



# eSign Cloud System Administration Guide

## Using this Guide

The self-paced learning approach to the implementation of IMM eSign provides an institution with control over the pace at which its employees will learn the materials needed to understand, implement, utilize, and support their solution.

This guide serves as a reference tool as well as a companion guide to the lessons in Stage 3: System Administration. This guide is a combination of the smaller guides provided within each lesson.

The purpose of Stage 3 is to provide a deep dive into all the Administrative screens, options and settings with the exception of Template and Attachments, which will be covered in Stage 4. During this Stage you will begin to implement some of the decisions made in Stage 2 and documented in your Implementation Workbook. Since you will be learning more specifics about each of the administrative setting and options, you will also make new decisions and/or refine others. We recommend that all members of your implementation team engage in all the training elements of Stage 3 even if not all will be directly responsible for system administration. This way you'll be able to gather input from all parties as needed.

The guides and lessons in this Stage should be used in concert with the Implementation Workbook, which will serve as a single location for documenting and maintaining your decisions. If you have not done so yet, the workbook can be downloaded from the main Stage 2 webpage.

You should watch the videos located on the lesson pages and use this document (or the individual Reference Guides available on each lesson page) as a reminder of what you learned and perhaps a place to make notes and identify areas of question or concern.

The guides in this Stage will also include recommended activities for steps that should be taken when setting up your eSign solution.

The lessons in Stage 3 will enable you to:

- Configure many elements your IMM eSign Cloud solution with the exception of Templates/Attachments
- Continue making decisions about how your users will interact with eSign
- Continue making decisions about how your customers will interact with eSign
- Understand the options in Adobe Sign that will affect the remote signing experience

## Contents

	Page
Lesson 1: Navigating and General Settings .....	3
Lesson 2: User and Group Settings .....	14
Lesson 3: Archiving and Imaging .....	24
Lesson 4: Setting Signing Options .....	34
Lesson 5: Additional Administrative Topics .....	46

# Lesson 1: Navigating and General Settings

---

## Overview

Now that your installation activity is successfully complete, you have access to your eSign solution and can begin setting it up.

As with any new software application, there is an adjustment period of becoming comfortable with the components, options, and navigation of the solution. This first lesson covers basics around navigating the IMM eSign application and online documentation and will present the General Settings configuration screens.

The key elements of this lesson are:

- Accessing and navigating the IMM eSign cloud application on the desktop
- Exploration of the help menu and online documentation
- Thorough presentation of the general settings
- Enablement of your eSign System Administrator to set options according to your solution needs

And after watching the video you should:

- Understand how to launch IMM eSign in all situations
- Be able to search for online help on a specific topic
- Configure your IMM eSign system's general settings

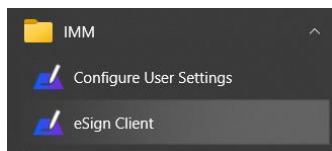
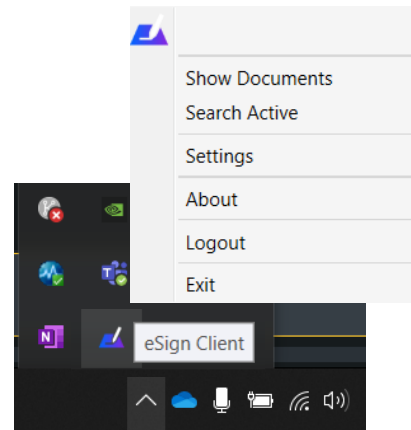
## Activity Checklist

- Watch the Lesson 1 video
- Explore the online help documentation to get familiar with how it is organized and how to perform searches
- Go into the General Settings area of Administration. Make any desired changes, and take note of any questions or concerns you may have

## Accessing eSign

Accessing eSign for most users will be as simple as sending a document from a business system or desktop application. Sometimes, however, you will need to open eSign without adding a new document.

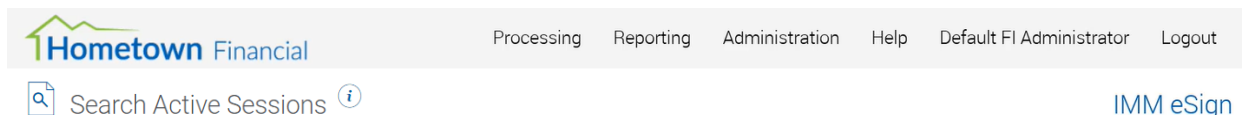
In most cases, eSign will automatically start and log you in when you sign into your workstation and in the system tray (bottom right corner) you will find the eSign Client icon. Right-clicking on it will open the menu seen here which allows you to launch a browser at the chosen location in eSign.



If eSign does not automatically log you in, or you do not see this icon or menu you can launch eSign from the Start Menu by selecting the eSign Client from the IMM Program group. This will place the client option in the System tray.

## Navigation

The header of the eSign screen will look similar to this



The logo you supplied or that you upload will appear in the upper left corner. Below that will be the page title and in some cases a small “i” that, upon clicking, will provide some basic information about navigating the page that you’re on—describing icons and the like.

In the upper right portion of the page are the menus. Depending both on your institution’s setup as well as a user’s access rights you may or may not see all menus or all options in each menu.

The menus include:

**Processing** access to open existing sessions, access collected documents, and go to saved websites.

**Reporting** contains access to multiple management level reports.

**Administration** again depending on user rights provides access to administrative settings, including General Settings, Document Templates, Indexes, Users, Groups, Imaging, and more.

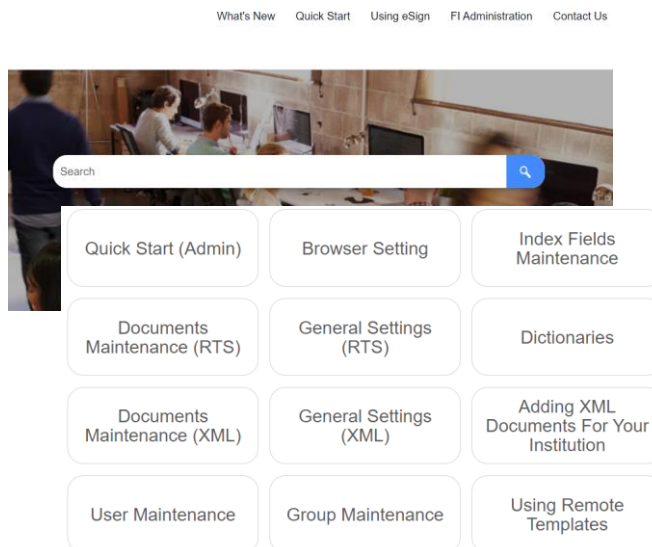
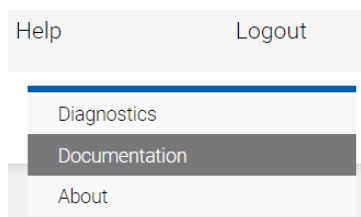
**Help** contains an access point to documentation as well as diagnostic and about information.

**User** this menu is labeled as the user’s UserID and is a way to view user account settings.

**Logout** is important to use when the user is done with their eSign session.

## Help Menu

Nearly every function and option of eSign are documented in the eSign Help Documentation. Users are shown a user specific assortment of help topics based on their permissions.



There are various support topic categories as well as a search bar.

Keep in mind that you may see some options that do not necessarily pertain to your implementation. One such item that could cause some confusion is “XML” and “RTS,” and you might also see “eSign Plus”. These are different “flavors” of eSign used by different institutions. If you are uncertain which flavor you are using, ask your IMM Project Manager, but a general rule of thumb is that banks will utilize RTS and credit unions will utilize XML. However, this is not an absolute.

You can either browse using the categories and menus or use the text search.

## Searching

After opening the Help→Documents screen you can type a word or phrase into the search bar—this is often the most effective way to search. A good rule of thumb is to use the exact language on the page or option you’re searching about.

Your search for "Remote Attachments" returned 27 result(s).

### Remote Attachment Template

Remote Attachment Templates are groups of attachment definitions that can be associated with discrete processes (Car Loan, Home Loan, etc.). The **Remote Attachment Template** can be applied to any or all individual document signers in a session on the eSignature Management page. Refer to eSignatures ...  
C\_Fa2FaFiMaintRemAtTmplRemote Attachment Template.htm

### Requesting Remote Attachments

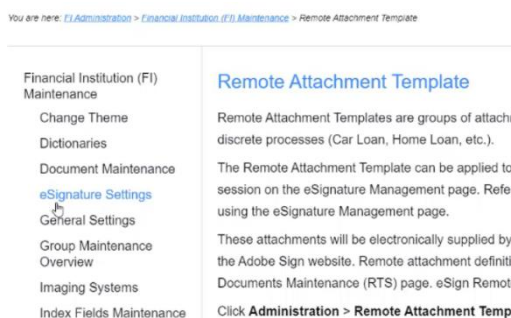
Supporting documents such as pay stubs, W2s, Driver License, Passport, etc. can be requested as required from a **remote** signer using the Request **Attachments** option on the Document Designer page or the eSignature Management page. Prior to requesting **attachments**, a signer must be designated to sign ...  
Procedures/DocumentDesigner/RequestingAttachments.htm

### Remote Signing

eSign provides a simple, guided process to sign and review documents **remotely**. Instead of signing in each signature field in each document, the signer creates a signature that is used throughout the entire signing process. Once the signature is created, the signer must accept the signature to ...  
Procedures/Signing/RemoteSigning.htm

Search results will display as a list of topics showing the category into which the result fits as well as a snippet of the text from the page.

Click on one of the links to open the actual documentation page.



the documentation this topic falls, click on any other topic that might interest you.

There are multiple topics available in the menus at the top of the help screen: some are more user focused and some are more administrative in content. Please note, not all topics will be relevant to your implementation.

## General Settings

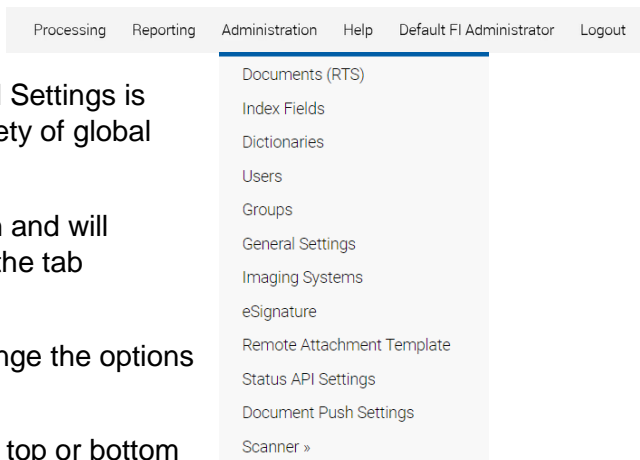
The General Settings option from the Administration drop down menu displays the General Setting screen shown below. General Settings is where the system administrator can set a variety of global system settings.

The fields in the upper section are all common and will display at the top of this screen regardless of the tab selected at the bottom.

There are tabs which, when selected, will change the options in the lower section.

To make changes on this page whether at the top or bottom you will always start by clicking EDIT to unlock all fields.

NOTE: Not all settings shown here will be available for your institution and will depend on options and add-ons used during your installation. Also some fields may only be edited by an IMM installer or support admin.



### General Settings

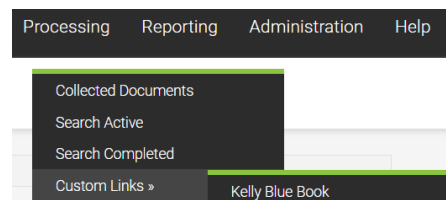
IMM eSign

A screenshot of the 'General Settings' page in the IMM eSign system. The page has a light gray background. At the top, there's a header with a gear icon and the text 'General Settings' on the left, and 'IMM eSign' on the right. Below the header, the settings are organized into two columns. The left column includes: 'Home URL' (http://www.immonline.com), 'Custom Label 1' (Bank of Tim), 'Custom Label 2' (empty), 'Custom Label 3' (empty), 'Custom Logo' (with 'Browse' and 'Upload' buttons), 'Retain Audit Trail (Days)' (90), 'Session Audit Report Time Zone' ((UTC) Coordinated Universal Time), 'Password Unlock Period' (30), 'Unknown Document Label' (Unknown), 'Define Image-Based Documents' (checked), and 'Allowed Domains' (empty). The right column includes: 'Custom URL 1' (http://www.google.com), 'Custom URL 2' (empty), 'Custom URL 3' (empty), and 'Documents Key' (imm\$0IAaWRGt7uJYZ95En03c31vgkDH). At the bottom, there's a row of six tabs: 'Add-Ons', 'Archive', 'Check In/Out', 'eSign Zip', 'eSign Client', and 'Platform Settings'. Below the tabs are three buttons: 'Edit' (with a pencil icon), 'Save' (with a floppy disk icon), and 'Cancel' (with an 'X' icon).

## Header section

**Home URL** creates a link to a website to which users will be taken when the institution logo in the client is clicked – this could be used to direct to your intranet if you like.

**Custom Label** (1-3) and **Custom URL** (1-3) are used to add links to the Processing → Custom Links menu – in the example in the video, we added a link to Kelly Blue Book simply by entering the label and the URL. These fields could also be useful as quick links to an intranet site.



**Custom logo** is how your system administrator can upload your institution's logo if that has not already been done. The allowable formats are GIF or PNG and eSign will automatically resize the logo to be 45 pixels high – it is best to size your logo appropriately prior to uploading to avoid any performance issues.

**Documents Key** is used in *CSi* processing and should be entered by an IMM support resource.

**Retain Audit Trail** is the number of days eSign retains the audit information in the database tables – the default and maximum is 90 days. Note that your *session* audit files will be archived along with your sessions and *this* value is only for running the internal audit report which provides only limited tracking of activities within eSign.

**Login Retries Allowed** is the number of tries allowed for a user (between 3 and 10) before the user's Active flag is unchecked. This is often not applicable as most environments utilize active directory authentication (such as eSign Cloud).

**Auto-Unlock Password** allows that a user will automatically be unlocked the next time they log in so long as the Password Unlock Period has passed. Again, this option is often not applicable.

**Password Unlock Period** (which is measured in minutes) is the amount of time the user will have to wait before their password is automatically unlocked, if Auto-Unlock Password is checked. This option is often not applicable, and the range of minutes is from 10-3600 minutes.




**Session Audit Report Time Zone** set the time zone used in the session audit reports which are different from the audit trail report (referenced above). The session audit report document is created for each session and generally archived with the session documents.

**Unknown Document Label** is what a source document uploaded to eSign will be labeled when a template cannot be applied to it. Unknown is the standard value.

**Define Image-Based Documents** is a setting used by eSign RTS that allows defining and editing image-based (OCR) documents. When not selected, only PDFs with readable text can be used for template recognition. This setting requires an IMM resource for activation.

**Allow domains** is also used by eSign RTS systems and is a list of domains allowed to log into the eSign client. This setting can only be accessed by an IMM installer or support representative.

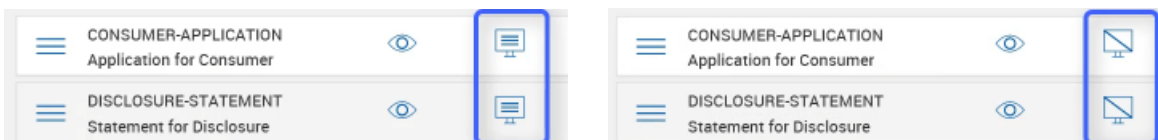
## Add-Ons tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
<div> Edit  Save  Cancel</div> <div><div>Retain Active Sessions (Days):</div><div>90</div></div> <div><div>Archive on Session Expiration (Completed Sessions):</div><div><input checked="" type="checkbox"/></div></div> <div><div>Retrieved Session Default:</div><div><input checked="" type="radio"/> Preserve original selection <input type="radio"/> All documents selected <input type="radio"/> No documents selected</div></div> <div><div>Use common scanner:</div><div><input type="checkbox"/></div></div> <div><div>Expand Session Details Indexes by Default:</div><div><input type="checkbox"/></div></div> <div><div>Download Documents for Session Status (Days):</div><div>365</div></div>					

**Retain Active Sessions (Days)** determines the number of days before an active but unsigned session is retained before it is deleted. When a new session is created by a user, it remains active until it is fully signed and archived which makes it then closed or completed. If a session is not fully signed or archived, it will remain active. This can be set between 30 and 90 days.

**Archive on Session Expiration** will automatically archive completely signed sessions. This may be confusing as it says “Completed Sessions” but it means completely **signed** sessions.

**Retrieved Session Default** determines the state of the document display icons used to set which documents display for document processing. This does **not** impact which documents display to the signing parties. When an active session is retrieved and the document display options were changed when the session was open previously, *Preserve original selection* will honor those selections. *All documents selected* and *No documents selected* set the options as either all selected or all deselected as we see in the examples in the lesson video (and below).






**Use Common Scanner** is a setting for institutions in a thin client environment and is generally deselected.

**Expand Session Details Indexes by Default** determines the look of a session screen to the institution user. With this selected, each document in the session list will be expanded to show the index values. This could offer a good reminder to users to check index values but is often left unchecked. Users can always expand the document details manually.

**Download Documents for Session Status** determines the number of days physical, archived documents are stored in eSign after they are indexed before they are purged. This setting does not impact the database records and the default is 365 days. Since nearly all institutions will be archiving to an imaging system, this can be set to a much lower value if desired.

## Archive tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
---------	---------	--------------	-----------	--------------	-------------------

 Edit  Save  Cancel

Encrypt Archived Documents: ☒

Retain Archived History Docs(Days):

Auto-fill indexes on Session Details : ☒

[Download Imaging Index Service](#)

**Encrypt Archive Documents** protects archived PDF documents by encrypting them. By default, this is turned on and it is not recommended that it be turned off. If it is changed, a password must be entered and would be supplied by IMM Support.




**Retain Archived History Docs** represents the number of days that the DATA about archived documents is kept in the eSign database. The default is 360 days but can be as long as 2555 days (7 years). This setting does not impact the number of days archived documents are maintained by eSign which was set on the Add-Ons tab.

**Auto-fill indexes on Session Details** will fill index field information missing from individual documents from index field information extracted from other documents in the session's document set. When not checked, missing field information will not automatically be populated, but the user will still have the option of clicking the Fill Indexes link. This setting only applies to RTS documents and sessions.

You may see a button in this tab to **Download Imaging Index Service**. It is recommended that you consult with your IMM Installer and/or refer to the help documentation for more information on this download option.


## Check In/Out tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
---------	---------	--------------	-----------	--------------	-------------------

 Edit  Save  Cancel

Check Out

Check In



Use this page to extract and/or install the file(s) needed to support custom fields specific to your FI.  
When you **Check Out** the files, a Zip file will be created which you will be able to download to your local computer. This file may then be sent to your Customer Support representative.  
When you **Check In**, you may specify a single support file or a zip file containing one or more of these support files. They will automatically be placed in the proper location for use by the program.

The Check In/Out tab is used to download and/or upload the file(s) needed to support custom fields and functions specific to your FI.




The most frequently used of these is referred to as the “parameters file.” Whenever you need to make changes to the parameters file you should use this tab to check it out (download it) first. (Unless this is the first time you’re creating it, in which case your IMM Specialist will help you create the file for the first time.)

Click the **Check Out** button which will download a ZIP file to your workstation. Open the file within the ZIP and make and needed changes to it and save it to your desktop with the same file name (e.g., parameters.txt). Once the file is updated (or replaced) and saved, use the **Browse** button to access it and then use the **Check In** button to upload it back into eSign.

As with all changes, you must click the **Edit** button first to start and then the **Save** button once you are done.

## eSign Zip tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
---------	---------	--------------	-----------	--------------	-------------------

 Edit  Save  Cancel

Zip Handler Assembly:




Zip Handler Class:

Zip Handler Password:


This tab is only available/applicable with certain implementations. If it is required, your IMM Specialist will set this up for you.

## eSign Client tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
---------	---------	--------------	-----------	--------------	-------------------

 Edit  Save  Cancel

Input Folder 1:	%InstallPath%\Output
Input Folder 2:	C:\IMM\ManualOutput
Static Output Folder:	
Document Expiration (Minutes):	20
Default Browser:	Chrome 
Access Valid for (Days):	365
Delay for Index File (secs):	0
Enable User Level Settings:	<input type="checkbox"/>

It is unlikely you'll need to make and changes on this tab. These are universal settings that will apply to all eSign clients in your Institution. If necessary, users can be given the rights to alter their own settings, but this is not generally the case.

**Input Folder 1 and 2** are the locations where documents uploaded or printed using the virtual printer will be placed for eSign to import.

**Static Output Folder** is only used for integration with a single institution platform and will be blank by default. If needed, your IMM Specialist will advise you.

**Document Expiration** is the number of minutes a document that has been sent to eSign but NOT added to a session is retained for use. After the time limit is reached the document will be purged and no longer available in the Collected Documents page.

**Default Browser** is the browser used to launch the Collected Documents page. If the selected browser is not available on the user workstation, the user's workstation default browser will be used.

**Access Valid for (Days)** manages long-term access authentication It is unlikely this setting will be used by your institution.

**Delay for Index File** is used when a PDF is paired with an index file for processing and eSign will wait for X number of seconds before importing. This setting is only used with certain specific implementations and your IMM Specialist will advise you accordingly.

**Enable User Level Settings** determines if users can locally edit eSign Client settings. This is uncommon and only recommended in limited circumstances.

## Platform Settings tab

Add-Ons	Archive	Check In/Out	eSign Zip	eSign Client	Platform Settings
No platforms available to customize					

This tab will likely display the message shown above and is only used with certain specific implementations and your IMM Specialist will advise you accordingly.

## Recommended Activities

Determine setting values as a project team.

Document these decisions in the Implementation Workbook.

Make desired changes in your eSign system's General Settings page.

Note any questions or concerns you have so that you can ask your IMM Product Expert during the consulting/training session.

## Lesson 2: User and Group Settings

---

### Overview

You have already learned a great deal about how users are set up and what sorts of permissions exist for users and groups in previous stages. Now it's time to see where those settings are configured and begin configuring them in your solution.

As with any new software application, there is an adjustment period of becoming comfortable with the components, options, and navigation of the solution. This second lesson covers basics around navigating the IMM eSign application and online documentation and will present the General Settings configuration screens.

The key elements of this lesson are:

- Refresher on MS Azure AD/IMM eSign relationship and how users are created
- Detailed exploration of the User Settings options
- Detailed exploration of the Group Settings options

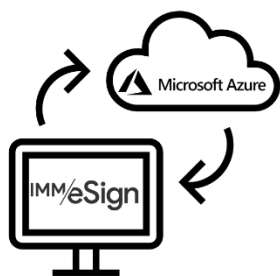
And after watching the video you should:

- Set up an initial set of users in IMM eSign
- Make any desired alterations to the default Users Group
- Set up at least one group in addition to the three default groups to practice how it is done
- Record any questions your team would like to discuss with your IMM Solution Specialist

### Activity Checklist

- Watch the Lesson 2 video
- Review the information you entered in the Implementation Workbook and make updates, changes, additions as needed
- Go into the User and Groups Settings area of Administration and make any desired changes, add users and at least one user group, and take note of any questions or concerns you may have

## User Access



The IMM eSign *Cloud* solution utilizes your institution's Microsoft Azure Active Directory credentials for authentication. (Either previously existing or those created for you by IMM.)

By now your IMM eSign system has been granted permission to your Azure Active directory – this would have taken place during the installation activity.

If you are using a newly created Azure Active Directory, you will need to be sure your users are created. You can do this in the Microsoft Azure Directory Portal. Remember, each person at your financial institution that will be processing documents in IMM eSign will need a Microsoft Azure account. (There is a short reference guide to adding users in Azure located in the Resources section of this lesson.)

## User Settings

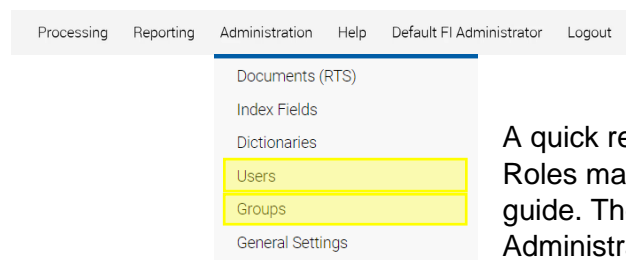
Users will be created in eSign and activated **automatically** when accessing eSign for the first time thanks to the connection with Azure AD.

All new users will be placed in a standard “USERS” group by default and after a user has accessed eSign for the first time, the system administrator can then change their individual permissions and/or user groups, as necessary.

When a user accesses eSign initially and is created, their name and default email should populate based on their active directory information; however, it is always a good idea to verify this since the email address will be essential for remote signing sessions.

Your system administrator should check users' account for: correct user name and email address which will be labeled Default Senders Email.

## User/Group Settings and Permissions



A quick review of Stage 2 | Lesson 1: Users and Their Roles may be valuable in addition to utilizing this lesson guide. The Users and Groups settings are found in the Administration drop down menu as seen here.

## User Maintenance

 User Maintenance 


IMM eSign


Search

Name


User ID


Domain


 Search

 Clear

Total Users : 7  
Selected : 0





 Add

 Delete

 Export

Select All

Sort By

User ID: DocAdmin	Name: Default Document Administrator	
User ID: FIAdmin	Name: Default FI Administrator	
User ID: FIUser	Name: Default FI User	
<input type="checkbox"/> User ID: tester	Name: Test User	
<input type="checkbox"/> User ID: tim (bankoftim)	Name: tim	
<input type="checkbox"/> User ID: usertim	Name: usertim	
<input type="checkbox"/> User ID: usertim (bankoftim)	Name: Tim K	

When accessing the Users option in the Administration menu you will see this screen.

You can easily see the total number of users currently set up in your system, including the 3 default users used primarily by IMM installers and support personnel.


Use the Search component on the left to search for a user by their name, User ID or even domain.

The buttons on the top right let you add a user, delete a user, and also export the list of users and user details to a CSV file.

Click on a line in the list to open the additional information. Click again to close them.

☐ User ID: usertim

Name:



Details


Groups


Permissions

Effective Permission Summary

Partner Alias

eSign Client

 Save

 Cancel


Domain:

Default Senders Email:

Last Login Date:

Active:

☒

 Reset Password

*Expanded view*

## Details Tab

The first tab is Details. It is **important** because this is where you want to check to make sure each user's email address is entered in the **Default Senders Email** field. This will be the email address that will match to the Adobe Sign user account, so it's imperative it is there.

The **Domain** will fill if relevant and the **Last Login Date** is self-explanatory. The **Active** checkbox can be used to deactivate a user, or to activate a user who has become locked out – this is rare in the Cloud environment because of the use of Azure Active Directory. Lastly the Reset Password will almost never be used in the Cloud environment.

## Groups Tab

The screenshot shows the 'Groups' tab for a user named 'usertim'. At the top, there is a header bar with the user ID 'usertim' and a 'Name' field containing 'usertim'. Below this is a navigation bar with tabs: 'Details', 'Groups' (selected), 'Permissions', 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. To the right of the tabs are 'Save' and 'Cancel' buttons. Below the navigation bar is a table with a search bar and a trash icon. The table has two columns: 'Group Title' and 'Description'. It lists four groups: 'Administrators' (Default Administrators Group), 'Call Center' (Call Center Employees), and 'Users' (Default Users Group). Each group has a checkbox in the 'Group Title' column.

<input type="checkbox"/>	Group Title	Description
<input type="checkbox"/>	Administrators	Default Administrators Group
<input type="checkbox"/>	Call Center	Call Center Employees
<input type="checkbox"/>	Users	Default Users Group

The next tab displays the group or groups the user is in. If you want to add or remove a user from a group you can either do it here, or on the groups screens, which are covered later in this document. To delete a group, simply check the box next to the group title and click the garbage can. To add, simply click the plus icon, check off the group in the pop-up window, and click Done.

## Permissions Tab

The screenshot shows the 'Permissions' tab for a user named 'usertim'. The interface includes a header with 'User ID: usertim' and 'Name: usertim'. Below the header are tabs for 'Details', 'Groups', 'Permissions' (selected), 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. There are 'Save' and 'Cancel' buttons. The main content area is divided into two columns: 'Sessions' and 'Documents'. Each column contains three sections with checkboxes and radio buttons.

Section	Option	Selected
Sessions	User Can Search and View Active Sessions	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> User's Sessions Only	
Documents	User Can Delete Unsigned Documents	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> User's Sessions Only	
Sessions	User Can Unlock Sessions	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> User's Sessions Only	
Documents	User Can Process Documents (Existing Session Only)	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> User's Sessions Only	
Sessions	User Can Transfer Sessions	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> No Access	
Documents	User Can Edit Indexes/Imaging Indexes	<input checked="" type="checkbox"/> Apply User's Highest Group Permissions
	<input type="radio"/> Any Session	
	<input type="radio"/> No Access	

The Permissions tab is where you can adjust the permissions for this **specific** user at the user level. By default, new users will have “Apply User’s Highest Group Permissions” selected for all the options. If you make a selection here other than that, your selection will supersede any permissions the user would normally have at the group level for that permission type. This could either give them MORE rights, or less rights. In general, it is advisable to use groups to assign permissions, but there are cases where more granularity is needed for some users, so having this flexibility is helpful. The individual permissions are discussed in further detail in the Permissions Tab under the **Group Maintenance** section below.

## Effective Permission Summary Tab

The screenshot shows the 'Effective Permission Summary' tab for a user named 'usertim'. The interface includes a header with 'User ID: usertim' and 'Name: usertim'. Below the header are tabs for 'Details', 'Groups', 'Permissions', 'Effective Permission Summary' (selected), 'Partner Alias', and 'eSign Client'. There are 'Save' and 'Cancel' buttons. The main content area is a table with two columns: 'Permission' and 'Access Level'.

Permission	Access Level
User Can Search and View Active Sessions	Any Session
User Can Unlock Sessions	Any Session
User Can Transfer Sessions	Any Session
User Can Delete Unsigned Sessions	Denied
User Can Delete Signed Sessions	Denied
User Can Archive Sessions	Any Session
User Can Search and View Completed Sessions	Any Session

The Effective Permission Summary tab displays in a list the permissions a user has. In our example, since all the permissions listed at the user level have Apply User’s Highest Group

Permissions selected, this list displays the effective permissions based on the group or groups the user is in.

## Partner Alias Tab

The Partner Alias tab is only used in unique circumstances.

## eSign Client Tab

The screenshot shows the 'eSign Client' tab in a user settings window. At the top, there's a header bar with 'User ID: usertim' and 'Name: usertim'. Below this is a navigation bar with tabs: 'Details', 'Groups', 'Permissions', 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. The 'eSign Client' tab is active. To the right of the tabs are 'Save' and 'Cancel' buttons. The main content area contains several settings: 'Input Folder 1' with a text box containing '%InstallPath%\Output', 'Input Folder 2' with a text box containing 'C:\IMM\ManualOutput', 'Static Output Folder' with an empty text box, 'Document Expiration (Minutes)' with a text box containing '20', 'Default Browser' with a dropdown menu showing 'Chrome', 'Auto Launch eSign in Browser' with a checked checkbox, and 'Display Notification for (Seconds)' with a text box containing '5'.

The eSign Client tab may look familiar as it displays the settings from the eSign client tab on the General Settings covered in the previous lesson.

In the User record, the **User ID** and **Name** may or may not be different. The Name field will be reflected at the top of the user's screen as a drop down menu. As noted in the previous lesson, in that menu there is an option called User account settings. This will display the same tabbed information covered above. For most users, this will be read only. However, users with administrative privileges may be able to make changes there.

## Group Maintenance



IMM eSign

Total Groups : 4 Selected : 0	
<a href="#">+ Add</a> <a href="#">Delete</a> <a href="#">Export</a>	
<a href="#">Select All</a> <a href="#">Sort By</a>	
Title: Administrators	Description: Default Administrators Group
Title: DocumentAdmins	Description: Default Document Administrators Group
Title: Users	Description: Default Users Group
<input type="checkbox"/> Title: Call Center	Description: Call Center Employees <a href="#">Delete</a>

When accessing the Groups option from the Administration menu you will see a screen like the Users screen. Here we see how many total groups we have, including the 3 default User Groups that come with every IMM eSign cloud implementation, as well as any groups that have been added. You have the options to add, delete, and export from the top right, and to search based on group title on the left. Like on the Users screen, clicking on a line will open the additional information.

**Reminder**, when users access eSign for the first time, they will automatically be added to the Default Users Group. Users can be made members of more than one group and a single User that is a part of several groups, will have the **highest** access or **combined** access based on all the groups they are in.

There are only two tabs of concern on the Group Maintenance screen in eSign Cloud: Permissions and Group Members:

Title: Users Description: Default Users Group

[Permissions](#) [Group Members](#) [Save](#) [Cancel](#)

### Permissions Tab

Permissions fall into the following categories: sessions, documents, signing, remote authorization, designer, reports, and administration.

Permissions that pertain to the *session* or *documents* have the same options: namely,

- “Any Session,”
- “Their Own and This Group Members Sessions,” and
- “Their Own Sessions,”
- as well as “Deny Access.”

Most sessions and documents permissions are self-explanatory. They are:

## Sessions

- Group Members Can Search and View Active Sessions
- Group Members Can Unlock Sessions
- Group Members Can Transfer Sessions  
*Transfer means the user can assign another user access to the session. The mechanics of this will be covered in the user training stage.*
- Group Members Can Delete Unsigned Sessions
- Group Members Can Delete Signed Sessions
- Group Members Can Archive Sessions  
*This option only applies for fully in branch signed sessions which require the user to select archive after completion. When a session goes out for remote signature, it will archive automatically after all signatures are obtained.*
- Group Members Can Search and View Completed Sessions  
*This refers to **completely signed and archived** sessions. This option provides access to the **Search Completed** menu item under the Processing menu.*
- Group Members Can Add Documents/Attachments to Sessions

## Documents

- Group Members Can Delete Unsigned Documents
- Group Members Can Process Documents (Existing Session Only)  
*Allows users to enter data in data entry fields on documents before being sent to signers. These data entry fields are added in the templating process and can be available to either employees or only to signers to complete. A user must have this permission to fill those fields using the Process function*
- Group Members Can Edit Indexes/Imaging Indexes  
*Allows users to edit captured index values on the session screen*
- Group Members Can Reindex Documents (The only option is Allow to Reindex or not)  
*Allows users to reprocess a document or documents through the indexing service which creates the archive files. This may be necessary if an incorrect index was captured on documents or there was some validation error that needs to be corrected. In most circumstances, this permission is limited to users at an **administrative** level.*
- Group Members Can Modify Document Visibility Action  
*Allows users to turn off the viewing of documents or attachments that do not require signature*

**Note** that if “Deny Access” is the choice for a permission type in a given group and a user is in that group AND another group that otherwise provides access, the “Deny Access” will **supersede** access given for that permission type in the other group or groups.

The additional permission types have different choice options, but “Deny Access” (or in a few cases, simply no access) is still an option.

## Signing/Remote

- In Person Signing  
*This permission controls both **if** a user in this group can perform the in-person signing process at all and if they can, what **signing types** are they allowed to use*
  - **Options:** Type, Draw, Signature Pad, Deny Access*The Remote Access Authentication and eDelivery Access Authentication options are set in the system setup done by your installer. If there is an option not displaying that you require, please reach out to your IMM Project manager using the support request form.*

*The options checked will be the options available to users in this group*

- Remote Access Authentication (to send sessions for remote signing)
  - **Options:** Email, Password, KBA, Phone, Government ID, Deny Access
- eDelivery Access Authentication (to send sessions for eDelivery)
  - **Options:** Email, Password, KBA, Phone, Government ID, Deny Access
- Remote Action Completion Order (the order in which remote signers sign)
  - **Option:** Change Completion Order (*by default users cannot change the order*)

## Designer

Designer is a tool available to users to make certain adjustments to documents in a session. These might include assigning a template to an unknown document, managing signature or initial fields by assigning party information or setting them as required or not, or adding, editing, or deleting other fields. Although most templates will handle the bulk of this decisioning for the user, there are circumstances where some user intervention is required, and **Designer** is the tool for that job. The functionality of Designer will be covered in lessons in later stages.

- Can use Designer Application
  - Allows user to open session documents in the designer make needed adjustments*
    - **Options:** Any Session, Their Own and This Group Members Sessions, Their Own Sessions Only, Deny Access
- Review Assignments in Designer
  - Specific to signature and initial fields—allows the user to review party assignments, change the party assigned to a field if necessary, and mark a field as required or optional where applicable*
    - **Options:** Any Session, Their Own and This Group Members Sessions, Their Own Sessions Only, Deny Access
- Can Define Unknown Documents
  - Allows the user to select one of the **previously defined** templates to assign to an unknown or unrecognized document. Importantly, this option does **not** give the user the ability to create a new template for the recognition of future documents, but rather only applies to the document in the current session*
    - **Option:** Allow to Define Unknown Documents

## Reports/Administration

- Group Members Can Access Selected Reports
  - **Report Types:** Audit, Login Failure, Sessions Status, Status API Notifications, Remote Signature Status, Error, Transaction Based, Expiring Sessions, Document Push, Remote Signature Batches and Failed Documents, Deny Access
- Create/Modify Group/User Permissions
  - **Options:** Create/Edit Group Permissions, Create/Edit User Permissions
- Create/Manage Templates
  - Allows users to access the Documents (RTS) menu from the Administration menu to define templates and attachments – the main topic of Onboarding Stage 4*
    - **Option:** Create and Manage Templates

## Group Members tab

Title: Users

Description: Default Users Group

Permissions

Group Members

Save

Cancel


Trash

+

Search

<input type="checkbox"/>	Login Id	Name	Default Sender's Email
<input type="checkbox"/>	FIUser	Default FI User	
<input type="checkbox"/>	usertim	usertim	

Use the Group Members tab to add or remove users. (Of course, you can also do this in User Maintenance.)

Click the plus icon  to retrieve a list of available users, place a check in the box by their name and click Done. To delete users from a group, place a check in the box by their name and click the trash can icon.

## Recommended Activities

Determine user and group details and desired permissions as a project team.

Document these decisions in the Implementation Workbook.

Create Groups in your eSign system and, if applicable, assign existing users to these groups..

Note any questions or concerns you have so that you can ask your IMM Product Expert during the consulting/training session.

## Lesson 3: Archiving and Imaging

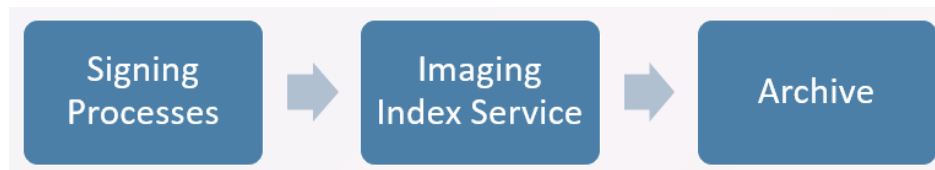
---

### Overview

There are several considerations when it comes to the final step in the eSignature process – the archiving of the signed documents to your imaging system. In this Lesson, we explore IMM eSign’s flexible and configurable architecture, which we introduced in a previous lesson, and set the stage for you to start designing your solution.

As a reminder, the very high-level process flow of eSign consists of the Signing Processes which are managed by eSign and, when remote, Adobe Sign. Once all signing ceremonies are complete, all documents, including the audit files, are organized by IMM eSign and moved to a server in your institution’s environment. A copy of the documents and the data are stored in the eSign cloud for a duration set by you in the General Settings. Any documents sent for remote signature will be stored in the Adobe cloud for a period determined by you, and that setting will be discussed in a lesson devoted to Remote signature.

Finally, the documents and data that are downloaded to your institution’s server will be available for archiving to your imaging system.



The key elements of this lesson are:

- A review of archives and the overall process leading to the archiving of documents to an imaging system
- Discussion and exploration of indexes
- Deep examination of the Imaging System Settings screen and options

And after watching the video you should:

- Fully understand the default archives the come with any IMM eSign system
- Be prepared to discuss your imaging settings with your IMM Solution Specialist
- Be prepared to discuss your imaging process and requirements with your imaging vendor
- Set up indexes and imaging settings and take note of any questions or areas of confusion

### Activity Checklist

- Watch the Lesson 3 video
- Review the information you entered in the Implementation Workbook regarding documents, indexes, and imaging systems (Documents tab of workbook) and make updates, changes, additions as needed
- Go into the Index Fields and Imaging Systems areas of Administration and explore the settings and options to familiarize yourself with them. Take note of any questions or concerns you may have

## Indexes

Index fields play a major role not only in the processing, categorization, and retrieval of documents and sessions while they are in eSign, but also in the storage of documents in your imaging system.

Index fields, or indexes, fall into three main categories, IMM standard indexes, FI level indexes, and Document specific indexes.

There are several IMM **standard** indexes. Three of them are displayed on the Index Fields Maintenance Screen which we are about to look at and they are:

- IMM Date
- IMM Time
- IMM Transaction ID

There are a few other IMM standard indexes which are available for use in file naming and image archiving as well as email template creation (which will be covered in a future lesson) and they are:

- Archive Document ID
- Document Set Name
- Document Name
- Document Path

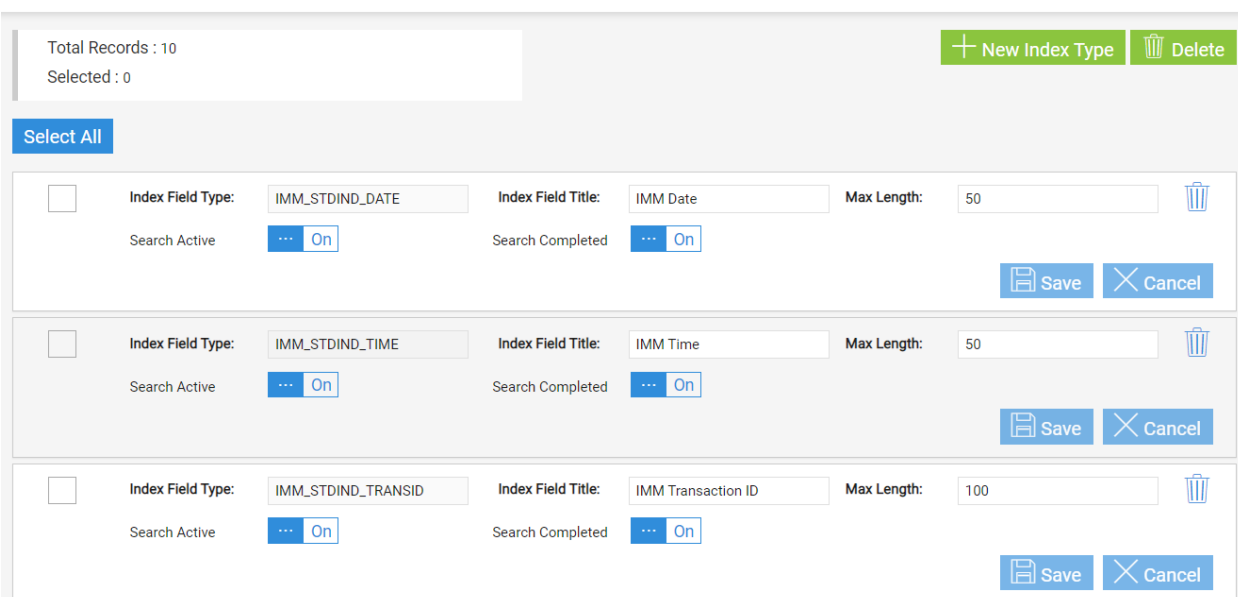
FI level indexes are created and controlled by the Institution. IMM eSign comes with several of these fields as defaults, but not all will be relevant to your environment. The default values include

- Full Name
- Account Number
- Tax ID
- Sub Account Number.

If you do not need these or call them by different names, you can edit their labels and other specifics about them as we'll see below. Institutions can add up to **twenty (20)** different index fields in addition to the 3 standard IMM fields (Date, Time, and Transaction ID)

Lastly there are Document Indexes. This refers to the ability to assign specific index fields to specific documents to address unique archiving situations.

## Index Field Maintenance



Total Records : 10  
Selected : 0

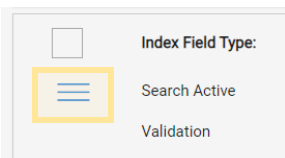
[+ New Index Type](#) [Delete](#)

[Select All](#)

<input type="checkbox"/>	Index Field Type: IMM_STDIND_DATE	Index Field Title: IMM Date	Max Length: 50	<a href="#">Search Active</a> <a href="#">On</a>	<a href="#">Search Completed</a> <a href="#">On</a>	<a href="#">Save</a> <a href="#">Cancel</a>
<input type="checkbox"/>	Index Field Type: IMM_STDIND_TIME	Index Field Title: IMM Time	Max Length: 50	<a href="#">Search Active</a> <a href="#">On</a>	<a href="#">Search Completed</a> <a href="#">On</a>	<a href="#">Save</a> <a href="#">Cancel</a>
<input type="checkbox"/>	Index Field Type: IMM_STDIND_TRANSID	Index Field Title: IMM Transaction ID	Max Length: 100	<a href="#">Search Active</a> <a href="#">On</a>	<a href="#">Search Completed</a> <a href="#">On</a>	<a href="#">Save</a> <a href="#">Cancel</a>

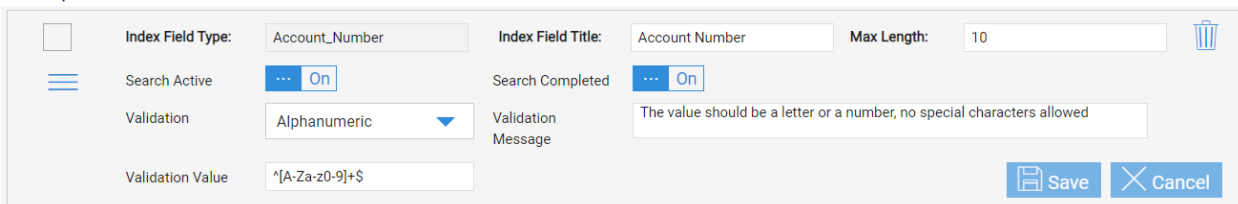
The Index Fields Maintenance page is accessed from the Administration Menu.

The two buttons on the top right are used to add a New Index Type and to Delete an index type. Though the option exists to delete the three standard index fields, this is not recommended.



Below the three IMM fields you will notice the standard provided fields. The main difference visually is that you will see the reorder icon on the fields that are not the IMM fields. You can click and drag on this “handle” to change the order of the FI fields if you like. This will change the order of the fields in the search column when a user is searching for a session. So, it could be helpful to have the most used index for searching at the top.

### Components of an index field.



☐ Index Field Type: Account\_Number

Index Field Title: Account Number

Max Length: 10

[Search Active](#) [On](#)

[Search Completed](#) [On](#)

Validation: Alphanumeric

Validation Message: The value should be a letter or a number, no special characters allowed

Validation Value: \*[A-Za-z0-9]+

[Save](#) [Cancel](#)

**Index Field Type** is predominantly an internal name. Because it is a database identifier, once it has been entered, it is not changeable. Additionally, it cannot contain spaces, but rather only letters, numbers, hyphens, periods, or underscores

**Index Field Title** is required and will display as the value label when users are searching for or viewing documents or sessions.

**Max Length** is the maximum number of characters that can be entered in a field.

**Search Active** and **Search Completed** determine whether this field will display to the user by default in the search column. (Note, users will still be able to use these values to search under an “Advanced Search” option.)

The three validation fields work to ensure that values captured into or entered into fields meet certain criteria.

When validation requirements are not met, the associated document or documents cannot be processed, and the user will see an indication on their screen. This will be covered in the User Training lessons.

The options for validation types are displayed in the **Validation** drop down menu and include Alphanumeric, Alphanumeric or Empty, Date, Numeric, Numeric or Empty, and Custom.

The **Validation Message** will appear on the user’s screen when the value in the index field does not meet the requirements.

And the Validation Value is a regular expression that determines what the allowable characters are – here are some examples:

<i>Alphanumeric</i>	<code>^[A-Za-z0-9]+\$</code>
<i>Alphanumeric or Empty</i>	<code>^[A-Za-z0-9]*\$</code>
<i>Date</i>	<code>^\d{1,2}\/\d{1,2}\/\d{4}\$</code>
<i>Numeric</i>	<code>^[0-9]+\$</code>
<i>Numeric or Empty</i>	<code>^[0-9]*\$</code>
<i>Custom</i>	Any Regular Expression

If you click in any of the blank space in the Index configuration line, more options open up:

The screenshot shows a configuration window for an index field. At the top, there are fields for 'Index Field Type' (set to 'Account\_Number'), 'Index Field Title' (set to 'Account Number'), and 'Max Length' (set to '10'). Below these are 'Search Active' and 'Search Completed' buttons, both set to 'On'. The 'Validation' dropdown is set to 'Alphanumeric', and the 'Validation Message' field contains the text 'The value should be a letter or a number, no special characters allowed'. The 'Validation Value' field contains the regular expression '^[A-Za-z0-9]+\$'. A section below is titled 'Dictionary Code: TeSign Documents'. It includes 'Index Field Name' (set to 'Account\_Number'), 'Default Value' (empty), 'Use for Imaging' (set to 'On'), 'Display Index' (set to 'On'), 'External Index Title' (empty), and 'Imaging Index Title' (empty). There are four 'Functions' listed: 'Custom Function1', 'Custom Function2', 'Custom Function3', and 'Custom Function4'. At the bottom right are 'Save' and 'Cancel' buttons.

**Dictionary Code** is only used in certain situations for certain host and imaging systems where XML is used, it is unlikely you will have an option here. This will say TeSign Documents – TeSign is an older moniker we use to use at IMM.

**Index Field Name** represents the corresponding name in the dictionary. With only TeSign this will default to the Index Field Type name above.

**Default Value** can be used if a certain index type might have a standard value, but still could be changed during the process. E.g., maybe this is a system name or number that is used for archiving purposes. This is not frequently used.

**Use for Imaging** represents whether this value will be available in the configuration of archive files. This defaults to ON.

**Display Index:** When this is On, the index will display to the user when they expand details on a document in Session Details, Search Active results, and Search Completed results.

**External Index Title** is used with specific Host/Imaging system combinations to match XML field names. If blank, the Index Field Type name is used.

**Imaging Index Title** is also used only in specific circumstances to label a field name in a generated XML for the imaging system. When used, the Imaging Index Title is displayed instead of the Index Field Name in the generated XML output.

**Functions** – Custom functions may optionally be used to modify the data stored. You can replace characters, delete characters, change date formats, etc. Functions are applied in order: Custom Function 1, Custom Function 2, Custom Function 3, Custom Function 4. Functions are generally used to address unique situations and it is recommended that you work with your IMM solution expert if you have a need for these functions. There is additional information available in the online documentation. Simply search by “Custom Functions.”

After making any changes to the index configuration, be sure to click **Save** before navigating away from the page.

## Archiving to Imaging Systems

Facilitating the moving of your signed documents to your imaging system is a key component of the IMM eSign product and our Implementation Teams are ready to help you. That said, we are just a **facilitator** in the process. As discussed previously, it is imperative that you understand any requirements of your imaging system, acquire any necessary modules or ancillary products that may be needed, and coordinate with your imaging system team. The earlier this process is started, the better.

## Imaging System Settings



Imaging System Settings

IMM eSign

Imaging System:  
Index TXT

None

ImageSoft

OTG

ProfitStars SYNERGY

Other XML

Other TXT

Index TXT

eFichency

AccessRMS

True Image

Bluepoint

Imagio

Bankware

AMS

Nautilus

Galaxy

☐ Use FI Level Indexes for RTS Documents

The Imaging System Settings is used to configure the file names and data file contents for the files that will be downloaded from the IMM cloud to your institution's server in preparation for archiving to your imaging service.

Changes should not be made to this screen during business hours, and we recommend that any changes required after you have gone live be made with the guidance of an IMM system specialist.

In the drop-down menu there are multiple Imaging System templates that can be used for certain integrations and circumstances. For our purposes, we will use one of the most employed imaging system settings, **Index TXT**. Your IMM Specialist will happily guide you in your decision-making process.

On the screen we see there are three items that will be configured.

**File Name Template** is the NAME of the Index File (that is, the file that contains the index values for the archive document). The import mechanism of the imaging system will be set up to “expect” a certain file name or file name structure.

**Line Template** is the structure of the information on each line of the Index File – one line equals one document. This may contain any of the values from the available indexes list and static values, if needed. Each line will also contain the file name of the archive file as well, which we set in the 3<sup>rd</sup> section.

**Archived File Name Template** is the file name applied to the archive-ready PDF. This file name can contain static values or available indexes but **MUST** include either the Archive\_Document\_ID system value OR BOTH the Document\_Name and IMM\_Standard Time index values. These will ensure each archive file name is unique.

File Name Template

4321\_%FormatDate({IMM\_STDIND\_DATE}, 'yyyyMMdd\_hhmm').txt

Line Template

TAX:{Tax\_ID}%ReplaceCharacters({Account\_Number}, ',')%Lookup({Document\_Name}, 'parameters.txt', ',', '1', 'true'){Full\_Name}\_{Document\_Name}\_{Archive\_Document\_ID}.pdf

Archived File Name Template

{Full\_Name}\_{Document\_Name}\_{Archive\_Document\_ID}

When constructing the three values, you use Available Indexes and Available Functions as needed. Expanding each will display the options below them:

Available Indexes			
(x)	{Document_Path}	Document Path	
(x)	{Document_Name}	Document Name	
(x)	{Document_Set_Name}	Document Set Name	
(x)	{Archive_Document_ID}	Archive Document ID	
(x)	{IMM_STDIND_DATE}	IMM Date	
(x)	{IMM_STDIND_TIME}	IMM Time	
(x)	{IMM_STDIND_TRANS...}	IMM Transaction ID	
(x)	{Full_Name}	Full Name	
(x)	{Account_Number}	Account Number	
(x)	{Tax_ID}	Tax_ID	

Available Functions			
f(x)	%CharFromCode()	Add Custom Character	
f(x)	%Concatenation()	Concatenation	
f(x)	%CreateUserIndexStrin...	Create UserIndex String	
f(x)	%FormatDate()	Format Date	
f(x)	%Left()	Left	
f(x)	%Len()	Len	
f(x)	%Lookup()	Lookup	
f(x)	%PadLeft()	Pad Left	
f(x)	%PadRight()	Pad Right	
f(x)	%RemoveLeadingChar...	Remove Leading Chara...	

The options in the **Available Indexes** list will reflect additions made on the Indexes page discussed above. The **Available Functions** are used to manipulate index values, if necessary, to ensure they are in the correct format for the imaging system.

Consider this scenario:

#### File Name Template

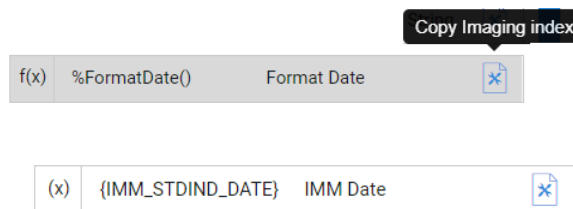
The imaging system vendor has indicated that the index files must be named with the institution number (e.g., 4321) followed by an underscore, then the current date in the format 4-digit YEAR 2 digit MONTH 2 digit DAY followed by an underscore, then the time in HOUR MINUTE.

To set that up, in the File Name Template box, type 4321 and an underscore.

From the Available Functions list choose Format Date and click Copy Imaging Index. This function appears where the cursor is located:

`%FormatDate(dateIndex, format)`

Replace **dateIndex** with the IMM System Date copied from the Available Indexes list.



Then enter the format `yyyyMMdd_hhmm` in place of the word **format** in single quotes.

Lastly, add `.txt` at the end since this will be a TEXT file. The result looks like this:

```
4321_%FormatDate({IMM_STDIND_DATE}, 'yyyyMMdd_hhmm').txt
```

Note: clicking on a function in the Available Functions list will bring up basic information on how to use that function.

### Archived File Name Template

The imaging system vendor doesn't specify what the archive file name should be, but our institution has decided they'd like to have the consumer's name and the document name in case they need to find files by file name.

To set that up, with the cursor in the Archived File Name Template field, select Full Name from the Available Indexes and click copy, then enter an underscore, then select Document Name also from the Available Indexes and click copy and enter an underscore. Lastly, since the file name must be unique, add the Archive Document ID to the end. The result looks like this:

```
{Full_Name}_{Document_Name}_{Archive_Document_ID}
```

### Line Template

The imaging system vendor would like values separated using a PIPE symbol (|) and requires that the account number, the document name, and the archive file name are in each line. Anything else we might add would be ignored by the import tool.

Because the account numbers, when imported into the imaging system, cannot contain any dashes, but the values captured from documents in eSign may contain dashes, a function must be used to remove dashes. Place the cursor in the Line Template box and Copy the ReplaceCharacters function. The function will look like this:

```
%ReplaceCharacters(index, oldValue, newValue)
```

Highlight the word **index** and copy the Account Number from the Available Indexes to replace it.

Insert a dash in single quotes for the oldValue, and then just two single quotes for the newValue (indicating no value). The result will look like this:

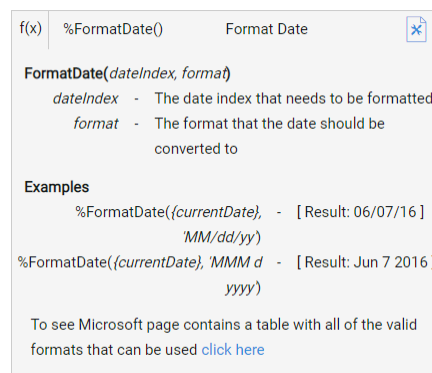
```
%ReplaceCharacters({Account_Number}, '-', '')
```

Additional guidance on the Available Functions can be found in the online documentation using the term Available Functions.

The second field is the document name, so first add a PIPE (|) character. Since the document name in eSign is not the same as the document name in the imaging system, use the Lookup function to swap out the name. In eSign we use a file called Parameters.txt to map eSign document names to imaging system document names when necessary. Your IMM Specialist can help you set that up. To utilize the mapped file copy the Lookup function to the line template:

```
%Lookup(index, fileName, separator, columnNumber, createFlag)
```

Replace **index** with Document Name, **fileName** with 'Parameters.txt', **separator** with a comma, **columnNumber** with the number 1, and **createFlag** with the word true.



```
%Lookup({Document_Name}, 'parameters.txt', ',', '1', 'true')
```

The Parameters.txt file simply contains lines with the eSign document name COMMA the imaging system document name (e.g., DIRECT\_DEPOSIT, Direct Deposit). Note that **separator** is the character used in the parameters file to separate the values. The **columnNumber** is the column containing the replacement value (this being something techy, we start counting columns with zero, so the first value in each line is column zero and the second value, the one we want, is column 1). The **createFlag** determines what to do if the search value (namely the Document Name index) is not found. If this is set to 'true' the system will use the existing Document Name. However, if the process of indexing should fail if the replacement value is not found, set this to 'false'.

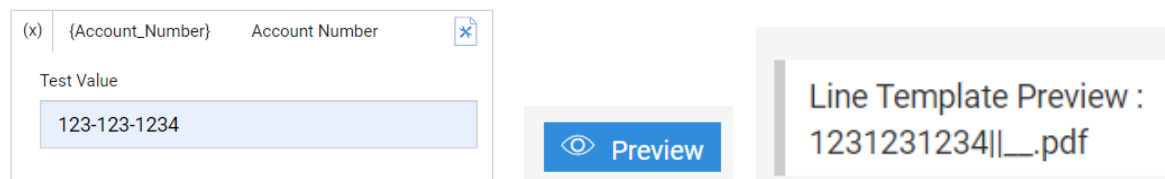
The last element in the Line Template is the archive file name. Copy the string in the Archived File Name Template field and add .PDF. The final entry will look like this:

```
%ReplaceCharacters({Account_Number}, '-', '')|%Lookup({Document_Name},  
                'parameters.txt', ',', '1', 'true')|  
{Full_Name}_{Document_Name}_{Archive_Document_ID}.pdf
```

Then click SAVE.

If you would like to test or preview a function, you can add a sample value by clicking on the appropriate available index and entering a test value and then click Preview.

For example, enter an account number with dashes in it and then click Preview:



The screenshot shows a web interface for testing a line template. On the left, there is a field labeled '{Account\_Number}' with the text 'Account Number' next to it. Below this is a 'Test Value' input box containing '123-123-1234'. To the right of the input box is a blue button with an eye icon and the text 'Preview'. Further right is a preview box titled 'Line Template Preview :' showing the result '1231231234||\_.pdf'.

Remember, you are not alone to figure this all out. The IMM Specialists are ready, willing, available, and highly experienced at setting up these files for nearly all imaging systems. As you can see there are many different options so the **most important step** is knowing what your institution and your imaging system need – then we can help you configure the solution.

## Imaging Index Service

Once a session is sent for archive whether automatically because it had a remote signature component, or manually when your user clicks the archive option, IMM will name the archive files themselves, and start assembling the index file. It will add a line for each archive PDF.

On a scheduled interval, a server in **your environment** will poll the IMM cloud using the Imaging Index Service. This service is a small piece of software that was installed during your installation activity and that runs according to a schedule you set up using Windows Task Scheduler.

The service knows where to look (namely the IMM cloud) and where to place the files (namely a network location in your environment). The service can run at whatever interval you deem necessary.

Once the archive ready files have been copied down it will be up to you to ensure your imaging service tool can access them and import them as needed – and again, we can assist you in determining the specifics of that process.

## Recommended Activities

Determine what index values your institution will require for archiving to your imaging system.

Document the document names as they appear in your imaging system.

Determine what specific addons, set-ups, licenses, are needed from your imaging system vendor to enable document import from eSign.

Go into the Index Fields and Imaging Systems areas of Administration and explore the settings and options to familiarize yourself with them.

Note any questions or concerns you have so that you can ask your IMM Product Expert during the consulting/training session.

## Lesson 4: Setting Signing Options

---

### Overview

The actual process of a person signing documents electronically has a certain flow and requirements. In this lesson we will briefly review the elements already introduced and then look at where the settings are configured in both eSign and Adobe Sign.

The key elements of this lesson are:

- A brief review of the signing elements, considerations, and permissions
- Walkthrough of the eSignature Settings screens, options, and areas of discussion
- Introduction of the Adobe Sign administrative screens and considerations

And after watching the video you should:

- Develop a robust understanding of the signing process both in person and remote
- Apply your institution's decisions around signing in the IMM eSign configuration screens
- Apply your institution's decisions around remote signing in Adobe Sign
- Record any questions your team has to discuss with your IMM Solution Specialist

### Activity Checklist

- Watch the Lesson 4 video
- Review the information you entered in the Implementation Workbook regarding signing decisions (Signing tab of workbook) and make updates, changes, additions as needed
- Go into the eSignature area of Administration and explore the settings and options to familiarize yourself with them. Take note of any questions or concerns you may have.
- Review the Adobe Sign Help pages. The link to these is found on the Stage 3/Lesson 4 webpage and will direct you to <https://helpx.adobe.com/sign/user-guide.html>

## Signing Elements

In previous lessons, you have learned about signing considerations and user permissions set in eSign including those surrounding signing.

Remember, users can sign documents either in person or remotely and when in person, they will generally use some sort of device: signature pad, pen display, or tablet, or possibly use the “keyboard” method which we sometimes call “click to sign.” The in-person user will need to consent to certain terms, create and apply their electronic signature, and confirm their signatures.



The Remote signer will utilize Adobe sign, with which eSign is integrated. They will use their own device (whether a computer, tablet, or cell phone) to also agree to terms, create and apply their electronic signature, and confirm their signatures. They'll also be able to apply their signature using different methods, such as drawing on their device or using their smartphone, type, or upload an image.

In addition, there are various two factor authentication methods available for the eSign user and your institution can administratively decide which methods your users will have access to.

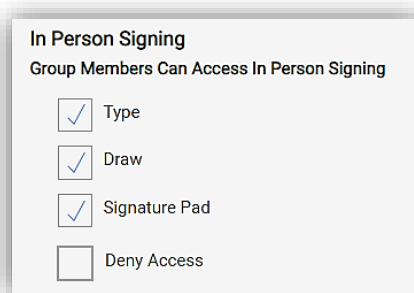
Other than those settings and the institution user's email being set as their default, the rest of the remote signing options (such as the language in the consent and the methods of signing) are set by your Adobe Administrator in the Adobe Sign system **directly**. This lesson takes a look at some of those settings in addition to the eSign settings.

## In Person Signing

There is a single permission type for In Person Signing which determines which methods, if any, an eSign user has when working with an in-person signer. This is in **both** the User and Groups permissions.

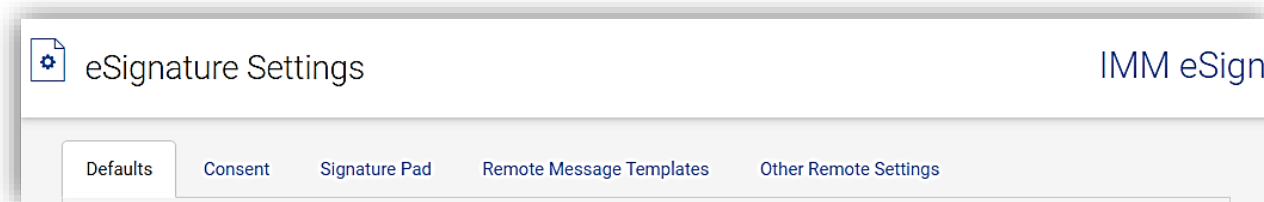
Additional signature settings managed in eSign are located under the **Administration** menu by selecting **eSignature**.

The eSignature Settings page has five tabs.



In Person Signing  
Group Members Can Access In Person Signing

<input checked="" type="checkbox"/>	Type
<input checked="" type="checkbox"/>	Draw
<input checked="" type="checkbox"/>	Signature Pad
<input type="checkbox"/>	Deny Access



eSignature Settings IMM eSign

Defaults Consent Signature Pad Remote Message Templates Other Remote Settings

Remember, you can always go to Help | Documentation and search for “eSignature Settings” if you’d like to review the online documentation.

## eSignature Settings

### Defaults tab

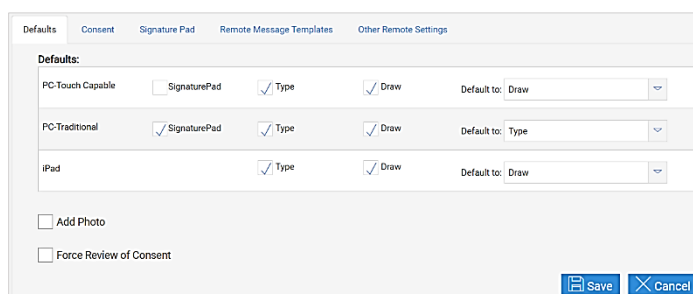
Set the available signing methods and default method that will be used when the eSign institution user is utilizing one of the three workstation types displayed here: PC Touch Capable (e.g., surface pro tablet), PC Traditional (e.g., desktop or laptop), or iPad.

The options for signing are

- Signature Pad
- Type
- Draw

Use case: If your employees utilize standard PCs and some employees will have signature pads and others will have pen display signature devices, you may choose to select only SignaturePad and Draw as available options. By not selecting Type, employees will not have the option to utilize the keyboard to type in a name in place of a signature. The option chosen as the default will be just that, and the employee will be able to change the method if needed.

*Add Photo* enables the Add Photo button on the eSignature Consent page so that employees can capture a photo of the signer to include with their electronic signature.



Defaults Consent Signature Pad Remote Message Templates Other Remote Settings

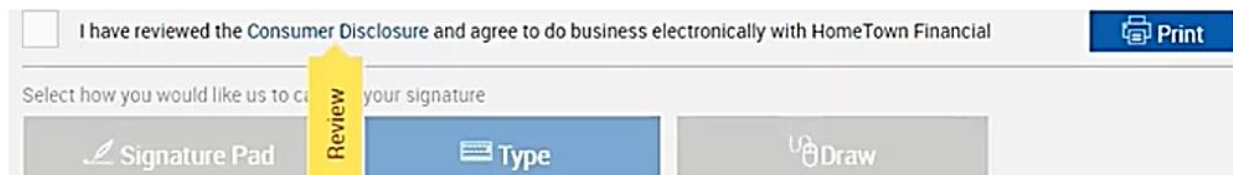
Defaults:

PC-Touch Capable	<input type="checkbox"/> SignaturePad	<input checked="" type="checkbox"/> Type	<input checked="" type="checkbox"/> Draw	Default to: Draw
PC-Traditional	<input checked="" type="checkbox"/> SignaturePad	<input checked="" type="checkbox"/> Type	<input checked="" type="checkbox"/> Draw	Default to: Type
iPad		<input checked="" type="checkbox"/> Type	<input checked="" type="checkbox"/> Draw	Default to: Draw

☐ Add Photo  
☐ Force Review of Consent

Save Cancel

*Force Review of Consent* will require that the user click on the Consumer Disclosure link in order to indicate that they reviewed and agree to your institution's consent language.

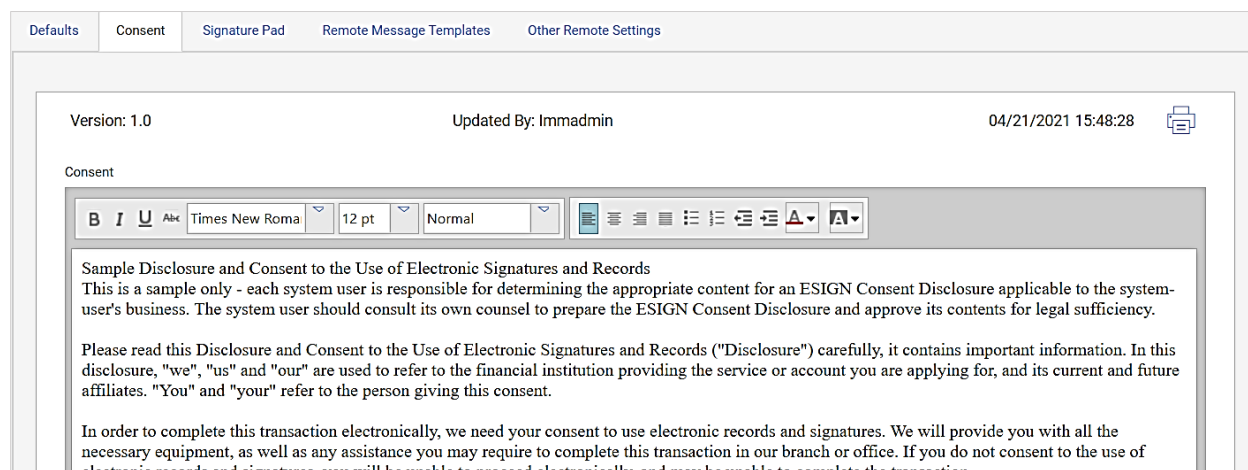


After making changes on this tab be sure to click Save.

## Consent tab

By default, there is wording provided in the Consent dialogue. This is only a **sample** and your team should verify the contents meet with your institution standards.

When you update the consent language, either type directly in the box, or copy and paste from Notepad. Copying and pasting from Word or other word processor may inadvertently copy in embedded control characters and result in undesired effects. The formatting bar at the top of the window provides the ability to add text formatting as desired.



Note that the fonts used may not be compatible with all display devices. Testing is imperative.

After updates are made and the Save button is clicked, the Version number will increment, and the old version will be a new line on the screen so that you can go back to it if needed. Just click on the line to expand the details. The version number will also be shown in the audit report when a signer signs a document in person.

The **Notes** section below the consent language is there if you would like to keep track of changes or any other relevant information about the version.

Additionally, we are required by law to provide you with certain information in this transaction "in writing" which means you have a right to receive that information on paper. However, with your consent, we may also provide this information to you electronically.

Notes

Save Cancel

As always, don't forget to click save after making changes.

## Signature Pad tab

Here, the administrator sets what the user sees when a signer is utilizing a signature pad during an in person signing session and how the signing process will flow. These settings are specific to signature pads and do not apply to other signing devices.

Defaults Consent **Signature Pad** Remote Message Templates Other Remote Settings

☒ Display messages on signature pad (Supported with IE Browser only)

☐ Operator must click "Next" to navigate the signature pad user to the next signature field.

☐ Operator must click "Sign", "Click Here to Sign", "Review", and/or "Confirm Review" to prompt the signature pad user to sign or review.

☐ Turn Off the Backlight after Signing

Consent:  
I, %SignerName%, have reviewed the provided Disclosure and Consent and agree to the Terms of Use.

Signing or Reviewing Message:  
I, %SignerName% %MarkAction% %CurrentDocumentName%.

Importantly, as of the writing of this document, display messages on the signature pad is only supported with the IE Browser. As signature pad manufacturers implement support for other browsers in the future, IMM will enhance the functionality accordingly.

When *Display messages on signature pad* is selected, messages appear on signature pads during the in-person signing process giving signers more control ultimately enabling a faster signing process. When this setting is not selected, the signature pads are blank and are only used to capture signatures and initials.

*Operator must click "Next" to navigate the signature pad user to the next signature field* results in the employee needing to click **next** in order to move the signer from field to field. When not selected, the user will automatically be routed through the documents.

*Operator must click "Sign", "Click Here to Sign", "Review", and/or "Confirm Review" to prompt the signature pad user to sign or review* also requires the employee to click and prompt the signer to act on the item.

*Turn off the backlight after signing* will turn off the signature pad backlight after the signature pad user has completed the signing experience.

There are three message templates that can be set that will display for the signer on applicable Signature Pads: Consent, Signing or Reviewing Message, and Confirm Signing or Reviewing Messages.

Consent:  
I, %SignerName%, have reviewed the provided Disclosure and Consent and agree to the Terms of Use.

Signing or Reviewing Message:  
I, %SignerName% %MarkAction% %CurrentDocumentName%.

Confirm Signing or Reviewing Messages:  
I, %SignerName%, confirm that I %MarkAction% the %DocumentSetName% document set.

Save Cancel

The messages can contain both static text and what are called **monikers**. Monikers are variables that will put unique text in their place.

- For Consent, the only available moniker is: %SignerName%
- For Signing Message, the available monikers are: %SignerName%, %CurrentDocumentName%, %MarkAction%, and %MarkType%
- And for Confirm Signatures, the available monikers are: %SignerName%, %DocumentSetName%, %MarkAction%, and %MarkType%

## Remote Message Templates tab

This tab is used to create customized message templates for the emails signers receive when being notified of a signing session or when receiving documents via eDelivery.

Defaults Consent Signature Pad Remote Message Templates Other Remote Settings

Total Records : 2  
Selected : 0

+ Add Delete

Select All

<input type="checkbox"/>	Template Title: Default Template	Message Subject: %DOCUMENTSETNAME% (for %SIGNER%)	<input checked="" type="checkbox"/> Default	
<input type="checkbox"/>	Template Title: Testing Docs	Message Subject: %DOCUMENTSETNAME% (TESTING)	<input checked="" type="checkbox"/> Set as Default	

To expand the details of a template, click on a template line.

This screenshot shows a configuration window for a template. At the top, there is a 'Template Title' field with the value 'Default Template' and a 'Message Subject' field with the value '%DOCUMENTSETNAME% (for %SIGNER%'. To the right of these fields are a 'Default' checkbox (checked) and a trash icon. Below these fields are two text areas: 'Signing Message' and 'eDelivery Message', both containing the text 'Your documents are available for viewing, signing and printing.' At the bottom right, there are 'Save' and 'Cancel' buttons.

When the user selects a template at the time of sending a session for signing or documents for eDelivery, they can still modify the language if needed to customize or personalize the message.

Signing Message will be used when the email is being sent from the eSignature Management page

This screenshot shows the 'eSignature Management' page. At the top, there is a header with 'eSignature Management' and 'IMM eSign'. Below the header is a navigation bar with 'Design', 'Request Remote Attachments', and 'Back' buttons. The main content area shows a card for 'HALEY WALKER' with fields for 'Email' (demo@email.com) and 'Phone' (555-555-4444). Below this is a 'Message Details' section with fields for 'Sender' (timk@immonline.com), 'Template' (Default Template), 'Subject' (Document Set (for HALEY WALKER)), and 'Message' (Your documents are available for viewing, signing and printing.). At the bottom right, there is a 'Send' button.

eDelivery Message will be used when an email is being sent using the Delivery option:

This screenshot shows the 'eDelivery' page. On the left, there is a green 'Delivery' button. The main content area shows a card for 'HALEY WALKER' with a 'Delivery' icon and a field for 'Email' (email@email.com). Below this is a card for 'WILL IAM NELSON FARMS'. Below the cards is a 'Message Details' section with fields for 'Sender' (timk@immonline.com), 'Template' (Default Template), 'Subject' (Document Set (for HALEY WALKER)), and 'Message' (Your documents are available for viewing and printing.). At the bottom right, there is a 'Send' button.

Like with the consent page, when entering message text you should type directly in the box or copy from Notepad and not copy and paste from Word as embedded control characters may cause erratic behavior.

You can see from the example above that the monikers of SignerName and DocumentSetName can be used in the message subject line. The SignerName will be the full name of the first party

in the session and not necessarily the signer receiving the email. The DocumentSetName will use the Default Product Type Name which we will see on the next tab. (**Note**, this option is more relevant with other eSign products and isn't necessarily useful in this setting. For clarity, simply using static text here is recommended.)

Use the *Set as Default* button to indicate which template will be the default for all users. The other templates will appear in a drop-down list, so naming them in a useful way in the Template Title field is important.

Use the **+Add** button to create a new template.

If you need to delete a template, you can use the trash can icon at the template level or place a check mark in the box or boxes of the templates you wish to delete and click the **Delete** button at the top of the tab.

### Other Remote Settings tab

Sender's Email provides a way to enter email addresses that will appear in the Sender and CC drop down lists when sending a document set for eSignature or eDelivery. By default, eSign will fill the sender field with the current user's default sender's email (which does NOT need to be in this list). However, the user may select a different sender email address or add CC addresses if needed. Note that just like the user's email addresses, these email addresses must be activated with the Adobe sign system to be utilized as the Sender. In most cases, these email addresses must also utilize the same email **domain**; however, if you have more than one domain you may add additional CC domains in this box:

**Note:** it is **not** necessary to add all user's email addresses to the Sender's Email list.

Sender's Email:

<input type="checkbox"/>	Email	Delete
<input type="checkbox"/>	<a href="#">Edit</a> bobtest@email.com	
<input type="checkbox"/>	<a href="#">Edit</a> Bryce.Hometown@immonline.com	
<input type="checkbox"/>	<a href="#">Edit</a> mball@immonline.com	
<input type="checkbox"/>	<a href="#">Edit</a> tim.kanaley@immonline.com	

Additional CC Domain:

CC user receive notifications and can access documents like Sender

Default Product Type Name:

Document Set

Alternate signature pattern:

LightsOut Settings:

LightsOut Default Email:

LightsOut Default Service:

Email Verification

The options below the email list and CC domain are not frequently utilized.

*Default Product Type Name* is the field used to populate the Document Set Name moniker when a document set name is not otherwise provided by your host system.

The additional three options used only in very specific circumstances and will be set or addressed by your installer or consultant.

As always, click save if you've made any changes.

## Remote Signing

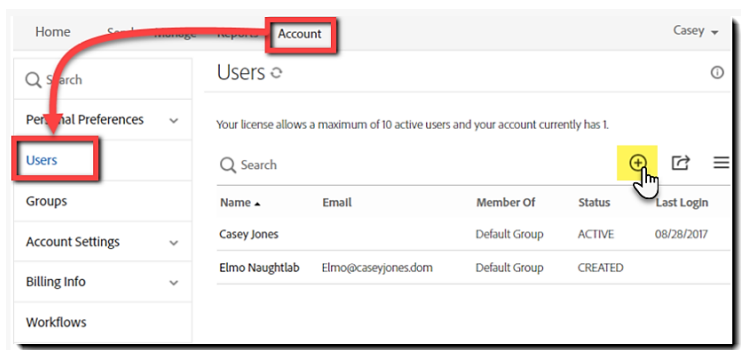
### Adobe Sign

The designated Adobe Sign administrator at your institution will receive a link from IMM that they will use to access Adobe Sign. In Adobe sign, your administrator will need to ensure that all your users have been set up with their email address that matches the value in eSign in the Default Sender Email field in User Maintenance.

#### Adding Individual users

To add a single user to your Adobe account, log in and navigate to the Users section of the Account tab.

Click on the plus sign and enter the user's email address, first and last name, and assign them to the default group on the *Create a user* tab



#### Adding users in bulk

Use the *Create users in bulk* from the same Create Users screen.

You will use a simple CSV file and you can download the sample CSV file and change it accordingly.

All you will need to worry about is Email Address, First Name, and Last Name.

	A	B	C
1	Email Address	First Name	Last Name
2	JohnDoe@emaildomain.com	John	Doe
3	CeliaDoe@emaildomain.com	Celia	Doe
4	FredDoe@emaildomain.com	Fred	Doe

There is a handy “Learn More” link on the tab as well if you would like to explore.

Once you have your CSV of users to upload, you'll simply browse to it and click Import. If you're just adding new users, you can select just the "Allow Create Users" option.

When users are set up in Adobe Sign, they will receive an email with a link to confirm their account and set their password which they **must** do before their account is active.

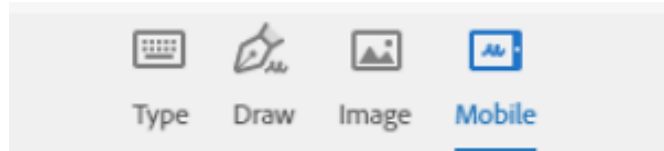
## Additional Adobe Sign settings

### Signature Preferences

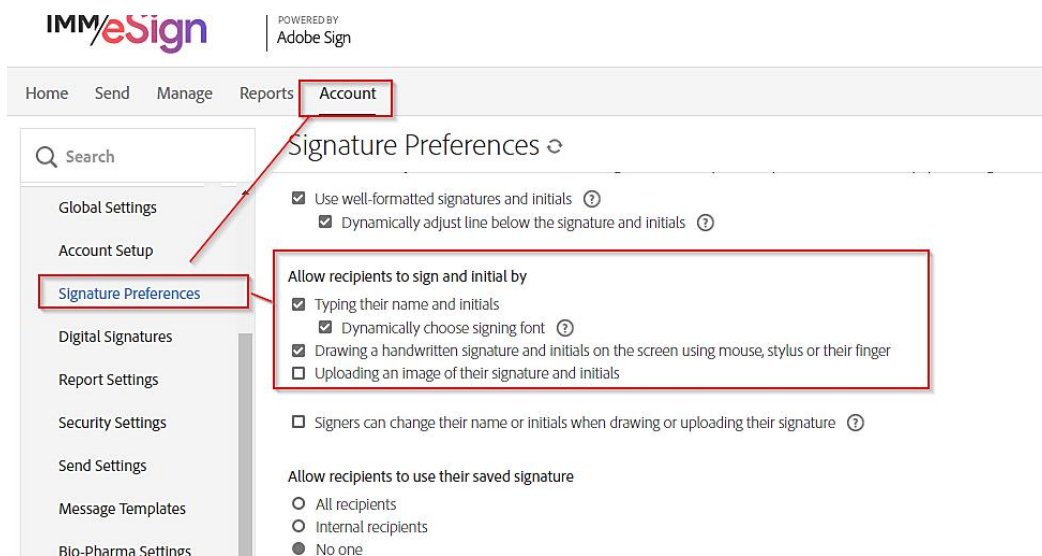
After users are authenticated to Adobe Sign using the two factor authentication method chosen by the user, they will have options for how their signature will be captured.

This illustration shows the 4 possibilities:

- Type
- Draw
- Image
- Mobile



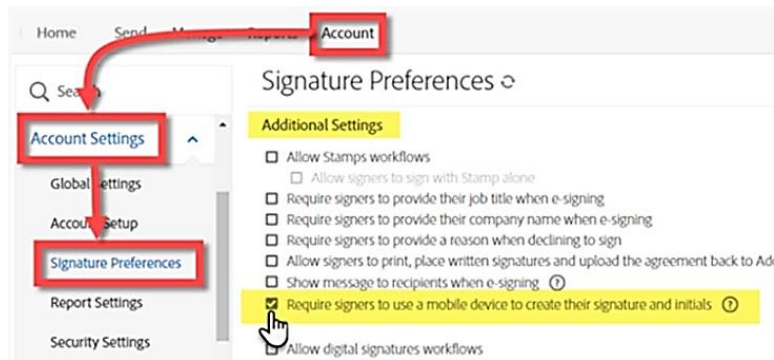
To determine what you'd like your signers to see you will access Signature Preferences from the Account tab. There you will see "Allow recipients to sign and initial by ..."



If you would not like your signers to type, but prefer they use some capture method you can deselect "Typing their name and initials."

**Drawing and Uploading an image** options will also enable the Mobile option that is referred to as "Cross-device Signature capture." This allows a signer on a desktop or laptop to send an SMS text to their mobile device with a link to *create* a signature, *capture* just the signature, and then *relay* that signature image back to the document on the desktop or laptop system.

You can **MANDATE** that signers use the Cross-device Signature capture by enabling MANDATORY Mobile Signature. It is unlikely you'll want to mandate this, but if you do, you can set *Require signers to use a mobile device to create their signature and initials* in the Additional Setting section of the Signature Preferences section (toward the bottom).

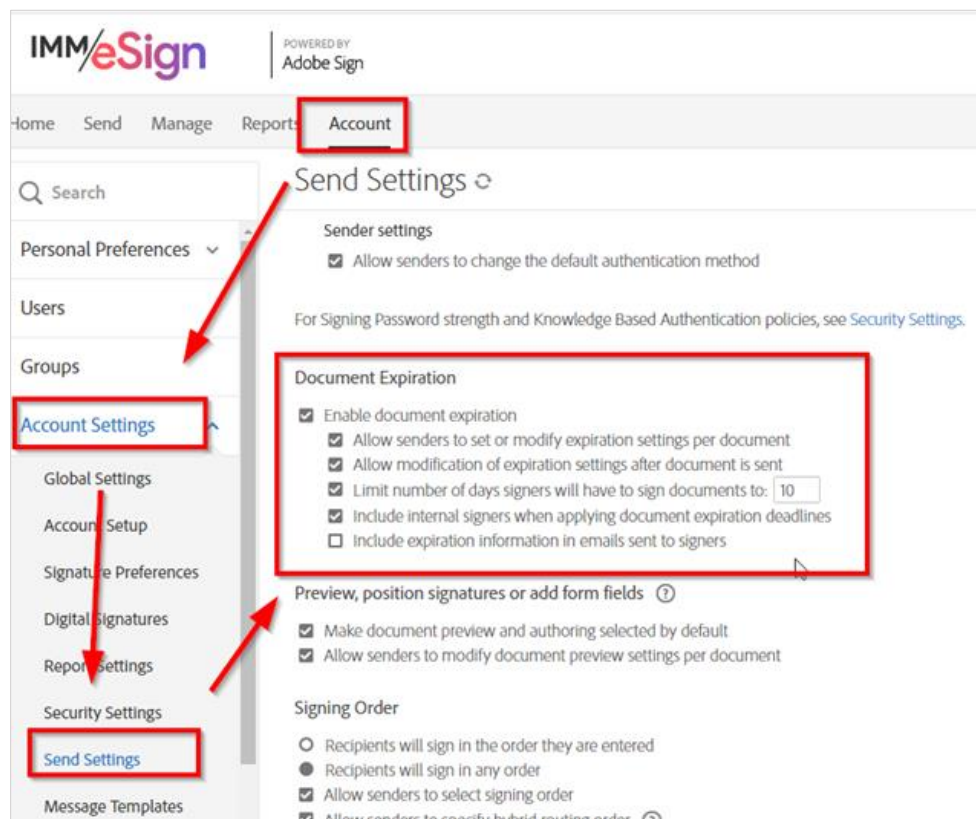


Enabling this over-rides the existing *Allow recipients to sign and initial by settings*.

### Document Expiration

A common question we hear is, “How long will the remote signature link be good for?”

The default is 10 days, but this can be changed under Account Settings, Send Settings, *Limit number of days signers will have to sign documents to*: as shown here.



Adobe has a robust help environment that you can access at [helpx.adobe.com](https://helpx.adobe.com) and your IMM Project Manager can always point you to additional information you may need.

## Recommended Activities

Determine what signing options and settings your institution will require to both enable and control your employee and signer interactions.

Document your decisions either in the Implementation Workbook or another location.

Apply your institution's decisions in the eSign configuration screens and in the Adobe Sign settings.

Review the Adobe Sign Help pages (<https://helpx.adobe.com/sign/user-guide.html>).

Note any questions or concerns you have so that you can ask your IMM Product Expert during the consulting/training session.

## Lesson 5: Additional Administrative Topics

---

### Overview

The preceding lessons in this Stage have covered nearly every aspect of the administrative settings available in the IMM eSign system and touched on Microsoft Azure Active Directory and Adobe Sign elements. In this lesson tie up a few loose ends and get you ready for your Consulting session followed by Stage 4: Templates and Attachments.

The key elements of this lesson are:

- Examine the remaining areas of IMM eSign not covered in the preceding lessons in this Stage, namely, Dictionaries|Select Default Attachment Type, Status API Settings, Document Push Settings, Scanner Settings, Help|Diagnostics, and About)
- Exploration of IMM eSign Reports
- Recap of Stage 3
- Discussion of items for Review

And after watching the video you should:

- Have a complete understanding of (or at least familiarity with) the System Administration configuration tools
- Assess your team's level of comfort with the materials and record any questions or areas of confusion
- Configure your solution according to your new knowledge, understanding, and decisions made
- Prepare for your Consulting/Training session with an IMM Solution Specialist

### Activity Checklist

- Watch the Lesson 5 video
- Review the materials in this document
- Complete the Readiness Form and be sure to include your list of questions or concerns for your upcoming consulting session.

## Remaining Menu Items

Thus far we have covered almost all administrative options—the options in the Processing menu will be covered in detail in Stage 5: User Preparedness and the Reporting items will be covered below.

The Administration menu has been our primary focus and we are holding off on the Documents (RTS) item and the Remote Attachment Template item until Stage 4 when we teach you about templates and attachments. But there are a few other items in the Administration menu that we have yet to cover: Dictionaries, Status API Settings, Document Push Settings, and Scanner.

### Dictionary Maintenance

The Dictionaries option allows the Administrator to view or modify certain dictionary settings. That said, as we mentioned in the lesson on indexing, you will most likely only have a single dictionary, the default, which is called TeSign, so there's nothing to concern yourself with here. That said, a **Dictionary** is a set of information that maps certain values pertaining to indexes and documents between specific host systems and imaging systems. If it is relevant to your implementation, your IMM Specialist will be sure to address it with you.

Dict Code	Description	App Prefix	CoApp Prefix	Other App Prefix	Default Recurrence	Default Attachment Type
TeSign	TeSign Documents				None	Select Default Attachment Type

Displaying records: 1 through 1. Total records available: 1

One item on this page that can be helpful even if you're just using the default TeSign dictionary is *Default Attachment Type*. Since we haven't learned about Attachments much yet and haven't set any up yet, this drop down will most likely be blank. However, once you have some attachment types created, you can set the **default** type that will be displayed on the Add Documents page when your users are processing sessions—and that is done here.

### Status API Settings and Document Push Settings

Total Records : 1  
Selected : 0

☐ TeSign

URL

Attempts: 1 2 3 4 5 6

Time Out: 0.5 min 1 min 1.5 min 2 min 2.5 min 3 min

These two items are used when an implementation that will take advantage of the IMM eSign API toolkit. Only certain business systems currently utilize the eSign API and your IMM Specialist or Installer will set these up when needed. For your knowledge, notifications are automatically generated when there are changes

in a Session's status and those notifications can be sent to an application or service managed by the institution, and this Status API settings page provides the settings used to specify where

the notifications should be sent, how many attempts should be made and what the time out values should be. Messages pushed can include information about downloading PDF documents and audit reports.

**Document Push Settings** similarly works with implementations utilizing the eSign API and is only used at this time with Meridian Link/ML and nCino. If your institution is using one of those systems, your IMM Specialist will review or make these settings for you.

## Scanner

If your institution will employ a scanner at the user workstation, it can be used to add attachments directly in a session.

There is a setting in General Settings called “Use common scanner” which you may recall we said is only used in thin

client environments. If Use common scanner is checked the scanner settings that will apply globally are set here, and the user is not prompted with the Scanner settings page when attaching a document. However, if it is not checked, the user will be prompted. Either way, settings entered in the default Scanner Settings will be the defaults in both situations. Prior to using a scanner or even configuring this setting, the scanner service must be installed on the user workstation and can be downloaded from the scanner settings dialogue using this button.

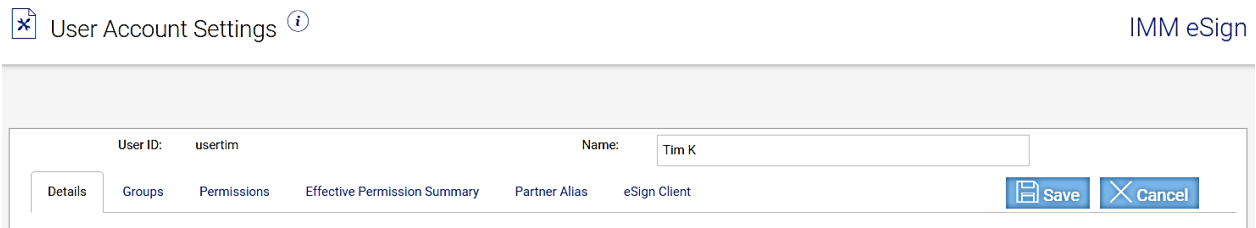
Also note, the first time a user attempts to use a scanner they may be prompted to install a small TWAIN driver if it has not already been done. The scanner settings overall are self explanatory.

## Help Menu

Under the Help menu you have access to Documentation, but there are other options called **Diagnostics** and **About**. These are both informational only and may come in handy during any support efforts.

## User Menu

The User menu will be labeled with your user name. Under it is an option labeled User Account Settings. This displays the current settings and permissions for the user to the user.

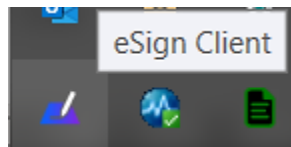


The screenshot shows the 'User Account Settings' window. At the top left is a close button (X) and the title 'User Account Settings' with an information icon (i). At the top right is the text 'IMM eSign'. The main area has a header with 'User ID: usertim' and 'Name: Tim K'. Below this is a tabbed interface with tabs: 'Details' (selected), 'Groups', 'Permissions', 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. At the bottom right are 'Save' and 'Cancel' buttons.

## Logout Menu

The Logout Menu is actually simply an single click to log out of the system.

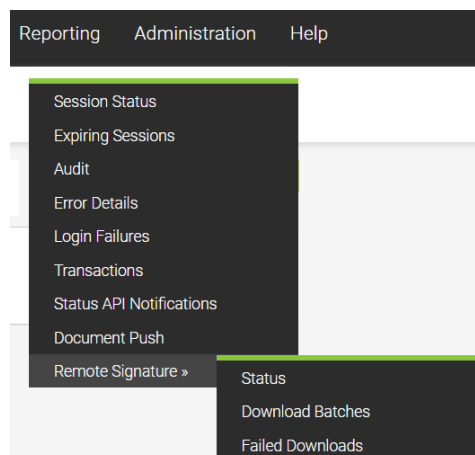
It is advisable to use Logout when you wish to Exit eSign to avoid any inadvertent session or document locks. You can always reaccess eSign from the eSign option in the system tray:



## Reporting

There are twelve administrative reports available in IMM eSign and they are listed here.

1. Audit
2. Login Failure
3. Session Status
4. Status API Notifications
5. Remote Signature Status
6. Error Details
7. Transaction Based
8. Expiring Sessions
9. Document Push
10. Remote Signature → Status
11. Remote Signature → Download Batches
12. Remote Signature → Failed Downloads



Access to the reports is set in the User or Group permissions, and in many cases, standard users will not need access to any of these reports.

Rather than walking through each report, we recommend taking some time to navigate through them after you have begun testing and have some data in your system. These reports draw information from the eSign database and are not generally used to find or report on documents or sessions specifically.

Reports will have different parameters that can be used to run them, and they can be exported in CSV format for further data analysis if desired.

Each report is discussed in detail in the Help Documentation and if you should have additional questions, don't hesitate to reach out to your IMM team.

## Stage 3 Recap/To Do List

This stage has been filled with a large amount of information and it may take your team a while to digest it all. In this stage we have covered the Help documentation materials available to you from within the eSign application as well as the totality of the General Settings. We covered the User and Group permissions and settings including MS Azure Active Directory considerations. The exploration of archiving and imaging systems showed you what is possible and likely generated more questions than answers. And finally, the signing options lesson showed you where to set your device settings, consent language, and how to work with Adobe Sign.

- Lesson 1 – Help and General Settings
- Lesson 2 – User and Group Settings
- Lesson 3 – Archiving/Imaging System Settings
- Lesson 4 – Setting Signing Options

Now it's time for Teamwork!

Once the members of your project team have watched the lessons, we recommend that you get together as a team, have conversations, make decisions, and configure the items with which you are comfortable. In the case of **Index and Imaging** items, you may not be able to make those decisions completely until after you've worked with your imaging vendor or in house imaging system administrator and begun learning about and setting up your eSign Templates.

Be sure to record your decisions and your settings somewhere – we recommend using the Implementation Workbook. This will give you something to reference moving forward.

## Activities

Compile any questions or concerns you have so that you can ask your IMM Product Expert during the consulting/training session.

Complete the Readiness Form and be sure to include your questions/concerns.

Schedule and participate in the Administrative Consultation/Training session

Buckle up for Stage 4: Templates and Attachments