eSign Cloud

Getting Started Guide – Signing Considerations, In Branch, & Remote

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 third lesson in Stage 2: Getting Started—Signing Considerations, In Branch & Remote.

After watching the video located on the lesson page use the materials at the end of this guide to assist you and your team in making and documenting initial decisions and processes and to help you prepare for the initial installation activity.

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 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

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.

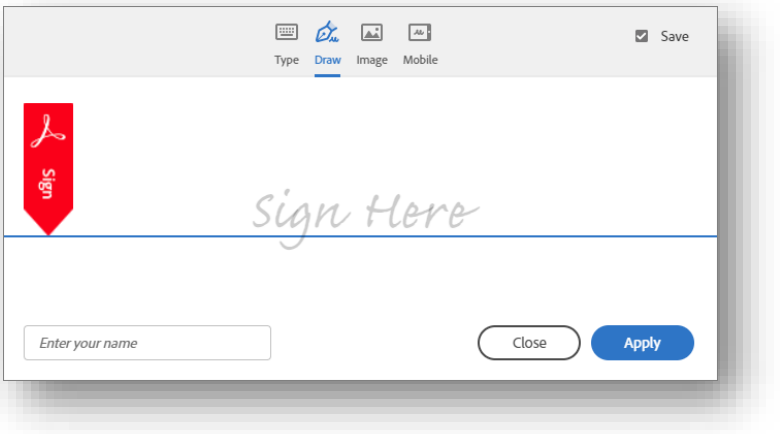
Authentication

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.