



eSign Cloud

System Administration: User and Group Settings

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 second lesson in Stage 3: System Administration—User and Group Settings.

You should watch the video located on the lesson page and use this document 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

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

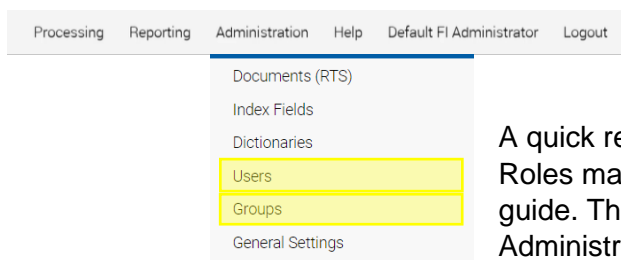
Users will be created in eSign and activated **automatically** when accessing eSign for the first time thanks to the connection with Azure AD.

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

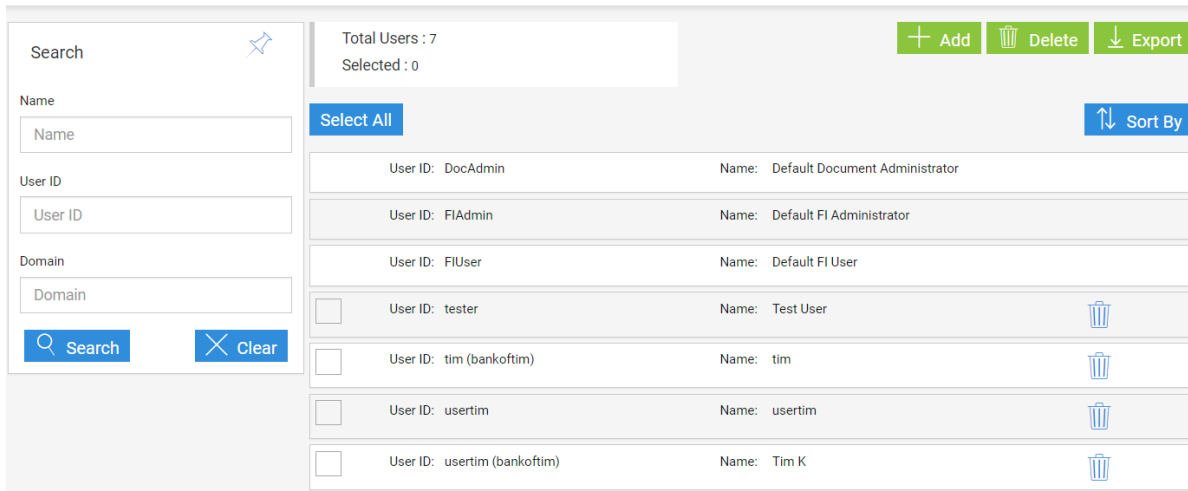


A quick review of Stage 2 | Lesson 1: Users and Their Roles may be valuable in addition to utilizing this lesson guide. The Users and Groups settings are found in the Administration drop down menu as seen here.

User Maintenance

User Maintenance 





IMM eSign



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 |  |

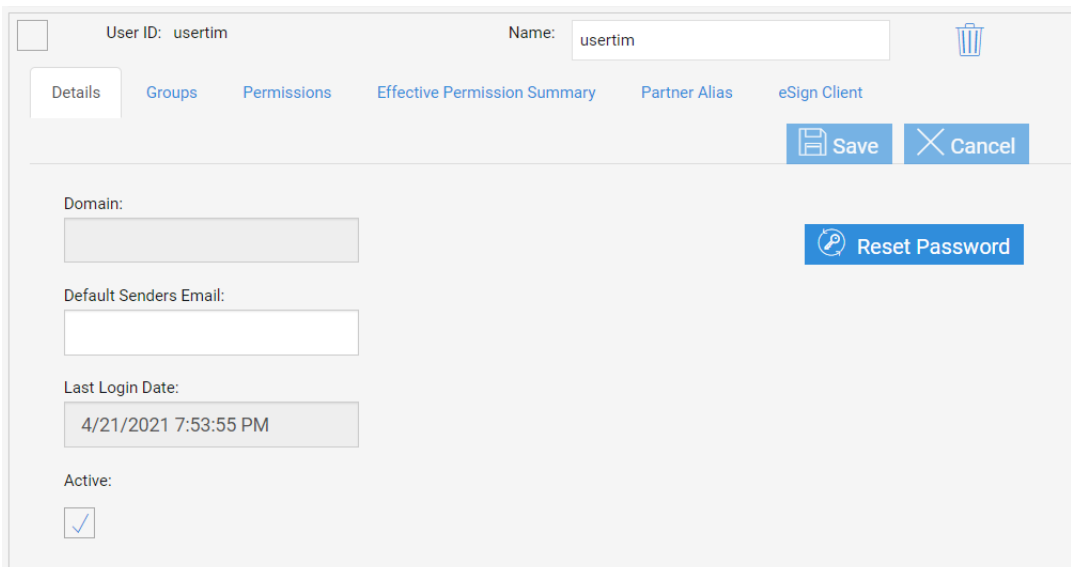
When accessing the Users option in the Administration menu you will see this screen.


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: usertim 

[Details](#) [Groups](#) [Permissions](#) [Effective Permission Summary](#) [Partner Alias](#) [eSign Client](#)

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

Domain:

Default Senders Email:

Last Login Date: 4/21/2021 7:53:55 PM

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 'User ID: usertim' and a 'Name: usertim' field with a trash icon. Below this are navigation tabs: 'Details', 'Groups' (selected), 'Permissions', 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. There are 'Save' and 'Cancel' buttons. A search bar is present above a table of groups. The table has columns for 'Group Title' and 'Description'. The groups listed are 'Administrators' (Default Administrators Group), 'Call Center' (Call Center Employees), and 'Users' (Default Users Group). Each row has a checkbox on the left and a trash icon on the right.

| <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

User ID: usertim Name: usertim

Details Groups **Permissions** Effective Permission Summary Partner Alias eSign Client

Save Cancel

Sessions

User Can Search and View Active Sessions

Apply User's Highest Group Permissions

Any Session

User's Sessions Only

No Access

User Can Unlock Sessions

Apply User's Highest Group Permissions

Any Session

User's Sessions Only

No Access

User Can Transfer Sessions

Apply User's Highest Group Permissions

Documents

User Can Delete Unsigned Documents

Apply User's Highest Group Permissions

Any Session

User's Sessions Only

No Access

User Can Process Documents (Existing Session Only)

Apply User's Highest Group Permissions

Any Session

User's Sessions Only

No Access

User Can Edit Indexes/Imaging Indexes

Apply User's Highest Group Permissions

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

User ID: usertim Name: usertim

Details Groups Permissions **Effective Permission Summary** Partner Alias eSign Client

Save Cancel

| 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 management interface. At the top, the 'User ID' is 'usertim' and the 'Name' is 'usertim'. Below this are navigation tabs: 'Details', 'Groups', 'Permissions', 'Effective Permission Summary', 'Partner Alias', and 'eSign Client'. The 'eSign Client' tab is active, showing several settings:

- Input Folder 1: %InstallPath%\Output
- Input Folder 2: C:\IMM\ManualOutput
- Static Output Folder: (empty)
- Document Expiration (Minutes): 20
- Default Browser: Chrome
- Auto Launch eSign in Browser:
- Display Notification for (Seconds): 5

At the top right of the settings area, there are 'Save' and 'Cancel' buttons.

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

| | | | | |
|---|--|---------|--------|--------|
| Total Groups : 4 | | + Add | Delete | Export |
| Selected : 0 | | | | |
| Select All | | Sort By | | |
| 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 | | | |

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

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.