

# **IMM eSign Cloud Service: Managing Microsoft Azure Users**

# Contents

Introduction

User Directory Roles

How to Create a User

How to Elevate a User to Limited Administrator/Global Administrator

How to Delete a User

# Introduction

This guide will help you manage users in your Microsoft Azure Directory Portal.

This guide will review:

- Microsoft Azure User Directory Roles
- How to create a user
- How to elevate a typical user to a Limited Administrator User
- How to delete a user

Please review the following video for more information about the above Microsoft Azure settings.

Refer to [IMM eSign Cloud Azure Training](#).

## User Directory Roles

- **Global Administrator (GA):** GA user has full control and can manage all aspects of the Azure Active Directory Portal.
- **Limited Administrator (LA):** LA users are password and user administrators. A password administrator can reset passwords for a non-administrator/regular user, can manage all aspects of users and groups and can reset passwords for other Limited Administrators.
- **User:** User has no administrative control.

**Note:** Each person at your financial institution that will be processing documents in IMM eSign will need a Microsoft Azure account.

## How to Create a User

- Navigate to <https://azure.portal.com> and login with your Azure credentials.

Search resources, services, an

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory**
- Monitor
- Advisor
- Security Center
- Help + support
- Cost Management + Billing

## Welcome to Azure!

Don't have a subscription? Check out the following options

### Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.

[Start](#) [Learn more](#)

### Azure services

- Create a resource
- Azure Active Directory
- All resources

- Click on “Users”

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

## IMM eSign

Search your tenant

Tenant information	Azure AD Connect
<p><b>Your role</b> Global administrator <a href="#">More info</a></p> <p><b>License</b> Azure AD Free</p> <p><b>Tenant ID</b> d2e0f1ba-168a-4cb9-99be-0036... <a href="#">Copy</a></p> <p><b>Primary domain</b> immesign.onmicrosoft.com</p>	<p><b>Status</b> Not enabled</p> <p><b>Last sync</b> Sync has never run</p>

- Click on “New User”

Users | All users (Preview)  
IMM eSign - Azure Active Directory

<< + New user + New guest

All users (Preview)  
Deleted users  
Password reset

Search users

Name

- Fill out “Name” and “Username.” Ensure the “Directory Role” is set to User. Then, click “create” at the bottom of the screen.

## New user

IMM eSign

[Got feedback?](#)



### Create user

Create a new user in your organization. This user will have a user name like `alice@immesign.onmicrosoft.com`.  
[I want to create users in bulk](#)



### Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.  
[I want to invite guest users in bulk](#)

[Help me decide](#)

## Identity

User name \* ⓘ

Example: chris

@ immesign.onmicrosoft.com The domain name I need isn't shown here

Name \* ⓘ

Example: 'Chris Green'

First name

Last name

## Groups and roles

Groups

0 groups selected

Roles

User

[Create](#)

- Click “Show Password.” Make a note/save this password as you will need to share this password with the User. The User will be prompted to use this password during the initial login process.  
**Note:** If you forget to copy this password, the Global Administrator or Limited Administrator can click on this User on the “Users-All users” page and reset the password.

#### Password

Auto-generate password  
 Let me create the password

Initial password

Show Password

## How to Elevate a User to Limited Administrator

- Click on the user name on the “Users-All Users” page that you wish to elevate to a Limited Administrator role.

[Home](#) > [IMM eSign](#) > [Users | All users \(Preview\)](#) >

- Once you have clicked on the user that you want to promote to Limited Administrator. Click “Assigned Roles.”

«

[Diagnose and solve problems](#)

Manage

- [Profile](#)
- [Assigned roles](#)
- [Administrative units \(Preview\)](#)
- [Groups](#)
- [Applications](#)
- [Licenses](#)
- [Devices](#)
- [Azure role assignments](#)
- [Authentication methods](#)

Activity

- Click “Add Assignments”

Administrative roles

Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Role	↑↓ Description
No directory roles assigned.	

- You will see a list of Director roles on the below screen. In order to elevate the user to Limited Administrator, you will need to select “Password administrator” and “User administrator.” In order to elevate the user to Global Administrator – select Global Administrator only. Then click “Add” at the bottom of the screen.

Directory roles ×

**i** To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.

<input type="checkbox"/>	Office apps administrator	Can manage Office apps cloud services, including policy and settings managem...
<input type="checkbox"/>	Password administrator	Can reset passwords for non-administrators and Password administrators.
<input type="checkbox"/>	Power BI administrator	Can manage all aspects of the Power BI product.
<input type="checkbox"/>	Power platform administrator	Can create and manage all aspects of Microsoft Dynamics 365, PowerApps, and...
<input type="checkbox"/>	Printer administrator	Can manage all aspects of printers and printer connectors.
<input type="checkbox"/>	Printer technician	Can register and unregister printers and update printer status.
<input type="checkbox"/>	Privileged authentication administrator	Allowed to view, set and reset authentication method information for any user (...)
<input type="checkbox"/>	Privileged role administrator	Can manage role assignments in Azure AD, and all aspects of Privileged Identit...
<input type="checkbox"/>	Reports reader	Can read sign-in and audit reports.
<input type="checkbox"/>	Search administrator	Can create and manage all aspects of Microsoft Search settings.
<input type="checkbox"/>	Search editor	Can create and manage the editorial content such as bookmarks, Q and As, loc...
<input type="checkbox"/>	Security administrator	Can read security information and reports, and manage configuration in Azure ...
<input type="checkbox"/>	Security operator	Can create and manage security events.
<input type="checkbox"/>	Security reader	Can read security information and reports in Azure AD and Office 365.
<input type="checkbox"/>	Service support administrator	Can read service health information and manage support tickets.
<input type="checkbox"/>	SharePoint administrator	Can manage all aspects of the SharePoint service.
<input type="checkbox"/>	Skype for Business administrator	Can manage all aspects of the Skype for Business product.
<input type="checkbox"/>	Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.
<input type="checkbox"/>	Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.
<input type="checkbox"/>	Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.
<input type="checkbox"/>	Teams Service Administrator	Can manage the Microsoft Teams service.
<input type="checkbox"/>	User administrator	Can manage all aspects of users and groups, including resetting passwords for l...

- You will then see the below screen which will confirm you have successfully added the necessary directory roles in order to make the user a Limited Administrator.

Successfully added directory roles  
Successfully added 2 directory roles  
2:29 PM

Role	Description	Resource Name
User administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Directory
Password administrator	Can reset passwords for non-administrators and Password administrators.	Directory

## How to Delete a User

- Navigate to the “Users-All users” page and select the User you want to delete. Click “Delete User.”

Users | All users (Preview)  
IMM eSign - Azure Active Directory

Navigation: + New user + New guest user Bulk activities Refresh Reset password Multi-Factor Authentication **Delete user**

Search: Search users Add filters

Name	User principal name	User type
<input checked="" type="checkbox"/> Datasafe Admin	admins1@testds1.partners.immesign.com	Member
<input type="checkbox"/> Datasafe Admin2	admins2@testds2.partners.immesign.com	Member

- A screen will populate and ask you “Delete selected users?” Click “Yes.”
- You will see the below screen which will confirm you have successfully deleted the User