I. Group Policy.

1. Giới thiệu :

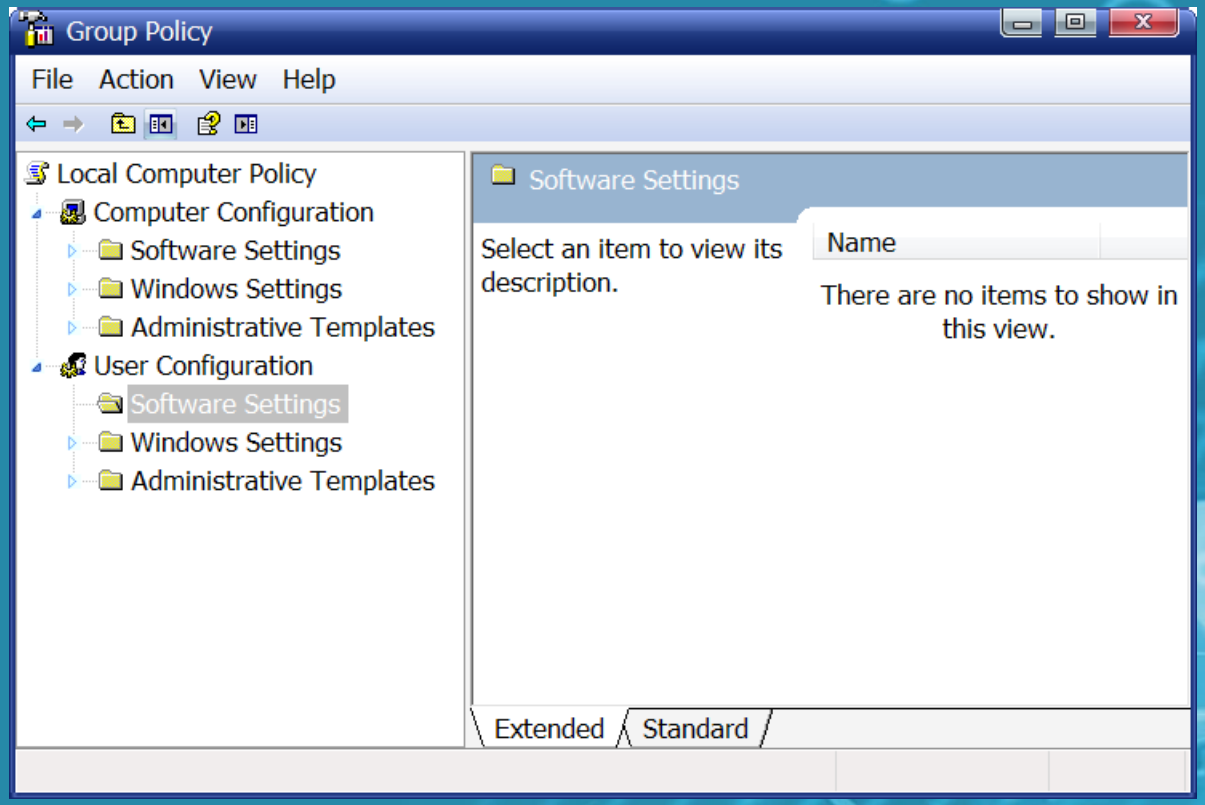
- Trong Windows XP trở về sau, tích hợp sẵn 1 công cụ rất hay đó là Group Policy.

- Group Policy là 1 trong các thành phần của Microsoft Management Console chỉ có thành viên của Administrators mới có quyền sử dụng chương trình này.

- Đây là nơi để Admin cấu hình, hoạch định các chính sách cho toàn bộ các thành phần trong máy : Tài khoản, Thiết bị, Chương trình, Bảo mật….

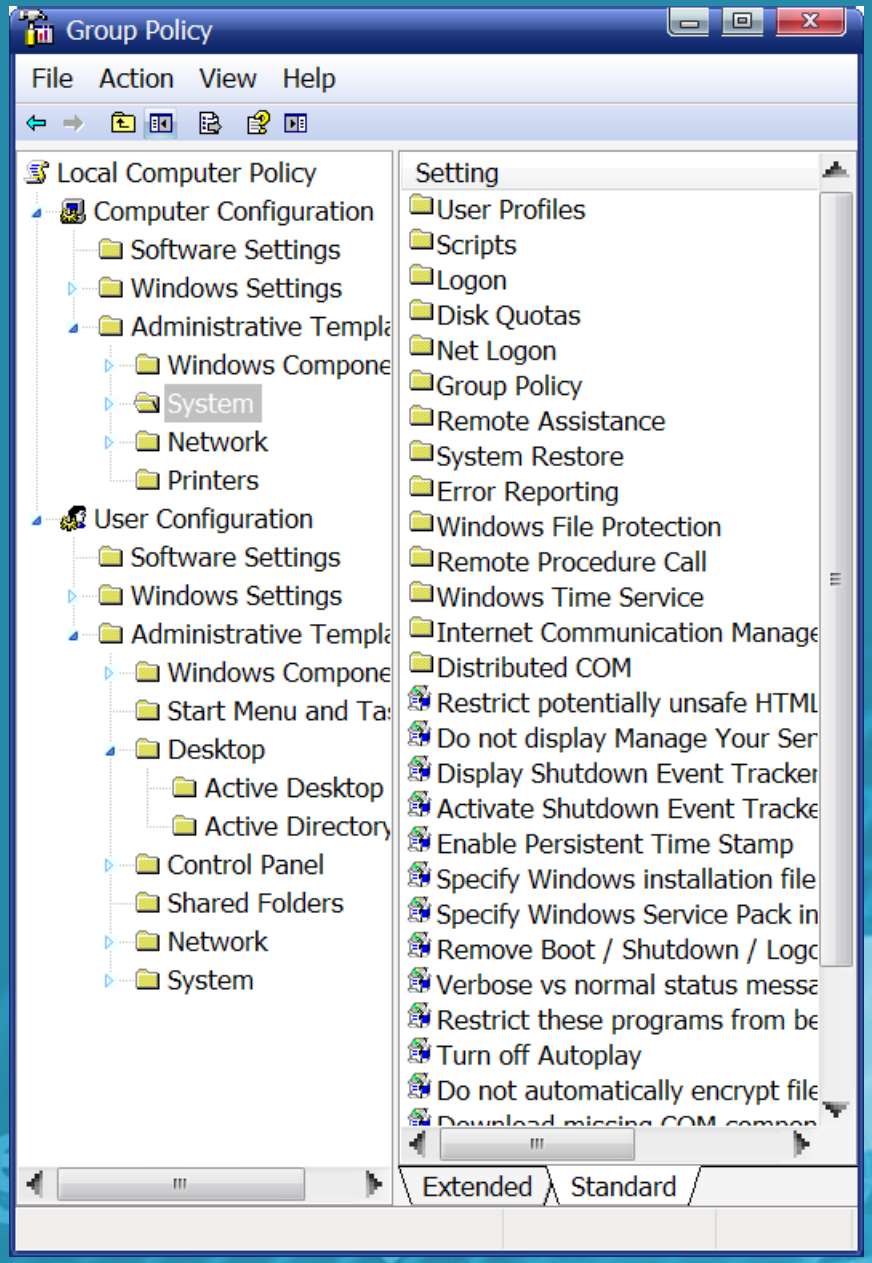
2. Khởi động chương trình :

- Từ nút Start ☞ Run ☞ nhập vào “gpedit.msc” ↵
- Giao diện chương trình xuất hiện như hình bên dưới



- Chương trình được phân theo dạng cây thư mục nên rất dễ dàng sử dụng.

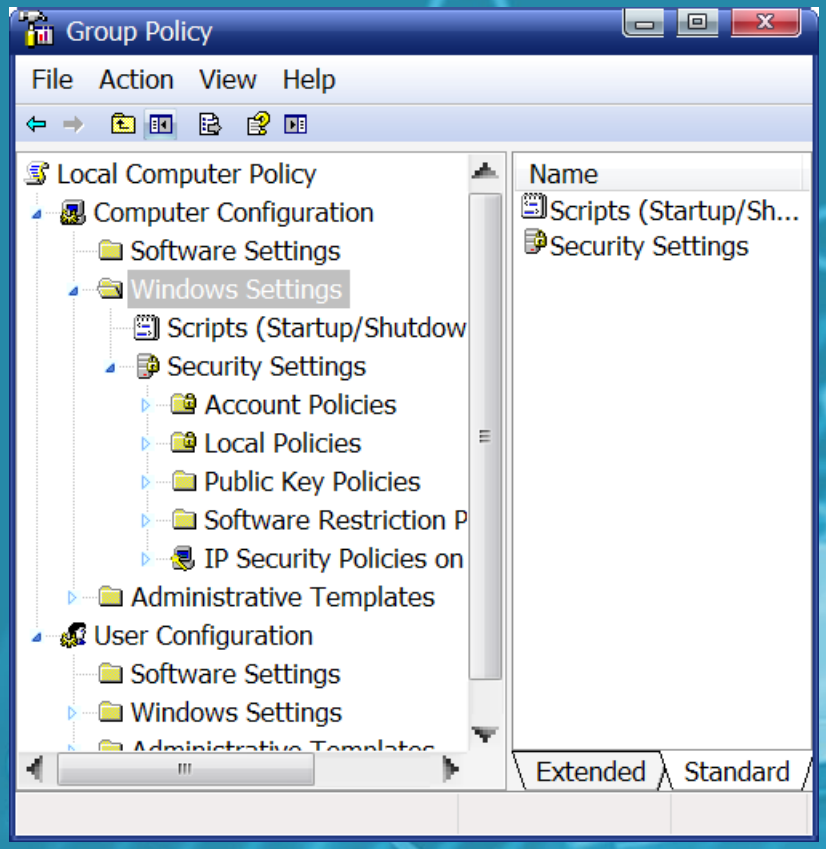
- Hầu hết các tùy chọn cấu hình hệ thống đều có trong GP. Ta có thể sử dụng GP để quản trị hệ thống mà không cần cài thêm phần mềm nào khác.



3. Các thành phần chính :

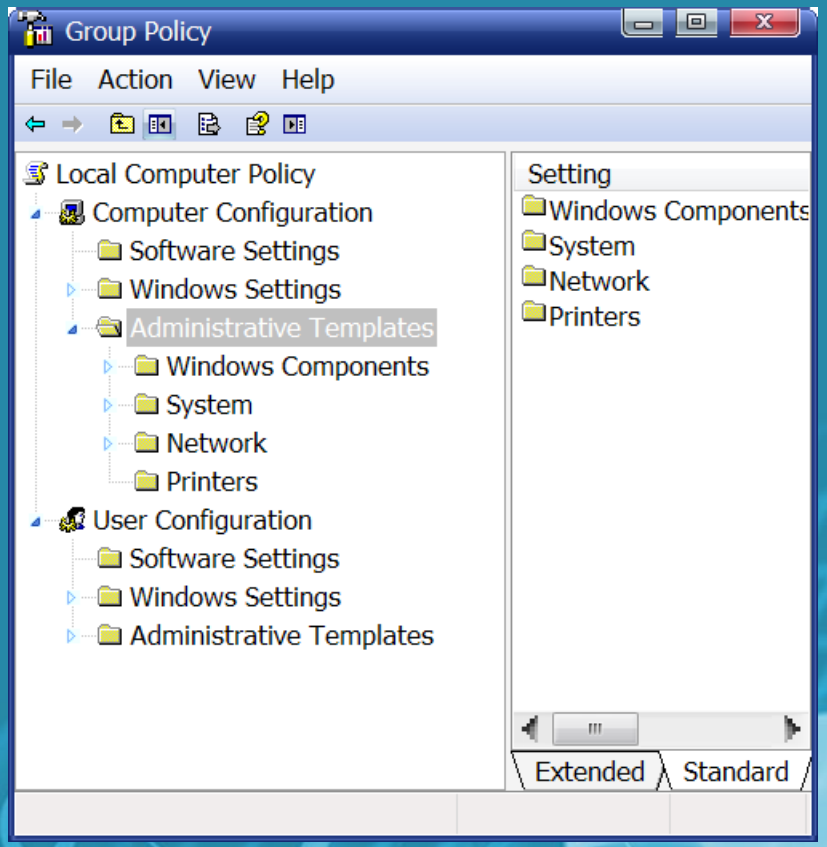
 Computer Configuration : Các thay đổi trong phần này sẽ áp dụng cho toàn bộ người dùng trên máy, trong nhánh này có nhiều nhánh con như :

- **Windows Settings:** áp đặt chính sách về việc sử dụng tài khoản, password tài khoản, quản lý việc khởi động và đăng nhập hệ thống...

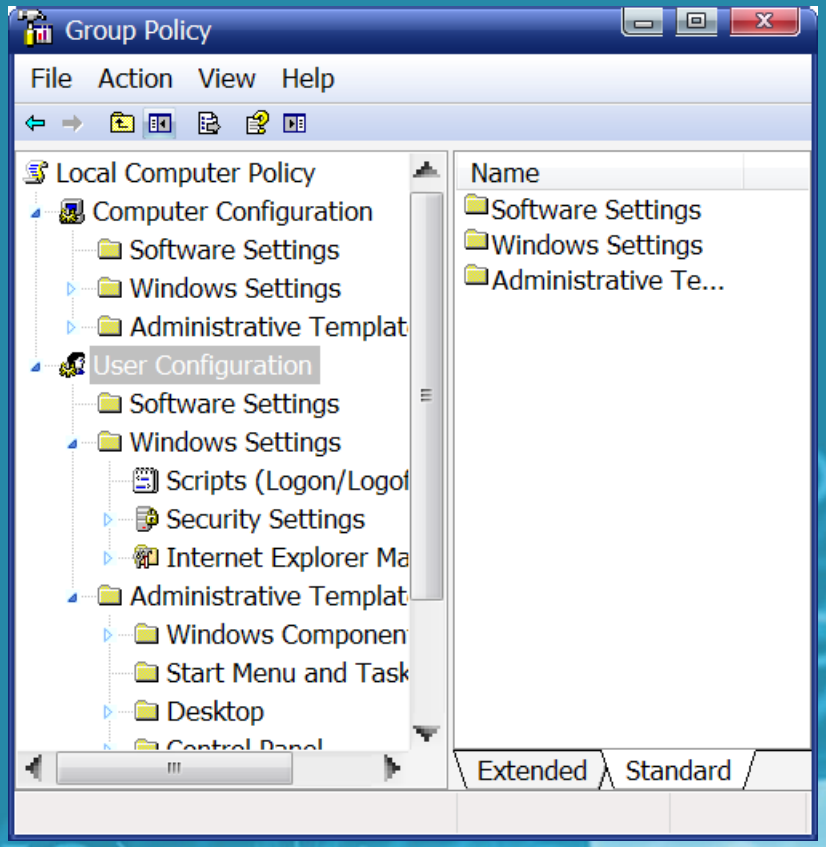


- **Administrative Templates :**

  - **Windows Components** : áp đặt chính sách cho các thành phần cài đặt trong Windows như: Internet Explorer, NetMeeting...
    - **System** : áp đặt những tùy chọn chính sách hệ thống.



- **User Configuration:** dùng để Admin áp đặt chính sách cho tài khoản đang sử dụng. Các thành phần có khác đôi chút nhưng việc sử dụng và cấu hình cũng tương tự Computer Configuration.



- Mặc định thì tình trạng ban đầu của các thành phần này là "Not configured".

4. Cách sử dụng chung :

- Mở đến các nhánh, tìm thành phần muốn cấu hình, sau đó để thay đổi tình trạng cho thành phần nào đó, bạn chọn thẻ Setting trong cửa sổ Properties, sẽ có 3 tùy chọn cho bạn chọn lựa là:

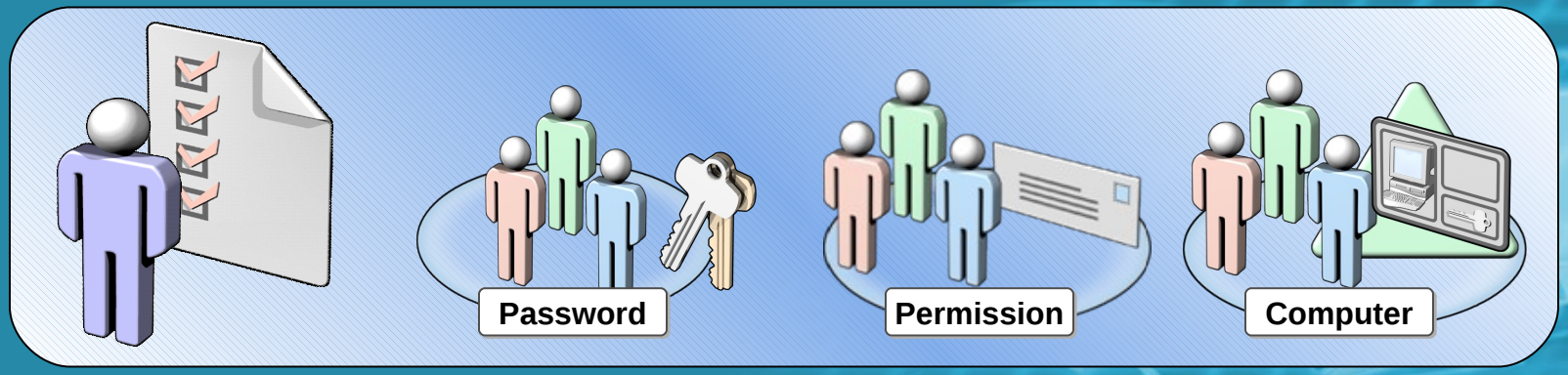
  - Not configured nếu không định cấu hình cho tính năng đó
  - Enabled để kick hoạt tính năng
  - Disabled để vô hiệu hóa tính năng.

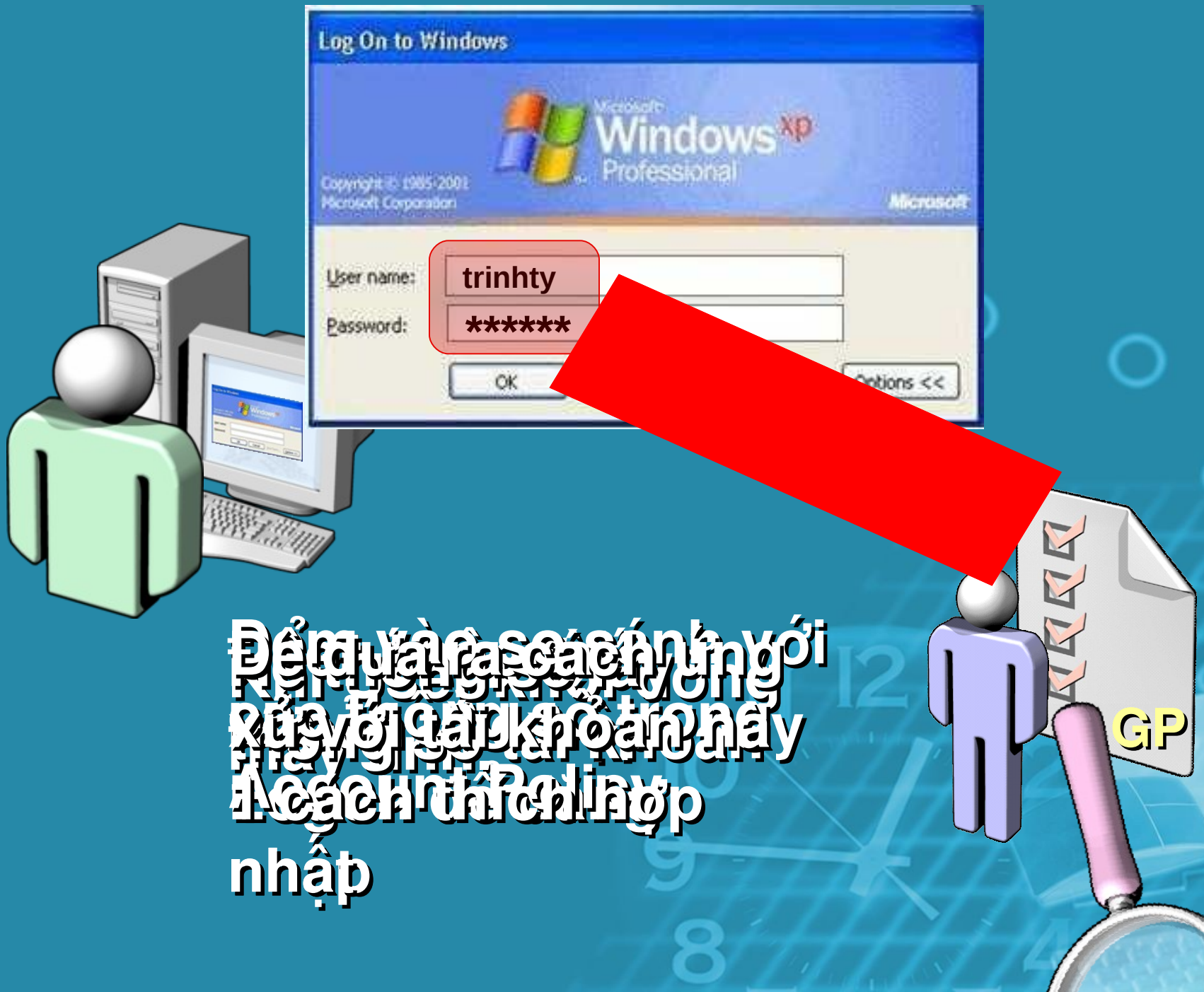
- Có rất nhiều chính sách trong GP cho phép Admin cấu hình đến từng chi tiết cho hệ thống cả phần cứng lẫn phần mềm.

- Trong bài này ta chỉ tham khảo vài chính sách tương đối thông dụng nhất mà các user quản trị máy thường sử dụng.

II. Account Policy.

- Chính sách tài khoản người dùng (Account Policy) dùng để chỉ định các thông số, các ràng buộc về tài khoản người dùng mà nó được sử dụng khi tiến trình Logon xảy ra.
- Cho phép ta cấu hình các thông số bảo mật cho mật khẩu, khoá tài khoản và chứng thực.



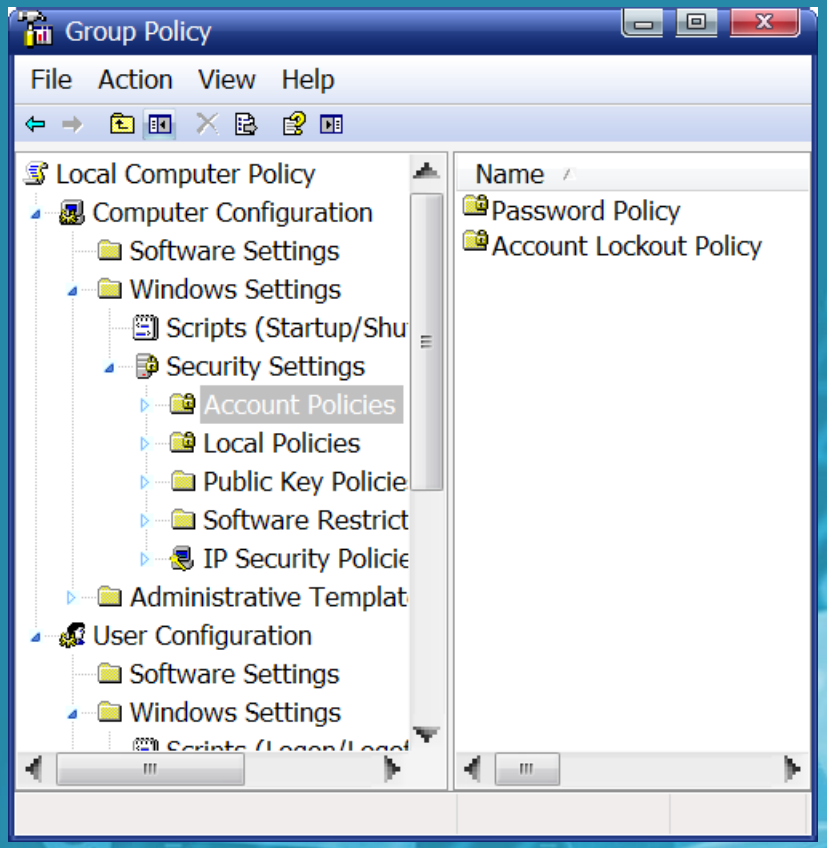


Đưa ra cách ứng xử với tài khoản này

Đưa ra cách thích hợp nhập

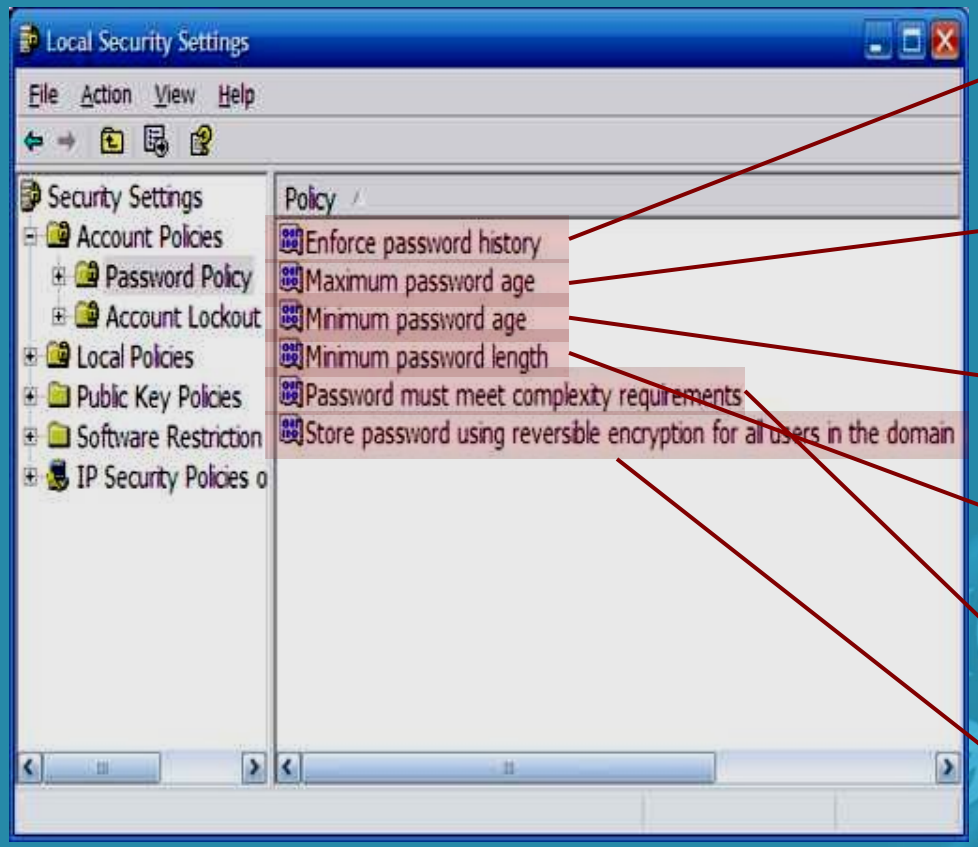
- Computer Configuration ☞ Windows Setting ☞ Security Settings ☞ Account Policies.

- Khảo sát 2 thành phần :
  - Password Policy
  - Account Lockout Policy.



1. Password Policy.

- Password Policy nhằm đảm bảo an toàn mật khẩu cho người dùng, tránh các trường hợp đăng nhập bất hợp pháp vào hệ thống



Số lần đặt mật mã không được trùng nhau (def 24)

Số ngày nhiều nhất mà mật mã có hiệu lực (def 42)

Số ngày tối thiểu trước khi User được phép đổi mật mã (1)

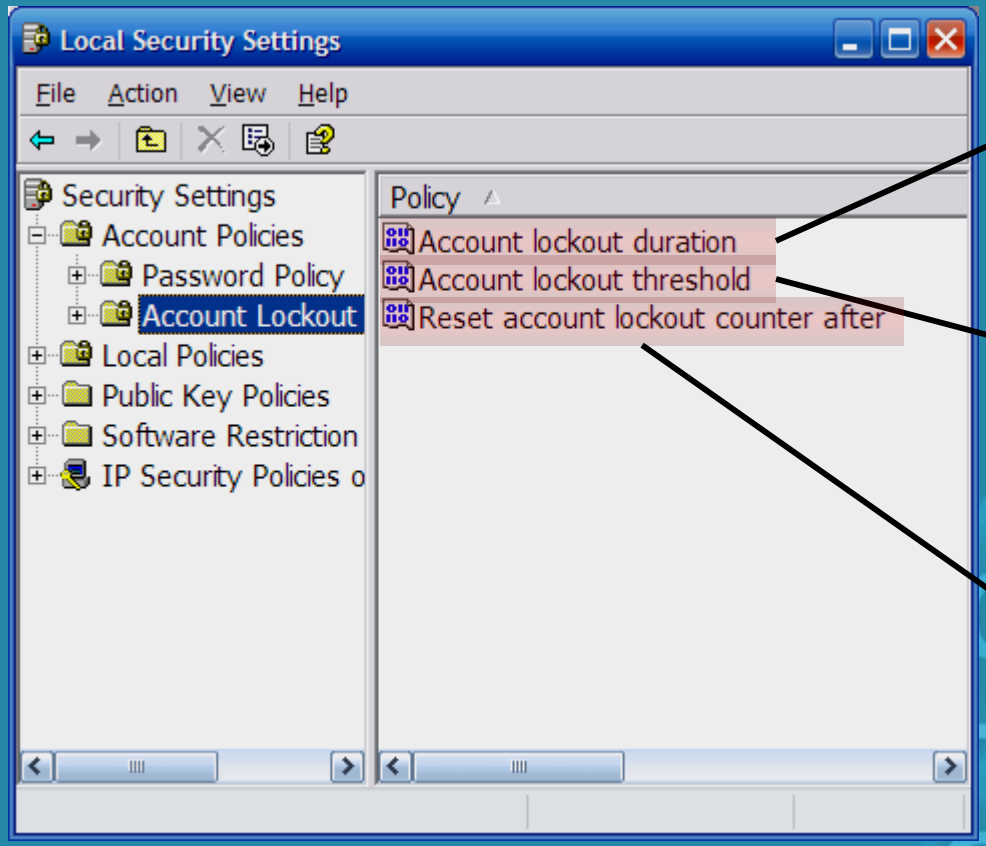
Số ký tự ngắn nhất của mật mã (7)

Mật mã phải có độ phức tạp (Y)

Mật mã được mã hoá (N)

2. Account Lockout Policy.

- Account Lockout Policy quy định cách thức khoá tài khoản trong vùng hay trong hệ thống cục bộ. Chính sách này giúp ta hạn chế bị tấn công bằng phương pháp Logon từ xa.



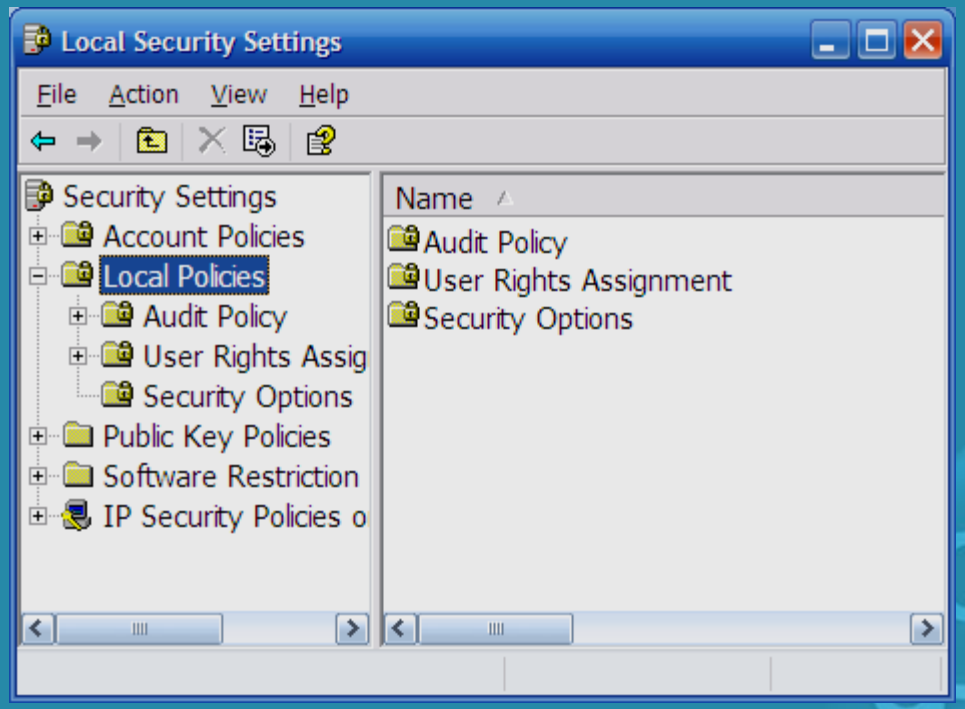
Quy định thời gian khoá. Là 0, Nhưng nếu Account Lockout Threshold được thiết lập thì giá trị này mặc định là 30 phút.

Quy định số lần đăng nhập sai, tài khoản sẽ bị khoá.

Quy định thời gian đếm lại số lần đăng nhập không thành công. Là 0, nếu Account Lockout Threshold được thiết lập thì giá trị này mặc định là 30 phút.

II. Chính sách c c b

- Cho phép thiết lập các chính sách giám sát tài khoản người dùng trên máy.

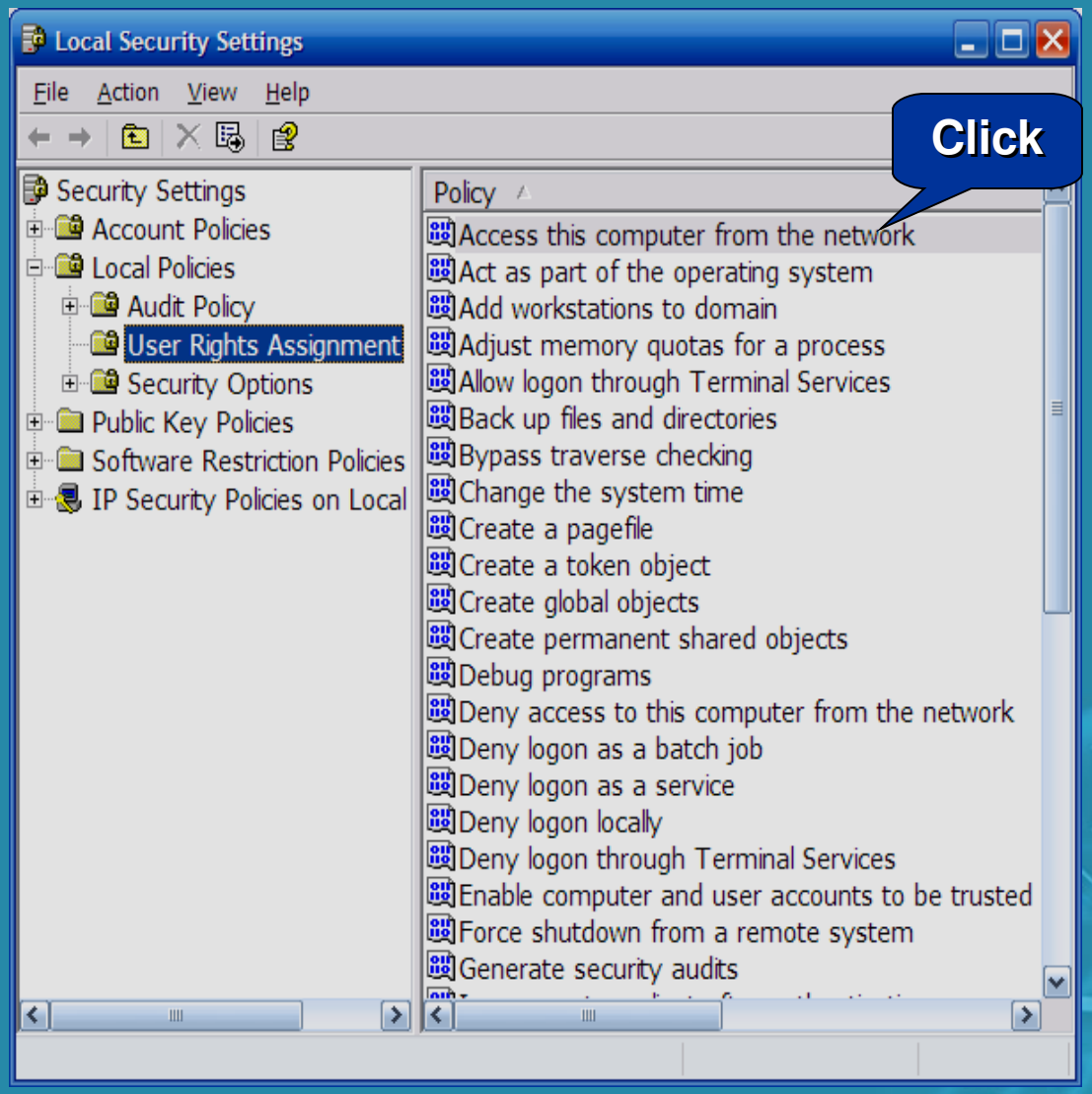


- Đồng thời có thể cấp quyền hệ thống (Rights) cho các người dùng và thiết lập các lựa chọn bảo mật.

Audit System Events

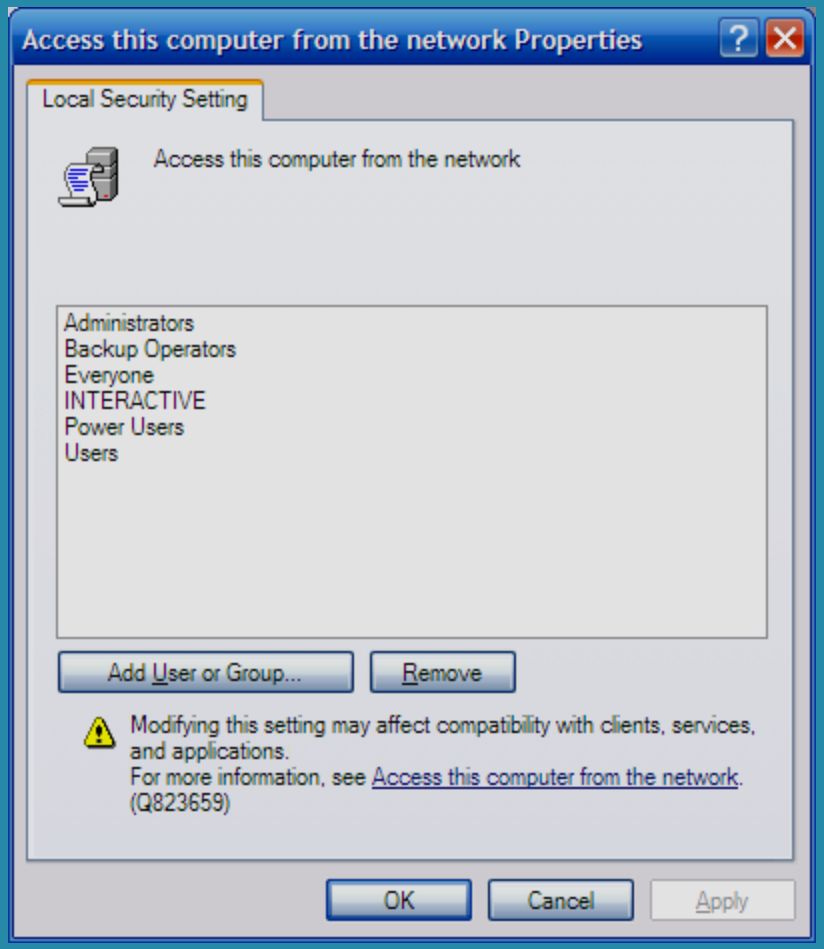
Ghi nhận lại những

II.2. Quyền hệ thống



Có hai cách để ta cấp quyền hệ thống (Rights) cho người dùng:

1. Đưa User Account vào các nhóm có sẵn (built-in). (đã học)
2. Hoặc ta dùng công cụ User Rights Assignment để gán từng quyền rời rạc (Double click)



- Xuất hiện hộp thoại
- Nhấn vào nút Add User or Group… để thêm người dùng hoặc nhóm có sẵn được quyền này, hoặc nhấn Remove để xóa người dùng khỏi danh sách

Danh sách các quyền hệ thống cấp cho người dùng và nhóm

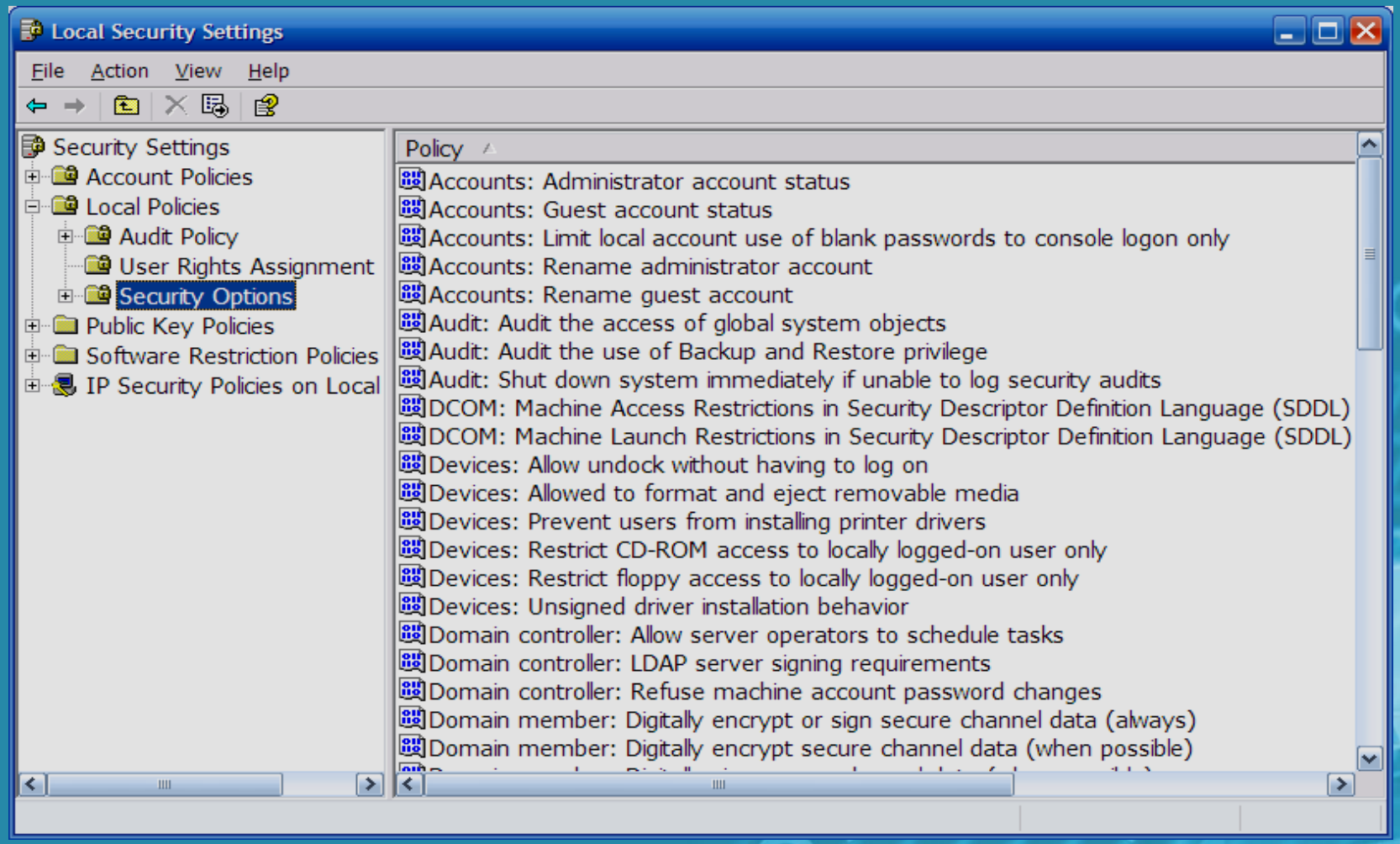
Quyền	Mô tả
Access This Computer in the Network	Cho phép người dùng truy cập máy tính này thông qua mạng, mặc định mọi người đều có quyền
Act as Part of the Operating System	Cho phép các dịch vụ chứng thực ở mức thấp, được chứng thực bởi bất cứ người dùng nào
Add Workstations to the Domain	Cho phép người dùng thêm 1 tài khoản máy tính vào vùng
Backup file and Directories	Cho phép người dùng sao lưu
Bypass Traverse checking	Cho phép duyệt cấu trúc thư mục nếu không có quyền xem (list) thư mục này
Change the System time	Cho phép thay đổi giờ hệ thống

Quyền	Mô tả
Creat a Pagefile	Cho phép thay đổi kích thước Pagefile
Creat a Token Object	Cho phép 1 tiến trình tạo 1 thẻ bài nếu tiến trình này dùng NTCreat Token API
Creat Permanent Shared Object	Cho phép 1 tiến trình tạo 1 đối tượng thư mục thông qua Win 2000 Object Manager
Debug Programs	Cho phép người dùng gắn 1 chương trình debug vào bất cứ tiến trình nào
Deny Access to This Computer from the Net	Cho phép khoá người dùng hoặc nhóm không được truy cập đến các máy tính khác trên mạng
Deny Logon as Batch file	Cho phép ngăn cản users và nhóm được phép logon như 1 batch file

Quyền	Mô tả
Deny Logon as Service	Cấm users và nhóm logon như 1 service
Deny Logon Locally	Cấm users và nhóm truy cập đến máy tính cục bộ
Enable Computer and User Accounts to Be Trusted by Delegation	Cho phép users hoặc nhóm được uỷ quyền cho người dùng hoặc máy tính
Force shutdow from a remote system	Cho phép người dùng Shutdow máy từ xa thông qua mạng
Generate Security Audits	Cho phép tạo 1 entry vào Security log
Increase Quotas	Cho phép users điều khiển hạn nghạch của các tiến trình

II.3. Các lựa chọn bảo mật

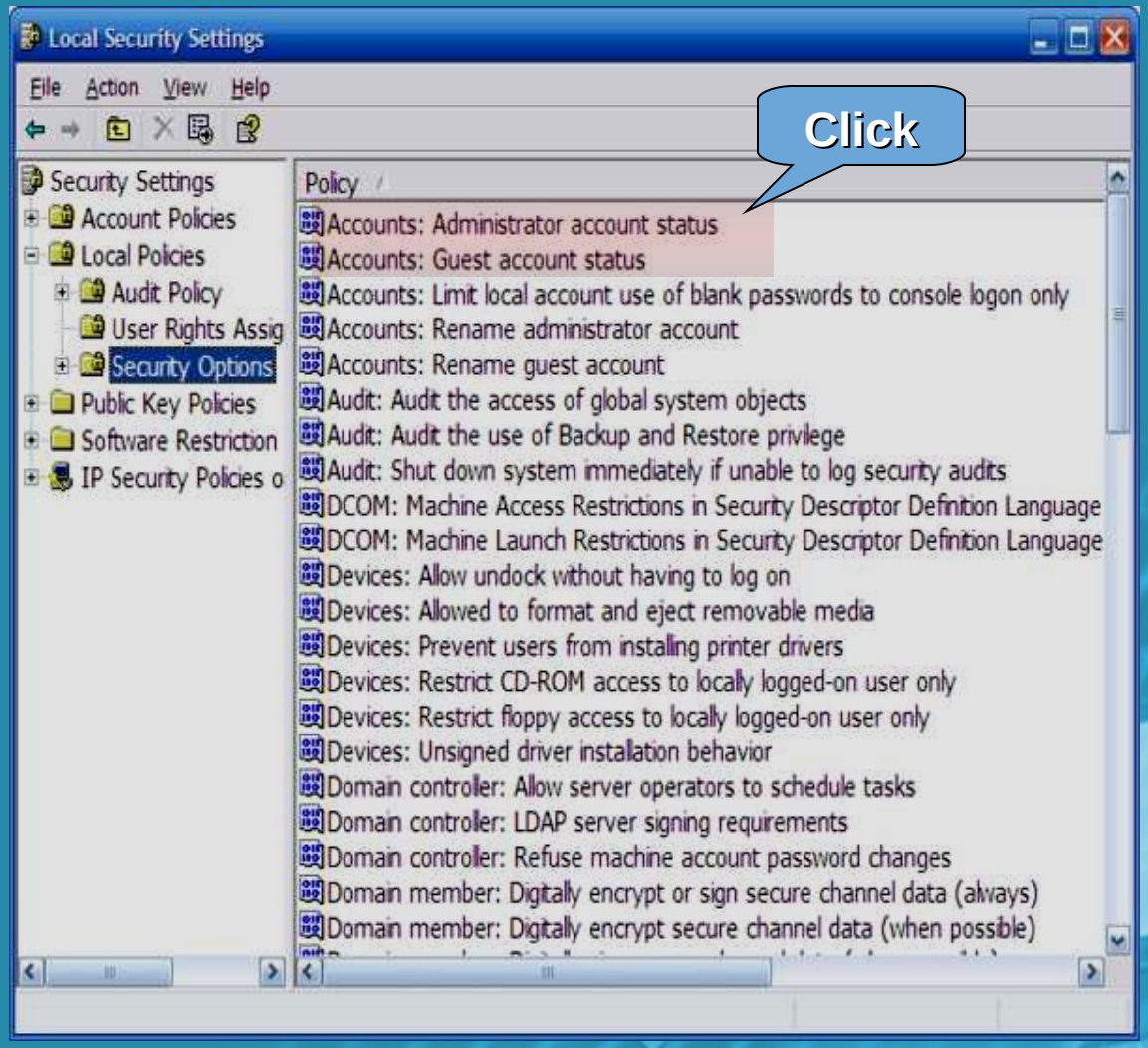
Security Options cho phép người quản trị khai báo thêm các thông số nhằm tăng tính bảo mật cho hệ thống



Một số lựa chọn bảo mật thông dụng

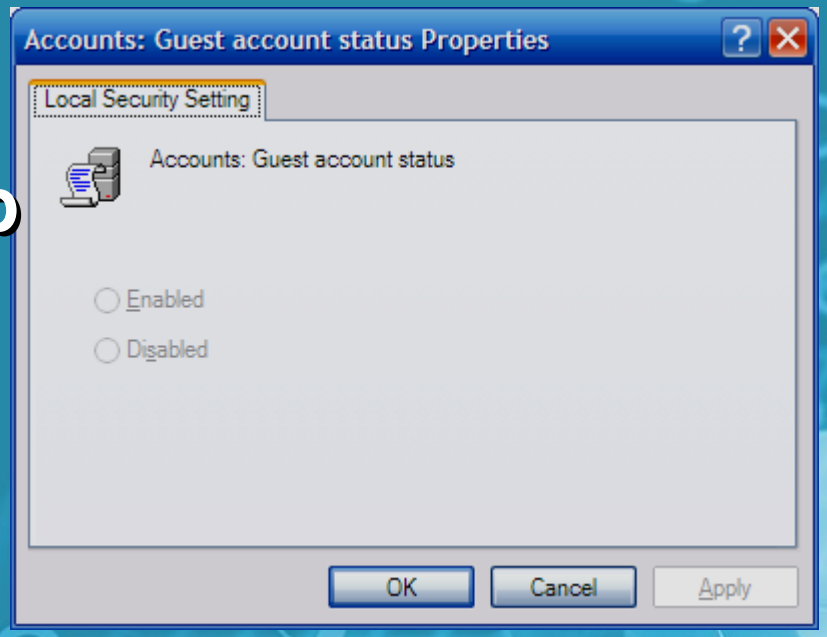
Win XP hổ trợ chúng ta rất nhiều lựa chọn bảo mật. Nhưng trong tài liệu này chúng ta chỉ khảo sát những lựa chọn thông dụng như:

Thay đổi trạng thái hoạt động của User



- Xuất hiện hộp thoại cho phép ta cấu hình thay đổi

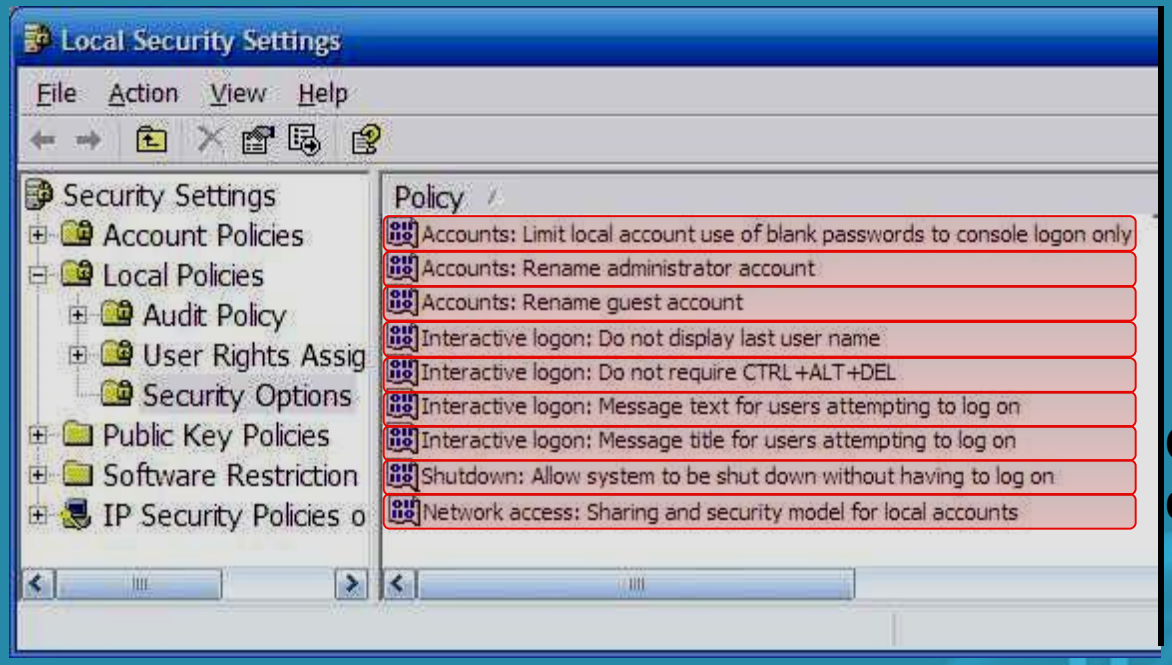
- Enable : Cho tài khoản này được phép hoạt động
- Disable : Tài khoản này bị tạm khóa.



Giới hạn người dùng sử dụng Password rổng

Đổi tên tài khoản Administrator

Đổi tên tài khoản Guest



Không hiển thị tên người dùng vừa logon trên hộp thoại logon

Không cần nhấn CTRL+ATL+DEL khi khởi động

Gởi 1 message cho người sử dụng khi họ logon

Tiêu đề của message

Cho phép Shutdown máy mà không cần logon

Tính chất của tài khoản khi truy cập hệ thống từ mạng