

# Kofax iRemit

## Administration Guide

Version: 7.5.0

Date: 2020-02-14

**KOFAX**

© 2020 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

# Table of Contents

<b>About Kofax iRemit.....</b>	<b>6</b>
Getting help with Kofax products.....	6
<b>Chapter 1: Group Management.....</b>	<b>8</b>
Open Group Management.....	8
Add a group.....	9
Edit a group.....	9
Manage site mappings.....	10
Add a site mapping.....	10
Site mapping fields.....	10
Edit a site mapping.....	11
Manage fields.....	11
Add a field.....	11
Edit a field.....	11
Field properties.....	11
Change field appearance.....	13
Add field filters.....	13
Define valid field values.....	14
Set preferences.....	14
Security preferences.....	14
LTA preferences.....	16
PPW preferences.....	16
CDM preferences.....	17
Correspondence preferences.....	18
Workflow preferences.....	19
Manage sweep.....	20
Manage broadcasts.....	20
Set IP filters.....	20
Test Group Management settings.....	21
Promote settings to production.....	21
<b>Chapter 2: User Management.....</b>	<b>22</b>
Open User Management.....	22
Add a user.....	22
User details.....	23
Available roles.....	23

Edit a user.....	25
Change a user password.....	26
Enable or disable a user.....	26
Reset challenge response questions and answers.....	26
Create a user privileges report.....	26
<b>Chapter 3: Notifications and Broadcast Management.....</b>	<b>27</b>
Send a broadcast message to groups.....	27
Send a broadcast message to individuals and distribution lists.....	28
Send the message.....	28
Send a homepage notification message.....	28
Open the Subscriptions screen.....	29
Add a subscription.....	29
Add filters to a subscription.....	29
Add a delivery to a subscription.....	30
Edit a subscription.....	31
Delete a subscription.....	31
Display expired subscriptions.....	31
<b>Chapter 4: Holiday Calendar.....</b>	<b>32</b>
Add a calendar.....	32
Edit a calendar.....	32
Copy a calendar.....	33
Delete a calendar.....	33
<b>Chapter 5: Sweep Management.....</b>	<b>34</b>
Main sweep.....	34
Mini-sweeps.....	34
Add a sweep.....	35
Sweep details.....	35
Add a mini-sweep.....	35
Delete a mini-sweep.....	35
<b>Chapter 6: Stop File Management.....</b>	<b>36</b>
<b>Chapter 7: Data Management.....</b>	<b>37</b>
<b>Chapter 8: IDX Administration.....</b>	<b>38</b>
Open IDX Administration.....	38
Create a job.....	38
General.....	38
Schedule.....	39
Custom filters.....	39
Edit a job.....	39

Activate or deactivate a job.....	40
Copy a job.....	40
Delete a job.....	40
View the job audit.....	40
<b>Chapter 9: Auditing.....</b>	<b>41</b>
Admin Report.....	41
Administrative.....	41
Authentication.....	41
LTA Audit Report.....	41
Search.....	41
Image.....	42
CDM Audit Report.....	42
PPW Audit Report.....	42
Load Report.....	42
Download IDX Report.....	42
Download IDX Purge Report.....	42

# 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 decision 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 these features:

- Dashboard  
This module provides an at-a-glance view of 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.

## 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, go to the [Kofax website](#) and select **Support** on the home page.

**Note** 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.
- Access to the Kofax Customer Portal (for eligible customers).  
Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Kofax Partner Portal (for eligible partners).  
Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.  
Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

## Chapter 1

# 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 can complete their own 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 screen. The group currently being worked on is highlighted. Click on a group to select it. The group's properties are displayed in the center of the screen.


**Note** 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 buttons on the right of the screen to configure the group. Which buttons are available here depends on the selected group and your assigned user roles.

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

Icon	Description
	Top level.
	Group level. This level represents the processor organization.
	Virtual group level. Virtual groups are used for 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 screen 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 own templates, contact your Kofax representative.

**Note** You cannot delete a group after you have saved it, but you can disable it.

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

Property	Description
Name	A name for the group. This name is displayed in the group selection list throughout the application.
Description	A description for the group.
Code	A unique code that identifies the group in the system. You can enter your own code if you have special requirements. If you do not enter a code here, the system automatically generates a code.
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.

## Edit a group


Click on 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 subgroup level.



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

## 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** 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 on 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 for 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 on **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 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 on 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.
2. In the **Add new fields** window, 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 that is 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.

Property	Description
Default Value	<p>(Optional) Enter a value. This value is automatically entered in the field. For date fields, you can specify a dynamic value, for example:</p> <ul style="list-style-type: none"> <li>• <b>%today%</b>: Today's date.</li> <li>• <b>%curmonthfirst%</b>: First day of the current month.</li> <li>• <b>%curmonthlast%</b>: Last day of the current month.</li> <li>• <b>%prevmonthfirst%</b>: First day of the previous month.</li> <li>• <b>%prevmonthlast%</b>: Last day of the previous month.</li> </ul>
Search Form	<p>Select an option for the display of the field on the <b>Search</b> page.</p> <ul style="list-style-type: none"> <li>• <b>No</b>: The field is not displayed.</li> <li>• <b>Visible</b>: The field is displayed.</li> <li>• <b>Required</b>: The field is displayed, and the user must enter a value.</li> </ul>
Result Grid	<p>Select <b>Visible</b> to display the field on the Results page.</p>
Edit Form	<p>Select an option for the display of the Edit field. This field applies only to IR Workflow.</p> <ul style="list-style-type: none"> <li>• <b>No</b>: The field is not displayed.</li> <li>• <b>Read-only</b>: The field is displayed, but it cannot be edited.</li> <li>• <b>Visible</b>: The field is displayed.</li> <li>• <b>Required</b>: The field is displayed, and the user must enter a value.</li> </ul>
Result Display Order	<p>Enter a number to specify where the field is displayed on the <b>Results</b> page. For example, if you enter 3, the field is displayed in the third column of the results list.</p> <p>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.</p> <div data-bbox="870 1388 1451 1577" style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b> 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.</p> </div>
Search Position Row	<p>Enter a number to specify in which row of the Search page the field is displayed.</p>
Search Position Column	<p>Enter a number to specify in which column of the Search page the field is displayed.</p>

## Change field appearance

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

Property	Description
Header Style	The appearance of 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 the Set as auto button.
Default Search Operator	The operator that is 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 lock box numbers:

- Users in Subgroup 1 should only be able to access data for lock boxes numbered between 1000 and 1999.
- Users in Subgroup 2 should only be able to access data for lock boxes 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.

Note the following:

- 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.

Follow these steps:

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

Note the following:

- Use a comma to separate the values for the operators **Between** and **NotBetween**, or **In** and **NotIn**, for example, 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 on 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 the **Save Changes** button 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 you have added manually to a CSV file, first click **Save Changes** at the top of the page, then click **Download** (📄) at the top of the values list.

## Set preferences

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

Click on the group to select it and then click the Preferences button. On the left of the page, click the button for the type of preferences you want to set:

- Security Preferences
- LTA Preferences
- PPW Preferences
- CDM Preferences
- Correspondence Preferences
- Workflow Preferences

When you edit a preference setting 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.

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.

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

## User Authenticate Settings

In this section 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 different kinds 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 user name and previous password.

## Password settings

In this section 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.
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 prior to timeout.
Warning Window for Expiring Passwords	Switch this setting on 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	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	Click to enable or disable the Daily Summary. The Daily Summary allows Archive users to research activities in the image archive by lockbox, batch, and transaction. See Daily Summary in the <i>Kofax iRemit User Guide</i> for more information.
Enable AutoSearch	Click 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	The number of search results to display on a page in the Results tab. 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.

### 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

In this section, you can add values for the PPW status and add rollup codes. Unprocessed and Completed are 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

You can specify the following preferences for the Client Decisioning Module (CDM).

### General settings

Setting	Description
Lease Timeout (Min)	Set 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 of time. This is known as leasing the transaction. Other users can view the transaction, but they cannot decision it until the person with the lease either finishes decisioning the item, exits the item, or the lease expires.
Holiday Calendar	Select a holiday calendar to apply. 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	Specify 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	Activate this setting to enable users with the role <b>StopFile Management</b> to upload stop files for the CDM. Stop files are used to validate accounts entered by CDM users.
Enable deleting Checks	Activate this setting to allow users to delete checks.
Enable adding or deleting of new stubs	Activate this setting to allow users to add or delete new coupons.
Enable deletion of original Checks	Active this setting to allow users to delete the original check.
Enable deletion of original items	Active this setting to allow users to delete the original coupons.
Allow out of balance transactions	Activate this setting to allow transactions that do not balance to be accepted. If this setting is deactivated, checks and coupons must always balance prior 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.

Setting	Description
Auto-Decision for Held/Unworked items	Select the decision that will be applied to items that were put on hold or not worked on when the sweep takes place.
Image display location	Specify a location for the image viewer: below or to the right of the data.
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 <b>Add</b> .

## 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	Activate this setting to allow users to generate correspondence based on predefined templates. This setting applies for the Archive, CDM and PPW. See the <i>Kofax iRemitUser Guide</i> for information on generating correspondence. You must add at least one correspondence template.
Enable PDF splitting by sweep time	Activate this setting to create a PDF for an organization for each sweep time.
Enable PDF splitting by Site/SubSite	Activate 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.  <b>Note</b> Do not use this setting in combination with Enable PDF splitting at sweep time. Choose either one option or the other.
Create cover page on correspondence	Activate 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	Activate 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	Select 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 in which they were added. Subgroups may see a template in the list that was added in a parent group, but they cannot delete the template.

## Workflow preferences

For workflows, you can configure the following settings:

Settings	Description
Enable	This enables or disables the Workflow module for the group along with any subgroups. 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 <b>Add</b> . To delete a rollup code, click the trash can symbol next to the value to be removed.
Stages	Workflow supports multi-level authorization. The number of levels can be defined here. Type the name of the level you want to create in the text field and click <b>Add</b> . To delete a stage, click the trash can symbol next to the stage to be removed.

### Add a workflow to a group

When adding a workflow to a group, note the following:

- Contact iRemithelp@kofax.com to set up validation for incoming ACH transactions.
  - The Workflow module does not appear until files have been loaded.
1. Go to **Group Management**.
  2. Go to **Preferences/Workflow**.
  3. Click **Enable**.
  4. Create the name and number of stages.

### Add Workflow Privilege to a user

1. Go to **User Admin**.

2. In the user list, click the user.
3. On the **Group Privilege** tab, assign the **Archive User** role.  
The user must be assigned to the Archive User role the first time you grant access so the other workflow privileges become available.
4. Click **Save**.
5. On the **Group Privilege** tab, scroll to the end of the list of the roles where the workflow roles are listed.
6. Select the roles you want to assign to the user.
7. Assign the appropriate workflow stage to the user.
8. Save the user.

## Manage sweep

The **Sweep Management** button is only displayed if you have the user role **CDM Sweep Admin**. 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

The **Broadcast Management** button is only displayed if you have the user role **Broadcast Admin**. Broadcast Management enables you to send broadcast messages to users. Broadcast messages are displayed on the Kofax iRemit home page.

## Set IP filters

You can restrict the use of iRemit to computers with specific IP addresses. Users can only sign-in to iRemit on computers whose IP address is specified in the IP filters list. If no IP filters are defined, users can sign-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 and then click the **IP Filters** button.
2. Enable **Ip Filtering**.
3. Save the changes.
4. Click the **Ip Filters** button on the right side of the screen.
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** (  ).

## 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.

**Note** Prior to testing, in the **Group Management** window, 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 changes 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 on 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. Your changes will therefore only be available to users on the following day.

The progress of the promotion to production is displayed in the **Group Management** window in both the configuration environment and the production environment.

## Chapter 2

# 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 which data they can view and which 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.

Which user data you can modify depends on which 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 homepage, select the group to which the user will belong (or its parent) and then, on the toolbar, select **Administration > User Management**.

A list of existing users for the selected group and its subgroups 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**.

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

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 list to display only **Enabled** users, only **Disabled** users, or **Enabled & Disabled** users.

Use the paging buttons at the bottom of the list to view more users.

## Add a user

1. Click **Add User** (+) at the top right of the user list.
2. In the **Info** tab, enter details for the user.
3. Click **Next Step**.

4. In 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 processor level.
5. Click **Next Step**.
6. In the **Group Privileges** tab, click on the group for which you want to assign the user's roles.
7. Click on each role you want to assign to the user. Assigned roles are highlighted. You must assign at least one role for each user.  
To remove a role, click the role to remove the highlight.
8. 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	Set to ON to allow the user to log on to iRemit.

## Available roles

You can assign the following roles.

Role	Description
Select All	Check this check box to assign all roles.
Archive User	The user can access the Archive module.
Archive-Restricted	This Archive user has access to 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 decided 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 homepage and the Dashboard page.
Dashboard User	The user can view charts and reports on the iRemit homepage, 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.



Role	Description
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 that has that group assignment can only see that group and none of its children.
Notifications Admin	The user can create "subscriptions" to send messages to users when specific system events occur.
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

**Note** You cannot edit your own user profile.

1. In the user list, click on the user.
2. Make the required changes to the user details.
3. To view or edit the user's roles, in the **Group Privileges** tab, click on the appropriate group then click the **View Roles**  or **Edit Roles**  button.

4. To change the groups to which the user belongs:
  - To add a new group, click **Add Group** (⊕) at the top right. In the group hierarchy, select the new group, then assign roles and click **Save**.
  - To remove a group, in the **Assigned Groups** list, click the group, then click **Delete Group** (🗑️ Group).

## Change a user password

1. In the user list, click on the user.
2. In the **Sign in** tab, enter and verify the password, making sure that it adheres to the password rules. Password rules are defined at processor level.
3. Click **Save**. This button is only enabled if you enter a password that adheres to the rules.

## Enable or disable a user

1. In the user list, click on the user.
2. In the Info tab, click the **Enabled** setting to change the setting to **On** or **Off**.
3. Click **Save**.

## 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

To view and download a report of all users and the roles assigned to each user, on the toolbar select **Administration > User Privileges**.

Select a **Group** and **User Status**, then click the **Search** button.

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

The following example shows some of the information included in the report.

Click **Download** to download the report details for the selected group only to a CSV file.

Click **Download including sub groups** to download details for the selected group and its subgroups.

## Chapter 3

# 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 homepage. 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 role Broadcast Management 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. In the group selection list, select the group for the message.
2. On the toolbar, select **Administration > Broadcast Management**.
3. Click **Add** (⊕) at the top right of the list.
4. Enter the message details and click **Save**.

Setting	Description
Message text	The text of the message.
Start Date/Time	The date and time from which the message will be displayed on the home page.
End Date/Time	The date and time at which the message will be removed from the home page.
Active	Activate this setting to enable 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.

## Send a broadcast message to individuals and distribution lists

To send a broadcast message to an individual user or a distribution list, first set up a notification subscription. Then, you can send the broadcast message. Users can view up to 5 messages at a time, and they remain for 15 days before being removed.

1. On the toolbar, select **Administration > Notifications > Notification Management**.
2. Click **Add Subscription**.
3. Select the event type **Broadcast Message**.
4. Enter a start date and an end date.  
These dates represent the time in which you will have the ability to send these users a message.
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 role **Notifications Admin** 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:
  - CDM Import Complete
  - IDX Extraction Complete
  - Import Complete
  - IRWF Import Complete
  - IRWF Item Changed
5. Enter a start date and an expiration date, then click **Update**.
6. Click on **Add Delivery**.
7. In the **Delivery Information** selection list, select **ApplicationMessage**.

8. In the **Send To** field, select the email addresses of the users who should see the notification on their home page.
9. Enter the header and body text for the notification, then click **Update**.
10. On the toolbar, select **Administration > Notifications > Create**.

## Open the Subscriptions screen

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

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 Served) and when the notification will be sent again (Next Delivery).

## Add a subscription

1. Select a group from the selection list on the left of the screen.
2. Click **+ Add Subscription**.
3. In the **Edit** window, enter the **Event Type**, **Start Date**, and **Expiration** date. Click the calendar button ( ) to select the dates from a calendar.

Whenever the selected event occurs between the given start and expiration dates, a notification is sent to users.

You can select the following event types:

- CDM Import Complete
- IDX Extraction Complete
- LTA Import Complete
- Report Import Complete
- IRWF Import Complete
- IRWF Item Changed

4. Click **Update**.

After creating a subscription, you can add filters. You then need to add a delivery method for the subscription.

## 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 the **Filter** button ( ) next to the subscription.

The **Filter Builder** window opens. Which filter properties are available here depends on the subscription's event type.

2. In the **Operator** column, double-click **Equals** beside the filter property you want to set.
3. Select the appropriate operator from the list.
4. Click in the **Value** column for the property and enter a value.
5. Click **Update**.

## Add a delivery to a subscription

After you have created a subscription, you must set up the delivery method and frequency.

1. Click on the subscription, then click the **Add Delivery** button.
2. In the **Edit** window, select a **Frequency**.
  - **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.
3. Enter the notification details.

Field	Description
Delivery Information	Select <b>Email</b> to send notifications via email. Select <b>ApplicationMessage</b> to display notifications on the iRemit home page.
Start Time	For the frequency <b>Daily</b> or <b>Monthly</b> , the time at which the notification will be sent.
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 <b>Category</b> 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 <b>Message</b> 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 <b>Header</b> or <b>Body</b> text box, all variables containing that character are displayed. Click a variable to insert it in the text.
Footer	For email notifications only. This text is displayed at the end of the email.

4. Click **Update**.

## Edit a subscription

1. Click **Edit** (✎) next to the subscription.
2. In the **Edit** window, change the start date or the expiration date.
3. Click **Update**.

## Delete a subscription

1. Click **Delete** (🗑) next to the subscription.
2. Click **Delete** when prompted to confirm the deletion.

## Display expired subscriptions

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

## Chapter 4

# Holiday Calendar

Users with the role **Holiday Calendar Manager** 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.

**Note** 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 a **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 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 automatically saved.



## 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. Click **OK** to confirm the deletion.

## Chapter 5

# 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 role **Sweep Management** 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 (for example, 5 p.m. 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 (for example, 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.

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

## Add a sweep

- 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**.
- Click **Add** (⊕) at the top right of the list.
- Enter the details for the sweep, then click **Save**.

## Sweep details

Setting	Description
Site/Subsite ID	The ID of the site/subsite.
Bank ID	The ID of the bank. (Optional)
CID	The processor organization's internal client ID. (Optional)
First Run Date	The first date on which the sweep will run.
Sweep Time (local)	The time at which the sweep will run. Local means the time at the site where the sweep will run.
AutoSchedule	Activate this setting to schedule the next sweep automatically to run at the specified time and interval when the current one has completed
Interval	How often the sweep will run.

## Add a mini-sweep

- In the sweeps list, click **Edit** (✎) to the right of the main sweep.
- Click **Time** (🕒).
- Click in the **Hour** and **Minute** columns to select a time.
- Click **Add MiniSweep**.

## Delete a mini-sweep

- In the sweeps list, click **Edit** (✎) to the right of the main sweep.
- Click **Delete** (🗑) next to the mini-sweep.

# Stop File Management

Users with the role **Stop File Management** can upload a stop file to validate accounts entered by CDM users. The stop file determines which account numbers users are allowed to enter when editing CDM items. An error message is displayed if the user tries to enter an invalid account.

A stop file may be a blacklist or a whitelist:

- **Blacklist (default):** Excludes accounts. All account numbers except those listed in the stop file are valid.
- **Whitelist:** Includes accounts. Only the account numbers listed in the stop file are valid.

The stop file must be in CSV format, with each account number separated by a comma.

To upload a stop file, do the following.

1. On the toolbar, select **Administration > Stop File Management**.
2. Click **Add new record**.
3. Enter a name for the stop file and click **Choose File** to select the CSV file.
4. By default, the stop file is a blacklist. Select the **Whitelist** check box if you prefer to use a whitelist.
5. Click **Insert**  to add the stop file.

## Chapter 7

# Data Management

Users with the role Data Management can delete transactions from the iRemit archive.

1. On the toolbar, select **Administration > Data Management > Delete Transaction**.
2. Enter the details of the transaction. You must fill in all fields.
3. Click **Delete**.

## Chapter 8

# IDX Administration

The iRemit Information 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 **Welcome to IDX** page displays 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 on **Create new Job** on the left of the page.
2. Enter the job details and schedule the job.

Note the following:

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

3. Click **Save Job Configuration**.

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

## General

Setting	Description
Job Name by User	A name for the job.
Description	A description of the job.

Setting	Description
Template Id	Select a template that defines which fields will be exported. If no templates are available, select <b>Standard Extract</b> . Kofax can create custom code for your extract and deliver this code as a plugin. To use a plugin instead of a template, select <b>No template (retrieve it from plugin)</b> .
Output Filename	The name of the output file. The output file is saved to the FTP site. If you activate the option <b>Download on Demand</b> , it is only available to users with the <b>Download IDX</b> privilege. To automatically include the extract date in the file name, include the following syntax in the file name: {P:Mmddy}. If you download several files a day, you can include the date and time using the following syntax: {P:MMddyhhmm}.
Download on Demand	Select this option to make the extract function available to users with the <b>Download IDX</b> function.

## Schedule

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.

## Custom filters

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

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

## 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 the 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.



## Chapter 9

# Auditing

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

To view an audit report, on the toolbar, select **Administration > Auditing**, then select the desired report.

Enter search criteria, then click **Search**. Which criteria are available depends on the selected report.

You can download the report results to a CSV file by clicking **Download** at the top of a 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.

## Admin Report

The **Admin Report** allows you to view the activities of users in the application. Two report types are available: **Administrative** and **Authentication**.

Both report types can be generated for all users or an individual user.

### Administrative

The **Administrative** report shows details of the activities users performed in the application.

### Authentication

The **Authentication** report shows details of when users logged in and logged out.

## LTA Audit Report

The **LTA Audit Report** allows you to view the activities of users in the Archive module. Two report types are available: **Search** and **Image**.

Both reports can be generated for all users or an individual user.

### Search

The **Search** report shows details of the searches performed by users.

## Image

The **Image** report 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. The report can be generated for all users or an individual user.

## PPW Audit Report

The **PPW Audit Report** allows you to view the activities of users in the Post Processing Workflow module. The report can be generated for all users or an individual user.

## 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**.

## Download IDX Report

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

## Download IDX Purge Report

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