**Module 4 Identity & Access Management**

**4.4 Account Practices**

**General Concepts**

* Onboarding/Offboarding
* Standard naming convention (for user IDs)
* Least privilege
* Time-of-day restrictions
* Location-based policies
* Group-based access control
* Account maintenance/privilege audit
* Recertification/permission creep
* Permission auditing & review
* Usage auditing & access review

**Account Types**

* User accounts – human users
* Guest accounts – should be disabled by default with minimal privileges & time limits
* Shared & generic accounts

1. No repudiation
2. Eg. Conference rooms, kiosk computer
3. Restrict as much as possible

* Change names of default system accounts
* Service accounts

1. Used by systems/apps
2. Restrict human use
3. Restrict access rights/authorisation
4. Set complex passwords

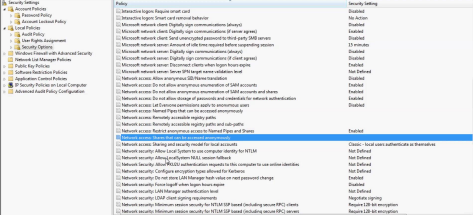
* Privileged accounts/administrator accounts

1. Each user should have separate administrator account
2. Types – Windows Administrator & Linux Root
3. Run as general user & only increase privileges as needed – Windows UAC (user account control), Linux sudo
4. Restrict authorisation & increase logging

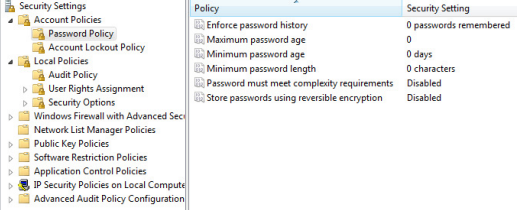
**Account Policy Enforcement**

* Credential management
* Group policy
* Password policies/complexity
* Expiration
* Recovery
* Disablement/locking

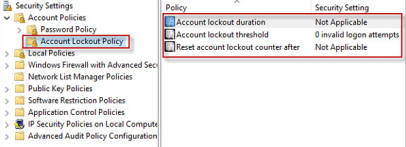
**Windows Policies**



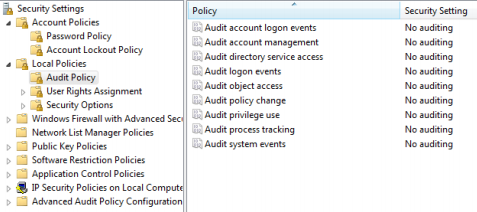
* Windows password policies



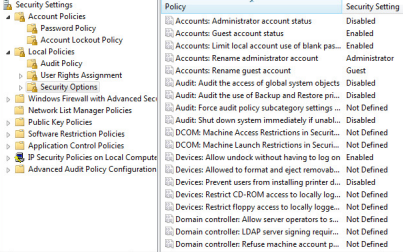
* Windows account lockout policies



* Windows audit policies



* Windows Access Policies



**Linux Password Policies**

