7-Default Domain Policy

Data collected on: 21/05/2014 08:38:28

General

Details

Domain	curriculum.local
Owner	CURRICULUM\Domain Admins
Created	01/02/2011 13:25:08
Modified	04/07/2013 09:33:04
User Revisions	1 (AD), 1 (sysvol)
Computer Revisions	51 (AD), 51 (sysvol)
Unique ID	{CCF6CB2C-B946-41E8-B97F-6F4F43460123}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
curriculum	No	Enabled	curricu

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	W7
Description	Windows 7 filter

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
CURRICULUM\Domain Admins	Edit settings, delete, modify security	No
CURRICULUM\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	3 passwords remembered
Maximum password age	120 days
Minimum password age	0 days

Minimum password length	6 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Security Options

Interactive Logon

Policy	Setting
Interactive logon: Do not display last user name	Enabled
Interactive logon: Message text for users attempting to log on	By clicking OK below I agree that the username I am logging or MY OWN, username and that I will abide by the School Accept Use Policy., Every website visited is logged and these ARE che Every time you log on or log off a computer a log IS created., ** COMPUTER GAMES ARE BANNED FROM THE SCHOOL NE ****, If you are found to be playing a computer game your accou be suspended without warning. This means that you will have n access to the school system., To have your account re-instated must see me to explain your actions., Mr Arris., Network Manag
Interactive logon: Message title for users attempting to log on	"Computer Policy"
Interactive logon: Prompt user to change password before expiration	14 days

Network Security

Policy	Setting
Network security: Force logoff when logon hours expire	Enabled

Event Log

Policy	Setting
Maximum application log size	50048 kilobytes
Maximum security log size	50048 kilobytes
Maximum system log size	50048 kilobytes
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed

Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date

Admin	Admin	07/01/2006 14:13:22

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities

Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

Windows Firewall with Advanced Security

Global Settings

Policy	Setting
Policy version	Not Configured
Disable stateful FTP	Not Configured
Disable stateful PPTP	Not Configured
IPsec exempt	Not Configured
IPsec through NAT	Not Configured
Preshared key encoding	Not Configured
SA idle time	Not Configured
Strong CRL check	Not Configured

Domain Profile Settings

Policy	Setting
Firewall state	Off
Inbound connections	Not Configured
Outbound connections	Not Configured
Apply local firewall rules	Not Configured
Apply local connection security rules	Not Configured
Display notifications	Not Configured
Allow unicast responses	Not Configured
Log dropped packets	Not Configured
Log successful connections	Not Configured
Log file path	Not Configured
Log file maximum size (KB)	Not Configured

Connection Security Settings

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Network/Network Connections

Policy	Setting	Comment
Prohibit use of Internet Connection Firewall on your DNS domain network	Enabled	

Network/Network Connections/Windows Firewall/Domain Profile

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Disabled	

Network/Network Connections/Windows Firewall/Standard Profile

Policy	Setting	Comment
Windows Firewall: Protect all network connections	Disabled	

Network/Offline Files

Policy	Setting	Comment
Action on server disconnect	Enabled	
Specify how the system is to respond when a network server becomes unavailable. Action: Never go offline Never go offline = Server's files are unavailable to local computer Work offline = Server's files are available to local computer		

Policy	Setting	Comment
Allow or Disallow use of the Offline Files feature	Disabled	
Default cache size	Enabled	
Value entered is [percent disk used * 10,000]. For example, to indicate 12.53%, enter 1253. Default cache size: 0		

Policy	Setting	Comment
Files not cached	Enabled	
Files may be excluded from caching on auto-cache shared folders based on their extension. Enter a list of extensions to be excluded. Extensions must be preceded by an asterisk and period. "e.g. *.dbf;*.ndx;*.lnk Extensions:		

Policy	Setting	Comment
Remove 'Make Available Offline'	Enabled	
Synchronize all offline files before logging off	Disabled	

System/Device Installation

Policy	Setting	Comment
Specify search order for device driver source locations	Enabled	
Select search order: Do not search Windows Update		

System/Group Policy

Policy	Setting	Comment
Group Policy slow link detection	Enabled	
Connection speed (Kbps): 0 Enter 0 to disable slow link detection.		

System/Internet Communication Management/Internet Communication settings

Policy	Setting	Comment
Turn off Windows Update device driver searching	Enabled	

System/Logon

Policy	Setting	Comment
Always wait for the network at computer startup and logon	Enabled	

System/Scripts

Policy	Setting	Comment
Run logon scripts synchronously	Enabled	

Windows Components/Windows Messenger

Policy	Setting	Comment
Do not allow Windows Messenger to be run	Enabled	
Do not automatically start Windows Messenger initially	Enabled	

Windows Components/Windows Update

Policy	Setting	Comment
Configure Automatic Updates	Enabled	

Configure automatic updating:	3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.	
Scheduled install day:	0 - Every day
Scheduled install time:	02:00

User Configuration (Enabled)

Policies

Windows Settings

Remote Installation Services

Client Installation Wizard options

Policy	Setting
Custom Setup	Disabled
Restart Setup	Disabled
Tools	Disabled

Internet Explorer Maintenance

Connection/Automatic Browser Configuration

Policy	Setting
Automatically detect configuration settings	Disabled
Automatic Browser Configuration	Not configured

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Network/Offline Files

Policy	Setting	Comment
Action on server disconnect	Enabled	

Specify how the system is to respond when a network server

becomes unavailable.

Action: Never go offline

Never go offline = Server's files are unavailable to local computer

Work offline = Server's files are available to local computer

Policy	Setting	Comment
Synchronize all offline files before logging off	Disabled	

Windows Components/Windows Explorer

Policy	Setting	Comment
Do not track Shell shortcuts during roaming	Enabled	