly to the custodians.

Whenever you apply changes to a published hold notice, a new version of the notice is created. The changes are tracked in the reporting database. To compile a summary of the changes to a notice, you can run the built-in Notice History Report. In addition, you can create your own custom reports based on the notice history reporting views. For more information on these views, see [“Hold notice views” on page 136](#).

The following information does not apply to silent custodians because they do not receive any notifications.

### **Changes of which active custodians can be notified**

When you apply any changes to the body of the initial notice, you can add further information about the changes to the notification if you select to notify the custodians of these changes. To do so, you can include a *change message*. This change message is prepended to the initial notice in the change notification. However, notifications sent to custodians who are added to the hold notice after the change will not include the change message. For changes to the body of the initial notice, you can also choose whether to notify all active custodians or to apply the changes without sending any notification. Courtesy copy recipients also are notified when you select to send notifications. Suspended and released custodians do not receive any notification.

Custodians who are added to the hold notice as active custodians after the change will receive the modified initial notice.

Custodians who were suspended before any notice changes will still see the modified content when responding to the initial notice.

### **Changes of which custodians are not notified**

When you apply any of the following changes, no immediate notification is sent but any future notifications will include the changes. Further follow-up and reminder messages are then based on the rules applied with the change.

#### **Changes to the rules applying to the initial notice**

You can change the settings for confirmation and follow-up and the settings for cc recipients. You can also select to include additional information about any changes when you republish a hold notice. However, this setting only takes effect for notices where you changed the content of the initial notice.

If you enable escalation with the change, a custodian's status changes to escalated only after the next follow-up. If you disable escalation with the change, a custodian's status changes from escalated to response pending.

#### **Changes to the rules applying to the reminder notice**

If the original notice did not include a reminder, you can change the reminder type to global or individual. For an individual reminder, provide the appropriate values.

If the reminder type originally was global, you can change it to none to stop sending reminder notices. Or, you can set the reminder type to individual providing the appropriate settings.

If the reminder type originally was individual, you can either change the reminder type, or update the reminder schedule and the settings for confirmation and follow-up. Additionally, you can change the setting for cc recipients.

If you enable escalation with the change, a custodian's status changes to escalated only after the next follow-up. If you disable escalation with the change, a custodian's status changes from escalated to response pending.

If the notice had already entered the reminder cycle and you remove the reminder with the change, a custodian's status is reset to the status of the initial notice.

#### **Changes to the message subject**

You can change the subject of the initial notice, the reminder notice, or any follow-up messages at any time.

#### **Changes to the notice details**

At any time, you can change the notice name and description.

#### **Changes to the notice information**

At any time, you can change the notice information.

#### **Related tasks**

##### Modifying published hold notices

You can modify and resend published hold notices to accommodate any new requirements.

## **Planning for workflows**

---

A data request requires at least two workflows. Workflows can also be used to change the way an action is completed.

For example, if matters are to be closed only after the attorneys give their approval, you can associate the 'close matter' action with an approval workflow. Then, the approval workflow is started each time that you request to close the matter. The matter is closed after the approval workflow is completed successfully.

#### **General information**

The workflows must exist. You cannot create workflows with StoredIQ for Legal. A workflow must be defined in an XML file. A workflow definition can have several versions.

If you want to use the workflow to change the way an action is completed, you must associate it with that action, which then starts the workflow. You can associate a workflow with several starting actions. However, each action can start only one workflow. Workflows that contain the sequence of tasks to be completed for a data request must not be associated with a starting action. Workflows that lock any of their associated entities must not be associated with a **Data request - cancel** starting action.

In the workflow, you must specify, for each task, the user or users who are allowed to complete this task. You have the following options:

- Specify an assignee. Then, this user is assigned the task and must complete it.
- Specify candidate users, where you list the users who can be assigned the task and are allowed to complete it (assignee candidates)
- A candidate group. The users who are allowed to complete the task must be members of this group.

All users that you specify in the workflow must exist in StoredIQ for Legal. For each candidate group, you must create a role in StoredIQ for Legal and assign this role to all users in the candidate group. It is best practice to create a role without any privileges. The role name must match the candidate group name. The roles must exist when the workflow is imported into StoredIQ for Legal.

For more information, see [“Managing and assigning roles and privileges” on page 76](#).

StoredIQ for Legal provides a set of workflow services that you can call from within your workflow, for example, to update custom attributes or add data sources.

#### **Additional information about workflows for data requests**

A data request requires the following workflows:

- A main workflow that covers the entire data request. It starts when a data request is submitted and ends when the data request is marked as complete.

Create a workflow definition that, as a minimum, allows for refining a data request, starting the workflow for the fulfillment of the data request, and completing the request. Include approval tasks as needed and any other tasks that your organization requires.

If you want to make the selection of data source categories optional in a data request, create a workflow definition that generates a list of data source categories. You decide whether the selection is optional or mandatory when you create the data request template.

The names of the data source categories in the workflow definition must match the names of the data source categories in StoredIQ for Legal. For more information, see [“Managing data sources” on page 105](#).

- A workflow for the fulfillment phase. It is started for each work package when the work package is submitted. Design this workflow as required by your organization.

### Related reference

#### Workflow services

StoredIQ for Legal provides a set of built-in functions that you can use in your workflow.

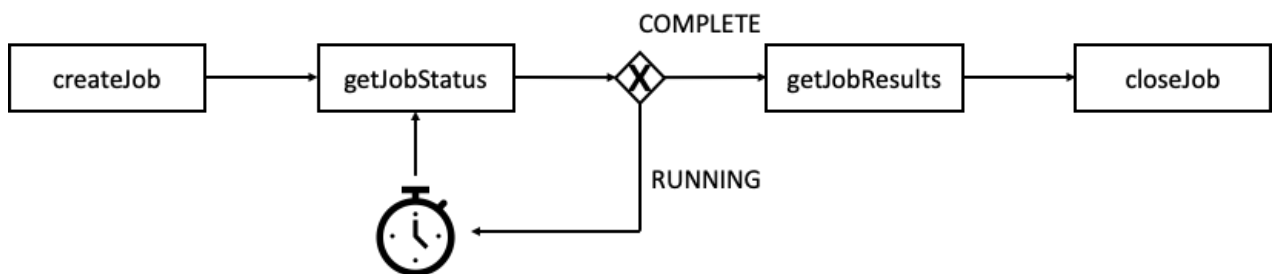
## Planning for automating fulfillment item creation

You can automate the process of creating fulfillment items for a data request by using a server discovery service in your workflow. Starting with version 2.0.3.10, StoredIQ for Legal allows for server discovery in a more organized way: Fulfillment items can be imported without adding data source mappings in the GUI or loading CSV files manually.

Automatic creation of fulfillment items works as follows:

1. StoredIQ for Legal passes the data request information to the server discovery service by using a **createJob** call.
2. The service start server discovery.
3. While waiting for the service to complete the request, StoredIQ for Legal periodically queries the job status. The service returns `status == COMPLETE` upon completion.
4. StoredIQ for Legal fetches the discovery results by using a **getJobResults** call and uses them to create fulfillment items.
5. StoredIQ for Legal triggers cleanup of the service discovery job by sending a **closeJob** request to the service.

This flow is illustrated in the following graphic:



To allow for server discovery, you must create a *server discovery connector* and register it with StoredIQ for Legal. Server discovery connectors are SOAP-based, URL-accessible web services. You can implement such a service in the general way of top-down web service development following the Web Services Description Language (WSDL) file that is provided with the product. You can find the WSDL file in the `ilg_sol_plugin` container at the following location:

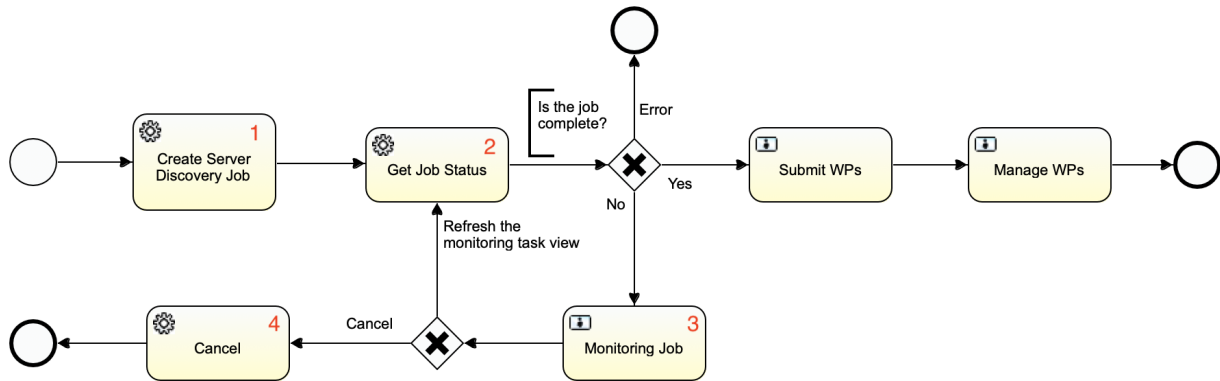
```
/home/was/WebSphere/AppServer/profiles/ilgnext/installedApps/  
websphereNode01Cell/ilg-sol-rest.ear/ilg-sol-rest.war/META-INF/wsd1/  
ServerDiscovery.wsd1
```

For more information about developing such a web service, see this IBM Developer article: [Developing the code and contract first approach web service with Axis2](#)

For more information about server discovery connectors, see the following topics:

- “[Registering and managing server discovery connectors](#)” on page 66
- “[Monitoring and managing server discovery jobs](#)” on page 67

After you register a server discover connector, you can implement workflows with the respective calls to the connector. The following example shows a typical workflow that uses a server discovery service.



1. Create Server Discovery Job: This service task calls `com.ibm.ilg.workflow.server.discovery.bpmn.DiscoverServers` to send a server discovery job request to the service. As a result, `com.ibm.ilg.workflow.server.discovery.bpmn.GetJobStatus` and `com.ibm.ilg.workflow.server.discovery.bpmn.CancelJob` become available for use.
2. Get Job Status: This service task calls `com.ibm.ilg.workflow.server.discovery.bpmn.GetJobStatus` to obtain any cached job values, which are available in form of the `serverDiscoveryJob` process variable. These cached values are refreshed periodically. The default refresh period is 5 minutes but you can set a different value in the server discovery connector configuration in the GUI.
3. Monitoring Job: This user task makes the job status available to the users defined in the task description.
4. Cancel: This service task calls `com.ibm.ilg.workflow.server.discovery.bpmn.CancelJob` to tell the service to stop the server discovery job.

For more information about the classes used in the workflow, see “[Server discovery Java class reference](#)” on page 250.

## Planning for fulfillment automation

Starting with version 2.0.3.7, StoredIQ for Legal allows for full automation of fulfillment activities. A fulfillment workflow can be configured, for example, to submit the fulfillment items within a work package to a ticketing system or to other fulfillment tools that support preserving or collecting items automatically.

You can combine automatic and manual fulfillment at work package level within a data request. You can also mix manual and automatic tasks within a single work package. For example, the workflow can send a work package to automation but when the fulfillment results are returned, the workflow routes the work package to a user task for manual postcorrection or quality assurance of the automated results.

To allow for fulfillment automation, you must configure and use the IBM StoredIQ for Legal Policy Syndication Framework on the StoredIQ for Legal system. In addition, you must create a *fulfillment connector* and register it with StoredIQ for Legal. Fulfillment connectors are SOAP-based, URL-accessible web services that you develop by using the IBM StoredIQ for Legal Policy Syndication SDK. This software development kit (SDK) is not part of the base StoredIQ for Legal product bundle. The Policy Syndication SDK includes an API and a Web Services Description Language (WSDL) file. For more information about



fulfillment connectors, see the documentation provided with the package. For more information about configuring and using the Policy Syndication Framework, see the following topics:

- [“Registering and managing fulfillment connectors” on page 65](#)
- [“Monitoring and managing fulfillment jobs” on page 110](#)

To be able to associate a connector with a data source, its external ID must be available as a value of the Automation Connector data source attribute.

After you register a fulfillment connector, you can use workflow service tasks to call the connector from within a workflow. You can include such tasks in a work package workflow (not the data request workflow) to automate all or selected subtypes of work packages. The logic for deciding which types of work packages are fulfilled manually and which automatically is also configured in the workflow. For more information, see the documentation provided with the Policy Syndication SDK.

### Related tasks

[Registering and managing fulfillment connectors](#)

You must set up and register a fulfillment connector before you can implement a work package fulfillment workflow with automatic fulfillment. For every fulfillment connector in use, you can monitor fulfillment jobs.

### Related reference

[Workflow services](#)

StoredIQ for Legal provides a set of built-in functions that you can use in your workflow.

## Planning for reports

StoredIQ for Legal supplies predefined reports. You can add custom reports.

The following reports are ready to run, in alphabetical order:

Report name	Cross-matter or matter-specific report	Description	Output format	Privileges required to create the report	Privileges required to view the report
Active Matter Summary Report	Cross-matter Is run on request.	Provides information about the active matters for which you are either the attorney or the paralegal. This information includes the matter details, and the names and states of the notices.	HTML PDF	Limited-access reports: View	
Custodian History Report	Matter-specific and entity-specific Is run on request.	Provides the history of changes to person details for all active custodians who are involved in a specific hold notice, interview, or data requests in the selected matter.	HTML PDF	Notices: View, Interviews: View, and Data requests: View	

Table 5. Reports (continued)

Report name	Cross-matter or matter-specific report	Description	Output format	Privileges required to create the report	Privileges required to view the report
Custodian Non-Confirmed Hold Notice - Matter Detail	Cross-matter Is run on request.	Provides insight about the responsiveness and compliance of custodians to hold notices.	HTML PDF	Limited-access reports: View	
Custodians -on-Hold Report	Cross-matter Is run automatically once a day at midnight Coordinated Universal Time (UTC). To change the schedule, the system settings for reports must be changed.	Provides an overview of the custodians across all matters who received hold notices and of the status of the hold notices.	CSV HTML PDF	n/a	Limited-access reports: View
Global Hold Reminder Report	Cross-matter Is run on request.	Provides information about the global hold reminder sent on a particular day.	HTML PDF	Limited-access reports: View	
Matter Audit Report	Matter-specific Is run on request.  It can be created only if low-level auditing is enabled as part of the system settings.	Lists all operations that were recorded for a matter and its contents.  <b>Important:</b> Low-level auditing is no longer necessary. Therefore, do not activate this report, if possible. For more information, see <a href="#">“Auditing” on page 220.</a>	CSV	Audit events: View	
Matter Custodian Report	Matter-specific Is run on request.	Lists all custodians who are involved in a matter's hold notices, interviews, and data requests that are not in draft state or closed.	CSV PDF HTML	Matters: View, Notices: View, Interviews: View, and Data requests: View	
Master List Report	Matter-specific Is run on request.	Lists all people who were involved in the notices, interviews, and data requests of a given matter.	HTML PDF	Notices: View, Interviews: View, and Data requests: View	

Table 5. Reports (continued)

Report name	Cross-matter or matter-specific report	Description	Output format	Privileges required to create the report	Privileges required to view the report
Migrated Notices Report	Cross-matter Is run on request.	Lists all hold notices that are migrated from IBM Atlas Policy Suite and that need to be manually verified.  This report can be generated only from the <b>Reports</b> page in the migration portal. It is not available as a regular report.	HTML	Notices: Manage	
Notice Confirmation Report	Matter-specific Is run on request.	Provides an overview of the confirmation status of a hold notice per custodian.	HTML PDF	Notices: View	
Notice History Report	Matter-specific Is run on request.	Provides information about the changes to a published hold notice.	HTML	Matters: View and Notices: View	
Notice Recipients List	Matter-specific	Provides information about the notices that were sent for a matter and includes details about the notice type and the notice recipients, and a summary of the confirmation status of each recipient.	HTML PDF	Notices: View	
Organization Structure Report	Cross-matter Is run on request.	Depicts your organization hierarchy.	HTML PDF	Limited-access reports: View	
Person Aliases Report	Cross-matter Is run on request.	Lists the primary entries of all people in the catalog, together with their aliases.	PDF HTML	Limited-access reports: View	
Sent Notices Report	Matter-specific Is run on request.	Lists all hold notices in a matter as they were sent and lists the custodians who received the hold notices.	HTML	Matters: View and Notices: View	
User Audit Report	Cross-matter Is run on request.	Lists the person accounts that were created, modified, and deactivated within a given date range.	HTML PDF	Limited-access reports: View	

<i>Table 5. Reports (continued)</i>					
<b>Report name</b>	<b>Cross-matter or matter-specific report</b>	<b>Description</b>	<b>Output format</b>	<b>Privileges required to create the report</b>	<b>Privileges required to view the report</b>
User Information Report	Cross-matter Is run on request.	Lists and describes the active users who were assigned one or more roles within an organization.	HTML PDF	Limited-access reports: View	
User Login Report	Cross-matter Is run on request.	Lists the users (active and inactive) who signed in to the system within a given date range.	HTML PDF	Limited-access reports: View	

By default, a report is available for viewing for 30 days. The report retention period can be changed as part of the system settings. For more information, see [“Configuring system settings” on page 58](#).

Even if key-based access control is enabled in your StoredIQ for Legal system, these built-in reports do not implement any key-based access control. If you want to make use of such restrictions, you must customize the report definitions accordingly.

Except for the Matter Audit Report, the Notice History Report, and the Sent Notices Report, the definitions of the predefined reports can be changed. For more information, see [“Managing report definitions” on page 124](#).

Any custom attributes that you define are automatically added to the reporting views provided with StoredIQ for Legal after the reporting database is refreshed. If you create your own custom reporting views, you must add any custom attributes manually to those views.

### **Custom reports**

However, the predefined reports might still not meet your demands. To create a custom report, you must add a report definition to StoredIQ for Legal. StoredIQ for Legal supports custom reports with the following characteristics:

#### **Scheduled cross-matter reports**

Contain data from several matters or from all matters. They are run automatically according to a schedule. The schedule is defined as part of the system settings. The reports can include custom attributes.

The report definition can contain the privileges that are needed to view those reports. All users with those privileges or with the **Limited-access reports: View** privilege can view the reports.

Access can be limited further by implementing key-based access control.

#### **Requested cross-matter reports**

Contain data from all matters that the user has access to. They must be requested by a user. They can include custom attributes. The reports can be further customized when they are created. In this case, the report definition must contain the information that the user is prompted for.

Report definitions for this type of reports should contain the **\_userid** parameter. By default, this parameter is used for security filtering. If your report definition does not contain this parameter, a warning message is issued when you add or activate your report definition.

The report definition can contain the privileges that are needed to create those reports. All users with those privileges or with the **Limited-access reports: View** privilege can create and view the reports.

Access can be limited further by implementing key-based access control.

## Matter-specific reports

Contain data from one matter only. They must be requested by a user.

Report definitions for this type of reports should contain the parameters `_userid` and `_matterid`. By default, these parameters are used for security filtering. If your report definition does not contain these parameters, a warning message is issued when you add or activate your report definition.

The report definition specifies the privileges that are needed to create and view those reports. In addition to these privileges, the user needs the **Matters: View** privilege and access to the matter.

Access can be limited further by implementing key-based access control.

Custom reports are also kept for 30 days by default. The report retention period can be changed as part of the system settings. In the report definition, you can specify the output format of the reports: CSV, HTML, and PDF. For a common look and feel of your custom reports, you can also provide a set of definition and design resources that your reports can share.

## Access control

In general, you control access to the reports by assigning the appropriate privileges to the users. Be careful with the **Limited-access reports: View** privilege. Without further restriction, users with this privilege can view all cross-matter reports even if they include data from sensitive matters and from matters that they do not have access to.

If key-based access control is enabled, you can limit the access on the report level by adding the `ilg_rpt_accessRestrictions` property with one or more keys to your report definition. With this property, you can restrict the access to the report to those users who provide the required key information in their sign-in information. For example, to base the restriction on location, the property value can be a single key such as US to restrict access to just one location or a comma-separated list of keys such as US, UK, IN to allow access from these locations.

Your report definition must then also contain the `_aclFilter` parameter. StoredIQ for Legal uses this report parameter to pass on the access key information.

If you don't want such a restriction for your reports, do not include the `ilg_rpt_accessRestrictions` property in your report definition.

The reports that are listed on the **Reports** page or show up on a matter's **Reports** pages or in the migration portal are filtered based on the setting in the report definition. Basically, access to matter-specific reports is controlled by the matter settings and by the report definition. If users cannot access a matter, they cannot see any reports under that matter. If users can access the matter but any of the reports is restricted, the respective report might not show up in the list of reports for that matter. For cross-matter reports, access restrictions can be applied only based on the report definition. You cannot apply key-based access restrictions to scheduled reports.

## Reporting views

You can also create reports outside of StoredIQ for Legal from the data in the StoredIQ for Legal reporting database. In this case, you use the reporting views. For more information, see [“Creating reports by using reporting views”](#) on page 126.

## Customization of the reporting database

To meet your specific reporting requirements, you might also want to customize the reporting database by adding your own reporting views or specific roles, or by setting additional permissions. To do so, create an SQL file with the required statements and store it in StoredIQ for Legal. The SQL statements in the customization file must follow a specific format: each statement must be immediately followed by the end delimiter `-- ###end### --` as shown in the following example:

```
CREATE ROLE john LOGIN;
-- ###end### --
```

```
CREATE ROLE jane LOGIN;  
-- ##end## --
```

To apply and persist your customizations, the SQL commands in this file are automatically executed as user `reportadmin` after each refresh of the reporting database. You manage such a customization file in the system settings.

---

# Deploying and configuring

Before you deploy and configure StoredIQ for Legal, ensure that you meet all hardware and software requirements. For details, see [“System requirements” on page 19](#).

## Deploying and configuring StoredIQ for Legal as a VMware virtual appliance

---

Deploy and configure StoredIQ for Legal as a virtual appliance in a VMware virtual host environment.

### Deploying StoredIQ for Legal (VM)

Use VMware vSphere Client to deploy StoredIQ for Legal on a VMware ESX or VMware vCenter server. StoredIQ for Legal is delivered as a single OVA file.

[“Planning for deploying StoredIQ for Legal” on page 19](#)

The following procedure applies to deploying StoredIQ for Legal by using the VMware vSphere 6.5 web client. For other vSphere clients, the steps and windows might be slightly different.

To deploy the StoredIQ for Legal, complete these steps:

1. Connect to the VMware ESX server or VMware vCenter server with the VMware vSphere client.
2. In the vSphere web client, right-click any object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **Deploy OVF Template**.
3. In the **Deploy OVF Template** wizard, complete the following steps:

- a) On the **Select template** page, specify the location of the appropriate source OVA file and click **Next**.

You can specify the URL to an OVA file located on a web site or you can select a local file.

**Restriction:** When you deploy StoredIQ for Legal by using the VMware vSphere 6.5 Web Client in Internet Explorer 11 or Microsoft Edge, the OVA file must be available at a web site. You cannot deploy the OVA from the local file system because of the file upload limits in Internet Explorer and Microsoft Edge.

- b) On the **Select name and location** page, enter the host name for the virtual machine (VM) and select the inventory folder in which to put the VM. Click **Next**.

**Important:** The host name must be unique within the inventory folder. Ensure that you select the correct folder in which to put the VM.

Also, the host name is used when you do the VM network configuration and in the web address (URL) that is used by all users to connect to StoredIQ for Legal. Carefully choose the host name now, as it is frequently used.

- c) On the **Select a resource** page, select the resource where the deployed VM template is to run, and click **Next**.
- d) On the **Review details** page, review the OVF template details. Click **Next**.

These storage requirements are critical and are used to select a data store during deployment.

- e) On the **Select storage** page, select the virtual disk format and the destination storage for the VM files. Click **Next**.

**Tip:** Selection of the **Thin Provision** option saves disk space, but can affect the performance. If disk usage is not a concern, select **Thick Provision Lazy Zeroed**.

- f) On the **Select networks** page, select a source network and map it to a destination network. Click **Next**.

- g) On the **Ready to complete** page, review the deployment settings and ensure that they are correct. If any settings are incorrect, click **Back** to the appropriate settings page, correct the settings, and click **Next** to the **Ready to complete** page.

h) Click **Finish** to complete deployment of the OVF template.

A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task is complete, the new virtual machine is available.

Power on the VM after deployment is complete.

## Configuring StoredIQ for Legal (VM)

After you deploy IBM StoredIQ for Legal, power on the virtual machine (VM) and configure the network settings.

- Decide whether you want to assign a static IP address to your VM. In this case, you must know the IP address to be able to complete this configuration task. If you do not know the IP address, contact your VMWare system administrator to get it.
- You can use an IP address for one VM only.

To configure the network settings, take these steps:

1. In VMWare vSphere Client, select the VM that you deployed and right-click.
2. Click **Open Console** to start the VM console.
3. When prompted, accept the license agreements.
4. Enter a password for the user `root`.

**Important:** Record this password for future reference, that is, to sign in to the VM from a console window.

5. Enter a password for the bootstrap `ilgadmin` administrative account at the prompt.

**Important:** Record this password for future reference. However, this password can be changed later by running the `/siq/bin/change_ilgadmin_password.sh` script. The script request the old and the new password as input and must be run as root user.

6. Set up your network configuration.

The default networking service is provided by RHEL NetworkManager. To interact with this service, the initial StoredIQ for Legal configuration uses the NetworkManager Text User Interface (`nmtui`).

In the console window:

- a) Set the fully qualified host name for this system.
- b) Configure the network connection.

For an IPv4 configuration with static IP addresses (manual configuration), for example, you must enter the following information:

- The assigned IP address, including the netmask in CIDR notation
- The IP address of the default gateway for the IP subnet
- The IP address for the domain name server
- One or more search domain names

For details about network configuration, see the *RHEL Networking Guide*.

When your configuration is complete, the network services of the VM are automatically restarted.

7. When you are prompted, sign in as `root`.

You are signed in to the StoredIQ for Legal VM, which is the StoredIQ for Legal server, as the root user in a Linux console window.

8. Verify that you can sign in to the StoredIQ for Legal web client.

- a) Open a web browser on a host that has network access to the StoredIQ for Legal server.
- b) In the browser address field, enter the web address in the following form:

```
https://siqserver/navigator
```



Where *siqserver* stands for the fully qualified host name or the IP address of the StoredIQ for Legal server.

**Important:** All StoredIQ for Legal users will use this web address to sign in to StoredIQ for Legal.

- c) Sign in to the StoredIQ for Legal web client with the credentials of the StoredIQ for Legal administrative user.

Use the default signin ID of the administrative user, which is *ilgadmin*, and the password that you specified in step “5” on page 42.

After a successful signin, the **Administration** page is displayed.

9. To reconfigure the VM, you can run the following applications from the console window:

Task	Script command
Network configuration	<code>/siq/bin/netcfg</code>
SSL certificate configuration	<code>/siq/bin/cert_install</code>
Change system administrator password for the first time you start the VM	<code>/usr/local/sbin/create_ilgadmin</code>
Change system administrator password	<code>/siq/bin/change_ilgadmin_password</code>
Change report administrator password	<code>/siq/bin/change_reportadmin_password</code>
Logging configuration	<code>/siq/bin/logs</code>
Reset the security domain	<code>/siq/bin/remove_secdom</code>

#### Related reference

[Administration scripts](#)

StoredIQ for Legal comes with a set administration scripts, for example, for reconfiguring the virtual machine (StoredIQ for Legal (VM)) or for changing passwords.

#### Related information

[RHEL Networking Guide: IP Networking](#)

## Upgrading StoredIQ for Legal (VM)

StoredIQ for Legal provides a script for upgrading your Open Virtual Appliance (OVA) to the latest version.

- If your IBM StoredIQ for Legal system is connected to IBM StoredIQ, ensure that your IBM StoredIQ is at Version 7.6.0.9 or later before you begin the IBM StoredIQ for Legal upgrade.
- These instructions apply to upgrades from the preceding fix pack to the current fix pack. Direct upgrades from other fix packs are not supported.

To upgrade your Open Virtual Appliance (OVA) to the latest version of StoredIQ for Legal:

1. Back up your StoredIQ for Legal VMware image in case the upgrade fails. You can use one of the following methods:
  - Create a snapshot of the current state of the image.
  - Create a clone of the current state of the image.

**Important:** After you successfully upgrade your OVA, do not try to restore any database backup of an earlier version of StoredIQ for Legal.

2. Optional: If you customized your reporting database, back up those customizations to an SQL file. During the upgrade, any custom objects are deleted. To be able to reapply your customizations after the upgrade, create an SQL file with the required statements.

3. Transfer the latest upgrade package to the StoredIQ for Legal server.

Upgrade packages are named following this convention:

`IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_UPGRADE.bin`. The upgrade package for the first StoredIQ for Legal V2.0.3 fix pack, for example, would be named

IBM\_STOREDIQ\_FOR\_LEGAL\_V2.0.3.1\_UPGRADE.bin. Make the package executable by entering the following command: `chmod +x IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_UPGRADE.bin`

4. **Optional in SSO-enabled environments:** You can configure a list of trusted IdP realms. If you want to configure these automatically during the upgrade and haven't done so before, edit the `/siq/conf/sso_configuration.properties` file and add a new property with the list of trusted realms (separated by "|").

For example: `trusted_realms=example.com|otherexample.com`

5. Either in the console or an SSH session, navigate to the directory where you stored the upgrade package.

Issue the following command: `./IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_UPGRADE.bin [password]`

The script requires the system administrator (ilgadmin) password to be specified. Optionally, you can pass this password with the command directly. If you don't, you will be prompted to specify the password. You will also be prompted to accept the license terms and conditions.

The first step in the upgrade process is to check the available disk space. If sufficient space is available, the upgrade process continues. Otherwise, the upgrade process fails with an error message. To solve space issues, you can follow the process as described in the [FAQ technote \*Extending the size of the StoredIQ for Legal data containers\*](#).

Depending on the amount of data that needs to be migrated, upgrading can take a while. Begin and end of the migration step are indicated by messages like the following ones that are written to the console during the upgrade:

```
Data migration task initiated, this could take a while to complete
2019-07-02 10:34:36 Additional logs available at:
...
2019-07-02 11:01:53 Data migration task complete
```

Also, `upgrade_yyyymmddhhmmss/upgrade_rest_prologue_second.log` and `upgrade_yyyymmddhhmmss/upgrade_rest_epilogue_second.log` files are written to the `/var/bootstrap/` path. The log files include information about the notification migration status.

6. View the `/var/bootstrap/solserver.log` log file to verify that the upgrade succeeded.

The log should contain a message similar to the following:

```
Upgrade to IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_UPGRADE completed
```

If the upgrade failed, restore your original system from the backup you created prior to the upgrade.

If you migrated IBM Atlas Policy Suite notices in the previous release, be aware that the staging database that is used for migration is dropped during the upgrade. It is re-created on the next migration run.

7. Remove the upgrade package from the StoredIQ for Legal server.
8. Sign in to StoredIQ for Legal as a system administrator with the **System: Manage** privilege, and go to **Admin > System Settings** and review the system settings. Switch off any licenses that you do not have to hide the corresponding features.

Make sure you complete the post-upgrade tasks and review the [migration information](#) before you use the new version.

#### **Related tasks**

[Backing up and restoring your StoredIQ for Legal \(VM\) databases](#)

You can back up and restore your StoredIQ for Legal (VM) databases using a script provided with the product.

#### **Related reference**

[Administration scripts](#)

StoredIQ for Legal comes with a set administration scripts, for example, for reconfiguring the virtual machine (StoredIQ for Legal (VM)) or for changing passwords.

### Post-upgrade tasks

After upgrading StoredIQ for Legal, you must perform several post-upgrade tasks to ensure that StoredIQ for Legal works as expected.

You must be signed in to StoredIQ for Legal as a system administrator.

Complete post-upgrade tasks as required.

- Set a new password for the report administrator.

During the upgrade, the report administrator (`reportadmin`) password is reset to the StoredIQ for Legal default password. Run the `/siq/bin/change_reportadmin_password` script to set a new password:

```
/siq/bin/change_reportadmin_password -n new_pwd -p ilgadmin_pwd
```

- Reapply any customizations of the reporting database.
  - a) Make sure that the SQL statements in your backup file follow the required format. Each statement must be immediately followed by an `-- ##end## --` end delimiter.
  - b) In the StoredIQ for Legal web client, go to **Admin > System Settings**.
  - c) Under **Reports**, add your database customization file to store it in StoredIQ for Legal. These customizations are applied after every refresh of the database.
  - d) To apply and persist your customizations right away, refresh the database manually by clicking **Run Now**.
- If you use the import command line interface (CLI), check whether the fix pack contains a new version of the import CLI: on the application server where StoredIQ for Legal is installed, change to the `/siq/samples` path and check the name of the `siq41-cli-version.tar.gz` file, where *version* stands for the version of the supplied import CLI. If you have an older version installed, install the new import CLI.

For more information, see [“Installing the import command line interface \(CLI\)”](#) on page 179.

If you want to reuse specific custom mappings or mapping templates, the information in the [“Upgrading from Version 2.0.3.2”](#) on page 46 section in the migration information also applies.
- If IBM StoredIQ is part of your solution and is configured to use HTTPS connections, some additional configuration steps might be necessary to ensure the two systems can connect. You must import the IBM StoredIQ certificate into the StoredIQ for Legal IBM WebSphere Application Server keystore if, on StoredIQ for Legal side, either a self-signed certificate is used or the certificate was not imported by using the `/siq/bin/cert_install` script. For more information, see [the instructions for importing the IBM StoredIQ certificate](#).

### Migration information

If you are upgrading to StoredIQ for Legal Version 2.0.3.10 from an earlier 2.0.3.x version, review this migration information.

#### Upgrading from Version 2.0.3.9 to Version 2.0.3.10

No additional migration steps are required.

#### Upgrading from Version 2.0.3.8 to Version 2.0.3.9

No additional migration steps are required.

#### Upgrading from Version 2.0.3.7 to Version 2.0.3.8

No additional migration steps are required.

### **Upgrading from Version 2.0.3.6 to Version 2.0.3.7**

If you want to have the IBM Atlas Policy Suite transmission and response history information for notices that were migrated in StoredIQ for Legal 2.0.3.5 to be available in StoredIQ for Legal, make sure to run the migration tool with the **--update-existing** option before migrating to version 2.0.3.7.

### **Upgrading from Version 2.0.3.5 to Version 2.0.3.6**

No additional migration steps are required.

### **Upgrading from Version 2.0.3.4**

#### **Import mappings**

If you use the import command line interface (CLI), you might have custom mappings or mapping templates for the target entity `persondistinct` that you want to reuse in Version 2.0.3.6. In this case, change the value of the `updateaction` attribute from `UPDATE_ENTITY` to `UPDATE_PERSON` to allow for person-specific updates.

Also check the migration information for upgrades from Version 2.0.3.5 and later.

### **Upgrading from Version 2.0.3.3**

Check the migration information for upgrades from Version 2.0.3.4 and later. No additional migration steps are required.

### **Upgrading from Version 2.0.3.2**

#### **Import mappings**

If you use the import command line interface (CLI), you might have custom mappings or mapping templates for the following target entities that you want to reuse:

- `datarequest_custodians`
- `datarequest_custodians_adhoc`
- `notice_custodians`
- `notice_custodians_adhoc`
- `interview_custodians`
- `interview_custodians_adhoc`

Check whether the Mappings section contains a mapping for the target entity attribute `reason`. If so, remove the `reason` attribute mapping.

Also check the migration information for upgrades from Version 2.0.3.3 and later.

### **Upgrading from Version 2.0.3.1**

#### **Impact of the changed behavior for reminder notices and recurring interviews on existing hold notices and interviews**

The reminder cycle for hold notices that require confirmation now starts only after the custodian confirms the initial notice. However, if a short follow-up cycle is defined for existing hold notices, which is complete before the reminder cycle was supposed to start, and the custodians forget to confirm the initial notice, they now would never get any reminders. To avoid this, the follow-up schedule for existing initial hold notices is automatically changed during the upgrade. The updated schedule is to repeat sending follow-up messages until the initial notice is confirmed.

The same applies to recurring interviews.

Existing hold notice and interview templates remain unchanged during the upgrade.

Also check the migration information for upgrades from Version 2.0.3.2 and later.

## Upgrading from Version 2.0.3.0

### New import privileges

To be able to use the import API, users must now have the appropriate import privileges set. For details, see [“Roles and privileges: Overview”](#) on page 77.

### Unique person identifier

Each person in the catalog is uniquely identified by an attribute. After the upgrade, you must set the person attribute that is to be used as identifier in the system settings before you can import more people from the directory server or by using the import API.

If you previously imported people from the directory server, set the person attribute to the signin ID. If you imported people by using the import API, set the person attribute to the attribute that you used in your import mappings.

For details, see [“Planning for importing people into StoredIQ for Legal”](#) on page 21.

### Import mappings

Due to the introduction of the person attribute for identifying persons in the catalog, the default import mappings for the following target entities no longer contain the `identityattribute` attribute. If you still use V2.0.3.0 import mappings, remove the `identityattribute` attribute.

- `datarequest_custodians_adhoc`
- `notice_custodians_adhoc`
- `persondistinct`
- `persondistinct_adhoc`

For details, see [“Import mapping structure: Target entity definition section”](#) on page 175.

Also check the migration information for upgrades from Version 2.0.3.1 and later.

## Installing and removing custom SSL certificates for StoredIQ for Legal (VM)

StoredIQ for Legal (VM) is already configured with self-signed certificates that are used with SSL connections. However, you can install your own certificates, either self-signed or from a certificate authority (CA), to be used instead of the preconfigured certificates.

You need the IP address and host name of your StoredIQ for Legal virtual machine (VM).

You need to open a Linux® command window connection (or console, for short) to the VM to run the certificate command-line tool. The VMWare vSphere client application supports opening console connections. If you choose not to use VMWare vSphere console, you must install on a remote host an application that uses the SSH protocol. You will use the SSH application to open a console connection to the VM. Some example applications are OpenSSH and PuTTY.

If you need to copy files to the VM, you must install on the remote host from which you will copy the files a *secure copy application* that uses the SSH protocol to securely copy files. An example application is WinSCP.

If you plan to use your own certificate, which can be either from a certificate authority (CA) or self-signed, then you must package your private key and certificate in a single password-protected keystore file and import the keystore file. Do not password-protect the private key and certificate. Password-protect only the keystore file. The supported keystore file formats include PKCS12, JCEKS, CMSKS, JKS, and PKCS11. If you use OpenSSH, it has command-line facilities and documentation that explain how to package your private key and certificate in a supported file format with a password and decrypt and strip out passwords, if necessary.

**Important:** Make sure you renew or remove certificates before they expire or are revoked. Otherwise, the StoredIQ for Legal commands for administering the application in the web application server will no longer work.

To install and remove custom certificates:

1. In VMWare vSphere client, right-click the VM and then click **Open Console**.
2. Sign in with the `root` user ID and its password.

3. With a server-to-server copy tool that uses the SCP protocol, copy your DER encoded certificate from the web service to the path `/siq/conf`.
4. In the `/siq/conf` path, copy the `cert_configuration_default.properties` file and save it as `cert_configuration.properties` at the same location.

If the file with the default values is not available, contact your VM system administrator or IBM Customer Support.

5. Open the `cert_configuration.properties` file to edit it.

**Tip:** Use an editor that comes with the operating system, such as VI, to ensure that no characters are included that corrupt the configuration.

6. Required: Set the `certificateAlias` property to a name of your choice.

The default property setting is `certificateAlias=customer_certificate_alias`. Write down the `certificateAlias` setting for future reference if your certificate needs to be replaced. This value is required.

**Important:** Make sure you renew or remove your certificate before it expires. Otherwise, administration commands addressing the web application server will no longer work.

7. Uncomment the following line and add the file name of the certificate you uploaded:

```
#certificateFileName=certificate.cer
```

8. Optional: Complete this step only if you are creating a self-signed certificate.

- a) In the section with the `### Certificate creation option ###` heading, under the `## Required` subheading, remove the comment character `#` at the start of the line for the required properties.
- b) Under the `## Optional` subheading, remove the comment character `#` at the start of the line for the optional properties that you want to include.
- c) Enter values for all required fields and for any optional fields that you want to include.
- d) Comment out optional fields that you are not using by leaving the `#` character at the front of the line.
- e) Comment out all the properties in the section with the `### Certificate import option ###` subheading, which are the import settings.
- f) Save your changes and exit the file.
- g) In the console, enter `cd /siq/bin`.
- h) Enter `./cert_install deploy -t -p admin_password`

The certificate is created as a trusted certificate to the appliance.

**Important:** Make sure you renew or remove your certificate before it expires. Otherwise, administration commands addressing the web application server will no longer work.

9. Optional: Complete this step only if you are importing a keystore file that contains a self-signed or CA-signed certificate.

- a) In the section with the `### Certificate import option ###` heading, under the `## Required` subheading, remove the comment character `#` at the start of the line for the required properties.
- b) Enter the values for all required properties.
- c) Comment out all of the properties in the section with the `### Certificate creation option ###` heading, which are the creation settings.
- d) Save your changes and exit the file.
- e) Using the secure copy application, copy your keystore file from the remote host to the `/root/certs` directory.
- f) In the console, enter `cd /siq/bin`.
- g) Enter `./cert_install deploy -i -t -p admin_password`

The certificate is imported as a trusted certificate to the appliance.

**Important:** Make sure you renew or remove your certificate before it expires. Otherwise, administration commands addressing the web application server will no longer work.

10. Optional: Complete this step only if you are removing certificates.

- a) Make a backup copy of the `cert_configuration.properties` file. Then open the original file.
- b) In the section with the `### General ###` heading, under the `## Required` subheading, set `certificateAlias` to the certificate alias of the certificate that you want to remove.
- c) In the console, enter `cd /siq/bin`.
- d) Enter `./cert_install remove -t -p admin_password`

The certificate is removed as a trusted certificate from the appliance.

11. Here is a summary of the commands that you used in the previous steps.

Task	Script command
Create certificate	<code>./cert_install deploy -t -p admin_password</code>
Import certificate	<code>./cert_install deploy -i -t -p admin_password</code>
Remove certificate	<code>./cert_install remove -t -p admin_password</code>

## Configuring single sign-on for StoredIQ for Legal (VM)

StoredIQ for Legal (VM) supports Security Assertion Markup Language (SAML) and Kerberos single sign-on (SSO).

Before enabling SSO, ensure you have users of your Identity Provider's (IdP) directory server imported into the catalog of StoredIQ for Legal. For details, see [“Planning for importing people into StoredIQ for Legal”](#) on page 21. At least one of these users must have the **Users and roles: Manage** privilege.

To enable SSO, you must set up a properties file to contain your SSO configuration and then run a script that applies this configuration.

1. Open a Linux command window connection (or console, for short) to the VM.  
Sign in as root.
2. Copy the default SSO properties file named `/siq/conf/sso_configuration_default.properties` to a file named `/siq/conf/sso_configuration.properties`.  
Ensure that the new file has 755 permissions set.
3. Complete the steps that apply to the identity management system you use:

- [“Configuration steps for SAML SSO”](#) on page 50
- [“Configuration steps for SAML SSO without LDAP”](#) on page 50
- [“Configuration steps for Kerberos SSO”](#) on page 51
- [“Configuration steps for CA SiteMinder SSO”](#) on page 52

4. To apply the SSO configuration, run the `/siq/bin/enable_sso.sh` script.

If you set up CA SiteMinder SSO, follow the instructions on the screen to register the agent with CA SiteMinder. The installation must be `/home/sso/smwasasa`. A different installation location is not supported.

If you set up SAML SSO, the service provider metadata is now available in the `/siq/conf/sp-metadata-file.xml` file on the VM and can be used for further IdP configuration, if required.

**Tip:** If, at any time, you want to disable SSO, run the `/siq/bin/disable_sso.sh` script.

For SAML SSO, you can define a URL for invalidating the SSO session after the user signed out to prevent unauthorized access to StoredIQ for Legal. To do so, go to **Admin > System Settings**.

### Related reference

[Administration scripts](#)

StoredIQ for Legal comes with a set administration scripts, for example, for reconfiguring the virtual machine (StoredIQ for Legal (VM)) or for changing passwords.

### Configuration steps for SAML SSO

Complete the following steps to configure SAML SSO if an internal or external LDAP server exists.

Complete steps 1 and 2 in “Configuring single sign-on for StoredIQ for Legal (VM)” on page 49.

1. Copy your IDP metadata file to a file named `/siq/conf/saml2-idp-metadata.xml`. Ensure that the new file has 755 permissions set.
2. Edit the `sso_configuration.properties` file, and add or update configuration settings as follows:

Property	Description	Value
<code>sso_standard</code>	The type of SSO.	SAML
<code>idp_metadata_filepath</code>	The name of the metadata file.	<code>saml2-idp-metadata.xml</code>
<code>idp_cert_alias</code>	The alias of the certificate referenced in the metadata file.	<code>certificate_name</code>
<code>tai_property_x</code>	One or more trust association interceptor (TAI) properties that define your SSO configuration. The properties must be numbered sequentially, starting with <code>tai_property_0</code> . You can choose from the set of TAI properties that can be used in WebSphere Application Server. For details about these properties, see the <a href="#">WebSphere Application Server documentation about SAML web SSO TAI custom properties</a> .  For StoredIQ for Legal, SSO is configured with IdP ID <code>idp_1</code> and SSO ID <code>sso_1</code> .	<code>TAI_property</code>
<code>trusted_realms</code>	One or more trusted IdP realms (separated by <code> </code> ).  For example: <code>trusted_realms=example.com otherexample.com</code>  Configuring trusted IdP realms is optional.	<code>list_of_trusted_realms</code>

The `sso_configuration.properties` file should look similar to this example:

```
sso_standard=SAML
idp_metadata_filepath=saml2-idp-metadata.xml
idp_cert_alias=your_cert_alias
tai_property_0=sso_1.sp.acsUrl=https://hostname:sslport/samlsp/URI_pattern
tai_property_1=sso_1.sp.idMap=localRealm
tai_property_2=sso_1.sp.login.error.page=redirection_target_unauth_request
tai_property_3=sso_1.sp.filter=request-url%=navigator
tai_property_4=sso_1.idp_1.EntityID=some_acl_url
tai_property_5=sso_1.idp_1.SingleSignOnUrl=sso_service_url
tai_property_6=sso_1.idp_1.certAlias=your_cert_alias
tai_property_7=sso_1.sp.useRelayStateForTarget=false
tai_property_8=sso_1.sp.targetUrl=https://hostname:sslport/navigator
```

Continue with step 4 in “Configuring single sign-on for StoredIQ for Legal (VM)” on page 49.

### Configuration steps for SAML SSO without LDAP

Complete the following steps to configure SAML SSO if no internal or external LDAP server exists.

“Configuration steps for SAML SSO” on page 50

1. Adapt the `sso_configuration.properties` as follows:
  - Add the following TAI properties:



- `sso_1.sp.useRealm` and set it to `defaultWIMFileBasedRealm`
- `sso_1.idp_1.SingleSignOnUrl` and set it to `hostname/idp/profile/SAML2/Unsolicited/SSO`
- `sso_1.idp_1.EntityID` and set it to `hostname/idp/shibboleth`

*hostname* stands for the fully qualified host name or the IP address of the IdP directory server that you use.

- Remove the TAI property `sso_1.sp.idMap` or set it to `idAssertion`
2. Add the `idp-signing.crt` certificate of the IdP directory server to WebSphere Application Server.
  3. Complete these steps in WebSphere Application Server:
    - a) Change the user account to use federated repositories instead of a standalone LDAP repository: go to **Security > Global security**. Specify the administrator credentials.
    - b) Ensure that `defaultWIMFileBasedRealm` is a trusted realm.
    - c) Go to **Security > Security domains** and open **ILGNSecurityDomain**. Ensure that `defaultWIMFileBasedRealm` is a trusted realm.
  4. Restart WebSphere Application Server.

Continue with step 4 in [“Configuring single sign-on for StoredIQ for Legal \(VM\)”](#) on page 49.

### Configuration steps for Kerberos SSO

Complete the following steps to configure Kerberos SSO

Complete steps 1 and 2 in [“Configuring single sign-on for StoredIQ for Legal \(VM\)”](#) on page 49.

1. Copy your keytab file to a file named `/siq/conf/kerb.keytab`. Ensure that the new file has 755 permissions set.
2. Edit the `sso_configuration.properties` file, and add or update configuration settings as follows:

Property	Description	Value
<code>sso_standard</code>	The type of SSO	KERBEROS
<code>keytab_filepath</code>	The name of the keytab file	<code>kerb.keytab</code>
<code>kerberos_realm</code>	The Active Directory domain name	<i>AD_domain_name</i> This value is case sensitive and must be in all capital letters.
<code>ad_hostname</code>	The fully qualified host name of the Active Directory server	<i>AD_host_name</i>
<code>dns_domain</code>	The domain name service (DNS) of the Key Distribution Center (KDC)	<i>KDC_DNS</i>
<code>application_server_hostname</code>	The hostname of the application server	<i>host_name</i>
<code>trusted_realms</code>	One or more trusted IdP realms (separated by  ). For example: <code>trusted_realms=example.com otherexample.com</code> Configuring trusted IdP realms is optional.	<i>list_of_trusted_realms</i>

Continue with step 4 in [“Configuring single sign-on for StoredIQ for Legal \(VM\)”](#) on page 49.

## Configuration steps for CA SiteMinder SSO

Complete the following steps to configure SSO with CA SiteMinder (CA SiteMinder is the former product name of CA Single Sign-On).

Complete steps 1 and 2 in [“Configuring single sign-on for StoredIQ for Legal \(VM\)”](#) on page 49.

1. Download the CA SiteMinder Agent for IBM WebSphere installer for Unix/Linux to your StoredIQ for Legal system.
2. Extract the contents of the `ca-asa-was-12.0-sp02` file to a folder named `/siq/conf/sm_asa_was`.
3. Edit the `sso_configuration.properties` file, and add or update configuration settings as follows:

Property	Description	Value
<code>sso_standard</code>	The type of SSO	SITEMINDER

Continue with step 4 in [“Configuring single sign-on for StoredIQ for Legal \(VM\)”](#) on page 49.

## Backing up and restoring your StoredIQ for Legal (VM) databases

You can back up and restore your StoredIQ for Legal (VM) databases using a script provided with the product.

With StoredIQ for Legal Version 2.0.3.2, some of the internal keystore settings changed. Therefore, you cannot restore data in a later version of StoredIQ for Legal from backup files created with product versions before Version 2.0.3.2.

To manage backup and restore of your StoredIQ for Legal databases:

- To back up your StoredIQ for Legal database information, use the **`/siq/bin/backup create`** command. When you run the command without any options, a backup file is created in the `/root/backup` folder and is named in the format `data_timestamp.dat`, for example `data_2017.Apr.06_22.08.45.dat`. However, you can specify a file name of your choice, and you can use the **`-folder`** option to specify the location of the backup file.
- To list your available backups, use the **`/siq/bin/backup list`** command. If your backup files are not stored in the default backup folder `/root/backup`, use the **`-folder`** option to specify the respective folder.
- To restore your StoredIQ for Legal database information:
  - a) Run the **`/siq/bin/backup restore`** command.

When you run this command, you must specify the name of the backup file to restore and pass your system administration password with the **`-p`** option, for example:

```
/siq/bin/backup restore data_2017.Apr.06_22.08.45.dat -p password
```

If your backup file is not stored in the default backup folder `/root/backup`, use the **`-folder`** option to specify the appropriate folder.

- b) When your StoredIQ for Legal database information is successfully restored, sign in to the StoredIQ for Legal web client as `ilgadmin`.

Verify that StoredIQ for Legal can still communicate with the external servers:

- a. Go to **Admin > External Servers > Email Server** and complete the following steps:
  - 1) Make a note of the settings. You will need them later to revert to the proper configuration.
  - 2) Although all settings are correct, make a small change to the server name. Then, save your changes.
  - 3) Wait for the notification that the connection to the email server could not be established.
  - 4) Undo your changes to the server name by resetting it to the proper the value. Then, save your changes.
  - 5) Wait for the notification that StoredIQ for Legal successfully connected to the email server.

- b. Go to **Admin > External Servers > Directory Server** and verify that StoredIQ for Legal can still communicate with the directory server by completing the same steps as for verifying the communication between StoredIQ for Legal and the email server.
- c. Go to **Admin > External Servers > StoredIQ Server** and verify that StoredIQ for Legal can still communicate with the IBM StoredIQ server by completing the same steps as for verifying the communication between StoredIQ for Legal and the email server.

## Deploying and configuring StoredIQ for Legal on Red Hat OpenShift

Starting with version 2.0.3.10, you can deploy and configure StoredIQ for Legal in a Red Hat OpenShift environment.

You can run **oc** commands on any OpenShift client that has the **oc** client tool installed and that has access to the cluster where IBM StoredIQ for Legal is deployed, or from the master node of the cluster. For more information about the **oc** client tool, see [Get Started with the CLI](#) in the OpenShift documentation.

### Deploying StoredIQ for Legal (Container)

Deploy StoredIQ for Legal in an OpenShift environment.

Supported platform version: Red Hat OpenShift 3.11

To complete this task, you must be a user with cluster administrator privileges.

The StoredIQ for Legal product package must be available on the machine where you plan to complete this task. If it is not, obtain the package:

1. Download the package from Fix Central. The package is named following this convention:  
IBM\_STOREDIQ\_FOR\_LEGAL\_Vv.r.m.fp\_CLOUD.tar.gz.
2. Extract the contents of the package by running the following command:

```
tar -xzf IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_CLOUD.tar.gz
```

Replace *v.r.m.fp* with the appropriate version information.

The package content is extracted to the IBM\_STOREDIQ\_FOR\_LEGAL\_Vv.r.m.fp\_CLOUD subdirectory.

As an alternative to completing the following steps by using the command-line interface on an OpenShift client or the master node as described, you can use the OpenShift web console to complete the task.

1. Load the docker images located in the `docker-images` directory into a Docker image registry that is accessible from all nodes in the cluster, for example, artifactory.
2. Edit the `config.properties` file and update the values of the following keys to match the settings in your environment:

Key	Sample value
HOST_NAME	siq41.example.com
DOCKER_REPO	siq41-docker.artifactory.com/ilgnext
IMAGE_PULL_SECRET_NAME	artifactory or the registry name provided in step “9” on page 54

3. Run the `setup.sh` script to create the deployment scripts based on the configurations that you defined in the previous steps.
4. Create a namespace for StoredIQ for Legal:

```
oc create namespace siq41openshift
```

5. Switch to the `siq41openshift` project:  
`oc project siq41openshift`
6. Create a custom SecurityContextConstraint (SCC):

```
oc apply -f scc/siq4lsccl.yml
```

7. Create a service account:

```
oc create serviceaccount siq4lserviceaccount
```

8. Add the SCC to the service account:

```
oc adm policy add-scc-to-user siq4lsccl -z siq4lserviceaccount -n siq4lopenshift
```

9. Create a secret in OpenShift for pulling images from your artifactory or Docker registry if such a secret does not exist yet.

A sample secrets configuration is provided with StoredIQ for Legal (Container). To be able to use this sample secrets configuration, you must complete the following steps:

- a) Edit the `secret/config.json` file and fill in all the details for the elements enclosed in angle brackets (< >).
- b) Encode the file in base64.
- c) Use the base64-encoded version in the `secrets/artifactory-secret.yml` configuration file.
- d) Apply the updated configuration by running this command:

```
oc apply -f secrets/artifactory-secret.yml
```

10. Create volumes.

StoredIQ for Legal requires four storage areas, one for each container. Setting up these volumes is entirely up to the OpenShift cluster administrator. As an administrator, take into account the minimum storage capacity required for each volume before allocating any storage.

A sample configuration set is provided for reference which uses NFS for storage. To work with the sample configuration, complete the following steps:

- a) Ensure that the NFS mounts are created with ownership `nfsnobody` and exported.
- b) Update the path and `server` details in the `nfs` section of each configuration file by replacing the placeholders with the correct values.
- c) Apply the changes:

```
oc apply -f pv/db2-storage.yml
oc apply -f pv/pg-storage.yml
oc apply -f pv/tds-storage.yml
oc apply -f pv/websphere-storage.yml
```

11. Create persistent volume claims:

```
oc apply -f pvc/pvcs.yml
```

12. Deploy all the applications (.yml files) from the `deployment-config` directory in the following order:

```
oc apply -f config-maps/sso-config.yml
oc apply -f dc/tds.yml
oc apply -f dc/postgres.yml
oc apply -f dc/ilg-sol-plugin-data.yml
oc apply -f dc/ilg-sol-plugin.yml
```

13. Create routes for accessing StoredIQ for Legal from outside the OpenShift cluster.

Replace `hostname` in the routes file with a public IP address or hostname and create the route by using this command:

```
oc apply -f routes/siq4l.yml
```

Routes are created using the `reencrypt` mechanism. You can provide your own SSL certificates by editing this configuration and appending the `certificate` and `key` blocks in the `tls` configuration.

Create these additional routes in the same way:

- WebSphere console

```
oc apply -f routes/was-console.yml
```

- Monitoring

```
oc apply -f routes/monitoring.yml
```

To access the application, use the URL defined in the `siq41.yml` file.

## Configuring custom SSL certificates for StoredIQ for Legal (Container)

StoredIQ for Legal (Container) is already configured with self-signed certificates that are used with SSL connections. However, you can install your own certificates, either self-signed or from a certificate authority (CA), to be used instead of the preconfigured certificates.

To configure and manage custom certificates, follow the instructions in the [OpenShift documentation](#).

## Setting up single sign-on for StoredIQ for Legal on OpenShift

In an OpenShift environment, StoredIQ for Legal supports Security Assertion Markup Language (SAML) and Kerberos single sign-on (SSO).

To set up SSO, you must set up a properties file to contain your SSO configuration and then run a script that applies this configuration.

The following commands must be run from the `config-maps` directory, which is a subdirectory of the StoredIQ for Legal installation folder.

All commands must be on a single continuous command line. They must not contain any line breaks. However, in the instructions, the commands might be split into multiple lines for readability.

1. Edit the `configs/sso_configuration.properties` file and update it with the information provided by your identity provider (IDP).
  - For SAML SSO, create the `configs/saml2-idp-metadata.xml` file. This file must contain the IDP's metadata.
  - For Kerberos SSO, copy the keytab file to the `configs` directory and rename the file to `kerb.keytab`.
2. Delete the preconfigured configmap by using the following command:

```
oc delete configmap sso-config
```

3. Create a new configmap by appending all the files in the directory:

```
oc create configmap sso-config --from-file=configs/
```

4. Run the following commands to enable SSO:

- a) Get the name of the WebSphere Application Server container:

```
CONTAINER_NAME=$(oc get pods -n siq41openshift -l app=ilg-sol-plugin -o name | sed "s/^\{4\}//" )
```

- b) Get the password for the WebSphere Application Server container:

```
waspaswd=$(oc exec $CONTAINER_NAME -- /bin/retrieveCredentials.sh $ilgadminPwd was);  
export TEMP_SIQ4L_WASPW=$waspaswd
```

- c) Get the type of SSO to use:

```
sso_standard=$(awk '/sso_standard/ {split($1, parts, "="); print tolower(parts[2])}'  
configs/sso_configuration.properties)
```

- d) Add the StoredIQ for Legal SSO configuration:

```
oc exec -t $CONTAINER_NAME -- /bin/bash -c "runuser -l was -c \"/home/was/WebSphere/  
AppServer/profiles/ilgnext/bin/wsadmin.sh  
-lang jython -javaoption '-Xms512m -Xmx1024m' -user administrator -password $waspaswd -
```

```
f /usr/bin/deploy/sso_configuration.py
/home/sso/sso_configuration.properties --$sso_standard\""
```

e) Enable SSO:

```
oc exec -t $CONTAINER_NAME -- /usr/bin/siq4l_icn_sso_enable.sh
```

f) For SAML SSO, additionally run the following commands to create and copy the metadata file from the service provider.

The metadata file can be used for further IdP configuration, if required.

1) Create the appropriate directory:

```
oc exec -t $CONTAINER_NAME -- /bin/bash -c "runuser -l was -c \"mkdir -p /home/was/
WebSphere/AppServer/sso\""
```

2) Create the metadata file:

```
oc exec -t $CONTAINER_NAME -- /bin/bash -c "runuser -l was -c
\"/home/was/WebSphere/AppServer/profiles/ilgnext/bin/wsadmin.sh -lang jython
-javaoption '-Xms512m -Xmx1024m' -user administrator -password $waspasswd -c
'AdminTask.exportSAMLSpMetadata(\\\"-spMetadataFileName
/home/was/WebSphere/AppServer/sso/sp-metadata.xml -ssoId 1\\\")'\\""
```

3) Copy the metadata file:

```
oc cp $CONTAINER_NAME:/home/was/WebSphere/AppServer/sso/sp-metadata.xml .
```

4) Create a route for the SAML application:

```
oc apply -f routes/saml.yml
```

## Disable SSO

Complete these steps to disable SSO for StoredIQ for Legal.

The following commands must be run from the `config-maps` directory, which is a subdirectory of the StoredIQ for Legal installation folder.

All commands must be on a single continuous command line. They must not contain any line breaks. However, in the instructions, the commands might be split into multiple lines for readability.

1. Get the name of the WebSphere Application Server container:

```
CONTAINER_NAME=$(oc get pods -n siq4lopenshift -l app=ilg-sol-plugin -o name | sed "s/^.\
{4\}//" )
```

2. Get the password for the WebSphere Application Server container:

```
waspasswd=$(oc exec $CONTAINER_NAME -- /bin/retrieveCredentials.sh $ilgadminPwd was) export
TEMP_SIQ4L_WASPW=$waspasswd
```

3. Remove the StoredIQ for Legal SSO configuration:

```
oc exec -t $CONTAINER_NAME -- /bin/bash -c "runuser -l was -c \"/home/was/WebSphere/
AppServer/profiles/ilgnext/bin/wsadmin.sh
-lang jython -javaoption '-Xms512m -Xmx1024m' -user administrator -password $waspasswd -
f /usr/bin/deploy/sso_configuration.py
/home/sso/sso_configuration.properties --remove\""
```

4. Disable SSO:

```
oc exec -t $CONTAINER_NAME -- /usr/bin/siq4l_icn_sso_disable.sh
```

## Backing up and restoring StoredIQ for Legal (Container)

Back up and restore StoredIQ for Legal (Container) data by the means provided through OpenShift administration.

For more information about backup and restore procedures in an OpenShift environment, see the OpenShift documentation:

- [Creating an environment-wide backup](#)
- [Restoring OpenShift Container Platform components](#)

## Migrating from StoredIQ for Legal (VM) to StoredIQ for Legal (Container)

If you want to start working with StoredIQ for Legal in a Red Hat OpenShift environment instead of a VMWare virtual host environment, you can migrate the application.

You must have deployed StoredIQ for Legal (VM) and StoredIQ for Legal (Container). Both deployments must be at the same product level. The minimum required product version is version 2.0.3.10.

Verify that you can bring up both StoredIQ for Legal systems without any issues before you start the migration.

1. Back up your StoredIQ for Legal (VM) data by using the provided backup tool.

Sign in to the VM as `root` and run the `/siq/bin/backup create` command. When you run the command without any options, a backup file is created in the `/root/backup` folder. The backup file is named `data_timestamp.dat`. However, you can specify a file name of your choice, and you can use the `-folder` option to specify the location of the backup file

2. Copy the backup file to a directory of your choice on the master node of the OpenShift cluster where StoredIQ for Legal (Container) is deployed.

Use a secure copy tool such as `scp` to do so.

Complete the following steps on the master node of this cluster as user with cluster administration privileges.

3. Stop all StoredIQ for Legal applications in your OpenShift environment by running the following command:

```
oc scale --replicas=0 deployment/your_deployment -n siq4lopernsift
```

4. Extract the contents of the StoredIQ for Legal (VM) backup file to a directory of your choice. Change to the directory where you stored the backup file and extract the package content.

In the following example, the backup file is extracted into the `/tmp` directory.

```
tar -xvf data_timestamp.dat --directory="/tmp"
```

The following files and directories are created in the directory:

- `pluginData.tar`
- `postgres.tar`
- `security`
- `tds.tar`

**Important:** Make sure that all permissions and ownerships are preserved in steps 5 through 8.

5. Extract the contents of the `pluginData.tar` file into the directory to which the persistent volume named `db2-storage` points.
6. Extract the contents of the `tds.tar` file into the directory to which the persistent volume named `tds-storage` points.
7. Extract the contents of the `postgres.tar` file into the directory to which the persistent volume named `pg-storage` points.
8. Copy the content of the `security` directory (`security/*`) into the `security` subdirectory of the directory to which the persistent volume named `websphere-storage` points.

- Start all StoredIQ for Legal applications in your OpenShift environment by running the following command:

```
oc scale --replicas=1 deployment/your deployment -n siq4lopenshift
```

- After all pods are active (check with the **oc get pods** command), run the `post_restore_script` script to finalize the setup.

The script is stored in the `IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_CLOUD/scripts` directory.

You can now start working with StoredIQ for Legal (Container).

## Configuring system settings

You can configure various StoredIQ for Legal system settings.

- [“Planning for secure matters”](#) on page 23.
- [“Planning for reports”](#) on page 35.
- [“Planning for importing people into StoredIQ for Legal”](#) on page 21.
- You must be signed in with the **System: Manage** privilege.

To configure the system settings, complete the following steps:

- Go to **Admin > System Settings**.
- Change the system settings as needed.

Settings	Description
Dashboard caching options	<p><b>Caching</b></p> <p>If set to <b>Yes</b>, the metrics on the dashboard are, by default, updated every 30 minutes. However, the refresh of the dashboard takes less time than without caching. If set to <b>No</b>, you always see the latest metrics when you open the dashboard. However, a large amount of matters, notices, interviews, and data requests increases the response time of the dashboard.</p> <p><b>Refresh cache immediately</b></p> <p>To avoid an increase in the response time of the dashboard, select <b>Yes</b> only if you expect few changes to the matters. If set to <b>Yes</b>, the dashboard always shows the latest metrics. If set to <b>No</b>, the metrics on the dashboard are, by default, updated every 30 minutes. The advantage is that the dashboard is displayed faster.</p> <p><b>In-memory caching</b></p> <p>If set to <b>Yes</b>, the cached metrics are stored in memory, which decreases the response time of the dashboard. However, if you have a large number of matters, the response time might increase again. If set to <b>No</b>, the persistent storage is used to store the cache, which increases the response time of the dashboard. However, the latency for the retrieval of the dashboard pages is more consistent."</p>



Settings	Description
Report settings	<p><b>Enable scheduling</b>            If scheduling is enabled, the reporting database is refreshed and scheduled reports are generated according to the specified schedule. Generated reports are available from <b>Reports &gt; Scheduled Reports</b>.</p> <p>When you disable report scheduling, the refresh schedule is suspended and cannot be changed. This setting becomes active after all currently running tasks are completed. After that, the reporting database is not refreshed and no reports are automatically generated until you enable scheduling again. However, you can manually refresh the database (<b>Run Now</b> button). Also, you can still request reports that are not scheduled.</p> <p><b>Run frequency</b>            Determine how often the scheduled reports are to be generated and the reporting database is to be refreshed. You must be signed in as the default system administrator <code>ilgadmin</code> to change the schedule.</p> <p><b>First run</b>            Set the time of day at which scheduled reports are generated for the first time.</p> <p><b>Report retention period</b>            Set the number of days that reports are kept.</p> <p><b>Database customization file</b>            Store a file that contains all of your customizations to the reporting database. When you add a customization file, these customizations are applied after every refresh of the reporting database to preserve any custom views, roles, permissions granted to those roles, or other changes you might have made. To apply any customization immediately, you must manually refresh the database.</p> <p><b>Important:</b> It is your responsibility to ensure the integrity of the customization file.</p> <p>When you delete the customization file, customizations such as custom views, sequences, triggers, functions and roles are removed the next time the reporting database is refreshed.</p> <p>For details about the customization file, see <a href="#">“Planning for reports” on page 35</a>.</p>

Settings	Description
Audit settings	<p><b>Low-level auditing</b></p> <p>By default, each action that a user performs and each action that the system performs as a result of a user action is recorded. Therefore, it is no longer necessary to enable low-level auditing. Low-level auditing creates a separate record for each operation that stores data and can increase the response time considerably.</p>
Matter security settings	<p><b>Security groups</b></p> <p>If you enable the use of security groups, the access to the matters is restricted to the members of a security group. New matters must be assigned a security group. Existing matters are associated with the default security group. To restrict the access further, a matter can be changed to a sensitive matter.</p> <p>If you do not enable this option, matters can be accessed by any user with the appropriate privileges. To restrict the access, a matter can be changed to a sensitive matter.</p> <p><b>Important:</b> You cannot disable the use of security groups later.</p> <p><b>Key-based access control</b></p> <p>Specify whether the access to any matter can be restricted based on access key information in the request.</p> <p>Before you enable key-based access control, make sure that a custom matter attribute for holding the key is defined. The custom matter attribute must be of the data type drop-down list (single-select) or drop-down list (multiple-select). This attribute must then be set as key attribute.</p> <p>In addition, ensure that a system external to StoredIQ for Legal such as a single sign-on (SSO) system provides the required key value in the header of all incoming user sign-in requests. The lookup key defines the HTTP header field to be checked by StoredIQ for Legal. For each access request, the value of the specified field is compared to the keys set for the matter. If there's a match, access to the matter is granted. Otherwise, access is denied.</p> <p>If you change the lookup key later, you must restart StoredIQ for Legal for this change to take effect.</p>

Settings	Description
Matter settings	If you set the <b>Allow to reopen matters</b> option to <b>Yes</b> , users with the <b>Matters: Close</b> privilege can reopen closed matters.
File attachment settings	Define the maximum file size for attachments in MB.
Help information settings	If you provide your own help information, specify the URL of that help information. Any links in the product that lead to IBM Knowledge Center are then also replaced with this URL.
Licensed programs	You can hide any feature for which you don't have a license.
SSO settings	<p><b>Redirect URL</b></p> <p>To prevent unauthorized access to StoredIQ for Legal in a single sign-on (SSO) environment, you can require people to authenticate again when they try to access StoredIQ for Legal in the same browser where they signed out. Specify the URL that invalidates a session in your SSO environment.</p>
Unique ID for catalog entries	<p>To import people, you must select a person attribute that uniquely identifies each person in the catalog, regardless of whether this person is imported from the directory server or by using the import API. All predefined and custom person attributes with data type String are available for selection. For more information, see <a href="#">“Customizing attributes” on page 68</a>.</p> <p>To preserve data integrity, do not select another person attribute after you start importing people.</p>
User interface search settings	If you enable incremental search, search is done as the user types the search string. Otherwise, the user must press Enter to start the search.
Release data request settings	<p><b>Enable release data requests</b></p> <p>If you enable release data requests, users can create release requests for data of completed preservation or preservation and collection data requests.</p> <p><b>Important:</b> After you enable release data requests, you cannot disable the option again.</p> <p><b>Allow to release data by date ranges</b></p> <p>Users can specify date ranges for the data to be released.</p> <p>This option is available only if release data requests are enabled.</p>

Settings	Description
Comment and attachment deletion	If you enable deletion of comments and attachments, users can delete task comments and attachments in the task view.
Migration portal settings	If you set <b>Show migration portal</b> to <b>Yes</b> , the migration portal becomes available to users with the <b>Notices: Manage</b> or <b>Interviews: Manage</b> privilege. For matters they have access to, they can then check the items that are migrated from IBM Atlas Policy Suite.

## Configuring connections to external servers or services

Depending on the tasks that you want to complete, you must establish a connection to a specific server, or register and manage fulfillment or server discovery connectors.

You must be signed in with the **System: Manage** privilege.

### Configuring the connection to the directory server

If you want to import the people to use IBM StoredIQ for Legal from a directory server, configure the connection to this server. The directory server must be LDAP-compliant.

- [“Planning for importing people into StoredIQ for Legal”](#) on page 21.
- [“Configuring system settings”](#) on page 58. Under **Unique ID for Catalog Entries**, select the person attribute that uniquely identifies each imported person.
- [“Customizing attributes”](#) on page 68. Define all the person attributes for which you want to import values from the directory server.

1. Go to **Admin > External Servers > Directory Server**.

2. Complete the fields and map the attributes.

As a minimum, map the signin ID and the person ID.

3. Click **Save**.

The connection is verified.

4. If you did not specify a synchronization frequency, click **Sync** to import the people together with the mapped attributes.

5. Restart the StoredIQ for Legal server so that the imported people can sign in to StoredIQ for Legal.

Before you restart the StoredIQ for Legal server, wait until you are informed that the synchronization process was completed. Otherwise, not all people are imported and you must complete steps [“4”](#) on page 62 and [“5”](#) on page 62 again.

All people that are defined on the directory server are imported and added to the catalog. You can import more people or retrieve the values for new attributes later by synchronizing StoredIQ for Legal with the directory server.

The imported people have the minimum access rights that are required to respond to hold notices and interviews. To give them more rights, continue with [“Managing and assigning roles and privileges”](#) on page 76.

#### Related tasks

[Importing people](#)

## Configuring the connection to the email server

The email server is used for sending hold notices, interviews, reminders, and other notifications. Configure the connection to the email server. In addition, specify the email addresses for the notifications and the schedule for the custodian notifications.

The email server must use the SMTP protocol.

To configure the connection and the notifications, complete these steps:

1. Go to **Admin > External Servers > Email Server**.
2. Complete the fields. Then, click **Save**.

The connection is verified.

## Configuring the connection to the IBM StoredIQ server

If you want to create and manage data requests that are to be fulfilled by IBM StoredIQ, configure the connection to the IBM StoredIQ server.

IBM StoredIQ must be installed. If IBM StoredIQ is configured to use HTTPS connections, you might need to import the IBM StoredIQ certificate into the StoredIQ for Legal IBM WebSphere Application Server keystore. This is necessary if, on StoredIQ for Legal side, either a self-signed certificate is used or, for StoredIQ for Legal (VM), the certificate was not imported by using the `/siq/bin/cert_install` script. For more information, see the [“Importing the IBM StoredIQ certificate”](#) on page 63.

To configure the connection, complete these steps:

1. Go to **Admin > External Servers > StoredIQ Server**.
2. Set **Enable connection** to **Yes** and provide the following information:
  - The URL to the IBM StoredIQ application stack. Specify the fully qualified hostname or the IP address, the port number, and the path.
  - The credentials of a StoredIQ for Legal user that is defined in IBM StoredIQ with the SDK User role.

```
URL
ilgserver.example.com:9080/siq
User name:
Password:
Enable infoset link:
```

3. Optional: Set **Enable links to infosets** to **Yes**.

With this setting, links are provided to directly view returned document sets in IBM StoredIQ Insights. Enable this option only if IBM StoredIQ 7.6.0.17 or later is installed and is set up with an Elasticsearch cluster.

4. Save your settings.

The connection is verified.

## Importing the IBM StoredIQ certificate

If IBM StoredIQ is configured to use HTTPS connections, you might need to import the IBM StoredIQ certificate into the StoredIQ for Legal IBM WebSphere Application Server keystore.

If IBM StoredIQ is part of your solution and is configured to use HTTPS connections, some additional configuration steps might be necessary to ensure the two systems can connect. You must import the IBM StoredIQ certificate into the StoredIQ for Legal IBM WebSphere Application Server keystore if, on StoredIQ for Legal side, either a self-signed certificate is used or, for StoredIQ for Legal (VM), the certificate was not imported by using the `/siq/bin/cert_install` script.

To import the certificate, complete these steps:

- StoredIQ for Legal (VM):
  - a) Copy the IBM StoredIQ root certificate to the StoredIQ for Legal system:
    - a. Sign in to the IBM StoredIQ application stack as root.

b. Copy the `/etc/ssl/root.crt` file to the root directory on the StoredIQ for Legal system. Use a secure copy tool such as `scp` to do so.

b) Sign in to the StoredIQ for Legal virtual machine as the root user.

c) Run the following command:

```
docker cp root.crt ilg_sol_plugin:/opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/bin
```

d) Open the WebSphere Application Server container by running this command:

```
docker exec -it ilg_sol_plugin bash
```

e) Create a backup copy of the `/opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts` folder.

f) Navigate to the directory to which you copied the `root.crt` file:

```
cd /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/bin
```

g) To import the certificate, run the **keytool** command:

```
./keytool -importcert -alias appstack -file root.crt -keystore /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts
```

At the password prompt, enter the password for the JRE keystore (the default password is `changeit`).

Enter `y` when asked whether to trust the certificate.

- StoredIQ for Legal (Container):

All commands must be on a single continuous command line. They must not contain any line breaks. However, in the instructions, the commands might be split into multiple lines for readability.

a) Copy the IBM StoredIQ root certificate to an OpenShift client or the OpenShift master node.

b) Run the following commands:

```
CONTAINER_NAME=$(oc get pods -n siq4lopernsift -l app=ilg-sol-plugin -o name | sed "s/^.\{4\}//" )
```

```
oc cp root.crt $CONTAINER_NAME:/opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/bin
```

c) Create a backup copy of the `/opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts` folder.

```
oc exec -it $CONTAINER_NAME -- cp /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts.backup
```

d) To import the certificate, run the following command:

```
oc exec -it $CONTAINER_NAME -- /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/bin/keytool -importcert -alias appstack -file /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/bin/root.crt -keystore /opt/IBM/WebSphere/AppServer/java_1.7.1_64/jre/lib/security/cacerts
```

At the password prompt, enter the password for the JRE keystore (the default password is `changeit`).

Enter `y` when asked whether to trust the certificate.

## Registering and managing fulfillment connectors

You must set up and register a fulfillment connector before you can implement a work package fulfillment workflow with automatic fulfillment. For every fulfillment connector in use, you can monitor fulfillment jobs.

- You must have set up a fulfillment service that you can register as fulfillment connector. You develop such a service by using the IBM StoredIQ for Legal Policy Syndication SDK.
- To be able to connect your fulfillment service to StoredIQ for Legal via SSL connection, the certificate of your service must be trusted by StoredIQ for Legal. Therefore, you might need to import the certificate. For details, see [“Installing and removing custom SSL certificates for StoredIQ for Legal \(VM\)”](#) on page 47.
- You must be signed in with the **System: Manage** privilege.

To register a fulfillment connector:

1. Go to **Admin > External Servers > Fulfillment Connectors**.
2. On the **Fulfillment Connectors** page, click **Register New Fulfillment Connector**.
3. Complete the information as follows:

### **Name**

Specify a display name for the connector. The connector name can be up to 250 characters long.

### **External ID**

Specify a unique connector ID. The ID can be up to 250 characters long and can consist of a combination of any of these characters: A-Z, a-z, 0-9, underscore (\_), or a hyphen (-)

### **URL**

Specify the URL pointing to the fulfillment service endpoint, for example: `https://myserver.example.com:9080/FulfillmentService`

### **Credentials**

Specify a user name and password to authenticate to the fulfillment service if the service has implemented HTTP Basic Authentication.

### **Logging level**

Set the logging level for the connector. The available levels correspond to the standard StoredIQ for Legal logging levels as described in [“Collecting log and trace data from the GUI”](#) on page 243.

Except for the external ID, you can update these settings any time later.

4. Click **Register**

Remember to add the fulfillment connector's external ID to the Automation Connector data source attribute.

At any time, you can download the logs for a specific fulfillment connector. If you choose to unregister a fulfillment connector, you must make sure that no jobs for the connector in question are still running. Otherwise, any running job or workflow that assigns a job to this connector will be broken. Also, you must set the unregistered fulfillment connector's external ID inactive in the Automation Connector data source attribute.

### **Related concepts**

[Planning for fulfillment automation](#)

Starting with version 2.0.3.7, StoredIQ for Legal allows for full automation of fulfillment activities. A fulfillment workflow can be configured, for example, to submit the fulfillment items within a work package to a ticketing system or to other fulfillment tools that support preserving or collecting items automatically.

### **Related reference**

[Workflow services](#)

StoredIQ for Legal provides a set of built-in functions that you can use in your workflow.

## Registering and managing server discovery connectors

You must set up and register a server discovery connector before you can create data request with automatic creation of work packages. For every server discovery connector in use, you can monitor server discovery jobs.

- You must have set up a server discovery service that you can register as server discovery connector. For more information, see [“Planning for automating fulfillment item creation”](#) on page 33.
- To be able to connect your server discovery service to StoredIQ for Legal via SSL connection, the certificate of your service must be trusted by StoredIQ for Legal. Therefore, you might need to import the certificate. For details, see [“Installing and removing custom SSL certificates for StoredIQ for Legal \(VM\)”](#) on page 47.
- You must be signed in with the **System: Manage** privilege.

Instead of creating fulfillment items for a data request manually, you can use a server discovery service to have your workflow automatically create the fulfillment items, organized by work packages. A server discovery service must map data source categories to data sources, add system IDs on the server for custodians, and provide date ranges for a custodian on a data source. Such a service must be registered as a service discovery connector,

To register a server discovery connector:

1. Go to **Admin > External Servers > Server Discovery Connectors**.
2. On the **Server Discovery Connectors** page, click **Register New Server Discovery Connector**.
3. Complete the information as follows:

### **Name**

Specify a display name for the connector. The connector name can be up to 250 characters long.

### **External ID**

Specify a unique connector ID. The ID can be up to 250 characters long and can consist of a combination of any of these characters: A-Z, a-z, 0-9, underscore (\_), or a hyphen (-)

### **URL**

Specify the URL pointing to the server discovery service endpoint, for example: `https://myserver.example.com:9080/ServerDiscoveryService`

You can change the endpoint URL at any time. The change affects new and active jobs.

### **Credentials**

Specify a user name and password to authenticate to the server discovery service if the service has implemented HTTP Basic Authentication.

### **Logging level**

Set the logging level for the connector. The available levels correspond to the standard StoredIQ for Legal logging levels as described in [“Collecting log and trace data from the GUI”](#) on page 243.

### **Polling interval**

Specify in minutes how long the connector must wait before polling the job status again. You can change the polling interval at any time. However, the new value is applied only to jobs that are created after the change.

Except for the external ID, you can update these settings any time later.

4. Click **Register**

Remember to add the server discovery connector's external ID to the Automation Connector data source attribute.

At any time, you can download the logs for a specific server discovery connector. If you choose to unregister a server discovery connector, you must make sure that no jobs for the connector in question are still running. Otherwise, any running job or workflow that assigns a job to this connector will be



broken. Also, you must set the unregistered server discovery connector's external ID inactive in the Automation Connector data source attribute.

### Monitoring and managing server discovery jobs

Track the processing of server discovery jobs, basically for troubleshooting purposes.

You must be signed in with the **System: Manage** privilege.

You can get an overview of all server discovery jobs for all server discovery connectors. By monitoring the jobs, you can identify jobs that might not run as expected and remain active although they shouldn't. For example, a job might still be running although its parent workflow stopped, for example, because it ended unexpectedly or because it was canceled. In this case, you might probably want to end any active job pertaining to the stopped workflow to free resources.

However, if a connector becomes inactive, you might not need to end any server discovery jobs. End jobs only if the server discovery connector remains unresponsive.

Monitor server discovery jobs to identify and end jobs where completion is overdue.

1. You can view all server discovery jobs or just the jobs for a specific connector.
  - To view all server discovery jobs, go to the **Server Discovery Jobs** page.
  - To view a connector-specific subset of jobs, open the connector's details view by clicking its name in the list of server discovery connectors.

The server discovery jobs are listed from oldest to newest, so that you can easily identify those that did not complete in a timely manner.

2. Select one or more server discovery jobs from the list of jobs and click **End Job**.
3. Check the information in the confirmation message and click **Yes** to end the selected jobs.

## Putting the system into maintenance mode

---

To prevent users from signing in to IBM StoredIQ for Legal during maintenance, you can put the system into maintenance mode.

You must be signed in with the **System: Manage** privilege.

Put IBM StoredIQ for Legal into maintenance mode when you complete routine maintenance tasks such as applying fixes or making configuration changes or when you need investigate an issue thoroughly. When the system is in maintenance mode, only users with the **System: Manage** privilege have full access to the application. All other users are presented a **Maintenance** page after signing in; no other pages are available.

To put StoredIQ for Legal into maintenance mode, complete the following steps:

1. Go to **Admin > Maintenance**.
2. Set the **Enable maintenance mode** option to **Yes**.
3. Define a message for making the users aware that the system is under maintenance.

This message displayed on the **Maintenance** page that users without the **System: Manage** privilege see when signing in while the system is in maintenance mode. For example, you can include the start and end time of the maintenance window.

**Tip:** Signed-in users are not notified when the maintenance mode is enabled. They will see the notification only after signing out and back in again. Therefore, you might want to notify users via email or in a welcome or a global message about upcoming maintenance activities.

4. Save the settings.

Users without the **System: Manage** privilege can see only the **Maintenance** page with the configured maintenance message.

After you complete any required maintenance tasks, disable the maintenance mode again by setting the **Enable maintenance mode** option to **No**.

---

# Customizing

Attributes and jurisdictions are used throughout IBM StoredIQ for Legal. Customize them according to your needs. In addition, you can create messages that are available to all people who can sign in.

## Customizing attributes

---

Attributes define information about a person, data source, data request, fulfillment item, work package, matter, hold notice, interview, server, task, or an application. An initial set of attributes is provided for each of those objects. You can add custom attributes.

You must be signed in with the **Content settings: Manage** privilege.

The initial set of attributes cannot be deleted. However, you can edit their display names. In addition, you can change the settings for attributes of data type **Drop-down list** by adding more items or by activating or deactivating existing ones.

You can customize the attribute sets. From the set of person attributes, you can select attributes for these purposes:

- One attribute as an additional descriptor to be displayed in person selection lists, for example, when you select the attorney or paralegal for a matter or when you select the custodians that are involved in a legal hold. With this descriptor, you can clearly identify a person, especially if several people have the same name.

**Important:** If you do not select the sign-in ID, the email address, or the person ID as descriptor, complete the following task before you add custodians to a hold notice, an interview, a data box, or a data request: [“Creating the mapping for adding custodians if the descriptor is set to a special person attribute” on page 183](#). Otherwise, the descriptor is not displayed in the person selection lists.

- One or more attributes as the information that is displayed when you hover over a person's name.
- One attribute as the unique identifier for a person during the import of people and in the catalog. You determine which person attribute is to be used as unique identifier when you change the system settings. For more information, see [“Configuring system settings” on page 58](#).

You can also export or import attribute information, for example, to port your set of custom attributes from the development environment to the production environment. Or, you might need to know the internal attribute names when you create report or process definitions. These internal names are shown in the user interface, but you can also find them in the resulting JSON file in your download folder when you export the attribute mappings. The internal names of custom attributes are prefixed with `ca_`.

When you import attribute information, only new information is written to the database; existing attributes remain unchanged.

To add custom attributes, complete the following steps:

1. Go to **Admin > Attributes** and click which object to customize attributes for.
2. On the appropriate **Attributes** page, click **New Attribute**.
3. Specify a meaningful name for the attribute.

Therefore, do not create names that consist of numbers or special characters only. Attribute names that you created before V2.0.3.1 and that contain numbers or special characters can cause issues with the reporting database.

4. Select the data type to determine the format of the attribute and the type of value that can be specified. Then, click the **Settings** icon to specify the required settings.

Data type	Description	Required settings
String	A field for a string.	Specify its maximum length allowed. This value cannot exceed 32672.  After the attribute is saved, the string length cannot be changed anymore.
Number	A field for a number.	Specify the number of digits that can be entered to the right of the decimal point.  After the attribute is saved, the decimal places cannot be changed anymore.
Date	A field for a date.	Not applicable.
Date range (single)	An area for specifying a data range. It includes a <b>From</b> field and a <b>To</b> field.	Not applicable.
Date ranges (multiple)	An area for specifying several date ranges.	Not applicable.
True or false	A drop-down list to select true or false from.	Not applicable.
Drop-down list (single-select)	A drop-down list to select one item from.	Specify at least one item for selection.  More items can be added later. Existing items can be activated or deactivated.
Drop-down list (multiple-select)	A drop-down list to select more than one item from.	Specify at least one item for selection.  More items can be added later. Existing items can be activated or deactivated.
Combination box (single-select)	A drop-down list to select one item from. In addition, a field for a string. The string is visible only to the user who enters it.	Specify at least one item for selection.  More items can be added later. Existing items can be activated or deactivated.
Combination box (multiple-select)	A drop-down list to select more than one item from. In addition, a field for a string. The string is visible only to the user who enters it.	Specify at least one item for selection.  More items can be added later. Existing items can be activated or deactivated.

Data type	Description	Required settings
Object list (single-select)	A field for an object name. Depending on the setting for this attribute, the object can be a person, a matter, a data source, a data source application, or a data source server.	Select the object. A different object can be selected later.
Object list (multiple-select)	A field for a comma-separated listed of object names. Depending on the setting for this attribute, the object can be a person, a matter, a data source, a data source application, or a data source server.	Select the object. A different object can be selected later.
Radio buttons (single-select)	A list of radio buttons to select from.	Specify at least one item for selection. More items can be added later. Existing items can be activated or deactivated.
Attachment (single)	A button for adding a file.	Not applicable.
Attachments (multiple)	A button for adding more than one file.	Not applicable.

**Notes:**

- When you add custom person attributes, any attribute of data type String can be used to uniquely identify a person during the import of people and in the catalog.
- All custom matter attributes that have one of the following data types can be added as system variables to hold notice templates, hold notices, interview templates, and interviews:

- String
- Number
- Date
- True or false
- Drop-down list (single-select)
- Combination box (single-select)
- Radio buttons (single-select)

Custom hold notice or interview attributes of these data types can be added as system variables to hold notice templates and hold notices, or interview templates and interviews respectively.

- Custom task attributes can only have the data type String.
5. Check the list of new custom attributes and their settings.  
After you save them, you cannot delete custom attributes of data type **Object list (multiple-select)** and **Attachments (multiple)**. Also, you cannot delete attributes that are in use.
  6. Save the custom attributes.

## Customizing jurisdictions

Each person and data source belong to a specific jurisdiction. StoredIQ for Legal supplies a set of countries and country codes. You can add jurisdictions and activate or deactivate those that you do not need.

You must be signed in with the **Content settings: Manage** privilege.

To customize jurisdictions, complete these steps:

1. Go to **Admin > Content Settings > Jurisdiction**.
2. Click **New Jurisdiction** to specify a new name and code.  
You can also modify existing names or codes.
3. Set a jurisdiction to **Active** to make it available in the **Jurisdiction** choice list, or **Inactive** to hide it.  
You can delete jurisdictions that are not in use. If they are in use, you can only set them to **Inactive**.
4. Click **Save** to save your changes.

#### Related tasks

[Importing data by using the import API](#)

## Creating global messages

---

Your organization might want to inform all people who can sign in to StoredIQ for Legal about news or rules regarding StoredIQ for Legal, or provide customized instructions for users of the custodian portal. You can create a broadcast message, a compliance message, and custodian portal instructions. The message type determines where the information is displayed and how users are made aware of it.

You must be signed in with the **Content settings: Manage** privilege.

A *broadcast message* is designed for making people aware of product news. The people are informed about a new message with a visual cue next to the user menu. They can view the message by clicking **News** from the user menu.

A *compliance message* is designed for informing people about specific rules that they must comply with when they work with StoredIQ for Legal. The message is displayed on each GUI page.

No default texts are provided for these types of messages.

With *instructions for custodians*, you can customize the information that is displayed when custodians click **Have Questions?** in the custodian portal or in the response view of hold notices or interviews. For example, you can provide instructions for dealing with hold notice and interview messages or contact information. If you do not provide any customized text, the default instructions text provided by StoredIQ for Legal is displayed.

To create the messages, complete these steps:

1. Go to **Admin > Content Settings > Global Messages**.
2. Specify the messages, as needed.

All three types of messages are displayed or are available for viewing the next time that you sign in to, or start to work with, StoredIQ for Legal.

## Setting a welcome message

---

You can define and enable a welcome message that is displayed every time a user signs in to StoredIQ for Legal.

You must be signed in with the **Content settings: Manage** privilege.

In a *welcome message*, you can provide the information when the user last signed in and any other information that you want users to be aware of. Users see this message after they sign in. At any time later, users can view the welcome message by clicking **Welcome Message** from the user menu.

To set up the welcome message, complete these steps:

1. Go to **Admin > Content Settings > Welcome Message**.
2. Set the **Enable welcome message** option to **Yes**.
3. Define the message content.

Select at least one of these content options:

- Set the **Include last sign-in** option to **Yes** to have the welcome message shown the date and time of the user's last sign-in.

- Enter the message text for the welcome message.
4. Optional: To check what the welcome message will look like, click **Preview**.

## Configuring the person history view

---

You can configure the person history view to provide users with the option to look up the history of changes to a person's record.

You must have imported your HR history records, so that this information is available in the system. To configure the view, you must be signed in with the **Content settings: Manage** privilege.

If you select to show the person history in the user interface, this information becomes available in draft and published versions of hold notices, interviews, and data requests, and in a person's profile. For the person history, you can also configure whether certain changes trigger an automatic update to the information or whether the information must be updated by importing updated person information on a regular basis.

If you plan to enable snapshots of custodian information, take the following considerations into account:

- A person history must exist in the system before you enable snapshots.
- Snapshots are taken only for those attributes that are monitored for automatically capturing changes.
- By default, a snapshot is taken when a data request is submitted. However, you can change the point in time for taking a snapshot for each data request by changing the data request date (the value of the `drcdate` attribute) in the UI or through a workflow.

For release requests, the information when to take a snapshot is inherited from the parent preservation request. Thus, it does not correspond to the submission date of the release request. Snapshots shown for release requests equal the snapshot for the parent preservation request.

- By default, no snapshots are taken for data requests that were submitted in an earlier release of StoredIQ for Legal even if snapshots are enabled. To generate snapshots for such data requests, you must manually set a value for the `drcdate` attribute for each data request, either in the UI (which requires a change to the underlying form) or through a workflow.
- Reporting is not available for snapshots.

To configure the person history view:

1. Go to **Admin > Content Settings > Person History**.

2. Select to show the person history in the user interface.

By default, this information is not shown.

3. To have the history information automatically updated, set the **Automatically capture changes** option to **Yes**.


Then, select the attributes that trigger an update to the person history when they are changed via UI or import. Note that changes that result from ad hoc import of person information are not automatically captured.

With automatic capture of attribute changes enabled, manual cleanup of the person history is no longer possible. This is also true if automatic capture is disabled but a history of automatically captured changes already exists. Therefore, you should refrain from manually importing any person history after enabling automatic capture. A manual import would result in an inconsistent person history that you cannot clean up.

If you do not enable automatic capture of attribute changes, change history records are written only when you import updated person information by using the import API (`persondistincthistory` entries).

4. Optional: If automatic capture of attribute changes is enabled, you can also enable snapshots of custodian information.

When you enable this option, a snapshot of the initial settings of the monitored person information for a custodian in a data request is taken when the data request is submitted. Thus, any changes to these person attributes after the data request submission can easily be identified and the initial custodian

information is available throughout the lifetime of a data request. The  next to a custodian's name in the custodian list of a data request indicates such changes. When you click the icon, the custodian profile is displayed. The person information snapshots are available on the **Attributes Snapshot** page of the profile.

5. Click **Save** to save your changes.

## Setting user preferences

---

Users can customize notification and out-of-office settings, the appearance of the matter list, and filter options for and the layout of the work packages list.

Configure personal settings on the **User Preferences** page, which is available from the user menu.

- Configure which columns are displayed in the matter list.
- Configure if and when you want to be notified via email.
- Configure out-of-office settings to ensure that tasks that a list or group of users is allowed to work on cannot be assigned or reassigned to you during a specific period.
- Configure filter options and the layout of the work packages list.

Choose whether you want to allow selection of multiple data source categories for filtering the selected set of work packages. By default, the work packages can be displayed for all data source categories or for one selected category.

In addition, you can define which information is displayed in the work packages list. You can select different columns for draft, open, completed, or canceled work packages.

---

# Managing

After you deployed, configured, and customized StoredIQ for Legal, you can start working with StoredIQ for Legal.

## Managing the people to use StoredIQ for Legal

---

The people to use StoredIQ for Legal must be imported into StoredIQ for Legal. All imported people are added to the catalog, where you can edit the profiles, create groups, and define the relationship between the entries in the catalog. To give the people more rights, you must assign roles to them.

Starting with StoredIQ for Legal version 2.0.3.10, you can download people or group member information from the catalog. The resulting CSV file contains the columns that you selected for display. Note, however, that this export option is primarily intended for exporting the information for a selected set of people, that is, for a filtered people or group member list. It is not intended for downloading the information for all entries in the catalog.

### Importing people

You can import the people in your company from an LDAP-compliant directory server or by using the import API of StoredIQ for Legal. For the people who are not regular employees, you can use the ad hoc import of StoredIQ for Legal.

- [“Planning for importing people into StoredIQ for Legal” on page 21.](#)
- [“Configuring system settings” on page 58.](#) Under **Unique ID for Catalog Entries**, select the person attribute that uniquely identifies each imported person.
- Define all the person attributes for which you want to import values from the CSV file. For more information, see [“Customizing attributes” on page 68.](#)
- You must be signed in with the **People: Manage** privilege.

For information about importing people from a directory server, see [“Configuring the connection to the directory server” on page 62.](#) For information about how to use the import API, see [“Importing data by using the import API” on page 168.](#)

For an ad hoc import of people, complete one of the following tasks:

- To import people from within the catalog, go to **Catalog > People > All People** and then click **Import**.
- To import people when you create a hold notice, see [“Creating and sending hold notices” on page 94.](#)
- To import people when you create an interview, see [“Creating and sending interviews” on page 99.](#)
- To import people when you create a data request, see [“Creating data requests” on page 106.](#)

The new people are added to the catalog. They are available for use by all matters.

The imported people have the minimum access rights that are required to respond to hold notices and interviews. To give them more rights, continue with [“Managing and assigning roles and privileges” on page 76.](#)

### Editing profiles, creating relationships, and viewing a person's change records

You can edit a profile, and you can add the information that was not supplied during the import. If a person has several entries in the catalog, you can define the relationship between those entries. Starting with Fix Pack 5, you can also view the history of changes to a person's details, depending on the configuration.

- [“Planning for importing people into StoredIQ for Legal” on page 21.](#)
- [“Importing people” on page 74.](#)
- If you want to change the profile of a person that you imported from a directory server, you can change only those person attributes that are not mapped to LDAP attributes. To unmap an attribute, go to



**Admin > External Servers > Directory Server > Attribute Mapping**, or contact your system administrator.

- You must be signed in with the **People: Manage** privilege.

Complete either of the following tasks:

- To change the profile of one or more people, go to **Catalog > People > All People**, select one or more persons, and then click **Edit**.
- To create a relationship between entries that belong to one physical person, complete these steps:
  1. Select the entry that is to stay the primary entry and then click **Edit**.
  2. On the **Aliases** page of the **Edit Profile** window, click **Add** and then continue with selecting the entries that are to become aliases of the primary entry.

Only a primary entry without any aliases can become an alias. To get an overview of which entry is an alias and which one is a primary entry, make the Relationship column visible by selecting it from the

**Select columns** list .

- To view the change history for updates to a person's profile information, select a person on the **All People** page and click **Edit**.

The change history provides details about which person attribute values were changed by whom and when. This information can help you, for example, to select appropriate aliases.

Display of the change history in the user interface must be explicitly enabled by the administrator.

## Creating groups

You can create groups to make it easier to add people to a matter, a notice, an interview, a data request, or a data box.

- [“Importing people” on page 74.](#)
- You must be signed in with the **People: Manage** privilege.

Complete the steps:

1. Go to **Catalog > People > All Groups**.
2. Create the groups that you need.

## Creating test users

You can create local users to test StoredIQ for Legal before it goes into production.

- [“Planning for people and users ” on page 22.](#)
- You must be signed in with the **Users and roles: Manage** privilege.

To create a test user, complete these steps:

1. Go to **Admin > Users and Roles > Role Assignments**.
2. Click **Add Test User** to create a local user and add it to the list of users.

The **Signin ID** must comply with the following rules:

- It consists of letters (a-z, A-Z), numerals (0-9), the underscore character ( \_ ), the at symbol ( @ ), or a combination of them.
- It is unique.
- Its length is 60 characters or less.

**Tip:** Keep the length to fewer than 20 characters to avoid display problems.

- It does not start with sql, sys, or a numeral.
- It is not ilgadmin, administrator, admin, user, guest, public, local, or any SQL reserved word.

To prevent naming conflicts with LDAP users, adopt a naming convention for test users, such as `test_paralegal_1`, `test_attorney_1`, `test_dataops_1`, `test_administrator_1`, or `test_custodian_1`.

These rules are enforced when the test user signs in to StoredIQ for Legal, not at the time that you add a user.

The password of a test user cannot be specified or changed. It always defaults to the signin ID.

3. Optional: Assign roles as needed.

The test user is added to the list of users on the **Role Assignments** page and to the catalog.

**Important:** If you assigned roles to the test user, you can remove them at any time. For more information, see [“Managing and assigning roles and privileges” on page 76](#). The test user then becomes a person with limited access rights, is removed from the **Role Assignments** page, and is listed in the catalog only. However, you cannot delete a test user from StoredIQ for Legal.

## Managing and assigning roles and privileges

With a role, a person is considered a *user* in StoredIQ for Legal. Each role has specific privileges, which allow users to view and modify particular business items and to complete certain tasks. To ensure that the right people have the appropriate access to complete their tasks, you must assign one or more roles to the people. A role can be assigned to each person who can sign in to StoredIQ for Legal.

- [“Planning for people and users” on page 22](#).
- [“Importing people” on page 74](#).
- You must be signed in with the **Users and roles: Manage** privilege.

StoredIQ for Legal supplies an initial set of roles with privileges. You can assign other privileges to these roles. You can also define new roles.

The following list gives an overview of the roles that are supplied by StoredIQ for Legal:

### Attorney

Attorneys are responsible for overseeing legal responsibilities and compliance. They can only view business items, that is, matters, hold notices, interviews, data requests, and data boxes.

### Paralegal

Paralegals are the primary legal users of the product, and can work with business items. They are typically responsible for creating and managing matters, matter security, hold notices, interviews, data requests, and data boxes, and for conducting the process around them. They are usually also the point of contact for custodians, and follow up when custodians do not respond to hold notices or interviews.

### Data expert

Data experts handle data requests that they receive from StoredIQ for Legal and that are to be fulfilled by IBM StoredIQ. They typically do not sign in to StoredIQ for Legal. However, a data expert must have the same signin ID in StoredIQ for Legal and on the IBM StoredIQ server. On the IBM StoredIQ server, the data expert must have the role of a data user.

### System administrator

System administrators plan for, deploy, and configure StoredIQ for Legal and configure the integration with other systems, such as the directory server or the email server. The default system administrator is `ilgadmin`. After you use the `ilgadmin` user to initially set up StoredIQ for Legal, create new system administrators for routine administration so that their actions can be audited.

### Process administrator

Process administrators understand the domain thoroughly. They manage the people to use StoredIQ for Legal and complete all preparatory tasks required to create and manage matters and their contents and to create and view reports.

People that are not assigned a role have the minimum access that is required to respond to hold notices and interviews.

Complete one of the following tasks:

- To assign roles to people, go to **Admin > Users and Roles > Role Assignments** and click **Assign Roles**.
- To remove the roles from a user, select the user and then click **Remove**.  
The user is removed from the list and is changed back to a person with the minimum access rights. The user is not deleted from StoredIQ for Legal but remains part of the catalog.
- To create, edit, or delete roles, to assign other privileges to a role, or to view a list of users that have the same role, go to **Admin > Users and Roles > Roles and Privileges**.

**Notes:**

- You can edit and delete the roles that are supplied by StoredIQ for Legal. However, you cannot delete the system administrator. You can delete roles only if they are not assigned to a person.
- If you want to view only the list of users with the same role, the **Users and roles: View** privilege is sufficient.

**Related tasks**

[Importing data by using the import API](#)

**Roles and privileges: Overview**

StoredIQ for Legal supplies an initial set of roles with privileges, which the administrator can adapt to your needs.

The following tables describe the available privileges and show which privileges are assigned to the initial set of roles.

*Table 6. Contents-related privileges*

Privilege	Description	System Administrator	Process Administrator	Paralegal	Attorney	Data Expert
Matters: View	View the matter details. To view the contents of the matters, you must also select the view privilege for notices, interviews, and data requests.		X	X	X	X
Matters: Manage	Create regular matters. The privilege does not provide the right to make regular matters sensitive and vice versa. Update or delete any matter including sensitive matters, and change who has access to such a matter. The user must be on the core matter team, on the list of additional assignees, or, if the use of security groups is enabled, a member of the assigned security group. <b>Important:</b> As the creator of a matter, you do not have any special privileges regarding matters. To manage the contents of the matters, you must also select the manage privilege for notices, interviews, and data requests. The privilege does not provide the right to set or update a matter access key in case key-based access control is enabled.		X	X		
Matters: Close	Close matters.					
Sensitive matters: Manage	Create sensitive matters and change a matter from being regular to sensitive and vice versa. Update or delete a sensitive matter, and change who has access to such a matter. The user must also be on the core matter team or on the list of additional assignees. <b>Important:</b> As the creator of a matter, you do not have any special privileges regarding sensitive matters. This privilege includes all rights that the <b>Matters: Manage</b> privilege grants. If key-based access control is enabled, set or update matter access keys.					

Table 6. Contents-related privileges (continued)

Privilege	Description	System Administrator	Process Administrator	Paralegal	Attorney	Data Expert
Notices: View	View hold notices and their status, and create and view matter reports.		X	X	X	
Notices: Manage	Create, edit, and delete notices, and change their status.		X	X		
Interviews: View	View interviews, their status, and the returned answers.		X	X	X	
Interviews: Manage	Create, edit, and delete interviews, and change their status.		X	X		
Data boxes: View	View data boxes, their status, and their results, and approve data boxes.		X	X	X	X
Data boxes: Manage	Create and delete data boxes.		X	X		
Data requests: View	View data requests, their status, and their results, and approve data requests.		X	X	X	
Data requests: Manage	Create and delete data requests.		X	X		
Work packages: View	View work packages, their status, and their results, and approve work packages.		X	X	X	
Work packages: Manage	Refine the global details for the data requests, change the custodian priority, add data sources to custodians, edit work packages, and work on fulfillment items.  In addition to this privilege, you must be authorized, in the workflow that is associated with the data request, to complete tasks that relate to work packages and fulfillment items.		X	X		
Limited-access reports: View	View reports that contain information that should be available to specific users only, such as reports with personally identifiable information (PII).  You can then view all cross-matter reports even if they include data from sensitive matters or matters that you do not have access to.					
Workflow tasks: Manage	Manage tasks that are not assigned to you. For example, reassign tasks or change the priority of a task.					
Workflow subscribers: Manage	Subscribe to a workflow and add other users as subscribers to a workflow.					
Audit events: View	View details about the actions that were recorded. View and download all audit records in the system.					
People: View	View all people in the catalog and view groups.	X	X	X		
People: Manage	Create, edit, and delete groups of people, and edit and delete the profiles of people. Ad hoc import of people. Create relationships between entries in the catalog that belong to one person.		X			
Shared queries: Manage	Create, edit, and delete shared task queries.					

Table 7. Administration-related privileges

Privilege	Description	System administrator	Process administrator	Paralegal
Content settings: View	View matter categories, hold-notice settings, jurisdictions, data sources, forms, and templates. View and export attributes.		X	X
Content settings: Manage	Create, edit, and delete matter categories, hold-notice settings, jurisdictions, data sources, forms, and templates. Create, edit, import, and delete attributes.		X	X
Users and roles: View	View the roles and their privileges and view all users with the same role. View the security groups and the members of each security group.	X	X	
Users and roles: Manage	Assign roles to people, change the privileges of a role, and create and delete roles. Create test users. Create, edit, and delete security groups.	X	X	

Table 7. Administration-related privileges (continued)

Privilege	Description	System administrator	Process administrator	Paralegal
Workflow definitions: View	View the imported workflow definitions.		X	
Workflow definitions: Manage	Add, activate, or suspend workflow definitions.		X	
Workflow instances: Manage	View and terminate active workflow instances.			
Report definitions and resources: View	View the imported report definitions and resources.			
Report definitions and resources: Manage	Add, replace, export, delete, activate, or suspend report definitions. Add, export, or delete report resources.			
System: Manage	Define the connection to the directory server, the email server, and the IBM StoredIQ server, and edit the settings. Edit the system settings, which include enabling or disabling the use of security groups. Edit the logging settings. Manage fulfillment connectors and fulfillment jobs.	X		
Custodian-related actions across matters: Manage	Suspend and resume all hold notices and all interviews for selected custodians, conclude all interviews for selected hold notices, and release selected custodians from all hold notices.			
Global hold reminder: Manage	Create, view, edit, enable, and disable the global hold reminder. Monitor global hold reminder status.	X	X	

Table 8. API-related privileges

Privilege	Description	System administrator	Process administrator	Paralegal
Import: General	Import files to create or update people or data, except for matters. This privilege is not needed for the ad hoc import of people. To import the files, you also need the <b>Content settings: Manage</b> privilege or the <b>System: Manage</b> privilege.			
Import: Matters	Import files to create or update people or data, including regular and sensitive matters. This privilege is not needed for the ad hoc import of people. To import the files, you also need the <b>Content settings: Manage</b> privilege or the <b>System: Manage</b> privilege.			

People without a role have only the minimum access that is required to respond to hold notices and interviews.

## Managing workflows

A data request requires at least two workflows. With workflows, you can also change the way that an action is completed for matters, interviews, hold notices, and data requests.

### Managing workflow definitions

To use workflows, you must import their definitions.

- “Planning for workflows” on page 32. The workflows and the necessary roles must exist.
- You must be signed in with the **Workflow definitions: Manage** privilege.

To manage workflow definitions:

1. Go to **Admin > Workflows > Workflow Definitions**.
2. Click **Add Workflow Definition** to import an XML file that contains a new definition or a new version for an existing definition.
3. If the workflow changes the way an action is completed, select the actions that are to start the workflow. If the workflow contains the sequence of tasks to be completed for a data request and is to be started when a data request or a work package is submitted, do not select any actions.
4. Activate and suspend the workflow definition according to your needs.

If a workflow definition has more than one version, you can activate the version of your choice.

When you suspend a workflow definition that is associated with an action, the action is completed without the workflow. When you suspend a workflow that is used by a data request, the data request is completed with the suspended workflow. However, deactivate the data request templates that use the suspended workflow so that they are no longer available for selection when you create data requests.

### Managing workflow instances

Identify and terminate workflow instances whose completion is overdue.

You must be signed in with the **Workflow instances: Manage** privilege.

Sometimes, a workflow might not run as expected and remain active indefinitely. A possible cause can be a user task that is never completed because it was dynamically assigned to a user that does not exist, or any other task that does not require human intervention generates an infinite loop. To prevent such a workflow instance from locking any StoredIQ for Legal objects or cluttering your system, you can terminate it.

To terminate a workflow instance:

1. Go to **Admin > Workflows > Workflow Instances**.

The workflow instances are listed from oldest to newest, so that you can easily identify those that did not complete in a timely manner.

2. Select one or more workflow instances from the list of active instances and click **Terminate Workflow**.
3. Enter a reason for terminating the selected workflow instances and click **Terminate**.
4. Optional: Change the notification setting.

By default, users are notified of the termination of any workflow in which they participate. To avoid notifications being sent, clear the **Notify participating users** checkbox.

Any tasks associated with those workflow instances are canceled. A terminated workflow instance cannot be restarted.

## Managing matters

---

Before you can create a hold notice, an interview, a data box, or a data request, you must create their container, the matter.

### Managing security groups

If the use of security groups is enabled, each regular matter must be assigned a security group. Then, only the members of that group, the core matter team, and designated additional assignees have access.

- Read the information in [“Planning for secure matters”](#) on page 23.
- Enable the use of security groups. For details, see [“Configuring system settings”](#) on page 58.
- You must be signed in with the **Users and roles: Manage** privilege.

StoredIQ for Legal supplies a default security group that is automatically assigned to all regular matters that exist at the point when you enable the use of security groups. All users that are defined in the system at that point are members of the default security group. Consequently, users with the appropriate privileges have access to all matters that have the default security group assigned. To restrict the access, either change the default security group, or add security groups as needed and assign them accordingly.

To manage security groups, go to **Admin > Users and Roles > Security Groups**:

- Create new security groups as needed.
- Change the security groups, including the default security group, by adding or removing members.
- Rename security groups at any time as appropriate.
- If a security group is no longer used by any matter, you can also delete it.

If you attempt to delete a security group that is still assigned to a matter, you will get a corresponding error message and the security group will not be deleted.

All security groups are available for selection when you create regular matters.

#### Related tasks

[Importing data by using the import API](#)

### Creating matter categories

To make it easier for you to manage matters, you can categorize them and filter them by categories. For example, you might want to create categories for IP Related, Internal, Financial, Regulatory, and Securities.

You must be signed in with the **Content settings: Manage** privilege.

To create a matter category, complete the following steps:

1. Go to **Admin > Content Settings > Matter Categories**.
2. Create the categories that you need.
3. If you no longer need a category, you can remove it temporarily or delete it permanently.  
To remove it temporarily, drag it to the **Inactive Matter Categories** section. To delete it, it must first be removed from all the matters that use it.
4. Click **Save** to save the changes.

All active matter categories can be assigned to matters, either during matter creation or later by editing the matter details.

#### **Related tasks**

[Importing data by using the import API](#)

## **Creating matters**

Create a matter to contain all activities that pertain to a legal case.

- You must be signed in with the **Matters: Manage** privilege, or, if you want to create sensitive matters, the **Sensitive matters: Manage** privilege.

If key-based access control is enabled, the **Sensitive matters: Manage** privilege is also required for manually setting the access key for a matter.

- Check the information in “[Planning for secure matters](#)” on page 23. Depending on your security requirements, you might have to use security groups or create sensitive matters.
- If you want to assign a data expert to the matter, complete this task: [Configuring the IBM StoredIQ server connection](#).

Matters can be *regular* or *sensitive*, depending on who's allowed to access the matter. As long as the use of security groups or key-based access control is not enabled, every StoredIQ for Legal user has access to each regular matter. As soon as the use of security groups is enabled, only those users who are members of the security group that is assigned to the regular matter have access. Exception: When matters are imported by using the import API or created by a matter management system (MMS), the assigned core matter team does not necessarily have to be part of the security group assigned to the matter. In contrast, access to a sensitive matter is always restricted to the assigned core matter team and the designated additional assignees.

If key-based access control is enabled, you can also restrict access to any matter, whether it is regular or sensitive, protected by use of a security group or not, based on specific access keys.

**Important:** As the creator of a matter, you do not have any special privileges regarding matters. To be able to change the matter details later, to update the matter content, or to delete a matter, you must have the appropriate privileges and access to the matter.

For details, see “[Roles and privileges: Overview](#)” on page 77.

To create matters, complete these steps:

1. Go to **Matters** and click **New Matter**.
2. Create the matters that you need.

At any time, a user with the appropriate privileges and access rights can change the matter details and add hold notices, interviews, data boxes, and data requests to the matters.

#### **Related tasks**

[Importing data by using the import API](#)

## **Changing the matter details**

At any time after a matter is created, you can change specific matter details, such as the matter category, or the attorney and the paralegal, or you can add files to the matter. If you have the **Sensitive matters:**

**Manage** privilege, you can also make a matter sensitive, change a sensitive matter into a regular one, or set or update matter access keys.

To change matter details, you must be signed in with the **Matters: Manage** or **Sensitive matters: Manage** privilege. The right to change the matter details is further restricted as follows:

- For regular matters: If the use of security groups is enabled, you must be on the core matter team, on the list of additional assignees, or a member of the assigned security group.
- For sensitive matters: You must be on the core matter team or on the list of additional assignees.
- For both types of matters regardless of whether the use of security groups is enabled: If key-based matter access is enabled and an access key is set, your sign-in information must provide the required access key.

To change the details of a matter:

1. Go to **Matters > All Matters** and then click the name of the matter.
2. Click **Expand Details**. Change the details and add files as needed.

When you set or change a matter access key, consider that this will revoke access to the matter for any person whose sign-in information does not provide the required key.

## Closing and deleting matters

You can close a matter if all of its hold notices and interviews are closed and its data requests and data boxes are completed. You can delete a matter if it does not contain any of these business items or if they are in draft state.

You must be signed in with the **Matters: Manage** or **Sensitive matters: Manage** privilege. The right to delete a matter is further restricted as follows:

- For regular matters: If the use of security groups is enabled, you must be on the core matter team, on the list of additional assignees, or a member of the assigned security group.
- For sensitive matters: You must be on the core matter team or on the list of additional assignees.

To close or reopen a matter, you must also have the **Matters: Close** privilege.

Whether you can reopen a matter after it is closed depends on how the system is configured. The default configuration does not permit to reopen matters. If the option is enabled, you can reopen a closed matter from the **All Matters** or **Closed Matters** list or by clicking **Actions > Open** when you view that matter.

To close or delete a matter:

1. Click **Matters** and then click the matter that you want to close or delete.
2. Click **Actions > Close** or **Actions > Delete**.

By deleting a matter, you remove it physically from the StoredIQ for Legal database.

## Managing custodian-related actions across all matters

You can suspend and resume all hold notices and all interviews for selected custodians. You can conclude all interviews for selected custodians. In addition, you can release selected custodians from all hold notices.

- You must be signed in with the **Custodian-related actions across matters: Manage** privilege.
- The hold notices and interviews must already be published.

**Remember:** The custodian-related actions are completed for all matters that are available in StoredIQ for Legal, including sensitive matters and matters that were not created by you or that you have no access to.

To perform the actions, take these steps:

1. Click **Catalog > People > All People**.
2. Select the custodians and then select the appropriate action from the **More** menu.



The custodians that you suspended the hold notices and interviews for remain part of the hold notices and interviews but do not receive any further messages. However, they can respond to the messages that they received so far.

If you resumed the hold notices and interviews, the custodians that the hold notices and interviews were suspended for receive messages again according to the original schedule.

If you released custodians from the hold notices, they are removed from the hold notices. They do not receive a release notice. At any time, you can add them to the hold notices again.

If you concluded the interviews for selected custodians, these custodians cannot respond to the interviews anymore. They are not informed about the conclusion. At any time, you can add them to the interviews again.

## Viewing a person's hold obligations and involvement in matters


You might need an overview of who has hold obligations, who is involved in matters, and who is involved in which hold notices, interviews, and data requests. In particular, when an employee leaves your organization, you need to know whether this person received hold notices or has data that must be preserved. You can access all of this information on each UI page that lists people or custodians.


You completed one or more of the following tasks:

- [“Creating and sending hold notices” on page 94](#)
- [“Creating and sending interviews” on page 99](#)
- [“Creating data requests” on page 106](#)

Take these steps to view a person's involvement in matters and hold obligations:

1. Go to a UI page that lists people or custodians.  
For example, go to **Catalog > People > All People**.

The **Hold obligations** icon  indicates that a person received hold notices, or has data that must be preserved and is thus involved in requests for preserving data or for preserving and collecting data.

The **Matter involvement** icon  indicates that a person is involved in interviews or in requests for identifying data or for collecting data, or was released from a preservation or preservation and collection request. If a custodian's data is released for a completed preservation or preservation and collection request, this custodian is no longer considered to have a hold obligation with respect to this request. However, the custodian is still considered to be involved in the matter that the request belongs to.

2. Click the appropriate icon to find out more information about the matters, hold notices, interviews, and data requests that the person is involved in.

You can view this information only for matters that you have access to.

3. To save the information in a CSV file, click the **Export as CSV** icon .

## Viewing the overall status of a matter

You can get a quick overview of the status of the hold notices, data requests, and data boxes in a matter by viewing the displayed counters.

You must be signed in with the **Matters: View** privilege.

To view the overall status of a matter regarding hold notices, data requests, or data boxes:

1. On the **Matters** page, check the entries for a specific matter.

Depending on your browser window size, the layout of the matter list might be slightly different.

**Tip:** In the matter list settings of your user preferences, you can customize which charts are shown.

EX01

## Example Civil Suit

Attorney: **Athena Attorney** Paralegal: **Paige Paralegal**  
Data Expert: *Unassigned*

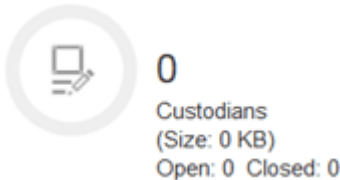
The first column in the matter list gives some basic information about the matter: matter ID and name, the assigned attorney, paralegal, and data expert, and, if applicable, the security group.

The folder icon indicates whether the matter is open or closed, and whether it's a regular or a sensitive matter.



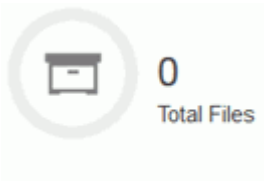
The hold notices column shows the total number of unique custodians included in the published hold notices of this matter.

The segments of the donut chart indicate the percentage of unique custodians with a specific status.



The data requests column shows the total number of unique custodians included in the data requests of this matter (regardless of the data request state), the aggregated data size of the matter's data requests, and the number of open and closed data requests.

The segments of the donut chart indicate the numbers of unique custodians per data request type. Because custodians can be included in several types of data requests, the sum of the numbers calculated for each segment might not match the total number of unique custodians.



The data boxes column shows the total number of data objects covered by the data boxes of this matter.

The segments of the donut chart indicate the number of data boxes per type, excluding closed data boxes.

2. Hover over the segments of a donut chart to display the information that you are interested in.

## Managing the global hold reminder

---

Create a global hold reminder if you want to consolidate the reminder notices that the custodians get for their hold notices.

- [“Planning for the global hold reminder”](#) on page 27.
- You must be signed in with the **Global hold reminder: Manage** privilege.

To create, activate, and update the global hold reminder, complete these steps.

1. Go to **Catalog > Global Hold Reminder**.
2. To create the global hold reminder, click **New**.
3. In the **Create Global Hold Reminder** window, specify the necessary information. Then, click **Activate** to make the global hold reminder available for use in hold notice templates and hold notices.  
If an approval workflow is associated with the activation, the global hold reminder becomes automatically active when it is approved. The approver must have the **Global hold reminder: Manage** privilege.
4. Use the **Global Hold Reminder** page to view the global hold reminder settings and the reminder status for the custodians that received hold notices that use the global hold reminder.
5. At any time, you can change the date of the next reminder on the **Overview** page.  
Then, the schedule for all future reminders and any follow-up messages is based on the new date.
6. At any time, you can update all other settings of the global hold reminder by editing a copy of the global reminder and then activating the changes. On the **Global Hold Reminder** page, click **Edit**.

### Viewing the status of global hold reminder notices

You can get a quick overview of the status of all global hold reminder notices by viewing the displayed counters.

You must be signed in with the **Global Hold Reminder: Manage** privilege.

To view the status of the global hold reminder notices, complete these steps:

1. Go to **Catalog > Global Hold Reminder**.
2. On the **Overview** page, check the counters.

Description of the statuses that are represented in the donut chart:

#### **Notified**

The number of custodians who received a global hold reminder notice.

#### **Confirmed**

The number of custodians who confirmed the latest *issuance* of a global hold reminder notice.

This status is also shown separately.

#### **Pending**

The difference between the number of notified custodians and the sum of:

- The number of custodians who already confirmed.
- The number of custodians who did not receive a global hold reminder notice because of a transmission error.
- The number of custodians whose managers were informed because they did not confirm the global hold reminder notice.

This status is also shown separately.

#### **Attention**

This counter includes:

- The number of custodians who did not receive a global hold reminder notice because of a transmission error.

- The number of custodians whose managers were informed because they did not confirm the global hold reminder notice.

This status is also shown separately.

To complement the status, the **Overview** page also informs you when the previous reminder and the previous follow-up message were sent out and when the global hold reminder was last updated.

**Note:** If transmission errors occur when a follow-up message is sent out, it can happen that the date shown does not reflect the schedule that you set for follow-up messages. Assume, for example, that a follow-up message is scheduled to be sent out every week, with the first follow-up due on 7 July 2017. Also, assume that the follow-up message is to be sent to seven custodians, where three of them are affected by transmission errors that are resolved a day later. In this case, the date of the previous follow-up message changes to 7 July when the first follow-up message is sent out for the first time. It is updated to 8 July when the transmissions are finally successful for the last three custodians. The schedule of the follow-up messages is not affected by the transmission errors. On 14 July, the second follow-up message is sent to the custodians who received their first follow-up on 7 July. On 15 July, the second follow-up message is sent to the custodians who received their first follow-up on 8 July. The date of the previous follow-up is updated each time.

## Managing templates

---

Before you can create a hold notice, interview, or data request, you must create at least one template for each of these objects. A template defines how an object is processed.

You must be signed in with the **Content settings: Manage** privilege.

### Creating hold notice templates

A hold notice template defines how a hold notice is processed.

See [“Managing the global hold reminder” on page 85](#) if you want to use the global hold reminder instead of configuring an individual reminder.

To create a hold notice template, complete these steps:

1. Go to **Catalog > Templates**.
2. Click **New Template**.
3. In the **Create Template** window, specify a unique template name.
4. Under **Type**, click **Hold notice**. Then, click **Create**.
5. If you want to prevent the creator of a hold notice to change the rules that you specify, select the **Lock the rules in hold notices that use this template** checkbox.
6. Decide whether hold notices that are based on this template can be optionally include silent custodians.

Silent custodians are on active hold but do not receive any notifications. To allow for hold notices with silent custodians, in the **Rules** section under **Initial notice**, select the **Include silent custodians** checkbox. When you create a hold notice, you must additionally enable this option at the hold notice level.

7. Decide whether a copy of the initial notice, the reminder notice, or both, can be sent to additional people, such as the managers of the custodians. Such people are not on hold and cannot respond to the hold notice. To allow for sending a copy to additional people, in the **Rules** section under **Initial notice** and under **Reminder notice**, select the **Send to courtesy copy (cc) recipients** checkbox.

The courtesy copy recipients are defined in the hold notice itself.

8. If reminder notices are to be sent out and a global hold reminder is set up, decide whether you want to use the global hold reminder or configure an individual reminder.

For more information about the global hold reminder, see [“Planning for the global hold reminder” on page 27](#).

If you use the global hold reminder, you cannot view or change the rules for, or the contents of, the reminder notices

- Under **Contents**, you can specify the subject and the contents of the hold notices and the follow-up messages, if necessary.

You can include system variables as part of the subject or the content. They are replaced with actual values when the hold notice or follow-up message is sent out. If you want the custodians to confirm the receipt of a hold notice, you must include at least one of the **Link to confirmation page** or **Link to confirmation page - no Contact me link** variables.

Custom matter and hold notice attributes with specific data types are also available as system variables. For information about the required data types, see [“Customizing attributes” on page 68](#).

Instead of typing text in the **Contents** section, you can paste text directly from any word processor or text editor. In the text to be pasted, system variables must be specified with their internal names. For more information, see [“System variables in hold notices: internal names” on page 87](#).

By using **Send Preview**, you can send copies of the messages you're currently creating to members of your team for testing, review, or information only. You can select to send all messages or just specific ones. Sending these messages does not activate the template; it remains in draft status and you can still edit it.

In activated templates, you also have the option to send copies for informational purposes. When you do so, the status of the template remains unchanged.

- Activate the template to make it available for use.

Activated templates can be duplicated only.

### System variables in hold notices: internal names

You can include system variables as part of the subject or the content of a hold notice. They are replaced with actual values when the hold notice or follow-up message is sent out. Text that you paste from a word processor or text editor must contain the internal names of the system variables.

The following table shows the internal names of the system variables that you can use in hold notices.

System variable	Internal name
{Attorney email address}	`\${matterAttorneyEmail}`
{Attorney name}	`\${matterAttorney}`
{Courtesy copy recipients}	`\${ccRecipientNames}`
{Custodian email address}	`\${custodianEmail}`
{Custodian list: email addresses}	`\${recipients}`
{Custodian list: names}	`\${recipientNames}`
{Custodian name}	`\${custodian}`
{Link to confirmation page}	`\${confirmationLink}`
{Link to confirmation page - no Contact me link}	`\${confirmationLinkWithoutContactMe}`
{Link to custodian portal}	`\${custodianPortal}`
{Matter description}	`\${matterDescription}`
{Matter ID}	`\${matterId}`
{Matter name}	`\${matterName}`
{Notice description}	`\${noticeDescription}`
{Notice name}	`\${noticeName}`
{Paralegal email address}	`\${matterParalegalEmail}`
{Paralegal name}	`\${matterParalegal}`

System variable	Internal name
{Signin ID}	#{custodianSignInId}

## Creating interview templates

An interview template defines how interview questionnaires are processed.

To create an interview template, complete these steps:

1. Go to **Catalog > Templates**.
2. Click **New Template**.
3. In the **Create Template** window, specify a unique template name.
4. Under **Type**, click **Interview**. Then, click **Create**.
5. If you want to prevent the creator of an interview to change the rules or questionnaire that you specify, select the appropriate checkbox on the **Rules and Contents** or **Questionnaire** page.
6. Under **Contents**, specify the subject and the contents of the interview and the follow-up messages, if necessary.

You can include system variables as part of the subject or the content. They are replaced with actual values when the interview or follow-up message is sent out. As a minimum, include the **Link to interview** variable in the initial interview and any recurring interview.

Custom matter and interview attributes with specific data types are also available as system variables. For information about the required data types, see [“Customizing attributes”](#) on page 68.


Instead of typing text in the **Contents** section, you can paste text directly from any word processor or text editor. In the text to be pasted, system variables must be specified with their internal names. For more information, see [“System variables in interviews: internal names”](#) on page 88.

By using **Send Preview**, you can send copies of the messages you're currently creating to members of your team for testing, review, or information only. You can select to send all messages or just specific ones. Sending these messages does not activate the template; it remains in draft status and you can still edit it.

In activated templates, you also have the option to send copies for informational purposes. When you do so, the status of the template remains unchanged.

7. On the **Questionnaire** page, create the questions and the possible answers for each question.

For each answer, you have the following additional options:

- If the paralegal must complete a follow-up action, select the **Follow-up action required** checkbox. The paralegal is informed by an email when one or more custodians select this answer.
- If an answer requires a conditional question, click the **Create a conditional question** icon . Then, complete the conditional question.
- If you want to give the custodians the possibility to provide their own answers, click **Add "Other"** instead of **Add Answer**.

**Important:** If you create dependencies between questions, be careful when you move and delete questions to not create an invalid or confusing questionnaire.

8. Activate the template to make it available for use.

Activated templates can be duplicated only.

### System variables in interviews: internal names

You can include system variables as part of the subject or the content of an interview. They are replaced with actual values when the interview or follow-up message is sent out. Text that you paste from a word processor or text editor must contain the internal names of the system variables.

The following table shows the internal names of the system variables that you can use in interviews.

System variable	Internal name
{Attorney email address}	\$_{matterAttorneyEmail}
{Attorney name}	\$_{matterAttorney}
{Custodian email address}	\$_{custodianEmail}
{Custodian list: email addresses}	\$_{recipients}
{Custodian list: names}	\$_{recipientNames}
{Custodian name}	\$_{custodian}
{Interview description}	\$_{interviewDescription}
{Interview name}	\$_{interviewName}
{Link to custodian portal}	\$_{custodianPortal}
{Link to interview}	\$_{interviewLink}
{Matter description}	\$_{matterDescription}
{Matter ID}	\$_{matterId}
{Matter name}	\$_{matterName}
{Paralegal email address}	\$_{matterParalegalEmail}
{Paralegal name}	\$_{matterParalegal}
{Signin ID}	\$_{custodianSignInId}

## Creating templates for data requests

A data request template defines how a data request is processed. The contents and the layout of a data request and the tasks involved are determined by forms. You must create the forms and the template before you can create a data request.

### Creating forms

When you create, or work on, a data request, you must specify information such as the request information or the results. You provide this information in forms.

- Define all the fields that you want to use in the form as attributes. Go to **Admin > Attributes** and check the data request attributes, fulfillment item attributes, and work package attributes. For more information, see [“Customizing attributes”](#) on page 68.
- Ensure that all data sources that contain the data of the custodians are available and active. For more information, see [“Managing data sources”](#) on page 105.

You need these forms:

- A request information form, where you enter the information that is needed to make a data request as specific as possible. The form covers the global information, which applies to all custodians for which no custom information is specified.
- A request refinement form, which is used for refining the global request information after the data request is submitted.
- A work package form, where you can change information about a work package, such as the fulfillment team.

The work to be completed for a data request is organized in work packages. A *work package* covers one data source and contains the fulfillment items for all custodians of the same priority and jurisdiction who have one or more user IDs on that data source.

- A fulfillment details form, where you can change the details for a fulfillment item, such as the fulfillment instructions.

- A fulfillment results form, where you enter the results for a fulfillment item, such as the number of items found, the size of the data, the exact location of the data.

The forms can also contain read-only fields that provide additional information to the users who complete the forms. In forms for release data requests, you might want to make most of the fields read-only.

It is not mandatory to have two forms for the request and two forms for the fulfillment item. A form can include both the request information and the request refinement. Also, a form can cover the fulfillment details and the fulfillment results.

To create a form, complete these steps:

1. Go to **Catalog > Templates**.
2. Click **New Template > Create**.
3. In the **Create Template** window, specify a unique template name.
4. Under **Type**, click **Form**. Then, click **Create**.
5. On the **Object Type** page of the **New Template** window, select the type of object that you want to create the form for.
6. The **Layout and Contents** page lists all attributes, including the custom attributes, that you defined for the selected object type. Each attribute is displayed as a field in the form. Use the middle section of the **Design** page to design the form:
  - Rearrange and delete fields as needed.
  - To redesign a field, change its settings.
  - To structure the form, add containers. Use drag to move a container and to fill it with the appropriate fields.
  - To add a deleted field, drag it from the Attributes section.
  - To preview your form, go to the **Test** page.

If you are creating a request information or request refinement form for use with data requests other than release requests, decide whether you must include the data source categories. If the workflow that is used by the data request generates a list of data source categories, no further data source categories might be needed. You decide whether the selection of data source categories in data requests is mandatory or optional when you create the data request template.

If you are creating a request information form for use with release data requests, you must include the data source categories. A request refinement form for use with release data requests does not require the data source categories to be included because those can't be modified after the request is submitted. Consider making most of the attributes read-only. You might also want to configure and include some custom attributes for release-specific information. In addition, the following considerations apply:

- If scoping release data by date range is not enabled, the data ranges must be read-only.

If you are creating a fulfillment results form for use with release data requests, make the following attributes read-only:

- resultcount (initial display name **Total Items**)
- resultsize (initial display name **Total Size**)
- resultsizeunit (initial display name **Unit**)
- otherunit\_cpx (initial display name **Other Unit**)

In addition, make sure that no default value is set for any of these read-only attributes.

- If scoping release data by date range is enabled, date ranges and the attributes resultcount, resultsize, resultsizeunit, and otherunit\_cpx should be editable.
7. To customize your form to dynamically change the layout and content based on specific settings, open the **Customization** page.

Add customizations as required. You must add a separate customization for each change that you want to make based on a condition. For example, you want a field to be displayed only under certain



conditions and, if displayed, to be required. In this case, you can add one customization that defines the condition for displaying the field and making it required. Provide the following information:

- The name of the attribute for which the customization applies. A list of attributes is available from which you can pick. The list is derived from the attributes (fields) included in the form.
- The condition on which the customization applies: select an attribute, a dependency value, and an operator. For attributes of the following data types, you can specify multiple dependency values:
  - Drop-down list (single-select)
  - Drop-down list (multiple-select)
  - Combination box (single-select)
  - Combination (multiple-select)
  - Object list (single-select)
  - Object list (multiple-select)

Attributes of the following data types cannot be specified in the **Depends On** field:

- Attachment (single)
- Attachments (multiple)
- Date range (single)
- Date ranges (multiple)

The operators = (IS) and != (IS NOT) are valid for all selectable attributes. For attributes of the data type Number, you can also pick one of these operators: < (less than), <= (less than or equal to), >= (greater than or equal to), > (greater than)

- The customized settings of any properties that are defined on the **Layout and Contents** page for an attribute in the form. For example, you can customize whether a field is hidden or read only, required, or has the specified default value on the defined condition.

While the form is in draft state, you can add or remove customizations as required.

Let's assume that you have a custom attribute for additional email information defined and want the respective field **Additional Email Information** to be displayed if the data source category is email. Also, you then want this to be mandatory information. In this case, you include the **Additional Email Information** field in the form and set it to be hidden by default. You make this configuration on the **Layout and Contents** page. Then, your customization looks like this:

<b>Attribute Name</b>	Additional Email Information
<b>Depends On</b>	Data Source Category
<b>Dependency Value</b>	Email
<b>Operator</b>	=
<b>Property</b>	hidden
<b>Property Value</b>	false
<b>Property</b>	required
<b>Property Value</b>	true

8. Optional: If the layout and contents do not meet your requirements, you can export them as a JSON file by clicking **Export Form**, edit the JSON file outside StoredIQ for Legal, and then import it again. However, ensure that all the fields that you include in the form are defined as attributes.
9. Decide whether you want to save the form as a draft or activate it.

A data request template can use forms in draft or active state. If you leave a form in draft state, you can still edit it. However, you cannot activate the templates that use it. And if you decide later to add

more fields to the form, the new fields are also available in the data request templates and data requests that use this form.

Therefore, in a production environment, activate the form so that it cannot be deleted or edited again later.

### Creating data request templates

A data request template determines which forms and workflows are used for a data request. You can create templates for an identification request, a preservation request, a collection request, a preservation and collection request, a release data request, and a deletion request.

- [Create forms](#).
- Make the necessary workflows available for use by the data request template. Complete these steps:
  1. Create the workflows and the necessary roles. For more information, see [“Planning for workflows” on page 32](#).
  2. Import the workflow definitions into StoredIQ for Legal. For more information, see [“Managing workflow definitions” on page 79](#).
  3. Activate the definitions of the workflows that are to be used.

To create a data request template, complete these steps:

1. Go to **Catalog > Templates**.
2. Click **New Template**.
3. In the **Create Template** window, specify a unique template name.
4. Under **Type**, click **Data request**. Then, click **Create**.
5. Complete the information in the **New Template** window.
6. Decide whether you want to save the template as a draft or activate it.

The template can be used by a data request even if it is in draft state. However, in a production environment, activate the template so that it cannot be deleted or edited again later. To activate the template, the forms that it uses must be active.

**Important:** If you decide to suspend a workflow that is used by an active template, deactivate the template so that is no longer available for selection when you create data requests.

### Copying templates and forms to another system

You might want to create and test templates and forms on a test system before you use them on a production system. You can export and import templates for hold notices, templates for interviews, and forms for data requests.

To export templates and forms, you must be signed in with the **Content settings: View**. To import templates and forms, you must be signed in with the **Content settings: Manage** privilege.

The template or form to export can be in draft state or be active. The template or form to import must have a unique name. You cannot overwrite an existing template or form by importing a new edition.

To copy a template or form from a test system to a production system, for example, complete these steps:

1. On the test system, go to **Catalog > Templates**.
2. Under **Hold Notice Templates**, **Interview Templates**, or **Forms**, click **Export** next to the template or form that you want to export. Save the template or form as a JSON file.
3. On the production system, go to **Catalog > Templates**.
4. Click **New Template > Import** and select the JSON file that contains the template or form to import. The imported template or form is opened.
5. Edit the template or form as needed.

If a form does not meet your requirements, you can also export its layout and contents as a JSON file by clicking **Export Form**, edit the JSON file outside StoredIQ for Legal, and then import it again. In this case, you must ensure that all the fields that you include in the form are defined as attributes.

6. Save the form as a draft or activate it.

## Managing hold notices

---

In general, a *hold notice* is a formal instruction to custodians to preserve documents and information that is relevant to a matter, and to suspend normal retention and destruction schedules.

Hold notices provide details about the nature of a matter and the information that must be preserved. The custodians who are included in a hold notice are considered on hold until a release disoblges them of the preservation requirement.

Hold notices can include active and silent custodians and courtesy copy (cc) recipients. Active custodians and cc recipients receive hold notices and any follow-up messages or reminders by email and in the custodian portal and are thus informed about their obligations. Silent custodians do not receive such notifications.

### Customizing text for hold notices

You can customize the text that prompts the custodians to respond to, and confirm, hold notices.

You must be signed in with the **Content settings: Manage** privilege.

When custodians must confirm a hold notice, they receive a notice message where they are asked to respond to the hold notice. After they click **Click to Respond**, a web page opens where they can confirm the hold notice. You can specify the text that is shown before the **Click to Respond** link in the notice message and the text that is to be shown before the **Confirm** button on the confirmation page.

To customize the text, complete these steps:

1. Go to **Admin > Content Settings > Hold Notices**.
2. Specify the text for the notice message and the confirmation page.

### Preparing hold notices for courtesy copy recipients

Hold notices are sent to the custodians who are to preserve documents and information that are relevant to a matter. However, you might want to inform more people, such as the managers of the custodians, about a hold notice by sending them a copy.

You must be signed in with the **Content settings: Manage** privilege.

When you create a hold notice template, you can decide whether the hold notices that use this template are also sent to people other than the custodians who are to be on hold. When you create a hold notice that is based on this template, you determine who is on the list of these courtesy copy recipients.

Courtesy copy recipients are not on hold and cannot respond to a hold notice. To inform them that they receive only a copy of the hold notice, a prefix is added by default to the subject of all initial notices and reminder notices that are sent to the courtesy copy recipients. You can customize the prefix by overwriting the provided default.

To change the prefix, complete these steps:

1. Go to **Admin > Content Settings > Hold Notices**.
2. Update the prefix.

It can be up to 128 characters long. You do not need to specify a separator. A colon (:) is automatically inserted as a separator when the notice is created.

If you do not want to include a prefix at all, clear the field.

Your customized prefix is automatically added to the subject of all initial notices and all reminder notices that are sent to the courtesy copy recipients, unless you decided to not include a prefix.

#### **Related tasks**

[Creating and sending hold notices](#)

Hold notices advise custodians to preserve documents and information that are pertinent to a legal case, and to suspend normal retention and destruction schedules. You can request custodians to confirm that they understand their obligations and that they comply.

## Creating and sending hold notices

Hold notices advise custodians to preserve documents and information that are pertinent to a legal case, and to suspend normal retention and destruction schedules. You can request custodians to confirm that they understand their obligations and that they comply.

- You must be signed in with the **Notices: Manage** privilege.
- Make sure StoredIQ for Legal can connect to the email server. For details, see [“Configuring the connection to the email server”](#) on page 63.
- If the selected descriptor is not the sign-in ID, the email address, or the person ID, create a custom attribute mapping. For details, see [“Creating the mapping for adding custodians if the descriptor is set to a special person attribute”](#) on page 183 and [“Customizing attributes”](#) on page 68.
- Optional: To include hold notice information beyond what's provided by the system, create custom attributes. Additions to the set of attributes become instantly available for new hold notices and hold notices in draft state.
- Review the information in [“Planning for custodian notifications”](#) on page 25.
- At least one hold notice template must be available. See [“Creating hold notice templates”](#) on page 86.
- Optional: Provide some boilerplate text that is always included in the email notification the custodian receives and on the confirmation page in the custodian portal. See [“Customizing text for hold notices”](#) on page 93.
- Optional: If you plan to include courtesy copy recipients, review the information in [“Preparing hold notices for courtesy copy recipients”](#) on page 93.

To create and send a hold notice, complete these steps:

1. On the **Matters** page, click the matter that is to contain the hold notice.
2. On the **Hold Notices** page, click **New Hold Notice**.
3. Complete the **Create Hold Notice** window, then click **Create**.
4. On the **Templates** page, select the template that best fits the hold notice that you want to create.
5. On the **Rules and Contents** page, you can change the rules according to your needs, provided that they were not locked by the user who created the template.

If the template allows for adding silent custodians, you enable this option for the hold notice. In this case, the **Silent Custodians** page becomes available.

If the global hold reminder is applied, you cannot view or change the rules for, and the contents of, the reminder notices.

6. Under **Contents**, change or specify the subject and the contents of the hold notices and the follow-up messages, as necessary.

You can include system variables as part of the subject or the content. They are replaced with actual values when the hold notice or follow-up message is sent out. If you want the custodians to confirm the receipt of a hold notice, you must include at least one of the **Link to confirmation page** or **Link to confirmation page - no Contact me link** variables.

**Tip:** Include the **Custodian list: email addresses** or **Custodian list: names** variable only in hold notices that are sent to few custodians. Otherwise, opening the hold notice in the custodian portal might take a while.

Custom matter and hold notice attributes with specific data types are also available as system variables. For information about the required data types, see [“Customizing attributes”](#) on page 68.

Instead of typing text in the **Contents** section, you can paste text directly from any word processor or text editor. In the text to be pasted, system variables must be specified with their internal names. For more information, see [“System variables in hold notices: internal names”](#) on page 87.

By using **Send Preview**, you can send copies of the messages you're currently creating to members of your team for testing, review, or information only. You can select to send all messages or specific ones. You do not publish the hold notice by sending these messages. It remains in draft status and you can still edit it.

You also have the option to send copies of the message in published hold notices by clicking **Send Copy**. When you do so, the status of the hold notice remains unchanged.

7. On the **Custodians** page, add the custodians to receive the hold notice.

You can add people who exist in StoredIQ for Legal, either by selecting them from the catalog or by adding them from a CSV file. To select people who belong to a specific department or who belonged to your company or a particular department at a specific time, you must first import the department hierarchy (target entity `orgtreehistory`), which includes a record of all changes to the hierarchy, and the employment history of the people (target entity `personhistory`). For more information, see [“Importing data by using the import API” on page 168](#).

If your system is configured to show the person history, you can look up a custodian's profile data and check which details changed at which point in time. This information can help you select the custodians to include in the hold notice.

If the hold notice is to be sent to custodians who are not regular employees and therefore are not listed in the catalog, you can import these people into StoredIQ for Legal from a CSV file. They are then added to the catalog and can be used by all matters. For more information about this ad hoc import, see [“Planning for importing people into StoredIQ for Legal” on page 21](#).

An icon indicates if a custodian is already involved in a matter or has hold obligations. For more information, see [“Viewing a person's hold obligations and involvement in matters” on page 83](#).

8. On the **Silent Custodians** page, if available, add the people that you want to be on silent hold.

These recipients are on hold but do not get any notifications. However, silent holds are reflected by the hold indicator.

Custodians who are already included in the hold notice as regular active custodians or cc recipients cannot be added as silent custodians. However, you can change the custodian type at any time. To do so, select the custodian from the list of active custodians and select **More > Change to Silent**. Likewise you can make a silent custodian an active custodian. Select the custodian from the list of silent custodians and select **More > Change to Active**. If an active custodian is also a cc recipient on the same hold notice, you must remove the custodian from the cc recipients list before you can add the custodian type as a silent custodian.

If you want people to be silent custodians who are not regular employees and therefore are not listed in the catalog, you also can import these people into StoredIQ for Legal from a CSV file.

9. On the **Courtesy Copy Recipients** page, if available, add the people to receive a copy of the hold notice.

These recipients are not on hold and cannot respond to a hold notice. Courtesy copy notifications show up in a separate section of the **Custodian Portal** page.

10. On the **Notice Information** page, add information as required.

However, the only field that is available by default is the **Comment** field. Any other fields are determined by what is defined as custom hold notice attributes.

In a published hold notice, all of this information is available in read-only format but becomes editable again when you change the published hold notice.

You can find status and version information in the notice details.

11. To send the hold notice, click **Publish**.

The exact sending time depends on the schedule that is defined for the email server. Contact your system administrator for more information.

At any time, you can view the contents of a published hold notice, its status for each custodian, and the responses from the custodians.

Even in a published hold notice, you can make a silent custodian an active custodian at any time and vice versa. If the **Include silent custodians** is already selected (either in the template on which the notice is based or in the rules for this specific hold notice), you can just use the **Change to Silent** and **Change to Active** options. If the **Include silent custodians** option is not enabled, you must modify the published hold notice accordingly and publish it again. Notifications are then started or stopped depending on how the custodian type changed.

### Related tasks

[Importing data by using the import API](#)

## Modifying published hold notices

You can modify and resend published hold notices to accommodate any new requirements.

- You must be signed in with the **Notices: Manage** privilege.
- Review the information in [“Planning for notice changes”](#) on page 31.

When you modify a published hold notice, you can change the name, the description, the rules, the content, and any additional notice information that might be included. Information about when and by whom the hold notice was last modified is included in the notice details.

To modify and, if required, resend a hold notice, follow these steps:

1. Navigate to the published hold notice that you want to change and open it.
2. Click **Actions > Modify Notice**.

You are asked to confirm this action. You can then edit the notice.

3. Optional: To modify the notice name or description, expand the details.
4. Change the rules, the content, and any notice information as required.

When you change the content of the initial notice, you might want to provide the custodians with additional information regarding the modifications. For this purpose, you can create a change message that is then prepended to the actual content of the initial notice:

- a) In the **Rules** section, select the **Include change message** option.  
This option enables the **Change Message** editor.
  - b) In the **Contents** section, navigate to **Change Message**.  
Depending on your browser window size, you might need to scroll horizontally to see the editor.
  - c) Enter a subject and any information that you want to provide.  
The subject that you enter here becomes the subject of the email notification for initial notice changes.
5. Optional: Save the changes without applying them right away.  
In this case, the icon in the hold notices list or in the notice view that indicates the notice status is changed to show that a draft version of a modified notice exists. To apply the changes, enter the edit mode again.  
In edit mode, you can also delete any changes and reset the notice to its original state until you apply the changes.
  6. To put the changes into effect, click **Apply Changes** in edit mode.  
In general, custodians are not notified of the changes. Future notifications will just reflect the changes. However, if you modified the content of the initial notice, you can choose whether to republish the notice to all active custodians or to apply the changes without notification.

**Migrated notices:** Different editors are used in IBM Atlas Policy Suite and IBM StoredIQ for Legal. Thus, some special characters are converted and the notice format changes when the message is edited in IBM StoredIQ for Legal for the first time. As a result, the notice body is considered modified and the respective publishing options are displayed when you apply the changes even if you did not make any changes to the initial notice.

After you apply the changes, notifications are sent as required and a new version of the hold notice is created. All versions and the modifications that are made to each version are tracked in the reporting

database. You can run the predefined Notice History Report to get an overview of the changes made to a specific notice. Alternatively, you can create custom reports. For more information, see [“Hold notice views” on page 136](#).

## Receiving and responding to hold notices

As a custodian, you receive the initial notice and any reminder notices by email and in the custodian portal. You might have to confirm its receipt. As a courtesy copy recipient, you receive a copy of the initial notice and any reminder notices by email and in the custodian portal. You cannot respond to them.

You must have a valid email account on the email server that is configured in the IBM StoredIQ for Legal. In addition, you must have an email application that communicates with the configured email server.

For the hold notices that are in the reminder cycle and that use the global hold reminder, one reminder notice is sent to each affected custodian and courtesy copy recipient. The reminder notice is personalized, which means that it lists only the hold notices that the custodian or courtesy copy recipient is included in and thus allowed to see. If an individual reminder is used, a reminder notice is sent out for each hold notice.

To respond to a hold notice, use either of the following procedures:

- If you start in the email application, complete these steps:
  - a) Open the email with the hold notice.
  - b) If you must confirm the receipt of the hold notice, click **Click to Respond**.
  - c) Sign in to StoredIQ for Legal.
  - d) Open the appropriate notification.
  - e) To confirm receipt of the hold notice email, click **Confirm**.  
The notification might also contain a **Contact me** link. If you want to be contacted by the StoredIQ for Legal user who sent you the hold notice, click that link.
- If you start from the custodian portal, take these steps:
  - a) Open the appropriate notification.  
For more information, see [“Managing custodian notifications” on page 120](#).  
**Important:** If the hold notice does not require confirmation, you must change to the **Done** view to see the notification.
  - b) If you must confirm the receipt of the hold notice email, click **Confirm**.  
The email might also contain a **Contact me** link. If you want to be contacted by the StoredIQ for Legal user who sent you the hold notice, click that link.

## Managing the custodians in a published hold notice

After a hold notice is published, you can add more custodians, release custodians from the hold notice, read released custodians, suspend and resume the hold notice for custodians, and confirm hold notices on behalf of selected custodians.

You must be signed in with the **Notices: Manage** privilege, and the hold notice must not be closed yet.

When you add one or more custodians, all new active custodians receive the initial notice immediately. Follow-up messages are sent to them as scheduled based on the send date of the initial notice. The reminder cycle starts only after a custodian confirms the initial notice, independently of when the custodian was added. Silent custodians do not receive any notices or follow-up messages. You can change the custodian type even after the hold notice is published. You do so by removing the custodian from either the list of active custodians or the list of silent custodians and rereading that custodian as an active or as a silent custodian. When you make a silent custodian an active custodian, this custodian is treated like a new custodian. When you make an active custodian a silent custodian, all notifications are stopped. If applicable, existing notifications are removed from the custodian portal. If an active custodian is also a cc recipient on the same hold notice, you must remove the custodian from the cc recipients list before you can change the custodian type from active to silent.

When a custodian requests to be contacted by the paralegal, the follow-up cycle is interrupted or does not even start. The paralegal has then to make sure that the custodian confirms the initial notice.

When you release custodians, they are removed from the hold notice. They do not receive a release notice but, for active custodians, their notification is removed from the custodian portal. It is possible to readd a released custodian to a hold notice. In this case, an active custodian will again receive the initial hold notice, and subsequently all follow-up or reminder messages according to the original schedule.

At any time after the initial notice is sent, the hold notice can be suspended for selected (active) custodians. In this case, the custodians remain part of the hold notice but do not receive any further messages. However, they can respond to the messages that they received so far. The hold notice can be resumed for the suspended custodians at any time. Then, they receive messages again according to the original schedule.

At any time after the initial notice is sent, you can confirm the initial notice or any reminder notices on behalf of selected (active) custodians. You can confirm even if the hold notice is suspended for these custodians.

To manage custodians in a published hold notice, complete these steps

1. On the **Matters** page, open the matter that contains the published hold notice.
2. On the **Hold Notices** page, open the published hold notice and manage the custodians as needed.

Any status updates for a custodian are reflected in the custodian's status history, which you can access through the link provided in the **Status** column.

The status in this column always reflects the custodian status for the latest issuance of the notice, which can be the initial notice, a changed notice, a reminder, or any follow-up message.

### **Related tasks**

#### Viewing a person's hold obligations and involvement in matters

You might need an overview of who has hold obligations, who is involved in matters, and who is involved in which hold notices, interviews, and data requests. In particular, when an employee leaves your organization, you need to know whether this person received hold notices or has data that must be preserved. You can access all of this information on each UI page that lists people or custodians.

## **Managing the courtesy copy recipients in a published hold notice**

After a hold notice is published, you can add more courtesy copy recipients and you can remove one or more of them.

You must be signed in with the **Notices: Manage** privilege, and the hold notice must not be closed yet.

When you add one or more courtesy copy recipients, all new recipients receive the initial notice immediately. If reminder notices are sent to courtesy copy recipients, they are sent according to the original schedule, independently of when the recipients were added.

Courtesy copy recipients who are removed are not informed. However, their notification is removed from the custodian portal. Removed courtesy copy recipients can be added to the hold notice again.

To manage courtesy copy recipients in a published hold notice, complete these steps

1. On the **Matters** page, open the matter that contains the published hold notice.
2. On the **Hold Notices** page, open the published hold notice.
3. On the **Courtesy Copy Recipients** page, manage the courtesy copy recipients as needed.

## **Viewing the status of a matter's hold notices**

You can get a quick overview of the status of all hold notices in a matter by viewing the displayed counters.

You must be signed in with the **Notices: View** privilege.

To view the status of the hold notices, complete these steps:

1. On the **Matters** page, open the matter that contains the published hold notices.
2. On the **Hold Notices** page, check the counters.



Description of the statuses that are represented in the donut chart:

**Custodians**

The number of custodians (active and silent) who are included in all hold notices.

**Pending**

The number of custodians who must confirm the latest issuance of a hold notice but have not done so yet.

**Confirmed**

The number of custodians who confirmed the latest *issuance* of a hold notice. If, for a hold notice, only the initial notice has been sent out yet, the custodians are counted who have confirmed the initial notice. If, for a hold notice, the first reminder notice has been sent out to at least one custodian, the custodians are counted who have confirmed this reminder.

The number is also incremented if the paralegal confirms on behalf of a custodian.

**Contact**

The number of custodians who clicked the **Contact me** link in the latest issuance of a hold notice.

**Attention**

This counter includes:

- The number of custodians who did not receive an initial notice or any of the reminder notices because of a transmission error.
- The number of custodians whose managers were informed because they did not confirm the initial notice or any of the reminder notices.

**Silent**

The number of silent custodians who are included in all hold notices.

**Released**

The number of active custodians who were released from any of the hold notices.

**Released - Silent**

The number of silent custodians who were released from any of the hold notices.

Description of the statuses that are shown separately:

**Confirmed**

See [“Confirmed” on page 99](#).

**Contact requested**

See [“Contact” on page 99](#).

**Attention**

See [“Attention” on page 99](#).

## Managing interviews

---

An interview is a questionnaire that is sent to one or more custodians to obtain information that pertains to legal matters.

You can send out an interview once, or repeatedly to determine whether any of the information that was returned for a prior interview, has changed in the meantime. In addition, you can define an escalation process for custodians who do not respond in a timely manner.

### Creating and sending interviews

You can create interviews to identify information that pertains to legal matters and send them to selected custodians.

- You must be signed in with the **Interviews: Manage** privilege.
- Make sure StoredIQ for Legal can connect to the email server. For details, see [“Configuring the connection to the email server” on page 63](#).

- If the selected descriptor is not the sign-in ID, the email address, or the person ID, create a custom attribute mapping. For details, see [“Creating the mapping for adding custodians if the descriptor is set to a special person attribute” on page 183](#) and [“Customizing attributes” on page 68](#).
- Review the information in [“Planning for custodian notifications” on page 25](#).
- At least one interview template must be available. See [“Creating interview templates” on page 88](#).

To create and send an interview:

1. On the **Matters** page, click the matter that is to contain the interview.
2. On the **Interviews** page, click **New Interview**.
3. Complete the **Create Interview** window, then click **Create**.
4. On the **Templates** page, select the template that best fits the interview that you want to create.
5. On the **Rules and Contents** page, you can change the rules according to your needs, provided that they were not locked by the user who created the template.
6. Under **Contents**, change the subject and the contents of the interview and the follow-up messages, if necessary, and add any missing information.

You can include system variables as part of the subject or the content. They are replaced with actual values when the interview or follow-up message is sent out. As a minimum, include the **Link to interview** variable in the initial interview and any recurring interview.

**Tip:** Include the **Custodian list: email addresses** or **Custodian list: names** variable only in interviews that are sent to few custodians. Otherwise, opening the interview in the custodian portal might take a while.

Custom matter and interview attributes with specific data types are also available as system variables. For information about the required data types, see [“Customizing attributes” on page 68](#).


Instead of typing text in the **Contents** section, you can paste text directly from any word processor or text editor. In the text to be pasted, system variables must be specified with their internal names. For more information, see [“System variables in interviews: internal names” on page 88](#).

By using **Send Preview**, you can send copies of the messages you're currently creating to members of your team for testing, review, or information only. You can select to send all messages or just specific ones. You do not publish the interview by sending these messages. It remains in draft status and you can still edit it.

You also have the option to send copies of the message in published interviews by clicking **Send Copy**. When you do so, the status of the interview remains unchanged.

7. On the **Questionnaire** page, change the questions and answers as necessary, provided that they were not locked by the user who created the template. You can also add questions and possible answers.

For each answer, you have the following additional options:

- If the paralegal must complete a follow-up action, select the **Follow-up action required** checkbox. The paralegal is informed by an email when one or more custodians select this answer.
- If an answer requires a conditional question, click the **Create a conditional question** icon . Then, complete the conditional question.
- If you want to give the custodians the possibility to provide their own answers, click **Add "Other"** instead of **Add Answer**.

**Important:** If you create dependencies between questions, be careful when you move and delete questions to not create an invalid or confusing questionnaire.

8. On the **Custodians** page, add the custodians to receive the interview.

You can add people who exist in StoredIQ for Legal, either by selecting them from the catalog or by adding them from a CSV file. To select people who belong to a specific department or who belonged to your company or a particular department at a specific time, you must first import the department hierarchy (target entity `orgtreehistory`), which includes a record of all changes to the hierarchy,

and the employment history of the people (target entity personhistory). For more information, see [“Importing data by using the import API” on page 168](#).

If your system is configured to show the person history, you can look up a custodian's profile data and check which details changed at which point in time. This information can help you select which custodians to include in the interview.

If the interview is to be sent to custodians who are not regular employees and therefore are not listed in the catalog, you can import these people into StoredIQ for Legal from a CSV file. They are then added to the catalog and can be used by all matters. For more information about this ad hoc import, see [“Planning for importing people into StoredIQ for Legal” on page 21](#).

An icon indicates if a custodian is already involved in a matter or has hold obligations. For more information, see [“Viewing a person's hold obligations and involvement in matters” on page 83](#).

**Important:** All people that you add to an interview must be able to sign in to StoredIQ for Legal.

9. To send the interview, click **Publish**.

The exact sending time depends on the schedule that is defined for the email server. Contact your system administrator for more information.

At any time, you can view its contents, its status for each custodian, and the answers from the custodians. If the answer of a custodian requires a follow-up action, the paralegal is informed and can take the appropriate action.

### **Related tasks**

[Importing data by using the import API](#)

## **Receiving and responding to interviews**

As a custodian, you receive the initial interview and any recurring interviews by email and in the custodian portal.

You must have a valid email account on the email server that is configured in the IBM StoredIQ for Legal. In addition, you must have an email application that communicates with the configured email server.

To respond to an interview, complete these steps:

1. Start with either of the following steps:

- In the email application, open the email that takes you to the interview.
- In the custodian portal, open the appropriate notification. For more information, see [“Managing custodian notifications” on page 120](#).

2. Click **Take the questionnaire**.

3. If you came from the email application, sign in to StoredIQ for Legal.

4. Complete the questionnaire.

5. Click **Submit**.

At any time, you can change your submitted answers. Complete these steps:

1. Open the questionnaire again.

2. Click **View the questionnaire**.

3. Click **Revise Answers**, change your answers, and then click **Resubmit**.

## **Managing the custodians in a published interview**

After an interview is published, you can add more custodians and suspend, resume, or conclude the interview for specific custodians.

You must be signed in with the **Interviews: Manage** privilege.

When you add one or more custodians, all new custodians receive the initial interview immediately. Follow-up messages are sent to them as scheduled based on when the initial interview was sent. The

cycle of recurring interviews starts only after a custodian has responded to the initial interview, independently of when the custodian was added.

At any time after the initial interview is sent, the interview can be suspended for selected custodians. In this case, the custodians remain part of the interview but do not receive any further messages. However, they can respond to the messages that they received so far. The interview can be resumed for the suspended custodians at any time. Then, they receive messages again according to the original schedule.

At any time after the initial interview is sent, you can conclude the interview for selected custodians. The custodians are not informed about the conclusion but their notification is removed from the custodian portal. At any time, these custodians can be added to the interview again. In this case, the custodian will again receive the initial interview, and subsequently all follow-up messages or recurring interviews according to the original schedule.

To manage custodians in a published interview, complete these steps

1. On the **Matters** page, open the matter that contains the published interview.
2. On the **Interviews** page, open the published interview and manage the custodians as needed.

### **Related tasks**

Viewing a person's hold obligations and involvement in matters

You might need an overview of who has hold obligations, who is involved in matters, and who is involved in which hold notices, interviews, and data requests. In particular, when an employee leaves your organization, you need to know whether this person received hold notices or has data that must be preserved. You can access all of this information on each UI page that lists people or custodians.

## **Viewing the status of a matter's interviews**

You can get a quick overview of the status of all interviews in a matter by viewing the displayed counters.

You must be signed in with the **Interviews: View** privilege.

To view the status of the interviews, complete these steps:

1. On the **Matters** page, open the matter that contains the published interviews.
2. On the **Interviews** page, check the counters.

Description of the statuses that are represented in the donut chart:

### **Sent**

The number of custodians who received an interview.

### **Responded**

The number of custodians who responded to the latest *issuance* of an interview. If, for an interview, only the initial interview has been sent out yet, the custodians are counted who have responded to the initial interview. If, for an interview, the first recurring interview has been sent out to at least one custodian, the custodians are counted who have responded to this interview.

This status is also shown separately.

### **Pending**

The number of custodians who must respond to the latest issuance of an interview but have not done so yet.

### **Concluded**

The number of custodians that the interview was concluded for.

### **Attention**

This counter includes:

- The number of custodians who did not receive an initial interview or any of the recurring interviews because of a transmission error.
- The number of custodians whose managers were informed because they did not respond the initial interview or any of the recurring interviews.

This status is also shown separately.

## Managing data boxes

---

A legal matter often requires the discovery of data that pertains to specific custodians. If StoredIQ for Legal can connect to an IBM StoredIQ server, you can create data requests that are fulfilled by IBM StoredIQ.

- [Configure the connection to the IBM StoredIQ server.](#)
- At least one user must be available in StoredIQ for Legal who has the Data Expert role and, as a minimum, the privilege to view data boxes.

Depending on the configuration, a link to IBM StoredIQ might be provided for the returned data. To access this information, the user must also be IBM StoredIQ user with at least the Insights User role.

Data requests to be fulfilled by IBM StoredIQ require at least one data box. A data box is a container for the requested data within a matter. Requests for identifying, collecting, and exporting data for preservation are handled under a data box.

In IBM StoredIQ, the document set that is compiled and returned for an identification request is called an *info*set.

### Configuring data locales

In data requests that are to be fulfilled by IBM StoredIQ, you must specify where the data can come from. Configure the list of data locales in your enterprise.

You must be signed in with the **Content settings: Manage** privilege.

To configure a data locale, complete the following steps:

1. Go to **Admin > Content Settings > Data Locales**.
2. Change the data locales, activate and deactivate source types, move source types, or add new data locales.

If you reconfigure the data locales after a data box is created, that data box retains the old configuration.

### Creating data boxes

You must create an identification box and a request for identifying data. When the data is available, you can change the identification box to a collection box or an export box by creating the appropriate request. The data box serves as a container for identifying, collecting, and exporting matter-relevant data.

- You must be signed in with the **Data boxes: Manage** privilege.
- [“Creating the mapping for adding custodians if the descriptor is set to a special person attribute” on page 183](#) if the selected descriptor is not the sign-in ID, the email address, or the person ID. See also [“Customizing attributes” on page 68](#).
- [“Configuring data locales” on page 103](#).

To create an identification box, complete these steps:

1. Click **Matters** and then click the matter that is to contain the data boxes.
2. On the **Data Boxes** page, click **New Data Box**.
3. Complete the **Create Data Box** window, then click **Create**.
4. On the **Request Criteria** page, describe the data to be identified.
5. On the **Custodians** page, add the custodians whose data is to be identified.

You can add people who exist in StoredIQ for Legal, either by selecting them from the catalog or by adding them from a CSV file.

6. Click **Request** to send the request to the data expert that is specified for the matter.

#### Related tasks

[Importing data by using the import API](#)

## Managing and modifying data boxes

At any time after the request for identifying data is completed, you can view the data that was returned by IBM StoredIQ, collect the data, or export it for preservation. You can request a refresh of the data and revise your request. In addition, you can run reports on a data box.

You must be signed in with the **Data boxes: Manage** privilege.

Depending on the configuration, a link might be provided to the infoset in IBM StoredIQ that corresponds to the returned document set. To access this infoset and examine the documents in more detail, you must also be a IBM StoredIQ user with at least the Insights User role. With this role, you can perform dynamic queries on the documents and preview their content and metadata .

To manage and modify a data box request:

1. Click **Matters** and then click the matter that contains the data boxes.
2. The **Data Boxes** page provides an overview of all data boxes and their status. To view the data that was returned for a request and to manage or modify a data box, open the data box.
3. Optional: If a link to IBM StoredIQ is provided, click the link to access the infoset in IBM StoredIQ Insights.

If you're not logged in to IBM StoredIQ, you are redirected to the login page. After you log in, click the link again to access the infoset.

### Refreshing the identified data

You can refresh the data in an identification box that is not closed yet.

To refresh a data box, complete these steps:

1. Open the identification box that is to be refreshed.
2. Click **Actions > Refresh**.

A new request is sent to the data expert.

### Collecting or exporting the data

You can collect the identified data or export the identified or collected data. In either case, a request is sent to the data expert. At the same time, an identification box is changed to a collection box or an export box or a collection box is changed to an export box.

To collect or export the data, complete these steps:

1. Open the data box that contains the data to be collected or exported.
2. Click **Actions > Create Collection Request** or **Actions > Create Export Request**

A request is sent to the data expert.

### Revising a data box

You can refine an identification box or collection box, or expand an identification box.

When you refine a data box, you can add search terms to the request and remove custodians. When you expand a data box, you can change the request criteria and the list of custodians. In either case, a new request is sent to the data expert. A collection box is changed back to an identification box.

To revise a data box:

1. Open the appropriate identification box or collection box.
2. Click **Actions > Revise**.
3. Decide whether you want to refine the data box or expand it.

A new request is sent to the data expert. A collection box is changed back to an identification box.

### Running reports for data boxes

You can run reports on data boxes that are in open state.

You can generate the following reports:

- CSV Infoset Data Object Export

- Data Topology Report
- Data Assessment Report
- Compliance Report
- Overlay Hit Report
- Duplication Summary Report
- Term Hit Report
- Content Collector Manifest File CSV Export
- CSV All Audited Objects Export

To run reports on a data box:

1. Go to **Matters > All Matters** and then click the matter for which you want to run reports.
2. Go to the **Data Boxes** section and from the list of data boxes, open the data box that you want to run the report for.
3. Click **Actions > Report > Create Reports**.
4. Select which reports to generate and click **Create**.

When the report is generated, a notification Reports available is displayed, and **New** is displayed next to the **Report** menu. Click **Actions > Report > View Reports** to download them.

## Closing and deleting data boxes

You can close a data box that is in open state. You can delete a data box that is in draft state.

You must be signed in with the **Data boxes: Manage** privilege.

To close or delete a data box, complete these steps:

1. On the **Matters** page, open the matter that contains the data box.
2. On the **Data Boxes** page, click **Close** or **Delete** next to the data box.

## Managing data requests

---

A legal matter often requires the discovery, preservation, or collection of data that pertains to specific custodians. At some point, data might need to be released again or deleted for cleanup. With StoredIQ for Legal, you can create data requests for each case that are fulfilled by fulfillment teams manually, automatically, or in a combination of both.

To be able to identify and further act on data, you must make the data sources known to StoredIQ for Legal. Then, you can create the data requests for acting on that data.

## Managing data sources

A *data source* describes the source of data itself and the connection information that is necessary for accessing the data. Data sources are needed to fulfill data requests. You must import the data sources from a CSV file.

- You must be signed in with the **Content settings: Manage** privilege.
- Each data source belongs to a certain jurisdiction. Ensure that all jurisdictions that are listed in the CSV file are active. For more information, see [“Customizing jurisdictions” on page 70](#).
- Each data source can be accessed by a specific group of users only, the fulfillment team. Define a role for each fulfillment team that is listed in the CSV file and assign each role the **Work packages: Manage** privilege. Use the name of the fulfillment team as role name. For more information, see [“Managing and assigning roles and privileges” on page 76](#).

To manage data sources, complete the following steps:

1. Go to **Admin > Attributes > Data Source Attributes** and complete these steps:
  - a) For the Data Source Category attribute, specify all categories that are listed in the CSV file.
  - b) For the Fulfillment Team attribute, specify all fulfillment teams that are listed in the CSV file.

c) Optional: To allow for fulfillment automation, provide one or more external IDs of registered fulfillment connectors for the Automation Connector attribute.

These entries are not validated, so make sure to enter the correct IDs. Also, make sure to maintain the list of IDs. If you unregister a connector, you must set the respective attribute value inactive. You cannot delete an entry from the list after you save it.

d) Optional: Add custom attributes as needed.

**Important:** The names of the categories and fulfillment teams are case-sensitive. Type the names exactly as they are shown in the CSV file. If the list of data source categories that are used in a data request are generated by a workflow, ensure that the workflow definition contains the correct category names.

For more information, see [“Customizing attributes” on page 68](#).

2. Import the data sources.

For more information, see [“Importing data by using the import API” on page 168](#).

3. Go to **Catalog > Data Sources** and edit and activate the data sources as needed.

Only active data sources can be used for the data requests. If you deactivate a data source, it will still be referenced in existing data requests.

If you change the data sources after one or more data requests are created, the existing data requests are not affected. The changes apply only to new data requests.

#### **Related tasks**

[Importing data by using the import API](#)

## **Creating data requests**

You can create requests for identifying, preserving, collecting, or preserving and collecting, and deleting data. In addition, you can create release data request as child requests to completed preservation, or preservation and collection requests. For more information about release data requests, see [“Releasing preserved data” on page 113](#).

- You must be signed in with the **Data requests: Manage** privilege.
- [Create the mapping for adding custodians if the descriptor is set a special person attribute](#) if the selected descriptor is not the sign-in ID, the email address, or the person ID. See also [Customize attributes](#).
- [Create data request templates](#). Create at least one template for each type of data request that you need.

To create data requests for identification, preservation, preservation and collection, or deletion of data, complete these steps:

1. Click **Matters** and then click the matter that is to contain the data requests.
2. On the **Data Requests** page, click **New Data Request**.
3. Complete the **Create Data Request** window, then click **Create**.
4. On the **Request Information** page, specify the information that helps the fulfillment team find the data that you want to have identified, preserved, collected, or deleted.
5. On the **Custodians** page, add the custodians whose data is to be searched for.

You can add people who exist in StoredIQ for Legal, either by selecting them from the catalog or by adding them from a CSV file. To select people who belong to a specific department or who belonged to your company or a particular department at a specific time, you must first import the department hierarchy (target entity orgtreehistory), which includes a record of all changes to the hierarchy, and the employment history of the people (target entity personhistory). For more information, see [“Importing data by using the import API” on page 168](#).

If your system is configured to show the person history, you can look up a custodian's profile data and check which details changed at which point in time. This information can help you make informed decisions when scoping data requests, for example, to assess whether collection of a specific custodian's data requires additional approvals.



If data is to be searched of custodians who are not regular employees and therefore are not listed in the catalog, you can import these people into StoredIQ for Legal from a CSV file. They are then added to the catalog and can be used by all matters. For more information about this ad hoc import, see [“Planning for importing people into StoredIQ for Legal” on page 21.](#)

An icon indicates if a custodian is already involved in a matter or has hold obligations. For more information, see [“Viewing a person's hold obligations and involvement in matters” on page 83.](#)

6. If the global information that you specified on the **Request Information** page does not fit all custodians, you can edit the information.

You can change the priority, date ranges, and fulfillment instructions.

If you add custodians from a CSV file, you can supply the custom information in the CSV file and skip this step. For more information, see [“Creating the mapping for overriding global information when adding custodians to a data request” on page 184.](#)

**Important:** In the GUI, dates and date ranges are displayed according to the time zone of the browser that you use to work with StoredIQ for Legal. If users are working in different time zones, it can happen that they see different dates. In data requests, date ranges are key and are, therefore, shown independent of the browser time zone. The start date and the end date include the Coordinated Universal Time (UTC) offset, which reflects the time zone where the dates were set. The UTC offset takes into account Daylight Saving Time. For example, if a user who is located in Germany specifies a date range from 13 March 2017 through 2 June 2017, all StoredIQ for Legal users see a date range similar to the following one:

2017/03/13 (UTC+01:00) - 2017/06/02 (UTC+2:00)

7. Before you click **Submit**, verify your information.

While the request is in draft state, you can change the global and the custom information. After the request is submitted, you can change only specific global information and the custodian priority. For more information about built-in attributes that cannot be changed after the data request is submitted, see [“Nonmodifiable data request attributes” on page 250.](#)

The main workflow is started, which ends when the data request is marked as complete. The next step depends on the tasks that are defined in the workflow. Typically, the data request is sent to a user for approval. At the same time, it is made available for refinement.

#### **Related tasks**

[Importing data by using the import API](#)

## **Refining data requests**

After the data request is submitted, you can refine it. Read here how to refine identification, preservation, preservation and collection, or deletion data requests. For more information about refining release data requests, see [“Refining release data requests” on page 116.](#)

You must be signed in as a user with the role that allows for refining data requests and with the **Data requests: Manage** and **Work packages: Manage** privileges.

During refinement, you can change the list of custodians and specific global request information, and you add data sources to the custodians. Some attributes cannot be changed during refinement. For more information about these attributes, see [“Nonmodifiable data request attributes” on page 250.](#)

If you decide that you no longer need the data request, you can cancel it. In this case, all of this data request's work packages are set to the state canceled. If you decide to reopen the data request, you must create new work packages.

If you use a tool or workflow that generates the fulfillment items based on the information in the data request, the fulfillment items are available and organized in work packages when you open the data request to refine. If you do not have such a tool, you must add data sources to the custodians manually or from a CSV file so that StoredIQ for Legal can generate the fulfillment items.

A work package covers one data source and contains the fulfillment items for all custodians of the same priority and jurisdiction who have one or more user IDs on that data source. By default, a work package contains one fulfillment item for each custodian. If a custodian has more than one user ID on the data

source, you can add all user IDs to one fulfillment item, or you can duplicate a fulfillment item to create one fulfillment item for each user ID.

In their user preferences, users can customize which information is displayed in the work packages list. The settings can be different for draft, open, completed, or canceled work packages.

To refine a data request, complete these steps:

1. Go to **Tasks > Unassigned Tasks** and assign the appropriate refinement task to you. Under **Objects for Review**, click the data request to refine.  
Alternatively, you can access the data request through the matter. However, after the refinement task is assigned, the data request is locked and you can only view it.
2. To change the global request information, click **Actions > Edit**.
3. Continue with either of the following tasks:
  - a) Use the tool or workflow that creates the fulfillment items directly from the submitted data request.  
To use a workflow, see [Using a workflow in IBM StoredIQ for Legal to create fulfillment items automatically](#).
  - b) If you do not have a tool or a workflow, go to the **Custodians** page and add the data sources that contain the custodians' data. You have the following options:
    - Manually add one or more data sources to one or more custodians: select the custodians and then click **Add Data Sources**. The data sources that you can choose from fit the data source categories that are specified in the request or defined in the workflow.
    - Add the data sources from a CSV file. For this option, you can use a tool that accepts custodian and data request information from a CSV file and creates a CSV file that maps the custodians to the appropriate data sources. The new CSV file can also contain details about each fulfillment item that will be created. Complete these steps:
      - 1) Click **More > Export Request Information for Custodians** to export the information about all listed custodians and the request information for each custodian as a CSV file.
      - 2) To understand which information must be in the CSV to be imported again, download the sample CSV: click **More > Add Data Sources from CSV** and then click **Download Sample CSV**. This CSV file also shows the basic set of fulfillment item attributes, which you can extend with custom attributes that you defined for fulfillment items.
      - 3) Create the CSV to be imported.
      - 4) Click **More > Add Data Sources from CSV** and select the new CSV.
4. If you decide to change the priority of a custodian after fulfillment items are created for this custodian, you have the following possibilities:
  - If the new priority is to be applied to new fulfillment items only, change the priority within the data request: click **Actions > Edit**.
  - If the new priority is also to be applied to existing fulfillment items, select the custodian on the **Custodians** page and then click **Edit Priority**. However, remember that the existing fulfillment items must be reorganized because a work package can contain custodians of the same priority only. The reorganization can take a while.
5. On the **Work Packages** page, change to the **Draft Work Packages** view. Edit or delete the work packages as necessary.  
For example, you might want to change the fulfillment team that is assigned to each work package.
6. Edit, remove, or duplicate the fulfillment items as needed.  
For example, you might want to change the fulfillment instructions or add more user IDs.
7. Submit the work packages.  
If the data request required approval, the approval task must be completed before the work packages can be submitted. Submit individual work packages by clicking **Submit** for each work package.  
Alternatively, submit all work packages at once by clicking **Submit All**.

**Tip:** You can also submit a subset of work packages by filtering the list of work packages before you click **Submit All**.

After you submit a work package, its status changes from **Draft** to **Submitted** to **Open**. How long the work package remains in status **Submitted** depends on the number of work packages that are submitted in parallel and also on the process defined in the workflow. You cannot work with a work package while it has the status **Submitted**.

8. Mark the refinement task as complete.

A workflow is started for each work package that is submitted. It ends when all fulfillment items in a work package are completed.

#### **Related tasks**

Viewing a person's hold obligations and involvement in matters

You might need an overview of who has hold obligations, who is involved in matters, and who is involved in which hold notices, interviews, and data requests. In particular, when an employee leaves your organization, you need to know whether this person received hold notices or has data that must be preserved. You can access all of this information on each UI page that lists people or custodians.

## **Fulfilling data requests**

After the work packages are submitted, fulfillment can start. Depending on your fulfillment workflow, fulfillment of the items within a work package can be completely manual, completely automatic, or a combination of automatic and manual fulfillment.

Workflows with manual fulfillment can be set up with the standard StoredIQ for Legal configuration. Fulfillment automation requires configuration and use of the IBM StoredIQ for Legal Policy Syndication Framework on the StoredIQ for Legal system and connectors built with the IBM StoredIQ for Legal Policy Syndication SDK. This software development kit (SDK) must be acquired separately.

#### **Related tasks**

Importing data by using the import API

#### **Fulfilling data requests manually**

Complete fulfillment activities by adding results manually.

- You must be signed in as a user with the role that allows for fulfilling data requests, as defined in the corresponding workflow.
- You must be a member of the fulfillment team that is associated with the work package that contains the fulfillment items.
- You must have the **Work packages: Manage** privilege.

During fulfillment, you search for the data based on the details that are provided in each fulfillment item. Then, you update each fulfillment item with your results.

For release fulfillment items, you cannot add fulfillment results from a CSV file or indicate that errors happened during fulfillment.

To complete the fulfillment items in a work package, take these steps:

1. Go to **Tasks > Unassigned Tasks** and assign the appropriate fulfillment task to you. Under **Objects for Review**, click the work package.
2. Add the results to each fulfillment item in the work package. You have the following options:
  - Open each fulfillment item and add the results. For release fulfillment items that are scoped to specific date ranges, the **Total Items** and **Total Size** fields are initially empty. If the form allows for it, you can set values. The overall number and size of completed fulfillment items in this work package are reflected at the top of the page.

After you finish adding results, click **Mark as Complete**.

- Add the fulfillment results from a CSV file. Complete these steps:
  - a. Click **Actions > Export** to export all fulfillment items in the work package as a CSV file.
  - b. In the CSV file, specify the results and status for each fulfillment item.

c. Click **Add Results from CSV** and select the updated CSV file.

This option is not available for release fulfillment items.

3. After you complete all fulfillment items in the work package, mark the fulfillment task as complete.

### Monitoring and managing fulfillment jobs

Track the processing of fulfillment jobs, basically for troubleshooting purposes.

You must be signed in with the **System: Manage** privilege.

You can get an overview of all fulfillment jobs for all fulfillment connectors in all work packages. By monitoring the jobs, you can identify jobs that might not run as expected and remain active although they shouldn't. For example, a job might still be running although its parent workflow stopped, for example, because it ended unexpectedly or because it was canceled. In this case, you might probably want to end any active job pertaining to the stopped workflow to free resources.

However, if a connector becomes inactive, you might not need to end any fulfillment jobs. End jobs only if the fulfillment connector remains unresponsive.

Monitor fulfillment jobs to identify and end jobs where completion is overdue.

1. You can view all fulfillment jobs or just the jobs for a specific connector.

- To view all fulfillment jobs, go to the **Fulfillment Jobs** page.
- To view a connector-specific subset of jobs, open the connector's details view by clicking its name in the list of fulfillment connectors.

The fulfillment jobs are listed from oldest to newest, so that you can easily identify those that did not complete in a timely manner.

2. Select one or more fulfillment jobs from the list of jobs and click **End Job**.

3. Check the information in the confirmation message and click **Yes** to end the selected jobs.

### Splitting work packages

If the work package contains many fulfillment items, fulfillment can take a long time. Therefore, you might want to divide the work among several members of the fulfillment team, or you might want to make the results of the completed fulfillment items available before continuing with the remaining fulfillment items.

- The work package to split has been submitted.
- You must be signed in with the **Work packages: Manage** privilege.
- You must be allowed to complete the fulfillment items in the work package.

You split a work package by moving one or more the fulfillment items to a new work package, which can then be worked on independently.

With automated fulfillment, a work package is locked while an automation job is running. Therefore, you cannot split the work package during an active run. However, if the workflow includes manual tasks before or after the automation job runs, you can split the work package in these tasks. If a fulfillment job ends prematurely, you can manually release the lock on the work packages and then split them to separate the completed items from the incomplete items.

To split a work package, complete these steps:

1. Open the work package and then click **Actions > Split**.
2. Select the fulfillment items to be moved to a new work package.

A work package is created with the moved fulfillment items. For the new work package, a new fulfillment workflow is started. If necessary, the new work package can be split again.

## Monitoring and managing the fulfillment of data requests

At any time during fulfillment, you can view the progress that was made for the data request, the work package, and the custodian. You can view the latest results and the errors that occurred during fulfillment

if any. In addition, you can change the custodian priority, add or remove data sources, and get an overview of all attachments associated with the data request.

To view the progress, the errors, the results, and the attachments, you must be signed in with the **Data requests: View** and **Work packages: View** privileges. To make any changes, you must be signed in with the **Data requests: Manage** and **Work packages: Manage** privileges.

To monitor or manage a data request, complete these steps:

1. Click **Matters** and then click the matter that contains the data request.
2. Go to the **Data Requests** page.

You can see some statistics about the data requests in this matter: the number custodians involved, how many data requests per type exist in the matter, the number of fulfillment items, and the amount of data that is covered by the fulfillment items. When release fulfillment items are completed, these numbers are adjusted.

3. Click the appropriate data request to view its status, the results, and the errors that might have occurred during fulfillment.

- To view this information for each custodian, go to the **Custodians** page and change to the List view.
- To view the information for each work package, go to the **Work Packages** page. The layout of the work packages list and the available filter options depend on the user preferences that you configured. With the default settings, this page initially shows the work packages of all data source categories. For a submitted data request, it's the list of open work packages. For a completed or canceled data request, it's the list of completed work packages. You can change the list by filtering on the work package status and on data source category.

To view the task comments and activities of a work package, expand the entry by clicking the work package ID. Clicking **Show Details** opens the work package details showing the task comments and activities. The information is read-only. You cannot add or delete comments or attachments here but only in the task view.

- To view task comments, attachments, and activities of the data request, go to the **Task Information** page. The **Comments** page lists all task comments and attachments. The information is read-only. You cannot add or delete comments or attachments here but only in the task view.

To display the task activities pertaining to the specific data request, go to the **Activity** page. To view comments and activities at work package level, go to the **Work Packages** page.

- To view a list of all attachments associated with the data request, go to the **Attachments** page. At a glance, you can see whether a file is attached to the data request directly or whether it is attached to a work package or a fulfillment item. The information also includes the ID of the respective data request, work package, fulfillment item, or task, the name of the field where the attachment was added, and the attachment name. Clicking the ID of any work package or fulfillment item takes you to the respective work package.

The attachment field **Task Details** is system-generated for attachments stemming from workflows; any other attribute field name is derived from the custom attributes you defined. You can download any attachment by clicking its name.

You cannot delete attachments from this view or upload attachments or other files. If an attachment is deleted in the task view, it is also removed from this list.

4. To change the custodian priority or add or remove data sources, go to the **Custodians** page.

You can change the priority of one custodian at a time but add data sources to, and remove data sources from, several custodians. Be aware of the following consequences and limitations:

- If you change the custodian priority, new work packages are created with the fulfillment items that are not yet completed. The new work packages can be completed independent of the due date for the original work packages.
- You can add data sources that you added earlier and where fulfillment started already. In this case, new fulfillment items are created.
- Data sources can be removed only if the associated work packages are not submitted yet.

## Managing negative identification results

During identification, it might turn out that a custodian does not have any data on the assigned data source. You can monitor and manage such identification results.

To customize attributes, you must be signed in as a user with the **Content settings: Manage** privilege.

To complete any tasks related to refining or fulfilling a data request, you must be signed in as a user with the **Data requests: Manage** and **Work packages: Manage** privileges.

The identification results determine whether work packages can be created and submitted:

1. The data source contains data of the custodian in the defined categories.
2. The data source contains data of the custodian but outside the defined categories.
3. The custodian is defined on the data but does not have any data there.
4. The custodian is not even defined on the data source.

Without further configuration, fulfillment items are created only for results of type 1 (*positive* identification results) because these results require actual work. However, you might want to capture results of the other types (*negative* identification results for tracking and reporting purposes. You can configure StoredIQ for Legal to create a special type of fulfillment item for such results that does not require any fulfillment activities.

To enable tracking of such cases:

1. Configure the system attribute with the internal attribute name `nodatacomment_cpx` (initial display name **No Data Comment**) according to your needs.

a) Go to **Admin > Attributes > Fulfillment Item Attributes**.

b) Navigate to the attribute with the display name **No Data Comment** and click the **Settings** icon to customize the pull-down list.

Initially, the pull-down list does not have any items. If you do not add any items, only positive identification results are handled.

You can change the display name of this attribute as required.

c) Add an item for each negative result type that you want to capture.

You can have multiple entries covering the same result type.

d) Save your changes.

After you configure this attribute, it becomes mandatory. Leaving the field empty when you add data sources indicates a positive identification result.

2. To be able to add the respective information for a fulfillment item, you must also update
3. To make the respective information available in the data request, add data sources from CSV.

You cannot add such information by adding data sources manually.

**Tip:** If you already have a custom import mapping for `fulfillment_detail` in use, you have to update this mapping. You must add a new column for the `nodatacomment_cpx` attribute. The attribute is added to the default import mapping when you configure the attribute. You can use the default mapping as a reference when you update your custom mapping.

Work packages and fulfillment items are created. For each entry that indicates a negative identification result, the created fulfillment item is marked *inactive* when the work package is submitted.

4. To check a work package for inactive fulfillment items, go to the **Work Packages** page within the data request.
  - Click the ID of the work package you are interested in. You can then filter the list of fulfillment items for inactive items.
  - Expand the work package you are interested in and check the **Status** column. If the fulfillment details form that is used in this data request contains the respective field, this view also shows the **No Data Comment** information for each fulfillment item. For a draft work package, you can also edit the information. After you submit the work package, the information is read only.

**Restriction:** You cannot update the fulfillment results for those custodians whose fulfillment status is inactive when you import fulfillment results in the task's work package view.

## Releasing preserved data

Release holds on documents after the legal obligation to preserve them is removed.

The respective system settings must be enabled.

Data under legal hold usually is preserved for long periods but at some point the legal obligation to preserve that data might be removed. In this case, you should release the data to avoid accumulating data. Preserving data unnecessarily adds to storage cost and to legal and business risk. With IBM StoredIQ for Legal, you can release data after the initial preservation data requests is closed. The following release preservation scenarios are supported:

- A *complete release* for a single data request by releasing all documents at once.
- A *partial release* for a single data request by releasing only a subset of documents while others remain in preservation state. The subset can be based on custodians, data source categories, data sources, or a combination of these. Starting with version 2.0.3.10, the scope can be further reduced by defining one or more date ranges for which the data is to be released. You can do multiple partial releases for a data request until all data is released.
- A complete release for a matter by releasing the data of all data requests within the matter, for example, when the matter is about to be closed and no more hold obligations exist.
- Partial releases for a matter by releasing data by custodian, data source category, or data source for all data requests within the matter. Starting with version 2.0.3.10, the scope of such requests can also be limited to specific date ranges.

Each completed preservation or preservation and collection request has an indicator that shows whether no, part of, or all data was released.

You can create the appropriate release data request for each of these scenarios. The general flow for release data requests is similar to that of the other data request types:

1. Create the necessary forms, workflows, and templates.

Release data requests are created from completed preservation or preservation and collection data requests. All attribute information from the original data request is available for reference. However, you can configure in your form whether any attribute information is read-only or even hidden completely. You might also want to allow for release specific comments or instructions by defining the respective custom attributes and including them in your form.

2. Create a release data request from a completed preservation or preservation and collection data request.

In a release data request, the scope of what can be edited will most probably be limited. Primarily, it will just be possible to reduce the scope of the release by removing custodians or data source categories.

Finer grained release scopes are possible if the option to allow releasing data by date range is enabled (system-wide and at the data request level). The underlying form must allow for editing the date ranges.

What other information is editable also depends on the underlying form.

3. Submit the request.

The release workflow defined in the template is started. Unlike other data requests, a release data request already has all applicable work packages defined after it is submitted. *Applicable* means that subset of the work packages in the parent preservation request covering the custodians and data source categories in the release.

All fulfillment items and work packages are represented in the release data request, even if a fulfillment item does not have preserved data associated.

4. If necessary, refine the request by further reducing the scope.

You can do so by deleting entire work packages or by deleting fulfillment items from a work package. However, you cannot remove custodians after the data request is submitted. If the respective options are enabled, you can also further reduce the scope by editing the fulfillment item date ranges.

5. Submit the work packages into the fulfillment workflow.

Release fulfillment items are tracked like any other fulfillment items, with minor differences for manual fulfillment. For more information, see [“Fulfilling data requests manually” on page 109](#).

When all fulfillment items are complete, the work package is complete. The release request can be completed only if all work packages are complete. Therefore, make sure to configure your workflow accordingly. The overall counts and size information for preservation are adjusted for each complete release data request. The original size and counts are still available at the fulfillment item level.

Release data requests show up on the matter's **Data Requests** page. If applicable, an extra **Data Requests** page listing the preservation request's child release requests is also available. In turn, a release request's **Data Requests** page shows the parent preservation request.

A custodian whose data is released for a specific preservation request is no longer considered to have a hold obligation with respect to this request. However, the custodian is still considered to be involved in the matter that the request belongs to.

### Creating release data requests

Create release data requests to release data of completed preservation or preservation and collection data requests.

- You must be signed in with the **Data requests: Manage** privilege.
- At least one release data request template must be available.
- To be able to scope release requests to date ranges, the respective option must be enabled in the system settings.

For better readability, the term *preservation request* used here refers to both preservation data requests and preservation and collection data requests.

When creating release data requests, you have these options:

- Create a release request for a single preservation request to do a complete or a partial release.
- Create multiple release requests at once for selected preservation requests within a matter to do a complete or a partial release for each of them. However, release data requests do not span preservation requests. Each release request has exactly one parent preservation request.
- Create release requests to release the data of all completed preservation requests in the matter at once.

To create release data requests:

1. Click **Matters** and then click the matter for which you want to release preserved data.
2. On the **Data Requests** page, choose one of the following options:
  - To create a release request for a single preservation request to do a complete or a partial release:
    - a. Click **Release** next to the data request for which you want to release data. Alternatively, you can open the data request and click **Actions > Release**.  
The **Release** action is available only for completed (but not canceled) preservation requests.  
You cannot create release request by clicking **New Data Request**.
    - b. In the **Create Release Data Request** window, either accept the system-generated name or specify a different unique name, select a template and change any of the other fields as required. The type is preset and cannot be changed.  
If you want to scope the release to one or more date ranges, select **Allow to release data by date ranges**.
  - c. Click **Create**.



A release data request in draft state is created in the same matter as the parent preservation request. If you accepted the system-generated name, the new data request is displayed as *Release - original\_DR\_name (n)*, where *n* is the number of the release request starting at 1. When you do partial releases, further release data requests for the parent preservation request are numbered consecutively.

- d. On the **Request Information** page, all data source categories that were used in the parent preservation request are preselected. You cannot add any data source categories but only reduce the scope of the release. To exclude data source categories from the release (partial release), clear the checkbox for any data source category that you do not want to release. The release data request will not include any work packages or fulfillment items for the excluded categories. To do a partial release by data source, you must delete the respective work packages after the release data request is submitted.

If the option to release by date range is enabled, you can edit the periods of interest. The initial values are inherited from the parent preservation request.

Adjust any other information as required.

- e. On the **Custodians** page, you can see the list of custodians that had a hold obligation in the parent preservation request and the request information for these custodians. You cannot add custodians or edit a custodian's request information.

To do a partial release, you can remove custodians, or overwrite the date ranges for selected custodians, or both. Select the custodians that you want to exclude from the release and click **Remove**. The release data request will not contain any fulfillment items for the excluded custodians. To change date ranges for specific custodians, select the custodians, click **Edit Date Ranges**, and update the date ranges as required. The release request then covers only the data in the specified date ranges.

- f. Submit the new data request. Work packages for the selected release scope are automatically created:
  - If you did not change any date ranges, the new work packages are duplicates of the corresponding work packages in the parent preservation request.
  - If you edited any date ranges, the fulfillment items in question are split and marked as subsets (the attribute `releaseChild` is set to true). The initial date range for a fulfillment item is the intersection of the fulfillment item's date range in the parent preservation request and the date range specified for the custodian in release request. You can further adjust the fulfillment item date ranges in the refine phase.

You can combine partial releases by data source categories, data sources, and custodians in one release data request. Also, you can create as many release data requests for partial releases as required until all data of the parent preservation request is released.

- To create release data requests for several completed preservation requests within a matter in one go:
  - a. Click **New Data Request > Create Multiple Release Data Requests**.
  - b. In the **Release Data Request** wizard, check and adjust the settings:
    - 1) On the **Basic** page, the name field contains a default string with several variables that ensures unique names for the release request. When the release requests are created, the variables are replaced as follows:

**`${externalId}`**

The external ID of the parent preservation request

**`${name}`**

The name of the parent preservation request

**`${count}`**

The release request count for the parent preservation request

You can change the value, for example, by adding prefixes or suffixes or by rearranging the variables but make sure to keep all variables to avoid naming conflicts.

Select a template and change any of the other fields as required. These settings are used for all release requests. The type is preset and cannot be changed.

If you want to scope the release to one or more date ranges, select **Allow to release data by date ranges**. When you do so, an additional page for editing date ranges becomes available.

- 2) On the **Data Request** page, select the preservation requests for which you want to create release requests.
- 3) On the **Custodians** page, select the custodians that you want to include in the release request. Only custodians that have fulfillment items in any of the parent preservation requests are listed.
- 4) On the **Data Sources** page, select the data sources that you want to include in the release request. Only applicable data sources are listed.
- 5) On the **Date Ranges** page (if available), edit the date ranges for all data requests that you selected in step “3.b.ii” on page 116.
- 6) On the **Review** page, you can see a summary of your selections. You can correct your choices by clicking back to the respective page and revising the selection.
- 7) When you are done, click **Create**. The release requests are created and submitted automatically.

If you edit any date ranges, the values in each release request are the date ranges that you specified during request creation. For all custodians including those who had different date ranges in the parent preservation request, the specified date ranges are set. For the fulfillment items, date ranges are the intersection of date ranges with unreleased data and the specified date ranges.

- To create release requests for all completed preservation requests:
  - a. Click **New Data Request > Release All**.
  - b. In the **Release Data Request** window, you'll see the same default string as for the **Create Multiple Release Data Requests** option. The same considerations with regard to changing the string apply.
  - c. Select a template and change any of the other fields as required. These settings are used for all release requests. The type is preset and cannot be changed.
  - d. On the **Review** page, you can see a summary of the request information.
  - e. Click **Create**. The release requests are created and submitted automatically.

After submission, you can edit a release data request and refine it, for example, by further reducing the release scope.

### Refining release data requests

Refining a release data request has several limitations compared to other data request types.

You must be signed in as a user with the role that allows for refining data requests and with the **Data requests: Manage** and **Work packages: Manage** privileges.

During refinement, you can update specific global request information and you can remove data sources. Basically, you can just reduce the scope of the release request. Depending on the configuration of the underlying form, some attributes might be read-only in addition to those attributes that are in general not editable during refinement.

A work package covers one data source and contains the fulfillment items for those custodians in the release who have the same priority and jurisdiction.

Before you can cancel a release data request, you must delete all its work packages.

To refine a data request, complete these steps:

1. Go to **Tasks > Unassigned Tasks** and assign the appropriate refinement task to you. Under **Objects for Review**, click the data request to refine.

Alternatively, you can access the data request through the matter. However, after the refinement task is assigned, the data request is locked and you can only view it.

2. To change the global request information, click **Actions > Edit**.
3. On the **Work Packages** page, change to the **Draft Work Packages** view. Edit or delete the work packages as necessary.  
For example, you might want to change the fulfillment team that is assigned to each work package.
4. Edit, remove, or duplicate the fulfillment items as needed.  
For example, you might want to change the fulfillment instructions or update custodian date ranges for the fulfillment item. Remember that editing the date ranges is possible only if the form is set up accordingly.
5. Submit the work packages.
6. Mark the refinement task as complete.

A workflow is started for each work package that is submitted. It ends when all fulfillment items in a work package are completed. Fulfilling release requests basically works the same way as for other data requests. For more information about the differences, see [“Fulfilling data requests manually” on page 109](#).

## Duplicating data requests

You might have to create data requests that are almost identical or very similar to an existing one. For this purpose, you can duplicate data requests and update the duplicates as needed.

- You must be signed in with the **Data requests: Manage** privilege.
- The data request to be duplicated can be in draft state, submitted, or completed but must be in a matter that is open. Release data requests cannot be duplicated.

The new data request will differ from the duplicated data request in the following respects:

- The new data request gets a new ID and a new creation date. In addition, it must have a new unique name, which you can specify.
- The user who duplicates the existing data request becomes the creator of the new data request.
- Attachments are not copied to the new data request.

In the duplicate, you can change all fields and add and delete custodians as needed. You can even change the data request type or the template used.

To duplicate a data request, complete these steps:

1. Click **Matters** and then click the matter that contains the data request to be duplicated.
2. On the **Data Requests** page, click **Duplicate** next to the data request to be duplicated.
3. In the **Duplicate Data Request** window, either accept the system-generated name or specify a different unique name, and change any of the other fields as required. Then, click **Duplicate**.

A data request in draft state is created in the same matter as the original data request. If you accepted the system-generated name, the new data request is displayed as *original\_DR\_name - Copy (n)* of *DR\_ID*, where *n* is the number of the copy.

When you change the template, keep in mind that only those attributes are copied that exist in the request information of both the original and the new template.









4. On the **Request Information**, adjust the request information if necessary.
5. On the **Custodians** page, you can change the list of custodians and the request information for the custodians.
6. Submit the new data request.

## Data request icons

Icons next to a data request name on the **Data Requests** page of a matter provide information about its type and its status.

When you hover over an icon, the type of data request is displayed. The icon color indicates the status of the data request. A black icon indicates that the data request is active or closed. A light grey icon is shown for draft or published data requests. The lock icon indicates that the data request is locked by a workflow. The lock icon is displayed only if you are not the assignee of the respective task.

See the following image for an illustration:

1	 (18) Preservation DR Requester: Super Star Data Source Category: Email,Bloomberg	Priority: Medium Due Date: Undefined Submission Date: 9/5/2019	<b>Complete</b> Phase
2	 (26) Release - (18) Preservation DR - (1) Requester: Super Star Data Source Category: Email,Bloomberg	Priority: High Due Date: Undefined Submission Date: -	<b>Submit Request</b> Phase
3	 (20) Prev&Collection (1) Requester: Super Star Data Source Category: Email,Bloomberg,Instant Messaging,Home Drive	Priority: Medium Due Date: Undefined Submission Date: -	<b>Submit Request</b> Phase
4	 (22) Collection Data Request Requester: Super Star Data Source Category: Email,Bloomberg,Instant Messaging,Home Drive	Priority: Medium Due Date: Undefined Submission Date: 9/5/2019	<b>Complete</b> Phase
5	 (23) Identification DR-01 Requester: Super Star Data Source Category: Bloomberg,Home Drive,Business Transactions	Priority: Medium Due Date: Undefined Submission Date: 9/5/2019	<b>Complete (Cancel)</b> Phase
6	 (24) Identification DR-03 Requester: Super Star Data Source Category: Bloomberg,Home Drive,Business Transactions	Priority: Medium Due Date: Undefined Submission Date: 9/5/2019	<b>Refine Request</b> Phase
7	 (25) Identification DR-04 Requester: Super Star Data Source Category: Bloomberg,Home Drive,Business Transactions	Priority: Medium Due Date: Undefined Submission Date: 9/5/2019	<b>Manage &amp; Monitor</b> Phase
8	 (21) DR for Deletion Requester: Super Star Data Source Category: Bloomberg	Priority: Low Due Date: Undefined Submission Date: 9/5/2019	<b>Submit Request</b> Phase

- 1 A completed preservation request
- 2 A release request in draft state
- 3 A preservation and collection request in draft state
- 4 A completed collection request
- 5 A canceled identification request
- 6 A published locked identification request
- 7 An active identification request that is locked
- 8 A deletion request in draft state

## Managing tasks

You can view the tasks that you own, that can be assigned to you, and that you assigned or reassigned to another user. If you have the **Workflow subscribers: Manage** privilege, you can subscribe to a workflow. Then, you can also see the tasks that are defined for this workflow. However, you can work only on tasks that you own.

If you are the only assignee for a task, you automatically own this task and you must complete, approve, or reject it depending on the action required. You cannot give it to another user.

If you belong to a list or group of users who is allowed to work on a task, you must explicitly assign the task to yourself to be able to work on it. At any time, you can reassign it to another user in the list or group, or you can return it so that another user in the list or group can take it. Like all tasks that do not currently have an owner, a returned task is considered an unassigned task.

If you have the **Workflow tasks: Manage** privilege, you can supervise the tasks of all users and reassign or reprioritize tasks as you see fit.

You can transfer tasks (assign, reassign, return) one by one or multiple tasks at once.

To manage tasks, complete the following steps:

1. Click **Tasks**.

The **My Tasks** page shows how many tasks are due within the next seven days, how many tasks are new, and how many tasks are still unassigned. The page also lists any tasks that are assigned to you but not yet completed. You can also filter the tasks:

**Unassigned Tasks**

All tasks that you can assign to yourself to work on

**Sent Tasks**

All tasks that you assigned or reassigned to another user

**Completed Tasks**

All tasks that you completed

**Canceled Tasks**

All tasks that you canceled

**Active Tasks**

All active tasks that already are or can be assigned to you

**All Tasks**

All tasks independent of their status

You can customize the information that is shown in the task list by selecting or deselecting task attributes. Any user with the **Content Settings: Manage** privilege can customize the set of task attributes.

You can narrow the task list by searching for a specific keyword. To build and manage more sophisticated queries, use **Advanced Search**:

- Add fields for searching on custom attributes to the existing search form.
- Save queries that you run often with a descriptive name. If you are signed in as a user with the **Shared queries: Manage** privilege, you can select to share your query with others. Shared queries are available to all co-workers.
- To run or delete a saved query, click **Manage Saved Queries** and select a private or a shared query.

2. Assign, reassign, or return tasks.

Assigning tasks to an assignee candidate or reassigning tasks require you to enter a reason.

- Work with a single task.

Select the task, then click **Assign to Me** to assign the task to yourself or click **Change Assignee** to transfer or return the task. To transfer the task, select a new assignee. To return the task, make sure the **New assignee** field is empty. Then, click **Assign**.

- Work with multiple tasks.

While you can selectively pick from the tasks in the current view, filtering the list to create a selected set of tasks is probably the better option when the list is large. To select all tasks for transfer, you can select the first task and then drag your mouse pointer down to the last task that you want to include. Alternatively, you can select the first task, and then press Shift and click the last task in the list. A **Select All** checkbox is available if the number of tasks does not exceed the maximum number of items that can be displayed on the page.

After you pick the tasks, you have several options depending on the current assignee:

- Assign the tasks to yourself by clicking **Assign to Me**.
  - Transfer the tasks by clicking **Change Assignee**. The list of possible new assignees to pick from shows only those candidates who have the appropriate permissions for all tasks in the list. Select the new assignee and click **Assign**.
  - Return tasks by clicking **Return**.
3. To ensure that tasks that a list or group of users is allowed to work on, cannot be assigned or reassigned to you during a specific period, you must configure your out-of-office settings: Click **User Preferences** from your user menu and go to **Out-of-Office Settings**.
- After your settings are enabled, your name no longer appears in the list of possible assignees during the specified period.

## Managing notifications

---

Notifications are sent out when hold notices and interviews are published, when custodian-related or task-related changes are made, or when system-related problems occur. Some notifications are sent automatically while others are sent on request only.

- [“Configuring the connection to the email server” on page 63](#).
- All users who receive notifications must have a valid email account on the email server. In addition, they must have an email application that communicates with the configured email server.

StoredIQ for Legal supports the following type of notifications:

### Managing custodian notifications

When a hold notice or an interview is published or a reminder is sent out, all affected custodians and any courtesy copy (cc) recipients are notified by an email and in the custodian portal. A custodian can respond to a hold notice or an interview directly from the email application or the custodian portal.

The custodian portal shows only those notifications that you are allowed to view. To see notifications regarding a hold notice, you must have been explicitly added as an active custodian or as a courtesy copy recipient to the hold notice. Silent custodians do not receive any notifications. To see notifications regarding an interview, you must have been explicitly added as a custodian to the interview.

The custodian portal contains only active notifications. This means that if an active custodian is released from a hold notice, a courtesy copy recipient is removed from a hold notice, or an interview is concluded, the appropriate notification is also removed from the custodian portal.

The subject of notifications that are sent to courtesy copy recipients can be preceded by a prefix, where FYI: is the default prefix.

You can also access the custodian portal from your tablet device. However, there are certain limitations:

- Supported devices are the Apple iPad tablet computer and the Apple iPhone 8 mobile phone.
- The only supported browser is Safari iOS.
- For the tablet computer, the layout is optimized for horizontal orientation. For the mobile phone, it is optimized for vertical orientation.
- File operations:
  - Only a limited set of file operations is available on the mobile devices.
  - Attachments might open in a separate browser tab, and you cannot save them as a file.
  - Some file types, such as ZIP, allow for saving the file to local storage or to Apple iCloud Drive.
- Only a subset of the activities that are triggered by hover UI events, such as hover help, work.
- List scrolling: Momentum scroll is not supported. Therefore, swiping does not keep the list scrolling; as soon as your finger leaves the screen, scrolling stops. This also applies to bounce scrolling.

### Related concepts

[Planning for custodian notifications](#)

## Related tasks

### Preparing hold notices for courtesy copy recipients

Hold notices are sent to the custodians who are to preserve documents and information that are relevant to a matter. However, you might want to inform more people, such as the managers of the custodians, about a hold notice by sending them a copy.

### Receiving and responding to hold notices

As a custodian, you receive the initial notice and any reminder notices by email and in the custodian portal. You might have to confirm its receipt. As a courtesy copy recipient, you receive a copy of the initial notice and any reminder notices by email and in the custodian portal. You cannot respond to them.

### Receiving and responding to interviews

As a custodian, you receive the initial interview and any recurring interviews by email and in the custodian portal.

## Managing alert notifications

Paralegals are automatically informed about custodian-related changes in matters that they are responsible for or when an interview response requires follow-up actions. Users who are involved in tasks can be informed about task-related changes. For some changes, they receive an automatic notification while for other changes they must request a notification.

When a change occurs, an alert notification is sent immediately, except for changes that are summarized in a report. For summarized changes, a notification is sent once a day.

The following table provides an overview of the notifications that are sent automatically.

Change prompting the notification	Users who are informed	Notification
The priority of a custodian in a data request changes.	<ul style="list-style-type: none"><li>• Task assignee</li><li>• Assignee candidates</li><li>• Task subscribers</li></ul>	Immediately
A custodian is removed from a data request.	<ul style="list-style-type: none"><li>• Task assignee</li><li>• Assignee candidates</li><li>• Task subscribers</li></ul>	Immediately
A data request is canceled.	<ul style="list-style-type: none"><li>• Assignees of all active or completed tasks</li><li>• Task subscribers</li></ul>	Immediately
A workflow instance is terminated.	<ul style="list-style-type: none"><li>• Task assignee</li><li>• Assignee candidates</li><li>• Task subscribers</li></ul>	Immediately
The employment status of one or more custodians in a matter changes.	Paralegals of the matters that contain at least one of the affected custodians	Once a day
An interview response requires a follow-up action.	Paralegal of the affected matter	Once a day

To request a notification on specific task-related changes, complete the following steps:

1. Click **User Preferences** from your user menu and then go to **Notification Settings**.
2. Specify which users are to be informed about which task changes.

The following table provides an overview of the changes that prompt a notification, of the users who can be informed, and of the user preference setting that is necessary for a notification.

<b>Change prompting the notification</b>	<b>Users who can be informed</b>	<b>User preference setting</b>	<b>Notification</b>
A task is claimed.	Task subscribers	Assignee is changed	Immediately
A task is assigned.	<ul style="list-style-type: none"> <li>• Task assignee</li> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	Assignee is changed	Immediately
A task is returned.	<ul style="list-style-type: none"> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	Assignee is changed	Immediately
A comment is added to a task.	<ul style="list-style-type: none"> <li>• Task assignee</li> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	New comment is added	Immediately
The task priority or the task due date is changed.	<ul style="list-style-type: none"> <li>• Task assignee</li> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	Priority or due date is changed	Immediately
A subscriber is added to a task or is removed from a task.	<ul style="list-style-type: none"> <li>• Task assignee</li> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	Subscriber is added or removed	Immediately
A task is completed.	<ul style="list-style-type: none"> <li>• Task assignee</li> <li>• Task assigner</li> <li>• Task subscribers</li> <li>• Manager of task assignee</li> </ul>	Task is completed	Immediately
The task due date approaches.	Task assignee	Email me when one of my tasks is due within <i>number</i> days	Immediately

Except for the managers, all of the users listed receive notifications by default. To inform the managers, you must explicitly select them.



## Managing system notifications

When a system-related problem occurs that requires immediate attention, such as when a workflow ends abnormally, the administrator receives a system notification.

To view a system notification, open it in your email application.

## Creating and viewing reports

---

Reports can be run automatically or on request. They can include data from one matter or from more than one matter.

Review the information in [“Planning for reports”](#) on page 35.

Scheduled reports, which run automatically, are generated sequentially after the reporting database was refreshed. You can schedule a refresh to happen up to four times a day. For more information, see [“Configuring system settings”](#) on page 58.

Reports that do not run automatically can be requested at any time. If several reports are requested at the same time, they are generated sequentially. However, requested reports and scheduled reports can run at the same time.

Large reports can impact the performance of the system. If you have many large reports, keep in mind:

- Schedule large reports so that they are generated only after a report database refresh. Scheduled reports can be viewed by all users with the privileges that are specified in the report definition or with the **Limited-access reports: View** privilege. If key-based access control is enabled, access to such a report can be limited to users with a specific key in their sign-in information. Such a restriction, for example, to one or more location keys, is specified in the report definition.
- Reduce the run frequency of the reports in the system settings.
- Do not generate scheduled reports on an ad hoc basis by using the **Run Now** button in the system settings.
- For reports that include more than 100,000 rows, use CSV as output format. Generating reports in PDF or HTML format consumes more system resources.
- If a report includes more than 1,000,000 records, design the report such that the user who requests the report is prompted for filtering information. For example, if a report is to contain fulfillment items, you might want to prompt the user for a start date and an end date.

When date and time values are stored in the reporting database, they are converted to Coordinated Universal Time (UTC), where the time stamp includes the respective UTC offset. Thus, date and time values are automatically converted to the local date and time (per the client time zone) at display time.

To convert time stamps in your reports to any other time zone, use the `AT TIME ZONE timezone` construct in your SQL query. For example, to create output with all creation dates in the `appauditworkflow` table converted to California time, Pacific Daylight Saving Time (PDT), use the following SELECT statement:

```
SELECT creationdate AT TIME ZONE 'PDT' AS creationdate_pdt FROM appauditworkflow;
```

The resulting column named `creationdate_pdt` contains the creation dates in PDT regardless of the time zones defined in the StoredIQ for Legal server or the respective SQL client.

## Managing report definitions and resources

Manage the definitions of the predefined reports, which StoredIQ for Legal supplies, and of any custom reports. Also, manage the resources that your custom reports are to share.

You must be signed in with the **Report definitions: Manage** privilege.

Under **Admin > Reports**, you can find all report definitions and report resources that are available in StoredIQ for Legal.

## Managing report definitions

You can suspend, activate, edit, and delete the definitions of the predefined reports as needed. To create custom reports, you must import the appropriate report definitions and prepare StoredIQ for Legal for these reports.

If the reports are to include custom attributes, add these attributes. For more information, see [“Customizing attributes”](#) on page 68.

You can suspend, activate, and delete the report definitions that StoredIQ for Legal supplies. Except for the sent notices report and matter audit report definitions, you can also edit them. For example, if you add a custom attribute and a report is to cover it, you must update the report definition.

In addition to the predefined reports, you can create custom reports by maintaining your own report definitions.

To manage reports:

1. On the **Report Definitions** page, add or update a report definition.
  - To add a custom report definition, click **Add Report Definition** and select the report definition file (.rptdesign file) that you want to add.
  - To update any report definition, you must replace the existing one:
    - a. Open the report definition, download the report definition file, and then change the file.
    - b. Suspend the current report definition.
    - c. On the **Report Definitions** page, click **Replace Report Definition** and select the updated report definition file.

**Important:** The existing report definition is permanently replaced with the new one. You cannot restore a previous version of the report definition file. However, any reports that were generated before you update the report definition are preserved.

You can add or update report definitions that reference shared report resources even if these report resources are not yet available. In this case, a warning message is issued. However, you can activate a report definition only after all required resources are available in StoredIQ for Legal.

2. Activate the report definition to enable the creation of the reports.

You cannot delete an active report definition; you must suspend it first.
3. If the reports are run automatically, complete these steps:
  - a) In the report definition, ensure that the wanted output format is listed first in the **Available output format** field.
  - b) Check whether you must update the schedule in the system settings.

For more information, see [“Configuring system settings”](#) on page 58.
4. Decide which users are allowed to create or view which predefined and custom reports and assign the appropriate privileges.

For more information, see [“Planning for reports”](#) on page 35 and [“Managing and assigning roles and privileges”](#) on page 76.

Depending on the report definition, the reports are now run automatically or can be created on request.

## Managing report resources

Make external resources such as stylesheets, or property and library files available as shared resources for all your custom reports.

To support standard report formats, you can provide a set of report resources with common configuration and styling information that any of your custom report definitions have access to. In addition, you might want to provide translated versions of labels and other report text. To have these shared resources available for report rendering, import the resources into StoredIQ for Legal. The following resource types are supported:

- Report libraries (.rptlibrary files), which contain predesigned report elements

- Stylesheets (CSS files), which contain formatting information for your report
- Property files (.properties files), which contain translated content

**Restriction:** Report parameters defined in a report library cannot be shared across reports. You must add any report parameters individually to each report.

To manage report resources:

- Add a report resource.

On the **Report Resources** page, click **Add Report Resource** and select the resource that you want to add.

- Delete a report resource.

On the **Report Resources** page, select the resource that you want to delete and click **Delete**.

- Replace a report resource.

On the **Report Resources** page, select the resource that you want to update and click **Replace**. Then, select the report resource file with which you want to replace the existing resource.

**Important:** You can delete or replace only resources that are not in use by any active report definition.

- Export a report resource.

On the **Report Resources** page, select the resource that you want to export and click **Export**.

## Creating and viewing matter-specific reports

For each matter, you can create reports. Which matter-specific reports you can create and view, depends on your privileges.

- [“Managing report definitions” on page 124](#). Ensure that the report definitions are activated.
- You must be signed in with the appropriate privilege. For an overview of the predefined reports and of the privileges that are required to create and view the reports, see [“Planning for reports” on page 35](#).
- If key-based access control is enabled, not all report types might be available.

To create matter-specific reports, complete these steps:

1. Open the matter for which you want to create one or more reports.
2. On the **Reports** page, next to each report that you want to create, select the output format and then click **Create**.

You might be prompted for information to further customize the report.

When you request a Notice Confirmation report, the report parameter values must not contain any characters from the following set :

```
! @ # $ % & * ( ) + = [ ] { } ; ' : " | , . < > \ / ?
```

Searching for more than one first name or last name is allowed. However, wildcard searches are not supported.

3. To view a report, you can either open it directly from the `A new report is available` message or open it from the list of reports.

**Tip:** If a Custodian History Report contains a huge amount of data, opening the report in HTML format might not work in Internet Explorer. A workaround is to create and open the report in PDF format or to use a different browser such as Firefox or Chrome to open the report in HTML format.

A report is available for viewing 30 days or for a period that is specified by your administrator.

## Creating and viewing cross-matter reports

Reports that include data from more than one matter are run automatically or must be requested. Which cross-matter reports you can create and view, depends on your privileges.

- [“Managing report definitions” on page 124](#). Ensure that the report definitions are activated.

- You must be signed in with the appropriate privilege. For an overview of the predefined reports and of the privileges that are required to create and view the reports, see [“Planning for reports” on page 35](#).
- If key-based access control is enabled, not all report types might be available.

To create and view cross-matter reports, complete these steps:

1. Click **Reports > My Reports**.
2. Next to each report that you want to create, select the output format and then click **Create**.

You might be prompted for information to further customize the report.

The report that is returned contains data from the matters that you have access to.

3. To view the reports that were created by other users, go to the **All Reports** page.

The reports are available in the format that was requested by those users.

4. To view the reports that are run automatically, go to the **Scheduled Reports** page.

The reports are available in the format that is specified in the report definition.

**Tip:** If a User Audit Report, a User Information Report, or a User Login Report contains a huge amount of data, opening the report in HTML format in a browser might not work. A workaround is to create and open the report in PDF format. It might still take some time to load all data when you open the report.

All reports are available for viewing for 30 days or for a period that is specified by your administrator.

## Creating reports by using reporting views

The reporting views provide a relational view of the data within the StoredIQ for Legal system that can be used by an external reporting engine. You can integrate your own reporting engine with the StoredIQ for Legal system, or develop reports that can integrate with the reporting views by using the standard ODBC or JDBC connectivity.

Using reporting views, you can run specific SQL queries on the StoredIQ for Legal reporting database to create the reports. The data that is shown in these views is fetched from the StoredIQ for Legal database by a background task.

The reporting database is, by default, refreshed once a day at midnight Coordinated Universal Time (UTC). To refresh it more often, you must change the system settings. If scheduling is disabled, the refresh schedule is suspended. For more information, see [“Configuring system settings” on page 58](#).

For better refresh performance, the table entries for the following entities are refreshed incrementally:

- appauditusersession
- appauditworkflow
- fulfillmentitem

**Note:** Draft items will not show up in reports for this entity.

- fulfillmentworkpackage

**Note:** Draft items will not show up in reports for this entity.

- orgtreehistory
- persondistinct
- transmission

Here, *incrementally* means that when refreshing the reporting database not the complete tables and views with such entries are dropped and re-created. For those tables, only rows that were inserted or updated after the last refresh are loaded into the reporting database.

**Important:** Do not use any of the tables in the reporting database for other purposes. They can change depending on the version of StoredIQ for Legal.

Also, when you create custom views in the reporting database, do not use any special characters that the database system does not accept in a view or table name.

In general, create your custom views with specific column names instead of using `select *`. Otherwise, your view will contain exactly those columns that are available in StoredIQ for Legal at the time you create that view. If columns are added in later versions of the product, your view will not include the new columns.

- To connect to the reporting views, you need a Postgres compatible ODBC or JDBC driver. With JDBC, you can connect to the reporting database, `reportdb`, by using the following JDBC URL (ensure that the port is open and accessible):

```
jdbc:postgresql://user@host:port/reportdb
```

The default for StoredIQ for Legal (VM) is:

```
jdbc:postgresql://reportadmin@hostname:5432/reportdb
```

The default for StoredIQ for Legal (Container) is:

```
jdbc:postgresql://reportadmin@hostname:30001/reportdb
```

You can change the node port for the reporting data base as described in the [NodePort](#) topic in the OpenShift documentation.

For security, make sure that you change the initial password of `passw0rd`. To do so, run the respective script:

- StoredIQ for Legal (VM): Run the `/siq/bin/change_reportadmin_password` script as StoredIQ for Legal system administrator:

```
/siq/bin/change_reportadmin_password -n new_pwd -p ilgadmin_pwd
```

- StoredIQ for Legal (Container): Run the `change_reportadmin_password` script as StoredIQ for Legal system administrator. You can run the command on the master node of your cluster or from any OpenShift client that has access to the cluster.

```
change_reportadmin_password -n new_pwd -p ilgadmin_pwd
```

Two other user IDs are used by default to populate the reporting database and generate the reports:

#### **ilgreportadmin**

User ID that populates the reporting database.

#### **ilgreportuser**

User ID that generates the reports.

### **Related reference**

[Administration scripts](#)

StoredIQ for Legal comes with a set administration scripts, for example, for reconfiguring the virtual machine (StoredIQ for Legal (VM)) or for changing passwords.

### **Audit views**

The audit views provide user session related info, showing which user accessed the StoredIQ for Legal system at what time and from what IP address.

#### **rep\_audit\_user\_session\_view (User session audit view)**

Each row in this view represents an audit entry corresponding to a user action such as logging into the system or logging out from the StoredIQ for Legal system.

Column	Attribute Name	Type	Description
loginid	Login ID	character varying(50)	The signin ID of the user.
ipaddress	IP Address	character varying(45)	IP address of the client machine from where the signin event occurred.

Column	Attribute Name	Type	Description
eventtype	Event Type	character varying(512)	Type of event (signin, signout).
eventdate	Event Date	timestamp without time zone	Date when the event occurred.

### rep\_audit\_workflow\_view (Workflow audit view)

Each row in this view represents an audit entry related to the workflow.

Column	Attribute Name	Type	Description
id	ID	bigint	Unique identifier for this workflow audit event.
creationdate	Creation Date	timestamp without time zone	Creation time stamp for the workflow audit event.
modifieddate	Modified Date	timestamp without time zone	Last modified time stamp for the workflow audit event.
task_category	Task Category	character varying(255)	Task category.
proc_inst_id	Process Instance ID	character varying(64)	Workflow process instance ID.
proc_inst_entity_definition_id	Process Instance Entity Definition ID	bigint	Entity definition ID associated with the process instance.
proc_inst_matter_id	Process Instance Matter ID	bigint	Matter ID associated with the process instance.
proc_inst_entity_id	Process Instance Entity ID	bigint	Entity ID of the process instance.
proc_inst_status	Process Instance Status	character varying(512)	Status of the process instance.
actor_id	Actor ID	bigint	Unique identifier representing the initiator of this event.
task_type	Task Type	character varying(512)	Task type.
proc_def_key	Process Definition Key	character varying(255)	Process definition key.
correlation_id	Correlation ID	bigint	Correlation ID.
raw_data	Raw Data	character varying(10240)	JSON data containing the details of this audit event.
task_assignee_id	Task Assignee ID	bigint	Unique identifier for the task assignee.
proc_error	Process Error	character varying(512)	Workflow process error.
event_date	Event Date	timestamp without time zone	Time of this event.
task_id	Task ID	character varying(64)	Task unique identifier.
task_name	Task Name	character varying(255)	Task name.
event_type	Event Type	character varying(512)	Type of audit event.
proc_def_id	Process Definition ID	character varying(64)	Workflow process definition unique identifier.

### Data request views

The data request views provide data source and data request information within the StoredIQ for Legal application.

#### rep\_datasource\_view (Data Source View)

Each row in this view represents a data source within the StoredIQ for Legal application.

Column	Attribute name	Type	Description
id	n/a	bigint	Data source identifier.
creationdate	n/a	timestamp without time zone	Date when created.
modifieddate	n/a	timestamp without time zone	Date when the data source was last modified.
datasteward	n/a	bigint	Data steward for this data source.
datastewardname	Data Steward	text	Name of the data steward for this data source.
datasourceid	Unique ID	character varying(250)	Data source identifier.
name	Name	character varying(250)	Name of this data source.
jurisdiction	n/a	bigint	Jurisdiction identifier of this data source.
jurisdictionname	Jurisdiction	character varying(250)	Jurisdiction name of this data source.
status	Status	character varying(512)	Status of this data source.
description	Description	character varying(2000)	Description of this data source.
datasourcecategory	Data Source Category	character varying(128)	Category of this data source. This is a multi-valued attribute where the values are stored as a JSON array of strings. Note that the JSON structure is subject to change.

#### rep\_datarequest\_view (Data Request View)

Each row in this view represents a data request within the StoredIQ for Legal application.

Column	Attribute name	Type	Description
id	n/a	bigint	Identifier for this data request.
name	Name	character varying(250)	Name of this data request.
description	Description	character varying(2000)	Description of this data request.
creationdate	n/a	timestamp without time zone	Creation date of this data request.
modifieddate	n/a	timestamp without time zone	Date when the data request was last modified.
completiondate	Completion Date	timestamp without time zone	Completion date of this data request.

Column	Attribute name	Type	Description
datasourcecategory	Data Source Category	character varying(128)	Data source category of this data request. This is a multi-valued attribute where the values are stored as a JSON array of strings. Note that the JSON structure is subject to change.
cloneclount	n/a	binint	Number of duplicated work packages.
age	n/a	interval	Age of this data request. If a completion date exists, this age is calculated as the interval from the creation date until the completion date. Otherwise, the interval from creation date until the current time.
definition	n/a	bigint	Definition of this data request.
externalid	Unique ID	character varying(250)	External identifier for this data request.
custodianoverride	n/a	text	Flag indicating custodian override.
requestor	n/a	bigint	Person who created this data request.
requestorname	Requester	text	Name of the requester.
terms	Terms	character varying(2000)	Terms of this data request.
matterid	n/a	bigint	Matter identifier corresponding to this data request.
requiresjurisdictionapproval	Jurisdiction Approval	integer	Flag indicating whether jurisdiction approval is required for this data request.
duedate	Due Date	timestamp without time zone	Due date for the data request.
type	Type	character varying(512)	Type of data request.
status	Status	character varying(512)	Status of the data request.
lifecyclestate	Lifecycle State	character varying(64)	Lifecycle state of the data request.
priority	Custodian Priority	character varying(128)	Priority.
requestpriority	Request Priority	character varying(128)	Default custodian priority for the data request.
inprocessing	n/a	integer	Flag indicating whether this data request is processing.
lifecyclestatedate	Lifecycle State Date	timestamp without time zone	Lifecycle estate.
dateranges	Date Ranges	character varying(128)	Date ranges for this data request. This is a multi-valued attribute where the values are stored as a JSON array of strings. Note that the JSON structure is subject to change.



Column	Attribute name	Type	Description
fulfillmentinstructions	Fulfillment Instructions	character varying(2000)	Fulfillment instructions.
discoveryinfomessage	Discovery Info Message	character varying(2000)	User provided text.
submissiondate	Submission Date	timestamp without time zone	Submission date of the request.
substatus	Substatus	character varying(512)	Status.
releaseparentrequest	Release Source	bigint	ID of the parent preservation, or preservation and collection request. A value is set only for data requests of the type release. For other data request types, the value is NULL.
releasestatus	Release Status	character varying	Release status of the parent preservation, or preservation and collection request. Possible values are NotStarted, Started, Completed, or Canceled. This status is associated with the status indicator shown in the UI.  For data requests of other types, this value is NULL.

#### rep\_fulfillmentitem\_view (Fulfillment Item View)

Each row in this view represents a fulfillment item within the StoredIQ for Legal application.

Column	Attribute name	Type	Description
id	n/a	bigint	Identifier.
creationdate	n/a	timestamp without time zone	Date created.
modifieddate	n/a	timestamp without time zone	Date when the fulfillment item was last modified.
datasourcecategory	Date Source Category	character varying(128)	Data source category of this fulfillment item.
priority	Custodian Priority	character varying(128)	Priority.
otherunit	Other Unit	character varying(64)	Other unit.
taskatcompletion	Task At Completion	character varying(255)	Task at completion.
duedate	Due Date	timestamp without time zone	Due date.
completiondate	Completion Date	timestamp without time zone	Completion date.
fulfillmentinstructions	Fulfillment Instructions	character varying(2000)	Additional fulfillment instructions.

Column	Attribute name	Type	Description
discoveryinfomessage		character varying(2000)	
custodian	n/a	bigint	Custodian for this fulfillment item.
resultsizeunit	Unit	character varying(512)	Unit for the result size, for example, bytes, KB, MB, or GB.
useridforsearch	User IDs on Data Source	character varying(250)	User ID for search.
resultcount	Total Items	bigint	Number of results.
resultsize	Total Size	bigint	Size of result items.
request	n/a	bigint	Data request ID.
status	Status	character varying(512)	Status of this fulfillment item.
workpackage	n/a	bigint	Work package to which this fulfillment item belongs to.
type	Type	character varying(512)	Type of fulfillment item.
comment	Comment	character varying(5000)	Comment added to the fulfillment item.
currenttaskstatus	Current Task Status	character varying(512)	Status of the current task.
externalid	Unique ID	bigint	External identifier.
datasource	n/a	bigint	Data source associated.
dateranges	Date Ranges	character varying(1460)	Date ranges for this fulfillment item. This is a multi-valued attribute where the values are stored as a JSON array of strings. Note that the JSON structure is subject to change.
releasestatus	Release Status	character varying	Release status of the fulfillment item. Possible values are NotReleased, Requested (release data request is submitted), Submitted (release work package is submitted), and Completed (release of this fulfillment item is completed).
releaseworkpackage	n/a	bigint	ID of the work package under which this fulfillment item is released.
releaserequest	n/a	bigint	ID of the data request under which this fulfillment item is released.
releasesource	n/a	bigint	ID of the parent preservation, or preservation and collection request. A value is set only for data requests of the type release. For other data request types, the value is NULL.

Column	Attribute name	Type	Description
releasechild	n/a	integer	ID of the child release request under which this fulfillment item is released.
unreleaseddateranges_cpx	n/a	varchar(1460)	List of the date ranges with unreleased data.

### rep\_fulfillmentworkpackage\_view (Work Package View)

Each row in this view represents a work package that is part of a data request within the StoredIQ for Legal application.

Column	Attribute name	Type	Description
id	n/a	bigint	Identifier.
creationdate	n/a	timestamp without time zone	Date created.
modifieddate	n/a	timestamp without time zone	Date when the work package was last modified.
datasourcecategory	Data Source Category	character varying(128)	Data source category. This is a multi-valued attribute where the values are stored as a JSON array of strings. Note that the JSON structure is subject to change.
fulfillmentteam	Fulfillment Team	character varying(128)	Fulfillment team.
priority	Custodian Priority	character varying(128)	Priority.
resultsize	Total Size	bigint	Result size. See resultsizeunit too.
completiondate	Completion Date	timestamp without time zone	Completion date.
externalid	Unique ID	bigint	External ID.
totalitemcount	Total Items	bigint	Number of items in the search result.
status	Status	character varying(512)	Status of this work package.
lifecyclestatedate	Lifecycle State Date	timestamp without time zone	Date when this lifecycle state was set.
lifecyclestate	Current Lifecycle State	character varying(64)	Current lifecycle state of the work package.
lifecyclestates	Overall Lifecycle State	character varying(512)	Overall lifecycle state of the work package. This column is populated only after the work package was completed.
substatus	Sub Status	character varying(512)	Status the work package was in when it was canceled.

Column	Attribute name	Type	Description
fulfillmentinstructions	Fulfillment Instructions	character varying(2000)	Additional fulfillment instructions.
fulfillmentitemimportmapping	Fulfillment Import Mapping	character varying(250)	Import mapping associated with the fulfillment item.
resultcount	n/a	bigint	Number of items in the result.
eta	Estimated Completion Date	timestamp without time zone	Expected arrival time.
duedate	Work Package Due Date	timestamp without time zone	Due date for the work package.
request	n/a	bigint	Data request to which this work package belongs to.
inprocessing	n/a	integer	Flag indicating whether this work package is in process.
datasource	Data Source	bigint	Associated data sources.
resultsaggregated	n/a	integer	Flag indicating whether the results are aggregated.
resultsizeunit	Unit	character varying(512)	Unit of the result size, for example, bytes, KB, MB or GB.
jurisdiction	Jurisdiction	bigint	Jurisdiction of this work package.
otherunit	Other Unit	character varying(64)	Other unit.
terms	Terms	character varying(2000)	Additional terms for this work package.

### rep\_dsapplication\_view (Data Source Applications View)

Each row in this view represents a data source application within StoredIQ for Legal.

Column	Attribute name	Type	Description
id	n/a	bigint	Data source application identifier.
creationdate	n/a	timestamp without time zone	Date when created.
modifieddate	n/a	timestamp without time zone	Date when the data source was last modified.
name	Name	character varying(250)	Name of this data source application.
status	Status	character varying(512)	Status of this data source application.
description	Description	character varying(2000)	Description of this data source application.
dsappid	Unique ID	character varying(250)	ID for this data source application.

### rep\_dserver\_view (Data Source Servers View)

Each row in this view represents a data source server within StoredIQ for Legal.

Column	Attribute name	Type	Description
id	n/a	bigint	Data source server unique identifier.
creationdate	n/a	timestamp without time zone	Date when created.

Column	Attribute name	Type	Description
modifieddate	n/a	timestamp without time zone	Date when the data source server was last modified.
dserverid	Unique ID	character varying(250)	ID for this data source server.
description	Description	character varying(2000)	Description of this data source server.
name	Name	character varying(250)	Name of this data source server.
hostname	Host name	character varying(255)	Host name for this data source server.

### Global hold reminder views

The global hold reminder views provide general information about the global hold reminder in StoredIQ for Legal.

#### rep\_ghr\_view (Global Hold Reminder View)

This view lists the custodians of the current issuance of the global hold reminder.

Column	Attribute Name	Type	Description
firstname	First Name	character varying(250)	First name of the custodian
lastname	Last Name	character varying(250)	Last name of the custodian
lastissuancedate	Last Issuance Date	timestamp without time zone	Date of the last issuance of the global hold reminder
email	Email	character varying(250)	Email ID of the custodian
status	Status	character varying(250)	Latest status (current issuance) of the custodian
personidentifier	Person Identifier	character varying(250)	Person identifier of the custodian
loginid	Signin ID	character varying(250)	Signin ID of custodian
noticeid	Notice ID	bigint	The unique ID of the notice to which the global hold reminder for the custodian is associated
globalreminderid	Global Reminder Id	bigint	The unique ID that identifies the global hold reminder

#### rep\_ghr\_transmission\_view (Global Hold Reminder Transmission View)

This view lists the custodians of all issuances of the global hold reminder to date, including past issuances.

Column	Attribute Name	Type	Description
id	ID	bigint	The transmission ID of global hold reminder transmissions
ghrid	Global Reminder Id	bigint	The unique ID that identifies the global hold reminder
creationdate	Creation Date	timestamp without time zone	Creation date of this transmission entry

Column	Attribute Name	Type	Description
transmissiontype	Transmission Type	character varying(250)	The transmission type of the transmission entry; possible value are globalholdreminder and globalholdreminderfollowup
transmissionset	Transmission Set	bigint	Transmission set of global hold reminder transmissions; usually each issuance has a separate ID
persondistinctid	Person Distinct Id	bigint	The ID that uniquely identifies a person
loginid	Signin ID	character varying(250)	Signin ID of the person
firstname	First Name	character varying(250)	First Name of the person
lastname	Last Name	character varying(250)	Last Name of the person
email	Email	character varying(250)	Email ID of the person
confirmationstatus	Confirmation Status	text	The confirmation status of the custodian: <b>No Reply</b> The global hold reminder was sent successfully but the custodian did not yet reply to the notification. <b>Replied Confirmed</b> The global hold reminder was sent successfully and the custodian replied to the notification. <b>Transmission Error</b> An error occurred during the transmission to the global hold reminder

### Hold notice views

The hold notice views provide general information about hold notices that were created by using StoredIQ for Legal.

### rep\_notices\_view (Hold notice view)

Each row in this view describes a single notice that announces a hold. It provides details such as notice ID, name, description, status, creation date, last modification date, publish date, matter ID, matter name, and matter external ID.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	Uniquely identifies the matter to which this notice belongs.
noticedescription	Notice Description	character varying(2000)	Description of the notice.
noticestatus	Notice Status	character varying(512)	Describes notice status and can be Draft, Suspended, or Published.

Column	Attribute Name	Type	Description
noticecreatedon	Notice Creation Date	timestamp without time zone	Date on which notice was created.
noticemodifiedon	Notice Modified Date	timestamp without time zone	Date on which notice was modified.
noticepublishedon	Notice Publication Date	timestamp without time zone	Date on which notice was published.
noticematterexternalid	Matter External ID	character varying(250)	External ID of the matter to which this notice belongs.
noticematterid	Matter ID	bigint	Matter ID of the matter to which this notice belongs.
noticemattername	Matter Name	character varying(250)	Name of the matter to which this notice belongs.

### rep\_notice\_details\_view (Hold Notice Details View)

This view contains details of a hold notice such as intervals, subject and email content corresponding to the initial, follow up and reminder notices.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
noticeinitialsubject	Notice Initial Subject	text	The subject line in the initial notice email message.
noticeinitialemail	Notice Initial Email	text	The email body in the initial notice email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticeisfollowupenabled	Notice Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the initial notice.
noticeisreminderfollowupenabled	Notice Reminder Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the reminder notice.
noticefollowupsubject	Notice Follow-Up Subject	text	The subject line in the notice follow-up email message.
noticefollowupemail	Notice Follow-Up Email	text	The email body in the notice follow-up email message. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticefollowuprepeatinterval	Notice Follow-Up Repeat Interval	bigint	Describes follow-up repeat interval for the notice. This attribute sets the frequency

Column	Attribute Name	Type	Description
			with which the followup notice is sent.
noticefollowuprepeatunit	Notice Follow-up Repeat Unit	character varying	Text that describes the follow-up repeat unit. It is used with noticefollowuprepeatinterval. The value can be Days, Weeks, Months, or Years.
noticefollowupmaxrepeat	Notice Follow-Up Maximum Repeat Interval	bigint	Describes the follow-up maximum repeat interval for the notice. It is used with noticefollowuprepeatinterval. The value specifies for how many times (maximum) the follow-up notice should be sent.
noticefollowupescalation	Notice Follow-Up Escalation	integer	Describes whether follow-up escalation is enabled(1) OR not(0) for the notice.
noticeremindersubject	Notice Reminder Subject	text	The subject line in the notice reminder email message.
noticereminderemail	Notice Reminder Email	text	The email body in the reminder notice email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticereminderrepeatinterval	Notice Reminder Repeat Interval	bigint	Describes notice reminder repeat interval for the notice. This attribute sets the frequency with which the reminder notice is sent.
noticereminderrepeatunit	Notice Reminder Repeat Unit	character varying	Text that describes the reminder repeat unit. It can be Days, Weeks, Months, or Years. It is used with noticereminderrepeatinterval.
noticeremindermaxrepeat	Notice Reminder Maximum Repeat Interval	bigint	Describes reminder maximum repeat interval for the notice. It is used with noticereminderrepeatinterval. This attribute describes for how many times (maximum) the notice reminder should be sent.
noticereminderfollowupescalation	Notice Reminder Follow-Up Escalation	integer	Describes whether reminder follow-up escalation is enabled(1) OR not(0) for the notice.
noticereminderfollowupsubject	Notice Reminder Follow-Up Subject	text	The subject line in the reminder follow-up email message.
noticereminderfollowupemail	Notice Reminder Follow-Up Email	text	The email body in the reminder follow-up email. Predefined



Column	Attribute Name	Type	Description
			variables are not expanded. The email body contains HTML tags, so handle it appropriately.
noticereminderfollowuprepeatinterval	Notice Reminder Follow-Up Repeat Interval	bigint	Describes the reminder follow-up repeat interval for the notice. This attribute sets the frequency with which the reminder follow-up notices are sent.
noticereminderfollowuprepeatunit	Notice Reminder Follow-Up Repeat Unit	character varying	Describes the reminder follow-up repeat unit. It can be Days, Weeks, Months, or Years. It is used with noticereminderfollowuprepeatinterval.
noticereminderfollowupmaxrepeat	Notice Reminder Follow-Up Maximum Repeat Interval	bigint	Describes reminder follow-up maxrepeat interval for the notice. It is used with noticereminderfollowuprepeatinterval. This attribute describes for how many times (maximum) the reminder follow-up should be sent.
noticepublisheddate	Notice Publication Date	timestamp without time zone	Date when the initial notice was sent to the custodians.
noticelastissuancedate	Notice Last Issuance Date	timestamp without time zone	Date when the last issuance was sent.
noticelastfollowupdate	Notice Last Follow-Up Date	timestamp without time zone	Date when the last follow-up was sent.

### rep\_notice\_history\_view (Hold Notice History View)

This view provides information about the history of the notice. Each time a notice is republished, the previous version is stored as a history record and an entry is created in the reporting database.

Column	Attribute Name	Type	Description
Id	Notice ID	bigint	The unique identifier of the notice.
name	Notice Name	character varying(250)	The name of the notice.
description	Description	character varying(2000)	The notice description.
matterid	Matter ID	bigint	The unique ID of the matter to which notice is associated.
creationdate	Notice Creation Date	timestamp with time zone	The date on which this notice history record was created.
lastissuanceset	Issuance Set	Bigint	Indicates what the last issuance was before the notice was republished, that is, either the

Column	Attribute Name	Type	Description
			initial notice or a reminder and, in the latter case, the number of the reminder.
lastissuancedate	Last Issuance Date	timestamp with time zone	The date on which the last issuance was sent before the notice was republished.
lastfollowupset	Follow-up Set	Bigint	Indicates the last follow-up before the notice was republished, that is, either a follow-up to the initial notice or a reminder follow-up and the number of the follow-up.
lastfollowupdate	Last Follow-up Date	timestamp with time zone	The date on which the last follow-up was sent before the notice was republished.
sendchangenoticeto	Changed Notice Sent	integer	Describes whether the changed notice was sent to all active custodians (1) or whether no notifications were sent at all (0).

### **rep\_notice\_message\_history\_view (Hold Notice Message History View)**

this view provides an overview of the changes to the messages of a hold notice. Each time a notice history record is created, entries are created in the reporting database that show the various types of messages that each specific version of the notice contained.

Column	Attribute Name	Type	Description
Id	Message ID	bigint	The identifier of the message.
noticeId	Notice ID	bigint	The unique identifier of the notice.
type	Type	character varying(512)	The message type: initial, initial follow-up, reminder, reminder follow-up, or change message.
messagemask	n/a	-	Internally used only.
repeatinterval	Repeat Interval	bigint	Describes the repeat interval for the respective message. This attribute sets the frequency with which the message is sent.
repeatunit	Repeat Unit	character varying(512)	Text that describes the repeat unit. It is used with repeatinterval. The value can be Days, Weeks, Months, or Years.
maxrepeat	Maximum Repeat Interval	bigint	The maximum number of times this message is repeated. This attribute is used with repeatinterval.
courtesycopy	Courtesy Copy	integer	Describes whether courtesy copies can be sent for this message (1) or not (0).
escalation	Escalation	integer	Describes whether escalation is disabled (0). Any number other than zero indicates that escalation is enabled.
creationdate	Creation Date	timestamp with time zone	The date on which this notice message history record was created.
version	Version	bigint	The version of the notice to which the message belongs.

### **rep\_notice\_recipients\_view (Hold Notice Recipient View)**

This view lists the custodians in a hold notice along with custodian response status.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	Matter ID of the matter for which notice belongs.
mattername	Matter Name	character varying(250)	Matter name of the matter to which the notice belongs.
personidentifier	Person ID	character varying(250)	Identifier of the person that is part of notice.
firstname	First Name	character varying(250)	First name of the person that is part of notice.
loginid	Signin ID	character varying(256)	Signin ID of the person.
lastname	Last Name	character varying(250)	Last name of the person that is part of notice.
email	Email	character varying(256)	Email ID of the person that is part of notice.
status	Status	character varying	Status of the person that is part of notice.
publisheddate		timestamp without time zone	Date on which notice is published.
lastissuancedate		timestamp without time zone	Date on which notice last issuance is sent.
lastfollowupdate		timestamp without time zone	Date on which last follow-up is sent.

#### **rep\_notice\_responses\_view (Hold Notice Response View)**

Each row in this view represents the response received from a custodian for a hold notice.

Column	Attribute Name	Type	Description
noticetransmissionresponseid	Notice Transmission Response ID	bigint	Unique identification for notice transmission response.
noticereipientid	Notice Recipient ID	bigint	Unique identification for the recipient.
noticereipientname	Notice Recipient Name	text	Full name of the recipient.
noticereipientemail	Email ID	character varying(250)	Email ID of the recipient.
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
noticesentdate	Notice Sent Date	timestamp without time zone	Date when the notice was sent.
noticetransmissiontype	Notice Transmission Type	character varying(256)	Identifies transmission type.
noticereipientresponserecieveddate	Notice Recipient Response Date	timestamp without time zone	Recipients response date.
noticeisconfirmed	Confirmed Notice	integer	Integer value as 1.

### rep\_notice\_silent\_custodians\_view (Hold Notice Silent Custodians View)

This view lists the silent custodians in a hold notice.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	Matter ID of the matter for which notice belongs.
mattername	Matter Name	character varying(250)	Matter name of the matter to which the notice belongs.
personidentifier	Person ID	character varying(250)	Identifier of the person that is part of notice.
firstname	First Name	character varying(250)	First name of the person that is part of notice.
loginid	Signin ID	character varying(256)	Signin ID of the person.
lastname	Last Name	character varying(250)	Last name of the person that is part of notice.
email	Email	character varying(256)	Email ID of the person that is part of notice.
status	Status	character varying	Status of the person that is part of notice.
publisheddate		timestamp without time zone	Date on which notice is published.

### rep\_notice\_transmissions\_view (Hold Notice Transmission view)

This view lists transmissions of hold notices including initial, follow up and reminder transmission along with the success or failure status of the transmission.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Unique identification.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	ID of the matter to which the notice belongs.
mattername	Matter Name	character varying(250)	Name of the matter to which the notice belongs.
personidentifier	Person ID	character varying(250)	Identifier of the person associated with the notice.
firstname	First Name	character varying(250)	First name of the person associated with the notice.
lastname	Last Name	character varying(250)	Last name of the person associated with the notice.
email	Email	character varying(250)	Email ID of the person associated with the notice.
transmissiondate	Transmission Date	timestamp without time zone	Date corresponding to notice transmission.
transmissionid	Transmission	bigint	Uniquely identifies transmission for each notice.
transmissiontype	Transmission Type	character varying(256)	Identifies transmission type initial, follow-up, and so on.

### rep\_migrated\_notice\_details\_view (Migrated Hold Notices Details view )

This view contains details of a migrated hold notice such as intervals, subject and email content corresponding to the initial, follow up and reminder notices.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
noticeinitialsubject	Notice Initial Subject	text	The subject line in the initial notice email message.
noticeinitialemail	Notice Initial Email	text	The email body in the initial notice email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticeisfollowupenabled	Notice Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the initial notice.
noticeisreminderfollowupenabled	Notice Reminder Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the reminder notice.
noticefollowupsubject	Notice Follow-Up Subject	text	The subject line in the notice follow-up email message.
noticefollowupemail	Notice Follow-Up Email	text	The email body in the notice follow-up email message. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticefollowuprepeatinterval	Notice Follow-Up Repeat Interval	bigint	Describes follow-up repeat interval for the notice. This attribute sets the frequency with which the followup notice is sent.
noticefollowuprepeatunit	Notice Follow-up Repeat Unit	character varying	Text that describes the follow-up repeat unit. It is used with noticefollowuprepeatinterval. The value can be Days, Weeks, Months, or Years.
noticefollowupmaxrepeat	Notice Follow-Up Maximum Repeat Interval	bigint	Describes the follow-up maximum repeat interval for the notice. It is used with noticefollowuprepeatinterval. The value specifies for how many times (maximum) the follow-up notice should be sent.
noticefollowupescalation	Notice Follow-Up Escalation	integer	Describes whether follow-up escalation is enabled(1) OR not(0) for the notice.

Column	Attribute Name	Type	Description
noticeremindersubject	Notice Reminder Subject	text	The subject line in the notice reminder email message.
noticereminderemail	Notice Reminder Email	text	The email body in the reminder notice email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
noticereminderrepeatinterval	Notice Reminder Repeat Interval	bigint	Describes notice reminder repeat interval for the notice. This attribute sets the frequency with which the reminder notice is sent.
noticereminderrepeatunit	Notice Reminder Repeat Unit	character varying	Text that describes the reminder repeat unit. It can be Days, Weeks, Months, or Years. It is used with noticereminderrepeatinterval.
noticeremindermaxrepeat	Notice Reminder Maximum Repeat Interval	bigint	Describes reminder maximum repeat interval for the notice. It is used with noticereminderrepeatinterval. This attribute describes for how many times (maximum) the notice reminder should be sent.
noticereminderfollowupescalation	Notice Reminder Follow-Up Escalation	integer	Describes whether reminder follow-up escalation is enabled(1) OR not(0) for the notice.
noticereminderfollowupsubject	Notice Reminder Follow-Up Subject	text	The subject line in the reminder follow-up email message.
noticereminderfollowupemail	Notice Reminder Follow-Up Email	text	The email body in the reminder follow-up email. Predefined variables are not expanded. The email body contains HTML tags, so handle it appropriately.
noticereminderfollowuprepeatinterval	Notice Reminder Follow-Up Repeat Interval	bigint	Describes the reminder follow-up repeat interval for the notice. This attribute sets the frequency with which the reminder follow-up notices are sent.
noticereminderfollowuprepeatunit	Notice Reminder Follow-Up Repeat Unit	character varying	Describes the reminder follow-up repeat unit. It can be Days, Weeks, Months, or Years. It is used with noticereminderfollowuprepeatinterval.
noticereminderfollowupmaxrepeat	Notice Reminder Follow-Up Maximum Repeat Interval	bigint	Describes reminder follow-up maxrepeat interval for the notice. It is used with

Column	Attribute Name	Type	Description
			noticereminderfollowuprepeati nterval. This attribute describes for how many times (maximum) the reminder follow-up should be sent.
noticepublisheddate	Notice Publication Date	timestamp without time zone	Date when the initial notice was sent to the custodians.
noticelastissuancedate	Notice Last Issuance Date	timestamp without time zone	Date when the last issuance was sent.
noticelastfollowupdate	Notice Last Follow- Up Date	timestamp without time zone	Date when the last follow-up was sent.

### rep\_migrated\_notice\_recipients\_view (Migrated Hold Notices Recipients view)

This view lists the custodians in a migrated hold notice.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	Matter ID of the matter for which notice belongs.
mattername	Matter Name	character varying(250)	Matter name of the matter to which the notice belongs.
personidentifier	Person ID	character varying(250)	Identifier of the person that is part of notice.
firstname	First Name	character varying(250)	First name of the person that is part of notice.
loginid	Signin ID	character varying(50)	Signin ID of the person.
lastname	Last Name	character varying(250)	Last name of the person that is part of notice.
email	Email	character varying(250)	Email ID of the person that is part of notice.
status	Status	character varying	Status of the person that is part of notice.
publisheddate		timestamp without time zone	Date on which notice is published.
lastissuancedate		timestamp without time zone	Date on which notice last issuance is sent.
lastfollowupdate		timestamp without time zone	Date on which last follow-up is sent.

### rep\_silent\_custodians\_view (Hold Notices Silent Custodians view)

This view lists the silent custodians in a hold notice.

Column	Attribute Name	Type	Description
noticeid	Notice ID	bigint	Notice ID that uniquely identifies the notice.
noticename	Notice Name	character varying(250)	Name of the notice.
matterid	Matter ID	bigint	Matter ID of the matter for which notice belongs.

Column	Attribute Name	Type	Description
mattername	Matter Name	character varying(250)	Matter name of the matter to which the notice belongs.
personidentifier	Person ID	character varying(250)	Identifier of the person that is part of notice.
firstname	First Name	character varying(250)	First name of the person that is part of notice.
loginid	Signin ID	character varying(256)	Signin ID of the person.
lastname	Last Name	character varying(250)	Last name of the person that is part of notice.
email	Email	character varying(256)	Email ID of the person that is part of notice.
status	Status	character varying	Status of the person that is part of notice.
publisheddate		timestamp without time zone	Date on which notice is published.

### Interview views

The interview views provide general information about interviews that were created by using StoredIQ for Legal.

#### rep\_interview\_view (Interview View)

Each row in this view describes a single interview.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
interviewdescription	Interview Description	character varying(2000)	Description of the interview.
mattername	Matter Name	character varying(250)	Name of the matter for which this interview belongs.
matterid	Matter ID	bigint	ID of the matter for which this interview belongs.
interviewstatus	Interview Status	character varying(512)	Describes interview state. It can be Draft or Published state.
interviewpublisheddate	Interview Published Date	timestamp without time zone	Date on which interview was published.
interviewcreationdate	Interview Creation Date	timestamp without time zone	Date on which interview was created.
interviewmodifieddate	Interview Modified Date	timestamp without time zone	Date on which interview was modified.

#### rep\_interview\_details\_view (Interview details View)

This view gives details of an interview such as intervals, subject, and email content corresponding to the initial, follow up and reminder interviews.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.



Column	Attribute Name	Type	Description
interviewinitialsubject	Initial Interview Subject	text	The subject line in the initial interview email message.
interviewinitialemail	Initial Interview Email	text	The email body in the initial interview email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewisfollowupenabled	Interview Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the interview.
interviewisreminderfollowupenabled	Interview Reminder Follow-Up Enabled	integer	Describes whether follow-up reminder is set(1) OR not(0) for the interview.
interviewfollowupsubject	Interview Follow-Up Subject	text	The subject line in the interview follow-up email message.
interviewfollowupemail	Interview Follow-Up Email	text	The email body in the interview follow-up email message. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewfollowuprepeatinterval	Interview Follow-Up Repeat Interval	bigint	Describes follow-up repeat interval for the interview. This attribute sets the frequency with which the followup interview is sent.
interviewfollowuprepeatunit	Interview Follow-Up Repeat Unit	character varying	Text that describes the follow-up repeat unit. It is used with interviewfollowuprepeatinterval. The value can be Days, Weeks, Months, or Years.
interviewfollowupmaxrepeat	Interview Follow-Up Maximum Repeat Interval	bigint	Describes the follow-up maximum repeat interval for the interview. It is used with interviewfollowuprepeatinterval. The value specifies for how many times (maximum) the follow-up interview should be sent.
interviewfollowupescalation	Interview Follow-Up Escalation	integer	Describes whether followup escalation is enabled(1) OR not(0) for the interview.
interviewremindersubject	Interview Reminder Subject	text	The subject line in the interview reminder email message.
interviewreminderemail	Interview Reminder Email	text	The email body in the reminder interview email. Predefined variables are not expanded. The

Column	Attribute Name	Type	Description
			email body contains HTML tags so handle it appropriately.
interviewreminderrepeatinterval	Interview Reminder Repeat Interval	bigint	Describes interview reminder repeat interval for the interview. This attribute sets the frequency with which the reminder interview is sent.
interviewreminderrepeatunit	Interview Reminder Repeat Unit	character varying	Text that describes the reminder repeat unit. It can be Days, Weeks, Months, or Years. It is used with interviewreminderrepeatinterval.
interviewremindermaxrepeat	Interview Reminder Maximum Repeat Interval	bigint	Describes reminder maximum repeat interval for the interview. It is used with interviewreminderrepeatinterval. This attribute describes for how many times (maximum) the interview reminder should be sent.
interviewfollowupreminderescalation	Interview Reminder Escalation	integer	Describes whether reminder follow-up escalation is enabled(1) OR not(0) for the interview.
interviewreminderfollowupsubject	Interview Reminder Follow-Up Subject	text	The subject line in the reminder follow-up email message.
interviewreminderfollowupemail	Interview Reminder Follow-Up Email	text	The email body in the reminder follow-up email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewreminderfollowuprepeatinterval	Interview Reminder Follow-Up Repeat Interval	bigint	Describes the reminder follow-up repeat interval for the interview. This attribute sets the frequency with which the reminder follow-up interviews are sent.
interviewreminderfollowuprepeatunit	Interview Reminder Follow-Up Repeat Unit	character varying	Text that describes the reminder follow-up repeat unit. It can be Days, Weeks, Months, or Years. It is used with interviewreminderfollowuprepeatinterval.
interviewreminderfollowupmaxrepeat	Interview Reminder Follow-Up Maximum Repeat Interval	bigint	Describes reminder follow-up maxrepeat interval for the interview. It is used with interviewreminderfollowuprepeatinterval. This attribute describes for how many times (maximum) the reminder follow-up should be sent.

Column	Attribute Name	Type	Description
interviewpublisheddate	Interview Published Date	timestamp without time zone	Date when the initial interview was sent to the custodians.
interviewlastissuancedate	Interview Last Issuance Date	timestamp without time zone	Date when the last issuance was sent.
interviewlastfollowupdate	Interview Last Follow-Up Date	timestamp without time zone	Date when the last follow-up was sent.

### rep\_interview\_question\_view (Interview Question View)

Each row in this view contains an interview questionnaire.

Column	Attribute Name	Type	Description
interviewquestionid	Interview Question ID	bigint	Uniquely identifies the interview question.
interviewid	Interview ID	bigint	Identifies in which interview the question is being used.
interviewname	Interview Name	character varying(250)	Name of the interview for which the question is added.
interviewquestion	Interview Question Name	character varying(500)	Name of the interview question.
interviewquestiondescription	Interview Question Description	character varying(2000)	Describes the interview question.
interviewquestionanswerspace	Interview Question Answer	text	JSON structure that describes the interview question answer space. Make sure you handle the JSON structure appropriately. Note that the JSON structure is subject to change. <b>Restriction:</b> Only Unicode characters are supported.
interviewquestionisrequired	Required Question	integer	Describes whether the interview question is required(1 OR MANDATORY) OR NOT(0).
interviewquestioncreationdate	Interview Question Creation Date	timestamp without time zone	Date when the interview question was created.
interviewquestionmodifieddate	Interview Question Modified Date	timestamp without time zone	Date when the interview question was modified or updated.

### rep\_interview\_recipients\_view (Interview Recipients View)

This view lists the persons who have responded to an interview

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
matterid	Matter ID	bigint	ID of the matter to which this interview is associated.
mattername	Matter Name	character varying(250)	Name of the matter to which this interview is associated.
personidentifier	Person ID	character varying(250)	The ID of the person who responded to the interview.
firstname	First Name	character varying(250)	First name of the person who responded to the interview.
loginid	Signin ID	character varying(256)	Signin ID of the person.
lastname	Last Name	character varying(50)	Last name of the person who responded to the interview.
email	Email	character varying(256)	Email ID of the person who responded to the interview.
status	Status	character varying	Status of the person that is part of interview.
publisheddate		timestamp without time zone	Date on which interview was published.
lastissuancedate		timestamp without time zone	Date on which the interview's last issuance was sent.
lastfollowupdate		timestamp without time zone	Date on which last follow-up was sent.

### rep\_interview\_responses\_view (Interview Response View)

Each row in this view contains an individual custodian's response to an interview.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
matterid	Matter ID	bigint	ID of the matter to which this interview is associated.
mattername	Matter Name	character varying(250)	Name of the matter to which this interview is associated.
firstname	First Name	character varying(250)	First name of the person who responded to the interview.
lastname	Last Name	character varying(250)	Last name of the person who responded to the interview.
email	Email	character varying(256)	Email ID of the person who responded to the interview.
personidentifier	Person ID	character varying(250)	ID of the person who responded to the interview.

Column	Attribute Name	Type	Description
issuancetype	Issuance Type	character varying(512)	This identifies issuance type initial, follow-up, and so on.

### rep\_interview\_transmissions\_view (Interview Transmission View)

This view lists transmission records for interview.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
matterid	Matter ID	bigint	ID of the matter to which this interview is associated.
mattername	Matter Name	character varying(250)	Name of the matter to which this interview is associated.
personidentifier	Person ID	character varying(250)	ID of the person associated with interview transmission.
firstname	First Name	character varying(250)	First name of the person associated with interview transmission.
lastname	Last Name	character varying(250)	Last name of the person associated with interview transmission.
email	Email	character varying(256)	Email ID of the person associated with interview transmission.
transmissiondate	Transmission Date	timestamp without time zone	Date corresponding to interview transmission.
transmissionid	Transmission ID	bigint	Uniquely identifies transmission for each interview.
transmissiontype	Transmission Type	character varying(256)	Identifies transmission type initial, follow-up, and so on.

### rep\_migrated\_interview\_details\_view (Migrated Interview details View)

This view gives details of a migrated interview such as intervals, subject, and email content corresponding to the initial, follow up and reminder interviews.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
interviewinitialsubject	Initial Interview Subject	text	The subject line in the initial interview email message.
interviewinitialemail	Initial Interview Email	text	The email body in the initial interview email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.

Column	Attribute Name	Type	Description
interviewisfollowupenabled	Interview Follow-Up Enabled	integer	Describes whether follow-up is set(1) OR not(0) for the interview.
interviewisreminderfollowupenabled	Interview Reminder Follow-Up Enabled	integer	Describes whether follow-up reminder is set(1) OR not(0) for the interview.
interviewfollowupsubject	Interview Follow-Up Subject	text	The subject line in the interview follow-up email message.
interviewfollowupemail	Interview Follow-Up Email	text	The email body in the interview follow-up email message. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewfollowuprepeatinterval	Interview Follow-Up Repeat Interval	bigint	Describes follow-up repeat interval for the interview. This attribute sets the frequency with which the followup interview is sent.
interviewfollowuprepeatunit	Interview Follow-Up Repeat Unit	character varying	Text that describes the follow-up repeat unit. It is used with interviewfollowuprepeatinterval. The value can be Days, Weeks, Months, or Years.
interviewfollowupmaxrepeat	Interview Follow-Up Maximum Repeat Interval	bigint	Describes the follow-up maximum repeat interval for the interview. It is used with interviewfollowuprepeatinterval. The value specifies for how many times (maximum) the follow-up interview should be sent.
interviewfollowupescalation	Interview Follow-Up Escalation	integer	Describes whether followup escalation is enabled(1) OR not(0) for the interview.
interviewremindersubject	Interview Reminder Subject	text	The subject line in the interview reminder email message.
interviewreminderemail	Interview Reminder Email	text	The email body in the reminder interview email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewreminderrepeatinterval	Interview Reminder Repeat Interval	bigint	Describes interview reminder repeat interval for the interview. This attribute sets the frequency with which the reminder interview is sent.

Column	Attribute Name	Type	Description
interviewreminderrepeatunit	Interview Reminder Repeat Unit	character varying	Text that describes the reminder repeat unit. It can be Days, Weeks, Months, or Years. It is used with interviewreminderrepeatinterval.
interviewremindermaxrepeat	Interview Reminder Maximum Repeat Interval	bigint	Describes reminder maximum repeat interval for the interview. It is used with interviewreminderrepeatinterval. This attribute describes for how many times (maximum) the interview reminder should be sent.
interviewfollowupreminderescalation	Interview Reminder Escalation	integer	Describes whether reminder follow-up escalation is enabled(1) OR not(0) for the interview.
interviewreminderfollowupsubject	Interview Reminder Follow-Up Subject	text	The subject line in the reminder follow-up email message.
interviewreminderfollowupemail	Interview Reminder Follow-Up Email	text	The email body in the reminder follow-up email. Predefined variables are not expanded. The email body contains HTML tags so handle it appropriately.
interviewreminderfollowuprepeatinterval	Interview Reminder Follow-Up Repeat Interval	bigint	Describes the reminder follow-up repeat interval for the interview. This attribute sets the frequency with which the reminder follow-up interviews are sent.
interviewreminderfollowuprepeatunit	Interview Reminder Follow-Up Repeat Unit	character varying	Text that describes the reminder follow-up repeat unit. It can be Days, Weeks, Months, or Years. It is used with interviewreminderfollowuprepeatinterval.
interviewreminderfollowupmaxrepeat	Interview Reminder Follow-Up Maximum Repeat Interval	bigint	Describes reminder follow-up maxrepeat interval for the interview. It is used with interviewreminderfollowuprepeatinterval. This attribute describes for how many times (maximum) the reminder follow-up should be sent.
interviewpublisheddate	Interview Published Date	timestamp without time zone	Date when the initial interview was sent to the custodians.
interviewlastissuancedate	Interview Last Issuance Date	timestamp without time zone	Date when the last issuance was sent.
interviewlastfollowupdate	Interview Last Follow-Up Date	timestamp without time zone	Date when the last follow-up was sent.

### rep\_migrated\_interview\_question\_view (Migrated Interview Question View)

Each row in this view contains a migrated interview's questionnaire.

Column	Attribute Name	Type	Description
interviewquestionid	Interview Question ID	bigint	Uniquely identifies the interview question.
interviewid	Interview ID	bigint	Identifies in which interview the question is being used.
interviewname	Interview Name	character varying(250)	Name of the interview for which the question is added.
interviewquestion	Interview Question Name	character varying(500)	Name of the interview question.
interviewquestiondescription	Interview Question Description	character varying(2000)	Describes the interview question.
interviewquestionanswerspace	Interview Question Answer	text	JSON structure that describes the interview question answer space. Make sure you handle the JSON structure appropriately. Note that the JSON structure is subject to change. <b>Restriction:</b> Only Unicode characters are supported.
interviewquestionisrequired	Required Question	integer	Describes whether the interview question is required(1 OR MANDATORY) OR NOT(0).
interviewquestioncreationdate	Interview Question Creation Date	timestamp without time zone	Date when the interview question was created.
interviewquestionmodifieddate	Interview Question Modified Date	timestamp without time zone	Date when the interview question was modified or updated.

### rep\_migrated\_interview\_recipients\_view (Migrated Interview Recipients View)

This view lists the persons who have responded to a migrated interview.

Column	Attribute Name	Type	Description
interviewid	Interview ID	bigint	Uniquely identifies the interview.
interviewname	Interview Name	character varying(250)	Name of the interview.
matterid	Matter ID	bigint	ID of the matter to which this interview is associated.
mattername	Matter Name	character varying(250)	Name of the matter to which this interview is associated.



Column	Attribute Name	Type	Description
personidentifier	Person ID	character varying(250)	The ID of the person who responded to the interview.
firstname	First Name	character varying(250)	First name of the person who responded to the interview.
loginid	Signin ID	character varying(256)	Signin ID of the person.
lastname	Last Name	character varying(50)	Last name of the person who responded to the interview.
email	Email	character varying(256)	Email ID of the person who responded to the interview.
status	Status	character varying	Status of the person that is part of interview.
publisheddate		timestamp without time zone	Date on which interview was published.
lastissuancedate		timestamp without time zone	Date on which the interview's last issuance was sent.
lastfollowupdate		timestamp without time zone	Date on which last follow-up was sent.

### Matter views

The Matter View describes all of the matters that were added to the system. The Matter Details View lists basic details of a legal matter and includes additional information, such as attorney or paralegal names. The Matter Master List View lists all of the users who were ever in scope for all active matters, and describes how they were involved.

### rep\_matter\_view (Matter View)

Each row in this view contains the details of a legal matter.

Attribute	Column label	Type	Description
id	Matter ID	bigint	Uniquely identifies the matter.
name	Matter Name	character varying(250)	Name of the matter.
category	Matter Category	character varying(250)	Category for the matter.
externalid	Matter External ID	character varying(250)	External ID of the matter.
description	Matter Description	character varying(2000)	Matter description.
notes	Matter Notes	character varying(2000)	Matter notes and comments.
securitygroup	Matter Security Group ID	bigint	Uniquely identifies the associated matter security group.
issensitive	Sensitive Matter	integer	Identifies whether the matter is marked sensitive.
attorney	Matter Attorney ID	bigint	Uniquely identifies the associated attorney.
paralegal	Matter Paralegal ID	bigint	Uniquely identifies the associated paralegal.
dataexpert	Matter Data Expert ID	bigint	Uniquely identifies the associated data expert.

Attribute	Column label	Type	Description
status	Matter Status	character varying(512)	Status of the matter.
startdate	Matter Start Date	timestamp without time zone	Start date of the matter.
enddate	Matter End Date	timestamp without time zone	End date of the matter.
creationdate	Matter Creation Date	timestamp without time zone	Creation date of the matter.
modifieddate	Matter Modified Date	timestamp without time zone	Date when the matter was last modified.

### rep\_matter\_prettyprint\_view (Matter Details View)

Each row in this view contains the basic details of a legal matter and includes additional information, such as attorney or paralegal names.

Attribute	Column label	Type	Description
matterid	Matter ID	bigint	Uniquely identifies the matter.
mattername	Matter Name	character varying(250)	Name of the matter.
mattercategory-group	Matter Category	character varying(250)	Category for the matter.
matterdescription	Matter Description	character varying(2000)	Matter description.
matternotes	Matter Notes	character varying(2000)	Matter notes and comments.
mattersecuritygroup-id	Matter Security Group ID	bigint	Uniquely identifies the associated matter security group.
mattersecuritygroup-name	Matter Security Group Name	character varying	Matter security group name.
matterissensitive	Matter Sensitive Matter	integer	Identifies whether the matter is marked sensitive.
matterattorneyid	Matter Attorney ID	bigint	Uniquely identifies the associated attorney.
matterattorney-name	Matter Attorney Name	text	Attorney name.
matterparalegalid	Matter Paralegal ID	bigint	Uniquely identifies the associated paralegal.
matterparalegal-name	Matter Paralegal Name	text	Paralegal name.
matterdataexpertid	Matter Data Expert ID	bigint	Uniquely identifies the associated data expert.
matterdataexpert-name	Matter Data Expert Name	text	Data expert name.
matterstatus	Matter Status	character varying(512)	Status of the matter.
matterstartdate	Matter Start Date	timestamp without time zone	Start date of the matter.

Attribute	Column label	Type	Description
matterenddate	Matter End Date	timestamp without time zone	End date of the matter.
creationdate	Matter Creation Date	timestamp without time zone	Creation date of the matter.
modifieddate	Matter Modified Date	timestamp without time zone	Date when the matter was last modified.

### rep\_mml\_view (Matter Custodian View)

Each row in this view contains the details of a custodian involved in the matter.

Attribute	Column label	Type	Description
firstname	First Name	character varying(250)	First name of the custodian.
lastname	Last Name	character varying(250)	Last name of the custodian.
personidentifier	Person Identifier	character varying(250)	ID of the custodian.
noticetype	Type	character varying(250)	Notice, interview, or data request.
name	Name	character varying(250)	Name of the notice, interview, or data request.
employmentstatus	Employment Status	character varying(250)	Custodian employment status.
firstissuancedate	First Issuance Date	timestamp without time zone	Date when the notice, interview, or data request was sent.
status	Status	character varying(512)	Custodian status.
releaseddate	Released/Concluded Date	timestamp without time zone	Date when the custodian was released from the notice or the interview was concluded.
matterid	MatterId	bigint	Uniquely identifies the matter to which this notice, interview, or data request belongs.

### Organization structure views

The Organization Tree View provides information about the changes in an organization.

### rep\_org\_tree\_view (Organization Tree View)

This view lists the department or organization history.

Column	Attribute Name	Type	Description
departmentid	Department ID	character varying(255)	The unique identifier of a department or organization.
parentdepartmentid	Parent Department ID	character varying(255)	The department identifier of the hierarchical parent.
departmentname	Department	character varying(250)	The name of the department or organization.
nodetype	n/a	character varying(32)	A constant value (ORG_UNIT ) stemming from the import mapping for the organization history.

Column	Attribute Name	Type	Description
managerpersonid	Manager	character varying(255)	The unique identifier of the person who manages a department.
creationdate	Creation Date	timestamp with time zone	The date when the organization was created.
modifieddate	Modification Date	timestamp with time zone	The date when the organization was changed.
datefrom	Date From	timestamp with time zone	The start date from when on the organization hierarchy is valid. The start date is set when the organization hierarchy is imported.
dateto	Date To	timestamp with time zone	The date until which the department hierarchy is valid. This date is set when a new version of the organization is created.
jurisdiction	Jurisdiction	bigint	Jurisdiction for the organization.

### Person views

The Person View lists and describes the persons that were added to the system. The Custodian History View provides an overview of person attribute changes for all active custodians in a hold notice. The Custodians-on-Hold View lists the people who were identified as custodians in a matter across all matters. The Custodians-on-Hold Report Access View lists the users with access to the Custodians-on-Hold Report. The Jurisdiction view provides details about the available jurisdictions.

### rep\_person\_view (Person View)

Each row in this table represents a unique user of the StoredIQ for Legal system. It consists of person identifier, email, first name, last name, status, job title, manager id and name, department, and other attributes.

Column	Attribute name	Type	Description
personid	n/a	bigint	Uniquely identifies the person.
identifier	Person ID	character varying(250)	Identifier for the person.
firstname	First Name	character varying(250)	First name of the person.
lastname	Last Name	character varying(250)	Last name of the person.
loginid	Signin ID	character varying(50)	Signin ID of the person.
type	Person Type	character varying(256)	Type of person.
email	Email Address	character varying(250)	Email ID of the person.
status	n/a	character varying(512)	Status of the person.
jobtitle	Job Title	character varying(250)	Job title of the person.
creationdate	n/a	timestamp without time zone	Date when the person was added.
terminationdate	Termination Date	timestamp without time zone	Date when the person was terminated.
returnfromleavedate	Planned Return Date	timestamp without time zone	Return from leave date.

Column	Attribute name	Type	Description
employmentstatus	Employment Status	character varying(512)	Employment status of a person.
department	Department	character varying(250)	Department to which the person is associated.
modifieddate	n/a	timestamp without time zone	Date when the person's settings were last modified.
managerid	Manager	bigint	Unique identification of the person's manager.
isalias	n/a	integer	Flag indicating whether this entry is an alias.
primaryalias	n/a	bigint	Unique identification for the primary alias for an alias entry.
islocal	n/a	integer	Indicates whether this entry local (not present in the LDAP server).
canlogon	n/a	integer	Flag indicating whether this person can sign in to the system.
hasaliases	n/a	integer	Flag indicating whether this person has any other aliases.
matterinvolvementindicator	n/a	character varying(512)	Indicates whether the person is involved in any matter. Possible values are NO_INVOLVEMENTS, ON_HOLD_OR_PRESERVATION, or HAS_INVOLVEMENTS.
managername	n/a	text	Name of this person's manager (if any).
jurisdiction	Jurisdiction	character varying(250)	Jurisdiction of this person.

### rep\_person\_history\_view (Person History View)

This report details the person history of all active custodians of a notice, an interview, or a data request.

Column	Attribute name	Type	Description
personidentifier	Person Identifier	character varying(250)	Uniquely identifies the person.
personname	Person Name	character varying(250)	Full name of the person.
whochanged	Changed By	character varying(50)	Indicates who changed the attribute.
whenchanged	Changed On	character varying(256)	Shows the date and time of the change.
attributename	Attribute Name	character varying(250)	Name of the modified attribute.
previouschange	Old Value	character varying(512)	Old value of the attribute.

Column	Attribute name	Type	Description
newvalue	New Value	character varying(250)	New value of the attribute.
entitytype	Type	character varying(250)	Type of the entity: notice, interview, or data request
name	Name	character varying(250)	Name of the selected notice, interview, or data request.
entityid	n/a	bigint	ID of the selected notice, interview, or data request.
matterid	Matter Id	bigint	Uniquely identifies the matter to which this notice belongs.
entitystatus	n/a	character varying(512)	Status of the selected notice, interview, or data request.

### rep\_gcr\_view (Custodians-on-Hold View)

Each row in this report contains the details of a user who is on hold against a notice across all matters in the system.

Column	Attribute Name	Type	Description
matterid	Matter Id	bigint	Uniquely identifies the matter to which this notice belongs.
mattername	Matter Name	character varying(250)	Name of the matter.
attorney	Attorney	text	Name of the attorney.
paralegal	Paralegal	text	Name of the paralegal.
mattertype	Matter Type	character varying	Matter category.
noticename	Notice Name	character varying(250)	Name of the notice for the particular matter.
noticesentdate	Notice Sent Date	timestamp without time zone	Date when the notice was sent to the custodian.
firstname	First Name	character varying(250)	First name of the custodian.
lastname	Last Name	character varying(250)	Last name of the custodian.
email	Email	character varying(250)	Email ID of the custodian.
personidentifier	Person ID	character varying(250)	Person identifier of the custodian.
employmentstatus	Employment Status	character varying(128)	Custodian employment status.
userid	Signin ID	character varying(50)	Signin ID of the custodian.
confirmationstatus	Confirmation Status	character varying	Status of the custodian.

### rep\_gcr\_access\_view (Custodians-on-Hold Report Access View)

This view lists which users have access to the Custodians-on-Hold Report.

Column	Attribute Name	Type	Description
roleid	Role ID	bigint	Unique primary key of the role.
rolename	Role Name	character varying(250)	Name that describes the role.

Column	Attribute Name	Type	Description
isgcrviewaccessible	Access Enabled	double precision	An integer that denotes whether(1) or not(0) the role has access to GCR view.

### rep\_jurisdiction\_view (Jurisdiction view)

This view contains details about the jurisdictions that are defined in StoredIQ for Legal.

Column	Attribute Name	Type	Description
id	Jurisdiction ID	bigint	Uniquely identifies the jurisdiction.
creationdate	Creation Date	timestamp without time zone	Creation date of the jurisdiction
modifieddate	Modification Date	timestamp without time zone	Date when the jurisdiction information was last modified.
name	Name	character varying(250)	Name of the jurisdiction.
status	Status	character varying(512)	Status of the jurisdiction, which can be Active or Inactive.
code	Code	character varying(50)	The code associated with the jurisdiction.

### Request and collection log views (migrated data)

The request views provide information about the request migrated from IBM Atlas Policy Suite. The collection log view lists the entries that were made in the collection log in IBM Atlas Policy Suite.

### rep\_legal\_request\_view (Migrated Requests view)

The request view describes all requests within all matters. A request is the set of holds, collections, and interviews that are needed to fulfill a requirement to gather information about a matter.

Column	Type	Description
id	bigint	Unique identifier of the request in StoredIQ for Legal
creationdate	timestamp without time zone	Date when the request was created in StoredIQ for Legal
modifieddate	timestamp without time zone	Date when last modified in StoredIQ for Legal
description	character varying(2000)	Description of the request
reasonforchange	character varying(2000)	Reason for the latest modification of the request as described by the user
keywords	character varying(2000)	Value of the \$RequestKeywords variable
systemqueries	character varying(2000)	Value of the \$RequestSystemQueries variable
status	character varying(100)	Status of the request: in progress, inactive, completed
comments	character varying(2000)	Comments about the request

Column	Type	Description
pafield1	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield2	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield3	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield4	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield5	character varying(2000)	Custom field in IBM Atlas Policy Suite
interviewsrequired	character varying(1)	Indicates whether the matter includes virtual interviews (Y or N)
collectionsrequired	character varying(1)	Indicates whether the request is included in any collection plan (Y or N)
requestname	character varying(250)	Name of the request
iscompleteall	character varying(1)	Indicates whether the request is marked complete when the matter is closed, that is, when all notices are complete or closed (Y or Null)
matterrequestid	bigint	Unique ID of the request within the matter to which this request pertains
enddate	timestamp without time zone	Date and time when the request ended
startdate	timestamp without time zone	Date and time when the request started
requestid	bigint	Unique identifier of the request in IBM Atlas Policy Suite
document_modified_date	timestamp without time zone	The start date set in the <b>Document date range</b> field in the IBM Atlas Policy Suite UI
atlas_modifiedby	bigint	Person ID of the person who most recently modified the request in IBM Atlas Policy Suite
siq4l_modifiedby	bigint	Person ID in StoredIQ for Legal to which the value of the atlas_modifiedby field is mapped
atlas_legalmatterid	bigint	ID of the IBM Atlas Policy Suite matter to which this request pertains
atlas_createdby	bigint	Person ID of the person who created the request in IBM Atlas Policy Suite
document_created_date	timestamp without time zone	The end date set in the <b>Document date range</b> field in the IBM Atlas Policy Suite UI
changedate	timestamp without time zone	Date and time when the request was changed
siq4l_createdby	bigint	Person ID in StoredIQ for Legal to which the value of the atlas_createdby field is mapped



Column	Type	Description
createdon	timestamp without time zone	Date and time when the request was created in IBM Atlas Policy Suite
siq4l_legalmatterid	bigint	ID of the StoredIQ for Legal matter to which this request pertains
modifiedon	timestamp without time zone	Date and time when the request was last modified in IBM Atlas Policy Suite

#### rep\_scope\_element\_view (Migrated Requests Element Scope view)

Column	Type	Description
id	bigint	Unique identifier
creationdate	timestamp without time zone	Date when created in StoredIQ for Legal
modifieddate	timestamp without time zone	Date when last modified in StoredIQ for Legal
status	character varying(100)	Status of the target with regard to this request
pafield1	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield2	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield3	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield4	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield5	character varying(2000)	Custom field in IBM Atlas Policy Suite
reasonforinclusion	character varying(2000)	The reason for adding an element to the scope of the request as entered by the user
includerelatedds	bigint	Boolean value of the <b>Add Related Data Sources</b> checkbox when an organization or a schedule is added to the scope of a request
scopeelementid	bigint	Unique ID of the element added to the scope of the request
scopesysteminstanceid	bigint	Primary key of the object (Person, Org, DataSource, etc.) contained in this scope element
modifiedon	timestamp without time zone	Date and time when the scope element was last modified in IBM Atlas Policy Suite
atlas_modifiedby	bigint	Person ID of the person who modified the scope element in IBM Atlas Policy Suite
requestid	bigint	ID of the request that this element is part of
type	character varying(250)	Type of element
scopesystemobjecttype	bigint	System object ID of the record, for example: 1 = org unit, 2 = Person, 3 = Citation, etc.

Column	Type	Description
siq4l_modifiedby	bigint	Person ID in StoredIQ for Legal to which the value of the atlas_modifiedby field is mapped

#### rep\_scope\_target\_view (Migrated Requests Target Scope view)

Column	Type	Description
id	bigint	Unique identifier
creationdate	timestamp without time zone	Date when created in StoredIQ for Legal
modifieddate	timestamp without time zone	Date when last modified in StoredIQ for Legal
status	character varying(100)	Status of the target with regard to this request.
comments	character varying(2000)	Null
pafield1	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield2	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield3	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield4	character varying(2000)	Custom field in IBM Atlas Policy Suite
pafield5	character varying(2000)	Custom field in IBM Atlas Policy Suite
targetreason	character varying(4000)	Reason why the target is in scope
targetname	character varying(4000)	Name of the target at the time it was added to scope
targetemailid	character varying(4000)	Email address of the target (person) at the time he or she was added to scope
targetidentifier	character varying(4000)	Person identifier of the target (person) at the time he or she was added to scope
inuseinnotice	character varying(1)	Target is involved in a notice
targetdescription	character varying(4000)	Description of the target
inuseininterviewplan	character varying(1)	Target is involved in an interview
inuseincollectionplan	character varying(1)	Target is involved in a collection plan
ismanuallyadded	character varying(1)	Whether or not the target was added to the scope of the request manually
reasondeleted	character varying(2000)	Reason why the target was released from scope (if so)
isstewardordelegate	character varying(1)	Indicates whether the target is steward or a delegate (Y or N)

Column	Type	Description
inuseintransaction	character varying(1)	Indicates whether target (person) is in a preservation plan (Y or N)
targetorgunitname	character varying(2000)	Name of the organization
scopeelementid	bigint	Foreign key for the scopeelement table's scopeelement column
targetorgunitid	bigint	Identifier of the organization of the target
siq4l_modifiedby	bigint	Person ID in StoredIQ for Legal to which the value of the atlas_modifiedby field is mapped
atlas_modifiedby	bigint	Person ID of the person who released the target (if so) in IBM Atlas Policy Suite
nohold	bigint	Indicates whether the person is on hold (0) or not (1)
targetsysteminstanceid	bigint	Primary key of the scope target
requestid	bigint	ID of the request that this target is part of
releaseissued	bigint	Indicates whether the target is still in scope
otherpersonid	bigint	Person ID of the person in IBM Atlas Policy Suite that was added to the scope target
scopetargetid	bigint	Unique ID of the scopetarget row
modifiedon	timestamp without time zone	Day and time that the target was released from scope (if so)
draftrelease	bigint	Set to 1 if there is a release notice in draft state
createdon	timestamp without time zone	Day and time that the target was added to the scope of the request
targetsystemtype	bigint	System object ID of the record, for example: 1 = org unit, 2 = Person, 3 = Citation, etc.

#### rep\_collection\_interview\_log\_view (Migrated Requests Collection Logs view)

Column	Type	Description
id	bigint	Unique identifier for the collection log entry
creationdate	timestamp without time zone	Date when created in StoredIQ for Legal
modifieddate	timestamp without time zone	Date when last modified in StoredIQ for Legal
description	character varying(2000)	Description
pafield1	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield2	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield3	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI

Column	Type	Description
pafield4	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield5	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
actionplan	character varying(2000)	Null
enteredby	character varying(250)	Name of the person who created the log entry, or, in the case of a system-generated entry, for whom the entry was created
lognotes	character varying(4000)	Description of the event that is being logged, as composed by the log creator or by the system (for events such as the fulfillment of the collection request)
pafield6	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield7	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield8	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield9	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
pafield10	character varying(2000)	Custom field as available on the <b>MatterCollectionLog</b> page in the IBM Atlas Policy Suite UI
storedatlocation	character varying(2000)	Value of the <b>Stored In</b> field in the IBM Atlas Policy Suite UI (available only for a collection)
previouslyexported	character varying(1)	Indicates whether this collection log entry was exported previously
documentexists	character varying(1)	Indicates whether collection log entry has attachments
usercontent	character varying(1)	Reflects the selection for the <b>Is the Collection complete?</b> option in the IBM Atlas Policy Suite
submissionstatus	character varying(2000)	Completed (set internally)
ext_manifrst_uid	character varying(500)	Null (available only if external collections are used)
enteredbyid_name	character varying(2000)	
enteredbyid_email	character varying(2000)	
enteredbyid_pidenifier	character varying(2000)	
logtype	character varying(256)	Type of log: INTERVIEW or COLLECTION
logid	bigint	ID of the collection log
targetid	bigint	ID of the collection target
ext_collected_volume	bigint	For log entries that represent an external collection, the size of the collected information in bytes

Column	Type	Description
ext_page_count	bigint	For log entries that represent an external collection, the size of the collected information in pages
createdon	timestamp without time zone	
enteredon	timestamp without time zone	Day and time of the event for which this log entry was created
atlas_createdby	bigint	Person ID of the person who created the log entry in IBM Atlas Policy Suite
requestid	bigint	ID of the request that this collection log is part of
nextdate	timestamp without time zone	Null
achtransactionid	bigint	
resourcetype	bigint	ID of the resource type specified in the <b>Type</b> field in the IBM Atlas Policy Suite UI (available only for a collection)
ext_cost_enteredon	timestamp without time zone	Null (available only if external collections are used)
atlas_enteredbyid	bigint	Value of the <b>Conducted By</b> field in the IBM Atlas Policy Suite UI
fcevent	timestamp without time zone	Current date or Null
siq4l_createdby	bigint	Person ID in StoredIQ for Legal to which the value of the atlas_createdby field is mapped
dateconducted	timestamp without time zone	Day and time of the event that is described by the log entry
matterperformerid	bigint	Foreign key from the IBM Atlas Policy Suite MatterPerformer table
completed	bigint	Indicates whether the collection is marked complete
planid	bigint	ID of the collection plan

**rep\_collectioninterview\_log\_attachment\_view (Migrated Requests Collection Log Attachments view)**

Column	Type	Description
id	bigint	Unique identifier of the collection log attachment
logid	bigint	Unique identifier of the collection log entry to which the attachment belongs
requestid	bigint	ID of the request that this collection log attachment is part of
instanceid	bigint	ID of the collectioninterviewlog entity
entitydef	character varying(250)	Object type that the attachment is associated with, for example, Matter, Citation, PlanNote, and so on
requestpath	character varying(50)	
instanceidext	bigint	

Column	Type	Description
mimetype	character varying(250)	Mimetype that is associated with the attachment
filename	character varying(250)	File name of the attachment
attribname	character varying(250)	

### Security group views

The request views provide information about the request migrated from IBM Atlas Policy Suite. The collection log view lists the entries that were made in the collection log in IBM Atlas Policy Suite.

### rep\_securitygroups\_members\_view (Security Groups Members view)

This view lists all members of a security group.

Column	Type	Description
securitygroupid	bigint	Unique identifier of the security group in StoredIQ for Legal
persondistinctid	bigint	The ID that uniquely identifies a person

### rep\_securitygroups\_view (Security Groups view)

This view lists all security groups.

Column	Type	Description
id	bigint	Unique identifier
name	character varying(250)	Name of the security group
description	character varying(2000)	Description of the security group

### User role views

The User Role View lists the users of the system along with the role assignments.

### rep\_user\_roles\_view (User Role View)

Lists what roles each user has.

Column	Attribute Name	Type	Description
personID	Person ID	bigint	Uniquely identifies the person.
roleId	Role ID	bigint	Uniquely identifies the role.
roleName	Role Name	character varying(250)	Name of the role.
personLoginID	Person Login ID	character varying(50)	Unique signin ID of the person.
roleDescription	Role Description	character varying(2000)	Description of the role.

## Importing data by using the import API

Instead of manually creating or updating data in StoredIQ for Legal, you can import data from a CSV file. The import from a CSV file is helpful if you want to import a large amount of data. Also, specific data can be made available in StoredIQ for Legal only by importing it, such as data sources. Depending on the data, you import it from the command line or from the GUI. StoredIQ for Legal provides the import mappings, which contain the import configuration and map the columns in the CSV to the appropriate attributes in StoredIQ for Legal. In addition, it provides the import command line interface (CLI) to use for an import from the command line.

## Overview and basic concepts

Learn about the basic concepts of an data import by using the import API.

### Data to import: Target entities

You can import people, objects like matters, and relationships like role assignments. In the context of import, they are referred to as *target entities*.

The following tables provide an overview of the target entities that StoredIQ for Legal supports and of the method that is used to import them. For each target entity, only one import method is supported.

Name of target entity	Description	Supported import method
persondistinct	Create people in the catalog. Used to import large numbers of people where the initial import is typically followed by scheduled, incremental updates to keep the catalog of StoredIQ for Legal up-to-date.	Command line
persondistinct_adhoc	Create people in the catalog who are not regular employees of a company.	On the <b>All People</b> page in the catalog, click <b>Import</b> .
persondistinct_delete	Delete people from the catalog. Only persons that are not referred to can be deleted.	Command line

Name of target entity	Description	Supported import method
databox_custodians	Add people from the catalog as custodians to a data box.	On the <b>Custodians</b> page of a data box, click <b>Add from CSV</b> .
datarequest_custodians	Add people from the catalog as custodians to a data request.	On the <b>Custodians</b> page of a data request, click <b>Add from CSV</b> .
datarequest_custodians_adhoc	Create people in the catalog and add them as custodians to the data request.	On the <b>Custodians</b> page of a data request, click <b>Import People from CSV</b> .
interview_custodians	Add people from the catalog as custodians to an interview.	On the <b>Custodians</b> page of an interview, click <b>Add from CSV</b> .
interview_custodians_adhoc	Create people in the catalog and add them as custodians to an interview.	On the <b>Custodians</b> page of an interview, click <b>Import People from CSV</b> .
notice_custodians	Add people from the catalog as custodians to a hold notice.	On the <b>Custodians</b> page of a hold notice, click <b>Add from CSV</b> .
notice_custodians_adhoc	Create people in the catalog and add them as custodians to a hold notice.	On the <b>Custodians</b> page of a hold notice, click <b>Import People from CSV</b> .
notice_silent_custodians	Add people from the catalog as silent custodians to a hold notice.	On the <b>Custodians</b> page of a hold notice, click <b>Add Silent Custodians from CSV</b> .
notice_silent_custodians_adhoc	Create people in the catalog and add them as silent custodians to a hold notice.	On the <b>Custodians</b> page of a hold notice, click <b>Import People from CSV as Silent Custodians</b> .

Name of target entity	Description	Supported import method
orgtreehistory	Create or update the department hierarchy, including a record of all changes to the hierarchy.	Command line
personhistory	Create or update the employment history of a person.	Command line
persondistincthistory	Create the person information history.	Command line

Name of target entity	Description	Supported import method
datasource	Create or update data sources.	Command line
datasourceapplication	Create or update the applications that are associated with the data sources.	Command line
datasourceserver	Create or update the servers that are associated with the data sources.	Command line

Name of target entity	Description	Supported import method
fulfillment_detail	Add data sources to custodians and optionally, details about each fulfillment item.	On the <b>Custodians</b> page of a data request to be refined, click <b>More &gt; Add Data Sources from CSV</b> .
fulfillment_results	Add the results to each fulfillment item in the work package.	Open a work package from the appropriate task, then click <b>Add Results from CSV</b> .
jurisdiction	Create or update jurisdictions.	Command line
matter	Create or update matters, including sensitive matters and matters with a security group.  If you import matters that are associated with a security group, the core matter team does not necessarily have to be part of the assigned security group.	Command line
mattercategory	Create or update matter categories.	Command line
person_roles	Assign roles that are already defined to people who are already in the catalog.	Command line
securitygroup	Create or update security groups. The members of a security group must already be in the catalog.	Command line

### Import mappings

An import mapping contains the information necessary to import a specific target entity and to map the columns in the CSV file to the appropriate target entity attributes, which are stored in StoredIQ for Legal. A mapping can be reused and adapted to fit your needs. It is used by an import that is started from the



command line or from the GUI. StoredIQ for Legal supplies default mappings for specific target entities and mapping templates for all target entities. Use them to create custom mappings.

### ***Import mapping structure***

To adapt a default mapping or a mapping template to your needs or to create a custom mapping, you must understand the structure and the contents of a mapping.

An import mapping consists of several sections where each section contains a list of import mapping attributes. In the default mapping and the mapping template, the import mapping attributes are shown in a specific sequence. You can rearrange them within a section.

#### *Import mapping structure: General section*

The general section provides general information about an import mapping.

#### **mappingtype**

Currently, only CSV files are supported. Therefore, do not change the value.

#### **name**

The name of the import mapping. The name of a mapping template is *targetentityname\_template*. The name of a default mapping is *targetentityname\_default*. When you create a custom mapping, specify a unique name.

#### **description**

The description of the import mapping. This information is not used during the import.

#### **status**

Possible values are: TEMPLATE, DEFAULT, ACTIVE, and INACTIVE.

Default mappings have the status DEFAULT. Mapping templates have the status TEMPLATE. Do not change the status in a default mapping.

Mappings that are used for an import from the GUI must have a specific status. For more information, see [“Custom mappings for an import from the GUI” on page 178](#).

#### **targetentity**

The name of the target entity. Do not change the name.

#### *Import mapping structure: Feedback section*

The feedback section evaluates and complements the import results. You can view this information only if you have the necessary access rights. For more information, see [“Registering a client with the REST API” on page 179](#).

#### **feedbackaction**

The feedback to be returned.

Possible values are:

##### **CSV\_FAILED\_ITEMS**

Writes those CSV entries to a file where the import failed. For each entry, a reason for the failure is provided. This value can be included in the import mappings for all target entities.

##### **CSV\_IMPORT\_RESULT\_CUSTODIANS**

Writes the import results to a JSON file. This value can be included in the import mappings for the following target entities:

- databox\_custodians
- datarequest\_custodians
- interview\_custodians
- notice\_custodians
- notice\_silent\_custodians

##### **CSV\_IMPORT\_RESULT\_CUSTODIANS\_ADHOC**

Writes the results for an ad hoc import to a JSON file. This value can be included in the import mappings for the following target entities:

- databox\_custodians\_adhoc

datarequest\_custodians\_adhoc  
interview\_custodians\_adhoc  
notice\_custodians\_adhoc  
notice\_silent\_custodians\_adhoc

#### **CSV\_IMPORT\_RESULT\_JSON**

Writes the import result for each CSV entry, together with the contents of the CSV entry, to a JSON file. This value can be included in the import mappings of all target entities. However, do not use it for large imports where the number of CSV entries exceeds 1000. If an entry in the JSON file is too long, it is cropped.

#### **CSV\_IMPORT\_RESULT\_PERSONS\_ADHOC**

Writes the results for an ad hoc import of people to a JSON file. This value can be included in the import mappings for the following target entity: `persondistinct_adhoc`

#### **CSV\_NON\_EXISTENT\_CUSTODIANS**

Writes those CSV entries to a file where the reference to a custodian could not be resolved. Do not remove this value from the import mappings for the following target entities:

databox\_custodians  
datarequest\_custodians  
interview\_custodians  
notice\_custodians  
notice\_silent\_custodians

#### **CSV\_SKIPPED\_ITEMS**

Writes skipped CSV entries to a file. Mostly, skipped entries are duplicates. This value can be included in the import mappings for all target entries.

*Import mapping structure: Mappings section*

The mappings section defines which columns in the CSV file are mapped to which target entity attributes and how they are mapped.

### **Mapping attributes that are available in each mapping**

#### **attributename**

The name of the target entity attribute that is to be mapped. It shows the internal attribute name, which is the name under which the attribute is stored in the StoredIQ for Legal database.

#### **columnname**

The name of the CSV column that the target entity attribute is to be mapped to. In default mappings and mapping templates, the display name of the target entity attribute is shown. If the CSV file contains a different name for the column, specify that name here.

#### **mappingtype**

Possible values are `COLUMN_NAME` or `CONSTANT_VALUE`.

`COLUMN_NAME` specifies that the value from the CSV file is accepted. `CONSTANT_VALUE` specifies that a fixed value is expected, as defined for the `constantvalue` attribute.

#### **constantvalue**

Available only if `"mappingtype": "CONSTANT_VALUE"`. It specifies the fixed value for the target entity attribute.

### **Mapping attributes that might be available in addition**

#### **attributeinfo**

The settings for the target entity attribute, as shown in the GUI on the appropriate **Attributes** page, such as the string length or the items in a drop-down list.

#### **batchsize**

Specifies how many CSV entries are processed in one batch. A large number can accelerate processing. However, if an error occurs, all entries in the batch are considered as failed.

The default value is 200.

**dateformat**

The syntax for the date format. For information about the supported syntax, see [Java SimpleDateFormat syntax](#).

**maxfailures**

The number of errors that can occur across all batches before the import stops and is marked as failed. The default value is 1000.

**missingvalue**

The value that is used if a CSV column does not have a value. This attribute is often used with the *valuemappings subsection*. For more information, see [“valuemappings subsection” on page 173](#).

**unmappedvalue**

The value that is used if a CSV column has a value that cannot be mapped. This attribute must be used with the *valuemappings subsection*. For more information, see [“valuemappings subsection” on page 173](#).

**referencemapping subsection**

Used to resolve references to an item that is defined in another entity. An *entity* can be a target entity or an entity to which you add new items by using the GUI, such as *ilgrole*. The subsection contains the following attributes:

**lookupattribute**

The entity attribute that uniquely identifies an item. When you reference people, you can specify any person attribute that uniquely identifies them.

If the mapping template shows the variable `lookup identifier` as value, you must replace the variable with the unique identifier.

**lookupentity**

The entity that contains the referenced item.

**lookupfilter**

Filters the items to be searched. For example, when you import matters, paralegals must be assigned. You can define that only users are searched for paralegals instead of all people in the catalog. Your specification would look as follows:

```
"lookupfilter": "filter canlogon = true AND type = 'User'"
```

**Important:** The filter criteria must always start with the term `filter`.

**readallitems**

Possible values are TRUE or FALSE. TRUE specifies that a cache is built and populated with all items from the referenced entity. FALSE specifies that the cache includes only those items that resolve the references.

The default is FALSE if the `lookupentity` attribute contains the target entity `persondistinct`. The default is TRUE for all other entities.

**Tip:** Leave the default values unless you encounter performance problems.

**valuedelimiter**

The delimiter that is to be used if a CSV column contains more than one value. For example, when you assign roles to people by importing the target entity `person_roles`, all roles that one person receives must be specified in one CSV column and separated by the defined delimiter.

The default delimiter is the vertical bar (`|`).

**valuemappings subsection**

Used to replace the value that is found in the CSV file with a different value. It contains the following attributes:

**sourcevalue**

The value that is to be replaced.

## attributevalue

The value that is to be used instead.

You must use this subsection if your CSV file contains Boolean values. Boolean values must be replaced with strings because StoredIQ for Legal can interpret strings only.

You would also use this subsection, for example, to store a value with a data type other than String. All values in a CSV file are considered strings whereas the attributes that you define in StoredIQ for Legal can have a different data type.

Assume, for example, that you want to import people. StoredIQ for Legal needs to know whether a person can sign in. The Can Sign In attribute is a Boolean value of `true` or `false`. Also, assume that you decide to import people without sign-in information or with sign-in information that cannot be interpreted by StoredIQ for Legal, as people who cannot sign in. The specification can then look similar to the following one:

```
"attributename": "canlogon",
"columnname": "Can Sign In",
"mappingtype": "COLUMN_NAME",
"unmappedvalue": false,
"missingvalue": false,
"valuemappings": [
  {
    "sourcevalue": "TRUE",
    "attributevalue": true
  }
  {
    "sourcevalue": "FALSE",
    "attributevalue": false
  }
  {
    "sourcevalue": "1",
    "attributevalue": true
  }
  {
    "sourcevalue": "0",
    "attributevalue": false
  }
]
```

### Notes:

- If a value is found in the CSV file that is not covered by a `sourcevalue` definition, the value of the `unmappedvalue` attribute is used instead. If the `unmappedvalue` attribute does not exist, an error occurs. To avoid errors, it is good practice to always include the `unmappedvalue` attribute in the mappings section and set it to a default value or to `null` if a more appropriate value cannot be provided.
- If a CSV column does not have a value, the `missingvalue` value is used. If the `missingvalue` attribute is not defined, the affected target entity attribute is considered to have no value.

### *History-related import mappings*

The mappings section for the target entities `orgtreehistory` and `personhistory` contain a specific set of target entity attributes.

## Mappings section for `orgtreehistory`

### **nodeid**

The unique identifier of a department, such as a department number.

### **parentnodeid**

The unique identifier of the parent department, such as the department number.

### **managernodeid**

The unique identifier of the person who manages a department. If possible, use the value that is set as unique identifier in the system settings.

### **nodelabel**

The department name.

**nodetype**

Is always ORG\_UNIT.

**dateto**

The date until which the department hierarchy is valid. You set the start date when you import the department hierarchy. For rules and restrictions regarding this attribute, see [“Person-related imports” on page 186](#).

**Mappings section for personhistory****nodeid**

The unique identifier of an employee. If possible, use the value that you set for the `identityattribute` attribute.

**parentnodeid**

The unique identifier of the department that the employee belongs to. Use the same identifier as in the department hierarchy.

**managernodeid**

The unique identifier of the person who manages the employee. Use the same identifier as in the department hierarchy.

**nodelabel**

The name of the employee, such as the first name and the last name.

**nodetype**

Is always PERSON.

**dateto**

The end date of the employment. You set the start date when you import the employment history for a person. For rules and restrictions regarding this attribute, see [“Person-related imports” on page 186](#).

**Important:**

- Although the employment history and the department hierarchy are closely related, no cross-checks are made between the attributes of the two target entities. Thus, if you update the department hierarchy, you must also update the employment history.
- If you change the profile of a person in the GUI and that change affects the employment history or the department hierarchy, you must also update the employment history and the department hierarchy.

*Import mapping structure: Source file definition section*

The source file definition section describes the format and the structure of the source file. Unless your CSV file has a different structure, you can leave this section as provided by the default mapping or mapping template. Do not remove this section or any of its attributes.

**columnnumberrow**

The number of the row where the header starts.

**columnnamesource**

Can only be SOURCE. Do not change this value.

**headerrowcount**

The number of records in a header. If you set it to a number greater than 1, only the first header record is expected to hold the header information. All other header records are ignored.

**type**

The type of the file that can be imported. Currently, only CSV files are supported. Therefore, do not change this value.

For information about the CSV format, see [“Supported CSV format” on page 178](#).

*Import mapping structure: Target entity definition section*

The target entity definition section describes how to import the data and how to identify new and existing items.

Except for the `identityattribute` attribute, leave this section as provided by the default mapping or mapping template. Do not remove this section or any of its attributes.

The `identityattribute` attribute uniquely identifies a person. The following table shows which target entities use the `identityattribute` attribute and which target entities use the unique identifier that is specified in the system settings:

Target entity	identityattribute attribute	Person attribute from system settings
<code>databox_custodians</code>	X	
<code>datarequest_custodians</code>	X	
<code>datarequest_custodians_adhoc</code>		X
<code>fulfillment_detail</code>	X	
<code>fulfillment_results</code>	X	
<code>interview_custodians</code>	X	
<code>interview_custodians_adhoc</code>		X
<code>notice_custodians</code>	X	
<code>notice_custodians_adhoc</code>		X
<code>notice_silent_custodians</code>	X	
<code>notice_silent_custodians_adhoc</code>		X
<code>orgtreehistory</code>	X	
<code>person_roles</code>	X	
<code>persondistinct</code>		X
<code>persondistinct_adhoc</code>		X
<code>persondistinct_delete</code>	X	
<code>personhistory</code>	X	

**Note:** Since V2.0.3.1, the default import mappings that are supplied no longer contain the `identityattribute` attribute for target entries that use the person attribute from the system settings. If you still use V2.0.3.0 import mappings, remove the `identityattribute` attribute from the appropriate mappings.

### **Default mappings, mapping templates, and custom mappings**

A default mapping is available for specific target entities only whereas a mapping template can be generated for all target entities.

A *default mapping* is a prebuilt mapping that is delivered with StoredIQ for Legal. It is based on the minimum set of attributes that cannot be deleted for a target entity. Thus, a default mapping can always be used unchanged and is always ready to use. A default mapping is overwritten when the StoredIQ for Legal database schema is initialized, that is, each time the server is restarted. Therefore, do not edit a default mapping. Copy it instead, edit the copy, and then save the custom mapping under a new name.

A *mapping template* is built on the current database schema of StoredIQ for Legal. For target entities that describe the relationship between several objects, such as `person_roles` and `databox_custodians`, the mapping template has the same contents as the default mapping. For those target entities, the mapping template can always be used unchanged and is always ready to use. For all other target entities, the mapping template includes all attributes and attribute settings that are currently defined. If the mapping template contains references to items in other target entities, check the mapping template before you use it and edit it as necessary. If it does not contain any references, the mapping template can

be used unchanged until the list of attributes or the attribute settings change again. At any time, a mapping template can be edited to fit your needs.

Use a mapping template when no default mapping is available or to cover more attributes than the minimum set. Create custom mappings based on a default mapping or a mapping template.

You can retrieve a default mapping or mapping template at any time by using the import command line interface. For more information, see [“Creating the import mapping” on page 181](#).

When you import data from the command line, you can specify whether the default mapping, the mapping template, or a custom mapping is to be used. When you import data from the GUI, the default mapping is used by default. If you want to use a custom mapping, see [“Custom mappings for an import from the GUI” on page 178](#).

The following table shows for which target entities a default mapping is available and for which target entities the mapping template has the same contents as the default mapping.

<b>Name of target entity</b>	<b>Default mapping available</b>	<b>Mapping template equals default mapping</b>
databox_custodians	X	X
datarequest_custodians	X	X
datarequest_custodians_adhoc	X	X
datasource		
datasourceapplication		
datasourceserver		
fulfillment_detail	X	X
fulfillment_results	X	X
interview_custodians	X	X
interview_custodians_adhoc	X	X
jurisdiction		
matter	X	
mattercategory		
notice_custodians	X	X
notice_custodians_adhoc	X	X
notice_silent_custodians	X	X
notice_silent_custodians_adhoc	X	X
orgtreehistory	X	
person_roles	X	X
persondistinct	X	
persondistincthistory	X	
persondistinct_adhoc	X	X
persondistinct_delete	X	
personhistory	X	X
securitygroup		X

## Custom mappings for an import from the GUI

The following target entities are imported from the GUI:

databox\_custodians  
datarequest\_custodians  
datarequest\_custodians\_adhoc  
fulfillment\_detail  
fulfillment\_results  
interview\_custodians  
interview\_custodians\_adhoc  
notice\_custodians  
notice\_custodians\_adhoc  
notice\_silent\_custodians  
notice\_silent\_custodians\_adhoc  
persondistinct\_adhoc

When you create custom mappings for those target entities, follow these rules:

- The custom mapping must contain the same target entity as the default mapping or mapping template that the custom mapping is based on.
- Change the status in the custom mapping to ACTIVE so that the custom mapping is used for the import instead of the default mapping.
- For all target entities, except for `fulfillment_results`, one default mapping with a status of DEFAULT and optionally, one custom mapping with a status of ACTIVE are supported. All other custom mappings must have a status of INACTIVE.
- For `fulfillment_results`, you can create a custom mapping with a name of your choice and specify the mapping name in the fulfillment workflow. Only if no mapping name is found in the fulfillment workflow, the default import mapping is used.

### Supported CSV format

The format of the CSV files that is accepted by the import API of StoredIQ for Legal corresponds to the CSV format of Microsoft Excel. When you create a CSV file, follow the rules and observe the restrictions that apply to Excel files.

The following list gives an overview of the most important rules and restrictions:

- Use UTF-8 character encoding to create a CSV file that is independent of the operating system. Any byte order marks (BOMs) in the file are ignored.
- Use a comma to separate the individual values.
- If a comma is part of the value, include the value in double quotation marks. For example:  
"value4,5"
- If a double quotation mark is part of a value, escape it by duplicating it. For example:  
Robert ""Bob"" Doe
- Use the newline character `\n` or the carriage return character `\r` as record separator.
- Column names and values are case-sensitive.
- Empty lines are not ignored.
- Leading or trailing white space is not ignored. A white space is considered part of a value.
- The `headerrowcount` attribute in the source file definition section of an import mapping defines whether the CSV file can contain a header and specifies the number of records in a header. Even if you set the `headerrowcount` attribute to a number greater than 1, only the first header record is expected to hold the header information. All other header records are ignored.



## Importing the data

For each target entity, one import method is supported: import from the GUI or import by using the command line. For an overview, see [“Data to import: Target entities”](#) on page 169.

For an import from the GUI, the default mapping of the appropriate target entity is used. If the default mapping fits your needs, you only have to create the CSV file. Then, you can start the import. However, if you want to use a custom mapping instead or if you have to import a target entity from a command line, you must use the import command line interface (CLI) that StoredIQ for Legal supplies.

### Installing the import command line interface (CLI)

To use the command line, you must install the import CLI on your local computer or on the computer that you use to import data.

- Install Python 2.7.5 or later. If you want to use TLS 1.2, install Python 2.7.9 or later.

Use a 2.7 version. Version 3 is not supported.

- If the preferred installer program (PIP) is not installed with your Python version, also install PIP.

- Install the Requests package.

1. On the node where StoredIQ for Legal is installed, navigate to the directory where the CLI package is stored.

- StoredIQ for Legal (VM): Change to the `/siq/samples` directory.
- StoredIQ for Legal (Container): Change to the `IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_CLOUD/tools/siq41` directory

2. Download the file `siq41-cli-1.3.0.tar.gz` to the computer from which you want to import data into StoredIQ for Legal.

3. Change to the download directory and run the following command to install the import CLI:

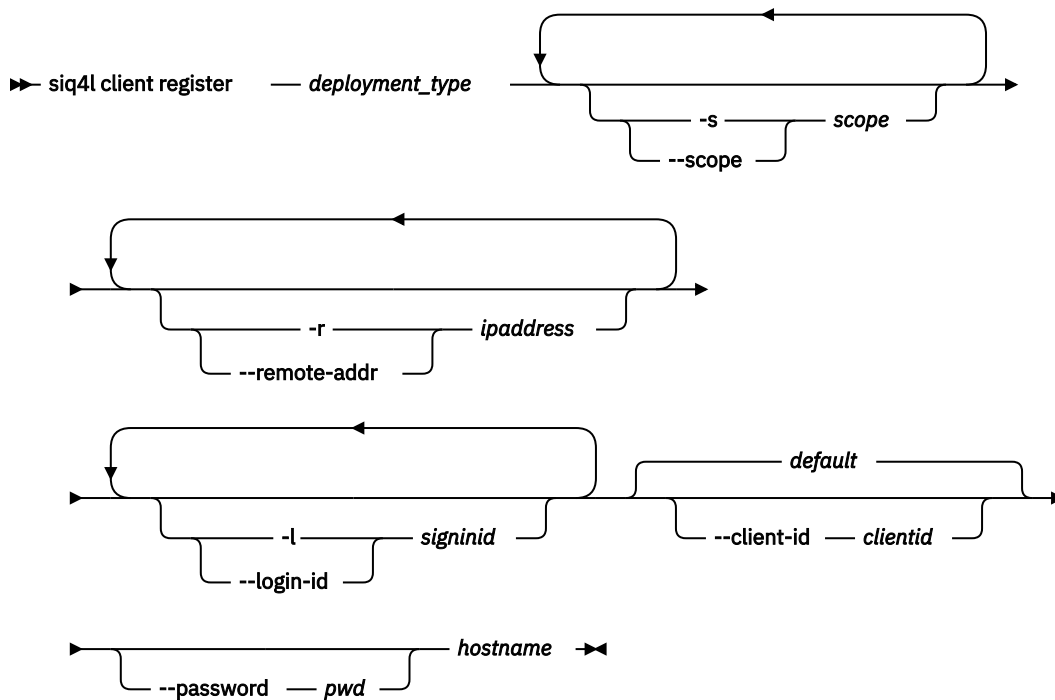
```
Python_install_dir\Scripts\pip install ./siq41-cli-1.3.0.tar.gz
```

The import CLI V1.3.0 is installed.

### Registering a client with the REST API

The import CLI uses specific endpoints of the REST API for managing import mappings, import requests, and import results. The REST API requires HTTP basic authentication. Therefore, you must register a client that is defined by a key (user name) and a secret (password) with the REST API. During registration, you can restrict the access to specific REST API endpoints, signin IDs, and IP addresses.

1. Open a command line.
2. Use the following syntax for your command:



Where:

***deployment\_type***

The StoredIQ for Legal deployment type, which can be **ova** or **openshift**.

**-s *scope***

**--scope *scope***

The first segment of a REST API endpoint path. You need access to the `/import` segment and optionally, the `/attachments` segment. Access to the latter is necessary for viewing the import results.

**-r *ipaddr***

**--remote-addr *ipaddr***

The IP address that the REST API can be accessed from. You can include a subnet mask. For example, specify `192.168.0.1/24` to cover the IP addresses 192.168.0.1 - 192.168.0.24.

**-l *signinid***

**--login-id *signinid***

The signin ID of the user to be authorized to access the REST API. As a minimum, the user must have the **Import: General** privilege. If the user is to import matters, the **Import: Matters** privilege is needed.

**--client-id *clientid***

The name for the client that you are registering. The default name is `default`.

**--password *pwd***

The password of user `ilgadmin`. If you do not specify it, you are prompted for it.

***hostname***

The fully qualified host name of the virtual machine (VM) where StoredIQ for Legal is deployed.

Example:

Assume that you want to give users with the signin IDs `procadmin` and `paralegal1` access to all import tasks and results from IP address `127.0.0.1`. Also, assume that StoredIQ for Legal is deployed as OVA on the VM `siq4l.myhost.yourserver.com`. You decide not to specify a name for

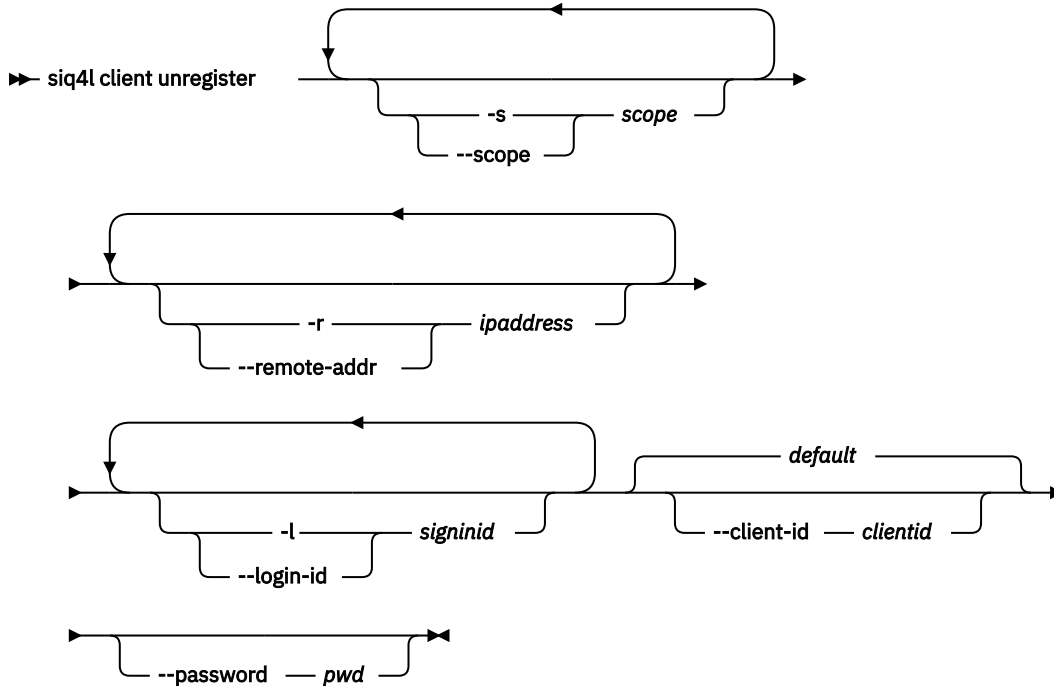
the client, and you want to be prompted for the ilgadmin password. Your command would then look as follows. Specify it on one line:

```
siq4l client register ova -s import -s attachment
-r 127.0.0.1 -l procadmin -l paralegal1
siq4l.myhost.yourserver.com
```

3. If you are prompted for the password for user ilgadmin, enter it.

The key, the secret, the deployment type, and the host name are saved to the following file: *clientid.credentials*.

4. At any time, you can unregister a client. Use the following syntax for your command:



5. At any time, you can enter `siq4l client --help` if you need help with one of the commands. For an overview of the REST API endpoints that are used, see [“Overview of commands and REST API endpoints”](#) on page 189.

### Creating the import mapping

Create an import mapping for each target entity that you want to import and reuse the mapping for as many import requests as possible.

- You must be signed in with the **Import: General** privilege.
- [“Default mappings, mapping templates, and custom mappings”](#) on page 176.
- Create the appropriate CSV file. For more information, see [“Supported CSV format”](#) on page 178.

The following procedure describes the steps that you are most likely to complete when you import data for the first time. For an overview of all commands relating to import mappings and of the REST API endpoints that are used, see [“Overview of commands and REST API endpoints”](#) on page 189.

**Important:** Do not create an import mapping from scratch. Always use a default mapping or mapping template as the basis.

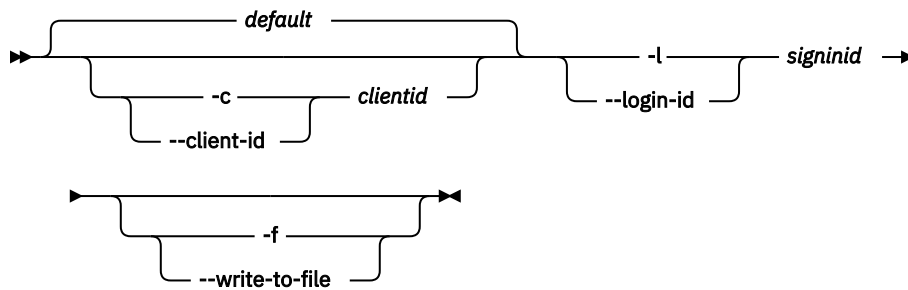
1. List all target entities that are supported by StoredIQ for Legal. See also [“Data to import: Target entities”](#) on page 169.

Complete this step after each upgrade of StoredIQ for Legal to get an overview of the currently supported target entities.

Use the following syntax for your command:

►► siq4l importmapping — list-target-entities — **OPTIONS** ◄◄

### OPTIONS



Where:

**-c *clientid***

**--client-id *clientid***

The client that accesses the REST API. The default name is `default`.

**-l *signinid***

**--login-id *signinid***

The signin ID of an authorized user. The user must have the **Import: General** privilege.

**-f**

**--write-to-file**

Writes the result to a JSON file.

- Retrieve the default mapping for the target entity that you want to import. If no default mapping is available or you want to import more attributes than the minimum set, retrieve the mapping template. For more information, see also [“Default mappings, mapping templates, and custom mappings” on page 176](#).

Retrieve the default mapping after each upgrade of StoredIQ for Legal to get an overview of its contents. If you use a mapping template, retrieve it after each attribute change to check whether adjustments are necessary.

- To retrieve the default mapping, use the following syntax for your command:

►► siq4l importmapping — get-default — **OPTIONS** — *target-entity-name* ◄◄

- To retrieve the mapping template, use the following syntax for your command:

►► siq4l importmapping — get-template — **OPTIONS** — *target-entity-name* ◄◄

Where:

***target-entity-name***

The name of the target entity.

For a description of the options, see step [“1” on page 181](#).

- Decide whether you can use the default mapping or the mapping template unchanged, whether changes are necessary, or whether you want to create a custom mapping based on the default mapping or the mapping template. Compare your import mapping to your CSV file to find out where in the mapping changes are necessary.

For guidance, see also [“Import mapping structure” on page 171](#).

- If you decide to create a custom mapping based on the default mapping or mapping template, you must make the custom mapping available for use. If you decide to change the mapping template, you must make the changed mapping available. See also [“Custom mappings for an import from the GUI” on page 178](#).

Use the following syntax for your command:

► siq4l importmapping — define — **OPTIONS** — file ►

Where:

**file**

The name of the import mapping file that is made available.

For a description of the options, see step “1” on page 181.

**Creating the mapping for adding custodians if the descriptor is set to a special person attribute**

When you add existing custodians to a hold notice, an interview, a data box, or a data request, which is an action that you complete from the GUI, the default import mapping is used. This mapping provides attribute mappings for the signin ID, the email address, and the person ID. If the descriptor, which is the person attribute that is used to identify a person in person selection lists, is set to a different person attribute, you must create a custom mapping. Otherwise, the descriptor is not displayed in the GUI. The following target entities are affected: databox\_custodians, datarequest\_custodians, interview\_custodians, and notice\_custodians.

The descriptor is set to an attribute other than the signin ID, the email address, or the person ID. For more information, see “Customizing attributes” on page 68.

Complete these steps:

1. If a custom mapping does not exist yet, copy the default import mapping of each affected target entity and save the copy under a unique name.
2. In the custom mapping, add the following attribute mapping to the mappings section:

```
{
  "attributename": "descriptor-attribute-name",
  "columnname": "corresponding-csv-columnname",
  "mappingtype": "COLUMN_NAME"
}
```

Where *corresponding-csv-columnname* stands for the name of the corresponding column in the CSV file.

Assume, for example, that the job title is used as descriptor. The internal name of that person attribute is *jobtitle*. Also, assume that the name of the CSV column that contains the job title of each custodian is *Descriptor*. Your specification would then look as follows:

```
{
  "attributename": "jobtitle",
  "columnname": "Descriptor",
  "mappingtype": "COLUMN_NAME"
}
```

3. Set the status in the custom mapping to ACTIVE and then save your changes.
4. Make the changes available for use.

If you created a custom mapping, use the `siq4l importmapping define` command. See step “4” on page 182. If you updated an existing custom mapping, use the `siq4l importmapping update` command.

In the CSV file, add a column with the descriptor values.

**Creating the mapping for adding information to a person record**

When you import persons, you can now directly create relationships by defining an alias in the mapping. You can also expand the mapping to include information about when and by whom a person record was changed. For this purpose, you must create a custom mapping for the *persondistinct* target entity that includes additional attributes.

Keep in mind that *modifiedon* and *modifiedby* information is used only when changes to a person record are automatically captured. Thus, these attributes are ignored unless automatic capture of person history changes is enabled.

Complete these steps:

1. If a custom mapping does not exist yet, copy the default import mapping of each affected target entity and save the copy under a unique name.
2. In the custom mapping, add the following attribute mappings to the mappings section:

```
{
  "attributename": "primaryalias",
  "columnname": "Primary Alias",
  "mappingtype": "COLUMN_NAME",
  "referencemapping": {
    "lookupattribute": "loginid",
    "lookupentity": "persondistinct"
  }
},
{
  "attributename": "modifiedon",
  "columnname": "modifiedon",
  "dateformat": "yyyy-MM-dd'T'HH:mm:ssZ",
  "mappingtype": "COLUMN_NAME"
},
{
  "attributename": "modifiedby",
  "columnname": "modifiedby",
  "mappingtype": "COLUMN_NAME",
  "referencemapping": {
    "lookupattribute": "loginid",
    "lookupentity": "persondistinct"
  }
}
}
```

3. Set the status in the custom mapping to ACTIVE and then save your changes.
4. Make the changes available for use.

If you created a custom mapping, use the `siq4l importmapping define` command. See step “4” on [page 182](#). If you updated an existing custom mapping, use the `siq4l importmapping update` command.

5. Add the columns to the CSV file.

#### **Creating the mapping for overriding global information when adding custodians to a data request**

When you add existing custodians to a data request, you might want to override the global information that applies to all custodians in the data request, with custom information. For each custodian, you can override the custodian priority, the date ranges, and the fulfillment instructions. For this purpose, you must create a custom mapping for the `datarequest_custodians` target entity that includes additional attributes.

Complete these steps:

1. If a custom mapping does not exist yet, copy the default import mapping of each affected target entity and save the copy under a unique name.
2. In the custom mapping, add the following attribute mappings to the mappings section:

```
{
  "attributename": "priority_cpx",
  "columnname": "corresponding-csv-columnname",
  "mappingtype": "COLUMN_NAME"
},
{
  "attributename": "dateranges_cpx",
  "columnname": "corresponding-csv-columnname",
  "mappingtype": "COLUMN_NAME"
},
{
  "attributename": "fulfillmentinstructions",
  "columnname": "corresponding-csv-columnname",
  "mappingtype": "COLUMN_NAME"
}
}
```

Where `corresponding-csv-columnname` stands for the name of the corresponding column in the CSV file.

3. Set the status in the custom mapping to ACTIVE and then save your changes.

4. Make the changes available for use.

If you created a custom mapping, use the `siq4l importmapping define` command. See step “4” on page 182. If you updated an existing custom mapping, use the `siq4l importmapping update` command.

5. Add the columns to the CSV file.

When you specify the values, keep the following in mind:

- The value that you provide for the `priority_cpx` attribute must match one of the values that are defined for the data request attribute `Custodian Priority`.
- Date ranges must be specified as a JSON array in the following format and on one line:

```
"[{ "start": "yyyy-MM-dd'T'HH:mm:ssZ", "end": "yyyy-MM-dd'T'HH:mm:ssZ" }, { ... } ]"
```

- For the `fulfillmentinstructions` attribute, provide a string. If the string contains special characters, enclose it in double quotation marks (").

### Importing the data by using the command line

To import data, the appropriate mapping file and CSV file must exist.

You must be signed in with the **Import: General** privilege. If you want to import a matter, you must be signed in with the **Import: Matters** privilege.

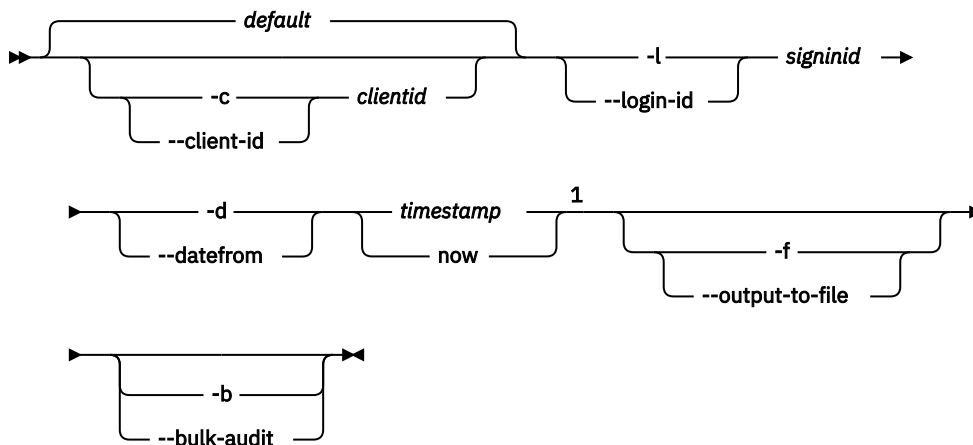
The following procedure describes the command that you probably use most often. For an overview of all commands relating to the import and of the REST API endpoints that are used, see “[Overview of commands and REST API endpoints](#)” on page 189.

Import requests are regularly cleaned up. Once a month, a scheduled task checks for import requests that are older than 1 month and deletes such import requests along with any associated attachments.

1. Open a command line.
2. Use the following syntax for your command:

```
► siq4l importrequest — run — OPTIONS — mappingid — file ►
```

#### OPTIONS



Notes:

<sup>1</sup> For target entities `orgtreehistory` and `personhistory` only

Where:

**-c *clientid***

**--client-id *clientid***

The client that accesses the REST API. The default name is `default`.

**-l *signinid***

**--login-id *signinid***

The signin ID of an authorized user. The user must have the **Import: General** privilege. To import matters, the **Import: Matters** privilege is needed.

**-d *timestamp***

**-d now**

**--datefrom *timestamp***

**--datefrom now**

The date and time when the department hierarchy or employment history becomes valid. Specify the time stamp in Coordinated Universal Time (UTC), in the following format:

*yyyy-MM-dd'T'HH:mm:ssZ*

When you specify now, the current time stamp in UTC format is applied.

For more information, see [“Rules and restrictions regarding history-related imports” on page 186.](#)

**-f**

**--output-to-file**

Writes the import progress and the results to files. The number of files returned and their contents depends on your specification in the feedback section of the import mapping.

For more information, see [“Import mapping structure: Feedback section” on page 171.](#)

***mappingid***

The ID of the import mapping to use.

***file***

The name of the import mapping file to use.

**-b**

**--bulk-audit**

Prevents recording of IMPORT\_REQUEST\_UPDATE and IMPORT\_REQUEST\_EXECUTION audit events for this import request.

The import request is run asynchronously. During the import, the JSON file is updated with the import status, any errors, and any problems with the CSV file. After the import is completed, the request is saved for reuse.

### ***Person-related imports***

Specific rules apply when you import data that references people, such as security groups, role assignments, employment histories, or department hierarchies.

### **Prerequisites**

- [“Importing people” on page 74.](#) The referenced people must exist in StoredIQ for Legal.
- If you want to find a person by searching departments, this person must be referenced in the department hierarchy. Import the department hierarchy (target entity *orgtreehistory*) before you import the employment history (target entity *personhistory*).

### **General remarks**

Depending on the amount of data to be processed, the import of person history records (target entity *persondistincthistory*) might take a while.

### **Rules and restrictions regarding history-related imports**

When you import an employment history or a department hierarchy, you must include the **datefrom** parameter in the import command. When you import an employment history for the first time, the **datefrom** parameter defines when this person became an employee of your company. Therefore, include only those new employees in a CSV file who have the same employment start date.

When you update an employment history or a department hierarchy, the **datefrom** parameter specifies when the changes took place. For example, if a department was renamed on 20 July 2016, you must



import the department hierarchy that reflects this change and all affected employment histories with a **datefrom** of 20 July 2016.

The CSV file must contain a column for the **date** values. The **date** attribute defines when the employment of a person ends or when a department is disbanded. When you import an employment history or a department hierarchy for the first time, leave the column empty. Specify the dates in a later import. However, remember that the dates cannot be changed after they are set.

If a person left the company and is reemployed later, you can import the employment history of this person again. Ensure that the date for the **datefrom** parameter is after the end date of the previous employment.

### Cleaning up history-related data

You can correct incorrect information that was introduced with the import of organization hierarchy or person information.

#### Cleaning up organization hierarchy data

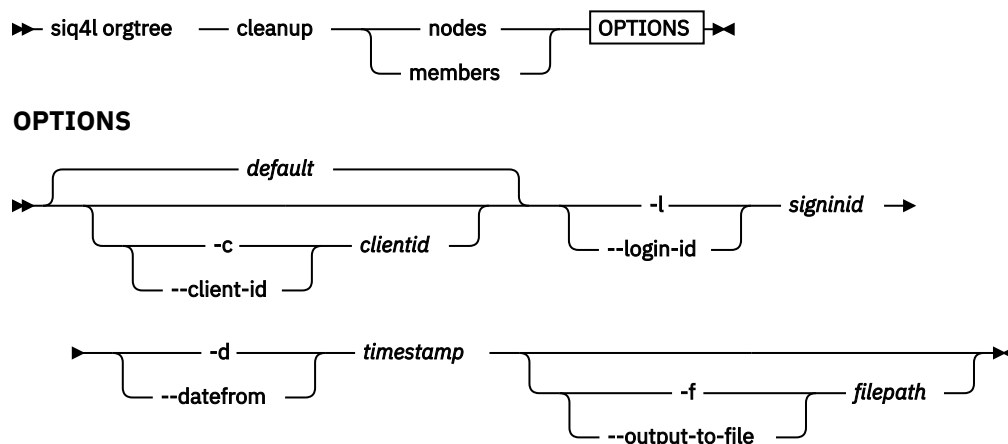
When you import the target entities **orgtreehistory** and **personhistory**, it can happen that you update or create a department or person by mistake. It can also happen that you become aware of this mistake only months later after several updates. You can restore the department hierarchy and the employment history to a specific state by removing all changes that you made on and after a specific time stamp.

You must be signed in with the **Import: General** privilege.

Always clean up both the department hierarchy and the employment history. If you have a large amount of data to clean up and want to avoid performance problems, do a multipart cleanup, where you go further back in time with each cleanup.

Use the following command. For the REST API endpoints that are used, see [“Overview of commands and REST API endpoints”](#) on page 189.

1. Open a command line.
2. Use the following syntax for your command:



Where:

#### nodes

Specifies that you want to clean up the department hierarchy.

#### members

Specifies that you want to clean up the employment history.

#### -c clientid

#### --client-id clientid

The client that accesses the REST API. The default name is `default`.

**-l *signinid***

**--login-id *signinid***

The signin ID of an authorized user. The user must have the **Import: General** privilege.

**-d *timestamp***

**--datefrom *timestamp***

The date and time that marks the beginning of the cleanup. Specify the time stamp in Coordinated Universal Time (UTC), in the following format:

*yyyy-MM-dd'T'HH:mm:ssZ*

**Important:** If you have a large amount of data to clean up, use a more recent time stamp for your first clean up, then gradually go back in time.

**-f**

**--output-to-file *filepath***

Writes the list of removed items to the specified file.

Assume that you have the signin ID `admin` and you want to remove all changes to the department hierarchy and the employment history that you made on or after 5 June 2014, 1 PM. Your commands would then look as follows. Specify them on one line.

```
siq4l orgtree cleanup nodes
-l admin -d 2014-06-05T13:00:00Z
-f c:\imports\cleanup-departments.csv
```

```
siq4l orgtree cleanup members
-l admin -d 2014-06-05T13:00:00Z
-f c:\imports\cleanup-employees.csv
```

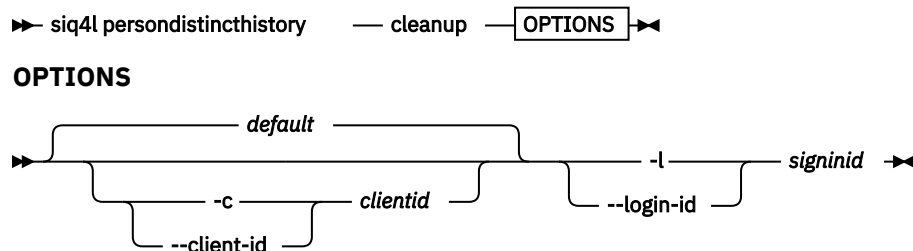
### **Cleaning up person information**

When you import the target entity `persondistincthistory`, it can happen that you update or create person information records by mistake. You can clean up that information if changes to person information are not automatically captured and no history of automatically captured attribute changes exists.

You must be signed in with the **Import: General** privilege.

Use the following command. For the REST API endpoint that is used, see [“Overview of commands and REST API endpoints”](#) on page 189.

1. Open a command line.
2. Use the following syntax for your command:



Where:

**-c *clientid***

**--client-id *clientid***

The client that accesses the REST API. The default name is `default`.

**-l *signinid***

**--login-id *signinid***

The signin ID of an authorized user. The user must have the **Import: General** privilege.

## Overview of commands and REST API endpoints

Each command that you enter by using the import CLI uses a REST API endpoint. The following table provides an overview of all commands that the import CLI accepts and the appropriate REST API endpoint call.

### Registering and unregistering a client

Task	Command	REST API endpoint call
Register a client	<pre>siq4l client register deployment_type</pre> <p>For more information about this command, see <a href="#">“Registering a client with the REST API” on page 179</a>.</p>	<pre>POST /security/registerClient {   "scopes": scopelist,   "remoteaddr": ipaddress-list,   "loginids": signinid-list, }</pre> <p>Example:</p> <pre>POST /security/registerClient {   "scopes": ["import", "attachment"],   "remoteaddr": "127.0.0.1"   "loginids": ["procadm", "paralegal1"], }</pre> <p>A JSON file is returned, which contains the key and the secret. Store the file in a safe place.</p>
Unregister a client	<pre>siq4l client unregister</pre> <p>For more information about this command, see <a href="#">“Registering a client with the REST API” on page 179</a>.</p>	<pre>POST /security/unregisterClient {   "key": "client-key",   "secret": "client-secret", }</pre>

### Commands for creating and managing the import mappings

Task	Command	REST API endpoint call
List all target entities that StoredIQ for Legal supports	<pre>siq4l importmapping list- target-entities</pre> <p>For more information about this command, see <a href="#">“Creating the import mapping” on page 181</a>.</p>	GET /import/mappings/targetentities
List all available mappings, together with their mapping IDs	<pre>siq4l importmapping list</pre> <p>For more information about this command, enter the following command:</p> <pre>siq4l importmapping list --help</pre>	GET /import/mappings
Make a new mapping available for use	<pre>siq4l importmapping define</pre> <p>For more information about this command, see <a href="#">“Creating the import mapping” on page 181</a>.</p>	POST /import/mappings/mappingid

<b>Task</b>	<b>Command</b>	<b>REST API endpoint call</b>
Make a changed mapping available for use	siq4l importmapping update For more information about this command, enter the following command: siq4l importmapping update --help	PUT /import/mappings/mappingid
Retrieve a mapping by its ID	siq4l importmapping get For more information about this command, enter the following command: siq4l importmapping get --help	GET /import/mappings/mappingid
Retrieve a default mapping for a specific target entity	siq4l importmapping get-default For more information about this command, see <a href="#">“Creating the import mapping”</a> on page 181.	GET /import/mappings/defaults/targetentityname
Retrieve a mapping template for a specific target entity	siq4l importmapping get-template For more information about this command, see <a href="#">“Creating the import mapping”</a> on page 181.	GET /import/mappings/templates/targetentityname
Delete a mapping	siq4l importmapping delete For more information about this command, enter the following command: siq4l importmapping delete --help	DELETE /import/mappings/mappingid

#### Commands regarding the import of data

<b>Task</b>	<b>Command</b>	<b>REST API endpoint call</b>
Import data	siq4l importrequest run For more information about this command, see <a href="#">“Importing the data by using the command line”</a> on page 185.	The following series of calls: 1. POST /import/requests 2. POST /import/requests/requestid/start 3. GET /import/requests/requestid/status Repeat this call until the status is COMPLETE or FAILED.
List all import requests	siq4l importrequest list For more information about this command, enter the following command: siq4l importmapping list --help	GET /import/requests

Task	Command	REST API endpoint call
Retrieve a specific import request	<pre>siq4l importmapping get</pre> <p>For more information about this command, enter the following command:</p> <pre>siq4l importmapping get --help</pre>	GET /import/requests/ <i>requestid</i>
Delete an import request	<pre>siq4l importmapping delete</pre> <p>For more information about this command, enter the following command:</p> <pre>siq4l importmapping delete --help</pre>	DELETE /import/requests/ <i>requestid</i>

### Cleaning up history-related data


Task	Command	REST API endpoint call
Clean up the department hierarchy	<pre>siq4l orgtree cleanup nodes</pre> <p>For more information about this command, see <a href="#">“Cleaning up organization hierarchy data”</a> on page 187.</p>	<pre>POST /orgtreenodes/cleanup {"datefrom": "timestamp"}</pre> <p>Example:</p> <pre>POST /orgtreenodes/cleanup {"datefrom": "2014-01-01T00:00:00Z"}</pre>
Clean up the employment history	<pre>siq4l orgtree cleanup members</pre> <p>For more information about this command, see <a href="#">“Cleaning up organization hierarchy data”</a> on page 187.</p>	<pre>POST /orgtreemembers/cleanup {"datefrom": "timestamp"}</pre> <p>Example:</p> <pre>POST /orgtreemembers/cleanup {"datefrom": "2014-01-01T00:00:00Z"}</pre>
Clean up the person history	<pre>siq4l persondistincthistory cleanup</pre> <p>For more information about this command, see <a href="#">“Cleaning up person information”</a> on page 188.</p>	DELETE /personhistory


## Exporting lists as CSV

You can export the lists of matters, tasks, custodians, or persons that are displayed in StoredIQ for Legal, as CSV files. In addition, you can export details about the matters that a custodian is involved in. The CSV files can then be used outside StoredIQ for Legal, for example, as attachments to emails.



You must be signed in with the appropriate **View** privilege.

The CSV files contain the following information:

- For matters, all matter attributes, including any custom matter attributes.
- For tasks, the entire information that is available about the tasks.
- For custodians, all the details that are displayed to you in the GUI. You can show and hide details by using the **Select columns** list .

- For a single custodian, the matters that this custodian is involved in, including the number of hold notices, interviews, and data requests.
- For persons in the people and group catalogs, all the details that are displayed to you in the GUI. You can show and hide details by using the **Select columns** list .

To export the list of matters that a custodian is involved in, see “[Viewing a person's hold obligations and involvement in matters](#)” on page 83. To export all other lists, complete the following steps:

1. Start as follows:
  - To export the list of matters, click **Matters**.
  - To export the list of tasks, click **Tasks**.
  - To export the list of custodians, go to any GUI page that lists custodians.
  - To export the list of persons, go to any GUI page under **Catalog > People**.
2. If you want to export a list of custodians or persons, make all the details visible that you want to include in the CSV file. Use the **Select columns** list .
3. Optional: If you want to export only specific matters, tasks, or custodians, reduce the list to be exported by using **Advanced Search**.
4. Click the **Export as CSV** icon .

The CSV file is created and stored at the specified location.

## Migrating IBM Atlas Policy Suite data

---

When moving from IBM Atlas Policy Suite to IBM StoredIQ for Legal, migrate existing notice, interview, and request data.

After the migration, legacy and active IBM Atlas Policy Suite hold notices, interviews, and requests are available in IBM StoredIQ for Legal and can then be managed here.

Release notices can be migrated for reference purposes.

### Overview and basic concepts

You can migrate notices (as of IBM StoredIQ for Legal version 2.0.3.5), interviews (as of version 2.3.0.7), and requests (as of version 2.0.3.8) from IBM Atlas Policy Suite 6.0.3.3 to IBM StoredIQ for Legal .

A migration tool is provided with StoredIQ for Legal and is run on the IBM StoredIQ for Legal system. Not all steps of the migration process are automated. Some manual preparation and validation steps are required.

Connectivity between the IBM Atlas Policy Suite system and the IBM StoredIQ for Legal system is provided through a JDBC driver.

You can select whether you want to migrate all notices, interviews, or requests existing in the IBM Atlas Policy Suite system, notices, interviews, or requests that are specific to certain matters, or just choice notices, interviews, or requests. However, the respective matters and involved persons must exist in IBM StoredIQ for Legal before you can migrate any items.

When you start the migration, the notices and interviews are extracted along with their custodians and their transmission and response records, transformed, and inserted into the staging database (named staging). For requests, scope information and the interview logs retrieved and added to the staging database. The content of the staging database is then migrated to IBM StoredIQ for Legal. To view the content of the staging database, you can access the database in PostgreSQL with user name `importuser` and password `passwd`. Each migration run clears the existing content from the staging database.

Some of the notice and interview attributes that are available in IBM Atlas Policy Suite are not readily available in IBM StoredIQ for Legal. Any such attribute is either mapped to the closest match in IBM StoredIQ for Legal or a corresponding custom attribute is created in IBM StoredIQ for Legal during migration. For details, see “[System and request variable mappings](#)” on page 197.

After the custom attributes are created in IBM StoredIQ for Legal, the selected hold notices or interviews are migrated. If you want to migrate notices or interviews with the same name stemming from different data requests, you can avoid name clashes by setting a specific configuration option.

For each notice or interview, transmission and response records are also migrated. Such records are written to CSV files, at least one for the transmission history (`transmission_history.csv`) and one for the response history (`response_history.csv`). If the number of records to be migrated exceeds the defined maximum size of the CSV file, the records are written to multiple files. The files are then numbered sequentially. The CSV files containing the history are added to the migrated notice or interview as one or more attachments. The layout of the CSV files matches the layout of the IBM Atlas Policy Suite reporting views. You can look up the column names in the [topic about reporting views](#) in the IBM Atlas Policy Suite documentation.

You must verify the migrated notices and interviews manually in the migration portal before they are set to the status they had in IBM Atlas Policy Suite and, if required, any notifications are sent. Note that the migration portal provides access only to notices and interviews in matters to which you have access; so, this might not be all migrated items. After notices or interviews are verified and have the appropriate status set, they become available in the regular matter and notices or interview lists. Be aware that although IBM Atlas Policy Suite allows the same attachment to be added to a notice multiple times, only one instance of the attachment will be available in the notice after the migration. A respective warning is written to the log file in such a case. Be sure to check this log, especially when multiple attachments with same name were added to an IBM Atlas Policy Suite notice from different machines or locations.

When requests are migrated, the content of the following IBM Atlas Policy Suite database tables is migrated:

- LegalRequest
- Scopetarget
- Scopeelement
- Collectioninterviewlog

Only records where `logtype` is `interview` are migrated.

To verify migrated requests in IBM StoredIQ for Legal, you can use the provided reporting views.

An audit record is written at the start and at the end of the migration, and when notices or interviews are verified. At the end of a migration run, a status summary is displayed that shows the total number of eligible items, the counts of migrated or skipped items, and of items for which migration failed.

For reference purposes, release notices can also be migrated although IBM StoredIQ for Legal does not support this concept. When you verify a migrated release notice in IBM StoredIQ for Legal, its status changes as shown in the following table.

In IBM Atlas Policy Suite, an interview has an interview plan status and an interview sent status. The concept of an interview plan does not exist in IBM StoredIQ for Legal. Therefore, the respective status is mapped to a custom attribute in IBM StoredIQ for Legal.

Statuses of notices and interviews are mapped as shown in the following table. Requests have the same status in IBM StoredIQ for Legal that they had in IBM Atlas Policy Suite: in progress, inactive, or completed.

Table 9. Status mapping for notices and interviews

Status in IBM Atlas Policy Suite	Status in IBM StoredIQ for Legal	Notes for hold notices	Notes for Release notices	Interviews
Drafted	Draft		Custodians are migrated as active custodians. When you verify the migrated notice, the custodians stay active. You must release them manually after publishing the notice.	
Approved	Draft			
Rejected	Draft			
Pending approval	Draft			
Published	Published		Custodians are migrated as active custodians. When you verify the migrated notice, the custodian status is changed to released. However, no notification email is sent to the custodians.	
Sent	Published	A notice with this status is published as soon as it's verified and is thus re-issued to all the custodians involved in the notice. If the notice rules require confirmation, the custodians must re-respond even if they already responded to the IBM Atlas Policy Suite notice.		
Error	Published			
Suspended	Suspended	If such a notice is resumed in IBM StoredIQ for Legal, any reminders or follow-up messages are scheduled based on the settings available when the notice was resumed.		
Modified	Closed			Not applicable.



Table 9. Status mapping for notices and interviews (continued)

Status in IBM Atlas Policy Suite	Status in IBM StoredIQ for Legal	Notes for hold notices	Notes for Release notices	Interviews
Inactive	Closed	Because draft notices don't have transmission records, the initial sent date for inactive draft notices will not have a value after the migration.		

### Migration prerequisites

Before you start the migration, check these prerequisites and make sure that all requirements are met.

#### Disable timer tasks in IBM Atlas Policy Suite

In IBM Atlas Policy Suite, the following timer tasks must be disabled to ensure that no more notifications are sent as soon as the migration is started:

- AlertEmail Sender task
- Email Receiver task
- Notice Sender task
- Send ReminderNotice task

To disable these tasks:

1. In the IBM Atlas Policy Suite web client, go to **Admin > Timer Task Configuration** and click **Edit**.
2. Clear the **Active** checkbox for each listed task and save your changes.

The tasks are now inactive and will no longer be executed.

**Important:** Leave those tasks permanently disabled.

#### Verify allowed attachment size and types

The maximum allowed document size for an attachment must be the same in both systems. Check the size in both systems and adjust the setting in IBM StoredIQ for Legal if required:

- In IBM Atlas Policy Suite, go to **Admin > Components > Document Library** and check the setting of the **MAXIMUM\_UPLOAD\_SIZE** parameter.
- In IBM StoredIQ for Legal, go to **Admin > System Settings** and check the size setting under **File Attachments**. The size value must be at least the same value as in IBM Atlas Policy Suite.

You must be signed in with the **System: Manage** privilege to do so.

You might also need to add file types to the current set of supported file types. To add file extensions, update the file extension whitelist as follows.

#### StoredIQ for Legal (VM)

1. Sign in to the IBM StoredIQ for Legal VM as root.
2. Open the WebSphere Application Server container by running this command:

```
docker exec -it ilg_sol_plugin bash
```

3. Stop the application server by running this command:

```
systemctl stop was
```

4. Edit the `/home/was/WebSphere/AppServer/profiles/ilgnext/config/cells/websphereNode01Cell/applications/ilg-sol-rest.ear/deployments/ilg-sol-rest/ilg-sol-rest.war/WEB-INF/web_merged.xml` file.
5. Locate the `<param-name>whitelist</param-name>` entry in `<context-param>` section. Check the value of the matching `<param-value>` entry and add file extensions as required.
6. Start the application server again by running this command:

```
systemctl start was
```

7. Sign out of the IBM StoredIQ for Legal VM.

### StoredIQ for Legal (Container)

Complete these steps on an OpenShift client that has access to the cluster where IBM StoredIQ for Legal is deployed.

1. Obtain the name of the `ilg-sol-plugin` container by running this command:

```
CONTAINER_NAME=$(oc get pods -n siq4lopernsift -l app=ilg-sol-plugin -o name | sed "s/^\{4\}//" )
```

2. Open the `ilg-sol-plugin` container by running the following command. Replace `$CONTAINER_NAME` with the name returned in the previous step.

```
oc exec -it $CONTAINER_NAME bash
```

3. Stop the application server by running this command:

```
systemctl stop was
```

4. Edit the `/home/was/WebSphere/AppServer/profiles/ilgnext/config/cells/websphereNode01Cell/applications/ilg-sol-rest.ear/deployments/ilg-sol-rest/ilg-sol-rest.war/WEB-INF/web_merged.xml` file.
5. Locate the `<param-name>whitelist</param-name>` entry in `<context-param>` section. Check the value of the matching `<param-value>` entry and add file extensions as required.
6. Start the application server again by running this command:

```
systemctl start was
```

### Activate the migration portal

You must activate the migration portal before you or other users with the **Notice: Manage** privilege can access it:

1. Go to **Admin > System Settings**.
2. Under **Migration**, select to show the migration portal.

### Ensure the required matters and persons exist in IBM StoredIQ for Legal

The matters that are to hold the migrated notices or interviews must exist in IBM StoredIQ for Legal and must be active before you start the migration. Also, all persons who are involved in the notices or interviews to be migrated must be available in IBM StoredIQ for Legal. Note that persons are mapped based on email address.

If any custodian of a notice or interview to be migrated does not exist in the IBM StoredIQ for Legal catalog, the notice or interview is still migrated but an error message is written to the migration log files. For such a notice or interview, the "IBM Atlas Policy Suite to staging database" migration step is considered failed, and the "staging database to IBM StoredIQ for Legal" migration step is considered passed.

### System and request variable mappings

A set of IBM Atlas Policy Suite system variables are directly mapped to IBM StoredIQ for Legal system variables. For some system variables, there is no one-to-one mapping. Some system variables cannot be mapped at all.

#### 1:1 mapping

IBM Atlas Policy Suite system variable	IBM StoredIQ for Legal system variable
\$CourtesyCopyRecipients	{Courtesy copy recipients} (notices only)
\$EmployeePortalURL	{Link to custodian portal}
\$interviewurl	{Link to interview}
\$Login	{Signin ID}
\$MatterAttorney	{Attorney name}
\$MatterAttorneyEmail	{Attorney email address}
\$MatterDescription	{Matter description}
\$MatterID	{Matter ID}
\$MatterLegalAssistant	{Paralegal name}
\$MatterLegalAssistantEmail	{Paralegal email address}
\$MatterName	{Matter name}
\$NoticeName	{Notice name} or {Interview name} depending on the type of notice that is migrated
\$NoticeRecipientName	{Custodian name}
\$NoticeResponseURL	{Link to confirmation page} (notices only)
\$RecipientNames	{Custodian list: names}
\$Recipients	{Custodian list: email addresses}
\$ResentNoticeNumber	{Follow-up count} (notices only)

#### No 1:1 mapping or no mapping at all

The names of custom notice or interview attributes that are created in IBM StoredIQ for Legal for mapping IBM Atlas Policy Suite system variables are derived from the variable name in IBM Atlas Policy Suite and prefixed with `atlas`.

IBM Atlas Policy Suite system variable	Mapping in IBM StoredIQ for Legal
\$collectionurl	Not mapped
\$ConfirmationBasedScope	{Link to confirmation page} (notices only)
\$ConfirmationInstruction	Mapped based on the value in IBM Atlas Policy Suite
\$interviewurlview	{Link to interview}
\$emailConfirmation	Not mapped
\$EnterPasswordURL	Not mapped
\$Image1	The respective IBM Atlas Policy Suite image is inserted into the IBM StoredIQ for Legal template.

IBM Atlas Policy Suite system variable	Mapping in IBM StoredIQ for Legal
\$MatterCustom1-5	Mapped to custom attributes of the notice or interview
\$Q:FullyComply	{Link to confirmation page} (notices only)
\$RequestDescription	Mapped to a custom attribute of the notice or interview
\$RequestDueByDate	Mapped to a custom attribute of the notice or interview
\$RequestID	Mapped to a custom attribute of the notice or interview
\$RequestKeywords	Mapped to a custom attribute of the notice or interview
\$RequestName	Mapped to a custom attribute of the notice or interview
\$RequestStartDate	Mapped to a custom attribute of the notice or interview
\$RequestSystemQueries	Mapped to a custom attribute of the notice or interview
\$ResetPasswordURL	Not mapped

### The migration tool

With the **migrate.py** tool, you can migrate your data in full or partially, and do the required cleanup after migration is complete. The tool also provides logging for the migration process. The tool must be run from the Python interpreter.

You can find the tool in the `/siq/migration` directory on your StoredIQ for Legal (VM) system and in the `IBM_STOREDIQ_FOR_LEGAL_Vu.r.m.fp_CLOUD/tools/migration` directory for StoredIQ for Legal (Container). This directory holds the following content:

- The `jdbc_drivers` subdirectory that holds the appropriate IBM Atlas Policy Suite JDBC driver:
  - `ojdbc6.jar` for an Oracle database
  - `db2jcc.jar` and `db2jcc_license_cu.jar` for a Db2 database (Supported Db2 versions are version 10.5 and later.)

**Important:** This directory is initially empty. You must store a copy of the driver here before you can start migration.

- The **migrate.py** migration tool
- The `log4j.properties` file containing the logging configuration
- The `logs` subdirectory to which any output is written that is generated during the migration:
  - `migration.log`, which contains general log information for each run of the migration tool. Note that this file is overwritten with each run.
  - One or more *date* subdirectories, where *date* is the date on which the migration tool was run and the log files were generated. Each of these directories contains this set of files:
    - `atlas_to_siq41_timestamp.log`, which contains information about the data that was successfully retrieved from IBM Atlas Policy Suite and put into the staging database. For example, it might list what notices, interviews, and requests were retrieved and transformed to that they can be migrated. It also includes information about the data processed in the migration step from the staging database to IBM StoredIQ for Legal. Consider this log file the complete migration output log.

In addition to any migration information, this log file also holds information pertaining to the deletion of migrated requests.

You can configure the level of detail for the logging in the `log4j.properties` file in the parent `/siq/migration` directory.

- `atlas_to_staging_summary_status_timestamp.txt`, which contains the statistics for the "IBM Atlas Policy Suite to staging database" migration step, for example:

```
===== Hold Notice Migration Summary =====
Total Count   Failed Count   Passed Count
25             19                6
===== Interview Migration Summary =====
Total Count   Failed Count   Passed Count
15             3                12
===== Request Migration Summary =====
Total Count   Failed Count   Passed Count
4              0                4
```

- `staging_to_siq41_summary_status_timestamp.txt`, which contains the statistics for the "staging database to IBM StoredIQ for Legal" migration step, for example:

```
Hold Notice Migration Summary
Total Count   Failed Count   Skipped Count   Passed Count
25             19                0                6
Interview Migration Summary
Total Count   Failed Count   Skipped Count   Passed Count
15             3                0                12
Request Migration Summary
Total Count   Failed Count   Skipped Count   Passed Count
4              0                0                4
```

- `request_deletion_summary_status_timestamp.txt`, which contains the statistics for the deletion request, for example:

```
Request Deletion Summary Status
===== LegalRequest Deletion Summary Stats =====
Total Count   Failed Count   Passed Count
17             2                15
```

- `failed_notices_timestamp.csv`, which lists the notices that could not be retrieved from IBM Atlas Policy Suite to be put into the staging database.
- `failed_interviews_timestamp.csv`, which lists the interviews that could not be retrieved from IBM Atlas Policy Suite to be put into the staging database.
- `failed_requests_timestamp.csv`, which lists the requests that could not be retrieved from IBM Atlas Policy Suite to be put into the staging database.
- `failed_delete_requests_timestamp.csv`, which lists the requests that could not be deleted from IBM StoredIQ for Legal.

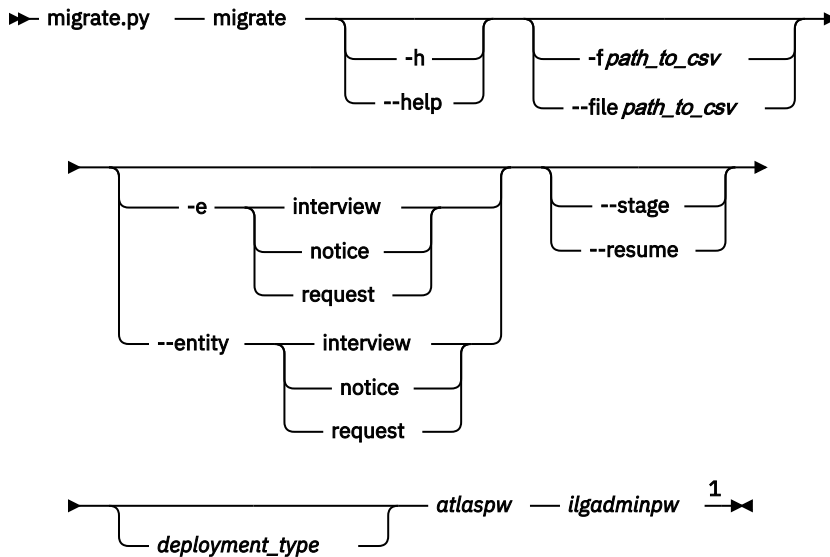
The tool requires the `migration_configuration.json` migration configuration file to be present in the `/siq/conf` directory (for details, see [“The migration configuration file”](#) on page 202).

## Basic syntax

The command syntax for the migration tool is as follows:

```
➤ migrate.py [ -h | --help ] subcommand ➤
```

## Command-specific syntax: migrate



Notes:

<sup>1</sup> `deployment_type`, `atlaspw` and `ilgadminpw` are positional parameters.

Where:

**-h**

**--help**

Displays help information.

This parameter is optional.

**-f path\_to\_csv**

**--file path\_to\_csv**

Specifies the path to a CSV file containing the list of items to migrate. The CSV file must contain two columns. The first column is for holding a reference to the matter ID (`matterId`), which is not mandatory. The second column is for holding a reference to the notice ID (`noticeId`) for notices and interviews, or the request ID (`requestId`) for requests. If you omit the matter ID, you must specify a notice ID or a request ID. If you specify just the matter ID, all entities of the type specified with the `-e` option are migrated for this matter. The first row of the CSV file is considered the header and is ignored during processing.

To migrate a selected set of notices, interviews, requests run the tool with the **--stage** option and specify the **--entity** parameter.

Depending on your selection for the **--entity** parameter, the following objects are migrated for a `noticeId` associated with a hold notice containing a virtual interview :

- The tool is run without the **--entity** option: both the hold notice and the interview are migrated as separate objects.
- The tool is run with **--entity notice**: only the hold notice is migrated for this `noticeId`.
- The tool is run with **--entity interview**: only the interview is migrated for this `noticeId`.

This parameter is optional.

**-e interview | notice | request**

**--entity interview | notice | request**

Migrates just interviews or notices or requests. If you do not specify this option, hold notices and interviews are migrated during this run of the tool. For request migration, you must specify this option.

If you did not migrate any IBM Atlas Policy Suite data before, you must manually restart the system after the first migration run for custom attributes to show up in the migration portal.

**--stage**

Stages the IBM Atlas Policy Suite data for migration.

This parameter is optional.

**--resume**

Resumes migration from the staging database to IBM StoredIQ for Legal.

This parameter is optional.

**deployment\_type**

Specifies the IBM StoredIQ for Legal deployment type, which can be **ova** or **openshift**. The default value is **ova**.

**atlaspwd**

Specifies the password part of the credentials that are used to connect to the IBM Atlas Policy Suite database (IBM Atlas Policy Suite schema user password).

This parameter is required.

**ilgadminpwd**

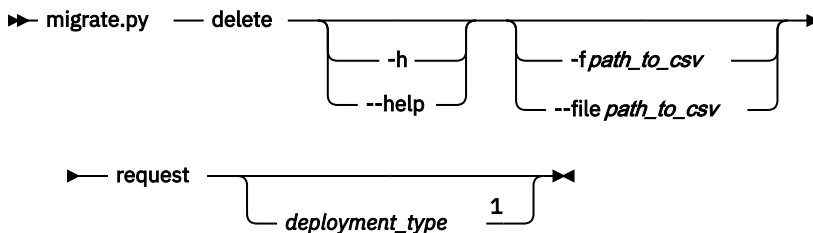
Specifies the password for the ilgadmin user.

This parameter is required.

At a maximum, 200 entities can be migrated per run.

**Command-specific syntax: delete**

Use the **delete** subcommand to delete migrated requests from IBM StoredIQ for Legal including the reporting database.



Notes:

<sup>1</sup> **request** and *deployment\_type* are positional parameters.

Where:

**-h****--help**

Displays help information.

This parameter is optional.

**-f path\_to\_csv****--file path\_to\_csv**

Specifies the path to a CSV file containing the list of requests to delete. The CSV file must contain only one column that holds one request ID (`requestId`) per row. However, the first row is considered the header and is ignored during processing. If you do not provide an input file for selective deletion, all migrated requests are deleted.

This parameter is optional.

**request**

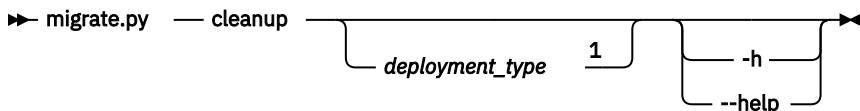
Specifies the entity type. You can delete only requests. For deleting interviews or notices, use the **cleanup** subcommand.

This parameter is required.

### **deployment\_type**

Specifies the IBM StoredIQ for Legal deployment type, which can be **ova** or **openshift**. The default value is **ova**.

### **Command-specific syntax: cleanup**



Notes:

<sup>1</sup> *deployment\_type* is a positional parameter.

Where:

**-h**

**--help**

Displays help information.

This parameter is optional.

### **deployment\_type**

Specifies the IBM StoredIQ for Legal deployment type, which can be **ova** or **openshift**. The default value is **ova**.

### **The migration configuration file**

The migration tool requires specific input that you provide in a configuration file.

The `migration_configuration.json` file in the `/siq/conf` directory serves as input to the migration tool and must provide the following information:

Setting	Subsection	Entity subsection	Type	Required	Description
connection			JSONObject	Yes	Contains connection information.
	jdbcUrl		String	Yes	JDBC URL pointing to an IBM Atlas Policy Suite database, for example: <pre>jdbc:oracle:thin:@192.0.2.11:1521:orcl jdbc:db2://host:port/ DBname:useJDBC4ColumnNameAndLabelSemantics=false;</pre>
	dbuser		String	Yes	User with administrator access to the IBM Atlas Policy Suite database (IBM Atlas Policy Suite schema user).



Setting	Subsection	Entity subsection	Type	Required	Description
options			JSONObject	Yes	Additional settings for the migration tool.
	user		String	Yes	IBM StoredIQ for Legal user with the <b>Notice: Manage</b> privilege.
	generate_template		Boolean	No	Automatically generate the hold notice or interview template to be used for all migrated notices. Default value: true
	append_request_name		Boolean	No	Append the request name for all migrated notices or interviews. Use this option to avoid name clashes. Default value: false
	request_name_field		String	No	The custom attribute field in IBM StoredIQ for Legal to which the request name is mapped. Default value: ca_atlasrequestname <b>Important:</b> Do not modify this entry.
	max_csv_row_number		Number	No	Sets the maximum number of rows per CSV file for migrating transmission or response records. If the number of records to be migrated exceeds this value, further CSV files are created. Default value: 10000

Setting	Subsection	Entity subsection	Type	Required	Description
options continued	hold_notice				
		unique_field	String	No	Unique field to identify an IBM Atlas Policy Suite notice. This field is mapped to a custom attribute in IBM StoredIQ for Legal. Default value: ca_atlasid
		status_field	String	No	The custom attribute field in IBM StoredIQ for Legal to which the notice status from IBM Atlas Policy Suite is mapped. Default value: ca_atlasstatus
		modified_fields	JSONArray	No	List of attributes that you want to be checked for changes made after the previous run of the migration tool. The (migrated) notices in IBM StoredIQ for Legal are then updated with any changed or new attribute values.  This configuration option has one preset value:ca_atlashasvirtualinterview
	interview				
		unique_field	String	No	Unique field to identify an IBM Atlas Policy Suite interview. This field is mapped to a custom attribute in IBM StoredIQ for Legal. Default value: ca_atlasid
		status_field	String	No	The custom attribute field in IBM StoredIQ for Legal to which the interview status from IBM Atlas Policy Suite is mapped. Default value: ca_atlasstatus
pre_populate			JSONArray	No	List of tables to prepopulate in the staging database before running the migration. The tables are prepopulated with data from the IBM StoredIQ for Legal reporting database.

## Migrating hold notices, interviews, and requests

Migrate hold notices, interviews, and requests from your IBM Atlas Policy Suite system to IBM StoredIQ for Legal and start managing those items here.

Ensure that IBM StoredIQ for Legal can connect to IBM Atlas Policy Suite by storing a copy of the appropriate IBM Atlas Policy Suite JDBC driver to the `/siq/migration/jdbc_drivers` directory on your IBM StoredIQ for Legal system:

- `ojdbc6.jar` for an Oracle database
- `db2jcc.jar` and `db2jcc_license_cu.jar` for a Db2 database (Supported Db2 versions are version 10.5 and later.)

Also, make sure all prerequisites that are described in [“Migration prerequisites”](#) on page 195 are met.

Run the **migrate.py** program on the IBM StoredIQ for Legal server to migrate hold and release notices. However, release notices can be migrated for reference purposes only. Also use the program to migrate interviews or requests.

Migration is a staged process: extract IBM Atlas Policy Suite information > populate the staging database > migrate information to IBM StoredIQ for Legal. You can view the content of the staging database in PostgreSQL by accessing it with user name `importuser` and password `passw0rd`. Each migration run clears the existing content from the staging database.

1. Refresh the reporting database to ensure that the staging tables are populated (or updated) with up-to-date information.

Go to **Admin > System Settings** and click **Run Now**.

**Important:** Usually, you must do this only once before you start migrating items. Refreshing the reporting database again is required only if you create further migration-related matters or persons in IBM StoredIQ for Legal later. In this case, you must also run the migration tool with the **cleanup** subcommand before you can migrate further items.

2. Optional: If you want to migrate only a subset of the IBM Atlas Policy Suite notices, interviews, or requests, create a CSV file containing the list of items to migrate.

For notices and interviews, the CSV file must have the columns `matterId` and `noticeId`. You don't have to specify a value for `matterId` but the field must be present. The `noticeId` value must be the value from the `legalnotice` table in IBM Atlas Policy Suite, where the notice type 4 stands for interviews and the notice type 1 for notices.

For requests, the CSV file must be set up with the columns `matterId` and `requestId`

3. Update the `migration_configuration.json` file with the proper settings.

For details, see the information about the [migration configuration file](#).

4. Run the migration tool with the **migrate** subcommand.

For details and full syntax, see the information about the [migration tool](#).

**Important:** When you run the tool with the **migrate** subcommand for the first time, the IBM StoredIQ for Legal application server is restarted after the run is complete. This is done only once to set up the system for migration.

5. Ask your users to verify the migrated notices and interviews.

Users can check and verify the migrated items in the migration portal. For access to the migration portal in general, a user must have the **Notice: Manage** or **Interview: Manage** privilege. Access to migrated items requires access to the matters holding migrated notices or interviews. Otherwise, the user won't be able to view those items.

A migrated notice or interview is not reflected in a matter's status or included in a matter's notices or interviews list until it is verified and its status is adjusted. The status you see in the migration portal corresponds to the status that the notice or interview had in IBM Atlas Policy Suite at the time of migration. After you verify an item, the status is changed to an equivalent IBM StoredIQ for Legal status, and the notice or interview behaves like any other IBM StoredIQ for Legal hold notice or interview.

Before users verify migrated items, they might want to check them. Users can view the status, content, schedule, custodians, and courtesy copy recipients of a migrated notice by clicking the notice in the migration portal. By clicking an interview in the migration portal, a user can review and verify the status, content, schedule, custodians, and questionnaire of a migrated interview. The notice or interview is opened in edit mode. Thus, users can modify any settings that do not meet the requirements.

Transmission and response records are also migrated and attached to the migrated notice or interview as CSV file. Users can find these files on the **Notice Information** page under **Atlas Transmission History** and **Atlas Response History**. For interviews, these files can be found on the **Interview Information** page under **Atlas Transmission History** and **Atlas Interview Results**. For notices, the data in these files reflects the data in the IBM Atlas Policy Suite notice history view (rep\_notice\_trans\_hist\_vw) and the hold notice response history view (rep\_notice\_resp\_history\_vw). For interviews, the data in these files reflects the data in the IBM Atlas Policy Suite interview history view (rep\_rt\_int\_transmission\_hist\_vw) and the interview response view (rep\_interview\_results\_vw). These files can contain more information than what is displayed in the IBM Atlas Policy Suite UI. For example, transmission records with the reasons `Silent Confirmation reminder` or `Transmission Exception` are not shown in the UI but included in the files. However, after downloading the CSV files, users can filter the data as required to see only relevant information.

You might need to release custodians manually after you verify a migrated release notice.

If you want to check the contents of all migrated notices in one go before verification, you can create a Migrated Notices Report. You can request such a report from the **Reports** page in the migration portal. After you check the report, you can edit the migrated items as required from the **Hold Notices** page in the migration portal.

For more information about how statuses are mapped, see the [Status mapping table](#).

**Important:** The following information is not migrated or migrated with slightly different results:

#### **Notices**

- Escalation template: This template is not migrated and thus not included in the migrated notice.
- Courtesy copy (cc) recipients: If the notice to be migrated includes any cc recipients, be it for the initial notice, the change notice, or both, the migrated notice has these cc recipients set for the initial notice and the reminder notice.
- Grace period: This information is not migrated.
- Interview details: If the notice to be migrated includes an interview, the details are no longer available in the migrated notice.

#### **Interviews**

- Alerts: This information is not migrated.
- Interview headers and footers: The concept of header and footer templates does not exist in IBM StoredIQ for Legal. Therefore, header and footer text in interviews to be migrated cannot be mapped to system variables. Instead, the `$interviewurl` variable in the migrated item's message body is surrounded with the respective header and footer. If the message body contains several `$interviewurl` entries, only the last one has the header and footer information.

Verification and deletion of migrated notices or interviews in the migration portal are not impacted by workflow events for approval. The only approval process for migrated notices and interviews is managing them in the migration portal.

---

# Monitoring and auditing

You can monitor the health of StoredIQ for Legal, diagnose performance issues, and view the recorded audit events.

## Monitoring APIs

---

Monitoring provides data that helps you evaluate the health of your IBM StoredIQ for Legal system and diagnose performance issues.

StoredIQ for Legal provides Representational State Transfer (REST) APIs that you can use to access this information.

REST Services provide a set of Uniform Resource Identifiers (URIs) that allow you to interact with the monitoring system. The services can be invoked by any HTTP client application, and define an expected response in the form of a JavaScript Object Notation (JSON) object. The JSON format can be easily parsed and consumed by JavaScript and other products, tools, and languages

### Ping

The ping REST API endpoint for StoredIQ for Legal checks the availability of the REST services.

#### Universal Resource Identifier (URI) pattern

```
http://host:port/ilg/monitoring/v1/ping
```

#### HTTP method

GET

#### URL parameters

None.

#### Query parameters

None.

#### Request object

None.

#### Response

If the REST services are available, the response object contains the response code 200 (OK) and the string pong.

### Health

The health REST API endpoint for StoredIQ for Legal verifies whether the REST application has access to required databases, the LDAP, and to the monitoring system.

#### Universal Resource Identifier (URI) pattern

```
http://host:port/ilg/monitoring/v1/health
```

```
https://host:port/ilg/monitoring/v1/health
```

When you do not specify a port, the default port is used. The default ports are 9080 for HTTP and 9443 for HTTPS unless they were reconfigured in WebSphere Application Server.

**HTTP method**

GET

**URL parameters**

None.

**Query parameters**

You can add the following query parameters to the URI to tailor and filter the response output:

**pretty**

A Boolean value. This parameter specifies whether the JSON response object is pretty-printed.

By default, the parameter value is false.

**Request object**

None.

**Response object**

A JSON response object containing the health check results for the following connections:

Table 10. Health: Response contents

Connection property	"healthy" : true is returned.	"healthy" : false is returned.
database.legal.connection	The client REST application can successfully open a JDBC connection to the StoredIQ for Legal database.	The connection could not be established. A generic error message is returned. For details about the error, check the liger.log file.
database.reporting.connection	The client REST application can successfully open a JDBC connection to the reporting database.	
database.task_manager.connection	The client REST application can successfully open a JDBC connection to the WebSphere Application Server task manager database.	
database.web_config.connection	The client REST application can successfully open a JDBC connection to the WebSphere Application Server web configuration database.	
database.workflow.connection	The client REST application can successfully open a JDBC connection to the workflow database.	
ldap.connection	The client REST application can successfully connect to the local LDAP (TDS).	
monitoring.system.connection	The StoredIQ for Legal REST application can successfully connect to the system monitoring database.	

## Metrics

The metrics REST API endpoint for StoredIQ for Legal returns the current system metrics such as CPU and disk usage. For details about these endpoints, see [“Retrieve all metrics” on page 212](#) and [“Retrieve a filtered list of metrics” on page 212](#).

### Metrics types

StoredIQ for Legal collects metrics in the following categories:

Metrics type	Description
counter	An incrementing and decrementing 64-bit integer.
gauge	Simplest metric type that just returns a value.
histogram	Measure of the distribution of values in a stream of data, for example, the number of results returned by a search.
meter	Measure of the rate at which a set of event occurs.

Metrics type	Description
timer	Histogram of the duration of a type of event and a meter of the rate of its occurrence.

### Monitored metrics

StoredIQ for Legal collects the following metrics:

#### Java Virtual Machine (JVM) metrics

For details about JVM metrics, see the [JVM metrics library documentation](#).

#### Overall REST request metrics

Name	Type	Description
requests	timer	Average time a request needs on the server
requests.active.count	counter	Number of requests currently in process
requests.status_code.meter	meter	Response code count per time unit

#### Per REST service endpoint call

Name	Type	Description
rest.requests.class.method	timer	Average time the specific REST call takes
rest.requests.class.method.status_code.meter	meter	Response code count per REST endpoint per time unit

### System metrics

System metrics monitor the following containers:

- db (corresponds to ilg\_sol\_plugin\_db2inst)
- web (corresponds to ilg\_sol\_plugin)
- ldap (corresponds to tds)
- reporting\_db (corresponds to postgres)
- host (corresponds to virtual machine host)

All collected system metrics are of type gauge.

Name	Description
system.containerOrHost.cpu.num_cores	Number of cores available to a container (used to calculate usage in percent).
system.containerOrHost.cpu.usage.interval.ms	Interval in which the current CPU usage was measured. By default, the CPU usage is measured in an interval of circa 2 seconds and the metrics are refreshed every 20 seconds.
system.containerOrHost.cpu.usage.total.percent	CPU usage in percent in the last measured interval. New CPU usage is measured every 20 seconds.
system.containerOrHost.memory.available.mb	Total amount of memory available in megabytes. Every container sees the total memory assigned to the host.



Name	Description
system.containerOrHost.memory.usage.cache.mb	Amount of memory reported as cached.
system.containerOrHost.memory.usage.total.mb	Total memory usage in megabytes (corresponds to cache memory usage plus RSS memory usage; currently the RSS memory size is not reported).
system.containerOrHost.memory.usage.total.percent is the	Total memory usage in percent (total used memory / memory available * 100).
system.containerOrHost.memory.usage.working_set.mb	Memory usage of working sets (Total - inactive (not recently accessed memory = inactive_anon + inactive_file).
system.containerOrHost.memory.usage.working_set.percent	Memory usage of working_sets in percent (corresponds to working_set used memory / memory available * 100).
system.dm.disk.devicemapper_disk_id.usage.percent	Usage percent of devicemapper disks which are virtual disks managed and assigned to containers as root ('/'). The devicemapper disks are all using storage of the physical disk (see also system.host.disk.container.usage.percent). So even if the devicemapper drive reports free space, you can get write errors in a container if the physical disk is full.
system.host.disk.boot.usage.percent	Host boot disk usage in percent (see also the disk name mapping).
system.host.disk.container.usage.percent	Host container disk usage in percent (see also the disk name mapping). The container disk contains all the data stored in docker containers, which are not mapped to a volume container.
system.host.disk.root.usage.percent	Host root disk usage in percent (see also the disk name mapping).
system.host.disk.volume.usage.percent	Host volume disk usage in percent (see also the disk name mapping). The volume disk contains all the data stored to volume containers like tds_data, postgres_data, and ilg_sol_plugin_db2inst_data.
system.host.process.zombie.count	Current number of zombie processes.

### Monitoring considerations

Collect key metrics to obtain data that prepares you to address performance issues. These metrics are useful to monitor:

To evaluate	Metrics
CPU usage (percentage)	system.host.cpu.usage.total.percent
Disk usage (percentage)	system.host.disk.boot.usage.percent system.host.disk.container.usage.percent system.host.disk.root.usage.percent system.host.disk.volume.usage.percent
Garbage Collection	jvm.gc.*

To evaluate	Metrics
Java heap usage	jvm.memory.heap.usage
Number of active threads	jvm.threads.*
Number of zombie processes	system.host.process.zombie.count
Response time	rest.request.*.meter (mean_rate in events per second)
Return codes of the StoredIQ for Legal web page	requests.response_code.*

### Retrieve all metrics

This REST API endpoint returns all system metrics.

### Universal Resource Identifier (URI) pattern

```
http://host:port/ilg/monitoring/v1/metrics
```

```
https://host:port/ilg/monitoring/v1/metrics
```

When you do not specify a port, the default port is used. The default ports are 9080 for HTTP and 9443 for HTTPS unless they were reconfigured in WebSphere Application Server.

### HTTP method

GET

### URL parameters

None.

### Query parameters

You can add the following query parameters to the URI to tailor and filter the response output:

#### pretty

A Boolean value. This parameter specifies whether the JSON response object is pretty-printed.

By default, the parameter value is false.

### Request object

None.

### Response object

A JSON response object containing the all available system metrics. If for a given metric name no value exists, it is not part of the result.

### Retrieve a filtered list of metrics

This REST API endpoint returns a filtered list of system metrics.

### Universal Resource Identifier (URI) pattern

```
http://host:port/ilg/monitoring/v1/metrics/filter
```

```
https://host:port/ilg/monitoring/v1/metrics/filter
```

When you do not specify a port, the default port is used. The default ports are 9080 for HTTP and 9443 for HTTPS unless they were reconfigured in WebSphere Application Server.

## HTTP method

POST

## URL parameters

None.

## Query parameters

You can add the following query parameters to the URI to tailor and filter the response output:

### pretty

A Boolean value. This parameter specifies whether the JSON response object is pretty-printed.

By default, the parameter value is false.

## Request object

A JSON request object containing the metric names to include in the result.

## Response object

A JSON response object containing the requested metrics. If for a given metric name no value exists, it is not part of the result.

## Examples

The following POST requests (in CURL format) exemplify how to filter metrics in monitoring:

```
curl -X POST -H "Content-Type: application/json" -H "Cache-Control: no-cache"
-d '{"includes": ["system.web.memory.available.mb"]}'
"https://example.com/ilg/monitoring/v1/metrics/filter"
curl -X POST -H "Content-Type: application/json" -H "Cache-Control: no-cache"
-d '{"includes": ["requests.active.count", "requests",
"system.host.cpu.usage.total.percent"]}'
"https://example.com/ilg/monitoring/v1/metrics/filter"
```

## Statistics

The objectcount REST API endpoints for StoredIQ for Legal provide a statistical view of the number of StoredIQ for Legal objects in the database. For details about these endpoints, see [“Retrieve all object counts” on page 216](#) and [“Retrieve a filtered set of object counts” on page 217](#).

You can retrieve the total numbers and, where applicable, the numbers per status, event type, or other additional attributes for key objects in the database. This information can help you address performance issues, or when planning your storage requirements. By default, StoredIQ for Legal provides statistics for the following objects:

Objects	Label	Entity Name	Additional Counts
Audit events	Application Audit Custodian Event	appauditcustodians	Per event type (see <a href="#">“Audit events: Overview” on page 221</a> )
	Application Audit Object Modification Event	appauditobjectmod	
	Application Audit User Session Event	appauditusersession	
	Application Audit Workflow Event	appauditworkflow	

Table 11. Default object counts (continued)

Objects	Label	Entity Name	Additional Counts
Data requests	Data Request	datarequest	<p>Per status</p> <p>Per type</p> <p>maxCustodians: across all data requests in the system, the maximum number of custodians associated with one data request</p> <p>maxDatarequestsPerMatter: across all data requests in the system, the maximum number of data requests associated with one matter</p> <p>minCustodians: across all data requests in the system, the minimum number of custodians associated with one data request</p> <p>minDatarequestsPerMatter: across all data requests in the system, the minimum number of data requests associated with one matter</p>
Data sources	Data Source	datasource	Per status
Data source applications	Data Source Application	datasourceapplication	Per status
Data source servers	Data Source Server	datasourceserver	Not applicable
Fulfillment Items	Fulfillment Item	fulfillmentitem	Per status
Work packages	Fulfillment Workpackage	fulfillmentworkpackage	Per status
Notices	Hold Notice	notice	<p>Per status</p> <p>maxCustodians: across all data requests in the system, the maximum number of custodians associated with one data request</p> <p>minCustodians: across all data requests in the system, the minimum number of custodians associated with one data request</p>

Table 11. Default object counts (continued)

Objects	Label	Entity Name	Additional Counts
Interviews	Interview	interview	Per status maxQuestions: across all interviews in the system, the maximum number of questions associated with one interview minQuestions: across all interviews in the system, the minimum number of questions associated with one interview
Matters	Matter	matter	Per status maxDatarequests: across all matters in the system, the maximum number of data requests associated with one matter maxInterviews: across all matters in the system, the maximum number of interviews associated with one matter maxNotices: across all matters in the system, the maximum number of notices associated with one matter minDatarequests: across all matters in the system, the minimum number of data requests associated with one matter minInterviews: across all matters in the system, the minimum number of interviews associated with one matter minNotices: across all matters in the system, the maximum number of notices associated with one matter numCategory: the number of matter categories
Persons	Person	persondistinct	Per status

Table 11. Default object counts (continued)

Objects	Label	Entity Name	Additional Counts
Workflow-related objects	Not available	processdefinition	Per status
		processinstance	
		task	

### Retrieve all object counts

This REST API endpoint returns all counts for a predefined set of objects.

### Universal Resource Identifier (URI) pattern

```
https://host:port/ilg/monitoring/v1/objectcount
```

When you do not specify a port, the default port is used, which is 9443 unless it was reconfigured in WebSphere Application Server.

### HTTP method

GET

### URL parameters

None.

### Query parameters

You can add the following query parameters to the URI to tailor the response output:

#### pretty

A Boolean value. This parameter specifies whether the JSON response object is pretty-printed.

By default, the parameter value is false.

### Request object

None.

### Response object

A JSON response object containing the all counts for the objects listed in the [Default object counts](#) table. If no value is available for a given object, a zero value is returned. The response object also includes a time stamp of when the data was collected. The time stamp is in UTC format (ISO8601) and is recorded in the time zone of the StoredIQ for Legal server.

Example:

```
{
  "objectCount" : {
    "fulfillmentitem" : {
      "label": "Fulfillment Item",
      "total" : 480,
      "status" : {
        "IN_PROGRESS" : 18,
        "NOT_STARTED" : 462
      }
    }
  },
  ...
  "datarequest" : {
    "label": "Data Request",
    "total" : 7,
    "status" : {
      "Refine" : 4,
      "Open" : 2,

```

```
    "Draft" : 1
  }
  "timestamp": "2017-04-01T13:04:36+00:00"
}
```

### Retrieve a filtered set of object counts

This REST API endpoint returns a subset of object counts based on the specified filter.

### Universal Resource Identifier (URI) pattern

```
https://host:port/ilg/monitoring/v1/objectcount/filter
```

When you do not specify a port, the default port is used, which is 9443 unless it was reconfigured in WebSphere Application Server.

### HTTP method

POST

### URL parameters

None.

### Query parameters

You can add the following query parameters to the URI to tailor the response output:

#### basicInfo

A Boolean value. This parameter specifies the detail level of the returned information. If set to `true`, only basic information, such as the label, status information, and the total numbers, is returned. If set to `false`, the response includes additional information (see the [Additional Counts column of the Default object counts table](#)).

By default, the parameter value is `true`.

#### pretty

A Boolean value. This parameter specifies whether the JSON response object is pretty-printed.

By default, the parameter value is `false`.

### Request object

A JSON request object containing the filter for the object counts to include in the result. The filter is defined by the `includes` parameter and is an array of strings. You can filter on objects, on status, type, or any other additional attribute, and you can use the asterisk (\*) as wildcard. If you combine filter criteria, the results are merged. If no value is available for a given object, a zero value is returned.

Statistics are also available for objects that are not included in the default set. To obtain a complete list of objects and their attributes, submit a request filtering on `*.*`.

### Response object

A JSON response object containing the requested object counts. Status or type information for a given object is returned only if a value is available. The response object also includes a time stamp of when the data was collected. The time stamp is in UTC format (ISO8601) and is recorded in the time zone of the StoredIQ for Legal server.

### Examples

The following POST requests (in CURL format) show how to filter the object counts and what the response will look like:

- Filter on all counters for matter objects and on the status of notice objects

Request:

```
curl -X POST -H "Content-Type: application/json" -H "Cache-Control: no-cache"
-d '{"includes": ["matter.*", "notice.status"]}'
"https://example.com/ilg/monitoring/v1/objectcount/filter?pretty=true"
```

Response:

```
{
  "objectCount": {
    "matter": {
      "label": "Matter",
      "status": {
        "Active": 6
      },
      "total": 6
    },
    "notice": {
      "status": {
        "Draft": 8
        "PartiallySent": 5
        "Published": 26
      }
    },
    "timestamp": "2017-04-17T17:18:50+00:00"
  }
}
```

- Filter on the total numbers for all default object counts

Request:

```
curl -X POST -H "Content-Type: application/json" -H "Cache-Control: no-cache"
-d '{"includes": ["*.total"]}'
"https://example.com/ilg/monitoring/v1/objectcount/filter?pretty=true"
```

Response:

```
{
  "objectCount": {
    "appauditcustodians": {
      "total": 14
    },
    "appauditobjectmod": {
      "total": 39
    },
    "appauditusersession": {
      "total": 8
    },
    "appauditworkflow": {
      "total": 0
    },
    "datarequest": {
      "total": 0
    },
    "datasource": {
      "total": 0
    },
    "datasourceapplication": {
      "total": 0
    },
    "datasourceserver": {
      "total": 0
    },
    "fulfillmentitem": {
      "total": 0
    }
  }
}
```



```

    },
    "fulfillmentworkpackage":
    {
        "total": 0
    },
    "interview":
    {
        "total": 0
    },
    "matter":
    {
        "total": 1
    },
    "notice":
    {
        "total": 2
    },
    "persondistinct":
    {
        "total": 7
    },
    "processdefinition":
    {
        "total": 0
    },
    "processinstance":
    {
        "total": 0
    },
    "task":
    {
        "total": 0
    },
    "timestamp": "2017-04-12T11:11:53+00:00"
}
}

```

## Monitoring system alerts

IBM StoredIQ for Legal provides system alerts for several performance issues. You can choose to have these displayed in the **Admin** section.

To view and remove system alerts and to change the notification setting, you must be signed in with the **System: Manage** privilege.

**New installations:** To have system alerts generated and displayed, complete the following steps after deploying the product:

- For StoredIQ for Legal (VM), complete these steps on the virtual machine as `root`:

1. Open the WebSphere Application Server container by running this command:

```
docker exec -it ilg_sol_plugin bash
```

2. A script to create a dummy alert and delete it again is provided with the product. Run this script:

```
sh /opt/ibm/ilg-sol-toolkit/scripts/dummy_alert_create_delete.sh
```

3. Restart the web application server:

```
systemctl restart was
```

- For StoredIQ for Legal (Container), complete these steps on an OpenShift client that has access to the cluster where IBM StoredIQ for Legal is deployed:

1. Obtain the name of the `ilg-sol-plugin` container by running this command:

```
CONTAINER_NAME=$(oc get pods -n siq4lopernsift -l app=ilg-sol-plugin -o name | sed "s/^\.
\{4\}//" )
```

2. Open the `ilg-sol-plugin` container by running the following command. Replace `$CONTAINER_NAME` with the name returned in the previous step.

```
oc exec -it $CONTAINER_NAME bash
```

3. A script to create a dummy alert and delete it again is provided with the product. Run this script:

```
sh /opt/ibm/ilg-sol-toolkit/scripts/dummy_alert_create_delete.sh
```

4. Restart the web application server:

```
systemctl restart was
```

You have to do this only once after installing.

StoredIQ for Legal runs scheduled script for checking the following issues and sends system alerts if required:

- Hung threads. The script stays in wait state listening for hung thread notifications and sends an alert if it detects any. By default, the web application server waits for 10 minutes before marking a thread as hung.

**Tip:** For alerts of this type, check the `SystemOut.log` in the `/home/was/WebSphere/AppServer/profiles/ilgnext/logs/server1` directory of the web application server container for details. Some hung threads are caused by system threads managed by the web application server and do not impact StoredIQ for Legal.

Check the file for hung threads associated with `WorkManager.ilgWorkManager`. Monitor such threads to see whether they remain hung for an extended period.

- SMTP connection issues, for example, when the mail server is down. The script runs every 10 minutes and send an alert if necessary.
- Temp space availability. The script runs once per day and sends an alert if less than 1 GB of free temporary disk space is left.

In addition to these alerts, an alert is also added whenever the refresh of the reporting database fails. Unlike the other alerts, this alert is event-based.

Such alerts are listed on the **System Alerts** page, at a maximum one entry per alert type. Whenever a new alert is added, older entries of the same alert type are deleted. You can configure to be notified of new alerts every time you go to the **Admin** section.

To manage system alerts:

1. Go to **Admin > System Alerts**.

The page shows all system alerts. You can remove alerts at any time.

2. Optional: To be notified of alerts that occurred since you last signed in, enable alert notification.

Then, a message with the number of new alerts is displayed when you access the Admin page for the first time after sign-in. The message also provides direct access to the list of alerts.

## Auditing

---

StoredIQ for Legal records each action that a user performs and each action that the system performs as a result of a user action. You can view details about the audit events.

You must be signed in with the **Audit events: View** privilege.

If you have a previous release of StoredIQ for Legal, you might use low-level auditing, which creates a separate record for each operation that stores data. Action auditing now covers all the audit events that you need and provides a large number of details about an audit event. It is no longer necessary to use low-level auditing, which can have a considerable impact on the performance.

Therefore, do not enable low-level auditing as part of the system settings. In addition, do not activate the matter audit report, which is supplied with StoredIQ for Legal and can be run on request.

To view details about the audit events that were created as part of action auditing, complete these steps:

1. Go to **Admin > Audit Queries**.
2. Create the appropriate queries to view details about the audit events.

For an overview of the recorded audit events, see [“Audit events: Overview”](#) on page 221.

Select **Any** from the **Object type** list if the audit events can be related to any object type. Select **None or variable** if you want to view audit events that are not related to any of the listed object types or where the object type can vary.

The broader the query, the longer it takes for StoredIQ for Legal to retrieve the results.

**Tips:**

- To reduce the number of results that are returned, you can specify a data range.
- If your query exceeds the 1000 search results that can be displayed, export them to a CSV file. The CSV file is available for download in compressed format for 30 days.

## Audit events: Overview

To view details about the audit events, you must know their names. The following tables give an overview of the audit events and describe when they are created. Each event captures who triggered the event and when.

### User session

Session-related events capture the following attributes: actor\_id, event\_date, event\_type, ip\_address, and login\_id.

<i>Table 12. Session-related, licensing, and logging events</i>	
Event name	Description of the action that created the event
LOGON	A user signs in to StoredIQ for Legal.
<b>Import</b>	
CLIENT_ADD	A new REST API client is registered for import.
CLIENT_REMOVE	A REST API client is unregistered.

### Object modification

Object-related events capture the following attributes: raw\_data, actor\_id, correlation\_id, effect\_type, event\_date, event\_type, object\_id, object\_type, parent\_id, parent\_type, and reason.

<i>Table 13. Object-related events</i>	
Event name	Description of the action that created the event
<b>Attachments</b>	
ATTACHMENT_CREATE	A file is added to an object, such as a matter, a task, or a fulfillment item.
ATTACHMENT_DELETE	A file is deleted from an object.
ATTACHMENT_REFERENCES_ADD	One or more files are added to an object. The button for adding the files was defined as a custom attribute of data type <b>Attribute</b> or <b>Attributes</b> .
<b>Audit queries</b>	
REPORT_APPAUDIT_DOWNLOAD	The CSV file that contains the audit query results is downloaded in compressed format.
REPORT_APPAUDIT_REQUEST	The audit query results are exported to a CSV file.
<b>Comments</b>	
COMMENT_CREATE	A comment is added to a task.

<i>Table 13. Object-related events (continued)</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
COMMENT_DELETE	A comment is deleted from a task. If the comment included an attachment, also an ATTACHMENT_DELETE event is written.
<b>Configuration</b>	
CONFIG_CREATE	A configuration is created. For example, the connection to the directory server is defined.
CONFIG_DELETE	A configuration is deleted.
CONFIG_UPDATE	A configuration is changed.
<b>Custom attributes</b>	
ATTRIBUTE_CREATE	A new attribute is added to the list of predefined and custom attributes.
ATTRIBUTE_DELETE	A custom attribute is deleted.
ATTRIBUTE_UPDATE	The name or the settings of a custom attribute are changed.
<b>Data boxes and data requests</b>	
BOX_CANCEL_REQUEST	A data request is canceled.
BOX_CLOSE	A data box is closed.
BOX_COLLECT	A collection request is submitted.
BOX_CREATE_EXPAND	An existing data box is expanded.
BOX_CREATE_IDENTIFY	A data request is saved as a draft.
BOX_CREATE_REFINE	An existing data box is refined.
BOX_DELETE	A data box is deleted.
BOX_EXPAND_SAVE	An expanded data request is saved.
BOX_EXPORT	An export request is submitted.
BOX_OPEN	A data box is reopened.
BOX_REFINE_SAVE	A refined data request is saved.
BOX_REFRESH	A data box is refreshed.
BOX_REQUEST_EXCEPTIONS	Exception details are requested for a collection data box.
BOX_REQUEST_EXPAND	An expanded data request is submitted.
BOX_REQUEST_IDENTIFY	A data request is submitted.
BOX_REQUEST_REFINE	A refined data request is submitted.
BOX_UPDATE	A data request is changed, except for the list of custodians.
REPORT_BOX_REQUEST	One or more data box reports are requested.
REPORT_BOX_DOWNLOAD	A data box report is downloaded.
<b>Data locales</b>	
DATALOCALE_CREATE	A data locale is created.
DATALOCALE_DELETE	A data locale is deleted.
DATALOCALE_UPDATE	A data locale is changed.
<b>Data requests</b>	
DATAREQUEST_CANCEL	A submitted data request is canceled. All fulfillment activities are stopped.
DATAREQUEST_CREATE	A data request is created.
DATAREQUEST_CUSTODIANS_REFINEMENT_DOWNLOAD	Request information for custodians was exported to CSV.

Table 13. Object-related events (continued)

Event name	Description of the action that created the event
DATAREQUEST_DELETE	A data request is deleted.
DATAREQUEST_DUPLICATE	A data request is duplicated.
DATAREQUEST_RELEASE	A release data request is created.
DATAREQUEST_REOPEN	A completed data request is reopened.
DATAREQUEST_SUBMIT	A data request is submitted.
DATAREQUEST_UPDATE	A data request in draft state is changed, or the request information is updated after the data request is submitted.
DATAREQUESTDEFINITION_CREATE	A data request template is created.
DATAREQUESTDEFINITION_DELETE	A data request template is deleted.
DATAREQUESTDEFINITION_UPDATE	A data request template is changed.
<b>Data sources</b>	
DATASOURCE_CREATE	A new data source is imported.
DATASOURCE_DELETE	A data source is deleted.
DATASOURCE_UPDATE	A data source is edited.
<b>Data source applications</b>	
DATASOURCEAPPLICATION_CREATE	An application that contains one or more data sources is imported.
DATASOURCEAPPLICATION_DELETE	An application that contains one or more data sources is deleted.
DATASOURCEAPPLICATION_UPDATE	An application that contains one or more data sources is edited.
<b>Data source servers</b>	
DATASOURCESERVER_CREATE	A server that contains one or more data sources is imported.
DATASOURCESERVER_DELETE	A data source server is deleted.
DATASOURCESERVER_UPDATE	A data source server is changed.
<b>Data type</b>	
DATATYPE_UPDATE	A data type is updated through an internal program call.
<b>Fulfillment connectors</b>	
FULFILLMENTCONNECTOR_LOG_DOWNLOAD	A fulfillment connector log is downloaded.
FULFILLMENTCONNECTOR_REGISTER	A fulfillment connector is registered.
FULFILLMENTCONNECTOR_UNREGISTER	A fulfillment connector is unregistered.
FULFILLMENTCONNECTOR_UPDATE	Fulfillment connector settings are updated.
<b>Fulfillment items</b>	
FULFILLMENTITEM_CREATE	A fulfillment item is created.
FULFILLMENTITEM_DELETE	A fulfillment item is deleted.
FULFILLMENTITEMS_DOWNLOAD	One or more fulfillment items are downloaded.
FULFILLMENTITEM_DUPLICATE	A fulfillment item is duplicated.
FULFILLMENTITEM_RESULTS_UPDATE	A fulfillment item is updated with the results of the data identification, preservation, or collection.
FULFILLMENTITEM_UPDATE	A fulfillment item is edited.
FULFILLMENTWORKPACKAGE_CREATE	A work package is created.
FULFILLMENTWORKPACKAGE_DELETE	A work package is deleted.
FULFILLMENTWORKPACKAGE_SPLIT	A work package is split.

<i>Table 13. Object-related events (continued)</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
FULFILLMENTWORKPACKAGE_SUBMIT	A work package is submitted.
FULFILLMENTWORKPACKAGE_UPDATE	The information about a work package is edited.
<b>Fulfillment jobs</b>	
FULFILLMENTJOB_CREATE	A fulfillment job is created.
FULFILLMENTJOB_DELETE	A fulfillment is deleted.
FULFILLMENTJOB_KILL_REQUEST_ACCEPTED	The request to end a fulfillment job is accepted.
FULFILLMENTJOB_UPDATE	A fulfillment job is updated.
<b>Global hold reminder</b>	
GLOBALHOLDREMINDER_CREATE	The global hold reminder is created.
GLOBALHOLDREMINDER_EXPORT	The information about the custodians who received a single reminder notice for all of their hold notices is exported as a CSV file.
GLOBALHOLDREMINDER_RESUME	The global hold reminder is enabled.
GLOBALHOLDREMINDER_SETACTIVE	The global hold reminder, or any updates to it, are activated.
GLOBALHOLDREMINDER_SETNEXTTRANSMISSIONDATE	The date of the next reminder is changed.
GLOBALHOLDREMINDER_SUSPEND	The global hold reminder is disabled.
GLOBALHOLDREMINDER_UPDATE_DRAFT	The global hold reminder is updated.
<b>Groups</b>	
GROUP_CREATE	A group is created.
GROUP_DELETE	A group is deleted.
GROUP_DOWNLOAD	A list of members in a group is downloaded from the people catalog.
GROUP_UPDATE	The list of members in a group is changed.
<b>Hold notices</b>	
NOTICE_CREATE	A hold notice is created.
NOTICE_UPDATE	The details about a hold notice in draft state are changed.
NOTICE_PUBLISH	A hold notice is published.
NOTICE_DELETE	A hold notice is deleted.
NOTICE_DRAFT_APPLY	A hold notice is republished or other changes to a published hold notice are applied.
<b>Import mapping</b>	
IMPORT_MAPPING_CREATE	During the import of a CSV file, a file column is mapped to the corresponding attribute, which is defined in StoredIQ for Legal.
IMPORT_MAPPING_UPDATE	An import mapping is changed.
IMPORT_MAPPING_DELETE	An import mapping is deleted.
<b>Import request</b>	
IMPORT_REQUEST_CREATE	An import request is created.
IMPORT_REQUEST_UPDATE	An import request is changed.
IMPORT_REQUEST_DELETE	An import request is deleted.
IMPORT_REQUEST_START	The processing of an import request is started.
IMPORT_REQUEST_EXECUTION	The import is completed.
ORGTREE_HISTORY_CLEANUP	The department hierarchy is cleaned up.
PERSON_HISTORY_CLEANUP	The employment history is cleaned up.

<i>Table 13. Object-related events (continued)</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
PERSONDISTINCTHISTORY_CLEANUP	Person history records are cleaned up.
<b>Interviews</b>	
INTERVIEW_CREATE	An interview is created.
INTERVIEW_UPDATE	The details about an interview are changed.
INTERVIEW_DELETE	An interview is deleted.
<b>Jurisdictions</b>	
JURISDICTION_CREATE	A new jurisdiction is added to the list of jurisdictions.
JURISDICTION_UPDATE	A jurisdiction is activated or deactivated.
JURISDICTION_DELETE	A jurisdiction is deleted.
<b>Matters</b>	
MATTER_CREATE	A matter is created.
MATTER_UPDATE	The matter details are changed.
MATTER_ASSIGNEES_ADD	One or more assignees are added to a matter.
MATTER_ASSIGNEES_REMOVE	One or more assignees are removed from a matter.
MATTER_CLOSE	A matter is closed.
MATTER_REOPEN	A closed matter is reopened.
MATTER_DELETE	A matter is deleted.
MATTER_LIST_DOWNLOAD	The list of matters is downloaded.
<b>Matter categories</b>	
MATTERCATEGORY_CREATE	A new matter category is imported, or a new matter category is added.
MATTERCATEGORY_UPDATE	A matter category is edited.
MATTERCATEGORY_DELETE	A matter category is deleted.
<b>Miscellaneous (object type <b>None</b> or <b>variable</b>)</b>	
DELETE_DANGLING_REFERENCE	The reference to a deleted object is deleted.
LOG_CONFIG_UPDATE	A user changed the log settings.
LOG_FILES_DOWNLOAD	The log files are collected and downloaded.
MIGRATION_START	Migration of notices or interviews from IBM Atlas Policy Suite to StoredIQ for Legal started. This event is written once per migration run.
MIGRATION_END	Migration of notices or interviews from IBM Atlas Policy Suite to StoredIQ for Legal ended. This event is written once per migration run.
TASK_LICENSES_COUNT	A user licenses task is started.
<b>People</b>	
MATTER_INVOLVEMENT_DOWNLOAD	The information about a person's hold obligations and involvement in matters is exported as a CSV file.
PERSON_CREATE	A test user is created in StoredIQ for Legal or a person is imported with a CSV file.
PERSON_LIST_DOWNLOAD	A list of people is downloaded from the people catalog.
PERSON_UPDATE CUSTODIAN_UPDATE	The profile of a person is changed.

<i>Table 13. Object-related events (continued)</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
PERSON_UPDATE_ROLES CUSTODIAN_UPDATE_ROLES	A user is assigned roles or is assigned different or additional roles.
<b>Server discovery connectors</b>	
SERVERDISCOVERYCONNECTOR_LOG_DOWNLOAD	A server discovery connector log is downloaded.
SERVERDISCOVERYCONNECTOR_REGISTER	A server discovery connector is registered.
SERVERDISCOVERYCONNECTOR_UNREGISTER	A server discovery connector is unregistered.
SERVERDISCOVERYCONNECTOR_UPDATE	Server discovery connector settings are updated.
<b>Server discovery jobs</b>	
SERVERDISCOVERYJOB_CREATE	A server discovery job is created.
SERVERDISCOVERYJOB_DELETE	A server discovery job is deleted.
SERVERDISCOVERYJOB_KILL_REQUEST_ACCEPTED	The request to end a server discovery job is accepted.
SERVERDISCOVERYJOB_UPDATE	A server discovery job is updated.
<b>Report definitions, report resources, and custom reports</b>	
REPORT_BIRT_DEFINITION_CREATE	A custom report definition is imported.
REPORT_BIRT_DEFINITION_UPDATE	A custom report definition is activated or suspended.
REPORT_BIRT_DEFINITION_DOWNLOAD	A custom report definition is downloaded.
REPORT_BIRT_DEFINITION_DELETE	A custom report definition is deleted.
REPORT_BIRT_DOWNLOAD	A custom report is opened.
REPORT_BIRT_REQUEST	The creation of a custom report is requested.
REPORT_BIRT_RESOURCE_CREATE	A report resource is imported.
REPORT_BIRT_RESOURCE_DELETE	A report resource is deleted.
REPORT_BIRT_RESOURCE_UPDATE	A report resource is replaced.
REPORT_BIRT_RESOURCE_DOWNLOAD	A report resource is exported.
REPORT_CUSTOMIZATION_CREATE	Database customizations are added.
REPORT_CUSTOMIZATION_DELETE	Database customizations are deleted.
REPORT_CUSTOMIZATION_DOWNLOAD	Database customization information is downloaded.
REPORT_CUSTOMIZATION_UPDATE	Database customizations have been replaced.
<b>Scheduled reports and reporting database</b>	
TASK_REPORT_BIRT_CREATE	A scheduled custom report is being created.
TASK_REPORTS_DELETE	One or more scheduled reports are deleted.
TASK_REPORTING_DB_EXPORT	The reporting database is refreshed.
<b>Security groups</b>	
SECURITYGROUP_CREATE	A security group is created.
SECURITYGROUP_UPDATE	The list of members in a security group is changed.
SECURITYGROUP_DELETE	A security group is deleted.
<b>Templates</b>	
TEMPLATE_HOLD_CREATE	A hold notice template is created.
TEMPLATE_HOLD_UPDATE	A hold notice template in draft state is changed.
TEMPLATE_HOLD_ACTIVATE	A hold notice template is activated.
TEMPLATE_HOLD_DEACTIVATE	A hold notice template is deactivated.



<i>Table 13. Object-related events (continued)</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
TEMPLATE_HOLD_DELETE	A hold notice template is deleted.
TEMPLATE_HOLD_IMPORT	A hold notice template is imported.
TEMPLATE_HOLD_EXPORT	A hold notice template is exported.
TEMPLATE_INTERVIEW_CREATE	An interview template is created.
TEMPLATE_INTERVIEW_UPDATE	An interview template in draft state is changed.
TEMPLATE_INTERVIEW_ACTIVATE	An interview template is activated.
TEMPLATE_INTERVIEW_DEACTIVATE	An interview template is deactivated.
TEMPLATE_INTERVIEW_DELETE	An interview template is deleted.
TEMPLATE_INTERVIEW_IMPORT	An interview template is imported.
TEMPLATE_INTERVIEW_EXPORT	An interview template is exported.
TEMPLATE_FORM_CREATE	A form template is created.
TEMPLATE_FORM_UPDATE	A form template in draft state is changed.
TEMPLATE_FORM_ACTIVATE	A form template is activated.
TEMPLATE_FORM_DEACTIVATE	A form template is deactivated.
TEMPLATE_FORM_DELETE	A form template is deleted.
TEMPLATE_FORM_IMPORT	A form template is imported.
TEMPLATE_FORM_EXPORT	A form template is exported.
<b>User preferences</b>	
USERPREFERENCE_CREATE	Notification settings are specified or out-of-office settings are enabled.
USERPREFERENCE_UPDATE	Notification settings or out-of-office settings are changed.
USERPREFERENCE_DELETE	Notification settings are removed or out-of-office settings are disabled.
<b>User roles</b>	
ROLE_CREATE	A user role is created.
ROLE_UPDATE	A user role is edited.
ROLE_DELETE	A user role is deleted.

### People, users, and custodians

Events related to people, users, and custodians capture the following attributes: actor\_id, correlation\_id, custodian\_id, custodian\_id\_max, custodian\_id\_min, custodians, event\_date, event\_type, object\_id, object\_type, parent\_id, parent\_type, and reason.

<i>Table 14. Events related to people, users, and custodians</i>	
<b>Event name</b>	<b>Description of the action that created the event</b>
<b>Actions on people, users, and custodians</b>	
BOX_CUSTODIANS_ADD	One or more custodians are added to the data box.
BOX_CUSTODIANS_RELEASE	One or more custodians are removed from the data box.
BOX_CUSTODIANS_DOWNLOAD	The list of custodians that belongs to a data box is downloaded.
DATAREQUEST_CUSTODIANS_ADD	One or more custodians are added to a data request.

Table 14. Events related to people, users, and custodians (continued)

Event name	Description of the action that created the event
DATAREQUEST_CUSTODIANS_DOWNLOAD	The list of custodians that belongs to a data request is downloaded.
DATAREQUEST_CUSTODIANS_REMOVE	One or more custodians are removed from a data request.
DATAREQUEST_CUSTODIANS_OVERRIDE_CRITERIA	The request information is edited for one or more custodians of a data request.
DATAREQUEST_CUSTODIANS_UPDATE_PRIORITY	The priority of one or more custodians is changed.
DATAREQUEST_CUSTODIANS_DATASOURCES_ADD	One or more data sources are added to one or more custodians.
DATAREQUEST_CUSTODIANS_DATASOURCES_REMOVE	One or more data sources are removed from one or more custodians.
GROUP_CUSTODIANS_ADD	A person is added to a group.
GROUP_CUSTODIANS_REMOVE	A person is removed from a group.
INTERVIEW_CUSTODIAN_NOTES_UPDATE	A note is added to one or more custodians when viewing the status of the custodians within an interview or when viewing the results of an interview.
INTERVIEW_DRAFT_CUSTODIANS_ADD	One or more custodians are added to an interview that is not published yet.
INTERVIEW_DRAFT_CUSTODIANS_REMOVE	One or more custodians are removed from an interview that is not published yet.
INTERVIEW_CUSTODIANS_ADD	One or more custodians are added to a published interview.
INTERVIEW_CUSTODIANS_SUSPEND	An interview is suspended for one or more custodians.
INTERVIEW_CUSTODIANS_RESUME	An interview is resumed for one or more custodians.
INTERVIEW_CUSTODIANS_CONCLUDE	An interview is concluded for one or more custodians.
INTERVIEW_CUSTODIANS_DOWNLOAD	The list of custodians that belong to an interview is downloaded.
INTERVIEW_QUESTIONRESPONSE_NOTES_UPDATE	A note is added to the custodian when viewing the results of an interview by custodian.
NOTICE_CUSTODIAN_NOTES_UPDATE	A note is added to one or more custodians when viewing the status of the custodians within a hold notice.
NOTICE_CUSTODIAN_CC_NOTES_UPDATE	A note is added to one or more courtesy copy recipients when viewing the status of the courtesy copy recipients within a hold notice.
NOTICE_CUSTODIANS_ADD	One or more custodians are added to a published hold notice.
NOTICE_CUSTODIANS_RELEASE	One or more custodians are released from a published notice.
NOTICE_CUSTODIANS_RESUME	A hold notice is released for one or more custodians.
NOTICE_CUSTODIANS_SUSPEND	A hold notice is suspended for one or more custodians.
NOTICE_CUSTODIANS_DOWNLOAD	The list of custodians that belong to a hold notice is downloaded.
NOTICE_CUSTODIANS_CC_ADD	One or more courtesy copy recipients are added to a hold notice.
NOTICE_CUSTODIANS_CC_REMOVE	One or more courtesy copy recipients are removed from a hold notice.

Table 14. Events related to people, users, and custodians (continued)

<b>Event name</b>	<b>Description of the action that created the event</b>
NOTICE_DRAFT_CUSTODIANS_ADD	One or more custodians are added to a hold notice that is not published yet.
NOTICE_DRAFT_CUSTODIANS_REMOVE	One or more custodians are removed from a hold notice that is not published yet.
NOTICE_DRAFT_SILENT_CUSTODIANS_ADD	One or more silent custodians are added to a hold notice that is not published yet.
NOTICE_DRAFT_SILENT_CUSTODIANS_REMOVE	One or more silent custodians are removed from a hold notice that is not published yet.
NOTICE_SILENT_CUSTODIANS_ADD	One or more users are added to a hold notice as silent custodians.
NOTICE_SILENT_CUSTODIANS_MOVE_TO_ACTIVE	One or more silent custodians on a hold notice are made active custodians.
NOTICE_SILENT_CUSTODIANS_MOVE_TO_SILENT	One or more active custodians on a hold notice are made silent custodians.
NOTICE_SILENT_CUSTODIANS_REMOVE	One or more silent custodians are removed from a hold notice.
SECURITYGROUP_CUSTODIANS_ADD	One or more users are added to a security group.
SECURITYGROUP_CUSTODIANS_REMOVE	One or more users are removed from a security group.
<b>Responses to hold notices</b>	
NOTICE_CONFIRM	A custodian confirms a hold notice.
NOTICE_CONTACT	A custodian requests to be contacted.
NOTICE_CONFIRM_ON_BEHALF	A paralegal confirms a hold notice on behalf of a custodian.
<b>Responses to interviews</b>	
INTERVIEW_RESPOND	A custodian responds to an interview.
INTERVIEW_RESPOND_ON_BEHALF	A paralegal responds to an interview on behalf of a custodian.
<b>Interview transmissions</b>	
INTERVIEW_SEND_INITIAL	The initial interview is sent.
INTERVIEW_SEND_INITIAL_FOLLOWUP	The message to follow up on the initial interview is sent.
INTERVIEW_SEND_REMINDER	The recurring interview is sent.
INTERVIEW_SEND_REMINDER_FOLLOWUP	The message to follow up on the recurring interview is sent.
INTERVIEW_RESEND_INITIAL	The initial interview is resent.
INTERVIEW_RESEND_INITIAL_FOLLOWUP	The message to follow up on the initial interview is resent.
INTERVIEW_RESEND_REMINDER	The recurring interview is resent.
INTERVIEW_RESEND_REMINDER_FOLLOWUP	The message to follow up on the recurring interview is resent.
<b>Hold-notice transmissions</b>	
NOTICE_SEND_INITIAL	The initial notice is sent.
NOTICE_SEND_INITIAL_FOLLOWUP	The message to follow up on the initial notice is sent.
NOTICE_SEND_REMINDER	An individual reminder notice is sent.
NOTICE_SEND_GLOBAL_REMINDER	The global reminder notice is sent.

Table 14. Events related to people, users, and custodians (continued)

Event name	Description of the action that created the event
NOTICE_SEND_REMINDER_FOLLOWUP	The message to follow up on an individual reminder notice is sent.
NOTICE_SEND_GLOBAL_REMINDER_FOLLOWUP	The message to follow up on the global reminder notice is sent.
NOTICE_RESEND_INITIAL	The initial notice is resent.
NOTICE_RESEND_INITIAL_FOLLOWUP	The message to follow up on the initial notice is resent.
NOTICE_RESEND_REMINDER	An individual reminder notice is resent.
NOTICE_RESEND_GLOBAL_REMINDER	The global reminder notice is resent.
NOTICE_RESEND_REMINDER_FOLLOWUP	The message to follow up on an individual reminder notice is resent.
NOTICE_RESEND_GLOBAL_REMINDER_FOLLOWUP	The message to follow up on the global reminder notice is resent.
<b>Email notifications</b>	
EMAIL_NOTIFICATION_SEND_DATA_REQUEST_CANCEL	The data request is canceled.
EMAIL_NOTIFICATION_SEND_WF_COMMENT_ADD	A comment is added to the task.
EMAIL_NOTIFICATION_SEND_WF_TERMINATE	A workflow instance is terminated.
EMAIL_NOTIFICATION_SEND_WF_TASK_ASSIGNEE_CHANGE	The task is assigned or returned.
EMAIL_NOTIFICATION_SEND_WF_TASK_COMPLETE	The task is completed.
EMAIL_NOTIFICATION_SEND_WF_TASK_OVERDUE_REMINDER	The due date of the task approaches.
EMAIL_NOTIFICATION_SEND_WF_TASK_UPDATE	The priority or the due date of the task is updated.
EMAIL_NOTIFICATION_SEND_WF_SUBSCRIBER_USERS_ADD	A subscriber is added to the task.
EMAIL_NOTIFICATION_SEND_WF_SUBSCRIBER_USERS_REMOVE	A subscriber is removed from the task.
EMAIL_NOTIFICATION_SEND_WORK_PACKAGE_CUSTODIANS_REMOVE	A custodian is removed from the data request.
EMAIL_NOTIFICATION_SEND_WORK_PACKAGE_PRIORITY_CHANGE	The priority of a custodian in a data request is changed.

## Workflow

Workflow-related events capture the following attributes: raw\_data, actor\_id, correlation\_id, event\_date, event\_type, proc\_def\_id, proc\_def\_key, proc\_error, proc\_inst\_id, task\_assignee\_id, task\_category, task\_id, task\_name, and task\_type.

Table 15. Workflow-related events


Event name	Description of the action that created the event
WF_ERROR	A workflow fails due an error. For more information, see <a href="#">“Workflow fails due to an error”</a> on page 238.
WF_INSTANCE_CANCEL	A workflow instance is terminated.
WF_INSTANCE_END	A workflow instance is finished.
WF_INSTANCE_RESUME	A suspended workflow instance was resumed.
WF_INSTANCE_START	A workflow instance is started.
WF_INSTANCE_SUBSCRIBERS_ADD	A subscriber is added to a task. The subscriber is then informed about all changes with regard to all tasks in the same workflow.
WF_INSTANCE_SUBSCRIBERS_REMOVE	A subscriber is removed from a task. The subscriber is then no longer informed about any task changes in the workflow.
WF_INSTANCE_SUSPEND	A workflow instances was suspended.

Table 15. Workflow-related events (continued)

Event name	Description of the action that created the event
WF_PROCDEF_CREATE	A workflow definition is added.
WF_PROCDEF_DELETE	A workflow definition is deleted.
WF_PROCDEF_ACTIVATE	A workflow is activated.
WF_PROCDEF_SUSPEND	A workflow is suspended.
WF_PROCDEF_CANCEL_SCHEDULE	The schedule for activating or suspending a workflow is canceled.
WF_MAPPING_CREATE WORKFLOWMAPPING_CREATE	A workflow definition is mapped to an object.
WF_MAPPING_DELETE WORKFLOWMAPPING_DELETE	A workflow definition is no longer mapped to a specific object.
WF_MAPPING_UPDATE WORKFLOWMAPPING_UPDATE	A workflow definition is mapped to another object.
WF_TASK_READ	A task is opened.
WF_TASK_START	A task is started.
WF_TASK_UPDATE	A task is changed.
WF_TASK_CLAIM	A task is assigned to oneself.
WF_TASK_ASSIGN	A task is assigned or reassigned.
WF_TASK_RETURN	A task is returned.
WF_TASK_COMPLETE	A task is completed.
WF_TASK_END	A task is finished.
WF_TASK_LIST_DOWNLOAD	A list of tasks was downloaded.

### Audit events: Query results

The details that are returned for an audit query depend on the type of object that was affected by the action.

The following tables give an overview of all details possible, in alphabetical order. Many details are displayed only after you select them from the **Select columns** list .

Key-based access control does not restrict the result scope. Irrespective of any access restrictions to matters, an audit query returns all events within the request scope.

Detail	Description
Container ID	The ID of the object that contains the selected object. For example, if the action modified a hold notice, the ID of the matter that contains the hold notice would be shown.
Container name	The name of the object that contains the selected object. For example, if the action modified a hold notice, the name of the matter that contains the hold notice would be shown.
Container type	The type of object that contains the selected object. For example, if the action modified a hold notice, the container type would be <code>matter</code> .
Correlation ID	The ID that is used for all audit events in the same workflow.
Custodians	The names of the custodians that are involved in the action.

Detail	Description
Event date	The time stamp of the audit event, in Coordinated Universal Time (UTC).
Audit event	The name of the audit event.
ID	The ID of the audit event.
IP address	The IP address of the StoredIQ for Legal session.
More details	Further details about the audit event.
Object ID	The ID of the object that was affected by the action.
Object name	The name of the object that was affected by the action.
Object type	The type of object that was affected by the action.
Reason	The reason for performing the action.
Signin ID	The signin ID of the user who established the StoredIQ for Legal session.
Task ID	The ID of the affected task in the workflow definition.
Task name	The name of the task that was affected by the action.
Task number	The number of the affected task on the <b>Tasks</b> page.
Task type	The type of the task that was affected by the action.
User	The user who performed the action.
Workflow - Matter ID	The ID of the matter that contains the object that uses the workflow and is involved in the action.
Workflow - Matter name	The name of the matter that contains the object that uses the workflow and is involved in the action.
Workflow - Object ID	The ID of the object that uses the workflow and is involved in the action.
Workflow - Object name	The name of the object that uses the workflow and is involved in the action.
Workflow - Object type	The type of the object that uses the workflow and is involved in the action.
Workflow - Status variable	The current value of the <i>Status</i> variable in the workflow that is involved in the action.
Workflow definition ID	The ID of the workflow definition that is involved in the action.
Workflow error	The workflow error that occurred when the action was performed.
Workflow ID	The ID of the workflow.

---

# Troubleshooting and support

To isolate and resolve problems with your IBM products, you can use the troubleshooting tools that are provided with the product and the resources that are offered by IBM Support.

## Before contacting IBM Support

---

Review this information before you contact IBM Support. There are resources that might help you find possible solutions for your issue, or make your support experience more efficient if you need to contact IBM Support.

1. Check the following information for possible solutions to your issue:
  - [“Known problems and solutions” on page 235](#)
  - [“Searching the knowledge bases” on page 239](#)
2. If you need to contact IBM Support, you can speed up your support experience by having the information ready that assists IBM Support in resolving problems with StoredIQ for Legal.

### MustGather: Collecting diagnostic data

Before you contact IBM Support, you must capture diagnostic data that is required to resolve a problem.

Collect the following information:

- Log and trace data. For details, see [“Collecting log and trace data” on page 242](#).
- In the case of docker problems, collect information about the docker. Run the following command:  

```
docker info
```

You must be signed in to the StoredIQ for Legal virtual machine as the root user.
- If StoredIQ for Legal no longer works correctly, log the browser's interaction with StoredIQ for Legal in HAR (HTTP Archive format) files. Complete these steps:
  - a) In your browser, open the developer tools, for example by pressing F12, and go to the **Network** page. Ensure that the network activity is recorded:
    - If you use Mozilla Firefox, the recording of the network activity is automatically enabled.
    - If you use Google Chrome or Microsoft Internet Explorer 11 or later, press Ctrl+E to enable or disable the recording of the network activity.
  - b) Reproduce the steps that lead to the problem.
  - c) On the **Network** page, save the recorded HTTP requests in HAR format, as follows:
    - If you use Firefox V41, or later, right-click anywhere on the **Network** page and then click **Save as HAR with content**.
    - If you use Chrome, right-click anywhere on the **Network** page and then click **Save All as HAR**.
    - If you use Internet Explorer, press Ctrl+S.

## Techniques for troubleshooting problems

---

*Troubleshooting* is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as you expect it to work, and then decide how to resolve the problem.

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical support representative know where to look for the cause of the problem. Ask yourself the following basic questions:

- What are the symptoms of the problem?

- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically establish a good description of the problem, which can then lead you to a resolution.

### **What are the symptoms of the problem?**

When you begin to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward. However, you can break this question into several focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is the failure manifested as a loop, hang, crash, performance degradation, or an incorrect result?

### **Where does the problem occur?**

One of the most important steps in resolving a problem is to determine where the problem originates. Multiple layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you investigate problems.

The following questions help you to focus on the layer of technology in which the problem occurs:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported by the product?
- Do all the users encounter the problem?
- For a multiple-site installation, do all the sites encounter the problem?

When one layer of technology reports the problem, the problem does not necessarily originate in that layer. By understanding the environment in which a problem exists, you can more easily identify where that problem originates. Take the time to completely describe the environment in which the problem exists, including the operating system and version, all the corresponding software and versions, and the hardware that is used in the environment. Verify that you run in an environment that is supported by StoredIQ for Legal. Many problems can be traced to incompatible software levels that are not intended to run together or have not been thoroughly tested together.

### **When does the problem occur?**

Develop a detailed timeline of the events that lead to the failure, especially for the problems that occur only once. By working backwards, you can easily develop a timeline of events. Begin at the time when an error was reported, and be as precise as possible by including even the millisecond. Work backwards through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, and construct a frame of reference in which to investigate the problem, answer these questions:

- Does the problem occur only at a specific time of day or night?
- How frequently does the problem occur?
- What sequence of events leads to the time when the problem is reported?
- Does the problem occur after an environment change such as an upgrade, or after installing software or hardware?



### **Under which conditions does the problem occur?**

For troubleshooting purposes, it is important to know which systems and applications are running when a problem occurs. The following questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur during one particular task or operation?
- Does the problem occur only after a specific sequence of events?
- Do other applications fail at the same time?

By answering questions such as these, you can explain the environment in which the problem occurs and correlate any dependencies. However, when multiple problems occur at about the same time, the problems are not necessarily related.

### **Can the problem be reproduced?**

Under ideal troubleshooting conditions, the problem can be reproduced. When a problem can be reproduced, you typically have a larger set of tools or procedures that can help you to investigate the problem. The problems that you can reproduce are often easier to debug and resolve.

However, the problems that you can reproduce can have a disadvantage. If the problem is of significant business impact, you do not want the problem to occur again. In this case and if it is possible, reproduce the problem in a test environment or a development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be reproduced on a test system?
- Do multiple users or applications encounter the same type of problem?
- Can the problem be reproduced by running a single command, a set of commands, or a particular application?

## **Known problems and solutions**

---

Some common problems with StoredIQ for Legal are documented, along with their solutions or workarounds. If you have a problem with StoredIQ for Legal, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

### **Signin fails due to an incorrect signin ID**

When creating test users, administrators must self-enforce the StoredIQ for Legal restrictions for signin IDs. Otherwise, the test user will not be able to sign in successfully.

#### **Symptoms**

Signin to StoredIQ for Legal fails because a signin ID exceeds the maximum length or contains characters or keywords that are not allowed.

#### **Causes**

StoredIQ for Legal does not automatically block administrators from creating test users that violate the signin ID restrictions.

#### **Resolving the problem**

When creating test users, administrators must ensure that they enforce the StoredIQ for Legal restrictions for signin IDs. See [“Creating test users” on page 75](#) for the restrictions.

## Signin fails due to LDAP referral errors

If you can no longer sign in to StoredIQ for Legal due to LDAP partial result errors or referral errors, you can run a script to reset the configured security domain.

### Symptoms

You configured the connection to the directory server in StoredIQ for Legal and then restarted the StoredIQ for Legal server. You can no longer sign in to StoredIQ for Legal, not even using `ilgadmin`. The `liger.log` file shows nested `host not found` exceptions.

### Causes

The directory server might not be configured properly for referrals and the configured security domain might be corrupted.

### Resolving the problem

Complete these steps:

1. Fix the referral issues on the directory server.
2. Reset the configured security domain by taking these steps:
  - Sign in to the StoredIQ for Legal server.
  - Run the `/siq/bin/remove_secdom.sh` script.
  - Restart the StoredIQ for Legal server.
3. Sign in to StoredIQ for Legal as `ilgadmin` and configure the connection to the directory server again.

## Signin fails after upgrading StoredIQ for Legal

If users can no longer sign in to StoredIQ for Legal after the product has been upgraded, you can apply the following workaround.

### Symptoms

After StoredIQ for Legal has been upgraded, LDAP users can no longer sign in. The upgrade log contains the following error message:

```
Restoring the external directory failed
```

### Causes

The external LDAP directory server could not be reached during the upgrade of StoredIQ for Legal. Therefore, the LDAP configuration could not be applied to the web application server. However, the upgrade completed successfully.

### Resolving the problem

When the LDAP directory server is available again, restart StoredIQ for Legal to create the application server configuration. After that, users can sign in again.

## Signin fails because a connection to the web client could not be established

Your signin can stop working for various reasons.

### Symptoms

Signin to StoredIQ for Legal succeeded previously, but now fails and the following error message is displayed: A connection to the web client cannot be established using the following URL.

### Causes

- You signed out while the signin page was still loaded.

- Your signin session timed out due to the lack of activity.
- You changed your LDAP password but your web browser still uses the old password.
- You lost your network connection.
- Your power went out.
- The StoredIQ for Legal server shut down.

### Resolving the problem

Close your sessions, check your connection to the StoredIQ for Legal server, and retry the signin.

## Enabling single sign-on fails

An error occurs when you try to set up the SSO environment for StoredIQ for Legal.

### Symptoms

After you run the `/siq/bin/enable_sso.sh` script, the SSO environment is not set up properly.

### Causes

Your SSO configuration settings might be incomplete or incorrect.

### Resolving the problem

Complete these steps:

1. Run the `/siq/bin/disable_sso.sh` script to disable SSO authentication.
2. Check your SSO configuration: Edit the `sso_configuration.properties` file, check the settings and update as required.

For details, see [“Configuring single sign-on for StoredIQ for Legal \(VM\)” on page 49](#).

3. Run the `/siq/bin/enable_sso.sh` script again.

## The email server does not send out any emails

As system administrator, you want to send out all available emails immediately. However, an error occurs.

### Symptoms

After you click **Send Now** on the **Email Server** page, you get the following message:

An error occurred when the email server tried to send the emails.

No emails are sent out.

### Resolving the problem

Complete these steps:

1. Check the `liger.log` file for the cause of the problem.
2. If the log file does not help solve the problem, restart the StoredIQ for Legal server.
3. Sign in again. Go to **Admin > External Servers > Email Server** and then click **Send Now**.
4. If you receive the message that all emails were sent out successfully, verify that the emails were sent. If no emails were sent or if you receive an error again, contact IBM Support.

## Search results include false positives

When you search on some special characters, the results can contain false positives.

### Symptoms

The search result list can show false positives, when you search on these special characters: `, [ ] "`

### Causes

The comma, the opening and closing brackets, and the double quotation marks are internally used as delimiters in multivalued custom attributes. Therefore, when you use only one of these special characters as search argument, your results will include all entries that have custom attributes with multiple values.

### Resolving the problem

Expand your search term by one or more characters and repeat the search.

## Workflow fails due to an error

A workflow that is associated with an action or is performed as part of a data request fails due an error.

### Symptoms

The workflow stops and the audit event WF\_ERROR is created.

### Resolving the problem

Complete these steps:

1. Create an audit query for object type Workflow and audit event WF\_ERROR. For more information, see [“Auditing” on page 220](#).
2. Save the audit query results to a CSV file.
3. Open the CSV file and check the `proc_error` column for the cause of the error. The following table provides an overview of how to solve specific problems. For all other problems, contact IBM Support.

Information in <code>proc_error</code> column	Description	What to do
Problem evaluating script	A script cannot be executed.	Check the appropriate script task and fix the affected workflow. The <code>proc_def_id</code> and <code>proc_def_key</code> columns provide more information about the workflow.
Could not send e-mail in execution	The email task could not be completed.	Check the email task and the email variable that is used in the workflow.
No outgoing sequence flow of <i>id</i>	The workflow could not continue with the next outgoing sequence flow.	Ensure that there is at least one sequence flow without a condition or with a condition that evaluates to true.
Exception while executing event-listener	An error was displayed to the user who requested the action that started the workflow.	Request the action again.

### Related tasks

[Contacting IBM Support](#)

## A report in HTML format cannot be viewed

Opening a report in HTML format in a web browser does not work.

### Symptoms

When you try to open and view a report in HTML format in a web browser, the content is not loaded or the browser even might crash.

### **Causes**

This error can occur if a report of one of the following report types contains a huge amount of data:

- Custodian History Report
- User Audit Report
- User Information Report
- User Login Report

### **Environment**

For the Custodian History Report, such errors are limited to Internet Explorer. For the other reports, this error can occur with any web browser.

### **Resolving the problem**

A workaround is to create and open the report in PDF format. It might still take some time to load all data when you open the report. Another workaround for the Custodian History Report is to use a different browser such as Firefox or Chrome to open the report in HTML format.

## **An empty User Audit Report or User Login Report is generated**

Running a User Audit Report or a User Login Report renders a report file without any records.

### **Symptoms**

When you run a User Audit Report or a User Login Report, the generated file does not contain any information besides the information who generated the report and when, and the report parameters.

### **Causes**

Both types of report require a start and end date to be specified. However, due to a limitation in BIRT, these dates cannot be validated. Therefore, specifying an end date that is before the specified start date does not result in an error. Instead, an empty report is created.

### **Resolving the problem**

Check and correct the specified start and end dates. Then, run the report again.

## **The global hold reminder overview lists released custodians until the next reminder cycle starts**

After being released, custodians still show up in the global hold reminder overview.

### **Symptoms**

A custodian who is released from all hold notices that participate in the current global hold reminder cycle will still show up on the Global Hold Reminder Overview page with the status the custodian had before being released from the last hold notice. However, no further follow-up messages to the global hold reminder will be sent to the released custodian.

### **Resolving the problem**

No action required. As soon as the next reminder cycle starts, the list of custodians is updated to reflect only those custodians who have active notices participating in the global hold reminder.

## **Searching the knowledge bases**

---

You can often find the solutions to problems by searching the IBM knowledge bases. You can optimize your results by using the available resources, support tools, and search methods.

You can find useful information about StoredIQ for Legal by searching the StoredIQ for Legal Knowledge Center. Also, search the knowledge bases by using the approaches in the following procedure.

- Find the content that you need by using the [StoredIQ for Legal Support Portal](#).

The Support Portal is a unified, centralized view of the technical support tools and information for StoredIQ for Legal systems, software, and services. From the Support Portal, you have access to the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution.

- Find the content that you need by using the following links.  
These links open queries for StoredIQ for Legal documents on the IBM Support Portal:
    - [StoredIQ for Legal V2.0.3 known problems](#)
    - [All StoredIQ for Legal V2.0.3 documents on the Support Portal](#)
  - Search for content by using the IBM masthead search.  
You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com page.
  - Search for content by using any external search engine, such as Google, Yahoo, or Bing.  
If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, you can find useful problem-solving information about StoredIQ for Legal in news groups, forums, and blogs that are not on ibm.com.
- Tip:** To find information about this product, include *IBM* and *StoredIQ for Legal* in your search.

## Getting fixes from Fix Central

---

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including StoredIQ for Legal. From Fix Central, you can search, select, order, and download fixes for your system and choose from different delivery options. An StoredIQ for Legal product fix might be available for your problem.

Before you download a fix from Fix Central:

- Know your IBM user ID and password. You are required to log in to the Fix Central website before you can download a fix.
- To get information about the download process, or help during the process, see [Fix Central help](http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html) ([http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq\\_sw.html](http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html)).
- If you know exactly which fix you need, you can search for it directly from the **Search Fix Central** field on the [Fix Central](#) website.

To find and download fixes from Fix Central:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from [Fix Central](#).  
This site provides download, installation, and configuration instructions for the update installer.
2. From the Fix Central page, specify the product information for the fix that you need:
  - a) Click **Find product**.
  - b) Select **Product Group > All Software**.
  - c) In the **Product selector** field, type `StoredIQ for Legal`.
  - d) From the **Installed Version** list, select the version that is currently installed on your system.
  - e) From the **Platform** list, select the platform on which you run StoredIQ for Legal.
3. On the **Identify Fixes** page, specify how you want to search for the fix. You have the following options:
  - Browse all the fixes for the specified product, version, and platform.
  - Enter the APAR or SPR numbers that you want to search for.
  - Enter the fix ID.
  - Enter the text for your search keywords.
  - Search a list of the recommended fixes.
  - From the **Additional query options**, mark the checkbox if you want to exclude from your search any fixes for the currently installed version of the product.

4. On the **Select fixes** page, you have the following options:
  - Mark the checkbox next to any fix that you want to download.
  - Clear the list of fixes and return to the Identify fixes page to create a new query and a new list of fixes to choose from.
5. From the Download options page, specify how you prefer to download the fix and any other required information, and click **Download Now**.
6. To apply the fix, follow the instructions in the Readme file that is downloaded with the fix.
7. Optional: Subscribe to the weekly email notifications about fixes and other important IBM Support updates.

## Contacting IBM Support

---

IBM Support provides assistance with product defects, answers FAQs, and helps you to resolve the problems that you encounter with the product.

After trying to find the solution to your problem by using other self-help options such as Technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the [Support portfolio](#) topic in the *"Software Support Handbook"*.

To contact IBM Support about a problem:

1. Define the problem, gather the background information, and determine the severity of the problem. For more information, see [Getting IBM Support](#) in the *"Software Support Handbook"*.
2. Gather the diagnostic information. See ["MustGather: Collecting diagnostic data"](#) on page 233.
3. Submit the problem to IBM Support in one of the following ways:
  - Online through the [IBM Support Portal](#): You can open, update, and view all your service requests from the Service Request portlet on the [Service requests & PMRs](#) page.
  - By phone according to the phone number that is specified for your region in the [Directory of worldwide contacts](#).

If you submit a problem for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever it is possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes the resolved APARs on the IBM Support website daily so that those who experience the same problem can benefit from the same resolution.

## Exchanging information with IBM

---

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Exchanging diagnostic data with IBM happens by using Enhanced Customer Data Repository (ECuRep). ECuRep is a secure and fully supported data repository with problem determination tools and functions. For more information about ECuRep and the processes involved, see the [Enhanced Customer Data Repository \(ECuRep\)](#) website.

For more information about the diagnostic data you need to collect, see ["MustGather: Collecting diagnostic data"](#) on page 233.

## Subscribing to Support updates

---

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

By subscribing to updates about StoredIQ for Legal, you can receive important technical information and updates for specific IBM Support tools and resources.

- To subscribe to Support updates, go to the [IBM Support Portal: Support home](#) and click **Other > My notifications**. Enter the product name and then click **Subscribe**.

## Collecting log and trace data

---

StoredIQ for Legal generates log and trace data that can help you identify, diagnose, and resolve problems with the product.

StoredIQ for Legal automatically logs events and messages, based on the logging level that is set. You can request the log files from the GUI or the command line. The following log files are available:

- The web application server log files
- The StoredIQ for Legal `liger.log` files

If you use the command line, you also get these log files:

- The database log file
- The Security Directory Server log file

The default logging level for the `liger.log` file is ERROR, which usually is sufficient for diagnosing and resolving issues. However, should a more verbose level of logging be required, IBM Support might ask you to set the log level to TRACE.

You can change the logging level for the `liger.log` file from the GUI or the command line. If you use the command line, the web application server is restarted. In the GUI, you also can change the maximum log file size and the maximum number of log files. None of the GUI changes require a restart of the web application server.

### Collecting log and trace data from the command line

You can request the log files and change the logging level by using the `/siq/bin/logs` tool.

You must be signed in to the StoredIQ for Legal virtual machine as the root user.

You can use one of the following commands:

- To request the log files, enter:  
`/siq/bin/logs fetch`

The log files are written to the compressed file `/root/sysData.tar.gz` and are available in the `/root/sysData` directory.

- To delete the current log files from the `/root/sysData` directory, enter:  
`/siq/bin/logs clear`

- To change the logging level, enter one of the following commands:

**`/siq/bin/logs level trace`**

Logs all messages. This is the most verbose level of logging. Use this level for problem analysis only.

**`/siq/bin/logs level debug`**

Logs fine-grained informational messages and all messages of the types INFO, WARN, ERROR, and FATAL.

**`/siq/bin/logs level info`**

Logs informational messages and all messages of the types WARN, ERROR, and FATAL.

**`/siq/bin/logs level warn`**

Logs messages that could potentially cause issues and all messages of the types ERROR and FATAL.

**`/siq/bin/logs level error`**

Logs severe errors and all messages of the type FATAL. This is the default setting and should usually be sufficient for troubleshooting.



### **/siq/bin/logs level fatal**

Logs all errors that might cause the application to end abnormally.

**Important:** When you specify a new logging level, the web application server is restarted.

## **Collecting log and trace data from the GUI**

You can request the log files and change the logging level.

You must be signed in with the **System: Manage** privilege.

Complete these steps:

1. Go to **Admin > Logging**.
2. Change the settings as needed.
  - Change the logging level:

<b>Logging level</b>	<b>Description</b>
TRACE	Logs all messages. This is the most verbose level of logging. Use this level for problem analysis only; usually when told to do so by IBM Support.
DEBUG	Logs fine-grained informational messages and all messages of the types INFO, WARN, ERROR, and FATAL.
INFO	Logs informational messages and all messages of the types WARN, ERROR, and FATAL.
WARN	Logs messages that could potentially cause issues and all messages of the types ERROR and FATAL.
ERROR	Logs severe errors and all messages of the type FATAL. This is the default setting and should usually be sufficient for troubleshooting.
FATAL	Logs all errors that might cause the application to end abnormally.

- Change the maximum log file size. The default value is 5 MB.
- Change the maximum number of log files. The default value is 5.

The `liger.log` file is a rolling file, which means that a new file is written whenever the specified file size is exceeded. The most recent log file is the `liger.log` file. The older files are numbered consecutively, for example, `liger.log.1`. When the defined number of log files is reached, the oldest file is discarded before a new one is created and the numbers of the others are incremented by 1.

3. To collect and download the log files, click **Export Log Files**.

## **Disaster recovery with vSphere Replication**

You can replicate and recover a production StoredIQ for Legal virtual machine (VM) by using VMware vSphere Replication.

**Restriction:** vSphere Replication supports replication in one direction only (from site A to site B). For a bidirectional replication, you must duplicate the replication relationship in the opposite direction (from site B to site A) or purchase an SRM solution.

vSphere Replication has some operational limits. Ensure that your virtual infrastructure complies with these limits before the replication is started.

- You can deploy only one vSphere Replication appliance on a vCenter Server instance. If you deploy another one, vSphere Replication detects, during its restart, that another appliance is already deployed and registered as an extension to vCenter Server. Then, you must confirm whether you want to proceed with the new appliance and re-create all replications or shut it down and restart the old appliance to restore the original vSphere Replication extension thumbprint in vCenter Server.
- Each newly deployed vSphere Replication appliance can manage a maximum of 2000 replications.

For more information, see [Operational Limits for vSphere Replication 6.x \(2102453\)](#).

To set up vSphere Replication, complete the following steps:

1. Download the vSphere Replication appliance from VMware.
2. Deploy the vSphere Replication appliance as a standard OVF template.
3. Sign in to the vSphere Replication appliance as root at `https://ip_address_of_appliance:5480/`.
4. Configure the VRM service.
5. Start the VRM service, and check the vCenter to verify that the VRM is running.
6. Configure the replication between the primary and the secondary site: right-click the VM and then select **All vSphere Replication Actions > Configure Replication**.  
When the primary site is live, the VRM service automatically synchronizes the changes from the primary site to the secondary site.
7. Monitor the progress of the automatic synchronization: go to **vCenter > Monitor > vSphere Replication**.
8. At any time after the replication finishes, you can invoke disaster recovery (when the VM is lost): go to **vCenter > Monitor > Incoming Replications**, right-click the VM, and then click **Recovery**.
9. Power on the recovered VM and connect to the network: right-click the VM and then click **Edit Setting**. Enable the connection.
10. Restart and verify the recovered VM in the browser.  
The IP address of the recovered VM is the same as for the VM that you recovered.

## Managing the size of string attributes

---

You can use the following StoredIQ for Legal tool scripts to check and eventually change the size of string attributes.

The scripts must be run inside the WebSphere Application Server container on the StoredIQ for Legal virtual machine.

The following limitations apply:

- Only custom attributes of the following data types are supported:

- String
- Date range (single)
- Date ranges (multiple)
- Drop-down list (single-select and multiple-select)
- Combination box (single-select and multiple-select)
- Radio button

The following data types are not supported:

- Number
- Date
- Boolean
- Object list (single-select and multiple-select)
- Attachment (single)
- Attachments (multiple)

- You cannot change the size of built-in attributes. Trying to do so results in an error.
- You can reduce the attribute size only to the already consumed size. Trying to reduce it further results in an error.

Complete these steps on an OpenShift client that has access to the cluster where IBM StoredIQ for Legal is deployed.

1. Complete these steps depending on your deployment type:

For StoredIQ for Legal (VM):

- a) Sign in to the StoredIQ for Legal VM as root.
- b) Open the WebSphere Application Server container by running this command:

```
docker exec -it ilg_sol_plugin bash
```

For StoredIQ for Legal (Container), complete these steps on an OpenShift client that has access to the cluster where IBM StoredIQ for Legal is deployed:

- a) Obtain the name of the ilg-sol-plugin container by running this command:

```
CONTAINER_NAME=$(oc get pods -n siq41openshift -l app=ilg-sol-plugin -o name | sed "s/^.\{4\}/")
```

- b) Open the ilg-sol-plugin container by running the following command. Replace `$CONTAINER_NAME` with the name returned in the previous step.

```
oc exec -it $CONTAINER_NAME bash
```

2. Change to the directory where the scripts are stored by running this command:

```
cd /opt/ibm/ilg-sol-toolkit/scripts
```

3. Run one of the following commands.

- To check the attribute size, run this command: `./get_max_string_size.sh entityName`  
The output shows all custom string attributes within the specified attribute category by name, and the allocated size and the maximum consumed size for each attribute.  
Sample command: `./get_max_string_size.sh datarequest`
- To change the attribute size, run this command: `./change_string_field_size.sh entityName attributeName newSize`  
Sample command: `./change_string_field_size.sh datarequest ca_attribute1 10`

The parameters are as follows:

***entityName***

One of the following values:

<b><i>entityName</i></b>	<b>Type of attributes</b>
datasource	Data source
datasourceapplication	Application
datasourceserver	Server
datarequest	Data request
fulfillmentitem	Fulfillment item
fulfillmentworkpackage	Work package
interview	Interview
matter	Matter
notice	Hold notice
noticedraft	Hold notice (draft)
noticehistory	Hold notice (history)
persondistinct	Person

***attributeName***

The name of the attribute for which you want to change the size.

***newSize***

The new size to apply to the attribute. The minimum size for an attribute must be calculated as follows:

- For single-select attributes:  $\text{size of the longest option} * \text{number of options} + 100$
- For multiple-select attributes:  $\text{size of the longest option} + 100$

# Reference

Find information about StoredIQ for Legal tools, default file names, nonmodifiable data request attributes, and the available workflow services.

## Administration scripts

StoredIQ for Legal comes with a set administration scripts, for example, for reconfiguring the virtual machine (StoredIQ for Legal (VM)) or for changing passwords.

### StoredIQ for Legal (VM) scripts

To run these tools, log in to the StoredIQ for Legal virtual machine as `root`.

Command	Purpose
<code>/siq/bin/netcfg</code>	Change the network configuration for StoredIQ for Legal.  For more information, see <a href="#">“Configuring StoredIQ for Legal (VM)”</a> on page 42.
<code>/siq/bin/cert_install -t -p ilgadmin_pwd</code>	Install and remove SSL certificates.  For more information, see <a href="#">“Installing and removing custom SSL certificates for StoredIQ for Legal (VM)”</a> on page 47.
<code>/siq/bin/enable_sso /siq/bin/disable_sso</code>	Enable or disable single sign-on.  For more information, see <a href="#">“Configuring single sign-on for StoredIQ for Legal (VM)”</a> on page 49.
<code>/siq/bin/change_ilgadmin_password -o old_pwd -n new_pwd</code>	Change the password for the default system administrator <code>ilgadmin</code> .
<code>/siq/bin/change_reportadmin_password - n new_pwd -p ilgadmin_pwd</code>	Change the password for the default report administrator <code>reportadmin</code> .  In addition, the script updates the web application server connection settings with the new password and restarts the application server after the password change is complete.
<code>/siq/bin/logs</code>	Collect the log files and change the logging level.  For more information, see <a href="#">“Collecting log and trace data from the command line”</a> on page 242.
<code>/siq/bin/remove_secdom</code>	Reset the configured security domain.  For more information, see <a href="#">“Signin fails due to LDAP referral errors”</a> on page 236.

Additional scripts are stored as listed:

Package or tool	Purpose
CLI package	<code>siq41</code> command line interface. The package must be downloaded and installed as described in

Package or tool	Purpose
	<a href="#">“Installing the import command line interface (CLI)” on page 179.</a>
Migration tool	Migrate Atlas Policy Suite data to StoredIQ for Legal. The <b>migrate.py</b> tool is located in the <code>/siq/migration</code> directory on your StoredIQ for Legal system.  For more information, see <a href="#">“The migration tool” on page 198.</a>

### StoredIQ for Legal (Container) scripts

You can run these scripts from any OpenShift client that has the **oc** client tool installed (for more information, see [Get Started with the CLI in the OpenShift documentation](#)) and that has access to the cluster where IBM StoredIQ for Legal is deployed, or from the master node of the cluster.

These scripts are stored in the `IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_CLOUD/scripts` directory:

Command	Purpose
<code>change_ilgadmin_password -o <i>old_pwd</i> -n <i>new_pwd</i></code>	Change the password for the default system administrator <code>ilgadmin</code> .
<code>change_reportadmin_password -n <i>new_pwd</i> -p <i>ilgadmin_pwd</i></code>	Change the password for the default report administrator <code>reportadmin</code> .  In addition, the script updates the web application server connection settings with the new password and restarts the application server after the password change is complete.
<code>post_restore_script</code>	Finalize migration from StoredIQ for Legal (VM) to an OpenShift environment, for example, by updating the encoded <code>ilgadmin</code> password in the configuration file, by initializing the schema, and by re-initializing the external LDAP.

These scripts are stored in the `IBM_STOREDIQ_FOR_LEGAL_Vv.r.m.fp_CLOUD/tools` directory:

Package or tool	Purpose
CLI package in the <code>siq41</code> subdirectory	<code>siq41</code> command line interface. The package must be downloaded and installed as described in <a href="#">“Installing the import command line interface (CLI)” on page 179.</a>
Migration tool package in the <code>migration</code> subdirectory	Migrate Atlas Policy Suite data to StoredIQ for Legal. The directory holds the tool and all related setup and configuration files.  For more information, see <a href="#">“The migration tool” on page 198.</a>

## Default file names

Starting with StoredIQ for Legal version 2.0.3.4, the default names of files that are created by StoredIQ for Legal have a different format. Review the default file name mapping to learn about the changes.

Exported data	StoredIQ for Legal version 2.0.3.3 and earlier	StoredIQ for Legal version 2.0.3.4 and later
Task list	YYYY-MM-DD hh-mm-ss Tasks Export.csv	TaskList_task_filter_YYYY-MM-DD_hh-mm-ss.csv <i>task_filter</i> corresponds to your <b>Tasks &gt; selection</b> .
Matter list	YYYY-MM-DD hh-mm-ss Matters Export.csv	MatterList_YYYY-MM-DD_hh-mm-ss.csv
Data request: custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	DR_datarequestID_Custodians_YYYY-MM-DD_hh-mm-ss.csv
Data request: request information for custodians	datarequest_custodians.csv	DR_datarequestID_CustodiansRequestInfo_YYYY-MM-DD_hh-mm-ss.csv
Hold notice (draft): custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	Notice_notice_name_Custodians_YYYY-MM-DD_hh-mm-ss_DraftCustodians_YYYY-MM-DD_hh-mm-ss.csv
Hold notice (published): custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	Notice_notice_name_Custodians_YYYY-MM-DD_hh-mm-ss_Custodians_YYYY-MM-DD_hh-mm-ss.csv
Interview (draft): custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	Interview_interview_name_Custodians_YYYY-MM-DD_hh-mm-ss_DraftCustodians_YYYY-MM-DD_hh-mm-ss.csv
Interview (published): custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	Interview_interview_name_Custodians_YYYY-MM-DD_hh-mm-ss_Custodians_YYYY-MM-DD_hh-mm-ss.csv
Interview results	responses.zip	Interview_interview_name_Results_YYYY-MM-DD_hh-mm-ss.csv
Data box: custodian list	YYYY-MM-DD hh-mm-ss Custodians Export.csv	DataBox_databox_name_Custodians_YYYY-MM-DD_hh-mm-ss.csv
Work package: list of fulfillment items	workpackage_items.csv	DR_datarequestID_WP_workpackageID_YYYY-MM-DD_hh-mm-ss.csv  If the user exporting the data does not have the privilege to view or manage data requests, the file name defaults to:

Exported data	StoredIQ for Legal version 2.0.3.3 and earlier	StoredIQ for Legal version 2.0.3.4 and later
		WP_workpackageID_YYYY-MM-DD_hh-mm-ss.csv
List of the matters in which a custodian is involved	YYYY-MM-DD hh-mm-ss Matters Export.csv	MatterInvolvements_personID_YYYY-MM-DD_hh-mm-ss.csv
Attributes	exportAttributes_attribute_filter.json <i>attribute_filter</i> corresponds to your <b>Attributes &gt; selection</b> .	No change
People: (filtered) list of all people	N/A	People_YYYY-MM-DD_hh-mm-ss.csv
People: (filtered) list of external persons	N/A	People_ExternalPersons_YY-YY-MM-DD_hh-mm-ss.csv
People: (filtered) list of employees	N/A	People_Employees_YYYY-MM-DD_hh-mm-ss.csv
People: (filtered) list of temporary employees	N/A	People_TemporaryEmployees_YYYY-MM-DD_hh-mm-ss.csv
People: (filtered) list of functional IDs	N/A	People_FunctionalIDs_YYYY-MM-DD_hh-mm-ss.csv
People: (filtered) list of any additional person category	N/A	People_category_name_YYYY-MM-DD_hh-mm-ss.csv
Groups: (filtered) list of people in a custodian group	N/A	CustodianGroup_group_name_YYYY-MM-DD_hh-mm-ss.csv

## Nonmodifiable data request attributes

The values of some built-in data request attributes cannot be modified after a data request is submitted.

The following built-in attributes cannot be updated during refinement of the data request:

- type
- externalid
- requestor
- fulfillmentinstructions
- requiresjurisdictionapproval
- terms
- priority\_cpx

In addition to these attributes, the built-in datasourcecategory attribute cannot be modified while the data request is open.

## Server discovery Java class reference

The following classes can be used in workflows that use server discovery for creating fulfillment items automatically.

The details of the Java classes used in the workflow are as follows:



### **com.ibm.ilg.workflow.server.discovery.bpmn.DiscoverServers**

Sends server discovery job requests to the service. It internally calls the SOAP method createJob. This class has the following parameters:

<b>Name</b>	<b>Type</b>	<b>Description</b>
connectorId	String	Required. The external ID of the registered server discovery service connector to be used.
custodianIdAttribute	String	Optional. The system ID of the attribute to be used as the person identifier on the service side. If not specified, the system default is used.
discoveryInfoMessage	String	Optional. It allows to pass additional information for this discovery request to the service.
autoCompleteUserTask	String	Optional. If the ID of a user task is specified, this task is automatically closed when the server discovery job process completes.

### **com.ibm.ilg.workflow.server.discovery.bpmn.GetJobStatus**

Obtains any cached job values, which are available in form of the serverDiscoveryJob process variable. No internal calls to any SOAP methods are issued. This class also does not have any parameters.

The serverDiscoveryJob process variable contains this information:

<b>Name</b>	<b>Type</b>	<b>Description</b>
connectorJobId	Long	The service side job ID.
status	String	Possible values: <b>REQUEST_SENDING</b> createJob has been called but the service has yet to respond. <b>STARTED</b> createJob is done but getJobStatus has yet to be called. <b>RUNNING</b> getJobStatus returned RUNNING. <b>COMPLETE_RESULT_FETCHING</b> getJobStatus returned COMPLETE and the system is calling getJobResults to create fulfillment items.

Name	Type	Description
		<p><b>COMPLETE_RESULT_FETCHED</b> Fulfillment items are created and the job can be closed.</p> <p><b>CLOSE</b> closeJob has been called.</p> <p><b>ERROR</b> An error occurred in the service or on StoredIQ for Legal side.</p>
statusstring	String	Optional. Human-readable message returned from the service through getJobStatus.
errorId	String	The error ID returned from the service if an error happened, otherwise null.

#### **com.ibm.ilg.workflow.server.discovery.bpmn.CancelJob**

Requests to stop the job by the calling the SOAP method closeJob. This class does not have any parameters.

## Server discovery WSDL reference

Use the server discovery WSDL reference when you create a server discovery connector.

To implement a server discovery connector, set up a web service that implements the definitions in the Web Services Description Language (WSDL) file provided with StoredIQ for Legal and register it. You can find the WSDL file in the ilg\_sol\_plugin container at the following location:

```
/home/was/WebSphere/AppServer/profiles/ilgnext/installedApps/
websphereNode01Cell/ilg-sol-rest.ear/ilg-sol-rest.war/META-INF/wsd1/
ServerDiscovery.wsdl
```

#### **getHealthStatus**

This action provides information about whether the server discovery service is ready to be connected to StoredIQ for Legal. It is used to validate the connection when you register the service in the StoredIQ for Legal GUI and for showing the server status.

#### **Request object**

None.

#### **Response object.**

None. An exception is thrown if the server is not ready.

#### **createJob**

This action starts a server discovery job. It's expected that the actual server discovery is executed asynchronously so that createJob can respond quickly. The server discovery results are fetched later in separate call (getJobResults).

#### **Request object**

##### **discoveryRequests**

Custodian-specific information. One discovery request per custodian.

Type: *ArrayDiscoveryRequest*

**custodianId**

The ID of the custodian. It's one of the person attributes defined in StoredIQ for Legal, such as signin ID or email address. You specify which attribute to use as the custodian ID by using a process variable.

Type: String

**custodianIdAttribute**

The attribute that `custodianId` is mapped to in StoredIQ for Legal. You don't have to handle this value on the service side. You just have to return in the `getJobResults` call.

Type: String

**discoveryInfoMessage**

Custodian-specific information from the requestor.

Type: String

**overwriteDateRanges**

Individual date ranges per custodian (periods of interest), which overwrite any globally defined date ranges. For example, if the global data range is 2019/4/1 - 2019/4/30 and the overwrite value is 2019/5/1 - 2019/5/31, the actual date range that is taken into account is 2019/5/1 - 2019/5/31, not 2019/4/1 - 2019/5/31. If no overwrite values are provided, the global date ranges are applied.

Type: *ArrayDateRange*

**globalCriteria**

Data request information.

**dataSourceCategories**

Categories of data sources. The list of available data source categories is defined on the **Data Source Attributes** page in the StoredIQ for Legal **Admin** section.

Type: Array

**dateRanges**

Periods of interest for the identification. **dateRanges** can be overwritten per custodian. If the array is empty, everything is expected (from the past until the date of fulfillment).

Type: *ArrayDateRange*

**discoveryInfoMessage**

Message from the requestor.

Type: String

**Response object****connectorJobId**

The ID of the job. You can set any number on the service side as long as the ID is unique within one registered connector. StoredIQ for Legal uses this ID for querying the job results.

Type: Integer

**getJobStatus**

This action provides the job status. It is executed periodically after the `createJob` call until the status becomes COMPLETE or ERROR.

**Request object****connectorJobId**

The ID of the job.

Type: Integer

## Response object

### **jobStatus**

The job status. This information is used to direct the workflow. The job status can be one of these values:

#### **RUNNING**

The job is active.

#### **COMPLETE**

The job completed successfully and the results are ready to be fetched.

#### **ERROR**

The job ended with an error.

### **jobStatusMessage**

Human readable details about the status that surface in the task view of StoredIQ for Legal.

Data type: String

## getJobResults

This action returns the results of the server discovery. It's executed after the job status becomes COMPLETE. Usually, this is done only once, but don't dispose of the result until `closeJob` is called. You might need to retry in case of an error.

## Request object

### **connectorJobId**

The ID of the job.

Type: Integer

## Response object

### **discoveryResults**

A list of fulfillment items found by the server discovery service.

Type: *ArrayDiscoveryResult*

### **custodianId**

The ID of the custodian given in the request object.

Type: String

### **custodianIdAttribute**

The attribute that `custodianId` is mapped to in StoredIQ for Legal. The attribute is provided in the request object.

Type: String

### **attributes**

A collection of attributes that you want to set on the fulfillment item to be created. The allowed attributes are the same as the ones allowed for creating fulfillment items from a CSV file. For example, you can't set `resultcount`. If an invalid attribute is specified, the fulfillment item won't be created.

Type: *ArrayAttribute*

#### **key**

The internal ID of the respective fulfillment item attribute

Type: String

#### **value**

The attribute value to be set for the fulfillment item to be created

Type: Object

**dataSourceId**

The data source catalog ID defined in StoredIQ for Legal.

Type: String

**dateRanges**

Periods of interest for the fulfillment item.

Type: *ArrayDateRange*

**discoveryInfoMessage**

Fulfillment-item specific message from the service side.

Type: String

**errorInfoMessage**

Error message for the workflow. If `errorInfoMessage` has a value, the workflow is regarded as showing an error and no fulfillment items are created.

Type: String

**userInfoMessage**

Global message to the workflow.

Type: String

**closeJob**

This action does all required job cleanup on the service side. It notifies the service that no further connector calls with this `connectorJobID` are made (You can have the service throw an exception if another call is made after `closeJob`). `closeJob` can also be called before job completion to cancel a job.

**Request object****connectorJobId**

The ID of the job.

Data type: Integer

**Response object**

None.

**Exceptions**

Any exception should be converted to `ServerDiscoveryServiceException`.

**ServerDiscoveryServiceException****errorId**

The error ID. Set error IDs based on your naming conventions.

Data type: String

**message**

Error details that are written to the log.

Data type: String

## Workflow services

---

StoredIQ for Legal provides a set of built-in functions that you can use in your workflow.

You can use these functions in BMPN expressions and script tasks to serve purposes such as showing information to users, creating branch conditions in your workflow, or modifying the behavior of the system. Functions are bundled in so-called *services* and are usually related to specific legal objects, such as matters, data requests, or fulfillment items.

Service	Type of object
<a href="#">“Custom attribute update service” on page 257</a>	Any object
<a href="#">“Data request service” on page 257</a>	Data request
<a href="#">“Data source service” on page 260</a>	Data source
<a href="#">“Fulfillment automation service” on page 261</a>	Fulfillment item
<a href="#">“Fulfillment item service” on page 261</a>	Fulfillment item
<a href="#">“Work package service” on page 262</a>	Work package
<a href="#">“Interview service” on page 263</a>	Interview
<a href="#">“Lifecycle state service” on page 263</a>	Data request Work package
<a href="#">“Matter category service” on page 264</a>	Matter category
<a href="#">“Matter service” on page 264</a>	Matter
<a href="#">“Notice service” on page 266</a>	Notice
<a href="#">“People service” on page 266</a>	Person
<a href="#">“Role service” on page 266</a>	Role

The following sections describe the workflow services for reference only. You can find details about how to work with these services and samples for their use in this series of articles about workflows in StoredIQ for Legal:

- [Workflows in IBM StoredIQ for Legal: Part 1 - Your first workflow](#)
- [Workflows in IBM StoredIQ for Legal: Part 2 - Refined approval workflow](#)
- [Workflows in IBM StoredIQ for Legal: Part 3 - Introducing process variables](#)
- [Workflows in IBM StoredIQ for Legal: Part 4 - Workflow services](#)

For more information about the fulfillment automation service, see [“Planning for fulfillment automation” on page 34](#)

All service calls return a JSON response, which in general contains a collection of attribute/value pairs, or a list of values, or both. The attributes are specific to the object for which a service is called. Besides the set of predefined attributes for an object and their respective values, additional information such as the custom attributes defined for an object type and other object-specific information is returned.

**Tip:** For more information about the predefined attributes, see the report views sections ([“Creating reports by using reporting views” on page 126](#)). To check which custom attributes exist for a given object type, go to the respective attributes section under **Admin > Attributes**.

A JSON response looks similar to the following response to a `noticeService.get(noticeID)` call:

```
{
  "template": {
    "id": 16,
    "name": "Notice Template 1",
    "uiconfig": {
      "lockmsg": false
    }
  },
  "suspendedcustodianset": 12,
  "respondto": 38,
  "status": "Published",
  "ccrecipientcustodianset": 11,
  "removedccrecipientcustodianset": 11,
  "CreationDate": "2017-04-05T15:02:53+00:00",
  "publisheddate": "2017-04-05T15:04:43+00:00",
  "messagemask": null,
}
```

```

"activecustodianset": 12,
"lastfollowupset": null,
" id": 1,
"ModifiedDate": "2017-04-05T15:04:43+00:00",
"lastissuancedate": null,
"workflowlock": null,
"description": "",
"lastfollowupdate": null,
"name": "Test Notice",
"defaultlanguage": null,
"matterid": 17,
"releasestatus": "Released",
"releasedcustodianset": 11,
"lastissuanceset": null
}

```

### Custom attribute update service

This service has the following method:

#### update

Updates custom attributes of any StoredIQ for Legal object

##### Input parameters

###### *type*

The type of the object that will be updated, for example, matter, custodian, or work package

###### *id*

The ID of the object that will be updated

###### *update*

The JSON object containing the update payload

##### Response

A JSON response object containing the updated object

##### Syntax

```
customAttributeUpdateService.update('type', id, update)
```

### Data request service

This service has the following methods:

#### get

Retrieves a data request

##### Input parameters

###### *dataRequestID*

The ID of the data request to retrieve

##### Response

A JSON response object containing the retrieved data request

##### Syntax

```
dataRequestService.get(dataRequestID)
```

### numberOfNonMappedCustodians

Returns the number of custodians not mapped to a data source

##### Input parameters

###### *dataRequestID*

The ID of the data request

##### Response

The number of custodians not mapped to a data source

## Syntax

```
dataRequestService.numberOfNonMappedCustodians(dataRequestID)
```

## setAllowWorkPackageSubmit

Enables or disables the submission of work packages of the specified data request

### Input parameters

#### ***dataRequestID***

The ID of the data request

#### ***allow***

Boolean value of `true` to enable submission or `false` to disable submission

## Syntax

```
dataRequestService.setAllowWorkPackageSubmit(dataRequestID,allow)
```

## addDatasource

Adds a data source to a custodian of a data request

### Input parameters

#### ***matterID***

The ID of the matter to which the data request belongs

#### ***dataRequestID***

The ID of the data request

#### ***custodianID***

The ID of the custodian

#### ***dataSourceID***

The ID of the data source to be added to the custodian

### Response

A JSON response object of created fulfillment items. If the custodian is already mapped to the data source, `null` is returned.

## Syntax

```
dataRequestService.addDatasource(matterID,dataRequestID,custodianID,dataSourceID)
```

## listCustodians

Lists all custodians including any edited request information of the given data request

### Input parameters

#### ***matterID***

The ID of the matter to which the data request belongs

#### ***dataRequestID***

The ID of the data request

#### ***start***

The start index

#### ***pageSize***

The maximum number of custodians to return

### Response

A JSON response object containing the list of custodians

## Syntax

```
dataRequestService.listCustodians(matterID,dataRequestID,start,pageSize)
```



## clone

Creates a new data request based on an existing data request. This works very similar to duplicating a data request in the UI. The attributes defined in the request information form (intake criteria form) and the custodians are copied from the source data request.

### Input parameters

#### ***sourceDataRequestID***

The ID of the data request to be cloned

#### ***attributes***

A JSON object containing the attributes for the new data request

#### ***name***

The name of the new data request. This attribute is required.

#### ***description***

A human-readable description of the new data request.

#### ***requestpriority\_cpx***

The priority of the new data request. Possible values are High, Medium, and Low.

This attribute is required. It cannot be modified after the new data request is created.

#### ***type***

The type of the new data request. Possible values are identification, preservation, collection, preservationAndCollection, and deletion.

This attribute is required. It cannot be modified after the new data request is created.

#### ***templatename***

The name of the data request template to be applied to the new data request

This attribute is required. It cannot be modified after the new data request is created.

#### ***duedate***

The due date of the new data request in ISO 8601 format. This attribute cannot be modified after the new data request is created.

#### ***requestor***

The person ID of person who creates this data request. If not specified, requester of the source data request is set. This attribute cannot be modified after the new data request is created.

### Response

A JSON response object containing the newly created data request

### Syntax

```
dataRequestService.clone(sourceDataRequestID,attributes)
```

## submitDataRequest

Submits a data request into the workflow. Scripts or service tasks that call this API must be marked asynchronous.

### Input parameters

#### ***dataRequestID***

The ID of the data request to be submitted

#### ***starter***

The ID of the person who submits the data request. Usually, the ID of the person who started the parent workflow (*starter.id*) is set.

### Response

A JSON response object representing the data request

### Syntax

```
dataRequestService.submitDataRequest(dataRequestID,starter)
```

## **submitAllWorkPackages**

Submits all work packages in draft state under the specified data request. Scripts or service tasks that call this API must be marked asynchronous.

### **Input parameters**

#### ***matterID***

The ID of the matter to which the data request belongs

#### ***dataRequestID***

The ID of the data request to which the work packages belongs

#### ***starter***

The ID of the person who submits the work packages. Usually, the ID of the person who started the data request's workflow (*starter.id*) is set.

### **Syntax**

```
dataRequestService.submitAllWorkPackages(matterID,dataRequestID,starter)
```

## **Data source service**

This service has the following methods:

### **list**

Retrieves all data sources

### **Input parameters**

#### ***start***

The start index

#### ***pageSize***

The maximum number of data sources to return

### **Response**

A JSON response object containing the list of data sources

### **Syntax**

```
dataSourceService.list(start,pageSize)
```

### **listByCategory**

Retrieves a list of all data sources of the specified data source category

### **Input parameters**

#### ***start***

The start index

#### ***pageSize***

The maximum number of data sources to return

#### ***category***

The data source category to list the data sources for

### **Response**

A JSON response object containing a filtered list of data sources

### **Syntax**

```
dataSourceService.listByCategory(start,pageSize, 'category')
```

### **getByExternalId**

Retrieves the data source with the specified unique ID

### **Input parameters**

#### ***uniqueID***

The unique ID of the data source to return

**Response**

A JSON response object containing the data source

**Syntax**

```
dataSourceService.getByExternalId('uniqueID')
```

**Fulfillment automation service**

This service has the following method:

**getJob**

Retrieves the status of the fulfillment job and additional status information.

**Input parameters*****frameworkJobID***

The ID of the fulfillment job within the connector framework.

**Response**

A JSON response object containing information about the progress and the status of the job. Status information can be JobCreationPending, running, complete, complete\_cancelled, complete\_wrapped\_up, complete\_killed, or error.

**Syntax**

```
fulfillmentAutomationService.getJob(frameworkJobID)
```

**Fulfillment item service**

This service has the following methods:

**get**

Retrieves the fulfillment item with the specified ID

**Input parameters*****fulfillmentItemID***

The ID of the fulfillment item to retrieve

**Response**

A JSON response object containing the fulfillment item

**Syntax**

```
fulfillmentItemService.get(fulfillmentItemID)
```

**update**

Updates a fulfillment item with the given content. The following attributes can be updated: resultcount, resultsize, currenttaskstatus, resultsizeunit, otherunit\_cpx, comment, fulfillmentinstructions, dateranges\_cpx, and useridforsearch

**Input parameters*****dataRequestID***

The ID of the data request

***workPackageID***

The ID of the work package

***fulfillmentItemID***

The ID of the fulfillment item

***update***

The JSON object containing the update payload

**Response**

A JSON response object containing the updated fulfillment item

## Syntax

```
fulfillmentItemService.update(dataRequestID,workPackageID,fulfillmentItemID,update)
```

## Work package service

This service has the following methods:

### get

Retrieves a work package

#### Input parameters

##### *workPackageid*

The ID of the work package to retrieve

#### Response

A JSON response object containing the work package

#### Syntax

```
fulfillmentWorkPackageService.get(workPackageID)
```

### getFulfillmentItems

Returns a list of the fulfillment items of the work package

#### Input parameters

##### *id*

The ID of the work package for which the fulfillment items are retrieved

#### Response

A JSON response object containing the list of fulfillment items

#### Syntax

```
fulfillmentWorkPackageService.getFulfillmentItems(workPackageID)
```

### enableItemTaskStatus

Resets the status of fulfillment items to enable repeated checks

#### Input parameters

##### *workPackageID*

The ID of the work package

#### Syntax

```
fulfillmentWorkPackageService.enableItemTaskStatus(workPackageID)
```

### disableItemTaskStatus

Displays an editable status of fulfillment items

#### Input parameters

##### *workPackageID*

The ID of the work package

#### Syntax

```
fulfillmentWorkPackageService.disableItemTaskStatus(workPackageID)
```

### areAllFulfillmentItemsDone

Checks whether all fulfillment items of the work package have the status completed or completed with error

#### Input parameters

##### *workPackageID*

The ID of the work package

## Response

Boolean value of `true` if all fulfillment items have the status `completed` or `completed with error`, or of `false` if any of the fulfillment items does have any other status.

## Syntax

```
fulfillmentWorkPackageService.areAllFulfillmentItemsDone(workPackageID)
```

## setAllowWorkPackageSubmit

Enables or disables the submission of individual work packages of the specified data request

### Input parameters

#### *matterID*

The matter ID of the data request

#### *dataRequestID*

The ID of the data request

#### *workPackageIDs*

An array of those work package IDs for which you want to enable or disable submission

#### *allow*

##### **true**

Enables submission of the specified work packages regardless of whether work package submission is enabled or disabled at the data request level.

##### **false**

Disables submission of the specified work packages regardless of whether work package submission is enabled or disabled at the data request level.

##### **null**

Applies the setting specified at the data request level. This is the default.

## Syntax

```
fulfillmentWorkPackageService.setAllowWorkPackageSubmit(matterID,dataRequestID,workPackageIDs,allow)
```

## Interview service

This service has the following method:

### **get**

Retrieves an interview

### Input parameters

#### *interviewID*

The ID of the interview to retrieve

### Response

A JSON response object containing the interview

### Syntax

```
interviewService.get(interviewID)
```

## Lifecycle state service

This service has the following methods:

### **getStates**

Retrieves a list of possible lifecycle states

### Input parameters

***processInstanceID***

The process instance ID

### Response

A list of possible lifecycle states

### Syntax

```
lifecycleStateService.getStates('processInstanceID')
```

### setState

Sets the lifecycle state of a data request or work package

### Input parameters

***type***

The object type: datarequest or fulfillmentworkpackage

***id***

The ID of the data request or work package

***state***

The state to set

***matterID***

The matter ID

### Syntax

```
lifecycleStateService.setState('type',id,'state',matterID)
```

### Matter category service

This service has the following methods:

#### get

Retrieves a matter category

### Input parameters

***matterCategoryID***

The ID of the matter category to retrieve

### Response

A JSON response object containing the matter category

### Syntax

```
JSONObject matterCategoryService.get(matterCategoryID)
```

### Matter service

This service has the following methods:

#### get

Retrieves a matter

### Input parameters

***matterID***

The ID of the matter to retrieve

### Response

A JSON response object containing the matter

### Syntax

```
matterService.get(matterID)
```

## getMatterStatistics

Retrieves statistics for all matters in StoredIQ for Legal

### Input parameters

Not applicable

### Response

A JSON response object containing the total count of matters in the system, the total number of matters created in the current year, and the number of matters in the current year that include data requests

### Example

```
{
  *   "totalNumberOfMatters" : 20;
  *   "numberOfMattersCreatedInCurrentYear": 8;
  *   "numberOfMattersInCurrentYearWithDataRequests": 5;
  * }
```

### Syntax

```
matterService.getMatterStatistics()
```

## listDataRequests

Retrieves all data requests for the specified matter irrespective of their status or their type.

### Input parameters

#### *matterID*

The matter ID

### Response

A JSON response object containing the list of data requests containing the ID, the name, the type, and the status of each data request

### Syntax

```
matterService.listDataRequests(matterID)
```

## listInterviews

Retrieves all interviews for the specified matter irrespective of their status or their type. Migrated interviews are listed only after they are verified in the migration portal.

### Input parameters

#### *matterID*

The matter ID

### Response

A JSON response object containing the list of interviews containing the ID, the name, and the status of each interview

### Syntax

```
matterService.listInterviews(matterID)
```

## listNotices

Retrieves all notices for the specified matter irrespective of their status or their type. Migrated notices are listed only after they are verified in the migration portal.

### Input parameters

#### *matterID*

The matter ID

### Response

A JSON response object containing the list of notices containing the ID, the name, and the status of each notice

## Syntax

```
matterService.listNotices(matterID)
```

## Notice service

This service has the following method:

### get

Retrieves a notice

### Input parameters

#### *noticeID*

The ID of the notice to retrieve

### Response

A JSON response object containing the notice

## Syntax

```
noticeService.get(noticeID)
```

## People service

This service has the following method:

### get

Retrieves a user entry

### Input parameters

#### *personID*

The ID of the person for whom to retrieve the data

### Response

A JSON response object containing the person information

## Syntax

```
peopleService.get(personID)
```

## Role service

This service has the following method:

### getByName

Retrieves a role object

### Input parameters

#### *name*

The name of the role

### Response

A JSON response object containing the role information including the role ID

## Syntax

```
roleService.getByName('name')
```



## Notices

---

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM 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 IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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.

#### 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 IBM, 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. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown.

© (your company name) (year).

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. \_enter the year or years\_.

## Trademarks

---

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

VMware, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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.

Red Hat and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

## Terms and conditions for product documentation

---

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 IBM 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 IBM.

### 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 IBM.

### 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.

IBM 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 IBM, 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.

IBM 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.

## IBM Online Privacy Statement

---

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, user name, password and role for purposes of session management, authentication, or other usage tracking or functional purposes. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at [www.ibm.com/privacy](http://www.ibm.com/privacy) and IBM's Online Privacy Statement at [www.ibm.com/privacy/details](http://www.ibm.com/privacy/details) the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at [www.ibm.com/software/info/product-privacy](http://www.ibm.com/software/info/product-privacy).



Product Number: 5725-W53