Global Information Assurance Certification Paper

Step-by-Step Procedures for Implementing a Security System Policy Using the System Policy Editor

Reynold T. Hioki

June 12, 2000

Introduction

Administering a large organization's NT systems can quickly become unmanageable as the continually changing environment demands corresponding system changes in response. Furthermore, when required changes are security-related, immediate attention must usually be provided at the cost of rescheduling or completely eliminating other critical but competing projects. Although the inexperienced administrator initially responds using manual and time consuming methods, with experience, the same administrator searches and eventually finds automation tools that can reduce manual times by several magnitudes.

The Windows NT built-in system registry configuration tool, System Policy Editor (SPE), provides the ability to automatically and dynamically configure many security-related registry settings that would take much longer to complete manually. Additionally, by writing custom system policy templates, or ADM files, SPE capabilities can be extended to accomplish an almost unlimited number of system registry changes.

This document provides step-by-step procedures to implement several security-related system policy settings using SPE. Due to the large number of available security-related settings and the limited scope of this paper, this author has selected five highly useful settings representative of options available. Furthermore, by applying techniques outlined in this paper, many more NT registry settings can also be configured by developing custom templates.

Following are the security-related settings discussed in this paper:

User-specific SPE settings
- Setting a default background wallpaper bitmap
- Setting a default Screen Saver

Computer-specific SPE settings
- Setting password authentication level
- Setting a default logon banner
- Disable displaying last logged on username

Where appropriate, hints, tips and tweaks learned through the author's experiences with SPE are presented as notes to minimize implementation time for the reader. Lastly, while system policies

can be used with Windows 9x, only Windows NT 4.0 systems in a domain configuration are discussed here.

NOTE: System policies do not work in a Windows NT 3.x environment.

System Policy Editor (SPE)

System Policy Editor (SPE) allows for the automated configuration of a system's registry settings during each normal user logon process. During logon, changes to settings that affect the local machine and/or the current user are carried out by modifying the system's HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER registry hives, respectively. These changes can be selectively applied to domain systems in several ways to include the following:

Computer-specific
a. A specific computer
b. All computers in the domain

User-specific
a. A specific user
b. A specific global group
c. All users in the domain

Since machines and users can be affected by multiple policies, SPE applies precedence rules to resolve which policy will override the other. For example, if a certain registry setting is defined in both a specific user policy and group policy, the specific user policy will always take precedence over the group policy. The precedence hierarchy rules followed by the SPE are listed below in Table 1.

	User-Specific	**Machine-Specific**
Highest Precedence		
	Specific User	
	Group Policy	Specific Computer
	Default Policy	Default Computer
	User Profile	Hardware Profile
Lowest Precedence		

Table 1. System Policy Editor Precedence Hierarchy

The ability to use a system policy occurs by default for NT systems. However, to enable it, the administrator must first use SPE to build a system policy file and then save it as NTCONFIG.POL to all domain NETLOGON shares for use during logon. To propagate the system policy file to all domain NETLOGON shares, the built-in Windows NT directory replication service can be used. Once the system policy file is saved and propagated, the settings

within the system policy file are activated on all assigned systems following the next logon. The remainder of this paper will provide step-by-step procedures for implementing a domain-wide security system policy using SPE. In step one, the directory replication service will be configured to synchronize the system policy file to each domain controller's NETLOGON share. Step two will provide procedures to design a custom system policy template required to implement security features not included with the default Windows NT templates. And lastly, step three will implement a domain-wide security system policy using standard and custom templates.

Throughout this paper, a two-server network model will be used to demonstrate all procedures provided. Figure 1 below details the naming convention used by this model.

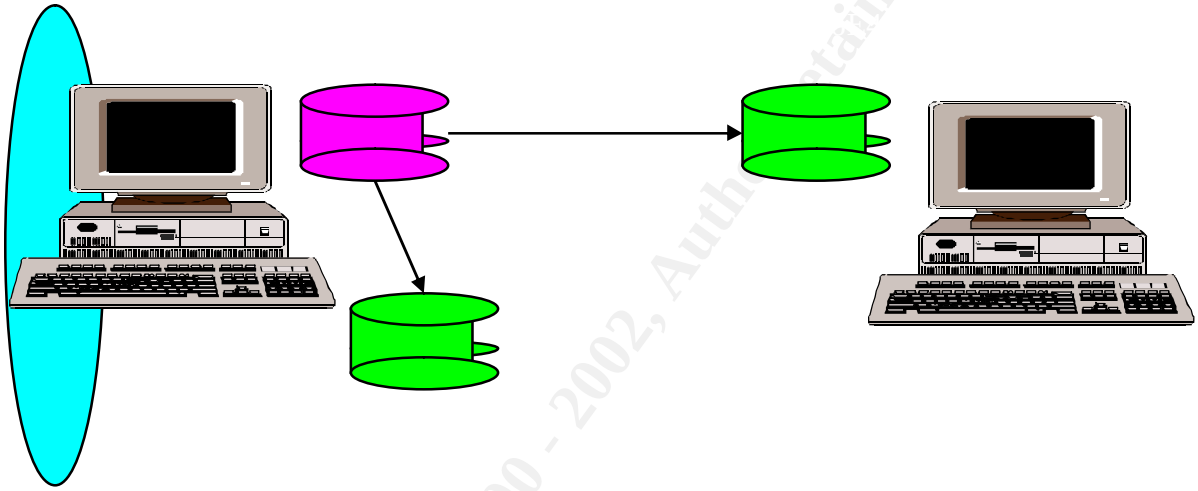

Figure 1. Two-Server Network Model

Step One – Implementing Directory Replication

To implement a system policy, the system policy file (i.e., NTCONFIG.POL) must be placed in the NETLOGON share of each domain controller. To accomplish this, the Windows NT built-in directory replication service can be used. In general, this process starts by first configuring the export and import servers. Once configured, the export server will automatically copy the contents of its export directory to the import directory of all import servers. By default, the export directory is located at %SystemRoot%\system32\Repl\Export\Scripts and the import directory is located at %SystemRoot%\system32\Repl\Import\Scripts. The import directory is also referred to as the NETLOGON share and, as mentioned above, is the default location that the NTCONFIG.POL is placed to activate a system policy. Once the directory replication service is started, NTCONFIG.POL synchronization between the export server and all import servers occurs. Lastly, by default, any changes that occur to NTCONFIG.POL on the export server are propagated to all import servers within five minutes. As presented in Figure 1 above, the PDC server is an export and import server while the BDC is only an import server.

NOTE: Any changes to NTCONFIG.POL on import servers will be overwritten with the latest version of the NTCONFIG.POL from the export server.

To configure the directory replication service on the PDC, follow the procedures below.

1. Create a Directory Replication service account
   a. Logon to PDC with Administrator rights.
   b. Select Start|Programs|Administrative Tools|User Manager for Domains.
   c. Create new user DirRep (or any descriptive name). Uncheck the *Change Password at Next Logon* option. Check *Password Never Expires* checkbox.
   d. Add DirRep to the *Replicator* and *Backup Operators* local group.
   e. Select Policies|User Rights and click the *Show Advanced User Rights*. Select the *Logon as a Service* right. Click Add and add user DirRep.
   f. Exit User Manager for Domains.

2. Configure Directory Replication service
   a. Select Start|Programs|Administrative Tools|Server Manager.
   b. Highlight the PDC and select Computer|Services.
   c. Select the Director Replicator service and click Startup.
   d. At top left, select Automatic (see Figure 2 below).
   e. Select *This Account*, click ellipsis button, select DirRep, and enter password twice.
   f. Click OK then Close.

Figure 2. PDC Directory Replication Service Settings

3. Configuring Directory Replication
   a. Go back to Server Manager and double-click PDC.
   b. Click *Replication* (see Figure 3 below).
   c. On left, select *Export Directories* (Note: default path appears).
   d. On left, select Add. Double-click DOMAIN and double-click PDC.
   e. On left, select Add. Double-click DOMAIN and double-click BDC.
   f. On right, select *Import Directories* (Note: default path appears).
   g. On right, select Add. Double-click DOMAIN and double-click PDC. Click OK.
   h. The Directory Replication service will start automatically. Click OK.

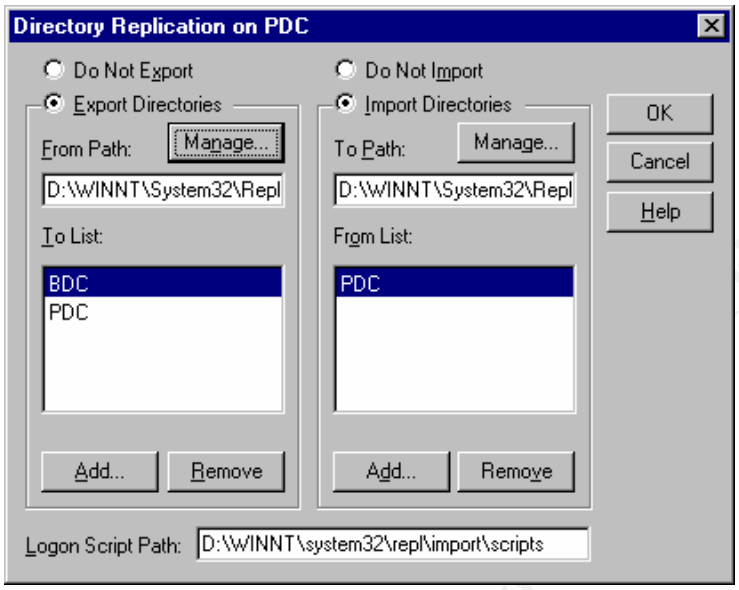

Figure 3. PDC Directory Replication Settings

To configure the directory replication service on the BDC, follow the procedures below.

1. Configure Directory Replication service
   a. On PDC, set focus to Server Manager.
   b. Highlight the BDC and select Computer|Services.
   c. Select the Director Replicator service and click Startup.
   d. At top left, select Automatic (see Figure 4 below).
   e. Select *This Account*, click ellipsis button, select DirRep, and enter password twice.
   f. Click OK then Close.

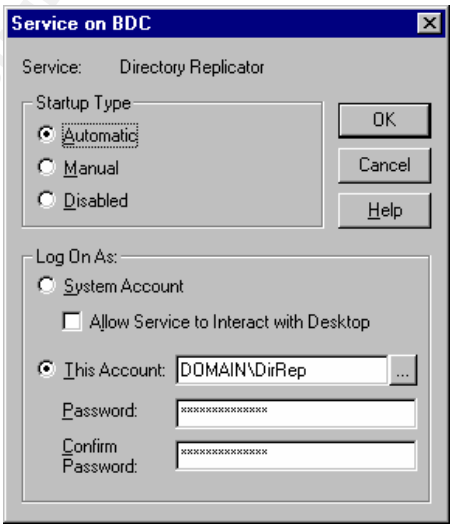

Figure 4. BDC Directory Replication Service Settings

2. Configuring Directory Replication
   a. Go back to Server Manager and double-click BDC.
   b. Next, click *Replication* (see Figure 5 below).
   c. On right, select Import Directories (Note: default path appears).
   d. On right, select Add. Double-click DOMAIN and double-click PDC. Click OK.
   e. The Directory Replication service will start automatically. Click OK.
   f. Exit Server Manager.

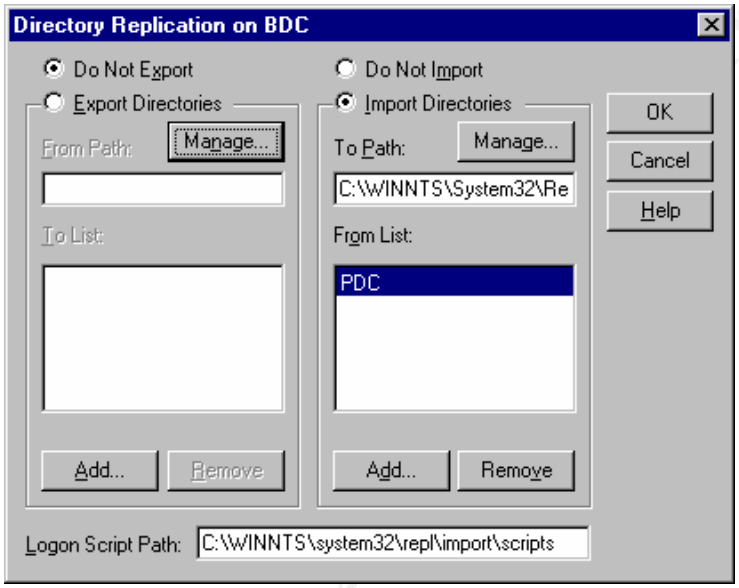

Figure 5. BDC Directory Replication Settings

To test the directory replication service, follow the procedures below.

1. Create a file in the PDC \WINNT\system32\Repl\Export\Scripts directory and name with current date and time (e.g., TestFile000528.1000 for 10:00 am on May 28, 2000).
2. Confirm file automatically copies over to all import shares within 5 minutes.

NOTE: In the event the directory replication fails, stop and restart the Directory Replication service on each server.

Once the directory replication service is active, the next step is building a custom system policy template for custom settings not included with the default. By building custom templates, administrators can expand SPE's capabilities to modify almost any registry setting.

Step Two - Building a Custom System Policy Template

The most difficult issue with custom templates is determining the registry settings to modify to provide the desired effect. In this example, a technique that identifies the registry changes needed to enable a screen saver with custom settings listed in Table 2 below is presented.

Display Properties	Setting/Values
Screen Saver	Screen Saver=Marquee Display
	Password Protected=Enabled
	Wait=20 Minutes
Settings	Position=Random
	Background Color=Red
	Speed=Slow
	Text="I Will Return Shortly"
Format Text	Font=Arial
	Font Style=Bold
	Size=48
	Color=White

Table 2. Marquee Display Screen Saver Setting Values

The general approach to determining the Marquee Display screen saver registry settings is: 1) take a registry snapshot before screen saver activation, 2) activate screen saver, 3) take a registry snapshot after screen saver activation, and 4) compare snapshots to identify resulting changes. Since screen savers are unique to each user, we can confirm that these settings will only affect the HKEY_CURRENT_USER hive.

For this example, the REGEDIT Registry|Export Registry File feature is used to take snapshots, the Display Applet Screen Saver tab is used to activate the screen saver, and the NT Resource Kit WINDIFF.EXE utility is used to compare registry snapshots.

The procedure below describes, in detail, the process of identifying registry settings to implement the Marquee Display screen saver using the general approach described above.

Identifying Registry Settings for Implementing the Marquee Display screen saver

1. Take a snapshot of the current registry settings
   a. Logon with Administrator rights.
   b. Select Start|Run, type REGEDIT and click OK.
   c. In the left pane, highlight HKEY_CURRENT_USER.
   d. From the menu, select Registry|Export Registry File.
   e. For File Name, type C:\TEMP\BEFORE .REG and click SAVE.
   f. Exit REGEDIT.

2. Enable the Marquee Display screen saver
   a. Select Start|Settings|Control Panel|Display then click the Screen Saver tab (See Figure 6 below).
   b. Select Marquee Display for *Screen Saver*.
   c. Select checkbox for *Password Protection*.
   d. Enter 20 minutes for *Wait*.

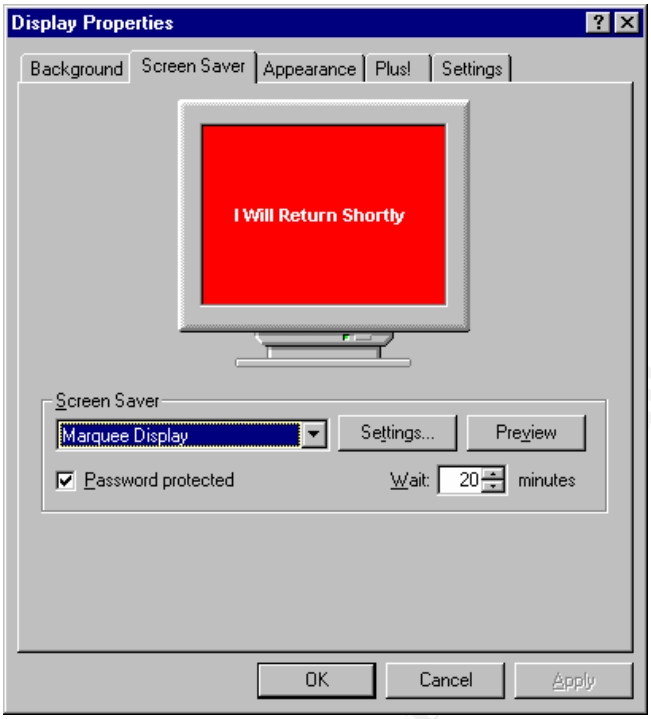

Figure 6. Marquee Display Screen Saver with Password Protection Enabled

e. Click *Settings* button (see Figure 7 below).
f. Select Random for *Position*.
g. Select Slow for *Speed*.
h. Enter "I'll Return Shortly" for *Text*.

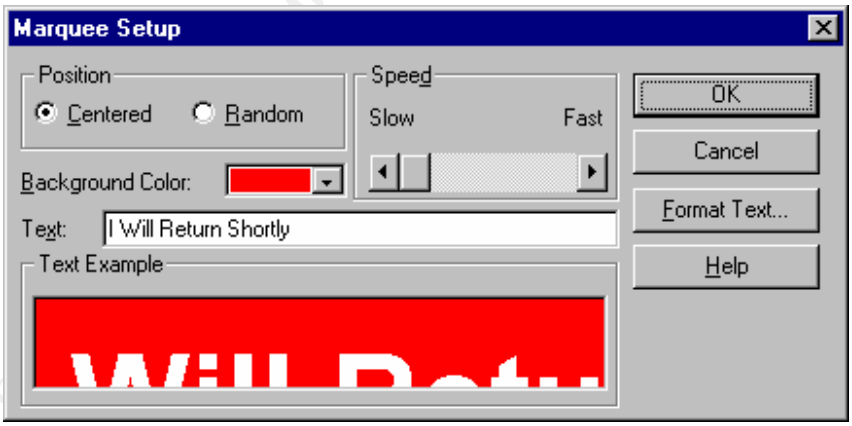

Figure 7. Marquee Display Screen Saver with Various Settings

i. Click *Format Text* button (see Figure 8 below).
j. Select Arial for *Font*.
k. Select Bold for *Font Style*.
l. Select 48 for *Size*.
m. Select White for *Color*.
n. Click OK two times, then Apply and OK.

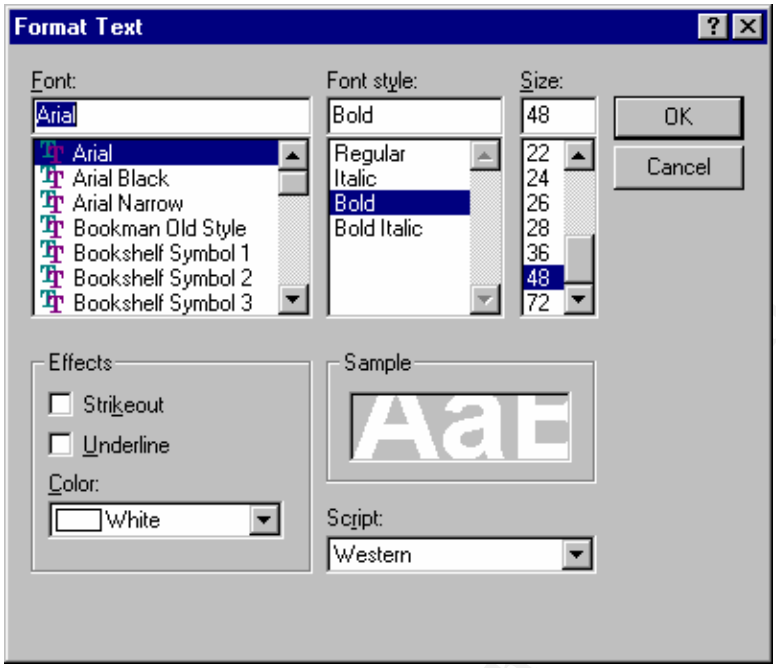

Figure 8. Marquee Display Text Format Settings

3. Take a snapshot of the current registry settings
   a. Select Start|Run and type REGEDIT and click OK.
   b. In the left pane, highlight HKEY_CURRENT_USER.
   c. From the menu, select Registry|Export Registry File.
   d. For File Name, type C:\TEMP\AFTER.REG and click SAVE.
   e. Exit REGEDIT.

4. Compare the BEFORE .REG and AFTER.REG registry setting file contents
   a. Select Start|Run and type WINDIFF.EXE and click OK.
   b. Select File|Compare Files and select C:\TEMP\BEFORE.REG followed by C:\TEMP\AFTER.REG (see Figure 9 below).
   c. Highlight the first (and only) line and click the *Expand* button.
   d. Once expanded, select the F8 as required to view changes.

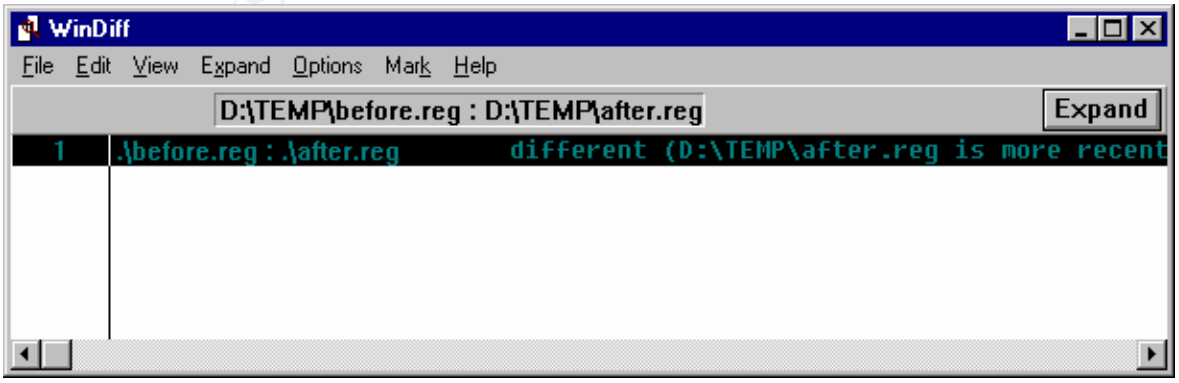

Figure 9. WINDIFF.EXE Loaded with Files to Compare

e. Note changes highlighted in red (before) and yellow (after) between both registry snapshots (See Figures 10 and 11 below).
f. Exit WINNDIFF.EXE.

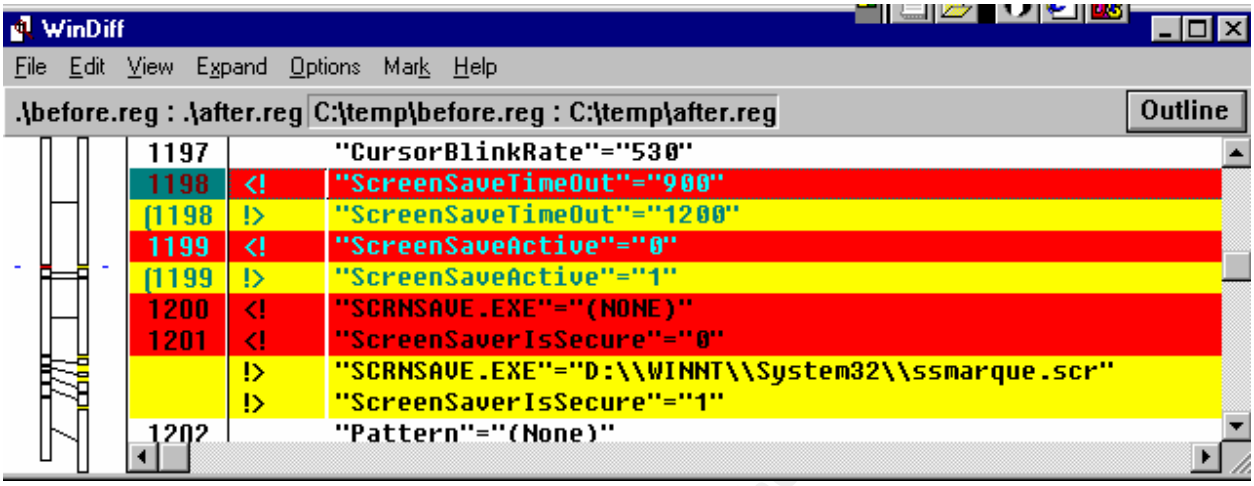

Figure 10. Before (Red) and After (Yellow) Registry Changes to the HKEY_LOCAL_MACHINE Hive After Setting the Marquee Display Screen Saver

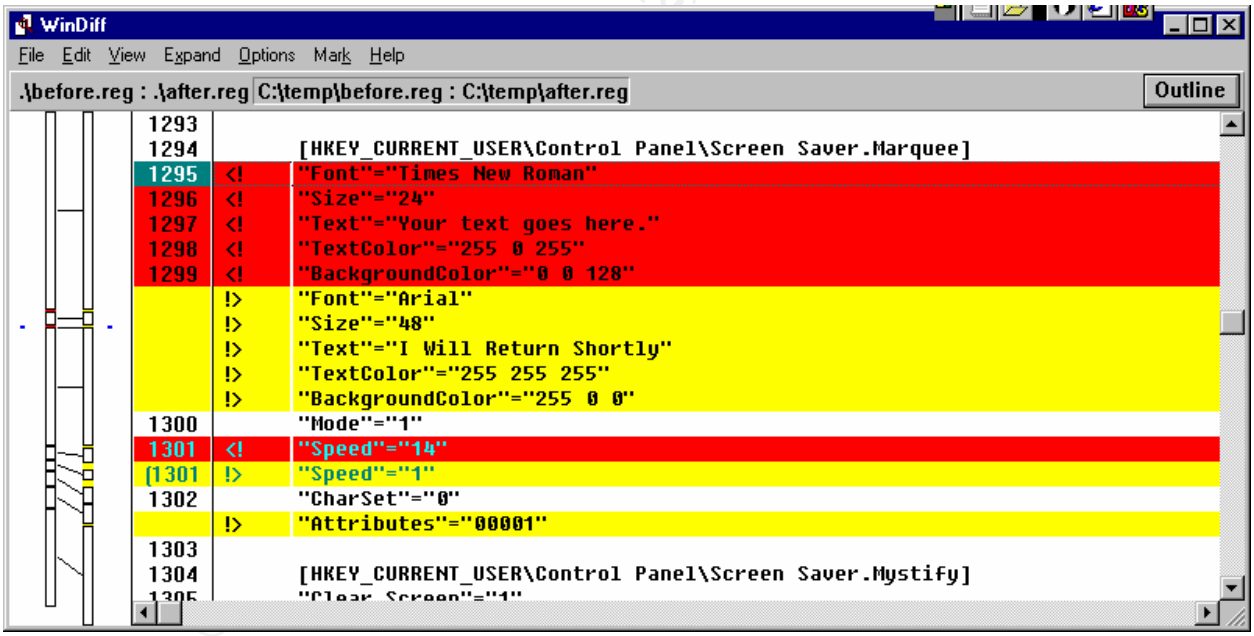

Figure 11. Before (Red) and After (Yellow) Registry Changes to the HKEY_CURRENT_USER Hive After Setting the Marquee Display Screen Saver

Table 3 below summarizes changes identified by the WINDIFF.EXE utility resulting from implementing the Marquee Display screen saver over the default screen saver.

Key/Value	Before	After	Comments
HKEY_CURRENT_USER\ Control Panel\Desktop			Computer-Specific Changes
ScreenSaveTimeOut	900	1200	15 to 20 min
ScreenSaveActive	0	1	Disable/Enable
SCRNSAVE.EXE	(NONE)	D:\\WINNT\\System32\\ssmarque.scr	Screen Saver file selected
ScreenSaverIsSecure	0	1	Disable/Enable password protection
HKEY_CURRENT_USER\ Control Panel\Screen Saver.Marquee			User-Specific Changes
Font	Times New Roman	Arial	Font change
Size	24	48	Font size change
Text	Your text goes here	I'll Return Shortly	Text change
TextColor	255 0 255	255 255 255	Fuchsia to White
BackgroundColor	0 0 128	255 0 0	Blue to Red
Mode	N/A	1	
Speed	14	1	Medium to Slow
CharSet	N/A	0	
Attributes	N/A	00001	Centered to Random and Regular to Bold

Table 3. Summary of Before and After Registry Changes After Setting the Marquee Display Screen Saver

With the registry settings required to build a custom Marquee Display screen saver identified under the *After* column in Table 3 above, developing the custom system policy template is now possible.

Developing A Custom System Policy Template

When developing a custom template, the first step is determining which hive (i.e., HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE) the settings fall under. Fortunately, we already concluded from the previous section that screen saver settings fall under the HKEY_CURRENT_USER hive. Based on this, the first line in our custom template, which identifies the affected hive, is:

CLASS USER

Next, we must name the system policy book our settings will be placed. Since our settings deal with activating the Marquee Display screen saver, we will label our book "Marquee Display Screen Saver" and incorporate it within a CATEGORY/END CATEGORY nesting. Our second

line (and matching nesting termination), which basically provides a label for the category we created, is:

```
CATEGORY "Marquee Display Screen Saver"
    :                                   :
    :                                   :
END CATEGORY
```

The next item allows us to toggle on and off the Marquee Display screen saver system policy and is incorporated within another nesting structure called POLICY/END POLICY. This third entry (and matching nesting termination) is:

```
POLICY "Activate Marquee Display Screen Saver Settings"
    :                                                   :
    :                                                   :
END POLICY
```

The next section is the generic registry path that all settings fall under. Since all settings will go either under HKEY_CURRENT_USER\Control Panel\Desktop or HKEY_CURRENT_USER\ Control Panel\Screen Saver.Marquee, the generic path is HKEY_CURRENT_USER\Control Panel. Since the affected HKEY hive has already been identified with the CLASS statement above, class reference is omitted and the fourth entry is:

```
KEYNAME "Control Panel"
```

In this last section, we will use a special keyword nesting (ACTIONLISTON and END ACTIONLISTON). Following system policy template syntax, the ACTIONLISTON/END ACTIONLISTON keywords allow for setting numerous registry values simultaneously. To use this function, we will embed KEYNAME\VALUENAME pairs for each desired setting. The purpose of the KEYNAME keyword is to describe the specific registry path. The VALUENAME keyword identifies the registry value name being modified while the VALUE keyword identifies the value data. To change the registry settings to reflect the screen saver security system policy presented above in Table 2, the following ACTIONLISTON/END ACTIONLISTON nesting structure with imbedded KEYNAME\VALUENAME pairs as shown below in Listing 1 and make up the fifth and final entry.

```
ACTIONLISTON
   KEYNAME "Control Panel\Desktop"
   VALUENAME "ScreenSaveTimeOut" VALUE "1200"
   KEYNAME "Control Panel\Desktop"
   VALUENAME "ScreenSaveActive" VALUE "1"
   KEYNAME "Control Panel\Desktop"
   VALUENAME "SCRNSAVE.EXE" VALUE "D:\\WINNT\\System32\\ssmarque.scr"
   KEYNAME "Control Panel\Desktop"
   VALUENAME "ScreenSaverIsSecure" VALUE "1"
   KEYNAME "Control Panel\Screen Saver.Marquee"
```

```
  VALUENAME "Font" VALUE "Arial"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Size" VALUE "48"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Text" VALUE "I'll Return Shortly"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "TextColor" VALUE "255 255 255"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "BackgroundColor" VALUE "255 0 0"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Mode" VALUE "1"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Speed" VALUE "1"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "CharSet" VALUE "0"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Attributes" VALUE "00001"
 END ACTIONLISTON
```

Listing 1. ACTIONLISTON/END ACTIONLISTON Nesting

Below, in Listing 2, is the complete Marquee Display screen saver custom system policy template.

```
CLASS USER

 CATEGORY "Marquee Display Screen Saver"
 POLICY "Activate Marquee Display Screen Saver Settings"
 KEYNAME "Control Panel"
 ACTIONLISTON
  KEYNAME "Control Panel\Desktop"
  VALUENAME "ScreenSaveTimeOut" VALUE "1200"
  KEYNAME "Control Panel\Desktop"
  VALUENAME "ScreenSaveActive" VALUE "1"
  KEYNAME "Control Panel\Desktop"
  VALUENAME "SCRNSAVE.EXE" VALUE "D:\\WINNT\\System32\\ssmarque.scr"
  KEYNAME "Control Panel\Desktop"
  VALUENAME "ScreenSaverIsSecure" VALUE "1"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Font" VALUE "Arial"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Size" VALUE "48"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Text" VALUE "I'll Return Shortly"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "TextColor" VALUE "255 255 255"
```

```
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "BackgroundColor" VALUE "255 0 0"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Mode" VALUE "1"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Speed" VALUE "1"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "CharSet" VALUE "0"
  KEYNAME "Control Panel\Screen Saver.Marquee"
  VALUENAME "Attributes" VALUE "00001"

 END ACTIONLISTON
 END POLICY
 END CATEGORY
```

Listing 2. Custom Marquee Display Screen Saver Template

Saving this as a text file under %SYSTEMROOT\WINNT\SYSTEM32\INF with an ADM extension (e.g., SECURITY.ADM), will preposition it for the System Policy Editor to use in developing our security system policy in Step Three.

Using the procedure provided above, a custom template to enable the LMCompatibilityLevel registry setting (e.g., numeric 3) from within the System Policy Editor was developed and is presented below in Listing 3. By adding this template fragment to the file above, the NTLMv2 password hashing algorithm, which modifies the HKEY_LOCAL_MACHINE hive, can be configured along with the Marquee Display screen saver.

```
CLASS MACHINE

 CATEGORY "NTLMv2 Enhanced Password Security"
 POLICY "Activate NTLMv2 Enhanced Password Security”
 KEYNAME "System”
 ACTIONLISTON
  KEYNAME "System\CurrentControlSet\Control\LSA"
  VALUENAME "LMCompatibilityLevel" VALUE NUMERIC 3
 END ACTIONLISTON
 END POLICY
 END CATEGORY
```

Listing 3. Custom NTLMv2 Password Hashing Algorithm Template Fragment

Step Three - Using System Policy Editor to build a domain security system policy

So far, we have activated the directory replication service between domain controllers so that the contents of the export directory automatically synchronize with the NETLOGON shares. Following this, we presented a technique to build custom system policy templates that can be

used to fill-in-the-gap where built-in templates fall short. Now, we will incorporate these steps to develop a domain security system policy. As previously discussed, this policy will automatically modify the system's registry during the logon process to implement the following security-related changes either through the default or custom templates:

User-specific SPE settings
- Setting a default background wallpaper bitmap (default)
- Setting a default Screen Saver for (custom)

Computer-specific SPE settings
- Setting password authentication level (custom)
- Setting a default logon banner (default)
- Disable displaying last logged on username (default)

The procedure below describes, in detail, the steps to build a domain security system policy using SPE.

Building a Domain Security System Policy

1. Build a test user account
   a. Logon to PDC with Administrator rights.
   b. Select Start|Programs|Administrative Tools|User Manager for Domains.
   c. Create a new user called TestUser. Uncheck *Change Password at Next Logon* option.
   d. Select Policies|User Rights and select *Log on Locally*. Click Add and add TestUser.
   e. Exit User Manager for Domains.

2. Open System Policy Editor and Adding a Custom Template
   a. Select Start|Programs|Administrative Tools|System Policy Editor.
   b. Select Options|Policy Template (see Figure 12 below).
   c. Click Add and select SECURITY.ADM template file then OK.
   d. Select File|New Policy

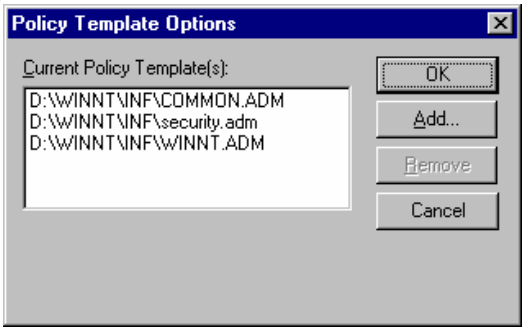

Figure 12. Adding a Custom System Policy Template

3. Create System Policy for TestUser
   a. Select Edit|Add User, enter TestUser and click OK.
   b. Double-click TestUser icon to display all user-specific options (see Figure 13 below).

c. Double-click Desktop book icon.
d. Check checkbox to enable *Wallpaper*.
e. At bottom, type full bitmap location (e.g., C:\winnt\winnt256.bmp)
f. Deselect *Tile Wallpaper* checkbox.
g. Double-click Marquee Display Screen Saver book icon.
h. Enable checkbox for *Activate Marquee Display Screen Saver Settings* and click OK.

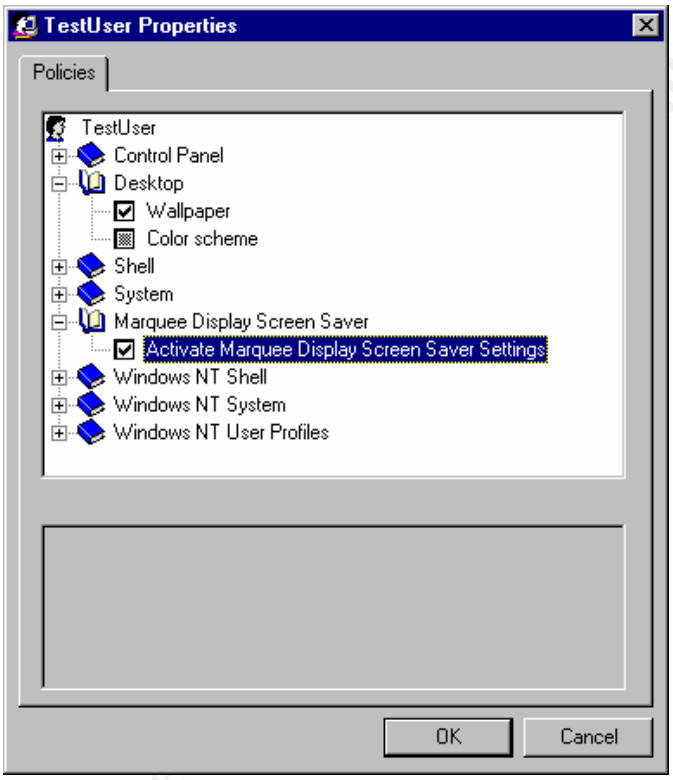

Figure 13. Enabling User-Specific System Policies

4. Create System Policy for BDC
   a. Select Edit|Add Computer, enter BDC and click OK.
   b. Double-click BDC icon to display all computer-specific system policy options (see Figure 14 below).
   c. Double-click NTLMv2 Enhanced Password Security book icon.
   d. Check checkbox to enable *Activate NTLMv2 Enhanced Password Security*.
   e. Double-click Windows NT System book icon then Logon book icon.
   f. Check checkbox to enable *Logon banner*.
   g. At bottom, type the following as a test Logon Banner
      - *Logon Caption*: Important Notice:
      - *Logon Text*: Do not attempt to log on unless you are an authorized user.
   h. Check checkbox to enable *Do not display last logged on username* and click OK.

NOTE: To implement *Logon Text* up to 2048 characters, the latest service pack must be installed and the WINNT.ADM file must be modified.

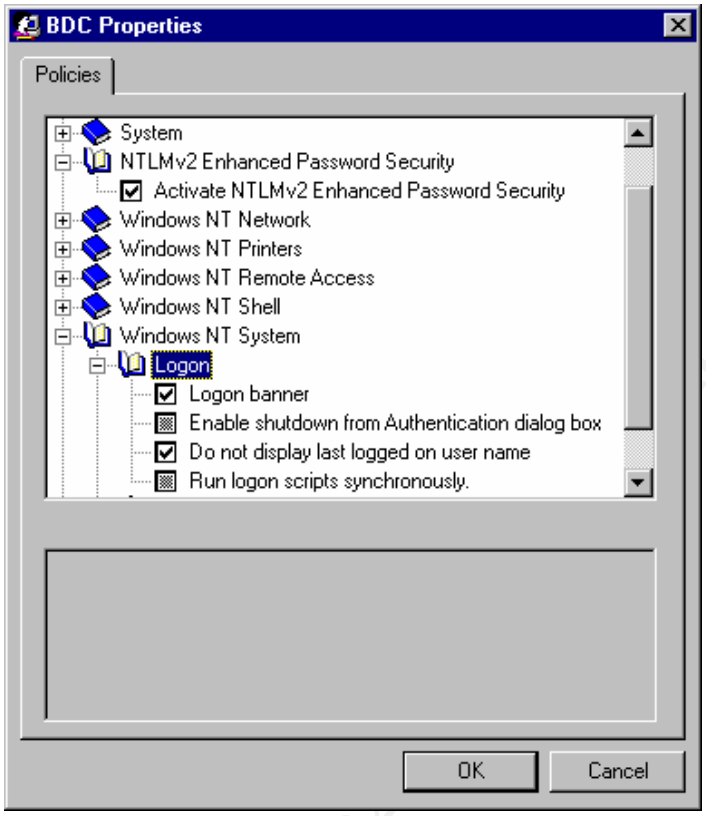

Figure 14. Enabling Computer-Specific System Policies

5. Enabling System Policy Domain-wide
   a. Click File|Save and save to C:\winnt\system32\Repl\Export\Scripts path and NTCONFIG.POL filename.
   b. Close System Policy Editor.

Once saved, the new security system policy will be implemented on the user's workstation during the next logon. In this example, computer- and user-specific registry settings will be modified to meet the five security system policy options configured. If changes are required, the NTCONFIG.POL file must be edited and then resaved to enable the new options.

NOTE: Although users can change registry settings, system policy registry settings will be reset during the next logon sequence.

Summary

Implementing configuration changes domain-wide can be overwhelming if manual methods are used. However, utilizing automated tools to accomplish the same task can result in a significant amount of saved time. Using the Systems Policy Editor with the step-by-step procedures provided, an administrator can automate the manual task of changing system registry settings domain-wide. Compared to manual methods that require the administrator to "touch" each system, administrative efficiencies gained using this approach are tremendous. Keeping utilities like System Policy Editor in one's "toolkit" is what separates the novice administrator from the experienced professional.

References

Fossen, J., & Johansson, J. (2000, April 4). Guide to implementing Windows NT in secure network environments. Fredericksburg, VA: SANS Institute.

Guide to MS Windows profiles and policies. (1997, August). NT Server Technical Notes – Planning. Redmond, WA: Microsoft Press.

HOWTO: How to set a screen saver through a system policy. (1999, February 24). Microsoft TechNet, ID number Q1956550. Redmond, WA: Microsoft Press.

Johnson, C. (1997). Troubleshooting and configuring the Windows NT/95 registry. Indianapolis, IN: SAMS Publishing.

System policy editor will not allow more than 255 characters. (1999, September 1). Microsoft TechNet, ID number Q173385. Redmond, WA: Microsoft Press.

Writing custom adm files for system policy editor. (1999, October 12). Microsoft TechNet, ID number Q225087. Redmond, WA: Microsoft Press.

Last Updated: July 28th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
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**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**