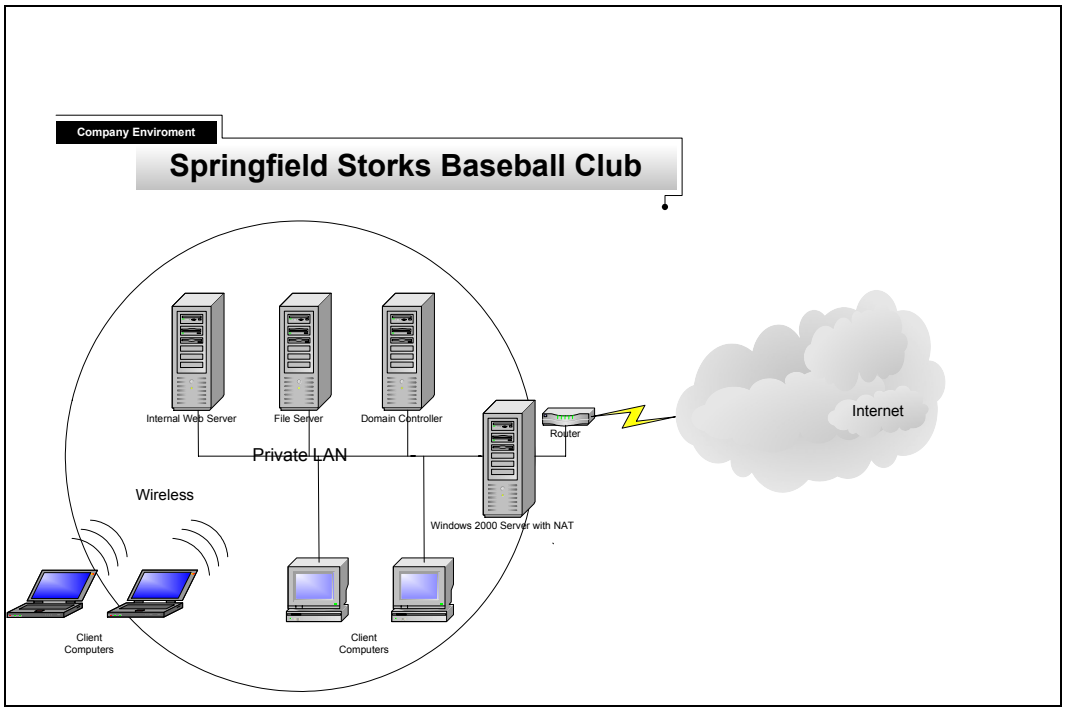
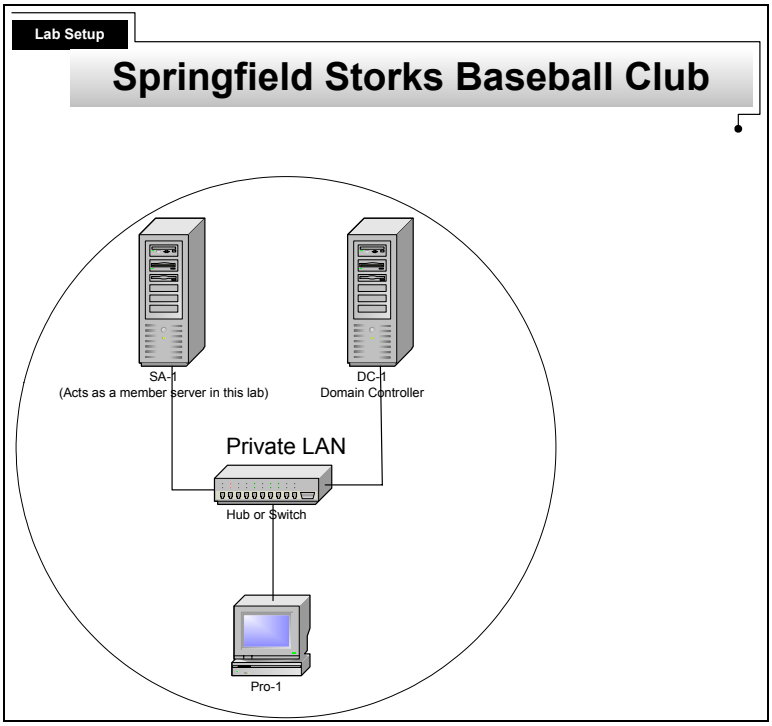
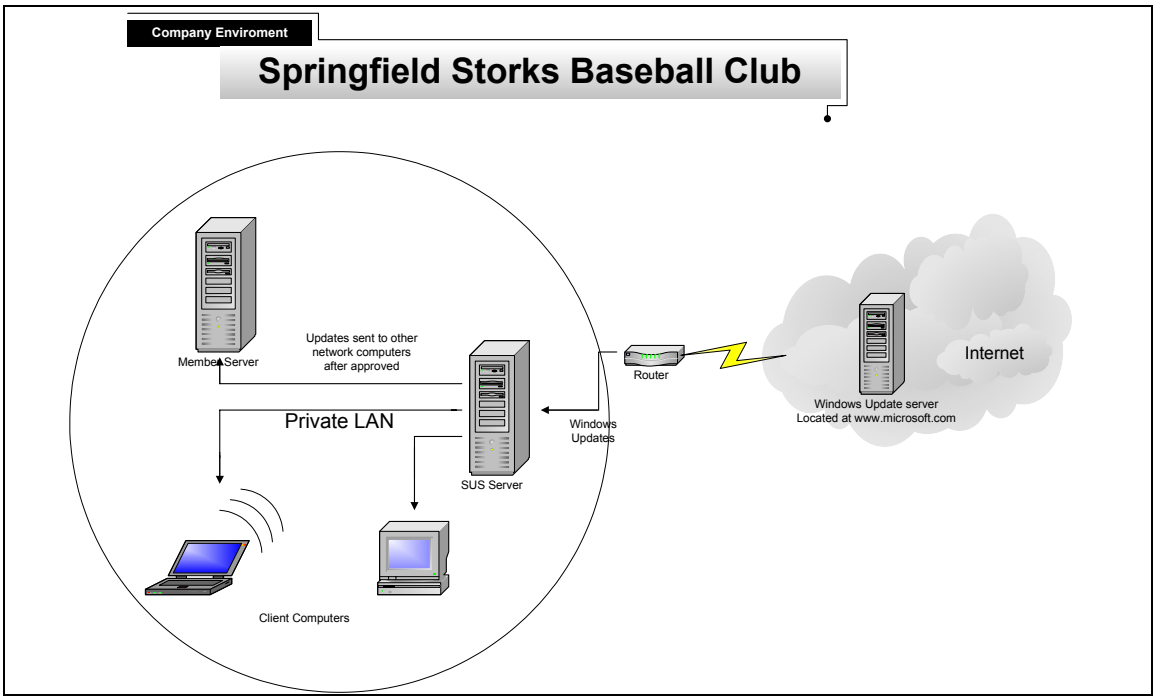
Network Lockdown - Configuring Windows 2000 and Server 2003
Network Security for the Springfield Storks Baseball Club

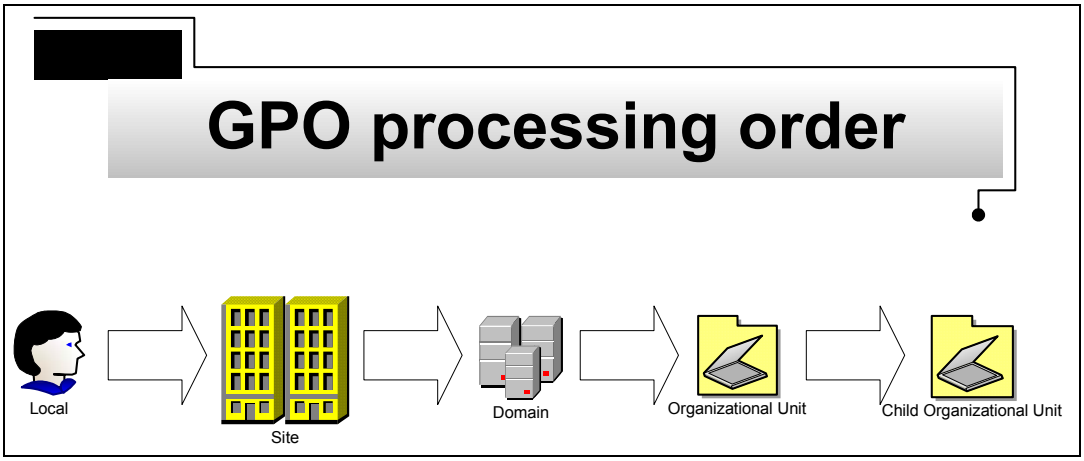
Mega Lab 11

Part 2 of 3 in the Windows 2000/Server 2003
Network Security Series









Network Lockdown – Configuring Windows 2000 & Server 2003 Network Security for the Springfield Storks

Mega Lab 11

Part 2 of 3 in the Windows 2000 & Server 2003 Network Security Series

About the Authors

Scott Skinger (MCSE, CNE, CCNP, A+) is the owner of Train Signal, Inc. and is an experienced Windows 2000 & Server 2003 instructor. He has also worked in the trenches as a Network Engineer, Director of Technology and currently as an Independent Consultant through his own company, SAS Technology Advisors. As an instructor, he has taught over 50 courses, covering topics such as Windows 2000, Server 2003, NT 4, Novell NetWare, Red Hat Linux, Cisco Routers and security.

Wilson Chan (MCSA) is responsible for content development for the Security Mega Lab Series. He also does network support, computer hardware repair and software support for a computer consulting company.

Train Signal, Inc.
400 West Dundee Road
Suite #106
Buffalo Grove, IL 60089
Phone - (847) 229-8780
Fax – (847) 229-8760
www.trainsignal.com

Copyright and other Intellectual Property Information

Disclaimer and Limitation of Liability

Although the publishers and authors of the Information have made every effort to ensure that the information within both the lab books and video were correct at the time of publication, the publishers and the authors do not assume and hereby disclaim any liability to any party for any loss or damage caused by errors, omissions, or misleading information.

TRAIN SIGNAL, INC. PROVIDES THE INFORMATION "AS-IS." NEITHER TRAIN SIGNAL, INC. NOR ANY OF ITS SUPPLIERS MAKES ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. TRAIN SIGNAL, INC. AND ITS SUPPLIERS SPECIFICALLY DISCLAIM THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THERE IS NO WARRANTY OR GUARANTEE THAT THE OPERATION OF THE INFORMATION WILL BE UNINTERRUPTED, ERROR-FREE, VIRUS-FREE, OR THAT THE INFORMATION WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY. YOU ASSUME THE ENTIRE RISK OF SELECTION, INSTALLATION AND USE OF THE INFORMATION.
IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING WITHOUT LIMITATION, TORT, CONTRACT, OR STRICT PRODUCTS LIABILITY, SHALL TRAIN SIGNAL, INC. OR ANY OF ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER MALFUNCTION, OR ANY OTHER KIND OF DAMAGE, EVEN IF TRAIN SIGNAL, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL TRAIN SIGNAL, INC. BE LIABLE FOR DAMAGES IN EXCESS OF TRAIN SIGNAL, INC.'S LIST PRICE FOR THE INFORMATION.

To the extent that this Limitation is inconsistent with the locality where You use the Software, the Limitation shall be deemed to be modified consistent with such local law.

Choice of Law:

You agree that any and all claims, suits or other disputes arising from your use of the Information shall be determined in accordance with the laws of the State of Illinois, in the event Train Signal, Inc. is made a party thereto. You agree to submit to the jurisdiction of the state and federal courts in Cook County, Illinois for all actions, whether in contract or in tort, arising from your use or purchase of the Information.

TABLE OF CONTENTS

Introduction

Welcome to Train Signal!

This series of labs on Windows 2000 & Server 2003 is designed to give you detailed, hands-on experience working with both Windows 2000 and Server 2003. Train Signal's Audio-Visual Mega Labs are targeted towards the serious learner, those who want to know more than just the answers to the test questions. We have gone to great lengths to make this series appealing to both those who are seeking Microsoft certification and to those who want an excellent overall knowledge of Windows 2000 & Server 2003.

Each of our Mega Labs puts you in the driver's seat, working for different fictitious companies, deploying complex configurations and then modifying them as your company grows. Mega Labs are not designed to be a "cookbook lab," where you follow the steps of the "recipe" until you have completed the lab and have learned nothing. Instead, we recommend that you perform each step and then analyze the results of your actions in detail.

To complete these labs yourself, you will need at least three computers equipped as described in the Lab Setup section. You also need to have a basic foundation in Windows 2000 and TCP/IP concepts. You should be comfortable with installing Windows 2000 Professional or Server and getting the basic operating system up and running. Each of the labs in this series will start from a default installation of Windows 2000 and will then run you through the basic configurations and settings that you must use for the labs to be successful. It is very important that you follow these guidelines **exactly**, in order to get the best results from this course.

The course also includes a CD-ROM that features an audio-visual walk-through of all of the labs in the course. In the walk-through, you will be shown all of the details from start to finish on each step, for every lab in the course. During the instruction, you will also benefit from live training that discusses the current topic in great detail, making you aware of many of the associated fine points.

Thanks for choosing Train Signal!

Scott Skinger
Owner
Train Signal, Inc.

Lab Setup

Setting up the Lab

1. Computer Equipment Needed

Item	Minimum	Recommended
Computers	(3) Pentium I 133 MHz	(3) Pentium II 300MHz or greater
Memory	128 MB	256 MB
Hard Drive	4 GB	6 GB or larger
NIC	1/machine (3 computers)	1/machine (3 computers)
Hub/Switch	1	1
Network Cable	(3) Category 5 cables	(3) Category 5 cables

You are strongly urged to acquire all of the recommended equipment in the list above. It can all be easily purchased from eBay or another source, for around $400 (less if you already have some of the equipment). This same equipment is used over and over again in all of Train Signal's labs and will also work great in all sorts of other network configurations that you may want to set up in the future. It will be an excellent investment in your education. Call or email us at: support@trainsignal.com, if you need help locating networking equipment. Two other products that you may also want to look into are a KVM (Keyboard-Video-Mouse) switch and a disk-imaging product, such as Norton Ghost. The KVM switch will allow you to run all of your computers using a single keyboard/monitor/mouse set. A button allows you to quickly control which PC you are managing. Disk imaging software will save you a tremendous amount of time when it comes to reinstalling Windows 2000 for future labs. Many vendors offer trial versions or personal versions of their products that are very inexpensive.

2. Computer Configuration Overview

Computer Number	1	2	3
Computer Name	SA-1 (Member Server)	DC-1 (Domain Controller)	Pro-1 (Client)
IP Address	192.168.1.201/24	192.168.1.200/24	192.168.1.1/24
Default Gateway	TBA	TBA	TBA
OS	W2K Server	W2K Server	W2K Pro
Additional Configurations	SP2 or higher	SP2 or higher	SP2 or higher

*****Important Note*****
This lab should NOT be performed on a live production network. You should only use computer equipment that is not part of a business network AND is not connected to a business network. Train Signal Inc. is not responsible for any damages. Refer to the full disclaimer and limitation of liability, which appears at the beginning of this document and on our Website at: http://www.trainsignal.com/legalinfo.html

3. Detailed Lab Configuration

Computer 1

Computer 1 will be named SA-1 and the operating system on this computer will be Windows 2000 Server or Advanced Server. Service Pack 2 or higher should be installed on this machine in order to perform some of the steps in this lab.

SA-1 needs only one network card, which should be configured with a static IP address of 192.168.1.201 and a subnet mask of 255.255.255.0. Set the preferred DNS Server to **192.168.1.200** and leave the alternate DNS setting **blank**. There will be no default gateway at this time. You will need to make this computer a member server of the storksbaseball.com domain (see note below), by simply right clicking on the **My Computer** icon on the desktop and selecting **Properties**. Select the **Network identification** tab, **Properties**, **domain** and type in the domain name of the domain it will join, which is **storksbaseball.com** or its NetBIOS name, **storksbaseball**. Note: NetBIOS names are a single label (no periods) up to 15 characters in length. Then click **OK**. Windows 2000 will then ask for a username and password. Use a domain administrator account name and password from the storksbaseball.com domain. When it has joined successfully, it will "welcome you to the domain" and then tell you that it needs to restart in order for the changes to take effect. After restarting the computer, make sure you change the "Log on to" dialog box to the domain rather than this computer". See figure 1, page 14.

*****Important Note*****

This last step (joining SA-1 to the domain) cannot be performed until you have created the storksbaseball.com domain by running dcpromo on DC-1 in the Computer 2 setup below.

Computer 2

Computer 2 will be named DC-1 and Windows 2000 Server or Advanced Server will be installed on this computer along with Service Pack 2 or higher. DC-1 will have a static IP address of 192.168.1.200 with a 255.255.255.0 subnet mask. The Preferred DNS server setting should be configured with DC-1's own IP address, **192.168.1.200** and no default gateway is necessary at this time. See figure 1, page 14.

DC-1 will be setup as the domain controller for the Springfield Storks Baseball Club, called storksbaseball.com by using the dcpromo.exe program. In order to make this machine a domain controller, Active Directory and DNS will need to be installed. There are 2 ways to install DNS – automatically when you run dcpromo.exe or manually when you install it through Add/Remove Programs in Control Panel. For the purposes of this lab, we are going to install DNS automatically. To run dcpromo.exe on this machine go to the desktop, click on **Start → Run**, then type in **DCPROMO** in the run command and click **OK**.

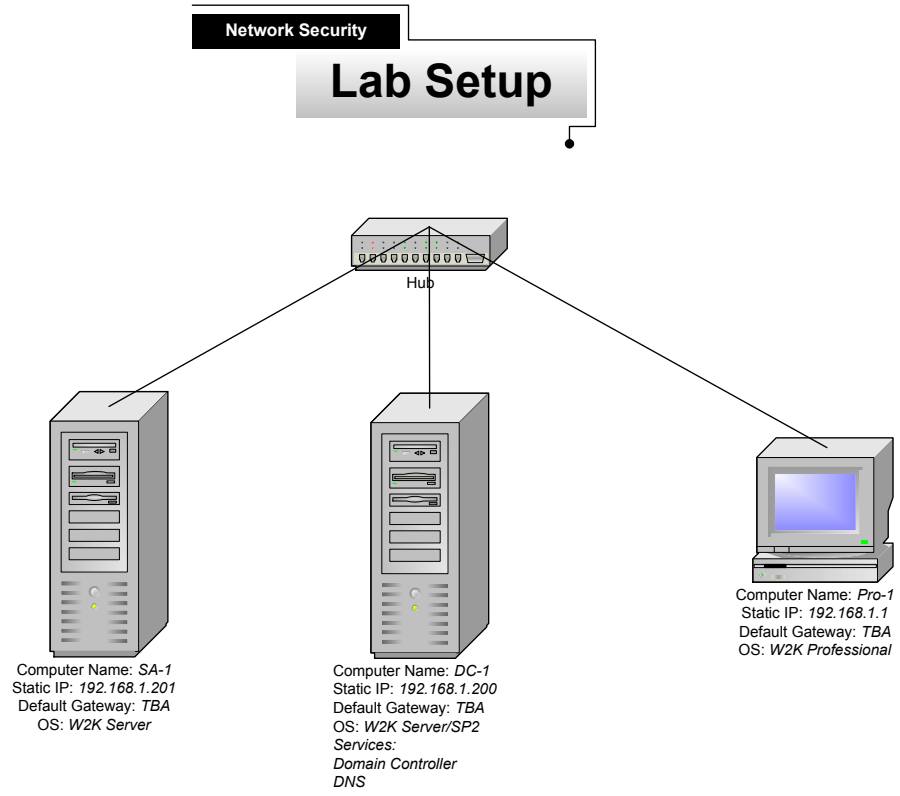
Make the following selections as you are prompted: **Domain controller for a new domain; Create a new domain tree; Create a new forest of domain trees.** The DNS domain name for the scenario is storksbaseball.com. The NetBIOS name will be storksbaseball. Leave all the other settings at their defaults. When the wizard asks if you would like to install and configure DNS on this computer, select **Yes, install and configure DNS on this computer**. Also choose permissions compatible with pre-Windows 2000 servers. In the next step, you will be asked for an AD password – for our purposes, we will leave this blank. Active Directory installation should then take place and you can restart the computer when you are prompted. **MAKE SURE** that the network card is plugged into a hub or into another computer with a crossover cable before you run dcpromo. Otherwise, Active Directory installation will fail, without giving you a clear cause. See figure 1, next page.

Computer 3

Computer 3 will be named Pro-1 and will have Windows 2000 Professional installed as the operating system. It is not necessary to install any Service Packs or hot fixes on this machine because it will be updated within the lab. If you have already installed service packs, or if your operating system came with a service pack, this is also ok. At this time don't install any further updates.

Pro-1 will have a static IP address of 192.168.1.1 with a 255.255.255.0 subnet mask. Set the preferred DNS Server to **192.168.1.200** and leave the alternate DNS setting blank. There will be no default gateway. You will need to make this computer a member of the storksbaseball.com domain, by right clicking on the **My Computer** icon on the desktop and selecting **Properties**. Select the **Network identification** tab, **Properties**, **domain** and type in the domain name of the domain it will join, which is **storksbaseball.com** or its NetBIOS name, **storksbaseball**. Note: NetBIOS names are a single label (no periods) up to 15 characters in length. Then click **OK**. Windows 2000 will then ask for a username and password. Use the administrator account name and password from the storksbaseball.com domain. When it has joined successfully, it will "welcome you to the domain" and then tell you that it needs to restart in order for the changes to take effect. After restarting the computer, make sure you change the "Log on to" dialog box to the domain rather than "this computer". See figure 1, next page.

Important - You should test the network connections (using the PING command) between each of these machines to ensure that your network is set up properly. Testing before you get started will save you major time and effort later.



(figure 1)

Lab 1

Analyzing and Applying Security Settings to Computers on the Springfield Storks' Network

You will learn how to:

- Use the Security Configuration and Analysis tool
- Configure security with the Security Configuration and Analysis tool
- Create a custom security template
- Import a custom security template into Active Directory

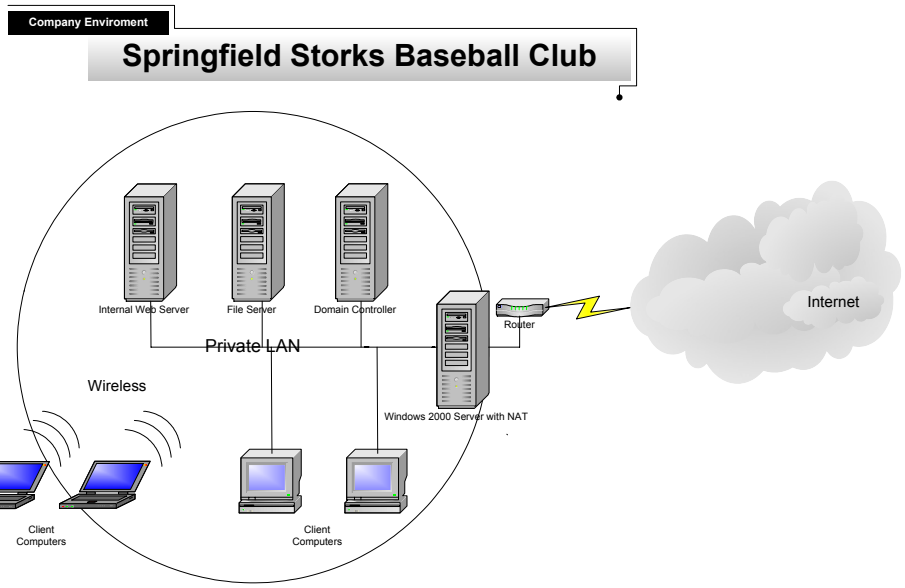
Scenario

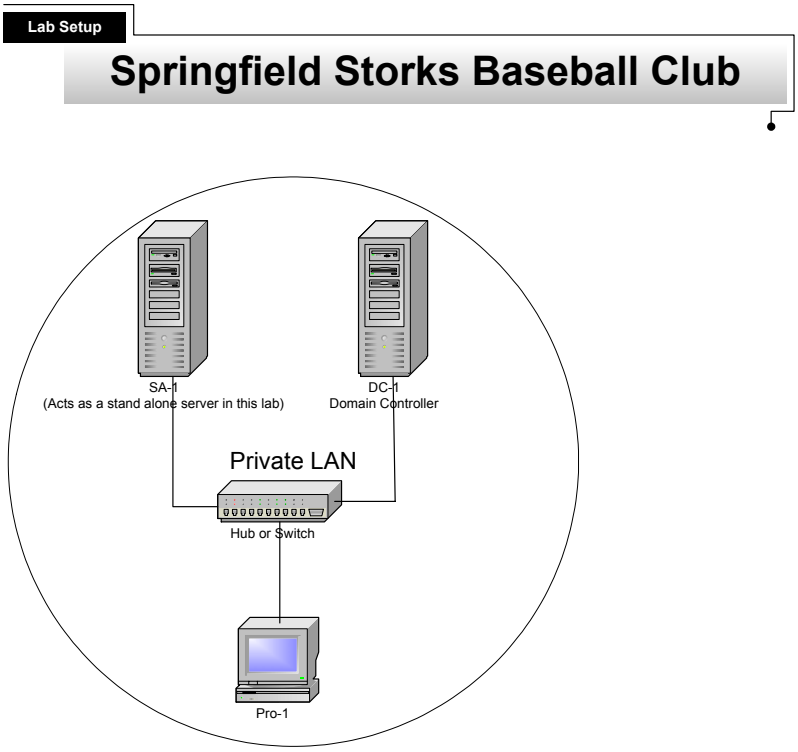
The Springfield Storks are a minor league baseball team that plays their home baseball in Springfield, NY. Over the past three years the Storks have been one of the most successful minor league franchises both on and off the field. Their great marketing success off the field has given them the financial resources necessary to develop a state-of-the-art IT infrastructure within their stadium. The Storks have their entire stadium networked. Ticket sales, concession sales and souvenir sales are all automatically tracked and recorded. Fans in the club section have Internet access and can order food and drinks using the Storks automated ordering systems. The executive offices, broadcast booths and clubhouses are all networked using a combination of wired and wireless access. Even members of the press can bring their laptops and hook into the Storks' network for up to the minute news from the team's management.

So far this season the Storks are in 1st place and are posting record sales figures, but they now face a serious problem. During a recent home stand, parts of the network have started to perform unacceptably slow or have failed completely. Within a couple of days, the problems have spread and the entire network is now down. The Storks' management is extremely concerned because they have been forced to manually track sales and inventory, tasks for which they are both unprepared and understaffed. Furthermore, the Storks' network administrator isn't sure, but his gut tells him that the network has been hacked into. The network administrator, Joe, does not have much experience with security and he really isn't sure how to solve the problem.

Joe has called upon you, an independent consultant, to help solve their network woes. After you assess the situation, you have determined that a hacker(s) has indeed penetrated the network and has left it in shambles. Viruses and worms are also running rampant across the network, hence the network performance problems. Because of the wide-spread damage and the fact that this is a fairly small network, you have made the recommendation to the Storks' management that the network be completely rebuilt, reinstalling all of the operating systems and then carefully reinstating the data, after a thorough virus scan. The management reluctantly agrees and vows to never put security on the back burner again.

In this lab, you will learn how to secure a Windows 2000 Network using powerful tools that make managing a network more efficient and effective. You will start by learning how security templates can be used to establish common security settings on all of your systems. Next, you will use Group Policy to take security to the next level by assigning specific policies to different Active Directory containers. Finally, you will learn about Software Update Services (SUS), a free tool from Microsoft that will help you automate the process of patching servers and workstations on your network.

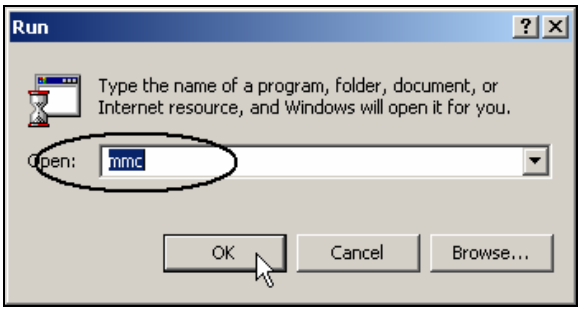




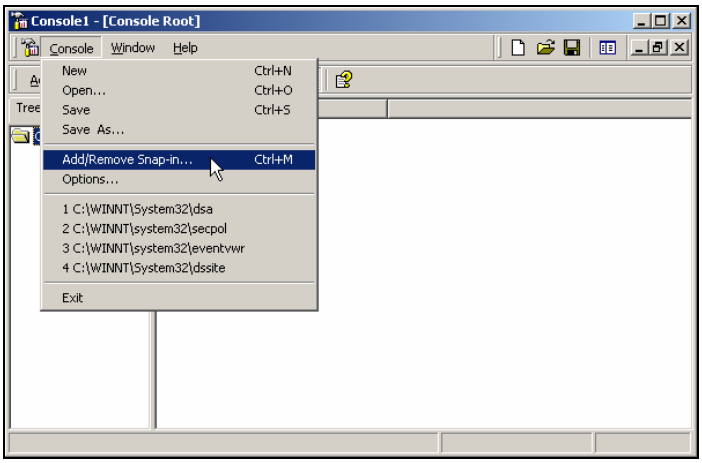
Security Templates

Security templates are a set of security settings stored within a text file. Windows 2000 and Server 2003 come with many predefined security templates that can be applied to your clients or servers. These templates range from basic (default) security to high security. You can compare your current computer security settings against any of the security templates, by using the Security Configuration and Analysis tool. This tool can then be used to apply the template security settings to your current configuration all at once. To assist Joe and the Storks in the future, you are going to show him how these tools work.

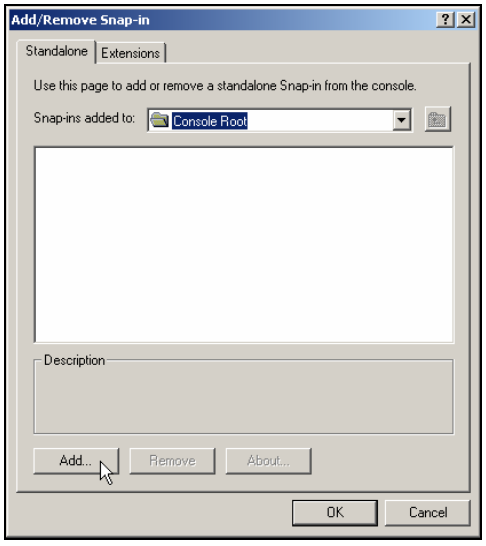
1. To open the Security Configuration and Analysis and the Security Templates snap-ins, log on to **SA-1** and go to **Start→Run.** Type in **mmc** and click **OK** to open the Microsoft Management Console (MMC).

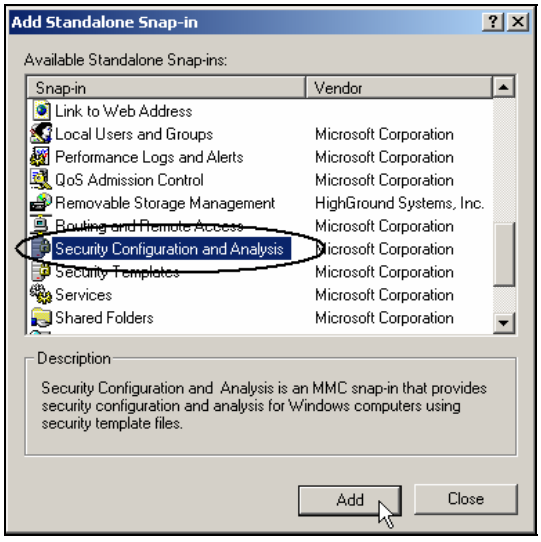


2. This will bring you to the Console 1 window. Select **Console→Add/Remove Snap-in** from the menu.

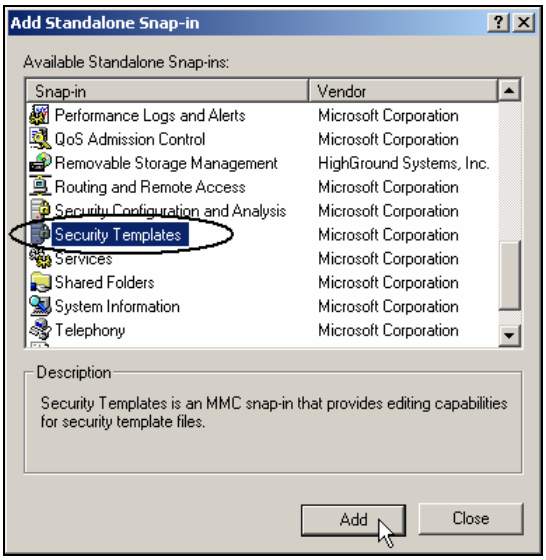


3. In this Add/Remove Snap-in screen, just click **Add** and you will see that there are many snaps-ins available for you to add. Select **Security Configuration and Analysis** and click **Add**.

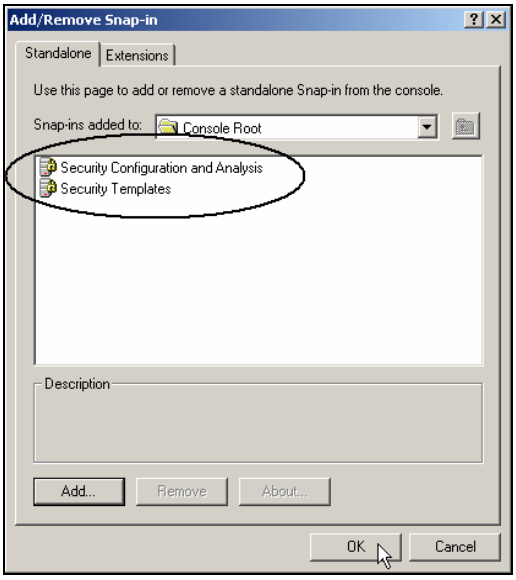




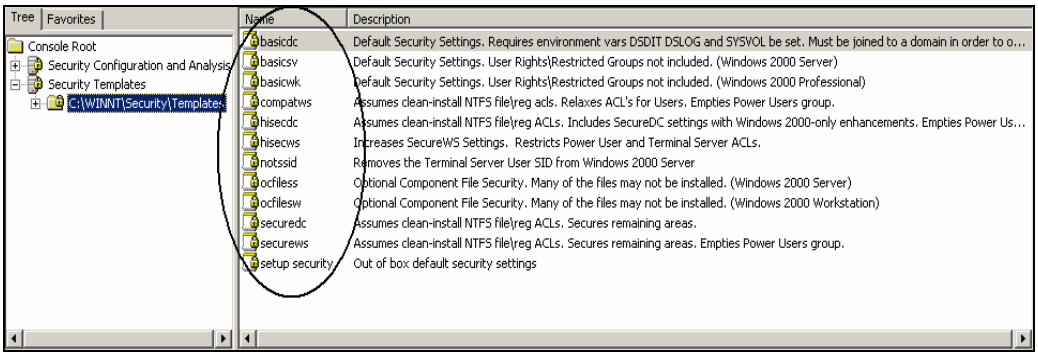
4. Additionally, select **Security Templates** as a second snap-in. Click **Add** and **Close**.



5. Next, verify that the Security Configuration and Analysis and Security Templates Snap-ins are added and click **OK** to close this Add/Remove Snap-in window.



6. Click on **Security Templates** and then select **C:\WINNT\Security\Templates** under the Console Root in the left pane. This will bring you to all of the available security templates located within SA-1.



Windows 2000 & Server 2003 Templates

By default, Windows 2000 and Server 2003 include an assortment of security templates located in the %systemroot%\Security\Templates folder. For the most part, the names of these templates describe their purpose and correspond to their level of security. However, keep the following points in mind:

- Template names that end with sv are for standalone or member servers
- Template names that end with dc are for Domain Controllers
- Template names that end with wk are for workstations
- Template names that end with ws are for workstations ***and*** member/stand-alone servers

basic*.inf - Used to set the initial configuration of a computer back to the installation default settings. There are 3 different basic templates: basicwk.inf, basicsv.inf and basicdc.inf.

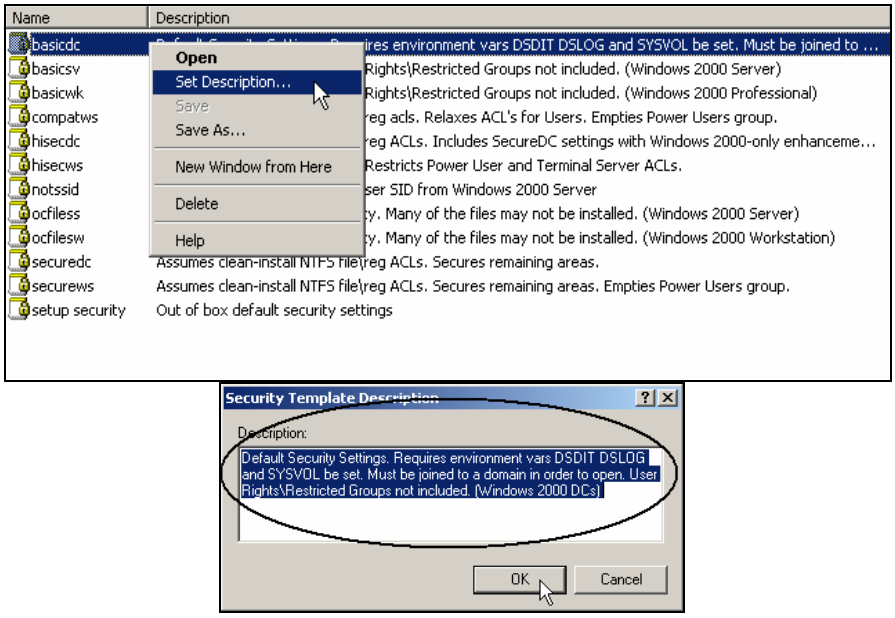
compatws.inf – Lowers security allowing users to run legacy applications without being a power user. It reduces security levels on folders, files, and registry keys that applications typically access.

secure*.inf - These templates provide an intermediate level of security, securing the registry, account policies and auditing. There are 2 different secure templates: securews.inf and securedc.inf.

hisec*.inf - These templates are used to provide the highest level of pre-configured security. They increase the security of network communications by requiring IPSec. They can cause network communication problems, especially with legacy operating systems. There are 2 different high security templates: hisecws.inf and hisecdc.inf.

notssid.inf – When this template is applied it removes the terminal server SID from all registry and file system objects, which have an ACE for the terminal server SID.

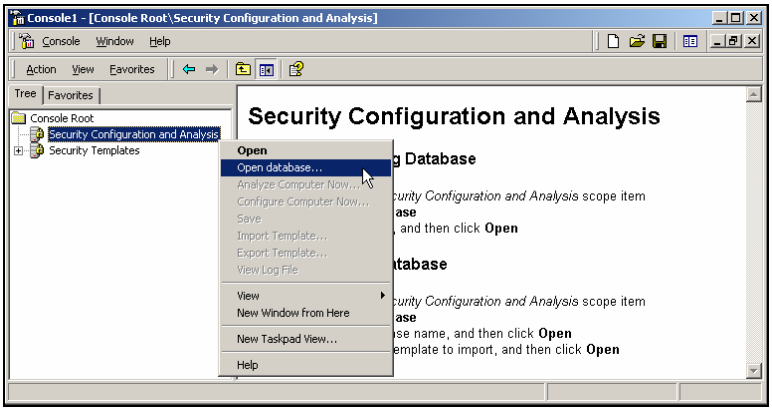
7. Right click on one of the templates. Select **Set Description**. Notice that you can change the default description name if you desire. Click **OK** to close.



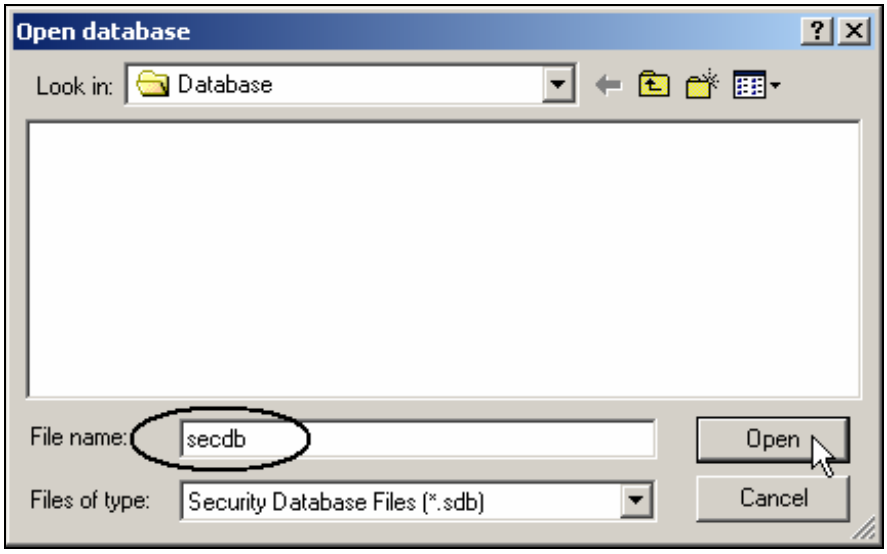
Analyze and configure SA-1 security settings

In this section, you will analyze the security on SA-1, by comparing it to one of the default templates described above. First though, you must create a baseline security configuration database, SDB file.

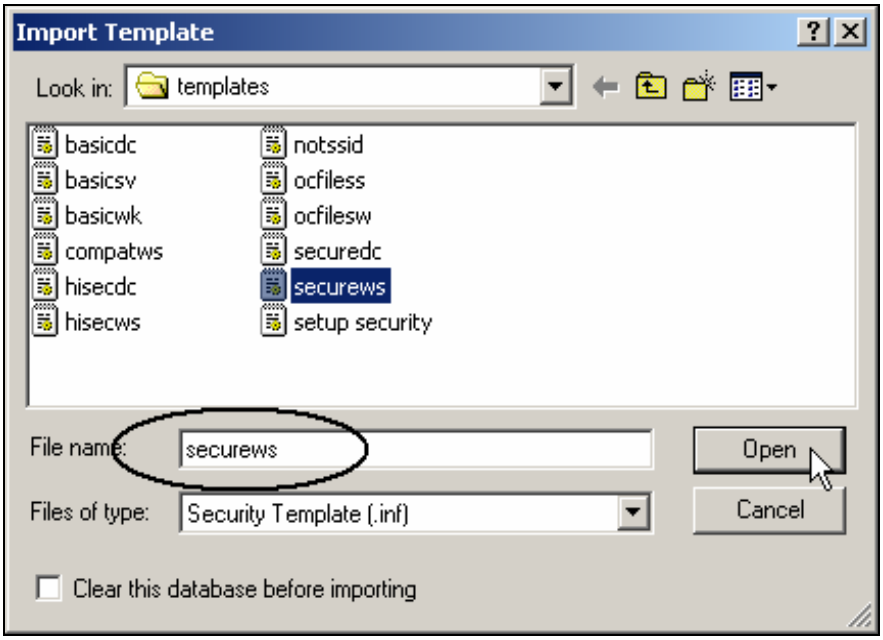
1. Right click on **Security Configuration and Analysis** under the Console Root in the left pane. Next, select **Open database** to create a new database.



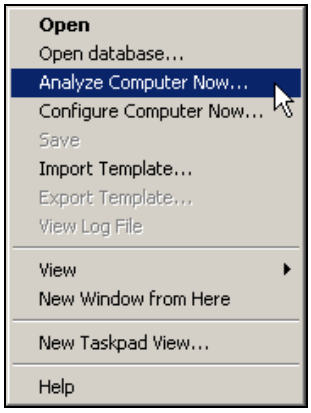
2. This will bring up the Open database dialog box. Type in **secdb** (you can use any name) as the Security Database File name and click **Open.**.



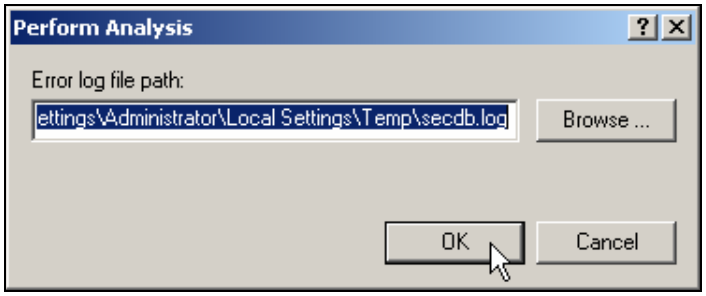
3. Next, in the Import Template dialog box, select **securews.inf** and click **Open**. This security template will be used to compare the current security settings on SA-1 with the settings in this template.



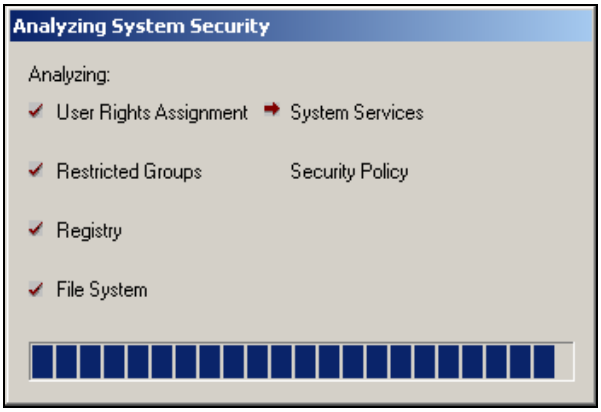
4. In order to analyze the security settings on SA-1, right click on **Security Configuration and Analysis** under the Console Root and select **Analyze Computer Now**.



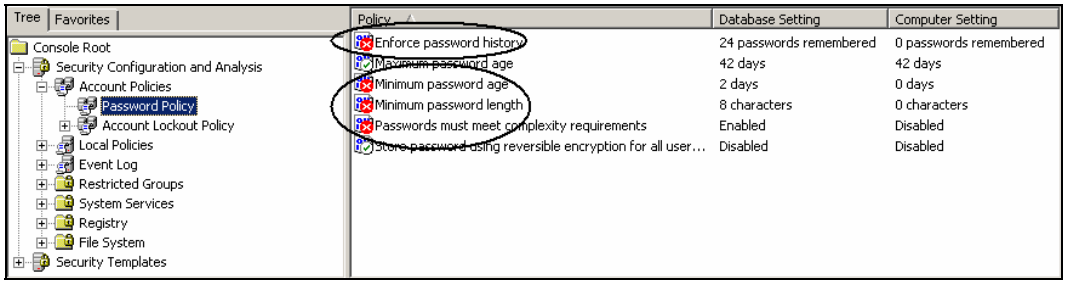
5. This will bring up a dialog box that allows you to specify a location for the Error log. Click **OK** to accept the default log file path for the analysis results.

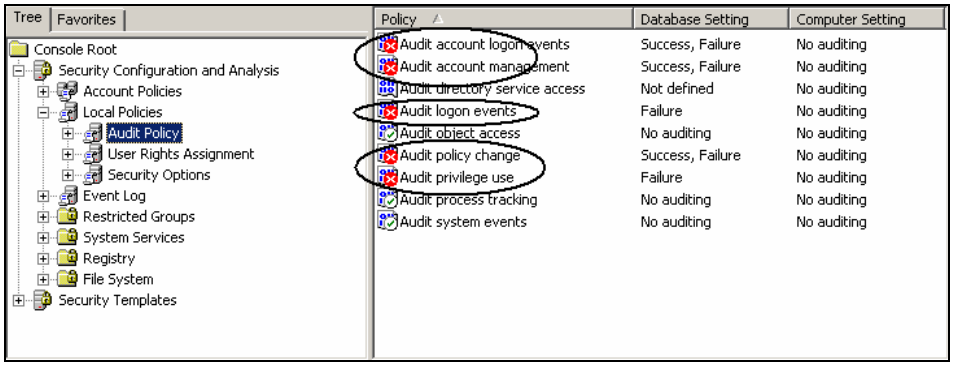


6. The analysis will then begin and you will see the progress in the Analyzing System Security dialog box.

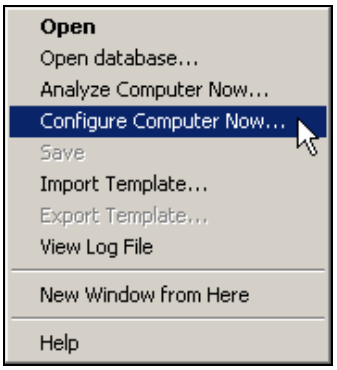


7. After the analysis is completed, you can view the results by clicking on any of the nodes in which you're interested. The right pane of the console displays the actual computer settings and the database settings. If the computer's current settings do not meet the minimum requirements of the security template's settings, then the specific policy is marked with a red X as you can see below.

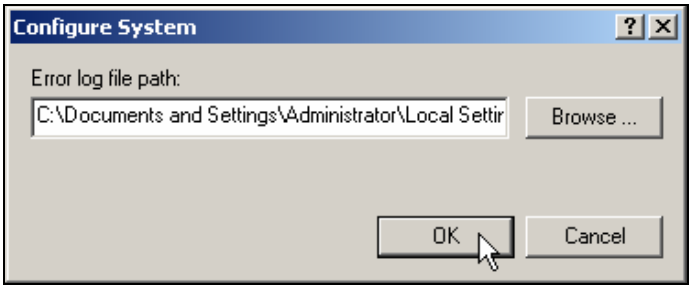




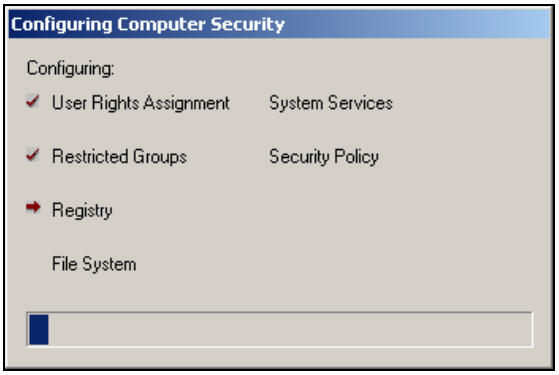
8. After you and Joe have compared SA-1's current security settings with the securews security template settings, you decide to use all of the settings within the security template on SA-1. To accomplish this, right click on **Security Configuration and Analysis** and select **Configure Computer Now**. Keep in mind that this action will change *all* of the configured security settings in the template and can lead to severe network problems. In a production environment, **TEST** these settings thoroughly before applying them blindly to a server.



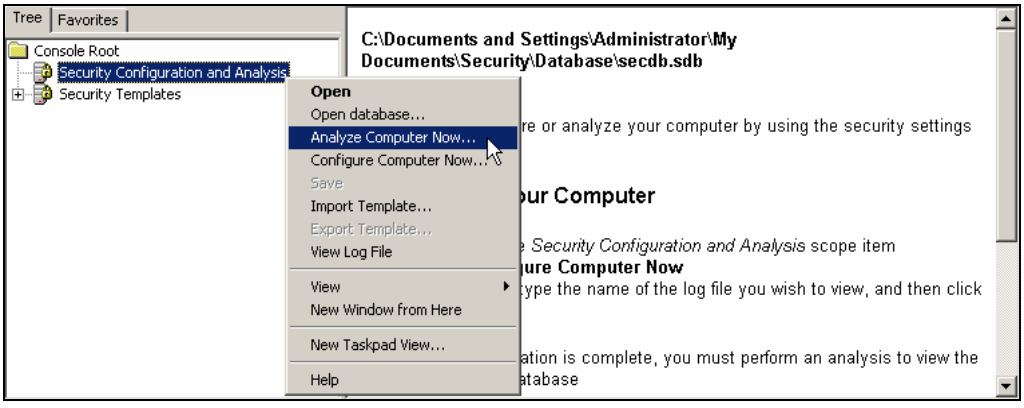
9. Next, you will see the same type of dialog box you saw previously, allowing you to specify a location for the error log. Accept the default by clicking on **OK**.



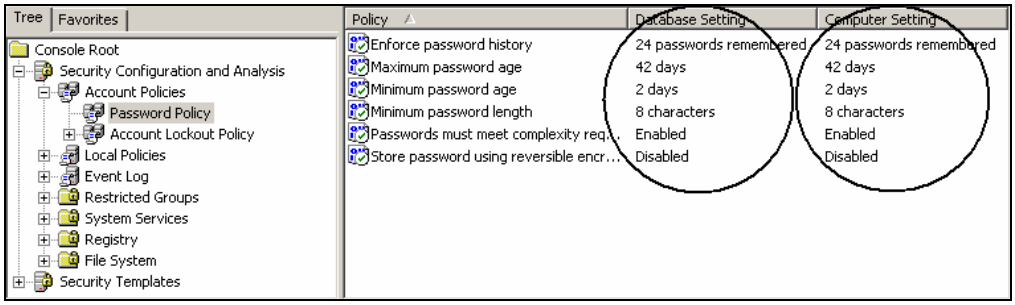
10. The configuration will then begin and you will see the progress in this Configuring Computer Security dialog box.

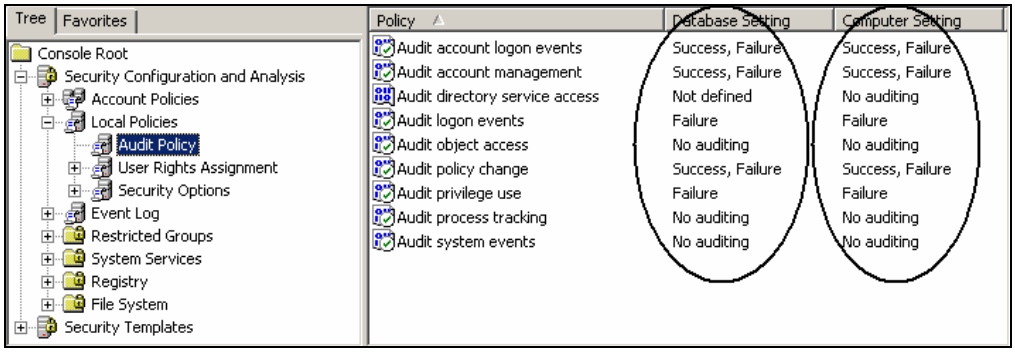


11. After the configuration is completed, right click on **Security Configuration and Analysis** and select **Analyze Computer Now**.



12. When the analysis is completed, you can view the results by clicking on any of the nodes. After applying the securews.inf security template, you'll find that the local computer settings and the database settings are now the same. All of the settings should be the same throughout the different types of policies.

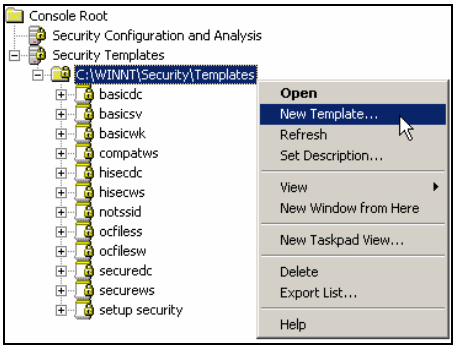




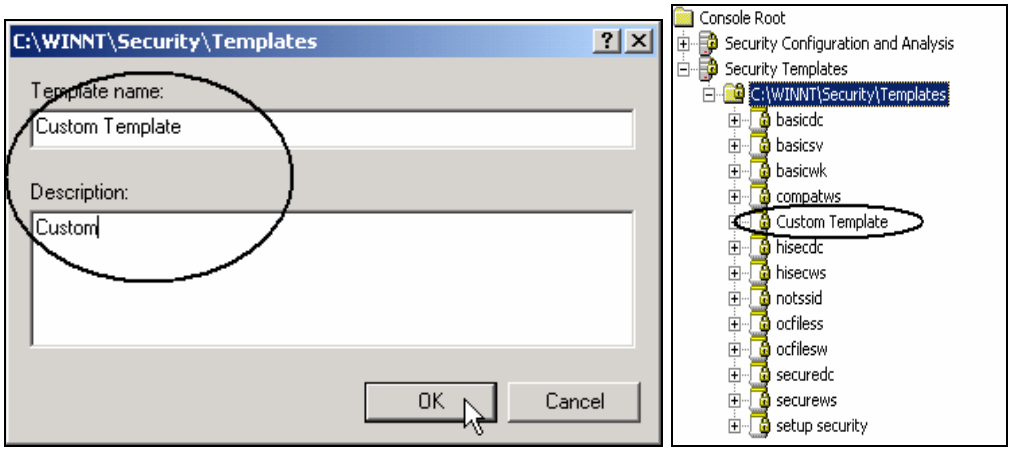
Custom Templates

In addition to the default templates that come with Windows 2000 and Server 2003, you can also create your own custom security templates.

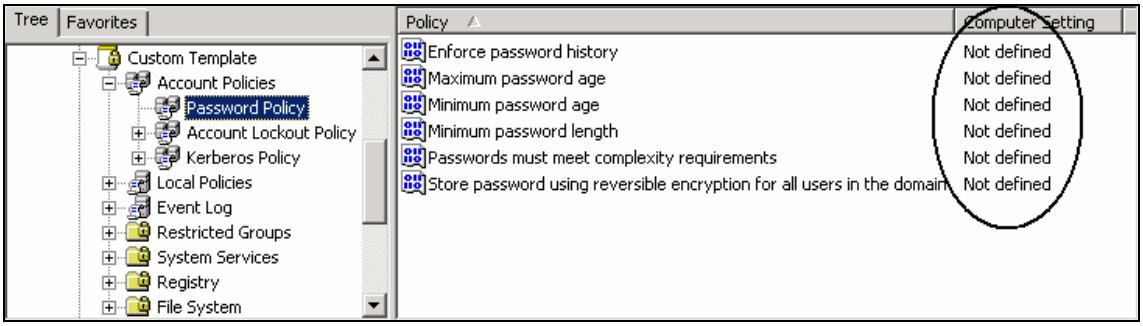
1. To create a custom template, click on **Security Templates** and right click on **C:\WINNT\Security\Templates** under the Console Root in the left pane. Select **New Template**.



2. This brings up a dialog box allowing you to name and describe your new template. Type in **Custom Template** as the Template name and **Custom** as the Description. Click **OK** to create this new custom template.

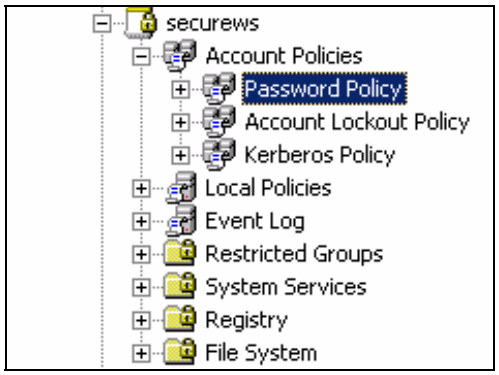


3. The template that you have created is brand new and has not been configured. Therefore, none of the settings have being defined. This will require you to go through and configure every setting or risk leaving your computer and/or network unsecured.



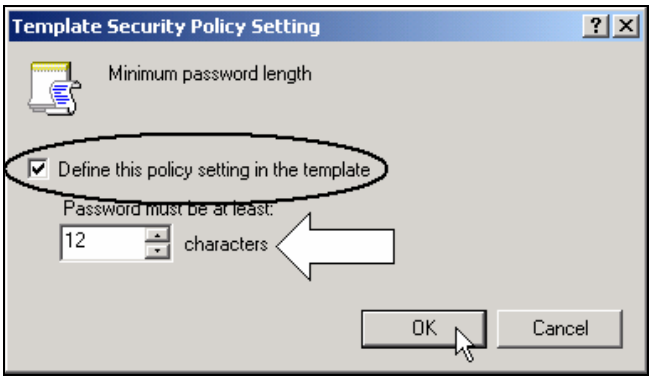
4. In most cases, the settings that you want to configure on your computer and/or network may vary only slightly from one of the default templates. In this case, you can modify one of the default templates and save it with a different name, thereby creating a custom template. The Storks have decided to try this, using the securews.inf security template for their baseline security settings. Once they have modified the necessary settings, the template will be saved with a custom name and they will apply it to the Servers OU in the storksbaseball.com domain.

   The first setting that you will modify is the minimum password length. To accomplish this, double-click **Account Policies** under **securews** in the left pane and click on **Password Policy**.

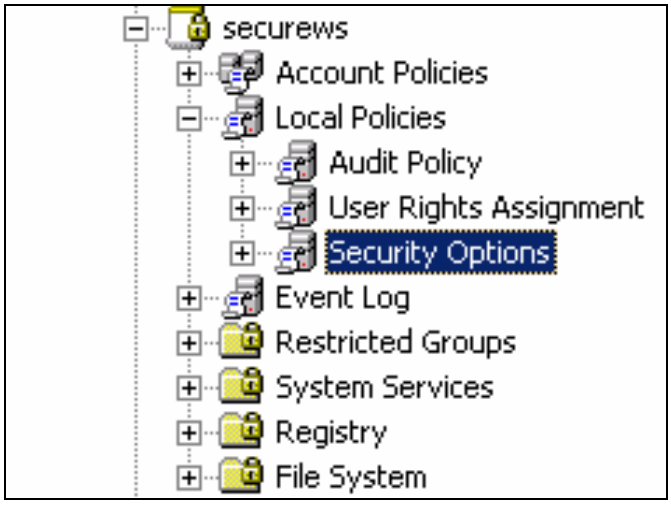


5. Double-click the **Minimum password length** policy in the right pane. This will bring up the Template Security Policy Setting dialog box. Place a check mark in the box **define this policy setting in the template** and configure the Password must be at least **box** to **12** characters. Click **OK** to continue.

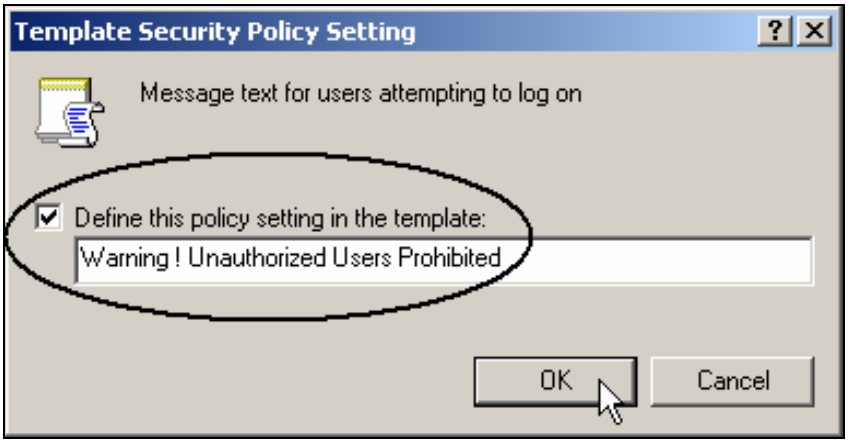
   Note: Account Policies must be set at the domain level. You can set account policies at the OU level but they will not work. The Minimum password length setting is being created for demonstration purposes only.



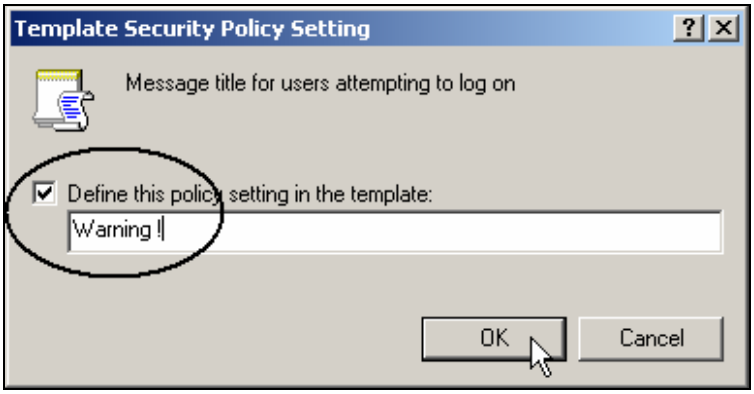
6. The next setting that the Storks want to modify is to enable a logon message text and title, which is not part of the securews security template. Double-click **Local Policies** under securews in the left pane and click on **Security Options**.



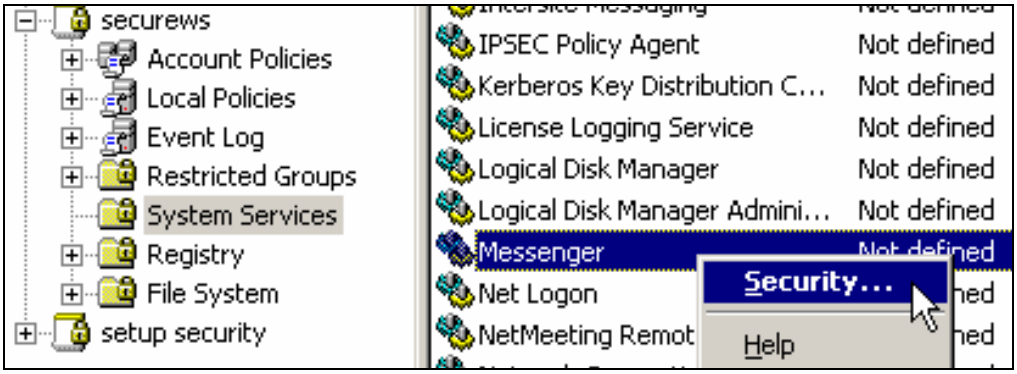
7. In the right pane, select and double click the **Message text for users attempting to log on**, which will open up the **Template Security Policy Setting** dialog box. In this dialog box, make sure Define this policy setting in the template is **checked**. Type in **Warning! Unauthorized Users Prohibited** and click **OK**.



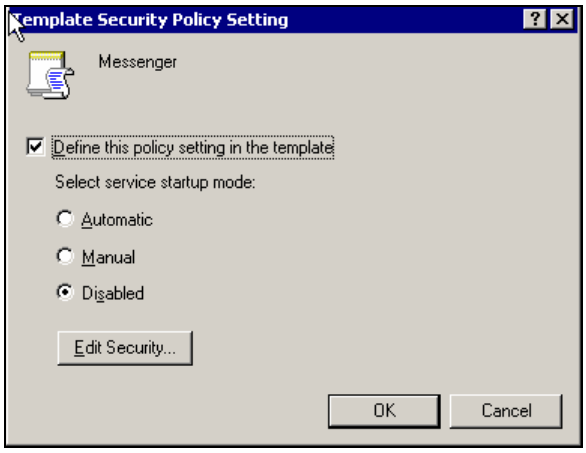
8. Again, from the right pane, select and double click the **Message title for users attempting to log on**, which will open up the **Template Security Policy Setting** dialog box. In this dialog box, make sure Define this policy setting in the template is **checked**. Type in **Warning!** and click **OK**. This setting (message title) controls the title that appears at the top of the logon dialog box, while the previous setting (message text) controls the main body of text that will appear during logon.

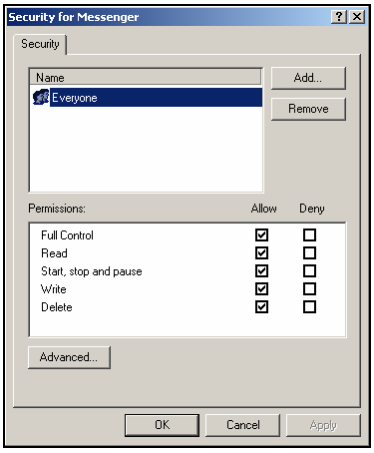


9. The next setting that the Storks want to modify is the Messenger service. The Storks have decided to disable this service to eliminate broadcast messages including SPAM. To access this, double-click **System Services** and from the right task pane, right click on **Messenger**. Select **Properties** and click **Security.**

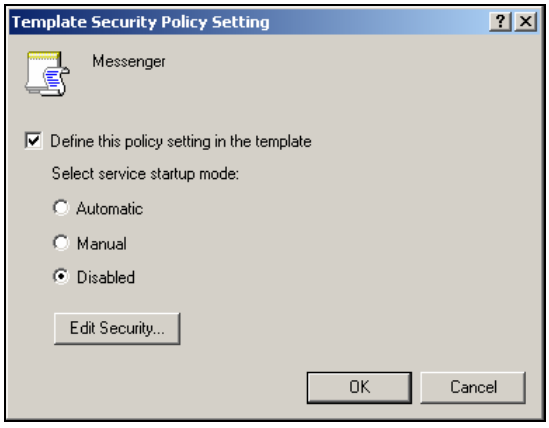


10. Check **Define this policy setting in the template** and then click **OK** to accept the default security permissions for now.

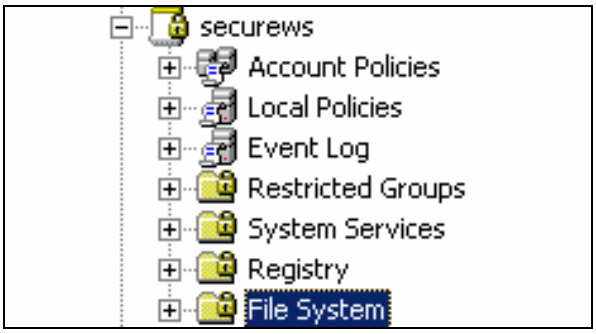


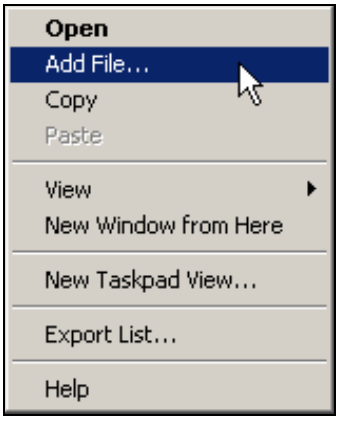


11. Make sure that the Messenger service is marked as **Disabled** and click **OK**.

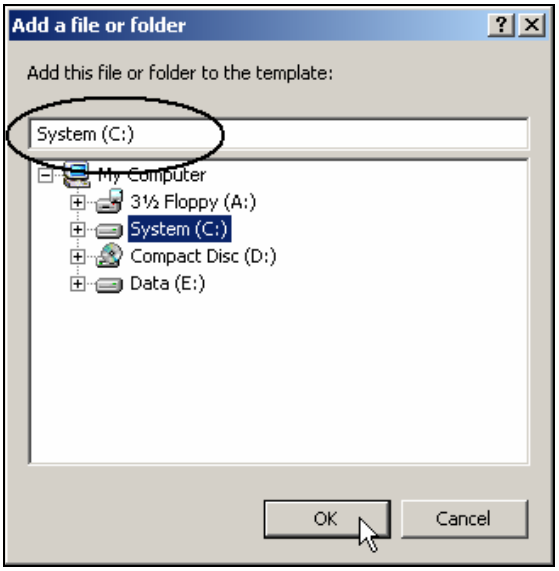


12. For now, the last setting the Storks will modify is to set the default NTFS permissions on the C drive. This can be configured by right clicking on **File System** under securews in the left pane and selecting **Add File**.

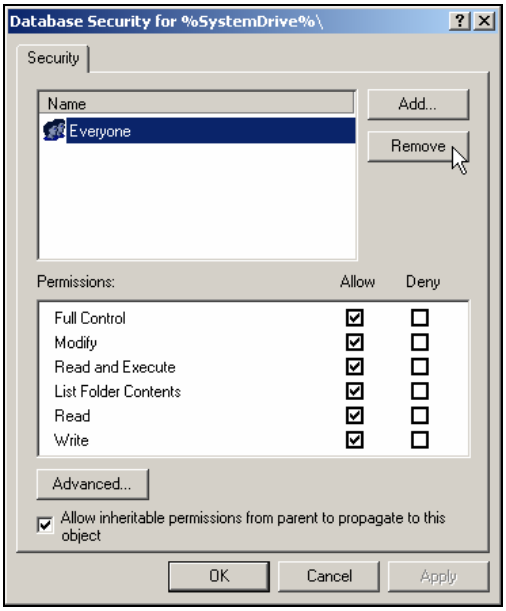




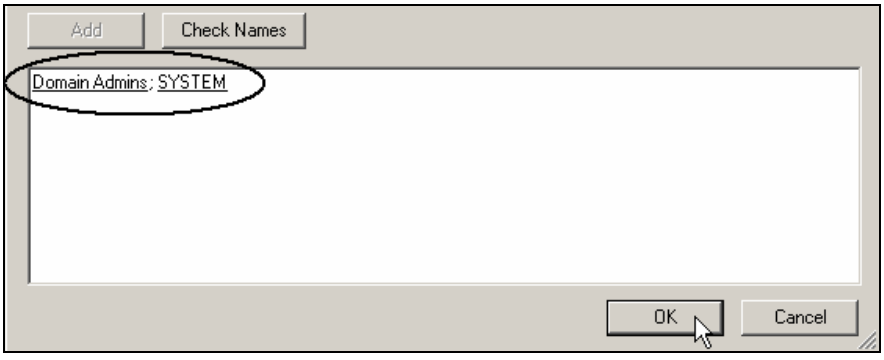
13. This will bring up the Add a file or folder dialog box. Add C: by highlighting it and clicking **OK**. The Storks want to set the default NTFS permissions on the C: drive so that only the Domain Admins group and the System group have access.



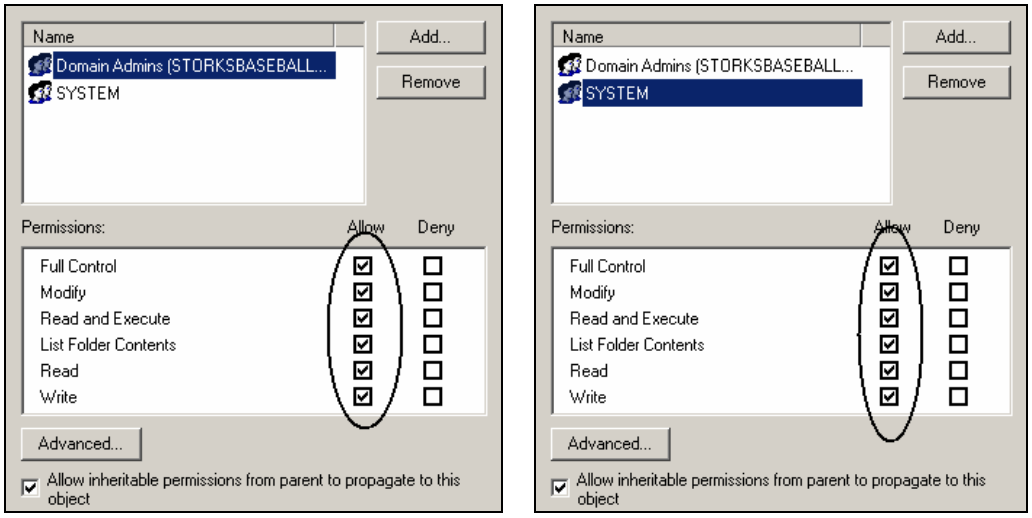
14. Clicking OK will bring up the Database Security for %SystemDrive%\ dialog box. By default, the Everyone group has full control permissions to the root of C:, which is not very secure. Highlight the **Everyone** group and click **Remove** to remove it.



15. Next, click on the **Add** button. This will bring you to the Select Users or Groups dialog box. In the Look in drop-down menu, select **storksbaseball.com**. Find and add the **Domain Admins** group and the **System** group from storksbaseball.com. Click **OK** to continue.



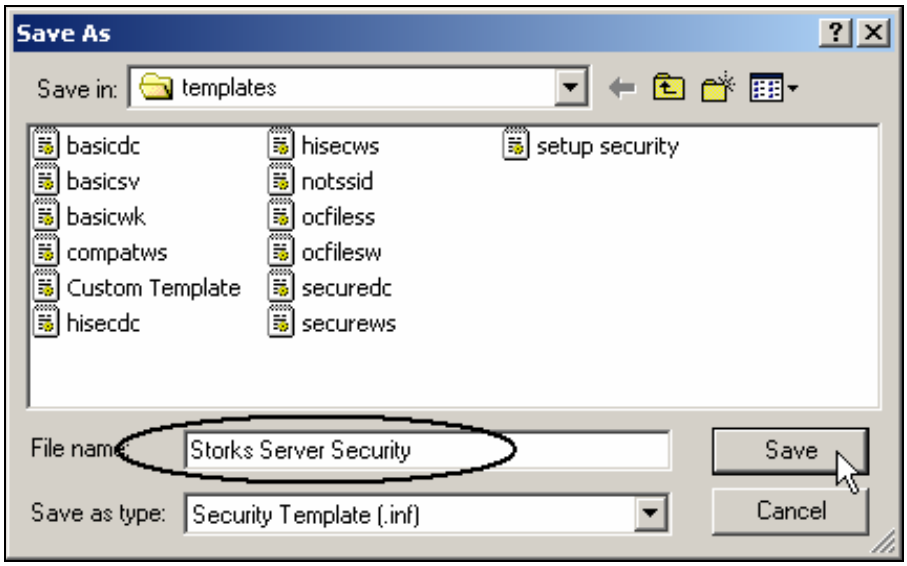
16. The two groups will now appear on the security list. By default, these two groups have limited permissions. Highlight **Domain Admins** and check the **Full Control** box in the Allow Column. This will automatically select everything in the column. Repeat the same steps to give full control permissions to the System group. Click **OK** to continue.



17. This brings up the Template Security Policy Setting dialog box. Leave the default selection to **Propagate inheritable permissions to all subfolders and files** and click **OK**.

18. You are now done modifying the settings on the **securews** security template and are ready to save this custom template. Right click on **securews** and select **Save As**.

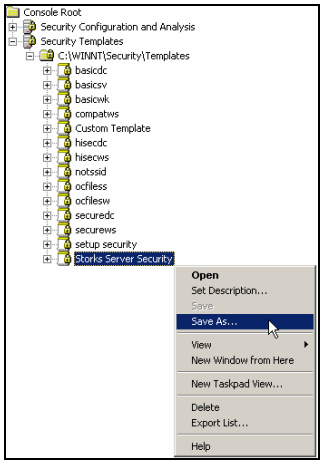
19. Type in **Storks Server Security** for the file name and click **Save** to save the template.



Importing the Security Template

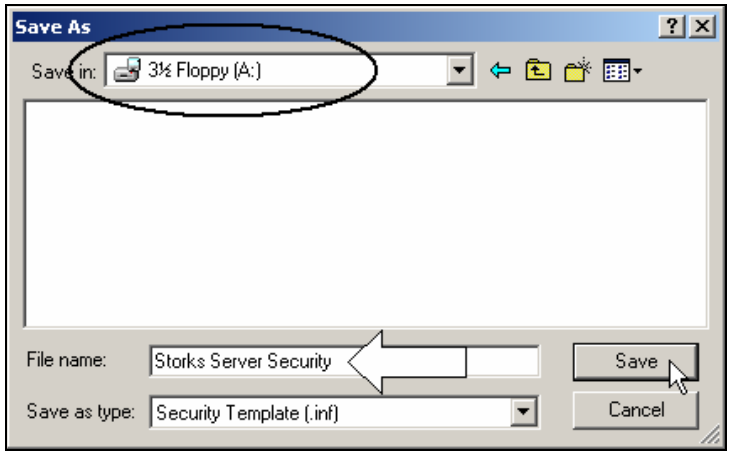
There are several different ways to import the Storks' Server Security template into Active Directory. For example, you can set up a shared folder on SA-1 and place the Storks Server Security template in it or you can save the template on to a floppy disk and manually transfer the file. For the purposes of this lab, we are going to save the template to a floppy and manually transfer it over to DC-1.

1. To save the Storks' Server Security template on a floppy, right click on **Storks Server Security** and select **Save As**.



2. Change the drive letter from C: to **A:** and leave the default file name. Insert a floppy into the drive and click **Save** to continue.

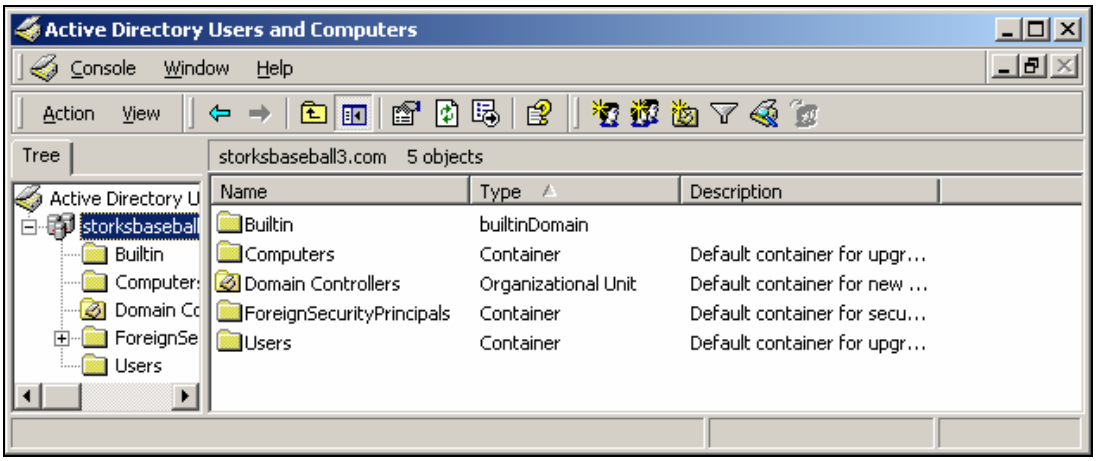
   Note: You will use this floppy later in order to import the template to the Servers OU in Active Directory.



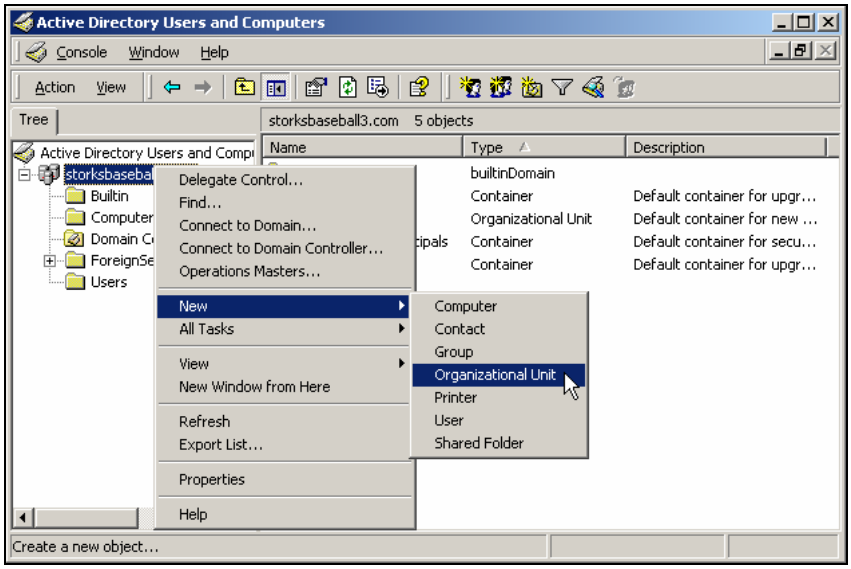
Creating the Servers OU

Next, you will need to create the Servers OU on DC-1. The Storks are creating this OU to hold all of their servers, which will simplify management and administration.

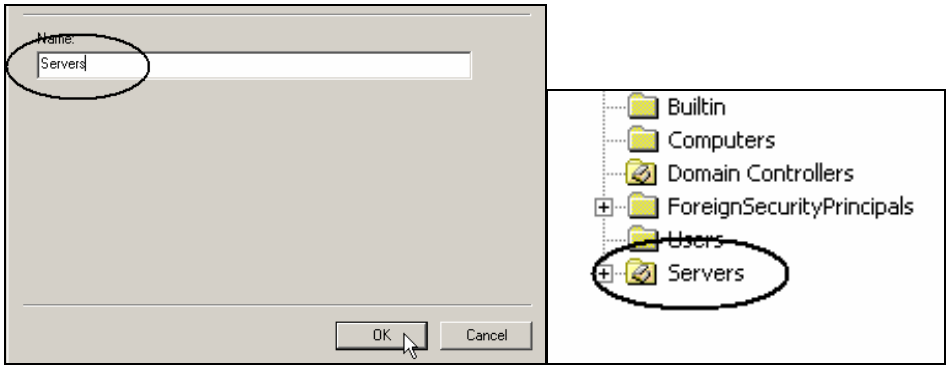
1. Log on to **DC-1** and open the **Active Directory Users and Computers** console by going to **Start→Programs→Administrative Tools→Active Directory Users and Computers**.



2. On the left side, right click on **storksbaseball.com** and select **New→Organizational Unit**.

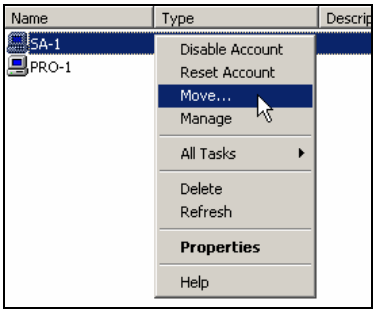


3. A screen will appear asking you to specify a name for the new OU. Type in **Servers** and click **OK**. You will now have an OU named Servers within Active Directory.



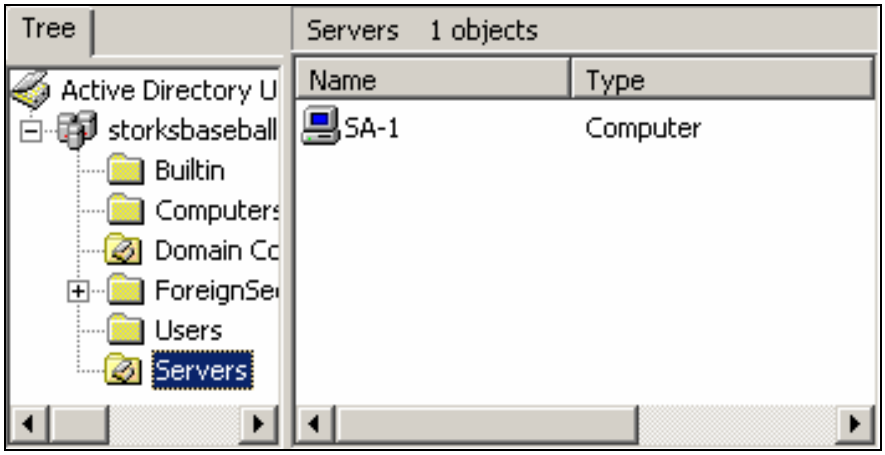
Moving SA-1 to the Servers OU

1. To move SA-1 to the Servers OU, first find SA-1, which is located within the Computers folder in Active Directory. Next, right click on **SA-1** and select **Move**.



2. That will bring up a small explorer window where you can browse through all the containers that are available within the domain. Select the **Servers OU** and click **OK**.

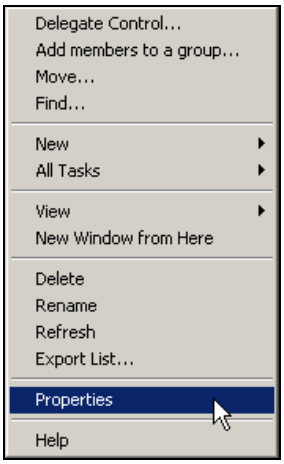
3. SA-1 should now appear within the Servers OU.



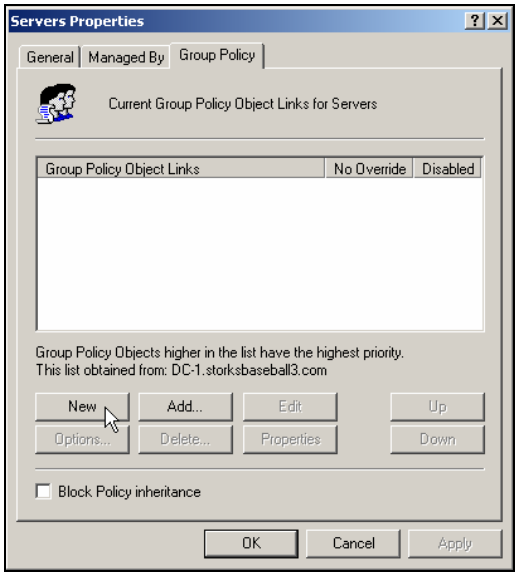
Importing Security Template to Active Directory

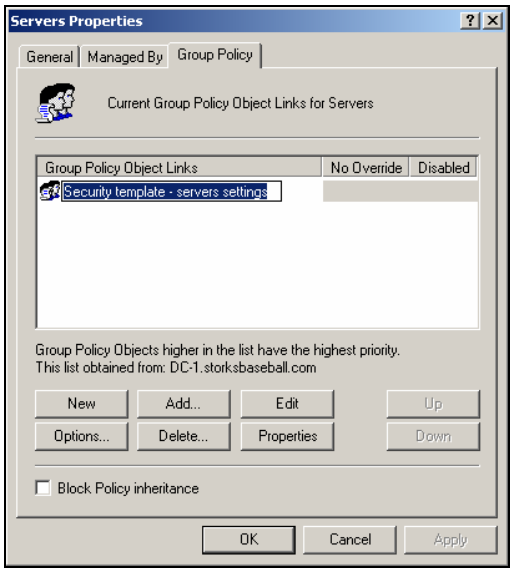
The custom template created earlier in this lab will now be imported into Active Directory and applied to the Servers OU. Applying the template to the Servers OU will apply the template's baseline security settings to all of the servers within the Servers OU.

1. Start this process by right clicking the **Servers OU** and selecting **Properties**.

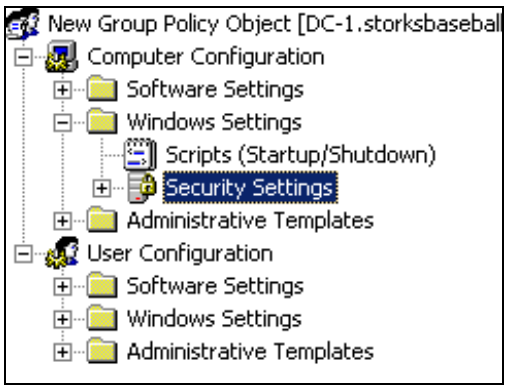


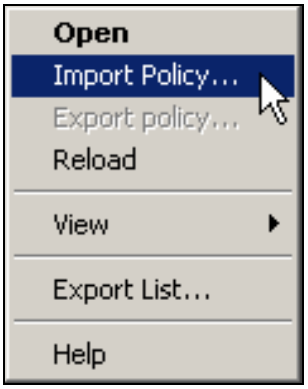
2. This will open the Servers Properties dialog box. Select the **Group Policy** tab and click **New**. Type in **Security template – servers settings** for the new policy name and click **Edit**.



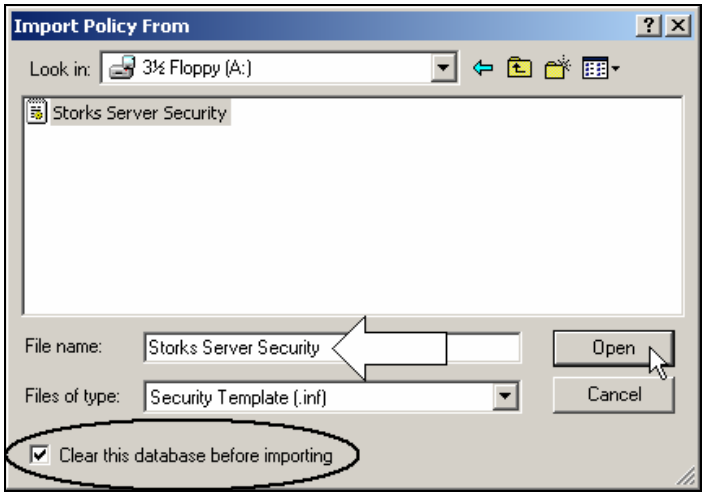


3. From within the Group Policy dialog box, click on **Computer Configuration** → **Windows Settings** and right click on **Security Settings.** Now select **Import Policy**.

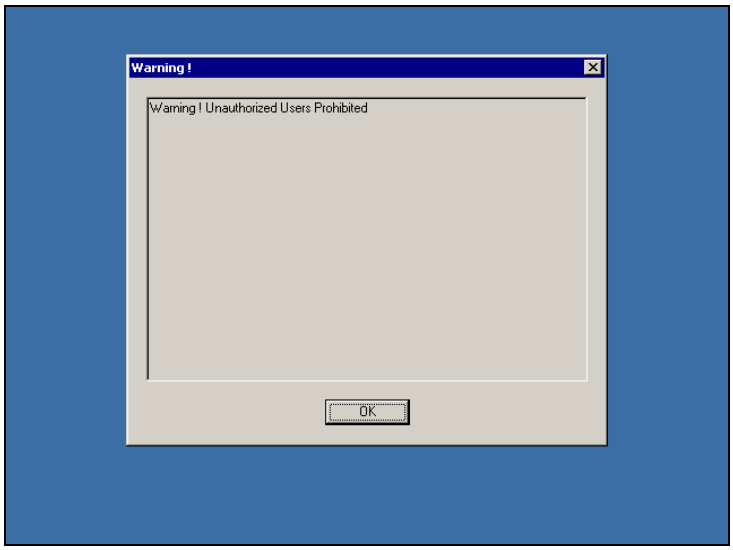




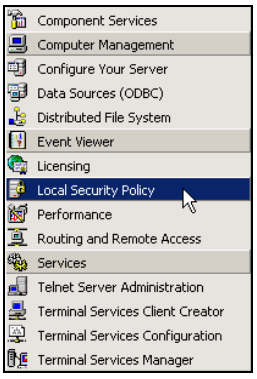
4. This will open the Import Policy From dialog box. In order to import the Storks' Server Security template, you will need to insert the floppy disk that contains the template file that you created earlier. Make sure that you select **Clear this database before importing,** which will clear any policies that may already exist on the GPO (there are none in this case). If you fail to check this box and current policies exist, they will be merged with the settings from the security template. Change the drive letter from C: to **A:**, select the **Storks Server Security** file and click **Open** to import.



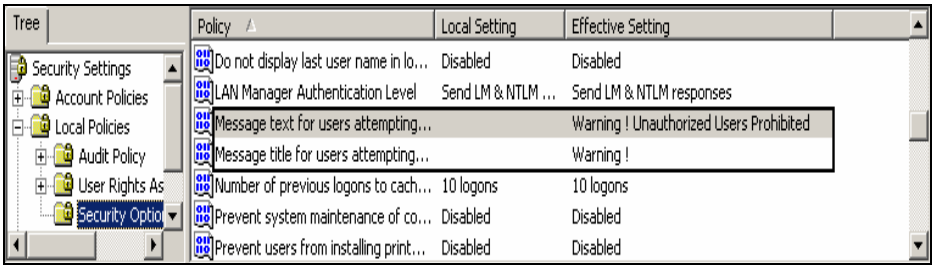
5. After you have imported the Storks' Server Security file to the Servers OU, SA-1 will need to obtain the policy change before any settings will take effect. For all of these settings to take effect you will need to reboot SA-1. **Reboot SA-1**. When SA-1 has rebooted, the message title and text will appear when you try to logon, as shown below.



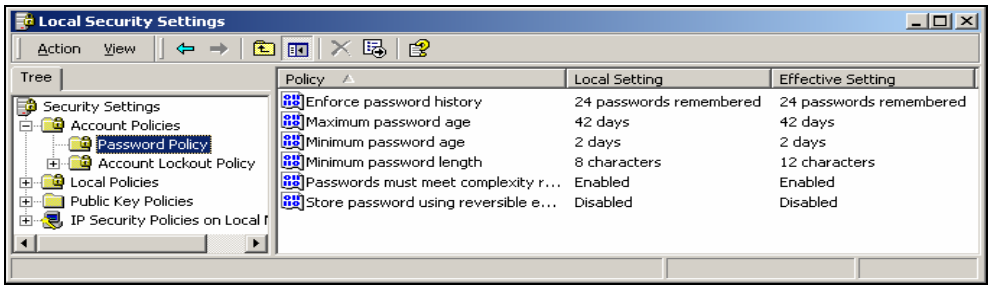
6. Logon to **SA-1**, go to **Start→Programs→Administrative Tools** and click on **Local Security Policy**.



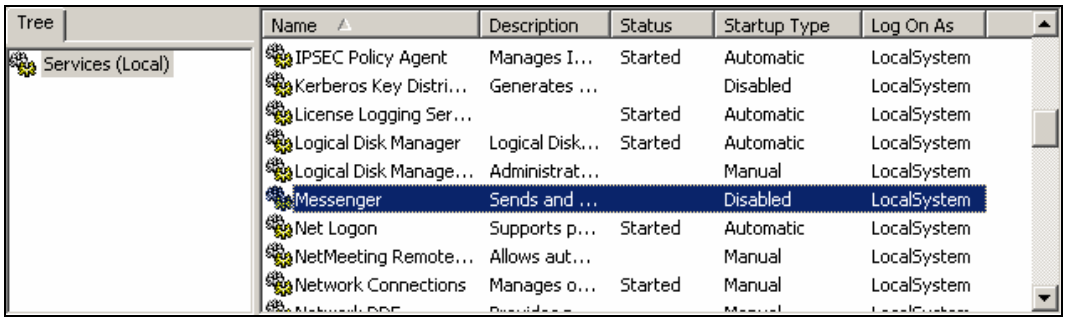
7. Open **Security Settings → Local Policies → Security Options** in the left pane of the local security settings. Notice that there are now effective settings, but no local settings for the logon message text and title. These effective settings are the security settings you applied to the Servers OU earlier in the lab.

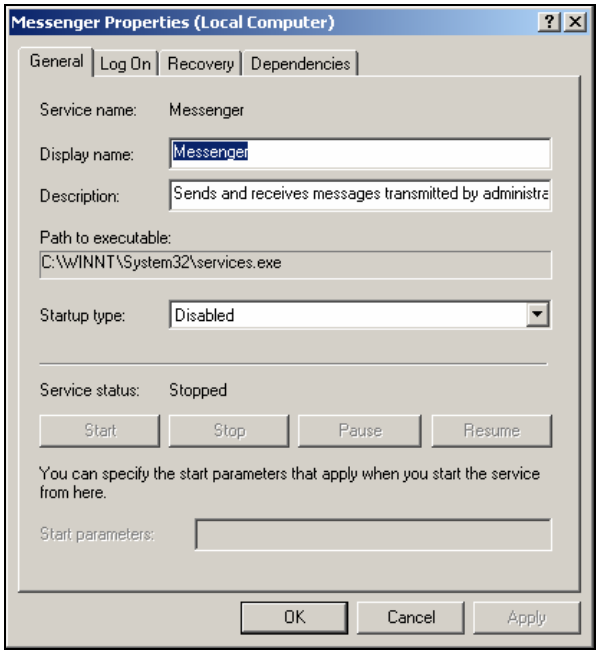


8. Next, open **Account Policies → Password Policies,** also found in Local Security Settings. Notice that the effective setting for the Minimum password length is 12 characters. This effective setting is due to the security setting that was applied to the Servers OU earlier in the lab. However, any settings under the **Account Policies** (i.e. Password Policies and Account Lockout Policies) must be set within a domain level policy for them to take effect on the domain. Therefore, even though the effective setting shows that the policy has taken effect, this setting will **not** actually work. The minimum password setting will be based on the domain GPOs.

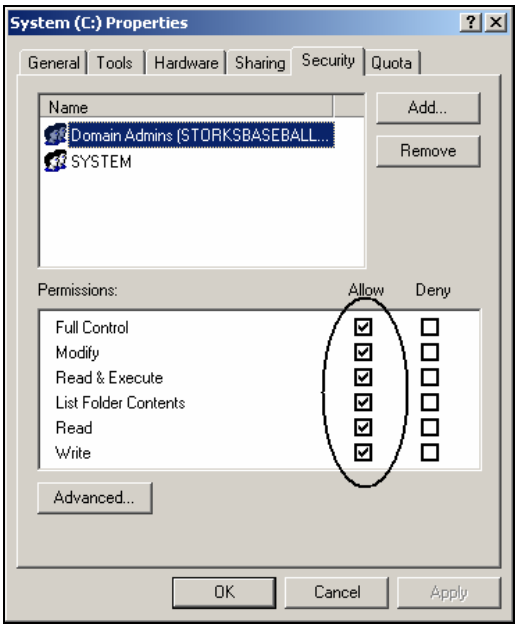


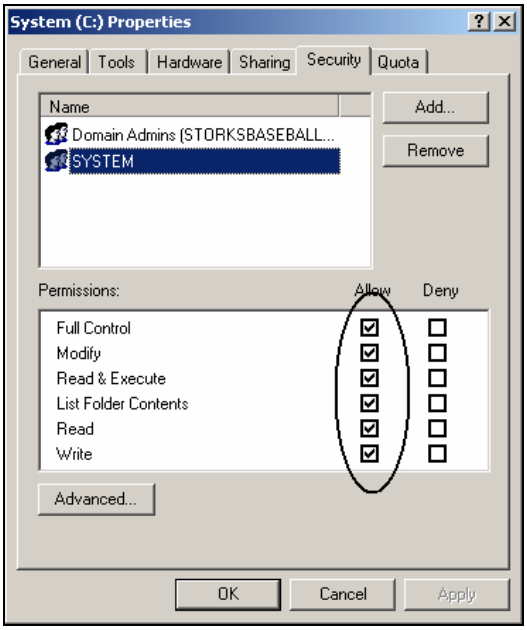
9. Furthermore, verify that the Messenger service has been disabled, by going to **Start→Programs→Administrative Tools** and clicking on **Services**. Double click **Messenger** from the right pane. Note that the Messenger service has been stopped and disabled.





10. Finally, check the NTFS permission settings that you also configured within the security template. Open **Windows Explorer,** right click on the **C:** drive and select **Properties**. On the Properties page, select the **Security** tab. Notice that the Everyone group is removed and both the Domain Admins and System groups are present with Full Control permissions.





Lab 2

Securing the Springfield Storks' Network Using Group Policy

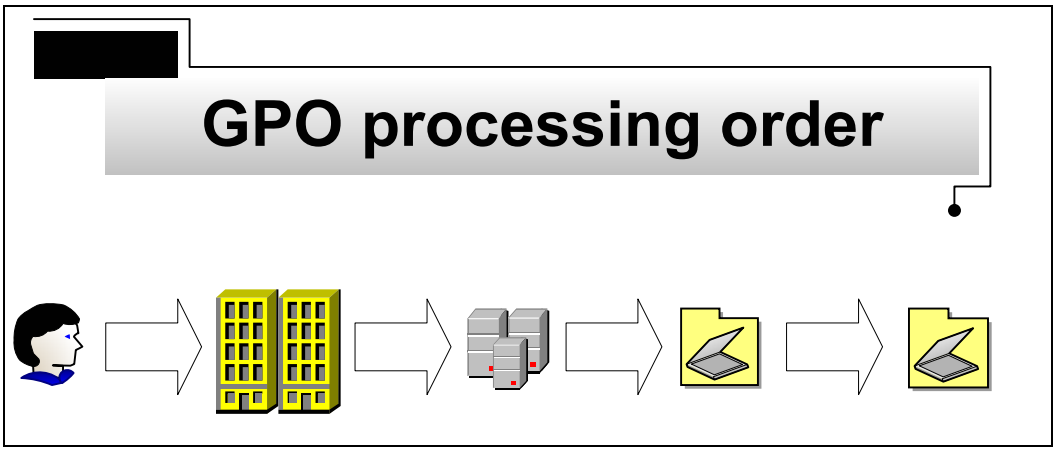
You will learn how to:

- Configure settings in the default domain policy.
- Create and configure new group policy objects
- Assign logon scripts within group policy at the OU level
- Use the LANguard network security scanner

Scenario

Joe, the Storks' network administrator, is happy with the progress that you two have made so far. He now has a good understanding of how to use security templates to establish baseline security on the new workstations and servers that are deployed. However, you are just getting started. Now it's time to get more detailed with security settings and really lock down the Storks' network. Group policy is arguably the best new enhancement to Windows 2000, allowing you to control security across your entire company with the click of the mouse.

In this lab, you will configure group policy within the Storks' Active Directory environment. You will see how to create GPOs and then link them to different containers within the domain. You will set and configure security settings such as NTFS permissions, services, security options, administrative templates, Internet Explorer settings and login scripts that have the potential to affect hundreds or thousands of users through one setting.

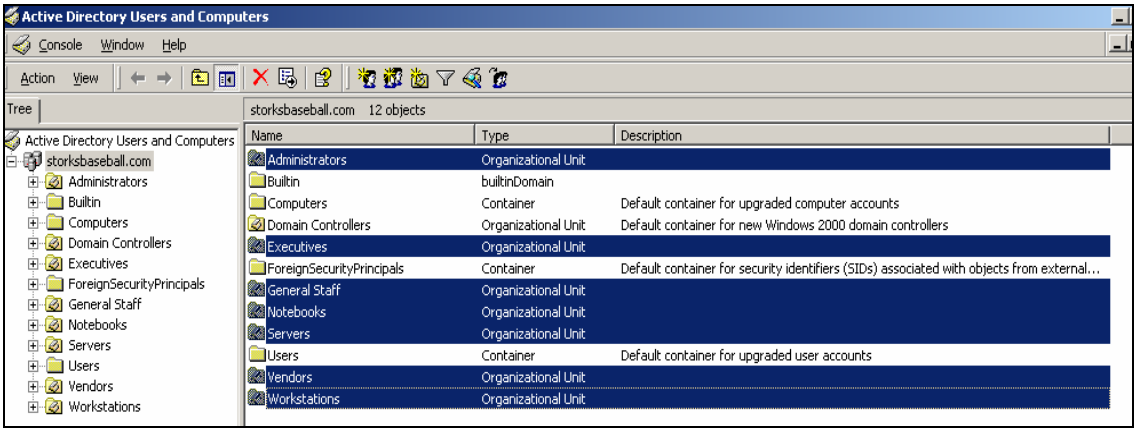


Creating users, OUs and folders

The Storks have decided to create custom OUs for their Servers, Workstations, Notebooks, Vendors, Executives, Administrators, and General Staff. These OUs will help standardize the Storks' network and improve security.

1. **Note:** The Servers OU has already been created in Lab1 and SA-1 was moved to the Servers OU. Use the steps in Lab 1 (Creating a Servers OU) to create the rest of the custom OUs. Also, move **Pro-1** to the Workstations OU.

   After you have completed this task, you should see the following custom OUs in your Active Directory Users and Computers console.

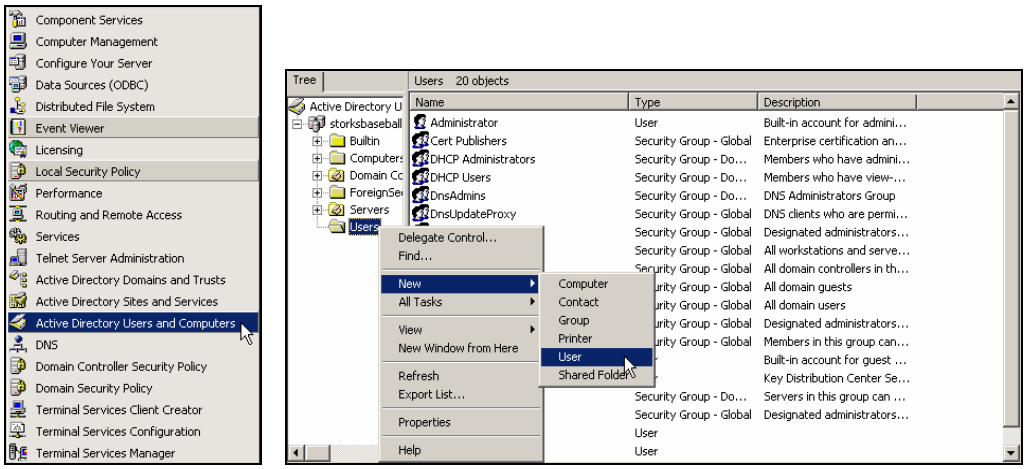


2. Next, create the following users in Active Directory Users and Computers and move them to their appropriate OUs

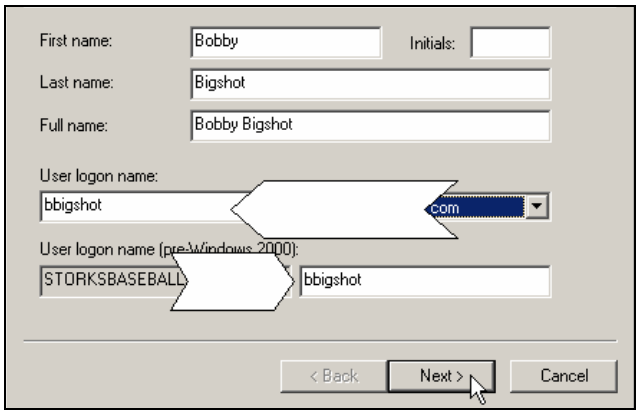
   Note: You can either create the user account directly in the selected OU by right clicking on the **OU** and selecting **New → User** or you can move the user account after it has been created.

First Name	Last Name	Username	Password	OU
Bobby	Bigshot	bbigshot	test	Executives
Rudy	Redhot	rredhot	test	Vendors
Carter	Crackerjack	ccrackerjack	test	Vendors

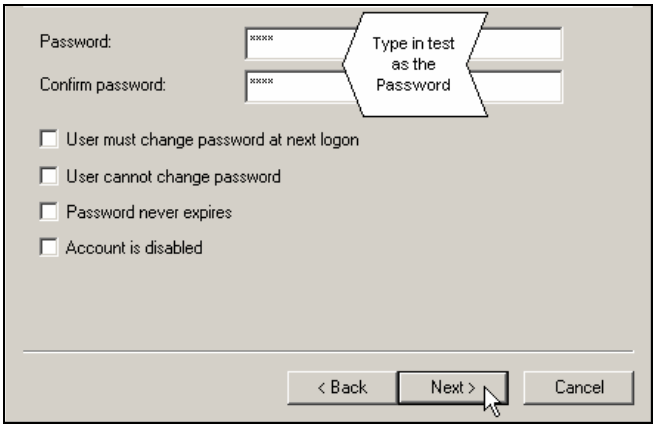
3. To create the user accounts, log on to **DC-1** and open the **Active Directory Users and Computers** tool. Right click on the **Users** container and select **New → User.** You need to create the three users from the table above in the same way by following these steps. If you create the user accounts in the Users container, you will have to manually move them to the correct OU, as specified above.



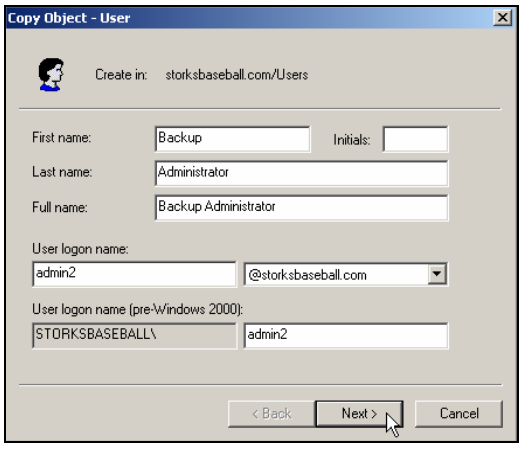
4. Make sure that you supply accurate information from the table above. The following is an example of what your user accounts should look like.

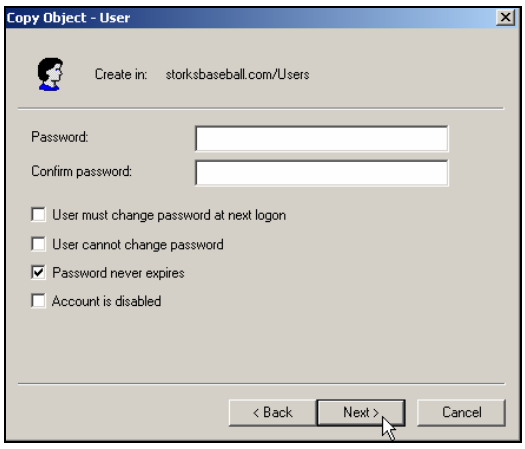


5. Type in the password of **test** for each user. Make sure that "User must change password at next logon" is ***not*** **checked**.

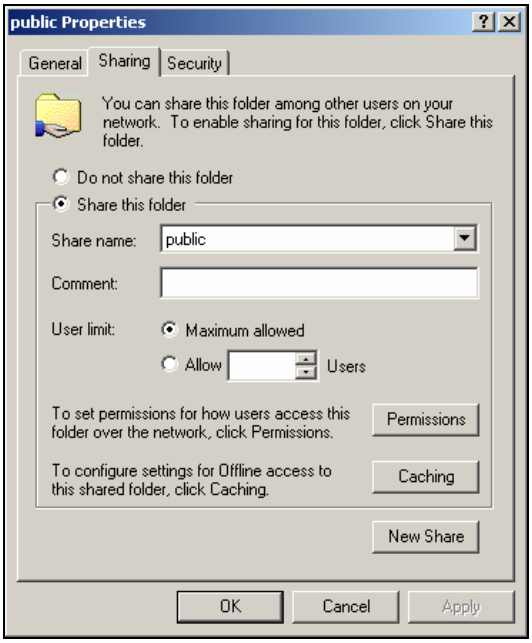


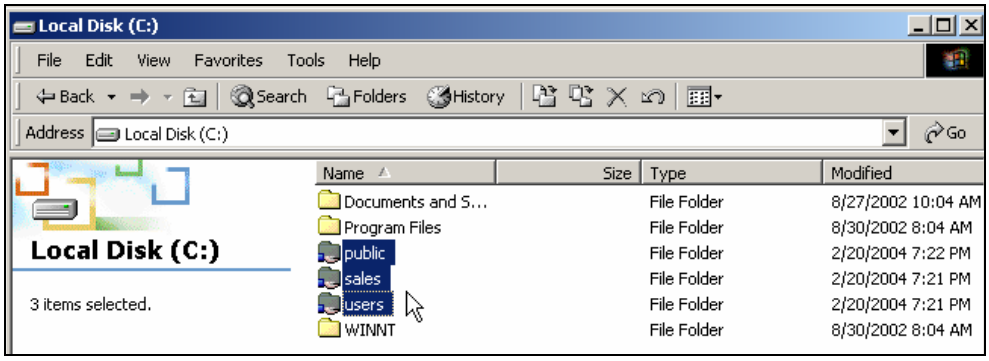
6. For backup purposes (in case you lock yourself out later in this lab), you will need to create a second administrator account and name it **admin2**. To create the account, right click on the **Administrator** (inside the Users container) and click **Copy**. Type in the following information (from the picture below) and click **Next**. Leave the password blank, click **Next** and then **Finish**. Now, move the original **Administrator** account and **admin2** to the Administrators OU.





7. Next, log on to **SA-1** and create the following folders **public**, **users**, and **sales** under the root of the c:\ drive. Share these folders and leave the share name as the folder name. These folders will be used later in the exercise.

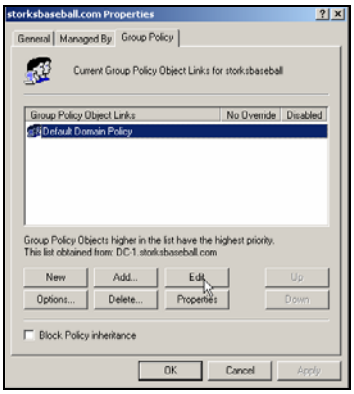




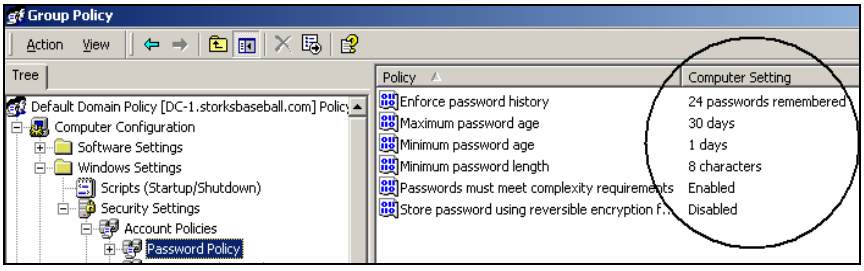
Default Domain Policy Modifications

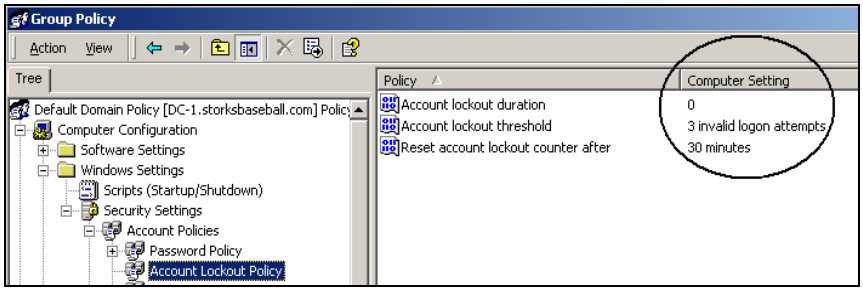
Password Settings and Account Lockout settings for the domain must be set in a domain policy. These settings cannot be deployed individually within policies on Organizational Units or other containers. Therefore, if you want to modify these settings, they must be changed in the default domain policy.

1. Log on to **DC-1** and launch **Active Directory Users and Computers**. Right click on your domain (**storksbaseball.com**) and click **Properties**. Click the **Group Policy** tab, select **Default Domain Policy** and click **Edit**.



2. In Mega Lab 10 secure settings for both the Password Policy and Account Lockout Policy on a local server were discussed. These same settings can be applied to the Storks domain environment in order to increase security. These settings are shown in the diagrams below:



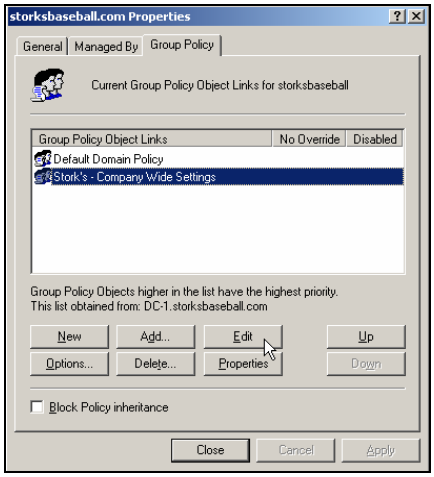


Creating and Configuring a Group Policy Object (GPO)

In the following exercise, you will create a new Group Policy for the Storks. After creating the Group Policy, you will configure various security settings within it to boost security on the Storks' network.

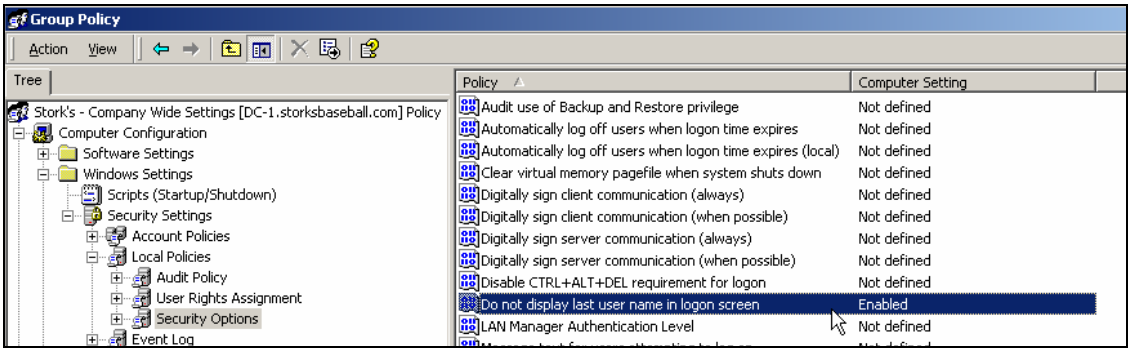
1. From within Active Directory Users and Computers right click on your domain (**storksbaseball.com**) and click **Properties**. Click the **Group Policy** tab and click **New**. Type in **Stork's - Company Wide Settings** for the new policy name and click **Edit**.

   Note: This policy will be applied at the domain level.

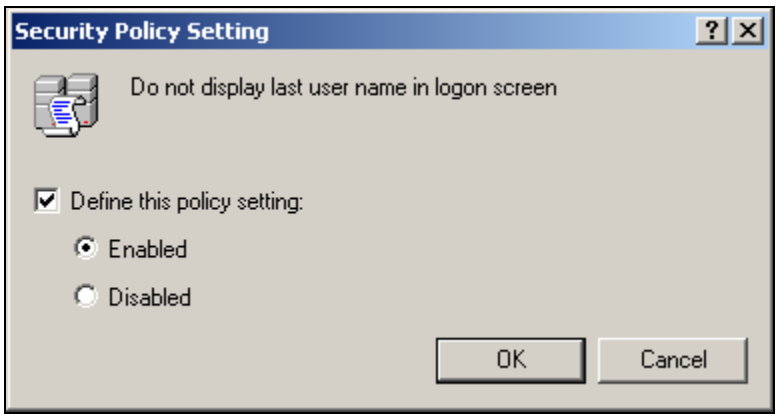


Security Options

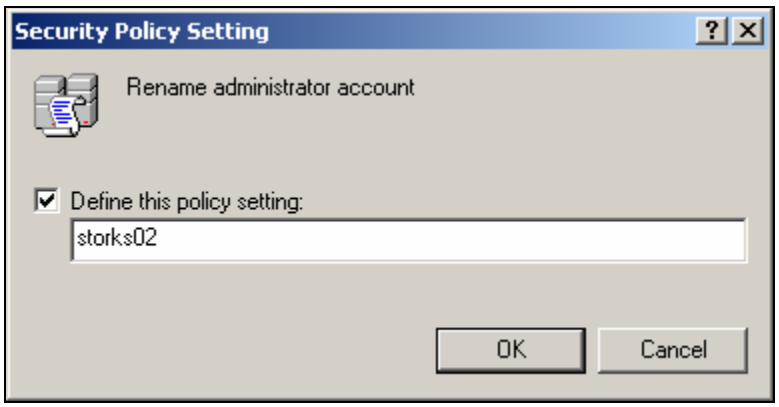
1. Expand **Computer Configuration → Windows Settings → Security Settings → Local Policies** and click **Security Options**. From the right task pane, right click on **Do not display last user name in logon screen** and click **Security**.



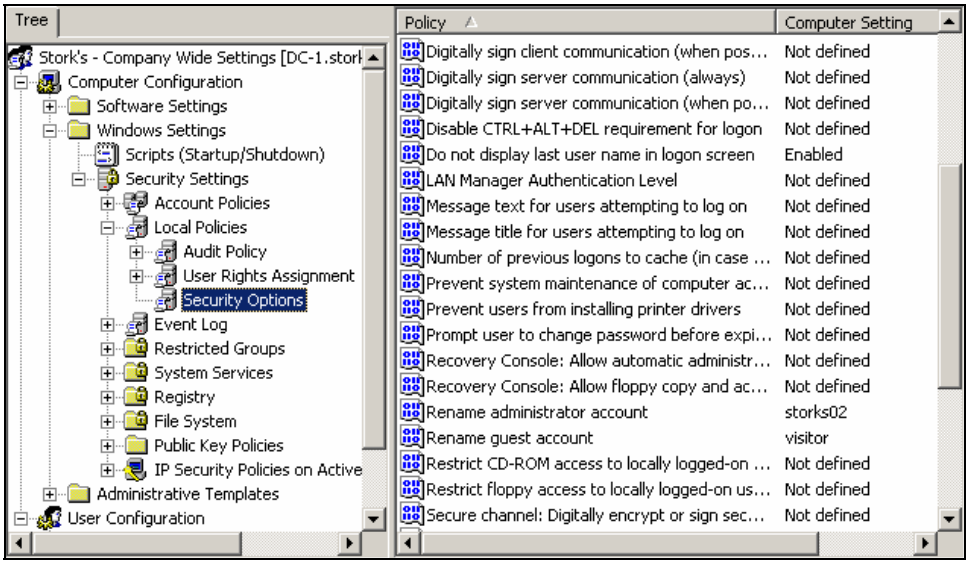
2. Check the box to **Define this policy setting,** select **Enabled** and click **OK**.



3. Within the same Security Options window, right click on **Rename administrator account** and click **Security**. Select **Define this policy setting**, type in **storks02** and click **OK.**



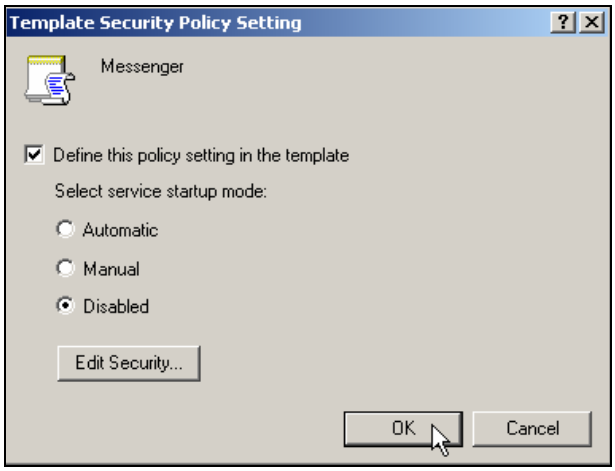
4. Next, select the policy **Rename guest account** and configure it with the name **visitor**. These options will rename the administrator account to storks02 and the guest account to visitor on all of the computers that are part of the storksbaseball.com domain. At this point, you should restart **DC-1** to ensure that all of the changes propagate through Active Directory. **MAKE SURE** that you are sure of your administrator name and password so that you are not locked out once you reboot.



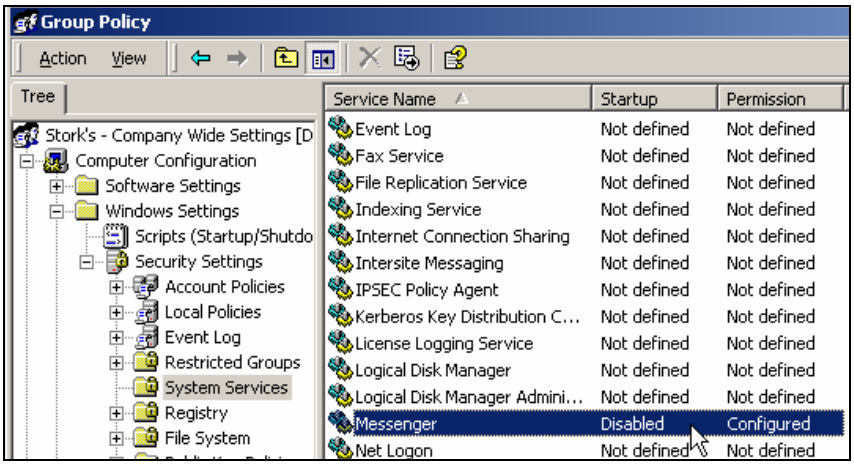
Note: If you do not restart the domain controller (DC-1), you will receive errors on DC-1 because the administrator account you are logged on as has been renamed to storks02. Remember, you can always use the backup administrator account (admin2) if you have problems logging on with the default admin account.

Disabling the Messenger Service

1. Log on to **DC-1** with the Storks02 account and go to **Active Directory Users and Computers**. Right click on your domain (**storksbaseball.com**) and click **Properties**. Click the **Group Policy** tab, select **Stork's - Company Wide Settings** and click **Edit.** Next, expand **Computer Configuration → Windows Settings → Security Settings**, and click on **System Services**. From the right task pane, right click on **Messenger** and click **Security**. Check mark **Define this policy setting in the template** and select **Disabled** from the choices below. Click **OK** to save your changes.



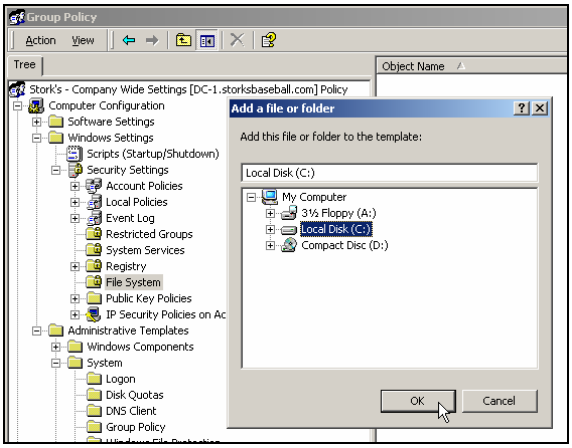
2. Stopping the Messenger service will help to stop unwanted traffic, such as SPAM.



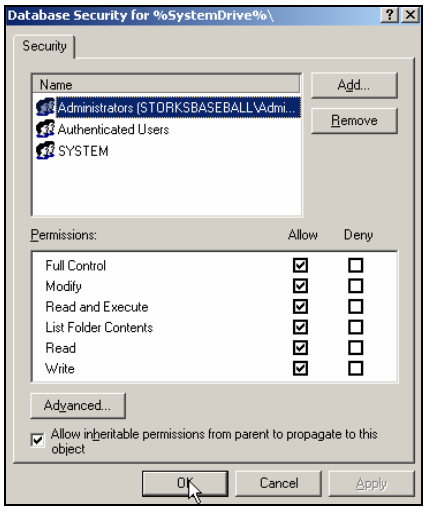
Changing the default NTFS Permissions

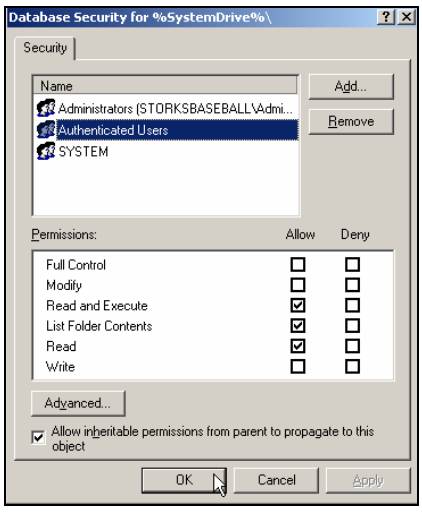
A default installation of Windows 2000 (Pro or Server) grants the Everyone group full control NTFS permissions starting from the root of the c: drive. To increase security on all of the computers on the storksbaseball.com domain, the Storks have decided to modify the default NTFS permissions by using a group policy.

1. From within the Stork's - Company Wide Settings policy, expand **Computer Configuration → Windows Settings → Security Settings** and select **File System**. Right click on **File System** and click **Add File**. Select **Local Disk (C:)** and click **OK**.



2. From the Access Control List (ACL), remove the **Everyone** group and add the **Administrators, Authenticated Users** and **System** groups. Grant **Full Control** to Administrators and System and leave the default permissions (Read and Execute, List Folder Contents, and Read) for the Authenticated Users. Click **OK** to save your changes.



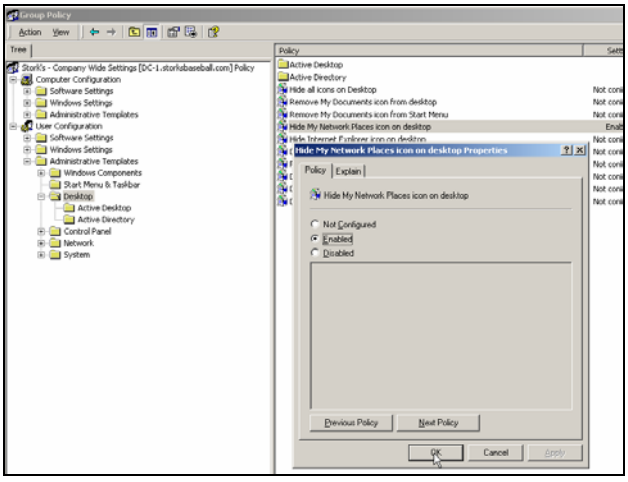


3. Choose the following settings and click **OK**.

Restrict access to My Network Places

To prevent users from browsing your network you have to restrict access to My Network Places. If you allow users to access My Network Places, then the users might be able to explore and access some of the systems on your network that are accidentally not secured. To prevent this problem, the Storks have decided to restrict access to the My Network Places icon for all users within the domain.

1. In the **Stork's - Company Wide Settings** policy, expand **User Configuration** → **Administrative Templates** and click **Desktop**. From the right task pane, right click on the **Hide My Network Places** icon on your desktop and click **Properties**. Select **Enabled** and click **OK.** Reboot **DC-1** to ensure that all of the policies are applied.



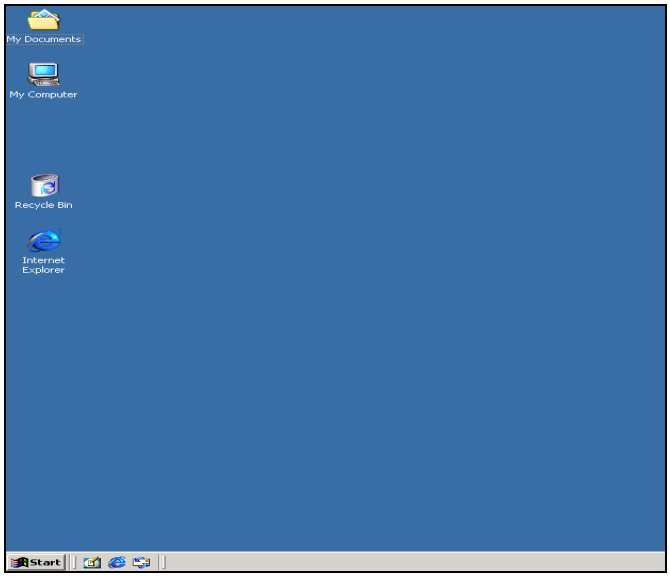
Verifying the Group Policy settings

Before you check to see if your new policies are applied, you will need to restart **Pro-1** and **SA-1**. In the following section, you will be working on Pro-1. To make sure the Group Policy has been applied to SA-1, repeat the same steps on SA-1 to verify the new settings.

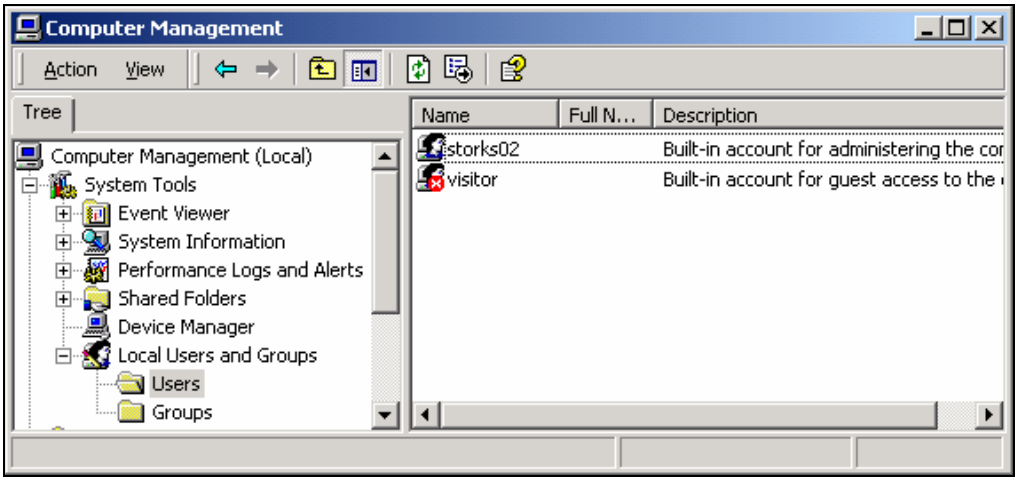
Note: Computer policy (Computer Configuration) settings are applied when a computer boots and the User policy (User Configuration) settings are applied when a user logs on.

1. Go to **Pro-1** and press **Ctrl+Alt+Del**. Note that the User name is blank - this verifies that the Do not display last user name in logon screen option in group policy has been applied to the storksbaseball.com domain. Now log on to the **storksbaseball.com** domain as the administrator, **storks02,** from Pro-1.

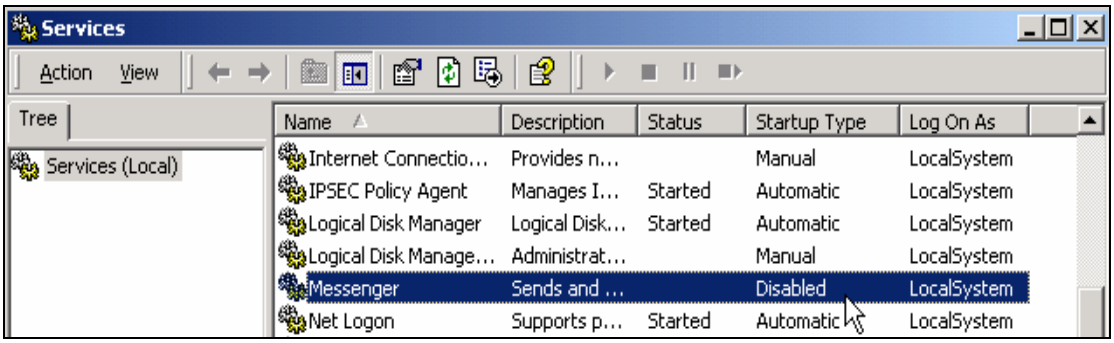
2. Once you have logged on, you will notice that My Network Places has disappeared from the desktop. However, the UNC path can still be used to access resources on the network (i.e. \\sa-1\public).



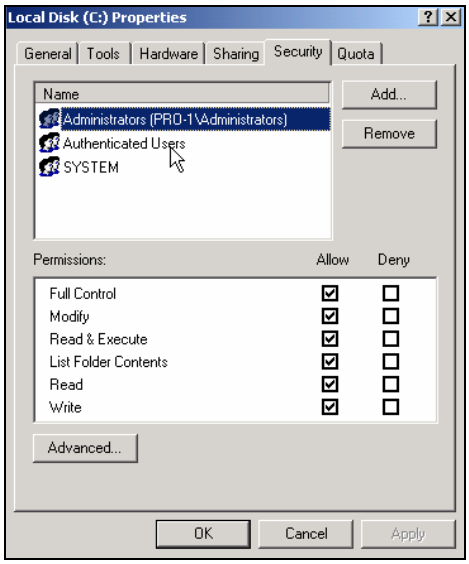
3. To verify that the local administrator and guest account have been renamed, open Computer Management by right clicking on **My Computer** and clicking **Manage**. From the System Tools, expand **Local Users and Groups** and click **Users**. Note that the administrator account has been renamed to **storks02** and the guest account to **visitor**.

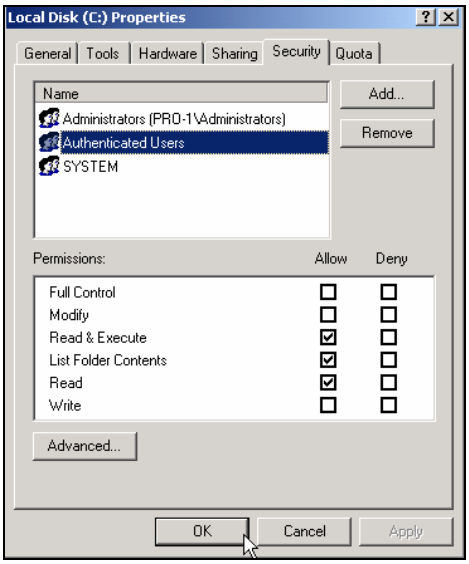


4. To verify that the Messenger service has been disabled, go to **Start → Settings → Control Panel** and double click on **Administrative Tools**. Double click on **Services** and look at the Messenger service. Note that the Messenger service has been stopped and disabled.



5. Finally, go to your desktop and double click on **My Computer**. Right click on the **C:** drive, click **Properties** and click on the **Security** tab. You will notice that the NTFS permissions are set according to the Stork's - Company Wide Settings group policy.

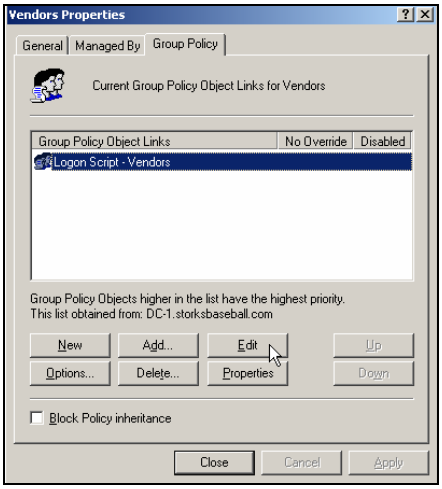




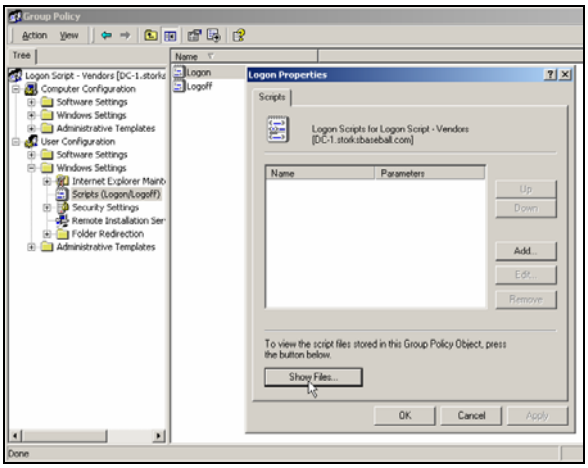
Assigning a Logon Script within Group Policy

In the following exercise, you will need to create a logon script for the Vendors OU. This logon script will map network drives and delete temporary files (.tmp) for the vendors that log on to the Storks' domain. In order to assign a logon script to the Vendors OU, you have to create a GPO on the Vendors OU. Automating these procedures makes the process more secure and efficient.

1. Log on to **DC-1** as **storks02** and launch **Active Directory Users and Computers**. Expand **storksbaseball.com,** right click on the **Vendors** OU**,** click **Properties** and click on the **Group Policy** tab. Click **New,** type in **Logon Script - Vendors** as the policy name and click **Edit** to edit the policy.

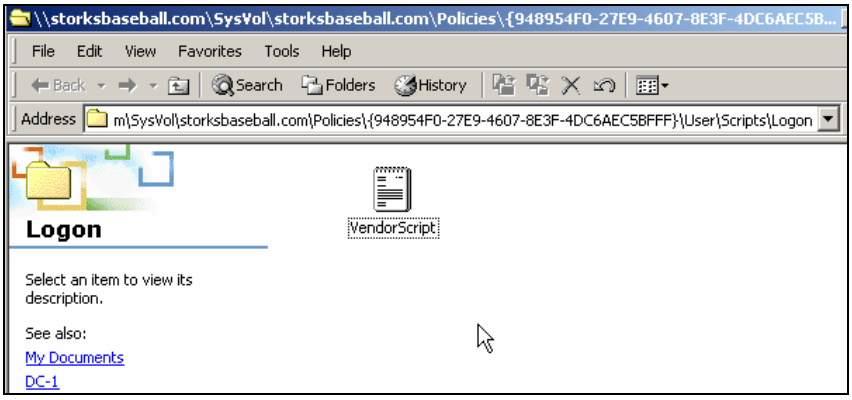


2. Expand **User Configuration → Windows Settings** and select **Scripts (Logon/Logoff)**. From the right task pane, double click on **Logon** and click on **Show Files**.

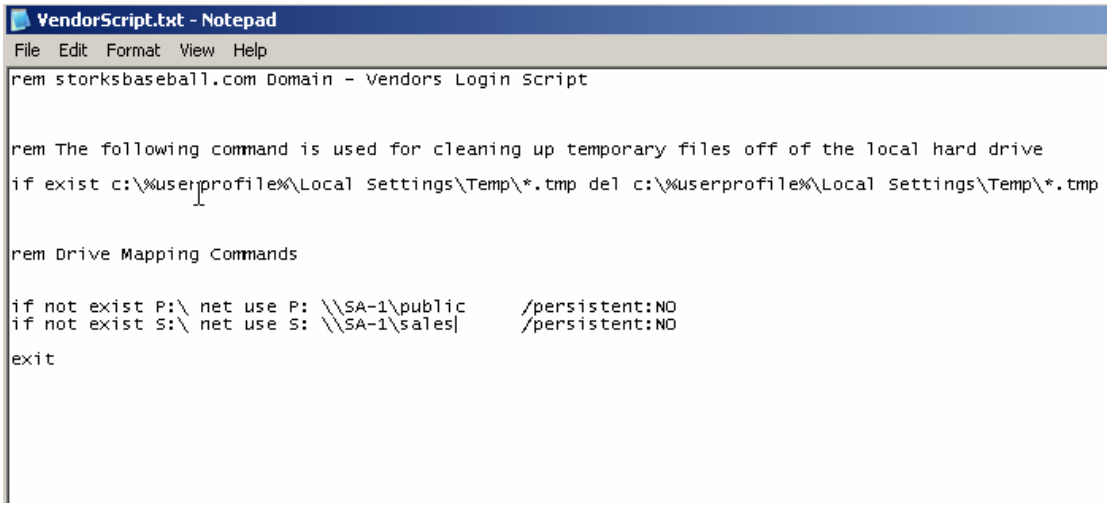


3. Create a new text file inside the Logon folder (the folder that opened when you clicked Show Files) and name it **VendorScript**.

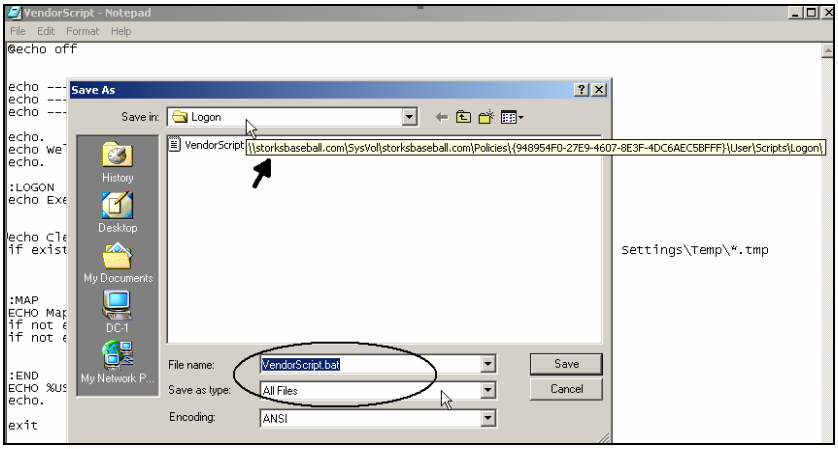
   Note: The location of script file is: \\storksbaseball.com\SysVol\storksbaseball.com\Policies**{948954F0-27E9-4607-8E3F-4DC6AEC5BFFF}**\User\Scripts\Logon, however the bold portion of the path will be different on your system. You can navigate to this location through your file system.



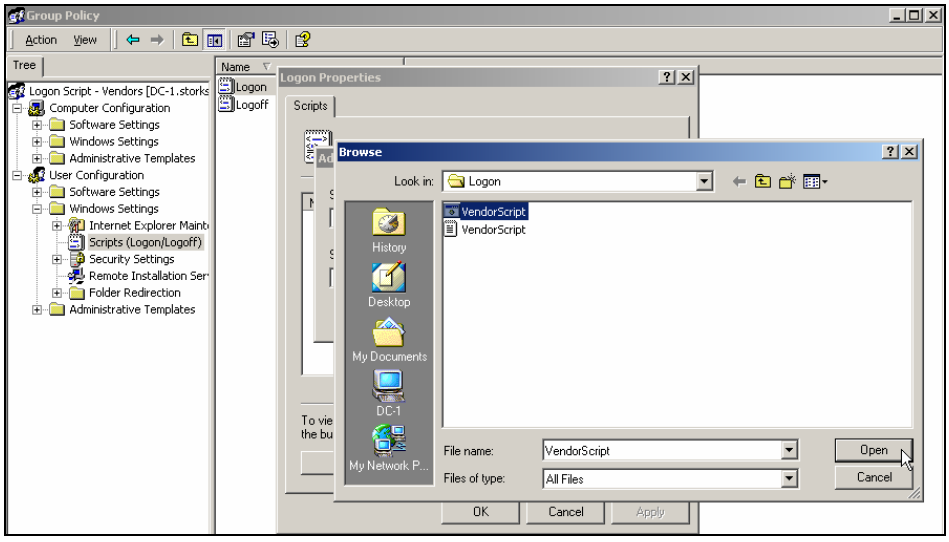
4. Open the VendorScript file and type in the following. Note that the following logon script is only for the Vendors group. You should create different logon scripts for each group that requires unique network drive mappings. Also, if you prefer, this file is available on the CD that came with this course. You should copy this file to the above location and make modifications directly to it.



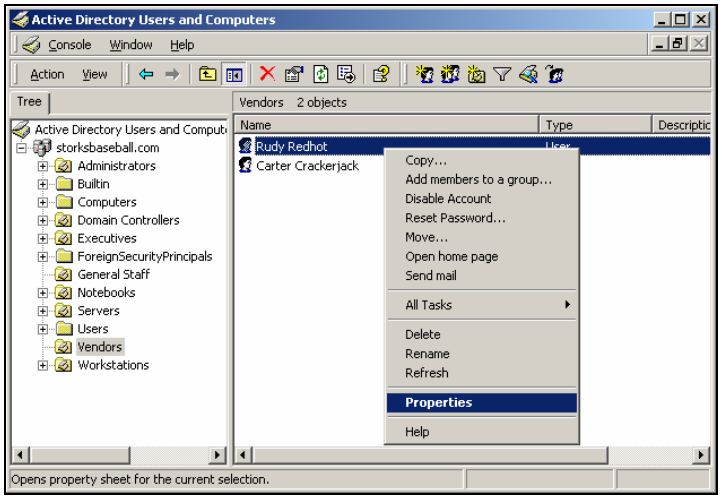
5. When you are finished modifying the file, you must save the file as a batch file (program) by clicking **File → Save As** and then entering in **VendorScript.bat** as the file name. Click **Save**. Close this file and go back to **Vendors Group Policy** console.



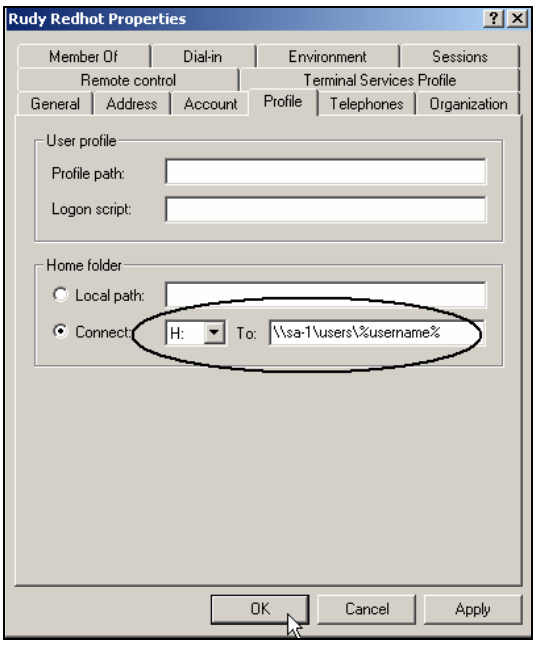
6. On the Logon Properties screen, click **Add** and then click **Browse**. Select **VendorScript** (the batch file not the text file) and click **Open**. Click **OK** twice to go back to the Group Policy console.



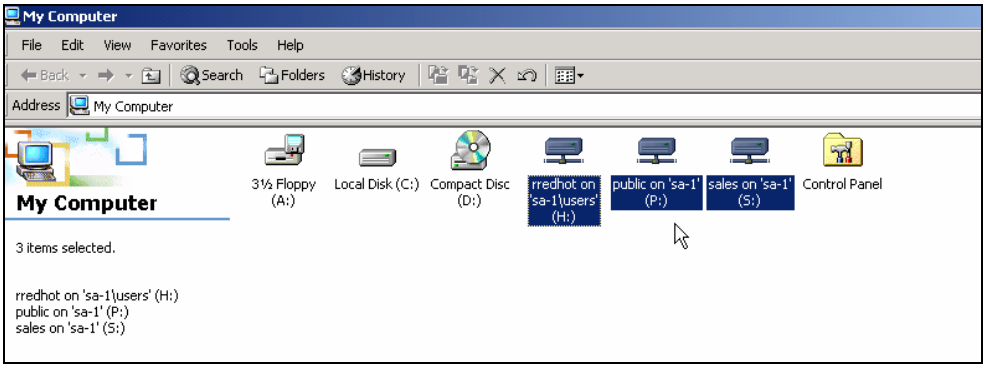
7. Next, go to **Active Directory Users and Computers** and open the **Vendors OU**. Right click on **Rudy Redhot** and click **Properties**.



8. Click on the **Profile** tab and select **Connect**. Change the drive letter to **H,** type in **\\sa-1\users\%username%** in the To: section and click **OK**. This setting will map an H: drive (personal home drive) for Rudy when he logs on to the storksbaseball.com domain. Rudy can use this drive to store his personal data. For security reasons, only Rudy and the Administrators will be able to access this drive.



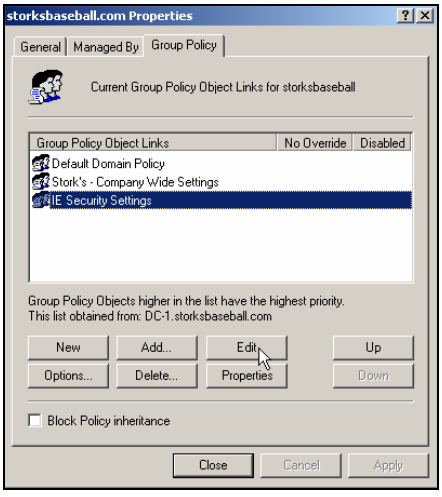
9. From **Pro-1**, log on to the storksbaseball.com domain as **rredhot**. Double click on **My Computer** from the desktop. Along with your normal drives, you should now see that three network drives are mapped for Rudy. When you are finished exploring, logoff Rudy from **Pro-1** and go to **DC-1**.



Securing Internet Explorer on the Storks' network

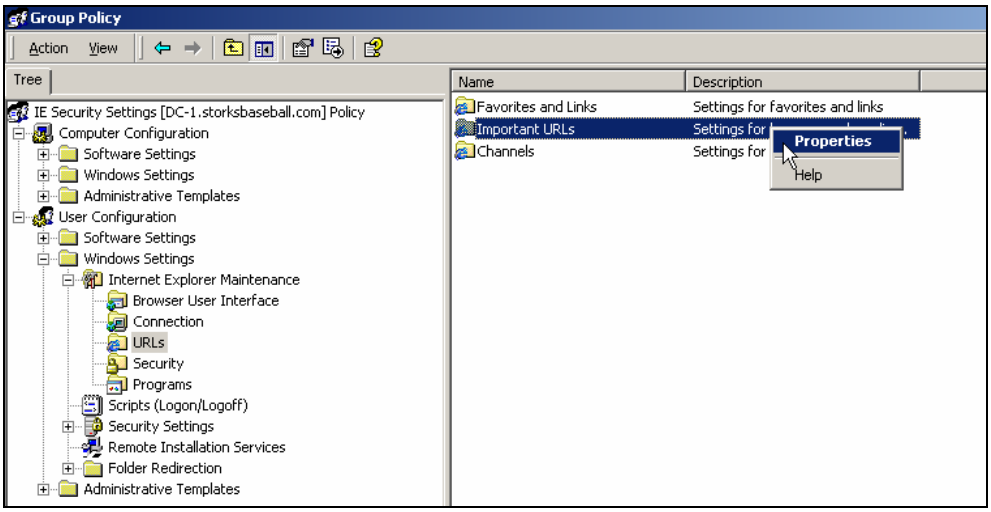
All of the users on the Storks' network use Internet Explorer as their web browser. Because of the recent security breaches, you and Joe have decided to lock down Internet Explorer so that it is more secure. However, instead of visiting each desktop to accomplish this, you will make these configurations with a GPO. To set the Internet Explorer security settings for the Storks' network, you will need to create a new GPO at the domain level in Active Directory. This GPO will be configured to secure Internet Explorer settings on all of the systems on the Storks' network.

1. Log on to **DC-1** as **storks02** and launch **Active Directory Users and Computers**. Right click on **storksbaseball.com** and click **Properties**. Click the **Group Policy** tab, and then click **New**. Type **IE Security Settings** as the policy name and then click **Edit**.

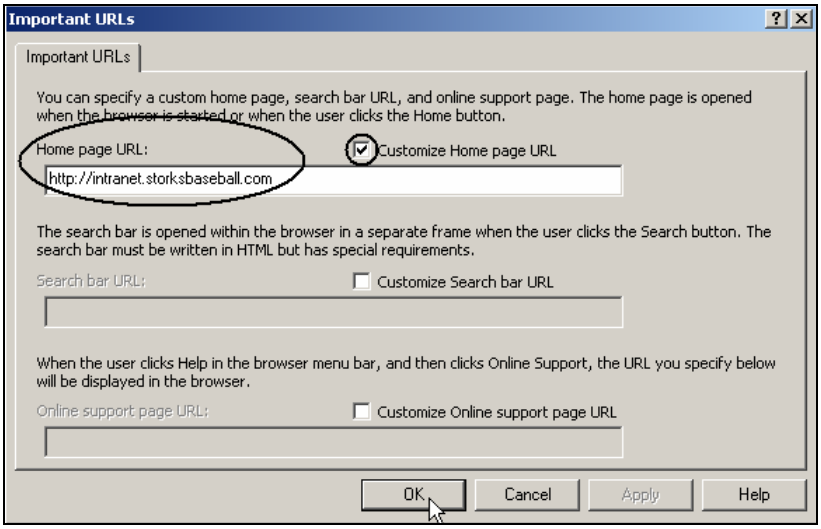


2. The Storks have decided to use their Intranet website as the home page for all of the users on the network. The Intranet website will provide security alerts, awareness and other information related to the Storks' organization.

   To configure this, expand **User Configuration → Windows Settings → Internet Explorer Maintenance** and then click on **URLs**. From the right task pane, right click on **Important URLs** and click **Properties**.

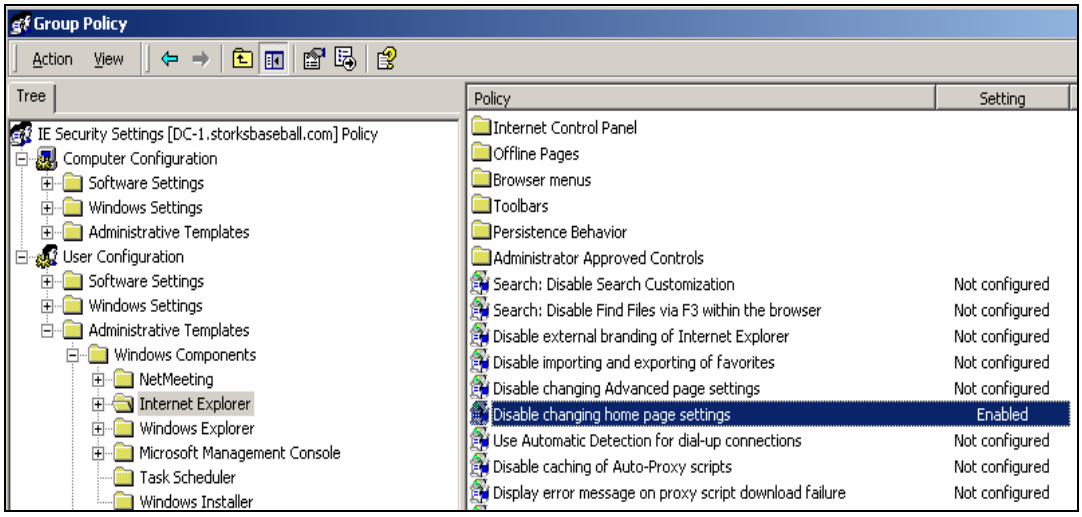


3. Place a check mark next to **Customize Home page URL,** type in: **http://intranet .storksbaseball.com** in the text box as the Home page and click **OK**. This will set the Storks' Intranet website as the default home page for all users. Keep in mind that we have not configured a website on the Storks' network, so this page will not come up.



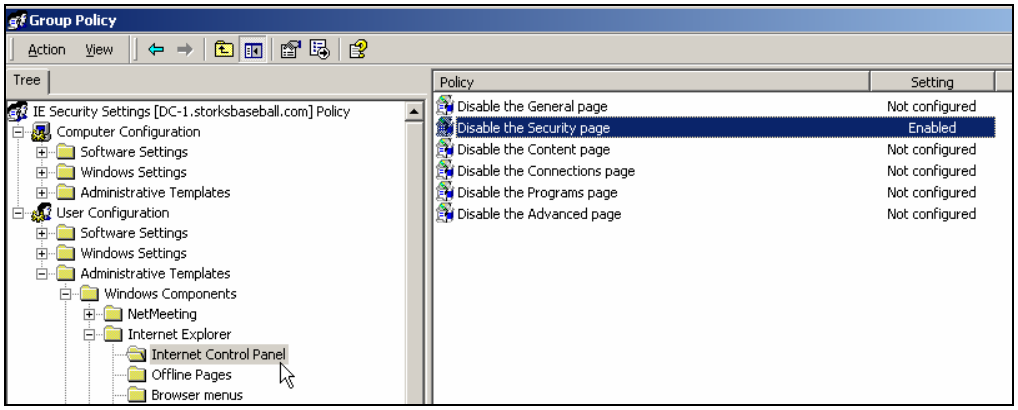
4. Next, you will disable the users ability to change their home page settings within Internet Explorer.

   Expand **User Configuration → Administrative Templates → Windows Components** and then click on **Internet Explorer**. From the right task pane, right click on **Disable changing home page settings** and click **Properties**. Select **Enabled** and then click **OK**.

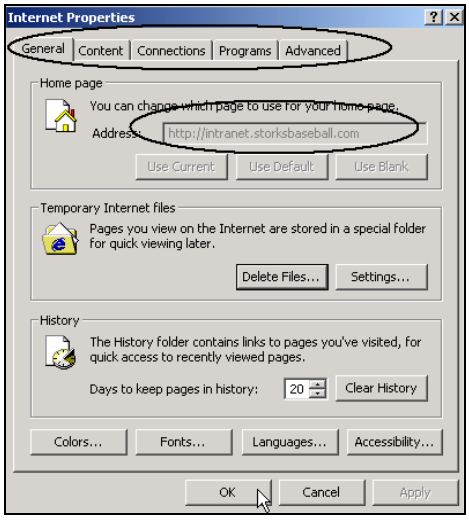


5. Joe, the Storks' administrator, is also concerned with users seeing and changing the settings for security zones, such as scripting, download and user authentication. You will need to hide the Security page on Internet Options to prevent users from seeing and changing these settings.

   Expand **User Configuration → Administrative Templates → Windows Components → Internet Explorer** and then click on **Internet Control Panel**. From the right task pane, right click on **Disable the Security page** and click **Properties**. Select **Enabled** and then click **OK**.



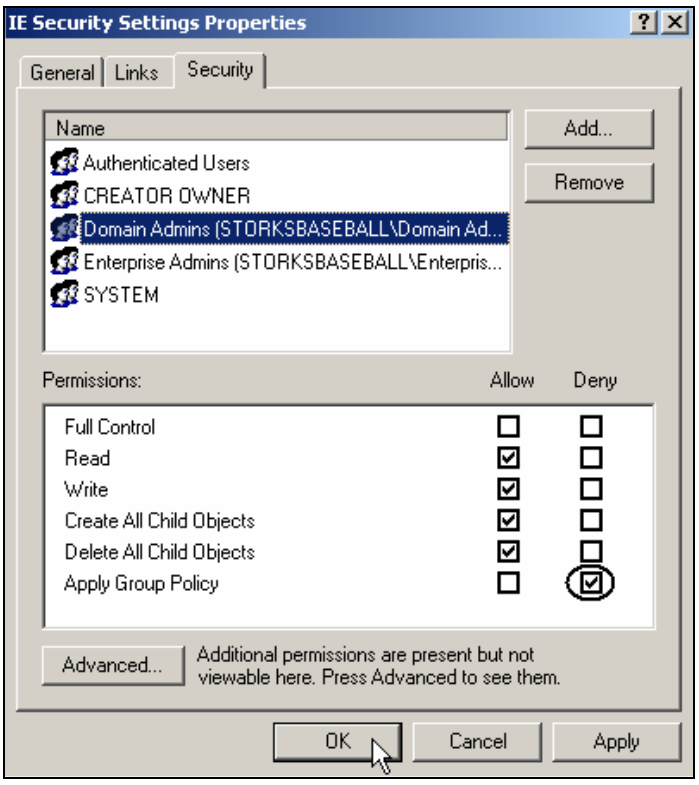
6. To test these settings, from **Pro-1**, log on to the storksbaseball.com domain as **rredhot.** Right click on **Internet Explorer** and click **Properties**. Notice, that the home page is set to http://intranet.storksbaseball.com and the address is grayed out (users cannot change the home page). Also, the Security tab is hidden so the users cannot see or change any of these security settings.



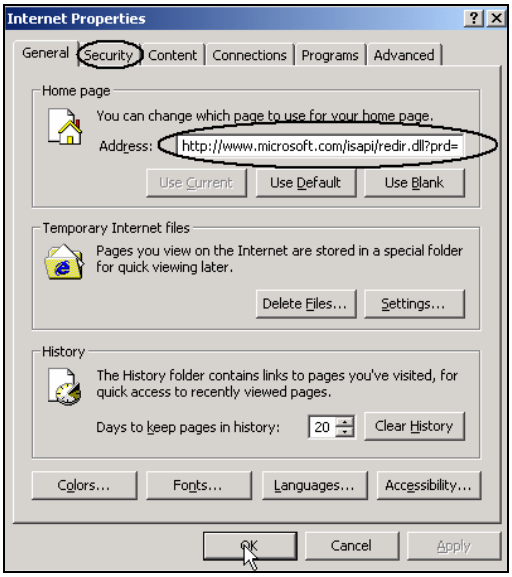
7. Now, from **Pro-1**, log on to the storksbaseball.com domain as **storks02** and go to the **Internet Properties**. You will notice that you cannot change the home page or see the security tab even though you are logged on as administrator. To prevent this group policy from applying to the domain admins group, you have to filter out the domain admins group with permissions so that the Group Policy Object settings do not apply to them. Logoff **Pro-1**.

   When a group policy is first configured it applies to everybody in the domain (via the authenticated users group). One way of preventing the policy from applying to certain groups is to assign **deny** for the **apply group policy** permission. This setting prevents the policy from applying to the particular user or group that is denied the permission.

   Log on to **DC-1** as **storks02,** and launch **Active Directory Users and Computers**. Right click on **storksbaseball.com** and click **Properties**. Click the **Group Policy** tab, select **IE Security Settings** and click **Properties**. Click on the **Security** tab, select **Domain Admins** and check **Deny** to Apply Group Policy. Click **OK,** click **Yes** when you receive the caution message and then click **OK** to go back to the group policy.



8. Once again, log on to the storksbaseball.com domain as **storks02** from **Pro-1** and go to the **Internet Properties**. Notice that after filtering out the domain admins group from the IE Security Settings policy, storks02 (domain admin) is now able to change the Address of the home page and the Security settings. Basically, the IE Security Settings group policy no longer applies to the domain admins group.

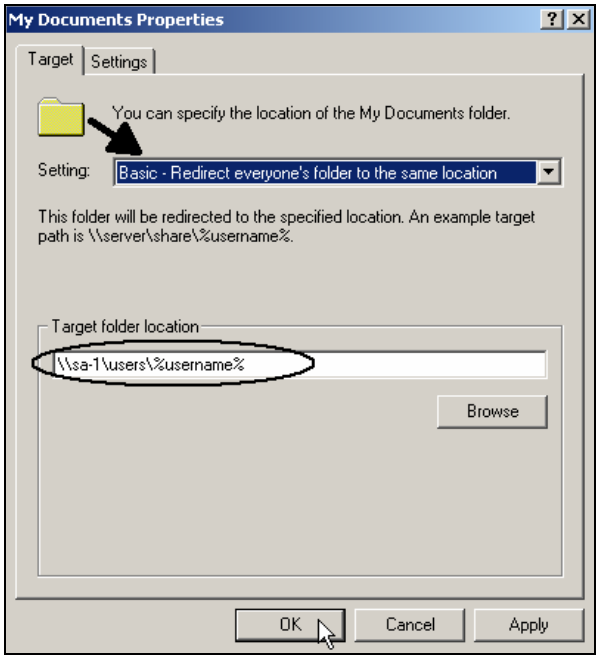


Folder Redirection

In Windows 2000 the administrator has the ability to redirect folders so that they appear to the users as a local folder, while they are actually redirected to a more secure location on a network server. The Storks' administrator, Joe, has decided to redirect all of the users' My Documents folders to their home drive (mapped as "H" earlier in this lab). This will store their documents on the network server (home drive), whenever they save information to their My Documents folder. It is always a good idea to save data on a server because it is backed up more regularly and is more reliable than a normal desktop PC.

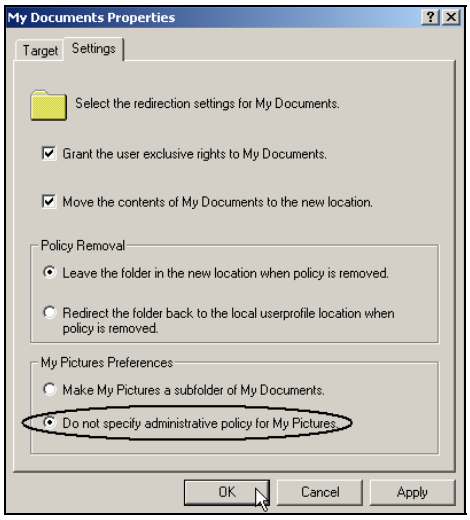
1. Go to **DC-1** and launch **Active Directory Users and Computers**. Right click on your domain (**storksbaseball.com**) and click **Properties**. Click the **Group Policy** tab, select **Default Domain Policy** and click **Edit**. Expand **User Configuration → Windows Settings → Folder Redirection** and then click on **My Documents**. Right click on **My Documents** and click **Properties**. From the drop down menu, select **Basic - Redirect everyone's folder to the same location** and type in **\\sa-1\users\%username%** under Target folder location.

   Note: The path for Target folder location is the same as the Storks' users home drive. All users should have home drives setup similar to Rudy Redhot shown earlier in this lab. The variable %username% will automatically create a folder (or create a path) to the currently logged on user.

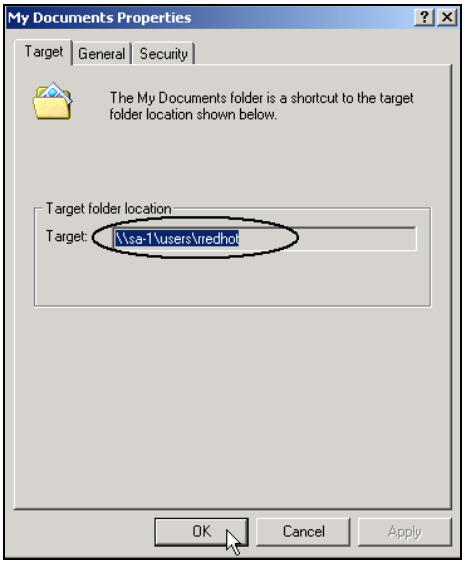


2. Joe also wants to prevent users from storing pictures on the network. To accomplish this, you will have to set an option to leave the My Pictures folder on the local computer. If you do not set this option, pictures that users save in the My Pictures folder will be saved on the network, which can take up a lot of disk space.

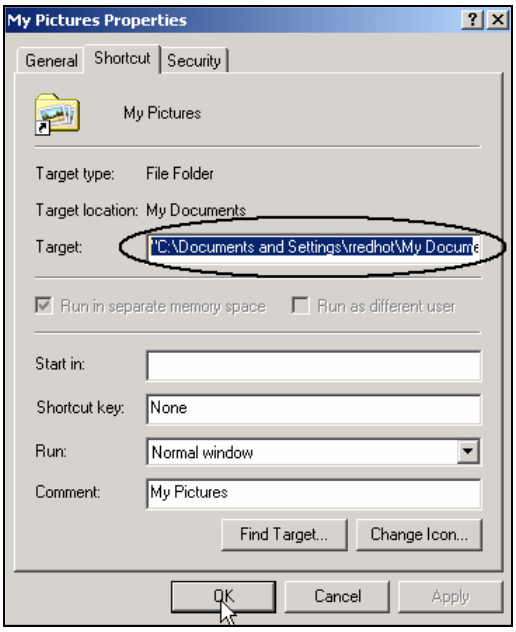
   Click on the **Settings** tab and select **Do not specify administrative policy for My Pictures**. Click **Apply** and then click **OK**.



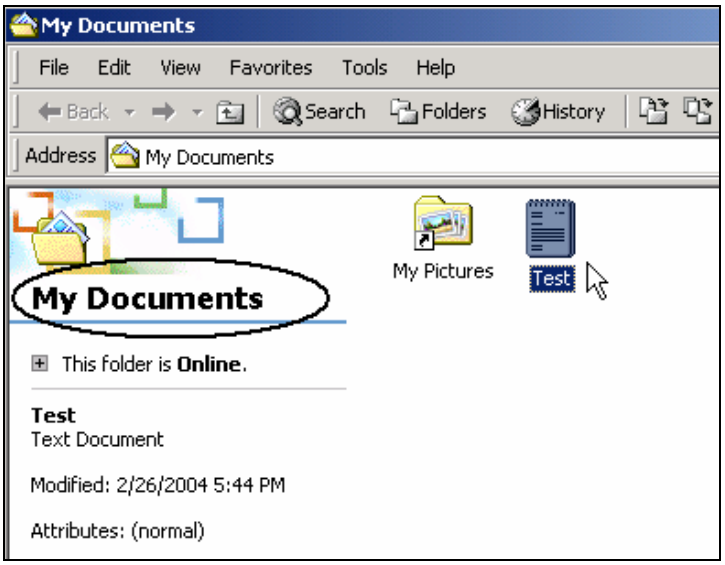
3. Log on to the storksbaseball.com domain as **rredhot** from **Pro-1**. Right click on the **My Documents** folder and click **Properties**. Note that the target folder location is pointing to Rudy's home drive. Click **OK** to go back to the desktop.



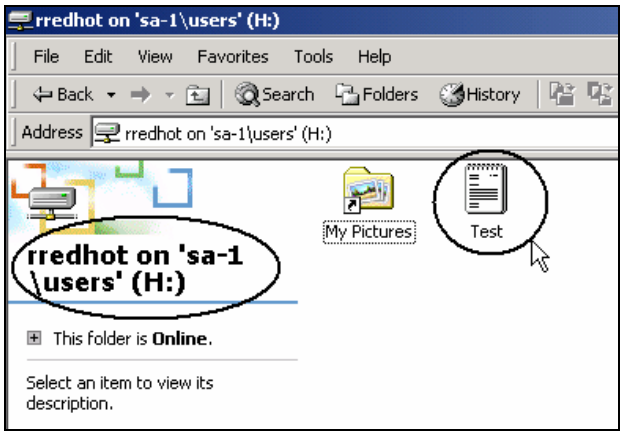
4. Next, double click on the **My Documents** folder. Right click on **My Pictures** and then click **Properties**. Notice that the Target: is set to C:\Documents and Settings\rredhot\My Documents\My Pictures. Pictures will be saved locally. Click **OK** to go back to the My Documents folder.



5. Create a text file called **Test** inside the My Documents folder and close the folder.



6. Next, open **My Computer** and double click the **H: drive** (rredhot on 'sa-1\users'). The text file (Test) that you created inside the My Documents folder is also on your home drive. Basically, the My Documents folder and the H: drive (home drive) are the exact same thing.



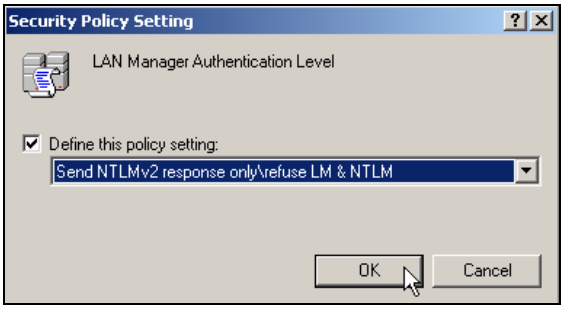
Authentication Protocols

Authentication protocols are used during the network authentication process between two computers. They basically ensure that users and servers are who they claim to be. The following table describes four authentication protocols used in Microsoft operating systems.

Types of Authentication Protocols	
LM	Default for Windows 95 and 98. Weakest of the Authentication Protocols in this list. The password protection method can easily be cracked.
NTLM	Default for NT 4.0. Authentication is slower than Kerberos. Performs only one-way authentication. Not compatible with non-Microsoft networks.
NTLMv2	Can configure Windows 95, 98, and NT 4.0 to use NTLMv2. Unique session key per connection. Not as secured as Kerberos, but more secured than LM & NTLM. Used in Windows 2000.
Kerberos	Used in Windows 2000 and later. Also used for Unix authentication. More secure than NTLM. Uses Mutual Authentication so both users and server are authenticated.

The Storks have decided to use the NTLM v2 authentication protocol on their network in addition to Kerberos. Kerberos will work between the Windows 2000 computers but NTLM is required to support legacy clients running Windows 98 and NT 4.0. These systems will have to be updated to support NTLM v2

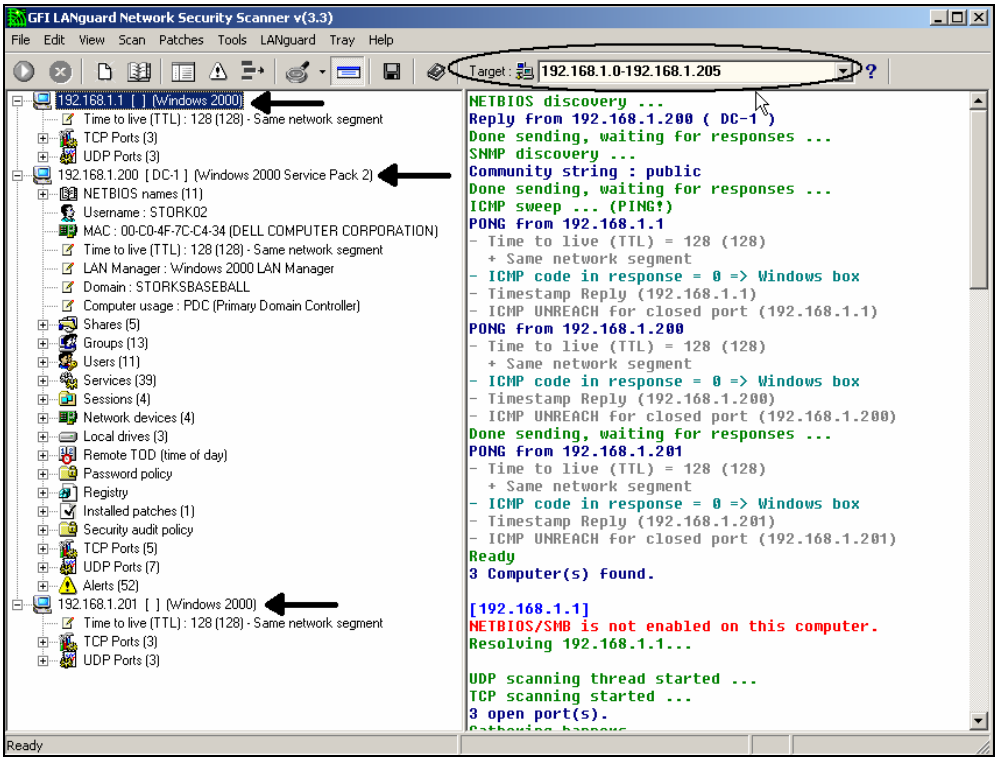
1. To define the NTLMv2 Authentication level, launch **Active Directory Users and Computers** on **DC-1**. Expand **storksbaseball.com**, right click on the **Domain Controllers** OU and click **Properties**. Click the **Group Policy** tab, select **Default Domain Controllers Policy** and click **Edit**. Expand **Computer Configuration → Windows Settings → Security Settings → Local Policies** and click on **Security Options**. From the right task pane, right click on **LAN Manager Authentication level** and click **Security**. Place a check mark next to **Define this policy setting**, select **Send NTLMv2 response only\refuse LM & NTLM** and click **OK**.



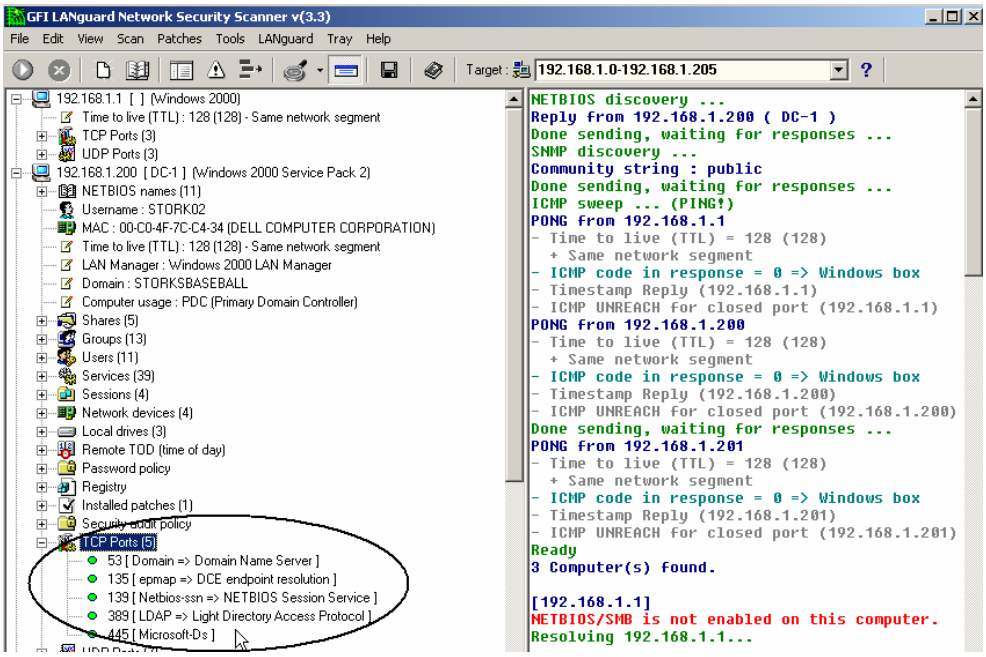
LANguard Network Security Scanner

The Storks have decided to use the LANguard Network Scanner tool to scan their network for security holes. By analyzing the operating system and the applications running on the Storks' network, it will identify possible security holes if they exist. At the time of writing, you can download an evaluation copy of GFI LANguard for non-commercial use from their website at **http://www.gfi.com**. Look for the product by name once you reach their website.

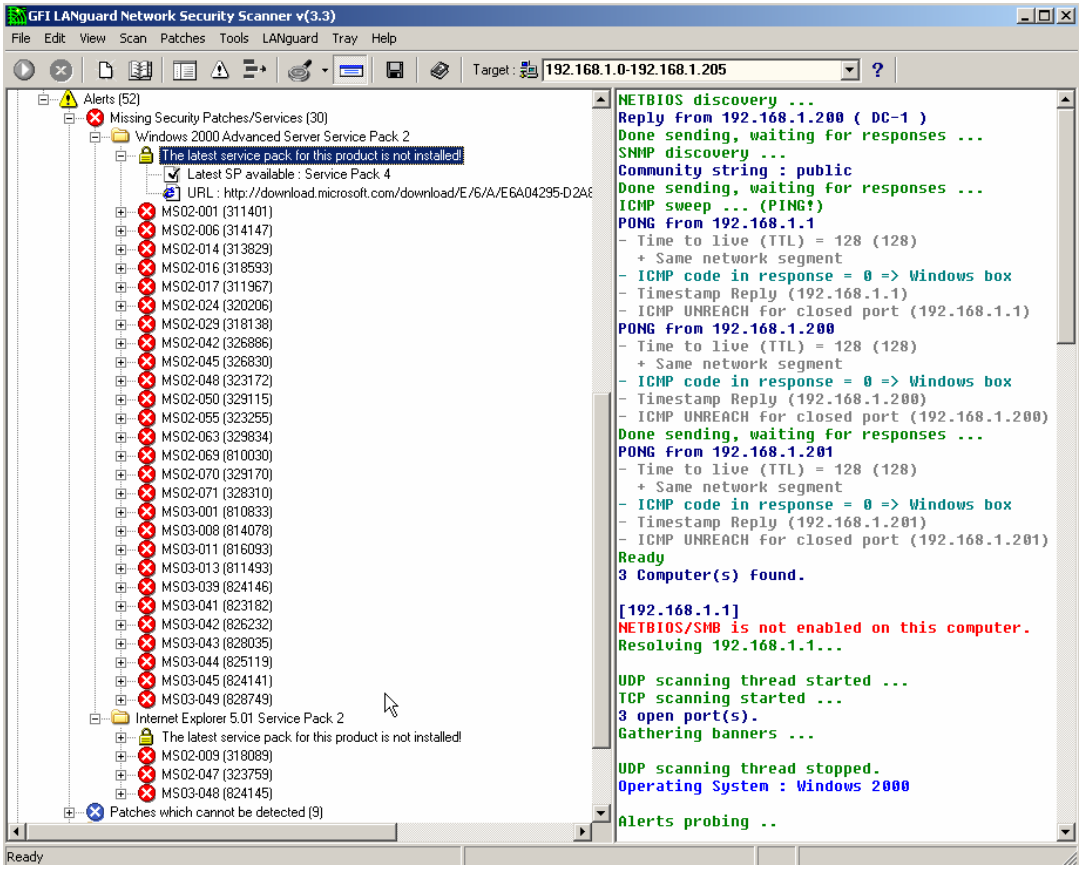
1. Install **LANguard** on **DC-1**. After LANguard is installed, launch it, type in **192.168.1.0-192.168.1.205** and hit **Enter** to scan the computers within this IP range. You will notice that 3 computers are found (DC-1, SA-1 and Pro-1) within the IP range you provided.



2. Expand the **TCP Ports** for **192.168.1.200** (DC-1) and notice that there are 5 TCP Ports open on this server. These ports were opened by the system and they should be kept open in order for your Domain Controller to function properly on the network. However, if you see some other ports (21 (FTP), 23 (Telnet), 25 (SMTP), 80 (HTTP), 110 (POP3), etc) that are open and you are not using the service linked to the port, then you should consider closing the port.



3. Next, expand **Alerts** for DC-1 and notice that Service Pack 4 (the latest service pack) for Windows 2000 Advanced Server is not installed on this system along with other security patches. Also, Internet Explorer is missing the latest service pack and security patches. It is very important to keep your system updated by using Windows Update to protect your system from malicious viruses and hackers.



Lab 3

Installing and Configuring Software Update Services (SUS)

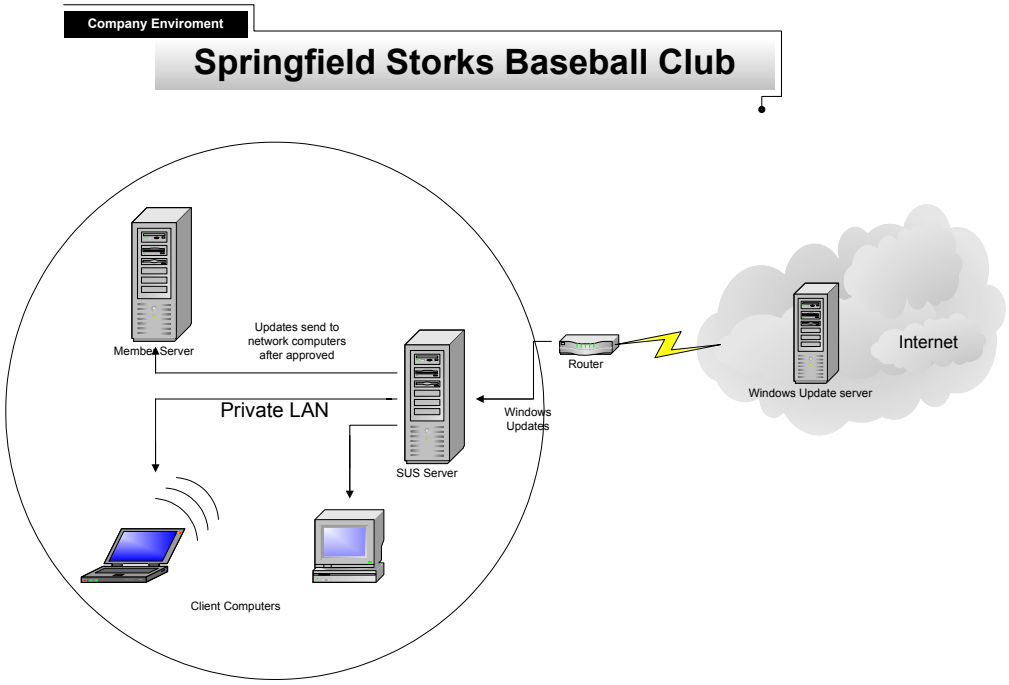
You will learn how to:

- Install Software Update Services (SUS)
- Synchronize the SUS Server
- Approve updates on a Software Update Services Server
- Install the Automatic Updates Client
- Configure Automatic Updates Client and install updates

Scenario

Keeping servers and workstations up to date is essential for better network security. In a small network, running Windows Update on individual systems is adequate. But, as an environment starts to grow, performing these tasks can become very time consuming. Joe, the Storks' network administrator, is currently required to analyze and update each computer individually. You recommend to him that he try the free utility Software Update Services (SUS) from Microsoft. You explain that SUS will download and manage Service Packs and updates for Windows 2000, Server 2003 and XP. The SUS server will download the updates and the clients will update themselves once Joe has approved the updates for distribution.

In this lab, you will install and configure Software Update Services on DC-1. DC-1 will download all of the updates and then distribute them to the Windows Update Clients.



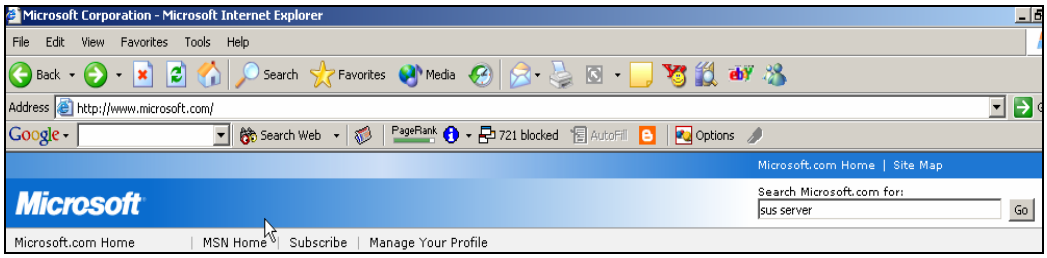
Software Update Services

An Internet connection for DC-1 is required before you can start this portion of lab. Before you install SUS on DC-1, you will need to have the following on your computer:

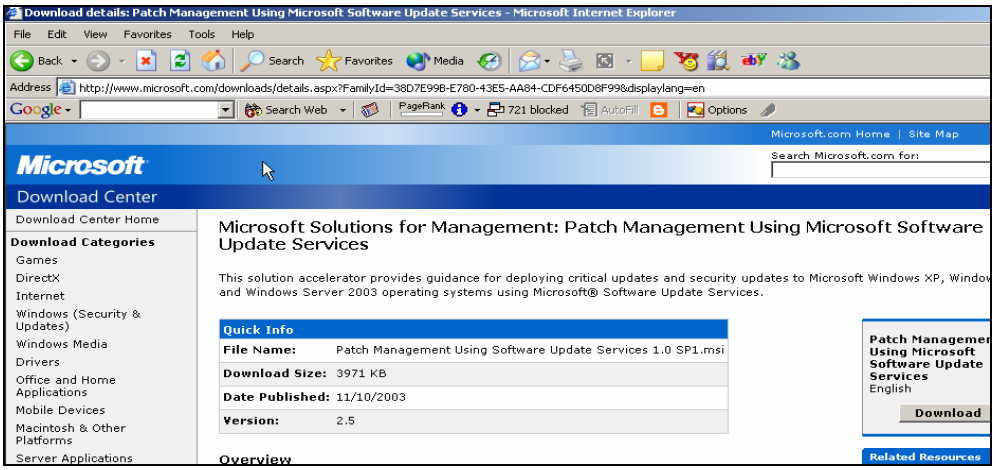
1. Windows 2000 Server, SP2 or higher.
2. IIS 5.0 or later (this service should be installed by default along with your Windows 2000 installation).
3. Internet Explorer 5.5 or later.
4. SUS must be installed on an NTFS v.5 partition.

Once your system meets the above prerequisites you can download and install the Software Update Service package from Microsoft's Website. This package is a GUI-based tool that was developed by Microsoft to allow you to setup a Windows Update server on your own LAN.

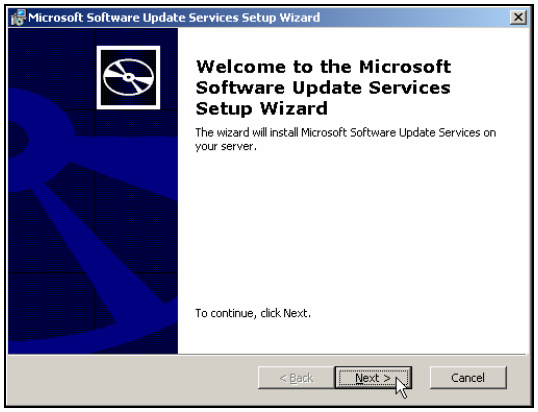
1. To download SUS, go to www.microsoft.com and enter **sus server** in the search box.

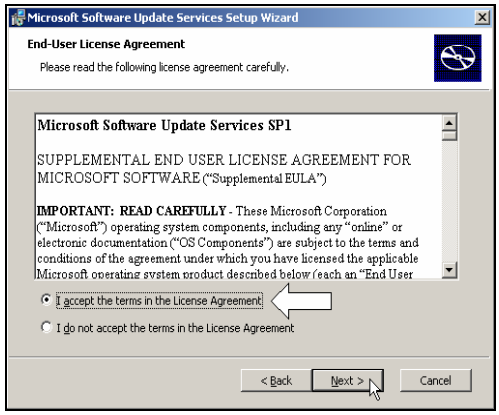


2. Click on the search result that references SUS. This page should allow you to download SUS.

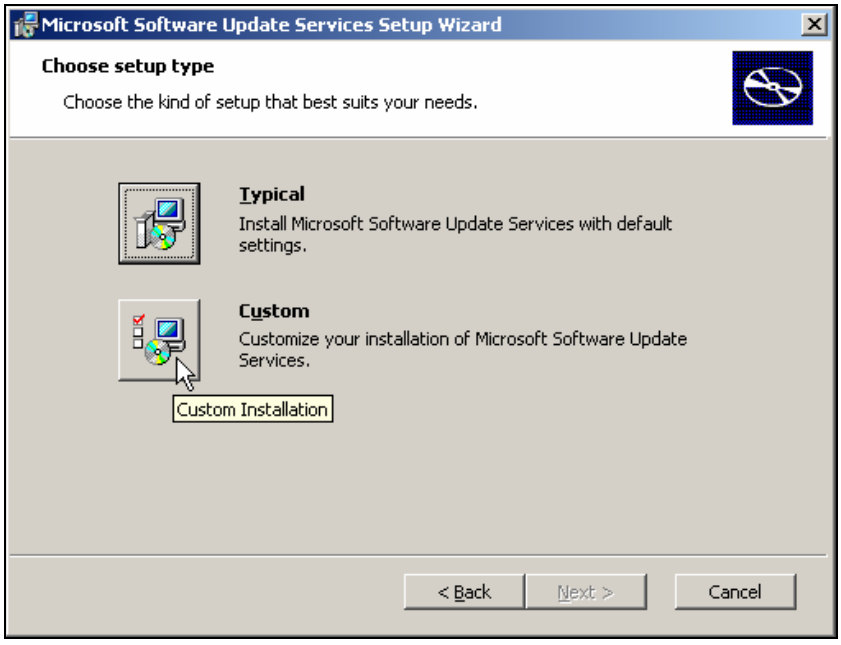


3. After you have completed the download, double-click the **SUS 1.0 SP1** file (your file name may be different) on DC-1's desktop to install this service. The first screen you will see is the welcome screen. Just click **Next** to pass this screen and also click **Next** to accept the license agreement.

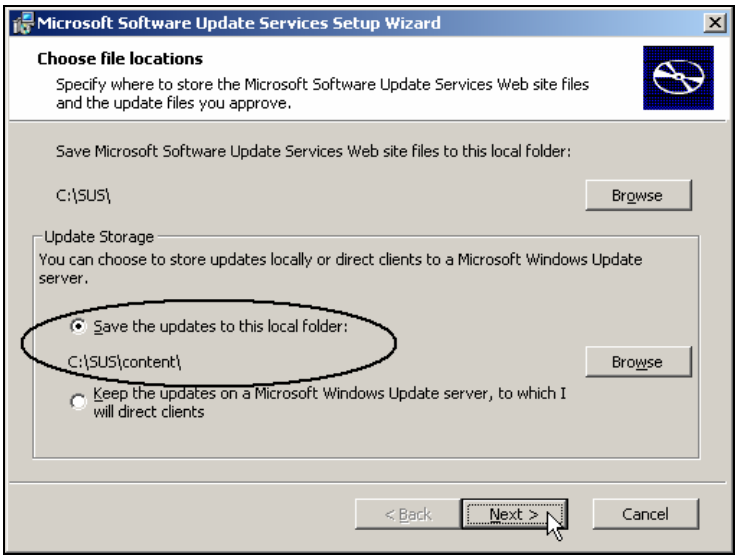




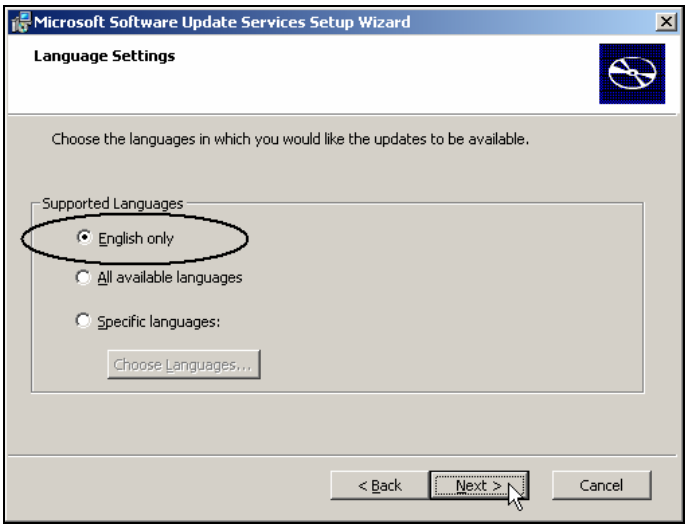
4. The next screen will ask you to choose a setup type. For the purposes of this lab, click **Custom**.



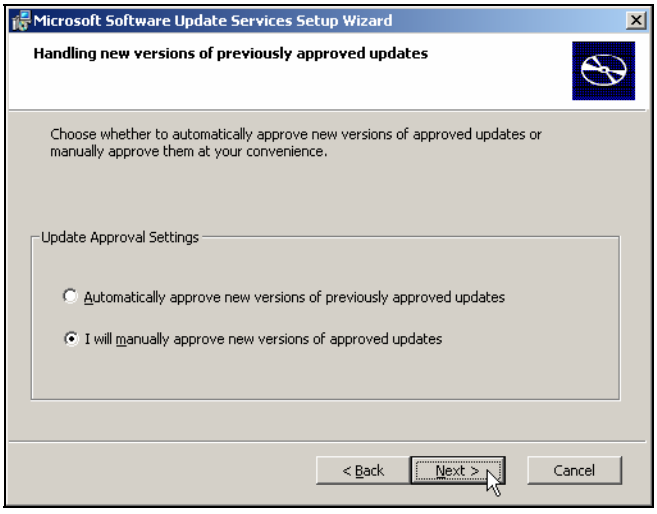
5. On the choose file locations screen, you can select to either save updates to a local folder or to direct clients to a Microsoft Windows Update server. Make sure that the **Save the updates to the local folder:** is selected and click **Next** to continue.



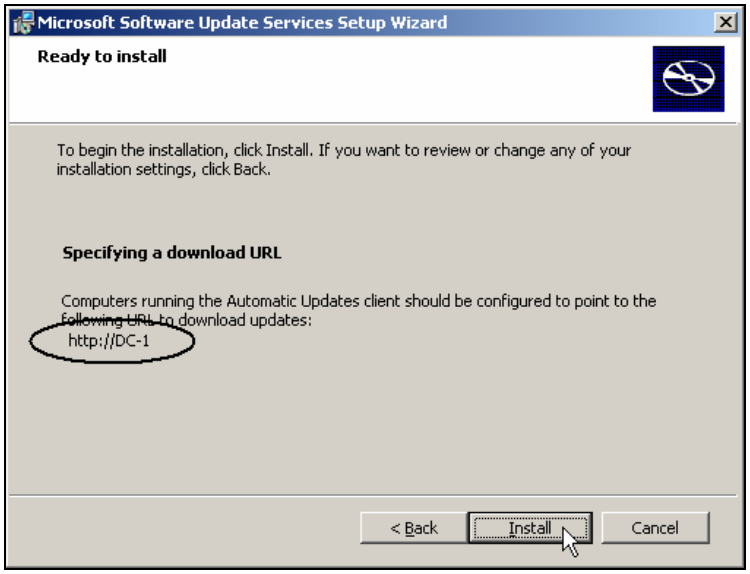
6. This will bring you to the Language Settings screen. There are 3 selections you can choose from: English only, All available languages and Specific languages. The default is set on All available languages. This setting requires a lot of available hard disk space for update storage and takes a considerable amount of time for downloads. Therefore, just select **English only** as the supported language. Click **Next** to continue.



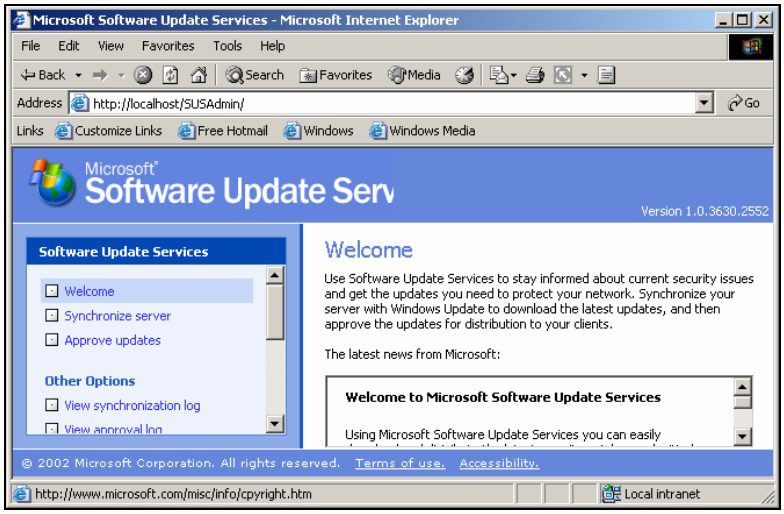
7. Next, is the "Handling new versions of previously approved updates" screen. Select **I will manually approve new versions of approved updates** as the update approval setting. This will avoid any compatibility issues you might face by turning new version updates loose on your network. Click **Next** to continue.



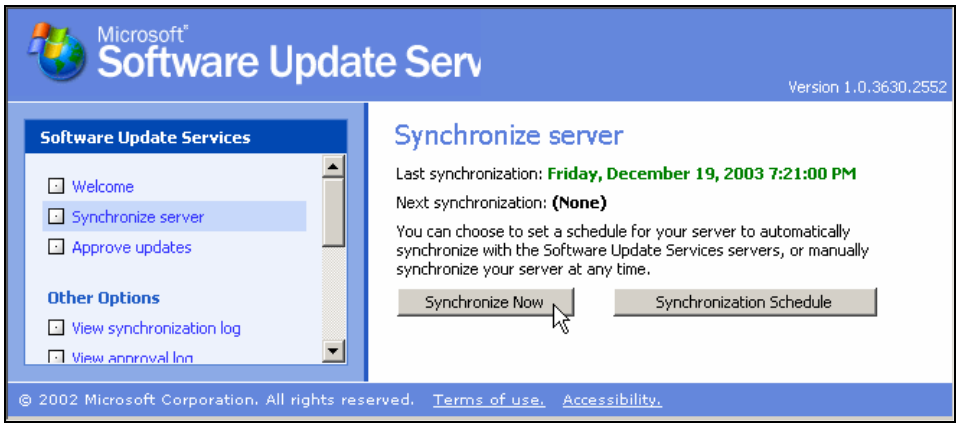
8. This will bring you to the Ready to install screen. This screen provides you with the URL to which Automatic Updates client computers should be configured to point, which will be **http://DC-1** on the Storks' network. Click **Install** to begin the installation.



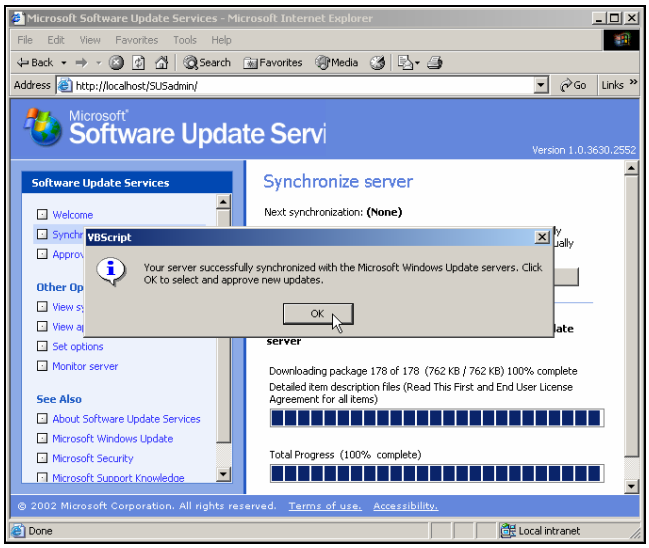
9. After you have successfully installed Software Update Services, open **Internet Explorer** and type in http://DC-1/SUSAdmin (you can also type in http://localhost/SUSAdmin). This will bring you to the Software Update Services admin page.



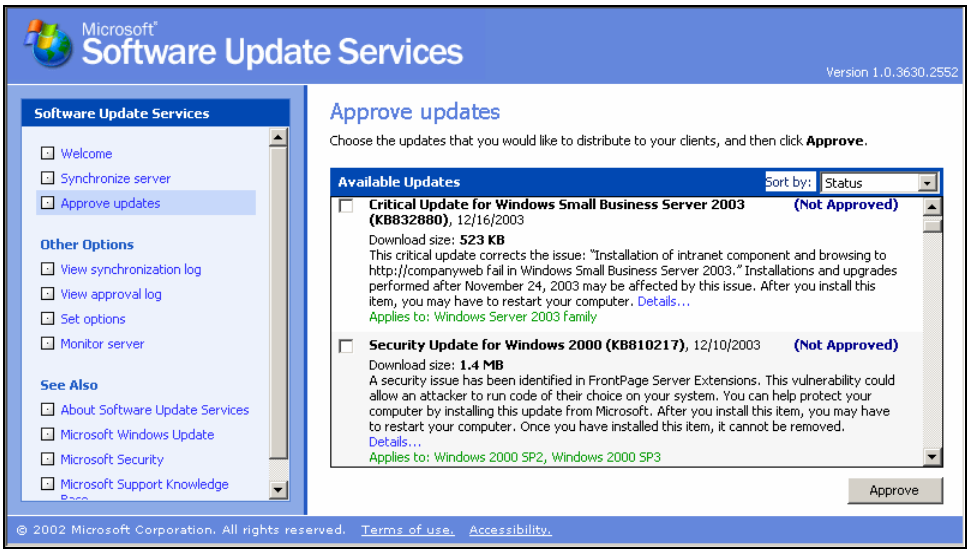
10. Before you can distribute any updates to your clients, you will need to synchronize your SUS server with the Microsoft Windows Updates server. Click the **Synchronize server** button on the left side of the SUS server admin page. On the right pane of the SUS server admin page, as you see, there are 2 selections: Synchronize Now and Synchronization Schedule. You can either manually synchronize or schedule a date and time for synchronization. Since this server has never been synchronized with the Microsoft Windows Updates server, click **Synchronize now** to synchronize it. The server will start downloading updates right away from the Microsoft Windows Update server. There are a lot of updates to download so this process may take quite some time.



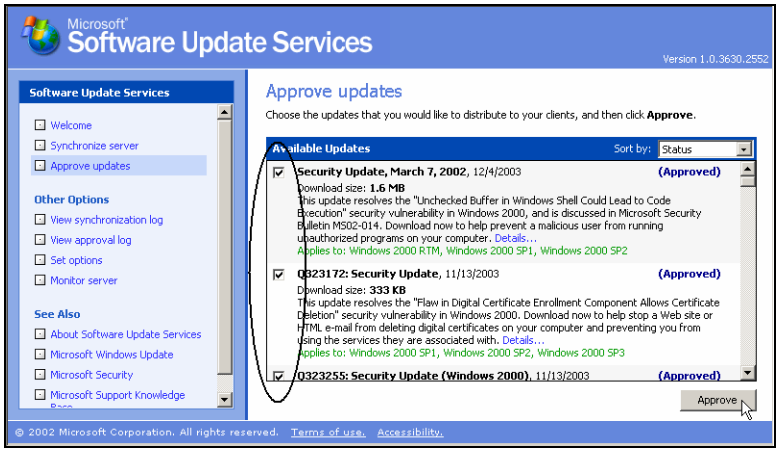
11. After all of the updates have been downloaded, you will be asked to select and approve new updates. Click **OK** to continue.

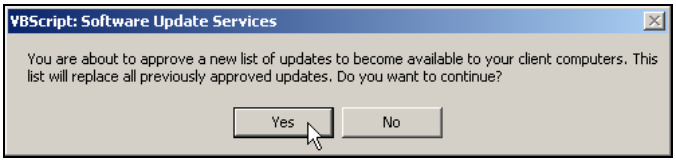


12. When using SUS, updates need to be approved before you can distribute them to your clients. This gives the administrator control of exactly what to distribute on the network. To approve updates for distribution, just click **Approve updates** in the left pane of the SUS server admin page. In the right pane of the SUS server admin page, there are many updates waiting to be approved for distribution.

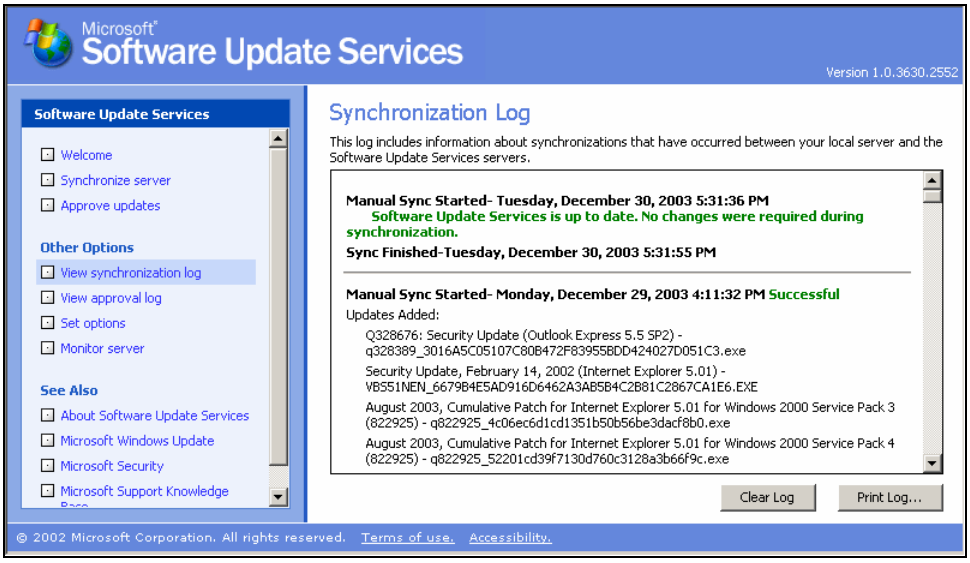


13. Check all of the updates that apply to the Windows 2000 family and click **Approve** for distribution. Also, click **Yes** to approve this new list of updates to become available to your Automatic updates clients.

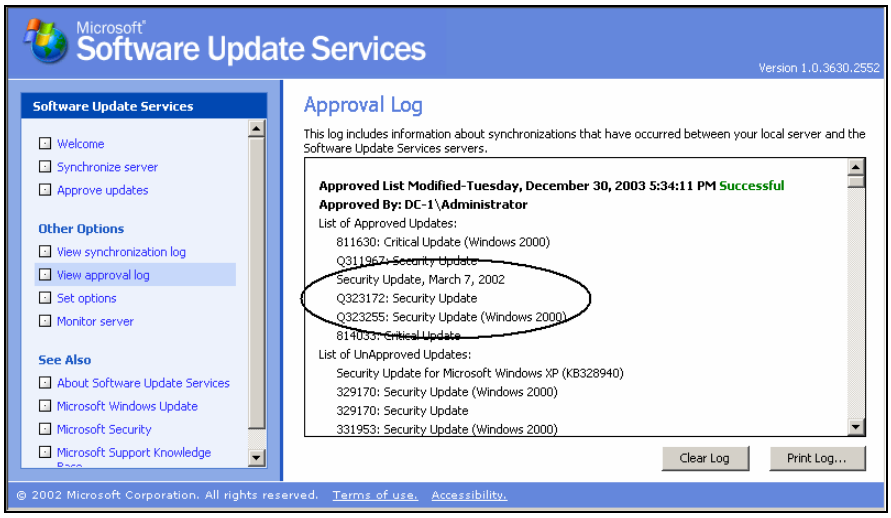




14. On the Software Update Services admin page, you can also view a Synchronization Log. This log provides you with information about synchronization that has occurred between DC-1 and the Windows Update servers. Click **View synchronization log** to view the log.

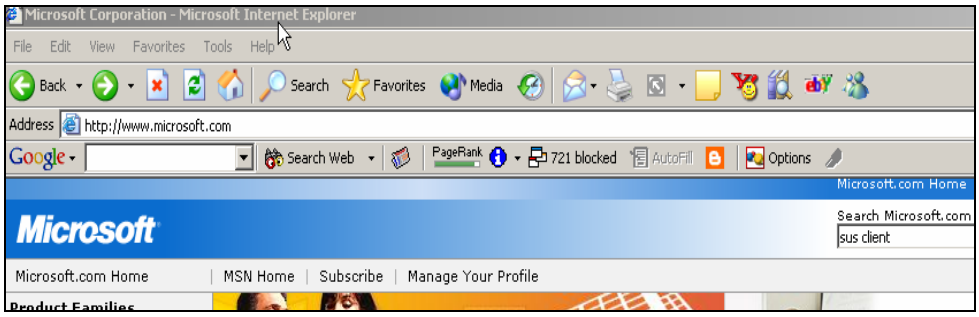


15. You can also view approved and unapproved updates by clicking on the **View approval log** in the SUS admin page.

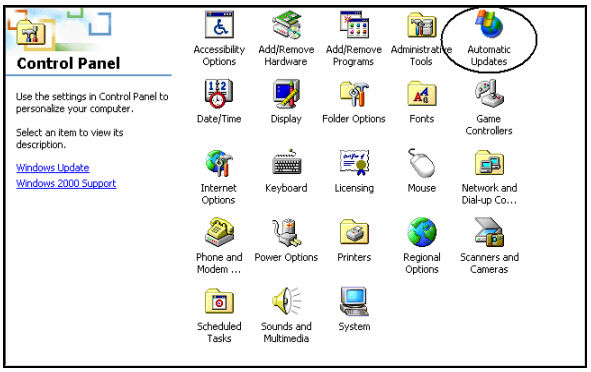


Automatic Updates client

1. After you have approved the required updates on the Storks' SUS server, you need to download and install the Automatic Updates client software on your client machine, Pro-1. This client is already present with Windows 2000 SP3 or later, XP SP1 and Server 2003. Otherwise, go to www.microsoft.com and do a search for: **susclient**

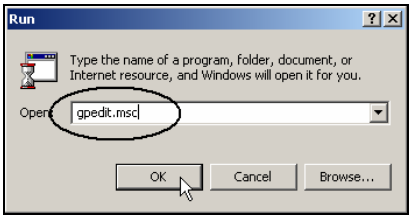


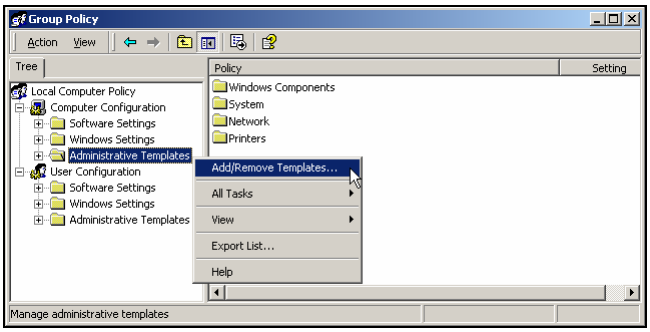
2. After you have downloaded the Automatic Updates client installation package, just double-click the **wuau22.msi** file (the name of the file at time of writing) on Pro-1's desktop to install it. The installation will take less than a minute. After you have completed the installation, a new applet will be created in the Control Panel.



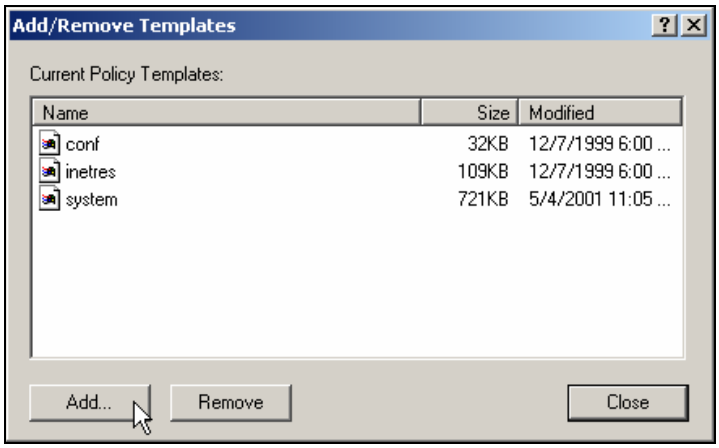
3. The Automatic Updates client is initially not enabled to download updates from your SUS server. It is configured to download updates from the Windows Update server by default. Therefore, you will need to configure it so that it will download updates from your dedicated SUS server.

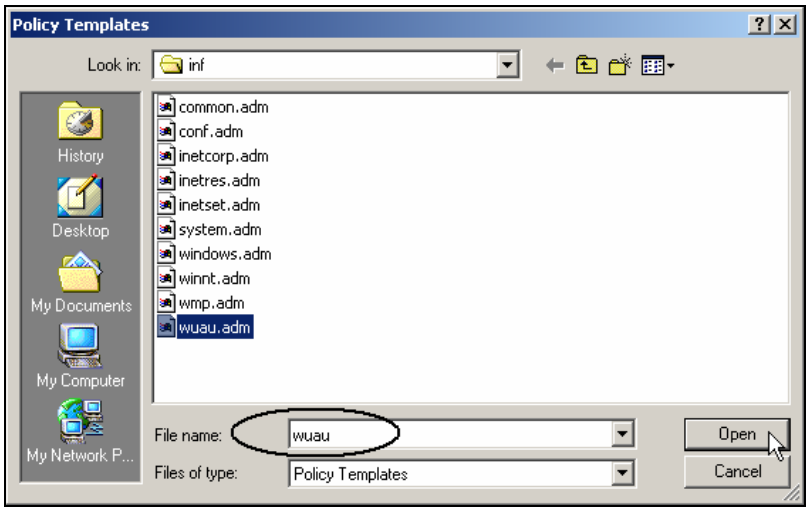
   Automatic Updates settings are configured through a special administrative template. You need to add this template to the group policy console. To do this, go to **Start→ Run**, type in **gpedit.msc** and click **OK**. This brings up the Group policy console. Right click on **Administrative Templates** and select **Add/Remove Templates**.



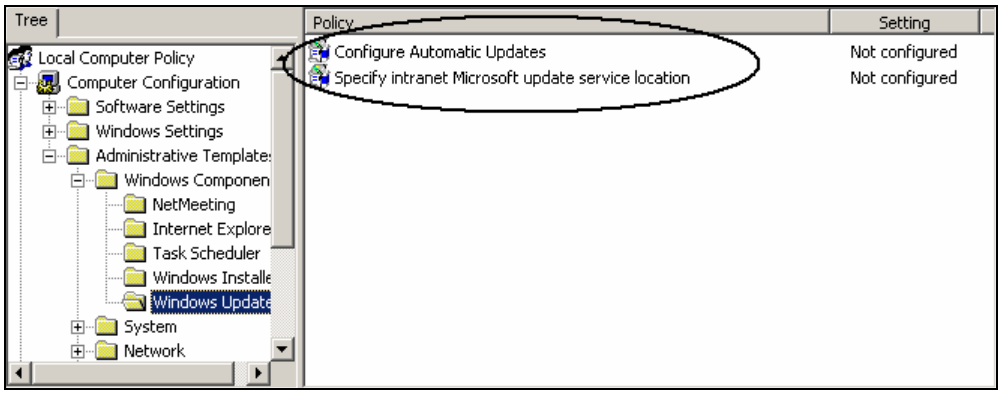


4. In the Add/Remove Templates dialog box, click **Add** and then select the **wuau.adm** template. Click **Open** to confirm this choice. Then click **Close** to close the Add/Remove Templates box.

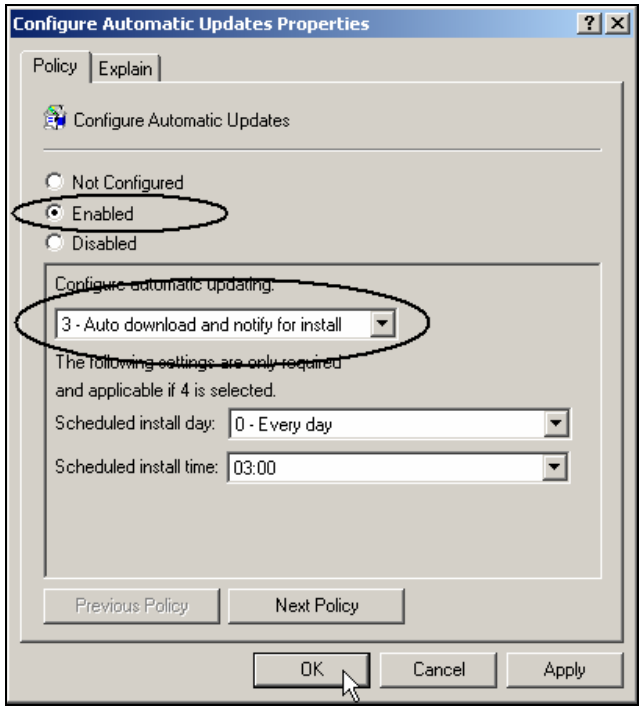




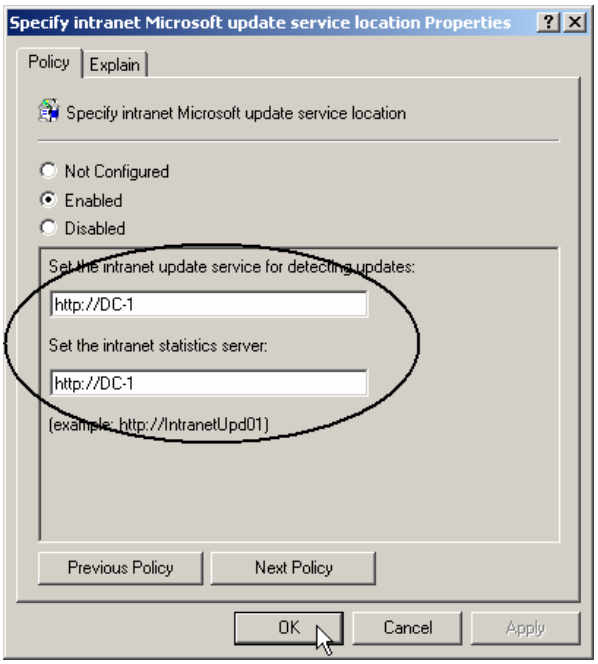
5. In the group policy console, expand the **Administrative Templates** node and expand the **Windows component** node. Click on the **Windows Updates** folder. As you see in the right pane of the group policy console, there are 2 policies you need to configure for your SUS client.



6. Double click on the **Configure Automatic Updates** policy. It will bring you to its properties dialog box. Select **Enabled** and choose **Auto download and notify for install**. Click **OK** to complete the configuration.

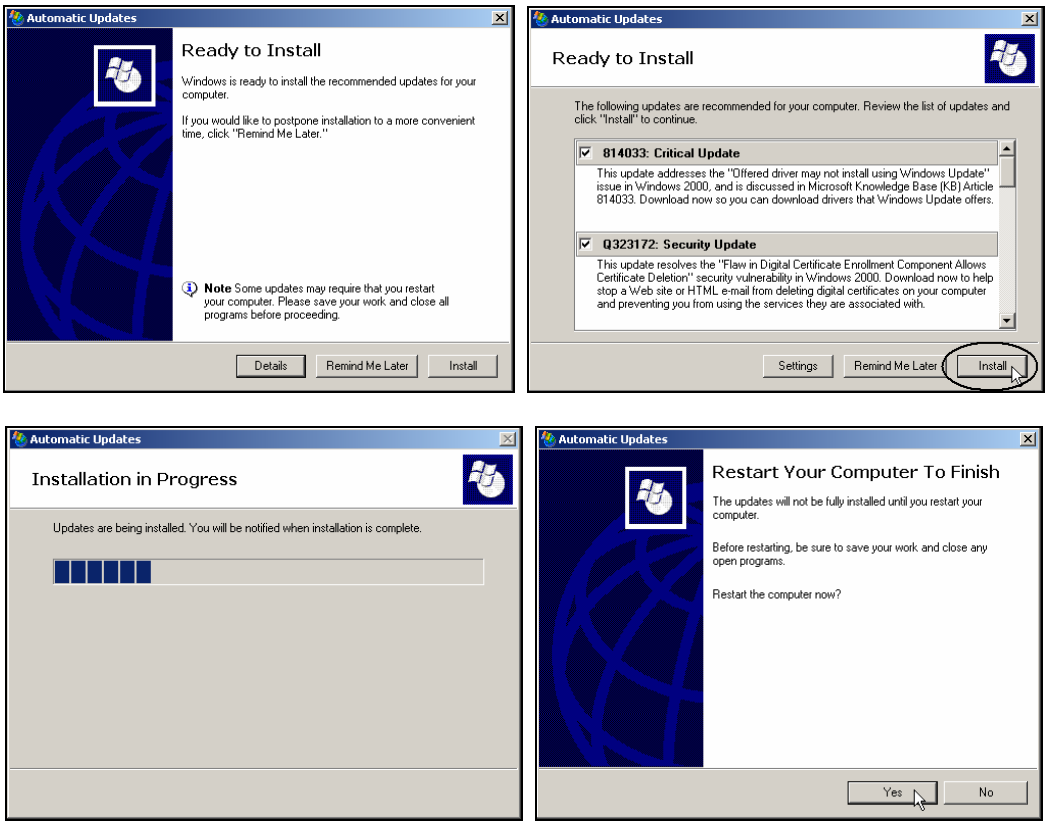


7. Next, double click the **Specify intranet Microsoft update service location** policy. You will see the properties dialog box below. Select **Enabled** and enter **http://DC1** as the update service and statistics server. Click **OK** to complete the configuration. You have now completed configuration of the Automatic Updates client.

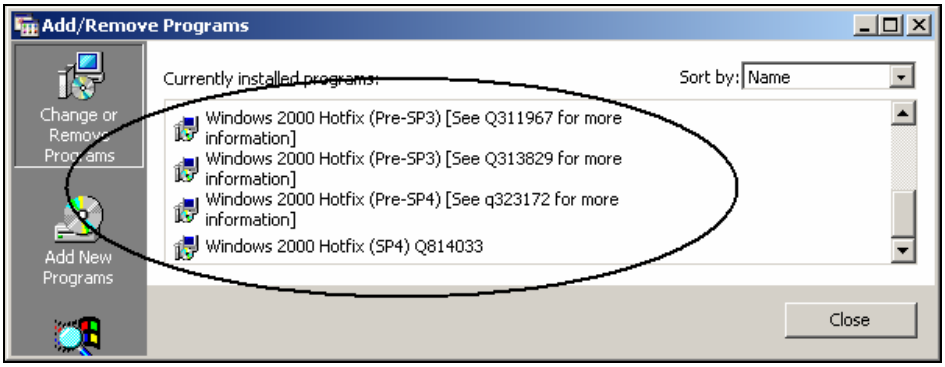


8. After you have completed the Automatic Updates client configuration on Pro-1, a Windows Update notification will be appear on the task bar. It will sometimes take a period of time (up to 24 hours) for this to appear depending on the number of updates you have approved. When this appears, double click it.

9. This brings you to the Automatic Updates dialog box. Click on **Details** to verify all of the updates that you approved in your SUS server and click **Install** to start the installation process. As soon as the installation is completed, click **Yes** to restart **Pro-1**.



10. After you have completed the installation, you can go to **Add/Remove** programs in Control Panel and verify that all of your updates have been installed.

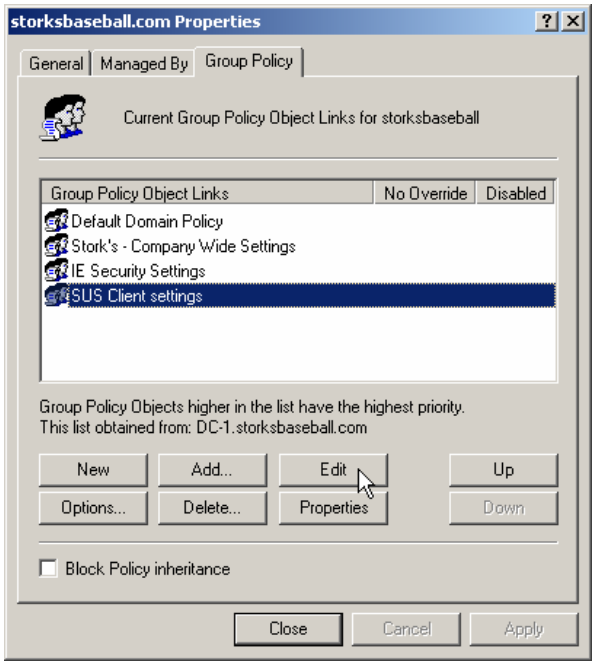


Configuring Automatic Updates with a GPO

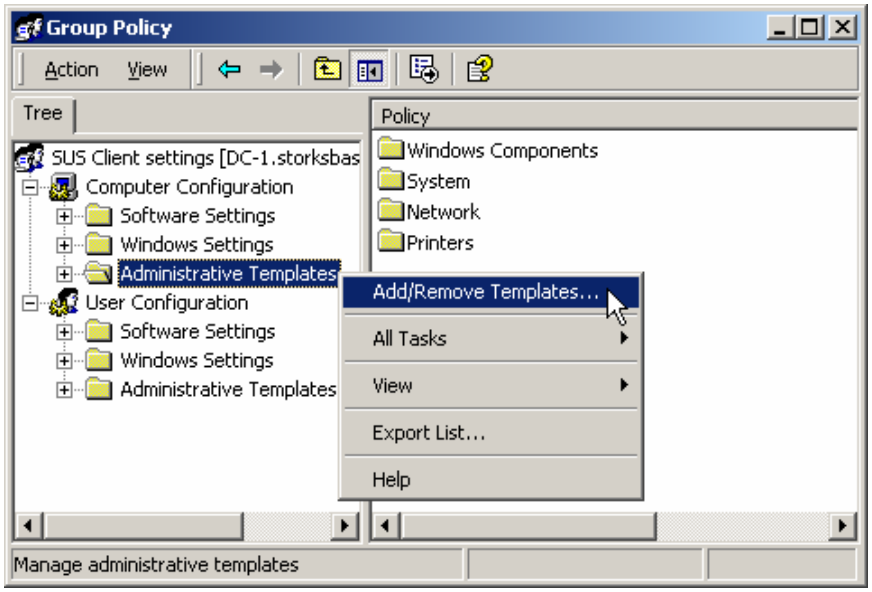
Configuring the Automatic Updates client on all of the machines in your network is time consuming and inefficient. Instead, you can deploy the settings through a group policy object (GPO).

1. Log on to **DC-1** and launch **Active Directory Users and Computers**. Right click on your domain (**storksbaseball.com**) and click **Properties**. Click the **Group Policy** tab and click **New**. Type in **SUS Client Settings** for the new policy name and click **Edit**.

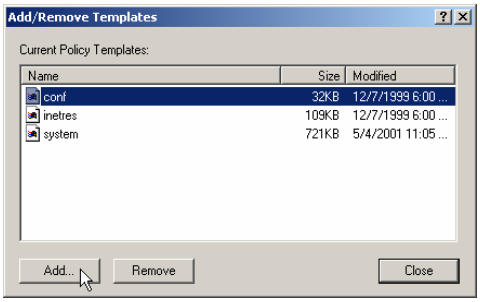
Note: This policy will be applied at the domain level. In a production environment you may not want to deploy this policy onto servers.

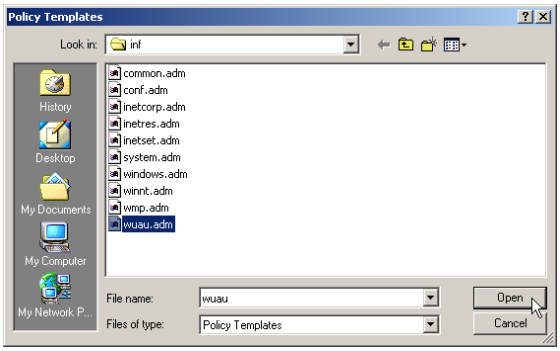


2. Under **Computer Configuration**, right click on **Administrative Templates** and click **Add/Remove Templates**.

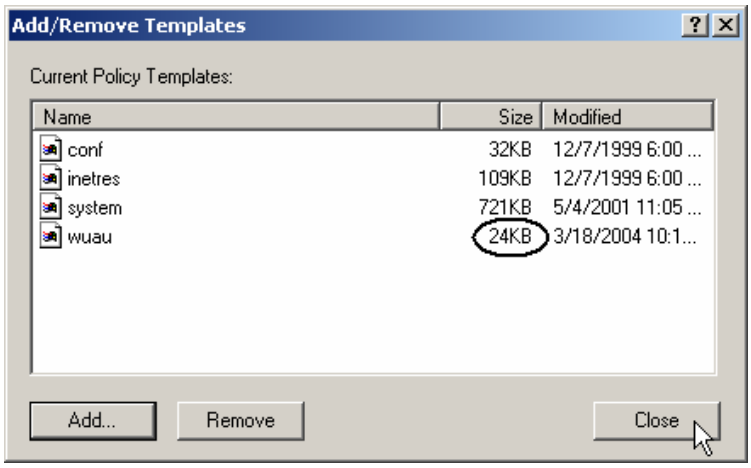


3. In the **Add/Remove Templates** dialog box, click **Add** and select the **wuau.adm** template. If this file is not present in the **Policy Templates** dialog box, you can download it from the Microsoft web site and save it to c:\winnt\inf (assuming that you have Windows 2000 installed on your C: drive). If the file is present, make sure you check its size. If it is 18KB (or 19KB), this is an older version. There is a newer version, 24KB (or 25KB), that has two additional configuration options. The newer version is demonstrated in this lab. Click **Open** to continue.

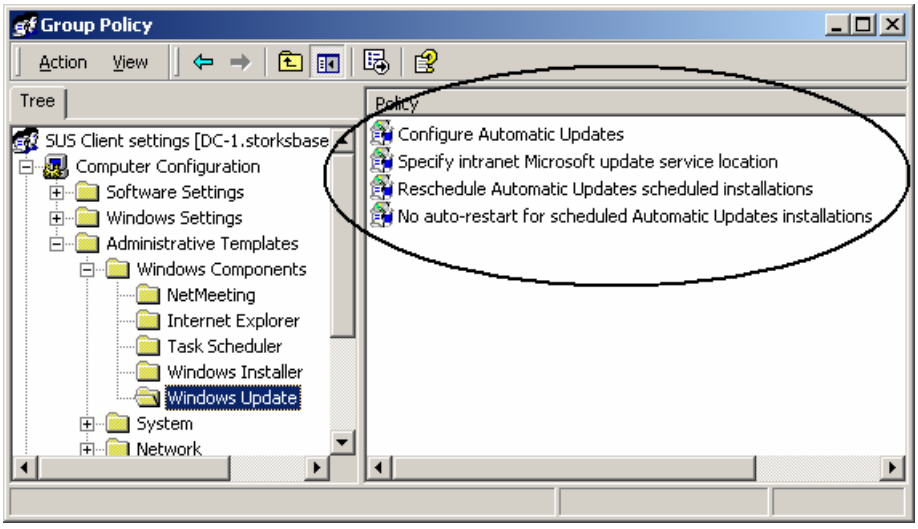




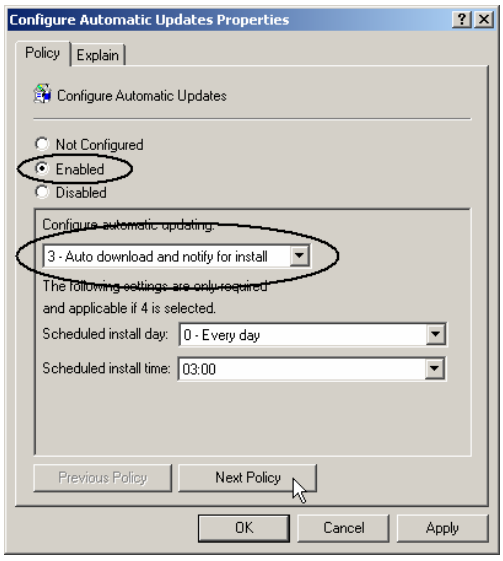
4. You should now see **wuau.adm** included in the list of templates. Make sure this file shows up as 24KB in size and click **Close**.



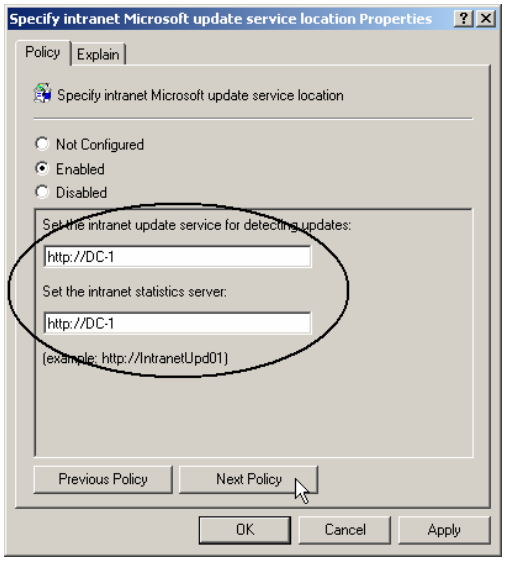
5. Back in the group policy console, expand the **Administrative Templates** node and expand the **Windows components** node. Click on the **Windows Updates** folder. In the right pane of the group policy console, there are 4 policies that you can configure.



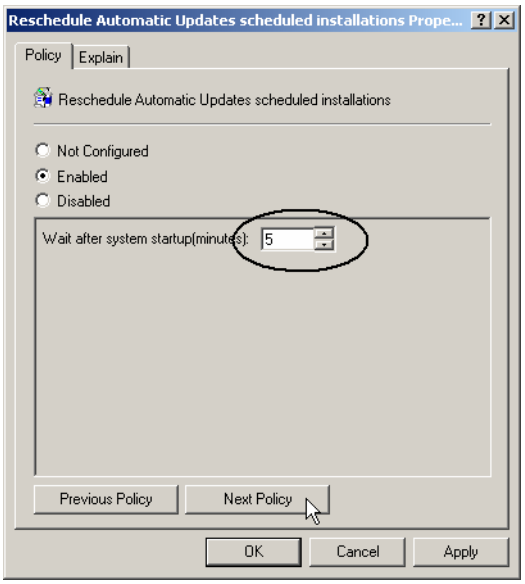
6. Double click the **Configure Automatic Updates** policy. This brings you the properties dialog box. Select **Enabled** and **Auto download and notify for install.** Click **Next Policy**.



7. The next policy is **Specify intranet Microsoft update service location Properties**. Select **Enabled** and enter **http://DC-1** as the update service and statistics server. Click **Next Policy** to continue.



8. In the **Reschedule Automatic Updates scheduled installations Properties** dialog box, select **Enabled** and leave the **Wait after system startup** at the default setting of 5 minutes. Click **Next Policy** to continue.



9. The last policy is **No auto-restart for scheduled Automatic Updates installations.** Select **Enabled** to prevent computers from restarting automatically after performing updates. Click **OK** and you have finished configuring the windows update client through group policy.