IDENTIFI ADMIN GUIDE

TABLE OF CONTENTS

COPYRIGHT INFORMATION AND CHANGES

INTRODUCTION

Identifi

Identifi is a suite of software products allowing the storage and retrieval of document images. Additionally, documents can be signed electronically, tracked for expiration, retention and compliance, and set to trigger actions and workflows.

The product suite includes:

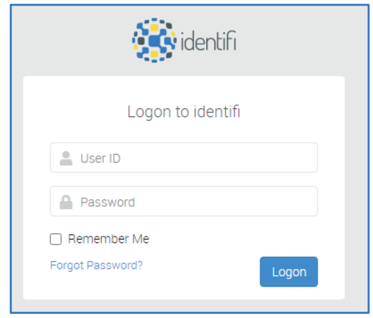
- Documents
- Tracking
- Electronic Signatures
- Electronic Receipts
- Workflow
- Reporting

This Guide is designed to help Identifi Administrators manage all aspects of their installation(s), including (but not limited to): Applications, Entities, Document Types, Attributes, Reports, as well as Scanning and Indexing. Additionally, User Management and Security will be addressed.

Note: All Identifi products are available in Identifi and are “turned on” for each customer based on which products have been licensed.

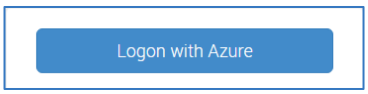
For the purposes of this Guide, all available products are represented; however, if a product is not licensed to the customer, the User will not see the specific menu(s) for the unlicensed product(s).

Logging in to Identifi



Log into Identifi by double-clicking the Identifi shortcut located on the desktop or by entering the installation's address into an internet browser page (http://[servername]/identifi.net).

If Identifi is configured to use the customer's Active Directory (AD), then the logon is seamless. The User will not be prompted to enter the logon credentials. With other SSO, the user will be presented a single logon button. With no SSO in place, the User will be prompted to enter their credentials. The password is case-sensitive.



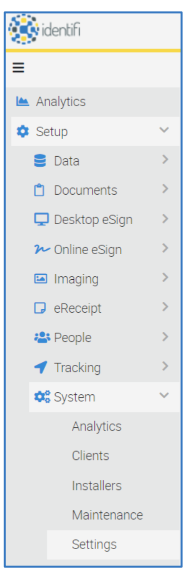
Identifi is certified to work with Okta and Azure Identity Providers, allowing for a Single Sign-On experience. See Managing Installation Configuration & Clients for details.

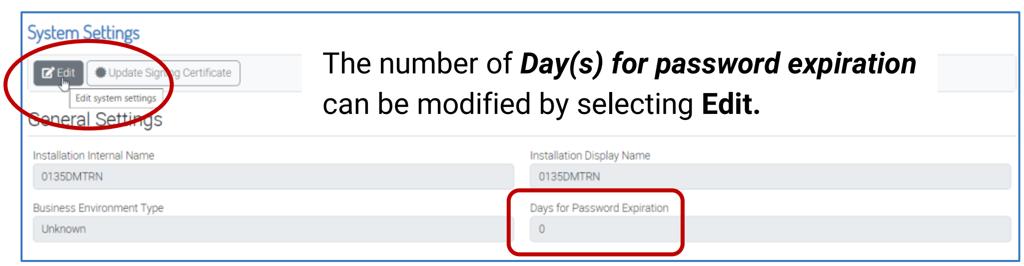
The **Forgot Password** link will initiate an email with a link to reset the password. It is only available if a single sign on solution is not being used, as passwords are managed in those applications rather than Identifi. It is suggested that Users change their password at least every 60-90 days. Administrators may choose to set expiration of passwords at the installation level (see below).

Managing Passwords

User passwords are required to be twelve characters long, including a digit or special character, an uppercase and lowercase character, with no spaces. See *Editing Users* for management of an individual user's password.

Password expiration is managed under ***Setup ->System->Settings***



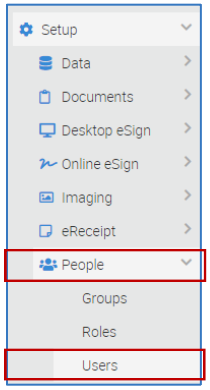


The number of ***Day(s) for password expiration*** can be modified by selecting **Edit.**

Managing Users/Groups

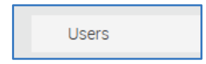
Users and Groups are managed under the ***Setup*** menu.

Users

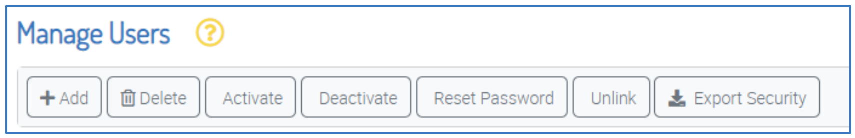


In order to log in to Identifi, a user must be given and UserID and set up as a User. Security (roles and permissions) can be applied directly to the User or to a Group that the User belongs to.

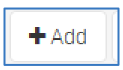
From the Main Menu, select ***Setup***, then ***People*** and click ***Users.***

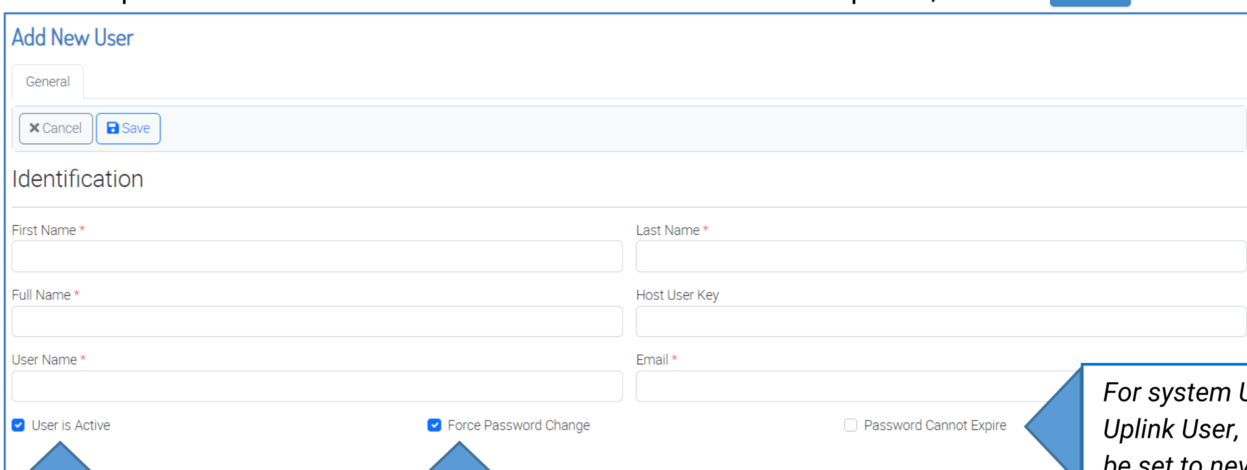


The list of all Users will be presented along with the following menu at the top of the page:



Adding Users

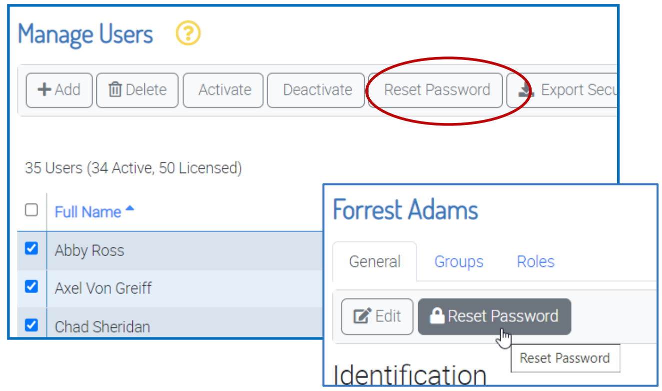
Click on  button in the top menu, which will open a New User Form. Required fields are marked with an asterisk * . When completed, select  .



For system Users, like the Uplink User, the Password can be set to never expire.

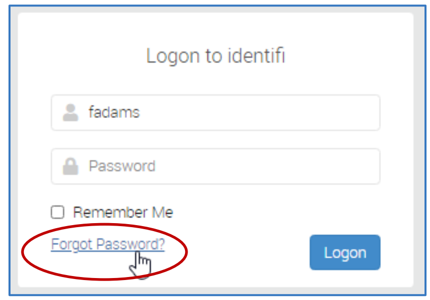
Note: **User is Active** and **Force Password Change** *are checked by default.* The first time the user logs in, they will use the *Forgot Password* link to create their own password. ***NOTE:*** *Installations using SSO do not need for their users to set up passwords in Identifi.*

New Users and Passwords



In order for new users to log in to Identifi, a Password Reset must be initiated for them. An individual reset can be sent from the User's *General* tab or, if multiple users have been added, from the main Users list.

NOTE: *Users on installations using SSO do not need to set up Passwords in Identifi.*

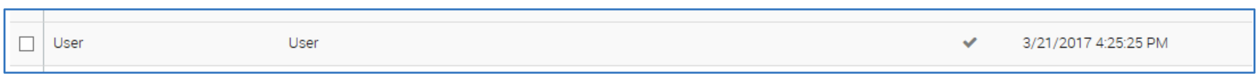


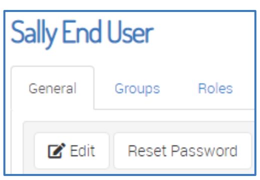
Alternatively, if the User has the URL, they can use the ***Forgot Password*** link to initiate the email themselves.

NOTE: In all cases, the User will need to be provided their User ID by an Administrator.

Editing Users

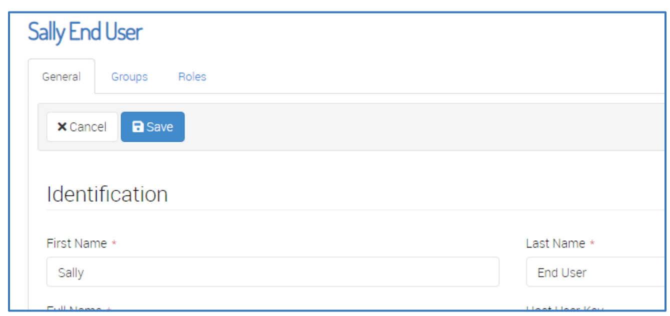
To make changes to an existing User, click the name in the Users List.

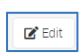


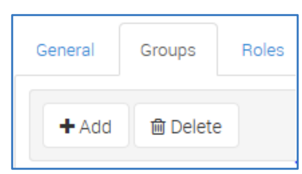


To reset the user's password, simply select ***Reset Password***.

The user will receive an email prompting them to change their password.



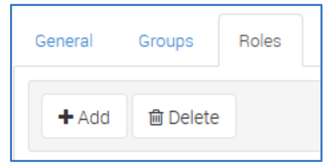
Under the ***General*** tab, select  to make changes to the User's name, login name and other information, including forcing a password change on their next login. Click ***Save*** when complete.



Under the ***Groups*** tab, Users can be added or removed from existing Groups.

When a User is added to a Group, the User is granted all permissions assigned to the Group. Likewise, when a User is removed from a Group, any associated permissions are revoked from the User.

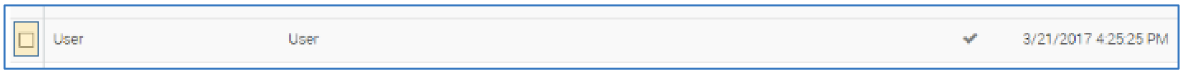
Under the ***Roles*** tab, Users can be assigned Roles and have Roles removed.



Adding and Deleting Roles here does not affect any Roles associated with Groups to which the User belongs.

Deleting Users

To Delete a User, place a check in the box next to the name and select Delete in the top menu.

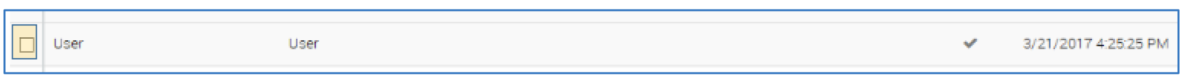


The User will be removed from the User List and will have no access to Identifi, but all actions taken by the User within the system will remain associated with them.

Note: The UserID of the deleted User can not be used again. If it could be possible that they will need to be an Identifi user again in the future, consider *Deactivating* the User instead.

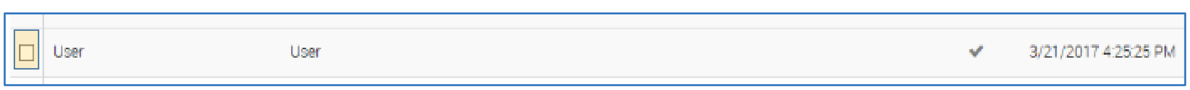
Deactivating Users

Deactivating a User prevents them from being able to log into Identifi and frees a 'seat' for another User to log onto the Identifi installation. To Deactivate a User, place a check in the box next to the name and select Deactivate in the top menu.

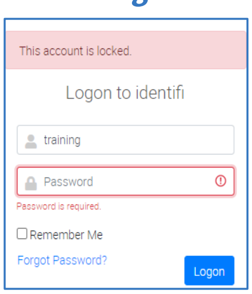


Activating Users

Activate users that have been Deactivated to allow them the ability to log onto the Identifi installation. Place a check in the box next to the name and select Activate in the top menu.

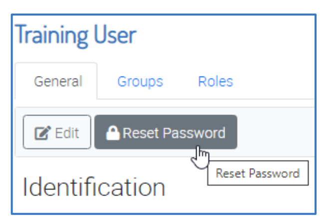


Unlocking Users

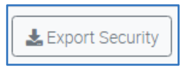


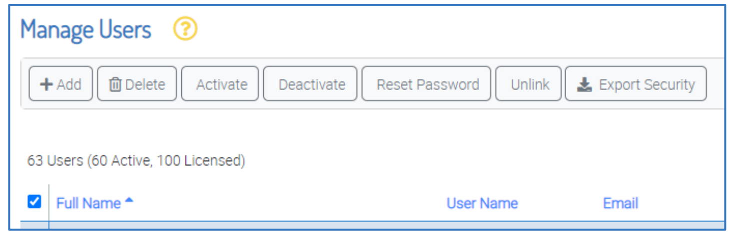
Five unsuccessful login attempts will lock the User. The account will automatically unlock after five minutes.

If the user is not able to recall their password, select ***Reset Password*** here or ask them to use the ***Forgot Password*** link on the login page.

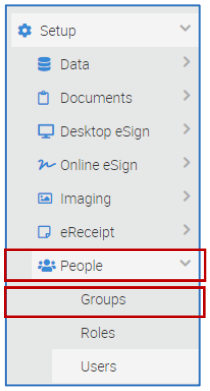


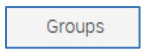
Exporting User Security

To see a list of Users and the Roles assigned to them, select one or more Users from the list and then click ***Export Security*** in the top menu. This will create an Excel spreadsheet. 

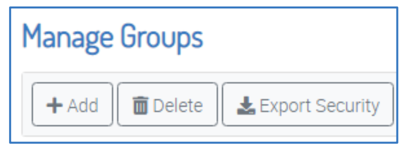


Managing Groups

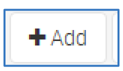


Groups are a tool to assign all levels of security to a number of Users simultaneously. From the Main Menu, select ***Setup***, then ***System*** and click ***Groups.*** 

Adding a User to a Group automatically provides the Group's security to them, likewise removing a User from Group automatically strips that Group's access from the User.



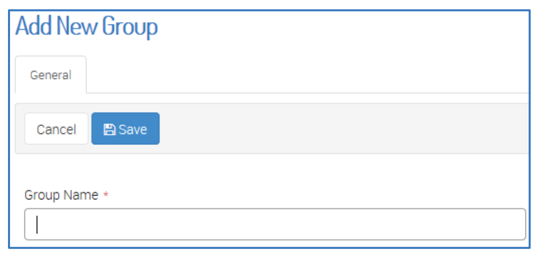
Adding Groups

Click on 

button in the top menu, then enter the name of the Group being created.

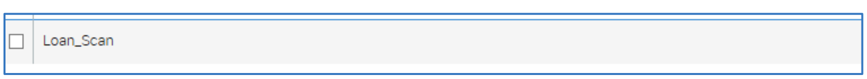
When completed, select 

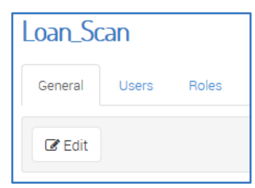
.



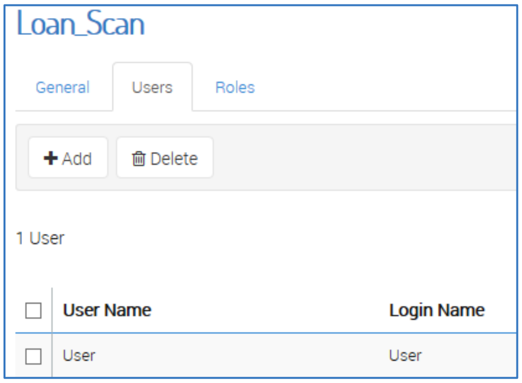
Editing Groups

To make changes to an existing Group, click the name in the Group List.



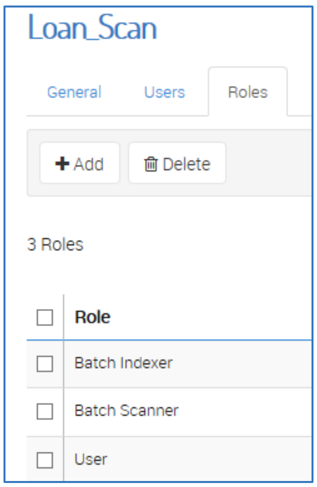


Under the ***General*** tab, select ***Edit*** to make change the Group's Name. Click ***Save*** when complete.



Under the ***Users*** tab, select ***Add*** to add additional Users to the Group. To remove Users from the Group, place a check in the box next to their name and select ***Delete.***

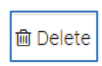
Note: Users added to a Group are automatically granted all permissions assigned to the Group. When Users are removed from a Group, any associated permissions are revoked from the them.



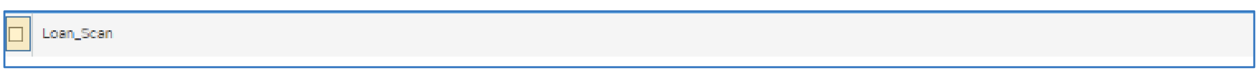
Under the ***Roles*** tab, select ***Add*** to add additional Roles to the Group. To remove Roles from the Group, place a check in the box next to the Role and select ***Delete.***

Note: Roles assigned to a Group are automatically granted to all members of the Group. Permissions granted to a Group in other areas of the product (Entities, Applications, Scan Plans, etc) are automatically extended to all of its members.

Deleting Groups

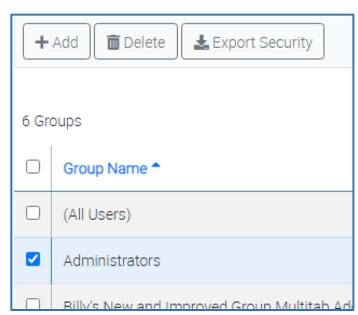
To Delete a Group, place a check in the box next to the name and select 

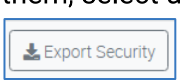
in the top menu.



The Group will be removed, however any Users that were members of the Group will remain in Identifi. Any Roles/Permissions the Users had as members of the Group, though, will be revoked.

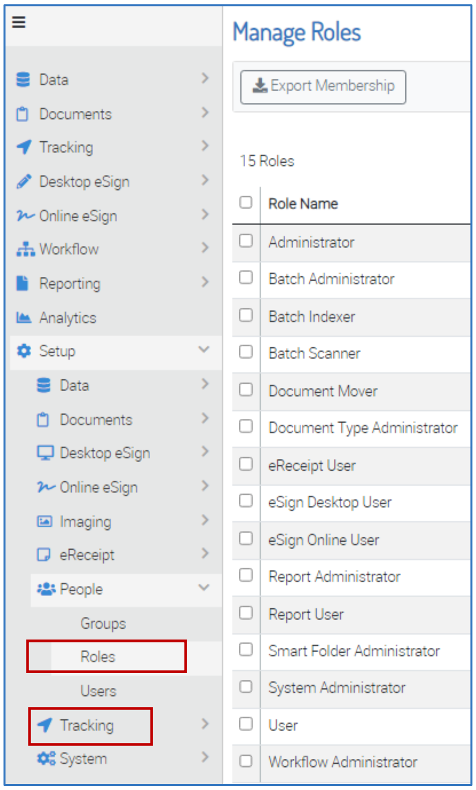
Exporting Group Security



To see a list of all Groups, their members and the Roles assigned to them, select at least one Group from the list and then click 

in the top menu. This will create an Excel spreadsheet.

Identifi User Roles

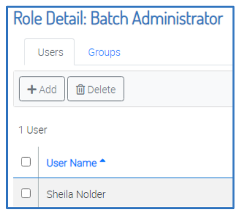


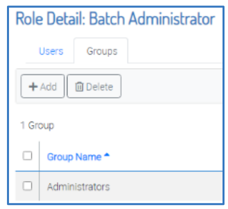
User Roles provide access to specific features of Identifi. All User must have a User Role assigned to them or be part of a Group with a User Role assigned to it. The minimum Role required is the *User*.

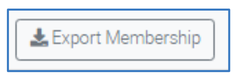
Roles are found in the Main Menu, by selecting ***Setup***, ***People*** and then ***Roles.***

Role Membership

Clicking on a Role in the list will present two tabs showing which Users and Groups have the Role assigned.

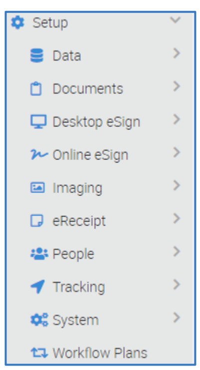
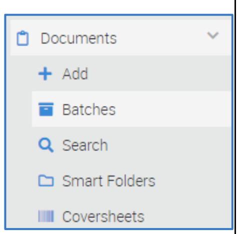


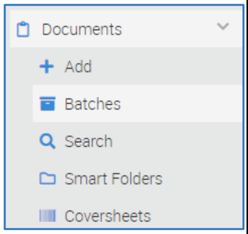


Selecting 

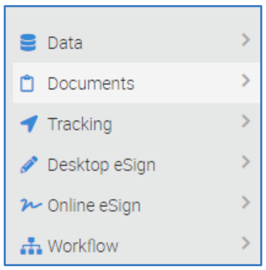
will produce an Excel spreadsheet listing all roles and the Users and Groups assigned to them.

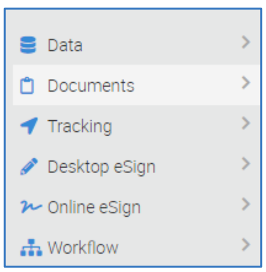
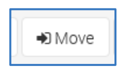
Role Descriptions

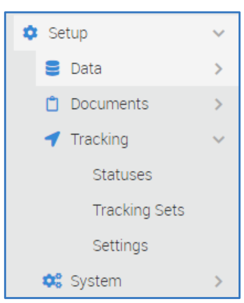
ROLE	ACCESS
Administrator 	Access to all features and the ability to manage all aspects of the installation (except Online eSign *Settings* which is only available to those with the **System Administrator Role**). **Note:** A user with this role cannot be prevented from accessing documents, data, system menus, etc. through Permissions or Rights. Able to delete documents with active Retention Policies.
Batch Administrator 	Access to the ***Batches*** and ***Add*** features under the **Documents** menu. Able to index, reassign and delete all batches. Able to upload and index electronic documents through Add, pending Application Permissions. Must also have **User Role**.

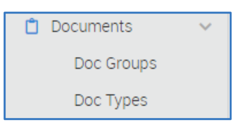
<table>
<tr>
<td>Batch Indexer

</td>
<td>Access to the Batches and Add features under the Documents menu. Able to index their own or unassigned Batches.

May be able to delete their own Batches (if set at the installation level. See here). Able to upload and index electronic documents through Add, pending Application Permissions.

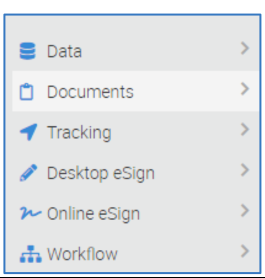
Must also have User Role.</td>
</tr>
<tr>
<td>Batch Scanner

</td>
<td>Ability to use the Scan Client.

Must also have User Role.</td>
</tr>
<tr>
<td>Document Mover

</td>
<td>Ability to use the  feature in Document Search, to move a document from one Application to another. Must have Permissions for both Applications.

Must also have User Role.</td>
</tr>
<tr>
<td>Document Type Administrator


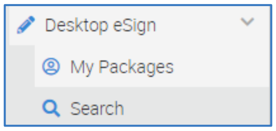
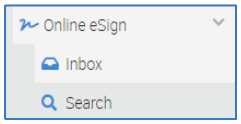
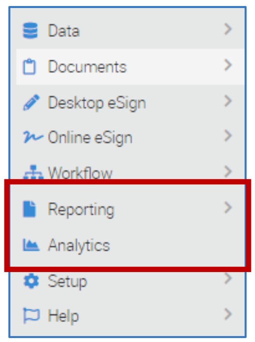
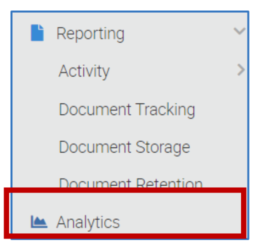
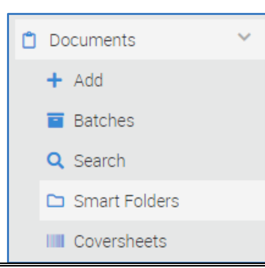

</td>
<td>Ability to manage all Document Groups and Document Types (Delete, Add and modify).

Must also have User Role.

Document Tracking: Ability to manage Tracking Sets, including at the Entity, as well as Tracking Statuses and perform Tracking Maintenance.</td>
</tr>
<tr>
<td>eReceipt User

</td>
<td>Ability to access the eReceipt client.

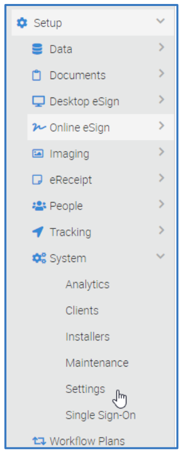
Must also have User Role.

Note: In order for the User to also be able to scan barcoded Drive-Thru receipts, the Batch Scan User Role is also required.</td>
</tr>
</table>

Desktop eSign User 	The ability to access the Desktop eSign Client, eSign Search and Packages. Must also have **User Role.**
eSign Online User 	The ability to create, manage and index Online eSign Packages. Retrieval of indexed documents pending Application Permissions. Access to create Packages limited by Profile Rights.
Report Administrator 	Ability to view and manage all reports within **Analytics**; ability to access all reports within *Reporting*. Must also have **User Role**.
Report User 	Access to any reports within **Analytics** that the user has been granted Permissions to view as well as *Document Tracking* and *Document Retention* under **Reporting**. Viewing of items and documents referenced on reports limited by Permissions. Must also have **User Role**.
Smart Folder Administrator 	The ability to create and manage Public Smart Folders. Access to specific Documents dependent upon Application Permissions. Must also have **User Role.**

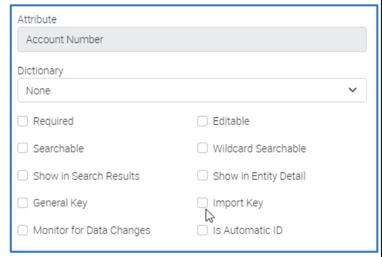
<table>
<tr>
<td>

System Administrator



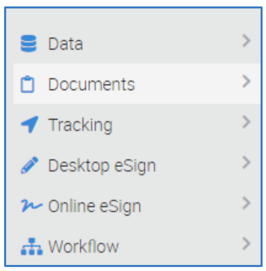
</td>
<td>

Access to all features and menus, including *Settings* for the installation (**Setup->System-> Settings**) and *Settings* for Online eSign (**Setup->Online eSign-> Settings**) and the ability to set 'Import Key' attributes for an Entity.



</td>
</tr>
<tr>
<td>

User

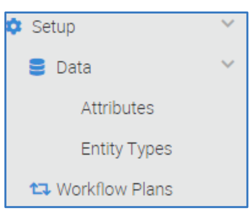


</td>
<td>

Basic user functions for Data, Documents, Tracking and Workflow. Includes access to Coversheets.

Access to specific Data, Documents and Workflow Plans dependent upon Entity and Application Permissions and Work Plan Rights.
</td>
</tr>
<tr>
<td>

Workflow Administrator



</td>
<td>

Ability to design and manage Workflow Plans.

Design Rights on existing Plans required to access them.

Must also have **User Role.**
</td>
</tr>
</table>

Identifi User Permissions

These permissions are assigned to Users and Groups at the following levels:

- Application
- Entity Type
- Attribute
- Document Type
- Security Profile

Security Exports showing which Users and Groups have these Permissions assigned are available from the Application, Entity and Document Type management screens.

Permission Descriptions

***Application, Attribute, Document Type & Security Profile* Permissions**	
Add Note	Allows Users to Add Notes on the document. Can also Delete their own Note. *Must also have View Note permission*.
Change Note	Allows Users to Delete Notes on the document. Note: *Must also have View Note permission.*
Delete	Allows Users to Delete the documents. Note: *Deletion is permanent*
Download & Print	Allows Users to use the Download and Print features in Document Search to print a .pdf or download the document image(s).
Index	Allows Users access to edit attributes in the Indexing Panel within the Document Viewer and to mass modify documents using Index in Document Search.
Revise	Allows Users access to the Upload Rescan features in the Document Viewer
Set Security	Allows Users to Set Security on the documents of a certain Document Type, within an Application or with a certain Attribute.
View	Allows Users to View the document. *Default*
View Note	Allows Users to access Notes Panel in Document Viewer and View Notes on the document.

***Entity Type* Permissions**	
Add Note	Allows Users to Add Notes on the entity items. Can also delete or modify their Note. *Must also have View Note permission*. **Document Tracking:** Ability to Add Requirement level notes.
Change Note	Allows Users to delete and modify any Note on an entity item. Note: *Must also have View Note permission.* **Document Tracking:** Ability to delete and modify Requirement level notes.
Create	Allows Users to Create new items in the entity using Add in the Data menu.
Delete	Allows Users to Delete entity items. Note: *Deletion is permanent* **Document Tracking:** Ability to *Delete* Requirements.
Set Security	Allows Users to Set Security on entity items.
Update	Allows Users access to modify details of entity items. **Document Tracking:** Ability to *Add* Requirements, Tracking Sets and Assigned Users. Access to override and adjust Requirement Status and Due periods.

<table>
<tr><th colspan="2">Other Permissions</th></tr>
<tr><td>

Analytics Report Rights: Allows Users to see specific custom reports in **Analytics.**

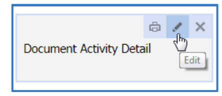
- ***None***- The report will not appear for the user.
- ***Full***- User will be able view, print and export report
- ***Read Only-*** Same access as *Full* rights.
- ***View Only-*** Same access as *Full* rights.
- ***Locked-*** Same access as *Full* rights

Notes:

Installations without this Custom Report feature will not see **Analytics** *in the menu at all.*

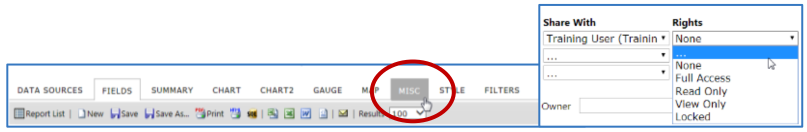
Identifi's Analytics Platform is nearing the end of life. It is being replaced with a combination of new reporting features in the main product as well as new features that make custom reports obsolete. For additional information, please refer to this article.

</td><td>



Click the ***Edit*** icon for the report from the main menu.

Rights are set under the ***Misc*** tab of the report.

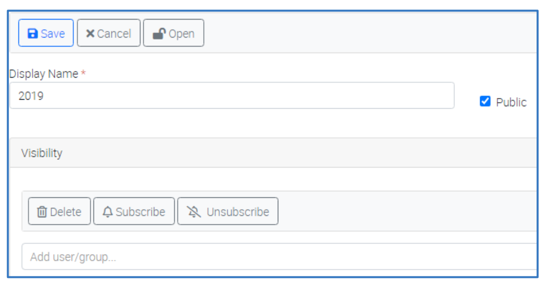


*Note: Limit 3 Users per Report. Those with ***Report Administrator Role*** do not need to be granted rights, since that role allows users access to all reports.

</td></tr>
<tr><td>

Public Smart Folder Visibility: Allows Users to see Public Smart Folders and Subscribe to them

</td><td>

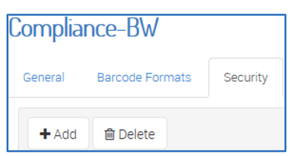


**Visibility can be granted by users with the Administrator Role or the Smart Folder Administrator Role.*

</td></tr>
<tr><td>

Scan Plan Security: Limits which Users will have access to use the Scan Plan.

</td><td>



*Note: Without any security assigned, the Scan Plan is available to all users with the ***Batch Scanner Role***.

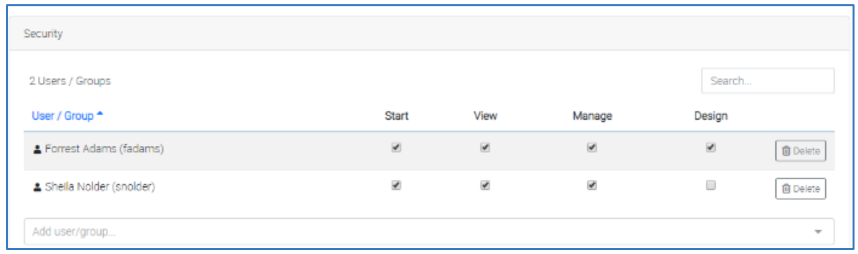
</td></tr>
</table>

<table>
<tr>
<td>

Work Plan Permissions: Determine what actions a User can take within a Workflow.

- ***Start***- Plan will appear in the Workflow *Start* menu
- ***View***- Plan and its steps will appear in Browse menu. User will also have the ability to run Workflow Reports on that Plan.
- ***Manage***- Plan and its steps will appear in Browse menu and User will be able to Reassign, change Priority, Terminate, and Resend Notifications for the Plan's items.
- ***Design-*** Will be able to edit the Plan design and settings.

</td>
<td>



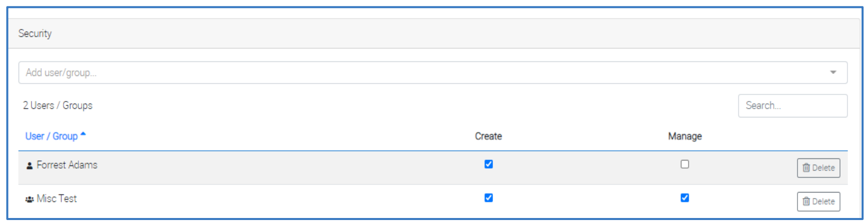
Must have **Administrator or **Workflow Administrator** Role (with Design Permissions on the Plan) to access the Workflow Plans menu under Setup.*

</td>
</tr>
<tr>
<td>

Online eSign Profile Permissions: Determine which Profiles a User is able to select when creating a Package and what rights they have to the Package during its completion.

- ***Create***- Profile can be selected when creating new Packages.
- ***Manage***- User will be able to Reassign, Delete and edit the Packages sent using this Profile.

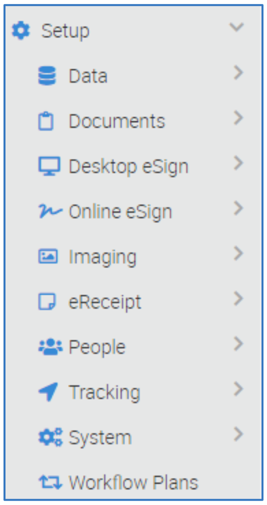
</td>
<td>



</td>
</tr>
</table>

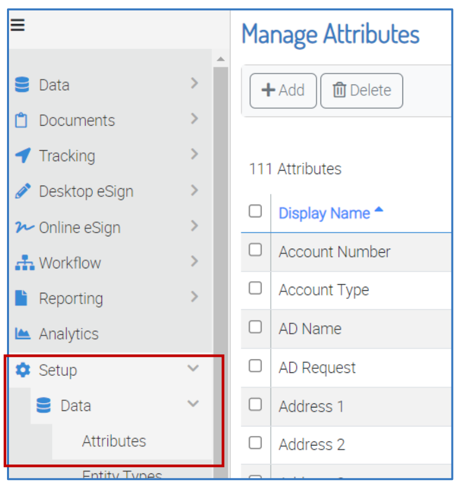
OTHER ADMINISTRATOR FUNCTIONS

SETUP MENU



Administrative settings and configurations for all features of Identifi are found under **Setup** in the main menu.

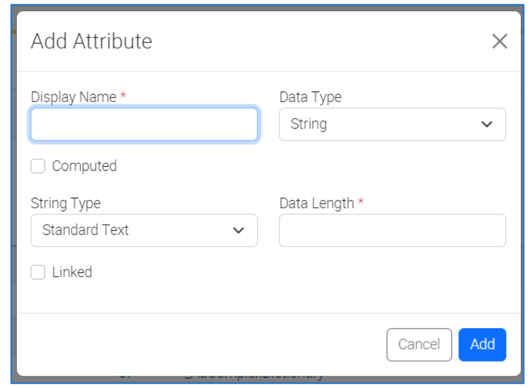
Setup – Data – Attributes



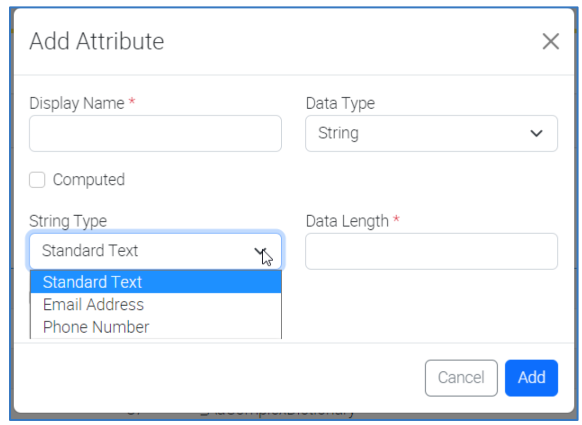
Allows Users to ***Add*** new attributes and ***Delete*** or modify existing attributes.

Adding an Attribute

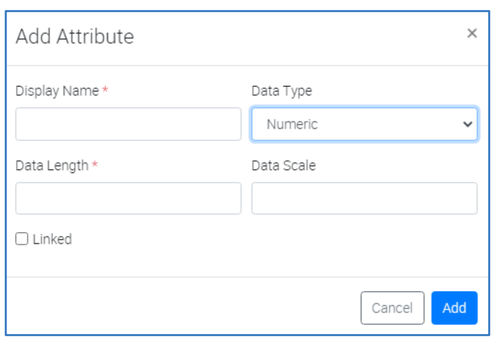
Select  from the top menu.



1. Enter a **Display Name** for the attribute.
2. Select the **Data Type**.

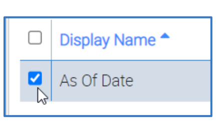


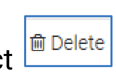
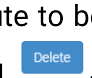
- For **String,** enter the following:
  - Select the **String Type** from the drop down
  - **Data Length**
- For **Numeric,** enter the following:
  - **Data Length**
  - **Data Scale**

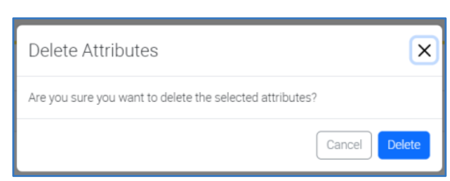


3. Place a check in the appropriate boxes if the attribute will be **Computed** or **Linked.**

Deleting an Attribute



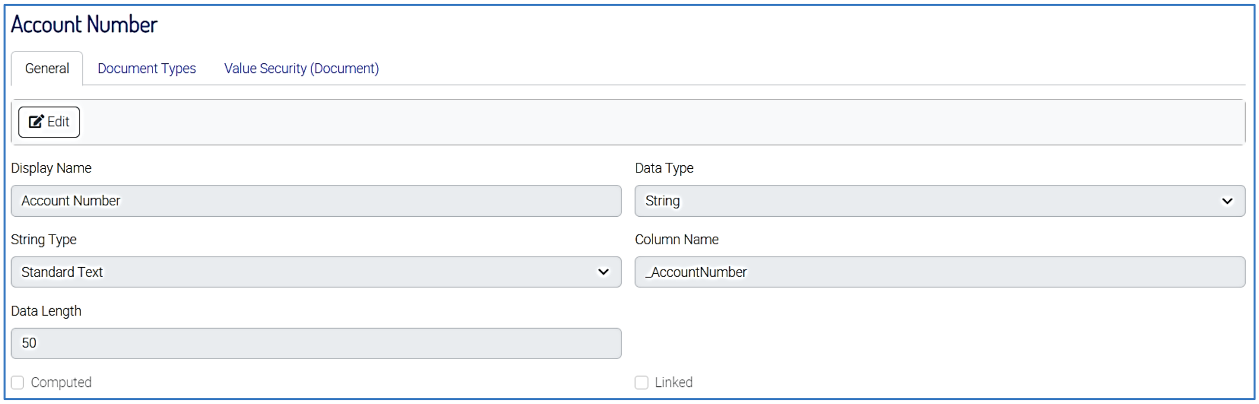
Place a check in the box next to the attribute to be deleted and select  from the top menu, then confirm by clicking .



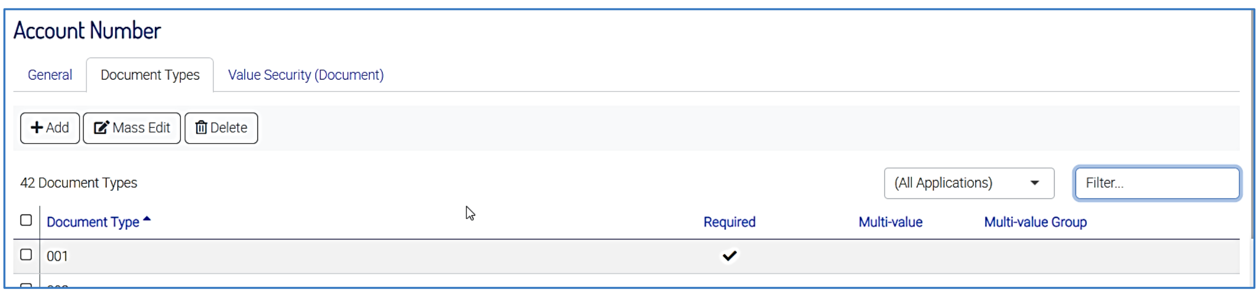
Modifiying an Attribute

Open an Attribute's details by clicking its Display Name.

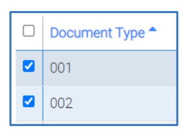
Under the ***General*** tab, select Edit to open the fields and make changes.



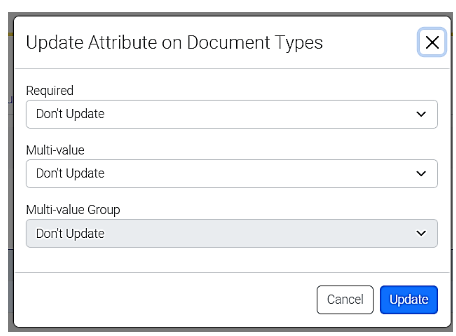
Under the ***Document Types*** tab, the attribute can be **added** to, or **deleted** from a document type.



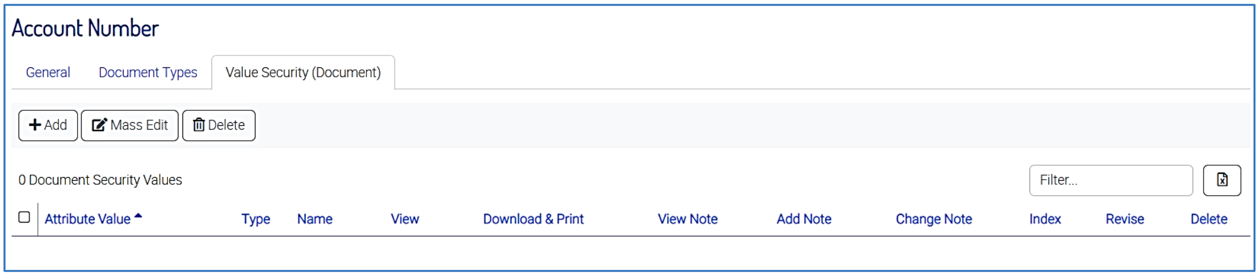
Mass Edit Allows a User to change the settings for the attribute on several Document Types simultaneously.



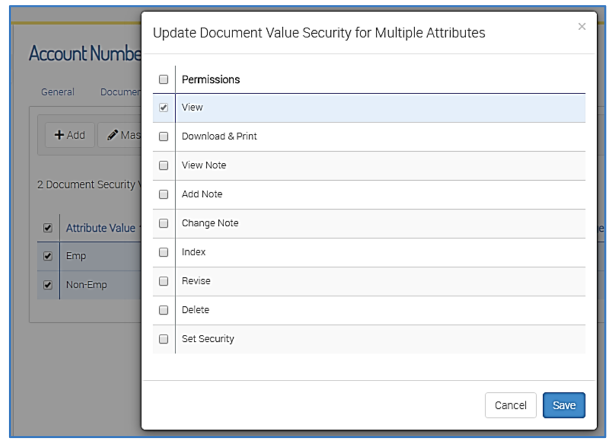
1. Place check marks next to all documents to be affected.
2. Make necessary changes and select Update



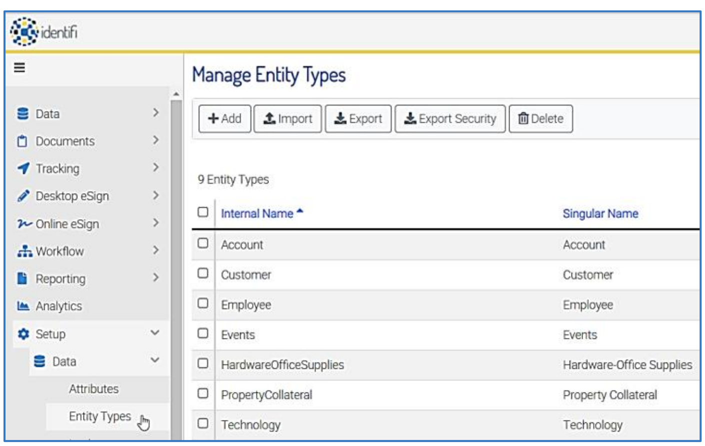
Under the ***Value Security*** tab, User access can be assigned based on an attribute value.



Mass Edit Allows a User to apply security to more than one Attribute value simultaneously.



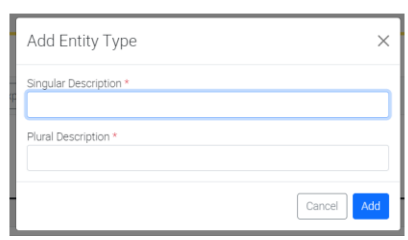
Setup – Data – Entity Types



Allows Users to ***Add*** or ***Import*** new Entity Types, as well as modify, ***Delete***, or ***Export*** existing ones.

Entity Permission security as assigned to Users/Groups is also available here.

Adding an Entity Type

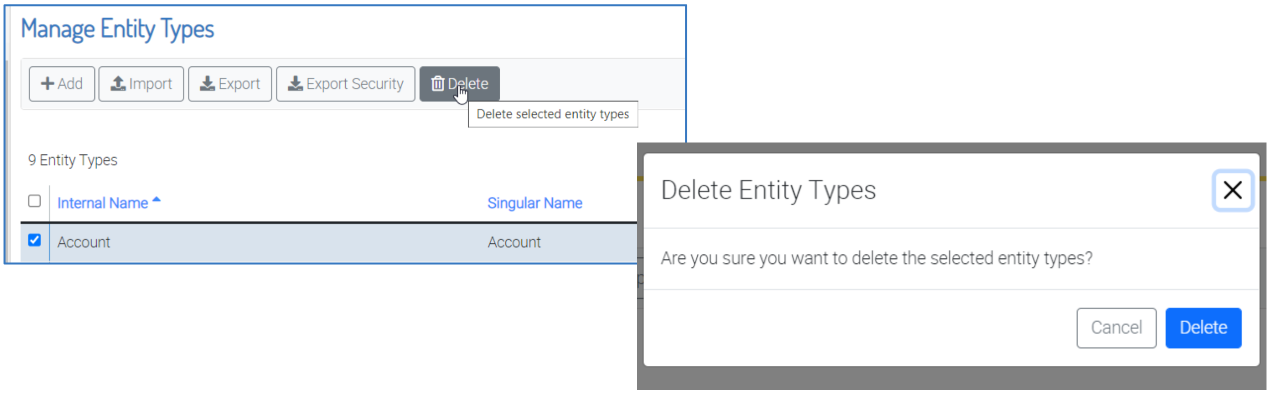


Select + Add from the top menu and enter the name of the new Entity Type in the **Singular Description** field. Enter the plural form of the name in **Plural Description** and click Save.

Attributes, User Roles and Relationships can then be added. See Modifying an Entity Type for details on these tabs.

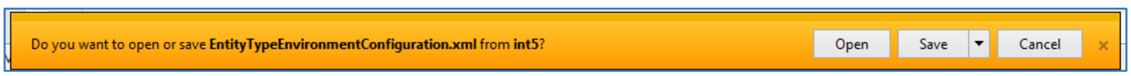
Deleting an Entity Type

Place a check in the box next to the entity type to be deleted and select Delete from the top menu, then confirm by clicking Delete

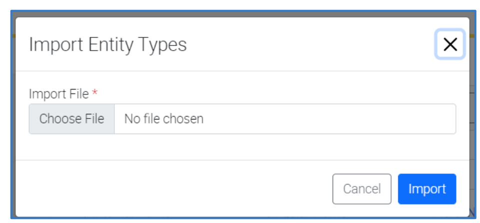


Exporting an Entity Type

If planning to copy an Entity Type from another installation, users may click the Export button to create the Entity Type's configuration .xml which can then be imported into the new Identifi installation.



Importing an Entity Type

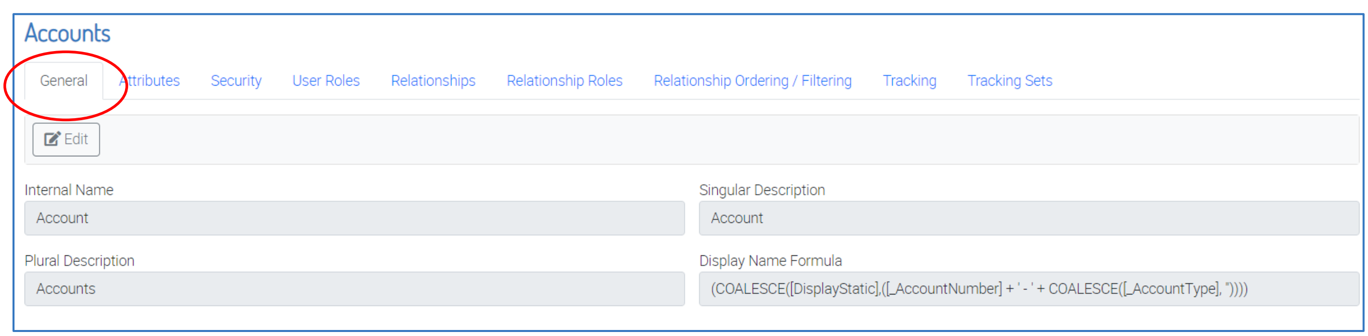


If copying an Entity Type from another installation, users may click the Import button to select the configuration .xml.

Modifying an Entity Type

Open an Entity Type's details by clicking its Internal Name.

Under the ***General*** tab, select Edit to open the fields and make changes



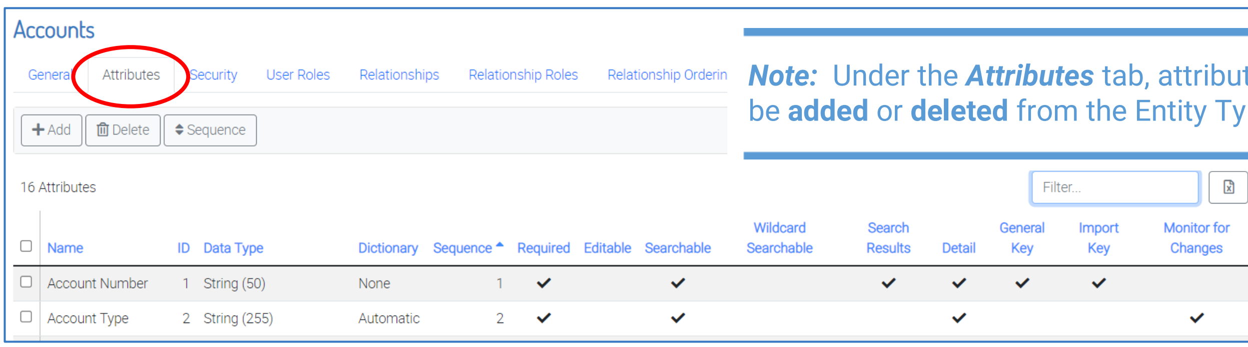
The **Singular** and **Plural Descriptions** can be edited here, however the **Internal Name** is created by the system when the Entity is intially created and cannot be modified. It is the Entity's name in the SQL table.

Display Name Formula: Determines how items are named when added to this Entity. It is a SQL formula made up of specific attributes associated with the item.

Best Practice: *Copy the Display Name Formula from another Entity and replace the attributes as needed, being sure to leave all other characters and spaces intact.*

Example: *(COALESCE([DisplayStatic],([_AccountNumber] + ' - ' + COALESCE([_AccountType], ''))*

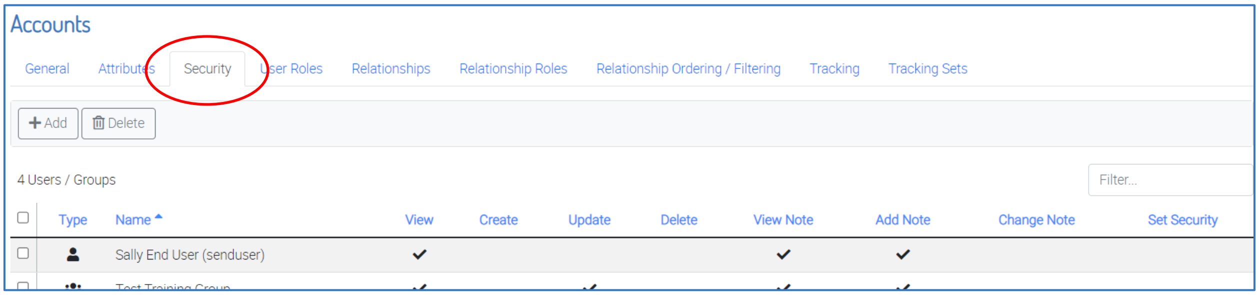
Settings for attributes within the Entity can be adjusted under the ***Attributes*** tab.



Note: Under the ***Attributes*** tab, attributes can be **added** or **deleted** from the Entity Type.

- **Data Type** – displays the data type of the attribute
- **Dictionary** – displays if there is a drop-down menu for the attribute during batch indexing and on the indexing panel
- **Sequence**- designates the position of the attribute on the *Data Detail* tab of an item in the Entity.
- **Required**- sets the attribute as required for new items added to the Entity.
- **Editable** – designates whether or not the attribute is editable.
- **Searchable**- enables the attribute to be searchable through Data Search.
- **Wildcard Searchable** – enables the attribute to be searchable using a partial term accompanied by an asterisk (*).
- **Search Results** – displays if the attribute is shown as a column in Document Search.
- **Detail** – designates if the attribute is shown on the *Indexing Panel* of a document stored in the Application ("Detail Visible").
- **General Key-** triggers Trak to look for this attribute; sets the unique record for Work items. ***Note:*** *If the installation is enabled for the "Desktop eSign to Online eSign Bridge" feature, the General Key for that Entity will be set to "Receipt Number."*
- **Import Key-** sets the unique attribute marked for import of the host data file.
- **Monitor for Changes-** enables the attribute, and all related attributes, to be updated as part of the Data Sync process.

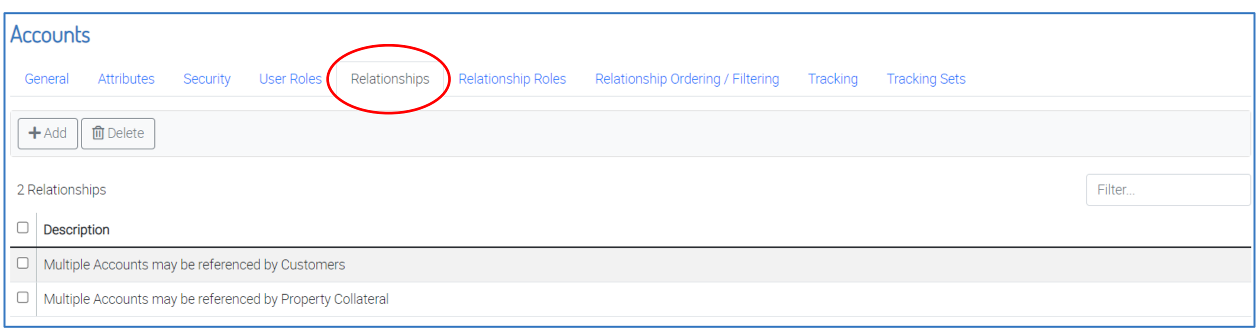
Under the ***Security*** tab, Users are granted Permissions for the items within the entity. For a description of each Permission, see [*Identifi User Permissions.*]



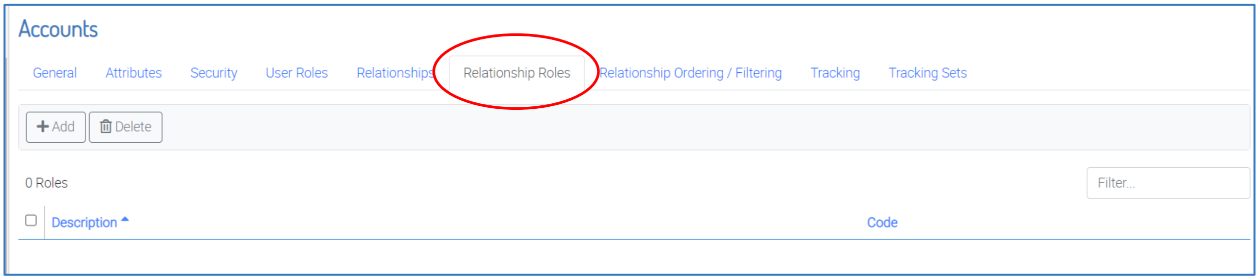
Under the ***User Roles*** tab, the User Roles associated with the Entity are listed. Additional User Roles can be added and existing roles deleted as well.

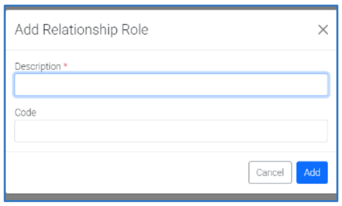
Under the ***Relationship*** T***abs***, users can manage the Entity's relationship with other entities on the installation, User Roles and how the Entity items are ordered/filtered.

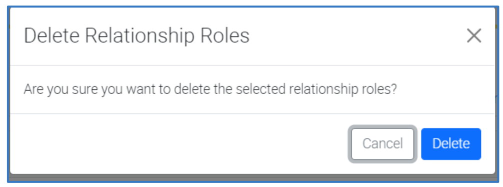
- Information from an entity item's related entities are displayed under the ***Relationships*** tab.



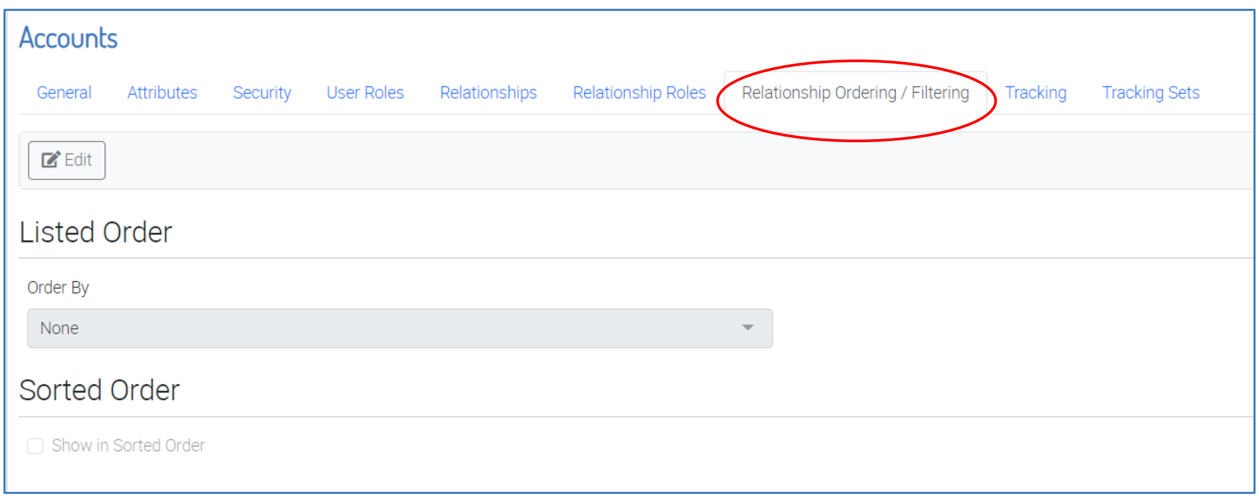
- Associated **Roles** and their descriptions are listed under the ***Relationship Roles*** tab. Additional Roles can be added and existing Roles deleted.

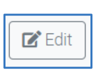


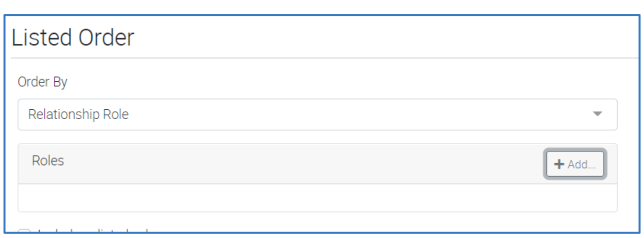


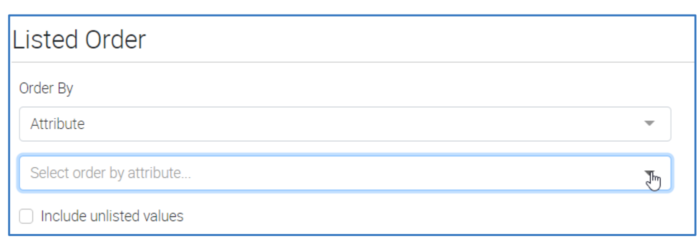


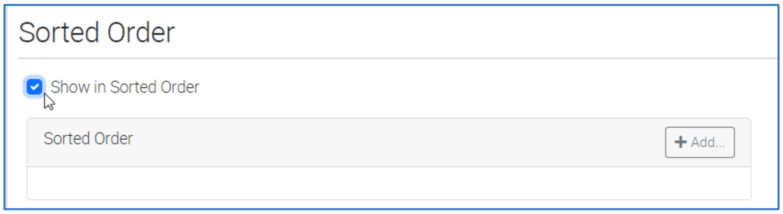
Relationship Ordering/Filtering settings determine what attributes are listed for the Related Entities and how they are ordered when viewing an entity item's details.



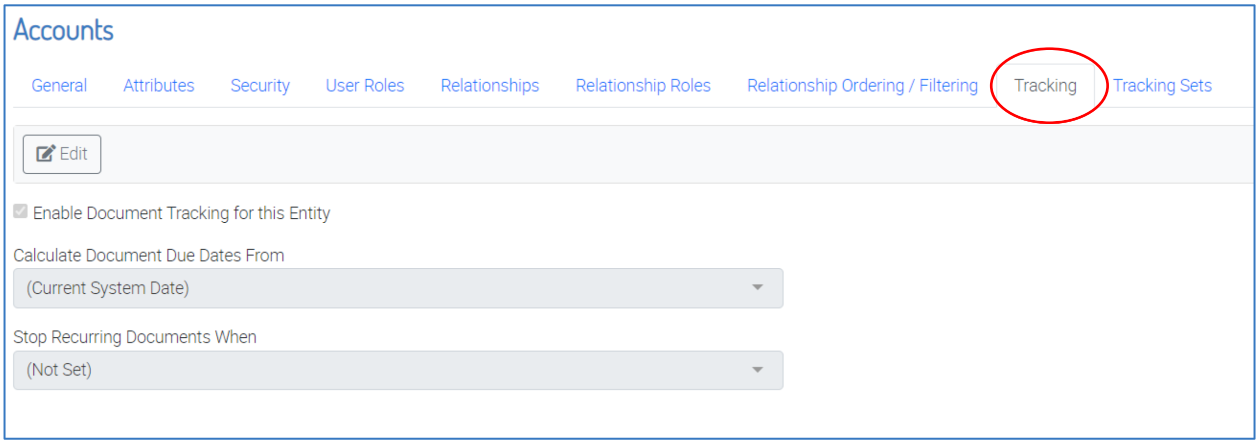
Select  to adjust the Listed Order by *Relationship Role* or *Attribute* and use a check mark to show in Sorted Order.



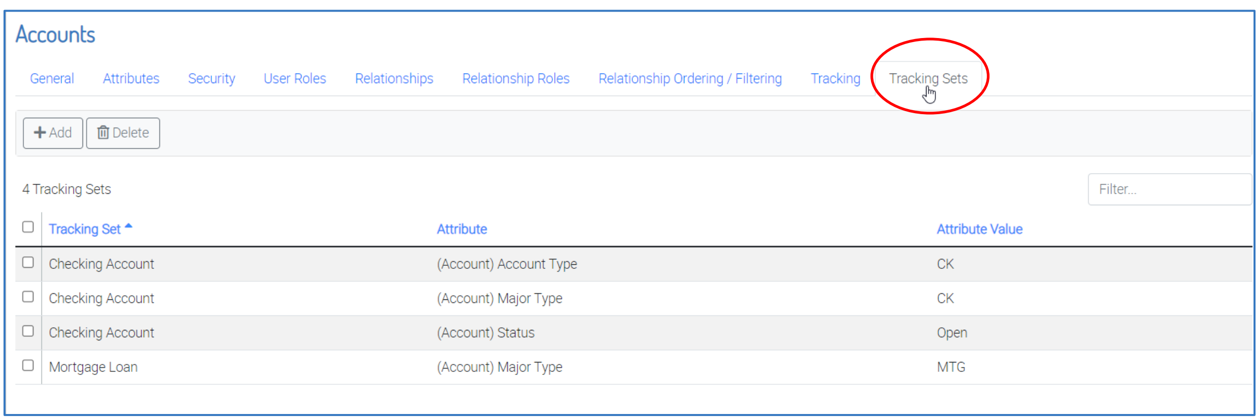


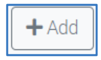


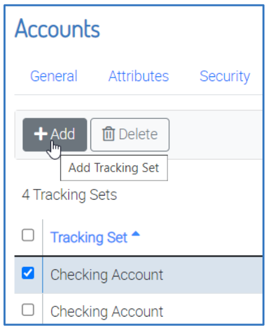
Under the ***Tracking*** tab, edit the data used for document tracking for the Entity by clicking

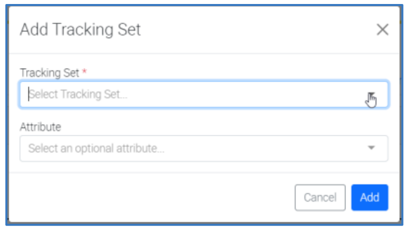


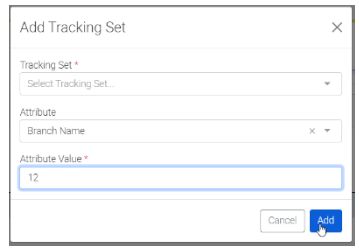
The ***Tracking sets*** tab displays sets being tracked.



To add additional Tracking Sets, click  and then select the **Tracking Set** (required); additionally, select an **Attribute** (optional) and enter an **Attribute Value** (required if Attribute is selected).



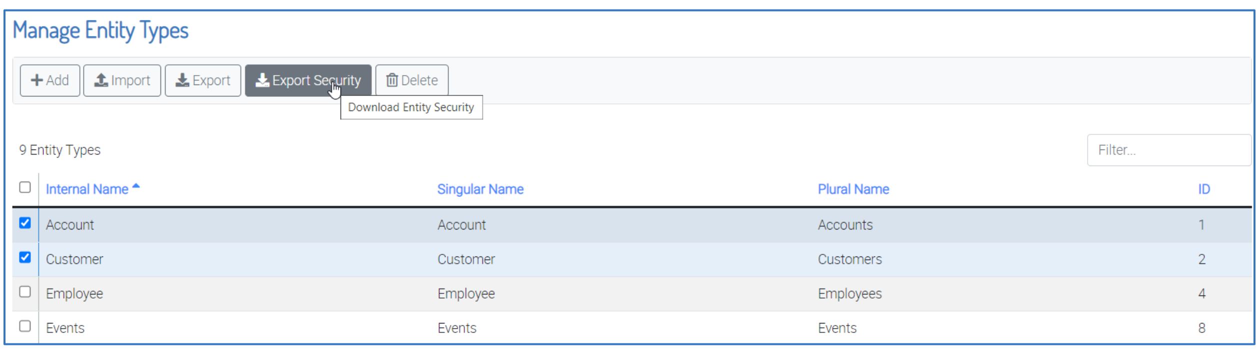




For details on the *Tracking* & *Tracking Sets* tabs: ***Document Tracking.***

Export Security for an Entity

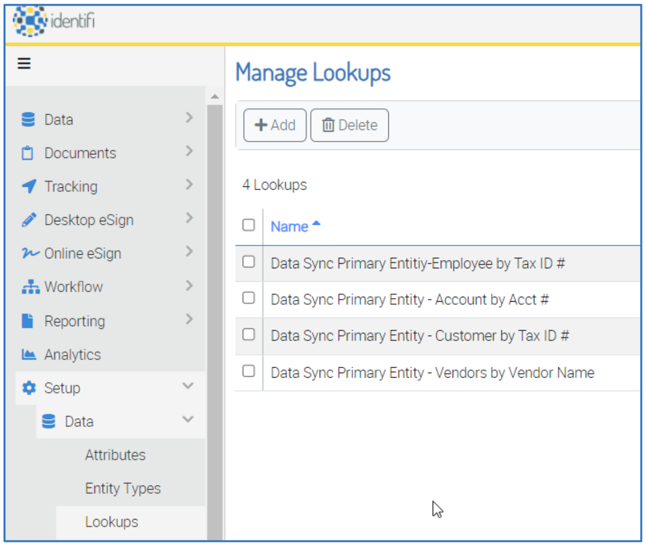
To export to Excel a list of all Users with access to Entities, select at least one Entity from the list and then click  .



The file will include Users, Groups and the specific Permissions granted to them for the Entity.

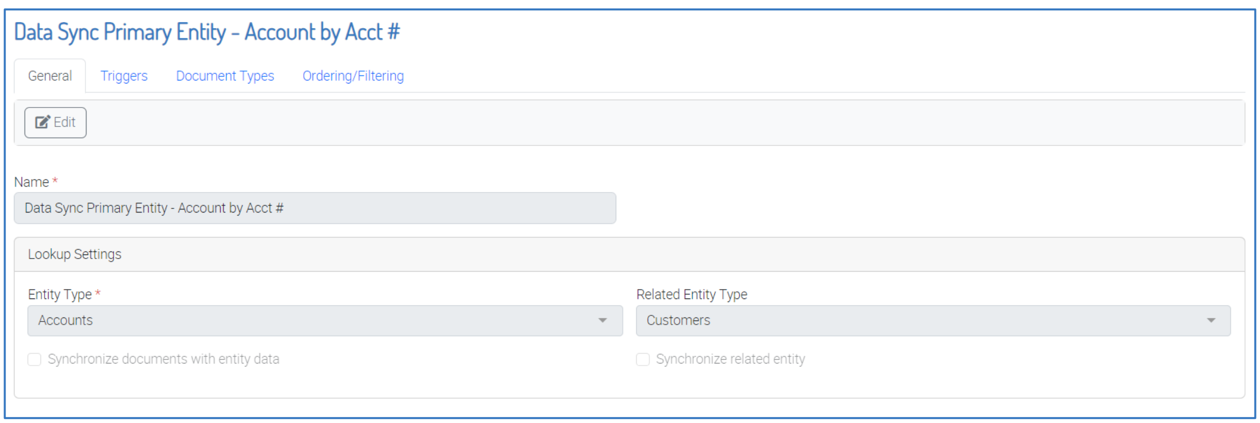
Setup – Data- Lookups

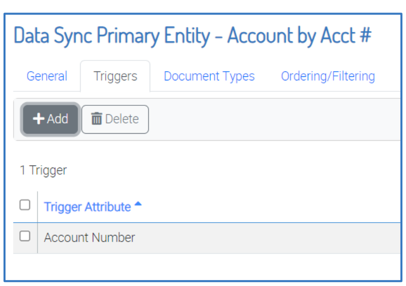
Allows Users to **Add**, **Delete** and **Modify** Document Type Lookups.

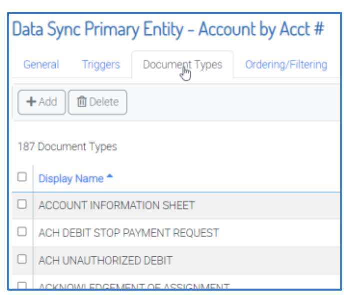


Lookups are associated with an Entity Type and can also be set to associate with that Entity Type's Related Entities.

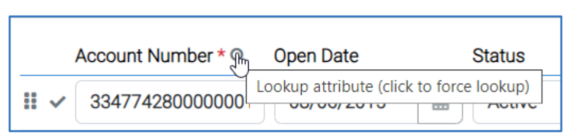
The **Lookup Settings** determine what type of data is updated on documents as host data changes.



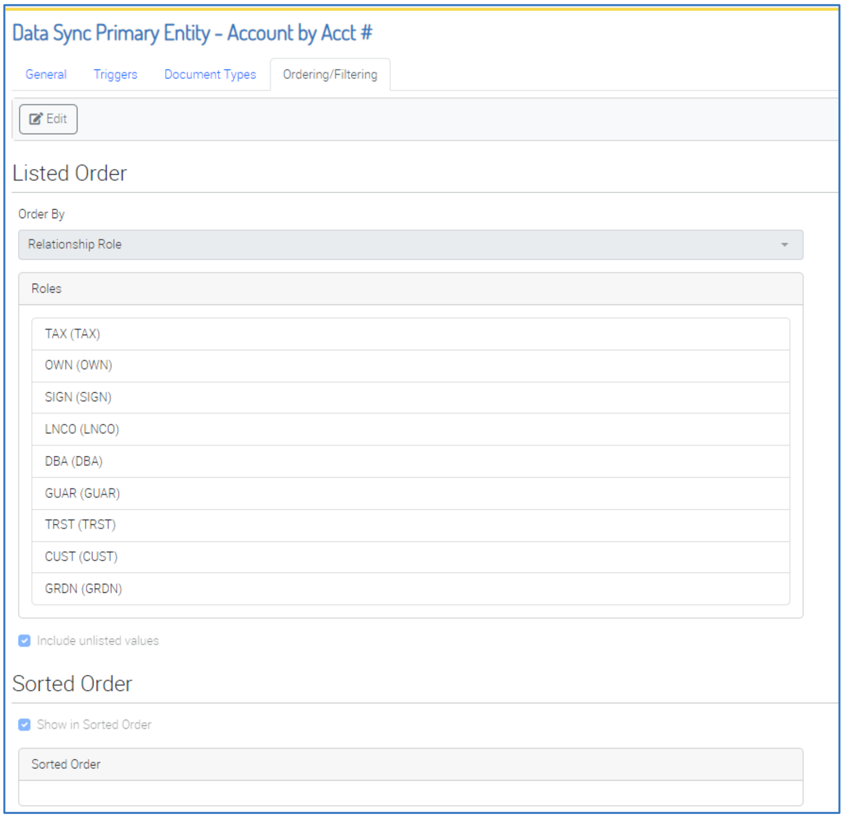




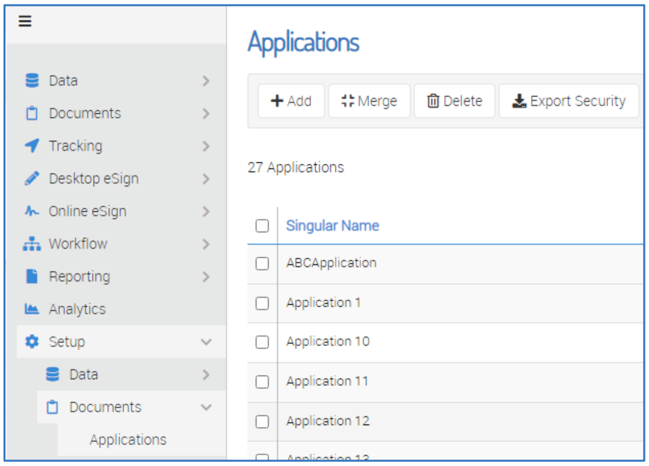
When assigned to a Document Type, the **Lookup Trigger** field is marked with a magnifying glass in the Indexing Panel, and associated fields are locked for editing.



The **Ordering/Filtering** tab is visible when the Lookup is enabled to synchronize related entity data. This allows the order and filter of the related entities that are returned and displayed as part of the lookup.



Setup- Documents-Applications



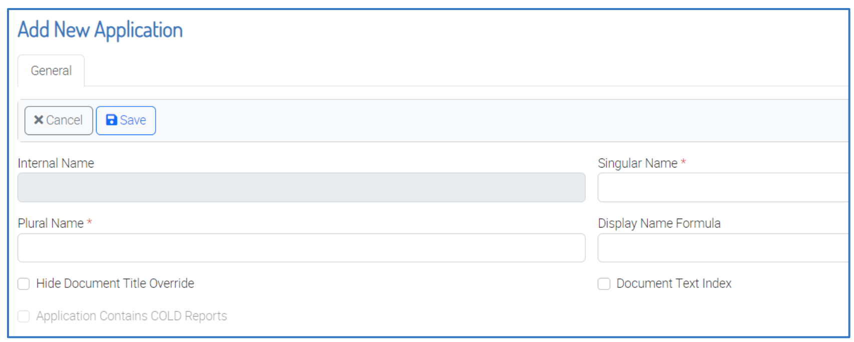
Allows Users to ***Add*** new Applications, as well as modify, ***Delete***, or ***Merge*** existing ones.

Adding an Application

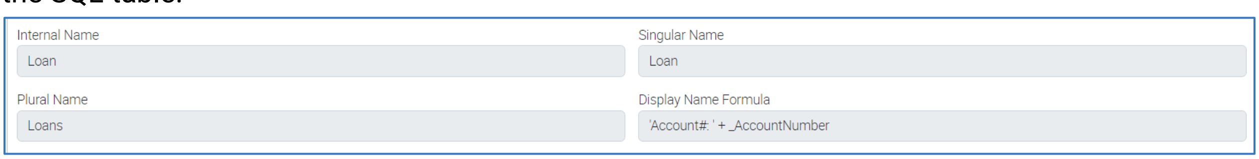
Select + Add from the top menu.

Enter the name of the new Application in the **Singular Name** field and the plural form of the name in **Plural Name**. If the Application will be document text indexed and/or will contain COLD Reports, select the appropriate check boxes.

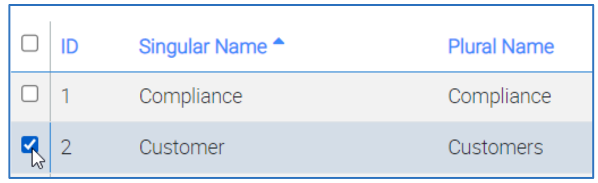
When finished, click Save.



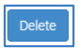
The **Internal Name** will be automatically created by the sytem and is the Application's name in the SQL table.

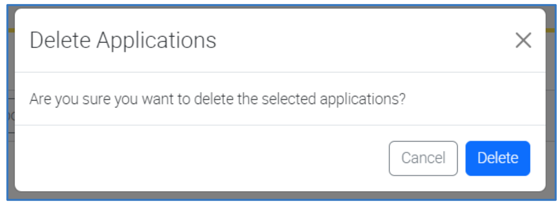


Deleting an Application

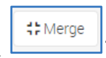


Place a checkmark next to the Application that will be removed, then select  from the top menu.

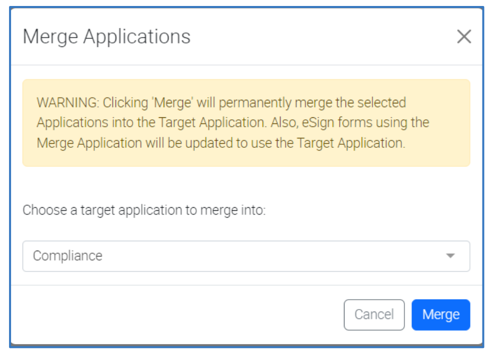
Then click  in the dialogue box.



Merging Applications

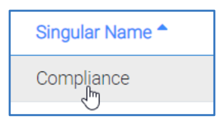
Place a checkmark next to the Application that will be 'absorbed', then click  from the top menu.

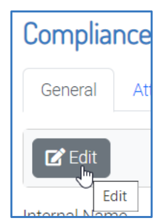
In the dialogue box, select the target Application from the dropdown menu and click  .

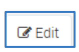


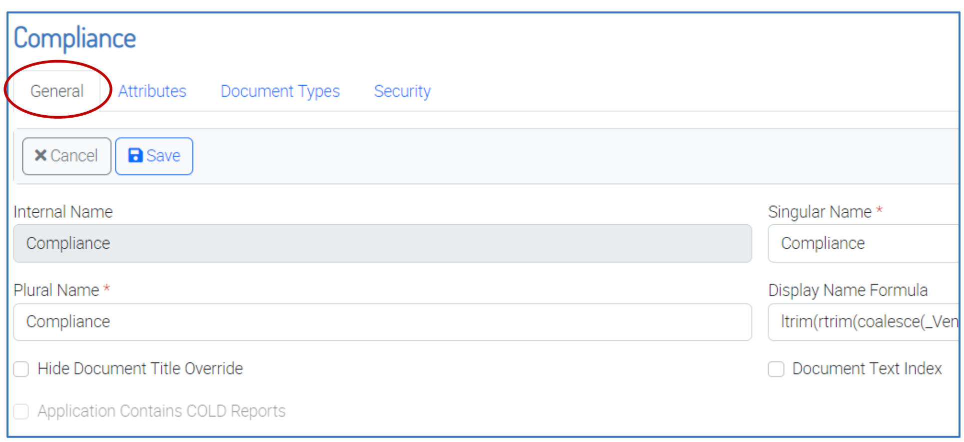
Modifying an Application

Open an Application's details by clicking its Name





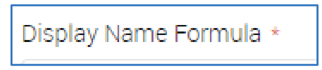
Under the ***General*** tab, select  to open the fields and make changes.



Click  when finished.

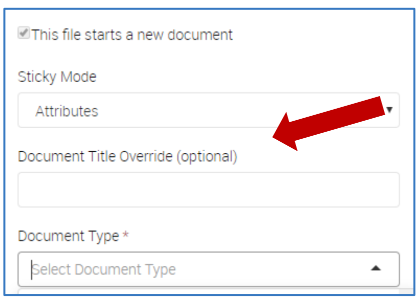
The **Singular** and **Plural Names** can be edited here, however the **Internal Name** is created by the sytem when the Application is intially created and cannot be modified. It is the Application’s name in the SQL table.

Display Name Formula: Determines how documents stored in this Application will be titled. It is a SQL formula made up of a document type and other attributes associated with the application.



Best Practice: *Copy the Display Name Formula from another Application and replace the attributes as needed, being sure to leave all other characters and spaces intact.*

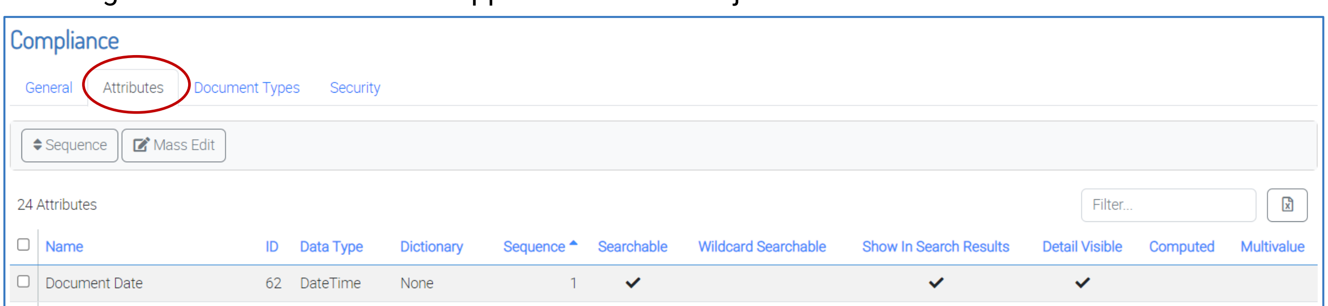
Example: *ltrim(rtrim(coalesce(**_VendorName**,'') +' '+ **DocumentTypeDisplayName** + ' ' + coalesce(convert(varchar, **_DocumentDate**, 111),'') + '-' + coalesce(convert(varchar, **_ExpirationDate**, 111),'No Exp.')))*



Hide Document Title Override: Checking this box hides the Document Title Override field from appearing in the indexing panel for documents stored in the Application. Anything entered in the Document Title Override field replaces the automatic titling of the document based on the Application’s Display Name Formula.

Under the ***Attributes*** tab, the list of attributes associated with the Application is presented. This list is populated based on the attributes on the Document Types that make up the Application.

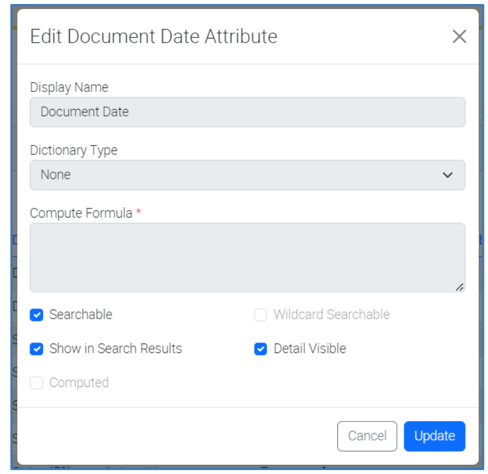
Settings for attributes within the Application can be adjusted here:



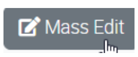
As Document Types are added, their Attributes are added to the Application. Likewise, when a Document Type is removed, its unique Attributes are removed from the Application.

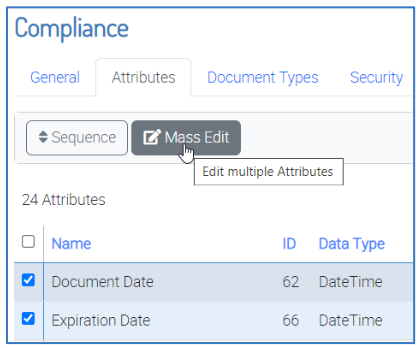
- **Data Type**- displays the Data Type of the attribute, not typically modified here.
- **Dictionary**- displays whether the attribute has a dictionary value (drop-down menu for the attribute during batch indexing and on the indexing panel.)

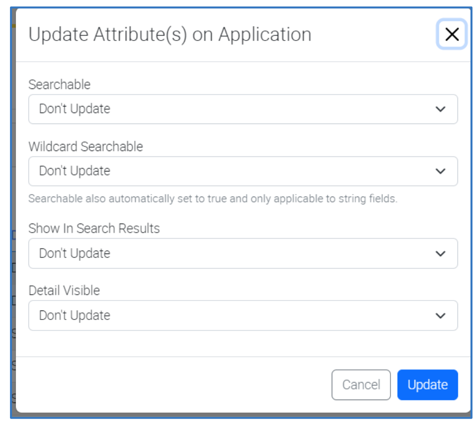
- **Sequence**- designates the position of the attribute on the *Indexing Panel* of a document stored in the Application. Attributes can be reordered here.
- **Searchable**- enables the attribute to be searchable through Document Search.
- **Wildcard Searchable**- enables the attribute to be searchable by entering a partial term with an asterisk.
- **Show in Search Results**- enables the attribute to show as a column in Document Search.
- **Detail Visible**- enables the attribute to be shown on the *Indexing Panel* of a document stored in the Application.
- **Computed**- indicates if an attribute has a computed formula associated with it. This field cannot be changed without adding or removing a computed formula from the attribute.
- **Multi Value-** indicates if an attribute is part of a multi value group, not typically modified here



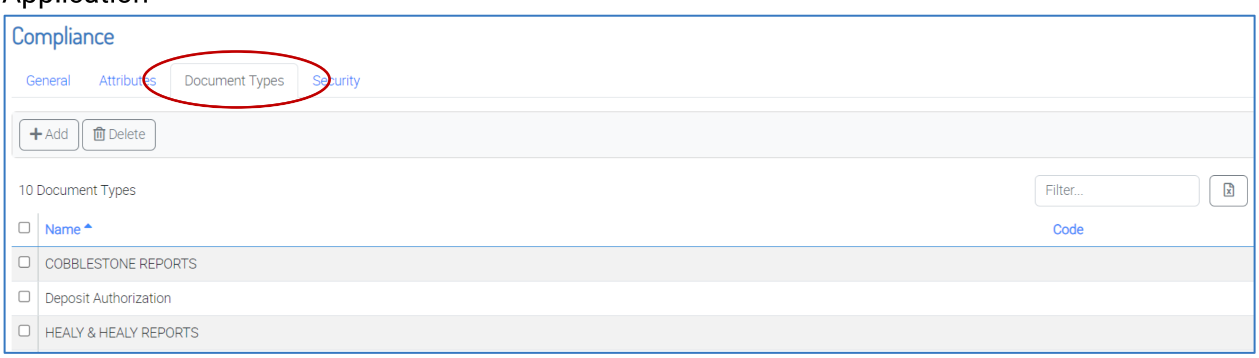
Changes can be made to multiple Attributes within an Application by selecting the Attributes and selecting



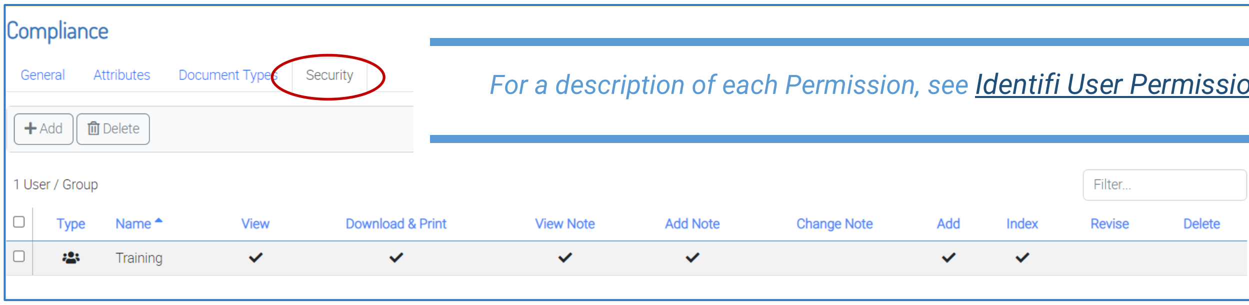




Under the ***Document Types*** tab, Document Types can be **added** to, or **deleted** from the Application



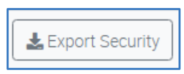
Under the ***Security*** tab, Users are granted Permissions for the Document Types within the Application. The permissions applied here extend to all documents stored in the Application, unless there is security set at the Doc Type or Attribute level.



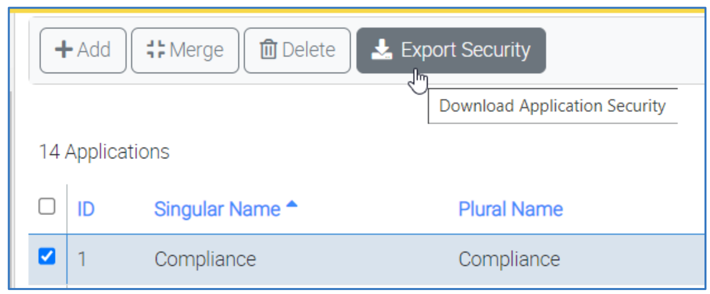
For a description of each Permission, see [Identifi User Permissions]

Export Security for an Application

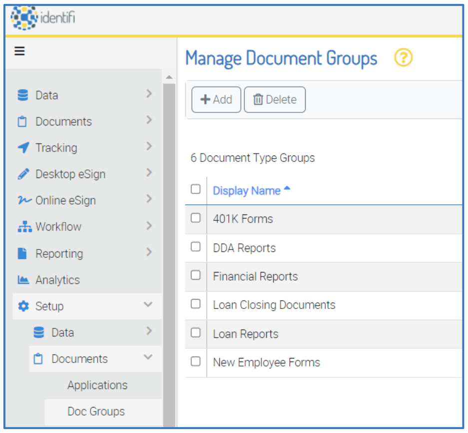
To export to Excel a list of all Users with access to Applications, select at least one Application from the list and then click “Export Security.”



The file will include Users, Groups and the specific Permissions granted to them for the Application.

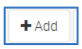


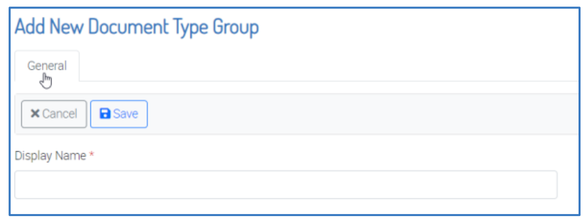
Setup-Documents-Doc Groups



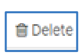
Allows Users to ***Add*** new Document Groups, as well as modify or ***Delete*** existing groups

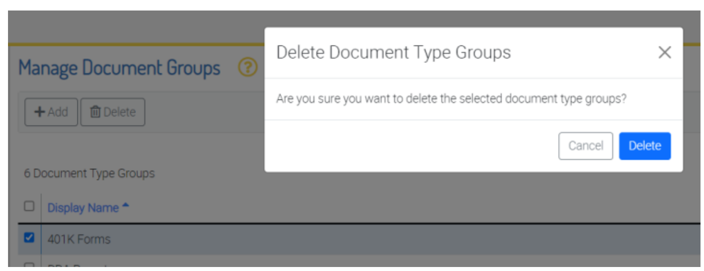
Adding a Document Group

Select  from the top menu. Enter a Display Name for the group and click **Save.** Once saved, Document Types can be added to the group under the ***Document Types*** tab (see *Modifying Document Groups* below).



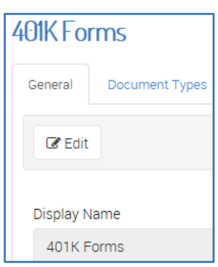
Deleting a Document Group

Place a checkmark next to the Document Group to be removed, then select  from the top menu.



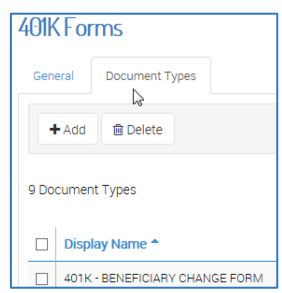
Modifying a Document Group

Open a Document Group's details by clicking its Display Name.

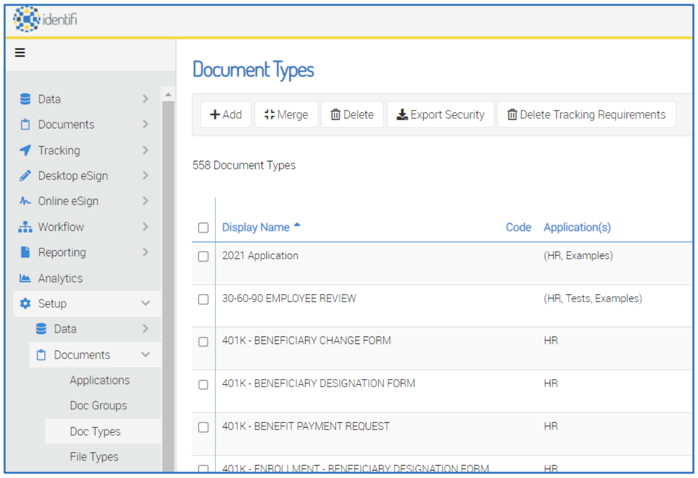


Under the ***General*** tab, the Display Name can be edited.

Under the ***Document Types*** tab, users can ***Add*** or ***Delete*** Document Types.

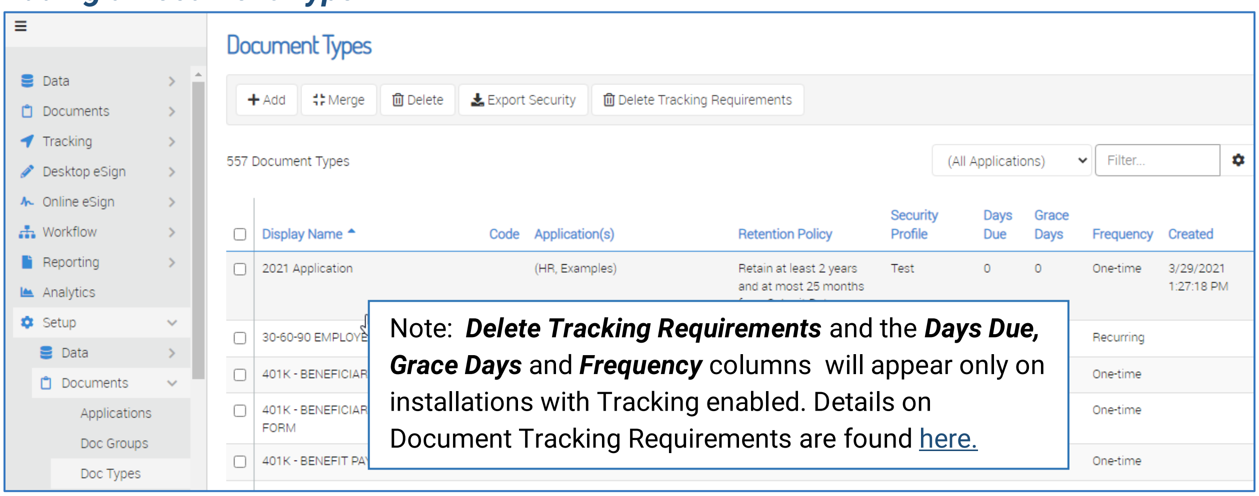


Setup-Documents-Doc Types

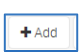


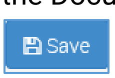
Allows Users to ***Add*** new Document Types, as well as modify, ***Delete***, or ***Merge*** existing ones.

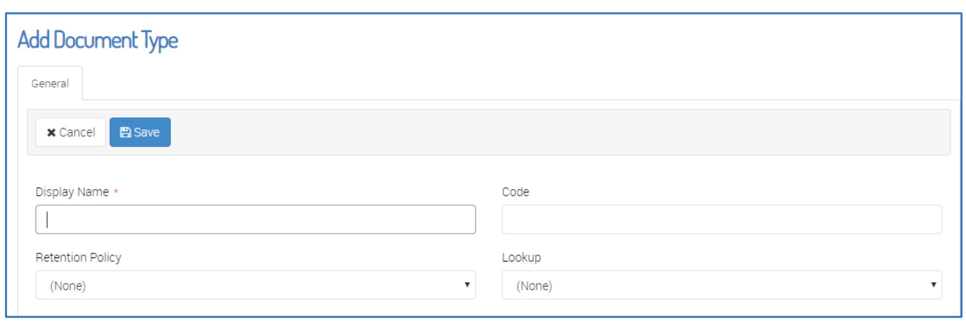
Adding a Document Type



Note: ***Delete Tracking Requirements*** and the ***Days Due, Grace Days*** and ***Frequency*** columns will appear only on installations with Tracking enabled. Details on Document Tracking Requirements are found [here.]

Select  from the top menu.

Enter the Display Name of the Document Type and click .

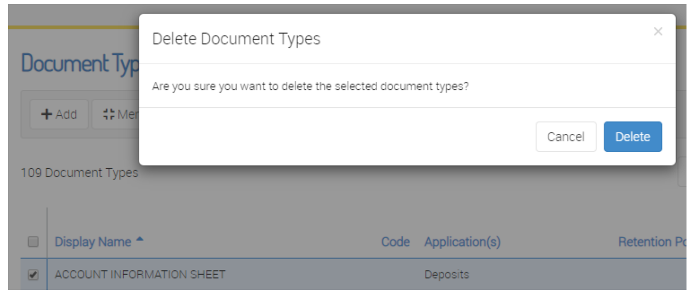


Once saved, attributes and security can be added to the document type. Additionally, the document type can be added to Applications and Document Groups. See *Modifying Document Types* below. ***Note:*** *For a shortcut, see* ***[Cloning a Document Type]***.

Deleting a Document Type

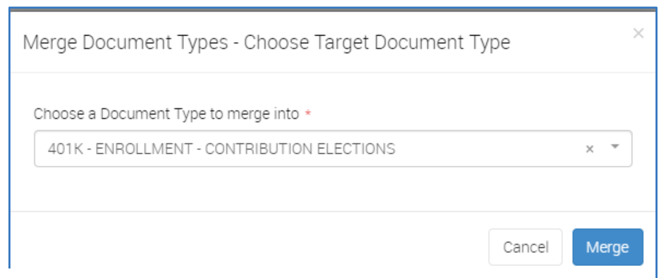
Place a checkmark next to the Document Type to be removed, then select Delete from the top menu.

If documents are currently stored as the Document Type, the system will not allow it to be deleted.



Merging Document Types

Place a checkmark next to the Document Type that will be 'absorbed', then click Merge in the top menu. In the dialogue box, select the target Application from the dropdown menu and click Merge .



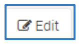
Note: *This process does not move the Document Type into the target Document Type's Application.*

Example: Document Type **Authorization Form**, found in the Customer Application, is merged with the Document Type **Consent Form**, found in the HR Application. The result is one Document Type called **Consent Form**, found in both the Customer and HR Applications.

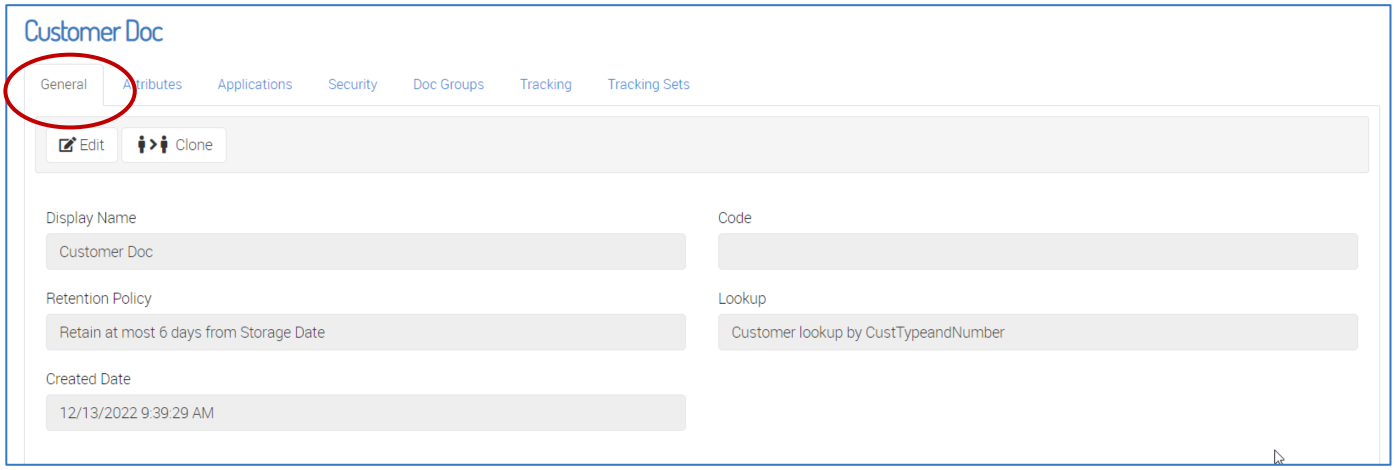
☐		Title ▲	Application	Document Type
☐	ℹ	111111111 John Doe Consent Form 2017/09/12	HR	Consent Form
☐	ℹ	222222222 Jane Doe Consent Form 2017/09/12	Customers	Consent Form

Modifying a Document Type

Open a Document Type's details by clicking its Display Name.

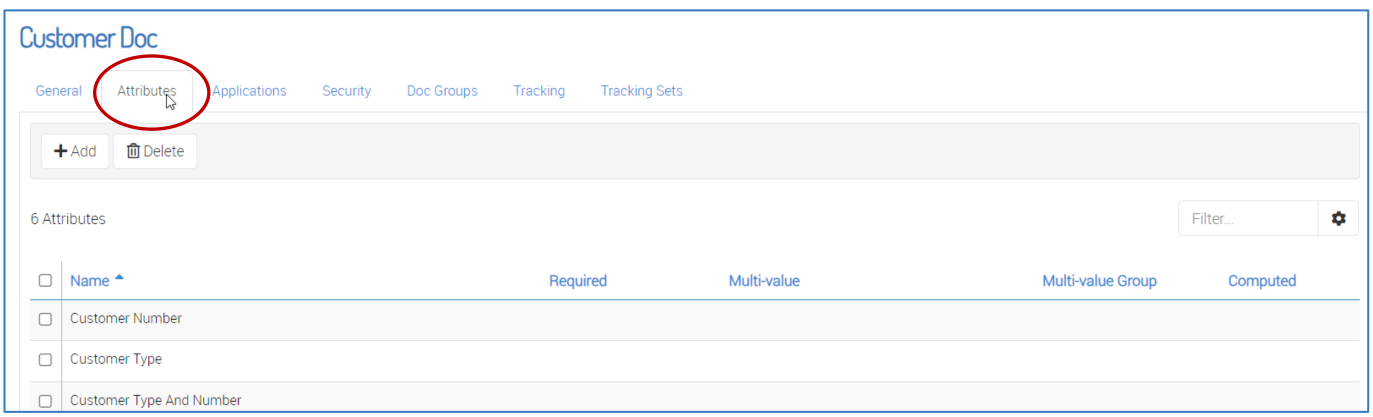
Under the ***General*** tab, select 

to open the fields and make changes.



Note: *See* ***[Cloning a Document Type]*** for details on that process.

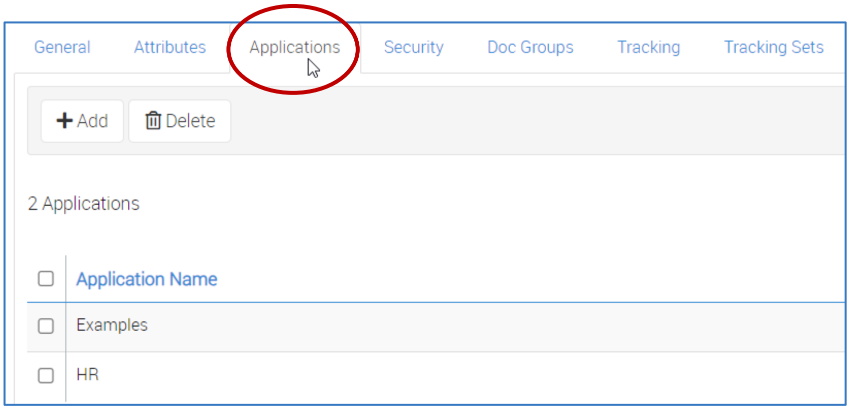
Under the ***Attributes*** tab, the list of attributes on the Document Type is presented. Users can ***Add*** and ***Delete*** attributes here.



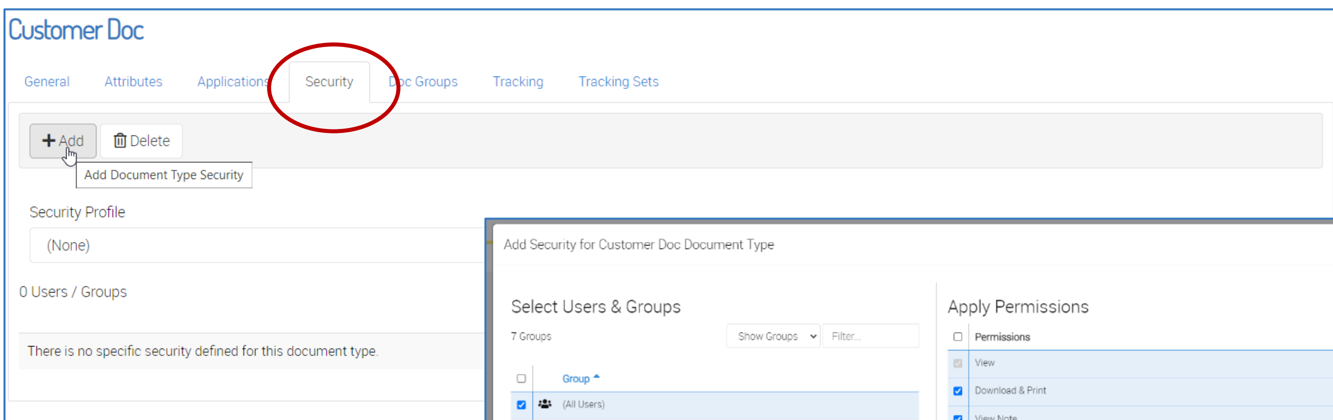
Settings for attributes within the Application can be adjusted here:

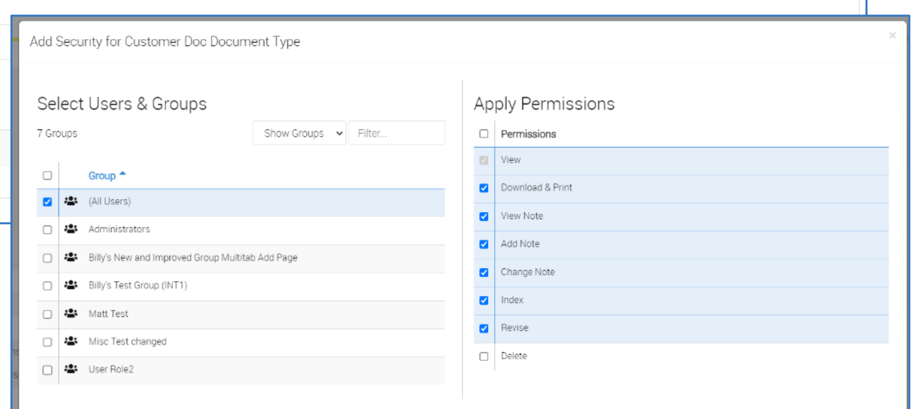
- **Required-** designates the attribute as required for indexing.
- **Multi Value-** indicates if an attribute is part of a multi value group
- **Multi Value Group-** indicates the multi value group the attribute belongs to
- **Computed**- indicates if an attribute has a computed formula associated with it

Under the ***Applications*** tab, Document Types can be **added** to, or **deleted** from Applications.



Under the ***Security*** tab, Users are granted Permissions for the document images stored as the Document Types. Without specific security set here, the documents are accessible based on the Doc Type's Application security settings.



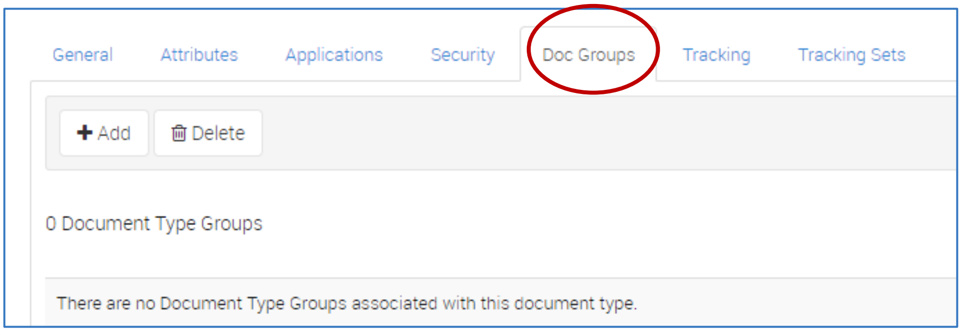


For a description of each Permission, see *[Identifi User Permissions.]*

Security Profiles offer a way to set Document Type security for several Users/ Groups at once. See more [here.]

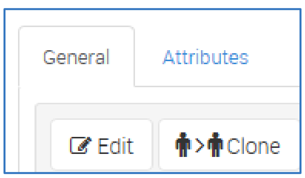
Note: *As security is placed on a document type granting a User/Group access, all others will be prevented from viewing documents stored as that Doc Type. Therefore, if Document Type Security is used, all users/groups that need to be able to access the doc type must be added here.*

Under the ***Document Groups*** tab, the list of document groups that the Document Type belongs to is presented. Users can ***Add*** the document type to groups here, as well as ***Delete*** them from groups.

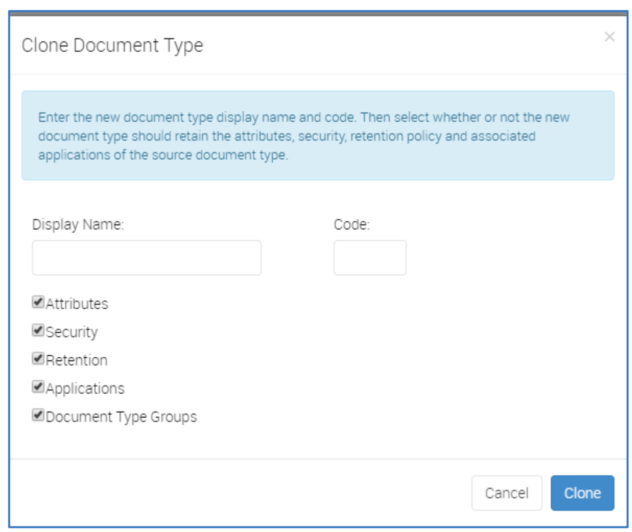


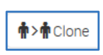
For details of the ***Tracking*** and ***Tracking Sets*** tabs, see here.

Cloning a Document Type



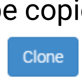
Document Cloning allows Users to quickly create a new Document Type, replicating the original document type's Application(s), Attributes, Retention, Security and Document Type Groups in a single step.



Under the ***General*** tab, select the  button.

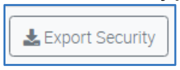
Enter a Display Name for the new document type and, optionally, a short-hand Code.

Click in the box for any of the settings that should *not* be copied on the new document type.

Click  and the new Doc Type will be saved.

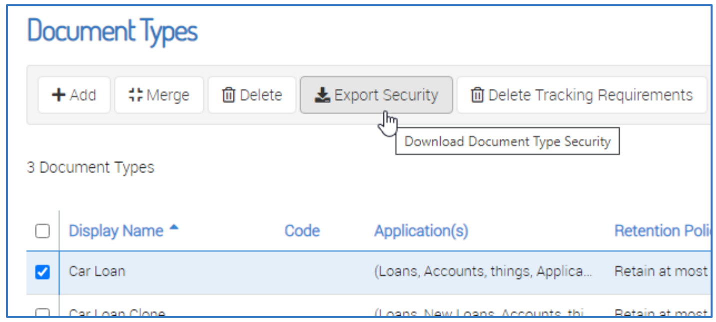
Export Security for Document Types

To export to Excel a list of all Users with access to Document Types, select at least one Document Type from the list and then click

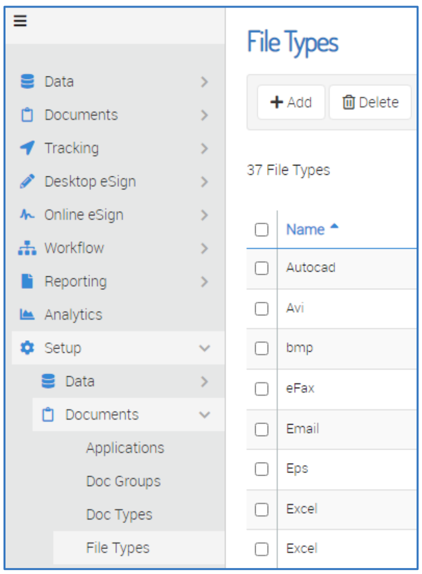


.

The file will include Users, Groups and the specific Permissions granted to them for the Document Type.

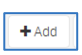


Setup - Documents-File Types

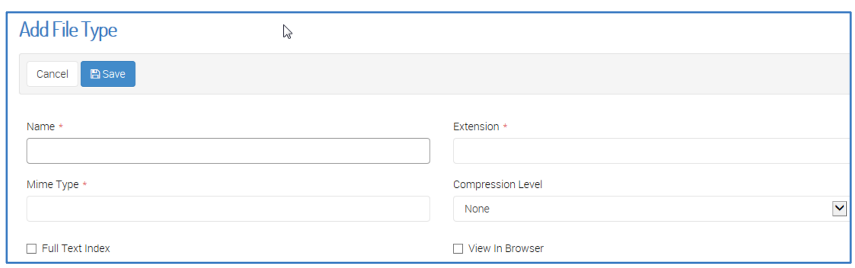


Many different types of files can be stored within Identifi and several are configured at the time of installation. In this menu, new file types can be added and existing ones can be deleted or modified.

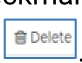
Adding a File Type

Click


and fill in the required fields to configure additional file types.

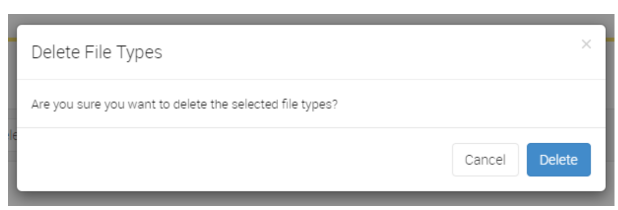


Deleting a File Type

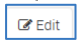
Place a checkmark next to the File Type to be removed, then select


.

If files are currently stored as the File Type, the system will not allow it to be deleted.

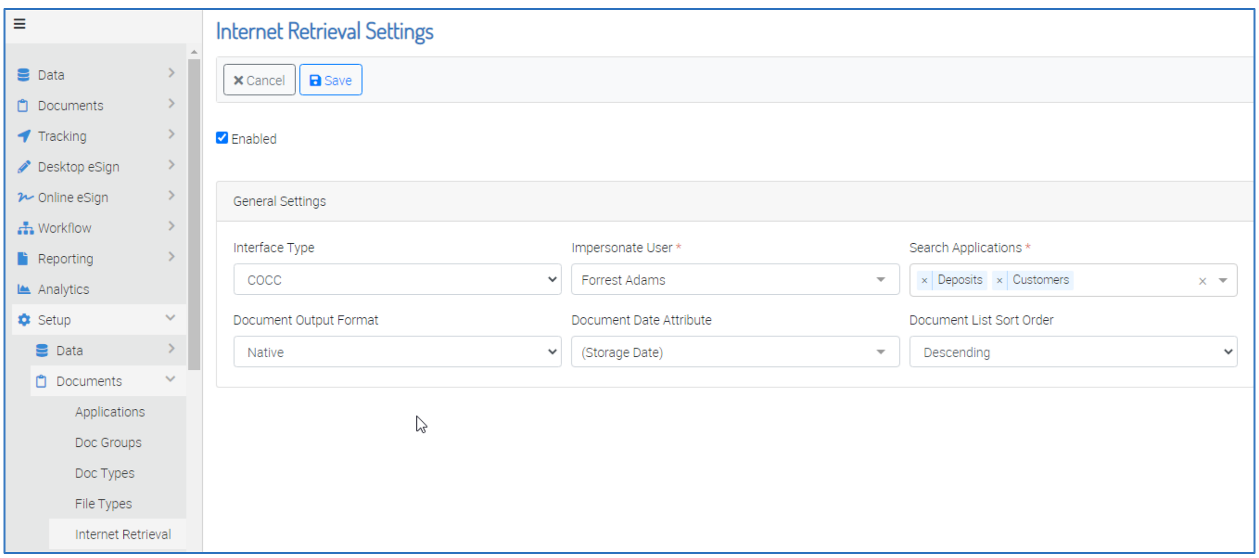


Modifying a File Type

Click the Name of the file type to open its configuration details. Select  to make changes and then click ***Save.***

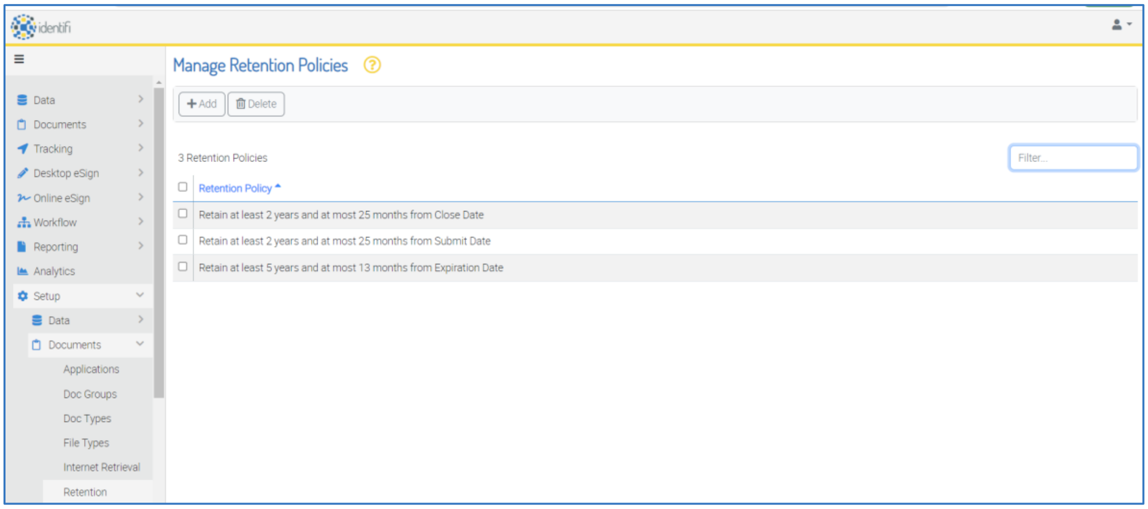
Setup-Documents-Internet Retrieval

When the Internet Retrieval product is licensed on the installation, the configuration settings are found under the ***Documents*** menu.



Setup-Documents-Retention

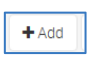
Retention Policies for documents stored within Identifi are created and managed here.



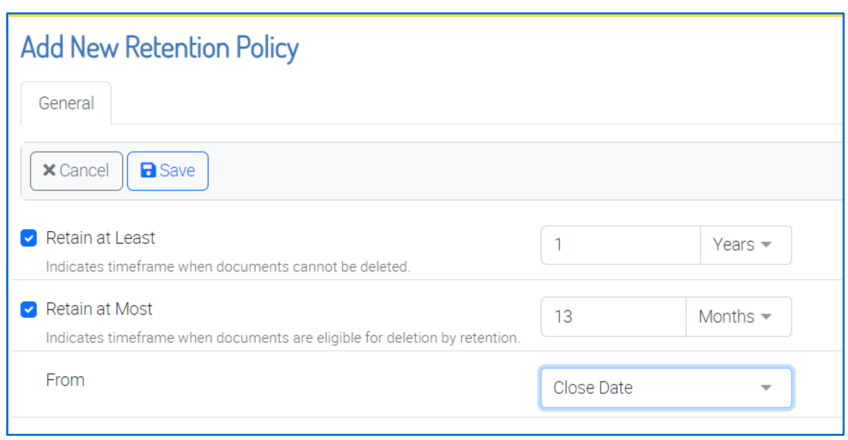
Policies can be applied to multiple Document Types; however, a Document Type can have only one Retention Policy associated with it.

Retention can be based on any date attribute (i.e. Document Date, Storage Date, Close Date, etc.) and set in **Days**, **Months**, or **Years.**

Creating a Retention Policy

Click  in the upper menu.

A policy can have two parameters, **At Least** and **At Most**, and it is a best practice to set both in order to prevent documents from being deleted in error.



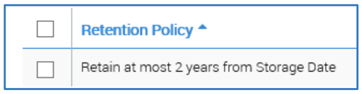
- ***Retain At Least*** determines time frame in which the documents cannot be deleted.

  **Note: a user with the Administrator Role is able to delete documents with an active Retention Policy.*

- ***Retain At Most*** will ensure the document is deleted with Retention Maintenance at the end of the period.

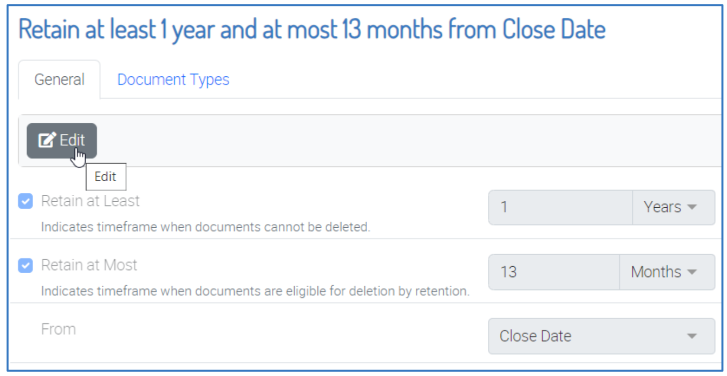
Note: *The policy above will prevent the documents from being deleted for one year from the Close Date and will allow the documents to be deleted with Retention Maintenance one year and one month after Close Date.*

Modifying a Retention Policy



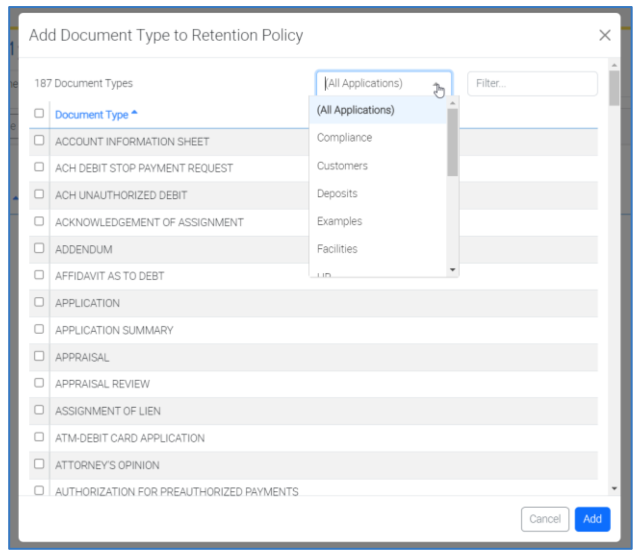
Click the title of a Retention Policy to see its details and make changes.

Under the ***General*** tab, click ***Edit*** to open the fields for changes.

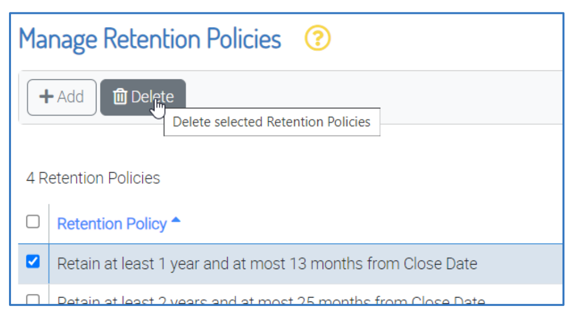


Under the **Document Types** tab, Document Types can be added to or removed from the Retention Policy.

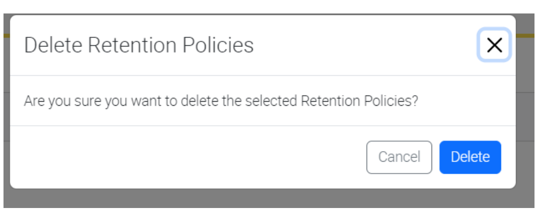
Use the drop-down box to select Document Types within a specific Application.



Deleting a Retention Policy



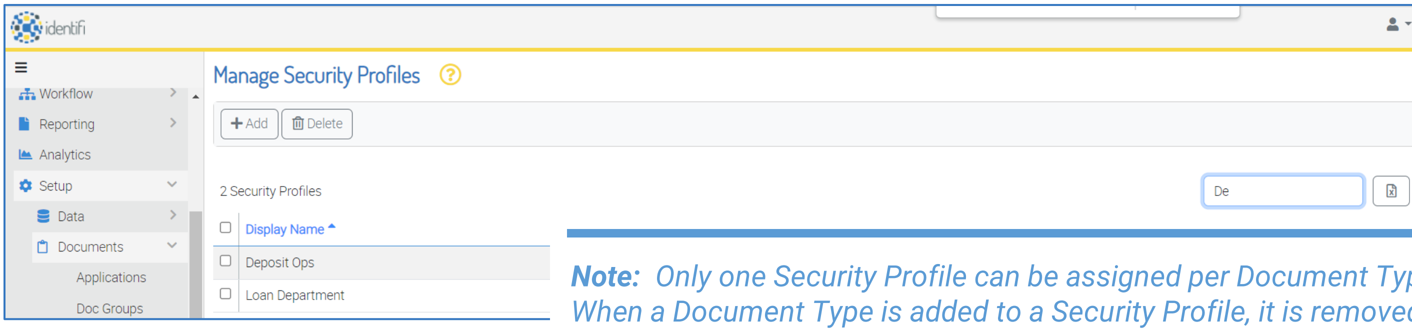
Place a checkmark next to the Retention Policy to be removed, then click Delete .



Setup-Documents-Security Profiles

Security Profiles allow for complex security to be applied to Document Types, based on Permissions and involving multiple Users/Groups, with just a couple of steps.

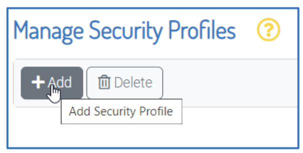
Administrators are able to **Add** new Security Profiles, as well as **Delete** or modify existing ones.



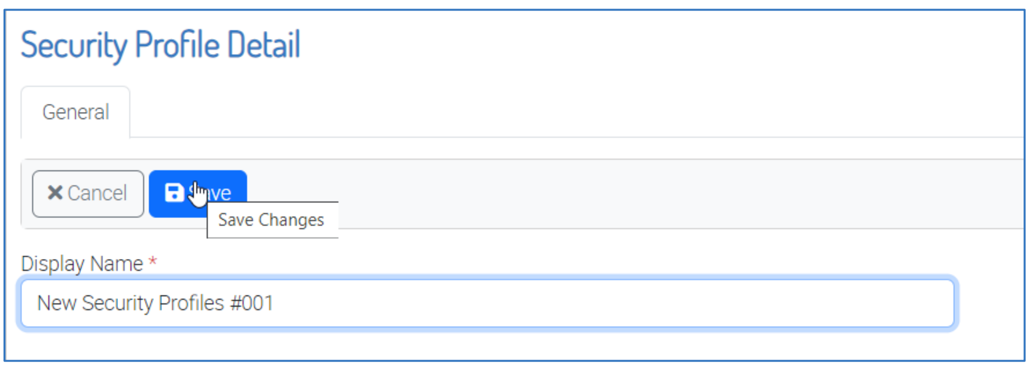
***Note:** Only one Security Profile can be assigned per Document Type. When a Document Type is added to a Security Profile, it is removed from any other Security Profiles*

Adding a Security Profile

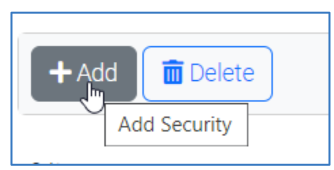
Click +Add in the upper menu.

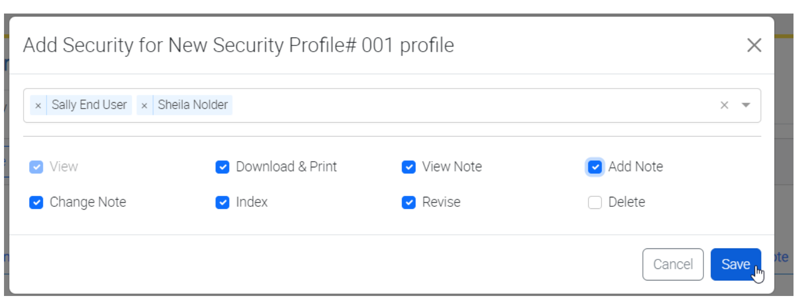


Enter a Display Name and select **Save.**

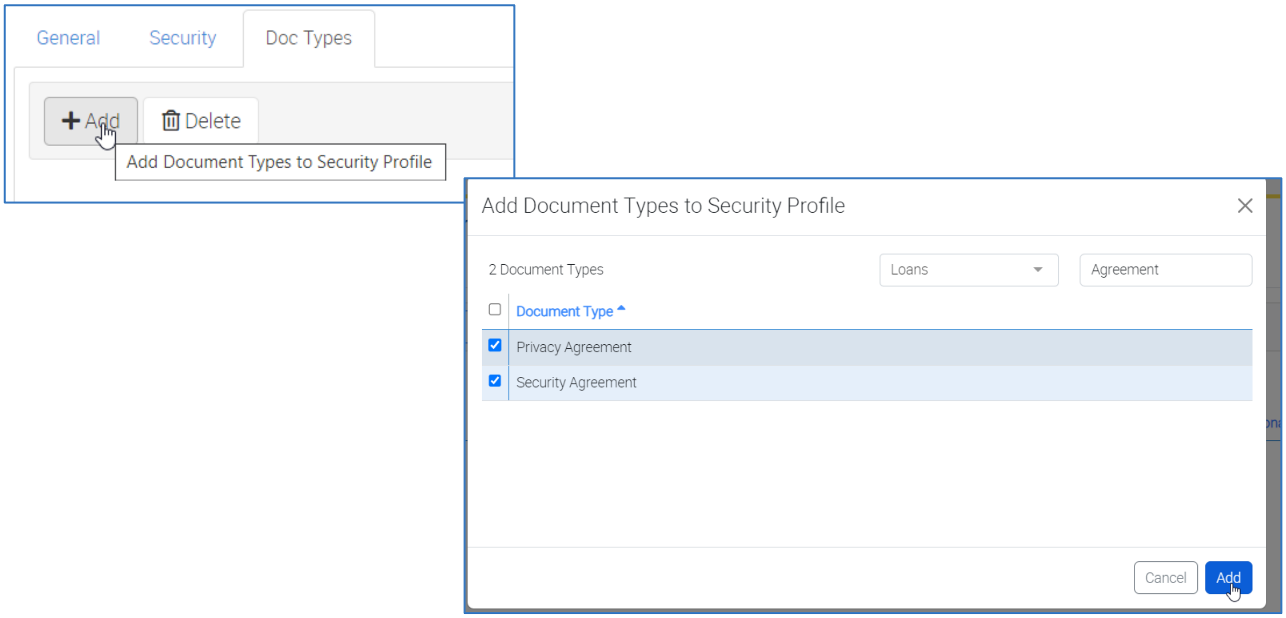


Under the ***Security*** tab, click **Add** to select Users/Groups and make the appropriate selections for their permissions to documents under this Security Profile. Click **Save.**

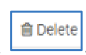


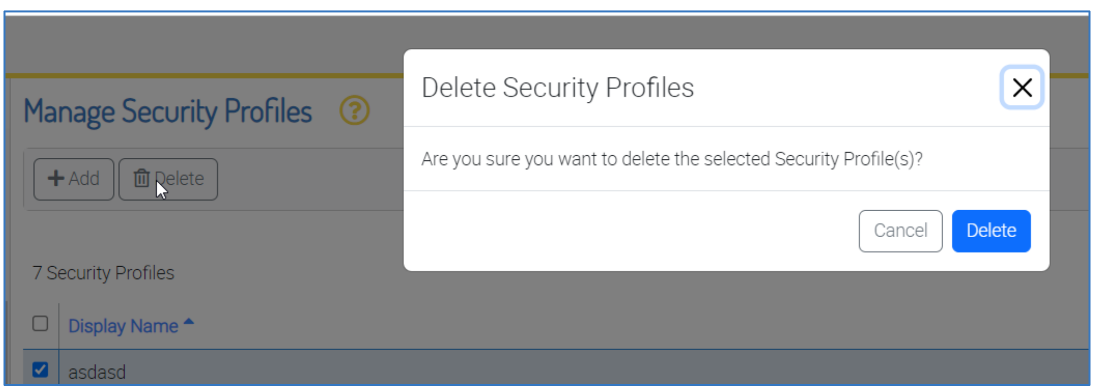


Under the ***Document Types*** tab, click **Add** to select the Document Types to which this Security Profile will be assigned.



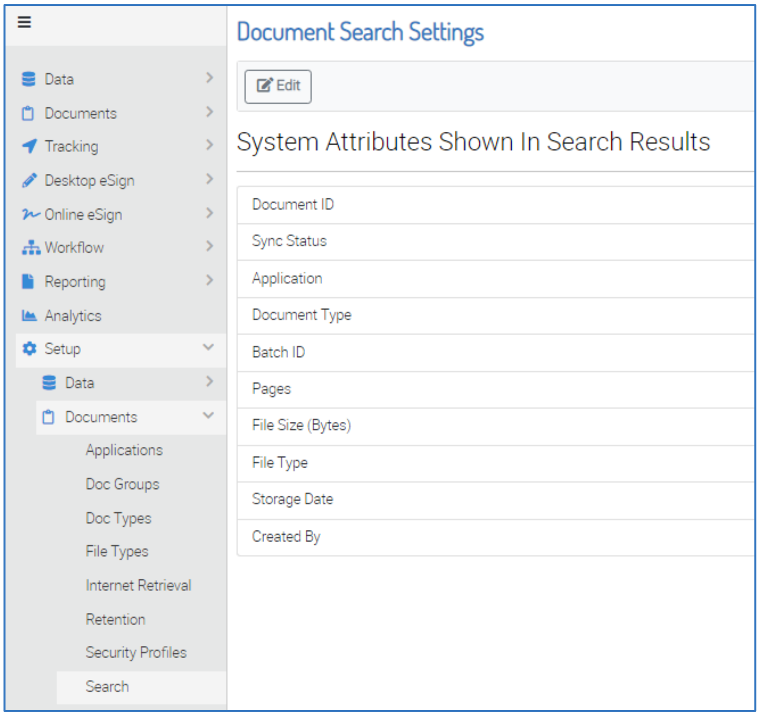
Deleting a Security Profile

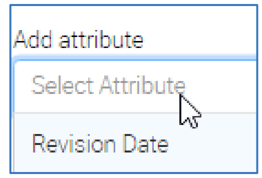
Place a checkmark next to the Security Profile to be removed, then click .



Setup-Documents-Search

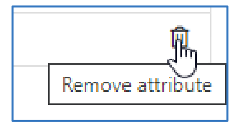
Determine what System Attributes are represented as columns in *Search Results*.

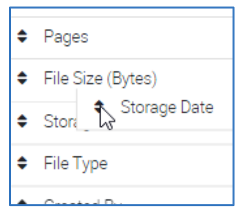




Clicking ***Edit*** allows users to add additional attributes to the list.

Selecting the *trashcan* icon to the far right of the attribute will remove it from the list.





Use the *arrows* icon to the left of the attribute to drag and drop to another location in the list.

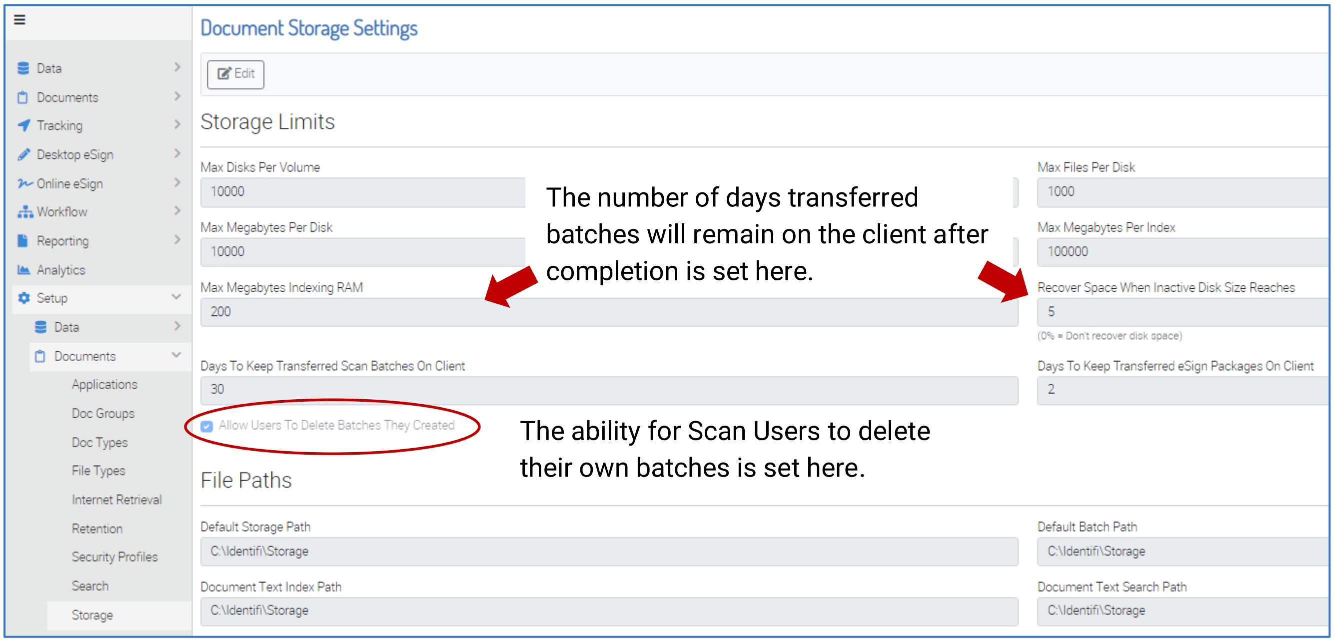
Top to bottom= left to right in ***Search Results***.

Setup-Documents-Storage

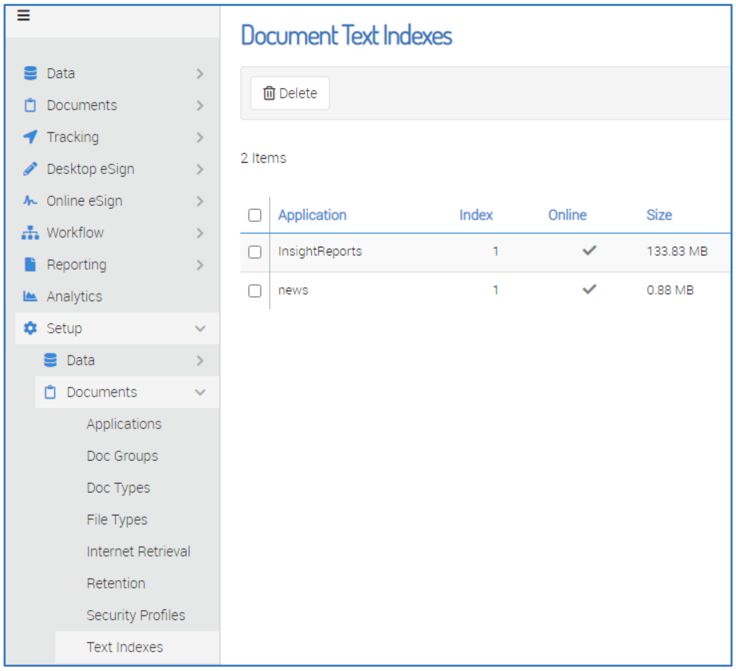
File paths and storage limits, can be viewed and adjusted here. Preferences related to batches are also set here.

Setup->Installation->*Document Storage*

Under the ***Document Storage*** tab, storage limits, file paths can be viewed and adjusted.



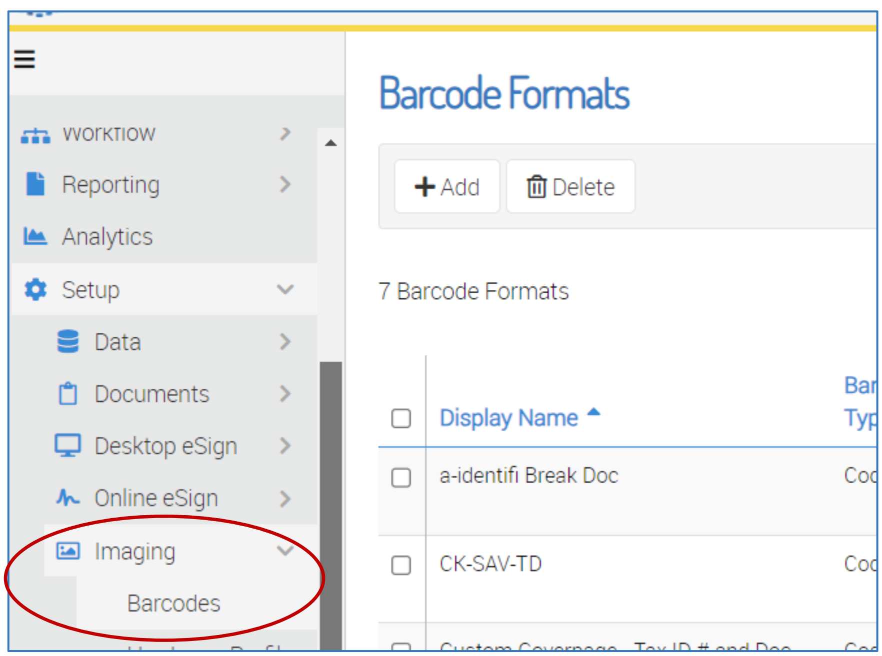
Setup-Documents-**Text Indexes**



The Text Indexes for any types of documents that are document text indexed in the installation.

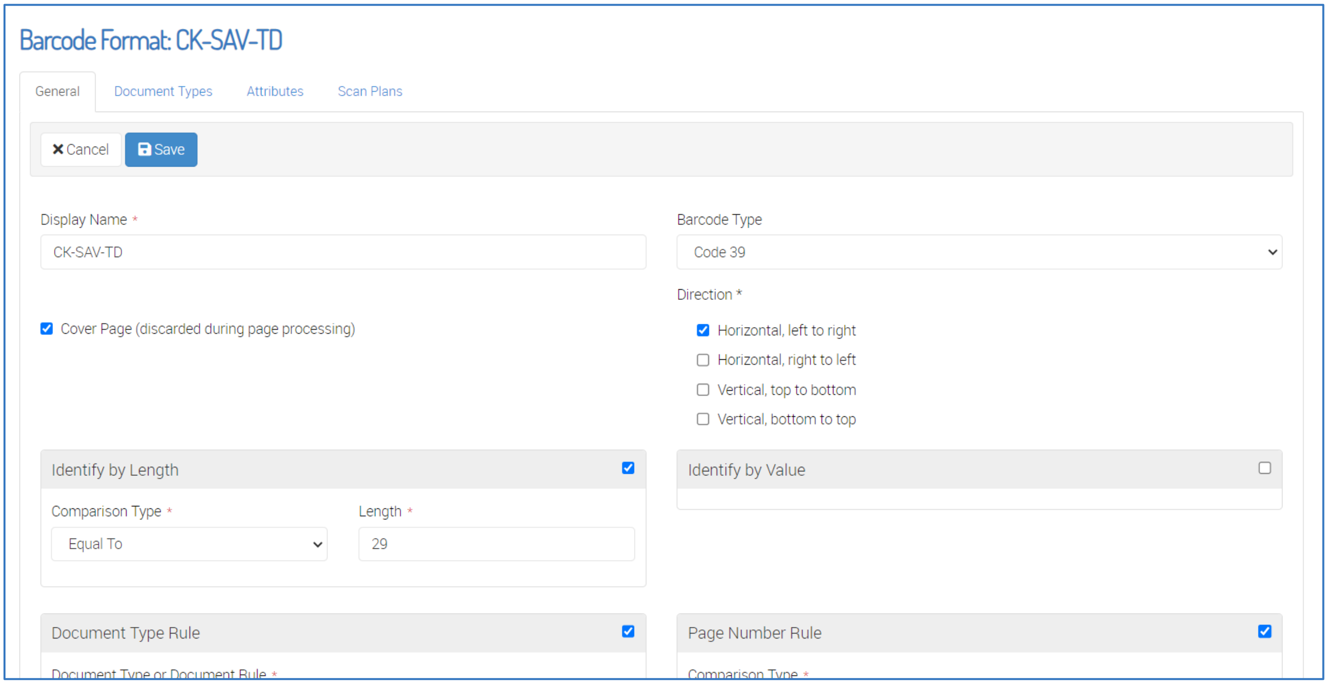
Setup-Imaging-Barcodes

Barcode Formats are managed from this menu. Users are able to add new barcode formats and delete or modify existing ones.



Adding a Barcode Format

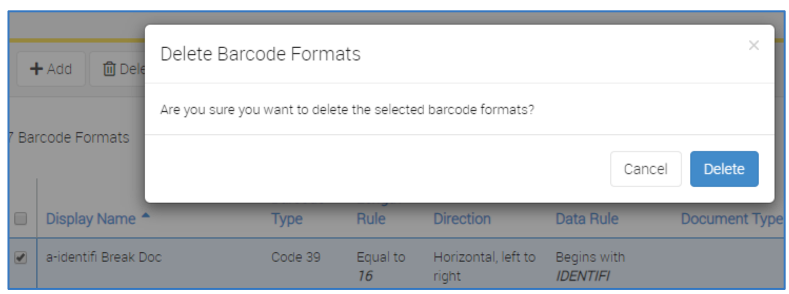
Click + Add and enter the appropriate information and select ***Save*** when finished.



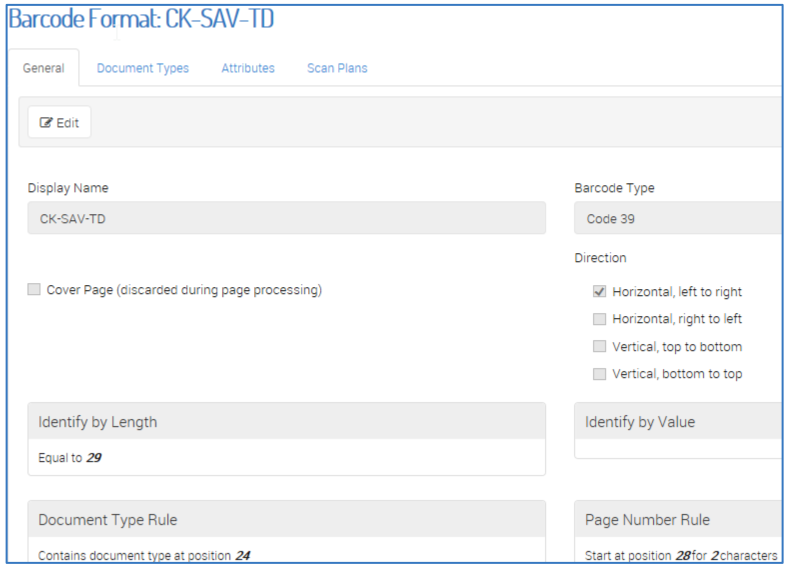
See *[Modifying a Barcode Format](#)* below for instructions to add Document Types, Attributes and Scan Plans to the Barcode Format just created.

Deleting a Barcode Format

Place a checkmark next to the Barcode Format to be removed, then select Delete.



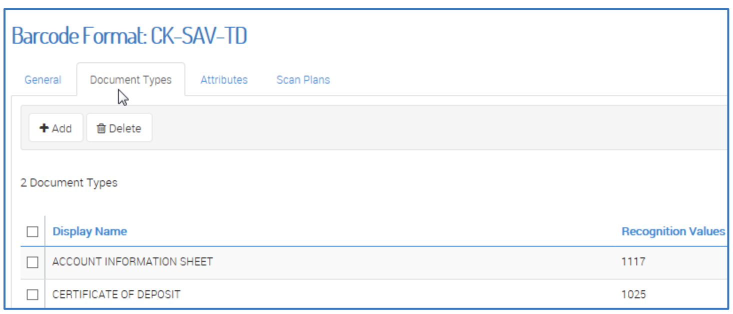
Modifying a Barcode Format



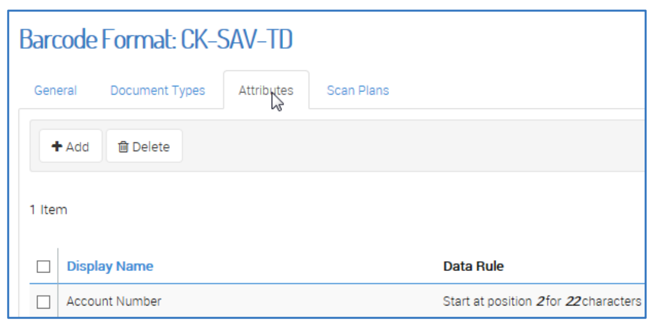
Click the Name of the Barcode Format to open its configuration details.

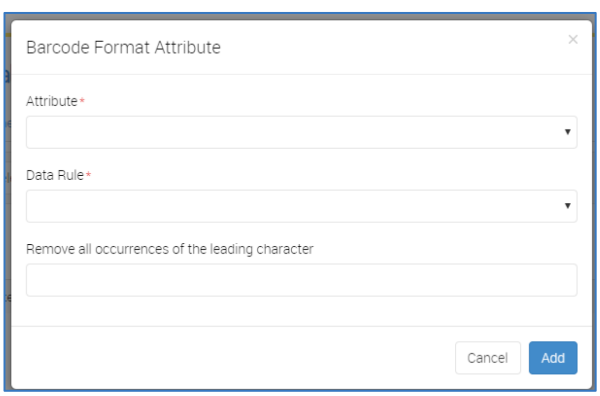
Under the ***General*** tab, select Edit to make changes and then click ***Save.***

Under the ***Document Types*** tab, Document Types can be **added** to or **deleted** from the Barcode Format.

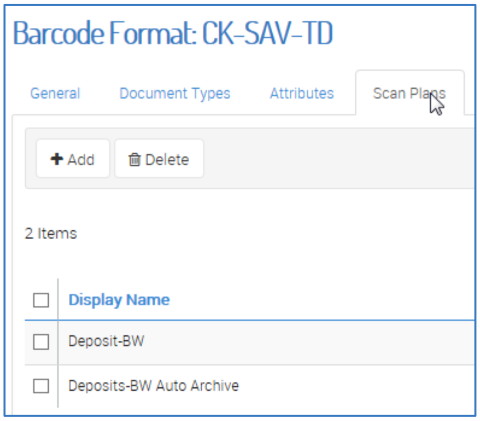


Under the ***Attributes*** tab, Attributes are **added** to or **deleted** from the Barcode Format.



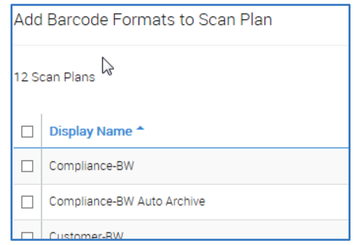


When adding an Attribute, select the Attribute from the drop-down menu. Then apply the appropriate Data Rule and indicate if any leading characters (such as zeros) should be removed.



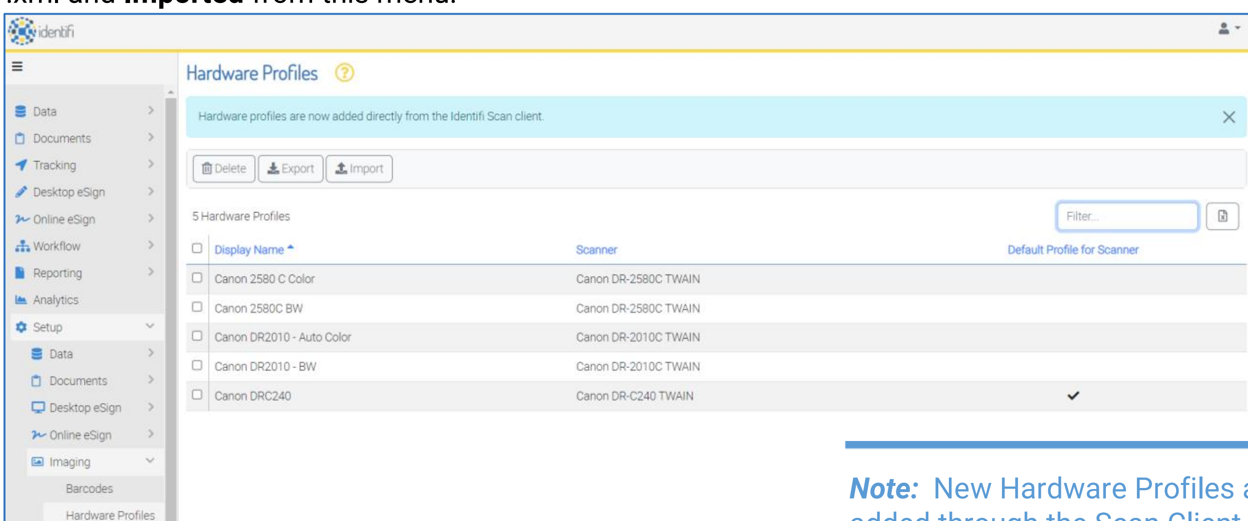
Under the ***Scan Plans*** tab, Scan Plans are **added** to or **deleted** from the Barcode Format.

When adding a Scan Plan, the list of all Scan Plans on the installation is presented and multiple scan plans can be selected at one time.

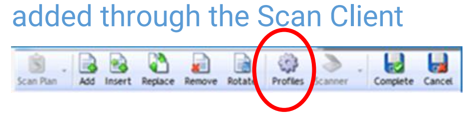


Setup-Imaging-Hardware Profiles

Allows Users to manage Hardware Profiles. Profiles can be modified, **Deleted**, **Exported** as an .xml and **Imported** from this menu.



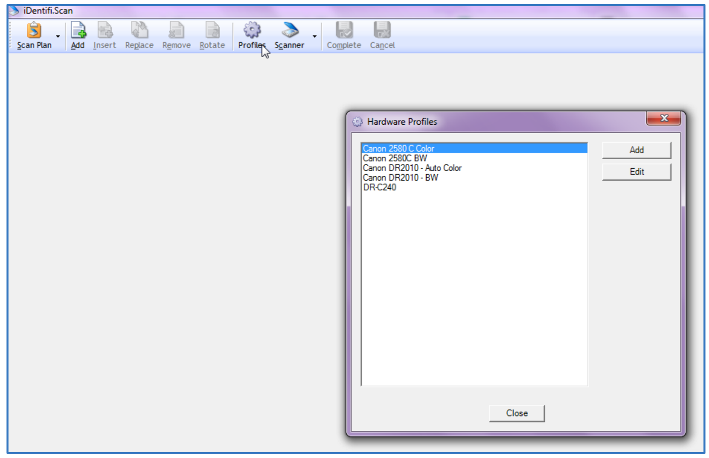
Note: New Hardware Profiles are added through the Scan Client

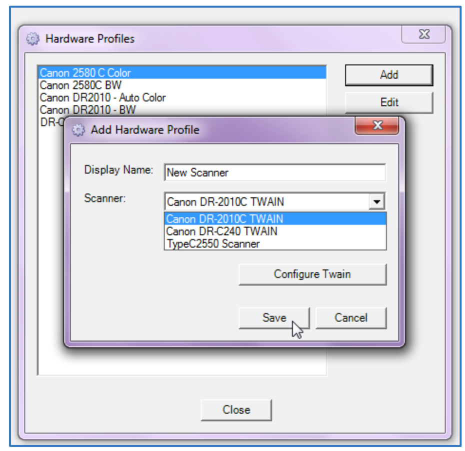


New Hardware Profiles are added through the Scan Client.

Creating a New Hardware Profile

1. From the Start Menu, launch the Scan client.



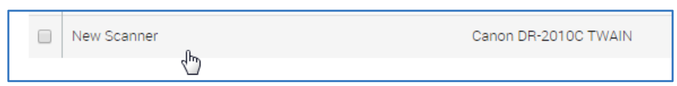


2. Click ***Profiles*** in the menu bar, then select ***Add***
3. Enter a Display Name.

   With the scanner connected to the PC and the driver installed, the new scanner should be listed under the dropdown.

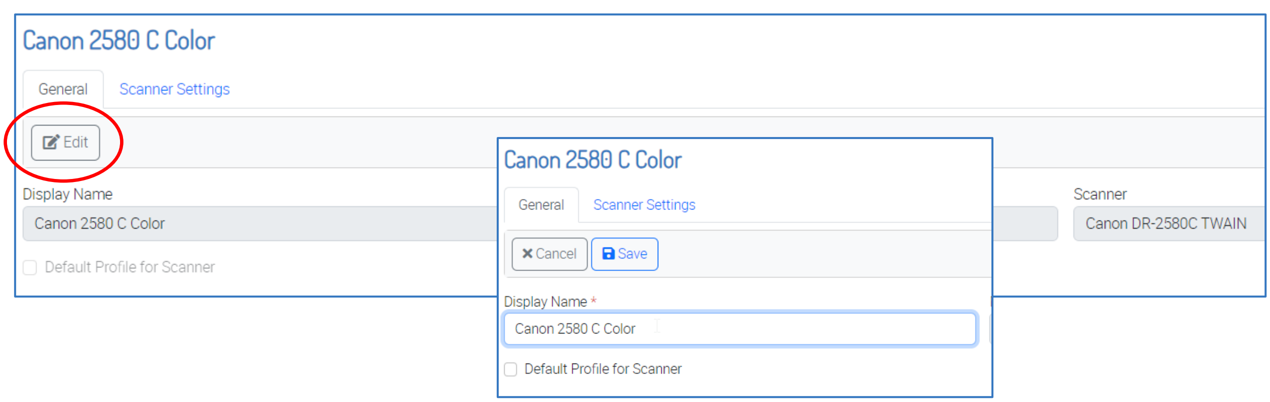
   Click ***Save.***

4. The new Profile will then appear in the list and can be configured.

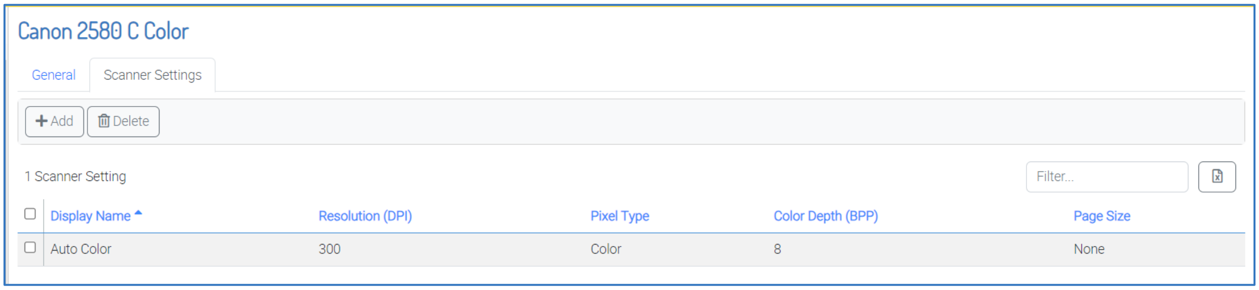


Modifying a Hardware Profile

Under the ***General*** tab, the Name of the profile can be edited.

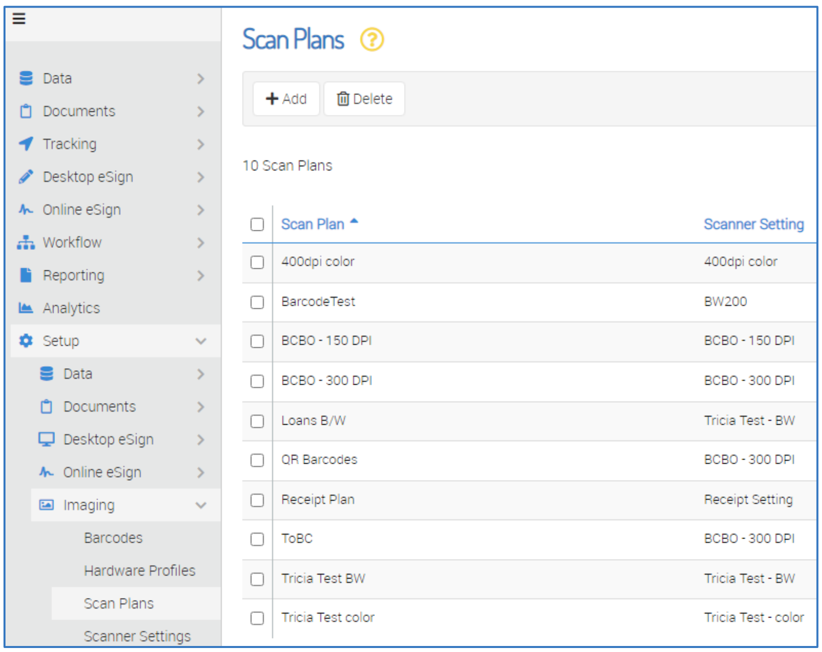


Under the ***Scanner Settings*** tab, Scanner Settings can be added and removed.

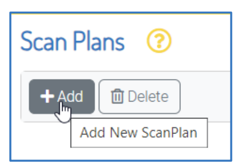


Setup-Imaging-Scan Plans

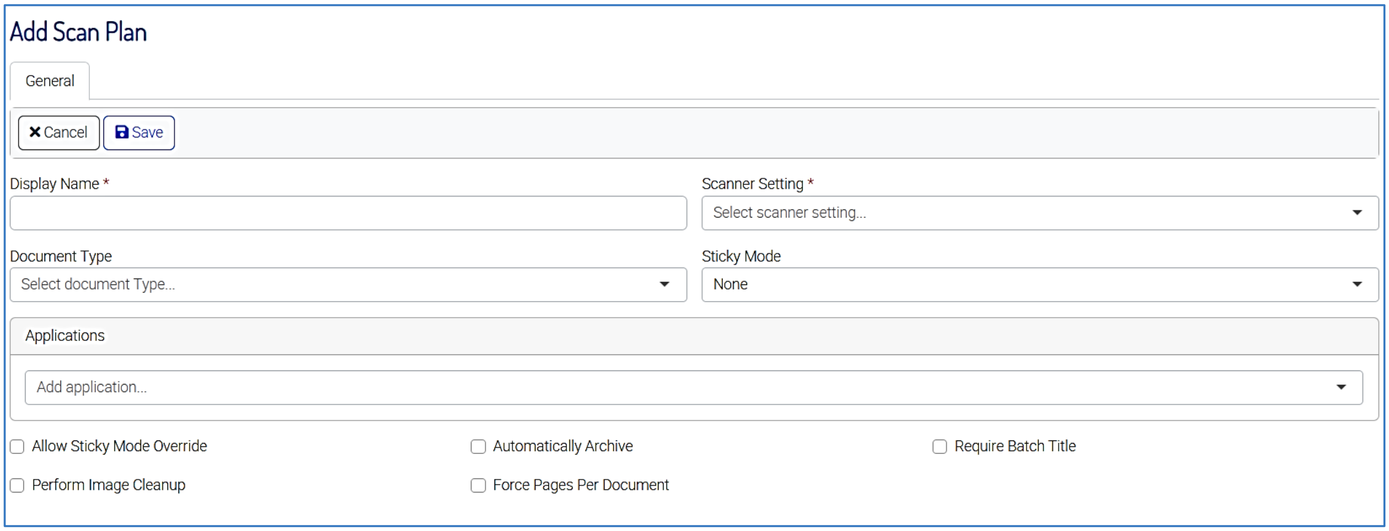
Allows Users to **Add** new Scan Plans, as well as **Delete** or modify existing Scan Plans.



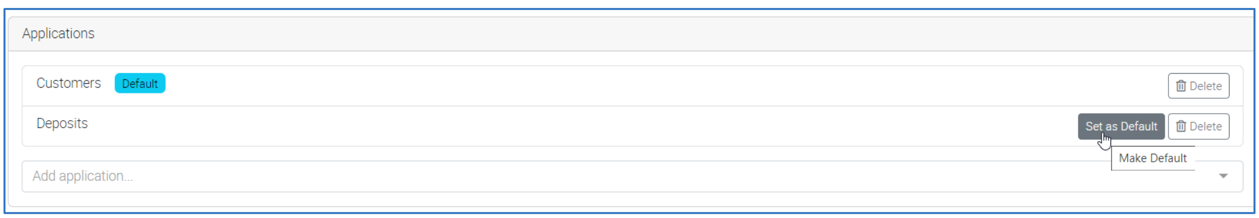
Adding a Scan Plan



Click [+ Add] in the upper menu and enter the plan's details.

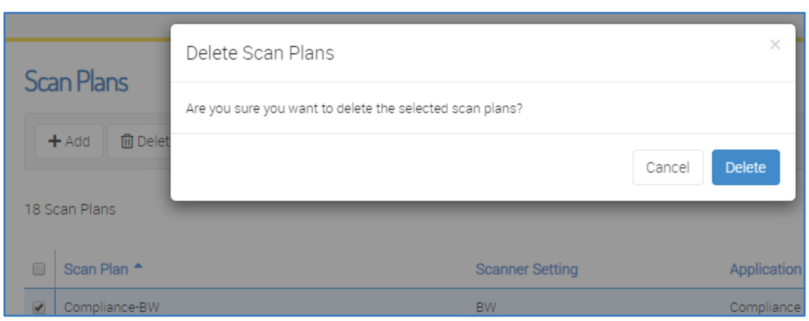


Note: Scan Plans can have more than one Application assigned. This configuration enables Users to index documents across multiple Applications.
The system will assign the first Application selected as the Default Application; however, this can be changed.



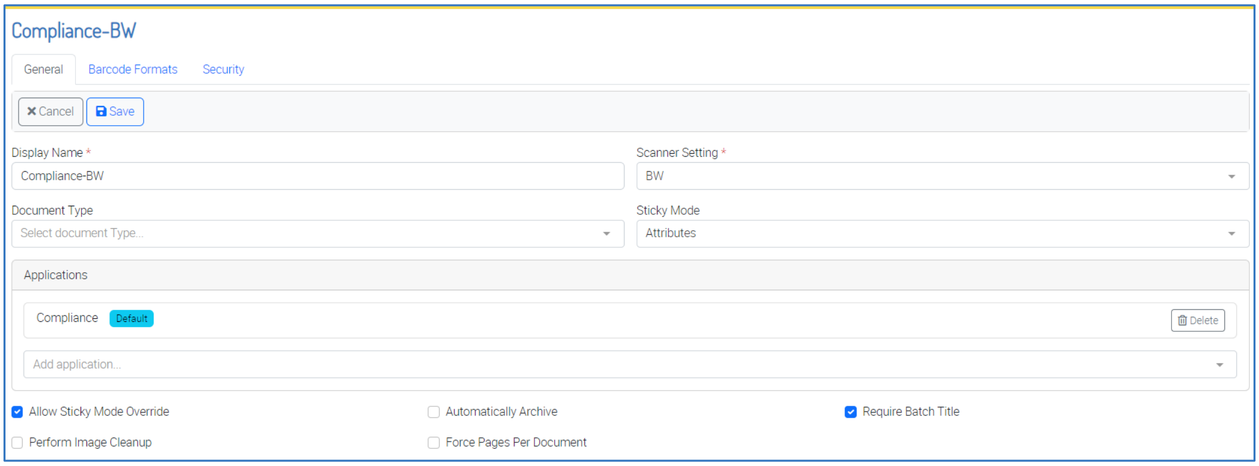
Deleting a Scan Plan

Place a checkmark next to Scan Plan to be removed, then select Delete.

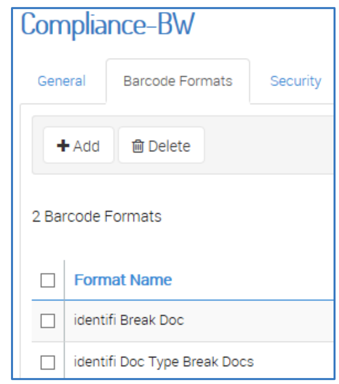


Modifying a Scan Plan

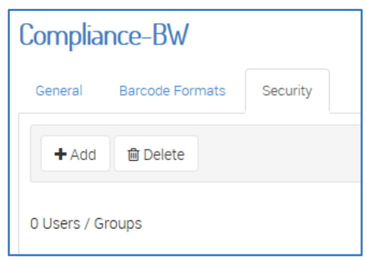
Under the ***General*** tab the basic details and settings of the Scan Plan can be edited.



Under the ***Barcode Formats*** tab, Barcode Formats can be **added** to or **deleted** from the Scan Plan.

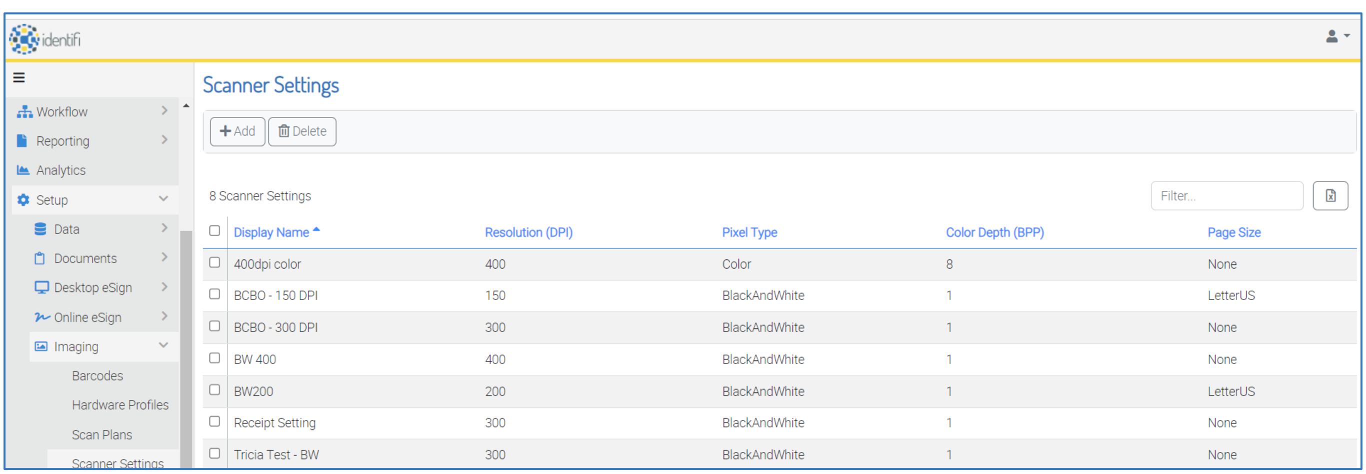


Under the ***Security*** tab, Users and Groups can be added to the Scan Plan.

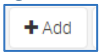


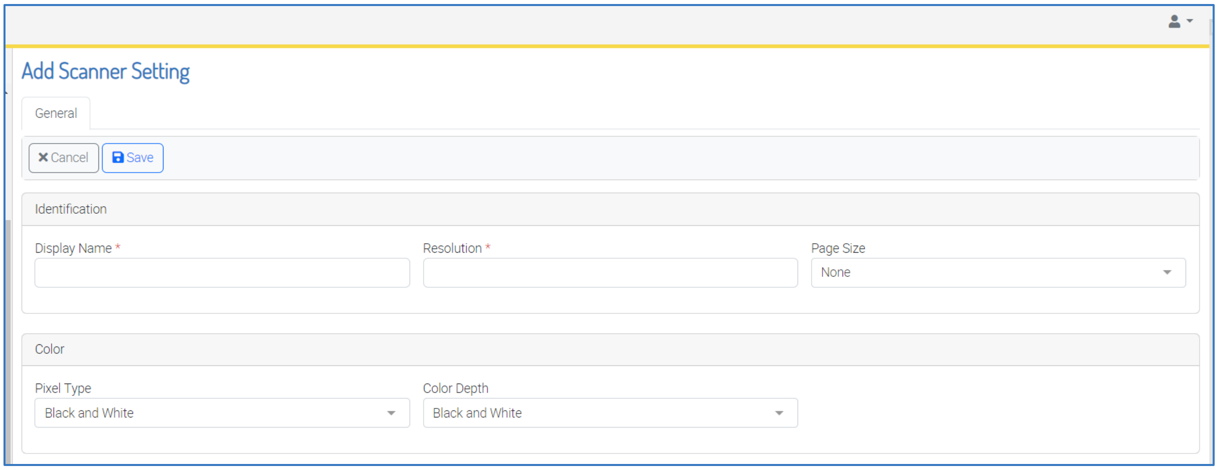
Setup-Imaging-Scanner Settings

Allows User to **Add** new Scanner Settings and **Delete** or **Modify** existing ones.

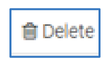


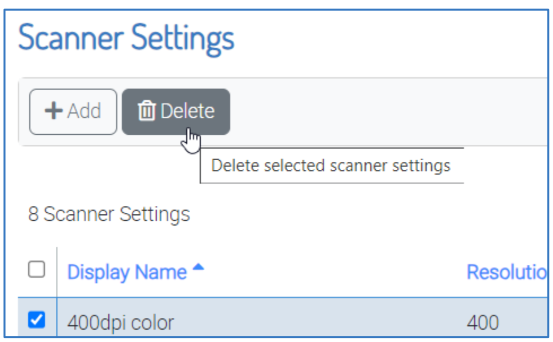
Adding a Scanner Setting

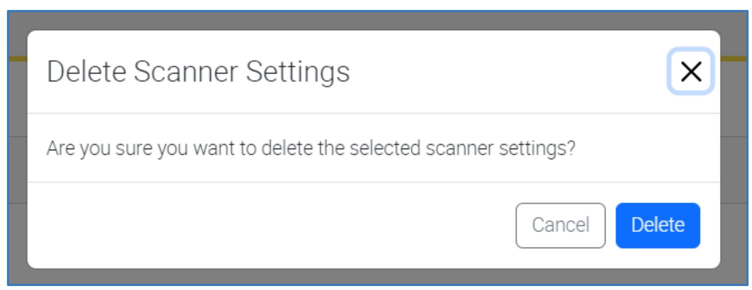
Click  in the upper menu and enter the Scanner Setting's details and click **Save.**



Deleting a Scanner Setting

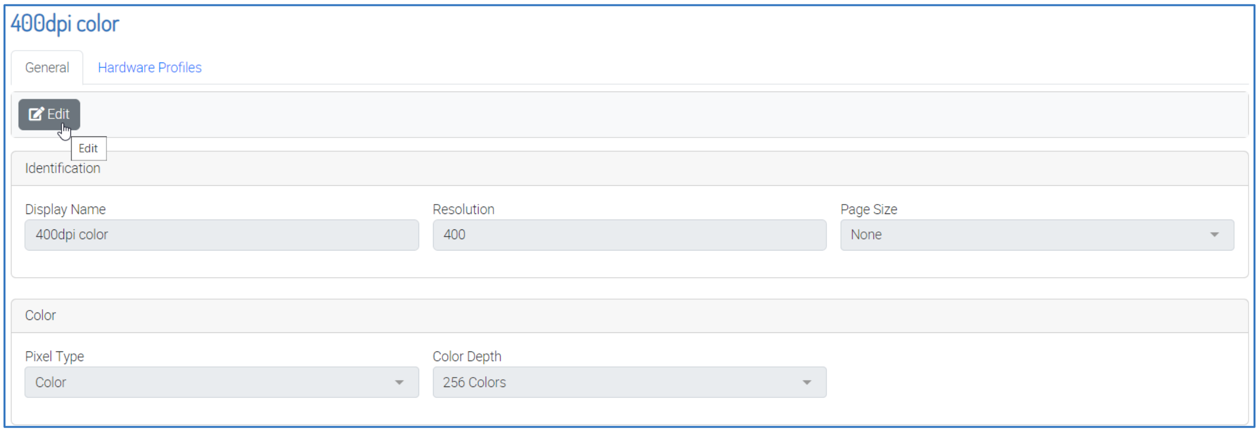
Place a checkmark next to Scan Plan to be removed, then select  .



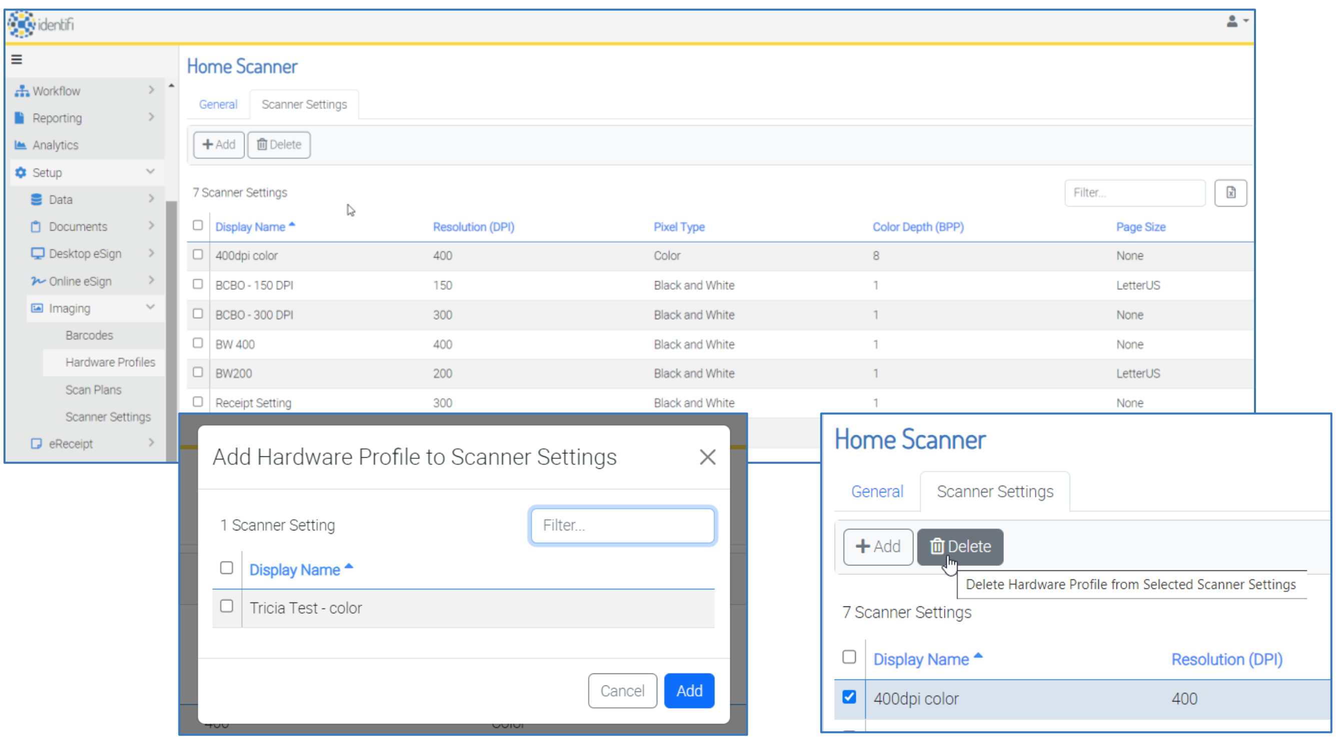


Modifying a Scanner Setting

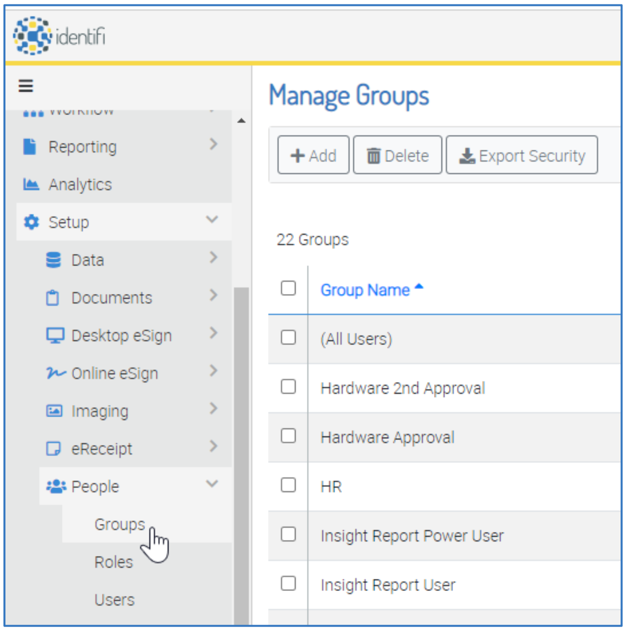
Under the ***General*** tab the basic details and settings of the Scanner Setting can be edited.



Under the ***Hardware Profiles*** tab, the Scanner Setting can be **Added** to and **Deleted** from Hardware Profiles.

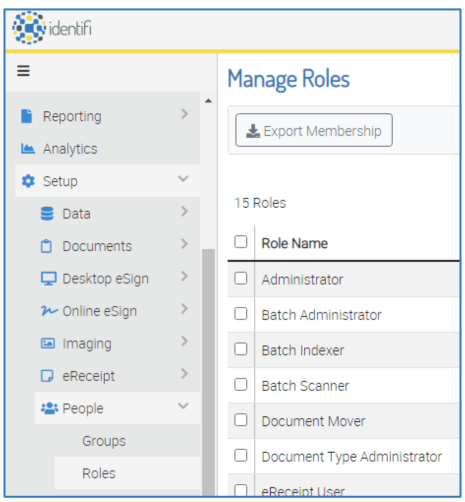


Setup-People -Groups



For details related to managing groups, including the Users and Roles associated with them, please refer to Managing Groups at the beginning of this document.

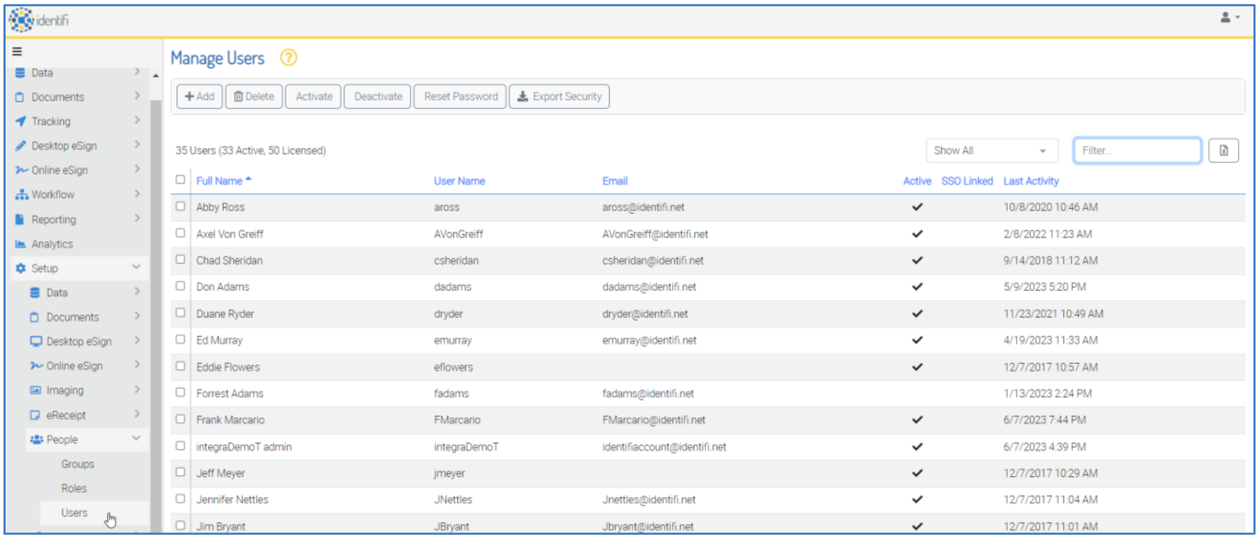
Setup-People-Roles



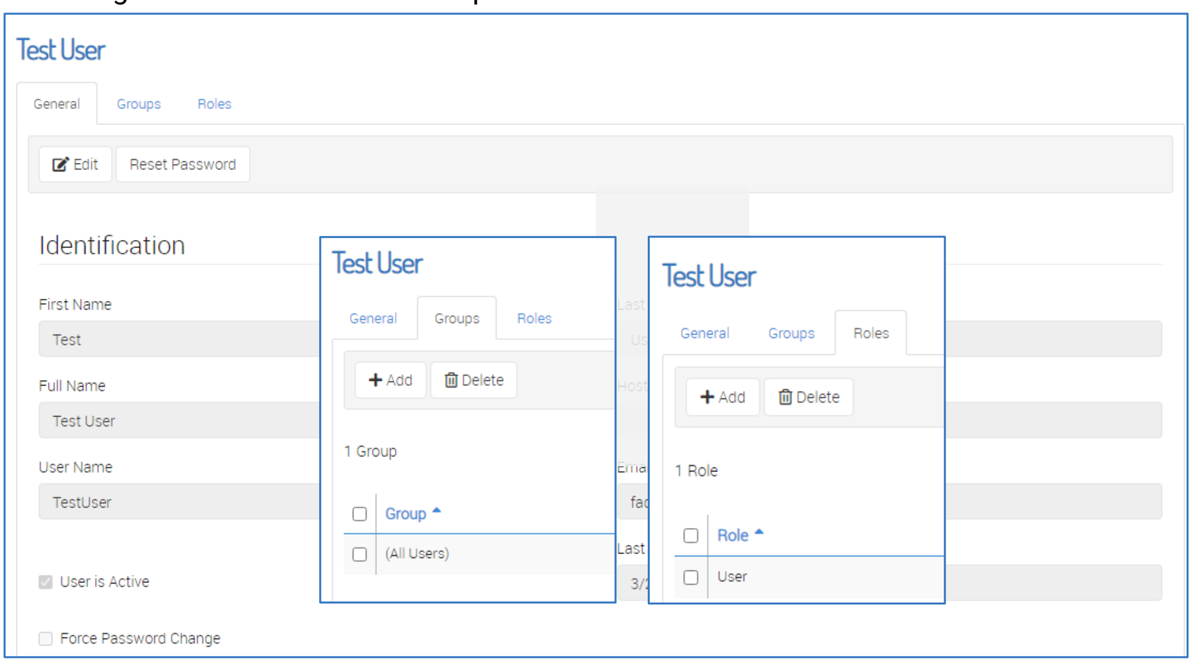
For details on Roles, please refer to User Roles at the beginning of this document.

Setup-People-Users

All Users configured in Identifi. Active and SSO status available on this screen, as well as the date/time of Last Activity.



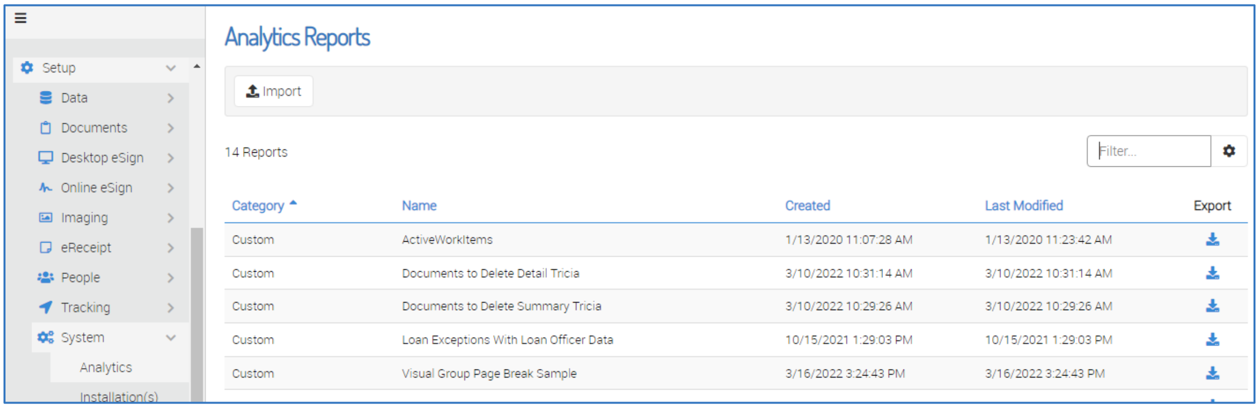
Clicking on a name in the list will open the User's details.



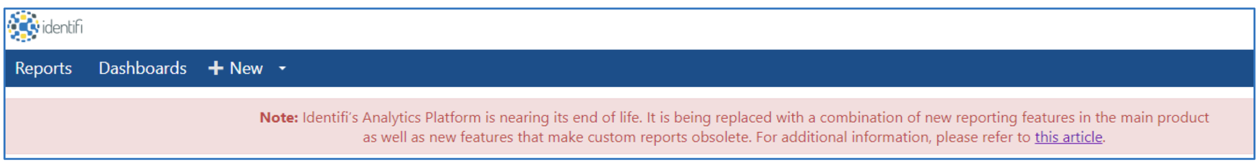
Note: Please refer to Managing Users at the beginning of this document for more information on the User Details screens, adding and deleting Users and managing Passwords.

Setup-System-Analytics

For installations with Analytics, a list of configured custom Reports is found here. Reports can be exported (.izrpt) and imported to another Identifi installation.



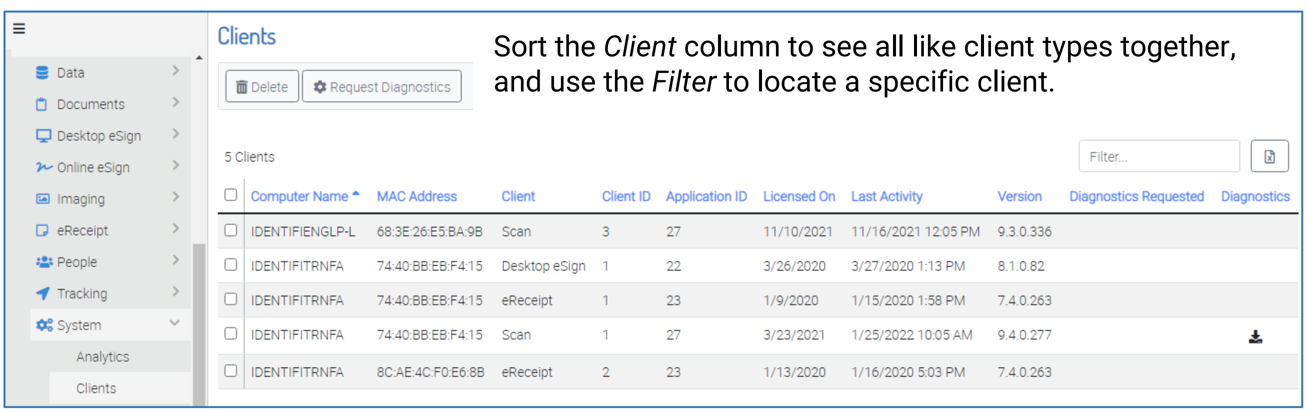
Note: Identifi's Analytics Platform is nearing the end of life. It is being replaced with a combination of new reporting features in the main product as well as new features that make custom reports obsolete.
For additional information, please refer to this article.



Setup-System- Clients

All active clients on an installation will be appear here.

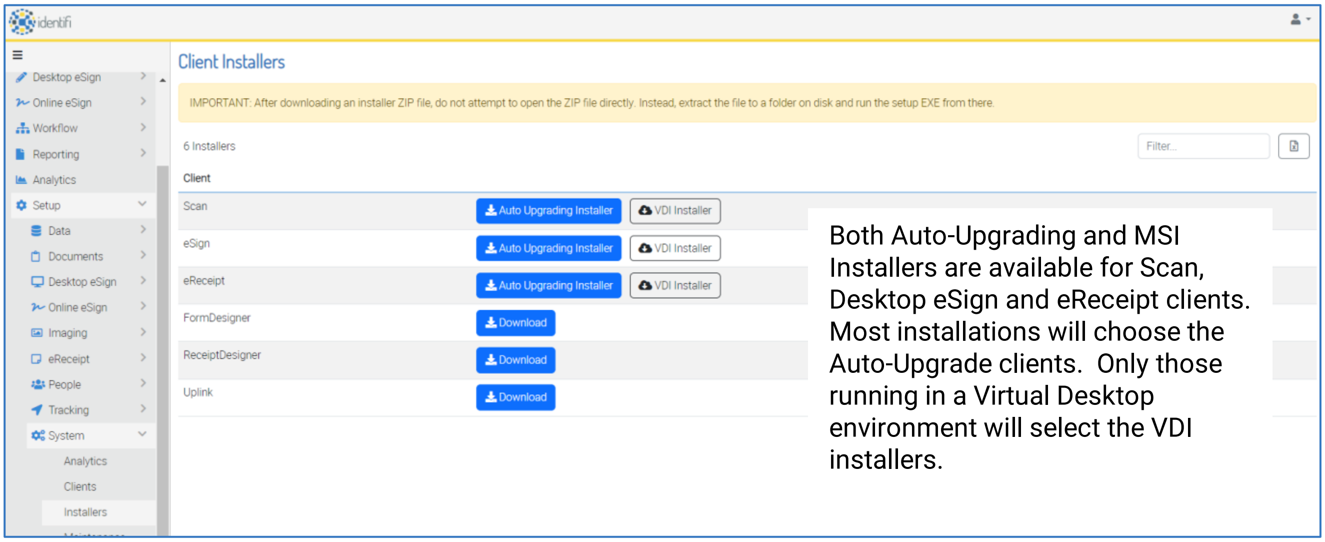
To remove an unused client or to open a license 'seat', place a checkmark in the box to the left of the Computer Name and click ***Delete*** in the upper menu. If that particular client is launched again and there is an open seat, it will repopulate in the list.



Setup-System- Installers

A list of the installation's available client installers will appear here. This list is determined by the Identifi modules licensed on the installation.

From here, the clients are downloaded and can then be deployed to other workstations as needed.



Installing Identifi Clients

Auto-Upgrade Client Installation Instructions

Scan Client

1. Locate *Scan* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run the Identifi Scan Machine-Wide Installer as an administrator.
5. Follow the prompts, but before clicking *Finish* choose whether the Scan client will be installed on the PC for the current user.
6. When users with the Scan User Role log in on the workstation, it will be available from the Start menu and will fully install when launched.

eSign Client

1. Locate *eSign* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run the Identifi eSign Machine-Wide Installer as an administrator.
5. Follow the prompts. *For typical installations, it's recommended to leave all boxes checked and click through the install wizard's prompts.*
6. When users with the Desktop eSign User Role log in on the workstation, it will be available to 'print to' and will fully install when launched.

Repeat these steps for the **Form Designer**. Once finished, it will be available from the Start menu.

eReceipt Client

1. Locate *eReceipt* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run the Identifi eReceipt Machine-Wide Installer as an administrator.
5. Follow the prompts. *For typical installations, it's recommended to leave all boxes checked and click through the install wizard's prompts.*
6. When users with the Desktop eReceipt User Role log in on the workstation, it will be available to 'print to' and will fully install when launched.

Repeat these steps for the **Receipt Designer**. Once finished, it will be available from the Start menu.

MSI Client Installation Instructions

Scan Client

1. Locate *Scan* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run the installer as an administrator.
5. Follow the prompts, but before clicking *Finish* choose whether the Scan client will be installed on the PC for the current user.
6. When users with the Scan User Role log in on the workstation, it will be available from the Start menu and will fully install when launched.

eSign Client

1. Locate *eSign* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run the installer as an administrator.
5. Follow the prompts. *For typical installations, it's recommended to leave all boxes checked and click through the install wizard's prompts.*
6. When users with the Desktop eSign User Role log in on the workstation, it will be available to 'print to' and will fully install when launched.

Repeat these steps for the **Form Designer.** Once finished, it will be available from the Start menu.

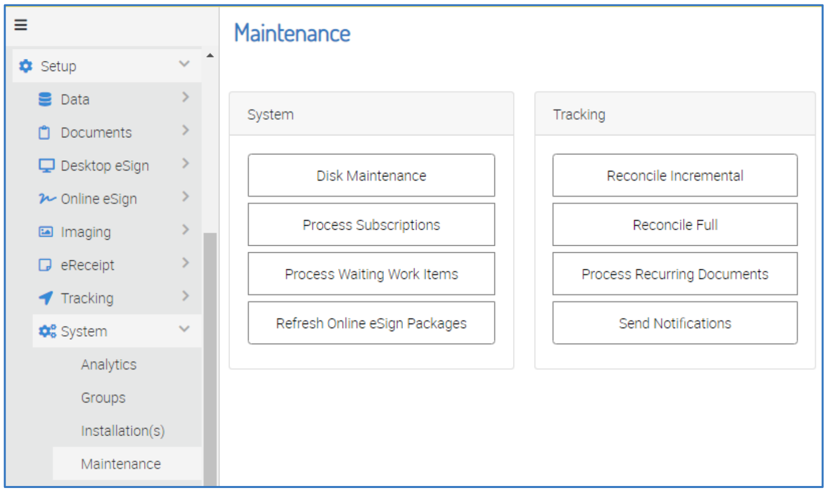
eReceipt Client

1. Locate *eReceipt* in the list of Clients and click *Download*.
2. Extract the files from the zip file before opening.
3. Select the location where the files will be saved.
4. Right-click the .exe to run Installer as an administrator.
5. Follow the prompts. *For typical installations, it's recommended to leave all boxes checked and click through the install wizard's prompts.*
6. Once finished, eReceipt will be available to "print" to.

Repeat these steps for the **Receipt Designer.** Once finished, it will be available from the Start menu.

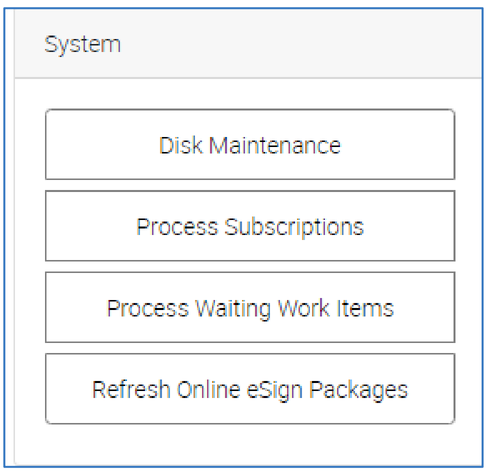
Note: To upgrade the MSI eSign and eReceipt clients on an installation with auto-upgrade clients installed all components of the previous version must be uninstalled. Follow the instructions found in the Identifi Help Center article: https://identifi.zendesk.com/hc/en-us/articles/4402885146519

Setup-System-Maintenance



Under this menu, Users are able to run background maintenance processes manually.

System



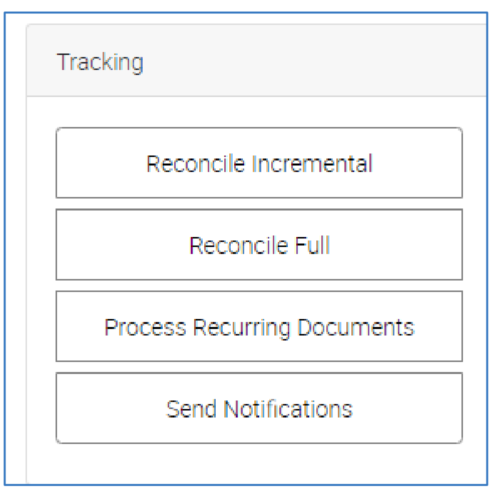
Disk Maintenance: Zips (without compression) the volume's disks, reducing the time required to back up document images.

Process Subscriptions: Sends email notifications for Smart Folder subscriptions. Emails will be initiated for all users subscribed to Smart Folders that have had documents added since the last time the process was run.

Process Waiting Work Items: Updates active Work Plans with documents added to Web.

Refresh Online eSign Packages: Updates Online eSign batches and packages.

Tracking



This maintenance menu will appear only on installations with Document Tracking licensed.

Reconcile Incremental: Evaluates all new documents and data since last reconcile to update Tracking.

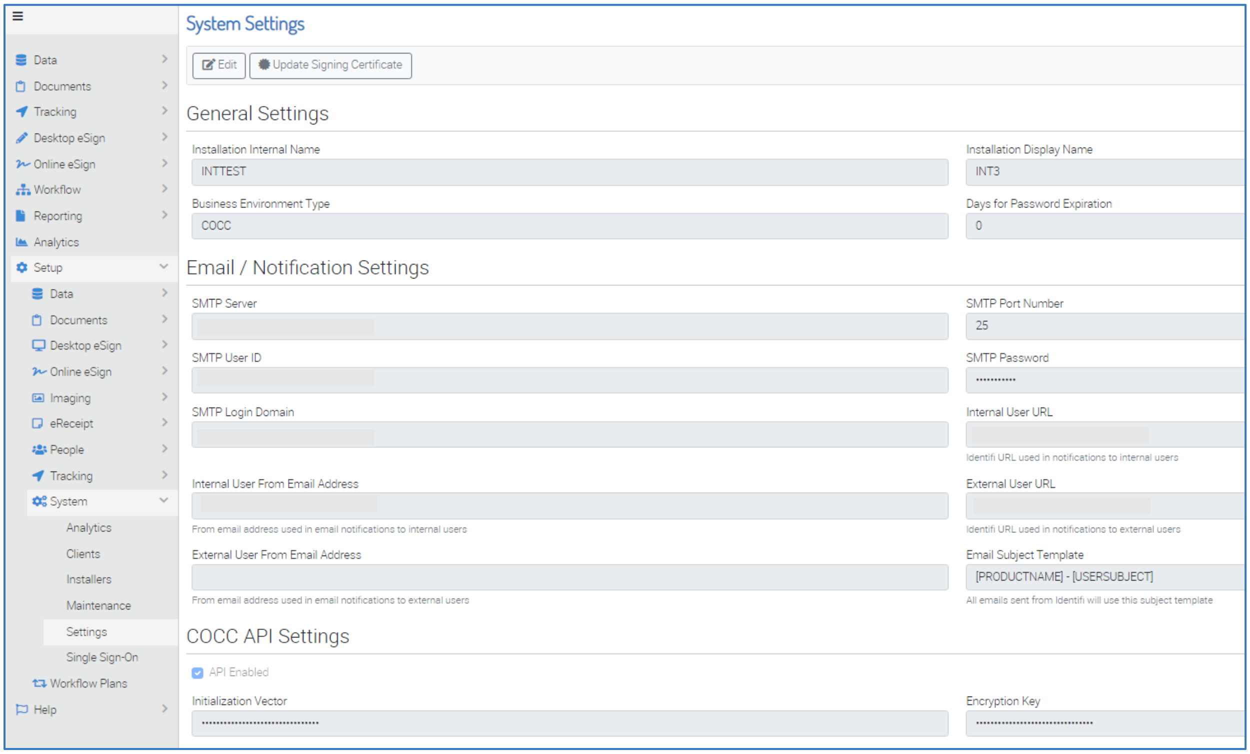
Reconcile Full: Evaluates all documents and data to update Tracking.

Process Recurring Documents: Evaluates all recurring documents to update Tracking.

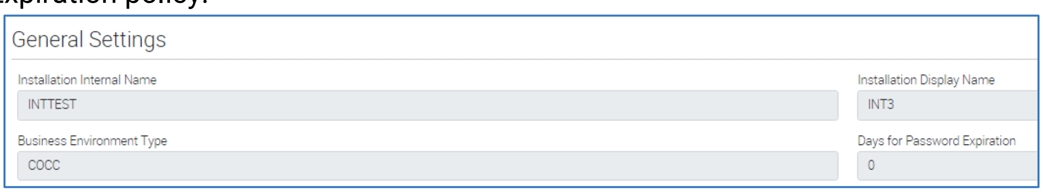
Send Notifications: Sends notifications to assigned users regarding Exceptions.

Setup-System-Settings

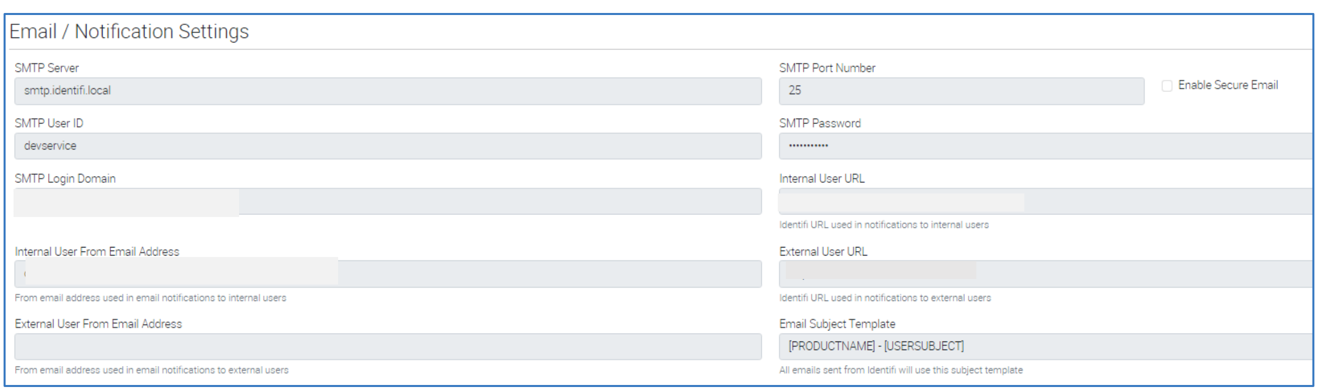
Allows Users to make adjustments to the System Settings.



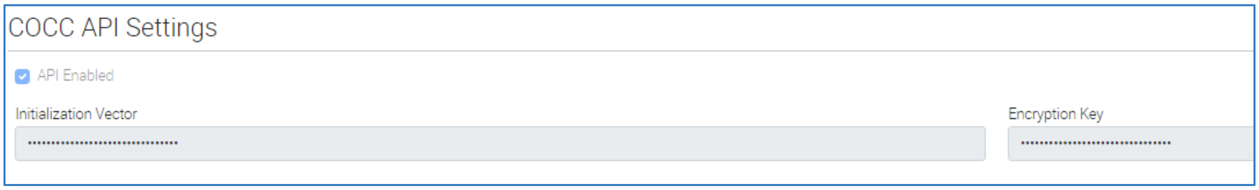
General Settings include the installation's Name, Business Environment Type and Password Expiration policy.



Email/Notification Settings include settings and configuration for the installation's email services.

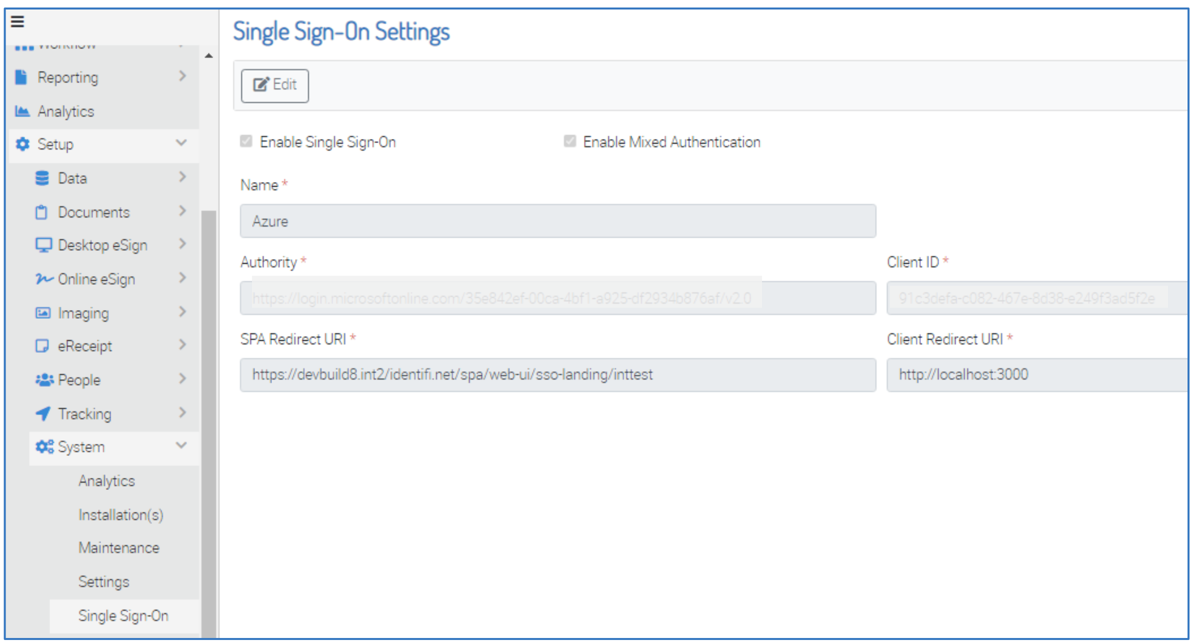


COCC API Settings (Note: This section will only appear on installation's with COCC selected as their Business Environment Type).



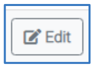
Setup-System-**Single Sign-On**

Single Sign-On configuration for Azure and Okta entered here. Before configuring Single Sign-On (SSO) within Identifi, you must first create and setup the "Application" within your Identity Provider (Azure or Okta) to establish things like the Client ID, the Client Secret and the Redirect URI. These values are required when enabling the SSO option here in Identifi.



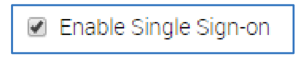
Below are instructions to configure the details found **Setup->System->*Single Sign-on*** to be completed once your Identifi application has been added to your Identity Provider.

For specific directions on adding Identifi as an application in both Azure and Okta, see [Appendix A](#).

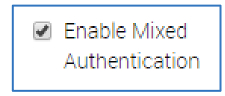
Click ***Edit*** 

to begin.

Complete **fields** as described:

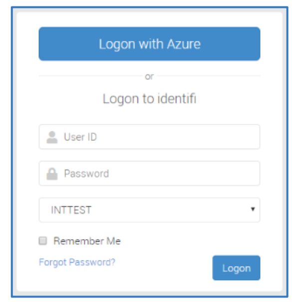


- *Enable Single Sign-on*: This option enables the Single Sign-on integration
  - Currently Identifi is certified to work with Azure and Okta

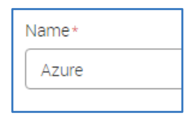


- *Enable Mixed Authentication*: When this is selected, users have the ability to either logon with their IDP credentials (SSO) or their Identifi Private Credentials.

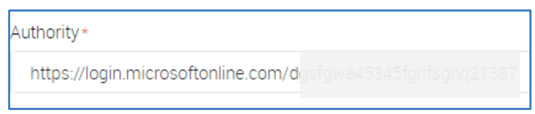
  Note: We recommend that this feature remain enabled until you can verify that your connection to the IDP is working and users are able to successfully logon and link their accounts. If this is disabled and your IDP is not configured properly, then no one will be able to logon to Identifi to address the issue.



- *Name*: This value is displayed on the SSO Logon button on the Logon Page



- *Authority*: This value can be obtained from your IDP's setup. Essentially this field represents the URL associated with the IDP's authorization server.



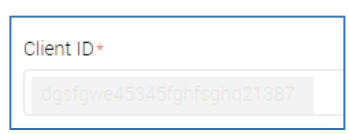
  - Azure Active Directory Authority: **https://login.microsoftonline.com/<Azure ADApplication>/v2**

    This will be the Tenant ID which is found on the application's Overview screen. Use the clipboard icon to copy and paste the ID number.

    Note: See [*Appendix A*]() *for details on using the v2.0 versus v2.1 Azure Open ID Connect endpoint.*

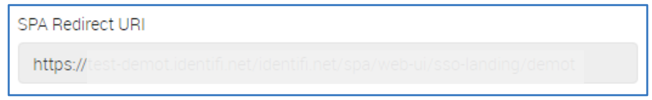
  - Okta Authority: **https://{yourOktaDomain}/oauth2/v1/authorize**

- *Identifi Server Application*: These values will be obtained from your Identify Provider once the Identifi application has been added and configured.

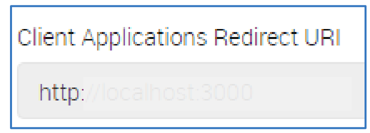


- ○ **Client ID**: This represents a unique client identifier for the Identifi application. This value is established once you set up Identifi within the Identity Provider.

- ○ **SPA Redirect URI:** This URI is very similar to the Redirect URI. It is the installation's URL followed by */spa/web-ui/sso-landing/[installation name]*



- *Identifi Client Applications*: Identifi Client Applications include Scan, Desktop eSign, Uplink and eReceipt.

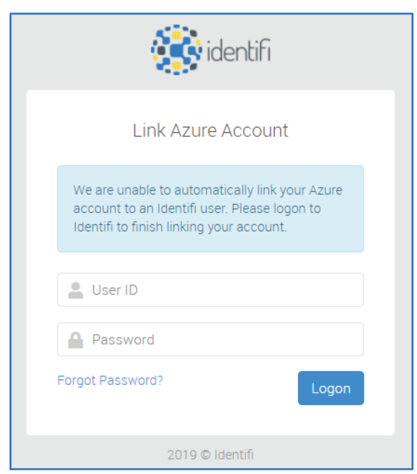


  - ○ **Redirect URI**: This is the callback location where the authorization code or tokens should be sent. For the Identifi client applications, the web browser and the client application itself run together on the same PC, so "localhost" will be used in the URI. A unique port number is also required in the URI. We recommend using port number 3000 and only changing this port number if it conflicts with another application running on a user's PCs. A typical value for the redirect URI is "http://localhost:3000/".

  - ○ **If you are integrating with Azure**, then the same ***Client ID*** and ***Redirect URI*** will be entered here as is being used for the *Identifi Server Application*.

  - ○ **If you are integrating with Okta**, you will need to configure a separate 'Application' within Okta that will represent the Identifi Client Applications (e.g. Scan, eSign etc.). This one should be setup as a Public Application therefore it will not have a Client Secret. Once the Public Application is setup on Okta, the generated Client ID can be configured here.

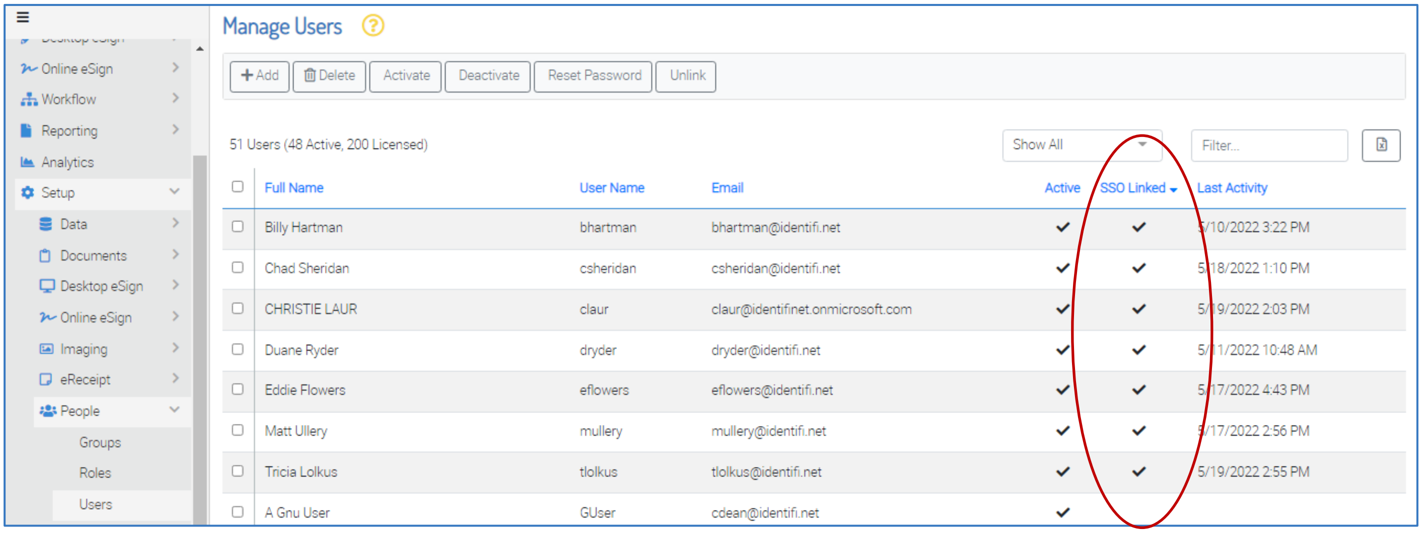
Linking Users Once SSO is enabled



When SSO is enabled, there is a process in place to link existing private user accounts when they attempt to log on for the first time. The email address is used to link the IDP credentials to the Identifi private account credentials. The first time a user logs on with their IDP credentials, the linking process will be initiated. If there is a match between the IDP email address and a single Identifi account, then the accounts are automatically linked.

If there is no match or a multiple match, then the user will be prompted to manually link their accounts. This will only happen once and from that point on the accounts are linked.

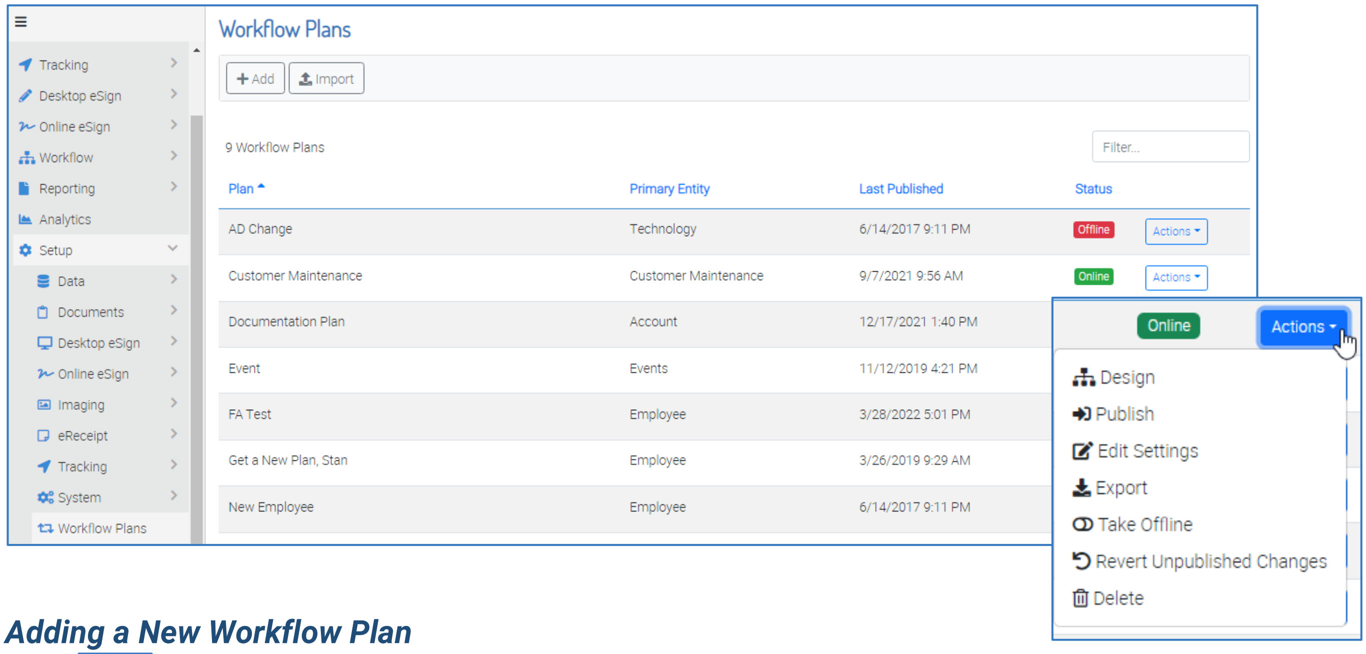
Review the Users menu to verify Linked status:



WORKFLOW

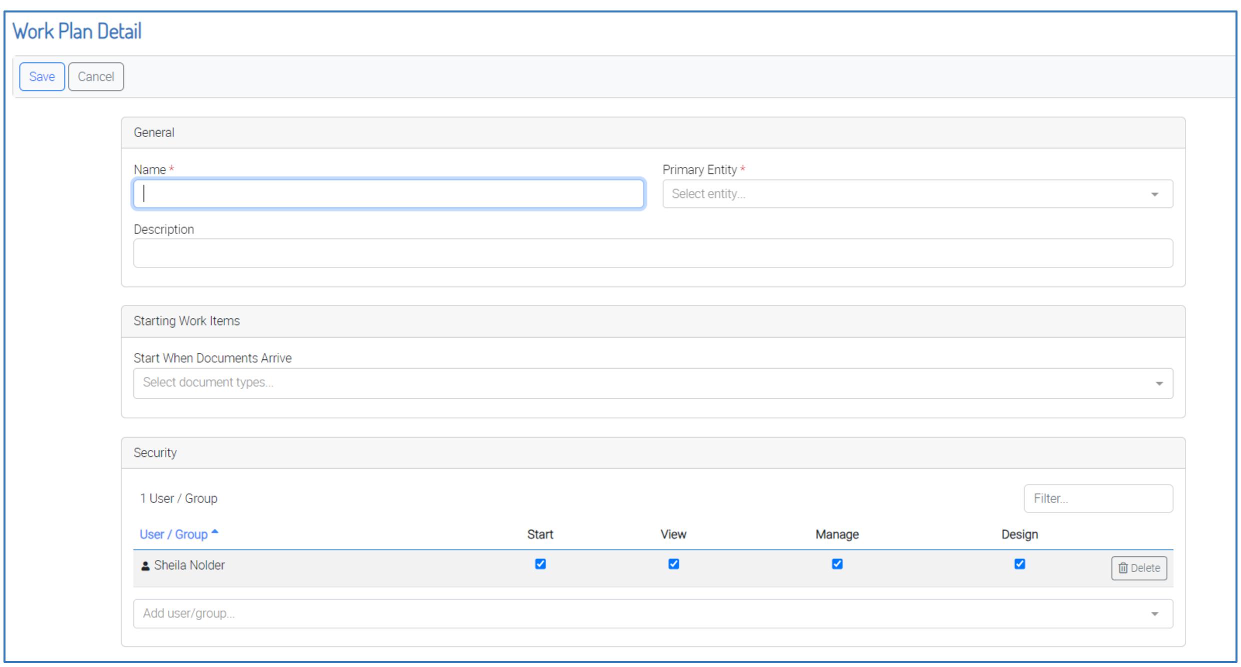
Setup-Workflow Plans

Allows Users to **Add** and **Import** Workflow Plans, as well *Publish, Export, Take Offline, Revert to a Previous Plan, Delete* and modify existing Plans.

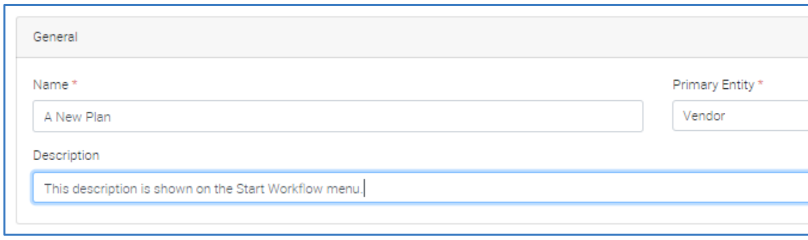


Adding a New Workflow Plan

Click + Add in the upper menu to begin creating a new Plan.



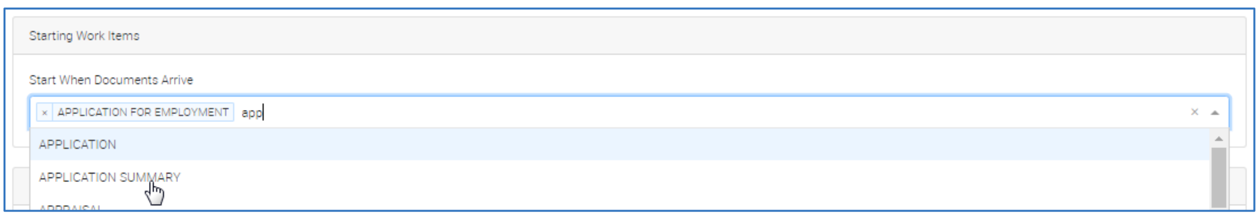
Step 1: General
Name and Primary Entity fields are required; Description is optional. When finished, click **Continue.**



Note: *The Plan's Name and Description can be edited at a later time, however, the Primary Entity cannot be changed once the Plan is saved.*

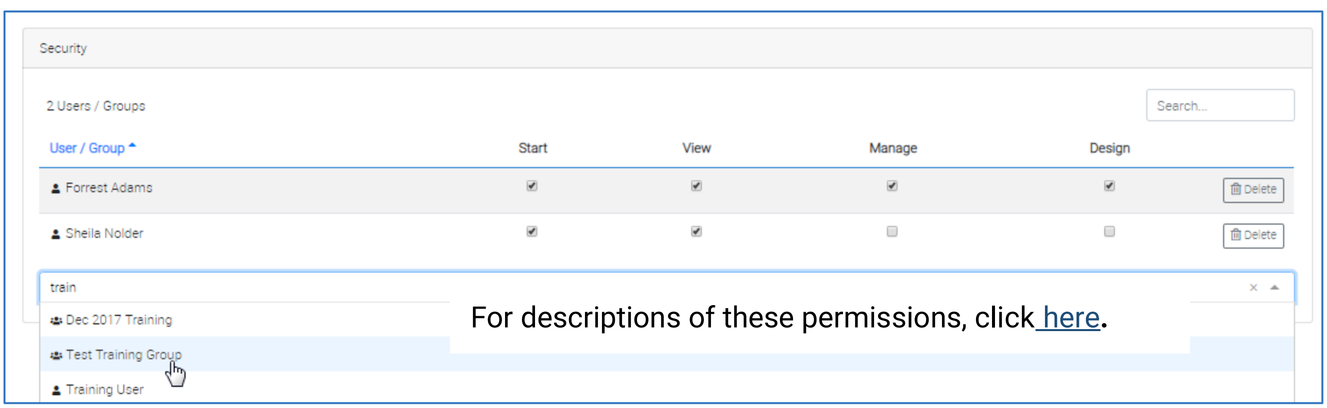
Step 2: Starting Work Items

Determine what document(s) will automatically trigger the Workflow to begin. If no document types are selected here, the Plan will be manual start only.



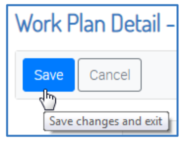
Step 3: Security

Add Users to the Plan, designate their Permissions and click **Continue.**

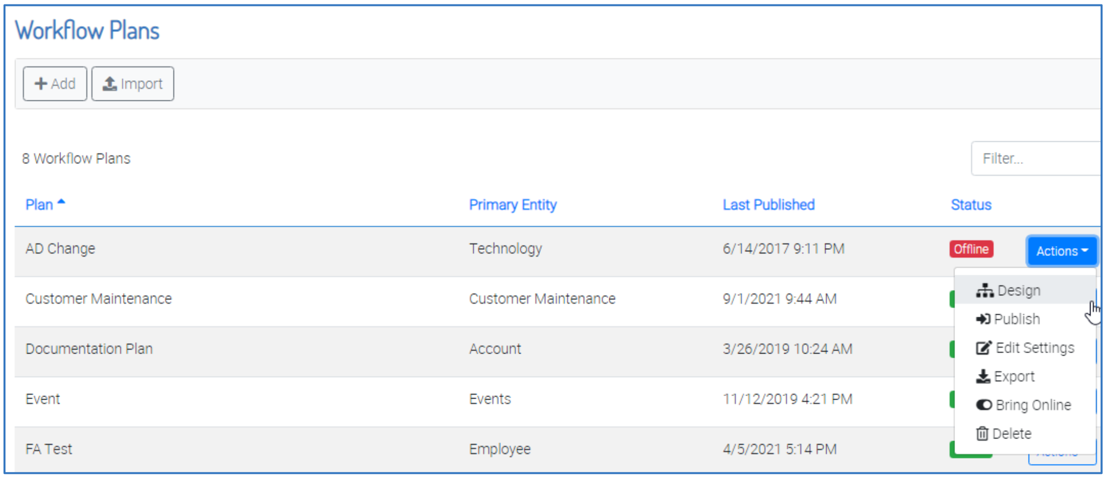


For descriptions of these permissions, click here.

Step 4: Save the Plan
Select *Save* from the top menu



The new plan will now be found among the the list of Workflow Plans.
Choose ***Design*** from the plan's *Actions* dropdown menu.

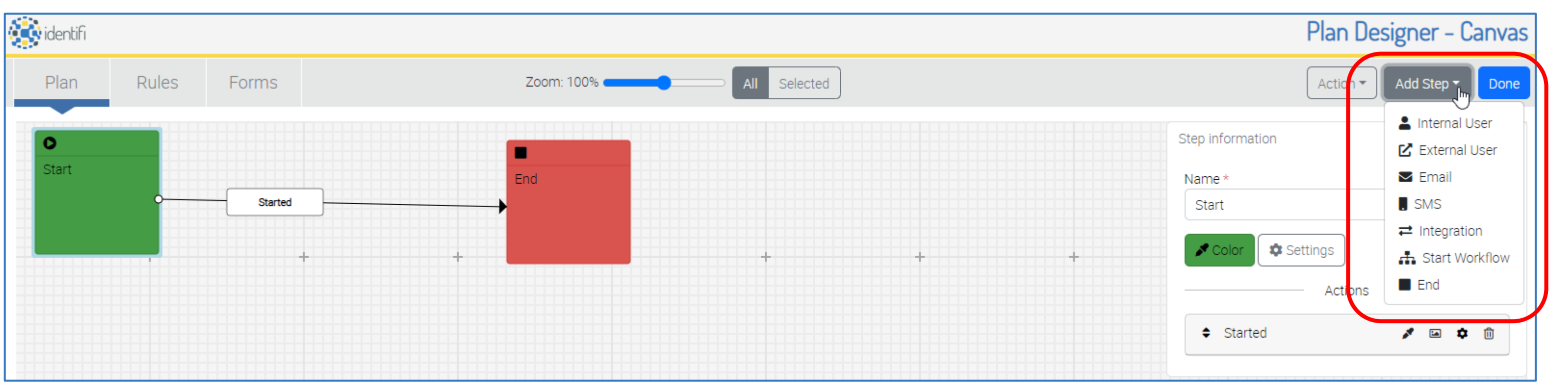


Workflow Plan Designer: Creating & Connecting Steps

Launch ***Plan Designer*** by selecting **Design** from the Plan's dropdown ***Actions*** menu.

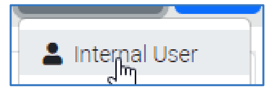
Step 1: Add Steps

Under the **Add Step** drop down, select the type of Step: *Internal User, External User, Email, SMS, Integration, Start Workflow* or *End.*

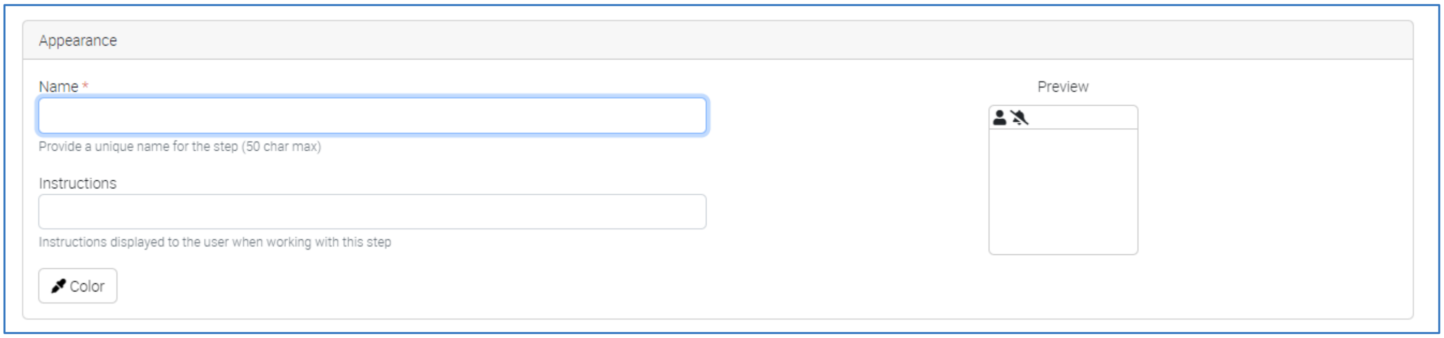


Types of Steps

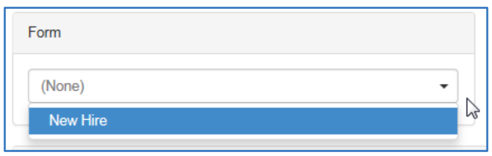
➢ **Internal User Steps** require that internal users take action.

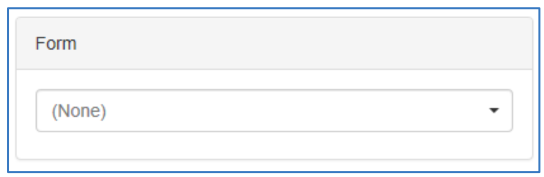


Appearance fields determine what the user will see at the top of the step when the step is being worked, as well as how the step will appear in the Plan Designer.

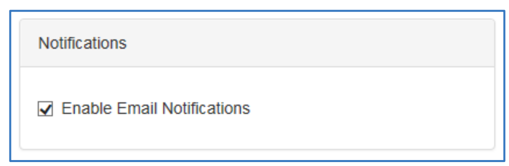


Under **Form** select the appropriate Form template, if applicable. *See *Creating Forms*.





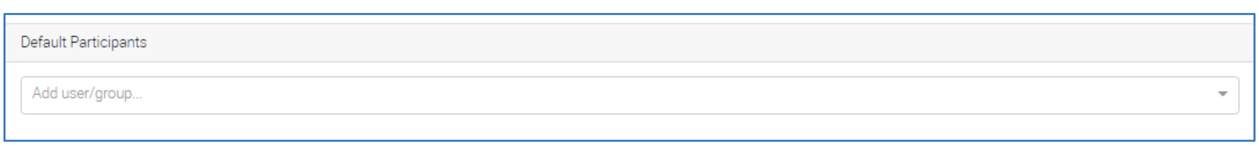
Under **Notifications,** check the box if Plan members should receive an email as the step is completed.



Add Users to the step under **Participants & Assignment Method**

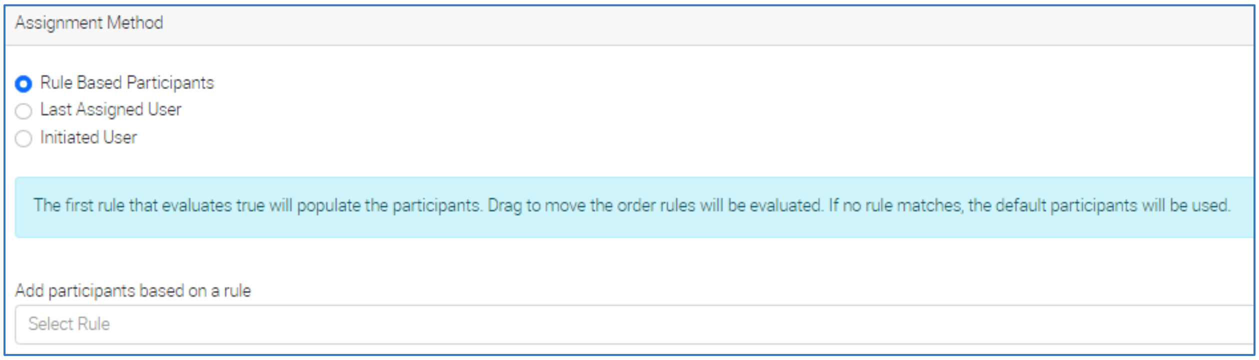
Default Participants

Select default step participants from the dropdown.



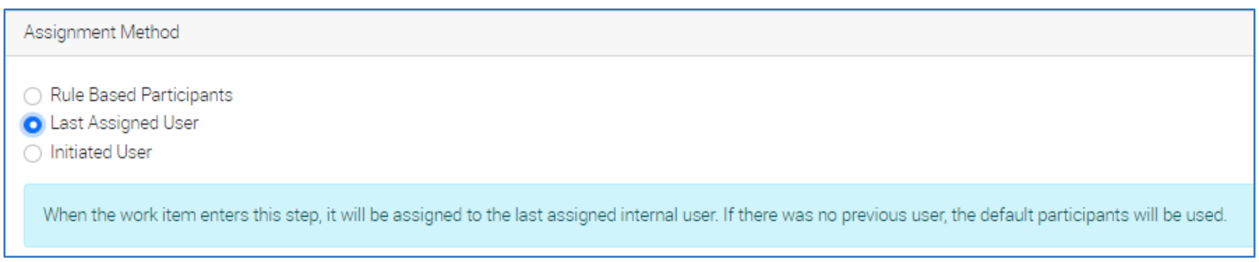
Rule Based Participants

Click the radio button by Rule Based Participants and select the Rule from the dropdown. *See *Creating Rules*.



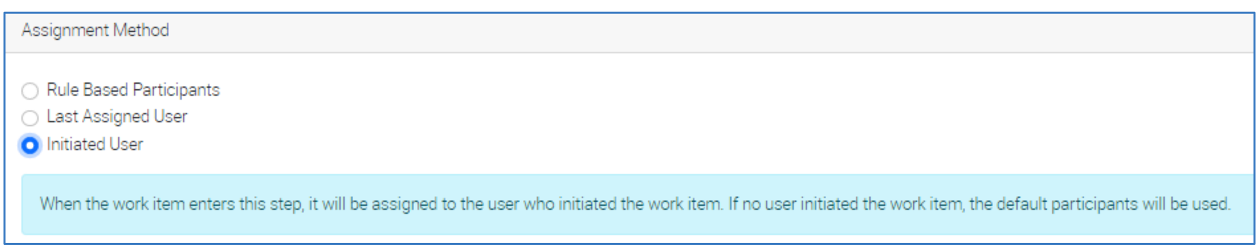
Last Assigned User

Click the radio button by Last Assigned User will assign items in this step automatically to the user last assigned at this step. If there is no previous user, it will be assigned to the default participants.

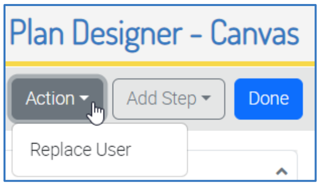


Initiated User

Click the radio button by Initiated User will assign items in this step automatically to the user that initiated the work item. If a user did not initiate the work item, the default participants will be used.

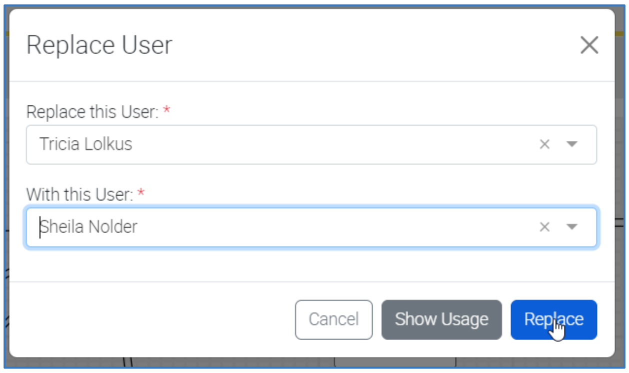


Replace User

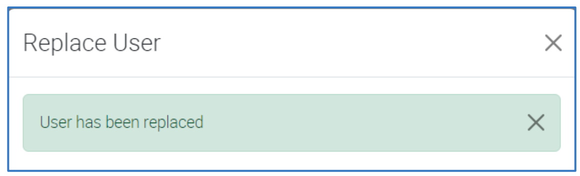


In the event a User needs to be replaced (i.e., change in job function or leaves the company), a global "replace user" function is available.

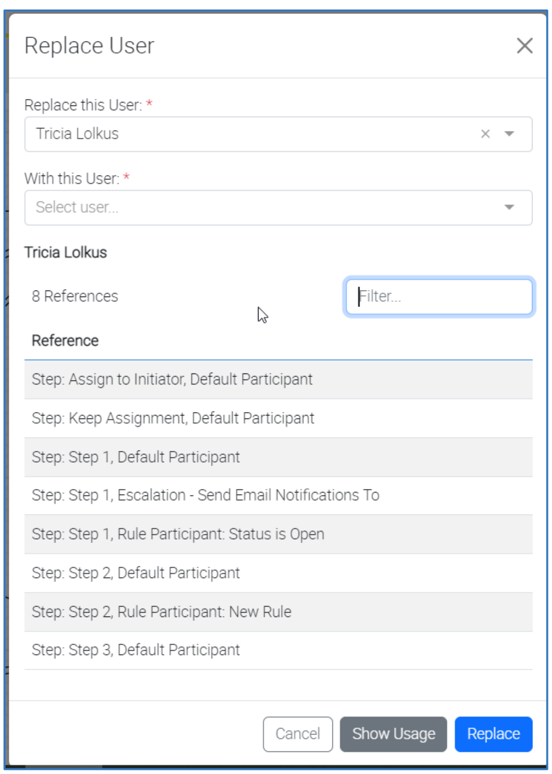
Click Action and select ***Replace User***. Select the original User's name from the drop-down and then the replacement User from the second drop-down and click Replace



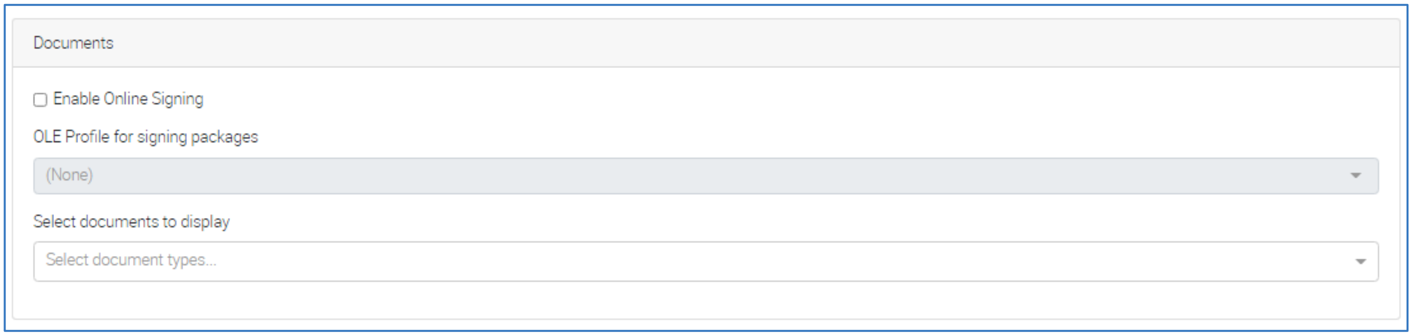
The User will be replaced across the Workflow Plan.



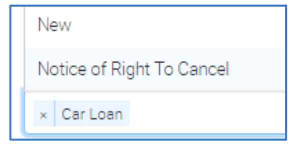
To see where the User ID is referenced within the Workflow Plan, click ***Show Usage.*** Show Usage



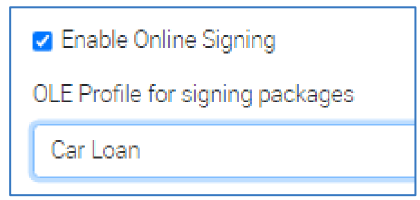
If documents are needed for this step, they are added under **Documents.**



Click in the *Select documents to display* field and choose the documents from the drop-down list.

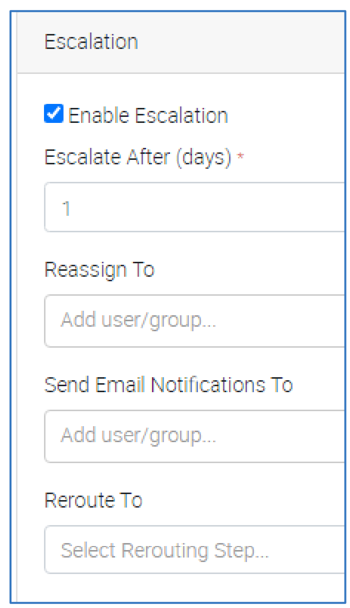


If these Online eSign Packages will be created as part of the step, click the check box next to ***Enable Online Signing*** and then select the Profile from the drop down menu.



End Users will then see a "Sign" button under the *Documents* tab of the Step as well as a *Signing Packages* tab where the status of the Packages will be displayed.

Lastly, check the box to **Enable Escalation** if the item should be automatically re-assigned or re-routed due to inactivity.



1. Begin by checking the box to *Enable Escalation*

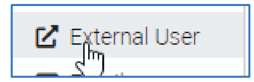
2. Determine the number of days an item must be inactive before being escalated.

3. Choose how the item will be escalated:
   - **Reassign To**: Select a User/Group to reassign the work item to after the escalation period.

   - **Reminder Notification Email To:** Enter User/Group to receive a reminder email after the escalation period.

   - **Reroute To:** Select a Step in the Plan to reroute the item to after the escalation period.

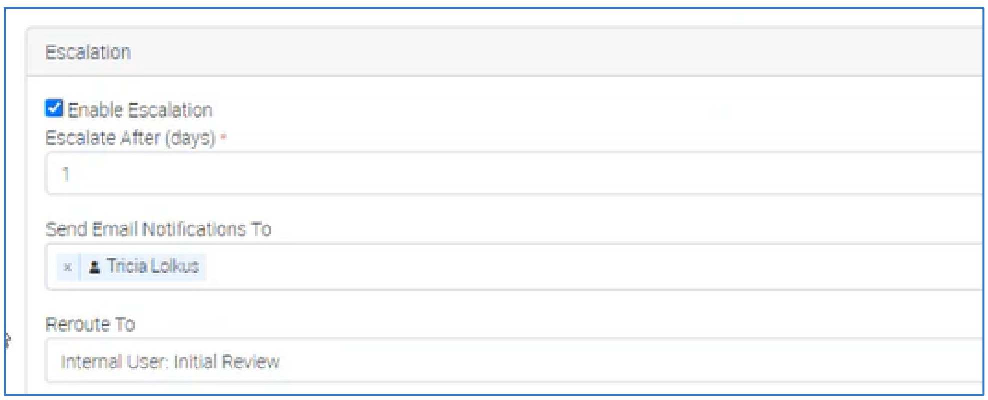
➢ **External User Steps** produce an email to an external user.



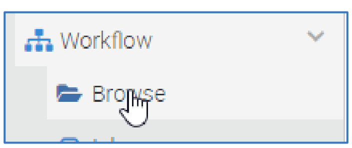
- **Escalation for External Workflow Steps:** This feature allows for the system can escalate a Work Item that resides in an External Step for too long.

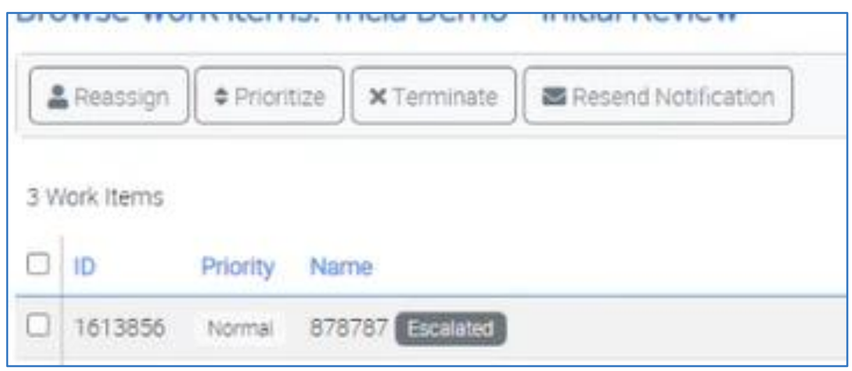
  Within the Plan's Settings, the Escalation parameters can be found at the bottom of the External Step Settings page in the Plan Designer,

  Similar to the escalation for Internal steps, once the required number of days is entered into the form, the user will have the option to send an email notification and/or reroute the item to another step.

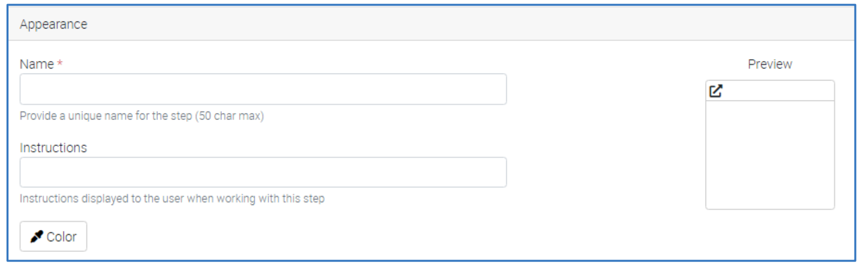


If an item is escalated, it will now have the 'Escalated' badge which is visible in both the Work Item Browse and the User's Inbox.

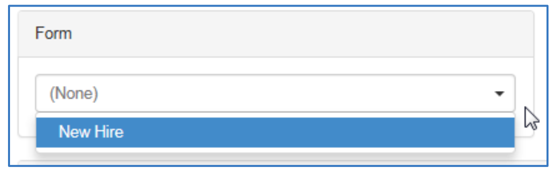




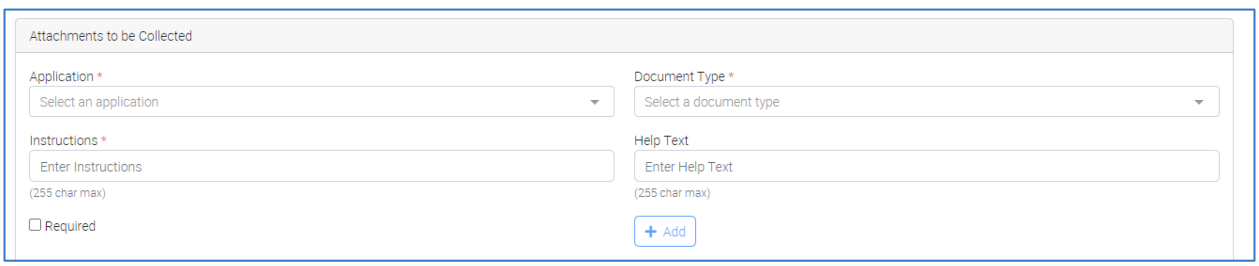
Appearance fields determine what the user will see at the top of the step when the step is being worked, as well as how the step will appear in the Plan Designer.



Under **Form** select the appropriate Form template, if applicable. *See *Creating Forms*.

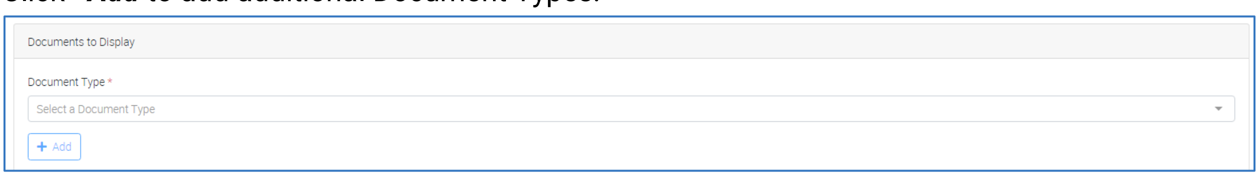


Attachments to be Collected fields allow for the External Users to return attach a document as part of the step. Begin by selecting the Application, followed by the Document Type. The *Instructions* field is required, *Help Text* is optional. As in Internal Steps, these documents are automatically added to the archive. Click ***+Add*** to add additional Document Types.

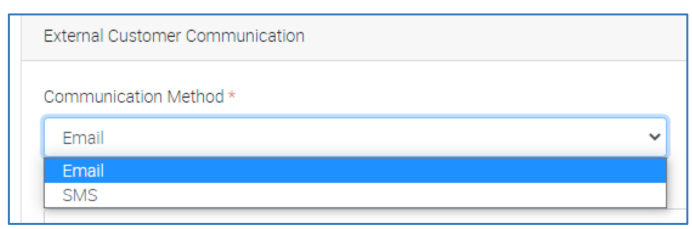


Documents to Display fields allow for a document to accompany the work item and display for the External User.

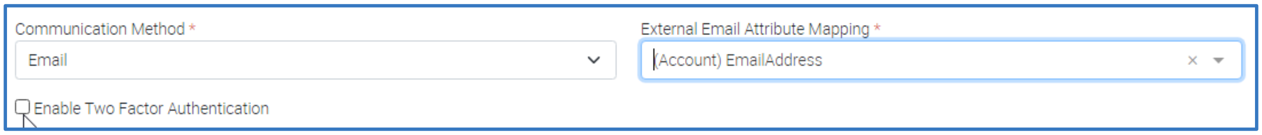
Click ***+Add*** to add additional Document Types.



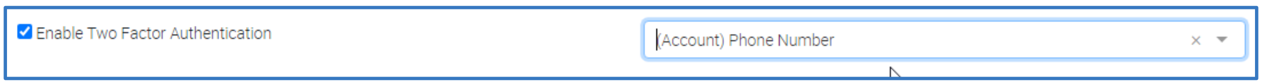
In the **External Customer Communication** area, users will determine how the item is sent to the external participant: Email or SMS.



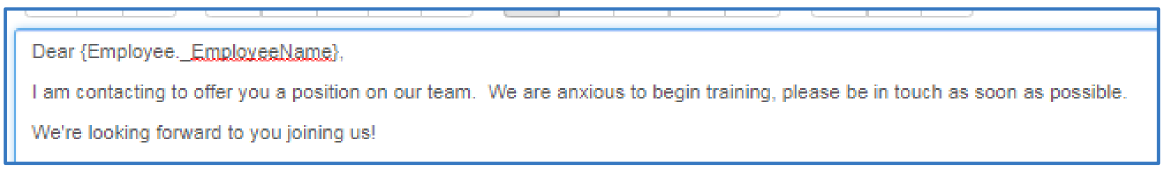
- **Email**: Choose *Email* and then select the appropriate email attribute from the dropdown.



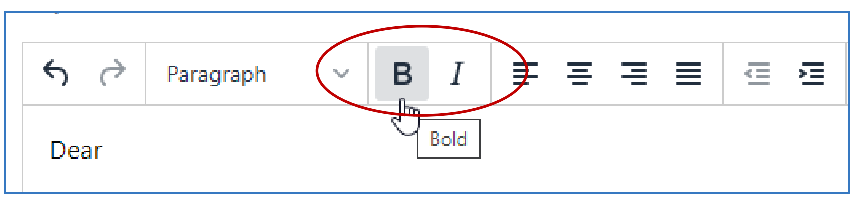
Check the box to 'Enable Two Factor Authentication' and then select the appropriate phone number attribute from the dropdown that appears. When the receipient of the work item clicks the link to load the web form, a text message will be sent and they will be prompted to enter it correctly before they are able to access the item.



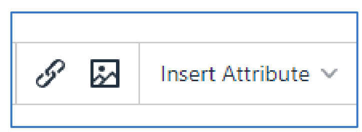
Then enter the Subject and Body of the email that the External User will receive.

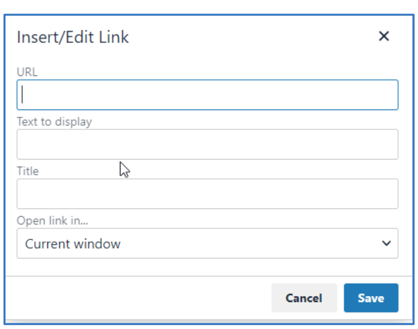


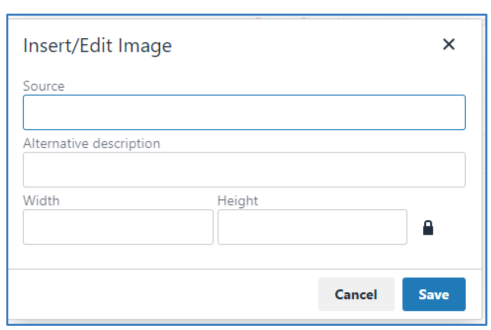
Rich Text Formatting available.

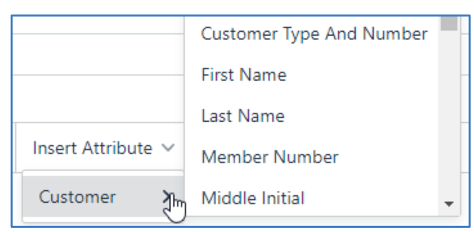


Insert links, images and ***attribute placeholders*** in the message.

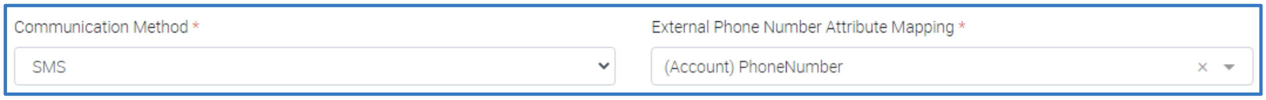




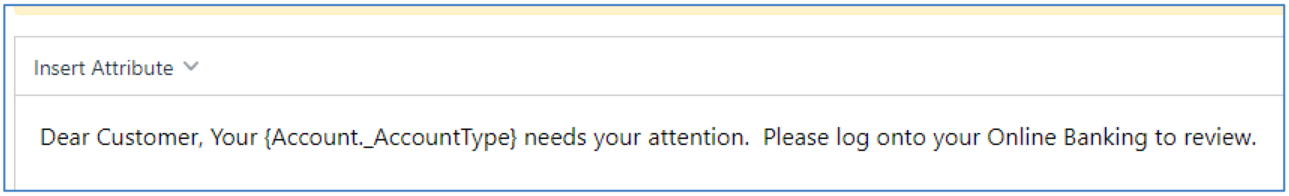


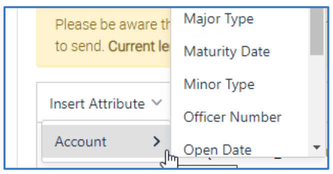


- **SMS:** Choose *SMS* and then select the appropriate phone number attribute from the drop-down.



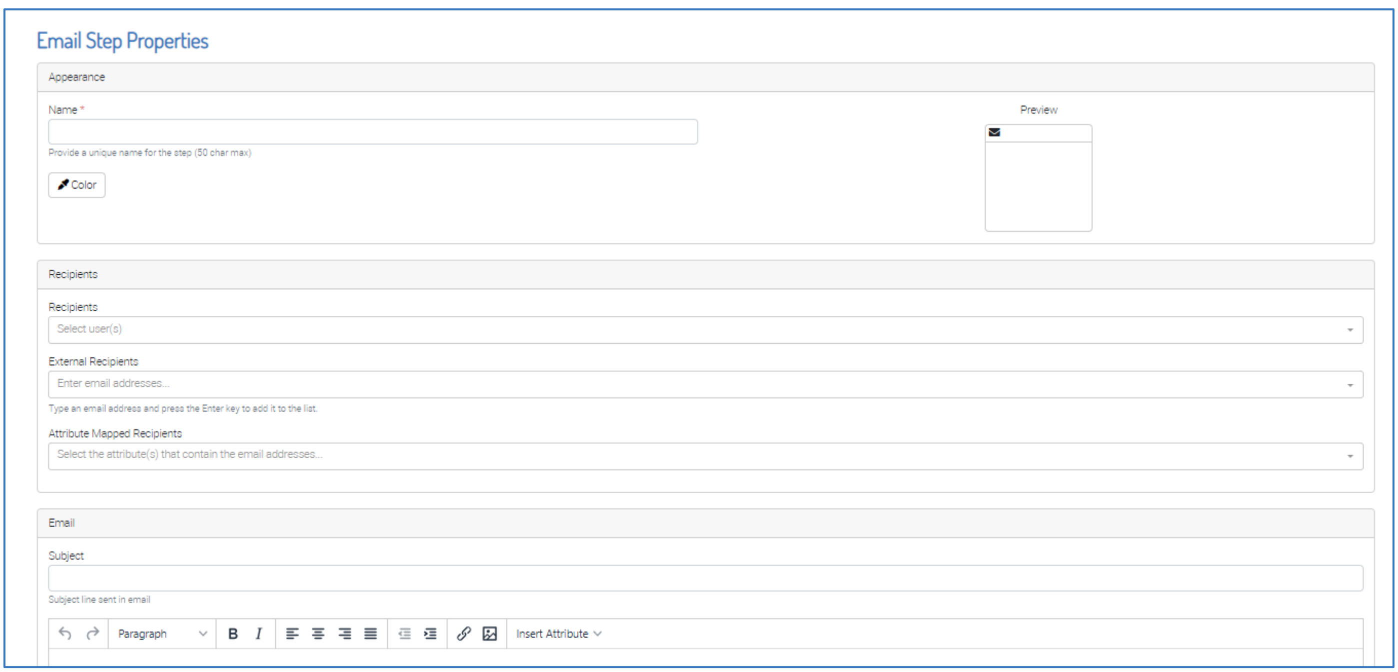
Enter the content of the text message that the External User will receive.



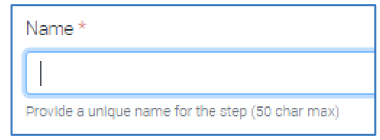


Insert an ***attribute placeholder*** to include in the message.

- **Email Steps** trigger an email.

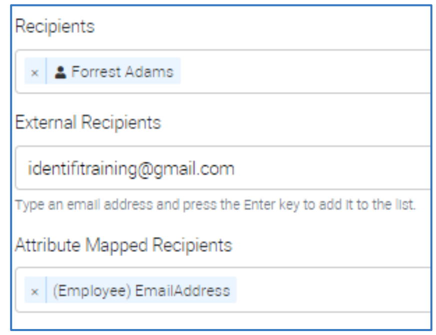


Appearance fields allow the user to give the step a Name, color and an icon.

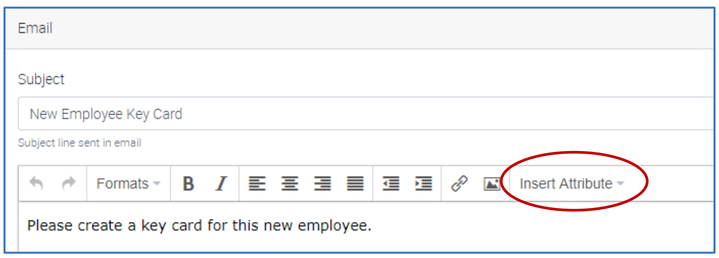


Add **Recipients** by:

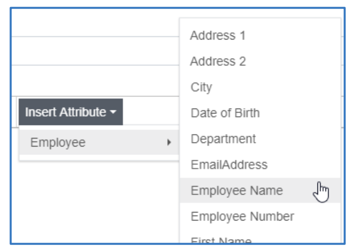
- Selecting other Identifi Users under *Recipients*
- Entering email addresses under *External Recipients*
- And/or selecting email address attributes from the associated Entity under *Attribute Mapped Recipients*.



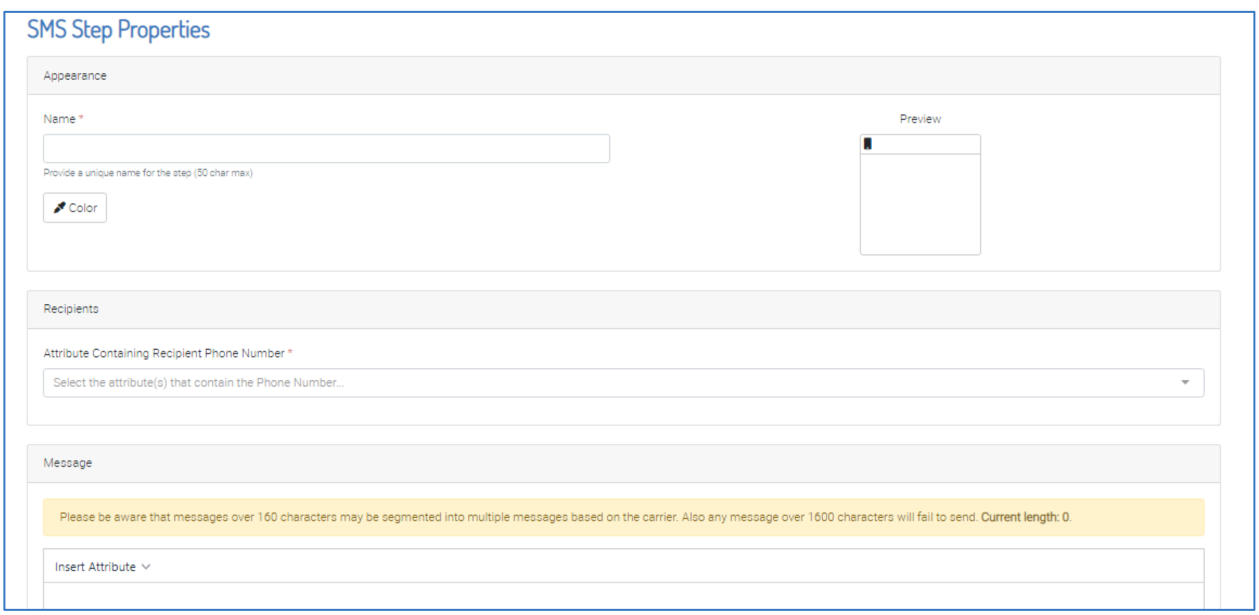
Finally, enter the Subject and Body of the **Email**. Rich Text formatting available.



Use ***Insert Attribute*** to add atrribute data to the email.

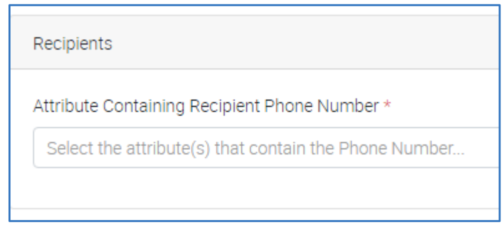


➢ **SMS Steps** trigger a text message to a mobile phone.

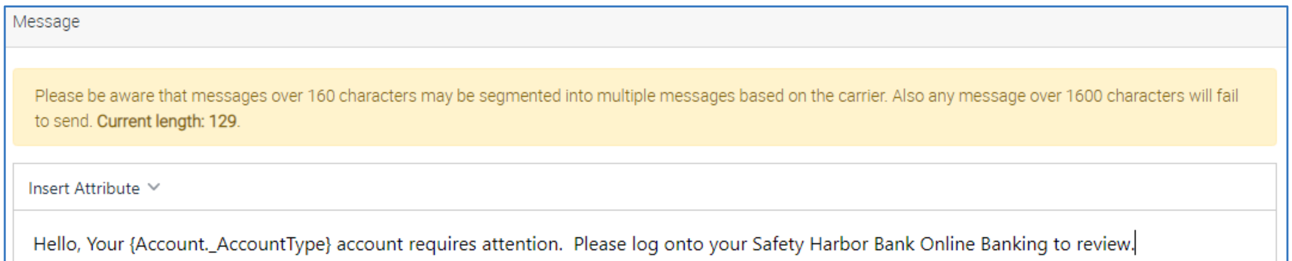


Appearance fields allow the user to give the step a Name, color and an icon.

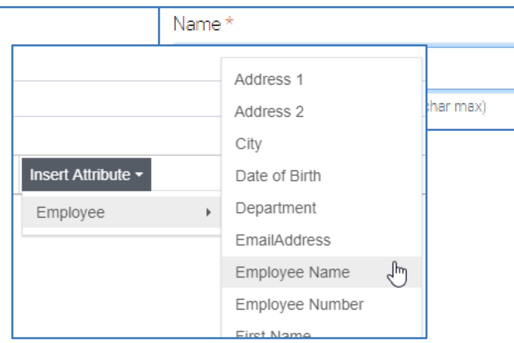
Add **Recipients Phone Number** by selecting the appropriate attribute from the drop down list.



Finally, enter the content of the **Message**.



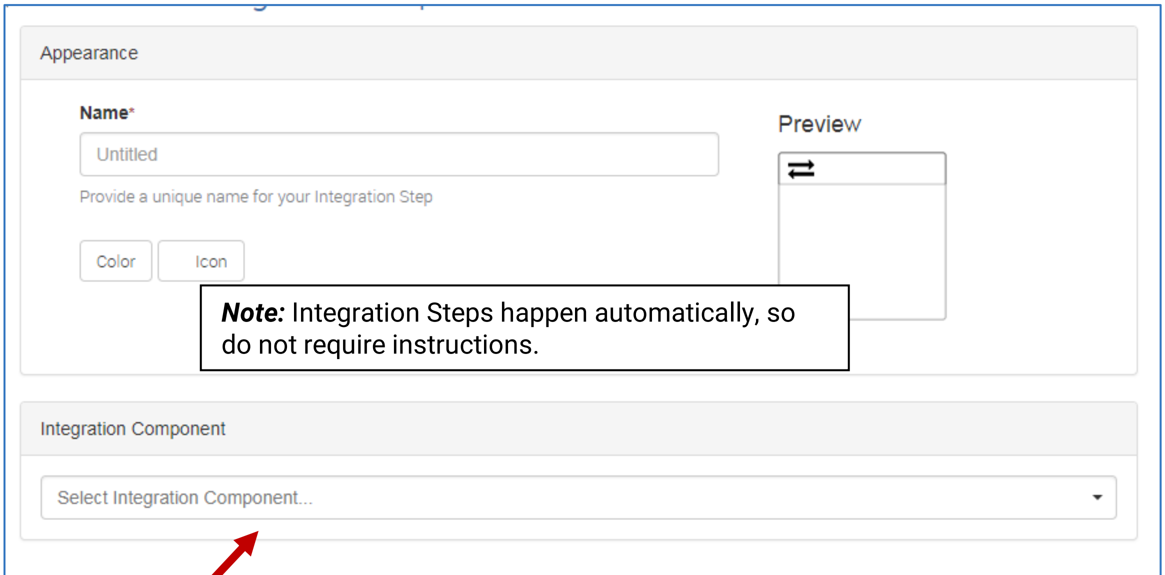
Use ***Insert Attribute*** to add atrribute data to the email.



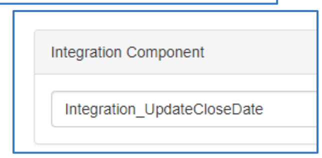
- **Integration Steps** initiate a change to an entity attribute.

For example, this type of step may generate a file that would upload into a CRM.

Appearance fields determine how the step will appear in the Plan Designer.



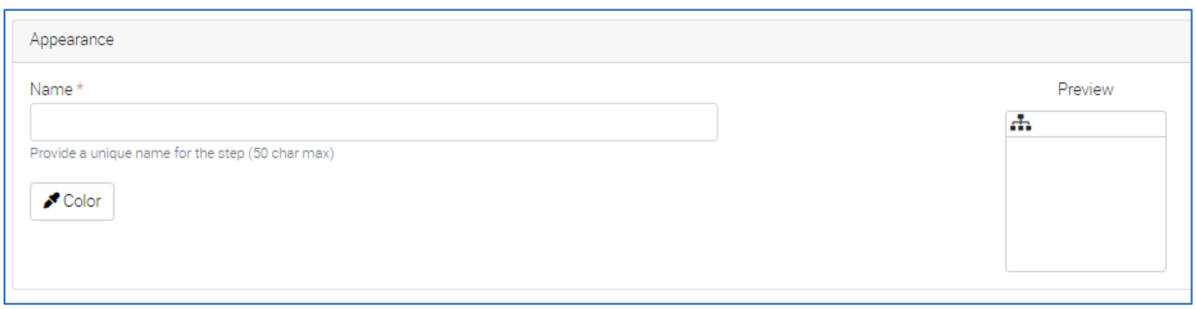
Integration Components are specially configured entity attributes. Select the appropriate one for the step being created.



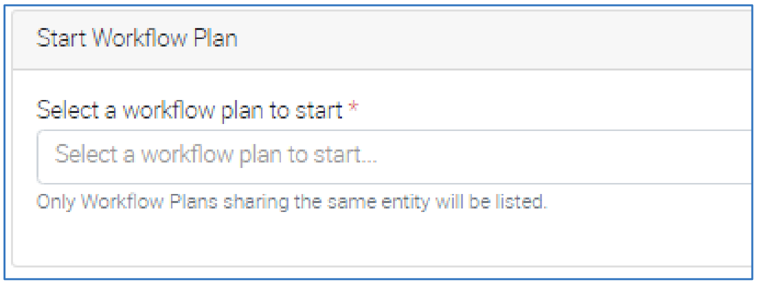
- **Start a Workflow Steps** launch a new workflow.

  Actions taken from a step of this type will start a separate workflow.

  Appearance fields determine how the step will appear in the Plan Designer.



Select a workflow plan to start by choosing the appropriate plan from the drop down list.

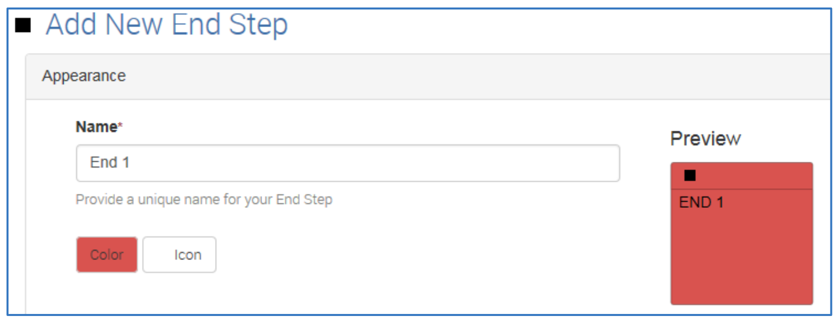


Note that only Plans that share the same entity will be offered.

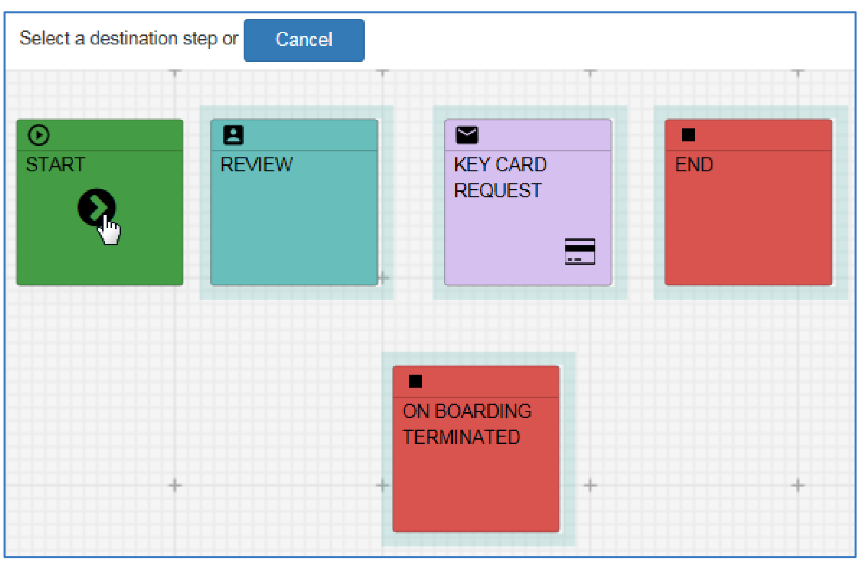
- **End Steps** end the workflow.

A plan can have multiple End Steps.

Appearance fields determine how the step will appear in the Plan Designer. The color will default to red, but can be changed.



Step 2: Connect Steps



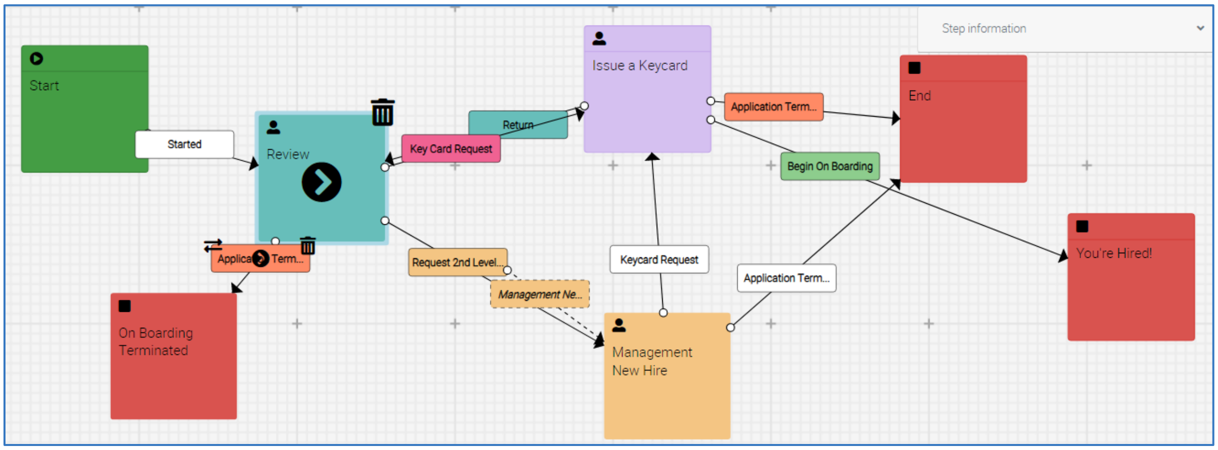
Click on the Step, then click the arrow that appears.

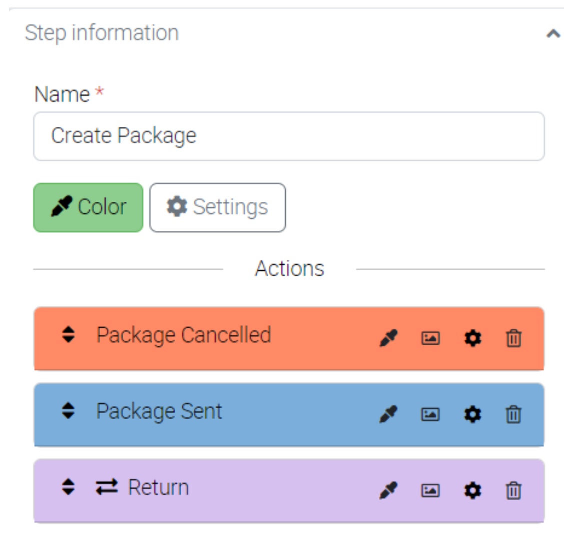
Select the Step that should follow in the workflow by clicking on it.

These connections form ***Actions***.

Step Actions

Actions connect steps and appear as buttons in the work items for the end user move items through the workflow.



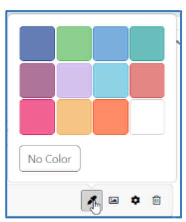


Step 3: Editing Actions

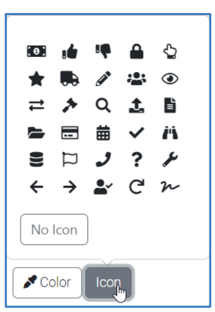
Click on the Step to access the *Step Information* Panel.

For each step Action on the Step, the following can be edited from this panel:

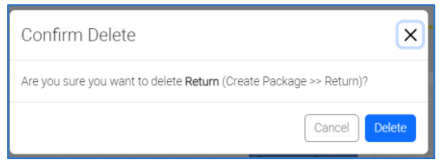
- **Re-order** Actions by dragging and dropping them.
- **Action Name**- click on the name to edit it.
- **Color** of the Action



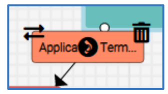
- **Icon** for the Action



- **Delete** Action



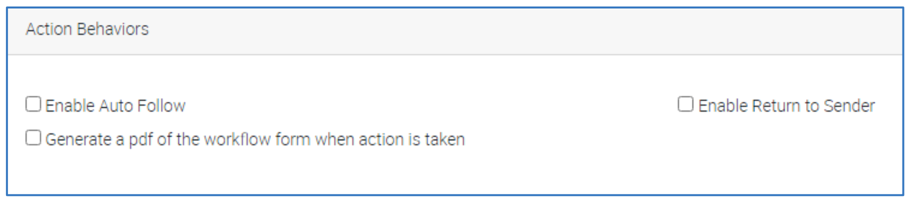
- **Move** an Action to another Step



    1. Select the Action on the Plan Designer.
    2. Click the Re-Route icon
    3. Select the new step where the Action will route the work items.

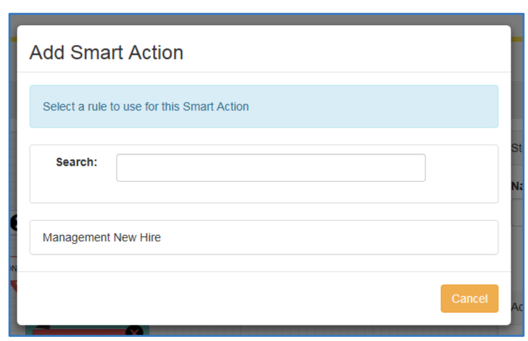
- **Additional Settings accessed through the gear.**

In additional to the above listed settings, the following Action behaviors can be be configured here:

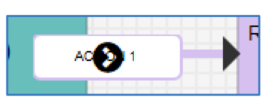


  - Turn on ***AutoFollow***: With AutoFollow enabled, if the User is the designated assignee for the item's next step, the item is automatically moved to the next step in the workflow, assigned to the user and displayed for continued processing.
  - Turn on ***Return to Sender***: With Return to Sender enabled, when the action is taken the item will be returned to the last user to interact with it. A dialogue box will present for a comment describing the reason for the return. The item will appear in their Inbox with a *Returned* badge and the comment will be added as a Note.
  - **Generate a PDF of the workflow form**: When the action is taken, a PDF of the Step's form will automatically be generated and archived and will be retrievable through Documents Search.

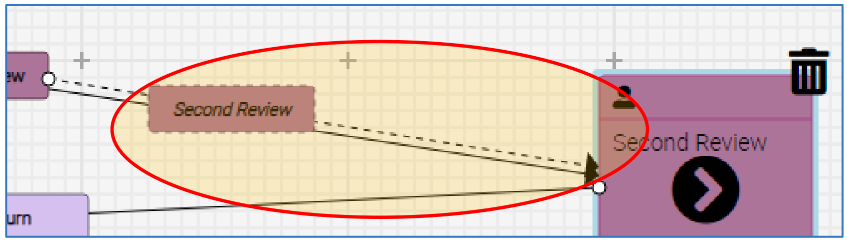
Smart Actions: Smart Actions are associated with Rules and allow items to move through steps in the workflow without user action. *See Creating Rules



1. Click on an existing Action to access the arrow and then select the Step that will follow the Smart Action.

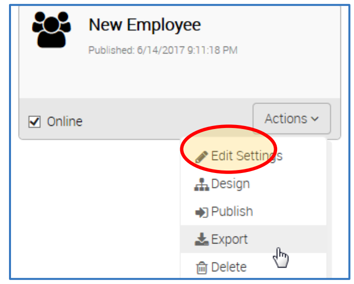


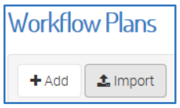
2. Select the Rule that will run this Action. The Smart Action will automatically save and retain both the original name of the Action and well as the Rule Name.



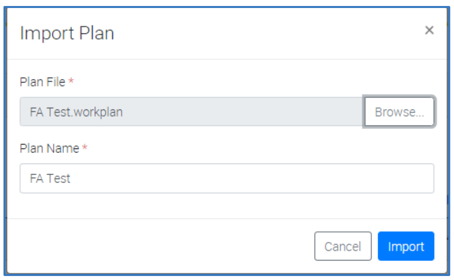
Importing & Exporting Workflow Plans

Existing Workflow Plans can be exported from an installation and imported into another; or re-imported as a copy/template into the same installation.

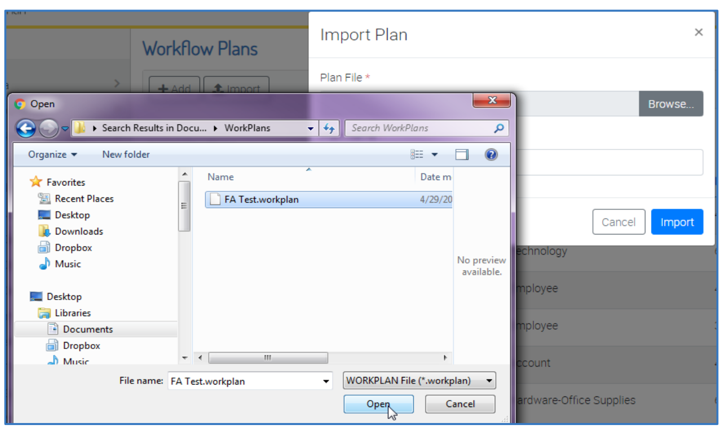




To import a workplan, select ***Import*** from the upper menu and select the workplan file then enter a Plan Name and click ***Import***.

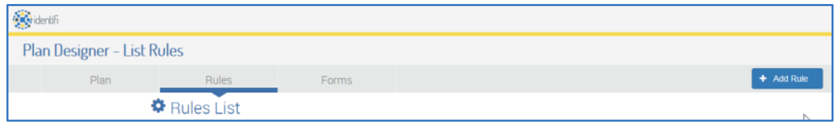


Note: *If importing to another installation, Entity Type, Attributes and Users/Groups must be same as the original installation or Workflow Plan will fail.*

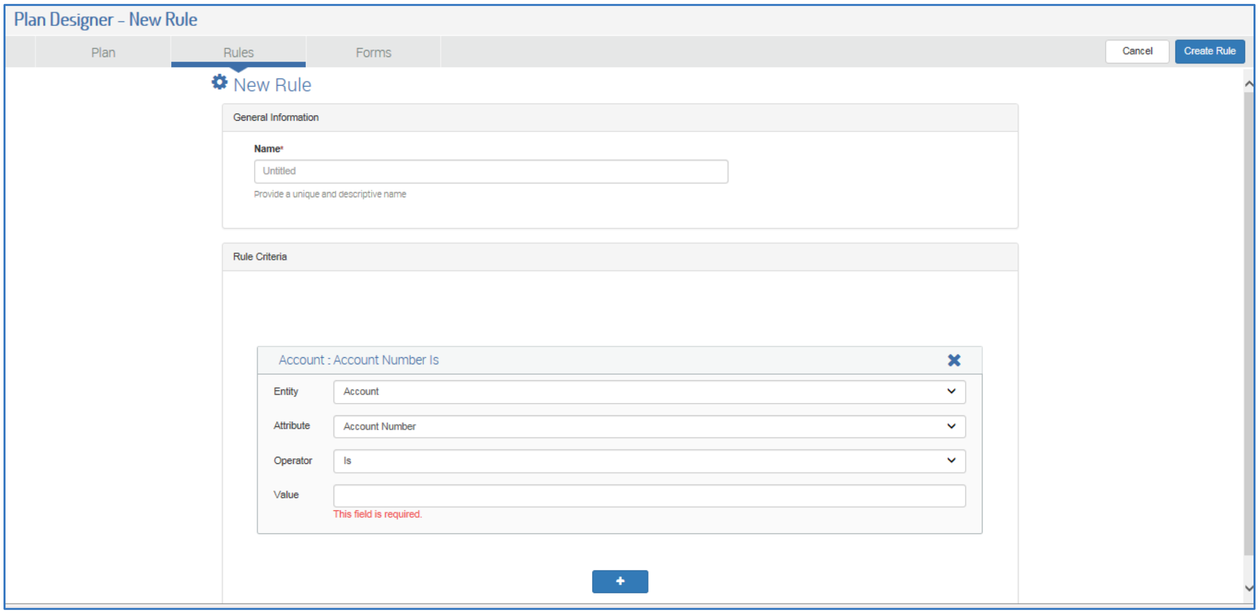


Creating Rules for Workflow Plans

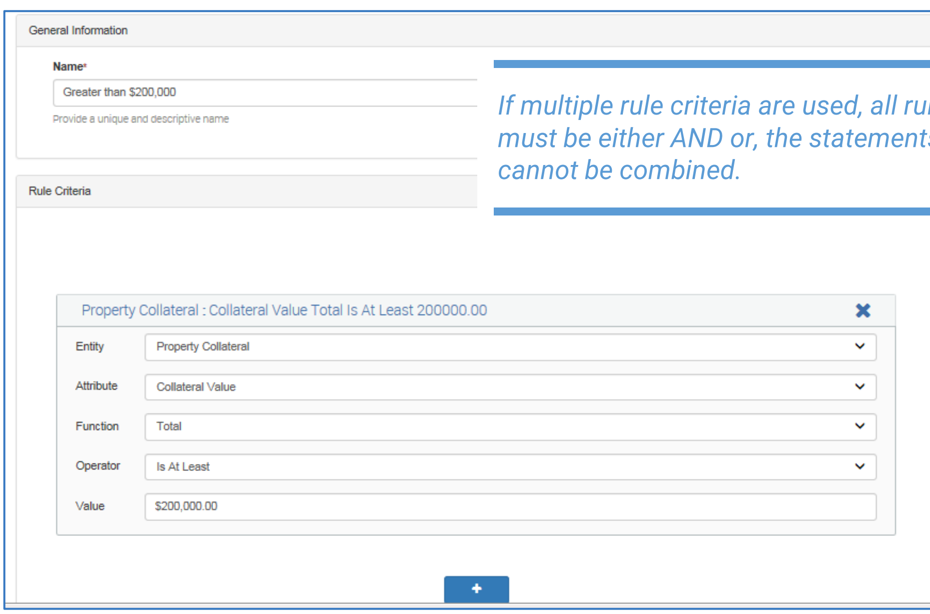
Rules are added under the ***Rules*** tab of the Plan Designer.



1. Click ***Add Rule***

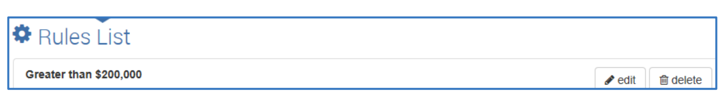


2. Enter a Name for the Rule and Rule Criteria: Entity, Attribute and Value information. Select the **plus** sign to add addition Rule Criteria.



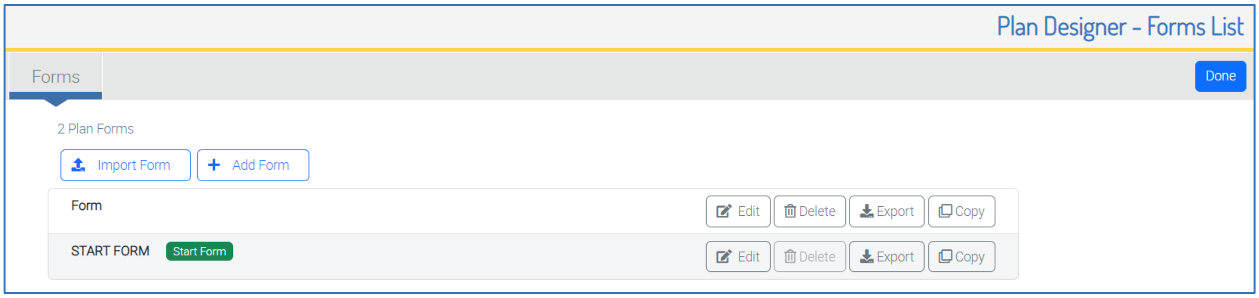
If multiple rule criteria are used, all rules must be either AND or, the statements cannot be combined.

3. When all criteria have been added, click ***Create Rule*** in the upper right corner. The rule can then be edited or deleted from the Plan's **Rules List**.



Creating Forms for Workflow

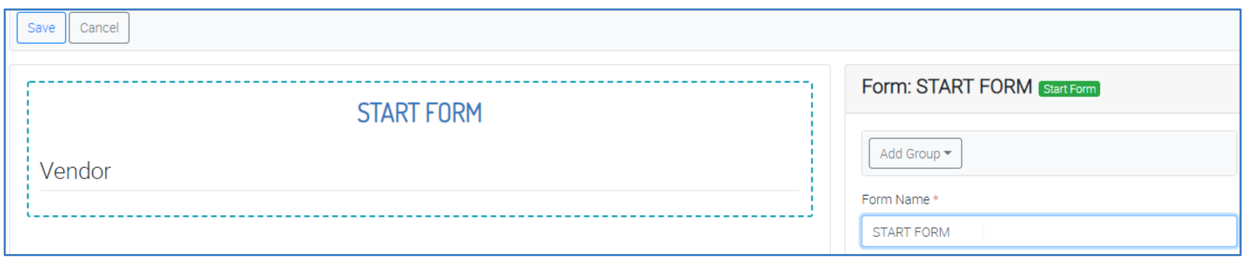
Forms are added under the ***Forms*** tab of the Plan Designer.   All Plans will have a default *Start Form* which should be configured and customized and will present when a Plan item is manually started.



Additional Forms can be created and can be associated with specific steps in the Plan.

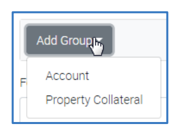
Modifying the Start Form

1. Select Edit to open the Form Designer.

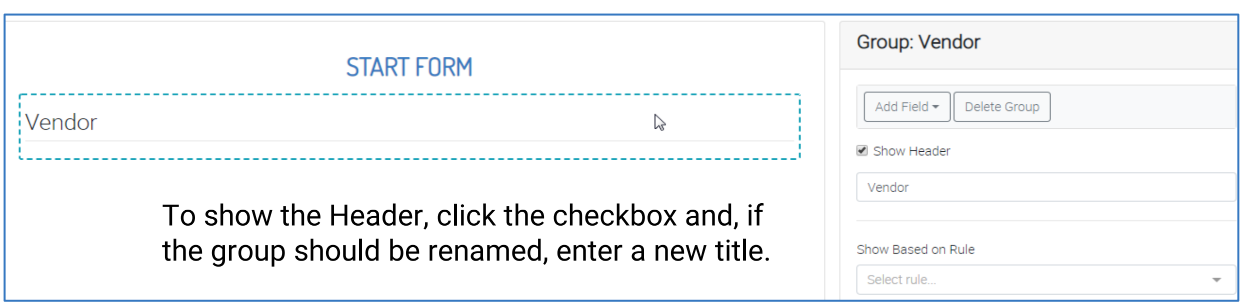


The form is titled ***Start Form***, but can be edited in the *Form Name* field.

The form will open ready to configure a group of attribute fields from the Plan's entity – if there is an entity related to that one, it will be available under the *Add Group* dropdown menu.

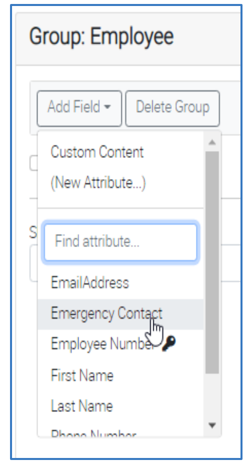


2. Click inside the Group area to begin customizing the fields on the form.

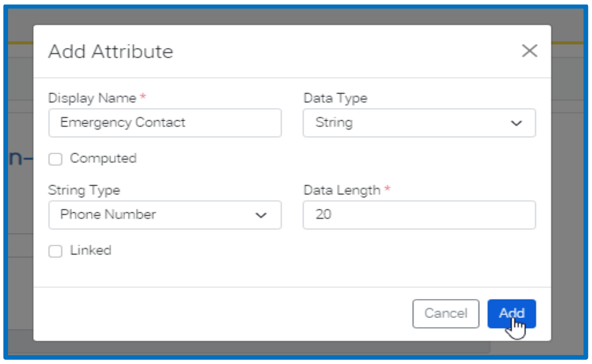


To show the Header, click the checkbox and, if the group should be renamed, enter a new title.

3. Next, ***Add Fields.*** The fields offered will be based on the attributes within the Group Selected.

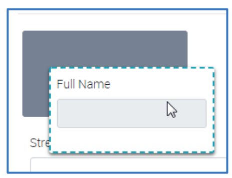


   - Select an existing attribute from the list.
   - New entity attributes can be configured directly from here to be used on the form.

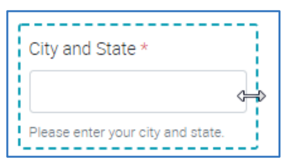


4. Fields can be modified in the following ways:

- **Reposition:** Drag to reposition

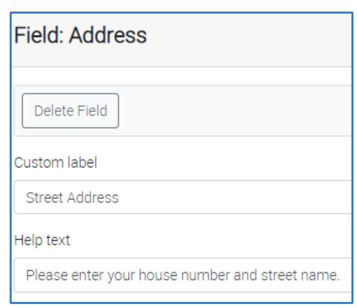


- **Resize:** Hover cursor and use arrows to resize

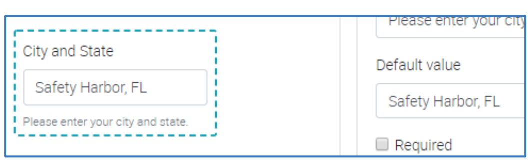


Note: *With the fields resized to their smallest dimensions, a maximum of 6 fields can be positioned in a single row.*

- **Custom Label:** Add a custom label and help text to make it the form clearer for users and customers.



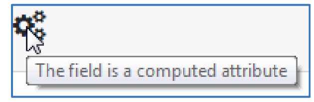
- **Set Default Value:** Populate with a default value if no other value is entered into the field.



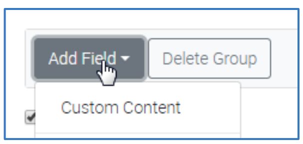
- **Required:** Set as required and prevent the Step from being completed without that field being populated.

- **Read Only:** Set as Read Only and prevent changes

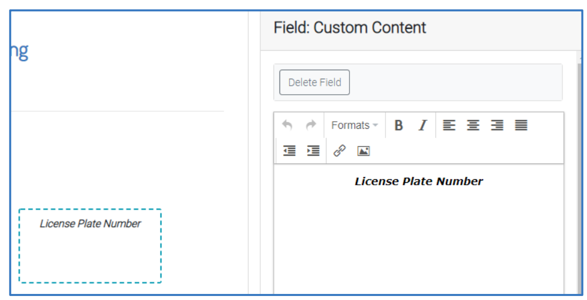
__Note:__ Computed Attribute fields will not have Default Value, Required or Read-Only settings available.



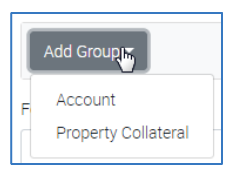
- **Create a New Field:** Select *Custom Field* and using the Rich Text Editor to create an entirely unique field.



__Note:__ Custom Fields can be used to add a company logo to the form. See __Adding a Logo to a Workflow Form__ in the Identifi Help Center.



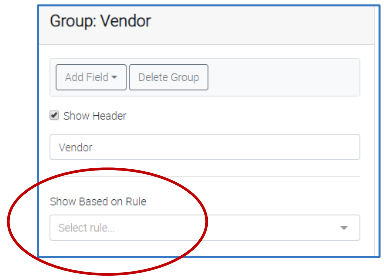
5. Additional Groups can be added by clicking outside the current Group's field area and then selecting ***Add Group*** again.

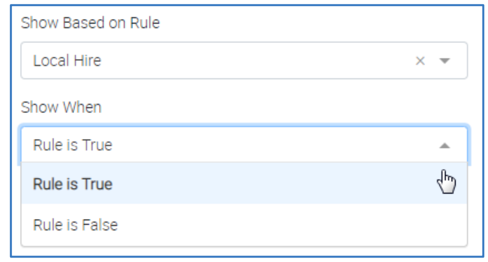


__Note:__ Multiple Groups will only be listed if there are Entities related to the one selected for the Plan.

Select the new Group and repeat the steps above.

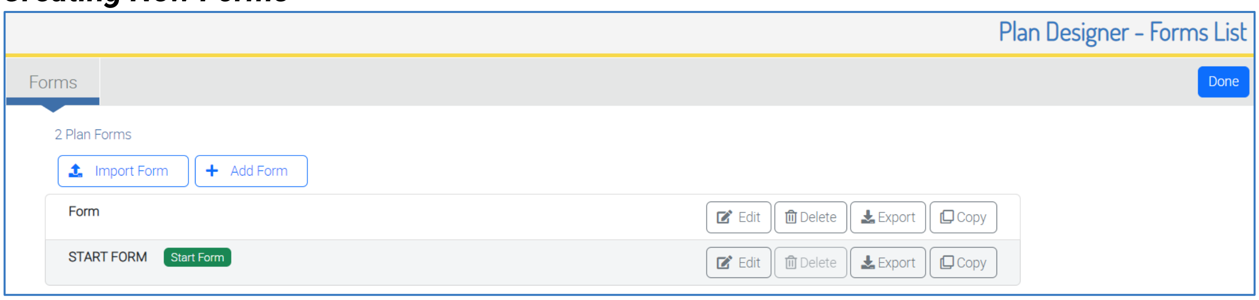
Note that Groups can be configured to show conditionally, based on Rules. *See Creating Rules





6. When all criteria have been added, click Save in the upper right corner.

Creating New Forms



1. **Copy an Existing Form** Copy: Selecting *Copy* on an existing form performs a 'Save As' and opens a copy of the form in the Form Designer for editing.

   Follow instructions for configuring Form Groups and Fields beginning on page 86.

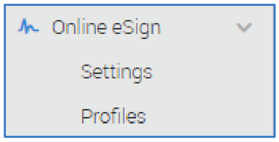
2. **Import a Form exported from another Plan** Import Form: Select *Import Form* to choose an exported form from another Workflow Plan. ***Note:*** Only forms exported from Work Plans based on the same entities of the existing Work Plan can be imported.

   Follow instructions for configuring Form Groups and Fields beginning on page 86.

3. **Add a New Form** Add Form: Select *Add Form* to launch the Form Designer and begin a new form from scratch.

   Follow instructions for configuring Form Groups and Fields beginning on page 86.

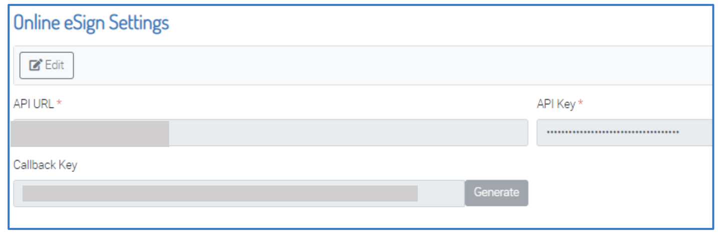
ONLINE ESIGN



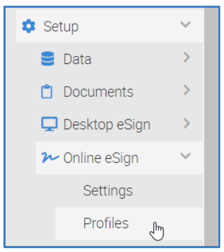
Users with the ***Administrator Role*** assigned to them have the ability to manage Profiles, and those that have the ***System Administrator Role*** are able to also access Settings.

Settings

Settings is where the installation's Online eSign API configurations are set. If assistance is needed with these settings, please contact Identifi Support.

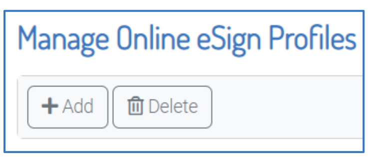


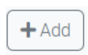
Profiles

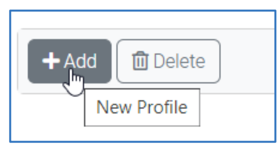


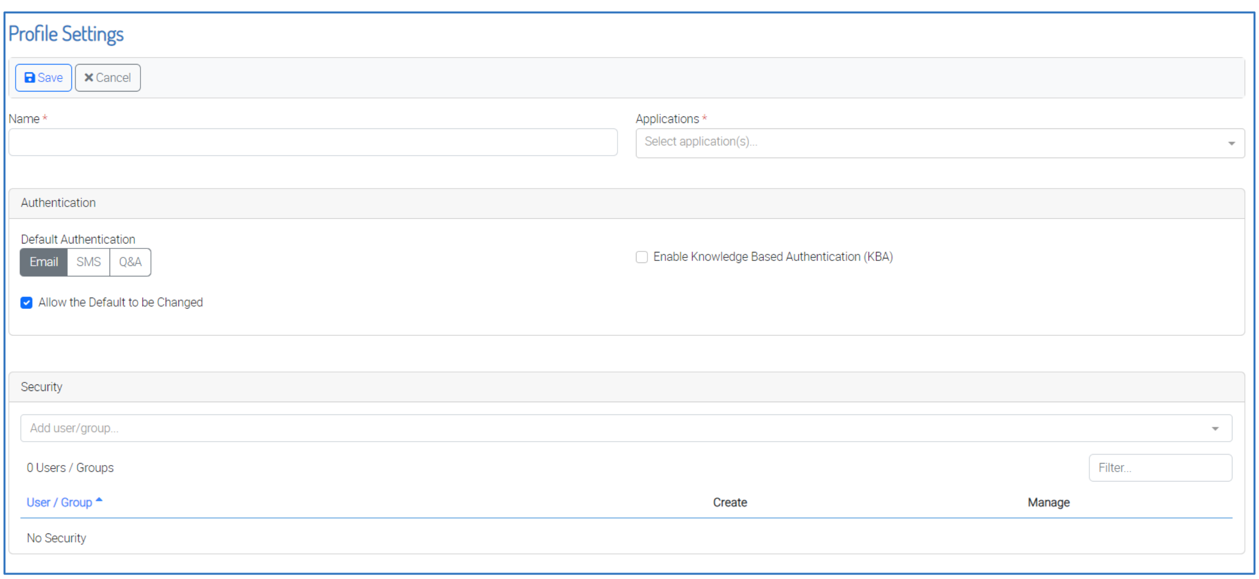
Profiles are configured to determine Application(s), Security and Authentication settings for Packages. A Profile is selected as the first step in creating a new Online eSign Package.

Adding a Profile



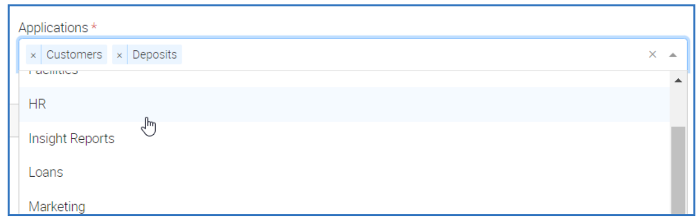
Click  in the upper menu.



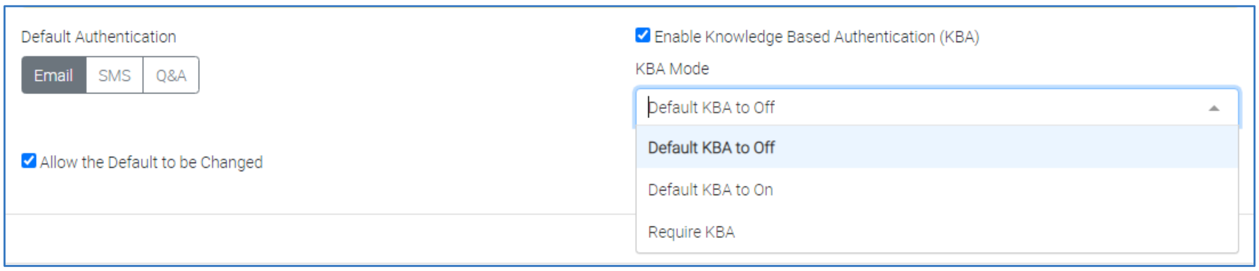


1. Enter a *Name* for the Profile.

2. Assign at least one *Application* to the Profile by selecting from the drop-down menu. ***Note:*** Multiple Applications can be selected.

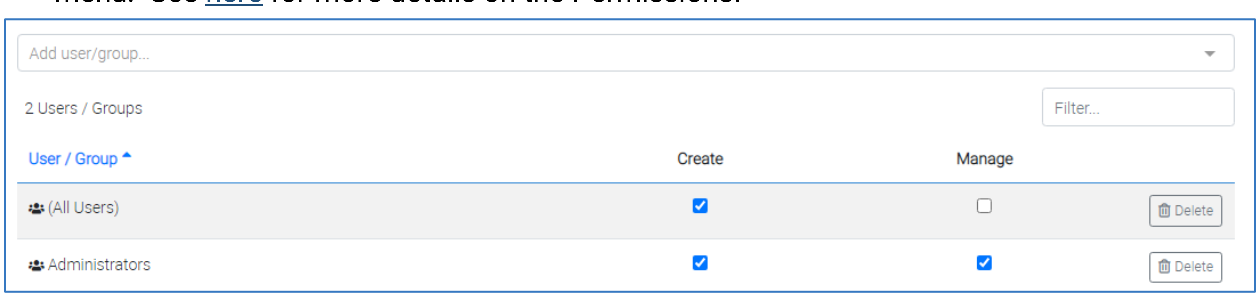


3. Choose a *Default Authentication.*

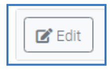


- With *Allow the Default to be Changed* checked, this can be overridden at the Package level. The box will be checked by default when creating a new Profile. With this option un-checked, all Packages sent using this Profile can only be sent using the Default Authentication selected.
- To use KBA with this Profile, check the box to *Enable Knowledge Based Authentication (KBA)* and then making the appropriate selection from the dropdown menu:
  - *Default KBA to Off*: KBA will be available for Packages sent with this Profile if desired. This will in addition to Email, SMS or Q & A authentication as well.
  - *Default KBA to On:* KBA will default as the authentication for Packages sent with this Profile, this will be in addition to Email, SMS or Q & A authentication as well.
  - *Require KBA:* Packages sent with the Profile must use KBA. This will be in addition to Email, SMS or Q & A authentication as well.

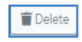
4. Grant access to use the Profile to Users and Groups by selecting them from the drop-down menu. See here for more details on the Permissions.

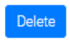


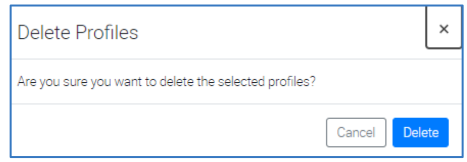
Modifying a Profile

Select a Profile from the list and click  to open the fields for changes. See Adding a Profile for details on the fields.

Deleting a Profile

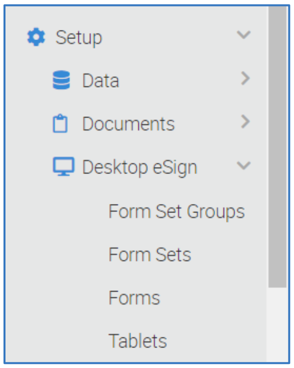
1. Click the checkbox next to the Profile and then select  in the upper menu.

2. Confirm by clicking  in the dialogue box that follows.



Note: If unsigned Packages associated with Profile are outstanding, a message will present and the Profile will not successfully delete.

DESKTOP ESIGN

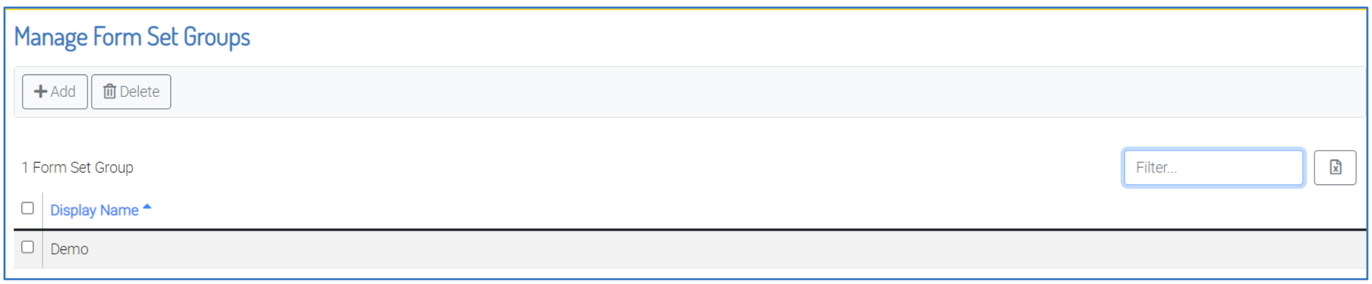


Users with the ***Administrator Role*** assigned to them have the ability to manage Forms, Form Sets and Form Set Groups.

Note: *Changes made to forms can affect the indexing of documents and potentially "break" Document Indexing. Proceed with caution and contact Support for assistance if unsure.*

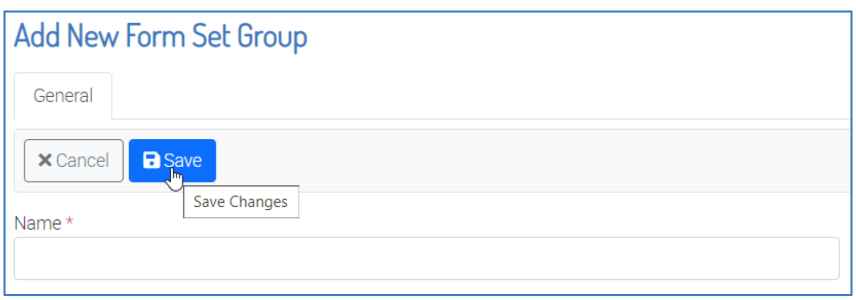
Manage Form Set Groups

Add new Form Set Groups and ***Delete*** or Modify existing ones.



Adding a Form Set Group

Click + Add and enter a Display Name and select ***Save*** when finished.

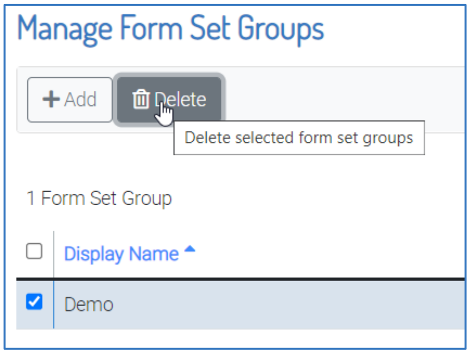


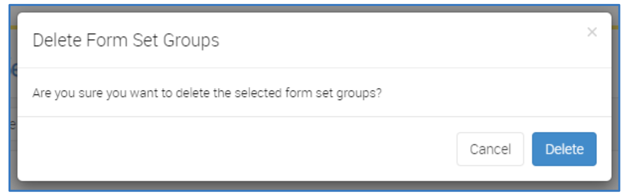
See ***Modifying a Form Set Group*** for how to add Form Sets to the new Group.

Deleting a Form Set Group

Place a checkmark next to the Form Set to be removed and select 

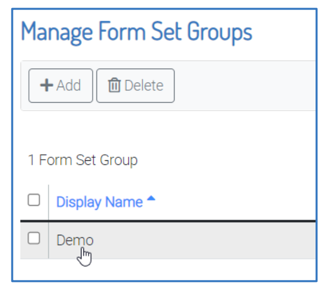
. Then confirm by clicking ***Delete*** in the dialogue box that is presented.





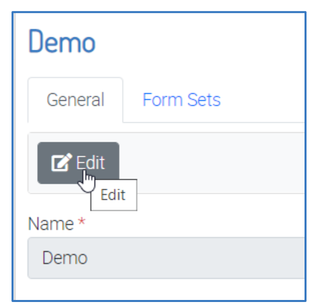
Modifiying a Form Set Group

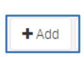
To make changes to a Form Set Group, click the title of the Group.



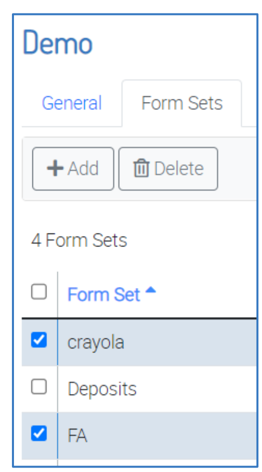
Under the ***General***, click 

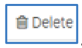
to modify the Display Name.



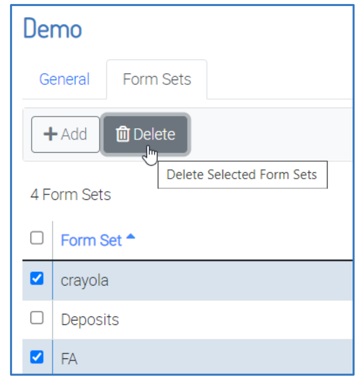
Under the ***Form Sets*** tab, click 

to add Form Sets to the Form Set Group. Place a check next to the sets desired and click ***Add***.

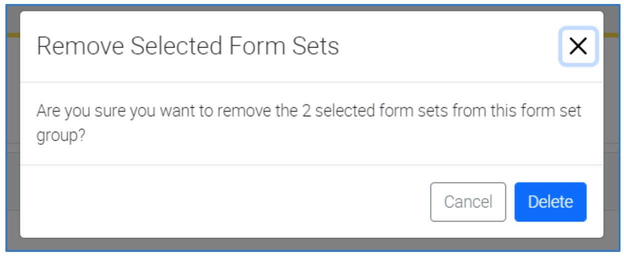


To remove Form Sets from the Group, place a check mark next to the Form Sets to be removed and click 

.

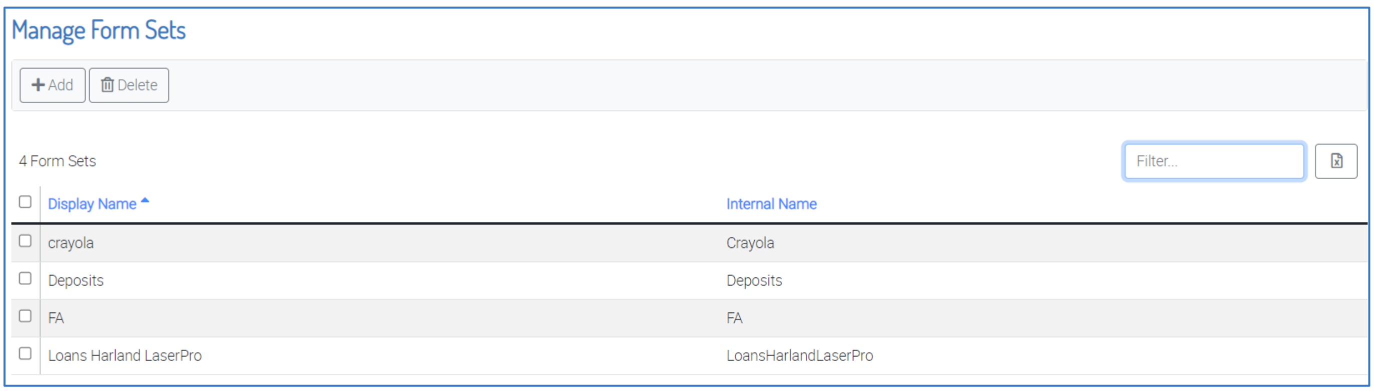


Then confirm by clicking ***Delete*** in the dialogue box that is presented



Manage Form Sets

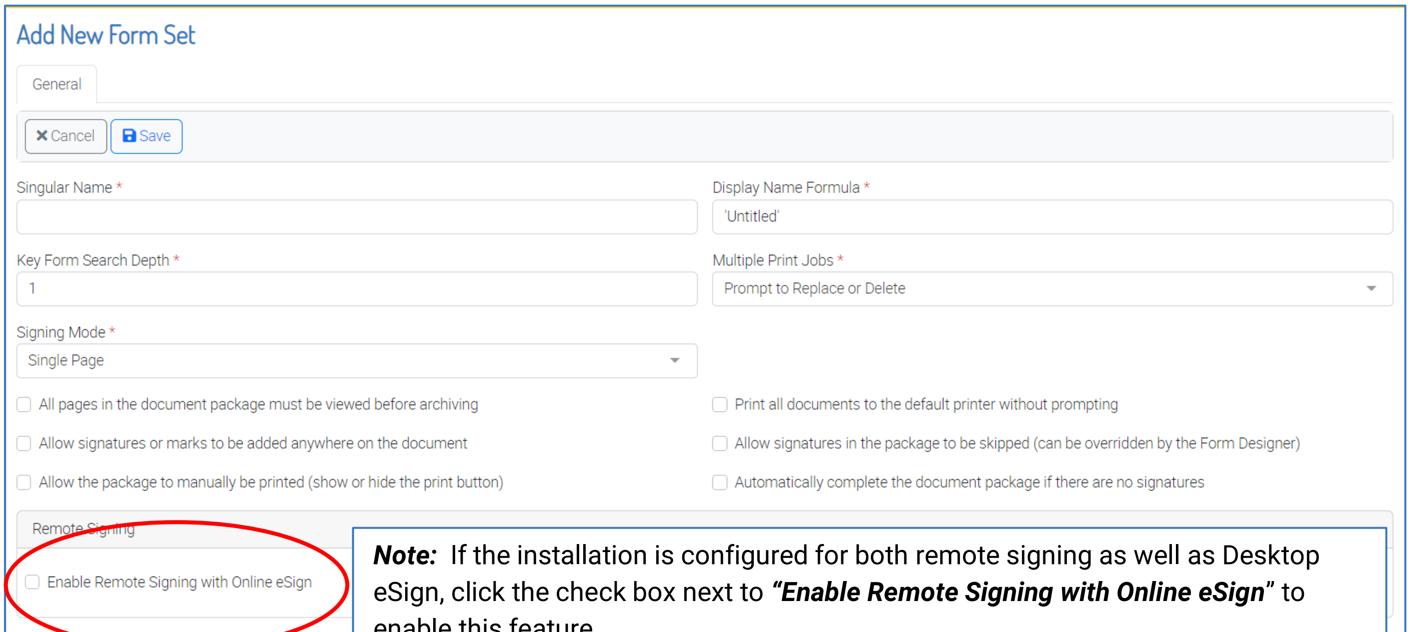
Add new Form Sets and ***Delete*** or Modify existing ones.



Adding a Form Set

Click + Add and fill in the required fields and place a check next to any applicable options. Select ***Save*** when finished.

See ***Modifying a Form Set*** for instructions on managing Forms and Attributes in the Form Set.



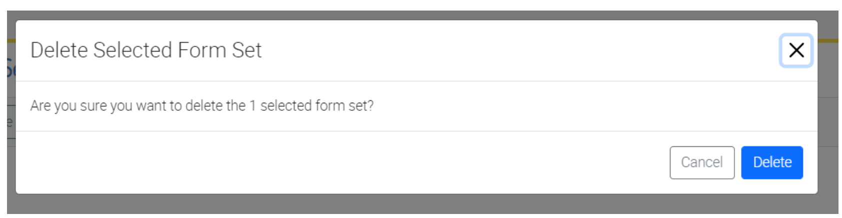
Note: If the installation is configured for both remote signing as well as Desktop eSign, click the check box next to ***"Enable Remote Signing with Online eSign"*** to enable this feature.

Deleting a Form Set

Place a checkmark next to the Form Set to be removed and select Delete.

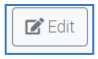
Then confirm by clicking ***Delete*** in the dialogue box that is presented.

Note: Any On Hold packages belonging to the Form Set will also be deleted.

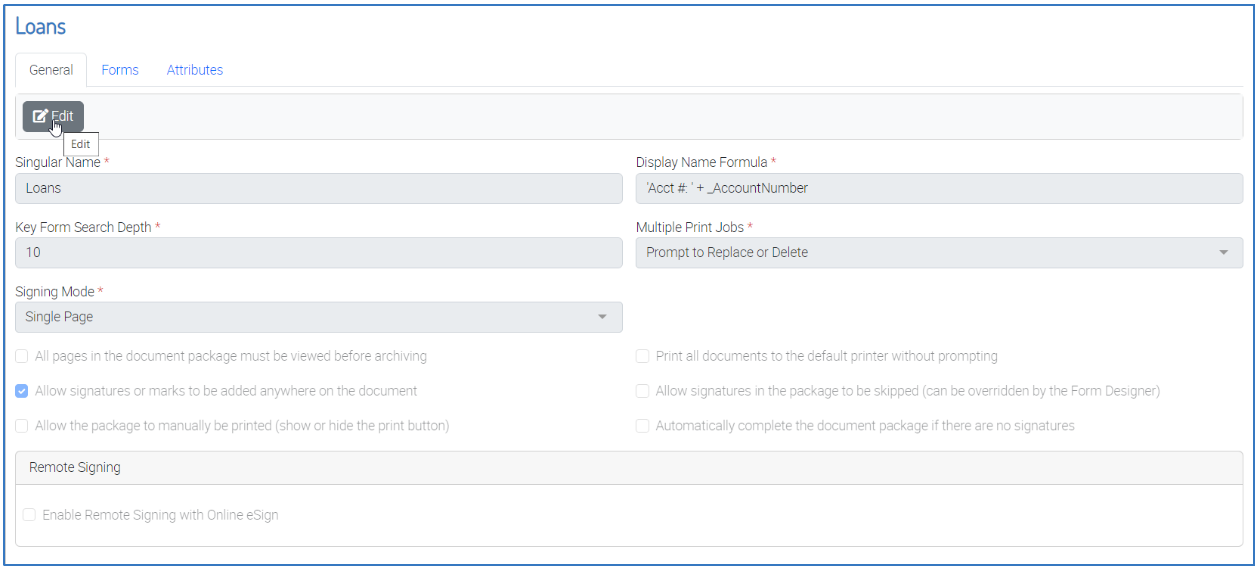


Modifiying a Form Set

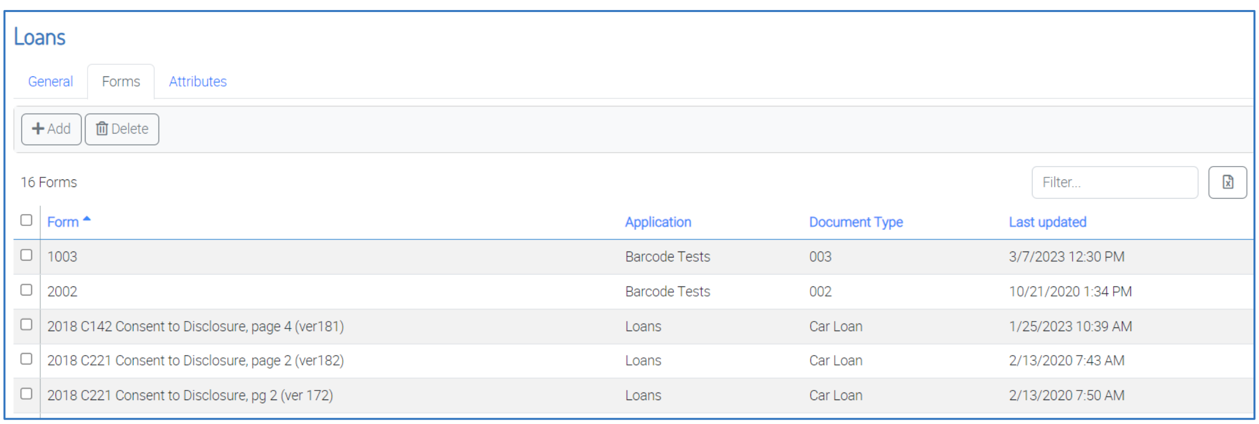
To make changes to a Form Set, click the title of the Set

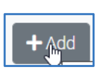
Under the ***General***, click 

to modify the Display Name Formula and other configuration settings for the Form Set.

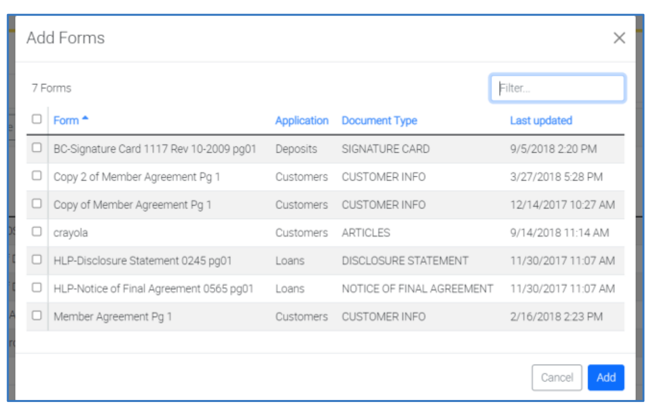


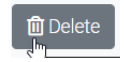
Under the ***Forms*** tab, Forms can be ***Added*** or ***Deleted***.

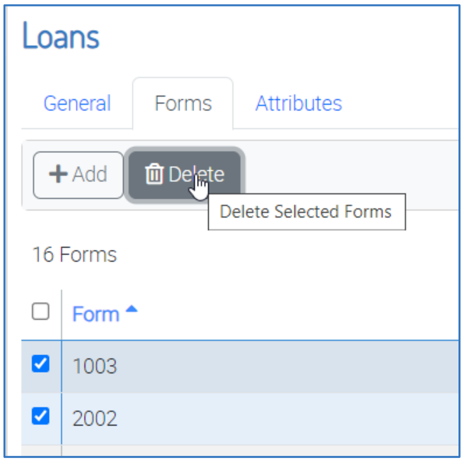


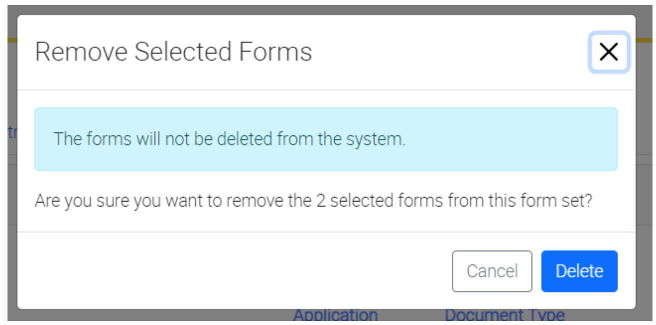
Click 

to add new Forms to the Set.



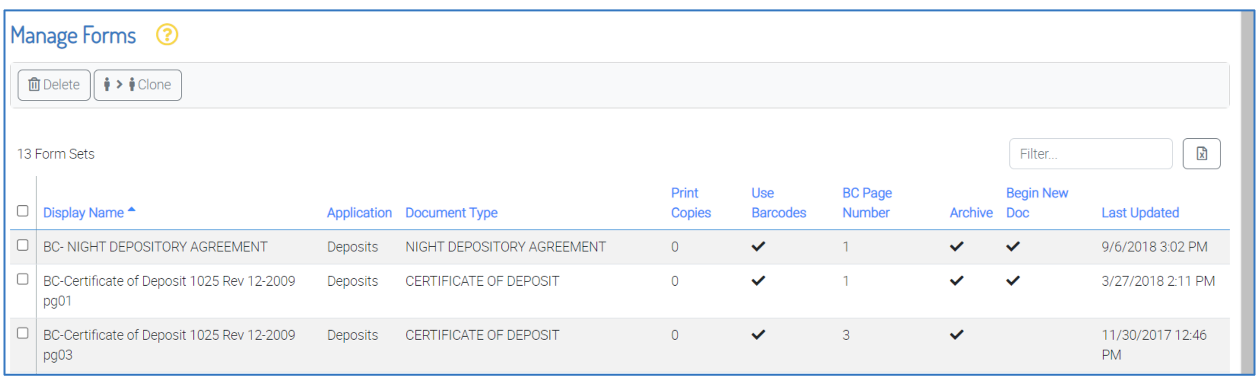
To delete, select a Form in the list by placing a check mark in the box; click  , and then confirm by clicking ***Delete*** in the dialogue box that is presented.



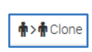


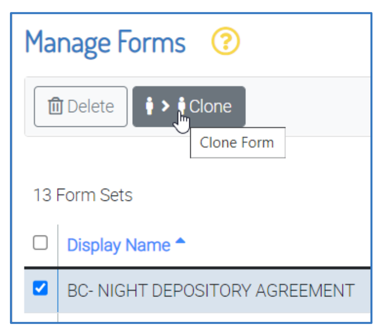
Manage Forms

Clone, ***Delete*** and Modify general details of Forms.



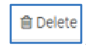
Cloning a Form

Place a checkmark next to the Form to be copied and select .

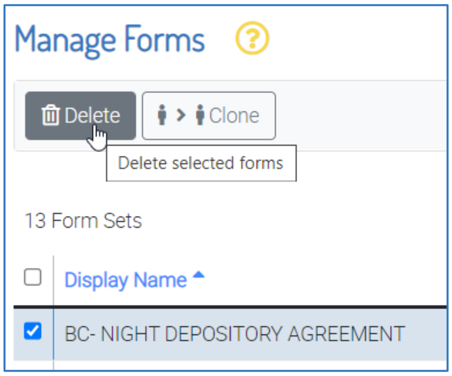


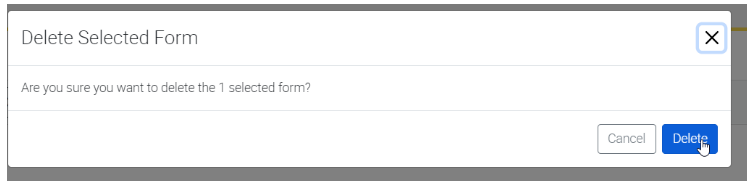
See ***Using the Form Designer*** for instructions to edit the new form.

Deleting a Form

Place a checkmark next to the Form to be removed and select .

Then confirm by clicking ***Delete*** in the dialogue box that is presented.

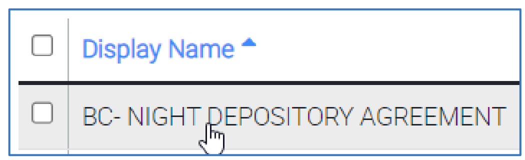




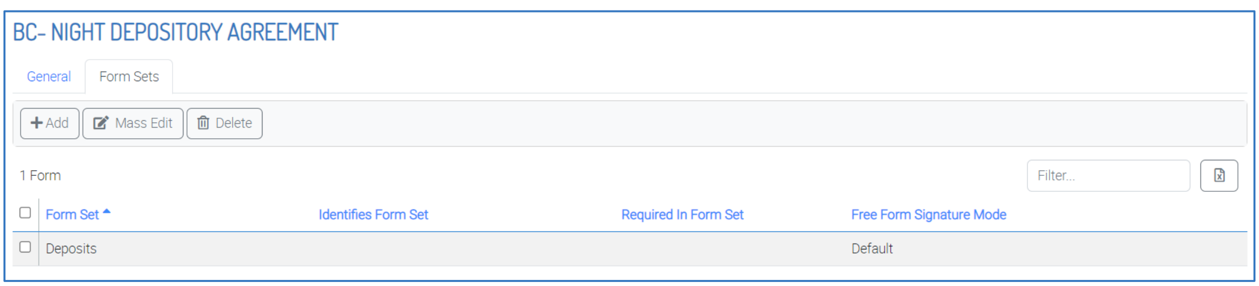
Modifiying a Form

To make changes to the Form itself, see [***Using the Form Designer***.]

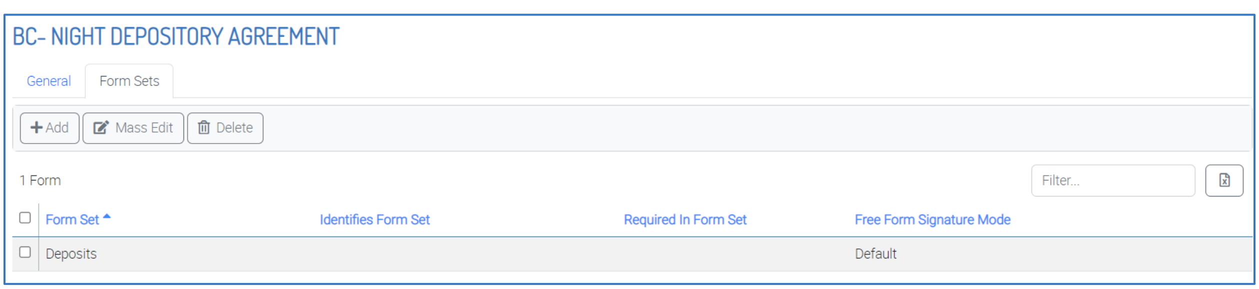
To modify a form, click its title,

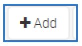


Under the ***General***, view the details of the Form.

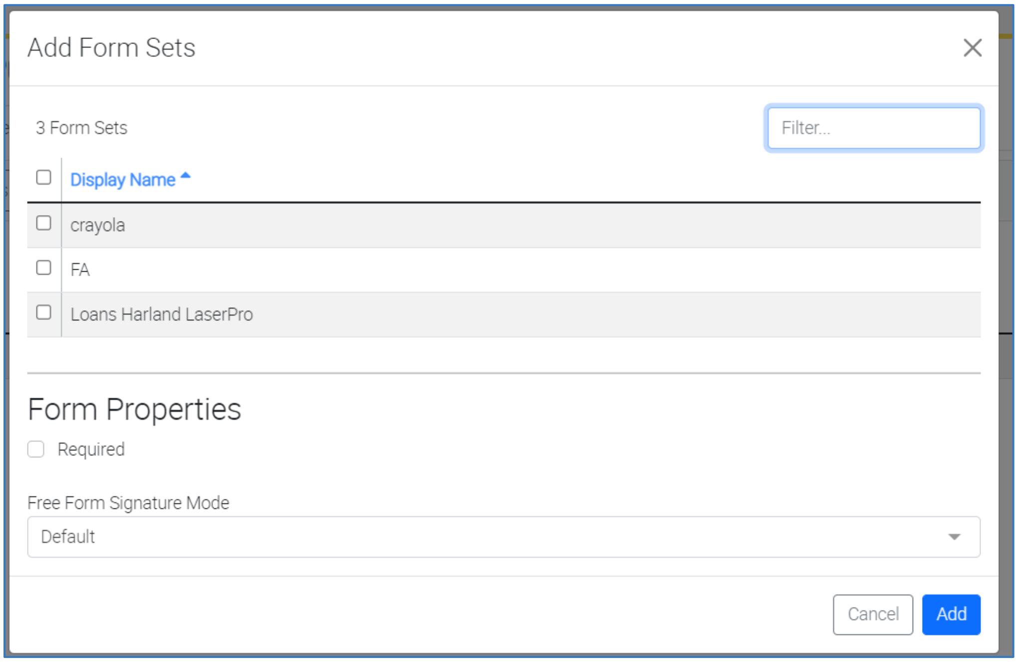


Under the ***Form Sets*** tab, Forms can be ***Added*** to or ***Deleted*** from Form Sets. ***Edit*** allows the behavior of that form within a set to be modified.



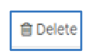
Click 

to add the Form to a Form Set.

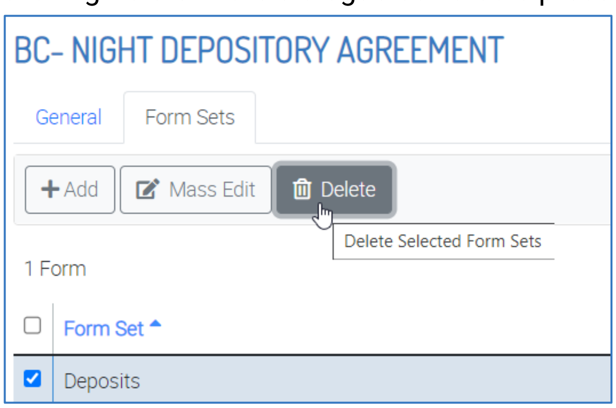


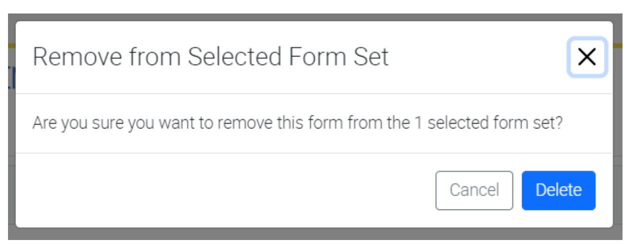
Place a checkmark at ***Required*** if this form will be required in the set.

Select the ***Free Form Signature Mode***.

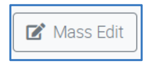
Place a checkmark next to a Form in the list to be removed and select 

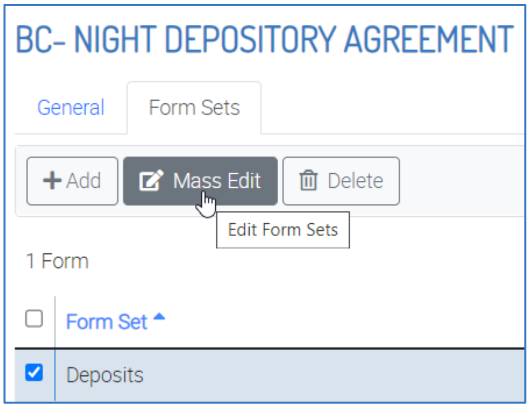
then confirm by clicking ***Delete*** in the dialogue box that is presented.

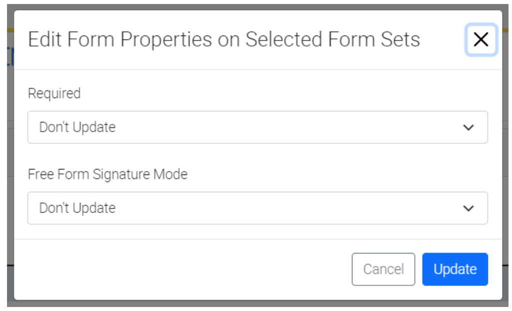




Place a checkmark next to the Form(s) in the list to be edited and select .

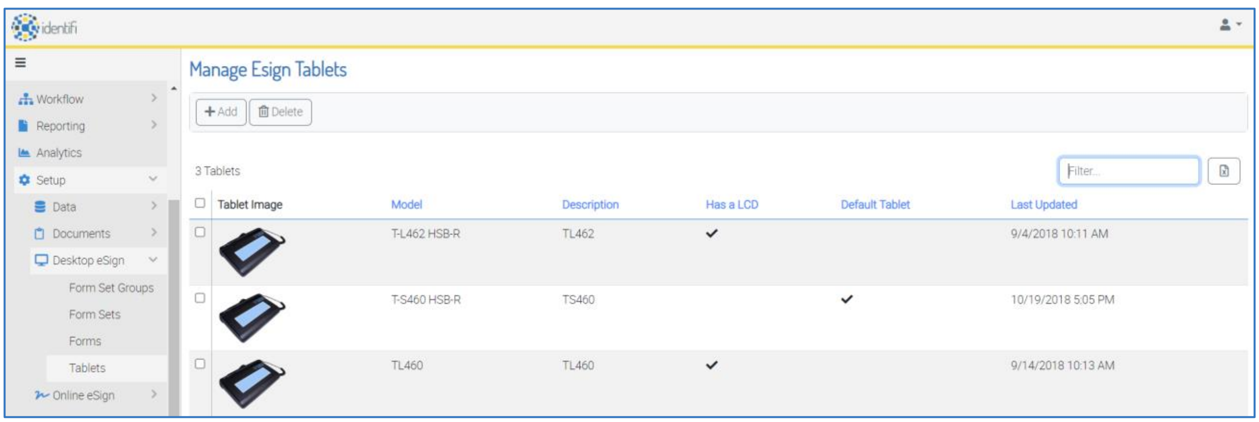
Here, the behavior of the form within the Form Set can be changed. 



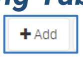


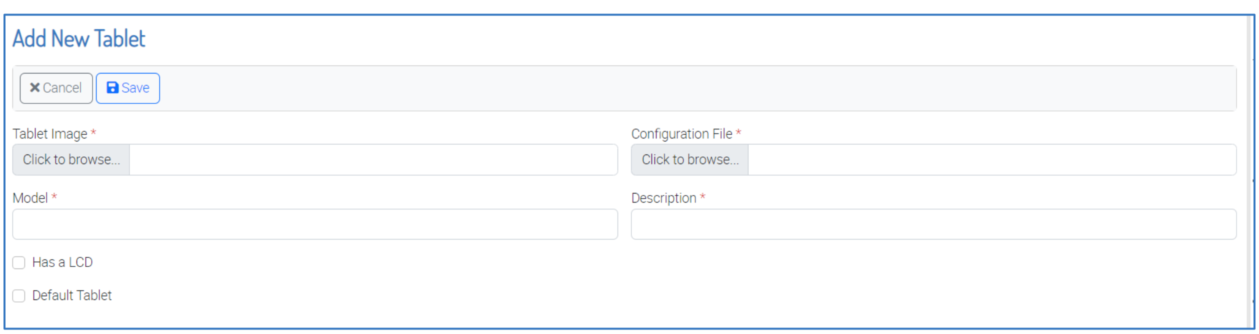
Managing Signing Tablets

Add, ***Delete*** and Modify tablets and their settings.



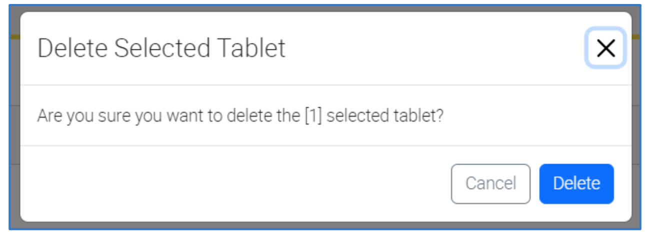
Adding Tablets

Click  to add a Signature Tablet. Fill in the required fields and select **Save.**



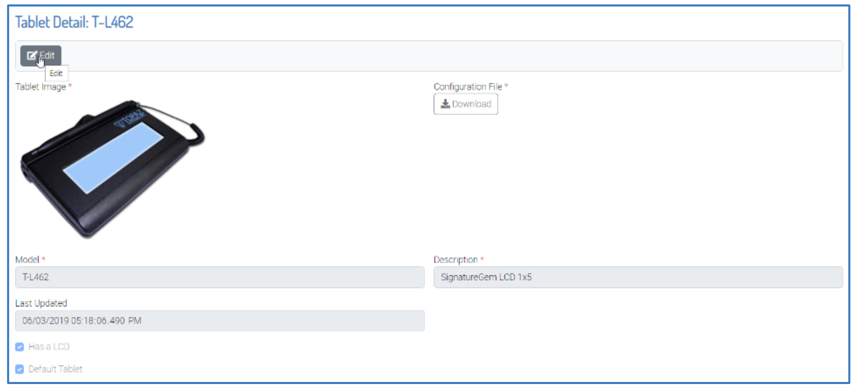
Removing Tablets

Place a checkmark next to the tablet that should be removed and select Delete. Then confirm by clicking ***Delete*** in the dialogue box that is presented.

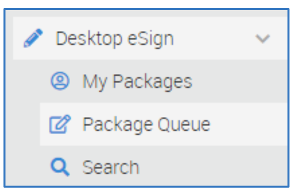


Modifying Tablet Settings

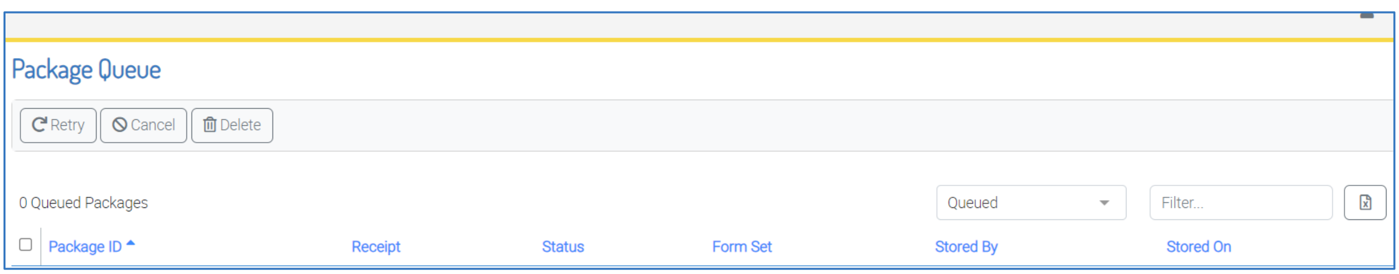
Click the title of the Tablet that should be changed, then select Edit to open the fields for editing.



Managing the Package Queue

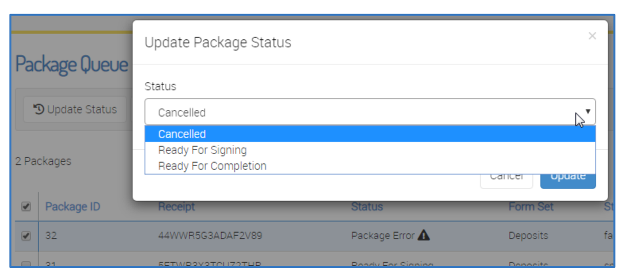


Any packages that do not complete successfully are found here; only Administrators will see this area in the menu.

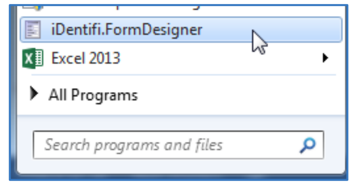


To resolve the package, place a check in the box next to the Package ID and then click ***Update Status*** and select the appropriate status from the dropdown menu.

*These statuses are all searchable through ***eSign Search***.



Using the eSign Desktop Form Designer

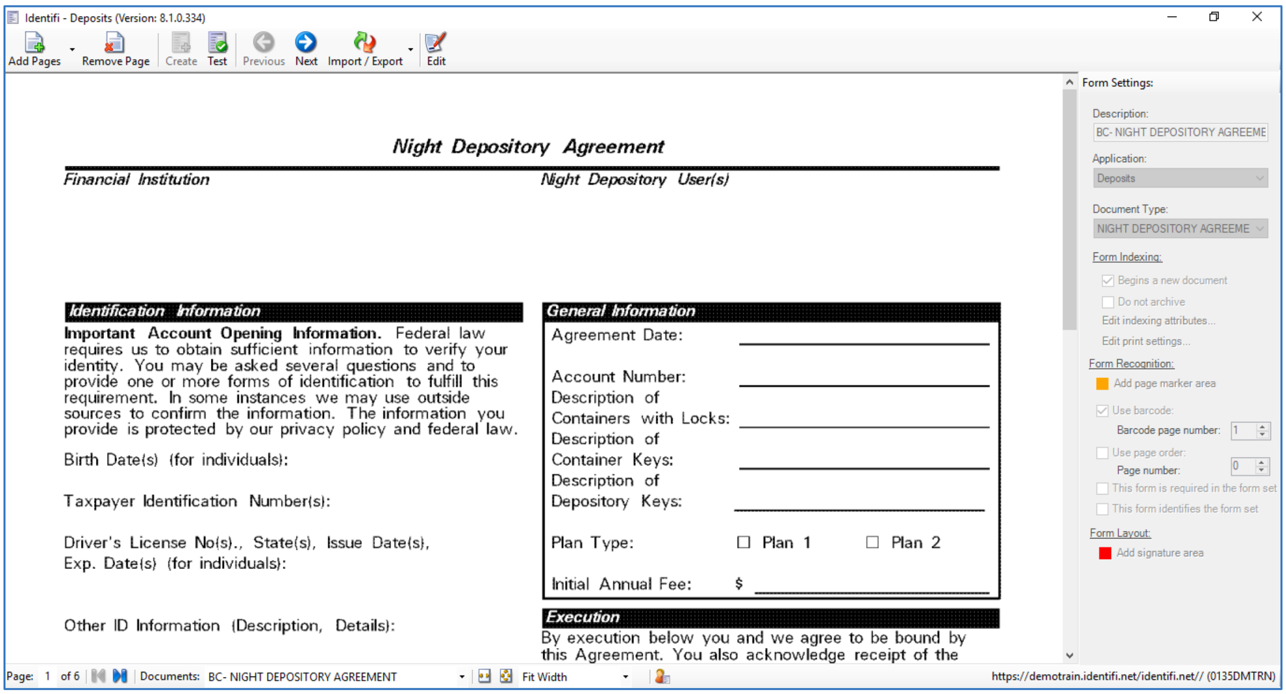


Documents are added and configured as forms in the eSign Form Designer.

Note: For client installation instructions click here.

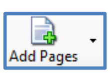
Launching the Form Designer

To launch the Form Designer, navigate to the PC's Start Menu  and locate it in Programs.

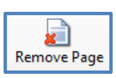


Navigating the Form Designer

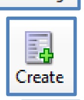
Upper Menu Bar



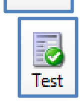
Add forms to the Form Set. Either TIFs/PDFs



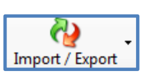
Remove forms from the Form Set



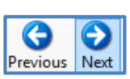
When new pages have been added, add form to the new page.



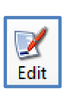
Launches the eSign Client in order to view the documents and ensure that the pages are being recognized, barcodes read and signature areas correctly placed.



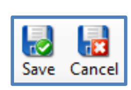
Import or Export forms belonging to the Form Set.



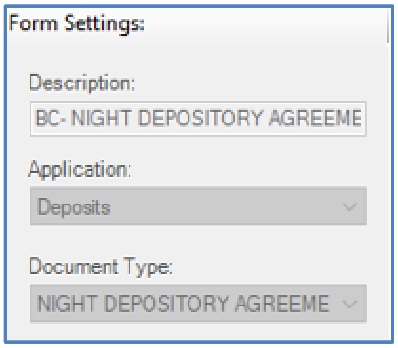
Navigate between forms, and their multiple pages, in the Form Set



Allows changes to be made to the form. Click ***Save*** to keep the changes or ***Cancel*** to discard them.



Right Side Bar

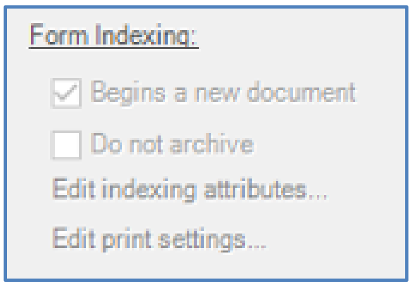


Form Settings:

Description- The form’s name. *See below for best practices*

Application: Application to which the document will be archived

Document Type: Document Type to which the form corresponds



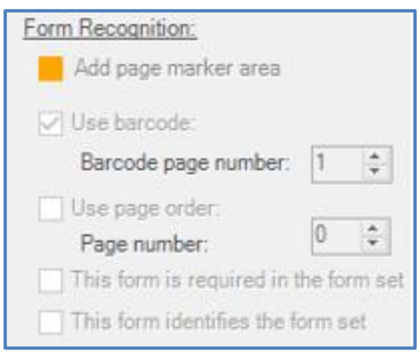
Form Indexing:

Begins a new document- select to indicate the first page of a document

Do not archive- document image will not be archived

Edit indexing attributes- set required attributes for indexing. *Best Practices*

Edit print settings- configure number and format of copies *Best Practices*



Form Recognition:

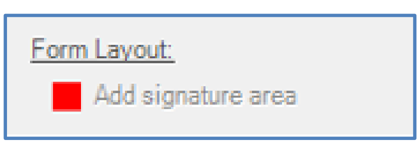
Add page marker area- allows the user to use the mouse to mark a unique area of the document to be used to identify the form *Best Practices*

Use barcode- select this if the document barcoded, then indicate the page number the barcode is found on

Use page order- select if the form should be identified by page order

This form is required in the form set- select to indicate the form is required in the set

This form identifies the form set- select if the form identifies the set



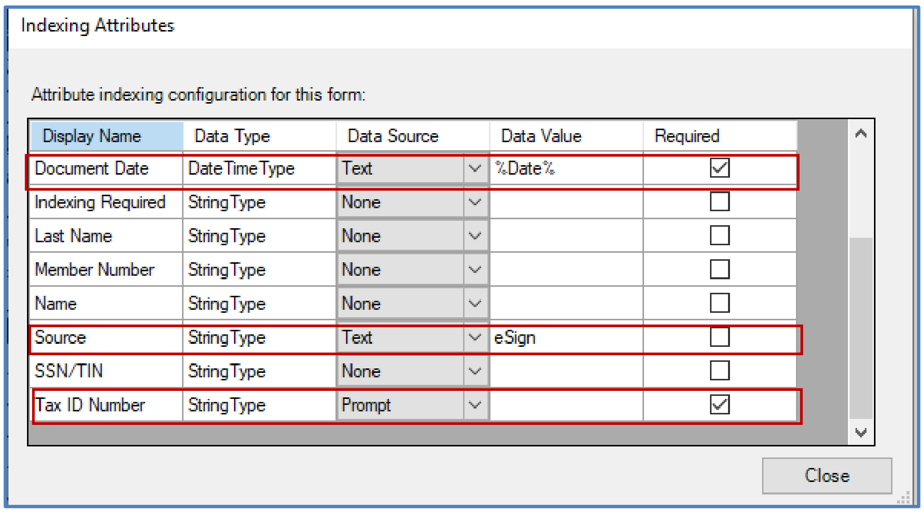
Form Layout:

Add signature area- clicking here allows the user to draw signature areas on the document using the mouse. For details on how to configure a signature area, see *Best Practices*

Desktop eSign Form Configuration Best Practices

- ***Form Name Recommended Format***: *BC* (if the document is barcoded), Document Type Name, Barcode Value (if Barcoded), *REV* Revision Month-Year and page number. ***Example*- BC Certificate of Deposit 1025 REV12-2009 pg01**

- ***Attribute Settings Recommendations:*** Attributes set with a Data Source of **Prompt** must be entered before the Package can be completed. This data can be entered manually or passed from the barcode. Any attributes marked as ***Required*** for the Document Type that the form represents will automatically be set as **Prompt.**



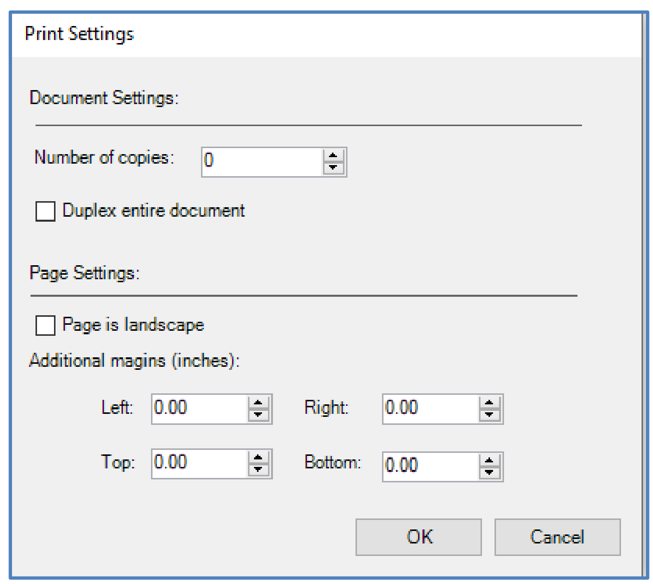
Example Setup

Document Date = *Text*

Source = *Text* ('eSign')

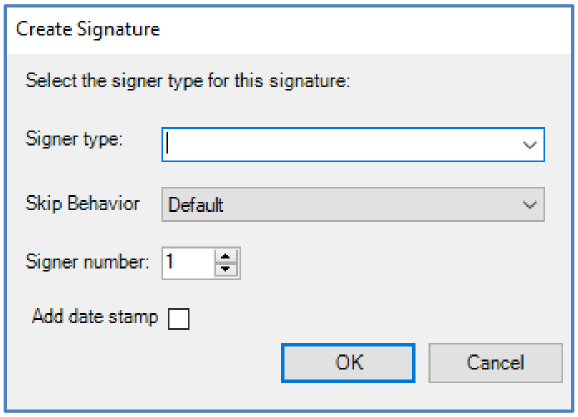
Account #/Tax ID = *Prompt*

- ***Print Settings***: These settings determine document are printed from eSign, either at the completion of a package or using the ***Print*** button within the eSign Client. The settings are limited by the capability of the attached printer.



- ***Page Marker***: A recommended area of the form to select for the *Page Marker* is the form's title. Draw the marker area, then right-click and select ***Enable Search Region.***

- ***Adding and Modifying Signature Areas:*** Once the Signature Area has been drawn, make the following selections in the dialogue box:

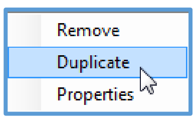


Signer Type –The first time a new signer type is used, it must be typed in, after that it will be available from a drop-down menu. Other examples are *Spouse, Employee, etc.*

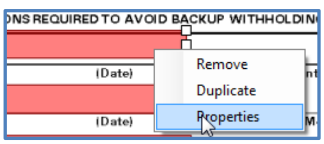
Skip Behavior –*Default*, *Skip Allowed* or *Require* (all signature areas must be Signed or Skipped to place the package on Hold or Complete) *Default* is standard.

Signer Number – Identify the Signer Number this box is being configured for, i.e. Signer 1, Signer 2, Signer 3…

Add date Stamp –Applies time/date stamp to signature



Create additional signature areas by right-clicking on one already configured and selecting ***Duplicate***. These new signature areas can then be dragged into place on the form.

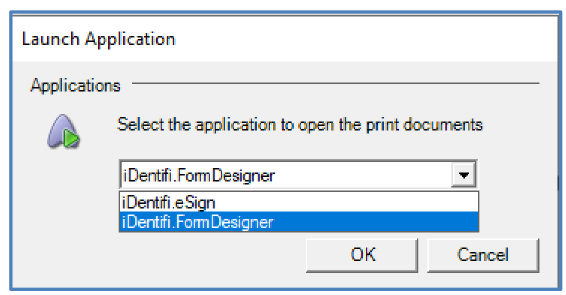


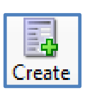
These settings can be modified for existing signature areas by right-clicking the signature area and selecting ***Properties***.

.

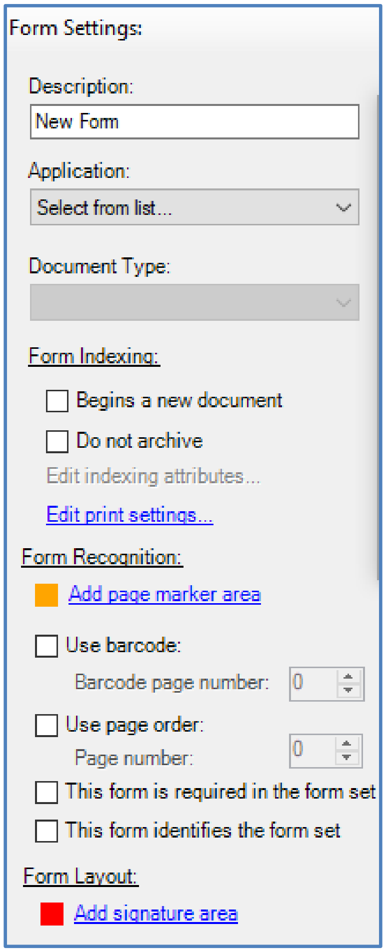
Adding Forms

When the ***Capture documents from the Identifi printer*** icon is present in the lower menu of the Form Designer, documents (.tif, .jpg and .pdf) can be 'printed' to the eSign Printer. When prompted, select the eSign Form Designer and the forms will open in the Designer for configuration.



Click 

Create in the menu bar to open the right menu for editing.



For each new form, the following menu items must be addressed, see [Navigating the Form Designer](#) for details:

Form Settings: -including *Description, Application* and *Document Type*

Form Indexing: - including where the document begins, its archive behavior, indexing attributes and print settings.

Form Recognition: -including page markers, barcode details, page order and required and/or identifying forms

Form Layout: - including signature areas.

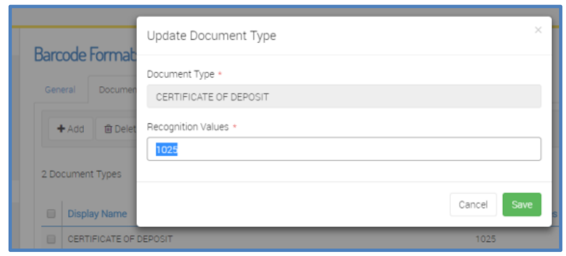
Click Complete ***Complete*** and the Form Set Designer will close.

*Note: **Page 1** must be configured for each form; however subsequent pages need only be configured if they contain a signature area.*

“Grabbing” TIFs

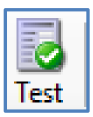
New forms can be created by ‘grabbing’ .tif images:

1. Print the form to eSign, but do not proceed with eSign when the client opens and prompts for the type and number of signers.
2. Open the *C:\Users\%username%\AppData\Local\Temp* folder
3. Move the TIF image to the eSign template folder and rename it for easy identification.
4. ***Cancel*** and ***Close*** eSign when complete.



<u>For Barcoded Documents:</u>
Add the Barcode ID to the Barcode Format under the *Setup-Imaging-Barcodes* menu.
Select the Barcode Format from the list and then, under the Document Types tab, add the Barcode ID in the Recognition Value field.

Testing New Forms



Once all new forms have been added, it’s best to test them. Select ***Test Form Set*** from the upper menu inside the Form Designer. The forms will ‘print’ to eSign so that the form recognition, signature areas and barcodes can be assessed for accuracy.

Importing/Exporting Forms

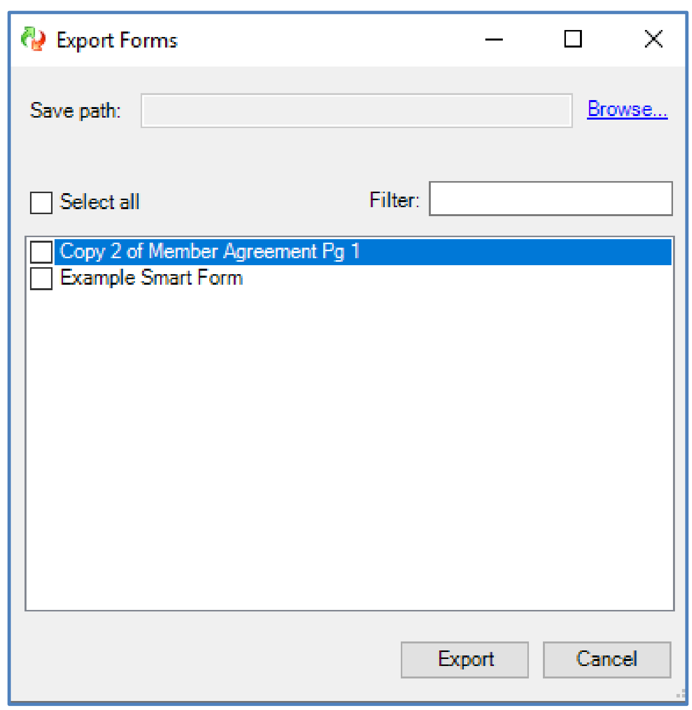
Forms can be exported from the Form Designer.

Exporting Forms

Select ***Export*** from the **Import/Export** dropdown menu.

Choose which forms in the Form Set are to be exported and where they will be saved.

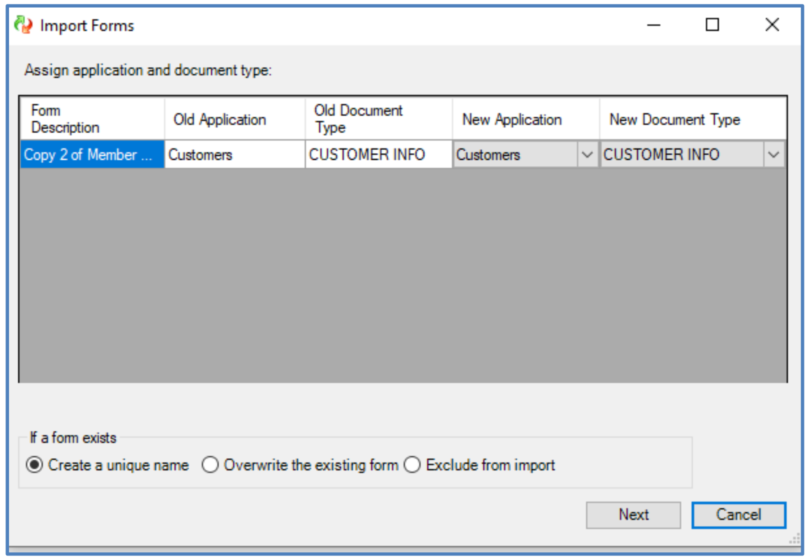
Click ***Export***.

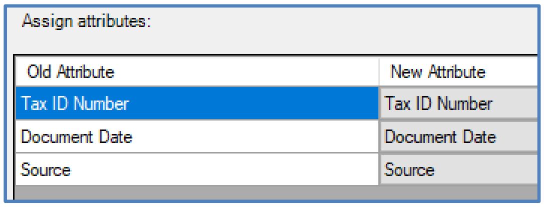


Importing Forms

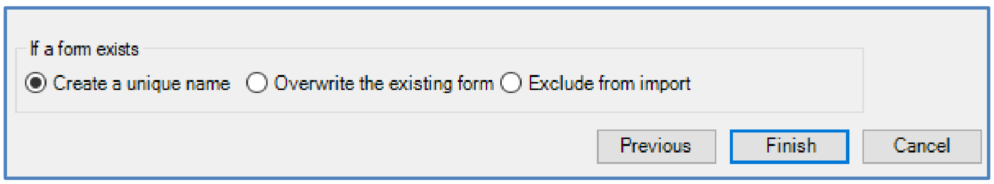
Select ***Import*** from the **Import/Export** dropdown menu.

Make any necessary changes to the Form Description, Application and Doc Type and click ***Next.***





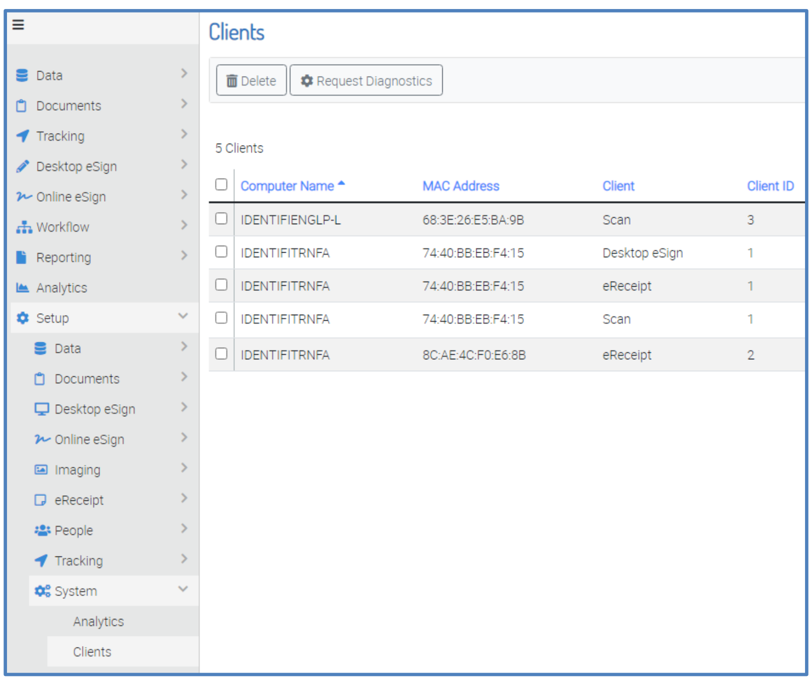
Then, once the last 3 radio buttons have been addressed, click ***Finish.***



Managing Desktop eSign and eSign Form Designer Clients

The clients are downloaded and managed under the ***System*** menu.

Clients:

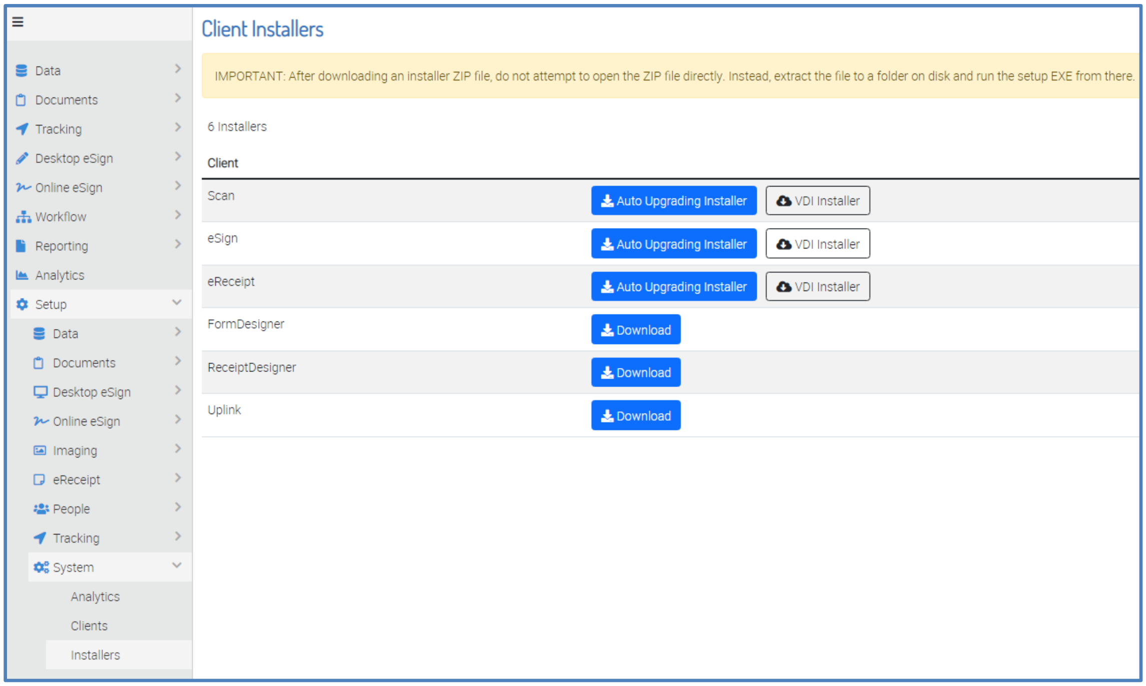


A list of all installed eSign and Form Designer Clients can be viewed here. Those that are not needed can be removed from this screen as well.

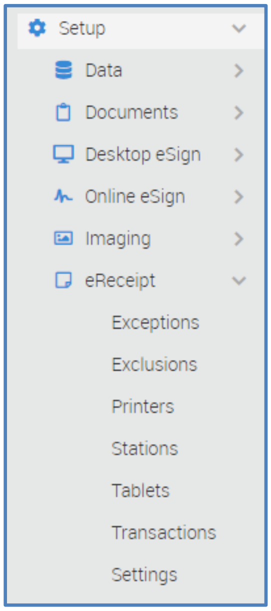
For more details: Setup-System- Clients

Installers:

The Installers for the Desktop eSign Client and Form Designer are downloaded for installation and deployment from here. For more details: [Setup-System- Installers]



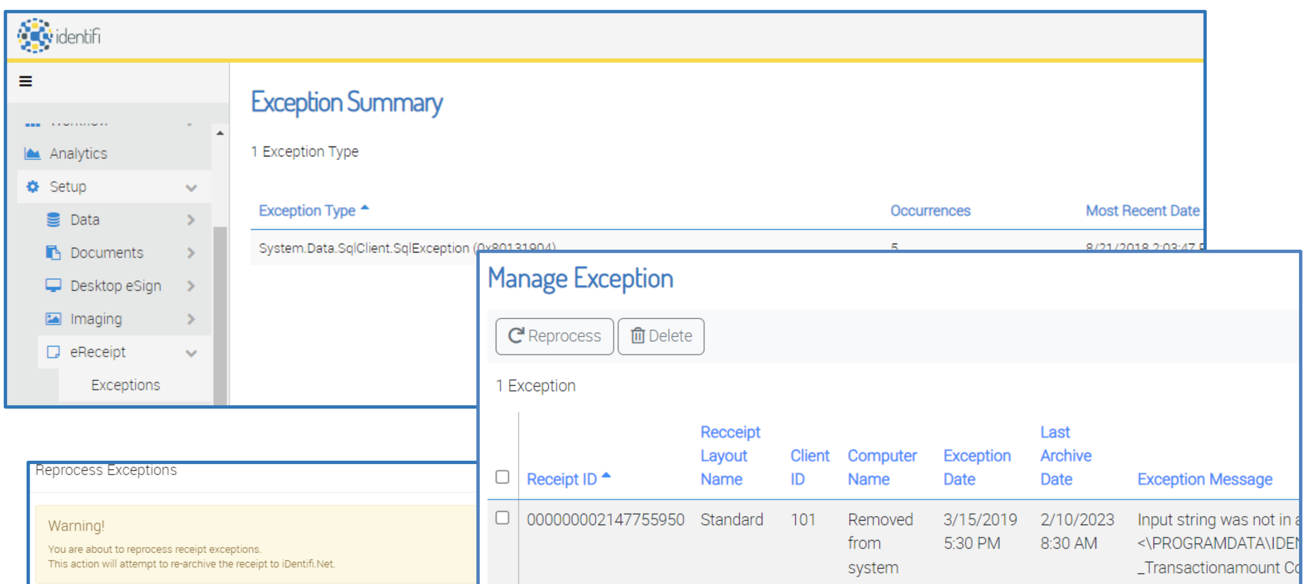
ELECTRONIC RECEIPTS

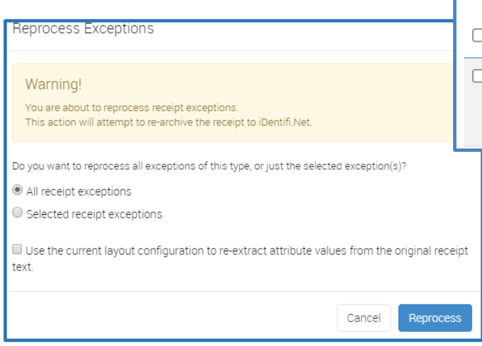


Users with the ***Administrator Role*** assigned to them have the ability to manage all aspects of the Receipts module.

Exceptions

Exceptions are receipt transactions that Identifi was unable to process. This menu should be checked periodically by Administrators.

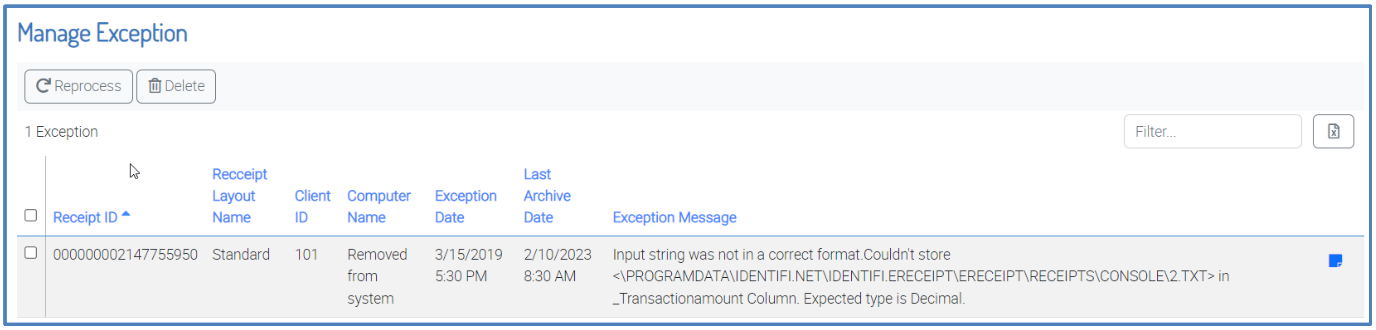


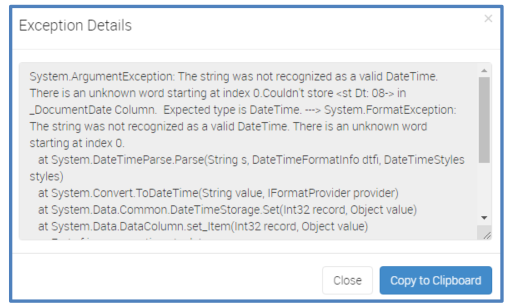


Note: Any receipts listed here are *not* archived. If receipts remain here after reprocessing, they will need to be individually addressed to correct errors.

** An email will automatically be sent to all users with the Administrator Role when there are exceptions.

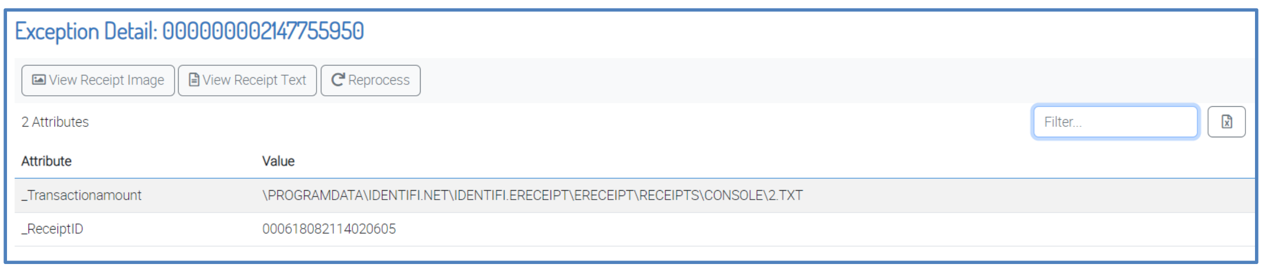
Resolving Exceptions



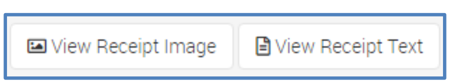


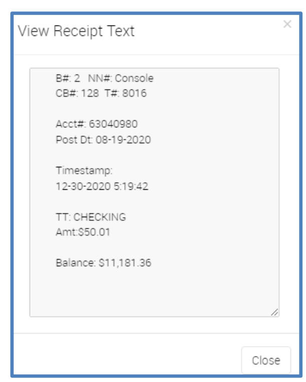
Select the icon to the right of the Exception to see the Exception type details

Click on the receipt exception in the list to see the transaction details

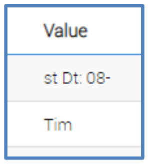


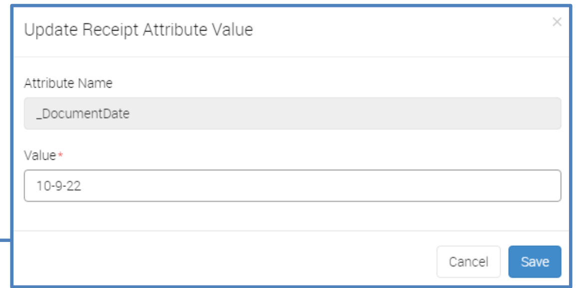
From the upper menu, use the buttons to view the actual receipt image and the text of the receipt:

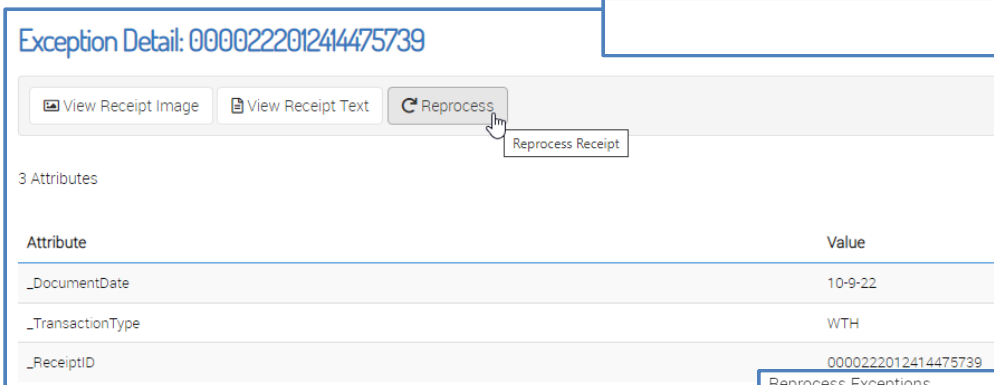




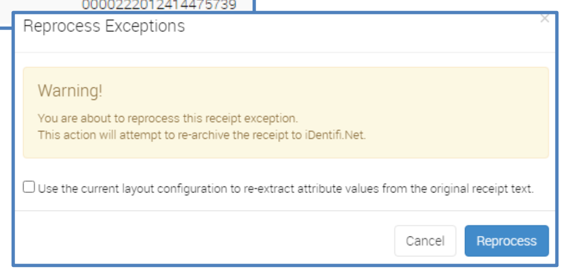
Clicking on a Value opens a screen to edit the data collected from the receipt.





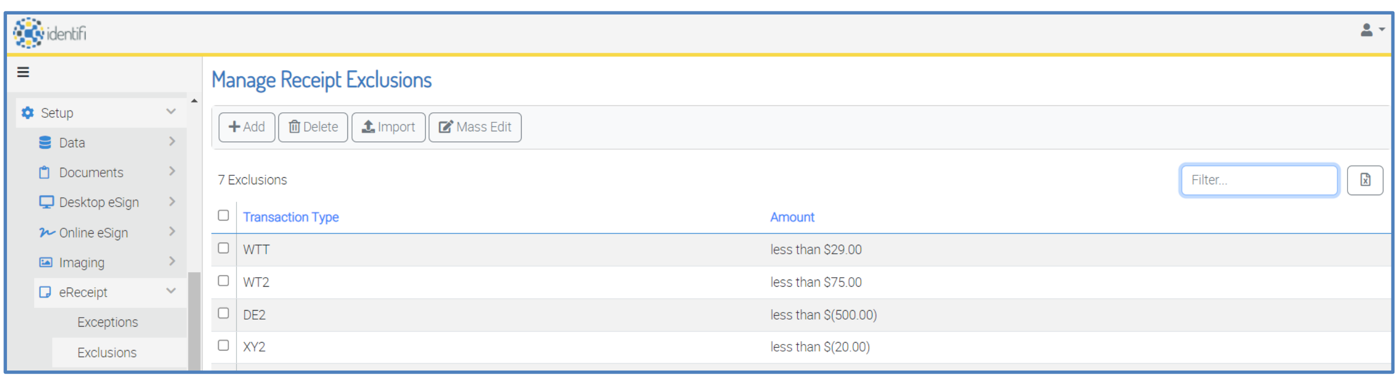


Once all corrections have been made, select ***Reprocess*** to archive the receipt.

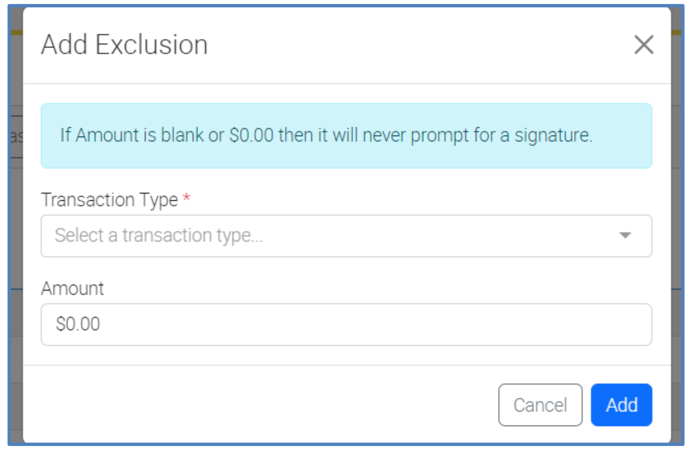


Receipt Exclusions

Transaction Types that do not require a signature on the receipt stored in Identifi are configured as **Exclusions**.

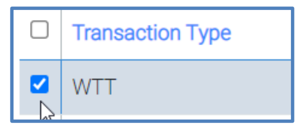


Manually Add an Exclusion

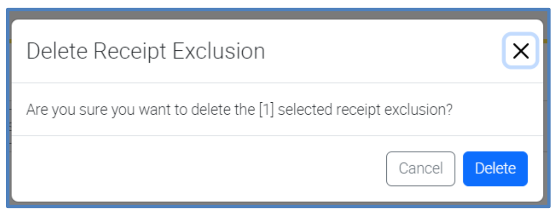


- Click + Add in the menu bar.
- Use the dropdown to choose the Transaction Type.
- Type in the amount of the exclusion
- Click Add Add

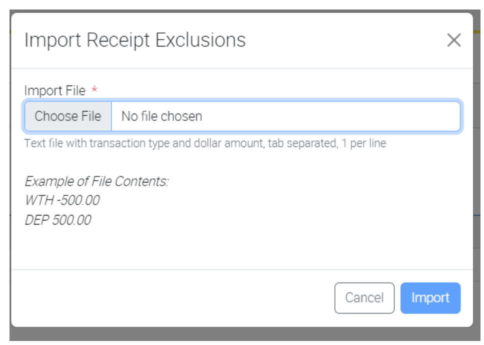
Manually Delete an Exclusion



- From the list of exclusions, select the check box to the left of the Transaction Type exception(s) to be deleted.
- Click Delete in the menu bar.
- Click Delete to confirm.



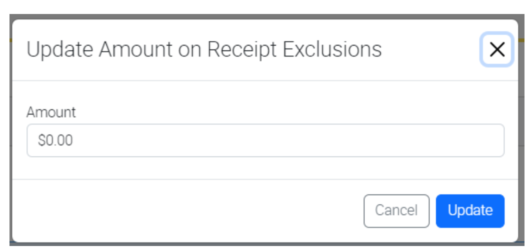
Manually Import an Exclusion



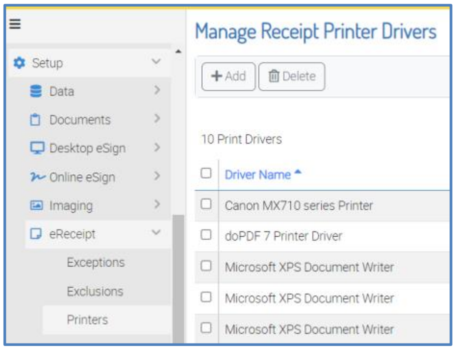
- Click Import in the menu bar.
- Browse out to locate the file and click Import

Mass Edit Exclusions

- From the list of exclusions, select the check box to the left of the Transaction Type exception(s).
- Update the amount of the Exclusion and click Update

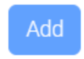


Printers

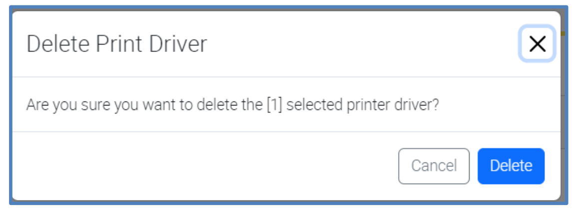


In order for Receipts to perform correctly, printers must be installed and configured at the workstation.

Once the driver has been installed on the PC, select ***Add***, then enter the printer's name and click .



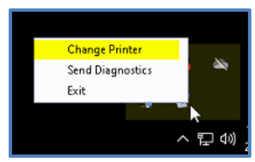
To remove a printer that is no longer needed, click the box next to the printer's name and select ***Delete*** from the upper menu.

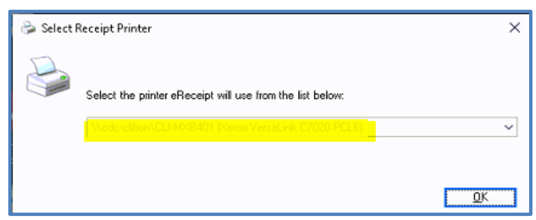


Using Network Printers with eReceipt

Follow these instructions to configure an eReceipt client to print receipts to a network printer rather than a printer connected directly to the workstation:

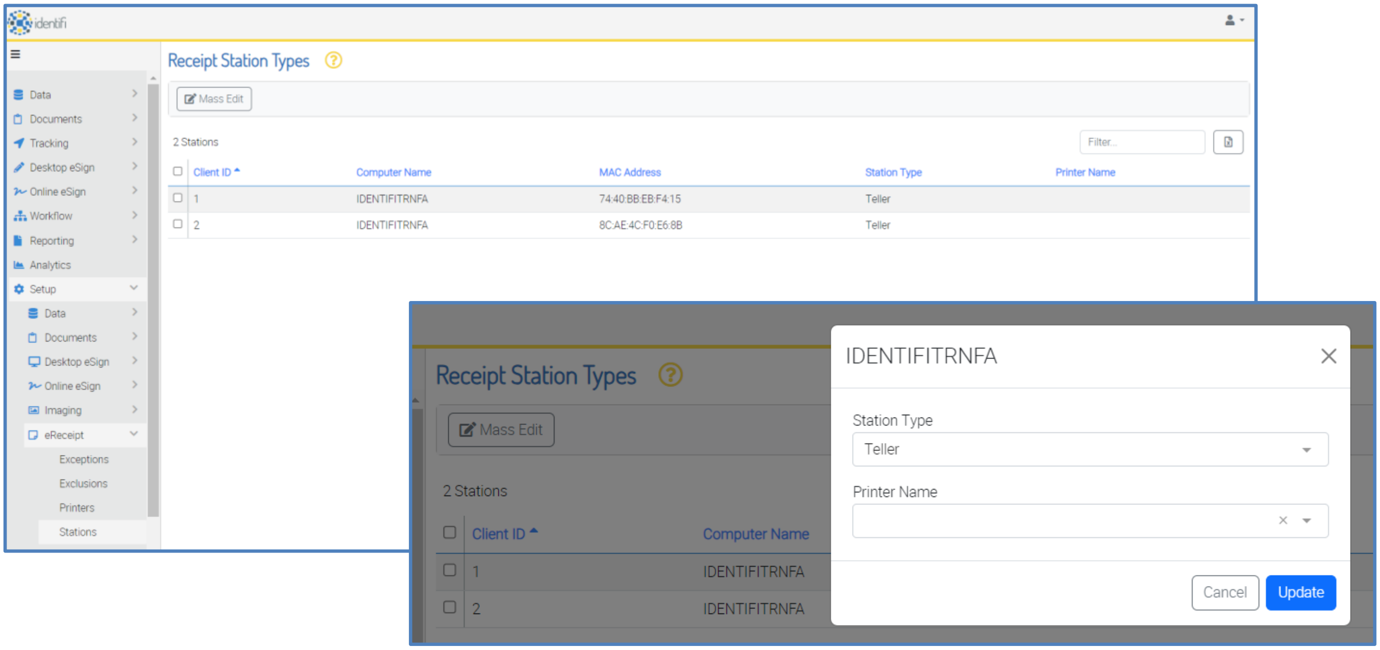
1. Install the client on the workstation.
2. From the applet in the task bar, select *Change Printer*.
3. Then select the network printer from the drop down.



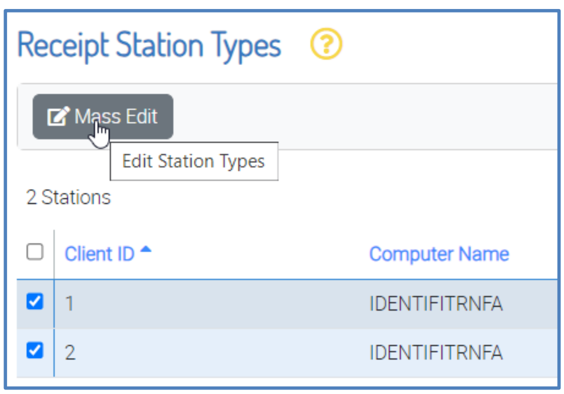


Stations

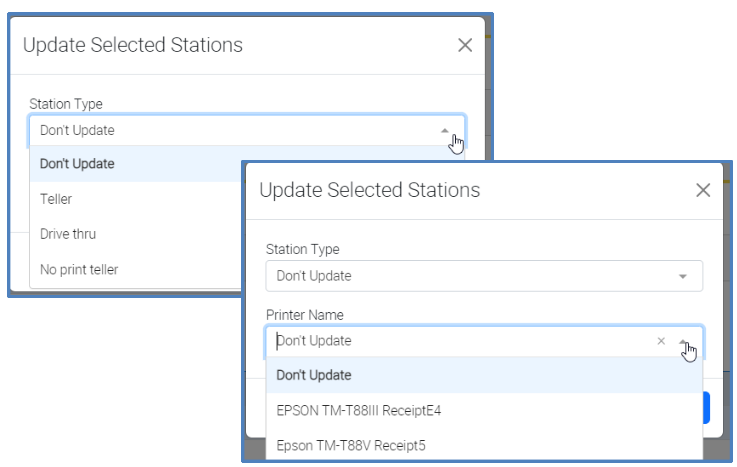
The Receipt Station Types list is comprised of each Receipts Client installed.



Click the Client ID of the station and select ***Edit*** to add the Printer Name and adjust the Station Type.

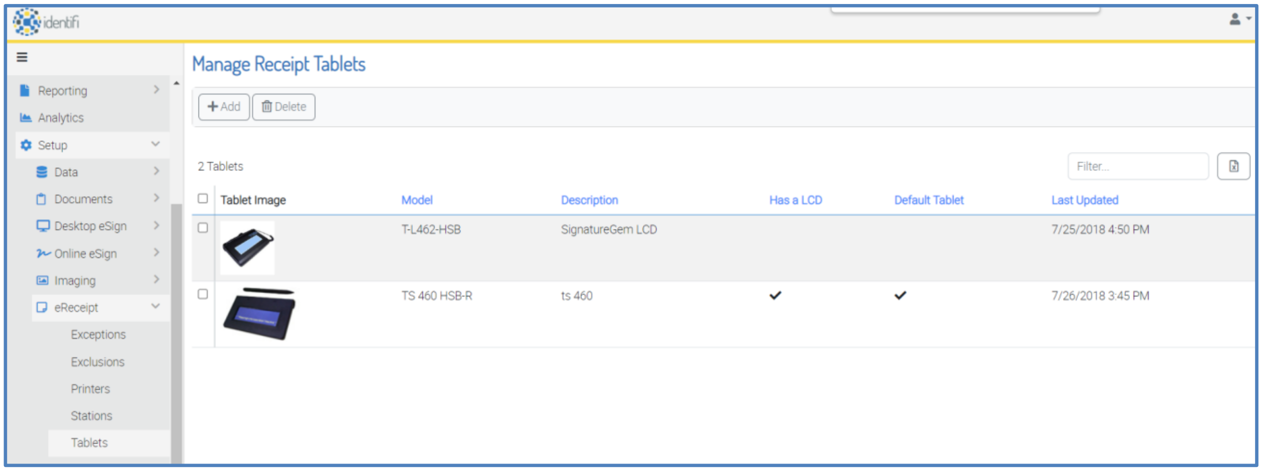


Edit multiple Station Types by selecting the box next to the Client ID and clicking "Mass Edit" at the top:

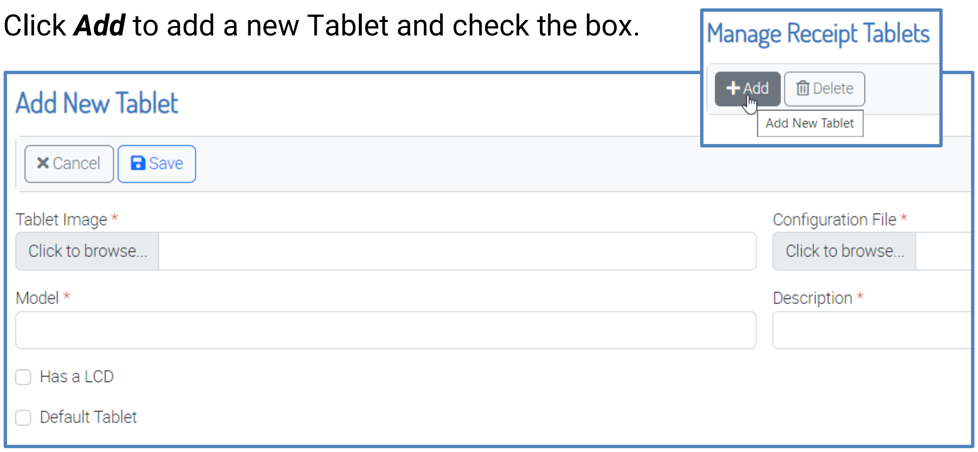


Tablets

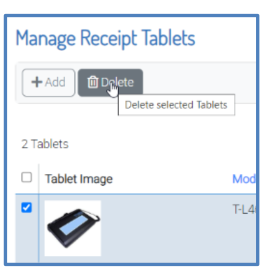
In addition to installing the signature tablets on the Receipts workstations, the tablets also must be configured in Identifi.

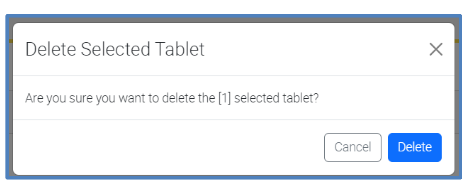


Click ***Add*** to add a new Tablet and check the box.



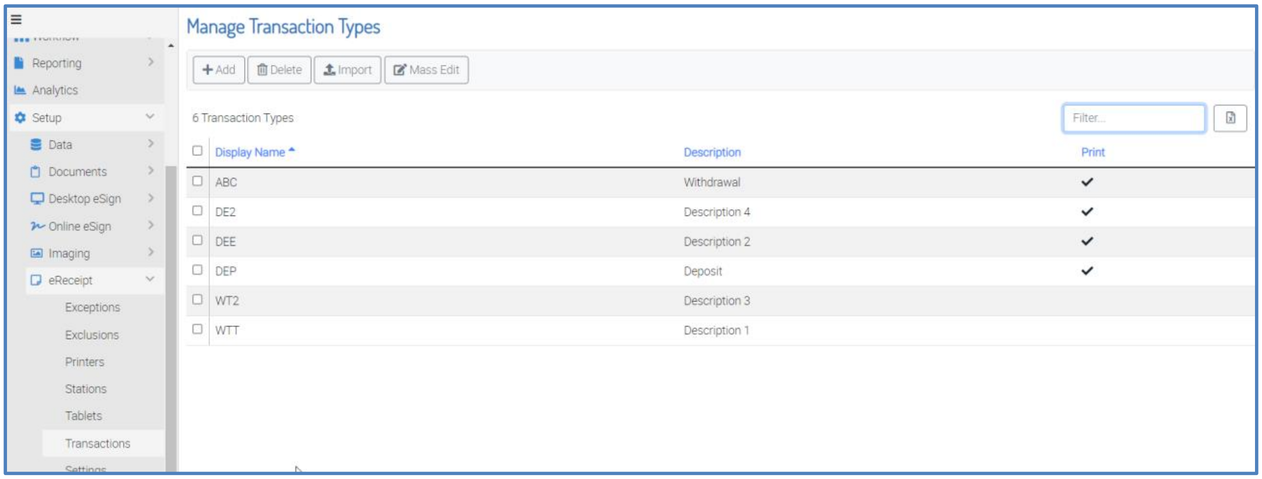
To remove a tablet, select the tablet to be deleted and click ***Delete***.





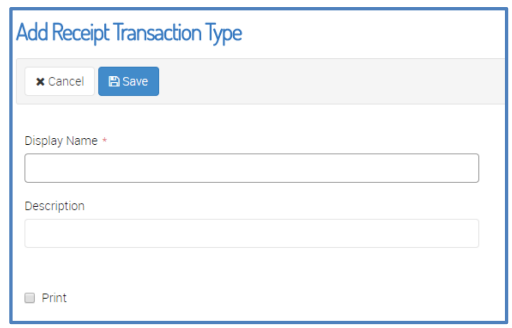
Transactions

Transactions that Receipts should handle are managed here.



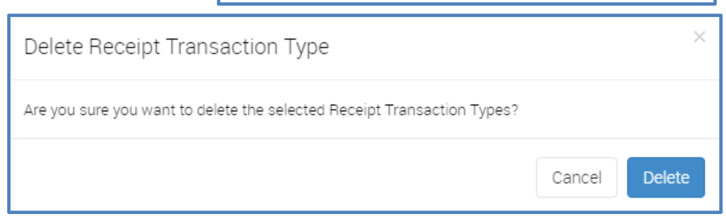
Adding a Transaction Type

Select ***Add*** from the menu, enter a Display Name and determine whether receipts should print for this type of transaction.



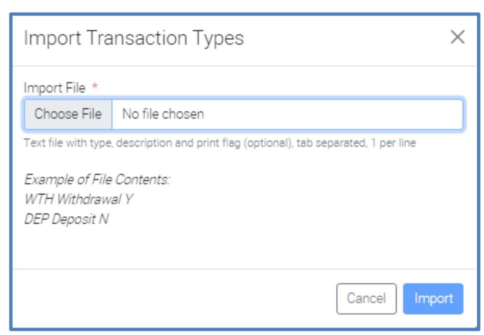
Deleting a Transaction Type

Click the box next to the Transaction Type in the list and select ***Delete*** from the menu.

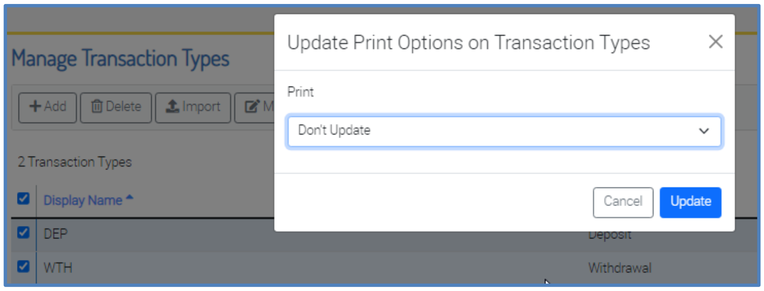


Importing Transaction Types

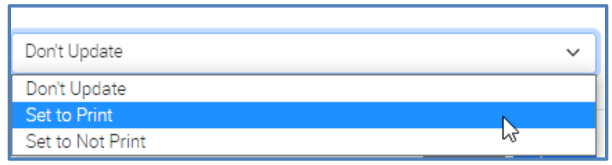
Select ***Import*** from the menu and select an appropriate .txt file to upload.



Mass Editing Transaction Types

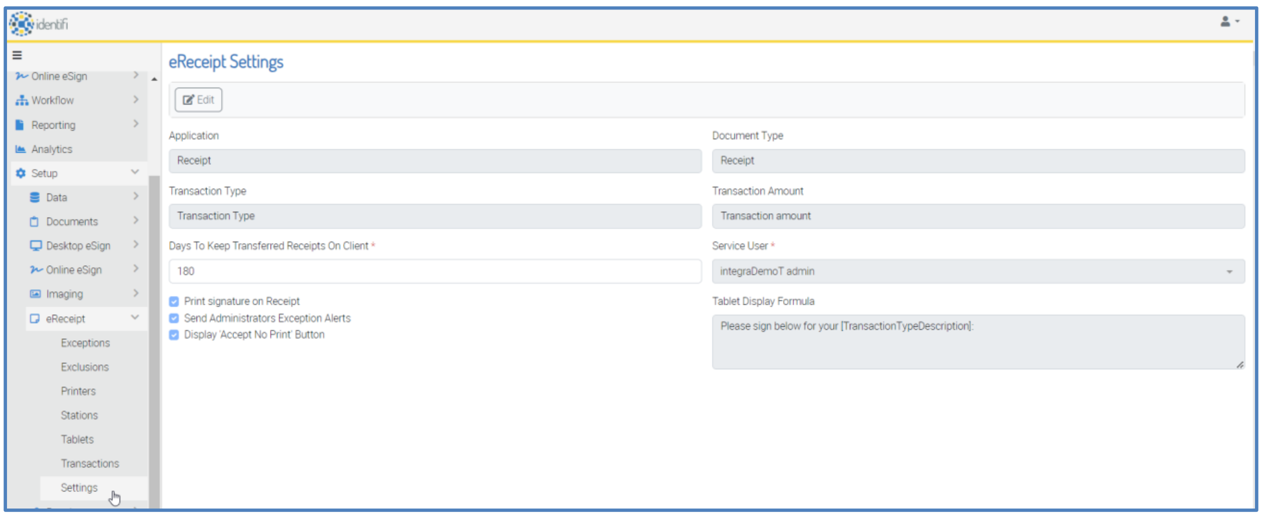


Place a check next to all transaction types to be modified and then click ***Mass Modify*** in the upper menu.



Make the appropriate selection from the drop-down menu and then click ***Update.***

Settings



The following fields can be modified here:

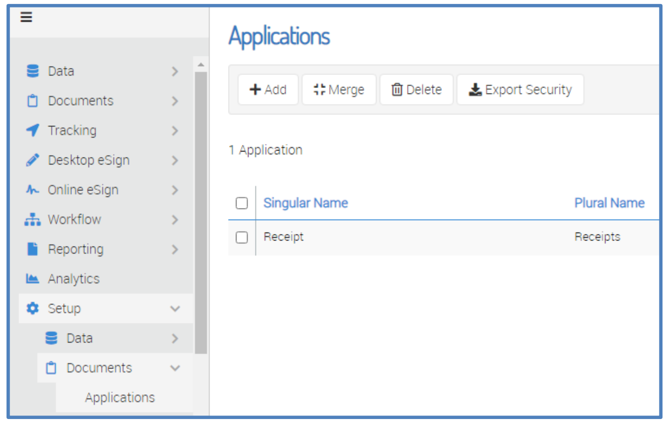
- ***Days To Keep Transferred Receipts on Client-*** Signed receipts will remain on the workstation client for the specified amount of time for retrieval in the case of an issue.
- ***Service User-*** Service account. Not typically modified after implementation.
- ***Tablet Display Formula-*** Message displayed and attribute referenced on the signature tablet during signing.
- **Check boxes to:**
  - ***Print Signature on Receipt***
  - ***Send Administrators Exception Alerts***
  - ***Display "Accept No Print" Button*** on screen during signing.

Other Receipt Settings

Application

Receipts will be stored in their own Application.

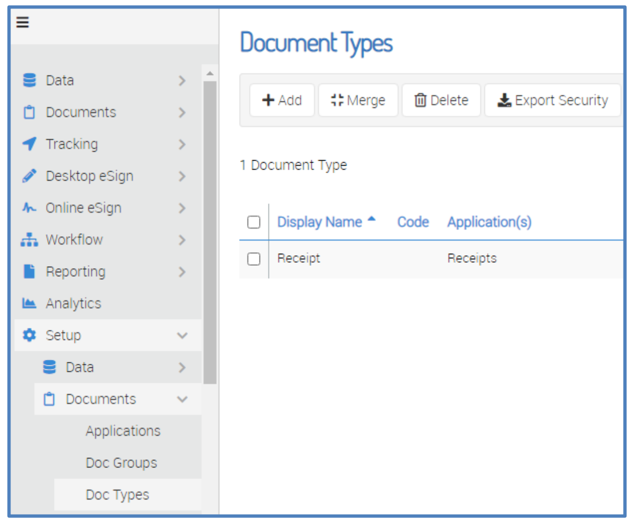
See Adding an Application for details.



Doc Types

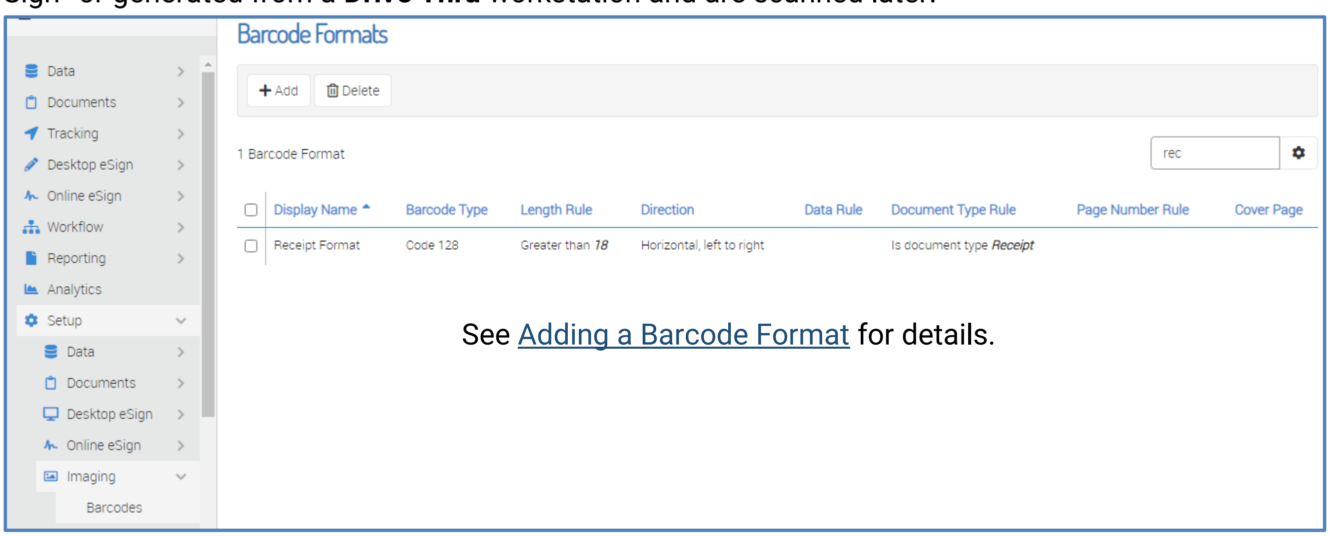
A Document Type will be created for a receipt.

See Adding a Doc Type for details.



Barcode

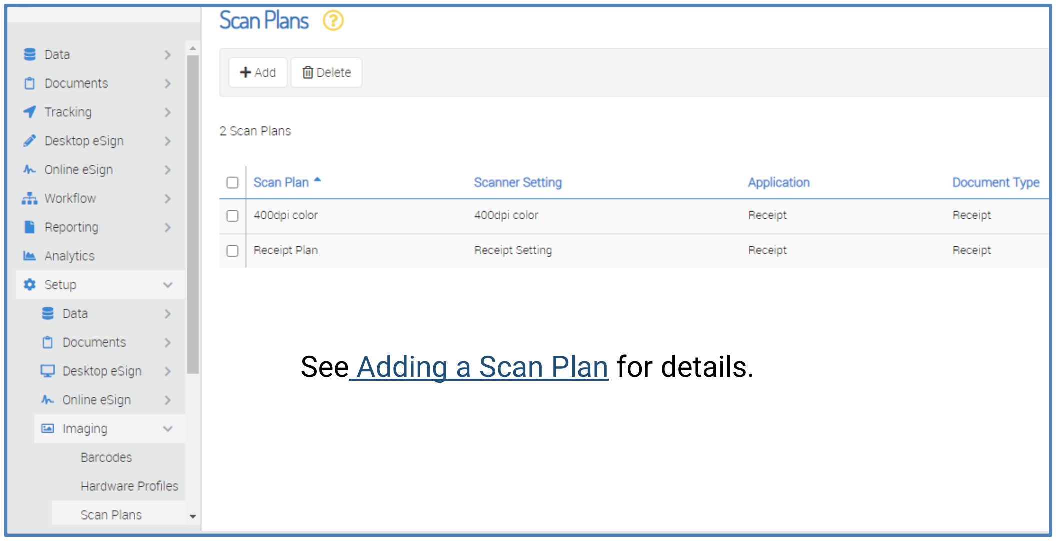
A Receipt barcode format must be configured for those receipts that are signed using “Print to Sign” or generated from a **Drive Thru** workstation and are scanned later.



See Adding a Barcode Format for details.

Scan Plan

A Scan Plan is required for scanning in the receipts signed through “Print to Sign”. With the barcode on the receipt and the Scan Plan set to *auto-archive*, the batch will not require any manual indexing.

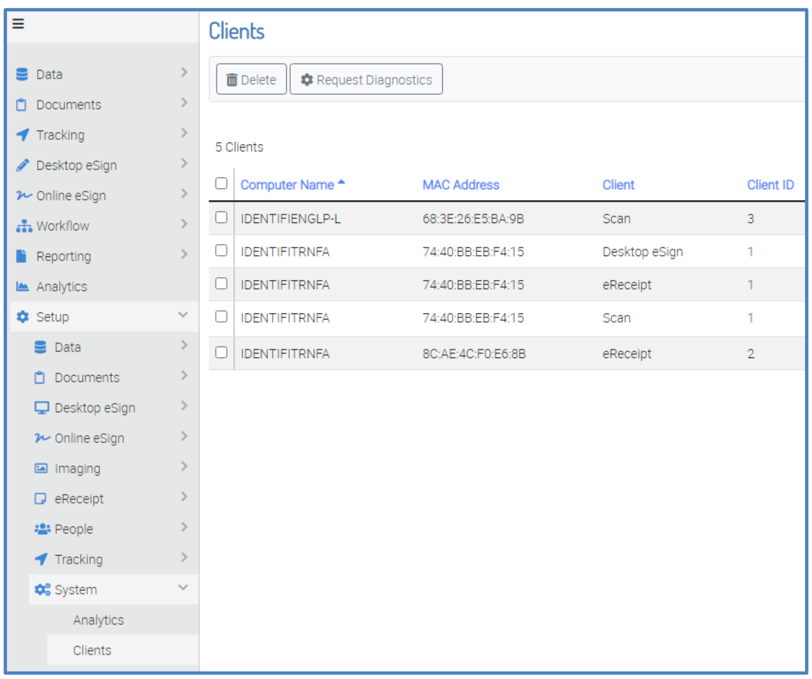


See [Adding a Scan Plan](#) for details.

Managing eReceipt and Receipt Designer Clients

The clients are downloaded and managed under the ***System*** menu.

Clients:

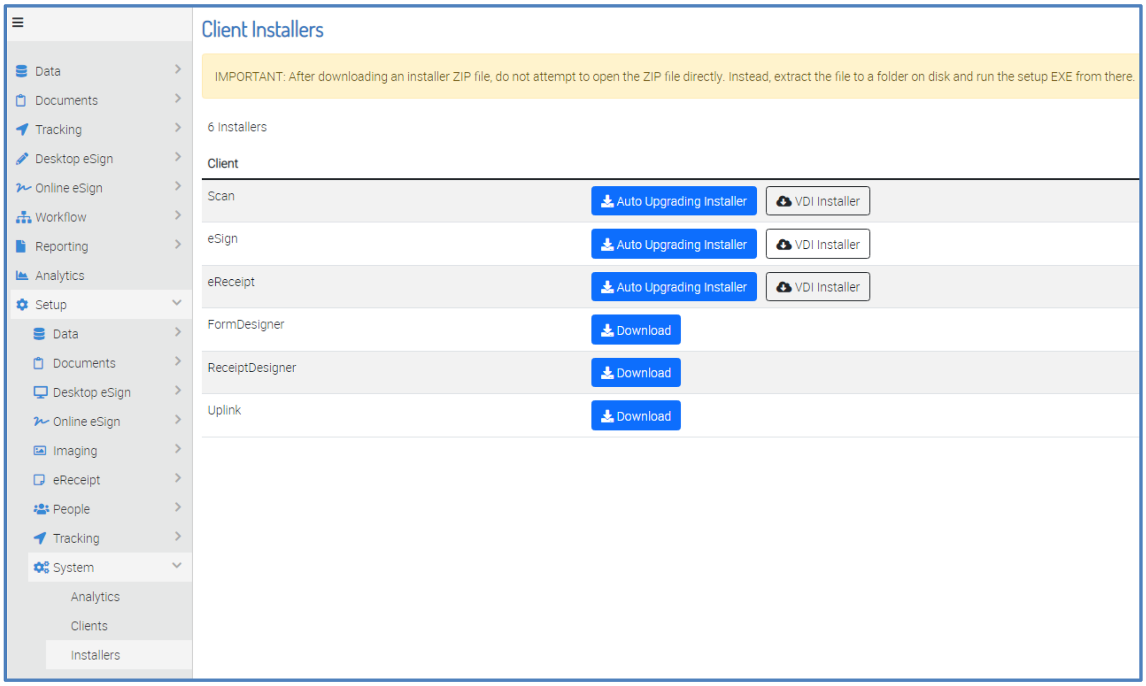


A list of all installed eReceipt and Receipt Designer Clients can be viewed here. Those that are not needed can be removed from this screen as well.

For more details: [Setup-System- Clients](#)

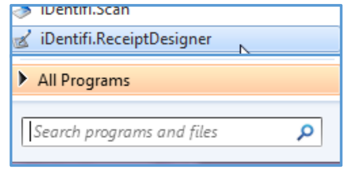
Installers:

The Installers for the eReceipt Client and Receipt Designer are downloaded for installation and deployment from here. For more details: [Setup-System- Installers]



Using the Receipt Designer

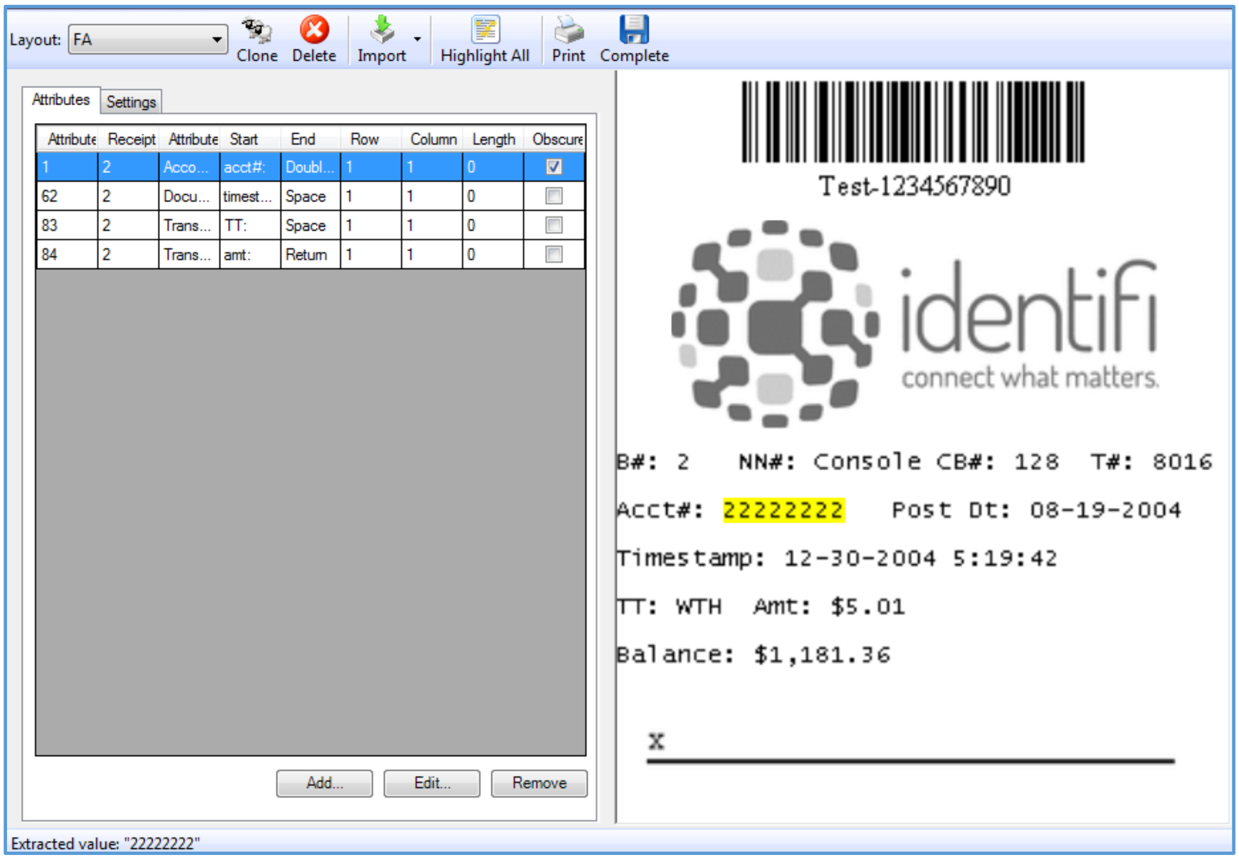
Receipts are designed and configured in the Receipt Designer to be recognized and read by Identifi.



Launching the Receipt Designer

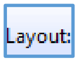
To launch the Receipt Designer, navigate to the PC's Start Menu and locate it in Programs.

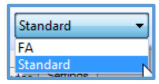
The receipt image will be presented in the right panel and settings and configurations in the left.

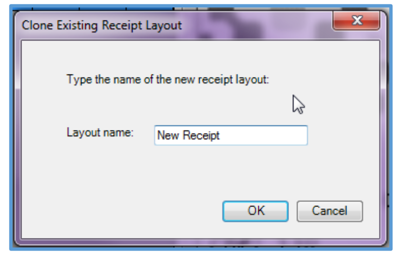


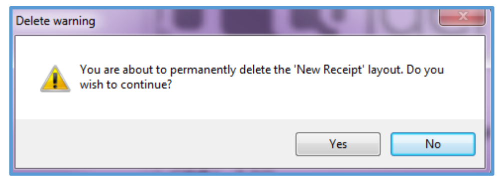
Navigating the Receipt Designer

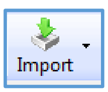
Upper Menu Bar 

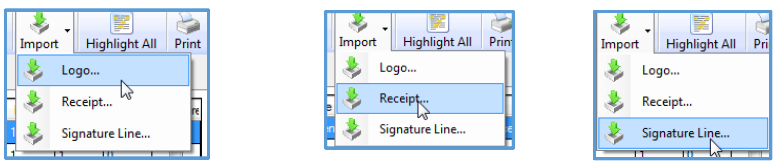


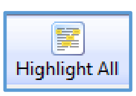
Select the receipt to view or modify.


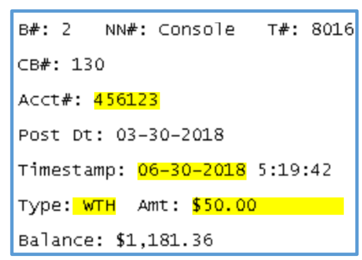
Create a new receipt by cloning the active receipt layout. The new receipt can then be modified.


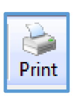
Delete the active receipt layout. ****Note:** Contact Identifi Support before deleting active receipt layout.




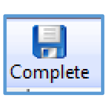
Import a logo, receipt image or signature line to be applied to the active receipt layout.




Highlight the areas of the receipt that will be identified and used for indexing based on the settings.

B#: 2 NN#: Console T#: 8016
CB#: 130
Acct#: 456123
Post Dt: 03-30-2018
Timestamp: 06-30-2018 5:19:42
Type: WTH Amt: $50.00
Balance: $1,181.36

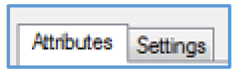


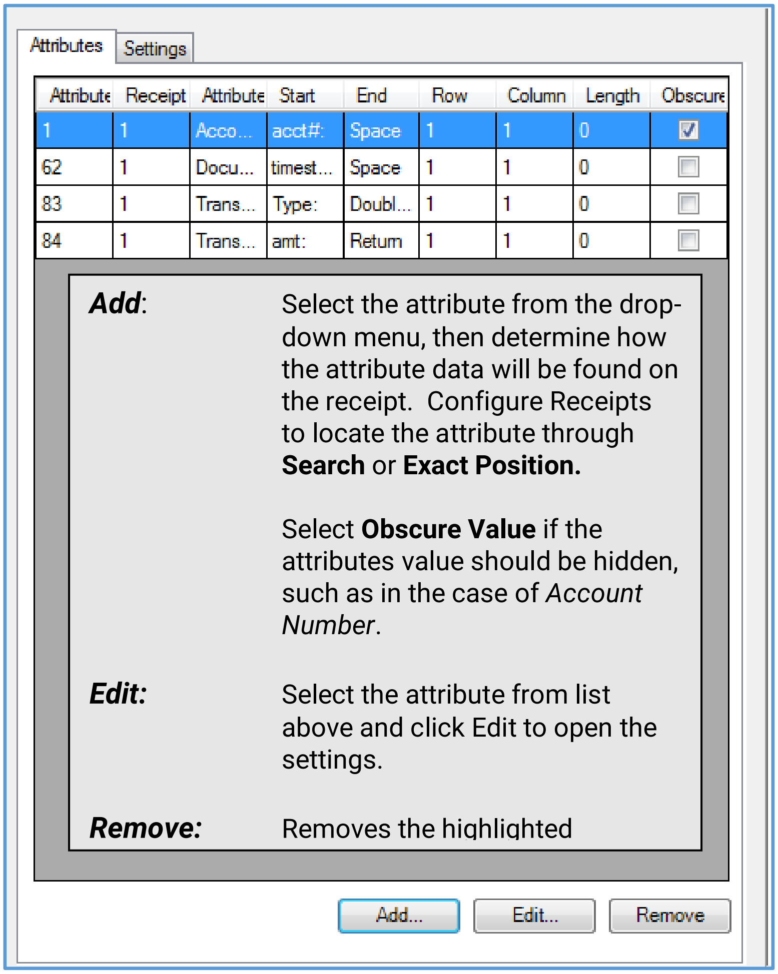
Prints a paper copy of the receipt from the attached receipt printer.



Saves receipt layout and closes the Receipt Designer.

Attributes and Settings



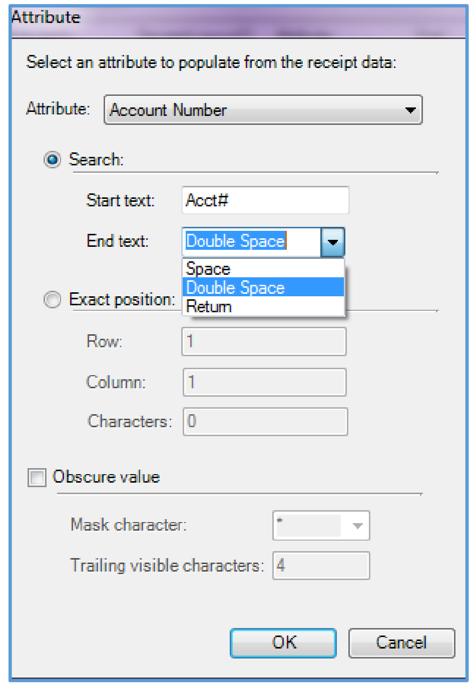


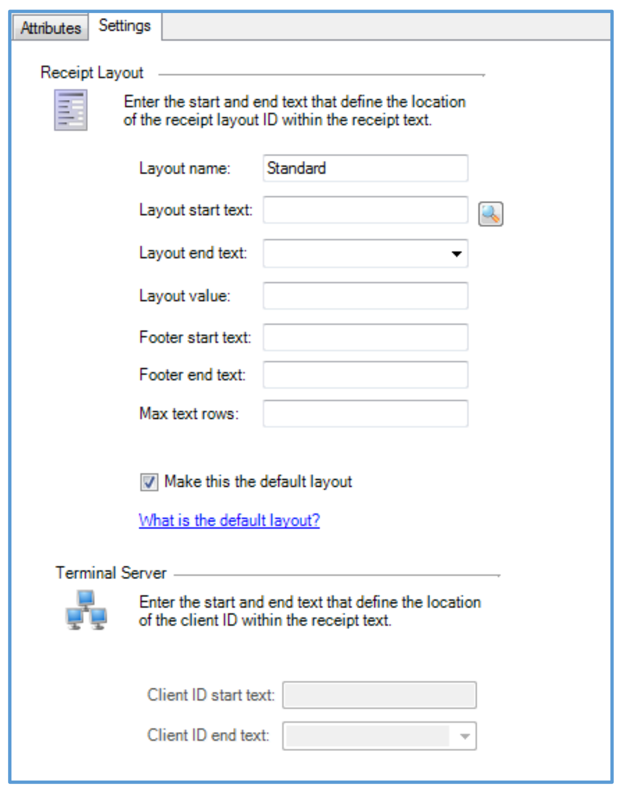
Add: Select the attribute from the drop-down menu, then determine how the attribute data will be found on the receipt. Configure Receipts to locate the attribute through **Search** or **Exact Position.**

Select **Obscure Value** if the attributes value should be hidden, such as in the case of *Account Number*.

Edit: Select the attribute from list above and click Edit to open the settings.

Remove: Removes the highlighted

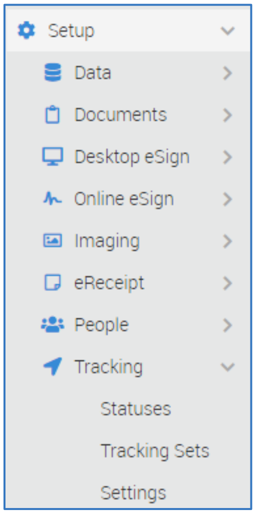




Under the ***Settings*** tab, details like the name of the receipt layout can be modified. Footer text, such as a slogan, can be added.

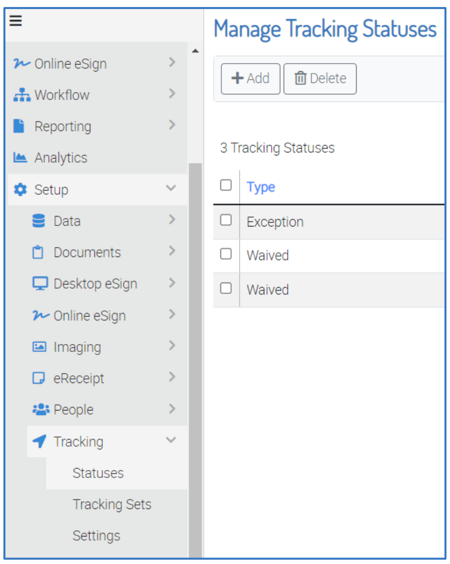
The *Default Layout* is what Receipts will assume when no layout can be identified.

DOCUMENT TRACKING



Users with the ***Administrator Role*** assigned to them have the ability to manage all aspects of the Tracking module.

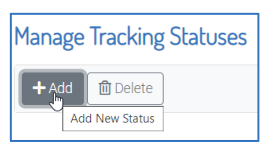
Statuses



In addition to the default *Exception: Past Due* Status, Document Tracking allows users to create and manage other Tracking Statuses.

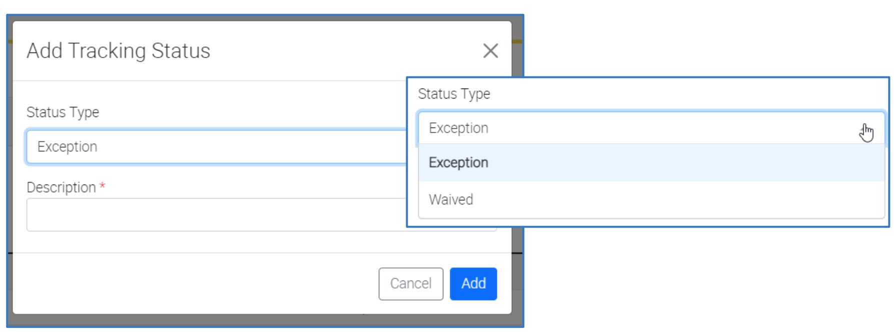
These statuses will be available to users when overriding an Exception-Past Due status.

Adding a Tracking Status

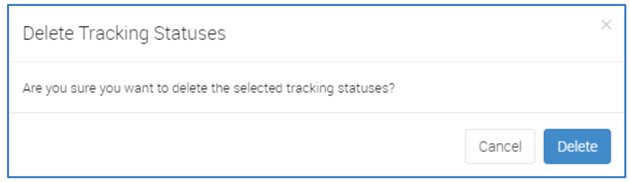


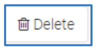
To add a Tracking Status, select + Add from the upper menu.

Choose whether it will be an Exception or a Waived status, then provide a Description. Click Save.

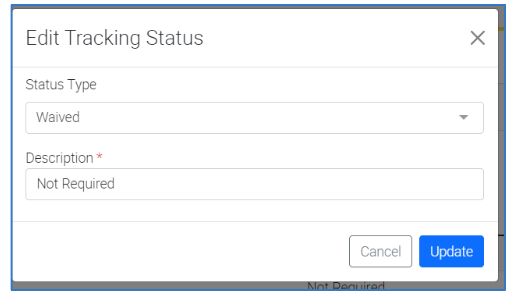


Deleting a Tracking Status



To delete an existing Tracking Status, select it from the list and click . Confirm by selecting ***Delete*** on the following screen as well.

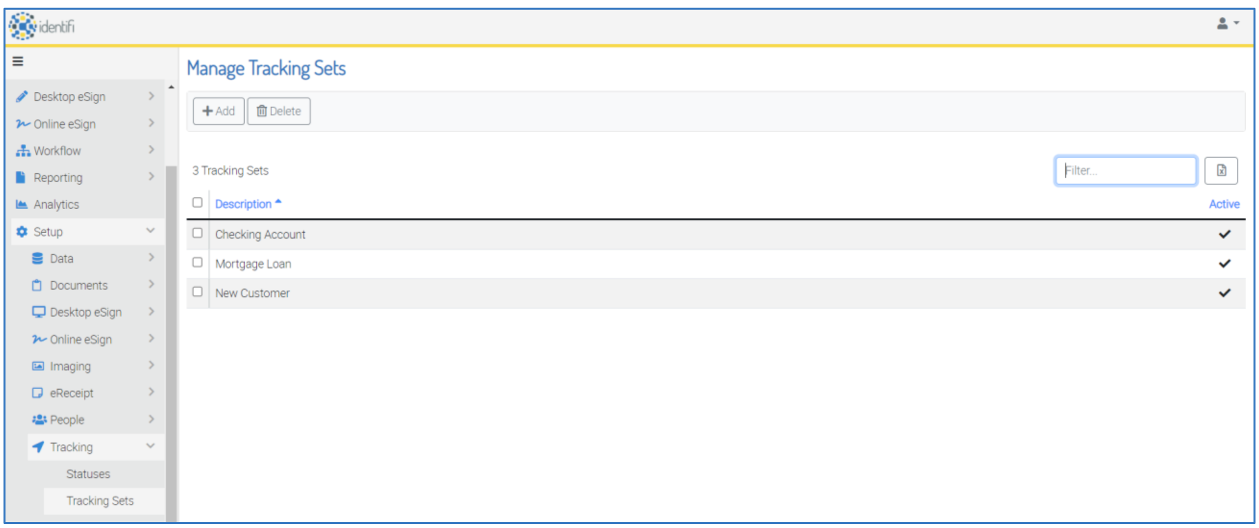
Modifying a Tracking Status



Clicking the title of a Status will open the **Edit Tracking Status** screen. Edit Status Type and/or Description and click ***Save*** when finished.

Tracking Sets

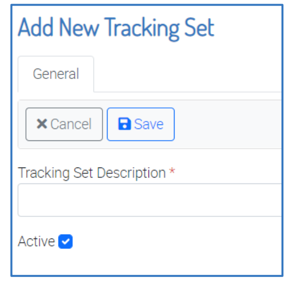
The documents that are required for a Tracked item are collected in a Tracking Set, which is then assigned to the appropriate Entity.



As a new tracked entity item is added, the documents within the Tracking Set will appear as Requirements on the item.

This menu allows users to ***Add*** new Tracking Sets, as well as ***Delete*** or Modify existing ones.

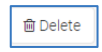
Adding a Tracking Set

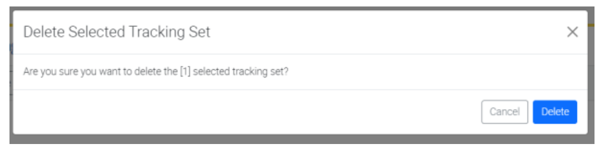


To add a Tracking Set, select  from the upper menu. Provide a Description and determine whether it should be ***Active*** or not. Click  .

See [*Modifying a Tracking Set*]() for details on managing the document types in the Set.

Deleting a Tracking Set

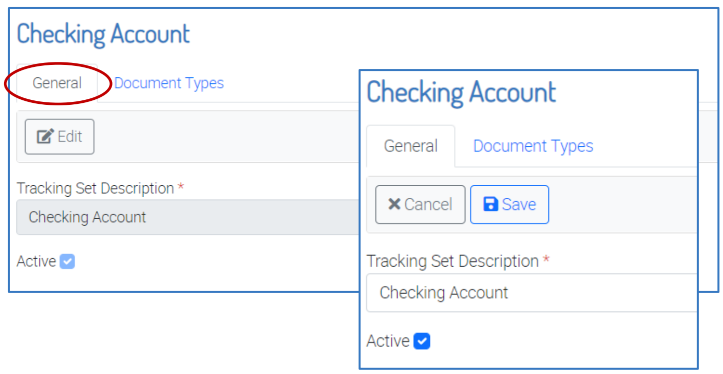
To delete an existing Tracking Set, select it from the list and click . Confirm by selecting ***Delete*** on the following screen as well.



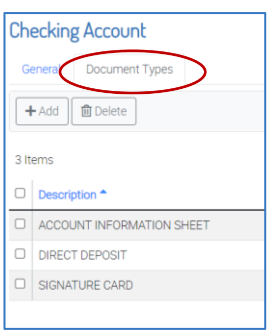
Modifying a Tracking Set

Clicking the title of a Set will open the details screen to the *General* tab.

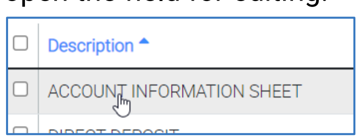
Select ***Edit*** to open the fields for changes and click ***Save*** when finished.

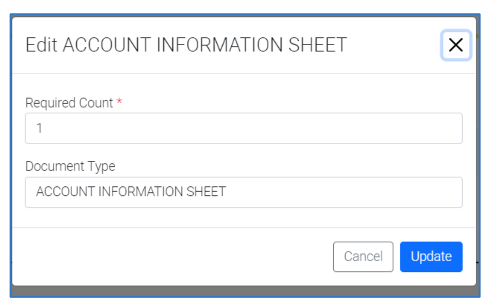


Under the *Document Types* tab, users can ***Add*** or ***Delete*** Document Types from the Set.

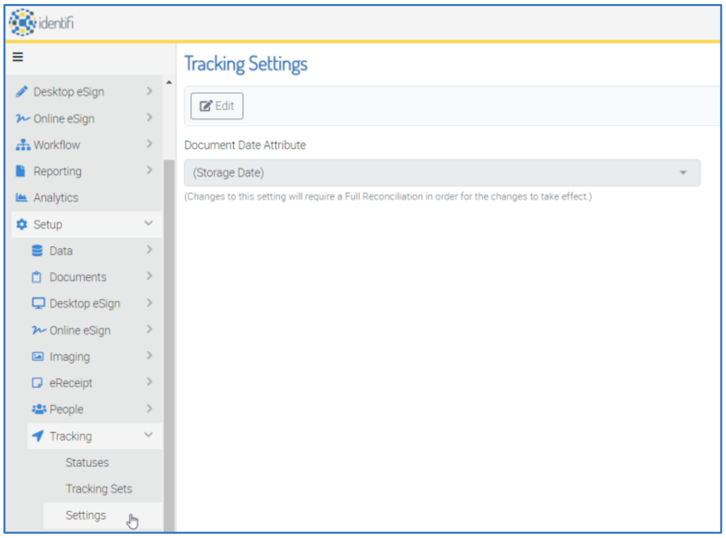


To set the **Required Count**, telling Document Tracking how many of the document should be associated with the item, click the document type's Description to open the field for editing.





Settings



Tracking Settings is where the date that the installation's Document Tracking is based on is set.

Though this is typically Storage Date, any date attribute could be set.

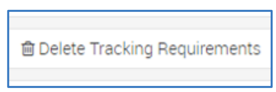
****Please contact Identifi Support when considering making a change to the Tracking Settings date.**

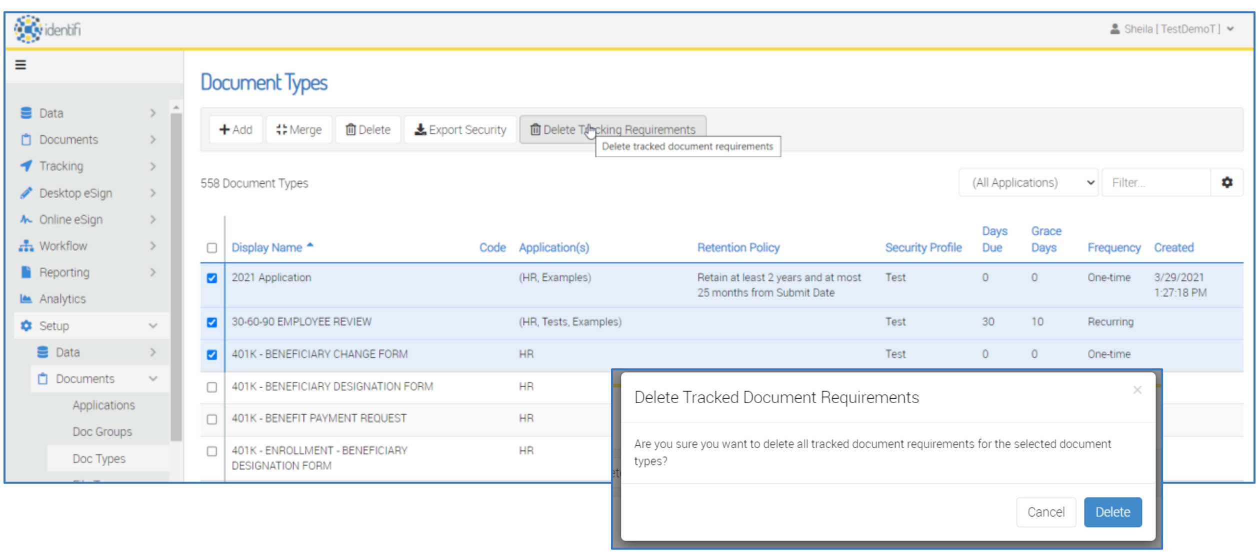
Other Tracking Settings

In addition to the main Tracking menus, settings for Document Tracking are also found at the Document Type and Entity Type level

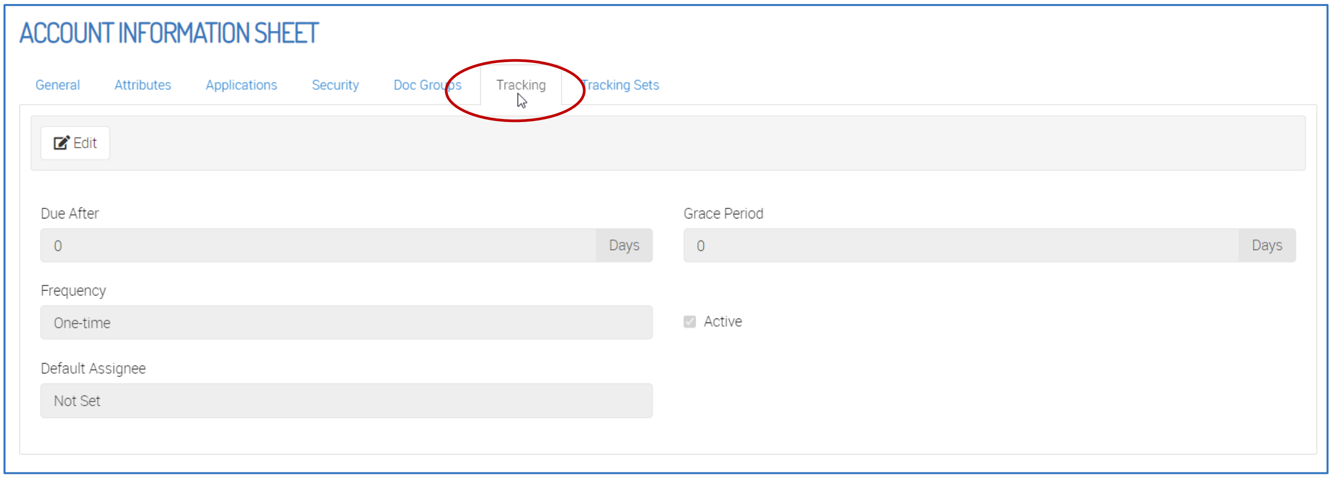
Document Types

- Tracking Requirements can be deleted in bulk from the main ***Document Types*** menu.

  Select the Document Types and select  .

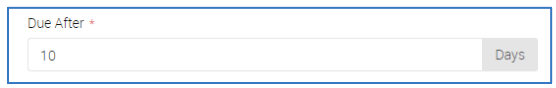


- Tracking Periods and Frequency are set under the ***Tracking*** Tab for the Doc Type.



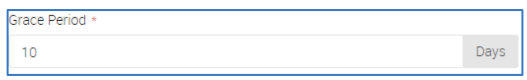
   - **Due After-** the timeframe after which the document is considered in exception.

     For example, each new account opened requires an Account Application document within 10 days of the account open date.



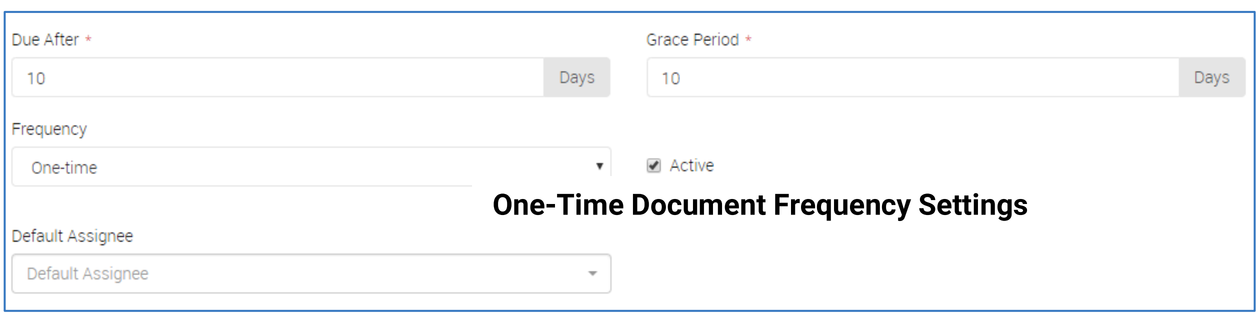
   - **Grace Period-** the timeframe after the Due After period has passed before the item shows in exception.

     For example, the customer is allowed an additional 10 days to submit all account documents after the opening date.



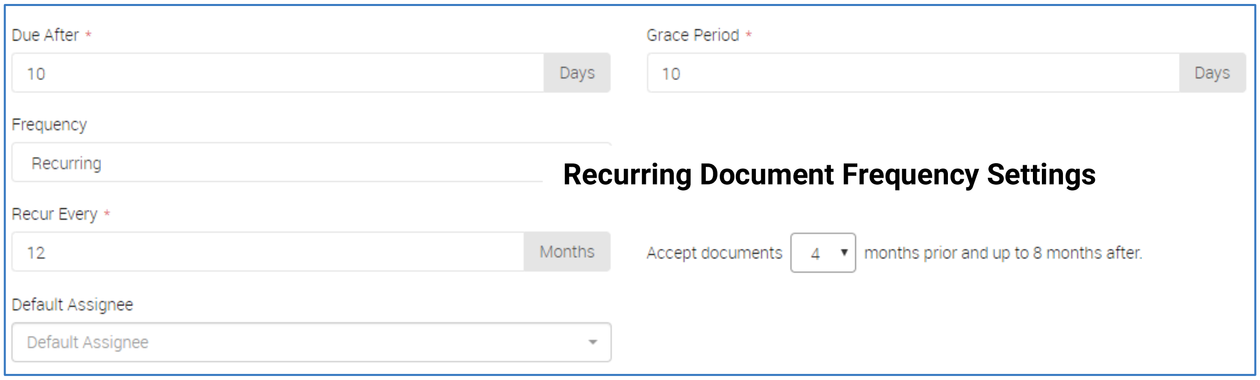
   - **Frequency:**

     - ***One-time-*** for documents that are submitted once.



One-Time Document Frequency Settings

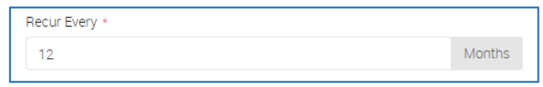
- ***Recurring-*** for documents replaced at regular intervals.



Recurring Document Frequency Settings

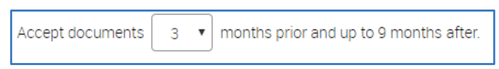
- *Recur Every*: the number of months that the document will be valid

  For example, current year's tax documents are required to be submitted each year, so they would recur every 12 months.



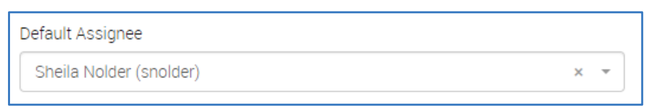
- *Accept documents___months prior and up to___months after*: the number of months prior to the due date that the new document will be accepted as satisfying the exception. The 'up to months after' will fill in automatically.

  For example, tax documents might be submitted as early as January of that year.

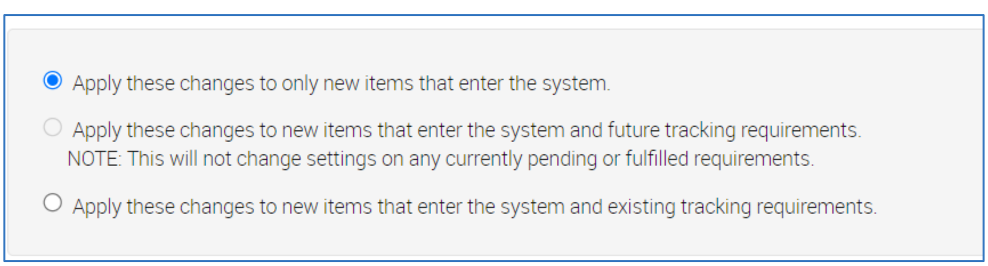


- ***Default Assignee*** - Select a user to automatically be assigned to any requirement related to this document type.

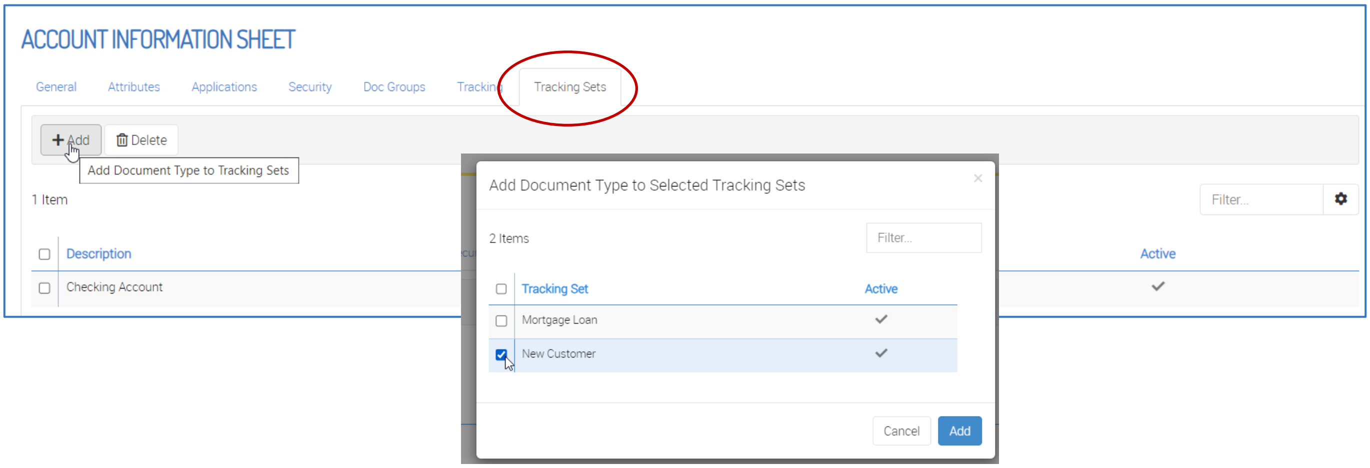
  If no user is selected here, the requirements will show as unassigned or will be assigned based User Roles from the host import.



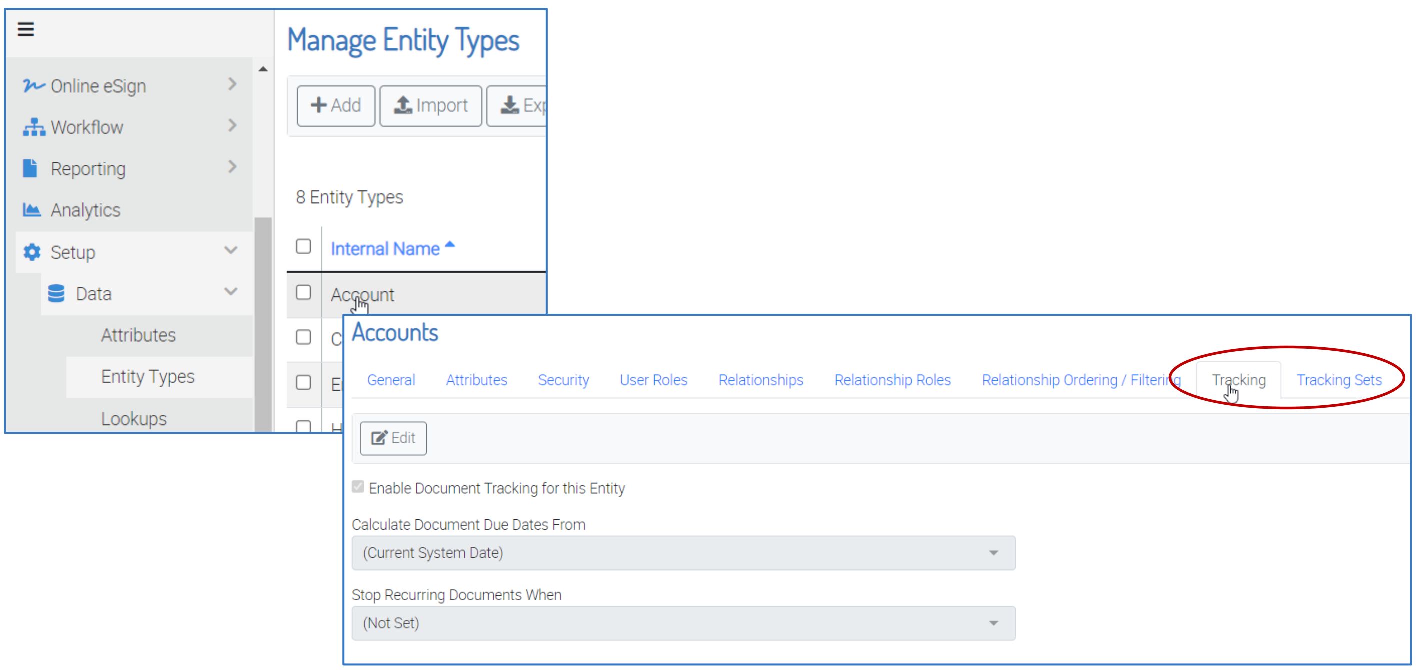
- ***Applying Changes-*** When making changes to a Document Type's Tracking details, select the degree to which these changes will be extended



- Doc Types can be added to or deleted from Tracking Sets under the ***Tracking Sets*** Tab.

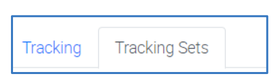


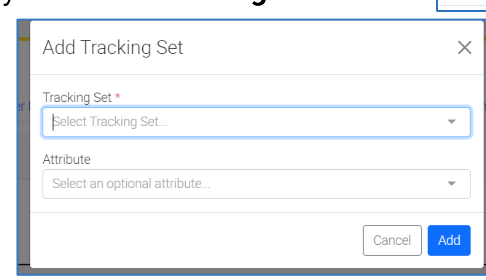
Entity Types



- The date by which Due Dates are determined for tracking items in the entity, as well as the Recurring date, is set under the Entity's ***Tracking*** Tab.

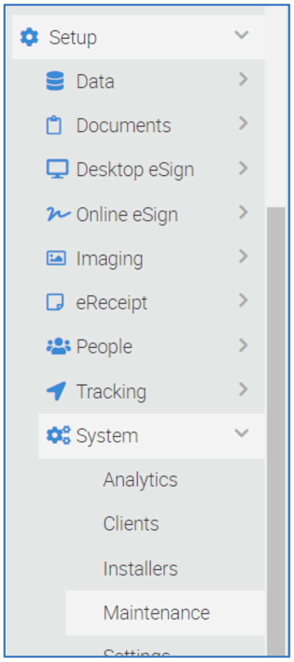
- Tracking Sets are assigned to the Entity under the ***Tracking Sets*** tab. The identifying attribute value is also configured here.

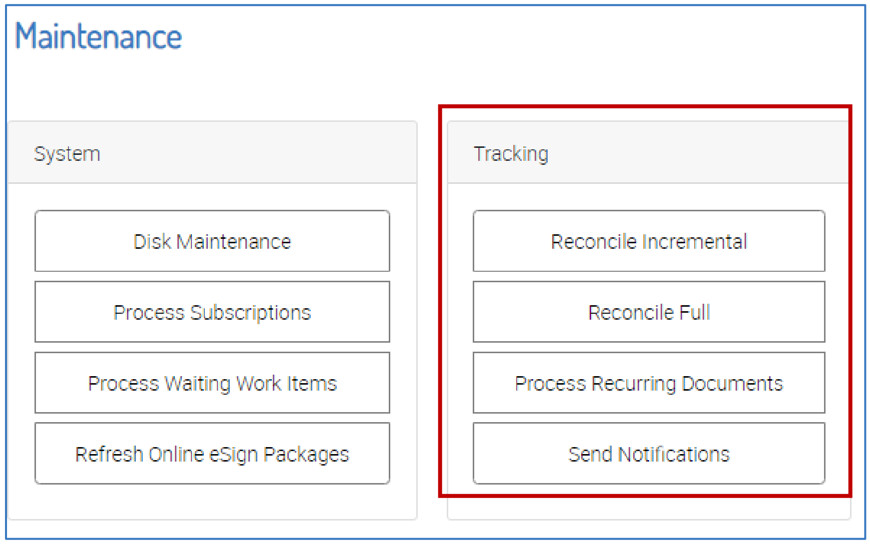




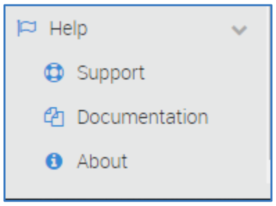
Tracking Maintenance

For details on running the background Tracking maintenances manually, see here.

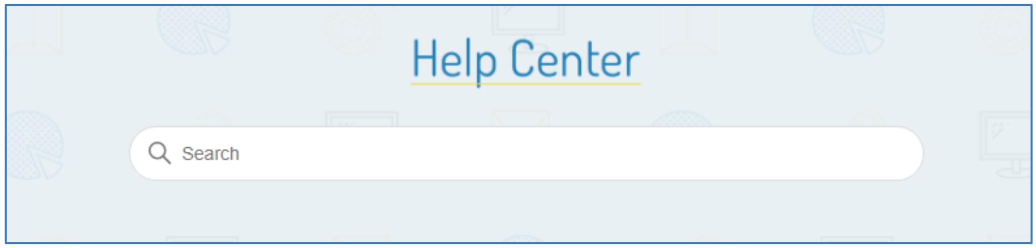




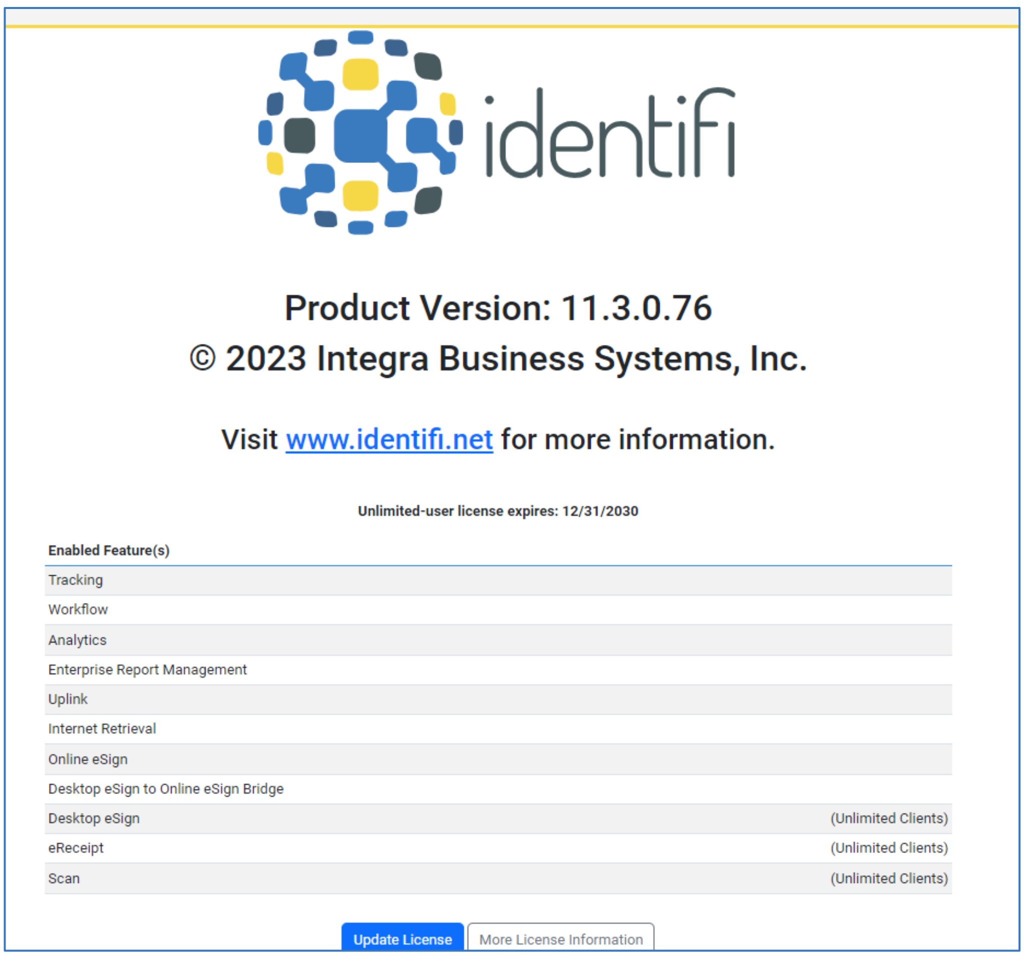
ADDITIONAL RESOURCES



For more information and step by step guides covering many of the topics in the manual in more detail, see our Help Center under ***Documentation.***



All Active licenses and client seats can be viewed by selecting ***About*** in this menu:



Note: Additional setup from Identifi Professional Services is required for Desktop eSign to Online eSign Bridge. Contact a member of the Identifi Sales Team with any questions regarding this feature.

APPENDIX

Appendix A – Configuring Azure & Okta for Identifi SSO

Azure

V2.0 Azure Open ID Connect Endpoint
Identifi version 7.4 has been modified to utilize Azure's Open ID Connect v2.0 integration in order to be able to sync users' email addresses. V1.0 does not return email addresses, requiring that the user login to Azure to complete the syncing process.

To invoke v2.0, simply add ***/v2.0*** to the end of the Authority on the *SSO* tab beneath **Installation** in Identifi. The Authority is the URL associated with the IDP's authorization server.

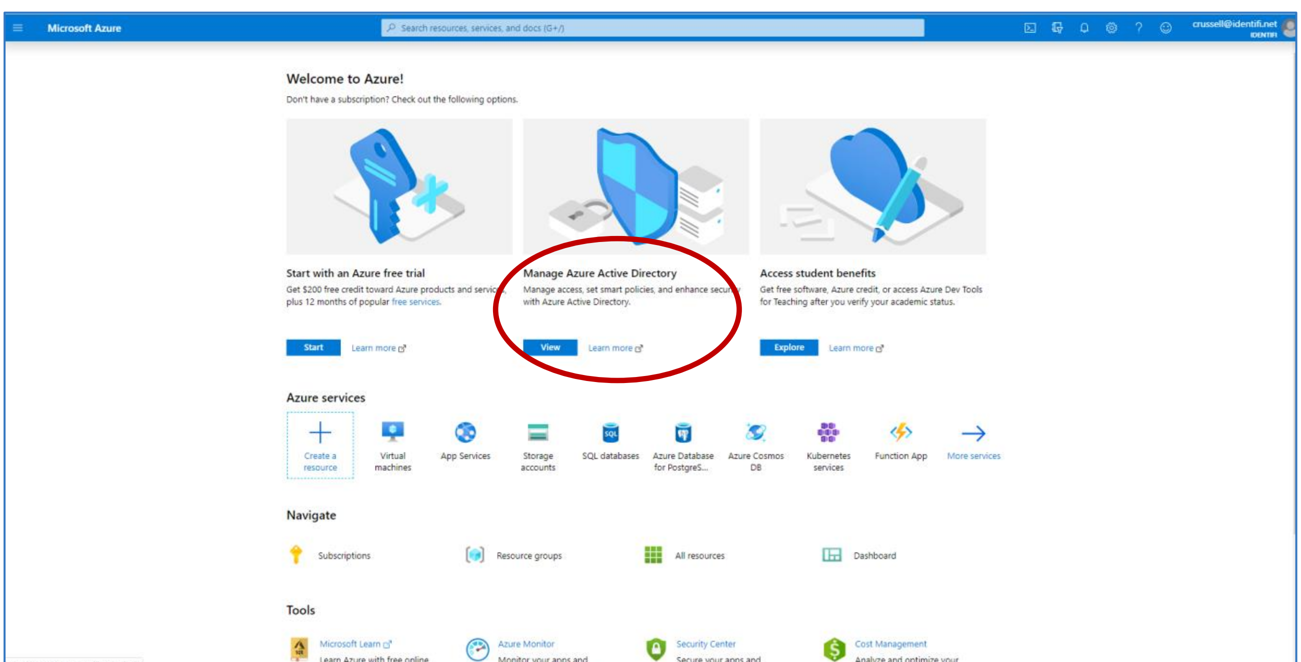
This applies to any existing SSO Azure AD deployments; simply by modifying the Authority in their existing configurations will invoke the change to v2.0.

Examples
With v1.0: https://login.microsoftonline.com/35e842ef-00ca-4bf1-a925-df2934b876af
With v2.0: https://login.microsoftonline.com/35e842ef-00ca-4bf1-a925-df2934b876af/v2.0

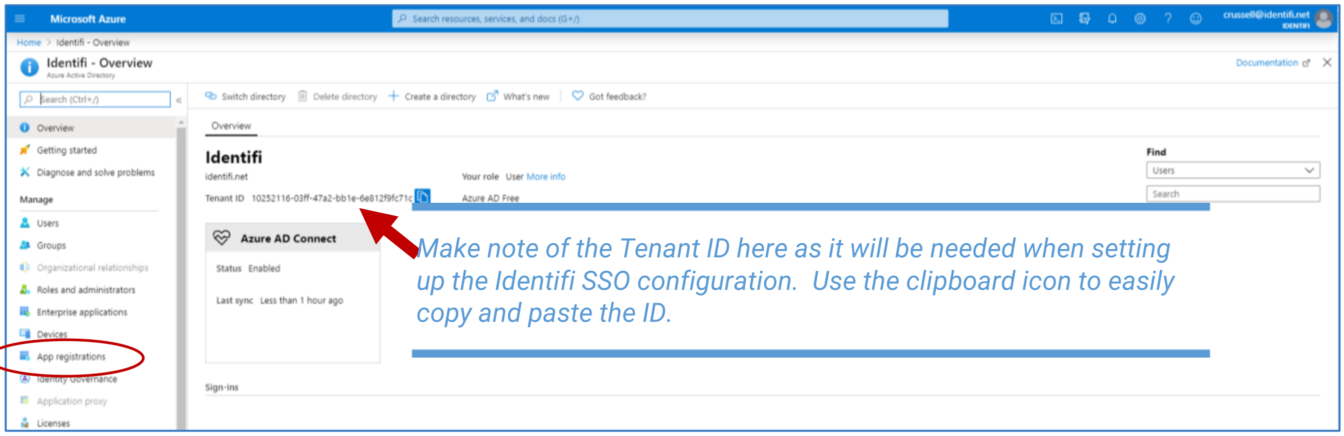
Adding Identifi as an Application Within Azure
If you are using Azure as your Identity Provider below are some instructions on how to register and configure the Identifi Application within Azure. This step must be completed before you can configure SSO within Identifi.

1. Logon to the Azure portal

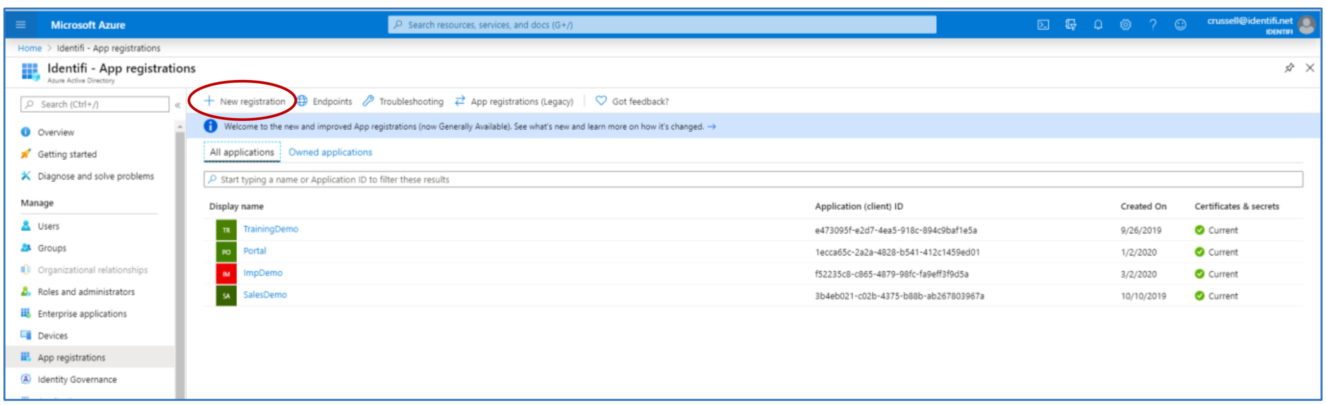
2. Click ***View*** under **Manage Azure Active Directory**

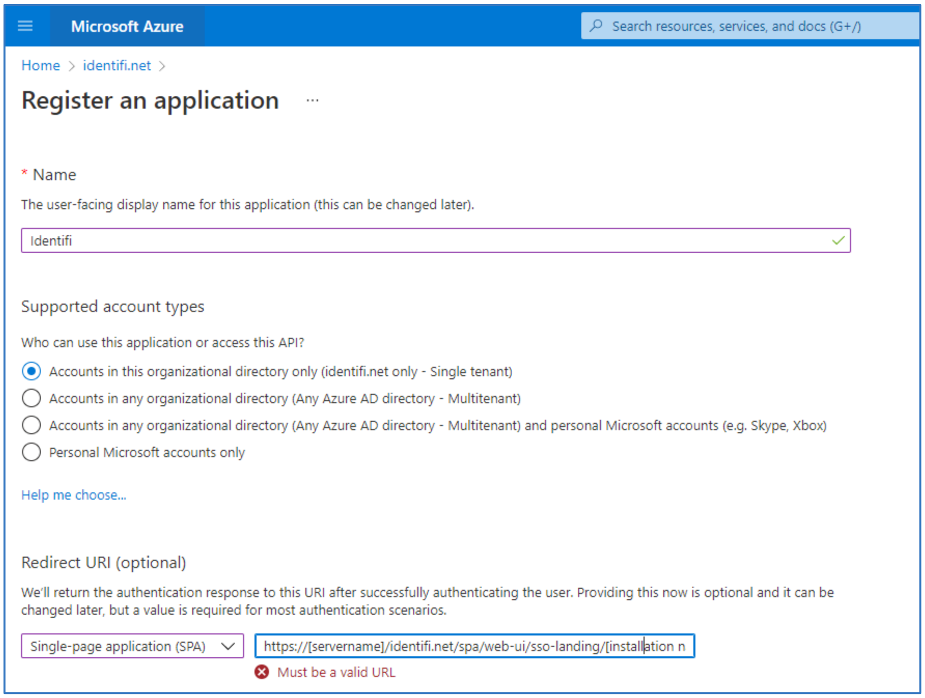


Select **App registrations** in the left menu



3. Click the ***+ New Registration*** button in the upper menu.

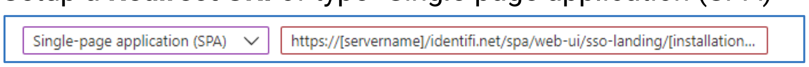




4. Enter a suitable name (e.g. "Identifi")

5. Choose the Single tenant option

6. Setup a **Redirect URI** of type "Single-page application (SPA)"



A redirect URI is where Azure sends the authentication response and ID token. The redirect URI will need to be configured to reflect the Identifi server's URL.
For example: 'https://[servername]/identifi.net/spa/web-ui/sso/[installation name]'.

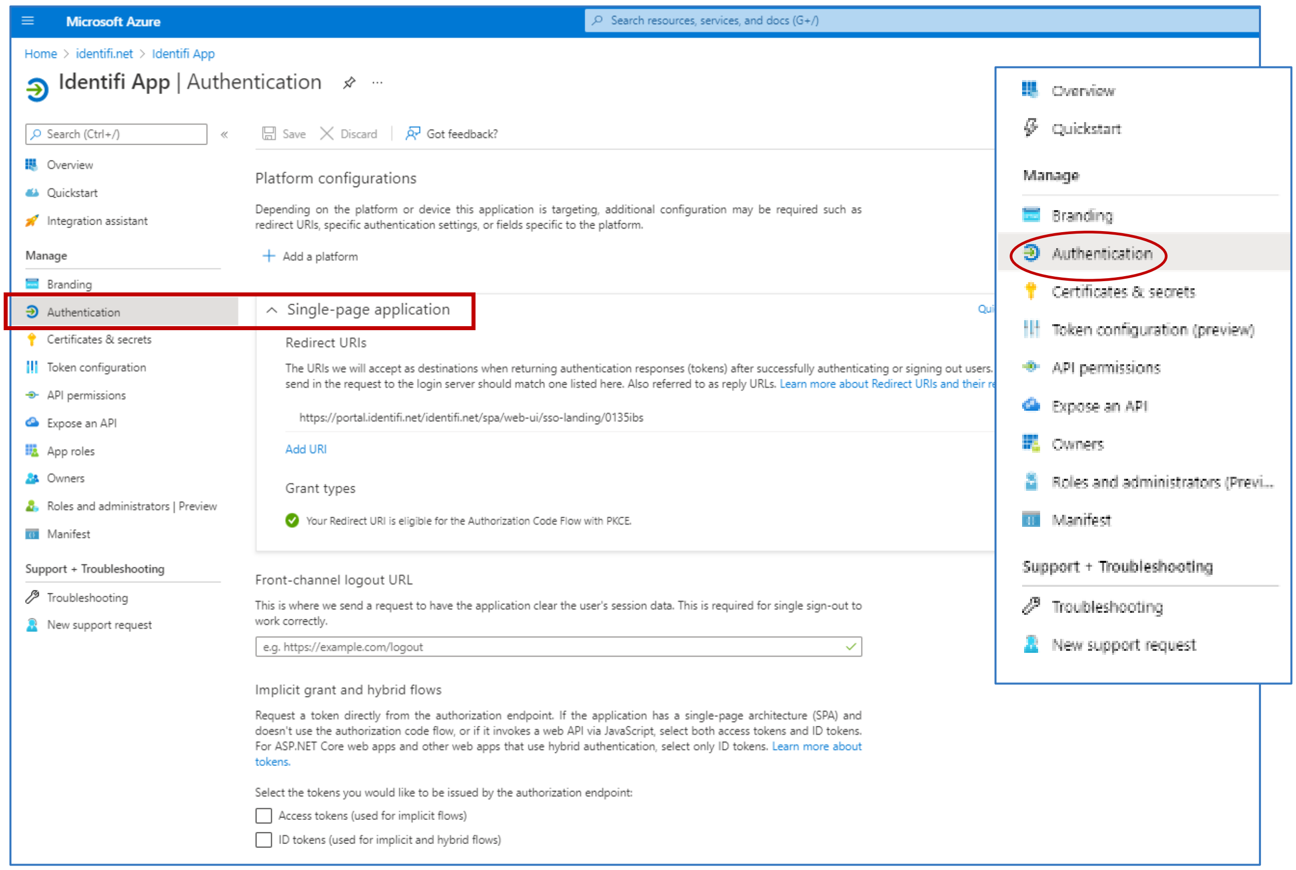
The redirect URI that is configured in Azure must match the redirect URI configured in Identifi in order for this integration to work properly. There are some important aspects of the redirect URI that are important to understand:

- The URI should use the https: protocol to ensure the security of the authentication response and ID token.
- The [servername] must match the fully qualified domain name of the Identifi web server as it appears to users in the browser. For example, if the user accesses Identifi via "https://abc123.identifi.net/identifi.net", the fully qualified domain name "abc123.identifi.net" must be used in the redirect URI.

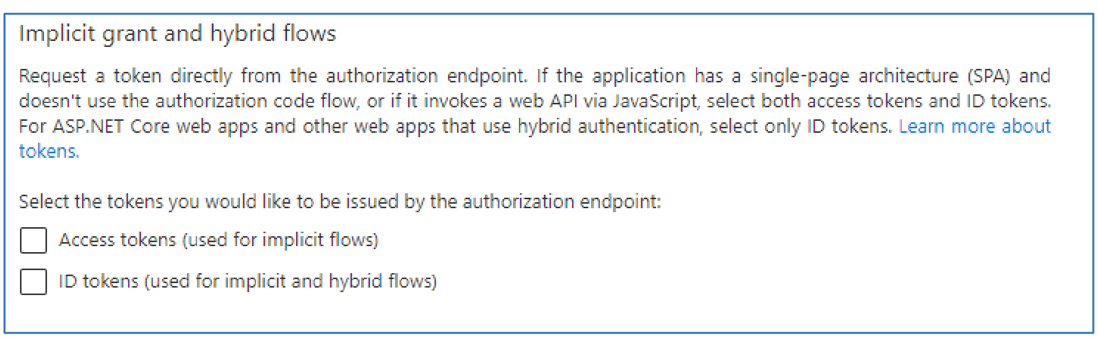
- The [installation name] must match the “internal” installation name associated with your Identifi installation. The internal installation name can be found on the Installation Detail page
- The redirect URI must match the redirect URI configured in Identifi exactly.

7. Click the ‘Register’ button and then the application will be created. 

8. Click the ‘***Authentication***’ menu item



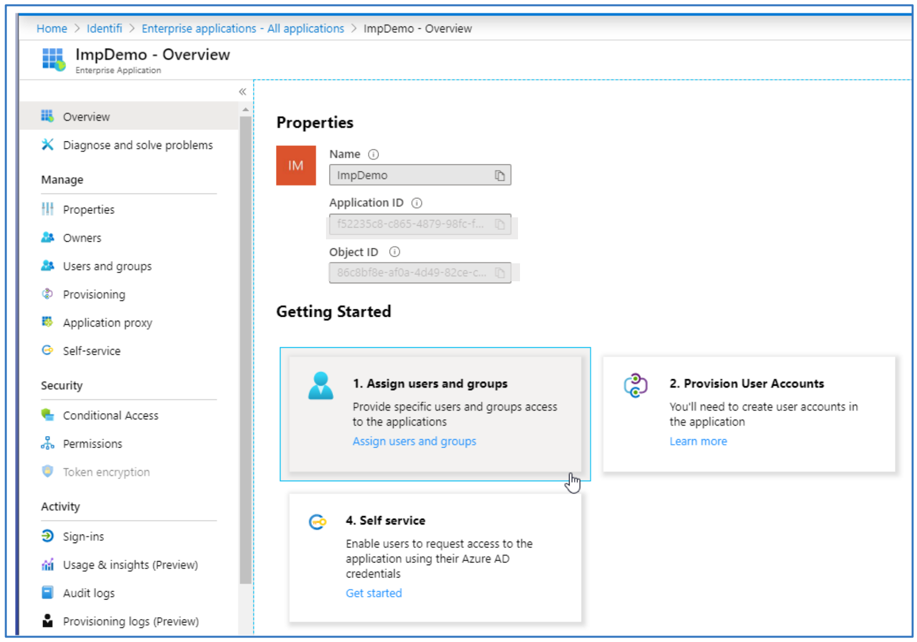
9. Select the second checkbox for *ID tokens*

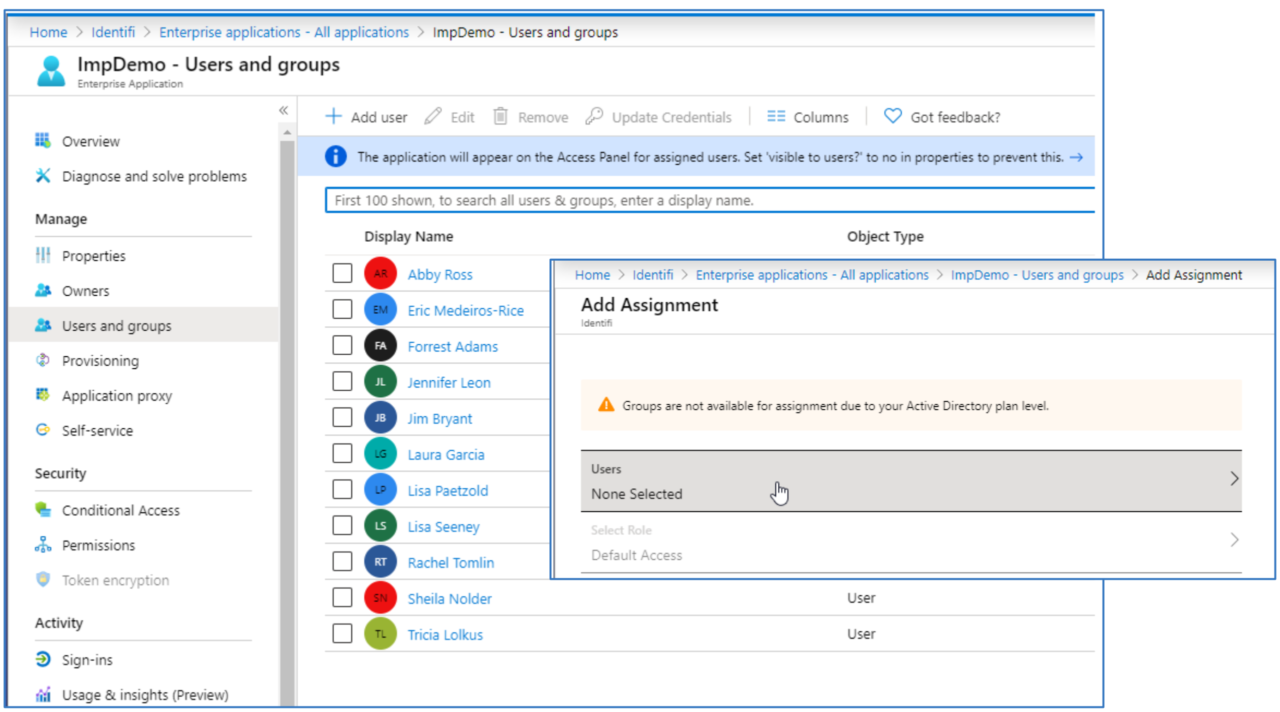


10. Click the ‘Save’ button in the top menu to save the settings  The Identifi application is now registered in Azure.

To further manage the application, including which users and groups have access, click the Azure Active Directory -> Enterprise Applications menu item to view your registered enterprise applications and then click the application you just registered for Identifi integration.

From here you can manage all aspects of the Identifi application, including which users and groups have access to the application.





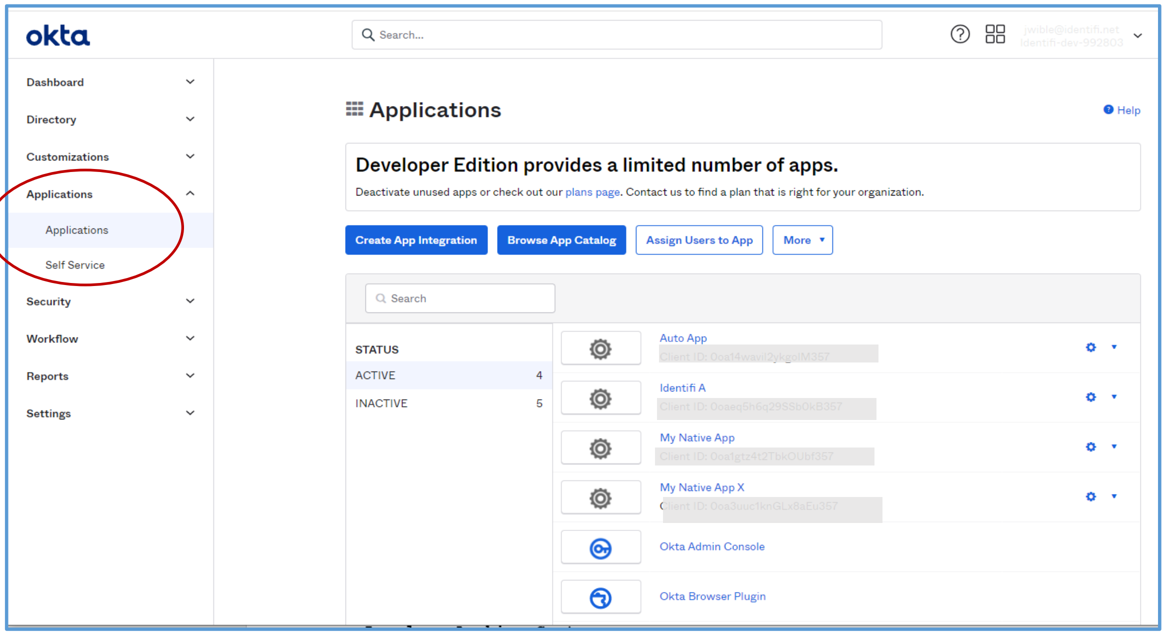
References: https://docs.microsoft.com/en-us/dynamics365/customer-engagement/portals/configure-openid-settings

Okta

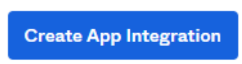
Below are some instructions on how to register and configure the Identifi Application within Okta. This step must be completed before you can configure SSO within Identifi.

Select *Create* ***New Application***

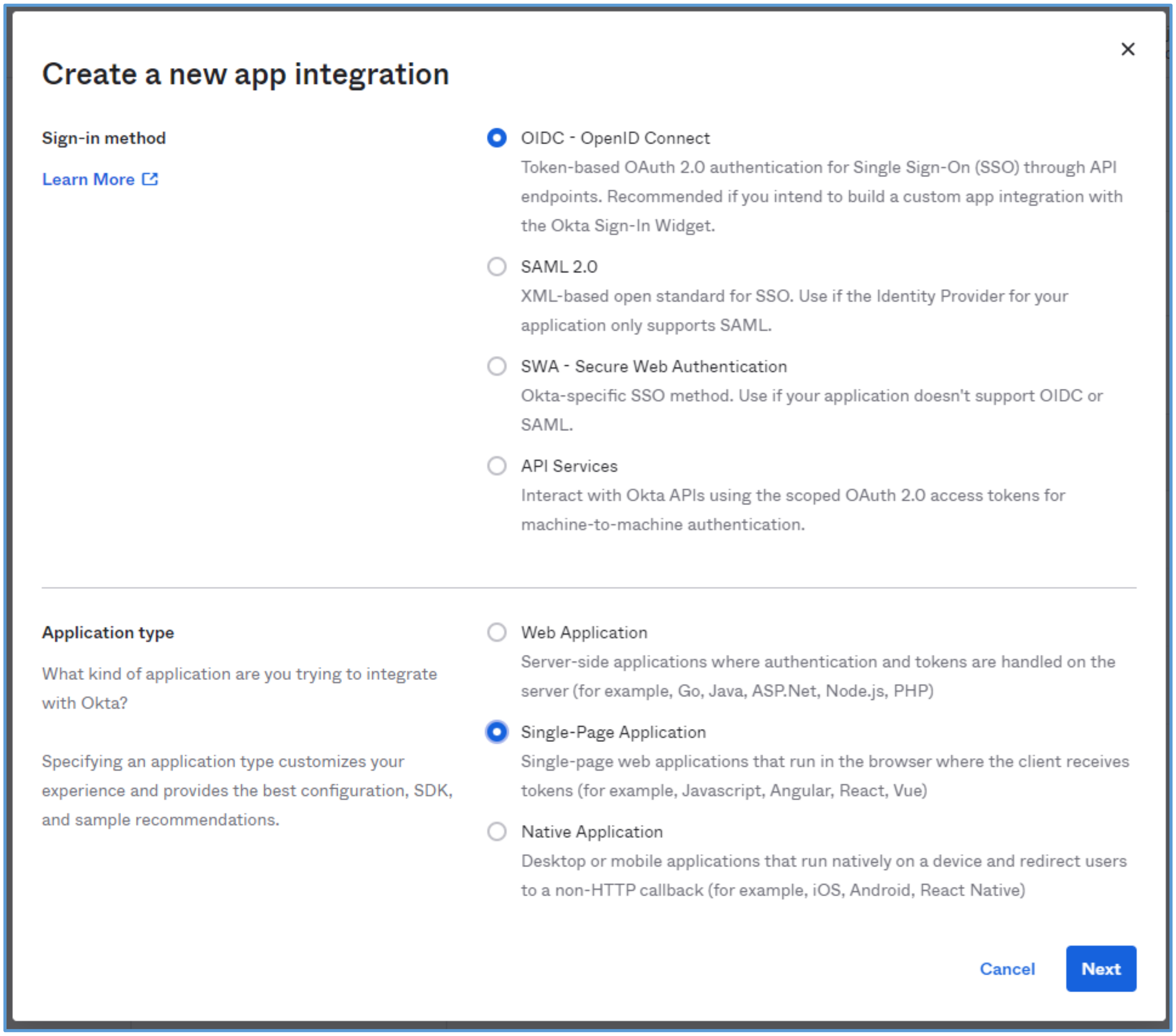
- Select **Applications**



- Then click ***Create App Integration***



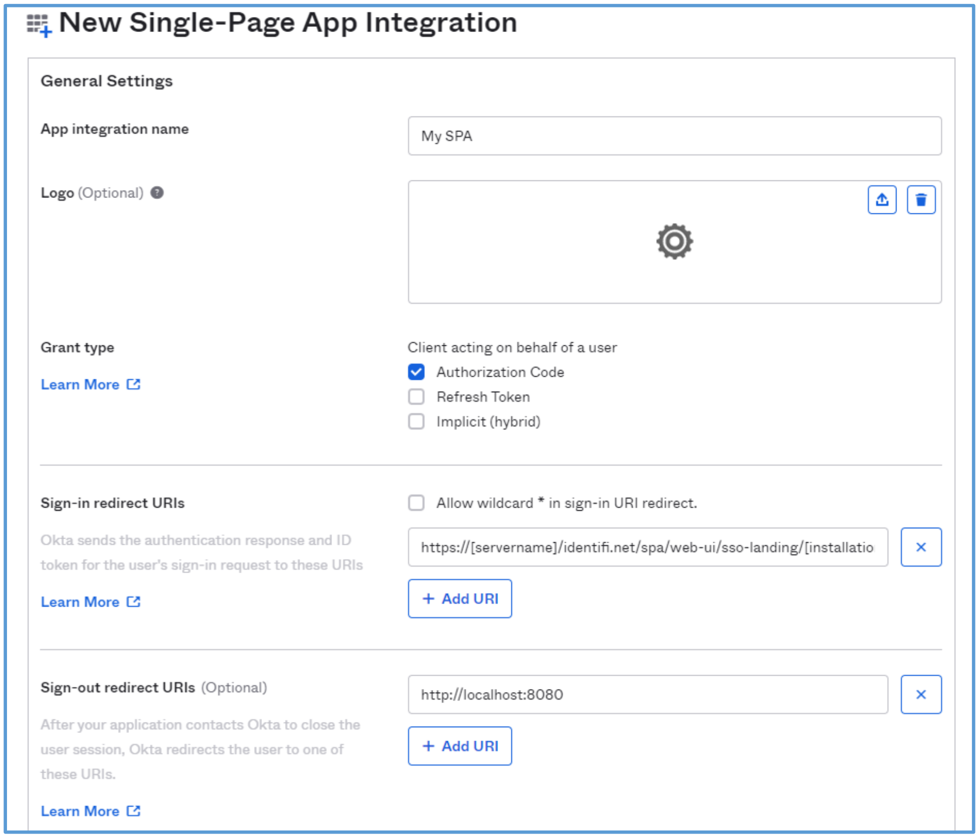
- Select *OIDC- OpenID Connect* as the **Sign On Method** and *Single Page Application* as the **Application Type.**



Single-Page Application Configuration

The following Application Settings are available when creating an Okta Single-Page Application

Field Descriptions

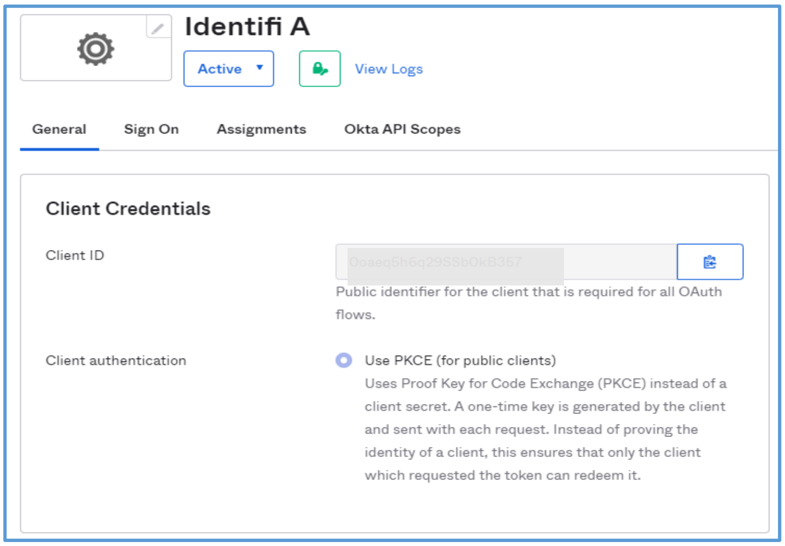


- ***Name***: Enter a descriptive name for this application (e.g. Identifi Server)
- ***Grant Type***: Select **Authorization Code**
- ***Sign in redirect URIs***: A redirect URI is where Okta sends the authentication response and ID token. The redirect URI will need to be configured to reflect the Identifi server's URL. For example: 'https://[servername]/identifi.net/spa/web-ui/sso-landing/[installation name]". The redirect URI that is configured in Okta must match the redirect URI configured in Identifi in order for this integration to work properly. There are some important aspects of the redirect URI that are important to understand:
    - The URI should use the https: protocol to ensure the security of the authentication response and ID token. Okta allows the use of the http: protocol, but this should not be used in a production environment.
    - The [servername] must match the fully qualified domain name of the Identifi web server as it appears to users in the browser. For example, if the user accesses Identifi via "https://abc123.identifi.net/identifi.net", the fully qualified domain name "abc123.identifi.net" must be used in the redirect URI.

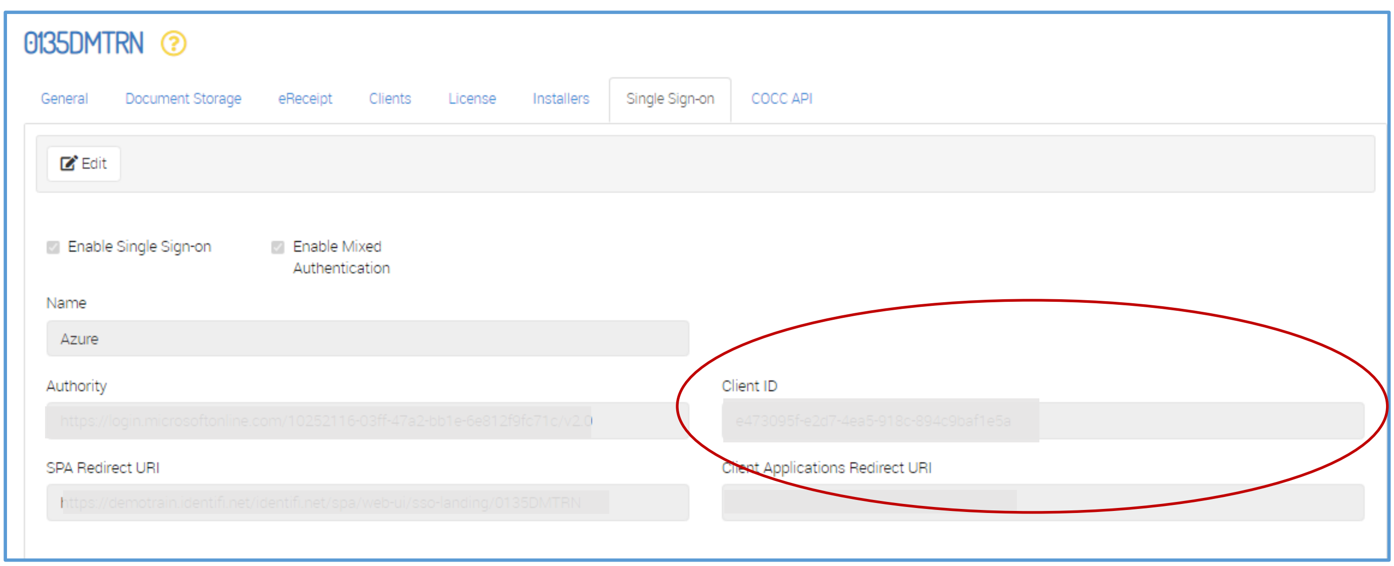
- The [installation name] must match the “internal” installation name associated with your Identifi installation. The internal installation name can be found on the Installation Detail page.

- Click **Save.**

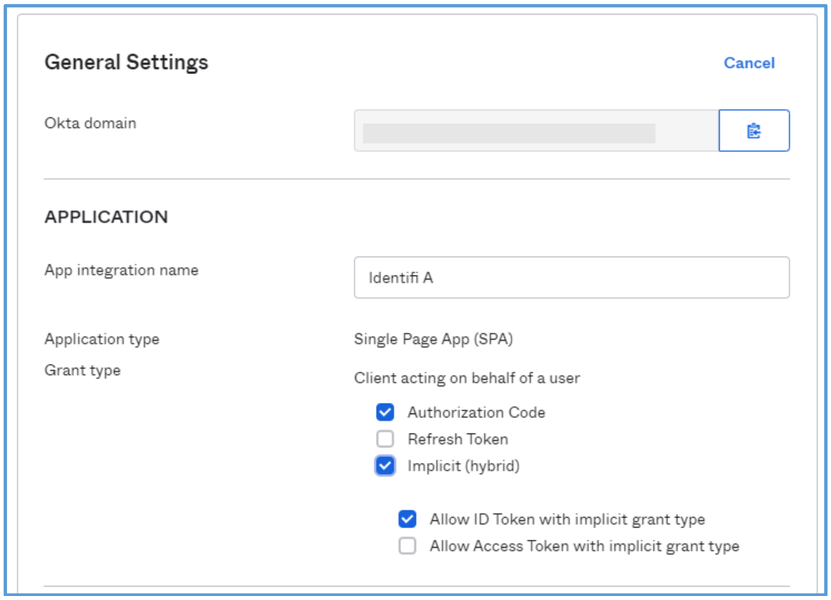
Once the application is created, you will see a screen like the following which includes the Client Credentials.



- The Client ID will need to be configured in Identifi in order for the Single Sign-on integration to work. Navigate to ***Setup- Installations- [Installation Name].***

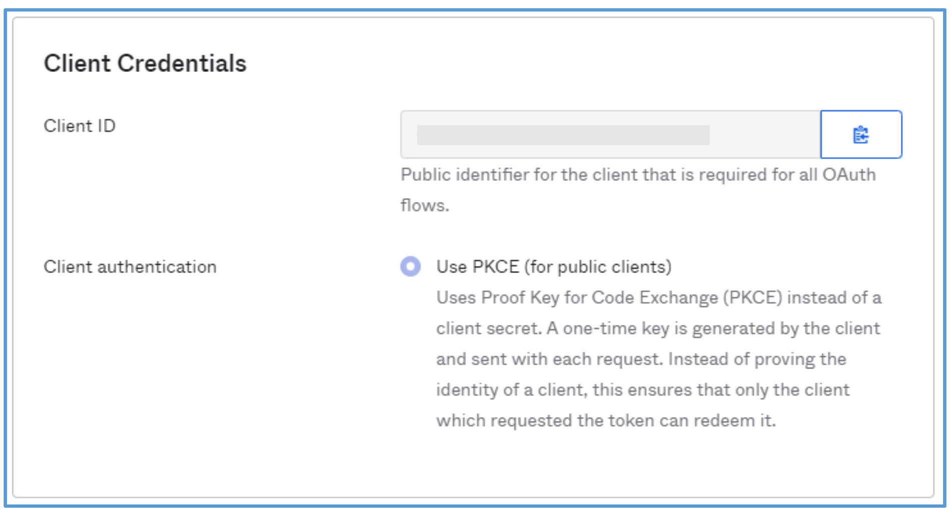


- Back in the Okta application, click **Edit** in the General Settings section to address the following. Place the checkmarks as pictured below:



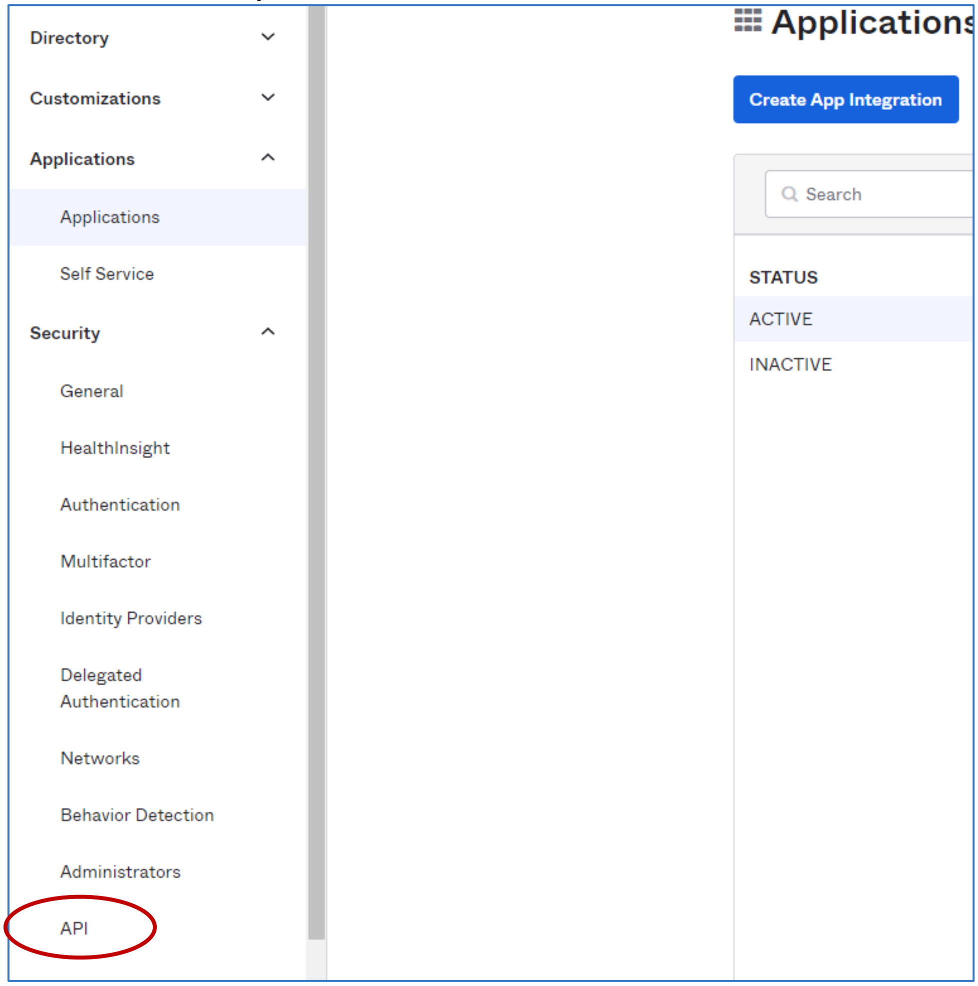
This needs to be configured to allow *Authorization Code* and *Implicit (hybrid)*. ***Do not select to Refresh Token.***

Choose *Allow ID Token with implicit grant type* below.

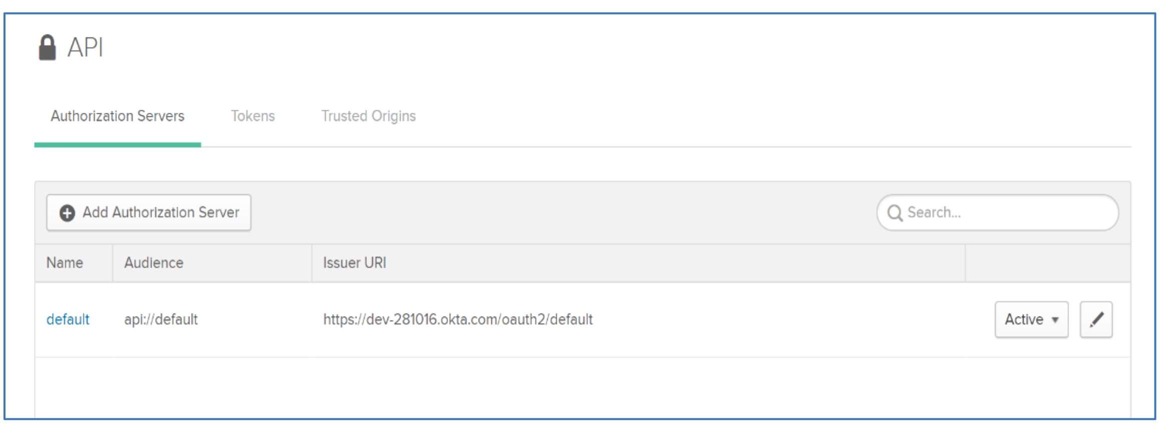


Setup a default scope

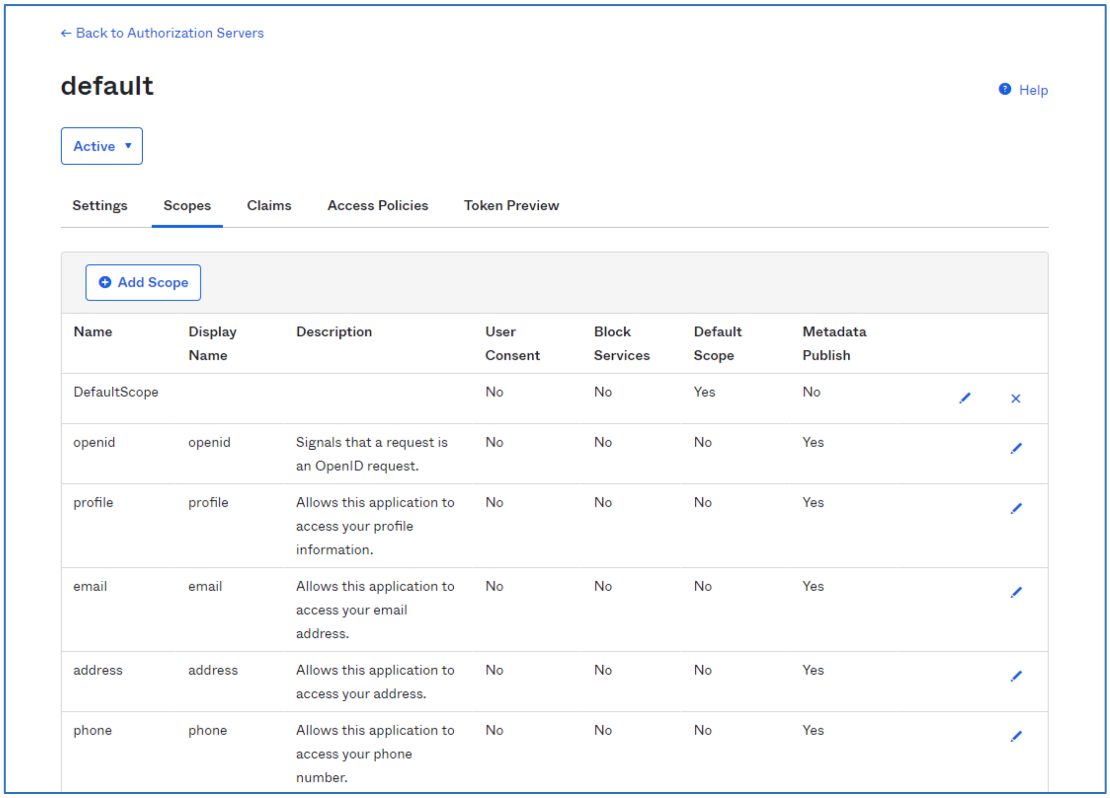
Click on the Security -> API and locate Authorization Servers.



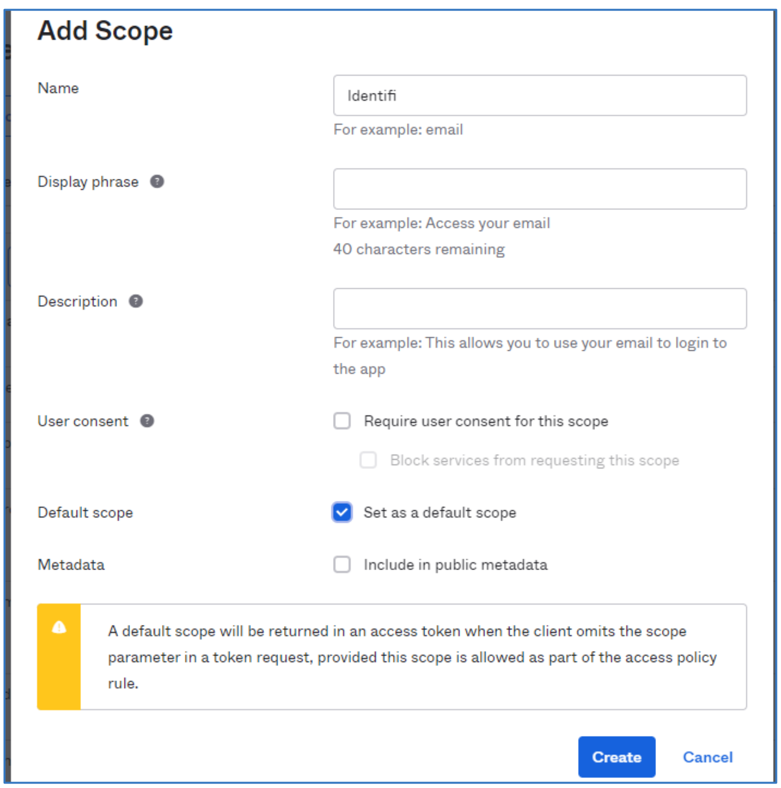
The authorization server will display.



Click the hyperlink for the default authorization server to open the settings:

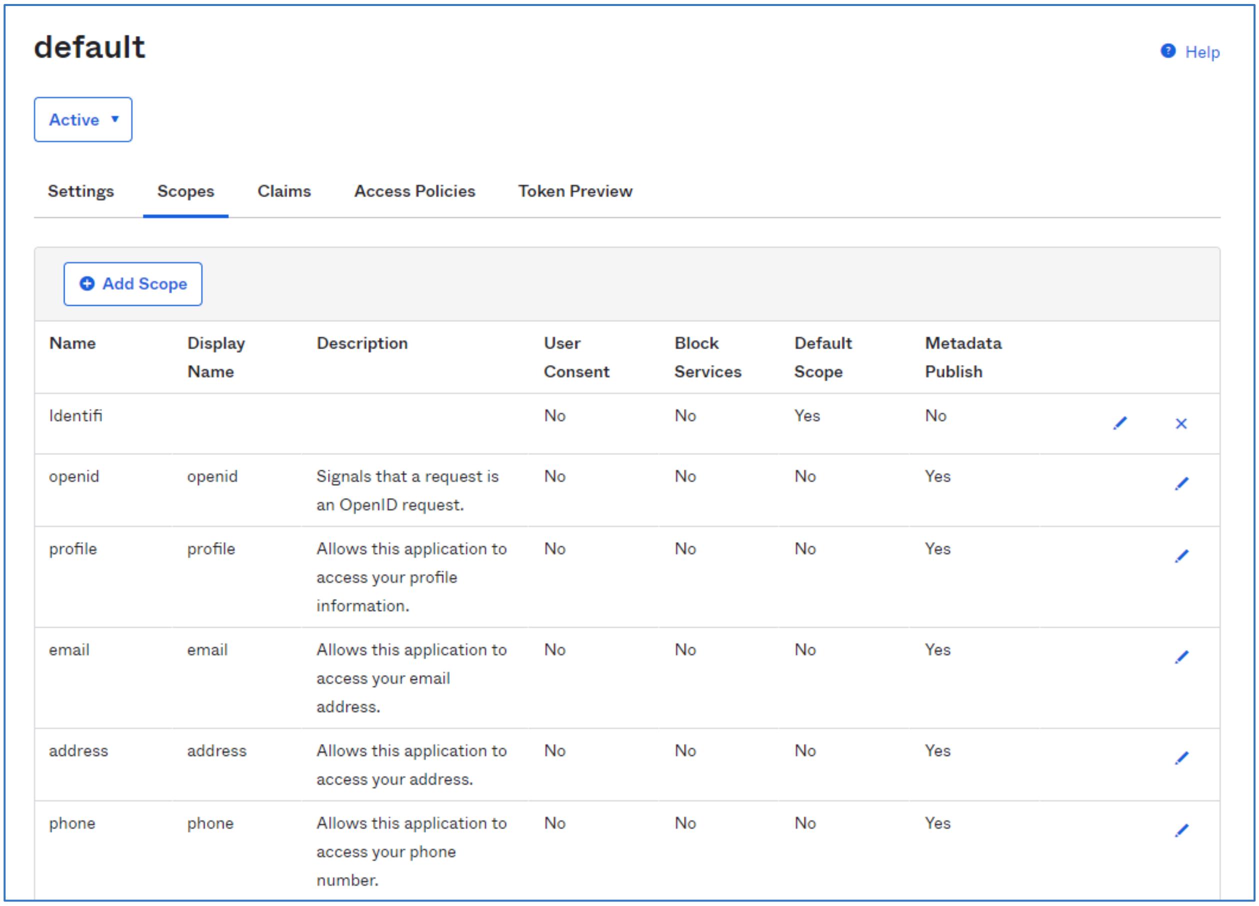


Click on the Scopes tab and click Add Scope:



Enter the name Identifi, check the Set as a default scope checkbox, and click the Create button.

The new default scope will be created and added to the list:



Name	Display Name	Description	User Consent	Block Services	Default Scope	Metadata Publish
Identifi			No	No	Yes	No
openid	openid	Signals that a request is an OpenID request.	No	No	No	Yes
profile	profile	Allows this application to access your profile information.	No	No	No	Yes
email	email	Allows this application to access your email address.	No	No	No	Yes
address	address	Allows this application to access your address.	No	No	No	Yes
phone	phone	Allows this application to access your phone number.	No	No	No	Yes