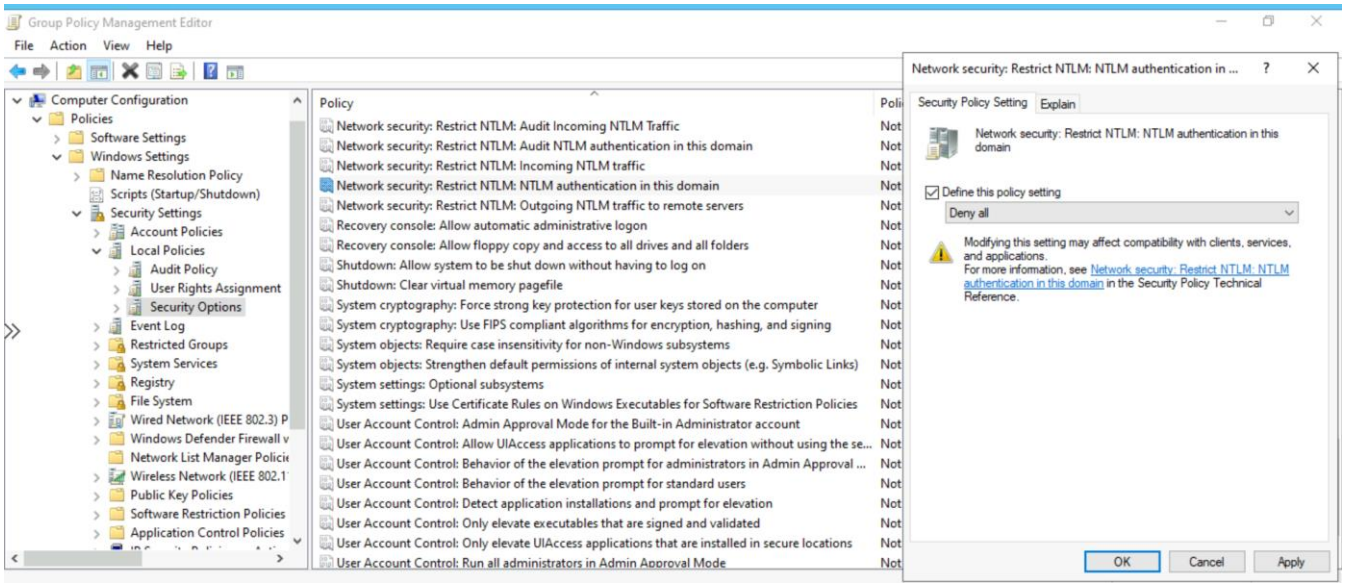
Exercise-4: Advanced Group Policy Hardening

Restrict NTLM Authentication

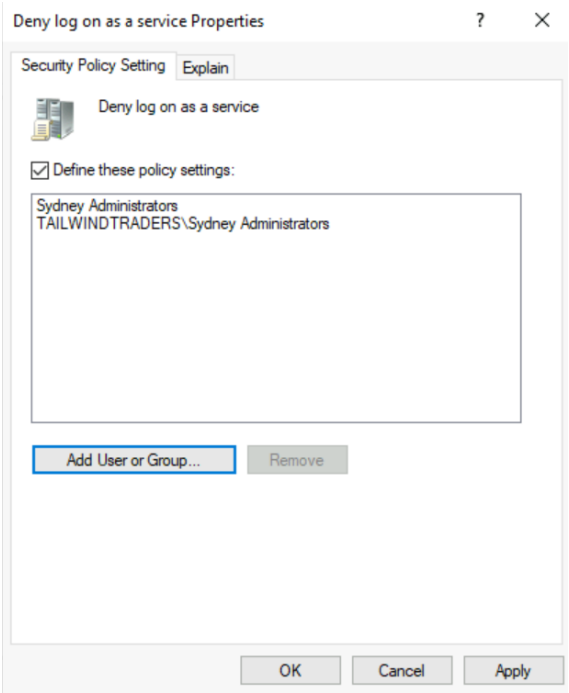
NTLM authentication was restricted at the domain controller level using Group Policy Management. The policy setting for "Network security: Restrict NTLM: NTLM authentication in this domain" was defined (set to Deny all) in the Default Domain Controller Policy.

Screenshot:

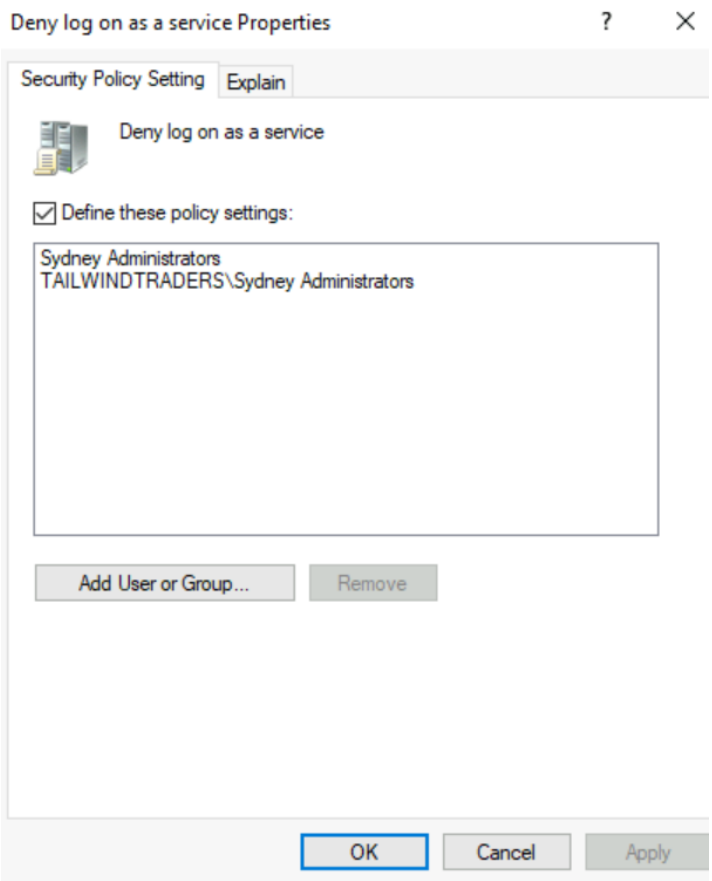
- Illustrates the Group Policy setting restricting NTLM authentication



- Shows the actual policy setting, 'Deny all'



- H-CNF-1.jpg: Confirmation of hardening/setting change

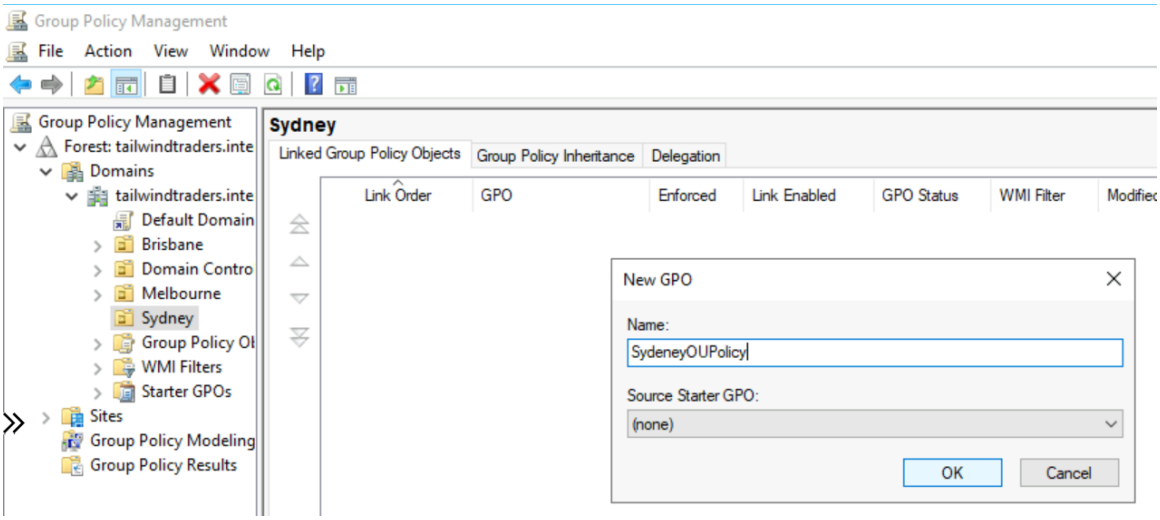


Audit User Account Management in Sydney OU

A dedicated GPO named "SydneyOUPolicy" was created and linked to the Sydney OU. User Account Management auditing was enabled under Advanced Audit Policy Configuration, enforcing logging of both Success and Failure events for changes to user accounts.

Screenshot placeholder:

- Creation of new Group Policy Object (SydneyOUPolicy)



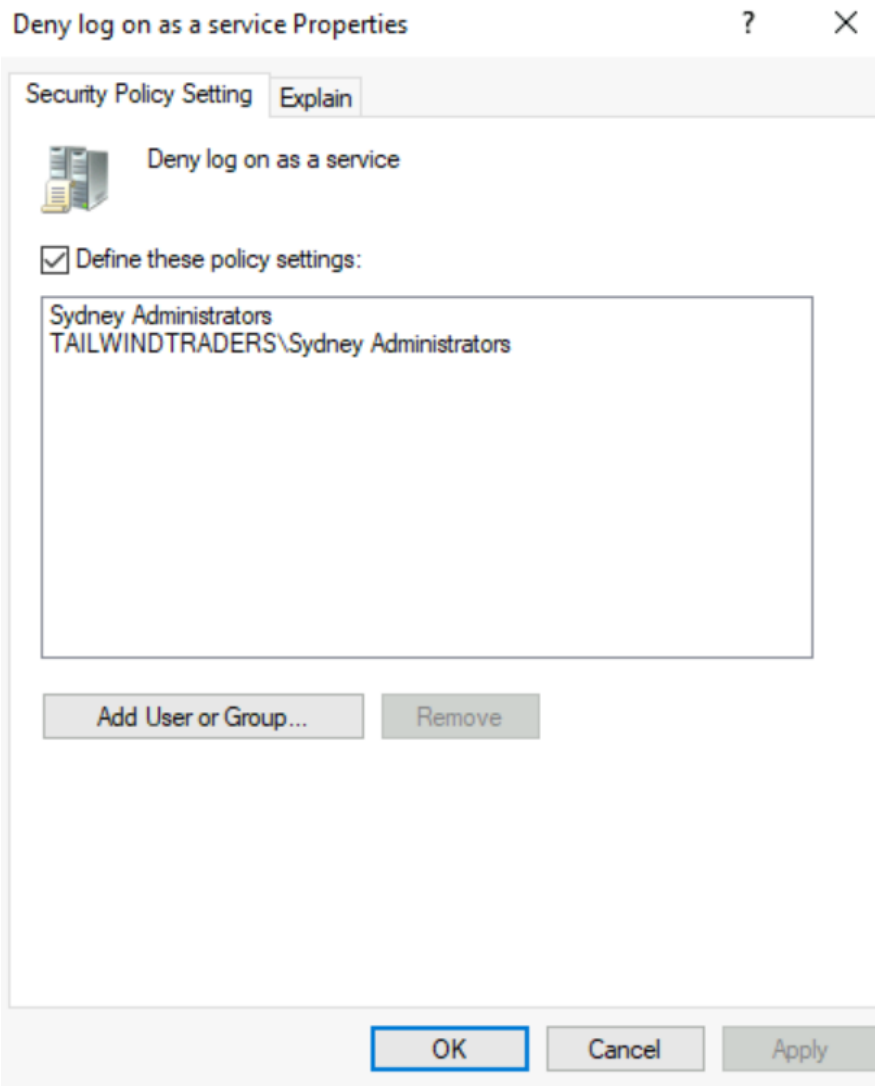
- Properties dialog showing audit events for user account management

Deny Log On As a Service (Sydney Administrators Group)

The "Deny log on as a service" user rights assignment in SydneyOUPolicy was configured, explicitly adding Sydney Administrators to the list. This further restricts administrative session capabilities for this group within the OU.

Screenshot placeholder:

- Policy properties showing Sydney Administrators group assigned to 'Deny log on as a service'



This documentation summarizes the NTLM authentication hardening, auditing of user account management, and denial of log on as a service for the Sydney Administrators.