

Episode Title: Manage AD built-in administrative groups

Objectives:

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

1. Locate and add users to built-in groups
2. Manage group membership
3. Audit and review group membership access

Key Points:

Key Point 1

The built-in administrative groups can be managed through Active Directory Users and Computers or the AD Admin Center.

Key Point 2

Adding a member to a built-in group will grant permissions that the group has. Ensure that you are following the principle of least privilege.

Key Point 3

Users typically get added to groups over time, and it's easy for them to accumulate permissions that might not be necessary. Remember to review membership and access on a regular basis.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- Privileged Accounts and Groups in Active Directory
: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory>