# Global Information Assurance Certification Paper

# Securing a Windows 2000 Domain Using Group Policies and The Security Configuration and Analysis MMC Snap-In

**Submitted By:**
**Perry L. Pierce**
**For GCNT Certification Version 2.1a**

## Introduction

This paper will discuss Microsoft Windows 2000 Advanced Server Group Policy Object features that can be used to assist in the configuration of security settings for domain controllers as well as local computers who are members of the domain. The paper will then discuss the Microsoft Management Console, the Security Configuration and Analysis Snap-in, and how these features can be used to analyze the effects the group policy object created with Group Policy editor have had on the computer. Finally I will explain how to use the MMC console and the Security Configuration and Analysis Snap-In to apply the newly created template and save the template for use on other computers.

# Group Policy

In this section of the paper I will give a brief explanation of Group Policy Object (GPO) and the procedure to create and edit group policies. Group Policy Objects could be the subject of a paper by themselves. However this is not the intent of this paper.

The primary purpose of GPO is to reduce the workload of the system administrator. By using GPO the system administrator can deploy configuration settings to individual users, computers, groups of users or groups of computers. The GPO can be used to set security configuration, deploy software, configure desktop settings and many more functions that go beyond the scope of this paper. This paper will only briefly cover GPO and how it can be used to make security management easier.

When you set up an Active Directory there are two default Group Policy Objects created. The default domain policy and the default domain controller policy. The default domain policy is evaluated at the domain level and therefore could potentially be applied to all of the objects in the domain. The default domain policy is the Group Policy Object I will work with for this paper.

The GPO is divided into two sections, the User Configuration section and the Computer Configuration section. The User Configuration section configures user environment settings and is applied when the user logs on. The Computer Configuration section configures computer-based setting such as service settings, startup and shut down scripts and security settings. The Computer Configuration section is applied when the computer boots up. This paper will primarily discuss the Computer Configuration section.

I recommend you set your broadest security setting in the Computer Configuration section at the domain level then push them down to the local computers and Organizational Units with the no override attribute.[1] You can then set more specific user settings at the OU level.

I will explain step by step how to set some of these security setting for all computers in the domain by using the group policy that are part of Active Directory Users and Computers. Later I will then explain how to compare these settings to a security template provided by Microsoft, by using the Microsoft Management Console, (MMC) Security Configuration and Analysis snap-in.

The MMC is designed to provide a single location for all management tools. The MMC alone does not provide any management functions, but provides a common environment for the snap-ins which performs the actual management functions. There are thirty-four

[1] The no override attribute will be explained later in this paper.

snap-ins available with the standard Windows 2000 installation. This paper will only describe the use of one of these snap-ins.

The basic installation of Windows 2000 Advanced Server configures very few security settings. An administrator should go back and manually configure these setting to match the particular security needs for your specific needs.

To begin the configuration for our Domain, open the Active Directory Users and Computers by clicking **START, PROGRAMS, ADMINISTRATIVE TOOLS** and then **ACTIVE DIRECTORY USERS AND COMPUTERS**. An MMC console that looks like figure one will open.

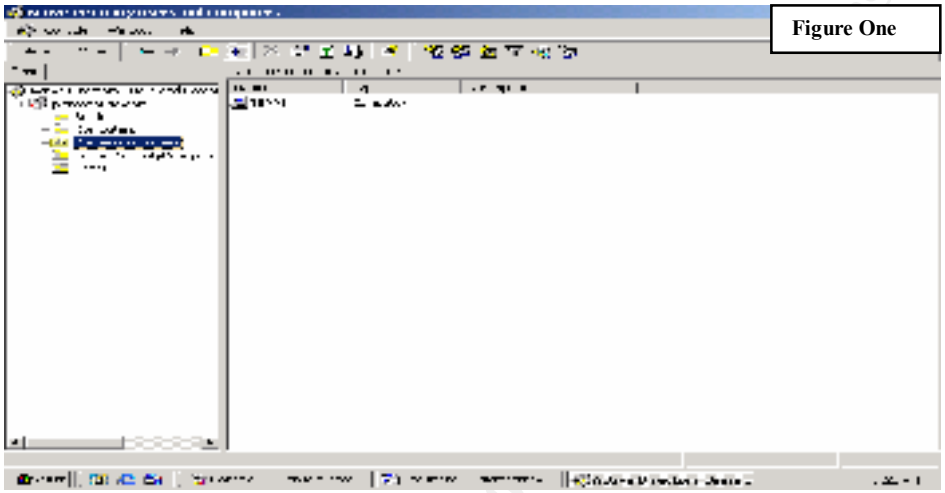


**Figure One**

Navigate to the icon that displays your domain name and right click. Chose the properties menu item and left click to open the properties dialog box. Click the Group Policy tab.

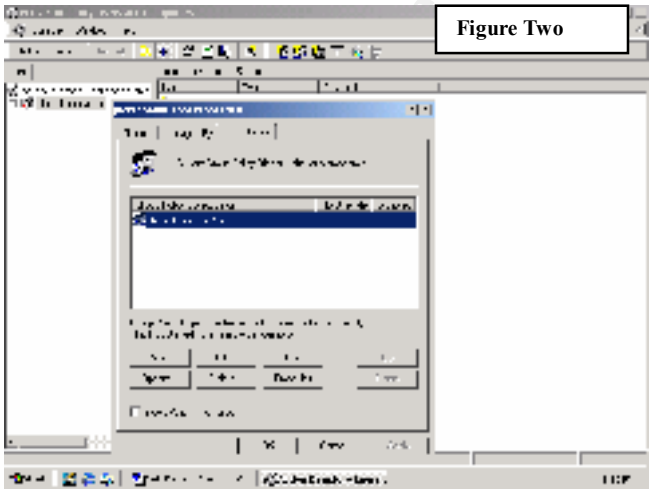
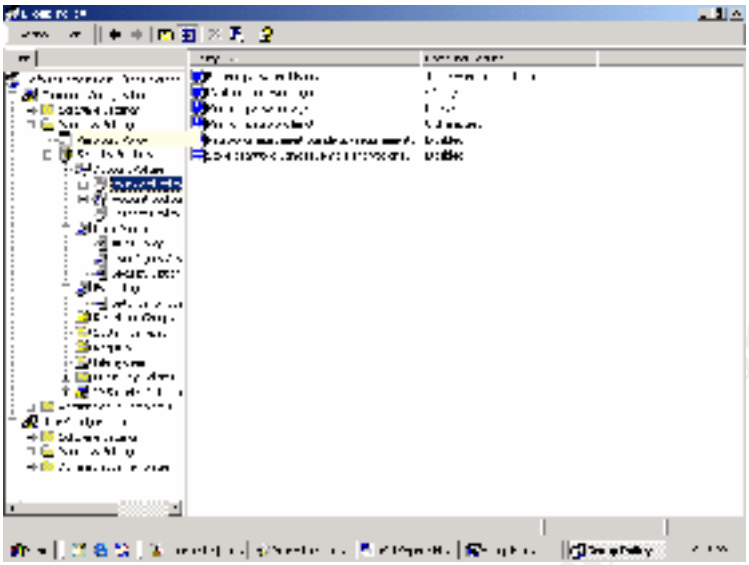


**Figure Two**

Ensure the Default Domain Policy is highlighted and click the edit button to open the Group Policy window. From here you will begin to configure the security settings you wish to be applied to all computers within the Domain. The settings set here will automatically be applied to all computers that are added to the Domain.

After opening the group policy for editing you will notice several folders devided into two separate groups. One group titled Computer Configuation and one group tilted User Configuration. To start with I will explain some of the settings in the Computer Configuration area. Settings in the User Configuration will be edited in a separate policy.

The Security Setting we are going to configuire first are located in the Computer Configuaration group under the Windows Setting Folder, by expanding the Windows Setting folder you will reveal the section titled Security Settings. By clicking on the plus sign next to Security Settings you will expand the security setting to reveal the settings that can be applied to the Domain. After expanding the Windows Setting Folder and the Security Settings your screen should look like the figure below.



From this point you can manually configure all of the security settings for the computers within this domain. I will step through several of these Security setting to explain their function and demonstrate how to edit the value of these setting to manually configure your system.

The first group under the Security Settings is the Account Policy section. The Account Policy Section is where the Password Policy and the Account Lockout Policy is defined.

The Password Policy area is where you set the password policy for the domain. Setting strong password policies is the first line of defense in implementing a secure network. The following is a list of policies that may be set in this area, and a brief explanation of each:

**Enforce Password History**, prevents users from reusing the same passwords over again. This setting configures how frequently an old password can be used. By default Windows 2000 stores one password in the password history. The setting can be changed to remember up to 24 passwords. However by configuring this setting too high the administrator runs the risk of users writing password down in order to remember them.[2]

**Maximum Password Age**, Sets the maximum time a user can keep a password before it has to be changed. By default Windows 2000 sets this at 42 days. The user will get a warning box when the aging date is less than 30 days away. The greater your security needs the lower this number should be. Note however multiple password changes can cause a hardship on your users and they may be tempted to write passwords down to remember them.

[2] Because the way passwords are saved in a table a user cannot reuse a password until they have changed passwords n+2 times where n is the number of passwords remembered. So if Enforce Password History is set to 3, users cannot revert to the first password until they have changed their password five times (3+2).

**Minimum Password Age**, This determines how long a user must keep a password before it can be changed. This is used to prevent a user from immediately changing his/her password back to the password they were just forced to abandon. By default Windows does not set this. If you set an Enforce Password History value, do not set this value to zero.

**Minimum Password Length**, Sets the minimum length of the password. By default Windows sets this value at zero. For security purposes this should be changed to match your security policy.

**Password Must Meet Complexity Requirements**, Configures the system to use the default password filter for password changes. The default password filter will enforce a password that is at least six characters in length, doesn't contain the username or parts of the user's full name, and uses three of the following: numbers, symbols, lowercase, and uppercase letters. By default this setting is not enabled.

**Store Password Using Reversible Encryption**, Allows the password to be stored in a reversible manner. This is mainly needed if you are using Digest Authentication. By default this setting is not enabled.

The Account Lockout Policies section is the key area to prevent brute force attacks. The following values can be set from this area.

**Account Logout Duration**, Configures the amount of time that an account will be locked out, after exceeding the Account Logout Threshold, before it is unlocked. This value can be set from 0-99,999, if set to 0 then the account must be unlocked manually. By default this setting is not defined.

**Account Logout Threshold**, This sets the number of failed logon attempts that are allowed before an account is locked out. The default value is set to zero, which means there is no lockout policy in effect. By leaving this setting at zero there is no protection against password guessing attacks. This setting only applies to initial logons, it does not apply to screen saver or desktop locking.

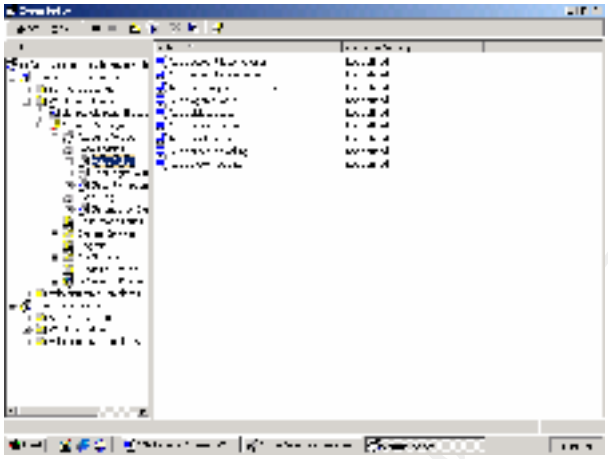
**Reset Account Lockout Counter After**, configures the number of minutes that must pass between failed logon attempts before the bad log logon count is reset. The bad logon count is also reset on a successful logon. By default this setting is not defined.

The remaining section in the Account Policies area is the Kerberos section. Miss configuration of these setting can render a Domain or entire Forest out of service. It is recommended the default setting not be changed unless you are very familiar with their operation. This paper will not address these settings.

The next area for discussion will be the Local Policy Section, specifically the Audit Policy and the Settings for Event Logs which is located under the Event Log section. There are numerous other values that can be set in these areas, but for the purpose of this paper I will only discuss these two areas.

Establishing a good auditing policy is critical when you need to examine what has occurred to your system. It requires a delicate balance to achieve the desired results, yet not negatively impact your systems performance. Each individual Security Administrator will have to evaluate their situation to determine what is the right setting for his/her needs.

By clicking on the Audit Policy icon your screen should resemble the screen shown below.



In the Audit Policy section the following values can be set:

**Audit Account Logon Events** Audits user logon/logoff events where this computer was used to validate the account. This means the Domain Controller that validated the user will record an entry in its security log.

**Audit Account Management** Audits account management events such as creating or deleting a user, user group, or changes in users passwords.

**Audit Directory Service Access** Audits access objects in the Active Directory

**Audit Logon Events** Audits user logon and logoff activity on the machine the user is logging into. When used in conjunction with the Audit Account Logon Events setting this provides an audit trail with both the Domain the account logon to as well as the system logon information.

**Audit Object Access** Audits access to objects such as files.

**Audit Policy Change** Audits all changes to user rights assignments, audit policies and trusts.

**Audit Privilege Use** Audits use of user rights with the exception of Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories and Restore Files and Directories.

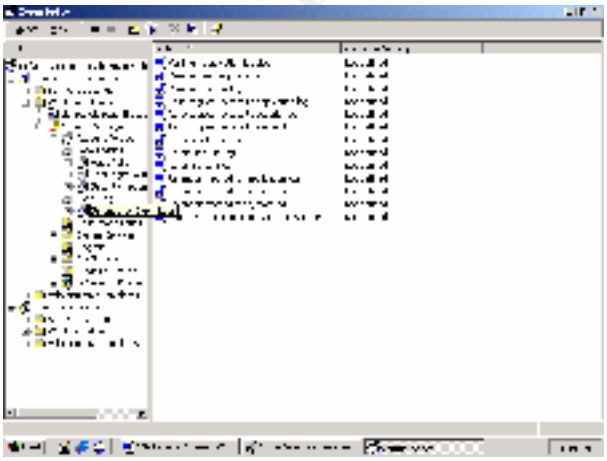
**Audit Process Tracking** Audits system processes such as program execution, process termination and indirect object access.

**Audit System Events** Audits system events such as system shut downs, restarts and events that effect the security log, such as clearing a log.

The following table list recommended Audit policy settings.

| Event Category | Success | Failure |
|---|---|---|
| **Audit Account Logon Events** | **X** | **X** |
| **Audit Account Management** | **X** | **X** |
| **Audit Directory Service Access** | | **X** |
| **Audit Logon Events** | **X** | **X** |
| **Audit Object Access** | | **X** |
| **Audit Policy Change** | **X** | **X** |
| **Audit Privilege Use** | | **X** |
| **Audit Process Tracking** | | |
| **Audit System Events** | | **X** |

When you click on the Event Log Settings Icon your screen will now resemble the screen shown below:



The values that can be set for Event Logs Settings are as follows:

**Maximum Size** This setting can be set for each of the three logs. This setting is dependent upon the user.

**Retention Time** This defines the time the log will maintain an event before it is overwritten.

**Retention Method** Determines the action to take if the log files reaches its maximum size.

**Overwrite Events By Days** Causes the events that are older then the set retention time to be overwritten. If the log file reaches it maximum size before this time period has been reached then events will not be logged until this time has passed. The log file size should be set to adequately provide for the needed space to prevent this from happening.

**Do Not Overwrite Events** This causes no events to be overwritten. This has the same problem as the Overwrite Events by Days setting. If the log reaches its maximum size before the events are manually cleared no new events will be logged.

**Restrict Guest Access** Removes the ability of the Everyone group to access the logs.

**Shut Down the Computer When the Security Audit Log is Full** If this setting is enabled and the security logs reach its maximum size and no events can be overwritten the computer will stop. Only Administrators will be allowed to logon. This setting should not be enabled on systems that require high availability.

The following table list log size recommendations:

| Log | Domain Controller | File /Print Server | Database Server | Web Server | RAS Server | Workstation |
|---|---|---|---|---|---|---|
| Security log | 5-10MB | 2-4MB | 2-4MB | 2-4MB | 5-10MB | 1MB |
| System Log | 1-2MB | 1-2MB | 1-2MB | 1-2MB | 1-2MB | 1MB |
| Application Log | 1-2MB | 1-2MB | 1-2MB | 1-2MB | 1-2MB | 1MB |

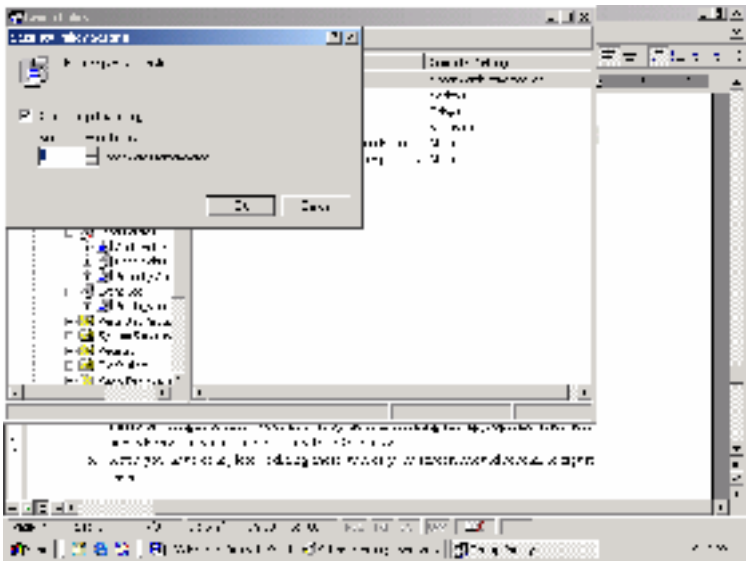
Now that I have discussed the various security setting that can be defined in the Computer Configuration section I will now explain step by step the process to edit several of these setting using the Group Policy Editor. I will then explain step by step the process to compare our settings to a security template provided by Microsoft using the Security Configuration and Analysis Snap-in.

To begin this demonstration I will start at the Desktop. Perform the following tasks

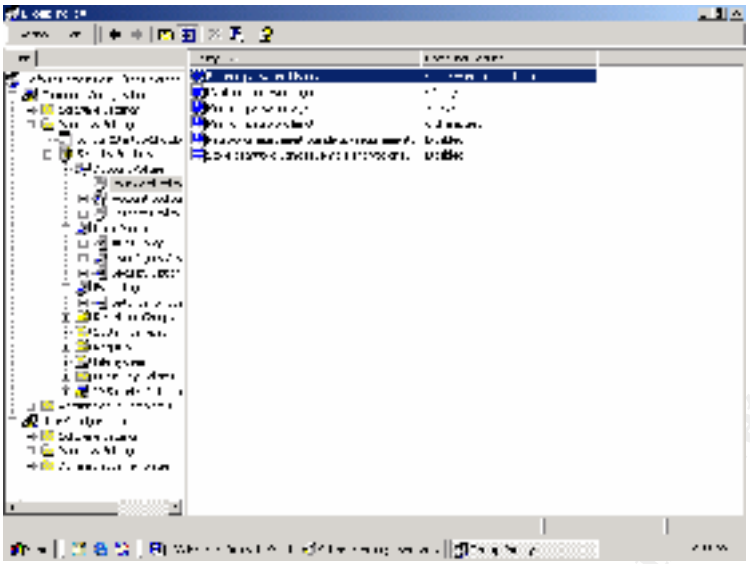
1. Click on the Start button.
2. Click or highlight the Programs menu item and then the Administrative Tools menu item.
3. Click the Active Directory Users and Computers menu item to open the MMC displayed in figure one.
4. Right Click on *Domain.com* (where domain is the name of your Domain).
5. Right click the properties menu item to open the *domain.com* Properties window.
6. Click on the Group Policy Tab to change the view to figure two.
7. Ensure the Default Domain Policy is highlighted and click the Edit button.

From this point you can edit all of the settings displayed under the various sections. Lets edit the Security Settings in the Account Policies section.

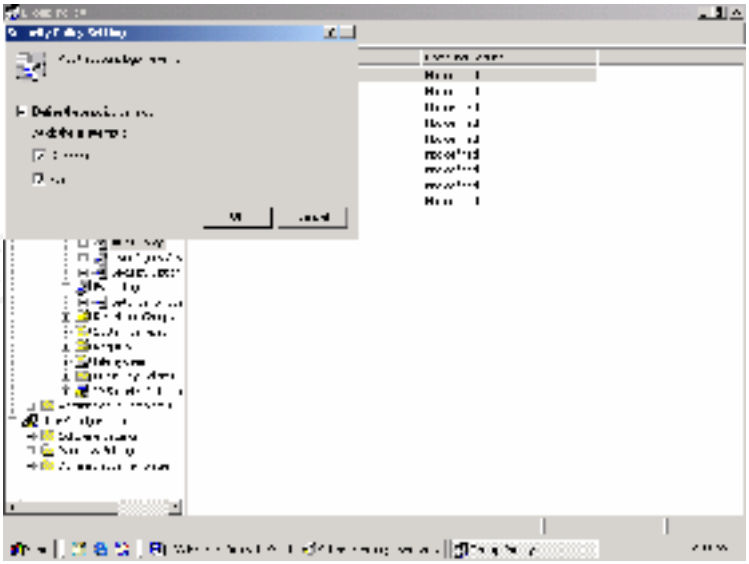
1. Click the plus sign next to the Windows Settings and then click the plus sign next to the Security Settings.
2. Click one time on the Password Policy and review the selections that appear in the right pane.
3. To edit the Enforce Password History value double click Enforce Password History in the right pane.
4. This will open the dialog box displayed in the figure below.
5. Edit the number to match your particular company policy. For demonstration purposes I will edit this value to four. Click the OK button to accept your changes and close the dialog box.
6. Next edit the Maximum Password Age, Minimum Password Age, and Minimum Password length to meet your needs, by double clicking the appropriate selection and editing the value and clicking the OK button.



After you have completed editing these values your screen should resemble the screen shot displayed below.

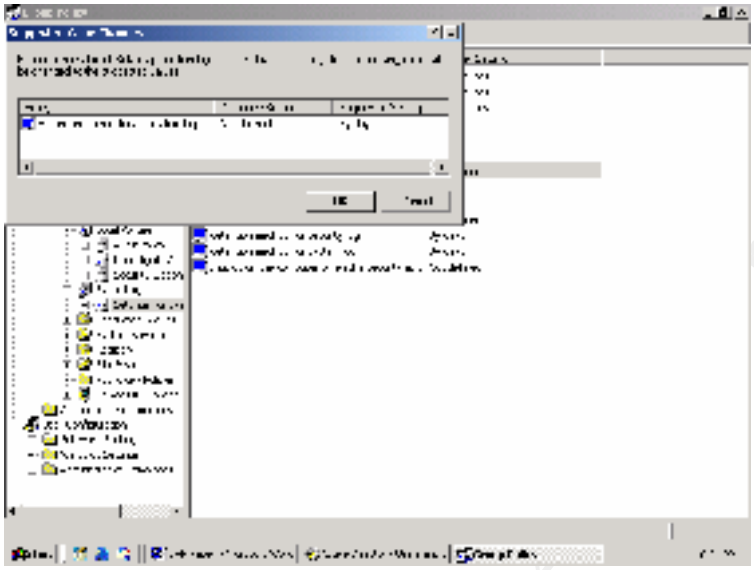


Now lets move on and edit the settings to set up our audit policy.



1. Click the plus sign next to local policies and click Audit Policy.
2. Double click Audit Account Logon Events to open the dialog box displayed in figure to the right.
3. Place a check mark in "*Define these Policy Settings*" which will then activate the success, failure check boxes. Place a check in the box to indicate the auditing you wish to achieve.
4. Click the OK button to accept the setting and close the dialog box.
5. Continue to edit these setting to match your needs.
6. Click the plus sign next to the Event Log and click on the Settings for Event Log in the left pane.
7. Edit the setting in the right pane the same way the settings above were edited.

Next configure your setting in the Event Log section by double clicking the selection in the right pane and choosing the values that meet your needs. The only thing I would like to point out here is when you set you values for the Retain Security Log, Retain Application Log and Retain System Log, when you click the ok button the dialog box displayed in the figure below will appear when you click the OK button Windows will automatically configure the Retention Method for application log, security log and system log.



Continue to define your security policy by defining the values in the various areas in the Computer Configuration area. Keep in mind the setting you make in this policy will be the policy for the entire Domain. Settings that can be applied at an Organizational Unit level or Site level that you wish to vary from this policy are easier to manage with a separate policy set at the appropriate level. Also keep in mind though account security settings may only be set at the domain level.

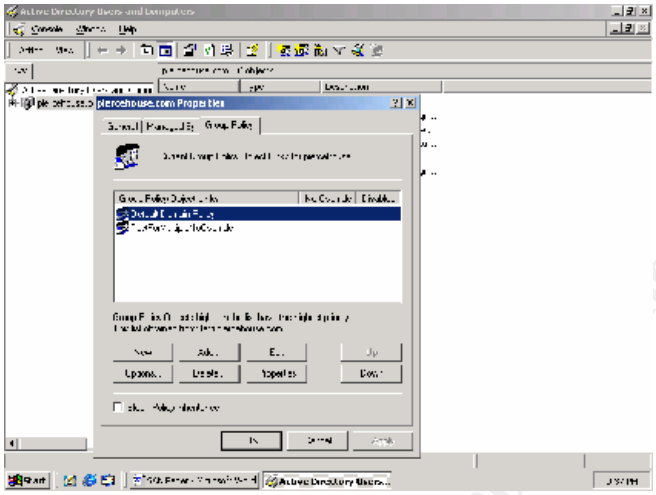
After you have completed setting your security policy in the Computer Configuration section lets set a policy in the User Configuration section. For this demonstration I will set a policy to disable a user from password protecting a screen saver.

I could set this policy by setting the proper values in the User Configuration of our existing domain policy, but I want to create a separate policy to demonstrate a point later in this paper on multiple policies in a container. So lets get started with this new policy.

Lets start back at the desktop. Close any open windows you have displayed and perform the following steps:

1. Click on the Start button.
2. Click or highlight the Programs menu item and then the Administrative Tools menu item.

3. Click the Active Directory Users and Computers menu item to open the MMC displayed in figure one.
4. Right Click on *Domain.com* (where domain is the name of your Domain).
5. Right click the properties menu item to open the *domain.com* Properties window.
6. Click on the Group Policy Tab to change the view to figure two
7. Click the New Button and name your new policy Screen Saver. Your screen should look like the screen shot shown below.



Make sure the new policy is highlighted and click the Edit button. You should now be back at the familiar screen as shown in the graphic on the top of page eleven. Expand the User Configuration section by clicking the plus sign.

Expand the Administrative Templates section
Expand the Control Panel Section
In the left pane click Display
In right Pane double click Password Protect the Screen Saver
Click the disable selection on the policy tab
Click Apply
Click OK
Close the MMC

Now that we have set our security policy there are a couple of ways to activate the policy. You can simple reboot the computer or you can right click on Security settings icon in the left pane and then click the reload menu item. This will cause the security policy to be reloaded on the machine.

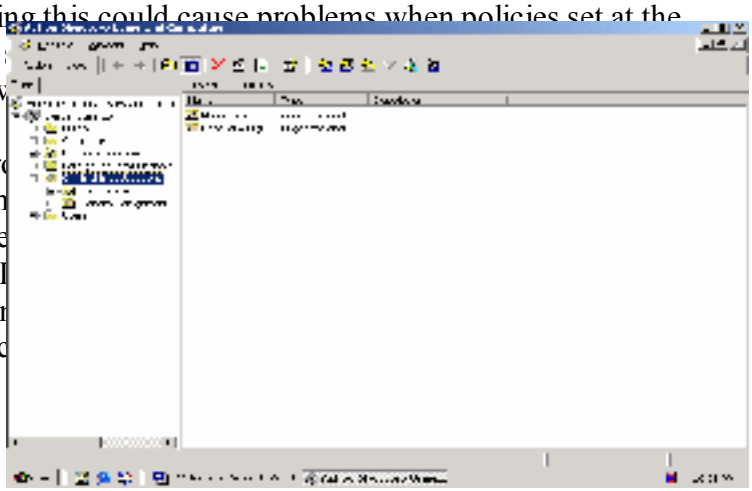
Reload the security policy by either method and then check to see if your setting were applied. If you set a minimum password length, try to create a new user and assign a password shorter than the required password length. You should get an error message advising the password you assigned did not meet the security requirements.

Now that we have defined some of the settings in our group policy lets take some time to discuss how the policy will be applied. A Group Policy Object is an enterprise object, meaning it can be applied to container objects such as sites, domains or organizational units (OU). Each of these container objects can have multiple GPOs applied to them.

Since container objects in an active directory can have separate Group Policy Objects applied to them it is necessary to understand the order of inheritance of these policies so you will know the combined results of these policies. The following is the evaluation and application procedure for a computer boot and user logon.

1. On initial startup the computer evaluates any WinNT system policies that are applicable.[3]
2. If the Local Group Policy Object, Computer Configuration section is defined it will be evaluated
3. The Computer Configuration portion of the site-related GPO(s) in order of precedence, from bottom to the top, is evaluated.
4. The Computer Configuration portion of the domain-related GPO(s) in order of precedence, from bottom to the top, are evaluated.
5. The Computer Configuration portion of the OU-related GPO(s) in order of preference, from the outer to innermost OU and within an OU from lowest to highest, are evaluated.
6. After all of the GPs have been evaluated, their cumulative values are applied.
7. The startup script runs
8. The user logs on and if a profile is set it is loaded.
9. The User Configuration Section of the applicable GPOs are applied[i]

As you can see the group policies start at the top of the network and work down to the local computer. You may be thinking this could cause problems when policies set at the domain level conflict with policies
prevent that from happening and I



To better explain the inheritance pr
policy set at the domain levels from
the active directory displayed to the
Unit titled Criminal Investigations I
Major Case and General Assignmer
the domain level. Remember the sc
policy?

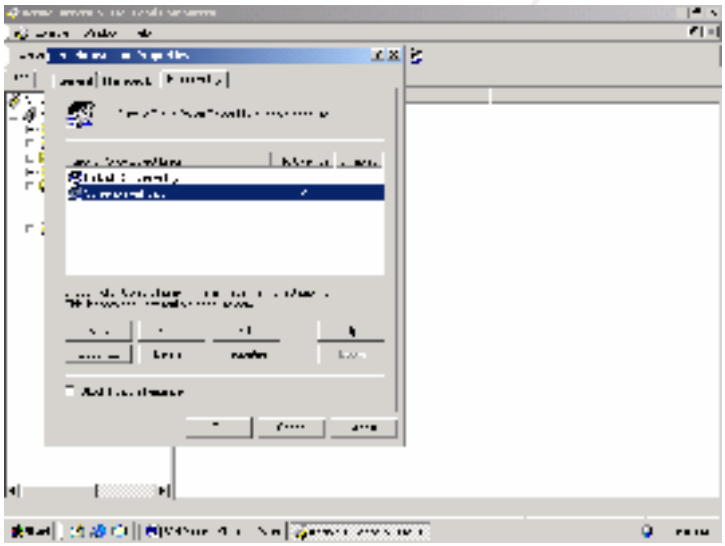
[3] Using WinNt system policies on a Win2K system may write registries entries outside of the GPO scope to an unexpected location.

The screen saver password policy was set at the domain level, but I have a Junior Administrator designated for the Criminal Investigations OU. From the description of policy inheritance provided above you can see that a policy set at the OU level is evaluated after the domain policy. The Junior Administrator at the OU level could block the inheritance of the Domain screen saver password policy by creating his or her own policy, thus preventing the domain screen saver password policy mandated by company policy from being applied to his domain.

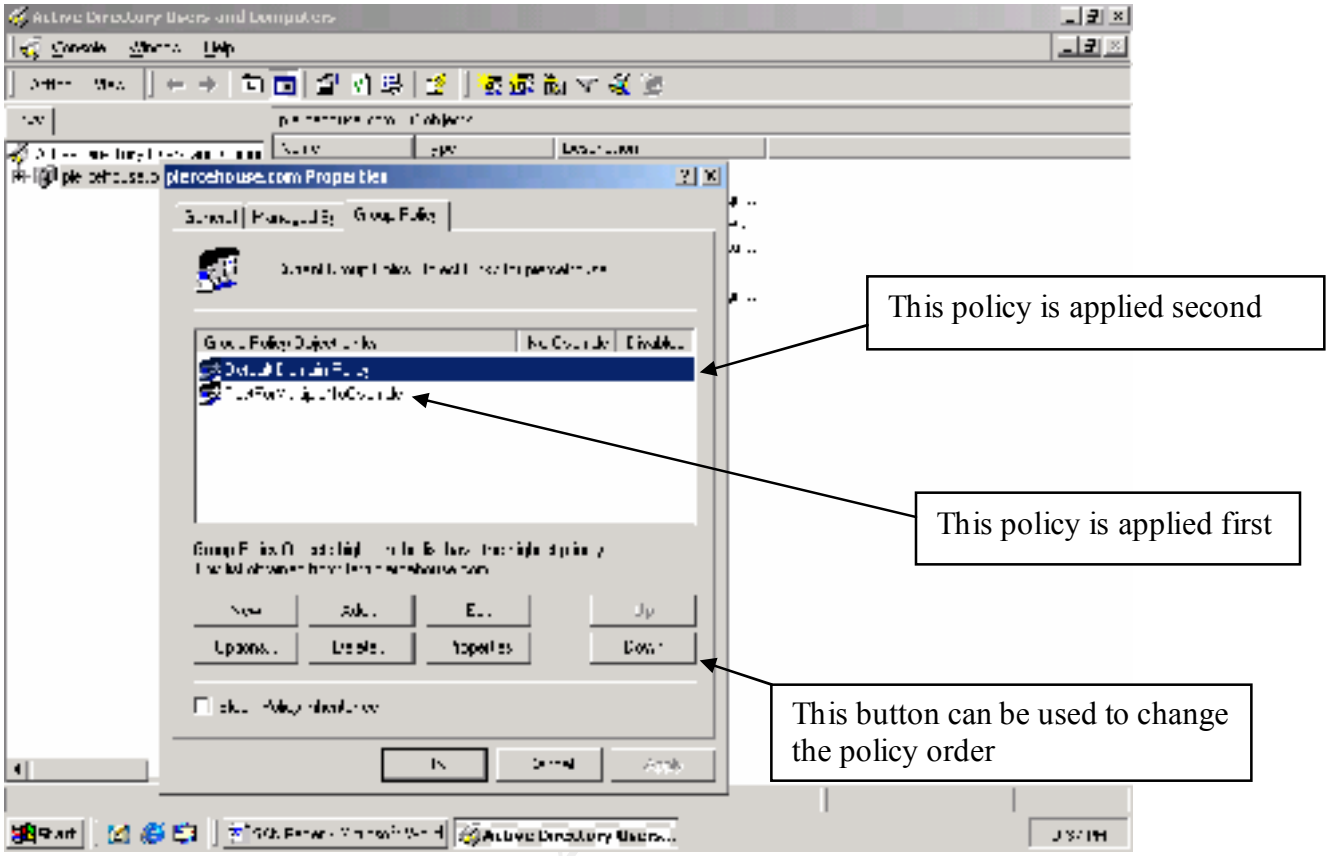
So how do you as the Administrator prevent this from occurring? Windows 2000 allows you to set a no override attribute for a policy that prevents a child object from blocking the inheritance of the policy. To set the no override attribute perform the following steps:

1. Open the Domain Properties window by right clicking on your Domain in the left pane of your Active Directory User and Computers tool.
2. Select the properties item from the menu.
3. Click one time on the screen saver policy to highlight your selection.
4. Click the Options button.
5. In the screen saver password Policy Options window place a check mark in the No Override option.

Upon completion of these steps your screen should look like the figure shown below. By completing these steps the policy will not be blocked or overwritten at a lower level.



Not only can container objects inherit multiple policies from above, the container can also have multiple policies applied directly to it. When the container has multiple policies applied, the order of precedence is opposite than the order of inheritance. This sound confusing but the following illustration should clear this up.




## Security Configuration and Analysis

Now that you have set your security requirements you can now compare them to several security templates provided by Microsoft. These security templates can be located in the %systemroot%\security\templates folder.

The predefined security templates are:

- Default workstation (basicwk.inf)
- Default server (basicsv.inf)
- Default domain controller (basicdc.inf)
- Compatible workstation or server (compatws.inf)
- Secure workstation or server (securews.inf)
- Highly secure workstation or server (hisecws.inf)
- Secure domain controller (securedc.inf)
- Highly secure domain controller (hisecdc.inf)

Basic*.inf – "*the basic configuration templates are provided as a means to reverse the application of a different security configuration. The basic configurations apply the Windows 2000 default security settings to all security areas except those pertaining to user rights. These are not modified in the basic templates because application setup programs commonly modify user rights, to enable successful use of the application. It is not the intent of the basic configuration files to undo such modifications.*"

Compatws.inf- "*The compatible workstation or server template. The default Windows 2000 security configuration gives members of the local Users group strict security settings, while members of the local Power Users group have security settings that are compatible with Windows NT 4.0 user assignments. This default configuration enables certified Windows 2000 applications to run in the standard Windows environment for Users, while still allowing applications that are not certified for Windows 2000 to run successfully under the less secure Power Users configuration. However, if Windows 2000 users are members of the Power Users group in order to run applications not certified for Windows 2000, this may be too unsecure for some environments. Some organizations may find it preferable to assign users, by default, only as members of the Users group and then decrease the security privileges for the Users group to the level where applications not certified for Windows 2000 run successfully. The compatible template is designed for such organizations. By lowering the security levels on specific files, folders, and registry keys that are commonly accessed by applications, the compatible template allows most applications to run successfully under a User context. In addition, since it is assumed that the administrator applying the compatible template does not want users to be Power Users, all members of the Power Users group are removed.*"

Secure*.inf- "*A secure workstation or server template. The secure templates implement recommended security settings for all security areas except files, folders, and registry keys. These are not modified because file system and registry permissions are configured securely by default*."

Hisec*.inf –" *A high security workstation or server template. The highly secure templates define security settings for Windows 2000 network communications. The security areas are set to require maximum protection for network traffic and protocols used between computer running Windows 2000. As a result, such computers configured with a highly secure template can only communicate with other Windows 2000 computers. They will not be able to communicate with computers running Windows 95 or 98 or Windows NT.*"[4]

With these templates and the MMC console it is possible to completely configure your system or compare your setting to these suggested settings. In this demonstration I will compare the values we assigned to the security setting to the hisecws template.

To begin this procedure we must first built the MMC console. Follow the below listed steps to build the Security Configuration and analysis console:

[4] All definitions from the Microsoft Windows 2000Advanced Server help file.

Click the Start button, the click the run button. In the dialog box type mmc and press enter, a blank MMC console will open.

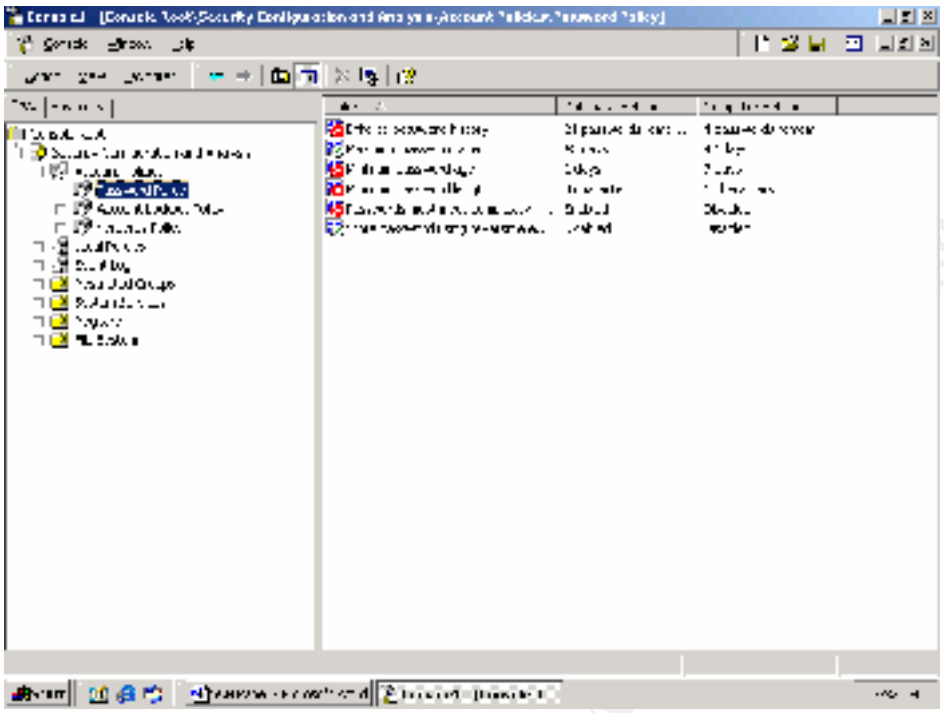
Click Console on the top menu bar and then click the Add/Remove Snap-in menu item. This will open the Add Standalone Snap-in window. Highlight the Security Configuration and Analysis listing and click the add button. Then click the close button. Click the OK button on Add Standalone Snap-in window

Now right click Security Configuration and Analysis in the left pane and click the open database menu item. The Open Database window will open and allow you to supply a database name. After typing in a name of your choice click the Open button. The Import Template window will now open allowing you to select one of the templates already discussed.

Select the hisecws template and click the open button. After a couple of seconds the Open Database window will close and you will be back at the Console. Right-click the Security Configuration and Analysis scope item in the left pane and select Analyze Computer Now. In the dialog, type the log file path or accept the default entry, and then click OK.

The Analyze System Security window will open and the various areas will be analyzed and compared to the HISECWS template. When the analysis is completed the window will close and you will be returned to the MMC console.

To compare your settings to the suggested settings in the template click the plus sign next to the area you wish to review in the left pane. For this example we will review the Password Policy that is under the Account Policy section. Click the plus sign next to Account Policy and then click on Password Policy. Your MMC console should now resemble the figure below.



In the right pane you will see three columns, the policy column, the Database column and the Computer Settings column. The Database column displays the values set by the template. The Computer column displays your current settings. Look closely at the icon to the left of the Policy column. You should see a red circle with an X or a white circle with a green check mark. The red X indicates your current setting does not meet the requirements of the template. The green checks indicate your settings match the templates settings. If your settings exceed the template settings there is neither a check mark nor X displayed.

From this point you can now configure the template to match your policy setting and then save this new template as a custom template to be applied to other computers within your domain. The following section will describe how to edit the template, apply it to your computer and save it for distribution to other computers.

From the figure above you can see I have set my Enforce Password History to 4 remembered password and the template's value is set to 24. 24 passwords remembered would cause my users to rebel so I am going to edit the template to match my company policy. To perform this task complete the following steps:

Double click the Enforce Password History listing, the Analyzed Security Policy Setting window will open. Change the number 24 to the number 4 and click the OK button.

Continue to review the template setting and compare to your policy, making changes where necessary. When you have completed the review and edit you can now apply

this template to your computer if necessary and save the template to be applied to other computers in your network.

For demonstration purposes I did not fully configure all of the security settings therefore I want to replace my existing computer settings with the edited security template. I will first save the newly created template and then apply it to my domain. If I did not make any changes in the template there would be no need to save it, I could just apply it to my computer.

To save the new template perform the following procedure:

Right click Security Configuration and Analysis and click the **SAVE** menu item. Right click on Security Configuration and Analysis again and click the **EXPORT TEMPLATE** menu item. When the **EXPORT TEMPLATE TO** window appears type in a name for your new template and click the **SAVE** button.

You have now created a new template and saved this template for later use. You now need to configure your computer to the new template settings. To complete this task perform the following steps.

Right click Security Configuration and Analysis, click the **CONFIGURE COMPUTER NOW** menu item. Accept the default location for the log file location and name or enter your own. Click the **OK** button, the Configure Computer Security window will open and configure the various areas. When the Configure Computer Security window closes your computer has now been configured with your template settings. To verify your settings have been applied you can reanalyze the computer and confirm the computer setting match the new template.

Congratulations you have now completed the security configuration for all of the computers within your domain. If you have a multi domain environment you could copy the security template you designed, place it on one of your domain controllers in the other domain and use it to configure all the computers in that domain by using the Security Configuration and Analysis snap in.

References:


1. Windows 2000 Security Handbook
2. Microsoft Official Curriculum #2150A Designing a Secure Microsoft Windows 2000 Network
3. Microsoft Windows 2000 Server White Paper Security Configuration Tool Set
4. Microsoft Windows 2000 Server White Paper Step-by-Step Guide to Configuring Enterprise Security Policies


[i] Windows 2000 Security Handbook

Last Updated: September 24th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **Secure DevOps Summit & Training** | **Denver, CO** | **Oct 10, 2017 - Oct 17, 2017** | **Live Event** |
| **SANS San Francisco Winter 2017** | **San Francisco, CA** | **Nov 27, 2017 - Dec 02, 2017** | **Live Event** |
| **San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation** | **San Francisco, CA** | **Nov 27, 2017 - Dec 02, 2017** | **vLive** |
| **SANS Cyber Defense Initiative 2017** | **Washington, DC** | **Dec 12, 2017 - Dec 19, 2017** | **Live Event** |
| **SANS Southern California- Anaheim 2018** | **Anaheim, CA** | **Feb 12, 2018 - Feb 17, 2018** | **Live Event** |
| **Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation** | **Anaheim, CA** | **Feb 12, 2018 - Feb 17, 2018** | **vLive** |
| **SANS 2018** | **Orlando, FL** | **Apr 03, 2018 - Apr 10, 2018** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |