Global Information Assurance Certification Paper

Securing Task Station Computers Using Windows 2000 Group Policy

Roger McClinton
GIAC-GCWN
Version 3.1 Option 2

Abstract

Numerous security checklists and best practices make securing a Windows computer a daunting task. Fortunately in Windows 2000, Microsoft provides tools to make the job easier. This paper will examine the Kiosk Group Policy Template provided by Microsoft and evaluate the effectiveness of the template.

Introduction

At long last, System Administrators realize the need to secure computers to prevent corporate embarrassment and the exposure of data. There are many checklists available that list how to secure Windows 2000 computers. No one checklist can secure every computer. Web servers on a DMZ have a far different need for security than a desktop computer behind a firewall on a corporate LAN. Desktop computers in Payroll may have a completely different need for security than a laptop computer that is loaned out, as needed, to Road Warriors. As a result, there are checklists designed for a specific computer use. The blizzard of documents is heightened by several competing standards for security. NSA, NIST, and Microsoft, among others have documents that shoot for a different level of security. Recently, efforts have been made to form a consensus security document. The Center for Internet Security (http://www.cisecurity.org) has a consensus document commonly referred to as the gold standard that is the sum of many of the existing Windows 2000 security checklists. Even they offer two distinct documents depending on the level of security desired. When configuring a computer, an administrator must make intelligent decisions based on corporate security requirements and the tolerance for risk. It may be helpful to look at multiple security documents to determine for yourself what items really are "best practice" and in what areas you may wish to be more secure.

We have a "town center" area with a refrigerator and couches. Management would like to put a computer there to facilitate the use of the area. Users could check facts quickly on the internet, enter their electronic timecard, check webmail or watch TV news reports. Of course, computers such as this have special security requirements.

Our security people are, of course, concerned. Those computers have the inherent problem that they are accessible to anyone with a badge to access the building. Any employee, temp, contractor or Pepsi delivery person, will be able to walk up to this terminal and use it. There is a severe lack of accountability with anything tracked back to that computer. If there is any questionable activity tracked to the computer, it is impossible to know who specifically performed the action. Also individuals using the computer could be subject to shoulder surfing or terminal hopping. If a user walks way without closing the browser, that session can be assumed by a opportunistic malicious user. Because of these risks, Kiosk computer systems may not be appropriate for a truly secure environment.

There are important considerations to securing a Kiosk computer. Microsoft has provided a Group Policy Template specifically for Kiosk Computers. In this paper, I will examine the security settings of Microsoft's Kiosk Group Policy and its appropriateness for securing a computer.

Description of System

OS:	Windows 2000 Professional
Role:	Task Station Computer
Hardware:	Dell GX150 Matrox Marvel
Software	Internet Explorer 6.0 Matrox Drivers and TV Tuner Software Norton Antivirus Corporate Edition 7.61 SMS 2.0 Netscape 4.73

Role

The task station computer will be placed in a "town center" area on each floor. The "town center" is a common area where employees can interact in small groups in a less formal environment than a conference room. It is envisioned that the computer will be used for the following tasks:

1. Television (Matrox TV Tuner card)
2. Time entry through the web client
3. Internal phone directory (locate the person's office you are visiting)
4. Web mail
5. Web browsing

As a system without individual responsibility, it is important to limit what users are allowed to do on the system. The system cannot be used to circumvent existing corporate requirements. It must be protected from virus and Trojan infection. It must not be used as a staging area for attacks on other computers.

Hardware

The Dell GX150 was the standard desktop model at the time of their purchase. There is nothing unusual about the hardware other than the addition of the Matrox Marvel TV Tuner Card.

The Matrox Marvel video card is an extremely limiting factor. It is not designed to work well with Windows 2000. Testing shows that it only works with the account that installed the software. Compatibility with non-administrator accounts should be a priority when purchasing hardware for a kiosk computer. If possible, peruse any online support forums for problems when used with a non-Administrator account.

Software

The operating system of this computer is Windows 2000 SP3. The hard drive is formatted with NTFS. The latest Service Pack at the time of install should be used. The computer is a member of a domain to allow for management through Group Policy. IP address is obtained through DHCP.

Norton Anti-Virus is commonly used software. In this environment, the local configuration is locked down and controlled though a Norton parent server. The client is controlled through registry settings that are downloaded from a centralized service within the company. This adds to security because the antivirus software cannot be disabled by a user. The configuration on Kiosk computers matches the configuration on all desktop systems.

Norton Anti-Virus Configuration
Real Time Protection: All File Types Scheduled Scans: Sunday and Thursday at 2 AM, All File Types Updates: Daily at 7:30 am (randomized within 60 minutes) via Live Update (Internal FTP Server) Upon File Detection: Attempt to clean and then log only (real-time scan) Attempt to clean and then Quarantine (scheduled scan). Notify administrator via e-mail using Norton Alert Messaging System.

Internet Explorer is used as a web browser. Since Internet Explorer offers such close integration with Windows Explorer, this will be an area to watch. Does Group Policy lock down Internet Explorer so that it is secure?

Netscape is the default browser of this corporation. Although it will not be the default browser on this computer, it must be provided. This is an area

of concern. Netscape has known difficulties working for a user without administrative rights. When we apply the security policy to this computer this is one are we must examine carefully.

Microsoft Systems Management Server is installed, mainly for remote control purposes. It allows administrators to monitor the software that is on the system. It could be used for deploying software patches.

The TV Tuner card has software for changing the channels. It is unknown how the template will affect this.

Questions about the ability of these software packages to work on a kiosk computer will be addressed during the testing process.

The Template

Microsoft provides security templates that can be applied using Group Policy. These templates are available at http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp in a file called intellimirrorsenarios.msi. This file contains 6 scenarios for securing a computer: Kiosk, Task Station, Application Station, Public Computing Environment, Low TCO Desktop, and Laptop. The MSI file also includes a White Paper on installing the scenarios and an Excel document detailing each scenario. These scenarios range from total lockdown with the kiosk template, to the mildly restrictive "Low TCO" template that merely attempts to maintain some control without restricting the user from doing too many things. After examining the different templates, Microsoft's Task Station and Application Station scenarios appear to be too permissive. The Task Station template has similar settings to the kiosk computer except that is designed for use by multiple user accounts. We want one account that is always logged in. Additionally, this template allows users to save data and personalize the configuration.[1] The Application Station scenario has a similar design. This is not secure enough for our environment, so we have chosen to use the kiosk template. It is easier to relax a policy that is too restrictive than it is to tighten a policy.

The kiosk template is designed for computers in a public environment.

[1] "Windows 2000 Server: Using Group Policy Templates White Paper." [http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp]. September 2000, 2.

Although it is designed to run one application, we plan to modify it to allow multiple applications. Because it runs attended, and has users that won't specifically be known, the system is designed to be highly secure, not letting users change configuration or save items to disk.[2]

This template is the closest match for our specific needs. Since it is provided by Microsoft, it is more likely to be supported by Microsoft in the event there are any questions. Also, it comes with clear instructions on how to implement the policy.

Security Settings

The Kiosk template is based on Microsoft's High Security template.[3] Modifications have been made by Microsoft in creating a kiosk template. These changes are listed in the Notes column of kiosk.xls. Some of the notes seem to be questions a developer had that are either included for our consideration or should have been removed prior to releasing the documentation to the public.

When the computer is turned on, it will log in automatically to the kiosk account. By default, the security setting of the template replaces the Windows Shell with Internet Explorer. There is no desktop and no access beyond what can be exploited in Internet Explorer. In our environment, the computers will be used as TV watching terminals in addition to Intranet browsers. The first change to the template is to remove this setting. Upon login, Internet Explorer and the TV Tuner application will be launched automatically.

The prime restriction of this policy is who can log into the computer. Most of the restrictions are applied through the account that is logged on. For that reason, it is mandatory to restrict who can log into the computer. On a restricted use computer there is no reason for individual users to be logging in. It is easier to manage the computer by providing a user settings group policy to one account and have that account be the only one besides the administrator who is allowed to log in locally. Microsoft has made it possible to apply one policy to the same user account at a kiosk station and another policy on every other computer. That is not helpful in this

[2] IBID, 2..

[3] IBID, 24.

computer setting.

The kiosk account is allowed to run only specific programs by the policy. This prevents rogue applications from being used on the machine. We allow Internet Explorer, Netscape, the TV Tuner card, Norton Live Update and Microsoft SMS to be run. This configuration occurs in group policy by the executable name. Even if an executable is loaded onto the machine somehow, the user cannot run it.

It is easy to restrict access to applications that are group policy aware. Microsoft includes specific settings for many of its applications in group policy. Internet Explorer is a key application for this computer. However, there are vulnerabilities in Internet Explorer and its abilities are meshed with Windows Explorer. Hence, it is important to lock down Internet Explorer.

In this template Internet Explorer is prevented from the following:

- Remembering Passwords
- Auto completing URLs
- Changing the home page
- Accessing Internet Options
- Accessing the File menu
- Right click

The use of non-group policy aware software should be considered very carefully. For example, with Netscape it is not possible to remove access to menu items. Each new application should be tested. If it cannot be locked down appropriately, it should not be used where the prime goal is security.

Access is restricted at the desktop level. My Computer, the Control Panel and Network Neighborhood are removed from user access. Start -> Run, is not available to the user. Internet Explorer is restricted from acting as Windows Explorer. This prevents a malicious user from performing any registry related exploits or installing software.

The user is allowed to log off, but access to other buttons on the logon/logoff screen is denied. This keeps the user from attempting to change the password, lock the screen or access task manager. Access to Task Manager would clearly allow the user to attempt to start and stop processes and is not necessary at a task station computer.

Many of the other settings are redundant such as not allowing changes to

the task scheduler. There is no way for the user to access the task scheduler. If there is some sort of policy failure that would allow access to the task scheduler, it is likely that the task scheduler protections would have failed as well.

Apply the Template

The template is applied through group policy. While this could be applied through a local Group Policy, it is easiest to perform through a domain to allow for centralized administration.

The first step in applying this template is to install the scenario files to a local computer. This is done by installing IntelimirrorScenarios.msi.[4] This will install Microsoft's 6 Group Policy scenarios to the local computer along with the Group Policy Scenario White Paper and scripts designed to install the Policy scenarios into Active Directory.

The second step is to install the scenarios on a domain controller. Note: you must have sufficient rights to perform this action. To install the scenarios to a domain controller run loadpol.bat which by default will be in %ProgramFiles%\Group Policy Scenarios on the computer you ran IntellimirrorScenarios.msi. This batch file will create 12 Group Policy Objects (GPOs) on the domain controller you are currently logged into. The Kiosk Computer Policy and the Kiosk User Policy are the templates that we will be using. The other Group Policy Objects are not needed for this exercise.

Next, open Active Directory Users and Computers and create an Organizational Unit (OU). The location of that OU is a function of your existing Active Directory Structure. Open the Properties of that OU, and select the Group Policy tab. Add the Kiosk Computer Group Policy and the Kiosk User Group Policy. Create a new Security Group in Active Directory for Kiosk Users and Kiosk Computers. Create a kiosk account. Add the kiosk account to the Kiosk Users Group. Move the Kiosk account to the OU that you created. Set permissions on the OU and the group policy so that members of the kiosk users and kiosk computers can apply the group

[4] Available at http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp. This file formerly known as Group Policy Senarios.msi. Microsoft changed the name of this file since I downloaded it.

policy. Make your kiosk computers members of the kiosk computers group and move them to OU that you created.

Lastly, log in with the kiosk account you created and verify that the policy has been applied at both the computer and user level.

To apply the policy to additional systems, you should merely have to add the computer to the kiosk computer security group and move the computer to the OU you created.

Template Maintenance and Updates

Maintenance of the policy is automatic. Within Group Policy, you can set it to refresh at a given interval. In this case, the policy is set to refresh every ten minutes. In larger implementations, this may cause unnecessary network traffic. Change this setting as necessary. Any changes to the Group Policy Object will propagate automatically. However, it is still a good idea to monitor the systems and reboot if the policy is not applied correctly.

Updates to the software can be performed quite easily if the update is supplied with a MSI file. You merely need to create a computer policy to install the given software and reboot the computer. If permissions need to be changed on a registry key or on a file, this can also be performed using Group Policy.

Software updates not in the form of a MSI file, such as patches, are more problematic. If a patch is in the form of an executable and you have existing script writing skills, you can use a computer based log-in script. Some testing should be performed to ensure this works. The software must be able to be installed without the user having administrative rights. It also must not require the ability to write to any new directories. Software that is not user profile aware can be a problem. With a small number of Kiosks, I have I can use Microsoft SMS to log in as the Administrator and manually make changes.

Microsoft Software Update Services

Software patches can be applied easily and uniformly through the use of Microsoft Software Update Services (SUS). With SUS a central server is designated as the update center. Through group policy, the kiosk computers can be told which server to get updates from, when to get the

updates and when to install them.

There are limitations to SUS:

- It cannot be installed on a domain controller[5]
- It cannot deploy service packs
- SUS will run the IIS Lockdown utility on the corporate update server. Verify this will not interfere with any other web services on the server.
- Non-administrator users have no control over when patches are applied or when the system is rebooted after applying those patches.
- Can only deploy patches approved by Microsoft.

Of these limitations, the most important to be aware of is the lack of control for non-administrator users. Through Group Policy you must set updates to be downloaded automatically and installed at a set time. A non-administrator will never be notified that updates are available. Schedule the installation of patches for late at night, the computer will reboot automatically after the patch is applied. The security template allows the kiosk user account to log in automatically returning the computer to a useable state.

The updates available to the clients managed through Software Update Services must be approved by the Administrator. This is accomplished through a website. Using Internet Explorer 5.5 or later, go to http://<yourservername>/SUSAdmin. Note that you must be a member of the local administrators group on the computer running SUS.[6] You will only be able to see patches that Microsoft has made available. Patches may be available for direct download as part of a security bulliten before they are made available at Windows Update (http://windowsupdate.microsoft.com). There is a similar delay in availability for SUS.

The SUS client is included in Service Pack 3 for Windows 2000. By including the latest Service Pack in the Windows install, the SUS client does not have to be installed separately on each client. Some administrators have reported errors trying to install the SUS client on a

[5] Microsoft Software Update Services FAQ. [http://www.microsoft.com/windows2000/windows/update/sus/susfaq.asp]. June 2002.

[6] "Software Update Services Deployment Whitepaper." [http://www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp]. June 2002, 12.

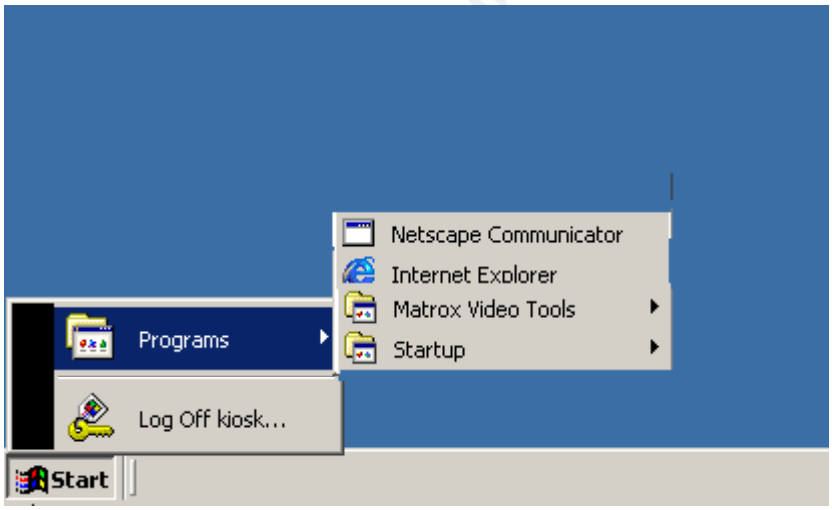
Windows 2000 SP3 computer. The error is generated because the client was released separately as a stopgap measure until Service Pack 3 was released. Do not attempt to install the stand alone client on a Windows 2000 SP3 computer.

Test the Template

Creating a template is only half the work. The most important part is verifying that it is applied correctly. A kiosk computer is going to be open to a wide variety of users and any problems will likely not be reported by them.

Start Menu

The first item to test is whether the controls on the start menu are applied correctly. As you can see from the screenshot, the Start Menu now consists of the programs that we want the user to be able to run. The template does recommend removing the "Log off" option. I found it helpful to have on the screen. If someone were to log the kiosk user out, the worst case scenario is the kiosk would not be useable. There is no security problem with leaving that there. Run, Help, Search, and Settings are now inaccessible to the user. The Run option would effectively give the user access to the command line.



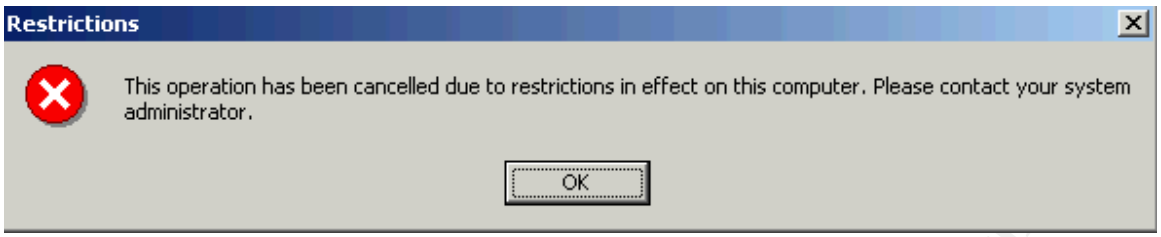
Desktop

At the desktop, there are only icons for the approved applications. Icons for My Computer, Network Neighborhood and My Documents have been removed. Clearly the user will have no need to be browsing the computers hard drive or changing network settings.

Software Installation

Next it is important to make sure that users cannot download their own software to the system. Specifically, there is concern that the computer not be used as a platform for hacking other computer. An attempt to install Packetstorm's SMBDIE evaluates whether or not this is possible. This program takes advantage of a recent SMB buffer overflow to force a reboot on remote unpatched systems. An attempt to install the software resulted in the following error:

Downloading an executable that does not require unzipping or installing tested a different way to get unapproved software onto the system. Putty is a telnet/SSH application that runs by running the executable without installing any other component. An attempt to download this file using http forced us to save the file to disk. Trying to save the file to disk resulted in the following error.

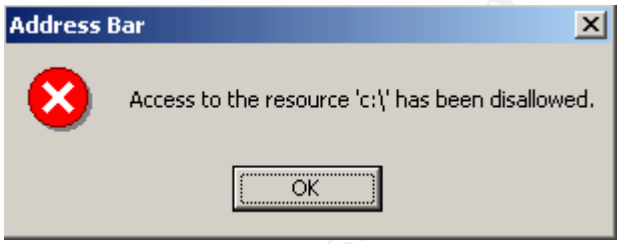


An attempt to download putty via FTP and run it without saving it to disk resulted in the original "Access to the specified device, path or file is denied" error.

Internet Explorer Security

Internet Explorer's integration with Windows Explorer can be a major security problem. Of course, anyone who subscribes to Microsoft Security Bulletins is already aware of this. SANS lists Internet Explorer as one of the top ten windows vulnerabilities.[7] It is important to make sure the policy has been applied and to patch Internet Explorer religiously.

In the address window, type c:\. On a computer that is not locked down, the expect result is to see the C:\ drive. Fortunately the policy works correctly and the user receives a message indicating that accessing the c:\ drive is not allowed. This is one of the rare times the error message is direct and understandable.



There is one item in Internet Explorer that is not locked down. For some unknown reason a user can type ftp://computer.domain.com into the address bar and successfully access remote sites. Telnet and Gopher are disabled. Yet FTP works. Fortunately as we have already demonstrated, the account does not have permission to save the file. Even if the file could be saved, it would not be on the list of files that can be run.

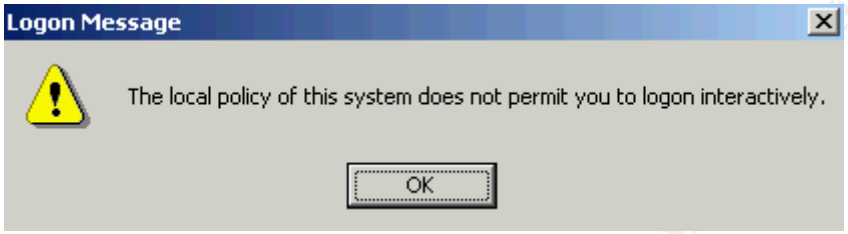
Unfortunately the name of files that can be run is not backed up by an md5

[7] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus" [http://www.sans.org/top20/#W8], October 2002.

hash check or even the requirement to be in the correct file path. If a hacker calls his file iexplore.exe it will be able to run. Of course, there is still the problem of getting it onto the computer.

Operating System Restrictions

All of the restrictions on the kiosk account are meaningless if users are able to log into the computer using their own account. To verify that users without the "logon locally" right cannot access the computer, attempt to log in with another account. The result is, as expected, a message that the user does not have sufficient permissions to log in.



Select Control – Alt – Delete and verify the user restrictions are in effect. The ability to lock the computer, shutdown or change the password has been removed. As mentioned previously, the Log Off option will remain available in our environment to ease troubleshooting. This eases troubleshooting because while at the computer a technician will be able to log the kiosk account out and log in as an administrator. If the logout option were not available, the technician would have to log out the user from a remote computer in order to access the machine in a non-restricted environment.

Testing System Functionality

The tightening of security settings may have unintended consequences. Many programs are written as if security is not a concern and every user is the administrator. Programmers do not write profile aware programs. If files were stored in the correct location, there would not be nearly as much difficultly in locking down systems. Users generally have the ability to write to files in their user profile and in the Application Data folder. Applications that store everything in Program Files will likely not have the correct access rights. Every new application must be tried in a test environment so you know what settings must be changed at the desktop level. Otherwise, the rollout of a new application will not be smooth. Often newer versions of programs have been designed correctly, largely through the influence of corporations with a large deployment of Windows 2000 computers.

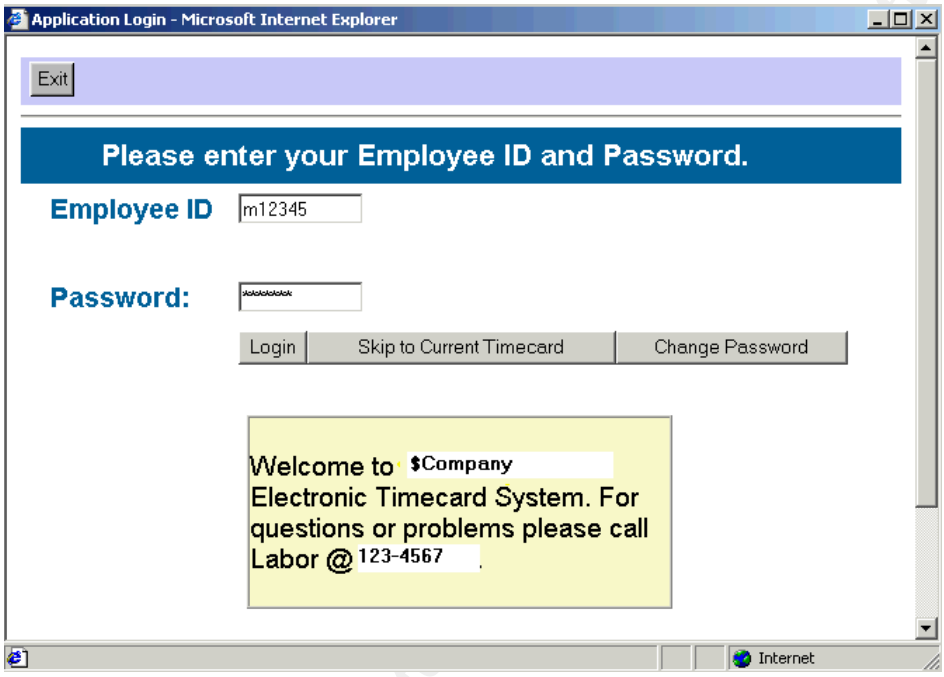
Testing of system functionality may be a final step before deployment, but it is likely to be part of the installation process as well. This should be where the errors are found and corrected. It is far better to a have a refined procedure to apply to all kiosk workstations, than to have to take steps on each machine.

Testing IE

If Internet Explorer does not work with Group Policy restrictions, few

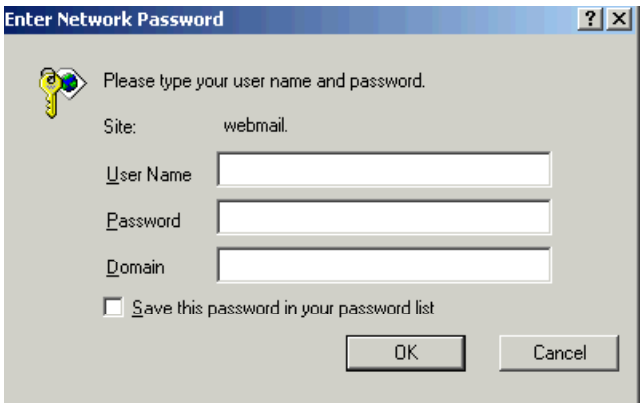
applications will. Since it is from Microsoft, Internet Explorer settings can be controlled through Group Policy. I have IE launching automatically and going to the Intranet homepage. So we have verified that this works out of the box.

One of the uses of the computer will be used to enter electronic time via a web based application. To verify that this works, from the Intranet Homepage we select the "Timecard" link. This takes us to http://timecard.domain.com/cgi-bin/uwe_etstart.



We are able to log into the timecard system and enter time correctly.

Accessing email is another likely use of this station. In the address field of Internet Explorer, enter the address of the web mail server. In this case, it is https://webmail.domain.com. When accessing this address, the user is prompted to log in.



After logging in, the user has access to their mailbox which includes mail, calendar and contacts. There are two problems. The user is able to save the password and it is available even after closing and opening the browser. Also, there is not a login timeout that would prevent shoulder surfing where someone takes your place at the kiosk after you forget to sign out and walk away.

There is a specific group policy for Internet Explorer called *Do Not Allow Auto-Complete to Save Passwords.* This policy is enabled. That should mean that the password is not saved. In situation such as this when a policy does not do what you expect, you can open the properties for that policy and select the Explain tab for clarification.

In this case, the description reveals that it does not do what is expected. It grays out the *Prompt Me to Save Passwords* checkbox and it disables the automatic completion of usernames and password in forms and on web pages. However, the "gotcha" is the last paragraph. When *Disable the Content Page* is enabled, the *Do Not Allow Auto-Complete to Save Passwords* is ignored.

Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.

If you enable this policy, the User Names and Passwords on Forms and Prompt Me to Save Passwords check boxes appear dimmed. To display these check boxes, users open the Internet Options dialog box, click the Content tab, and then click the AutoComplete button.

If you disable this policy or don't configure it, users can determine whether Internet Explorer automatically completes user names and passwords on forms and prompts them to save passwords.

The "Disable the Content page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Content tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

The solution then is to not enable the *Disable the Content Page* policy. Access to Internet Options is already disabled in Internet Explorer. Access to the Control Panel, another method to access Internet Options, is disabled as well.

The second Internet Explorer problem is more difficult. Without a timeout on the Outlook Web Access log in, it is possible that a user will walk away leaving themselves logged in. I am not able to discover a programmatic way to solve this problem. This is one problem that may have to be addressed through signage and user education.

Group Policy does allow for the profile to be logged out after a specified period of inactivity. No time out would really be short enough to prevent someone else from walking up and assuming the credentials signed into webmail. Also, the frequent logouts could potentially cause software problems. It does not lend itself to a conducive computing environment.

Testing the TV Tuner Card

When attempting to use the TV Tuner card for the first time, an error is received stating that the software would only run with Administrative rights. After some investigation, it was determined that the software also would only run for the user who installed it. Otherwise there would be errors that said no compatible video card is installed. Temporarily granting the kiosk account administrative rights allowed the installation of the video card and the correlating TV Tuner software. After removing the administrative rights, the original error was no longer a problem. Some software places

important information in the current user profile rather than in “all users.” This makes the software unusable for other users. Since this computer will only be used by one account, this is not a major problem. If we had attempted to allow any user to log into the system, the video card would not have worked for them.

After resolving the initial errors, the TV Tuner software is found to be giving a different error message. This message said, “This Program has generated an error.” This is not the most helpful error message in the world.

Many times program errors occur while using an account with restricted user rights. Regmon and Filemon from SysInternals can be used to determine whether registry or NTFS file permissions are causing the problem. After removing the kiosk user and computer accounts from the OU associated with the kiosk policy, the machine was rebooted so that the computer would not have any associated policy. This allowed the kiosk user to log in with only normal user rights. After starting SysInternals FileMon, the TV Tuner software was opened. After the error occurred, the captured the data in FileMon was examined. In this case we discover that there is a file to which we need to be able to write. NTFS permissions on that file were changed so that the local User group, which domain users are a member of by default, had write access to this file. This resolved the problem. A quicker but less precise solution would have been to just give write permission for Users to the applications entire directory.

Testing Netscape

Netscape 4.7x, which works fine for an account with advanced user rights, does not work correctly with the policy applied. When opening Netscape, it does not remember that a Netscape user profile has been created. Upon attempting to create a new profile, the program existed without error. Upon investigation I found that I did not have the correct permission to the file nsreg.dat which contains essential user profile information.

Netscape will also give the user an error whenever it does not have the permissions to write to the registry.

Fortunately, the yeoman's work has been completed. Chris Uhl has done testing with SysInternal's Regmon and Filemon and recorded the optimal settings into an inf file that can be imported through Security Configuration and Analysis.[8] First download a copy of Netscape security template. Once you have a security template, you are able to import the settings into to a Group Policy object. Once it is merged with the Kiosk computer Group Policy object, it can be applied to many computers at once, easing the administration burden.[9]

To import a security template to a Group Policy object:[10]

1. Open Active Directory, Users and Computers
2. Go to the Kiosk OU that you created. Select Properties and on the Group Policy Tab select the Kiosk Computers Group Policy and select edit.
3. Under Computer configuration go to Windows Settings and then Security Settings.
4. Right-click **Security Settings**.
5. Click **Import Policy**.
6. Click the Netscape476.inf security template.
7. Verify that Netscape still has an acceptable level of access for your environment.

After importing the Netscape Security Template, test Netscape and verify that you are now able to open Netscape without error and browse the web.

System Preparation

The systems are loaded with the standard desktop Windows 2000 ghost

[8] Uhl, Chris. "Netscape v4.7x under Windows 2000 User Account." [http://duke.usask.ca/~uhl/netscape/], July 5, 2001.

[9] Cone, Eric K., Jon Boggs and Sergio Perez. Planning for Windows 2000. New Rigers: Indianapolis, Indiana, 1999, p 250.

[10] Microsoft Corporation. "Security Templates; Overview." Microsoft Windows 2000 Help System, 1999.

load. Ghost is a system imaging software that is used to provide a standard system install in a minimum of time.

First, install the software. There are two ways to install the software. Log in a user with administrative rights and install the software. The second method is to install the software by right-clicking the software installation package and selecting "run-as." Normally this would allow the installation of software without taking the time to log out and log in as an administrator.

Evaluate the Template

In its introduction to the Group Policy templates, Microsoft says, "These scenarios are intended to be starting points from which you can develop settings that are tailored to your environment."[11] As much as we would like there to be one perfect template for every situation, this has not happened yet. If that were the case, each system would come already locked down or the configuration would be performed by mindless automatons. Fortunately for our paycheck, experience, intelligence and the ability to research are still key components to securing a computer.

Areas Where Template Too Strong

Account Policy

The default account policy in the template is stronger than my domain policy. The key to security on this kiosk computer is not safeguarding the password to the kiosk account. If they crack that password, what is gained? The account is locked down. The computer is logged in with that account already. I made this change just to have a uniform password policy. This is not a change to the original template that needs to be made for general use. The complex password requirement should still be followed on the local administrator account.

Account Policies		
Password Policy	**Template**	**Domain**

[11] "Windows 2000 Server: Using Group Policy Templates White Paper." [http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp]. September 2000, 1

Enforce password history	24 Passwords remembered	3 passwords remembered
Maximum password age	42 days	90 days
Minimum password age	2 days	zero days
Minimum password length	8 characters	
Passwords must meet complexity requirements of the installed password filter	Enabled	Not Defined
Store password using reversible encryption for all users in the domain	Disabled	
User must log on to change the password	Disabled	

Log on Banner

A Log On Banner is often used as an advisory to users of the machine. It reminds the user that the computer is not their property, the use of the system is monitored, and that their activity could result in criminal prosecution or termination of employment.

While a log on banner is advisable for most systems, having a logon banner can interfere with auto-logins. Since the point of a kiosk system is to offer the Web Browser and the TV Tuner, it is not a good idea to have the logon process halted. This is particularly true when the user will not be able to log in with their account.

By removing the logon banner, there is little loss of security. It would be rare that a user would see that logon banner anyway. Plus the banner merely reminds the user of the existing Policies that they have already agreed to anyway.

This is a case of good security principle not being applicable to every situation. If your kiosk is something that users can individually log into, then yes, you need a log on banner. The definition of a kiosk tends to assume one account that is always logged into the computer. In this environment, the log on banner is not needed.

Unsigned driver installation behavior

In Windows 2000, Microsoft attempts to improve the stability of the operating system by discouraging the use of drivers that have not been tested and approved by Microsoft. This driver testing process costs time

and money for hardware manufacturers. As a result generally the only signed drivers you will find are on the Operating System CD. To be able to install the drivers for the video card, it is necessary to change the value for unsigned driver installation behavior from Block to Ask. This change should not significantly effect security. This change should be made in the template by all users.

Desktop

The Kiosk Group Policy by default removes all items from the desktop. Since my kiosk computer allows the user access to multiple applications, this is not the best configuration. Instead of hiding all icons on the desktop, enable the hiding of Network Neighborhood and My Computer. Other Icons can be selectively removed from the user profile. Users only have icons for programs they are able to access. This change was made for the specifics of my environment. If you are using the kiosk template and still allowing the user to run multiple applications, then you need to make this modification.

Custom User Interface

The Kiosk Group Policy is intended to be used with only one user and one application. As such, it is set to open Internet Explorer as its shell. In this environment, we will remove that setting so that the computer could be used for multiple applications. If you are using the kiosk template and still allowing the user to run multiple applications, then you need to make this modification.

Areas Where Template Too Weak

User Rights Assignment

The template does not place any restriction on user rights assignment. The User Rights Assignment component of the policy controls what users are able to do. Items such as who can access the computer from the network, log on locally, or shut down the system can be assigned through the User Rights Assignment portion of Group Policy.

The *Log on Locally* User Rights Assignment can be used to insure that only specific people are able to log into the computer. If you recall, I left the *Log Off* button available to the kiosk users. If the *Log On Locally*

permission were available to everyone, then any user could log off the restricted user and use the Kiosk computer for whatever they wanted. They would be able to download proprietary documents and leave them on a public computer. They would be able to download hacking tools and cause havoc on the computer systems. Even a user with only a modicum of knowledge could log in using someone else's ID and a bogus password until the lockout threshold is reached. This mild denial of service attack would disturb the owner of the target account and the only log trail would lead to what is basically an anonymous workstation.

Now you may say, if it is such a risk for a user to be able to log into this station, then why have the Log Off option available at all. Even if the Log Off option were not available, a knowledgeable user would be able to access the log on prompt by forcing a reboot and then holding down the shift key during the boot sequence.[12]

The solution then is to set the *Log on Locally* User Rights Assignment to include the kiosk user account, the local administrators account and any other Kiosk Administrators. Preferably create a group for kiosk administrators at the domain level, and add it to the list.

This functionality has been verified in the Test the Template section of this paper. This change is applicable to all users of the kiosk template. It is recommended that all users make this change to increase security.

How template affects applications

When we tested the system functionality after applying the template, we saw that security settings can have unexpected results. Programs can behave in a peculiar manner when they don't have free range to do what they want on a system.

Internet Explorer
Internet Explorer, as expected, worked flawlessly in a restricted environment. Netscape and the Matrox Marvel TV Tuner card, on the other hand, offered a difficult challenge.

Netscape

[12] Microsoft Corporation. Group Policy Senarios White Paper. Microsoft Corp: Redmond Washington, 28.

Netscape requires changes to the Registry and NTFS permissions in order to perform correctly. This fix does affect security. The kiosk user now has access to Netscape Mail and is able to save the configuration. To keep the users from being able to use Netscape Messenger, change the prefs.js file to be read only. This will keep the mail settings from being configurable.

Matrox TV-Tuner Card

The Matrox TV Tuner card presented initial difficulties in installation and use as outlined earlier. Fortunately most of these changes are one time changes that have little effect on the day to day use of the product.

There is a file permission change affecting the file that records the favorite channels available to the user. The "scan for available channels" can only be performed by someone with power user rights. The only time this would come into play is if the channel lineup changes. Since this is an internal cable system, it is not likely that the channel lineup will change.

Areas for Improvement in the Template

User Rights Assignment

The entire area of user rights assignment needs to be addressed in this template. In the table, I have included an example configuration for user rights assignment in a secure area. Since this computer will be on the corporate network controlling access to the computer from the network is of primary concern. Now, some of these things are only available to the system administrator to begin with. There is no cost associated with being explicit in your permission assignments.

User Rights Assignment[13]

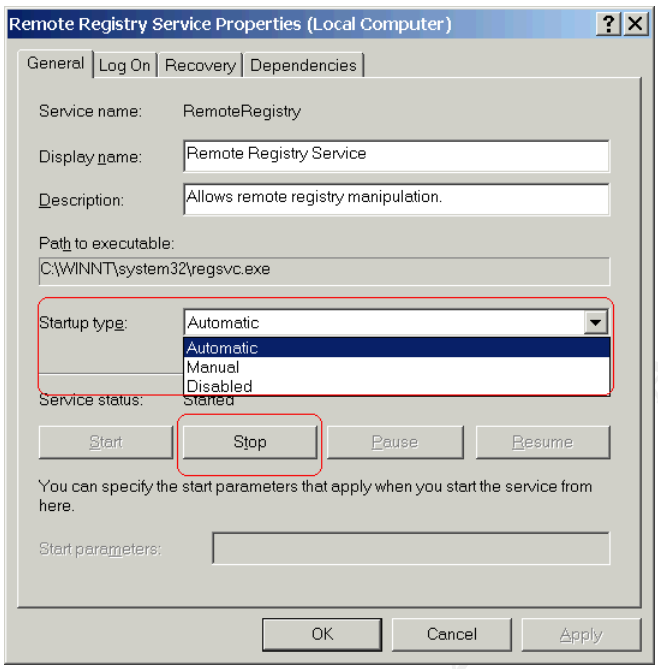
Access this computer from the network	Administrators, Users
Act as part of the operating system	No One
Add workstations to domain	No One - Administrators don't need explicit rights
Back up files and directories	Administrators
Bypass traverse checking	Authenticated Users
Change the system time	Administrators

[13] Taken from an internal computer configuration guide.

Create a page file	Administrators
Create a token object	No one
Create permanent shared objects	No one
Debug programs	No one
Deny access to this computer from the network	No One
Deny logon as a batch job	No One
Deny logon as a service	No One
Deny logon locally	No One
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	No One
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	No One
Log on as a batch job	No One - Task Scheduler will automatically give Administrators this right when tasks are scheduled.
Log on as a service	No One
Log on locally	Administrators, kiosk user
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	No One
Replace a process level token	No One
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	No One
Take ownership of files or other objects	Administrators

Unneeded Services

Windows 2000 comes installed with many services that run automatically. Many of these services are only needed in specific situations and should be disabled if they are not used. Unneeded services can be unnecessary potential security problems. NIST points out that it is best to uninstall unneeded services from the system by using Add/ Remove programs in the control panel.[14] If it cannot be uninstalled, select **Start -> Programs -> Administrative Tools -> Services**. Open the properties for the selected service. Stop the Service and change the start up type to disabled.



To add this change into the group policy, open the computer configuration. Go to Windows Settings -> Security Settings -> System Services. Select the appropriate service, select define this policy, set it to disabled and through security control who can start the service again.

Disable the Messenger service. The Messenger service sends pop up alerts to the console of a Windows computer. It is unlikely this service will be used in this environment

The Remote Registry Service allows the registry to be accessed remotely by administrators. It is a good idea to disable this service. In our environment, we have left this enabled to allow administrators to work with the kiosk

[14] System Administration Guidance for Securing Microsoft Windows 2000 Professional System. National Institute of Standards and Technology. January 2002, 47.

computers remotely.

The Runas service allows the logged on user to run a program as someone else. The kiosk user is not able to right click to access the run as option or run it through the command prompt. Disable this service.

The Server service allows the computer to share files. In our environment, it is helpful for an Administrator to access the administrative share remotely. In an environment with more restrictive security requirements, this service must be disabled.

The Fax Service allows faxes to be sent or received. This is not necessary on a kiosk computer and the service should be disabled.

The Indexing service indexes the files on the hard drive to allow for rapid searching of the hard drive. Since the kiosk user is not allowed access to this functionality, the service should be disabled.

Restrictions on Group Membership

Group Policy allows us to determine group memberships. If at a later date someone is added into the administrator group, for example, group policy will change the membership back to the preconfigured list. Open the Group Policy and Computer Configuration. Go to Windows Settings -> Security Settings -> Restricted Groups. Right Click Restricted Groups and select Add Group. Add the administrators group as the group to be managed. Then specify all members of the group such as administrator, domain\domain admins, domain\kiosk administrators.

Restricting Ports

Restricting ports will have the result of keeping users from doing what you do not want them to do and keeping remote systems from doing anything on those ports.

Although it cannot be deployed via group policy, Windows 2000 offers built in TCP-IP Port Filtering. To enable this feature open the TCP-IP properties on the Network Adaptor, select the Advanced, and Options. Select TCP/IP Filtering and select Properties. Select the ports that require access. Note that this will require extensive testing. Also it is highly likely that any changes in the future may have problems because the right port isn't opened.

IPSec provides a way to restrict ports via Group Policy which allows for easier configuration. It also allows the port restrictions to apply to specific IP addresses. IPSec uses IP filtering to encrypt or ignore specific packets. The downside is that without the use of a network interface card specifically designed to process IPSec traffic, the CPU of the computer will be used quite a bit.

Areas not covered by the template

As good as the template is, there are areas that it is just not designed to cover. Some things cannot be secured automatically. It would be helpful if there was a checklist that went with this group policy template. It could discuss basic security concepts and requirements that couldn't possibly be included in a template.

Physical Security

The kiosk computer needs to be secured against possible theft and tampering. The failure to physically secure the computer could allow booting into an alternate operating system or all kinds of physical attacks on the computer. We have protected the computer against this form of attack by locking them in cabinets designed for that purpose. Be aware that proper airflow is an important requirement to avoid overheating the computer.

Anti-Virus

Anti-Virus software and the ability to update it is a requirement on any Windows based computer system. On this system, Norton Anti-Virus Corporate Edition version 7.61 is used. Its settings are locked down and controlled through a central server by using the Symantec System Console, which is a MMC plug-in. Updates are driven by an internal live update server. If any viruses are detected, a warning appears on the screen and an email is sent to the system administrators.

Patching

Patching applications and Operating System components is required for security. This is not addressed in the template. Anyone responsible for a system should be on the relevant security mailing lists such as so they are

notified when new patches are available. NTBugtraq (www.ntbugtraq.com) or Microsoft Security Bulletins (http://www.microsoft.com/technet/security/bulletin/notify.asp) are two good lists for a Windows System Administrator. Patches should be tested prior to being applied in the production environment. There are many ways to deploy patches; Login Scripts, SMS, Microsoft Software Update Services, etc. If possible use the same update mechanism that you use for your other desktop clients.

Removal of OS2 and POSIX

Windows 2000 includes support for down-level clients. Backwards compatibility often introduces vulnerabilities. Since there is no real need for the OS2 and POSIX clients, it is recommended that they be removed through the following process.[15]

Files
First delete os2.exe, os2ss.exe and os2srv.exe from %system root%\dllcache.
Next remove os2.exe, os2ss.exe, os2srv.exe, psxss.exe and posix.exe same files from the %system root% directory.

Registry Keys
Delete the following keys from the HKEY_Local_Machine hive.
\System\CurrentControlSet\Control\Session Manager\Environment\OS2LibPath
\System\CurrentControlSet\Control\Session Manager\Subsystem\Optional
\System\CurrentControlSet\Control\Session Manager\Subsystem\OS2
\System\CurrentControlSet\Control\Session Manager\Subsystem\POSIX

Removal of OS2 and POSIX should occur when originally imaging the computer. There is no Group Policy item to implement this security.

Further Research

This template does not include registry or file system permissions. This environment does not warrant this level of security. If your environment requires stricter security standards, this should be addressed.

[15] System Administration Guidance for Securing Microsoft Windows 2000 Professional System. National Institute of Standards and Technology. January 2002. 39.

Summary

The Microsoft Kiosk Group Policy does not purport to be the be all and end all of security. It is a good starting point in securing a system. For administrators that need to configure a system quickly, a template is a good place to start. With the MSI file located at http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp, you get a white paper describing how to make the templates available in group policy, the policy files and excel files with the discrete settings for 6 templates.

As I have shown, any restriction of rights requires hours of testing to make sure that all necessary software will work in a restricted environment. Administrators need to have knowledge and consult the standard security lists. The template provides a good start to securing the computer against attacks at the console.

It would be helpful if there was a security checklist written specifically with this kiosk template in mind. The template leaves many important security areas uncovered. By itself, this template could be used in a corporate environment that is moderately well controlled. If the computer were to be place in a more open location, it should be locked down much more intently.

References

Cone, Erik K., Jon Boggs and Sergio Perez. Planning for Windows 2000. Indianapolis, In: New Riders, 1999.

"Windows 2000 Server: Using Group Policy Templates White Paper." [http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicy.asp]. September 2000.

"Microsoft Software Update Services FAQ." [http://www.microsoft.com/windows2000/windowsupdate/sus/susfaq.asp]. June 2002.

Microsoft Corporation. "Security Templates: Overview." Microsoft Windows 2000 Help System, 1999.

"The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus" [http://www.sans.org/top20/#W8], October 2002.

"Software Update Services Deployment Whitepaper." [http://www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp]. June 2002.

System Administration Guidence for Securing Microsoft Windows 2000 Professional System: Recommendations of the National Institute of Standards and Technology. Washington, DC: US Government Printing Office, 2002

Uhl, Chris. "Netscape v4.7x under Windows 2000 User Account." [http://duke.usask.ca/~uhl/netscape]. July 2001.

Appendix

Group Policy Settings	
GPO Name	Kiosk Settings
Domain	
GPO Version	

Policy	Setting
Computer Configuration	
Windows Settings	
Security Settings	
Restricted Groups	
System Services	
Registry	
File System	
Account Policies	
Password Policy	
Enforce password history	24 Passwords remembered
Maximum password age	42 days
Minimum password age	2 days
Minimum password length	8 characters
Passwords must meet complexity requirements of the installed password filter	Enabled
Store password using reversible encyrption for all users in the domain	Disabled
User must log on to change the password	Disabled
Account Lockout Policy	
Account lockout threshold	0 min
Account lockout duration	5 invalid logon attempts
Reset account lockout counter after	30 minutes
Kerberos Policy	
Enforce user logon restrictions	
Maximum lifetime for service ticket	

Maximum lifetime for user ticket	
Maximum lifetime for user ticket renewal	
Maximum tolerance for computer clock synchronization	
Local Policies	
Audit Policy	
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure
User Rights Assignment	
Access this computer from the network	
Act as part of the operating system	
Add workstations to domain	
Back up files and directories	
Bypass traverse checking	
Change the system time	
Create a pagefile	
Create a token object	
Create permanent shared objects	
Debug programs	
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	
Enable computer and user accounts to be trusted for delegation	

	Force shutdown from a remote system	
	Generate security audits	
	Increase quotas	
	Increase scheduling priority	
	Load and unload device drivers	
	Lock pages in memory	
	Log on as a batch job	
	Log on as a service	
	Log on locally	
	Manage auditing and security log	
	Modify firmware environment variables	
	Profile single process	
	Profile system performance	
	Remove computer from docking station	
	Replace a process level token	
	Restore files and directories	
	Shut down the system	Administrators
	Synchronize directory service data	
	Take ownership of files or other objects	
Security Options		
	Additional restrictions for anonymous connections	No access without explicit anonymous permiss
	Allow server operators to schedule tasks (domain controllers only)	
	Allow system to be shut down without having to log on	Disabled
	Allowed to eject removable NTFS media	Administrators
	Amount of idle time required before disconnecting a session	15 minutes
	Audit the access of global system objects	Disabled
	Audit use of Backup and Restore privilege	Disabled

	Automatically log off users when logon time expires	
	Automatically log off users when logon time expires (local)	Enabled
	Clear virtual memory pagefile when system shuts down	Enabled
	Digitally sign client communications (always)	Enabled
	Digitally sign client communications (when possible)	Enabled
	Digitally sign server communications (always)	Enabled
	Digitally sign server communications (when possible)	Enabled
	Disable CTRL+ALT+DEL requirement for logon	Disabled
	Do not display last user name in logon screen	Enabled
	LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NT
	Message text for users attempting to log on	Only authorized users of this machine should log on.
	Message title for users attempting to log on	Warning!
	Number of previous logons to cache (in case domain controller is not available)	0 logons
	Prevent system maintenance of computer account password	Disabled
	Prevent users from installing printer drivers	Enabled
	Prompt user to change password before expiration	14 days
	Recovery console: Allow automatic administrative logon	Disabled
	Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
	Rename administrator account	%Admin!!!
	Rename guest account	%Guest!!!
	Restrict CD-ROM access to locally logged-on user only	Enabled
	Restrict floppy access to locally logged-on user only	Enabled

	Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
	Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
	Secure channel: Digitally sign secure channel data (when possible)	Enabled
	Secure channel: Require strong (Windows 2000 or later) session key	Enabled
	Secure system partition (for RISC platforms only)	
	Send unencrypted password to connect to third-party SMB servers	Disabled
	Shut down system immediately if unable to log security audits	Disabled
	Smart card removal behavior	Lock Workstation
	Strengthen default permissions of global system objects (e.g. Symbolic links)	Enabled
	Unsigned driver installation behavior	Do not allow installation
	Unsigned non-driver installation behavior	Do not allow installation
Event Log		
Settings for Event Logs		
	Maximum application log size	10240 kilobytes
	Maximum security log size	20480 kilobytes
	Maximum system log size	10240 kilobytes
	Restrict guest access to application log	Enabled
	Restrict guest access to security log	Enabled
	Restrict guest access to system log	Enabled
	Retain application log	
	Retain security log	
	Retain system log	
	Retention method for application log	As needed
	Retention method for security log	As needed

	Retention method for system log	As needed
	Shut down the computer when the security audit log is full	
IP Security Policies		
	Client	Assigned
Administrative Templates		
Windows Components		
NetMeeting		
	Disable remote Desktop Sharing	Enabled
Internet Explorer		
	Security Zones: Use only machine settings	
	Security Zones: Do not allow users to change policies	Enabled
	Security Zones: Do not allow users to add/delete sites	Enabled
	Make proxy settings per-machine (rather than per-user)	
	Disable Automatic Install of Internet Explorer components	Enabled
	Disable Periodic Check for Internet Explorer software updates	Enabled
	Disable software update shell notifications on program launch	Enabled
	Disable showing the splash screen	Enabled
Task Scheduler		
	Hide Property Pages	Enabled
	Prevent Task Run or End	Enabled
	Disable Drag-and-Drop	Enabled
	Disable New Task Creation	Enabled
	Disable Task Deletion	Enabled
	Disable Advanced Menu	Enabled
	Prohibit Browse	Enabled
Windows Installer		
	Disable Windows Installer	
	Always install with elevated privileges	

	Disable rollback	
	Disable browse dialog box for new source	Enabled
	Disable patching	
	Disable IE security prompt for Windows Installer scripts	
	Enable user control over installs	
	Enable user to browse for source while elevated	
	Enable user to use media source while elevated	
	Enable user to patch elevated products	
	Allow admin to install from Terminal Services session	
	Cache transforms in secure location on workstation	
	Logging	
System		
	Remove security option from Start menu (Terminal Services only)	
	Remove Disconnect item from Start menu (Terminal Services only)	
	Disable Boot / Shutdown / Logon / Logoff status messages	
	Verbose vs normal status messages	
	Disable Autoplay	Enabled
	Don't display welcome screen at logon	Enabled
	Run these programs at user logon	Disabled
	Disable the run once list	Disabled
	Disable legacy run list	Disabled
	Do not automatically encrypt files moved to encrypted folders	
	Download missing COM components	
Logon		
	Run logon scripts synchronously	Enabled
	Run startup scripts asynchronously	

	Run startup scripts visible	
	Run shutdown scripts visible	
	Maximum wait time for Group Policy scripts	
	Delete cached copies of roaming profiles	
	Do not detect slow network connections	
	Slow network connection timeout for user profiles	
	Wait for remote user profile	
	Prompt user when slow link is detected	
	Timeout for dialog boxes	
	Log users off when roaming profile fails	
Disk Quotas		
	Enable disk quotas	
	Enforce disk quota limit	
	Default quota limit and warning level	
	Log event when quota limit exceeded	
	Log event when quota warning level exceeded	
	Apply policy to removable media	
DNS Client		
	Primary DNS Suffix	
Group Policy		
	Disable background refresh of Group Policy	
	Apply Group Policy for computers asynchronously during startup	
	Apply Group Policy for users asynchronously during logon	
	Group Policy refresh interval for computers	
	Group Policy refresh interval for domain controllers	
	User Group Policy loopback processing mode	
	Group Policy slow link detection	

	Registry policy processing	
	Internet Explorer Maintenance policy processing	
	Software Installation policy processing	
	Folder Redirection policy processing	
	Scripts policy processing	
	Security policy processing	
	IP Security policy processing	
	EFS recovery policy processing	
	Disk Quota policy processing	
Windows File Protection		
	Set Windows File Protection scanning	
	Hide the file scan progress window	
	Limit Windows File Protection cache size	
	Specify Windows File Protection cache location	
Network		
Offline files		
	Enabled	Disabled
	Disable user configuration of Offline Files	Enabled
	Synchronize all offline files before logging off	
	Default cache size	
	Action on server disconnect	
	Non-default server disconnect actions	
	Disable "Make Available Offline"	Enabled
	Prevent use of Offline Files folder	Enabled
	Files not cached	
	Administratively assigned offline files	
	Disable reminder balloons	
	Reminder balloon frequency	
	Initial reminder balloon lifetime	
	Reminder balloon lifetime	

	At logoff, delete local copy of user's offline files	
	Event logging level	
Network & Dial-up Connections		
	Allow configuration of connection sharing	Disabled
Printers		
	Allow printers to be published	
	Automatically publish new printers in Active Directory	
	Allow pruning of published printers	
	Printer browsing	
	Prune printers that are not automatically republished	
	Directory pruning interval	
	Directory pruning retry	
	Directory pruning priority	
	Check published state	
	Web-based printing	
	Custom support URL in the Printers folder's left pane	
	Computer location	
	Pre-populate printer search location text	
User Configuration		
Windows Settings		
Internet Explorer Maintenance		
Connection		
	Connection Settings	
Administrative Templates		
Windows Components		
NetMeeting		
	Enable Automatic Configuration	
	Disable Directory services	
	Prevent adding Directory servers	

	Prevent viewing Web directory	
	Set the intranet support Web page	
	Set the NetMeeting home page	
	Set Call Security options	
	Prevent changing Call placement method	
	Prevent automatic acceptance of Calls	
	Prevent sending files	
	Prevent receiving files	
	Limit the size of sent files	
	Disable Chat	
	Disable NetMeeting 2.x Whiteboard	
	Disable Whiteboard	
Application Sharing		
	Disable application Sharing	
	Prevent Sharing	
	Prevent Desktop Sharing	
	Prevent Sharing Command Prompts	
	Prevent Sharing Explorer windows	
	Prevent Control	
	Prevent Application Sharing in true color	
Audio & Video		
	Limit the bandwidth of Audio and Video	
	Disable Audio	
	Disable full duplex Audio	
	Prevent changing DirectSound Audio setting	
	Prevent sending Video	
	Prevent receiving Video	
Options Page		
	Hide the General page	
	Disable the Advanced Calling button	
	Hide the Security page	

	Hide the Audio page	
	Disable the Advanced Audio button	
	Hide the Video page	
Internet Explorer		
	Search: Disable Search Customization	Enabled
	Search: Disable Find Files via F3 within the browser	Enabled
	Disable external branding of Internet Explorer	Enabled
	Disable importing and exporting of favorites	Enabled
	Disable changing Advanced page settings	Enabled
	Disable changing home page settings	Enabled
	Use Automatic Detection for dial-up connections	Enabled
	Disable caching of Auto-Proxy scripts	
	Display error message on proxy script download failure	
	Disable changing Temporary Internet files settings	Enabled
	Disable changing history settings	Enabled
	Disable changing color settings	Enabled
	Disable changing link color settings	Enabled
	Disable changing font settings	Enabled
	Disable changing language settings	Enabled
	Disable changing accessibility settings	Enabled
	Disable Internet Connection wizard	Enabled
	Disable changing connection settings	Enabled
	Disable changing proxy settings	Enabled
	Disable changing Automatic Configuration settings	Enabled
	Disable changing ratings settings	Enabled
	Disable changing certificate settings	Enabled

	Disable changing Profile Assistant settings	Enabled
	Disable AutoComplete for forms	Enabled
	Do not allow AutoComplete to save passwords	Enabled
	Disable changing Messaging settings	Enabled
	Disable changing Calendar and Contact settings	Enabled
	Disable the Reset Web Settings feature	Enabled
	Disable changing default browser check	Enabled
	Identity Manager: Prevent users from using Identities	Enabled
Internet Control Panel		
	Disable the General page	Enabled
	Disable the Security page	Enabled
	Disable the Content page	Enabled
	Disable the Connections page	Enabled
	Disable the Programs page	Enabled
	Disable the Advanced page	Enabled
Offline Pages		
	Disable adding channels	Enabled
	Disable removing channels	Enabled
	Disable adding schedules for offline pages	Enabled
	Disable editing schedules for offline pages	Enabled
	Disable removing schedules for offline pages	Enabled
	Disable offline page hit logging	Enabled
	Disable all scheduled offline pages	Enabled
	Disable channel user interface completely	Enabled
	Disable downloading of site subscription content	Enabled
	Disable editing and creating of schedule groups	Enabled
	Subscription Limits	Disabled
Browser menus		

	File menu: Disable Save As... menu option	Enabled
	File menu: Disable New menu option	Enabled
	File menu: Disable Open menu option	Enabled
	File menu: Disable Save As Web Page Complete	Enabled
	File menu: Disable closing the browser and Explorer windows	Enabled
	View menu: Disable Source menu option	
	View menu: Disable Full Screen menu option	
	Hide Favorites menu	Enabled
	Tools menu: Disable Internet Options... menu option	Enabled
	Help menu: Remove 'Tip of the Day' menu option	Enabled
	Help menu: Remove 'For Netscape Users' menu option	Enabled
	Help menu: Remove 'Tour' menu option	Enabled
	Help menu: Remove 'Send Feedback' menu option	Enabled
	Disable Context menu	Enabled
	Disable Open in New Window menu option	
	Disable Save this program to disk option	Enabled
Toolbars		
	Disable customizing browser toolbar buttons	Enabled
	Disable customizing browser toolbars	Enabled
	Configure Toolbar Buttons	Enabled
Persistance Behavior		
	File size limits for Local Machine zone	
	File size limits for Intranet zone	
	File size limits for Trusted Sites zone	
	File size limits for Internet zone	
	File size limits for Restricted Sites zone	
Administrator Approved Controls		

Databinding	
RDS	
TDC	
XML	
Internet Explorer	
Active Setup	
Media Player	
Extras	
Menu Controls	
Microsoft Agent	
Microsoft Chat	
Webpost	
MSN	
Cache Preloader	
Carpoint	
Install	
Investor	
MSNBC	
Music	
Quick View Access	
Windows Explorer	Following settings should not be needed as a shell is used
Enable Classic Shell	
Remove the Folder Options menu item from the Tools menu	Enabled
Remove File menu from Windows Explorer	Enabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Remove Search button from Windows Explorer	Enabled
Disable Windows Explorer's default context menu	Enabled
Hides the Manage item on the Windows Explorer context menu	Enabled
Only allow approved Shell extensions	Enabled

	Do not track Shell shortcuts during roaming	
	Hide these specified drives in My Computer	Enabled
	Prevent access to drives from My Computer	Enabled
	Hide Hardware tab	Enabled
	Disable UI to change menu animation setting	Enabled
	Disable UI to change keyboard navigation indicator setting	Enabled
	Disable DFS Tab	Enabled
	No "Computers Near Me" in My Network Places	Enabled
	No "Entire Network" in My Network Places	Enabled
	Maximum number of recent documents	
	Do not request alternate credentials	Enabled
	Request credentials for network installations	
Common Open File Dialog		
	Hide the common dialog places bar	Enabled
	Hide the common dialog back button	
	Hide list of recently used files	Enabled
Microsoft Management Console		
	Restrict the user from entering author mode	Enabled
	Restrict users to the explicitly permitted list of snap-ins	Enabled
Restricted/Permitted snap-ins		
	Active Directory Users and Computers	
	Active Directory Domains and Trusts	

	Active Directory Sites and Services	
	Certificates	
	Computer Management	
	DCOM Config	
	Device Manager	
	Disk Management	
	Disk Defragmenter	
	Distributed File System	
	Event Viewer	
	FAX Service	
	Indexing Service	
	Internet Authentication Service (IAS)	
	IAS Logging	
	Internet Information Services	
	IP Security	
	Local Users and Groups	
	Performance Logs and Alerts	
	QoS Admission Control	
	Removable Storage Management	
	Routing and Remote Access	
	Security Configuration and Analysis	
	Security Templates	
	Services	
	Shared Folders	
	System Information	
	Telephony	
Extension snap-ins		
	AppleTalk Routing	
	Certification Authority	
	Component Services	
	Connection Sharing (NAT)	
	Device Manager	
	DHCP Relay Management	

	Event Viewer	
	FAX Service	
	IGMP Routing	
	IP Routing	
	IPX RIP Routing	
	IPX Routing	
	IPX SAP Routing	
	Logical and Mapped Drives	
	OSPF Routing	
	Public Key Policies	
	RAS Dialin - User Node	
	Remote Access	
	Removable Storage	
	RIP Routing	
	Routing	
	Send Console Message	
	Service Dependencies	
	SMTP Protocol	
	SNMP	
	System Properties	
Group Policy		
	Group Policy snap-in	
	Group Policy Tab for Active Directory Tools	
	Administrative Templates (Computers)	
	Administrative Templates (Users)	
	Folder Redirection	
	Remote Installation Services	
	Scripts (Logon/Logoff)	
	Scripts (Startup/Shutdown)	
	Security Settings	
	Software Installation (Computers)	
	Software Installation (Users)	
Task Scheduler		

	Hide Property Pages	Enabled
	Prevent Task Run or End	Enabled
	Disable Drag-and-Drop	Enabled
	Disable New Task Creation	Enabled
	Disable Task Deletion	Enabled
	Disable Advanced Menu	Enabled
	Prohibit Browse	Enabled
Windows Installer		
	Always install with elevated privileges	
	Search order	
	Disable rollback	
	Disable media source for any install	Enabled
Start Menu & Taskbar		Following settings should not be needed as a shell is used
	Remove user's folders from the Start Menu	Enabled
	Disable and remove links to Windows Update	Enabled
	Remove common program groups from Start Menu	Enabled
	Remove Documents menu from Start Menu	Enabled
	Disable programs on Settings menu	Enabled
	Remove Network and Dial-up Connections from Start Menu	Enabled
	Remove Favorites menu from Start Menu	Enabled
	Remove Search menu from Start Menu	Enabled
	Remove Help menu from Start Menu	Enabled
	Remove Run menu from Start Menu	Enabled
	Add Logoff to the Start Menu	

	Disable Logoff on the Start Menu	
	Disable and remove the Shut Down command	Enabled
	Disable drag-and-drop context menus on the Start Menu	Enabled
	Disable changes to Taskbar and Start Menu Settings	Enabled
	Disable context menu for taskbar	Enabled
	Do not keep history of recently opened documents	Enabled
	Clear history of recently opened documents on exit	Enabled
	Disable personalized menus	Enabled
	Disable user tracking	
	Add "Run in Separate Memory Space check box" to Run dialog box	
	Do not use the search-based method when resolving shell shortcuts	
	Do not use the tracking-based method when resolving shell shortcuts	
	Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled
Desktop		
	Hide all icons on Desktop	Enabled
	Remove My Documents icon from Start Menu	Enabled
	Remove My Documents icon Start Menu	Enabled
	Hide My Network Places icon on desktop	
	Hide Internet Explorer icon on desktop	
	Do not add shares from recently opened documents to the My Network Places folder	Enabled
	Prohibit user from changing My Documents path	Enabled
	Disable adding, dragging, dropping and closing the Taskbar's toolbars	Enabled

	Disable adjusting desktop toolbars	Enabled
	Don't save settings at exit	Enabled
Active Directory		
	Maximum size of Active Directory searches	
	Enable filter in Find dialog box	
	Hide Active Direcotry folder	
Active Desktop		
	Enable Active Desktop	
	Disable Active Desktop	Enabled
	Prohibit changes	
	Disable all items	
	Prohibit adding items	
	Prohibit editing items	
	Prohibit deleting items	
	Prohibit editing items	
	Add/Delete items	
	Active Desktop Wallpaper	
	Allow only bitmapped wallpaper	
Control Panel		
	Disable Control Panel	Enabled
	Show only specified control panel applets	
	Hide specified control panel applets	
Add/Remove Programs		
	Disable Add/Remove Programs	Enabled
	Hide Change or Remove Programs page	
	Hide Add New Programs page	
	Hide Add/Remove Windows Components page	
	Hide the "Add a program from CD-ROM or floppy disk" option	
	Hide the "Add programs from Microsoft" option	
	Hide the "Add programs from your network" option	

	Go directly to Components wizard	
	Disable Support Information	
	Specify default category for Add New Programs	
Display		
	Disable Display in Control Panel	Enabled
	Hide Background tab	
	Disable changing wallpaper	
	Hide Appearance tab	
	Hide Settings tab	
	Hide Screen Saver tab	
	No screen saver	
	Screen saver executable name	Enabled
	Password protect the screen saver	
Printers		
	Disable deletion of printers	Enabled
	Disable addition of printers	Enabled
	Browse the network to find printers	
	Default Active Directory path when searching for printers	
	Browse a common web site to find printers	
Regional Options		
	Restrict selection of Windows 2000 menus and dialogs language	
Network		
Offline Files		
	Disable user configuration of Offline Files	Enabled
	Synchronize all offline files before logging off	
	Action on server disconnect	
	Non-default server disconnect actions	
	Disable "Make Available Offline"	Enabled
	Prevent use of Offline Files Folder	Enabled
	Disable reminder balloons	

	Reminder balloon frequency	
	Initial reminder balloon lifetime	
	Reminder balloon lifetime	
	Event logging level	
Network and Dial-up Connections		
	Enable deletion of RAS connections	Disable
	Enable deletion of RAS connections available to all users	Disable
	Enable connecting and disconnecting a RAS connection	Disable
	Enable connecting and disconnecting a LAN connection	Disable
	Enable access to properties of a LAN connection	Disable
	Allow access to current user's RAS connection properties	Disable
	Enable access to properties of RAS connections available to all users	Disable
	Enable renaming of connections, if supported	Disable
	Enable renaming of RAS connections belonging to the current user	Disable
	Enable adding or removing components of a RAS or LAN connection	Disable
	Allow connection components to be enabled or disabled	Disable
	Enable access to properties of components of a LAN connection	Disable
	Enable access to properties of components of a RAS connection	Disable
	Display and enable the Network Connection wizard	Disable
	Enable status statistics for an active connection	Disable
	Enable the Dial-up Preferences item on the Advanced menu	Disable
	Enable the Advanced Settings item on the Advanced menu	Disable

	Allow configuration of connection sharing	Disable
	Allow TCP/IP advanced configuration	Disable
System		
	Don't display welcome screen at logon	Enabled
	Century interpretation for Year 2000	
	Code signing for device drivers	
	Custom user interface	Enabled
	Disable the command prompt	Enabled
	Disable registry editing tools	Enabled
	Run only allowed Windows applications	
	Don't run specified Windows applications	
	Disable Autoplay	Enabled
	Download missing COM components	
Logon/Logoff		
	Disable Task Manager	Enabled
	Disable Lock Computer	Enabled
	Disable Change Password	Enabled
	Disable Logoff	
	Run logon scripts synchronously	Enabled
	Run legacy logon scripts hidden	
	Run logon scripts visible	
	Run logoff scripts visible	
	Connect home directory to root of the share	
	Limit profile size	
	Exclude directories in roaming profile	
	Run these programs at user logon	
	Disable the run once list	Enabled
	Disable legacy run list	Enabled
Group Policy		
	Group Policy refresh interval for users	
	Group Policy slow link detection	

	Group Policy domain controller selection	
	Create new Group Policy object links disabled by default	
	Enforce Show Policies Only	
	Disable automatic update of ADM files	