

# Advantages case study examples

[Technology](#), [Internet](#)



Group Policy is one of features laid down by the server editions of Microsoft that comprises of a specific set of rules that create control over the working environment of the user accounts and system accounts. It enables to create a centrally managed, configuration of operating systems, applications and settings while working in an environment based on active directory. Group policy is mostly seen in enterprise environments and is best suited to activities, when required to be done on network systems that cannot be physically accessed. The policy has also incorporated a system to refresh the sessions and this feature is called as GPO (Group Policy Object).

It helps to maintain uniform settings across terminal servers and the server settings can be changed at one place rather than doing it to individual servers. Only authentic administrators can change the settings and the process is extremely flexible. This is a granular application.

## **Disadvantages**

The group policies require an active directory and it should have the rights and skills to edit a GPO. For different settings on different servers there is a requirement of multiple GPOs or extensive filtering.

## **TACACS+**

Terminal Access Controller Access Control System or TACACS is a protocol that provides access control to various applications like network servers, routers and other devices related to computing. The protocol provides unique services related to accounting, authorization and authentication.

TACACS+ is a product of CISCO. TACACS+ uses TCP and is used on widespread networks. TACACS provides great security and uses TCP which

are its advantages however the disadvantages include weakness towards Birthday Attacks, buffer overflow and is also not very safe against packet sniffing.

RADIUS uses UDP and therefore if TCP is required then TACACS is the right option, moreover RADIUS is vulnerable to buffer overflow attacks however TACACS is not. Kerberos on the other hand uses encryption key (SSO) single sign on to provide authentication and it is primarily the secured option for communication between client and KDC server however TACACS is required as an overall server to network authentication protocol.