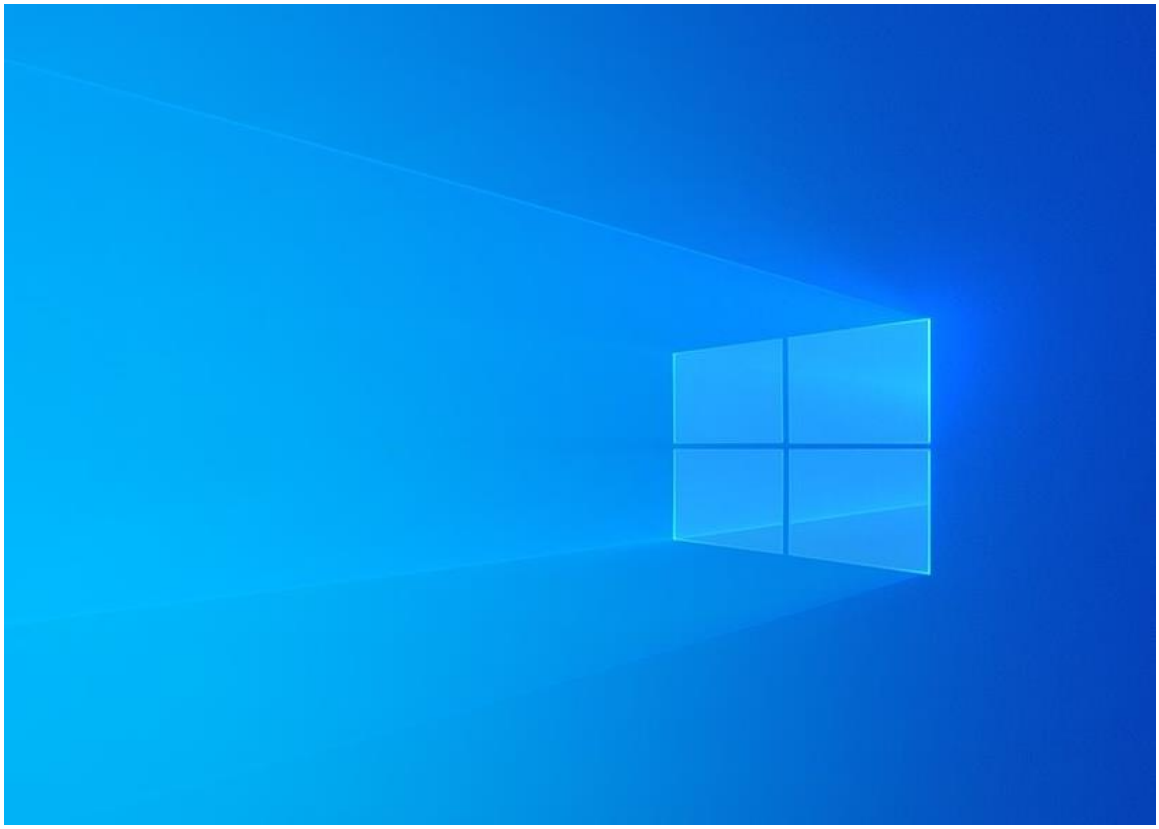
Arkansas Department of information Systems

EMPOWERING THE CITIZENS OF ARKANSAS THROUGH TECHNOLOGY



WINDOWS SERVER 2019

INSTALLATION AND CONFIGURATION

Prepared By
DIS APSCN/LAN Support

Table of Contents

Intro to Windows Server 2019 – Installation and Configuration.....1
Table of Contents.....2 - 3
Windows Server 2019 Requirements.....4
Windows Server 2019 Glossary of Terms.....5 - 8
Virtualization Rights 9
Pre-Installation Requirements & Installation .....10 - 14
Licensing Editions.....11
Server Initial Configuration.....15
Disable IPV6 via Registry Editor 17
Disable Windows Firewall.....19
Domain Services and Active Directory Setup.....23 - 25
Additional DNS Configuration 25
Reverse Lookup Zones.....26
Stale Record Scavenging.....27
DNS Forwarders.....28
DIS DNS Forwarders & OpenDNS Servers 29
DHCP Installation and Configuration. .....30 -32
WINS Installation and Configuration.....32
Windows Server Update Services (WSUS).....34
Configuring WSUS after Installation.....34 - 40
WSUS Group Policy.....39 - 40
Basic Active Directory Structure for K12.....41
Single Site Active Directory Networks..... 41
Create Shares and Home Directories.....43 - 47
Creating User Template.....48
Creating New User using Template.....48 - 51
Creating Faculty & Student Batch File for Active Directory – Mass Import.....52 - 53
Logon Scripts – Batch File Method.....55 - 58
Implementing Shadow Copies.....57 - 61
Implementing Volume Based Quota Limits.....64
Directory Level Quota Limits Using File Server Resource Manager.....65
Install File Server Resource Manager.....64
Configure Quota Templates.....64
Apply Quota Template to Directory.....65
Fine-Grained Password Policies (ACT-723).....66 - 68
Some Common K12 Group Policies.....69 - 79
Retain Security Event Log for 90 Days Group Policy.....69
Auto-Backup and Clear Event Logs (At Least Windows Vista).....70
Security Event Auditing – Security Event Log Contents.....71
Group Policy for Logon Banner.....72

Locking Screen Saver Group Policy.....73
Folder Redirection Group Policy……74 - 75
Restrict Computers to Faculty Use Only……76 - 77
Refresh Group Policy Settings with GPUDATE.EXE……77 - 79
How To Check Applied Group Policy Setting on a Domain Computer (GUI)……79
How To Check Applied Group Policy Setting on a Domain Computer (CMD) Rsop.msc…80
Troubleshooting Windows Sever 2019……81 - 96
Disabling the Shutdown Event Tracker……81
Set Time Source to DIS / NTP Time Servers……82
Active Directory Maintenance……83
Steps to Check Active Directory Replication in Windows Server (GUI)……83 - 85
Steps to Check Active Directory Replication in Windows Server (CMD) Repadmin..85 – 88
Testing / Diagnose The Health Of Active Directory Domain Controllers, DNS Servers, AD Replication, And Other Adds Infrastructure Services (CMD) - Dcdiag……89
Delete Dead / Tomb-Stoned Domain Controller from Active Directory……90
Removing the Server from the Active Directory Site……90
Removing the Server from the File Replication Service……91 - 92
Removing the Server from Active Directory Sites and Services……92
Removing the Server from Active Directory Users and Computers……92 - 93
Manually Seize FSMO Roles……93 - 94
How to Rest the Directory Service Restore Mode Administrator Account Password…….95
How to create a Bootable USB (GUI) ……96
How to create a Bootable USB (PS) ……97 - 100

This document is DIS' recommended method for implementing a Windows Server 2019 and Active Directory (AD) Environment within a K12 network.

WINDOWS SERVER 2019 REQUIREMENTS

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

WINDOWS SERVER 2019 GLOSSARY OF TERMS

TERMS	DEFINITION
Windows Server	Windows Server is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. In a technical sense, a server is an instance of a computer program that accepts and responds to requests made by another program, known as a client. Examples: Application, Proxy, Mail, Web, DHCP, FTP & VPN Servers
Active Directory	Active Directory **(AD)** is a directory service that Microsoft developed for the Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.
Active Directory Domain Services **Domain Controller**	A server running Active Directory Domain Services **(AD DS)** is called a domain controller **(DC)**. It authenticates and authorizes all users and computers in a Windows domain type network assigning and enforcing security policies for all computers & installing or updating software. For ex., when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Active Directory Federation Services, Lightweight Directory Services and Rights Management Services.

TERMS	DEFINITION
Organizational Unit	An organizational unit **(OU)** is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure. Each domain can implement its own organizational unit hierarchy.
Groups	Groups are used to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps simplify network maintenance and administration. There are two types of groups in Active Directory: **Distribution Group** used to create email distribution lists. A **Security Group** provides a logical grouping of objects and the group itself can be used as a security principal in an Access Control List (ACL)
Group Policy	Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. A version of Group Policy called Local Group Policy ("LGPO" or "LocalGPO") also allows Group Policy Object management on standalone and non-domain computers.
Group Policy Object	A Group Policy Object **(GPO)** is a collection of settings that define what a system will look like and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console (MMC)
IP Address	An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.
Firewall	A technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts

TERMS	DEFINITION
Dynamic Host Configuration Protocol	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address. DHCP can be implemented on networks ranging in size from home networks to large campus networks and regional Internet service provider networks. A router or a residential gateway can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.
Domain Name System	The Domain Name System **(DNS)** is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985.The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their allocated name space to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid a single large central database.

TERMS	DEFINITION
Server Manager	Server Manager is a management console in Windows Server that helps IT professionals provision and manage both local and remote Windows-based servers from their desktops, without requiring either physical access to servers, or the need to enable Remote Desktop protocol **(rdP)** connections to each server.
Sysvol	The System Volume **(Sysvol)** is a shared directory that stores the server copy of the domain's public files that must be shared for common access and replication throughout a domain. The Sysvol folder on a domain controller contains the following items: Net Logon shares. These typically host logon scripts and policy objects for network client computers. User logon scripts for domains where the administrator uses Active Directory Users and Computers. Windows Group Policy & File system junctions. File replication service (FRS) staging folder and files that must be available and synchronized between domain controllers.
RAID	**RAID** (Redundant **Array** of Independent Disks, originally Redundant **Array** of Inexpensive Disks) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement or both.
Virtualization	In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Even something as simple as partitioning a hard drive is considered virtualization because you take one drive and partition it to create two separate hard drives. Devices, applications and human users are able to interact with the virtual resource as if it were a real single logical resource.

Virtualization RIGHTS

Attribute	Datacenter	Standard	Essentials
Licensing model	Per Core/CAL[1]	Per Core/CAL[1]	Specialty servers[2]
License type	Core license	Core license	Server license
OSEs/Hyper-V containers	Unlimited	Two[3]	One[4]
Windows Server containers	Unlimited	Unlimited	

[1] All physical cores on the server must be licensed, subject to a minimum of 8 core licenses per physical processor and a minimum of 16 core licenses per server.

[2] Windows Server Essentials edition server is for either one or two processor servers.

[3] Windows Server Standard edition permits use of one running instance of the server software in the physical OSE on the licensed server (in addition to two virtual OSEs), if the physical OSE is used solely to host and manage the virtual OSEs.

[4] Windows Server Essentials edition permits use of one running instance of the server software in the physical OSE on the licensed server (in addition to one virtual OSE), if the physical OSE is used solely to host and manage the virtual OSE.

- **Datacenter Edition –** When all physical cores on the server are licensed, Windows Server Datacenter edition provides rights to use unlimited operating system environments (OSEs) or Hyper-V containers and unlimited Windows Server containers on the licensed server.
- **Standard Edition –** When all physical cores on the server are licensed, Windows Server Standard edition provides rights to use two Operating System Environments (OSEs) or Hyper-V containers and unlimited Windows Server containers on the licensed server.

  **For example, a 2-processor server with 8 cores per processor requires 16 core licenses (in other words, one 16-pack of core licenses or eight 2-packs of core licenses) and gives rights to two OSEs or two Hyper-V containers. In the case of this example, for each additional two OSEs or two Hyper-V containers the customer wishes to use, an additional 16 core licenses must be assigned to the server.

PRE-INSTALLATION REQUIREMENTS

- Microsoft Windows Server 2019 DVD (with Service pack IF applicable).
- 1 NAT IP Address (Statically Assigned)
- Bootable USB Drive / DVD (At least 8Gb USB Drive / Blank Dual Layer DVD-R)
  ****For Assistance with creating a Bootable USB Drive skip to page 96 - 100**
  ****Certain Servers will have to have SCSI/RAID Controller Drivers.**
  ****RAID Configuration & Logical Drives should be configured before server installation.**

INSTALLATION

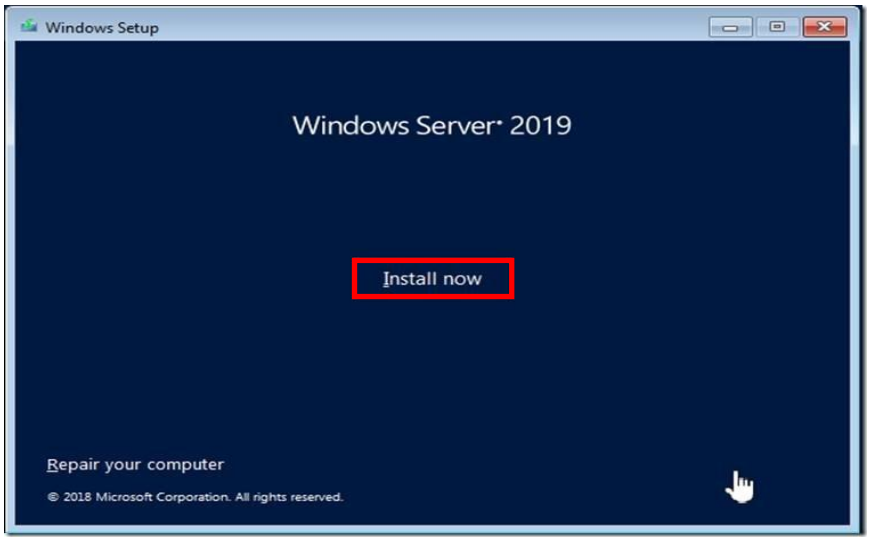
1. Purchase Windows Server Edition / Download .ISO & Activation Key
   For ESS Agreement logon onto - Microsoft Volume Licensing Service Center (VLSC) https://www.microsoft.com/Licensing/servicecenter/default.aspx

2. Insert the appropriate Windows Server 2019 installation media into your server and reboot (DVD-ROM / Bootable USB)

3. After restarting the server, boot to the DVD-ROM / USB. Wait for Setup to display a dialog box.

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

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



LICENSING EDITIONS

Choose from three primary editions of Windows Server, based on the size of your organization as well as virtualization and datacenter requirements:

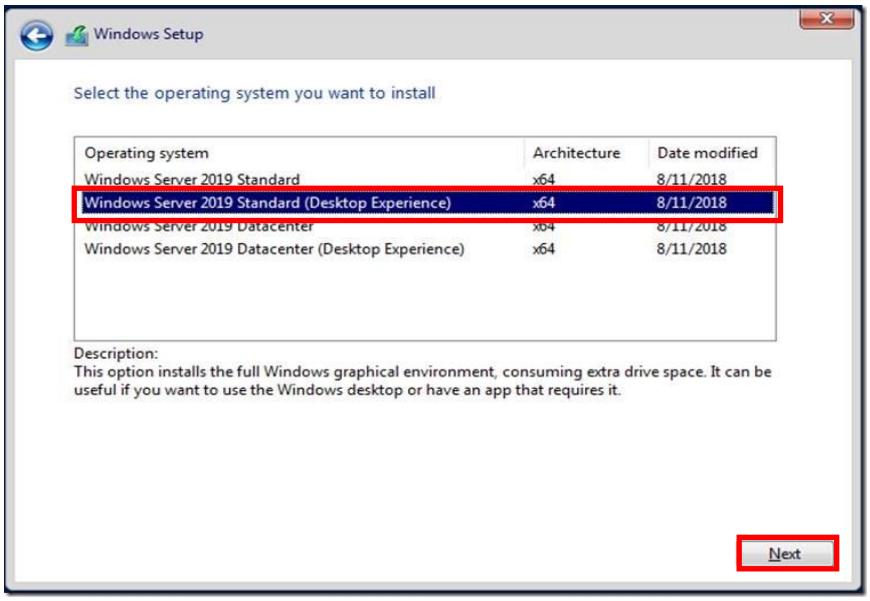
- **Datacenter Edition** is ideal for highly virtualized and software-defined datacenter environments.
- **Standard Edition** is ideal for customers with low density or non-virtualized environments.
- **Essentials Edition** is a cloud-connected first server, ideal for small businesses with up to 25 users and 50 devices. Essentials is a good option for customers currently using the Foundation edition, which is not available with Windows Server 2019.

***All physical cores on the server must be licensed, subject to a minimum of 8 core licenses per physical processor and a minimum of 16 core licenses per server.*

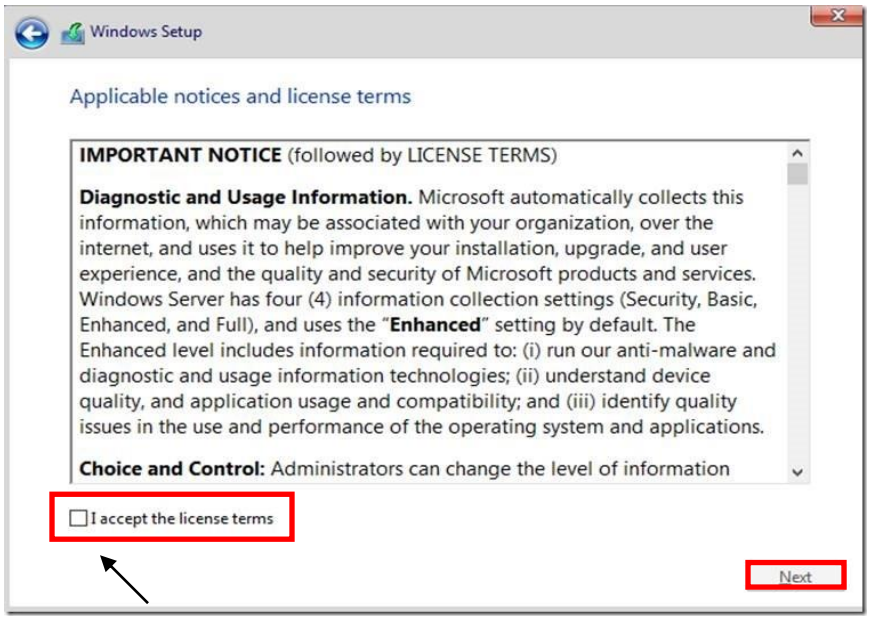
***CALs are required for every user or device accessing a server. See the **Product Terms** for details.*

Windows Server 2019 offers additional features in Standard and Datacenter editions. Features exclusive to the Windows Server 2019 Datacenter edition include Shielded Virtual Machines, software-defined networking, Storage Spaces Direct, and Storage Replica. While no features from the Windows Server 2012 R2 Standard edition have been removed, we have added features like Nano Server and unlimited Windows Server containers to the Windows Server 2019 Standard edition.

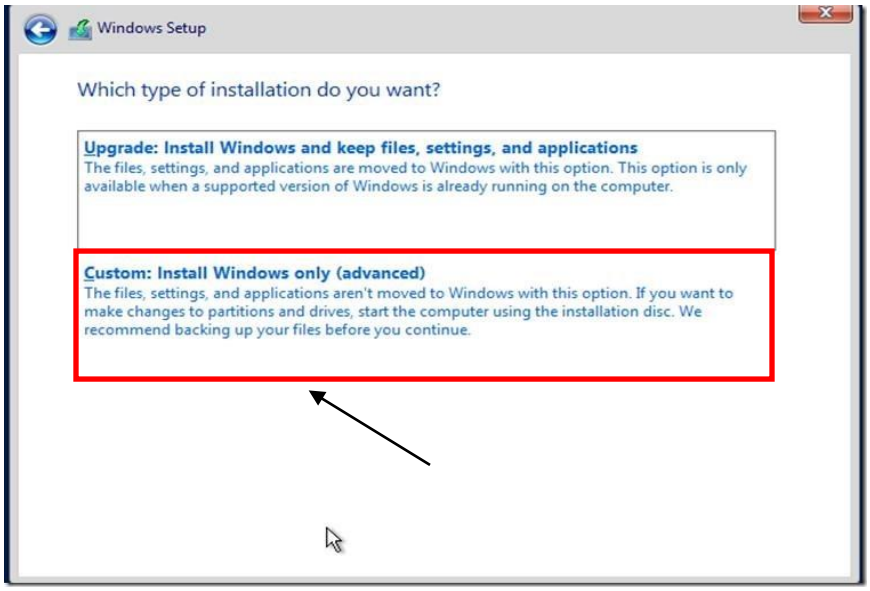
6. Select the proper edition of Windows Server 2019 that is to be installed and press **Next**.
    - **Note - Choose Desktop Experience for Operating System with GUI (Graphical User Interface)**



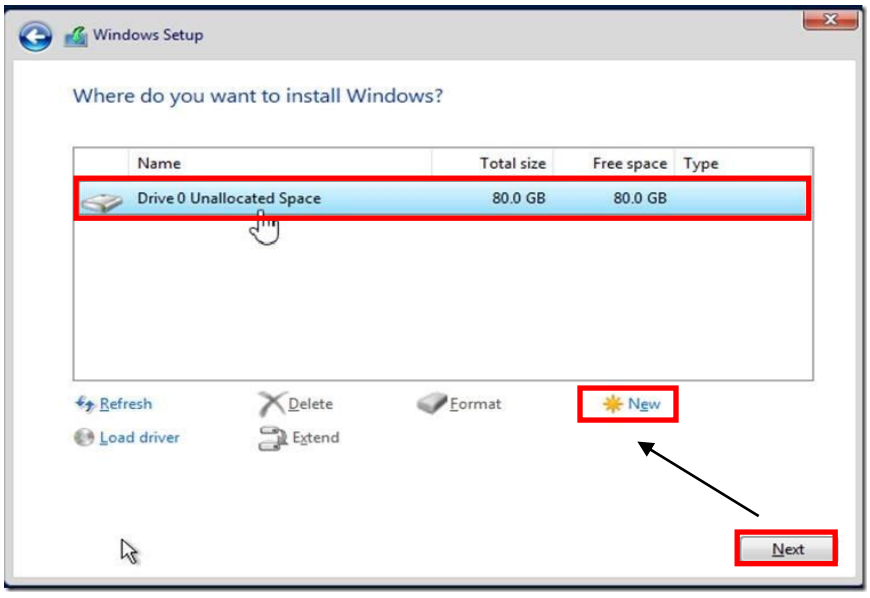
7. Read and accept the license terms by clicking to select the **checkbox** and pressing **Next**.



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

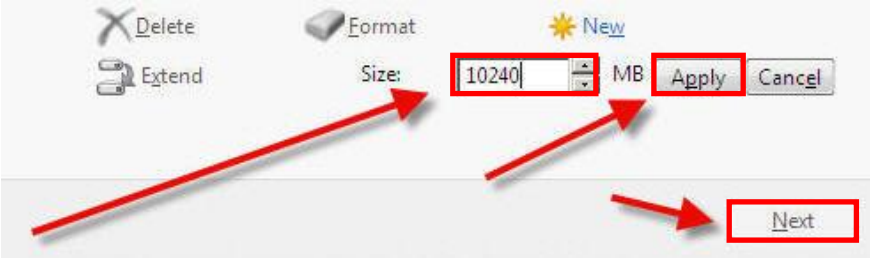


9. Select the disk that you will be installing Windows Server 2019 onto and then click **New** to create a partition that Windows Server 2019 will be installed on.



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

*****The size format is in megabytes. MB * 10240 = Size to be entered.***
***** Example 10240MB x 10 = 102.4 GB Drive, Recommend at least 100GB C:/***



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

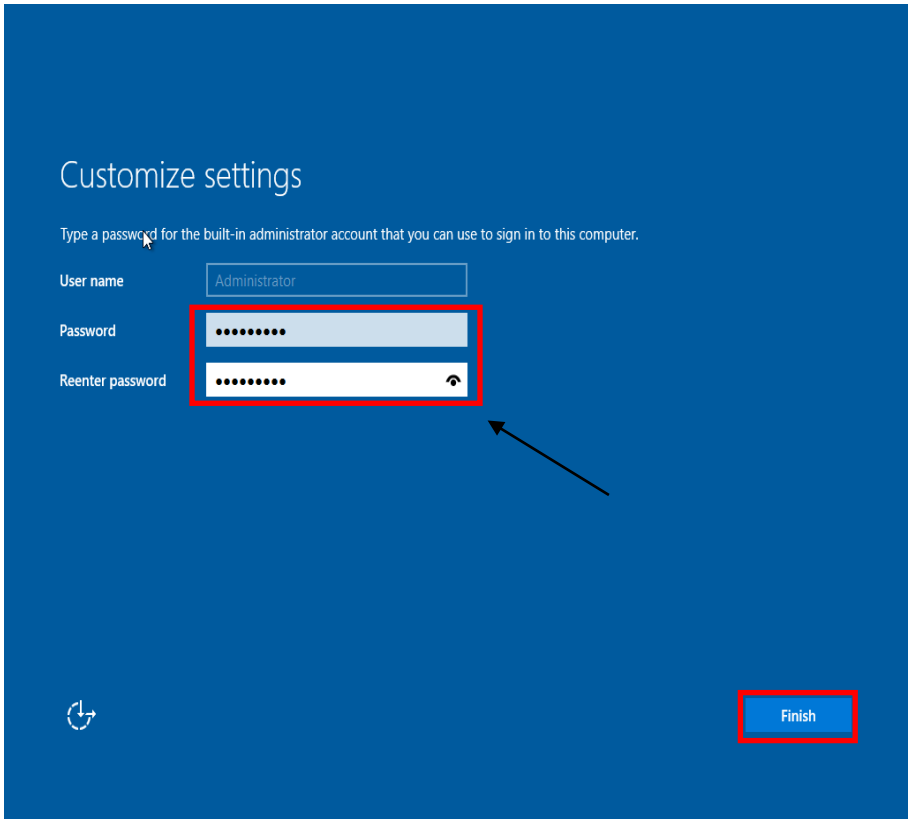
****See notes on partition types:**
**** When creating new partitions, if it's over 2 TB or if it UEFI Boot it recommended to be GPT.**

You don't usually have to worry about partition style - Windows automatically uses the appropriate disk type. Most PCs use the GUID Partition Table (GPT) disk type for hard drives and SSDs. GPT is more robust and allows for volumes bigger than 2 TB. The older Master Boot Record (MBR) disk type is used by 32-bit PCs, older PCs, and removable drives such as memory cards. To convert a disk from MBR to GPT or vice versa, you first have to delete all volumes from the disk, erasing everything on the disk.

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 8 characters and three out of the four following:

- Create complex Password / Password Phrase
- Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.

****Do Not Use Default Passwords for the Administrator Account such as Password1 / Password123 & etc.**



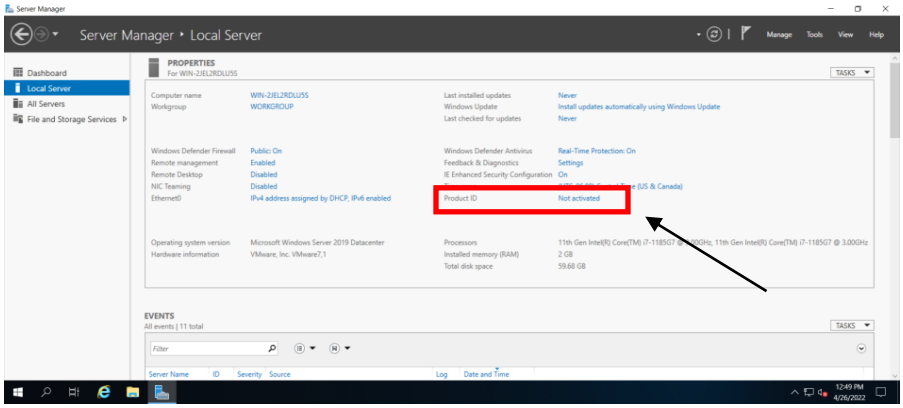
12. Once the password is successfully changed, the server will login to the initial desktop and Server Manager will start up automatically.

SERVER INITIAL CONFIGURATION

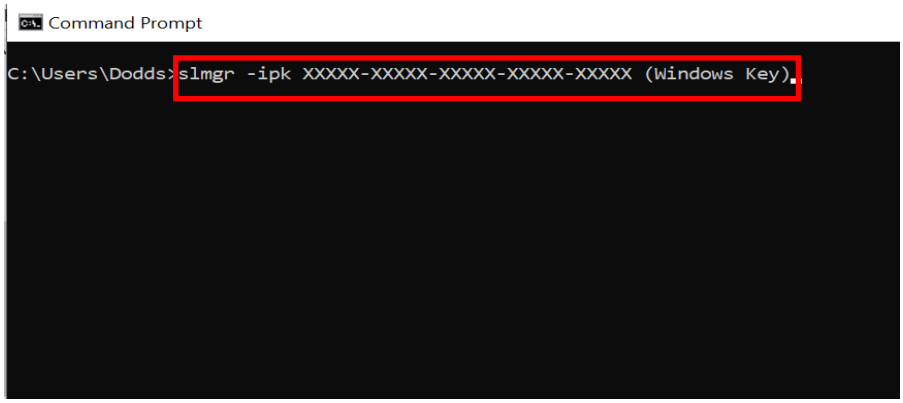
1. On the Server Manager screen, click on Local Server.

2. Activate Windows and insert key. (Must Have an Internet Connection)

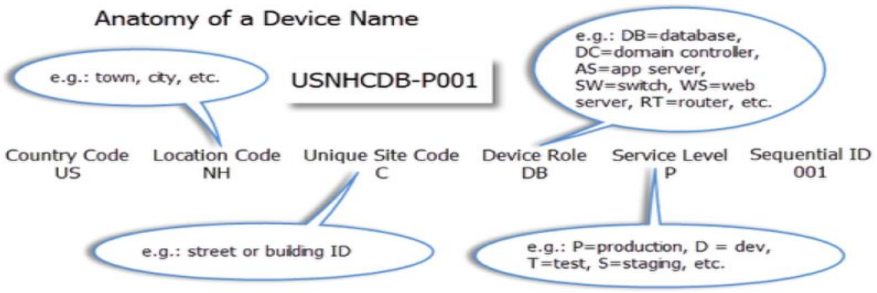
   Click Product ID and enter windows license key (MAK)



   *Note if activation is not available, then you can manually activate using command SLMGR command. Open command prompt and enter the following command: slmgr -ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (windows key)



3. Change Computer Name – Use a good naming convention for asset management **Example – Building Name + Device = Admin-DC1, HS-DC1, MS-AS1 etc.



4. Set Time zone – Correct Time Zone (Central Time)

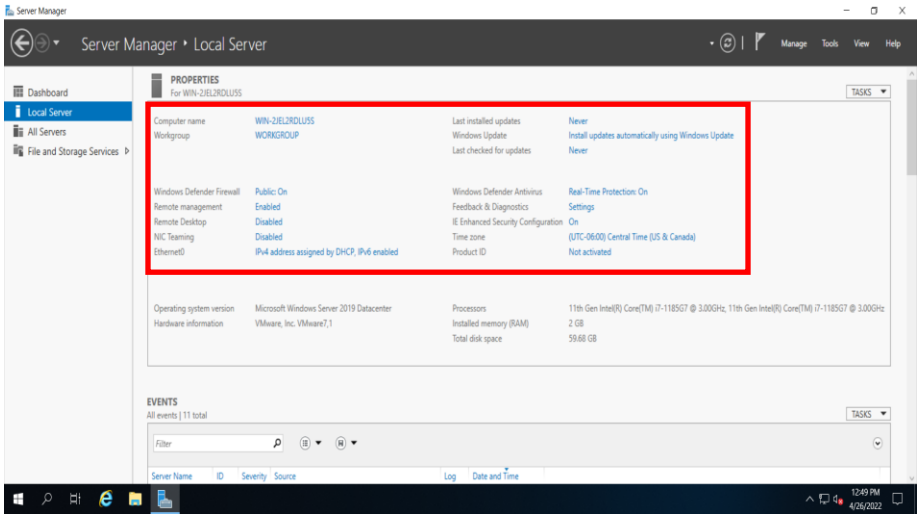
5. Enable Remote Desktop for Remote Management
   ****Click – allow connections only from computers running remote desktop with network level authentication (recommended)**

6. Configure Networking and change to Static IP and disable IPv6 by unchecking the option for TCP/IPv6.

7. Enable Windows Updates.

8. Download and Install updates.

9. Turn off IE Enhanced Security Configuration for Administrators only.



DISABLE IPV6 VIA REGISTRY EDITOR

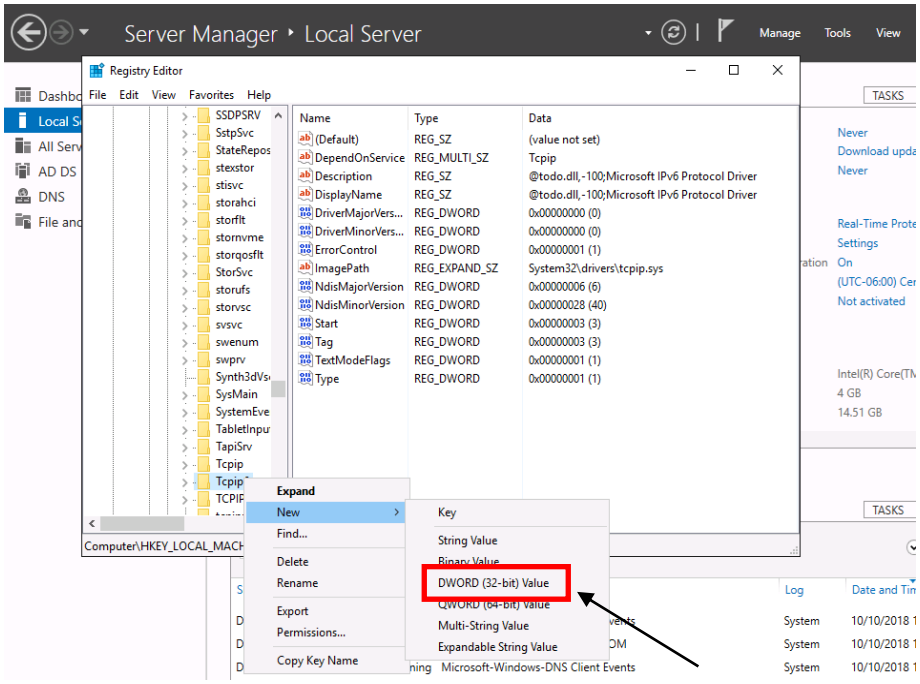
*****Recommended To Be Done***

1. Open the Registry Editor by moving your mouse over the bottom-left Windows Key or click Keyboard Key and type **REGEDIT** and press **Enter**

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

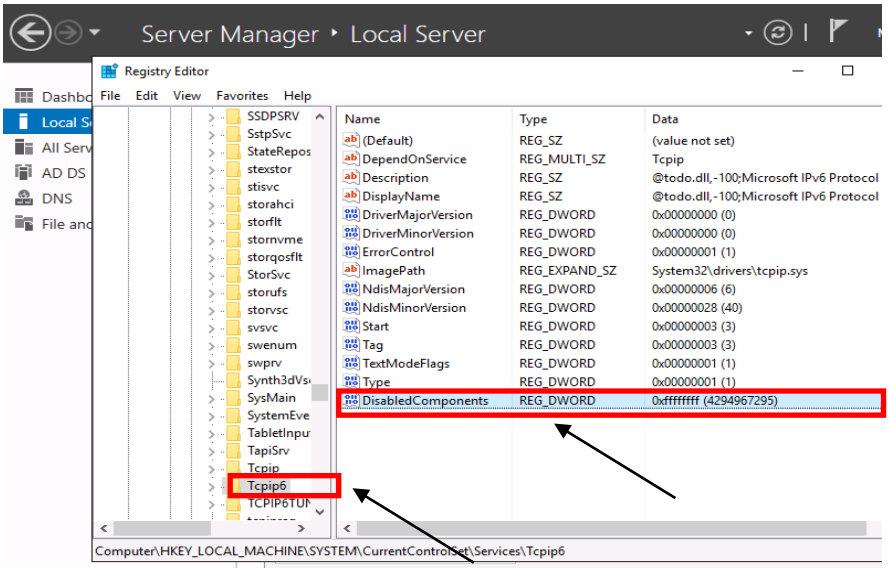
   HKEY_LOCAL_MACHINE
   |---System
   |---CurrentControlSet
   |---Services
   |---Tcpip6
   |---Parameters

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



4. Type in the name **DisabledComponents** and press **Enter**. (name is case sensitive)

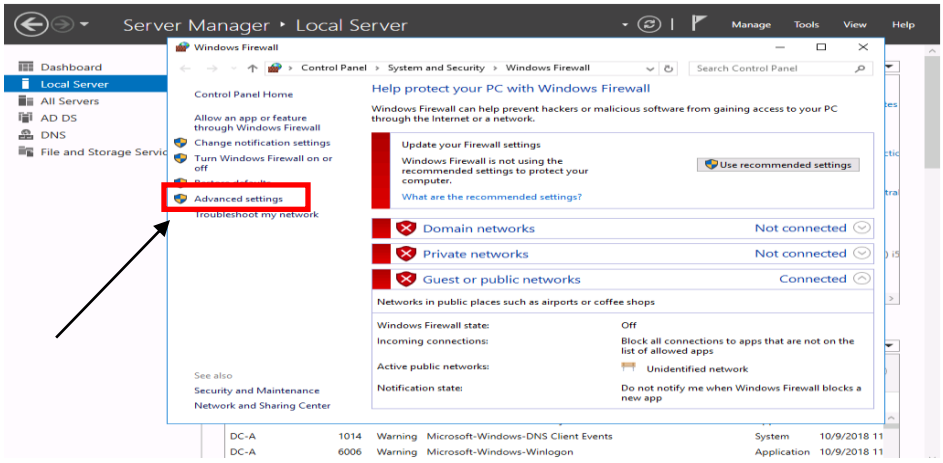
5. Double-click on the newly created key and enter **ffffffff (8 f's)** for the value data in Hexadecimal mode.



6. Close the Registry Editor

DISABLE WINDOWS FIREWALL

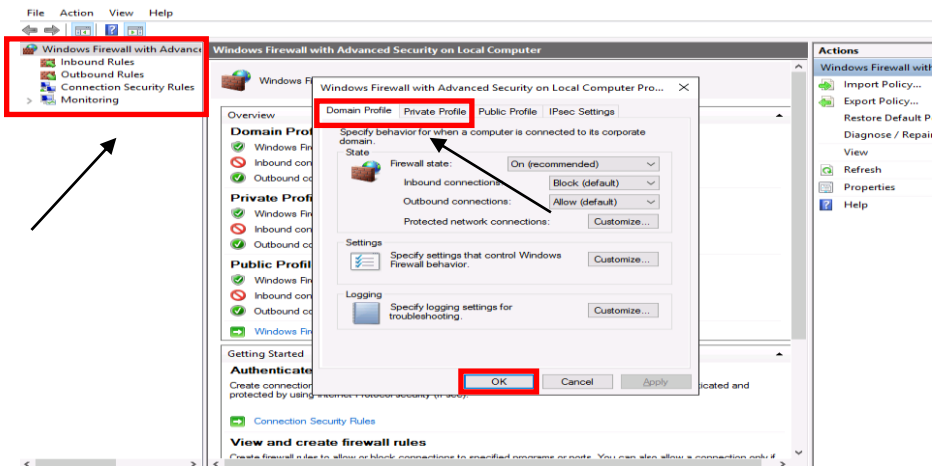
7. Open the Windows Firewall with Advanced Security by moving your mouse over the bottom-left Windows Key ⊞ or click Keyboard Key ⊞ and type **FIREWALL** and press **Enter**



1. Choose Advance Setting

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

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



*****It is highly recommended that the Firewall be enabled on DIS Router if you are not using a third-party firewall. If you do not have any firewall appliance, you may wish to leave the windows firewall enabled. Adjust the scopes of the Inbound/Outbound rules to meet application requirements***.
***** Recommended to create inbound / outbound rules, allow specific ports & programs thru firewall instead of just turning off firewalls***

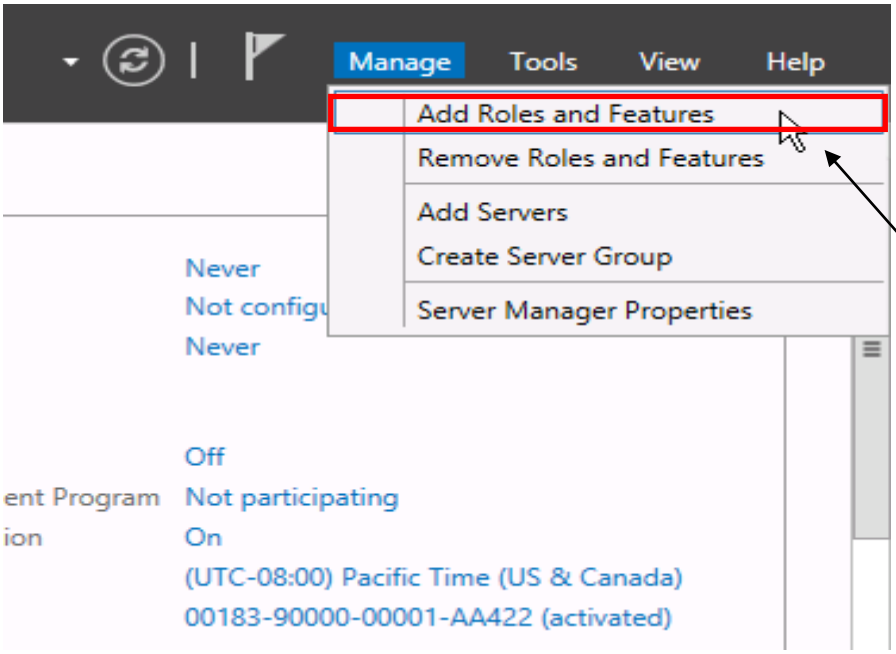
DOMAIN SERVICES AND ACTIVE DIRECTORY SETUP

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

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

1. Launch **Server Manager**.

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

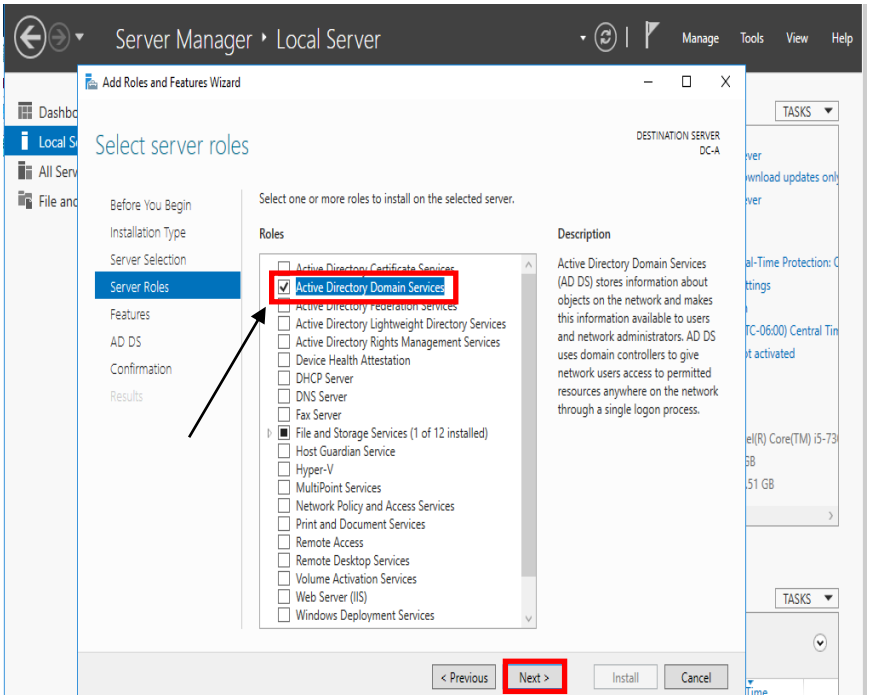


3. On the **Before You Begin screen**, click **Next**.

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

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

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

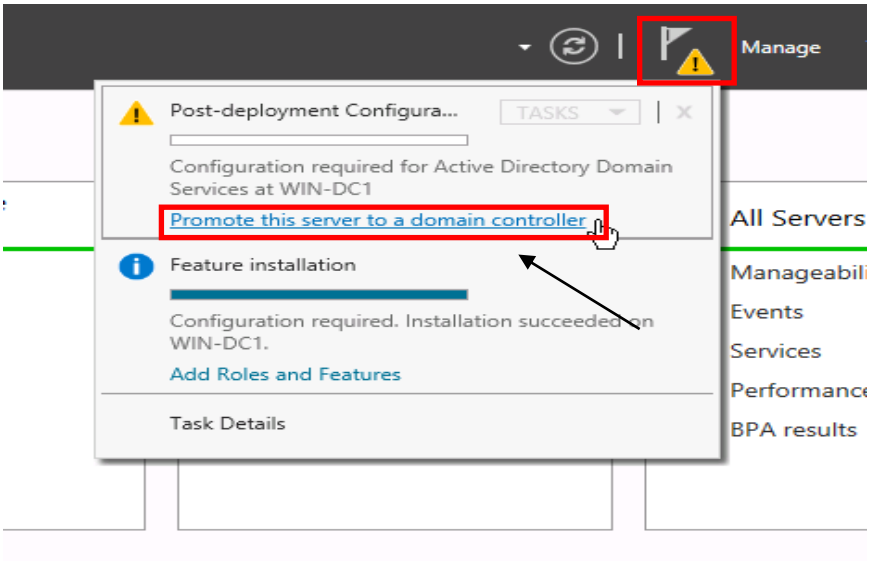


7. On the **Add Roles and Features Wizard** dialogue box, click **Add Features**.

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

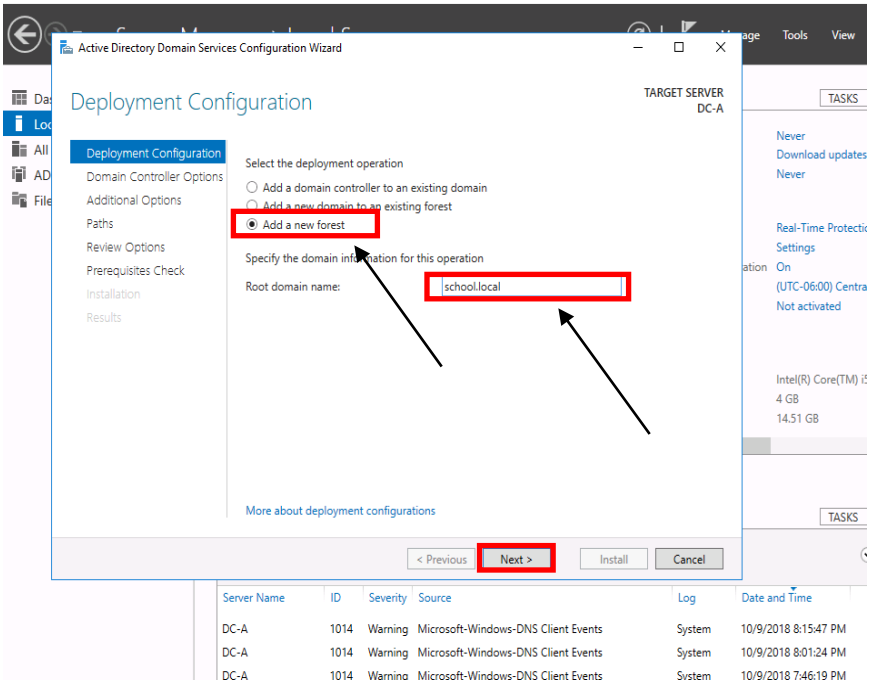
9. When the installation is finished, click **Close**.

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



.

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



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

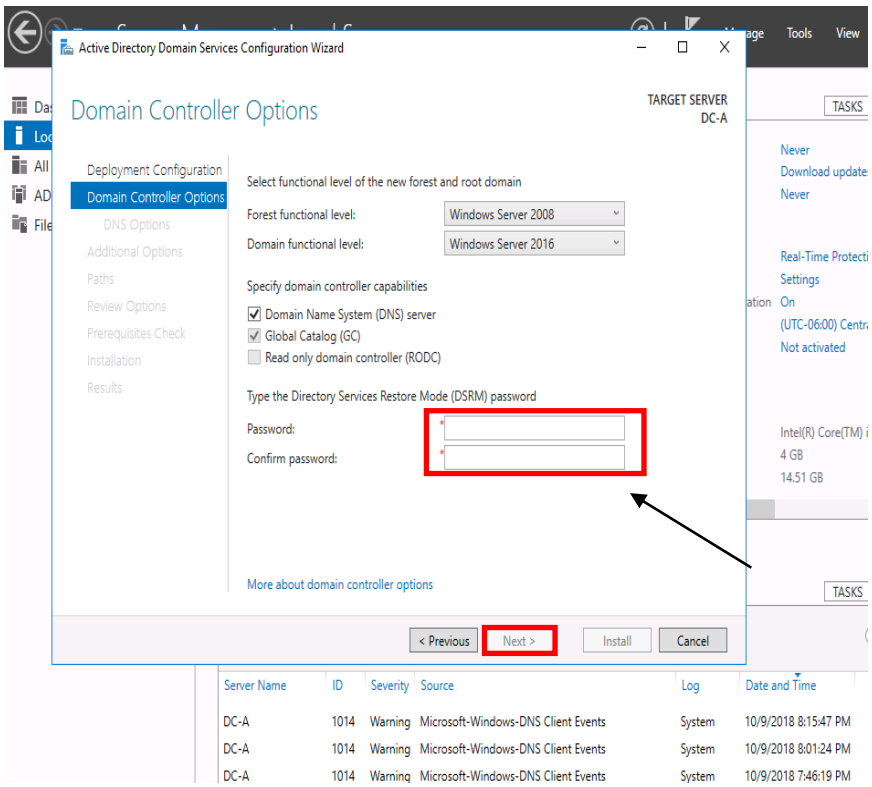
***This domain name is for INTERNAL resolution only**.

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

12. For the Forest Functional Level and the Domain Functional Level, select **Windows Server 2019** and click **Next**.

***If any previous versions of Windows Server Operating (2012 or 2016 R2) are present in the domain or will be introduced as Domain Controllers, select the corresponding Forest and Domain Functional level**.

***Windows Server 2012 End-of-life mainstream support October 10, 2023**
***Windows Server 2016 End-of-life mainstream support January 11, 2022**
***Windows Server 2019 End-of-life mainstream support January 09, 2024**



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

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

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

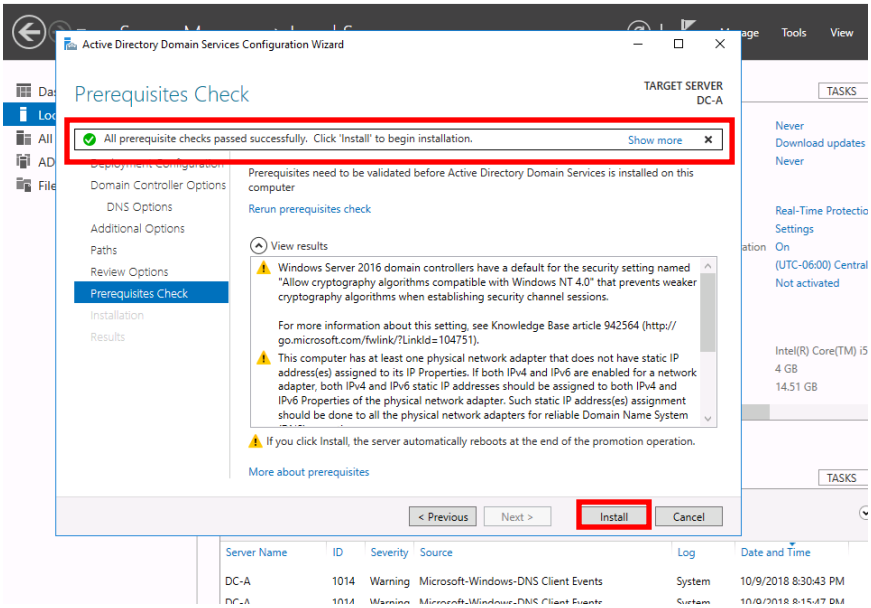
    *****Ignore the Parent zone delegation warning on top of the screen. It will be created during initial AD installation.***

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

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

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

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



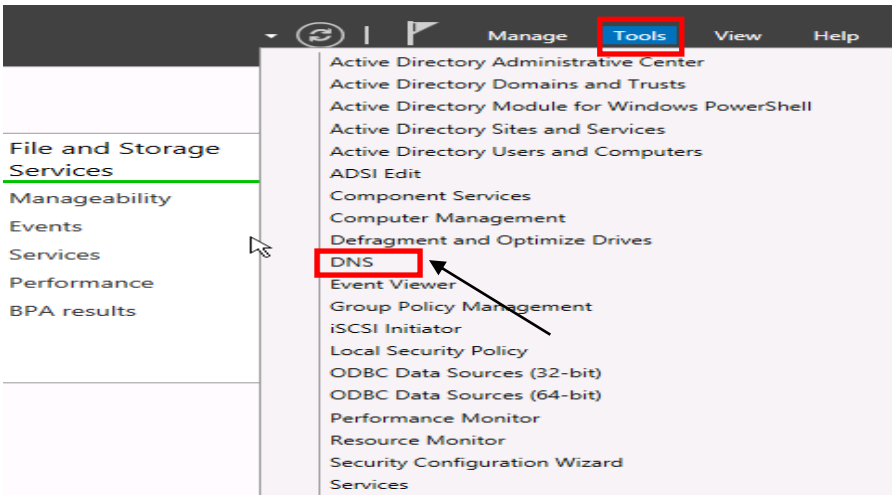
20. When the Active Directory installation finishes, the computer will automatically restart.

ADDITIONAL DNS CONFIGURATION

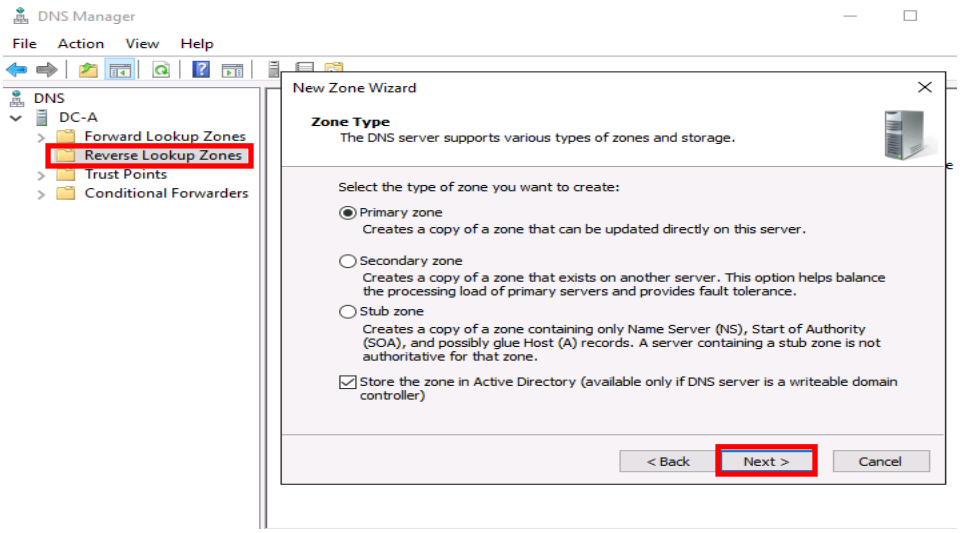
REVERSE LOOKUP ZONES

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

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

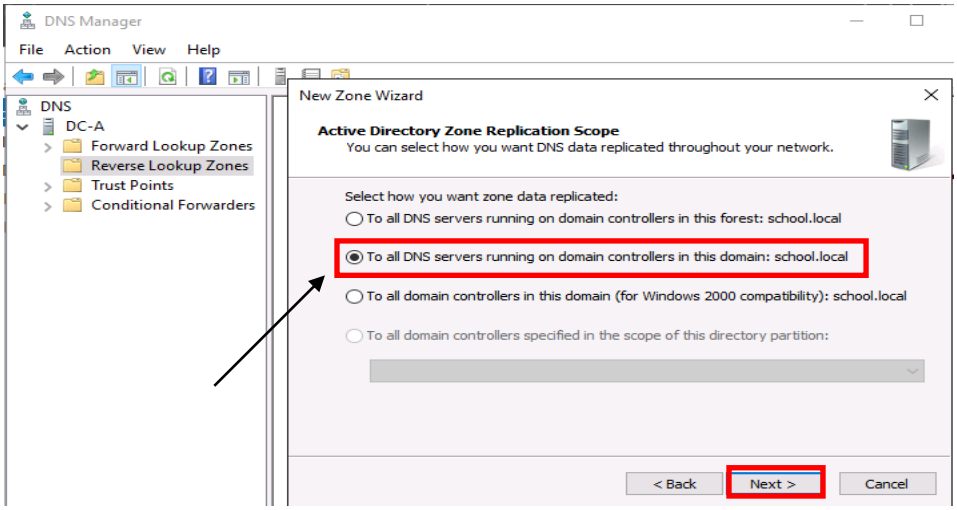


23. Expand your server name, right-click on **Reverse Lookup Zones** and click **New Zone**.



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

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



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

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

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

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

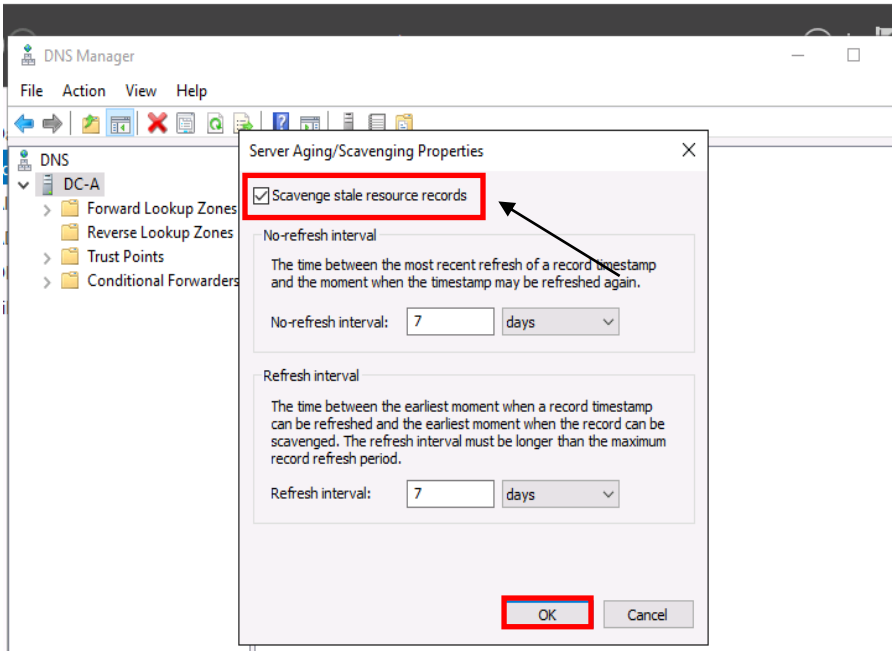
29. Click **Finish** to create the new zone.

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

STALE RECORD SCAVENGING

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

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



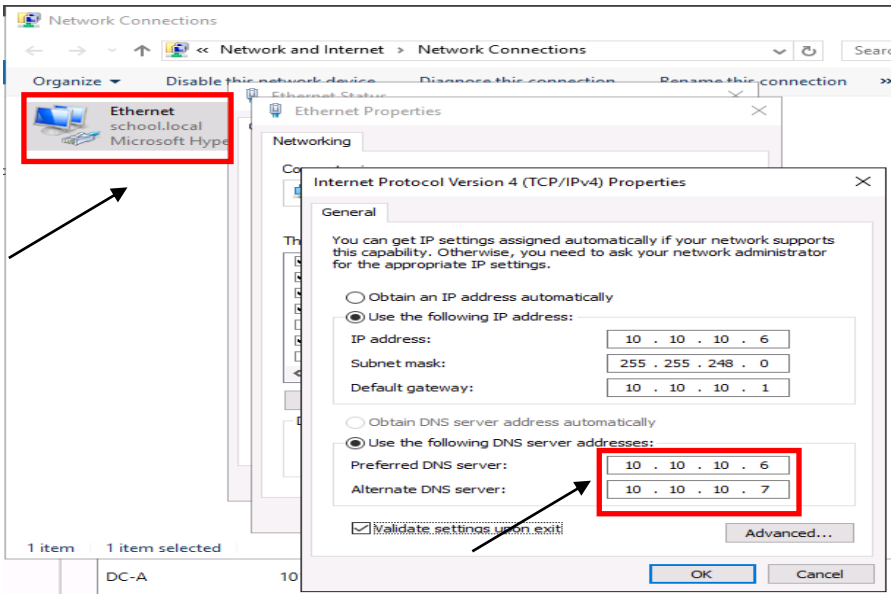
32. When prompted with the Server Aging/Scavenging Confirmation box, check the **Apply these settings to the existing Active Directory-integrated zones option** and then click **OK.**

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

Static IP Address & DNS Servers must be assigned to the network adapter (not a loopback address 127.0.0.1)
The correct method is "Self First" (As Preferred DNS), then other DCS as alternates
Warning – Do Not Point Windows Server DNS to OpenDNS Virtual Appliance Servers

Example
DC1 – IP Address 10.10.10.6
DC2 – IP Address 10.10.10.7

When promoting a new server into an existing Forrest or domain, the new server will have to point to another DC first and can then be changed after the server has been successfully promoted



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 2019, 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.

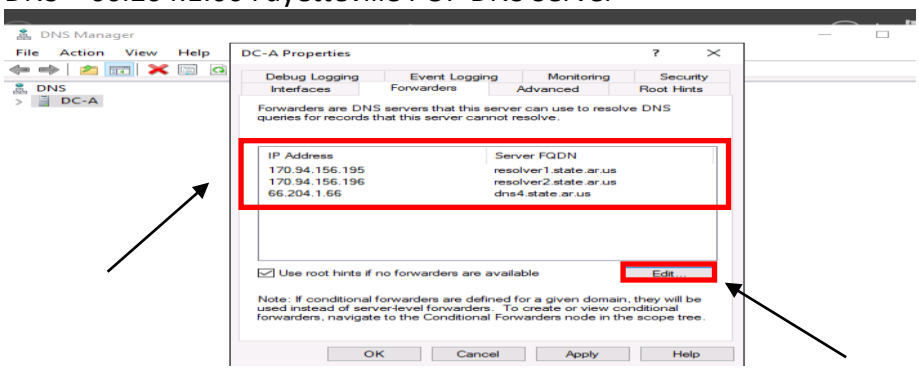
****Exception Cisco Umbrella (OpenDNS Server) – Do Not Use DNS Root Hint**

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

2. Click the **Forwarders** tab and then click the **Edit** button. Add the appropriate Forwarders for your windows environment.

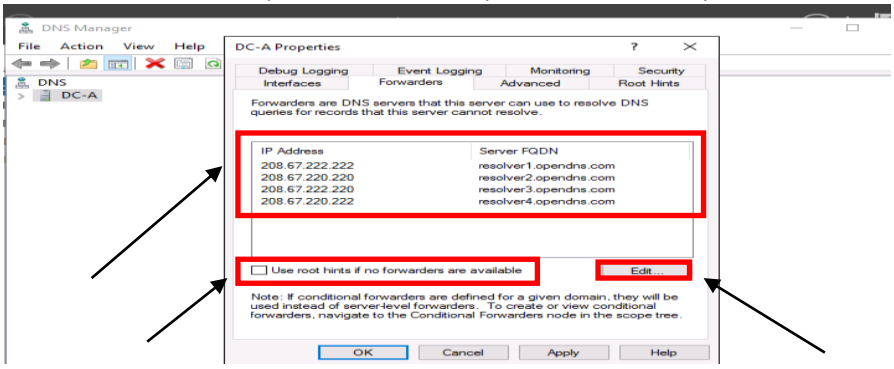
3. Enter your **DIS DNS Servers / OpenDNS Server** as specified below and click **OK**.
   ****OpenDNS Servers are used for Cisco Umbrella Content Filtering**

DIS DNS Servers
DNS = 170.94.156.195, 170.94.156.196 Little Rock DNS Servers
DNS = 66.204.1.66 Fayetteville POP DNS Server



****Please remove all old state DIS DNS Servers (165.29.X.X and 170.211.X.X)**

OpenDNS Servers – Cisco Umbrella (OpenDNS)
DNS = 208.67.222.222, 208.67.220.220, 208.67.222.220, 208.67.220.222



****Warning – Do Not Point Forwarders to OpenDNS Virtual Appliance Servers**
****Do Not Use Google DNS Servers 8.8.8.8, 8.8.4.4 - (Lockdown Browser)**
****Uncheck – Use root hints if no forwarders are available (Do Not Use)**

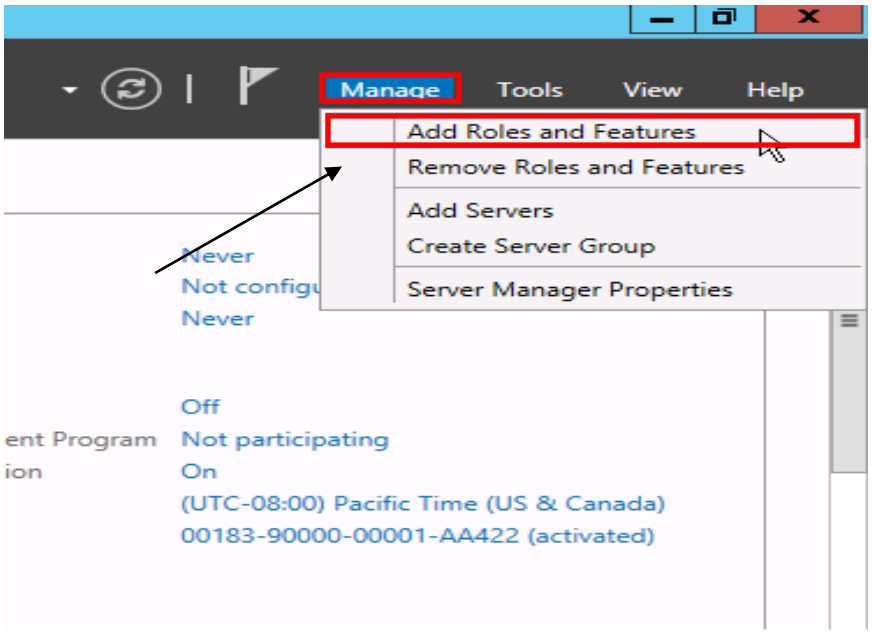
4. Click **Apply** and then **OK**.

5. Close the DNS Manager

DHCP INSTALLATION AND CONFIGURATION

1. Launch **Server Manager.**

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



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

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

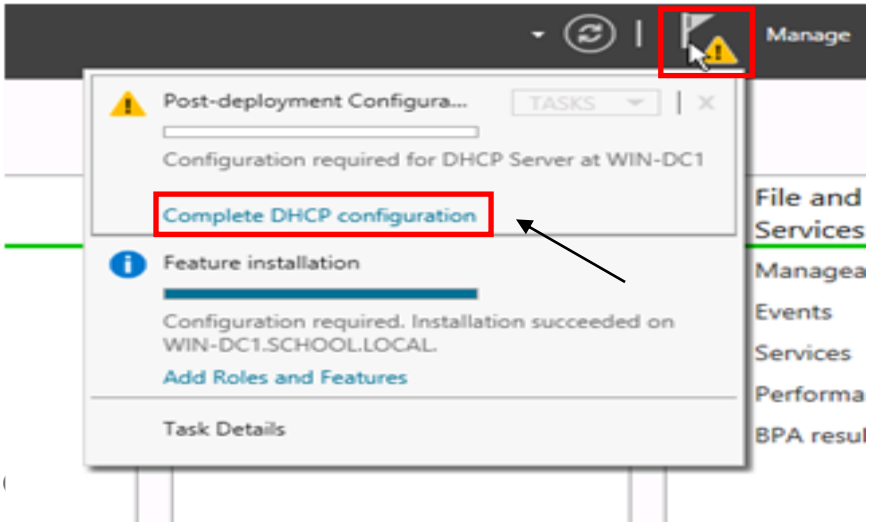
5. On the **Select Destination server** screen**,** click **Next**.

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

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

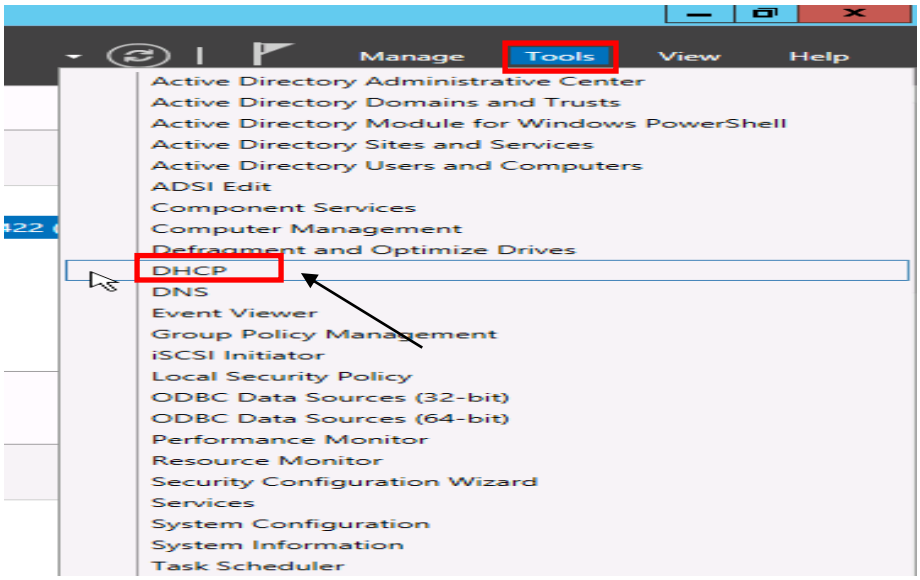
8. When the installation is finished, click **Close**.

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

10. 

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

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



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

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

15. On the **Scope Name** screen enter the Scope name and description you want to use for this scope e.g. IP NAT POOL
16. On the **IP Address Range** screen type in the starting and ending IP address for this scope along with the subnet mask. This is the range of IP addresses this DHCP server will be issuing. Click **Next**.

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

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

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

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

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

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

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

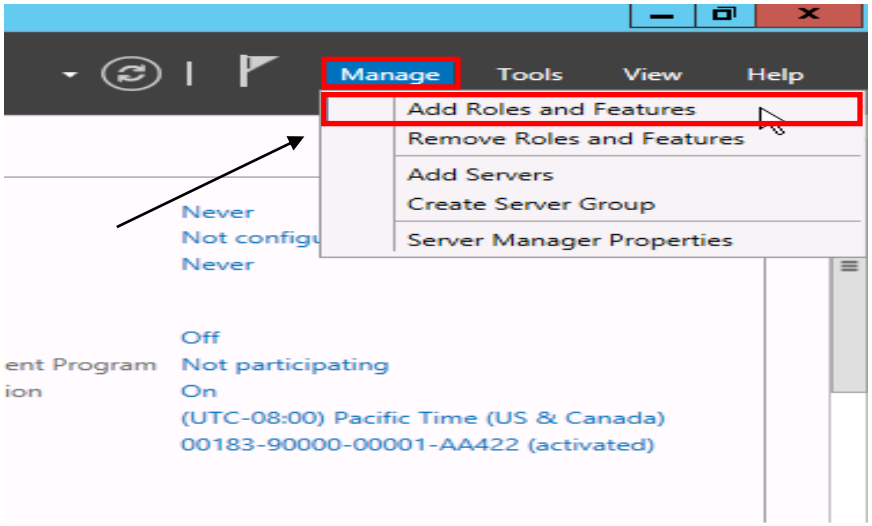
22. Also, under **Advanced** tab click on the **Bindings** button and verify that the only network adapter checked is the adapter that is on the same subnet the DHCP server will be serving IP addresses for.

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

WINS INSTALLATION AND CONFIGURATION

1. Launch **Server Manager.**

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



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

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

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

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

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

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

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

10. Open up **WINS** Manager by selecting **Tools** in the **Server Manager** and then selecting WINS from the drop down list.
11. Expand the respective WINS Server and click on **Replication Partners.**

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

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

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

WINDOWS SERVER UPDATE SERVICES (WSUS)

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

For Windows Server 2019, WSUS requires the following:

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

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

CONFIGURING WSUS AFTER INSTALLATION

1. Launch Server Manager.

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

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

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

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

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

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

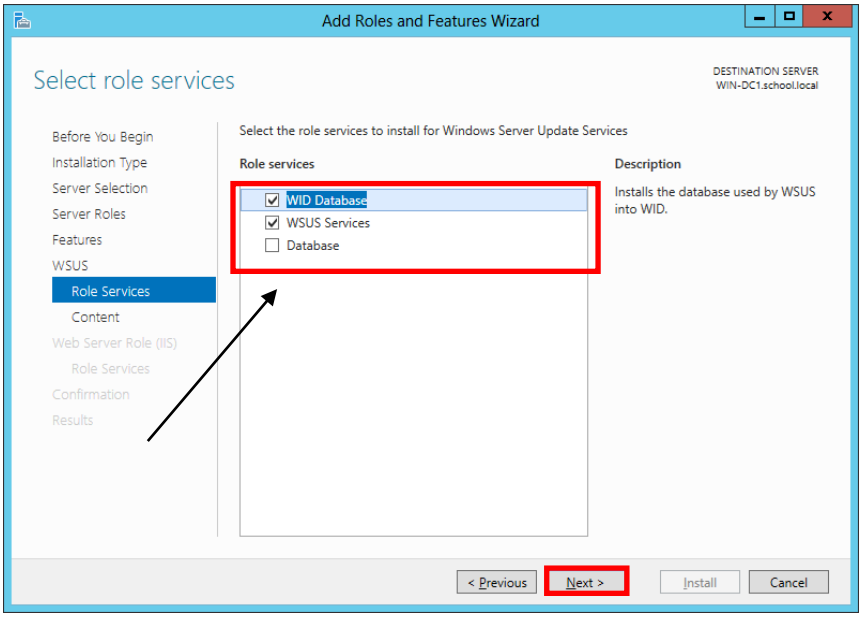
8. On the **Select features** page, leave the default selections, and then click **Next.**

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

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

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

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



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

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

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

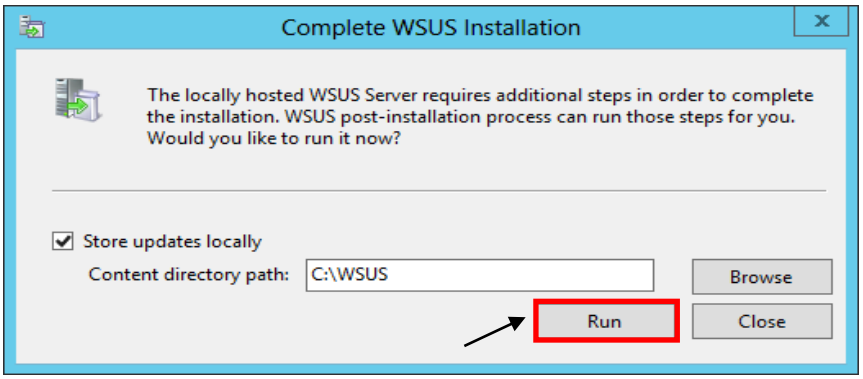
13. On the **Select role services** page, leave the default selections, and then click **Next**.

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

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

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

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



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

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

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

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

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

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

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

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

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

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

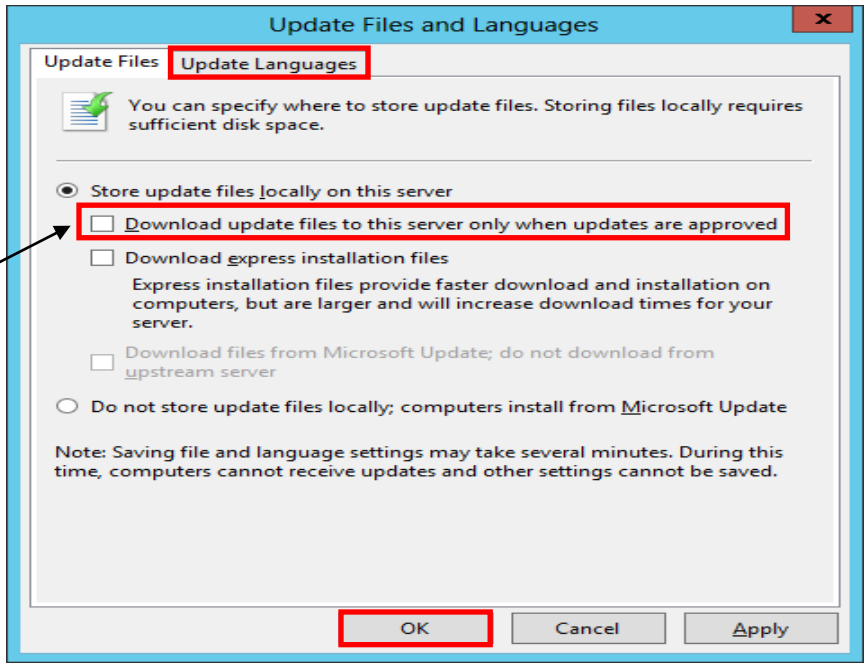
27. On the **Choose Classifications** page, it is recommended to select everything **EXCEPT** Drivers and click **Next**.

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

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

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

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

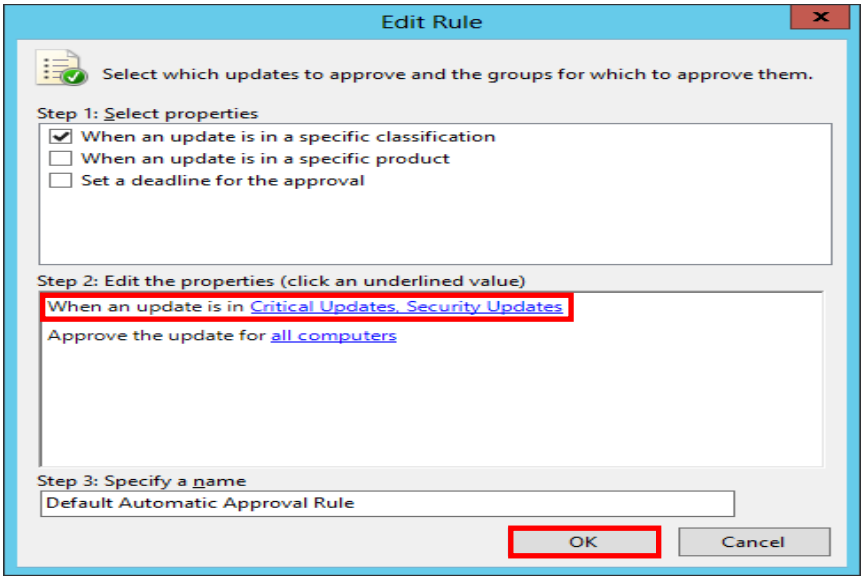


*****If you choose to manually approve updates, your workstations will not have to wait until after the next WSUS Sync with Microsoft to get the updates.***

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

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

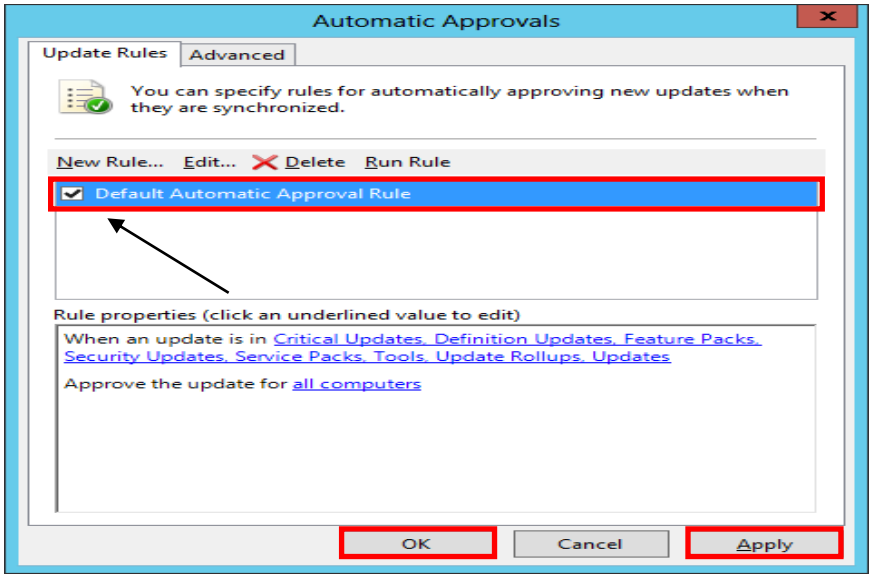
34. In the Step 2 box, click on **Critical Updates, Security Updates.**



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

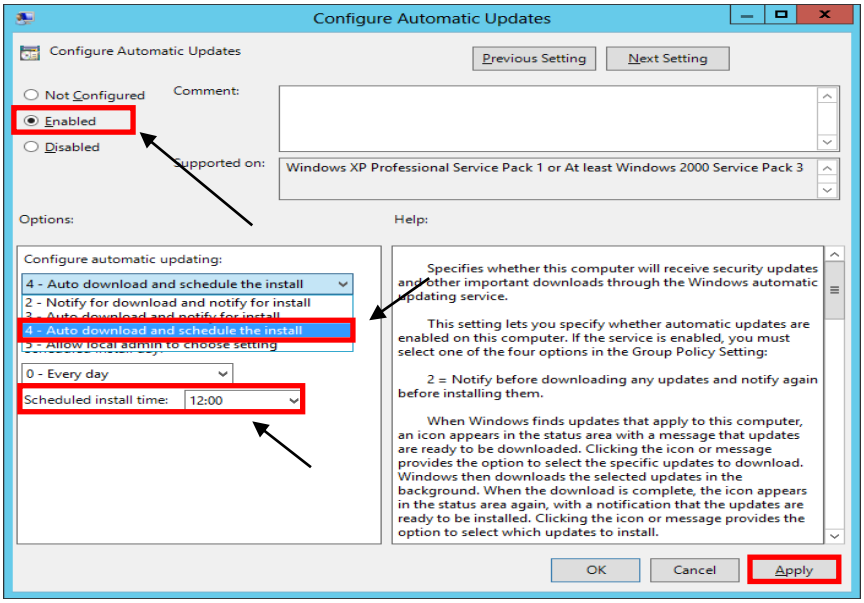
*****Some districts choose not to select Feature Packs. These include items such as Silver Light and Desktop Search.***

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



WSUS Group Policy

1. Launch **Server Manager**.
2. Click on **Tools** and select **Group Policy Management** from the drop down list.
3. Expand Forest: **yourdomain.local.**
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Group Policy Objects**.
5. Right-click on the **Group Policy Objects** and then select **New**.
6. Name the new group policy **WSUS Policy** and click **OK**.
7. Expand **Group Policy Objects**. Right-click the newly created W**SUS Policy** and click **Edit** to open the Group Policy Editor.
8. Expand **Computer Configuration > Policies > Administrative Templates** > **Windows Components** and select **Windows Update**.
9. Double-click on **Configure Automatic Updates,** change **Not Configured** to **Enabled** and select option **4 – Auto Download and schedule install** under Configure automatic updating drop-down menu.
10. Set the desired scheduled install day and time.



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

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

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

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

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

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

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

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

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

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

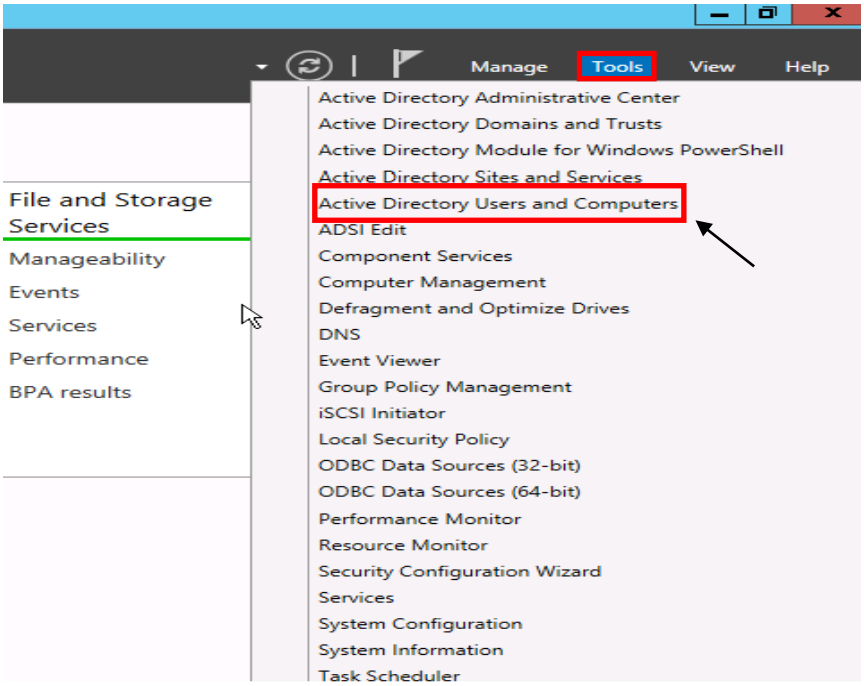
*****It is recommended to have a separate Group Policy for Domain Servers and Domain workstations to avoid automatic restart on servers.***

BASIC ACTIVE DIRECTORY STRUCTURE FOR K12

SINGLE SITE ACTIVE DIRECTORY NETWORKS

1. Launch **Server Manager**.

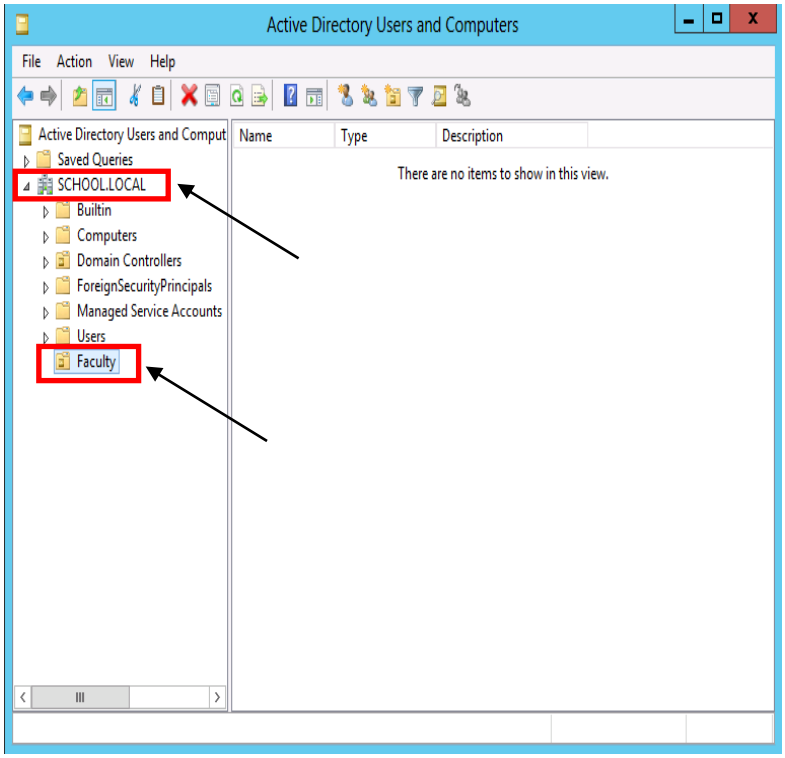
2. Click on **Tools** and select **Active Directory Users and Computers** from the drop down list



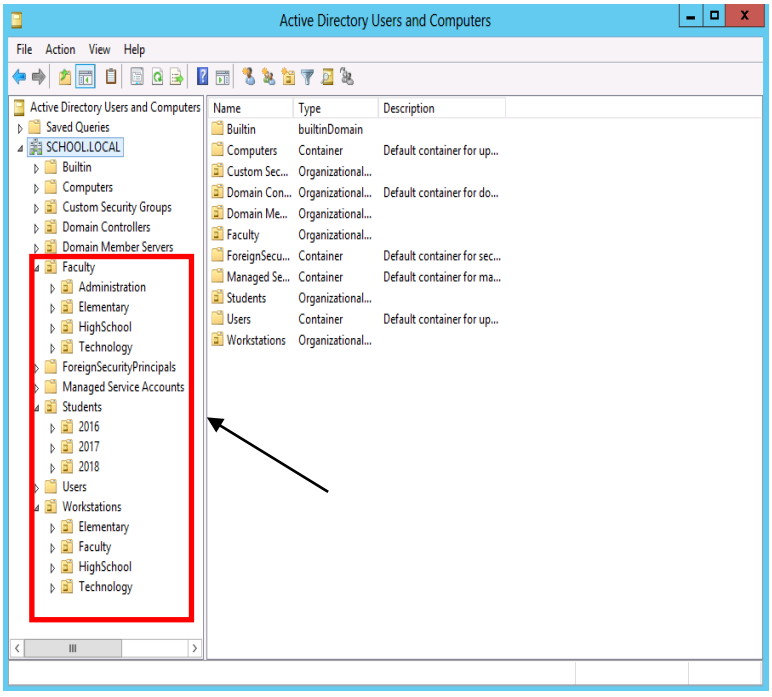
3. Right-click on **YourDomain.LOCAL**, click **New**, then **Organizational Unit (OU)**.

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

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



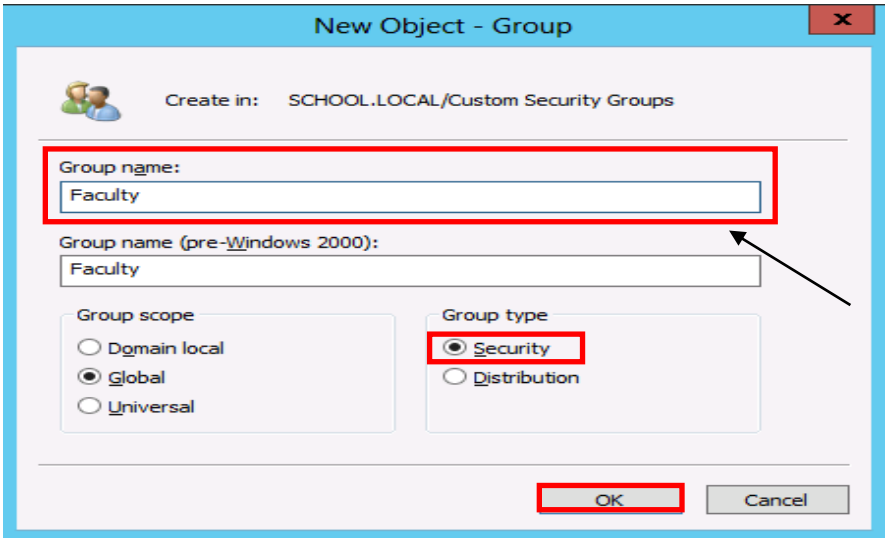
Repeat Steps 2 and 3 for Organizational Units required in your Active Directory environment e.g. Students, Workstations, Domain Member Servers, and Custom Security Groups.



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

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

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



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

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

CREATE SHARES AND HOME DIRECTORIES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

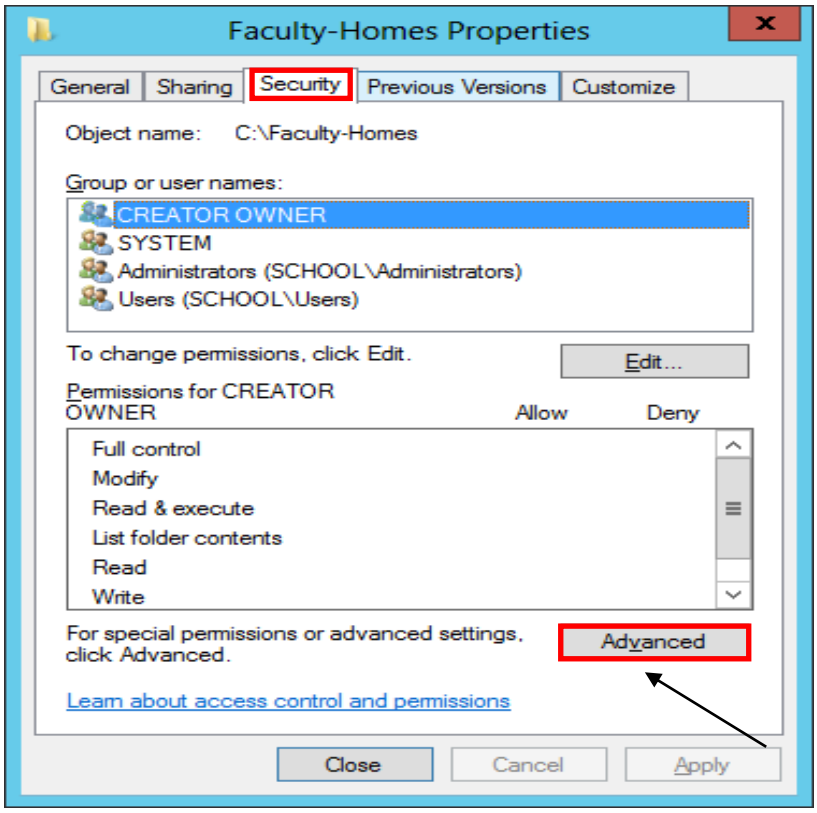
11. Give the **Faculty** group **Change** rights, they will receive Read automatically.

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

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

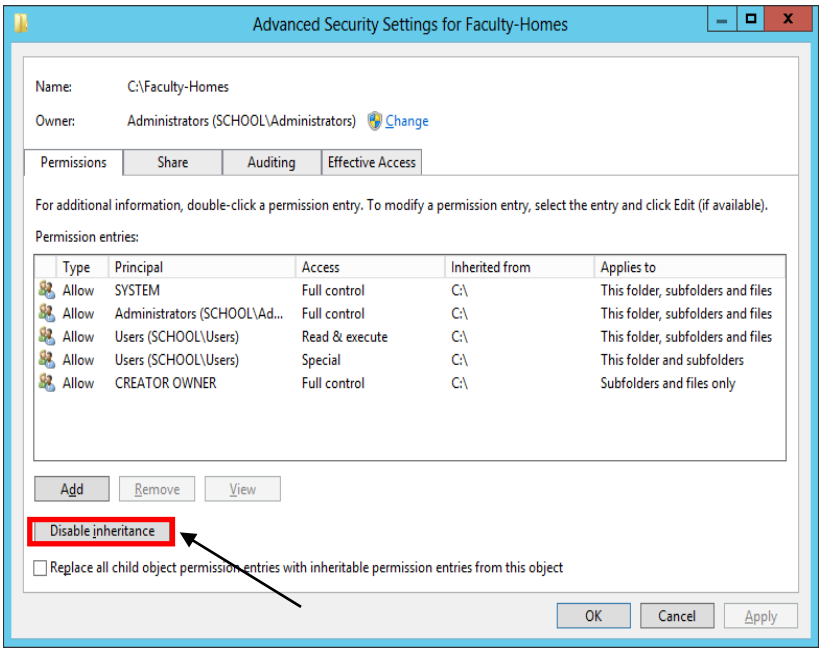
13. Click **OK**, **Apply**, and then **OK** until all property windows are closed.

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



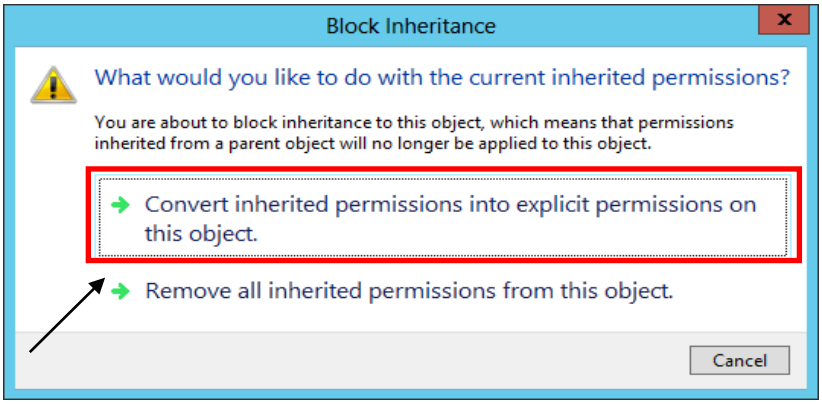
15. On the **Advanced Security Settings** page, click on **Disable inheritance**.

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



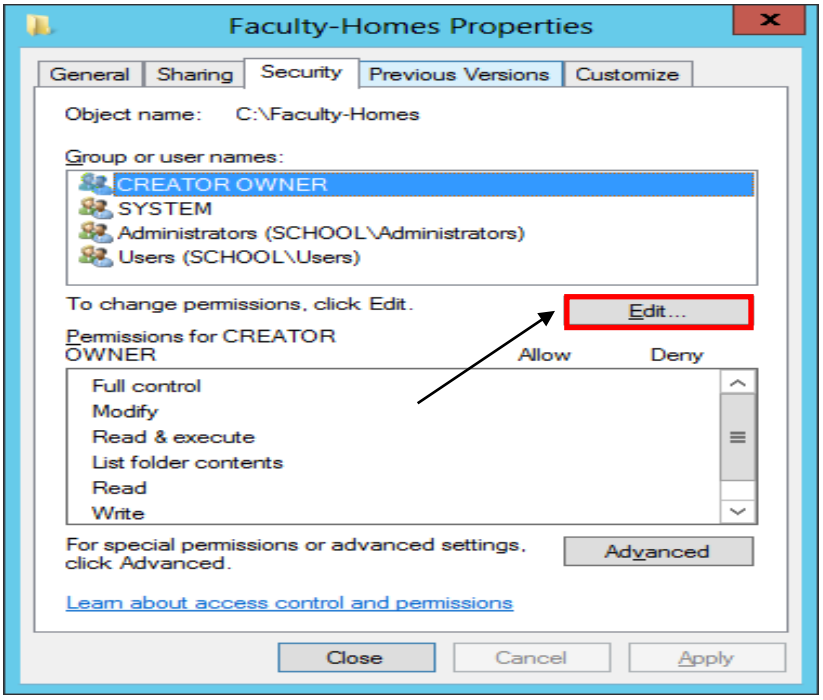
16. A dialog box prompting that permission inheritance from the parent folder is being blocked will popup.

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



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

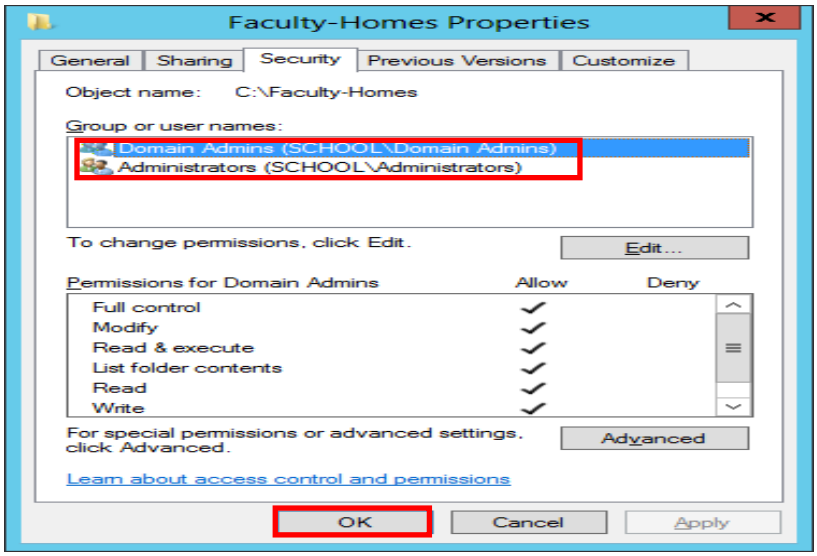
19. Your permissions to Faculty-Homes should now look like the following screen.



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

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

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

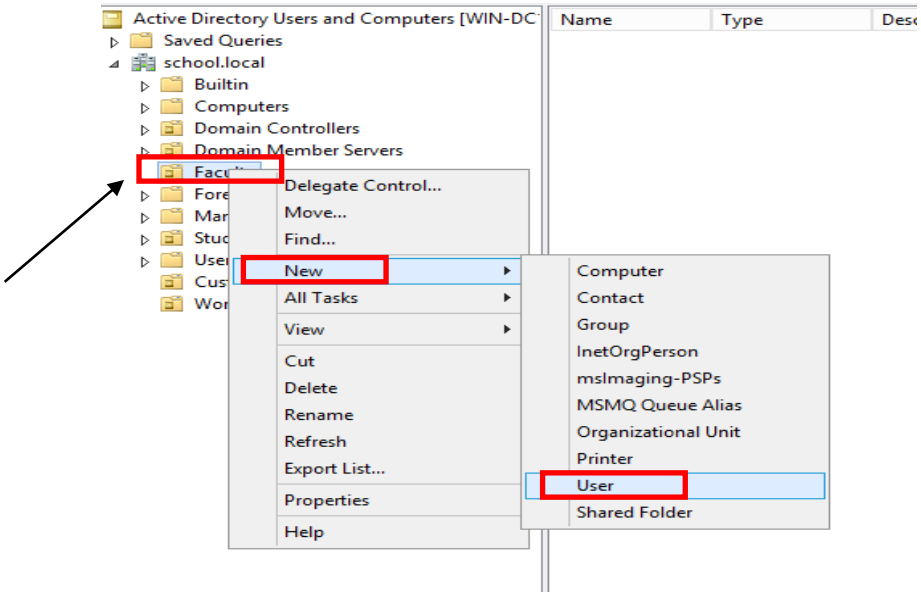


CREATING USER TEMPLATE

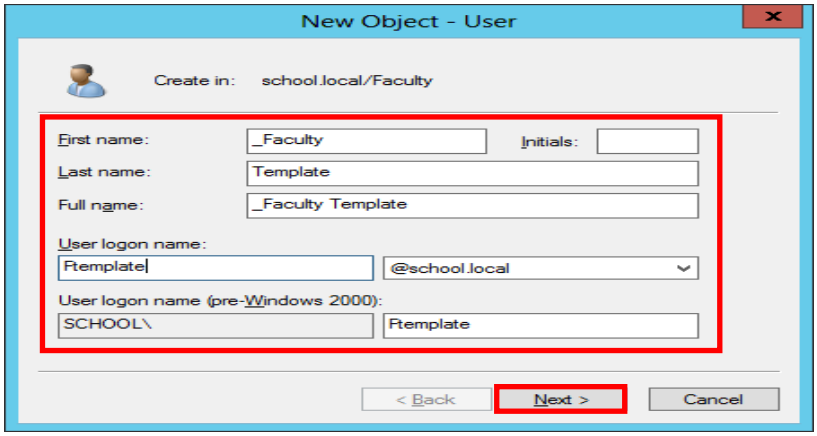
Now that the network share to store home directories is set up, User template will be created using the following steps:

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

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



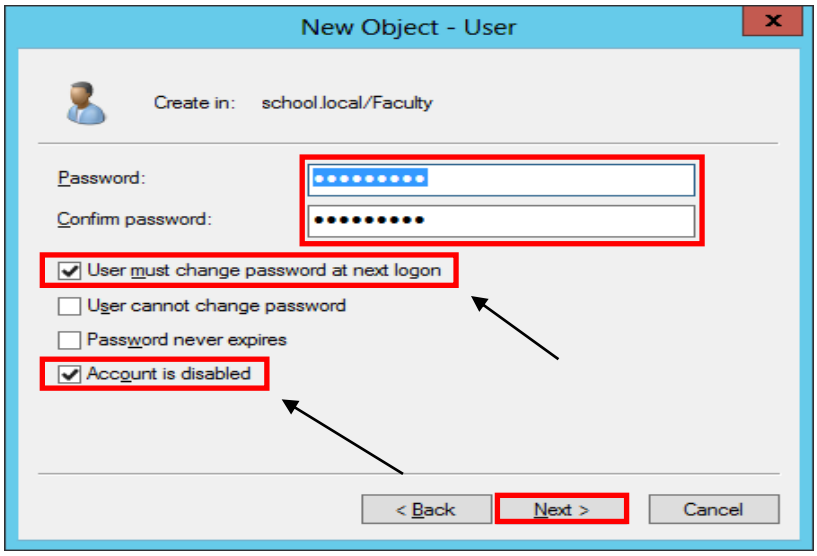
25. In the information screen fill it out as shown in this screen and then click **Next**.



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

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

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



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

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

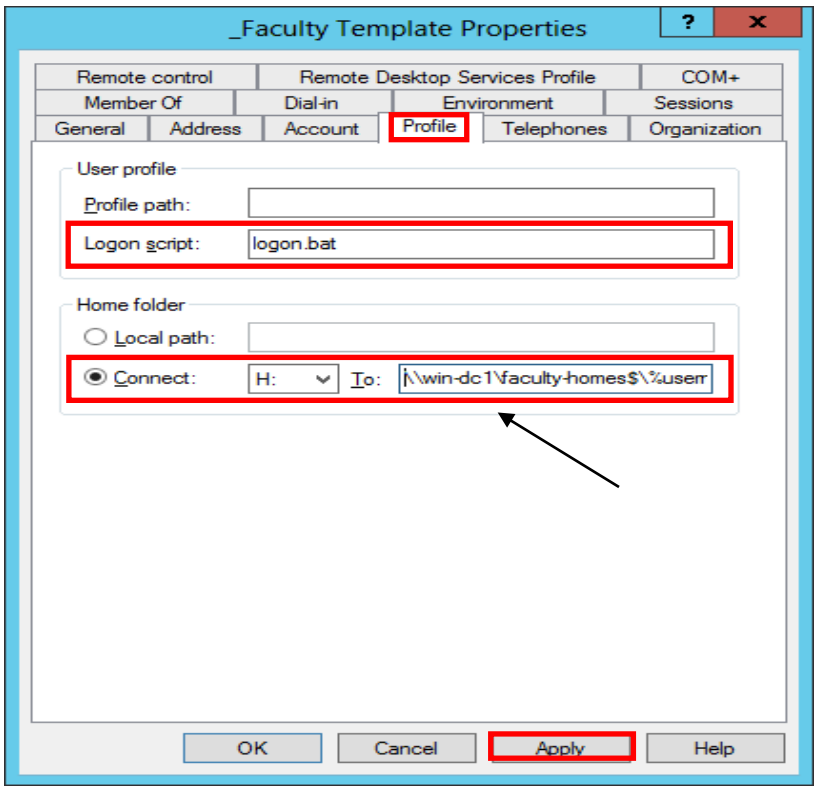
28. Click on the **Member Of** tab and then click on **Add**.

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

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

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

32. Select the drive letter to be used for user's home directory when it is mapped.
33. In the **To:** text box enter **\\servername\Faculty-Homes$\%username%**



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

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

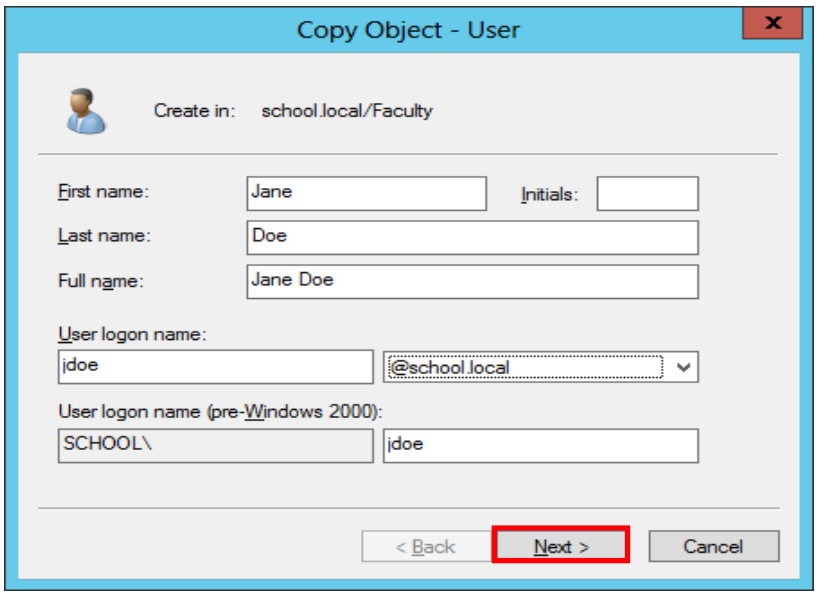
35. This will create a new subfolder called **FTemplate** under **Faculty-Homes** folder with the proper rights.

CREATING NEW USER USING TEMPLATE

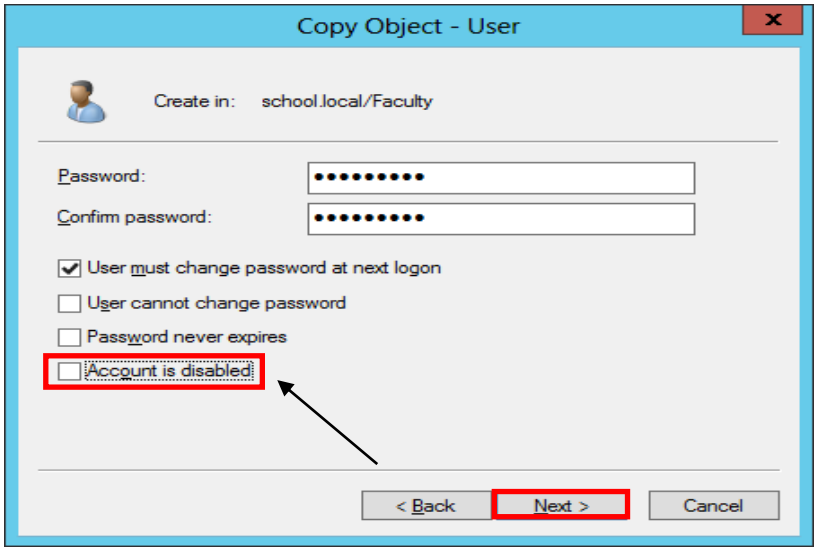
To create a new account based off the template, use the following steps:

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

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



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



CREATING FACULTY & STUDENT BATCH FILE FOR ACTIVE DIRECTORY – MASS IMPORT

Script for Active Directory (AD) Name Importing
****Notes: Must be revised for the domain!!!** (school.local)

Student Script: (Column F)

```
="dsadd user " & CHAR(34) & "CN=" & PROPER(A1) & " " & PROPER(B1) & ",OU=" & C1 &
",OU=Students,DC=school,DC=Local" & CHAR(34) & " -samid " & PROPER(A1) & "." &
PROPER(B1) & " -upn " & Lower(D1) & "@school.local -fn " & PROPER(A1) & " -ln " &
PROPER(B1) & " -display " & CHAR(34) & PROPER(A1) & " " & PROPER(B1) & CHAR(34) &
" -pwd " & E1 & " -mustchpwd Yes -memberof
CN=Students,OU=Students,DC=school,DC=Local"
```

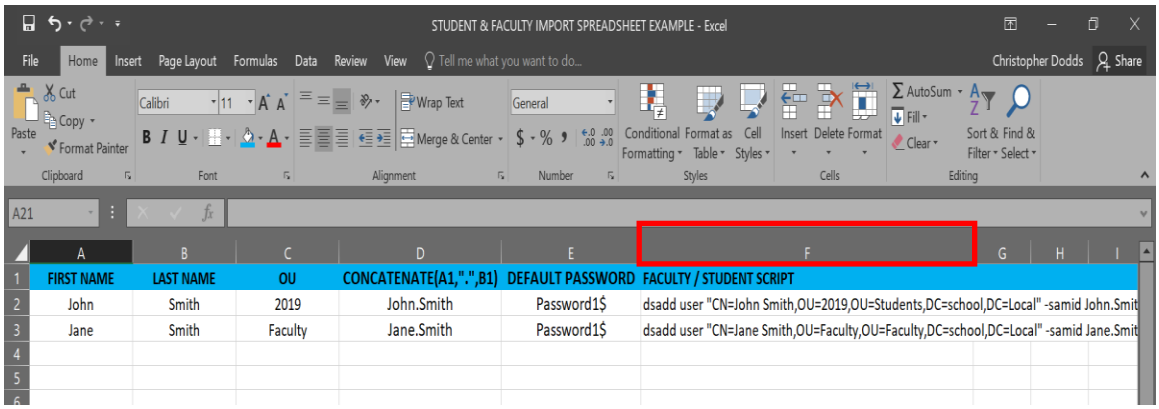
Faculty Script: (Column F)

```
="dsadd user " & CHAR(34) & "CN=" & PROPER(A1) & " " & PROPER(B1) & ",OU=" & C1 &
",OU=Faculty,DC=school,DC=Local" & CHAR(34) & " -samid " & PROPER(A1) & "." &
PROPER(B1) & " -upn " & Lower(D1) & "@school.local -fn " & PROPER(A1) & " -ln " &
PROPER(B1) & " -display " & CHAR(34) & PROPER(A1) & " " & PROPER(B1) & CHAR(34) &
" -pwd " & E1 & " -mustchpwd Yes -memberof
CN=Faculty,OU=Faculty,DC=school,DC=Local"
```

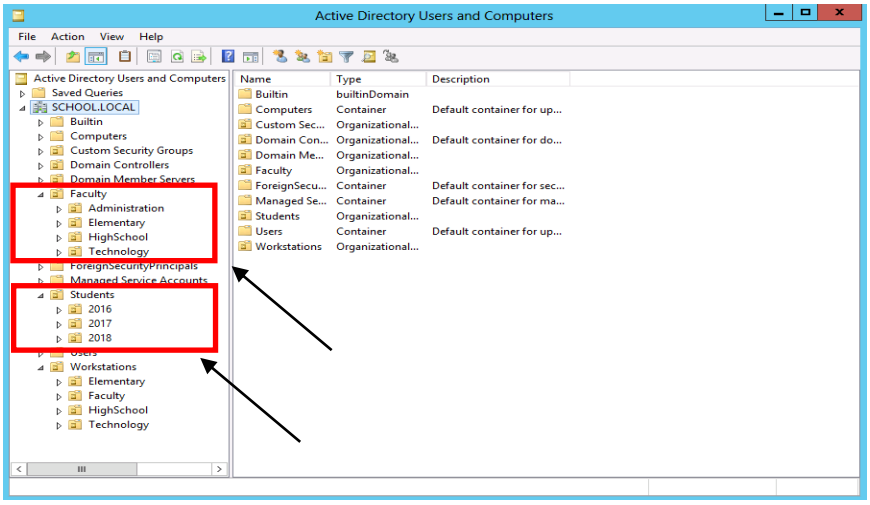
SPREAD SHEET DATA EXAMPLE

A1	B1	C1	D1	E1	F1
FIRST NAME	LAST NAME	OU Graduation Year	=CONCATENATE(A1,".",B1)	Password (default)	STUDENT / FACULTY SCRIPT
John	Smith	STUDENT 2019, 2020	John.Smith	Password1$	STUDENT SCRIPT
Jane	Smith	FACULTY High School	Jane.Smith	Password1$	FACULTY SCRIPT

SPREAD SHEET REFERENCE GUIDE



1. **Create Organizational Units (OU's)** in Active Directory (AD) new accounts



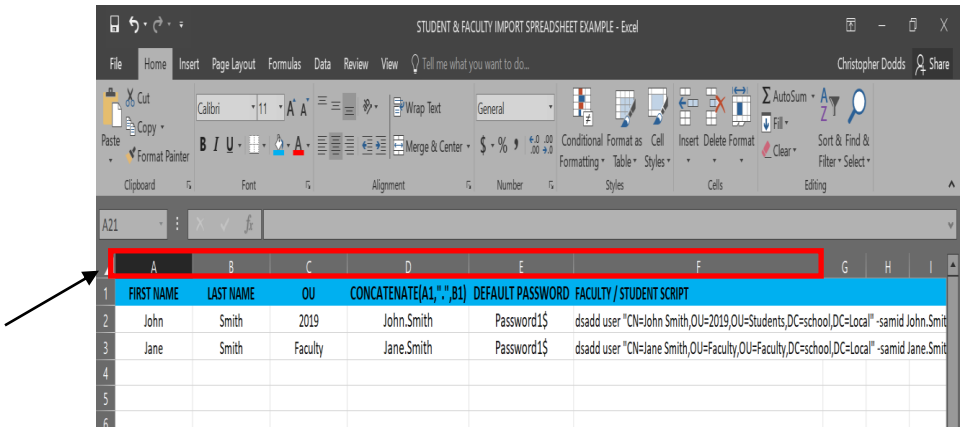
2. Student Graduation Year Reference Guide
   ****Add graduation year versus grade level for data management**

```
State law requires student logins for Grades 4th - 12th Grades

2022 - 12
2023 - 11
2024 - 10
2025 - 9
2026 - 8
2027 - 7
2028 - 6
2029 - 5
2030 - 4
2031 - 3
2032 - 2
2033 - 1
```

3. **Export Student / Faculty File** from Cognos (excel csv.)

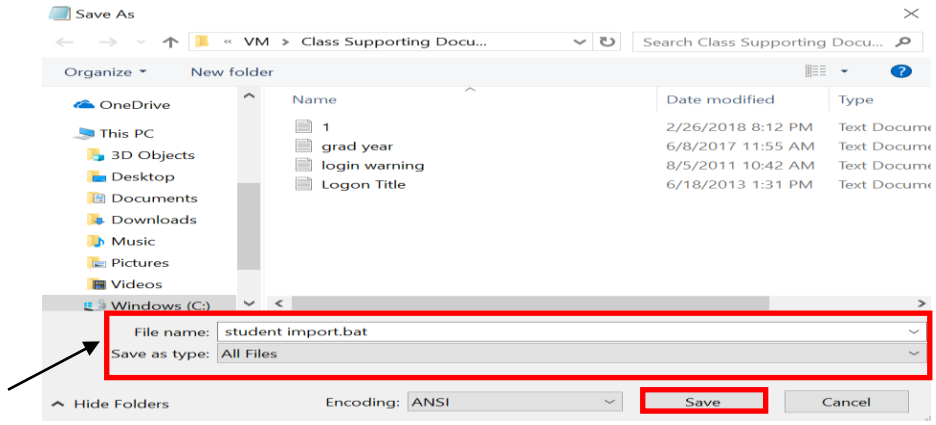
4. Open Excel Spreadsheet with Student / Faculty Data & Copy Data into Correct Columns (**A,B,C,D,E & F**)
   ****Data must be texted to columns and all special characters removed**



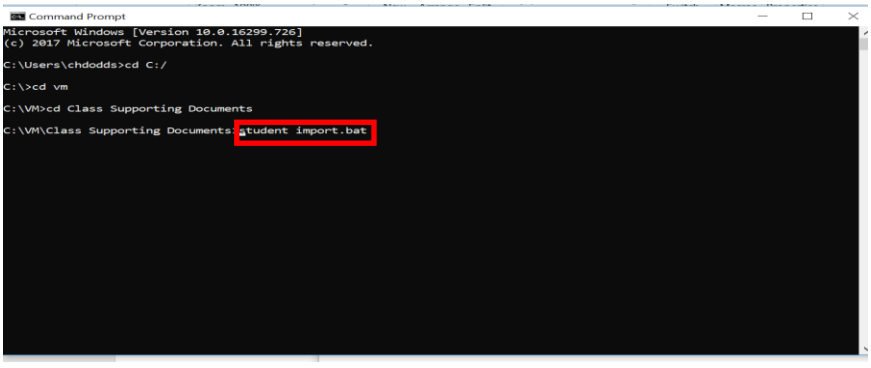
5. **Copy Data** from **Column F** and save to **New Text Document** (.txt)

```
File  Edit  Format  View  Help
dsadd user "CN=Charlie Brown,OU=2018,OU=Students,DC=school,DC=Local" -samid Charlie.Brown -upn charlie.brown@school.local -fn Charlie -ln Brown -d
dsadd user "CN=Johnny Appleseed,OU=2018,OU=Students,DC=school,DC=Local" -samid Johnny.Appleseed -upn johnny.appleseed@school.local -fn Johnny -ln
dsadd user "CN=Michael Jackson,OU=2019,OU=Students,DC=school,DC=Local" -samid Michael.Jackson -upn michael.jackson@school.local -fn Michael -ln Ja
dsadd user "CN=Abraham Lincoln,OU=2020,OU=Students,DC=school,DC=Local" -samid Abraham.Lincoln -upn abraham.lincoln@school.local -fn Abraham -ln Li
dsadd user "CN=Brad Pitt,OU=2021,OU=Students,DC=school,DC=Local" -samid Brad.Pitt -upn brad.pitt@school.local -fn Brad -ln Pitt -display "Brad Pit
dsadd user "CN=Robert Downey,OU=2022,OU=Students,DC=school,DC=Local" -samid Robert.Downey -upn robert.downey@school.local -fn Robert -ln Downey -d
dsadd user "CN=Tom Cruise,OU=2023,OU=Students,DC=school,DC=Local" -samid Tom.Cruise -upn tom.cruise@school.local -fn Tom -ln Cruise -display "Tom
dsadd user "CN=Tom Hanks,OU=2024,OU=Students,DC=school,DC=Local" -samid Tom.Hanks -upn tom.hanks@school.local -fn Tom -ln Hanks -display "Tom Hank
dsadd user "CN=Matt Damon,OU=2025,OU=Students,DC=school,DC=Local" -samid Matt.Damon -upn matt.damon@school.local -fn Matt -ln Damon -display "Matt
dsadd user "CN=Jed Clampett,OU=2026,OU=Students,DC=school,DC=Local" -samid Jed.Clampett -upn jed.clampett@school.local -fn Jed -ln Clampett -displ
dsadd user "CN=Mickey Mouse,OU=2018,OU=Students,DC=school,DC=Local" -samid Mickey.Mouse -upn mickey.mouse@school.local -fn Mickey -ln Mouse -displ
dsadd user "CN=Daffy Duck,OU=2019,OU=Students,DC=school,DC=Local" -samid Daffy.Duck -upn daffy.duck@school.local -fn Daffy -ln Duck -display "Daff
dsadd user "CN=Homer Simpson,OU=2020,OU=Students,DC=school,DC=Local" -samid Homer.Simpson -upn homer.simpson@school.local -fn Homer -ln Simpson -d
dsadd user "CN=Stewie Griffin,OU=2021,OU=Students,DC=school,DC=Local" -samid Stewie.Griffin -upn stewie.griffin@school.local -fn Stewie -ln Griffi
dsadd user "CN=Fred Flintstone,OU=2022,OU=Students,DC=school,DC=Local" -samid Fred.Flintstone -upn fred.flintstone@school.local -fn Fred -ln Flint
dsadd user "CN=Foghorn Leghorn,OU=2023,OU=Students,DC=school,DC=Local" -samid Foghorn.Leghorn -upn foghorn.leghorn@school.local -fn Foghorn -ln Le
dsadd user "CN=Woody Woodpecker,OU=2024,OU=Students,DC=school,DC=Local" -samid Woody.Woodpecker -upn woody.woodpecker@school.local -fn Woody -ln W
dsadd user "CN=Peter Rabbit,OU=2025,OU=Students,DC=school,DC=Local" -samid Peter.Rabbit -upn peter.rabbit@school.local -fn Peter -ln Rabbit -displ
dsadd user "CN=Elmer Fudd,OU=2026,OU=Students,DC=school,DC=Local" -samid Elmer.Fudd -upn elmer.fudd@school.local -fn Elmer -ln Fudd -display "Elme
dsadd user "CN=Porky Pig,OU=2027,OU=Students,DC=school,DC=Local" -samid Porky.Pig -upn porky.pig@school.local -fn Porky -ln Pig -display "Porky Pi
```

6. **Rename** texted document to batch file (.bat) and Change **Save as type:** All Files



7. Open **Command Prompt** (Run As Administrator) Change Directories to Batch file and Run



8. Once Batch file successfully runs open **Active Directory Users and Computers** & new user accounts should be in their perspective OU's
   ****Use Refresh if accounts don't appear in Active Directory OU's**

LOGON SCRIPTS – BATCH FILE METHOD

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

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

NET USE N: \\DC1\APPS

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

A logon script would look similar to the following:

DO NOT ADD THE REM STATEMENTS

LOGON.BAT

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

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

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

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

```
REM Rename Mapped Drives in My Computer
Wscript.exe \\%userdnsdomain%\netlogon\rename-mapped-drives.vbs

:END
EXIT
```

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

Before

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%**. These commands can be placed in the login script and can also be run from a DOS prompt to check the validity of your syntax.

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

IMPLEMENTING SHADOW COPIES

CLIENT USAGE SCENARIOS

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

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

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

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

WHAT SHADOW COPIES OF SHARED FOLDERS CAN DO

Shadow Copies of Shared Folders helps end users:

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

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

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

IT USAGE SCENARIOS

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

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

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

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

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

Table 1: Benefits of Using Shadow Copies of Shared Folders

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

HOW SHADOW COPY WORKS

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

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

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

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

IMPLEMENTING SHADOW COPIES

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

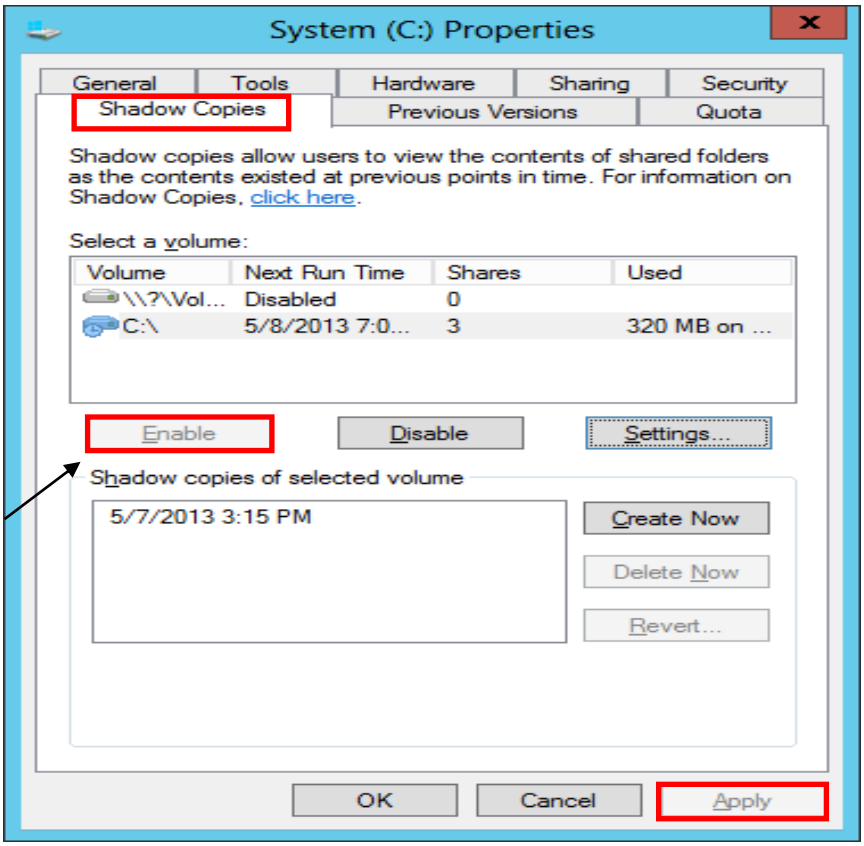
2. **Right-click** on the volume that you would like to enable Shadow Copies and then click **Properties**.

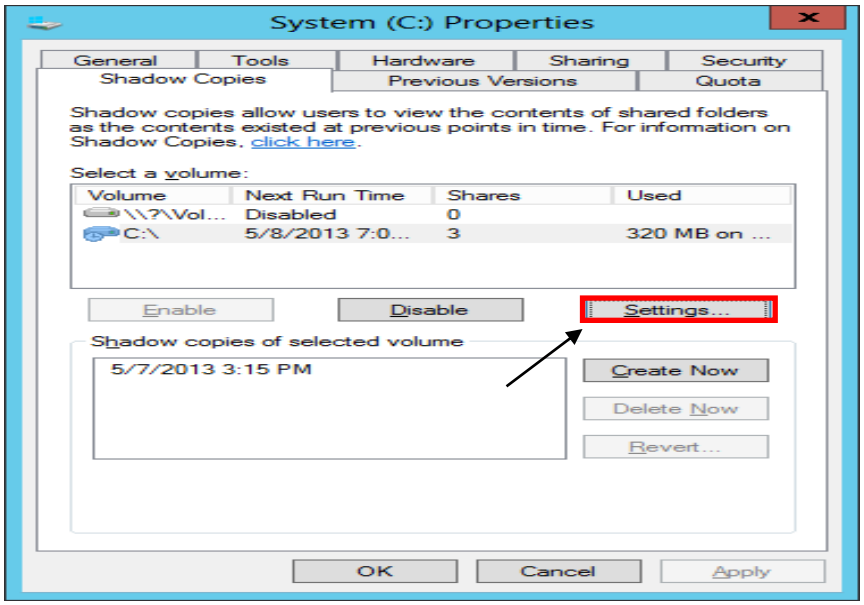
3. Click on the **Shadow Copies** tab.

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

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

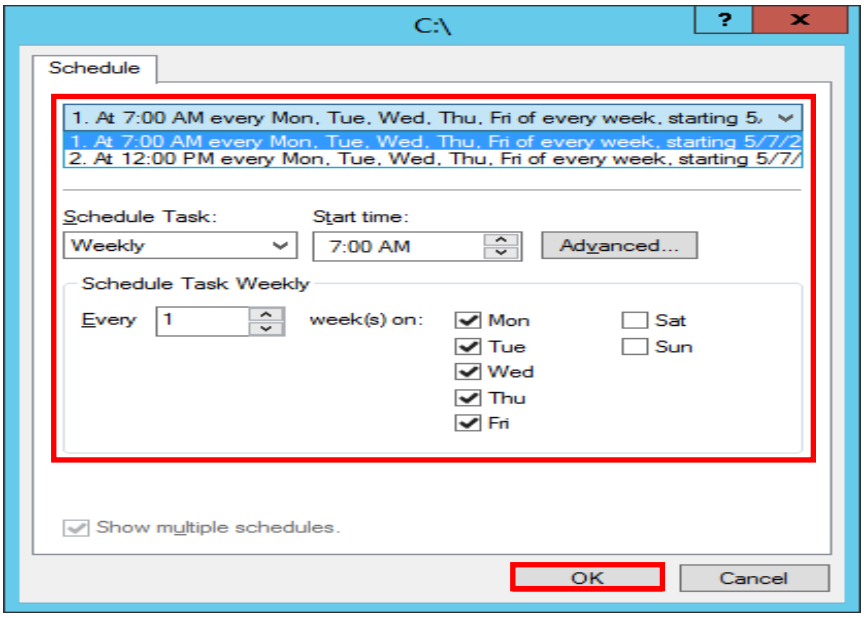
6. Click on the volume that you enabled Shadow Copies for then click the **Settings** button.





7. Click the **Schedule** button.

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



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

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

Implementing Volume Based Quota Limits

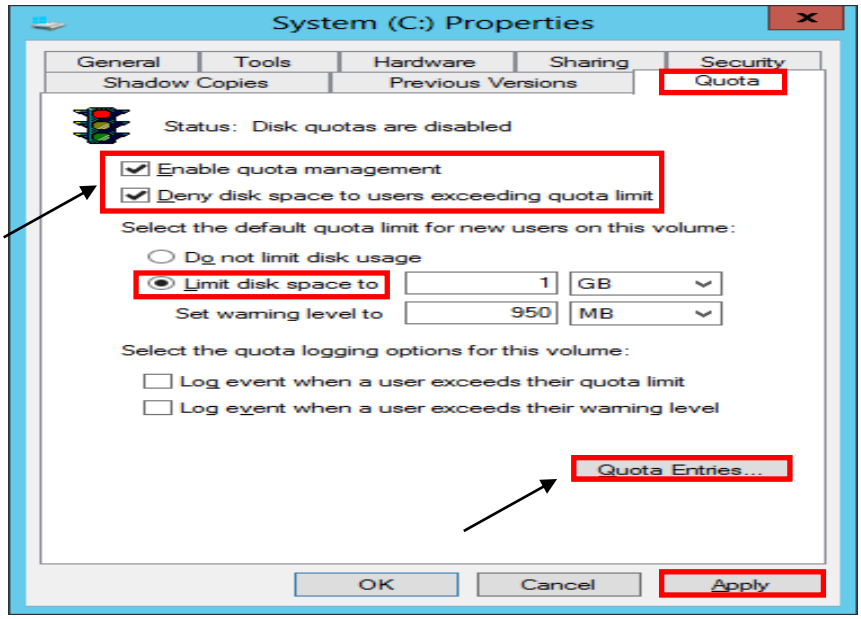
Volume Level Quota Limits using Properties

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

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

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

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



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

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

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

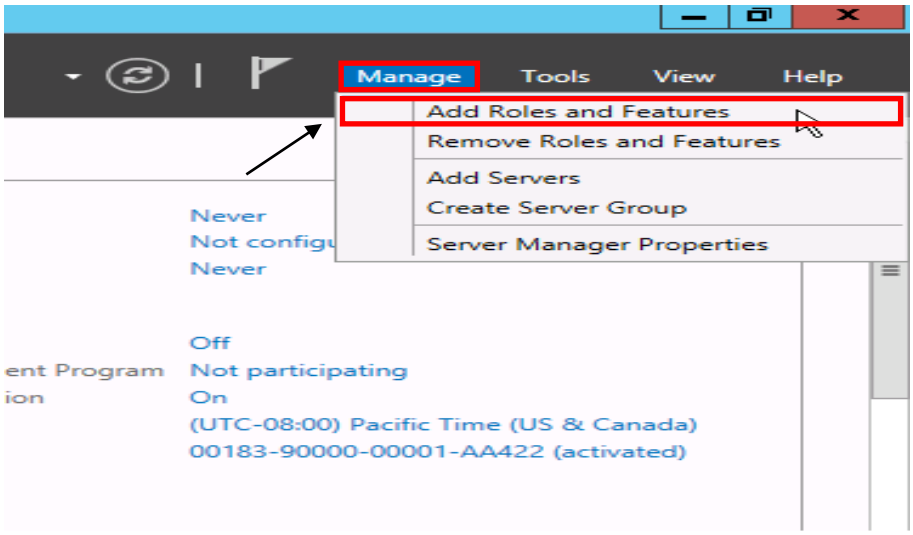
To view user's current disk utilization, click on the Quota Entries button from within the window.

DIRECTORY LEVEL QUOTA LIMITS USING FILE SERVER RESOURCE MANAGER

INSTALL FILE SERVER RESOURCE MANAGER

1. Launch **Server Manager**.

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



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

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

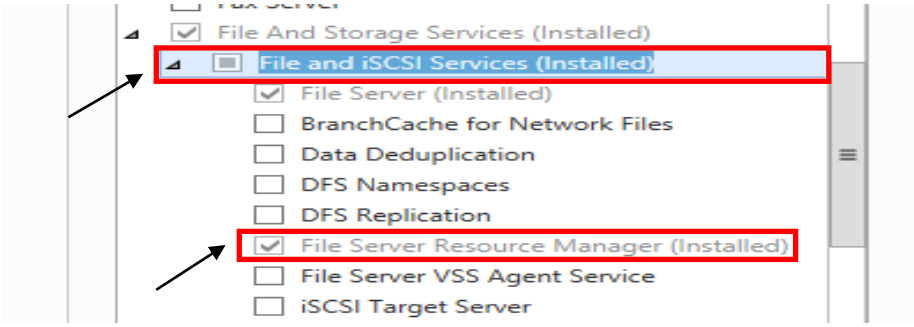
5. On the **Select Destination server** screen**,** click **Next.**

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

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

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

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



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

CONFIGURE QUOTA TEMPLATES

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

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

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

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

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

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

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

APPLY QUOTA TEMPLATE TO DIRECTORY

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

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

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

21. Select the following quota type:

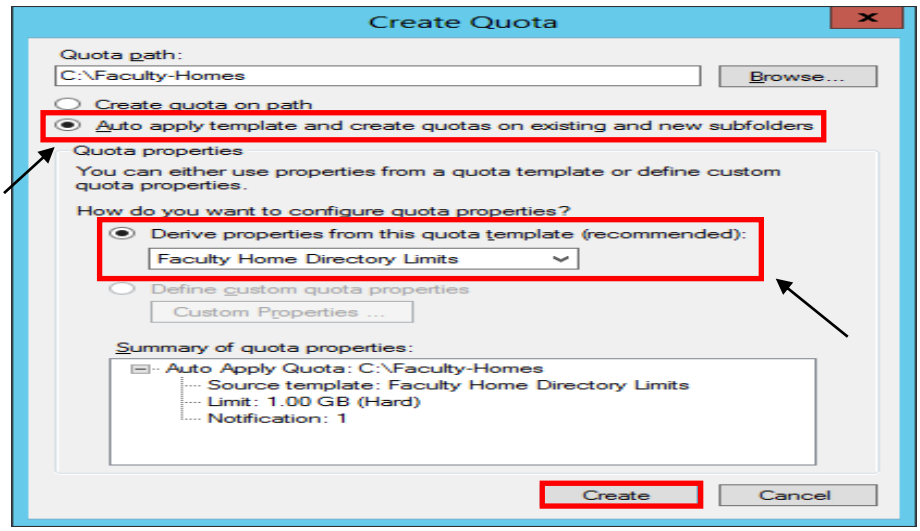
    Create quota on path – This will apply the space limitation to ALL files and folders within the parent directory.

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

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

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

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



FINE-GRAINED PASSWORD POLICIES (ACT-723)

One of the nice features introduced in Windows Server 2019 AD DS is the ability to configure fine grained password policies through GUI.

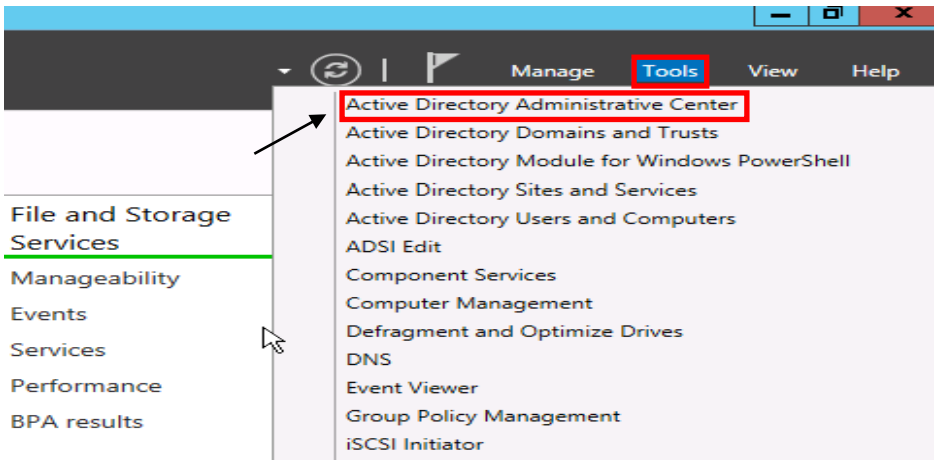
Fine grained password policies allow Network Administrators to configure multiple password policies within a single domain which can be used to apply different restrictions for password and account lockout policies to different sets of users and groups.

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

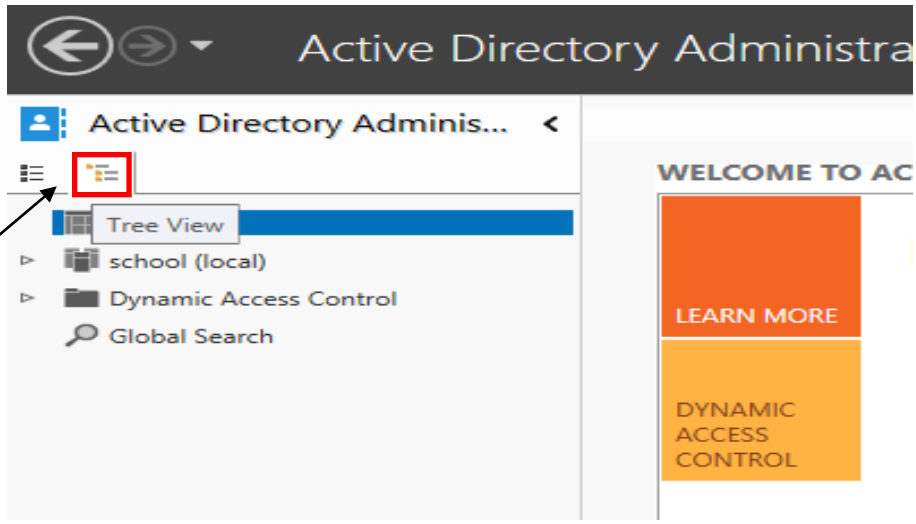
To configure fine-grained password policies as per the table above (ACT723 - K12 State Security Policies), use the following steps:

1. Launch **Server Manager**.

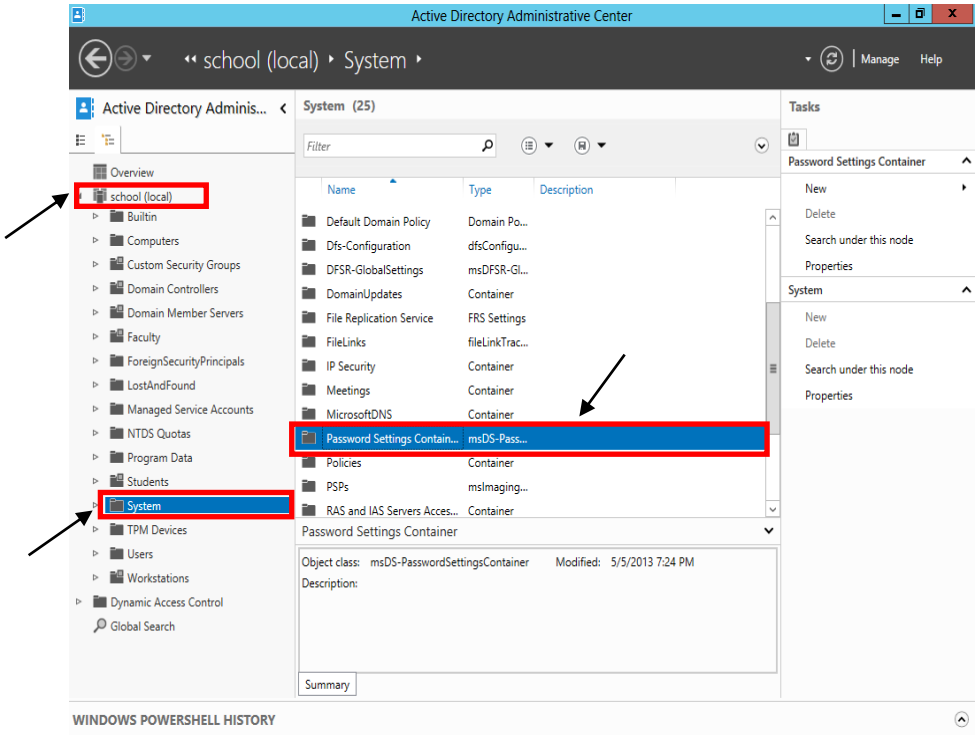
2. Click on **Tools** and select **Active Directory Administrative Center (ADAC)** from the drop down list.



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

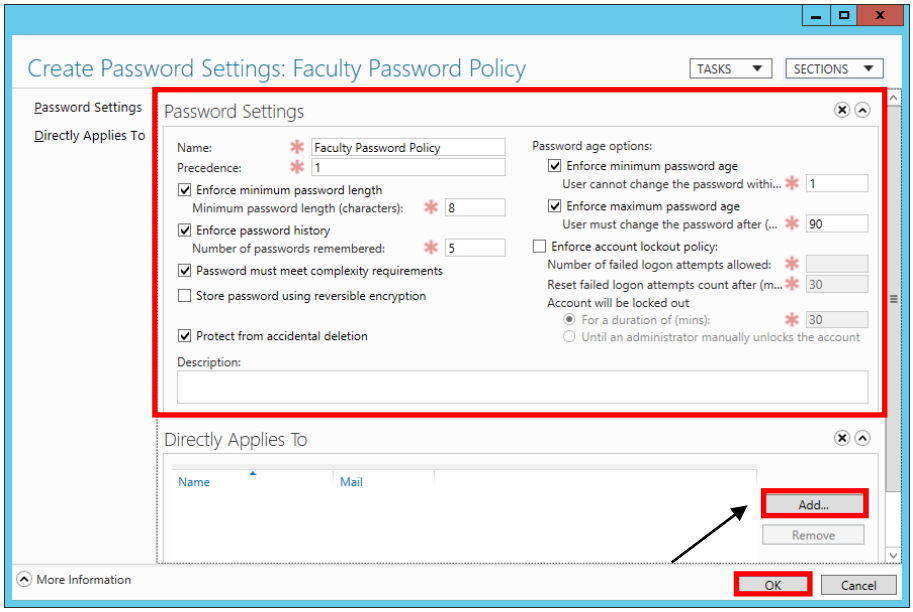


4. Expand the Domain name and navigate to System and then Password Settings Container.

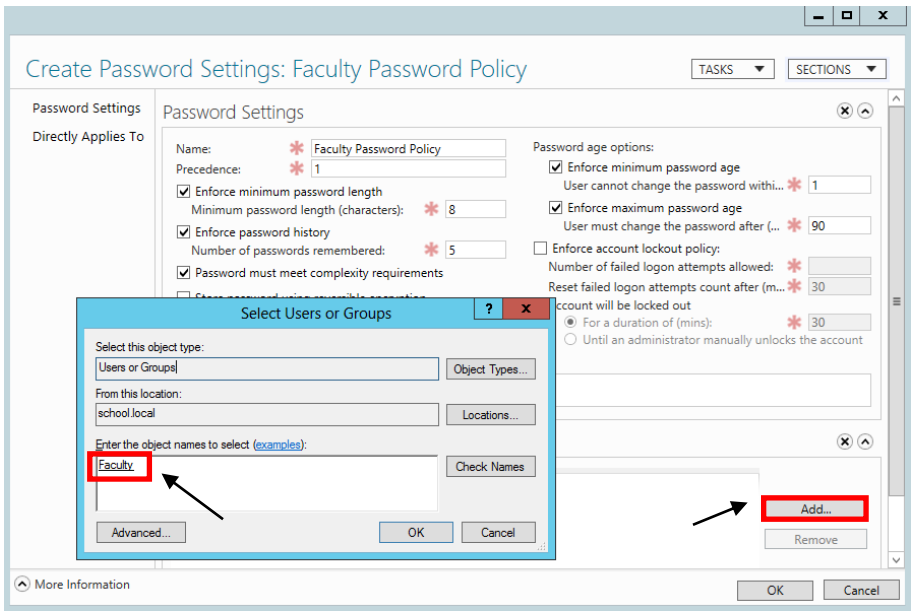


5. **Right-click on** Password Settings Container, **select** New **and then** Password Settings**.**

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



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



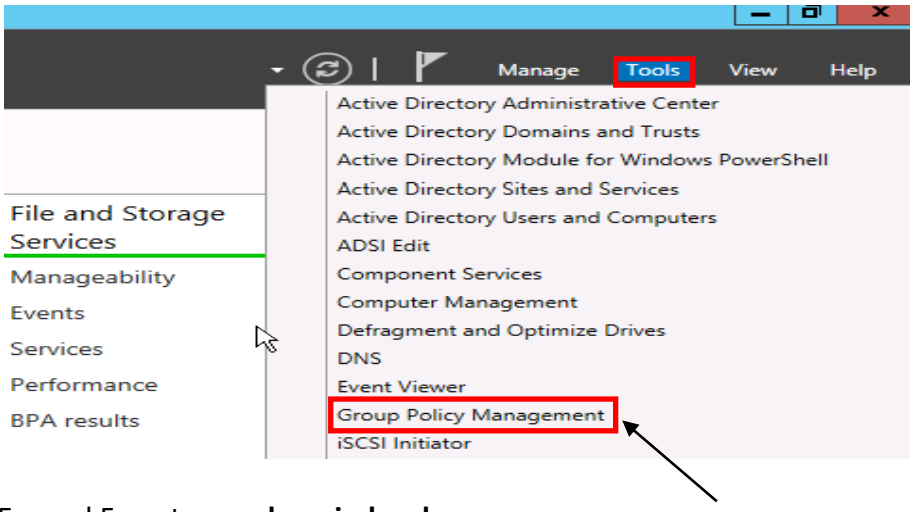
*****Repeat steps 5 – 7 for Students password policy***

SOME COMMON K12 GROUP POLICIES

RETAIN SECURITY EVENT LOG FOR 90 DAYS GROUP POLICY

1. Launch **Server Manager**.

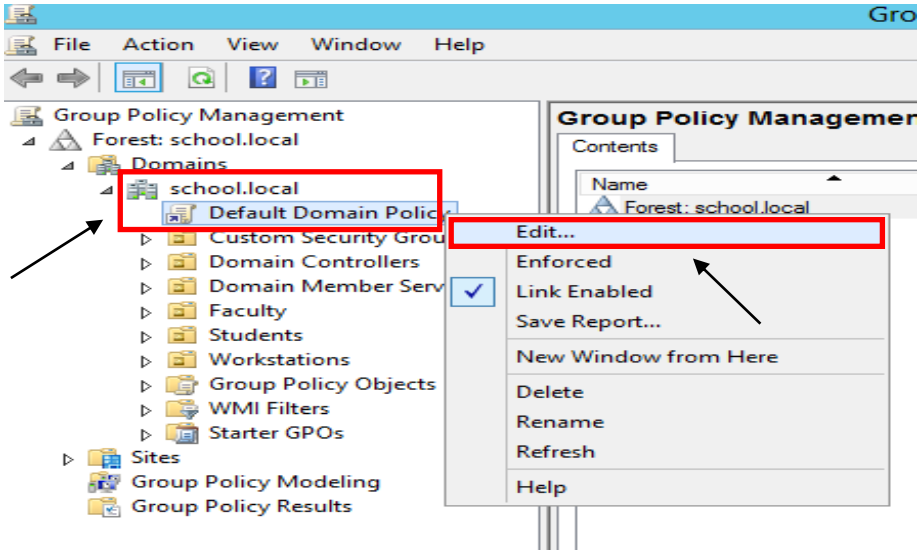
2. Click on **Tools** and select **Group Policy Management** from the drop-down list.



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

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

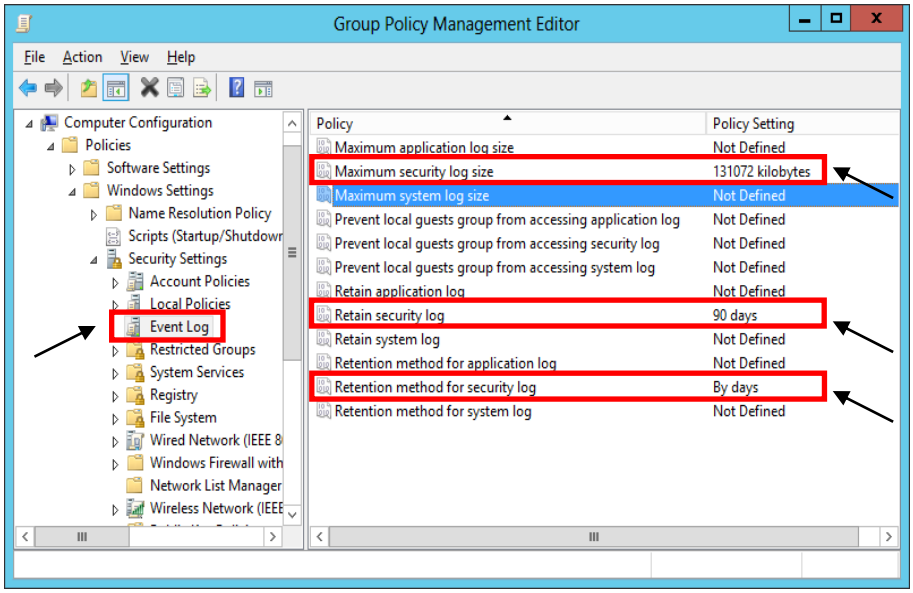
5. Right-click the **Default Domain Policy** and click **Edit**.



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

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

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



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

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

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

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

SECURITY EVENT AUDITING – SECURITY EVENT LOG CONTENTS

1. Launch **Server Manager**.

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

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

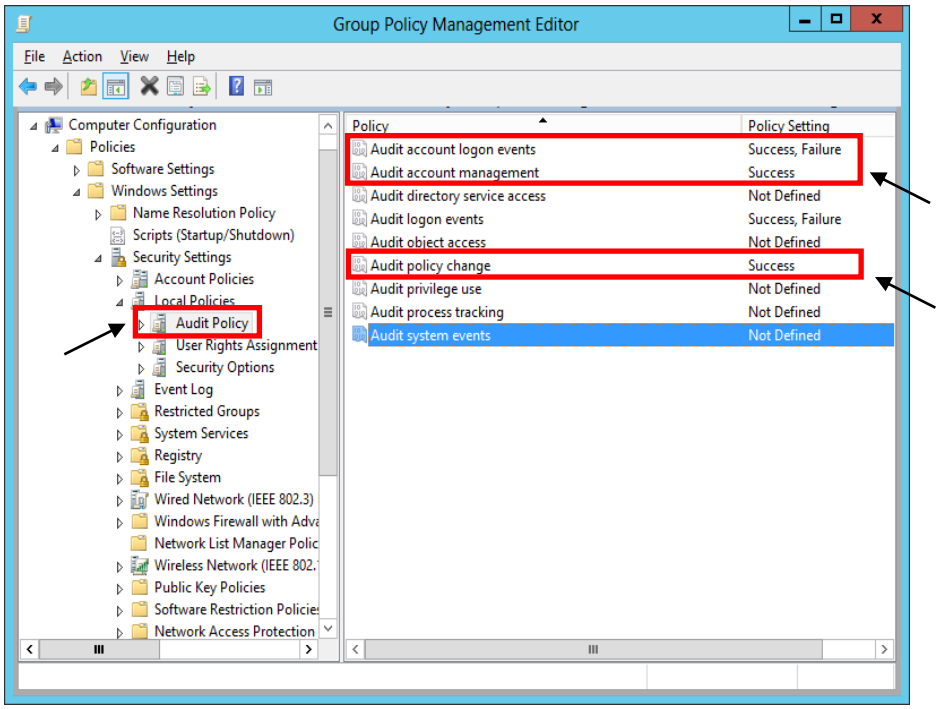
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

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

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

7. Enable auditing for the following Policy Settings:

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



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

GROUP POLICY FOR LOGON BANNER

1. Launch **Server Manager**.

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

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

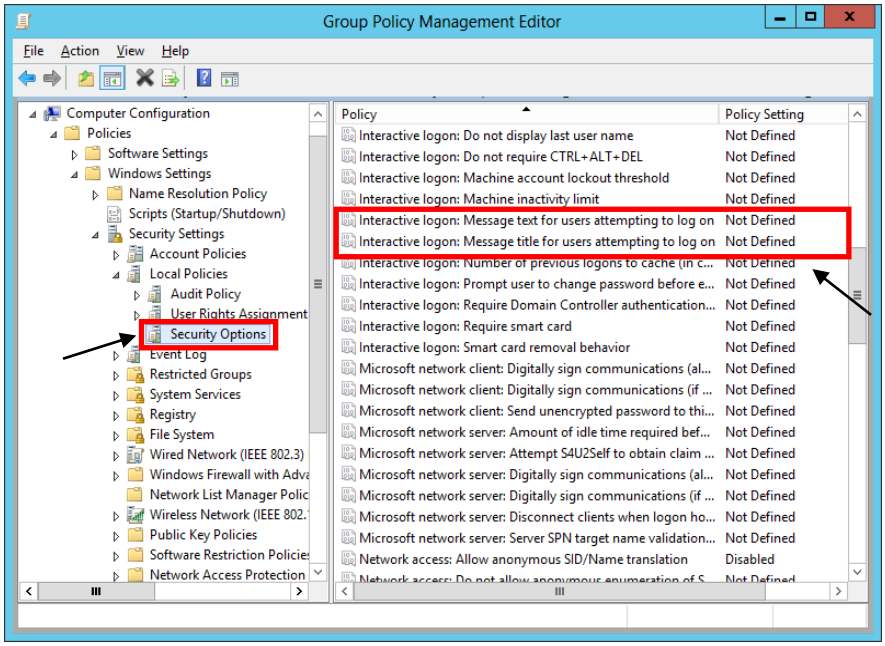
4. Expand **Domains** and then expand **yourdomain.local** and navigate to **Default Domain Policy**.

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

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

7. Navigate to the following options and Enable them:

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



8. Close the Group Policy Management Editor.

LOCKING SCREEN SAVER GROUP POLICY

1. Launch **Server Manager**.

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

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

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

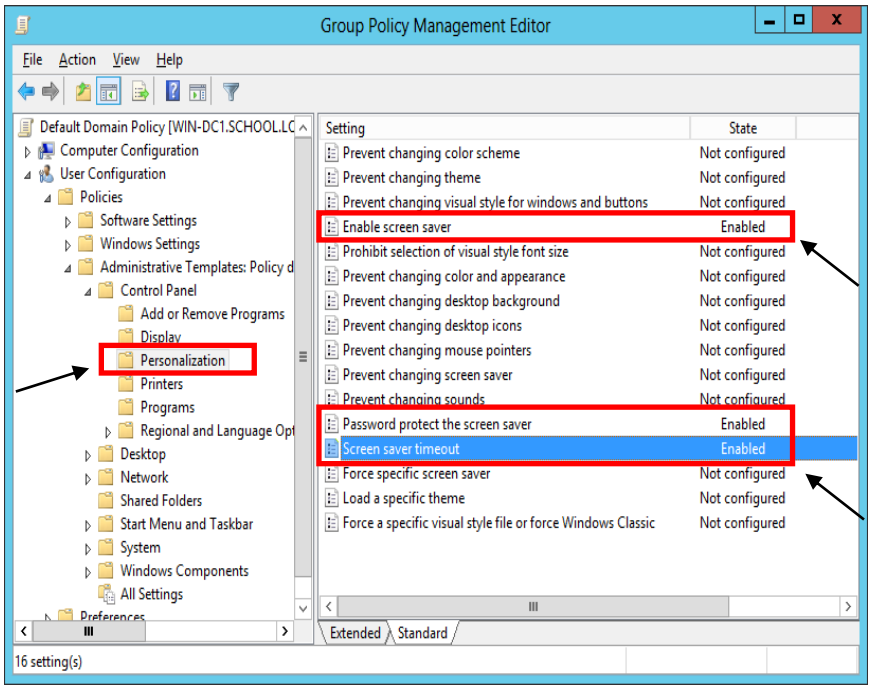
5. Right-click the **Default Domain Policy** and click **Edit**.

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

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

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

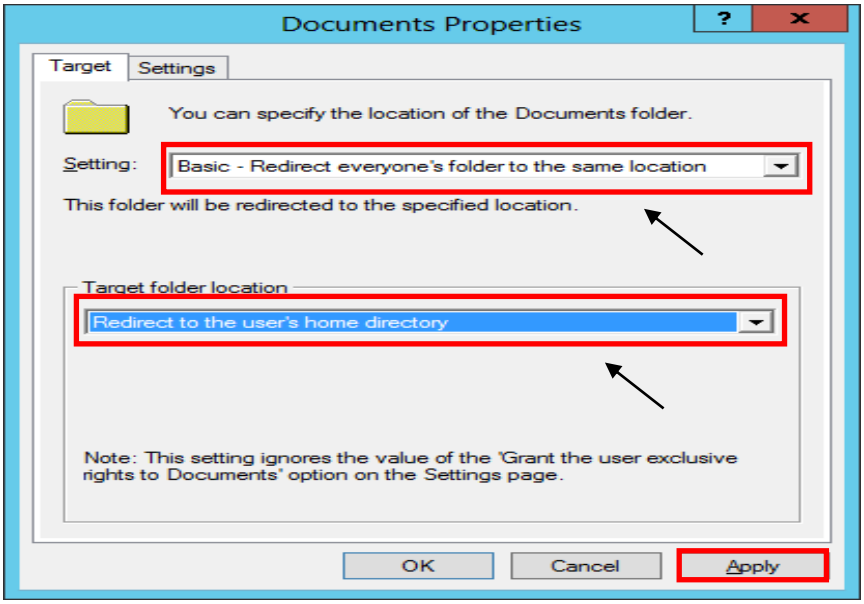
9. Set the **Screen Saver timeout** to **Enabled** and to a recommended time of **900 seconds** (15 minutes).



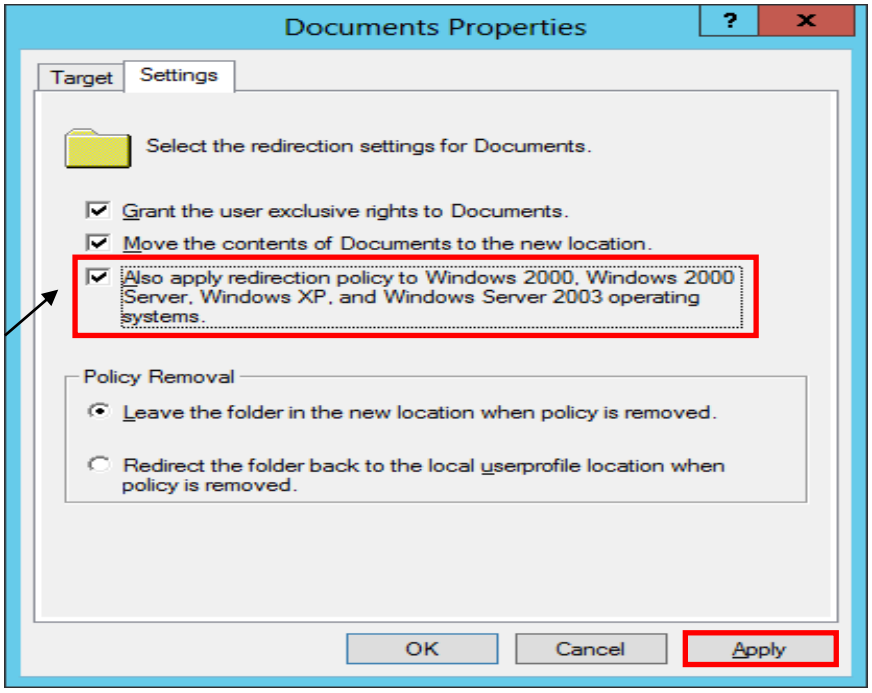
10. Close the **Group Policy Management Editor.**

FOLDER REDIRECTION GROUP POLICY

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



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



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

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

RESTRICT COMPUTERS TO FACULTY USE ONLY

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

1. Launch **Server Manager**.

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

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

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

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

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

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

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

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

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

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

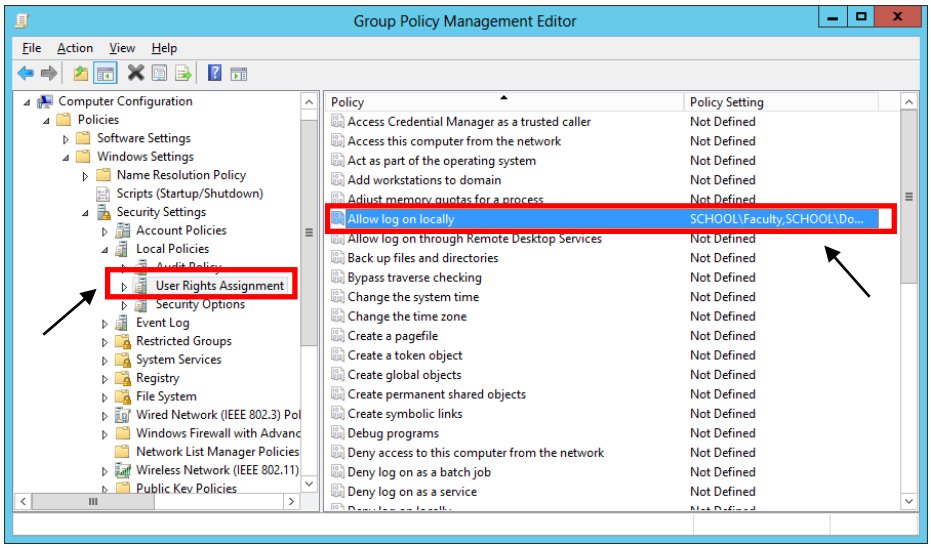
12. Right-click on the newly created **Faculty Use Only Computers** policy and select **Edit**.

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

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

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

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



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

*****Once this policy is created and applied, add computers to the Faculty Use Only Computers security group to apply the policy. A reboot is required after the computer is added to and removed from the group to enforce/remove the policy.***

REFRESH GROUP POLICY SETTINGS WITH GPUPDATE.EXE

Syntax

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

Parameters

/target:{computer|user}

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

/force

Ignores all processing optimizations and reapplies all settings. The Group Policy engine on the client tracks versions of the GPOs that are applied to the user and

computer. By default, if none of the GPO versions change and the list of GPOs remains the same, the Group Policy engine will not reprocess policy. This option overrides this optimization and forces the Group Policy engine to reprocess all policy information.

/wait:*value*

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

/logoff

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

/boot

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

/?

Displays help at the command prompt.

Examples

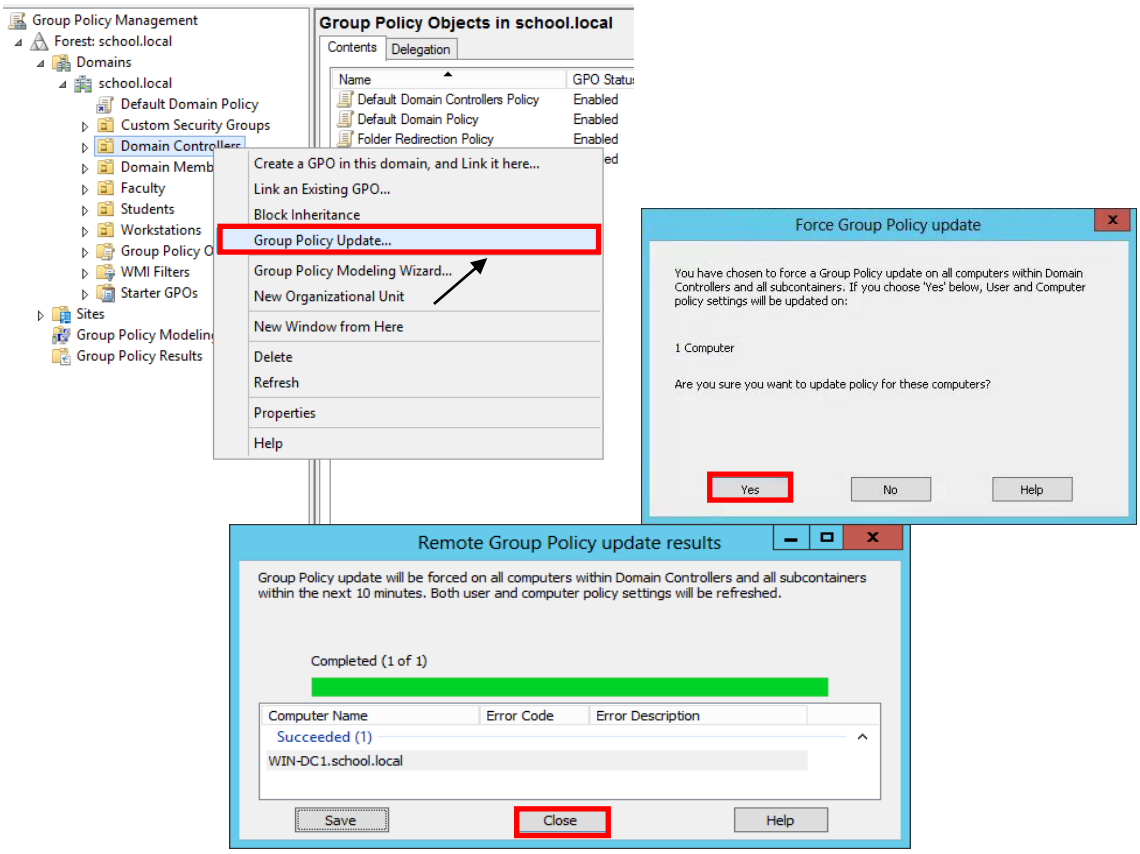
The following examples show how you can use the **gpupdate** command:

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

UPDATE GROUP POLICY SETTINGS FROM GROUP POLICY MANAGEMENT CONSOLE

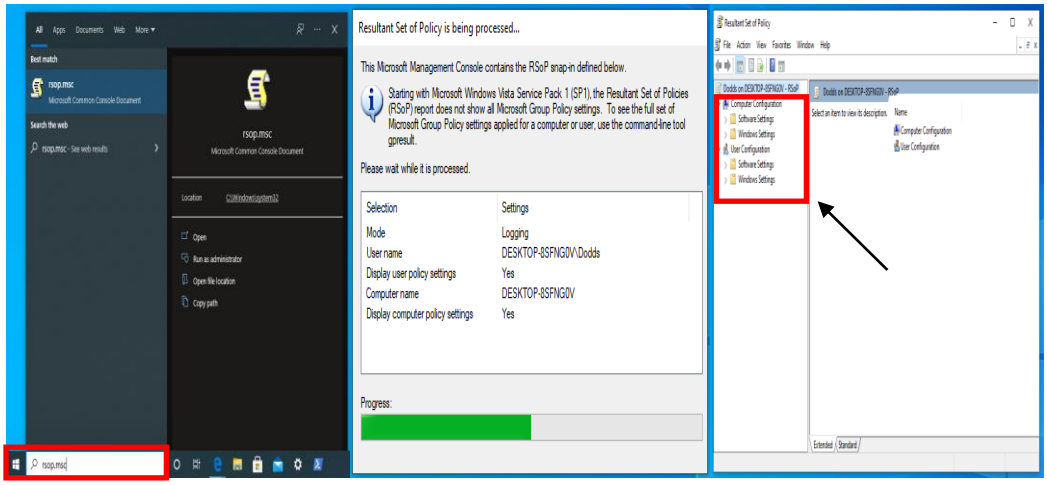
A new feature introduced with Windows Server 2019 is that from within the Group Policy Management Console. The update process also notifies how many computer objects will be affected by the update operation.

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



How To Check Group Policy settings on a Domain Computer (GUI)

1. Open the Resultant Set of Policy utility by moving your mouse over the bottom-left Windows Key ⊞ or click Keyboard Key ⊞ and type **rsop.msc** and press **Enter**

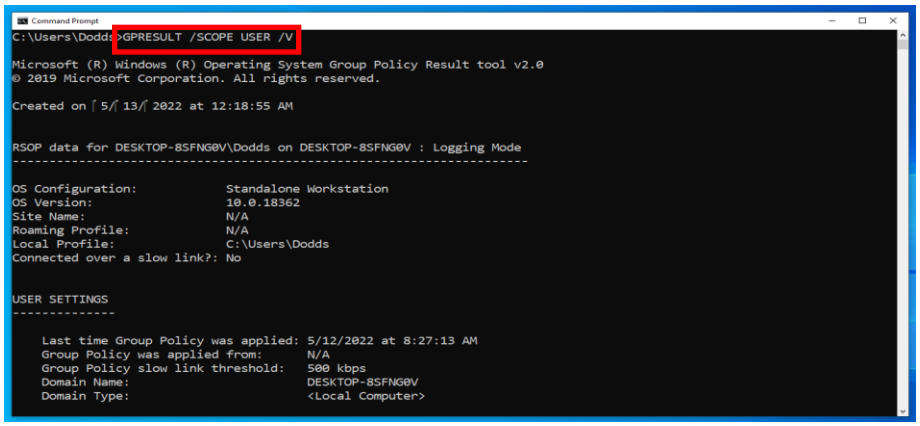


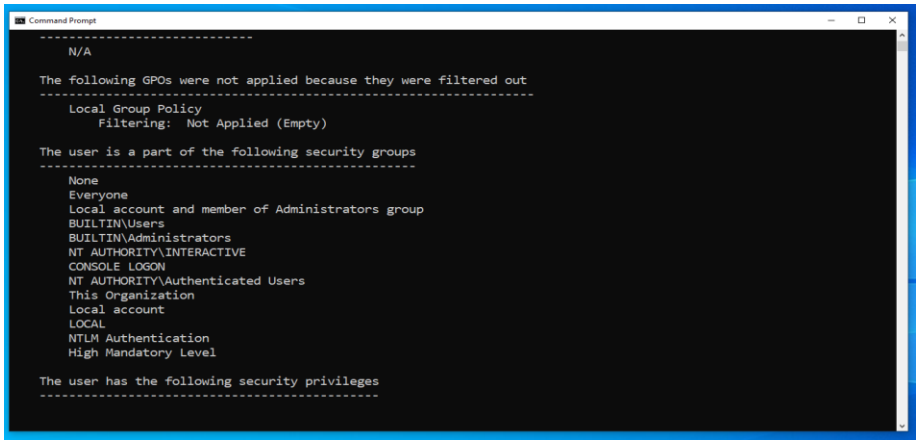
2. To check & verify applied group policy's, expand Computer & User Configurations

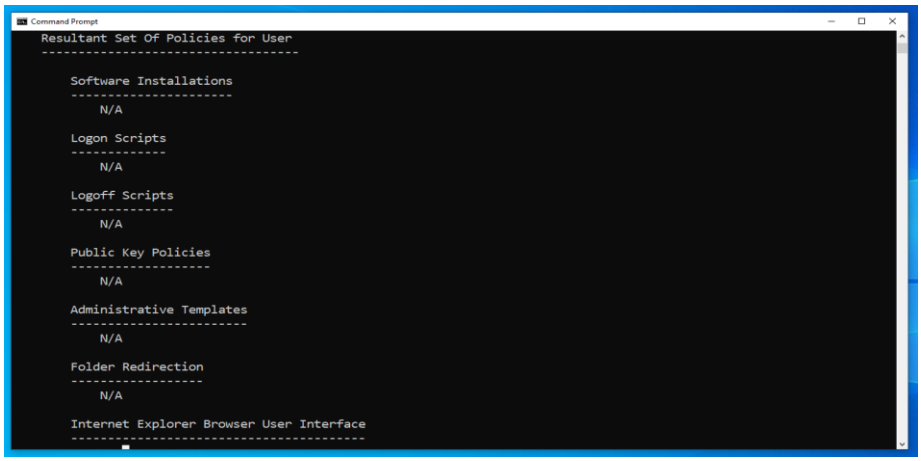
How To Check Group Policy settings on a Domain Computer (CMD)

To view all the policies applied to the user account you are currently logged in with, you would use the following command:

1. **Open** Command Prompt **CMD**
2. **Type** Command "**GPRESULT /SCOPE USER /V**"







DISABLING THE SHUTDOWN EVENT TRACKER

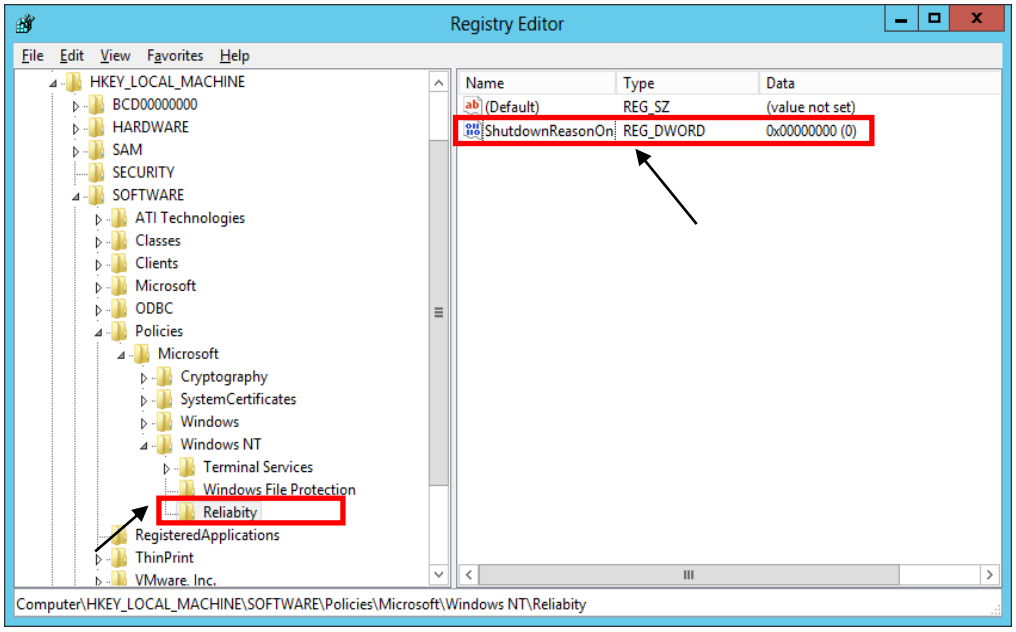
To turn off the Shutdown Event Tracker, navigate to the following key in your registry:

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

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

Create a new DWORD with the following values:

Value Name: ShutdownReasonOn
Value: 0 (HEX)



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

SET TIME SOURCE TO DIS / NTP TIME SERVER

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

  netdom /query fsmo

- Log in to your PDC Server and open the command prompt.
- Stop the W32Time service

  net stop w32time

- Configure the external time sources, type:

w32tm /config /syncfromflags:manual /manualpeerlist:"165.29.1.11,170.94.1.1"

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

  w32tm /config /reliable:yes

- Start the w32time service:

  net start w32time

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

  w32tm /query /configuration

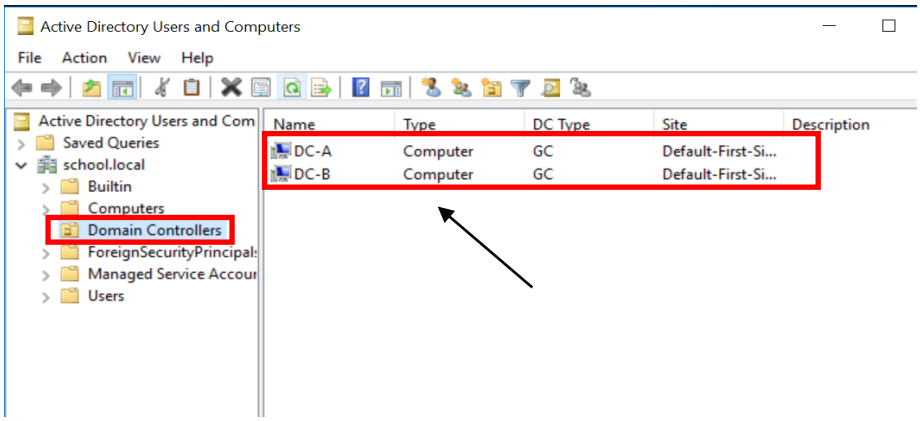
*****Check the Event Viewer for any errors.***

****DIS Time Servers - dsn1.state.ar.us, dns2.state.ar.us, dns3.state.ar.us**
****NTP Time Servers - time.windows.com, time.nist.gov, us.pool.ntp.org**

ACTIVE DIRECTORY MAINTENANCE

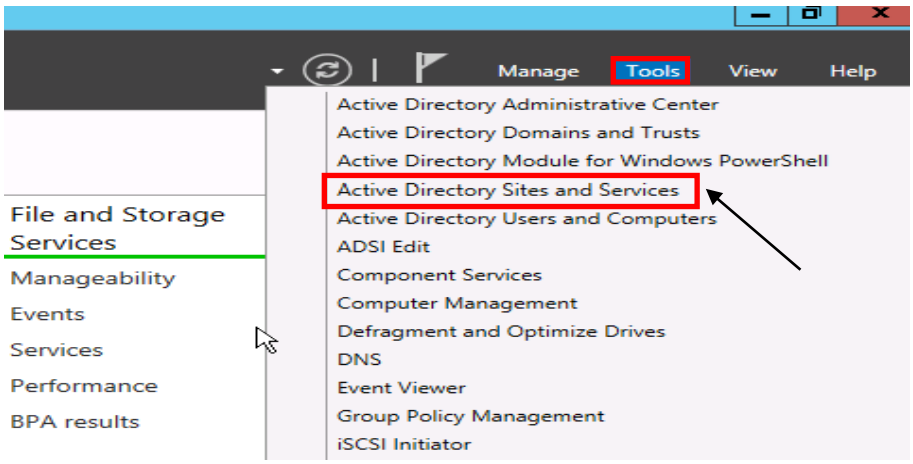
STEPS TO CHECK ACTIVE DIRECTORY REPLICATION IN WINDOWS SERVER (GUI)

Check Active Directory objects replication between these two Domain Controller.



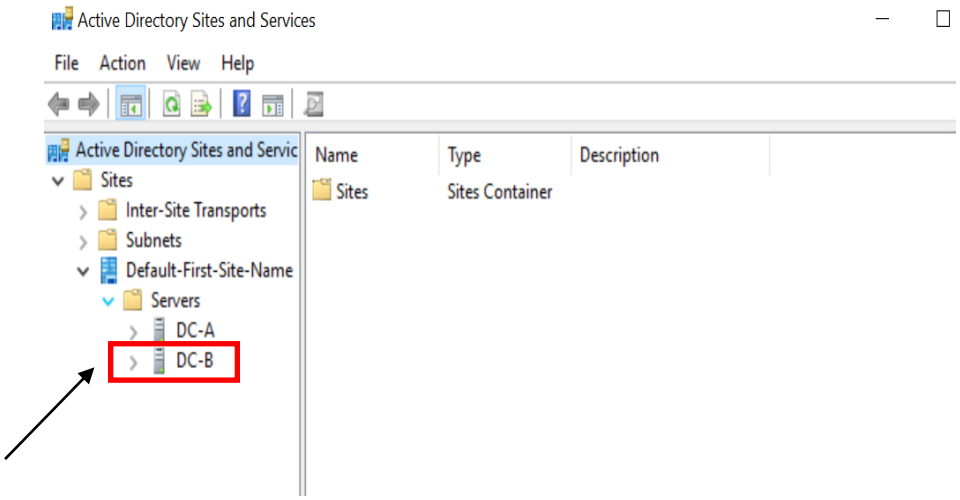
1. Launch **Server Manager.**

2. Click on **Tools** and select **Active Directory Sites and Services** from the drop-down list.

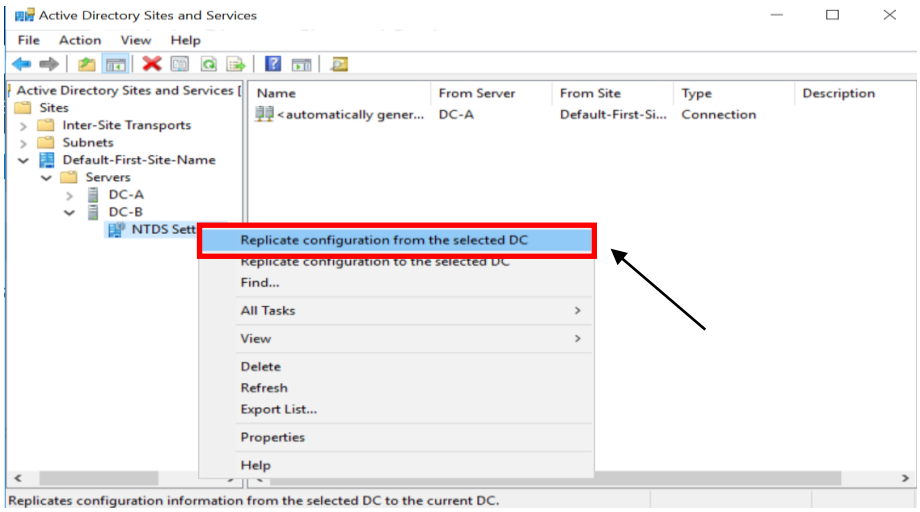


Active Directory sites and services is a primary console used to replicate the AD objects between the Domain Controllers. We can also manage the objects represent the sites and servers which reside in those sites. Site links are automatically created as and when we add any new Domain Controller in our environment.

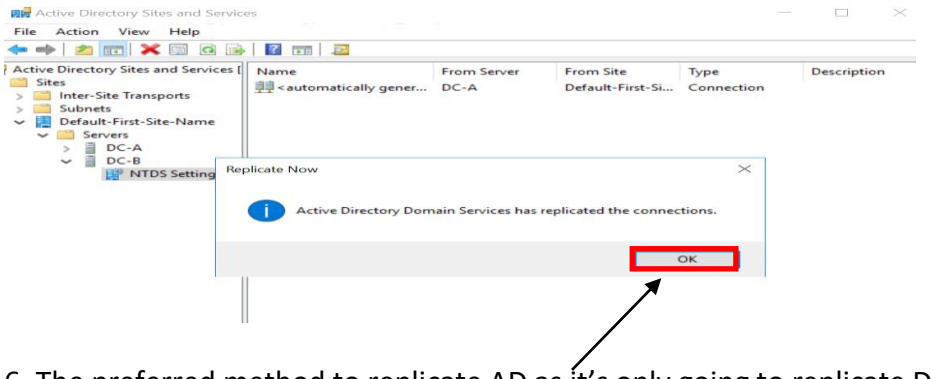
3. **Expand** and **Left Click** Sites, Default-First-Site-Name, Servers



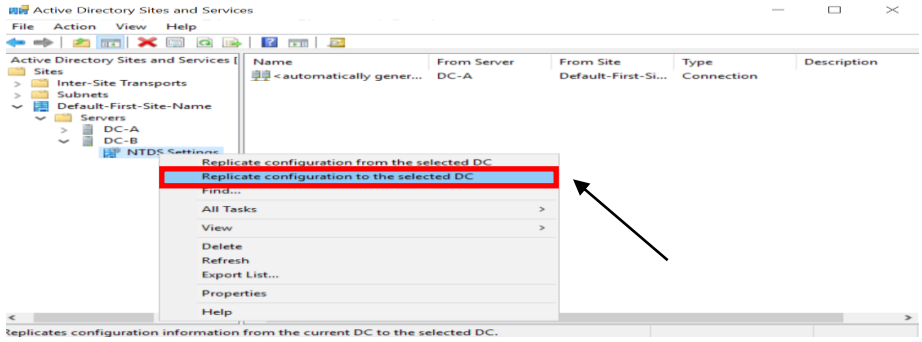
4. To forcefully replicate AD, open **Active Directory sites and services** console, click on **DC-B** than right click on **NTDS Settings**. Under the NTDS Settings "Click on Replicate configuration from the selected DC". Through this option, we pull the information from the selected DC (FYI, replication is of 2 types i.e. Pull and Push).



5. It opens the confirmation **dialogue box** which tells that Active Directory Domain Services are replicated the connections. Click on OK. If you see any error or if Additional Domain Controller is recently promoted, then you need to wait for sometime (about 30 minutes if intra-site and about two to four hours if inter-site) before you try to do forceful AD replication.



6. The preferred method to replicate AD as it's only going to replicate Data between Domain Controllers that we select. It would not start replication between all the DCs which consumes most of the bandwidth and can create congestion in the environment.

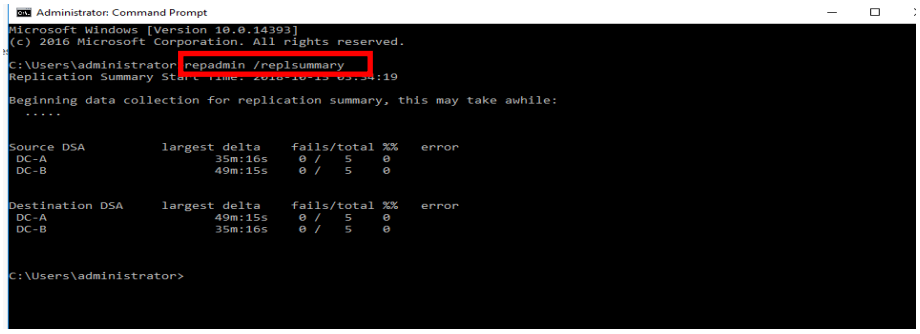


STEPS TO CHECK ACTIVE DIRECTORY REPLICATION IN WINDOWS SERVER (CMD) REPADMIN

1. **Open** Command Prompt **CMD** (run as administrator)

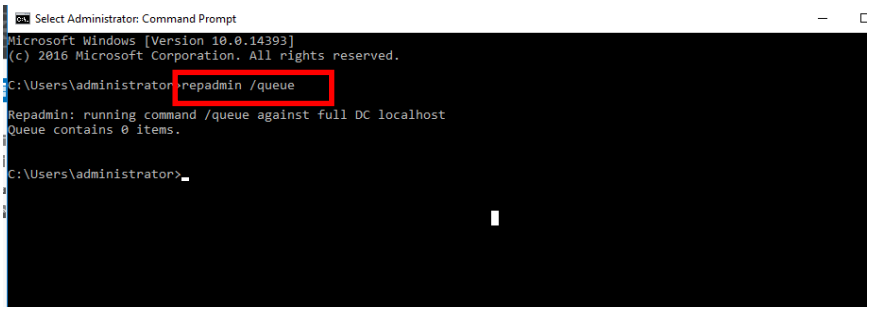
2. The first command that we are run is "**Repadmin /replsummary**" to check the current replication health between the domain controllers. The "**/replsummary**" operation quickly and concisely summarizes replication state and relative health of a forest.

****After running the command it shows some information which was in two parts – Source DSA and Destination DSA.**

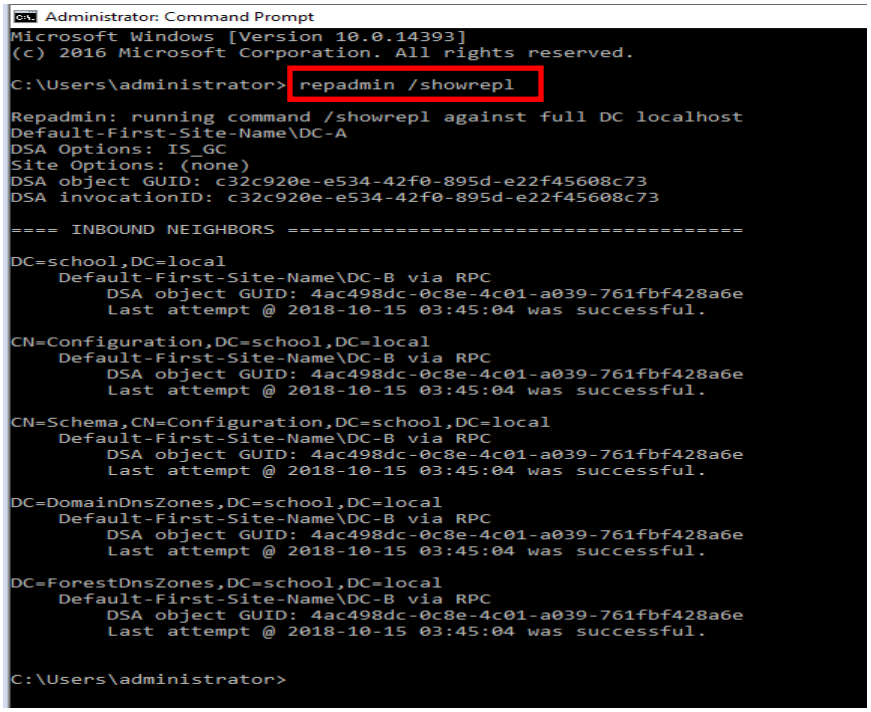


We can see that both servers are listed in both sections, the reason behind this is the Active Directory uses multi-master domain model. Active Directory can be updated from any writable Domain Controller except the Read-only Domain Controller. The RODC would only be listed in Destination DSA section.

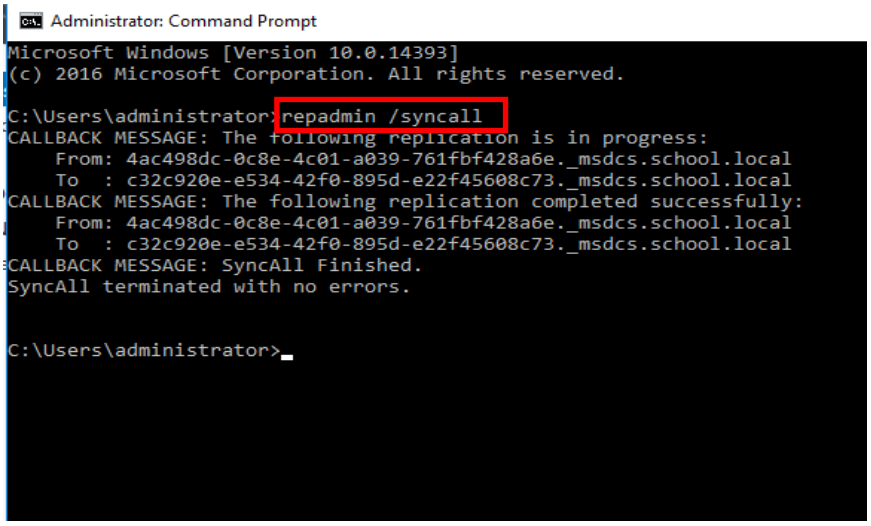
3. The second command is "**Repadmin /Queue**" shows the elements are remaining in the queue to replicate. It Displays inbound replication requests that the Domain Controller needs to issue to become consistent with its source replication partners.



4. The Third command is "**Repadmin /Showrepl** displays the replication status when the specified domain controller last attempted to implement inbound replication of Active Directory partitions. It helps to figure out the replication topology and replication failure.

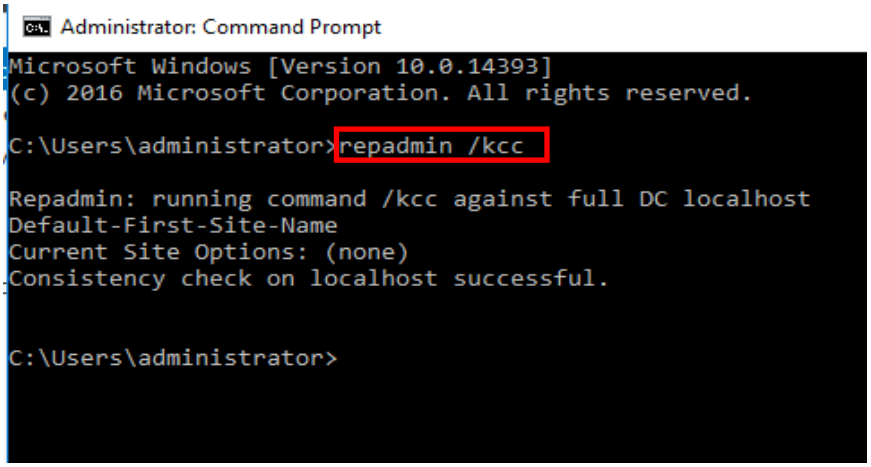


5. The Fourth command is "**Repadmin /syncall**" it Synchronizes a specified domain controller with all replication partners. We recommend you not to run this command in the big environment because it forcefully replicates Active Directory objects between all the domain controller which leads to excessive load on the network and can result in network congestion.

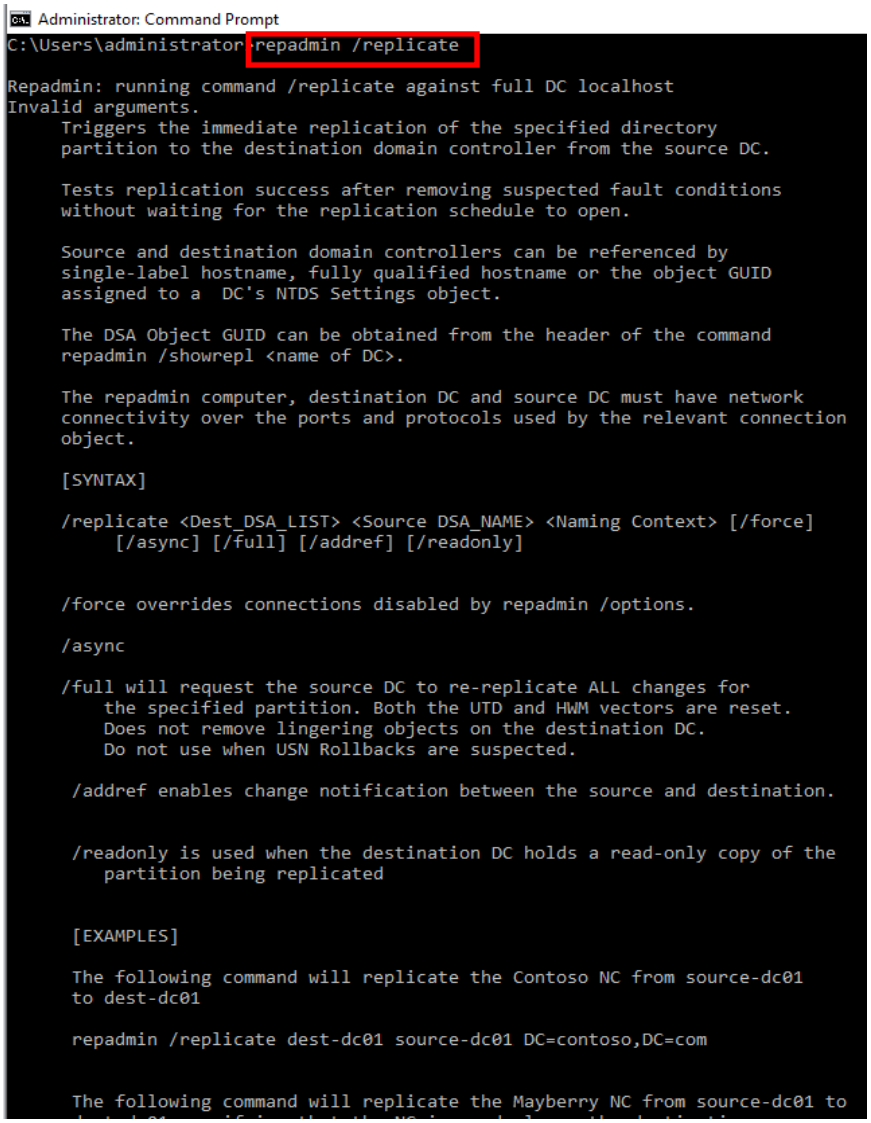


6. Repadmin /KCC this command forces the KCC (Knowledge Consistency Checker) on targeted domain controller(s) to immediately recalculate its inbound replication topology. It checks and creates the connections between the Domain Controllers. By default KCC runs in the background every 15 minutes to check if new connection is established between DCs or not.

****By running the command we are forcing DCs to check if new Domain Controller is found in the environment and if yes then add connection to the same.**



7. **Repadmin /replicate** starts the immediate replication of the specified directory partition to the destination domain controller from the source DC.

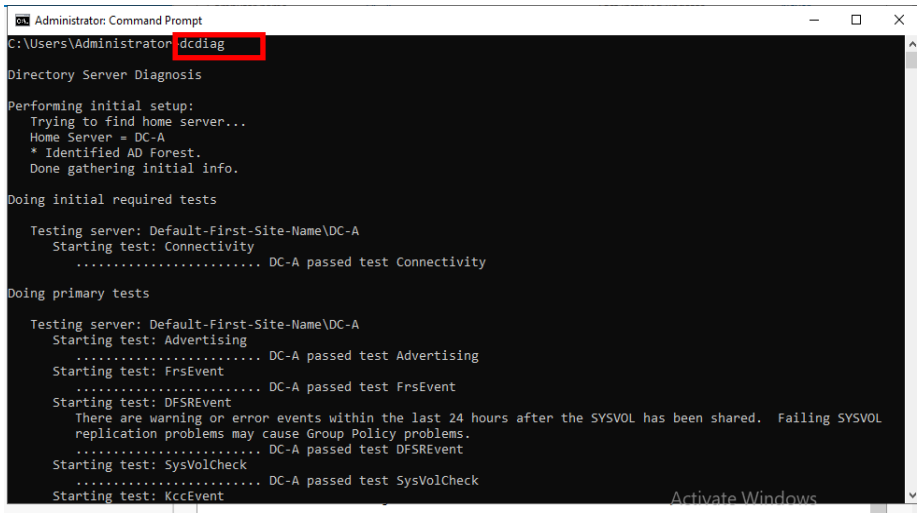


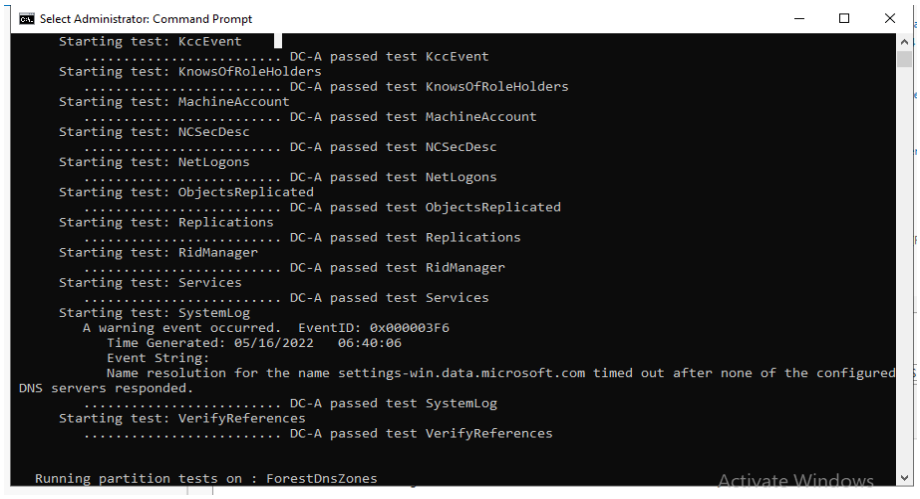
****The replication tools listed above are used to check AD replication and to Replicate AD using GUI mode and from command prompt.**

TESTING / DIAGNOSE THE HEALTH OF ACTIVE DIRECTORY DOMAIN CONTROLLERS, DNS SERVERS, AD REPLICATION, AND OTHER ADDS INFRASTRUCTURE SERVICES (CMD)

1. From the Domain Controller, open a command prompt

2. Run Command
   dcdiag





**** It is recommended to run the Dcdiag test on the domain controller itself, and not remotely**

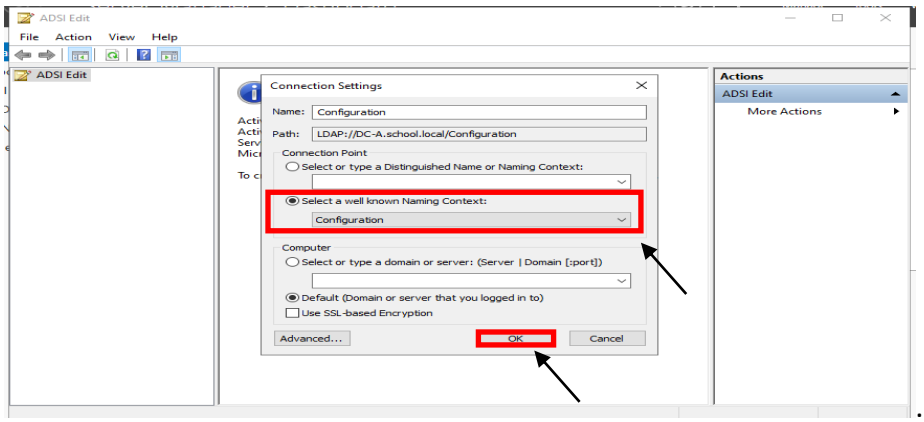
****The Dcdiag utility can perform up to 30 different tests related to the AD domain infrastructure, DNS, FSMO roles, etc.**

DELETE DEAD/TOMB-STONED DOMAIN CONTROLLER FROM ACTIVE DIRECTORY

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

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

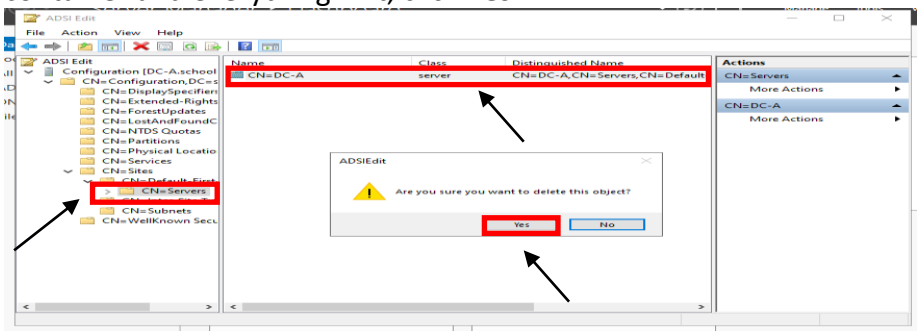
3. In the **Select a Well Known Naming Context** drop-down menu, select **Configuration**, and click **OK**.



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> corresponds 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**.



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

Removing the Server from the File Replication Service

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

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

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

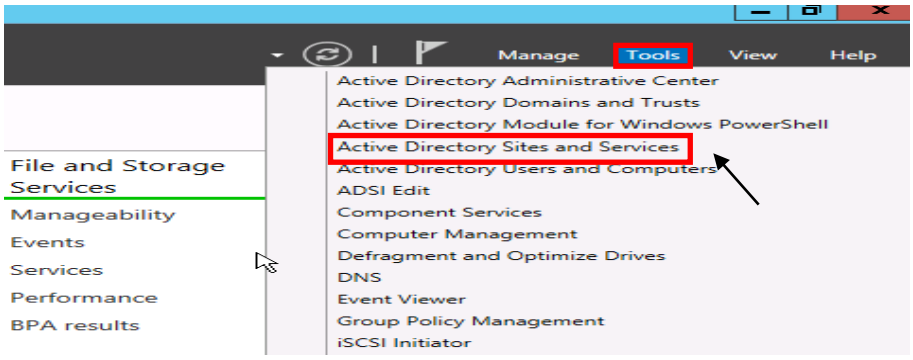
10. Navigate to Configuration\CN=System\CN=File Replication Service\CN=Domain System Volume(SYSVOL share)\CN=<ServerName> where <ServerName> correstpond to the location of the dead domain controller.

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

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

Removing the Server from Active Directory Sites and Services

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



14. Expand Sites.

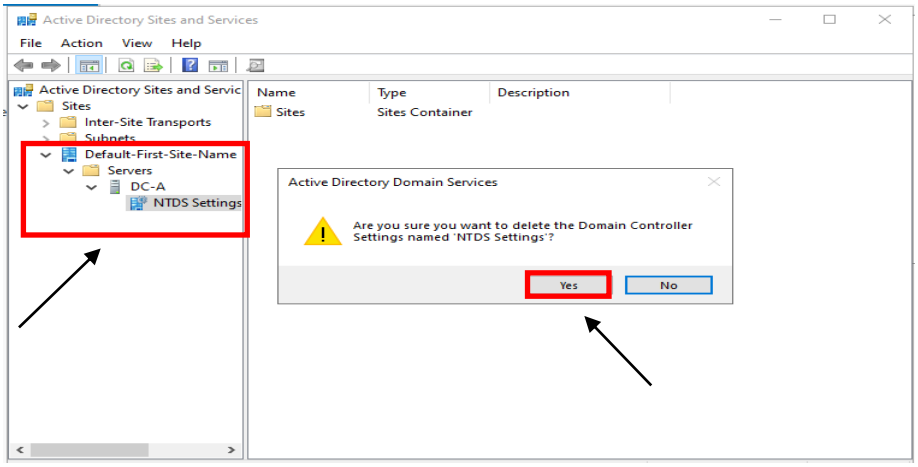
15. Expand the AD Site that the dead Domain Controller was a member of.

16. Expand the dead Domain Controller.

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

18. When prompted, click Yes.

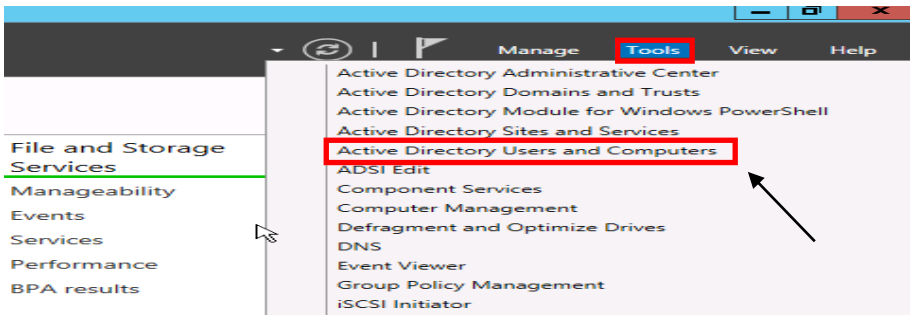
19. You will receive the Confirm Subtree Deletion box as shown below. Check the **Use Delete Subtree server control** option and click Yes.



20. Close Active Directory Sites and Services.

REMOVING THE SERVER FROM ACTIVE DIRECTORY USERS AND COMPUTERS

21. Open Active Directory Users & Computer.

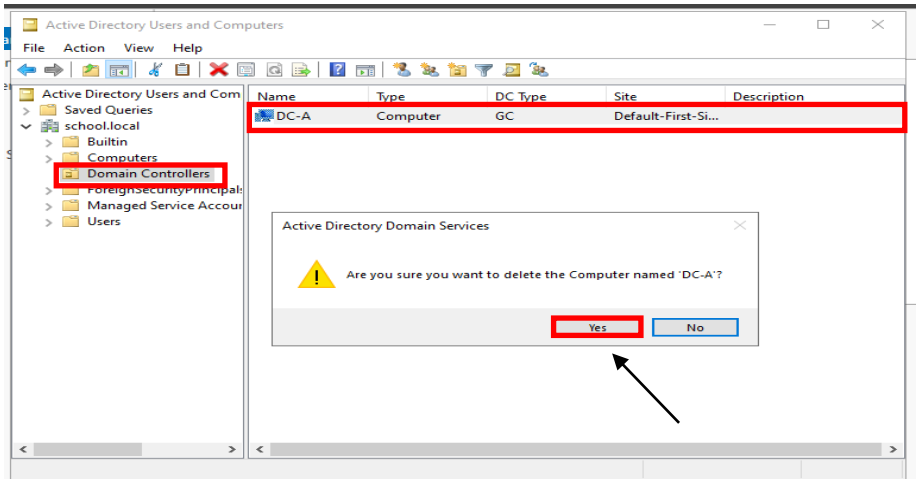


22. Browse to the Domain Controller Computer object, right-click and select **Delete**.

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

24. Another confirmation box will pop up.

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



26. Close Active Directory Users & Computers

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

MANUALLY SEIZE FSMO ROLES

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

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

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

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

- Open the Command Prompt utility by moving your mouse over the bottom-left Windows Key or click Keyboard Key and type **cmd, run as a administrator** and press **Enter**
- On the Command Prompt type **ntdsutil** , and then click ENTER.

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

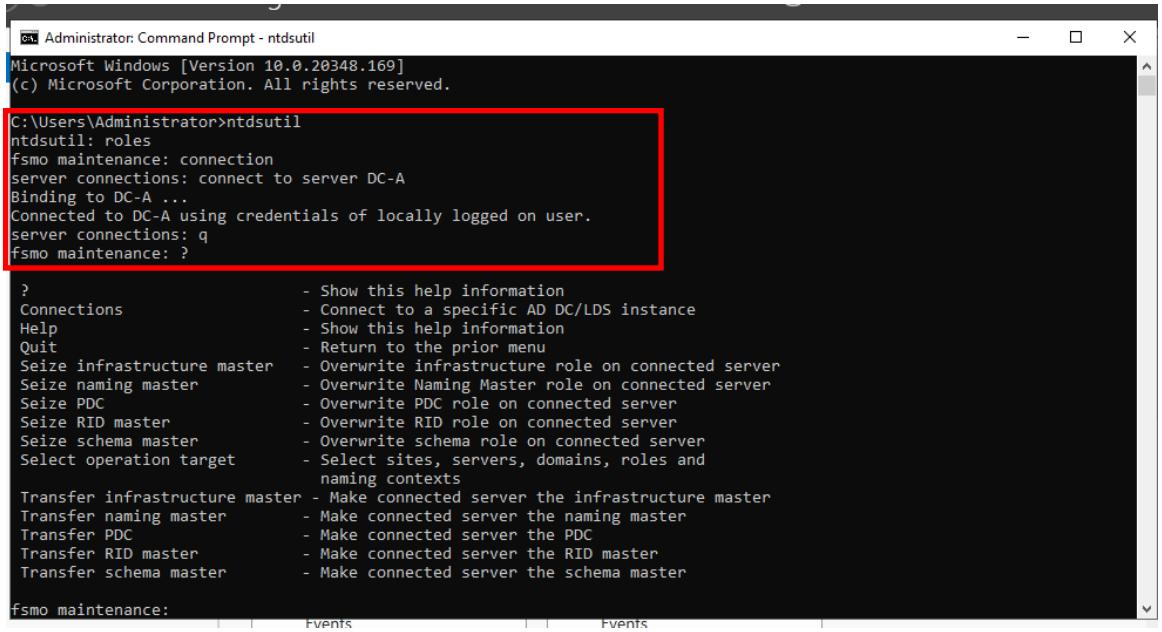
- Type **connections**, and then press ENTER.

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

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

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

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



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

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

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

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

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

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

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

       reset password on server null

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

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

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

       reset password on server *servername*

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

    c. Type the new password when you are prompted.

27. At the DSRM command prompt, type q.

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

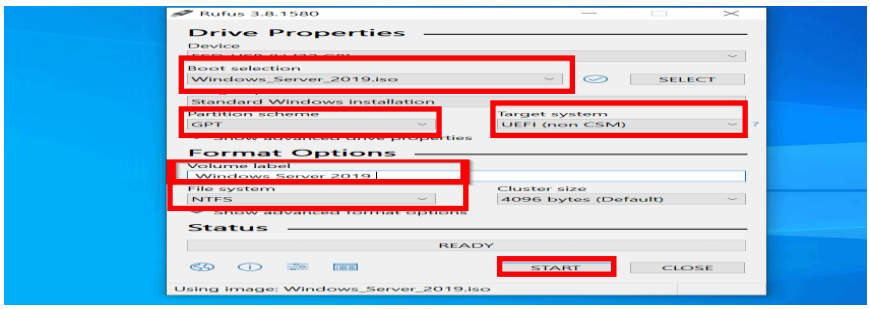
How to Create a Bootable USB Drive From ISO To Install Windows Server 2019 (GUI)

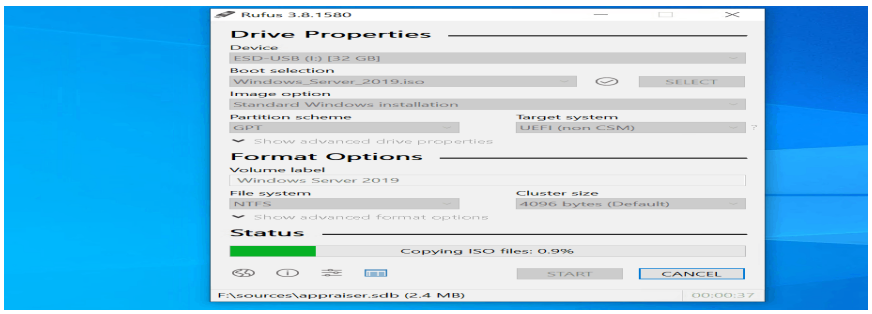
1. **Purchase** Windows Server Edition / **Download** .ISO & Activation Key
   For ESS Agreement logon onto - Microsoft Volume Licensing Service Center (VLSC) https://www.microsoft.com/Licensing/servicecenter/default.aspx

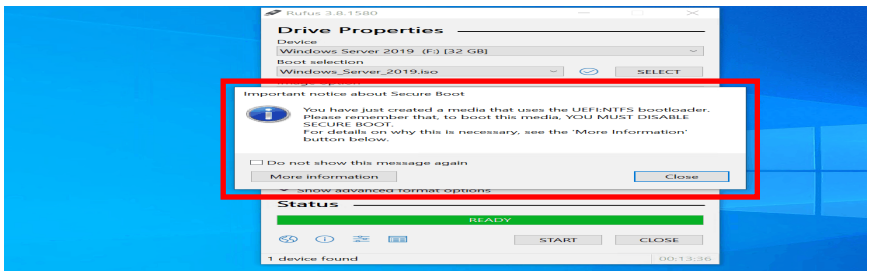
2. Download & install software to a computer to burn ISO – Rufus, etc.

3. Install at least 8Gb USB Drive / Blank Dual Layer DVD-R into computer

4. Open Software & Configure Options and Click **Start** to copy ISO to USB / DVD
   - Configure Boot Selection – Choose the downloaded Windows Server 2019 iso file
   - Configure Partition select Scheme GPT
   - Configure Target System select UEFI (non CSM)
   - File System – select NTFS







5. After Completion, Install USB Drive / DVD Disc into Server, and boot to drive
   ****Must Disable Secure Boot in Server Bios to Install Software**

HOW TO CREATE A BOOTABLE USB DRIVE FROM ISO TO INSTALL WINDOWS SERVER 2019 (PS)

1. **Purchase** Windows Server Edition / **Download** .ISO & Activation Key
   For ESS Agreement logon onto - Microsoft Volume Licensing Service Center (VLSC) https://www.microsoft.com/Licensing/servicecenter/default.aspx

2. Download Windows Server 2019 ISO to a computer

3. Install at least 8Gb USB Drive into computer
   **must follow steps 4 – 15 to prepare USB Drive for ISO

4. Create a variable for the file location on computer (windows server 2019 iso)
   $isopath = 'C:\Users\Public\Downloads\WindowsServer2019.iso'

5. Open the Powershell utility by moving your mouse over the bottom-left Windows Key ⊞ or click Keyboard Key ⊞ and type **powershell, run as a administrator** and press **Enter**
   ** Before we can format the USB drive, we need to establish the disk number Windows has assigned it. Run the command below to list all the USB drives attached to your computer:

6. Run Command
   Get-Disk | Where-Object BusType -eq USB | Format-Table -AutoSize
   ** I know that my USB drive is called 'Patriot Memory', so it is disk number '2'. Let's create an object ($usb) for disk '2'. You should replace -eq 2 with the number of your USB drive.

7. Run Command
   $usb = Get-Disk | Where-Object Number -eq 2
   **Now, we're going to delete all the data on the USB drive using Clear-Disk. Type Y and press ENTER to confirm you want to delete all data on the drive. This is a good time to double-check that you have the correct disk number!

8. Run Command
   $usb | Clear-Disk -RemoveData

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> $isopath = 'C:\Users\Public\Downloads\WindowsServer2019.iso'
PS C:\WINDOWS\system32> Get-Disk | Where-Object BusType -eq USB | Format-Table -AutoSize

Number Friendly Name   Serial Number HealthStatus OperationalStatus Total Size Partition Style
------ -------------   ------------- ------------ ----------------- ---------- ---------------
2       Patriot Memory 078A01B0098F  Healthy      Online               7.47 GB GPT
1      asmedia ASM1153 F57100000000  Healthy      No Media                0 B RAW


PS C:\WINDOWS\system32> $usb = Get-Disk | Where-Object Number -eq 2
PS C:\WINDOWS\system32> $usb | Clear-Disk -RemoveData

Confirm
Are you sure you want to perform this action?
This will erase all data on disk 2 " Patriot Memory".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
PS C:\WINDOWS\system32>
```

9. Format the USB drive
   Now let's make sure the disk is configured with a GUID Partition Table so that we can use it to boot UEFI systems.

10. Run Command
    $usb | Set-Disk -PartitionStyle GPT
    ** Create a new volume on the drive using New-Partition. When prompted in the Format USB Drive dialog, format the volume using FAT32. You must use FAT32. Optionally, give the drive a volume name in the Volume label field. Click Start to format the USB drive. Click OK in the warning dialog to confirm that formatting the drive will erase all data.

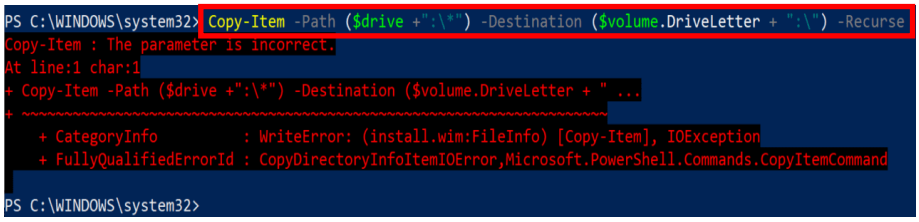
11. Run Command
    $volume = $usb | New-Partition -UseMaximumSize -AssignDriveLetter
    ** Close the Format USB Drive dialog once formatting is complete.

12. Copy the Windows Server 2019 media files to the USB drive
    **Now that we have configured the USB drive so that it can be used to boot our server hardware, all that's left to do is copy the Windows Server media files to the USB drive. Let's start by mounting the downloaded Windows Server .iso file to a drive in Windows

13. Run Command
    $mount = Mount-DiskImage -ImagePath $isopath -StorageType ISO
    **Windows will assign the new mounted drive a letter. We can use Get-Volume to get the assigned drive letter:

14. Run Command
    $drive = ($mount | Get-Volume).DriveLetter

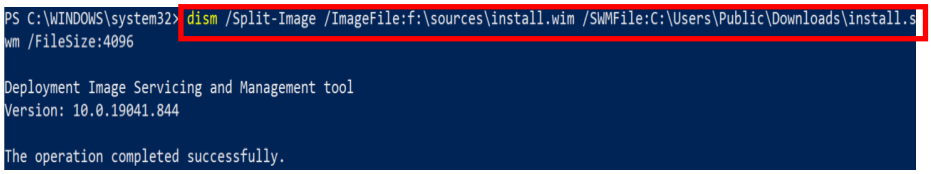
**Now, let's copy the entire contents of the mounted .iso file to the UBB disk using Copy-Item:



15. Run Command
    Copy-Item -Path ($drive +":*") -Destination ($volume.DriveLetter + ":\") -Recurse
    **If Copy-Item exits with an error, it's because it failed to copy the largest file, install.wim, to the USB drive. FAT32 has a file limit of 4GB and install.wim might be larger than the limit. To solve the problem, we can use the Windows 10 DISM tool to split the install.wim file into two smaller files: install.swm and install2.swm.

16. Windows 10 DISM tool
    First, we'll need to create the two new files on our local disk. In this example, I've chosen to create them in C:\Users\Public\Downloads. Note that you may need to replace 'f' in 'f:\sources\install.wim' with a different drive letter. Windows might have assigned a different drive letter to your mounted .iso file. You can check the drive letter Windows assigned by opening File Explorer (WIN+E).

17. Run Command
    dism /Split-Image /ImageFile:f:\sources\install.wim /SWMFile:C:\Users\Public\Downloads\install.swm /FileSize:4096



18. Now, let's copy the two new files, install.swm and install2.swm, to our USB drive:

19. Run Commands
    Copy-Item -Path C:\Users\Public\Downloads\install.swm -Destination ($volume.DriveLetter + ":\sources\install.swm")

    Copy-Item -Path C:\Users\Public\Downloads\install2.swm -Destination ($volume.DriveLetter + ":\sources\install2.swm")

20. Finally, all that's left to do is to unmount the Windows Server .iso file from our local device using Dismount-DiskImage:

21. Run Command
    Dismount-DiskImage -ImagePath $isopath

22. After Completion, Install USB Drive into Server, and boot to drive
    **Must Disable Secure Boot in Server Bios to Install Software

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

Active Directory, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Active Directory, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

This product contains graphics filter software; this software is based, in part, on the work of the Independent JPEG Group.

All other trademarks are property of their respective owners.