HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 3.
Bảo mật cơ bản trên Window 7

Học phần: BẢO ĐẢM VÀ AN TOÀN THÔNG TIN

NỘI DUNG

Bài 1: Tìm hiểu User Account Control (UAC)
Bài 2: Thiết lập chính sách cho Password (Password Policy)
Bài 3: Phòng chống dò Password, hạn chế số lần nhập sai Password
Bài 4: Thiết lập chính sách hạn chế quyền thực thi ứng dụng cụ thể với người dùng
Bài 5: Cấu hình chính sách Audit và Event Log của Windows.

Bài 1: Tìm hiểu User Account Control (UAC)

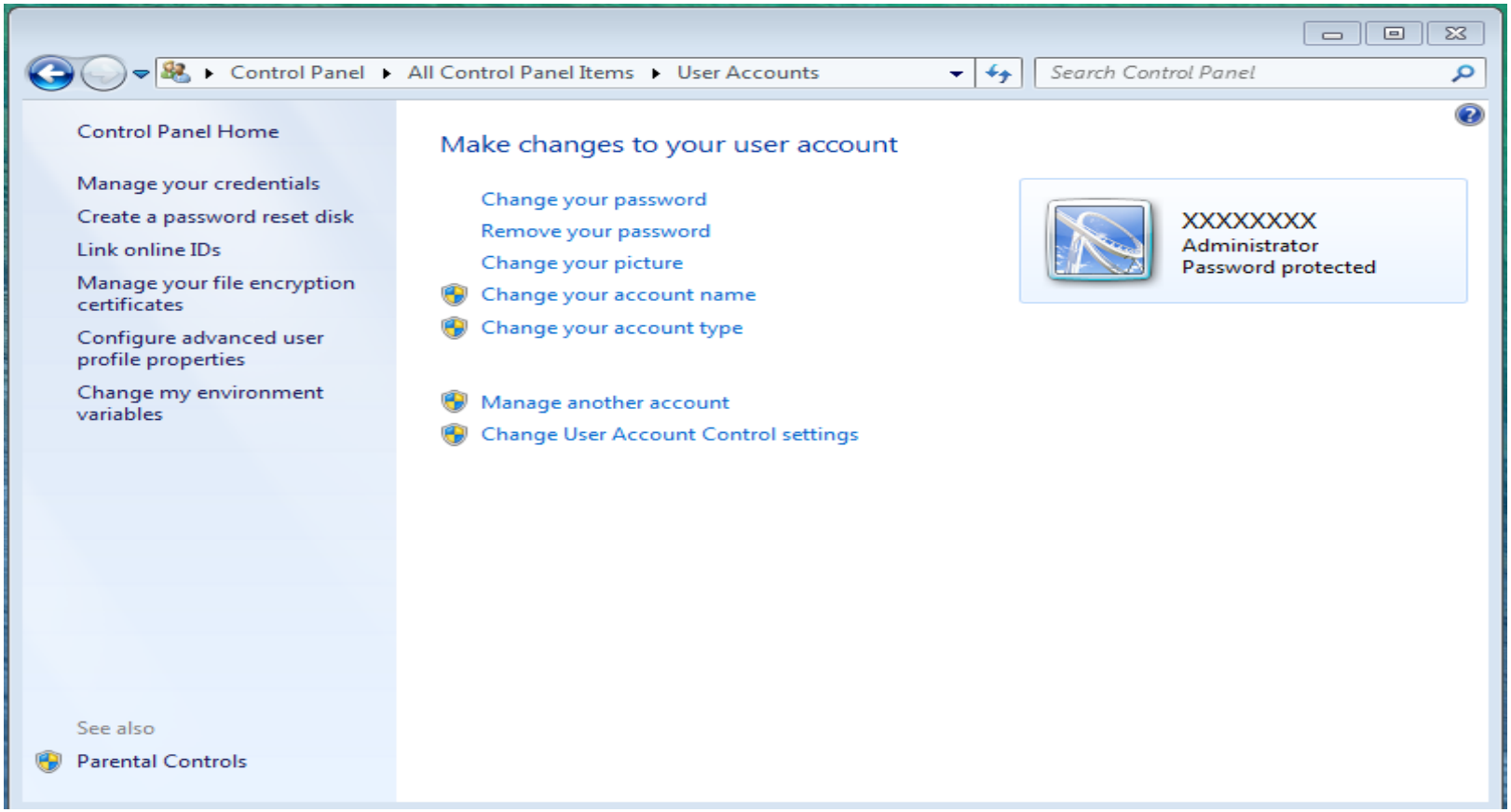
Trong Windows 7 những chương trình có hành động can thiệp sâu vào hệ thống như thay đổi giao diện, yêu cầu sử dụng chung các thư viện *.DLL của hệ thống, cài thêm phần mềm mới... UAC sẽ hiển thị và yêu cầu sự xác nhận của người sử dụng:

Giao diện chính của UAC trong Windows 7

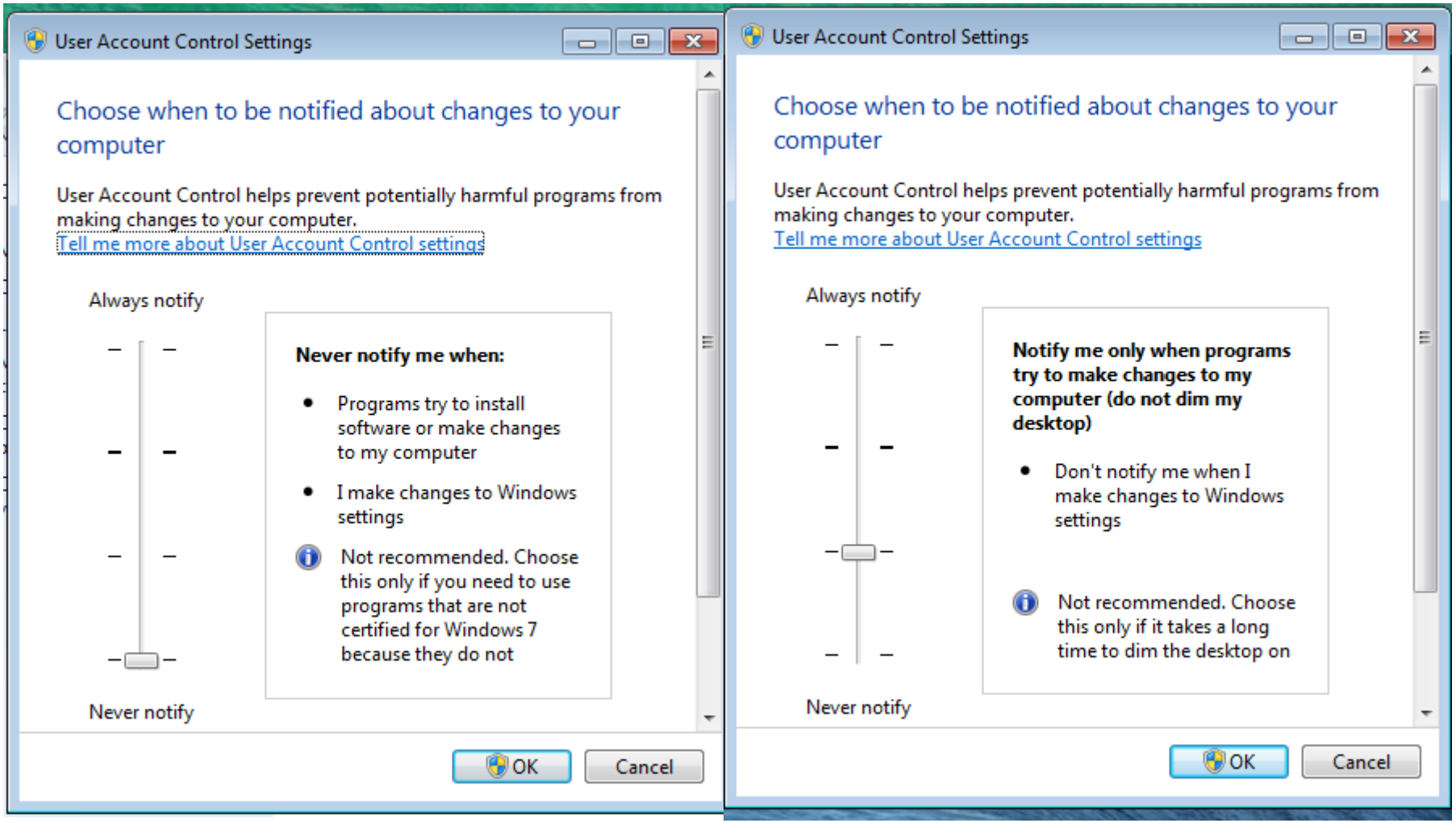
Bài 1: Tìm hiểu User Account Control (UAC)

Cách sử dụng: vào window ->control panel->User Acount

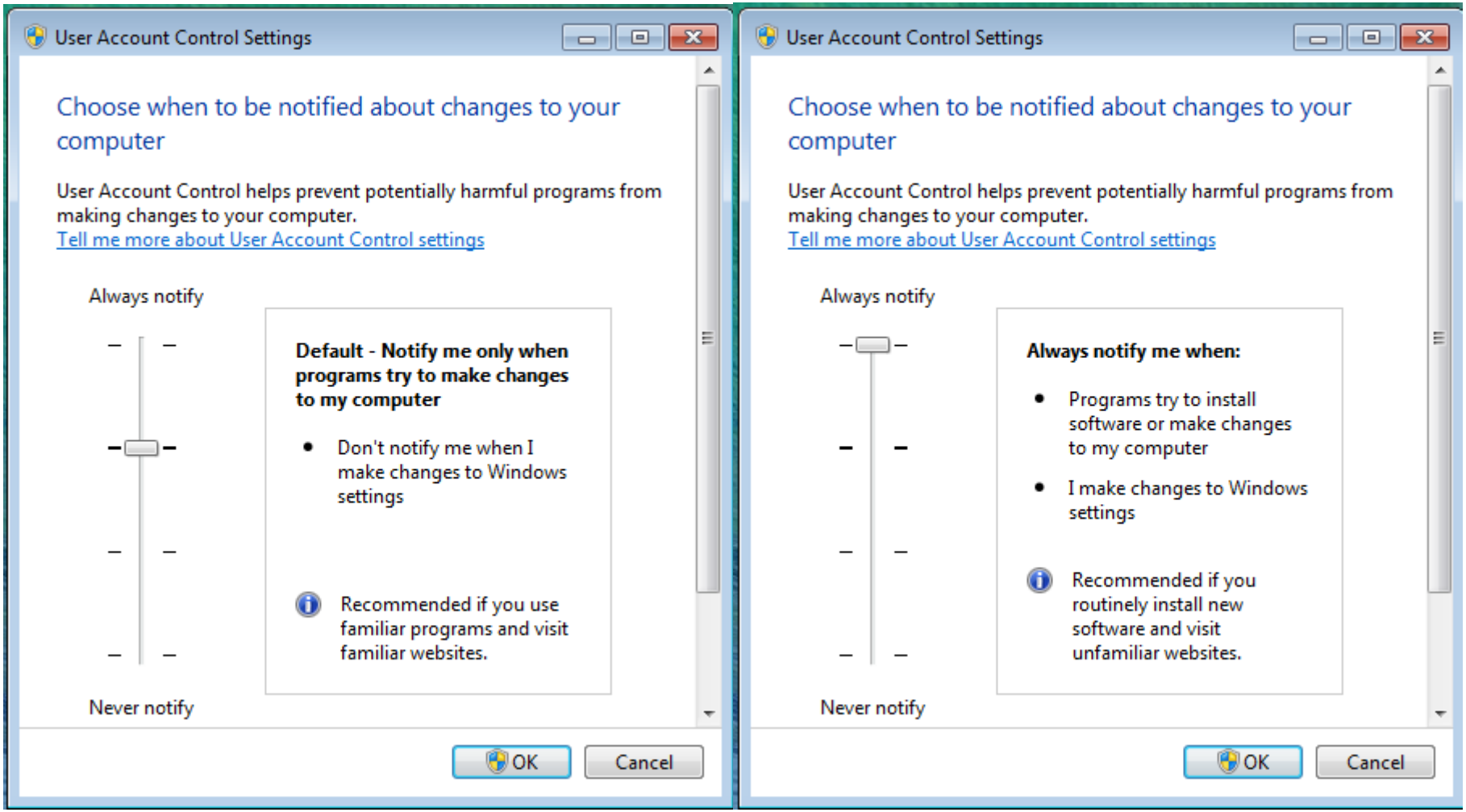
→ Change user account setting



Bài 1: Tìm hiểu User Account Control (UAC)



Bài 1: Tìm hiểu User Account Control (UAC)



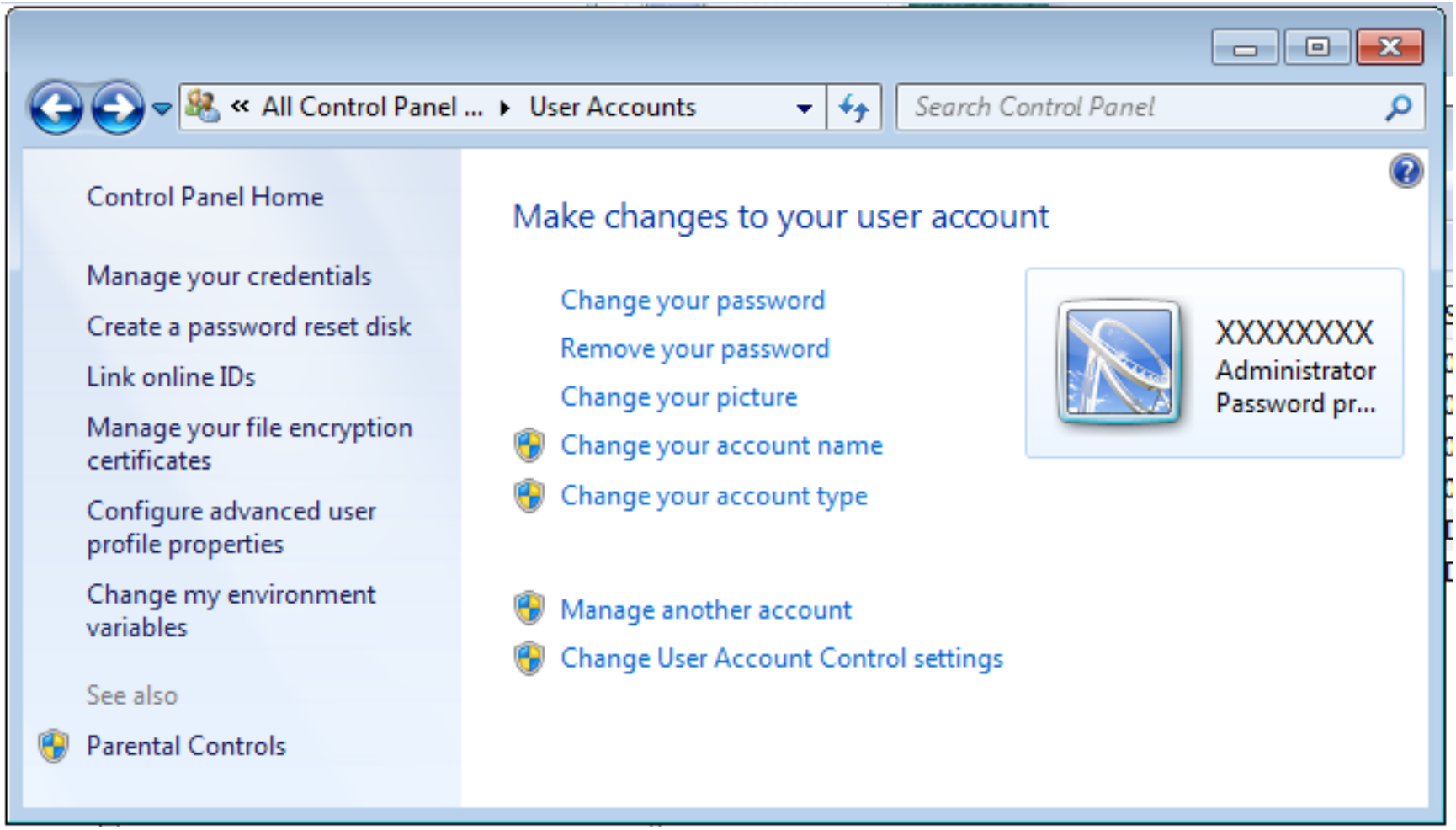
Bài 2: Thiết lập chính sách cho Password

- Sử dụng mật khẩu yếu.

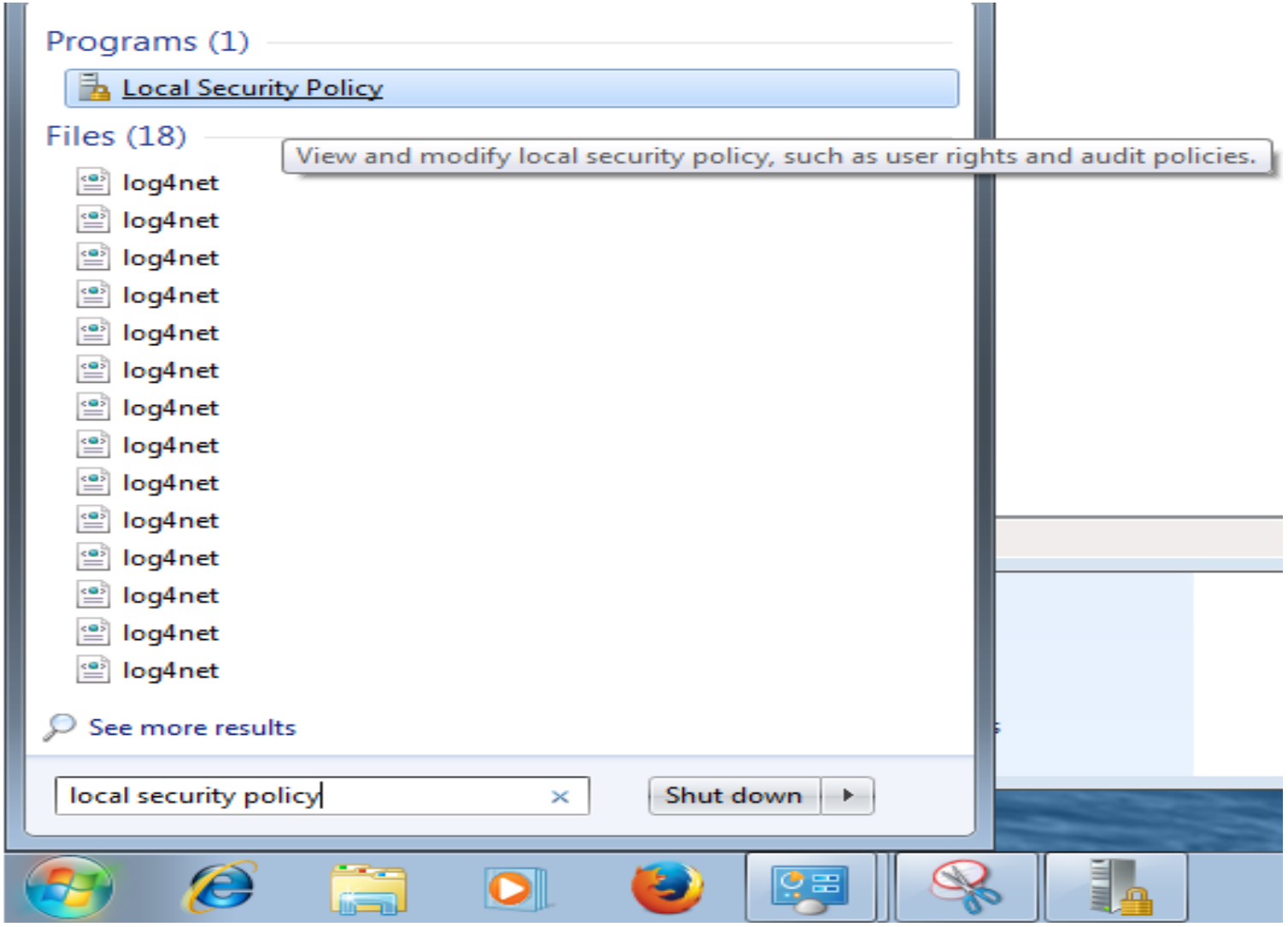
- Không thay đổi mật khẩu theo định kỳ.

- Dùng lại những mật khẩu cũ khi hệ thống yêu cầu đổi mật khẩu.

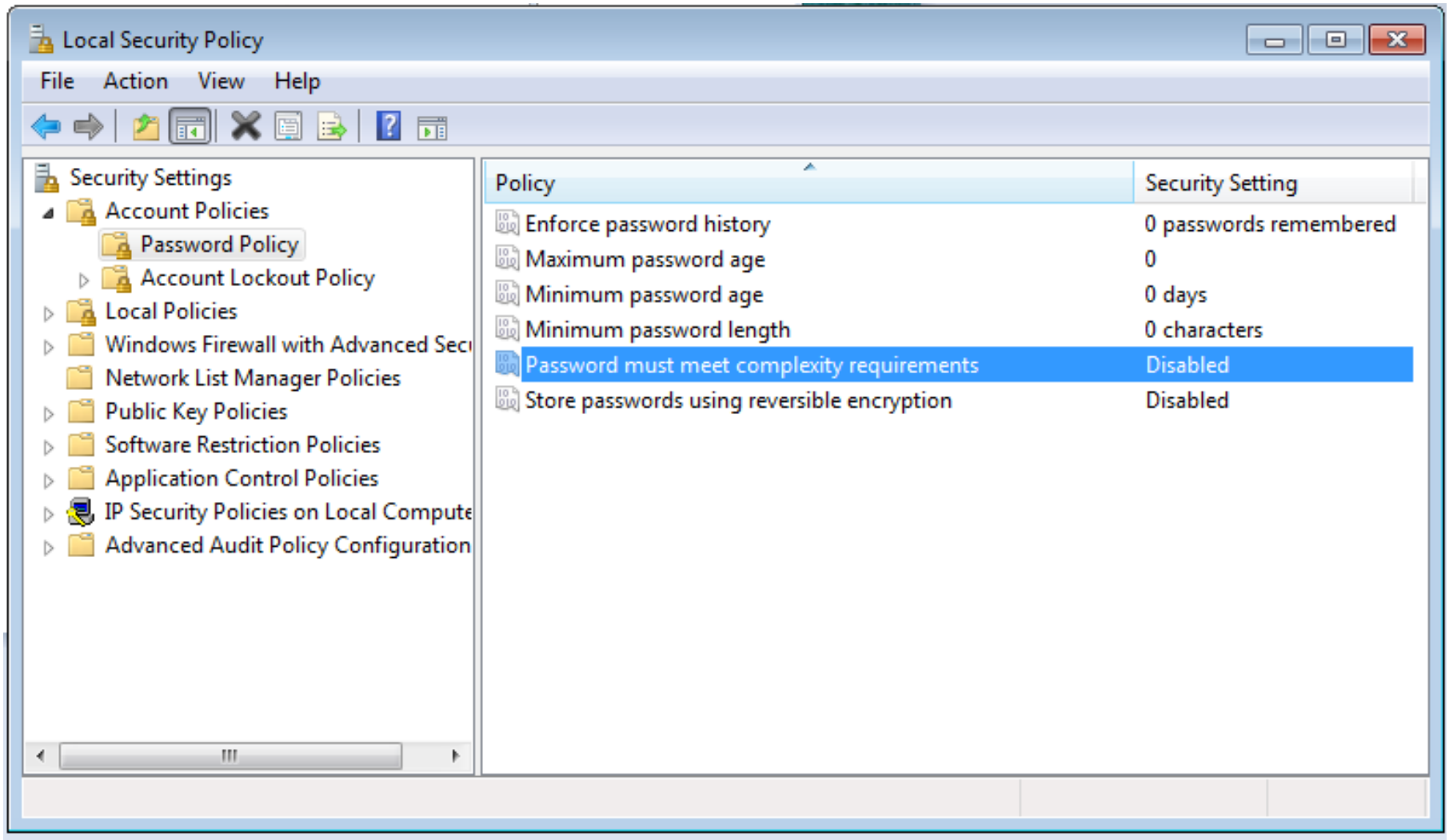
Bài 2: Thiết lập chính sách cho Password



Bài 2: Thiết lập chính sách cho Password



Bài 2: Thiết lập chính sách cho Password



Bài 2: Thiết lập chính sách cho Password

Cấu hình bằng lệnh

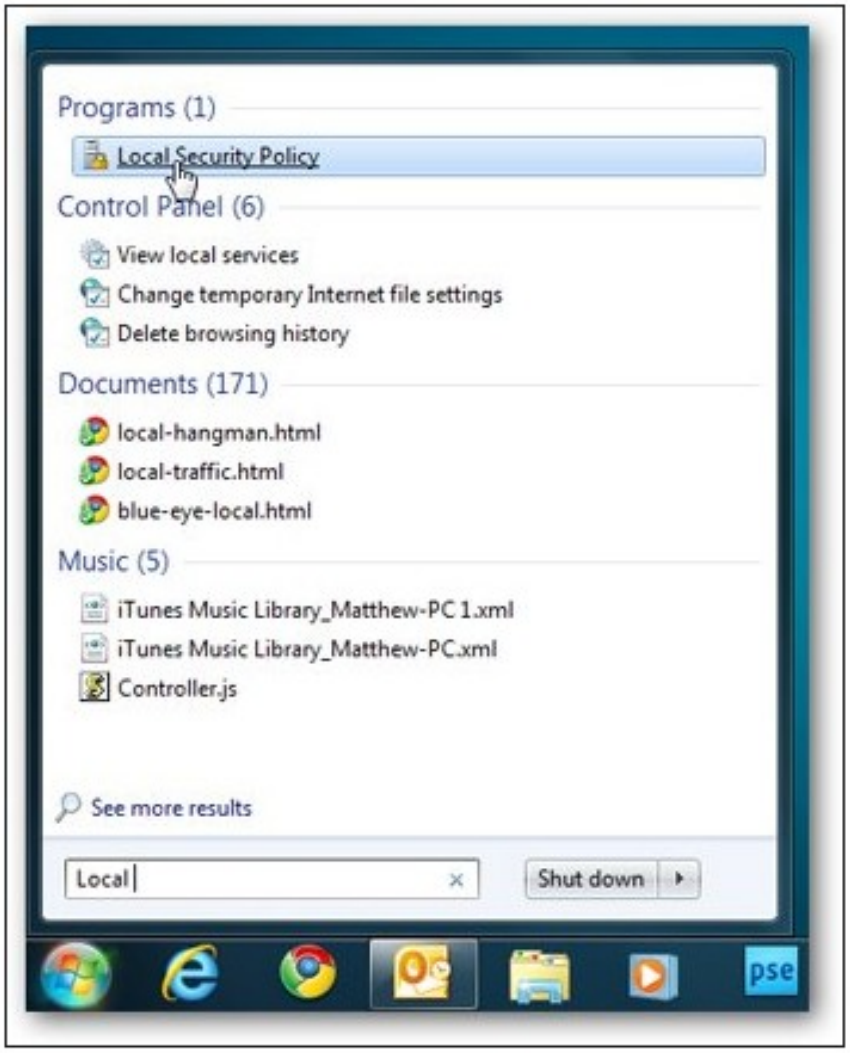
B1 - bật cmd

B2 - gõ lệnh

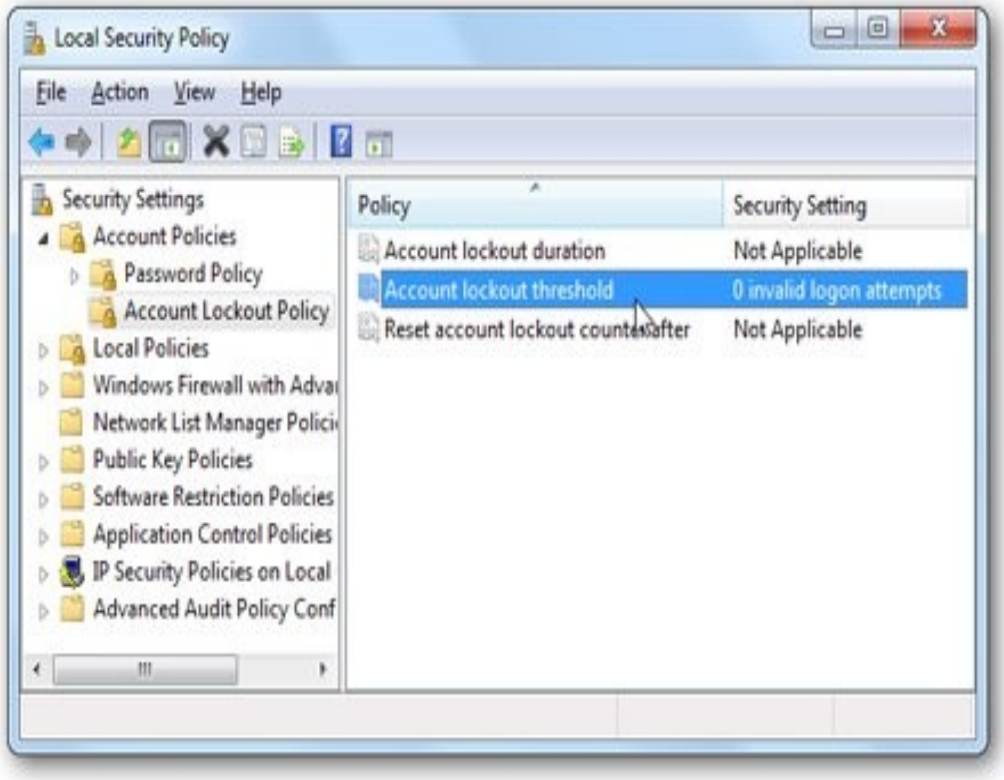
- net accounts /minpwlen:length // chiều dài tối thiểu của mật khẩu
- net accounts /maxpwage:days // số ngày tối đa phải thay đổi mật khẩu
- net accounts *minpwage:days* // số ngày tối đa phải thay đổi mật khẩu
- ...

Bài 3: Phòng chống dò Password, hạn chế số lần nhập sai Password

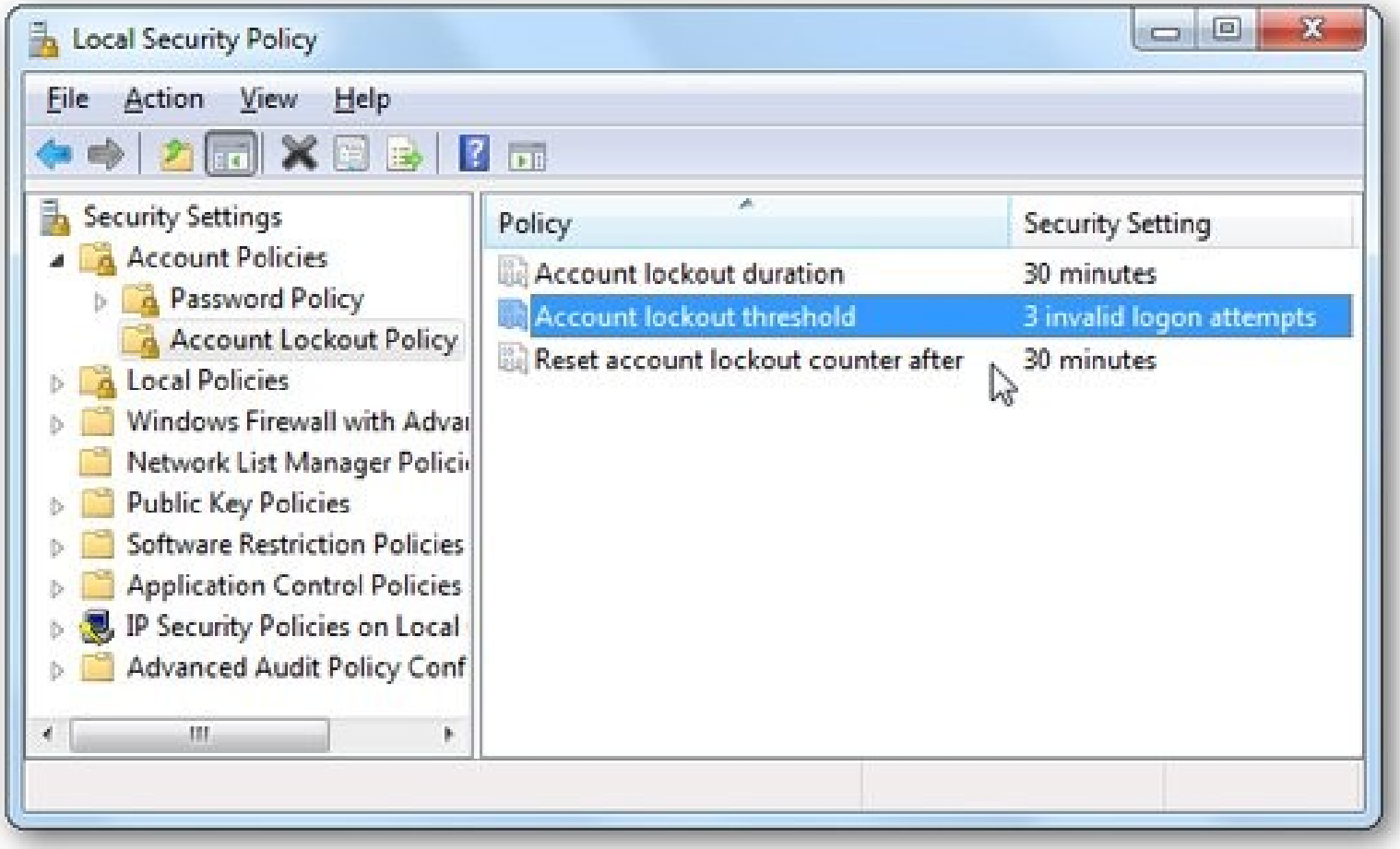
- Là phương pháp để khóa tất cả các tài khoản sử dụng trong thời gian cài đặt trước khi mật khẩu được nhập **N** lần mà không chính xác



Bài 3: Phòng chống dò Password, hạn chế số lần nhập sai Password



Bài 3: Phòng chống dò Password, hạn chế số lần nhập sai Password



Bài 3: Phòng chống dò Password, hạn chế số lần nhập sai Password

Cấu hình bằng lệnh

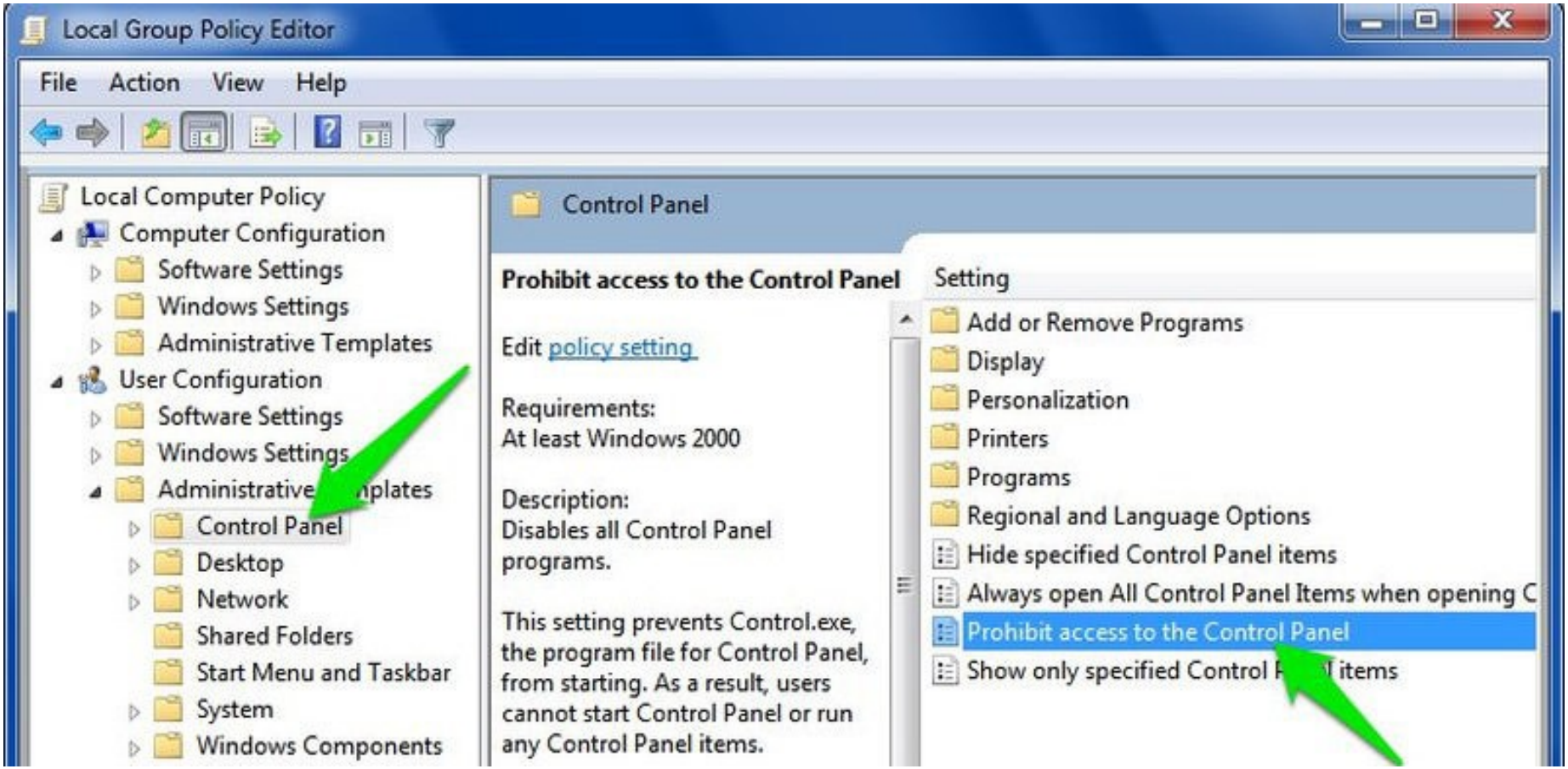
B1 - bật cmd

B2 - gõ lệnh

- net accounts
- net accounts /lockoutthreshold:3
- net accounts /lockoutduration:30
- net accounts /lockoutwindow:30
- net accounts

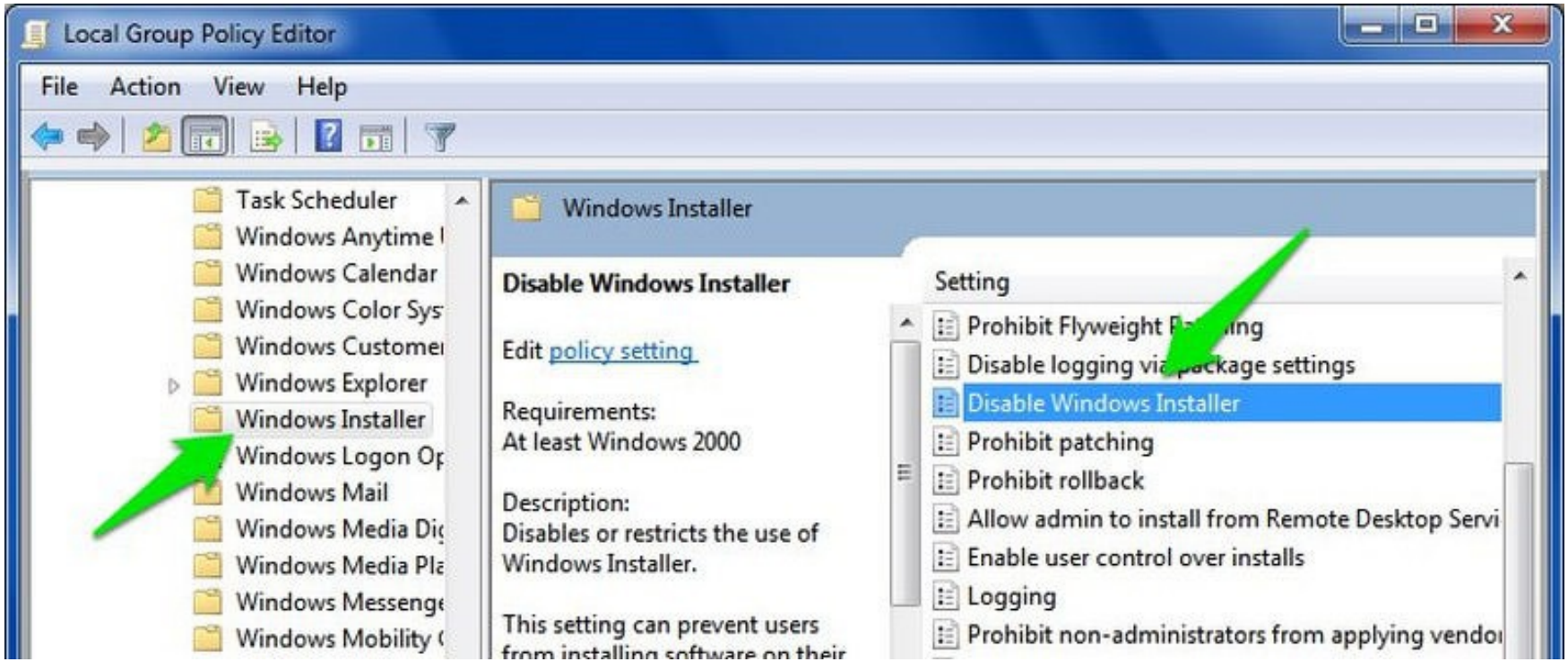
Bài 4: Thiết lập chính sách hạn chế quyền thực thi ứng dụng cụ thể với người dùng

1. Cấm truy cập vào Control Panel



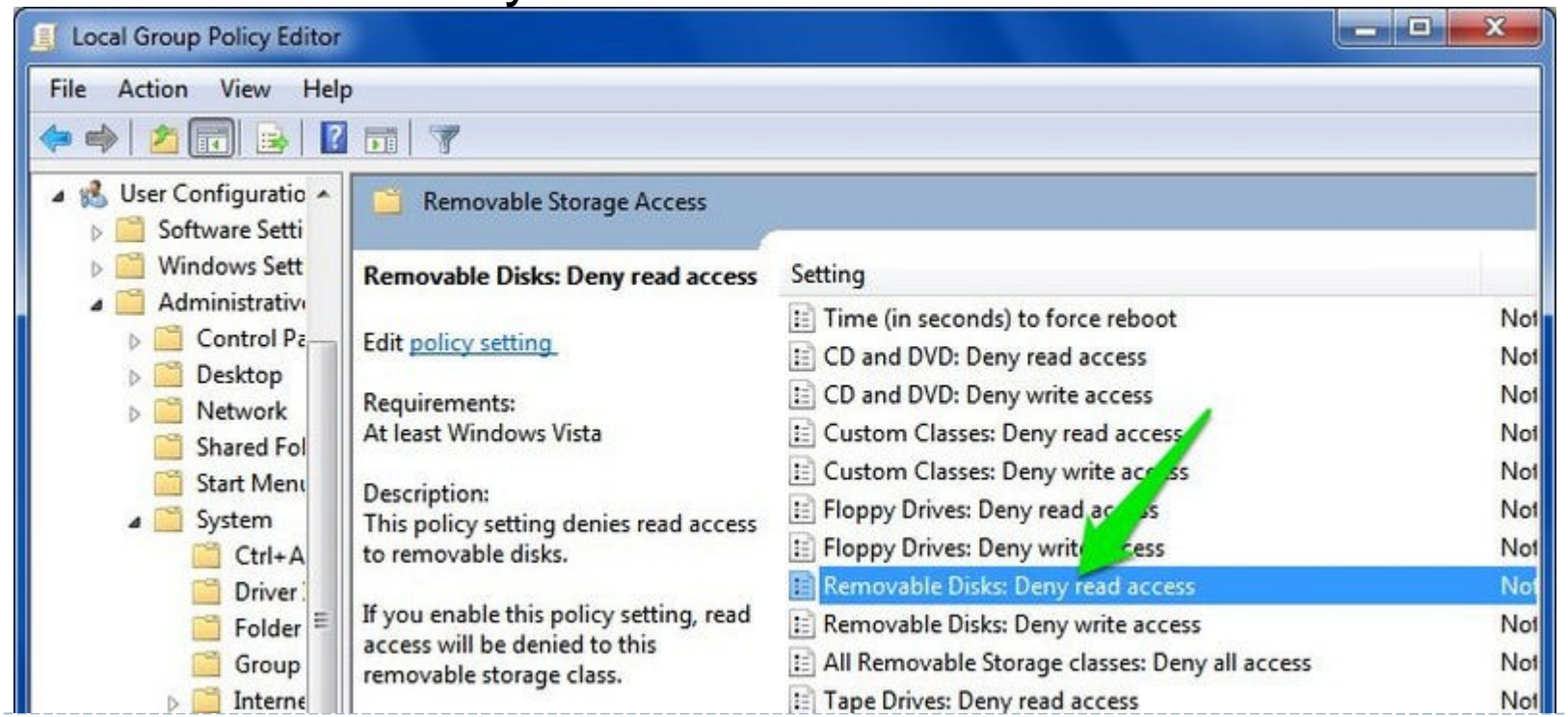
Bài 4: Thiết lập chính sách hạn chế quyền thực thi ứng dụng cụ thể với người dùng

2. Cấm cài đặt phần mềm : vào đường dẫn sau Computer Configuration > Administrative Templates > Windows Components > Windows Installer



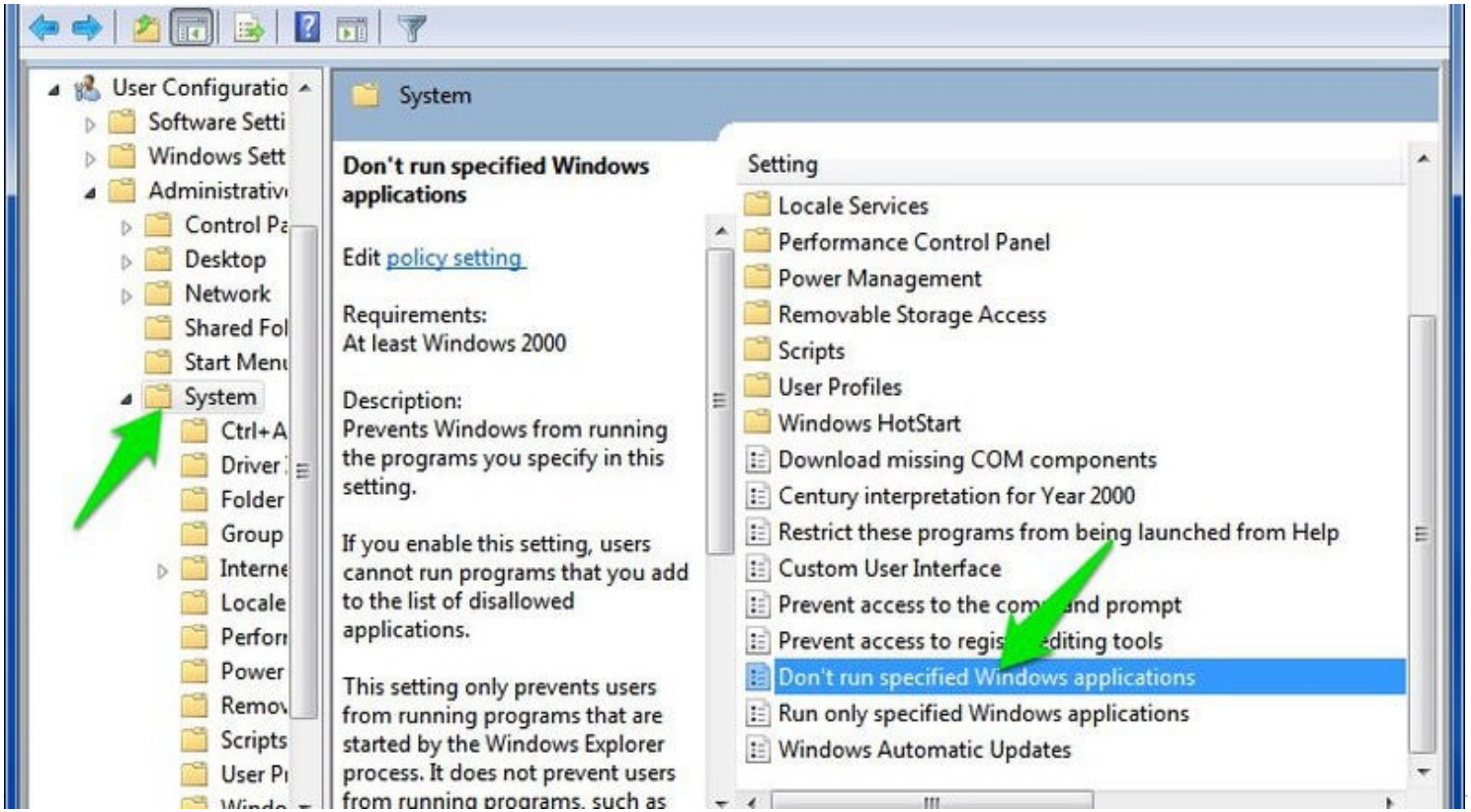
Bài 4: Thiết lập chính sách hạn chế quyền thực thi ứng dụng cụ thể với người dùng

3. Ngăn thiết bị di động kết nối với máy tính - vào theo hướng dẫn Configuration > Administrative Templates > System > Removable Storage Access rồi nhấn đúp vào tùy chọn Removable Disk: Deny read access



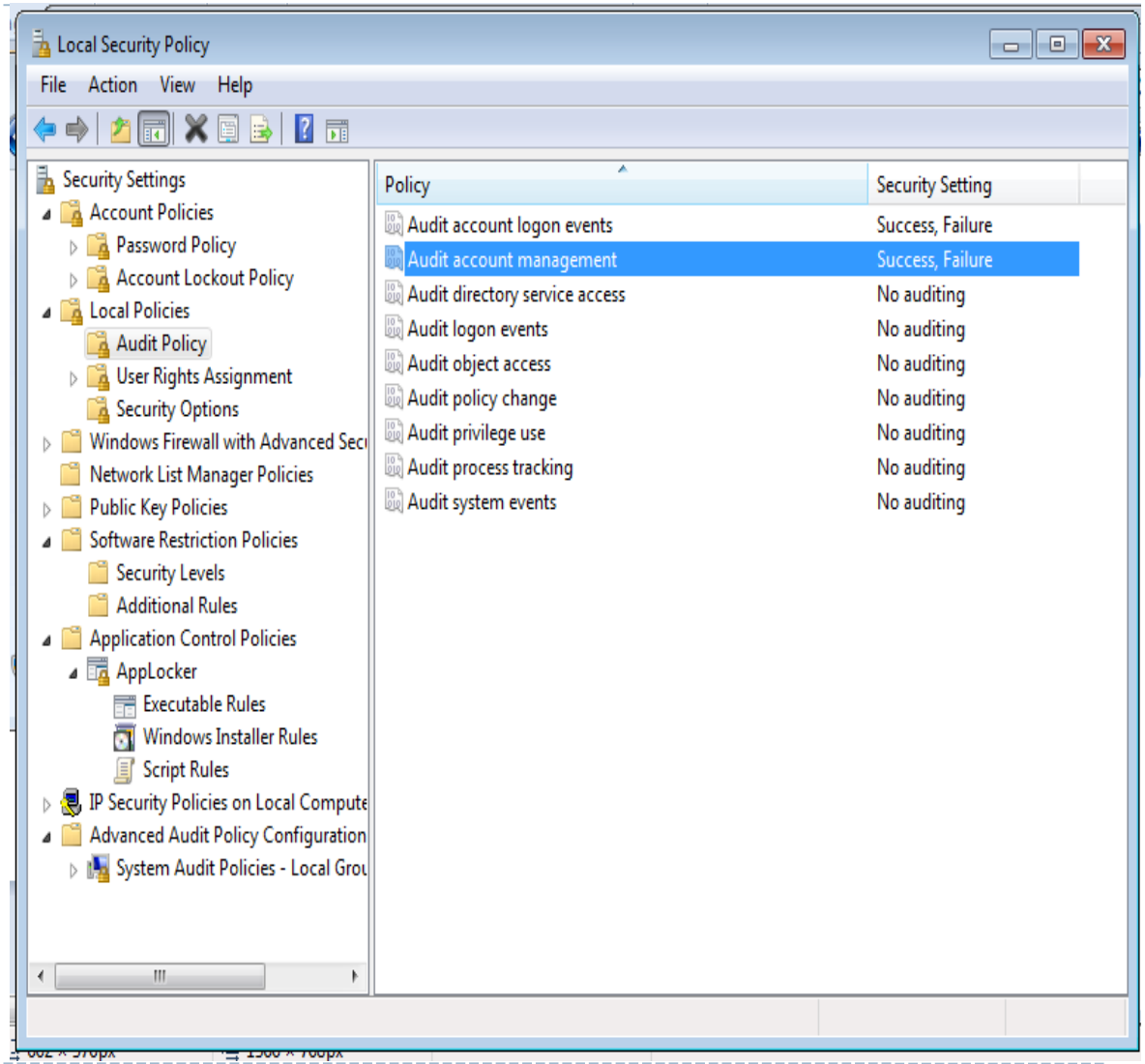
Bài 4: Thiết lập chính sách hạn chế quyền thực thi ứng dụng cụ thể với người dùng

4. Ngăn chặn một số phần mềm cụ thể - User Configuration > Administrative Templates > System. Sau đó, hãy nhấn đúp vào thiết lập Don’t run specified Windows applications



Bài 5: Cấu hình chính sách Audit và Event Log của Windows.

Default Domain Controllers Policy-> Edit →Computer Configuration-> Policies ->Windows Settings ->Security Settings -> Local Policies → Audit Policy.



Bài 5: Cấu hình chính sách Audit và Event Log của Windows.

1. Audit account logon event
2. Audit account management
3. Audit Directory Service Access
4. Audit Logon event
5. Audit object access
6. Audit Policy change
7. Aduit privilege use
8. Audit process tracking
9. Audit system events

Bài 5: Cấu hình chính sách Audit và Event Log của Windows.

Có 3 đối tượng mà Audit Policy đi giám sát:

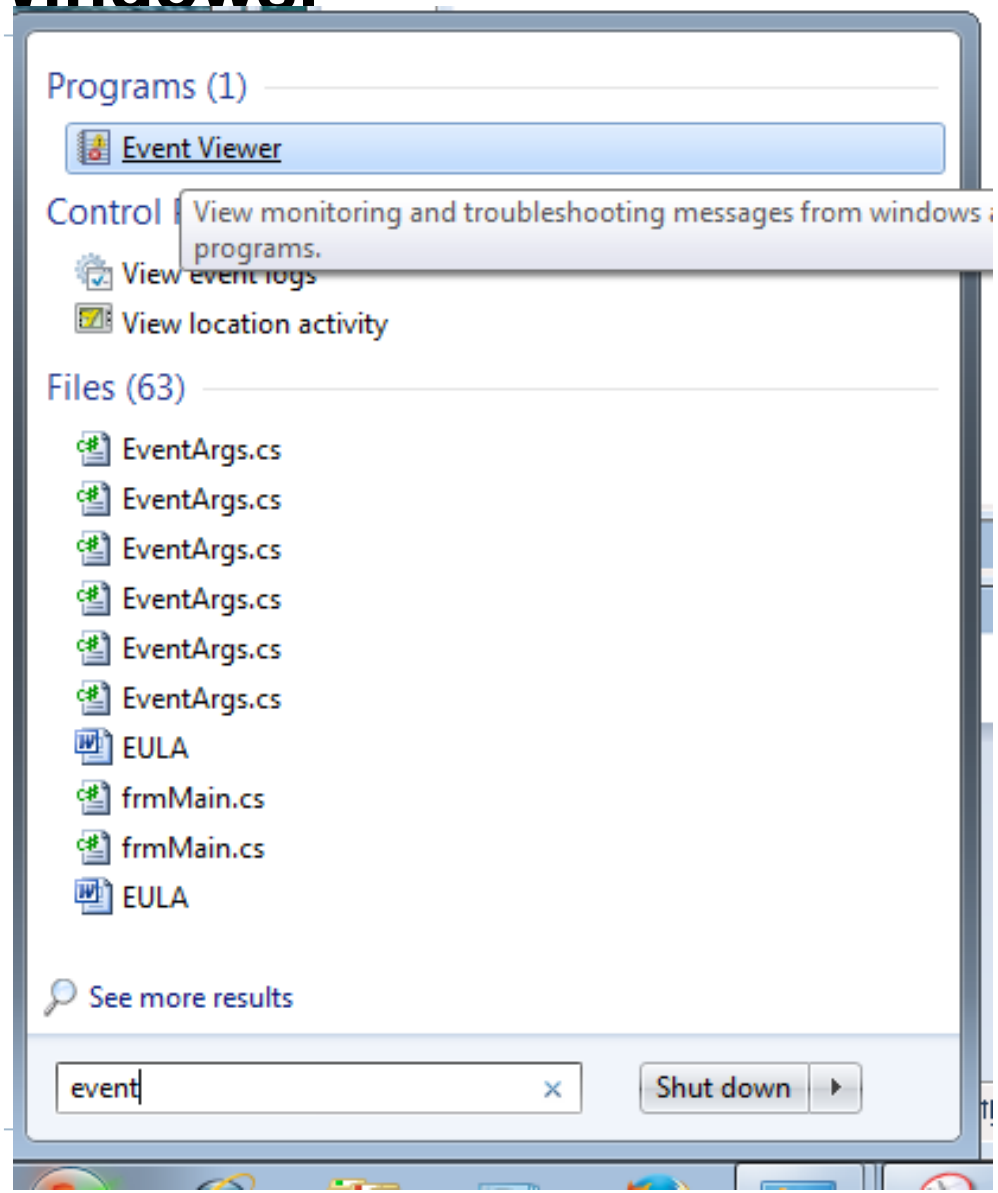
1.User : Policy (1) ,(2), (4), (5), (7)

2.Hệ thống: Policy: (3), (6), (9)

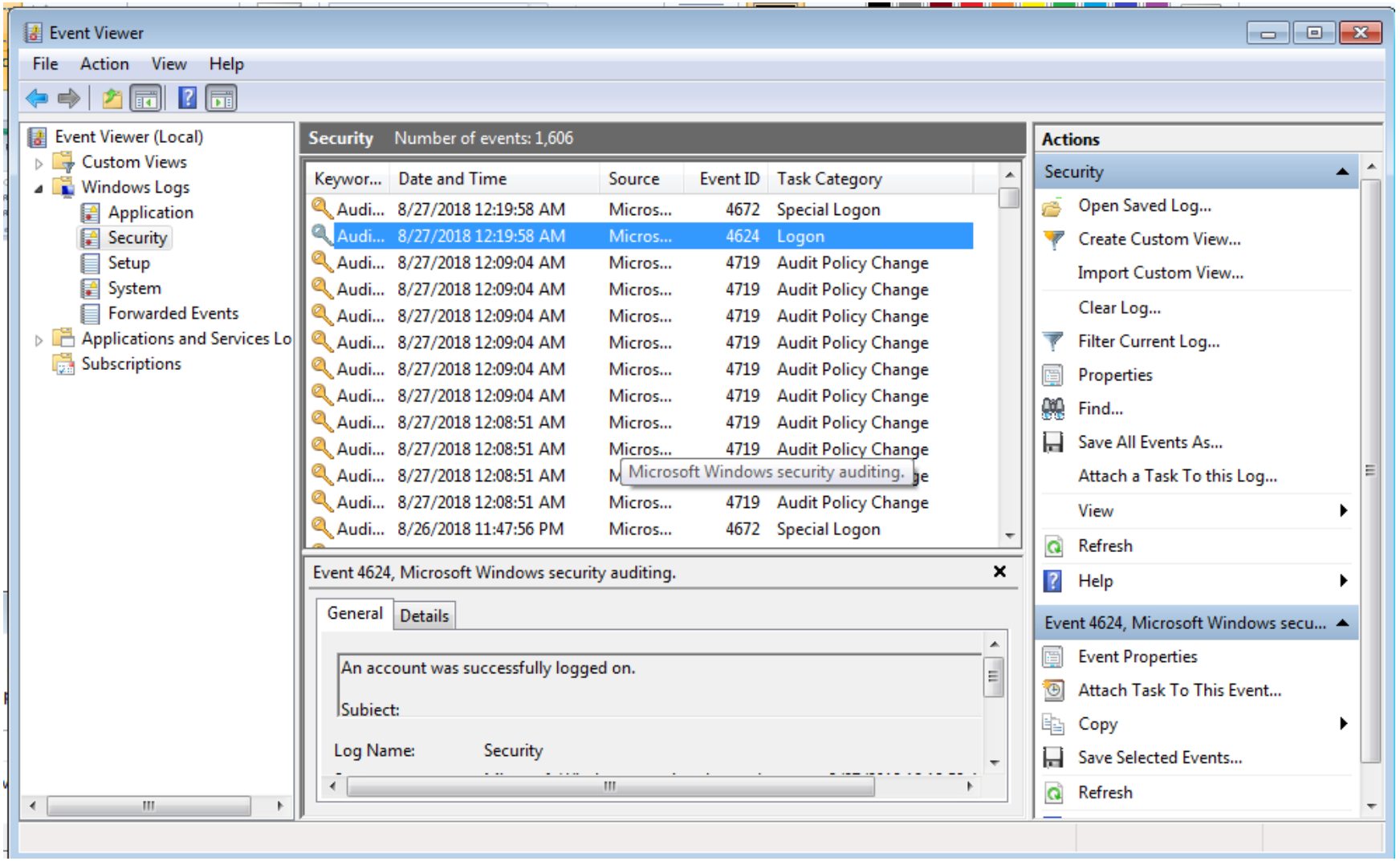
3.Ứng dụng có trên hệ thống: Policy (8)

Bài 5: Cấu hình chính sách Audit và Event Log của Windows.

Cách xem Event Log



Bài 5: Cấu hình chính sách Audit và Event Log của Windows.



HỎI VÀ ĐÁP