What is an administrative account

What is an administrative account?

An Administrator account is someone or something can can perform a change on an object. If you are enacting change on a user, group, computer, organizational unit, or any object on a domain, you need an administrative account.

Where do you need to begin with administrative accounts?

First step is to figure out who in your environment should have an admin account. When does anyone need an administrative account? How can you find administrators hiding in your domain? What standard can you define that forces a policy for people to use an administrator accounts?

The idea of an administrator account, an account used to perform administrative actions, had evolved. A frequently adopted model is for people to have a separate administrator account for their domain admin permissions. (If this model is not already in place in your environment, it should be adopted ASAP.) Where this model is a good first step, there is always room for improvement. Who all on the environment should have both a regular user account AND an administrative account?

If you answer yes to any of the following scenarios, the person needs a separate administrator account to perform work functions.

Reason 1: Permissions are granted on user objects

Can the person in control of the user object do any of the following:

- Group membership
- Manager
- Security ACLS
- Delete a user?
- Create a user?
- Disable a user?
- Reset a users password?
- Unexpire an expired password?
- Change the smart card requirements?
- Change the login script?
- Set an SPN?

Reason 2: Permissions are granted on computer objects

Can this person perform these computer actions?

- Create a computer
- Deleted a computer
- Set spn of a computer
- Set Security ACLS on a computer?

Reason 3: Permissions are granted on group objects

Can this person perform these actions to any group?

- Create a group
- Delete a group
- Change group membership
- Add and remove users to a group
- Change the group's type
- Change the ACLs on a group

Reason 4: Permissions are granted on OUs and Containers

Can this person perform these actions on organization units or containers?

- Create / delete OUs
- Link/unlink GPOs to OUs
- Change precedence of GPOs
- Change ACLs on an OU
- Edit / delete a GPO
- Change ACLs on a GPO

If the person answers yes to any of the items above for users, groups, computers, or containers, then this person needs a separate admin account.