.

Active Directory

stuff to make active directory better.

- Service account leash

Service account leash

Service accounts should not be logging in interactively. You help desk genius should not be using a service account to log into desktops and servers with domain admin or any other permissions. Service accounts are for SERVICES.

Limit the damage of service account abuse by preventing interactive and local console logon of these accounts.

1. Make a security group for service accounts. Call it what you like- mine is "Service Accounts - Deny Interactive Logon" because i like things to say what they are.
2. put your service accounts in it.
3. Make a GPO with the following:

```
Computer Configuration / Windows Settings / Security Settings / Local Policies / User Rights Assignment
```

```
Deny log on locally: {service accounts' security group}
```

```
Deny log on through Terminal Services: {service accounts' security group}
```

Apply this GPO to any OU with computers you dont want interactive service account logins. i.e. All Of Them.

This might break some stuff- some people like to use a service account to run excel macros and other terrifying things unattended. Watch your logs and make sure you know what those accounts are supposed to be doing.