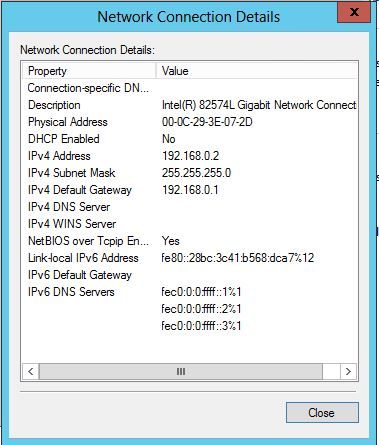


* Trước hết cần cấu hình IP tĩnh cho máy: 

Server:192.168.1.2

255.255

192.168.1.1

192.168.1.2

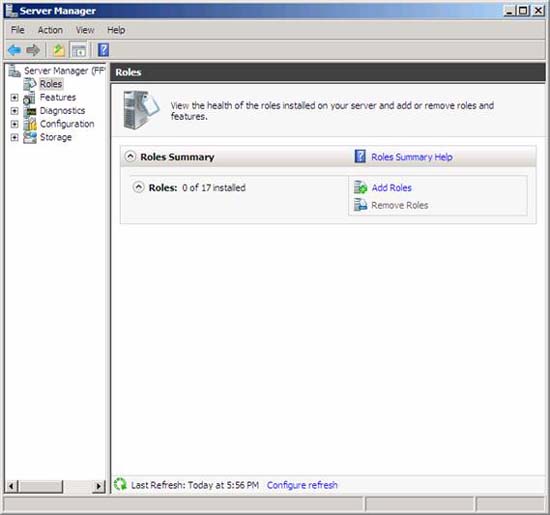
User: 192.168.1.4

255

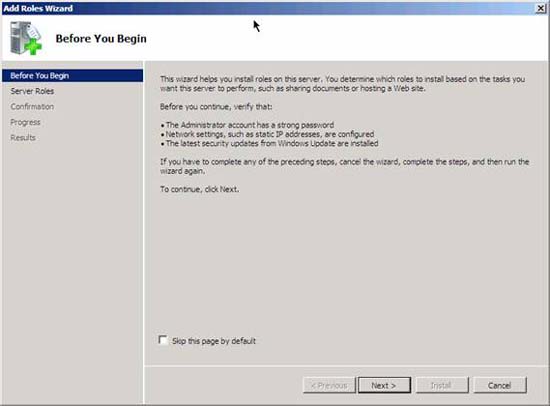
192.168.1.1

192.168.1.2

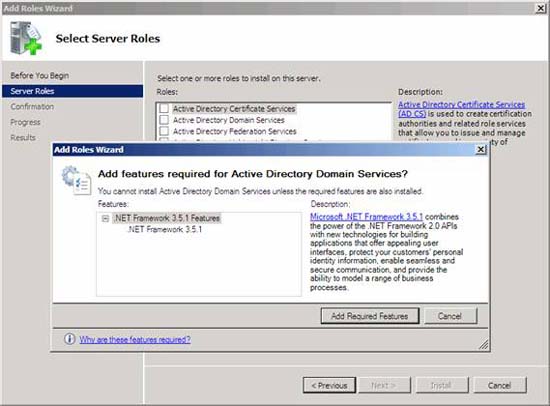
Vào **Server Manager** và kích nút **Roles** trong panel bên trái của giao diện điều khiển. Sau đó kích vào liên kết **Add Roles** trong phần panel bên phải.



Thao tác đó sẽ làm xuất hiện trang **Before You Begin** khi đó hãy kích **Next**để tiếp tục.

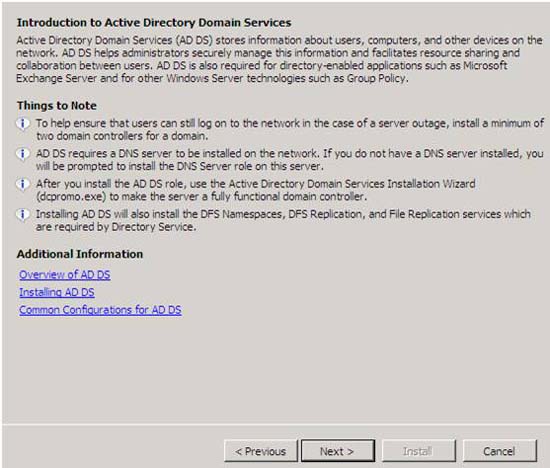
  
Hình 13

Ở đây bạn chọn những Server Roles gì mà mình muốn cài đặt. Chúng tôi sẽ cài đặt các Server Role khác sau, tuy nhiên chúng tôi muốn cài đặt DC role trước. Chọn **Active Directory Domain Services** bằng cách đặt một dấu tích vào hộp kiểm. Lưu ý rằng wizard sẽ hiển thị cho bạn số lượng các tính năng sẽ được cài đặt cùng với Active Directory Server Role. Kích nút **Add Required Features** để cài đặt thêm các tính năng này với Active Directory Server Role.

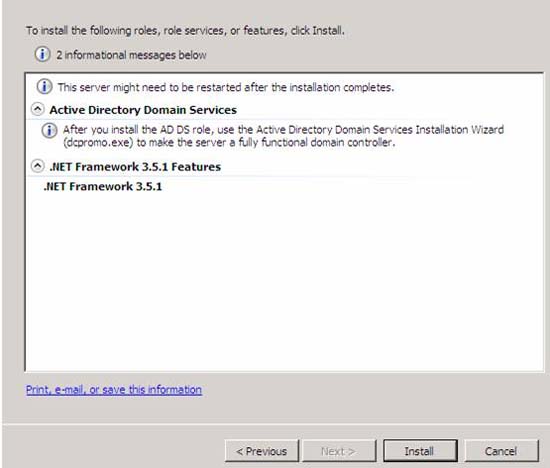
  
Hình 14

Sau khi chọn Active Directory DC Server Role, bạn sẽ thấy các thông tin về Server Role. Một số điều cần lưu ý ở đây là:

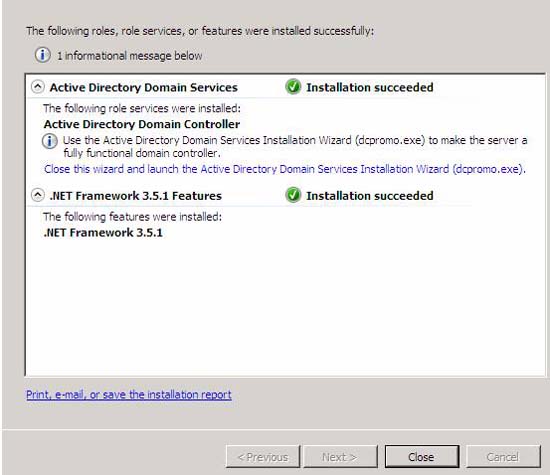
* Bạn nên cài đặt tối thiểu hai DC trên mạng của mình để tự động chuyển đổi dự phòng. Việc cài đặt một DC trên một mạng rất dễ dẫn đến thảm họa.
* Yêu cầu DNS. Tuy nhiên khi chạy **dcpromo**, chúng ta sẽ cài đặt DNS server role để hỗ trợ cho các dịch vụ Active Directory.
* Bạn cần chạy **dcpromo** sau khi cài đặt role. Bạn sẽ không phải truy cập vào các bước mở rộng giống như khi cài đặt các role máy chủ khác, toàn bộ quá trình cài đặt role có thể được thực hiện thông qua Manager. Active Directory Domain Services role chỉ là một trong các role cần đến hai bước để cài đặt.
* Lưu ý rằng việc cài đặt Active Directory Domain Services Role cũng kéo theo cài đặt S Namespaces, DFS Replication và File Replication Services – tất cả đều được sử dụng bởi Active Directory Domain Services vì vậy chúng sẽ được cài đặt một cách tự động.

  
Hình 15

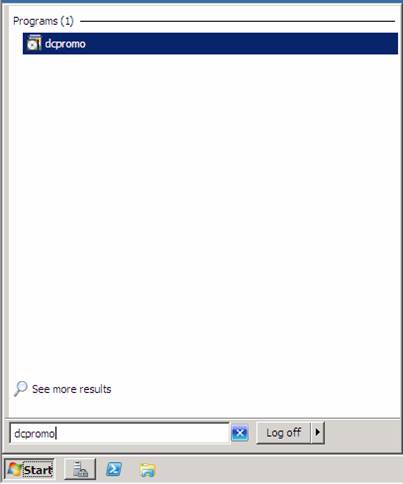
Kích **Install** để cài đặt các file yêu cầu nhằm chạy **dcpromo**.

  
Hình 16

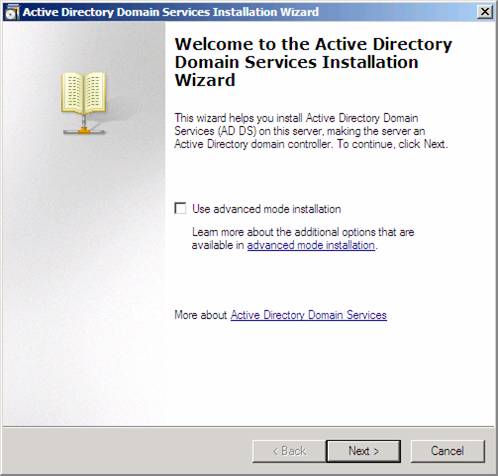
Cài đặt được thực hiện thành công. Kích **Close**.

  
Hình 17

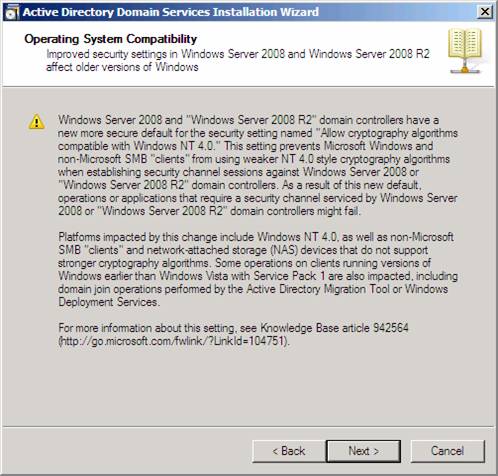
Lúc này hãy vào menu **Start**, đánh **dcpromo** vào hộp tìm kiếm. Khi đó bạn sẽ tìm thấy nó trong danh sách như thể hiện trong hình bên dưới. Kích **dcpromo**.

  
Hình 18

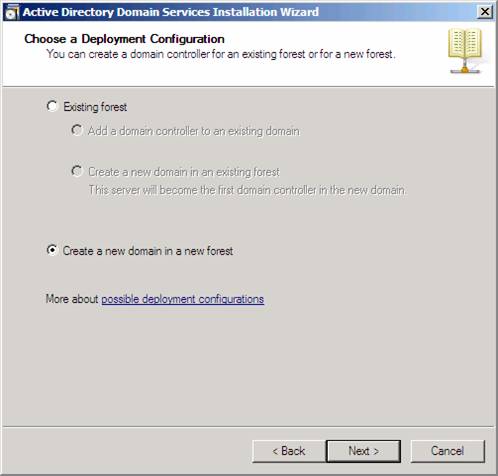
Thao tác này sẽ khởi chạy **Welcome to the Active Directory Domain Service Installation Wizard**. Chúng ta không cần các tùy chọn nâng cao trong kịch bản này, chính vì vậy chỉ cần kích **Next**.

  
Hình 19

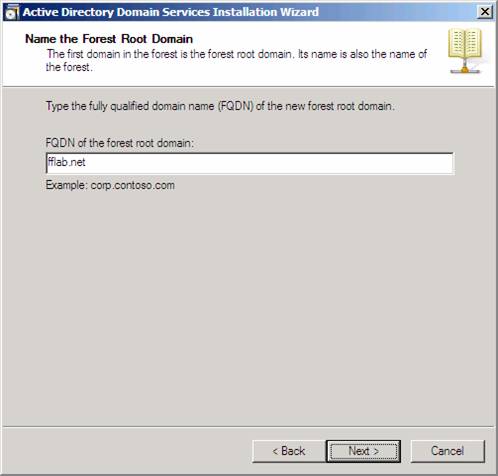
Trong trang **Operating System Compatibility**, bạn sẽ được cảnh báo rằng các máy khách NT và non-Microsoft SMB sẽ gặp các vấn đề với một số thuật toán mật mã được sử dụng bởi Windows Server 2008 R2. Chúng ta không có vấn đề này trong mạng thử nghiệm, chính vì vậy hãy kích **Next**.

  
Hình 20

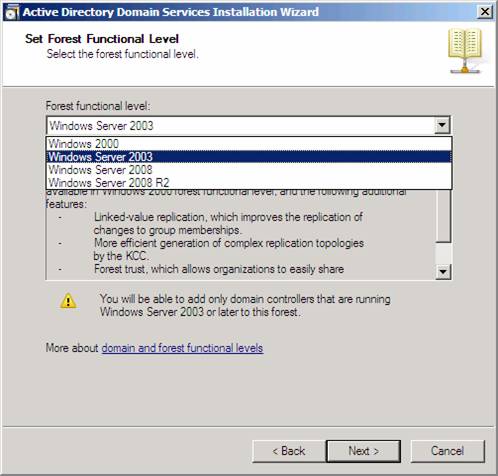
Trong trang **Choose a Deployment Configuration**chọn tùy chọn **Create a new domain in a new forest.**Chúng ta thực hiện như vậy vì đây là một miền mới nằm trong một forest mới.

  
Hình 21

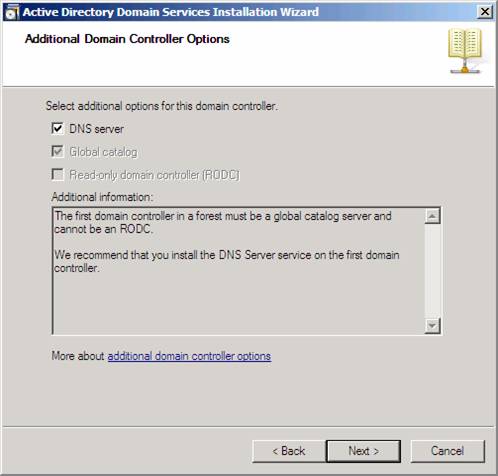
Trong trang **Name the Forest Root Domain**, nhập vào tên của miền trong hộp nhập liệu **FQDN of the forest room domain**. Trong ví dụ này chúng tôi sẽ đặt tên cho miền là **fflab.net**. Tuy nhiên các bạn có thể đặt bất cứ tên nào tùy chọn ý thích của mình. Kích **Next.**

****  
Hình 22

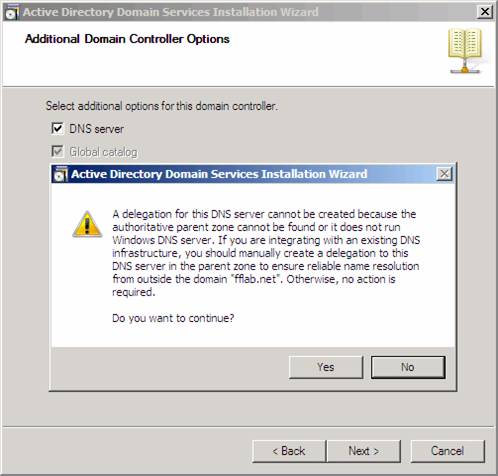
Trong trang **Set Forest Functional Level**, chọn tùy chọn **Windows Server 2008 R2**(không phải tùy chọn như bạn thấy trong hình bên dưới). Ở đây chúng tôi muốn chọn tùy chọn để chúng ta có thể lợi dụng tất cả các tính năng mới thú vị có trong Windows Server 2008 R2. Kích **Next**.

  
Hình 23

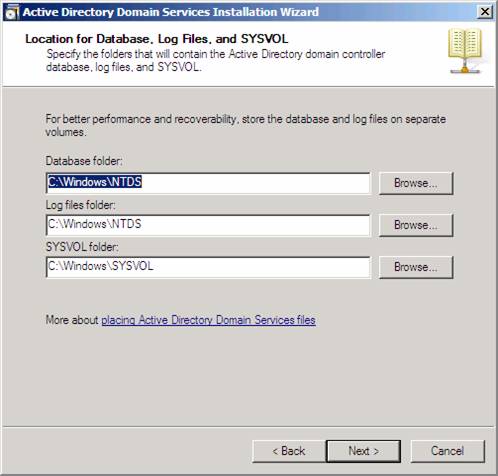
Trong trang **Additional Domain Controller Options**, chúng ta chỉ có một lựa chọn đó là **DNS server**. Tùy chọn Global catalog được tích mặc định vì đây chỉ là một DC trong miền này, vì vậy nó phải là một máy chủ Global Catalog. Tùy chọn Read-only domain controller (RODC) bị hủy chọn vì bạn phải có một non-RODC khác trong mạng để kích hoạt tùy chọn này. Chọn tùy chọn **DNS server** và kích **Next**.

  
Hình 24

Một hộp thoại sẽ xuất hiện nói răng không thể tạo đại biểu cho máy chủ DNS này vì không thể tìm thấy vùng xác thực hoặc nó không chạy Windows DNS server. Lý do cho điều này là vì đây là DC đầu tiên trên mạng. Bạn không nên lo lắng về điều này và chỉ cần kích **Yes** để tiếp tục.

  
Hình 25

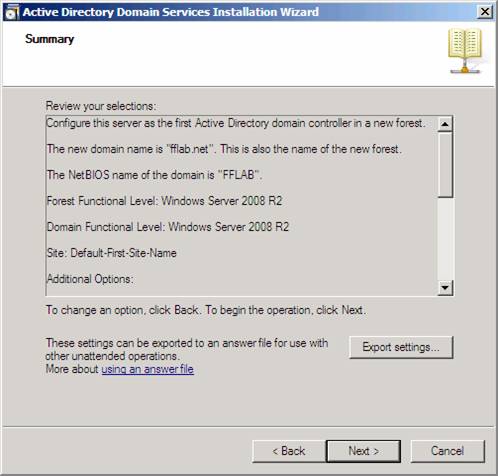
Để lại thư mục Database, Log Files và SYSVOL trong các location mặc định của chúng và kích **Next**.

  
Hình 26

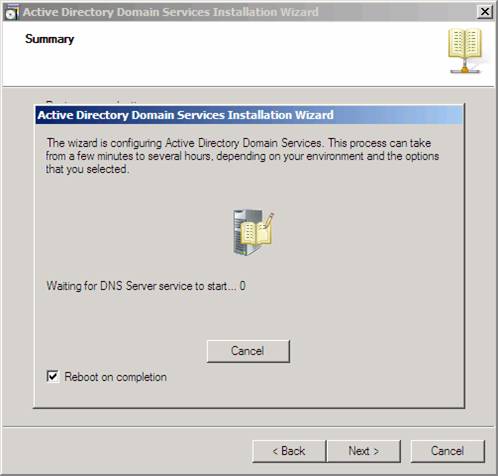
Trong **Directory Service Restore Mode Administrator Password**, nhập một mật khẩu mạnh vào các hộp nhập liệu **Password** và **Confirm password.**

  
Hình 27

Xác nhận các thông tin trên trang **Summary** và kích **Next**.

  
Hình 28

Active Directory sẽ cài đặt. DC đầu tiên sẽ cài đặt khá nhanh. Đặt một dấu kiểm vào hộp chọn **Reboot on completion** để máy tính sẽ tự động khởi động lại khi cài đặt DC được hoàn tất.

  
Hình 29

Máy tính sẽ tự động khởi động lại vì chúng ta đã chọn tùy chọn đó. Cài đặt sẽ hoàn tất khi bạn đăng nhập. Với Windows Server 2008 bạn sẽ thấy một số cấu hình xảy ra khi đã đăng nhập, tuy nhiên điều này không xảy ra với Windows Server 2008 R2.

Dịch vụ DNS đã được cài đặt trong quá trình cài đặt Active Directory, chính vì vậy chúng ta không cần lo lắng về nó. Có một vài dịch vụ khác mà chúng ta nên cài đặt trên miền này đó là:

* DHCP
* WINS
* Enterprise Certificate Services

Tuy nhiên, chỉ có DHCP và Certificate Services được xem như các “role” còn WINS được xem như một tính năng.

I. Giới thiệu

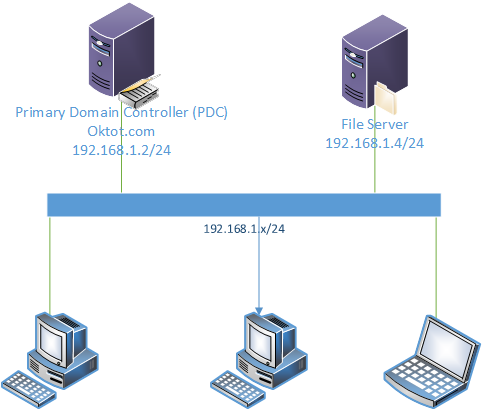
Sau khi xây dựng thành công máy chủ [Domain Controller trên Windows Server 2016](https://sinhvientot.net/xay-dung-domain-controller-tren-windows-server-2016-2012-2008-2003/) và tiến hành join các máy clients vào Domain. Ở bài viết này sinhvientot.net sẽ giới thiệu đến các bạn cách tạo user, OU và phân quyền quản lý OU([Organizational Unit](https://sinhvientot.net/tong-quan-ve-active-directory/)) trên Windows Server 2016.

**Tạo các tài khoản người dùng theo OU tương ứng với phòng ban**

* **Ban giám đốc**: Nguyễn Văn Tâm, Trần Văn Phú
* **Hành chánh**: Nguyễn Đức Hoàng, Nguyễn Xuân Sang
* **Kế toán**: Trần Thái Hà, Lê  Minh Hoàng
* **Kinh doanh**: Vũ Huy Hoàng, Nguyễn Thị Diệu, Nguyễn Đức Hùng
* **Thiết kế**: Trần Thanh Bình, Nguyễn Thị Phùng Anh, Đăng Thanh Tùng, Nguyễn Phi Thái, Trần Thành Nam, Võ Thị Tuyết, Trần Thanh Thủy, Lê Hải Sơn.
* **Các User gạch chân là user quản lý OU.**

**II. Chuẩn bị**

– 01 máy Windows Server 2016 đã triển khai làm **Primary Domain Controller (PDC)**  
– 01 máy Domain member chạy Windows 7/8/10.  
**Mô hình hệ thống**



**III. Các bước chính**

Bước 1.Mở công cụ Active Directory Users and Computers  
Bước 2.Tạo các OU và User  
Bước 3.Ủy quyền cho các User quản lý OU  
Bước 4.Đăng nhập với quyền User quản lý để kiểm tra

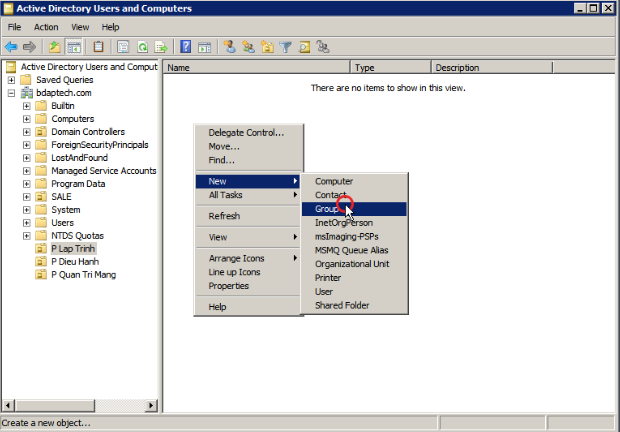
Hướng dẫn tạo Users, OU và phân quyền quản lý OU trên Windows Server 2016/2012/2008/2003

**Tạo tài khoản người dùng và tài khoản nhóm trên miền bdaptech.com. Thiết lập thuộc tính cho các đối tượng người dùng và nhóm như sau:**

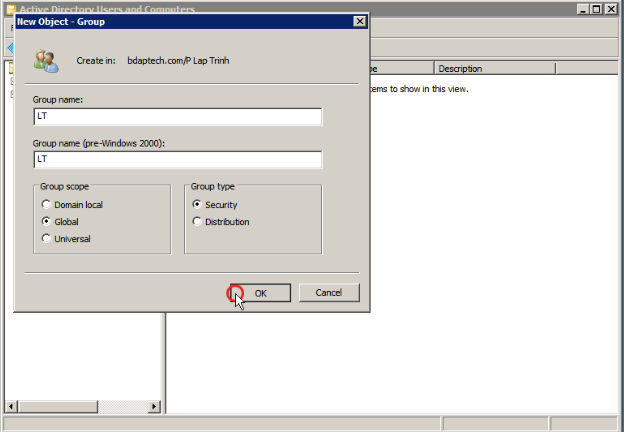
* Tất cả các tài khoản người dùng trên là thành viên nhóm Backup Operator
* Tài khoản người dùng manhnv và tottd phải thay đổi mật khẩu khi đăng nhập vào hệ thống lần đầu tiên
* Người dùng tungnv không được phép đổi mật khẩu từ máy trạm.
* Tạm khóa tài khoản người dùng tungnv vì anh này đi học nước ngoài.
* Nhân viên thuộc nhóm giảng viên chỉ được phép đăng nhập vào mạng từ 7h sáng đến 9h tối mỗi ngày, từ thứ 2 đến thứ 6
* Sử dụng công cụ Active Directory Users and Computers để tạo và quản lý tài khoản người dùng.

**Tạo tài khoản nhóm và tài khoản người dùng:**

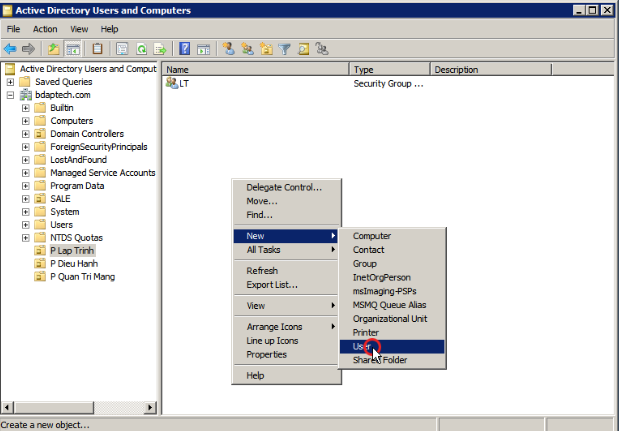
* **Start > Programs > Administrative Tools > Active Directory Users and Computers**. Nhấp phải chuột trên mục **Users > New > Group**.



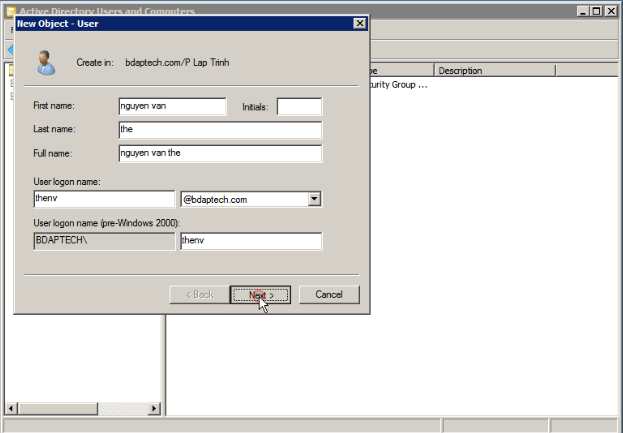
* Tại cửa sổ **New Object – Group** nhập tên nhóm cần tạo và nhấn **OK** để kết thúc.



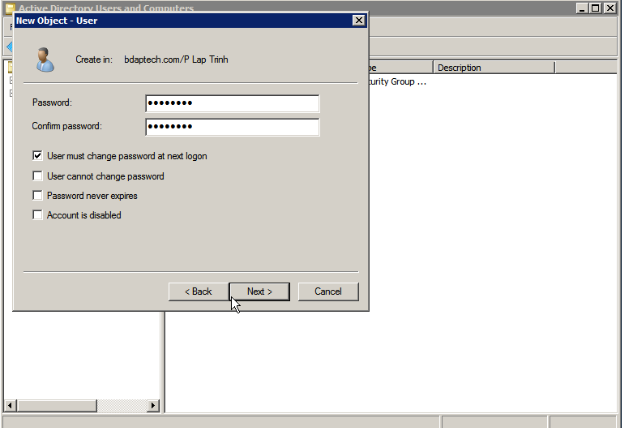
* Tương tự tạo tài khoản nhóm: GG-s-gd.
* **Tạo tài khoản người dùng:** Nhấp phải trên thư mục **User > New > User.**



* Hộp thoại tạo tài khoản người dùng xuất hiện, nhập thông tin và nhấn **Next**



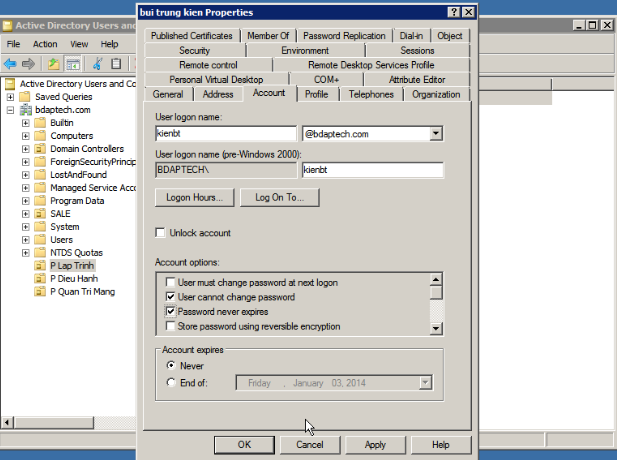
* Tại hộp thoại kế tiếp, nhập thông tin về mật khẩu, nhấn Next. (với tùy chọn **User must change password at next logon** thì người dùng sẽ phải thay đổi mật khẩu khi đăng nhập vào hệ thống lần kế tiếp).
* Tại hộp thoại tiếp theo, nhấn **Finish** để hoàn tất việc tạo tài khoản người dùng.



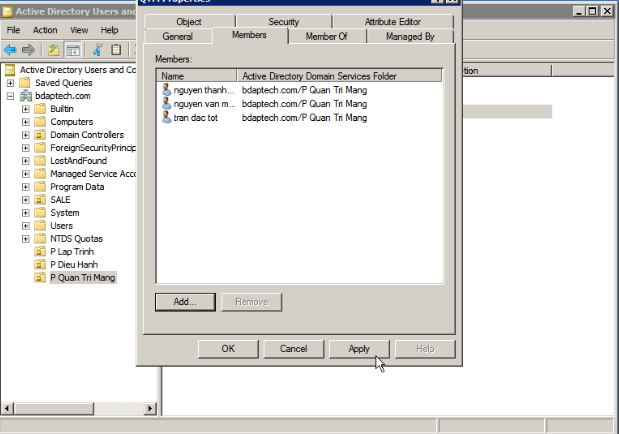
Tương tự cho các user khác.

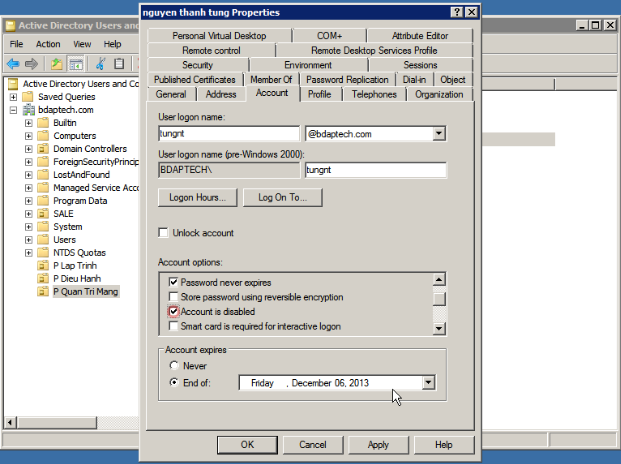
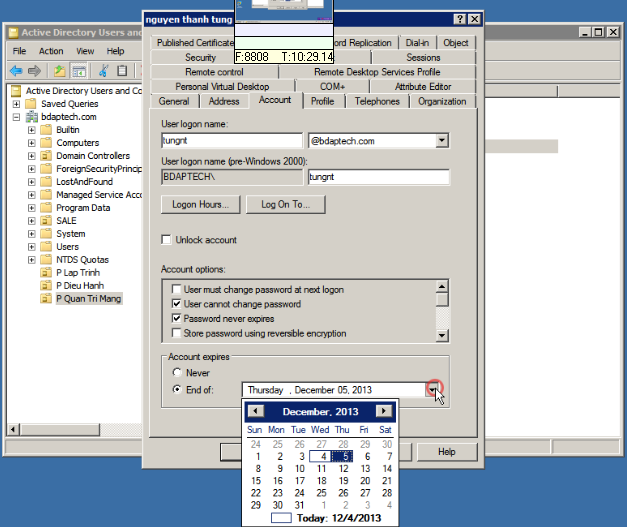
**Thay đổi thuộc tính tài khoản:**

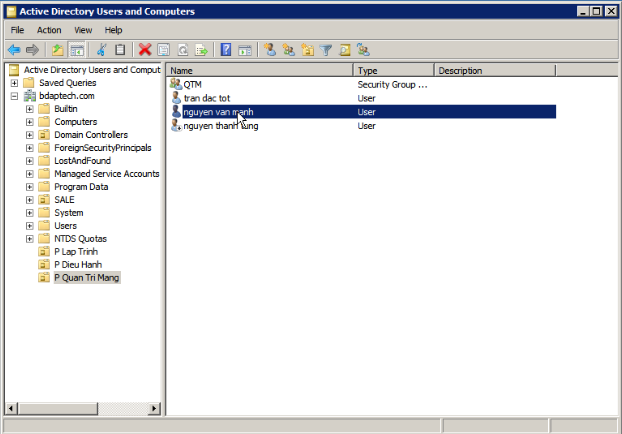
* **Start > Programs > Administrative Tools > Active Directory User and  Computers**> chọn miền **bdaptech.com > Users**
* Phải chuột lên tài khoản người dùng cần thay đổi thông tin, chọn **Properties**, chọn tab **Account.**



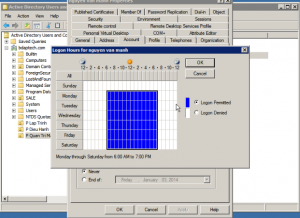
Để thêm tài khoản hoanvq vào nhóm **QTM** và nhóm **Backup Operators** chọn tab **Member of** và chọn **Add** để thêm thông nhóm người dùng cho tài khoản:



* Tương tự,  thực hiện tạo tài khoản cho tài khoản anhln, hungtn và gia nhập vào nhóm cho các User theo yêu cầu đề bài.
* Trên tài khoản **hungtn**, để thiết lập không cho phép thay đổi mật khẩu và khóa tài khoản, trên tab **Account**của tài khoản **hungtn** tick vào **User cannot change password và Account is disabled.**
* Để thiết lập hạn sử dụng cho tài khoản **hungtn**, trong phần **Account expires** tick vào **End of** và thiết lập ngày hết hạn của tài khoản
* Để thiết lập thời gian đăng nhập cho người dùng thuộc nhóm Lập Trình, click chọn các thành viên thuộc nhóm Lập Trình, nhấn phải chọn **Properties**



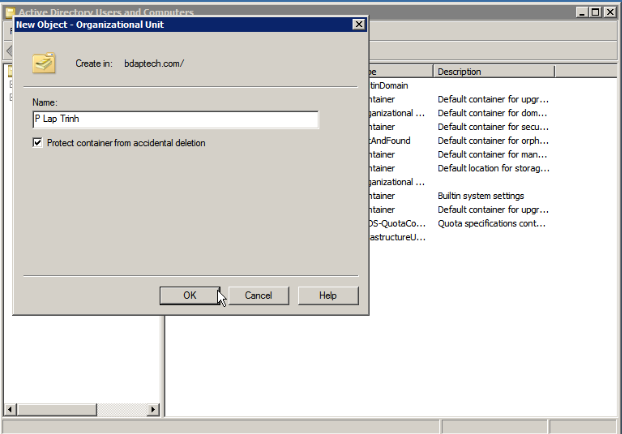
Tại  tab **Account** tick chọn **Logon hours** rồi nhấp vào **Logon hours** để tiếp tục



* Sau khi thiết lập thời gian đăng nhập, nhấn **OK** để kết thúc.

**Tạo OU:**

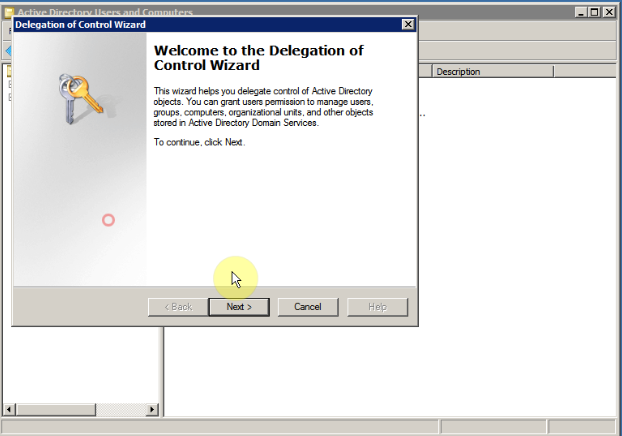
* **Start > Programs > Administrative Tools > Active Directory Users and Computer.**
* Nhấp phải trên domain **bdaptech.com > New > Organizational Unit.**
* Nhập vào OU cần tạo.



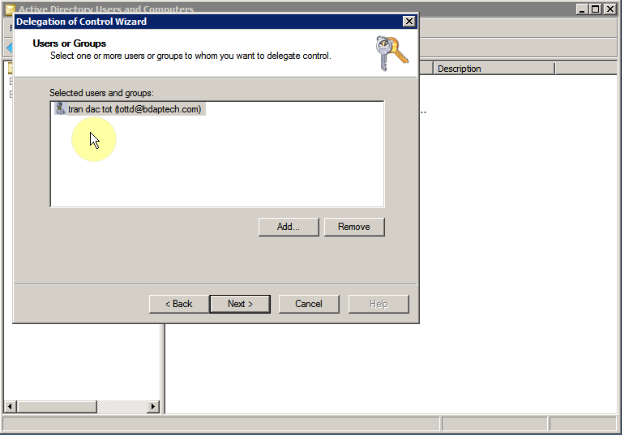
* Tương tự các bạn  tạo các **OU của**phòng ban: **Lập Trình, Quản Trị Mạng, Điều Hành**

**Thiết lập tài khoản có quyền quản trị trên OU:**

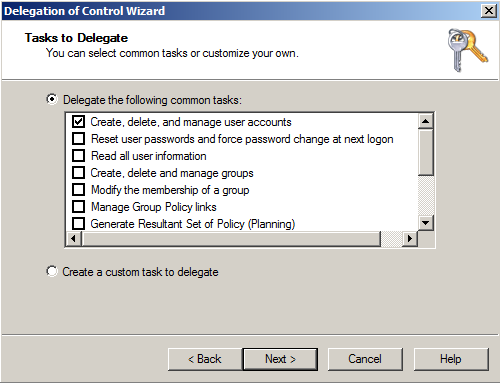
* Nhấp phải trên **OU** cần thiết lập > **Delegate control**, màn hình **Welcome to the Delegation of Control Wizard** xuất hiện, nhấp **Next**.



* Tại màn hình **User or Groups**, nhấp **Add** để thêm vào đối tượng cần thiết lập quyền hạn, nhấn **Next**.



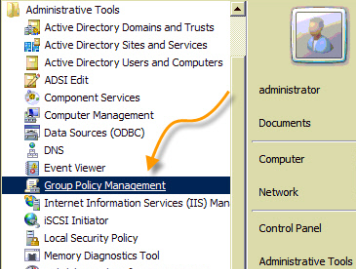
* Tại màn hình **Task to Delegete**, chọn các tác vụ người quản trị được phép thực hiện trên đối tượng OU, sao khi thiết lập xong > nhấn **Next**.



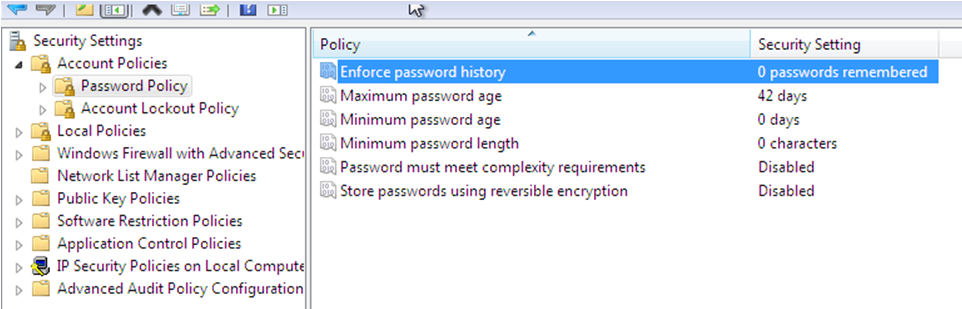
* Tại màn hình **Completing the Delegation of Control Wizard**, nhấn **Finish** để hoàn tất.

# **Cách thiết lập chính sách về mật khẩu trên máy chủ quản lý miền.**

**Đặt vấn đề**  
Một trong những vấn đề mà người quản trị mạng nào cũng cần lưu tâm đó là thiết lập các chính sách về mật khẩu cho hệ thống máy tính mình đang quản lý. Như các bạn đã biết, người dùng thường có thói quen sử dụng mật khẩu một cách không an toàn, ví dụ:  
*- 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.*  
Vậy phải làm thế nào để giải quyết được những vấn đề trên bằng biện pháp kỹ thuật?  
**Giải pháp**  
Bài viết này trình bày tình huống quản trị trong môi trường domain: máy chủ quản lý domain (DC) chạy windows server 2008, các máy trạm chạy hệ điều hành windows 7.  
- Trên DC, truy cập vào mục *Group Policy Management>Default Domain Policy>Chọn Edit> Chọn mục Security Settings*

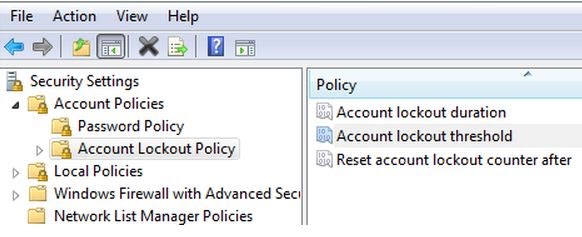
[](https://sites.google.com/a/trungtamdaotao.vn/security/windows-password-policy/group%20policy1.jpg?attredirects=0)

- Truy cập mục Security Settings

[](https://sites.google.com/a/trungtamdaotao.vn/security/windows-password-policy/Security%20Settings.PNG?attredirects=0)​

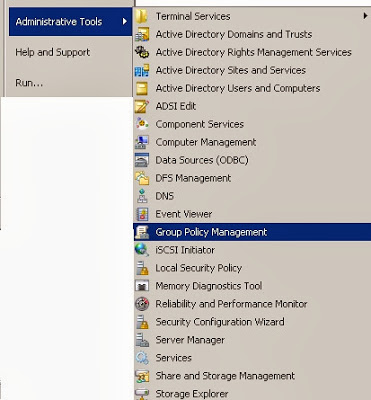
​

- **Thiết lập chính sách mật khẩu mạnh; ngoài ra mật khẩu phải có ít nhất 10 ký tự:**  
Chọn *Password must meet complexity requirements: chọn****Enable*.**  
Chọn *Minimum password length và nhập số****10.***  
  
- **Thiết lập chính sách thay đổi mật khẩu sau 30 ngày**  
Chọn *Maximum password age: nhập số****30***  
  
- **Thiết lập chính sách: người dùng không được sử dụng lại 5 mật khẩu cũ**: Chọn*Enforce password history: nhập số****5***  
  
Lưu ý: người dùng "láu cá", muốn dùng lại mật khẩu cũ, họ có thể đổi mật khẩu mới liên tiếp 5 lần 1 lúc. Đến lần thứ 6, họ đổi lại thành mật khẩu cũ thì hệ thống vẫn chấp nhận. Do đó người quản trị cần khống chế khoảng thời gian: sau 2 ngày mới cho phép đổi mật khẩu. Chọn *Minimum password age: nhập số 2*

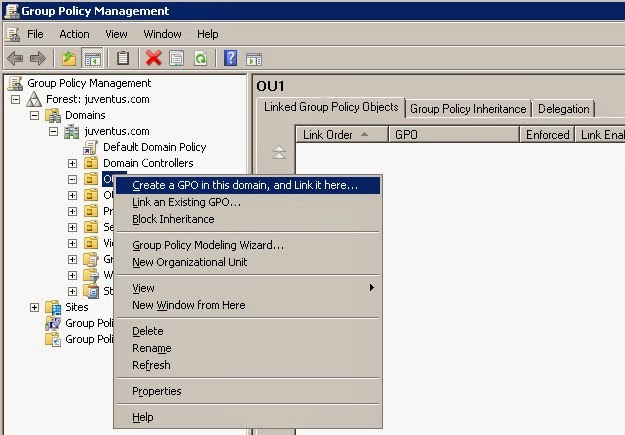
**Trong phần 2 này, mình muốn chia sẻ về chính sách khóa tài khoản**(Account lockout Policy) nhằm giới hạn số lần thử đăng nhập.  
**Trên máy chủ DC, chọn mục Account Lockout Policy**  
  
  
**- Account lockout duration:** xác định thời gian một account bị khóa (phút), cho đến khi tự động được mở lại hoặc được người quản trị mở.  
**- Account lockout threshold:** xác định số lần đăng nhập thất bại dẫn đến việc account sẽ bị khóa.  
**- Reset account lockout counter after:**Khi bạn login vào máy, máy tính sẽ đếm số lần đăng nhập thất bại. Nếu số lần thất bại bằng giá trị A**ccount lockout threshold**thì tài khoản của bạn sẽ bị khóa. Reset account lockout counter after là khoảng thời gian mà bộ đếm sẽ reset về 0, nếu người dùng không thử đăng nhập trong khoảng thời gian đó.  
Lưu ý: thời gian **Reset account lockout counter after**

# [**GPO : Disable USB / CD Drive / Floppy ...with Group Policy Object in a Domain**](http://juventusitprofessional.blogspot.com/2013/10/gpo-disable-usb-cd-drive-floppy-with.html)

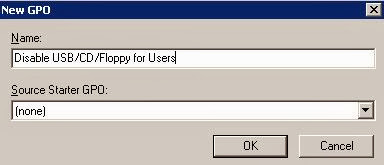
If you want to restrict users in your domain to don't have access to USB or CD-DVD / Floppy drive , you can do it with GPO (Group Policy Object) .  
  
You can assign this GPO to the Users or assign it to Computers.  
  
First open the "**Group Policy Management**" :

[](http://1.bp.blogspot.com/-aH_OOIv68M4/UksbulOCZ9I/AAAAAAAABHI/JjUMQ87BigM/s1600/1.JPG)

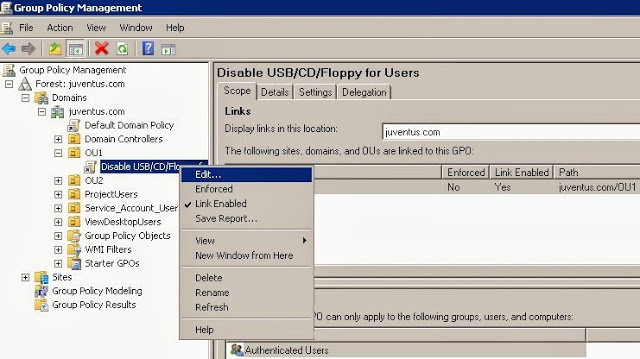
Now select the target that you want to assign the GPO to it : (in this example I select an OU containing some Users)  
Right Click and select : **Create a GPO in this domain,and link it here...**

[](http://3.bp.blogspot.com/-MnMDU_9pOj4/UkscY1PsR8I/AAAAAAAABHQ/IG2FJ356Pt8/s1600/1.JPG)

Now select a name for the new GPO :

[](http://1.bp.blogspot.com/-udN7LsSg4gg/Uksc9d_gHcI/AAAAAAAABHc/Z6n9-r5hqkg/s1600/1.JPG)

Select the created GPO , right click and select "Edit " to open "Group Policy Management Editor"

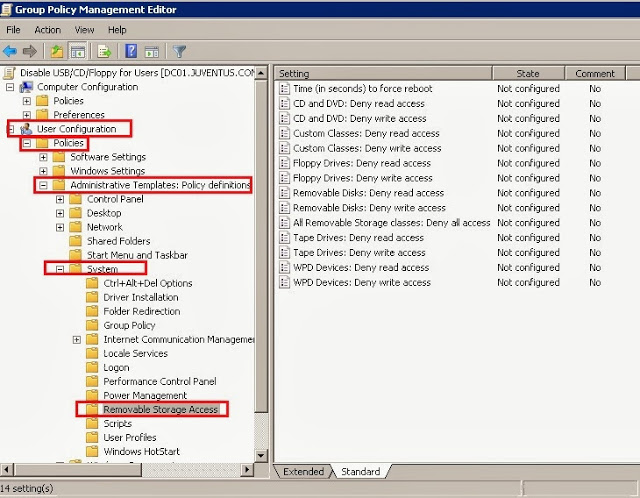
[](http://4.bp.blogspot.com/-U6U6rx7jHr0/UksdfLYKR-I/AAAAAAAABHk/FCi0xsz3YNo/s1600/1.JPG)

Now you have 2 options :  Set & config the GPO for the "Users" or "Computers"  
  
For the Computers :  
**Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access.**

And for Users :

**User Configuration\Policies\Administrative Templates\System\Removable Storage Access**

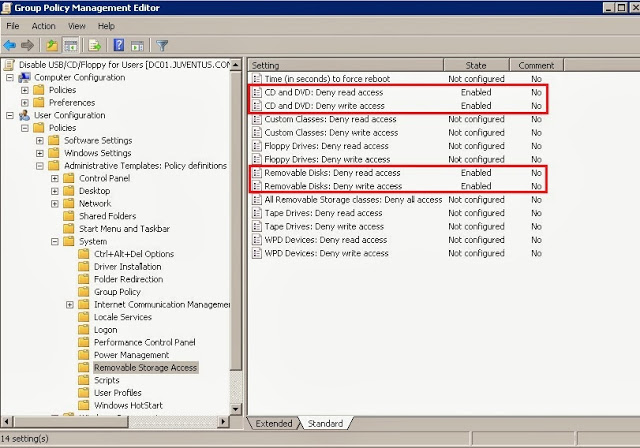
In this example, I will set the GPO for the Users :

[](http://1.bp.blogspot.com/-d8q1kMG2JS8/UksfdgxqcSI/AAAAAAAABHw/UnQKjWsMiOE/s1600/1.JPG)

The most restrictive setting is : **All Removable Storage Classes: Deny All Access**.

But if you prefer to select just the necessary ones and disable them , you can select the other options and Enable them.

I have restricted access to CD & DVD / Removable Disks by enabling the settings in my example :

[](http://2.bp.blogspot.com/-gRwukxkfy58/UkshAns44qI/AAAAAAAABH8/wpfyktxDrV8/s1600/1.JPG)

Also you have the option to disable access to Tape Drives , WPD devices , or disable access to any removable storage.