02 Local Users & Groups

Local Users

Security control that grants security AND adds usability. PAW security is enhanced when you control the membership of local groups via GPO. You enforce membership in the local admin group. It also increases ease in usability because you are automating a process that would otherwise have to be done manually.

Local Users

- **Local user account** - used as a backup in case any domain trust issues occur that knock the computer off the domain. It must be a standard user because local admins cannot log in. Only elevate.
- **Local Admin account (Separate from Default Local Admin)** - PAW user will use this account for all administrative purposes. We don't want to use the default local admin because that password will change every 30 days via LAPS.

Group Policy

Create a new GPO on the Domain.Subdomain.com\DomainName\Computers OU called **Security – Local Groups – PAW** with the following settings:

Computer Configuration > Preferences > Control Panel Settings > Local Users and Groups

Create the following new groups:

- Administrators (built-in) - You will add a new one of these for every PAW user that needs local admin on their PAW
    - Order: **1**
    - Action: **Update**
    - Description: **PAW Local Admins**
    - Delete all users and groups: **Unchecked**
    - Members:
        - **.admin** – The account you created in the Local Users section above
        - **AD\user.t0** – The tier 0 account belonging to the PAW user
        - **AD\user.t1** – The tier 1 account belonging to the PAW user
        - **AD\user.t3** – The tier 2 account belonging to the PAW user
    - Item-Level targeting
        - The NetBIOS computer name is <Select the specific User's PAW computer object>

- Repeat this step for **every** individual PAW, adding the correct local user to each.

NOTE: *It is required to add each of the tier admins accounts to the local admins group because that is the only way to permit the PAW users to run their admin tools (MMC/RSAT/Server Manager\etc...) as that user with a fingerprint. You run the tool as administrator, then swipe the finger for the given admin user.*

- Backup Operators (built-in)
    - Order: **2**
    - Action: **Update**
    - Description: **All PAW Backup Operators**
    - Delete all users and groups: **Checked**
    - Members: **None**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-AllPAWComputers
- Cryptographic Operators (built-in)
    - Order: **3**
    - Action: **Update**
    - Description: **All PAW Cryptographic Operators**
    - Delete all member user and groups: **Checked**
    - Members: **None**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-AllPAWComputers
- Network Configuration Operators (built-in)
    - Order: **4**
    - Action: **Update**
    - Description: **All PAW Network Configuration Operators**
    - Delete all users and groups: **Checked**
    - Members: **None**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-AllPAWComputers
- Power Users (built-in)
    - Order: **5**
    - Action: **Update**
    - Description: **All PAW Power Users**
    - Delete all member user and groups: **Checked**
    - Members: **None**
    - Item-level targeting

        - the computer is a member of the security group AD\PAW-AllPAWComputers

- Remote Desktop Users (built-in)
    - Order: **6**
    - Action: **Update**
    - Description: **All PAW Remote Desktop Users**
    - Delete all users and groups: **Checked**
    - Members: **None**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-AllPAWComputers
- Replicators (built-in)
    - Order: **7**
    - Action: **Update**
    - Description: **All PAW Replicators**
    - Delete all member user and groups: **Checked**
    - Members: **None**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-AllPAWComputers
- Hyper-V Administrators (built-in)
    - Order: **8**
    - Action: **Update**
    - Description: **PAW Tier 0 Hyper-V Admins**
    - Delete all users and groups: **Checked**
    - Members: **AD\PAW-Tier0-Users**
    - Item-level targeting
        - the computer is a member of the security group AD\PAW-Tier0-Computers
- Repeat this step for Tier1 and Tier2 PAWs

Close the policy window. On the scope tab:

- Ensure the Link to the Computers OU is Enabled.
- Ensure **Authenticated Users** is selected under **Security Filtering**.
- Ensure there is no WMI filter applied.

On the Details tab: Set GPO status to **User configuration settings disabled**