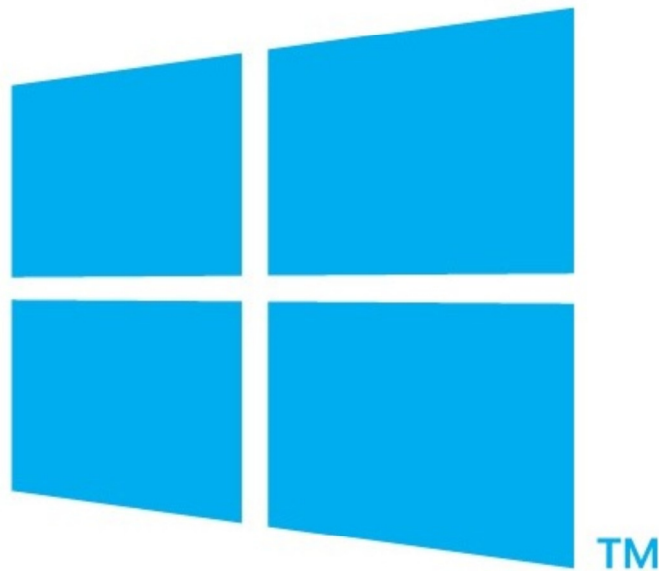




Department of Information Systems
Arkansas. A State of Technology.



GROUP POLICY SERVER 2012

Prepared By
DIS APSCN/LAN Support

Table of Contents

Tips for Group Policy	2
Major Categories of Group Policy	2
Group Policy for Server 2008	3
Enforcing K12 State Security Policies for ACT723 through Group Policies.....	3
Setting Non-Student (Faculty) Password Requirements	3
Setting Student Password Requirements using Fine-grained password policies.	4
Retain Security Event Log for 90 Days	6
Security Event Auditing – Security Event Log Contents.....	6
Logon Banner.....	6
Locking Screen Saver.....	7
Create the WSUS Group Policy	7
Common K12 Group Policies.....	8
Redirect 'My Documents' to User's Home-Directory	8
Restrict Computers to Faculty Use Only.....	8
Disable Internet Access by Group Policy/Security Group.....	9
Group Policy for Server 2012	13
Enforcing K12 State Security Policies for ACT723 through Group Policies.....	13
Setting Non-Student (Faculty) Password Requirements	13
Setting Student Password Requirements using Fine-grained password policies.	13
Retain Security Event Log for 90 Days	17
Security Event Auditing – Security Event Log Contents.....	18
Logon Banner.....	18
Locking Screen Saver.....	18
Create the WSUS Group Policy	18
Common K12 Group Policies.....	19
Redirect 'My Documents' to User's Home-Directory	19
Restrict Computers to Faculty Use Only.....	20
Disable Internet Access by Group Policy/Security Group.....	21
Windows 10 group policy and Central Store	28-53

Tips for Group Policy

1. You can manage Group Policy from the server or any workstation with RSAT (Remote Server Administration Tools). It's better to manage from the newest OS you have. 2012 or Win8.
2. Local Group Policy only affects the local machine you have applied the local policy to. AD group policy applies to the Domain, Site, or OU you apply it to.
3. Policies are applied in order of precedence, Local (least amount of precedence), Site, Domain, OU.
4. Group Policy Results under Group Policy management will help determine what policies are applied and to what or whom.
5. Gpupdate and gpupdate /force are both asynchronous ways to apply GPOs
6. Use Security Filtering to provide or deny access to a GPO based on groups or a user.

Major Categories of Group Policy

Group Policy Category	Where in Group	OS
Administrative Templates	User or Computer > Policies > Administrative Templates	Windows 2000+
Security Settings	User or Computer > Policies > Windows Settings > Security Settings	Windows 2000+
Wired Network	Computer > Policies > Windows Settings > Security Settings > Wired Network	Windows Vista+
Wireless Network	Computer > Policies > Windows Settings > Security Settings > Wireless Network	Windows XP and Vista+
Scripts	Computer > Policies > Windows Settings > Scripts (Startup/Shutdown) > Windows	

	Settings > Script (Logon/Logoff)	
Group Policy Software Installation	Computer or User > Policies > Software Settings	Windows 2000+
Folder Redirection	User > Policies > Windows Settings > Folder Redirection	Windows 2000+
Disk Quotas	Computer > Policies > Administrative Templates > System > Disk Quotas	Windows 2000+
Encrypted Data Recovery Agents	Computer > Policies > Windows Settings > Security Settings > Public Key > Policies > Encrypting File System	Windows 2000+
Internet Explorer Maintenance	User > Policies > Windows Settings > Internet Explorer Maintenance	Windows 2000+
Software Restriction Policies	Computer > Policies > Windows Settings > Security Settings > Software Restriction Policies	Windows XP+
Windows Search	Computer > Policies > Administrative Templates > Windows Components > Search	Windows Vista+
Group Policy Preference Extensions	Computer > Preferences (Only domain policies)	Windows Server 2008, Windows 7, and Windows 8. Additional download for Windows XP and Vista.

Group Policy for Server 2008

Enforcing K12 State Security Policies for ACT723 through Group Policies

Setting Non-Student (Faculty) Password Requirements

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Expand Forest: **yourdomain.local**.
3. Expand Domains and then expand **yourdomain.local**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.
6. Set the respective settings as shown below:

Enforce password history	6 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

7. Close the Group Policy Editor.

Setting Student Password Requirements using Fine-grained password policies.

This requires all domain controllers to be Windows Server 2008 and a Domain Functional Level of Windows 2008.

***** PERFORM 'SYSTEM STATE' BACKUPS OF DOMAIN CONTROLLERS BEFORE PROCEEDING
– THE EDITOR USED FOR THIS IS VERY POWERFUL AND CAN CAUSE SEVERE DAMAGE TO
ACTIVE DIRECTORY IF CAUTION IS NOT USED *****

1. From the Administrative Tools menu open **ADSI Edit**.
2. Click on **Action > Connect To** and click **OK** to take the default settings.
3. Double-click on the **Default Naming Context** that was added to the left-hand pane.
4. Double-click the Domain container (DC=school,DC=local).
5. Navigate to **CN=System, CN=Password Settings Container**.
6. Right-click on the **CN=Password Settings Container**, and choose **New, Object**.
7. Select **msDS-PasswordSettings**, and click **Next** to continue.

Set the attributes to be set in the table on the next page.

Attribute Name	Description	Value To Be Entered
CN	Common-Name	Student Password Policy
msDS-PasswordSettingsPrecedence	Password Settings Precedence	20
msDS-PasswordReversible	Password reversible encryption....	FALSE
msDS-PasswordHistory	Number of passwords "remembered".	6
msDS-PasswordComplexityEnabled	Force Complex Passwords	TRUE
msDS-MinimumPasswordLength	Minimum characters	8
msDS-MinimumPasswordAge	Days before password can be changed	1:00:00:00
msDS-MaximumPasswordAge	Force password change every 180 days.	180:00:00:00
msDS-LockoutThreshold	Invalid logon attempts before locking user account.	3
msDS-LockoutObservationWindow	Length of time before invalid password attempt counter is reset. 10 Minutes	0:00:10:00
msDS-LockoutDuration	Time user account will be locked for once the account login attempt threshold has been met. 15 Minutes	0:00:15:00
Click Finish Edit Policy again		
msDS-PSOAppliesTo	This is the distinguished name of the Global Security Group that your students are a member of	See next line for example. THIS IS CASE SENSITIVE TO YOUR ENVIRONMENT
Then add Group		
CN=Students,OU=Students,DC=school,DC=local		

Retain Security Event Log for 90 Days

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Expand Forest: **yourdomain.local**.
3. Expand Domains and then expand **yourdomain.local**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Event Log**.
6. Set the policy setting **Retain Security Event Log** to **90** days. You will automatically be prompted to change the retention method to days.
7. Set the Maximum Security Log Size to 131072 kilobytes (128MB).

**Auto-backup and clear event log when log file size limit is reached:
(Vista & 2008 Only – All other computers with log files at maximum size must be cleared manually and saved.)**

8. Expand **Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security**.
9. Enable the **Backup log automatically when full** setting.
10. Enable the **Retain old events** setting.

Close the Group Policy Editor

Security Event Auditing – Security Event Log Contents

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Expand Forest: **yourdomain.local**.
3. Expand Domains and then expand **yourdomain.local**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
6. Enable **Success AND Failure** auditing for the following Policy Settings:
 - a. Audit Account Logon Events
 - b. Audit Account Management
 - c. Audit logon event
 - d. Audit policy change

Logon Banner

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Expand Forest: **yourdomain.local**.
3. Expand Domains and then expand **yourdomain.local**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
6. Enable the following:
 - a. Interactive logon: Message text for users attempting to log on.
 - b. Interactive logon: Message title for users attempting to log on.

Locking Screen Saver

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Expand Forest: **yourdomain.local**.
3. Expand Domains and then expand **yourdomain.local**.
4. Right-click the **Default Domain Policy** and click **Edit**.
5. Expand **User Configuration > Policies > Administrative Templates > Control Panel > Personalization**.
6. Set the **Enable Screen Saver** policy to **Enabled**.
7. Set the **Password Protect the Screen Saver** policy to **Enabled**.
8. Set the **Screen Saver timeout** to **Enabled** and a time of **300** seconds (5 Minutes).

Create the WSUS Group Policy

1. Click **Start, Administrative Tools**, and then **Group Policy Management**.
2. Create a new policy named **WSUS Policy**.
3. Right click on the policy to open the Group Policy Editor.
4. Expand **Computer Configuration, Policies, Administrative Templates, Windows Components**. Click on **Windows Update**.
5. In the right hand pane double click on **Configure Automatic Updates**.
6. Select the radio button next to **Enabled**.
7. In the Configure automatic updating drop-down menu, select option **4**.
8. Set the desired scheduled install day and time.
9. Click the **Next Setting** button.

You should now be at the **Specify Intranet Microsoft Update Services Location** window.

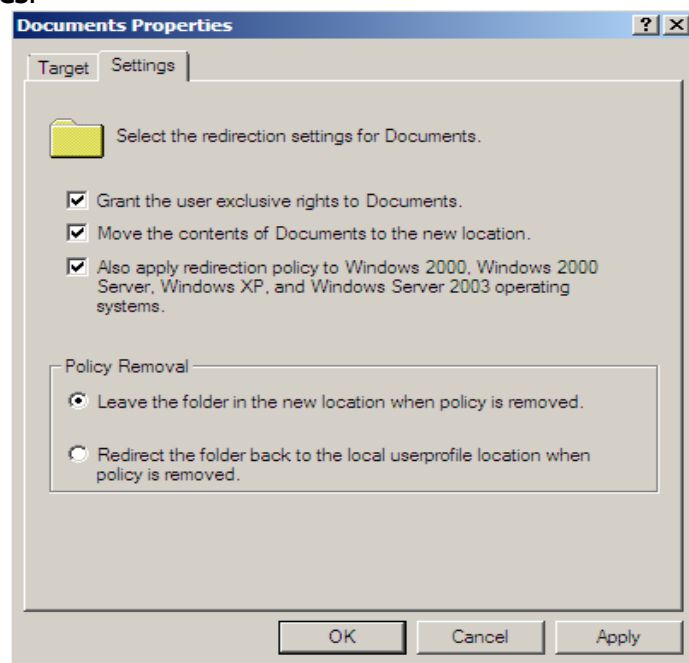
10. Select the radio button next to **Enabled**.
11. In both entry boxes enter <http://yourservername> and then click **OK**.
12. Double-click on **Reschedule Automatic Updates Scheduled Installations**.
13. Select the radio button next to **Enabled**.
14. Change the minutes from 1 to 5.
15. Click **OK**.
Double-click on **No auto-restart for scheduled Automatic Updates installations** window.
16. Select the radio button next to your desired option.
17. Click **OK**.
Double-click on **Automatic Updates detection frequency** window.
18. Select the radio button next to **Enabled**.
19. Set the desired interval.
20. Click **OK**.
Double-click **Allow Automatic Updates immediate installation** window.
21. Select the radio button next to **Enabled** and then click the **Next Setting** button.
22. Click **OK** to return to the Group Policy Editor.
23. Click **File** and then **Exit** to return to Active Directory Users & Computers.
24. Click **Close** at the properties window and then close the Active Directory Users & Computers

Common K12 Group Policies

Redirect 'My Documents' to User's Home-Directory

This policy can be either built as a separate policy or it can be added to the **Default Domain Policy**. This example adjusts the Default Domain Policy.

7. Click **Start, Administrative Tools**, and then **Group Policy Management**.
8. Expand Forest: **yourdomain.local**.
9. Expand Domains and then expand **yourdomain.local**.
10. Right-click the **Default Domain Policy** and click **Edit**.
11. Expand **User Configuration > Policies > Windows Settings > Folder Redirection**.
12. Right click on **Documents** and click **Properties**.
13. Change the setting to **Basic – Redirect everyone's folder to the same location**.
14. Set the **Target folder location** to **Redirect to the user's home directory**.
15. Click on the **Settings** tab.
16. Select the box **"Also apply redirection policy to Windows 2000....."**
17. Click **Apply** and then **OK**. If prompted to also redirect Pictures, Music, etc.. to the Home Directory, click **Yes**.



18. Close the Group Policy Object Editor.
19. Click **OK** to close the domain properties window.
20. Close **Active Directory Users & Computers**.

The My Documents folder will now automatically point to the user's home directory on Windows 2000 & XP machines. Files stored within the profile on the local machine will automatically be moved to the user's home directory on the server when the user logs on.

Restrict Computers to Faculty Use Only

Through the creation of this policy, you will be able to restrict computers of your choice to only allow members of the faculty to log on. This would make it so that students would not be allowed to log on to a teacher's desk computer, office computer, etc. This policy will be based off of the Faculty User group. You can adjust this policy to meet the group of users that meets your needs.

Process: Create Security Group, Create Policy, Add Computer Accounts to Security Group.

1. Open Active **Directory Users and Computers** (ADUC)
2. Create a security group called "**Faculty Use Only Computers**" in the OU of your choice. It is recommended that this policy be placed on the parent OU that your workstation computer accounts reside in.
3. Click **Start, Administrative Tools**, and then open **Group Policy Management**.
4. Expand Forest: **yourdomain.local**.
5. Expand Domains and then expand **yourdomain.local**.
6. Right-click yourdomain.local and select **Create a GPO in this domain, and link it here**.
7. Name the policy **Faculty Use Only Computers** and click **OK**.
8. In the left-hand pane, click on the new policy and click on the Scope tab in the right-hand pane.
9. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
10. Click the **Add** button.
11. In the box enter the group name "**Faculty Use Only Computers**" and then click the **OK** button.
12. Click on the **Details** tab and set **GPO Status** to **User Configuration Settings Disabled**.
13. In the left-hand pane, right-click the policy to open the **Group Policy Object Editor**.
14. Expand **Computer Configuration**.
15. Expand **Policies**.
16. Expand **Windows Settings**.
17. Expand **Security Settings**.
18. Expand **Local Policies**.
19. Click on **User Rights Assignment**.
20. In the right-hand window, double-click on "**Allow log on locally**".
21. In the properties window, place a check in the "**Define these policy settings**" box.
22. Click the **Add User or Group** button.
23. Add **Domain Admins, Administrators**, and **Faculty** to the list. When finished click **Apply** and **OK**.
24. Click **OK** to close the properties window for the Domain.
25. Add computers to the **Faculty Use Only Computers** security group to apply the policy. A reboot is required after the computer is added to and removed from the group to enforce/remove the policy.

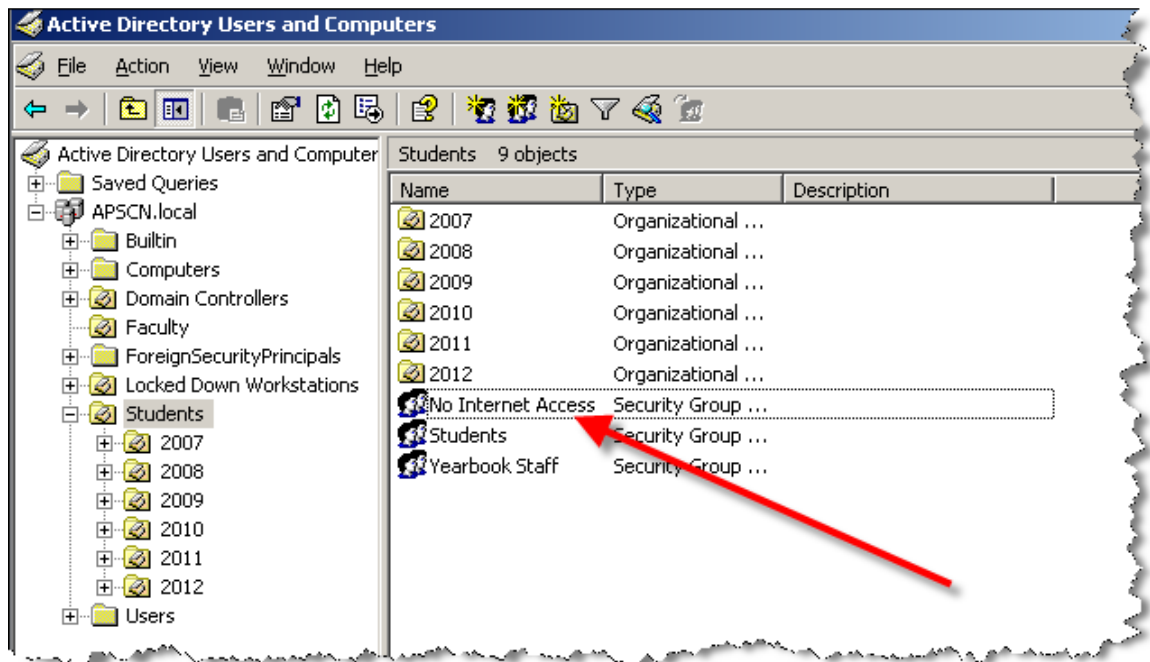
Disable Internet Access by Group Policy/Security Group

This process will step you through creating a group called "No Internet Access". When users lose the privileges to the Internet, they can simply be added to this group. They will only be able to get to the sites that you allow them to get to. When the user gets their privileges back, simply remove them from the group and they will have Internet access.

This process will have you create a webpage so that the user will know that their privileges have been revoked, rather than just an Internet Explorer error screen. **This section will only work if the browser is Internet Explorer.**

If Internet Information Services (IIS) are not installed, please see the IIS & Certificate Services installation section. IIS needs to be installed before proceeding.

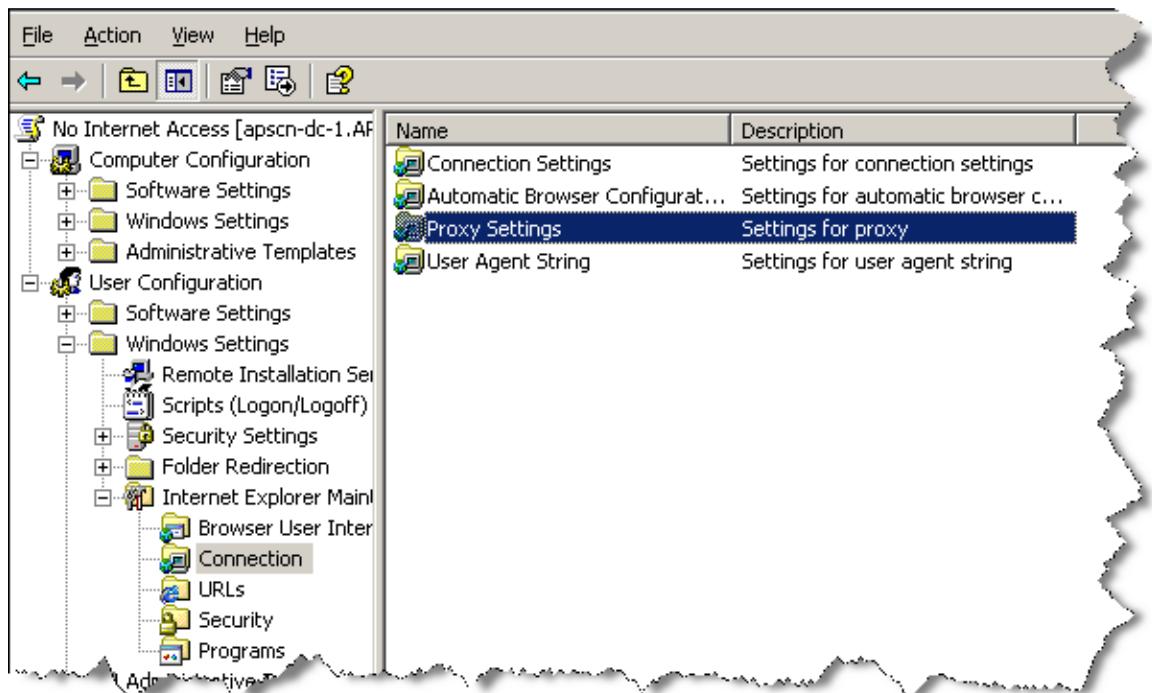
1. Open Active Directory Users and Computers.
2. Create a Security group called **"No Internet Access"** in the OU of your choice.



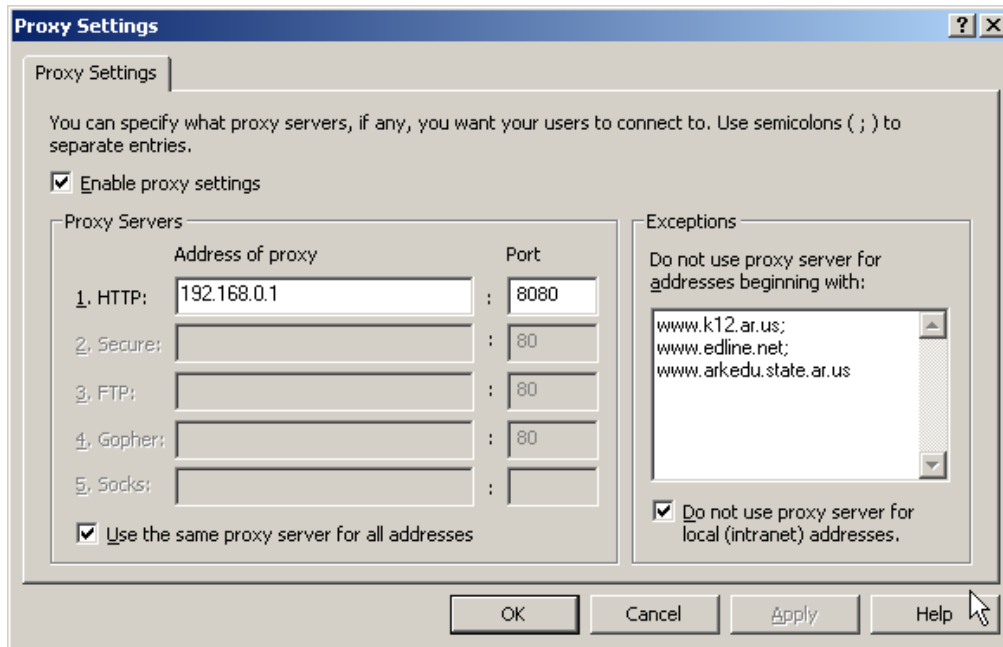
3. Right click on your domain (School.Local) and then click **Properties**. Select the Group Policy tab.
4. Click on the **New** button to create a new policy. Name the policy "No Internet Access".

2. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
3. Click the **Add** button.
4. In the box enter the group name "**No Internet Access**" and then click the **OK** button.
5. Select the No Internet Access policy from the list and then click Edit.

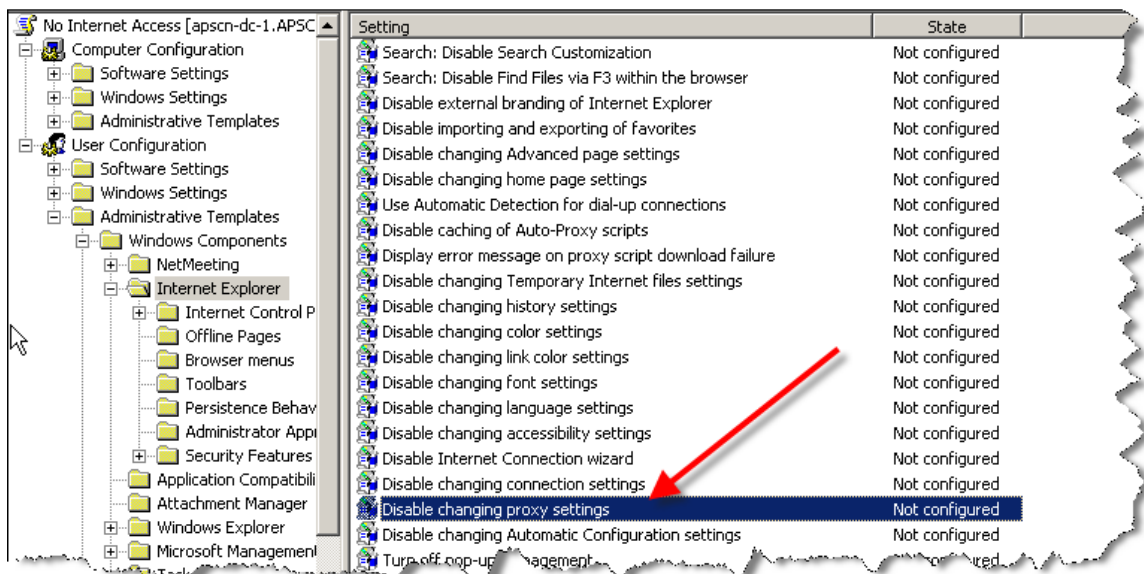
1. Expand **User Configuration**.
2. Expand **Policies**.
3. Expand **Windows Settings**.
4. Expand **Internet Explorer Maintenance**.
5. Select the **Connection** section and double click on "**Proxy Settings**" in the right window pane.



6. Check the **Enable Proxy Settings** option. Enter the IP address of your server for the **Address of Proxy**. Change the port from 80 to 8080. If there are websites that you wish users to still be able to access, such as your school website; enter those sites (separated by a semicolon) into the **Exceptions** box.



7. Click the **OK** button once you have entered in your settings.
8. Under User Configuration, expand **Administrative Templates**.
9. Expand **Windows Components**, Internet **Explorer**.
10. Double-click on the **Disable Changing Proxy Settings** option in the right-hand window pane.



11. Select the **Enabled** option and then click the **OK** button.
12. Close the Group Policy Editor.
13. Click the Close button to close the *Domain*.Local Properties Window.







To disable the Internet for any user, simply add them to the "No Internet Access" group. Remove the user to give access back to the Internet.

Group Policy for Server 2012

Enforcing K12 State Security Policies for ACT723 through Group Policies

Setting Non-Student (Faculty) Password Requirements

8. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
9. Expand Forest: **yourdomain.local**.
10. Expand Domains and then expand **yourdomain.local**.
11. Right-click the **Default Domain Policy** and click **Edit**.
12. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.
13. Set the respective settings as shown below:

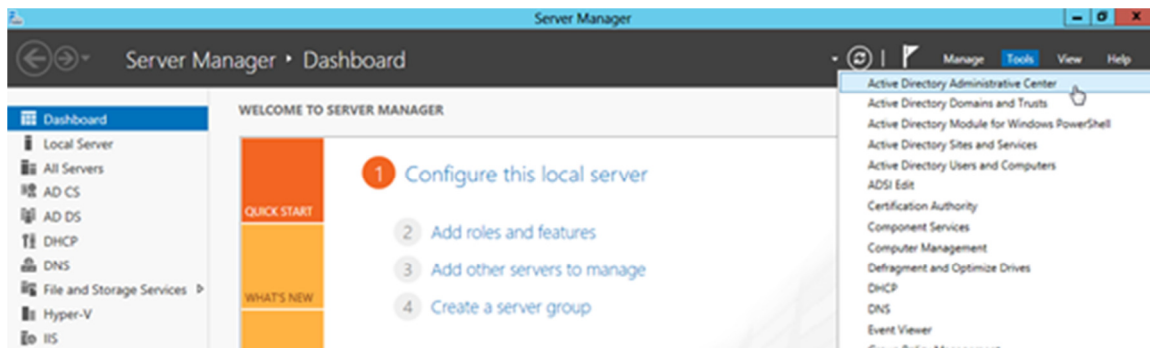
 Enforce password history	6 passwords remembered
 Maximum password age	90 days
 Minimum password age	1 days
 Minimum password length	8 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled

14. Close the Group Policy Editor.

Setting Student Password Requirements using Fine-grained password policies.

In Server 2012 you are able to create a Fine Grained Password Policy easier than before in 2008. Instead of setting it up in Group Policy Management or creating it through ASDI, you can now easily set it up through the GUI.

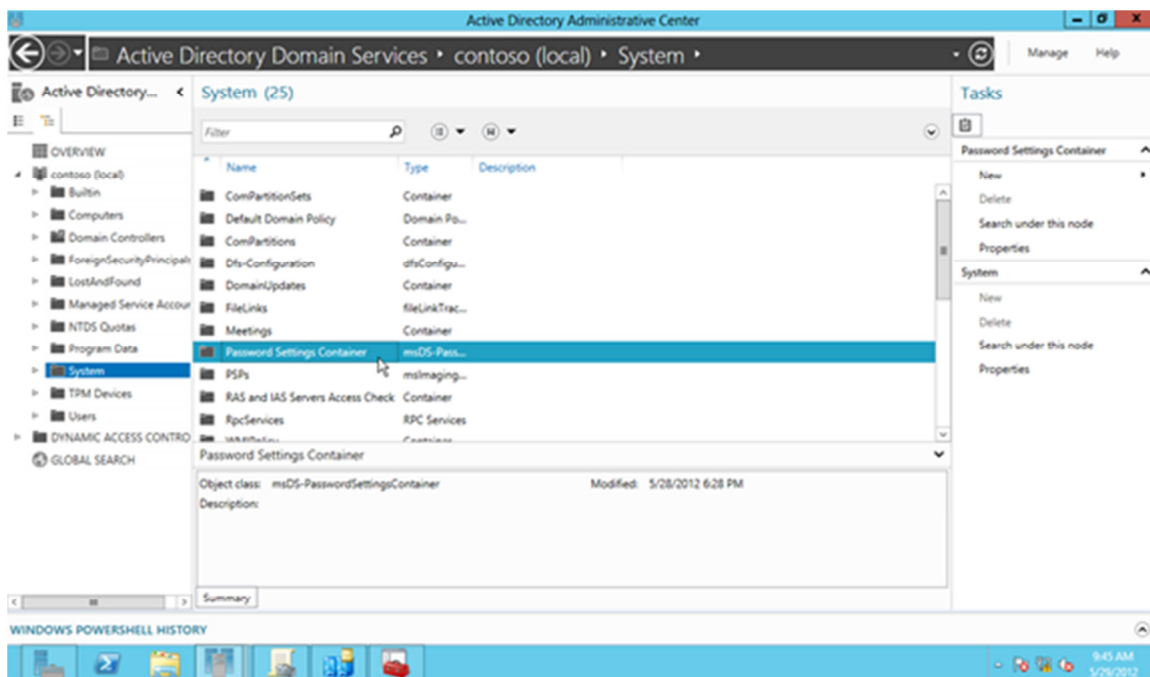
1. Open **Server Manager**.
2. Go to tools and open **Active Directory Administrative Center**.



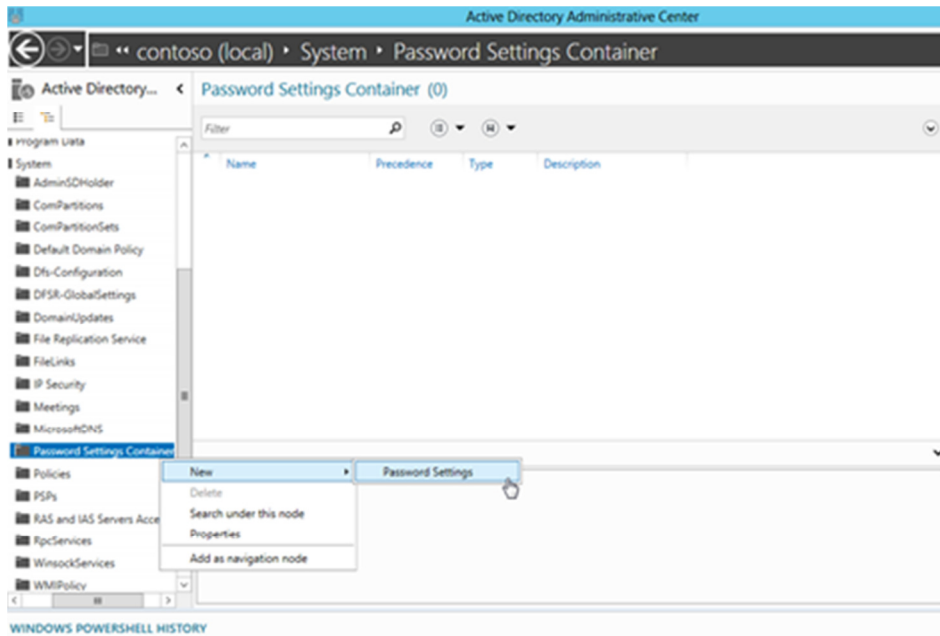
3. Click on **Tree View**.



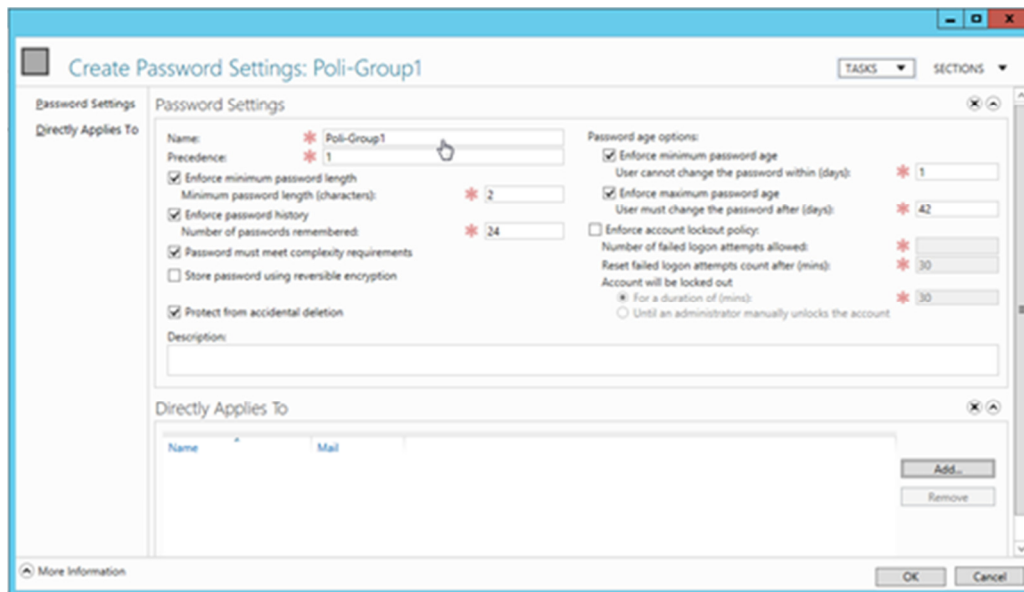
4. Navigate to **System** container then **Password Settings Container**.



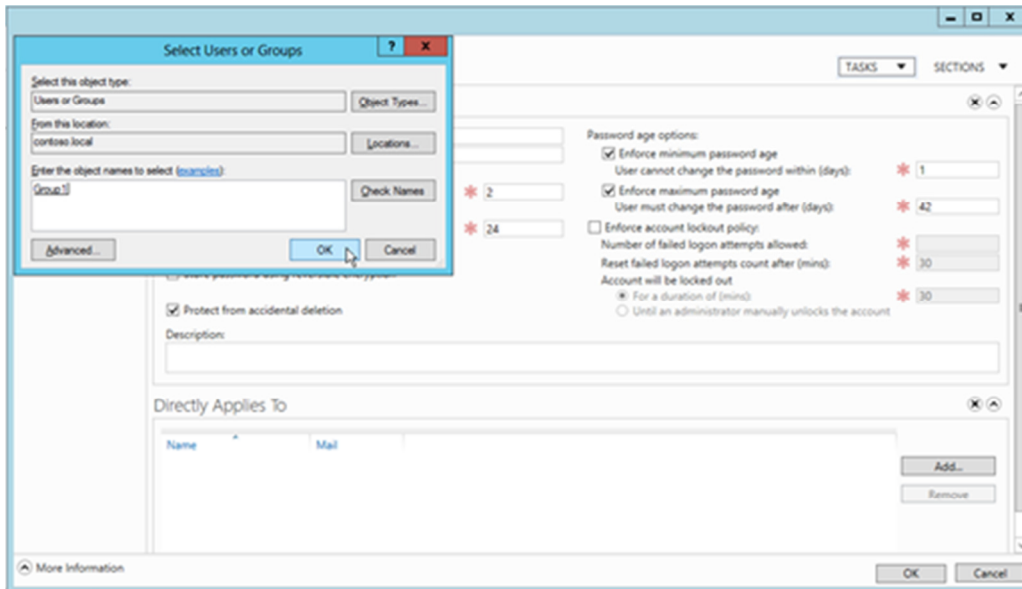
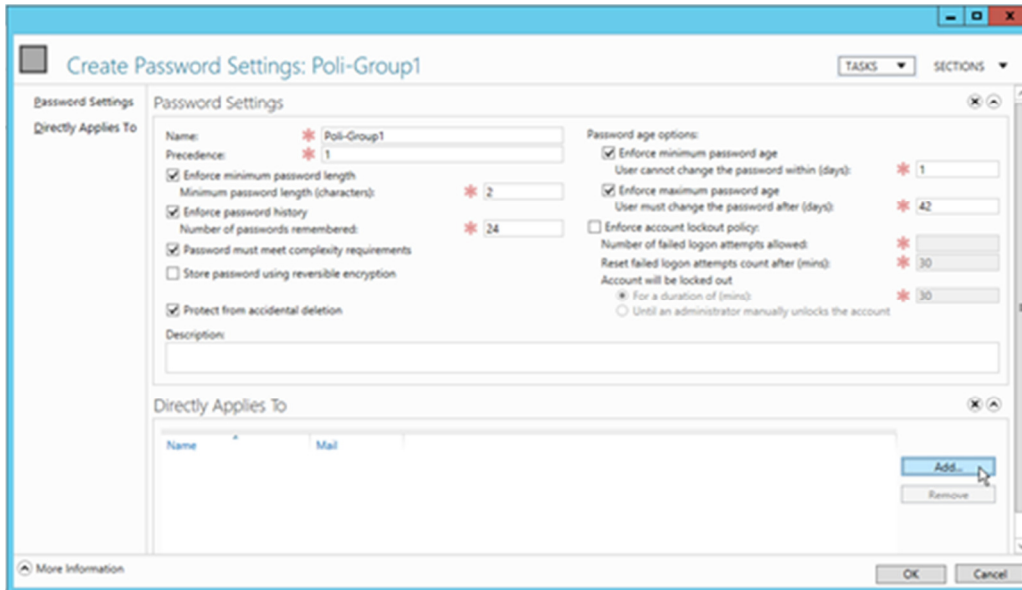
5. Right click **Password Settings Container**, then **New-Password Policy**

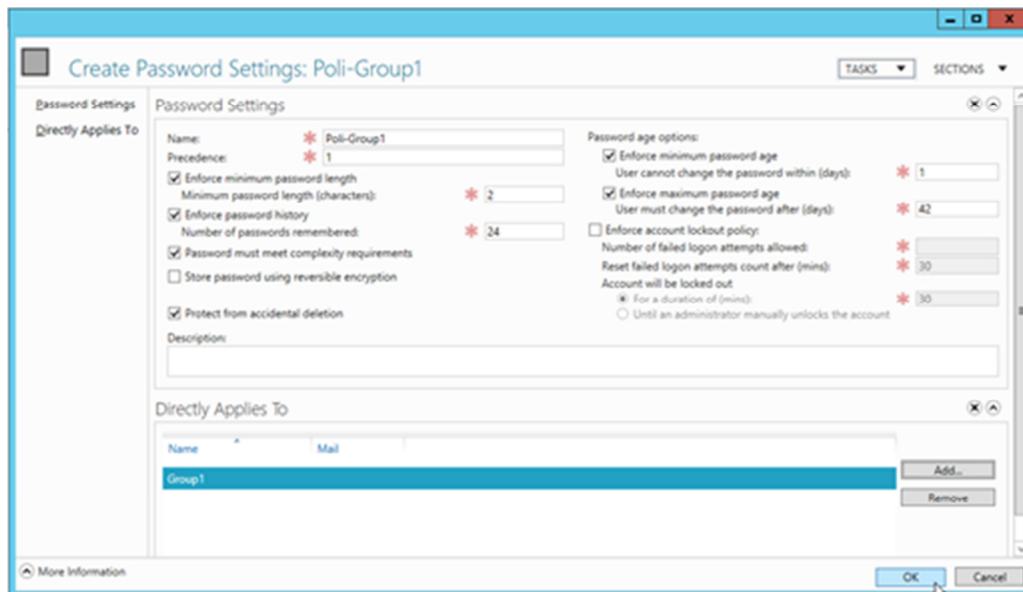


6. Specify the password policy settings for each of the required policies



7. Click add to link the created policy to users security group **Students**





Retain Security Event Log for 90 Days

11. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
12. Expand Forest: **yourdomain.local**.
13. Expand Domains and then expand **yourdomain.local**.
14. Right-click the **Default Domain Policy** and click **Edit**.
15. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Event Log**.
16. Set the policy setting **Retain Security Event Log** to **90** days. You will automatically be prompted to change the retention method to days.
17. Set the Maximum Security Log Size to 131072 kilobytes (128MB).

**Auto-backup and clear event log when log file size limit is reached:
(Vista & 2008 Only – All other computers with log files at maximum size must be cleared manually and saved.)**

18. Expand **Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security**.
19. Enable the **Backup log automatically when full** setting.
20. Enable the **Retain old events** setting.

Close the Group Policy Editor

Security Event Auditing – Security Event Log Contents

7. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
8. Expand Forest: **yourdomain.local**.
9. Expand Domains and then expand **yourdomain.local**.
10. Right-click the **Default Domain Policy** and click **Edit**.
11. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
12. Enable **Success AND Failure** auditing for the following Policy Settings:
 - a. Audit Account Logon Events
 - b. Audit Account Management
 - c. Audit logon event
 - d. Audit policy change

Logon Banner

21. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
22. Expand Forest: **yourdomain.local**.
23. Expand Domains and then expand **yourdomain.local**.
24. Right-click the **Default Domain Policy** and click **Edit**.
25. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
26. Enable the following:
 - a. Interactive logon: Message text for users attempting to log on.
 - b. Interactive logon: Message title for users attempting to log on.

Locking Screen Saver

9. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
10. Expand Forest: **yourdomain.local**.
11. Expand Domains and then expand **yourdomain.local**.
12. Right-click the **Default Domain Policy** and click **Edit**.
13. Expand **User Configuration > Policies > Administrative Templates > Control Panel > Personalization**.
14. Set the **Enable Screen Saver** policy to **Enabled**.
15. Set the **Password Protect the Screen Saver** policy to **Enabled**.
16. Set the **Screen Saver timeout** to **Enabled** and a time of **300** seconds (5 Minutes).

Create the WSUS Group Policy

25. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
26. Create a new policy named **WSUS Policy**.
27. Right click on the policy to open the Group Policy Editor.

28. Expand **Computer Configuration, Policies, Administrative Templates, Windows Components**. Click on **Windows Update**.
29. In the right hand pane double click on **Configure Automatic Updates**.
30. Select the radio button next to **Enabled**.
31. In the Configure automatic updating drop-down menu, select option **4**.
32. Set the desired scheduled install day and time.
33. Click the **Next Setting** button.

You should now be at the **Specify Intranet Microsoft Update Services Location** window.

34. Select the radio button next to **Enabled**.
35. In both entry boxes enter <http://yourservername> and then click **OK**.
36. Double-click on **Reschedule Automatic Updates Scheduled Installations**.
37. Select the radio button next to **Enabled**.
38. Change the minutes from 1 to 5.
39. Click **OK**.
Double-click on **No auto-restart for scheduled Automatic Updates installations** window.
40. Select the radio button next to your desired option.
41. Click **OK**.
Double-click on **Automatic Updates detection frequency** window.
42. Select the radio button next to **Enabled**.
43. Set the desired interval.
44. Click **OK**.
Double-click **Allow Automatic Updates immediate installation** window.
45. Select the radio button next to **Enabled** and then click the **Next Setting** button.
46. Click **OK** to return to the Group Policy Editor.
47. Click **File** and then **Exit** to return to Active Directory Users & Computers.
48. Click **Close** at the properties window and then close the Active Directory Users & Computers

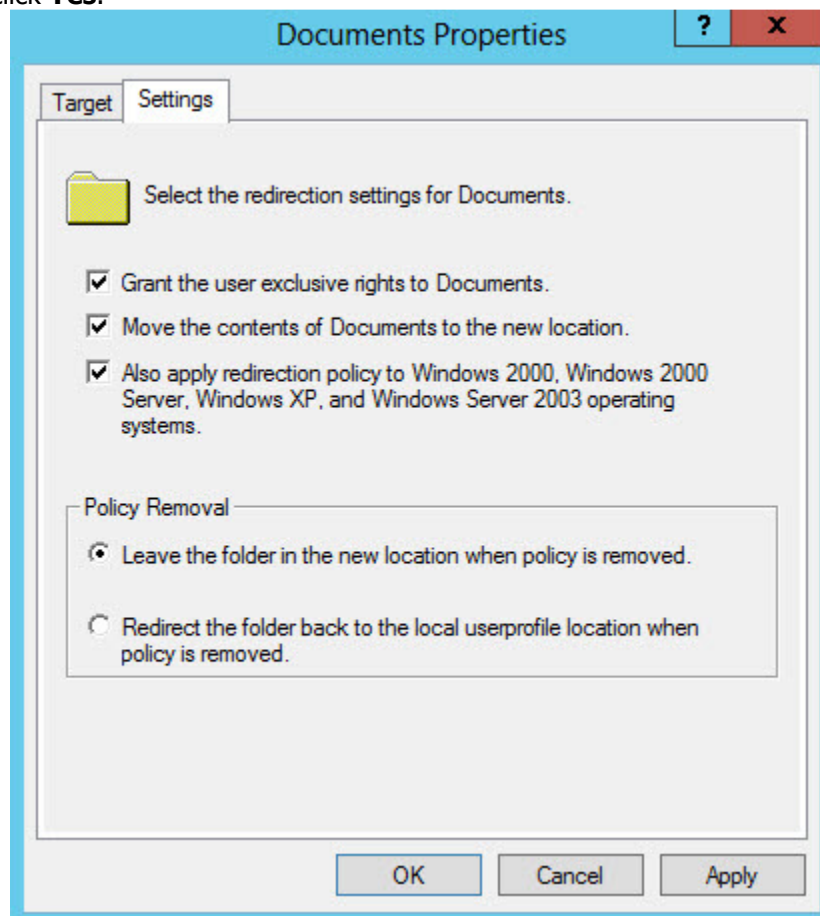
Common K12 Group Policies

Redirect 'My Documents' to User's Home-Directory

This policy can be either built as a separate policy or it can be added to the **Default Domain Policy**. This example adjusts the Default Domain Policy.

27. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
28. Expand Forest: **yourdomain.local**.
29. Expand Domains and then expand **yourdomain.local**.
30. Right-click the **Default Domain Policy** and click **Edit**.
31. Expand **User Configuration > Policies > Windows Settings > Folder Redirection**.
32. Right click on **Documents** and click **Properties**.
33. Change the setting to **Basic – Redirect everyone's folder to the same location**.
34. Set the **Target folder location** to **Redirect to the user's home directory**.

35. Click on the **Settings** tab.
36. Select the box "**Also apply redirection policy to Windows 2000.....**"
37. Click **Apply** and then **OK**. If prompted to also redirect Pictures, Music, etc.. to the Home Directory, click **Yes**.



38. Close the Group Policy Object Editor.
39. Click **OK** to close the domain properties window.
40. Close **Active Directory Users & Computers**.

The My Documents folder will now automatically point to the user's home directory on Windows 2000 & XP machines. Files stored within the profile on the local machine will automatically be moved to the user's home directory on the server when the user logs on.

Restrict Computers to Faculty Use Only

Through the creation of this policy, you will be able to restrict computers of your choice to only allow members of the faculty to log on. This would make it so that students would not be allowed to log on to a teacher's desk computer, office computer, etc. This policy will be based off of the Faculty User group. You can adjust this policy to meet the group of users that meets your needs.

Process: Create Security Group, Create Policy, Add Computer Accounts to Security Group.

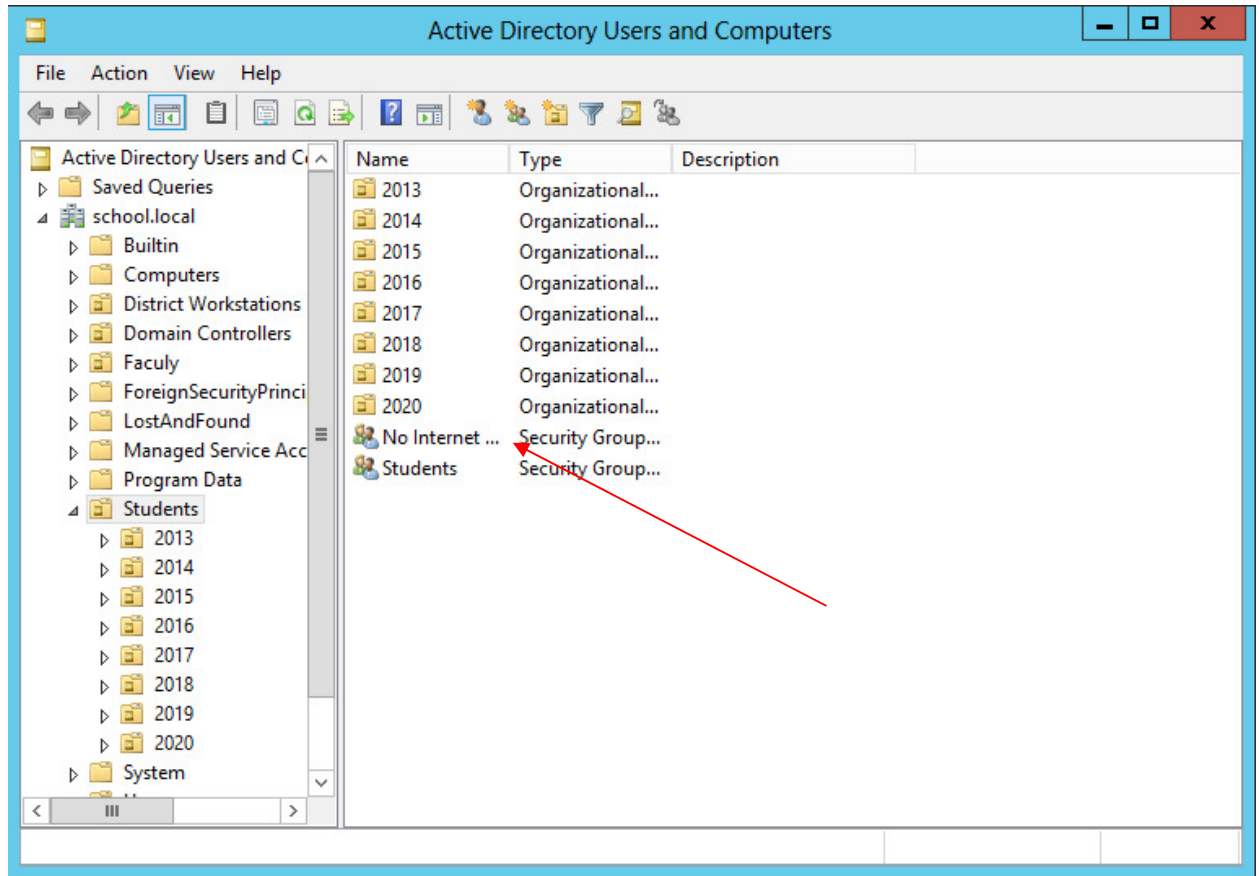
26. Open Active **Directory Users and Computers** (ADUC)

27. Create a security group called "**Faculty Use Only Computers**" in the OU of your choice. It is recommended that this policy be placed on the parent OU that your workstation computer accounts reside in.
28. Click **Start, Administrative Tools**, and then open **Group Policy Management**.
29. Expand Forest: **yourdomain.local**.
30. Expand Domains and then expand **yourdomain.local**.
31. Right-click yourdomain.local and select **Create a GPO in this domain, and link it here**.
32. Name the policy **Faculty Use Only Computers** and click **OK**.
33. In the left-hand pane, click on the new policy and click on the Scope tab in the right-hand pane.
34. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
35. Click the **Add** button.
36. In the box enter the group name "**Faculty Use Only Computers**" and then click the **OK** button.
37. Click on the **Details** tab and set **GPO Status** to **User Configuration Settings Disabled**.
38. In the left-hand pane, right-click the policy to open the **Group Policy Object Editor**.
39. Expand **Computer Configuration**.
40. Expand **Policies**.
41. Expand **Windows Settings**.
42. Expand **Security Settings**.
43. Expand **Local Policies**.
44. Click on **User Rights Assignment**.
45. In the right-hand window, double-click on "**Allow log on locally**".
46. In the properties window, place a check in the "**Define these policy settings**" box.
47. Click the **Add User or Group** button.
48. Add **Domain Admins**, **Administrators**, and **Faculty** to the list. When finished click **Apply** and **OK**.
49. Click **OK** to close the properties window for the Domain.
50. Add computers to the **Faculty Use Only Computers** security group to apply the policy. A reboot is required after the computer is added to and removed from the group to enforce/remove the policy.

Disable Internet Access by Group Policy/Security Group

Introduced in 2008, Group Policy Preferences is an extension of Group Policy. This makes making a GPO easier to create and also manage. In 2012 The proxy settings for Internet Explorer has removed from the original location and can be configured through Group Policy Preferences.

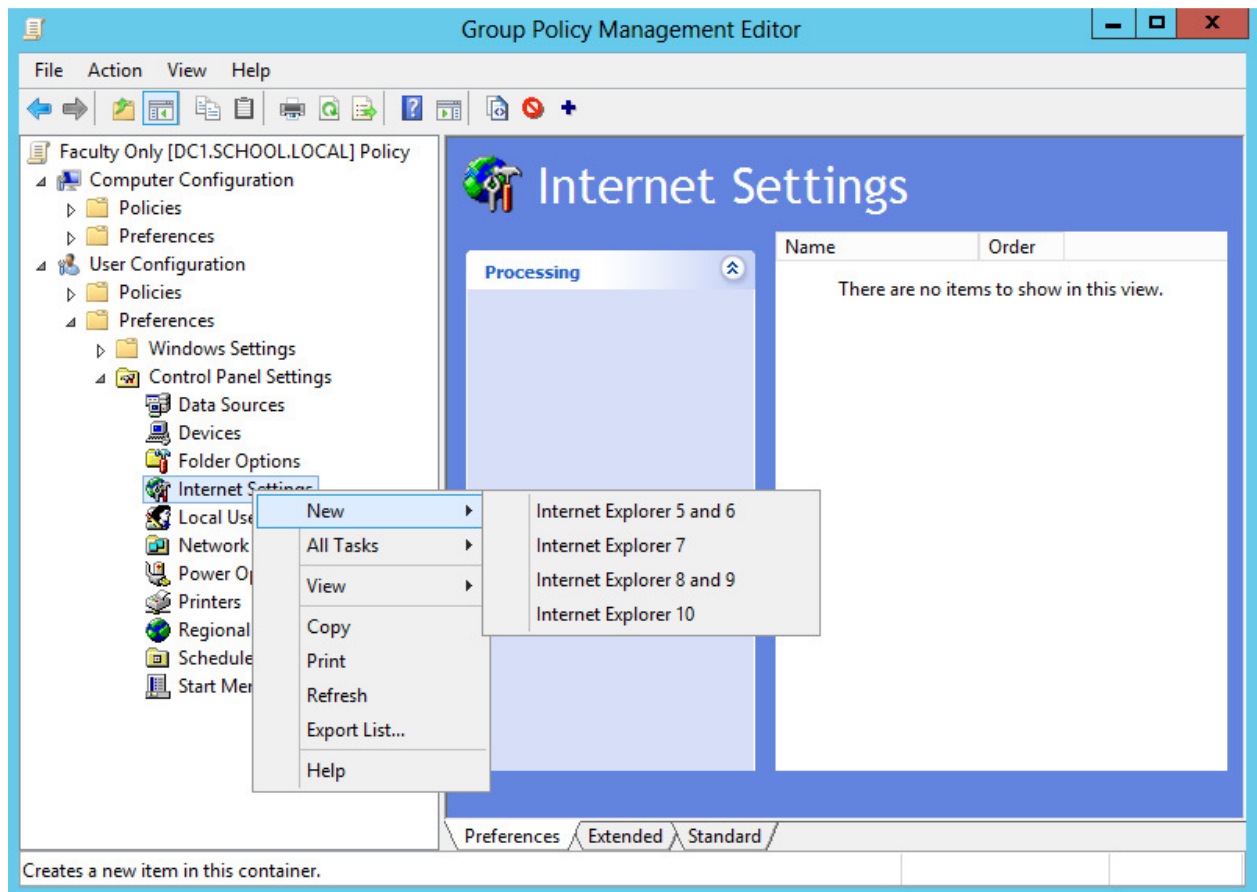
14. Open Active Directory Users and Computers.
15. Create a Security group called "**No Internet Access**" in the OU of your choice.



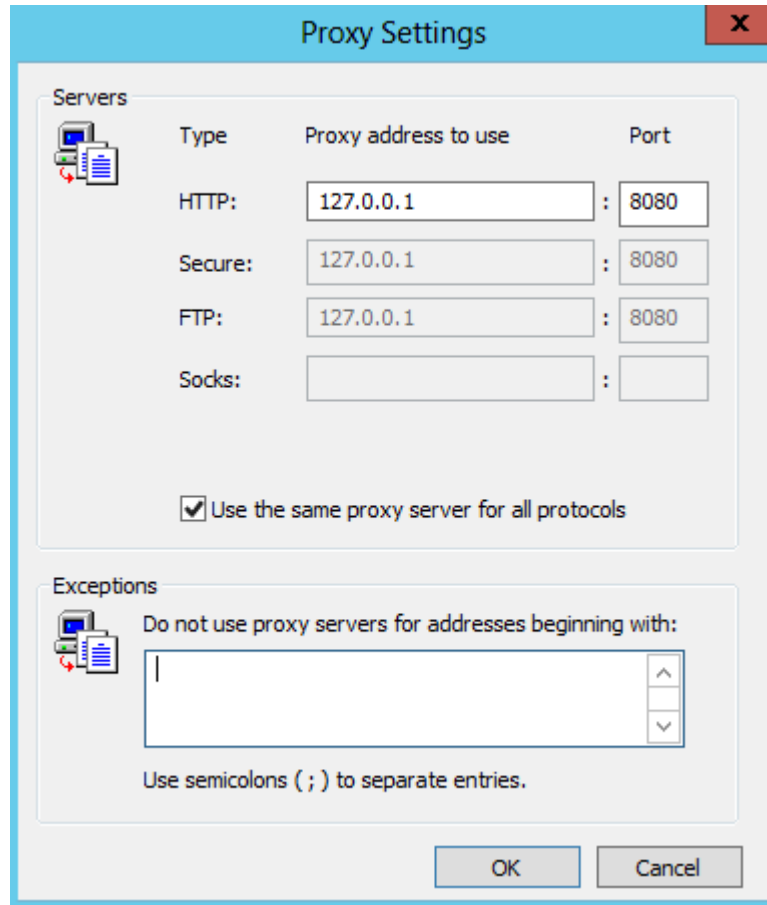
16. Open **Group Policy Management**

17. Click on the **New** button to create a new policy. Name the policy "No Internet Access".

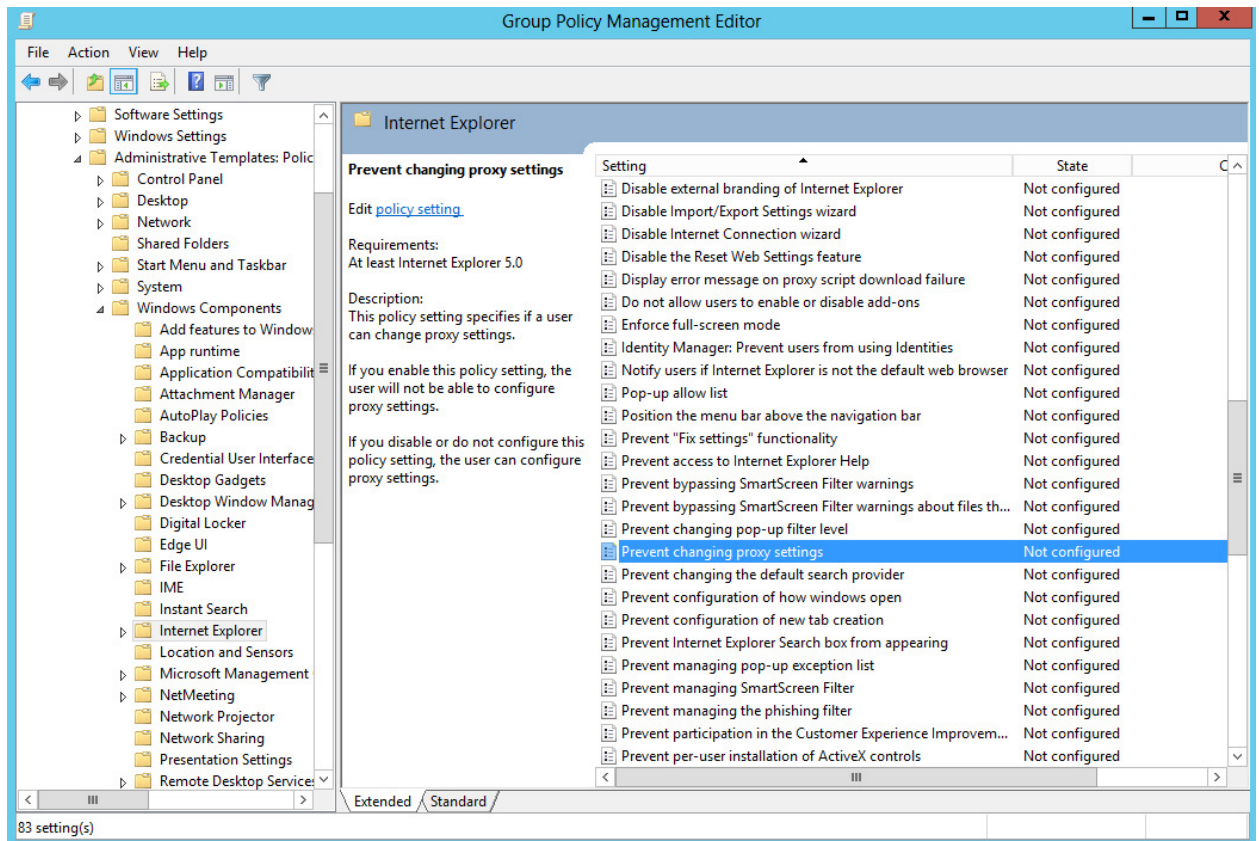
6. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
 7. Click the **Add** button.
 8. In the box enter the group name "**No Internet Access**" and then click the **OK** button.
 9. Select the No Internet Access policy from the list and then click Edit.
1. Expand **User Configuration**.
 2. Expand **Preferences**.
 3. Expand **Control Panel Settings**.
 4. Expand **Internet Settings**.
 5. Right click and highlight **New**, then select your Internet Explorer Browser.



6. Click on the **Connections** tab then check **Proxy Server**. Enter the IP address of your server for the **Address of Proxy**. Change the port from 80 to 8080. If there are websites that you wish users to still be able to access, such as your school website; click advanced and enter those sites (separated by a semicolon) into the **Exceptions** box.



7. Click the **OK** button once you have entered in your settings.
8. Under **User Configuration, Policies**, expand **Administrative Templates**.
9. Expand **Windows Components, Internet Explorer**.
10. Double-click on the **Prevent changing proxy settings** option in the right-hand window pane.

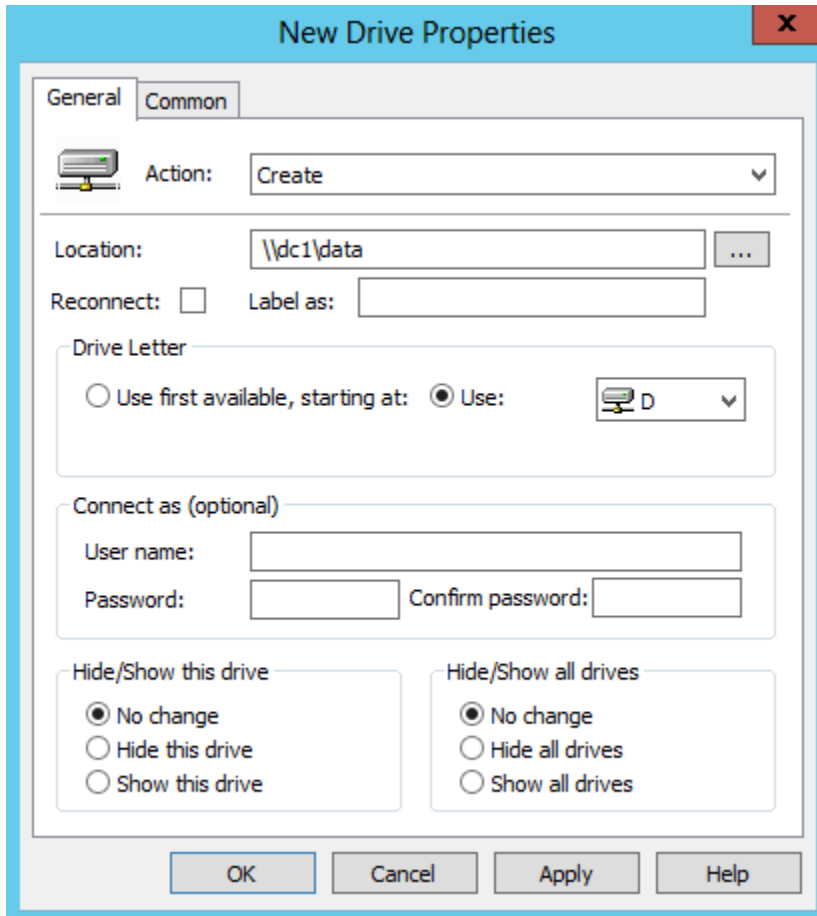


11. Select the **Enabled** option and then click the **OK** button.
12. Close the Group Policy Editor.
13. Click the Close button to close the *Domain*.Local Properties Window.

To disable the Internet for any user, simply add them to the "No Internet Access" group. Remove the user to give access back to the Internet.

Mapping Drives

1. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
2. Create a policy named **Mapped Data Drive**
3. Edit the policy
4. Under **User, Preferences**, expand **Windows Settings**.
5. Right click **Drive Maps**, highlight **new** and click on **Mapped Drive**
6. On the action tab leave it as **Create**.
7. On location, type in the UNC path to the drive or folder you are trying to create
8. Select which drive letter you want to use under **Drive Letter**
9. Click **Ok**

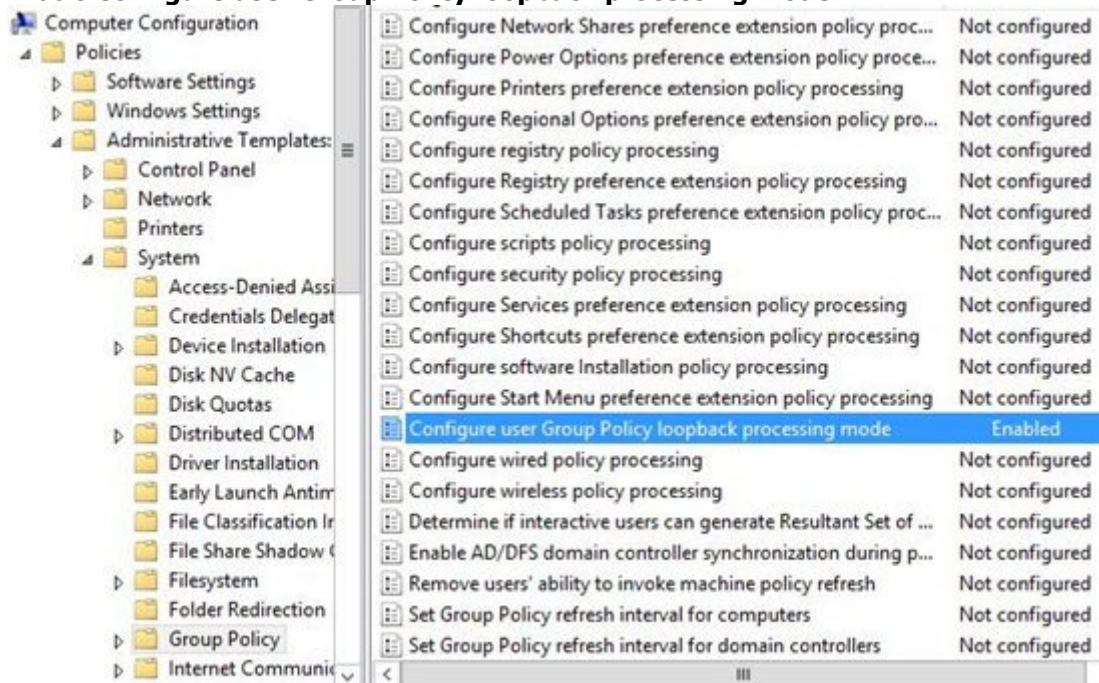


Loopback Processing

Loopback processing allows a computer to act like a user when applying a policy. This policy directs the system to apply the set of GPOs for the computer to any user who logs on to a computer. Examples of user policies are printers and internet settings

1. From **Start Menu** go to, **Administrative Tools**, and then **Group Policy Management** or from **Server Manager** go to, **Tools, Group Policy Management**
2. Create a policy named **Enable Loopback Processing**
3. Edit the policy
4. Under **Computer, Policies, Administrative Tools, System, Group Policy**

5. Enable **Configure user Group Policy loopback processing mode**



The Central Store

To take advantage of the benefits of .admx files, you must create a Central Store in the SYSVOL folder on a Windows domain controller. The Central Store is a file location that is checked by the Group Policy tools. The Group Policy tools use any .admx files that are in the Central Store. The files that are in the Central Store are later replicated to all domain controllers in the domain.

To create a Central Store for .admx and .adml files, create a folder that is named PolicyDefinitions in the following location (for example) on the domain controller:

```
\\contoso.com\SYSVOL\contoso.com\policies
```

Copy all files from the PolicyDefinitions folder on a source computer to the PolicyDefinitions folder on the domain controller. The source location can be either of the following:

- The C:\Windows folder on a Windows 8.1-based or Windows 10-based client computer
- The C:\Program Files (x86)\Microsoft Group Policy\client folder if you have downloaded any of the Administrative Templates separately

The PolicyDefinitions folder on the Windows domain controller stores all .admx files and .adml files for all languages that are enabled on the client computer.

The .adml files are stored in a language-specific folder. For example, English (United States) .adml files are stored in a folder that is named "en-US"; Korean .adml files are stored in a folder that is named "ko_KR"; and so on.

If .adml files for additional languages are required, you must copy the folder that contains the .adml files for that language to the Central Store. When you have copied all .admx and .adml files, the PolicyDefinitions folder on the domain controller should contain the .admx files and one or more folders that contain language-specific .adml files.

Note When you copy the .admx and .adml files from a Windows 8.1-based or Windows 10-based computer, verify that the most recent updates to these files are installed. Also, make sure that the most recent Administrative Templates files are replicated. This advice also applies to service packs, as applicable.

Group Policy administration

Windows 8.1 and Windows 10 do not include Administrative Templates that have an .adm extension. We recommend that you use computers that are running Windows 8.1 or later versions of Windows to perform Group Policy administration.

Updating the Administrative Templates files

In Group Policy for versions of Windows that are earlier than Windows Vista, if you change Administrative Templates policy settings on local computers, the Sysvol share on a domain controller within your domain is automatically updated to include the new .ADM files. Those changes are then replicated to all other domain controllers in the domain. This might increase the network load and storage requirements.

In Group Policy for Windows Server 2012 R2 and Windows 8.1, if you change Administrative Templates policy settings on local computers, Sysvol is not automatically updated to include the new .admx or .adml files. This change in behavior is implemented to reduce network load and disk storage requirements and to prevent conflicts between .admx and .adml files when changes are made to Administrative Templates policy settings across different locations.

To make sure that any local updates are reflected in Sysvol, you must manually copy the updated .admx or .adml files from the PolicyDefinitions file on the local computer to the Sysvol\PolicyDefinitions folder on the appropriate domain controller.

Most Common Central Store ERROR

SYSVOL and Group Policy out of Sync on Server 2012 R2 DCs using DFSR

Recently while making changes to group policy, I noticed a slew of issues between clients not accepting the policy. This eventually led me to the discovery that two of the DCs in this particular environment were not replicating properly and were resulting in inconsistent SYSVOL shares.

Symptoms

On the clients we were seeing the following errors when executing the **gpupdate** command:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\windows\system32>gpupdate
Updating policy...

Computer policy could not be updated successfully. The following errors were encountered:

The processing of Group Policy failed. Windows could not apply the registry-based policy settings for the Group Policy object LDAP://CN=Machine,cn={CF25ED30-3895-4147-8EB7-38789553F6A0},cn=policies,cn=system, .
Group Policy settings will not be resolved until this event is resolved. View the event details for more information on the file name and path that caused the failure.
User Policy update has completed successfully.

To diagnose the failure, review the event log or run GPRESULT /H GPREport.html from the command line to access information about Group Policy results.

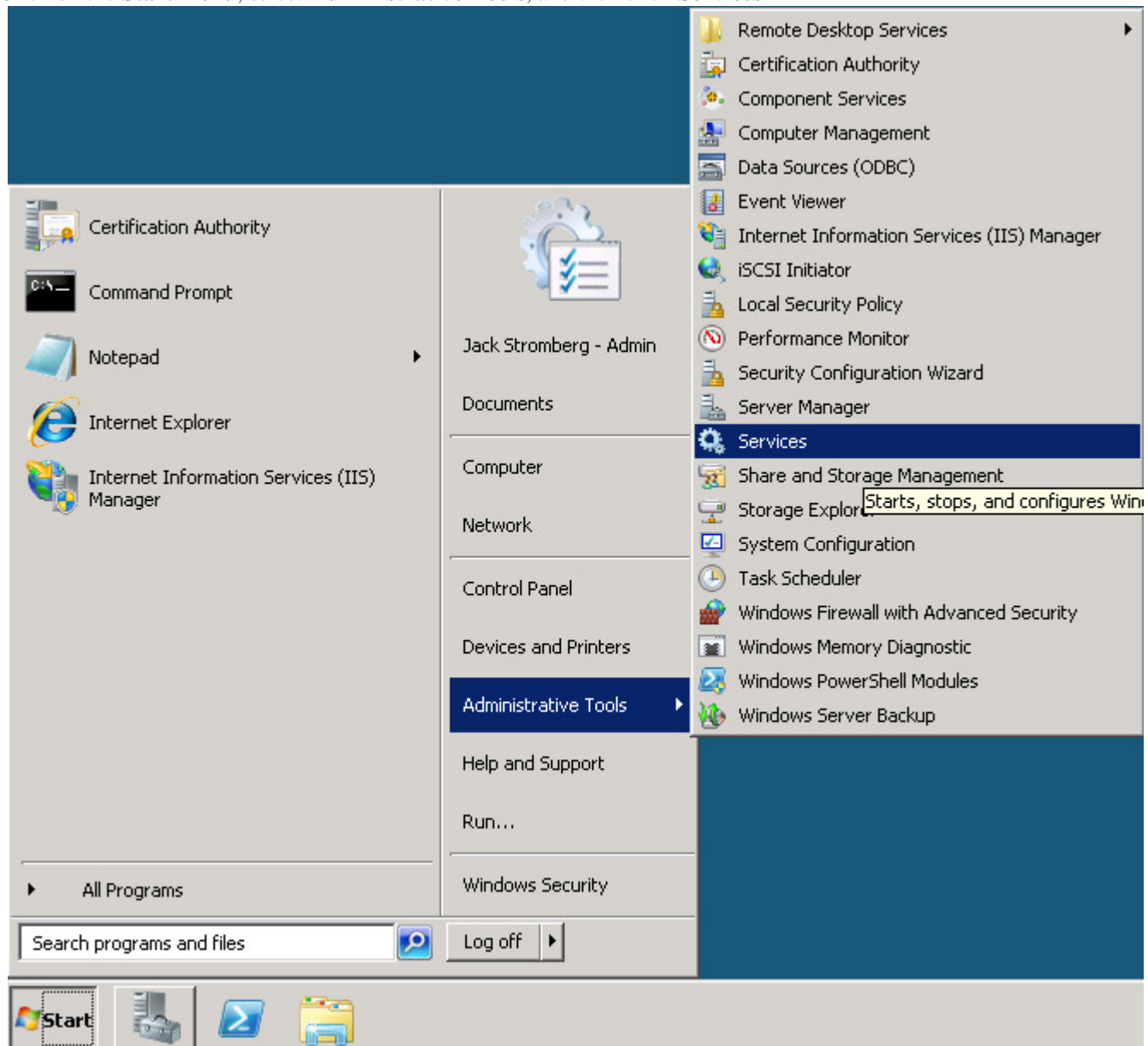
C:\windows\system32>_
```

Solution

Manually perform an authoritative synchronization between the two DCs. As you may know, DFSR no longer uses the same steps as FSR to do an authoritative sync. Below are my notes and experiences on completing an authoritative DFSR sync. You can find the official notes from Microsoft here: <http://support.microsoft.com/kb/2218556/en-us>

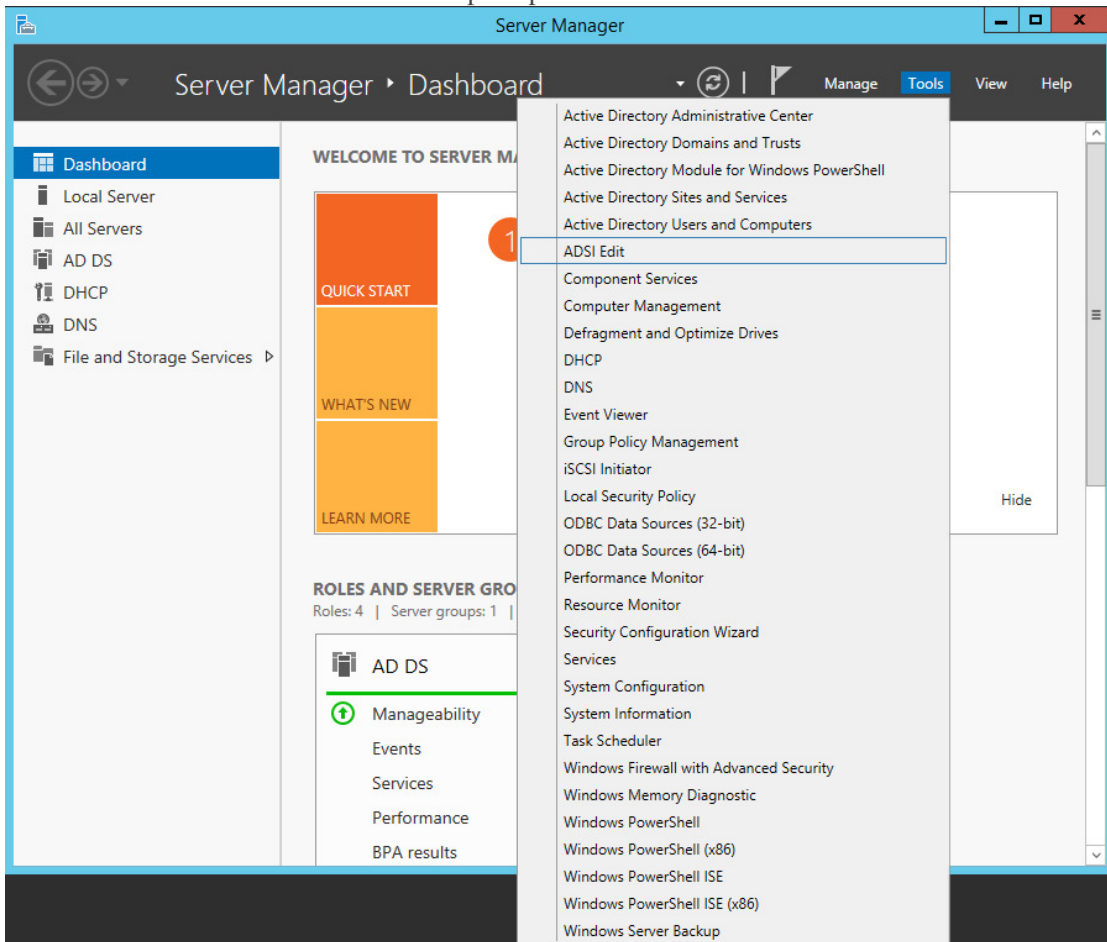
1. Logon to your primary DC
2. Stop the DFS Replication service

1. Click on the **Start menu**, select **Administrative Tools**, and then click **Services**

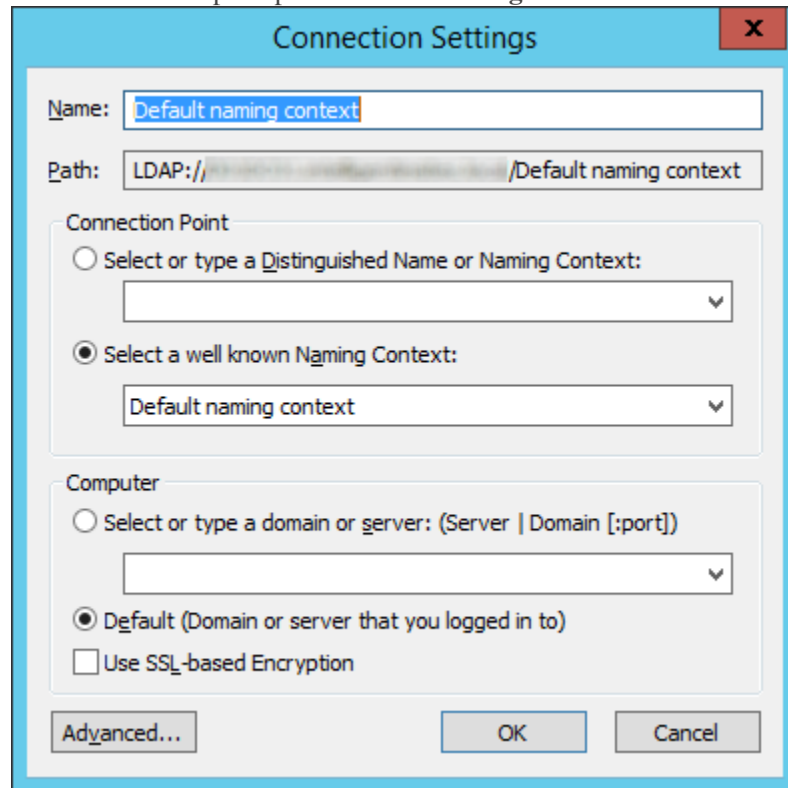


2. In the Name column, right-click **DFS Replication** or **Netlogon**, and then click **Stop**

3. Open up ADSI Edit

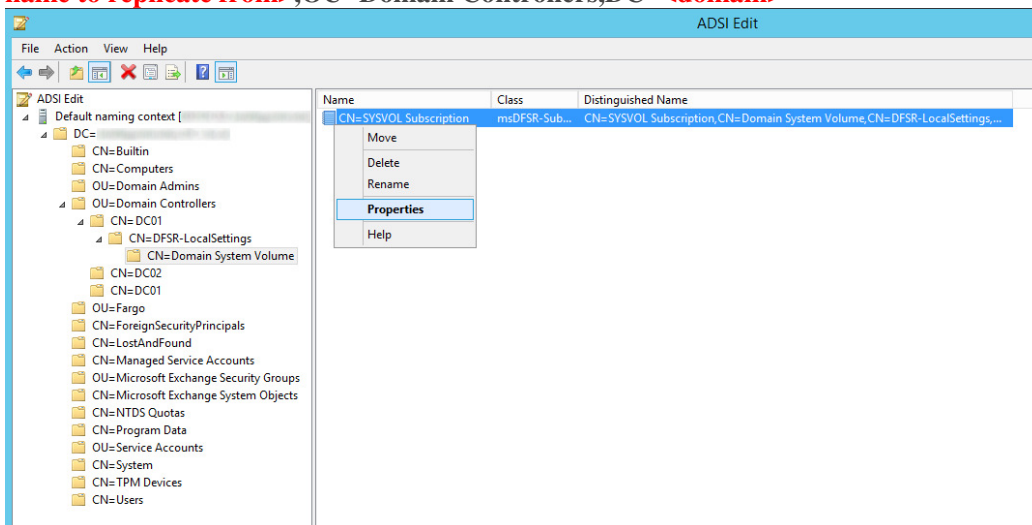


4. Open up the **Default naming context**



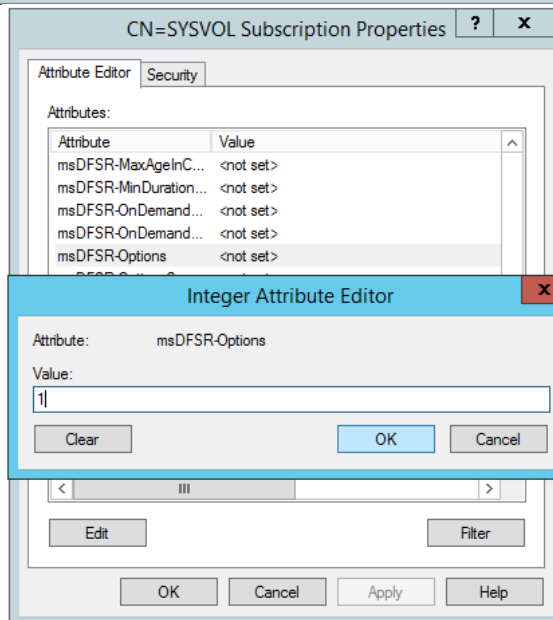
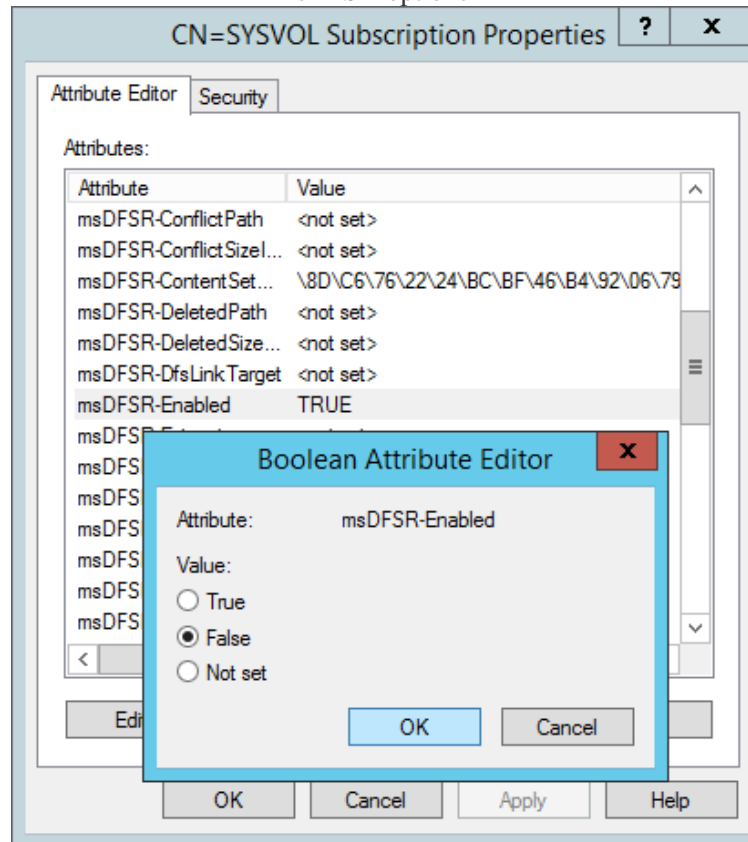
5. Navigate to the following

CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name to replicate from>,OU=Domain Controllers,DC=<domain>

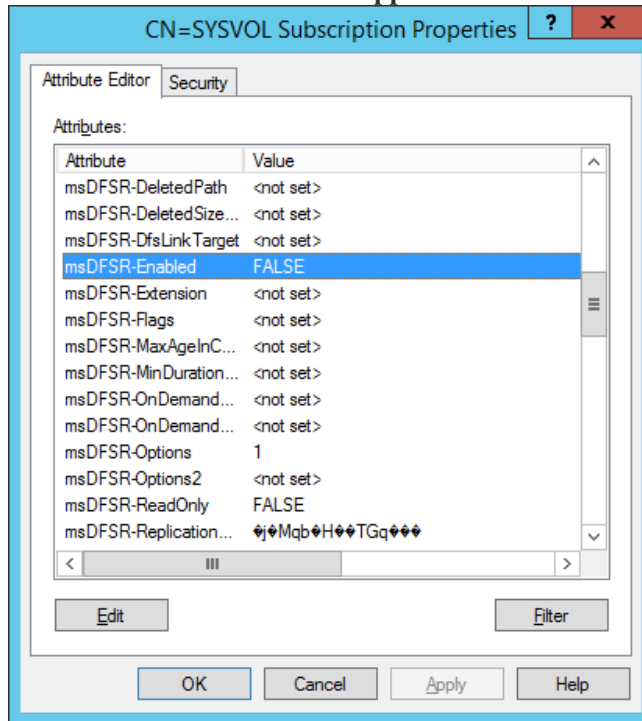


6. Change the following attributes to the following values

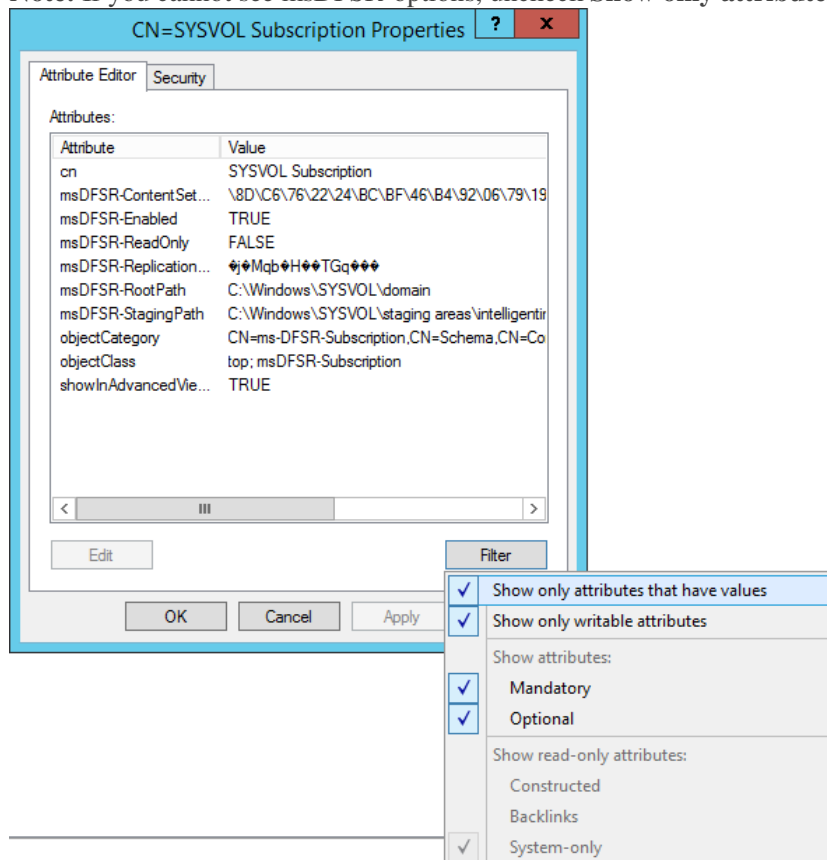
msDFSR-Enabled=FALSE
msDFSR-options=1



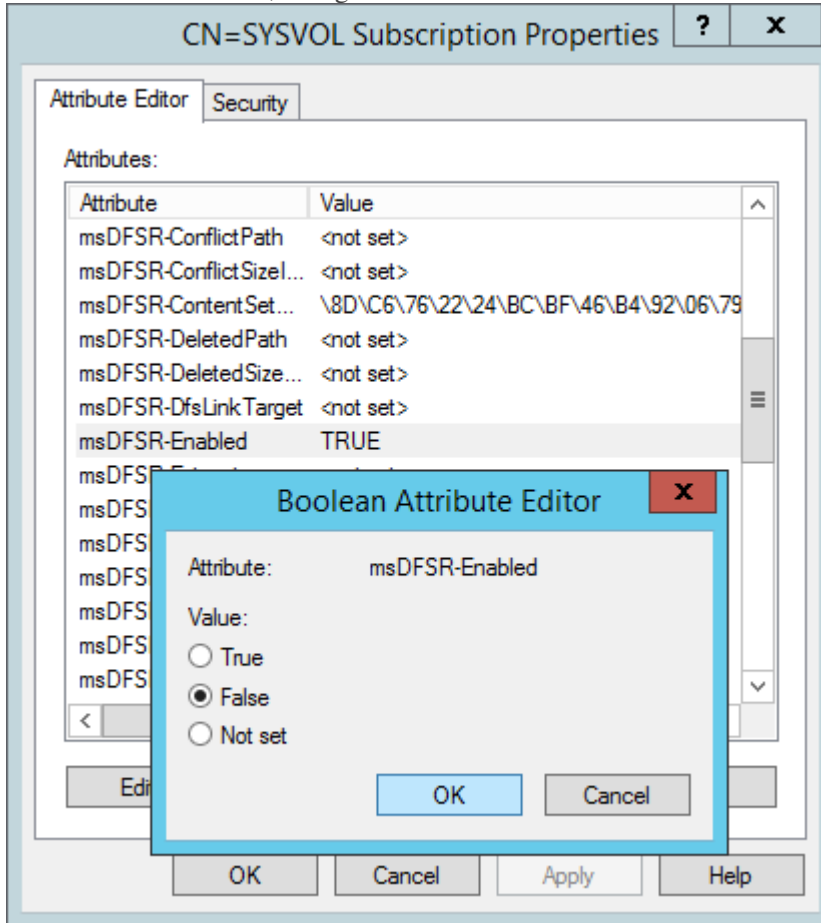
Both values applied



Note: If you cannot see msDFSR-options, uncheck **Show only attributes that have values**



7. On the ALL other DCs, change the **msDFSR-Enabled** attribute to **False**



8. Force Active Directory replication throughout the domain (ensure all sync responses terminate with no errors).

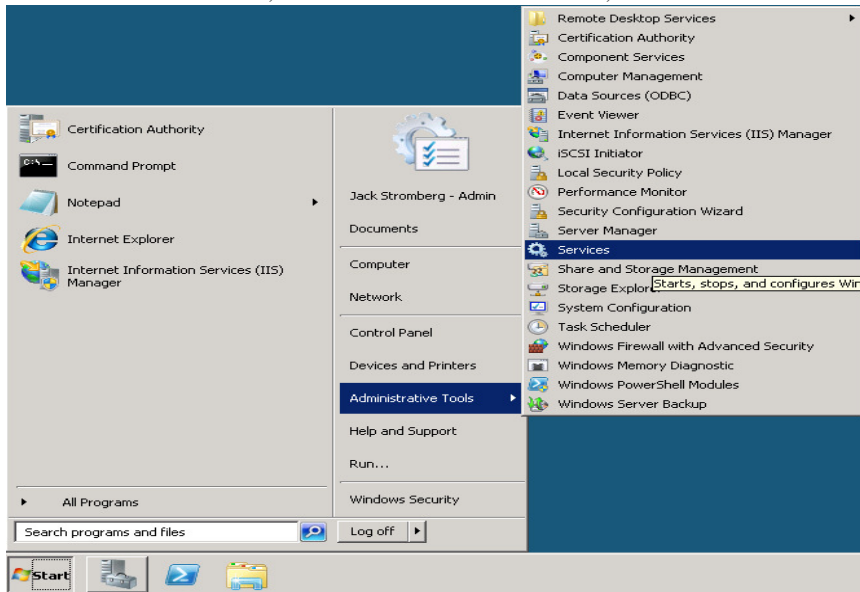
`repadmin /syncall primary_dc_name /Aped`

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> repadmin /syncall [redacted] /APed
Syncing all NC's held on [redacted]
[redacted]
[redacted]
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
[redacted]
[redacted]
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
[redacted]
[redacted]
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
[redacted]
[redacted]
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
[redacted]
[redacted]
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
PS C:\Windows\system32>
```

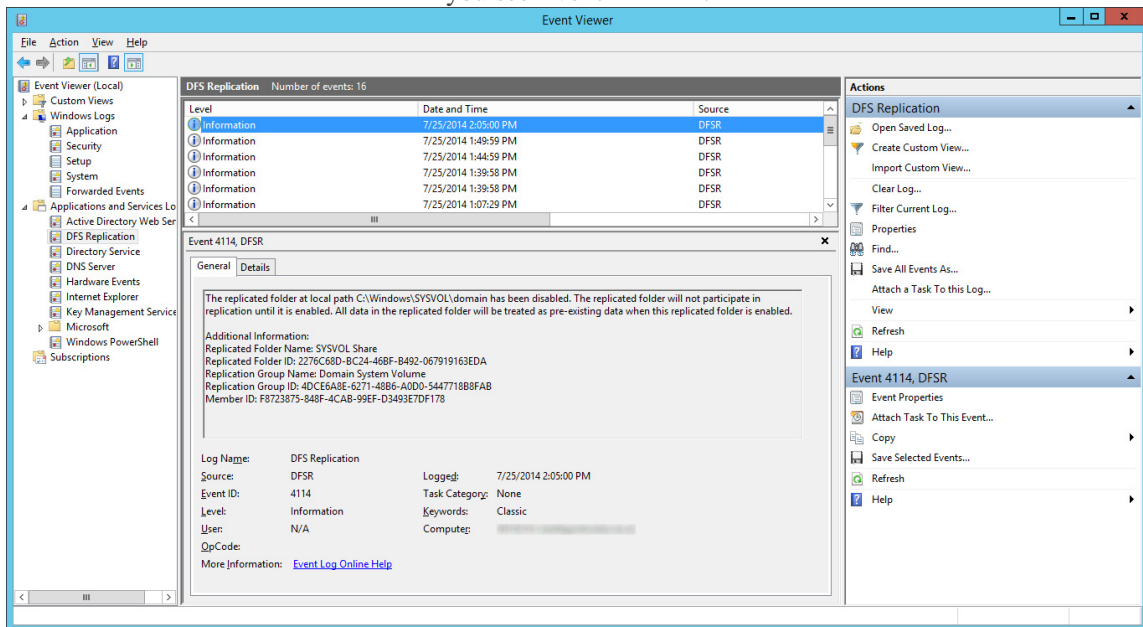
1. **NOTE:** Here is a list of what the switches mean
1. /A: Perform /SyncAll for all NC's held by <Dest DSA> (ignores <Naming Context>)
2. /P: Push changes outward from home server (default: pull changes)
3. /e: Enterprise, cross sites (default: only home site)
4. /d: ID servers by DN in messages (instead of GUID DNS)

- Click on the **Start** menu, select **Administrative Tools**, and then click **Services**



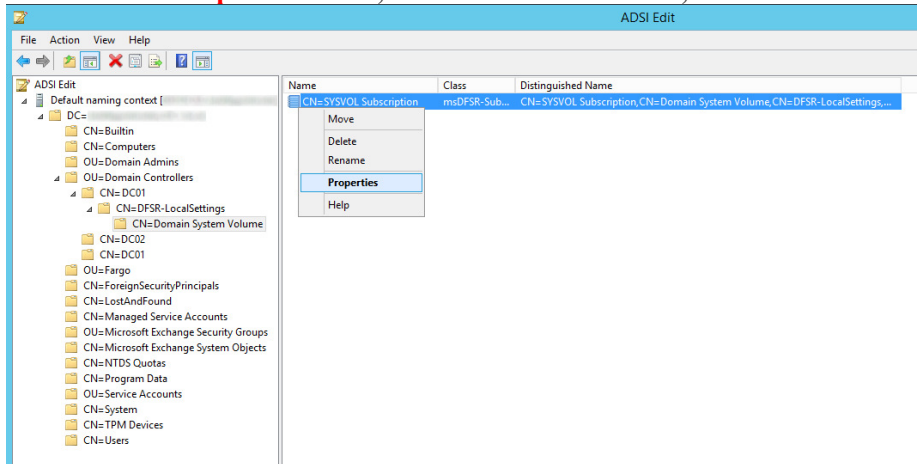
In the Name column, right-click **DFS Replication** or **Netlogon**, and then click **Start**

- Open up event viewer and navigate to **Applications and Services Logs -> DFS Replication**. Verify you see Event ID 4114.

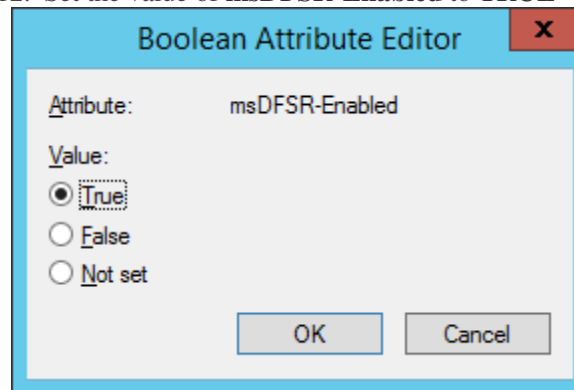


11. Navigate back to the following in ADSI

- i. **CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name to replicate from>,OU=Domain Controllers,DC=<domain>**



12. Set the value of **msDFSR-Enabled** to **TRUE**



13. Execute the following via an elevated command prompt
a. **DFSRDIAG POLLAD**

NOTE: This is a utility apart of DFS Management Tools. I completed the guide successfully without running this command, but Microsoft recommends you do run this command.

14. Force Replication in AD repadmin /syncall /APed

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> repadmin /syncall /APed
Syncing all NC's held on

CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

PS C:\Windows\system32>
```

15. Wait a few minutes and you should see Event ID 2002 and 4602

Level	Date and Time	Source	Event ID	Task Category
Information	7/25/2014 2:45:11 PM	DFSR	4602	None
Information	7/25/2014 2:45:11 PM	DFSR	2002	None
Information	7/25/2014 2:05:00 PM	DFSR	4114	None
Information	7/25/2014 1:48:59 PM	DFSR	4114	None
Information	7/25/2014 1:44:59 PM	DFSR	4114	None
Information	7/25/2014 1:39:58 PM	DFSR	2010	None
Information	7/25/2014 1:39:58 PM	DFSR	4114	None

Event 4602, DFSR

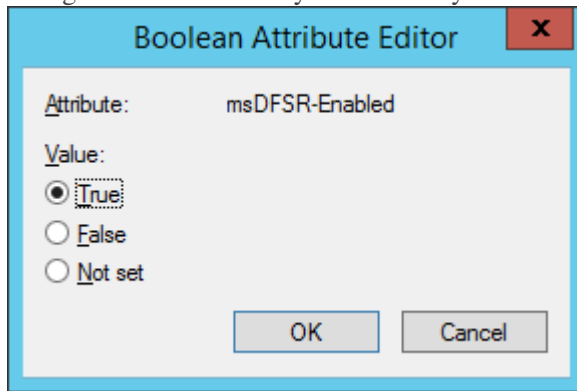
The DFS Replication service successfully initialized the SYSVOL replicated folder at local path C:\Windows\SYSVOL\domain. This member is the designated primary member for this replicated folder. No user action is required. To check for the presence of the SYSVOL share, open a command prompt window and then type "net share".

Additional Information:
Replicated Folder Name: SYSVOL Share
Replicated Folder ID: 2276C68D-B24-46BF-B492-067919163EDA
Replication Group Name: Domain System Volume
Replication Group ID: 4DCE6A8E-6271-4495-A000-54477188BFA8
Member ID: F8723875-848F-4CAB-99EF-D3493E7DF178
Read-Only: 0

Log Name: DFS Replication
Source: DFSR
Event ID: 4602
Level: Information
User: N/A
OpCode:

Logged: 7/25/2014 2:45:11 PM
Task Category: None
Keywords: Classic
Compute:

16. Navigate back to each of your secondary DCs and change the value of **msDFSR-Enabled** to **TRUE**

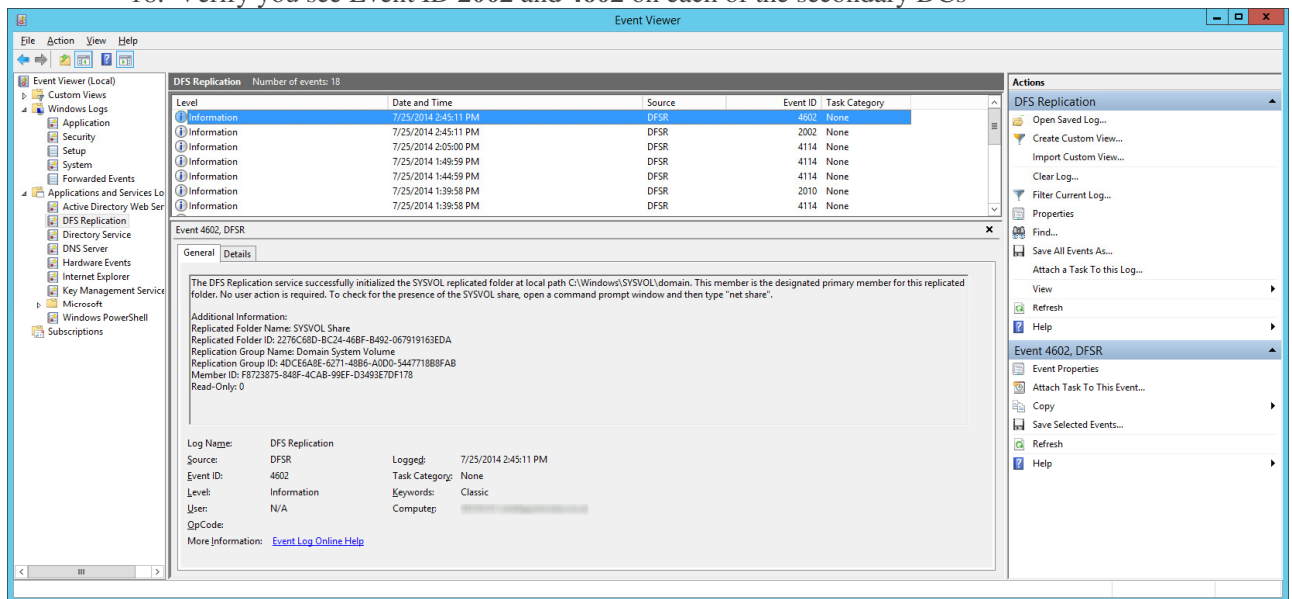


17. Execute the following via an elevated command prompt

a. **DFSRDIAG POLLAD**

i. **NOTE:** This is a utility apart of DFS Management Tools. I completed the guide successfully without running this command, but Microsoft recommends you do run this command. Force Active Directory replication throughout the domain

18. Verify you see Event ID **2002** and **4602** on each of the secondary DCs



At this point, try running a `gpupdate` on your client. If all has gone well, each of your shared SYSVOL folders on your DCs should contain the same amount of policies and your client should successfully pull down all policies.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\windows\system32>gpupdate
Updating policy...

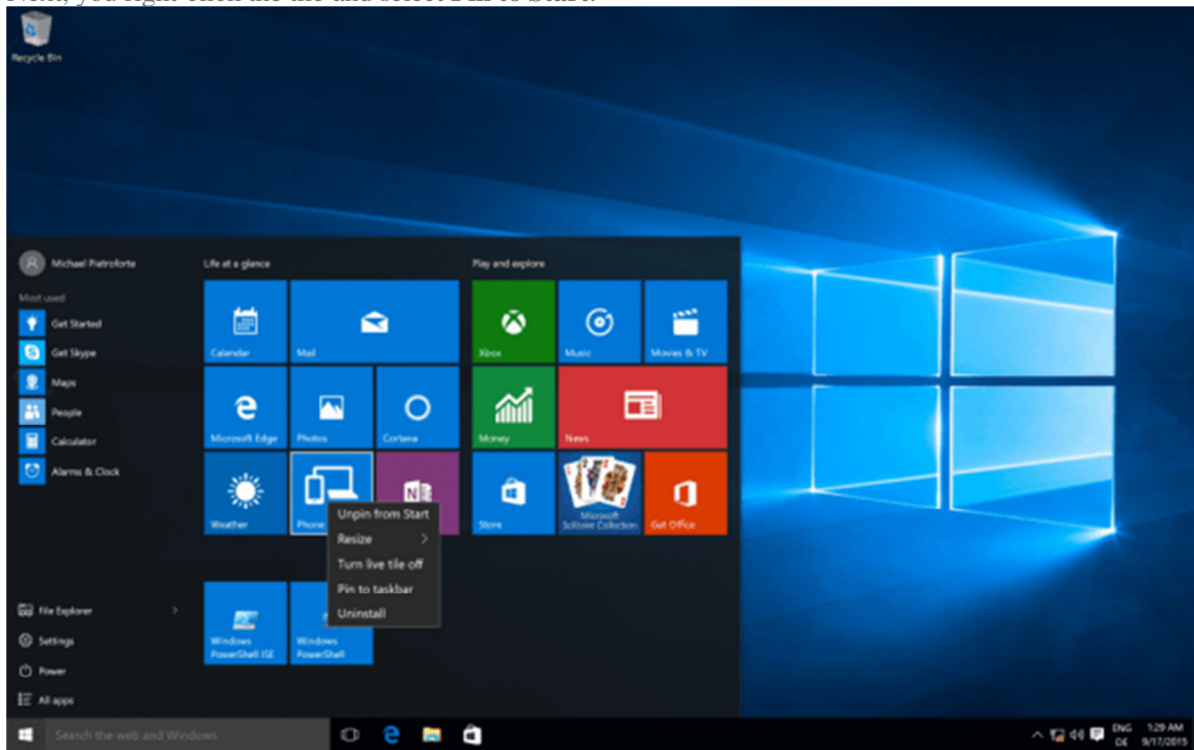
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\windows\system32>
```

WINDOWS 10 Group Policies

Creating your Start menu layout

The first thing you have to do is prepare a reference machine that has all the applications installed that you want to pin to the Start layout. To pin a new tile to the Start menu, you first have to find it through Start search. Next, you right-click the tile and select **Pin to Start**.



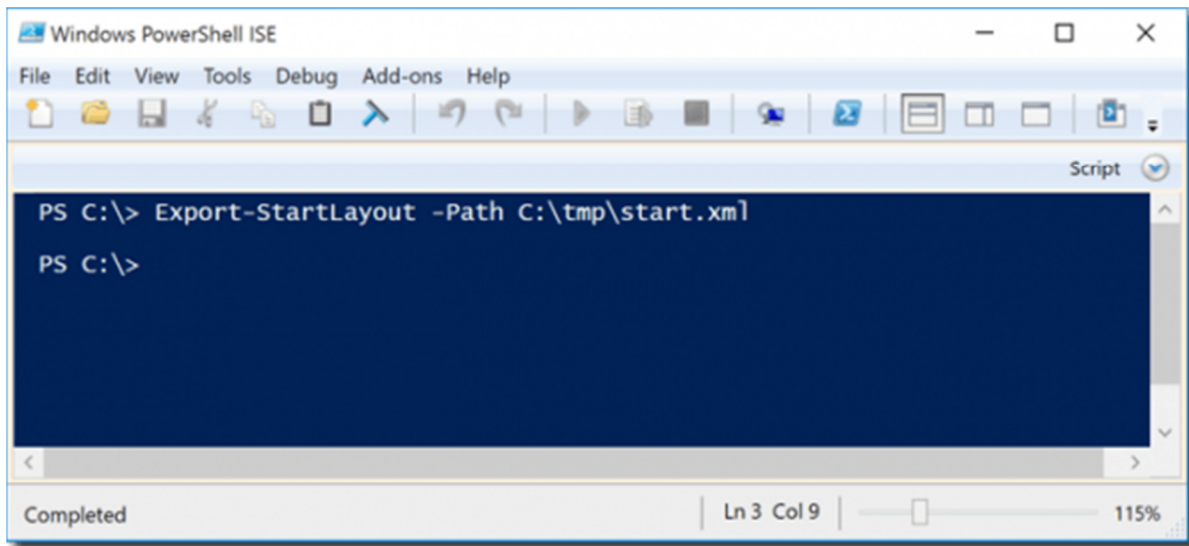
Configuring the Start layout in Windows 10

To remove a tile, right-click it and then click **Unpin from Start**. Of course, you can also arrange the tiles by just dragging them to their position.

After the Start menu has the configuration that you want to deploy, you have to run the following PowerShell command:



```
1 Export-StartLayout -Path C:\tmp\start.xml
```



Exporting the Start menu configuration with Export-StartLayout

This exports the current Start menu configuration to an XML file. Note that the *Export-StartLayout* cmdlet in Windows 10 differs from its [counterpart in Windows 8/8.1](#). The new cmdlet no longer offers the *-As* parameter that allowed you to choose between an XML and a binary format.

In theory, you can modify the XML file in a text editor because its structure is relatively simple. However, I think it is easier to use the Start menu of your reference machine to create the configuration that you want to deploy.

```

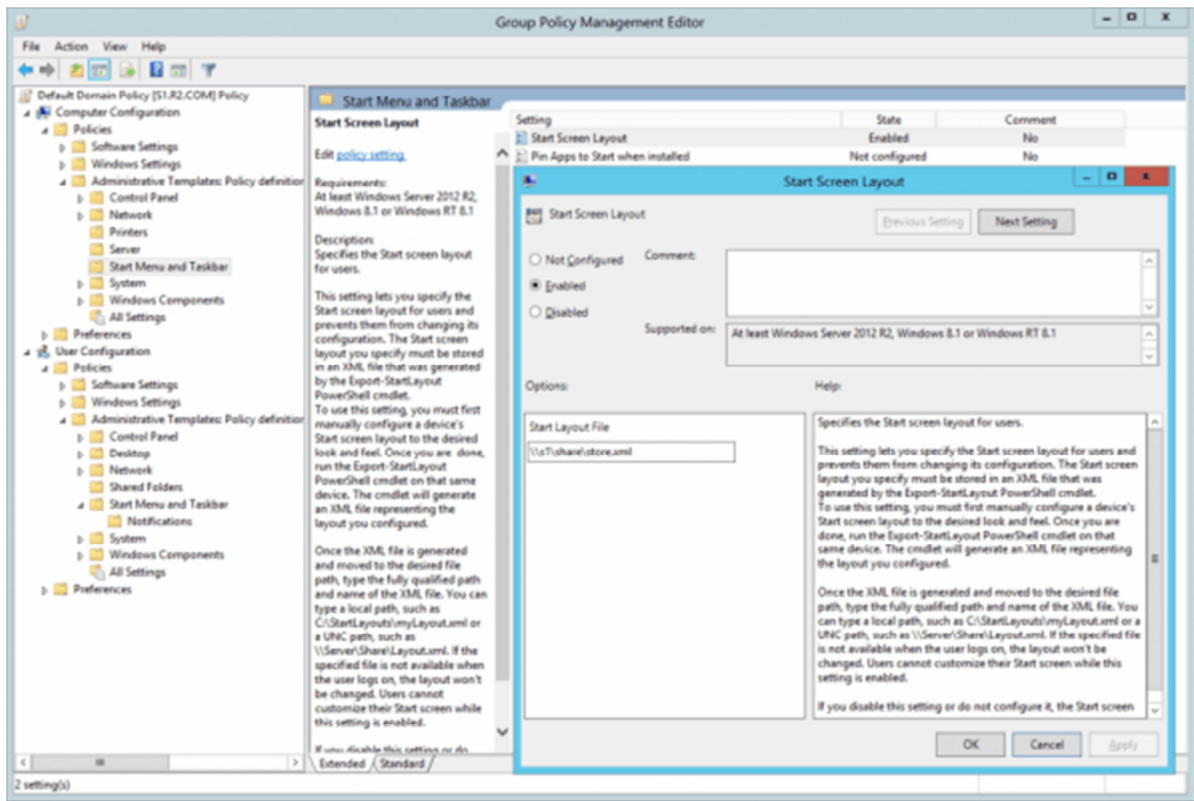
<?xml version="1.0"?>
<LayoutModificationTemplate xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification" Version="1">
  <DefaultLayoutOverride>
    <StartLayoutCollection>
      <defaultlayout:StartLayout xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" GroupCellWidth="6">
        <start:Group xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Name="Life at a glance">
          <start:Tile AppUserModelID="microsoft.windowscommunicationsapps_bwekyb3d8bbwe/microsoft.windowslive.calendar" Row="0" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="microsoft.windowscommunicationsapps_bwekyb3d8bbwe/microsoft.windowslive.mail" Row="0" Column="2" Size="4x2"/>
          <start:Tile AppUserModelID="Microsoft.MicrosoftEdge_bwekyb3d8bbwe/MicrosoftEdge" Row="2" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.Windows.Photos_bwekyb3d8bbwe/App" Row="2" Column="2" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.Windows.Cortana_cw5n3h2tzyewyl/CortanaUI" Row="2" Column="4" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.BingWeather_bwekyb3d8bbwe/App" Row="4" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.WindowsPhone_bwekyb3d8bbwe/CompanionApp.App" Row="4" Column="2" Size="2x2"/>
        </start:Group>
        <start:Group xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Name="Play and explore">
          <start:Tile AppUserModelID="Microsoft.XboxApp_bwekyb3d8bbwe/Microsoft.XboxApp" Row="0" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.ZuneMusic_bwekyb3d8bbwe/Microsoft.ZuneMusic" Row="0" Column="2" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.ZuneVideo_bwekyb3d8bbwe/Microsoft.ZuneVideo" Row="0" Column="4" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.BingFinance_bwekyb3d8bbwe/AppexFinance" Row="2" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.BingNews_bwekyb3d8bbwe/AppexNews" Row="2" Column="2" Size="4x2"/>
          <start:Tile AppUserModelID="Microsoft.WindowsStore_bwekyb3d8bbwe/App" Row="6" Column="0" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.MicrosoftSolitaireCollection_bwekyb3d8bbwe/App" Row="6" Column="2" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.MicrosoftOfficeHub_bwekyb3d8bbwe/Microsoft.MicrosoftOfficeHub" Row="6" Column="4" Size="2x2"/>
          <start:Tile AppUserModelID="Microsoft.Office.OneNote_bwekyb3d8bbwe/microsoft.onenoteim" Row="4" Column="3" Size="2x2"/>
        </start:Group>
        <start:Group xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Name="">
          <start:DesktopApplicationTile Row="0" Column="0" Size="2x2" DesktopApplicationID="{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\PowerShell_ISE.exe"/>
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>

```

Start menu configuration stored in an XML file

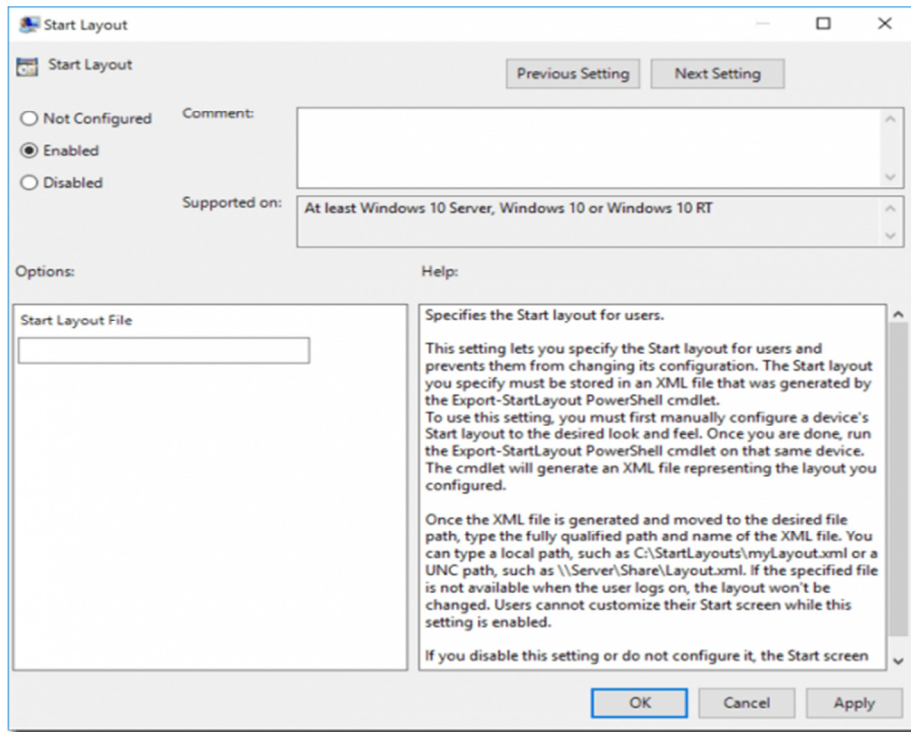
Deploying the Start menu layout via Group Policy [^]

Next, you can deploy the settings via Group Policy by specifying the XML file. The policy can be found at **User Configuration > Administrative Templates > Start Menu and Taskbar > Start Screen Layout**. The same policy is also available under **Computer Configuration**.



Start Screen Layout Group Policy

Note that the corresponding policy in Windows 10 is no longer called “Start Screen Layout” but just “Start Layout.” It will be interesting to see how the policy will be named in Windows Server 2016.



Start Layout Group Policy in Windows 10

A downside of this method might be that the Start menu will be locked. That is user can no longer pin or unpin tiles. However, perhaps this is just what you want.

Changes to Group Policy settings for Windows 10 Start

Start policy settings supported for Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Education

These policy settings are available in **Administrative Templates\Start Menu and Taskbar** under **User Configuration**.

Policy	Notes
--------	-------

Clear history of recently opened documents on exit	Documents that the user opens are tracked during the session. When the user signs off, the history of opened documents is deleted.
Do not allow pinning items in Jump Lists	Jump Lists are lists of recently opened items, such as files, folders, or websites, organized by the program that you use to open them. This policy prevents users from pinning items to any Jump List.
Do not display or track items in Jump Lists from remote locations	When this policy is applied, only items local on the computer are shown in Jump Lists.
Do not keep history of recently opened documents	Documents that the user opens are not tracked during the session.
Prevent changes to Taskbar and Start Menu Settings	In Windows 10, this disables all of the settings in Settings > Personalization > Start as well as the options in dialog available via right-click Taskbar > Properties
Prevent users from customizing their Start Screen	Use this policy in conjunction with CopyProfile or other methods for configuring the layout of Start to prevent users from changing it
Prevent users from uninstalling applications from Start	In Windows 10, this removes the uninstall button in the context menu. It does not prevent users from uninstalling the app through other entry points (e.g. PowerShell)
Remove All Programs list from the Start menu	In Windows 10, this removes the All apps button.

Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	This removes the Shut Down, Restart, Sleep, and Hibernate commands from the Start Menu, Start Menu power button, CTRL+ALT+DEL screen, and Alt+F4 Shut Down Windows menu.
Remove common program groups from Start Menu	As in earlier versions of Windows, this removes apps specified in the All Users profile from Start
Remove frequent programs list from the Start Menu	In Windows 10, this removes the top left Most used group of apps.
Remove Logoff on the Start Menu	Logoff has been changed to Sign Out in the user interface, however the functionality is the same.
Remove pinned programs list from the Start Menu	In Windows 10, this removes the bottom left group of apps (by default, only File Explorer and Settings are pinned).
Show "Run as different user" command on Start	This enables the Run as different user option in the right-click menu for apps.
Start Layout	This applies a specific Start layout, and it also prevents users from changing the layout. This policy can be configured in User Configuration or Computer Configuration . Note Start Layout policy setting applies only to Windows 10 Enterprise and Windows 10 Education.
Force Start to be either full screen size or menu size	This applies a specific size for Start.

Deprecated Group Policy settings for Start

The Start policy settings listed below do not work on Windows 10. Most of them were deprecated in Windows 8 however a few more were deprecated in Windows 10. Deprecation in this case means that the policy setting will not work on Windows 10. The "Supported on" text for a policy setting will not list Windows 10. The policy settings are still in the Group Policy Management Console and can be used on the operating systems that they apply to.

Policy	When deprecated
Go to the desktop instead of Start when signing in	Windows 10
List desktop apps first in the Apps view	Windows 10
Pin Apps to Start when installed (User or Computer)	Windows 10
Remove Default Programs link from the Start menu.	Windows 10
Remove Documents icon from Start Menu	Windows 10
Remove programs on Settings menu	Windows 10
Remove Run menu from Start Menu	Windows 10
Remove the "Undock PC" button from the Start Menu	Windows 10
Search just apps from the Apps view	Windows 10

Show Start on the display the user is using when they press the Windows logo key	Windows 10
Show the Apps view automatically when the user goes to Start	Windows 10
Add the Run command to the Start Menu	Windows 8
Change Start Menu power button	Windows 8
Gray unavailable Windows Installer programs Start Menu shortcuts	Windows 8
Remove Downloads link from Start Menu	Windows 8
Remove Favorites menu from Start Menu	Windows 8
Remove Games link from Start Menu	Windows 8
Remove Help menu from Start Menu	Windows 8
Remove Homegroup link from Start Menu	Windows 8

Remove Music icon from Start Menu	Windows 8
Remove Network icon from Start Menu	Windows 8
Remove Pictures icon from Start Menu	Windows 8
Remove Recent Items menu from Start Menu	Windows 8
Remove Recorded TV link from Start Menu	Windows 8
Remove user folder link from Start Menu	Windows 8
Remove Videos link from Start Menu	Windows 8

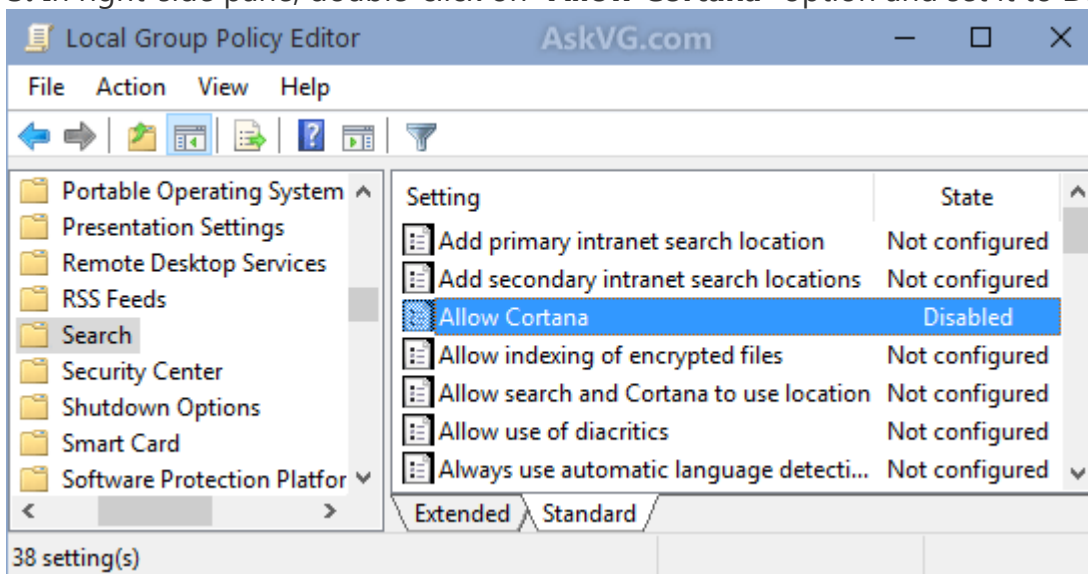
Disable One Drive

Computer Configuration -> Administrative Templates -> Windows Components -> OneDrive.

Disable Cortana

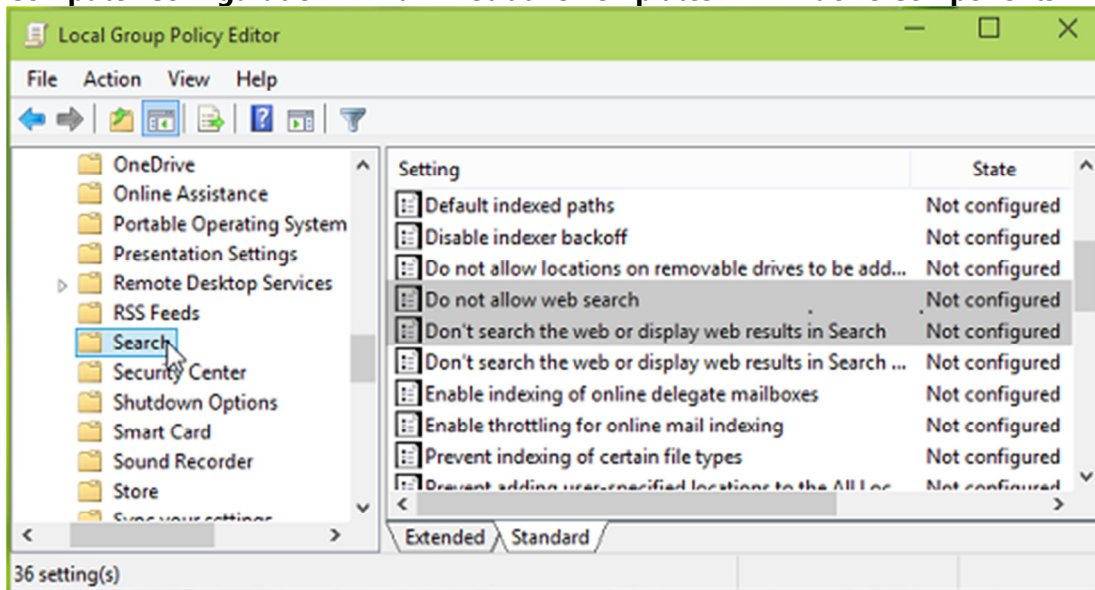
Computer Configuration -> Administrative Templates -> Windows Components -> Search

3. In right-side pane, double-click on "**Allow Cortana**" option and set it to **Disabled**.

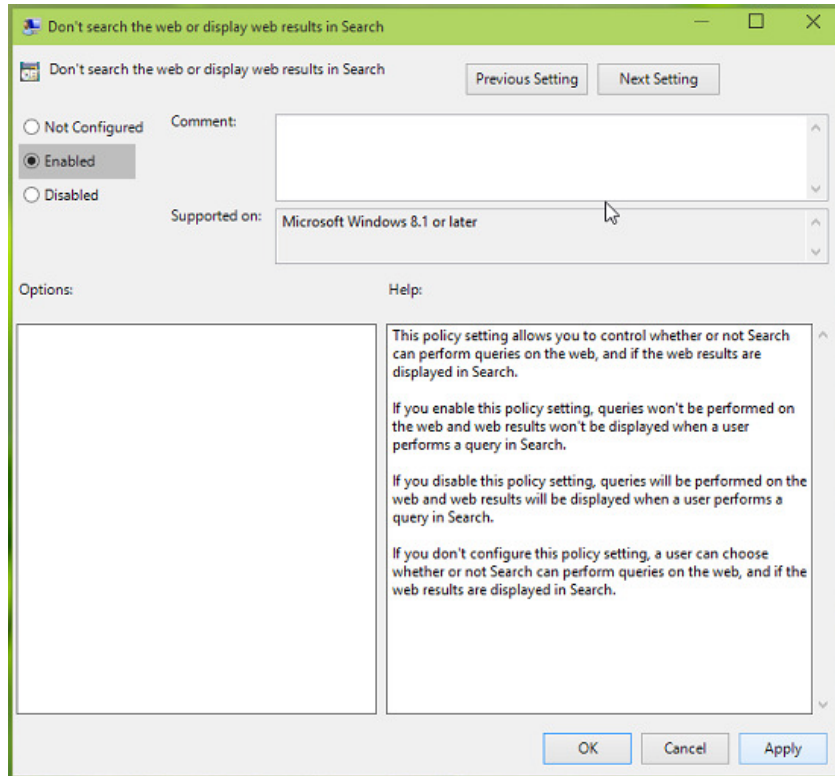


Disable Web Search in Windows 10

Computer Configuration -> Administrative Templates -> Windows Components -> Search



Moving on, in the right of above shown window and scroll down to look for *Settings* named **Do not allow web search** and **Don't search the web or display web results in Search**. Both of these are *Not Configured* by default. Double click on any one of them:



Finally in the above shown window, select **Enabled** and click **Apply** followed by **OK**. Enable the other *Setting* in similar way.