eSign Cloud
Getting Started Guide – Users & Their Roles

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 first lesson in Stage 2: Getting Started—Users & Their Roles.

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

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

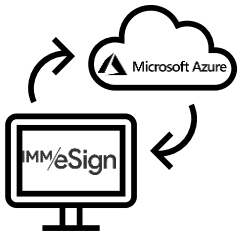
- Watch the Lesson 1: Users & Their Roles video
- Consider the questions posed in the lesson (they're reiterated in this guide)
- Enter information into the Users tab of the Implementation Workbook

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:

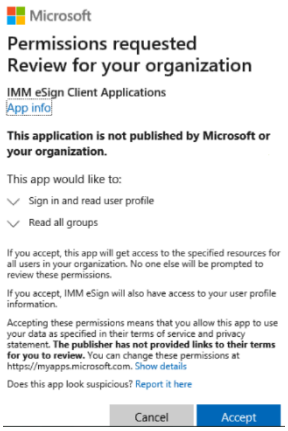
- If you are currently utilizing Microsoft Office365 you most likely have existing Azure AD credentials.
- You can go to portal.azure.com from your workstation. If you log in to that site automatically, or are prompted to log in and your standard domain credentials log you in, then once again, you most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

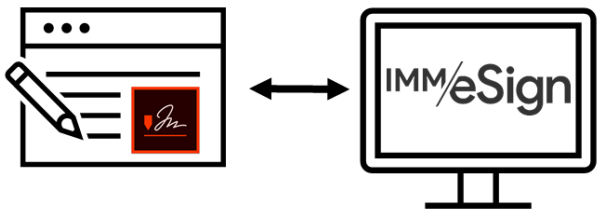
Designer

- 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.