# 01 Active Directory

See **AD Structure** for Recommended AD Hierarchy

## Users

### Each Domain Admin will have the following accounts:

- **Normal domain user account:** used for logging into the Tier 0 PAW. Will escalate to local admin to do admin stuff. Also logs into the PAW's VM to do day-to-day tasks.
- **Tier 0 Admin:** Member of domain admins, the normal domain account elevates to this account to admin stuff on Tier 0.
- **Tier 1 Admin:** Used to allow the user to RDP to Tier 1 member servers using RemoteCredentialGuard. Normal domain user also uses this to elevate certain remote management consoles (RSAT/Server Manager) to manage remote Tier 1 servers.
- **Tier 2 Admin:** If the user will ever administrate workstations, they will need this account. Used to allow the user to RDP to remote workstations using RemoteCredentialGuard. Normal domain user also uses this to elevate certain remote management consoles (MMC) to manage remote workstations.
- **Local user account:** Used as a contingency for any lost domain trusts. In other words, if you fubar the domain and you can no longer log in to your PAW, this is the account you would use.
- **Local Admin Account:** This account will be managed by LAPS. Also used for fixing domain trust issues. You would login with the local user account and elevate to this account to do admin stuff.
- **Access to server LAPS Accounts:** They can use this if RDP with /RestrictedAdmin is too restrictive.

### Each Server Administrator will have:

- **Normal domain user account:** used for logging into the Tier 1 PAW. Will escalate to local admin to do admin stuff. Also logs into the PAW's VM to do day-to-day tasks.
- **Tier 1 Admin:** Used to allow the user to RDP to Tier 1 member servers using RemoteCredentialGuard. Normal domain user also uses this to elevate certain remote management consoles (RSAT/Server Manager) to manage remote Tier 1 servers.
- **Local user account:** Used as a contingency for any lost domain trusts. In other words, if you fubar the domain and you can no longer log in to your PAW, this is the account you would use.
- **Local Admin Account:** This account will be managed by LAPS. Also used for fixing domain trust issues. You would login with the local user account and elevate to this account to do admin stuff.

- **Access to server LAPS Accounts:** They can use this if RDP with /RestrictedAdmin is too restrictive.

### Each Security Administrator will have:

- **Normal domain user account:** used for logging into the Tier 1 PAW. Will escalate to local admin to do admin stuff. Also logs into the PAW's VM to do day-to-day tasks.
- **Tier 2 Admin:** Normal domain user uses this to elevate certain remote management consoles (MMC) to manage remote workstations.
- **Local user account:** Used as a contingency for any lost domain trusts. In other words, if you fubar the domain and you can no longer log in to your PAW, this is the account you would use.
- **Local Admin Account:** This account will be managed by LAPS. Also used for fixing domain trust issues. You would login with the local user account and elevate to this account to do admin stuff.

## Groups

The following groups must be created under Groups. The sub-bullet point are the members of the specified group.

**PAW-AllPAW-Computers** - Members of this group include all PAW Tier groups. It is a collection of all PAW machines.

- PAW-Tier0-Computers
- PAW-Tier1-Computers
- PAW-Tier2-Computers

**PAW-BlockPowerShell** – Members of this group are blocked from using PowerShell via GPO

- PAW-Users

**PAW-BlockLocalLogon** - Members of this group are not literally blocked from logging in locally, but rather from running certain applications via the AppLocker GPO after they have logged in.

- PAW-Admins

**PAW-Tier0-Admins** - Members of this group are Tier 0 server admins.

- All members of the DOMAIN\Accounts\PAW Accounts\Tier 0 OU

**PAW-Tier0-Computers** - Members of this group are Tier 0 PAWs. Used mainly for GPO filtering.

- All Tier 0 PAWs

**PAW-Tier0-Users** - Members of this group are Tier 0 PAW users. They can log into Tier 0 PAWs. They are a normal user account on PAWs that use the Tier 0/1/2 Admin accounts to elevate certain tasks.

- All domain users accounts that need to log into Tier 0 PAWs

**PAW-Tier1-Admins** - Members of this group are Tier 1 server admins.

- All members of the DOMAIN\Accounts\PAW Accounts\Tier 1 OU

**PAW-Tier1-Computers** - Members of this group are Tier 1 PAWs. Used mainly for GPO filtering.

- All Tier 1 PAWs

**PAW-Tier1-Users** - Members of this group are Tier 1 PAW users. They can log into Tier 1 PAWs. They are a normal user account on PAWs that use the Tier 1 Admin accounts to elevate certain tasks.

- All domain users accounts that need to log into Tier 0 PAWs

**PAW-Tier2-Admin** - Members of this group are Tier 2 server admins.

- All members of the DOMAIN\Accounts\PAW Accounts\Tier 2 OU

**PAW-Tier2-Computers** - Members of this group are Tier 1 PAWs. Used mainly for GPO filtering.

- All Tier 2 PAWs

**PAW-Tier2-Users** - Members of this group are Tier 2 PAW users. They can log into Tier 2 PAWs. They are a normal user account on PAWs that use the Tier 1 Admin accounts to elevate certain tasks.

- All domain users accounts that need to log into Tier 0 PAWs

**PAW-Users** – Members of this group includes all Tier 0, 1, and 2 Users

- PAW-Tier0-Users
- PAW-Tier1-Users
- PAW-Tier2-Users

**PAW-Admins** - Members of this groups include all the Tier 0, 1, and 2 Admins

- PAW-Tier0-Admins
- PAW-Tier1-Admins
- PAW-Tier2-Admins