



Una volta creati dei gruppi di lavoro ci dirigiamo nella console Group Policy Management Editor, qui possiamo configurare le policy desiderate per ogni gruppo.

### Gruppo DIRIGENZA:

Bloccare l'accesso a determinati pannelli o funzionalità: andando in User Configuration > Administrative Templates > Control Panel e configurando:

- Prohibit access to Control Panel and PC settings su Enabled.

Impostare una home page per il browser: andando in User Configuration > Administrative Templates > Windows Components > Internet Explorer e configurando:

- Disable changing home page settings e imposta una home page specifica.

Impostare uno sfondo per il desktop: andando in User Configuration > Administrative Templates > Desktop > Desktop e configurando:

- Desktop Wallpaper, impostando il percorso di un'immagine.

### Gruppo MARKETING:

Accesso limitato ai dischi locali:

- User Configuration > Administrative Templates > Windows Components > File Explorer.
  - Prevent access to drives from My Computer: Blocca l'accesso a dischi specifici, come il disco C:\ (Enabled, scegli le lettere dei dischi da bloccare).

Imposta una cartella condivisa per i file:

- User Configuration > Preferences > Windows Settings > Drive Maps.
  - Crea una mappatura automatica per una cartella di rete, ad esempio "Cartella Marketing"

Blocco di applicazioni non autorizzate:

- User Configuration > Administrative Templates > System > Don't run specified Windows applications.

### Gruppo ALUNNI:

1. Bloccare l'accesso a Pannello di Controllo e Impostazioni:
  - User Configuration > Administrative Templates > Control Panel.
    - Prohibit access to Control Panel and PC Settings: Impedisce agli alunni di modificare configurazioni di sistema.
2. Impedire l'installazione di software:
  - Computer Configuration > Administrative Templates > Windows Components > Windows Installer.
    - Disable Windows Installer: Configura come Enabled per bloccare nuove installazioni.
3. Disabilitare l'accesso al Prompt dei comandi:
  - User Configuration > Administrative Templates > System.
    - Prevent access to the command prompt: Imposta su Enabled.
4. Bloccare l'utilizzo di dispositivi USB:
  - Computer Configuration > Administrative Templates > System > Removable Storage Access.
    - Configura Deny read and write access to removable drives per prevenire l'uso di USB.

### Gruppo DOCENTI:

1. Accesso completo al Pannello di Controllo:
  - User Configuration > Administrative Templates > Control Panel.

- Prohibit access to Control Panel and PC Settings:  
Configura su Disabled per permettere ai docenti di accedere e modificare alcune impostazioni.
- 2. Consentire l'utilizzo di dispositivi USB:
  - Computer Configuration > Administrative Templates > System > Removable Storage Access.
    - Configura Deny read and write access to removable drives su Disabled per consentire l'utilizzo di chiavette USB.
- 3. Accesso al Task Manager:
  - User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options.
    - Remove Task Manager: Configura su Disabled per permettere ai docenti di monitorare i processi.
- 4. Impostare una scadenza delle password:
  - Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.
    - Imposta una scadenza (es. 90 giorni) e obbliga password complesse per aumentare la sicurezza.

Questi sono solo alcuni esempi di policy che possono essere applicate per gestire e personalizzare i gruppi utenti all'interno di un dominio Active Directory. Le configurazioni possono essere ulteriormente adattate in base alle esigenze specifiche dell'organizzazione, come l'aggiunta di regole per il controllo delle applicazioni, l'accesso a risorse cloud o la gestione di dispositivi mobili.