



# Server Configuration

## Lab18

### Application Restriction Policies

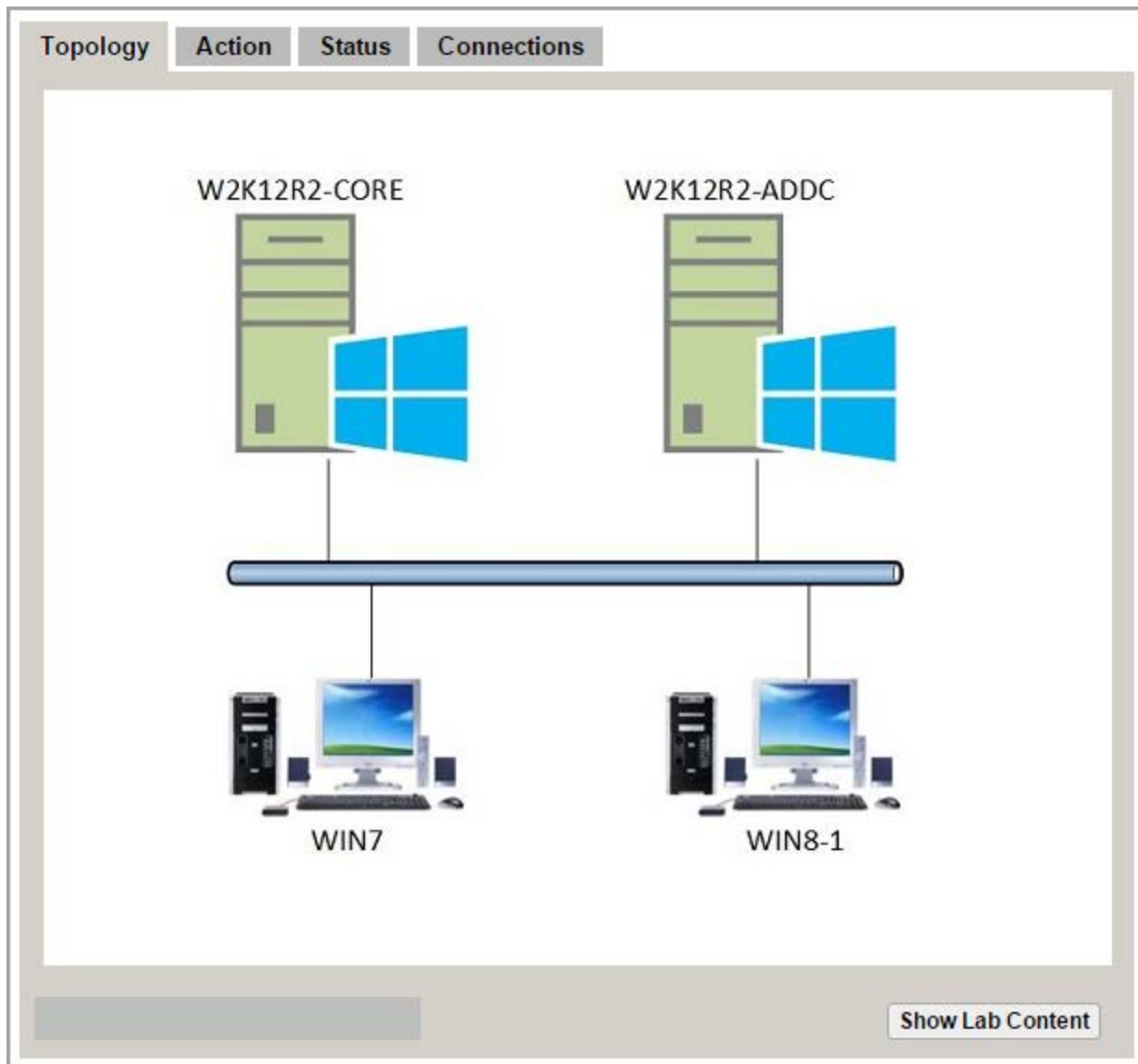


## Contents

Topology.....	3
1 Installing Software with Group Policy.....	4
1.1 Windows Installer Service Package File (MSI).....	4
1.2 Test the Software Installation.....	13
2 Restricting Software with Group Policy .....	17
2.1 Configuring Software Restriction .....	17
2.2 Test the Software Restriction .....	23
3 AppLocker .....	25
3.1 Examining the AppLocker Group Policy .....	25
4 Research (Optional) .....	28
References .....	28



## Topology

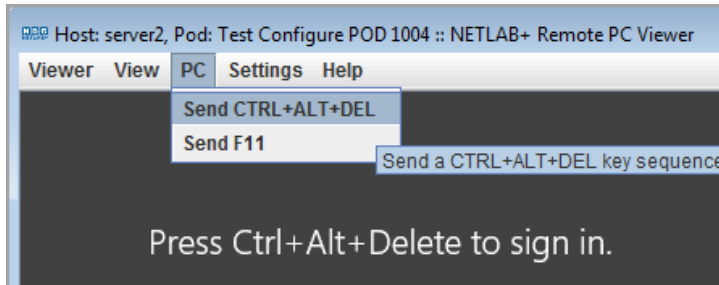


## 1 Installing Software with Group Policy

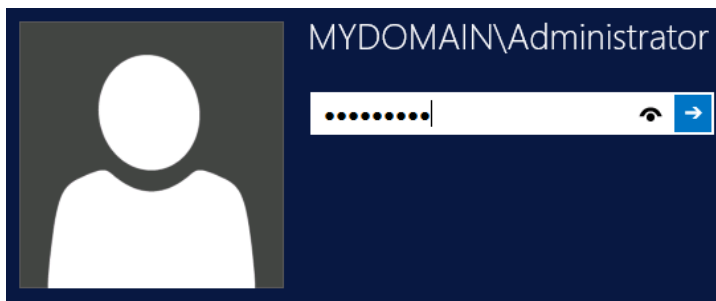
Instead of directing users to a network share or a website, administrators have the ability to use group policy to automatically install needed software on the domain computers.

### 1.1 Windows Installer Service Package File (MSI)

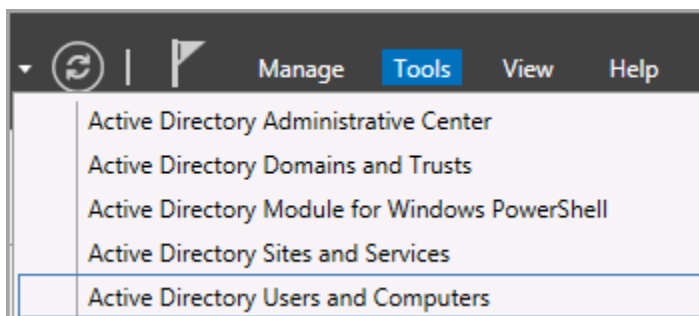
1. Open a console to the Windows W2K12R2-ADDC server by clicking the icon in the topology. Click “PC > Send CTRL+ALT+DEL”.



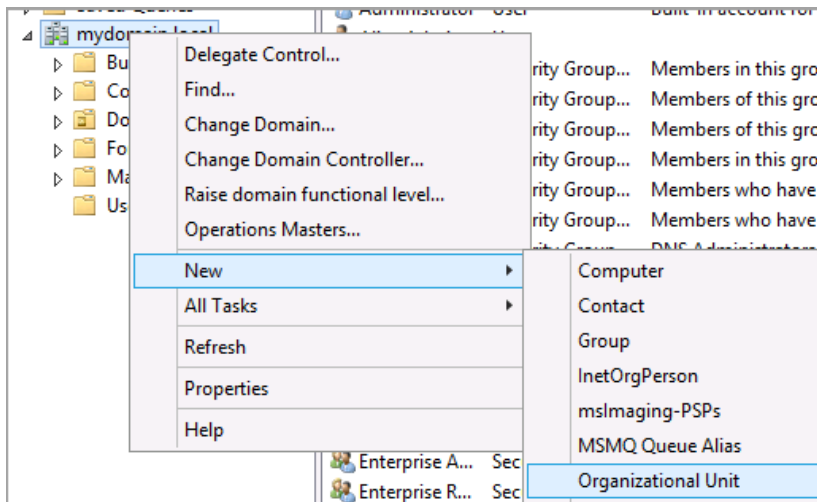
2. Type **P@ssw0rd1** as the administrator password and hit “Enter”.



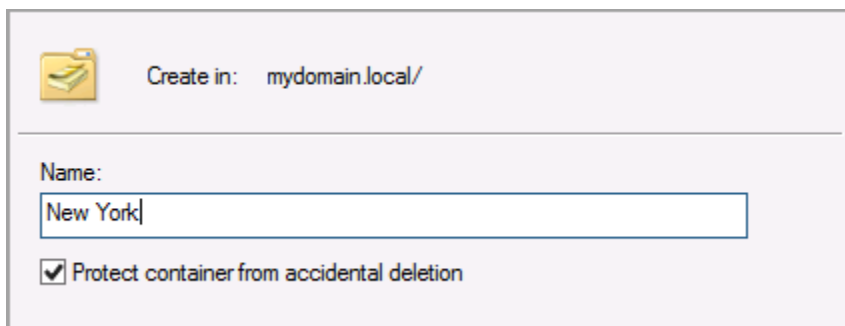
3. On the “Server Manager – Dashboard”, navigate to “Tools > Active Directory Users and Computers”.



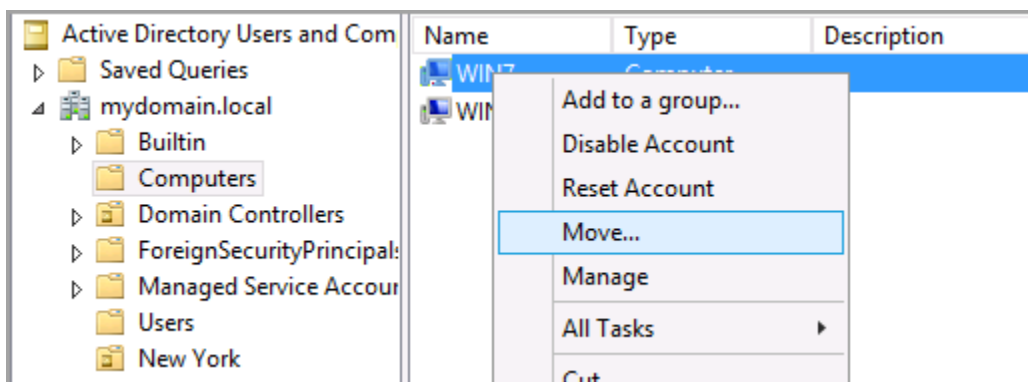
4. Right click “mydomain.local” and select “New > Organizational Unit”.



5. Type **New York** for the name and click “OK”.



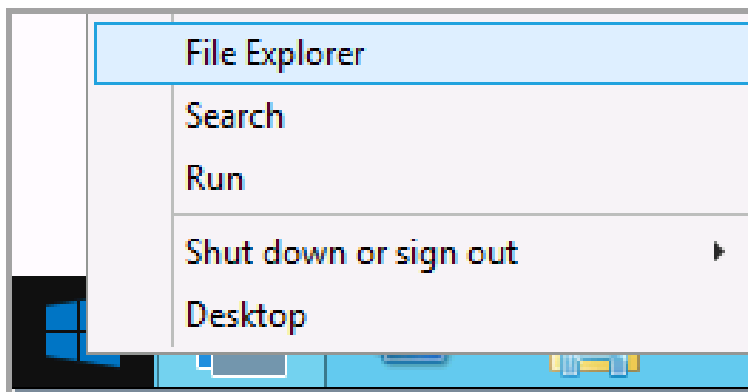
6. Left click on “Computers”. Right click on WIN7 and select “Move”.



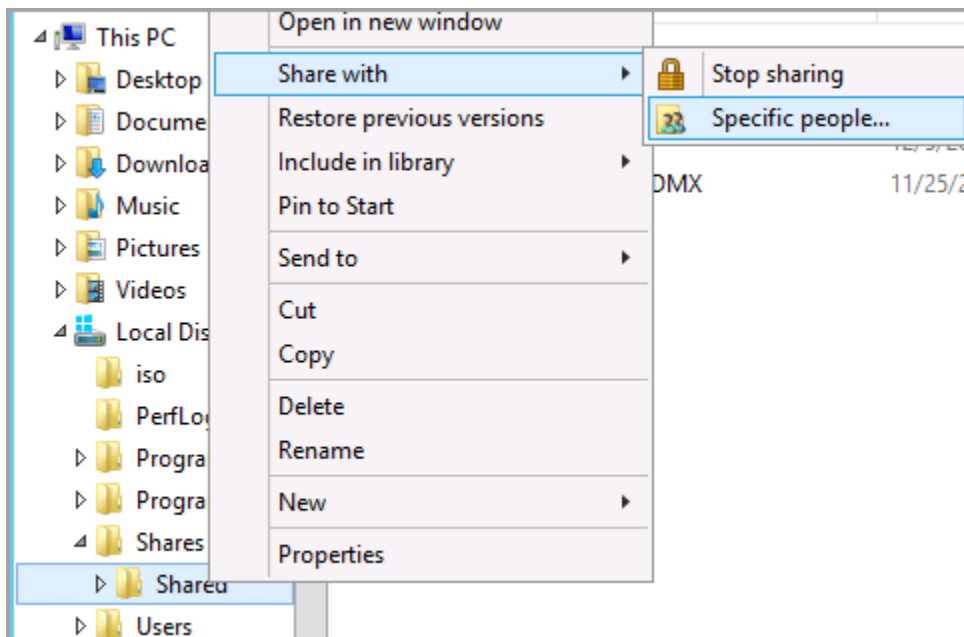
7. Highlight “New York” and click “OK”. Close the “Active Directory Users and Computers” window.



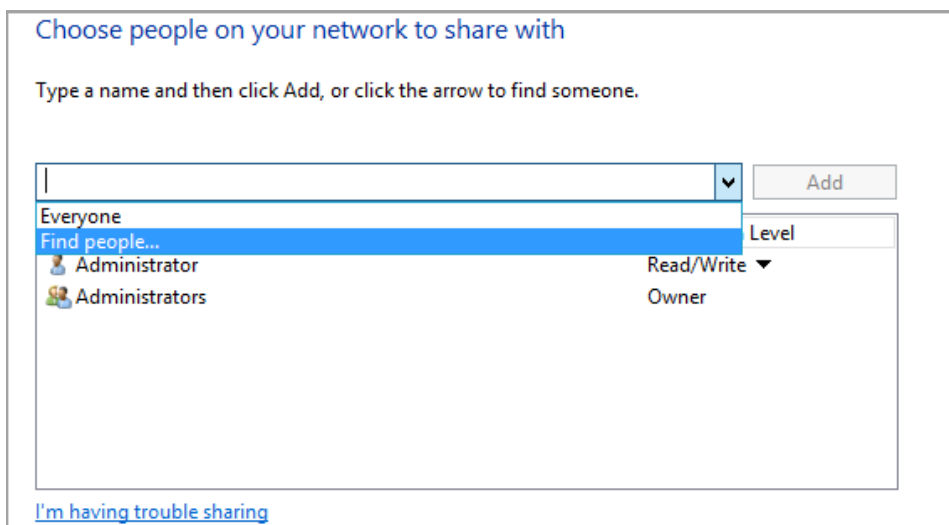
8. Right click the start button, and select “File Explorer”.



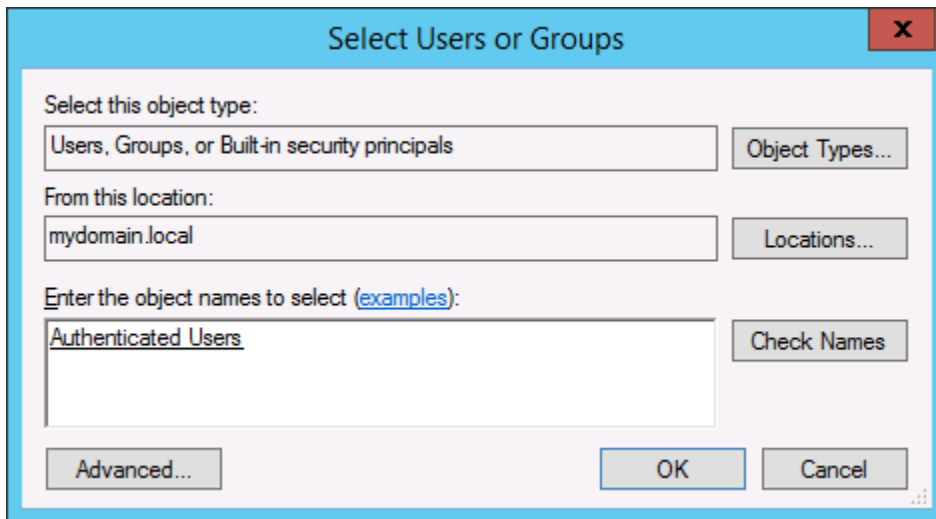
9. In the left pane, expand “Local Disk (C:)”, expand “Shares”, expand “Shared”. Right click on “Shared” and select “Share with > Specific people”.



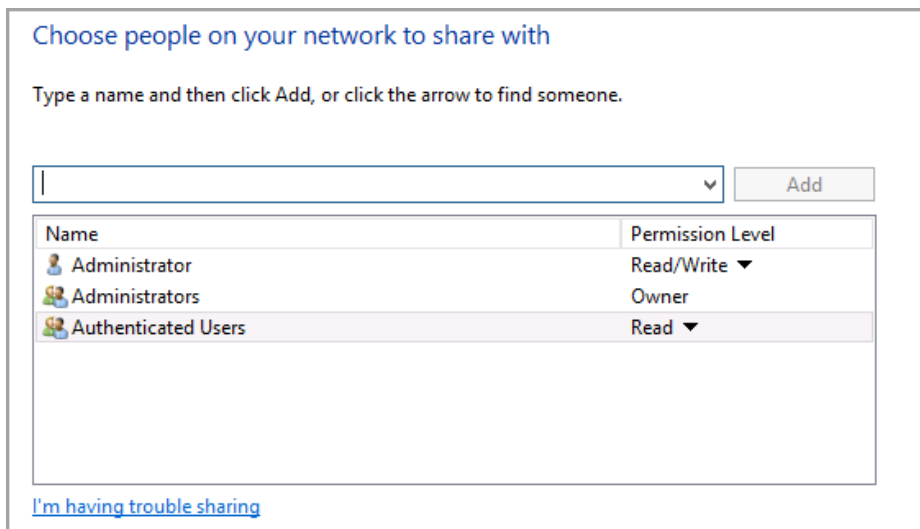
10. Use the dropdown arrow and select “Find people...”.



11. Type **Authenticated Users** and click “Check Names”. Click “OK”.

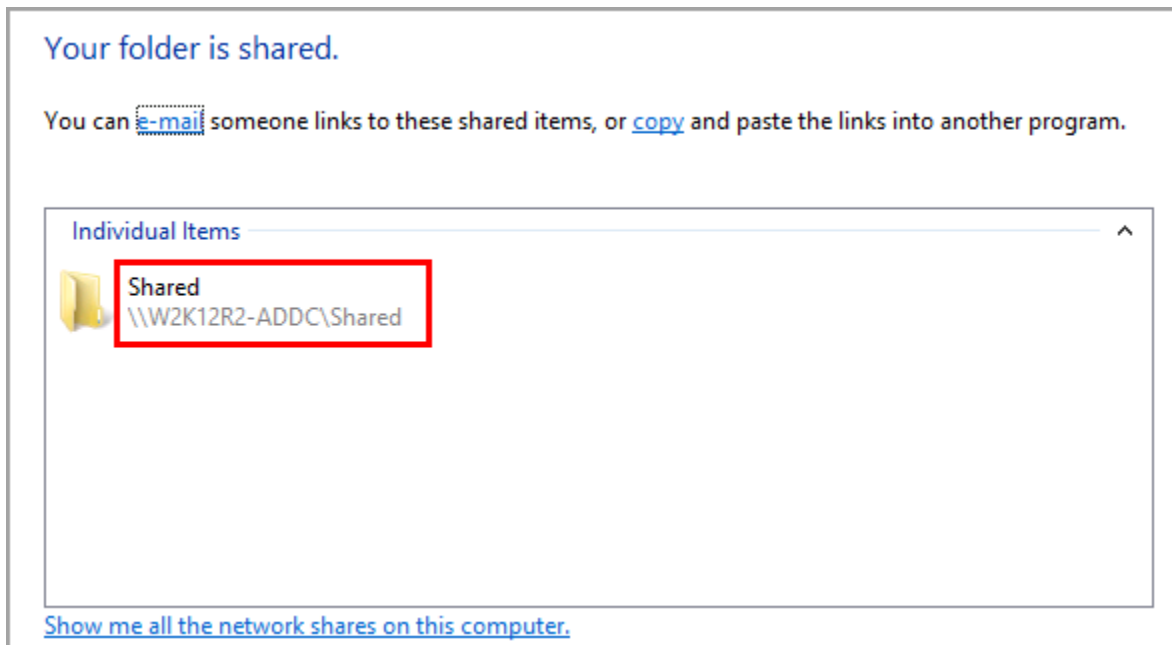


12. Click “Share”.

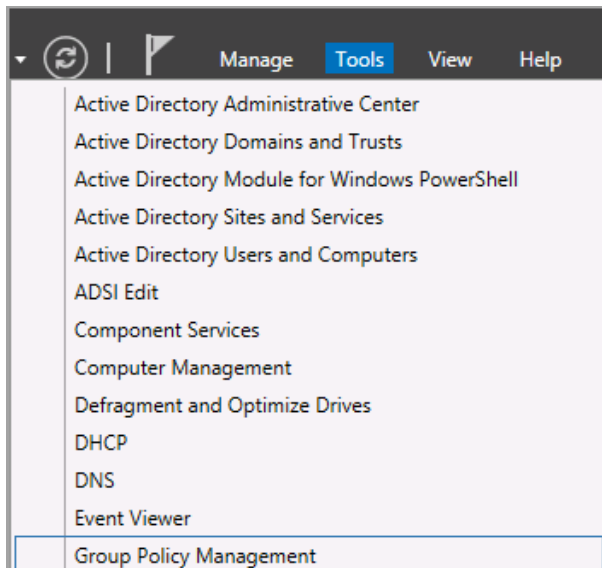




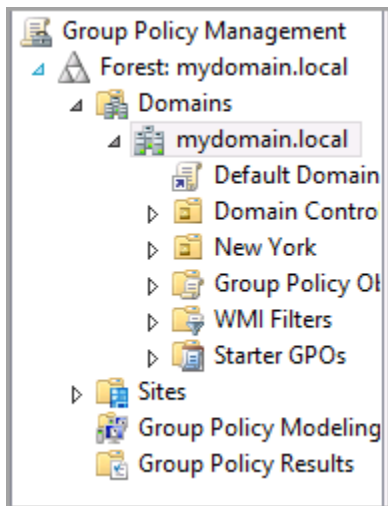
13. Make note of the UNC path and click “Done”. Close the “Shared” file explorer window.



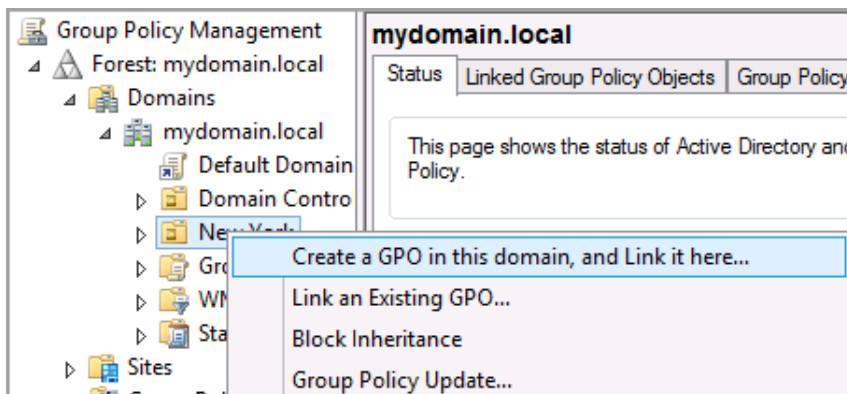
14. Navigate to “Tools > Group Policy Management”.



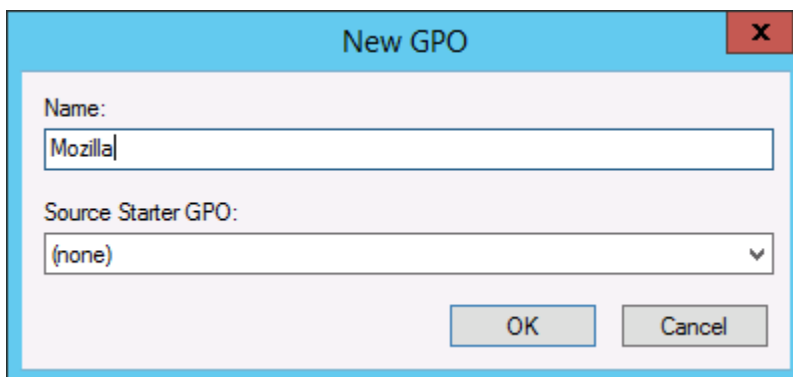
15. Expand “Forest: mydomain.local”, expand “Domains”, expand “mydomain.local”.



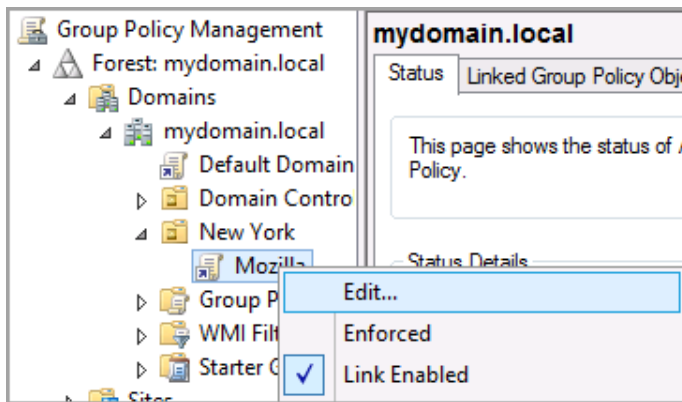
16. Right click the “New York” OU and select “Create GPO in this domain, and link it here”.



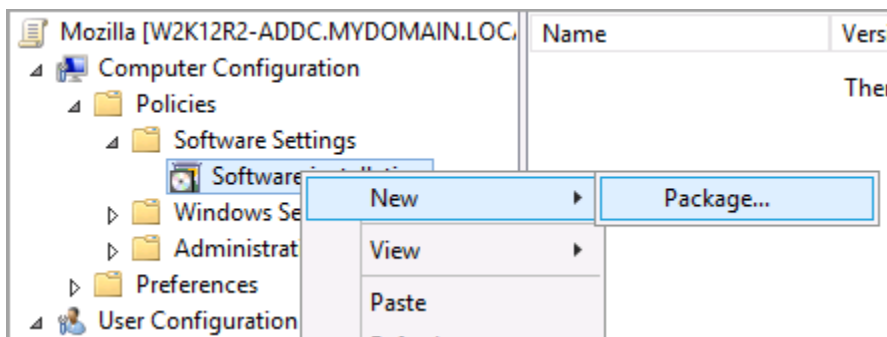
17. Type Mozilla for the name and click “OK”.



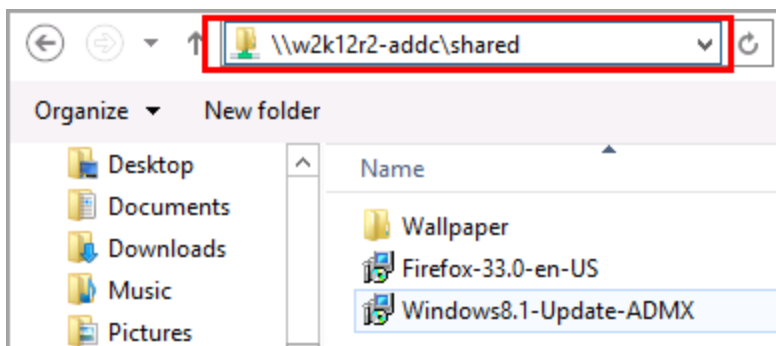
18. Expand the “New York” OU, right click the “Mozilla” GPO and select “Edit”.



19. Under “Computer Configuration”, expand “Policies > Software Settings”, right click on “Software installation” and select “New > Package”.



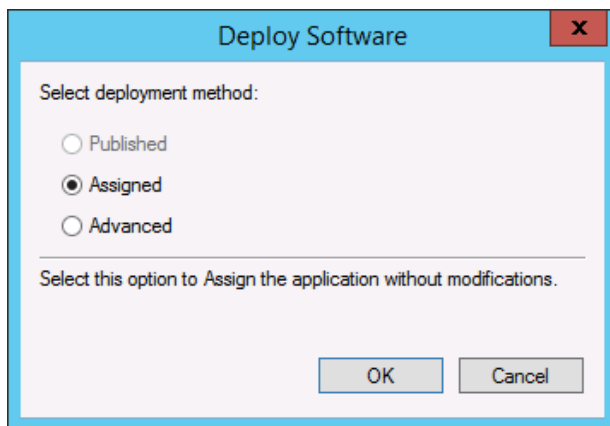
20. Type **\\w2k12r2-addc\shared** in the navigation bar and hit “Enter”.



21. Click on “Firefox 33.0-en-US”, click “Open”.

Name	Date modified	Type
Wallpaper	12/5/2014 1:29 PM	File folder
Firefox-33.0-en-US	12/5/2014 1:24 PM	Windows Installer ...
Windows8.1-Update-ADMX	11/25/2014 4:46 PM	Windows Installer ...

22. Leave “Assigned” selected and click “Ok”.



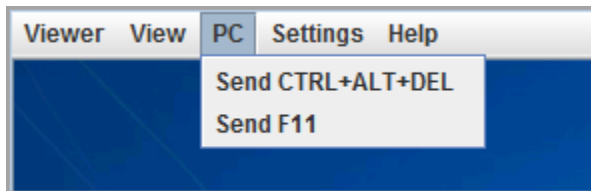
23. Left click on “Software installation”, wait 1-2 minutes and Mozilla will appear in the right hand pane.

Mozilla [W2K12R2-ADDC.MYDOMAIN.LOC]				
Computer Configuration	Name	Versi...	Deployment st...	Source
Policies	Mozilla Firefox (en-US)	33.0	Assigned	\\w2k12r2-addc\shared\Firefox-3...
Software Settings				
Software installation				
Windows Settings				
Administrative Templates: Policy				
Preferences				

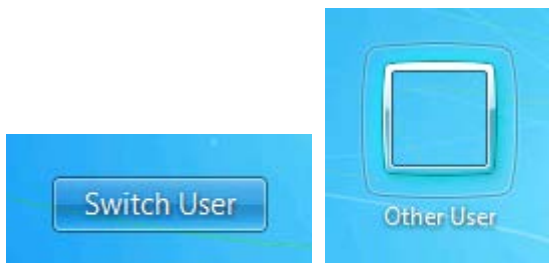
24. Close the GPO editor.

## 1.2 Test the Software Installation

1. Open a console to the WIN7 machine. Click “PC > Sent CTRL+ALT+DEL”.



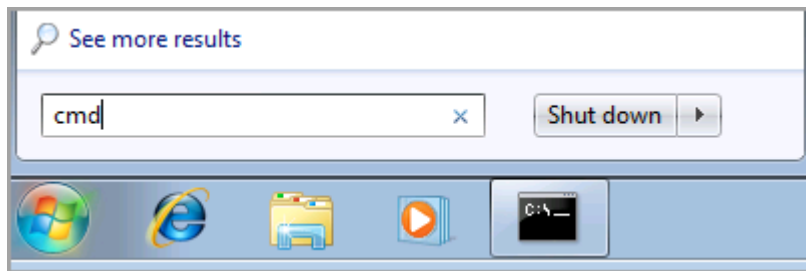
2. Click “Switch User” then “Other User”.



3. Type **mydomain\joeit** as the username and **Password1** as the password. Hit “Enter”.



- Left click the start button and type cmd in the search box. Hit “Enter”.



(Note: Because group policy can take up to 5 minutes to update, we will force an update.)

- Type **gpupdate /force** and hit “Enter”. Read the informational warning, type **Y** and hit “Enter”.

```
C:\Users\joeit>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

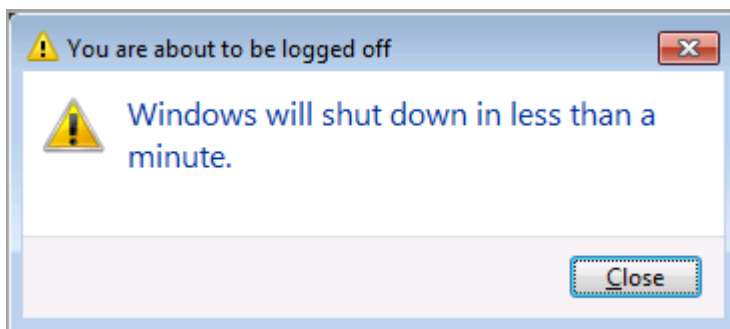
The Group Policy Client Side Extension Software Installation was unable to apply
one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or run GPRESULT /H GPreport.
html from the command line to access information about Group Policy results.

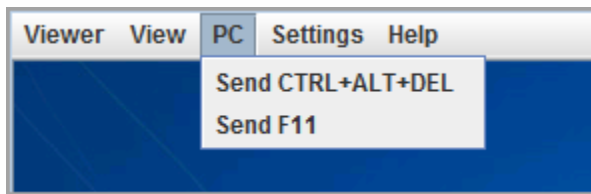
Certain Computer policies are enabled that can only run during startup.

OK to Restart?. <Y/N>_
```

- Windows will automatically reboot.



7. On the WIN7 machine. Click “PC > Sent CTRL+ALT+DEL”.



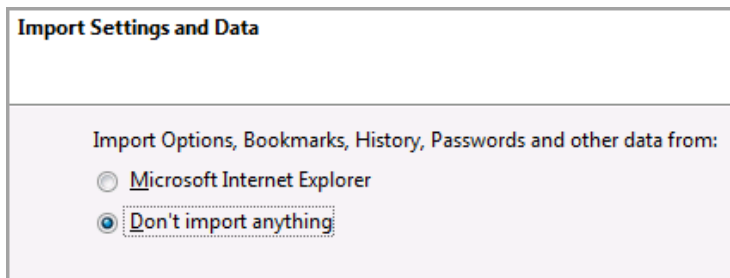
8. Log on to the WIN7 machine as **mydomain\joeit** using **Password1** as the password.



9. Mozilla is now installed and available on the desktop. Double click on the Mozilla shortcut to verify that it is accessible.



10. Select “Don’t import anything” and click “Next”.



11. There is no internet connection from inside the lab, so the browser will return an error page. Mozilla will also display the start page.



12. Leave “joeit” logged onto the WIN7 machine and continue the next steps.

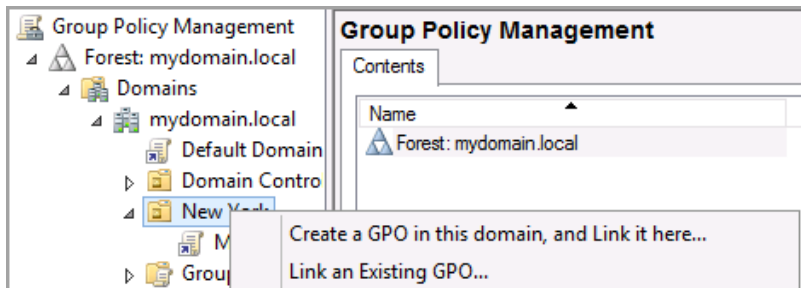


## 2 Restricting Software with Group Policy

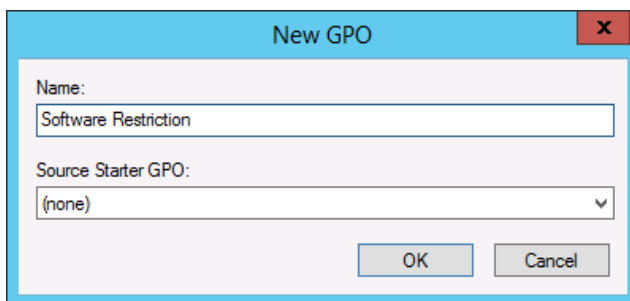
Streaming videos and certain software can consume expensive bandwidth. Administrators have the ability to restrict programs from being run by specific groups or on specific computers.

### 2.1 Configuring Software Restriction

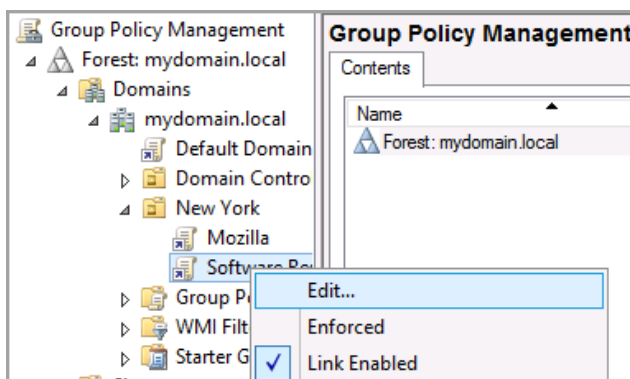
1. Return to the W2K12R2-ADDC machine. Right click on the “New York” OU and select “Create a GPO in this domain, and Link it here”.



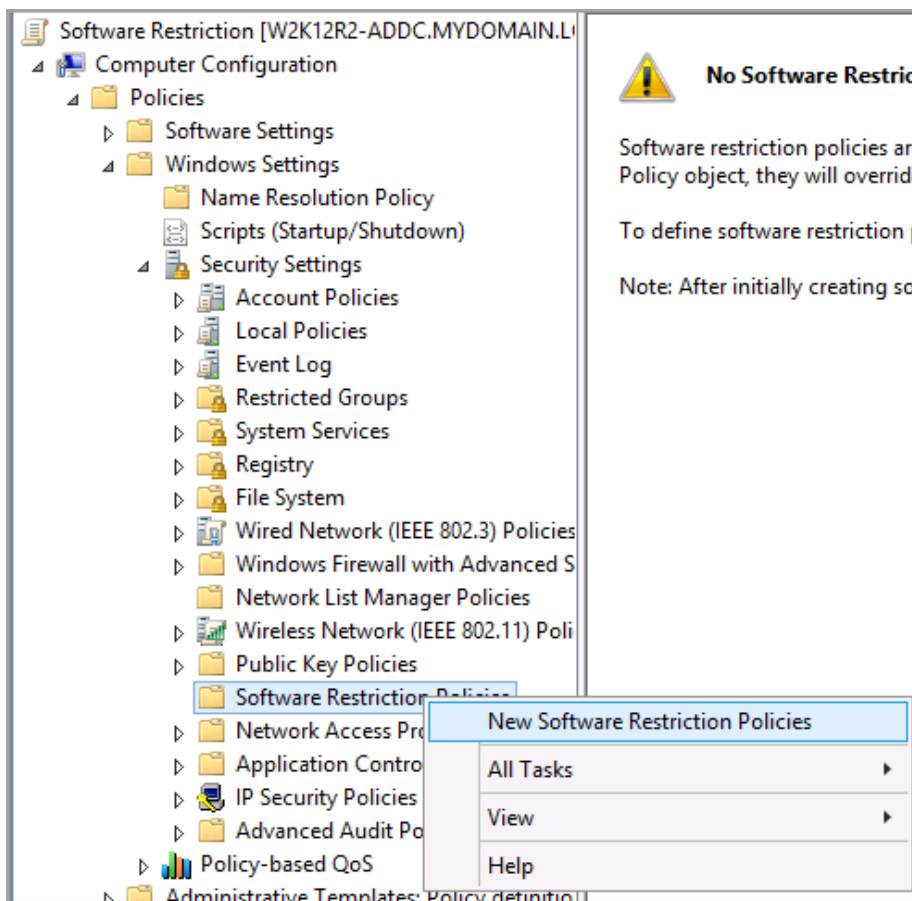
2. Type **Software Restriction** for the name and click “OK”.



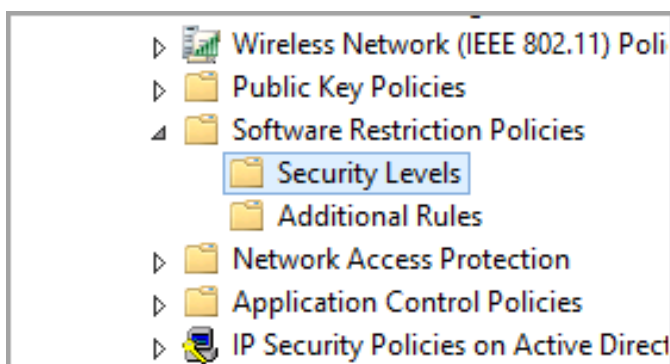
3. Right click “Software Restriction” and select “Edit”.






4. Under “Computer Configuration”, expand “Policies”, expand “Windows Settings”, and expand “Security Settings”. Left click and then right click on “Software Restriction Policies” and select “New Software Restriction Policies”.



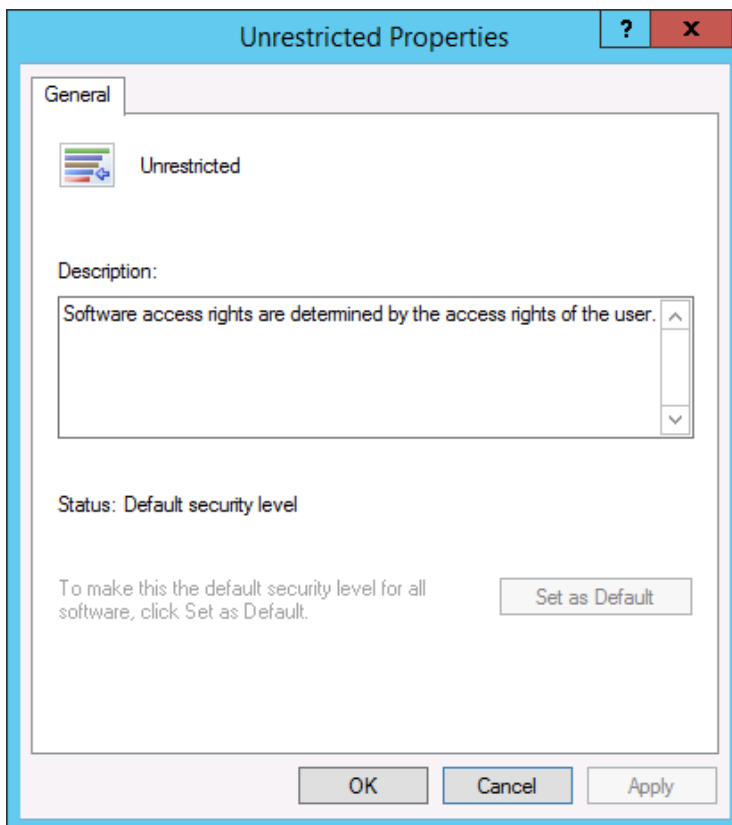
5. Expand “Software Restriction Policies” and left click on “Security Levels”.






6. Double click on the “Unrestricted” option in the right hand pane.

Name	Description
 Disallowed	Software will not run, regardless of the access rights of the user.
 Basic User	Allows programs to execute as a user that does not have Administrator ...
 Unrestricted	Software access rights are determined by the access rights of the user.

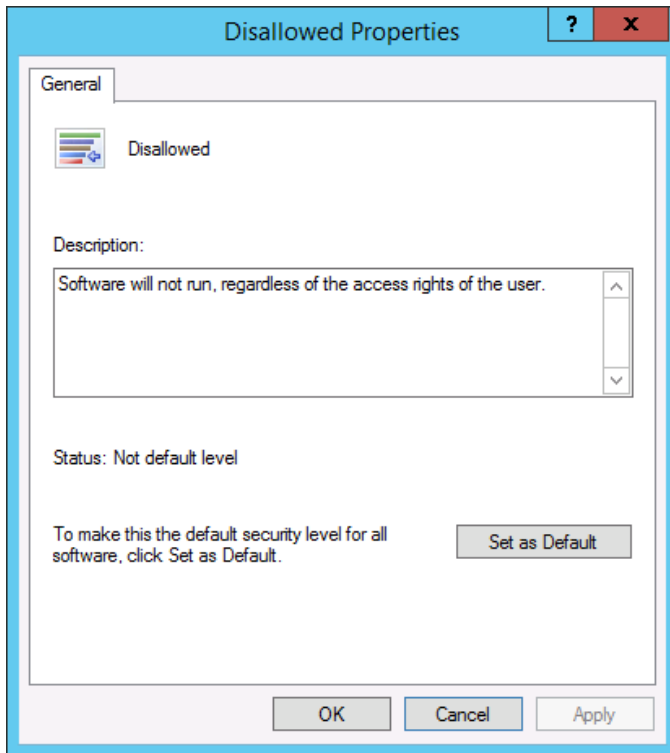
7. This is the default security level of this policy. Click “OK”.



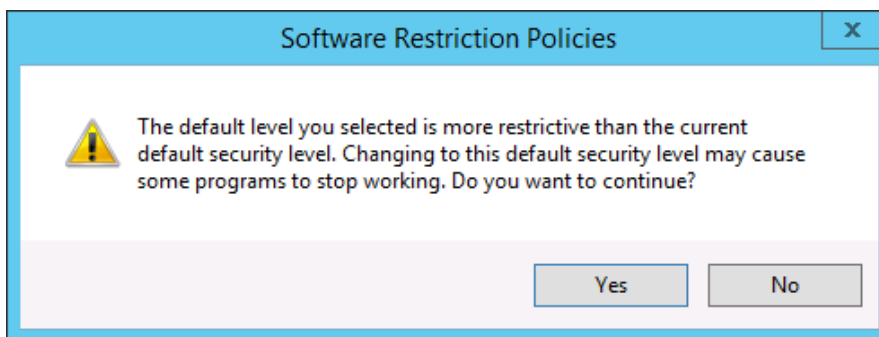
8. Double click on “Disallowed”.

Name	Description
 Disallowed	Software will not run, regardless of the access rights of the user.
 Basic User	Allows programs to execute as a user that does not have Administrator ...
 Unrestricted	Software access rights are determined by the access rights of the user.

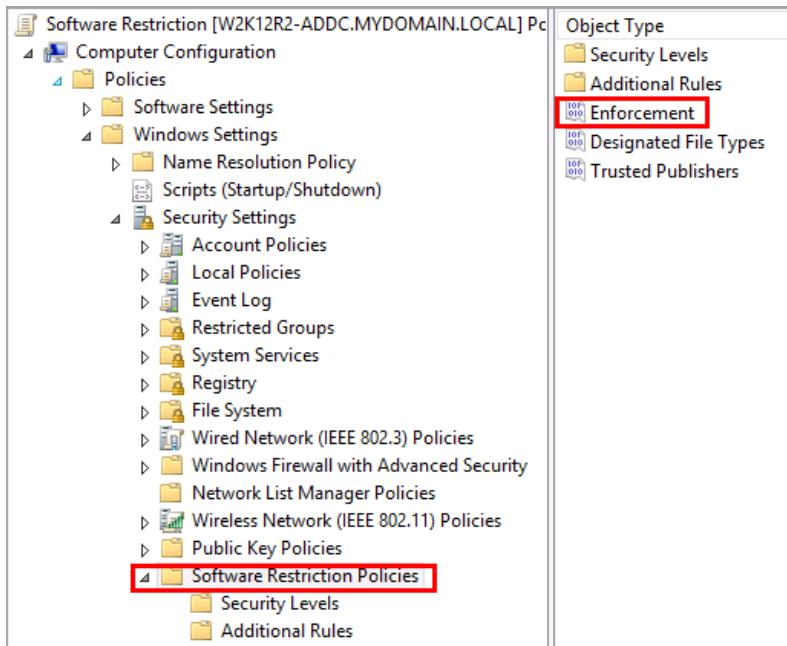
9. This is a full restriction policy and software will not run regardless of the user. Click “Set as Default”.



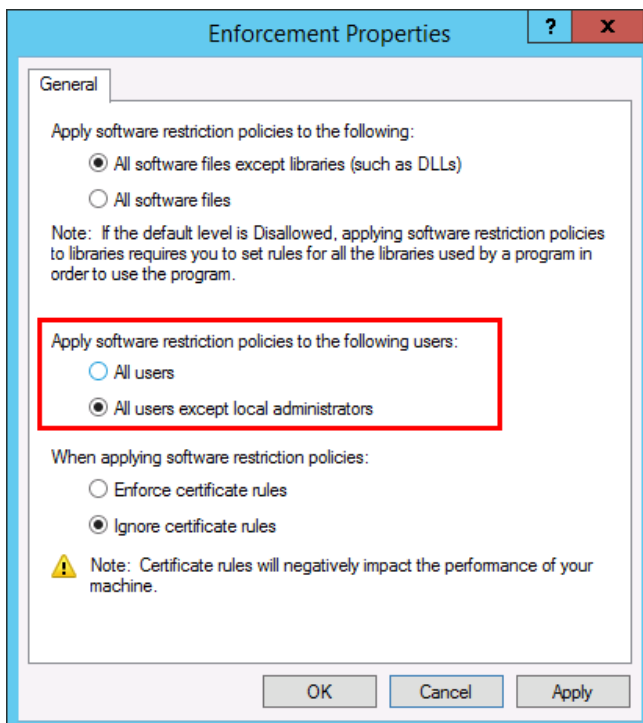
10. Click “Yes”, then click “OK”.



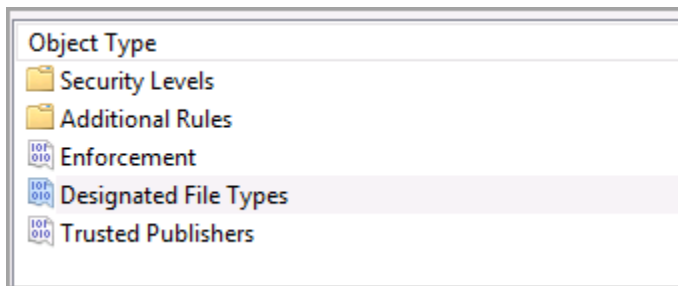
11. Click on “Software Restriction Policies” in the left pane and then double click on “Enforcement” located in the right hand pane.



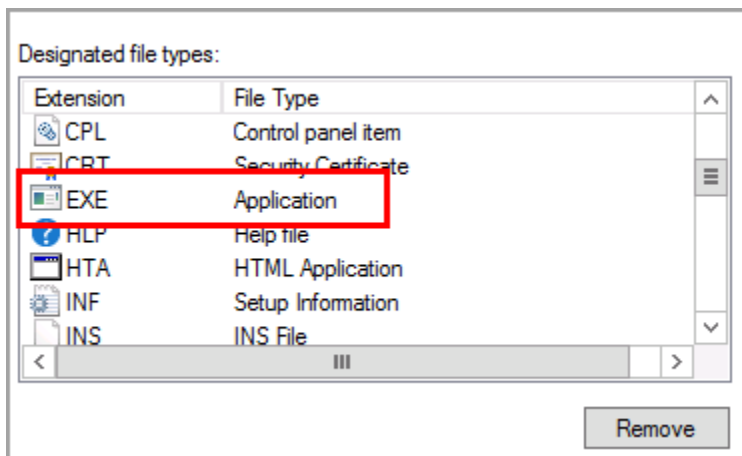
12. Click the radio button next to “All users except administrators”, click ‘OK’.



13. Double click “Designated File Types”.



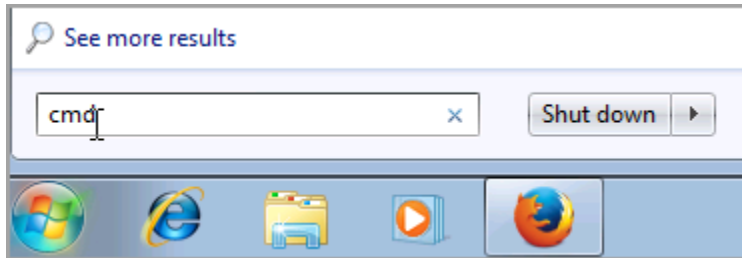
14. Scroll down and notice “EXE Application” along with everything else listed here will be restricted. Click “OK”.



15. Close the “Group Policy Management Editor”.

## 2.2 Test the Software Restriction Policy

1. Open a console to the WIN7 machine which should have joeit logged on. If not, log on as joeit. Left click the start button, type **cmd** in the search bar and hit “Enter”.



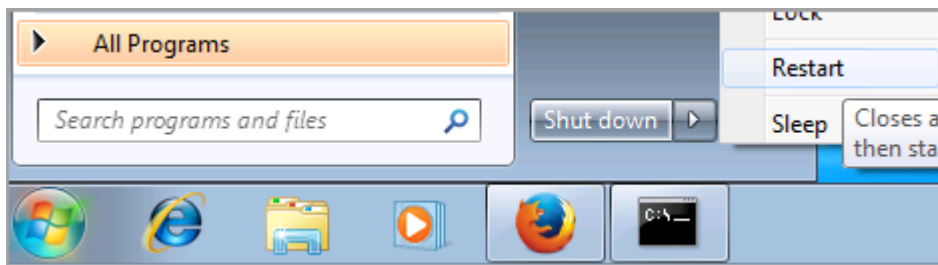
2. Type **gpupdate /force** and hit “Enter”.

```
C:\Users\joeit>gpupdate /force
Updating Policy...

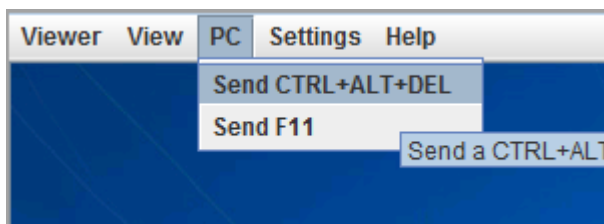
User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\Users\joeit>
```

3. Restart the WIN7 machine by left clicking the start button, clicking the arrow to the right of shut down and selecting “Restart”.



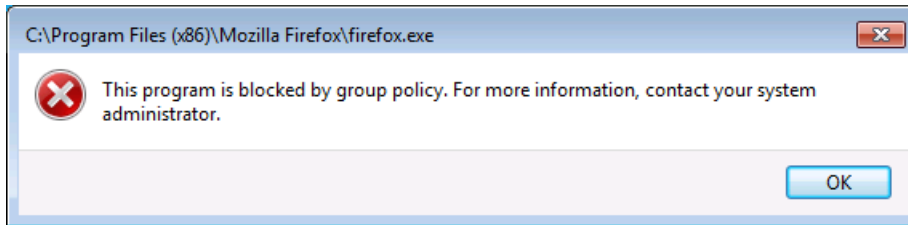
4. Log back onto the WIN7 machine as “joeit” using **Password1** as the password.



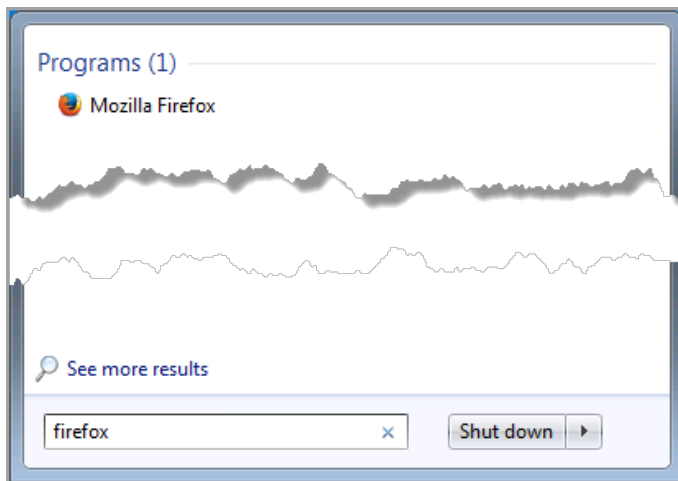
5. Double click the “Mozilla” icon on the desktop.



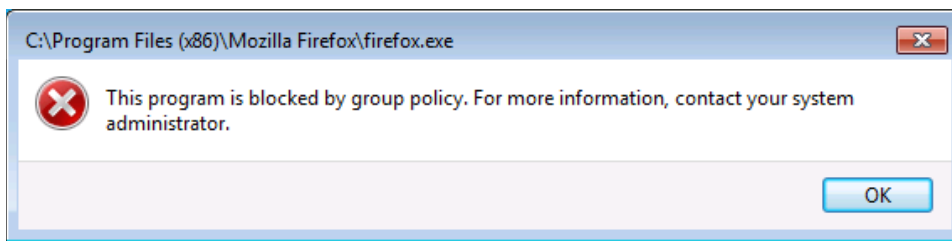
6. You will receive an alert that the program is being blocked by group policy. Click “OK”.



7. Left click the start button and type **firefox**. Double click the “Mozilla Firefox” search result.



8. You will receive the same group policy alert. Click “OK”.



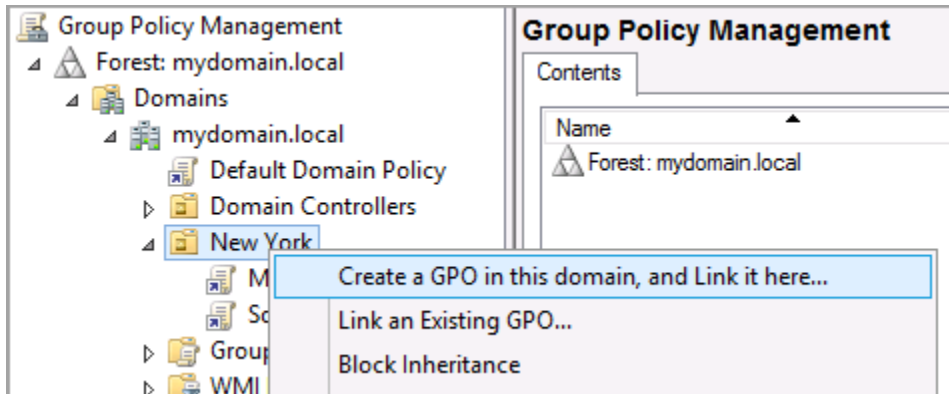


### 3 AppLocker

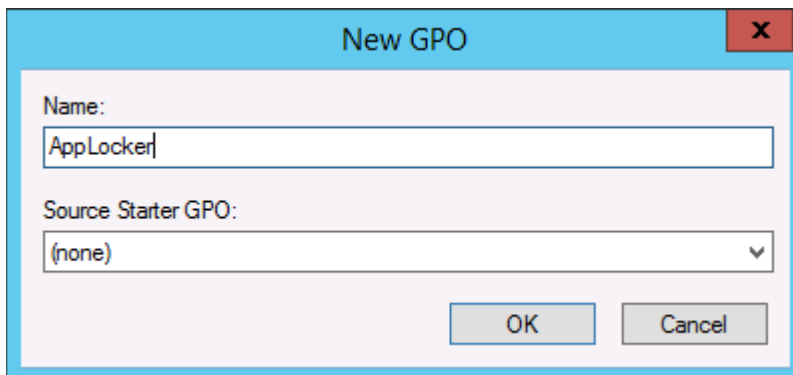
AppLocker can be identified as an improved version of software restriction.

#### 3.1 Examining the AppLocker Group Policy

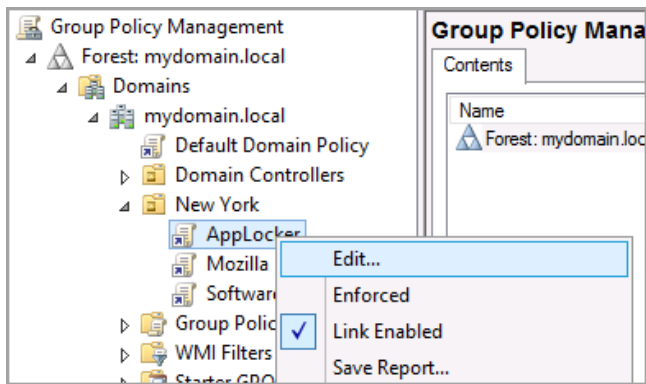
1. Return to the W2K12R2-ADDC machine. Right click on the “New York” OU and select “Create a GPO in this domain, and Link it here”.



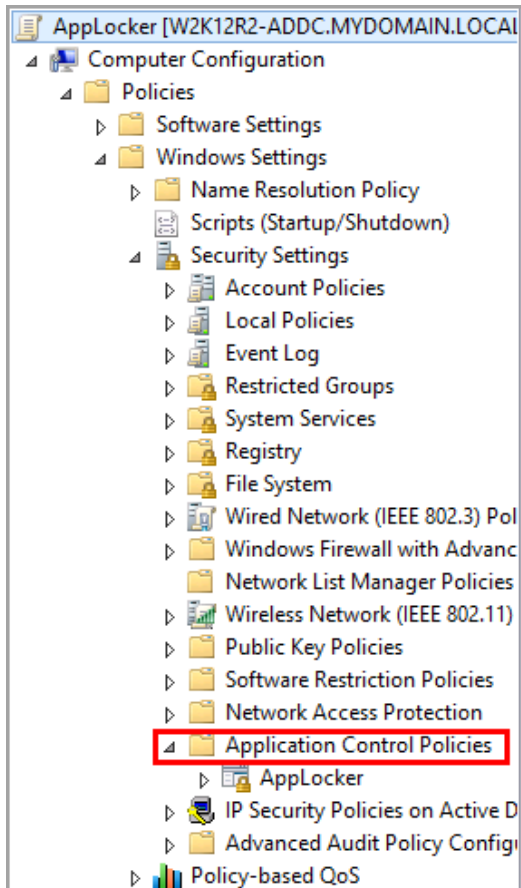
2. Type AppLocker for the name and click “OK”.



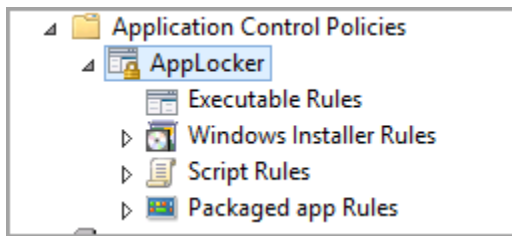
3. Right click the “AppLocker” OU and select “Edit”.



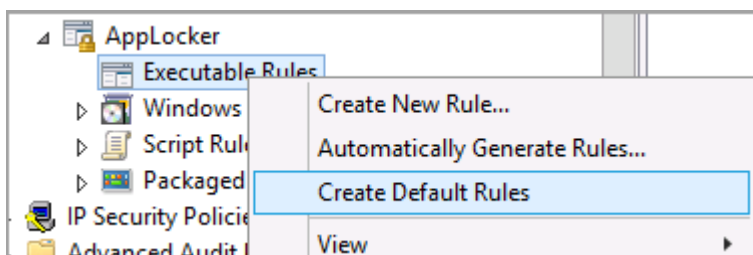
4. Under “Computer Configuration”, expand “Policies”, expand “Windows Settings”, expand “Security Settings” and expand “Application Control Policies”.



- Expand “AppLocker”, and we can see four distinct categories.



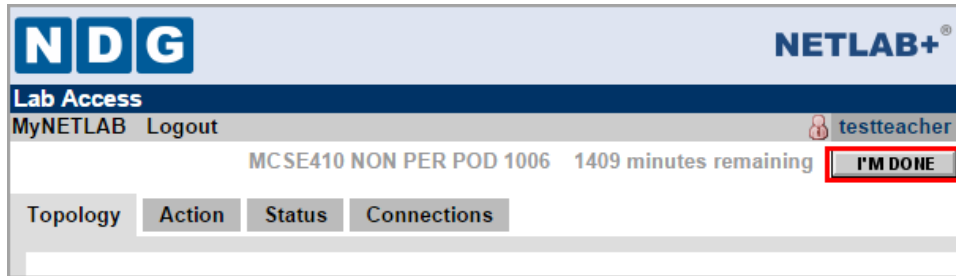
- Left click, then right click “Executable Rule” and notice that we have a couple of options. Click “Create Default Rules”.



- The default rules will appear in the right hand pane and are set to “Allow” by default. These default rules can be imported, exported and edited.

Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

Take any screenshots and notes required by your instructor and click “I’M DONE” at the top of the topology page. You may complete this lab as many times as you wish by making a new reservation.



## 4 Research (Optional)

1. System Center
2. AppLocker

## References

1. Windows Installer Package  
<http://technet.microsoft.com/en-us/library/cc978328.aspx>
2. How Software Restriction Policies Work  
<http://technet.microsoft.com/en-us/library/cc786941%28v=ws.10%29.aspx>
3. Create Your AppLocker Policies  
<http://technet.microsoft.com/en-us/library/ee791899.aspx>

