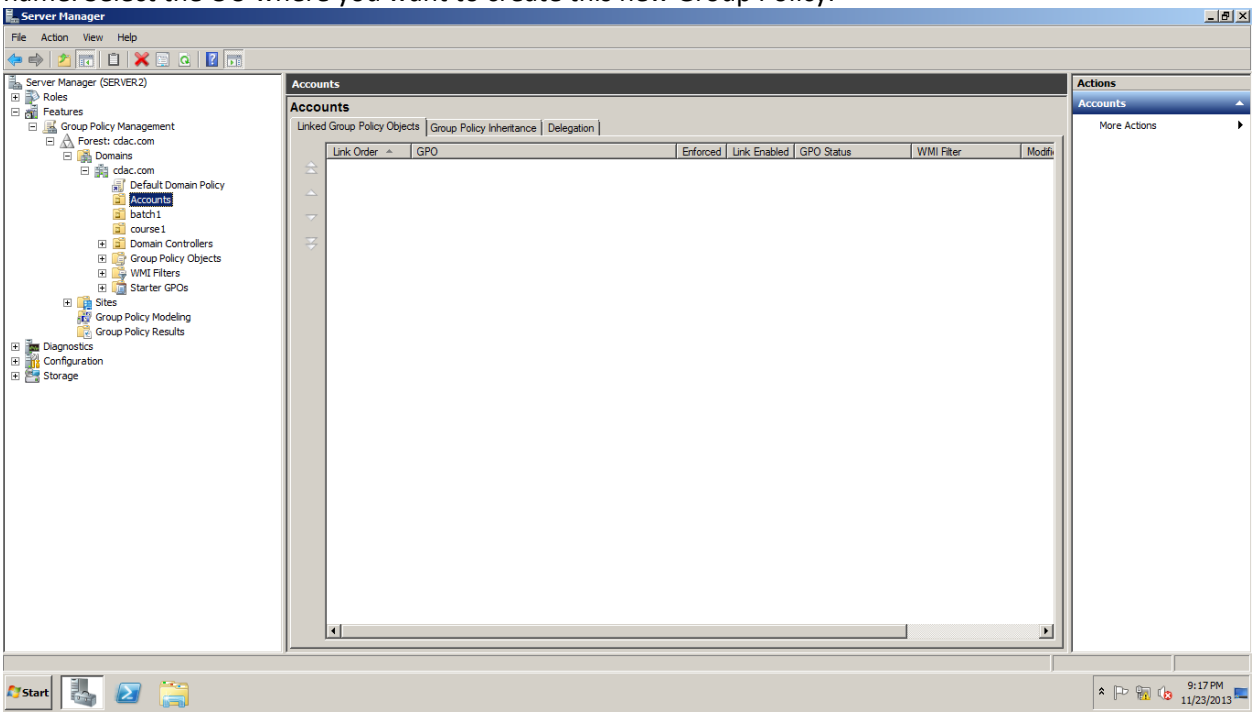
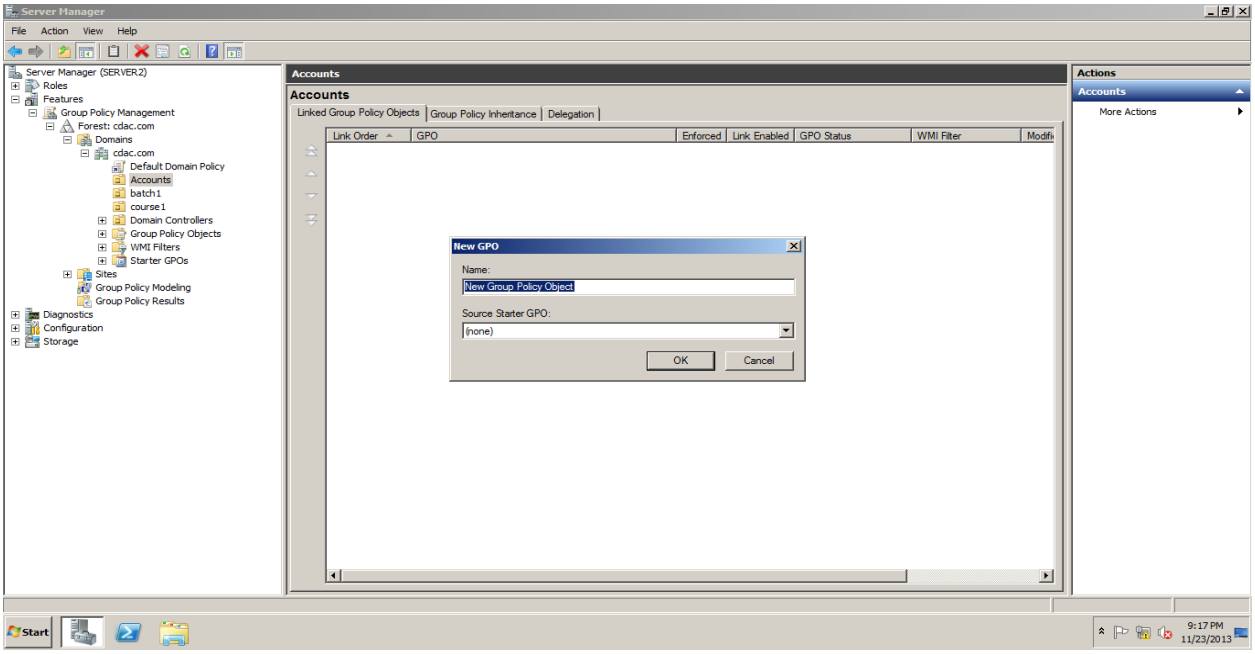
Creating a Group Policy

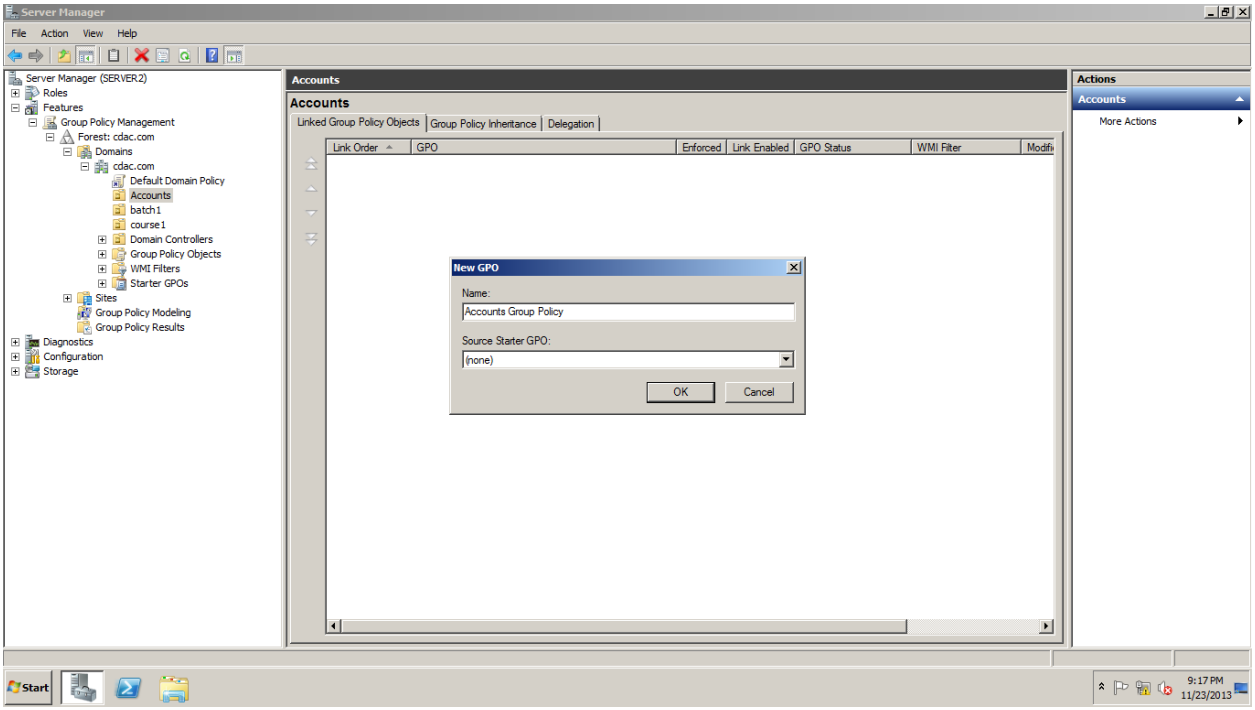
To create a group policy, logon as administrator to a domain controller. Open Server Manager. Expand Features. Expand Group Policy Management. Expand Forest. Expand Domains. Expand Your Domain name. Select the OU where you want to create this new Group Policy.



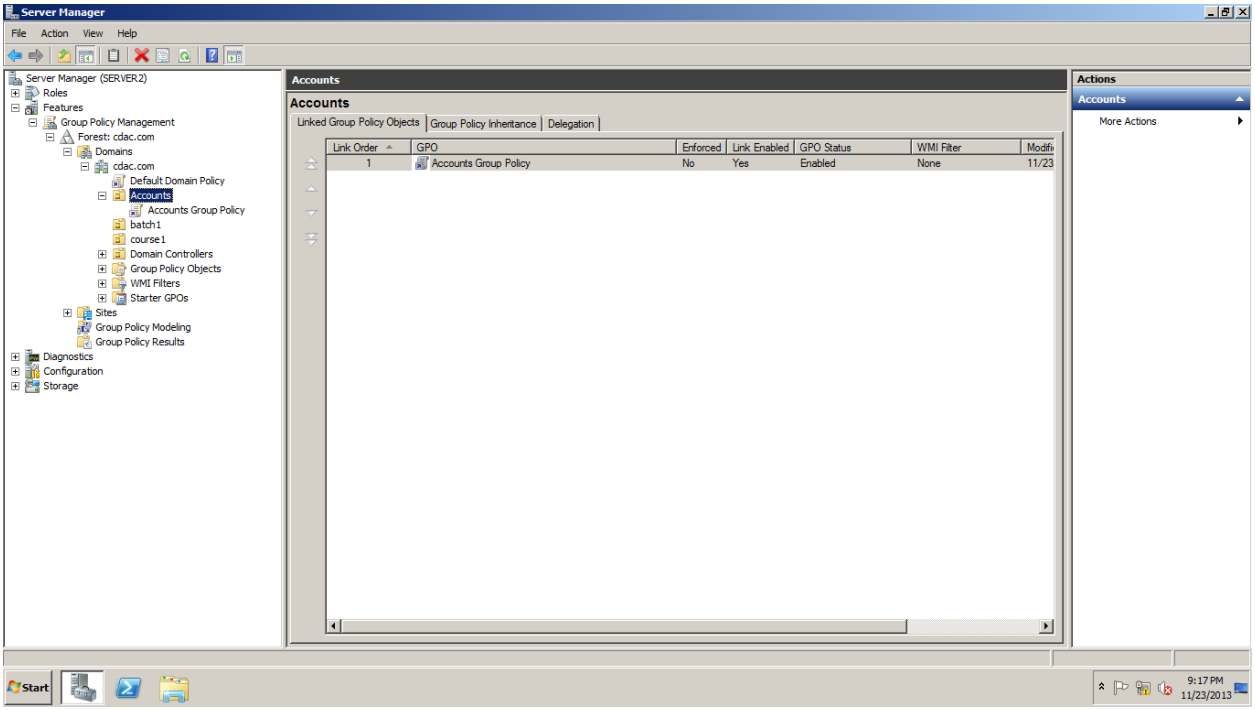
Right Click the OU and Select Create a new GPO option. A window as shown below appears.



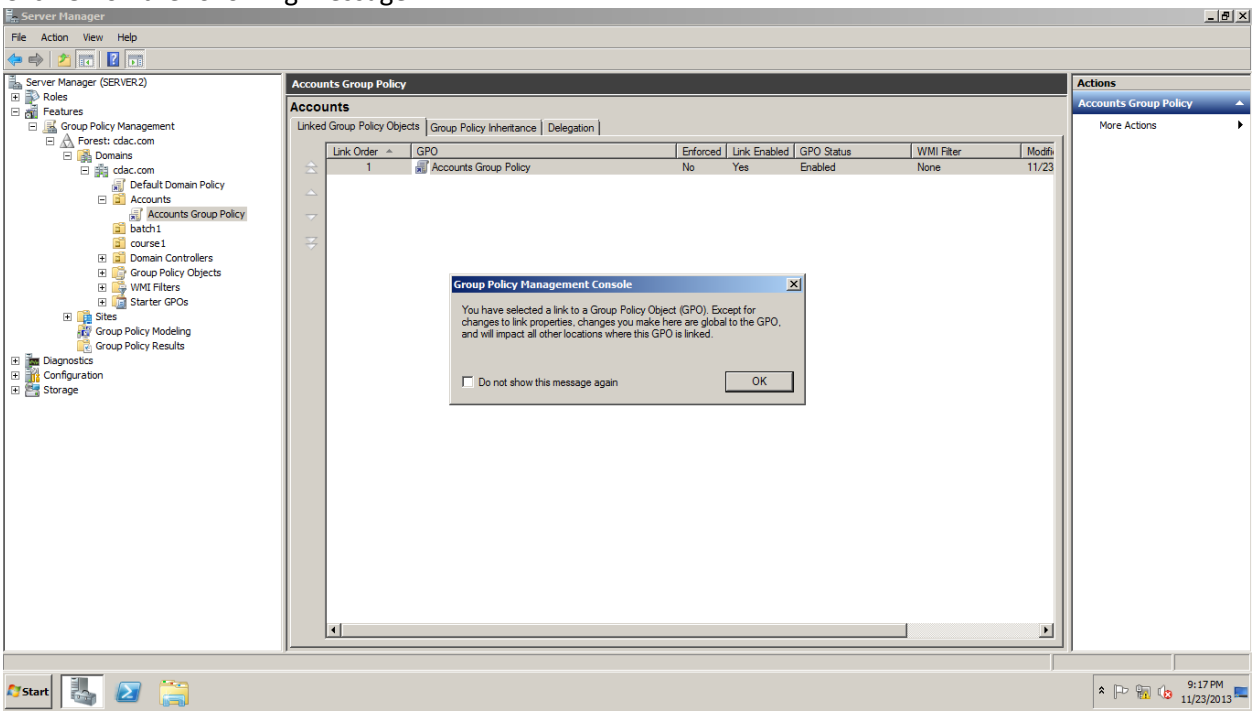
Specify a name for the group policy. Click OK.



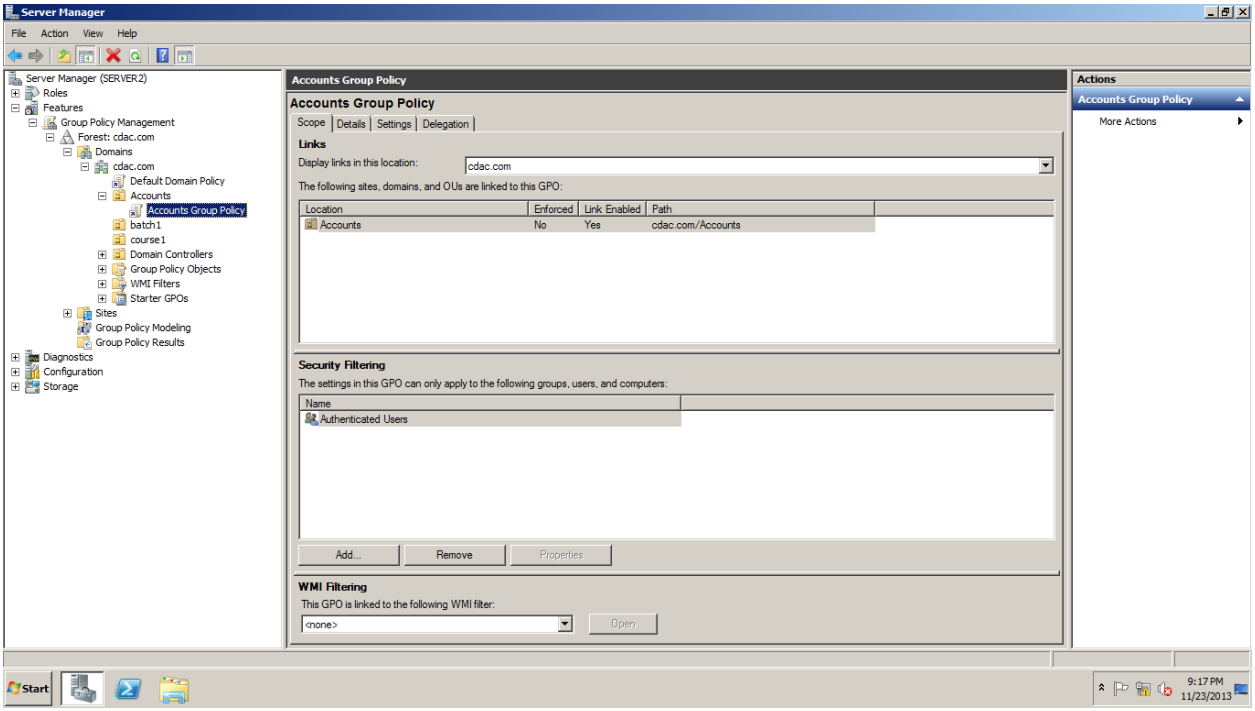
The new group policy setting is shown below the OU as displayed in the following figure. Click to select the new group policy.



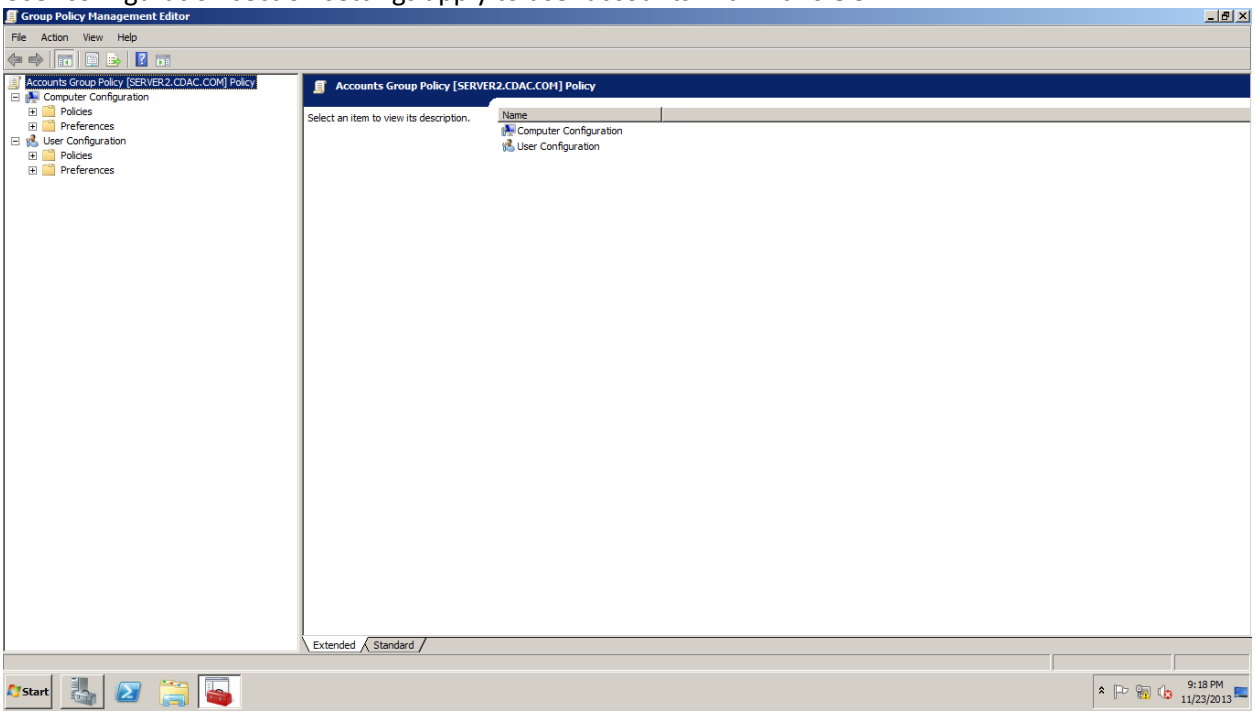
Click Ok on the following message.



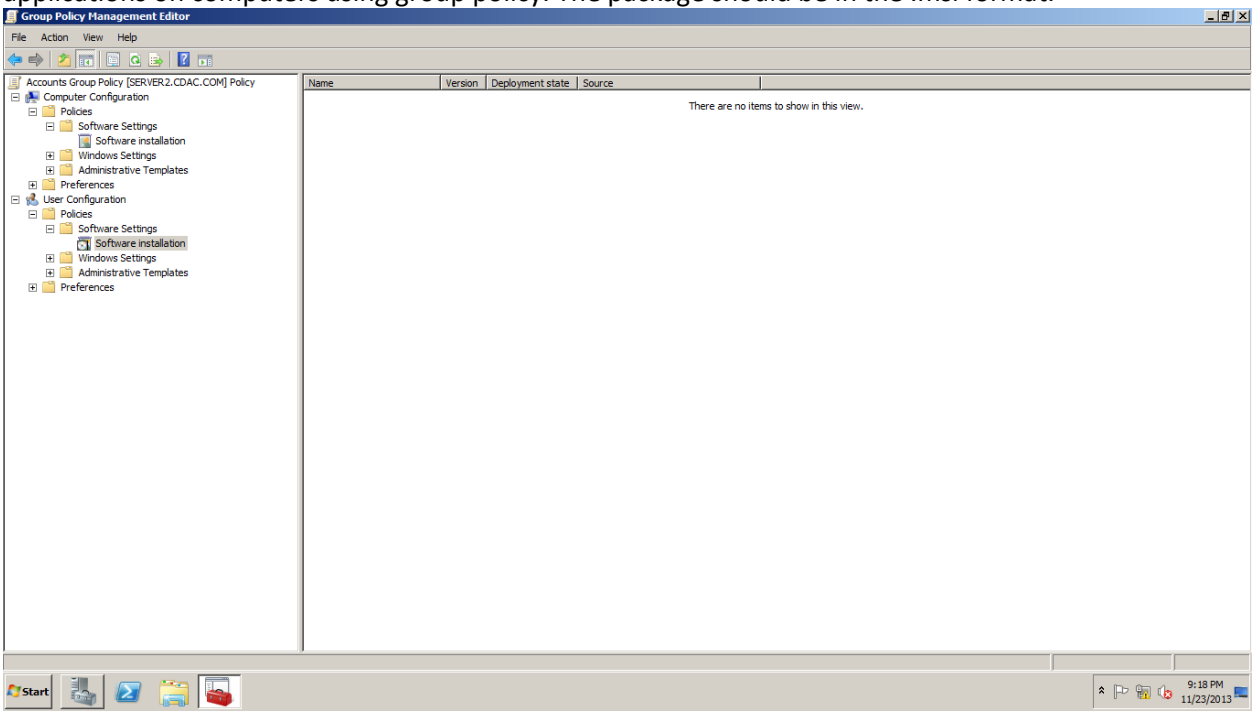
Right click the new group policy and click Edit.



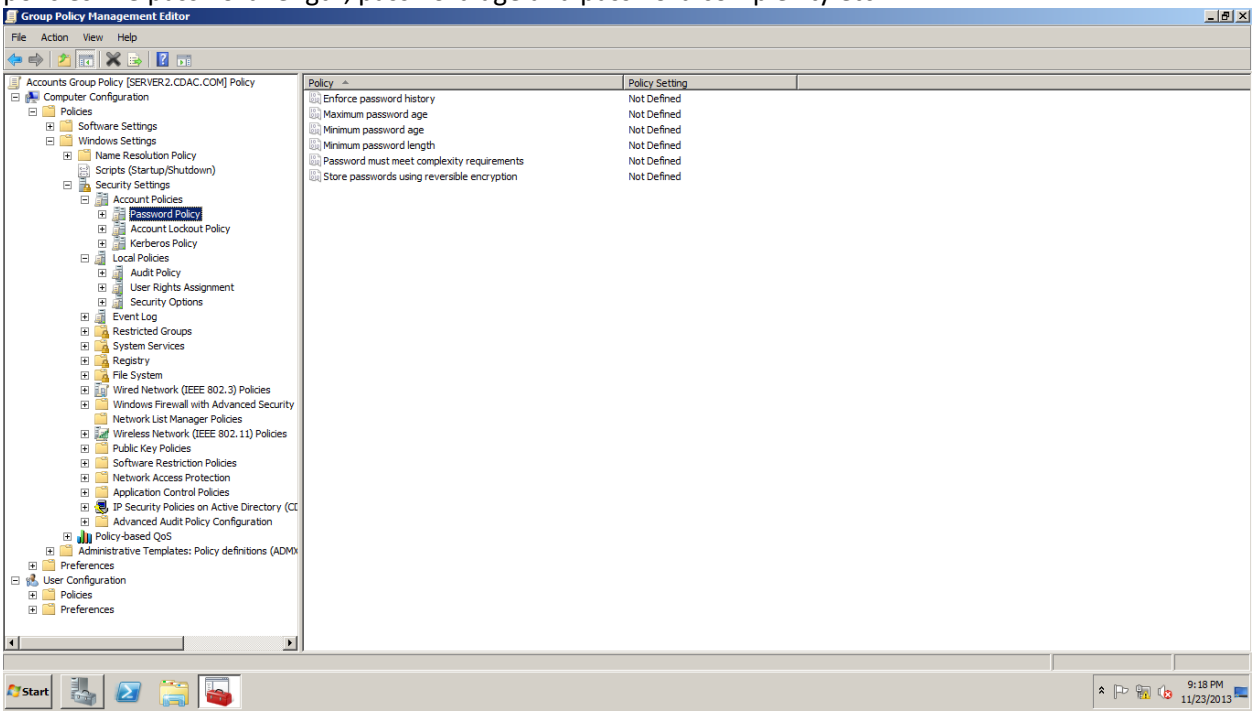
The following window appears. The group policy settings are divided into two sections. Computer configuration section contains policy settings that apply to the computer accounts within this OU. The User configuration section settings apply to user accounts within this OU.



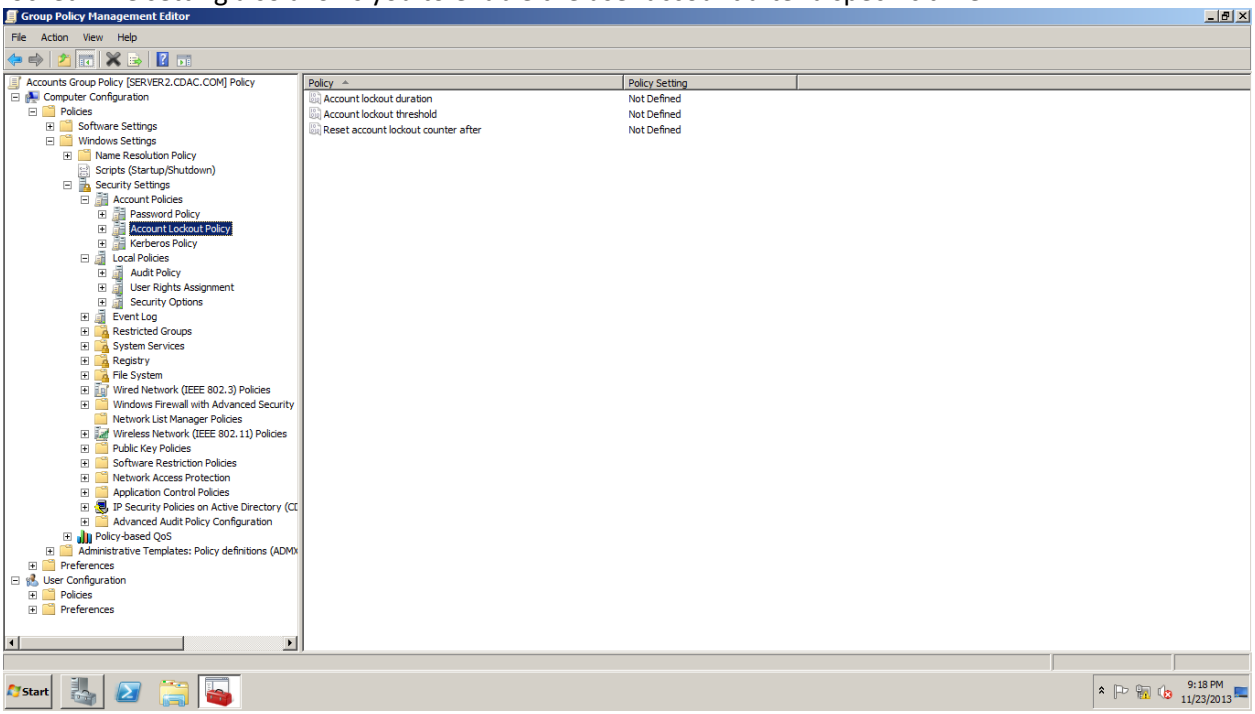
The Software installation setting is available under both the sections. This setting allows you to install applications on computers using group policy. The package should be in the .msi format.



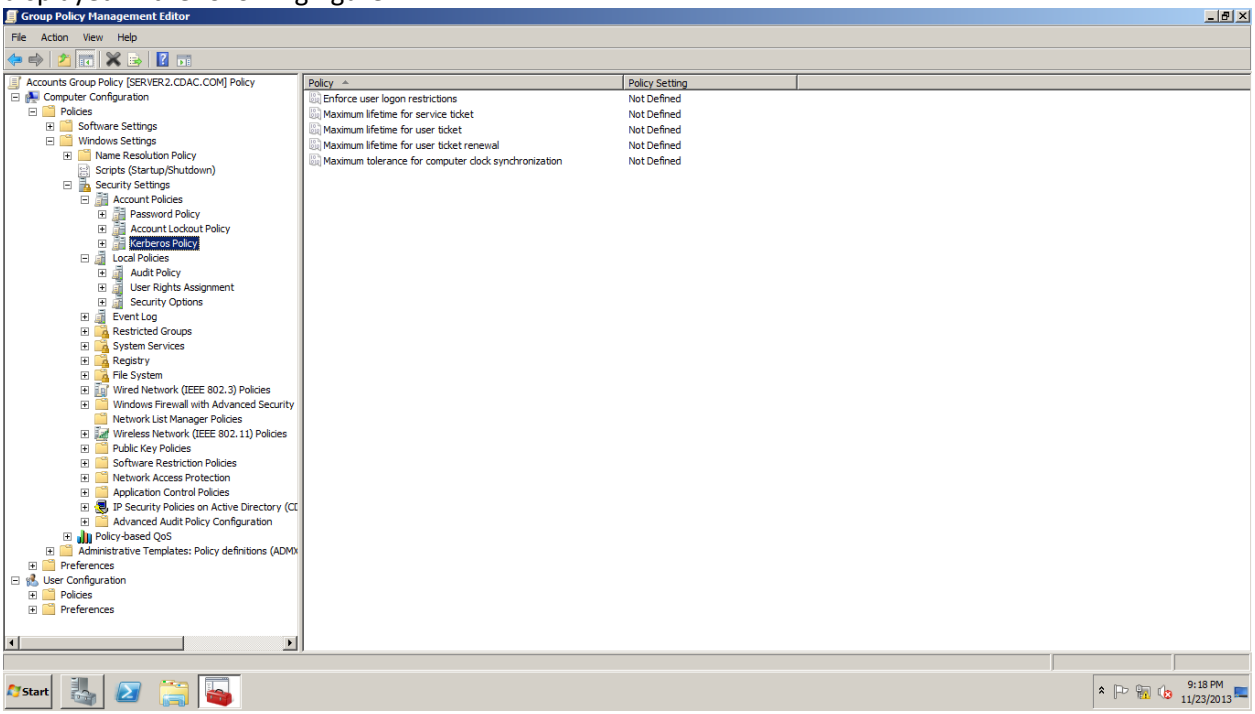
In computer configuration under Windows Settings expand security settings. This location contains a lot of important settings.
In Account Settings the Password Policy settings are shown below. From here you can set password policies like password length, password age and password complexity etc.



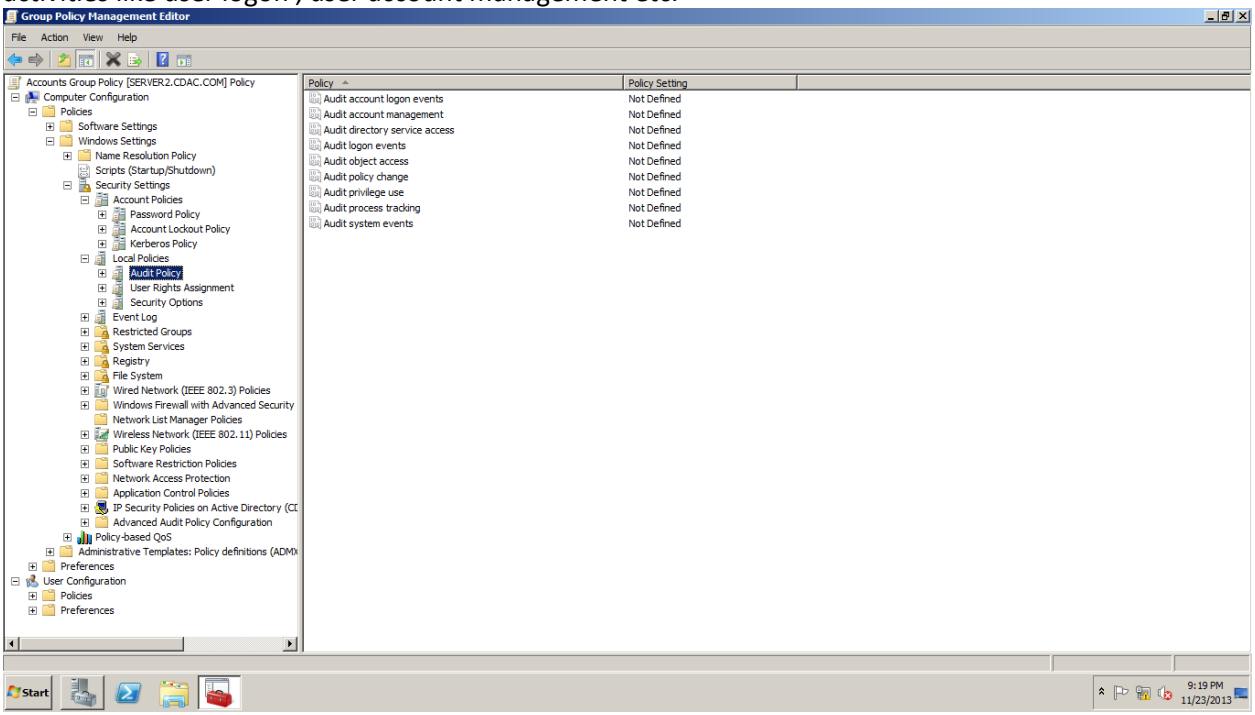
In Account settings there is another policy called Account Lockout Duration. This policy allows you to protect a user account from being hacked. After certain invalid logon attempts the user account will be locked. The setting also allows you to enable the user account after a specific time.



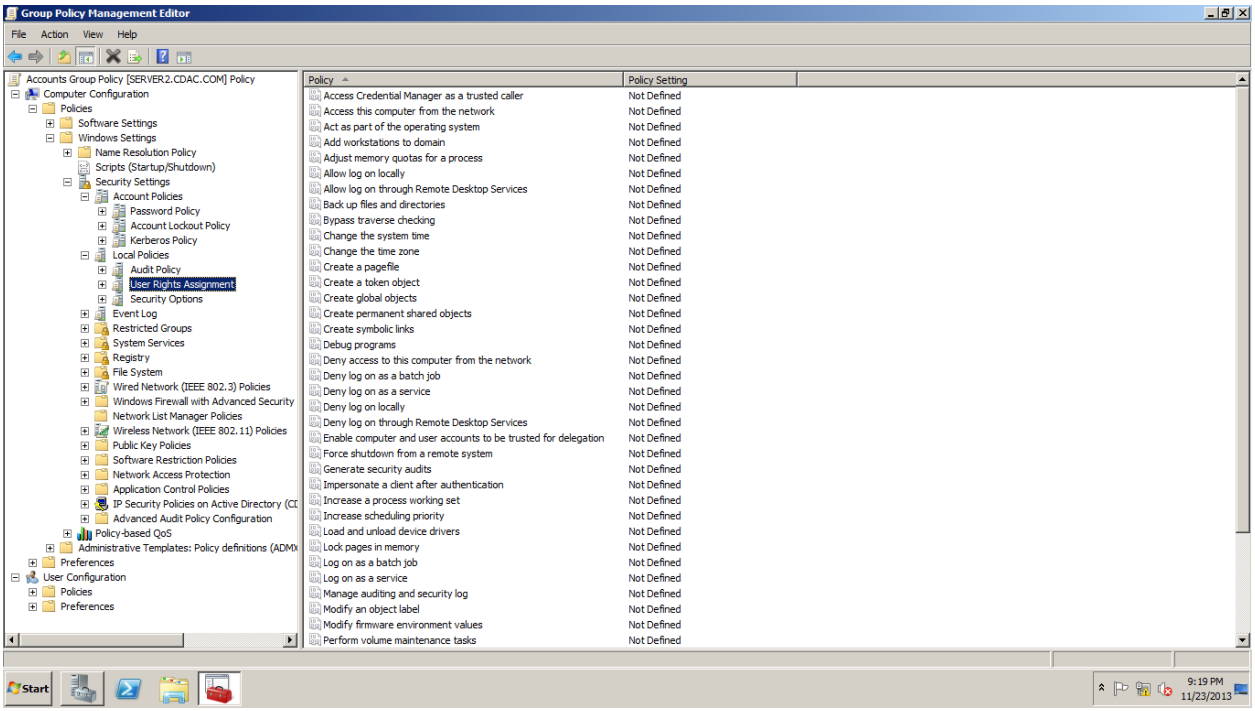
The Kerberos policy allows you to specify settings related to Kerberos Tickets. These settings are displayed in the following figure.



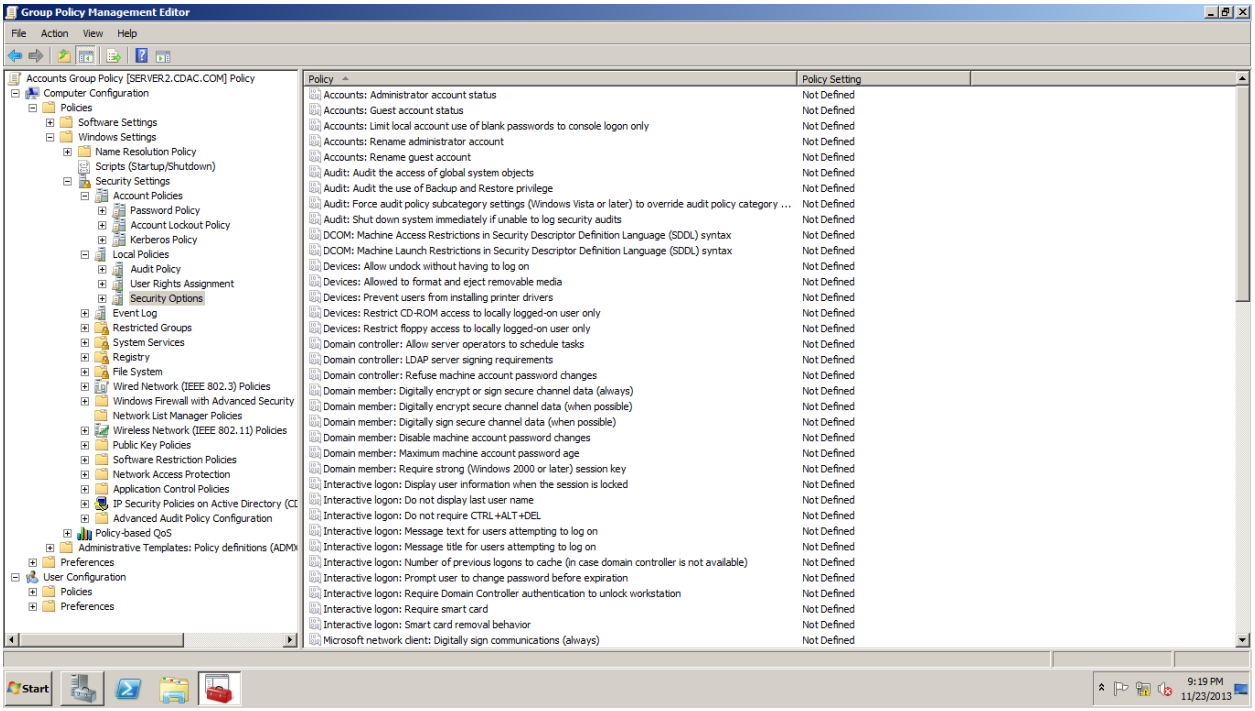
Under Security settings Local Policies are there. The Audit policies below it allows you to monitor activities like user logon , user account management etc.



The User Rights Assignment Section contains settings that can provide or deny users certain permissions. Some of the settings are “Access this computer over the network”, “Allow logon locally” etc. The following fig. shows these policies.

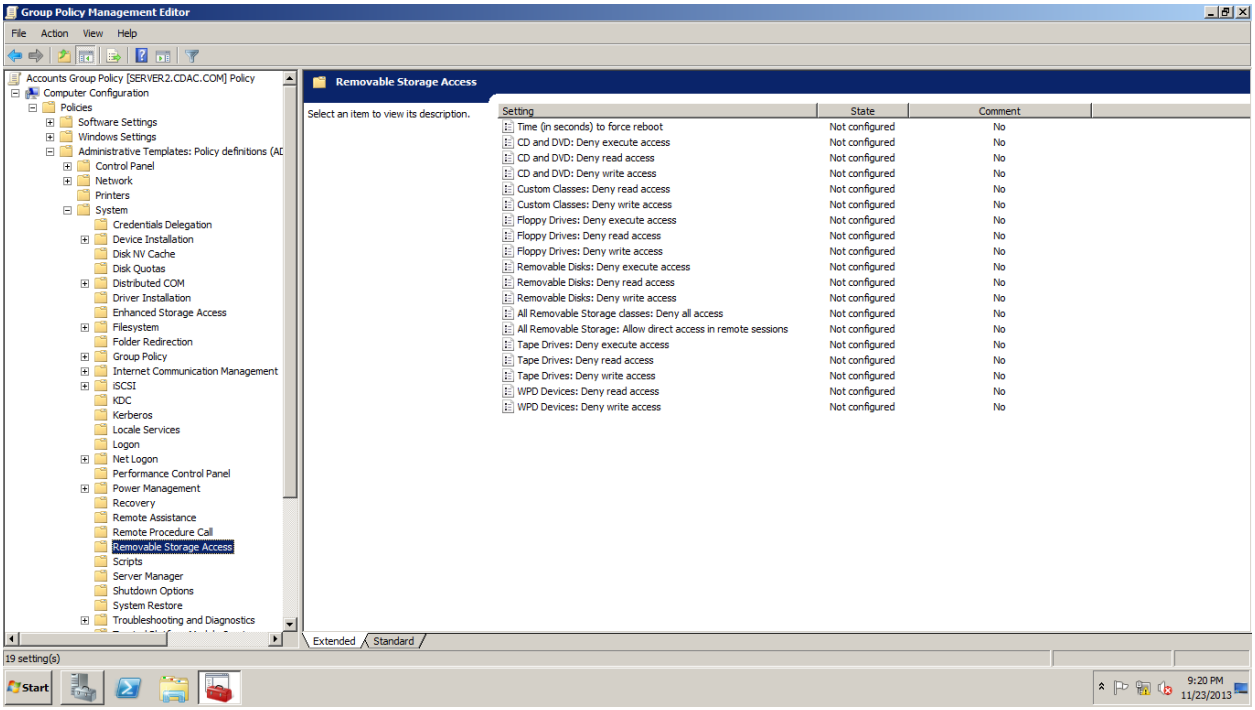


The Security options settings also contain important settings which work to secure a computer. The settings include “Disable Administrator Account”, “Rename Administrator Account” and “Restrict CD-ROM access to locally logged on users only” etc.

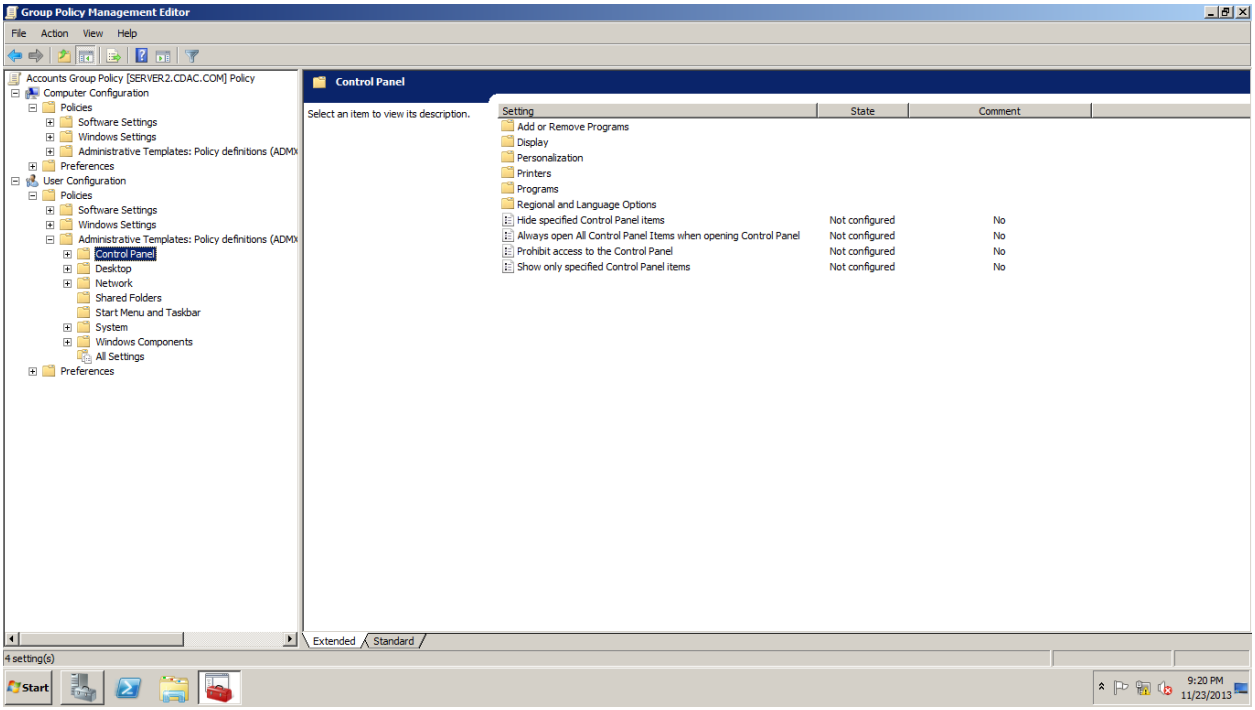


The Removable Storage Access settings are available under both User Configuration and Computer Configuration. These settings are under Administrator Templates, System. These settings allow you to

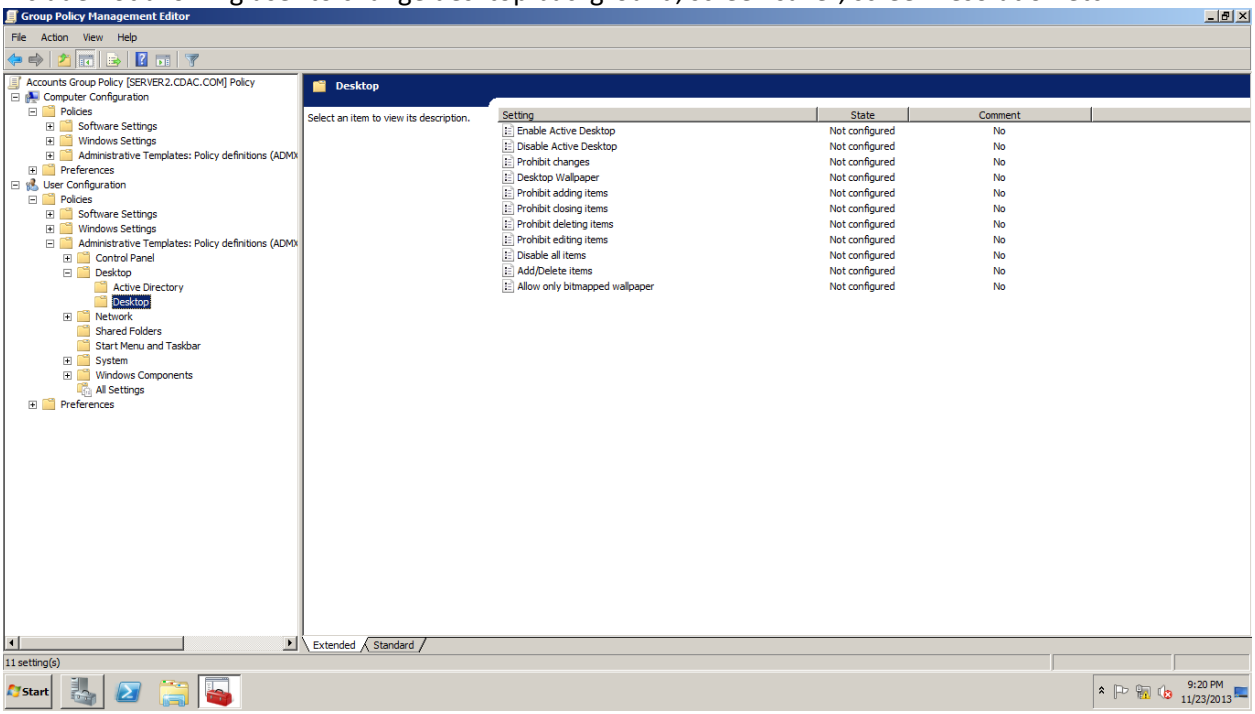
block access to external CDROMs, USB Hard Disks, Mobile phones etc. So users cannot use these devices on their computers.



Also the Control Panel section allows you to put restriction on certain utilities so that users cannot access them. These include Add Remove Programs, Printers etc.



Also the Desktop section under Administrative Templates allows you to put restrictions on users. These include not allowing user to change desktop background, screen saver, screen resolution etc.



The group policy also allows you to put restriction on type of softwares that user can execute. Italso helps administrator configure a lot of settings like proxy settings for internet explorer, wireless network settings for laptop users, registry settings for certain applications etc. Thus using group policy administrator can push these settings based on users or computers.