## Manage Roles and Role Groups

At the end of this episode, I will be able to:

1. Manage roles in Microsoft 365 and Azure AD
2. Manage role groups for Microsoft Defender, Microsoft Purview, and Microsoft 365 workloads

Learner Objective: *Learn to manage roles and role groups in Microsoft 365 and Azure AD.*

Description: In this episode, you will learn to manage roles in Microsoft 365 and Azure AD. You will also learn to manage role groups for Microsoft Defender, Microsoft Purview, Microsoft Defender, and Microsoft 365 workloads.

---

- MS 365 comes with a set of admin roles that you can assign to users
- Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers.
- Guidelines include:
    - Have two to four Global Admins
    - Assign the least permissive role
    - Require multi-factor authentication for admins
    - Admin roles include: Billing Admin, Exchange Admin, Global Admin, Global Reader, Groups Admin, Helpdesk Admin, License Admin, Message Center Privacy Reader, Message Center Reader, Office Apps Admin, Organization Message Writer, Password Admin, Power Platform Admin, Reports Reader, Service Support Admin, Teams Admin, User Admin, User Experience Success Manager
- You can create Administrative Units in Microsoft 365. This allows you to subdivide your organization in any way you might need and then assign administrative roles to these divisions.
- Role groups are a special kind of universal security group (USG) that is used in the RBAC model in Exchange Online

---

Additional Resources:

*Assign admin roles in the Microsoft 365 admin center*
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/assign-admin-roles?view=o365-worldwide

*About admin roles in the Microsoft 365 admin center*
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide