DIS

Department of Information Systems

Arkansas. A State of Technology.

Microsoft Server 2008 Installation & Configuration

Windows 2008 – Basic Installation

This document is DIS' recommended method for implementing a Windows Server 2008 & Active Directory within a K12 network.

Microsoft recommends only one method of installation, booting from the installation DVD itself. This method does not incorporate the transfer of source files to the hard drive. However, throughout this process, the source files will be copied to the hard-drive and service packed, thus allowing you to install components of the Windows Server without having to use the installation CD.

Windows Server 2008 Requirements

Component	**Requirement**
Processor	• Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor) • Recommended: 2GHz or faster **Note:** An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems
Memory	• Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum (32-bit systems): 4GB (Standard) or 64GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32GB (Standard) or 2TB (Enterprise, Datacenter and Itanium-Based Systems)
Available Disk Space	• Minimum: 10GB (60GB IS THE DIS RECOMMENDED MINIMUM!!!!!) • Recommended: 40GB or greater **Note:** Computers 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

Items needed prior to starting install:

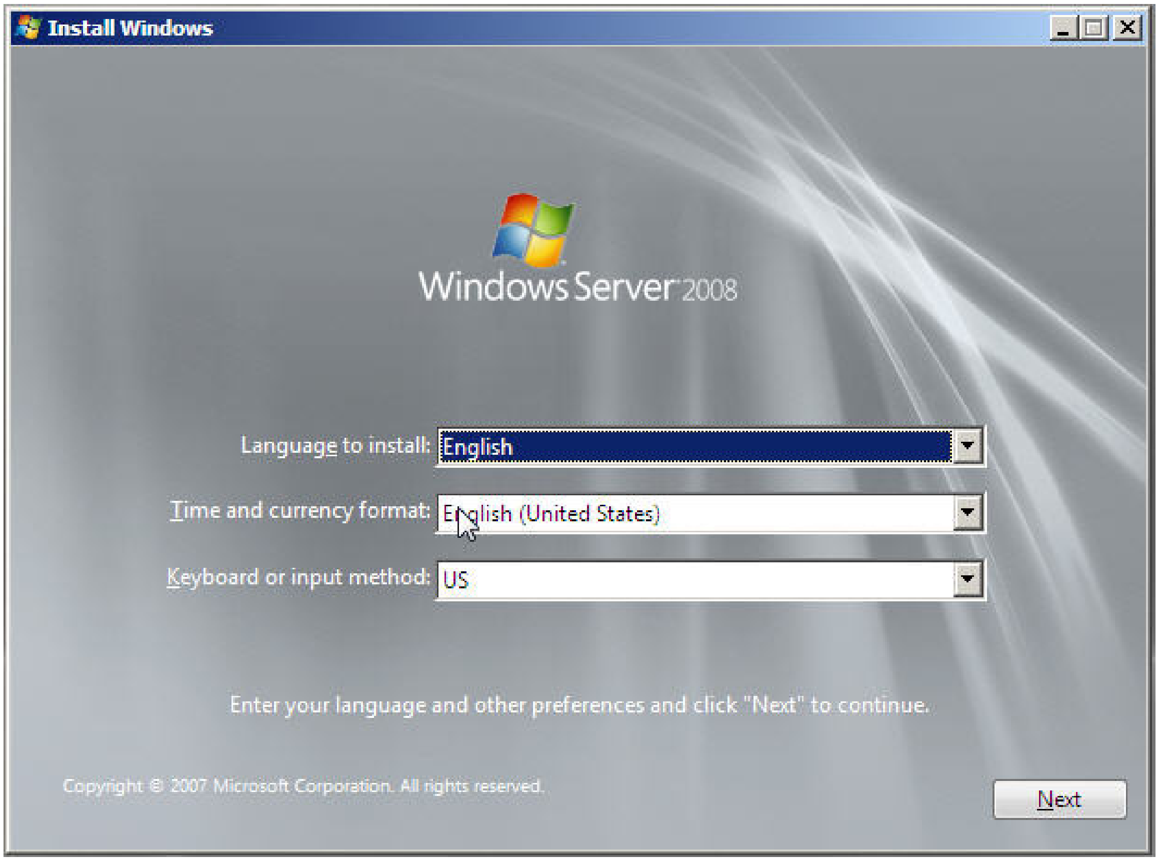
- Microsoft Windows Server 2008 DVD
- CD with the latest Windows 2008 Service Pack file, if the install DVD is not at the latest Service Pack.
- 1 NAT IP Address (If your district is implementing NAT)
- 1 Public IP Address
- Floppy Disk, USB Drive, CD/DVD containing your SCSI/RAID drivers.

Start setup from a bootable CD-Rom as follows:

1. Make sure that **all** network cables **AND UPS** cables are unplugged from the CPU.
2. Insert the Windows 2008 Server installation DVD into the drive.
3. Restart the computer and boot to the DVD-Rom. Wait for Setup to display a dialog box.
4. Follow the Setup instructions on the screen.

Installation

1. Insert the appropriate Windows Server 2008 installation media into your DVD drive and reboot the computer/server.
2. When prompted for an **installation language** and other regional options, make your selection and press **Next**.



Language to install: English

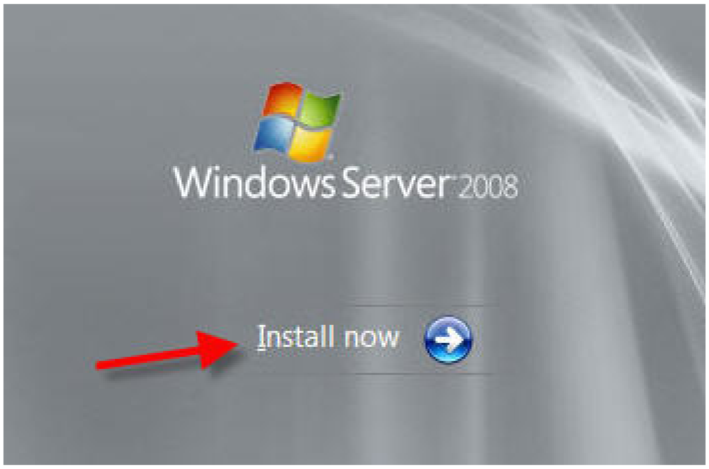
Time and currency format: English (United States)

Keyboard or input method: US

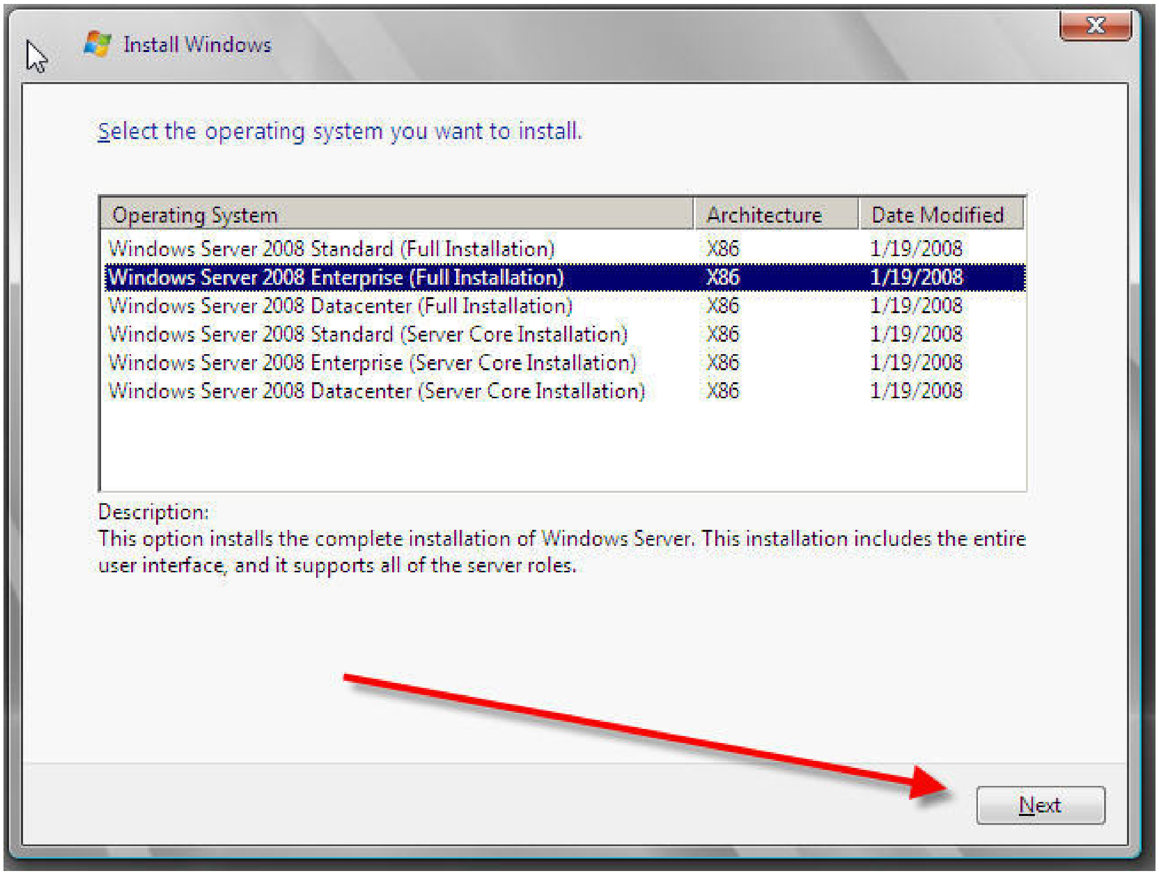
Enter your language and other preferences and click "Next" to continue.

Copyright © 2007 Microsoft Corporation. All rights reserved.

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



4. Select the proper edition of Windows Server 2008 that is to be installed and press **Next**.

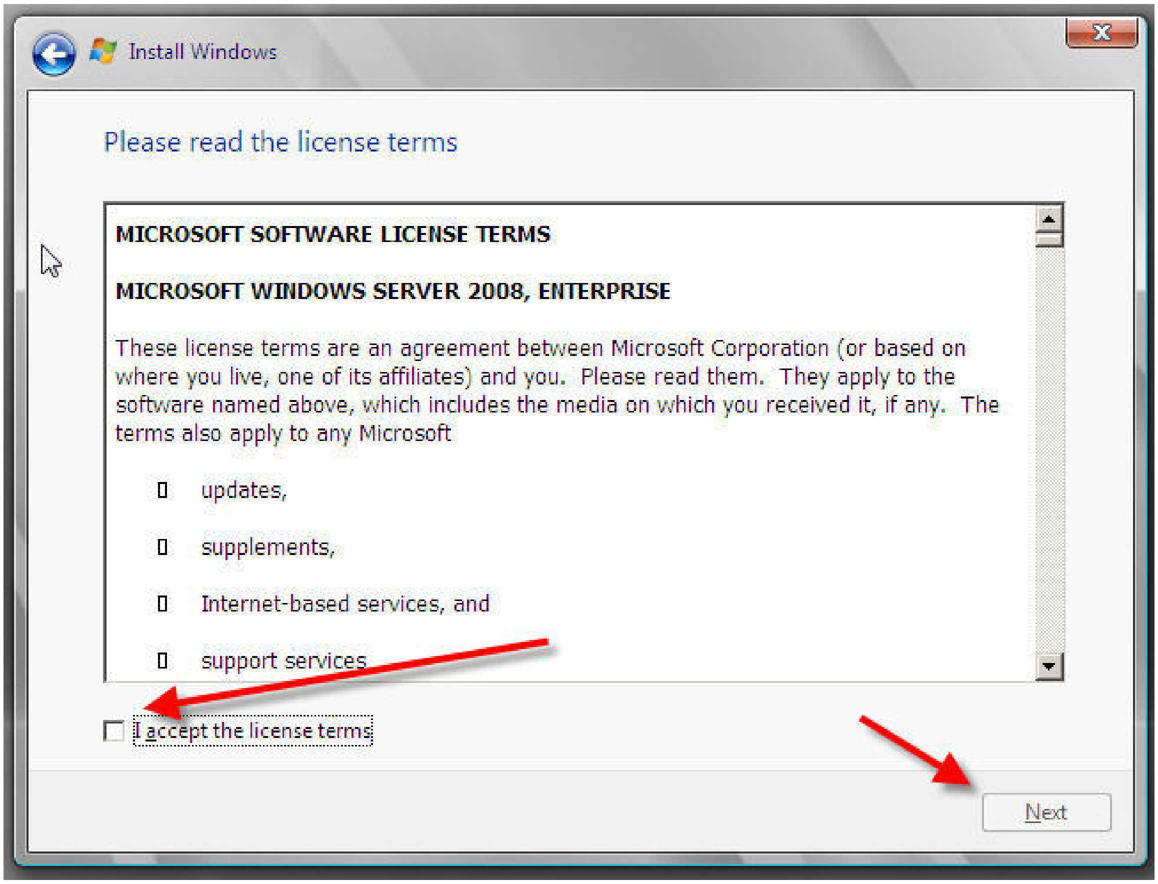


Select the operating system you want to install.

Operating System	Architecture	Date Modified
Windows Server 2008 Standard (Full Installation)	X86	1/19/2008
Windows Server 2008 Enterprise (Full Installation)	X86	1/19/2008
Windows Server 2008 Datacenter (Full Installation)	X86	1/19/2008
Windows Server 2008 Standard (Server Core Installation)	X86	1/19/2008
Windows Server 2008 Enterprise (Server Core Installation)	X86	1/19/2008
Windows Server 2008 Datacenter (Server Core Installation)	X86	1/19/2008

Description:
This option installs the complete installation of Windows Server. This installation includes the entire user interface, and it supports all of the server roles.

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



Please read the license terms

MICROSOFT SOFTWARE LICENSE TERMS

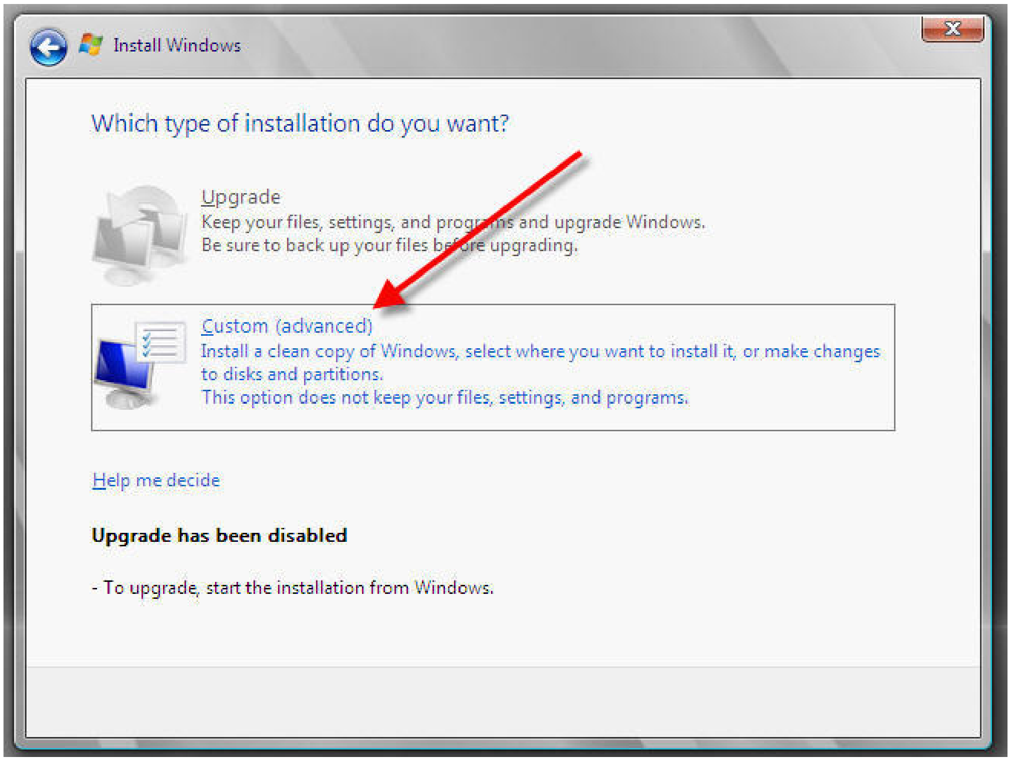
MICROSOFT WINDOWS SERVER 2008, ENTERPRISE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

□ I accept the license terms

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



Install Windows

Which type of installation do you want?

Upgrade
Keep your files, settings, and programs and upgrade Windows.
Be sure to back up your files before upgrading.

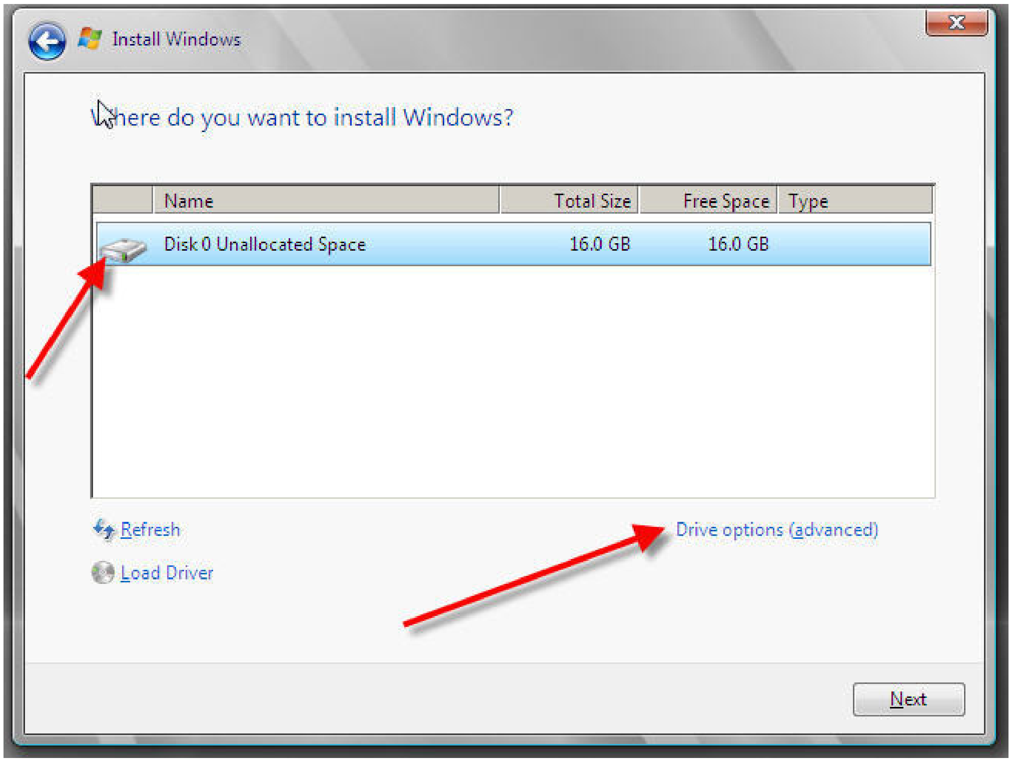
Custom (advanced)
Install a clean copy of Windows, select where you want to install it, or make changes to disks and partitions.
This option does not keep your files, settings, and programs.

Help me decide

Upgrade has been disabled

- To upgrade, start the installation from Windows.

7. Select the disk that you will be installing Windows Server 2008 onto and then click **Drive options (advanced)**.

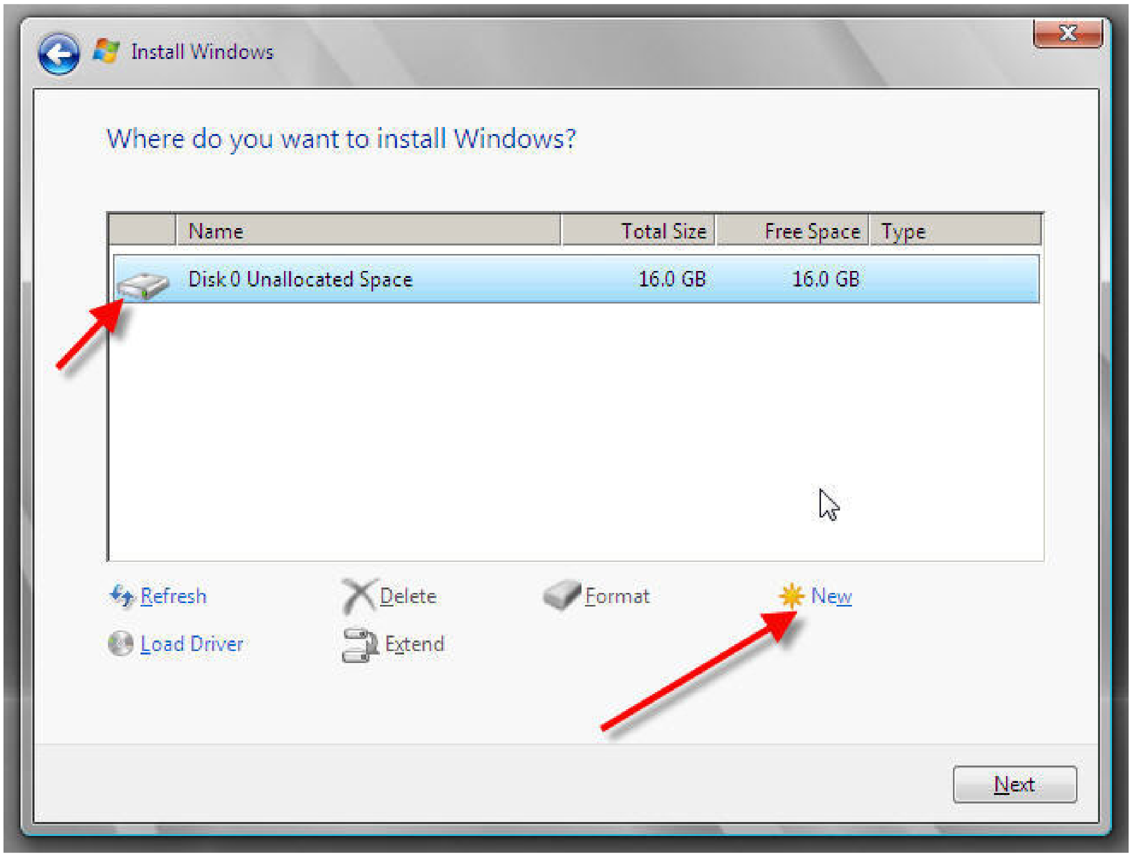


Install Windows

Where do you want to install Windows?

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	16.0 GB	16.0 GB	

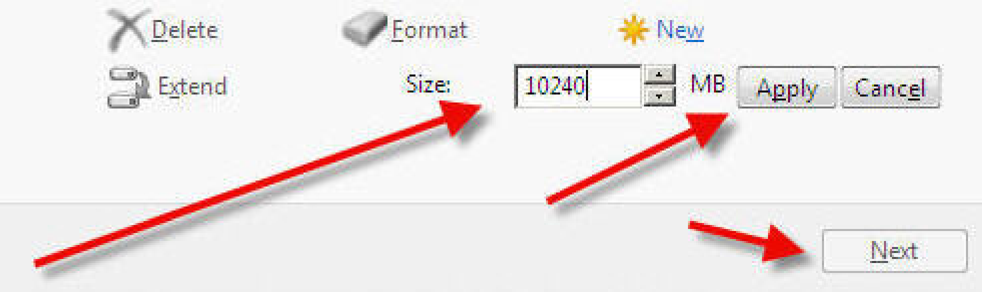
8. Select the disk that you will be installing Windows Server 2008 onto and then click **New** to create the partition that Windows Server 2008 will be installed on.



Where do you want to install Windows?

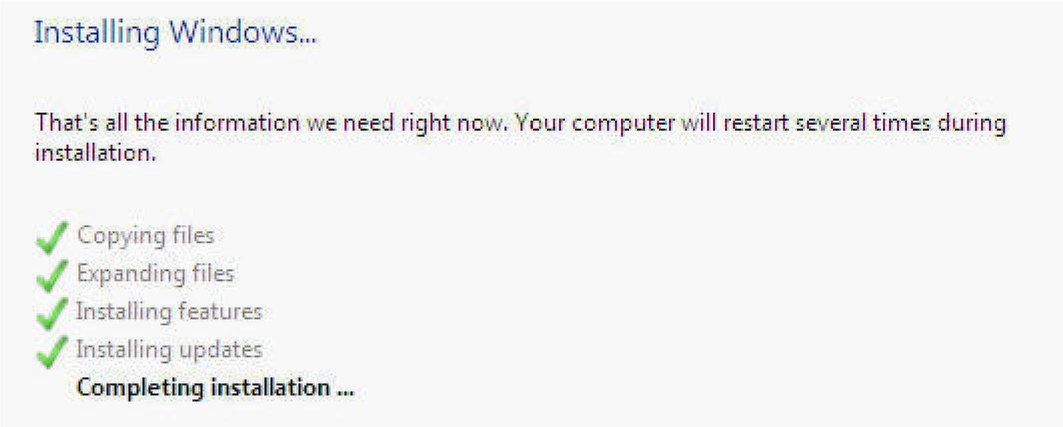
	Name	Total Size	Free Space	Type
	Disk 0 Unallocated Space	16.0 GB	16.0 GB	

9. 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.



Size: 10240 MB

10. You will see the following screen while the installation files are copied to the server. The server will reboot to complete the installation.



Installing Windows...

That's all the information we need right now. Your computer will restart several times during installation.

✓ Copying files
✓ Expanding files
✓ Installing features
✓ Installing updates
Completing installation ...

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 automatically login to the initial desktop.

Initial Config Tasks Steps

1. Activate Windows and insert key
2. Set time Zone
3. Configure Networking and change to Static IP
4. Enable automatic updating
5. Download and install updates

Disable Internet Explorer Enhanced Security Configuration

1. Click on Start > Administrative Tools > Server Manager.
2. Once the Server Manager opens, on the middle-right of the screen click on **Configure IE ESC**.
3. Set the **Administrators** section to **Off** and then click **OK**.

Disable IPv6 via Registry Key (THIS NEEDS TO BE DONE)

1. Open the Registry Editor by clicking **Start** > **Run** and type **REGEDIT** and click **OK**.
2. Expand the following Key Structure in the Registry Editor:

```
Computer
        +HKEY_LOCAL_MACHINE
                +System
```

```
+CurrentControlSet
          +Services
                    +Tcpip6
                              +Parameters
```

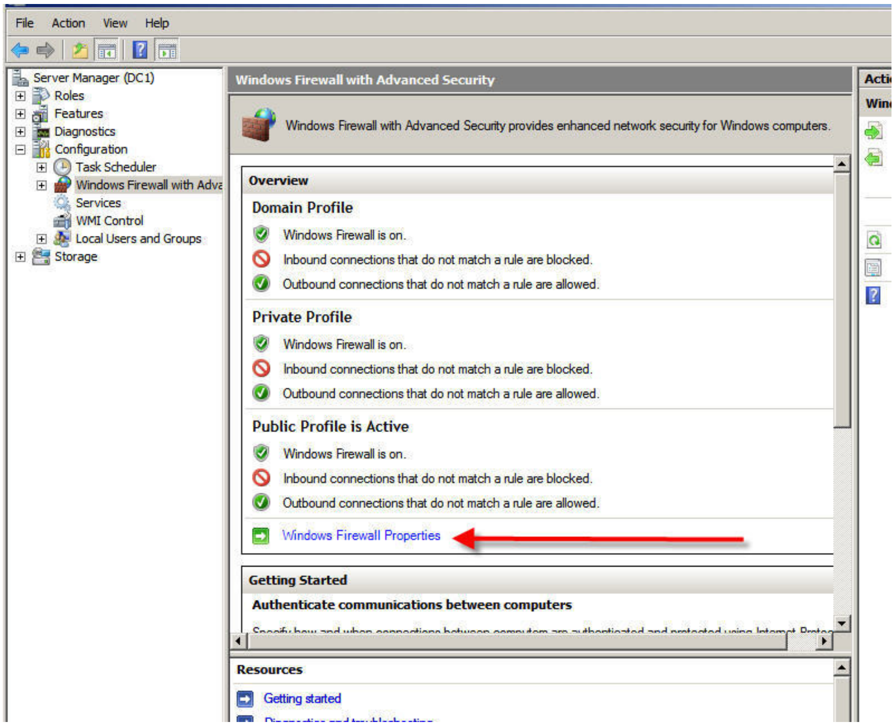
3. Right-Click on the Parameters Key and click **New** > **DWORD (32-Bit) Value**.
4. Type in the name **DisabledComponents** and press **Enter**.
5. Double-click on the newly created key and enter **ff** for the value data in Hexadecimal mode, **255** for Decimal mode.
6. Close the Registry Editor.
7. Click on **Start** > **Network**. When the window opens, click on the **Network and Sharing Center** icon in the middle of the toolbar menu.
8. Under the Tasks section to the left side of the screen, click **Manage Network Connections**.
9. Perform the following on each network connection: Right-click on the network connection and click **Properties**.
10. Uncheck the **Internet Protocol Version 6 (TCP/IPv6)** and click **OK**.
11. Reboot the server.
12. Plug in the LAN Cable.

Run Windows Updates

1. Click on the **Start** Menu > **Control Panel**.
2. Turn on Windows Updates. The server will automatically go out and check for updates. Once the check is complete, click the **Install Now** button. Before proceeding, install all Critical and Security updates. This make take several reboots and Update checks.

Disable Windows Firewall

1. Click on **Start** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
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

Windows Firewall with Advanced Security provides enhanced 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

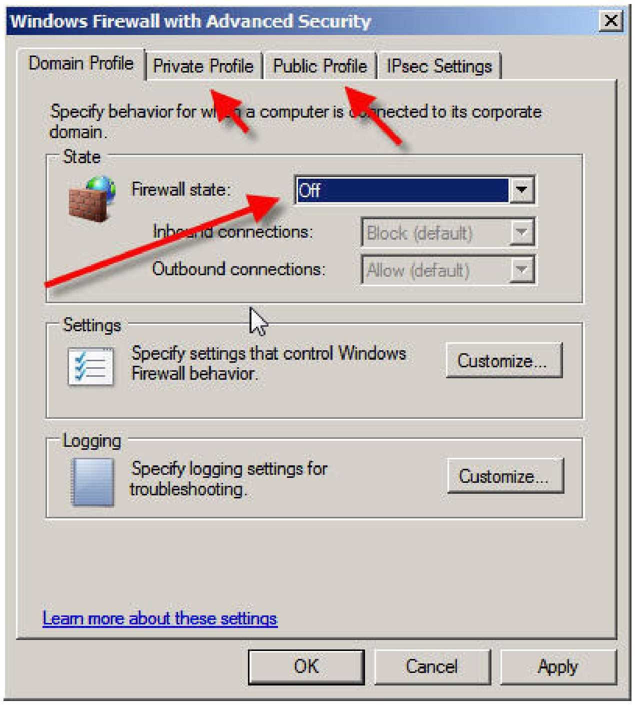
Getting Started

Authenticate communications between computers

Resources

Getting started

3. Select each of the Firewall Section tabs and turn the Firewall off.



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

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Settings

Specify settings that control Windows Firewall behavior.

Logging

Specify logging settings for troubleshooting.

Learn more about these settings

- **- IT IS HIGHLY RECOMMENDED THAT THE DIS FIREWALL BE ENABLED ON YOUR ROUTER IF YOU ARE NOT USING A THIRD-PARTY FIREWALL APPLIANCE. IF YOU DO NOT HAVE A FIREWALL OF ANY SORT, YOU MAY WISH TO LEAVE THE FIREWALL ENABLED AND ADJUST THE SCOPES OF THE INBOUND/OUTBOUND RULES TO MEET YOUR ENVIRONMENTAL NEEDS.**

Creating Volumes

1. From the Start menu, right-click Computer and click **Manage** OR **Click Start** > **Administrative Tools** > **Server Manager**.
2. In the left hand pane, expand **Storage** and click on **Disk Management**.
3. Right-click the CD-Rom Drive volume in the lower right window pane and click **Change Drive Letter**. Change the drive letter to L. A confirmation box will pop up, click **Yes**.
4. Locate the unallocated drive space and right click and select **New Simple Volume** to create a partition. The Partition wizard will launch. Click **Next** to continue.
5. Enter the intended volume size (in MB) and click **Next**.
6. Select **D** for the drive letter and click **Next**.
7. Enter **Data** as the Volume Label and check the **Perform a quick format** box.
8. Click **Next** and **Finish** to complete the build of the volume.

Repeat steps 4-8 to create the following volumes

Faculty-Homes	Drive Letter: F
Students-Homes	Drive Letter: E

NOTE: It is recommended to have separate volumes/partitions for Data, Faculty Home Directories and Student Home Directories. Quota Limitations are volume based natively. However, if you wish to combine the Faculty and Student home directories on the same volume, you can implement directory level quota limits with the File Server Resource Manager. The steps for implementing quota limits are covered later in this book.

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. Click on **Start** > **Administrative Tools** > **Server Manager**.
2. In the left-hand pane, click on **Roles**.
3. On the right-hand of the screen, click on **Add Roles**.
4. On the Before You Begin screen, click **Next**.
5. Check the box to the left of **Active Directory Domain Services** and click **Next**.
6. Click **Next** again and then click **Install**.

   The above steps allow for the Windows Firewall (and other services) to auto-adjust for the Roles (services) that are being installed. Without performing these steps, the

7. Click **Start** > **Run**, type **DCPROMO** and click **OK.** Click **Next** on the initial AD Installation Wizard Screen.
8. Read the **Operating System Compatibility** screen and click **Next**. * - Any lower level clients and servers, such as NT4.0, some Samba clients and some NAS devices

may no longer communicate with the server due to strong encryption algorithms in Windows Server 2008.

9. Select **Create a new domain in a new forest** and click **Next** to continue. * - This step and those following assume this is the first controller in a new domain, tree and forest.
10. Type the DNS name for the new domain. DIS recommends you type your abbreviated school district name followed by .local **DO NOT** end your domain name with .com, .net, .org, .edu or any other first level domain name that is resolvable on the internet. **<u>This domain name is for internal resolution only</u>**. Contrary to Microsoft's early instructions, using a resolvable internet name on your local domain presents some security issues. Click **Next** to continue.
11. For the Forest Functional Level, select **Windows Server 2008** and click **Next**. * ***NOTE – IF YOU INTEND ON USING ANY SERVER 2003 DOMAIN CONTROLLERS, SELECT Windows Server 2003 Native.***
12. On the **Additional Domain Controller Options** screen, be sure that **DNS** and **Global Catalog** options are selected and click **Next**.
13. If this is the first Domain Controller in your network, you will receive a warning box stating "A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server." This is normal, as the DNS Zone has not yet been created. It will be created during the initial Active Directory install. Click **Yes** to proceed.
14. On the **Location for Database, Log Files and SYSVOL** screen, click **Next**. If you are running your Windows file system on a single drive or a Raid 1 (Mirrored) set, you may wish to adjust these paths to reside on a more fault tolerant disk set, such as a RAID 5 volume. These are also often relocated to other folder paths for security reasons. If these are left at the default, they can be relocated at a later date and time.
15. On the **Directory Services Restore Mode Administrator Password**, enter in a complex password that is UNIQUE to this server and is NOT your normal administrator password and click **Next**. This password is NOT replicated to any other domain controllers and IS required to boot this server into Safe Mode or Active Directory Services Restore Mode. **DOCUMENT THIS PASSWORD AND DOCUMENT EVERY TIME YOU CHANGE THIS PASSWORD.**
16. On the **Summary** screen, click **Next** to start the Active Directory DC Creation/Promotion.
17. When the Active Directory installation starts, check the box **Reboot on completion**. The server will automatically reboot after the promotion process.

Additional DNS Configuration

Reverse Lookup Zones

18. Log into the server when the server has completely booted back up.
19. Click **Start** > **Administrative Tools** > **DNS**.
20. Expand your server name, right-click on **Reverse Lookup Zones** and click **New Zone.**
21. On the **Zone Type** screen, take the defaults and click **Next**.
22. For the Active Directory Zone Replication Scope, select **To all domain controllers in this domain** and click **Next**.
23. Select **IPv4Reverse Lookup Zone** and click **Next**.
24. For the reverse zone name, enter the first three octets of your public IP range and click **Next**. For example, if your public IP range is 165.29.1.X, you would enter 165.29.1. * - If your IP range spans multiple "class C subnets" then only enter the

first two octects. For example if your IP range is 10.10.0.0 to 10.10.1.255, then you would only enter 10.10 and then click Next.

25. On the **Dynamic Update** screen, take the default and click **Next**.
26. Click **Finish** to create the new zone.

Steps 18 through 26 must be completed for EVERY IP subnet that will be used in your Active Directory environment.

Stale Record Scavenging

27. Within the DNS Manager, right-click on your DNS server and click **Set Aging/Scavenging for All Zones**.
28. Check the box "**Scavenge stale resource records** and then click **OK**.
29. When prompted with the Server Aging/Scavening Confirmation box, check the **Apply these settings to the existing Active Directory-integrated zones option** and then click **OK**.

Steps 27 and 28 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 2008, 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.

30. Within the DNS Manager, right-click your server and click **Properties**.
31. Click the **Forwarders** tab and then click the **Edit** button.
32. Enter your DIS DNS servers as specified below and click **OK**.
33. Click **Apply** and then **OK**.
34. Close the DNS Manager.

DNS = 170.94.156.195
DNS = 170.94.156.196

If you are on the LR POP (165.29.X.X and 170.211.X.X), you will use the DNS Servers as listed above, using one as the Primary and the other as the Secondary DNS server, and one of the following DNS servers as the tertiary DNS server.

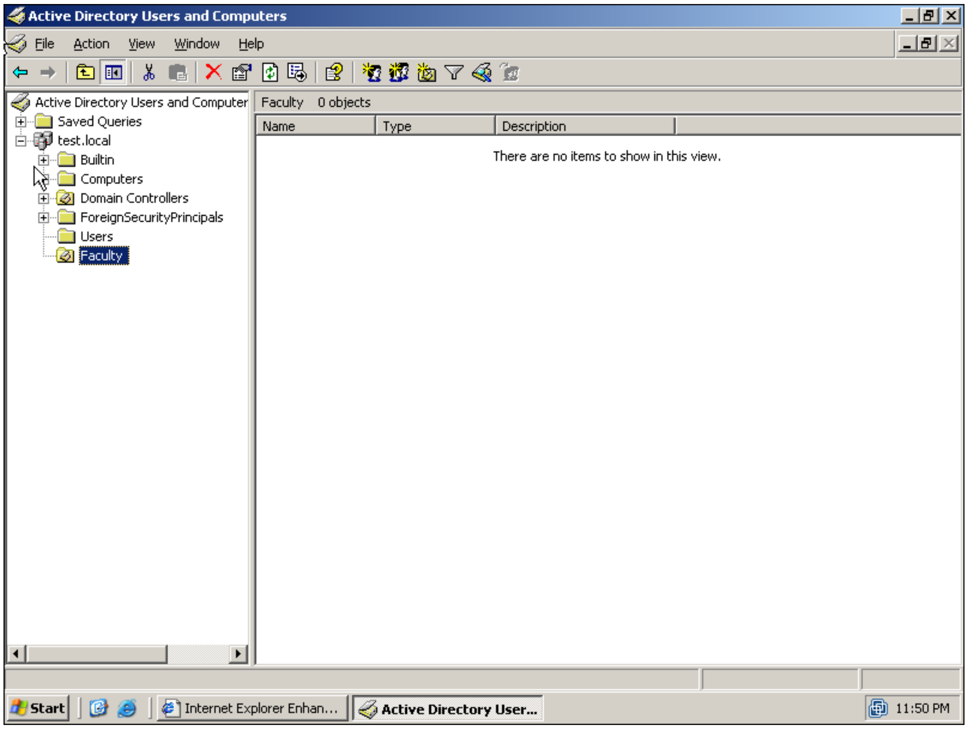
Pine Bluff POP DNS Server = 66.204.193.26 (THIS SERVER IS NOT A MAIL RELAY)
Fayetteville POP DNS Server = 66.204.1.66 (THIS SERVER IS NOT A MAIL RELAY)

If you are on the Pine Bluff or Fayetteville POP, then you will use one of the above as your Primary DNS Forwarder, with your respective LR DNS Server (170.94.156.x) as the secondary and tertiary DNS servers.

Basic AD Structuring for K12

Single Site Active Directory Networks

1. Click **Start**, **Administrative Tools**, **Active Directory Users and Computers**.
2. Right-click on **YourDomain.LOCAL**, click **New**, then **Organizational Unit**.
3. Enter **Faculty** as the name of the new Organizational Unit (OU) then click **Next.** *NOTE: A new option in Windows Server 2008 is to automatically protect the OU from being deleted or moved. If you do NOT want this option set, you must uncheck the **Protect container from accidental deletion** box before selecting **Next.** This is where we will place all of our faculty accounts, faculty account templates, security groups that will be pertained to the faculty, and faculty e-mail distribution lists. If you have a rather small amount of faculty you may only wish to have this single OU. However, if you are larger district or wish to sort things out more, you can create additional OU's under the newly created Faculty OU. Some schools choose to create an OU for High School, Middle School, Elementary, Central Office, Support Staff, and Technology **UNDERNEATH** the **Faculty** OU. Structure this to meet your needs and/or requirements.

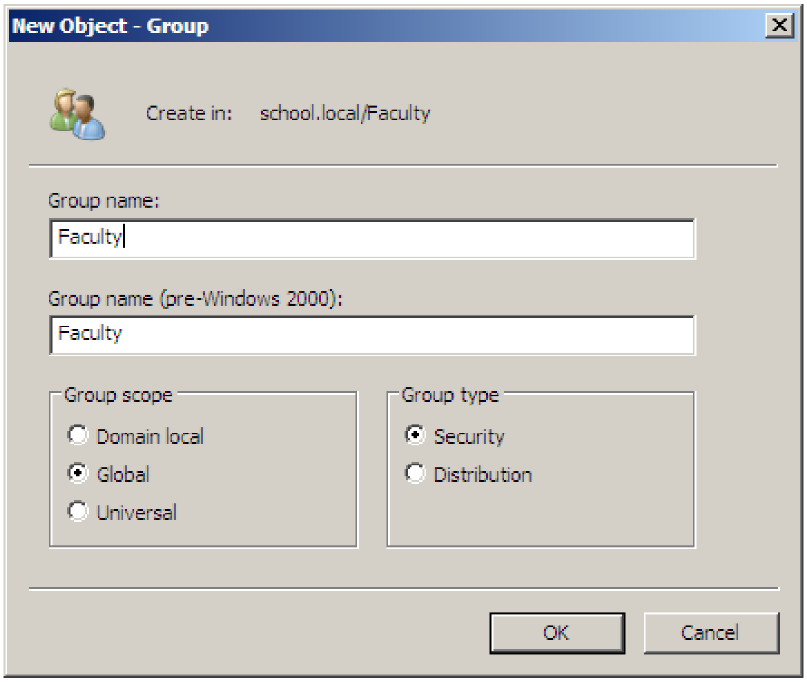


There are no items to show in this view.

4. Right-click on **YourDomain.LOCAL**, click **New**, then **Organizational Unit**.
5. Enter **Students** as the name of the new Organizational Unit (OU) then click **Next.** This is where we will place all of our student accounts, student account templates, security groups that will be pertained to the students, and student e-mail distribution lists.
6. Right-click on the **Students** OU that we just created and click **New**, then **Organizational Unit**. Enter the graduating year of this year's senior class. Repeat this step for every grade level that you are going to have student accounts for.

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.

7. Right-click on the **Faculty** OU then click **New**, **Group**.
8. Name this group **Faculty** and click **Next**.


New Object - Group

Create in: school.local/Faculty

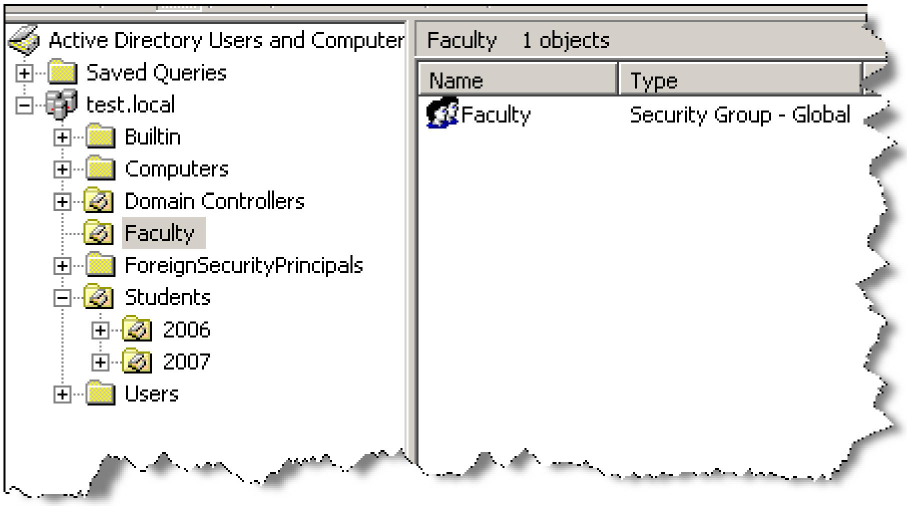
Group name: Faculty

Group name (pre-Windows 2000): Faculty

Group scope: ○ Domain local ● Global ○ Universal

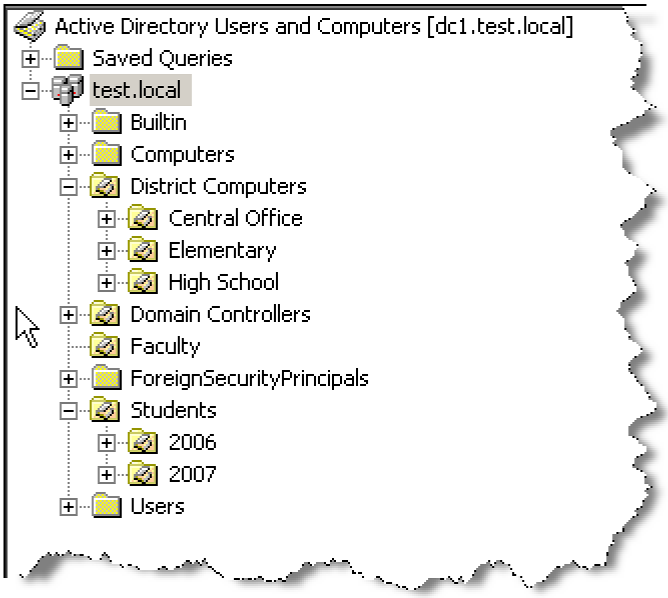
Group type: ● Security ○ Distribution

9. Do **<u>not</u>** check "Create an Exchange e-mail address" if prompted, click **Next**.
10. Click **Finish**.
11. Right-click on the **Students** OU, then click **New**, **Group**.
12. Name this group **Students** and click **Next**.
13. Do **<u>not</u>** check "Create an Exchange e-mail address" if prompted, click **Next**.
14. Your AD Structure should now look similar to this screenshot.



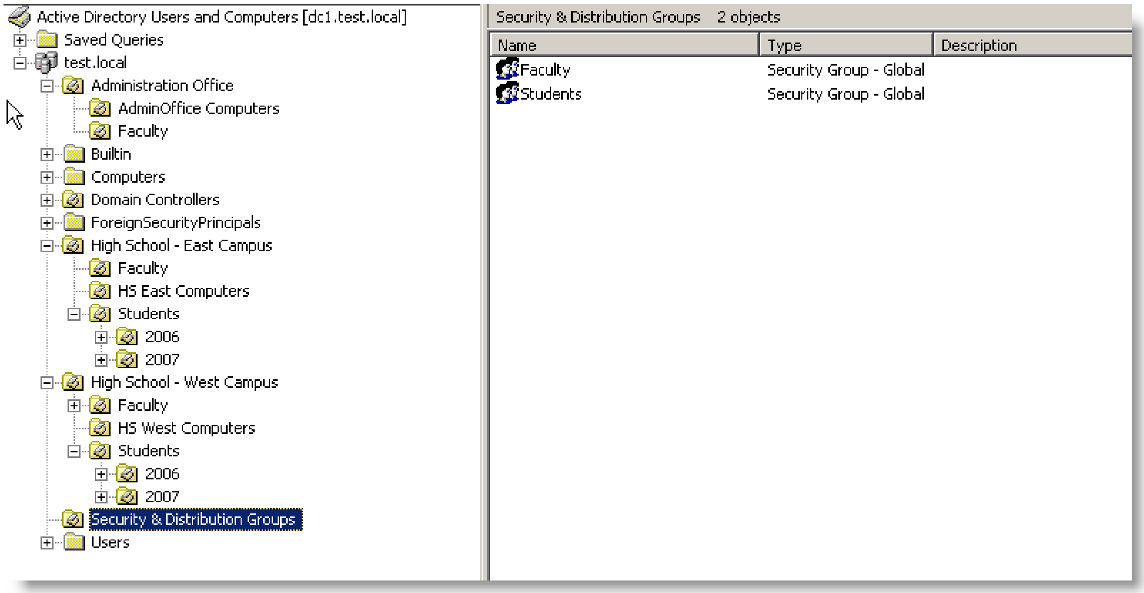
Now that we have our OU setup for our users and our security groups created, we need to setup OU's for computers. One of the reasons for creating OU's for your computers is Group Policies. For instance, if you have a lab that you would like to lock down with a specific set of restrictions, but no other stations, that lab would need its own OU, along with the computers for that lab placed in the lab's OU.

15. Right-click on **YourDomain.LOCAL**, click **New**, then **Organizational Unit**.
16. Enter **District Computers** as the name of the new Organizational Unit (OU) then click **Next**. This is where we will move all of the computers to after they have been joined into Active Directory. As with the Faculty or Student OU's, you can also sort these into deeper OU's to meet your district's needs. Some schools choose to create an OU for High School, Middle School, Elementary, Central Office, Support Staff, and Technology **<u>UNDERNEATH</u>** the **District Computers** OU. This also could be drilled down farther, such as a specific lab underneath the high school. Structure this to meet your needs and/or requirements.
17. Your AD Structure should now look similar to this screenshot.



Multiple Site Active Directory Networks

If you are running Active Directory over multiple sites (behind more than one router), you would want to create an OU for each site, then place the Campus Computers, Faculty, and Students OU's under that Site OU. It would also be wise to create an OU just for district wide security & distribution groups.   Example…..


Active Directory Users and Computers [dc1.test.local]
Saved Queries
test.local
Administration Office
AdminOffice Computers
Faculty
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
High School - East Campus
Faculty
HS East Computers
Students
2006
2007
High School - West Campus
Faculty
HS West Computers
Students
2006
2007
Security & Distribution Groups
Users
Security & Distribution Groups   2 objects

Name	Type	Description
Faculty	Security Group - Global	
Students	Security Group - Global	

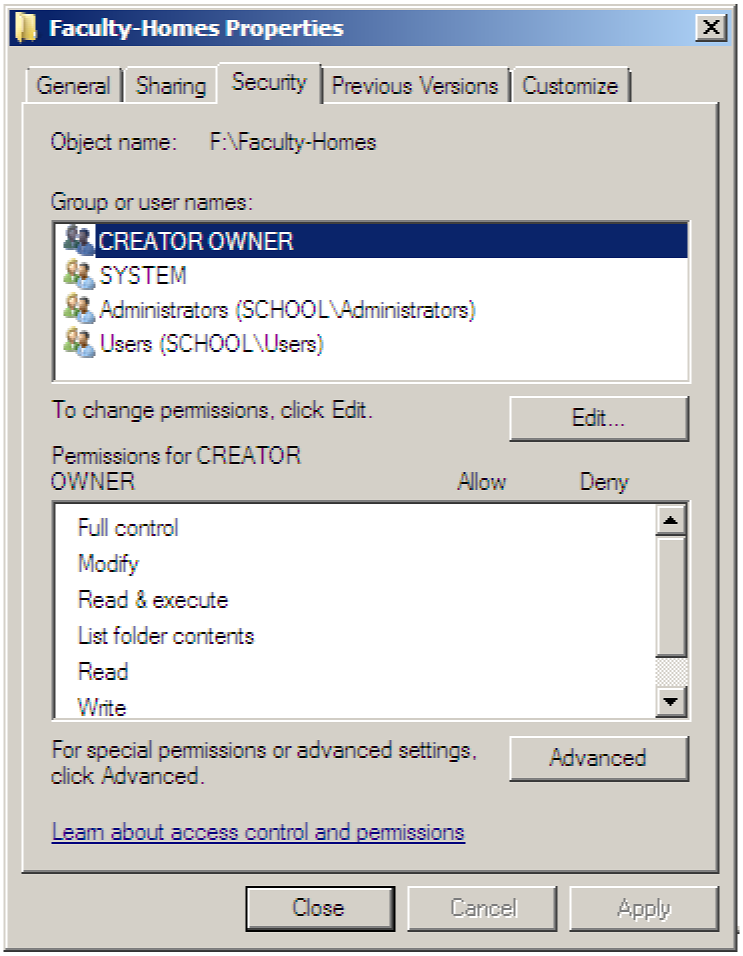
Another benefit of keeping sites separated by OU's, you can delegate campus level technicians to be able to have the authority to maintain user accounts, computer accounts, etc. that reside only in their campus' OU.

Create Share & 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 **My Computer** and browse to the volume that will hold the faculty home-directories. NOTE: It is recommended that Faculty & Student Home Directories be 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 **Apps**.
7. Click on the **Permissions** button.
8. Click on **Everyone** and click **Remove**.
9. Click **Add**.
10. In the name box enter **Domain Admins**, **Administrators, Faculty** and **Students,** each seperated by a semi-colon. Click the **Check Names** button and then **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.
11. Give **Domain Admins** and **Administrators** both **Full Control**.
12. Give the **Faculty** and **Students** group both **Change** rights, they will receive Read automatically.
13. Click on the **Caching** button. Select **Files or programs from this share will not be available offline**. It is NOT recommended to allow offline file-caching for any network shares that house database applications such as WinCAGI, MealTracker and RenLearn products, for example.
14. Click **OK**, **Apply**, and then **OK** until all property windows are closed.
15. Select on the **Sharing** tab and click the **Advanced Sharing** button.
16. Select the **Share this folder** check box.
17. For the share name type **Faculty-Homes$**. By adding a dollar sign to the end of the share name, the share is hidden when browsing the network. **This is highly recommended for ANY network share that will be housing home directories.**
18. Click on the **Permissions** button.
19. Click on **Everyone** and click **Remove**.
20. Click **Add**.
21. In the name box enter **Domain Admins**, **Administrators** and **Faculty,** each seperated by a semi-colon. Click the **Check Names** button and then **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.
22. Select each of the groups and then select **Full Control** under the **Allow** section.
23. Click on the **Caching** button. If you do not wish for these files to be available offline through file caching, select **Files or programs from this share will not be available offline**. If you wish provide cached content for your faculty, select the **Optimized for performance** option.
24. Click **OK**, **Apply**, and then **OK** until all property windows are closed.
25. Select the **Security** tab and click the **Advanced** button.

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



Object name: F:\Faculty-Homes

Group or user names:

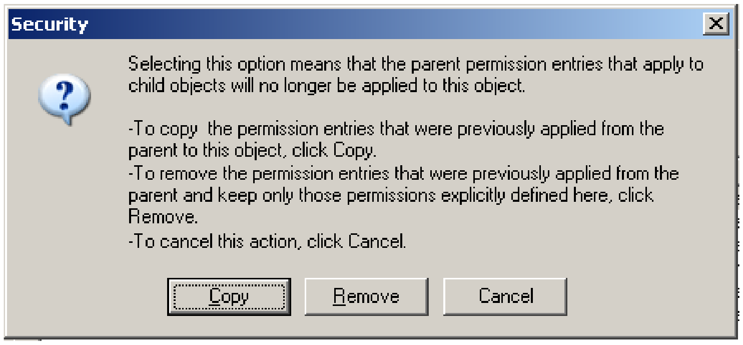
- CREATOR OWNER
- SYSTEM
- Administrators (SCHOOL\Administrators)
- Users (SCHOOL\Users)

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.

26. Click on the **Security** tab, then the **Advanced** button.
27. On the Permissions tab, select the **Edit** button.
28. In the bottom of the window uncheck the "**Allow inheritable permissions……**".
29.
30. Immediately a dialog box will popup asking whether you would like to copy the existing permissions to the folder OR completely remove them and start assigning the rights from scratch. Click "**Copy**".

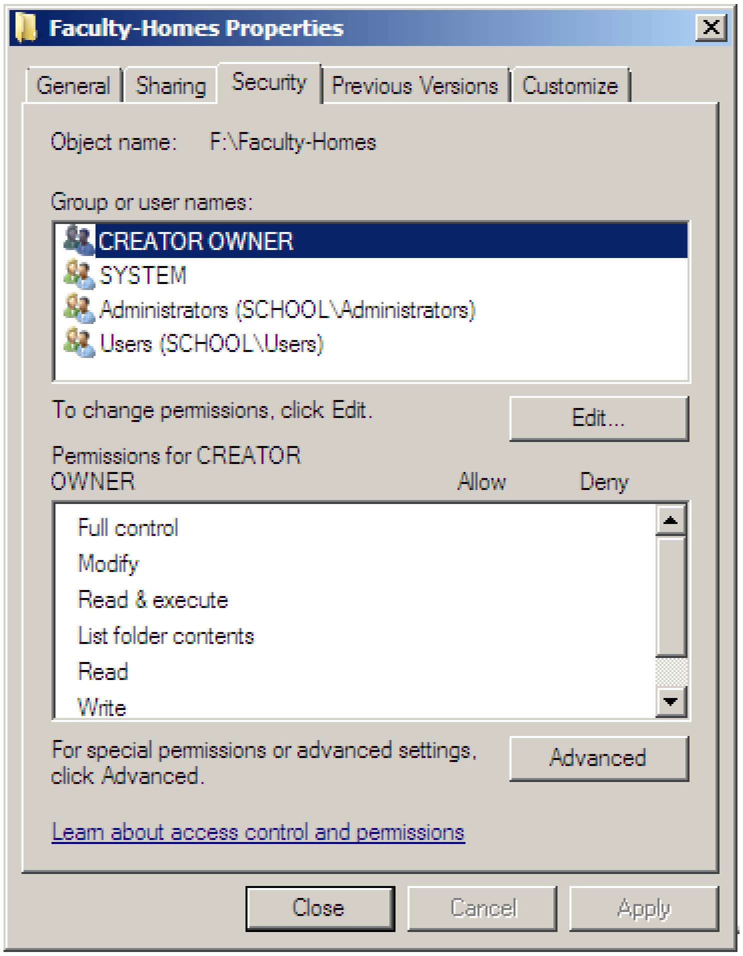


Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

31. Check the "**Replace permission entries…**", and then **Apply**.

32. Click **OK** two times to return to the **Faculty-Homes Properties** pop-up.
33. Your permissions to Faculty-Homes should now look like the following screen.



Object name: F:\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

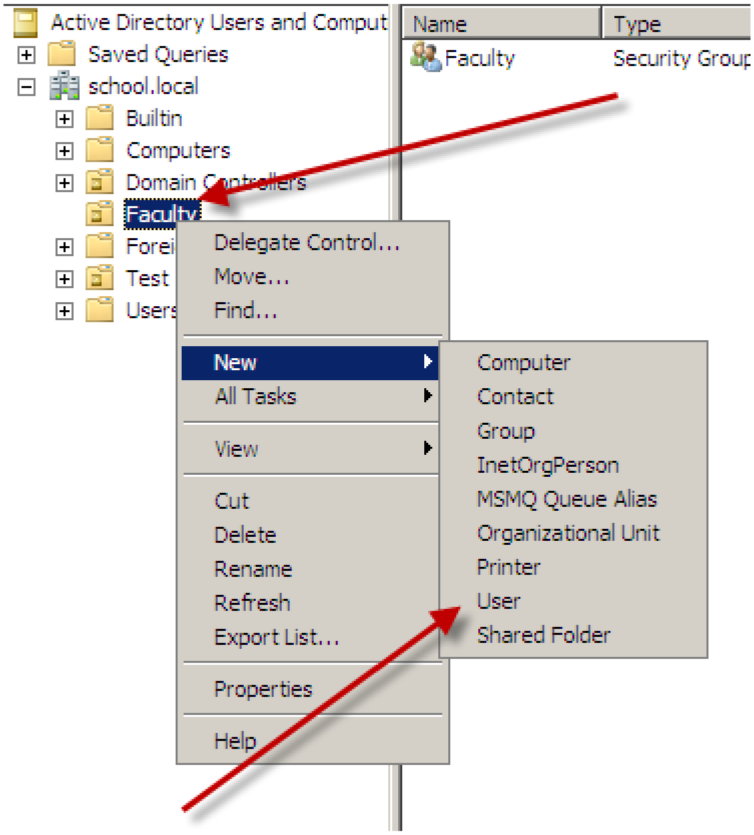
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

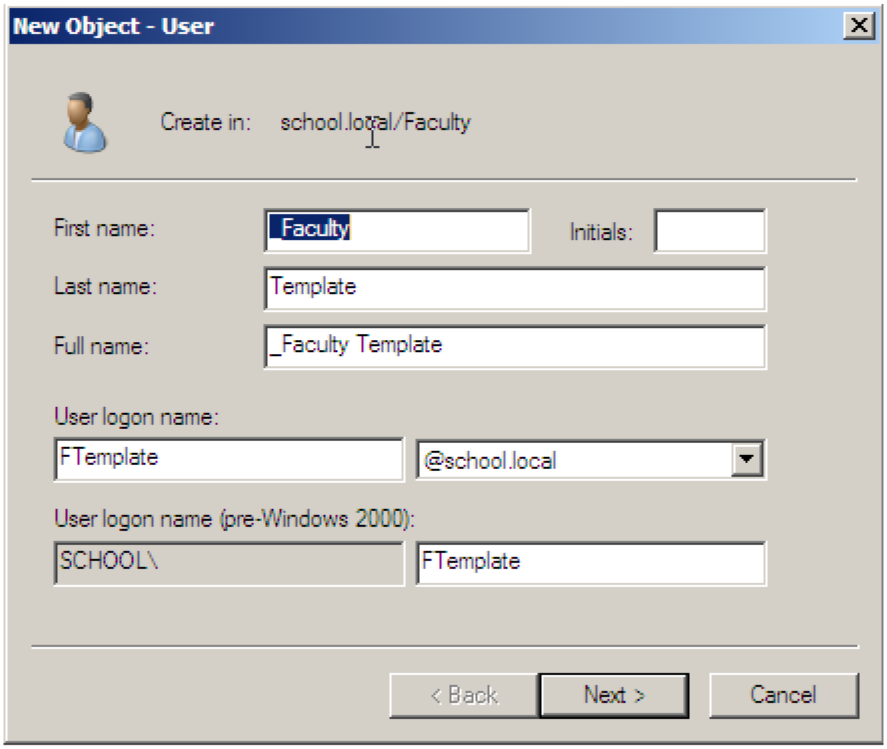
34. Click on the **Edit** button.
35. Remove all Groups from the top list except the Administrators group by selecting the respective group and clicking the Remove button.
36. Click on the **Add** button, enter **Domain Admins** and click **OK.**
37. Click on **Domain Admins**, and then check the **Full Control** under the **Allow** section. Click **Apply** and then **OK**.

Now that we have our network share setup to house the home directories, we can now create our user template.

38. Click **Start**, **Administrative Tools**, and then **Active Directory Users and Computers**.
39. Right click on the **Faculty** OU that was created using steps 1 through 3 of the **Basic AD Structuring for K12** section of this manual.
40. Click **New**, and then **User**.



41. In the information screen fill it out as shown in this screen and then click **Next**. If you place an underscore before the first name, your template will always be at the top of the list within its' Organizational Unit.



Create in: school.local/Faculty

First name: _Faculty

Initials:

Last name: Template

Full name: _Faculty Template

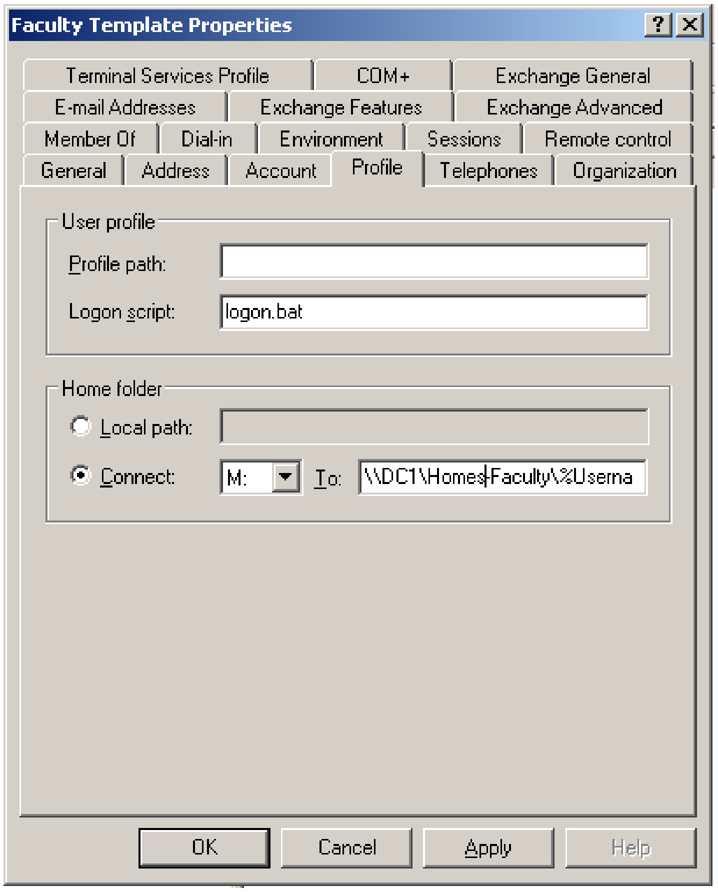
User logon name: FTemplate @school.local

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

42. Enter in a strong password for the template account. The password must meet the minimum password requirements.
43. Check **Account is disabled**. NOTE – You never want to have a template account enabled. **ALWAYS** disable template accounts.
44. Click **Next**.
45. If you are prompted to create an Exchange mailbox, uncheck the option to do so, click **Next** and then **Finish**.

Now that we have our template account in Active Directory, we need to finish configuring the account. We need to set the login script, home directory path, and make sure that this template is a member of the required security and distribution groups.

46. Right-click on the _**Faculty Template** account and click **Properties**.
47. Click on the **Member Of** tab.
48. Click Add.
49. In the **Select Groups** box, type **Faculty** and click **Check Names**. Add any additional security or distribution groups that this template may need.
50. Click **OK**.
51. Click on the **Profile** tab.
52. In the Logon Script text box, enter **logon.bat**.
53. Under the Home folder section, click the radio button next to **Connect**.
54. Select the drive letter that you wish to be mapped to users' home directories when they log in.
55. In the **To** text box enter **\\servername\Faculty-Homes$\%username%**.
56. Your screen should look like this.



Profile path:

Logon script: logon.bat

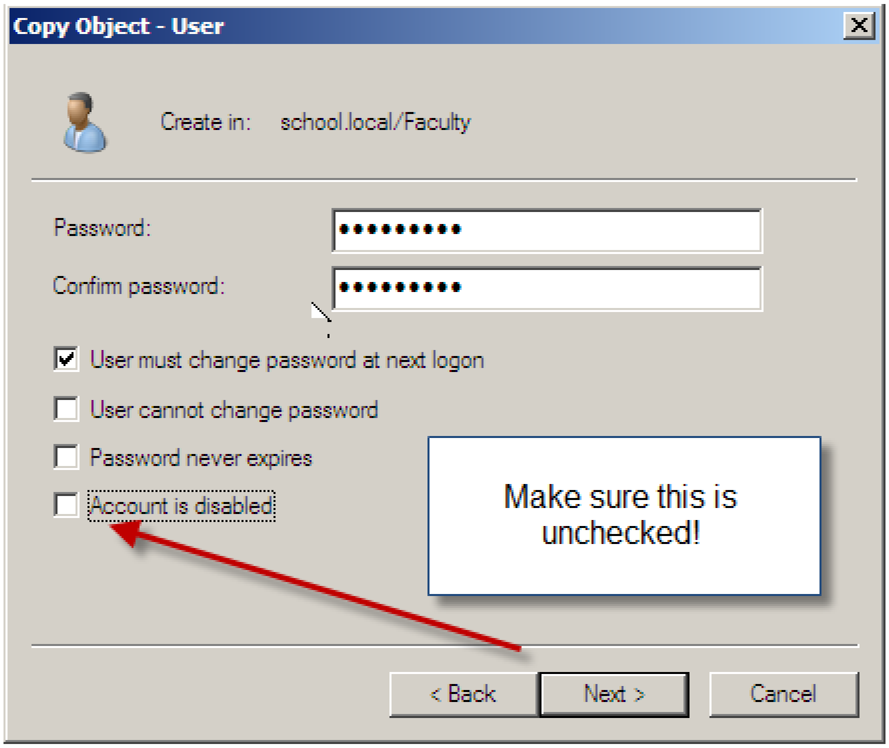
○ Local path:

● Connect: M: To: \\DC1\Homes\Faculty\%Userna

57. Click **Apply** and then **OK**. The %USERNAME% in the home directory path will automatically change to the login id of the user.

58. If you browse to **F:\Faculty-Homes**, you should see a newly created subfolder called **_FTemplate**.

The faculty user template is now complete. To create a new account based off of this template, right-click on the **_Faculty Template** account and click **Copy**. Be sure that when you are building the real user account; uncheck the **Account is disabled** box.



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

Make sure this is unchecked!

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 \\SERVER\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:

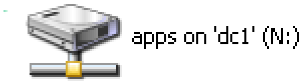
DO NOT ADD THE REM STATEMENTS

LOGON.BAT

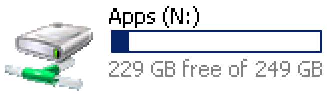
```
@ECHO OFF
NET USE N: /D                          REM Disconnects mapped N drive
NET USE O: /D                          REM Disconnects mapped O drive
NET USE P: /D                          REM Disconnects mapped N drive

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



After



Rename-Mapped-Drives.VBS

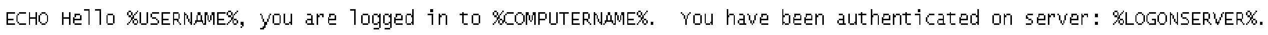
```
‘------Script Start
On Error Resume Next

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.

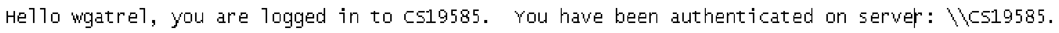
We placed the following command at the beginning to check and see if what type of OS is on the workstation that the user is logging in with by using the OS variable built into NT based clients.

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

Some of the other variables that are available are **LOGONSERVER**, **COMPUTERNAME**, and **USERNAME**. To use these in a command such as the one shown above, just surround it in percent signs. You can place commands like this either in your login script and you can also just run them from a DOS prompt to check the validity of your syntax.



```
ECHO Hello %USERNAME%, you are logged in to %COMPUTERNAME%.  You have been authenticated on server: %LOGONSERVER%.
```



```
Hello wgatrel, you are logged in to CS19585.  You have been authenticated on server: \\CS19585.
```

NOTE – All login scripts need to be placed in the NETLOGON folder of a domain controller. You can get to this folder by clicking on **Start**, **Run**, and typing **\\ServerName\NETLOGON** and clicking **OK**. Anything placed in this folder is replicated to ALL domain controllers.

Implementing Shadow Copies

A copy of the Shadow Copy Client can be downloaded from http://www.microsoft.com/technet/downloads/winsrvr/shadowcopyclient.mspx.

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 2003 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.

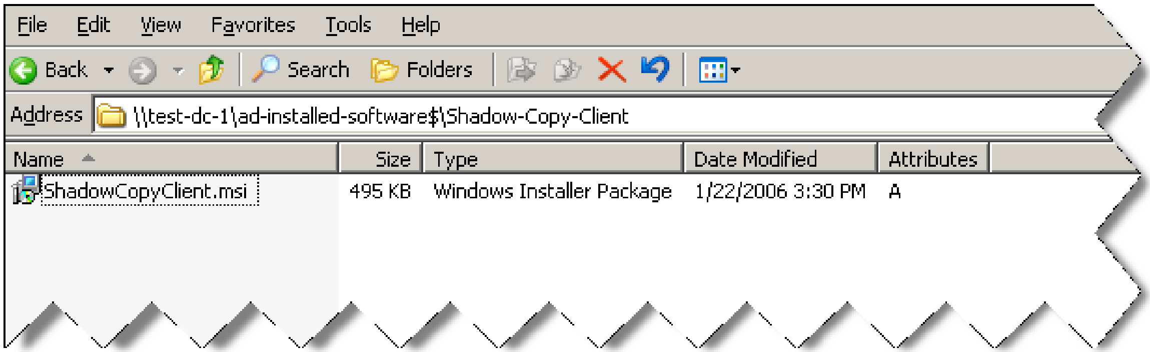
Important: Shadow copies do not eliminate the need to perform regular backups, nor do shadow copies provide protection from media failure. In addition, shadow copies are not permanent. As new shadow copies are taken, old shadow copies are purged when the size of all shadow copies reaches a configurable 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 configured.

Setup Shadow Copies

1. On the server go to My 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 volumes from the list and then click the **Enable** button.
5. If you are prompted with a box, click **OK.**
6. Click on the volume that you enabled Shadow Copies for then click the **Settings** button in the middle of the window.
7. Click the **Schedule** button.
8. By default a snapshot will be taken every day at 7AM & 12PM, M-F. Adjust the schedule to meet your district's needs.
9. Click **OK** twice to return to the Shadow Copies Settings window.
10. Click **OK** to return to My Computer.

Now that Shadow Copies has been enabled on the volumes, we must roll-out the Shadow Copies client to the workstations. Workstations must be at 2000 SP3 or above.

11. Follow the directions **Create Distribution Share** under the Deploying MS Office 2003 section to create the distribution share.
12. Under the \\Server\AD-Installed-Software$ folder, create a new folder called Shadow-Copy-Client and copy the downloaded MSI file into this folder.

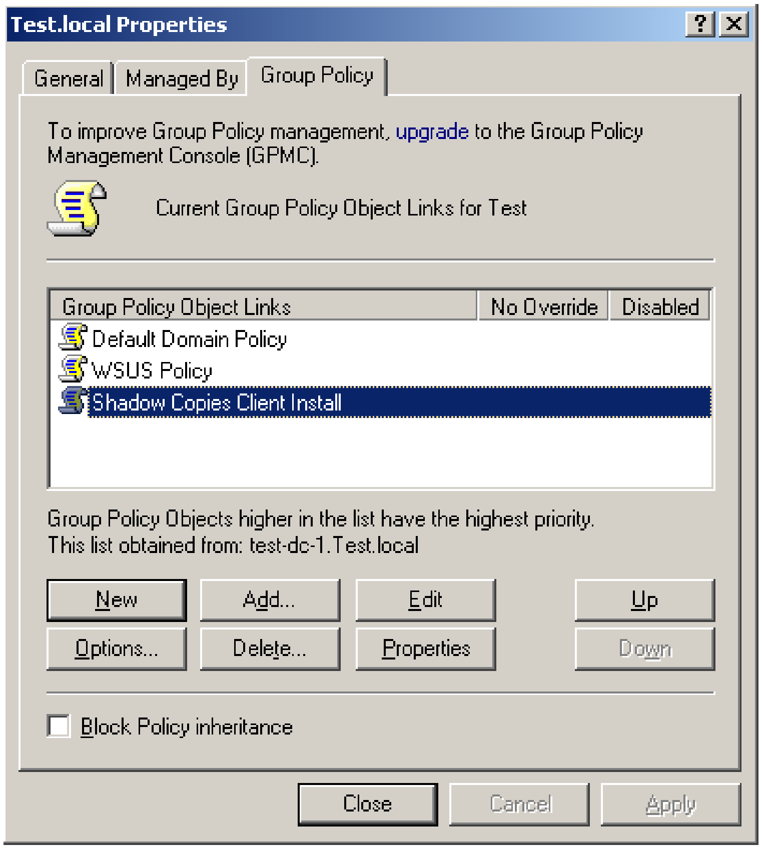


Address \\test-dc-1\ad-installed-software$\Shadow-Copy-Client

Name	Size	Type	Date Modified	Attributes
ShadowCopyClient.msi	495 KB	Windows Installer Package	1/22/2006 3:30 PM	A

Create Shadow Copies Client Software Distribution Policy

13. Right click on the OU where you would like to create the policy at and click **Properties**. If you are a single site, then you can place the policy at the top of the domain. If you are separate sites, then right click on the OU under District Computers that represents the site that you are creating the install policy for.
14. Click on the **Group Policy** tab and then click on the **New** button.
15. Name the new policy **Shadow Copy Client Install**.



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

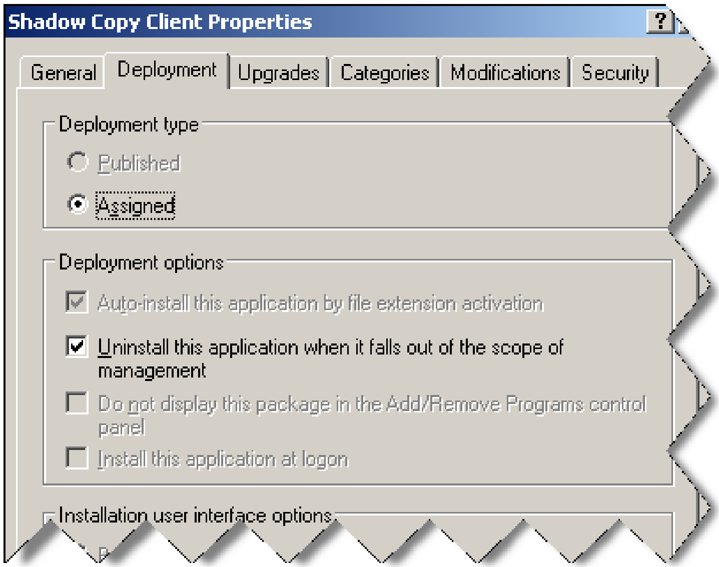
Current Group Policy Object Links for Test

Group Policy Object Links	No Override	Disabled
Default Domain Policy		
WSUS Policy		
Shadow Copies Client Install		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: test-dc-1.Test.local

□ Block Policy inheritance

16. Click once on the new policy and then click the **Properties** button.
17. Click on the **Security** tab.
18. Click the **Add** button.
19. In the entry box enter **Domain Computers** and then click **Check Names**. This should find the group in Active Directory and underline it in the box. If it does not find the group you will be prompted with a search box.
20. Double-click on the new policy to edit it.
21. Expand the **Computer Configuration** section.
22. Expand the **Software Settings** section.
23. Right click **on Software Installation** and then click **New**, **Package**.
24. In the Open box, for the file name enter \\servername\ad-installed-software$ and then click the **Open** button.
25. You should now see the Shadow-Copy-Client folder. Double click the folder to enter it.
26. Select the **ShadowCopyClient.MSI** file and then click the **Open** button.
27. At the **Deploy Software** window, select **Advanced** and then click **OK**.
28. Click on the **Deployment** tab and check the box next to **Uninstall this application when it falls out of the scope of management**.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☑ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

Installation user interface options

29. Click the **OK** button to return to the Group Policy Editor.
30. Select **File**, **Exit** to close the Group Policy Editor.
31. Click **Close** at the OU Properties window to return to Active Directory Users & Computers.

As the computers reboot and update their policies, the Shadow Copies Client will be automatically installed and available for use.

Implementing Volume Based Quota Limits

Quota limits are based off of volumes. Quota limits are a blanket setting, initially, for all users that save data on the volume. It is suggested that volumes containing Faculty & Student home directories be on their own each individual volumes. This will allow you to apply a larger quota limit to teachers, while having a smaller limit for your students.

1. Go to My Computer.
2. Right click on the volume that you want to enable quota limits on then click **Properties**.
3. Click on the **Quota** tab.
4. Check the box next to **Enable Quota Management.**
5. It is suggested that you enable **Deny Disk Space to Users Exceeding Quota Limit**.
6. Select the radio button next to **Limit disk space to**. Set the limit & warning level to meet your needs.
7. You can set the log options to meet your needs.
8. Click **Apply** and **OK**.

If you need to view users' current disk utilization, you can click on the Quota Entries button from within the window.

Implementing Directory Level Quota Limits using File Server Resource Manager

Install File Server Resource Manager

1. Open Server Manager and expand the **Roles** option.
2. Click on File Services in the left pane and select **Add Role Services** in the right-hand pane.
3. Select **File Server Resource Manager** and click **Install**.
4. When the wizard completes, click **Close**.

Configure Quota Templates

5. From Administrative Tools open the **File Server Resource Manager**.
6. Expand **Quota Management** in the left-hand pane and click on **Quota Templates**.
7. Under the **Actions** pane (far right) click **Create Quota Template**.
8. Enter a template name, such as **Faculty Home Directory Limits** or Student Home Directory Limits.
9. Enter the limit size and select either **Hard quota** or **Soft quota**.
10. If you wish to enable email notifications to either the user or network administrative staff, click on the **Add** button in the **Notification threshold** section.
11. Click **OK** to save the Quota Template.

Apply Quota Template to Directory

12. Under the Quota Management section of the left pane, click on **Quotas**.
13. In the **Action** pane (far right), click Create Quota.
14. Click the **Browse** button to select the directory that you wish to apply the quota limit to.
15. 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 would be useful for folders such as Yearbook Staff or Multimedia class where several people need to save to the same folder but you want to limit the total amount of space.

    A**uto apply template and create quotas on existing and new subfolders** – This will apply the template to the subfolders within the parent folder. This would be useful for applying limits on home directory folders. 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.

16. On the **"Derive properties…"** option, select the Quota Template from the drop-down menu and click **Create**.

Once the folders start collecting data, you can start adjusting the individual folder quotas as needed by double-clicking on the Quota shown in the list.

WINS Setup

The first thing that needs to be done is to make sure that WINS & DHCP Services are installed.

1. Open the Server Manager and select the **Features** option on the left pane.
2. In the right-hand pane, click **Add Features**.
3. On the Select Features window check the **WINS Server** option and click **Next**.
4. On the **Confirm Installation Selections** screen, click **Install**.
5. At the **Installation Results** screen, click **Close** to end the wizard.
6. Add the WINS IP addresses to each respective network cards in all servers. If your WINS server has a Public and Private network adapter, use the respective IP address for the same subnet on the public and private network adapters on each server.

   Multiple WINS Servers – Set WINS DB Replication

7. From Administrative Tools open the **WINS** Manager.
8. Expand the respective WINS Server and click on **Replication Partners**.
9. Right-click Replication Partners and select **New Replication Partner**.
10. Enter the respective server name that will be replicating with this WINS server.
11. Once the server is added to the replication partner list, close the WINS manager.

DHCP Setup

1. Open the Server Manager and select the **Roles** option.
2. In the right-hand pane, click **Add Roles**. On the **Before You Being** click **Next**.
3. Select the **DHCP Server** role and click **Next**.
4. On the **Intro to DHCP Server** screen click **Next**.
5. Select the IP address that you will be issuing IP addresses on and click **Next**.
6. Enter your Active Directory domain name and internal DNS server IP addresses for the same IP range as the DHCP scope and click **Next**.
7. Select WINS is required for applications on this network, enter in the respective WINS server IP addresses for the DHCP subnet and click **Next**.
8. Click on the Add button to create the initial IP Scope (Range) for the server to server.
9. Enter the DHCP Scope Name and respective network information. It is recommended that if your IP range is 10.10.10.0 to 10.10.11.255, that you enter 10.10.10.51 for the Starting IP Address and 10.10.11.250 for the Ending IP Address. This will leave 50 IP's at the beginning of your IP range for static assignment and four at the end. Once the information is filled out, click **OK** (the scope will be added to the Scope list) and then click **Next**.
10. On the **Configure DHCPv6 Stateless Mode**, select the **Disable DHCPv5 stateless mode for this server** option and click **Next**.
11. On the **Authorize DHCP Server** screen, click **Next**.
12. Click **Install** to complete the wizard. When the wizard is complete, click **Close**.
13. From Administrative Tools, open the **DHCP** Management Console.
14. Expand the DHCP server, right-click **IPv4** and select **Properties**.
15. For the **Conflict Detection Attempts**, change this value to **3** and click on the **Bindings** button.
16. Verify that the only network adapter DHCP is answering on is the adapter that is in the same subnet that DHCP is serving IP addresses for.
17. Click Apply and OK to return to the DHCP Management Console.

18. Right-click the respective DHCP server, select **All-Tasks** > **Restart**.
19. Once the DHCP Service has restarted, close the DHCP Management Console.

Windows Server Update Services (WSUS)

NOTE: You must have at least 6GB of free space to store updates locally.

Microsoft Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to Microsoft Windows Server 2000, Windows Server 2003, and Windows XP operating systems. 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.

How Windows Server Update Services Works

Windows Server Update Services is a patch and update component of Windows Server and offers an effective and quick way to help keep systems up to date. Windows Server Update Services provides a management infrastructure consisting of the following:

Microsoft Update: The Microsoft Web site that Windows Server Update Services components connect to for updates to Microsoft products.

Windows Server Update Services server: The server component that is installed on a computer running a Windows 2000 Server with Service Pack 4 (SP4) or Windows Server 2003 operating system inside the corporate firewall. Windows Server Update Services server provides the features that administrators need to manage and distribute updates through a Web-based tool, which can be accessed from Internet Explorer on any Windows computer in the corporate network. In addition, a Windows Server Update Services server can be the update source for other Windows Server Update Services servers.

Automatic Updates: The client computer component built into Windows 2000 with SP3, Windows XP, and Windows Server 2003 operating systems. Automatic Updates enables both server and client computers to receive updates from Microsoft Update or from a server running Windows Server Update Services.

For Windows Server 2003, WSUS requires the following:

- Microsoft Internet Information Services (IIS) 6.0
- Background Intelligent Transfer Service (BITS) 2.0. To obtain this software, see the Download WSUS page.
- Microsoft .NET Framework 1.1 Service Pack for Windows Server 2003. You can also obtain this software from the Windows Update site: Scan for Critical Updates and Service Packs. Install Microsoft .NET Framework 1.1 Service Pack 1 for Windows Server 2003.
- 1GB of free space on system partition.

For Windows 2000 Server, WSUS requires the following:

- IIS 5.0
- BITS 2.0. To obtain this software, see the Download WSUS page.
- Database software that is fully compatible with SQL Server. Microsoft recommends MSDE 2000 Release A.
- Microsoft Internet Explorer 6.0 SP1
- .NET Framework 1.1 Redistributable Package
- .NET Framework 1.1 SP1. You can also obtain this software from the Windows Update site: Scan for Critical Updates and Service Packs. Install Microsoft .NET Framework 1.1 Service Pack 1 for Windows 2000 Server.
- 1GB of free space on system partition.

Windows Software Update Services (WSUS)

NOTE: 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.

Installing Prerequisites Roles

1. Download and install Microsoft Report Viewer 2005 Redistributable.
2. Open Server Manager and click the **Roles** option.
3. Select **Add Roles**.
4. Select **Windows Server Update Services** and click **Next**.
5. On the **Web Services (IIS)** screen click **Next**.
6. On the **Select Role Service** screen select the additional following items and click **Next**. If you are prompted for additional services to be installed, click **Yes**.
   - -Common HTTP Features
     - **Directory Browsing**
     - **HTTP Errors**
   - -Application
     - **ASP**
     - **CGI**
   - -Security
     - **Basic Authentication**
   - -Management Tools
     - **SELECT ALL CHILD ROLE SERVICES**
7. Click **Install** to complete the wizard.
8. Click **Next** on the Welcome Wizard. The wizard will automatically download the latest version of WSUS and the install will start when the download is completed.
9. When prompted, agree to the licensing terms of WSUS and click **Next**.
10. Enter the path that WSUS will use to store the updates locally on the server and click **Next**.
11. On the Database Options screen, verify that **Install Windows Internal Database on this computer** is selected and click **Next**.
12. For the Web Site Selection Screen, select **Create a Windows Server Update Services Web site** and click **Next**. There will be a specific port number listed, WRITE THIS DOWN for the Group Policy configuration.
13. Click **Next** to start the Installation process.

Configuring WSUS after Installation

14. On the **Before you begin** screen, click **Next**.
15. Uncheck the option for the **Microsoft Update Improvement Program** and click **Next**.
16. Select the respective upstream server for this WSUS Server and click **Next**. If you are synchronizing from another WSUS server from within your district, be sure to enter the proper port number that WSUS is running on remotely.
17. Click **Next** on the **Proxy Server** settings, unless these settings are required for your environment.

18. Click the Start Connecting button to retrieve the updated list of products that WSUS currently updates.
19. When the initial product file download is completed, click the **Next** button.
20. Verify that **English** is the selected language and click **Next**.
21. On the **Products** selection, choose the products that you will be updating in your environment and click **Next**.
22. For the **Update Classifications** to download, select everything **<u>except</u>** Drivers and click **Next**.
23. **<u>Uncheck</u>** the **Begin initial synchronization** box and click **Finish.**
24. From Administrative Tools open the **Microsoft Windows Server Update Services** Management console.
25. In the left-hand pane, expand your WSUS Server and click **Options**. It should be at the bottom of the list.
26. 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**. 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.
27. In the Options pane, select **Synchronization Schedule**.
28. Select **Synchronize automatically** and set this to off-peak usage hours (after school hours) and click **OK**.

Automatic Approvals – aka "If Microsoft puts it out, deploy it!"

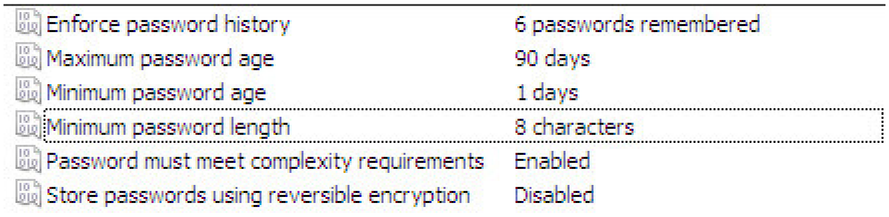
29. In the Options pane, select **Automatic Approvals**.
30. Select the **Default Automatic Approval Rule** and click **Edit**.
31. In the Step 2 box, click on **Critical Updates, Security Updates** (highlighted in blue).
32. Select all classification items **<u>EXCEPT</u>** drivers and click **OK**. Some districts choose not to select Feature Packs. This includes items such as Silver Light and Desktop Search.
33. Verify that **Default Automatic Approval Rule** <u>is checked</u> and click **Apply** AND **OK**.

Group Policy

Enforcing K12 State Security Policies for ACT723 through Group Policies

Setting Non-Student (Faculty) Password Requirements

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



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

7. Close the Group Policy Editor.

Setting Student Password Requirements using Fine-grained password policies.

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

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

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

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

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

Retain Security Event Log for 90 Days

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

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

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

Close the Group Policy Editor

Security Event Auditing – Security Event Log Contents

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

Logon Banner

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

Locking Screen Saver

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

Create the WSUS Group Policy

1. Open Active Directory Users & Computers.
2. Right click on the OU where you would like to create the policy at and click **Properties**. If you are a single site, then you can place the policy at the top of the domain. If you are separate sites, then right click on the OU under District Computers that represents the site that you are creating the install policy for.
3. Click on the **Group Policy** tab and then click on the **New** button.
4. Name the new policy **WSUS Policy**.
5. Expand **Policies**
6. Double-click on the WSUS Policy to open the Group Policy Editor.
7. Expand **Computer Configuration**, **Administrative Templates**, **Windows Components**. Click on **Windows Update**.
8. In the right hand pane double click on **Configure Automatic Updates**.
9. Select the radio button next to **Enabled**.
10. In the Configure automatic updating drop-down menu, select option **4.**
11. Set the desired scheduled install day and time.
12. Click the **Next Setting** button.

    You should now be at the **Specify Intranet Microsoft Update Services Location** window.
13. Select the radio button next to **Enabled**.
14. In both entry boxes enter http://yourservername and then click **OK.**
15. Double-click on **Reschedule Automatic Updates Scheduled Installations**.
16. Select the radio button next to **Enabled**.
17. Change the minutes from 1 to 5.
18. Click the **Next Setting** button.
    You should now be at the **No auto-restart for scheduled Automatic Updates installations** window.
19. Select the radio button next to your desired option.
20. Click the **Next Setting** button.
    You should now be at the **Automatic Updates detection frequency** window.
21. Select the radio button next to **Enabled**.
22. Set the desired interval.
23. Click the **Next Setting** button.
    You should now be at the **Allow Automatic Updates immediate installation** window.
24. Select the radio button next to **Enabled** and then click the **Next Setting** button.
25. Click **OK** to return to the Group Policy Editor.

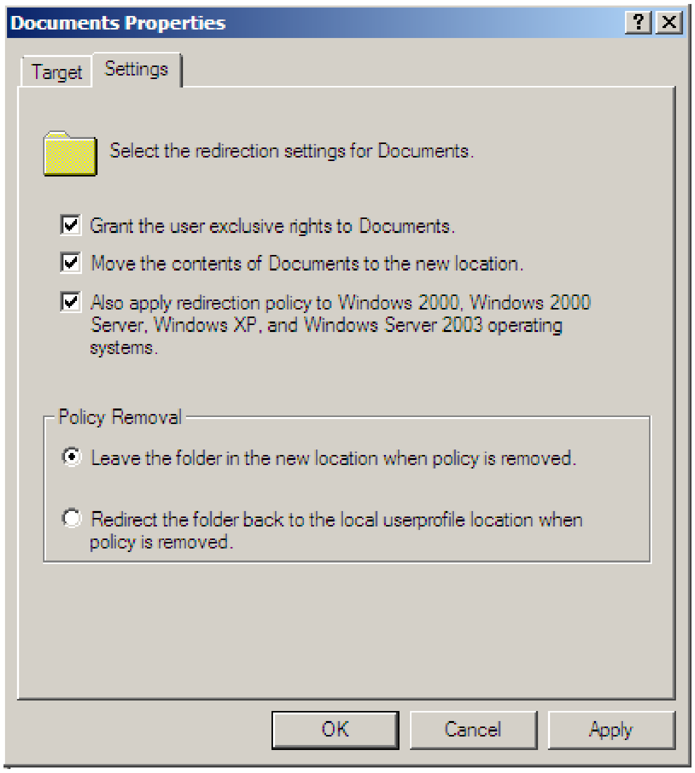
26. Click **File** and then **Exit** to return to Active Directory Users & Computers.
27. Click **Close** at the properties window and then close the Active Directory Users & Computers

Common K12 Group Policies

Redirect ‘My Documents’ to User’s Home-Directory

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

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



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.

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

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

Restrict Computers to Faculty Use Only

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

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

1. Open Active **Directory Users and Computers** (ADUC)
2. Create a security group called "**Faculty Use Only Computers**" in the OU of your choice. It is recommended that this policy be placed on the parent OU that your workstation computer accounts reside in.
3. Click **Start**, **Administrative Tools**, and then open **Group Policy Management**.
4. Expand Forest: **yourdomain.local.**
5. Expand Domains and then expand **yourdomain.local**.
6. Right-click yourdomain.local and select **Create a GPO in this domain, and link it here**.
7. Name the policy **Faculty Use Only Computers** and click **OK**.

8. In the left-hand pane, click on the new policy and click on the Scope tab in the right-hand pane.
9. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
10. Click the **Add** button.
11. In the box enter the group name "**Faculty Use Only Computers**" and then click the **OK** button.
12. Click on the **Settings** tab and set **GPO Status** to **User Configuration Settings Disabled**.
13. In the left-hand pane, right-click the policy to open the **Group Policy Object Editor**.
14. Expand **Computer Configuration**.
15. Expand **Windows Settings**.
16. Expand **Security Settings**.
17. Expand **Local Policies**.
18. Click on **User Rights Assignment**.
19. In the right-hand window, double-click on "**Allow log on locally**".
20. In the properties window, place a check in the "**Define these policy settings**" box.
21. Click the **Add User or Group** button.
22. Add **Domain Admins**, **Administrators**, and **Faculty** to the list. When finished click **Apply** and **OK**.
23. Click **OK** to close the properties window for the Domain.
24. Add computers to the **Faculty Use Only Computers** security group to apply the policy. A reboot is required after the computer is added to and removed from the group to enforce/remove the policy.

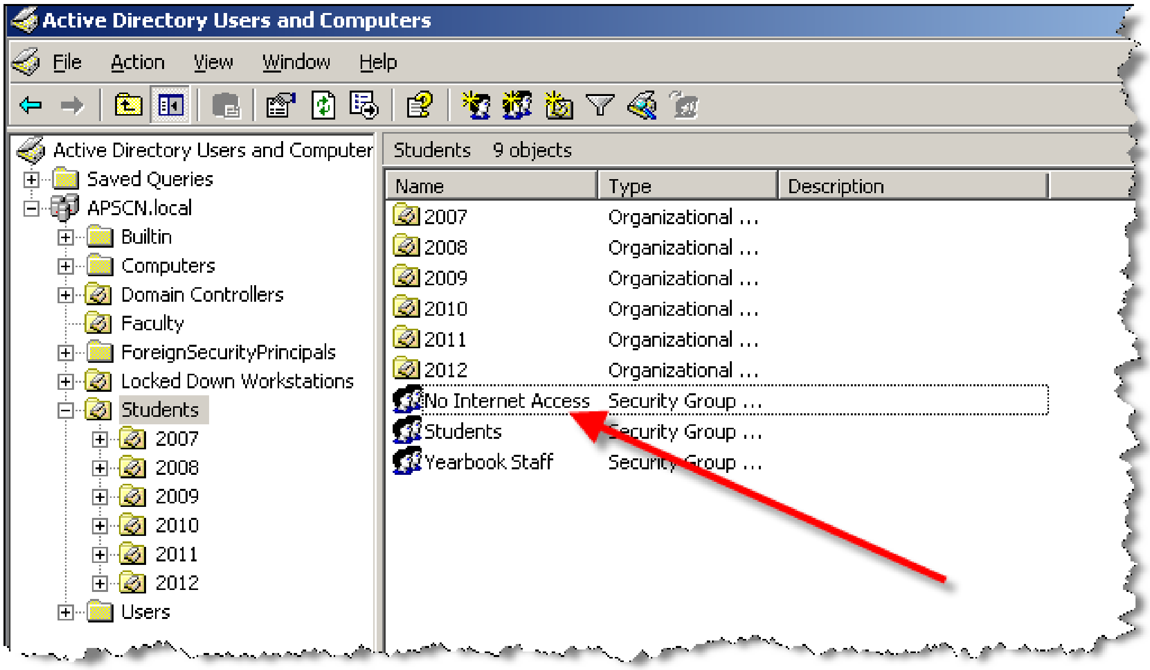
Disable Internet Access by Group Policy/Security Group

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

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

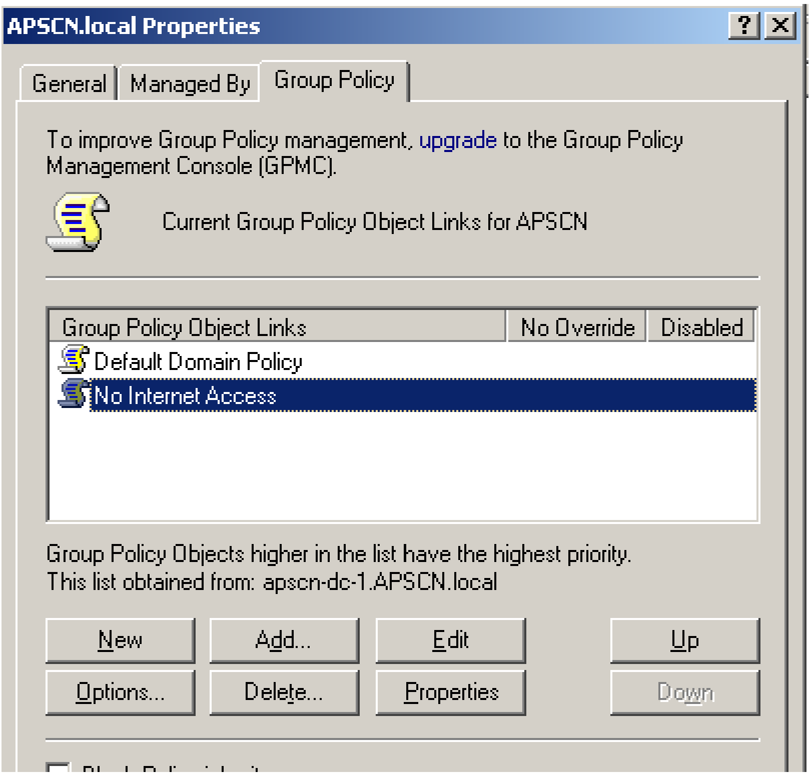
If Internet Information Services (IIS) are not installed, please see the IIS & Certificate Services installation section. IIS needs to be installed before proceeding.

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



Name	Type	Description
2007	Organizational ...	
2008	Organizational ...	
2009	Organizational ...	
2010	Organizational ...	
2011	Organizational ...	
2012	Organizational ...	
No Internet Access	Security Group ...	
Students	Security Group ...	
Yearbook Staff	Security Group ...	

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


APSCN.local Properties

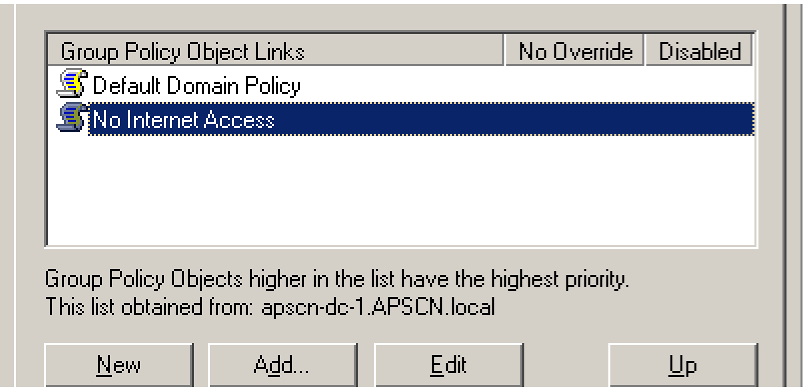
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for APSCN

Group Policy Object Links	No Override	Disabled
Default Domain Policy		
No Internet Access		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: apscn-dc-1.APSCN.local

5. Click on the **Properties** button. When the Properties window comes up, select the **Security** tab.
6. Select **Authenticated Users** from the list and then click the remove button.
7. Select **Domain Admins** from the list. In the permissions section, check the **Deny** option next to Apply Group Policy.
8. Click the **Add** button. Enter "**No Internet Access**" in the entry box and then click **OK**.
9. Select **No Internet Access** from the user list.
10. Check the **Allow** option next to Apply Group Policy from the options in the permissions window.
11. After the permissions are set, click **Apply** and then **OK**.
12. Select the No Internet Access policy from the list and then click Edit.



Group Policy Object Links	No Override	Disabled
Default Domain Policy		
No Internet Access		

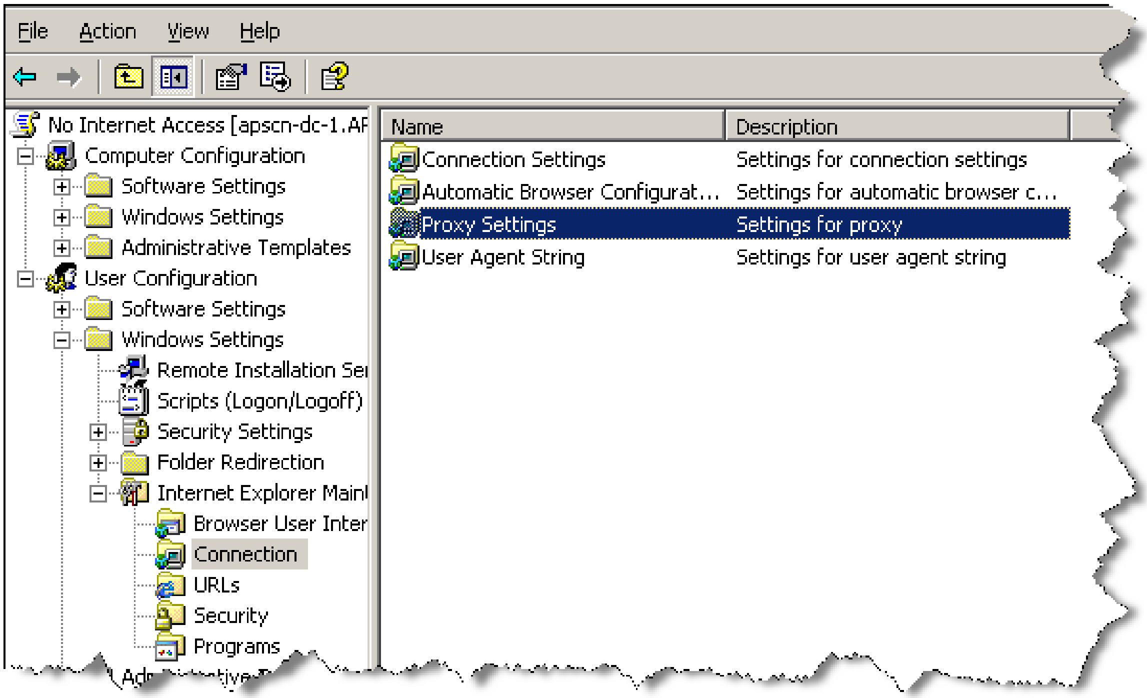
Group Policy Objects higher in the list have the highest priority.
This list obtained from: apscn-dc-1.APSCN.local

13. Expand **User Configuration**.

14. Expand **Windows Settings**.

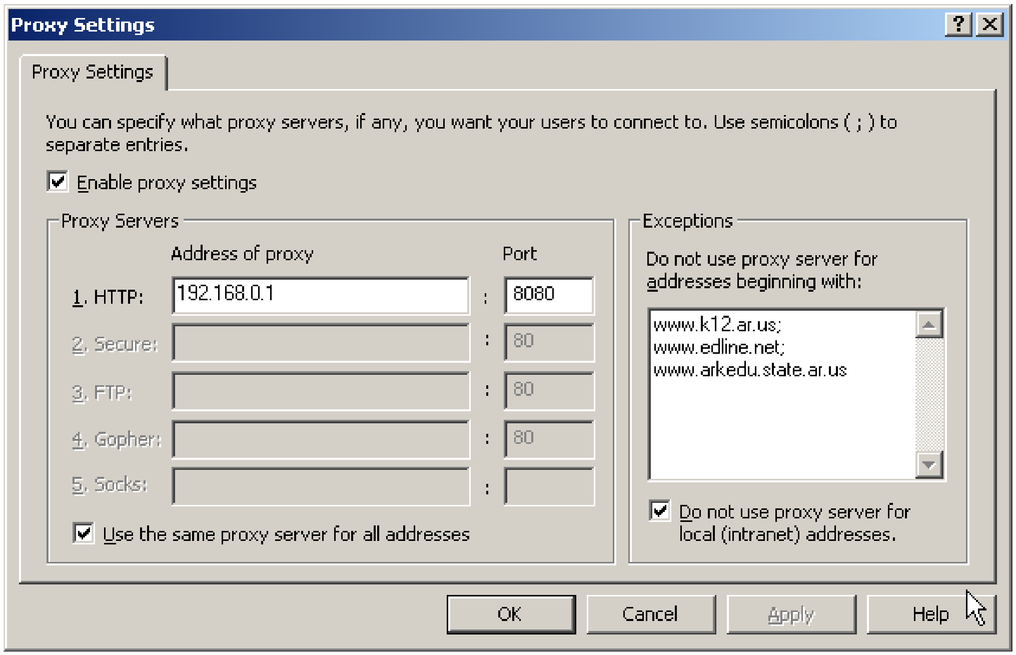
15. Expand **Internet Explorer Maintenance**.

16. Select the **Connection** section and double click on "**Proxy Settings**" in the right window pane.



Name	Description
Connection Settings	Settings for connection settings
Automatic Browser Configurat...	Settings for automatic browser c...
Proxy Settings	Settings for proxy
User Agent String	Settings for user agent string

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



You can specify what proxy servers, if any, you want your users to connect to. Use semicolons (;) to separate entries.

☑ Enable proxy settings

	Address of proxy	Port
1. HTTP:	192.168.0.1	8080
2. Secure:		80
3. FTP:		80
4. Gopher:		80
5. Socks:		

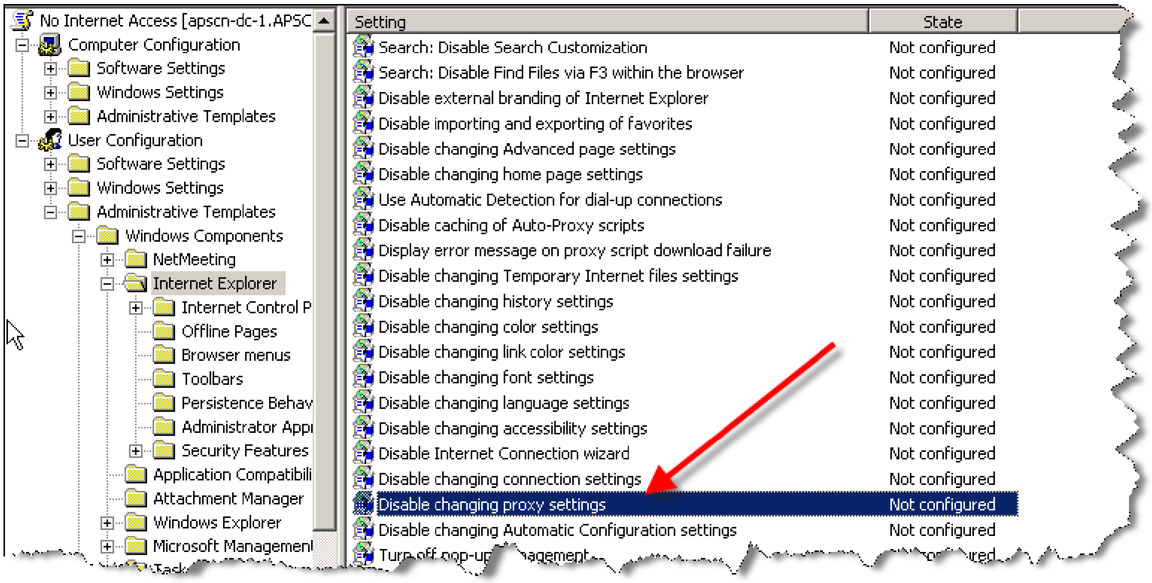
☑ Use the same proxy server for all addresses

Do not use proxy server for addresses beginning with:

www.k12.ar.us;
www.edline.net;
www.arkedu.state.ar.us

☑ Do not use proxy server for local (intranet) addresses.

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



Setting	State
Search: Disable Search Customization	Not configured
Search: Disable Find Files via F3 within the browser	Not configured
Disable external branding of Internet Explorer	Not configured
Disable importing and exporting of favorites	Not configured
Disable changing Advanced page settings	Not configured
Disable changing home page settings	Not configured
Use Automatic Detection for dial-up connections	Not configured
Disable caching of Auto-Proxy scripts	Not configured
Display error message on proxy script download failure	Not configured
Disable changing Temporary Internet files settings	Not configured
Disable changing history settings	Not configured
Disable changing color settings	Not configured
Disable changing link color settings	Not configured
Disable changing font settings	Not configured
Disable changing language settings	Not configured
Disable changing accessibility settings	Not configured
Disable Internet Connection wizard	Not configured
Disable changing connection settings	Not configured
Disable changing proxy settings	Not configured
Disable changing Automatic Configuration settings	Not configured
Turn off pop-up [illegible]	[illegible]

22. Expand **Windows Components**, **Internet Explorer**.
23. Select the **Enabled** option and then click the **OK** button.
24. Close the Group Policy Editor.
25. Click the Close button to close the *Domain*.Local Properties Window.

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

Deploying MS Office 2003 via Group Policy

Deploying Office and maintaining the license count can be a daunting task. Using this method of deployment, you will be able to automatically install and maintain all licenses for Office on all 2000/XP workstations.

NOTE: You will need to do this process on a server at each physical site that is behind a router. The reason is that you do not want computers at one campus going across the WAN to install MS Office.

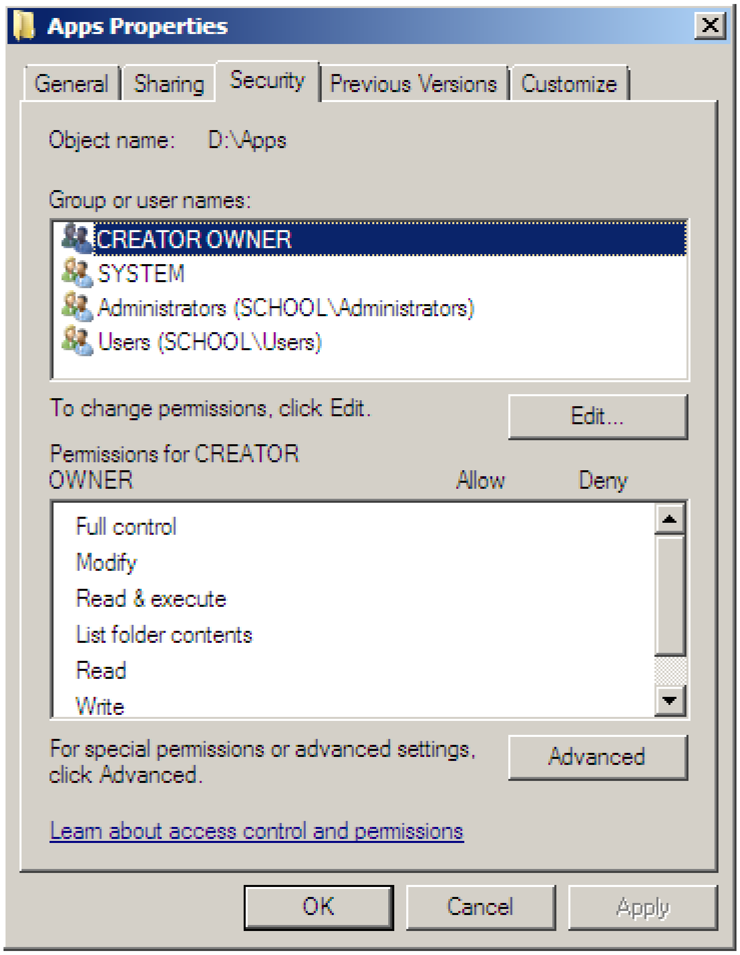
Setup Summary

- Create Distribution Share
- Administrative Setup Point of Microsoft Office
- Download & Install 2003 Office Resource Kit – Customized Installation Wizard http://www.microsoft.com/office/orkarchive/2003ddl.htm
- Create Customized Installation (MST) File
- Create "Licensed Office 2003 Installs" Security Group
- Create "MS Office – Automated Install" Group Policy
- Assign Computers to "Licensed Office 2003 Installs" Security Group

Create Distribution Share

1. Create a new folder on the **Data** volume/partition called "**AD-Installed-Software**".
2. Right click on the **AD-Installed-Software** folder and click **Properties**.
3. Select the **Security** tab and click the **Advanced** button.

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



Object name: D:\Apps

Group or user names:

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

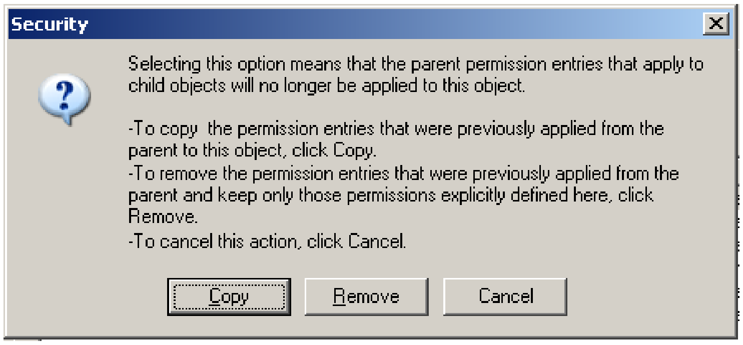
To change permissions, click Edit.

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

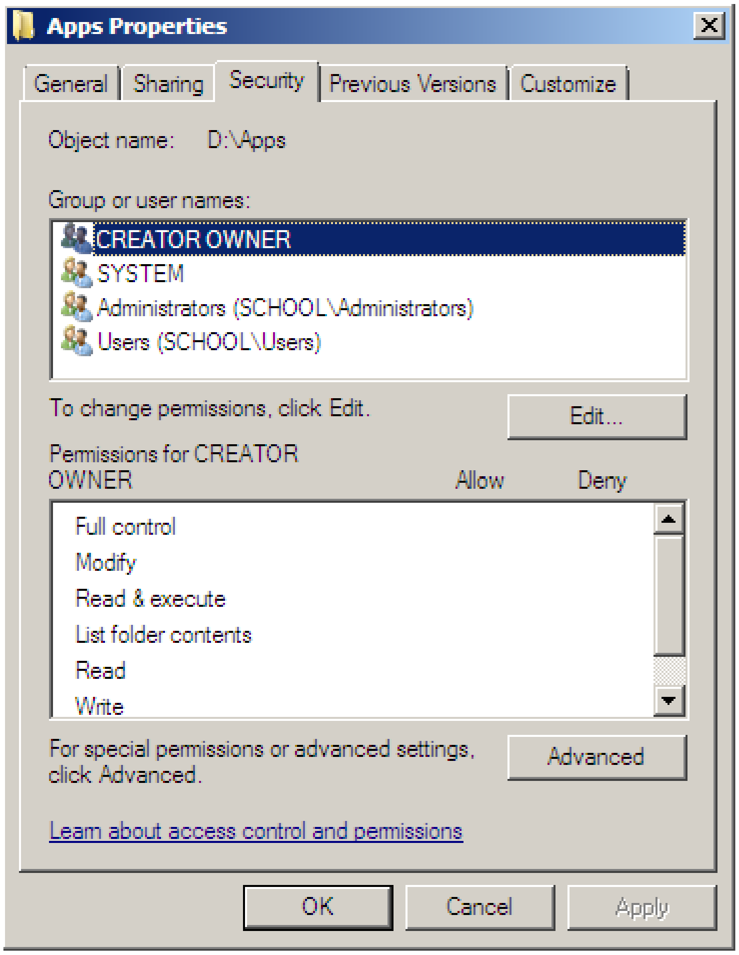
4. Click on the **Security** tab, then the **Advanced** button.
5. On the Permissions tab, select the **Edit** button.
6. In the bottom of the window uncheck the "**Allow inheritable permissions……**" option.
7. Immediately a dialog box will popup asking whether you would like to copy the existing permissions to the folder OR completely remove them and start assigning the rights from scratch. Click "**Copy**".



Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

8. Check the "**Replace permission entries…**", and then **Apply**.
9. Click **OK** two times to return to the **AD-Installed-Software Properties** pop-up.
10. Your permissions to **AD-Installed-Software** should now look like the following screen.



Object name: D:\Apps

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

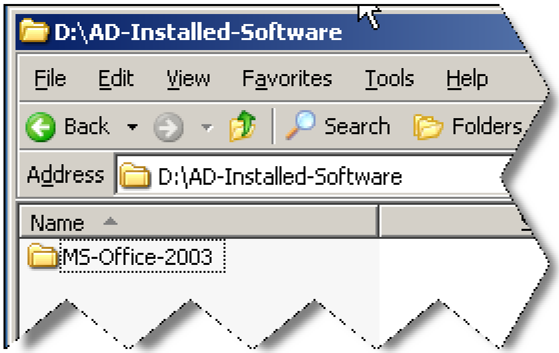
For special permissions or advanced settings, click Advanced.

11. Click on the **Edit** button.
12. Remove all Groups from the top list except the Administrators group by selecting the respective group and clicking the Remove button.
13. Click on the **Add** button, enter **Domain Admins** and click **OK.**
14. Click on **Domain Admins**, and then check the **Full Control** under the **Allow** section.

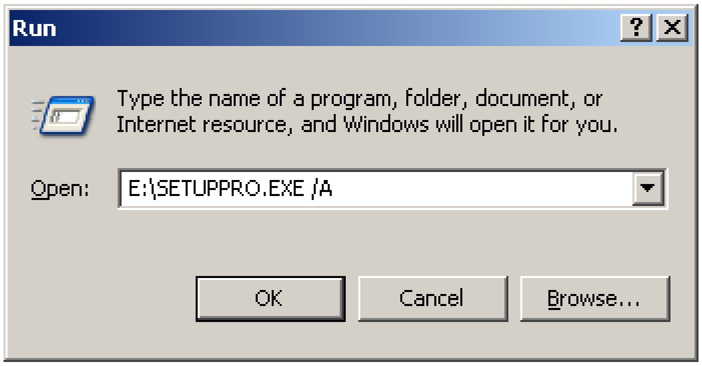
15. Click on the **Add** button, enter **Domain Users and Domain Computers** (separated by a semicolon) and click **Check Names** to verify the groups.
16. Click OK to return to the **Permissions** window.
17. Select Domain Computers and Domain users from the group list and select **Allow** for **Read & execute**.
18. Select on the **Sharing** tab and click the **Advanced Sharing** button.
19. Select the **Share this folder** check box.
20. For the share name type **AD-Installed-Software$**.
21. Click on the **Permissions** button.
22. Click on **Everyone** and click **Remove**.
23. Click **Add**.
24. In the name box enter **Domain Admins**, **Administrators, Domain Users** and **Domain Computers,** each seperated by a semi-colon. Click the **Check Names** button and then **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.
25. Give **Domain Admins** and **Administrators** both **Full Control**.
26. Give the **Domain Computers** and **Domain Users** group both **Read** rights, they will receive Read automatically.
27. Click on the **Caching** button. Select **Files or programs from this share will not be available offline**. It is NOT recommended to allow offline file-caching for any network shares that house database applications such as WinCAGI, MealTracker and RenLearn products, for example.
28. Click **OK**, **Apply**, and then **OK** until all property windows are closed.

Administrative Setup Point of Microsoft Office 2003

1. In the AD-Installed-Software folder create a new folder called **MS-Office-2003**.



2. Insert your MS Office 2003 CD-Rom. If it Auto Run starts, close out all instances.
3. Click on Start, Run, and Browse. Look for SETUPPRO.EXE in the root of the CD-Rom drive. Click the file **<u>ONCE</u>** and then click **Open**.
4. In the run prompt you should add a /A to the end of the command. This will allow us to create an administrative install point on the server.



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

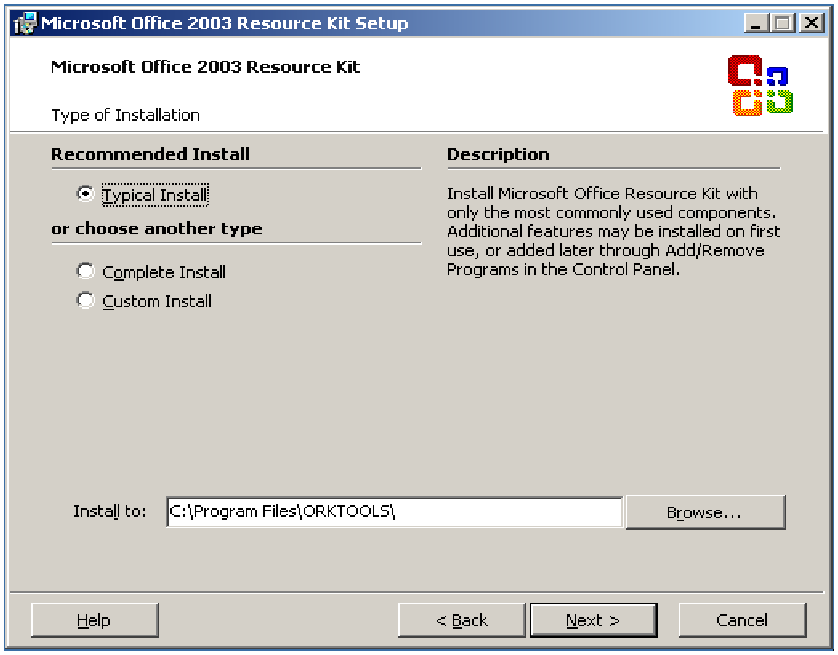
E:\SETUPPRO.EXE /A

5. Click **OK** to start the install.
6. Enter the Name for you school district in the Organization box.
7. For the Install Location, browse to the MS-Office-2003 folder that was created in step 19.
8. Enter your Product Key received with your MS Office 2003 License.
9. Click **Next** to proceed with the install.
10. On the EULA screen, check the acceptance box at the bottom left and then click the **Install** button. When the process is complete click the **OK** button.

At this point we are only copying the MS Office 2003 install files to the server. We will now install the Custom Installation Wizard. This will allow you to choose what you want installed on the workstations and will auto-configure Outlook to attach to your server.

Download & Install 2003 Office Resource Kit – Custom Installation Wizard

11. Go to http://www.microsoft.com/office/orkarchive/2003ddl.htm and download the Office 2003 Editions Resource Kit. Save the file to the Desktop.
12. After the download is complete. Double click to start the install.
13. On the EULA screen, check the acceptance box at the bottom left and then click the **Next** button.
14. At the **Type of Installation** screen take the defaults and click **Next** to continue.



Microsoft Office 2003 Resource Kit

Type of Installation

Recommended Install

● Typical Install

or choose another type

○ Complete Install

○ Custom Install

Description

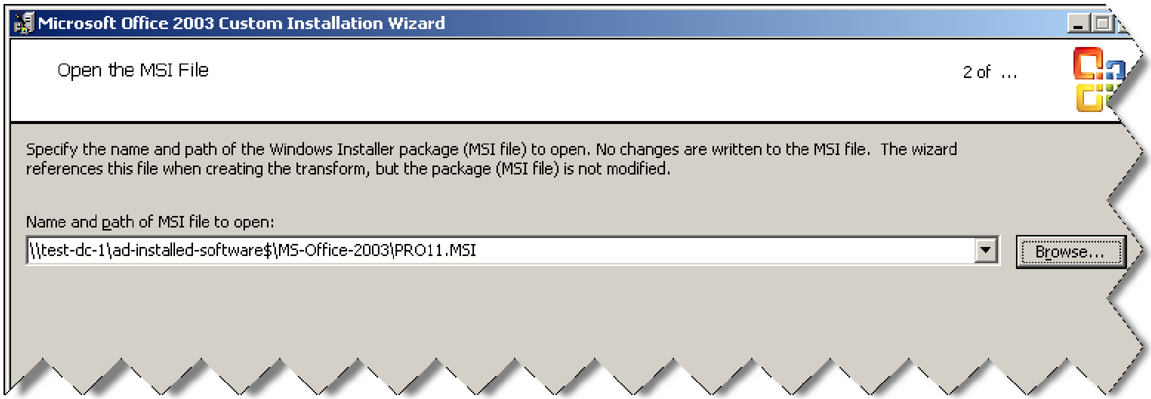
Install Microsoft Office Resource Kit with only the most commonly used components. Additional features may be installed on first use, or added later through Add/Remove Programs in the Control Panel.

Install to: C:\Program Files\ORKTOOLS\

15. Click the **Install** button to complete the install. When the process is complete click the **OK** button.

Create Customized Installation (MST) File

16. Click on Start, Run, All Programs, Microsoft office, Microsoft Office 2003 Resource Kit, **Custom Installation Wizard**. Take note of the screen number at the upper right corner of the windows.
17. At the beginning screen click **Next** to continue.
18. Enter in the UNC path name to the PRO11.MSI file within the MS-Office-2003 folder, as seen below.



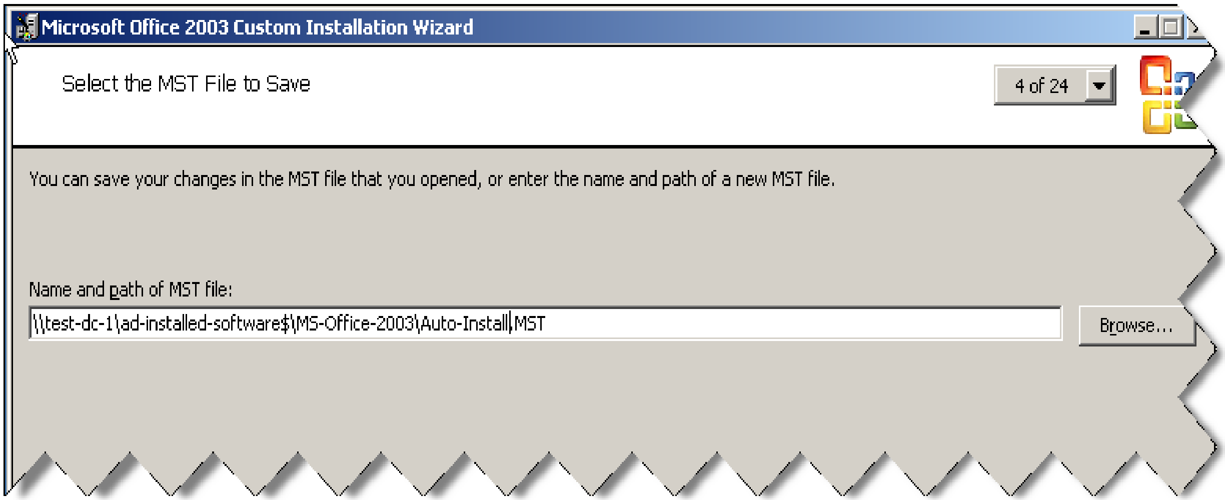
Open the MSI File

Specify the name and path of the Windows Installer package (MSI file) to open. No changes are written to the MSI file. The wizard references this file when creating the transform, but the package (MSI file) is not modified.

Name and path of MSI file to open:

\\test-dc-1\ad-installed-software$\MS-Office-2003\PRO11.MSI

19. Click **Next** to proceed.
20. Select **Create a new MST file** and then click **Next** to proceed.
21. When prompted, change the name in the path from "New Custom Setup File.MST" to "Auto-Install.MST", as seen below.



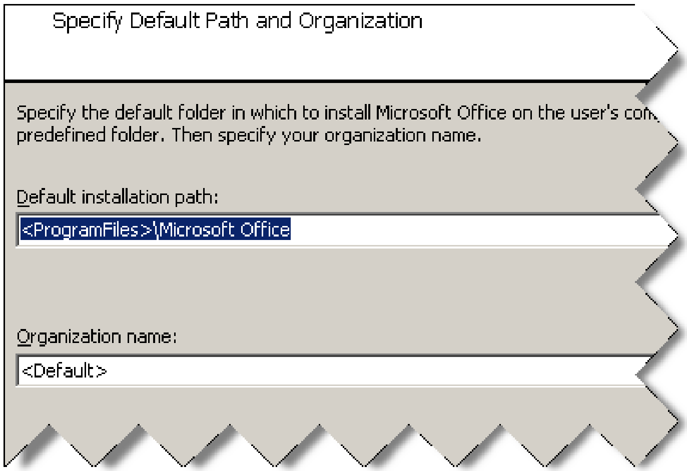
Microsoft Office 2003 Custom Installation Wizard

Select the MST File to Save

You can save your changes in the MST file that you opened, or enter the name and path of a new MST file.

Name and path of MST file: \\test-dc-1\ad-installed-software$\MS-Office-2003\Auto-Install.MST

22. Click **Next** to proceed.
23. You should now be on screen 5 of 24, the **Specify Default Path and Organization** screen. Take the defaults and click **Next**.



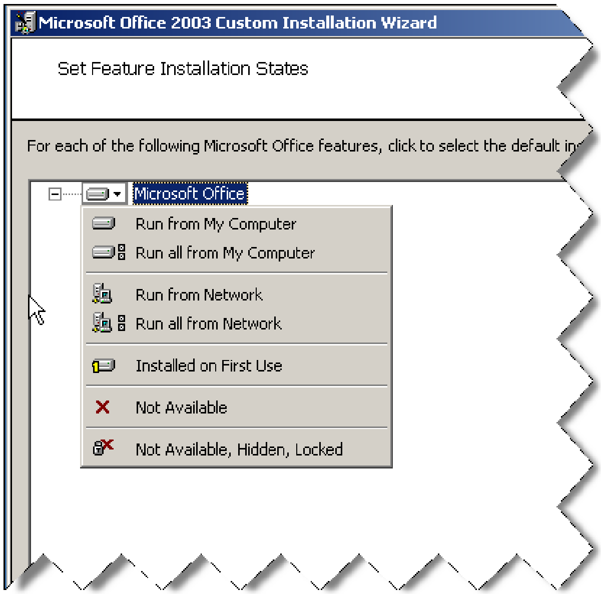
Specify Default Path and Organization

Specify the default folder in which to install Microsoft Office on the user's com predefined folder. Then specify your organization name.

Default installation path: <ProgramFiles>\Microsoft Office

Organization name: <Default>

24. You should now be on screen 6 of 24. Select **Default Setup Behavior** and click **Next** to continue.
25. Screen 7 of 24, the **Set Feature Installation States** screen. Click on "Microsoft Office" and then select **Run all from My Computer**. This should turn all drop-down boxes by each product white instead of grey. Choose the products that meet your districts needs.

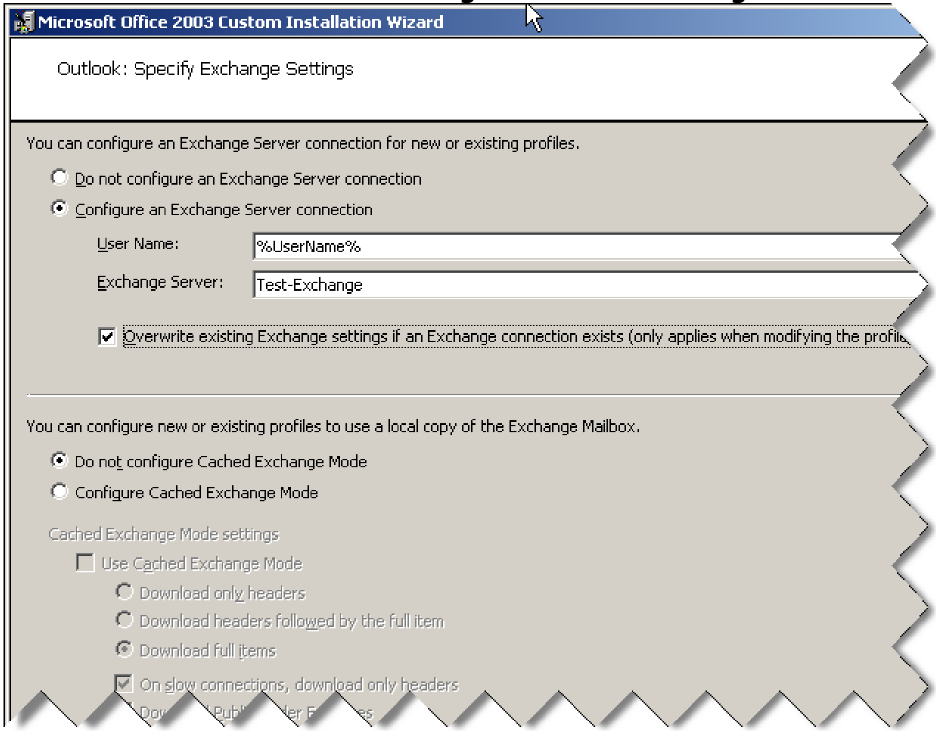


Microsoft Office 2003 Custom Installation Wizard

Set Feature Installation States

For each of the following Microsoft Office features, click to select the default in

26. Click **Next** to proceed.
27. On screen 8 of 24 select **Do not configure local installation source** and then click **Next** to continue.
28. On screen 9 through 16 take the defaults and click **Next** to continue.
29. You should now be on screen 17 of 24. Select **Modify Profile** and then click **Next** continue.
30. On screen 18 of 24 select **Configure an Exchange Server connection**. In the **Exchange Server** box enter then name of an Exchange server on your network. In the bottom section select **Do not configure Cached Exchange Mode**.



Microsoft Office 2003 Custom Installation Wizard

Outlook: Specify Exchange Settings

You can configure an Exchange Server connection for new or existing profiles.

○ Do not configure an Exchange Server connection

● Configure an Exchange Server connection

User Name: %UserName%

Exchange Server: Test-Exchange

☑ Overwrite existing Exchange settings if an Exchange connection exists (only applies when modifying the profile

You can configure new or existing profiles to use a local copy of the Exchange Mailbox.

● Do not configure Cached Exchange Mode

○ Configure Cached Exchange Mode

Cached Exchange Mode settings

□ Use Cached Exchange Mode

○ Download only headers

○ Download headers followed by the full item

● Download full items

☑ On slow connections, download only headers

31. Click **Next** to continue.
32. On screen 19 through 24 the defaults and click **Next** to continue.

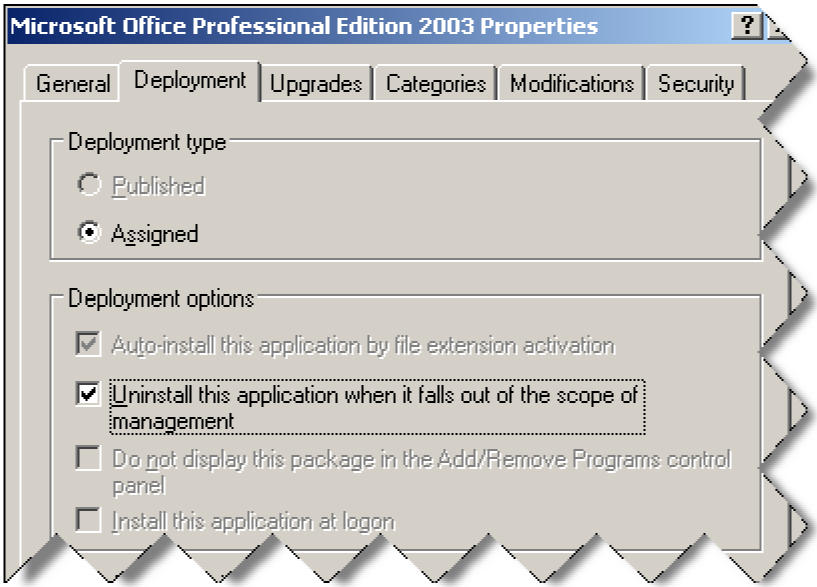
33. On screen 24 click **Finish**.
34. Copy & Paste the setup command into a text file and save to the MS-Office-2003 folder. Save the file as 2003-AutoInstall.BAT. This file will not be needed to deploy office. It, however, can be used to do a manual installation if necessary.
35. Click the **Exit** button to end the setup.

Create "Licensed Office 2003 Installs" Security Group

36. Click on Start, Administrative Tools, Active Directory Users & Computers.
37. Expand your domain so that you can see all of your Organizational Units (OU's).
38. Right click on the OU that you would like to hold the **Licensed Office 2003 Installs** security group and select New, Group.
39. For the group name enter **Licensed Office 2003 Installs** and click **Next** to continue.

Create "MS Office 2003 – Automated Install" Group Policy

40. Open Active **Directory Users and Computers** (ADUC)
41. Create a security group called "**Licensed Office 2003 Installs**" in the OU of your choice. It is recommended that this policy be placed on the parent OU that your workstation computer accounts reside in.
42. Click **Start**, **Administrative Tools**, and then **Group Policy Management**.
43. Expand Forest: **yourdomain.local.**
44. Expand Domains and then expand **yourdomain.local**.
45. Right-click yourdomain.local and select **Create a GPO in this domain, and link it here**. THIS WILL VARY BASED ON YOUR AD & LAN/WAN INFRASTRUCTURE.
46. Name the policy **Licensed Office 2003 Installs** and click **OK**.
47. In the left-hand pane, click on the new policy and click on the Scope tab in the right-hand pane.
48. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
49. Click the **Add** button.
50. In the box enter the group name "**Licensed Office 2003 Installs**" and then click the **OK** button.
51. Click on the **Settings** tab and set **GPO Status** to **User Configuration Settings Disabled**.
52. In the left-hand pane, right-click the policy to open the **Group Policy Object Editor**.
53. Expand the **Computer Configuration** section.
54. Expand the **Software Settings** section.
55. Right click **on Software Installation** and then click **New**, **Package**.
56. In the Open box, for the file name enter \\servername\ad-installed-software$ and then click the **Open** button.
57. You should now see the MS-Office-2003 install folder. Double click the folder to enter it.
58. Select the **PRO11.MSI** file and then click the **Open** button.
59. At the **Deploy Software** window, select **Advanced** and then click **OK**.
60. Click on the Deploy tab and check the box next to **Uninstall this application when it falls out of the scope of management**.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☑ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

61. Click on the **Modifications** tab and then click the **Add** button in the middle of the window.
62. Select the **Auto-Install.MST** file and then click **Open**.
63. Click the **OK** button to return to the Group Policy Editor.
64. Select **File**, **Exit** to close the Group Policy Editor.
65. Click **Close** at the OU Properties window to return to Active Directory Users & Computers.

Assign Computers to "Licensed Office 2003 Installs" Security Group

66. Browse to the OU that contains the **Licensed Office 2003 Installs** security group.
67. Double click on the group to edit the group membership.
68. Click on the **Members** tab and then click on the **Add** button.
69. By default AD only looks for Users & Security groups. Click the **Object Types** button to the upper right. Mark the check box next to Computers and then click **OK**.
70. In the entry box enter in the names of the computers that you have purchased licenses for MS Office 2003 and then click **OK**. If you misspell any computer names you will receive an error box.
71. Click **OK** to close the properties of the Licensed Office 2003 Installs group.
72. You should now be back at Active Directory Users & Computers.
73. Close out of Active Directory Users & Computers.
74. Give Active Directory a few moments to replicate the GPO to the rest of the servers, as well as the group membership changes. In about 15 minutes you can start rebooting computers. Upon startup MS Office 2003 will automatically install before your users are allowed to logon. When they open Outlook, it will automatically attach to the Exchange server and will be ready for use. You will not have to configure Outlook for your individual users.

Deploying MS Office 2007 via Group Policy

If a software distribution directory has not yet been created, follow Steps 1 through 28 of the MS Office 2003 section to build the AD-Installed-Software folder and share.

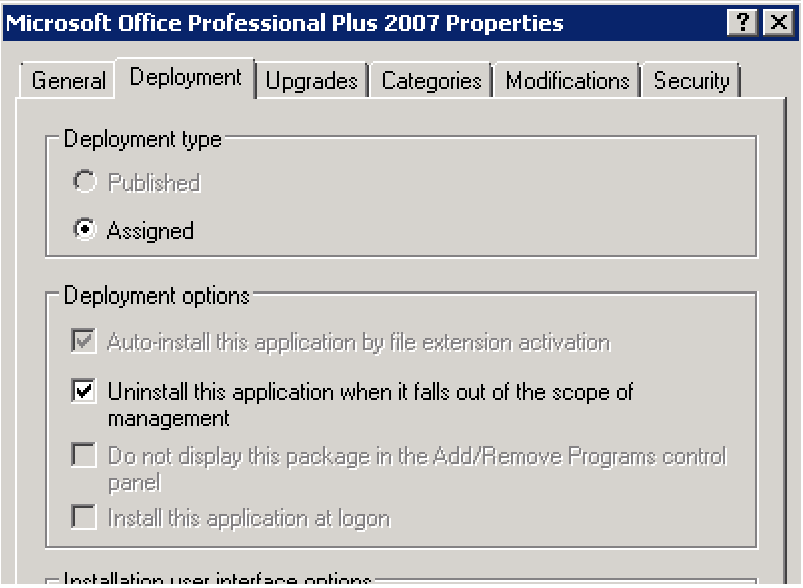
1. In the **AD-Installed-Software** folder, create a folder called MS-Office-2007. DO NOT PUT SPACES IN THE FOLDER NAME.
2. Copy the MS Office 2007 CD Contents to this folder.
3. Within the MS-Office-2007 folder, navigate to the ProPlus.WW folder or the Enterprise.WW folder. This will vary on the license type you are installing.
4. Right-click the config.xml file within this folder and open with Notepad to edit.
5. Make the XML file look as shown below and save it. Backup the original first. DO NOT COPY AND PASTE

```
<Configuration Product="Enterprise">

        <Display Level="none" nocancel="yes" CompletionNotice="yes" SuppressModal="yes" AcceptEula="yes" />

        <PIDKEY Value="BCDFGHJKMPQRTVWXY2346789B" />

        <USERNAME Value="Technology Coordinator" />

        <COMPANYNAME Value="Example School District" />

        <INSTALLLOCATION Value="%programfiles%\Microsoft Office" />

        <Setting Id="Reboot" Value="IfNeeded" />

</Configuration>
```

Create “MS Office 2007 – Automated Install” Group Policy

6. Open Active **Directory Users and Computers** (ADUC)
7. Create a security group called “**Licensed Office 2007 Installs**” in the OU of your choice. It is recommended that this policy be placed on the parent OU that your workstation computer accounts reside in.
8. Click **Start**, **Administrative Tools**, and then **Group Policy Management**.
9. Expand Forest: **yourdomain.local.**
10. Expand Domains and then expand **yourdomain.local**.
11. Right-click yourdomain.local and select **Create a GPO in this domain, and link it here**. THIS WILL VARY BASED ON YOUR AD & LAN/WAN INFRASTRUCTURE.
12. Name the policy **Licensed Office 2007 Installs** and click **OK**.
13. In the left-hand pane, click on the new policy and click on the Scope tab in the right-hand pane.
14. From the **Security Filtering** list, select **Authenticated Users** and then click the **Remove** button.
15. Click the **Add** button.
16. In the box enter the group name “**Licensed Office 2007 Installs**” and then click the **OK** button.
17. Click on the **Settings** tab and set **GPO Status** to **User Configuration Settings Disabled**.
18. In the left-hand pane, right-click the policy to open the **Group Policy Object Editor**.
19. Expand the **Computer Configuration** section.
20. Expand the **Software Settings** section.

21. Right click **on Software Installation** and then click **New**, **Package**.
22. In the Open box, for the file name enter \\servername\ad-installed-software$ and then click the **Open** button.
23. You should now see the MS-Office-2003 install folder. Double click the folder to enter it.
24. Select the **ProPlusWW.MSI** or **EnterpriseWW.MSI** file and then click the **Open** button.
25. At the **Deploy Software** window, select **Advanced** and then click **OK**.
26. Click on the Deploy tab and check the box next to **Uninstall this application when it falls out of the scope of management**.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

☑ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

Installation user interface options

27. Click the **OK** button to return to the Group Policy Editor.
28. Select **File**, **Exit** to close the Group Policy Editor.

Add the respective computer accounts to the **Licensed Office 2007 Installs** group**.** Once the group policy refreshes on the workstation and the workstation reboots, the install will start. The second half of the install will happen the first time a user logs into the workstation. They cannot cancel or close the install completion process nor can they log off or shutdown the computer within Windows. Since they can physically turn off the power, it would be wise to forward users when the policy is applied to their workstation.

Refresh Group Policy settings with GPUpdate.exe

Updated: January 21, 2005

To refresh Group Policy settings with GPUpdate

The **gpupdate** command refreshes local and Active Directory–based Group Policy settings, including security settings on the computer from where it is run. You can use **gpupdate** locally on Windows XP and higher computers to refresh policy immediately. On computers running Windows 2000, this functionality is provided by the using the **secedit** command with the refreshpolicy option.

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**

Troubleshooting Windows Server 2008

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
(You may need to create the Reliability key)

Insert or change a value with the following:
Data Type: DWORD
Value Name: ShutdownReasonOn
Value: 0

The change will take place immediately. You will not have to reboot.

Set Time Source to DIS

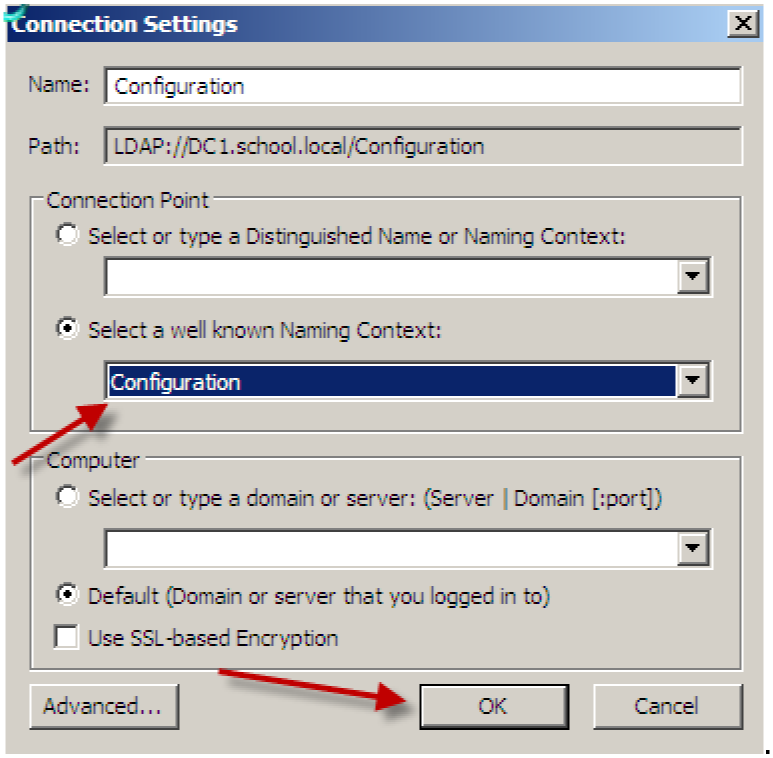
1. First, locate your PDC Server. Open the command prompt and type: ***C:|>netdom /query fsmo***
2. Log in to your PDC Server and open the command prompt.
3. Stop the W32Time service: ***C:|>net stop w32time***
4. Configure the external time sources, type: ***C:|> w32tm /config /syncfromflags:manual /manualpeerlist:"165.29.1.11,165.29.1.12"***
5. Make your PDC a reliable time source for the clients. Type: ***C:|>w32tm /config /reliable:yes***
6. Start the w32time service: ***C:|>net start w32time***
7. The windows time service should begin synchronizing the time. You can check the external NTP servers in the time configuration by typing: ***C:|>w32tm /query /configuration***

Check the Event Viewer for any errors.

Active Directory Maintenance How-To's

Delete Dead/Tombstoned Domain Controller from Active Directory

1. From another Domain Controller within the domain, click **Start** > **Run**, type **ADSIEDIT.MSC** and click **OK**.
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

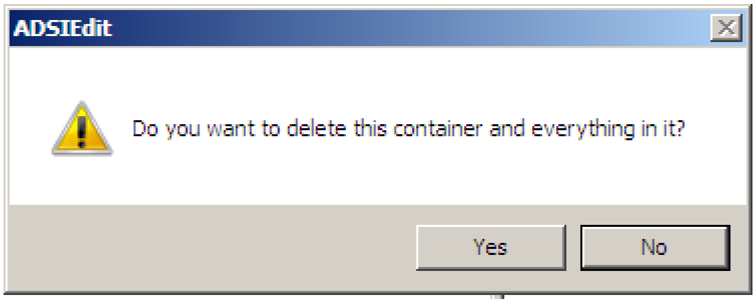
○ Select or type a domain or server: (Server | Domain [:port])

● 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**.



ADSIEdit

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.

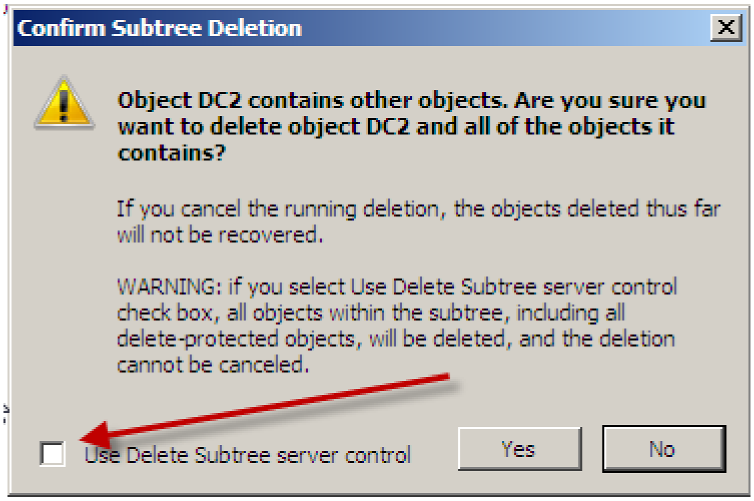
Removing the Server from the File Replication Service:

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 & Services

13. Open Active Directory Sites & 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.



Confirm Subtree Deletion

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.

□ Use Delete Subtree server control

20. Close Active Directory Sites & Services.

Removing the Server from Active Directory Users & Computers

21. Open Active Directory Users & Computers
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, check the box next to "This Domain Controller is permanently offline….." and click **Delete**.
25. 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:

1. Log on to a Windows 2000 Server-based or Windows Server 2003-based member computer or domain controller that is located in the forest where FSMO roles are being seized. We 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.
2. Click Start, click Run, type **ntdsutil** in the Open box, and then click OK.
3. Type **roles**, and then press ENTER.
4. Type **connections**, and then press ENTER.
5. Type **connect to server *servername***, and then press ENTER, where servername is the name of the domain controller that you want to assign the FSMO role to.
6. At the server connections prompt, type **q**, and then press ENTER.
7. 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.
8. At the fsmo maintenance prompt, type **q**, and then press ENTER to gain access to the ntdsutil prompt. Type **q**, and then press ENTER to quit the Ntdsutil utility.

How to Reset the Directory Services Restore Mode Administrator Account Password in Windows Server 2003

1. Click, Start, click Run, type **ntdsutil**, and then click OK.
2. At the Ntdsutil command prompt, type set dsrm password.
3. At the DSRM command prompt, type one of the following lines:
   - 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. Note that no characters appear while you type the password.

   -or-

   - 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. Type the new password when you are prompted. Note that no characters appear while you type the password.
4. At the DSRM command prompt, type q.
5. At the Ntdsutil command prompt, type q to exit.

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