SOP: Managing Microsoft Admin Center

Date Created: 06/05/2025
Owner: IT Department
Version: 1.0

Table of Contents

1. Purpose

This SOP provides comprehensive guidelines for managing the Microsoft Admin Center. It ensures proper administrative oversight across user accounts, licenses, devices, roles, and security settings within Microsoft 365. The procedure promotes consistency, security, regulatory compliance, and accountability in the use of Microsoft 365 services.

2. Scope

This SOP is intended for IT administrators, system engineers, and IT security staff responsible for:

- User and group management
- Role and permission assignment
- Device enrollment and compliance
- Security monitoring and incident response
- License allocation and usage tracking

It applies to the Microsoft 365 Admin Center and integrated portals, including **Microsoft Entra Admin Center**, Microsoft Intune Admin Center, and Exchange Admin Center.

3. Prerequisites

- Valid admin credentials with necessary role assignments (e.g., Global Admin, User Admin, Intune Admin)
- Active device with secure internet connection

4. Procedures

4.1 Accessing the Admin Center

1. Navigate to https://admin.microsoft.com.
2. Log in with admin credentials.
3. You will be redirected to the admin center dashboard.

4.2 User Management

Create a New User:

1. Go to **Users > Active Users**.
2. Click **Add a user**.
3. Add necessary details and click **Finish adding**.

Modify an Existing User:

1. Search for the user in **Active Users**.
2. Click the user's name > choose from tabs: **Account**, **Licenses and Apps**, **Roles**, etc.
3. Make required changes (e.g., reset password, block sign-in, update license).
4. Save all changes and document the update.

Delete or Restore a User:

1. Select the user > click **Delete user**.
2. Confirm deletion. User is moved to **Deleted users**.
3. To restore: Go to **Users > Deleted Users** > select user > click **Restore user**.

Note: For a detailed instruction for adding and managing users, please refer to the document available through this link.

4.3 License Management

1. Navigate to **Billing > Licenses**.
2. Review available and consumed licenses.
3. To assign or remove licenses:

- Go to **Users > Active Users** > select a user.
- Click **Licenses and Apps** tab.
- Enable/disable relevant licenses.
- Click **Save Changes**.

4.4 Group and Role Assignments

Manage Groups:

1. Within the Microsoft Admin Center, Go to **Groups > Active Groups**.
2. Click **Add a group**.
3. Choose group type: Microsoft 365, Security, or Mail-enabled Security.
4. Enter group name, description, and owner.
5. Add members and configure settings.
6. Save and document group creation.

Assign Admin Roles:

1. Navigate to **Roles > Admin Roles**.
2. Search or select a role (e.g., Exchange Admin).
3. Click **Assigned Admins > Add**.
4. Select the user(s) and confirm.
5. Document the role change for audit tracking.

4.5 Device Management (via Intune)

1. Go to **Endpoint Manager Admin Center (Intune) via** https://intune.microsoft.com
2. Navigate to **Devices > All Devices**.
3. Review the device list (filter by platform, compliance, status).
4. Select a device to:
   - View hardware/software inventory
   - Sync, Wipe, Retire, or Rename the device
   - Review device compliance policies
5. For new device enrollment:
   - Ensure the device is registered under **Azure AD**
   - Automatically assign it to the correct policy/profile via Dynamic Groups

6. Document device actions taken.

For the detailed instructions on enrolling and managing the endpoint devices using intune, please refer to the document available via this link.

4.6 Security Monitoring and Secure Score

1. Navigate to **Microsoft 365 Defender** via Admin Center available via https://security.microsoft.com/
2. Click **Incidents & Alerts**.
3. Review active incidents: analyze severity, impacted users, and threat source.
4. Take appropriate actions (e.g., block user, initiate password reset, isolate device).
5. Under **Reports > Security Report**, review the overall security posture.
6. Address recommended actions and update configurations as needed.

4.7 Compliance and Auditing

1. Go to Microsoft Purview via https://purview.microsoft.com/
2. Click on the **solutions**, on the left side of your screen.
3. Now click on the **compliance manager** option.
3. You will be redirected to the compliance manager dashboard where you can view the compliance score.
5. Click on Assessment to start the compliance check with the regulations you want.

5. Admin Center Maintenance

- Review and validate admin role assignments quarterly.
- Check unused licenses and deactivate unused accounts timely.
- Review alerts and Secure Score recommendations weekly.

6. Conclusion

This SOP provides clear guidance for managing the Microsoft Admin Center, helping IT staff maintain secure, consistent, and compliant operations across Microsoft 365 services. Regular use of these procedures supports effective user, device, and license management while reinforcing the organization’s overall IT governance and security posture.