IMM/eSign

eSign Cloud
Getting Started 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 2: Getting Started. This guide is a combination of the smaller guides provided within each lesson.

The purpose of Stage 2 is to build upon the base level of understanding established in Stage 1 and educate you on more of the specific elements of the eSign product and related components. During this Stage you will learn enough about eSign to make initial decisions, start to document your system and process, and be ready for the initial installation and setup of your eSign Cloud solution. We recommend that all members of your implementation team engage in all the training elements of Stage 2.

The guides 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. The workbook can be downloaded from the main Stage 2 website.

The lessons in Stage 2 will enable you to:

- Increase your understanding of the most important elements of eSign
- Prepare for and document your initial implementation
- Make decisions about how to set up user rights and permissions
- Make decisions about the signer experience both in branch and remotely
- Understand the installation process and your roles and responsibilities

Contents

Page

Lesson 1: Users and The Roles 3

Lesson 2: Templates and Attachments 9

Lesson 3: Signing Considerations, In Branch & Remote 15

Lesson 4: Archives and Imaging Systems 20

Lesson 5: eSign Components & Installation Requirements 25

Lesson 1: Users and The Roles

Overview

Like with most software utilized within your organization, users must have valid accounts to be **authorized** for access and those accounts must be managed to have certain privileges or **permissions** that determine what they can see and do and what actions they can take.

eSign Cloud security is handled in three parts and in this Lesson, you will learn the details of each of those parts as well as the types of permissions that can be employed and specifics to consider.

In this lesson, we will talk about your users who will interact with eSign.

As we think about Users, it will be important to understand the various components of both authentication (just having access) and authorization or permissions.

The key elements of this lesson are:

- How Microsoft Azure Active Directory relates to IMM eSign authentication
- Learn how to determine if your Institution currently uses MS Azure AD
- How users are authenticated to Adobe Sign for remote signature processes
- Exploration of the different permission types available in IMM eSign
- Learn about utilizing User Groups in IMM eSign

And after watching the video you should be able to:

- Define your institution's use of MS Azure AD
- Define how your users are currently utilizing Adobe Sign (if at all)
- Develop a user permissions plan

Activity Checklist

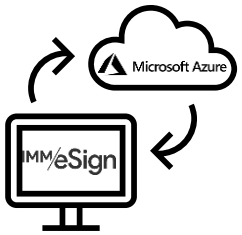
- Watch the Lesson 1: Users & Their Roles video
- Consider the questions posed in the lesson (they're reiterated in this guide)
- Enter information into the Users tab of the Implementation Workbook

User Authentication

IMM eSign Cloud utilizes *Microsoft Azure Active Directory* authentication.

If your institution already utilizes Azure Active Directory, we will simply link to it. IF you're unclear whether you have Azure AD or not:

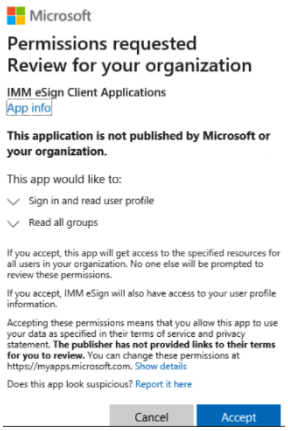
- If you are currently utilizing Microsoft Office365 you most likely have existing Azure AD credentials.
- You can go to portal.azure.com from your workstation. If you log in to that site automatically, or are prompted to log in and your standard domain credentials log you in, then once again, you most likely have existing Azure AD credentials.
- Check with your IT department or support organization and ask them.



Regardless of the answer, IMM will assist you either by linking your existing Azure domain to eSign, or we can work with you to set up a new Azure domain which you will then use to manage your user authentications.

The connection between IMM eSign and Azure AD is very simple.

Your IMM Installation Specialist will provide your Global Administrator (or GA) with two links. While logged in to Azure AD, the GA will simply click the links and accept the Permissions requests that pop up. Once this has been done, any user authenticated to your domain will have access to IMM eSign as a "default" user. (More on that below.)


Microsoft

Permissions requested
Review for your organization

IMM eSign Client Applications
App info

This application is not published by Microsoft or your organization.

This app would like to:

- Sign in and read user profile
- Read all groups

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

If you accept, IMM eSign will also have access to your user profile information.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel Accept

If you are unsure about any of this, please be sure to reach out to your IMM PM.

User Settings/Groups

Users will be created in eSign and activated automatically when accessing eSign for the first time thanks to the connection with Azure AD and all new users will be placed in a standard "USERS" group by default.

After a user has accessed eSign for the first time, your system administrator can then change their individual permissions and/or user groups, as necessary.

When a user accesses eSign initially their name and default email will populate based on their active directory information. However, it is best practice for your designated administrator to check users' accounts for: correct user name and email address, which will be labeled *Default Senders Email*—this value will be critical for Remote Signing.

With every eSign installation, there are 3 default User Groups: Administrators, Document Administrators, and Users.

The Administrators group gives the users assigned to it permissions to do almost everything an administrator would need to do.

The Document Administrators group gives the users assigned to it permissions to work with Document Designer (the templating tool).

The Users group gives the users assigned to it (all users by default when they first log in) limited but not overly restrictive rights. It will be important to know what permissions the Users group will give them so that you can adjust those "default" rights as needed.

These three standard groups are frequently all an institution needs to use; however, you might want to create your own group or groups that you'll put users in. 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, with some exceptions. Permissions are also assignable at the user level, and in most cases, those user level assignments supersede any groups the user is in.

Permissions

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

Permissions settings at the user level by default reflect an option to "Apply User's Highest Group Permissions". This means, only use the group level for this setting. If anything other than this option is chosen at the user level, that choice will supersede any of the group level settings for groups the user is in (including "Deny Access").

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
- Group Members Can Delete Unsigned Sessions
- Group Members Can Delete Signed Sessions
- Group Members Can Archive Sessions
- Group Members Can Search and View Completed Sessions
- Group Members Can Add Documents/Attachments to Sessions

Documents

- Group Members Can Delete Unsigned Documents
- Group Members Can Process Documents (Existing Session Only)
- Group Members Can Edit Indexes/Imaging Indexes
- Group Members Can Reindex Documents (The only option is *Allow to Reindex* or not)
- Group Members Can Modify Document Visibility Action

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
  - **Options**: Type, Draw, Signature Pad, Deny Access
- 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

Designer

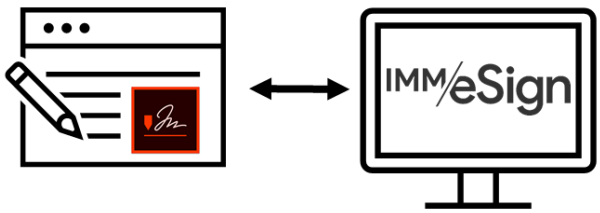
- Can use Designer Application
  - **Options**: Any Session, Their Own and This Group Members Sessions, Their Own Sessions Only, Deny Access
- Review Assignments in Designer
  - **Options**: Any Session, Their Own and This Group Members Sessions, Their Own Sessions Only, Deny Access
- Can Define Unknown Documents
  - **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
  - **Option**: Create and Manage Templates

Remote Signing

IMM maintains a close partnership with Adobe and utilizes Adobe Sign (formerly Echo Sign) for remote signing and eDelivery.



Users sending sessions from IMM eSign to remote recipients must have an Adobe Sign account linked by their email address. The *Default Sender* email address in the User setup will auto-populate when a user is sending a session and Adobe will recognize the sender as being “allowed” using that email address.

If your institution already uses Adobe Sign for a different process and some of your users already have their email addresses tied to an Adobe Sign account we will work with you to either migrate those addresses from your existing Adobe Sign account to the “IMM enabled” Adobe Sign account we will create for you. Alternatively, if you need to keep your separate Adobe Sign portal, users who already have accounts tied to it will need to have alias email

addresses created so they can be associated with the IMM process. Your IMM Project Manager can help you navigate that decision.

Administrators

You will need to identify specific users for certain administrative roles:

Global Administrator, or Azure AD GA, is most likely already a member of your IT team. Since giving new users access to eSign is as easy as adding them to your Azure AD, their role will not change with respect to eSign.

Adobe Sign Administrator can be anyone on your team and this person is responsible for making sure that users who will send sessions to remote signers from eSign have an account in Adobe.

eSign System Administrator(s) will have responsibility for working with the IMM eSign team on system configurations as well as managing users and permissions.

Document Administrator(s) will have responsibility for creating and maintaining document templates and attachments, which we will discuss further in the next lesson.

It is a good idea to have multiple people filling these roles, but they can all be filled by a single person if needed.

Questions to Consider

Who will be the users of eSign (list all users)?

Who is your MS Azure AD Global Administrator?

Who will act as the Adobe administrator(s)?

Which users will be eSign system administrators?

Which users will be document administrators?

What should the default User group permissions include?

Should all users be allowed to initiate in-person signing? If not, which users should be and what methods should they be able to use?

Should all users be allowed to initiate remote signing? If not, which users should be and what authentication methods should they be able to use?

What other capabilities should users have?

Begin answering and documenting these decisions in the Implementation Workbook.

Lesson 2: Templates and Attachments

Overview

Templates are foundational to all eSign projects. Without templates, eSign does not know where to place signature fields, what type of document is being signed, or what values to use to identify the signer(s) and to save the completed documents to the archive.

In this lesson we will dive deeper into the various components of templates and explore the considerations you should be discussing for your project. We will also discuss attachments, which, like templates, describe documents we will be handling, but have important differences.

The key elements of this lesson are:

- What Templates are and how they are used
- Source Documents, the different types, and how they get into eSign
- The different elements of a template and why each is important
- Attachments – when they are used instead of Templates

And after watching the video you should be able to:

- Record the various source documents you will need to have templates for
- Identify the different types of documents you will need to have attachments defined for
- Record the indexes to be used in relation to templates you'll define
- Be able to determine the types of source documents you'll use and their characteristics

Activity Checklist

- Watch the Lesson 2: Templates and Attachments video
- Consider the questions posed in the lesson (they're reiterated in this guide)
- Enter information into the Documents tab of the Implementation Workbook

Templates

Templates are like a set of instructions or a collection of information that are set up and administered by the institution both initially during implementation and ongoing as new types of documents are added or existing documents are changed. Templates allow eSign to “recognize” documents when they are “printed” or otherwise moved from a business system or other source into the eSign application.

Templates act first by identify a *Source Document* and assigning the correct Document Name to it, such as “Signature Card” or “Loan Application.”

Once the type of document is recognized, the template can do other things, such as:

Locate and extract **indexes** (such as names, account numbers, social security numbers, and dates). These can be captured from the text on the document.

Identify **Signature** and/or **Initial** field locations along with the signing parties’ names to which they correspond.

And place **Data** fields on the document so that after it is in eSign either the institution employee OR the signing party can enter additional information using text box fields, checkboxes, drop down menus or even radio buttons.

Source Documents

The eSign virtual printer is used to print Source Documents (again, examples could include signature cards, loan applications, etc.) from a business system which, in many cases until now, are printed out of that system onto paper so that the signing parties can sign them.

However, not all documents that you use originate in a business system or a **single** business system. And this is where the flexibility of eSign and templates can really stand out.

The eSign printer can be used across applications, so for a single session, documents can come from multiple business systems, or from the employee’s desktop, or even a network storage location. Sometimes source documents are forms your institution has created, or a standard form that you use as part of your business process. Regardless of where they originate, the documents that are part of the session (or packet of documents) are source documents that need to have a template designed for them.

In some cases, IMM has worked with a business system vendor to create an integration, sometimes referred to as an API. When that is the case, there will generally be a special option or button in the business system that will be used to push the documents to eSign. When that is the case, it may be that **some** or **all** of the “template instructions” can be sent along with the document removing the need for some, or sometimes all, of the template setup.

Once we know what business system or systems and document sources you use, we’ll be able to let you know what methods will be used for document recognition and templating.

Template Considerations

Since the eSign Virtual Printer is so flexible, and can be used in so many different scenarios, there are important considerations to keep in mind.

Text or Image based

Some source documents are text-based PDFs and others are image-based. When you open a PDF on your workstation, sometimes you can highlight and copy text and sometimes you can't. That is essentially the way to know when a PDF is text or image based.

This matters to eSign because if a PDF is image-based, we need to use OCR (or Optical Character Recognition) to read it and perform the critical template functions. So, as you're considering the documents that you'll send through eSign for signature, be sure to test them and see if they are text or image based.

OCR

OCR, unfortunately, is not perfect. It is the computer doing its best to decipher the letters on the page. Adding OCR to the template recognition process often results in a slower processing time when those documents are sent to eSign from the Source system using the virtual printer.

When the letters on a source document are in an unusual font, or bump up against lines or other characters, etc. the reliability of the OCR may be compromised.

So for these reasons, when considering the documents you'll send through eSign, pay close attention to any image based ones. And ask yourself, can they be made text based? If not, is the text clear? We'll help you test any image based PDFs and walk you through any adjustments that may need to be made.

Static vs Dynamic

A **static** document is one that will always be the same length, and all information in a static document will always be in the same place.

A **dynamic** document can vary in the number of pages and information may move depending on certain circumstances such as the number of applicants for a loan, for example. In many, but **not all** cases, dynamic documents require an additional level of configuration so it will be important to identify which of your source documents are static and which are dynamic and let your Implementation Consultant know. Depending on the source of the document, they will know whether the extra dynamic document process is necessary.

Printer settings

In some instances, when selecting a printer, the user is presented with a dialogue box with options. It will be essential, when this is the case, that all options chosen when creating the sample document for template definition are the same as when the document is being printed live. Some of these options could include "fit, "custom scale," "shrink pages," and the like. When troubleshooting unrecognized templates, this may be one place to look.

Browsers

For a similar reason to the Printer Settings above, it is essential that when a browser is used to print a source document (whether from within a business system or from a workstation) that all users utilize the same browser that was used to generate the sample document that was

templated. Different browsers have their own ways of generating the document so things tend to move (even slightly) and this can cause the template instructions to fail. With IMM eSign your institution should **standardize** on a single browser.

Also, if you decide to change your standard browser, you'll need to spend some time testing your templates with the new chosen browser and potentially update your templates.

Maintenance

Templates do require some degree of ongoing maintenance. One area of maintenance is if the structure or format of a source document changes – the location of a signature field, the name of the document, etc. Or, as mentioned above, if your organization changes browsers, or even business systems.

In these instances, your **document administrator** will need to make the required changes to the templates. The frequency with which this may happen will depend on your internal business processes.

Documenting Templates

At IMM we highly recommend and support starting with a **single** business process and a **single** business system at a time particularly for the first implementation. That way you're able to target the learning process while keeping it as straightforward as possible.

That said, for any implementation, structure and planning are the keys to success. Before you dive into creating templates, take the time to review your source documents as discussed so far in this lesson. Then:

Identify the source documents that are part of the process and where they originate (are they all generated in your business system? Or do some reside in a shared network folder or on individual workstations?)

Create samples of those source documents using the originating system—this will be good practice for preparing for testing.

Use test data and test accounts. You do not want to have actual customer data on documents that you might want to share outside of the institution or use to test, demonstrate, or document the solution.

Fill all relevant fields on your sample documents including all signature lines – for example, if you have a document that could be signed by 5 individuals, create a sample with five signers identified—this will make the templating process more straightforward and more accurate.

Then, use the Implementation Workbook to record the **document names** (what you call them, how they're identified in their source systems) and **indexes** (the values you're going to capture like names, dates, numbers, etc.), and identify the corresponding identifiers (document name/indexes) in the imaging system into which they'll be archived (for example, maybe in your Loan Origination System you call the Loan Application "Client Loan App" but maybe in your imaging system you call it LOS-Application)

Attachments

Another type of document managed in the eSign process is called an Attachment—a document or file that is not part of the collection of **templated** source documents. (E.g., driver license, passport, or other form of ID, or even a written set of instructions or policies or any other document.)

The files imported as attachments must be in an image format which could be PDF, JPEG, JPG, BMP, PNG, TIF(F), GIF. Since there isn't an "automatic" process for identifying these documents or extracting data, when attachments are added by the user, an attachment name (or type) is selected from a drop-down list and the indexes in the session are used to apply to it.

Attachments are not signed by the signers but may be included in the session for viewing and you can set whether attachments should be included in the session archive based on the attachment type.

Attachments can either be added by you when you are creating and working with a session, and they can also be requested from a remote signer – e.g., a copy of their ID to go along with an application package.

As you consider your use of eSign you should note any documents that may fall into this category so that they can be added to the document maintenance setup. Attachments can be detailed in your Implementation Workbook on the Documents tab along with the Templates.

Questions to Consider

What business system and process will you target for your first implementation?

What documents are part of the business process?

What are the documents called in the business system versus in the imaging system?

Which documents a signed versus initialed? Or both or neither?

What values exist on the document that should be captured (name, account number, etc.)?

Do you want to capture additional data on the document once it's in the eSign process?

Will you capture other documents as part of the process (e.g., ID, proof of insurance, terms, etc.)?

Which document would you like to use for your initial test? (choose one name(s), account number(s), and signature line(s) on it)

Who will be your "test data" signers? (Mickey Mouse? Bart Simpson? Lady Liberty?)

Begin answering and documenting these decisions in the Implementation Workbook.

Lesson 3: Signing Considerations, In Branch & Remote

Overview

It is called “eSign,” after all, so the process of signing is a core element and one that deserves consideration and discussion by your team.

There are multiple options to explore, best practices to think about, and decisions to be made. Once you have completed this lesson, your team should have the information needed to make those decisions and employ them in Stage 3 and/or with the help of your IMM Implementation Consultant.

The key elements of this lesson are:

- The options for and methods of in-branch signing
- Devices that are used most frequently to enable in-branch signing
- The elements involved in the remote signing process
- Two-factor authentication—options and considerations
- Settings at the user and system levels

And after watching the video you should be able to:

- Be able to define and discuss the in branch signing experience and come to decisions for the institution
- Be able to define and discuss the remote signing experience and come to decisions for the institution
- Formulate the institutional strategy around signing procedures – Consent verbiage and legal/policy requirements
- Identify areas of inquiry to discuss with the IMM Implementation Consultant

Activity Checklist

- Watch the Lesson 3: Signing Devices and Remote Signing Considerations video
- Consider the questions posed in the lesson (they’re reiterated in this guide)
- Enter information into the Signing tab of the Implementation Workbook

In Branch signing

The in-branch signing experience can differ depending on decisions you make as an institution.

Consent

One area for consideration is the consent that the signer will acknowledge prior to using electronic signature methods.

According to the E-Sign Act, financial institutions must provide the consumer a clear and conspicuous statement informing them of their rights. As we saw in the demonstration, prior to creating their electronic signature, eSign will display a statement for the signer to acknowledge that states: “I have reviewed the Consumer Disclosure and agree to do business electronically with [your institution].”

You can decide whether the user is forced to open the disclosure before agreeing to it, or not. (notice the yellow “Review” banner – this appears when you’re forcing the review)

The Disclosure itself will contain language that your institution’s legal or compliance department should create and approve. We have sample language that can be used as a starting point; however, it will be your own institution’s policies and any applicable laws and regulations that should guide your decisions.

Signing Methods

After an in-branch signer provides their consent, eSign will capture their signature mark and, if applicable, their intials mark as well. This can happen by one of the following methods: type, draw, or signature pad.

These are relatively self-explanatory. With type, a standard font will be used, and the signer simply types their name and initials on a keyboard. Draw may involve a tablet device or touch screen monitor, and signature pad utilizes a signature pad.

Signing Devices

The types of devices and methods your institution may want to use will vary based on any number of factors.

Signature pads provide a simple, tried and true, though limited, user experience. In general, signature pads do not offer the ability to display much other than prompts to the user, so any document viewing will need to take place on the employee’s screen or a secondary screen.

Tablets, such as iPads, offer a more complete user experience but in some cases can pose technical challenges.

Display devices, sometimes referred to as pen displays, are designed to facilitate the signing experience and act as a secondary (or additional) monitor onto which the signing experience can be moved with a keystroke by the employee.

“Click to Sign” refers to the type method where you or the signer simply uses a keyboard to type their name and initials and a standard font is used to display their signature mark.

Some considerations with any device may include:

- With what browsers are they compatible? Remember, eSign is a browser-based solution and we recommend standardizing on a single browser platform, so you’ll want to be sure any device is compatible with your chosen browser.
- Will the device be wired or wireless and what implications might that have for the ease of use?
- And of course, What is the desired user experience?

Your IMM Project Manager and Implementation team have a great deal of experience with the various options and are ready to help you think through the options if you like.

Remote Signing

The Remote Signing experience is handled through IMM’s tight integration with Adobe and the Adobe Sign (formerly Echo Sign) product.

Like with the in branch signing experience, before the consumer will be able to view and sign the documents in their session, they will need to agree to a consent to do business electronically.

Adobe offers standard language for this, and if you wish to use your own, your institution must publish a webpage with the verbiage and provide the URL to IMM. IMM will forward the request to Adobe on your behalf to update the link accordingly. Adobe settings also allow for the “forced review” if desired as well.

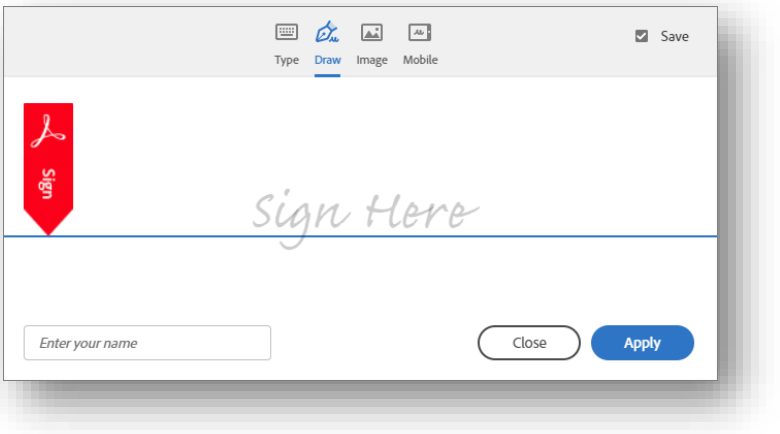
Authentication

We have talked several times about authentication for remote signers, and the same types of authentication are available for eDelivery (or the sending of documents from eSign to your consumer). Although it is possible to simply send an email with a link, we never recommend that, as there is no control over who might use the link in the email to view sensitive documents. Therefore, we always direct institutions to utilize one of the two factor authentication methods – which are, again, **password**, **phone** or text, **KBA**, and **GovernmentID**. Your employees can be set up to only have access to certain of these options at your discretion as part of the user permissions setup.

Adobe portal settings

As part of the IMM/eSign solution, you will have an Adobe Administrator designated at your institution.

This administrator will be able to alter settings in your Adobe portal that pertain to the options given to signers—such as signing methods: type, draw on a touch device, upload an image, or use a mobile device to create their signature. And as mentioned, also control the “force review” of the consent.



Your IMM project manager or installer will be able to show you the screens in Adobe where these settings are made, or you can always go to the Adobe help center. (https://helpx.adobe.com/sign/using/quick-setup-guide.html)

System Settings

Rounding out our discussion on Signing Considerations is a quick mention, and some repetition, of administrative settings:

- Allowed and default signing methods depending on what types of devices are being used (e.g., if a touch capable device is utilized by the employee, should the “Type” capture method even be an option?) as well as what the default method would be (in this example, likely “draw”).
- Force the review of the consent form? Like we saw, a signer can either just click the box, OR we can enforce having them view the consent verbiage. (For remote signers, this option is set in the Adobe Sign portal.)
- Consent language for in-branch signing. You will be able to enter and maintain the consent language from the administrative screens.
- User settings –
    - In-branch signing. Maybe you have call center employees and you don’t even want them to have that option? But for those that do, what methods can they use?
    - Remote signing and eDelivery. Can all employees do that? And if so, which authentication types should they have?

Questions to Consider

What is our consent language going to be for in-branch signing?

Do we want to use the Adobe standard consent language for remote signing or create out own webpage?

Do we want to force reading the consent language?

What signing devices will we use?

What signing methods will we use?

What signing methods will we allow for remote signers?

Do we need different signing options depending on who the users are?

What authentication methods will we use?

Do we need different groups to limit/allow different authentication option methods? (Yes, we asked this in Lesson 2 as well.)

Begin answering and documenting these decisions in the Implementation Workbook.

Lesson 4: Archives and Imaging Systems

Overview

Once the signing ceremony or ceremonies have been completed, there must be a process in place to maintain those records. With its flexible and configurable architecture, IMM eSign facilitates archiving signed documents and optionally any attachments to your imaging system. In this lesson we will examine the process flow, system and configuration requirements, and discuss considerations your team should discuss prior to the initial setup.

The key elements of this lesson are:

- The process flow of documents moving from business systems or other sources, to IMM eSign, to remote signing, to the imaging system
- The 3 archives: eSign, Adobe Sign, and Institutions' Imaging Systems
- The Imaging Index Service and connections to various Imaging Systems

And after watching the video you should be able to:

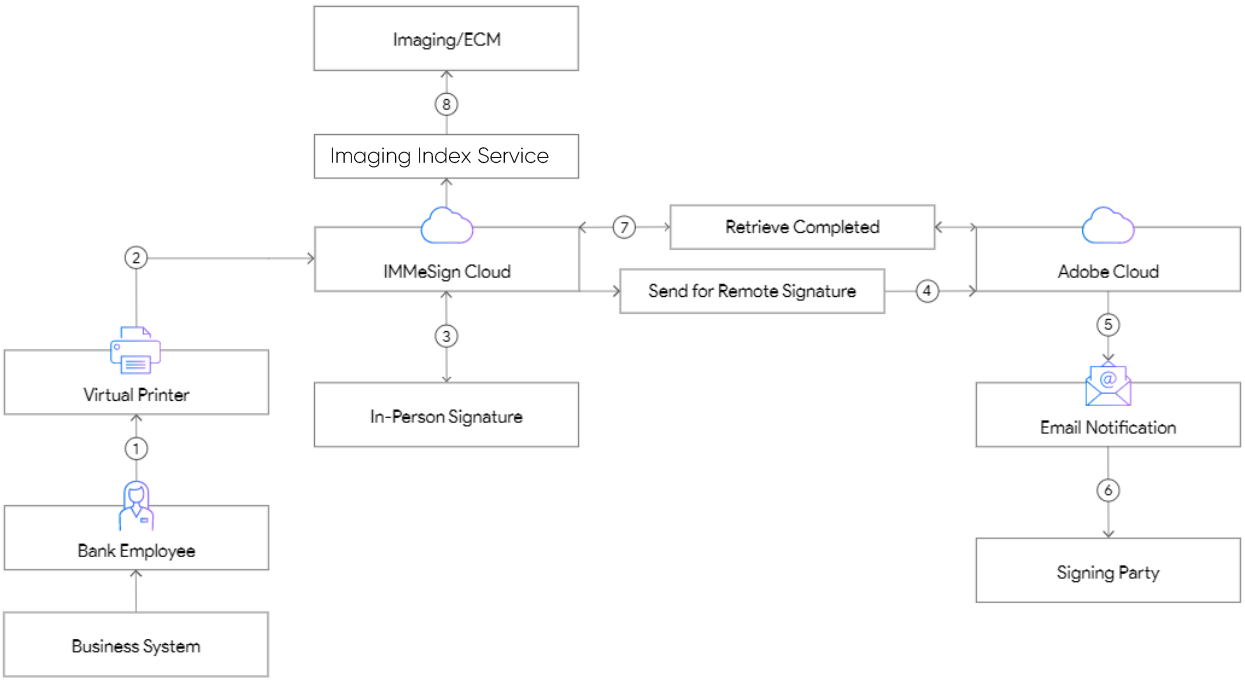
- Describe the process of archiving documents to your imaging system
- Identify the necessary components of the imaging system and archiving process based on your imaging system
- Decide what elements will be included in the archiving process
- Document any concerns or questions regarding the archiving process to discuss with your IMM Implementation Consultant

Activity Checklist

- Watch the Lesson 4: Archives and Imaging Systems video
- Consider the questions posed in the lesson (they're reiterated in this guide)
- Enter information into the Imaging tab of the Implementation Workbook

eSignature Process

The eSignature process with IMM eSign Cloud is managed primarily “in the cloud”.



Communications between your users’ workstations and the IMM cloud are secure via HTTPS and SSL certificate.

The signing processes that we have discussed so far either take place in branch or through the secure Adobe Sign service.

Once all signing ceremonies are complete, all the documents, including the audit files, are organized and retrieved to a server in your institution’s environment where they will be ready to pass to an Imaging System.

Archives

Once the documents in the session are all signed, the session is labeled “closed.”

eSign

Once those documents are moved successfully from the IMM eSign Cloud to the institution’s server, the documents are purged from the IMM eSign Cloud Service. The data records, however, are maintained for 365 days for audit purposes.

Adobe Sign

Any documents that have passed through Adobe Sign are subject to the retention policy in place. By default, Adobe Sign securely retains all customer documents on the service for as long as the account is active.

However, if you wish to delete the original documents from the Adobe Sign systems, you can define a “retention policy” that sets how long transaction data and documents should remain in Adobe Sign.

Imaging System

Ultimately, signed documents, data, and audit files will be passed to the institution’s imaging system where they can be stored according to the institution’s retention policies and be available for business process purposes.

Imaging Index Service

A key component of the eSign Cloud architecture is a small but important service called the Imaging Index Service.

This service must be set up on a server in the institution’s data center. Using a secure connection, the service will monitor the IMM eSign Cloud Service on a frequency set using Windows Scheduler on the server. Often this frequency is set at every hour on the half hour, but that decision is up to the institution.

The files that the Imaging Index Service retrieves are ready for the archive process.

Imaging Systems Settings

To enable the creation of the archive-ready files, there are settings that must be configured by the eSign Administrator (with the assistance of your IMM Implementation Consultant, of course.)

IMM eSign offers a menu of Imaging Systems in the administrative settings that can provide pre-configurations depending on the institution’s imaging vendor. IMM has worked with many vendors and has been able to streamline the archiving process both using these settings as well as our internal knowledge.

In many cases, the “default” “Index TXT” setting will be used to format the documents and data.

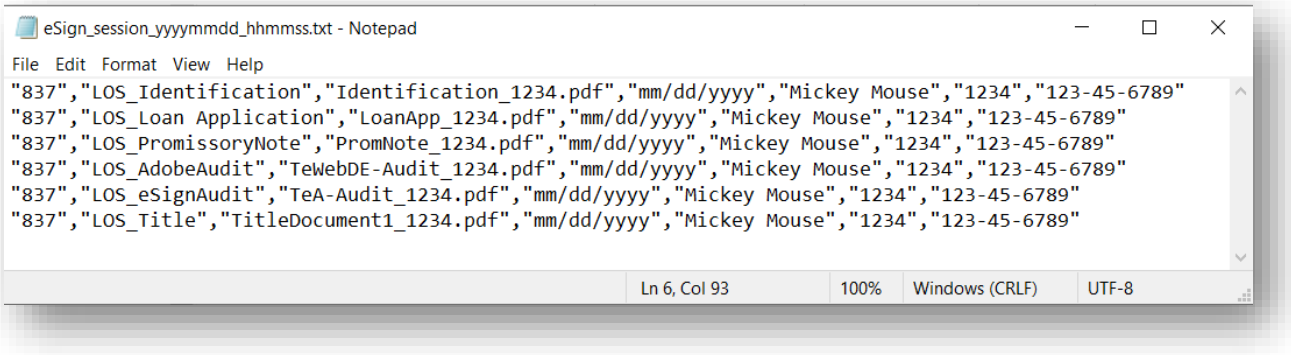
Regardless of the Imaging System employed, there are a few standards. In order to send the documents into an imaging system archive, IMM needs to provide the document itself (it’ll be a PDF) and data (indexes, keywords, document names, file names, etc.). Different imaging systems will have different input standards and we can accommodate them so long as we know what they are.

With the Index TXT method, there are three basic elements.

The index file is a text file (but could be a CSV or XML as well) that contains the data, or “instructions” for the imaging system. Two elements are set that pertain to the Index File:

File Name Template

The import tool of the imaging system will be set up to “expect” a certain file name or file name structure. In my example below, the file name is “eSign_session_[DATE]_[time]” – but you’ll want to check with your imaging system vendor to verify the best naming convention.



Line Template

The second element also has to do with the index file and that is the “line template” – this means, the structure of the information on each line of the Index File – one line equals one document. You can see from my example that we are passing a static value “837” followed by the document type name as it exists in the imaging system, followed by the name of the document file itself, followed then by some index data: a date, a name, a number, and a social security number. The values are double quote delimited and separated by commas. The decisions for what values go in what order delimited and separated by what characters should be made in partnership with your Imaging vendor.

Archive File Name Template

The file names above – such as Identification_1234.pdf –can be set to be unique and useful and in keeping with any requirements of the imaging system.

Imaging System Vendor

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. It will be 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.

It is a good idea to engage with your imaging system vendor **early** in the process (or with the system administrator at your institution if you have one) so that we can assist you in setting this up. Being the “LAST” part of the process, sometimes it is left until LAST, but we recommend a sooner than later strategy.

A note on Timing

A final element of the imaging process is the overall timing – the question, “when will the signed documents be in my imaging system?” is a common one. IMM only has partial control over this timing – it depends on whether documents are being signed remotely, what setting is being used for the retrieval of signed document by IMM from Adobe Sign, how frequently the Imaging Index Service runs and how frequently your imaging service retrieves files from your data center. You can see these linkages in the process diagram at the start of this document.

Be sure to talk amongst your team, document your specifics in the Implementation Workbook, and identify any questions or areas of concern you may have to bring to your IMM project manager or implementation consultant.

Questions to Consider

Who is our imaging system vendor?

Is our imaging system on premise or hosted (cloud based)?

Who is our imaging system administrator/contact?

Do we need any extra modules/products?

What values do we need to pass into the imaging system along with the documents?

What timing do we need from when a session is closed to when the images are in the archive? Is that important to this process?

Begin answering and documenting these decisions in the Implementation Workbook.

Lesson 5: eSign Components & Installation Requirements

Overview

As we draw closer to the installation activity, it is imperative that your team have a complete picture and understanding of the system and requirements for your IMM eSign system. Given the fact that your system is cloud-based, the number of on site requirements are minimal, yet no less deserving of your attention. At the conclusion of this lesson you should have a good understanding of these requirements and be prepared to discuss any questions with your IMM Implementation Consultant.

The key elements of this lesson are:

- IMM eSign is a browser-based application—what browsers are supported and what are some considerations
- The eSign client install
- Installation of the Imaging Index Service described in Lesson 4
- The initial installation activity—what to expect and how to prepare

And after watching the video you should be able to:

- Determine what browser your institution will utilize for IMM eSign
- Identify any areas of confusion or concern to discuss with your IMM Implementation Consultant
- Identify a server to be used to run the Imaging Index Service
- Confirm the identities of the team that will participate in the installation activity and the workstation(s) that will be used

Activity Checklist

- Watch the Lesson 5: Components of eSign and Implementation Requirements
- Consider the questions posed in the lesson (they're reiterated in this guide)
- Enter information into the Environment tab of the Implementation Workbook and validate information in the other tabs
- Submit the Implementation Workbook with your Readiness Form from the Stage 2 webpage: https://www.immonline.com/onboarding-esign-cloud-rts/stage2/

User Workstations

The System or Technical Components of the eSign Cloud architecture are very straightforward and are referenced in the IMM eSign for Cloud Environments: System Requirements document located here: https://www.immonline.com/wp-content/uploads/IMMeSignCloud-SystemRequirements-1.pdf

User workstations running Windows 10 (professional or enterprise) as well as thin client workstations such as Citrix XenApp and XenDesktop are supported.

Browsers

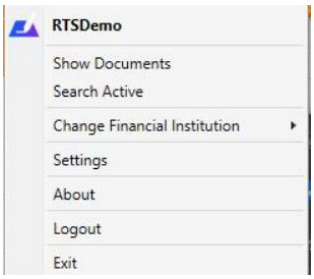
Since IMM eSign is a browser-based solution we highly recommended that all user workstations utilize the same browser – standardizing not only makes your support easier, but it also addresses some common situations that can arise when mixed browser environments are being utilized. IMM eSign is supported on IE 11x, Edge, Chrome, and Firefox. (Note, Edge is still being tested as of April 2021, with no issues yet identified.)

It is generally a good idea to keep your browsers up to date. Since many institutions continue to utilize Internet Explorer 11 due to line-of-business applications' dependencies, IMM eSign will continue to support it for the foreseeable future.

There may be nuanced differences with how certain browsers handle printing and with how certain signing devices may interface with browsers, so as we discussed in an earlier lesson, it will be important to understand the support levels of not only eSign and your business applications but of your peripheral devices as well and standardize.

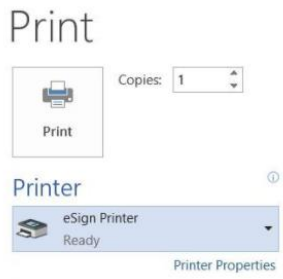
eSign Client

Although IMM eSign is browser-based, it still relies on a small piece of software that is installed on user workstations.



Once installed the small IMM eSign tool primarily lives in and is accessed from the workstation's system tray. It runs invisibly to most users and yet serves as an easy way for them to access the eSign Collected Documents page (*Show Documents*) or *Search Active* documents. (Choosing those options launches the chosen web browser and brings the user to their IMM eSign cloud site).

Virtual Printer



The other portion of the client installation is the eSign Virtual printer, which enables the "ready to sign," or RTS, functionality that you have been learning about. The eSign virtual printer will display in the Windows printers settings and will allow the user to send a document to eSign for processing from any application that has a print dialogue.

The eSign Client install process is quick and easily maintained by the institution's IT department.

Server

Once again, since the IMM eSign Cloud process is managed almost entirely in the IMM Cloud, there is little need for your institution's computing resources. However, there is one component required that we have mentioned several times, and that is the Imaging Index Service—sometimes referred to as the downloader or download service.

Imaging Index Service

This small application will run as a *service* on a server in your institution's data center and will retrieve the completed, or "closed," sessions from the IMM Cloud based on a schedule set up using the Windows Scheduler. Once retrieved using a secure connection, the files will be placed in a dedicated location, generally on the same server and generally in an *IMM/Archive* folder.

Once retrieved, the files are ready to be archived to your imaging system as we discussed in the previous lesson.

Your installer will help you with the initial setup during the installation activity, so be sure you have identified a server onto which you'll place the Imaging Index Service and that someone with administrative rights to that server will be on the installation activity call.

Installation Activity

After you have completed this lesson and had some internal discussions with your project team, you will be ready to submit your Readiness Form to your IMM Project Manager who will then schedule your Installation activity.

That activity will include the following items:

- Establishing the MS Azure AD connection
- Installation and setup of the Imaging Index Service on a server in your environment
- Installation of the eSign Client components on a designated testing/training workstation
- Verifying access to the Adobe Sign portal
- Creating a test templated document
- Fully testing a transaction with the test template, to include
    - generating the source document from your chosen business system and printing it to eSign,
    - signing the document as an in person signer and then as a remote signer, and
    - seeing that document retrieved to the archive folder on the Imaging Index Service's server.

Installation Users and Resources

To facilitate the installation activity, it will be imperative that certain resources are ready—both people and technology.

You must have a **designated workstation** that will be used for the installation and initial test as well as for ongoing testing and training. You will be able to test and train on multiple workstations, but at least one should be identified for interactions with IMM Implementation team members. That workstation should also be able to connect to a web conferencing session.

The **user** logged into that workstation must have **permission** to install software (or an administrator must also be on the call to enter needed credentials)

The installation workstation must have access to the **business system** that will provide the source documents, and one of the attendees must have **expertise** in the business system to generate the source document being used to test.

If a **signing device** will be used, it should be installed and configured on the workstation prior to the installation activity.

The designated **eSign Administrator** MUST be on the installation activity call as should be the **Document Administrator** if that is a different person.

Additionally, the MS Azure **Global Administrator** must be on the call to facilitate the link process described earlier and if different, an **IT resource** who will facilitate the installation and configuration of the Imaging Index Service in your institution's infrastructure must also be on the call.

The designated **Adobe Administrator** must be on the call as should any additional **subject matter experts** identified by your team.

Yes, this is an important activity with multiple attendees, some of these may be the same person:

- ✓ Institution Project Manager
- ✓ Business System user/Subject Matter Expert(s)
- ✓ Azure AD Global Administrator
- ✓ IT Resource
- ✓ Adobe Administrator
- ✓ eSign Administrator
- ✓ eSign Document Administrator

You will receive an invitation from the IMM Installer reiterating these pre-requisites and should ask them or your IMM Project Manager any clarifying questions.

Questions to Consider

Who will be the IT resource responsible for the technical components of the installation?

Are there any unique infrastructure settings that may make a software installation challenging in our environment? (If so, please let us know as soon as possible.)

Do all user workstations meet or exceed the System Requirements?

On what browser have we chosen to standardize?

What signing device(s) will be used?

What server will be used to run the Imaging Index Service? What retrieval schedule should be employed?

Begin answering and documenting these decisions in the Implementation Workbook.