DIS

Department of Information Systems

Arkansas. A State of Technology.

WINDOWS SERVER 2012 R2

INSTALLATION AND CONFIGURATION

Prepared By
DIS APSCN/LAN Support

DIS

Department of Information Systems

Arkansas. A State of Technology.

Table of Contents

This document is DIS' recommended method for implementing a Windows Server 2012 and Active Directory within a K12 network.

WINDOWS SERVER 2012 R2 REQUIREMENTS

Component	Requirement
Processor	• Minimum: 1.4GHz (x64 processor) • Recommended: 2GHz or faster **Note:** Processor performance depends not only on the clock frequency of the processor, but also on the number of processor cores and the size of the processor cache
Memory	• Minimum: 512 MB RAM or greater • Recommended: 6GB RAM or greater • Maximum (64-bit systems): 4TB (Standard and Datacenter editions)
Available Disk Space	• Minimum: 32GB or greater • Recommended: 80GB or greater **Note:** Servers with more than 16GB of RAM will require more disk space for paging, hibernation, and dump files
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device • Internet Access

PRE-INSTALLATION REQUIREMENTS

- Microsoft Windows Server 2012 R2 DVD (with Service pack IF applicable).
- 1 NAT IP Address.
- Public IP address (IF applicable).
- Floppy Disk, USB Drive, CD/DVD containing your SCSI/RAID drivers.

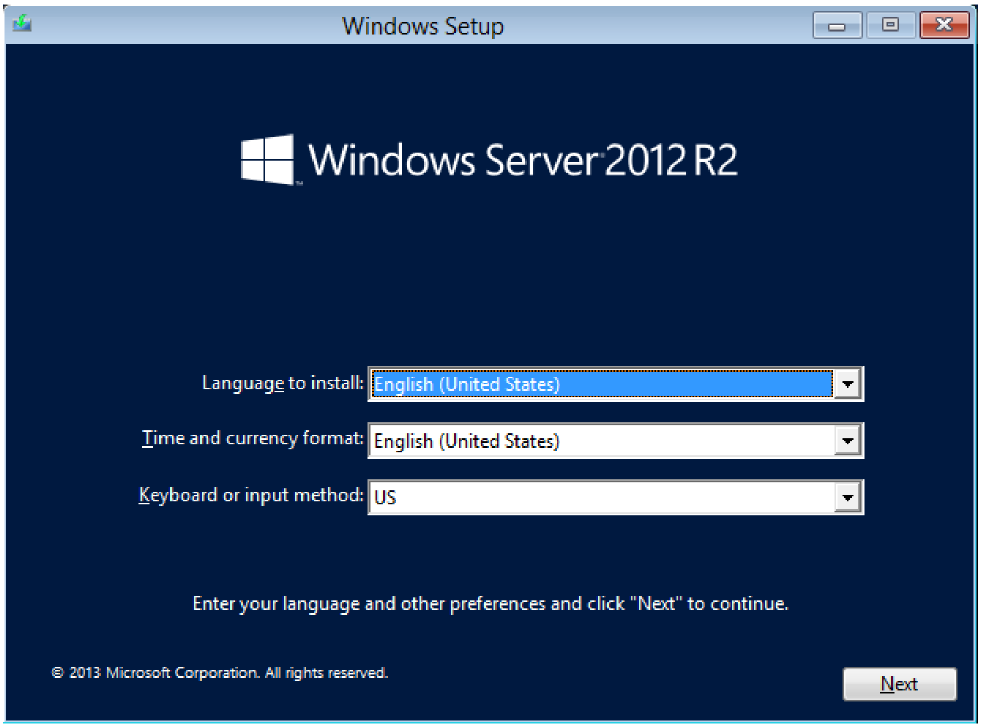
INSTALLATION

1. Insert the Windows 2012 Server installation DVD into the drive.

2. Restart the computer and boot to the DVD-ROM. Wait for Setup to display a dialog box.

3. Insert the appropriate Windows Server 2012 installation media into your DVD drive and reboot the computer/server.

4. When prompted for an installation language and other regional options, make your selection and press **Next**.



Language to install: English (United States)

Time and currency format: English (United States)

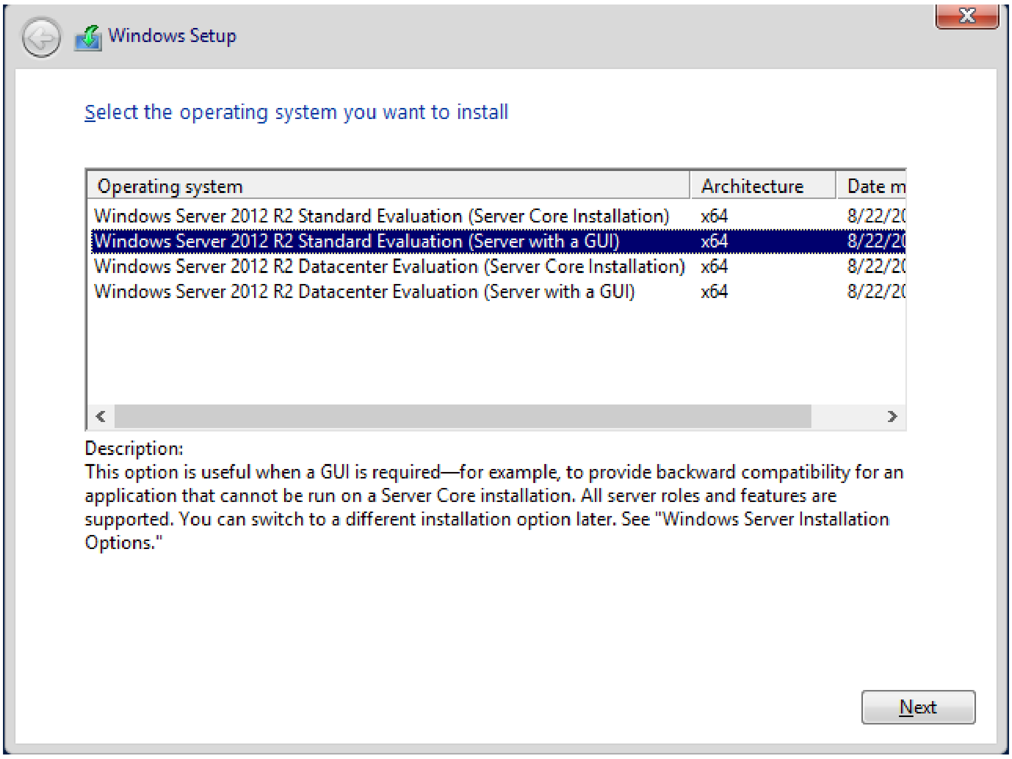
Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© 2013 Microsoft Corporation. All rights reserved.

5. Next, press **Install Now** to begin the installation process.

6. Select the proper edition of Windows Server 2012 R2 that is to be installed and press **Next**.



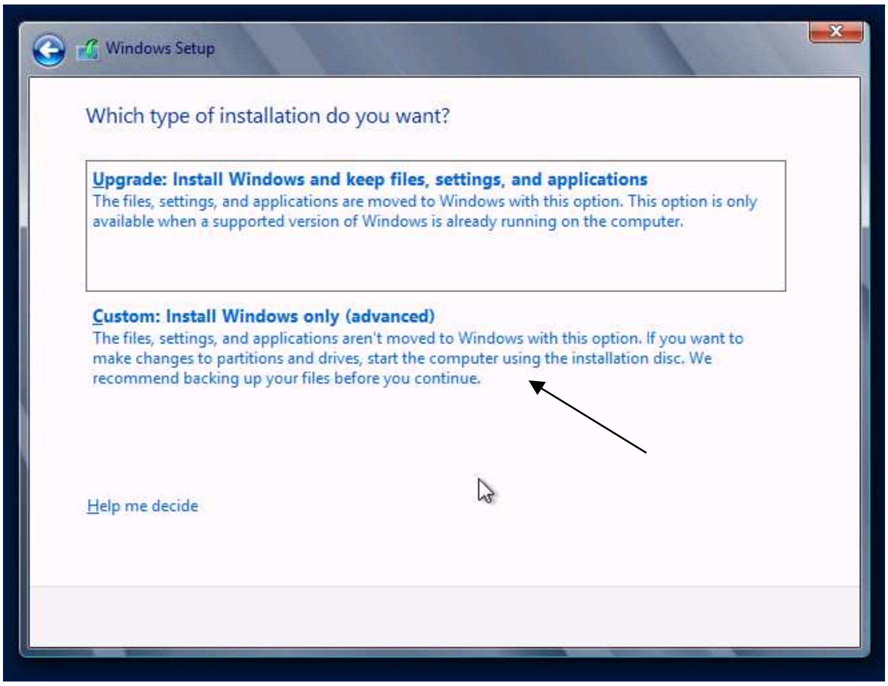
Select the operating system you want to install

Operating system	Architecture	Date m
Windows Server 2012 R2 Standard Evaluation (Server Core Installation)	x64	8/22/20
Windows Server 2012 R2 Standard Evaluation (Server with a GUI)	x64	8/22/20
Windows Server 2012 R2 Datacenter Evaluation (Server Core Installation)	x64	8/22/20
Windows Server 2012 R2 Datacenter Evaluation (Server with a GUI)	x64	8/22/20

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. You can switch to a different installation option later. See "Windows Server Installation Options."

7. Read and accept the license terms by clicking to select the **checkbox** and pressing **Next**.

8. In the "**Which type of installation do you want?**" window, click the only available option – **Custom (Advanced)**.



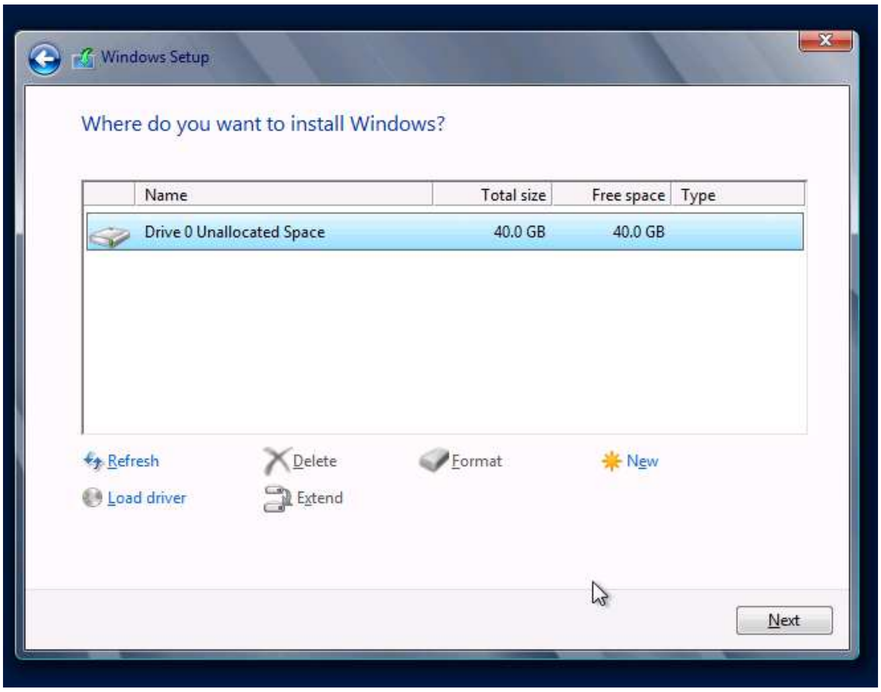
Windows Setup

Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

9. Select the disk that Windows Server 2012 R2 will be installed on and then click **New** to create a partition.



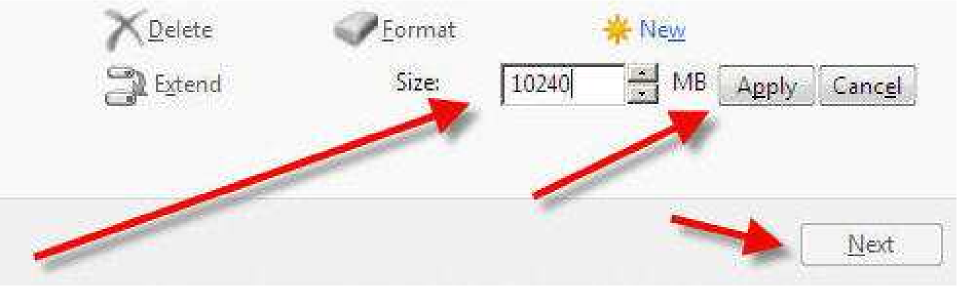
Windows Setup

Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	40.0 GB	40.0 GB	

10. In the “**Size:**” entry box, enter the size of the partition and press **Next**.

    *****The size format is in megabytes. GB * 1024 = Size to be entered.***



You will see the following screen while the installation files are copied to the server. The server will reboot to complete the installation (leave media inserted).

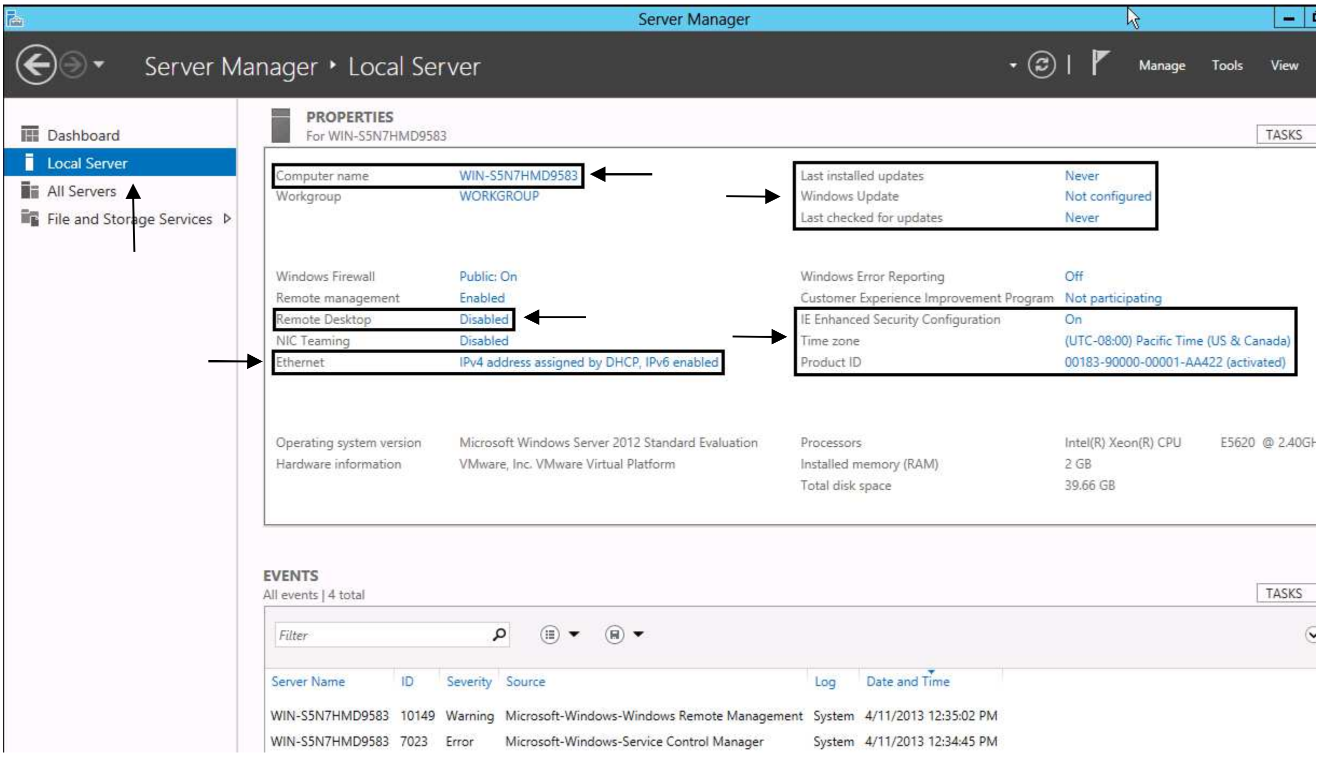
11. Once the server has completed the setup, it will notify you that the password needs to be set. This password **MUST** meet Microsoft password complexity requirements. It will require a minimum password length of 7 characters and three out of the four following:

    a. Upper Case
    b. Lower Case
    c. Numbers
    d. Special Characters

12. Once the password is successfully changed, the server will login to the initial desktop and Server Manager will start up automatically.

SERVER INITIAL CONFIGURATION

1. On the Server Manager screen, click on Local Server.
2. Activate Windows and insert key.
3. Change Computer name.
4. Set Time zone.
5. Configure Networking and change to Static IP and disable IPv6 by unchecking the option for TCP/IPv6.
6. Enable Windows Updates.
7. Download and Install updates.
8. Turn off IE Enhanced Security Configuration for Administrators only.



PROPERTIES
For WIN-S5N7HMD9583

Computer name	WIN-S5N7HMD9583	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Public: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00183-90000-00001-AA422 (activated)
Operating system version	Microsoft Windows Server 2012 Standard Evaluation	Processors	Intel(R) Xeon(R) CPU E5620 @ 2.40GH
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	2 GB
		Total disk space	39.66 GB

EVENTS
All events | 4 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
WIN-S5N7HMD9583	10149	Warning	Microsoft-Windows-Windows Remote Management	System	4/11/2013 12:35:02 PM
WIN-S5N7HMD9583	7023	Error	Microsoft-Windows-Service Control Manager	System	4/11/2013 12:34:45 PM

Disable IPv6 via Registry Editor

Recommended To Be Done

1. Open the Registry Editor by moving your mouse over the bottom-right or top-right corner of the screen. Click on the Search button (magnifying glass), type **REGEDIT** and press **Enter**

2. Expand the following Key Structure in the Registry Editor:

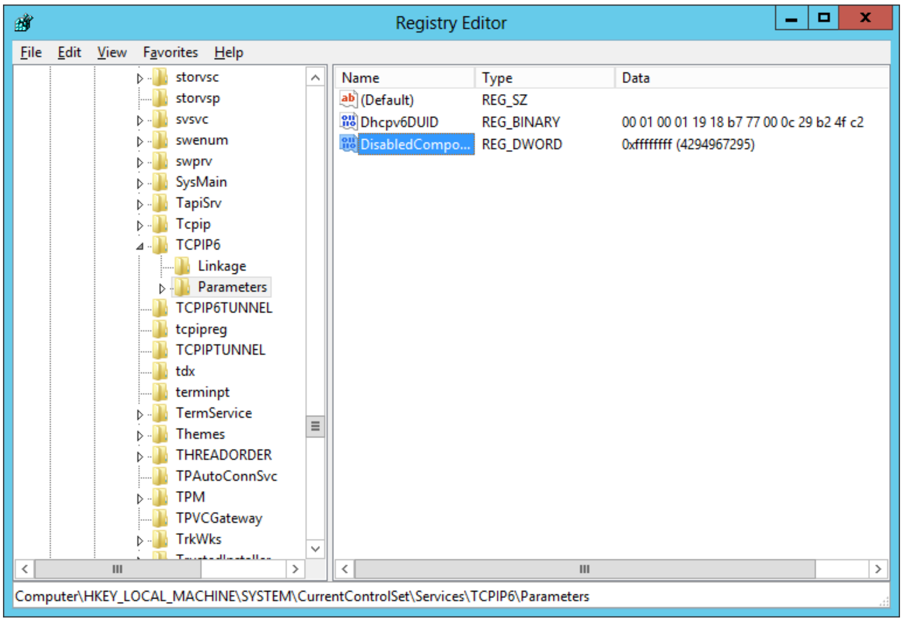
```
HKEY_LOCAL_MACHINE
  |---System
        |---CurrentControlSet
               |---Services
                     |---Tcpip6
                           |---Parameters
```

3. Right-Click on the Parameters Key and click **New** > **DWORD (32-Bit) Value**.

4. Type in the name **DisabledComponents** and press **Enter**.

5. Double-click on the newly created key and enter **ffffffff (8 f's)** for the value data in Hexadecimal mode.

6. Close the Registry Editor.



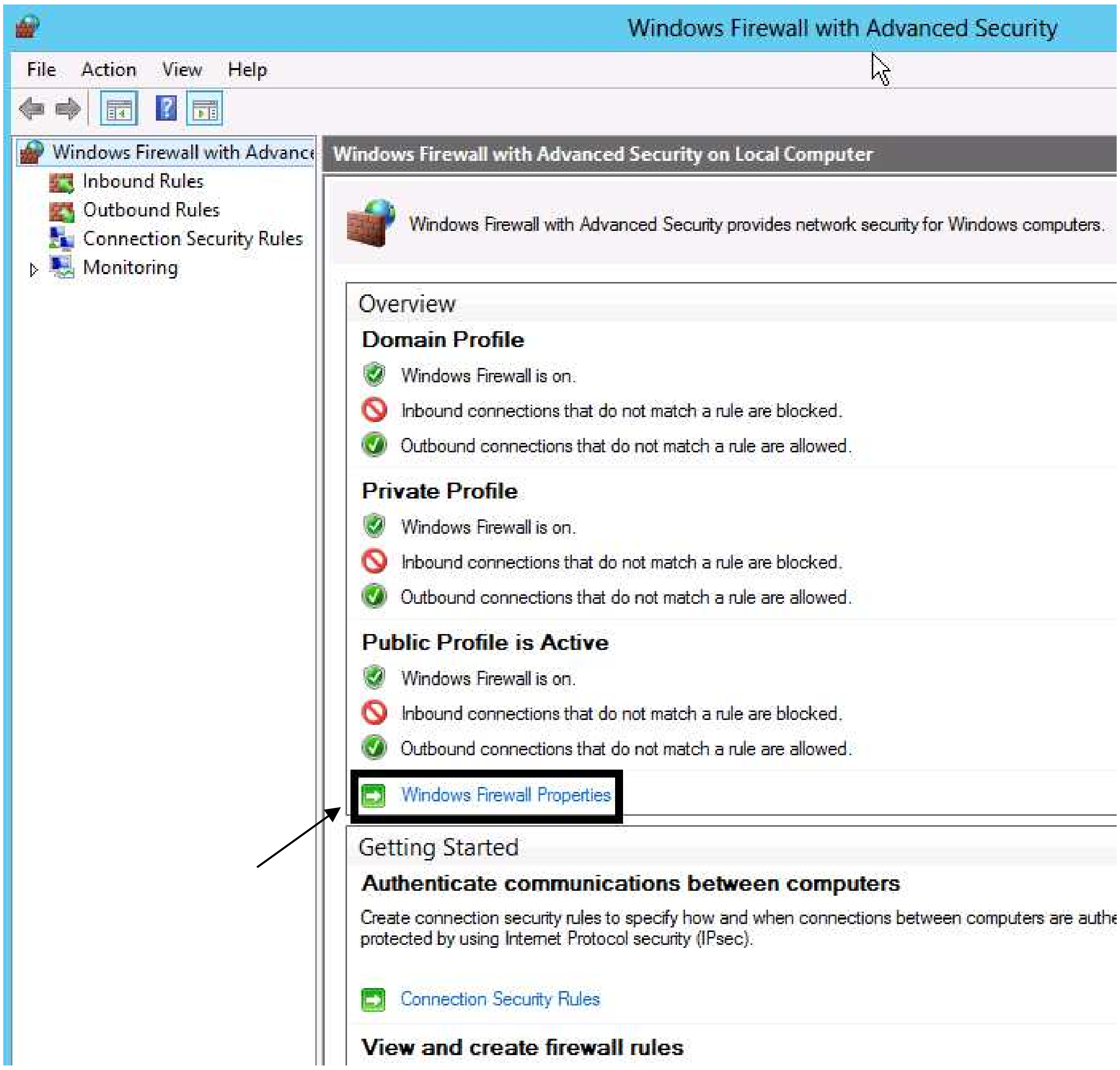
Name	Type	Data
(Default)	REG_SZ	
Dhcpv6DUID	REG_BINARY	00 01 00 01 19 18 b7 77 00 0c 29 b2 4f c2
DisabledCompo...	REG_DWORD	0xffffffff (4294967295)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters

Disable Windows Firewall

1. Open up Windows Firewall with Advanced Security by moving your mouse over the bottom-right or top-right corner of the screen. Click on the Search button (Magnifying glass), type **Firewall** and press **Enter**.

2. In the middle of the screen you will find an "**Overview**" section, at the bottom of this section click **Windows Firewall Properties**.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

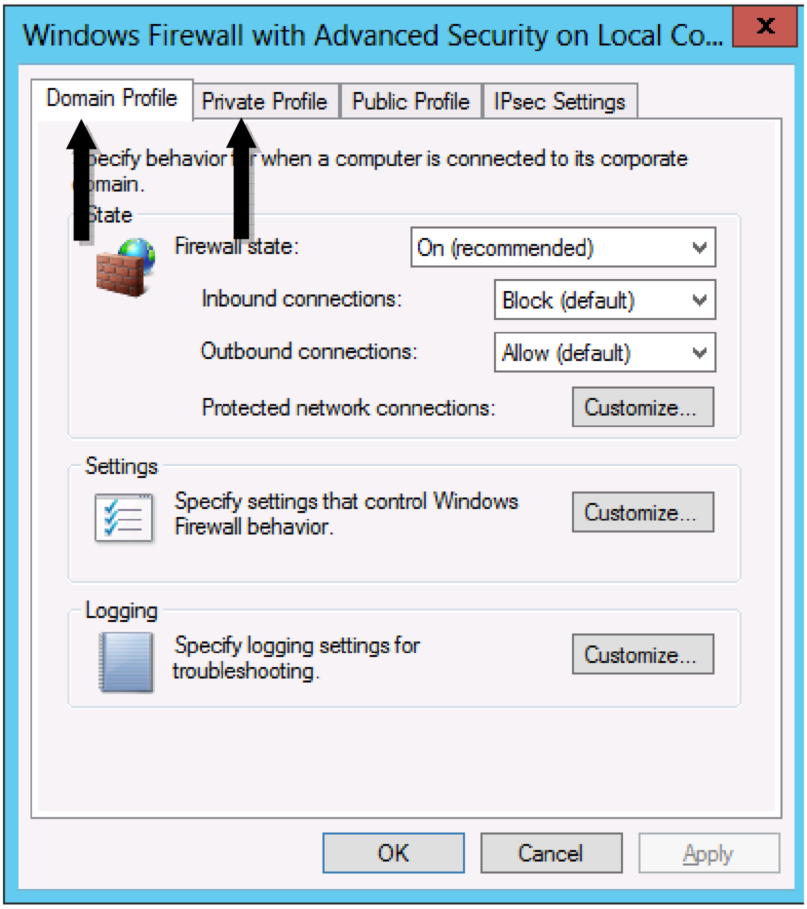
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authe protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

3. Turn off the Firewall state for **Doman** Profile and **Private** Profile.



Windows Firewall with Advanced Security on Local Co...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

*****It is highly recommended that the Firewall be enabled on DIS Router if you are not using a third-party firewall. If you do not have any firewall appliance, you may wish to leave the windows firewall enabled. Adjust the scopes of the Inbound/Outbound rules to meet application requirements***.

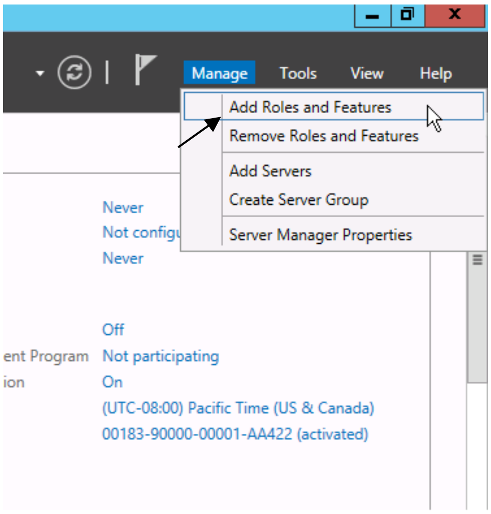
DOMAIN SERVICES AND ACTIVE DIRECTORY SETUP

*****Before starting this section, make sure that your server has a statically assigned IP address and that the DNS IP Address in the TCP/IP settings are pointing to itself.***

We do not have to pre-install the DNS Server Role or pre-create our DNS Zone. When the Active Directory Domain Services Role is installed the DNS Server Role will be automatically installed and configured with the DNS zone specified during the Active Directory installation.

1. Launch **Server Manager**.

2. Click **Manage** and then select **Add Roles and Features**.



Never
Not configu
Never
Off
ent Program Not participating
ion On
(UTC-08:00) Pacific Time (US & Canada)
00183-90000-00001-AA422 (activated)

3. On the **Before You Begin screen**, click **Next**.

4. On the **Select Installation type** screen, select **Role-based or Feature-based installation** and click **Next**.

5. On the **Select Destination server** screen**,** click **Next**.

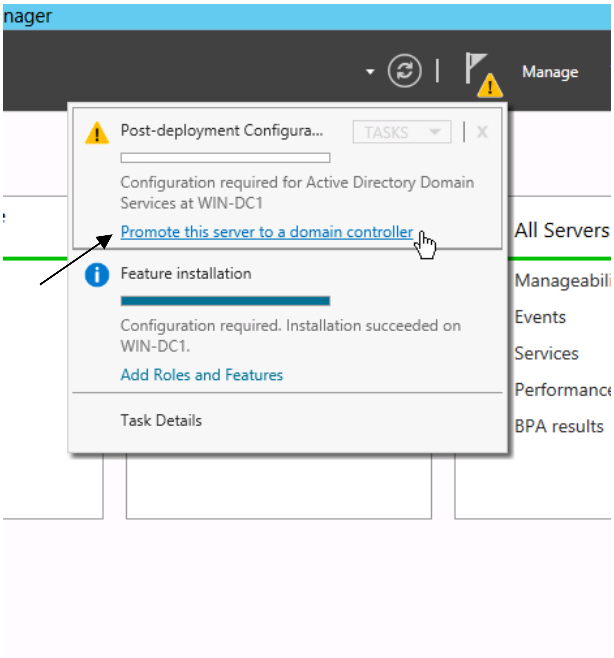
6. Check the box to the left of **Active Directory Domain Services**.

7. On the **Add Roles and Features Wizard** dialogue box, click **Add Features**.

8. Click **Next** for rest of the screens, and then click **Install**.

9. When the installation is finished, click **Close**.

10. Promote the Server to be a Domain Controller by clicking the **Notifications** icon (Flag Icon) and then selecting **Promote this Server** to a Domain Controller.



Post-deployment Configura...

Configuration required for Active Directory Domain Services at WIN-DC1

Promote this server to a domain controller

Feature installation

Configuration required. Installation succeeded on WIN-DC1.

Add Roles and Features

Task Details

11. On the **Deployment Configuration screen**, select **Add a new forest**. Type the DNS name for the new domain in **Root Domain Name** and click **Next**.

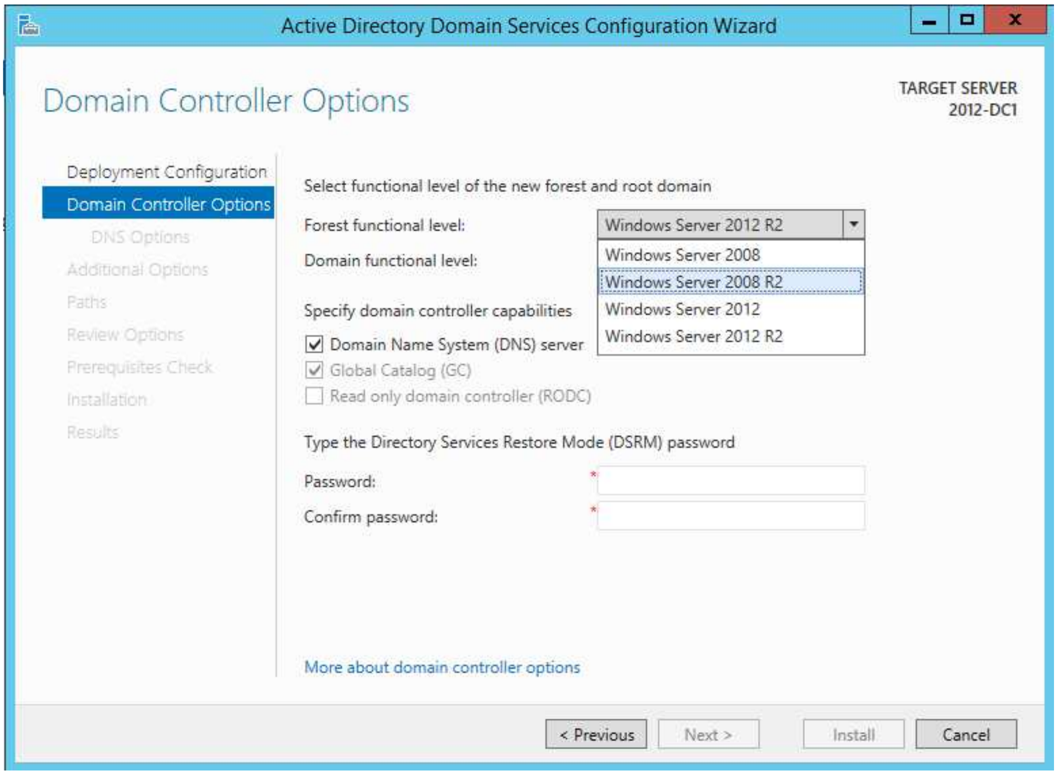
*****DIS recommends you type your abbreviated school district name followed by .local e.g. school.local. DO NOT end your domain name with .com, .net, .org, .edu, or any other domain names that are resolvable on the internet***.

*****This domain name is for INTERNAL resolution only***.

*****This step and those following assume this is the first Domain Controller in a new domain, tree and forest***.

12. For the Forest Functional Level and the Domain Functional Level, select **Windows Server 2012** and click **Next**.

*****If any previous versions of Windows Server Operating (2003 or 2008 R2) are present in the domain or will be introduced as Domain Controllers, select the corresponding Forest and Domain Functional level***.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
2012-DC1

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level:

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: *

Confirm password: *

13. Under **Domain Controller Capabilities**, make sure that **DNS** and **Global Catalog** options are selected.

14. Under **Directory Services Restore Mode (DSRM) Password**, enter in a complex password that is UNIQUE to this server and is **NOT** your administrator password and click **Next**.

15. On the DNS Options screen click **Next**.

    *****Ignore the Parent zone delegation warning on top of the screen. It will be created during initial AD installation.***

16. On the Additional Options screen click **Next**.

17. On the **Location for Database, Log Files and SYSVOL** screen click **Next**.

18. On the **Review Options** screen click **Next**.

19. On the **Prerequisites Check** screen, review warnings and errors if any. Click install to start Domain Controller promotion.

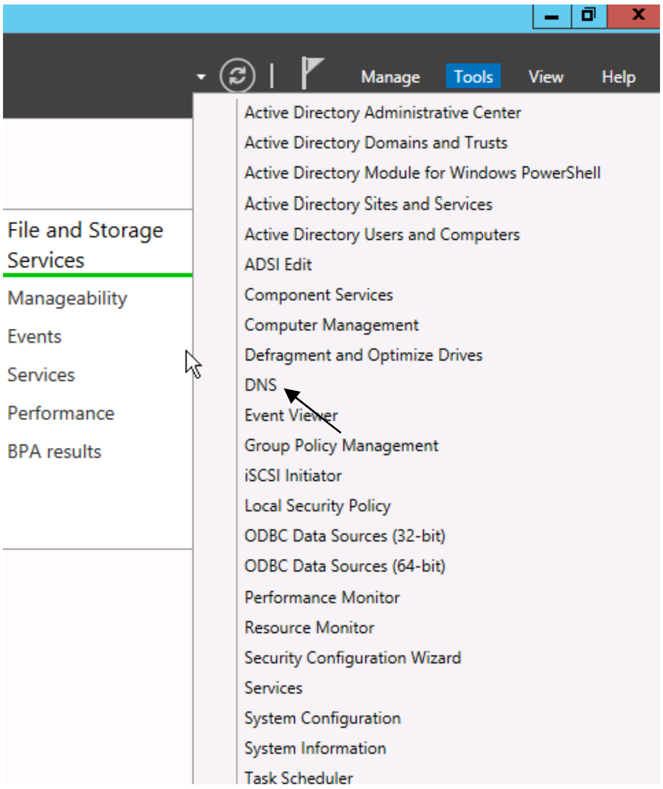
20. When the Active Directory installation finishes, the computer will automatically restart.

Additional DNS Configuration

Reverse Lookup Zones

21. Log into the server when the server has completely booted back up.

22. Launch **Server Manager**, click on **Tools** and select **DNS** from the drop down list.


Manage
Tools
View
Help
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
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

23. Expand your server name, right-click on **Reverse Lookup Zones** and click **New Zone**.

24. On the **Zone Type** screen, take the defaults and click **Next**.

25. For the Active Directory Zone Replication Scope, select **To all DNS Servers running on domain controllers in this domain** and click **Next**.

26. Select **IPv4Reverse Lookup Zone** and click **Next**.

27. For the reverse zone name, enter the first two/three octets of your IP range and click **Next**.

    *****If IP range spans multiple "class C subnets" ONLY enter the first two octets e.g. if the IP range is 10.10.0.0 to 10.10.1.255, then you would only enter 10.10***

28. On the **Dynamic Update** screen, take the default and click **Next**.

29. Click **Finish** to create the new zone.

*****Steps 23 through 26 must be completed for Public and Private IP subnets being used in the Active Directory environment***.

STALE RECORD SCAVENGING

30. Within the DNS Manager, right-click on your DNS server and click **Set Aging/Scavenging for All Zones**.

31. Check the box **Scavenge stale resource records** and then click **OK**.

32. When prompted with the Server Aging/Scavenging Confirmation box, check the **Apply these settings to the existing Active Directory-integrated zones option** and then click **OK.**

*****Steps 30 and 32 must be completed on each DNS server.***

DNS FORWARDERS

By setting the DNS Forwarders to DIS' DNS servers, your server will not have to perform a full DNS resolution of a requested domain name. Rather, it will query the DNS servers at DIS for the specified DNS entry and, if cached, the DIS DNS servers will return the results from its local cache. If the DIS DNS Server does not have the result in its cache, it will perform the full lookup of the DNS Name, and return the results to your DNS server to be delivered to your client.

With Windows Server 2012, should the DIS DNS Servers become unavailable, your DNS server will default to use the DNS Root Hint servers on the Internet for DNS resolution.

33. Within the DNS Manager, right-click your server and click **Properties**.

34. Click the **Forwarders** tab and then click the **Edit** button.

35. Enter your DIS DNS servers as specified below and click **OK**.

36. Click **Apply** and then **OK**.

37. Close the DNS Manager.

DNS Resolvers for Central Arkansas

DNS = 170.94.156.195 (resolver1.state.ar.us)
DNS = 170.94.156.196 (resolver2.state.ar.us)

DNS Resolver for Northwest Arkansas

DNS = 66.204.1.66 (dns4.state.ar.us)

DNS Resolver for South Arkansas

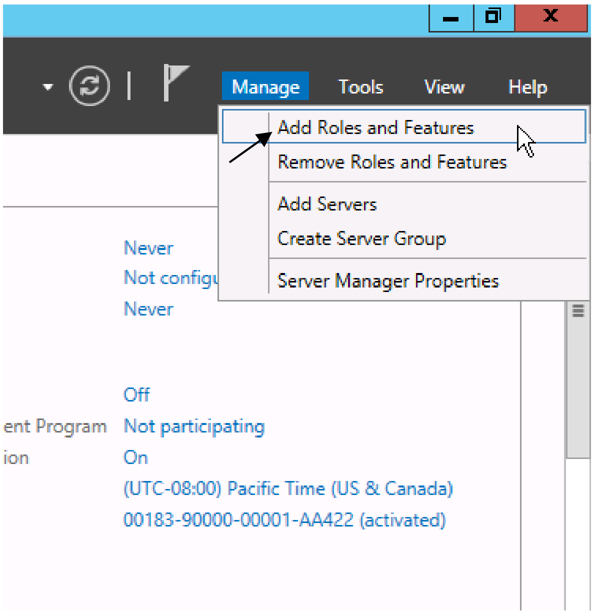
DNS = 66.204.193.26 (dns5.state.ar.us)

List the server in your area as the primary DNS resolver. For redundancy purposes, list an alternate DNS resolver in another part of the state.

DHCP Installation and Configuration

1. Launch **Server Manager.**

2. Click **Manage** and then select **Add Roles and Features**.



3. On the **Before You Begin screen**, click **Next**.

4. On the **Select Installation type** screen, select **Role-based or Feature-based installation** and click **Next**.

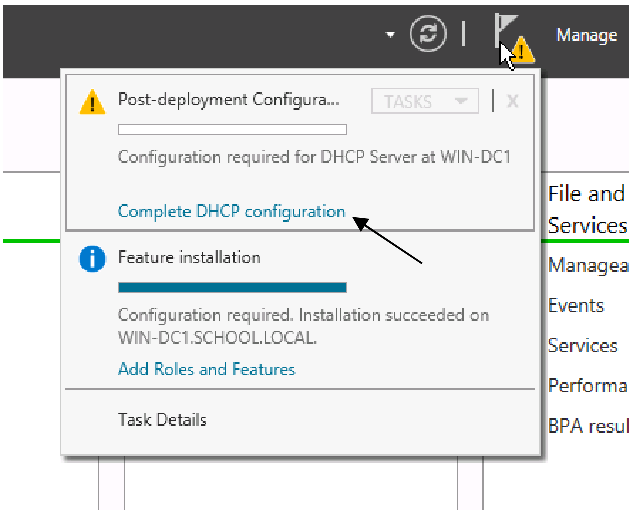
5. On the **Select Destination server** screen**,** click **Next**.

6. On the **Select server roles** screen, select the **DHCP Server** role, click on **Add Features** and click **Next**.

7. Click **Next** for rest of the screens, and then click **Install**.

8. When the installation is finished, click **Close**.

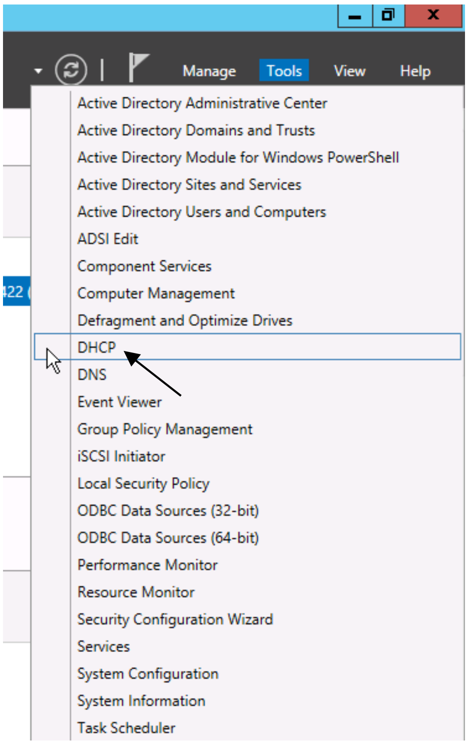
9. Configure the DHCP Server installation by clicking the **Notifications** icon (Flag Icon) and then selecting **Complete DHCP configuration**.


Manage
Post-deployment Configura...
TASKS
Configuration required for DHCP Server at WIN-DC1
Complete DHCP configuration
Feature installation
Configuration required. Installation succeeded on WIN-DC1.SCHOOL.LOCAL.
Add Roles and Features
Task Details
File and Services
Managea
Events
Services
Performa
BPA resul

10. On the **Description** screen click **Next**.

11. On the **Authorization** screen, click **Commit**.

12. Now that DHCP Server role has been installed, we will configure it in DHCP Manager by clicking on **Tools** and selecting **DHCP** from the drop down list.


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management
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

13. Expand the server node and **IPv4** node until you see Server Options, Policies.

14. Right click on **IPv4** and select **New Scope**.

15. On the **Scope Name** screen enter the Scope name and description you want to use for this scope e.g. IP NAT POOL

16. On the **IP Address Range** screen type in the starting and ending IP address for this scope along with the subnet mask. This is the range of IP addresses this DHCP server will be issuing. Click **Next**.

    *****It is recommended to leave a few numbers at the start of the scope for static assignment e.g. if the IP range is 10.10.10.0 - 10.10.11.255 enter 10.10.10.51 for the Starting IP Address and 10.10.11.254 for the Ending IP Address to leave 50 IP's at the beginning of your IP range for static assignment.***

17. On the **Exclusion** screen enter the IP addresses you want to be excluded from the DHCP range defined in the previous step and then click **Next.**

18. On the **Lease time** screen take the default values unless required otherwise and Click **Next.**

19. On the **Configure DHCP options** screen select **No, I will configure these options later** and click **Next** and then **Finish** to close the wizard.

20. Right click **Server Options** and select **Configure Options.** From the list opened select the following options:

    - 003 Router --- Gateway Address for devices
    - 006 DNS Server --- On premises DNS Servers typically DCs
    - 015 DNS Domain Name --- Domain name e.g. school.local
    - 044 WINS/NBNS Server --- On premises WINS Servers
    - 046 WINS/NBT Node Type --- Recommended to be configured as 0x8

21. Right-click **IPv4** and select **Properties**. Under the **Advanced** tab, for **Conflict Detection Attempts**, change this value to **3.**

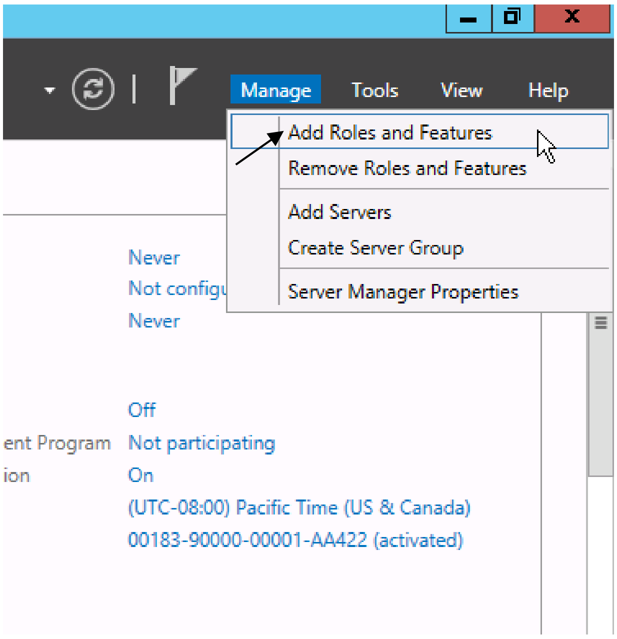
22. Also, under **Advanced** tab click on the **Bindings** button and verify that the only network adapter checked is the adapter that is on the same subnet the DHCP server will be serving IP addresses for.

23. Once all the settings are done, right click on the newly created scope and select **Activate** for the DHCP server to start giving out IP numbers.

WINS Installation and Configuration

1. Launch **Server Manager.**

2. Click **Manage** and then select **Add Roles and Features.**



3. On the **Before You Begin screen**, click **Next.**

4. On the **Select Installation type** screen, select **Role-based or Feature-based installation** and click **Next.**

5. On the **Select Destination server** screen**,** click **Next.**

6. On the **Select server roles** screen, click **Next.**

7. On the Select features screen, select **WINS Server**, click on **Add Features** and then click **Next** and then click **Install.**

8. Add the WINS IP addresses to each respective network cards in all servers.

9. If multiple WINS servers are being deployed, they need to be added as replication partners under WINS manager.

10. Open up **WINS** Manager by selecting **Tools** in the **Server Manager** and then selecting WINS from the drop down list.

11. Expand the respective WINS Server and click on **Replication Partners.**

12. Right-click Replication Partners and select **New Replication Partner.**

13. Enter the respective server name that will be replicating with this WINS server and close WINS manager.

***** Steps 12 and 13 needs to be repeated for all WINS servers in the domain.***

WINDOWS SERVER UPDATE SERVICES (WSUS)

Microsoft Windows Server Update Services (WSUS) enables information technology administrators to deploy latest Microsoft product updates to systems running Microsoft products. By using Windows Server Update Services, you can fully manage the distribution of updates that are released through Microsoft Update to computers in your network.

For Windows Server 2012, WSUS requires the following:

- At least Microsoft Internet Information Services (IIS) 6.0
- At least Microsoft .Net Framework 2.0
- WSUS 4.0 Management Console requires at least Windows 8
- 1GB of free space on system partition.

*****You will want to have a WSUS server at each physical site that is behind a router. The reason is that you do not want to have computers go across the WAN connection to get their updates.***

CONFIGURING WSUS AFTER INSTALLATION

1. Launch Server Manager.

2. Click **Manage** and then select **Add Roles and Features.**

3. On the **Before you begin** page, click **Next.**

4. On the **Select Installation type** screen, select **Role-based or Feature-based installation** and click **Next.**

5. On the **Select Destination server** screen**,** click **Next.**

6. On the **Select Server roles** page, select **Windows Server Update Services.**

7. In the **Add Roles and Features** dialog box that pops up, click **Add Features** and then click **Next**.

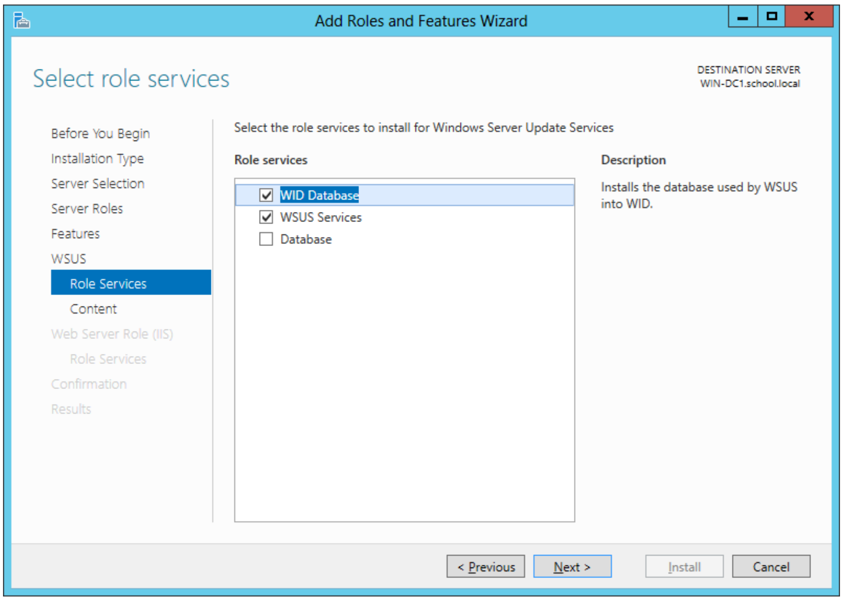
8. On the **Select features** page, leave the default selections, and then click **Next.**

   *****WSUS only requires the default Web Server role configuration. If you are prompted for additional Web Server role configuration while setting up***

WSUS you can safely accept the default values and continue setting up WSUS.

9. On the **Windows Server Update Services** page, click **Next**.

10. On the **Select Role Services** page, leave the default selections unless an external SQL Server database is being used, and then click **Next.**



Select role services

DESTINATION SERVER
WIN-DC1.school.local

Select the role services to install for Windows Server Update Services

Role services

☑ WID Database
☑ WSUS Services
☐ Database

Description

Installs the database used by WSUS into WID.

11. On the **Content location selection** page, type a valid location to store the updates e.g. D:\WSUS and then click **Next**.

*****You must have at least 200GB of free disk space, on the volume selected to store updates locally.***

12. On the **Web Server Role (IIS)** page, click **Next**.

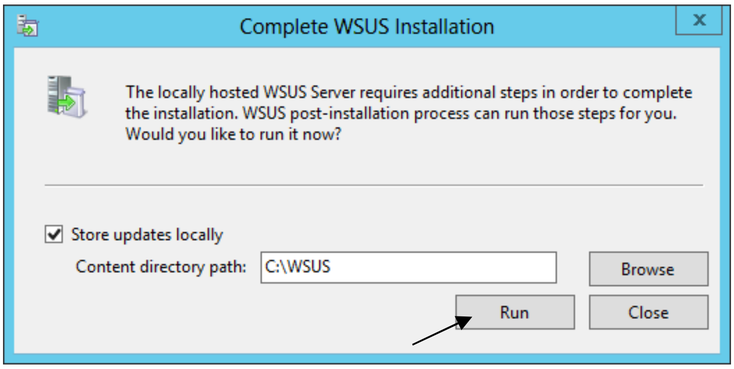
13. On the **Select role services** page, leave the default selections, and then click **Next**.

14. On the **Confirm installation selections** page, review the selected options, and then click **Install**.

15. On the **Installation progress** page, make sure that the installation succeeded, and then click **Close.**

16. Now that WSUS role is installed, it will be configured by clicking on **Tools** and selecting **Windows Server Update Services** from the drop down list.

17. On the **Complete WSUS Installation** dialog box appears, click **Run**.



Complete WSUS Installation

The locally hosted WSUS Server requires additional steps in order to complete the installation. WSUS post-installation process can run those steps for you. Would you like to run it now?

☑ Store updates locally

Content directory path: C:\WSUS

18. In the **Complete WSUS Installation** dialog box, click **Close** when the installation successfully finishes.

19. The Windows Server Update Services Wizard appears and on the **Before you Begin** page, click **Next.**

20. Read the instructions on the **Join the Microsoft Update Improvement Program** page and evaluate if you want to participate or not. If you do not want to participate, **Uncheck** the box and click **Next**.

21. On the **Choose Upstream Server** page, select **Synchronize from Microsoft Update** and click **Next**.

    *****If you are synchronizing from another WSUS server from within the district, be sure to enter the proper port number that WSUS is running on remotely.***

22. On **Specify Proxy Server** settings, leave the default values**,** unless these settings are required for your environment and then click **Next.**

23. On the **Connect to Upstream Server**, click **Start Connecting** to retrieve the current updated list of products available.

24. When the initial product file download is completed, click **Next**.

25. On the **Choose Languages** page, Verify that **English** is the ONLY selected language and then click **Next**.

26. On the **Choose Products** page, choose the Microsoft products running in your environment that will require updates and click **Next**.

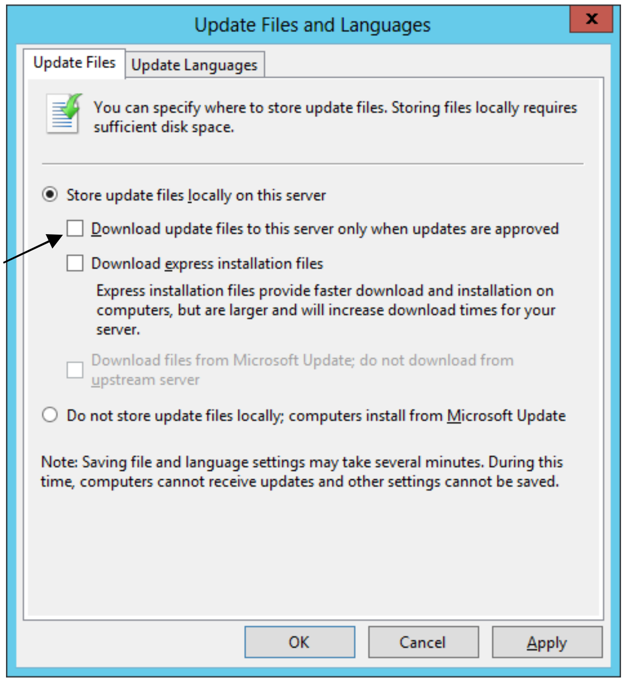
27. On the **Choose Classifications** page, it is recommended to select everything **EXCEPT** Drivers and click **Next**.

28. On the **Set Sync Schedule** page, select **Synchronize automatically** and set this to off-peak usage hours e.g. 11:00pm and then click **Next.**

29. Click **Finish** on the next screen to complete the configuration wizard.

30. On the **Update Services** management console screen, expand your WSUS Server and click **Options**.

31. In the Options pane, select **Update Files and Languages**. Uncheck the **Download update files to this server only when the updates are approved** and click **OK**.



You can specify where to store update files. Storing files locally requires sufficient disk space.

● Store update files locally on this server

□ Download update files to this server only when updates are approved

□ Download express installation files

Express installation files provide faster download and installation on computers, but are larger and will increase download times for your server.

□ Download files from Microsoft Update; do not download from upstream server

○ Do not store update files locally; computers install from Microsoft Update

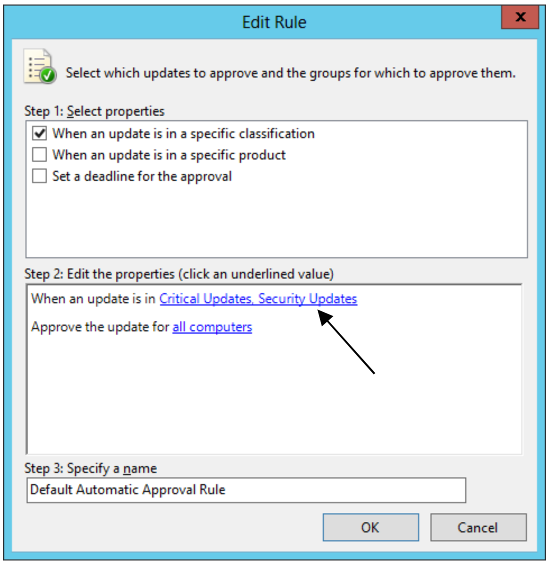
Note: Saving file and language settings may take several minutes. During this time, computers cannot receive updates and other settings cannot be saved.

****If you choose to manually approve updates, your workstations will not have to wait until after the next WSUS Sync with Microsoft to get the updates.***

32. In the Options pane, select **Automatic Approvals**.

33. Select the **Default Automatic Approval Rule** and click **Edit**.

34. In the Step 2 box, click on **Critical Updates, Security Updates.**



Edit Rule

Select which updates to approve and the groups for which to approve them.

Step 1: Select properties

☑ When an update is in a specific classification
☐ When an update is in a specific product
☐ Set a deadline for the approval

Step 2: Edit the properties (click an underlined value)

When an update is in Critical Updates, Security Updates

Approve the update for all computers

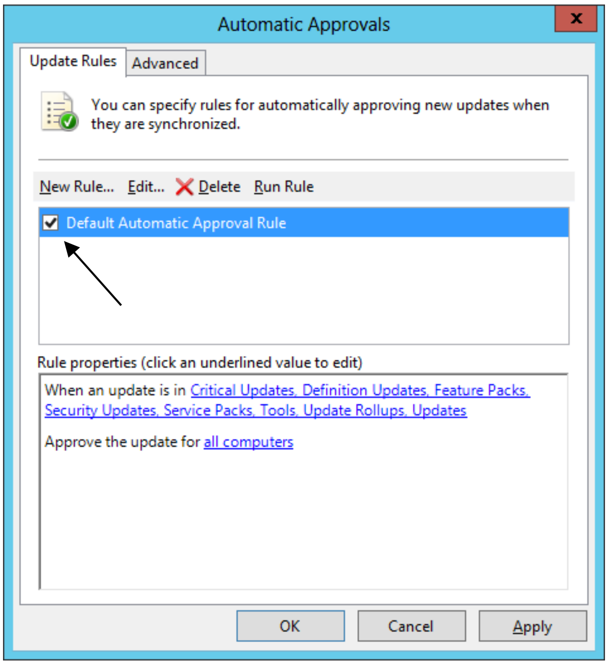
Step 3: Specify a name

Default Automatic Approval Rule

35. Select all classification items **EXCEPT** drivers and click **OK**.

*****Some districts choose not to select Feature Packs. These include items such as Silver Light and Desktop Search.***

36. Verify that **Default Automatic Approval Rule** is checked. Click **Apply** and **OK**.



Automatic Approvals

You can specify rules for automatically approving new updates when they are synchronized.

☑ Default Automatic Approval Rule

Rule properties (click an underlined value to edit)

When an update is in Critical Updates, Definition Updates, Feature Packs, Security Updates, Service Packs, Tools, Update Rollups, Updates

Approve the update for all computers

WSUS Group Policy

1. Launch **Server Manager**.

2. Click on **Tools** and select **Group Policy Management** from the drop down list.

3. Expand Forest: **yourdomain.local.**

4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Group Policy Objects**.

5. Right-click on the **Group Policy Objects** and then select **New**.

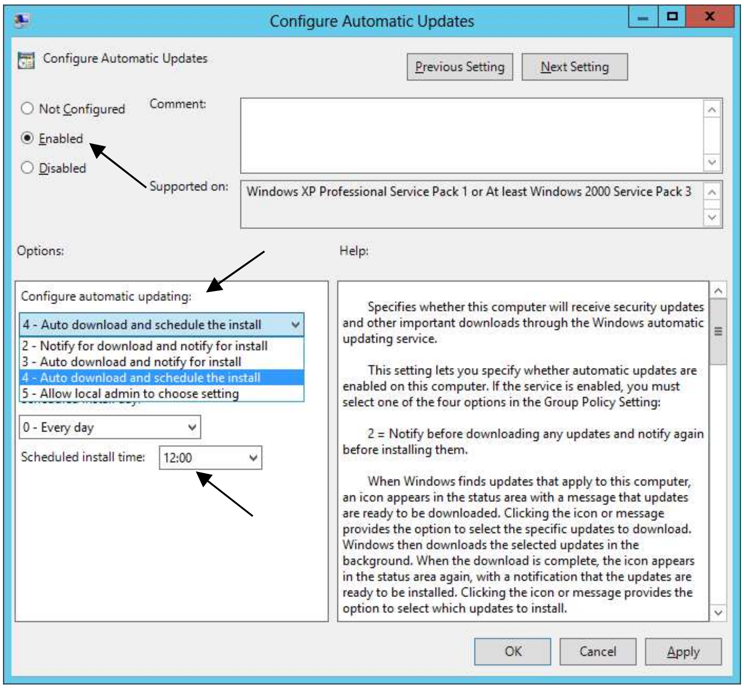
6. Name the new group policy **WSUS Policy** and click **OK**.

7. Expand **Group Policy Objects**. Right-click the newly created W**SUS Policy** and click **Edit** to open the Group Policy Editor.

8. Expand **Computer Configuration > Policies > Administrative Templates** > **Windows Components** and select **Windows Update**.

9. Double-click on **Configure Automatic Updates,** change **Not Configured** to **Enabled** and select option **4 – Auto Download and schedule install** under Configure automatic updating drop-down menu.

10. Set the desired scheduled install day and time.



Configure Automatic Updates

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:

4 - Auto download and schedule the install

2 - Notify for download and notify for install
3 - Auto download and notify for install
4 - Auto download and schedule the install
5 - Allow local admin to choose setting

0 - Every day

Scheduled install time: 12:00

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading any updates and notify again before installing them.

When Windows finds updates that apply to this computer, an icon appears in the status area with a message that updates are ready to be downloaded. Clicking the icon or message provides the option to select the specific updates to download. Windows then downloads the selected updates in the background. When the download is complete, the icon appears in the status area again, with a notification that the updates are ready to be installed. Clicking the icon or message provides the option to select which updates to install.

11. Click the **Next Setting** button to change to **Specify Intranet Microsoft Update Services Location** window.

12. Change **Not Configured** to **Enabled** and in both entry boxes enter **http://YourWsusServername:8530** and then click **OK**.

13. Click the **Next Setting** button to change to **Automatic Updates detection frequency** window.

14. Change **Not Configured** to **Enabled,** leave the default value for **Interval (hours)** and then click **OK.**

15. Double-click on **Allow Automatic Updates immediate installation,** change **Not Configured** to **Enabled** and then click **OK**.

16. Double-click on **No auto-restart for scheduled Automatic Updates installations,** change **Not Configured** to **Enabled** and then click **OK**.

17. Double-click on **Reschedule Automatic Updates Scheduled Installations**.

18. Change **Not Configured** to **Enabled, c**hange the **startup (minutes)** to any value between 1 – 5 (recommended) and then click **OK**.

19. Close the **Group Policy Management Editor.**

20. Drag and Drop **WSUS Policy** on the **Workstations** OU to link the policy to everything residing under **Workstations**.

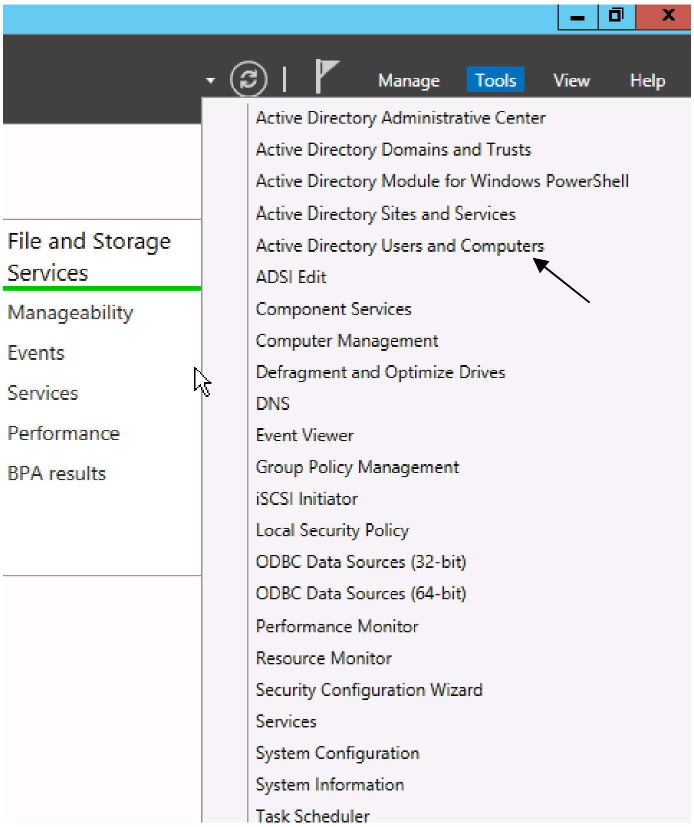
*****It is recommended to have a separate Group Policy for Domain Servers and Domain workstations to avoid automatic restart on servers.***

BASIC ACTIVE DIRECTORY STRUCTURE FOR K12

SINGLE SITE ACTIVE DIRECTORY NETWORKS

1. Launch **Server Manager**.

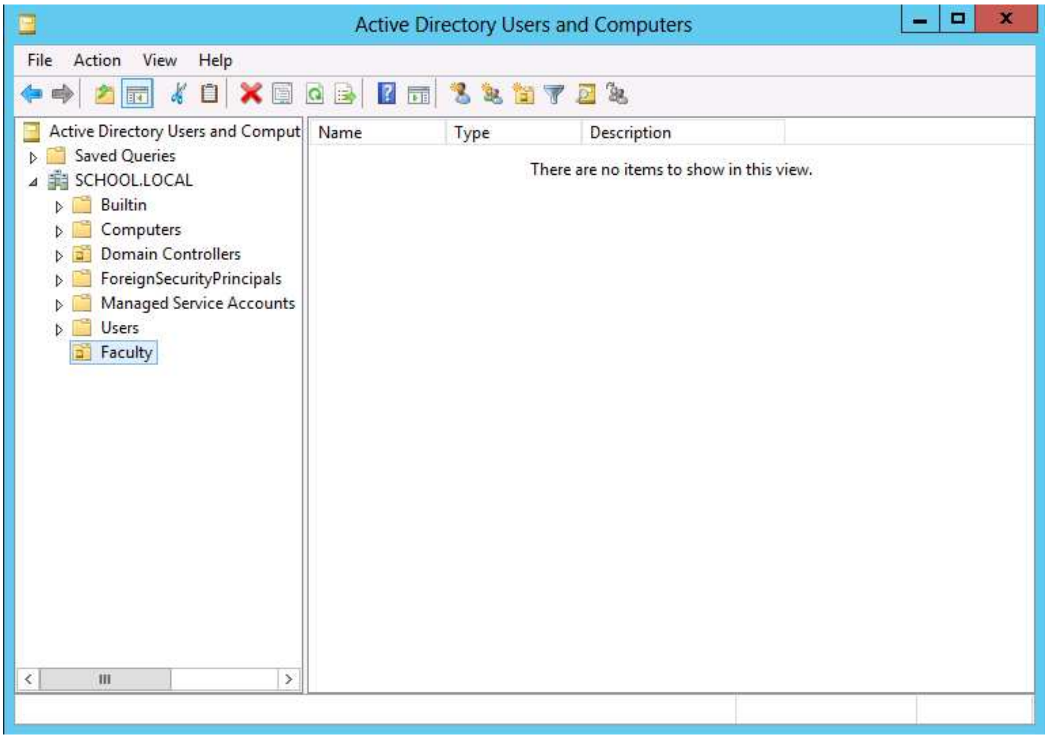
2. Click on **Tools** and select **Active Directory Users and Computers** from the drop down list


Manage
Tools
View
Help
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
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

3. Right-click on **YourDomain.LOCAL**, click **New**, then **Organizational Unit (OU)**.

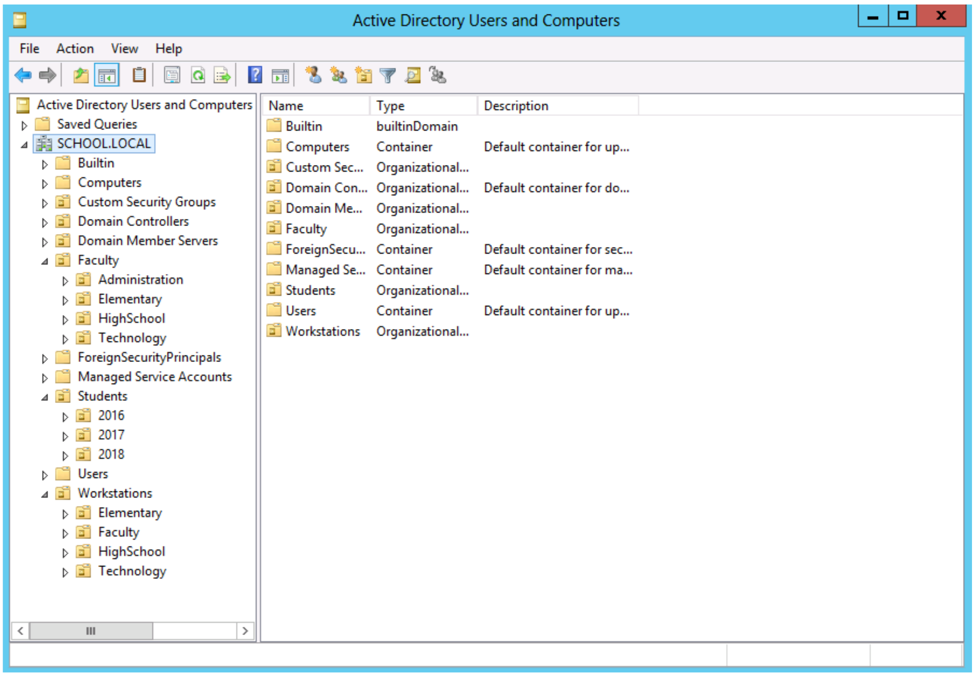
4. Enter **Faculty** as the name of the new Organizational Unit then click **Next**.

   ***** Uncheck the Protect container from accidental deletion box before selecting Next if you do NOT want to automatically protect the OU from being deleted or moved.***



There are no items to show in this view.

***** Repeat Steps 2 and 3 for Organizational Units required in your Active Directory environment e.g. Students, Workstations, Domain Member Servers, and Custom Security Groups.***

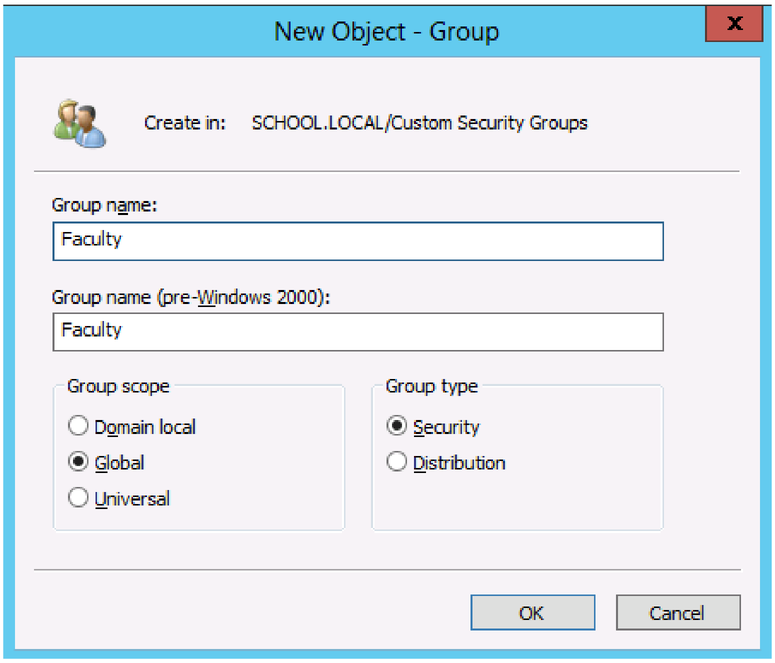


Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Custom Sec...	Organizational...	
Domain Con...	Organizational...	Default container for do...
Domain Me...	Organizational...	
Faculty	Organizational...	
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Students	Organizational...	
Users	Container	Default container for up...
Workstations	Organizational...	

Now that we have our basic OU structure setup, we need to create our security groups. It is best to use security groups to assign permissions rather than assigning permissions to network shares using individual accounts. It is much easier to find where someone is getting incorrect access to something if access to files and shares is based off of security groups.

5. Right-click on the **Custom Security Groups** OU then click **New Group**.

6. Name this group **Faculty** and click **OK**.



Create in: SCHOOL.LOCAL/Custom Security Groups

Group name: Faculty

Group name (pre-Windows 2000): Faculty

Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

****Repeat Steps 4 and 5 for all Custom Security Groups required in your Active Directory environment e.g. Students, Journalism, YearBook, and Technology etc.***

****If you are running Active Directory over multiple sites (behind more than one router), you would want to create an OU for each site, place Workstations, Faculty, and Students OU's under that Site OU. You can delegate campus level technicians to be able to have the authority to maintain user accounts, computer accounts, etc. that reside only in their campus' OU.***

CREATE SHARES AND HOME DIRECTORIES

The first thing we need to do before we can create our user template is to create a network share for the home directories.

1. Open **Computer** and browse to the volume that will hold the faculty home-directories.

   ***It is recommended that Faculty and Student Home folders be stored on individual volumes. Do not place them on the same volume or on the DATA volume*.

2. Create a new folder called **Faculty-Homes**.

3. Right click on the **Faculty-Homes** folder and click **Properties**.

4. Select on the **Sharing** tab and click the **Advanced Sharing** button.

5. Select the **Share this folder** check box.

6. For the share name type **Faculty-Homes$**.

   ***When sharing folders or drives with Windows, if a dollar sign ($) character is added to the end of a share name, the share name does not appear in a browsed list of available shares on the server*.

7. Click on the **Permissions** button.

8. Select **Everyone** and click **Remove**.

9. Click **Add.** In the name box enter **Domain Admins**, **Administrators, Faculty,** and each separated by a semi-colon. Click the **Check Names** button and then click **OK**.

   ***If a name or group is misspelled or not found in the Directory, you will be prompted to correct the spelling or to distinguish the proper group, should the same text exist within multiple groups*.

10. Give **Domain Admins** and **Administrators** both **Full Control**.

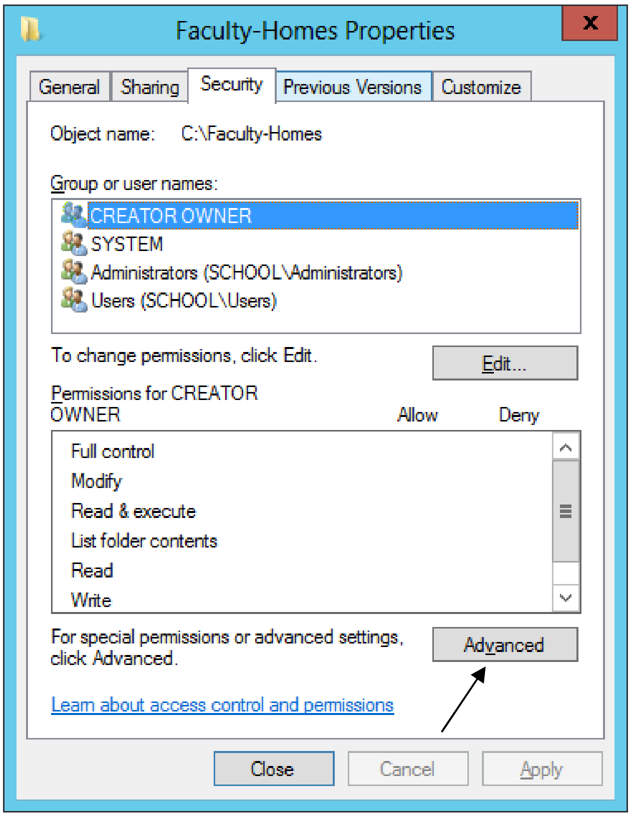
11. Give the **Faculty** group **Change** rights, they will receive Read automatically.

12. Click on the **Caching** button. Select **No files or programs from this shared folder will be available offline**.

*****Unless required, it is NOT recommended to allow offline file-caching for any network shares as these files will be synced at every log off for every user using the share***.

13. Click **OK**, **Apply**, and then **OK** until all property windows are closed.

14. Select the **Security** tab and click the **Advanced** button.



Object name: C:\Faculty-Homes

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SCHOOL\Administrators)
- Users (SCHOOL\Users)

To change permissions, click Edit.

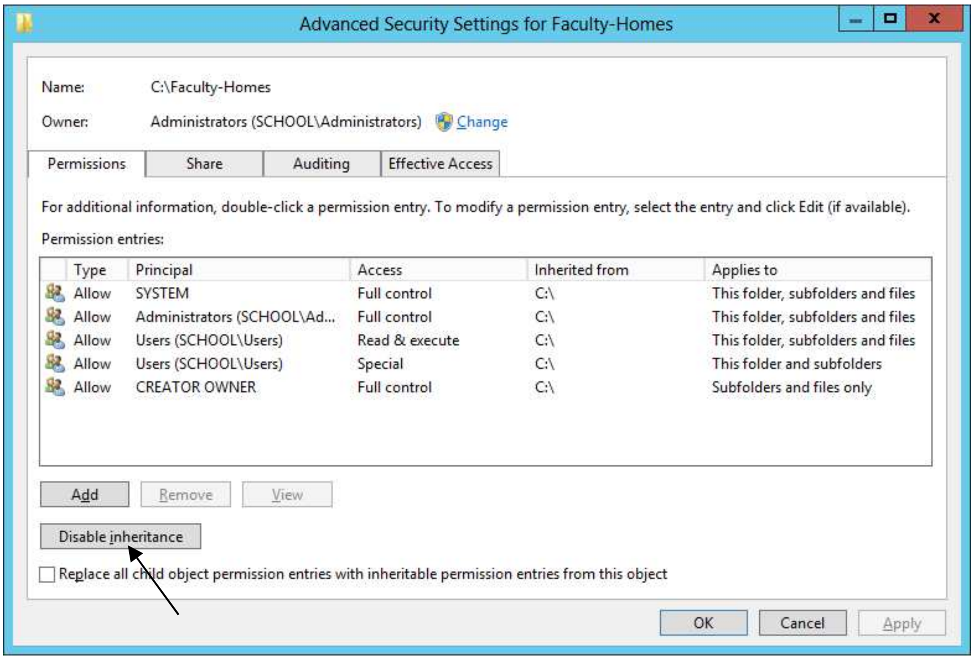
Permissions for CREATOR OWNER

- Full control
- Modify
- Read & execute
- List folder contents
- Read
- Write

For special permissions or advanced settings, click Advanced.

15. On the **Advanced Security Settings** page, click on **Disable inheritance**.

*****By Default all folders created have "Inheritance" turned on which means that the folder inherits its rights from its parent folder. The easiest way to distinguish this is to notice that the Allow or Deny selection boxes will be grayed out for a user or group that is getting rights through inheritance***.



Advanced Security Settings for Faculty-Homes

Name: C:\Faculty-Homes

Owner: Administrators (SCHOOL\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

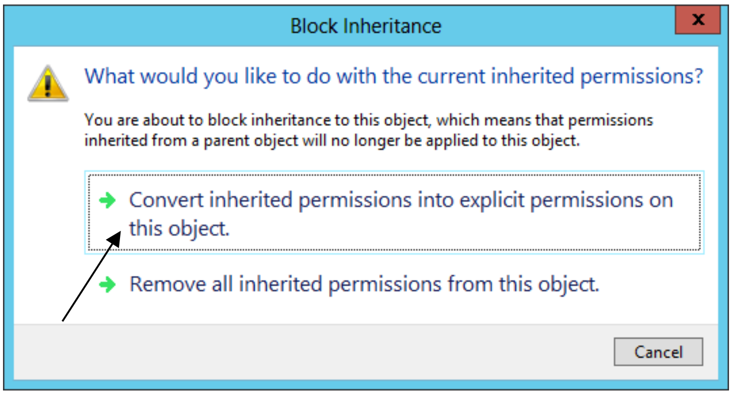
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (SCHOOL\Ad...	Full control	C:\	This folder, subfolders and files
Allow	Users (SCHOOL\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (SCHOOL\Users)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

□ Replace all child object permission entries with inheritable permission entries from this object

16. A dialog box prompting that permission inheritance from the parent folder is being blocked will popup.

17. Select **Convert inherited permissions into explicit permissions on this object**.



Block Inheritance

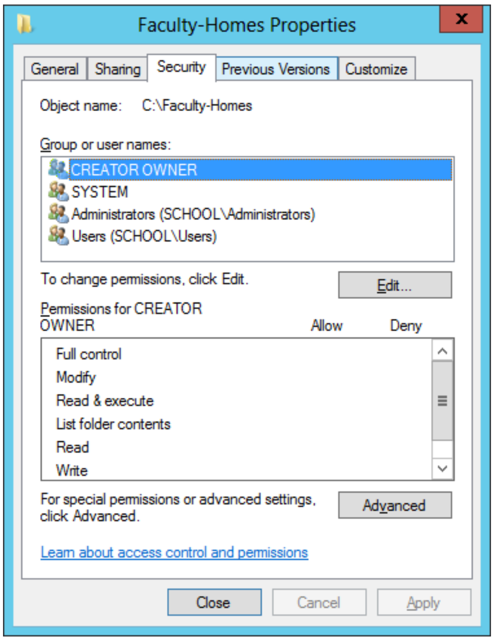
What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

Convert inherited permissions into explicit permissions on this object.
Remove all inherited permissions from this object.
Cancel

18. Click **Apply** and then **OK** to return to the **Faculty-Homes Properties** screen.

19. Your permissions to Faculty-Homes should now look like the following screen.



Object name: C:\Faculty-Homes

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SCHOOL\Administrators)
- Users (SCHOOL\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

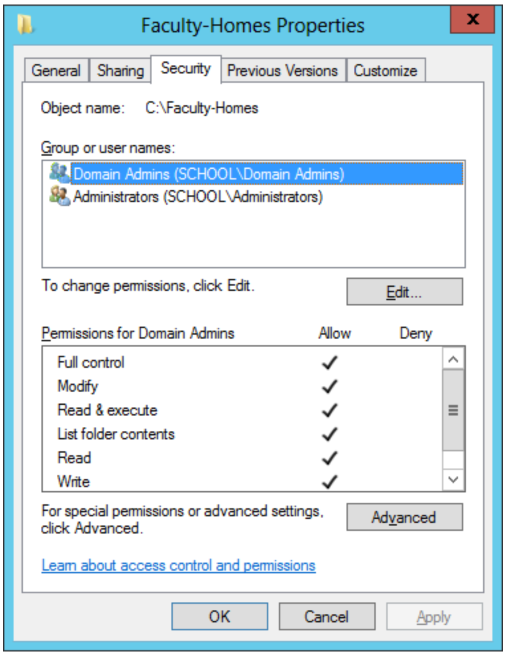
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

20. Click on **Edit** button and remove all Groups from the list except **Administrators** group.

21. Click on **Add**, enter **Domain Admins** and click **OK**.

22. Click on **Domain Admins**, then under **Permissions for Domain Admins** check **Full Control** under **Allow** section. Click **Apply** and **OK**.



Object name: C:\Faculty-Homes

Group or user names:

- Domain Admins (SCHOOL\Domain Admins)
- Administrators (SCHOOL\Administrators)

To change permissions, click Edit.

Permissions for Domain Admins	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

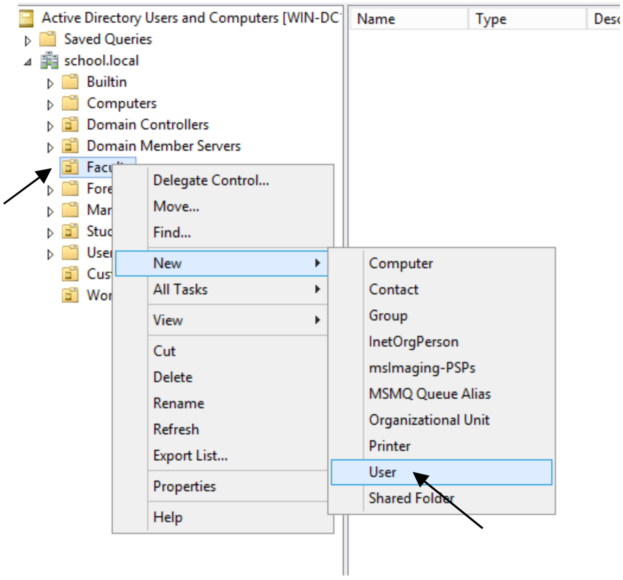
Learn about access control and permissions

Creating User Template

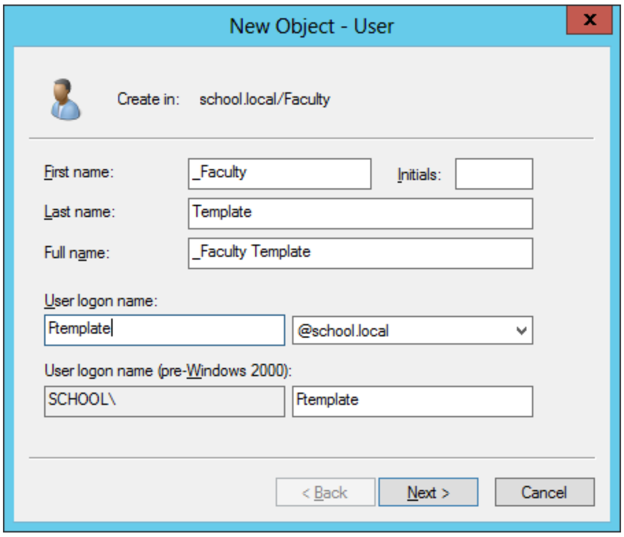
Now that the network share to store home directories is set up, User template will be created using the following steps:

23. Launch **Server Manager**, click on **Tools** and select **Active Directory Users and Computers** from the drop down list.

24. Right click on the **Faculty** OU, select N**ew**, and then **User**.



25. In the information screen fill it out as shown in this screen and then click **Next**.


New Object - User

Create in: school.local/Faculty

First name: _Faculty

Initials:

Last name: Template

Full name: _Faculty Template

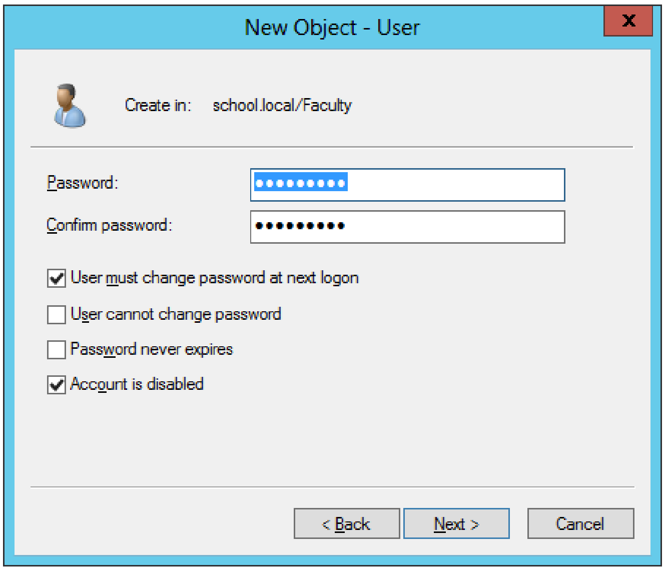
User logon name: Ftemplate @school.local

User logon name (pre-Windows 2000): SCHOOL\ Ftemplate

****An underscore before the first name places the template at top of the list within the Organizational Unit*.

26. Enter a password for the template account that meets the minimum password requirements. Make sure **User much change password at next logon** and **Account is disabled** are checked and click **Next**.

****It is recommended that a template account is ALWAYS disabled after creation*.



New Object - User

Create in: school.local/Faculty

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

☑ Account is disabled

Now that the template account is set up, it needs to be configured for login script, home directory path, and make sure that this template is a member of the required security group(s) by following these steps:

27. Right-click on the **_Faculty Template** account and click **Properties**.

28. Click on the **Member Of** tab and then click on **Add**.

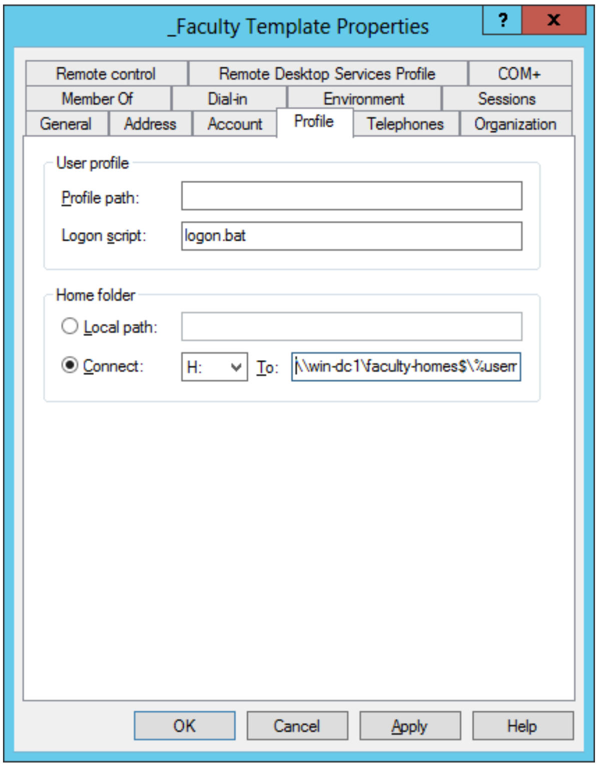
29. In the **Select Groups** box, type **Faculty** and click **Check Names**. Add any additional security group this template needs to be a member of and then click **OK**.

30. Click on the **Profile** tab and in the Logon Script text box, enter **logon.bat**

31. Under the Home folder section, click the radio button next to **Connect**.

32. Select the drive letter to be used for user's home directory when it is mapped.

33. In the **To:** text box enter **\\servername\Faculty-Homes$\%username%**



_Faculty Template Properties

User profile

Profile path:

Logon script: logon.bat

Home folder

○ Local path:

● Connect: H: To: \\win-dc1\faculty-homes$\%usern

34. Click **Apply** and then **OK**.

*****The %username% in the home directory path will automatically change to the login id of the user***.

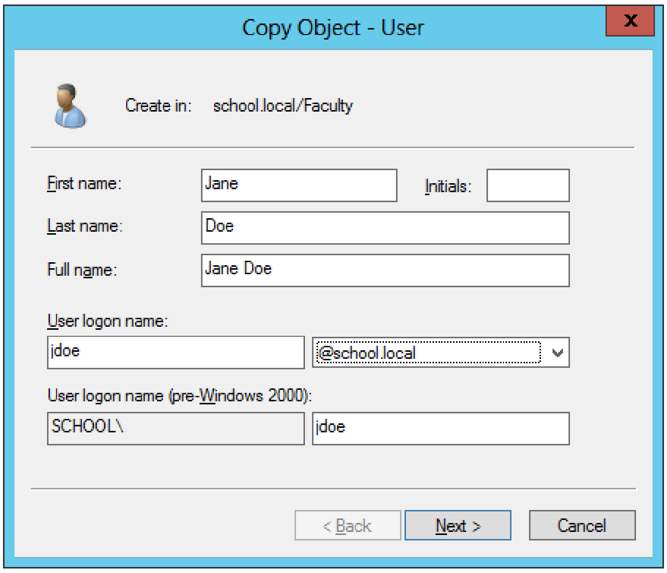
35. This will create a new subfolder called **FTemplate** under **Faculty-Homes** folder with the proper rights.

Creating New User using Template

To create a new account based off the template, use the following steps:

1. Right click on the **_Faculty Template** account and click **Copy**.

2. In the Information screen fill it out the information for the **New User** and then click **Next**.



Copy Object - User

Create in: school.local/Faculty

First name: Jane

Initials:

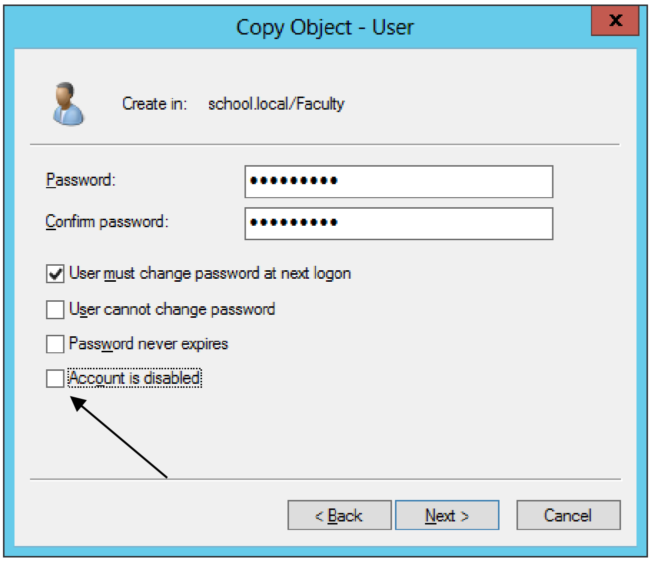
Last name: Doe

Full name: Jane Doe

User logon name: jdoe @school.local

User logon name (pre-Windows 2000): SCHOOL\ jdoe

3. Make sure that the **Account is disabled** box is **Unchecked** when creating a real user account. Click **Next** and then **Finish** to complete the creation.



Copy Object - User

Create in: school.local/Faculty

Password: ••••••••••

Confirm password: ••••••••••

☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Logon Scripts – Batch File Method

By default Windows does not know what shares users need access to or what drive letters they need to be mapped to. By creating a simple batch file logon script, this can be accomplished easily. All logon scripts should be saved in the \\DOMAINNAME\NETLOGON folder.

A batch file is nothing more than a series of DOS commands. The main command in a basic batch file logon script would be the **NET USE** command. For instance, if you have a server named **DC1** and it has a share name of **APPS**, the following command would map this drive as **N:** for the user, when the logon script runs.

```
NET USE N: \\DC1\APPS
```

You can use the REM to remark out anything that you type after the REM. This is helpful for documenting what each command is doing in your logon script. REM Statements **MUST** be on their own line. They are shown on the same line in this example.

A logon script would look similar to the following:

DO NOT ADD THE REM STATEMENTS

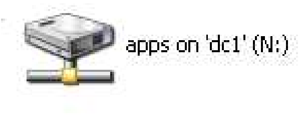
LOGON.BAT

```
@ECHO OFF
NET USE N: /D                          REM Disconnects mapped N drive
NET USE O: /D                          REM Disconnects mapped O drive
NET USE P: /D                          REM Disconnects mapped N drive

NET USE N: \\DC1\Apps        /Persistent:NO          REM Map Apps share on server DC1 to N
NET USE O: \\DC1\Faculty-Apps      /Persistent:NO    REM Map Faculty-Apps share on server DC1 to O
NET USE P: \\DC1\Student-Apps      /Persistent:NO    REM Map Student-Apps share on server DC1 to P

REM Copy All Icon Files in Shared Folder to Users’ Desktop – Overwrite any items that are duplicates.
Xcopy “\\server\sharename\desktopicons\*.*” “%USERPROFILE%\DESKTOP” /C /E /S /Y

REM Start BGInfo
\\%USERDNSDOMAIN%\netlogon\bginfo.exe \\%USERDNSDOMAIN%\netlogon\bginfo-settings.bgi  /timer:0
/accepteula

REM Rename Mapped Drives in My Computer
```

```
Wscript.exe \\%userdnsdomain%\netlogon\rename-mapped-drives.vbs

:END
EXIT
```

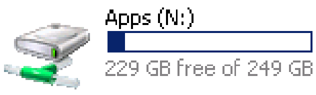
VBScript to rename mapped network drives. Example: In My Computer from “Apps on ‘DC1’ (O:)” to “Apps (O:)”.

Before



apps on 'dc1' (N:)

After



Apps (N:)
229 GB free of 249 GB

Rename-Mapped-Drives.VBS

```
‘------Script Start
On Error Resume Next

Dim UserName

Set oShell = CreateObject("Shell.Application")
Set objNetwork = CreateObject("WScript.NetWork")

Username = objNetwork.UserName
UserName = UCase(Left(UserName,1)) & LCase(Right(UserName,Len(UserName)-1))

mDrive = "M:"
oShell.NameSpace(mDrive).Self.Name = Username & " - Home Directory"
mDrive = "N:"
oShell.NameSpace(mDrive).Self.Name = "Apps"
mDrive = "O:"
oShell.NameSpace(mDrive).Self.Name = "Faculty Apps"
mDrive = "P:"
oShell.NameSpace(mDrive).Self.Name = "Student Apps"
mDrive = "W:"
oShell.NameSpace(mDrive).Self.Name = Username & " - Web Space"
mDrive = "Y:"
oShell.NameSpace(mDrive).Self.Name = "Student Home Directories"
mDrive = "Z:"
oShell.NameSpace(mDrive).Self.Name = "Faculty Home Directories"

‘------ Script End
```

As you may notice, there is a section for Windows 9X Clients and a section for NT-based clients. NT-based clients include the Operating Systems Windows NT Workstation 4.0 up to Windows XP, as well as Server 2003.

We placed the following command at the beginning to check and see if what type of OS is on the workstation that the user is logging in with by using the OS variable built into NT based clients.

```
IF “%OS%”==”Windows_NT” GOTO NTClients
```

Some of the other variables that are available are **%LOGONSERVER%**, **%COMPUTERNAME%** and **%USERNAME%**. These commands can be placed in the login script and can also be run from a DOS prompt to check the validity of your syntax.

*****All login scripts need to be placed in the NETLOGON folder \\\\DomainName\\NETLOGON. Anything placed in this folder is replicated to ALL domain controllers.***

IMPLEMENTING SHADOW COPIES

CLIENT USAGE SCENARIOS

Shadow copy usage scenarios for both client and IT administrators are relatively straightforward. Three common scenarios of data loss due to human error are:

- Accidental file deletions.
- Accidental overwrites of a file (for example, forgot to perform 'Save as').
- File corruption.

Shadow Copies of Shared Folders provides an end user-accessible tool that restores documents by accessing point-in-time shadow copies of documents and folders stored on network shares. Local volume recovery support of an end user's computer, for example, is not supported. The network file share must have the Volume Shadow Copy service enabled on a Windows Server 2003-based computer.

Shadow Copies of Shared Folders is transparent to end users when they store files on the network file server. Only when an end user needs to replace a lost or damaged file with a prior version will they activate the client user interface (UI) through Windows Explorer. Shadow Copies of Shared Folders also enables users to see network folder contents at specific points in time.

WHAT SHADOW COPIES OF SHARED FOLDERS CAN DO

Shadow Copies of Shared Folders helps end users:

- Recover files without assistance from the help desk
- Recover files that were not saved using the "Saved as" command.
- Recover files that were corrupted and not recovered with the file recovery capabilities of Windows XP Professional or Microsoft Office XP.

Shadow Copies of Shared Folders creates a safety net for end users by providing an easily and readily available previous version of a file. In this way, Shadow Copies of Shared Folders helps end users to:

- Manage their own files.
- Fix mistakes without rebuilding the file or calling the help desk.
- Save time and money for the business.

IT USAGE SCENARIOS

The most common scenario for recovering lost or corrupted files is a request by the end user to the IT help desk to find an archived version. Assuming that the organization has an archiving system in place, this request usually means a costly and time-intensive search of archived media, which in many instances is a tape back-up.
This situation creates several problems:

- Potential loss of business agility or revenue if the lost document is time- or context-sensitive.
- Increased unproductive time for end user.
- Increased cost to help desk and IT support services.

Shadow Copies of Shared Folders enables end users to view the contents of shared folders as they existed at specific points in time, and recover those files by themselves. This eliminates administrators having to restore accidentally deleted or overwritten files. Implementing Shadow Copies of Shared Folders for routine file recovery scenarios can help to:

- Reduce demand on busy administrators; for example, by reducing restore-from-tape requests.

Reduce the cost of recovering single or multiple files. Table 1 below presents a summary of how end users, IT departments, and organizations can benefit by implementing Shadow Copies of Shared Folders.

Table 1: Benefits of Using Shadow Copies of Shared Folders

Benefit	End User	IT Department	Company
Saves lost time by not having to rebuild file	✓	✓	
Empowers users to manage their own files	✓	✓	
Saves critical data and information	✓		✓
Saves money by avoiding data loss			✓
Avoids loss of revenue by retaining critical data			✓
Reduces end users' dependence on IT administrators	✓	✓	

HOW SHADOW COPY WORKS

The shadow copy feature in Windows Server works by making a block-level copy of any changes that have occurred to files since the last shadow copy. Only the changes are copied, not the entire file.

As a result, previous versions of files do not usually take up as much disk space as the current file, although the amount of disk space used for changes can vary, depending on the application that changed the file.
For example, some applications rewrite the entire file when a change is made, but other applications add changes to the existing file. If the entire file is rewritten to disk, then the shadow copy contains the entire file. Therefore, consider the type of applications in your organization, as well as the frequency and number of updates, when you determine how much disk space to allocate for shadow copies.

*****Shadow copies DO NOT eliminate the need to perform regular backups, nor do shadow copies provide protection from media failure. In addition, shadow copies are not permanent. As new shadow copies are taken, old shadow copies are purged when the size of all shadow copies reaches a configurable maximum, or when the number of shadow copies reaches 64, whichever is sooner. Therefore, shadow copies might not be present for as long as end users expect them to be. End user needs and expectations should be considered when shadow copies are configure***

A copy of the Shadow Copy Client can be downloaded for Windows XP or prior operating systems from the following link:

http://www.microsoft.com/en-us/download/details.aspx?id=16220

*****Windows Vista and later have the Shadow copy client installed by default***

Implementing Shadow Copies

1. On the server go to **File manager** and then select **Computer.**

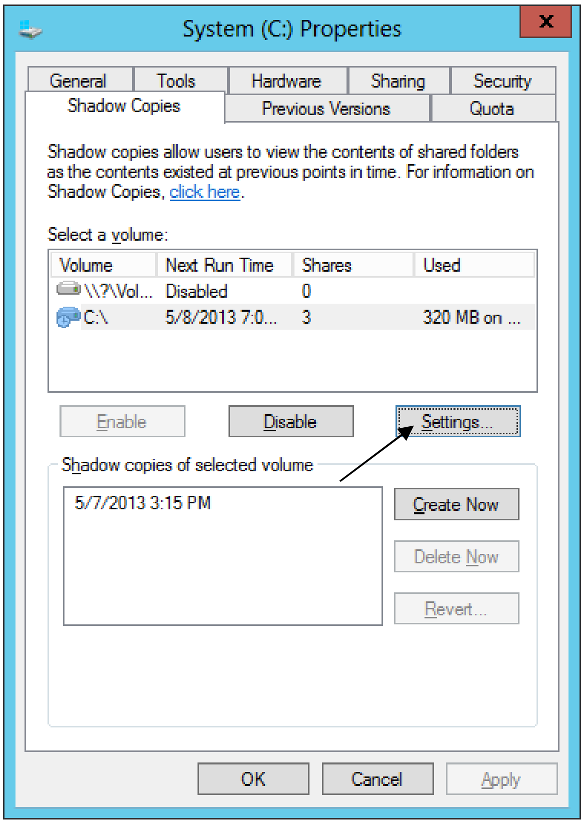
2. **Right-click** on the volume that you would like to enable Shadow Copies and then click **Properties**.

3. Click on the **Shadow Copies** tab.

4. Select the volume(s) from the list shadow copies needs to be enabled on and then click **Enable**.

5. On the Enable Shadow Copies dialog box that pops up check **Do not show this message again** and click **Yes**.

6. Click on the volume that you enabled Shadow Copies for then click the **Settings** button.



Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

Select a volume:

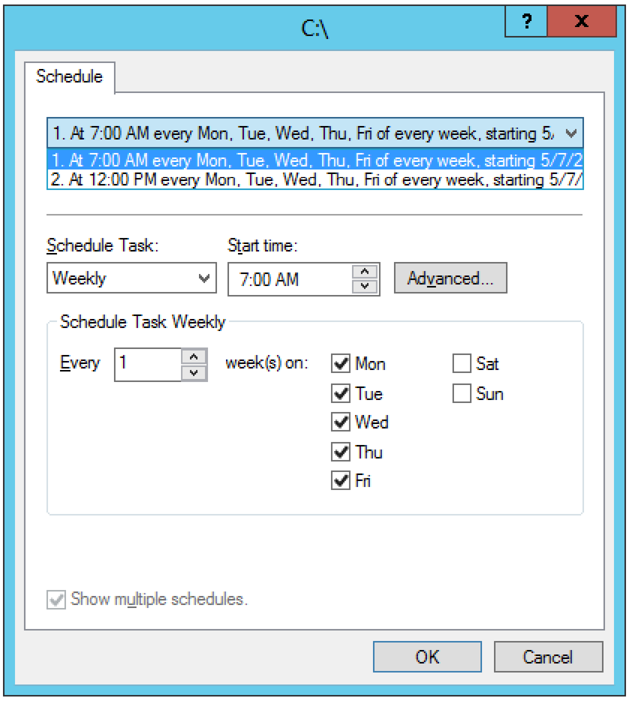
Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	5/8/2013 7:0...	3	320 MB on ...

Shadow copies of selected volume

5/7/2013 3:15 PM

7. Click the **Schedule** button.

8. By default, the only two options for a snapshot are every day at 7AM and 12PM, Mon - Friday. Adjust these schedule to meet the district's needs or create a new schedule per requirement.



1. At 7:00 AM every Mon, Tue, Wed, Thu, Fri of every week, starting 5/7/2
2. At 12:00 PM every Mon, Tue, Wed, Thu, Fri of every week, starting 5/7/

Schedule Task: Weekly

Start time: 7:00 AM

Schedule Task Weekly

Every 1 week(s) on: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

☑ Show multiple schedules.

9. Click **OK** twice to return to the Shadow Copies Settings window.

10. Click **OK** to return to Computer.

Implementing Volume Based Quota Limits

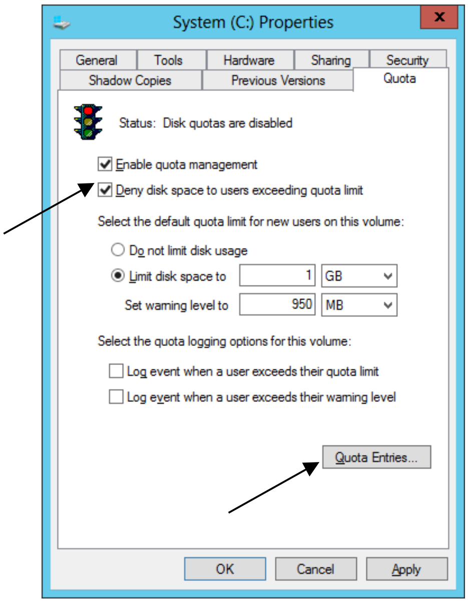
Volume Level Quota Limits using Properties

*****Quota limits are based off of volumes. Quota limits are, when applied, are for all users that save data on the volume. It is recommended that volumes containing Faculty and Student home folders be on separate volumes. This will allow different quota limits on volumes.***

1. On the server go to **File manager** and then select **Computer.**

2. Right click on the volume that Quota limits need to be enabled and then select **Properties** and click on the **Quota** tab.

3. Check the box next to **Enable Quota Management.**



Status: Disk quotas are disabled

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

○ Do not limit disk usage

● Limit disk space to 1 GB

Set warning level to 950 MB

Select the quota logging options for this volume:

□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level

*****It is recommended to enable Deny Disk Space to Users Exceeding Quota Limit.***

4. Select the radio button next to **Limit disk space to**. Set the limit and warning level to meet district's needs. You can set the log options to meet your needs.

5. Click **Apply** and **OK**.

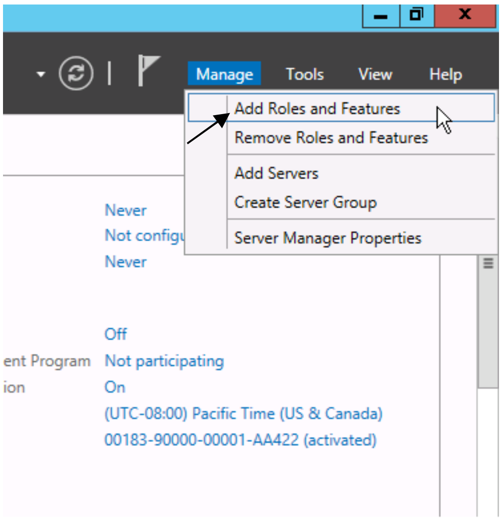
To view user's current disk utilization, click on the Quota Entries button from within the window.

Directory Level Quota Limits using File Server Resource Manager

Install File Server Resource Manager

1. Launch **Server Manager**.

2. Click **Manage** and then select **Add Roles and Features.**



3. On the **Before You Begin screen**, click **Next.**

4. On the **Select Installation type** screen, select **Role-based or Feature-based installation** and click **Next.**

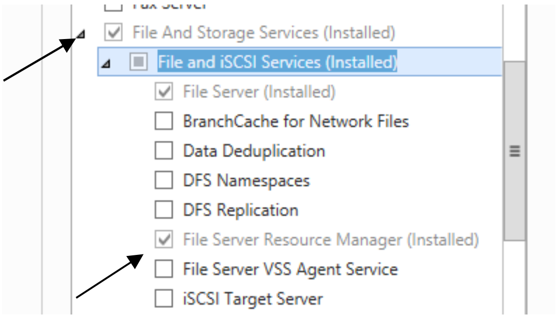
5. On the **Select Destination server** screen**,** click **Next.**

6. On the **Select Server roles** page expand **File and Storage Services** to view the options below.

7. Expand **File and iSCSI Services**, select **File Server Resource Manager.**

8. In the **Add Roles and Features** dialog **box** hat pops up, click **Add Features** and then click **Next**.

9. Click **Next** for rest of the screens, and then click **Install**.



□ Fax Server

☑ File And Storage Services (Installed)

▣ File and iSCSI Services (Installed)

☑ File Server (Installed)

□ BranchCache for Network Files

□ Data Deduplication

□ DFS Namespaces

□ DFS Replication

☑ File Server Resource Manager (Installed)

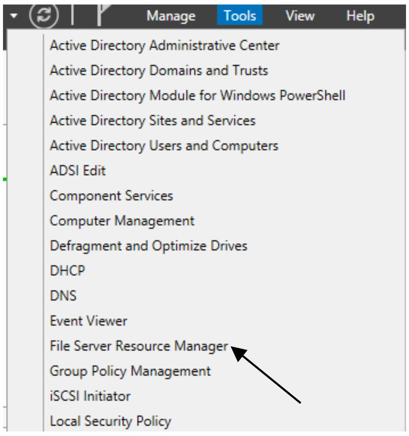
□ File Server VSS Agent Service

□ iSCSI Target Server

10. When the installation is finished, click **Close** and restart the server.

CONFIGURE QUOTA TEMPLATES

11. Now that File Server Resource Manager role is installed, it will be configure by clicking on **Tools** and selecting **File Server Resource Manager** from the drop down list.



Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
File Server Resource Manager
Group Policy Management
iSCSI Initiator
Local Security Policy

12. Expand **Quota Management** in the left-hand pane and click on **Quota Templates**.

13. Under the **Actions** pane (far right) click **Create Quota Template**.

14. Enter a template name, such as **Faculty Home Directory Limits** or **Student Home Directory Limits.**

15. Enter the limit size and select either **Hard quota** or **Soft quota**.

16. Email notifications to either the user or network administrative staff can be enabled by clicking on the **Add** button in the **Notification threshold** section.

17. Click **OK** to save the Quota Template.

Apply Quota Template to Directory

18. Under the Quota Management section of the left pane, click on **Quotas**.

19. Right-click **Quotas** and select **Create Quota**.

20. Click the **Browse** button to select the directory that you wish to apply the quota limit to.

21. Select the following quota type:

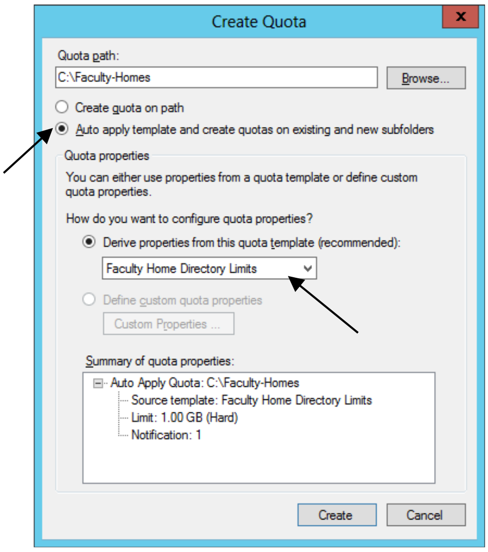
    Create quota on path – This will apply the space limitation to ALL files and folders within the parent directory.

    *****This option should be used for folders such as Yearbook Staff or Multimedia class where multiple users save to the same folder.***

    Auto apply template and create quotas on existing and new subfolders – This will apply the template to the subfolders within the parent folder.

    *****This option should be used for applying limits on home directory folders and is automatically applied to any new folders created. This method would allow you to have your Faculty-Homes and Student-Homes parent folders both on their own volume or you can also place them on the Data volume with the rest of your network shares.***

22. Select the Quota Template to be used from the drop-down menu under **Derive properties from this quota template** and click **Create**.



Create Quota

Quota path:
C:\Faculty-Homes

○ Create quota on path
● Auto apply template and create quotas on existing and new subfolders

Quota properties

You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

● Derive properties from this quota template (recommended):
Faculty Home Directory Limits

○ Define custom quota properties

Summary of quota properties:
- Auto Apply Quota: C:\Faculty-Homes
  - Source template: Faculty Home Directory Limits
  - Limit: 1.00 GB (Hard)
  - Notification: 1

FINE-GRAINED PASSWORD POLICIES (ACT-723)

One of the nice features introduced in Windows Server 2012 AD DS is the ability to configure fine grained password policies through GUI.

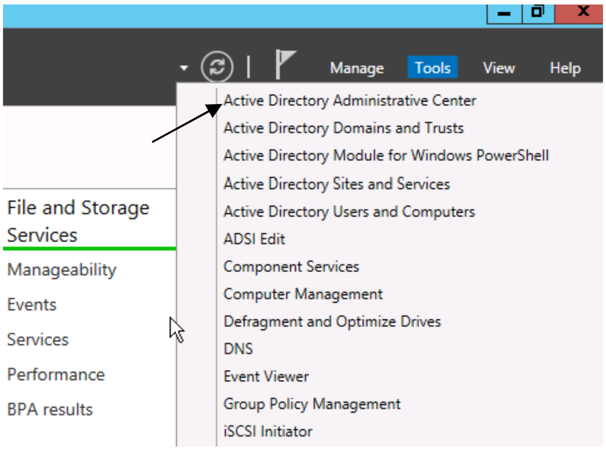
Fine grained password policies allow Network Administrators to configure multiple password policies within a single domain which can be used to apply different restrictions for password and account lockout policies to different sets of users and groups.

Policy Name	Faculty Password Policy	Students Password Policy
Precedence	1	1
Group Name	Faculty/Staff	Students
Minimum Password Length	8	8
Enforce Password History	5 (Recommended)	5 (Recommended)
Minimum Password Age	1	1
Maximum Password Age	90	180

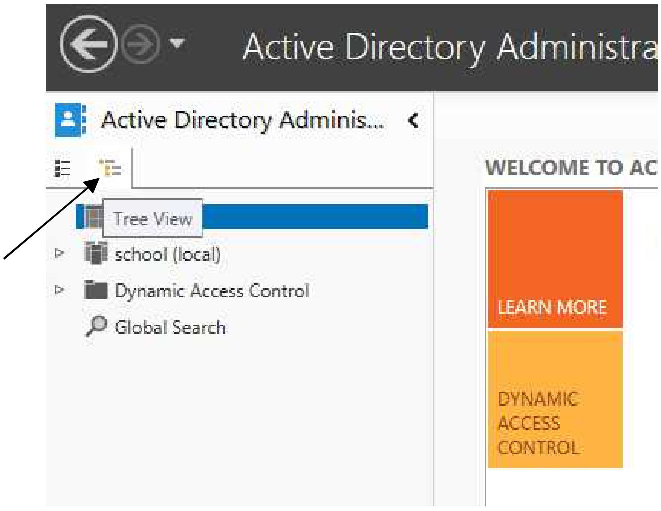
To configure fine-grained password policies as per the table above (ACT723 - K12 State Security Policies), use the following steps:

1. Launch **Server Manager**.

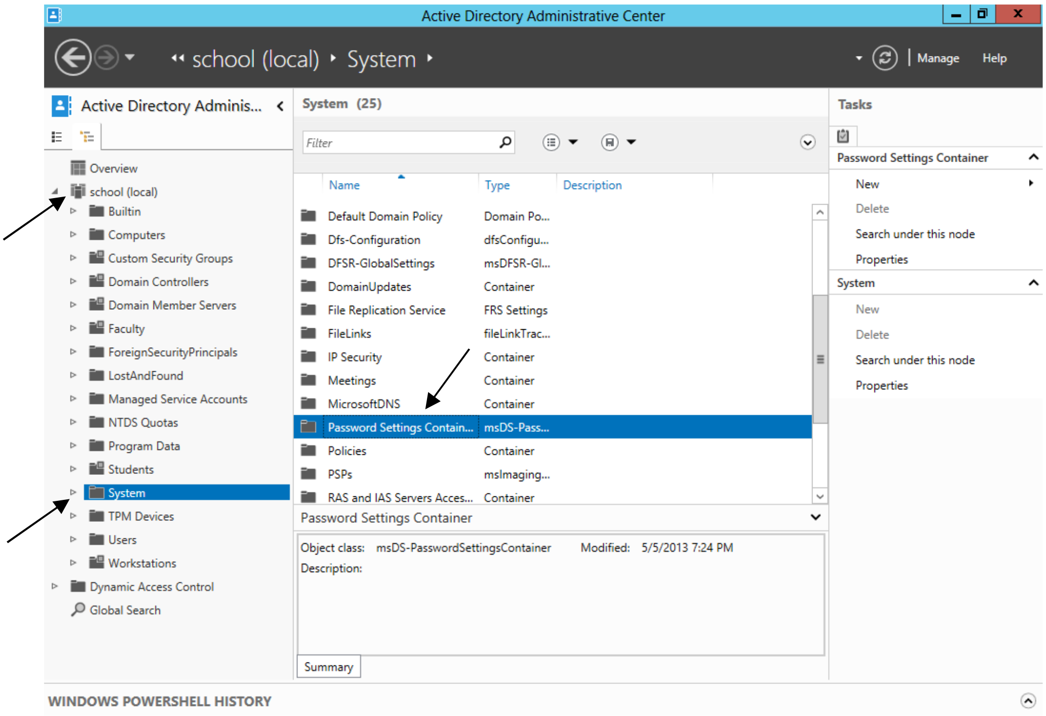
2. Click on **Tools** and select **Active Directory Administrative Center (ADAC)** from the drop down list.


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
File and Storage Services
Manageability
Events
Services
Performance
BPA results

3. When ADAC opens, change the view from List view to Tree View



4. Expand the Domain name and navigate to System and then Password Settings Container.



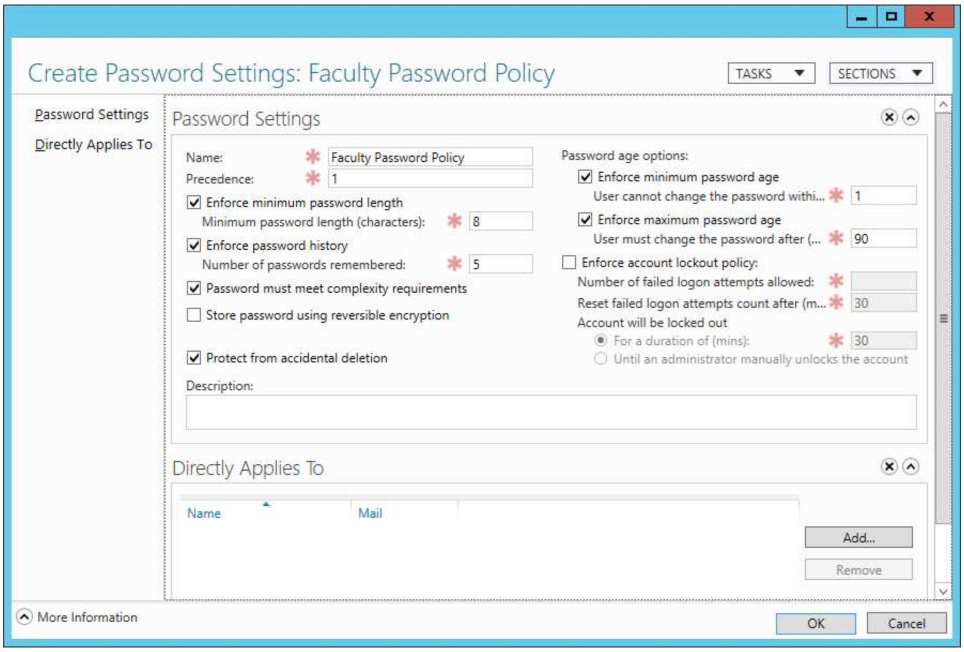
Name	Type	Description
Default Domain Policy	Domain Po...	
Dfs-Configuration	dfsConfigu...	
DFSR-GlobalSettings	msDFSR-Gl...	
DomainUpdates	Container	
File Replication Service	FRS Settings	
FileLinks	fileLinkTrac...	
IP Security	Container	
Meetings	Container	
MicrosoftDNS	Container	
Password Settings Contain...	msDS-Pass...	
Policies	Container	
PSPs	msImaging...	
RAS and IAS Servers Acces...	Container	

Password Settings Container

Object class: msDS-PasswordSettingsContainer Modified: 5/5/2013 7:24 PM
Description:

5. **Right-click on** Password Settings Container, **select** New **and then** Password Settings**.**

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



Create Password Settings: Faculty Password Policy

Password Settings

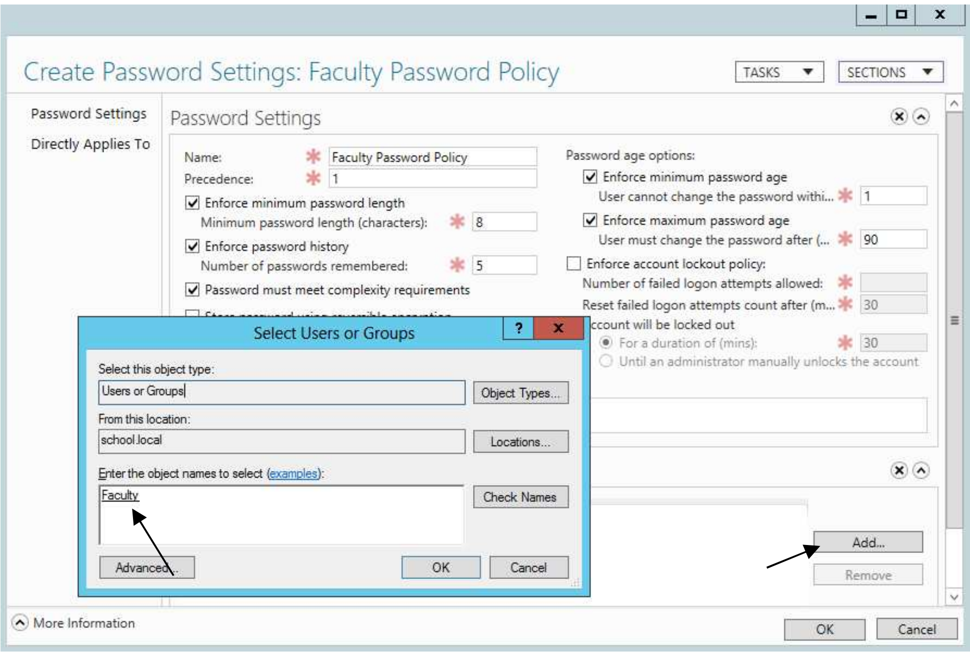
Name: Faculty Password Policy
Precedence: 1
☑ Enforce minimum password length
Minimum password length (characters): 8
☑ Enforce password history
Number of passwords remembered: 5
☑ Password must meet complexity requirements
□ Store password using reversible encryption
☑ Protect from accidental deletion
Description:

Password age options:
☑ Enforce minimum password age
User cannot change the password withi... 1
☑ Enforce maximum password age
User must change the password after (... 90
□ Enforce account lockout policy:
Number of failed logon attempts allowed:
Reset failed logon attempts count after (m... 30
Account will be locked out
● For a duration of (mins): 30
○ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail

7. After the attributes for the password policy has been filled in, click **Add** to link created policy to the required security group and click on **OK** twice.



Create Password Settings: Faculty Password Policy

Select Users or Groups

Select this object type:
Users or Groups
From this location:
school.local
Enter the object names to select (examples):
Faculty

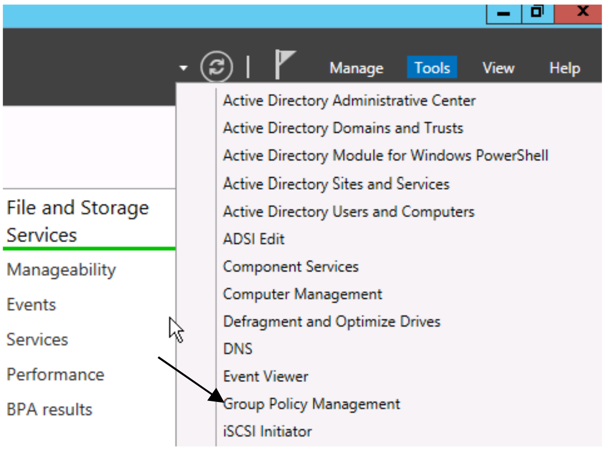
Repeat steps 5 – 7 for Students password policy

Some Common K12 Group Policies

Retain Security Event Log for 90 Days Group Policy

1. Launch **Server Manager**.

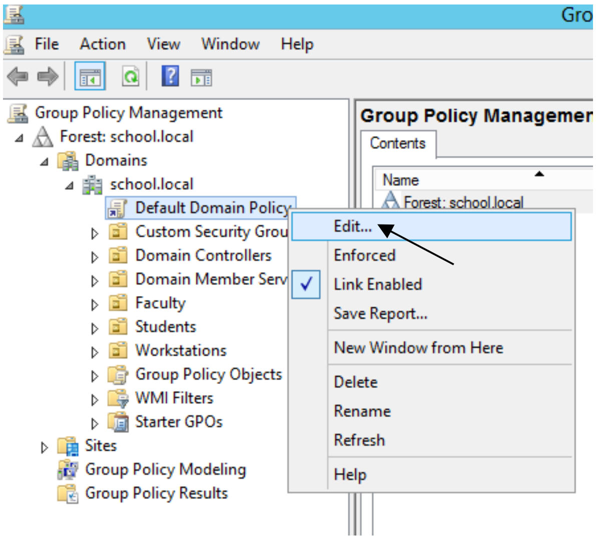
2. Click on **Tools** and select **Group Policy Management** from the drop down list.


Manage
Tools
View
Help
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

3. Expand Forest: **yourdomain.local.**

4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

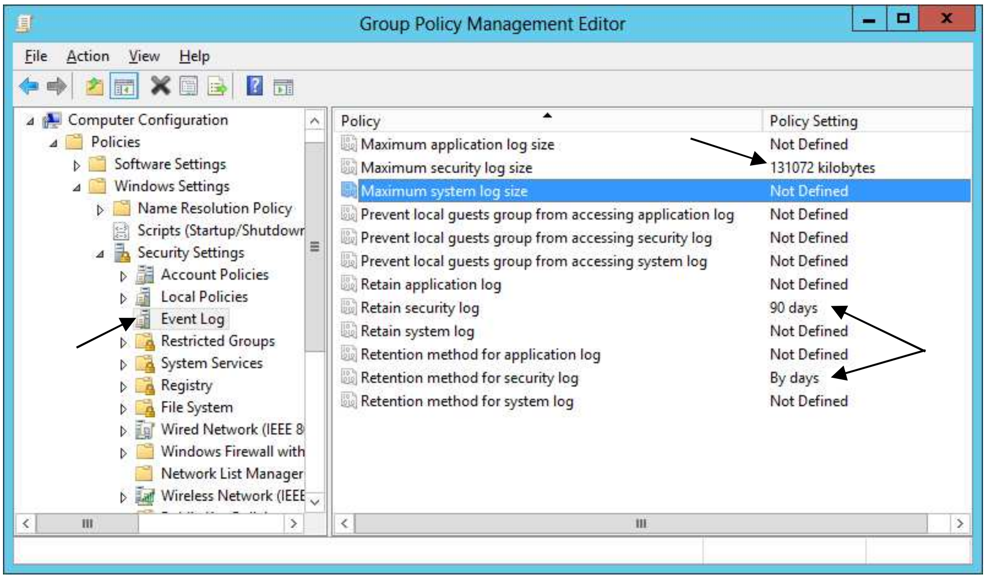
5. Right-click the **Default Domain Policy** and click **Edit**.



6. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** and select **Event Log.**

7. Set the policy setting **Retain Security Log** to **90** days. You will automatically prompted to change the **Retention method to days**. Click **OK.**

8. Set the Maximum Security Log Size to 131072 kilobytes (128MB).



Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	131072 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	90 days
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	By days
Retention method for system log	Not Defined

AUTO-BACKUP AND CLEAR EVENT LOGS (AT LEAST WINDOWS VISTA)

9. Expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Event Log Service** and select **Security**.

10. Enable the **Backup log automatically when full** setting.

11. Close the **Group Policy Management Editor.**

SECURITY EVENT AUDITING – SECURITY EVENT LOG CONTENTS

1. Launch **Server Manager**.

2. Click on **Tools** and select **Group Policy Management** from the drop down list.

3. Expand Forest: **yourdomain.local.**

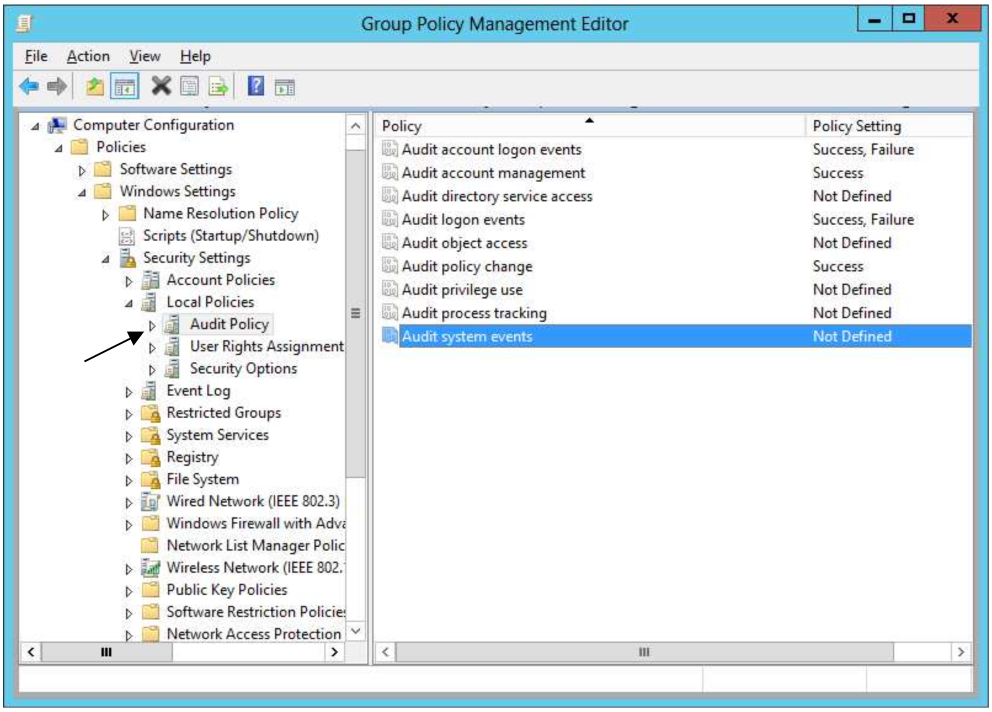
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

5. Right-click the **Default Domain Policy** and click **Edit**.

6. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** and select **Audit Policy.**

7. Enable auditing for the following Policy Settings:

   a. Audit Account Logon Events – (Success AND Failure)
   b. Audit Account Management – (Success)
   c. Audit logon event – (Success AND Failure)
   d. Audit policy change – (Success)



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Success
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

8. Close the **Group Policy Management Editor.**

GROUP POLICY FOR LOGON BANNER

1. Launch **Server Manager**.

2. Click on **Tools** and select **Group Policy Management** from the drop down list.

3. Expand Forest: **yourdomain.local.**

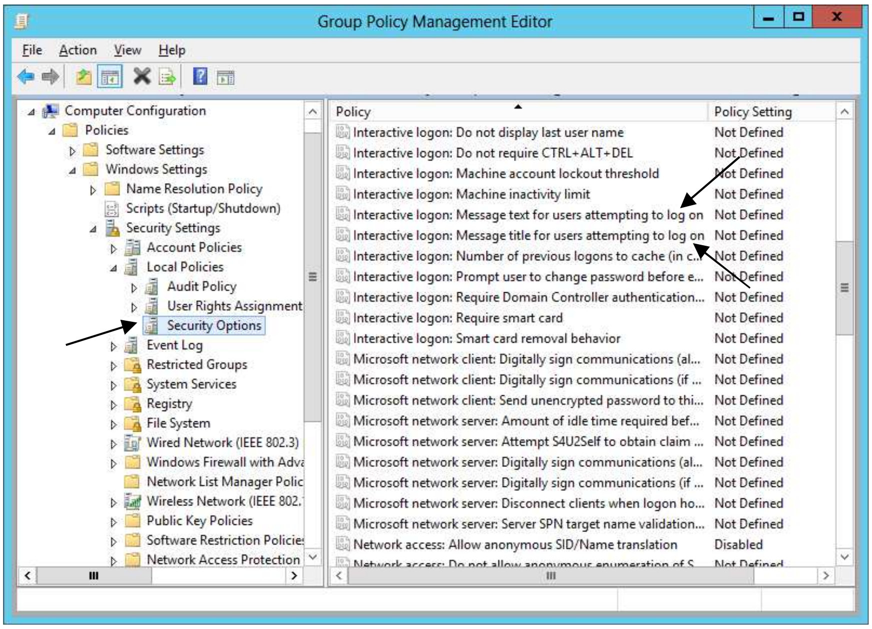
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

5. Right-click the **Default Domain Policy** and click **Edit**.

6. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** and select **Security Options.**

7. Navigate to the following options and Enable them:

   a. Interactive logon: Message text for users attempting to log on.
   b. Interactive logon: Message title for users attempting to log on.



Policy	Policy Setting
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	Not Defined
Interactive logon: Prompt user to change password before e...	Not Defined
Interactive logon: Require Domain Controller authentication...	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (al...	Not Defined
Microsoft network client: Digitally sign communications (if ...	Not Defined
Microsoft network client: Send unencrypted password to thi...	Not Defined
Microsoft network server: Amount of idle time required bef...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Not Defined
Microsoft network server: Digitally sign communications (if ...	Not Defined
Microsoft network server: Disconnect clients when logon ho...	Not Defined
Microsoft network server: Server SPN target name validation...	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of S...	Not Defined

8. Close the Group Policy Management Editor.

Locking Screen Saver Group Policy

1. Launch **Server Manager**.

2. Click on **Tools** and select **Group Policy Management** from the drop down list.

3. Expand Forest: **yourdomain.local.**

4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

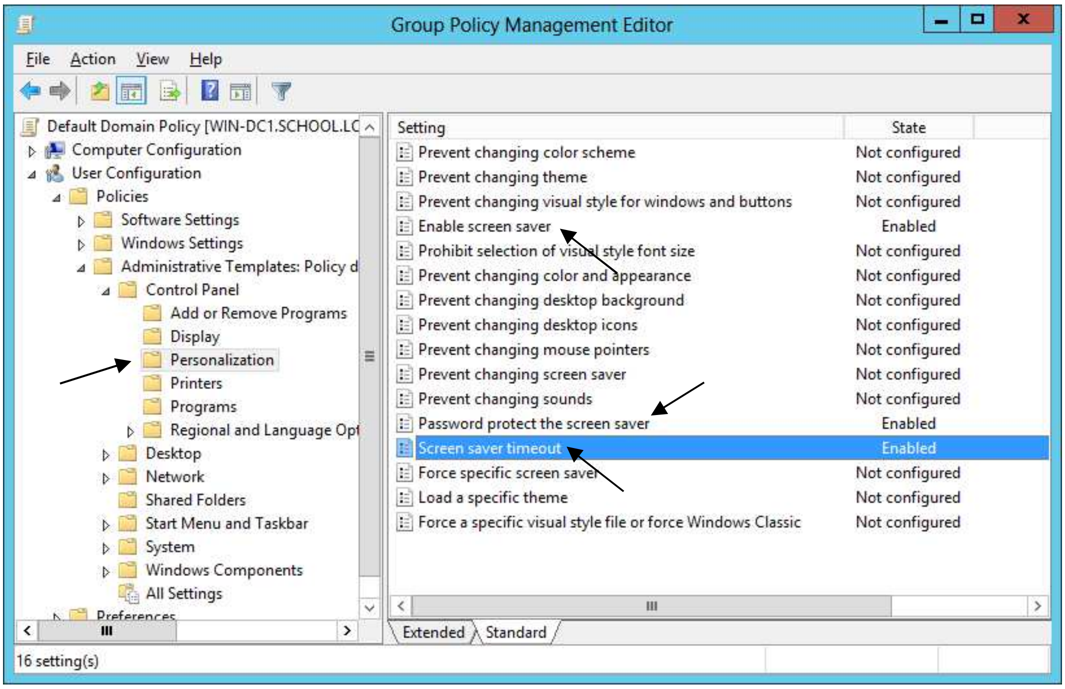
5. Right-click the **Default Domain Policy** and click **Edit**.

6. Expand **User Configuration** > **Policies** > **Administrative Templates** > **Control Panel** and select **Personalization**.

7. Set the **Enable Screen Saver** policy to **Enabled**.

8. Set the **Password Protect the Screen Saver** policy to **Enabled**.

9. Set the **Screen Saver timeout** to **Enabled** and to a recommended time of **900 seconds** (15 minutes).

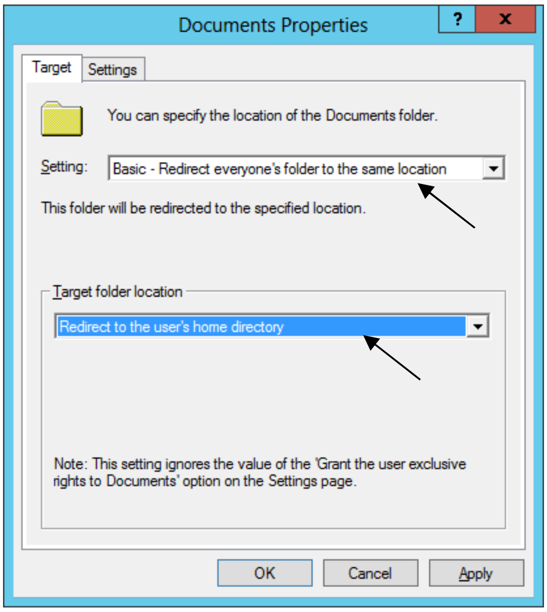


Setting	State
Prevent changing color scheme	Not configured
Prevent changing theme	Not configured
Prevent changing visual style for windows and buttons	Not configured
Enable screen saver	Enabled
Prohibit selection of visual style font size	Not configured
Prevent changing color and appearance	Not configured
Prevent changing desktop background	Not configured
Prevent changing desktop icons	Not configured
Prevent changing mouse pointers	Not configured
Prevent changing screen saver	Not configured
Prevent changing sounds	Not configured
Password protect the screen saver	Enabled
Screen saver timeout	Enabled
Force specific screen saver	Not configured
Load a specific theme	Not configured
Force a specific visual style file or force Windows Classic	Not configured

10. Close the **Group Policy Management Editor.**

Folder Redirection Group Policy

1. Launch **Server Manager**.
2. Click on **Tools** and select **Group Policy Management** from the drop down list.
3. Expand Forest: **yourdomain.local.**
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Group Policy Objects**.
5. Right-click on the **Group Policy Objects** and then select **New**.
6. Name the new group policy **Folder Redirection Policy** and click **OK**.
7. Expand **Group Policy Objects**. Right-click on the newly created **Folder Redirection Policy** and click **Edit** to open the Group Policy Editor.
8. Expand **User Configuration** > **Policies** > **Windows Settings** and select **Folder Redirection.**
9. Right click on **Documents** and click **Properties**.
10. Change the setting to **Basic – Redirect everyone's folder to the same location** and set the **Target folder location** to **Redirect to the user's home directory**.



You can specify the location of the Documents folder.

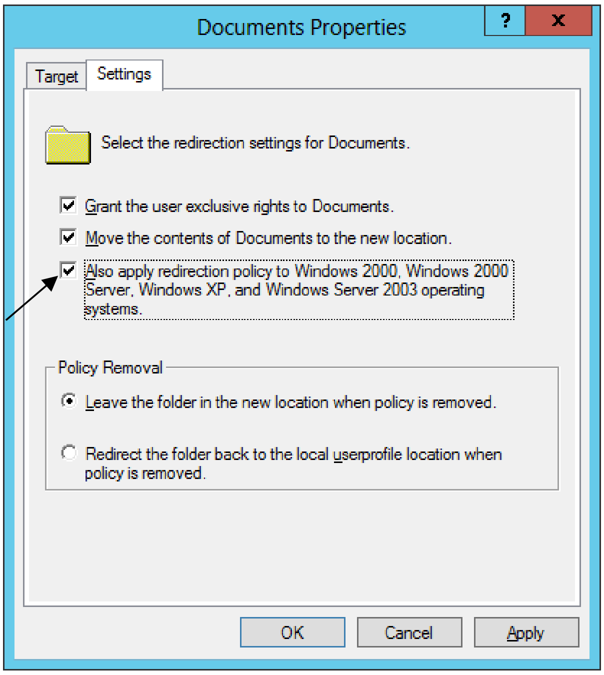
Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location.

Target folder location: Redirect to the user's home directory

Note: This setting ignores the value of the 'Grant the user exclusive rights to Documents' option on the Settings page.

11. Click the **Settings** tab and check the box **Also apply redirection policy to Windows 2000, Windows 2000 Server…**



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

● Leave the folder in the new location when policy is removed.

○ Redirect the folder back to the local userprofile location when policy is removed.

12. Click **Apply** and if prompted to also redirect Pictures, Music, etc. to the Home Directory, click **Yes**. Click **OK**.

13. Close the **Group Policy Management Editor.**

Restrict Computers to Faculty Use Only

This policy can be used to restrict access for students to log on to faculty machines. This policy will be based off of the Faculty User group and can be adjusted to meet the group of users that meets your needs.

1. Launch **Server Manager**.

2. Click on **Tools** and select **Active Directory Users and Computers** from the drop down list.

3. Create a security group called **Faculty Use Only Computers** under **Custom Security Groups** Organization Unit (OU).

4. Under **Server Manager**, click on **Tools** and select **Group Policy Management** from the drop down list.

5. Expand Forest: **yourdomain.local.**

6. Expand **Domains** and then expand **yourdomain.local** and navigate to **Group Policy Objects**.

7. Right-click on the **Group Policy Objects** and then select **New**.

8. Name the new group policy **Faculty Use Only Computers** and click **OK**.

9. Expand **Group Policy Objects** and select the newly created **Faculty Use Only Computers** policy.

10. In the right-hand pane, click on the Scope tab. Under **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.

11. Click the **Add** button, enter the group name **Faculty Use Only Computers** and then click the **OK**.

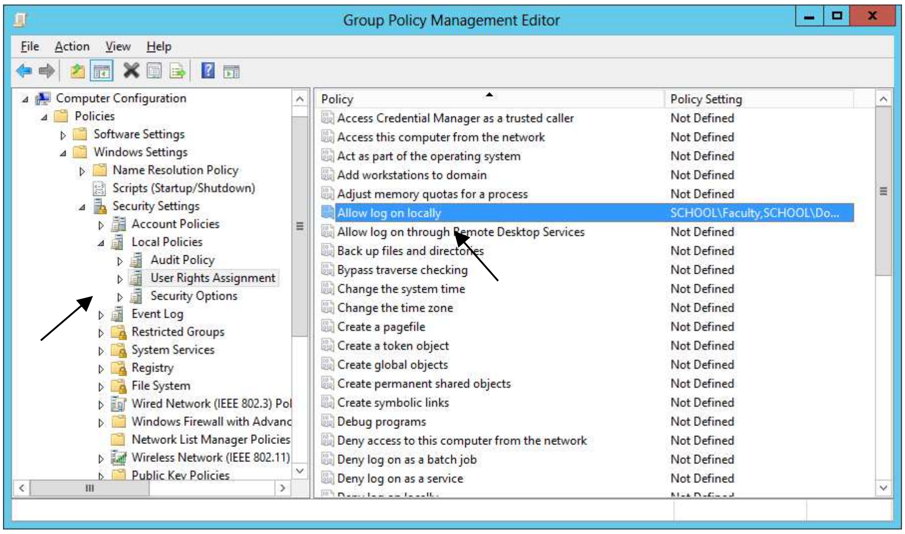
12. Right-click on the newly created **Faculty Use Only Computers** policy and select **Edit**.

13. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies** and select **User Rights Assignment**.

14. In the right-hand window, double-click on **Allow log on locally**.

15. Check the box for **Define these policy settings**.

16. Click the **Add User or Group** button and add **Domain Admins**, **Administrators**, and **Faculty** to the list. Click **Apply** and **OK**.



Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	SCHOOL\Faculty,SCHOOL\Do...
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined

17. Close the **Group Policy Management Editor** and link the policy to Faculty Workstations OU**.**

    *****Once this policy is created and applied, 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.***

REFRESH GROUP POLICY SETTINGS WITH GPUPDATE.EXE

Syntax

Gpupdate [**/target:**{**computer**|**user**}] [**/force**] [**/wait:***value*] [**/logoff**] [**/boot**]

Parameters

/target:{computer|user}

Processes only the *computer* settings or the current *user* settings. By default, both the computer settings and the user settings are processed.

/force

Ignores all processing optimizations and reapplies all settings. The Group Policy engine on the client tracks versions of the GPOs that are applied to the user and computer. By default, if none of the GPO versions change and the list of GPOs remains the same, the Group Policy engine will not reprocess policy. This option overrides this optimization and forces the Group Policy engine to reprocess all policy information.

/wait:value

Number of seconds that policy processing waits to finish. The default is 600 seconds. *0* means "no wait"; *-1* means "wait indefinitely."

/logoff

Logs off after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the user logs on, such as user Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require the user to log off.

/boot

Restarts the computer after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the computer starts up, such as computer Software Installation. This option has no effect if there are no extensions called that require the computer to be restarted.

/?

Displays help at the command prompt.

Examples

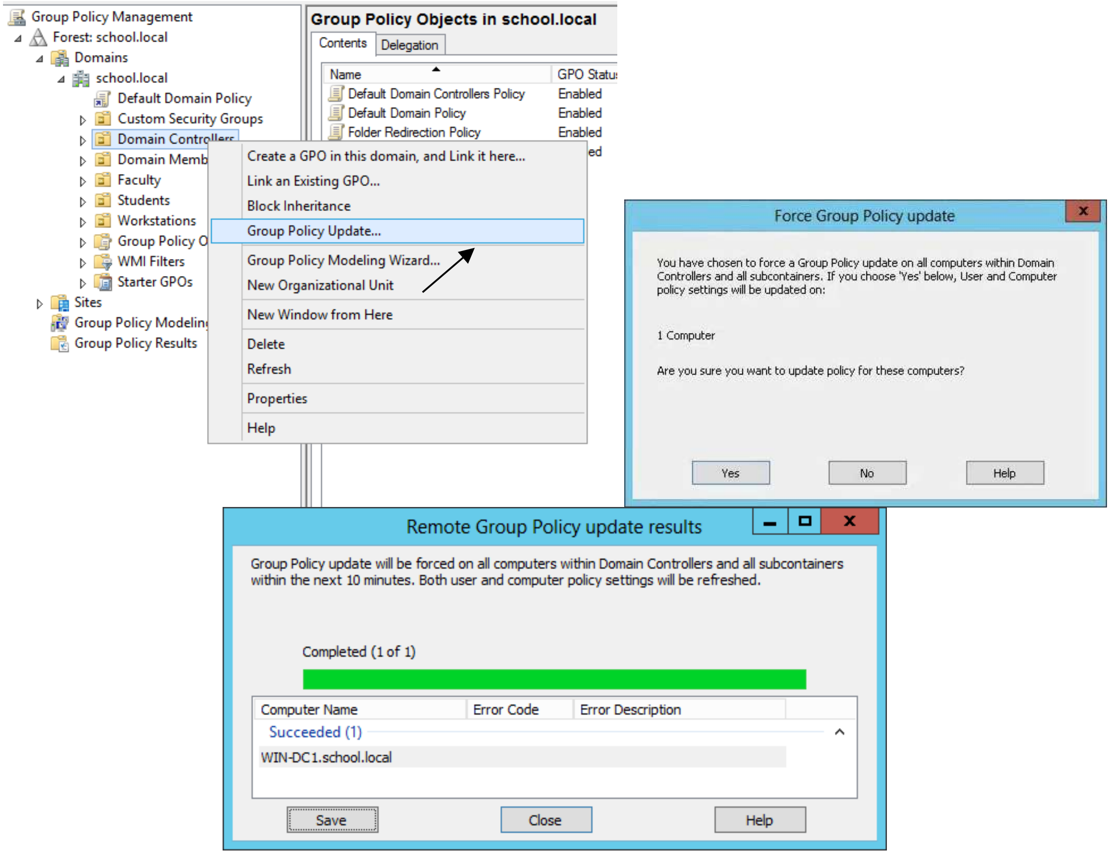
The following examples show how you can use the **gpupdate** command:

- **gpupdate**
- **gpupdate /target:computer**
- **gpupdate /force /wait:**100
- **gpupdate /boot**

Update Group Policy settings from Group Policy Management Console

A new feature introduced with Windows Server 2012 is that from within the Group Policy Management Console. The update process also notifies how many computer objects will be affected by the update operation.

This can be accomplished by **Right-clicking** an Active Directory Organization Unit (OU) select **Group Policy Update**.



You have chosen to force a Group Policy update on all computers within Domain Controllers and all subcontainers. If you choose 'Yes' below, User and Computer policy settings will be updated on:

1 Computer

Are you sure you want to update policy for these computers?

Group Policy update will be forced on all computers within Domain Controllers and all subcontainers within the next 10 minutes. Both user and computer policy settings will be refreshed.

Completed (1 of 1)

Computer Name	Error Code	Error Description
Succeeded (1)		
WIN-DC1.school.local		

TROUBLESHOOTING WINDOWS SERVER 2012

DISABLING THE SHUTDOWN EVENT TRACKER

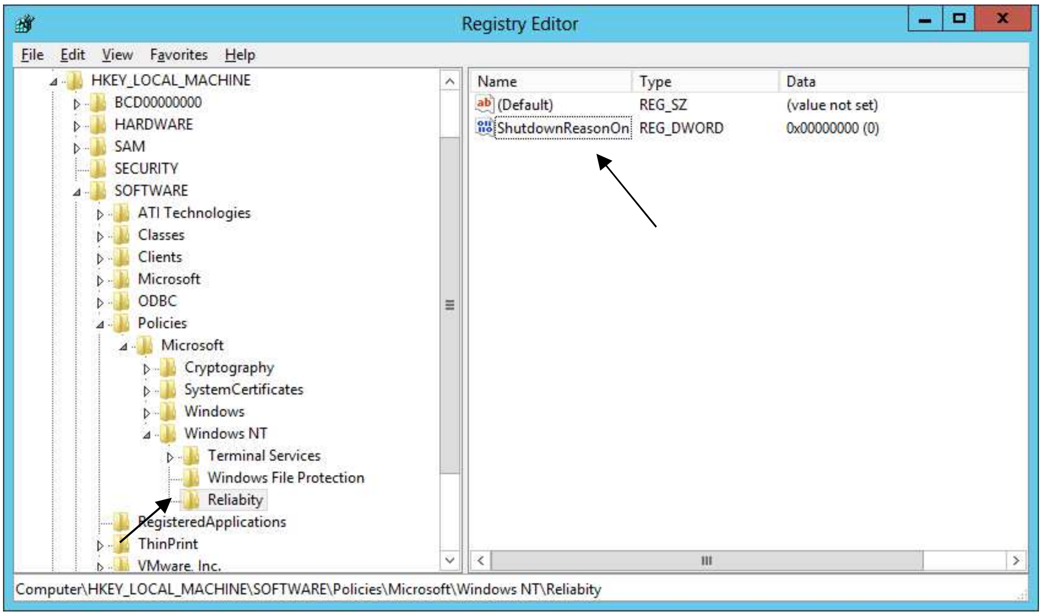
To turn off the Shutdown Event Tracker, navigate to the following key in your registry:

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Reliability

*****Creation of the Reliability is required***

Create a new DWORD with the following values:

Value Name: ShutdownReasonOn
Value: 0 (HEX)



Name	Type	Data
(Default)	REG_SZ	(value not set)
ShutdownReasonOn	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Reliabity

*****The change will take place immediately no reboot is required.***

SET TIME SOURCE TO DIS

- First, locate your PDC Server. Open command prompt on any server and type:

  ```
  netdom /query fsmo
  ```

- Log in to your PDC Server and open the command prompt.

- Stop the W32Time service

  ```
  net stop w32time
  ```

- Configure the external time sources, type:

```
w32tm /config /syncfromflags:manual /manualpeerlist:”165.29.1.11,165.29.1.12”
```

- Make your PDC a reliable time source for the clients. Type:

  ```
  w32tm /config /reliable:yes
  ```

- Start the w32time service:

  ```
  net start w32time
  ```

- The windows time service should begin synchronizing the time. You can check the external NTP servers in the time configuration by typing:

  ```
  w32tm /query /configuration
  ```

*****Check the Event Viewer for any errors.***

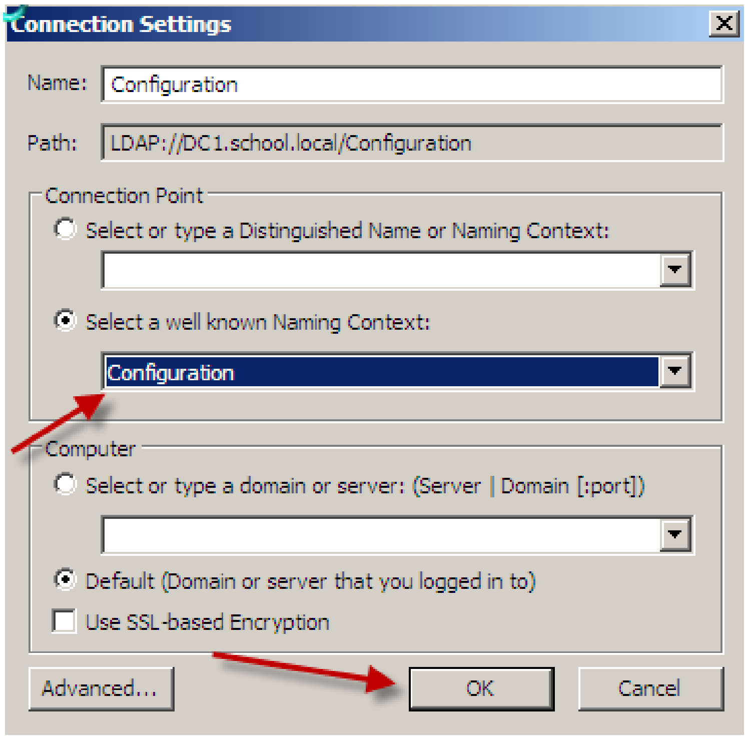
Active Directory Maintenance

Delete Dead/Tomb-stoned Domain Controller from Active Directory

1. From another Domain Controller within the domain, open a command prompt and type **ADSIEDIT.MSC**

2. In the ADSI Edit window, click **Action** > **Connect To**.

3. In the **Select a Well Known Naming Context** drop-down menu, select **Configuration**, and click **OK**.



Connection Settings

Name: Configuration

Path: LDAP://DC1.school.local/Configuration

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context: Configuration

Computer

○ Select or type a domain or server: (Server | Domain [:port])

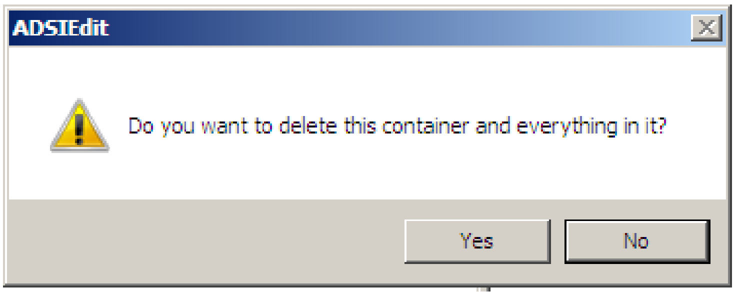
● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

Removing the Server from the Active Directory Site

4. Navigate to Configuration\CN=Configuration\CN=Sites\CN=<SiteName>\CN=Servers\CN=<ServerName>, where <SiteName> and <ServerName> correstpond to the location of the dead domain controller.

5. Right-Click on CN=NTDS Settings and click **Delete**, when prompted to delete the container and everything in it, click **Yes**.



Do you want to delete this container and everything in it?

6. Right-Click CN=Server Name that you are removing and click **Delete**. Click **Yes** to confirm the delete.

Removing the Server from the File Replication Service

7. In the ADSI Edit window, click on **ADSI Edit** in the left-hand pane.

8. Click **Action** > **Connect To**.

9. In the **Select a Well Known Naming Context** drop-down menu, select **Default naming context**, and click **OK**.

10. Navigate to Configuration\CN=System\CN=File Replication Service\CN=Domain System Volume(SYSVOL share)\CN=<ServerName> where <ServerName> correstpond to the location of the dead domain controller.

11. Right-click the CN=<ServerName>, and select **Delete**.

12. Click **Yes** to delete the object.

Removing the Server from Active Directory Sites and Services

13. Open **Active Directory Sites and Services.**

14. Expand Sites.

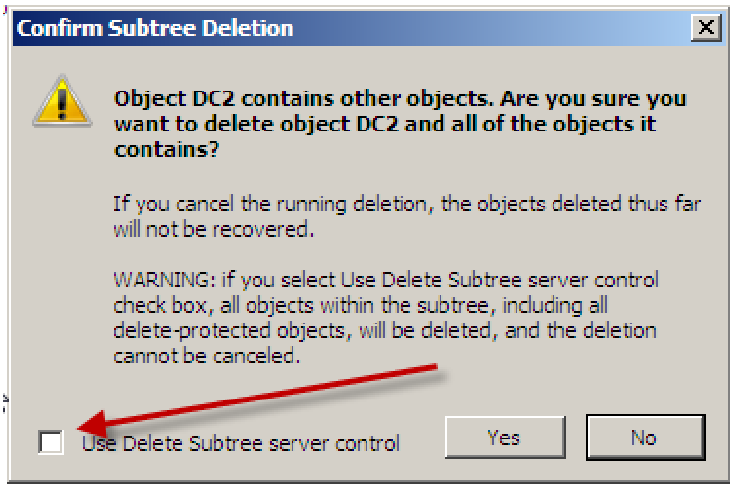
15. Expand the AD Site that the dead Domain Controller was a member of.

16. Expand the dead Domain Controller.

17. Right-click **NTDS Settings** and click **Delete**.

18. When prompted, click Yes.

19. You will receive the Confirm Subtree Deletion box as shown below. Check the **Use Delete Subtree server control** option and click Yes.



Object DC2 contains other objects. Are you sure you want to delete object DC2 and all of the objects it contains?

If you cancel the running deletion, the objects deleted thus far will not be recovered.

WARNING: if you select Use Delete Subtree server control check box, all objects within the subtree, including all delete-protected objects, will be deleted, and the deletion cannot be canceled.

20. Close Active Directory Sites and Services.

Removing the Server from Active Directory Users and Computers

21. Open Active Directory Users & Computer.

22. Browse to the Domain Controller Computer object, right-click and select **Delete**.

23. When prompted to confirm the deletion, select **Yes**.

24. Another confirmation box will pop up.

25. Check the box next to “This Domain Controller is permanent...” and click **Delete**.

26. Close Active Directory Users & Computers

*****DNS may need to be verified to make sure that there are not any records tied to the server that was removed from the domain.***

MANUALLY SEIZE FSMO ROLES

To seize the FSMO roles by using the Ntdsutil utility, follow these steps:

- Log on to a Windows Server-based member computer or Domain controller that is located in the forest where FSMO roles are being seized.

*****It is recommend that you log on to the domain controller that you are assigning FSMO roles to.***

*****The logged-on user should be a member of the Enterprise Administrators group to transfer schema or domain naming master roles, or a member of the Domain Administrators group of the domain where the PDC emulator, RID master and the Infrastructure master roles are being transferred.***

- Click Start, click Run, type **ntdsutil** in the Open box, and then click OK.

- Type **roles**, and then press ENTER.

- Type **connections**, and then press ENTER.

- Type **connect to server** ***servername***, and then press ENTER.

*****Servername is the name of the domain controller FSMO role is being transferred to.***

- At the server connections prompt, type **q**, and then press ENTER.

- Type **seize role**, where role is the role that you want to seize.

*****For a list of roles that you can seize, type ? at the fsmo maintenance prompt, and then press ENTER, or see the list of roles at the end of this section. For example, to seize the RID master role, type seize rid master. The one exception is for the PDC emulator role, whose syntax is seize pdc, not seize pdc emulator.***

- At the fsmo maintenance prompt, type **q**, and then press ENTER.

- Type **q**, and then press ENTER to quit the Ntdsutil utility.

How to Reset the Directory Services Restore Mode Administrator Account Password

24. Click, Start, click Run, type **ntdsutil**, and then click OK.

25. At the Ntdsutil command prompt, type set dsrm password.

26. At the DSRM command prompt, type one of the following lines:

    a. To reset the password on the server on which you are working, type:

       reset password on server null

*****The null variable assumes that the DSRM password is being reset on the local computer. Type the new password when you are prompted.***

*****No characters appear while you type the password.***

    b. To reset the password for another server, type:

       reset password on server *servername*

*****where servername is the DNS name for the server on which you are resetting the DSRM password.***

    c. Type the new password when you are prompted.

27. At the DSRM command prompt, type q.

28. At the Ntdsutil command prompt, type q to exit.

http://support.microsoft.com/default.aspx?scid=kb;en-us;322672