Kofax iRemit
Administrator's Guide

Version: 8.0.0

Date: 2022-06-27

KOFAX

Table of Contents

Preface

This guide details information about how to manage groups and their users, broadcast notifications, holiday calendars, sweep and data, and view the extracted data from archives. It also provides information on different audit reports.

Related documentation

To access the full documentation set online, see the Product Documentation page. However, if necessary, you can download the documentation to use offline.

Training

Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the Kofax Education Portal on the Kofax website.

Getting help with Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base:

1. Go to the Kofax website home page and select **Support**.

2. When the Support page appears, select **Customer Support** > **Knowledge Base**.

ⓘ The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.
  Type your search terms or phrase into the **Search** box, and then click the search icon.

- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:
- Access the Kofax Community (for all customers).

  Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

About Kofax iRemit

Kofax iRemit provides highly secure, distributed access to remittance data and related document images for historical transaction content management. Banks and third-party lockbox providers use iRemit to provide data and document access to their lockbox clients.

Authorized users can search for, display, download, or export data and related document images in the iRemit archive - including checks, remittance coupons, lists, invoices, correspondence, and envelopes - for one or more transactions.

In addition to the long-term archive (LTA), iRemit offers the following optional modules. These modules are only available to users with the appropriate access rights.

- Daily Summary

  This module gives users a drill-down view of their archive data.

- Client Decisioning Module (CDM)

  This module allows users to retrieve exception transactions and decisions and update the status of these transactions to allow for timely deposits of remittances.

- Post Processing Work (PPW)

  This module allows users to perform a variety of tasks on identified post-processing remittance transactions (checks, coupons, correspondence) that require some sort of action or status change.

Kofax iRemit also offers subscription services for the following features:

- Dashboard

  This module provides an at-a-glance view or daily totals.

- Download IDX

  This module enables users to download scheduled extracts from the archive.

- IR Workflow

  This module enables users to add or edit virtual stubs to electronic transactions.

- Notifications

  This module enables users to receive notifications for different application events.

- Auditing

  This module allows you to view different reports.

> ⓘ The menu labels, module names, and available features may differ depending upon the user roles and group (organization) selected.

Group Management

Groups are used in Kofax iRemit to organize and customize client sites and control user access to the data. You can define different settings for different groups, according to the individual requirements of each group. When you create users, you assign them to groups. Users can only access the data of the groups to which they are assigned.

Groups are arranged in a hierarchical structure, with the processor organization at the top group level. Groups and subgroups inherit their settings from the parent group unless you override the parent setting by defining an individual setting for the group.

Users with the role Group Admin role can complete their client setups using templates. They can add groups, customize fields, set preferences for Security, LTA, PPW, CDM and Correspondence, and add a site/work source to a client so that files may be imported. Client setup and editing can only be done in the configuration environment. Client setups must be tested by loading test files and checking that the setup appears and functions as expected. After this testing is completed, Group Admins can schedule the setup for promotion to the production environment.

Open Group Management

To manage groups, on the toolbar, select **Administration** > **Group Management**.

The group hierarchy is displayed in a tree on the left side of the page. The group currently being worked on is highlighted. Click a group to select it. The group's properties are displayed in the center of the page.

> ❶ If you selected a group in the group selection list on the **Home** page, only that group and its subgroups are displayed when you open **Group Management**.

Click the options on the right of the page to configure a group. The available options depend upon the selected group and your assigned user roles.

The following icons may be displayed to the left of a group:

Icon	Description
●	Top group level.
▢	Group level. This level represents the processor organization.
⋯	Virtual group level. Virtual groups are used for the organization and presentation of data within a group, and to restrict user access.
⬢	Data group level. Data is stored at this level.

Icon	Description
▼	Subgroup level. A subdivision of a data group. Subgroups allow you to further limit user access to the data. For example, you can apply a field filter for a subgroup to restrict the transactions displayed to that subgroup based on a specific field value.

After performing a group management task, such as adding groups, return to this page by clicking **Group Management** in the top left corner.

Add a group

To create a group, you need a template. Kofax provides standard templates for data groups, virtual groups, and subgroups. If you wish to create your templates, contact your Kofax representative.

> ⓘ You cannot delete a group after you have saved it, but you can disable it.

1. Click the parent group to which the new group will belong.
2. Click **Add group**.
3. In the **Organization Properties** area, enter the following details.

Property	Description
Inherit settings from	Use this option to inherit the settings from the parent or a template group. • **Template**: Inherits the properties of a data group, virtual group, or subgroup template. • **Parent**: Inherits the properties of the parent group under which you want to add the group. • **Sibling**: Inherits the properties of a subgroup that belongs to the parent group.
Template	Select the default templates provided for a data group, virtual group, and subgroup.
Name	Enter a name for the group. This name is displayed in the group selection list throughout the application.
Description	Enter a description for the group.
Code	Enter a unique code that identifies the group in the system. You can enter your code if you have special requirements. If you do not enter a code here, the system automatically generates a code.
Category	Select category. Categories enable TIS to create reports on request. For example, if you require TIS to create a report on all your PCI clients, select the category PCI.
Enabled	Click to enable or disable the group. If the group is disabled, users cannot access the group and its subgroups.
IP Filtering	Click to enable or disable IP filtering for the group. IP filters allow you to restrict access to the application from specific IP addresses only.

4. Click **Save**.

Edit a group

Click the group to select it, then edit the properties, preferences, and other settings.

Remember that groups and subgroups inherit their settings from the parent group, so you should consider where to apply the setting. For example, if you want a setting to apply to all subgroups of a group, configure the setting at the group level. If you only want the setting to apply to a specific subgroup, configure the setting at the subgroup level.

Only the options that are relevant for the selected group are displayed. For example, at the group level, only **Fields** and **Preferences** are available; at the data group level, **Fields**, **Preferences**, and **Promote to Production** are available.

Set IP filters

You can restrict the use of iRemit to computers with specific IP addresses. Users can only log in to iRemit on computers whose IP address is specified in the IP filters list. If no IP filters are defined, users can log in from any computer.

IP addresses can only be defined for first-level virtual groups. The setting **IP Filtering** must be activated in the group properties.

1. In **Group Management**, select the group for which you want to set the IP filters.
2. Enable **Ip Filtering**.
3. Save the changes.
4. Click **Ip Filters** on the right side of the page.
5. Click **Add**.
6. Enter the IP address in the top field. You can also enter a range of IP addresses by entering the beginning address in the first field and the ending address in the second field.
7. Make sure that the **Enabled** option is selected.
8. If you are adding single IP addresses rather than a range, repeat these steps for each IP address.
9. Click 💾 **Save**.

Manage site mappings

You must define a site mapping for each data level group 🝫. The import process requires site mappings to determine which group to load the incoming data to. Only users with the role **Site Manager** role can define site mappings.

After you create a site mapping, you cannot delete or disable it. If you need to remove a site mapping, contact your Kofax representative.

Add a site mapping

1. Click the data group to select it, then click **Site Mappings**.
2. Click ⊕ **Add** at the top right of the list.
3. Enter the details in the fields, then click 🖫 **Save**.

Site mapping fields

Field	Description
Site	The ID of the site.
Client ID	The processor organization's client ID.
Description	A description of the mapping.
Work Type	Select the appropriate Work Type for the group. This field is required for billing purposes.
Bank ID	The ID of the bank (optional).
CID	The client's internal client ID (optional).
Tran Expiration Days	Leave the default value of 0 (zero) in this field.
Start Date	The date from which data will be held in the archive.
End Date	The date until which the mapping is valid. We recommend that you enter 12/31/2099 here, and only change this value if the client decides to close their box.
Retention Days	The number of days that transaction data is available to users in the archive.
Active OrgCode	The subgroup for which the site mapping applies.

Edit a site mapping

Click ✏ **Edit** on the right of the mapping entry and change the field values, then click 🖫 **Save**.

You can only edit the **End Date** and the **Active OrgCode** fields.

Click ✕ **Cancel** to discard your changes.

Manage lockbox mappings

You can map a lockbox number to transactions performed in a period in a site/subsite of a group using LockBox mappings. You can map a lockbox number, edit a lockbox number, and activate or deactivate a mapping.

Add a lockbox mapping

1. Open Group Management.

2. Click **LockBox Mapping** on the right pane.
   The **Lockbox Mapping Management for <group_name>** page appears.
3. Click ⊕ **Add** and provide the following details.

Field	Description
Site	Select the organization business unit (site) ID.
SubSite	Enter the subsite ID of the business unit subunit (subsite).
LockBox	Enter the lockbox number for the group of transactions performed in the selected period.
DDA	Enter DDA to which the lockbox number belongs.
Start Date	Select the start date of the transaction period.
End Date	Select the end date of the transaction period.

4. Click 🖫 **Save**.

Edit a lockbox mapping

You can edit the lockbox ID, DDA, and end date of a mapping. You can activate or deactivate a lockbox mapping while editing.

1. Follow steps 1 through 2 of Add a lockbox mapping to view the list of lockbox mappings in the selected group.
2. Select the mapping to edit and click ✎ **Edit**.
3. Change the LockBox, DDA, and End Date settings as needed.
4. To activate or deactivate the mapping, in the Active column of the mapping toggle the button on (activated)/ off (deactivated).

Manage fields

You can customize the fields that are displayed in the different Kofax iRemit modules. For example, you can add fields, change the field labels, and change the order and appearance of the fields.

iRemit provides standard fields for each module, such as **Process Date**, and additional fields, such as amount and date fields, that you can add as needed. You must deliver data for these fields in your import file.

To manage fields for a group, click the group to select it and then click **Fields**.

A list of fields for the **Archive** module is displayed, with their labels and attributes. To display fields for a different module, select the module in the **Module** selection list.

Add a field

1. Click ⊕ **Add** at the top left of the list.
   The **Add new fields** tab appears.

2. Select an item type from the selection list to display all fields of that type.
3. Select the check box to the right of each field you want to add.
4. Click **Add selected fields**.
   The fields are added at the bottom of the list.

Edit a field

1. Click the field in the list.
   The field properties are displayed to the right of the list.
2. Edit the field properties, then click **Save Changes**.

Field properties

Property	Description
Field Label	The name of the field displayed in the interface.
Description / Tool Tip	(Optional) A description of the field. This description is displayed in a tooltip when the mouse cursor hovers over the field.
Default Value	(Optional) Enter a value. This value is automatically entered in the field. For date fields, you can specify a dynamic value, for example: • %today%: Today's date. • %curmonthfirst%: First day of the current month. • %curmonthlast%: Last day of the current month. • %prevmonthfirst%: First day of the previous month. • %prevmonthlast%: Last day of the previous month.
Search Form	Displays the field on the Search page. • **No**: The field is not displayed. • **Optional**: The field is optional, and the user can choose to enter or not enter a value to perform the search. • **Visible**: The field is displayed. • **Required**: The field is displayed, and the user must enter a value.
Result Grid	Displays the field on the Results page. Select **Visible** to display the field on the Results page.
Edit Form	Use this option to display and provide edit permissions for a field. This field only applies to IR Workflow, Post Processing Work, and Client Decisioning Module. • **No**: The field is not displayed. • **Read-only**: The field is displayed, but it cannot be edited. • **Visible**: The field is displayed. • **Required**: The field is displayed, and the user must enter a value.

Property	Description
Field Dependency	Use this option to define whether the field is dependent on other fields in the auto-populate process. • **Independent**: It is not dependent on other fields. • **Parent**: This field should be filled to auto-populate data for the child fields. • **Child**: Data is automatically populated if the parent fields are updated. Users can change the data if required. ⓘ The Parent/Child hierarchy applies to editable, non-editable and non-visible fields.
Result Display Order	Specifies the order of the field on the Results page. For example, if you enter 3, the field is displayed in the third column of the results list. You can also change the field order by clicking on the icon next to a field and dragging and dropping it to another position in the fields list. ⓘ The position of check fields always takes precedence over the position of coupon fields. For example, if you have the check account field in position 12 and the coupon account field in position 2, the check field will override the coupon field, and both will be in position 12.
Search Position Row	Specifies the row in which the field is displayed on the Search page.
Search Position Column	Specifies the column in which the field is displayed on the Search page.

Change field appearance

You can specify how the fields are displayed on the page. In the field properties, click the **Appearance** tab.

Property	Description
Header Style	The appearance of the label that is displayed next to the field on the Search page, or in the column heading on the Results page. Select from bold, italic, and left, center or right aligned.
Item Style	The appearance of the data within the field.
Field Width	The width of the field (number of characters). A value of -1 means that the field width is automatically adjusted to the width of the data. You can type in -1 or click **Set as auto**.
Default Search Operator	The operator displayed by default for the field on the Search page.

Add field filters

You can create filters to limit the transactions displayed to users depending on the field value. For example, you may want subgroups to access only a specific range of lockbox numbers:

• Users in Subgroup 1 should only be able to access data for lockboxes numbered between 1000 and 1999.

- Users in Subgroup 2 should only be able to access data for lockboxes numbered between 2000 and 2999.

For Subgroup 1, you would add a filter to the **Lockbox #** field that specifies values between 1000 and 1999.

For Subgroup 2, you would add a filter to the **Lockbox #** field that specifies values between 2000 and 2999.

> ℹ
>
> - You can only add one filter per field. Filters should be applied to subgroups only. Before adding field filters, make sure you have selected the appropriate subgroup in the group hierarchy tree.
> - A filter should not be added to a data-level group. This prevents data from filtering down to all subgroups.
> - Field filters are not available in the **Daily Summary** module.

Follow these steps:
1. In the field properties, click the **Filters** tab.
2. Select an operator, then enter the value for the filter and click **Save**.

> ℹ
>
> - Use a comma to separate the values for the **Between**, **NotBetween**, **In** or **NotIn** operators. For example, type 100,200 to specify values between 100 and 200.
> - To delete a filter, click 🗑 **Delete** in the filters list.

Define valid field values

You can create a list of valid values for a field so that users can select the values from a selection list instead of entering them manually.

You can add the valid values manually, or you can import them from a CSV file. The CSV file should contain the values and display values to be imported, separated by a comma. The **Value** is the value that is delivered in the import file. The **Display Value** is the value that is displayed to users in the application.

```
1000,Pittsburgh
2000,Boston
3000,New York
```

1. In the field properties, click the **Valid Values** tab.
2. Perform one of the following:
   - Enter a value and a display value, then click **Add Valid Value**. Repeat this step for all values that should be available in the field.
   - Click **Import CSV** and select a CSV file.
3. Click **Save Changes** at the top of the page.

You can do the following in the **Valid Values** tab.

- To delete a valid value, click 🗑 **Delete** in the values list.

- To export values added manually to a CSV file, click **Save Changes** at the top of the page, then click 🖫 **Download** at the top of the values list.

Simple Validation

You can configure simple validation rule for the fields which are available for data correction in Content Decision Module (CDM), Post Processing Workflow (PPW), and Integrated Receivables Workflow (IRWF). Simple validation allows you initially validate the data in the fields before the validation engine is called.

While validating the fields if the data in the field does not match the set length, value, limit or type a corresponding error message appears.

Validation field	Description
Minimum Length	You can set the minimum length of the data for the field.
Maximum Length	You can set the maximum length of the data for the field.
Regular Expression	You can define regular expression for the field. Data in the field should match the regular expression.
Minimum Value	Set the minimum value for the field.
Maximum Value	Set the maximum value for the field.
Data Type	You can set the data type for the field.

ⓘ Minimum or Maximum Value fields are available only for date, time, and numeric types of Organization Field.

Set preferences

Preferences determine the system behavior and the availability of data for a group.

1. In **Group Management**, select the group for which you want to set the preferences.
2. On the right pane, click **Preferences**.
   The preference editor page is displayed.
3. On the left pane, click the preference you want to edit. Available options are:
   - Security Preferences
   - LTA Preferences
   - PPW Preferences
   - CDM Preferences
   - Correspondence Preferences
   - Workflow Preferences
4. Modify the settings as needed. When you edit a preference for a group or subgroup, the ⚙ **Overridden** icon is displayed next to the setting to indicate that this setting differs from the parent group's setting.

5. Click **Save**.

   If you want to apply the same settings as the parent group, click **Return to Parent Settings**, then click **Save**.

Security preferences

Security preferences determine how users are authenticated in the application, and control password expiration and user inactivity.

> ℹ Security preferences are only available for users with the role **Group Security Admin** as well as **Group Admin**.

User Authenticated Settings

You can specify how user credentials are authenticated when users log in to Kofax iRemit.

Multi-Factor Authentication (MFA) is an optional security method to control access by requiring users to successfully pass multiple authentication stages. MFA does not apply to groups that use SSO (single sign-on) authentication.

Kofax iRemit offers two types of MFA authentication:

- **Challenge response questions**: When new users first log in with a temporary password, in addition to changing the password, they are required to select "challenge response" questions and provide answers to those questions. Thereafter, during the login process, they are prompted to answer one of these questions. Which question is presented at each login is determined at random by the system.
- **One-time passwords (OTP)**: New users receive a password via email, which they enter during login. The next time they log on, a new one-time password is sent to them by email when they enter their username and previous password.
- **Allow cookie for MFA**: Allows for a cookie to remember the challenge response answers.
- **Force MFA onto sub-groups**: Forces subgroups to use MFA.

Password settings

You can specify settings for password expiration and user inactivity. You can force users to change their passwords after a certain number of days.

Setting	Description
Password Expiration Days for Admins	The number of days after which the password for an Administrator user expires.
Password Expiration Days for Users	The number of days after which the password for a normal user expires.
Disable user account after inactivity days	If the user has not logged in for the number of days specified here, the user's account is deactivated, and the user can no longer log in.
Disable user account after reset and inactivity days	If an Admin has reset the user's password and the user has not logged in for the number of days specified here, the user's account is deactivated, and the user can no longer log in.

Setting	Description
Session Timeout (Min)	The number of minutes after which the system will timeout. If the user has not been actively working with the system for this number of minutes, the user is automatically logged out and must log in to the application again to continue working. A warning message is displayed to the user three minutes before timeout.
Warning Window for Expiring Passwords	Use this setting to display a warning to users a few days before their password expires. The number of days after which the warning appears is defined at the processor level.

LTA preferences

You can specify the following preferences for the archive.

Setting	Description
Enable Front Only Images	Use this setting to enable or display only the front page of an item in the image viewer. For example, display only the front side of a check, and not the reverse side.
Enable Daily Summary	Use this setting to enable or disable the Daily Summary. The Daily Summary allows Archive users to research activities in the image archive by a lockbox, batch, and transaction. See Daily Summary in the *Kofax iRemit User Guide* for more information.
Enable AutoSearch	Use this setting to enable automatic search. If default values have been configured for fields, the search is automatically performed using these default values when the user clicks **Archive** on the toolbar.
Results per page	Specifies the number of search results to display on a page when the user performs a search. If more than this number of results are available, paging controls appear to enable users to advance to additional pages.

PPW preferences

You can specify the following preferences for the Post Processing Work (PPW) module.

PPW Settings

Use the option **Display Checks in Editor** to display or hide the check details and check images for a user while editing a PPW transaction in the PPW module.

Enable PPW queues

PPW queues represent the type of work that must be processed by the PPW users. You can use up to 15 queues.

Enter the queue name and click queue number to activate.

PPW lists

You can add values for the PPW status and add rollup codes. Unprocessed and Completed are the default statuses.

PPW users select the status from the selection list after they have finished processing a PPW item.

Rollup codes can be used to filter data within a subgroup, similar to field filters. Rollup codes are delivered in the import file.

To add a new status or rollup code, enter the value in the appropriate text box and click **Add**.

To remove a status or rollup code, click 🗑 **Delete**.

CDM preferences

The following preferences are available for the Client Decisioning Module (CDM).

General settings

Setting	Description
Lease Timeout (Min)	Specifies the time in minutes for which a transaction is leased to a user. The default time is 10 minutes. When a user opens a CDM item, the item is automatically assigned to the user for decisioning for a specified period. This is known as leasing the transaction. Other users can view the transaction, but they cannot decision it until the person with the lease finishes decisioning the item, exits the item, or the lease expires.
Holiday Calendar	The holiday calendar linked to the group. Days that are defined as holidays in this calendar are skipped by CDM sweeps.

Site/Subsite settings

Setting	Description
Choose Site/Subsite	The site/subsite combination to which the import settings will be applied.
Max Days/Loads	The maximum number of days for the main sweep. Main sweeps usually run daily, but they can be spread over several days.
Enable Stop File Administration	Use this setting to enable users with the role **StopFile Management** to upload stop files for the CDM. Stop files are used to validate accounts entered by CDM users.
Enable deletion of original Checks	Use this setting to allow users to delete the original check.
Enable deletion of original coupons	Use this setting to allow users to delete the original coupons.
Enable adding or deleting of new coupons	Use this setting to allow users to add or delete new coupons.

Setting	Description
Allow out of balance transactions	Use this setting to allow transactions that do not balance to be accepted. If this setting is deactivated, checks and coupons must always balance before to being accepted. If the check amount is different from the total coupon amount, the difference (balance) is displayed in red in the transaction area and the user must correct the transaction to be able to accept it.
Require Reject Reason	If ON, the user must select a reason when rejecting a transaction. If the user does not select a reason an error message appears. If the RejectReasonCode field is not configured as Visible and Editable in the **Group Management** > **Fields** and the field doesn't have Valid Values configured, an error message appears.
Auto-Decision for Held/Unworked items	The decision applied to items that were put on hold or not worked on when the sweep takes place.
Rollup Codes	Rollup codes can be used to filter data within a subgroup, similar to field filters. Rollup codes are delivered in the import file. To add a rollup code, enter the value in the text box and click **Add**.
Balance Fields	Use balance fields to calculate the balance amount between the total amount of all checks and the total amount of all stubs in a transaction. To add a balance field, select the amount in the drop-down box and click **Add**.

Correspondence preferences

You can specify settings for correspondence and upload templates with which users can generate correspondence in the Archive, CDM, and PPW modules.

Correspondence settings

Setting	Description
Maximum images per page	The maximum number of images to include on a page in the generated correspondence.
Enable Correspondence	This setting allows users to generate correspondence based on predefined templates. This setting applies to the Archive, CDM and PPW. See the *Kofax iRemitUser Guide* for information on generating correspondence. You must add at least one correspondence template.
Enable PDF splitting by sweep time	Use this setting to create a PDF for an organization for each sweep time.
Enable PDF splitting by Site/SubSite	Use this setting to create a separate PDF for each site/subsite at sweep time. Deactivate the setting to include all correspondence in a single PDF file. ⓘ Do not use this setting in combination with **Enable PDF splitting by sweep time**. Choose either one option or the other.

Setting	Description
Create cover page for correspondence	Use this setting to create a cover page in the generated PDF for correspondence. This cover page provides information for the processor organization, such as the number of checks, coupons, and pieces of correspondence.
Correspondence on auto-decision	Use this setting to generate a default letter for the processor organization when items are auto-accepted or auto-rejected at sweep time. You must select a CDM default letter if you activate this setting.
CDM Default Letter	The default letter to use when the setting Correspondence on auto-decision is activated.

Correspondence templates

Correspondence templates must be in PDF format.

1. Click **Choose template file** and select a file.
2. In the selection list, select the module for which the template will be available.
3. Click **Upload Template**.

   The template is added to the list and is now available to users in the selected module, provided you have activated the **Enable Correspondence** setting.

To remove a correspondence template, click 🗑 **Delete**. Templates can only be deleted at the level to which they were added. Subgroups can see a template in the list that was added to a parent group, but they cannot delete the template.

Workflow preferences

The following settings are available for workflow preferences.

Settings	Description
Enable	Use this setting to enable or disable the Workflow module for a group along with any subgroups within the group. The ⚙ symbol indicates it has a different setting from its parent. IR Workflow templates can only be enabled at the data level group.
Rollup Codes	Rollup codes can filter data within a subgroup, similar to field filters. Rollup codes are delivered in the import file. To add a rollup code, enter the value in the text box and click **Add**. To delete a rollup code, click the trash can symbol next to the value to be removed.
Stages	Workflow supports multi-level authorization. You can define the number of levels here. Type the name of the level you want to create in the text field and click **Add**. To delete a stage, click 🗑 next to the stage that you want to delete.

Add a workflow to a group

Before adding a workflow to a group, contact iRemithelp@kofax.com to set up validation for incoming ACH transactions.

ℹ The Workflow module does not appear until the files are loaded.

1. Navigate to **Group Management** > **Preferences** > **IR Workflow**.
2. Click **Enable**.
3. Create the name and number of stages.

Add Workflow Privilege to a user

1. Navigate to **User Management**.
2. In the user list, click the user.
3. On the **Group Privilege** tab, select ✎ **Roles**.
   The **Edit Roles** tab is displayed.
4. In the **Edit Roles** tab, scroll to the end of the list of the roles where the workflow roles are listed.
5. Select the roles you want to assign to the user.
6. Assign the appropriate workflow stage to the user.
7. Click **Save**.

Lookup preferences

In lookup preferences you can upload and download the lookup data. This feature is configured on the data group level.

To upload lookup data, click **Choose File** and select the file that contains lookup data.

❗ By default, the uploaded file will overwrite the existing file.

This feature is designed to upload small lookup files. However, the limit depends on the internal configuration of the lookup process of your organization. It is recommended to use this page to upload a lookup file that contains less than 10000 lookup records. Otherwise, you can use other existing approaches to upload the lookup file, such as the QPS plugin.

To download lookup data, click **Download** and select the location where you want to save the file.

To configure notification for a successful or failed import, see the Send a Homepage notification message.

There are two related event types:

1. Generic Import Complete
2. Generic Import Failure

Manage sweep

Sweep Management is available only for users with the **CDM Sweep Admin** role. Sweep Management enables you to create sweeps and mini-sweeps for the Client Decisioning Module. A sweep pulls transactions from the CDM queue after they have been processed.

Manage broadcasts

Broadcast Management is available only for users with the **Broadcast Admin** role. Broadcast Management enables you to send broadcast messages to users. Broadcast messages are displayed on the Kofax iRemit **Home** page.

Manage files

Allows users to upload files, such as logos and manuals as per the product requirements.

Test Group Management settings

After you have completed your client setup, you should test it thoroughly in the configuration environment to ensure that the application works as expected.

ℹ Prior to testing, in **Group Management**, click **Reset Org Tree**, then log out of iRemit, close your browser and log in again. This refreshes the system with your configuration changes.

1. Upload files via FTP to the configuration environment.
2. In the configuration environment, conduct thorough tests on the groups you have configured.
3. If necessary, make changes to the configuration settings and retest.
   When you are satisfied with the results, you can promote your setup to the production environment.

Promote settings to production

After testing the changes that you have made to your client setup in the configuration environment, you must update the production environment with those changes to make them available to users.

1. Click the group you want to promote to select it.
2. Click **Promote to Production**.
3. To also promote subgroups of the selected group, set **Include all subgroups** to **ON**.
4. Click **Save**.

Client setups are promoted at night when users are not working with the system. Therefore, your changes are available to users the next day.

The progress of the promotion to production is displayed on the **Group Management** page in both the configuration as well as the production environment.

Chapter 3

User Management

Users with the appropriate user privileges can create or modify users and assign roles.

Roles control the user's access to the application and determine the data they can view and the actions they can perform. A user must have at least one role, but you can also assign multiple roles to a user. You can assign the user to multiple groups and assign the same or different roles for each group.

The user data that you can modify depends on the Admin role you have:
- A **Super Admin** can set up or edit any other Admin, or Non-Admin user.
- A **User Admin** can set up or edit any other User Admin, Password Admin or Non-Admin user.
- A **Password Admin** can only reset the password or challenge response for another Password Admin or Non-Admin user.
- A **Group Admin** has no access to users.

Open User Management

In the group selection list at the top right of the **Home** page, select the group or its parent to which the user belongs, and then, on the toolbar, select **Administration** > **User Management**.

A list of existing users for the selected group is displayed. To display only users assigned to the selected group, click **All Subgroups** at the top of the list to set it to **NO**.

To search for a specific user, in the **Search** field, enter the user's email/username, last name, first name, or part of the name. All users corresponding to the search criteria are displayed. To view all users again, clear the **Search** box.

Select an option from the user status drop-down list to display only **Enabled** users, only **Disabled** users, or **Enabled & Disabled** users.

Use the page navigation icons at the bottom of the list to view more users.

Click a user to view the user's properties on the right of the page.

Add a user

1. Click ⊕ **Add User** at the top right of the user list.
2. On the **Info** tab, enter details for the user. For more information, see User details.
3. Click **Next step**.

4. On the **Sign in** tab, enter and verify the temporary password for the user.

   The user must change this password the first time they log on.

   The password must adhere to the password rules. Password rules are defined at the processor level.

5. Click **Next step**.

6. On the **Group Privileges** tab, click the group for which you want to assign the user's roles, and then click each role you want to assign to the user. See Available roles for more information.

   Assigned roles are highlighted. You must assign at least one role for each user.

7. Click **Save**.

User details

Field	Description
Email/Username	Login name of the user. This name must be unique within the application. You may wish to use an email address instead of a name to ensure that the login name is unique.
Notification Address	A unique email address to which notifications for this user will be sent.
First Name	User's first name.
Last Name	User's last name.
Enabled	Use this option to enable or disable a user. Only active users for whom this option is set 'ON' can log in to the application.

Available roles

You can assign the following roles.

Role	Description
Select/Deselect All	Assign or unassign roles.
Archive User	The user can access the Archive module.
Archive-Restricted	This Archive user can access a subset of data based on a defined retention period.
Audit	The user can access all audit reports.
Broadcast Admin	The user can send broadcast messages.
CDM ReadONLY User	The user can view items that require decisioning in the Client Decisioning Module but cannot edit or decision transactions.
CDM Secondary	The user can provide secondary approval of CDM transactions. The CDM Secondary Queue contains items that have already been decisioned by a CDM user but require a second approval.

Role	Description
CDM Supervisor	The user can access the CDM Activity Report and the CDM Secondary Queue.
CDM User	The user can access the Client Decisioning Module and edit and decision CDM items.
Correspondence Generation	The user can generate correspondence in the LTA, PPW, and CDM modules.
Dashboard Advanced User	The user can access the Dashboard module and define which charts and reports to display on the iRemit Home page and the Dashboard page.
Dashboard User	The user can view charts and reports on the iRemit Home page, but cannot define which charts and reports are displayed, and cannot access the Dashboard page.
Data Management	The user can delete transactions from the Archive.
Download CSV	The user can download transaction data that is displayed in the application to a CSV file.
Exception1 User - Exception15 User	Each of these roles allows a PPW user to access a specific PPW queue.
Exceptions Supervisor	This role must be assigned in combination with the Exception1–Exception15 roles. The user can edit PPW items for the queues to which they are assigned.
Export PDF	The user can download any archived data to a PDF file.
Extra Fields	The user can access extra fields in the Archive. See the iRemit User Guide for information on extra fields.
Files Admin	Enables the Admin to import manuals and logos under File Management.
Group Admin	The user can create, enable, or disable groups, and establish and monitor group options within the application, including group reports, maintenance and broadcast messages.
Group Security Admin	The user can view and edit Security Preferences, which control how users access the system.
Holiday Calendar Manager	The user can set up a calendar of holiday events for the CDM module.
IDX Admin	The user can define and schedule jobs to extract data from the Archive at specified intervals.
IDX Download	The user can download extracted data.
MegaCSV	The user can download all available transaction data (that is, all data as it was sent in the source file) to a CSV file.
NONXGAUser	The user can see all data even when Explicit Group Assignment (XGA) has been turned on for an organization. XGA can be turned on for either a group or a user. If it is turned on for a specific group, any user who has that group assignment can only see that group but not the subgroups.
Notifications Admin	The user can create "subscriptions" to send messages to users when specific system events occur.

Role	Description
Password Admin	The user can reset passwords and challenge response questions.
Report User	The user can access all reports in the system.
Stop File Admin	The user can upload a CSV stop file to validate accounts entered by CDM users.
Site Manager	The user can define site mappings to enable the import of files.
Super Admin	The user can create Admin and non-Admin users, assign roles, create and edit groups, change passwords, and delete challenge response questions.
Sweep Admin	The user can schedule daily sweeps and mini sweeps for CDM.
User Admin	The user can create User Admin, Password Admin and non-Admin users, assign roles, change passwords, and delete challenge response questions.
View Correspondence	The user can view correspondence and attachments in the Archive.
View Rear Image	The user can view the rear side of transaction images even when the setting Enable Front Only Images is activated in the Archive settings.
XGAUser	The user has access to a subset of data based on Explicit Group Assignment (XGA). Even if XGA is not turned on for a group, a user with the XGAUser role would see only that group and none of its children.

Edit a user

ⓘ You cannot edit your own user profile.

1. In the user's list, click the user.
2. Make the required changes to the user details. For more information, see User details.
3. To enable or disable a user, on the **Info** tab, click the **Enabled** setting to change the setting to on or off, and click **Save**.
4. To change a user password, on the **Sign in** tab, enter and verify the password, and click **Save**.
   Make sure the password adheres to the password rules set in the application.
5. To view or edit the assigned privileges for a group, on the **Group Privileges** tab, select the group and click ⊙ **View Selected Group Assigned Privileges** Roles or ✎ **Edit Selected Group Assigned Privileges** Roles.
6. To change the groups to which the user belongs:
   • To assign a new group, click ⊕ **Add Group Privilege** at the top right. In the group hierarchy, select the new group, select roles, and click **Save**.
   • To delete the selected group from the user's privilege, in the **Assigned Groups** list, select the group and click 🗑 **Delete Group**.

Enable/disable SSO for a user

You can enable Single Sign On (SSO) for a user. SSO users can log in to iRemit without a password. They can log in to iRemit using a link provided by their organization after logging in to their organization's application.

1. In the user's list, click the user.
2. Click **Sign in** on the right pane.
   The **Authentication** tab appears.
3. Toggle **SSO User** to turn it On or Off.

Reset challenge response questions and answers

1. In the user list, click the user.
2. On the **Sign In** tab, click **Reset CR**.
3. When prompted, confirm that you want to clear the challenge response.

Create a user privileges report

You can view and download a report of all users and the roles assigned to each user.

1. On the toolbar select **Administration** > **User Privileges**.
2. Select **Group** and **User Status**, then click **Search**.

   > ⓘ If you selected a group in the group selection list on the **Home** page, only that group and its subgroups are available for selection.

3. Click **Download** to download the report details for the selected group only to a CSV file.
4. Click **Download including sub groups** to download details for the selected group and its subgroups.

Chapter 4

Notifications and Broadcast Management

Administrators with the appropriate user privileges can send messages to users in the following ways:

- Send a broadcast message that is displayed to all users of a group (and optionally its subgroups) in the **Broadcast Messages** section of the iRemit Home page.
- Send a Homepage notification message that is displayed to specific users in the **Homepage Notifications** section of the iRemit Home page.
- Create subscriptions to send messages to users when specific system events occur. Subscription notifications can be sent by email or displayed on the iRemit Home page. When you create a subscription, you select the type of event, the start date, and the expiration date. After you have created the subscription, you create a delivery method, add users, and set up the frequency.

Send a broadcast message to groups

Users with the Broadcast Management role can send broadcast messages to all users of a group (and optionally its subgroups). The message is displayed on the iRemit **Home** page for the duration you specify when you create the message.

1. On the groups list, select the group for the message.
2. On the toolbar, select **Administration** > **Broadcast Management**.
3. Click ⊕ **Create** at the top right of the list.
4. Enter the following details.

Setting	Description
Message text	Enter the text of the message.
Start Date/Time	Enter the date and time from which the message is displayed on the **Home** page.
End Date/Time	Enter the date and time at which the message is removed from the **Home** page.
Active	Activate this setting to enable the display of the message.
Include Child Groups	Activate this setting to display the message to the selected group and its subgroups. Deactivate the setting to display the message only to the selected group.

5. Click **Save**.

Send a broadcast message to individuals and distribution lists

To send a broadcast message to an individual user or a distribution list, you must first set up a notification subscription. Then, you can send the broadcast message. Users can view up to five messages at a time; messages remain for 15 days before being removed.

Set up a notification subscription

1. On the toolbar, select **Administration** > **Notifications** > **Notification Management**.
2. Click ⊕ **Add Subscription**.
3. Select **Broadcast Message** as the **Event Type**.
4. Enter a start date and an end date to specify the period within which you can send messages.
5. Click ⊕ **Add Delivery**.
6. In the **Delivery Information** field, select **ApplicationMessage**.
7. In the **Send To** field, select the email addresses of the users to receive broadcast messages.
8. In the header, add the variable **$Category$**.
9. In the body, add the variable **$Message$**.
10. Click **Create**.

Send the message

When you are ready, send the message as follows:

1. On the toolbar, select **Administration** > **Notifications** > **Create Broadcast**.
2. Add your message.
3. Click **Create**.

Send a Homepage notification message

Users with the **Notifications Admin** role can send homepage notification messages to specific users.

1. In the group selection list, select the group for the message.
2. On the toolbar, select **Administration** > **Notifications** > **Notifications Management**.
3. Click ⊕ **Add Subscription**.
4. Select an **Event Type**:
   - Import Complete
   - LTA Import Complete
   - CDM Import Complete
   - IDX Extraction Complete
   - Broadcast Message
   - Report Import Complete

- IRWF Item Changed
- IRWF Import Complete
- Extraction Complete
- Extraction Failure
- Generic Import Complete
- Generic Import Failure

5. Enter a start date and an expiration date, then click **Create**.

6. Click ⊕ **Add Delivery**.

7. To specify the frequency of notification, on the **Frequency** list, select one of the options:
    - **Immediate**: The notification will be sent immediately.
    - **Daily**: Specify the days of the week on which the notification will be sent.
    - **Monthly**: Specify the month and days of the month on which the notification will be sent.

8. Enter the **Delivery Information** details.

Field	Description
Delivery	Select **Email** to send notifications via email. Select **ApplicationMessage** to display notifications on the iRemit Home page.
Send To	Select or enter the email addresses of users who should receive the notification. If you leave this field blank, notifications are sent to all users of the selected group for whom a notification email address is entered in their user profile.
Header	The subject line of the email, or the title of the notification on the iRemit Home page. Type $ to display a list of data that you can insert into the header. For a broadcast message, you must select **Category** for the header.
Body	The text of the email. Type $ to display a list of data that you can insert into the body. For a broadcast message, you must select **Message** for the body. You can insert variables in the text which are replaced in the notification with the relevant values. For example, $TransactionCount$ would be replaced with the number of transactions in the import file. When you type a character in the **Header** or **Body** text box, all variables containing that character are displayed. Click a variable to insert it into the text.
Footer	For email notifications only. This text is displayed at the end of the email.

9. Click **Create**.

Open the subscriptions page

To create subscriptions, you must have the user **Notifications Management** role.

On the toolbar, select **Administration** > **Notifications** > **Notifications Management**.

The **Subscriptions** table displays all subscriptions defined for the selected group. The **Delivery** table displays all delivery methods for the selected subscription, showing when the notification was last sent (Last Serviced) and when the notification will be sent again (Next Delivery).

Add a subscription

To add a subscription, follow steps 1 through 5 in the Send a Homepage notification message procedure.

Add filters to a subscription

After you have created a subscription, you can add filters if needed. Notifications are only sent out if the filter criteria are met, for example, if the transaction count exceeds a specified number.

1. Click ▼ **Filter** next to the subscription.
   The **Edit Filters** page appears. The filter properties available here depend on the subscription's event type.
2. In the **Operator** column, select the operator for the property you want to set.
3. In the **Value** field for the property, enter a value.
4. Click **Save**.

Add delivery to a subscription

After you have created a subscription, you must set up the delivery method and frequency. Follow steps 6 through 9 in the Send a Homepage notification message procedure.

Edit a subscription

1. Click ✏ **Edit** next to the subscription.
   The **Edit Subscription** dialog box appears.
2. Modify **Start Date**, **Expiration Date**, or both.
3. Click **Update**.

Delete a subscription

1. Click 🗑 **Delete** next to the subscription.
2. When prompted, click **Delete** to confirm the deletion.

Display expired subscriptions

To display expired and unexpired subscriptions, select the **Show Expired Subscriptions** check box at the top right of the **Subscriptions** list.

Holiday Calendar Management

Users with the **Holiday Calendar Manager** role can define holiday calendars for the Client Decisioning Module. Days that are defined as holidays in a holiday calendar are skipped by CDM sweeps.

For clients that use loads, the sweep is skipped on the holiday and the items that should have expired will sweep the next business day.

For clients that use # of days, the files are loaded, but the incremental days will skip the holiday.

> ℹ A holiday calendar can only be added at the processor level. It cannot be added at a client level.

To define holiday calendars, on the toolbar, select **Administration** > **Holiday Calendar**.

Add a calendar

1. Click ⊕ **Add New Calendar**.
2. Enter a **Name** and **Description**, then click **Update**.
3. Select the date that will be a holiday. and enter the **SiteID** and **SubsiteID** for which the holiday applies.
   Depending on which sites use this holiday, complete the **SiteID** and **SubsiteID** fields as follows:
   - If it applies to all sites and subsites, leave both the fields empty.
   - If it applies to a site and all its subsites, complete the **SiteID** field and leave **SubsiteID** empty.
   - If it applies to a site and a specific subsite, complete both the **SiteID** and **SubsiteID** fields.
4. Click **Add**.
5. Repeat these steps for all holidays applicable for each site/subsite.

To delete a date, click 🗑 **Delete** next to the date.

Edit a calendar

1. In the calendar list, click ✏ **Edit** next to the calendar.
2. If you change the calendar name or description, click **Update** to save these changes.
3. Add or delete dates. These changes are saved automatically.

Copy a calendar

1. In the calendar list, click ⬚ **Clone** next to the calendar.
2. Enter a **Name** and a **Description**, then click **Update**.
   You can now edit the copied calendar.

Delete a calendar

1. In the calendar list, click 🗑 **Delete** next to the calendar.
2. When prompted, click **OK** to confirm the deletion.

Sweep Management

Sweeps can cover single or multiple days.

Single-day clients

Sweeps are used in the Client Decisioning Module. A sweep pulls transactions from the CDM queue after they have been processed. Exceptions (transaction items that were rejected during normal lockbox processing) must be decisioned (that is, edited) the same day they display. The sweep time indicates the deadline time by which all exception decisions must be completed. If a decision is not submitted online for an exception item before the sweep time, the item is automatically rejected or accepted, depending on the client's configuration.

Sweeps usually take place once a day. Users with the **Sweep Management** role can create main sweeps and mini sweeps, which pull transactions at frequent intervals during the day.

Multi-day CDM clients
Multi-day CDM clients have a predefined number of days to decision transactions. At sweep time for a multi-day client, only the Accepted and Rejected transactions, or any transactions not decisioned on their last day, will be swept. All remaining transactions will be available on the website for processing the next day. Any transaction on its last day will be visible in red.

Main sweep

At the defined sweep time, such as 5 PM each day, all CDM items are exported to a file and removed from the CDM queue. The exported file is made available for retrieval on the Kofax iRemit FTP site.

Items that have been decisioned by CDM users are assigned the decision status **Accepted** or **Rejected** (depending on the user's decision). For Single Day clients, Items that have not been decisioned or were put on hold by CDM users are automatically assigned the decision status **Auto-Accept** or **Auto-Reject**, depending on the **Auto-Decision** for **Held/Unworked items** setting in the CDM preferences. For multi-day clients, **Held/Unworked** items not on their last day will remain on the website to be worked on either after the sweep the same day or before the sweep the next day.

Mini sweeps

At mini sweep time, such as 11 a.m., 1 p.m., and 3 p.m., any transactions that have been decisioned are exported to a file and removed from the CDM queue. Transactions that have not been decisioned remain in the queue. Mini sweeps only pull batches that have been fully decisioned. Partially decisioned batches remain in the queue until the final sweep of the day.

ⓘ The last mini sweep must be at least 30 minutes prior to the main sweep time.

Add a sweep

1. On the toolbar, select either of the following:
   - For users who have the Sweep Management role but not Group Management:
     Administration > **Sweep Management**.
   - For users who have the Group Management role (which includes Sweep Management):
     Administration > **Group Management** > **Sweep Management**.
2. Click ⊕ **Create** at the top right of the list.
   The **Add Sweep** page appears.
3. Provide the following details.

Field	Description
Site/Sub Site ID	Select the ID of the site/subsite.
Bank ID	Enter bank ID. This field is optional.
CID	Enter the processor organization's internal client ID.
First Run Date	Select the ID of the site/subsite.
Sweep Time (local)	Select the date at which the sweep time will run.
AutoSchedule	Enable this to run the next sweep automatically at the specified interval when the current one is completed.
Interval	Select a frequency to determine how often the interval will run.

4. Click **Save**.

Add a mini sweep

1. In the sweeps list, click ✏ **Edit** to the right of the main sweep.
2. Under **Mini Sweep Times**, Click 🕐.
3. Select a time for the mini sweep event.
4. Click **Add MiniSweep**.

Delete a mini sweep

1. In the sweeps list, click ✏ **Edit** to the right of the main sweep.
2. Click 🗑 **Delete Mini Sweep** next to the mini sweep.

Chapter 7

Data Management

Users with the Data Management role can delete a transaction or items in a transaction from the iRemit archive. They can also move a transaction to another site, subsite, or lockbox.

Delete transaction

1. On the toolbar, select **Administration** > **Data Management** > **Delete Transaction**.
    The **Delete Items** page appears.
2. Provide the following details.

Field	Description
SiteID	Select the organization's business unit (site) ID.
SubSiteID	Enter the subsite ID of the business unit's subunit (subsite).
Process Date	Select the date on which the transaction was processed.
BatchNumber	Enter the batch number of the batch to which the transaction belongs.
Tran Number	Enter the transaction number.
Trans Amount	Enter the transaction amount.

3. Click **Find Items**.
    The list of items in the transaction is displayed.
    If the required transaction is not found, click **Reset** to clear the fields and enter new search criteria.
4. Click **Delete Transaction**.
5. When prompted to confirm, click **Yes**. The entire transaction and the items in it are deleted.

Delete an item in the transaction

1. To search for an item to delete, follow steps 1 through 3 in the Delete transaction procedure.
2. You can do the following after fetching the list of items in the transaction:
    *   **Delete a single item**:
        a. Select the item.
        b. Click **Delete Items(s)**.

    c. When prompted to confirm, click **Yes**.

> ⓘ
>
> - When you select an item type **Check**, and if there are multiple checks within the selected check, a confirmation prompt is displayed to let you know that you are about to delete all checks of the transaction.
> - Click **Yes** to delete the item.

- **Delete multiple items**:
  - **a.** Select items to delete.
  - **b.** Click **Delete Items(s)**.
  - **c.** When prompted to confirm, click **Yes**.
- **Delete all items**:
  - **a.** Select all items.

    You can use the check box in the **Transaction Details** table header to select all items at once. Alternatively, select each item individually.
  - **b.** Click **Delete Items(s)**.
  - **c.** When prompted to confirm, click **Yes**.

    Another confirmation prompt is displayed to let you know that the whole transaction is deleted if all the items in the transaction are deleted.
  - **d.** Click **Yes** to confirm.

Change site ID or lockbox

You can move a transaction to another site, subsite, or lockbox.

1. On the toolbar, select **Administration** > **Data Management** > **Change Lockbox**.
   The **Change Site Id/Lockbox** page appears.
2. Provide the following details.

Field	Description
Module	Select the module to which the transaction belongs, such as LTA or CDM.
Ref.ID	Enter the unique reference ID of the transaction. ⓘ If reference ID is provided, all other fields are ignored for search, and the search operation is performed based on reference ID only.
SiteID	Select the organization's business unit (site) ID.

Field	Description
SubSiteID	Enter the subsite ID of the business unit's subunit (subsite).
Process Date	Select the date when the transaction was processed.
BatchNumber	Enter the batch number to which the transaction belongs.
Tran Number	Enter the transaction number.

3. Click **Find**.
   The **Transaction Details** page appears.

   ⓘ An error message is displayed if more than one transaction is found.

4. Click ✏.
   The **SiteID**, **SubSiteID**, and **Lockbox #** fields become editable.
5. Select the **SiteID** and **SubSiteID** to which you want the transaction to be moved.
   In the **Lockbox #** box, you can choose to change the lockbox number or retain the same.
6. Click 💾 to save the changes.

IDX Administration

The iRemit Image Data Exchange module (IDX) extracts data from the archive. iRemit provides an offline viewer with which you can view the extracted data.

Users with the **IDX Admin** role can define and schedule jobs to extract data at specified intervals.

Open IDX Administration

On the toolbar, select **Administration** > **IDX Administration**.

The **Kofax Image Data Exchange** page appears. All extract jobs that have been defined for the currently selected group.

By default, the job list displays all jobs. To view only active jobs, click **Active Jobs** on the left of the page. To view only inactive jobs, click **Inactive Jobs**.

Create a job

1. Click **Create new Job** on the left of the page.
   The **Create Job** page appears.
2. Enter the following details.

   > ⓘ
   > - Fields marked with an asterisk * are mandatory (except **Download on Demand**, which is optional).
   > - You have the option to set filters to restrict which data is extracted.

   a. Enter the following in the **General** section.

Setting	Description
Job Name by User	Enter a name for the job.
Description	Enter the description of the job.
Template Id	Select a template that defines which fields will be exported. If no templates are available, select **Standard Extract**. Kofax can create custom code for your extract and deliver this code as a plugin. To use a plugin instead of a template, select **No template (retrieve it from plugin)**.

Setting	Description
Timeout SQL (seconds)	Enter the number of seconds allowed before SQL operation timeout.
Output Filename	Enter a name for the output file. The output file is saved to the FTP site. If you activate the option **Download on Demand**, it is only available to users with the **Download IDX** privilege. To automatically include the extract date in the file name, include the following syntax in the file name: {P:Mmddyy}. If you download several files a day, you can include the date and time using the following syntax: {P:MMddyyhhmm}.
Download on Demand	Select this option to make the extract function available to users with the **Download IDX** function.
Allow For Empty Files	Select this option to generate an empty file when there is no data.
Plugin Type Name	Enter the plugin type.

   b. Enter the following in the **Schedule** section.

Set the frequency at which the job will run. After you select the settings, click **View Run Times** to view the exact dates and times at which the job will run.

Frequency	Description
Daily	Select the days of the week on which the job will run and set the time.
Monthly	Enter the month and day on which the job will run and set the time.

   c. Do the following in the **Custom Filters** section.

You can create filters to extract only specific data, such as data for a specific process date or a specific lockbox.

     1. Click the arrow to view the fields available for filtering.

     2. For each field you want to use for filtering, select an operator and enter values in the field.

     3. Use commas to separate multiple values. In the **Process Date** field, you can use the variables displayed under **Help**.

3. Click **Save Job Configuration**.

The new job is displayed in the **Active Jobs** list.

Edit a job

1. In the jobs list, click **Edit Job** next to the job.

2. Make changes, then click **Save Job Configuration**.

Activate or deactivate a job

1. In the jobs list, click **Edit Job** next to the job.

2. In the job details, click **Active** to activate the job, or **Inactive** to deactivate it.

Copy a job

1. In the jobs list, click **Clone Job** next to the job.
   Copied jobs are initially inactive.
2. In the **Inactive Jobs** list, click **Edit Job** next to the copied job.
3. Make any necessary changes and click **Active** to activate the job.
4. Click **Save Job Configuration**.

Delete a job

1. In the jobs list, click **Edit Job** next to the job.
2. In the job details, click **Delete**.

View job audit

After a job has run, you can view details of the extract in the job audit.

In the jobs list, click **View Audit** next to the job.

Click **Run Stamp** for the job to view further details. If errors occur during extraction, they are listed in the **Monitor** section.

Auditing

Users with the **Audit** role can view detailed audit reports that provide information about file imports and user activity in the application.

The following types of reports are available:
- Admin Report
- LTA Audit Report
- CDM Audit Report
- PPW Audit Report
- Load Report
- Download IDX Report
- Download IDX Purge Report
- Reports Audit Report

Report columns with a filter icon enable you to filter the report to display only records that correspond to the criteria you enter. Filters are not applied to downloads, that is, all report data is downloaded even if you have set a filter.

View/download an audit report

1. On the toolbar, select **Administration** > **Auditing** and then select the required report.
   The report search page appears.
2. Enter the search criteria and click **Search**.

   ⓘ The search criteria depends upon the type of report selected. For types of report available and their respective search criteria, see Auditing.

3. Click **Download** to download the report as CSV.

Admin Report

The **Admin Report** allows you to view the activities of users in the application.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for an admin report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.
Activity Type	Activity details displayed in the report: **Administrative**: Shows details of the activities performed by users in the application. **Authentication**: Shows details of when users logged in and logged out from the application.

LTA Audit Report

The **LTA Audit Report** allows you to view the activities of users in the Archive module.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for LTA audit report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.
Activity Type	Activity details displayed in the report: **Search**: Shows details of the searches performed by users in the application. **Image**: Shows details of the transactions for which users viewed the images.

CDM Audit Report

The **CDM Audit Report** allows you to view the activities of users in the Client Decisioning Module, including the images they have viewed.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for CDM audit report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.

Field	Description
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.
Ref ID	Reference ID of a transaction.
Log Type	The type of log information displayed in the report: • **All**: Information related to both transaction status change and • **Status change**: Information related to transaction status change. • **Data modification**: Information about the transactions done, such as account number and transaction ID.

PPW Audit Report

The **PPW Audit Report** allows you to view the activities of users in the Post Processing Workflow module.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for PPW audit report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.
Ref ID	Reference ID of a transaction.

Load Report

The **Load Report** allows you to view at group level details of files that have been loaded, including load dates, process dates, item counts, and page counts. An error code indicates that a file may have had an import issue.

Two report types are available: **Summary** and **Detail**.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for Load report:

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.

Field	Description
From date	The from and to date for the period for which you want to generate the report.
Report Type	You can generate a **Summary** report or a **Detail** report.
Site ID	Organization business unit (site) ID.
Source Type	Source type for which the load report is generated, such as CDM, LTA, or All.

IDX Downloads Report

The **IDX Download Report** shows details of the extract files that were downloaded by users in the **IDX Download** module.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for the IDX Download report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.
IP Address	The IP address of the user whose IDX report is to be generated.

IDX Downloads Purge Report

The **IDX Download Purge** report shows details of when extract files were removed from the website.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for IDX Download Purge report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.

Reports Report

The **Reports** report allows you to view the activities of users in the Reports module, such as downloading a report. The report can be generated for all users or individual users.

To know how to view or download a report, see View/download an audit report.

The following search criteria are available for Reports report.

Field	Description
Report	Displays the report type selected.
Groups	The business group/unit.
From date	The from and to date for the period for which you want to generate the report.
User Name	The user whose report is to be generated. You can generate a report for single user or all the users.