Khoa Công nghệ Thông tin – Đại học Khoa học tự nhiên

Bộ môn Mạng máy tính và Viễn thông

Môn: Hệ điều hành

Bài thực hành số 3: GROUP POLICY

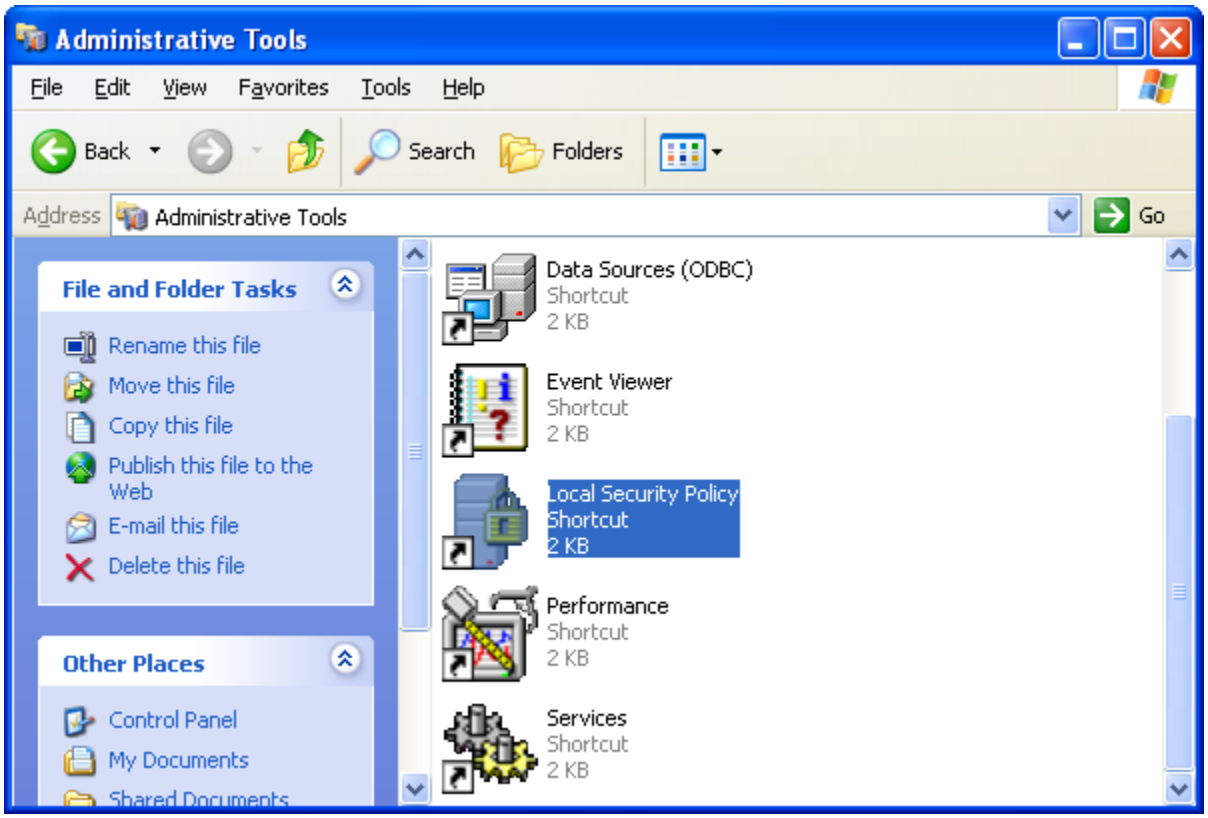
1. Giới thiệu:

Bài học giới thiệu về các chính sách, cấu hình về bảo mật trên Windows

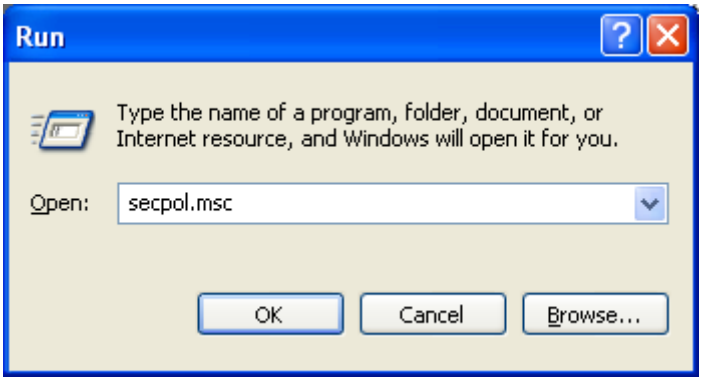
Các thao tác điều khiển về chính sách an toàn của Windows thường được thiết lập qua 2 cách:

- Local Security Policy:

Control Panel / Administrative Tools / Local Security Policy

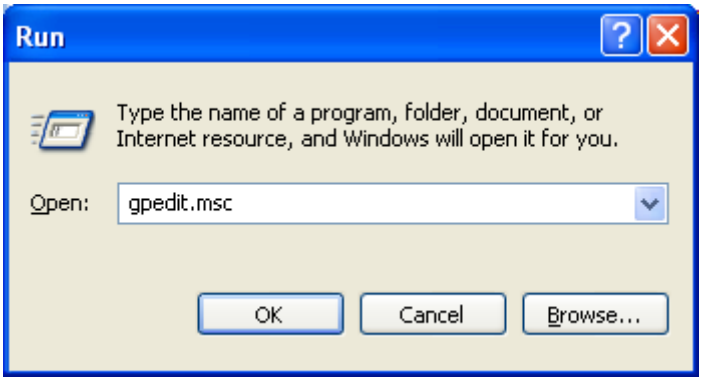


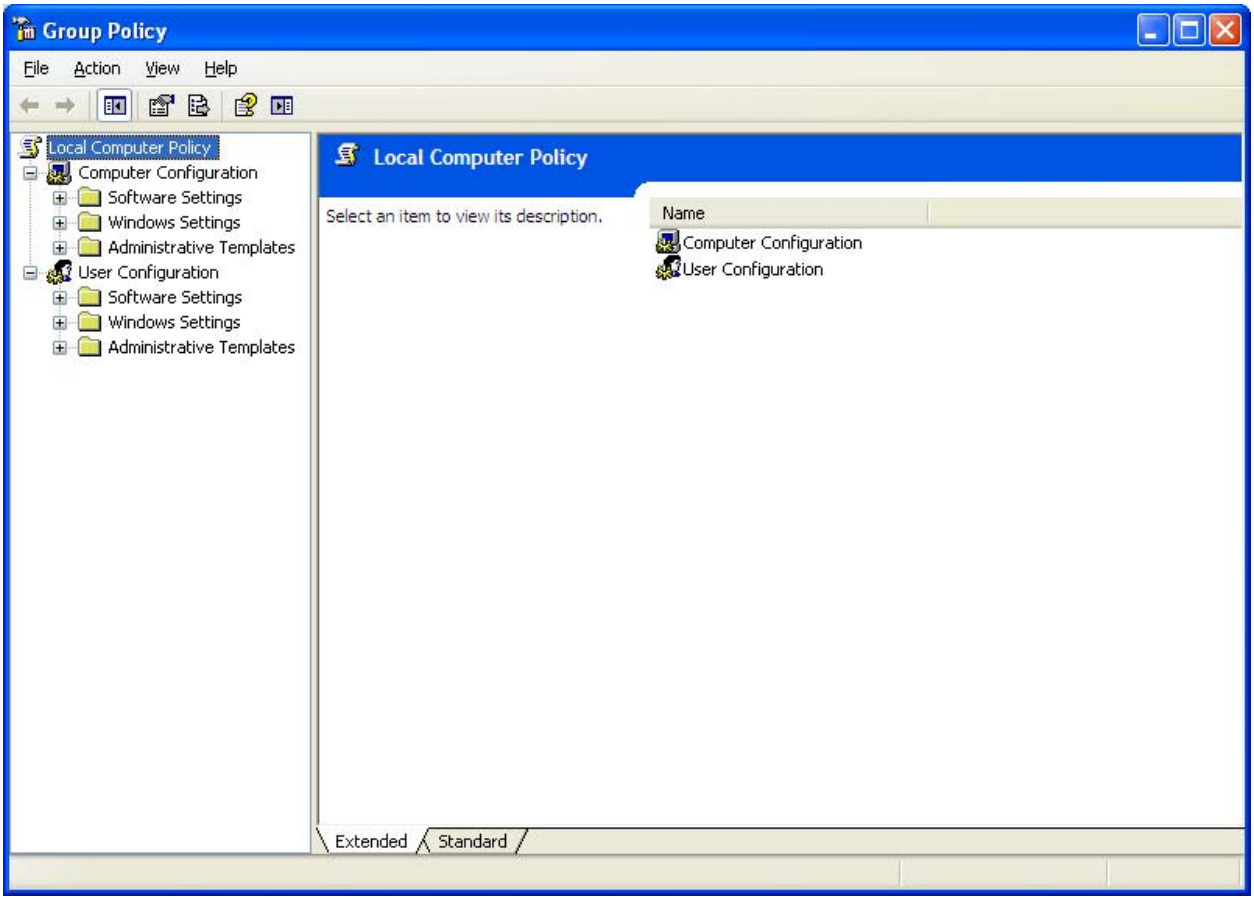
Hoặc từ mục run, gõ secpol.msc



- Group Policy:

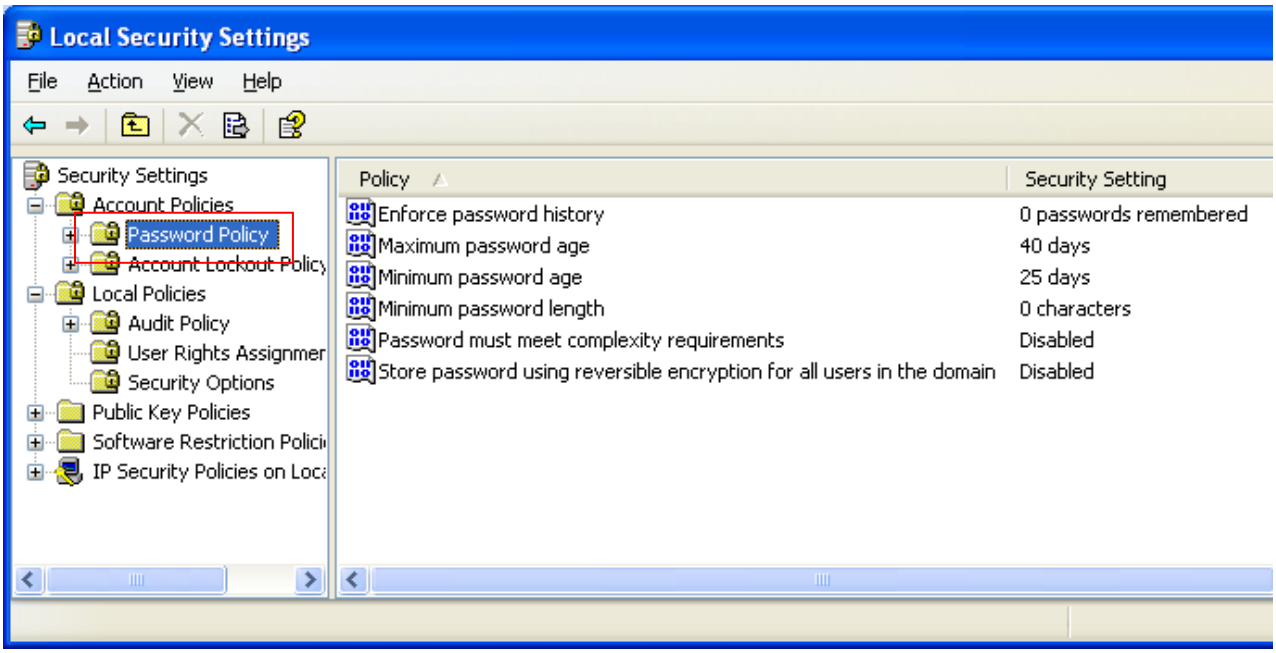
Từ menu Run, gõ gpedit.msc





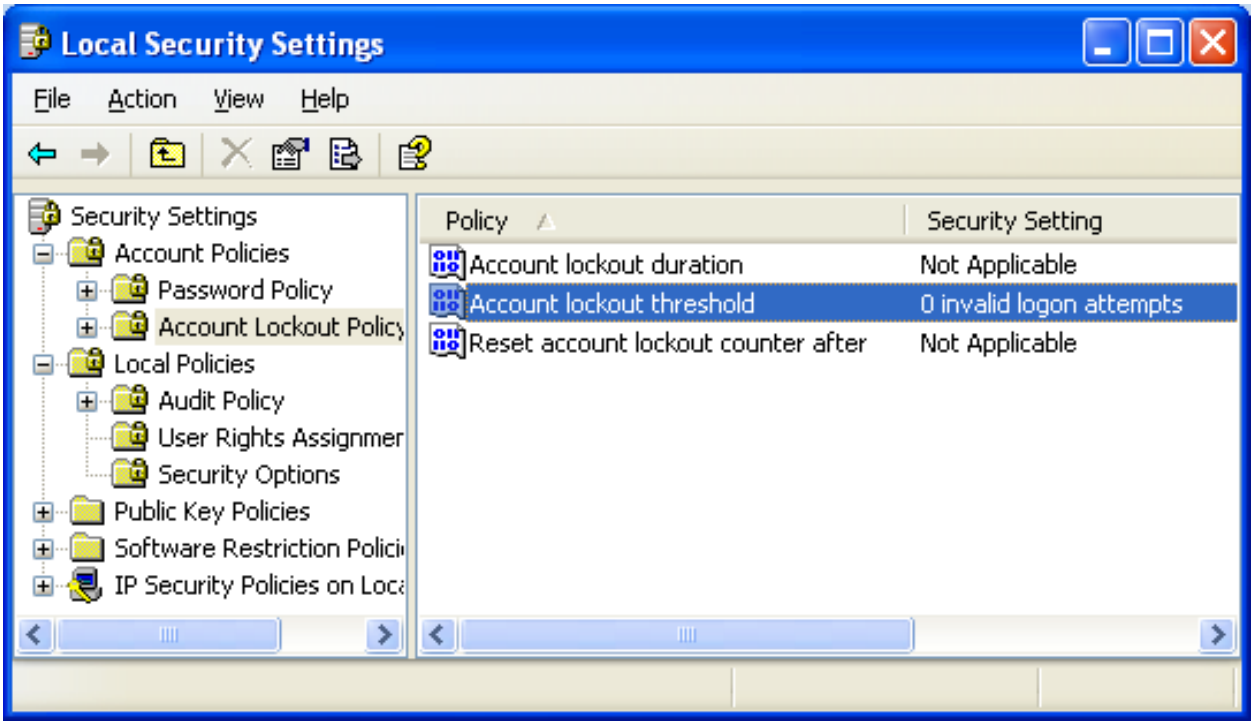
2. Các chính sách thiết lập thông qua Local Security Policy:

Password Policy: Qui định các chính sách về mật khẩu



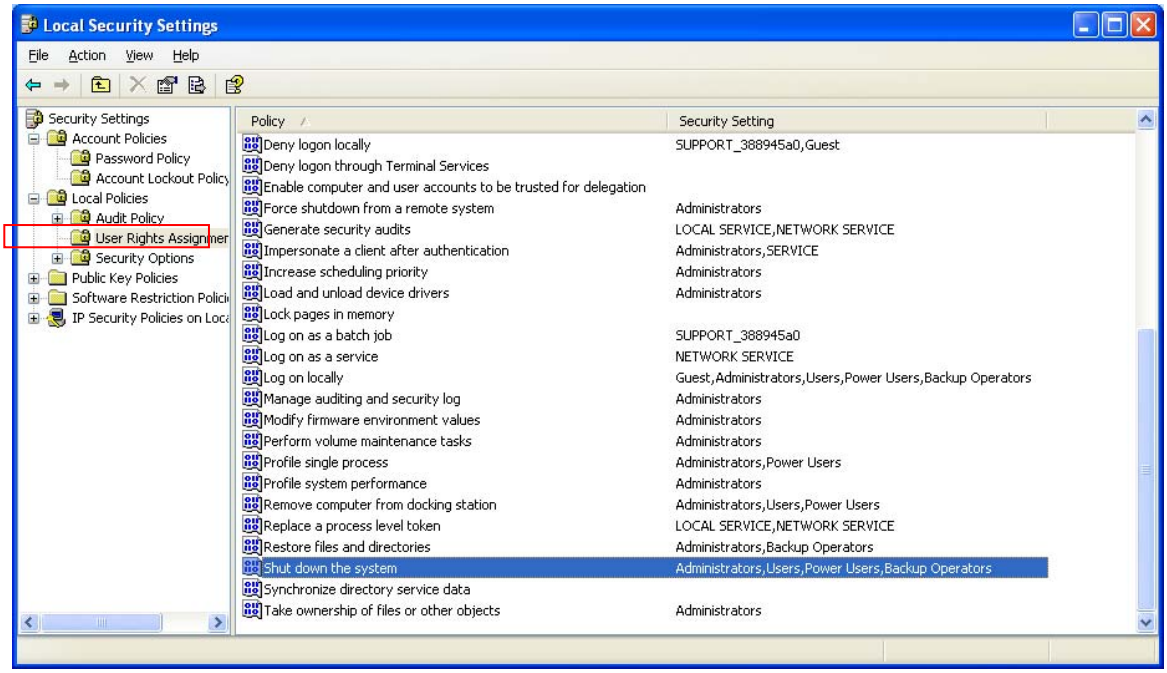
- Enforce password history: Sau bao nhiêu lần mới được lặp lại mật khẩu cũ, mặc định là 0 (không kiểm tra).
- Maximum password age: Thời gian tối đa một password được phép duy trì, sau thời gian này phải thay đổi password khác.
- Minimum password age: Sau bao lâu mới được tiếp tục thay đổi mật khẩu.
- Minimum password length: Password dài tối thiểu bao nhiêu ký tự
- Password must meet complexity … : Khởi động tính năng password mạnh (strong password: phải bao gồm 3 thành phần chữ hoa, thường và số).

Account Lockout Policy: Các chính sách về khóa tài khoản



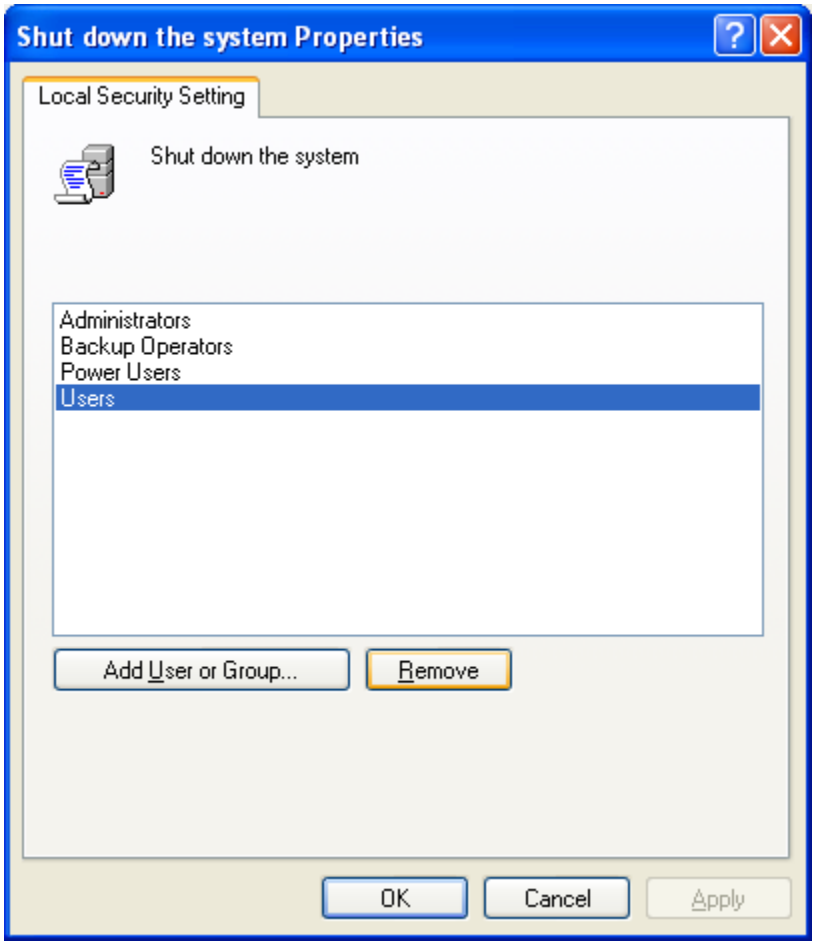
- Account lockout duration: Thời gian khóa tài khoản
- Account lockout threshold: Số lần nhập sai sau đó sẽ bắt đầu khóa tài khoản.
- Reset account lockout counter after : Sau bao lâu sẽ reset lại số lần nhập sai.

Các chính sách về User Rights Assignment: Quyền hạn người dùng



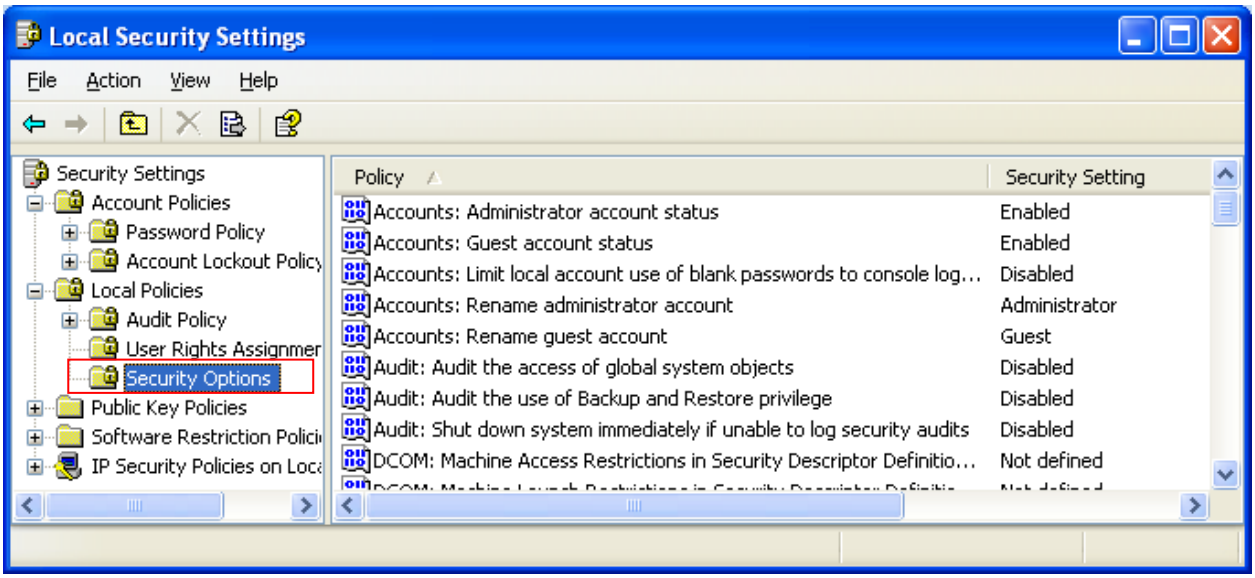
- Deny logon locally: Các user bị liệt kê trong mục này sẽ không được phép đăng nhập cục bộ vào máy. Chỉ được phép login từ xa thông qua các dịch vụ như chia sẻ file, ftp
- Logon locally: Ngược lại với mục trên, các users trong mục này sẽ được đăng nhập vào máy
- Shutdown the system: Mặc định có users thuộc các group Administrators, Users, Power Users, Backup Operators được phép tắt máy.

  Giả sử chúng ta muốn cấm nhóm Users tắt máy, ta double click và remove nhóm Users.



- Change system time: Các user được phép đổi giờ hệ thống trên máy

Security Option: Các chính sách khác về bảo mật



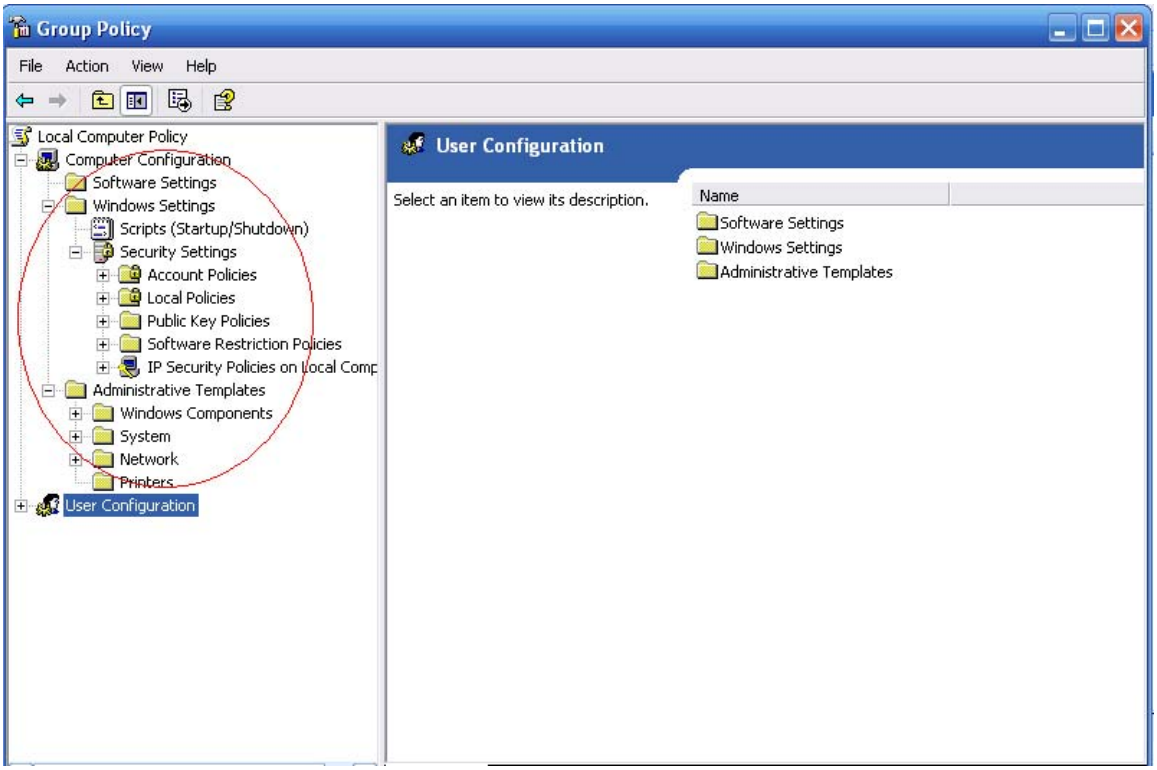
Có một số cấu hình đáng lưu ý trong mục này:

- Accounts: Administrator account status: qui định trạng thái của tài khoản administrator, vì một số lý do an toàn các hệ thống có thể disable tài khoản này.
- Accounts: Guest account status: trạng thái của tài khoản Guest
- Accounts: Rename administrator account : Đổi tên tài khoản administrator thành một tài khoản khác.
- Accounts: Rename guest account : Đổi tên tài khoản Guest thành một tài khoản khác
- Accounts: Limit local accounts use of blank passwords to console logon only: Không cho phép các tài khoản có password rỗng đăng nhập từ xa qua mạng
- Interactive logon: Do not display last username: Mặc định khi đăng nhập vào win, windows sẽ hiện một bảng thông báo cho người dùng nhập username và password. Windows tự động điền tên người đăng nhập cuối vào ô "username", mục này sẽ báo cho windows không hiện sẵn tên người dùng cuối cùng ở ô này
- Interactive logon: Do not require CTRL _ ALT _ DEL: không đòi hỏi phải ấn Ctrl Alt Del khi đăng nhập Windows
- Interactive logon: Prompt user to change password before expiration: Trước khi mật khẩu người dùng hết hạn bao nhiêu ngày sẽ cảnh báo người dùng

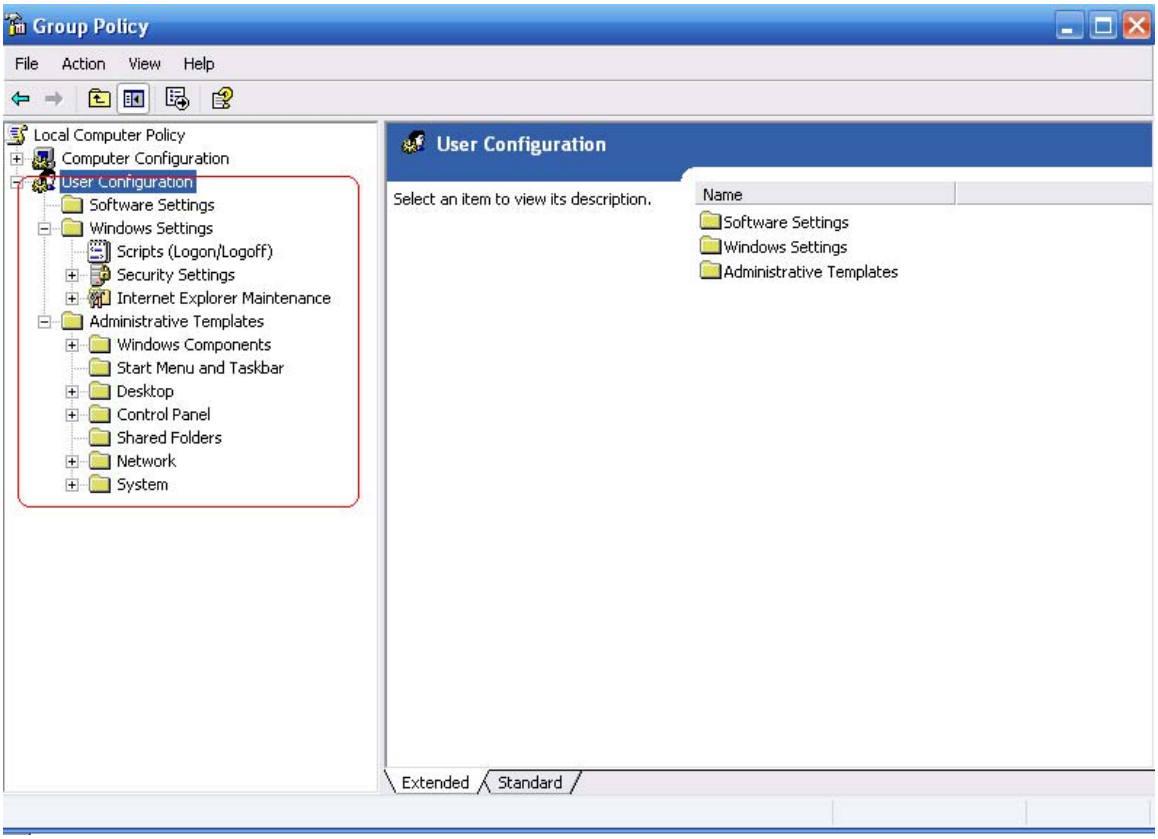
3. Các chính sách được thiết lập thông qua Group Policy:

Group Policy được chia làm 2 thành phần:

- Những thiết lập dành cho máy tính (Computer Configuration):



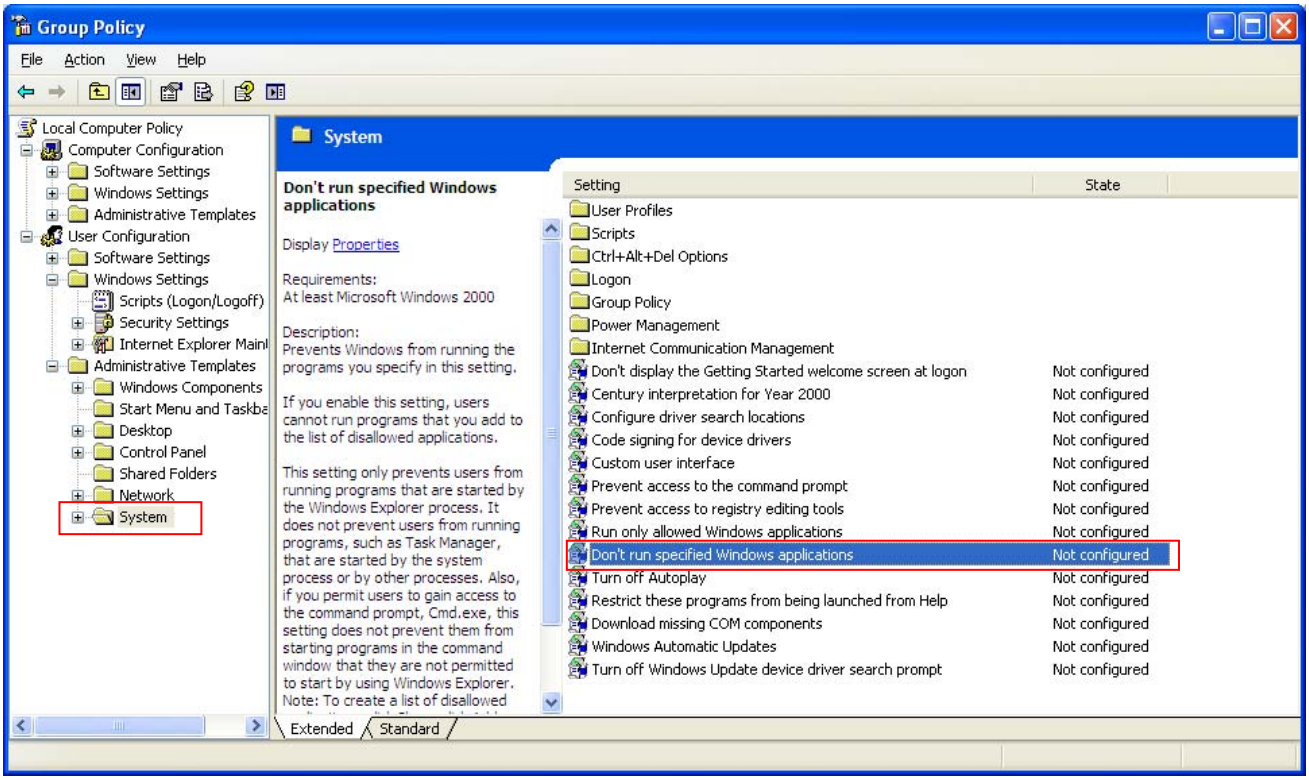
- Những thiết lập dành cho người dùng (User Configuration)



Hai mục này chỉ phân biệt rõ ràng khi đang áp dụng môi trường domain. Với môi trường workgroup, ta chỉ cần chỉnh sửa các chính sách cho người dùng (User Configuration) là đủ.

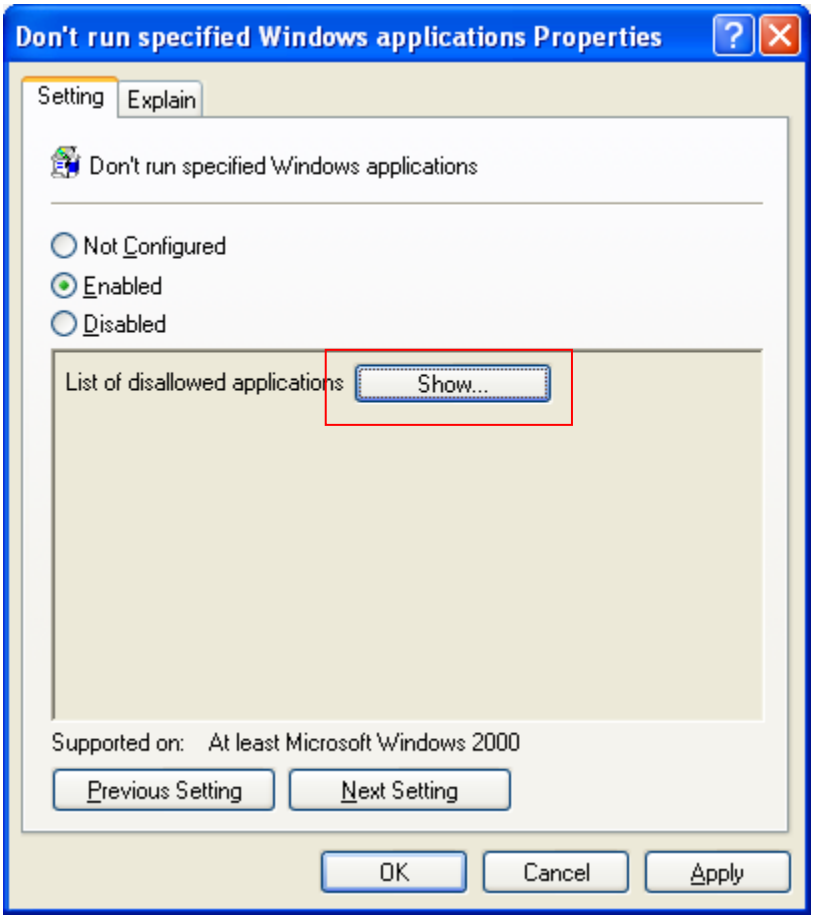
Một số chính sách tiêu biểu:

- Không cho phép người dùng mở ứng dụng Notepad (hoặc bất kỳ ứng dụng nào khác)



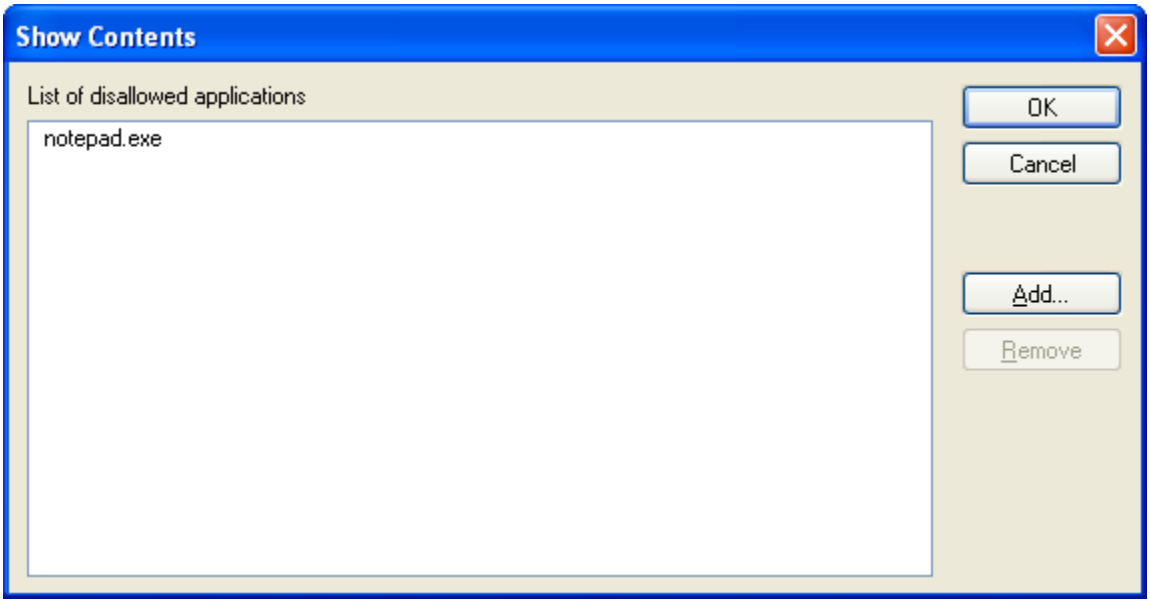
Tìm mục Don't run specified Windows applications như hình trên

Bổ sung Notepad.exe



Chọn phím Show…

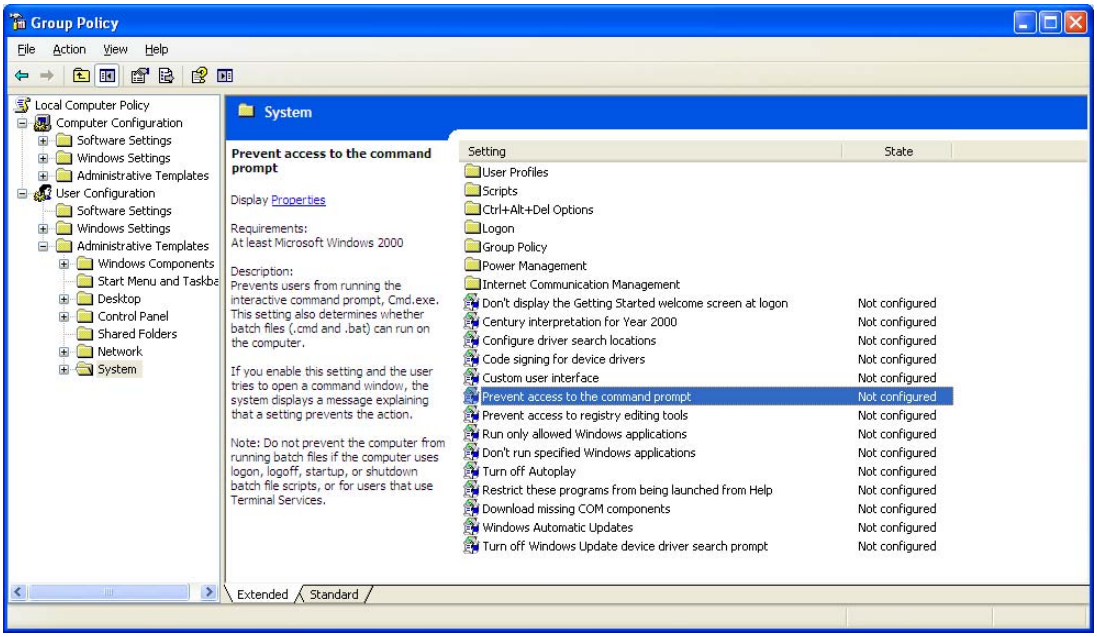
Bổ sung Notepad.exe



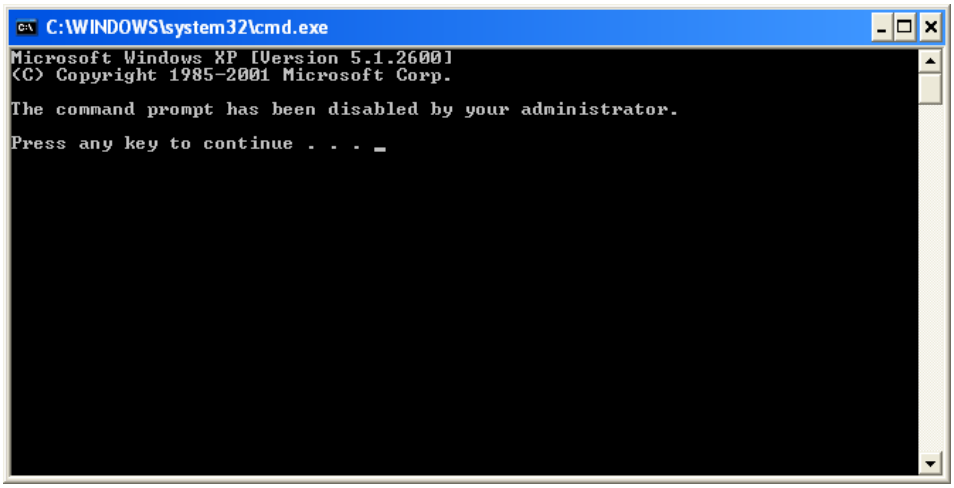
Sau đó các bạn có thể mở notepad và cho biết kết quả.

Tương tự cho winword.exe, excel.exe và các ứng dụng khác.

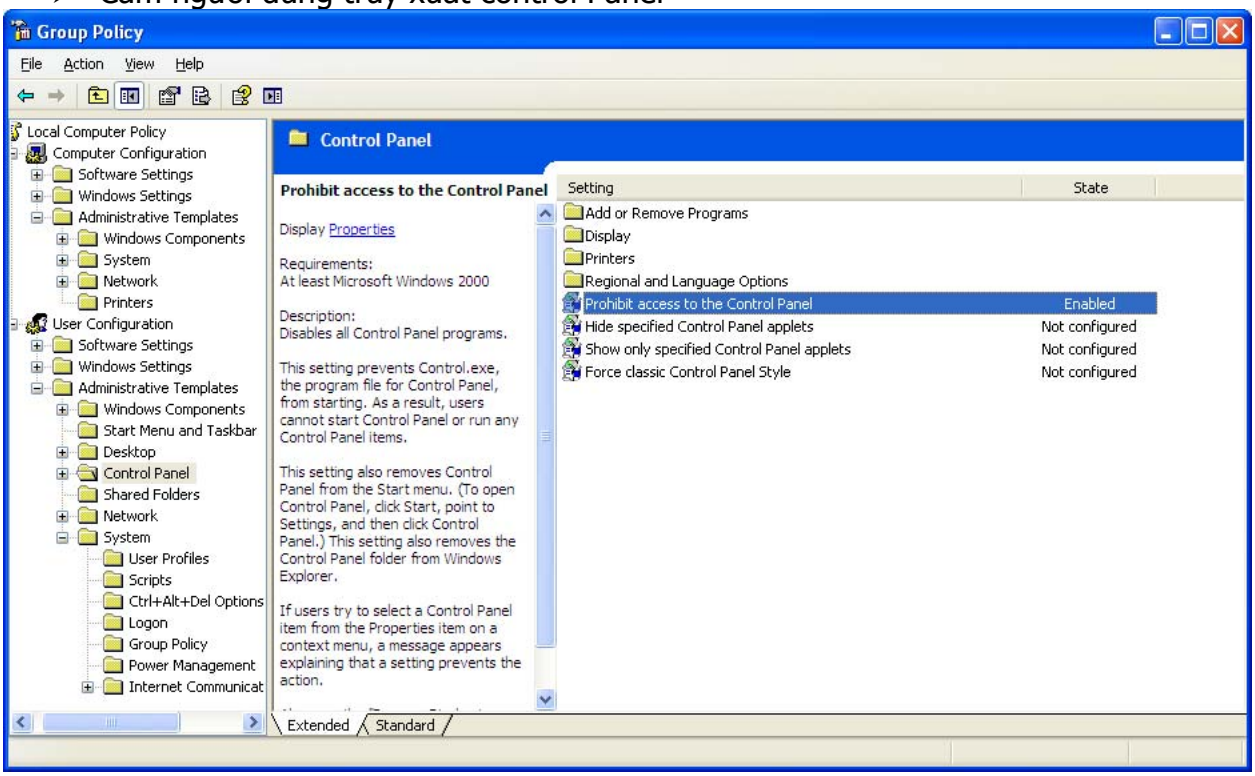
- Prevent access to the command prompt: Không cho phép truy xuất cmd từ Windows



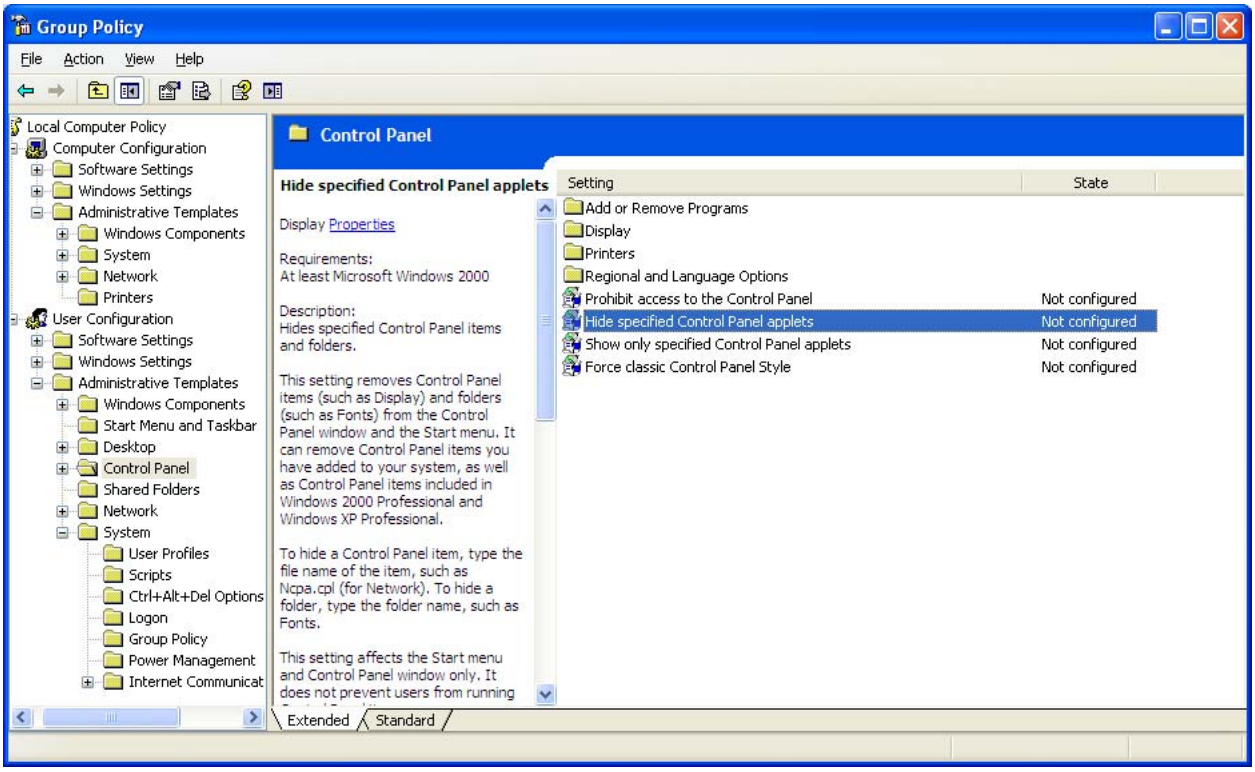
Khi truy xuất command promt



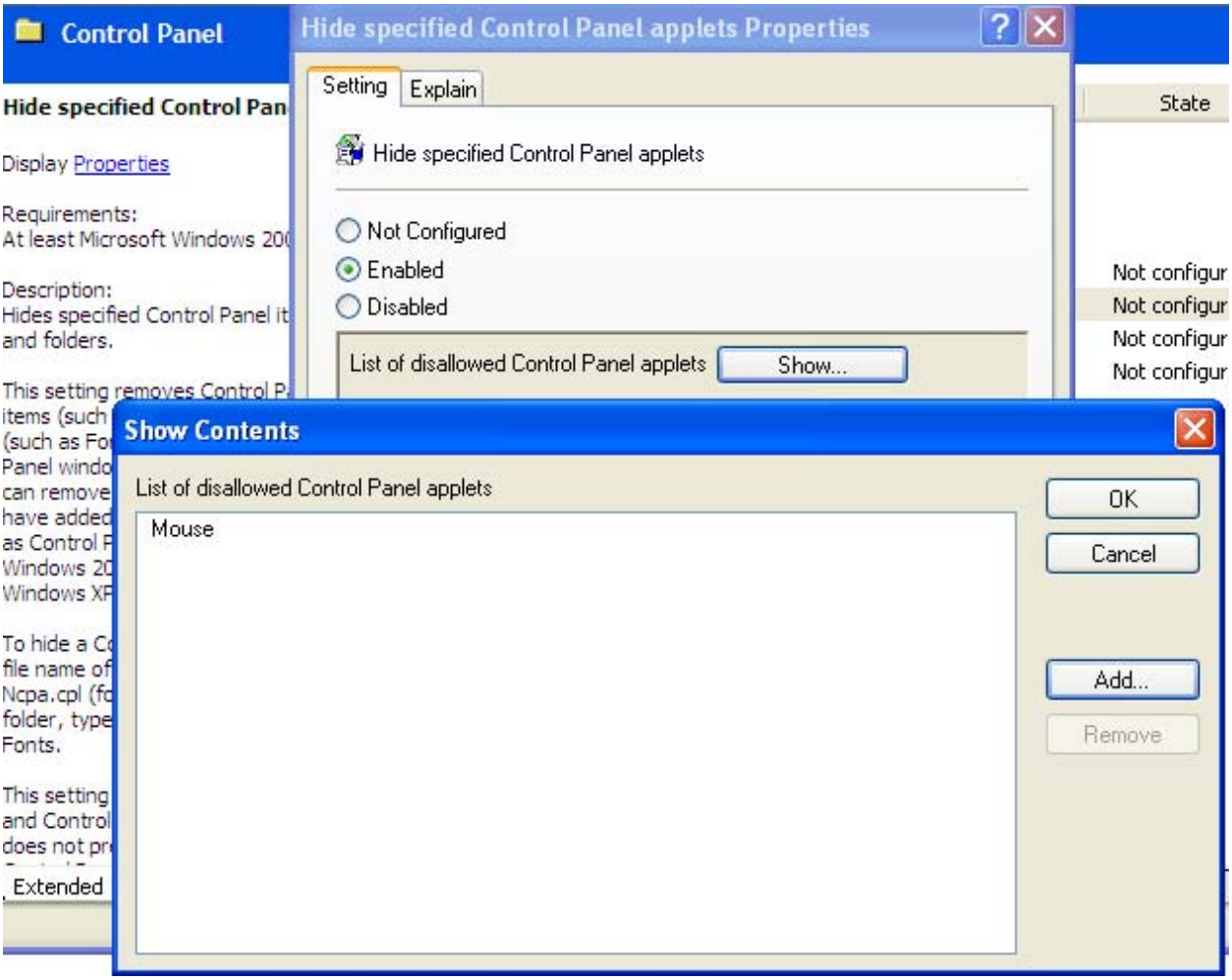
- Cấm người dùng truy xuất control Panel



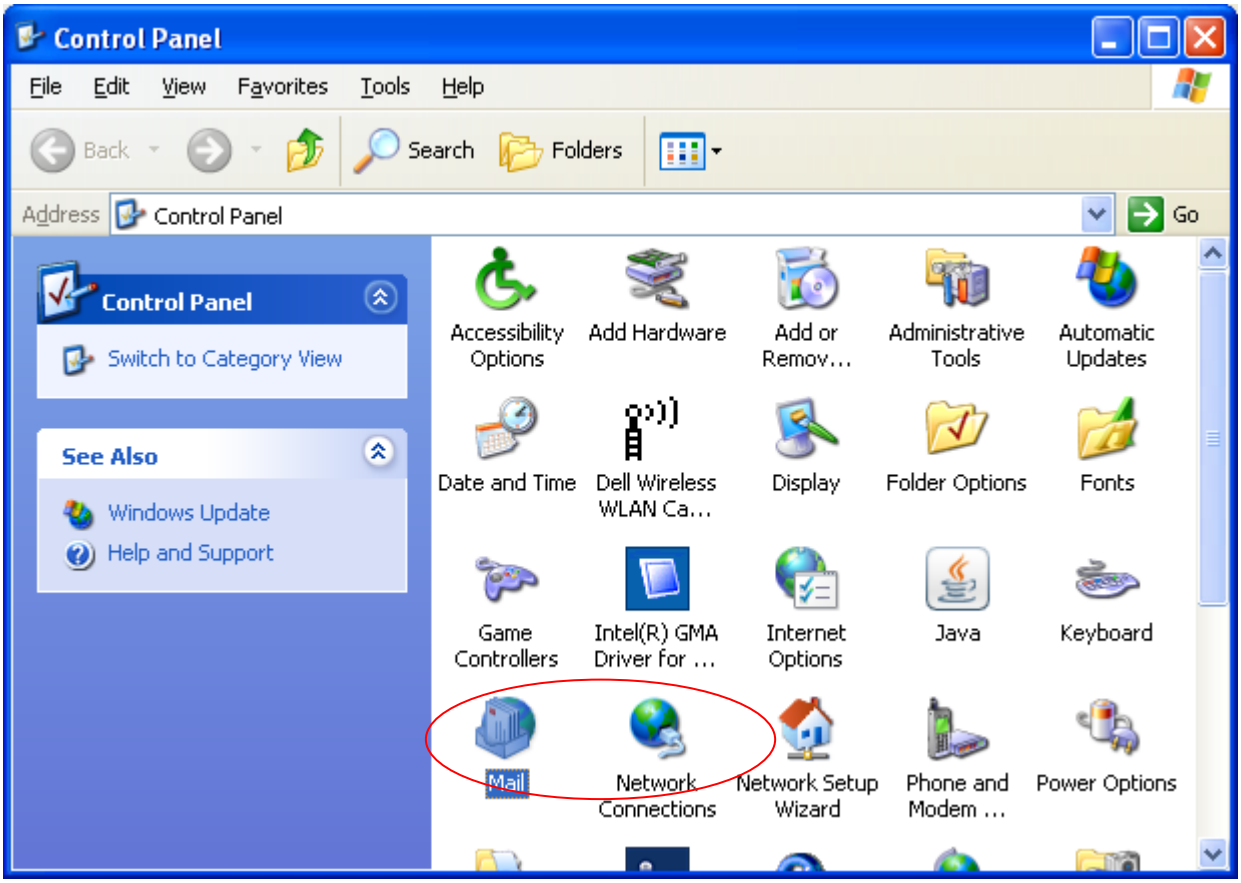
- Không cho người dùng truy xuất một số thành phần trong control panel, ví dụ như Mouse



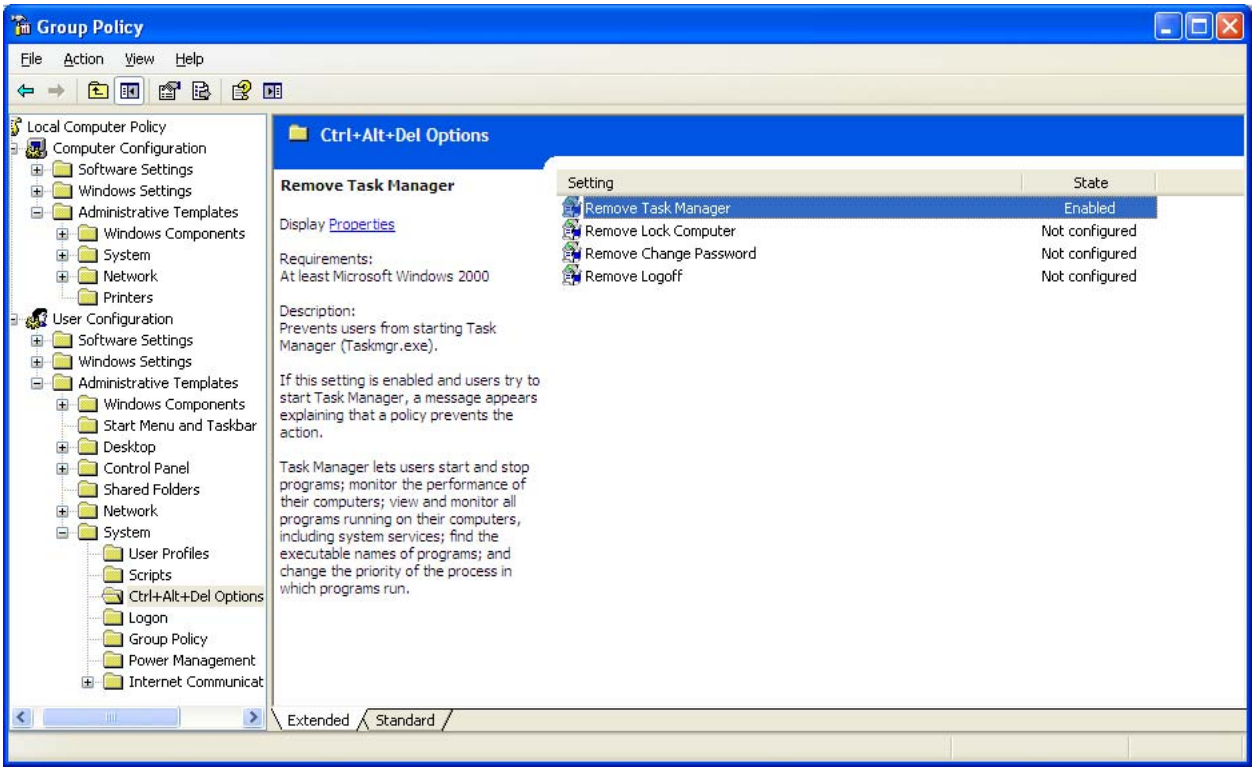
Bổ sung mục Mouse:



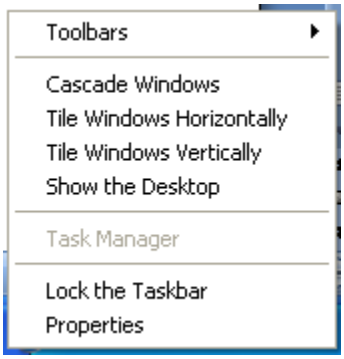
Khi vào Control Panel sẽ không thấy mục MOUSE:



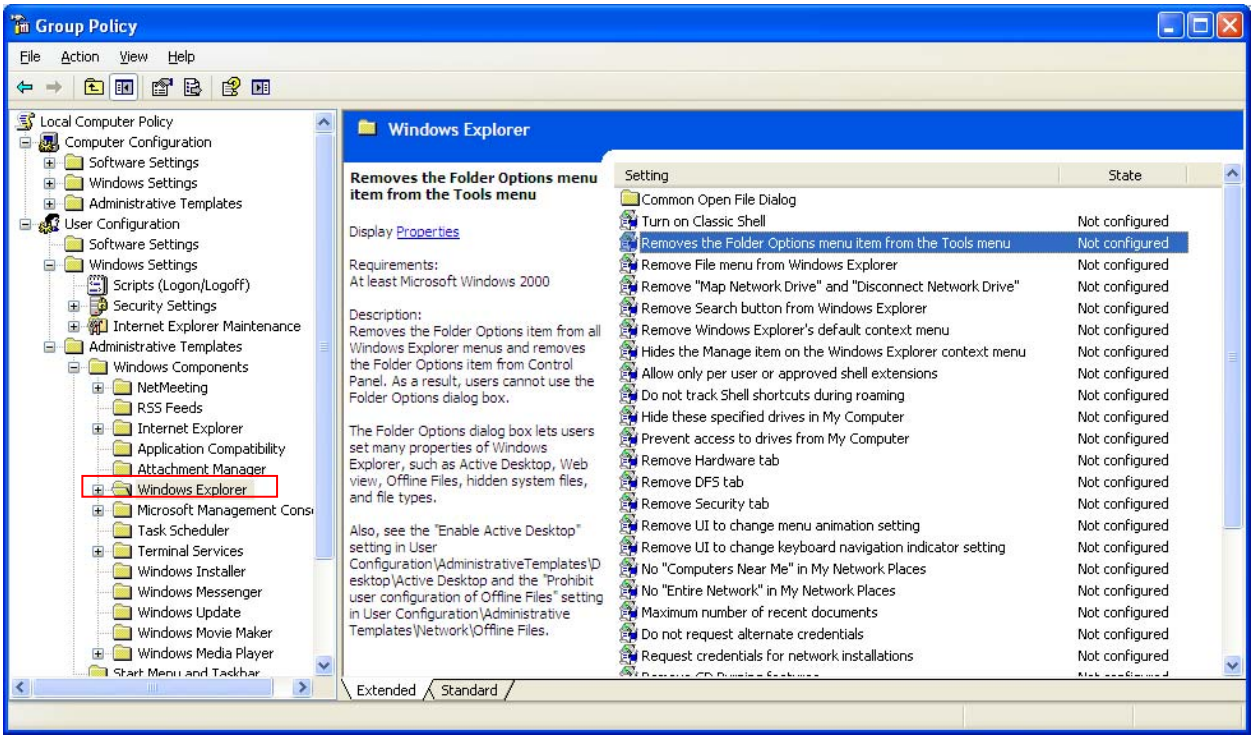
- Không cho truy xuất Task Manager



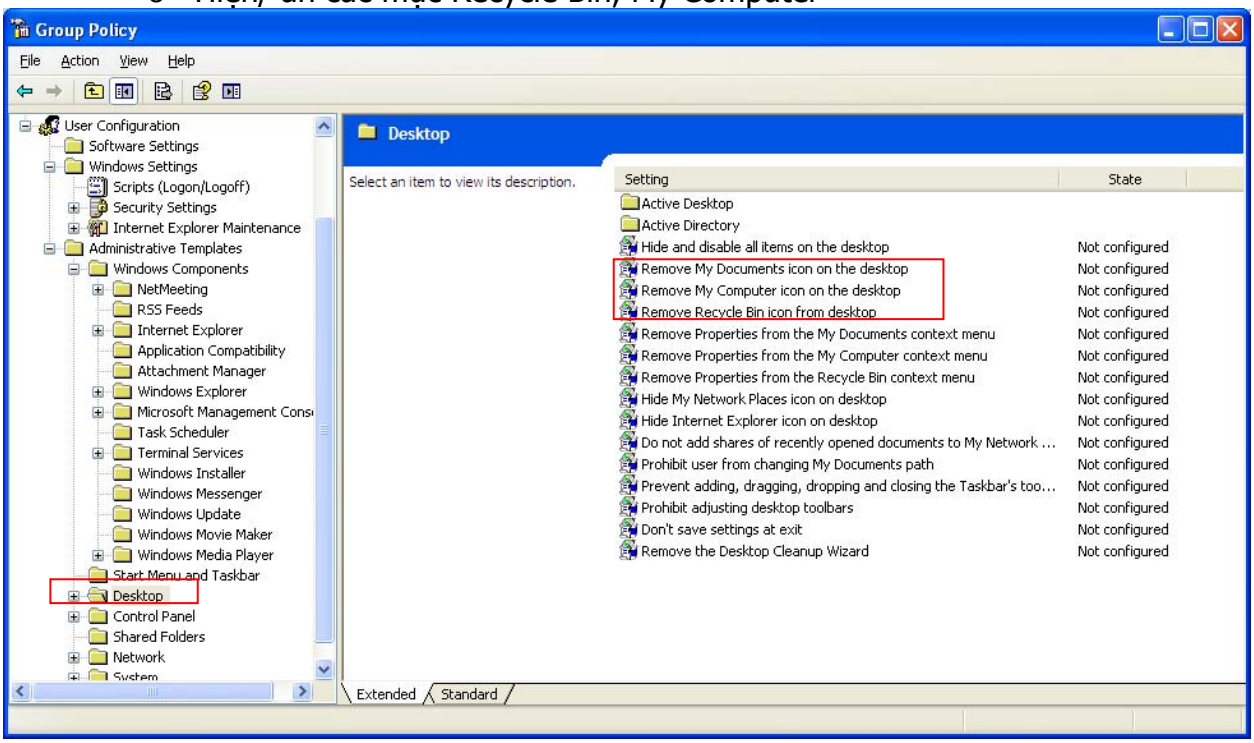
Menu Task Manager bị mờ



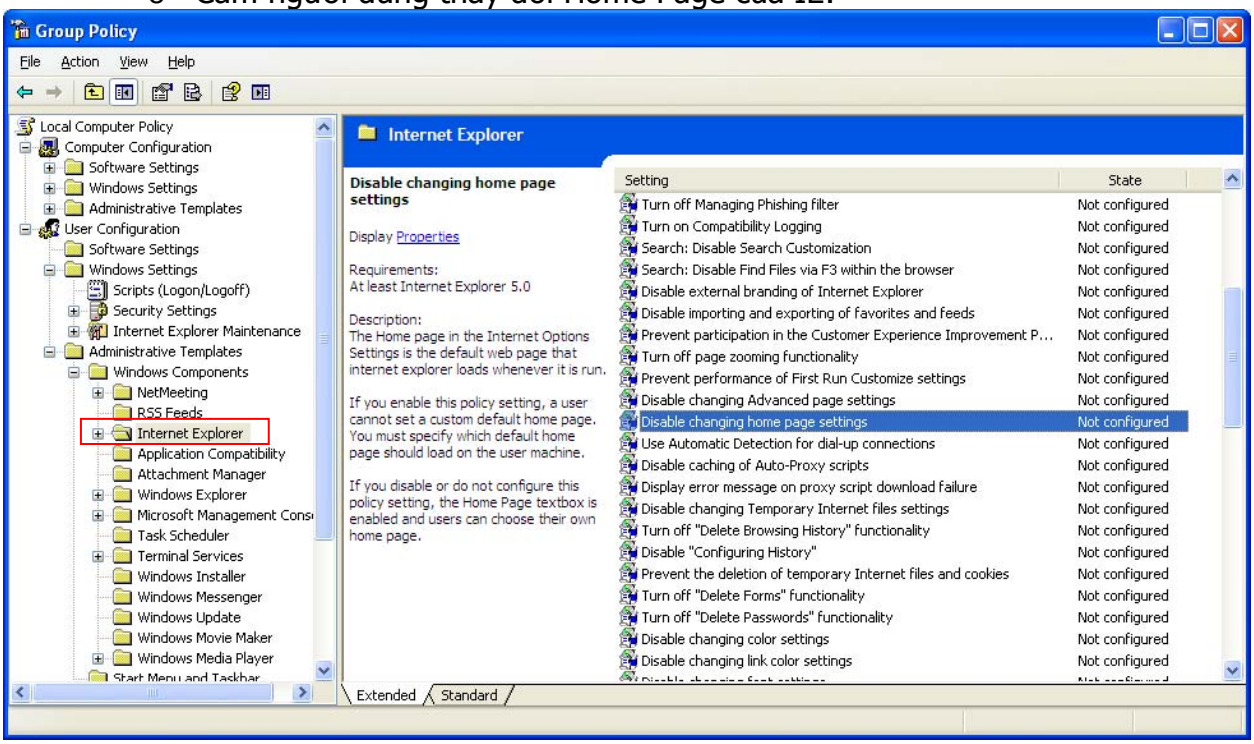
- Quản lý một số chương trình thông dụng:
  - Tắt mục Folder Option trong Windows Explorer



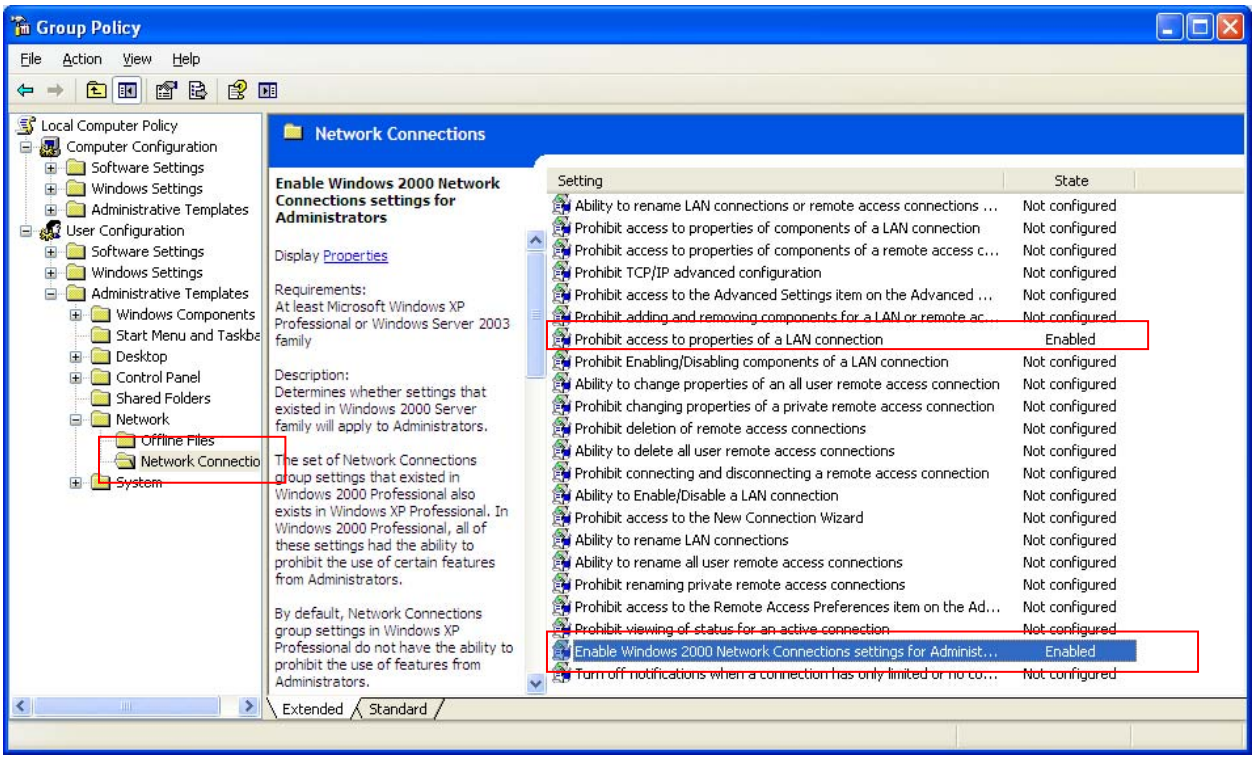
- Hiện/ ẩn các mục Recycle Bin, My Computer



- Cấm người dùng thay đổi Home Page của IE:



- Cấm người dùng thay đổi thông số card mạng:



Nếu chỉ chọn mục này, chỉ người dùng thông thường bị cấm. Nếu muốn cấm cả user administrator, ta phải enable mục "Enable Windows 2000 Network Connections settings for Administrators

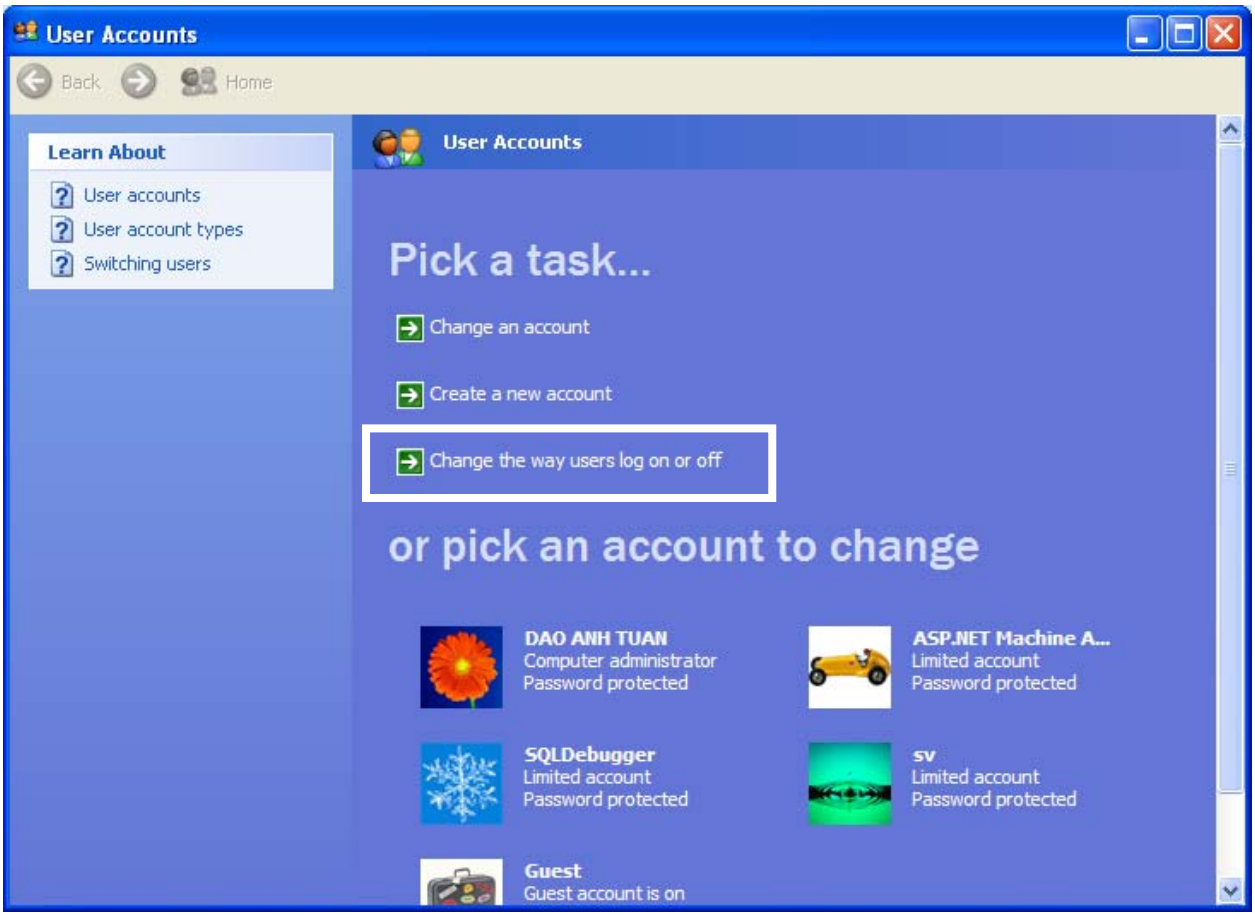
Với môi trường domain, sau khi thay đổi giá trị group policy cần thực thi câu lệnh

gpupdate /force để lan truyền thay đổi đến các máy khác.

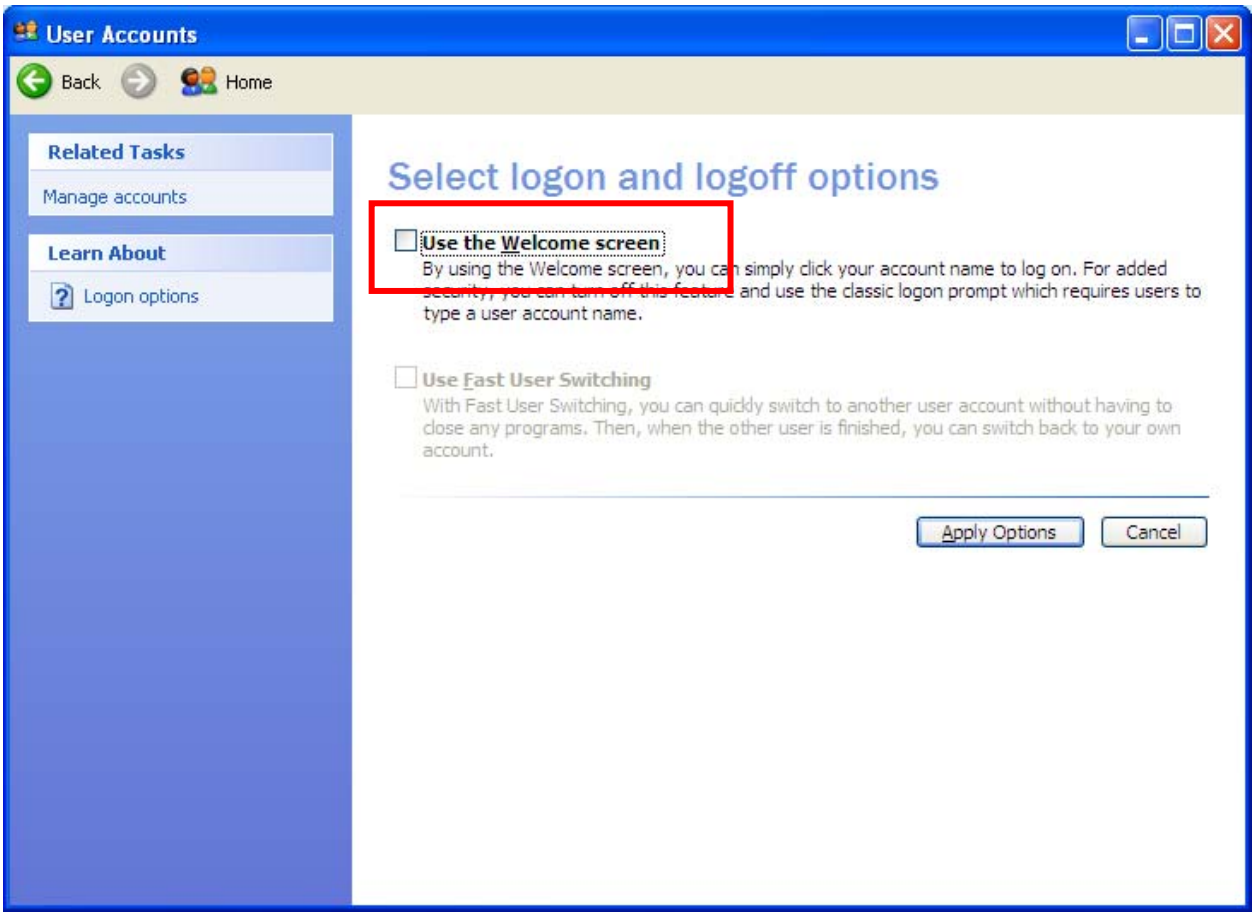
4. Thay đổi cách login của User Windows XP

Thông thường, khi đăng nhập Windows XP sẽ hiện danh sách các user cho người dùng click chuột và chọn. Ta có thể đổi về kiểu login truyền thống (người dùng phải nhập username và password) bằng cách vào Control Panel, mục User Accounts

Tìm mục Change the way user logon or off



Sau đó un-check mục Use Welcome Screen:



Bài tập:

1. Tắt chức năng yêu cầu phải nhấn tổ hợp Ctrl Alt Del khi khởi động hệ thống
2. Không hiển thị username của người dùng đăng nhập hệ thống lần gần nhất
3. Đối với Windows XP, không cho hiện tất cả người dùng đang có trong hệ thống mà hiện màn hình Logon (yêu cầu nhập Username, password)
4. Nếu người dùng nhập sai password 3 lần sẽ bị khóa tài khoản
5. Cấm người dùng chạy Word và Excel
6. Bắt buộc tất cả người dùng phải thay đổi password sau 10 ngày, password dài ít nhất 8 ký tự và phải bao gồm chữ hoa, chữ thường, số.
7. Cài đặt home page mặc định cho IE là http://vnexpress.net, không cho thay đổi Home Page mặc định
8. Không cho phép người dùng thay đổi thông số card mạng
9. Không cho người dùng truy xuất command promt, control panel
10. Tắt tính năng Task Manager của Windows
11. Không cho hiện My Computer và My Documents ra màn hình