

TM

GROUP POLICY SERVER 2012

Prepared By DIS APSCN/LAN Support

### **Table of Contents**

Tips for Group Policy
Major Categories of Group Policy
Group Policy for Server 2008
Enforcing K12 State Security Policies for ACT723 through Group Policies
Setting Non-Student (Faculty) Password Requirements
Setting Student Password Requirements using Fine-grained password policies4
Retain Security Event Log for 90 Days6
Security Event Auditing – Security Event Log Contents
Logon Banner
Locking Screen Saver
Create the WSUS Group Policy7
Common K12 Group Policies
Redirect 'My Documents' to User's Home-Directory
Restrict Computers to Faculty Use Only
Disable Internet Access by Group Policy/Security Group
Group Policy for Server 201213
Enforcing K12 State Security Policies for ACT723 through Group Policies
Setting Non-Student (Faculty) Password Requirements
Setting Student Password Requirements using Fine-grained password policies13
Retain Security Event Log for 90 Days17
Security Event Auditing – Security Event Log Contents18
Logon Banner18
Locking Screen Saver18
Create the WSUS Group Policy18
Common K12 Group Policies
Redirect 'My Documents' to User's Home-Directory19
Restrict Computers to Faculty Use Only20
Disable Internet Access by Group Policy/Security Group21
Windows 10 group policy and Central Store28-53

### **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 >	Windows 2000+
	Administrative Templates	
Security Settings	User or Computer > Policies >	Windows 2000+
	Windows Settings > Security	
	Settings	
Wired Network	Computer > Policies > Windows	Windows Vista+
	Settings > Security Settings >	
	Wired Network	
Wireless Network	Computer > Policies > Windows	Windows XP and Vista+
	Settings > Security Settings >	
	Wireless Network	
Scripts	Computer > Policies > Windows	
	Settings > Scripts	
	(Startup/Shutdown) > Windows	

	Settings > Script (Logon/Logoff)	
Group Policy Software	Computer or User > Policies >	Windows 2000+
Installation	Software Settings	
Folder Redirection	User > Policies > Windows	Windows 2000+
	Settings > Folder Redirection	
Disk Quotas	Computer > Policies>	Windows 2000+
	Administrative Templates >	
	System > Disk Quotas	
Encrypted Data Recovery Agents	Computer > Policies > Windows	Windows 2000+
	Settings > Security Settings >	
	Public Key > Policies >	
	Encrypting File System	
Internet Explorer Maintenance	User > Policies > Windows	Windows 2000+
	Settings > Internet Explorer	
	Maintenance	
Software Restriction Policies	Computer > Policies > Windows	Windows XP+
	Settings > Security Settings >	
	Software Restriction Policies	
Windows Search	Computer > Policies >	Windows Vista+
	Administrative Templates >	
	Windows Components > Search	
Group Policy Preference	Computer > Preferences (Only	Windows Server 2008, Windows
Extensions	domain policies)	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
B 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 defualt 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	20		
	Precedence			
msDS-PasswordReversible	Password reversible	FALSE		
	encryption			
msDS-PasswordHistory	Number of passwords	6		
	"remembered".			
msDS-PasswordComplexityEnabled	Force Complex	TRUE		
	Passwords			
msDS-MinimumPasswordLength	Minimum characters	8		
msDS-MinimumPasswordAge	Days before password	1:00:00:00		
	can be changed			
msDS-MaximumPasswordAge	Force password	180:00:00:00		
	change every 180			
	days.			
msDS-LockoutThreshold	Invalid logon attempts	3		
	before locking user			
	account.	0.00.10.00		
msDS-LockoutObservationWindow	Length of time before	0:00:10:00		
	Invalid password			
	reset 10 Minutes			
mcDS LockoutDuration	Time user account will	0.00.15.00		
IIISD3-LOCKOULDUI ALIOIT	he locked for once the	0.00.15.00		
	account login attempt			
	threshold has been			
	met 15 Minutes			
	med 15 mildes			
Click Finish				
Edit Policy again				
msDS-PSOAppliesTo	This is the	See next line for		
	distinquished name of	example. THIS IS CASE		
	the Global Security	SENSITIVE TO YOUR		
	Group that your	ENVIRONMENT		
	students are a			
	member of			
Then add <b>Group</b>				
CN-Studente OL-Studente DC-school DC-local				
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 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 <u>http://yourservername</u> 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**.

Documents Properties	<u>?</u> ×
Target Settings	
Select the redirection settings for Documents.	
Grant the user exclusive rights to Documents.	
Move the contents of Documents to the new location.	
Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.	
Policy Removal	
<ul> <li>Redirect the folder back to the local userprofile location when policy is removed.</li> </ul>	
OK Cancel Ap	oly

- 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)
- 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 loose 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.

🐗 Active Directory Users and Compu	ıters			1
🎻 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> e	lp			
	😫   🦉 🖉 🐚 🤊	7 🍕 🗽		- Ý
Active Directory Users and Computer	Students 9 objects			
🗄 📃 Saved Queries	Name	Туре	Description	1
🖻 🎒 APSCN.local	2007	Organizational		
⊞… <u>III</u> Builtin	2008	Organizational		- 1
⊡ Computers	2009 🔯	Organizational		- 5
	2010	Organizational		- 7
ForeignSecurityPrincipals	2011	Organizational		- 7
+ 1 Locked Down Workstations	2012	Organizational		- 5
	No Internet Access	Security Group		- 5
⊡	🕵 Students 💦 🔪	Security Group		- 5
⊡ 🕢 2008	🥵 Yearbook Staff	Security Group		- 5
⊡-@ 2009				- 1
⊡ 🔯 2010				- 5
⊡ 🙆 2011				- 5
				- 4
⊡ Users				$\sim$
and a second sec	Land and a start and a start of the start of		and the second	1

- 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.

ETUXY SELLIDOS 1		
Troxy bottings		
You can specify what pro separate entries.	oxy servers, if any, you want your users to connect to. Use se	emicolons ( ; ) to
Enable proxy setting:	s	
Proxy Servers		
Address c	of proxy Port Do not use pro	xy server for
1 HTTP: 192168	0.1 8080 addresses beg	inning with:
<u>_</u> ,,		IS;
2, Secure;	80 www.edline.ne	et;
3. FTP:	: 80 Www.arkedu.s	state.ar.us
4. Gopher:	: 80	-
5, Socks:	· · · · · · · · · · · · · · · · · · ·	
Lice the come ever	Do not use	e proxy server for
I <u>U</u> se the same pro:	xy server for all addresses local (intra	nec) addresses.
		. N
Click the <b>OK</b> buttor Under User Configu	n once you have entered in your settings. Iration, expand <b>Administrative Template</b> s	<b>.</b>
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane.	n once you have entered in your settings. Iration, expand <b>Administrative Templates</b> <b>Components</b> , Internet <b>Explorer</b> . <b>Disable Changing Proxy Settings</b> option	<b>s</b> . n in the right-hand
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane.	n once you have entered in your settings. Iration, expand Administrative Templates Components, Internet Explorer. Disable Changing Proxy Settings option	<b>s</b> . n in the right-hand
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration	n once you have entered in your settings. Iration, expand Administrative Templates Components, Internet Explorer. Disable Changing Proxy Settings option Setting Setting Setting Setting	s. n in the right-hand
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.APSC omputer Configuration Software Settings	<ul> <li>once you have entered in your settings.</li> <li>uration, expand Administrative Templates</li> <li>Components, Internet Explorer.</li> <li>Disable Changing Proxy Settings option</li> <li>Setting</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> </ul>	s. n in the right-hand
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C omputer Configuration Software Settings Windows Settings Administrative Templater	once you have entered in your settings. Ination, expand Administrative Templates     Components, Internet Explorer.     Disable Changing Proxy Settings option     Setting     Search: Disable Search Customization     Search: Disable Find Files via F3 within the browser     Disable external branding of Internet Explorer	s. n in the right-hand
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.APSC omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration	Setting Setting Setting Setting Setting Setting Setting Setting Search: Disable Find Files via F3 within the browser Disable external branding of Internet Explorer Disable external branding of Internet Explorer Disable importing and exporting of favorites	s. n in the right-hand <u>State</u> Not configured Not configured Not configured Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings	<ul> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable changing of Internet Explorer</li> <li>Disable importing and exporting of favorites</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> </ul>	s. n in the right-hand State Not configured Not configured Not configured Not configured Not configured Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Windows Settings	<ul> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable importing and exporting of favorites</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> </ul>	s. n in the right-hand State Not configured Not configured Not configured Not configured Not configured Not configured Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Windows Settings Software Settings Windows Settings Windows Settings	Setting Setting Setting Setting Setting Setting Setting Search: Disable Search Customization Search: Disable Find Files via F3 within the browser Disable external branding of Internet Explorer Disable importing and exporting of favorites Disable changing Advanced page settings Disable changing home page settings Disable changing home page settings Disable changing home page settings Disable changing of Auto-Proxy scripts	s. n in the right-hand State Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Windows Settings Software Settings Windows Settings Windows Settings Ministrative Templates Ministrative Templates	<ul> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings option</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> <li>Use Automatic Detection for dial-up connections</li> <li>Disable caching of Auto-Proxy scripts</li> <li>Display error message on proxy script download failure</li> </ul>	s. n in the right-hand State Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Windows Settings Windows Settings Windows Settings Internet Explorer	<ul> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> <li>Use Automatic Detection for dial-up connections</li> <li>Disable caching of Auto-Proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> </ul>	s. n in the right-hand State Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.AP5C] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Windows Settings Administrative Templates Windows Settings Mindows Settings Mindows Settings Internet Explorer Internet Explorer	<ul> <li>Setting</li> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> <li>Disable changing of Auto-Proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing history settings</li> </ul>	s. n in the right-hand State Not configured
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.APSC] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Windows Settings Administrative Templates Mindows Settings Administrative Templates Mindows Components Mindows Components Internet Explorer	<ul> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings</li> <li>Disable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing home page settings</li> <li>Disable changing of Auto-Proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing networks settings</li> <li>Disable changing color settings</li> <li>Disable changing color settings</li> </ul>	S. n in the right-hand State Not configured Not con
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. ternet Access [apscn-dc-1.APSC] omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Windows Settings Administrative Templates Windows Settings Administrative Templates Windows Components Windows Components Internet Explorer	<ul> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings</li> <li>Disable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing for proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing link color settings</li> <li>Disable changing link color settings</li> <li>Disable changing files via settings</li> <li>Disable changing for settings</li> <li>Disable changing files via settings</li> <li>Disable changing files via settings</li> <li>Disable changing for settings</li> <li>Disable changing files via settings</li> </ul>	S. n in the right-hand State Not configured Not con
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> Double-click on the window pane. ternet Access [apscn-dc-1.APSC omputer Configuration Software Settings Windows Settings Administrative Templates ser Configuration Software Settings Administrative Templates Mindows Settings Administrative Templates Mindows Settings Administrative Templates Mindows Components Mindows Components Mindow	<ul> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings</li> <li>Disable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable importing and exporting of favorites</li> <li>Disable changing Advanced page settings</li> <li>Disable changing for proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing for settings</li> <li>Disable changing language settions</li> </ul>	S. n in the right-hand State Not configured Not con
Click the <b>OK</b> buttor Under User Configu Expand <b>Windows</b> . Double-click on the window pane. cernet Access [apscn-dc-1.APSC] omputer Configuration Software Settings Administrative Templates ser Configuration Software Settings Administrative Templates Software Settings Windows Settings Administrative Templates Windows Components Windows Components NetMeeting Diffine Pages Browser menus Coffline Pages Browser menus Persistence Behav	<ul> <li>Setting</li> <li>Setting</li> <li>Search: Disable Changing Proxy Settings</li> <li>Obiable Changing Proxy Settings option</li> <li>Search: Disable Search Customization</li> <li>Search: Disable Find Files via F3 within the browser</li> <li>Disable external branding of Internet Explorer</li> <li>Disable changing Advanced page settings</li> <li>Disable changing for Auto-Proxy scripts</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing Temporary Internet files settings</li> <li>Disable changing for settings</li> <li>Disable changing neutrons</li> <li>Disable changing neutrons</li> <li>Disable changing and settings</li> <li>Disable changing neutrons</li> <li>Disable changing neutrons</li> <li>Disable changing neutrons</li> <li>Disable changing and settings</li> <li>Disable changing neutrons</li> <li>Disable changing language settings</li> <li>Disable changing neutrons<!--</td--><td>S. n in the right-hand State Not configured Not con</td></li></ul>	S. n in the right-hand State Not configured Not con

😤 Disable Internet Connection wizard

😤 Disable changing connection settings

Disable changing proxy settings

13. Click the Close button to close the *Domain*.Local Properties Window.

Disable changing Automatic Configuration settings

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

۲

11. Select the **Enabled** option and then click the **OK** button.

Not configured

Not configured

Not configured hor?^\ved

Not configured

🗄 📄 Security Features

🚞 Application Compatibili

12. Close the Group Policy Editor.

Remove the user to give access back to the Internet.

🚞 Attachment Manager

Windows Explorer
 Microsoft Management

💎 🔍 Tack

### **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
Reserved 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.

2	Server Manager	- 0 X
€ → Server Ma	anager • Dashboard	• 🛞   🎽 Manage 👖 View Help
III Dashboard	WELCOME TO SERVER MANAGER	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell
Local Server 副 All Servers 略 AD CS	1 Configure this local server	Active Directory Sites and Services Active Directory Users and Computers ADSI Edit
單 AD DS 種 DHCP	2 Add roles and features	Certification Authority Component Services Computer Management
DNS     File and Storage Services	3 Add other servers to manage	Defragment and Optimize Drives DHCP
II Hyper-V Io IS	4 Create a server group	DNS Event Viewer

### 3. Click on **Tree View.**



4. Navigate to System container then Password Settings Container.

6	Active Directory Administrative Center	- 0 X
🕞 🖿 Active D	irectory Domain Services + contoso (local) + System +	S Manage Help
Active Directory <	System (25)	Tasks
CVERVE Cretcions  CVERVEW  CVERVEW  Control (ocal)  Dubin  Domain Controllers  Dom	System (23)         Filter       Image: Construct of the system of the syste	IdSKS     Passeord Settings Container     New     Delete     Search under this node     Properties     System     New     Delete     Search under this node     Properties
	Summary	
		<ul> <li>Nº Via Vo science</li> </ul>

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

6		Active Directory Administrative Center	
🗲 🖻 🗝 🐨 cor	ntoso (local) • S	System • Password Settings Container	
Active Directory	Password Set	tings Container (0)	
Program Uata	Filter	• (ii) • (ii)	۲
System AdminSDHolder ComPartitions ComPartitionSets ComPartitionGets Default Domain Policy Difu-Configuration Difu-Conf	* Name	Precedence Type Description	
Policies Policies PSPs RAS and IAS Servers Acce RpcServices WinpockServices	New Delete Search under this node Properties Add as navigation node	Password Settings	~
< III :	>		

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

				Х	
Create P	assword Settings: Poli-Group1	•	SECTIONS	•	
Bassword Settings	Password Settings			•	^
<u>D</u> irectly Applies To	Name:       *       Poli-Group1         Precedence:       *       1         Inforce minimum password lage options:       Inforce minimum password lage         User cannot change the password lage       User cannot change the password lage         Inforce password length       *       2         Inforce password length       *       2         Inforce password length (chancten):       *       2         Inforce password length (chancten):       *       2         Inforce password length (chancten):       *       2         Inforce minimum password lage       User must change the password lage       User must change the password lage         Inforce password must meet complexity requirements       *       34       Inforce of label logon attempts allowed:         Inforce a duration of (mink)       Cocount will be locked out       0	* 1	80 Add_ Remove		< N
<ul> <li>More Information</li> </ul>		OK	Car	ncel	

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

assword Settings	Password Settings	86
jrectly Applies To	Name:     * [Pol-Group1       Precedence:     1       Inforce minimum password length Minimum password length (duracters):     * 2       Inforce password histoy Number of passwords remembered:     * 24       Password must meet complexity requirements     * 24       Store password using reversible encryption     *       Protect from accidental deletion     Description:       Directly Applies To     Mal	Pessword age options:
Ane Information		OK Caro

Password age options:  Inter booting:  Inter booting:  Inter booting:  Inter booting:  Password age options:  Password age options: Password age options:  Password age options:  Password age options:  Password age options:  Password age options:  Password age options:  Password age options:  Password age options: Password age optio	lect this object type:	0.017.00		
Interaction:       Passeord age option:         Interaction:		Ziles Mer		
	from this location: contrast local	Locations	Password age options: Ø Enforce minimum password age	
	[piter the object names to select ( <u>councies</u> ): [insue1]	Qieck Names * 2	User cannot change the password within (days): C Enforce maximum password age User must change the password after (days):	* 1
Directly Applies To Name * Mail	Advanced	* 24	Enforce account lockout policy:     Number of failed logon attempts allowed:     Reset failed logon attempts count after (mins):     Account will be locked out     @ For a duration of (mins)     Until an administrator manually unlocks the account	* 30 * 30
Name Mai	Directly Applies To			
	Name * Mail			 

issword Settings	Password Settings				80
Directly Applies To	Name: Procedence: Poli-Group1 Precedence: Poli-Group1 Precedence: Poli-Group1 Precedence: Poli-Group1 Procedence: Poli-Group1 Poli-Group2	* 2	Password age options:	* []	1 42 30
	Directly Applies To Name Mail Group1				Add

### **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 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 <u>http://yourservername</u> 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**.

	Documents Properties	?	x
Target Settings			
Select the real	direction settings for Documents.		
Grant the user e	exclusive rights to Documents.		
Move the conte	ents of Documents to the new location.		
Also apply redin Server, Window systems.	ection policy to Windows 2000, Window vs XP, and Windows Server 2003 operat	s 2000 iing	
Policy Removal —			
C Leave the folde	r in the new location when policy is remo	oved.	
C Redirect the fol policy is remove	der back to the local userprofile location ed.	when	
	OK Cancel	Арр	dy

- 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.

3	Active	Directory Users	and Computers	- 🗆 X
File       Action       View       Help         Image: Second Uper Second Upe	Active I	Directory Users	and Computers	
System V				

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.

<u>.</u>	Group Policy Management Editor
File Action View Help	
🗢 🏟 🙍 🖬 🛱 🖬 🖉	m 🖸 🙆 🔶 🕇
<ul> <li>Faculty Only [DC1.SCHOOL.LOCAL] Policy</li> <li>Computer Configuration         <ul> <li>Policies</li> <li>Preferences</li> <li>User Configuration</li> <li>Policies</li> <li>Policies</li> <li>Preferences</li> <li>Vindows Settings</li> <li>Control Panel Settings</li> <li>Devices</li> <li>Devices</li> <li>Folder Options</li> </ul> </li> </ul>	Internet Settings         Processing       Name       Order         There are no items to show in this view.
Internet Settingen	Internet Explorer 5 and 6
Network All Tasks	Internet Explorer 7
Power Ol View	Internet Explorer 8 and 9
Regional Copy Schedule Print Start Mer Refresh Export List	Internet Explorer 10
Help	
Creates a new item in this container.	Preferences Extended Standard

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.

		Proxy Settings		×		
Servers						
	Туре	Proxy address to use		Port		
ĢU <u>≡</u>	HTTP:	127.0.0.1	:	8080		
	Secure:	127.0.0.1	:	8080		
	FTP:	127.0.0.1	:	8080		
	Socks:		:			
Use the same proxy server for all protocols						
	I	xy servers for addresses begi				
	I			~		
L	Use semicolons ( ; ) to separate entries.					
		OK		Cancel		

- 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.

<u>.</u>	Group Polic	y Management Editor		- 🗆 X
File Action View Help				
🧇 🄿 🙍 📰 🔒 🛛 🗊 🝸				
<ul> <li>▷ Oftware Settings</li> <li>△ Windows Settings</li> </ul>	Internet Explorer			
⊿ Administrative Templates: Polic ▷ Control Panel	Prevent changing proxy settings	Setting E Disable external branding of Internet Explorer	State Not configured	C ^
Desktop     Desktop     Network	Edit policy setting	Disable Import/Export Settings wizard     Disable Internet Connection wizard	Not configured Not configured	
Shared Folders  Start Menu and Taskbar  System	At least Internet Explorer 5.0	<ul> <li>Disable the Reset Web Settings feature</li> <li>Display error message on proxy script download failure</li> </ul>	Not configured Not configured	
✓ Jysein ✓ Jysein ✓ Windows Components ✓ Add features to Window	Description: This policy setting specifies if a user	E Do not allow users to enable or disable add-ons E Enforce full-screen mode	Not configured Not configured	
🚆 App runtime 🧮 Application Compatibilit ≡	If you enable this policy setting, the	<ul> <li>Identity Manager: Prevent users from using Identities</li> <li>Notify users if Internet Explorer is not the default web browser</li> </ul>	Not configured Not configured	
Attachment Manager AutoPlay Policies	user will not be able to configure proxy settings.	<ul> <li>Pop-up allow list</li> <li>Position the menu bar above the navigation bar</li> </ul>	Not configured Not configured	
▷ ☐ Backup ☐ Credential User Interface	If you disable or do not configure this policy setting, the user can configure	Prevent "Fix settings" functionality     Prevent access to Internet Explorer Help	Not configured Not configured	
📴 Desktop Gadgets ▷ 🧰 Desktop Window Manag	proxy settings.	Prevent bypassing SmartScreen Filter warnings     Prevent bypassing SmartScreen Filter warnings about files th	Not configured Not configured	=
Digital Locker		Prevent changing pop-up filter level     Prevent changing proxy settings	Not configured Not configured	
File Explorer		<ul> <li>Prevent changing the default search provider</li> <li>Prevent configuration of how windows open</li> </ul>	Not configured Not configured	
instant Search ▷ Call Internet Explorer		Prevent configuration of new tab creation     Prevent Internet Explorer Search box from appearing	Not configured Not configured	
Location and sensors     Microsoft Management     Microsoft Management		Prevent managing pop-up exception list     Prevent managing SmartScreen Filter	Not configured Not configured	
Network Projector		Prevent managing the phishing filter  Prevent participation in the Customer Experience Improvem	Not configured Not configured	
Presentation Settings		Fill         Prevent per-user installation of ActiveX controls           <	Not configured	>
	Extended Standard /			

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

	New Drive Properties
General Common	]
Action:	Create 🗸
Location:	\\dc1\data
Reconnect:	Label as:
Drive Letter	
🔾 Use first ava	ailable, starting at:
Connect as (option	onal)
Password:	Confirm password:
Hide/Show this d	rive Hide/Show all drives
No change	No change
O Hide this driv	/e O Hide all drives
O Show this dri	O Show all drives
	OK Cancel Apply Help

### Loopback Processing

Loopback processing allows a computer to act like a user when applying a policy. This policy directs the system to aplly the set of GPSs 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

Computer Configuration  Computer Configuration  Policies  Software Settings  Mindows Settings  Administrative Templates:  Control Panel  Metwork  Printers  Control Panel  Administrative Templates:  Control Panel  Administrative Templates:  Control Panel  Control Panel  Administrative Templates:  Control Panel  Administrative Templates:  Control Panel  Control Panel  Control Panel  Control Panel  Disk NV Cache  Control Panel  Control Pane	<ul> <li>Configure Network Shares preference extension policy proc</li> <li>Configure Power Options preference extension policy processing</li> <li>Configure Printers preference extension policy processing</li> <li>Configure Regional Options preference extension policy processing</li> <li>Configure Registry preference extension policy processing</li> <li>Configure Registry preference extension policy processing</li> <li>Configure Scheduled Tasks preference extension policy proc</li> <li>Configure scripts policy processing</li> <li>Configure scripts policy processing</li> <li>Configure Services preference extension policy processing</li> <li>Configure Shortcuts preference extension policy processing</li> <li>Configure Shortcuts preference extension policy processing</li> <li>Configure Shortcuts preference extension policy processing</li> <li>Configure Software Installation policy processing</li> </ul>	Not configured Not configured
Disk Quotas	Configure user Group Policy loopback processing mode	Enabled
<ul> <li>Driver Installation</li> <li>Early Launch Antim</li> <li>File Classification Ir</li> <li>File Share Shadow (</li> <li>Filesystem</li> <li>Folder Redirection</li> <li>Group Policy</li> </ul>	<ul> <li>Configure wired policy processing</li> <li>Configure wireless policy processing</li> <li>Determine if interactive users can generate Resultant Set of</li> <li>Enable AD/DFS domain controller synchronization during p</li> <li>Remove users' ability to invoke machine policy refresh</li> <li>Set Group Policy refresh interval for computers</li> <li>Set Group Policy refresh interval for domain controllers</li> </ul>	Not configured Not configured Not configured Not configured Not configured Not configured Not configured
Internet Communic	< III	

### 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 10based 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:

CAL.	Administrator: Command Prompt	-		×	
Microsoft Windows [Version (c) 2013 Microsoft Corpora	6.3.9600] tion. All rights reserved.				•
C:\windows\system32>gpupda Updating policy	te			r	
Computer policy could not ountered:	be updated successfully. The following error	's we	re e	enc	
The processing of Group Po d policy settings for the 5-4147-8EB7-38789553F6A0>, Group Policy settings will e event details for more i ailure.	licy failed. Windows could not apply the reg Group Policy object LDAP://CN=Machine,cn={CF cn=policies,cn=system, not be resolved until this event is resolve nformation on the file name and path that ca	d. V	y-ba 30-3 iew the	ase 389 th e f	
User Policy update has com	pleted successfully.				
To diagnose the failure, r rom the command line to ac	eview the event log or run GPRESULT /H GPRep cess information about Group Policy results.	ort.	htm:	lf	
C:\windows\system32> <u></u>					

### Solution

Manually preform an authoritive synchronization between the two DCs. As you may know, DFSR no longer uses the same steps as FSR to do an authoritive sync. Below are my notes and experiences on completing an authoritive 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. C	lick on the	Start menu,	select Administrative	Tools,	and then	click Services
------	-------------	-------------	-----------------------	--------	----------	----------------

	,		
			Remote Desktop Services
		-	Certification Authority
		<b>(</b> 0,	Component Services
		-	Computer Management
		-	Data Sources (ODBC)
	035	8	Event Viewer
Certification Authority	, Chang	-	Internet Information Services (IIS) Manager
		e,	iSCSI Initiator
Command Prompt	~ <u>~</u>	-	Local Security Policy
	Jack Stromberg - Admin	0	Performance Monitor
		-	Security Configuration Wizard
	Documents		Server Manager
		0,	Services
internet Information Services (IIS)	Computer	3	Share and Storage Management
Manager	Network	-	Storage Explor
			System Configuration
	Control Panel	٢	Task Scheduler
			Windows Firewall with Advanced Security
	Devices and Printers		Windows Memory Diagnostic
		23	Windows PowerShell Modules
	Administrative Tools	1	Windows Server Backup
	Help and Support	Γ	
	Rup		
All Programs	Windows Security		
Search programs and files	Log off		
🍂 🛃 🖉			

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

	5. Open up	ADSI Euli	
<b>a</b>	Server	Manager	_ <b>D</b> X
Server N	lanager • Dashboard		View Help
<ul> <li>Dashboard</li> <li>Local Server</li> </ul>	WELCOME TO SERVER M	Active Directory Domains and Trusts Active Directory Module for Windows PowerShell Active Directory Sites and Services	<u>^</u>
<ul> <li>Il Servers</li> <li>AD DS</li> <li>DHCP</li> <li>DNS</li> <li>File and Storage Services ▷</li> </ul>	QUICK START	Active Directory Users and Computers ADSI Edit Component Services Computer Management Defragment and Optimize Drives DHCP DNS Event Viewer Group Policy Management	=
	LEARN MORE  ROLES AND SERVER GRO Roles: 4   Server groups: 1    AD DS  Manageability Events Services Performance BPA results	iSCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Security Configuration Wizard Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows Firewall with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell (x86)	Hide
		Windows PowerShell ISE Windows PowerShell ISE (x86)	
		Windows Server Backup	

### ADSI Edit 3 0

4. Open up the <b>Default naming context</b>
Connection Settings ×
Name: Default naming context
Path: LDAP:// /Default naming context
Connection Point
O Select or type a Distinguished Name or Naming Context:
✓
• Select a well known Naming Context:
Default naming context
Computer
O Select or type a domain or <u>s</u> erver: (Server   Domain [:port])
×
• Default (Domain or server that you logged in to)
Use SSL-based Encryption
Ad <u>v</u> anced OK Cancel

the Deferrit 4 0 •

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

	1	lisD1/SIC-options=1		
	CN=SYSV	OL Subscription Properties	?	x
Attribute Edit	tor Security			
Au de terre				
Attributes:				
Attribute	Configuration	Value		^
msDFSR	Conflict Path	<not set=""></not>		
msDFSR	-ContentSet	\8D\C6\76\22\24\BC\BE\46\B4\92	\06\7	o l
msDESR	-DeletedPath	<not set=""></not>		
msDFSR	-DeletedSize	<not set=""></not>		
msDFSR	-DfsLinkTarget	<not set=""></not>		≡
msDFSR	-Enabled	TRUE		
msDFSF			v	
msDFS	Bo	oolean Attribute Editor	^	
msDFS msDFS	Attribute:	msDFSR-Enabled		
msDES	Value:			
msDFS				
msDFS				$\overline{}$
<	False			
	○ Not set			
Edi		OK Cancel	٦ [	
			- [	
	ОК	Cancel Apply	He	alp
	CN=SY	'SVOL Subscription Properties 2	<b>K</b>	
Attri	ibute Editor Securi	tv		
At	tributes:	<u>a  </u>		
	Attribute	Value	1	
· · · · · · · · · · · · · · · · · · ·	msDFSR-MaxAgeIn(	C <not set=""></not>		
	msDFSR-MinDuratio msDESR-OnDeman	n <not set=""></not>		
· · · · · ·	msDFSR-OnDeman	d <not set=""></not>		
	msDFSR-Options	<not set=""></not>		1
		Integer Attribute Editor	x	
Attrib	oute: msD	FSR-Options		
Valu	e:		_	
1				
	Clear	OK Cancel		
	< 1			
	Edit	Filter		
	ОК	Cancel Apply Help	$\exists$	

### msDFSR-Enabled=FALSE msDFSR-options=1

Both values applied					
CN=SYSV	OL Subscription Properties	?	x		
Attribute Editor Security					
Attri <u>b</u> utes:					
Attribute	Value		~		
msDFSR-DeletedPath	<not set=""></not>				
msDFSR-DeletedSize	<not set=""></not>				
msDFSR-DfsLinkTarget	<not set=""></not>				
msDFSR-Enabled	FALSE				
msDFSR-Extension	<not set=""></not>		=		
msDFSR-Flags	<not set=""></not>		-		
msDFSR-MaxAgeInC	<not set=""></not>				
msDFSR-MinDuration	<not set=""></not>				
msDFSR-OnDemand	<not set=""></not>				
msDFSR-OnDemand	<not set=""></not>				
msDFSR-Options	1				
msDFSR-Options2	<not set=""></not>				
msDFSR-ReadOnly	FALSE				
msDFSR-Replication	<del>¢</del> j∲Mqb <b>%H</b> ∜∲TGq <del>%</del> %		$\overline{}$		
<		>			
		_			
Edit		<u>F</u> ilter			
ОК	Cancel Apply	H	elp		

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

CN=SYSVOL Subscription Properti	es 🔛	^			
Attribute Editor Security					
Attributes:		_			
Attribute Value					
cn SYSVOL Subscription	4) 02) 00) 70	N 10			
msDFSR-Enabled TRUE	4\32\00\7;	113			
msDFSR-ReadOnly FALSE					
msDFSR-Replication ♦j♦Mqb♦H♦♦TGq♦♦♦					
msDFSR-RootPath C:\Windows\SYSVOL\domain	re ne \intellie	- tir			
objectCategory CN=ms-DFSR-Subscription,CN=	Schema,CN	=Co			
objectClass top; msDFSR-Subscription					
showInAdvancedVie TRUE					
< III		>			
C III	Filter	>			
C III	Filter	> w only a	ttributes that	t have value	5
Cancel Apply	Filter	> w only a w only w	ttributes tha	t have value outes	5
Edit OK Cancel Apply	Filter       ✓     Sho       ✓     Sho       Sho     Sho	> w only a w only w attrib	ttributes tha ritable attrib ites:	t have value butes	s
Edit OK Cancel Apply	Filter       ✓     Sho       ✓     Sho       ✓     No	> w only a w only w attrib 1andato	ttributes tha rritable attrib ites: y	t have value outes	5
Edit     OK Cancel Apply	Filter ✓ Sho ✓ Sho Sho ✓ N ✓ C	> w only w w only w w attrib landato	ttributes tha rritable attrib rtes: Y	t have value outes	5
K     III       Edit     OK       Cancel     Apply	Filter       ✓     Shc       ✓     Shc       ✓     M       ✓     C       Shc     Shc	w only a w only a w only w attrib landato ptional w read-	ttributes tha ritable attrib ttes: y nly attribute	t have value outes	5
K     III       Edit     OK       OK     Cancel	Filter       ✓     She       ✓     She       ✓     M       ✓     C       She     C	w only w w only w w attrib fandato ptional w read- onstruct	ttributes tha ritable attrib ites: y mly attribute ed	t have value outes	S
K Cancel Apply	Filter ✓ Sho ✓ Sho Sho C Sho C B	w only v w only v w attrib landato ptional w read- onstruct acklinks	ttributes tha rritable attrib ites: Y mly attribute ed	t have value outes	5

	CN=SYSV	OL Subscription Properties	x
Attribute Edit	or Security		
Attributes:			
Attribute		Value ^	٦
msDFSR-	ConflictPath	<not set=""></not>	
msDFSR4	ConflictSize1	<not set=""></not>	
msDFSR4	ContentSet	\8D\C6\76\22\24\BC\BF\46\B4\92\06\79	
msDFSR-	DeletedPath	<not set=""></not>	ł
msDFSR-	DeletedSize	<not set=""></not>	
msDFSR-	DfsLink Target	<not set=""></not>	
msDFSR-	Enabled	TRUE	
msDFSF	 Do	alaan Attributa Editor X	
msDFS	DU		
msDFS	Attribute:	msDESR-Enabled	
msDFS	remotio.		
msDFS	Value:		
msDFS	○ True		
msDF5	False		ł
<	○ Not set		
<b>F</b> -3:			٦
EOI		OK Cancel	
			_
	OK	Cancel Apply Help	

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

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

repadmin /syncall primary\_dc\_name /Aped



- 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)

9. 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

10. Open up event viewer and navigate to Applications and Services Logs -> DFS Replication. Verify

		you see Event ID 41	14.	
		Event Viewer		_ <b>D</b> X
<u>File Action View H</u> elp				
🗢 🔿 🙍 🖬 🚺				
🛃 Event Viewer (Local)	DFS Replication Number of events: 16			Actions
Custom Views	Level	Date and Time	Source ^	DFS Replication
Application	Information	7/25/2014 2:05:00 PM	DFSR =	🍯 Open Saved Log
E Security	(1) Information	7/25/2014 1:49:59 PM	DFSR	Y Create Custom View
E Setup	Information	7/25/2014 1:44:59 PM	DFSR	Import Custom View
System	Information	7/25/2014 1:39:58 PM 7/25/2014 1:39:58 PM	DESR	Clearlog
Applications and Services Lo	Information	7/25/2014 1:07:29 PM	DESR	Tites Count Las
Active Directory Web Ser	<		>	Filter Current Log
DFS Replication	Event 4114 DESR		×	Properties
Directory Service				Find
DNS Server	General Details			Save All Events As
Internet Explorer	The replicated folder at local path C//Windows/	Attach a Task To this Log		
📓 Key Management Service	replication of the antical plant extended of the second many of the second abused on the spinated of the second many of the second second many of the second s			View 🕨
Microsoft				Q Refresh
Windows PowerShell				Help +
Subchpitons	Replicated Folder ID: 22/6C68D-BC24-46BF-B49 Replication Group Name: Domain System Volu	Event 4114. DESR		
	Replication Group ID: 4DCE6A8E-6271-48B6-A0	D0-5447718B8FAB		Event Properties
	Member 10. 10/230/3-0401-4CAD-55E1-03453E	10FT/6		Attack Tack To This Grant
				Attach Task To This Event
				re copy
	Log Name: DFS Replication			Save Selected Events
	Source: DFSR	Logged: 7/25/2014 2:05:00 PM		G Refresh
	Event ID: 4114	Task Category: None		🛛 Help 🕨 🕨
	Level: Information	Keywords: Classic		
	User: N/A	Computer		
	More Information: Event Los Online Help			
	wore provinceous. <u>Event Log Online Help</u>			
< III >				

- 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>

2		ADSI Edit
File Action View Help		
🗢 🔿 🙍 🔀 🖼 😹 🖬		
📝 ADSI Edit	Name	Class Distinguished Name
A JO Default naming context [	INARNE ICN-SYSVOL Subscription Move Delete Rename Properties Help	Chass         Joininguisee Vame           msDFSR-Sub         CN=SYSYOL Subscription, CN=Domain System Volume, CN=DFSR-LocalSettings,
	12. Set the	value of <b>msDFSR-Enabled</b> to <b>TRUE</b>
		Boolean Attribute Editor
	Attribute: Value: O True O False O Not se	et
		Cancel

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

**NOTE:** This is a utility apart of DFS Managment 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



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

6			Event Viewer		
<u>File Action View H</u> elp					
🗢 🔿 🙇 🖬 🔢 🖬					
🛃 Event Viewer (Local)	DFS Replication Number of events	: 18			Actions
Custom Views	Level	Date and Time	Source	Event ID Task Category	DFS Replication
Windows Logs     Application	Information	7/25/2014 2:45:11 PM	DFSR	4602 None	Open Saved Log
Security	(i) Information	7/25/2014 2:45:11 PM	DFSR	2002 None	Create Curtom View
E Setup	(1) Information	7/25/2014 2:05:00 PM	DFSR	4114 None	· · · · · · · · · · · · · · · · · · ·
System	<ol> <li>Information</li> </ol>	7/25/2014 1:49:59 PM	DFSR	4114 None	Import Custom View
Forwarded Events	(1) Information	7/25/2014 1:44:59 PM	DFSR	4114 None	Clear Log
Applications and Services Lo	(1) Information	7/25/2014 1:39:58 PM	DFSR	2010 None	Filter Current Log
Active Directory Web Ser	U Information	7/25/2014 1:39:58 PM	DFSR	4114 None	Properties
Directory Service	Event 4602, DFSR				× 000 Find
DNS Server	General D. ( 1				Save All Events As
Hardware Events	Details				Attack a Tack Ta this Lan
👔 Internet Explorer	The DFS Renlication sensice successfully initialized the SVSV/U renlicated folder at local nath C-Windows/SVSV/U/Udomain. This member is the designated nimany member for this renlicated				
Key Management Service	folder. No user action is required.	To check for the presence of the SYSVOL share, open a co	mmand prompt window and then type "	net share".	View
Microsoft	Additional Information				Refresh
Subscriptions	Replicated Folder Name: SYSVOL	Share			👔 Help
120 Subscriptions	Replicated Folder ID: 2276C68D-B	C24-46BF-B492-067919163EDA			Funt (CO) DECD
	Replication Group Name: Domain Replication Group ID: 4DCE648E-	1 System Volume 6271-4886-4000-544771888E48			Event 4002, DFSR
	Member ID: F8723875-848F-4CAB	-99EF-D3493E7DF178			Event Properties
	Read-Only: 0				Attach Task To This Event
					🖶 Сору
					Save Selected Events
	Log Name: DFS Replication	in .			G Refresh
	Source: DESB	Logged: 7/25/2014 2:45:11 PM			
	Event ID: 4602	Task Category: None			Негр
	Level: Information	Kenwords Classic			
	Uran N/A	Computer			
	OnCoder	comparez.			
	More Information: Event Log On	line Help			
	wore information: Event Log On	interneip			
	1				1

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

Boolean Attribute Editor						
<u>A</u> ttribute:	msDFSR-Enabled					
<u>V</u> alue: ● <u>True</u> ○ <u>F</u> alse ○ <u>N</u> ot set						
	OK Cancel					

17. Execute the following via an elevated command prompt

### a. **DFSRDIAG POLLAD**

i. **NOTE:** This is a utility apart of DFS Managment 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 I	Event ID 2002	and 4602 on	each of the	secondary DCs
-----	------------------	---------------	-------------	-------------	---------------

E Event Viewer	
File Action View Help	
	• <i>c</i>
Certa reset (coca)     O's replication     vurtue of events: 10	Actions
Vindows Level Date and Time Source Event ID Task Category	DFS Replication
Application 7/25/2014 245:11 PM DFSR 4502 None	Open Saved Log
E Security Distribution //22/2014/243/11 PM Dr5R 2002 None	Y Create Custom View
Setup Information 1/2/2/014 Jugs PM Drsn 4114 None	Import Custom View
E system Diano 1/2/2014 144-59 PM DSSP 4114 None	Clearlon
Convariance oversise in Conversion (Conversion Conversion) (Conversion Conversion Conver	Tites Count Los
R Active Directory Web Ser 11 Information 7/25/2014 1:39:58 PM DFSR 4114 None	Fliter Current Log
DFS Replication	Properties
E Directory Service	Find
🛃 DNS Server General Details	Save All Events As
Hardware Events	Attach a Task To this Log
The DFS Replication service successfully initialized the SYSOL of the Structure Explicated folder at local path C:\Windows\SYSVOL\domain. This member is the designated primary member for this replicated	View
Microsoft Microsoft	Refresh
E Windows PowerShell Additional Information:	
Keplicated Folder Name: SYSVOL Share Replicated Folder II: SYSVOL Share	I nep
Replication Group Name Domain System Volume	Event 4602, DFSR
Replication Group ID: 4DCE6A9E-6271-4886-A0D0-544771888FAB Marging ID: F8723678_46F. AD AD CEPT-13008FFAB	Event Properties
Read-Only 0	Attach Task To This Event
	E Conv
	Care Selected Events
Las Nacional DMC Back relies	
	G Kerresh
gource: DESK Loggeg //2/2014/240:11 PM	👔 Help 🕨 🕨
Event IU: 4002 Task Category: None	
Level: information <u>Reywords</u> : Classic	
User: IV/A Compute:	
Uppeade	
More information: Event Log Unline help	

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.



### 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**.

Regula Din								
Michael Petrolone	Life at a glance			Play and explore				
Get Started	間	<		A	(0)	1000	1202	
Get Skype	Calandar	Mail		Xires	Mail	Movies & TV	100	
😥 Maps								
🔣 People	е	~	0	<b>a i i i</b>				
Calculator	Microsoft Edge	Partes	Contena	Marray	News			
Alarna & Cock	e de la constante de la consta	Unpin 1 Resize	N R	۹. į	Margaret Kaline (darase	Cut Office		
		Turn Iv	e tile off					
		Pin to t	taskbar					
(iii) Ne toporer >		Uninsta	4					
(i) Settings	Windows RowerShell ISE	Windows PowerShell						
E at sea								
			-					
Search the web and Wind		0	C	-				∧ 12 49 ↓ D€ 9/17/2015



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

🚈 Windows PowerShell ISE	-		×
File Edit View Tools Debug Add-ons Help			
1 🛎 🖬 🤞 🖬 🔪 🖤 🔍 🕨 🗟 🔳 😪 🗖 🖽			B) .
		Scrip	pt 🕑
PS C:\> Export-StartLayout -Path C:\tmp\start.xml			^
PS C:\>			
			- 21
1999년 - 1997년 - 1997년 - 1997년 1998년 1997년 199 1997년 - 1997년 - 1997년 - 1997년 1997			~
			>
Completed Ln 3 Col 9			115%

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.



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.

File Action Vee Help   Image: Computer Configuration Image: Computer Configuration   Image: Configuration   Image: Control Predict   Image: Configuration   Image: Configuration   Image: Control Predict   Image: Configuration   Image: Control Predict   Image: Control Pred		Gr	oup Policy Management Editor	= 0 X
Image: Start Allow and Falsbar	File Action View Help			
Control Downed Parkoy (Parkoy     Parkoten Comparation     Parkoten Comparation     Parkoten Configuration     Parkoten Configuration     Parkoten Stating     Parkoten Stat	💠 🔶 🙇 🔂 🖬 🐨 🝸			
Image: Spectra in the stating in the special part in the specin part in the special part in the special part in the	Default Demain Policy (51.82.COM) Policy     A Computer Configuration     Policies     Policies     Policies     Software Settings     Administrative Templates: Policy definition     Policies Panel     Policies     Printers     Software     Softwa	Start Menu and Taskbar Start Screen Leyout Edit policy setting. A Requirements: At least Windows Server 2012 R2, Windows 8.1 er Windows RT 8.1 Description Specifies the Start screen leyout	Setting Start Screen Layout Pin Apps to Start when installed Start Screen Layout Not Configured Comment:	State Comment Enabled No Net configured No Start Screen Layout - 0 4 Drevious Setting
Administrative templates policy definition     Administrative templ	<ul> <li>System</li> <li>Windows Components</li> <li>All Settings</li> <li>Preferences</li> <li>User Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> </ul>	This sets. This setting lets you specify the Start screen layout for users and prevents them from changing its configuration. The Start screen layout you specify must be stored in an NAR, file that was generated by the Sport-StartLayout PowerShell cradiet. To use this setting, you must first	Enabled  Supported on:  At	Lieset Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1
W unit fluide this settion or do     Encoded /Randard /	Control Panel     Control Panel     Control Panel     Control Panel     Control Panel     Source Folders     Source Folder	manually configure a device's Start screen layout to the deviced look and feel. Once you are done, run the Epoch StartLayout PowerShell cradiet on that same device. The condiet will generate an XML file representing the layout you configured. Once the XML file is generated and moved to the deviced File path, type the fully qualified path and same of the XML file. You can type a local path, such as C.StartLayoutJampLayoutLand or a UMC path, such as C.StartLayoutLayoutLand or a UMC path, such as C.StartLayoutLayoutLand or a UMC path, such as (Visener/ShartLayoutLand, if the upscritted file is not available when the user logs on the layout won't be changed. Users cannot customic their Start screen while this setting is evabled.	Start Layout File [VisTishaw(store.aml	Specinds that Screen Hypour for uses.
2 setting(s)	< III > 2 setting(s)	Extended (Standard/		

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 <b>Settings &gt;Personalization &gt; Start</b> as well as the options in dialog available via right-click Taskbar <b>&gt; Properties</b>
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 <b>All apps</b> 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 <b>Most used</b> group of apps.
Remove Logoff on the Start Menu	<b>Logoff</b> has been changed to <b>Sign Out</b> 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 <b>Run as different user</b> 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 <b>User</b> <b>Configuration</b> or <b>Computer Configuration</b> . <b>Note</b> 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.

🧾 Local Group Policy Editor	AskVG.com		×
File Action View Help			
🗢 🄿 🗖 📰 🗟 🖬	7		
Portable Operating System   Presentation Settings	Setting	State	^
Remote Desktop Services     PSS Foods	Add primary intranet search location	Not configured Not configured	
Search	Allow Cortana	Disabled	
Security Center	Allow indexing of encrypted files	Not configured Not configured	
Smart Card	E Allow use of diacritics	Not configured	
Software Protection Platfor ¥	Always use automatic language detecti	Not configured	~
< > 38 setting(s)	\Extended \Standard /		

# Disable Web Search in Windows 10

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

🚊 Local Group Policy Editor		- 🗆 >	×
File         Action         View         Help           ◆         ◆         2         □         3         □         ▼			
<ul> <li>OneDrive</li> <li>Online Assistance</li> <li>Portable Operating System</li> <li>Presentation Settings</li> <li>Remote Desktop Services</li> <li>RSS Feeds</li> <li>Search</li> <li>Security Center</li> <li>Shutdown Options</li> <li>Smart Card</li> <li>Sound Recorder</li> <li>Store</li> </ul>	Setting Default indexed paths Default indexed paths Disable indexer backoff Do not allow locations on removable drives to be add Do not allow web search Don't search the web or display web results in Search Don't search the web or display web results in Search Enable indexing of online delegate mailboxes Enable throttling for online mail indexing Prevent indexing of certain file types Demant adding unerconsolited locations to the All Loc Extended Standard	State Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	<
36 setting(s)			

Moving on, in the right of above shown window and scroll down to look for *Settings* named **Do not** allow web searchand **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:

🍜 Don't search the	web or display wel	b results in Search	n			—		×
Don't search the web or display web results in Search Previous Setting Next Setting								
O Not Configured	Comment:							^
Enabled     Disabled								
	Supported on:	אונcrosoft Windows 8.1 or later						< _
Options:			Help:					
		This policy can perform displayed ii If you enab the web an performs a If you disat web and w query in Se If you don't whether or web results	setting allows yorn in queries on the v in Search. Ile this policy setti d web results wor query in Search. Set this policy setti eb results will be c arch. It configure this policy not Search can pr are displayed in S	i to control veb, and if t ng, queries 't be display ng, queries lisplayed wl licy setting, iform quer earch.	whether or n he web result won't be perf yed when a u will be perfo nen a user per a user can c ies on the we	ts arch ts are formed on iser rmed on ti iforms a ihoose ib, and if ti	ne ne	
					ОК	Cancel	Appl	y

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