Standard Operating Procedure (SOP): Microsoft Admin Center

Table of Contents

Objective:

The objective of this SOP is to provide a comprehensive guide on managing users, groups, roles, multi-factor authentication (MFA), and audit logs within the Microsoft Admin Center and Microsoft Entra. It ensures that administrators can efficiently perform user and group management tasks, assign roles, configure security settings such as MFA, and access audit logs for monitoring and compliance.

Scope:

This SOP covers the following areas within the Microsoft Admin Center and Microsoft Entra:

1. **User Management**: Adding, updating, and deleting user accounts, assigning product licenses, and managing user roles.
2. **Group Management**: Creating, updating, and deleting Microsoft groups, including managing group membership and permissions.
3. **Role Management**: Creating, assigning, updating, and deleting user roles within the Admin Center.
4. **Multi-Factor Authentication (MFA)**: Configuring, enforcing, and updating MFA settings for users.
5. **Audit Logs**: Accessing and reviewing user audit logs in Microsoft Entra to monitor user activity and ensure compliance.

Responsibilities:

1. **Administrator**: Responsible for adding, modifying, or deleting user accounts, managing group memberships, assigning roles, configuring MFA, and monitoring user activity through audit logs.
2. **Users**: Responsible for setting up and maintaining their own MFA settings as instructed and complying with any role-based security protocols established by the administrator.
3. **Security Officer**: Responsible for ensuring that multi-factor authentication and audit logs are enabled and monitored to meet organizational security standards.

Pre-requisites:

1. **Access to Microsoft Admin Center**: The administrator must have a valid administrator account with appropriate permissions in the Microsoft Admin Center.
2. **Microsoft Entra Access**: Administrator must have access to Microsoft Entra to view and manage user and audit logs.
3. **Required Licensing**: Ensure that Microsoft 365 licenses and necessary admin roles (e.g., Global Administrator, User Administrator) are assigned to the users.
4. **Network Access**: Ensure secure and reliable network connectivity for accessing the Admin Center and Entra dashboard.
5. **User Information**: The required user details, including names, roles, and product licenses, should be ready to add new users or update existing ones.

Procedure:

1. Adding User to Microsoft Admin Center

Step 1: Log into the Microsoft Admin Center

1. Open a web browser and go to the Microsoft Admin Center at: https://admin.microsoft.com .
2. Enter your **Admin credentials** (email and password) to log into the portal. Once logged in, you will be redirected to the admin dashboard.

Step 2: Navigate to the Users Section

1. Once logged in, from the left-hand navigation menu, click on **Users**.
2. In the Users section, click **Active Users** to manage current user accounts.

Step 3: Add a New User

1. At the top of the Active Users page, click the **Add a user** button to begin the process of creating a new account.

  - **Note:** You can also select **Bulk add users** if you need to add multiple users at once.

Step 4: Enter User Information

1. **First Name**: Enter the first name of the user.
2. **Last Name**: Enter the last name of the user.
3. **Display Name**: This is automatically generated, but you can adjust it if necessary.
4. **Username**: Enter the username for the new user (this will also create the user's email address).
   - Example: johndoe@companydomain.com
5. **Domain**: Ensure the user's domain is selected from the dropdown list (e.g., companydomain.com).

Step 5: Set Password

1. Choose the option, whether to automatically generate a password or create a custom password.
2. If generating a password automatically, a temporary password will be sent to the new user.
   - **Note**: Ensure the user will change their password upon their first login.

Step 6: Assign Product Licenses:

1. Choose the number of relevant and required product licenses to be granted for the users.

2. If the user is not to be provided with any licenses, select the option to create the user without any licenses.

Step 7: Adding the optional details and settings

1. To add the optional details, click on the profile info (dropdown option).

2. Fill in the user details in the fields such as: Job Title, Department, Office, Office Phone, Fax Number, Mobile Phone, Street Address, City, State/Province.

Step 8: Review and Confirm

1. Review the information entered for accuracy.
   - Double-check the user's name, username, password, email, profile information and licenses.
2. Once verified, click **Finish** or **Add User** to create the new user account.

Step 9: Communicate Credentials to User

1. After creating the user, the system will display a confirmation screen.
2. You will be provided with the new user’s login credentials, including the temporary password.
   - **Action**: Ensure the user receives their login details securely (e.g., via email or encrypted communication).

2. Create, Read, Update & Delete a Microsoft Group

2.1. Creating a Microsoft Group

Step 1: Log into the Microsoft Admin Center

1. Open a web browser and go to: https://admin.microsoft.com.
2. Enter your Admin credentials to log into the portal.
3. Once logged in, the Admin Center dashboard will load.
   - **Note:** If you are already signed in, skip **step 1**.

Step 2: Navigate to the Groups Section

1. From the left-hand navigation menu, click on **Groups**.
2. In the Groups section, select **Active groups** to view and manage existing groups.

Step 3: Create a New Group

1. At the top of the Active groups page, click on **Add a group**.
2. Select the group type:
   - **Microsoft 365 Group** – for collaborative teams.
   - **Security Group** – for managing access to resources.
   - **Distribution List** – for sending emails to a group.
3. After selecting the group type, click **Next**.

Step 4: Enter Group Information

1. **Group Name:** Enter a unique name for the group.
2. **Group Email (optional):** If applicable, provide an email address for the group.
3. **Group Description (optional):** Enter a description for the group (this helps users understand the group's purpose).
4. **Privacy:** Choose the privacy setting (Public or Private).
5. **Membership Type:** Choose either "Assigned" or "Dynamic" for membership type.
   - **Assigned:** Admins assign members manually.
   - **Dynamic:** Membership is automatically managed based on attributes like location or department.

Step 5: Assign Owners and Members

1. **Assign Owners:** Add owners who can manage the group (usually team leaders or IT admins).
2. **Assign Members:** Add members who will be part of the group (this can be done by searching for individual users).

Step 6: Review and Create

1. Review all entered information for accuracy.
2. Once verified, click **Create** to finalize the creation of the new group.

2.2 Reading and Viewing Microsoft Groups

Step 1: View Existing Groups

1. Navigate to the **Active groups** page under **Groups**.
2. In the list of groups, you can filter or search for specific groups by name or type.
3. Click on any group to view its details, such as:
   - Group name
   - Group type (Microsoft 365, Security, or Distribution)
   - Membership details (owners, members, and pending requests)
   - Settings and permissions

2.3 Updating a Microsoft Group

Step 1: Edit Group Details

1. From the **Active groups** page, select the group you wish to update.
2. On the group's settings page, click on **Edit** next to the section you want to modify (e.g., group name, description, email address).

Step 2: Modify Group Settings

1. **Group Name/Description/Email:** Change these fields as needed.
2. **Privacy Settings:** Adjust the privacy settings (Public or Private).
3. **Membership Type:** Change between "Assigned" or "Dynamic" if necessary.
4. **Owners/Members:** You can add or remove owners and members from this page.
   - **Add members/owners**: Click on **Add members** and search for users to add to the group.
   - **Remove members/owners**: Select the user and click **Remove**.

Step 3: Save Changes

1. After making the necessary changes, click **Save** or **Update** to apply the changes to the group.

2.4 Deleting a Microsoft Group

Step 1: Select the Group to Delete

1. Go to the **Active groups** page and select the group you wish to delete.
2. On the group's settings page, click **Delete**.

Step 2: Confirm Deletion

1. A confirmation message will appear asking if you’re sure you want to delete the group.
2. If you're certain, click **Delete** to permanently remove the group.
3. **Note:** Deleting a group will remove all members and any group-related data (emails, files, etc.). Ensure proper backup if necessary.

2.5 Managing Permissions and Roles for Groups

Step 1: Assigning Roles to Group Members

1. From the **Group settings** page, click on **Members**.
2. Select the member whose role you wish to modify.
3. Click on **Edit roles** to assign a role (e.g., member, owner).

Step 2: Changing Group Permissions

1. In the **Group settings** page, navigate to **Settings** and adjust group-specific permissions such as:
   - Email access
   - File sharing options

  - Permissions for external sharing
  - Calendar or other group resources access.

3. Creating and Updating User Roles in Microsoft Admin Center

3.1 Creating a New User Role in Microsoft Admin Center

Step 1: Go to the Microsoft Admin Center

Step 2: Navigate to the Roles Section

1. From the left-hand navigation menu, click on **Roles** under the **Admin Centers** section.
2. In the **Roles** section, you will see a list of available roles.

Step 3: Add a New Role

1. In the Roles page, click on **Add a role** at the top.
2. Choose **Custom Role** if you want to create a role with specific permissions not covered by the default roles.
   - **Custom Role:** Allows you to configure a role based on the organization's needs.
   - **Predefined Role:** If a predefined role like **Global Administrator** or **User Administrator** suits your needs, select that role.

Step 4: Define Role Settings and Permissions

1. **Role Name:** Enter a descriptive name for the new role (e.g., “HR Manager Role”).
2. **Role Description:** Provide a clear description of the role (e.g., “This role grants permissions to manage employee records and payroll”).
3. **Permissions:** Select the specific permissions associated with this role. Permissions could include access to:
   - User management (add, modify, delete users)

   - Service settings (e.g., SharePoint, Exchange, Teams)
   - Directory management (e.g., user/group settings)

4. **Assign Scope:** Specify which organizational units (OU) or users this role should apply to. This can be applied to:
   - All users
   - Specific organizational units (OUs)
   - Specific groups or departments

Step 5: Review and Save Role

1. Review all settings and permissions to ensure that they are correct.
2. Click **Create Role** to finalize and create the new role.

3.2 Assigning a Role to a User

Step 1: Navigate to the Users Section

1. In the Microsoft Admin Center, from the left-hand navigation menu, click on **Users**.
2. In the **Active Users** section, search for the user to whom you want to assign a role.

Step 2: Select the User

1. Once you have located the user, click on their name to open their user profile.
2. On the user's profile page, click on **Roles** in the left-hand menu.

Step 3: Assign the Role

1. Click on **Manage Roles** to assign a new role to the user.
2. In the **Roles** section, search for and select the role you wish to assign (e.g., **Global Administrator**, **User Administrator**, **Custom Role**).
3. Click **Save** to apply the role to the user.

Step 4: Verify Role Assignment

1. After saving the changes, the new role should appear under the **Roles** section in the user's profile.
2. Ensure the role is correctly displayed and that the user has the appropriate permissions.

3.3 Updating an Existing User Role

Step 1: Navigate to the Users Section

1. Go to the **Active Users** section in the **Users** tab of the Admin Center.
2. Search for and select the user whose role you want to update.

Step 2: Edit User's Roles

1. In the **Roles** section of the user's profile, click **Manage Roles**.
2. In the **Role Management** window, either:
   - **Add a New Role:** Select additional roles to grant to the user.
   - **Remove an Existing Role:** Uncheck the role you wish to remove from the user.

Step 3: Save Changes

1. Once you've made the necessary changes, click **Save** to apply the updated roles to the user.
2. The updated roles will immediately take effect.

Step 4: Verify Updated Roles

1. Review the user's profile to ensure the updated roles are listed correctly.
2. Double-check that the user now has the correct permissions and access based on their updated role.

3.4 Deleting a User Role

Step 1: Navigate to the Roles Section

1. From the **Roles** section, locate the role you want to delete (if it's a custom role).
2. Click on the role to open the details page.

Step 2: Remove Role from Users

1. Before deleting the role, ensure that it is not assigned to any active users. You can check which users have the role by reviewing the **Assigned Users** section.
2. If the role is assigned to any users, either:
    - Reassign a different role to those users.
    - Remove the role from the users.

Step 3: Delete the Role

1. Once the role is no longer assigned to any users, click **Delete Role** on the role details page.
2. A confirmation window will appear. Confirm that you want to delete the role permanently.

Step 4: Verify Deletion

1. After deleting the role, ensure that it no longer appears in the **Roles** section.
2. Confirm that no users are assigned the role.

4. Configuring Multi-Factor Authentication (MFA) in Microsoft Admin.

4.1 Enabling MFA for Users in Microsoft Admin Center

Step 1: Log into the Microsoft Admin Center

Step 2: Navigate to the MFA Settings

1. In the Admin Center, from the left-hand navigation menu, click on **Users**.

2. In the **Active Users** section, click on **Multi-Factor Authentication** at the top.
3. This will open the MFA management page, where you can view and manage user MFA settings.

Step 3: Enable MFA for Specific Users

1. On the **Multi-Factor Authentication** page, you will see a list of users in your organization.
2. Select the user(s) you want to enable MFA for by checking the box next to their name.
3. Once selected, click on the **Enable** button to turn on MFA for the user.
    - Note: You can also enable MFA for multiple users at once by selecting multiple checkboxes.

Step 4: Notify the User to Set Up MFA

1. After enabling MFA for the user, they will receive an email notifying them to set up their authentication method.
2. The user will be prompted to follow the MFA registration process the next time they log in.

4.2 Configuring MFA Settings for Users

Step 1: Select the User for Configuration

1. On the **Multi-Factor Authentication** page, find the user who needs to configure their MFA settings.
2. Click on the user’s name to open their MFA configuration options.

Step 2: Configure MFA Methods

1. The user will be prompted to choose from a variety of authentication methods. Available options include:
   - **Microsoft Authenticator App**: A mobile app that generates time-based one-time passwords (TOTPs).
   - **Phone Call**: Receive an automated phone call to authenticate.
   - **Text Message (SMS)**: Receive a one-time passcode via SMS.
   - **Security Key or Hardware Token**: A physical device that generates authentication codes or uses biometric data.
2. Select and set up the preferred method. For example, if the **Microsoft Authenticator App** is selected, the user will be instructed to download the app, scan a QR code, and complete the registration.

Step 3: Complete the MFA Setup

1. Once the method is selected and the user has completed the setup process, they will be asked to verify their method.
2. They will enter the verification code sent to their chosen method (e.g., from the Authenticator app or received via SMS).
3. After the code is verified, the MFA setup is complete.

4.3 Enforcing MFA Policies for Users

Step 1: Navigate to Conditional Access (Optional)

1. To enforce MFA based on specific conditions, you can set up **Conditional Access** policies.
2. In the Admin Center, from the left-hand menu, select **Security**.
3. Click on **Conditional Access** and then choose **New Policy**.

Step 2: Set Conditional Access Rules

1. In the **New Policy** settings, configure the conditions under which MFA will be required, such as:
   - **User/group**: Specify users or groups who need MFA.
   - **Cloud apps or actions**: Define which cloud apps require MFA (e.g., Microsoft 365, Exchange).
   - **Conditions**: Set additional conditions like location or device state.
2. Under **Grant**, choose **Require multi-factor authentication**.
3. Save the policy to enforce MFA under the specified conditions.

4.4 Updating MFA Settings for Users

Step 1: Navigate to User's MFA Settings

1. In the **Multi-Factor Authentication** page, find the user whose MFA settings need to be updated.
2. Click on their name to open the user's MFA configuration.

Step 2: Update MFA Methods

1. If the user needs to change their authentication method (e.g., change from phone call to Microsoft Authenticator), click **Manage Settings**.
2. The user will be able to update or reconfigure their authentication method.
   - For example, they can remove the old method and add a new one, such as setting up a different phone number or switching to a hardware token.

Step 3: Save Changes

1. Once the changes are made, click **Save** to apply the updated settings.

4.5 Disabling MFA for Users

Step 1: Navigate to the User's MFA Settings

1. In the **Multi-Factor Authentication** page, locate the user for whom you wish to disable MFA.
2. Click on the user's name to open their settings.

Step 2: Disable MFA

1. In the user's MFA settings, click **Disable** to turn off MFA for that user.
2. Confirm the action when prompted.

Step 3: Save Changes

1. After disabling MFA, ensure the user is aware and confirm the change with them.
2. The user will no longer be required to authenticate using MFA when logging into Microsoft 365 services.

4.6 Monitoring MFA Usage and Audit Logs

Step 1: Access the Sign-In Logs

1. To monitor MFA usage and view any authentication issues, go to the **Azure AD Sign-ins** page.
2. From the **Microsoft Admin Center**, click on **Azure Active Directory** > **Sign-ins**.
3. Use the filters to view specific sign-in events related to MFA authentication (e.g., failed MFA attempts, successful MFA).

Step 2: Review Authentication Details

1. Review logs to check for any potential issues, such as:
   - **Failed MFA attempts**: Monitor for unauthorized attempts or errors.
   - **Successful MFA logins**: Verify that MFA is being successfully used by users.

2. Ensure compliance with your organization’s security policies.

5. Viewing the Audit logs of the users.

5.1 Accessing Audit Logs in Microsoft Entra

Step 1: Log into Microsoft Entra

1. Open a web browser and navigate to Microsoft Entra.
2. Enter your **Admin credentials** (email and password) to log in.
3. After successful login, you will be directed to the **Microsoft Entra** dashboard.

Alternatively, you can access the **Microsoft Admin Center** and click on **Identity** on the left-hand navigation menu. You will be redirected to **Microsoft Entra Admin Dashboard**.

Step 2: Navigate to the Audit Logs Section

1. In the left-hand navigation menu, click on **Users.**
2. Under **Users** menu, you can find **Audit Logs** option, click on it to access the overall audit logs of all the users.
3. To view the **logs** of one particular user, click on the **Display Name** of any one of the users in the **All Users** option.
4. You will be redirected to the profile of the selected user.
5. Click on the **Audit logs** option in the User’s profile to view the logs of the selected user.