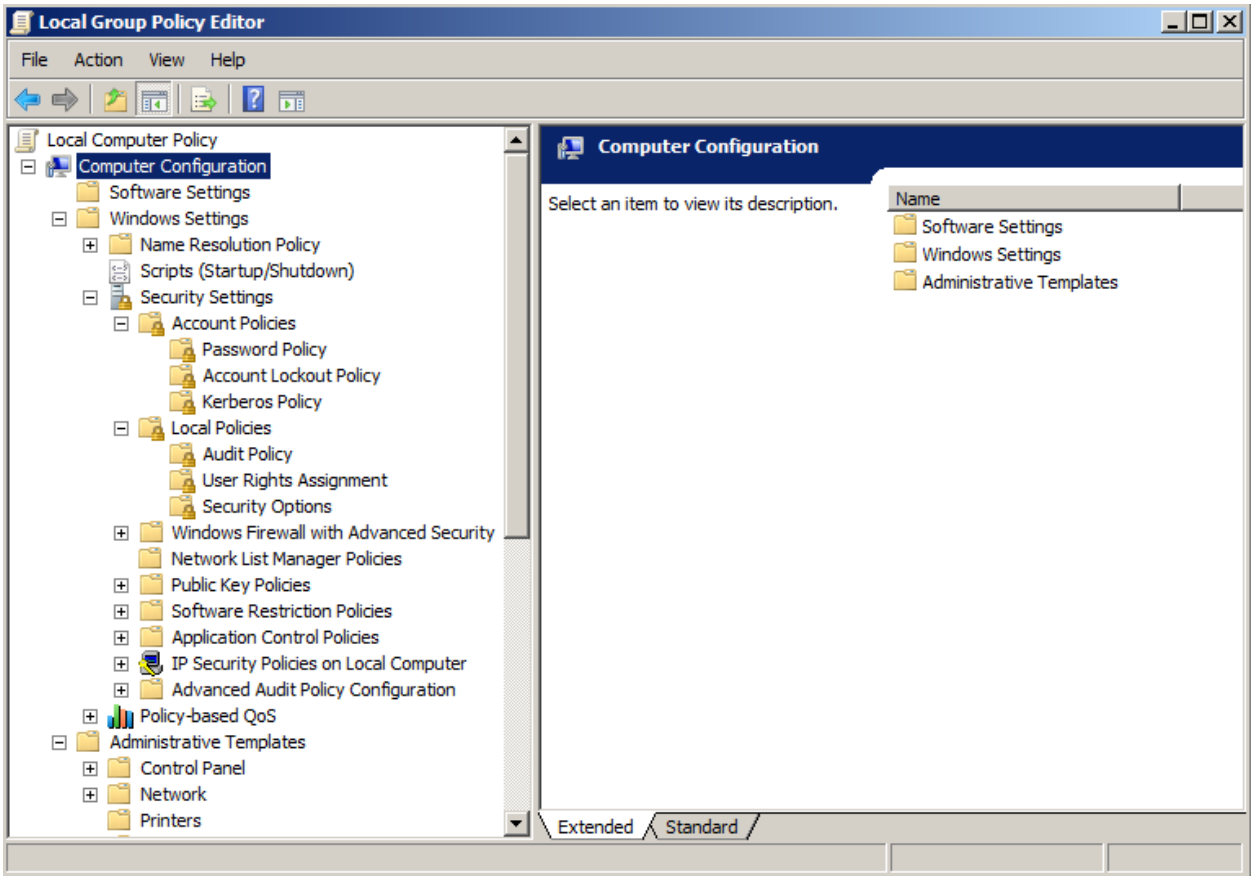
Group Policy có thể dùng để triển khai phần mềm cho một hoặc hoặc nhiều máy trạm nào đó một cách tự động; để ấn định quyền hạn cho một số người dùng mạng, để giới hạn những ứng dụng mà người dùng được phép chạy; để kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm; để thiết lập các kịch bản (script) đăng nhập (logon), đăng xuất (logout), khởi động (start up), và tắt máy (shut down)

Group Policy có thể được coi là một thứ *System Policy* (phiên bản cũ). Các chính sách này được MS phát minh ra từ Windows 2000, áp dụng được với các hệ điều hành kể từ bản Windows 2000. Một số đặc điểm của **Group Policy**:

- Các **Group Policy** chỉ có thể hiện hữu trên miền Active Directory.
- Các **Group Policy** có thể dùng để triển khai phần mềm cho một hoặc hoặc nhiều máy trạm nào đó một cách tự động; để ấn định quyền hạn cho một số người dùng mạng, để giới hạn những ứng dụng mà người dùng được phép chạy; để kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm; để thiết lập các kịch bản (script) đăng nhập (logon), đăng xuất (logout), khởi động (start up), và tắt máy (shut down); để đơn giản hóa và hạn chế các chương trình trên máy khách; để định hướng lại (redirector) một số folder trên máy khách (như Computer, My Document)…
- **Group Policy** tự động mất tác dụng đối với máy trạm khi chúng được xóa bảo khỏi miền AD.
- Các **Group Policy** chỉ được áp dụng vào lúc máy khách khởi động (đối với chính sách dành cho máy) hoặc đăng nhập (đối với chính sách dành cho người dùng). Các **Group Policy** được áp dụng lúc máy trạm khởi động, lúc máy trạm đăng nhập, vào mọi thời điểm (được cấu hình trước).
- Tuy gọi là *Group* nhưng các **Group Policy** chủ yếu được áp dụng cho các site, domain và OU (Organizational Unit). Thực ra cũng có thể áp dụng chúng cho các nhóm người dùng, nhưng phải sử dụng kỹ thuật lọc và chặn chính sách *(policy filtering)*, tuy nhiên việc áp dụng kỹ thuật này gây rắc rối cho việc quản trị và troubleshooting mạng về sau, và làm chậm quá trình đăng nhập của người dùng qua mạng.
- Trên các máy tính local, có thể sử dụng *Local Group Policy* để áp dụng cho máy đó (chỉ duy nhất máy đó).
- Các **Group Policy** áp dụng cho các đối tượng gọi là **Group Policy Object (GPO)**. Các **GPO** được lưu trữ một phần trong cơ sở dữ liệu của AD và một phần trong *share SYSVOL*. Phần nằm trong *share SYSVOL* của mỗi **GPO** bao gồm một số file và thư mục con bên trong thư mục WindowsINNT\SYSVOL\sysvol\Domainame\Plocyes\GUID, trong đó GUID là mã nhận diện đơn nhất toàn cầu (Global Unique Identifier) dành cho GPO.
- Chương trình để tạo ra và chỉnh sửa các **GPO** có tên là *Group Policy Object Editor,* có dạng mộc console MMC khác, ví dụ như: Console Active Directory Users and Computers, tức DSA.MSC, cũng được trang bị sẵn snap-in Group policy).

Các thành phần trong Group Policy Object.

Phần I: Computer Configuration:



Windows Setting:

Tại đây có thể tinh chỉnh, áp dụng các chính sách về vấn đề sử dụng tài khoản, quản lý việc khởi động và đăng nhập hệ thống…

– Scripts: (startup/Shutdown): Có thể chỉ định cho Windows sẽ chạy một mã nào đó khi Windows Startup hoặc Shutdown.

– Security setting: Các thiết lập bảo mật cho hệ thống, các thiết lập này được áp dụng cho toàn bộ hệ thống chứ không riêng người dùng nào.

Account Policies: Các chính sách áp dụng cho tài khoản người dùng.

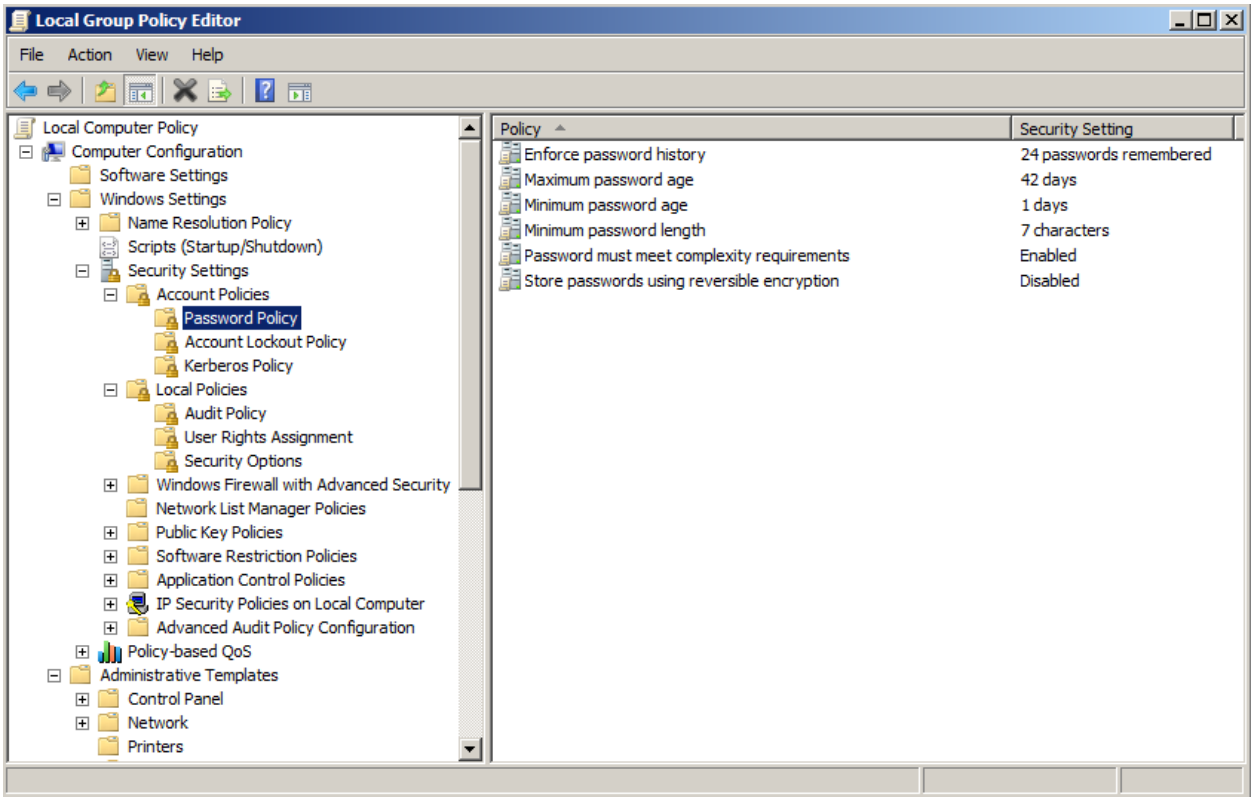
Local Policy: Kiểm định chính sách, những tùy chọn quyền lợi và chính sách an toàn cho người dùng cục bộ.

Public Key Policies. Các chính sách khóa dùng chung.

Chi tiết từng thành phần:

1. Account Policies:

a.Password Policies: Bao gồm các chính sách liên quan đến mật khẩu tài khoản của người sử dụng tài khoản trên máy.



– Enforce password history: Với những người sử dụng không có thói quen ghi nhớ nhiều mật khẩu, khi buộc phải thay đổi mật khẩu thì họ vẫn dùng chính mật khẩu cũ để thay cho mật khẩu mới, điều này là một kẽ hở lớn liên quan trực tiếp đến việc lộ mật khẩu. Thiết lập này bắt buộc một mật khẩu mới không được giống bất kỳ một số mật khẩu nào đó do ta quyết định. Có giá trị từ 0 đến 24 mật khẩu.

– Maximum password age: Thời gian tối đa mật khẩu còn hiệu lực, sau thời gian này hệ thống sẽ yêu cầu ta thay đổi mật khẩu. Việc thay đổi mật khẩu định kỳ nhằm nâng cao độ an toàn cho tài khoản, vì một kẻ xấu có thể theo dõi những thói quen của bạn, từ đó có thể tìm ra mật khẩu một cách dễ dàng. Số giá trị từ 1 đến 999 ngày, giá trị mặc định là 42 ngày.

– **Minimum password age:** Xác định thời gian tối thiểu trước khi có thể thay đổi mật khẩu. Hết thời gian này bạn mới có thể thay đổi mật khẩu của tài khoản, hoặc bạn có thể thay đổi ngay lập tức bằng cách thiết lập giá trị là 0. Giá trị từ 0 đến 999 ngày.

– Minimum password length: Độ dài nhỏ tối thiểu của mật khẩu tài khoản (tính bằng số ký tự nhập vào). Độ dài của mật khẩu có giá trị từ 1 đến 14 ký tự. Thiết lập giá trị là 0 nếu không muốn sử dụng mật khẩu. Giá trị mặc định là 0.

– Password must meet complexity requirements: Quyết định độ phức tạp của mật khẩu, nếu tính năng này có hiệu lực, mật khẩu của tài khoản ít nhất phải đạt những yêu cầu sau:

+ Không chứa tất cả hoặc một phần tên tài khoản người dùng.

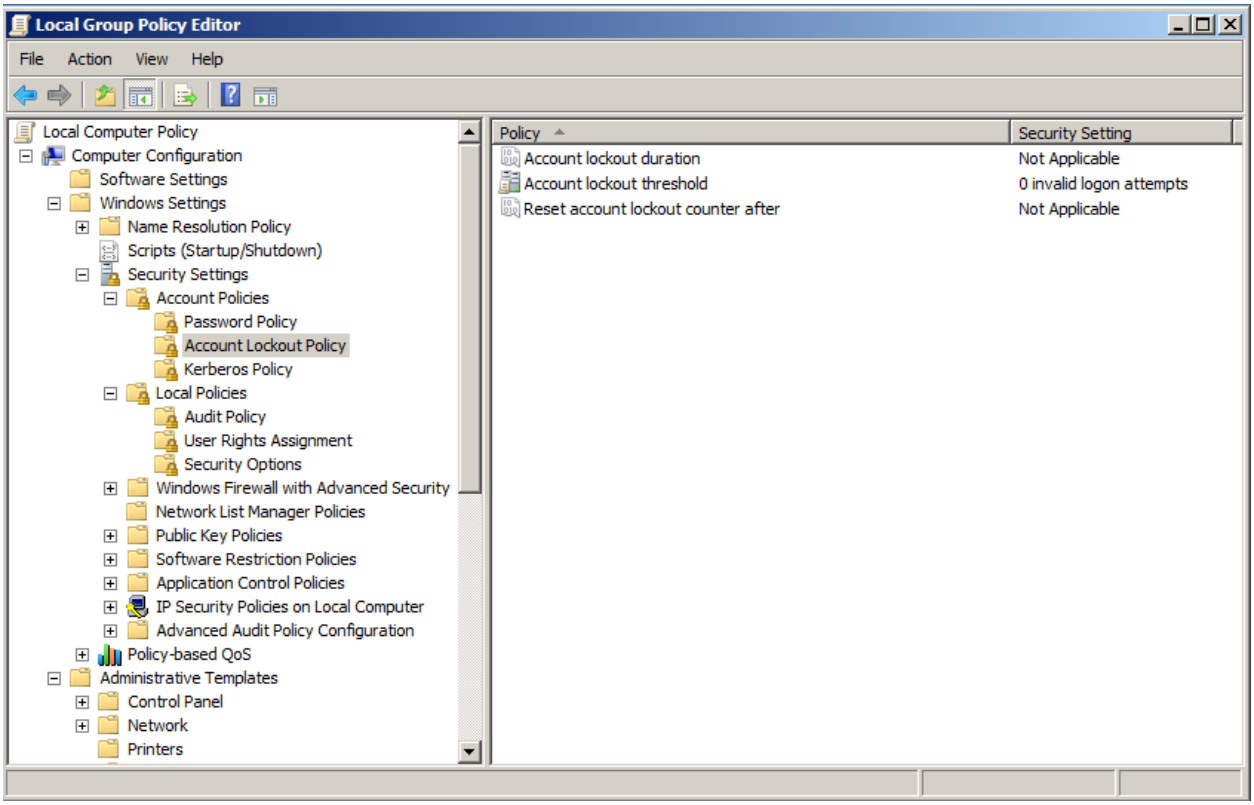
+ Độ dài nhỏ nhất là 6 ký tự.

+ Chứa 3 hoặc 4 loại ký tự sau: Các chữ cái thường (a->z), các chữ cái hoa (A->Z>), các chữ số (0->9) và các ký tự đặc biệt.

Độ phức tạp của mật khẩu được coi là bắt buộc khi tạo mới hoặc thay đổi mật khẩu, mặc định là: *Disable*.

Store password using reversible encryption fo all user in the domain: Lưu trữ mật khẩu sử dụng mã hóa ngược cho tất cả các người sử dụng domain. Tính năng cung cấp sự hỗ trợ cho các ứng dụng giao thức, nó yêu cầu sự am hiểu về mật khẩu người sử dụng. Việc lưu trữ mật khẩu sử dụng phương pháp mã hóa ngược thực chất giống như việc lưu trữ các văn bản mã hóa các thông tin bảo vệ mật khẩu. Mặc định: *Disable*.

b. Account lockout Policy:



– Account lockout duration: Xác định số phút còn sau khi tài khoản được khóa trước khi mở khóa được thực hiện. Có giá trị từ 0 đến 99.999 phút. Có thể thiết lập giá trị 0 nếu

không muốn tự đông Unlock. Mặc định không có hiệu lực vì chính sách này chỉ có khi chính sách *"Account lockout threshold"* được thiết lập.

– Account lockout threshold: Xác định số lần cố gắng đăng nhập nhưng không thành công. Trong trường hợp này Account sẽ bị khóa. Trong trường hợp này Account sẽ bị khóa. Việc mở khóa chỉ có thể thực hiện bởi người quản trị hoặc phải đợi đến khi thời hạn khóa hết hiệu lực. Có thể thiết lập giá trị cho số lần đăng nhập sai từ 1 đến 999. Trong trường hợp thiết lập giá trị 0, account sẽ không bị khóa.

– Reset account lockout counter after: Thiết lập lại số lần cố gắng đăng nhập về 0 sau một khoảng thời gian quy định. Thiết lập này chỉ có hiệu lực khi *"Account lockout threshold"* được thiết lập.

2. Local Policy: các chính sách cục bộ.

– User rights Assignments: Ấn định quyền cho người dùng.

Quyền của người dùng ở đây bao gồm các quyền truy cập, quyền backup dữ liệu, thay đổi thời gian cho hệ thống….

Trong phần này để cấu hình cho một mục nào đó, click đúp chuột lên mục và click Add user or group để trao quyền mặc định cho user hoặc group theo yêu cầu.

+ Access this computer from the network: Với những kẻ tò mò, tốt nhất chúng ta không cho phép chúng truy cập vào máy tính của mình. Với thiết lập này ta có thể tùy ý thêm, bớt quyền truy cập vào máy cho bất ký tài khoàn nào hoặc nhóm nào.

+ Act as part of the operating system: Chính sách này chỉ định tài khoản nào sẽ được phép hoạt động như một phần của hệ thống. Mặc định Administrator có quyền cao nhất, có thể thay đổi bất kỳ thiết lập nào của hệ thống, được xác nhận như bất kỳ một người dùng, vì thế có thể sử dụng tài nguyên hệ thống như bất kỳ người dùng nào. Chỉ có những dịch vụ chứng thực ở mức thấp mới yêu cầu đặc quyền này.

+ Add workstation to domain: Thêm một tài khoản hoặc nhóm vào miền. Chính sách này chỉ hoạt động trên hệ thống sự dụng Domain Controller. Khi được thêm vào miền, tài khoản này sẽ có thêm các quyền hoạt động trên dịch vụ thư mục (Active Directory), có thể truy cập tài nguyên mạc như một thành viên trong domain.

+ Adjust memory quotas for a process: Chỉ định những ai được phép điều chỉnh chi tiêu bộ nhớ dành cho một quá trình xử lý. Chính sách này có làm tăng hiệu suất hệ thống nhưng nó có thể bị lạm dụng phục vụ cho những mục đích xấu như tấn công từ chối dịch vụ DoS (Dial of Service).

+ Allow logon through Terminal Services: Terminal services là một dịch vụ cho phép đăng nhập từ xa đến máy tính. Chính sách này sẽ quyết định giúp chúng ta những ai được phép sử dụng dịch vụ Terminal services để đăng nhập hệ thống.

+ backup files add directories: Tương tự như các chính sách trên, ở đây cấp phép ai đó có quyền backup dữ liệu.

+ Change the system time: Cho phép người sử dụng nào có quyền thay đổi thời gian của hệ thống.

+ Create global objects: Cấp quyền cho ai có thể tạo ra các đối tượng dùng chung.

+ Force shutdown from a remote system: Cho phép ai có quyền tắt máy qua hệ thống điều khiển từ xa.

+ Shutdown the system: Cho phép ai có quyền shutdown máy.

+ Deny access to this computer from the net…: Cấm user không được phép truy xuất đến máy.

+ Deny logon localy: Cấm User Logon cục bộ.

+ Deny logon through Terminal Services: Cấm User Remote Desktop.

+ Logon localy: Thiết lập người dùng Logon cục bộ.

– Security Options:

+ Account: Administrator account status: Trạng thái hoạt động của Administrator.

+ Account: Guest account status: Trạng thái hoạt động của User Guest.

+ Account: Limit local account use of blank password to console: Đăng nhập không cần password.

+ Account: Rename administrator account: Đổi tên Administrator.

+ Account: Rename guest account: Đổi tên Guest.

+ Devices: Prevent users from installing printer drivers: Không cho phép cài Printer

+ Devices: Restrict CD-ROM access to localy logged-on user only: Cấm truy nhập xa từ CD-ROM.

+ Interactive: Do not require CTRL + ALT + DEL: Bỏ Ctrl + alt + Del

+ Interactive: Message text for users attempting to logon: Đặt tiêu đề khi logon.

+ Interactive: Message title for users attempting to log on: Đặt tiêu đề khi logon

+ Interactive: Number of previous logons to cache in cache: Cache kho logon

+ Shutdown: Allow system to be shut down

+ Shutdown: Allow system to be shut down without having to log on: Shutdown không cần logon.

+ Shutdown: Clear virtual memory pagefile. Xóa bộ nhớ ảo khi Shutdown.

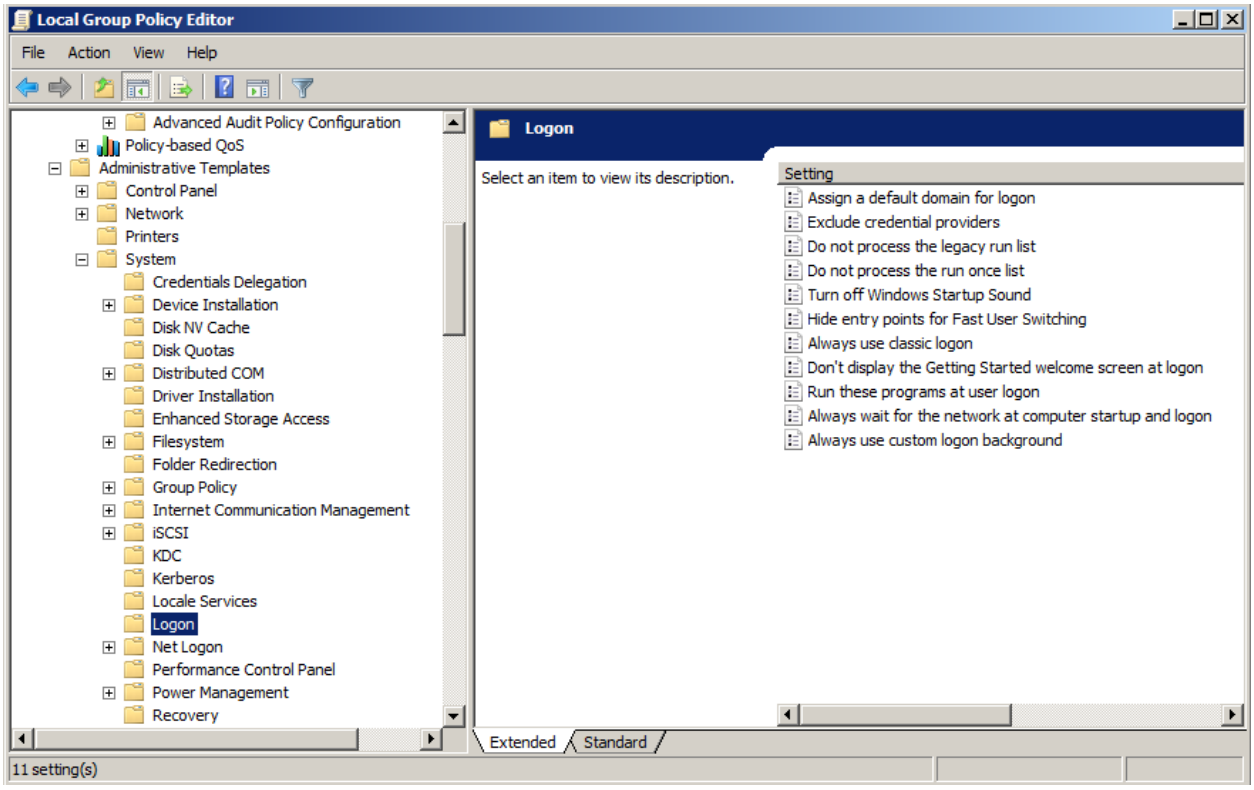
-Administrator Templates -> Windows Components -> Intenet Explorer (IE)

+ Security Zones: Use only machine settings: Bắt buộc tất cả các User đều chung một mức độ Security như nhau.

+ Security Zones: Do not allow users to change policies: Trong Security Zone có danh sách các Site nguy hiểm do người dùng thiết lập, Enable tùy chọn sẽ không co thay đổi danh sách đó (Tốt nhất là giấu thẻ Security).

+ Disable Periodic Check for Internet Explorer software updates: Ngăn không cho IE tự động Update.

-Administrator Templates -> System -> Logon



+ Don’t display the Getting Started welcome screen at logon: Ẩn màn hình Welcome khi User đăng nhập vào hệ thống.

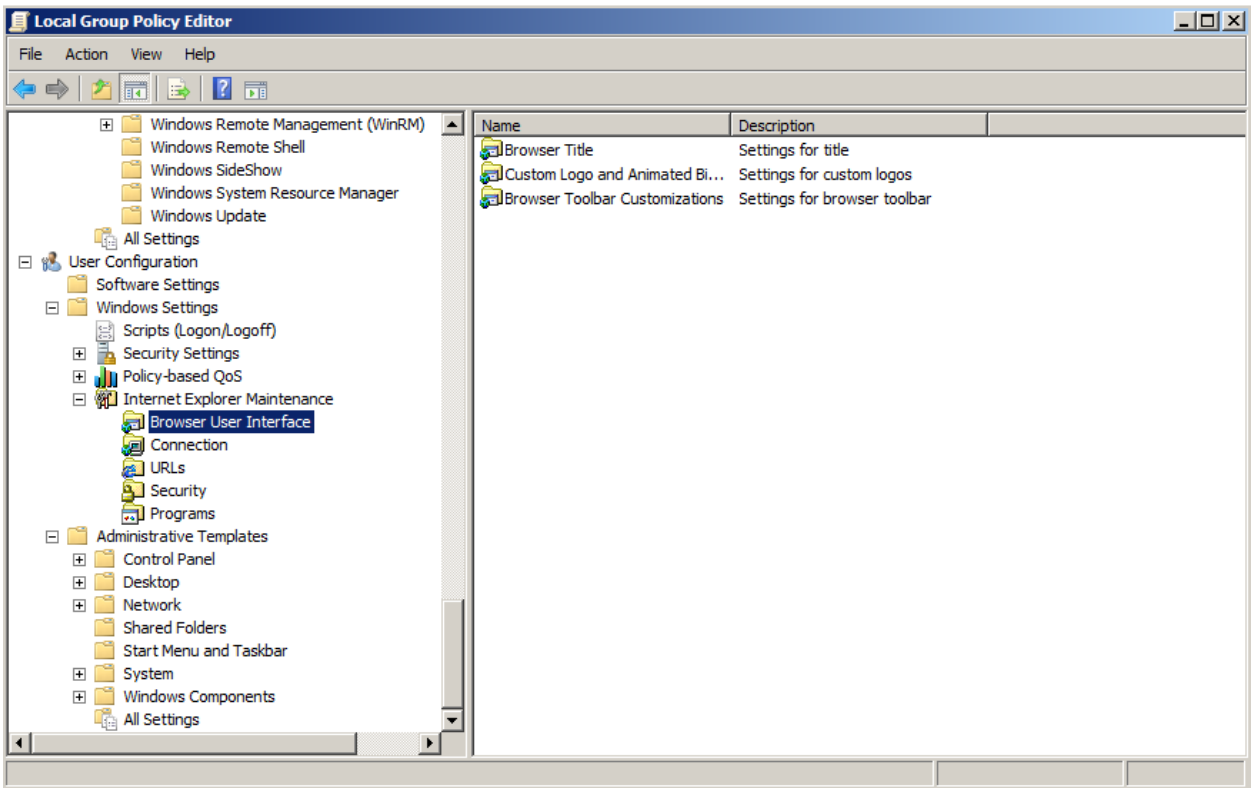
-Computer Configuration -> Policies – > Administrative Templates – > System -> System Restore.

+ Turn off System Restore: Tắt System Restore, khi user gọi System Restore thì xuất hiện thông báo "System Restore has been turn off by group policy. To turn on System Restore, contact your domain Administrator".

+ Turn off Configuration: Chỉ có tác dụng khi System Restore được kích hoạt, tính năng này vô hiệu hóa phần thiết lập cấu hình của System Restore.

Phần II: User configuration

-User configuration – >Windows Setting – > Internet Explorer Maintenance – > Browse User Interface.

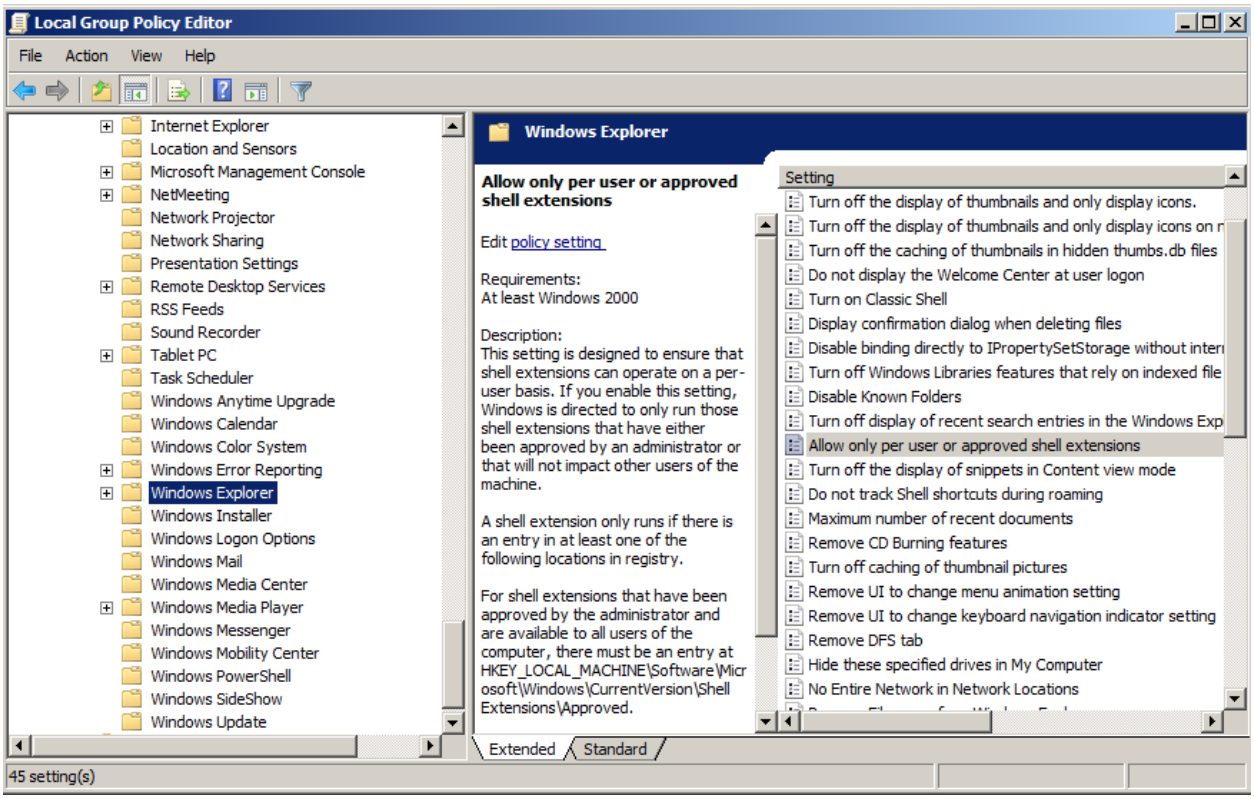


+ Browser Title: Thay đổi tiêu đề nội dung IE

+ Custom Logo: Thay đổi logo của IE (Chỉ hỗ trợ file BMP có 16-256 màu và kích cỡ 22×22 hoặc 38×38).

+ Browse Toolbar Customizations: Thay đổi Toolbar cho IE.

-User configuration – > Administrator Templates – > Windows Components – > Windows Expolorer



+ **Maximum number of recent documents:** Quy định số lượng tài liệu đã mở hiển thị trong My Recent Documents.

+ **Do not move deleted files to the Recycle Bin:** File bị xóa sẽ không được đưa vào Recycle Bin.

+ **Maximum allowed Recycle Bin size:** Giới hạn dung lượng Recycle Bin, tính bằng đơn vị phần trăm dung lượn của ổ đĩa cứng.

+ **Removes the Folder Options menu item from the Tools menu.** Ẩn Folder Option.

+ **Remove Search button from Windows Expolorer**. Ẩn Search trong Explorer.

+ **Remove Windows Explorer's default context menu**. Ẩn context khi click chuột phải.

+ **Hides the manage item the Windows Expolorer context**. Ẩn manage khi click chuột phải vào My Computer.

+ **Hide these specfied drivers in My Computer.** Ẩn ổ đĩa (access qua Addresss).

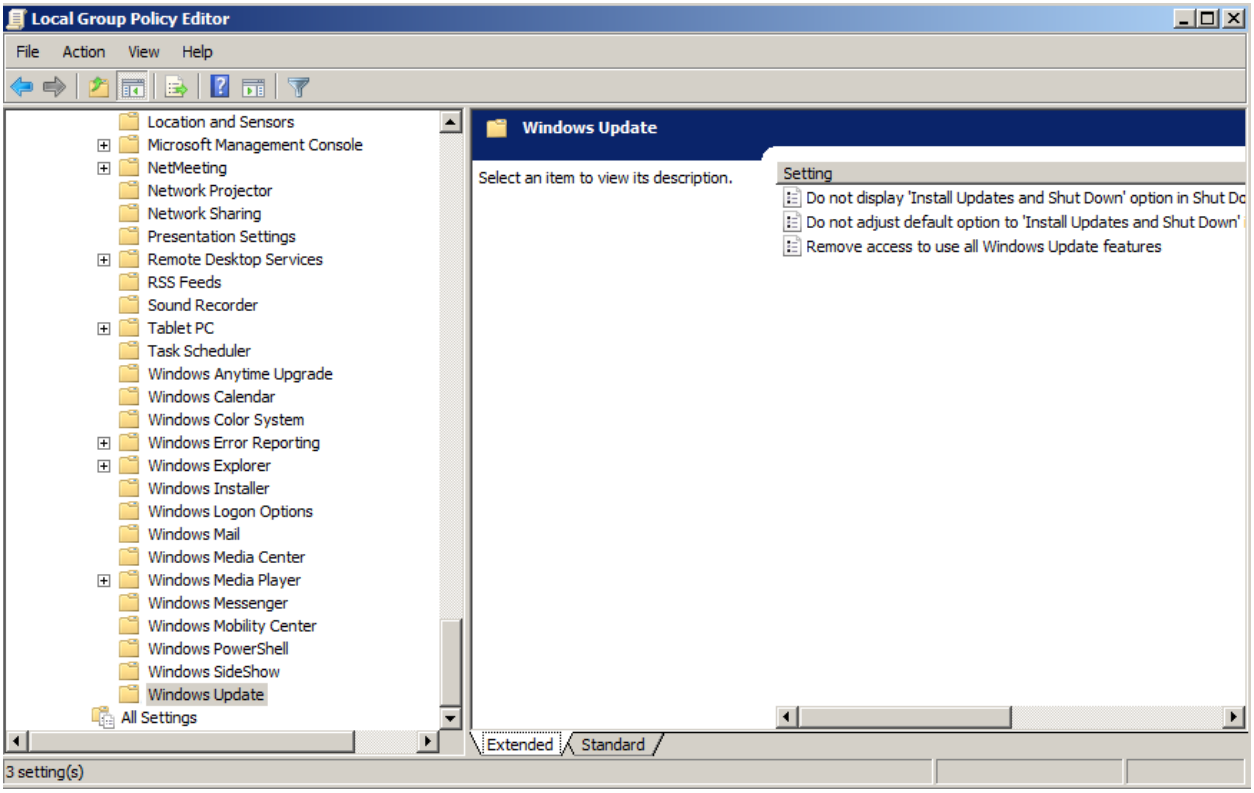
+ **Prevent access to drivers from My Computer**. Ngăn truy cập các ổ đĩa.

+ Remove Hardware tab. Ẩn tab Hardware.

+ Remove DFS tab. Ẩn tab DFS.

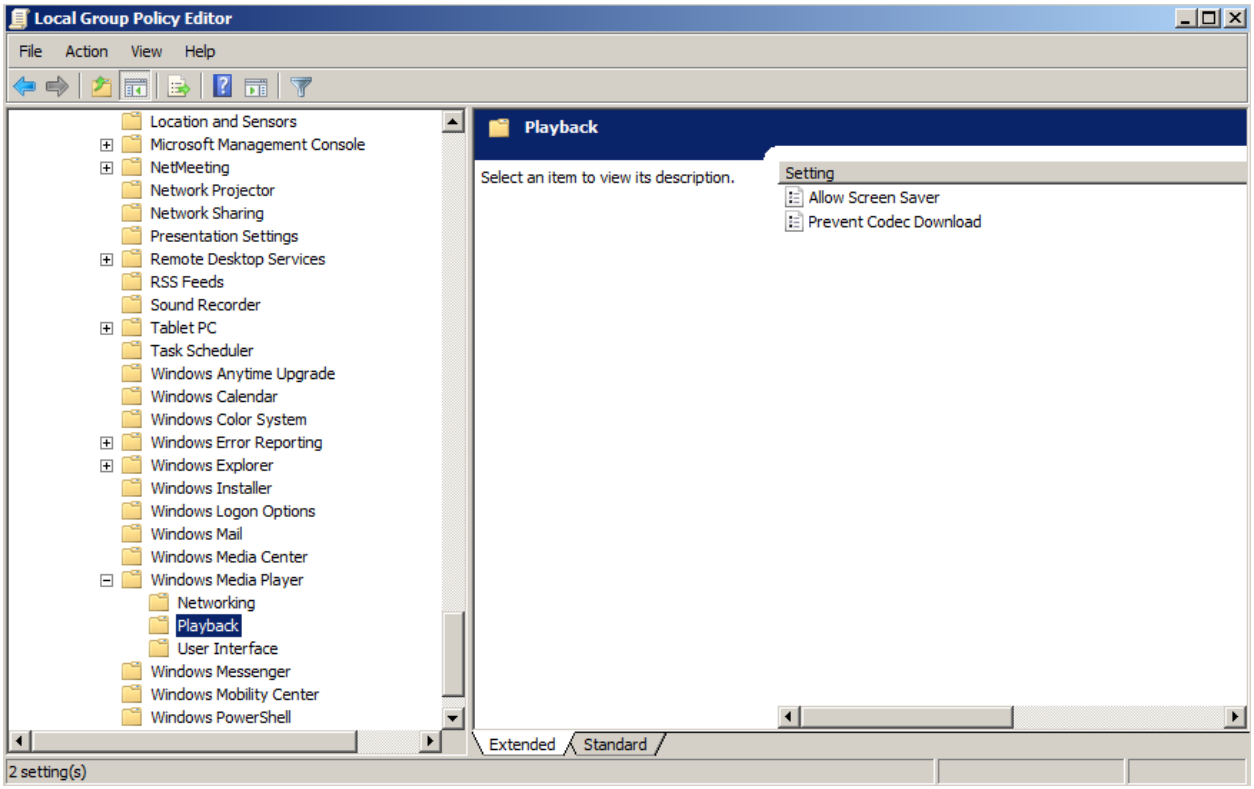
+ Remove Security tab. Ẩn tab Security.

-User configuration – > Administrator Templates – > Windows Components – > Windows Update



+ Remove access to use all Windows Update features : Cấm tải các bản cập nhật.

-User configuration – > Administrator Templates – > Windows Components – > Windows Media Player – > Playback



+ **Prevent Codec Download:** Ngăn không cho Windows Media Player tự động tải các codec.

+ **Allow Screen Saver:** Cho phép thiếp lập màn hình giao diện Windows Media Player.

Điều khiển đặc quyền tài khoản Administrator

Bạn có thể điều khiển các tài khoản để biết chúng có khả năng làm những gì và được phép truy cập những gì ?

Vì sao lại là điều khiển tài khoản Administrator ?

Có rất nhiều lý do cần kiểm soát tài khoản này. Đầu tiên, trên mỗi mạng, dù trung bình hay lớn cũng có thể có hàng nghìn tài khoản Administrator. Khả năng chúng vượt ra ngoài tầm kiểm soát là hoàn toàn có thực. Thứ hai, hầu hết các công ty đều cho phép "người dùng tiêu chuẩn" truy cập tài khoản Administrator cục bộ, có thể dẫn đến nguy cơ rủi ro hay tai nạn nào đó. Thứ ba, tài khoản administrator nguyên bản ban đầu sẽ buộc phải dùng một cách dè dặt. Vì vậy, giới hạn đặc quyền là một cách thông minh để quản lý hệ thống mạng trong doanh nghiệp.

Giới hạn đặc quyền đăng nhập

Chúng ta không làm được gì nhiều để giới hạn vật lý đặc quyền đăng nhập các tài khoản Administrator. Tuy nhiên không nên để chúng được sử dụng thường xuyên, cơ bản hàng

ngày. Cần giới hạn chúng bằng cách hạn chế số người dùng biết mật khẩu. Với tài khoản Administrator liên quan đến Active Directory, tốt hơn hết là không để cho người dùng nào biết toàn bộ mật khẩu. Điều này có thể thực hiện dễ dàng với hai tài khoản Administrator khác nhau, chỉ nhập một phần mật khẩu, và dùng một tài liệu dẫn dắt đến các phần chưa mật khẩu đó. Nếu tài khoản chưa cần phải dùng đến, cả hai phần dữ liệu của mật khẩu có thể được giữ nguyên. Một lựa chọn khác là sử dụng chương trình tự động tạo mật khẩu, có thể tạo ra mật khẩu tổng hợp.