Standard Operating Procedure (SOP) for User Management in Microsoft Entra Admin

Document Owner: IFC - IT Department
Date: 03/21/2025
Version: 2.0

Table of Contents

Introduction

This document provides step-by-step instructions for managing users in **Microsoft Entra Admin**. It covers creating, modifying, and deleting users, as well as handling user roles and group memberships. Proper user management ensures security, access control, and compliance with organizational policies.

Prerequisites

Before proceeding with any user management tasks, ensure the following:

- You have **administrator privileges** in Microsoft Entra Admin.
- A **stable internet connection** and a supported web browser (Microsoft Edge, Google Chrome, or Firefox).
- A **clear understanding of the organization's user roles**, security policies, and permissions.
- Necessary **approvals leadership/management team** for making user changes.

Procedure

1. Accessing Microsoft Entra Admin Center

Step 1: Open a web browser and navigate to Microsoft Entra Admin Center.

Step 2: On the **Sign-in page**, enter your admin username (e.g., admin@company.com), password and MFAs as needed.

Step 3: Once logged in, locate the **Navigation Pane** on the left side of the screen.

2. Managing User in Entra

2.1 Creating a New User

Step 1: On the **Navigation Pane,** Click on **Users** to access the User Management section.

Step 2: In the **Users** section, click on the **+ New user** button at the top.

Step 3: A panel will open with two options:

- **Create user** (manually add a new user).
- **Invite external user** (for external users or guest access).

Step 4: Select **Create user** to proceed.

Step 5: Fill in the following required fields:

- **User principal name (UPN)**: The unique username (e.g., johndoe@company.com).
- **First and last name**: Enter the employee's full legal name.
- **Display name**: This will appear in the directory (e.g., John Doe – IT Admin).
- **Password settings**: Choose whether to auto-generate a password or set a custom one.

Step 6: Assign roles and group memberships:

- Click on **Assignment Tab** and select the appropriate role (e.g., User, Global Admin, Helpdesk Admin).
- Under **Groups**, add the user to predefined security or Microsoft 365 groups.

Step 7: Click **Create** to finalize the user creation. The user will now appear in the directory.

2.2 Modifying an Existing User

Step 1: In the **Users > All Users** section, use the **search bar** to find the user by name or email.

Step 2: Click on the user's name to open their profile page.

Step 3: Modify user details as needed:

- **Change display name or department** by clicking **Edit properties**.
- **Reset password** by selecting **Reset password**, then choose to auto-generate or set a new one.

- **Update job title, phone number, or office location** under the **Profile** section.
- **Modify assigned roles** by navigating to **Roles** and selecting the appropriate permissions.
- **Change group memberships** by clicking **Groups**, then **Add to group** or **Remove from group**.

Step 4: Click **Save** after making changes.

2.3 Deleting a User

Step 1: Locate the user in the **Users** section.

Step 2: Click on the user’s name to open their profile.

Step 3: Click the **Delete user** button.

Step 4: A confirmation prompt will appear. Review the details and click **Confirm**.

Step 5: The user will be moved to the **Deleted Users** section, where they can be recovered for a limited period (default: 30 days).

2.4 Restoring a Deleted User

Step 1: In the **Users** section, navigate to **Deleted Users**.

Step 2: Find the user you wish to restore.

Step 3: Click **Restore user** to reinstate their access.

Step 4: If the restoration is successful, the user will appear back in the **Active Users** list.

3. Viewing Audit Logs and Sign-in Logs for Users

3.1 Accessing User Audit Logs

Step 1: Go to the **Users** section from the **Navigation Panel**

- In the **Microsoft Entra Admin Center**, click on **Users> All users** in the left-hand menu to view the overall audit logs.
- The **Audit logs** of one **specific user** can also be **viewed** by **selecting the user**, viewing their **profile** and clicking on the **Audit logs**.

Step 2: Filtering and **Searching** Audit Logs

- Click on **Filters** to refine and narrow the results based on: Activity, Category, Service, Date and more.

Step 3: Viewing Log Details

- Click on a log entry to expand details, which include:
  - **Action performed** (e.g., "User role changed").
  - **Timestamp** (date and time of the event).
  - **IP address**
  - **Initiator** (administrator or system).
  - **Outcome** (Successful or Failed).

Step 4: Exporting Audit Logs

- Click the **Download** button to export logs as a CSV file for reporting or analysis.

3.2 Accessing User Sign-in Logs

Step 1: Go to the **Users** section from the **Navigation Panel**

- Click on **Users > All users** in the left-hand menu.
- Select **Sign-in Logs** from the available options.
- **Sign-in Logs** of **specific/individual** users can also be viewed, by selecting a **User**, navigating to their **profile** and **Clicking** on **Sign-in Logs.**

Step 2: Filtering and **Searching Sign-in** Logs

- Go to the sign-in logs of the user and use the filters to find the specific sign-in history for any particular user.
- Apply filters such as: RequestID, Status, Sign-in error code, IP address and more.

Step 3: Viewing **Sign-in** Details

- Click on a log entry to review:
  - **Date and Time** of login attempt.
  - **IP Address and location** (to detect unusual access).
  - **Device details** (Operating system, browser).
  - **Authentication details** (MFA status, authentication method).
  - **Status** (Successful, Failed, Conditional Access applied).

Step 4: Investigating **Failed Sign-in Attempts**

- Look for multiple failed attempts in a short time (possible brute-force attack).
- Verify the **IP address and location**—unexpected locations may indicate unauthorized access.
- Check if **Multi-Factor Authentication (MFA)** was attempted.

Step 5: Exporting **Sign-in Logs**

- Click the **Download** button to save log data for further analysis.

4. Managing Groups in Microsoft Entra

4.1 Creating a New Group

Step 1: Go to the Groups section from the Navigation Panel

- In the **left-hand menu**, click on **Groups > All Groups**.
- Click **+ New group** at the top.

Step 2: Select Group Type

- Choose one of the following group types based on requirements:
  - **Microsoft 365 Group**: Used for collaboration (includes Teams, SharePoint, etc.).
  - **Security Group**: Used for access control to resources.

Step 3: Provide Group Detail

- **Group name**: Enter a meaningful name (e.g., "Finance Team" or "IT Support").
- **Group description**: Add a brief description of the group's purpose.
- **Membership type**:
  - **Assigned**: Manually add members.

- **Dynamic user**: Automatically includes users based on specific attributes.
- **Dynamic device**: Includes devices automatically based on criteria.

Step 4: Adding Members to the Group

- Click on **Members** and select **+ Add members**.
- Search for users and select them.
- Click **Add** to finalize the selection.

Step 5: Finalizing Group Creation

- Review the settings and ensure accuracy.
- Click **Create** to finalize the new group.

4.2 Editing an Existing Group

To modify group settings, follow these steps:

Step 1: Go to the Groups section from the Navigation Panel

- Click on **All Groups** Section.
- Select the group you want to edit.

Step 2: Modify Group Settings

- Under the **Manage** Section, Click **Properties** to change:
  - Group name
  - Description
  - Group Type

        - Membership type
    - Click **Save changes** after making modifications.

Step 3: Editing Memberships

- In the **Members** tab, click **+ Add members** to include new users to the group.
- To remove a member, select the user and click **Remove**.
- Click **Save** to confirm changes.

Step 4: Modifying Group Ownership

- Navigate to the **Owners** tab.
- Click **+ Add owners**, search for the new owner, and select them.
- Select the owner (Users) and click on Remove option to remove the owner.
- Click **Save** to apply changes.

4.3 Deleting a Group

Step 1: Navigate to the Groups section

- Locate the group using the **search** function.
- Click on the group name to open its settings.

Step 2: Initiate Group Deletion

- Go to the selected group's **Overview** Section.
- Click **Delete group** at the top.
- Confirm the deletion by clicking **Yes, delete** when prompted.

  Note: The group will be permanently removed.

4.4 Assigning a Group to a Role

Step 1: Navigate to Groups > Select Group

- Click on the group to open its profile.

Step 2: Assign the Group to a Role

- Under the **Manage** Section, go to **Roles & administrators**.
- Click **Add assignments**, select a role, and click **Assign**. Alternatively, find a link to add assignments.

5. Managing Authentication Methods

5.1 Configuring Authentication Methods for Users

Step 1: Navigate to the Microsoft Entra Admin Center.

- Click **Users** > **All Users** from the Navigation Pane.
- Select the user whose authentication method you want to configure.

Step 2: Access Authentication Methods.

- Click on **Authentication Methods** on the second navigation panel on the left.
- View the currently registered authentication methods (e.g., Phone, Email, Microsoft Authenticator, FIDO2 security keys).

Step 3: Add or Remove Authentication Methods.

- Click **+ Add authentication method** and select the desired method (e.g., Phone number, Authenticator App).
- Follow the prompts to configure the method.
- To remove an existing method, select it and click **Remove**.

Step 4: Save changes.

5.2 Enforcing Multi-Factor Authentication (MFA)

Step 1: Navigate to the Multi-Factor Authentication Settings

- Go to **Users > All Users**.
- Locate the three-dot menu on the right side of the screen and click on **Per-user MFA**.

Step 2: Selecting Users for MFA Enforcement

- In the **Per-user MFA** settings page, use the **search bar** to find specific users or select multiple users from the list.
- Click the checkbox next to each user's name to select them.

Step 3: Enabling MFA for Selected Users

- Click the **Enable** button at the top.
- A confirmation dialog will appear. Review the changes and click **Confirm** to proceed.

Step 4: Notifying Users to Complete MFA Setup

- After enabling MFA, users will be required to set up their authentication methods the next time they log in.
- Notify the user via email or internal communication, instructing them to:
    - Sign in to their Microsoft account.
    - Follow the on-screen prompts to configure MFA (e.g., setting up Microsoft Authenticator or SMS verification).
    - Ensure they complete the registration before their next sign-in.

Step 5: Verifying MFA Configuration

- To confirm that MFA has been successfully enabled, go to **Users > Per-user MFA** and check the **Status** column.
- A status of **Enabled** or **Enforced** indicates that MFA is active for the selected users.

6. Managing Password Resets

6.1 Resetting a User's Password

Step 1: Access the User's Profile

- In the Microsoft Entra's **Navigation Pane**, click **Users > All Users**.
- Find the user whose password needs to be reset.
- Click on the user's name to open their profile.

Step 2: Initiate the Password Reset

- In the user's profile page, locate the **Reset Password** option in the top menu.
- Click **Reset Password** to open the password reset settings.

Step 3: Choose a Password Reset Option

A new password can be generated in one of two ways:

- **Auto-generate password** – Microsoft will create a strong random password.
- **Set custom password** – Manually enter a new password following company security policies.

Step 4: Require Password Change on Next Sign-in

- Enable the option **Require this user to change their password when they first sign in** to enhance security.

Step 5: Confirm and Share the New Password Securely

- Click **Reset** to apply the changes.

- Copy the new password and securely share it with the user via an approved communication channel (e.g., a secure email or an encrypted messaging system).

7. Managing Enterprise Applications

7.1 Viewing and Managing Enterprise Applications

Step 1: Access Enterprise Applications

- Open **Microsoft Entra Admin Center**.
- In the **Navigation Pane**, click on **Application > Enterprise Applications**.
- The **All Applications** page will display a list of all enterprise applications in the organization.

Step 2: Searching for Specific Applications

- Use the **search bar** to find a particular application by name.
- Filter applications by **status, category, or security settings** for better visibility.

Step 3: Managing an Application's Settings

- Click on the application name to access its **Overview Page**.
- Modify settings such as **User Assignments, Permissions, or Conditional Access Policies** as needed.

7.2 Assigning Users to Enterprise Applications

Step 1: Select the Application

- In the **Enterprise Applications** section, click on the application you want to manage.

Step 2: Navigate to the User and Group Assignments

- Under the **Manage** section, click **Users and Groups**.

Step 3: Add Users or Groups

- Click **+ Add User/Group**.
- Search for users or groups by name and select them from the list.
- Click **Assign** to apply the changes.

Step 4: Confirm Role Assignments

- If applicable, assign roles such as **User, Administrator, or App Owner**.
- Click **Save** to finalize the user assignment.

Conclusion

This SOP has covered **user management** in **Microsoft Entra Admin**, including creating, modifying, and deleting users, managing groups, enforcing **Multi-Factor Authentication (MFA)**, resetting passwords, and handling **enterprise applications**. It also detailed how to **view audit and sign-in logs** for security monitoring. By following these procedures, administrators can ensure secure access control, compliance, and efficient IT operations.